
NSFOCUS WAF V6.0

User Guide



Version: V6.0R07F03 (2020-6-10)

© 2020 NSFOCUS

■ Copyright © 2018 NSFOCUS Technologies, Inc. All rights reserved.

Unless otherwise stated, **NSFOCUS Technologies, Inc.** holds the copyright for the content of this document, including but not limited to the layout, figures, photos, methods, and procedures, which are protected under the intellectual property and copyright laws. No part of this publication may be reproduced or quoted, in any form or by any means, without prior written permission of **NSFOCUS Technologies, Inc.**

Contents

Preface	1
Scope.....	1
Audience	1
Organization.....	1
Conventions	2
Customer Support.....	2
1 Product Introduction	3
1.1 Overview	3
1.2 Typical Application	4
1.3 Typical Deployment	5
2 Overview of the Web-based Manager	7
2.1 Login	7
2.2 System Users.....	9
2.3 Layout of the Web-Based Manager	10
2.4 Common Operations	11
3 System Monitoring	13
3.1 Overview	14
3.2 Security Event Data.....	16
3.2.1 Viewing Real-Time Data.....	16
3.2.2 Querying Historical Data	17
3.3 Service Loads.....	18
3.3.1 Viewing Real-Time Data.....	18
3.3.2 Querying Historical Data	19
3.4 Interface Traffic Data	20
3.4.1 Viewing Real-Time Data.....	21
3.4.2 Querying Historical Data	21
3.5 System Loads	23
3.5.1 Viewing Real-Time Data.....	23
3.5.2 Querying Historical Data	23
3.6 IP Block Management	24
3.7 Website Access Statistics.....	25
3.7.1 Viewing Real-Time Data.....	25
3.7.2 Querying Historical Data	26

3.8 Traffic Control Data	28
3.8.1 Viewing Real-Time Data	28
3.8.2 Querying Historical Data	28
3.9 Server Status Check	29
3.9.1 Viewing Real-Time Status	29
3.9.2 Configuring the Server Status Check Function	31
3.10 Device Monitoring	32
3.11 System Information	34
4 Security Management.....	36
4.1 Overview	36
4.2 Network-Layer Protection	38
4.2.1 Enabling/Disabling Policies	38
4.2.2 Configuring Network-Layer Access Control	39
4.2.3 Configuring TCP Flood Protection	42
4.2.4 Configuring ARP Spoofing Protection	43
4.2.5 Configuring WAF-ADS Collaboration	46
4.3 Website Protection	53
4.3.1 Managing Website Groups	54
4.3.2 Managing Websites	65
4.3.3 Managing Virtual Websites	96
4.4 Auto-Learning Policies	104
4.4.1 Creating an Auto-Learning Policy	104
4.4.2 Editing an Auto-Learning Policy	105
4.4.3 Deleting an Auto-Learning Policy	106
4.4.4 Enabling an Auto-Learning Policy	106
4.4.5 Disabling an Auto-Learning Policy	107
4.4.6 Other Operations	107
4.5 Auto-Learning Results	108
4.6 Rule Database Management	108
4.6.1 Querying Common Protection Rules	108
4.6.2 Configuring Custom Rules	110
4.7 Policy Management	112
4.7.1 HTTP Validation Policies	112
4.7.2 Basic Protection Policies	116
4.7.3 Advanced Protection	136
4.7.4 Precise Protection Policy	162
4.7.5 Other Protection Policies	164
4.8 Template Management	170
4.8.1 Website Template	171
4.8.2 Virtual Website Template	173
4.9 Smart Patching	175

4.9.1 Configuring the SAAS Scanning Service	178
4.9.2 Configuring the WVSS Scanning Service.....	180
4.9.3 Managing Scanning Files.....	183
4.9.4 Managing Patches	192
4.10 Secure Delivery	194
4.10.1 Viewing Page Caches.....	195
4.10.2 Adding Cache File Types	195
4.10.3 Configuring Anti-Defacement.....	198
4.10.4 Configuring Page Prefetch Management	203
4.10.5 Clearing Cache.....	206
4.10.6 Configuring Server Offline Takeover.....	206
4.11 Proxy Information Configuration	207
4.12 Uploaded File Management	209
4.12.1 SSL Certificate Management	209
4.12.2 XSD/WSDL File Management	210
4.12.3 Disguised Response File Management	212
4.13 IP Reputation.....	213
4.13.1 IP Reputation Overview	213
4.13.2 IP Reputation Configuration	214
5 Reports	218
5.1 Security Reports	218
5.1.1 Classification-Specific Alert Reports	218
5.1.2 Period-Specific Alert Reports	221
5.2 Traffic Reports.....	223
5.3 Regional Access Statistical Reports	226
5.4 PCI-DSS Compliance Reports	228
6 Logs.....	231
6.1 Querying Security Protection Logs	231
6.1.1 Web Security Logs	232
6.1.2 Network-Layer Access Control Logs	233
6.1.3 DDoS Protection Logs	235
6.1.4 High-Risk IP Blocking Logs	236
6.1.5 Web Anti-Defacement Logs	236
6.1.6 ARP Protection Logs.....	237
6.1.7 Web Access Logs	239
6.1.8 Session Track Logs	240
6.2 Querying Traffic Control Logs.....	241
6.3 Querying System Running Logs	242
6.4 Querying Login Logs	244
6.5 Querying Operation Logs.....	245
6.6 Exporting Logs.....	247

6.7 Log Management Configuration	248
6.7.1 Log Export and Backup	248
6.7.2 Syslog.....	250
6.7.3 SNMP.....	251
6.7.4 Log Sending Parameters	255
6.7.5 A Interface Configuration.....	256
6.7.6 Sensitive Parameter Configuration	257
7 System Management	258
7.1 Network Configurations	258
7.1.1 Work Group Management	258
7.1.2 Route Configuration.....	279
7.1.3 DNS Configuration	281
7.2 System Deployment	283
7.2.1 Running Mode Configuration	283
7.2.2 HA Configuration.....	285
7.2.3 Bypass Configuration.....	288
7.2.4 VRRP Configuration	292
7.2.5 VRRP Configuration Management	295
7.3 System Tools	297
7.3.1 System Information.....	297
7.3.2 System Upgrade	298
7.3.3 Rule Upgrade	299
7.3.4 Configuration Synchronization	305
7.3.5 License	308
7.3.6 System Time and Language	311
7.3.7 System Control.....	312
7.3.8 Port Setting.....	312
7.3.9 Google Analytics Setting	312
7.4 Test Tools	313
7.4.1 Ping	313
7.4.2 Neighbor List	314
7.4.3 Traceroute	315
7.4.4 Packet Capture	316
7.4.5 System Support Tools	319
7.4.6 Scanner.....	319
7.4.7 Debug Log Tracking	322
7.5 Collaboration with ESPC	324
7.6 User Management	328
7.6.1 Account Management	328
7.6.2 User Security.....	331
7.6.3 Login Control.....	333

7.6.4 User Authentication.....	333
7.6.5 Account Unlocking	335
7.7 Traffic Control Management	335
7.8 System Parameter Configuration.....	338
7.8.1 Engine Parameter	338
7.8.2 Kernel Parameter	339
7.8.3 Apache Parameter	340
7.8.4 Other Parameters.....	340
7.9 SSL Acceleration.....	340
7.10 System O&M	341
7.11 REST API.....	342
7.12 Site Control	342
8 Console-based Management.....	344
8.1 Login to the Console	344
8.2 Console Functions	348
8.2.1 System Information.....	349
8.2.2 Diagnostic Tools	350
8.2.3 Maintenance Tools	350
8.2.4 System Initialization	352
8.2.5 Appliance Control	352
8.2.6 Toggle Language.....	353
8.2.7 Exit.....	354
A Default Parameters	355
A.1 Default Settings of the Management Interface	355
A.2 Default Accounts	355
A.3 Console Port Communication Settings.....	355
B Regular Expressions.....	356
B.1 Single Character	356
B.2 Escape Character	356
B.3 Quantifiers	357
B.4 Grouping.....	357
B.5 Examples	358

Figures

Figure 1-1 Typical WAF application	5
Figure 1-2 Typical WAF deployment	6
Figure 2-1 Security alert prompt	8
Figure 2-2 Login page	8
Figure 2-3 Layout of the web-based manager	10
Figure 3-1 Overview page	14
Figure 3-2 Details of a security event	16
Figure 3-3 Security events — real-time data	17
Figure 3-4 Security events — historical data	18
Figure 3-5 Service loads — real-time data	19
Figure 3-6 Service loads — historical data	20
Figure 3-7 Interface traffic — real-time data	21
Figure 3-8 Interface traffic — historical data	22
Figure 3-9 System loads — real-time data	23
Figure 3-10 System loads — historical data	24
Figure 3-11 IP Block Management page	25
Figure 3-12 Website access statistics — real-time data	26
Figure 3-13 Website access statistics — historical data	27
Figure 3-14 Traffic control — real-time data	28
Figure 3-15 Traffic control — historical data	29
Figure 3-16 Server status check — real-time data	29
Figure 3-17 Adding a server	30
Figure 3-18 Parameters for server status check	32
Figure 3-19 Device Monitoring page	33
Figure 3-20 Status bar	34
Figure 4-1 Website protection configuration procedure	38
Figure 4-2 Network-layer protection — enabling and disabling policies	39

Figure 4-3 Network-layer protection — network-layer access control	40
Figure 4-4 Creating a network-layer access control policy	40
Figure 4-5 Network-layer protection — TCP flood protection	42
Figure 4-6 Network-layer protection — ARP spoofing protection	44
Figure 4-7 Creating an IP-MAC binding relationship	45
Figure 4-8 Network-layer protection — ADS collaboration configuration	47
Figure 4-9 Configuring single-IP diversion	48
Figure 4-10 Configuring overall-traffic diversion	49
Figure 4-11 Configuring hybrid diversion	50
Figure 4-12 List of IP addresses allowing traffic diversion	53
Figure 4-13 Website Group Mgmt page	54
Figure 4-14 Creating a website group in quick mode (in reverse proxy mode)	56
Figure 4-15 Creating a website group in quick mode (in in-path, out-of-path, or mirroring mode)	56
Figure 4-16 Specifying the website group name in quick mode	57
Figure 4-17 Specifying the website group name in guide mode	58
Figure 4-18 Website list in guide mode	58
Figure 4-19 Adding a website in guide mode	59
Figure 4-20 Selecting options of service system information	62
Figure 4-21 Website Group Mgmt page	63
Figure 4-22 Deleting a website group from the website group tree	64
Figure 4-23 Adding a website (in in-path or out-of-path mode)	65
Figure 4-24 Adding a website (in mirroring mode)	66
Figure 4-25 Adding a website (in reverse proxy mode)	68
Figure 4-26 Low-and-slow attack protection policy	72
Figure 4-27 HTTP Flood Protection page	73
Figure 4-28 Creating an HTTP flood protection policy	74
Figure 4-29 Creating a custom protection policy	75
Figure 4-30 Secure Data Transfer page	76
Figure 4-31 Creating a secure data transfer policy	77
Figure 4-32 Web Security Policy page	79
Figure 4-33 Select Website Template dialog box	80
Figure 4-34 Web Security Protection page	81
Figure 4-35 HTTP validation types	82

Figure 4-36 Website Template dialog box.....	83
Figure 4-37 Smart Patch Configuration dialog box	84
Figure 4-38 Exception Control page	84
Figure 4-39 Selecting exception policies	85
Figure 4-40 Session tracking page	86
Figure 4-41 Risk level control policy	87
Figure 4-42 Selecting risk level control policies	88
Figure 4-43 Web Decoding page	89
Figure 4-44 Creating a web decoding policy	89
Figure 4-45 False Positive Analysis page.....	91
Figure 4-46 Manual Analysis area.....	91
Figure 4-47 Auto Analysis area	92
Figure 4-48 Auto Adjustment area	93
Figure 4-49 False Positive Analysis Result page	94
Figure 4-50 Analysis result details	95
Figure 4-51 Adjustment details	96
Figure 4-52 Creating a virtual website (in in-path, out-of-path, or mirroring mode)	97
Figure 4-53 Creating a virtual website (in reverse proxy mode)	98
Figure 4-54 Virtual Website page (in in-path, out-of-path, or mirroring mode).....	101
Figure 4-55 Virtual Website page (in reverse proxy mode).....	101
Figure 4-56 Policy Configuration page	102
Figure 4-57 Virtual Website Template dialog box	103
Figure 4-58 Auto-Learning Policies page	104
Figure 4-59 Creating an auto-learning policy	105
Figure 4-60 Auto-Learning Policy Configuration page.....	106
Figure 4-61 Viewing learning results	108
Figure 4-62 Auto-Learning Results page	108
Figure 4-63 Web Server Vulnerability page	109
Figure 4-64 Details about a web server vulnerability rule	110
Figure 4-65 Custom rules	111
Figure 4-66 Creating a custom rule	111
Figure 4-67 HTTP Validation page	113
Figure 4-68 Creating an HTTP validation policy	114

Figure 4-69 Duplicating an HTTP validating policy	116
Figure 4-70 Web Server/Plug-in Protection page	117
Figure 4-71 Creating a web server/plug-in protection policy	118
Figure 4-72 HTTP Access Control page	120
Figure 4-73 Creating an HTTP access control policy	120
Figure 4-74 Crawler Protection page	122
Figure 4-75 Creating a crawler protection policy	122
Figure 4-76 Common Web Protection page	124
Figure 4-77 Creating a common web protection policy	125
Figure 4-78 Illegal Upload Restriction page	127
Figure 4-79 Creating an illegal upload restriction policy	127
Figure 4-80 Illegal Download Restriction page	129
Figure 4-81 Creating an illegal download restriction policy	130
Figure 4-82 Information Disclosure page	132
Figure 4-83 Creating an information disclosure policy	133
Figure 4-84 Leech Protection page	137
Figure 4-85 Creating a leech protection policy	138
Figure 4-86 CSRF Protection page	140
Figure 4-87 Creating a CSRF protection policy	141
Figure 4-88 Scanning Protection page	143
Figure 4-89 Creating a scanning protection policy	143
Figure 4-90 Cookie Security page	146
Figure 4-91 Creating a cookie security policy	147
Figure 4-92 Content Filtering page	149
Figure 4-93 Creating a content filtering policy	149
Figure 4-94 Sensitive Information Filtering page	151
Figure 4-95 Creating a sensitive information policy	151
Figure 4-96 Brute Force Protection page	153
Figure 4-97 Creating a brute force protection policy	154
Figure 4-98 XML Attack Protection page	156
Figure 4-99 Creating an XML attack protection policy	157
Figure 4-100 Smart Engine Inspection page	160
Figure 4-101 Creating a smart engine inspection policy	161

Figure 4-102 Whitelist page	163
Figure 4-103 Creating a whitelist	163
Figure 4-104 Exception Policy page	165
Figure 4-105 Creating an exception policy	165
Figure 4-106 Custom Policy page	167
Figure 4-107 Creating a custom policy	167
Figure 4-108 Risk Level Policy page	169
Figure 4-109 Creating a risk level policy	169
Figure 4-110 Website Management page	171
Figure 4-111 Creating a website template	172
Figure 4-112 Virtual Website Template page	173
Figure 4-113 Creating a virtual website template.....	174
Figure 4-114 Deployment topology — smart patching function via cloud-based scanning.....	176
Figure 4-115 Procedure of smart patching via cloud-based scanning	177
Figure 4-116 Procedure of the smart patching function via imported vulnerability scanning report	178
Figure 4-117 SAAS Scan Config page.....	178
Figure 4-118 DNS Configuration page	179
Figure 4-119 Creating the mapping between a domain name and an IP address.....	180
Figure 4-120 Configuring network-layer access control policies for penetration scanning	180
Figure 4-121 WVSS Scan Config page.....	181
Figure 4-122 Creating a WVSS scanning task	182
Figure 4-123 SAAS scanning file list.....	184
Figure 4-124 Related Scanning File dialog box	184
Figure 4-125 Cloud-based scanning report	185
Figure 4-126 Details of a vulnerability	186
Figure 4-127 Smart Patch Configuration page	187
Figure 4-128 Page for managing imported scanning files	188
Figure 4-129 Imported report.....	189
Figure 4-130 Details of a vulnerability	189
Figure 4-131 WVSS scanning files with patches	190
Figure 4-132 Patch application dialog box.....	191
Figure 4-133 List of websites to which the selected patches can apply	191
Figure 4-134 Patch Management page	193

Figure 4-135 Patch information	193
Figure 4-136 Details of a vulnerability fixed by the patch	194
Figure 4-137 Page Cache page	195
Figure 4-138 Customized MIME Types page	196
Figure 4-139 Creating a MIME type	197
Figure 4-140 Built-in MIME Types page	198
Figure 4-141 Common Anti-Defacement Configuration page	199
Figure 4-142 Editing the common anti-defacement configuration	200
Figure 4-143 URL Exception List page	201
Figure 4-144 Adding URL exceptions	202
Figure 4-145 Page Prefetch Management page	203
Figure 4-146 Setting the update interval	204
Figure 4-147 Creating a page prefetch task	205
Figure 4-148 Clear Cache page	206
Figure 4-149 Server Offline Takeover page	207
Figure 4-150 Proxy Information Configuration page	208
Figure 4-151 SSL certificate management	209
Figure 4-152 Importing an SSL certificate	210
Figure 4-153 Details of an SSL certificate	210
Figure 4-154 XSD/WSDL file management	211
Figure 4-155 Uploading an XSD or WSDL file	211
Figure 4-156 Disguised response file management	213
Figure 4-157 IP Reputation Overview page	214
Figure 4-158 IP Reputation Configuration page	215
Figure 4-159 Connection success	215
Figure 4-160 Creating an IP reputation policy	216
Figure 5-1 Classification-Specific Alert Report page	218
Figure 5-2 Classification-specific alert report	220
Figure 5-3 Period-Specific Alert Report page	221
Figure 5-4 Period-specific alert report	222
Figure 5-5 Traffic Pattern Reports page	223
Figure 5-6 Engine traffic pattern report	224
Figure 5-7 Interface traffic pattern report	225

Figure 5-8 Regional Access Statistical Report page.....	226
Figure 5-9 Regional access statistical report	227
Figure 5-10 PCI-DSS Compliance Report page.....	228
Figure 5-11 PCI-DSS compliance report.....	229
Figure 6-1 Web Security Logs page	232
Figure 6-2 Network-Layer Access Control Logs page	234
Figure 6-3 DDoS Protection Logs page	235
Figure 6-4 High-Risk IP Blocking Logs page	236
Figure 6-5 Web Anti-Defacement Logs page	237
Figure 6-6 ARP Protection Logs page	238
Figure 6-7 Web Access Logs page	239
Figure 6-8 Session Track Logs page	240
Figure 6-9 Traffic Control Logs page.....	242
Figure 6-10 Running Logs page.....	243
Figure 6-11 Login logs	244
Figure 6-12 Operation logs	246
Figure 6-13 Export Logs page.....	247
Figure 6-14 Log Export & Backup page	248
Figure 6-15 Syslog Configuration page	250
Figure 6-16 Adding a syslog server.....	250
Figure 6-17 SNMP Configuration page	251
Figure 6-18 Creating an SNMPv3 agent	252
Figure 6-19 Adding an SNMPv1/v2c server	253
Figure 6-20 Adding an SNMPv3 server	254
Figure 6-21 Log Sending Parameter Configuration page.....	255
Figure 6-22 A Interface Configuration page.....	256
Figure 6-23 Sensitive Parameter Config page	257
Figure 7-1 Work Group Management page in in-path mode.....	259
Figure 7-2 Adding management interfaces in in-path mode	260
Figure 7-3 Editing a management interface in in-path mode.	261
Figure 7-4 Creating a work group in in-path mode	263
Figure 7-5 Editing a working interface in in-path mode.	264
Figure 7-6 Editing a work group in in-path mode	266

Figure 7-7 Creating a VLAN in in-path mode	267
Figure 7-8 Work Group Management page in out-of-path mode	268
Figure 7-9 Creating a work group in out-of-path mode	269
Figure 7-10 Editing a working interface in out-of-path mode.....	270
Figure 7-11 Creating a subinterface in out-of-path mode.....	270
Figure 7-12 Forwarding table.....	271
Figure 7-13 Forwarding routing table	271
Figure 7-14 Editing a work group in out-of-path mode.	272
Figure 7-15 Configuring an injection route in out-of-path mode	273
Figure 7-16 Route injection configuration	274
Figure 7-17 Configuring an injection route.....	275
Figure 7-18 Work Group Management page in reverse proxy mode	276
Figure 7-19 Editing a working interface in reverse proxy mode.....	277
Figure 7-20 Work Group Management page in mirroring mode.....	278
Figure 7-21 Creating a work group in mirroring mode	279
Figure 7-22 Route Configuration page.....	280
Figure 7-23 Creating a static route	281
Figure 7-24 DNS Configuration page	282
Figure 7-25 Creating a custom domain name.....	283
Figure 7-26 Running Mode page	284
Figure 7-27 HA Configuration page.....	286
Figure 7-28 Built-in Bypass Configuration page	288
Figure 7-29 External bypass topology.....	290
Figure 7-30 External Bypass Configuration page	290
Figure 7-31 Editing an external bypass group.....	291
Figure 7-32 VRRP Configuration page	292
Figure 7-33 Adding interface G1/1	293
Figure 7-34 VRRP Configuration page after interface G1/1 is added.....	293
Figure 7-35 VRRP instance management	293
Figure 7-36 Adding a VRRP instance for interface G1/1	294
Figure 7-37 VRRP Config Info Mgmt page	296
Figure 7-38 Viewing an exported VRRP configuration file	297
Figure 7-39 System Information page — without SSL card	298

Figure 7-40 System Information page — with SSL card	298
Figure 7-41 System Upgrade page	299
Figure 7-42 Rule Upgrade page	300
Figure 7-43 Current version information	300
Figure 7-44 Scheduled upgrade.....	301
Figure 7-45 Manual upgrade	302
Figure 7-46 Check updates.....	302
Figure 7-47 Rule upgrade package details	303
Figure 7-48 Historical updates	304
Figure 7-49 Auto-Backup of Rule Database area	304
Figure 7-50 Offline configuration synchronization.....	305
Figure 7-51 Details of a restore point file	307
Figure 7-52 Online synchronization.....	307
Figure 7-53 Details of an online synchronization record	308
Figure 7-54 License page	309
Figure 7-55 License expiration notification	310
Figure 7-56 Confirming license information.....	310
Figure 7-57 Updating the license	311
Figure 7-58 Time & Language page.....	311
Figure 7-59 System Control page.....	312
Figure 7-60 Port Setting page.....	312
Figure 7-61 Google Analytics Setting page.....	313
Figure 7-62 Ping page	314
Figure 7-63 Ping result.....	314
Figure 7-64 Neighbors page	315
Figure 7-65 Trace Route page	315
Figure 7-66 Traceroute result	316
Figure 7-67 Capture Packets page.....	316
Figure 7-68 Setting packet capturing parameters	317
Figure 7-69 Capture Packets page in the process of a capture task	318
Figure 7-70 Capture Packets page after a capture task is successfully completed	319
Figure 7-71 System Support Tools page	319
Figure 7-72 Scanner page.....	320

Figure 7-73 Creating a scanning task	320
Figure 7-74 Scanning result	321
Figure 7-75 Debug Log Tracking page	322
Figure 7-76 Adding an IP address for tracking.....	323
Figure 7-77 Tracked IP addresses.....	323
Figure 7-78 Tracked logs.....	324
Figure 7-79 ESPC page – under non-centralized management	325
Figure 7-80 ESPC page – under centralized management	326
Figure 7-81 User Management page	329
Figure 7-82 Creating a user	330
Figure 7-83 User Security page.....	332
Figure 7-84 Login Control page.....	333
Figure 7-85 Authentication Configuration page.....	334
Figure 7-86 Account Unlocking page	335
Figure 7-87 Traffic Control Mgmt page	335
Figure 7-88 Creating a traffic control object.....	336
Figure 7-89 Engine Parameters page.....	339
Figure 7-90 Kernel Parameter page.....	339
Figure 7-91 Apache Parameter page	340
Figure 7-92 SSL Acceleration page.....	341
Figure 7-93 System O&M page	341
Figure 7-94 Digital Signature Parameters page.....	342
Figure 7-95 Site Control page	343
Figure 8-1 Location Information dialog box	345
Figure 8-2 Connection Description dialog box	345
Figure 8-3 Connect to dialog box.....	346
Figure 8-4 COM1 Properties dialog box	346
Figure 8-5 Login page	347
Figure 8-6 Language selection window	347
Figure 8-7 User Menu window	348
Figure 8-8 System Information window	349
Figure 8-9 Diagnostic Tools window	350
Figure 8-10 Maintenance Tools window	351

Figure 8-11 System Initialization window	352
Figure 8-12 Appliance Control window	353
Figure 8-13 Toggling language	354

Tables

Table 2-1 System users and their privileges	9
Table 2-2 Layout of the web-based manager	11
Table 2-3 Icons and buttons for common operations	11
Table 3-1 Risk level of security events.....	14
Table 3-2 Parameters for querying historical security events.....	18
Table 3-3 Parameters for querying historical service load data.....	20
Table 3-4 Parameters for querying historical interface traffic data	22
Table 3-5 Parameters for querying historical system load data	24
Table 3-6 Parameters for querying website access statistics	27
Table 3-7 Parameters for adding a server	30
Table 3-8 Parameters for server status check	32
Table 3-9 Parameters for partition monitoring	33
Table 3-10 Status bar information	34
Table 4-1 Parameters for creating a network-layer access control policy	40
Table 4-2 Parameters for editing the TCP flood protection policy	43
Table 4-3 Parameters for creating an IP-MAC binding relationship	45
Table 4-4 Parameters for configuring single-IP diversion.....	50
Table 4-5 Parameters for adding a website.....	59
Table 4-6 Parameters for adding a website in mirroring mode.....	66
Table 4-7 Parameters for adding a website in reverse proxy mode	68
Table 4-8 Parameters of the low-and-slow attack protection policy	72
Table 4-9 Parameters for global configuration	73
Table 4-10 Parameters for creating an HTTP flood protection policy.....	74
Table 4-11 Parameters for configuring a custom protection policy	75
Table 4-12 Parameters for configuring secure data transfer policies.....	77
Table 4-13 Parameters for configuring the session tracking policy.....	86
Table 4-14 Parameters for configuring a web decoding policy	89

Table 4-15 Parameters for creating a virtual website	98
Table 4-16 Parameters for querying a rule	109
Table 4-17 Parameters for creating an HTTP validation policy	114
Table 4-18 Parameters for creating a web server/plugin protection policy	118
Table 4-19 Parameters for creating HTTP access control policies	120
Table 4-20 Parameters for creating a crawler protection policy	123
Table 4-21 Parameters for creating a common web protection policy	125
Table 4-22 Parameters for creating an illegal upload restriction policy	128
Table 4-23 Parameters for creating an illegal download restriction policy	130
Table 4-24 Parameters for creating an information disclosure protection policy	133
Table 4-25 Common status codes	134
Table 4-26 Parameters for creating a leech protection policy	138
Table 4-27 Parameters for creating a CSRF protection policy	141
Table 4-28 Parameters for creating a scanning protection policy	143
Table 4-29 Parameters for creating a cookie security policy	147
Table 4-30 Parameters for creating a content filtering policy	150
Table 4-31 Parameters for creating a sensitive information filtering policy	152
Table 4-32 Parameters for creating a brute force protection policy	154
Table 4-33 Parameters for creating an XML attack protection policy	157
Table 4-34 Parameters for configuring a smart engine inspection policy	161
Table 4-35 Parameters for creating a whitelist policy	163
Table 4-36 Parameters for creating an exception policy	166
Table 4-37 Parameters for creating a custom policy	167
Table 4-38 Parameters for creating a risk level policy	169
Table 4-39 Parameters for creating a website template	172
Table 4-40 Parameters for creating a virtual website template	174
Table 4-41 Parameters for configuring SAAS scanning settings	178
Table 4-42 WVSS device parameters	181
Table 4-43 Parameters for creating a WVSS scanning task	182
Table 4-44 Common MIME types	196
Table 4-45 Parameters for creating a custom MIME type	197
Table 4-46 Parameters for editing the common anti-defacement configuration	200
Table 4-47 Parameters for creating a page prefetch task	205

Table 4-48 Proxy parameters.....	208
Table 4-49 IP reputation overview details.....	214
Table 4-50 Parameters for configuring an IP reputation policy.....	216
Table 5-1 Parameters for querying a classification-specific alert report.....	219
Table 5-2 Parameters for querying a period-specific alert report.....	221
Table 5-3 Parameters for querying a traffic pattern report.....	223
Table 5-4 Conditions for querying regional access statistical reports.....	226
Table 5-5 Parameters for generating a PCI-DSS compliance report.....	228
Table 6-1 Parameters for querying web security logs.....	232
Table 6-2 Parameters for querying network-layer access control logs.....	234
Table 6-3 Parameters for querying DDoS protection logs.....	235
Table 6-4 Parameters for querying high-risk IP blocking logs.....	236
Table 6-5 Parameters for querying web anti-defacement logs.....	237
Table 6-6 Parameters for querying ARP protection logs.....	238
Table 6-7 Parameters for querying web access logs.....	239
Table 6-8 Parameters for querying session tracing logs.....	241
Table 6-9 Parameters for querying traffic control logs.....	242
Table 6-10 Parameters for querying system running logs.....	243
Table 6-11 Parameters for querying login logs.....	245
Table 6-12 Parameters for querying operation logs.....	246
Table 6-13 Parameters for creating an SNMPv3 agent.....	253
Table 6-14 Parameters for configuring SNMPv3 trap.....	254
Table 6-15 Log sending parameters.....	255
Table 7-1 Parameters for editing a management interface in in-path mode.....	261
Table 7-2 Parameters for creating a work group in in-path mode.....	263
Table 7-3 Parameters for editing a work group in in-path mode.....	264
Table 7-4 Parameters for creating a static route.....	281
Table 7-5 Parameters for setting the emergency mode.....	285
Table 7-6 Parameters for configuring HA.....	286
Table 7-7 Parameters for editing an external bypass group.....	291
Table 7-8 Parameters for creating a VRRP instance.....	294
Table 7-9 Parameters for configuring scheduled upgrade.....	301
Table 7-10 Synchronization scope.....	306

Table 7-11 Parameters for capturing packets.....	317
Table 7-12 Parameters for creating a scanning task	320
Table 7-13 Global parameters for debug log tracking	322
Table 7-14 ESPC-related parameters on WAF	327
Table 7-15 Parameters for creating an account	330
Table 7-16 Parameters for configuring user security.....	332
Table 7-17 Parameters for configuring authentication	334
Table 7-18 Parameters for creating a traffic control object	337
Table 8-1 Meaning of keys	348

Preface

Scope

This document describes the functions and usage of the web-based manager and console interface of NSFOCUS Web Application Firewall (WAF) V6.0.

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.

Audience

This document is intended for the following users:

- Users who wish to know main features and usage of this product
- System administrator
- Network administrator

This document assumes that you have knowledge in the following areas:





- Network security
- Linux and Windows operating systems
- TCP/IP protocols

Organization

Chapter	Description
1 Product Introduction	Introduces features of WAF.
2 Overview of the Web-based Manager	Describes basic information about the web-based manager.
3 System Monitoring	Describes how to monitor the system on the web-based manager.
4 Security Management	Describes how to configure websites and policies on the web-based manager.
5 Reports	Describes how to view various reports on the web-based manager and what can be learned from such reports.
6 Logs	Describes how to view various logs on the web-based manager and what can be learned from such logs.
7 System Management	Describes common operations and methods for system management and maintenance.

Chapter	Description
8 Console-based Management	Describes how to log in to and use the console interface.
A Default Parameters	Describes default parameters of WAF.
B Regular Expressions	Describes the syntax of regular expressions used in policy configurations.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
 Note	Reminds users to take note.
 Tip	Indicates a tip to make your operations easier.
 Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
 Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Customer Support

Email: support@nsfocusglobal.com

Portal: <https://nsfocus.desk.com/>

Contacts:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

1 Product Introduction

1.1 Overview

Individuals and enterprises are becoming increasingly dependent on the Internet. The web technology is employed in more core services of enterprises. Unfortunately, according to most security experts, web applications are prone to security vulnerabilities and protection measures are far behind attack methods.

WAF can protect web applications from online attacks. With a continuously updated vulnerability database, WAF enables security professionals, network administrators, and application developers to reduce security risks for web applications, therefore ensuring the stable running of web applications.

Benefits to Customer

- Reduction of data leakage risks
Web-based interactive applications give access to databases. Attackers often intrude into databases via SQL injection or other methods, causing data leakage. WAF can reduce the risk of data leakage by:
 - Checking fields contained in HTTP requests
 - Filtering out attack packets with refined rules
 - Implementing mechanisms such as HTTP compliance inspection and status code filtering
- Support for web application availability
Distributed denial-of-service (DDoS) attacks are the major threats to web service availability. WAF boasts the professional DDoS prevention function that contains multiple dynamic protection algorithms and is capable of filtering out DDoS attack packets online. The combined use of DDoS protection and SQL injection protection enables WAF to filter out attack packets from the network layer to application layer, ensuring web service availability.
- Control of malicious access
Auto attack tools can produce large-scale malicious access, greatly compromising web application stability. WAF provides multiple web access control means to meet various customer needs, including HTTP access control, auto attack tool identification, control of illegal file upload and download, and leech and crawler prevention.
- Protection of web clients
A user may lose trust in a website once suffering a cross-site request forgery (CSRF) attack on it. Therefore, protecting web clients is also the responsibility and concern of web service providers. WAF can well protect web clients with security policies

regarding CSRF protection, cross-site scripting (XSS) protection, and cookie signature and encryption.

Product Advantages

- Integration of the professional DDoS protection function
- Support for multiple easy-to-use web access control policies
- Support for flexible custom rules
- Support for out-of-path deployment
- Support for traffic control based on domain names

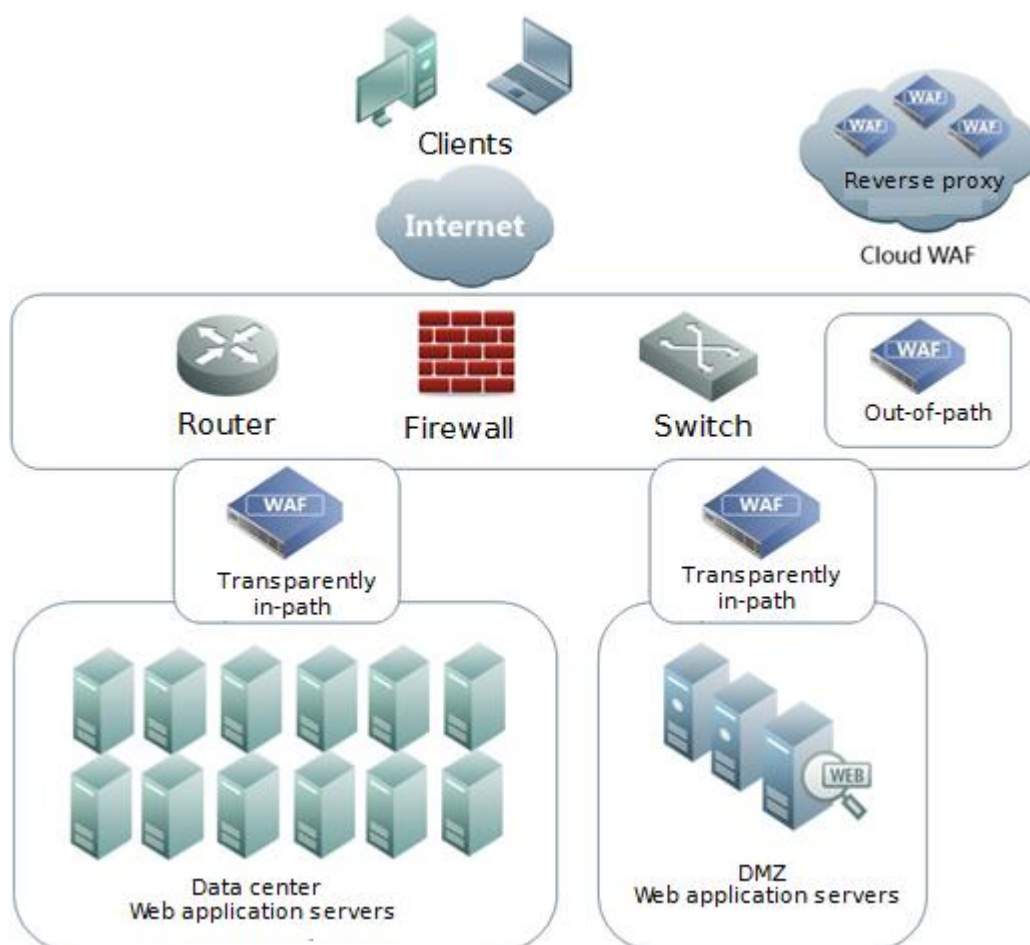
Key Functions

- Reduction of data leakage risks
 - SQL injection protection
 - HTTP protection
 - Web vulnerability attack protection
 - Information leakage protection via status code filtering and disguising
 - Web content security protection
 - Brute force protection
 - XML attack protection
- Support for web application availability
 - HTTP flood prevention
 - TCP flood prevention
 - Low-and-slow attack protection
- Control of malicious access
 - URL access control
 - Prevention of illegal file upload and download
 - Anti-leech
 - Anti-crawler
- Protection for web clients
 - CSRF protection
 - XSS protection
 - Cookie security protection via encryption and signature

1.2 Typical Application

WAF is widely used in data centers and demilitarized zones of a local area network (LAN). It can be deployed in transparent (in-path) mode, reverse proxy mode, mirroring mode, and multiple route-based out-of-path modes, providing high software and hardware availability.

Figure 1-1 Typical WAF application

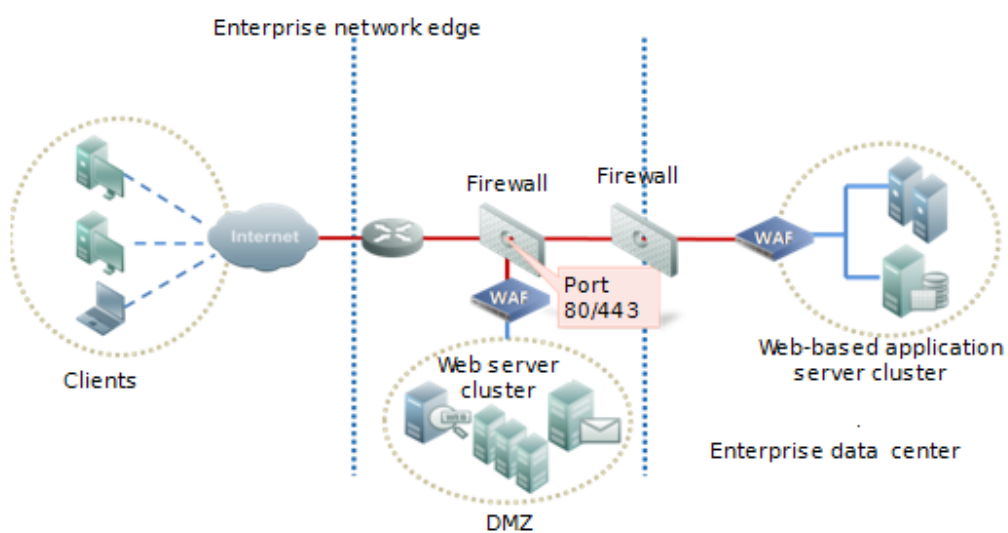


1.3 Typical Deployment

Usually, WAF operates in the DMZ. It is deployed in transparent (in-path) mode between web servers and the firewall, requiring no change in network or server configurations. It effectively monitors traffic to and from the web servers, therefore protecting the security of web applications. See [Figure 1-2](#).

WAF supports software and hardware bypass functions. If WAF fails, the bypass functions enable the devices on both sides of the WAF to be directly linked, ensuring service continuity.

Figure 1-2 Typical WAF deployment



For critical services, hot standby is recommended to avoid single points of failure (SPOFs) and ensure high web service availability.

2 Overview of the Web-based Manager

The web-based manager of WAF provides more intuitive man-machine interaction interfaces for users to manage and configure WAF.

This chapter describes basic information about the web-based manager of WAF. It covers the following topics:

Topic	Description
Login	Describes how to log in to the web-based manager.
System Users	Describes system user types and their privileges.
Layout of the Web-Based Manager	Describes the web page layout.
Common Operations	Describes icons and buttons for common operations on the web-based manager.

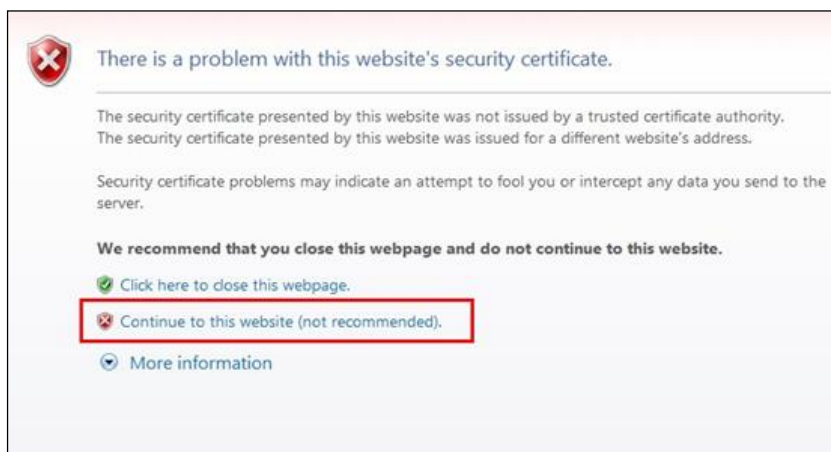
2.1 Login

To log in to the web-based manager, perform the following steps (Microsoft Internet Explorer is used as an example):

Make sure that the client communicates properly with WAF (open port 443 if the communication goes through a firewall).

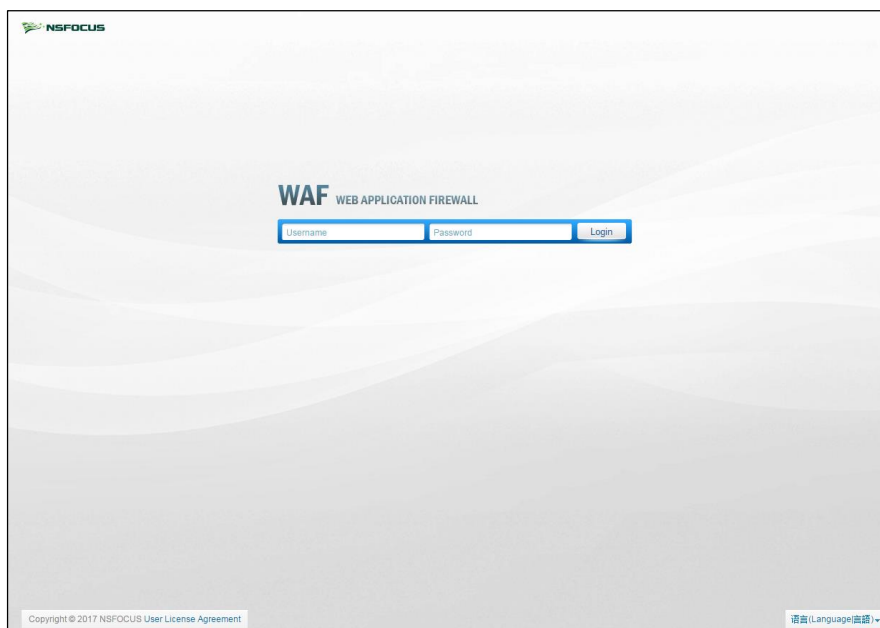
- Step 1** Start IE and access the web-based manager's IP address by HTTPS (<https://192.168.1.1> for example).
- Step 2** Click **Continue to this website (not recommended)** on the security alert page shown in [Figure 2-1](#).

Figure 2-1 Security alert prompt



Step 3 On the login page shown in Figure 2-2, select a language, type a correct user name and password, and click **Login** to log in to the web-based manager.

Figure 2-2 Login page



----End



Note the following when logging in to the web-based manager:

	<ul style="list-style-type: none"> You are advised to use the Internet Explorer 7.0, 8.0, or 9.0, Firefox 3.6 or later, or Chrome browser and set the display resolution to 1024 x 768 or higher. If you log in with a default account, you must change the initial password after login. For details about default accounts, see appendix A Default Parameters. Possible causes for login failures: incorrect user name, incorrect password, or upper/lower case confusion of the user name or password. Before login, check whether Turn on Pop-up Blocker is selected in the browser. If yes, deselect it.
--	--

2.2 System Users

WAF users fall into three types:

- Administrator**
 An administrator has privileges of managing and configuring the web-based manager. The default administrator account is **admin**.
- Auditor**
 An auditor has the privilege of viewing audit logs. The default auditor account is **auditor**.
- Maintainer**
 A maintainer has privileges of configuring engine parameters of the system. The default maintainer account is **maintainer**.
- Common user**
 A common user has some privileges of managing and configuring the web-based manager. The administrator creates common user accounts.

The **admin**, **auditor**, and **maintainer** accounts have different privileges. [Table 2-1](#) describes the privileges of WAF users.

Table 2-1 System users and their privileges

User		Privilege
Administrator	admin (default)	All privileges except managing auditors and viewing audit logs.
	Custom administrators (created by admin)	All privileges of admin , except creating custom administrators and modifying information about the default administrator account.
Auditor	auditor (default)	Privileges of viewing audit logs and managing auditors.
	Custom auditors (created by auditor)	Privileges of viewing audit logs and editing information about the current auditor account.
Maintainer	maintainer (default)	Privileges of configuring system engine parameters and managing maintenance accounts.
	Custom maintainers (created by maintainer)	Privileges of configuring system engine parameters and editing the current maintainer account.
Common user	Custom users (created by administrators)	Privileges of editing information about the current common user account and managing and configuring the web-based manager.

User		Privilege
Maintainer	maintainer (default)	Privileges of configuring system engine parameters and managing maintenance accounts.
	Custom maintainers (created by maintainer)	Privileges of configuring system engine parameters and editing the current maintainer account.
Common user	Custom users (created by administrators)	Privileges of editing information about the current common user account and managing and configuring the web-based manager.



For more details about system users, see section [7.6.1 Account Management](#).

2.3 Layout of the Web-Based Manager

After you log in to the web-based manager with the **admin** account, a web page shown in [Figure 2-3](#) appears.



The layout varies with user privileges.

Figure 2-3 Layout of the web-based manager

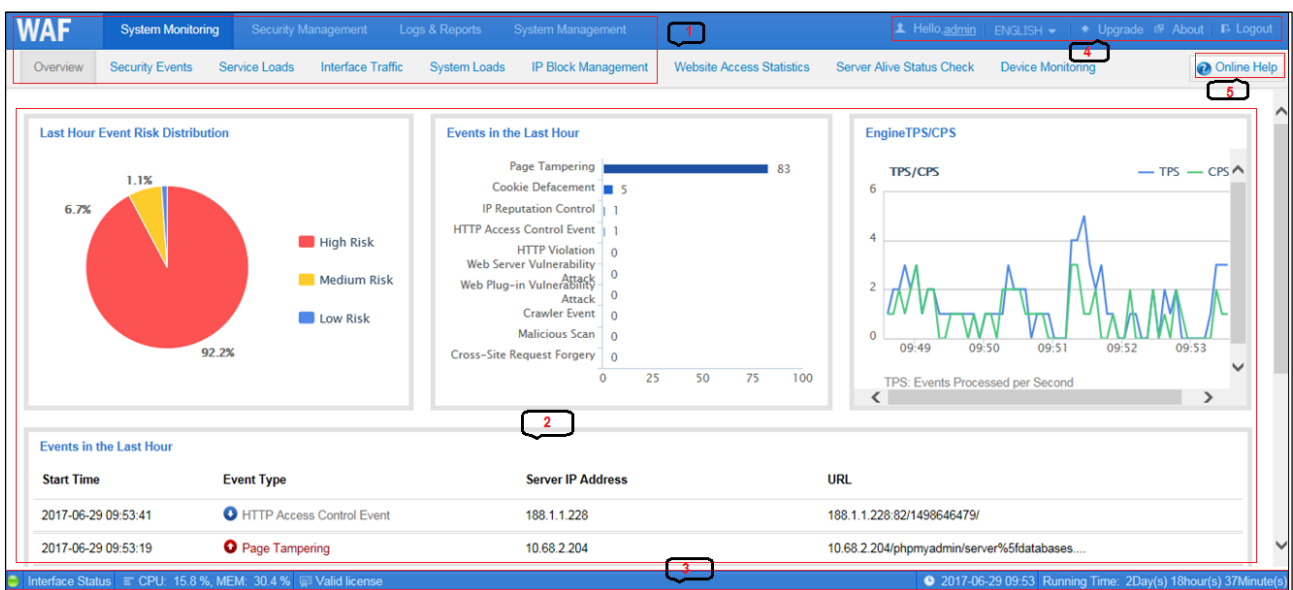
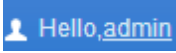

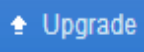
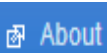
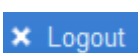



Table 2-2 describes the layout of the web-based manager.








Table 2-2 Layout of the web-based manager



No.	Area	Description
1	Menu bar	Areas where menus and related submenus are provided to help you locate system functions.
2	Work area	Area where you can perform configurations and operations and view data.
3	Status bar	Area displaying basic information about system operating. For details, see section 3.11 System Information.
4	Quick access bar	<p>Area providing several buttons for convenient operations.</p> <ul style="list-style-type: none">  Hello, admin: modifies information about the current user.  ENGLISH: switches to another language.  Upgrade: upgrades WAF.  About: displays information about WAF.  Logout: logs you out of the web-based manager. For security concern, you are advised to click this button to log out of the web-based manager.
5	Online help	Clicking  Online Help displays online help information of WAF.

2.4 Common Operations

There are some common operations in the web-based manager. Table 2-3 describes the icons and buttons for common operations.

Table 2-3 Icons and buttons for common operations

Icon/Button	Function
	Edits the current item.
	Deletes the current item.
	Copies the current configuration.
	Starts an operation.
	Stops an operation.
	Moves an item up.
	Moves an item down.

Icon/Button	Function
	Saves a configuration.
	Restores a configuration.

3

System Monitoring

The system monitoring module shows users information such as security events, service loads, WAF interface traffic, system loads, and IP block management information, website access statistics, traffic control, and system status, enabling users to understand the security status of a network.

This chapter covers the following topics:

Topic	Description
Overview	Describes how to view the following data: <ul style="list-style-type: none">• Distribution of risks of last-hour security events.• Types and numbers of last-hour security events.• Engine TPS/CPS. Here, TPS stands for transactions per second, and CPS for connections per second.
Security Event Data	Describes how to view real-time and historical security event data, and the event type distribution.
Service Loads	Describes how to view real-time and historical data on system loads (TPS/CPS, concurrent connections, and engine traffic).
Interface Traffic Data	Describes how to view real-time and historical data on interface traffic.
System Loads	Describes how to view real-time and historical data on system loads (CPU usage, memory usage, and disk space usage).
IP Block Management	Describes how to view and manage blocked IP addresses.
Website Access Statistics	Describes how to view access statistics of a specified website.
Traffic Control Data	Describes how to view real-time and historical traffic control data of a specified object.
Server Status Check	Describes how to view the status of the target server.
Device Monitoring	Describes how to enable or disable alerting for the CPU/memory, partitions, and processes, and configure related alerting thresholds.
System Information	Describes how to view system information in the status bar.

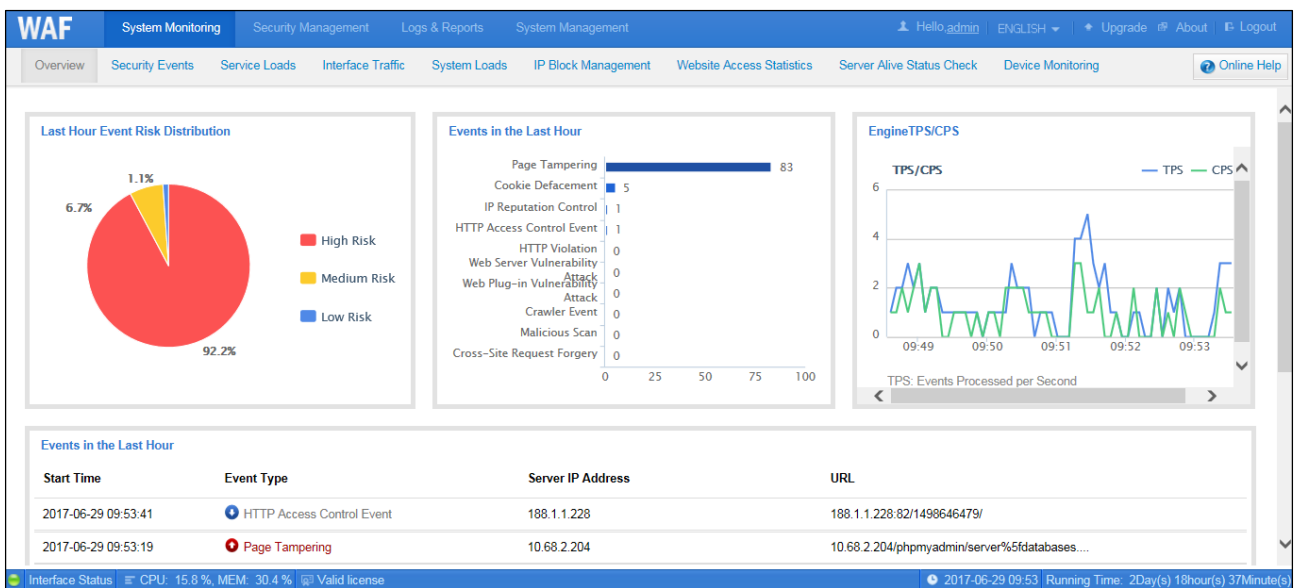
3.1 Overview

After you log in to the web-based manager, the **Overview** page appears. Alternatively, you can choose **System Monitoring > Overview** to open this page.

The **Overview** page shows the following data on the server protected by WAF:

- Distribution of the risks of last-hour security events
- Types and numbers of last-hour security events
- TPS/CPS of the engine in the last 5 minutes
- 10 most recent security events

Figure 3-1 Overview page



Risk levels of security events are categorized as follows:

- 🟡 : medium-risk
- 🔴 : high-risk
- 🔵 : low-risk

Table 3-1 defines the risk level of various security events.

Table 3-1 Risk level of security events

Security Event Type	Risk Level
HTTP violation	Medium
Web server vulnerability attack	Depending on the triggered rule
Web plug-in vulnerability attack	Depending on the triggered rule
Secure data transfer	Low
HTTP access control event	Low

Security Event Type	Risk Level
Crawler event	Low
XSS attack	Depending on the triggered rule
SQL injection	Depending on the triggered rule
LDAP injection	Depending on the triggered rule
SSI directive attack	Depending on the triggered rule
XPath injection	Depending on the triggered rule
Command injection	Depending on the triggered rule
Path traversal attack	Depending on the triggered rule
Remote file inclusion	Depending on the triggered rule
Directory index information disclosure	Depending on the triggered rule
WebShell access	High
Illegal file upload	High
Illegal download	Medium
Server information disclosure	High
Resource leech	Medium
Cross-site request forgery	High
Malicious scan	High
Cookie defacement	Medium
Illegal page content	Medium
Sensitive information filtering	High
Brute force attack	High
High-risk IP address	High
XML attack	High
IP reputation control	Medium
Smart engine inspection	High
Smart patch	High
Whitelist violation	Medium
SYN flood	High
ACK flood	High
HTTP flood	High
Collaboration event	High
Low-and-slow attack	High
Web page defacement	High

Security Event Type	Risk Level
Custom attack	Medium
ARP attack	High
IP access control event	Low

In the **Event Type** column of the **Events in the Last Hour** list shown in [Figure 3-1](#), click a specific security event to view its details. See [Figure 3-2](#). Log details displayed here are the same as those from **Security Protection Logs**. For details about the latter, see [section 6.1 Querying Security Protection Logs](#).

Figure 3-2 Details of a security event

The screenshot shows a 'Event Details' dialog box with a blue header and a close button (X) in the top right corner. The dialog contains a table of event details with the following fields:

Website ID	1351669588
Website Name	test
Virtual Website Name	vtest
Protection Object ID	123155
Server IP Address	140.140.1.5
Server Port	81
Client IP Address	140.140.1.200 (China)
Client Port	1373
HTTP Request Method	GET
Domain Name	140.140.1.5
URI	View Original URI Info /at_
Risk Level	⚠️
Alert Type	SQL Injection Attack

At the bottom of the dialog is a 'Close' button.

3.2 Security Event Data

On the **Security Events** page, you can view real-time data on last-hour security events, and query data on historical security events based on specific conditions. Historical data lags behind real-time data by 1–2 minutes.

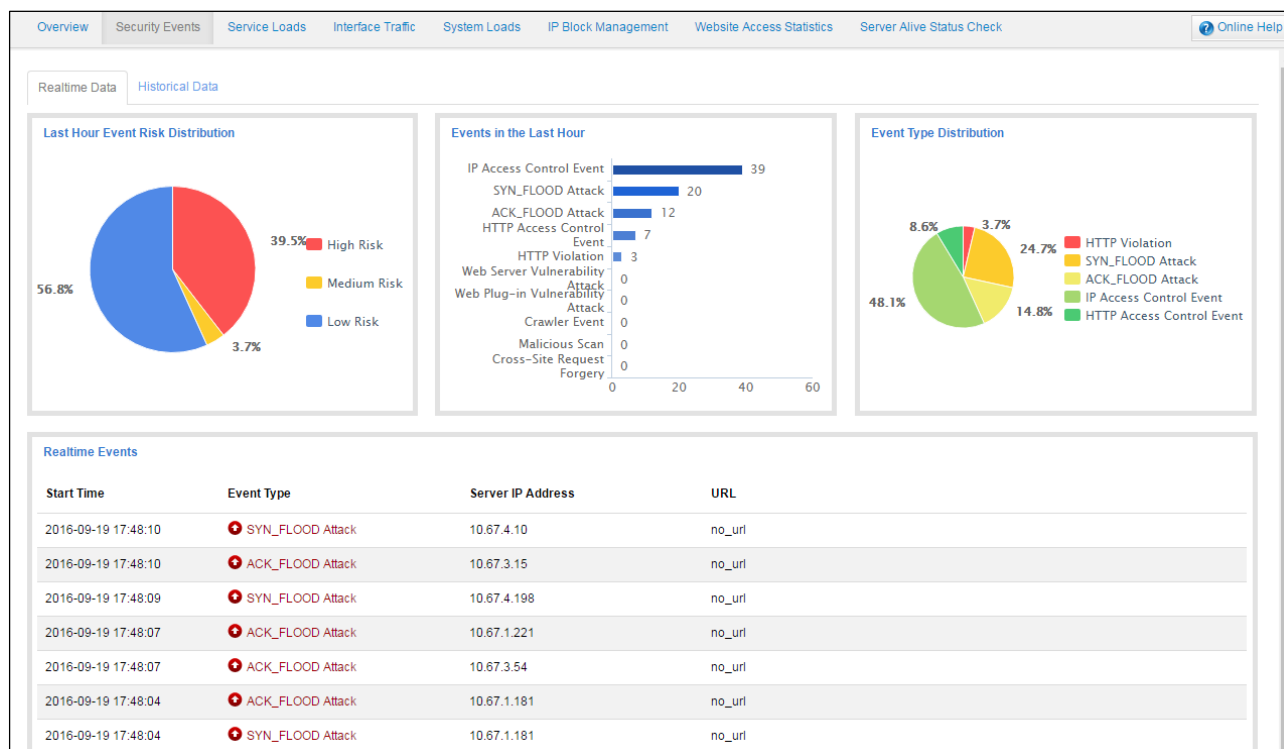
3.2.1 Viewing Real-Time Data

Choose **System Monitoring > Security Events**. The **Realtime Data** page appears, as shown in [Figure 3-3](#). Similar to the **Overview** page, this page shows the following data:

- Distribution of the risks of last-hour security events

- Types and numbers of last-hour security events
- Distribution of the types of last-hour security events
- Last-hour security events

Figure 3-3 Security events — real-time data



3.2.2 Querying Historical Data

Choose **System Monitoring > Security Events > Historical Data**. The **Historical Data** page appears, as shown in [Figure 3-4](#). You can query a specific range of security events by setting query conditions.

Figure 3-4 Security events — historical data

Realtime Data

Historical Data

Conditions

Event Type

Please select

Start Time

Please select

2016-09-18 09:40

Destination IP Address

Destination Port

URL

Query

First Page

Previous Page

Next Page

Last Page

1/1Page. Go to:

Event Type	Start Time	Duration	Destination	URL	Source	Action	Status	Matches
Cookie Defacement	2016-09-14 15:41:58	0	2408:80f0:4010::1:80	assets.changyan.sohu.com/upload/changyan.js?appid=c yqemw6s1&conf=prod%5f02 66e33d3f546cb5436a10798 e657d97	2013::310d:41e6:5267:5957	Clear	Triggered Event	1
SQL Injection Attack	2016-09-14 14:38:04	0	140.140.1.5:81	140.140.1.5:81/at_	140.140.1.200	Block	Triggered Event	3
SQL Injection Attack	2016-09-14 14:34:42	0	140.140.1.5:81	140.140.1.5:81/at_	140.140.1.200	Block	Triggered Event	2

Table 3-2 describes parameters for querying historical security events.

Table 3-2 Parameters for querying historical security events

Parameter	Description
Event Type	Specifies types of security events to be queried. The event types are built in the web-based manager.
Start Time	Specifies the time when security events to be queried occurred.
Destination IP Address	Specifies the destination IPv4 or IPv6 address of security events to be queried.
Destination Port	Specifies the destination port of security events to be queried.
URL	Specifies the destination URL of security events to be queried.

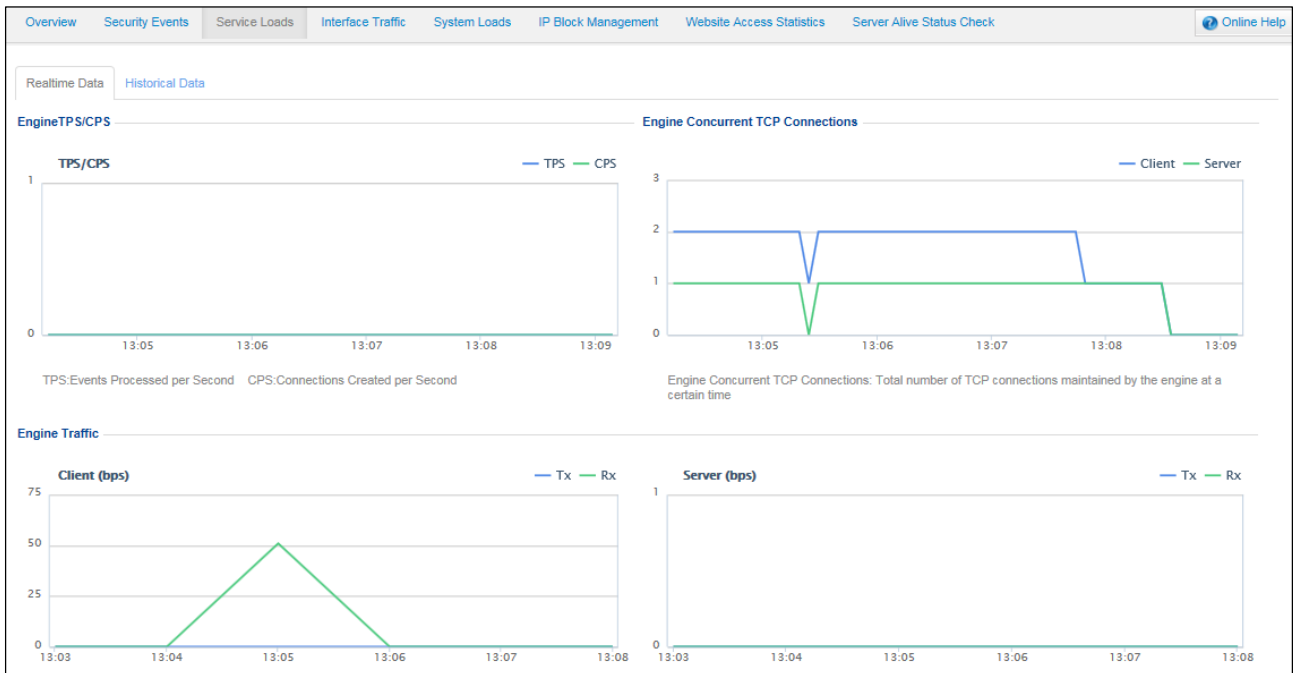
3.3 Service Loads

The **Service Loads** page shows real-time and historical data on the traffic through the port of the engine. Historical data lags behind real-time data by 1–2 minutes.

3.3.1 Viewing Real-Time Data

Choose **System Monitoring** > **Service Loads**. The **Realtime Data** page appears, as shown in [Figure 3-5](#).

Figure 3-5 Service loads — real-time data



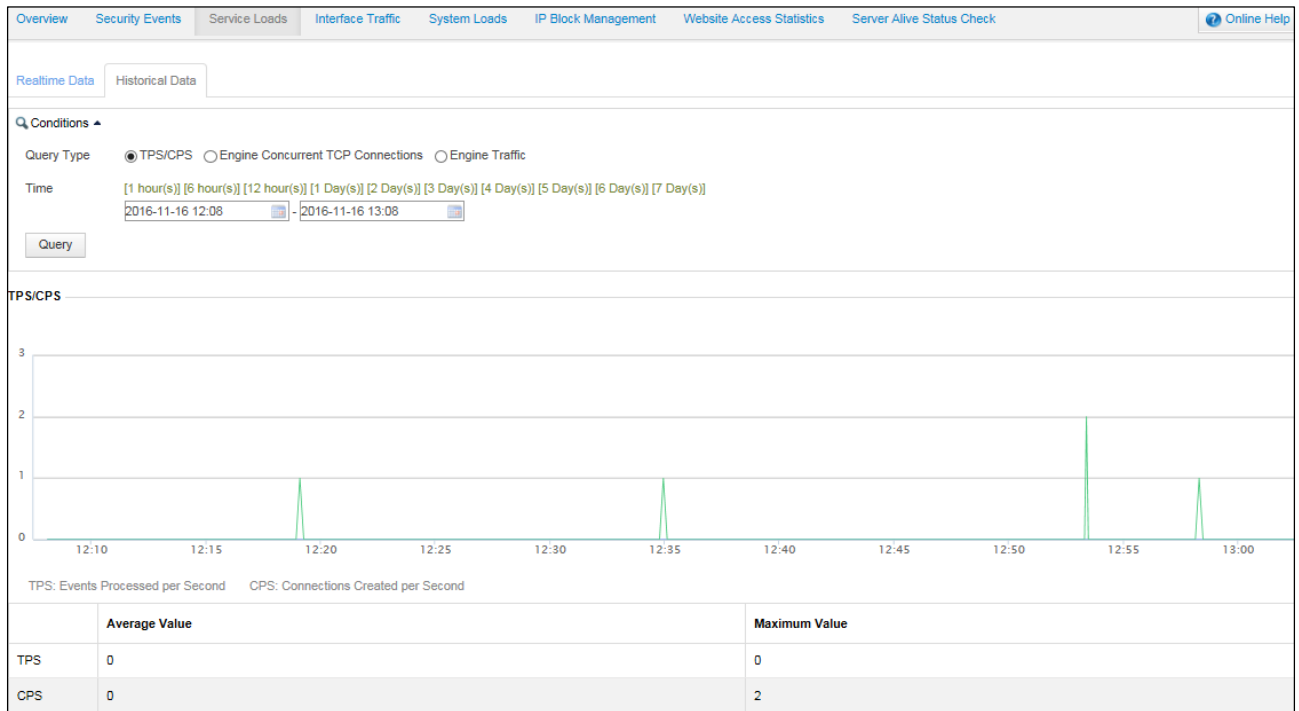
This page shows the following service load data of the engine in the last 5 minutes:

- TPS/CPS
- Concurrent TCP connections
- Engine traffic (Rx and Tx) on the client and server

3.3.2 Querying Historical Data

Choose **System Monitoring > Service Loads > Historical Data**. The **Historical Data** page appears, as shown in [Figure 3-6](#).

Figure 3-6 Service loads — historical data



This page shows following historical load data of the engine in a specified period:

- TPS/CPS
- Concurrent TCP connections
- Engine traffic on the client and server

You can query the historical data of a specific type of service load in a given period by setting parameters listed in [Table 3-3](#).

Table 3-3 Parameters for querying historical service load data

Parameter	Description
Query Type	Specifies the type of service load to be queried. The value can be TPS/CPS , Engine Concurrent TCP Connections , or Engine Traffic .
Built-in time periods	Time periods built in the web-based manager. They are displayed in green, and you can click one of them to query data in the last 1 hour, 6 hours, 12 hours, 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, or 7 days.
Custom time period	Custom time period. You need to set the start time and end time to query data in a specified period.

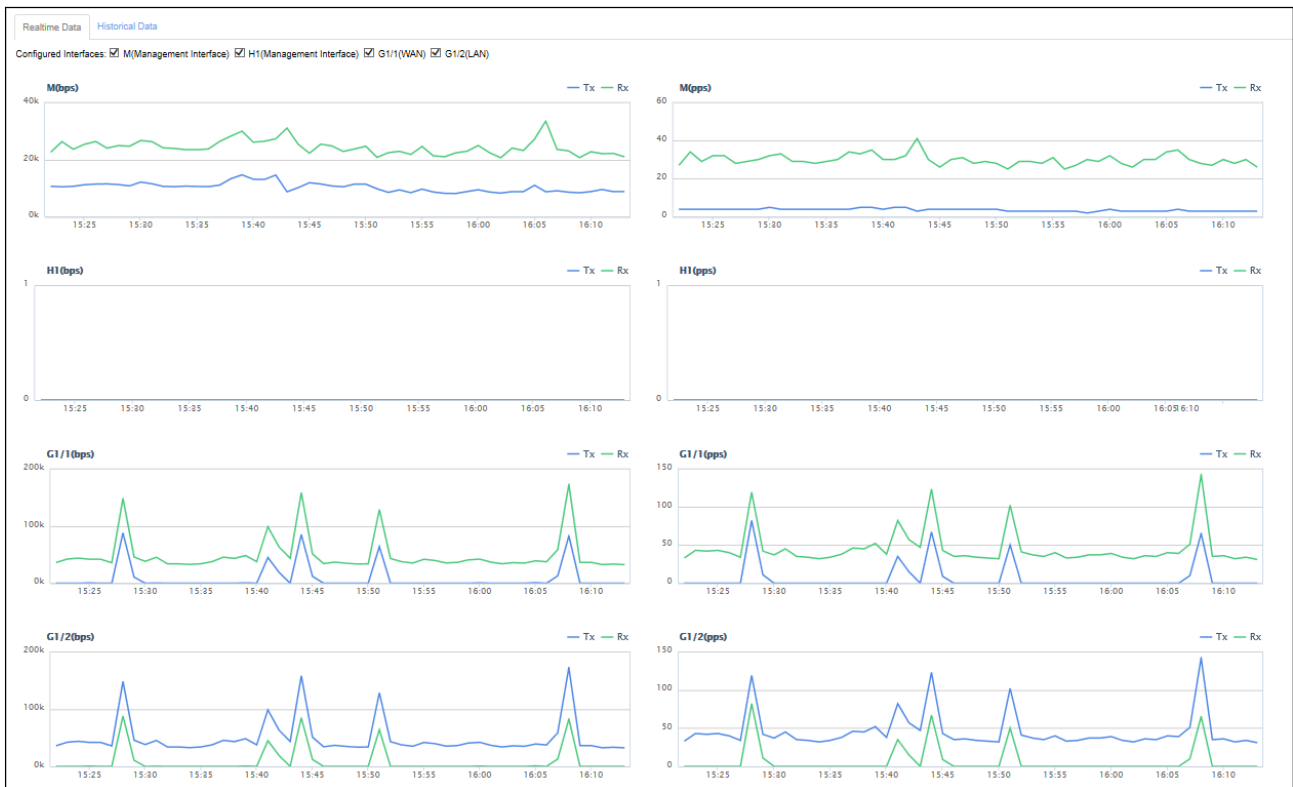
3.4 Interface Traffic Data

The **Interface Traffic** page shows real-time and historical data on traffic transmitted and received by each interface on WAF. Historical data lags behind real-time data by 1–2 minutes.

3.4.1 Viewing Real-Time Data

Choose **System Monitoring > Interface Traffic**. The **Realtime Data** page appears, as shown in [Figure 3-7](#).

Figure 3-7 Interface traffic — real-time data

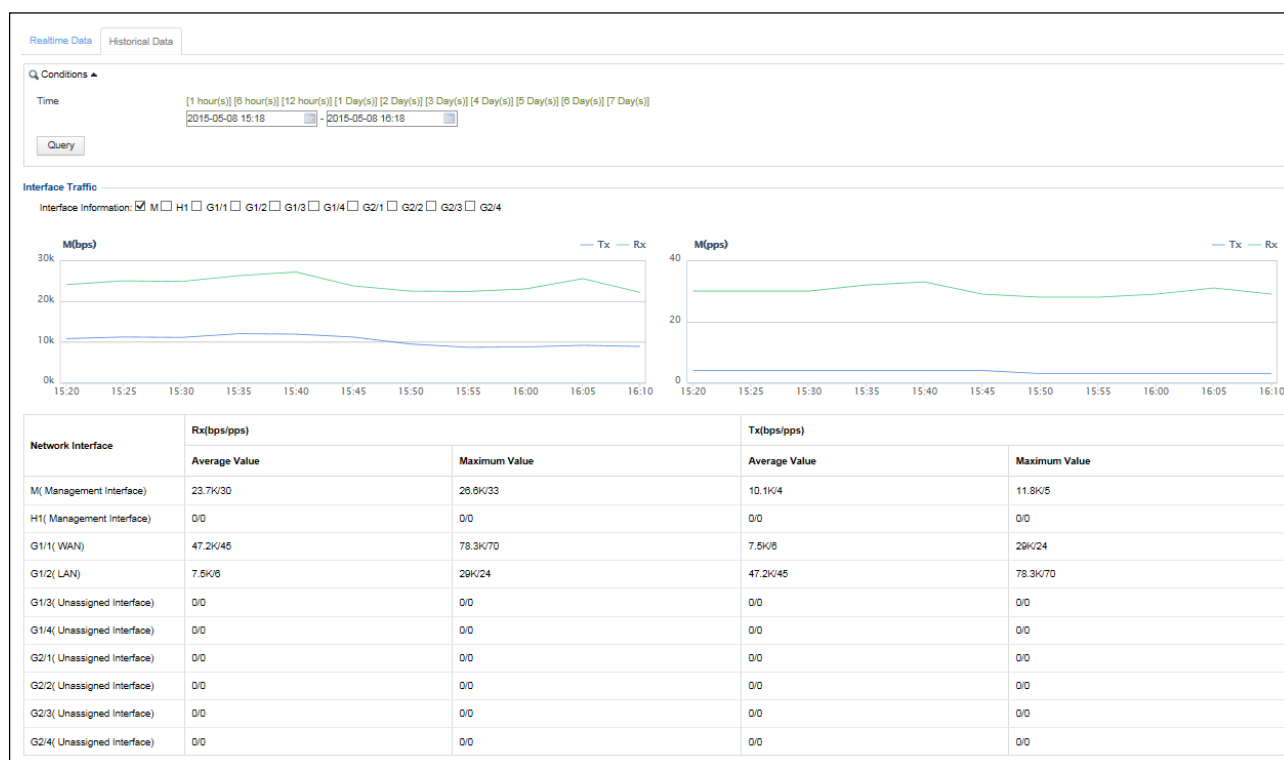


The **Realtime Data** page shows the specified interfaces' received and transmitted traffic (in bps and pps) trends in the last hour. The **Configured Interfaces** parameter in the upper-left corner provides all configured interfaces on WAF. You can select desired interfaces to view their traffic. The web-based manager memorizes your selection and displays traffic trends of the selected interfaces when you log in the next time.

3.4.2 Querying Historical Data

Choose **System Monitoring > Interface Traffic > Historical Data**. The **Historical Data** page appears, as shown in [Figure 3-8](#).

Figure 3-8 Interface traffic — historical data



The **Historical Data** page shows specified interfaces' traffic trends in a historical period, in graph and table.

- Interface traffic trend graph
The graphs show specified interfaces' traffic (in bps and pps) trend in a specified period.
- Interface traffic table
The table lists specified interfaces' maximum and average traffic (in bps and pps) in a specified period.

[Table 3-4](#) describes parameters for querying historical interface traffic data.

Table 3-4 Parameters for querying historical interface traffic data

Parameter	Description
Built-in time periods	Time periods built in the web-based manager. They are displayed in green, and you can click one of them to query data in the last 1 hour, 6 hours, 12 hours, 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, or 7 days.
Custom time	Custom time period. You need to set the start time and end time to query data in a specified period.

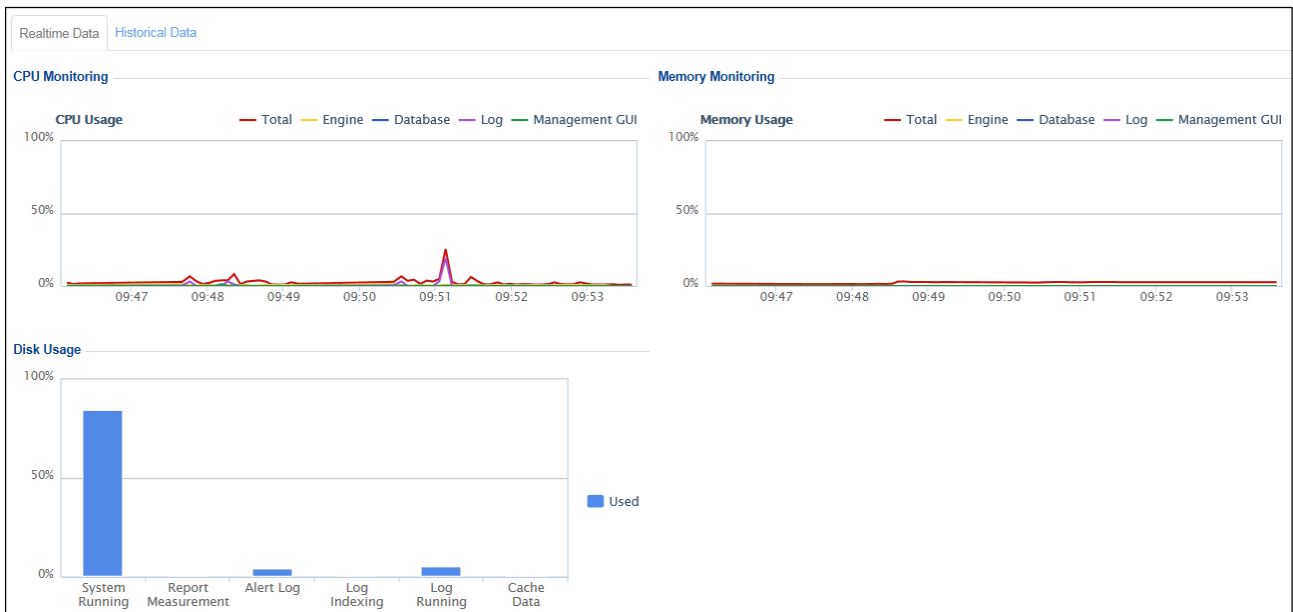
3.5 System Loads

The **System Loads** module shows the real-time and historical data on the CPU, memory, and disk usage of WAF. The historical data lags behind the real-time data by approximately 1 minute.

3.5.1 Viewing Real-Time Data

Choose **System Monitoring > System Loads**. The **Realtime Data** page appears, as shown in [Figure 3-9](#).

Figure 3-9 System loads — real-time data



The **Realtime Data** page shows the real-time disk usage, as well as CPU and memory usage trends in the last 5 minutes.

3.5.2 Querying Historical Data

Choose **System Monitoring > System Loads > Historical Data**. The **Historical Data** page appears, as shown in [Figure 3-10](#). This page shows the CPU or memory usage trend in a specific period.

Figure 3-10 System loads — historical data

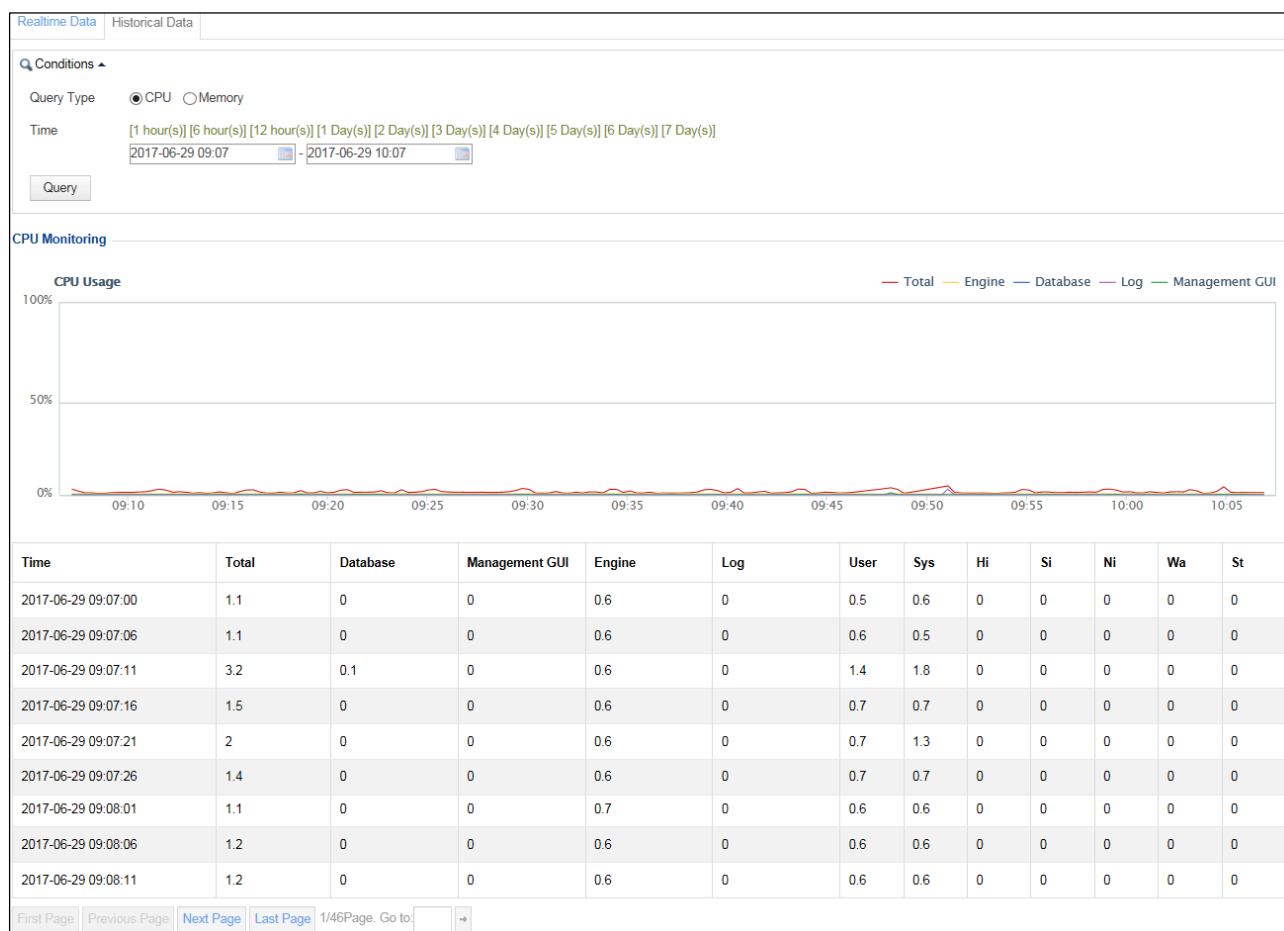


Table 3-5 describes parameters for querying historical system load data.

Table 3-5 Parameters for querying historical system load data

Parameter	Description
Query Type	Specifies the type of system load to be queried, which can be CPU or Memory .
Built-in time periods	Time periods built in the web-based manager. They are displayed in green, and you can click one of them to query data in the last 1 hour, 6 hours, 12 hours, 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, or 7 days.
Custom time period	Custom time period. You need to set the start time and end time to query data in a specified period.

3.6 IP Block Management

The **IP Block Management** page shows all events regarding block of source IP addresses after blocking policies are triggered. All HTTP requests from blocked source IP addresses are blocked by WAF until the IP addresses are unblocked. Blocked IP addresses are grouped into website groups for management. Administrators can unblock IP addresses manually.



IP block management can be performed on a website group only after the following conditions are met:

- The website group references a policy, in which **Action** is set to **Block** and **Source IP Blocking** is set to **Block as customized** or **Permanently block**.
- The policy is triggered.

Choose **System Monitoring > IP Block Management**. The **IP Block Management** page appears,

Figure 3-11 IP Block Management page

Click a website in the navigation area in the left pane to display all IP block events of the website group in the IP block list in the right pane.

- **Unblocking source IP addresses**
In the IP block event list shown in [Figure 3-11](#), select one or more source IP addresses, and click **Cancel IP Block** to unblock the IP address(es).
- **Querying block events by source IP address**
Set the **Source IP Address** parameter shown in [Figure 3-11](#) to a desired IP address, and click **Query** to view block events of the specified IP address.

3.7 Website Access Statistics

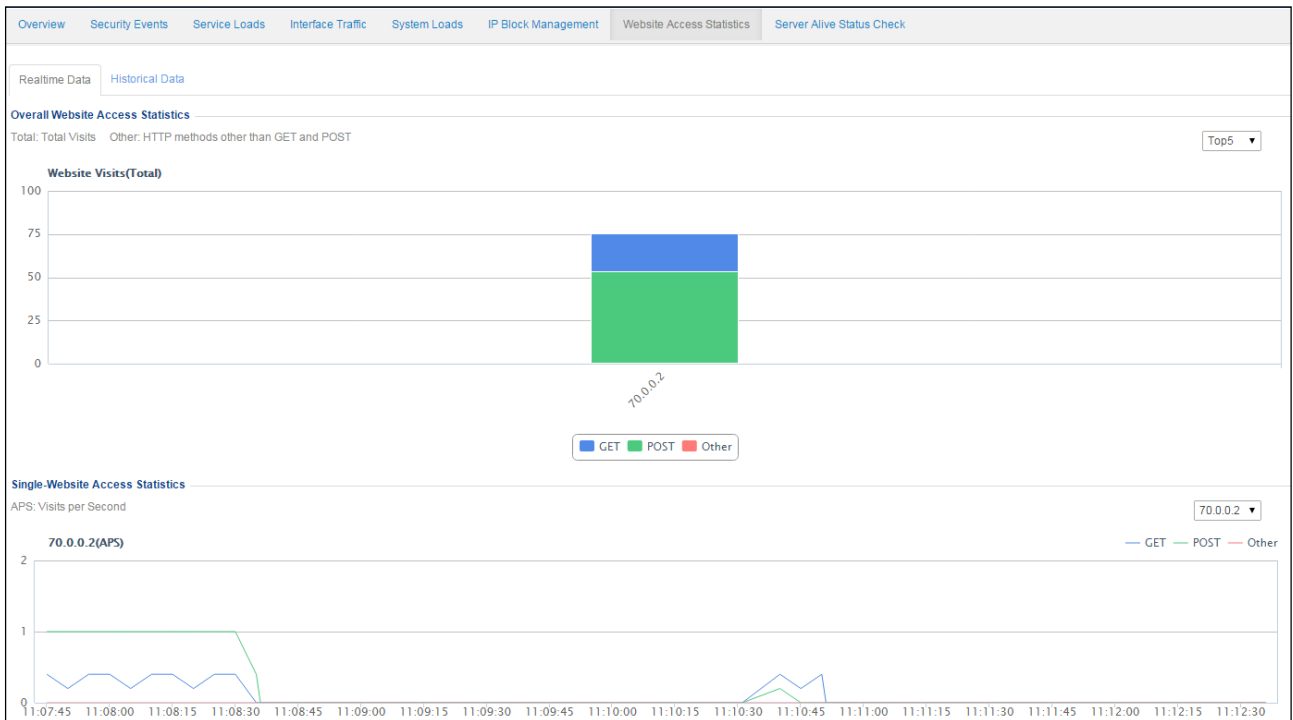
The **Website Access Statistics** module shows the real-time and historical access statistics of a specified website. The historical data lags behind the real-time data by approximately 1 minute.

Access statistics are available only for websites for which the access statistics function is enabled. For details on how to enable website access statistics, see section [4.3.1.1 Creating a Website Group](#).

3.7.1 Viewing Real-Time Data

Choose **System Monitoring > Website Access Statistics**. The **Realtime Data** page appears.

Figure 3-12 Website access statistics — real-time data



The **Realtime Data** page shows the top 5 websites by total access statistics and website access trends in the last 5 minutes.

3.7.2 Querying Historical Data

Choose **System Monitoring > Website Access Statistics > Historical Data**. The **Historical Data** page appears, as shown in [Figure 3-13](#). This page shows the total access statistics and access trends in a specific period.

Figure 3-13 Website access statistics — historical data

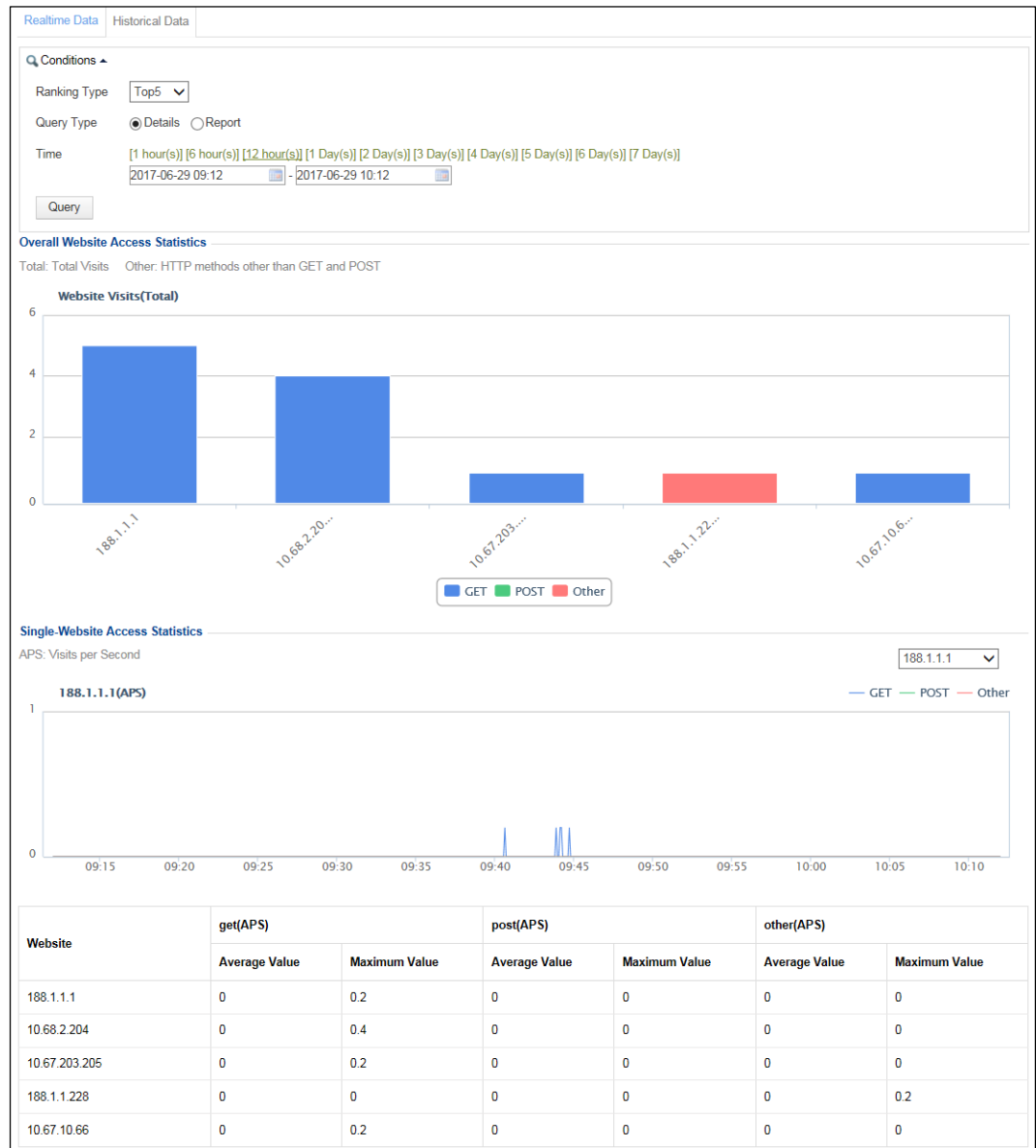


Table 3-6 describes the parameters for querying website access statistics.

Table 3-6 Parameters for querying website access statistics

Parameter	Description
Ranking Type	Specifies the ranking type, which can be Top5 , Top10 , Top15 , or Top20 .
Query Type	Specifies the query type, which can be Details or Report .
Select time	Time periods built in the web-based manager. They are displayed in green, and you can click one of them to query data in the last 1 hour, 6 hours, 12 hours, 1 day, 2 days, 3 days, 4 days, 5 days, 6 days, or 7 days.
Custom time objects	Custom time period whose start time and end time need to be specified. Data in the specified period is to be queried.

3.8 Traffic Control Data

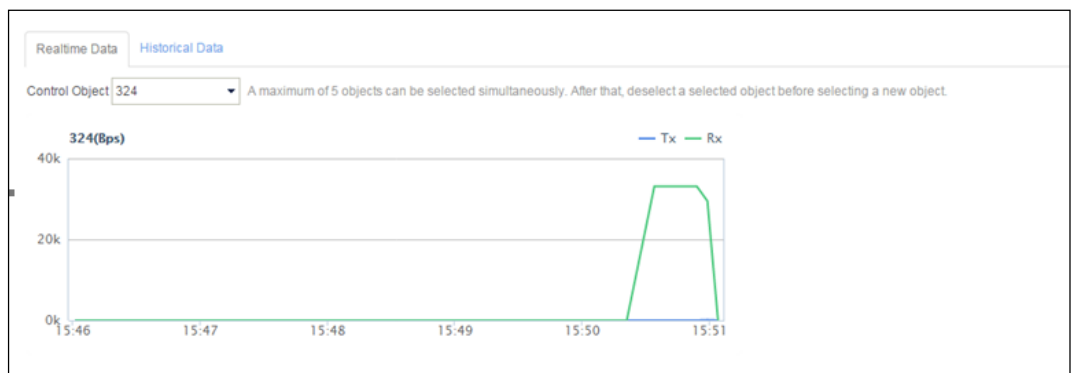
The traffic control function is available on WAF only in reverse proxy mode. For details, see section [7.7 Traffic Control Management](#).

The **Traffic Control** module presents the real-time data and historical data of specified objects on which the traffic rate limit is imposed. Historical data lags behind real-time data by 1–2 minutes.

3.8.1 Viewing Real-Time Data

Choose **System Monitoring > Traffic Control**. The **Realtime Data** page appears.

Figure 3-14 Traffic control — real-time data



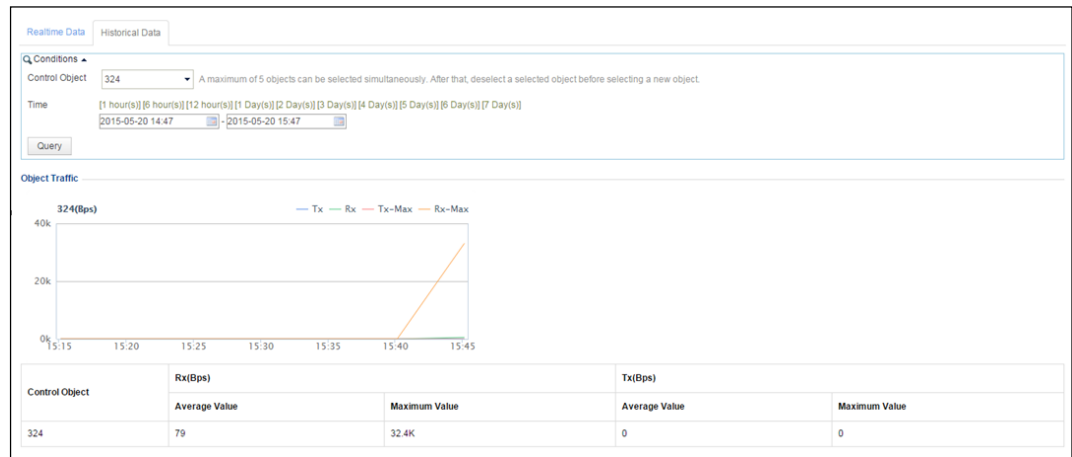
This page presents the real-time traffic trends of traffic control objects in the last 5 minutes.

Note that you can select a maximum of five traffic control objects each time.

3.8.2 Querying Historical Data

Choose **System Monitoring > Traffic Control > Historical Data**. The **Historical Data** page appears, as shown in [Figure 3-15](#).

Figure 3-15 Traffic control — historical data



This **Historical Data** page presents the data concerning WAF's traffic restriction on objects in a specific period.

3.9 Server Status Check

WAF can check the server status in in-path mode or out-of-path mode.

3.9.1 Viewing Real-Time Status

You can check the server status after you enable the server status check and manage server information.

Choose **System Monitoring > Server Alive Status Check**. The **Real-time Detection** page appears.

Figure 3-16 Server status check — real-time data



The server list displays the IP address, port, URL, and status of the added target server. In the **Operation** column, indicates that the server is active; indicates that the server is inactive; indicates that the server status check function is disabled.

Enabling/Disabling Server Status Check

As shown in [Figure 3-16](#), the server status check function is already enabled.

You can click **Close** to disable the server status check function.

Managing Servers

You can add, edit, enable, disable, reset, or delete a server.

Adding a Server

Step 1 Click **Create** in the upper right half of the server list.

Figure 3-17 Adding a server

Step 2 In the dialog box, set server parameters.


Table 3-7 Parameters for adding a server

Parameter	Description
Server IP Address	IP address of the target server.
Server Port	Port on the target server.
URL	Specifies the URL for which the server status check is performed.
Response Code	Response code returned by the target server to WAF, which can be 200 , 301 , 302 , or 401 .

Step 3 Click **OK** to save the settings.



----End

Editing a Server


On the server list, you click  in the **Operation** column and then edit its settings, including the IP address, port, URL, and response code of the server.

Enabling/Disabling the Status Check Function for Servers

You can enable or disable the status check function for servers as follows:


- On the server list, click  or  and then enable or disable the server status check function.
- On the server list, select one or more servers, click **Bulk Operation**, and select **Enable** or **Disable** to enable or disable the status check function for the server(s).

Resetting a Server

If a server with the status check function enabled is inactive, you can click  in the **Operation** column to activate this server.

Deleting Servers

On the sever list, you can delete servers as follows:

- Click  in the **Operation** column to delete a server.
- Select one or more servers, click **Bulk Operation**, and select **Delete** to delete the server(s).

3.9.2 Configuring the Server Status Check Function

Choose **System Monitoring > Server Alive Status Check**. You can click the **Inspection Configuration** tab to configure parameters for the server status check function.

Figure 3-18 Parameters for server status check

Parameter	Value	Range
Polling Detection Cycle (second)	5	(5-62400)
Single-Cycle Reconnections After Failure	4	(1-4)
Inactivity Detection Cycles	3	(1-720)

OK

Table 3-8 describes parameters for configuring the server status check function.

Table 3-8 Parameters for server status check

Parameter	Description
Polling Detection Cycle (second)	Specifies the polling check cycle for the server status. The cycle rang is 5–62400 in seconds.
Single-Cycle Reconnections After Failure	Specifies the number of reconnections initiated by WAF to the server if the first server status check failed during a polling check period. The number of reconnections varies with the polling detection cycle.
Inactivity Detection Cycles	Specifies the number of server status check cycles which the server needs to experience before exiting the inactive state. In other words, if all status checks initiated by WAF succeed during the Nth cycle, the server turns active from the inactive state.

3.10 Device Monitoring

On the **Device Monitoring** page, you can determine whether to enable alerting for the CPU/memory, partitions, and processes, and configure related alerting thresholds.

Choose **System Monitoring > Device Monitoring**. The **Device Monitoring** page appears.

Figure 3-19 Device Monitoring page

The screenshot displays the 'Device Monitoring' configuration page, which is divided into three main sections: CPU/MEM Monitoring, Partition Monitoring, and Process Monitoring.

- CPU/MEM Monitoring:** This section allows setting alert-triggering thresholds for CPU usage and memory usage. It includes a 'Monitoring Alert' toggle (set to 'Enable'), a 'CPU Alert Threshold' slider (set to 75%), and a 'MEM Alert Threshold' slider (set to 75%). An 'OK' button is present.
- Partition Monitoring:** This section sets usage thresholds for partitions. It includes a 'Monitoring Alert' toggle (set to 'Enable'), a 'Normal Threshold' slider (set to 85%), a 'Backup before clearance' toggle (set to 'Yes'), and a 'Critical Threshold' slider (set to 90%). An 'OK' button is present.
- Process Monitoring:** This section enables process monitoring to monitor the validity of processes in real time. It includes a 'Monitoring Alert' toggle (set to 'Enable') and an 'OK' button.

- CPU/memory monitoring

First, determine whether to enable the CPU/memory alerting. After this function is enabled, set the alerting threshold for the CPU/memory usage. If a specified threshold is reached, an alert is triggered and recorded in system running logs.

- Partition monitoring

First, determine whether to enable the partition alerting. After this function is enabled, set two thresholds for WAF to monitor the usage of critical partitions (such as the alert log partition) that store logs during the device running.

- Normal threshold

If the usage of a critical partition exceeds the specified normal threshold, WAF generates a running log, showing the actual usage of the critical partition and normal threshold. If this situation lasts for a period of time, running logs will be generated repeatedly. For the alert log partition, WAF clears all preceding logs when generating running logs. You can set **Backup before clearance** to determine whether to back up logs before WAF clears them.

- Critical threshold

If the usage of a critical partition exceeds the specified critical threshold, WAF generates a running log, showing the actual usage of the critical partition and critical threshold. If this situation lasts for a period of time, running logs will be generated repeatedly. For the alert log partition, WAF clears all preceding logs without backup when generating running logs.

Table 3-9 describes parameters for partition monitoring.

Table 3-9 Parameters for partition monitoring

Parameter	Description
Normal Threshold	If the usage of a critical partition exceeds the specified normal threshold, WAF generates a running log. For the alert log partition, WAF clears all preceding logs.
Backup before clearance	Controls whether to back up logs before they are cleared when the specified normal threshold is triggered.
Critical Threshold	If the usage of a critical partition exceeds the specified critical threshold, WAF

Parameter	Description
	generates a running log. For the alert log partition, WAF directly clears all preceding logs without backup.

- Process monitoring

After process monitoring is enabled, WAF can monitor the validity of processes in real time.

3.11 System Information

WAF provides basic system information in the status bar, including engine status, interface status, CPU and memory usage, license status, system time, and system uptime, as shown in [Figure 3-20](#).

Figure 3-20 Status bar



[Table 3-10](#) describes details about items in the status bar.

Table 3-10 Status bar information

Item	Description
	Indicates the engine status. <ul style="list-style-type: none"> : debugging state : abnormal state : normal state
	Provides a shortcut for viewing interface information. Pointing to Interface Status automatically displays interface configurations, including interface names, interface types, interface status, interface rates, and duplex modes. Clicking Interface Status displays the Work Group Management page under System Management > Network Configuration > Work Group Management .
	Indicates the CPU and memory usage and provides a shortcut for viewing system loads. Clicking it displays the Realtime Data page under System Monitoring > System Loads .
	Provides a shortcut for viewing the license status. Clicking Valid license displays the License page under System Management > License .
	Displays the current system time and provides a shortcut for time management. Clicking it brings you to the Time & Language page in the System Management module.

Item	Description
Running Time: 1hour(s) 16Minute(s)	Displays system uptime information.

4 Security Management

This chapter covers the following topics:

Topic	Description
Network-Layer Protection	Describes how to configure network-layer protection.
Website Protection	Describes how to configure website protection.
Auto-Learning Policies	Describes how to configure auto-learning policies.
Auto-Learning Results	Describe how to view auto-learning results.
Rule Database Management	Describes how to view and configure custom rule database.
Policy Management	Describes how to configure policies on WAF.
Template Management	Describes how to configure policy templates.
Smart Patching	Describes how to configure smart patches.
Secure Delivery	Describes how to configure security delivery.
Proxy Configuration Information	Describes how to configure a proxy.
Uploaded File Management	Describes how to manage SSL certificates and XSD/WSDL files.
IP Reputation	Describes IP reputation categories and how to configure IP reputation protection.

4.1 Overview

This section describes the protection idea, system, and procedure of WAF.

Protection Idea

Like a guard, WAF protects a website in three stages:

- Prevention in advance
 - Web vulnerability scanning: Via the built-in scanner, WAF can detect vulnerabilities in websites and fix them before websites are attacked.
 - Smart patching: Via the unique cloud service function, WAF can regularly detect changes of website vulnerabilities and apply smart patches, enabling users to dynamically tune protection policies in time.

- In-process protection
 - Policy configuration: Via various policies you configure, WAF can perform real-time protection on website servers under attack.
 - Auto-learning policy configuration: Via auto-learning policies you have configured for websites, WAF automatically learns about the data and traffic patterns of websites, enabling you to configure precise whitelist policies. This provides more precise protection on servers.
- Secure delivery afterwards

Despite prevention in advance and in-process protection, attackers may still be able to deface web pages. In this case, WAF can apply anti-defacement policies to shield web servers from defaced contents, enabling clients to access normal website content.

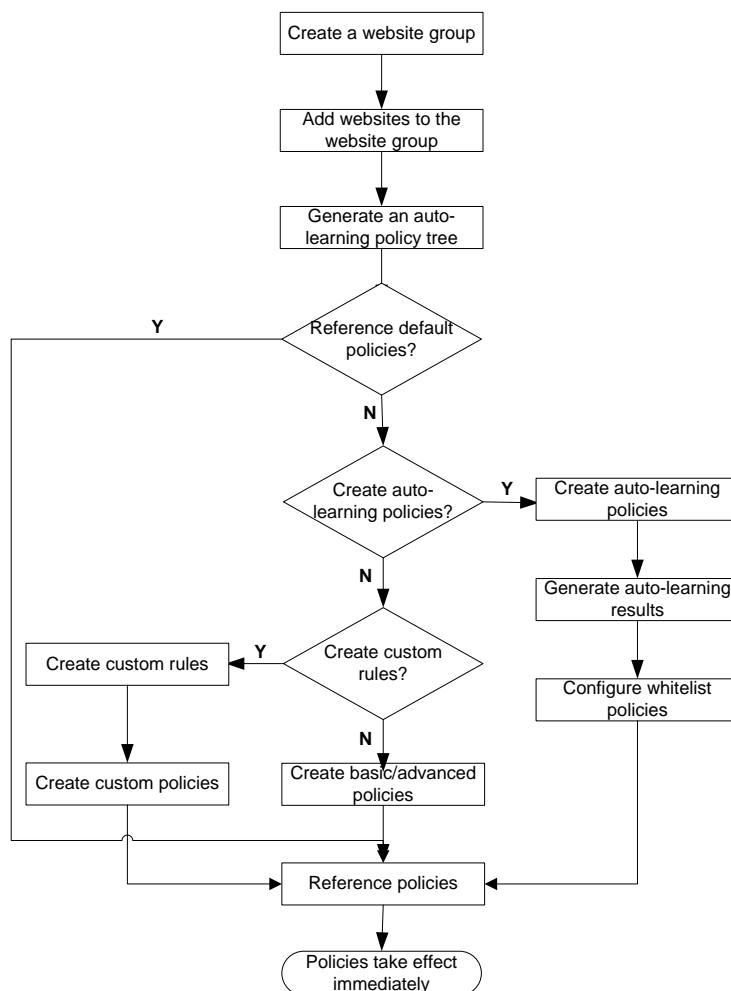
Protection System

Attacks or defacements against websites will exert adverse social impacts and cause immeasurable loss to website owners. WAF, deployed between clients and web servers, effectively blocks or eases attacks against servers via multi-layer protection.

Protection Procedure

Generally, servers protected by WAF appear as websites on the web-based manager. [Figure 4-1](#) shows how to create websites and configure protection policies for such websites.

Figure 4-1 Website protection configuration procedure



4.2 Network-Layer Protection

The network-layer protection function does not work on WAF in mirroring mode.

As the first protection line provided by WAF, network-layer protection is the global protection for the network layer. Network-layer protection includes the following:

- Network-layer access control
- TCP flood protection
- ARP spoofing protection
- WAF-ADS collaboration configuration

4.2.1 Enabling/Disabling Policies

The Policy Enable-Disable module controls whether to enable or disable network-layer access control, TCP flood protection, ARP spoofing protection, ADS collaboration, and transparent transmission protection. To make a specific policy take effect, you must first enable this policy.

Choose **Security Management > Network-Layer Protection > Policy Enable-Disable**. You can view, enable, and disable policies in the policy list on the **Policy Enable-Disable** page shown in [Figure 4-2](#).

Figure 4-2 Network-layer protection — enabling and disabling policies

Policy Enable-Disable Network-Layer Access Control TCP Flood Protection ARP Spoofing Protection ADS Collaboration Config		
Policy Name	Status	Operation
Network-Layer Access Control	✓	⏏
TCP Flood Protection	✓	⏏
ARP Spoofing Protection	✗	▶
ADS Collaboration	✗	▶
Transparent Transmission Protection ?	✗	▶

By default, the network-layer access control and TCP flood protection policies are enabled (✓), and the ARP spoofing protection, ADS collaboration, and transparent transmission protection are disabled (✗).

- Enabling a policy
In the policy list shown in [Figure 4-2](#), click ▶ in the **Operation** column to enable a policy. After a policy is enabled, its status turns to ✓.
- Disabling a policy
In the policy list shown in [Figure 4-2](#), click ⏏ in the **Operation** column to disable a policy. After a policy is disabled, its status turns to ✗.

4.2.2 Configuring Network-Layer Access Control

The network-layer access control function mainly controls the network layer and transport layer. It is a firewall function. WAF integrates this function to enable users to configure network-layer access control on WAF.

This function is available only when WAF is deployed in in-path mode and out-of-path mode, but unavailable when WAF is in reverse proxy mode and mirroring mode.



Network-layer access control is the first step of protection in WAF. WAF matches packets against the network-layer access control policy prior to any other policies.

Creating a Network-Layer Access Control Policy

To create a network-layer access control policy, perform the following steps:

Step 1 Choose **Security Management > Network-Layer Protection > Network-Layer Access Control**.

Figure 4-3 Network-layer protection — network-layer access control

Policy Enable-Disable Network-Layer Access Control TCP Flood Protection ARP Spoofing Protection ADS Collaboration Config										
Name	Status	Destination Network		Source Network		Protocol	Network Interface	Action	Alert or Not	Operation
		Network Address/Mask	Port Range	Network Address/Mask	Port Range					
test		10.67.1.201/255.255.255.255		10.67.3.201/255.255.255.255		Unlimited	G1/1	Block	Yes	
<div>Create</div>										

Step 2 Click **Create**.

Figure 4-4 Creating a network-layer access control policy

Create

Name

Destination IP Address/Mask - Source IP Address/Mask

Protocol

Unlimited

Network Interface

G1/1

Action

Block

Alert or Not

☒ Yes ☐ No

Enable or Not

☒

OK

Cancel

Step 3 In the dialog box, set the parameters.

Table 4-1 Parameters for creating a network-layer access control policy

Parameter	Description
Name	Specifies the policy name.
Destination IP Address/Mask-Source IP Address/Mask	Specifies a pair of destination IP address/subnet mask and source IP address/subnet mask. Both IPv4 and IPv6 addresses are allowed here. You can click to add multiple pairs of destination IP address/subnet mask and source IP address/subnet mask. A maximum of 50 entries can be specified for either address type.
	Note

Parameter	Description
	<ul style="list-style-type: none"> A maximum of 10 entries can be specified in a box for either address type. Multiple entries must be separated by carriage returns. Each pair of boxes supports one-to-many correspondence. That is to say, you can type one entry in the destination IP address/subnet mask box but multiple entries in the source IP address/subnet mask box, and vice versa. <p>If the same address pair exists in more than one policy, it should be handled as indicated in the policy matched first.</p>
Protocol	<p>Specifies the protocol of matching packets. The value can be ICMP, ICMPV6, TCP, UDP, or Unlimited. Unlimited specifies that all protocols are included.</p> <p>If TCP or UDP is selected, you also need to configure the source port range and destination port range of the target traffic.</p>
Network Interface	Specifies the interface from which WAF receives packets.
Action	<p>Specifies the action on a packet that matches this new policy:</p> <ul style="list-style-type: none"> Block: WAF discards the packet and disconnects the current TCP connection. Accept: WAF continues to match the packet against other policies. Forward: WAF directly forwards the packet without matching them against other policies.
Alert or Not	Controls whether to generate alert logs.
Enable or Not	Controls whether to enable the policy.



Network-layer access control policies take effect across the network. Note the following during policy configuration:

- If **Action** is set to **Block** or **Forward**, this policy must be configured on a WAN interface.
- If **Action** is set to **Accept**, this policy must be configured on both a WAN interface and a LAN interface.

Step 4 Click **OK** to save the settings.

----End

Editing a Network-Layer Access Control Policy

You can edit the parameter settings of a network-layer access control policy after it is configured. To do that, perform the following steps:


Step 1 In the policy list shown in [Figure 4-3](#), click  in the **Operation** column.

Step 2 In the dialog box, edit parameters of the policy and click **OK** to save settings and return to the policy list.





----End

Deleting a Network-Layer Access Control Policy

You can delete network-layer access control policies one by one.

In the policy list shown in [Figure 4-3](#), click  in the **Operation** column and then click **OK** in the conformation dialog box to delete a policy.

Enabling/Disabling a Network-Layer Access Control Policy

- In the policy list shown in [Figure 4-3](#), click  in the **Operation** column to enable a policy. After a policy is enabled, the policy status turns to .
- In the policy list shown in [Figure 4-3](#), click  in the **Operation** column to disable a policy. After a policy is disabled, the policy status turns to .

4.2.3 Configuring TCP Flood Protection

The TCP flood protection function does not work on WAF in mirroring mode.

According to the working principle of TCP/IP, only a certain amount of TCP/IP connections are allowed. Attackers exploit this to launch TCP flood attacks, which are divided into two types:

- **SYN flood attacks**
An attacker sends too many SYN packets to a target server for processing, exhausting the server's resources and making the server unresponsive to legitimate traffic.
- **ACK flood attacks**
An attacker sends a target server too many ACK packets for processing, exhausting the server's resources and making the server unresponsive to legitimate traffic.

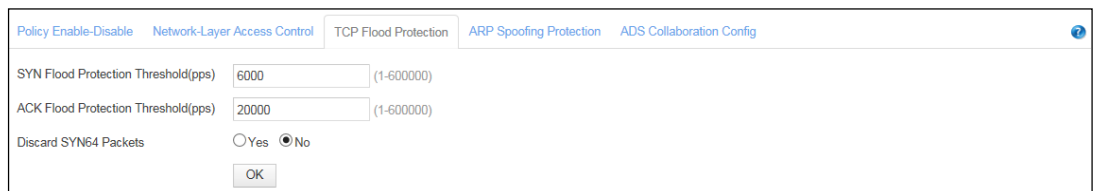
The TCP flood protection policy protects against SYN flood attacks and ACK flood attacks based on thresholds specified for the two types of attacks.

WAF counts the number of packets from each client per second. If the number of packets from a client exceeds the threshold, WAF determines that an attack occurs, and starts protection against the attack.

To configure the TCP flood protection policy, perform the following steps:

Step 1 Choose **Security Management > Network-Layer Protection > TCP Flood Protection**.

Figure 4-5 Network-layer protection — TCP flood protection



Step 2 Edit TCP flood protection parameters.

Table 4-2 Parameters for editing the TCP flood protection policy

Parameter	Description
SYN Flood Protection Threshold(pps)	Specifies the SYN flood attack threshold. WAF determines that an SYN flood attack occurs when the number of SYN packets received from a client per second exceeds the threshold. The default value is 6000 .
ACK Flood Protection Threshold(pps)	Specifies the ACK flood attack threshold. WAF determines that an ACK flood attack occurs when the number of ACK packets received from a client per second exceeds the threshold. The default value is 20000 .
Discard SYN64 Packets	Controls whether to discard SYN packets if the options field is empty.

Step 3 Click **OK** to save the settings.

Step 4 Enable this policy on the **Policy Enable-Disable** page.

----End

4.2.4 Configuring ARP Spoofing Protection

Common Address Resolution Protocol (ARP) attacks are divided into two types:

- False gateway

An ARP virus sends a false gateway-MAC binding relationship to the victim, which could result in the following problems:

 - From the perspective of Denial-of-Service (DoS) attacks, the communication between the victim and the real gateway may be broken, and the victim's responses cannot reach the real gateway, causing DoS.
 - From the perspective of data security, the victim's response is sent to the host with the MAC address specified by the attacker. Once the attacker obtains the data, or even worse, forwards tampered data to the real gateway, data theft and tampering can be caused.
- False end user/server
 - Gateway spoofing

A false IP-MAC binding relationship is sent to the gateway, disabling the gateway from communicating with the real end user, and possibly resulting in data theft and tampering due to transmission to the false end user.
 - End user spoofing

A false IP-MAC binding of an end user/server is sent to another end user, disabling the two end users from communicating with each other.

After ARP spoofing protection is enabled, WAF first learns IP-MAC binding relationships. When receiving the first ARP packet (ARP query or ARP response) from a server whose IP address is specified in "Proxy Service", WAF will record the IP-MAC binding relationship and take it as the standard IP-MAC binding relationship of the server.

After the **Auto-Learning MAC Address Table** is established, WAF performs ARP protection based on the standard IP-MAC binding relations in the list. For packets received over the LAN interface, if their source IP addresses and ports are the same as those specified in "Proxy

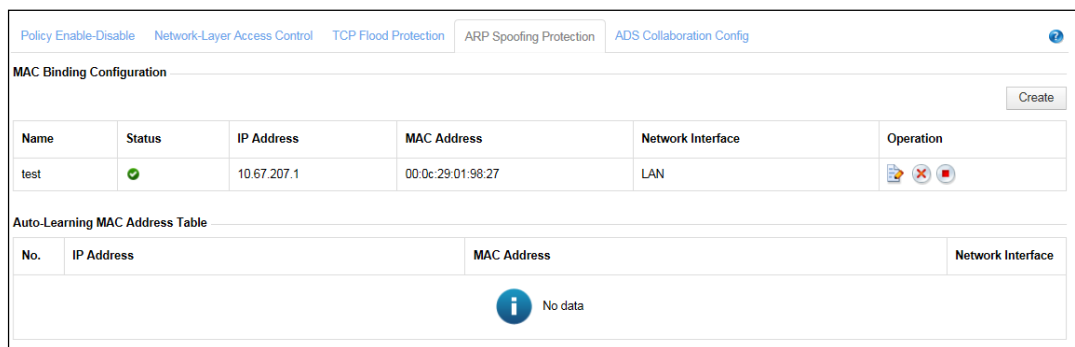
Service", their MAC addresses must be the same as the corresponding MAC addresses recorded in the **Auto-Learning MAC Address Table**.

On the **ARP Spoofing Protection** page, you can view the **Auto-Learning MAC Address Table**, and create, edit, delete, enable, and disable IP-MAC binding relationships in the **MAC Binding Configuration** list. The following describes how to view auto-learned IP-MAC binding relationships in the **Auto-Learning MAC Address Table** and create an IP-MAC binding relationship in the **MAC Binding Configuration** list. The operations of editing, deleting, enabling, and disabling an IP-MAP binding relationship are the same as those for network-layer access control policies.

4.2.4.1 Viewing the Auto-Learning MAC Address Table

Choose **Security Management > Network-Layer Protection > ARP Spoofing Protection**. The **ARP Spoofing Protection** page appears, as shown in [Figure 4-6](#). You can view auto-learned IP-MAC binding relationships in the **Auto-Learning MAC Address Table**.

Figure 4-6 Network-layer protection — ARP spoofing protection



4.2.4.2 Creating an IP-MAC Binding Relationship

In the **MAC Binding Configuration** list shown in [Figure 4-6](#), click **Create**. Then set parameters in the **Create** dialog box to create an IP-MAC binding relationship.

Figure 4-7 Creating an IP-MAC binding relationship

Create [X]

Name

IP Address IPv6 addresses are not allowed.

MAC Address MAC address format: 00:0C:29:01:98:27

Network Interface LAN ▼

Enable or Not ☒

OK Cancel

Table 4-3 Parameters for creating an IP-MAC binding relationship

Parameter	Description
Name	Name of the new IP-MAC binding relationship.
IP Address	IP address of the new IP-MAC binding relationship. This parameter can be set only to the IP address of a proxied server or gateway. Only IPv4 IP addresses are supported.
MAC Address	MAC address of the new IP-MAC binding relationship. This parameter can be set only to the MAC address of a proxied server or gateway.
Network Interface	Interface over which WAF detects IP-MAC binding relationships. This parameter can be set to WAN or LAN . Generally, this parameter is set to WAN if MAC Address is set to the MAC address of a gateway, or is set to LAN if MAC Address is set to the MAC address of a proxied server.
Enable or Not	Controls whether to enable the new IP-MAC binding relationship.



Note

- After being established, the **Auto-Learning MAC Address Table** cannot be automatically refreshed. You need to add IP-MAC binding relationships manually.
- After the system restarts, WAF automatically learns IP-MAC binding relationships and establishes the **Auto-Learning MAC Address Table** again.
- WAF performs ARP spoofing protection only on servers whose IP addresses are specified for the proxy service.

4.2.5 Configuring WAF-ADS Collaboration

WAF can collaborate with NSFOCUS Anti-DDoS System (ADS) which functions as an abnormal traffic inspection device, providing a more powerful solution for web security protection and DDoS protection.



WAF, when in mirroring mode, cannot collaborate with ADS.

Usually, WAF protects against TCP flood attacks. However, WAF's protection capability against TCP flood is limited. Upon detecting that traffic exceeds a specified threshold, WAF automatically notifies ADS. ADS automatically diverts abnormal traffic for cleansing and injects legitimate traffic back into WAF. In this way, WAF provides better web security protection.

WAF's collaboration with ADS can work in one of the following modes:

- **Single-IP diversion**
You need to configure thresholds (SYN pps, ACK pps, total pps, and total bps) for a target IP address. Diversion is triggered when the traffic destined for an IP address reaches any of the thresholds. Then ADS begins to divert such traffic.
- **Overall-traffic diversion**
You need to configure the overall traffic threshold (pps and bps). When the overall traffic reaches the threshold, the IP address with the largest traffic will be subject to traffic diversion by ADS.
- **Hybrid diversion (the preceding modes are enabled simultaneously)**
You need to configure the thresholds for both single-IP and overall traffic. ADS diversion is triggered when either of the thresholds is reached.

Configuring WAF-ADS Collaboration

Configurations need to be conducted on both WAF and ADS to implement collaboration. For details, see related description in the *NSFOCUS WAF V6.0 Configuration Guide*. This section describes related configurations on WAF.



Before configuring WAF-ADS collaboration, choose **Security Management > Network-Layer Protection > Policy Enable-Disable** and confirm that **ADS Collaboration** is enabled. For details, see section [4.2.1 Enabling/Disabling Policies](#).

To configure WAF-ADS collaboration on WAF, perform the following steps:

Step 1 Choose **Security Management > Network-Layer Protection > ADS Collaboration Config**.

Figure 4-8 Network-layer protection — ADS collaboration configuration

Policy Enable-Disable Network-Layer Access Control TCP Flood Protection ADS Collaboration Config

Diverted IP Status List

Basic Configuration

Collaboration with ADS ☐ Yes ☒ No

Running Mode Overall-Traffic Diversion ?

ADS IP and Port IP Address 0.0.0.0 Port 443 + Test

Time of Stopping Traffic Diversion ? ☒ Automatically ☒ Scheduled 3600 minutes later, traffic diversion will be stopped.

Overall Traffic ?

Statistic Dimension ☐ pps ☒ bps ☐ pps and bps

Traffic Rate (bps) Notification Threshold 800 Mbps (1-2000000000)bps

Advanced Options>>

OK

Diversion-Allowed IPs

Diversion-Allowed IPs 0.0.0.0-255.255.255.255 ?

Diversion-Allowed IPs

Diversion-Allowed IPs 0.0.0.0-255.255.255.255 ?

Step 2 Configure basic information.

- a. Select the running mode.

Different running modes correspond to different parameters.

- Figure 4-9 shows the configuration page when **Single-IP Diversion** is selected for **Running Mode**.

Figure 4-9 Configuring single-IP diversion

Basic Configuration	
Collaboration with ADS	<input type="radio"/> Yes <input checked="" type="radio"/> No
Running Mode	Single-IP Diversion ?
ADS IP and Port	IP Address <input type="text" value="0.0.0.0"/> Port <input type="text" value="443"/> + Test
Time of Stopping Traffic Diversion ?	<input type="radio"/> Automatically <input checked="" type="radio"/> Scheduled <input type="text" value="3600"/> minutes later, traffic diversion will be stopped.
Single-IP Traffic ?	
SYN Flood Notification Threshold	<input type="text" value="140000"/> <input type="text" value="pps"/> (6000-1500000)pps
ACK Flood Notification Threshold	<input type="text" value="140000"/> <input type="text" value="pps"/> (20000-1500000)pps
Traffic Rate (pps) Notification Threshold	<input type="text" value="14000"/> <input type="text" value="pps"/> (1-1500000)pps
Traffic Rate (bps) Notification Threshold	<input type="text" value="90"/> <input type="text" value="Mbps"/> (1-2000000000)bps
Advanced Options<<	
Query Interval	<input type="text" value="30"/> (5-1440)minutes
Retry Interval After Failed Notification	<input type="text" value="30"/> (30-86400)seconds
Maximum Number of Queries	<input type="text" value="5"/> ?
Maximum Number of Notification	<input type="text" value="100"/> ?
OK	

- [Figure 4-10](#) shows the configuration page when **Overall-Traffic Diversion** is selected for **Running Mode**.

Figure 4-10 Configuring overall-traffic diversion

Basic Configuration	
Collaboration with ADS	<input type="radio"/> Yes <input checked="" type="radio"/> No
Running Mode	Overall-Traffic Diversion ?
ADS IP and Port	IP Address <input type="text" value="0.0.0.0"/> Port <input type="text" value="443"/> <input type="button" value="+"/> <input type="button" value="Test"/>
Time of Stopping Traffic Diversion ?	<input type="radio"/> Automatically <input checked="" type="radio"/> Scheduled <input type="text" value="3600"/> minutes later, traffic diversion will be stopped.
Overall Traffic ?	
Statistic Dimension	<input type="radio"/> pps <input checked="" type="radio"/> bps <input type="radio"/> pps and bps
Traffic Rate (bps) Notification Threshold	<input type="text" value="800"/> <input type="text" value="Mbps"/> (1-2000000000)bps
Advanced Options<<	
Query Interval	<input type="text" value="30"/> (5-1440)minutes
Retry Interval After Failed Notification	<input type="text" value="30"/> (30-86400)seconds
Maximum Number of Queries	<input type="text" value="5"/> ?
Maximum Number of Notification	<input type="text" value="100"/> ?
<input type="button" value="OK"/>	

- [Figure 4-11](#) shows the configuration page when **Hybrid Diversion** is selected for **Running Mode**.

Figure 4-11 Configuring hybrid diversion

Basic Configuration

Collaboration with ADS

☐ Yes
☒ No

Running Mode

Hybrid Diversion

ADS IP and Port

IP Address

0.0.0.0

Port

443

+

Test

Time of Stopping Traffic Diversion

☐ Automatically
☒ Scheduled

3600

minutes later, traffic diversion will be stopped.

Single-IP Traffic

SYN Flood Notification Threshold

140000

pps

(6000-1500000)pps

ACK Flood Notification Threshold

140000

pps

(20000-1500000)pps

Traffic Rate (pps) Notification Threshold

14000

pps

(1-1500000)pps

Traffic Rate (bps) Notification Threshold

90

Mbps

(1-2000000000)bps

Overall Traffic

Statistic Dimension

☐ pps
☒ bps
☐ pps and bps

Traffic Rate (bps) Notification Threshold

800

Mbps

(1-2000000000)bps

Advanced Options<<

Query Interval

30

(5-1440)minutes

Retry Interval After Failed Notification

30

(30-86400)seconds

Maximum Number of Queries

5


Maximum Number of Notification



100

OK

b. Configure parameters under **Basic Configuration**.

Table 4-4 Parameters for configuring single-IP diversion

Parameter	Description
Collaboration with ADS	Controls whether to enable WAF's collaboration with ADS. ADS collaboration can work only when you select Yes .
ADS IP and Port	IP address (IPv4 and IPv6) and port of the management interface of ADS. After the IP address is configured, clicking Test displays the current status of the connection between WAF and ADS. A WAF can be configured to collaborate with up to four ADS devices.
Time of Stopping Traffic Diversion	<p>Specifies how to stop traffic diversion. It has the following values:</p> <ul style="list-style-type: none"> Automatically: WAF automatically determines whether to send notifications to ADS on stopping traffic diversion. Scheduled: WAF sends a notification to ADS on stopping traffic diversion after the specified timer expires. <p> Note</p>

Parameter		Description
		When ADS diverts traffic, WAF suspends TCP flood protection for the target IP address. After ADS's traffic diversion stops, WAF resumes TCP flood protection for this IP address.
Single-IP Traffic	SYN Flood Notification Threshold	<p>Threshold for SYN flood traffic. When the number of SYN packets reaches the threshold, WAF instructs ADS to divert the traffic.</p> <p> Note</p> <p>When TCP flood protection is enabled on WAF, this threshold must be greater than that specified in the TCP flood protection policy.</p>
	ACK Flood Notification Threshold	<p>Threshold for ACK flood traffic. When the number of ACK packets reaches the threshold, WAF instructs ADS to divert the traffic.</p> <p> Note</p> <p>When TCP flood protection is enabled on WAF, this threshold must be greater than that specified in the TCP flood protection policy.</p>
	Traffic Rate (pps) Notification Threshold	Threshold for traffic expressed in pps. When the traffic reaches the threshold, WAF instructs ADS to divert the traffic.
	Traffic Rate (bps) Notification Threshold	Threshold for traffic expressed in bps. When the traffic reaches the threshold, WAF instructs ADS to divert the traffic.
Overall Traffic	Statistic Dimension	Method of counting packets, which can be pps , bps , and pps and bps .
	Traffic Rate (pps) Notification Threshold	Threshold for traffic expressed in pps. When the total traffic of the network exceeds the threshold, WAF notifies ADS of the IP address with the largest traffic, asking it to divert traffic of this IP address until the total traffic is below the specified threshold.
	Traffic Rate (bps) Notification Threshold	Threshold for traffic expressed in bps. When the total traffic of the network exceeds the threshold, WAF notifies ADS of the IP address with the largest traffic, asking it to divert traffic of this IP address until the total traffic is below the specified threshold.
Advanced options (optional)	Query Interval	Specifies the interval for WAF to query from ADS the current traffic of the protected IP address after the traffic diversion succeeds.
	Retry Interval After Failed Notification	Specifies the interval for WAF to resend the diversion notification if no response is returned to the first notification
	Maximum Number of Queries	After the traffic diversion starts, WAF queries from ADS the current traffic of the protected IP address at intervals (specified with Query Interval). If the first query request fails, WAF resends the request regularly until the allowed maximum number of queries is reached. If there is still no response returned after the number of query attempts reaches the specified maximum, WAF cancels the diversion for the traffic of the protected IP address.
	Maximum Number of Notification	If the incoming traffic of an IP address exceeds the notification threshold, WAF sends a traffic diversion notification to ADS. Also, when the incoming traffic of the IP address falls below the diversion threshold after a successful traffic diversion, WAF sends a diversion cancellation notification to ADS. If no response is returned to a diversion notification or diversion cancellation notification, WAF keeps sending such a notification at intervals (specified with Query Interval) until the specified maximum number is reached. If there is still

Parameter		Description
		no diversion success response after the number of notifications sent by WAF reaches the specified maximum, WAF will delete notification record of this IP address from the notification list.

c. Click **OK** to save the settings.

Step 3 Verify the collaboration status.

Click **Test** on the page shown in [Figure 4-9](#), [Figure 4-10](#), or [Figure 4-11](#). If the system displays "Connected", the communication link between WAF and ADS is successfully established.

Step 4 (Optional) Specify IP addresses that allow traffic diversion.


Type IP addresses that allow traffic diversion in the text box below **Diversion-Allowed IPs** shown in [Figure 4-8](#), and then click **OK**.

If you leave this text box empty, traffic to IP addresses of all devices protected by WAF will be diverted by ADS.

Step 5 (Optional) Specify IP addresses that do not allow traffic diversion.

Type IP addresses that do not allow traffic diversion in the text box below **Diversion-Forbidden IPs** shown in [Figure 4-8](#), and then click **OK**.

After IP addresses are specified, even if traffic to these IP addresses exceeds the threshold, ADS does not divert such traffic, but WAF will log the related alert.

	<p>When configuring diversion-allowed or diversion-forbidden IP addresses, note the following:</p> <ul style="list-style-type: none"> • If an IP address is specified for both Diversion-Allowed IPs and Diversion-Forbidden IPs, this IP address does not allow for traffic diversion. • If an IP address is neither specified for Diversion-Allowed IPs nor Diversion-Forbidden IPs, this IP address does not allow for traffic diversion. • Individual IP addresses or IP ranges (such as 1.1.1.1–1.1.1.100) can be specified for Diversion-Allowed IPs and Diversion-Forbidden IPs. Multiple IP addresses and IP ranges are separated by carriage returns.
---	---

----End

Viewing the Status of IP Addresses Allowing Traffic Diversion

You can view IP addresses whose traffic is diverted and cleansed, as well as their current traffic on WAF and ADS. Their current traffic on ADS refers to traffic before being cleansed.

On the **ADS Collaboration Config** tab page shown in [Figure 4-8](#), click **Diverted IP Status List**. A dialog box appears, listing IP addresses whose traffic is diverted, their traffic information, and the status of collaboration with ADS, as shown in [Figure 4-12](#).

Figure 4-12 List of IP addresses allowing traffic diversion

Diverted IP Status List

ADS(0.0.0.0) Diverted IP Status List


No.	IP Address	Collaboration Status	Current WAF Traffic				Current ADS Traffic				Operation
			SYN(pps)	ACK(pps)	total pps	total bps	SYN(pps)	ACK(pps)	total pps	total bps	
<div><div></div><div>No diverted IP</div></div>											

Refresh

Close



Note

- Based on actual network situations, you can click  in the row of a diverted IP address to remove the IP address from the diverted IP addresses list. Then, ADS stops diverting traffic destined for the IP address, and WAF resumes TCP flood protection for the IP address.
- You can click **Refresh** to refresh the list and view the latest information about diverted IP addresses.

4.3 Website Protection

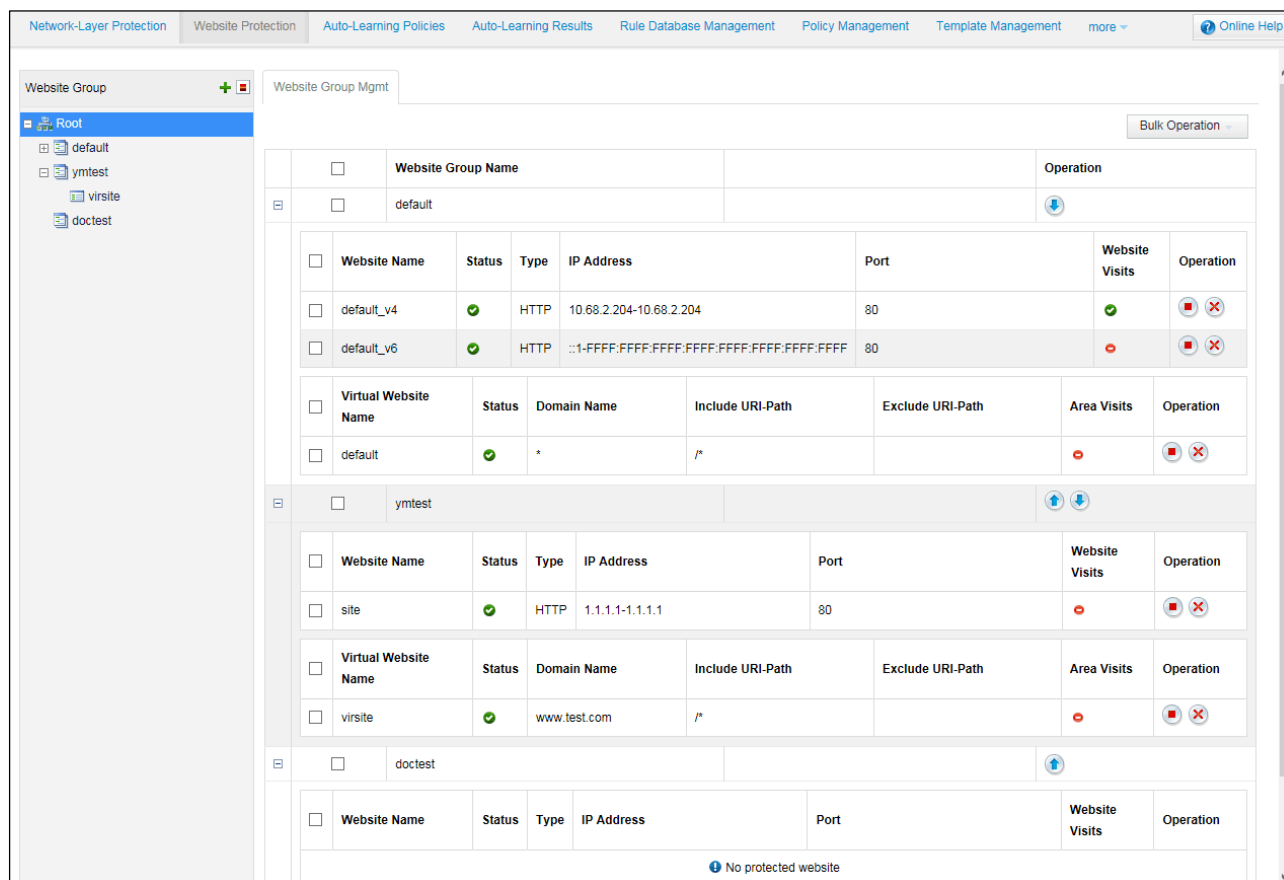
Websites are protection objects of WAF. A website may contain one or more IP addresses. Generally, multiple websites and virtual websites of the same type form a website group. WAF can apply policies and perform protection based on website groups.

WAF can upload information about protected assets (website groups, websites, and virtual websites) and policies (website group policies and virtual website policies) applied to such assets to NSFOCUS Cloud via the A interface.

Upon receiving a directive for periodical or instant upload from NSFOCUS Cloud, WAF will upload information about protected assets and protection policies applied to such assets to NSFOCUS Cloud.

Choose **Security Management > Website Protection**. The **Website Group Mgmt** page appears, as shown in [Figure 4-13](#).

Figure 4-13 Website Group Mgmt page



In the website group tree in the left pane:

- **Root** is the root directory of website groups.
- **default** is the default website group of the system.
- **ymtest** is a website group created by the administrator.
- **virsite** is a virtual website in the **ymtest** website group.

The following details how to manage website groups, websites, and virtual websites.

4.3.1 Managing Website Groups

On the **Website Group Mgmt** page, you can perform the following steps:

- [Creating a Website Group](#)
- [Editing a Website Group](#)
- [Enabling or Disabling Global Regional Access Statistics](#)
- [Altering Website Group Priorities](#)
- [Quickly Accepting Packets](#)
- [Deleting a Website Group](#)

4.3.1.1 Creating a Website Group

A website group can be created in either of the following methods:



- **Quick mode**
When you configure website group in quick mode, a set of security solutions are generated automatically to cover system-defined policies. After the website group is created, you need to add servers to the website group, so that the servers can be protected by the set of solutions.
- **Guide mode**
When you configure websites in guide mode, the system asks you to configure the information about websites to be protected and basic information of target web servers. A set of solutions are automatically generated based on the configuration information you enter, and take effect immediately after the configuration is complete.

The method of creating a website group differs in different deployment modes.

- On WAF in-path, out-of-path, or mirroring mode, a website group can be created in quick or guide mode.
- On WAF in reverse proxy mode, a website group can be created only in quick mode.

Creating a Website Group in Quick Mode

To create a website group in quick mode, perform the following steps:

- Step 1** On the **Website Protection** page shown in [Figure 4-13](#), click  in the upper-right corner of the website group tree. Alternatively, click  to the right of the root directory (this icon appears only when you point to the **Root** line).

The **Create Website Group** dialog box appears, as shown in [Figure 4-14](#).

On WAF in reverse proxy mode, a website group can only be created in quick mode, as shown in [Figure 4-14](#). In in-path, out-of-path, or mirroring mode, a website group can be created in either quick mode or guide mode and you need to select the quick mode, as shown in [Figure 4-15](#).

Figure 4-14 Creating a website group in quick mode (in reverse proxy mode)

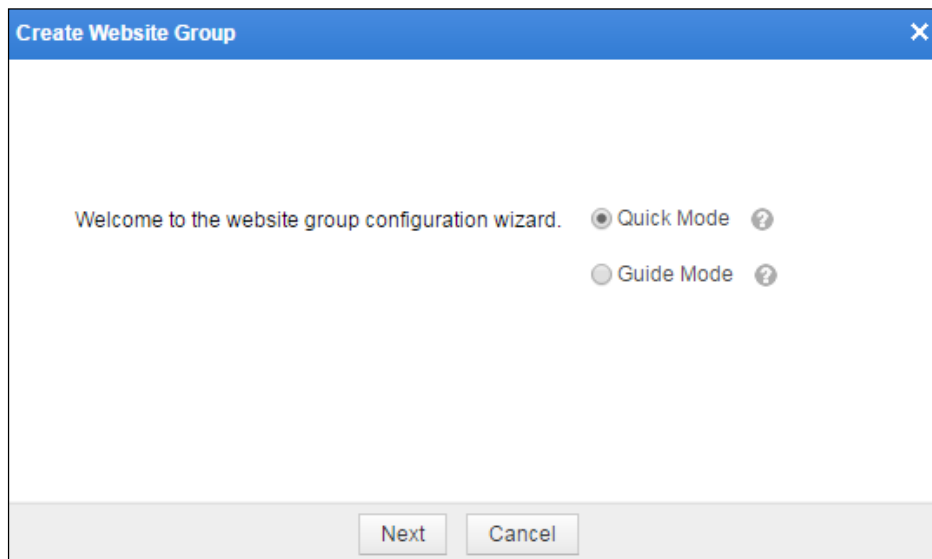
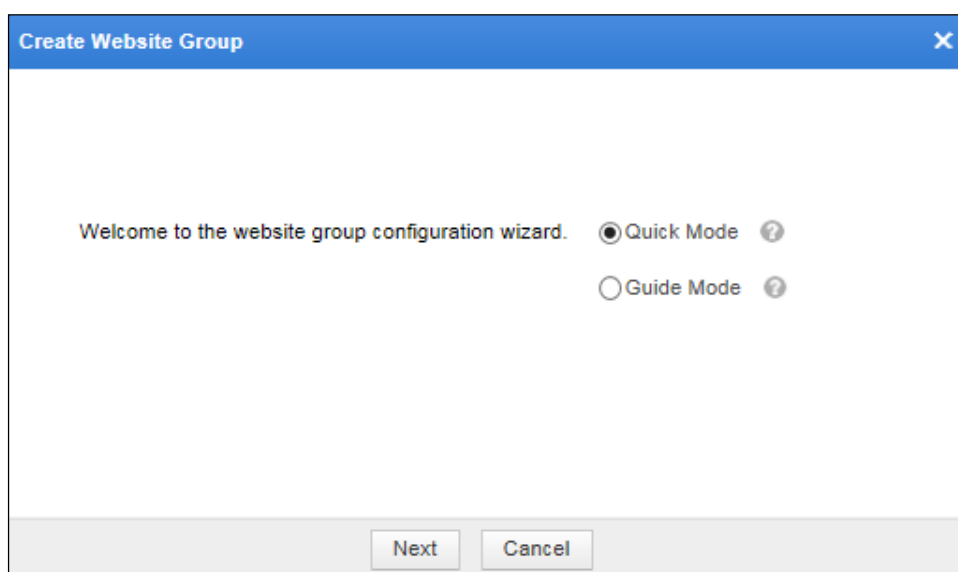


Figure 4-15 Creating a website group in quick mode (in in-path, out-of-path, or mirroring mode)



Step 2 Select **Quick Mode** and click **Next**.

The dialog box for specifying the website group name appears, as shown in [Figure 4-16](#).

Figure 4-16 Specifying the website group name in quick mode

Step 3 Enter a website group name and click **Complete**.

The new website group appears on the **Website Group Mgmt** page. At this time, this new website group contains no website, and can be used only after websites and policies are configured. For details on adding a website, see [To add more websites, click Add More](#).



----End

Creating a Website Group in Guide Mode

The guide mode is available only for in-path, out-of-path, and mirroring modes.

Here, WAF deployed in in-path mode is used as an example to describe how to create a website group.

To create a website group in guide mode, perform the following steps:

Step 1 On the **Website Protection** page shown in [Figure 4-13](#), click  in the upper-right corner of the website group tree. Alternatively, click  to the right of the root directory (this icon appears only when you point to the **Root** line).

The **Create Website Group** dialog box appears, as shown in [Figure 4-15](#).

Step 2 Select **Guide Mode** and click **Next**.

The dialog box shown in [Figure 4-17](#) appears.

Figure 4-17 Specifying the website group name in guide mode

Create Website Group > Guide Mode

Website Group Name *

Previous Next Cancel


Step 3 Enter a website group name and click **Next**.

The dialog box for creating websites appears, as shown in [Figure 4-18](#). The website group creation process can proceed only after at least one website is created.

Figure 4-18 Website list in guide mode

Create Website Group > Guide Mode > Website List

Website List Create

Name	Type	Address	Port	Certificate	Operation
 No Data					



Previous Next

Step 4 Click **Create**.



Figure 4-19 Adding a website in guide mode

Step 5 Set parameters to add a website.

Table 4-5 Parameters for adding a website

Parameter	Description
Server Name	Website name. The value can contain a maximum of 25 characters and excludes the smaller than sign (<), greater than sign (>), and double quotation mark.
Server Type	Protocol used to access the server. The value can be HTTP or HTTPS . If this parameter is set to HTTPS , Certificate File also needs to be specified.
Server IP Address	IP addresses of protected servers. You can specify an IP address range by entering a start IP address and end IP address, or specify a single IP address by entering only a start IP address. Also, you can click  to add multiple IP addresses or ranges. A maximum of 25 addresses or ranges are allowed here.  Note <ul style="list-style-type: none"> Multiple IP addresses can be typed only in in-path or out-of-path mode. Both IPv4 and IPv6 addresses and ranges are accepted here. If the same IP address or range is specified repeatedly here for one website, WAF stops matching against it once a hit is found.
Server Port	Ports for accessing protected servers. <ul style="list-style-type: none"> If Server Type is set to HTTP, you can specify a maximum of 128 ports, separated by commas. If Server Type is set to HTTPS, you can specify only one port.
Enable Web Access Log	Specifies whether WAF records access requests in web access logs. The

Parameter	Description
	value can be Yes or No .
Enable Website Access Statistics	Controls whether WAF records website access requests. The value can be Yes or No .
HTTP Decode Failure Alert	Controls whether to report an alert in the case of an HTTP decode failure. After this function is enabled, WAF decodes website access requests. If the request decoding fails, WAF generates an alert. If the alerting function is disabled, no alert will be generated in the case of a decoding failure.
Action upon HTTP Decode Failure	Specifies what WAF will do following a request decoding failure from this website: <ul style="list-style-type: none"> • Block for all: The action for all inspection items is Block. In this case, WAF will directly tear down the current connection upon a failed inspection item decoding attempt. • Pass for all: The action for all inspection items is Pass. In this case, WAF will forward all requests on this connection without matching them against any protection policy after a failed inspection item decoding attempt. • Custom: If the action for a certain inspection item is set to Block or Pass, WAF will handle matching requests as indicated by this inspection item.
Enable Gzip	Controls whether to enable Gzip compression. If one or more of cross-site forgery protection, sensitive information filtering, content filtering, and web shell protection policies are configured for filtering of responses from the server: <ul style="list-style-type: none"> • When Gzip is enabled, WAF filters responses from the server and returns Gzip responses to the client. • When Gzip is disabled, WAF filters responses from the server and returns the client responses in a format other than Gzip.
Gzip Compression Level	Specifies the Gzip compression level. It is optional. The value can be 1–9. A greater value indicates a higher compression ratio but a lower speed (1 indicates fastest compression and 9 indicates the highest compression ratio).
Content-type	Specifies the type of files for Gzip compression. By default, WAF supports Gzip compression for the following file types: text, application/x-javascript, application/json, and application/javascript. Also, you can type other file types.
Certificate File	Specifies the certificate file if Server Type is set to HTTPS . You can select an existing certificate file or upload a new one by selecting Select an Existing Certificate or Upload Certificate . <ul style="list-style-type: none"> • Select an Existing Certificate: Provides the built-in or uploaded certificate for selection. The administrator can manage the existing certificate. For details, see section 4.12 Uploaded File Management. • Upload Certificate: Uploads the certificate to WAF.
SSL Offload	Controls whether to enable SSL offload. This parameter is an advanced option available only when Server Type is set to HTTPS .

Parameter	Description
Client	<ul style="list-style-type: none"> • SSL Version: specifies one or more SSL versions to be supported by WAF. • Cipher Algorithm: specifies one or more built-in SSL encryption algorithms that WAF will use for communication with the client.  <p>Note</p> <p>This parameter is an advanced option available only when Server Type is set to HTTPS.</p>
Server	<ul style="list-style-type: none"> • SSL Version: specifies one or more SSL versions to be supported by WAF. • Cipher Algorithm: specifies one or more built-in SSL encryption algorithms that WAF will use for communication with the server.  <p>Note</p> <p>This parameter is an advanced option available only when Server Type is set to HTTPS.</p>

Step 6 Click **OK**.

The page of website list appears.

Step 7 Click **Next**.

The dialog box for selecting options of service system information is displayed, as shown in [Figure 4-20](#).

Figure 4-20 Selecting options of service system information

Create Website Group > Guide Mode > Service System Information

Operating System

- ☒ All Types
- ☒ Linux/Unix
- ☒ Windows
- ☒ Others

Web Server

- ☒ All Types
- ☒ IIS
- ☒ Nginx
- ☒ Others
- ☒ Apache
- ☒ Weblogic
- ☒ Tomcat
- ☒ Lighttpd

Database

- ☒ All Types
- ☒ SQL Server
- ☒ Postgres
- ☒ Others
- ☒ Access
- ☒ Oracle
- ☒ Mysql
- ☒ DB2

Programming Language

- ☒ All Types
- ☒ PHP
- ☒ Java
- ☒ Others
- ☒ ASP
- ☒ Python
- ☒ .Net
- ☒ Perl

[Previous](#) [Complete](#)

Step 8 Configure parameters for the service system.

You can set the operating systems, web server types, database types, and programming languages of protected servers.

By default, all options of service system information are selected. You can select options as desired.

Step 9 Click **Complete** to save the settings.

The website group list appears on the **Website Group Mgmt** page.

----End

4.3.1.2 Editing a Website Group

You can edit the following information about a website group:

- [Website Group Basic Information](#)
- [Website](#)
- [Virtual Website](#)

Clicking a website group in the website group tree displays the **Website Group Mgmt** page, as shown in [Figure 4-21](#).

Figure 4-21 Website Group Mgmt page

Website Group Mgmt [Low-and-Slow Attack Protection](#) [HTTP Flood Protection](#) [Web Security Protection](#) [Exception Control](#) [Risk Level Control](#)

Website Group Basic Information

Website Group Name	Operating System	Database	Web Server	Language	Operation
default	Linux/Unix Windows Others	SQL Server Access Mysql Postgres Oracle DB2 Others	IIS Apache Tomcat Nginx Weblogic Lighttpd Others	PHP ASP .Net Java Python Perl Others	

Website

[Add Website](#)

Website Name	Type	IP Address	Port	Certificate	Web Access Logs	Website Visits	Status	Operation
default_v4	HTTP	10.67.1.202- 10.67.1.202	80					

Virtual Website

[Add Virtual Website](#)

Virtual Website Name	Domain Name	Include URI-Path	Exclude URI-Path	Area Visits	Status	Operation
default	*	/*				

Website Group Basic Information

- Click in the **Operation** column of the **Website Group Basic Information** area to edit the website group name and system information.
- Click in the **Operation** column of the **Website Group Basic Information** area to open the **Auto-Learning Policies** page. For details about how to configure auto-learning policies, see section [4.4 Auto-Learning Policies](#).

Website





- Click **Add Website** to add a website to the website group.
- Click in the **Operation** column of the **Website** area to edit websites.

Virtual Website

- Click **Add Virtual Website** to add a virtual website to the website group.
- Click in the **Operation** column of the **Virtual Website** area to edit virtual websites.



4.3.1.3 Enabling or Disabling Global Regional Access Statistics

The global regional access statistics collection function refers to collecting statistics on visits to the WAF-protected IP addresses of all websites. Virtual websites are included.

- Clicking  in the upper-right corner of the website group tree enables this function. After the function is enabled, the icon turns to .
- Clicking  in the upper-right corner of the website group tree disables this function. After the function is disabled, the icon turns to .

4.3.1.4 Altering Website Group Priorities

Choose **Security Management > Website Protection**. The **Website Group Mgmt** page appears, as shown in [Figure 4-13](#).

In the website group list, click  or  to move a website group up or down. An upper website group has a higher priority than a lower website group.

4.3.1.5 Quickly Accepting Packets

The quick packet accepting function applies to web security protection (built-in HTTP validation excluded) and secure data transmission of website groups and virtual websites.

After the quick packet accepting function is enabled for a website group or virtual website, WAF accepts all packets, regardless of the action specified in policies.

You can enable or disable the quick packet accepting function as follows:

- In the website group tree, click the root directory of website groups, **Root**. On the **Website Group Mgmt** page that appears, select one or more website groups, click **Bulk Operation**, and select **Enable Accept** to enable the quick packet accepting function or select **Disable Accept** to disable this function.
- In the website group tree, click a website group and click **Enable** for **Accept** to enable the quick packet accepting function or click **Close** to disable this function.

4.3.1.6 Deleting a Website Group

You can delete a website group in either of the following methods:


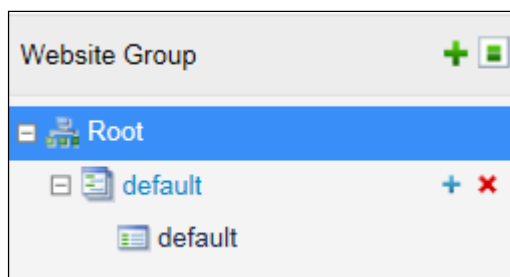

- When you point to a website group in the website group tree, the deleting icon  appears, as shown in [Figure 4-22](#). To delete the website group, click the icon and then click **OK** in the displayed dialog box.

Figure 4-22 Deleting a website group from the website group tree



- Click **Root** in the website group tree. On the **Website Group Mgmt** page, select a website, click  in the **Operation** column, and then click **OK** in the confirmation dialog box.

----End

4.3.2 Managing Websites

On the **Website Group Mgmt** page, you can perform the following steps:

- [Adding Websites](#)
- [Enabling/Disabling Websites](#)
- [Bulk Operation](#)
- [Configuring Website Security Policies](#)
- [Deleting Websites](#)

4.3.2.1 Adding Websites

Different modes of WAF require different parameters for adding a website.

Adding a Website (in in-path or out-of-path mode)

Step 1 Click a website group in the website group tree.

The **Website Group Mgmt** page appears.

Step 2 Click **Add Website** in the upper-right corner of the **Website** area.

Figure 4-23 Adding a website (in in-path or out-of-path mode)

Step 3 Set parameters.

[Table 4-5](#) describes parameters for adding a website.

Step 4 Click **Complete** to save the settings.

To add more websites, click **Add More**.

----End

Adding a Website (in mirroring mode)

Step 1 Click a website group in the website group tree.


The **Website Group Mgmt** page appears.

Step 2 Click **Add Website** at the lower-right corner of the **Website** area.

Figure 4-24 Adding a website (in mirroring mode)

Step 3 Set parameters.

Table 4-6 Parameters for adding a website in mirroring mode

Parameter	Description
Server Name	Website name. The value is at most 25-character long and excludes the smaller than sign (<), greater than sign (>), and double quotation mark.
Service Type	Protocol used to access the server. The value can be HTTP or HTTPS .  Note The option of HTTPS is available only when the HTTPS site switch is turned on by the system maintainer under System Management > Site Control .
Server IP Address	IP addresses of protected servers. You can specify an IP address segment by entering the start and end IP addresses, or specify a single IP address by entering only the start IP address.
Server Port	Specifies ports for accessing protected servers. A maximum of 128 ports can be specified. Multiple ports should be

Parameter	Description
	separated by commas.
Enable Web Access Log	Controls whether to generate web access logs for all access requests passing through WAF. The value can be Yes or No .
Enable Website Access Statistics	Controls whether to collect statistics on website visits. The value can be Yes or No .
HTTP Decode Failure Alert	Controls whether to enable HTTP decode failure alert. After this function is enabled, WAF decodes requests from the specified website. In the case of a decode failure, WAF generates an alert. If this function is disabled, WAF will not generate an alert.
Certificate File	<p>Specifies the certificate file if Server Type is set to HTTPS. You can select an existing certificate file or upload a new one:</p> <ul style="list-style-type: none"> Select an Existing Certificate (available only when there are certificates on WAF): selects an SSL certificate already uploaded for the server's use. You can manage all certificates currently available on WAF. For details, see section 4.12 Uploaded File Management. Upload Certificate: uploads a certificate to WAF.

Step 4 Click **Complete** to save the settings.

To add more websites, click **Add More**.

----End

Adding a Website (in reverse proxy mode)

Step 1 Click a website group in website group tree.

The **Website Group Mgmt** page appears.



Step 2 Click **Add Website** in the upper-right corner of the **Website** area.


Figure 4-25 Adding a website (in reverse proxy mode)

Step 3 Set parameters.

Table 4-7 Parameters for adding a website in reverse proxy mode

Parameter	Description
Server Name	Website name. The value is at most 25-character long and excludes the smaller than sign (<), greater than sign (>), and double quotation mark.
Server Type	Specifies the protocol used to access the server. The value can be HTTP or HTTPS . If this parameter is set to HTTPS , Certificate File also needs to be specified.
Proxy Interface	Interface for proxy access. Only a WAN interface can be selected. For the configuration of working interfaces, see Editing Work Group in section 7.1.1 Work Group Management .
Proxy IP	IP address of the proxy interface. After you select an interface, its existing IP addresses will automatically appear; if it does not have any existing IP address, you can directly configure an IP address for it. For details, see 7.1.1 Work Group Management . Both IPv4 and IPv6 addresses are supported. An interface can have a maximum of 253 IP addresses.
Proxy Port	Communication port of the proxy. For an HTTP or HTTPS server, you can enter only one port.
Enable Web Access Log	Specifies whether WAF records access requests in web access logs. The value can be Yes or No .

Parameter	Description
Enable Website Access Statistics	Controls whether to enable website access statistics. The value can be Yes or No .
HTTP Decode Failure Alert	Controls whether to enable HTTP decode failure alert. After this function is enabled, WAF decodes requests from the specified website. In the case of a decode failure, WAF generates an alert. If this function is disabled, WAF will not generate an alert.
Enable Gzip	Controls whether to enable Gzip compression. If one or more of cross-site forgery protection, sensitive information filtering, content filtering, and web shell protection policies are configured for filtering of responses from the server: <ul style="list-style-type: none"> When Gzip is enabled, WAF filters responses from the server and returns Gzip responses to the client. When Gzip is disabled, WAF filters responses from the server and returns the client responses in a format other than Gzip.
Gzip Compression Level	Specifies the Gzip compression level. It is optional. The value can be 1–9. A greater value indicates a higher compression ratio but a lower speed (1 indicates fastest compression and 9 indicates the highest compression ratio).
Content-type	Specifies the type of files for Gzip compression. By default, WAF supports Gzip compression for the following file types: text, application/x-javascript, application/json, and application/javascript. Also, you can type other file types.
Certificate File	Specifies the certificate file if Server Type is set to HTTPS . You can select an existing certificate file or upload a new one: <ul style="list-style-type: none"> Select an Existing Certificate: specifies a built-in certificate or a certificate already uploaded to WAF. You can manage all certificates currently available on WAF. For details, see section 4.12 Uploaded File Management. Upload Certificate: uploads a certificate to WAF.
SSL Offload	Controls whether to enable SSL offload.  Note This parameter is an advanced option available only when Server Type is set to HTTPS .
Client	<ul style="list-style-type: none"> SSL Version: specifies one or more SSL versions to be supported by WAF. Cipher Algorithm: specifies one or more built-in SSL encryption algorithms that WAF will use for communication with the client.  Note This parameter is an advanced option available only when Server Type is set to HTTPS .
Server	<ul style="list-style-type: none"> SSL Version: specifies one or more SSL versions to be supported by WAF.

Parameter	Description
	<ul style="list-style-type: none"> • Cipher Algorithm: specifies one or more built-in SSL encryption algorithms that WAF will use for communication with the server.  <p>Note</p> <p>This parameter is an advanced option available only when Server Type is set to HTTPS.</p>

Step 4 Click **Complete** to save the settings.





To add more websites, click **Continue Creating**.

----End

4.3.2.2 Enabling/Disabling Websites

By default, a website is enabled after being created.

To enable or disable a website, click **root** or a specific website group in the website group tree. Then perform the following steps on the displayed **Website Group Mgmt** page.

- Click  in the row of a disabled website. After it is enabled, its status turns to .
- Click  in the row of an enabled website. After it is disabled, its status turns to .

4.3.2.3 Bulk Operations

You can perform bulk operations on multiple website groups and websites, including **Enable Regional Access Statistics**, **Disable Regional Access Statistics**, **Enable Website Access Statistics**, **Disable Website Access Statistics**, **Delete**, **Enable**, and **Disable**.

Website access statistics refer to access data of all websites other than virtual websites.

Step 1 Click **Root** in the website group tree to open **Website Group Mgmt** page.

Step 2 Select multiple websites or website groups.

Step 3 Click **Bulk Operation**.

Step 4 Select the desired operation from the drop-down list.

----End

4.3.2.4 Configuring Website Security Policies

Website security policies include:

- [Low-and-Slow Attack Protection Policy](#)
- [HTTP Flood Protection Policy](#)
- [Secure Data Transfer Policy](#)
- [Web Security Protection Policy](#)
- [Exception Control Policy](#)
- [Session Tracking Policy](#)
- [Risk Level Control Policy](#)

- [Web Decoding](#)
- [False Positive Analysis](#)
- [False Positive Analysis Result](#)

Low-and-Slow Attack Protection Policy

This policy protects against low-and-slow attacks that behave in opposite ways to common distributed denial-of-service (DDoS) attacks.

A common DDoS attack is an attempt to make a server fail to respond to legitimate requests until it becomes down. A low-and-slow attack is an act, based on established connections to the target server, of sending packets to the server at a quite low rate to cause the resources on the server not to be released in time. If more than one client keeps establishing such a connection, the number of available TCP connections on the server will be used up in a short time and the server will reject new requests, causing denial-of-service attacks.

Low-and-slow attacks are classified into slow headers attacks, slow body attacks, and slow read attacks.

Currently, WAF's low-and-slow attack protection policy can effectively protect website groups against slow headers attacks and slow-body attacks. The two types of attacks are described as follows:

- **Slow headers**
According to the HTTP protocol, an HTTP packet with a trailing `\r\n\r\n` (0d0a0d0a) from the client indicates that the entire packet header is sent. After receiving this packet, the server starts processing. If such a packet is never sent, the server keeps waiting. Based on this, slow headers attacks are launched as a kind of DDoS attacks.
An attacker sets **Connection** to **Keep-Alive** in an HTTP header and sends the header data (such as `a:b\r\n`) in the key-value format every several minutes, holding the TCP connections to the server open. The server waits until the entire HTTP header is received. If the attacker acts this way by using multiple threads or zombies, all TCP connections on the server are occupied in a short time, causing the server to reject new requests.
- **Slow body**
Slow body attacks are also called slow POST attacks. For an HTTP request submitted via the POST method, the Content-Length field (POST data length) can be tampered with in the HTTP header. After accepting the specified length, the server waits for the POST data from the client. Sending the body of the HTTP POST request at a slow rate of one byte per 10s to 100s achieves the purpose of consuming resources on the server. Establishing more such connections will use up all resources on the server, causing the server to be down.

To configure the low-and-slow attack protection policy, perform the following steps:

- Step 1** Click a website group in website group tree. Click the **Low-and-Slow Attack Protection** tab in the right pane.

Figure 4-26 Low-and-slow attack protection policy

The screenshot shows a configuration window for the 'Low-and-slow attack protection policy'. At the top, there are several tabs: 'Website Group Mgmt', 'Low-and-Slow Attack Protection' (which is selected), 'HTTP Flood Protection', 'Secure Data Transfer', 'Web Security Protection', 'Exception Control', 'Session Trace', and 'Risk Level Control'. Below the tabs, the 'Protection Control' section contains the following settings:

- Low-and-Slow Attack protection:** A toggle switch currently set to 'Disabled', with an 'Enable' button next to it.
- Source IP Blocking:** A dropdown menu currently set to 'Unblock'.
- Inspection Cycle:** A text input field containing '5', with a range '(1-60s)' indicated to the right.
- Minimum Bytes:** A text input field containing '128', with a range '(26-1536 bytes)' indicated to the right.

An 'OK' button is located at the bottom center of the configuration area.

Step 2 Enable or disable the low-and-slow attack protection function.

By default, this policy is disabled. You can click **Enable** or **Close** to enable or disable this policy.

Step 3 Configure parameters of this policy.

Table 4-8 Parameters of the low-and-slow attack protection policy

Parameter	Description
Source IP Blocking	Controls whether to block the detected source IP addresses of low-and-slow attacks. <ul style="list-style-type: none"> Unblock: WAF does not block the source IP address. Permanently block: WAF permanently blocks the source IP address. Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Inspection Cycle	Specifies the cycle of collecting statistics on low-and-slow attacks. The value range is 1–60 in seconds, with 5 as the default.
Minimum Bytes	Specifies the minimum number of bytes a packet must contain in order not to be considered as one used for low-and-slow attacks. The value range is 26–1536, with 128 as the default.

Step 4 Click **OK** to save the settings.

----End

HTTP Flood Protection Policy

On the detection of an attack against a protected server, WAF includes authentication information in packets sent to clients. Clients whose response packets contain the same authentication information are authenticated successfully.

Click a website group in the website group tree. Click the **HTTP Flood Protection** tab in the right pane. The **HTTP Flood Protection** page appears, as shown in [Figure 4-27](#).

Figure 4-27 HTTP Flood Protection page

The screenshot displays the NSFOCUS WAF configuration interface for HTTP Flood Protection. The top navigation bar includes links for Website Group Mgmt, Low-and-Slow Attack Protection, HTTP Flood Protection, Secure Data Transfer, Web Security Protection, Exception Control, Session Trace, Risk Level Control, Web Decoding, False Positive Analysis, and False Positive Analysis Result. The left sidebar shows a tree view with 'Root' and 'default' under 'Website Group'. The main content area is titled 'Protection Control' and shows 'HTTP Flood Protection Status' as 'Enabled' with a 'Close' button. Below this is the 'Global Configuration' section with four input fields: 'Attack Duration' (300, range 300-7200 secs), 'Trust Time' (1800, range 300-86400 secs), 'Verification Code Auto-Update Cycle' (5, range 5-1440 mins), and 'Maximum Trust Times' (7200, range 0-7200 times). An 'OK' button is at the bottom of this section. The 'HTTP Flood Protection Policy' section is below, showing a table with columns: Name, Status, Destination IP, Destination Port, Algorithm, GET Threshold(pps), POST Threshold(pps), and Operation. The table is currently empty, displaying 'No data' and an information icon. A 'Create' button is at the bottom right of the policy section.

HTTP flood protection includes three parts: global configurations, HTTP flood protection policies, and custom protection policies.

Enabling/Disabling HTTP Flood Protection

By default, **HTTP Flood Protection Status** is **Enabled**. To disable it, click **Close** in the Protection Control area shown in [Figure 4-27](#).

Setting Global Parameters

Step 1 Set parameters in the **Global Configuration** area shown in [Figure 4-27](#).

Table 4-9 Parameters for global configuration

Parameter	Description
Attack Duration	Specifies the attack duration after which HTTP flood protection is triggered. The default value is 300 , in seconds.
Trust Time	Specifies the period during which IP addresses of authenticated clients stay in the trust list. The default value is 1800 , in seconds.
Verification Code Auto-Update Cycle	Specifies the interval at which WAF updates the verification code sent to clients for authentication. The default value is 5 , in minutes.
Maximum Trust Times	Specifies the maximum number of times that a client in the trust list is allowed to send more requests than the given threshold within the period specified by Trust Time . The default value is 7200 .

Step 2 Click **OK** to save the settings.

----End

Creating HTTP Flood Protection Policies

Step 1 Click **Create** in the **HTTP Flood Protection Policy** area shown in [Figure 4-27](#).

Figure 4-28 Creating an HTTP flood protection policy

Create HTTP Flood Protection Policy	
Name	<input type="text"/>
Website Selection	aaa ▼
Destination IP & Port	<input type="text"/> 999 ▼ IP address range of the current website: 1.1.1.1
Algorithm	HTTP Cookie ▼
ThresholdGet	1000
ThresholdPost	500
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Step 2 In the dialog box, set parameters.

Table 4-10 Parameters for creating an HTTP flood protection policy

Parameter	Description
Name	Specifies the new policy's name.
Website Selection	Specifies the website to which the new policy applies.
Destination IP & Port	Specifies the IP address and port of the proxy server. Both IPv4 and IPv6 addresses are supported.
Algorithm	<p>Specifies the authentication algorithm used in the new policy. The value can be one of the following:</p> <ul style="list-style-type: none"> HTTP Cookie: indicates that WAF uses HTTP Cookie as authentication information. If a client returns a packet containing the cookie value, the client is authenticated. URL Cookie: indicates that NSFOCUS WAF uses a redirect URL with a Cookie as authentication information. If a client returns a packet containing the cookie value, the client is authenticated. ascii-image: indicates an image-based authentication algorithm. An image containing authentication information (a string of characters) is sent to a client. If the client responds with the contained authentication information, it is authenticated. bmp-image: indicates a bmp-based authentication algorithm. A bmp image containing authentication information is sent to a client. If the client responds with the contained authentication information, it is authenticated.
ThresholdGet	Specifies the maximum number of GET requests received by WAF per second. If this threshold is exceeded, WAF considers that a flood attack occurs.

Parameter	Description
ThresholdPost	Specifies the maximum number of POST requests received by WAF per second. If this threshold is exceeded, WAF considers that a flood attack occurs.

Step 3 Click **OK** to save the settings.

----End

Creating a Custom Protection Policy

Step 1 Click **Create** in the **Customizing Protection Policy** area shown in [Figure 4-27](#).

Figure 4-29 Creating a custom protection policy

Create Customizing Protection Policy

Name:

Website Selection:

Destination IP & Port:
IP address range of the current website: 1.1.1.1

Domain Name:
Examples of valid domain names: www.httpflood.com, 5231:1::110:110:1:2, and 110.110.1.2. Port numbers are not allowed in a domain name. An invalid domain name would result in an ineffective policy.

Path:
An URI starting or ending with the wildcard "*" is supported. A URI without "*" means strict matching.

Algorithm:

Step 2 In the dialog box, set parameters.

Table 4-11 Parameters for configuring a custom protection policy

Parameter	Description
Name	Specifies the new policy's name.
Website Selection	Specifies the website to which the new policy applies.
Destination IP & Port	Specifies the IP address and port of the proxy server. Both IPv4 and IPv6 addresses are supported.

Parameter	Description
Domain Name	Domain name of the protected website
Where to Obtain	Specifies the URLs that are not protected by the new policy.
Algorithm	<p>Specifies the authentication algorithm used in the new policy. The value can be one of the following:</p> <ul style="list-style-type: none"> • HTTP Cookie: indicates that WAF uses HTTP Cookie as authentication information. If a client returns a packet containing the cookie value, the client is authenticated. • URL Cookie: indicates that NSFOCUS WAF uses a redirect URL with a Cookie as authentication information. If a client returns a packet containing the cookie value, the client is authenticated. • ascii-image: indicates an image-based authentication algorithm. An image containing authentication information (a string of characters) is sent to a client. If the client responds with the contained authentication information, it is authenticated. • bmp-image: indicates a bmp-based authentication algorithm. A bmp image containing authentication information is sent to a client. If the client responds with the contained authentication information, it is authenticated.

Step 3 Click **OK** to save the settings.



----End

Secure Data Transfer Policy

By configuring secure data transfer policies, WAF can forcibly change common HTTP requests to HTTPS requests, thereby enhancing the security of data transmission.

Click a website group in the website group tree and then click the **Secure Data Transfer** tab. The **Secure Data Transfer** page appears, as shown in [Figure 4-30](#).

Figure 4-30 Secure Data Transfer page

Website Group Mgmt	Low-and-Slow Attack Protection	HTTP Flood Protection	Secure Data Transfer	Web Security Protection	Exception Control	Session Trace	Risk Level Control	Web Decoding	False Positive Analysis	False Positive Analysis Result	
											<div>Create</div>
Policy Name	Domain Name	Alert or Not	Included URL	Excluded URL	Method	Action	Source IP Blocking	Status	Operation		
<div><div></div><div>No data</div></div>											

Creating a Secure Data Transfer Policy

Step 1 Click **Create**.

Figure 4-31 Creating a secure data transfer policy

Create Policy

Policy Name *

Domain Name *

Alert or Not ☒ Yes ☐ No

Included URL +

Excluded URL +

Method

<input type="checkbox"/> All	<input checked="" type="checkbox"/> GET	<input checked="" type="checkbox"/> POST	<input checked="" type="checkbox"/> HEAD	<input type="checkbox"/> PUT
	<input type="checkbox"/> DELETE	<input type="checkbox"/> MKCOL	<input type="checkbox"/> COPY	<input type="checkbox"/> MOVE
	<input type="checkbox"/> OPTIONS	<input type="checkbox"/> PROPFIND	<input type="checkbox"/> PROPPATCH	<input type="checkbox"/> LOCK
	<input type="checkbox"/> UNLOCK	<input type="checkbox"/> TRACE	<input type="checkbox"/> SEARCH	<input type="checkbox"/> CONNECT

Action ?


Source IP Blocking

OK Cancel

Step 2 In the dialog box, set parameters.

Table 4-12 Parameters for configuring secure data transfer policies

Parameter	Description
Policy Name	Specifies the name of the policy.
Domain Name	Specifies the domain name to be protected.
Alert or Not	Specifies whether to generate alert logs.
Included URL	Specifies one or more URLs for managing secure data transfer.
Excluded URL	Specifies one or more URLs excluded from the management of secure data transfer.
Method	Specifies one or more methods for managing secure data transfer when a client accesses the server.
Action	<p>Specifies WAF's action on requests matching this policy, which can be one of the following:</p> <ul style="list-style-type: none"> Block: WAF ends the current detection and disconnects the current TCP connection. In this case, the Source IP Block parameter is available. Accept: WAF completes the current detection and continues with other security detections on matching packets. Redirection: WAF constructs a 302 redirect page to respond to the client and disconnect the current TCP connection.






Parameter	Description
Source IP Blocking	<p>Specifies whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block.</p> <ul style="list-style-type: none"> Unblock: WAF does not block the source IP address. Permanently block: WAF permanently blocks the source IP address. Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	<p>Specifies the redirection URL. This parameter is required if Action is set to Redirection.</p> <ul style="list-style-type: none"> Custom: Enter the redirection URL address in the text box of Redirection Path. The redirection path should be a complete URL of up to 2048 characters such as http://www.example.com. Current URL HTTPS: You need to enter the current HTTPS port in the text box of HTTPS Port. The default value is 443. Previous Page: Indicates that it is redirected to the HTTPS version of the previous page accessed by the client. <p> Note</p> <ul style="list-style-type: none"> Make sure that the redirected URL exists and the corresponding website has been configured on WAF; otherwise, the URL would be found unavailable or the protection effect could not be achieved. In compliance with the RFC specification, you are advised not to select Redirection for Action unless you select GET and/or HEAD for HTTP Method.

Step 3 Click **OK** to save the settings.

----End

Other Operations for Secure Data Transfer

On the **Secure Data Transfer** page shown in [Figure 4-30](#), you can perform the following steps:

- Editing a policy
Click  in the **Operation** column to edit parameters.
- Enabling/disabling a policy
By default, the secure data transfer policy is enabled after being created.
Click  or  in the **Operation** column to enable or disable a policy.
- Deleting a policy
Click  in the **Operation** column and click **OK** in the displayed dialog box.
- Returning to the **Website Group Mgmt** page
Click  in the **Operation** column to return to the **Website Group Mgmt** page.

Web Security Protection Policy

On the **Web Security Protection** page, you can load existing general policies or create policies to website groups. A policy can be loaded to multiple website groups. For the configuration of general policies, see section [4.7 Policy Management](#).

Click a website group in website group tree. Click the **Web Security Protection** tab in the right pane. The **Web Security Protection** page appears, as shown in [Figure 4-32](#).

Figure 4-32 Web Security Policy page

Website Group Mgmt		Low-and-Slow Attack Protection		HTTP Flood Protection		Secure Data Transfer		Web Security Protection		Exception Control		Session Trace		Risk Level Control	
Policy Template															
Fast Config		<input type="button" value="Select Website Template"/>		Use templates to configure the following policies.											
Protocol Validation															
HTTP Validation		<input type="text" value="default_medium"/>													
Basic Protection															
HTTP Access Control		<input type="text" value="default_medium"/>													
Web Server/Plug-in Protection		<input type="text" value="default_medium"/>													
Crawler Protection		<input type="text" value="Select a policy."/>													
Common Web Protection		<input type="text" value="default_medium"/>													
Illegal Upload Restriction		<input type="text" value="default_medium"/>													
Illegal Download Restriction		<input type="text" value="default_medium"/>													
Information Disclosure Protection		<input type="text" value="default_medium"/>													
Advanced Protection															
Leech Protection		<input type="text" value="default_medium"/>													
CSRF Protection		<input type="text" value="Select a policy."/>													
Scanning Protection		<input type="text" value="default_medium"/>													
Cookie Security		<input type="text" value="default_medium"/>													
Content Filtering		<input type="text" value="Select a policy."/>													
Sensitive Information Filtering		<input type="text" value="Select a policy."/>													
Brute Force Protection		<input type="text" value="Select a policy."/>													
XML Attack Protection		<input type="text" value="Select a policy."/>													
Smart Engine Inspection		<input type="text" value="Select a policy."/>													
IP Reputation		<input type="text" value="Select a policy."/>													
Precise Protection															
Whitelist		<input type="text" value="Select a policy."/>													
Smart Patch		<input type="text" value="Smart Patch Configuration"/>													
Others															
Custom Policy		<input type="text" value="Select a policy."/>													
		<input type="button" value="OK"/>		<input type="button" value="Export as Website Template"/>											



Note

- The policy is hit as long as the host name (including the port number) in the HTTP request matches the host defined in the policy.
- Only one cookie security policy can be hit for a host name. WAF uniformly signs and encrypts cookies matching this cookie security policy.
- If multiple cookie security policies are configured, WAF matches traffic against the policies in a top-down manner. You can adjust the policy order as required.

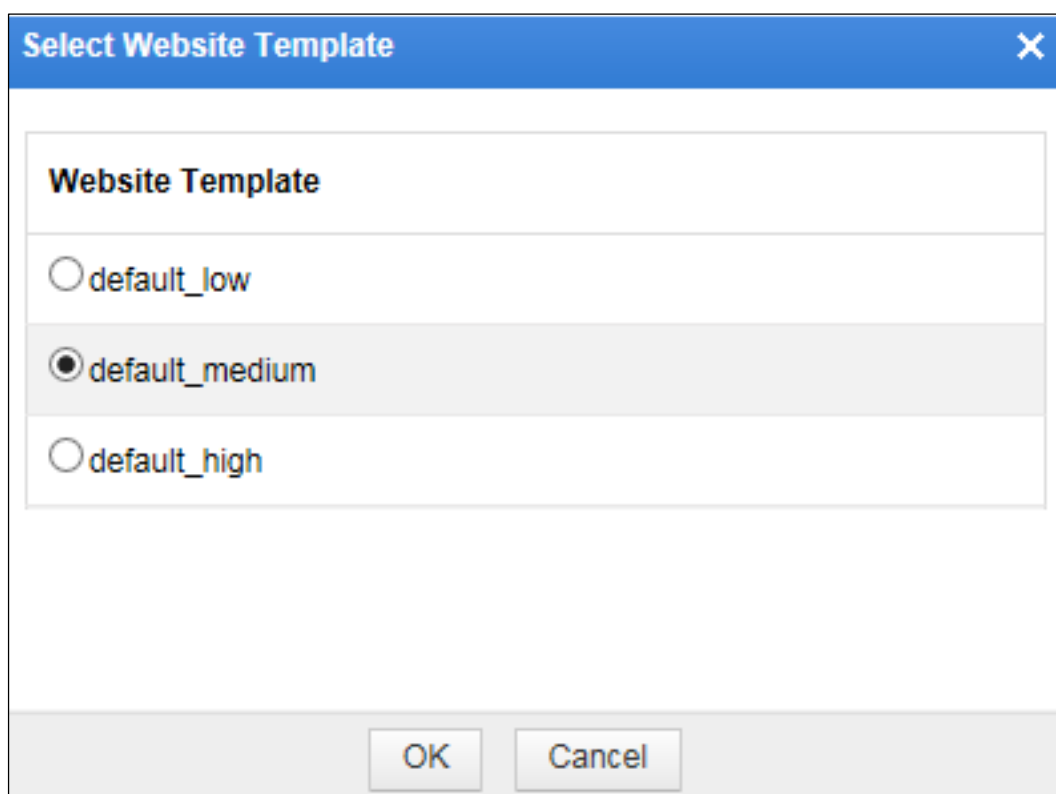
Quickly Configuring Web Security Protection Policies

If policy templates are configured, you can directly select a website template when configuring a web security protection policy. For details about website templates, see section [4.8.1 Website Template](#).

To quickly configure a web security protection policy, perform the following steps:

- Step 1** Click **Select Website Template** in the **Policy Template** area shown in [Figure 4-32](#).

Figure 4-33 Select Website Template dialog box



- Step 2** Select a website template, for example **default_medium**.

- Step 3** Click **OK**.

In this way, **default_medium** is selected for all protection policies by default, as shown in [Figure 4-34](#).

Figure 4-34 Web Security Protection page

Website Group Mgmt		Low-and-Slow Attack Protection		HTTP Flood Protection		Secure Data Transfer		Web Security Protection		Exception Control		Session Trace		Risk Level Control	
Policy Template															
Fast Config		<input type="button" value="Select Website Template"/>		Use templates to configure the following policies.											
Protocol Validation															
HTTP Validation		<input type="text" value="default_medium"/>													
Basic Protection															
HTTP Access Control		<input type="text" value="default_medium"/>													
Web Server/Plug-in Protection		<input type="text" value="default_medium"/>													
Crawler Protection		<input type="text" value="Select a policy."/>													
Common Web Protection		<input type="text" value="default_medium"/>													
Illegal Upload Restriction		<input type="text" value="default_medium"/>													
Illegal Download Restriction		<input type="text" value="default_medium"/>													
Information Disclosure Protection		<input type="text" value="default_medium"/>													
Advanced Protection															
Leech Protection		<input type="text" value="default_medium"/>													
CSRF Protection		<input type="text" value="Select a policy."/>													
Scanning Protection		<input type="text" value="default_medium"/>													
Cookie Security		<input type="text" value="default_medium"/>													
Content Filtering		<input type="text" value="Select a policy."/>													
Sensitive Information Filtering		<input type="text" value="Select a policy."/>													
Brute Force Protection		<input type="text" value="Select a policy."/>													
XML Attack Protection		<input type="text" value="Select a policy."/>													
Smart Engine Inspection		<input type="text" value="Select a policy."/>													
IP Reputation		<input type="text" value="Select a policy."/>													
Precise Protection															
Whitelist		<input type="text" value="Select a policy."/>													
Smart Patch		<input type="text" value="Smart Patch Configuration"/>													
Others															
Custom Policy		<input type="text" value="Select a policy."/>													
		<input type="button" value="OK"/> <input type="button" value="Export as Website Template"/>													

Step 4 Click **OK** to save the settings.

If the setting fails to be saved, a message appears, saying "Failed to save and apply the Web Security Policies, please retry later." You are advised to reactivate this policy a moment later.

----End

Loading Existing Policies

Step 1 Click the drop-down arrow in the **Protocol Validation** area shown in [Figure 4-32](#).

A list of HTTP validation types appears, as shown in [Figure 4-35](#).

Figure 4-35 HTTP validation types

Protection Type	Policy Type
HTTP Validation	default_low (selected)
HTTP Access Control	default_low
Web Server/Plug-in Protection	default_low
Crawler Protection	default_low
Common Web Protection	default_low
Illegal Upload Restriction	default_low
Illegal Download Restriction	default_low
Information Disclosure Protection	default_low

Step 2 Select an HTTP validation type.

Step 3 Click **OK** to save the settings.

If the setting fails to be saved, a message appears, saying "Failed to save and apply the Web Security Policies, please retry later." You are advised to reactivate this policy a moment later.

----End

Canceling Selected Policies

To cancel a selected policy, perform the following steps:

Step 1 On the **Web Security Protection** page shown in [Figure 4-32](#), click the drop-down arrow of a policy.

A list of existing policy types appears.

Step 2 Click **Cancel Selected Policy**.

Step 3 Click **OK** to save the settings.

----End

Creating a Policy

Step 1 On the **Web Security Protection** page shown in [Figure 4-32](#), click the drop-down arrow of a policy.

A list of existing policy types appears.

Step 2 Click **Create Policy**.

A dialog box for creating a policy appears.

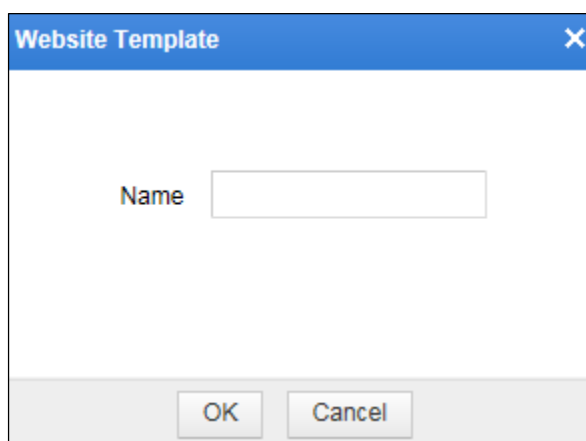
For how to create a policy, see section [4.7 Policy Management](#).

----End

Exporting as Website Templates

- Step 1** Click **Export as Website Template** at the bottom of the **Web Security Protection** page shown in [Figure 4-32](#). Click **OK** in the confirmation dialog box.
- Step 2** Enter the website template name in **Website Template** dialog box, as shown in [Figure 4-36](#).

Figure 4-36 Website Template dialog box



- Step 3** Click **OK**.

The prompt of "Export Succeeded" indicates that the current policy configuration is successfully exported as a website template.

You can view and manage the exported website template under **Security Management > Template Management**. For details about website templates, see section [4.8.1 Website Template](#).

----End

Configuring Smart Patches

- Step 1** Click **Smart Patch Configuration** in the **Precise Protection** area shown in [Figure 4-32](#).

The **Smart Patch Configuration** dialog box appears, as shown in [Figure 4-37](#).



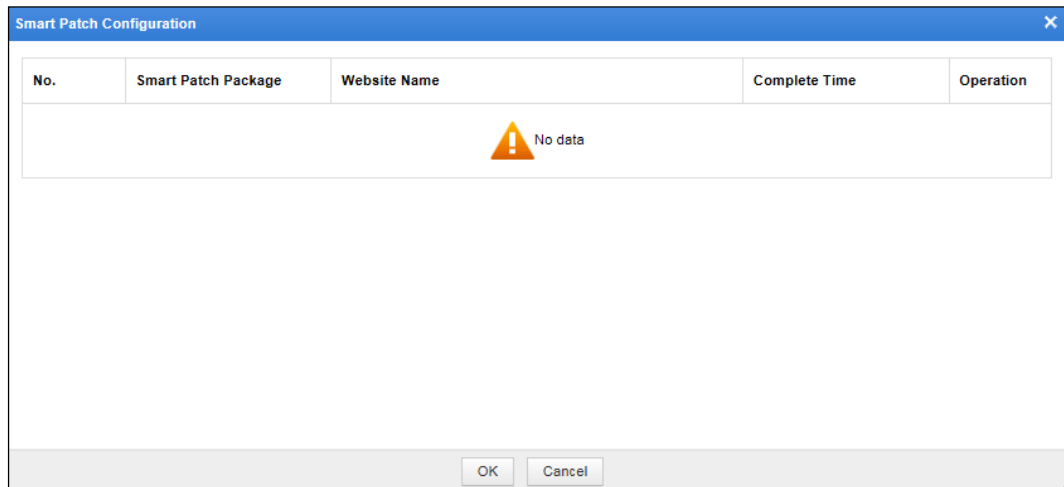
All smart patches and their application status are displayed.  indicates that the patch is not applied and the patch is deselected at the same time.  indicates that the patch is applied and the patch is selected at the same time.

Figure 4-37 Smart Patch Configuration dialog box



Step 2 Select the check boxes in the rows of desired smart patches and select **Block** or **Accept** to block or accept requests for the specified URLs.

To apply all smart patches, select the **All** check box at the upper-right corner of the list. After that, you can click **Block All** or **Accept All** to block or accept all requests to these URLs.

Step 3 Click **OK**.

A dialog box appears, saying "It might take a long period of time and the WAF might encounter a high CPU load while applying a great many patches. Continue?"

Step 4 Click **OK** in the confirmation dialog box to apply the selected smart patches. For details about smart patches, see section [4.9 Smart Patching](#).



Note

If applying smart patches fails, the system displays the message "Failed to apply the smart patch(es), please retry later." In this case, you are advised to reapply these smart patches a moment later.

----End

Exception Control Policy

Click a website in website group tree. Click the **Exception Control** tab in the right pane. The **Exception Control** page appears, as shown in [Figure 4-38](#).

Figure 4-38 Exception Control page



Loading Exception Policies

To load exception policies, perform the following steps:

- Step 1** On the **Exception Control** tab page shown in [Figure 4-38](#), click the drop-down arrow to the right of **Exception Policy**, and select desired policies from the drop-down list. See [Figure 4-39](#).

Figure 4-39 Selecting exception policies

Configured Exception Policies	
Name	Description
ccc	

- Step 2** Click **OK** to complete the configuration.

----End

Canceling Selected Exception Policies

To cancel selected exception policies, perform the following steps:

- Step 1** On the **Exception Control** page shown in [Figure 4-38](#), click the drop-down arrow to the right of **Exception Policy**, and click **Cancel Selected Exception Policy**, as shown in [Figure 4-39](#).

- Step 2** Click **OK** to complete the settings.

----End

Creating Exception Policies

Click **Create Policy** shown in [Figure 4-38](#). The **Create Exception Policy** dialog box appears. For how to create exception policies, see section [4.7 Policy Management](#).

Session Tracking Policy

The session tracking policy tracks users' access requests to the web application server and all their web operations as well as records detailed access logs, thereby providing data support for attack event analysis, attack scenario reproduction, and web operation correlation. Also, it can be used for user behavior research to determine whether potential attack motives lie behind user operations.

When a user accesses a WAF-protected web server via a browser on the client, this policy tracks the following types of sessions for website groups:

- After a connection to the browser is successfully set up, WAF delivers the browser a cookie that contains WAF_Client_Id (WCI). Within the WCI timeout period (one day by

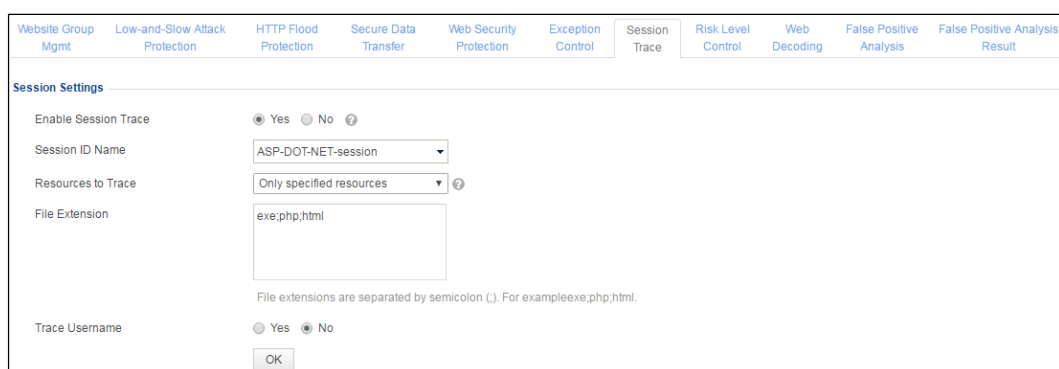
default and can be set on the background), this cookie is included in each request of this user to follow up all user operations. In addition, WAF assigns browser-specific WCIs to requests from the same client in order to follow up user access via various browsers on this client.

- If the web server returns the user a cookie that contains the session ID of the server, WAF will also send the user a one-off cookie that contains WAF_Session_Id (WSI). Then, all requests of this user contain both cookies that are used to keep track of all operations of this user.

To configure a session tracking policy, perform the following steps:

- Step 1** Click a website group in the left website group tree and click the **Session Trace** tab in the right pane.

Figure 4-40 Session tracking page




- Step 2** Enable or disable the session tracking function.

By default, the session tracking function is disabled. You can select **Yes** for **Enable Session Trace** to enable this function.

- Step 3** Configure session tracking parameters.

Table 4-13 Parameters for configuring the session tracking policy

Parameter	Description
Enable Session Trace	Controls whether to enable or the session tracking function.
Session ID Name	<p>Session ID name of the source IP address whose sessions are to be tracked. Sessions are tracked only when the source IP address accesses pages using selected session ID names.</p> <p>WAF supports the following session ID names:</p> <ul style="list-style-type: none"> • ASP-DOT-NET-session • ASPSESSIONID-session • ColdFusion-session • J2EE-JSESSIONID-Cookie-session • J2EE-JSESSIONID-URL-session • J2EE-session • JWS-ID-session

Parameter	Description
	<ul style="list-style-type: none"> PHP-BB-MYSQL-session PHPSESSID-session PHPSESSIONID-session SAP-session  <p>Note</p> <p>You can customize session ID names by modifying the configuration file on the background.</p>
Resources to Trace	<p>Specifies which resources can be tracked.</p> <ul style="list-style-type: none"> All: indicates that WAF tracks access to all resources. Only specified resources: indicates that WAF only tracks access to specified resources. Specified resources excluded: indicates that WAF only tracks access to other resources than the specified.
File Extension	<p>Specifies file name extensions that are tracked. Multiple file name extensions must be separated by semicolons.</p> <p>This parameter is mandatory when Resources to Trace is set to Only specified resources or Specified resources excluded.</p>
Trace Username	<p>Specifies whether the user name is specified.</p> <p>If you select Yes, all logs triggered for individual sessions can be associated with the user name during the user's access period.</p>
Login Parameters	<p>Login parameters of the traced user name.</p> <ul style="list-style-type: none"> URL: Each URL must be in the format of host + uri-path + query-string. An HTTP URL must be typed without http://, while an HTTPS URL must be typed with https://. A maximum of 10 URLs are allowed. Username: A maximum of 10 user names are supported, with each controlled within 256 bytes.

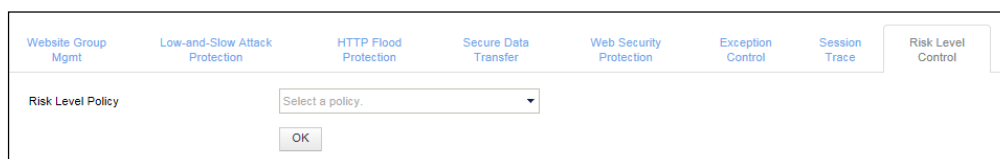
Step 4 Click **OK** to save the settings.

----End

Risk Level Control Policy

Click a website in the website group tree. Click the **Risk Level Control** tab in the right pane. The **Risk Level Control** page appears, as shown in [Figure 4-41](#).

Figure 4-41 Risk level control policy

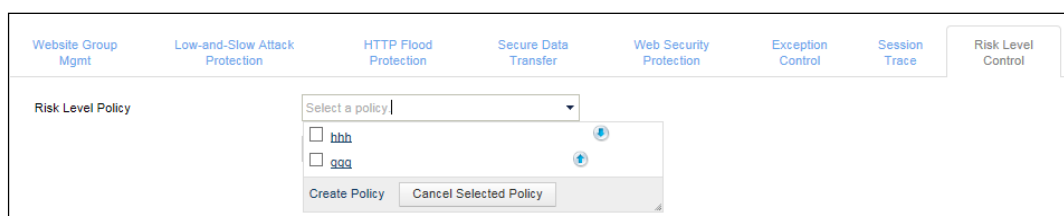


Loading Risk Level Control Policies

To load risk level control policies, perform the following steps:

- Step 1** On the page shown in [Figure 4-41](#), click the drop-down arrow to the right of **Risk Level Policy**. All current risk level controls policies are displayed, as shown in [Figure 4-42](#).

Figure 4-42 Selecting risk level control policies



- Step 2** Select one or more policies and click **OK** to save the setting.

----End

Cancelling Selected Risk Level Control Policies

To cancel selected risk level control policies, perform the following steps:

- Step 1** On the page shown in [Figure 4-41](#), click the drop-down arrow to the right of **Risk Level Policy**. Click **Cancel Selected Policy** to deselect risk level control policies that you have selected.

- Step 2** Click **OK** to save the settings.

----End

Creating a Risk Level Control Policy

On the page shown in [Figure 4-42](#), click **Create Policy** to create a risk level control policy. For details, see section [4.7.5.3 Risk Level Policy](#).

Web Decoding


After configuring web decoding, you enable WAF to decode Base64-encoded parameter values in requested URLs and then identify and protect against URL encoded attacks.

Click a website group in the website group tree. Click the **Web Decoding** tab in the right pane. The **Web Decoding** page appears, as shown in [Figure 4-43](#).

Figure 4-43 Web Decoding page

Website Group Mgmt	Low-and-Slow Attack Protection	HTTP Flood Protection	Secure Data Transfer	Web Security Protection	Exception Control	Session Trace	Risk Level Control	Web Decoding	False Positive Analysis	False Positive Analysis Result
--------------------	--------------------------------	-----------------------	----------------------	-------------------------	-------------------	---------------	--------------------	--------------	-------------------------	--------------------------------

Create

Policy Name	Domain Name	URL_Path	URL_Path Matching Mode	Decoding Mode	Operation
 No data					

Creating a Web Decoding Policy

Step 1 Click **Create** in the upper right corner.

Figure 4-44 Creating a web decoding policy

Create Policy
✕

Policy Name

*

Decoding Mode ?

base64 ▾

+

Protocol

☒ HTTP ☐ HTTPS

Host Name

*

?

URI_Path

Equal to ▾

?

*

?

Parameter

Equal to ▾

?

*



+



OK

Cancel

Step 2 In the **Create Policy** dialog box, configure parameters.

Table 4-14 Parameters for configuring a web decoding policy

Parameter	Description
Policy Name	Name of the new web decoding policy.
Decoding Mode	<p>Specifies the decoding scheme and level.</p> <p>You can select a decoding scheme from the drop-down list. You can also click  or  to add or delete decoding levels.</p> <p>The decoding sequence is from left to right and then from top to bottom.</p>



Parameter	Description
Protocol	Protocol to be supported, which can be HTTP or HTTPS .
Host Name	Name of the host to be decoded.
URI_Path	URI of the host to be decoded. This can be specified by using Equal to , Include , or RegEx Matching .
Parameter	Key parameter to be decoded. This can be specified by using Equal to , Include , or RegEx Matching . You can click  or  to add or delete parameters.

Step 3 Click **OK** to save the settings.

----End

Other Operations

You can also perform the following operations on the page shown in [Figure 4-43](#):

- Editing a policy
Click  in the **Operation** column of a policy and then edit parameters in the dialog box that appears.
- Deleting a policy
Click  in the **Operation** column of a policy and then click **OK** in the confirmation dialog box.

False Positive Analysis

This module allows you to identify false positives resulting from policies that conflict with the business through log analysis.

False positive analysis is website group-specific and can be performed manually or automatically.

You can enable automatic adjustment for both manual analysis and automatic analysis to call settings configured in the **Auto Adjustment** area.

Click a website group in the website group tree. Click the **False Positive Analysis** tab in the right pane. The **False Positive Analysis** page appears, as shown in [Figure 4-45](#).


Figure 4-45 False Positive Analysis page

Manual Analysis

Figure 4-46 shows the area for manual analysis configuration.

Figure 4-46 Manual Analysis area

Step 1 Configure analysis conditions.

- Specify a time frame so that logs generated in that period will be analyzed. You can directly select a period from default options of 10 minutes, 30 minutes, 1 hour, 6 hours, 12 hours, 1 day, 3 days, and 7 days. Alternatively, you can click  to specify a desired period.

- Choose whether to enable auto adjustment. If yes, settings configured in the **Auto Adjustment** area will be directly called for use.

Step 2 Click **Analyze**. After a dialog box appears prompting successful execution, click **OK** to issue the false positive analysis task.

After the analysis task is complete, you can click the **False Positive Analysis Result** tab to view the analysis result.

----End

Automatic Analysis

Figure 4-47 shows the area for automatic analysis configuration.

Figure 4-47 Auto Analysis area

Step 1 Configure analysis conditions.

- Enable automatic analysis.
- Choose whether to enable auto adjustment. If yes, settings configured in the **Auto Adjustment** area will be directly called for use.
- Configure the automatic analysis frequency.
- Specify the time when the automatic analysis will start.

Step 2 Click **Save**.

Then WAF will analyze logs automatically as configured.

After the analysis task is complete, you can click the **False Positive Analysis Result** tab to view the analysis result.

----End

Automatic Adjustment

Automatic adjustment enables WAF to preferentially modify policies or add the policies to the exception list.

After automatic adjustment is enabled during manual or automatic analysis configuration, policies resulting in false positives will be modified or added to the exception list, depending on the setting.

Figure 4-48 shows the area for automatic adjustment configuration.

Figure 4-48 Auto Adjustment area

Step 1 Specify the basis and threshold for determining whether false positives exist.

- WAF can determine whether an alert is a false positive on either of the following bases:
 - **Occurrences of Alerted IP:** indicates the number of different source IP addresses in security logs
 - **Alert Percentage:** indicates the proportion of different source IP addresses in security logs to the total number of source IP addresses in access logs.
- Threshold:
 - Threshold for the number of alerted IP addresses: When the number of source IP addresses found in alert logs reaches or exceeds this threshold, WAF will modify related policies or add them to the exception list, depending on the setting.
 - Threshold for the percentage of alerted IP addresses: When the percentage of source IP addresses found in alert logs reaches or exceeds this threshold, WAF will modify related policies or add them to the exception list, depending on the setting.

Step 2 Determine how to make adjustments.

Select policies and then select either of the following automatic adjustment schemes for them:

- Preferentially modify policies: When a policy triggers false positives and at the same time meets policy modification conditions, this policy will be modified preferentially.
Such modification should be based on the alert cause provided in the analysis result and made by modifying parameters or canceling a certain check item.
To modify a policy, you need to first duplicate it, then modify its parameters or cancel a certain check item, and finally commit the changes.
If all check items are canceled, the adjustment method will be "Cancel policy".
- Preferentially add policies to the exception list: When a policy triggers false positives and at the same time meets exception addition conditions, this policy will be added to the exception list preferentially.

This involves the following situations:

- Adding a policy to the exception list, including all its rules
- Adding a certain rule under a policy to the exception list

While you can adopt only the former method for algorithm-based policies, both methods work for rule-based policies (for details, see the description about manually [adding an exceptional item](#)).



- If a policy is found to trigger false positives and this policy should be modified preferentially according to the setting, but the alert cause or rule analysis result does not support such modification, WAF will check whether it meets the conditions for addition to the exception list. If yes, WAF will perform the corresponding operation.
- Conversely, if a policy is found to trigger false positives and this policy should be added to the exception list preferentially according to the setting, but the URL analysis result does not support such addition, WAF will check whether it meets modification conditions. If yes, WAF will perform the corresponding operation.

Step 3 Click **Save**.





----End

False Positive Analysis Result

After a manual or automatic false positive analysis, WAF will generate the analysis result. All such results are displayed on the **False Positive Analysis Result** tab page.

Click a website group in the website group tree and then click the **False Positive Analysis Result** tab in the right pane. The **False Positive Analysis Result** page appears, as shown in [Figure 4-49](#).

Figure 4-49 False Positive Analysis Result page

Website Group Mgmt	Low-and-Slow Attack Protection	HTTP Flood Protection	Secure Data Transfer	Web Security Protection	Exception Control	Session Trace	Risk Level Control	Web Decoding	False Positive Analysis	False Positive Analysis Result
Analysis Result										
Page Number: 1 / 1		Record Number: 2		First Page	Previous Page	Next Page	Last Page			
ID	Analysis Duration	Scheduled Task	Auto Adjust	Auto Adjustment Basis	Status	Analysis Result	Operation			
2	7day(s) ?	No	Yes Details	Occurrences of Alerted I P>=1	Adjusted	Yes	 			
1	6hr(s) ?	No	Yes Details	Occurrences of Alerted I P>=1	Adjusted	Yes	 			

Viewing the Analysis Result






In the **Operation** column of a result, click . Then details of the result are displayed, as shown in [Figure 4-50](#).

Figure 4-50 Analysis result details

Website Group Mgmt	Low-and-Slow Attack Protection	HTTP Flood Protection	Secure Data Transfer	Web Security Protection	Exception Control	Session Trace	Risk Level Control	Web Decoding	False Positive Analysis	False Positive Analysis Result
Analysis Result ID:2										
	Type	Name								
	Website	default_v4								
	Website Group	default								
	Virtual Website	default								

Clicking  or  on the left of **Type** displays or collapses the policy names and alert cause/URL/rule analysis details of the website, website group, and virtual website.

Clicking  or  on the left of **Website**, **Website Group**, or **Virtual Website** displays or collapses the policy names and alert cause/URL/rule analysis details of the website, website group, or virtual website.

- Clicking the blue link text following a policy name, you can view details about this policy.
- Clicking  following the alert cause analysis or rule analysis, you can manually modify the policy.
- Clicking  following URL analysis or rule analysis, you can add an exceptional item.
 - When URL analysis is involved, clicking this icon allows you to add the policy to the exception list.
 - When rule analysis is involved, clicking this icon allows you to add a rule under this policy to the exception list.


Viewing Adjustment Details

On the page shown in [Figure 4-49](#), click **Details** in the **Auto Adjust** column. Then details about the adjustment are displayed in a new dialog box, as shown in [Figure 4-51](#).


Figure 4-51 Adjustment details

Adjustment Log						
Protection Object	Adjustment Method	Policy Type	Original Policy	New Policy/Exception Policy	Adjusted Content	Adjustment Status
Virtual Website : default	Modify policy	Illegal Download Restriction	default_medium	Add_by_false_alarm_analyse_2883585	Disable file name extension check: pr m	Adjusted
Virtual Website : default	Modify policy	Illegal Upload Restriction	default_medium	Add_by_false_alarm_analyse_2621441	Disable file name extension check: p y	Adjusted
Virtual Website : default	Modify policy	Common Web Protection	default_medium	Add_by_false_alarm_analyse_2359298	Cancel rule: 18612240	Adjusted
Virtual Website : default	Modify policy	HTTP Validation	default_medium	Add_by_false_alarm_analyse_262145	Set Maximum HTTP Header Value Length: No Set Forbid Illegal Domain Name: No Set Max Number of GET Request Parameters: No Set Forbid Abnormal Anchor Point: No Set Maximum HTTP Header Name Length: No Set Maximum User-Agent Length: No Set Maximum Content-Length: No Set Max Number of POST Request Parameters: No Set Maximum Number of Range Sections: No	Adjusted
Website Group : default	Exception Policy	HTTP Access Control	ACL	Add_by_false_alarm_analyse_4718593	Exception URLs: 10.67.10.220:82/py/	Adjusted
Website : default_v4	Modify policy	Internal Protocol Validation	Internal Protocol Validation		Too long HTTP request header: No Unknown HTTP 0.9 request method: No Redundant request header: No Incompliant HTTP version field: No Incompliant request method field: No Too long URI packet: No	Adjusted

Deleting an Analysis Result

Click  in the **Operation** column of an analysis result and then click **OK** in the confirmation dialog box to delete this record.

4.3.2.5 Deleting Websites

Click **Root** or a specific website group in the website group tree. On the **Website Group Mgmt** page that appears, click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete a website.

4.3.3 Managing Virtual Websites

You can do as follows on virtual websites:

- [Creating a Virtual Website](#)
- [Enabling/Disabling a Virtual Website](#)
- [Configuring a Virtual Website](#)
- [Deleting a Virtual Website](#)
- [Bulk Operations](#)

4.3.3.1 Creating a Virtual Website


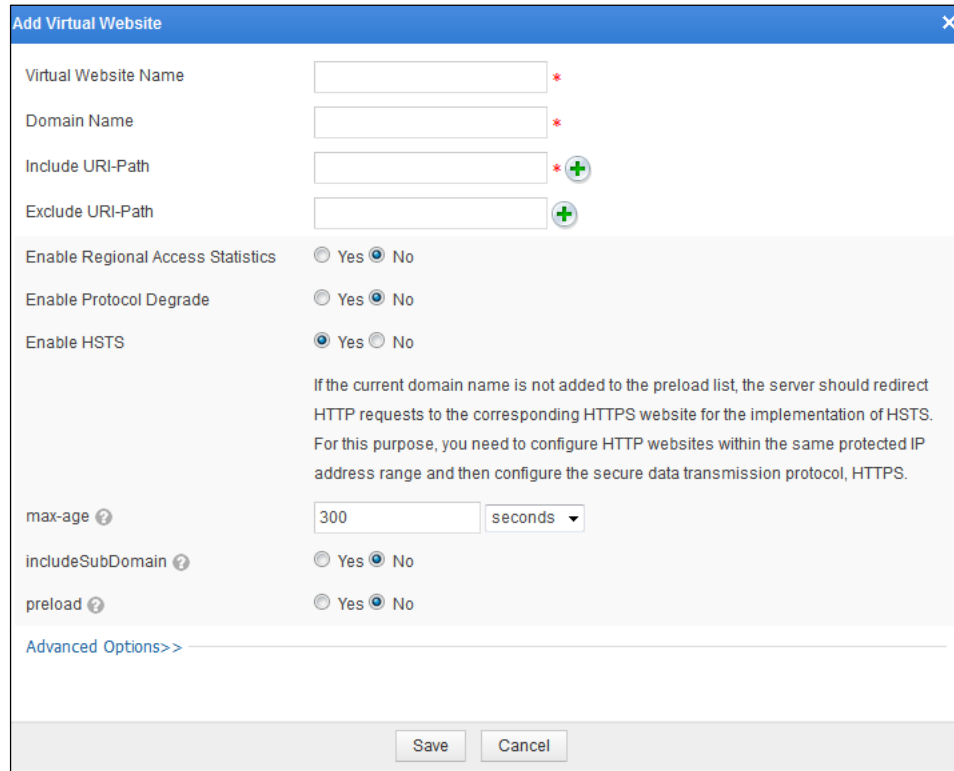
Step 1 In the website group tree, point to a desired website group, and click .

Figure 4-52 Creating a virtual website (in in-path, out-of-path, or mirroring mode)



Add Virtual Website

Virtual Website Name *

Domain Name *

Include URI-Path * +

Exclude URI-Path +

Enable Regional Access Statistics ☐ Yes ☒ No

Enable Protocol Degrade ☐ Yes ☒ No

Enable HSTS ☒ Yes ☐ No

If the current domain name is not added to the preload list, the server should redirect HTTP requests to the corresponding HTTPS website for the implementation of HSTS. For this purpose, you need to configure HTTP websites within the same protected IP address range and then configure the secure data transmission protocol, HTTPS.

max-age seconds

includeSubDomain ☐ Yes ☒ No

preload ☐ Yes ☒ No

[Advanced Options>>](#)

Save Cancel

Figure 4-53 Creating a virtual website (in reverse proxy mode)

Add Virtual Website

Virtual Website Name *

Proxied Server

Domain Name *

Include URI-Path +

Exclude URI-Path +

Enable Regional Access Statistics ☐ Yes ☒ No

Enable Protocol Degrade ☐ Yes ☒ No

Enable HSTS ☒ Yes ☐ No

If the current domain name is not added to the preload list, the server should redirect HTTP requests to the corresponding HTTPS website for the implementation of HSTS. For this purpose, you need to configure HTTP websites within the same protected IP address range and then configure the secure data transmission protocol, HTTPS.

max-age 300 seconds

includeSubDomain ☐ Yes ☒ No

preload ☐ Yes ☒ No

Server IP Address

Enable Load Balancing ☐ Yes ☒ No



IP Address Port

[Advanced Options>>](#)

Step 2 In the dialog box, set parameters.

Table 4-15 Parameters for creating a virtual website

Parameter	Description
Virtual Website Name	Specifies the name of the virtual website.
Domain Name	Specifies the domain name of the virtual website.
Include URI-Path	Specifies the URL address to be detected.
Exclude URI-Path	Specifies the URL address not to be detected.
Enable Regional Access Statistics	Controls whether to enable the regional access statistics.
Enable Protocol Downgrade	Controls whether to enable the protocol downgrade function for the virtual website. After this function is enabled, the long HTTP connection turns to the short HTTP connection.
Enable HSTS	Controls whether to enable HTTP Strict Transport Security (HSTS) for the virtual website.

Parameter	Description
	<p>After HSTS is enabled, you must set max-age to specify the amount of time an HSTS header can be cached. For the initial visit to this website, you need to type https: IP or domain name in the address bar of a browser. For the second visit, you only need to type the website's IP address or domain name by omitting https, as long as max-age specified for the first visit does not expire. This is because the browser, in this case, will automatically connect to the target website through HTTPS and max-age is reset automatically for the new HSTS header. If a subsequent visit is made beyond the time frame specified with max-age for the previous visit, the browser will not automatically connect to the website via HTTPS and you need to manually type the complete website URL with https included.</p> <p>If the current domain name is not added to the preload list, the server needs to provide the HTTP-to-HTTPS redirect function for the implementation of HSTS. For this purpose, you need to configure HTTP websites with the same IP address ranges and set Secure Data Transfer Policy.</p> <p> Note</p> <ul style="list-style-type: none"> • The HSTS function is unavailable in mirroring mode. • For WAF used in China, HSTS is disabled by default, indicating that WAF allows responses from the server to pass through, regardless of the setting of the corresponding HSTS response header. • For WAF used outside of China, HSTS is enabled by default, indicating that WAF handles responses as indicated in the corresponding HSTS response header.
max-age	<p>Specifies how long an HSTS head can be cached in a browser. It is available only after HSTS is enabled. If HSTS is enabled for the first time, you are advised to set a short time for this parameter.</p> <p> Note</p> <p>As each HTTPS response has an HSTS header, max-age is reset with each response. In other words, the caching time is the same for each HSTS header. Assume that max-age is set to 180 seconds and you type https: IP or domain name for your first visit to an HTTPS website and visit it again 120 seconds later. Upon your second visit, max-age is reset to 180 seconds.</p>
includeSubDomain	<p>Controls whether to make HSTS available to all child domain names of the current domain name.</p> <p>This parameter is available only when HSTS is enabled.</p> <p>Before enabling this function, make sure that all child domain names of the current domain name support HTTPS; otherwise, the access may fail.</p>
preload	<p>Controls whether to add the current domain to the preload list created by Google.</p> <p>This parameter is available only after HSTS is enabled.</p> <p>If this parameter is set to Yes, the current domain name will be added to the preload list. The current domain name can be added to the preload list only when the following conditions are met:</p> <ul style="list-style-type: none"> • max-age is set to a period no less than 18 weeks (126 days). • includeSubDomains must be set to Yes. • preload is enabled. As Google does not check the authenticity of applicants, use this function with caution.

Parameter	Description
Server	<p>Specifies the proxied server. This parameter is required only in reverse proxy mode.</p> <ul style="list-style-type: none"> If you select IP Address, you need to enter the IP address and port number of the proxied server, and choose whether to enable load balancing. Both IPv4 and IPv6 addresses are supported. If you select Actual Domain Name, you need to enter the actual domain name and port number of the proxied server and click Gain IP Address to obtain the IP address of the server. Both IPv4 and IPv6 addresses are supported.
Enable Load Balancing	<p>Controls whether to enable the load balancing function. This parameter is required only in reverse proxy mode.</p> <p>After Enable Load Balancing is set to Yes, you need to set IP Address and Port.</p>
Advanced Options	<p>If the website group contains websites with HTTPS servers, you can configure advanced options for the virtual website:</p> <ul style="list-style-type: none"> Certificate File: specifies a method to import the certificate file. Options include Select an Existing Certificate or Upload Certificate. Select an Existing Certificate: You need to select an existing certificate file from the drop-down list. SSL Version: specifies an SSL version supported by WAF. Cipher Algorithm: specifies a cipher algorithm.





Step 3 Click **Save** to save the settings.

----End

4.3.3.2 Enabling/Disabling a Virtual Website

By default, a virtual website is enabled after being created.

To enable or disable a virtual website, click **Root** or a specific website group in the website group tree. Then do as follows on the **Website Group Mgmt** page that appears:

- Click  in the **Operation** column to enable a virtual website. After it is enabled, its status turns to .
- Click  in the **Operation** column to disable a virtual website. After it is disabled, its status turns to .

4.3.3.3 Configuring a Virtual Website

In the website group tree, click a virtual website. The **Virtual Website** page appears.

Figure 4-54 Virtual Website page (in in-path, out-of-path, or mirroring mode)

The 'Edit Virtual Website' dialog box contains the following fields and options:

- Virtual Website Name:** test *
- Domain Name:** 1.1.1.1 *
- Include URI-Path:** * + (add icon)
- Exclude URI-Path:** + (add icon)
- Enable Regional Access Statistics:** ☐ Yes ☒ No
- Enable Protocol Degrade:** ☐ Yes ☒ No

Buttons: Save, Cancel

Figure 4-55 Virtual Website page (in reverse proxy mode)

The 'Virtual Website' page in reverse proxy mode shows the following configuration:

- Virtual Website Name:** test *
- Proxied Server:** (empty)
- Domain Name:** 1.1.1.1 *
- Include URI-Path:** * + (add icon)
- Exclude URI-Path:** + (add icon)
- Enable Regional Access Statistics:** ☐ Yes ☒ No
- Enable Protocol Degrade:** ☐ Yes ☒ No
- Server:** IP Address ▾
- Enable Load Balancing:** ☐ Yes ☒ No
- IP Address:** 1.1.1.100
- Port:** 80

Buttons: Save

Setting Virtual Website Parameters

Set parameters in the dialog boxes shown in [Figure 4-54](#) and [Figure 4-55](#). Then click **Save** to save the settings.

Configuring Virtual Website Policies

Step 1 Click **Policy Configuration** in [Figure 4-54](#) or [Figure 4-55](#).

Figure 4-56 Policy Configuration page

The screenshot shows the 'Policy Configuration' page. It includes sections for 'Policy Template', 'Protocol Validation', 'Basic Protection', 'Advanced Protection', and 'Others'. Each section contains a list of policies with checkboxes to 'Use corresponding policy of its website group' and a dropdown menu to select a specific policy. The 'XML Attack Protection' dropdown is currently set to 'Select a policy.'.

Step 2 Configure virtual website policies using one of the following methods:

- Quick configuration: Click **Select Virtual Website Template** to select a template.
- Referencing policies: Select a policy from the drop-down list for each type of policies.
- Enabling website policies: Select the **Use corresponding policy of its website group** check box. The policy of the website group to which the website belongs is automatically referenced.

Step 3 Click **OK** to save the settings.

----End

Creating Policies

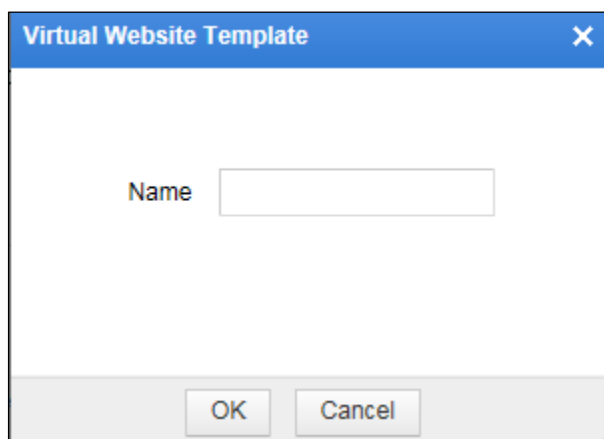
On the **Policy Configuration** page shown in [Figure 4-56](#), click the **Create Policy** link. The dialog box for creating a policy of this type appears. For how to create policies, see section [4.7 Policy Management](#).

Exporting as Virtual Website Templates

In [Figure 4-56](#), click **Export as Virtual Website Template**, enter the template name in the displayed **Virtual Website Template** dialog box, and click **OK**.




The prompt of "Export Succeeded" indicates that the current policy configuration is successfully exported as a virtual website template. You can view and manage the exported virtual website template under **Security Management > Template Management**. For details about virtual website templates, see section [4.8.2 Virtual Website Template](#).

Figure 4-57 Virtual Website Template dialog box



4.3.3.4 Deleting a Virtual Website

You can delete a virtual website using either of the following ways:

- In the website group tree, click  preceding a website group to list all its virtual websites. Point to a virtual website and click  and then click **OK** in the confirmation dialog box to delete this virtual website.
- Click **Root** or a specific website group in the website group tree. On the **Website Group Mgmt** page that appears, click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete a virtual website.

4.3.3.5 Bulk Operations

You can perform bulk operations on multiple website groups and virtual websites under a website group, including **Enable Regional Access Statistics**, **Disable Regional Access Statistics**, **Enable Website Access Statistics**, **Disable Website Access Statistics**, **Delete**, **Enable**, and **Disable**.

For virtual websites, the regional access statistics function refers to collecting access data of the IP address range of all virtual websites.

After the regional access statistics function is enabled, you can view regional access statistics by region under **Logs & Reports > Regional Access Statistical Report**.

Bulk operation of virtual websites is the same as that of real websites. For details, see section [4.3.2.3 Bulk Operations](#).

4.4 Auto-Learning Policies

The auto-learning module of WAF studies statistics on normal traffic of protected websites and learns their normal traffic patterns. Based on the normal traffic patterns, the auto-learning module allows users to generate corresponding whitelist policies and loads the policies to the whitelist rule engine to check and sanitize abnormal traffic. Auto-learning policies are used to specify which statistics are to be collected for study.

You can do as follows on auto-learning policies by website group:

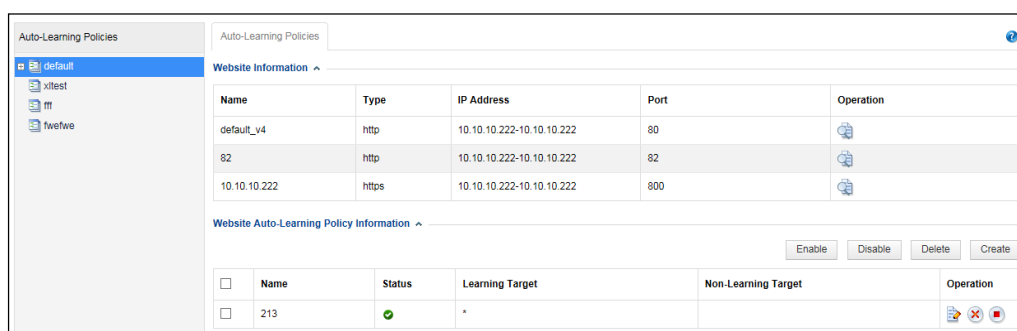
- [Creating an Auto-Learning Policy](#)
- [Editing an Auto-Learning Policy](#)
- [Deleting an Auto-Learning Policy](#)
- [Enabling an Auto-Learning Policy](#)
- [Disabling an Auto-Learning Policy](#)
- [Other Operations](#)

4.4.1 Creating an Auto-Learning Policy

To create an auto-learning policy, perform the following steps:

Step 1 Choose **Security Management > Auto-Learning Policies**.

Figure 4-58 Auto-Learning Policies page



Step 2 Click a website group in the auto-learning policy tree. Click **Create** on the **Auto-Learning Policies** page. Alternatively, point to a website group in the auto-learning policy tree, and click .

Figure 4-59 Creating an auto-learning policy

Create Auto-Learning Policy

Name *

HTTP Method ☒ POST ☒ GET Select at least one HTTP method.

HTTP Response Code ☒ 200 ☒ 302 ☒ 304 ☒ 307 Select at least one HTTP response code.

Learning Target (URL) *

Non-Learning Target (URL)

Advanced Options <<

Minimum Sample Number 3000 Number *

Min. Number of Sample Source IP 1000 Number *

☐ All

- ☒ HTTP Method Learns HTTP requests using specified HTTP methods.
- ☒ Number of Parameters Learns the number of parameters in HTTP requests.
- ☒ Parameter Type Learns whether parameters are of the String or Number type.
- ☒ Value Range Learns the string lengths of string-type parameters, and the value ranges of number-type parameters.
- ☒ Required Parameters Learns whether parameters are required to be always present in HTTP requests.

Learning Period 2015-05-15 2015-05-22

Data Processing Period 23:00 23:59 00:00 01:00

☒ Enable Immediately

OK Reset Cancel

Step 3 Set parameters in this dialog box.

Step 4 Click **OK** to save the settings.

----End

4.4.2 Editing an Auto-Learning Policy

To edit an auto-learning policy, perform the following steps:


Step 1 Click a website group in the auto-learning policy tree. In the right pane, click  in the **Operation** column in the **Website Auto-Learning Policy Information** area. Alternatively, click an auto-learning policy in the auto-learning policy tree.

Figure 4-60 Auto-Learning Policy Configuration page

Step 2 Set parameters in this dialog box.

Step 3 Click **OK** to save the settings.



During the editing process, you can click **Reset** to restore the previous parameter settings.

----End


4.4.3 Deleting an Auto-Learning Policy

An auto-learning policy can be deleted only after it is disabled. Auto-learning policies in different website groups cannot be deleted at the same time.





Auto-learning policies of a website group can be deleted individually or in batches. On the **Auto-Learning Policies** page shown in Figure 4-58, you can delete auto-learning policies using one of the following methods:

- Click  in the **Operation** column and click **OK** in the conformation dialog box to delete an auto-learning policy.
- Select one or more auto-learning policies, click **Delete** to the upper right of the list and then click **OK** in the conformation dialog box to delete the selected policy or policies.
- Point to a desired auto-learning policy and click .

4.4.4 Enabling an Auto-Learning Policy





By default, an auto-learning policy is enabled after being created. After it is disabled, its status is . A disabled auto-learning policy can be used after being enabled.

Auto-learning policies of a website group can be enabled individually or in bulk. Auto-learning policies in different website groups cannot be enabled at the same time. On the **Auto-Learning Policies** page shown in Figure 4-58, you can enable auto-learning policies as follows:

- Click  in the **Operation** column to enable an auto-learning policy. After it is enabled, its status turns to .
- Select one or more auto-learning policies and click **Enable** to the upper right of the list to enable the selected policy or policies. After they are enabled, their status turns to .
- Point to an auto-learning policy and then click  to enable it.

4.4.5 Disabling an Auto-Learning Policy

Auto-learning policies of a website group can be disabled individually or in batch. Auto-learning policies in different website groups cannot be disabled at one time. On the **Auto-Learning Policies** page shown in [Figure 4-58](#), you can disable auto-learning policies as follows:

- Click  in the **Operation** column to disable an auto-learning policy. After it is disabled, its status turns to .
- Select one or more auto-learning policies and then click **Disable** to the upper right of the list to disable the selected policy or policies. After they are disabled, their status turns to .
- Point to a desired auto-learning policy and then click the displayed  icon to disable it.

4.4.6 Other Operations

On the on the **Auto-Learning Policies** page shown in [Figure 4-58](#), you can do as follows:

- Switching to the **Website Group Mgmt** page of the current website group

In the **Operation** column, click  and then **Group Management**.

The **Website Group Mgmt** page appears, as shown in [Figure 4-21](#).

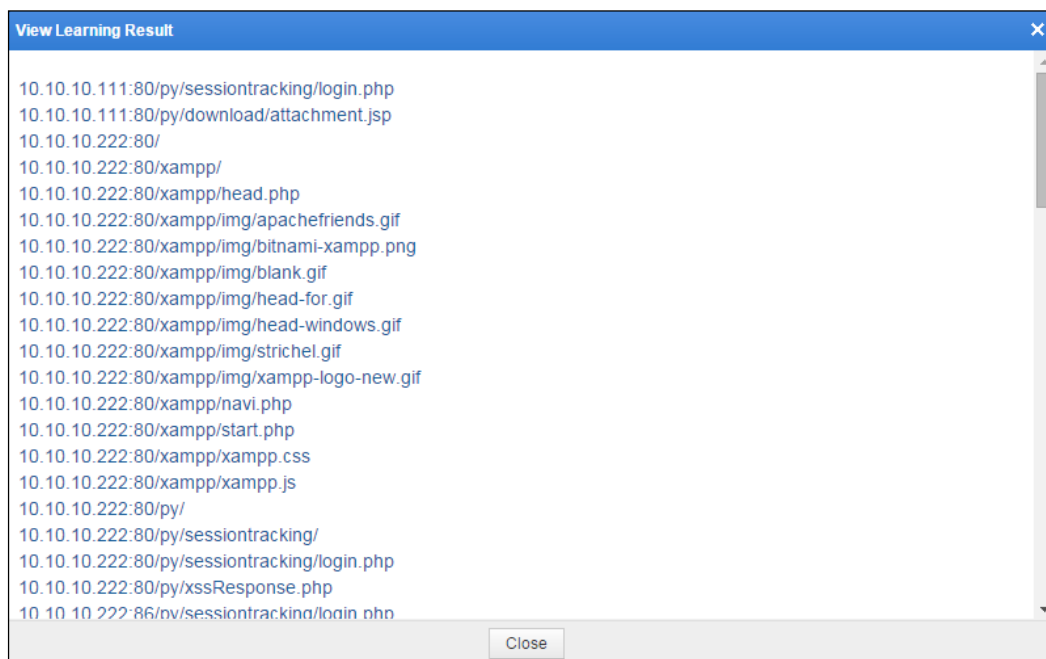
- Switching to the **View Learning Result** Page

In the **Operation** column, click  and then **Auto-Learning Results**.

The **View Learning Result** page appears, as shown in [Figure 4-61](#).

You can click a link in the dialog box to view the corresponding auto-learning results.

Figure 4-61 Viewing learning results



4.5 Auto-Learning Results


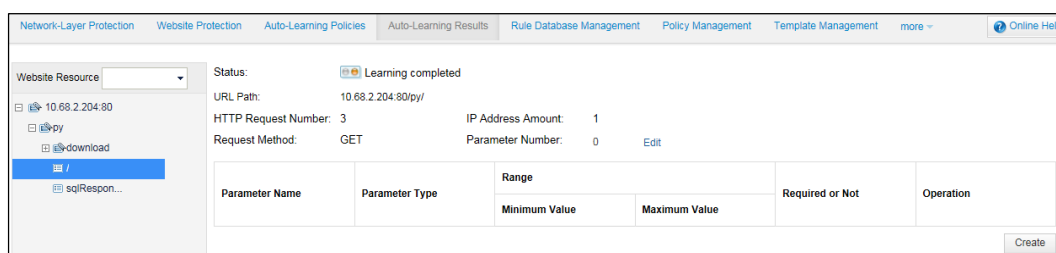
Choose **Security Management > Auto-Learning Results**. The **Auto-Learning Results** page appears, as shown in Figure 4-62. In the website group tree, select a website, the icon  indicates the auto-learning results of the website.

Figure 4-62 Auto-Learning Results page



4.6 Rule Database Management

When configuring a policy, you need to reference rules from the database. The WAF rule database contains the built-in common protection rule database and custom rule database.

4.6.1 Querying Common Protection Rules

Common protection rules are built-in rules. Users can only query them, but cannot edit them. To view common protection rules, perform the following steps:

Step 1 Choose **Security Management > Rule Database Management > Common Protection > Web Server Vulnerability**.

The **Web Server Vulnerability** page appears, as shown in [Figure 4-63](#). This page lists common protection rules for web server vulnerabilities.

Figure 4-63 Web Server Vulnerability page

Web Server Vulnerability

Conditions

ID:

Name:

Description:

Severity:

Accuracy:

Query

Page Number: 1 / 7 Record Number: 68

First Page Previous Page Next Page Last Page

ID	Name	Description	Operation
27526144	jboss_jmx_remote_command	CVE-ID: CVE-2015-7501 Rule Description: This is a common misconfiguration in JBoss Application Server (4.x, 5.x, ...). Whenever the JMX Invoker is exposed with the default configuration, a malicious "MarshaledInvocation" * serialized Java object allows to execute arbitrary code. Configuration Suggestion: JBoss users should enable the protection rule.	
27526143	iis_range_overflow	CVE-ID: CVE-2015-1635 Rule Description: HTTP.sys in Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 allows remote attackers to execute arbitrary code via crafted HTTP requests, aka "HTTP.sys Remote Code Execution Vulnerability." Configuration Suggestion: ou are advised to select this rule for IIS 6.0+ for which no corresponding patch has been loaded.	
		CVE-ID: CVE-2014-6271 Rule Description: GNU Bash 4.3 and earlier are prone to a vulnerability when handling the environment variables of certain structures. By appending an additional character string to a	

Step 2 Specify parameters to query a rule.

Table 4-16 Parameters for querying a rule

Parameter	Description
ID	ID of the rule to be queried.
Name	Name of the rule to be queried.
Description	Keyword to describe the rule.
Severity	Risk level of the rule, which can be High , Medium , or Low . Not select indicates no restriction to the risk level.
Accuracy	Accuracy of the rule, which can be High , Medium , or Low . Not select indicates no restriction to the accuracy.

Step 3 Click **Query**.

Qualified rules will be displayed.




Step 4 Click  to query details of a rule.

Figure 4-64 Details about a web server vulnerability rule

Details

Rule Overview	Rule Name	bash_specially_crafted_env_var_code_inj
	Rule ID	27526142
	Alert Type	Web_Server_Bug
	Severity	
	Accuracy	
Influence Range	Operating System	Linux/Unix
	Web Server	Apache Nginx Lighttpd Others
	Database	All Databases
	Programming Language	All System Languages
Detailed Description	<p>CVE-ID: CVE-2014-6271</p> <p>Rule Description: GNU Bash 4.3 and earlier are prone to a vulnerability when handling the environment variables of certain structures. By appending an additional character string to a function definition in an environment variable value, an attacker could exploit this vulnerability to change or bypass environment restrictions to execute shell commands. Certain services and applications allow unauthenticated remote attackers to exploit this vulnerability by providing environment variables. This vulnerability is caused because environment variables can be created using crafted values before the Bash shell is called. These variables can contain code that will be immediately executed after the shell is called.</p> <p>Configuration Suggestion: Users of Bash 4.3 and before should enable the protection rule.</p>	

Close

----End

4.6.2 Configuring Custom Rules

WAF's built-in protection rules are against known vulnerabilities. As web applications are usually customized, these built-in rules are insufficient to cover all web applications. You can customize protection rules and make them take effect by referencing them in policies.

Alert types of the custom rules can be various (such as **Web Server Vulnerability** and **Web Plug-in Vulnerability**) and **Custom**. When newly created policies reference a custom rule, the alert type of this custom rule determines how it is referenced.

- When **Alert Type** is set to **Custom**, the custom rule can be referenced only when a custom policy is created.
- When **Alert Type** is not set to **Custom**, the custom rule can be referenced when either a custom policy or other types of policies are created.

4.6.2.1 Creating Custom Rules

To create a custom rule, perform the following steps:

Step 1 Choose **Security Management > Rule Database Management > Custom Rules > Custom**.

Figure 4-65 Custom rules

The screenshot shows the 'Rule Database Management' interface. On the left, a tree view lists various protection rules under 'Common Protection' and 'Custom Rules'. The 'Custom Rules' section is selected, and the 'Custom' sub-section is highlighted. The main area displays a 'Custom' tab with a search bar and filters for ID, Name, and Description. Below the search bar, there are pagination controls showing 'Page Number: 0 / 1' and 'Record Number: 0'. A table with columns 'ID', 'Name', 'Description', and 'Operation' is shown, but it contains no data, indicated by a 'No data' message. A 'Create' button is located in the top right corner.

Step 2 Click **Create** to the upper right of the custom rule list.

Figure 4-66 Creating a custom rule

The screenshot shows the 'Create' dialog box for creating a custom rule. It has a blue header with the title 'Create' and a close button. The form contains the following fields and controls:


- Name:** A text input field.
- Description Information:** A large text area.
- Alert Type:** A dropdown menu set to 'Custom'.
- Inspection Direction:** A dropdown menu set to 'Request'.
- Set Constraint:** A section with three sub-fields:
 - Inspection Object:** A dropdown menu set to 'URI'.
 - Matching Relationship:** A dropdown menu set to 'Regular Expression Equal to'.
 - Inspection Value:** A text input field with a help icon.
- Buttons:** 'Add' and 'Remove' buttons are located below the 'Inspection Value' field.
- Constraints:** A text input field at the bottom of the form.
- Footer:** 'OK' and 'Cancel' buttons.

Step 3 Set the parameters and click **OK** to save the settings.

----End

4.6.2.2 Editing Custom Rules


You can edit the parameter settings of a custom rule after it is configured. To do that, perform the following steps:

- Step 1** On the **Custom** page shown in [Figure 4-65](#), click  in the **Operation** column of a rule and edit it.
- Step 2** Click **OK** to save settings and return to the **Custom** page.

----End

4.6.2.3 Deleting Custom Rules

You can delete custom rules one by one.

In the custom rule list of the **Custom** page shown in [Figure 4-65](#), click  in the **Operation** column and click **OK** in the confirmation dialog box, to delete a custom rule.

4.7 Policy Management

WAF provides various policies to defend against common web attacks. Policies can take effect only after being loaded by website groups. A policy can be loaded by multiple website groups.

WAF provides the following types of policies:

- Protocol validation: HTTP validation policies
- Basic protection: common protection policies in ordinary network environment
- Advanced protection: protection policies specific to network environment
- Precise protection: protection policies applied based on smart patches and auto-learning results
- Others: custom policies, exception policies, and risk level policies based on customer requirements

This section describes how to create, edit, delete, and duplicate policies on the **Policy Management** page. Policies can also be created and edited on the **Website Protection** page. For details, see [Secure Data Transfer](#) in section [4.3.2.4 Configuring Website Security Policies](#).

In addition, WAF provides default policies for certain type of policies, such as **default_low**, **default_medium**, and **default_high**. Each type of policy may contain one or more default policies, which cannot be deleted or modified but can be copied and saved as new policies.

4.7.1 HTTP Validation Policies

HTTP, standing for Hypertext Transfer Protocol, is used to transfer web page information over the Internet. A huge amount of malformed HTTP validation packets could delay server responses to legitimate requests, and even cause buffer overflows or server crashes. After HTTP validation is configured, WAF stops HTTP requests that do not comply with HTTP validation policies from accessing protected servers.






Creating an HTTP Validation Policy

To create an HTTP validation policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management**.

The **HTTP Validation** page appears, as shown in [Figure 4-67](#).

Figure 4-67 HTTP Validation page

HTTP Validation					Create
	Name	Description	Alert or Not	Operation	
+	default_low	Loose policy	Yes	 	
+	default_medium	Standard policy	Yes	 	
+	default_high	Strict policy	Yes	 	

Step 2 Click **Create**.

Figure 4-68 Creating an HTTP validation policy

Create HTTP Validation

Basic Information

Name
* The name length should not exceed 50 characters

Description
The description content should not exceed 200 characters.

Alert or Not ☒ Yes ☐ No

Inspection Item

☐ Detect all ☐ Block for all

<input checked="" type="checkbox"/>	Abnormal URI
<input checked="" type="checkbox"/>	Abnormal Host
<input checked="" type="checkbox"/>	Abnormal User-Agent
<input checked="" type="checkbox"/>	Abnormal Cookie
<input checked="" type="checkbox"/>	Abnormal Referer
<input checked="" type="checkbox"/>	Abnormal Accept
<input checked="" type="checkbox"/>	Abnormal Content
<input checked="" type="checkbox"/>	Abnormal Ranges
<input checked="" type="checkbox"/>	Abnormal HTTP Header
<input checked="" type="checkbox"/>	Abnormal Parameter
<input checked="" type="checkbox"/>	Abnormal Encoding
<input checked="" type="checkbox"/>	Abnormal Upload

HTTP Decoding Control

Clear Abnormal %	<input type="radio"/> Yes <input checked="" type="radio"/> No	When a URI or parameter value contains a percent symbol that is not followed by a hexadecimal value (such as %XY), security policies may not take effect.
Clear Null Character	<input type="radio"/> Yes <input checked="" type="radio"/> No	When a URI or parameter value contains NULL characters (such as \0 and %00), security policies may not take effect.

OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-17 Parameters for creating an HTTP validation policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Inspection Item	<p>Specifies items to be checked, such as abnormal headers, abnormal parameters, and abnormal encodings.</p> <ul style="list-style-type: none"> By default, except Forbid Duplicate HTTP Headers under Abnormal HTTP Header, all newly created inspection items are checked. You can cancel the selection of all the items by selecting Detect all in the upper-right corner of this area and then deselecting it.


Parameter	Description
	<ul style="list-style-type: none"> By default, except Forbid Duplicate HTTP Headers under Abnormal HTTP Header, all newly created inspection items have the action set to Block. You can change the "block" action to "accept" for all items by selecting Block for all in the upper-right corner of this area and then deselecting it.
HTTP Decoding Control	Controls whether WAF removes percent signs (%) or null characters in HTTP decoding.

Step 4 Click **OK** to save the settings.

----End

Editing an HTTP Validation Policy

You can edit an HTTP validation policy after it is configured. To do that, perform the following steps:

- Step 1** In the HTTP validation policy list of the **HTTP Validation** page shown in [Figure 4-67](#), click  in the **Operation** column of an HTTP validation policy.
- Step 2** In the dialog box, edit parameters of the HTTP validation policy, and then click **OK** to save settings and return to the **HTTP Validation** page.

----End

Duplicating an HTTP Validation Policy

To create an HTTP validation policy, you can directly create one or duplicate an existing policy and then modify parameters. To do that, perform the following steps:

- Step 1** On the page shown in [Figure 4-67](#), click  in the **Operation** column.

Figure 4-69 Duplicating an HTTP validating policy

Duplicate HTTP Validation

Basic Information

Name:
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Inspection Item

☐ Detect all ☐ Block for all

<input type="checkbox"/>	Abnormal URI
<input type="checkbox"/>	Abnormal Host
<input type="checkbox"/>	Abnormal User-Agent
<input type="checkbox"/>	Abnormal Cookie
<input type="checkbox"/>	Abnormal Referer
<input type="checkbox"/>	Abnormal Accept
<input type="checkbox"/>	Abnormal Content
<input type="checkbox"/>	Abnormal Ranges

OK Reset Close

Step 2 In the dialog box, modify parameters.


For details, see [Table 4-17](#).

Step 3 Click **OK** to save the settings.

----End

Deleting an HTTP Validation Policy

You can delete HTTP validation policies one by one.

In the HTTP validation policy list of the **HTTP Validation** page shown in [Figure 4-67](#), click  in the **Operation** column and click **OK** in the confirmation dialog box, to delete an HTTP validation policy.

4.7.2 Basic Protection Policies

Basic protection refers to common protection policies in the network environment, which includes:

- [Web Server/Plug-in Protection Policy](#)
- [HTTP Access Control Policy](#)
- [Crawler Protection Policy](#)
- [Common Web Protection Policy](#)
- [Illegal Upload Restriction Policy](#)
- [Illegal Download Restriction Policy](#)
- [Information Disclosure Protection Policy](#) (not applicable to the mirroring mode)

4.7.2.1 Web Server/Plug-in Protection Policy







"Web server/plug-in" refers to web servers and service logics running on web servers. Based on rules designed for known server vulnerabilities and service logic vulnerabilities, web server/plug-in protection mainly detects and defends against illegal requests and responses. WAF's web server/plug-in protection policies can flexibly load protection rules specific to web servers and service logics running on web servers.

On the **Web Server/Plug-in Protection** page, you can create, edit, delete, and duplicate web server/plug-in protection policies. The following only describes how to create web server/plug-in protection policies. The editing, deleting, and duplicating operations for web server/plug-in protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a web server/plug-in protection policy, perform the following steps:

- Step 1** Choose **Security Management > Policy Management > Basic Protection > Web Server/Plug-in Protection**.

Figure 4-70 Web Server/Plug-in Protection page

Web Server/Plug-in Protection						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
+	default_low	Loose policy	Yes	Block	Unblock	 
+	default_medium	Standard policy	Yes	Block	Unblock	 
+	default_high	Strict policy	Yes	Block	Unblock	 

- Step 2** Click **Create**.

Figure 4-71 Creating a web server/plug-in protection policy

Step 3 In the dialog box, set the parameters.

Table 4-18 Parameters for creating a web server/plug-in protection policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks. Accept: WAF ends the check against the current policy but will still check such request against other policies. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	Controls whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block . <ul style="list-style-type: none"> Unblock: WAF does not block the source IP address.

Parameter	Description
	<ul style="list-style-type: none"> • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set if Action is set to Redirection .
Response Code	Custom response code. This parameter needs to be set if Action is set to Disguise .
Response File	Response file. This parameter needs to be set if Action is set to Disguise . You can select an existing response file or upload a new one.
Matching Principle	Controls whether WAF continues to match a packet that has matched a rule in a policy against other rules in the policy. <ul style="list-style-type: none"> • Stop upon a match: WAF stops matching the packet against other rules in the policy. • Continue upon a match: WAF continues to match the packet against other rules in the policy.
Rule Filtering	Rule filtering conditions. After you set filtering conditions and click Filter , rules that meet filtering conditions are displayed under Rule List .
Rule List	Rule lists. To add a rule to a rule set (Web Server Vulnerability or Web Plug-in Vulnerability), just select the check box of the rule. At least one rule should be selected.

Step 4 Click **OK** to save the settings.

----End

4.7.2.2 HTTP Access Control Policy



WAF applies HTTP access control policies to HTTP requests from clients and handling matching packets as specified in policies. A single website can be configured with multiple HTTP access control policies. WAF matches packets against the policies from top down the policy list displayed in a page. Once a packet hits a policy, WAF stops matching the packet against subsequent policies.

On the **HTTP Access Control** page, you can create, edit, delete, and duplicate HTTP access control policies. The following only describes how to create HTTP access control policies. The editing, deleting, and duplicating operations for HTTP access control policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create an HTTP access control policies, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Basic Protection > HTTP Access Control**.

Figure 4-72 HTTP Access Control page

HTTP Access Control						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
+	default_low	Loose policy	Yes	Block	Unblock	 
+	default_medium	Standard policy	Yes	Block	Unblock	 
+	default_high	Strict policy	Yes	Block	Unblock	 
+	test1		Yes	Block	Unblock	 

Step 2 Click **Create**.

Figure 4-73 Creating an HTTP access control policy

Create HTTP Access Control

Basic Information

Name

The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Pass

Protection Information

☐ Host Name

Include

UTF-8

Case-sensitive

☐ URI-Path

Directory Matching

UTF-8

Case-sensitive

☐ HTTP Method

Include

☐ All
☒ GET
☐ DELETE
☐ OPTIONS
☐ UNLOCK

☒ POST
☐ MKCOL
☐ PROPFIND
☐ TRACE

☒ HEAD
☐ COPY
☐ PROPPATCH
☐ SEARCH

☐ PUT
☐ MOVE
☐ LOCK
☐ CONNECT

☐ Client IP Address

Include

OK

Reset

Cancel

Step 3 In the dialog box, set the parameters.

Table 4-19 Parameters for creating HTTP access control policies

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.

Parameter	Description
Alert or Not	Controls whether to generate alert logs.
Action	<p>Specifies the action WAF will take on a matched request. Actions include the following:</p> <ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Protection Information	Specifies which conditions need to be met for a packet to match the new policy. Those conditions include Host Name , URI-Path , HTTP Method , and Client IP Address . If multiple conditions are specified, the policy will be hit only when all specified conditions are matched. If no specific condition is specified, the policy will be hit if any of the conditions are matched. For details about how to specify the conditions, see help information in the dialog box.

Step 4 Click **OK** to save the settings.

----End

4.7.2.3 Crawler Protection Policy

A web crawler is a computer program or script that browses World Wide Web in an automated and orderly manner. Plenty of search engines such as Yahoo! and Baidu employ crawlers to provide the latest data. However, malicious crawling on a large number of web pages not only occupies bandwidth but also reduces server performance. Crawler protection policies enable WAF to protect information against search engines.

On the **Crawler Protection** page, you can create, edit, delete, and duplicate crawler protection policies. The following only describes how to create crawler protection policies.

The editing, deleting, and duplicating operations for crawler protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a crawler protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Basic Protection > Crawler Protection**.

Figure 4-74 Crawler Protection page

Crawler Protection						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
	default_high	Strict policy	Yes	Block	Unblock	

Step 2 Click **Create**.

Figure 4-75 Creating a crawler protection policy

Create Crawler Protection

Basic Information

Name

* The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Block

Source IP Blocking

Unblock

Rule Information

Matching Principle

☒ Stop upon a match ☐ Continue upon a match

Rule Filtering

Rule List

View All

☒ Crawler Protection

OK

Reset

Cancel

Step 3 In the dialog box, set the parameters.

Table 4-20 Parameters for creating a crawler protection policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	<p>Specifies the action WAF will take on a matched request. Actions include the following:</p> <ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter is required if Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Matching Principle	<p>Controls whether WAF continues to match a packet that has matched a rule in a policy against other rules in the policy.</p> <ul style="list-style-type: none"> • Stop upon a match: WAF stops matching the packet against other rules in the policy. • Continue upon a match: WAF continues to match the packet against other rules in the policy.
Rule Filtering	Rule filtering conditions. After you set filtering conditions and click Filter , rules that meet filtering conditions are displayed under Rule List .
Rule List	<p>Rule lists. By default, all rules are listed. After you filter rules, only rules that meet filtering conditions are displayed.</p> <p>To add a rule to a rule set (Web Server Vulnerability or Web Plug-in Vulnerability), just select the check box of the rule. At least one rule should be selected.</p>

Step 4 Click **OK** to save the settings.

----End

4.7.2.4 Common Web Protection Policy

Common web protection policies are mainly used for Structured Query Language (SQL) injection protection, command line injection protection, and cross-site scripting (XSS or CSS) protection.

SQL injection is a process of including SQL commands in data to be submitted to a server, in an attempt to entice the server to execute these SQL commands. SQL injection attacks tend to result from defects in the server code. For example, the server application may access the database via dynamic SQL statements crafted based on unauthenticated user inputs.


An XSS attack refers to the act of stealing information from users via exploitation of website vulnerabilities. Users usually click links while browsing websites, using Instant Messaging software, and reading e-mails. By embedding malicious code into the links, attackers could steal user information.

On the **Common Web Protection** page, you can create, edit, delete, and duplicate common web protection policies. The following only describes how to create common web protection policies. The editing, deleting, and duplicating operations for common web protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a common web protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Basic Protection > Common Web Protection**.

Figure 4-76 Common Web Protection page

Common Web Protection						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
+	default_low	Loose policy	Yes	Block	Unblock	 
+	default_medium	Standard policy	Yes	Block	Unblock	 
+	default_high	Strict policy	Yes	Block	Unblock	 

Step 2 Click **Create**.

Figure 4-77 Creating a common web protection policy

Step 3 In the dialog box, set the parameters.

Table 4-21 Parameters for creating a common web protection policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks. Accept: WAF ends the check against the current policy but will still check such request against other policies. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	Specifies whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block . <ul style="list-style-type: none"> Unblock: WAF does not block the source IP address.

Parameter	Description
	<ul style="list-style-type: none"> • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter is required if Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Matching Principle	Controls whether WAF continues to match a packet that has matched a rule in a policy against other rules in the policy. <ul style="list-style-type: none"> • Stop upon a match: WAF stops matching the packet against other rules in the policy. • Continue upon a match: WAF continues to match the packet against other rules in the policy.
Rule Filtering	Rule filtering conditions. After you set filtering conditions and click Filter , rules that meet filtering conditions are displayed under Rule List .
Rule List	<p>Rule lists. By default, all rules are listed. After you filter rules, only rules that meet filtering conditions are displayed.</p> <p>To add a rule to a rule set (Web Server Vulnerability or Web Plug-in Vulnerability), just select the check box of the rule. At least one rule should be selected.</p>

Step 4 Click **OK** to save the settings.

----End

4.7.2.5 Illegal Upload Restriction Policy

When a client uploads a file to a server, WAF performs protection based on the file type. If the file type matches an illegal upload restriction policy, WAF allows or blocks the upload based on the corresponding action specified in the policy, and logs the event.

On the **Illegal Upload Restriction** page, you can create, edit, delete, and duplicate illegal upload restriction policies. The following only describes how to create illegal upload restriction policies. The editing, deleting, and duplicating operations for illegal upload restriction policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create an illegal upload restriction policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Basic Protection > Illegal Upload Restriction**.

Figure 4-78 Illegal Upload Restriction page

Illegal Upload Restriction							Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation	
	default_low	Loose policy	Yes	Block	Unblock		
	default_medium	Standard policy	Yes	Block	Unblock		
	default_high	Strict policy	Yes	Block	Unblock		

Step 2 Click **Create**.

Figure 4-79 Creating an illegal upload restriction policy

Create Illegal Upload Restriction

Basic Information

Name

* The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Block

Source IP Blocking

Unblock

File Extensions to Be Inspected

Enter file extensions in this box.

File extensions are separated by semicolon (;). For example exe;php;html.

File Type to Be Inspected

Shell Type

☐ All
 ☐ PE(windows Executable File)
 ☐ ELF(linux Executable File)
 ☐ Php web shell
 ☐ Linux shell
 ☐ Power shell(windows Script File)

OK

Reset

Cancel

Step 3 In the dialog box, set the parameters.

Table 4-22 Parameters for creating an illegal upload restriction policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	<p>Specifies the action WAF will take on a matched request. Actions include the following:</p> <ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set if Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Enter file extensions in this box	Customized file extensions.
Shell Type	Shell types of upload files to be checked. After a file type is selected, WAF will handle this type of upload files according to the configured policy and action.

Step 4 Click **OK** to save the settings.

----End

4.7.2.6 Illegal Download Restriction Policy







When a client downloads a file from a server, WAF performs protection based on the file type. If the file type matches an illegal download restriction policy, WAF allows or blocks the download based on the corresponding action specified in the policy, and logs the event.

On the **Illegal Download Restriction** page, you can create, edit, delete, and duplicate illegal file download restriction policies. The following only describes how to create illegal file download restriction policies. The editing, deleting, and duplicating operations for illegal file download restriction policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create an illegal file download restriction policy, perform the following steps:

- Step 1** Choose **Security Management > Policy Management > Basic Protection > Illegal Download Restriction**.

Figure 4-80 Illegal Download Restriction page

Illegal Download Restriction						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
+	default_low	Loose policy	Yes	Block	Unblock	 
+	default_medium	Standard policy	Yes	Block	Unblock	 
+	default_high	Strict policy	Yes	Block	Unblock	 

- Step 2** Click **Create**.

Figure 4-81 Creating an illegal download restriction policy

Create Illegal Download Restriction

Basic Information

Name
* The name length should not exceed 50 characters

Description
The description content should not exceed 200 characters.

Alert or Not ☒ Yes ☐ No

Action ?

Source IP Blocking

Inspection Information

File Size Inspection ☐ Yes ☒ No

File Extension Inspection ☐ Yes ☒ No

MIME Type Inspection ☐ Yes ☒ No

OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-23 Parameters for creating an illegal download restriction policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks. Accept: WAF ends the check against the current policy but will still check such request against other policies. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection.

Parameter	Description
	<ul style="list-style-type: none"> • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Response Code	<p>Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action.</p> <p>When the response code is equal to or greater than 200 but smaller than 400, protection will be triggered and an alert will be generated for a security event.</p>
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
File Size Inspection	Controls whether to enable file size inspection. If this parameter is set to Yes , File Size(byte) also needs to be set to specify the file size threshold, and WAF handles the download of files larger than the threshold as specified in the policy.
File Extension Inspection	Controls whether to enable file extension inspection. If this parameter is set to Yes , File Extension also needs to be set to specify file extensions, and WAF handles the download of files with the specified file extensions as specified in the policy.
MIME Type Inspection	Controls whether to enable MIME inspection. If this parameter is set to Yes , MIME Type also needs to be set to specify MIME types, and WAF handles the download of files of the specified types as specified in the policy.

Step 4 Click **OK** to save the settings.

----End

4.7.2.7 Information Disclosure Protection Policy

A server gains different results in handling different requests, and returns results to clients by sending different status codes. Sometimes, a status code may disclosure important information about the server, providing attackers an opportunity to launch more effective attacks. Hence, it is necessary to prevent server from returning status codes with sensitive information to clients.

To prevent information disclosure, WAF filters server-to-client responses and removes sensitive information from them.








Information disclosure protection policies do not work on WAF in mirroring mode.

On the **Information Disclosure** page, you can create, edit, delete, and duplicate information disclosure protection policies. The following only describes how to create information disclosure protection policies. The editing, deleting, and duplicating operations for information disclosure protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create an information disclosure protection policy, perform the following steps:

- Step 1** Choose **Security Management > Policy Management > Basic Protection > Information Disclosure Protection**.

Figure 4-82 Information Disclosure page

Information Disclosure					
					Create
	Name	Description	Replace Service Name	Alert or Not	Operation
+	default_low	Loose policy		Yes	 
+	default_medium	Standard policy		Yes	 
+	default_high	Strict policy		Yes	 

- Step 2** Click **Create**.

Figure 4-83 Creating an information disclosure policy

Create Information Disclosure Protection Policy

Basic Information

Name * The name length should not exceed 50 characters

Alert or Not ☒ Yes ☐ No

Change Server Name to

Description The description content should not exceed 200 characters

Rule Definition

Action	Response Status	Redirection Path/Response Replacement Content ?

OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-24 Parameters for creating an information disclosure protection policy

Parameter	Description
Name	Name of the new policy.
Alert or Not	Controls whether to generate alert logs.
Change Server Name to	Specifies the alias name to which server names are changed. After this parameter is set to a value, all server names in HTTP responses are changed to the value. If this parameter is left empty, server names in HTTP responses are not changed.
Description	Brief description of the new policy.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Response Status	Status codes specified in a rule. Packets with the response status will hit

Parameter	Description
	the rule. For descriptions about status codes, see Table 4-25 .
Redirection Path/Response Replacement Content	<p>Redirection path or response replacement content.</p> <ul style="list-style-type: none"> If Action is set to Redirection, specify the redirection path for this parameter. The value should be a string of 1 to 2048 characters. If Action is set to Disguise, specify the response code and files for this parameter. If Action is set to Pass or Block, leave this parameter empty.

Table 4-25 Common status codes

Status Code	Description
200(OK)	Standard response for successful HTTP requests. Generally, this means that the server has provided the requested resource.
201(Created)	The request has been fulfilled and resulted in a new resource being created.
202(Accepted)	The request has been accepted for processing, but the processing has not been completed.
203(Non-Authoritative Information)	The server successfully processed the request, but is returning information that may be from another source.
204(No Content)	The server successfully processed the request, but is not returning any content.
205(Reset Content)	The server successfully processed the request, but is not returning any content. Unlike a 204 response, this response requires that the requester reset the document view.
206(Partial Content)	The server is delivering only part of the resource.
300(Multiple Choices)	Multiple options for the resource that the client may follow are provided. The server either chooses an option based on the requester (user agent) or provides a list of options for the requester to choose.
301(Moved Permanently)	This and all future requests should be directed to a new URI when this response is returned to a GET or HEAD request.
302(Moved Temporarily)	The server responds the request temporarily from a different URI, but the client should continue to use the Request-URI for future requests. This code is similar to 301, except that the new URI for 302 is temporary.
303(See Other)	The response to the request can be found under another URI and should be retrieved using a GET method on that resource. For requests other than HEAD, the server automatically redirects them to other URIs.
304(Not Modified)	<p>The resource has not been modified since last requested. The server does not return resource content.</p> <p>If the resource has not been modified since last requested, set the server to respond this code (called the If-Modified-Since header).</p>
305(Use Proxy)	The requested resource must be accessed through the proxy. This code indicates the requester should use proxy.
307(Temporary Redirect)	The requester is redirected to a different URI where resource resides temporarily, but future requests still use the original URI.

Status Code	Description
400(Bad Request)	The request contains bad syntax or cannot be fulfilled.
401(Unauthorized)	Authentication is required. This code often appears when a user requests to access a URI after login.
403(Forbidden)	The request was a legal request, but the server is refusing to respond to it.
404(Not Found)	The requested resource could not be found but may be available again in the future. For example, this code is usually returned to requests for websites that do not exist in the server.
405(Method Not Allowed)	A request was made of a resource using a request method not supported by that resource.
406(Not Acceptable)	The requested resource is only capable of generating content not acceptable according to the Accept headers sent in the request.
407(Proxy Authentication Required)	The client must first authenticate itself with the proxy.
408(Request Timeout)	The server timed out waiting for the request.
409(Conflict)	The request could not be completed due to a conflict with the current state of the resource. Information about the conflict must be contained in the server response. The server may return this code to a PUT request that conflicts with the previous request, together with a list of the differences between the two requests.
410(Gone)	The requested resource is no longer available at the server. This code is similar to 404 (Not Found), and may be replaced with 404 when the resource that used to be available is not available now. If the resource is moved permanently, use 301 (Moved Permanently).
411(Length Required)	The server refuses to accept the request without a defined Content- Length.
412(Precondition Failed)	The precondition given in one or more of the request-header fields evaluated to false when it was tested on the server.
413(Request Entity Too Large)	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
414(Request-URI Too Long)	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415(Unsupported Media Type)	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
416(Requested Range Not Satisfiable)	The client has asked for a portion of the file, but the server cannot supply that portion.
417(Expectation Failed)	The server cannot meet the requirements of the Expect request-header field.
500(Internal Server Error)	The server encountered an unexpected condition which prevented it from fulfilling the request.
501(Not Implemented)	The server either does not recognize the request method, or it lacks the ability to fulfill the request.
502(Bad Gateway)	The server was acting as a gateway or proxy and received an invalid response from the upstream server.
503(Service Unavailable)	The server is currently unavailable (because it is overloaded or down for maintenance). Generally, this is a temporary state.

Status Code	Description
504(Gateway Timeout)	The server was acting as a gateway or proxy and did not receive a timely response from the upstream server.
505(HTTP Version Not Supported)	The server does not support the HTTP protocol version used in the request.

Step 4 Click **OK** to save the settings.

----End

4.7.3 Advanced Protection

Advanced protection refers to protection policies specific to network environments, including the following:

- [Leech Protection Policy](#)
- [CSRF Protection Policy](#)
- [Scanning Protection Policy](#)
- [Cookie Security Policy](#)
- [Content Filtering Policy](#)
- [Sensitive Information Filtering Policy](#)
- [Brute Force Protection Policy](#)
- [XML Attack Protection Policy](#)
- [Smart Engine Inspection](#)



CSRF protection policies, cookie security policies, and sensitive information filtering policies do not work on WAF in mirroring mode.

4.7.3.1 Leech Protection Policy

Leech indicates the behavior of referencing, without proper authorization, resources (images, videos and audios) of other service providers by means of code injection and online play. Web leech may exhaust the bandwidth of a website (when the actual bandwidth usage is not so big) and even stop the website from providing service properly, severely compromising its benefit.





Via leech protection policies, WAF stops unauthorized use of resources such as images, videos, audios, and software.

On the **Leech Protection** page, you can create, edit, delete, and duplicate leech protection policies. The following only describes how to create leech protection policies. The editing, deleting, and duplicating operations for leech protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a leech protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Advanced Protection > Leech Protection**.

Figure 4-84 Leech Protection page

Leech Protection								
								Create
	Name	Description	Inspection Algorithm	Alert or Not	Action	Source IP Blocking	Allow Null Referer	Operation
+	default_medium	Standard policy	Referer Inspection	Yes	Accept	Unblock	Yes	 
+	default_high	Strict policy	Referer+Cookie Inspection	Yes	Block	Unblock	Yes	 

Step 2 Click **Create**.

Figure 4-85 Creating a leech protection policy

Create Leech Protection

Basic Information

Name
 * The name length should not exceed 50 characters

Description
 The description content should not exceed 200 characters.

Alert or Not ☒ Yes ☐ No

Action ?

Source IP Blocking

Policy Inspection Mode ?

Trusted Websites ?

Allow Null Referer ☒ Yes ☐ No


URI-Path Allowing Null Referer ?


OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-26 Parameters for creating a leech protection policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks.

Parameter	Description
	<ul style="list-style-type: none"> • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Policy Inspection Mode	<p>Policy inspection mode, which can be either of the following:</p> <ul style="list-style-type: none"> • Referer Inspection: Only the referer field in an HTTP request is checked. If the referer field matches a URL in the trust domain, WAF considers the HTTP request as a legitimate one; if no, WAF regards it as a leech request. • Referer+Cookie Inspection: The referer field and cookie ID in an HTTP request are checked. If the referer field matches a URL in the trust domain and the cookie ID is authorized by WAF, WAF considers the HTTP request as a legitimate one. If the referer field does not match any URL in the trust domain or the cookie ID is not authorized by WAF, WAF regards it as a leech request. <p> Note</p> <p>Referer+Cookie Inspection does not work on WAF in mirroring mode.</p>
Trusted Websites	<p>Entrance page of the target URL. A client has to first visit the entrance page (referer URL) before being redirected to the target URL. Other methods of visiting the target URL are considered as leeches.</p> <p>The value is URLs starting with http:// or https://. The wildcard * is supported, but this does not indicate that any URL parameters are allowed. For example, the format is http://*.example.com.</p>

Parameter	Description
	 Note Each URL takes up one line. If no trust domain is specified, referer URLs from the same website are always trusted.
Allow Null Referer	Controls whether the referer can be empty for URLs. If no URL is specified, the referer can be empty for all URLs. If any URL is specified, the referer can be empty only for the specified URL.
URIs Allowing Null Referer	URIs that can be without a referrer. If no URI is specified, the referer can be empty for all URIs. If any URI is specified, the referer can be empty only for the specified URI.

Step 4 Click **OK** to save the settings.

----End

4.7.3.2 CSRF Protection Policy

Cross-site request forgery (CSRF) is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts but is actually assumed by an attacker. Common CSRF attacks include: sending e-mails and messages in the user's name, stealing user accounts, or purchasing goods and performing virtual currency transfer. These attacks could cause privacy disclosure and fortune loss.

On the **CSRF Protection** page, you can create, edit, delete, and duplicate CSRF protection policies. The following only describes how to create CSRF protection policies. The editing, deleting, and duplicating operations for CSRF protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a CSRF protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Advanced Protection > CSRF Protection**.

Figure 4-86 CSRF Protection page

CSRF Protection Create						
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
	testabc		Yes	Block	Unblock	  

Step 2 Click **Create**.

Figure 4-87 Creating a CSRF protection policy

Step 3 In the dialog box, set the parameters.

Table 4-27 Parameters for creating a CSRF protection policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks. Accept: WAF ends the check against the current policy but will still check such request against other policies. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block .

Parameter	Description
	<ul style="list-style-type: none"> Unblock: WAF does not block the source IP address. Permanently block: WAF permanently blocks the source IP address. Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
URI to Submit	URLs to be protected. To visit the target URL, a client must send a request carrying the hash value that was assigned by WAF when it visited the referer URL; otherwise, WAF will block the access request.
URI containing the FORM	Entry URL for the URL to be protected. When a client visits a referer URL, WAF will generate a random hash value and return it to the client. To visit a target URL, the client will send a request carrying this hash value. If WAF considers that the hash is valid, it will let the access pass; otherwise, it will block the access.
Web 2.0 Config	<p>Controls whether to enable web 2.0 protection.</p> <p>After web 2.0 protection is enabled, a secret key generated by the security engine will be delivered to both the form and cookie. The valid time of the secret key is subject to the configuration, and the secret key will become invalid after authentication.</p>

Step 4 Click **OK** to save the settings.

----End

4.7.3.3 Scanning Protection Policy

Attackers usually use tools to scan a website for vulnerabilities. This is a huge threat to website security. WAF blocks malicious scanning by recognizing packet signatures of scanners.

WAF comes with built-in protection rules against common scanners such as pangolin, webinspect, and appscan, and allows you to configure signatures to protect against other scanners.

On the **Scanning Protection** page, you can create, edit, delete, and duplicate scanning protection policies. The following only describes how to create scanning protection policies. The editing, deleting, and duplicating operations for scanning protection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a scanning protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Advanced Protection > Scanning Protection**.

Figure 4-88 Scanning Protection page

Scanning Protection						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
+	default_low	Loose policy	Yes	Block	Unblock	 
+	default_medium	Standard policy	Yes	Block	Unblock	 
+	default_high	Strict policy	Yes	Block	Block5minutes	 

Step 2 Click **Create**.

Figure 4-89 Creating a scanning protection policy

Create Scanning Protection

Basic Information

Name

* The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Block

Source IP Blocking

Unblock

Rule Information

Rule Database Matching

Request Amount Measurement

Response Distribution Measurement

Threshold Alerting

Enable or Not

☒ Yes ☐ No

OK


Reset


Cancel

Step 3 In the dialog box, set the parameters.

Table 4-28 Parameters for creating a scanning protection policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include

Parameter	Description
	<p>the following:</p> <ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Rule Database Matching	Controls whether to enable rule database matching.
Request Measurement Amount	Controls whether to count HTTP requests in a given measurement period.
Request Measurement Amount	<ul style="list-style-type: none"> • Enable or Not: Controls whether to count HTTP requests in a given measurement period. • Minimum Sample Amount: Specifies the minimum sample amount, which is an integer from 2 to 20. WAF performs statistical analysis only after the measured request amount reaches or exceeds the value of this parameter. • Request Discrete Rate: Specifies the request discrete rate, which is a decimal between 0 and 1. Within a measurement period, a smaller request discrete rate indicates more regular statistics. Usually, regular statistics are contributed by scanners. • Maximum Request Amount: Specifies the maximum number of HTTP requests allowed by WAF in 5 seconds. <p> Note</p> <p>At least one of Request Discrete Rate and Maximum Request Amount should be specified. If only Maximum Request Amount is</p>

Parameter	Description
	specified, Request Discrete Rate is 0 by default.
Response Distribution Measurement	<ul style="list-style-type: none"> • Enable or Not: controls whether to enable response distribution measurement. After this function is enabled, WAF collects statistics about the distribution of HTTP response codes. • Successful Response Proportion: specifies the proportion of successful response codes within a measurement period, such as 100(Continue), 200(OK), and 302(Found). The value is a decimal between 0 and 1. • Failed Response Proportion: specifies the proportion of failed response codes within a measurement period, such as 404(Not Found) and 500(Internal Server Error). The value is a decimal between 0 and 1. <p> Note</p> <p>At least one of Successful Response Proportion and Failed Response Proportion should be specified. If only Successful Response Proportion is specified, Failed Response Proportion is 1 by default. If only Failed Response Proportion is specified, Successful Response Proportion is 0 by default.</p> <ul style="list-style-type: none"> • Minimum Measurement Amount: specifies the minimum measured amount in a measurement period. WAF performs proportion calculation only after the measured amount reaches or exceeds the value of this parameter. • Measurement Period: specifies the period of the scanning protection policy.
Threshold Alerting	<ul style="list-style-type: none"> • Enable or Not: controls whether to enable threshold-based alerting. • Maximum Alert Threshold: Specifies the maximum number of alerts of a specified source IP address within a measurement period. • Measurement Period: specifies the period of the scanning protection policy.

Step 4 Click **OK** to save the settings.

----End

4.7.3.4 Cookie Security Policy

Cookie is a piece of data, which is sent from a server to a client browser, saved in the browser, and submitted to the server in subsequent access. Cookie is usually used to save information, such as client information and session status. When a client accesses a server, some important information saved in the cookie may be exploited by others, causing information disclosure or other security issues. In addition, web applications may be prone to vulnerabilities in the handling of cookie values. Attackers could submit malicious requests to launch attacks by tampering submitted cookie contents.

WAF performs cookie protection in either of the following ways:

- **Cookie signature:** WAF signs a cookie value without changing its contents, and sends the signature as part of the cookie content to a client. Since cookie contents are in plain text, the client can view the cookie contents. However, if the client attempts to tamper the cookie signature, WAF will detect the tampering and take corresponding actions.
- **Cookie encryption:** WAF uses its own encryption algorithm to encrypt a cookie value, and sends the encrypted cookie value to a client. After the client submits the encrypted cookie to the server, WAF decrypts the encrypted cookie value, and sends the cookie value in plain text to the server. This can prevent attackers from obtaining cookie values and tampering cookie contents.

On the **Cookie Security** page, you can create, edit, delete, and duplicate cookie security policies. The following only describes how to create cookie security policies. The editing, deleting, and duplicating operations for cookie security policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a cookie security policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Advanced Protection > Cookie Security**.

Figure 4-90 Cookie Security page

Cookie Security						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
+	default_medium	Standard policy	Yes	Clear	Unblock	 
+	default_high	Strict policy	Yes	Clear	Unblock	 

Step 2 Click **Create**.

Figure 4-91 Creating a cookie security policy

Step 3 In the dialog box, set the parameters.

Table 4-29 Parameters for creating a cookie security policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	<p>Specifies the action WAF will take on a matched request. Actions include the following:</p> <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks. Accept: WAF ends the check against the current policy but will still check such request against other policies. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.

Parameter	Description
	<ul style="list-style-type: none"> • Clear: Upon detection of illegal cookies, WAF removes them and then sends data to servers, instead of blocking the HTTP sessions.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Host Name	Name of a protected host.
Enable HTTPOnly	Controls whether to enable the HTTP only feature. If yes, cookies are available to web browsers (IE, Firefox, and chrome), and but not to client-end scripts, better preventing cookies from being stolen.
Protection Algorithm	Cookie security protection algorithm, which can be Cookie Encryption or Cookie Signature .
Enable Source IP Validation	Controls whether to enable source IP address validation. Valid client IP addresses (source IP addresses) are used as part of the cookie encryption or signature algorithm. After receiving encrypted or signed cookies, WAF considers them valid only if they are from the same source IP addresses. This can prevent cookie stealing and resulting session support, thus better protecting cookie security.
Cookie Compatibility Time	<p>Cookie compatibility time. Before a cookie security policy is enabled, unencrypted or unsigned cookies may exist in web clients. After a cookie security policy is enabled, to ensure WAF's compatibility with cookies before the policy is enabled, WAF provides the Cookie Compatibility Time option. Before the specified time expires, WAF performs the following operations:</p> <ul style="list-style-type: none"> • For cookies delivered from the server, WAF signs or encrypts them as defined in the cookie security policy. • For cookies received from clients, WAF attempts to decrypt them or validate their signatures. If a cookie is properly encrypted or signed, WAF decrypts or unsigns it and sends it to the server. If a cookie is not encrypted or signed, WAF leaves it unchanged.
Cookie Name	Names of cookies to be protected. Multiple cookie names can be specified with each taking up one line.

Step 4 Click **OK** to save the settings.

----End

4.7.3.5 Content Filtering Policy

On the **Content Filtering** page, you can create, edit, delete, and duplicate content filtering policies. The following only describes how to create content filtering policies. The editing, deleting, and duplicating operations for content filtering policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a content filtering policy, perform the following steps:

- Step 1** Choose **Security Management > Policy Management > Advanced Protection > Content Filtering**.

Figure 4-92 Content Filtering page

Content Filtering					
					Create
	Name	Description	Alert or Not	Action	Operation
+	default_high	Strict policy	Yes	Block	 

- Step 2** Click **Create**.

Figure 4-93 Creating a content filtering policy

Create Content Filtering

Basic Information

Name

* The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Block

Rule Information

Matching Principle

☒ Stop upon a match ☐ Continue upon a match

Rule Filtering

Rule List

View All

☒ Content Filtering

OK

Reset

Cancel

- Step 3** In the dialog box, set the parameters.

Table 4-30 Parameters for creating a content filtering policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Redirection Path	Redirection URL. This parameter is required if Action is set to Redirection .
Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Matching Principle	Controls whether WAF continues to match a packet that has matched a rule in a policy to match other rules in the policy. <ul style="list-style-type: none"> • Stop upon a match: WAF stops matching the packet against other rules in the policy. • Continue upon a match: WAF continues to match the packet against other rules in the policy.
Rule Filtering	Rule filtering conditions. You can filter the rule list below based on the rule type, ID, severity, name, and one or more conditions selected from the Accuracy drop-down list. After specifying conditions, click Filter . Qualified rules will be displayed in the rule list.
Rule List	Rule lists. To add a rule into the rule set, just select the check box of the rule. At least one rule should be selected.

Step 4 Click **OK** to save the settings.

----End

4.7.3.6 Sensitive Information Filtering Policy

Sensitive information filtering policies are to filter specified sensitive information, such as identity card numbers and social security card numbers, block access to such sensitive information, or replace the sensitive information with specified characters, thereby avoiding user privacy leakage.

On the **Sensitive Information Filtering** page, you can create, edit, delete, and duplicate sensitive information filtering policies. The following describes how to create sensitive information filtering policies. The editing, deleting, and duplicating operations for sensitive information filtering policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a sensitive information policy, perform the following steps:

- Step 1** Choose **Security Management > Policy Management > Advanced Protection > Sensitive Information Filtering**.

Figure 4-94 Sensitive Information Filtering page

Sensitive Information Filtering					
					Create
	Name	Description	Alert or Not	Action	Operation
	default	default	Yes	Replace	

- Step 2** Click **Create** in the lower-right corner.

Figure 4-95 Creating a sensitive information policy

Create Sensitive Information Filtering

Basic Information

Name

* The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Replace

Replacement Method

Retain the pattern's first 0 and last 0 characters and replace each of the other characters with *

* The number of characters must be 0 or a positive integer

Rule Information

Matching Principle

☐ Stop upon a match ☒ Continue upon a match

Rule Filtering

Rule List

View All

☒ Sensitive Information Filtering

OK

Reset

Cancel

- Step 3** In the dialog box, set the parameters.

Table 4-31 Parameters for creating a sensitive information filtering policy.

Parameter	Description.
Name	Specifies the name of the sensitive information filtering policy.
Description.	Brief description of the sensitive information filtering policy.
Alert or Not	Control whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Block: WAF ends the current check and tears down the current TCP connection. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Replace: WAF replaces hit pattern characters in the matching request with specified characters and then ends the check against the current policy. Still, this request will be subject to other checks.
Replacement Method	This parameter is required if Action is set to Replace . The first n characters will be retained before and after match, and other characters will be replaced by the user with English characters or digits.
Matching Principle	This parameter has the following values: <ul style="list-style-type: none"> • Stop upon match means to stop matching after a rule is correctly matched; • Continue upon match means to continue matching after a rule is correctly matched; • If Action is set to Replace, only Continue upon match is available. If Action is set to Pass, Block, or Accept, both Stop upon match and Continue upon match are available.
Rule Filtering	Rule filtering conditions. You can filter the rule list below based on the rule type, ID, severity, name, and one or more conditions selected from the Accuracy drop-down list. After specifying conditions, click Filter . Qualified rules will be displayed in the rule list.
Rule List	At least one list rule should be selected. To add a rule into a rule set, select the check box before the rule.

Step 4 Click **OK** to save the settings.

----End

4.7.3.7 Brute Force Protection Policy

Brute-force guessing is an attack whereby an attacker collects user names and passwords disclosed on the Internet to generate a dictionary before checking these user names and passwords until the correct ones are found.

The main function of a brute force protection policy is to check whether a user attempts to hack a database by means of brute-force guessing. This can prevent attackers from stealing user information from a known database.

WAF relies on statistical inspection for brute force protection. A normal user does not submit login verification requests repeatedly in a very short time. If the login verification request is

submitted repeatedly, it is possible that a user attempts automatic login by using a tool or script. Therefore, WAF determines that a brute force attack exists.

If verification code is used to verify users, WAF, after the number of received verification requests exceeds the specified threshold during a detection threshold, returns a verification page, showing verification code for the user to type. The user can continue the requesting of the target URL only after correct code is typed; otherwise, WAF still sends a verification page, asking the user to type the verification code.

For brute force protection policies, WAF uses the statistics inspection method by default. You can determine whether to enable verification based on the verification code.




In mirroring mode, WAF only supports HTTP traffic checking, but does not support HTTPS traffic checking.

On the **Brute Force Filtering** page, you can create, edit, delete, and duplicate brute force filtering policies. The following describes how to create brute force filtering policies. The editing, deleting, and duplicating operations for sensitive information filtering policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a brute force protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Advanced Protection > Brute Force Protection**.

Figure 4-96 Brute Force Protection page

Name	Description	Alert or Not	Action	Source IP Blocking	Operation
 No data					

Step 2 Click **Create** in the upper-right corner.

Figure 4-97 Creating a brute force protection policy

Create Brute Force Protection

Basic Information

Name * The name length should not exceed 50 characters

Description The description content should not exceed 200 characters.

Alert or Not ☒ Yes ☐ No

Action ?

Source IP Blocking

Protection Information

Protected URL * ?	Request Threshold *	Detection Cycle (min) *	
<input type="text"/>	<input type="text" value="30"/>	<input type="text" value="5"/>	

OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-32 Parameters for creating a brute force protection policy

Parameter		Description
Basic Information	Name	Name of the new policy, which cannot be over 50 characters long.
	Description	Brief description of the new policy.
	Alert or Not	Controls whether to alert users when this policy is triggered.

Parameter		Description
	Action	<p>Specifies the action that WAF will take on a matched request. Actions include the following:</p> <ul style="list-style-type: none"> • Pass: WAF directly forwards such request to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. After selecting this action, you need to further set Redirection Path. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection. After selecting this action, you need to further set Response Code and Response File. You can select an existing response file or upload a response file. • Verification Code: WAF responds to the client with a verification code for a matched request.
	Source IP Blocking	<p>This is mandatory if you select Block for Action.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the related source IP address. • Permanently block: WAF permanently blocks the related source IP address. • Block as customized: WAF blocks the related source IP address for a specified period, which can be set to a value in seconds, minutes, or hours.
	Redirection Path	Specifies the redirection URL. This parameter is mandatory if Action is set to Redirection .
	Response Code	Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
	Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Protection Information	Protected URL	Specifies the login URL, which is the actual URL of the page requested by the browser from the server when a user types the user name and password and then clicks Login .
	Requested Threshold	Specifies the maximum allowed number of login attempts using the GET or POST method in a single inspection cycle. The value range is 1–300, with 30 as the default.
	Detection Cycle (min)	Specifies the length of a single inspection cycle. The value range is 1–360 minutes, with 5 as the default.
	Login Verification Mode	<p>Specifies the method by which the server verifies login requests from clients. Options include Form, Ajax, and Jsonp.</p> <p>This parameter is required when Action is set to Verification Code.</p>
	Login Referer	<p>Specifies the referer URL carried in the request submitted.</p> <p>This parameter is required when Action is set to Verification Code.</p>

Step 4 Click **OK** to save the settings.

----End

4.7.3.8 XML Attack Protection Policy

WAF implements XML attack protection by means of the following validation schemes:

- **Basic XML validation**
By validating basic elements of an XML document, WAF determines whether an XML attack is in process. Basic elements include the tree depth, number of elements, attributes, Unparsed Character Data (CDATA, indicating text data not parsed by the XML parser), and document type definitions (DTDs).
- **Schema validation**
WAF implements validation by checking an XML document to see whether it conforms to a specified XML schema, thereby determining whether an XML attack is in process.
An XML schema describes the structure of a type of XML documents. It defines elements and attributes that may appear in a document, child elements, number and sequence of child elements, whether an element is empty, data type of elements and attributes, and default and fixed values of elements or attributes.
- **SOAP validation**
SOAP validation means that WAF uses the Web Services Description Language (WSDL) to validate Simple Object Access Protocol (SOAP) messages before a web service is deployed, thereby eliminating the risk of XML attacks.
SOAP, WSDL, and Universal Description Discovery and Integration (UDDI) are the three elements of web services. SOAP describes the format of messages that are exchanged, WSDL describes how to access a specific interface, and UDDI is used to manage, distribute, and query web services.

On the **XML Attack Protection** page, you can create, edit, delete, and duplicate XML attack protection policies. The following describes how to create an XML protection policy. The editing, deleting, and duplicating operations for XML protection policies are the same as those for HTTP validation policies. For details, see related descriptions in section [4.7.1 HTTP Validation Policies](#).

To create an XML attack protection policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Advanced Protection > XML Attack Protection**.

Figure 4-98 XML Attack Protection page

XML Attack Protection						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
	default	default	Yes	Block	Unblock	
	XMLAttackProtection		Yes	Block	Unblock	

Step 2 Click **Create** in the upper-right corner.

Figure 4-99 Creating an XML attack protection policy

Create XML Attack Protection

Basic Information

Name: * The name length should not exceed 50 characters

Description: The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: ?

Source IP Blocking:

Inspection Item

Basic XML Validation: ☒ Yes ☐ No

Schema Validation

SOAP Validation

Enable Basic XML Validation: ☒ Yes ☐ No

Max Tree Depth	<input type="text" value="20"/>
Max Element Name Length	<input type="text" value="64"/>
Max Number of Elements	<input type="text" value="10000"/>
Max Number of Child Nodes	<input type="text" value="100"/>

OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-33 Parameters for creating an XML attack protection policy

Parameter		Description
Basic Information	Name	Name of the new policy, which cannot be over 50 characters long.
	Description	Description of the new policy.
	Alert or Not	Controls whether to alert users when this policy is triggered.
	Action	Specifies the action that WAF will take on a matched request. Actions include the following: <ul style="list-style-type: none"> Pass: WAF directly forwards such request to the server without any more security checks. Accept: WAF ends the check against the current policy but will still check such request against other policies. Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. After selecting this action, you need to further set Redirection Path.

Parameter			Description
			<ul style="list-style-type: none"> Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection. After selecting this action, you need to further set Response Code and Response File. For the latter, you can select an existing response file or upload a response file.
	Source IP Blocking		<p>Specifies whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block.</p> <ul style="list-style-type: none"> Unblock: WAF does not block the source IP address. Permanently block: WAF permanently blocks the source IP address. Block as customized: WAF blocks the source IP address for a specified period, which can be set to a value in seconds, minutes, or hours.
	Redirection Path		Specifies the redirection URL. This parameter is mandatory if Action is set to Redirection .
	Response Code		Specifies an HTTP response code. This parameter is mandatory if you select Disguise for Action .
	Response File		Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Inspection Item	Basic XML validation	Enable Basic XML validation	Controls whether to enable basic XML validation. For the selection of Yes , you need to further configure the following parameters.
		Max Tree Depth	Maximum depth of the XML tree structure.
		Max Element Name Length	Maximum length of an XML element name.
		Max Number of Elements	Maximum number of XML elements.
		Max Number of Child Nodes	Maximum number of child nodes that an XML node can contain.
		Max Number of Attributes	Maximum number of attributes that an XML element can contain.
		Max Attribute Name Length	Maximum attribute length of an XML element.
		Max Attribute Value Length	Maximum attribute value length of an XML element.
		Max CDATA Length	Maximum length of CDATA in an XML document.
		Max File Size	Maximum number of bytes in an XML document.
		Min File Size	Minimum number of bytes in an XML document.
		Exclude	Controls whether to forbid XML documents to contain processing directives. By default, this option

Parameter			Description
		Processing Directives	is enabled.
		Exclude DTDs	Controls whether to forbid XML documents to contain DTDs. By default, this option is enabled.
		Exclude External Entities	Controls whether to forbid XML documents to reference external entities. By default, this option is enabled.
	Schema Validation	Enable Schema Validation	Controls whether to enable schema validation. If it is enabled, you can configure up to 10 groups of schema validation parameters, each of which consists of Schema File and Target URL .
		Schema File	Indicates an XML Schema Definition (XSD) file. You can select an existing file or upload such a file from the local disk drive. For each group of validation parameters, you can select or upload only one schema file. Different groups must use different schema files. For how to manage XSD files, see section 4.12.2 XSD/WSDL File Management .
		Target URL	For each schema file, you can configure up to 10 target URLs. WAF will implement schema validation only for XML traffic destined for the target URLs. Note the following when entering target URLs: <ul style="list-style-type: none"> • Wildcard characters are not supported. • URL format: host + URI path + query string. • "http://" can be omitted as it will be automatically added in the background. • By default, only HTTP is supported. If you want to type an HTTPS URL, you must add "https://" in the input box. • The maximum length of a URL is 2048 characters.
	SOAP Validation	Enable SOAP Validation	Controls whether to enable SOAP validation. If it is enabled, you can configure up to 10 groups of SOAP validation parameters, each of which consists of WSDL File and Target URL .
		WSDL File	You can select an existing file or upload such a file from the local disk drive. For each group of validation parameters, you can select or upload only one WSDL file. Different groups must use different WSDL files. For how to manage WSDL files, see section 4.12.2 XSD/WSDL File Management .
		Target URL	For each WSDL file, you can configure up to 10 target URLs. Entering target URLs should conform to the same requirements as those for schema validation.

Step 4 Click **OK** to save the settings.

----End

4.7.3.9 Smart Engine Inspection

Smart engines are a new generation of web attack detection engines based on machine learning. Built on traditional rule detection, smart engine inspection policies introduce semantic analysis and statistical algorithms, delivering a higher detection rate and a lower false positive rate. Currently, the smart engine inspection of WAF can work on cross-site scripting (XSS), SQL injection, command line injection, and path traversal attacks.

On the **Smart Engine Inspection** page, you can create, edit, delete, and duplicate smart engine inspection policies. The following describes how to create a smart engine inspection policy. The editing, deleting, and duplicating operations for smart engine inspection policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a smart engine inspection policy, follow these steps:

- Step 1** Choose **Security Management > Policy Management > Advanced Protection > Smart Engine Inspection**.

Figure 4-100 Smart Engine Inspection page

Smart Engine Inspection						
						Create
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
	default		Yes	Block	Unblock	 

- Step 2** Click **Create** in the upper-right corner of the page.

Figure 4-101 Creating a smart engine inspection policy

Step 3 Configure parameters in the dialog box.

Table 4-34 Parameters for configuring a smart engine inspection policy

Parameter	Description
Name	Name of the smart engine inspection policy.
Description	Brief description of the smart engine inspection policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies how WAF acts on a packet matching this policy. The value can be one of the following: <ul style="list-style-type: none"> Pass: WAF directly forwards the matching packet without any more security detection. Block: WAF completes the current detection and disconnects the current TCP connection. Accept: WAF completes the current detection and continues with other security detections on matching packets. Redirection: WAF constructs a 302 redirect page to respond to the client and disconnect the current TCP connection. Disguise: WAF responds to the client with customized HTTP response code and response file contents, and disconnects the current TCP connection.
Source IP Blocking	Controls whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block . <ul style="list-style-type: none"> Unblock: WAF does not block the related source IP address. Permanently block: WAF permanently blocks the related source IP address.

Parameter	Description
	<ul style="list-style-type: none"> Block as customized: WAF blocks the source IP address for a specified period, which can be set to a value in seconds, minutes, or hours.
Redirection Path	Specifies the redirection URL. This parameter is mandatory if Action is set to Redirection .
Response Code	Specifies a custom response code. This parameter is required if Action is set to Disguise .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory if you select Disguise for Action .
Attack	Specifies the type of attacks that can be inspected by this policy, which can be Cross-Site Scripting Attack , or SQL Injection Attack , Command Line Injection Attack , and/or Path Traversal Attack .
Content	Specifies the contents that can be inspected by this policy, which can be URI , Parameter , or Cookie .


Step 4 Click **OK** to save the settings.

----End

4.7.4 Precise Protection Policy

WAF features precise protection. Based on auto-learning policies, WAF generates auto-learning results that record the actual traffic statistics of the protected server. By using auto-learning results, you can configure precise protection policies for refined protection.




On the **Whitelist** page, you can create, edit, delete, and duplicate whitelist policies. The following only describes how to create whitelist policies. The editing, deleting, and duplicating operations for whitelist policies are the same as those for HTTP validation policies. For details, see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

 Note	Precise protection policies do not work on WAF in mirroring mode.
--	---

To create a whitelist policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Precise Protection > Whitelist**.

Figure 4-102 Whitelist page

Whitelist Create						
	Name	Description	Alert or Not	Action	Source IP Blocking	Operation
	Whitelist		Yes	Disguise(default.html)	Unblock	 

Step 2 Click Create.

Figure 4-103 Creating a whitelist

Create Whitelist

Basic Information

Name

* The name length should not exceed 50 characters

Description

The description content should not exceed 200 characters.

Alert or Not

☒ Yes ☐ No

Action

Disguise

Response Code

403(Forbidden)

Response File

☒ Select an Existing Response File ☐ Upload Response File

default1.html

Optional Learning Result Object

No available learning result

Submit

Reset

Cancel

Step 3 In the dialog box, set the parameters.

Table 4-35 Parameters for creating a whitelist policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	<p>Specifies the action WAF will take on a matched request. Actions include the following:</p> <ul style="list-style-type: none"> Pass: WAF directly forwards such packet to the server without any more security checks.

Parameter	Description
	<ul style="list-style-type: none"> • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this new policy. This parameter needs to be set only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter needs to be set only when Action is set to Redirection .
Optional Learning Result Object	<p>Auto-learning objects that can be selected. Optional learning result objects are URLs for whom the auto learning process is completed</p> <p>If a website has too deep a directory structure or a directory has too many sub-directories, you are not advised to select the whole website or directory, because it may cause slow browser response.</p>

Step 4 Click **Submit** to save the settings.

----End

4.7.5 Other Protection Policies

Other policies include exception policies, custom policies, and risk level policies. The following describes how to manage the three types of policies.

4.7.5.1 Exception Policy

Exception policies are supplements or restrictions to configured basic or advanced protection policies.

On the **Exception Policy** page, you can create, edit, delete, and duplicate exception policies. The following only describes how to create exception policies. The editing, deleting, and duplicating operations for exception policies are the same as those for HTTP validation policies. see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create an exception policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Others > Exception Policy**.


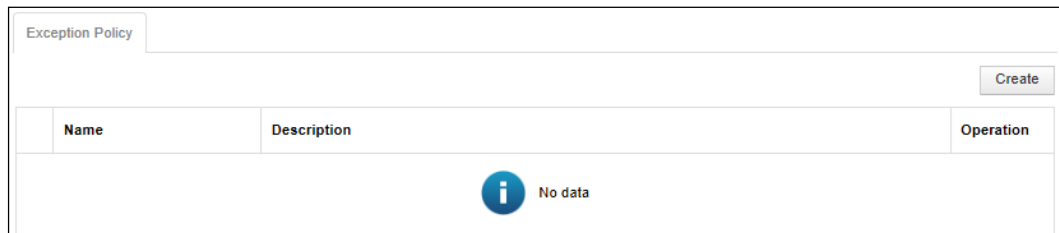

 Note	<p>You can create and edit exception policies on the Website Protection page. For details, see Exception Control Policy in section 4.3.2.4 Configuring Website Security Policies.</p>
--	--

Figure 4-104 Exception Policy page

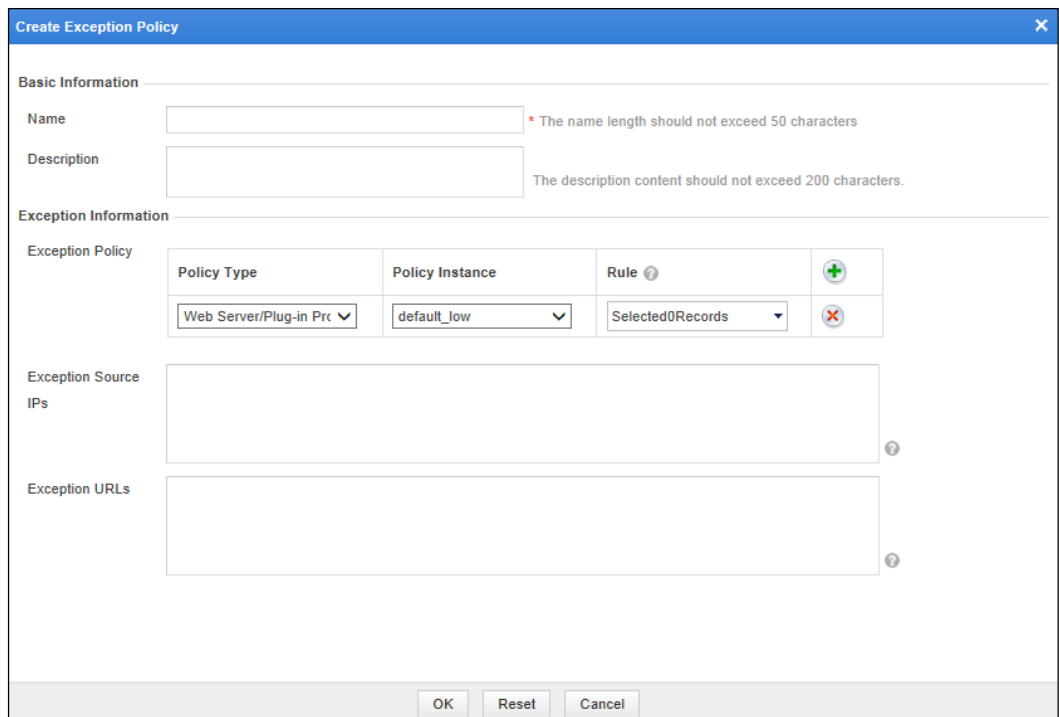


Name	Description	Operation
 No data		

Step 2 Click **Create**.

You can configure exception policies for multiple policies at the same time.

Figure 4-105 Creating an exception policy



Create Exception Policy

Basic Information

Name

Description

Exception Information

Exception Policy

Policy Type

Policy Instance

Rule ?

+

Web Server/Plug-in Prc

default_low

Selected0Records

-

Exception Source IPs

Exception URLs

OK

Reset

Cancel


Step 3 In the dialog box, set the parameters.

Copyright © NSFOCUS

165

V6.0R07F03 (2020-6-10)

Table 4-36 Parameters for creating an exception policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Exception Information	
Policy Type	Type of the target policy.
Policy Instance	Target policy instance.
Rule	<p>Target rule instance.</p>  <p>Note</p> <ul style="list-style-type: none"> If no rule set exists under the protection policy, the system displays "No rule". In this case, WAF adds the selected policy instance to the new risk level policy. If a rule set exists under the policy: <ol style="list-style-type: none"> If no rule is selected, WAF also adds the selected policy instance to the new risk level policy. If a rule is selected, WAF adds only this rule to the new rule level policy.
Exception Source IPs	<p>Specifies source IP addresses to which the new policy applies. You can enter a single IP address (such as 10.66.9.1) or an IP address range (such as 192.168.1.1-192.168.1.255).</p> <p>Leaving it empty means that the new policy applies to all IP addresses.</p>
Exception URLs	<p>Specifies URLs to which the new policy applies.</p> <p>Each URL takes up one line, in the format of [\$]domain name[:port]/path/file. A URL starting with \$ indicates matching based on regular expression. A URL not starting with \$ indicates exact match.</p> <p>Examples:</p> <ul style="list-style-type: none"> www.example1.com:8080/login.jsp \$www\.example2\.com:80/* <p>Leaving it empty means that the new policy applies to all URLs.</p>

Step 4 Click **OK** to save the settings.

----End

4.7.5.2 Custom Policies

You can customize protection policies by referencing multiple built-in or custom rules, thereby implementing multi-angle network security protection.

On the **Custom Policy** page, you can create, edit, delete, and duplicate custom policies. The following only describes how to create custom policies. The editing, deleting, and duplicating operations for custom policies are the same as those for HTTP validation policies. see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a custom policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Others > Custom Policy**.

Figure 4-106 Custom Policy page

Name	Description	Alert or Not	Action	Source IP Blocking	Operation
No data					

Step 2 Click **Create**.

Figure 4-107 Creating a custom policy

Step 3 In the dialog box, set the parameters.

Table 4-37 Parameters for creating a custom policy

Parameter	Description
Name	Name of the new policy.
Description	Brief description of the new policy.
Alert or Not	Controls whether to generate alert logs.
Action	Specifies the action WAF will take on a matched request. Actions include the following:

Parameter	Description
	<ul style="list-style-type: none"> • Pass: WAF directly forwards such packet to the server without any more security checks. • Accept: WAF ends the check against the current policy but will still check such request against other policies. • Block: WAF ends the current check and tears down the current TCP connection. After selecting this action, you need to further set Source IP Blocking. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Specifies whether to block the source IP address of a packet that matches this new policy. This parameter is available only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the source IP address. • Permanently block: WAF permanently blocks the source IP address. • Block as customized: WAF blocks the source IP address in the customized period. You can customize the period to seconds, minutes, and hours.
Redirection Path	Redirection URL. This parameter is required if Action is set to Redirection .
Matching Principle	<p>Controls whether WAF continues to match a packet that has matched a rule in a policy against other rules in the policy.</p> <ul style="list-style-type: none"> • Stop upon a match: WAF stops matching the packet against other rules in the policy. • Continue upon a match: WAF continues to match the packet against other rules in the policy.
Rule Filtering	Rule filtering conditions. You can filter the rule list below based on the rule type, ID, and/or name. After specifying conditions, click Filter . Qualified rules will be displayed in the rule list.
Rule List	Rule lists. To add a rule into the rule set, just select the check box of the rule. At least one rule should be selected.

Step 4 Click **OK** to save the settings.

----End

4.7.5.3 Risk Level Policy

A risk level policy customizes risk levels of protection policies so as to protect websites based on risk levels.

WAF can read and save risk level policies you have configured. In addition, it can check HTTP requests from clients based on such policies and determine whether these requests fall within the custom risk level set.

- If yes, WAF returns the user-defined risk level.
- If no, WAF returns nothing and logs such events with the original alert level.

On the **Risk Level Policy** page, you can create, edit, delete, and duplicate risk level policies. The following describes how to create a risk level policy. The editing, deleting, and

duplicating operations for risk level policies are the same as those for HTTP validation policies. see related descriptions of HTTP validation policies in section [4.7.1 HTTP Validation Policies](#).

To create a risk level policy, perform the following steps:

Step 1 Choose **Security Management > Policy Management > Others > Risk Level Policy**.

Figure 4-108 Risk Level Policy page

Name	Description	Risk Level	Operation
No data			

Step 2 Click **Create** in the upper-right corner.

Figure 4-109 Creating a risk level policy

Create Risk Level Policy

Basic Information

Name: * The name length should not exceed 50 characters

Description: The description content should not exceed 200 characters.

Risk Level: High

Risk Level Info

Policy Type	Policy Instance	Rule
HTTP Validation	default_low	No rule

Source IP:




URL:

OK Reset Cancel

Step 3 In the dialog box, set the parameters.

Table 4-38 Parameters for creating a risk level policy

Parameter	Description
Name	Name of the new policy.

Parameter	Description
Description	Brief description of the new policy.
Risk Level	Risk level of the new policy. The values include High , Medium , and Low .
Risk Level Info	
Risk Level Policy	<p>Specifies the type, instance, and rules of the new policy. You can click  to create more policies or click  to delete policies.</p> <ul style="list-style-type: none"> Policy Type: You can select a policy type from the drop-down list. Policy Instance: You can select a policy instance for the selected policy type from the drop-down list. Rule: You can select rules for the selected policy type from the drop-down list. <p> Note</p> <ul style="list-style-type: none"> If no rule set exists under the protection policy, the system displays "No rule". In this case, WAF adds this policy instance to the new risk level policy. If a rule set exists under the policy: <ol style="list-style-type: none"> If no rule is selected, WAF also adds the selected policy instance to the new risk level policy. If a rule is selected, WAF adds only this rule to the new rule level policy.
Source IP	<p>Specifies IP addresses of HTTP requests to which this new policy applies. You can type a single IP address (such as 10.66.9.1) or an IP address range (such as 192.168.1.1-192.168.1.255).</p> <p>Leaving it empty means that the new policy applies to all IP addresses.</p>
URL	<p>Specifies URLs to which this new policy applies.</p> <p>Each URL takes up one line, in the format of [\$]domain name[:port]/path/file. A URL starting with \$ indicates matching based on regular expressions. A URL without \$ indicates exact match.</p> <p>Examples: www.example1.com:8080/login.jsp, \$www.example2.com:80/*</p> <p>Leaving it empty indicates that the policy applies to all URLs.</p>

Step 4 Click **OK** to save the settings.

----End

4.8 Template Management

WAF provides three types of policy templates. You only need to create a policy template and select policies of different levels and then apply the policies to the website for protection. Three levels of default policies are available on WAF:

- default_low (loose policy template): enables the most needed policies and prevents high-risk vulnerabilities only, with a low probability of false positives but a limited protection effect.

- default_medium (standard policy template): enables all necessary policies and rules, to achieve a balance between the protection effect and the probability of false positives. (Recommended)
- default_high (strict policy template): enables all rules and protection methods, with a good protection effect but a high probability of false positives.

Templates can be divided into website templates and virtual website templates.

4.8.1 Website Template

Choose **Security Management > Template Management**.







The **Website Template** page appears, as shown in [Figure 4-110](#).

Figure 4-110 Website Management page

Website Template

Virtual Website Template

Create

No.	Name	Description	Operation	
	1	default_low	Loose policy template: enables the most needed policies and prevents high-risk vulnerabilities only, with a low probability of false positives but a limited protection effect.	
	2	default_medium	Standard policy template: enables all necessary policies and rules, to achieve a balance between the protection effect and the probability of false positives. (Recommended)	
	3	default_high	Strict policy template: enables all rules and protection methods, with a good protection effect but a high probability of false positives.	

Creating a Website Template




To create a website template, perform the following steps:

Step 1 Click **Create** in the lower-right corner of the **Website Template** page.

Figure 4-111 Creating a website template

Step 2 In the dialog box, set the parameters.

Table 4-39 Parameters for creating a website template

Parameter	Description.
Name	Name of the website template.
Description.	Brief description of the website template.
Selecting Policy	<p>Specifies policies for website protection. You can select a policy from the drop-down list.</p> <p> Note</p> <ul style="list-style-type: none"> WAF matches traffic against the policies in a top-down manner. You can click  or  to move a policy template up or down. Alternatively, you can click Create Policy to create a policy.




Step 3 Click **OK** to save the settings.

----End

Other Operations

After a website template is configured, you can select this website template when configuring web security protection for websites. For details, see [Web Security Protection Policy](#) in section 4.3.2.4 [Configuring Website Security Policies](#).

On the **Website Template** page shown in [Figure 4-110](#), you can also perform the following operations:

- Viewing templates: Clicking  displays template details. Template details are available only for built-in website templates.
- Editing templates: You can click  and then edit a website template. Only the website templates created by the administrator can be edited.
- Deleting templates: You can click  to delete a website template. Only the website templates created by the administrator can be deleted.

4.8.2 Virtual Website Template







Choose **Security Management > Template Management > Virtual Website Template**.

Figure 4-112 Virtual Website Template page

Website Template

Virtual Website Template

Create

	No.	Name	Description	Operation
	1	default_low	Loose policy template: enables the most needed policies and prevents high-risk vulnerabilities only, with a low probability of false positives but a limited protection effect.	
	2	default_medium	Standard policy template: enables all necessary policies and rules, to achieve a balance between the protection effect and the probability of false positives. (Recommended)	
	3	default_high	Strict policy template: enables all rules and protection methods, with a good protection effect but a high probability of false positives.	

Creating a Virtual Website Template

To create a virtual website template, perform the following steps:

- Step 1** Click **Create** in the lower-right corner of the **Website Management** page shown in [Figure 4-112](#).

Figure 4-113 Creating a virtual website template

Create Virtual Website Template

Name *

Description The description content should not exceed 200 characters.

Protocol Validation

HTTP Validation

Basic Protection

Web Server/Plug-in Protection

Crawler Protection

Common Web Protection

Illegal Upload Restriction

Illegal Download Restriction

Information Disclosure Protection

OK Cancel

Step 2 In the dialog box, set the parameters.

Table 4-40 Parameters for creating a virtual website template

Parameter	Description.
Name	Name of the new template.
Description.	Brief description of the new template.
Selecting Policy	<p>Specifies policies for protection. You can select a policy from the drop-down list.</p> <p> Note</p> <ul style="list-style-type: none"> WAF matches traffic against the policies in a top-down manner. You can click or to move a policy template up or down. Alternatively, you can click Create Policy to create a policy.




Step 3 Click **OK** to complete the settings.

----End

Other Operations

After a virtual website template is configured, you can select this website template when configuring web security protection for virtual websites. For details, see section [4.3.3.3 Configuring a Virtual Website](#).

On the **Virtual Website Template** page shown in [Figure 4-112](#), you can also perform the following operations:

- Viewing templates: Clicking  displays template details. Template details are available only for built-in virtual website templates.
- Editing templates: You can click  and then edit a virtual website template. Only the virtual website templates created by the administrator can be edited.
- Deleting templates: You can click  to delete a virtual website template. Only the website virtual templates created by the administrator can be deleted.

4.9 Smart Patching

Smart patching does not work on WAF in mirroring mode and only users who have acquired the smart patch module can use this function.

The smart patching function of WAF is implemented in two ways: cloud-based scanning and vulnerability scanning report import. The following describes the principles and procedures of the two ways.

Cloud-based Scanning

WAF has a unique "vulnerability perspective" and automatically provides patch packages based on detected vulnerabilities. As shown in [Figure 4-114](#), through third-party cloud-based scanning, WAF obtains the web vulnerability scanning report of a customer's network system, and generates security policies specific to the vulnerabilities. In this manner, you can configure better security policies to ensure in-depth network protection.

Figure 4-114 Deployment topology — smart patching function via cloud-based scanning

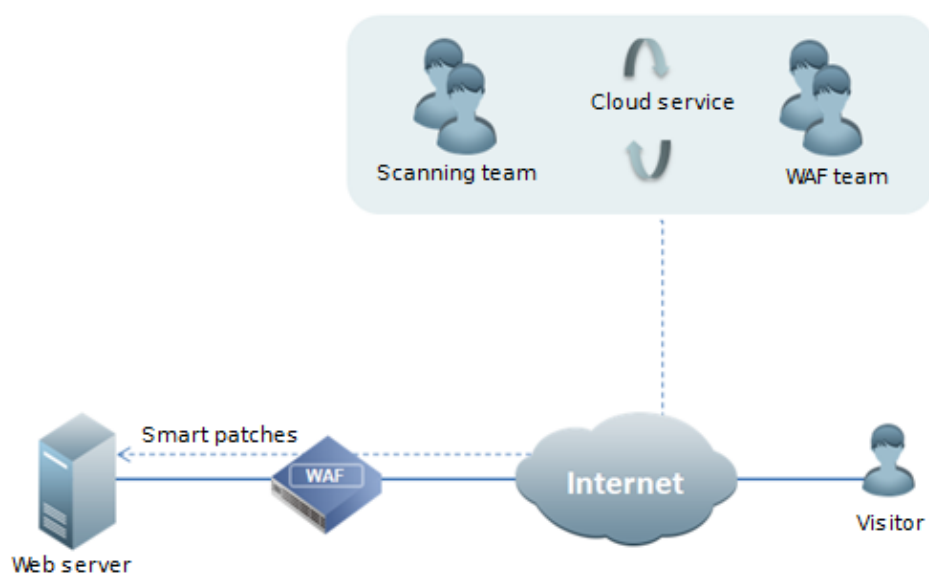
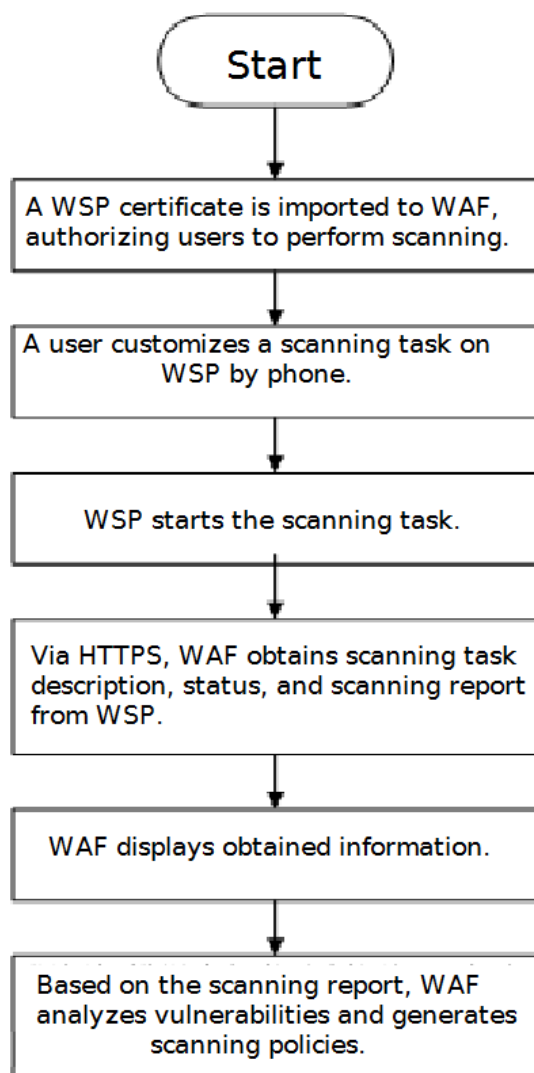


Figure 4-115 shows the procedure of smart patching via cloud-based scanning.

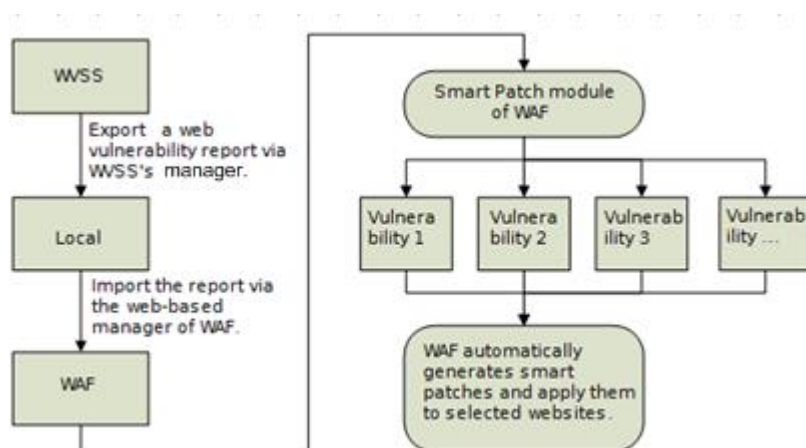
Figure 4-115 Procedure of smart patching via cloud-based scanning



Vulnerability Scanning Report Import

WAF also supports the import of web vulnerability scanning reports. Currently, only web vulnerability scanning reports exported from NSFOCUS WVSS can be imported. After importing a web vulnerability scanning report, by using the automatic smart patch module, WAF can generate accurate protection policies specific to web vulnerabilities in the report and integrate the policies into the WAF protection system, thus protecting customer websites from existing web vulnerabilities in real time. [Figure 4-116](#) shows the procedure of the smart patching function via imported vulnerability scanning report.

Figure 4-116 Procedure of the smart patching function via imported vulnerability scanning report



4.9.1 Configuring the SAAS Scanning Service

After customizing a scanning task by phone and obtaining the scanning IP address, you also need to perform the following steps on WAF:

Step 1 Set scanning configurations.

- a. Choose **Security Management > Smart Patch > SAAS Scan Config**. On the **SAAS Scan Config** page that appears, enable **Communication with the SaaS Scanning Service** and set **Penetration Scanning IP** or **Protection Scanning IP**. See [Figure 4-117](#).

Figure 4-117 SAAS Scan Config page

WAF	
System Monitoring	Security Management
Logs & Reports	System Management
Network-Layer Protection	Website Protection
Auto-Learning Policies	Auto-Learning Results
Rule Database Management	Policy Management
Template Management	Smart Patch
SAAS Scan Config	WVSS Scan Config
Scanning File Management	Patch Management
Authorization Information	Valid license Details
Service Running Status	Disabled
Communication with the SAAS Scanning Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Penetration Scanning IP	211.99.227.140
Protection Scanning IP	211.99.227.138
OK Reset	

- b. Set the parameters.

Table 4-41 Parameters for configuring SAAS scanning settings

Parameter	Description
Authorization Information	License for the smart patch module. You can click Details to open the license management page.
Service Running Status	Status of the cloud-based scanning service.
Communication with the SaaS Scanning Service	Controls whether to enable the communication with the SaaS scanning service. To set scanning configurations, it must be set to Enable .

Parameter	Description
Penetration Scanning IP	IP address of penetration scanning. WAF does not perform protection against penetration scanning. Penetration scanning penetrates WAF to detect web application vulnerabilities. Both IPv4 and IPv6 addresses are supported.
Protection Scanning IP	IP address of protection scanning. Protection scanning is used to verify the smart patch's effect on vulnerability protection. In this mode, cloud scanning goes through (not penetrate) WAF security policies. Both IPv4 and IPv6 addresses are supported.

Step 2 Configure communication interfaces for scanning.

- a. Choose **System Management > Network Configuration > DNS Configuration**.

Figure 4-118 DNS Configuration page

The screenshot shows the 'DNS Configuration' page. At the top, there are tabs for 'Network Configuration', 'System Deployment', 'System Tools', 'Test Tools', 'ESPC', and 'User Management'. Below these are sub-tabs for 'Work Group Management', 'Route Configuration', and 'DNS Configuration'. The 'DNS Server Configuration' section contains four input fields: 'IPv4 Preferred DNS Server' (8.8.8.8), 'IPv4 Alternate DNS Server' (114.114.114.114), 'IPv6 Preferred DNS Server', and 'IPv6 Alternate DNS Server'. An 'OK' button is below these fields. The 'Customized Domain Name' section has an 'Add' button. Below this is a table with columns: ID, Domain Name, IP Address, and Operation.

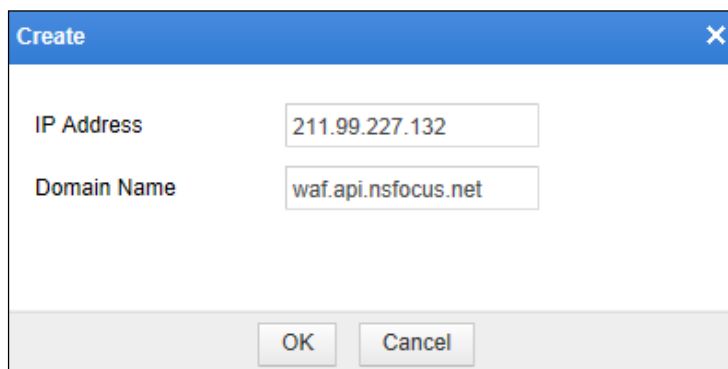
ID	Domain Name	IP Address	Operation
0	espp.api.nsfocus.com	10.5.39.1	

- b. Click **Add**.
- c. Type a domain name for cloud-based scanning and an IP address for receiving scanning reports.



Domain Name must be set to **waf.api.nsfocus.net**, and **IP Address** must be set to **211.99.227.132**.

Figure 4-119 Creating the mapping between a domain name and an IP address

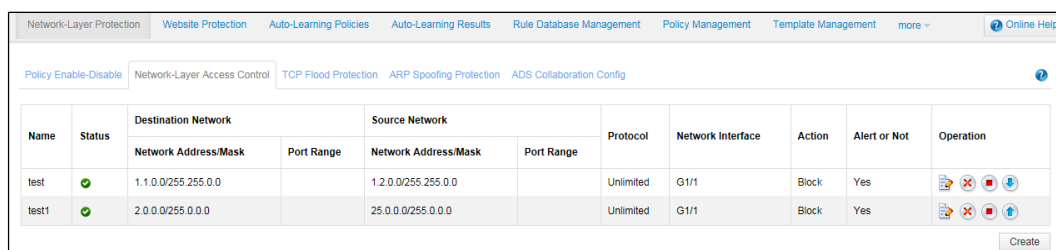


A 'Create' dialog box with a blue header bar containing a close button (X). The dialog contains two input fields: 'IP Address' with the value '211.99.227.132' and 'Domain Name' with the value 'waf.api.nsfocus.net'. At the bottom are 'OK' and 'Cancel' buttons.

Step 3 (Optional) Configure network-layer access control policies to allow the IP address of penetration scanning to directly access the customer network system.

Choose **Security Management > Network-Layer Protection > Network-Layer Access Control** and configure two network-layer access control policies, as shown in [Figure 4-120](#).

Figure 4-120 Configuring network-layer access control policies for penetration scanning



The interface shows the 'Network-Layer Protection' section with 'Network-Layer Access Control' selected. It displays a table of configured policies.

Name	Status	Destination Network		Source Network		Protocol	Network Interface	Action	Alert or Not	Operation
		Network Address/Mask	Port Range	Network Address/Mask	Port Range					
test	✓	1.1.0.0/255.255.0.0		1.2.0.0/255.255.0.0		Unlimited	G1/1	Block	Yes	[Icons]
test1	✓	2.0.0.0/255.0.0.0		25.0.0.0/255.0.0.0		Unlimited	G1/1	Block	Yes	[Icons]

Buttons: Policy Enable-Disable, Network-Layer Access Control, TCP Flood Protection, ARP Spoofing Protection, ADS Collaboration Config, Online Help, Create.

----End

4.9.2 Configuring the WVSS Scanning Service

WAF can collaborate with NSFOCUS Web Vulnerability Scanning System (WVSS). WAF dispatches scanning tasks to WVSS, which then uploads scanning reports to WAF after completing tasks. To configure WAF to collaborate with WVSS, perform the following steps:

Choose **Security Management > Smart Patch > WVSS Scan Config**.

Figure 4-121 WVSS Scan Config page

Configuring WVSS Device Parameters

Step 1 On the **WVSS Scan Config** page, set WVSS device parameters.

Table 4-42 WVSS device parameters

Parameter	Description
WVSS Address	Specifies the IP address of the WVSS device with which WAF will collaborate.
User Name	Specifies the user name for login to the WVSS device.
Password	Specifies the password for login to the WVSS device.

Step 2 Click **Connect** to connect WAF to WVSS.

----End

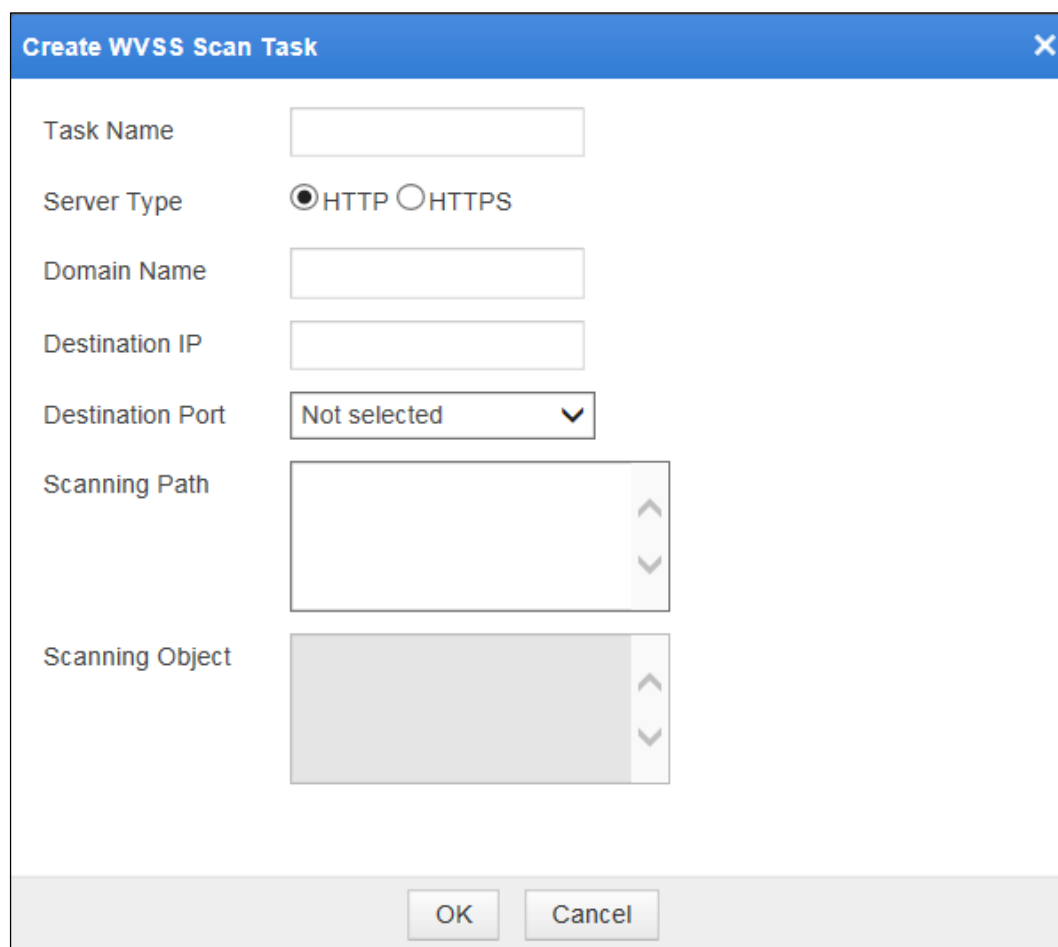
Managing WVSS Scanning Tasks

After WAF connects to WVSS, you can create, view, suspend/continue, restart, delete, and refresh WVSS scanning tasks on WAF.

Creating a Scanning Task

Step 1 Click **Create** to the upper right of the task list.

Figure 4-122 Creating a WVSS scanning task



The dialog box titled "Create WVSS Scan Task" contains the following fields and controls:

- Task Name:** A text input field.
- Server Type:** Radio buttons for ☒ HTTP and ☐ HTTPS.
- Domain Name:** A text input field.
- Destination IP:** A text input field.
- Destination Port:** A dropdown menu currently showing "Not selected".
- Scanning Path:** A text input field with a vertical scrollbar on the right.
- Scanning Object:** A text input field with a vertical scrollbar on the right.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Step 2 In the dialog box, set the parameters.


Table 4-43 Parameters for creating a WVSS scanning task

Parameter	Description
Task Name	Name of the new task
Server Type	Target server type, which can be HTTP or HTTPS
Domain Name	Target domain name of the new task
Destination IP	Destination IP address of the new task
Destination Port	Target port number of the new task
Scanning Path	Scanning path of the new task
Scanning Object	Object of the new task



Step 3 Click **OK** to save the settings and dispatch the task.

----End


Viewing Task Details

Click  in the **Operation** column of the task list on the **WVSS Scan Config** page to view details about a scanning task.

Suspending/Continuing a Scanning Task


- Click  in the **Operation** column of the task list on the **WVSS Scan Config** page to suspend an ongoing task.
- Click  in the **Operation** column of the task list on the **WVSS Scan Config** page to continue a suspended task.

Restarting a Scanning Task

Click  in the **Operation** column of the task list on the **WVSS Scan Config** page to restart a scanning task.

Deleting Scanning Tasks

Scanning tasks can be deleted as follows:

- Click  in the **Operation** column of the task list on the **WVSS Scan Config** page to delete a scanning task.
- Select one or more scanning tasks from the task list on the **WVSS Scan Config** page and click **Bulk Delete** to delete the selected task(s).

Refreshing the Task List

Click **Refresh** to the upper right of the task list to obtain the latest information about tasks.

4.9.3 Managing Scanning Files

On the **Scanning File Management** page, you can perform the following operations:

- Managing cloud-based scanning reports
You can view cloud-based scanning reports and generate smart patches based on vulnerabilities in the reports.
- Managing imported scanning reports
You can import, view, download, and delete imported web vulnerability scanning reports, and generate smart patches based on vulnerabilities in the reports.

Choose **Security Management > Smart Patch > Scanning File Management**. By default, the page for managing cloud-based scanning reports (SaaS reports) appears, as shown in [Figure 4-123](#). To switch to the page for managing web vulnerability scanning reports (WVSS reports), click **WVSS** in the upper-left corner of the page.

Figure 4-123 SAAS scanning file list

SAAS Scan Config WVSS Scan Config Scanning File Management Patch Management			
<input checked="" type="radio"/> SAAS <input type="radio"/> WVSS			
Scanning Domain Name	Latest Scanning Time	Scanning Status	Scanning File
zhuti.dianxinos.com	2012-12-26 17:29:09	Scanning completed.	Related Scanning File
theme01.dianxinos.com	2012-12-26 17:29:09	Scanning completed.	No scanning file
browser.dianxinos.com	2012-12-26 17:29:09	Scanning completed.	No scanning file
qianbian.dianxinos.com	2012-12-26 17:29:10	Scanning completed.	No scanning file
donut.dianxinos.com	2012-12-26 17:29:11	Scanning completed.	No scanning file
daohang.dianxinos.com	2012-12-26 17:29:11	Scanning completed.	No scanning file
widgetapi.dianxinos.com	2012-12-26 17:29:08	Scanning completed.	No scanning file

4.9.3.1 Cloud-based Scanning Reports

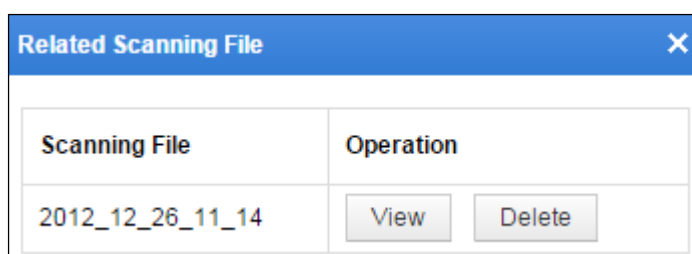
This section describes how to view cloud-based scanning reports and generate smart patches accordingly.

Viewing Cloud-Based Scanning Reports

After a cloud-based scanning file is completed, perform the following steps to view the scanning report:

- Step 1** On the **Scanning File Management** page shown in [Figure 4-123](#), click **Related Scanning File**.

Figure 4-124 Related Scanning File dialog box



- Step 2** Click **View**.

Figure 4-125 Cloud-based scanning report

SaaS Scanning File						
<input type="checkbox"/>	6	robots File Network Architecture Information Disclosure on Target Network	1200035	1	Q	
<input type="checkbox"/>	7	CRLF Injection Vulnerability in Target Website	1000061	1	Q	
<input type="checkbox"/>	8	PHP Source Code Disclosure Detected on Target Network	1000049	1	Q	
<input type="checkbox"/>	9	PHP Source Code Disclosure Detected on Target Network	1000049	1	Q	
<input type="checkbox"/>	10	PHP Source Code Disclosure Detected on Target Network	1000049	1	Q	
<input type="checkbox"/>	11	Invalid Links Detected on Target Network	1000013	1	Q	
<input type="checkbox"/>	12	Invalid Links Detected on Target Network	1000013	1	Q	
<input type="checkbox"/>	13	XSS Vulnerability Detected On Target URL	1000001	1	Q	
*After the selection, the resulting smart patch can be applied to websites.						Generate Patch

Step 3 Click  in the **View** column to view details of a vulnerability.

Figure 4-126 Details of a vulnerability

SaaS Scanning File

Web Vulnerability Information (Complete Time:2012-12-26 17:32:10 Detected 13 types of vulnerabilities)

<input type="checkbox"/>	Selection	No.	Vulnerability Name	Vulnerability ID	Vulnerable URL Amount	View
<input type="checkbox"/>		1	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q

Vulnerable URL	Validation Message	Request Method
http://zhuti.dianxinos.com/dx_themeserver/dx_themeserver.nocache.js	GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS	OPTIONS


Detailed Description:The target Web server is detected to be set to allow one or several of the following HTTP methods: DELETE, SEARCH, COPY, MOVE, PROPFIND, PROPPATCH, MKCOL, LOCK, and UNLOCK. These methods indicate that WebDAV may have been applied on the server. Since dav allows the client to manipulate files on the server, improper configuration of dav may allow unauthorized users to exploit this vulnerability and modify files on the server.

<input type="checkbox"/>	2	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q
<input type="checkbox"/>	3	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q

----End

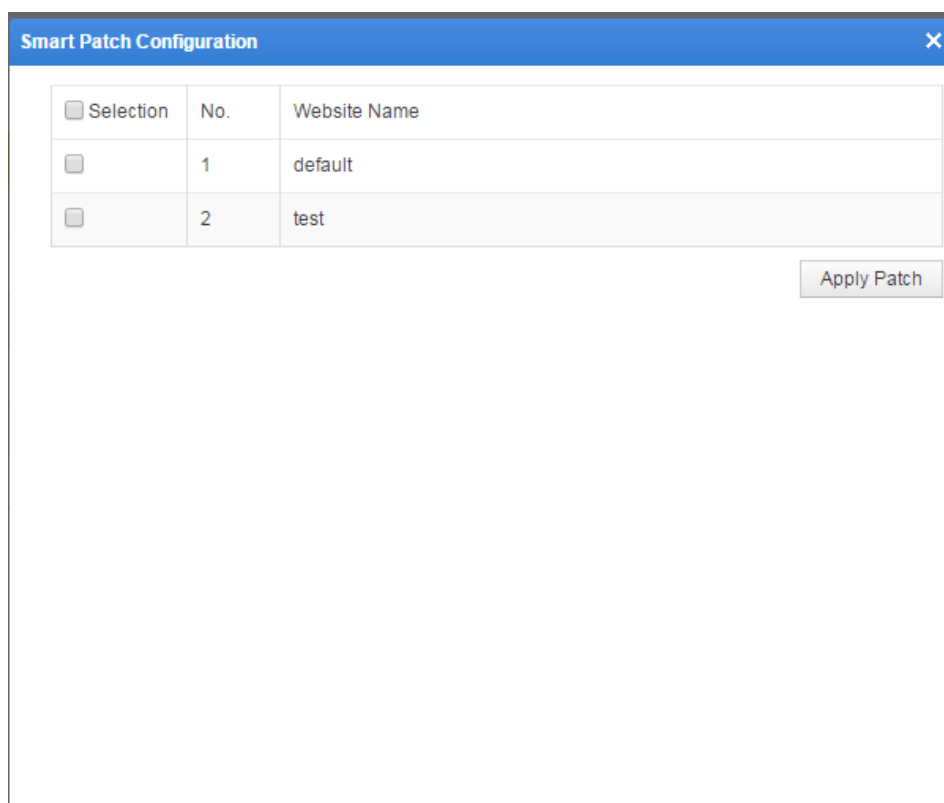
Generating Patches

Click **Generate Patch** in the lower-right corner of the **SaaS Scanning File** dialog box shown in [Figure 4-125](#). A dialog box appears, saying "It might take a long period of time and the WAF might encounter a high CPU load while generating a great many patches. Continue?" Click **OK** to generate patches.

	<p>If smart patches fail to be generated, a red message saying "Generation failed. Please try later." appears in the lower-right corner of the SaaS Scanning File dialog box as shown in Figure 4-125. You are advised to regenerate smart patches a moment later.</p>
---	---

If WAF successfully generates smart patches based on detected web vulnerabilities, the **Smart Patch Configuration** page appears, as shown in [Figure 4-127](#).

Figure 4-127 Smart Patch Configuration page



The image shows a 'Smart Patch Configuration' dialog box with a blue title bar and a close button. It contains a table with three columns: 'Selection', 'No.', and 'Website Name'. There are two rows of data. The first row has an unchecked checkbox, '1', and 'default'. The second row has an unchecked checkbox, '2', and 'test'. An 'Apply Patch' button is located at the bottom right of the dialog.

<input type="checkbox"/> Selection	No.	Website Name
<input type="checkbox"/>	1	default
<input type="checkbox"/>	2	test

Apply Patch

Applying Patches

On the **Smart Patch Configuration** page as shown in [Figure 4-127](#), select smart patches to be applied and click **Apply Patch**. A dialog box appears, saying "It might take a long period of time and the WAF might encounter a high CPU load while applying a great many patches. Continue?" Click **OK** to apply patches.



- If smart patches fail to be applied, a red message saying "Failed to generate the patch, please retry later." appears in the lower-right corner of the **Smart Patch Configuration** dialog box as shown in [Figure 4-127](#). You are advised to reapply smart patches a moment later.
- Unselected patches are not applied. To apply those unselected patches later, you need to go to the **Web Security Protection** page of the website group. For details, see related smart patch description in [Web Security Protection Policy](#) in section [4.3.2.4 Configuring Website Security Policies](#).

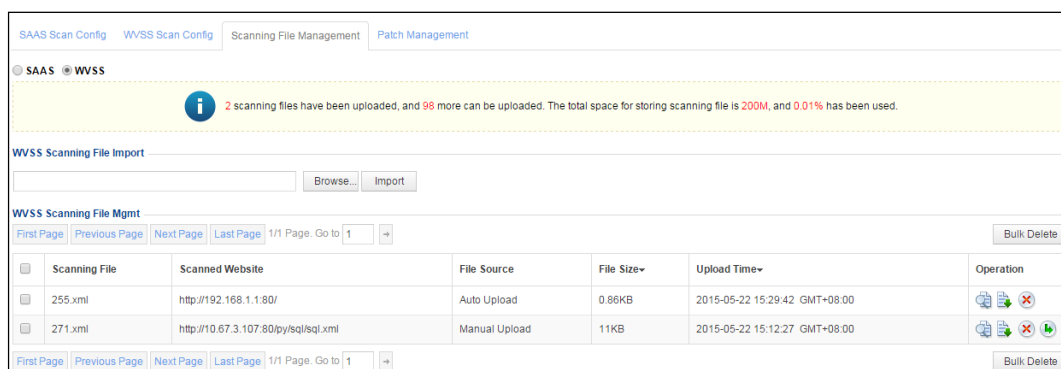
Deleting Cloud-Based Scanning Reports

In the **Related Scanning File** dialog box shown in [Figure 4-124](#), click **Delete** in the **Operation** column, and click **OK** in the confirmation dialog box, to delete the scanning report.

4.9.3.2 WVSS Scanning Reports

Choose **Security Management > Smart Patch > Scanning File Management**. Click **WVSS** in the upper-left corner of the page. The page for managing imported WVSS scanning files appears, as shown in [Figure 4-128](#). On this page, you can import, view, download, and delete imported reports. Also, based on vulnerabilities in the reports, you can generate and apply smart patches.

Figure 4-128 Page for managing imported scanning files



You can click **File Size** or **Upload Time** to rank WVSS scanning files by file size or upload time.

Importing a Report

To import a scanning report, perform the following steps:

- Step 1** On the page shown in [Figure 4-128](#), click **Browse** and select a desired WVSS scanning report.
- Step 2** Click **Import**.

After being imported, the scanning report is displayed in the **WVSS Scanning File Mgmt** list.

----End

Viewing Report Details

To view an imported report, perform the following steps:

- Step 1** In the **WVSS Scanning File Mgmt** list, click  in the **Operation** column.

Figure 4-129 Imported report

WVSS Scanning File				
Web Vulnerability Information (Complete Time:2015-05-13 11:06:29 (UTC+08:00) Detected 6 types of vulnerabilities)				
No.	Vulnerability Name	Vulnerability ID	Vulnerable URL Amount	View
1	System Directory Disclosure on Target Server	1000051	1	
2	System Directory Disclosure on Target Server	1000051	1	
3	A Directory Showing File List Detected in Target Server	1000003	1	
4	Database Error Information Disclosed	1000027	1	
5	Database Error Information Disclosed	1000027	1	
6	Invalid Links Detected on Target Network	1000013	1	
Page Number:1 /1 Record Number:6 First Page Previous Page Next Page Last Page Generate Patch				

Step 2 Click in the **View** column to view its details.

Figure 4-130 Details of a vulnerability

WVSS Scanning File

Web Vulnerability Information (Complete Time:2015-05-13 11:06:29 (UTC+08:00) Detected 6 types of vulnerabilities)

No.	Vulnerability Name	Vulnerability ID	Vulnerable URL Amount	View
1	System Directory Disclosure on Target Server	1000051	1	

Vulnerable URL	Validation Message	Request Method
http://10.67.3.107/py/sql/sqlget.php	C:\xampp\htdocs\py\sql\sqlget.php	GET

Detailed Description:Server responses may contain system directories, such as /home, /var, or c:\ and others, which is generally because the target web application does not handle error messages properly and lead to directory disclosure. If an attacker obtains this information, he can get the target server's directory structure, bringing convenience to the attack.

2	System Directory Disclosure on Target Server	1000051	1	
3	A Directory Showing File List Detected in Target Server	1000003	1	
4	Database Error Information Disclosed	1000027	1	
5	Database Error Information Disclosed	1000027	1	
6	Invalid Links Detected on Target Network	1000013	1	


----End

Generating Patches

Step 1 On the page shown in [Figure 4-129](#), click **Generate Patch**.

A dialog box appears, saying "It might take a long period of time and the WAF might encounter a high CPU load while generating a great many patches. Continue?"

Step 2 Click **OK** to generate patches.

 Note	<p>If smart patches fail to be generated, a red message saying "Generation failed. Please try later." appears in the lower-right corner of the WVSS Scanning File dialog box as shown in Figure 4-130. You are advised to regenerate smart patches a moment later.</p>
--	---

----End



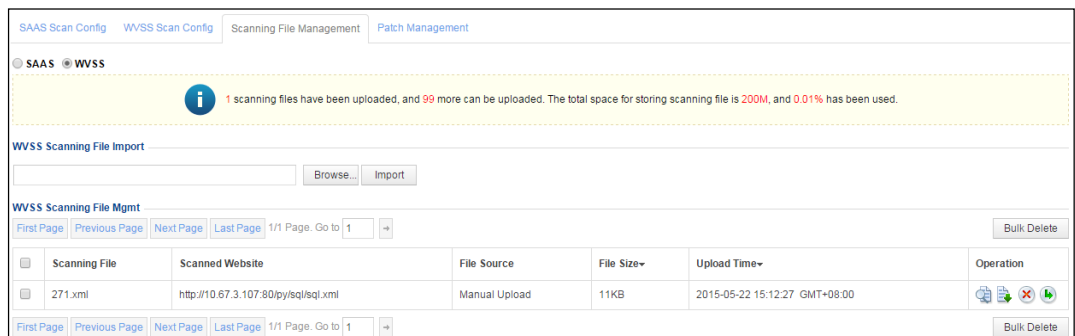
After patches are generated for the report,  appears in the **Operation** column in the **WVSS Scanning File Mgmt** list, as shown in [Figure 4-131](#). If no patch has been generated for an imported report,  does not appear in the **Operation** column of the report, and no patch can be applied for the imported report.

Figure 4-131 WVSS scanning files with patches




SAAS Scan Config WVSS Scan Config Scanning File Management Patch Management

SAAS WVSS

1 scanning files have been uploaded, and 99 more can be uploaded. The total space for storing scanning file is 200M, and 0.01% has been used.

WVSS Scanning File Import

WVSS Scanning File Mgmt

Scanning File	Scanned Website	File Source	File Size	Upload Time	Operation
271.xml	http://10.67.3.107:80/py/sql/sql.xml	Manual Upload	11KB	2015-05-22 15:12:27 GMT+08:00	

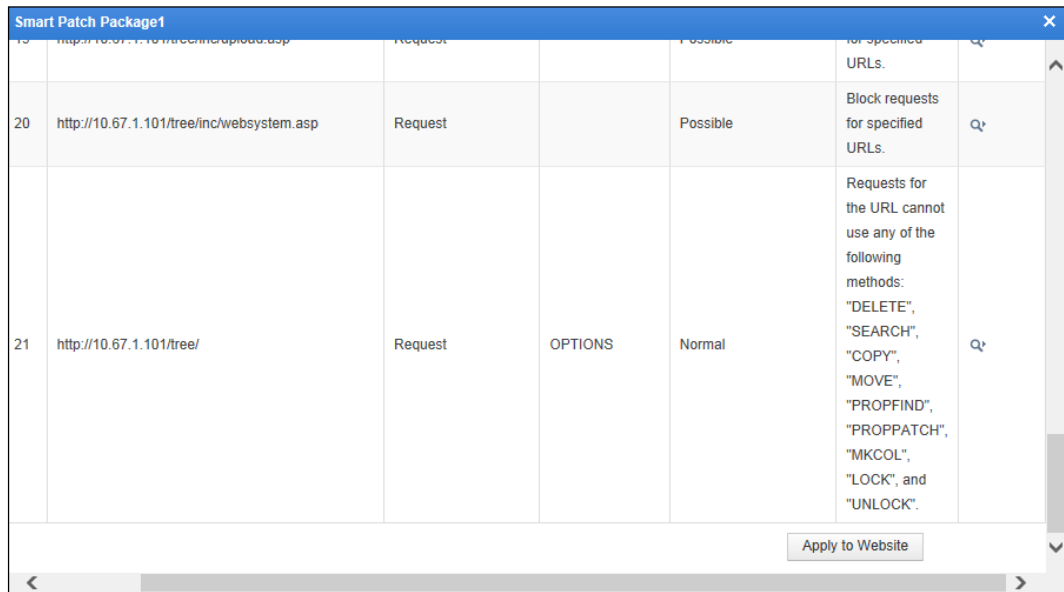
Applying Patches

To apply patches generated for an imported scanning report, perform the following steps:

Step 1 Click  in the **Operation** column on the page shown in [Figure 4-131](#).

A dialog box appears, as shown in [Figure 4-132](#).

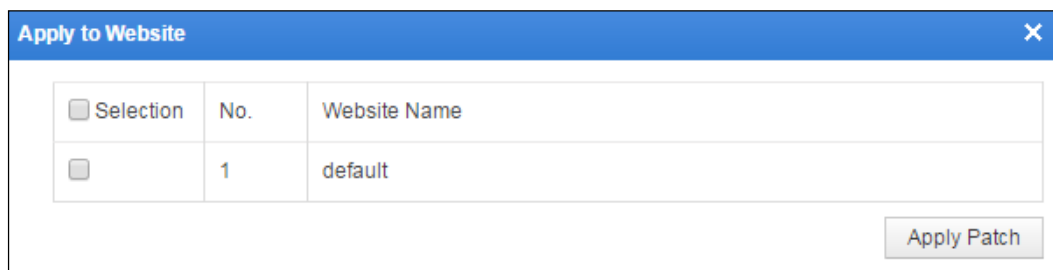
Figure 4-132 Patch application dialog box



- If all or part of a smart patch package has been applied to a website, the smart patch package cannot be applied again, and **Apply to Website** does not appear in the patch application dialog box shown in Figure 4-132. To apply such a smart patch package, you need to go to the **Web Security Protection** page. For details, see related smart patch description in [Web Security Protection Policy](#) in section 4.3.2.4 [Configuring Website Security Policies](#).
- If a smart patch package has not been dispatched and applied in the dialog box shown on the **Scanning File Management** page, the smart patch package can be applied on the **Patch Management** or **Web Security Protection** page.
- If a smart patch package has been applied on the **Web Security Protection** page, the smart patch package cannot be dispatched or applied on the **Patch Management** or **Web Security Protection** page.

Step 2 In the dialog box shown in Figure 4-132, select desired smart patches, and click **Apply to Website**.


Figure 4-133 List of websites to which the selected patches can apply



Step 3 Select one or more websites and click **Apply Patch**.


A dialog box appears, saying "It might take a long period of time and the WAF might encounter a high CPU load while applying a great many patches. Continue?"

Step 4 Click **OK** to apply the patch to the selected websites.

	<ul style="list-style-type: none"> Smart patches that are not selected in Figure 4-132 do not take effect after you click Apply Patch. Later, you can apply those unselected patches on the Web Security Protection page. For details, see Web Security Protection Policy in section 4.3.2.4 Configuring Website Security Policies. If smart patches fail to be applied, a red message saying "Failed to apply the smart patch(es), please retry later." appears in the lower-right corner of the Smart Patch Configuration dialog box shown in Figure 4-133. You are advised to reapply smart patches a moment later.
---	---


----End

Downloading a Report

In the **WVSS Scanning File Mgmt** list shown in [Figure 4-128](#), click  in the **Operation** column of a scanning report and **Save** in the displayed dialog box, to download the report as an XML file to a local directory.

Deleting Reports

In the **WVSS Scanning File Mgmt** list shown in [Figure 4-128](#), you can delete reports as follows:

- Click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete a report.
- Select one or more scanning reports, click **Bulk Delete**, and then click **OK** in the confirmation dialog box to delete the selected report(s).

4.9.4 Managing Patches

You can view generated smart patches on the **Patch Management** page and perform the following operations:

- Managing patches generated for cloud-based scanning reports
- Managing patches generated for imported web vulnerability scanning reports

Choose **Security Management > Smart Patch > Patch Management**. The **Patch Management** page for managing patches generated for cloud-scanning reports appears, as shown in [Figure 4-134](#).

To switch to the page for managing patches generated for imported web vulnerability scanning reports, click **WVSS**.

Figure 4-134 Patch Management page

SAAS Scan Config

WVSS Scan Config

Scanning File Management

Patch Management

SAAS

WVSS

12 SAAS and 4 WVSS smart patches have been generated, taking up 1.6% of the storage space.

First Page

Previous Page

Next Page

Last Page

1/1 Page. Go to 1

Bulk Delete

<input type="checkbox"/>	Smart Patch Package	Website Name	Scanning File	Complete Time	Package Source	Operation
<input type="checkbox"/>	Smart Patch Package2	default	2012_12_26_11_14_throughwaf.xml	2015-05-22 15:32:41	SAAS	<div><div></div><div></div></div>

First Page

Previous Page

Next Page

Last Page

1/1 Page. Go to 1

Bulk Delete

The operations of managing patches generated for cloud-based scanning reports are similar to managing patches generated for imported scanning reports. The following only describes the operations for managing patches generated for cloud-based scanning reports.

Viewing Patch Information

To view patch information, perform the following steps:


- Step 1** Click  in the **Operation** column of a patch package on the page shown in [Figure 4-134](#). Contents of the patch package are displayed, as shown in [Figure 4-135](#).

Figure 4-135 Patch information



Smart Patch Package2						
No.	URL	Inspection Direction	Request Method	False Alert Possibility	Patch Content	Operation
1	http://zhuti.dianxinios.com/dx_themeserver/dx_themeserv...	Request	OPTIONS	Normal	Requests for the URL cannot use any of the following methods: "DELETE", "SEARCH", "COPY", "MOVE", "PROPFIND", "PROPPATCH", "MKCOL", "LOCK", and "UNLOCK".	<div> <div></div> </div>

- Step 2** Click  in the **Operation** column of an item.

Details of the item are displayed, as shown in [Figure 4-136](#).

Figure 4-136 Details of a vulnerability fixed by the patch

Smart Patch Package2

No.	URL	Inspection Direction	Request Method	False Alert Possibility	Patch Content	Operation
1	http://zhuti.dianxinios.com/dx_themeserver/dx_themeserv... 	Request	OPTIONS	Normal	Requests for the URL cannot use any of the following methods: "DELETE", "SEARCH", "COPY", "MOVE", "PROPFIND", "PROPPATCH", "MKCOL", "LOCK", and "UNLOCK".	

Vulnerability ID	Vulnerability Name
1000063	Unsafe HTTP Method Enabled on Target URL
Detailed Description: The target Web server is detected to be set to allow one or several of the following HTTP methods: DELETE, SEARCH, COPY, MOVE, PROPFIND, PROPPATCH, MKCOL, LOCK, and UNLOCK.\r\nThese methods indicate that WebDAV may have been applied on the server. Since dav allows the client to manipulate files on the server, improper configuration of dav may allow unauthorized users to exploit this vulnerability and modify files on the server.	




- For patches in a patch package generated for imported scanning reports (WVSS reports), you can view them and click **Apply to Website** to apply them to selected websites if none of them have been applied. If some of them have been applied, you can apply those unselected patches later only on the **Web Security Protection** page of the website group. For details, see related smart patch description in [Web Security Protection Policy](#) in section 4.3.2.4 [Configuring Website Security Policies](#).
- For patches generated for cloud-based scanning reports (SaaS reports), you can only view them, but cannot apply them regardless of whether they have been applied.

----End

Deleting Patches

You can delete one or multiple reports at one time. You can delete any patch package regardless of whether it has been applied. After an applied patch package is deleted, its applied patches will lose effect.

Patch packages can be deleted as follows:

- Click  in the **Operation** column on the page shown in [Figure 4-134](#) and then click **OK** in the confirmation dialog box to delete a patch package.
- Select one or more patch packages, click **Bulk Delete**, and then click **OK** in the confirmation dialog box to delete the selected package(s).

4.10 Secure Delivery

The **Secure Delivery** module does not work on WAF in mirroring mode. It is specifically designed for web page protection. Its main functions include cache file type addition, anti-defacement configuration, page prefetch management, and server offline takeover.

This section contains the following parts:

- [Viewing Page Caches](#)
- [Adding Cache File Types](#)
- [Configuring Anti-Defacement](#)
- [Configuring Page Prefetch Management](#)
- [Clearing Cache](#)
- [Configuring Server Offline Takeover](#)

4.10.1 Viewing Page Caches

To view page caches, perform the following steps:

Step 1 Choose **Security Management > More > Secure Delivery > Page Cache**.

Step 2 Click a cache in the cache list in the left part of the page to view the URL update information corresponding to the cache.

Figure 4-137 Page Cache page

URL	Size	Last Update Time	Matches	Operation
10.68.2.204/xampp/e7d1hRQ2VY.testdir/	1621	2016-08-31 15:58:11	0	Update View

Step 3 Click **View** in the **Operation** column of the URL to view its details.

You can click **Update** to update the response cache of the URL and refresh information in the current list.

----End

4.10.2 Adding Cache File Types

To add a cache file type means to add a Multipurpose Internet Mail Extensions (MIME) type. A MIME type defines the application used to open files with a specific extension. When a user accesses a file with the extension in a browser, the browser automatically opens the file by using the defined application. A MIME type comes in two parts: a data type and a specific file type. [Table 4-44](#) describes common MIME types.

Table 4-44 Common MIME types

MIME Type	Description
text/html	Hypertext mark-up language: .html and .htm
text/plain	Plain text: .txt
application/rtf	RTF text: .rtf
image/gif	GIF image: .gif
image/jpeg	JPEG image: .jpeg, .jpg
audio/basic	Audio file: .au
audio/midi, audio/x-midi	Music file: .mid, .midi
audio/x-pn-realaudio	RealAudio audio file: .ra, .ram
video/mpeg	MPEG file: .mpg, .mpeg
video/x-msvideo	AVI file: .avi
application/x-gzIP	GZIP file: .gz
application/x-tar	TAR file

4.10.2.1 Customizing MIME Types

Although WAF has been embedded with common MIME types, there are still some special MIME types on some websites. These MIME types need to be customized.

Adding a Custom MIME Type

To add a custom MIME type, perform the following steps:

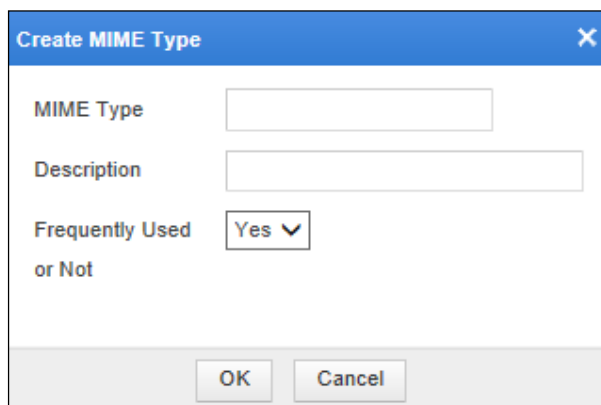
Step 1 Choose **Security Management > More > Secure Delivery > Cache File Types**.

Figure 4-138 Customized MIME Types page

ID	MIME Type	Description	Frequently Used or Not	Operation
----	-----------	-------------	------------------------	-----------

Step 2 Click **Create**.

Figure 4-139 Creating a MIME type



The dialog box titled "Create MIME Type" has a blue header bar with a close button (X). It contains three input fields: "MIME Type" (a single-line text box), "Description" (a multi-line text box), and "Frequently Used or Not" (a dropdown menu currently showing "Yes"). At the bottom are "OK" and "Cancel" buttons.

Step 3 In the dialog box, set the parameters.

Table 4-45 Parameters for creating a custom MIME type

Parameter	Description
MIME Type	Name of the MIME type.
Description	Description of the MIME type.
Frequently Used or Not	Controls whether the MIME type is frequently used.

Step 4 Click **OK** to save the settings.

----End

Editing a Custom MIME Type

You can edit a custom MIME type after it is configured. To do that, perform the following steps:


Step 1 In the MIME type list shown in [Figure 4-138](#), click  in the **Operation** column.

Step 2 In the dialog box, edit parameters of the custom MIME type, and then click **OK** to save settings and return to the page showing the MIME type list.

----End

Deleting a Custom MIME Type

You can delete MIME types one by one.

In the MIME type list shown in [Figure 4-138](#), click  in the **Operation** column and click **OK** in the confirmation dialog box to delete the MIME type.

4.10.2.2 Viewing Built-in MIME Types

Some common MIME types are built in the WAF.

Choose **Security Management > More > Secure Delivery > Cache File Types > Built-in MIME Types**.

Figure 4-140 Built-in MIME Types page

Network-Layer Protection Website Protection Auto-Learning Policies Auto-Learning Results Rule Database Management Policy Management more ▾ Online Help			
Customized MIME Types Built-in MIME Types			
ID	MIME Type	Description	Frequently Used or Not
0	application/x-001		No
1	application/x-301		No
2	text/h323		No
3	application/x-906		No
4	drawing/907		No
5	application/x-a11		No
6	audio/x-mel-aac		No

4.10.3 Configuring Anti-Defacement

WAF provides the anti-defacement function in proxy mode. WAF first uses the page prefetch function to capture contents of a web page to be protected and saves the contents locally. After conditions for anti-defacement are set, WAF will regularly capture contents from the web page, and compare them with locally saved contents. If any difference is found, WAF will determine that page defacement has occurred.

4.10.3.1 Editing the Common Anti-Defacement Configuration

To edit the common anti-defacement configuration, perform the following steps:

- Step 1** Choose **Security Management > More > Secure Delivery > Anti-Defacement Configuration**.

Figure 4-141 Common Anti-Defacement Configuration page

Network-Layer Protection Website Protection Auto-Learning Policies Auto-Learning Results Rule Database Management Policy Management Template Management more Online Help

Common Anti-Defacement Configuration URL Exception List Allowed URL List

Status	Enabled			
Single File Size(Byte)	1000000(Byte)			
Similarity	70%			
	Model/vnd.dwf	application/fractals	application/futuresplash	application/hta
	application/mac-binhex40	application/msaccess	application/msword	application/pdf
	application/pics-rules	application/pkcs10	application/pkcs7-mime	application/pkcs7-signature
	application/pkix-crl	application/postscript	application/rat-file	application/sdp
	application/smil	application/streamingmedia	application/vnd.adobe.edn	application/vnd.adobe.pdx
	application/vnd.adobe.rmf	application/vnd.adobe.workflow	application/vnd.adobe.xdp	application/vnd.adobe.xfd
	application/vnd.adobe.xfdf	application/vnd.fdf	application/vnd.ms-excel	application/vnd.ms-pki.certstore
	application/vnd.ms-pki.pko	application/vnd.ms-pki.seccat	application/vnd.ms-pki.stl	application/vnd.ms-powerpoint
	application/vnd.ms-project	application/vnd.ms-wpl	application/vnd.m-realmedia	application/vnd.m-realmedia-secure
	application/vnd.m-realmedia-vbr	application/vnd.m-realplayer	application/vnd.m-realsystem-rjs	application/vnd.m-realsystem-rjt
	application/vnd.m-realsystem-rmj	application/vnd.m-realsystem-rmx	application/vnd.m-recording	application/vnd.m-rn_music_package
	application/vnd.m-rsml	application/vnd.visio	application/x-001	application/x-301
	application/x-906	application/x-a11	application/x-anv	application/x-bittorrent
	application/x-bmp	application/x-bot	application/x-c4t	application/x-c90
	application/x-cals	application/x-cdr	application/x-cel	application/x-cgm

Step 2 Click **Edit**.

Figure 4-142 Editing the common anti-defacement configuration

Edit

Single File Size(Byte) 1-9999999

Similarity % ?

MIME Type

Extension
A null value allows all extensions. Multiple extensions should be separated by comma, for example, asp.jsp.

Website Synchronization Time
Time periods cannot overlap with each other, and a maximum of 10 time periods can be specified. Each line contains only one time period in the format like 08:01-09:01.

Client Access-Triggered Cache Update ☒ Enable ☐ Disable

Page Expiry Time(seconds)
0 indicates that the page never expires, and Client Access-Triggered Cache Update is disabled in this case.

Step 3 In the dialog box, set the parameters.

Table 4-46 Parameters for editing the common anti-defacement configuration

Parameter	Description
Single File Size(Byte)	Specifies the maximum size of a single file that can be protected. The anti-defacement function does not apply to files larger than the specified size.
Similarity	Specifies the agility of anti-defacement. The value is an integer ranging from 0 to 100.
MIME Type	Specifies the types of web page files to which anti-defacement applies. You can click All to select all types, or click Inverse to inverse the current selection.
Extension	Specifies extensions of files to which anti-defacement applies. Specifying no extension indicates that anti-defacement applies to files with any extensions. You can specify multiple extensions separated by commas, such as asp.jsp.
Website Synchronization Time	Specifies time periods in which WAF's local cache is updated. During the periods, anti-defacement is not performed. You can specify a maximum of 10 time periods, which do not

Parameter	Description
	overlap with each other. Each time period is in the format like 08:01-09:01 and takes up one line.
Client Access-Triggered Cache Update	Controls whether to enable client access-triggered cache update. If Enable is selected, when a client attempts to access a web page whose cache has expired on WAF, WAF requests the web page for content comparison and updates the web page's local cache in the case of acceptable similarity. If Disable is selected, WAF's cache will not expire, and no cache update is triggered.
Page Expiry Time(seconds)	Specifies the expiry time for page cache if Client Access-Triggered Cache Update is set to Enable .

Step 4 Click **OK** to save the settings.

----End

4.10.3.2 Configuring the URL Exception List

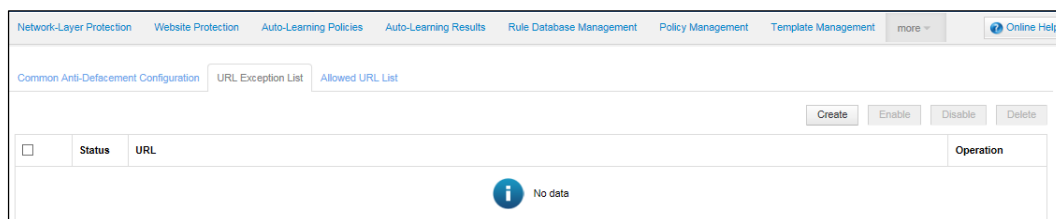
You can add URLs that do not need anti-defacement to the exception URL list. WAF does not apply anti-defacement to URLs in the list.

Adding Excluded URLs

To add excluded URLs, perform the following steps:

Step 1 Choose **Security Management > More > Secure Delivery > Anti-Defacement Configuration > URL Exception List**.

Figure 4-143 URL Exception List page



Step 2 Click **Create**.

Figure 4-144 Adding URL exceptions

Step 3 In the dialog box, set the parameters and then click **OK** to save the settings.

----End

	<p>A URL with a wildcard * is supported. For example, you can specify http://www.example.com/test/*, indicating all URLs starting with http://www.example.com/test/.</p>
--	--

Editing a URL Exception

You can edit an excluded URL after it is configured. To do that, perform the following steps:

Step 1 In the URL exception list shown in [Figure 4-143](#), click in the **Operation** column.

Step 2 Edit parameters in the dialog box and click **OK** to save the settings.

----End


Deleting Excluded URLs

In the URL exception list shown in [Figure 4-143](#), you can delete excluded URLs as follows:




- Click in the **Operation** column and then click **OK** in the confirmation dialog box to delete an excluded URL.

- Select one or more excluded URLs, click **Delete**, and then click **OK** in the confirmation dialog box to delete the selected URL(s).

Enabling Excluded URLs




By default, an excluded URL is enabled after being created. After it is disabled, its status turns to . A disabled excluded URL can be used only after being enabled.

In the URL exception list shown in [Figure 4-143](#), you can enable excluded URLs as follows:

- Click  in the **Operation** column. After an excluded URL is enabled, its status turns to .
- Select one or more excluded URLs and click **Enable**. After they are enabled, the status turns to .

Disabling Excluded URLs

In the URL exception list shown in [Figure 4-143](#), you can disable excluded URLs as follows:

- Click  in the **Operation** column. After an excluded URL is disabled, its status turns to .
- Select one or more excluded URLs and click **Disable**. After they are disabled, the status turns to .

4.10.3.3 Configuring the Allowed URL List

You can add URLs to which anti-defacement needs to apply. WAF applies anti-defacement only to URLs in the allowed URL list.

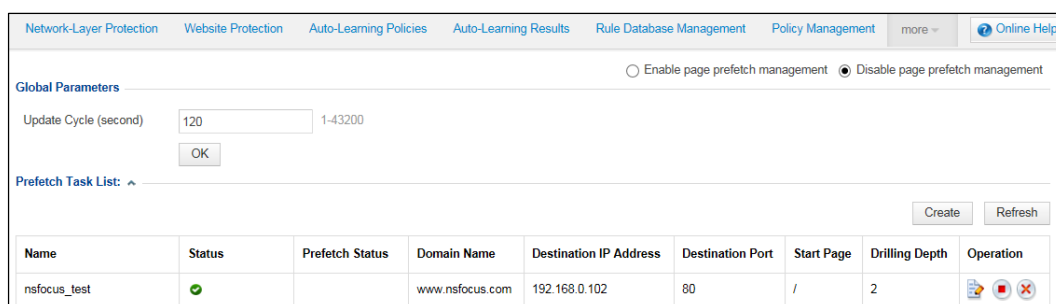
The adding, editing, deleting, enabling, and disabling operation for the allowed URL list are the same as those for the URL exception list. For details, see [section 4.10.3.2 Configuring the URL Exception List](#).





4.10.4 Configuring Page Prefetch Management

Via page prefetch, WAF can acquire a server's data in advance. Clients attempting to access the server can obtain requested data from WAF. Even if data in the server is tampered, clients can still obtain correct data from WAF.

To configure page prefetch management, choose **Security Management > More > Secure Delivery > Page Prefetch Management**.

Figure 4-145 Page Prefetch Management page



Name	Status	Prefetch Status	Domain Name	Destination IP Address	Destination Port	Start Page	Drilling Depth	Operation
nsfocus_test			www.nsfocus.com	192.168.0.102	80	/	2	  

Enabling/Disabling Page Prefetch Management

WAF can prefetch web page contents only after this function is enabled.

- On the **Page Prefetch Management** page shown in [Figure 4-145](#), select **Enable Page Prefetch Management** to enable the page prefetch management function.
- On the **Page Prefetch Management** page shown in [Figure 4-145](#), select **Disable Page Prefetch Management** to disable the page prefetch management function.

Setting Global Parameters

WAF captures pages that need to be cached from a website at a specified update interval. To specify the interval, perform the following steps:

- Step 1** On the **Page Prefetch Management** page shown in [Figure 4-145](#), click the **Update Cycle (second)** text box and change the value.

Figure 4-146 Setting the update interval

The screenshot shows a dialog box titled "Global Parameters". Inside, there is a label "Update Cycle (second)" followed by a text input field containing the value "600". To the right of the input field is a range indicator "1-43200". Below the input field is an "OK" button.

- Step 2** Click **OK** to save the settings.

----End

Creating Page Prefetch Tasks

To perform anti-defacement, WAF needs to capture web page contents from websites to be protected. You can configure page prefetch tasks to determine what web page contents need to be captured.

To create a page prefetch task, perform the following steps:

- Step 1** On the **Page Prefetch Management** page shown in [Figure 4-145](#), click **Create** to the lower right of the **Prefetch Task List**.

Figure 4-147 Creating a page prefetch task

Step 2 In the dialog box, set the parameters.

Table 4-47 Parameters for creating a page prefetch task

Parameter	Description
Name	Name of the new task.
Domain Name	Specifies a proxy server that is available.
Destination IP	IP address of a web server. Both IPv4 and IPv6 addresses are supported.
Destination Port	Port of the web server.
Start Page	First page to be crawled by WAF. It must start with "/" and exclude wildcards.
Drilling Depth	Specifies how deep WAF crawls in the website's link. The value ranges from 1 to 20.

Step 3 Click **OK** to save the settings.

----End

Editing a Page Prefetch Task

You can edit a page prefetch task after it is configured. To do that, perform the following steps:


Step 1 In the **Prefetch Task List** shown in [Figure 4-145](#), click  in the **Operation** column.

Step 2 In the dialog box, edit parameters of the page prefetch task, and then click **OK** to save settings and return to the **Page Prefetch Management** page.





----End

Deleting a Page Prefetch Task

You can delete page prefetch tasks one by one.

In the **Prefetch Task List** shown in [Figure 4-145](#), click  in the **Operation** column and click **OK** in the confirmation dialog box, to delete a page prefetch task.

Disabling/Disabling a Page Prefetch Task

- In the **Prefetch Task List** shown in [Figure 4-145](#), click  in the **Operation** column to enable a page prefetch task. After it is enabled, its status turns to .
- In the **Prefetch Task List** shown in [Figure 4-145](#), click  in the **Operation** column to disable a page prefetch task. After it is disabled, its status turns to .

4.10.5 Clearing Cache

The cache of WAF stores page contents for anti-defacement. Once stored in the cache, page contents cannot be automatically deleted. You need to clear them manually, because too many contents in the cache could be inconvenient for configuration and maintenance.

You are advised to clear WAF's cache before configuring an anti-defacement policy.



Before clearing the cache, you must disable the page prefetch management function.

To clear the cache of WAF, perform the following steps:

Step 1 Choose **Security Management > More > Secure Delivery > Clear Cache**.

Figure 4-148 Clear Cache page



Step 2 Click **Clear Cache** and then click **OK** in the confirmation dialog box.




----End

4.10.6 Configuring Server Offline Takeover

When a server protected by WAF needs to get offline for update, WAF can take over service requests from clients to the server. After page prefetch management is configured, WAF automatically stores data of protected servers according to page prefetch tasks. After taking over requests of a protected server, if requested pages exist in WAF's cache, WAF returns the requested pages; if requested pages do not exist in WAF's cache, WAF returns a response page with the 404 status code.


Choose **Security Management > More > Secure Delivery > Server Offline Takeover**.

Figure 4-149 Server Offline Takeover page

Network-Layer Protection Website Protection Auto-Learning Policies Auto-Learning Results Rule Database Management Policy Management more ▾ Online Help						
<div>Enable</div> <div>Forbid</div>						
<input type="checkbox"/>	Status	Website Name	IP	Port	Type	Operation
<input type="checkbox"/>	●	default_v4	0.0.0.0-255.255.255.255	80	HTTP	
<input type="checkbox"/>	●	default_v6	::1-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF	80	HTTP	
<input type="checkbox"/>	●	guide_1	1.1.1.1-1.1.1.1	88	HTTP	


Enabling Server Offline Takeover Tasks

You can enable server offline takeover tasks as follows:

- On the **Server Offline Takeover** page, select one or more tasks and click **Enable** to enable the selected task(s).
- On the **Server Offline Takeover** page, click  in the **Operation** column of a task to enable it.

Disabling Sever Offline Takeover Tasks

You can disable server offline takeover tasks as follows:

- On the **Server Offline Takeover** page, select one or more tasks, and then click **Forbid** to disable the selected task(s).
- On the **Server Offline Takeover** page, click  in the **Operation** column to disable a task.

4.11 Proxy Information Configuration

To enhance user experience by avoiding bottlenecks and sections of the Internet that may affect the data transmission speed and stability, more and more website operators choose to purchase the content delivery network (CDN) proxy service for their web servers.

After the CDN proxy service is used, the access request initiated from a client to the web server first reaches the nearest CDN server. If the requested content exists in the cache of this CDN server, it directly returns response data to the client. If not, the CDN server, as a reverse proxy, forwards the request to the real web server of the website.

If WAF is deployed before this real web server, the request reaches WAF instead of the web server. The IP address of this request forwarded by the CDN server is that of the CDN server. Generally, a CDN server includes the real client IP address in a request header field, such as the common X-Forwarded-For field or the Client-IP field used by some old proxy servers.

In this case, if WAF bases its policy-based checks on network-layer IP addresses, legitimate requests may be wrongly blocked. From V6.0R05F00, WAF can discern real client IP addresses based on the configured proxy information such as HTTP header fields. This effectively avoids incorrect blocking, making WAF suitable for the business scenario where the CDN proxy service is used.


To configure proxy information, perform the following steps:

Step 1 Choose **Security Management > More > Proxy Information Configuration**.

Figure 4-150 Proxy Information Configuration page

Step 2 Set proxy parameters.

Table 4-48 Proxy parameters

Parameter	Description
Proxy Mode	<p>Proxy mode. WAF supports the following proxy modes:</p> <ul style="list-style-type: none"> Ignore: indicates that WAF will not parse proxy information. In this case, the Proxy Information field in log details is empty, Client IP in web security logs and web access logs is recorded as a network-layer IP address, and the source IP address used in the check/encryption algorithms of security policies and in IP blocking is a network-layer IP address. Record Proxy Information: indicates that WAF will parse proxy information. In this case, the Proxy Information field in log details displays proxy information parsed from HTTP header fields, Client IP in web security logs and web access logs is recorded as a network-layer IP address, and the source IP address used in the check/encryption algorithms of security policies and in IP blocking is a network-layer IP address. Use Real Client IP in Policies: indicates that WAF will parse proxy information. In this case, the Proxy Information field in log details displays proxy information parsed from HTTP header fields, Client IP in web security logs and web access logs is recorded as the source IP address parsed from proxy information, and the source IP address used in the check/encryption algorithms of security policies and in IP blocking is the source IP address parsed from proxy information.
Http-Headers	<p>HTTP header fields. If an HTTP request that triggers a web security alert contains a listed HTTP header field, this field will be included in details of a web security log as proxy information.</p> <p>You can type at most 10 header fields, which must be separated by carriage returns. The total length should not exceed 256 bytes. Each carriage return is taken as a byte.</p> <p> Note</p>

Parameter	Description
	<ul style="list-style-type: none"> If multiple header fields are found to match those listed here, all these fields will be recorded. In parsing real IP addresses of clients, the header field with the highest priority will be parsed first. The priority of HTTP header fields depends on the order in which they are entered. The field entered first has the highest priority.
Max Proxy Depth	<p>Maximum depth of HTTP headers. The maximum depth of an HTTP header field should not exceed the value specified here; otherwise, WAF takes the field as a forged one and will not trust such proxy information.</p> <p>The value range is 0–10. The value 0 indicates that WAF will not check the header depth of proxy information.</p>
Server Trusted IP	<p>IPv4 and/or IPv6 addresses trusted by the server.</p> <p>You can type at most 10 IP addresses or IP ranges, which must be separated by commas. The total length should not exceed 1023 bytes.</p>

Step 3 Click **Save** to save the settings.

----End

4.12 Uploaded File Management

This section involves SSL certificate management, XSD/WSDL file management, and disguised response file management.

4.12.1 SSL Certificate Management

SSL certificate management does not work on WAF in mirroring mode. To create an HTTPS website, an SSL certificate must be uploaded. You can upload, view, or delete the SSL certificate.

4.12.1.1 Importing an SSL Certificate

To import an SSL certificate, perform the following steps:

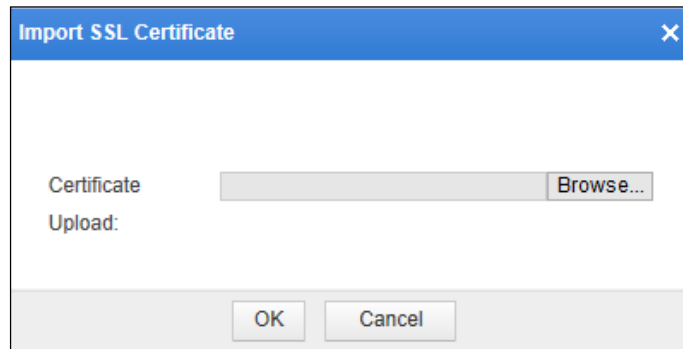
Step 1 Choose **Security Management > more > Uploaded File Mgmt > SSL Certificate Mgmt**.

Figure 4-151 SSL certificate management

Page Number:1 /1 Record Number:2		First Page	Previous Page	Next Page	Last Page	<input checked="" type="checkbox"/> Display certificate applied by website	Import	Bulk Delete
<input type="checkbox"/>	Certificate Name	Website Applying the Certificate		Certificate Upload Time		Operation		
<input type="checkbox"/>	nsfocus.cer	default_v4		2018-11-17 10:38:31				
<input type="checkbox"/>	nsfocus_sha256.cer			2018-11-17 10:38:31				

Step 2 Click **Import** on the page.

Figure 4-152 Importing an SSL certificate



Step 3 Click **Browse** and select the desired SSL certificate. Then click **OK**.

----End

You can also view or delete the SSL certificate.

4.12.1.2 Viewing an SSL Certificate


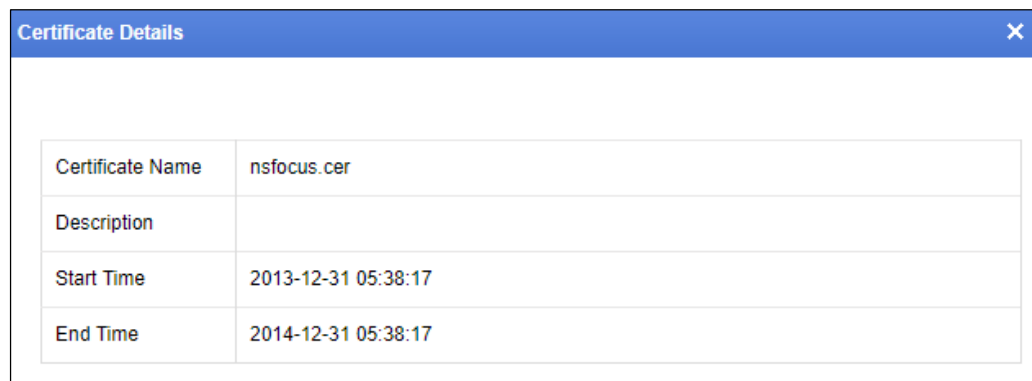

Click  in the **Operation** column of the certificate list to view details of an SSL certificate.

Figure 4-153 Details of an SSL certificate



Click  in the upper-right corner of dialog box to close it.

4.12.1.3 Deleting SSL Certificates

On the SSL certificate list, select one or more certificates, click **Bulk Delete**, and click **OK** in the confirmation dialog box to delete the selected certificate(s).

4.12.2 XSD/WSDL File Management

The **XSD/WSDL File Management** page lists all uploaded XSD/WSDL files. You can manage XSD/WSDL files on this page, such as uploading, downloading, and deleting a file.

XSD files and WSDL files respectively support the schema validation and SOAP validation for XML attack protection of WAF.

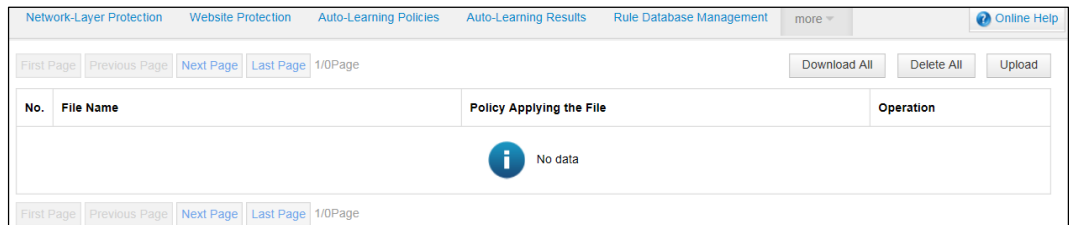
- **XSD files**
The XML schema language is referred to as XSD. XML schema defines the structure of a type of XML documents. WAF implements validation by checking an XML document to see whether it conforms to a specified XML schema.
- **WSDL files**
As an element of web services, WSDL describes how to access a specific interface. Before web service applications are deployed, SOAP messages are checked for XML attacks.

The following sections describe how to manage XSD and WSDL files.

4.12.2.1 Uploading a File

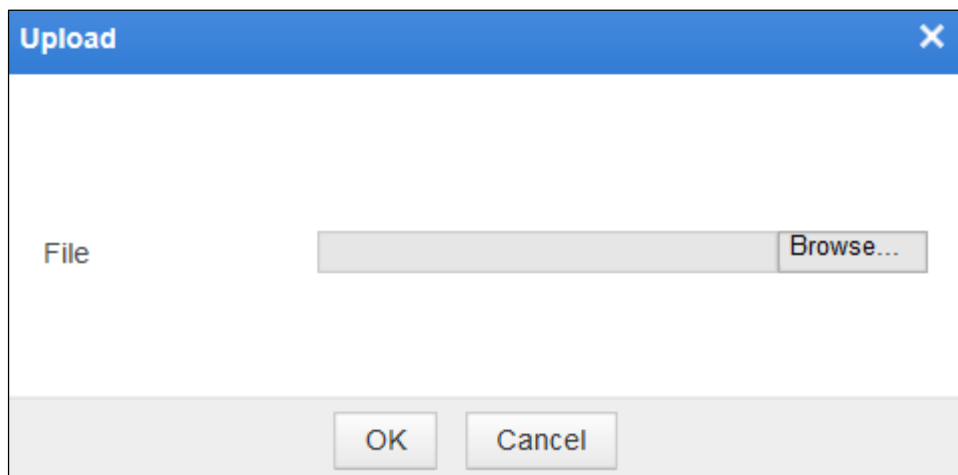
Step 1 Choose **Security Management > more > Uploaded File Mgmt > XSD/WSDL File Mgmt**.

Figure 4-154 XSD/WSDL file management



Step 2 Click **Upload** in the upper-right corner of the page.

Figure 4-155 Uploading an XSD or WSDL file



Step 3 Browse to an XSD or WSDL file in a local disk drive. Then click **OK**.



Pay attention to the following when uploading an XSD or WSDL file:

- | | |
|--|---|
| | <ul style="list-style-type: none"> • A single file cannot exceed 10 MB. • A maximum of 1000 files of each type can be uploaded. • The uploaded files on the file list cannot exceed 200 MB in total. |
|--|---|

----End

4.12.2.2 Downloading a File

On the page shown in [Figure 4-152](#), click **Download All**. Then WAF will compress all listed XSD/WSDL files into a file named **xsd_wsdl.tar.gz** and download it to a local disk drive.



	WinRAR can be used to compress XSD/WSDL files.
--	--

4.12.2.3 Deleting a File

Before deleting files, you are advised to make backup copies as files cannot be restored or referenced by policies once they are deleted.

Only the XSD/WSDL files that are not referenced by policies can be deleted. For files that are referenced by policies, there is no icon in the **Operation** column, indicating that such files cannot be deleted.

You can click in the **Operation** column to delete a file or click **Delete All** to delete all files.

After you click **Delete All**, only files that are not referenced by policies are deleted. That is to say, only files, for which the **Policy Applying the File** column is empty or is available in the **Operation** column, are deleted. Files that are referenced by policies, however, still exist.


4.12.3 Disguised Response File Management

When configuring a policy with **Action** set to **Disguise**, you need to select an existing disguised response file or upload a new one. Such files, whether existing or newly uploaded, will be displayed on the **Disguised Response File Mgmt** page. You can upload or delete files on this page.

4.12.3.1 Uploading a Disguised Response File


Step 1 Choose **Security Management > more > Uploaded File Mgmt > Disguised Response File Mgmt**.

Figure 4-156 Disguised response file management

Network-Layer Protection		Website Protection		Auto-Learning Policies		Auto-Learning Results		Rule Database Management		more ▾		 Online Help	
Page Number:1 /1		Record Number:2		First Page		Previous Page		Next Page		Last Page		<div>Upload</div> Upload an HTML or Image File	
No.	File Name											Operation	
1	default.gif											This is the system default file and cannot be deleted.	
2	default.html											This is the system default file and cannot be deleted.	

Step 2 Click **Upload** to open the file upload dialog box.

Step 3 Click **Select File** to select a disguised response file in the GIF or HTML format and click **OK** to upload this file.


		A disguised response file in the GIF format to upload cannot exceed 20 KB.
---	--	--


----End

4.12.3.2 Deleting a Disguised Response File

You are advised to back up files before deleting them as files, once deleted, cannot be recovered and referenced by policies.

Since default files and those that are referenced by policies cannot be deleted, only files that are not referenced by policies can be deleted.

You can click  in the **Operation** column of a file to delete it.

If **This file is being used by a policy and cannot be deleted.** is displayed but no  is shown in the **Operation** column of a file, this file is being referenced by a policy and cannot be deleted, as shown in Figure 4-156.

4.13 IP Reputation

IP reputation protection means that WAF checks IP addresses based on IP reputation data obtained from the NSFOCUS reputation cloud connecting to WAF, thereby providing more convenient and accurate IP protection services.

This section briefly introduces IP reputation and describes how to configure an IP reputation policy, which takes effect only after being loaded by website groups. For how to load an IP reputation policy, see [Web Security Protection Policy](#) in section 4.3.2.4 [Configuring Website Security Policies](#).

WAF in mirroring mode only supports advanced protection for IP reputation but not common protection.

4.13.1 IP Reputation Overview

To view the IP reputation overview, follow these steps:

Step 1 Choose **Security Management > IP Reputation > IP Reputation Overview**.

Figure 4-157 IP Reputation Overview page

IP Reputation Overview		IP Reputation Configuration																						
Service Status		Enabled																						
Service Due Time		20170914																						
Attack Type		DDoS attack Vulnerability Spam Web attack Scan source Botnet client																						
Reputation Match Count in the Last One Week		<table><tr><td>Date</td><td>6.30</td><td>6.29</td><td>6.28</td><td>6.27</td><td>6.26</td><td>6.25</td><td>6.24</td></tr><tr><td>Matches</td><td>7</td><td>7</td><td>37</td><td>0</td><td>0</td><td>0</td><td>0</td></tr></table>							Date	6.30	6.29	6.28	6.27	6.26	6.25	6.24	Matches	7	7	37	0	0	0	0
Date	6.30	6.29	6.28	6.27	6.26	6.25	6.24																	
Matches	7	7	37	0	0	0	0																	

Step 2 View IP reputation information.

Table 4-49 IP reputation overview details

Parameter	Description
Service Status	The status of the IP reputation protection module depends on the license. If the license is valid, Service Status is displayed as Enabled . If the license expires, Service Status is displayed as Disabled .
Service Due Time	Indicates the end time of the license.
Attack Type	Indicates the type of IP reputation data, including: <ul style="list-style-type: none"> DDoS attack Vulnerability Spam Web attack Scan source Botnet client
Numbers of Reputation Matches in the Past 7 Days	Indicates the numbers of attacks triggering common protection and advanced protection for IP reputation in the past 7 days.

----End

4.13.2 IP Reputation Configuration

Choose **Security Management > IP Reputation > IP Reputation Configuration**.

Figure 4-158 IP Reputation Configuration page

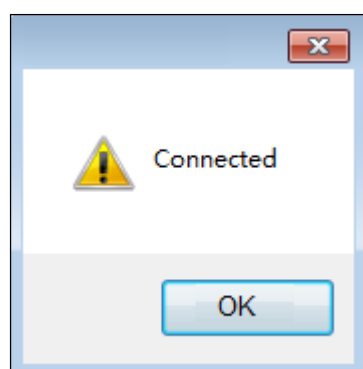
4.13.2.1 Reputation Cloud Connectivity Test

On the page shown in [Figure 4-158](#), the last synchronization time is displayed. In addition, you can also test the reputation cloud connectivity by following these steps:

Step 1 Click **Test**.

If WAF properly connects to the NSFOCUS reputation cloud, a dialog box indicating the connection success appears.

Figure 4-159 Connection success



Step 2 Click **OK** to complete the connectivity test.

----End

4.13.2.2 Enabling/Disabling Common Protection

Common protection indicates the application of IP reputation protection at the network layer.

On the page shown in [Figure 4-158](#), you can click **Enable** or **Disable** in the **Common Protection** area to enable or disable the common protection function.

4.13.2.3 Advanced Protection

Advanced protection indicates that by identifying geographical locations of source IP addresses based on GEOIP libraries, WAF implements access control by country or region

to which source IP addresses belong. Specifically, WAF allows or blocks access from specific regions according to the user's business requirements.

To create an advanced protection policy, follow these steps:

Step 1 In the **Advanced Protection** area in [Figure 4-158](#), click **Create** in the upper-right corner.

Figure 4-160 Creating an IP reputation policy

Step 2 In the dialog box, set parameters.

Table 4-50 Parameters for configuring an IP reputation policy

Parameter	Description
Name	Name of this IP reputation policy.
Description	Brief description about this IP reputation policy.
Alert or Not	Control whether to generate alert logs.
Action	Specifies how WAF acts on a packet matching this policy. The value can be one

Parameter	Description
	<p>of the following:</p> <ul style="list-style-type: none"> • Pass: WAF directly forwards the matching packet without any more security detection. • Block: WAF blocks matching packets and tears down the current TCP connection. • Accept: WAF completes the current detection and continues with other security detections on matching packets. • Redirection: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. • Disguise: WAF responds to the client with customized HTTP response code and response file contents, and tears down the current TCP connection.
Source IP Blocking	<p>Controls whether to block the source IP address of a packet that matches this policy. This parameter is available only when Action is set to Block.</p> <ul style="list-style-type: none"> • Unblock: WAF does not block the related source IP address. • Permanently block: WAF permanently blocks the related source IP address. • Block as customized: WAF blocks the source IP address for a specified period, which can be set to a value in seconds, minutes, or hours.
Redirection Path	Specifies the redirection URL. This parameter is mandatory when Action is set to Redirection .
Response Code	Specifies a custom response code. This parameter is mandatory when Action is set to Disguise .
Response File	Specifies a response file (by uploading or selecting an existing one). This parameter is mandatory when Action is set to Disguise .
Area	Specifies the region to which matching source IP addresses belong. You can set to include or exclude some countries and regions.

Step 3 Click **OK** to save the settings.

----End

5 Reports

This section describes reports provided by WAF. It covers the following topics:

Topic	Description
Security Reports	Describes how to view classification-specific alert reports and period-specific alert reports.
Traffic Reports	Describes how to view traffic reports.
Regional Access Statistical Reports	Describes how to view regional access statistical reports.
PCI-DSS Compliance Reports	Describes how to view CI-DSS compliance reports.

5.1 Security Reports

Security reports are divided into the classification-specific alert report and period-specific alert report. You can acquire reports based on query conditions, such as websites, event types, statistic collection periods, and statistic collection time.

5.1.1 Classification-Specific Alert Reports

Step 1 Choose **Logs & Reports > Security Reports > Classification-Specific Alert Report**.

Figure 5-1 Classification-Specific Alert Report page

Classification-Specific Alert Report [Period-Specific Alert Report](#)

Conditions ▲

Website

Frequency ☒ Daily Report ☐ Weekly Report ☐ Monthly Report

Date



 

Table 5-1 Parameters for querying a classification-specific alert report

Parameter	Description
Website	Websites whose statistics are to be queried. WAF automatically generates a website list based on your website configurations. For details about configuring websites, see section 4.3 Website Protection .
Frequency	Report preview interval, which can be Daily Report , Weekly Report , or Monthly Report .
Date	Date of statistics to be queried.

Step 2 Set the query conditions.

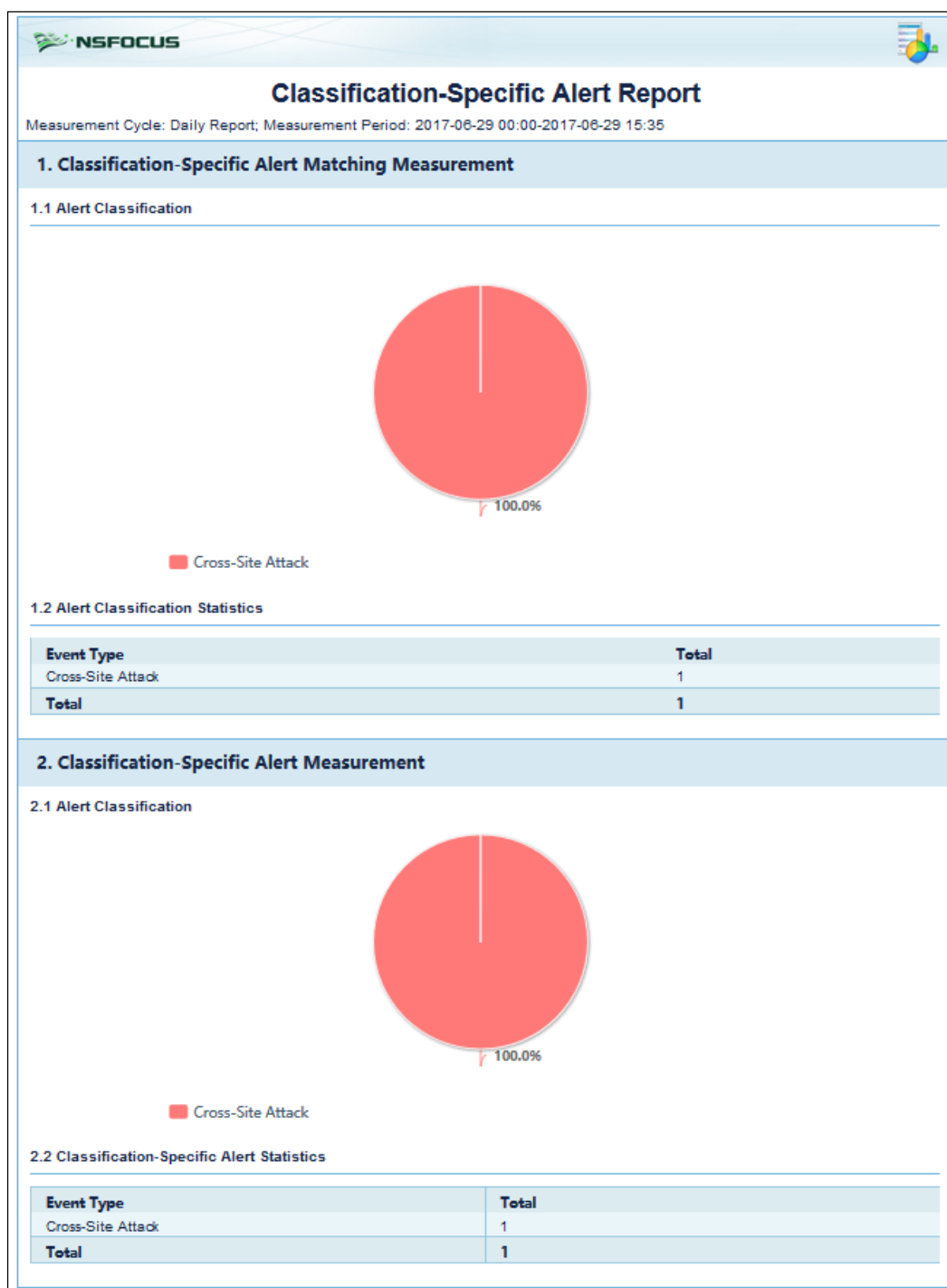
Step 3 Click **Generate**.


You can view statistics about web security events of the specified websites within the statistic collection period.

[Figure 5-2](#) shows classification-specific alert report with **Website** set to all and **Frequency** set to **Daily Report**. This report includes two parts: **Classification-Specific Alert Matching Measurement** and **Classification-Specific Alert Measurement**.

- The **Classification-Specific Alert Matching Measurement** part shows the occurrence times and proportions of various web security events.
- In the **Classification-Specific Alert Measurement** part, WAF merges web security events with the same elements into one security event every minute, and calculates the occurrence times and proportions of various merged web security events. The elements include the server, client IP address, port, and event type.

Figure 5-2 Classification-specific alert report



Step 4 (Optional) Click  to the upper right of the report and set parameters in the **Report Export** dialog box to save the report as an Excel file to a local disk drive.

Step 5 (Optional) Click  to print the report.

----End

5.1.2 Period-Specific Alert Reports

Step 1 Choose **Logs & Reports > Security Reports > Period-Specific Alert Report**.

Figure 5-3 Period-Specific Alert Report page

Table 5-2 Parameters for querying a period-specific alert report

Parameter	Description
Event Type	Security event types, which are built in WAF.
Frequency	Report preview interval, which can be Daily Report , Weekly Report , or Monthly Report .
Date	Date of statistics to be queried.

Step 2 Set the query conditions

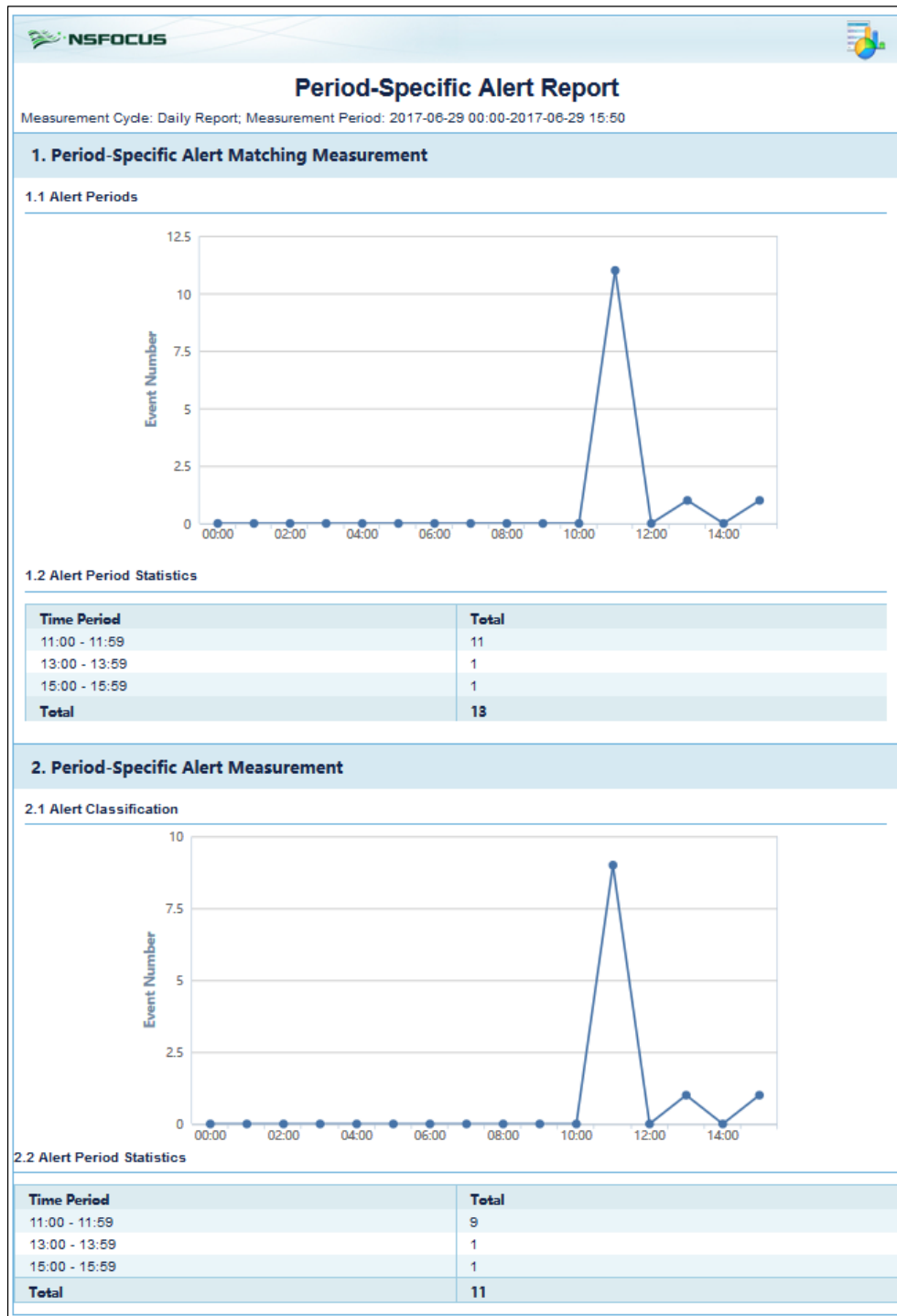
Step 3 Click **Generate**.


You can view statistics about various web security events in different time periods.

Figure 5-4 shows a period-specific alert report with **Event Type** set to all and **Frequency** set to **Weekly Report**. This report includes two parts: **Period-Specific Alert Matching Measurement** and **Period-Specific Alert Measurement**.

- The **Period-Specific Alert Matching Measurement** part shows the occurrence times and proportions of various web security events occurring in different time periods.
- In the **Period-Specific Alert Measurement** part, WAF merges web security events with the same elements into one security event every minute, and calculates the occurrence times and proportions of various merged web security events in each time period. The elements include the server, client IP address, port, and event type.

Figure 5-4 Period-specific alert report



Step 4 (Optional) Click  to the upper right of the report and set parameters in the **Report Export** dialog box to save the report as an Excel file to a local disk drive.

Step 5 (Optional) Click  to print the report.

----End

5.2 Traffic Reports

Traffic reports refer to traffic pattern reports obtained based on the device engine and interface traffic.

Step 1 Choose **Logs & Events > Traffic Reports > Traffic Pattern Reports**.

Figure 5-5 Traffic Pattern Reports page

Table 5-3 Parameters for querying a traffic pattern report

Parameter	Description
Measurement Target	Measurement target of a traffic pattern report, which can be one of the following: <ul style="list-style-type: none"> Engine: measures the traffic between the client end and server end. Interface: measures the traffic over selected interfaces.
Frequency	Report preview interval, which can be Daily Report , Weekly Report , or Monthly Report .
Date	Date of statistics to be queried.

Step 2 Set the query conditions.

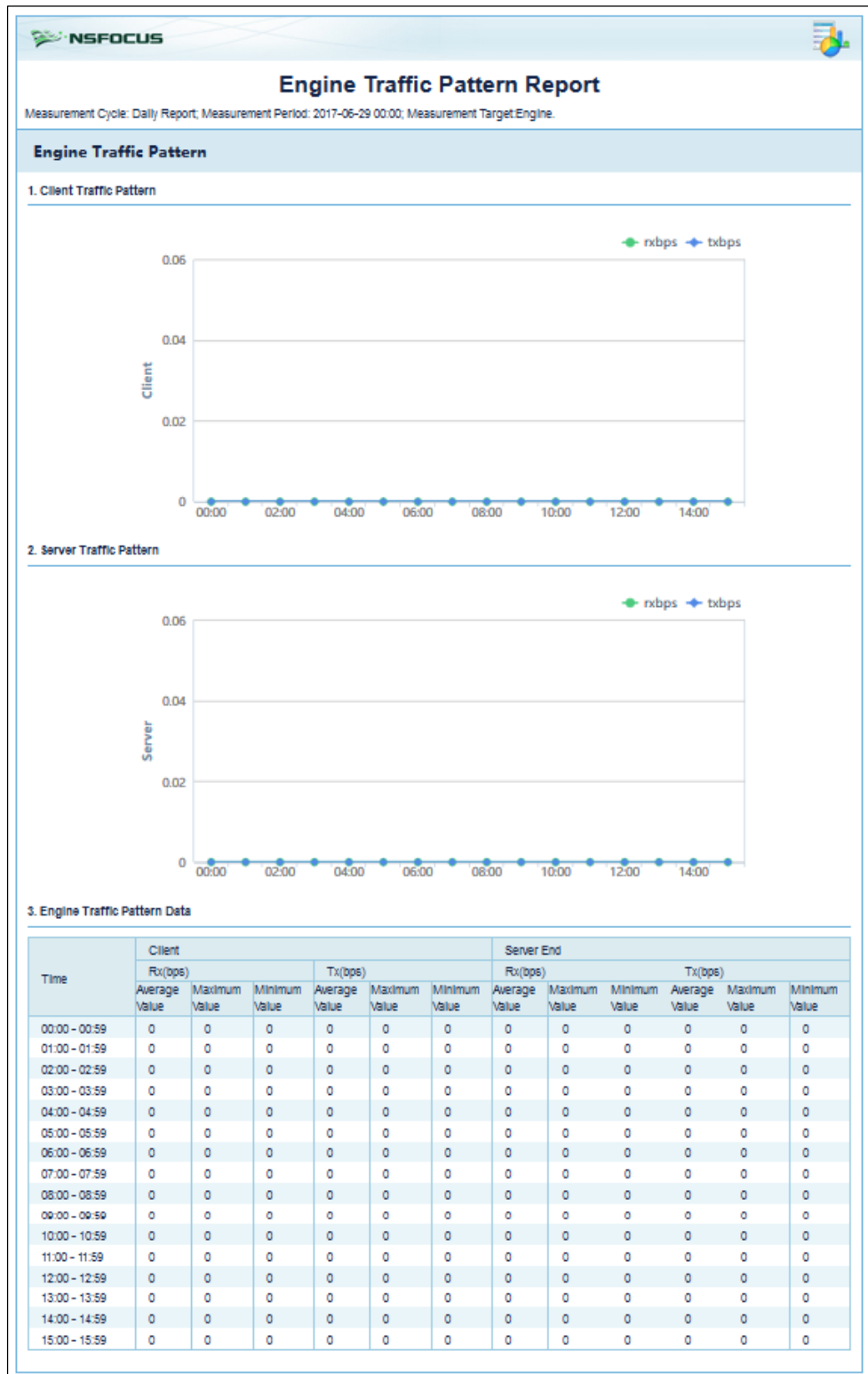
Step 3 Click **Generate**.


You can view traffic statistics of the measurement target within the specified period.

WAF provides two types of traffic statistics: engine traffic statistics and interface traffic statistics.

- Figure 5-6 shows an engine traffic pattern report with **Measurement Target** set to **Engine**. This report includes the following information of both the client end and server end:
 - Traffic pattern graphs (in Rx and Tx directions)
 - Average traffic rate
 - Maximum traffic rate
 - Minimum traffic rate

Figure 5-6 Engine traffic pattern report

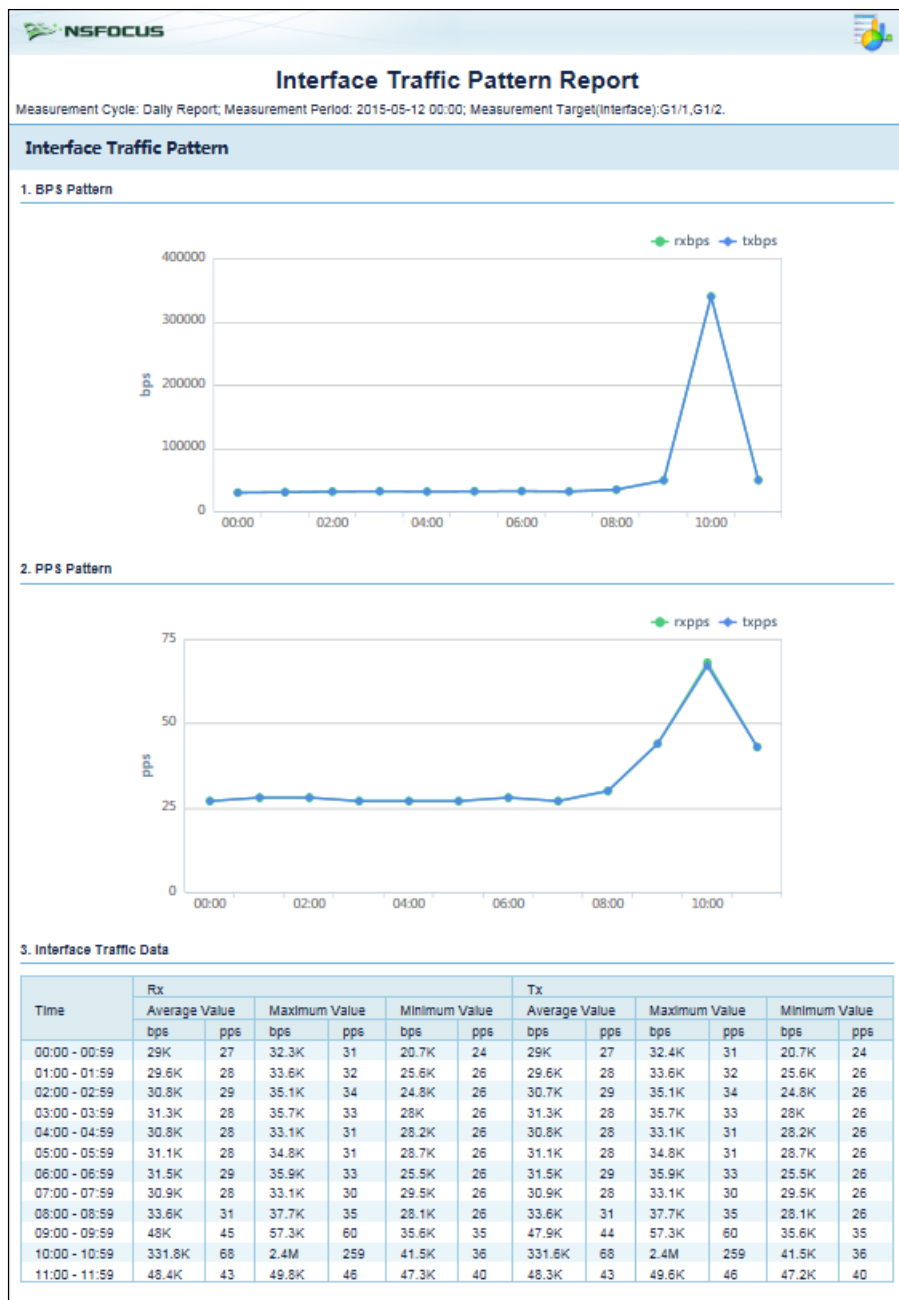



Step 4 (Optional) Click  to the upper right of the report and set parameters in the **Report Export** dialog box to save the report as an Excel file to a local disk drive.

Step 5 (Optional) Click  to print the report.

- Figure 5-7 shows an interface traffic pattern report with **Measurement Target** set to **Interface**. This report includes the following information of selected interfaces:
 - Traffic pattern graphs (in Rx and Tx directions)
 - Average traffic rate
 - Maximum traffic rate
 - Minimum traffic rate

Figure 5-7 Interface traffic pattern report



Step 6 (Optional) Click  to the upper right of the report and set parameters in the **Report Export** dialog box to save the report as an Excel file to a local disk drive.

Step 7 (Optional) Click  to print the report.

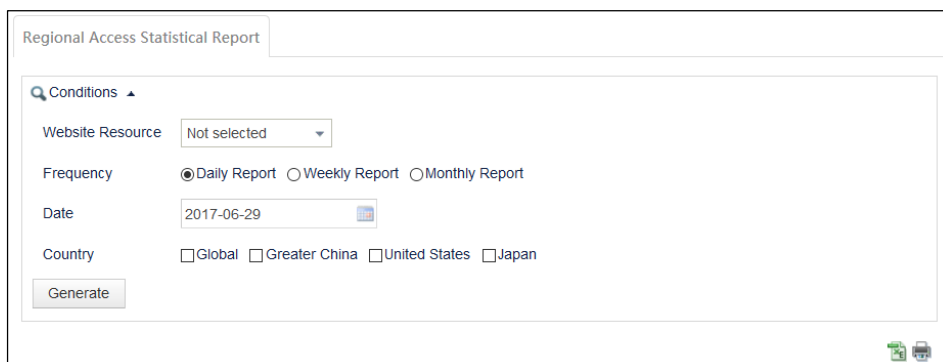
----End

5.3 Regional Access Statistical Reports

Data of regional access statistical reports come from virtual websites. Therefore, regional access statistical reports are available only after the regional access statistics function is enabled for virtual websites. For how to enable the regional access statistics function for virtual websites, see section [4.3.3 Managing Virtual Websites](#).

Step 1 Choose **Logs & Reports > Regional Access Statistical Report**.

Figure 5-8 Regional Access Statistical Report page



Step 2 Set the query conditions.

Table 5-4 Conditions for querying regional access statistical reports

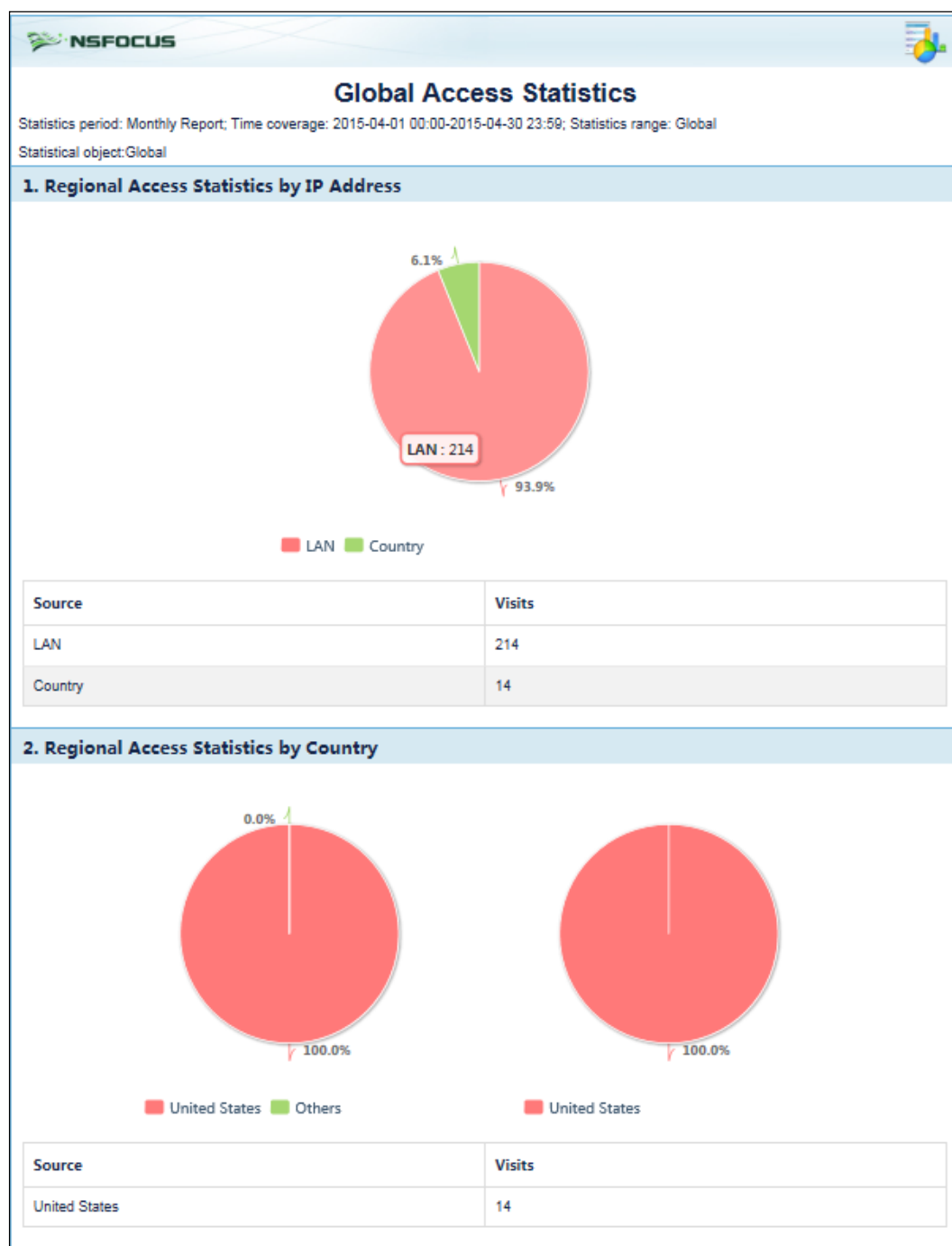
Parameter	Description
Website Resource	Specifies the virtual websites of the statistical reports in the specified period.
Frequency	Specifies the frequency of the statistical report, which can be Daily Report , Weekly Report , or Monthly Report .
Date	Specifies the period of the statistical report.
Country	Specifies the statistical region, which can be Global , Greater China , United States , or Japan .


Step 3 Click **Generate**.

The regional access statistical report meeting the conditions is displayed.

For example, if **Website Resource** is set to **Global**, **Frequency** is set to **Monthly Report**, **Date** is set to **2015-04**, and **Country** is set to **Global**. The regional access statistical report appears, as shown in [Figure 5-9](#).

Figure 5-9 Regional access statistical report



Step 4 (Optional) Click  to the upper right of the report and set parameters in the **Report Export** dialog box to save the report as an Excel file to a local disk drive.

Step 5 (Optional) Click  to print the report.

----End

5.4 PCI-DSS Compliance Reports

PCI-DSS compliance reports do not work on WAF in mirroring mode.

Based on the Payment Card Industry Security Standards (PCI-DSS), WAF performs a PCI-DSS compliance test for a specified website. Then WAF exports test results as a PCI-DSS compliance report in HTML format, and provides suggestions or solutions for configurations that partially meet or do not meet PCI-DSS requirements. The main contents of the test include website protection status and policies, and the status and work mode of the operating interface of WAF.

After configuring a protection policy for a website, a system administrator can generate a PCI-DSS compliance report to find out configurations that do not meet PCI-DSS requirements. Therefore, the system administrator can tune website configurations in time, enhancing the protection effect.

Generating a PCI-DSS Compliance Report

WAF can store a maximum of 100 PCI-DSS compliance reports. After the number of stored PCI-DSS compliance reports reaches 100, if you want to save new PCI-DSS compliance reports, you need to delete some stored PCI-DSS compliance reports. After WAF generates a new report, you need to click **Refresh** in the upper-right corner to refresh the report list.

To generate a PCI-DSS compliance report, perform the following steps:

Step 1 Choose **Logs & Reports > PCI-DSS Compliance Report**.

Figure 5-10 PCI-DSS Compliance Report page

Step 2 Set the query conditions.

Table 5-5 Parameters for generating a PCI-DSS compliance report


Parameter	Description
Report Name	Report name. The default value is default .
Website	Websites for which a PCI-DSS compliance test is performed. You can select one or multiple websites.

Step 3 Click **Generate**.

WAF generates the report in background and adds information about the generated report to the report list shown in [Figure 5-10](#).

----End

Downloading a Report

In the PCI-DSS compliance report list shown in [Figure 5-10](#), click  in the **Operation** column and **Save** in the displayed dialog box, to download a report as an XML file to a local directory.

Viewing a Report

To view a PCI-DSS compliance report, you need to download it to a local directory and view it in a browser, as shown in [Figure 5-11](#). WAF provides suggestions for configurations that partially meet or do not meet PCI-DSS requirements.


A system administrator can tune website configurations based on the report, effectively enhancing WAF's protection for the website.

Figure 5-11 PCI-DSS compliance report

PCI-DSS Compliance Report from NSFOCUS Web Application Firewall					
Generation Time: 2016-03-30 11:11:09					
Note: NSFOCUS WAF assists organizations to achieve Payment Card Industry Data Security Standards (PCI DSS) compliance. The PCI DSS compliance report from NSFOCUS WAF is used for program evaluation, but is not a substitute for a PCI audit report issued by qualification certification organizations QSA/ASV.					
Website Group Name: test Website Name: test IP: 172.16.12.94 Port: 80 Compliance Verification Result:					
PCI Section	PCI Directive	Fully Satisfied	Partially Satisfied	Unsatisfied	Solution
2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.			Yes	Make sure that Server Type is set to HTTPS for the website.
3.3	Display PAN to cover (up to display the first six and last four digits), it has only a legitimate business need square can see the full PAN.			Yes	Make sure that the website group to which the website belongs is enabled with the Sensitive Information Filtering policy, in which Action is set to Block/Replace.
4.1	Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.			Yes	Make sure that Server Type is set to HTTPS for the website.
6.1	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	Yes			WAF supports manual update of the rule database, and each rule is classified into high, medium, or low by hazard severity. Websites protected by WAF comply with this specification.
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.		Yes		Make sure that the website group to which the website belongs is enabled with the general protection policy, in which Action is set to Block/Redirect/Disguise and all SQL, LDAP, XPath, and command line injection protection rules are contained.

Deleting Reports

In the PCI-DSS compliance report list shown in [Figure 5-10](#), you can delete one or multiple reports at one time.

- Click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete a report.
- Select one or more reports, click **Bulk Delete**, and then click **OK** in the confirmation dialog box to delete the selected reports.

**Note**

WAF logs PCI-DSS compliance report operations, including starting generating, stopping generating, downloading, and deleting reports. You can view the logs after logging in to the web-based manager as an auditor.

6 Logs

The chapter describes detailed information about each type of logs. Login logs and operation logs are audit logs and can be viewed by auditors only. Other logs can be viewed by administrators and common users authorized by administrators. For information about the default administrator and auditor, see appendix [A Default Parameters](#).

It covers the following topics:

Topic	Description
Querying Security Protection Logs	Describes how to view security protection logs of WAF-protected servers, including network-layer access control logs, DDoS protection logs, web security logs, high-risk IP blocking logs, web anti-defacement logs, ARP protection logs, web access logs, and session tracing logs.
Querying Traffic Control Logs	Describes how to view traffic control logs.
Querying System Running Logs	Describes how to view system running logs.
Querying Login Logs	Describes how to view logs about login of users, including administrators and auditors.
Querying Operation Logs	Describes how to view logs about operations of users, including administrators and auditors.
Log Management Configuration	Describes how to configure log management parameters, such as parameters for backing up and sending logs.

6.1 Querying Security Protection Logs

Security protection logs include the following:

- [Web Security Logs](#)
- [Network-Layer Access Control Logs](#)
- [DDoS Protection Logs](#)
- [High-Risk IP Blocking Logs](#)
- [Web Anti-Defacement Logs](#)
- [ARP Protection Logs](#)
- [Web Access Logs](#)
- [Session Track Logs](#)

6.1.1 Web Security Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > Web Security Logs**.

Figure 6-1 Web Security Logs page

By default, the latest 1000 logs that meet query conditions are displayed. To view all logs, click **Query** to the right of **Last**.



Step 2 Set the query conditions.

Table 6-1 Parameters for querying web security logs



Parameter	Description
Date	Period when web security logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.
Event Type	Specifies web security event types, such as HTTP Validation and SQL Injection Attack .
Risk Level	Specifies risk levels of security events to be queried, including High , Medium , and Low .
Domain Name	Domain names of web security events to be queried. The domain names support both precise query and fuzzy query: <ul style="list-style-type: none"> = indicates precise query. >= indicates fuzzy query. != indicates contents excluded in the query.

Parameter	Description
URI	URI of web security events to be queried. NSFOCUS WAF support both precise query and fuzzy query based on URIs: <ul style="list-style-type: none"> = indicates precise query. >= indicates fuzzy query. != indicates contents excluded in the query.
Server/Client IP Address	Server/client IP addresses of web security events to be queried.
Server/Client Port	Server/client ports of web security events to be queried.
Client Location	Geographical location of the client of web security events to be queried.
Action	WAF's actions in web security events to be queried, such as Pass, Block, Accept, Redirection, Disguise, Clear, Replace, and Verification Code .
Method	HTTP request methods of web security events to be queried, such as GET and POST.
Proxy Information	Proxy information. For details, see section 4.11 Proxy Information Configuration .
Protocol Type	Protocol types of web security events to be queried.

Step 3 Click **Query** to view web security logs that meet query conditions.

- You can click a policy name in the **Matching Policy** column to view details about this common web protection policy.
- You can click a rule name in the **Matching Rule** column to view details about the rule used by the common web protection policy.
- You can click  in the **Operation** column view the event details, including website ID, HTTP request/response, and other information.
- Click  in the **Operation** column and select **Session Trace** or **Browser ID Tracing** to view the session tracing log of the web security log. For how to view session tracing logs, see section [6.1.8 Session Track Logs](#).

Step 4 (Optional) Add a policy.

- Click  in the **Operation** column and select **Add to Exception Policy**. The dialog box for creating an exception policy appears. For how to create an exception policy, see section [4.7.5.1 Exception Policy](#).
- Click  in the **Operation** column and select **Add to risk level policy**. The dialog box for creating a risk level policy appears. For how to create a risk level policy, see section [4.7.5.3 Risk Level Policy](#).

----End

6.1.2 Network-Layer Access Control Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > Network-Layer Access Control Logs**.

Figure 6-2 Network-Layer Access Control Logs page

The screenshot shows the 'Network-Layer Access Control Logs' page. At the top, there are navigation tabs: Web Security Logs, Network-Layer Access Control Logs (selected), DDoS Protection Logs, High-Risk IP Blocking Logs, Web Anti-Defacement Logs, ARP Protection Logs, Web Access Logs, and Session Track Logs. Below the tabs is a 'Conditions' section with a search icon and a dropdown arrow. It contains several filter groups: Date (with a 'between' dropdown and two date inputs), Server IP Address, Client IP Address, Server Port, Client Port, Policy ID, Matches, Action (with a dropdown set to 'Forward'), and Protocol (with a dropdown set to 'Unlimited'). A 'Query' button is at the bottom left of the conditions section. Below the conditions section, it says 'Page Number: 1 / 1' and 'Query Result: 0'. There are navigation buttons: First, Previous, Next, and Last. At the bottom, there is a table header with the following columns: Local Time, Event Type, Risk Level, Matches, Server IP:Port, Client IP:Port, Policy ID / Interface, Protocol, and Action. The table body is currently empty.

Step 2 Set the query conditions.

Table 6-2 Parameters for querying network-layer access control logs

Parameter	Description
Date	Period when network-layer access control events to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.
Server/Client IP Address	Specifies server/client IP addresses of network-layer access control events to be queried. Both IPv4 and IPv6 addresses are supported.
Server/Client Port	Server/client ports of network-layer access control events to be queried.
Policy ID	Policy IDs of network-layer access control events to be queried.
Matches	Number of times network-layer access control logs to be queried are generated.
Action	WAF's actions in network-layer access control events to be queried, including: <ul style="list-style-type: none"> Forward: WAF directly forwards the current packet without subsequent inspection. Block: WAF drops the current packet and terminates the current TCP connection. Accept: Without any processing, WAF lets the current packet go to subsequent inspections.
Protocol	Protocols of network-layer access control events to be queried, including Unlimited, ICMP, ICMPV6, TCP and UDP .

Step 3 Click **Query** to view network-layer access control logs that meet query conditions.

----End

6.1.3 DDoS Protection Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > DDoS Protection Logs**.

Figure 6-3 DDoS Protection Logs page

Step 2 Set the query conditions.

Table 6-3 Parameters for querying DDoS protection logs

Parameter	Description
Date	Period when DDoS protection logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> • <= plus a specific date: indicates the specific date and prior dates. • >= plus a specific date: indicates the specific date and subsequent dates. • Between plus two specific dates: indicates the period between the two specific dates.
Event Type	Event types of DDoS protection logs to be queried, including SYN_FLOOD Attack , ACK_FLOOD Attack , HTTP_FLOOD Attack , Collaboration Event , and Low-and-Slow Attack .
Action	WAF's actions in DDoS protection events, including: <ul style="list-style-type: none"> • Enter the Protected Status • Exit the Protected Status • Trigger divert threshold • DDoS Mitigated by ADS • DDoS Mitigated by WAF • Low-and-Slow Attack Started • Low-and-Slow Attack Ended
Server IP Address/Port	Server IP addresses and ports of DDoS protection logs to be queried.

Step 3 Click **Query** to view DDoS protection logs that meet query conditions.

----End

6.1.4 High-Risk IP Blocking Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > High-Risk IP Blocking Logs**.

Figure 6-4 High-Risk IP Blocking Logs page

Step 2 Set query conditions.

Table 6-4 Parameters for querying high-risk IP blocking logs

Parameter	Description
Date	Period when high-risk IP blocking logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.
Server IP Address	Server IP addresses of high-risk IP blocking logs to be queried. Both IPv4 and IPv6 addresses are supported.
Client IP Address	Client IP addresses of high-risk IP blocking logs to be queried. Both IPv4 and IPv6 addresses are supported.

Step 3 Click **Query** to view high-risk IP blocking logs that meet query conditions.

----End

6.1.5 Web Anti-Defacement Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > Web Anti-Defacement Logs**.

Figure 6-5 Web Anti-Defacement Logs page

Web Security Logs Network-Layer Access Control Logs DDoS Protection Logs High-Risk IP Blocking Logs Web Anti-Defacement Logs ARP Protection Logs Web Access Logs Session Track Logs

Q Conditions ▲

☐ Date between 2018-04-17 15:28 - 2018-04-17 15:28

☐ URL =

☐ Server IP Address

☐ Server Port

Query

Page Number: 1 / 1 Query Result: 0 First Previous Next Last

Date	Event Type	Server IP:Port	URL	Risk Level	Illegal Cause
------	------------	----------------	-----	------------	---------------

Step 2 Set the query conditions.

Table 6-5 Parameters for querying web anti-defacement logs

Parameter	Description
Date	<p>Period when web anti-defacement logs to be queried are generated. The value can be one of the following:</p> <ul style="list-style-type: none"> • <= plus a specific date: indicates the specific date and prior dates. • >= plus a specific date: indicates the specific date and subsequent dates. • Between plus two specific dates: indicates the period between the two specific dates.
URL	<p>URLs of web anti-defacement logs to be queried.</p> <p>WAF supports both precise query and fuzzy query based on URLs:</p> <ul style="list-style-type: none"> • = indicates precise query. • >= indicates fuzzy query. • != indicates contents excluded in the query.
Server IP Address/Port	<p>Server IP addresses and ports of web anti-defacement logs to be queried. Both IPv4 and IPv6 addresses are supported.</p>

Step 3 Click **Query** to view web anti-defacement logs that meet query conditions.

----End

6.1.6 ARP Protection Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > ARP Protection Logs**.

Figure 6-6 ARP Protection Logs page

Step 2 Set the query conditions.

Table 6-6 Parameters for querying ARP protection logs

Parameter	Description
Date	Period when ARP protection logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.
Attack Type	Attack types of ARP protection logs to be queried, including Illegal ARP Packet , MAC Collision , and Gateway-Type ARP Spoofing .
Source/Destination IP	Source/destination IP addresses in ARP protection logs to be queried.
Source/Destination MAC	Source/destination MAC addresses in ARP protection logs to be queried.
Binding IP/MAC	Binding IP addresses/MAC addresses of ARP protection logs to be queried. For details about IP/MAC binding, see section 4.2.4 Configuring ARP Spoofing Protection .
Conflicted MAC	Conflicting MAC addresses of ARP attack source hosts and servers. These MAC addresses conflict with MAC addresses or binding MAC addresses listed in the Auto-Learning MAC Address Table under Security Management > Network-Layer Protection > ARP Spoofing Protection .
Matches	Matches of ARP protection logs to be queried.
Action	WAF's actions in ARP protection logs to be queried, including Pass , Block , Accept , and Redirection .
Status	Attack status in ARP protection logs to be queried, which can be Attempting or Attack Succeeded .

Step 3 Click **Query** to view ARP protection logs that meet query conditions.

----End

6.1.7 Web Access Logs

You can view web access logs of a website only after the web access log function is enabled for the website. For how to enable the web access log function, see section [4.3.1.1 Creating a Website Group](#).

Step 1 Choose **Logs & Reports > Security Protection Logs > Web Access Logs**.

Figure 6-7 Web Access Logs page

Web Security Logs Network-Layer Access Control Logs DDoS Protection Logs High-Risk IP Blocking Logs Web Anti-Defacement Logs ARP Protection Logs Web Access Logs Session Track Logs

Conditions

☐ Date 2018-04-17 15:30 - 2018-04-17 15:30

☐ Server IP Address

☐ Client IP Address

☐ Server Port

☐ Client Port

☐ Method

☐ URI

☐ Matches

☐ Browser Agent

☐ Domain Name

☐ Referrer

☐ Protocol Type

☐ Client Location

Query

Page Number: 1 / 1 Query Result: 0 First Previous Next Last Query ?

Local Time	Event Type	Matches	Server IP:Port	Client IP:Port	Protocol Type	URI	Domain Name	Browser Agent	Method	Operation
------------	------------	---------	----------------	----------------	---------------	-----	-------------	---------------	--------	-----------

By default, the latest 1000 logs that meet query conditions are displayed. To view all logs, click **Query** to the right of **Last**.

Step 2 Set the query conditions.



Table 6-7 Parameters for querying web access logs

Parameter	Description
Date	Period when web access logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.
Server/Client IP Address	Server/client IP addresses in web access logs to be queried. Both IPv4 and IPv6 addresses are supported.
Server/Client Port	Server/client ports in web access logs to be queried.
Method	HTTP request methods in web access logs to be queried, such as GET and POST .
URI	URL of web access events to be queried. WAF supports both precise query and fuzzy query based on URIs:

Parameter	Description
	<ul style="list-style-type: none"> = indicates precise query. >= indicates fuzzy query. != indicates contents excluded in the query.
Matches	Number of times web access logs to be queried are generated.
Browser Agent	Browsers of web access logs to be queried.
Domain Name	Domain names in web access logs to be queried.
Referer	Referer content in web access logs to be queried.
Protocol Type	Protocol types of web access logs to be queried.
Client Location	Geographical location of web access events to be queried.

Step 3 Click **Query** to view web access logs that meet query conditions.

Step 4 (Optional) Operate on logs.

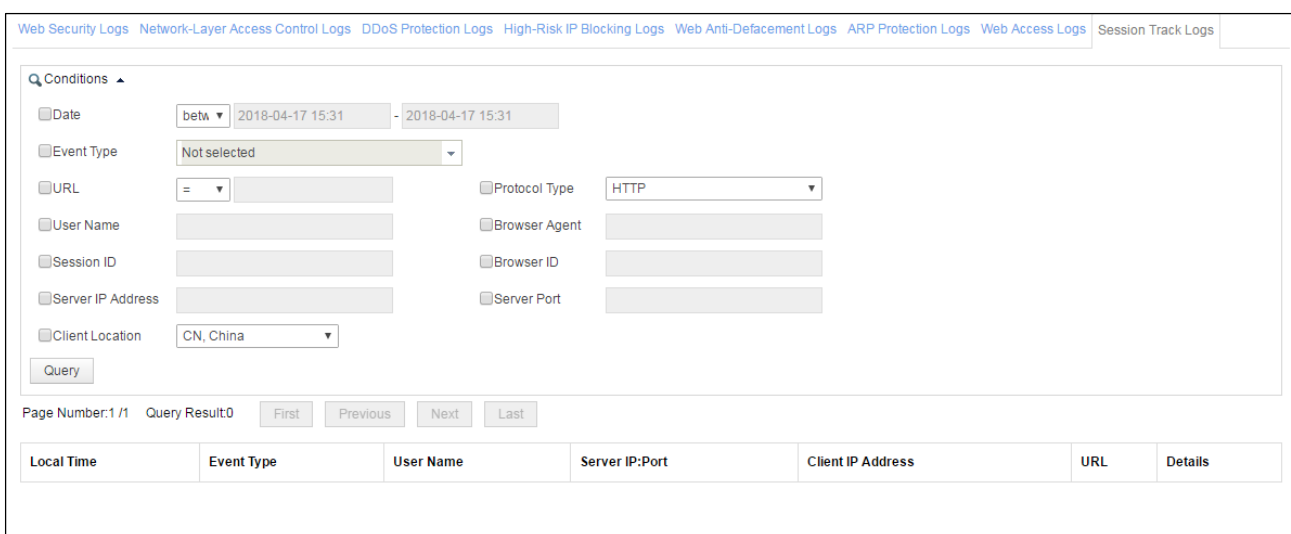
- You can click  in the **Operation** column to view the log details, including website ID, access date, and other information.
- Click  in the **Operation** column and select **Session Trace** or **Browser ID Tracing** to view the session tracing log of the web access log. For how to view session tracing logs, see section [6.1.8 Session Track Logs](#).

----End

6.1.8 Session Track Logs

Step 1 Choose **Logs & Reports > Security Protection Logs > Session Track Logs**.

Figure 6-8 Session Track Logs page



The screenshot displays the 'Session Track Logs' page. At the top, there is a navigation bar with links: Web Security Logs, Network-Layer Access Control Logs, DDoS Protection Logs, High-Risk IP Blocking Logs, Web Anti-Defacement Logs, ARP Protection Logs, Web Access Logs, and Session Track Logs (selected). Below the navigation bar is a 'Conditions' section with a search icon and a dropdown arrow. It contains several filter fields: Date (between 2018-04-17 15:31 and 2018-04-17 15:31), Event Type (Not selected), URL (with an equals sign dropdown), Protocol Type (HTTP), User Name, Browser Agent, Session ID, Browser ID, Server IP Address, Server Port, and Client Location (CN, China). A 'Query' button is at the bottom of the filter section. Below the filters, it shows 'Page Number: 1/1' and 'Query Result: 0', along with 'First', 'Previous', 'Next', and 'Last' buttons. At the bottom is a table with the following headers: Local Time, Event Type, User Name, Server IP:Port, Client IP Address, URL, and Details.

Step 2 Set the query conditions.

Table 6-8 Parameters for querying session tracing logs

Parameter	Description
Date	Species a period when session tracing logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none">• <= plus a specific date: indicates the specific date and prior dates.• >= plus a specific date: indicates the specific date and subsequent dates.• Between plus two specific dates: indicates the period between the two specific dates.
Event Type	Event types of session tracing logs to be queried, including Secure Data Transfer and SQL Injection Attack .
URL	URL of session tracing access events to be queried. WAF supports both exact query and fuzzy query based on URIs: <ul style="list-style-type: none">• = indicates exact query.• >= indicates fuzzy query.• != indicates contents excluded in the query.
Protocol Type	Protocol types of session tracing logs to be queried, which can be HTTP or HTTPS .
User Name	User name of the session tracing logs to be queried.
Browser Agent	Browser of session tracing logs to be queried.
Session ID	Session ID of session tracing logs to be queried, namely, the cookie that contains WAF_Session_Id (WSI) delivered by WAF.
Browser ID	Browser ID of session tracing logs to be queried, namely, the cookie that contains WAF_Client_Id (WCI) delivered by WAF.
Server Address/Port	IP Server/client IP addresses of session tracing logs to be queried. Both IPv4 and IPv6 addresses are supported.
Client Location	Geographical location of session tracing events to be queried.

Step 3 Click **Query** to view session tracing logs that meet query conditions.

----End

6.2 Querying Traffic Control Logs

Traffic control logs are available only when WAF is deployed in reverse proxy mode.

Step 1 Choose **Logs & Reports > Traffic Control Logs**.

Figure 6-9 Traffic Control Logs page

Step 2 Set the query conditions.

Table 6-9 Parameters for querying traffic control logs

Parameter	Description
Actual Uplink Rate	Actual uplink rate of traffic control logs to be queried. The traffic rate is greater than, equal to, or smaller than a specified value.
Actual Downlink Rate	Actual downlink rate of traffic control logs to be queried. The traffic rate is greater than, equal to, or smaller than a specified value.
Upper Traffic Limit	Upper traffic limit of traffic control logs to be queried. The upper traffic limit is greater than, equal to, or smaller than a specified value.
Object Name	Keyword in traffic control object names of traffic control logs to be queried.
Event Type	Traffic control status in traffic control logs to be queried, which can be Traffic control started or Traffic control ended .
Date	Period when traffic control logs to be queried are generated. The value can be one of the following: <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.

Step 3 Click **Query** to view traffic control logs that meet query conditions.

----End

6.3 Querying System Running Logs

Step 1 Choose **Logs & Reports > System Running Logs > Running Logs**.

Figure 6-10 Running Logs page

Security Protection Logs Traffic Control Logs **System Running Logs** Security Reports Traffic Reports Regional Access Statistical Report PCI-DSS Compliance Report more Online Help

Running Logs

Conditions

☐ Date between 2018-04-17 15:35 - 2018-04-17 15:35

☐ Type Host Start-Stop Control

☐ Source Interface Open-Close

☐ Description

Query

Page Number: 1 / 70 Query Result: 1394 First Previous Next Last

Date	Type	Source	Description
2018-04-17 15:35:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.
2018-04-17 15:34:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.
2018-04-17 15:33:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.
2018-04-17 15:32:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.
2018-04-17 15:31:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.
2018-04-17 15:30:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.
2018-04-17 15:29:13	Device Resource Status	System Monitoring	Disk / usage 90% is over the alert mode threshold value 90%.

Step 2 Set the query conditions.

Table 6-10 Parameters for querying system running logs

Parameter	Description
Date	<p>Period when system running logs to be queried are queried. The value can be one of the following:</p> <ul style="list-style-type: none"> <= plus a specific date: indicates the specific date and prior dates. >= plus a specific date: indicates the specific date and subsequent dates. Between plus two specific dates: indicates the period between the two specific dates.
Type	<p>Running status change type of system running logs to be queried, which can be one of the following:</p> <ul style="list-style-type: none"> Host Start-Stop Control Service Start-Stop Control Database Startup-Shutdown Control Engine Startup-Shutdown Control WEB Service Start-Stop Control Link Status Change Emergency Mode Switching ADS Collaboration Rule Upgrade Device Resource Status
Source	Specific operation that triggers the log to be queried, which can be Interface Open-

Parameter	Description
	Close, Normal System Startup-Shutdown, Engine Startup-Shutdown Control, or System Monitoring.
Description.	Brief description of system running logs to be queried.

Step 3 Click **Query** to view system running logs that meet query conditions.

---End

6.4 Querying Login Logs

After login, an auditor can view login logs of various accounts on the **Login Logs** page.

Step 1 Choose **Audit Logs** > **Login Logs** > **Login Logs**.

Figure 6-11 Login logs

Login Logs				
Conditions <div> <input type="checkbox"/> Date between <div> 2015-05-14 11:28 2015-05-14 11:28 </div> </div> <input type="checkbox"/> Client IP Address <div> <input type="checkbox"/> User </div> <input type="checkbox"/> Client Port <div> <input type="checkbox"/> Operation Result Succeeded </div> <input type="checkbox"/> Action Login				
Query				
Page Number: 1 / 26 Query Result: 515				
Homepage Previous Next Last				
Date	Client IP:PORT	User	Action	Operation Result
2015-05-14 11:27:24	192.168.5.237:55733	auditor	Login	Succeeded
2015-05-14 11:27:05	192.168.5.237:65059	admin	Exit	Succeeded
2015-05-14 11:26:38	10.67.3.69:50307	auditor	Login	Succeeded
2015-05-14 11:18:49	192.168.5.237:55924	admin	Login	Succeeded
2015-05-14 11:18:20	192.168.5.237:54839	auditor	Login	Failed
2015-05-14 11:18:12	192.168.5.237:54839	auditor	Login	Failed
2015-05-14 11:17:41	192.168.5.237:49249	auditor	Login	Failed
2015-05-14 11:17:20	192.168.5.237:59363	admin	Exit	Succeeded
2015-05-14 09:15:22	192.168.5.237:49999	admin	Login	Succeeded
2015-05-14 09:11:12	192.168.5.161:53145	admin	Login	Succeeded
2015-05-14 09:07:29	192.168.5.30:50230	admin	Login	Succeeded
2015-05-13 18:55:28	192.168.6.142:54073	admin	Exit	Succeeded
2015-05-13 18:39:39	192.168.6.142:53875	admin	Login	Succeeded

Step 2 Set the query conditions.

Table 6-11 Parameters for querying login logs

Parameter	Description
Date	Period when login logs are generated. The value can be one of the following: <ul style="list-style-type: none"> • <= plus a specific date: indicates the specific date and prior dates. • >= plus a specific date: indicates the specific date and subsequent dates. • Between plus two specific dates: indicates the period between the two specific dates.
Client IP Address	Client IP address of login logs to be queried. Both IPv4 and IPv6 addresses are supported.
User	User account of login logs to be queried.
Client Port	Client port of login logs to be queried.
Operation Result	Action result (Failed or Succeeded) of login logs to be queried.
Action	User action (Login or Exit) of login logs to be queried.

Step 3 Click **Query** to view login logs that meet query conditions.

----End

6.5 Querying Operation Logs

After login, an auditor can view WAF operation logs of various accounts on the **Operation Logs** page.

Step 1 Choose **Audit Logs > Operation Logs > Operation Logs**.

Figure 6-12 Operation logs

Operation Logs

Conditions

Date

between

2015-05-14 11:29

2015-05-14 11:29

Client IP Address

Operation Type

System Enable-D

User

Operation Result

Succeeded

Query

Page Number:1 /83 Query Result:1651

Homepage

Previous

Next

Last

Date	Client IP Address	User	Operation Type	Description	Operation Result
2015-05-14 11:21:36	192.168.5.237	admin	User Management	Account auditor is unlocked.	Succeeded
2015-05-14 11:20:18	192.168.5.237	admin	User Management	Disable user.testtest	Succeeded
2015-05-14 11:18:20	192.168.5.237	system	User Management	Account auditor is locked due to login failures.	Succeeded
2015-05-14 10:22:12	192.168.5.237	admin	Test Tools	Perform packet capture.	Succeeded
2015-05-14 10:20:40	192.168.5.237	admin	License Update	Update License	Failed
2015-05-14 10:11:43	192.168.5.237	admin	Logs & Reports	Generate Area Access Statistical Report,Time: 2015-04-01 00:00--2015-04-30 23:59	Succeeded
2015-05-14 10:11:38	192.168.5.237	admin	Logs & Reports	Generate Area Access Statistical Report,Time: 2015-04-01 00:00--2015-04-30 23:59	Succeeded
2015-05-14 10:11:34	192.168.5.237	admin	Logs & Reports	Generate Area Access Statistical Report,Time: 2015-04-01 00:00--2015-04-30 23:59	Succeeded
2015-05-14 10:10:22	192.168.5.237	admin	Logs & Reports	Generate Area Access Statistical Report,Time: 2015-04-01 00:00--2015-04-30 23:59	Succeeded

Step 2 Set the query conditions.

Table 6-12 Parameters for querying operation logs

Parameter	Description
Date	<p>Period when operation logs are generated. The value can be one of the following:</p> <ul style="list-style-type: none"> • <= plus a specific date: indicates the specific date and prior dates. • >= plus a specific date: indicates the specific date and subsequent dates. • Between plus two specific dates: indicates the period between the two specific dates.
Client IP Address	Client IP address of operation logs to be queried. Both IPv4 and IPv6 addresses are supported.
User	User account of operation logs to be queried.
Operation Type	<p>Operation type of operation logs to be queried, which can be one of the following:</p> <ul style="list-style-type: none"> • System Enable-Disable • License Update • System Upgrade • System Configuration • Security Configuration • User Management • Logs & Reports • Test Tools
Operation Result	Operation result (Failed or Succeeded) of operation logs to be queried.

Step 3 Click **Query** to view operation logs that meet query conditions.

----End

6.6 Exporting Logs

After login, an auditor can not only view login logs and operation logs of various accounts but also export, download, and clear these logs.

Choose **Audit Logs > Export Logs > Export Logs**.

Figure 6-13 Export Logs page

Export Logs		
Log Type	Download	Operation
Login Logs		Export by Period Export All Clear Files
Operation Logs		Export by Period Export All Clear Files

Exporting Logs

Exporting logs means saving logs as files in other storage media. Periodical log export is a good way to clear storage space.

On the **Export Logs** page shown in [Figure 6-13](#), click an export button in the **Operation** column.

The following uses login logs as an example to show how to export logs:

- To export login logs by period, click **Export by Period**, set a period, and click **Start Export**. Exported logs will appear in the **Download** column.
- To export all login logs, click **Export All**. Exported logs will appear in the **Download** column.

Downloading Logs

You can download exported logs to a local disk drive. In the **Download** column on the **Export Logs** page shown in [Figure 6-13](#), click a desired log file, and save the log file to a local disk drive.

Clearing Log Files

On the **Export Logs** page shown in [Figure 6-13](#), click **Clear Files** in the **Operation** column to clear a type of exported log files appearing in the **Download** column.



Clicking **Clear Files** only clears exported log files appearing in the **Download** column, and has no impact on original log information in the database.

6.7 Log Management Configuration

You can export and back up system logs in the following ways:

- Direct export and backup
- Via syslog
- Via SNMP

6.7.1 Log Export and Backup

Choose **Logs & Reports > Log Management > Log Export & Backup**. You can export, download, and clear various web security logs.

Figure 6-14 Log Export & Backup page

Log Export & Backup		
Syslog Configuration SNMP Configuration Log Sending Parameter Configuration A Interface Configuration Sensitive Parameter Config		
Log Type	Download	Operation
Web Security Logs		Export by Period Export All Clear Database Clear Files
Network-Layer Access Control Logs		Export by Period Export All Clear Database Clear Files
DDoS Protection Logs		Export by Period Export All Clear Database Clear Files
High-Risk IP Blocking Logs		Export by Period Export All Clear Database Clear Files
Web Anti-Defacement Logs		Export by Period Export All Clear Database Clear Files
ARP Protection Logs		Export by Period Export All Clear Database Clear Files
Web Access Logs		Export by Period Export All Clear Database Clear Files
		Clear Logs & Reports

Exporting Logs

Exporting logs means saving logs as files in other storage media. Periodical log export is a good way to release storage space.

On the **Log Export & Backup** page in [Figure 6-14](#), click an export button in the **Operation** column.

The following uses web security logs as an example to show how to export logs:

- To export web security logs by period, click **Export by Period**, set a period, and click **Start Export**. Exported logs will appear in the **Download** column.


- To export all web security logs, click **Export All**. Exported logs will appear in the **Download** column.

Downloading Logs

You can download exported logs to a local disk drive. In the **Download** column of the **Log Export & Backup** page shown in [Figure 6-14](#), click a desired log file, and save the log file to a local disk drive.


Clearing Log Files

On the **Log Export & Backup** page shown in [Figure 6-14](#), click **Clear Files** in the **Operation** column to clear a type of exported log files appearing in the **Download** column.

	<p>Clicking Clear Files only clears exported log files appearing in the Download column, and has no impact on original log information in the database.</p>
---	---

Clearing the Database


On the **Log Export & Backup** page shown in [Figure 6-14](#), click **Clear Database** in the row of a log type to clear the type's original log information from the database.

	<p>Log information in the database cannot be recovered once being deleting. Perform deletion only when necessary.</p>
---	---

Clearing Logs and Reports

On the **Log Export & Backup** page, click **Clear Logs & Reports** to clear the following contents:

- Data in the database, including engine/interface traffic, engine connections, and security protection logs
- Reports and processing data files generated based on data in the database

	<p>Data in the database, reports generated based on the data, and processing data files generated based on the data cannot be recovered once deleted. Perform deletion only when necessary.</p>
---	---

6.7.2 Syslog

WAF can send logs to a syslog server for storage. Choose **Logs & Reports > Log Management > Syslog Configuration**. By default, the **Syslog Configuration** page shows a list of IP addresses and ports of configured syslog servers. You can add or delete desired syslog servers.

Figure 6-15 Syslog Configuration page



The syslog configuration needs to be used in conjunction with log sending parameters. For details about log sending parameters, see section [6.7.4 Log Sending Parameters](#).

Adding a Syslog Server

Perform the following steps to add a syslog server:


Step 1 Click **Add** in the lower-right corner of the list shown in [Figure 6-15](#).

Figure 6-16 Adding a syslog server

Step 2 Set the server IP address and port, and click **Save**.

----End

Deleting a Syslog Server

In the list shown in [Figure 6-15](#), click  in the **Operation** column and click **OK** in the confirmation dialog box.

Enabling or Disabling the Syslog Service

On the page shown in [Figure 6-15](#), after selecting **Yes** for **Enable Syslog**, you need to configure the method for saving the log content to the syslog server, which can be **Plaintext** or **Base64 encoding**.

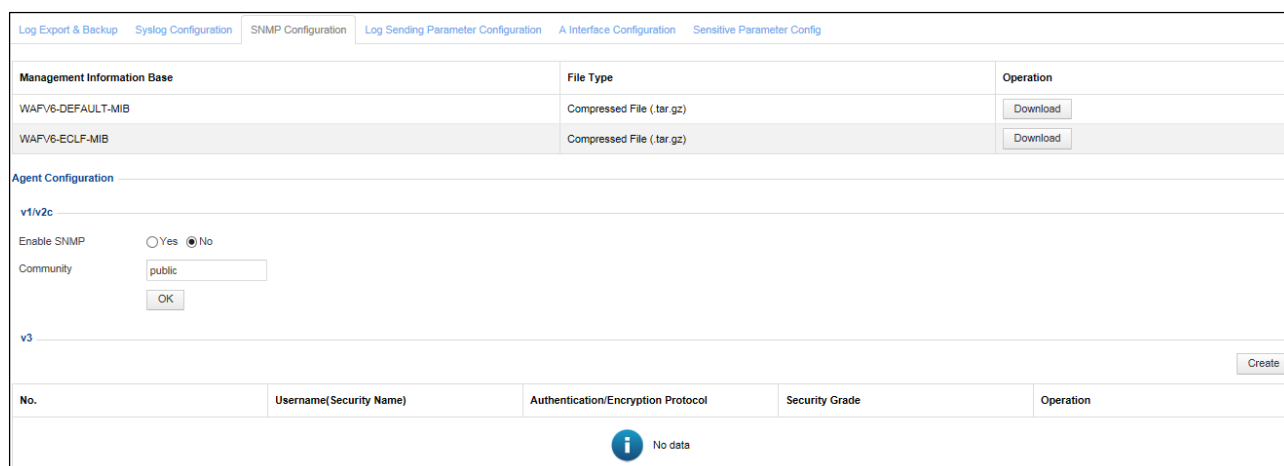
Click **OK** to commit the settings.

To disable the syslog server, select **No** for **Enable Syslog**.

6.7.3 SNMP

WAF can send logs to an SNMP server for storage. Choose **Logs & Reports > Log Management > SNMP Configuration**.

Figure 6-17 SNMP Configuration page



The screenshot shows the 'SNMP Configuration' page with several tabs: 'Log Export & Backup', 'Syslog Configuration', 'SNMP Configuration' (active), 'Log Sending Parameter Configuration', 'A Interface Configuration', and 'Sensitive Parameter Config'.

Management Information Base

	File Type	Operation
WAFV6-DEFAULT-MIB	Compressed File (.tar.gz)	Download
WAFV6-ECLF-MIB	Compressed File (.tar.gz)	Download


Agent Configuration

v1/v2c

Enable SNMP: ☐ Yes ☒ No

Community:

v3

No.	Username(Security Name)	Authentication/Encryption Protocol	Security Grade	Operation
 No data				



The SNMP configuration needs to be used in conjunction with log sending parameters. For details about log sending parameters, see [section 6.7.4 Log Sending Parameters](#).

6.7.3.1 Downloading the Management Information Base

Click **Download** in the page shown in [Figure 6-17](#) to download the management information base (MIB) file of WAF to a local disk drive.

Which MIB file is used depends on the log standard selected for web access logs (WEB_ACL) on the **Log Sending Parameter Configuration** page. For example,

- If **WAF_DEFAULT** is selected, WAFV6-DEFAULT-MIB is used.
- If **APACHE_ECLF** is selected, WAFV6-ECLF-MIB is used.

6.7.3.2 Configuring an SNMP Agent

WAF supports SNMPv1, v2c, and v3. This section describes SNMP agents of the three versions.

Configuring an SNMPv1/v2c Agent

Step 1 On the page shown in [Figure 6-17](#), select **Yes** for **Enable SNMP** and set **Community** in the **v1/v2c** area under **Agent Configuration**.

Step 2 Click **OK** to save the settings.

----End

Configuring an SNMPv3 Agent

Before configuring an SNMPv3 agent, you must enable SNMP.

Step 1 On the page shown in [Figure 6-17](#), select **Yes** for **Enable SNMP** in the **v1/v2c** area under **Agent Configuration**.

Step 2 Click **Create** to the upper right of the SNMP agent table in the **v3** area.

Figure 6-18 Creating an SNMPv3 agent

Step 3 Set parameters in the **Add** dialog box.

Table 6-13 Parameters for creating an SNMPv3 agent

Parameter	Description
User Name	Specifies the SNMPv3 user name.
Authentication Protocol	Specifies the protocol used for authentication, which can be MD5 or SHA .
Authentication Key	Specifies the key used for authentication.
Encryption Protocol	Specifies the encryption algorithm used for transmitting messages, which can be DES or AES .
Encryption Key	Specifies the key used for encryption.
Security Grade	Specifies the minimum security level for a user's access, which can be Not authenticated , Authenticated , or Authenticated and encrypted .

Step 4 Click **OK** to save the settings.

----End

6.7.3.3 Configuring SNMP Trap

Before configuring SNMP trap of different versions, you must enable SNMP. This section describes how to configure SNMP trap of different versions.

Configuring an SNMPv1/v2c Server

Step 1 On the page shown in [Figure 6-17](#), click **Create** in the **v1/v2c** area under **Trap Configuration** to add an SNMPv1/v2c server.

Figure 6-19 Adding an SNMPv1/v2c server

Step 2 Set the server IP address, port, and community, and click **Save**.

----End

Configuring an SNMPv3 Server

Step 1 On the page shown in [Figure 6-17](#), click **Create** in the **v3** area under **Trap Configuration** to add an SNMPv3 server.

Figure 6-20 Adding an SNMPv3 server

The 'Add' dialog box contains the following fields and options:

- Destination Host ***: Text input field.
- Receiving Port ***: Text input field.
- User Name ***: Text input field with a help icon.
- Authentication Protocol**: Radio buttons for **MD5** (selected) and **SHA**.
- Authentication Key ***: Text input field with a help icon.
- Encryption Protocol**: Radio buttons for **DES** (selected) and **AES**.
- Encryption Key ***: Text input field with a help icon.
- Security Grade**: Radio buttons for **Not authenticated** (selected), **Authenticated**, and **Authenticated and encrypted**.
- engineID ***: Text input field with a help icon.
- Buttons**: **Save** and **Cancel** buttons at the bottom.

Step 2 Set parameters in the **Add** dialog box.

Table 6-14 Parameters for configuring SNMPv3 trap

Parameter	Description
Destination Host	Specifies the host that receives SNMP trap alerts sent by WAF. You can type an IPv4 or IPv6 address, for example, 192.168.1.0 or 2001:abcd:123:1::.
Receiving Port	Specifies the port for receiving SNMP trap alerts.
User Name	Specifies the SNMPv3 user name.
Authentication Protocol	Specifies the protocol used for authentication, which can be MD5 or SHA .
Authentication Key	Specifies the key used for authentication.
Encryption Protocol	Specifies the encryption algorithm used for transmitting messages, which can be DES or AES .
Encryption Key	Specifies the key used for encryption.
Security Grade	Specifies the minimum security level for a user's access, which can be Not authenticated , Authenticated , or Authenticated and encrypted .
engineID	Specifies the ID of the SNMP engine. The ID is a 16-bit hexadecimal digit without starting with 0x.

Step 3 Click **OK** to save the settings.

----End

6.7.4 Log Sending Parameters

WAF allows users to set log sending parameters specific to log types. Log sending parameters include syslog parameters, SNMP parameters, and A Interface parameters.

Step 1 Choose **Logs & Reports > Log Management > Log Sending Parameter Configuration**.

Figure 6-21 Log Sending Parameter Configuration page

Log Export & Backup Syslog Configuration SNMP Configuration Log Sending Parameter Configuration A Interface Configuration Sensitive Parameter Config				
<input type="button" value="Save"/> <input type="button" value="Reset"/> <input type="button" value="Show default settings"/>				
Log Type	Store Locally	Syslog Parameters	SNMP Parameters	Interface A Parameters ⓘ
HTTP Protocol Validation	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Web Server Bug	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Web Plugin Bug	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Spider_Anti	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Scan_Anti	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
CSRF	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
File_Upload_Limit	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Cross_Site_Scripting	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
SQL_Injection	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
LDAP_Injection	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
SSI	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
XPATH	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
OS_CMD_Injection	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Path_Traversal	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
RFI	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Directory_Index	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Info_Leak	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Content_filter	<input type="checkbox"/>	<input checked="" type="checkbox"/> Enable Severity: <input type="text" value="Error"/>	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable

Step 2 Set the log sending parameters.

Table 6-15 Log sending parameters

Parameter	Description
Log Type	Log type, such as HTTP Protocol Validation , Web Server Bug , and Web Plugin Bug .
Store Locally	Whether to store various types of logs on WAF locally. For web access logs, local store is enabled by default. If it is disabled, web access logs will not be included in WAF's database, but are still available on ESPC by using "MSS for WAF".
Syslog Parameters	Parameters for exporting logs via syslog. Enable : controls whether to enable the syslog service for the specified log type.

Parameter	Description
	<p>Severity: risk level of logs. There are eight levels, which are listed as follows in a low-to-high order:</p> <ul style="list-style-type: none"> • Debugging message • Notification message • Common but important • Warning • Error • Critical • Immediate measure required • System unavailable
SNMP Parameters	<p>Parameters for exporting logs via SNMP.</p> <p>Enable: controls whether to enable the SNMP service for the specified log type.</p>
Interface A Parameters	<p>Parameters for exporting logs to NSFOCUS ESPC over the A interface.</p> <p>Enable: controls whether to enable the A interface service for the specified log type.</p>

Step 3 Click **OK** to save the settings.

You can click **Reset** to cancel your setting.

You can click **Display Default Configuration** to reset log sending parameters to the default setting.

----End

6.7.5 A Interface Configuration

WAF uploads data to NSFOCUS Cloud or ESPC only via the A interface. In this case, you need to enable the A interface. This interface is enabled by default. If it is disabled, enable it as follows:

Step 1 Choose **Logs & Reports > Log Management > A Interface Configuration**.

Figure 6-22 A Interface Configuration page

Log Export & Backup Syslog Configuration SNMP Configuration Log Sending Parameter Configuration **A Interface Configuration** Sensitive Parameter Config

A Interface ☒ Enable ☐ Disable

OK

Step 2 Select **Enable**.

Step 3 Click **OK** to save the settings.

----End

6.7.6 Sensitive Parameter Configuration

Sensitive parameter configuration does not work on WAF in mirroring mode.

After sensitive data masking is enabled and sensitive parameters are specified, if a request URL contains a specified sensitive parameter, the field corresponding to the sensitive parameter will be recorded by WAF to a web access log and web security log, with the field content being shielded.

For example, if "username" is specified as a sensitive parameter and a request URL <http://10.67.1.205/py/xssResponse.php?username=123456> is detected, then:

- In the web access log, the URL will be recorded as `"/py/sqlResponse.php?testid=1+&username=%5b**\x0A*****%5d\x0A"`.
- In the web security log, the URL will be recorded as `"/py/sqlResponse.php?testid=1 or 1=1&username=[*****]"`.



If the parameter content contains both sensitive information and an attack signature, the content will not be shielded.

To configure sensitive parameters, perform the following steps:

Step 1 Choose **Logs & Reports > Log Management > Sensitive Parameter Config**.

Figure 6-23 Sensitive Parameter Config page

Step 2 Select **Enable** for **Sensitive Data Masking** and type sensitive parameters in the text box.

Multiple sensitive parameters should be separated by semicolons.

Step 3 Click **OK** to save the settings.

----End

7 System Management

This chapter covers the following topics:

Topic	Description
Network Configurations	Describes how to manage work groups, configure routes, and configure DNS servers and domain names.
System Deployment	Describes how to configure the running mode, HA, BYPASS, and VRRP and manage VRRP configuration information.
System Tools	Describes how to use system tools.
Test Tools	Describes how to use test tools.
Collaboration with ESPC	Describes how to connect WAF to ESPC.
User Management	Describes how to manage users.
Traffic Control Management	Describes how to conduct traffic control.
System Configuration Parameter	Describes how to configure system engine parameters as a maintainer.
SSL Acceleration	Describes how to enable/disable the SSL card.
System O&M	Describes how to collect WAF-related information and restore system.
REST API	Describes how to manage digital signatures.
Site Control	Describes how to perform HTTPS website control.

7.1 Network Configurations

Network configurations include the following parts:

- Work group management
- Route configuration
- DNS configuration

7.1.1 Work Group Management

A work group means a working interface group. You can manage work groups on the **Work Group Management** pages that vary with system deployment modes. System deployment

modes include in-path, out-of-path, reverse proxy, and mirroring modes. For the setting of system deployment mode, see section [7.2.1 Running Mode Configuration](#).



By default, the M interface or both the M interface and H1 interface serve as the default management interfaces. Working interface names are in the format of G plus integer/integer (for example, G1/1 and G1/2). In earlier versions, working interface names are in the format of "eth" plus integer (for example, eth 0 and eth 1). In this section, WAF NX3-P1600B is used as an example to describe work group management.

7.1.1.1 Work Group Management in In-Path Mode

Choose **System Management > Network Configuration > Work Group Management**. The **Work Group Management** page appears, as shown in [Figure 7-1](#). On this page, you can view available interfaces in the system, and manage management interfaces and work groups.

Figure 7-1 Work Group Management page in in-path mode

Work Group Management

Route Configuration

DNS Configuration

Available Interfaces

G1/3

G1/4

G2/1

G2/2

G2/3

G2/4

Management Interfaces

Add

Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
M	Management Interface	Copper	1000M/Full	10.67.3.98/255.255.0.0	Auto	Auto	1500Byte	
H1	Management Interface	Copper	Unknown/Half		Auto	Auto	1500Byte	

Work Group

Add

default

Edit

Delete

Name	Type	Media	Status	IP Address/VLAN	Rate Configuration	Duplex Configuration	MTU	Operation
G1/1	WAN	Copper	100M/Full		Auto	Auto	1500Byte	
G1/2	LAN	Copper	1000M/Full	10.68.2.123/255.255.255.0 (forbidden)	Auto	Auto	1500Byte	

Adding Management Interfaces

To add management interfaces, perform the following steps:

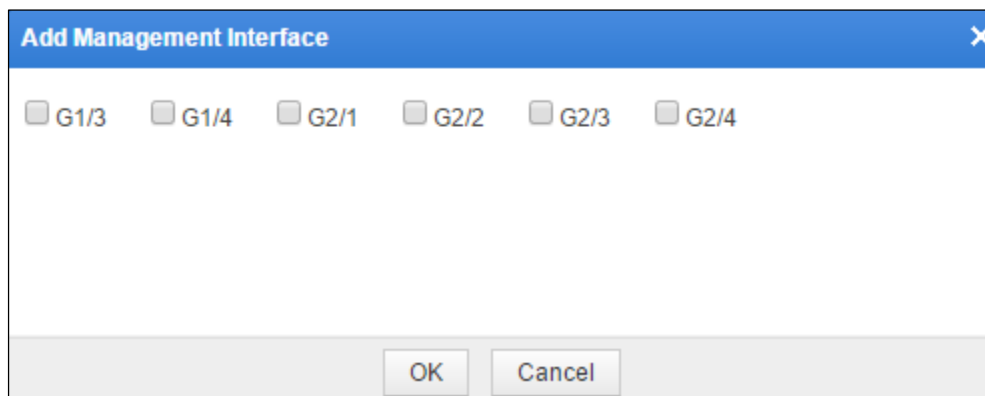
Step 1 Click **Add** in the upper-right corner of the **Management Interfaces** list shown in [Figure 7-1](#).

The **Add Management Interface** dialog box showing available interfaces in the system is displayed. See [Figure 7-2](#).



- If there is no more management interface to be added, the **Add** button under the **Management Interfaces** list disappears.
- If there is no available interface or available interfaces are insufficient, clicking the **Add** button displays a message, saying "No available interface" or "Insufficient available interface".

Figure 7-2 Adding management interfaces in in-path mode



Step 2 Select desired interfaces and click **OK** to complete the setting.



- The interface M or interfaces M and H1 serve as default management interfaces. However, only interface M has a default IP address. Generally, any working interface can be configured as an out-of-band management interface. However, you are advised not to change a default management interface to a working interface. Otherwise, the system may fail.
- Selecting interfaces in the dialog box shown in [Figure 7-2](#) only means that the physical interfaces are selected as management interfaces. They can function as management interfaces only after being edited and configured with some properties.

----End

Editing Management Interfaces

To edit a management interface, perform the following steps:


Step 1 In the **Management Interfaces** list shown in [Figure 7-1](#), click  in the **Operation** column.

Figure 7-3 Editing a management interface in in-path mode.

Edit Interface

Media(RO) Copper

☒ IP Address 10.67.3.89 Mask 255.255.0.0 Clear Add

☒ IP Address 2015:2014:2013:208 Mask 64 Delete

Rate Auto ▼

Duplex Mode Auto ▼

MTU(Byte) 1500
Please enter a number ranging from 512 to 1500.

Default Gateway IPV4 10.67.255.254
IPV6

OK Reset Cancel

Step 2 In the dialog box, edit the interface parameters.

Table 7-1 Parameters for editing a management interface in in-path mode

Parameter	Description
Media(RO)	Physical media of the interface. By default, the media of an electrical interface is Copper .
IP Address	<p>Pairs of IP addresses and subnet masks of the interface. This parameter can be configured only after the check box to its left is selected. Both IPv4 and IPv6 addresses are supported.</p> <p> Note</p> <p>You can add, delete, or clear a pair of the IP address and subnet mask:</p> <ul style="list-style-type: none"> Click Clear to clear the first pair. Click Add to set more pairs. Click Delete to delete a pair.
Rate	<p>Traffic rate of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> Auto: The traffic rate is negotiated with the connected interface. 10Mb/s: The traffic rate is 10 Mbps. 100Mb/s: The traffic rate is 100 Mbps. 1000Mb/s: The traffic rate is 1000 Mbps.
Duplex Mode	Working mode of this interface. The default value is Auto , indicating that the interface negotiates the working mode with the connected network interface.


Parameter	Description
MTU	Maximum transmission unit (MTU) of this interface. The value ranges from 512 to 1500, and the default value is 1500 .
Default Gateway	Default gateway of WAF. Note that the device has only one IPv4 or IPv6 default gateway.

Step 3 Click **OK** to save the settings.

----End

Deleting Management Interfaces

Only user-created management interfaces can be deleted. The default management interface, M and H1, cannot be deleted.

In the **Management Interfaces** list shown in [Figure 7-1](#), click  in the **Operation** column and click **OK** in the confirmation dialog box, to delete the management interface.

Creating Work Groups

There is one default work group on WAF. You can create work groups by performing the following steps:

Step 1 Click **Add** in the lower-right corner of the **Work Group** list shown in [Figure 7-1](#).

The dialog box for creating a work group appears, as shown in [Figure 7-4](#). Interfaces available in the system are automatically displayed in the **Available Interfaces** list.


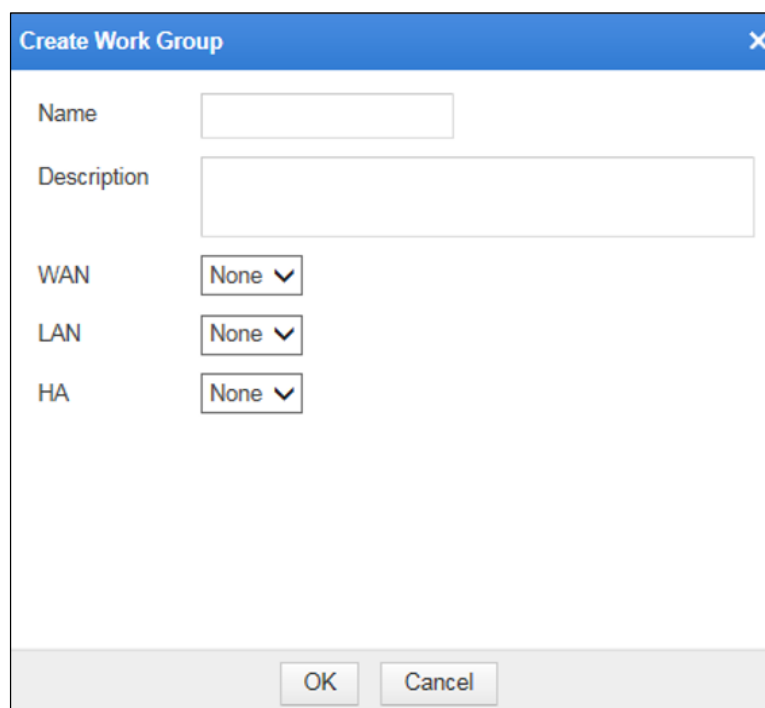
 Note	<ul style="list-style-type: none"> In in-path mode, a work group must contain at least two working interfaces. If there is one or no available interface, you cannot create a work group. The G1/1 and G1/2 interfaces are directly connected by default.
--	---

Figure 7-4 Creating a work group in in-path mode



The dialog box titled "Create Work Group" contains the following fields and controls:

- Name:** A single-line text input field.
- Description:** A multi-line text input field.
- WAN:** A dropdown menu with "None" selected.
- LAN:** A dropdown menu with "None" selected.
- HA:** A dropdown menu with "None" selected.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Step 2 In the dialog box, edit the work group parameters.

Table 7-2 Parameters for creating a work group in in-path mode

Parameter	Description
Name	Name of the new work group.
Description	Brief description about the new work group.
WAN/LAN/HA	WAN interface, LAN interface, and HA interface (if HA is available) used by the work group.

Step 3 Click **OK** to save the settings.

----End

Editing Working Interfaces

To edit a working interface, perform the following steps:

Step 1 In the **Work Group** list shown in [Figure 7-1](#), click  in the **Operation** column.

Figure 7-5 Editing a working interface in in-path mode.

Edit Interface

Name: G1/1

Media: Copper

Manageable: ☒ Yes ☐ No ?

☒ Configure IP Address ☐ Select a VLAN.

Status	IP Address	Mask	Web Access	SSH Login	Operation ?
	0.0.0.0	0.0.0.0	Prohibited ▼	Prohibited ▼	

Rate: Auto ▼

Duplex Mode: Auto ▼

MTU(Byte): 1500
Please enter a number ranging from 512 to 1500.

Default Gateway: IPV4: 10.67.255.254
IPV6:

☒ Advanced

Binding Peer MAC: ?





Enable Source MAC Replacement: ☐ Yes ☒ No ?

OK Reset Cancel

Step 2 In the dialog box, edit the interface parameters.

Table 7-3 Parameters for editing a work group in in-path mode

Parameter	Description
Name	Interface name.
Media	Physical media of the interface. By default, the media of an electrical interface is Copper .
Manageable	Control whether the interface is manageable. Only manageable interfaces can be configured with IP addresses. The in-band management and page prefetch functions can be used only after Manageable is set to Yes and IP addresses are configured.
Configure IP Address	This area specifies pairs of IP addresses and subnet masks of the interface and controls whether to allow or prohibit web access and SSH access. You can add a maximum of three pairs of IP addresses and subnet masks for this interface. Both IPv4 and IPv6 addresses are supported. You can access an IP address of the system via web or SSH only when the IP address is enabled and Allowed is selected for Web Access or SSH Login . You can add, delete, enable, or disable an IP address:

Parameter	Description
	<ul style="list-style-type: none"> Click  to add an IP address. Click  to delete an IP address. Click  to enable an IP address. Click  to disable an IP address.
Select a VLAN	VLAN to which this interface belongs.
Rate	<p>Traffic rate of the interface, which can be one of the following:</p> <ul style="list-style-type: none"> Auto: The traffic rate is negotiated with the connected interface. 10Mb/s: The traffic rate is 10 Mbps. 100Mb/s: The traffic rate is 100 Mbps. 1000Mb/s: The traffic rate is 1000 Mbps.
Duplex Mode	Working mode of this interface. The default value is Auto , indicating that the interface negotiates the working mode with the connected network interface.
MTU(Byte)	MTU of the interface. The value ranges from 512 to 1500, and the default value is 1500 .
Default Gateway	Default gateway of WAF. Note that the device has only one IPv4 or IPv6 default gateway.
Binding Peer MAC	MAC address of the network interface on a specific device to which the uplink traffic of this interface is forwarded. Usually, this option is configured for a WAN interface.
Enable Source MAC Replacement	<p>Controls whether the source MAC address of packets transmitting from this interface is replaced with the MAC address of this interface.</p> <ul style="list-style-type: none"> Yes: indicates that the source MAC address is replaced. No: indicates that the source MAC address is not replaced. <p>Usually, this option is configured for a WAN interface.</p>

Step 3 Click **OK** to save the settings.

----End

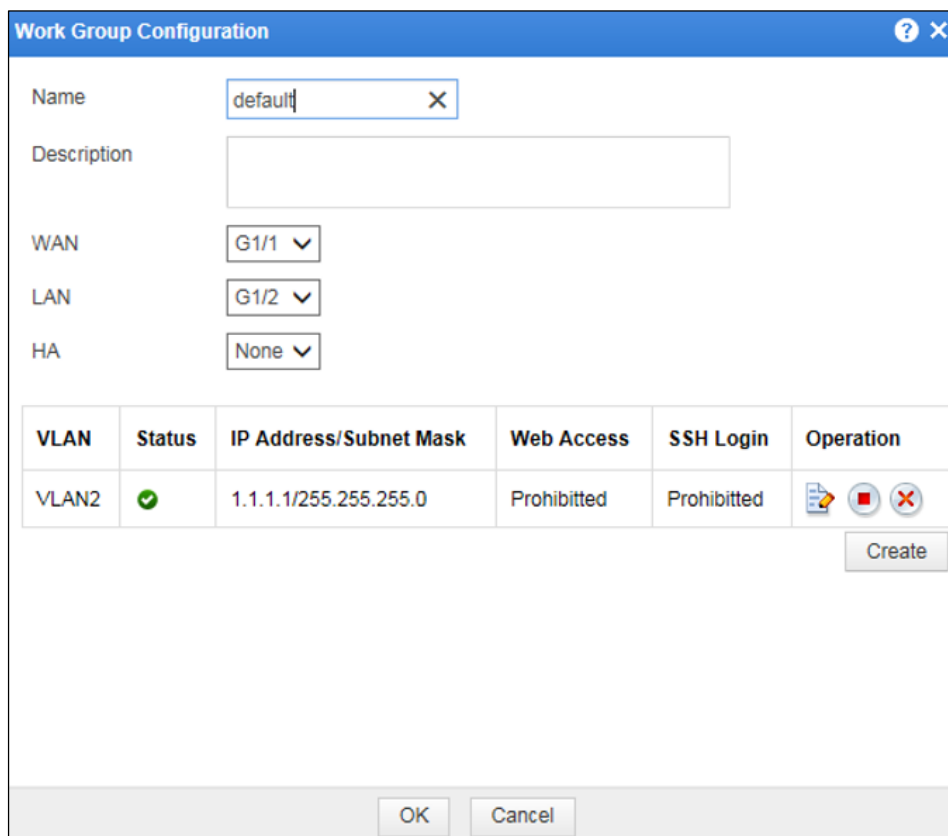
Editing Work Groups

To edit a work group, perform the following steps:

Step 1 In the **Work Group** list shown in [Figure 7-1](#), click **Edit** in the upper-right corner of a work group.




In the dialog box that appears, you can edit the basic information and VLAN subinterface of the work group.

Figure 7-6 Editing a work group in in-path mode



The dialog box titled "Work Group Configuration" contains the following fields and controls:

- Name:** A text box containing "default" with a clear button (X).
- Description:** An empty text box.
- WAN:** A dropdown menu showing "G1/1".
- LAN:** A dropdown menu showing "G1/2".
- HA:** A dropdown menu showing "None".
- Table:** A table with 6 columns: VLAN, Status, IP Address/Subnet Mask, Web Access, SSH Login, and Operation.

VLAN	Status	IP Address/Subnet Mask	Web Access	SSH Login	Operation
VLAN2	✓	1.1.1.1/255.255.255.0	Prohibited	Prohibited	  
- Create:** A button located below the table.
- OK/Cancel:** Buttons at the bottom of the dialog.

Step 2 In the dialog box, set the parameters.

Step 3 Click **OK** to save the settings.

----End

Deleting a Work Groups

In the **Work Group** list shown in [Figure 7-1](#), click **Delete** in the upper-right corner of a work group and click **OK** in the confirmation dialog box, to delete the work group.

Creating VLANs

Click **Create** in the dialog box for editing a work group shown in [Figure 7-6](#).

The area for creating a VLAN appears in the red frame as shown in [Figure 7-7](#).



You can access the specified IP address of the VLAN via web or SSH only when the VLAN is enabled and **Allowed** is selected for **Web Access** or **SSH Login**.

Figure 7-7 Creating a VLAN in in-path mode

Work Group Configuration

Name:

Description:

WAN:

LAN:

HA:

VLAN	Status	IP Address/Subnet Mask	Web Access	SSH Login	Operation
No data					

VLAN: Please enter a number ranging from 2 to 4094.

IPv4 Address: Mask: ☐ Web Access ☐ SSH Login

IPv6 Address: Mask: ☐ Web Access ☐ SSH Login

Step 2 In the dialog box, set the parameters.

Step 3 Click **OK** to save the settings.

----End

7.1.1.2 Work Group Management in Out-of-Path Mode

Figure 7-8 shows the page for managing work groups in out-of-path mode. On this page, you can view available interfaces in the system and manage management interfaces and work groups.

The following operations can be performed only in out-of-path mode:

- Creating subinterfaces
- Viewing the forwarding table
- Viewing the forwarding routing table
- Creating injection routes

Figure 7-8 Work Group Management page in out-of-path mode

Work Group Management
Route Configuration
DNS Configuration

Available Interfaces

G1/2
G1/3
G1/4
G2/1
G2/2
G2/3
G2/4

Management Interfaces

Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
M	Management Interface	Copper	1000M/Full	10.67.3.98/255.255.0.0	Auto	Auto	1500Byte	
H1	Management Interface	Copper	Unknown/Half		Auto	Auto	1500Byte	

Add

Work Group

Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
G1/1	WAN	Copper	Unknown/Unknown		Auto	Auto	1500Byte	

Add

default
View Forwarding Table
View Forwarding Routing Table
Edit
Delete

Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
G1/1	WAN	Copper	Unknown/Unknown		Auto	Auto	1500Byte	

Creating Work Groups

There is one default work group on WAF. You can create other work groups by performing the following steps:

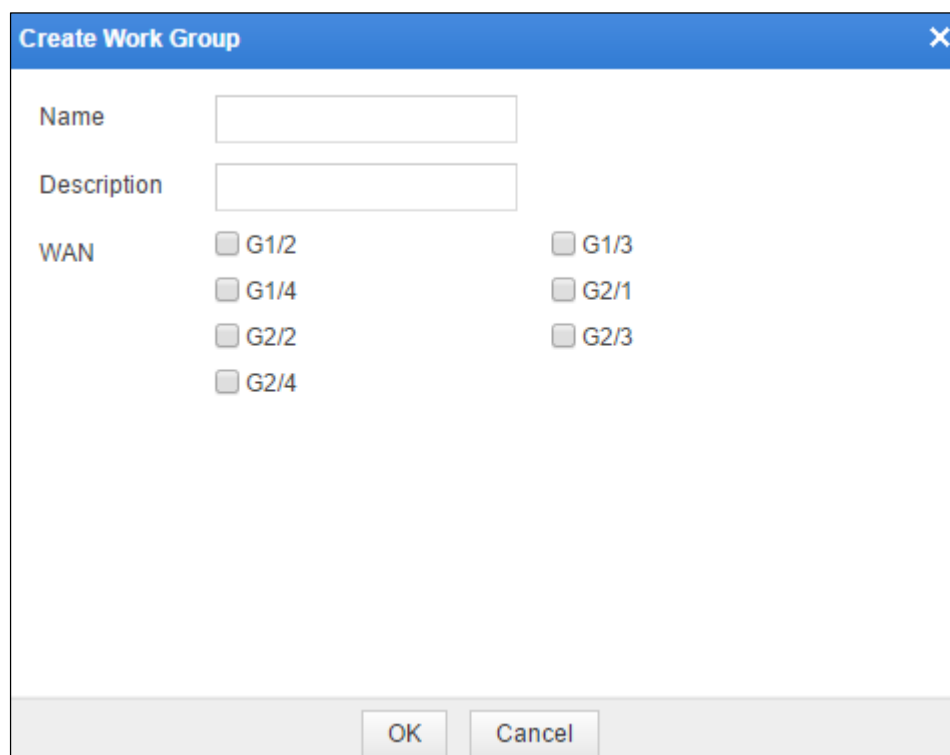
Step 1 Click **Add** in the lower-right corner of the **Work Group** list shown in [Figure 7-8](#).

The dialog box for creating a work group appears, as shown in [Figure 7-9](#). Interfaces available in the system are displayed in the **Available Interfaces** area.



In out-of-path mode, you can create a work group if there is any available interface.

Figure 7-9 Creating a work group in out-of-path mode



The dialog box titled "Create Work Group" has a blue header bar with a close button (X) on the right. It contains two text input fields: "Name" and "Description". Below these is a section labeled "WAN" containing two columns of checkboxes. The left column has checkboxes for G1/2, G1/4, G2/2, and G2/4. The right column has checkboxes for G1/3, G2/1, and G2/3. At the bottom of the dialog are "OK" and "Cancel" buttons.

Step 2 In the dialog box, set the parameters.

Step 3 Click **OK** to save the settings.



In the dialog box shown in [Figure 7-9](#), physical interfaces are selected as working interfaces only. They can function as working interfaces only after being edited and configured with some properties.

----End

Creating Subinterfaces

To create subinterfaces, perform the following steps:


Step 1 In the **Work Group** list shown in [Figure 7-8](#), click  in the **Operation** column to edit a working interface.

Figure 7-10 Editing a working interface in out-of-path mode

Edit Interface

Name: G1/1

Media: Copper

☐ IPv4 Address: [] Mask: [] ☐ Web Access ☐ SSH Login

☐ IPv6 Address: [] Mask: [] ☐ Web Access ☐ SSH Login

Subinterface Configuration: [Add Subinterface](#) (+) All subinterfaces use the 802.1q protocol for encapsulation.

Rate: Auto

Duplex Mode: Auto

MTU(Byte): 1500
Please enter a number ranging from 512 to 1500.

Default Gateway: IPv4: 10.67.255.254
IPv6: []

☐ Advanced

OK Reset Cancel

Step 2 Click **Add Subinterface**.

Figure 7-11 Creating a subinterface in out-of-path mode

Edit Interface

VLAN: [] Please enter a number ranging from 2 to 4094.

IPv4 Address: [] Mask: [] ☐ Web Access ☐ SSH Login

IPv6 Address: [] Mask: [] ☐ Web Access ☐ SSH Login

Add Return

Step 3 In the dialog box, set the parameters.

Step 4 Click **OK** to save the settings.

----End

Viewing the Forwarding Table

In the **Work Group** list shown in [Figure 7-8](#), click **View Forwarding Table** in the upper-right corner of a work group. A dialog box appears, showing details about the forwarding table of subinterfaces, as shown in [Figure 7-12](#).

Figure 7-12 Forwarding table

View Forwarding Table							
VLAN	IP	MAC	Time to Live (sec)	Interface	Type	Status	Encapsulate
---	192.168.1.210	b8:ac:6f:3a:ab:e6	2	G1/1	Dynamic	Ok	Native
---	192.168.1.243	00:0c:29:1c:56:df	13941	G1/1	Dynamic	Ok	Native
---	192.168.1.254	d0:c7:89:c3:ef:4e	3423	G1/1	Dynamic	Ok	Native

Refresh Cancel

Viewing the Forwarding Routing Table

In the **Work Group** list shown in [Figure 7-8](#), click **View Forwarding Routing Table** in the upper-right corner of a work group. A dialog box appears, showing details about the forwarding routing table, as shown in [Figure 7-13](#).

Figure 7-13 Forwarding routing table

View Forwarding Routing Table				
Type	Subnet IP Address	Subnet Mask	Next-hop	Interface
Connected	192.168.1.0	255.255.255.0	0.0.0.0	G1/1

Route Injection Configuration

Refresh Cancel

Configuring Injection Routes

There are two methods for configuring an injection route for a work group.

Method 1

Step 1 In the **Work Group** list shown in [Figure 7-8](#), click **Edit** in the upper-right corner of a work group.

Figure 7-14 Editing a work group in out-of-path mode.

Work Group Configuration

Basic Information

Name

default

Description

WAN

☒ G1/1

☐ G1/2

☐ G1/3

☐ G1/4

☐ G2/1

☐ G2/2

☐ G2/3

☐ G2/4

Route Injection Configuration

Destination Network	Subnet Mask	Next-hop	Operation
<div><div></div><div>No data</div></div>			

Add Route

Apply All

OK

Cancel

Step 2 Click **Add Route**.

Figure 7-15 Configuring an injection route in out-of-path mode

The image shows a 'Work Group Configuration' dialog box with a blue title bar and a close button (X) in the top right corner. Below the title bar is a section titled 'Add Injection Route'. This section contains three input fields: 'Destination Network', 'Subnet Mask', and 'Next-Hop IP Address'. To the right of the 'Next-Hop IP Address' field is a green circular button with a white plus sign. At the bottom of the dialog box are two buttons: 'OK' and 'Cancel'.

- Step 3** Set the parameters and click **OK** to save the setting and return to the **Route Injection Configuration** list.
- Step 4** Click **Apply All** in the lower-right corner of the **Route Injection Configuration** dialog box, to make the settings take effect.
- End

Method 2

- Step 1** In the **View Forwarding Routing Table** dialog box shown in [Figure 7-13](#), click **Route Injection Configuration**.

Figure 7-16 Route injection configuration

Route Injection Configuration

Destination Network

Subnet Mask

Next-hop

Operation ?

i

No data

Add Route

Apply All

Return

Step 2 Click **Add Route**.

Figure 7-17 Configuring an injection route

Destination Network	Subnet Mask	Next-hop	Operation ?
No data			
Destination Network	Subnet Mask	Next-Hop IP Address	Operation
<input type="text"/>	<input type="text"/>	<input type="text"/>	

Step 3 Set the parameters and click **Apply All** to make the settings take effect.

----End

7.1.1.3 Work Group Management in Reverse Proxy Mode

Figure 7-18 shows the page for managing work groups in reverse proxy mode. On this page, you can view available interfaces in the system and manage management interfaces and work groups.

Figure 7-18 Work Group Management page in reverse proxy mode

Work Group Management
Route Configuration
DNS Configuration

Available Interfaces

G1/3
G1/4
G2/1
G2/2
G2/3
G2/4

Management Interfaces

Add

Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
M	Management Interface	Copper	100M/Full	10.67.3.93/255.255.0.0	Auto	Auto	1500Byte	
H1	Management Interface	Copper	100M/Full		Auto	Auto	1500Byte	

Work Group

Add

default ▾

Edit Delete

Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
G1/1	WAN	Copper	1000M/Full		Auto	Auto	1500Byte	
G1/2	WAN	Copper	Unknown/Unknown		Auto	Auto	1500Byte	

In reverse proxy mode, you can add a maximum of 253 IP addresses for an interface in a work group. Also, you can manage the configured IP addresses in batches. [Figure 7-19](#) shows the page for editing an interface in reverse proxy mode. Work groups in reverse proxy mode are managed in a similar way as those in in-path mode. For details, see [section 7.1.1.1 Work Group Management in In-Path Mode](#).

Figure 7-19 Editing a working interface in reverse proxy mode

Edit Interface

Name

G1/2

Media

Copper

Manageable

☒ Yes
 ☐ No

?

☒ Configure IP Address

A maximum of 253 IP addresses are allowed. Current IPs: 1

Add IP

Bulk Operation

<input type="checkbox"/> All/None	Status	IP Address	Mask	Web Access	SSH Login	Operation
<input type="checkbox"/>	<div>✔</div>	<div>0.0.0.0</div>	<div>0.0.0.0</div>	<div>Prohibited</div>	<div>Prohibited</div>	<div>⏏</div> <div>+</div>

Add IP

Bulk Operation

Rate

Auto

Duplex Mode

Auto

MTU(Byte)

1500

Please enter a number ranging from 512 to 1500.

Default

IPV4

10.67.255.254

Gateway

IPV6

☐ Advanced

OK

Reset

Cancel

7.1.1.4 Work Group Management in Mirroring Mode

Figure 7-20 shows the page for managing work groups in mirroring mode. On this page, you can view available interfaces in the system and add, edit, and delete work groups.

Figure 7-20 Work Group Management page in mirroring mode

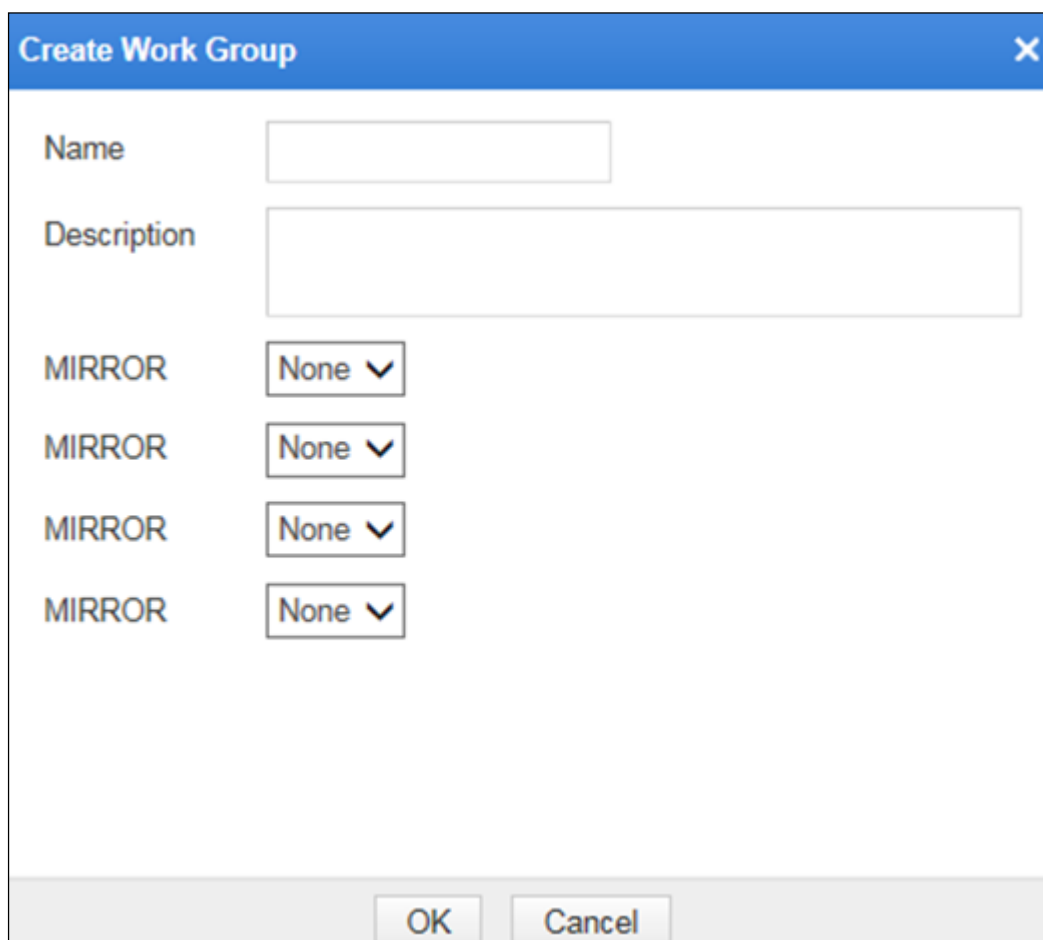
Work Group Management								
Route Configuration DNS Configuration								
Available Interfaces								
<div> <div></div> G1/4 <div></div> G1/5 <div></div> G1/6 </div>								
Management Interfaces								
Name	Type	Media	Status	IP Address	Rate Configuration	Duplex Configuration	MTU	Operation
M	Management Interface	Copper	<div></div> 100M/Full	10.67.3.94/255.255.0.0	Auto	Auto	1500Byte	
Work Group								
								Add
default ▲								<div>Edit</div> <div>Delete</div>
Name	Type	Media	Status					
G1/1	MIRROR	Copper	<div></div>					
G1/2	MIRROR	Copper	<div></div>					
G1/3	MIRROR	Copper	<div></div>					

Creating Work Groups

Initially, only one work group named default exists. You can create other work groups by performing the following steps:

- Step 1** Click **Add** in the upper-right corner of the **Work Group** list shown in [Figure 7-20](#).

Figure 7-21 Creating a work group in mirroring mode



The dialog box titled "Create Work Group" has a blue header bar with a close button (X) in the top right corner. It contains the following fields and controls:

- Name:** A single-line text input field.
- Description:** A multi-line text input field.
- MIRROR:** Four identical rows, each consisting of the label "MIRROR" and a dropdown menu currently showing "None" with a downward arrow.
- Buttons:** "OK" and "Cancel" buttons located at the bottom right of the dialog.

Step 2 In the dialog box, set the parameters.

Step 3 Click **OK** to save the settings.

----End

Editing Work Groups

In [Figure 7-20](#), click **Edit** in the upper-right corner of a work group and then you can rename the work group and edit mirroring interface settings.

Deleting Work Groups

In [Figure 7-20](#), click **Delete** in the upper-right corner of a work group and then click **OK** in the confirmation dialog box to delete the work group.

7.1.2 Route Configuration

WAF supports the configurations of the default gateway and static routes.

Static routes are a kind of routes that are manually configured by network administrators. For a simple network structure, static routes are enough to ensure normal network operations. However, if a network fails or a topology changes, routes may be unreachable, causing

network interruption. In this situation, the network administrator must manually modify the static route configuration.

There is a special kind of static routes, that is, default routes. If routes for transferring certain packets are unavailable in the routing table, these packets are usually discarded. However, if default routes are configured, these transfer packets can be transferred along the default routes.

The following describes how to configure the default gateway, create static routes, and delete static routes.

Configuring the Default Gateway

To configure the default gateway, perform the following steps:

Step 1 Choose **System Management > Network Configuration > Route Configuration**.

The default gateway is **10.30.255.254** as shown in [Figure 7-22](#).

Figure 7-22 Route Configuration page

Route Configuration		
Default Gateway		
IPv4	<input type="text" value="10.67.255.254"/>	
IPv6	<input type="text"/>	
<input type="button" value="OK"/>		
Static Route		
<input type="button" value="Add"/>		
Destination Network	Gateway	Operation
<div>i No data</div>		

Step 2 Type the IP address of the desired gateway in the **Default Gateway** text box and click **OK** to save the settings.

----End

Creating Static Routes

To create a static route, perform the following steps:

Step 1 Click **Add** in the upper-right corner of the **Static Route** list shown in [Figure 7-22](#).

Figure 7-23 Creating a static route

Step 2 In the dialog box, set the static route parameters.


Table 7-4 Parameters for creating a static route

Parameter	Description
Destination Network	IP address of the destination network. Both IPv4 and IPv6 addresses are supported.
Mask	Subnet mask of the IP address of the destination network.
Gateway	IP address of the gateway of the destination network, that is, the next hop in the static route.

Step 3 Click **OK** to save the settings.

----End

Deleting Static Routes

In the **Static Route** list shown in [Figure 7-22](#), click  in the **Operation** column and then click OK in the confirmation dialog box to delete a static route.

7.1.3 DNS Configuration

As an essential and fundamental service on the Internet, the DNS service is used to determine the mapping between host domain names and IP addresses. As a DNS client, WAF can request the domain name resolution service from a specified DNS server. WAF is designed with two domain name parsing methods:

- Parsing through DNS server
Prior to protection, WAF needs to parse the domain name of a website into an IP address. To do so, WAF will send a domain name parsing request to the DNS server. After

receiving the request, the DNS server searches among entries for the matching IP address and returns it to WAF.

- Parsing through custom domain names

When parsing a domain name, WAF searches among custom domain name entries for the corresponding IP address. After WAF finds the corresponding IP address, the parsing succeeds. The custom domain name configuration is generally used to translate domain names into private IP addresses.

7.1.3.1 Configuring DNS Servers

To configure DNS servers, perform the following steps:

Step 1 Choose **System Management > Network Configuration > DNS Configuration**.

Figure 7-24 DNS Configuration page

ID	Domain Name	IP Address	Operation
No data			

Step 2 Specifies IPv4 or IPv6 addresses for the preferred and alternate DNS servers.

Step 3 Click **OK** to save the settings.

----End

7.1.3.2 Managing Custom Domain Names

You can create, edit, and delete custom domain names.

Creating Custom Domain Names

In the **Customized Domain Name** list shown in [Figure 7-24](#), click **Add** in the upper-right corner.

Figure 7-25 Creating a custom domain name


The image shows a 'Create' dialog box with a blue title bar. Inside, there are two text input fields. The first is labeled 'IP Address' and the second is labeled 'Domain Name'. Below the input fields, there are two buttons: 'OK' and 'Cancel'.

Step 2 In the dialog box, set the parameters.

Step 3 Click **OK** to save the settings.

----End


Editing Custom Domain Names

Step 1 In the **Customized Domain Name** list shown in Figure 7-24, click  in the **Operation** column.

Step 2 In the dialog box that appears, edit the parameters and click **OK** to save the settings.

----End

Deleting Custom Domain Names

In the **Customized Domain Name** list shown in Figure 7-24, click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete a custom domain name.

7.2 System Deployment

System deployment configurations including the following parts:

- [Running Mode Configuration](#)
- [HA Configuration](#) (Unavailable in mirroring mode)
- [Bypass Configuration](#) (Unavailable in reverse proxy and mirroring modes)
- [VRRP Configuration](#) (Unavailable in in-path and mirroring modes)
- [VRRP Configuration Management](#) (Unavailable in in-path, out-of-path, and mirroring modes)

7.2.1 Running Mode Configuration

Choose **System Management** > **System Deployment** > **Running Mode** to open the **Running Mode** page, as shown in Figure 7-26.

Figure 7-26 Running Mode page

Running Mode [HA Configuration](#) [Built-in Bypass Configuration](#) [External Bypass Configuration](#)

Deployment Topology ☒ In-Path ☐ Out-of-Path ☐ Reverse Proxy ☐ Mirroring ?

OK

Mode Configuration ☐ Forwarding Mode ☒ Protection Mode ☐ Debugging Mode ?

OK

Emergency Mode ? ☐ Disable ☐ Permanently Enable ☒ Auto-Switching ?

Relaxation Time (second) ? It should greater than 5 seconds.

Connections ^

Enable emergency mode ☒ Yes ☐ No

Activation Threshold ?

Deactivation Threshold ?

CPU ^

Enable emergency mode ☒ Yes ☐ No

Activation Threshold % ?

Deactivation Threshold % ?

Memory ^

Enable emergency mode ☒ Yes ☐ No

Activation Threshold % ?

Deactivation Threshold % ?

OK

- **Deployment Topology** can be set to **In-Path**, **Out-of-Path**, **Reverse Proxy**, or **Mirroring**.
- **Mode Configuration** can be set to one of the following values (modes vary with deployment topologies):
 - **Forwarding Mode:** In this mode, the engine forwards traffic without processing, and thus has no protection effect. This mode is unavailable in reverse proxy deployment.
 - **Protection Mode:** In this mode, WAF implements protection for servers.
 - **Debugging Mode:** In this mode, WAF provides protection for servers as it functions in protection mode, but more debugging information is available on the background. This mode is usually used for WAF debugging.
- **Emergency Mode:** After entering the emergency mode, WAF continues handling traffic on established TCP connections, but directly forwards new requests.

Emergency Mode can be set to **Disable**, **Permanently Enable**, or **Auto-Switching**.

If **Permanently Enable** is selected, WAF will always be in emergency mode.

If **Auto-Switching** is selected, WAF determines whether to activate the emergency mode based on the number of TCP connections, CPU usage, or memory usage. In this case, one of the three triggering conditions must be enabled. If more than one condition is

enabled, when finding that the number of TCP connections, CPU usage, or memory usage becomes lower than the deactivation threshold and stays at that level for a period longer than the relaxation time, WAF deactivates the emergency mode.

Table 7-5 Parameters for setting the emergency mode

Parameter		Description
Relaxation Time (second)		When finding that the number of TCP connections, CPU usage, or memory usage becomes lower than the deactivation threshold and stays at that level for a period longer than the relaxation time, WAF deactivates the emergency mode.
Connections	Enable emergency mode	Controls whether to enable the emergency mode based on the number of connections.
	Activation Threshold	When finding that the number of connections exceeds this threshold, WAF activates the emergency mode.
	Deactivation Threshold	When finding that the number of connections becomes lower than the threshold and stays at that level for a period longer than the relaxation time, WAF deactivates the emergency mode.
CPU	Enable emergency mode	Controls whether to enable the emergency mode based on the CPU usage.
	Activation Threshold	When finding that the CPU usage exceeds this threshold, WAF activates the emergency mode.
	Deactivation Threshold	When finding that the CPU usage becomes lower than the threshold and stays at that level for a period longer than the relaxation time, WAF deactivates the emergency mode.
Memory	Enable emergency mode	Controls whether to enable the emergency mode based on the memory usage.
	Activation Threshold	When finding that the memory usage exceeds this threshold, WAF activates the emergency mode.
	Deactivation Threshold	When finding that the memory usage becomes lower than the threshold and stays at that level for a period longer than the relaxation time, WAF deactivates the emergency mode.

7.2.2 HA Configuration

High availability (HA) can reduce the system downtime caused by routine maintenance and unexpected system crash, enhancing the system and the application availability. HA is the most effective way for enterprises to stop core computer systems from breaking down.

In in-path and reverse proxy modes, HA adopts the master/slave or active-active work mode to realize following functions:

- Link status monitoring
- Policy synchronization

The HA mechanism (hot-standby) requires two WAF devices to communicate with each other over heartbeat cables, with one in master mode and the other in slave mode.

In normal situations, the master device functions while the slave device does not. If the number of consecutive lost heartbeats detected by the slave device reaches the specified

threshold, the slave device immediately enables work interfaces and takes over services, to ensure service continuity. As shown in Figure 7-27, if the slave device fails to receive heartbeat signals from the master device for three consecutive times, it considers that the master device has lost its heartbeat. The slave device will then, depending on the configuration, decide whether to start its work interfaces.

To configure HA, perform the following steps:


Step 1 Choose **System Management > System Deployment > HA Configuration**.

Figure 7-27 HA Configuration page

Step 2 In the dialog box, set the HA parameters.

Table 7-6 Parameters for configuring HA

Parameter	Description
Enable HA	Controls whether to enable HA. This parameter is mandatory.
Work Mode	Working mode of the current WAF, which can be one of the following:

Parameter	Description
	<ul style="list-style-type: none"> • Master: master WAF in master/slave mode. On the master WAF, the working interfaces in work groups and the heartbeat interface run properly. If a working interface on the master WAF is down, network traffic is switched from the master WAF to the slave WAF. • Slave: slave WAF in master/slave mode. On the slave WAF, the working interface stops running. After detecting the loss of heartbeat of the master WAF, the slave WAF immediately starts its working interface. • Special: In port synchronization mode, all existing work groups are supported and the status of the WAN port is associated with that of the LAN port. If the WAN port status changes from down to up (or from up to down), the LAN port status also changes in the same way. • Single: In single mode, if the working interface of the master work group is down, the master work group informs the slave work group of the status change via internal heartbeat messages, and traffic is switched to the slave work group. • Active-Active: In active-active mode, both WAFs are in the active state and work concurrently. <p>After HA is enabled, WAF's status will be displayed, as shown in the red frame in Figure 7-27.</p> <p> Note</p> <p>Working modes vary with deployment modes.</p>
Work Group	Work group for which HA is enabled.
Heartbeat Port	Interface over which the current WAF exchanges heartbeat signals with the peer WAF. It is a management interface.
Peer IP Address	<p>IP address of the peer heartbeat interface. Both IPv4 and IPv6 addresses are supported.</p> <p>You can click Synchronize Configuration to start configuration synchronization.</p> <ul style="list-style-type: none"> • Master-slave configuration synchronization: The master device can synchronize its configurations to the slave device. In master-slave mode, the configuration synchronization function is available only on the master device. • Active-active configuration synchronization: In active-active mode, the configuration synchronization function is available on both devices. You can click Synchronize Configuration on either device to synchronize its configurations to the other device. <p>After configurations are synchronized to a peer device, it takes a while for the configurations to take effect on the peer device. During the period, do not perform operations on the peer device.</p>
Heartbeat Protocol Port	Port number of the heartbeat interface. Heartbeat signals adopt the UDP protocol, and the heartbeat port is a UDP port.
Heartbeat Interval (ms)	Heartbeat interval.
Lost Heartbeats (times)	Number of consequent consecutive times that WAF fails to receive heartbeat signals from the peer host before WAF considers the peer host loses its heartbeat.
Configuration Synchronization	Interface over which the master device's configurations are synchronized to the slave device. Configuration synchronization uses

Parameter	Description
Port	TCP, and the synchronization port is a TCP port.
Synchronization Interval (sec)	Interval at which configurations are synchronized.
Gateway Info	You can add gateway information of the peer device if it is needed.

Step 3 Click **OK** to save the settings.

----End

7.2.3 Bypass Configuration

Bypass configuration is available only in in-path or out-of-path deployment, but not reverse proxy deployment or mirroring deployment.

WAF provides the built-in bypass and external bypass functions. Built-in bypass interfaces are electrical interfaces, and external bypass interfaces are optical interfaces. 100M-series WAF products support the built-in bypass only. 1000M-series and 10G-series WAF supports both built-in and external bypass functions.

7.2.3.1 Built-in Bypass

Built-in bypass is implemented by software. You can make the device enter or exit the bypass state via the settings of **Watchdog Heartbeat Process** and **Manual Bypass Enable-Disable Control**.

Choose **System Management > System Deployment > Built-in Bypass Configuration**. The **Built-in Bypass Configuration** page appears, as shown in [Figure 7-28](#).

Figure 7-28 Built-in Bypass Configuration page

Status	Bypass Group	Operation
⊘	G1/1-G1/2	▶
⊘	G1/3-G1/4	▶



Enabling Built-in Bypass Groups

- Enabling built-in bypass via **Watchdog Heartbeat Process**

After **Watchdog Heartbeat Process** is set to **Enable**, when the system is overloaded or fails, the watchdog's heartbeat messages cannot be updated in time, and the device automatically enters the bypass state.

- Enabling built-in bypass via **Manual Bypass Enable-Disable Control**

Before enabling manual bypass, please set **Watchdog Heartbeat Process** to **Disable**.



In the **Manual Bypass Enable-Disable Control** list shown in [Figure 7-28](#), click  in the **Operation** column to enable built-in bypass. After it is enabled, its status turns to .

Disabling Built-in Bypass Groups

- Disabling built-in bypass via **Watchdog Heartbeat Process**

After **Watchdog Heartbeat Process** is set to **Disable**, the system will not automatically enter the bypass state. You are advised to set **Watchdog Heartbeat Process** to **Enable**.

- Disabling built-in bypass via **Manual Bypass Enable-Disable Control**

In the **Manual Bypass Enable-Disable Control** list shown in [Figure 7-28](#), click  in the **Operation** column to disable a bypass group. After it is disabled, its status turns to .

7.2.3.2 (Optional) External Bypass

External bypass can be configured on 1000M-series and 10G-series WAF products only.

When interface inspection is enabled, if WAF is powered off or its heartbeat interface fails, an interface of the associated work group is down. The associated bypass switch automatically switches to out-of-path mode and transfers the traffic to the next hop device, bypassing WAF and ensuring network connection. After WAF recovers, the bypass switch switches to the normal mode and forwards traffic to WAF.



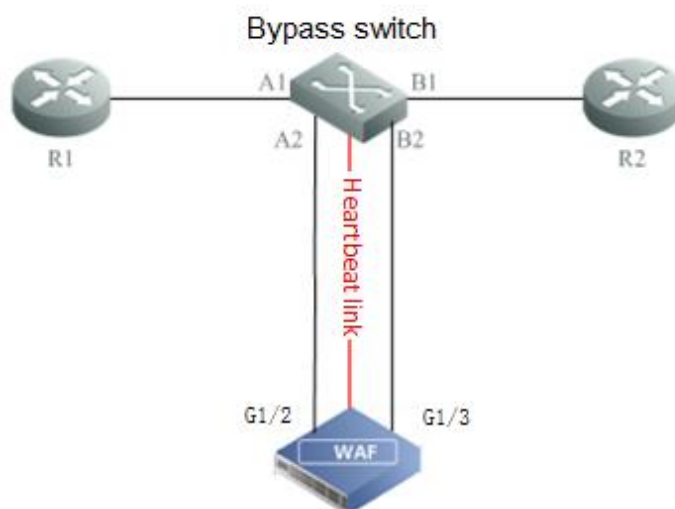
- The bypass switch switches to the out-of-path mode to ensure proper connections only if WAF is powered off or its heartbeat interface is down. When interface inspection is enabled, the bypass switch automatically switches to the out-of-path mode if the interface of the associated work group is down.
- After WAF recovers, you need to disable interface inspection for the bypass group, and then the bypass switch can switch back to the normal mode.
- When interface inspection is enabled, if a direct interface on WAF is down, the other direct interface is also down.

A topology shown in [Figure 7-29](#) is used as an example to illustrate how external bypass works.

When WAF is functioning properly, the bypass switch is in normal mode. The traffic path from R1 to R2 is as follows: R1 → A1 interface on the bypass switch → A2 interface on the bypass switch → G1/2 interface on WAF → G1/3 interface on WAF → B2 interface on the bypass switch → B1 interface on the bypass switch → R2.

If WAF is powered off or its heartbeat interface is down, the bypass switch switches to the bypass mode. The traffic from R1 to R2 bypasses WAF along the path: R1 → A1 interface on the bypass switch → B1 interface on the bypass switch → R2.

Figure 7-29 External bypass topology



Choose **System Management > System Deployment > External Bypass Configuration**. The **External Bypass Configuration** page appears, as shown in Figure 7-30.

Figure 7-30 External Bypass Configuration page

Running Mode HA Configuration Built-in Bypass Configuration External Bypass Configuration								
Bypass Group	Status	Enable Interface Inspection	IP Address	Local Heartbeat Process Status	External Bypass Device Status	Associated Work Group Name	Description	Operation
bypass1	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass1	
bypass2	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass2	
bypass3	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass3	
bypass4	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass4	
bypass5	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass5	
bypass6	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass6	
bypass7	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass7	
bypass8	⛔	⛔	0.0.0.0	Stopped	Failed to start the process!	No associated work group	bypass8	

Editing External Bypass Groups

To edit an external bypass group, perform the following steps:

Step 1 In the list shown in Figure 7-30, click in the **Operation** column.

Figure 7-31 Editing an external bypass group

Edit	
Name	<input type="text" value="bypass1"/>
IP Address	<input type="text" value="0.0.0.0"/> Note: Enter the IP address of the external bypass device.
Login Password	<input type="text"/> Empty for use pre-existing password. Note: A password can contain at most 15 characters, including digits and letters.
Associated Work Group	-- ▾
Enable External Bypass Heartbeats	No ▾ Note: When connecting to an external bypass device, this device enters the bypass status once heartbeats stop.
Enable Interface Inspection	No ▾ Note: After the interface inspection function is enabled, the system automatically enters the bypass state when detecting the WAN or LAN interface of an associated
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Step 2 In the dialog box, edit the external bypass parameters.



Table 7-7 Parameters for editing an external bypass group

Parameter	Description
Name	Name of an external bypass group.
IP Address	IP address of the heartbeat interface of the external bypass device. Both IPv4 and IPv6 addresses are supported.
Login Password	Password for communicating with the heartbeat interface of the external bypass device.
Associated Work Group	Work group to be associated with the bypass group. Only a work group whose interfaces are optical interfaces can be selected.
Enable External Bypass Heartbeats	Controls whether to enable the heartbeat interface to send heartbeat messages.
Enable Interface Inspection	Controls whether to enable interface inspection. When interface inspection is enabled and a work group is associated with, WAF immediately switches to the bypass state when detecting that the WAN or LAN interface of the associated work group is down.
Description	Brief description of the external bypass group.



Step 3 Click **OK** to save the settings.

----End

Enabling External Bypass Groups

In the list shown in [Figure 7-30](#), click  in the **Operation** column to enable a bypass group. After it is enabled, its status turns to .

Disabling External Bypass Groups

In the list shown in [Figure 7-30](#), click  in the **Operation** column to disable a bypass group. After it is disabled, its status turns to .

7.2.4 VRRP Configuration



VRRP configuration is available in out-of-path and reverse proxy deployment, but not in-path or mirroring deployment.


VRRP stands for Virtual Router Redundancy Protocol. As a standard RFC protocol, VRRP achieves hot standby via two or more WAFs on a network. In this case, once the master WAF fails (for example, an interface is down in a work group), the backup WAF takes over all traffic to ensure smooth network communications. VRRP is applicable to the out-of-path mode and reverse proxy mode.

Perform the following steps to configure VRRP in reverse proxy mode:

Step 1 Choose **System Management > System Deployment > VRRP Configuration**.

Figure 7-32 VRRP Configuration page

Running Mode		HA Configuration	VRRP Configuration	VRRP Config Info Mgmt	
					Create
	Name				Operation
 No VRRP instance					



Note

VRRP can be configured only on working interfaces on WAF, but cannot be configured on the management interfaces.

Step 2 Click **Create** to add interface G1/1, as shown in [Figure 7-33](#).

Figure 7-33 Adding interface G1/1

Step 3 Click **Save**.

The **VRRP Configuration** page appears, as shown in [Figure 7-34](#).

Figure 7-34 VRRP Configuration page after interface G1/1 is added

Step 4 Click the VRRP instance management icon  in the **Operation** column of interface G1/1.

The **G1/1 Instance Management** page appears, as shown in [Figure 7-35](#).

Figure 7-35 VRRP instance management

Step 5 Click **Add** in the lower-right corner of the page.




Parameters (such as **Group ID**, **Virtual IP Address**, and **Transfer Interval**) of VRRP instances in the same VRRP group must be set to the same values on the master WAF and backup WAF.

Figure 7-36 Adding a VRRP instance for interface G1/1

Running Mode	HA Configuration	VRRP Configuration	VRRP Config Info Mgmt
Add G1/1 VRRP Instance			
Group ID	<input type="text"/> * ?		
Priority	<input type="text" value="100"/> * ?		
Virtual IP Addresses	<input type="button" value="+"/> ?		
Enable or Not	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Allow Preemption	<input checked="" type="radio"/> Yes <input type="radio"/> No ?		
Initial State	Master ?		
Transfer Interval	<input type="text" value="1"/> *seconds ?		
Primary IP Address	<input type="text" value="172.168.1.87"/> ?		
Monitored Interface	<input checked="" type="checkbox"/> G1/1 <input type="checkbox"/> G1/2 <input type="checkbox"/> G1/3 <input type="checkbox"/> G1/4 <input type="checkbox"/> G1/5 <input type="checkbox"/> G1/6		
Routes	<input type="button" value="+"/>		
Description	<input type="text"/>		

Step 6 In the dialog box, set the VRRP instance parameters.

Table 7-8 Parameters for creating a VRRP instance

Parameter	Description
Group ID	<p>ID of the VRRP group to which the virtual WAF device belongs. WAF devices in the same VRRP group should have the same group ID. The value is an integer ranging from 1 to 255.</p> <p> Note</p> <p>The master WAF and backup WAF must have the same group ID.</p>
Priority	<p>Priority of a WAF device. A greater value indicates a higher priority. A WAF with a higher priority tends to be the master WAF. If two WAFs have the same priority, the one with a larger primary IP address tends to be the master WAF. The value is an integer ranging from 1 to 254.</p>
Virtual IP Addresses	<p>Virtual IP addresses of this virtual instance. A VRRP instance supports a maximum of 16 virtual IP addresses. Both IPv4 and IPv6 addresses are supported.</p>
Enable or Not	<p>Controls whether to enable the VRRP instance, which can be either of the following:</p> <ul style="list-style-type: none"> Yes: The VRRP instance is enabled. No: The VRRP instance is disabled. <p>This parameter is mandatory.</p>
Allow Preemption	<p>Working mode of the master WAF and backup WAF, which can be either of the</p>

Parameter	Description
	<p>following:</p> <ul style="list-style-type: none"> No: As long as the master WAF functions properly, the backup WAF will not become the master one even if it has a higher priority. Yes: A backup WAF sends VRRP advertisements when it finds that it has a higher priority than the current master WAF. Then the master device is reelected in the VRRP backup group to take over traffic from the original master device. After a new master device is elected, the original master WAF becomes a backup.
Initial State	<p>Initial state of WAFs in this instance, which can be either of the following:</p> <ul style="list-style-type: none"> Master: indicates the master WAF. The master WAF is protecting servers. Backup: indicates the backup WAF. The backup WAF is not protecting servers, but it will take over server protection from the master WAF if the master WAF fails.
Transfer Interval	Interval for sending VRRP advertisements. The value is an integer ranging from 1 to 255. To ensure that VRRP advertisements are properly transmitted, this interval should be set to the same value for VRRP instances on the master WAF and backup WAF.
Primary IP Address	<p>First IP address configured for the interface with the VRRP instance.</p> <p>The primary IP address is used as the source IP address of VRRP advertisements. By default, this VRRP instance is enabled on the primary IP address of the interface. Both IPv4 and IPv6 addresses are supported.</p>
Monitored Interface	Interface to be monitored when this VRRP instance is enabled. You can select multiple interfaces. By default, the interface with the current VRRP instance is selected, for example, interface G1/3.
Routes	Route needed to ensure smooth communication of the actual network.
Description	Brief description of this VRRP instance.

Step 7 Click **Save** to save the settings.

----End

7.2.5 VRRP Configuration Management

The VRRP configuration management function is available only in reverse proxy mode.

On the VRRP configuration management page, you can export the VRRP configuration information to the local disk or import a VRRP configuration file to WAF.

Importing a VRRP Configuration File

Step 1 Choose **System Management > System Deployment > VRRP Config Info Mgmt.**

Figure 7-37 VRRP Config Info Mgmt page

Running Mode HA Configuration VRRP Configuration VRRP Config Info Mgmt

Import Configuration

File Browse

Import Configuration

Import Result:

Import Time	File Name	Version ID	MD5 Value	Import Status	Remarks
-------------	-----------	------------	-----------	---------------	---------

Export Configuration

Export Configuration Refresh

Export Result:

Export Time	File Name	Version ID	MD5 Value	Operation
2017-08-05 16:05:18	wafv_6.0.6.1.36651_1501920318.wafv	6.0.6.1.36651	eb9d4a680b6296405dfb32ee738f5b03	

Step 2 Click **Browse** to select the target VRRP configuration file.

Click **Import Configuration** and then click **OK** in the displayed dialog box to import the file. After the file is successfully imported, the related file information is displayed in the import result table.



Importing VRRP configurations will result in WAF missing original protection policies. Therefore, remember to create a restore point under **System Management > System Tools > Backup and Restore** before importing VRRP configurations.

During VRRP configuration import, only site protection solutions on virtual IP addresses configured for the proxied IP address of the master WAF are imported.

----End

Exporting a VRRP Configuration File

On the page shown in [Figure 7-37](#), click **Export Configuration** to export the current VRRP configuration information on WAF to a VRRP configuration file. After the export succeeded, the related file information is displayed in the export result table.

Viewing an Exported VRRP Configuration File


After a VRRP configuration file is exported, you can click  in the **Operation** column of the export file list to view details about this file. See [Figure 7-38](#).

Figure 7-38 Viewing an exported VRRP configuration file

VRRP Configuration Details			
Date	2017-08-05 16:05:18		
File Name	wafv_6.0.6.1.36651_1501920318.wafv		
Version	6.0.6.1.36651		
MD5 Value	eb9d4a680b6296405dfb32ee738f5b03		
Backup Type		Backed-up Content	Content Not Backed Up
System Monitoring	Server Alive Status Check	Real-time Detection Inspection Configuration	
	Website Protection	Website Group Mgmt Low-and-Slow Attack HTTP Flood Protection Secure Data Transfer Web Security Protection Exception Control Session Trace Risk Level Control	
Security Management	Policy Management	Policy files	
	Rule Database Management	Custom Rules	Common Protection
	Proxy Information Configuration	Proxy Information Configuration	

7.3 System Tools

System tools include the following parts:

- System information
- System upgrade
- Rule upgrade
- Synchronization Configuration
- License
- Time & language
- System control
- Port setting
- Google Analytics Setting

7.3.1 System Information

Choose **System Management > System Tools > System Information**.

If no SSL card is loaded in WAF, the **System Information** shown in [Figure 7-39](#) appears.

The page shows the following system information:

- Device model
- Serial number
- Hardware hash
- Firmware version

- System version
- Rule database information
- Rule database reliance information.

Each WAF has a unique hardware hash.

Figure 7-39 System Information page — without SSL card

System Information

System Upgrade

Rule Upgrade

Synchronize Configuration

License

Time & Language

System Control

Port Setting

Google Analytics Setting

Model	Serial No.	Hardware Hash	SSL Acceleration	Firmware Version	System Version	Rule Database Information	Rule Database Dependency Information
NX3-P2000A		F804-5E8B-F3A3-4B7C	Supported	6.0.5.0	6.0.6.1.36651	6.0.6.1.36651	6.0.6.1.36651

If an SSL card is loaded in WAF, an extra **SSL Card** column will also appear, as shown in [Figure 7-40](#).

Figure 7-40 System Information page — with SSL card

System Information

System Upgrade

Rule Upgrade

Synchronize Configuration

License

Time & Language

System Control

Port Setting

Google Analytics Setting

Model	Serial No.	Hardware Hash	SSL Card	Firmware Version	System Version	Rule Database Information	Rule Database Dependency Information
NX5-P2020E		F804-5E8B-F3A3-4B7C	Support	6.0.5.0	6.0.6.0.34292	6.0.6.0.34292	6.0.6.0.34292

7.3.2 System Upgrade

For a licensed WAF, users can always conduct system upgrade before the license expires, to enhance system functions.

To conduct system upgrade, perform the following steps:

Step 1 Choose **System Management > System Tools > System Upgrade**.

Figure 7-41 System Upgrade page

System Information	System Upgrade	Rule Upgrade	Synchronize Configuration	License	Time & Language	System Control	Port Setting	Google Analytics Setting																												
System Upgrade The upgrade package <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Submit"/>																																				
Latest Upgrade Records <table border="1"> <thead> <tr> <th>Upgrade Time</th> <th>Version ID</th> <th>Upgrade Result</th> <th>Remarks</th> </tr> </thead> <tbody> <tr> <td>2016-09-01 10:00:23</td> <td>6.0.6.0.34292</td> <td>Succeeded</td> <td>success</td> </tr> <tr> <td>2016-08-20 19:01:14</td> <td>6.0.6.0.34175</td> <td>Succeeded</td> <td>success</td> </tr> <tr> <td>2016-08-08 21:22:14</td> <td>6.0.6.0.33943</td> <td>Succeeded</td> <td>success</td> </tr> <tr> <td>2016-08-08 21:21:46</td> <td>6.0.5.1.33742</td> <td>Succeeded</td> <td>success</td> </tr> <tr> <td>2016-08-08 21:21:19</td> <td>6.0.5.1.33056</td> <td>Succeeded</td> <td>success</td> </tr> <tr> <td>2016-08-08 21:20:49</td> <td>6.0.5.0.31604</td> <td>Succeeded</td> <td>success</td> </tr> </tbody> </table>									Upgrade Time	Version ID	Upgrade Result	Remarks	2016-09-01 10:00:23	6.0.6.0.34292	Succeeded	success	2016-08-20 19:01:14	6.0.6.0.34175	Succeeded	success	2016-08-08 21:22:14	6.0.6.0.33943	Succeeded	success	2016-08-08 21:21:46	6.0.5.1.33742	Succeeded	success	2016-08-08 21:21:19	6.0.5.1.33056	Succeeded	success	2016-08-08 21:20:49	6.0.5.0.31604	Succeeded	success
Upgrade Time	Version ID	Upgrade Result	Remarks																																	
2016-09-01 10:00:23	6.0.6.0.34292	Succeeded	success																																	
2016-08-20 19:01:14	6.0.6.0.34175	Succeeded	success																																	
2016-08-08 21:22:14	6.0.6.0.33943	Succeeded	success																																	
2016-08-08 21:21:46	6.0.5.1.33742	Succeeded	success																																	
2016-08-08 21:21:19	6.0.5.1.33056	Succeeded	success																																	
2016-08-08 21:20:49	6.0.5.0.31604	Succeeded	success																																	

Step 2 Click **Browse** and select the desired upgrade file with the extension of **.bin**.

Step 3 Click **Submit**.

A prompt "Upgrading... Please wait." appears during the upgrade process.

If the upgrade package can only be installed on specific versions, the system displays the current system version and asks you to install the package on specific versions.

Successful upgrade will be recorded in the "Latest Upgrade Records" list. If system upgrade fails, record extension information, and contact NSFOCUS technical support personnel.



- If **Disable auto update** is set for **Installation Method** in the **Scheduled Upgrade** area on the **Rule Upgrade** page before system upgrade, **Manually install after download** will be selected for this option after system upgrade.
- If **Manually install after download** or **Auto install** is selected for this option before system upgrade, the setting remains unchanged after system upgrade.


----End

7.3.3 Rule Upgrade

For a licensed WAF, users can always conduct rule upgrade before the license expires. Rule upgrade can increase the number of rules in the built-in rule database, improving the system's protection effect.

Choose **System Management > System Tools > Rule Upgrade**. The **Rule Upgrade** page appears, as shown in [Figure 7-42](#).

Figure 7-42 Rule Upgrade page

System Information		System Upgrade	Rule Upgrade	Backup and Restore	License	Time & Language	System Control	Port Setting	Google Analytics Setting
Current Version Info ^									
Current Rule Database Version	6.0.6.0.34292								
Dependency System Version	6.0.6.0.34292								
<div> <div> Scheduled Upgrade ^ </div> <div> Manual Upgrade ^ </div> </div>									
Upgrade URL *	<input type="text" value="http://update.nsfocus.com"/>			Select Upgrade Package			<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Submit"/>		
Upgrade Cycle	<input type="text" value="1"/> Day(s)								
Update Time *	<input type="text" value="00:00"/>								
Installation Method	<input checked="" type="radio"/> Disable auto update <input type="radio"/> Manually install after download <input type="radio"/> Auto install								
<input type="button" value="OK"/>									
Check Update ^									
<input type="button" value="Check Update"/> Historical Updates									
Auto-Backup of Rule Database ^									
Upgrade Package Name	Create Time	Rule Database Version	Dependency System Version	Operation					
 No data									

7.3.3.1 Viewing the Current Version Information

The current version information, including the current rule database version and dependency system version, is displayed in the **Current Version Info** area, as shown in [Figure 7-43](#).

Figure 7-43 Current version information

Current Version Info ^	
Current Rule Database Version	6.0.6.0.34292
Dependency System Version	6.0.6.0.34292

7.3.3.2 Rule Database Upgrade

WAF's rule database upgrade packages are full update package. The rule database can be upgraded in either of the following ways:

- Scheduled upgrade

For scheduled upgrade, the administrator needs to configure upgrade parameters to enable the system to check the upgrade server for new rule upgrade packages as scheduled and automatically download the latest upgrade package once available. After download, the rule upgrade package can be installed automatically or manually.

- Manual upgrade

For manual upgrade, the administrator needs to download the rule upgrade package and install it manually.

Scheduled Upgrade

Figure 7-44 shows the **Scheduled Upgrade** area on the **Rule Upgrade** page.

Figure 7-44 Scheduled upgrade

Scheduled Upgrade ^

Upgrade URL *

Upgrade Cycle Day(s)

Update Time *



Installation Method ☒ Disable auto update ☐ Manually install after download ☐ Auto install

OK

To configure scheduled upgrade, perform the following steps:

Step 2 Configure parameters in the **Scheduled Upgrade** area.

Table 7-9 Parameters for configuring scheduled upgrade

Parameter	Description
Upgrade URL	Specifies the address of the upgrade server where to obtain the rule upgrade package.  Note Make sure that WAF communicates properly with the upgrade server. Otherwise, WAF cannot perform scheduled upgrade and check update.
Upgrade Cycle	Specifies how often WAF installs the rule upgrade package. The interval is expressed in days.
Update Time	Specifies when WAF checks whether a new upgrade package is available on the upgrade server every day. The format should be in the format of 12:38.
Installation Method	Specifies how the new rule upgrade package is installed after download. <ul style="list-style-type: none"> Disable auto update: indicates that the auto upgrade is disabled. In this case, the system prompts "If you cancel automatic upgrade, you cannot get the latest product support". Manually install after download: indicates that the administrator is notified to install the new rule upgrade package after download. Auto install: indicates that the new rule upgrade package is automatically installed after download and the administrator will be notified of the installation completion.  Note Installation notifications are sent only to the administrator.

Parameter	Description
	<ul style="list-style-type: none"> If the administrator has logged in, the notification will be displayed on the current page of the web-based manager. If the administrator has not logged in, the notification will be displayed on the web-based manager upon login.

Step 3 Click **OK** to save the settings.

----End

Manual Upgrade

Figure 7-45 shows the **Manual Upgrade** area on the **Rule Upgrade** page.

Figure 7-45 Manual upgrade

To configure manual upgrade, perform the following steps:

Step 1 Click **Browse**, and select the desired upgrade file with the extension of .bin.

Step 2 Click **Submit**, and click **OK** in the confirmation dialog box.

A prompt "Upgrading... Please wait." appears during the upgrade process.

Successful upgrade will be recorded in the "Latest Upgrade Records" list. If a rule upgrade fails, you can roll the rule database to the previous version by using the backup and restore function.

----End

7.3.3.3 Checking Updates

Figure 7-46 shows the **Check Update** area on the **Rule Upgrade** page. In this area, you can check updates and view historical updates.

Figure 7-46 Check updates

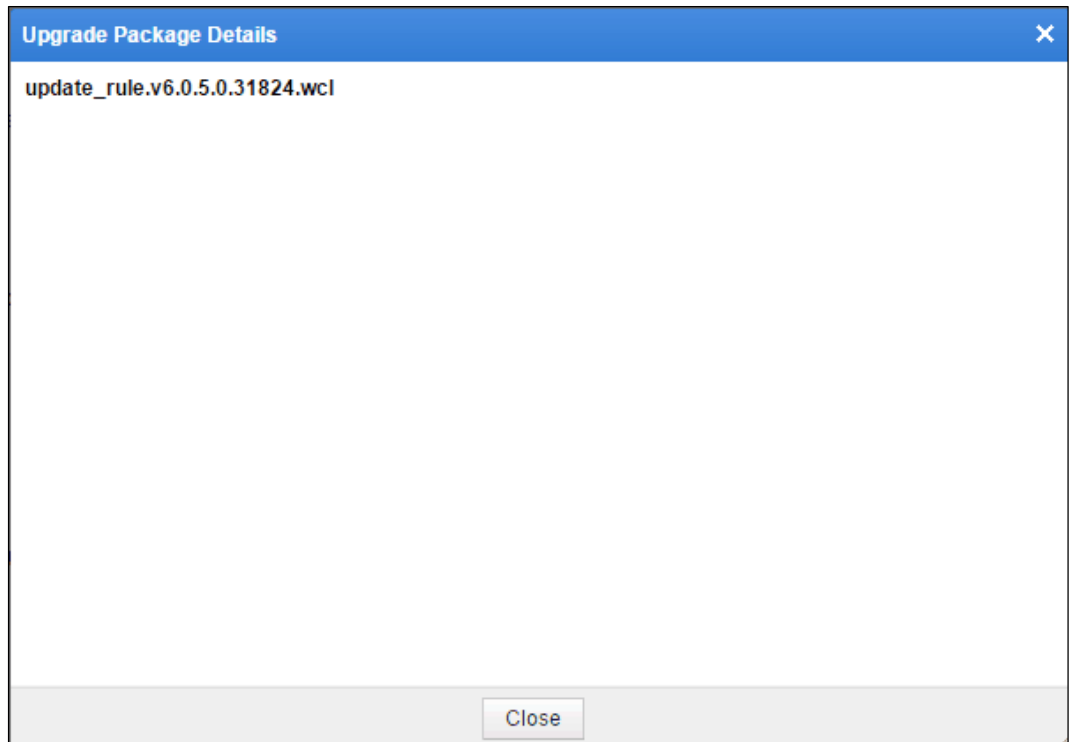
Check Update ^				
Check Update		Historical Updates		
Name	Release Date	Overview	Details	Operation
update_rule.v6.0.5.0.31824.wcl	2015-12-24		Details	Update

Checking Updates

If you click **Check Update**, WAF will check whether rule upgrade packages are available on the upgrade server. If yes, WAF downloads them and presents them in the rule package list. A dimmed **Check Update** button indicates that the current rule upgrade is up to date.

- Click the **Details** link in the **Details** column of a rule package.
The details about this rule upgrade package appear, as shown in [Figure 7-47](#).

Figure 7-47 Rule upgrade package details



- Click **Update Now** in the **Operation** column to install the rule upgrade package immediately.
WAF's rule upgrade packages are full update package. In other words, after a rule upgrade package is installed, all packages of earlier versions will be displayed as installed.

Viewing Historical Updates

Click **Historical Updates**. The **Historical updates** dialog box appears, as shown in [Figure 7-48](#).

Figure 7-48 Historical updates

Historical updates			
Upgrade Time	Version ID	Upgrade Result	Upgrade Mode
2016-09-01 10:00:23	6.0.6.0.34292	success	system upgrade
2016-08-20 19:01:14	6.0.6.0.34175	success	system upgrade
2016-08-08 21:22:14	6.0.6.0.33943	success	system upgrade
2016-08-08 21:21:46	6.0.5.1.33742	success	system upgrade
2016-08-08 21:21:19	6.0.5.1.33056	success	system upgrade
2016-08-08 21:20:49	6.0.5.0.31604	success	system upgrade
2015-09-26 09:56:26	6.0.5.0.31184	success	system upgrade
2015-09-26 09:55:03	6.0.5.0.31042	success	system upgrade
2015-09-25 19:33:27	6.0.5.0.30726	success	system upgrade

The upgrade time, version number, upgrade result, and upgrade mode of historical updates are displayed.

7.3.3.4 Managing Rule Upgrade Packages

After the rule upgrade packages are downloaded from the upgrade server and installed, WAF will record them in the rule upgrade package list. You can view and manage the rule upgrade packages in the **Auto-Backup of Rule Database** area, as shown in [Figure 7-49](#).

Figure 7-49 Auto-Backup of Rule Database area

Auto-Backup of Rule Database ^				
Upgrade Package Name	Create Time	Rule Database Version	Dependency System Version	Operation
waf_rule_bak.f.v6.0.5.0.29799_2015_03_27_11_52_22.waf	2015-03-27 11:52:22	6.0.5.0.29799	6.0.5.0.29799	Restore

Viewing Rule Upgrade Packages

As shown in [Figure 7-46](#), downloaded rule upgrade packages are displayed in the list in descending order of the version number. A maximum of 20 rule upgrade packages can be displayed in the list. If the number of rule upgrade packages exceeds 20, WAF will delete the one with the smallest version number and then download a new one.

The information about the upgrade package, including the name, creation time, description, details, and operation, is displayed in the rule upgrade package list. If a rule upgrade package

is displayed as installed in the **Operation** column, the upgrade package file will be automatically deleted in the background.

Restoring Rule Upgrade Packages

You can restore a rule upgrade package of WAF to a specific version.

For example, after the rule upgrade package of version A is installed and backed up, the rule upgrade package of version B is installed. In this case, if you click **Restore** in the **Operation** column of the rule upgrade package of version A, you can restore the rule upgrade package of version B to version A as long as the dependency system version is satisfied.

You can click **Restore** in the **Operation** column in the list shown in [Figure 7-49](#) to restore a rule upgrade package to a specific version.

7.3.4 Configuration Synchronization

WAF provides the configuration synchronization function. If configuration files (such as system configuration and policy configuration under Security Management and System Management) are damaged because of WAF exceptions, you can restore the configuration files in either of the following ways, thereby restoring system configurations:

- Offline synchronization: Back up and restore configuration files via a restore point.
- Online Synchronization: Synchronize selected configuration files to another device.

7.3.4.1 Offline Synchronization

Perform the following steps to synchronize configurations in offline mode:

Step 1 Choose **System Management > System Tools > Synchronize Configuration**.

Figure 7-50 Offline configuration synchronization

Sync Scope	Date	File Name	Version	Operation
All	2016-09-05 14:54:23	wafc_0_6.0.6.0.34352_1473058463_all.wafc	6.0.6.0.34352	
	2016-08-30 14:55:46	wafc_0_6.0.6.0.34292_1472540146_all.wafc	6.0.6.0.34292	
Assets and policies	2016-09-05 14:54:45	wafc_1_6.0.6.0.34352_1473058485_policyandproperty.wafc	6.0.6.0.34352	
	2016-08-30 14:52:45	wafc_1_6.0.6.0.34292_1472539965_policyandproperty.wafc	6.0.6.0.34292	
Policies	2016-09-05 14:56:26	wafc_2_6.0.6.0.34352_1473058586_policy.wafc	6.0.6.0.34352	
	2016-08-30 14:55:42	wafc_2_6.0.6.0.34292_1472540142_policy.wafc	6.0.6.0.34292	

Step 2 Create restore point.

- Specify the synchronization scope.


Table 7-10 Synchronization scope

Parameter	Description
All	The scope covers the customer's assets, protection policies and network interface settings. Rule base backup is also included.
Assets and policies	<p>The scope covers:</p> <ul style="list-style-type: none"> The following configurations under Security Management: Website Protection, Custom Rules, Policy Management, Template Management, Smart Patch, Secure Delivery, Proxy Information Configuration, XSD/WSDL File Mgmt, Rule Database Management, and IP Reputation. Server Alive Status Check under System Monitoring.
Policies	The scope covers all types of policies in Rule Database Management, Template Management, Policy Management, and Advanced Protection Policies for IP Reputation.

- b. Select **Offline** for **Sync Mode**.
- c. Click **Create Restore Point**. A .wafc file will be automatically generated.

Step 3 Restore configurations.

In offline synchronization, configurations can be restored in either of the following ways:

- Among the listed restore point files as shown in [Figure 7-50](#), select a desired one, click  in the row of the file, and click **OK** in the confirmation dialog box.
- If you want to restore configurations based on a restore point file previously downloaded to local, click **Browse** in **Import Backup File** area shown in [Figure 7-50](#), choose the desire file, and click **OK**.



Note

- If **Sync Scope** is set to **All**: (1) Restart the device to make network interface configurations take effect; (2) Restart the Apache service to make the network configuration (device IP address) take effect. You can choose **Yes** to restart it during synchronization or choose **No** to manually restart the device after the synchronization is complete
- Ignore device restart if **Sync Scope** is set to another value.

----End

You can also perform the following operations on a restore point file listed in [Figure 7-50](#):




- Click  to download it for local backup.
- Click  to delete it.
- Click  to view its details, as shown in [Figure 7-51](#).

Figure 7-51 Details of a restore point file

Details		
Date	2016-08-30 14:55:46	
File Name	wafc_0_6.0.6.0.34292_1472540146_all.wafc	
Version	6.0.6.0.34292	
Backup Type		Backed-up Content
System Monitoring	Server Alive Status Check	Real-time Detection Inspection Configuration
	Network-Layer Protection	Policy Enable-Disable Network-Layer Access Control TCP Flood Protection IP Reputation ARP Spoofing Protection ADS Collaboration Config
	Website Protection	Website Group Mgmt Low-and-Slow Attack HTTP Flood Protection Secure Data Transfer Web Security Protection Exception Control Session Trace Risk Level Control
	Auto-Learning Policies	Auto-Learning Policy Configuration
Security Management	Rule Database Management	Rule files

7.3.4.2 Online Synchronization

Perform the following steps to synchronize configurations in online mode:

Step 1 Choose **System Management > System Tools > Synchronize Configuration**.

Figure 7-52 Online synchronization

System Information	System Upgrade	Rule Upgrade	Synchronize Configuration	License	Time & Language	System Control	Port Setting	Google Analytics Setting
--------------------	----------------	--------------	---------------------------	---------	-----------------	----------------	--------------	--------------------------

Import Backup File
Restore Point Management

Synchronize Configuration
Sync Scope ☒ All ☐ Assets and policies ☐ Policies
Sync Mode ☐ Offline ☒ Online
IP Address

Time	Sync Scope	Operation
2016-11-14 10:50:53	Policies	
2016-11-12 17:16:58	Policies	
2016-11-12 17:13:32	Policies	

Step 2 Specify the synchronization scope.

Step 3 Set **Sync Mode** to **Online**, and set **IP Address** to the IP address of the desired peer device.

Step 4 Click **Synchronize**. The specified configurations will be synchronized to the desired peer device.

The online synchronization history will be recorded. You can click **Clear** at the upper-right corner to clear the history.

----End


You can click  in the row of an online synchronization record to view its details, as shown in [Figure 7-53](#).

Figure 7-53 Details of an online synchronization record

Details

Backup Type		Backed-up Content
Policy Management	Protocol Validation	
	Basic Protection	
	Advanced Protection	
	Precise Protection	
	Others	Risk Level Control
Template Management		
Uploaded File Mgmt		
Rule Database Management		

Close

7.3.5 License

You must load a valid license when you use WAF for the first time.

WAF licenses are classified into two types:

- Trial-use license

After a trial-use license expires:

 - System upgrade cannot be conducted.
 - The **Submit** button is dimmed.
 - The engine stops running.
 - The system automatically enters the forwarding mode.
 - Protection functions of the system lose effect.



If a new license is imported, you need to first check the system running mode. If the system is in forwarding mode, switch to the protection mode.

- Paid license

After a paid license expires, the system can still provide protection functions. You can still import the expired license and upgrade the system to the latest version released within the validation period.

7.3.5.1 Viewing License Information

Choose **System Management > System Tools > License**. The **License** page appears, as shown in [Figure 7-54](#).

Figure 7-54 License page

Owner	Type ?	License Hash	Start Date	Expiry Date	Used Days	Status
test	Trial Use	297A-ED93-A9BC-B116	20180305	20180612	44	Valid license

Authorized Registration Information

Authorized Module
Anti-DDoS Module (Including Low-and-Slow Attack) Webpage Defacement Protection Module Traffic Control Module Brute Force Protection Module Session Tracking Module XML Attack Protection Module SAAS Collaboration Smart Patching Module WVS Collaboration Smart Patching Module

License: No file selected

After importing a license, you can view license information and authorized registration information. When the remaining period is less than 30 days, the system prompts a message indicating that the license is about to expire. See [Figure 7-55](#).

Figure 7-55 License expiration notification

Owner	Type	License Hash	Start Date	Expiry Date	Used Days	Status
test	Trial Use	69E0-5341-9D91-1CA4	20180413	20180515	6	Valid license

Authorized Registration Information

Authorized Module

- Anti-DDoS Module (Including Low-and-Slow Attack)
- Webpage Defacement Protection Module
- Traffic Control Module
- Brute Force Protection Module
- Session Tracking Module
- XML Attack Protection Module
- SAAS Collaboration Smart Patching Module
- WVS Collaboration Smart Patching Module

License: No file selected.

7.3.5.2 Loading a License

To load a license, perform the following steps:

- Step 1** On the **License** page shown in Figure 7-54, click **Browse**, select a license file (*.lic), and click **Submit**.

The dialog box for confirming the license information and the End User License Agreement (EULA) appears.

Figure 7-56 Confirming license information

Owner	test
Type	Trial Use
Model	WAFV6
Product No.	F804-5E8B-F3A3-4B7C
Running Mode	Single Host
Start Date	20170525
Expiry Date	20170824

Before updating the license, please sign the End User License Agreement. (EULA)

- Step 2** Check whether license information is correct. If yes, click **EULA** and read the content that appears.

- Step 3** Click **Agree**.

The page for updating the license appears.

Figure 7-57 Updating the license

License Management	
Owner	test
Type	Trial Use
Model	WAFV6
Product No.	F804-5E8B-F3A3-4B7C
Running Mode	Single Host
Start Date	20170525
Expiry Date	20170824
<p>Before updating the license, please sign the End User License Agreement. (EULA)</p> <p> <input type="button" value="Update"/> <input type="button" value="Return"/> </p>	

Step 4 Click **Update** to make the license take effect or click **Return** to load another license.

A license takes effect immediately after being loaded.

----End

7.3.6 System Time and Language

Choose **System Management > System Tools > Time & Language**. The **Time & Language** page appears, as shown in [Figure 7-58](#). You can set the system time, time server, and system language.

Figure 7-58 Time & Language page

System Information	System Upgrade	Rule Upgrade	Backup and Restore	License	Time & Language	System Control	Port Setting	Google Analytics Setting
System Time Settings ^								
System Time		2016-03-30 11:12:10						
Timezone		(GMT+08:00), Beijing, Chongqing, Hong Kong, Urumqi, Shanghai ▼						
		<input type="button" value="OK"/>						
Time Server Settings ^								
Last Synchronization Time								
Last Synchronization Result								
Time Server		<input type="text"/>						
		<input type="button" value="OK"/> <input type="button" value="Synchronize"/>						
System Language Settings ^								
Default System Language		Simplified Chinese ▼						
		<input type="button" value="OK"/>						
<input type="button" value="Reset"/>								

7.3.7 System Control

Choose **System Management > System Tools > System Control**. The **System Control** page appears, as shown in [Figure 7-59](#).

Figure 7-59 System Control page

You can perform the following system control operations:

- Click **Apply** to the right of **Restart Engine** to restart the engine, thereby reloading all configuration files. After a trial license expires, the engine stops running and the **Apply** button is unavailable for **Restart Engine**.
- Click **Apply** to the right of **Restart System** to restart the hardware system of WAF.
- Click **Apply** to the right of **Shutdown System** to shut down WAF before powering off WAF.

7.3.8 Port Setting

Choose **System Management > System Tools > Port Setting**. The **Port Setting** page appears, as shown in [Figure 7-60](#).

Figure 7-60 Port Setting page

The default port on WAF is port 443. If port 443 is occupied, set another port for accessing WAF. After the port for accessing WAF is changed from port 443 to another port, to access WAF, you need to suffix the new port number to WAF's address. For example, if WAF's IP address is `https://192.168.1.1` and its port is changed from 443 to 445, you use `https://192.168.1.1:445` to access WAF.

7.3.9 Google Analytics Setting

WAF introduces a third-party data collection tool, Google Analytics, to collect, store, and analyze user behaviors on WAF. This is for the purpose of continuously improving user experience.

User behavior information includes the access time, geographic location, operating system, browser, and page access path.



All user behavior information is only used for improving user experience and will not be disclosed to any third party without user permission, unless otherwise prescribed by laws and regulations.

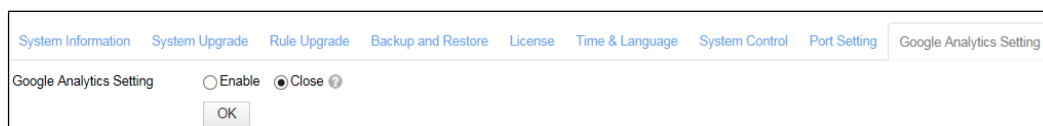
In the process of collecting, storing, and analyzing user behavior information, WAF adopts effective security measures to ensure the security of such information.



Do not upload other information in the process of using Google Analytics.

Step 1 Choose **System Management > System Tools > Google Analytics Setting**.

Figure 7-61 Google Analytics Setting page



Step 2 Select **Enable** or **Disable** to enable or disable the user behavior analysis function.

By default, this function is enabled.

Step 3 Click **OK** to save the settings.

----End

7.4 Test Tools

This section describes common tools used in debugging, to view information such as network connection status and network adapter status. For example, you can use ping or traceroute to view information and perform diagnosis.

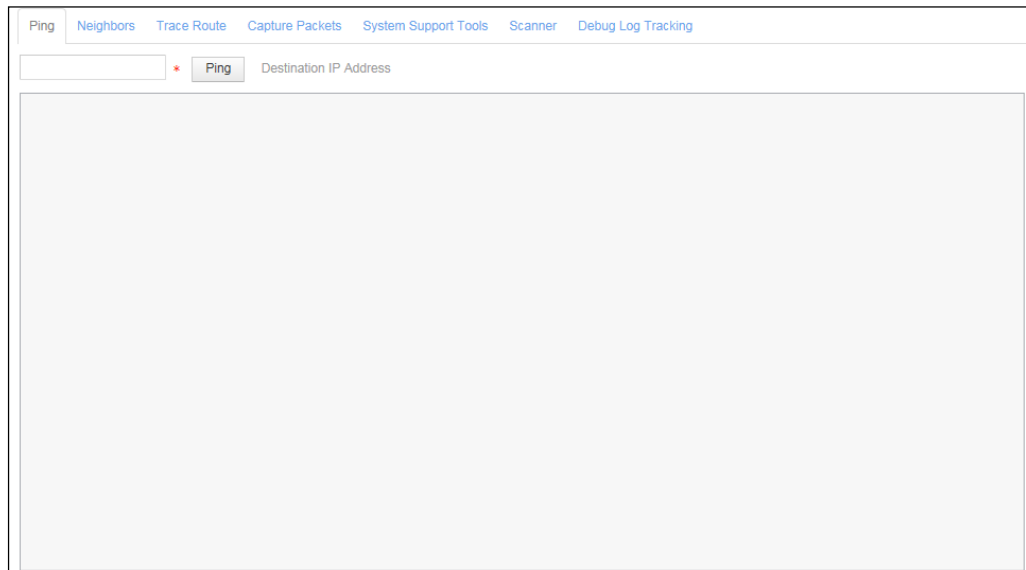
Test tools include common tools and a scanner:

- Common tools refer to tools frequently used in system maintenance and debugging, such as ping, packet capture tool, traceroute, neighbor list, system support tools, and debug log tracking.
- The scanner is used to check the security status of the system.

7.4.1 Ping

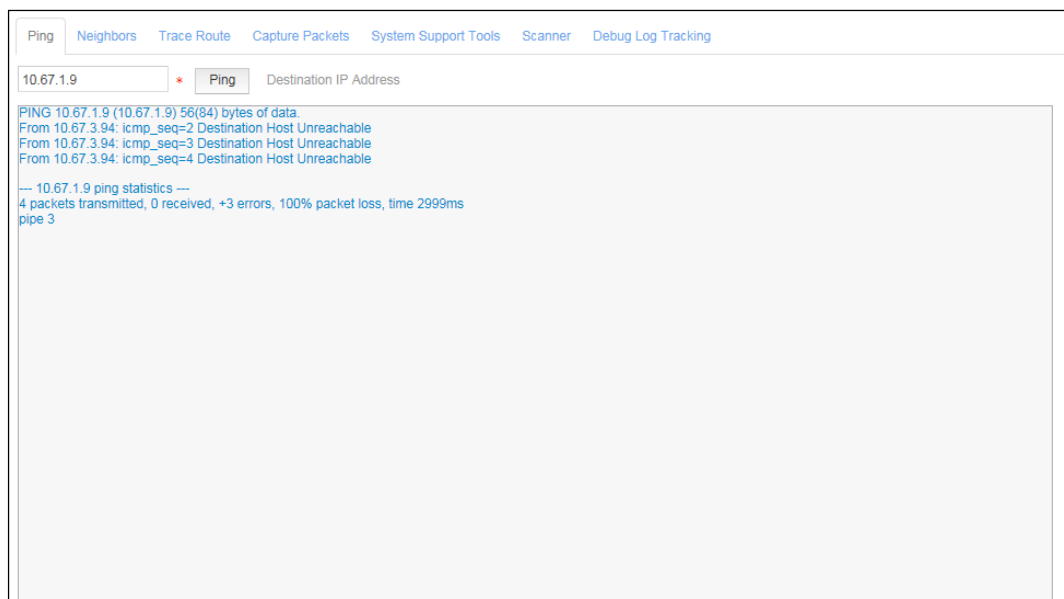
The ping operation is used to check the host availability or network connections. Choose **System Management > Test Tools > Ping**. The **Ping** page appears, as shown in [Figure 7-62](#).

Figure 7-62 Ping page



Type the IP address of a target host in the **Destination IP Address** text box and click **Ping**. The ping result appears, as shown in [Figure 7-63](#).

Figure 7-63 Ping result



7.4.2 Neighbor List

WAF provides a neighbor list for you to view the layer-2 forwarding IP-MAC table, facilitating network troubleshooting. Choose **System Management** > **Test Tools** > **Neighbors**. The **Neighbors** page appears, as shown in [Figure 7-64](#).

Figure 7-64 Neighbors page

Ping Neighbors Trace Route Capture Packets System Support Tools Scanner Debug Log Tracking		
IP Address	MAC	Interface
10.67.3.57	5c:f9:dd:73:8a:fe	M
10.67.3.6	5c:f9:dd:73:8c:c9	M
10.67.3.39	12:34:66:78:90:12	M
172.16.12.107		G1/1
172.16.12.57	5c:f9:dd:73:8a:fe	G1/1
10.67.1.9		M
10.67.255.254	e8:40:40:97:c3:c2	M
fe80::d2c7:89ff:fec3:ef40	d0:c7:89:c3:ef:40	M
fe80::d6d7:48ff:fe92:5440	d4:d7:48:92:54:40	M
fe80::d2c7:89ff:fec3:ef40	d0:c7:89:c3:ef:40	G1/1
fe80::d6d7:48ff:fe92:5440	d4:d7:48:92:54:40	G1/1

Refresh

7.4.3 Traceroute

Traceroute is used to trace routes and check network routing. Choose **System Management > Test Tools > Trace Route**. The **Trace Route** page appears, as shown in [Figure 7-65](#).

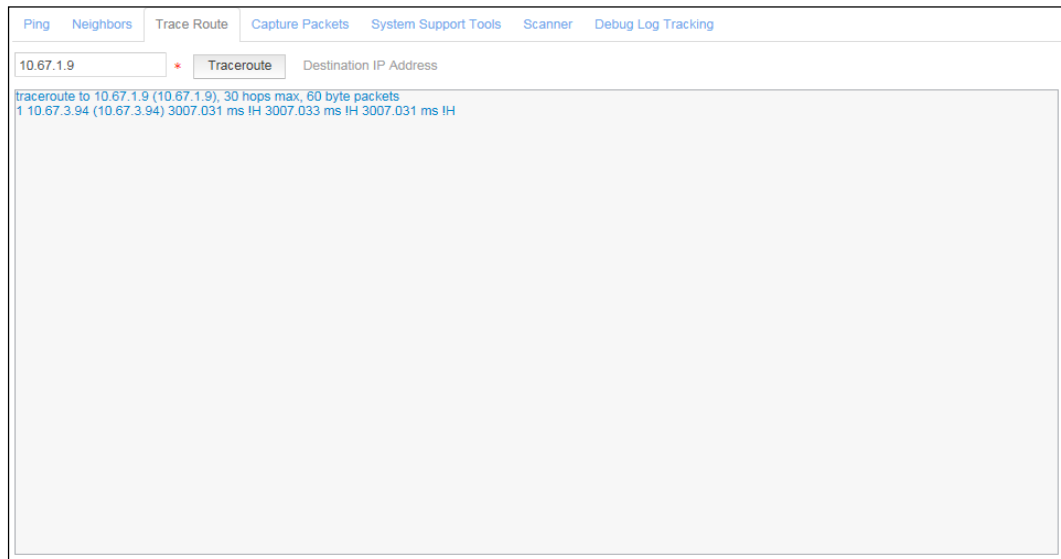
Figure 7-65 Trace Route page

Ping	Neighbors	Trace Route	Capture Packets	System Support Tools	Scanner	Debug Log Tracking
------	-----------	-------------	-----------------	----------------------	---------	--------------------

* Traceroute Destination IP Address

Type the IP address of a target host in the **Destination IP Address** text box and click **Traceroute**. The trace result appears, as shown in [Figure 7-66](#).

Figure 7-66 Traceroute result



7.4.4 Packet Capture

You can use the packet capture tool to capture packets transferred through An interface on WAF. This facilitates analysis, debugging, and troubleshooting during deployment.



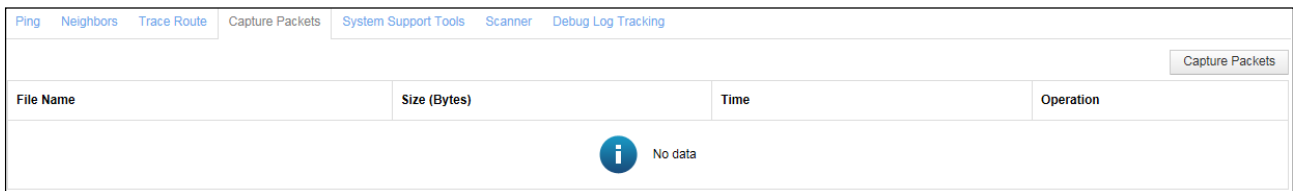
Note

The packet capture tool can be used to capture packets transferred only through working interfaces, but not those through out-of-band management interfaces.

To capture packets, perform the following steps:

Step 1 Choose **System Management > Test Tools > Capture Packets**.

Figure 7-67 Capture Packets page



Step 2 Click **Capture Packets**.

Figure 7-68 Setting packet capturing parameters

Capture Packets [X]

☐ Packet Number

☐ cap File Capacity (MB)

☐ Packet Length (bytes)

☐ Packet Direction

☐ Source IP Address

☐ Destination IP Address

☐ IP Address in Any Direction

☐ Protocol

☐ Interface ?

☐ Source Port

☐ Destination Port

☐ Port in Any Direction

Step 3 In the dialog box, set the packet capture parameters.

Table 7-11 Parameters for capturing packets

Parameter	Description
Packet Number	Number of packets to be captured.
cap File Capacity	Maximum size of a packet capture file.
Packet Length	Length (in bytes) of packets to be captured. The value 0 indicates that the packet length is not restricted.
Packet Direction	Direction of packets to be captured. The value can be Rx , Tx , or All . <ul style="list-style-type: none"> Rx: indicates the system captures packets that are received. Tx: indicates that the system captures packets that are sent. All: indicates that the system captures packets that are sent and that are received.

Parameter	Description
Source IP Address	Source IP address of packets to be captured. If no source IP address is specified, packets from any IP address can be captured.
Destination IP Address	Destination IP address of packets to be captured. If no destination IP address is specified, packets destined for any IP address can be captured.
IP Address in Any Direction	Source or destination IP address of packets to be captured. If no IP address is specified, packets from and destined for any IP address can be captured.
Protocol	Protocol adopted by packets to be captured. The protocol type can be NON , ARP , TCP , UDP , or ICMP . If no protocol is specified, packets using any protocol can be captured.
Interface	Interface over which packets to be captured are transmitted.
Source Port	Source port of packets to be captured. If no source port is specified, packets from any port can be captured.
Destination Port	Destination port of packets to be captured. If no destination port is specified, packets destined for any port can be captured.
Port in Any Direction	Source port or destination port of packets to be captured. If no port is specified, packets from and destined for any port can be captured.

Step 4 Click **OK** to start capturing packets.

If you want to reset the parameters, click **Reset** to restore the default settings of the parameters.

Figure 7-69 Capture Packets page in the process of a capture task



Ping Neighbors Trace Route Capture Packets System Support Tools Scanner Debug Log Tracking			
			Capturing packets... Stop Packet Capturing
File Name	Size (Bytes)	Time	Operation
wafg2_2016_03_30_11_19_13.cap	22991	2016-03-30 11:19:27	


During a capture task, you can click **Stop Packet Capturing** to stop capturing packets. After a packet capture task is successfully completed, the packet capture file will be listed in the list on the **Capture Packets** page, as shown in [Figure 7-70](#).

Step 5 Click a packet capture file listed in the **File Name** column or click  in the **Operation** column to download it to a local directory.

The downloaded file can be used to analyze whether the device sends and receives packets as expected, or analyze alert details.

Figure 7-70 Capture Packets page after a capture task is successfully completed

Ping Neighbors Trace Route Capture Packets System Support Tools Scanner Debug Log Tracking			
Capture Packets			
File Name	Size (Bytes)	Time	Operation
wafg2_2016_03_30_11_19_13.cap	91846	2016-03-30 11:19:57	 

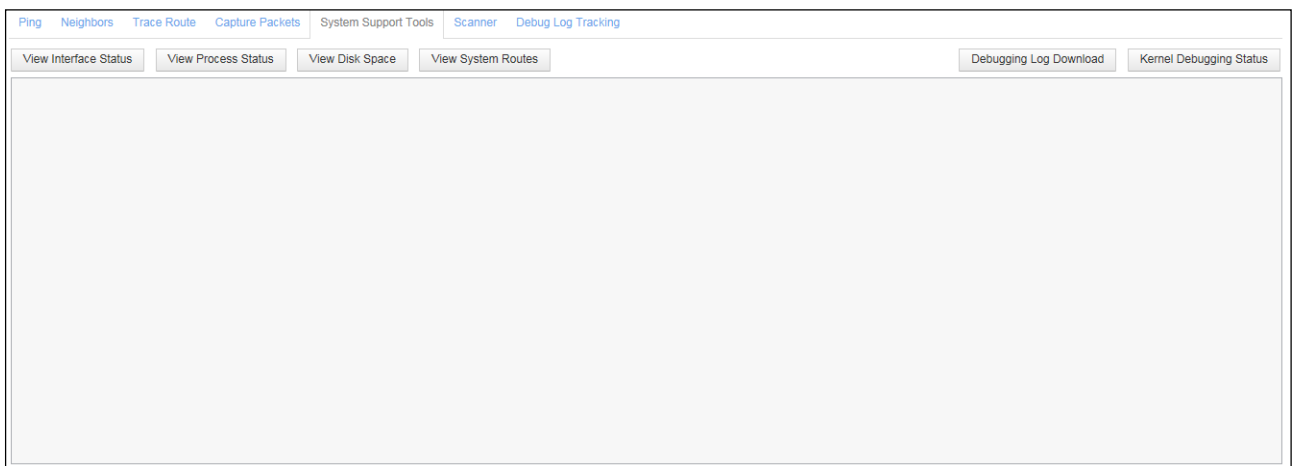
You can delete a packet capture file by clicking  in the **Operation** column.

----End

7.4.5 System Support Tools

System support tools are used by debugging personnel to download debug logs and view system interface status, process status, routes, and disk usage. Choose **System Management > Test Tools > System Support Tools**. The **System Support Tools** page appears, as shown in [Figure 7-71](#). You can click listed buttons to perform corresponding operations.

Figure 7-71 System Support Tools page



7.4.6 Scanner

A scanner is built in WAF to scan protected servers for website vulnerabilities.

To conduct scanning, perform the following steps:

Step 1 Choose **System Management > Test Tools > Scanner**.

Figure 7-72 Scanner page

Step 2 Click **Create**.

Figure 7-73 Creating a scanning task

Step 3 In the dialog box, set the scanning parameters.

Table 7-12 Parameters for creating a scanning task

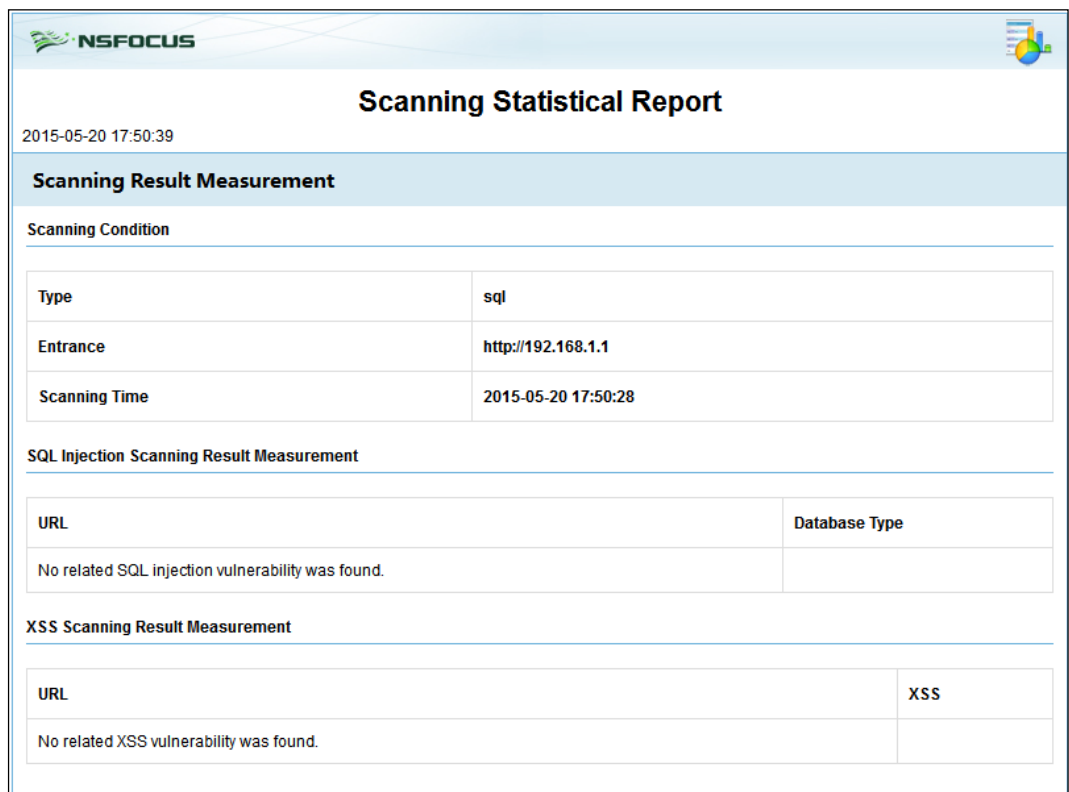
Parameter	Description
Name	Name of the new scanning task.
Scanning Mode	Scanning mode, which can be either of the following: <ul style="list-style-type: none"> SQL Injection and XSS Vulnerability Scanning Trojan scanning
Entrance URL	Starting URL to be scanned, for example, http:192.168.1.100/index.html.

Parameter	Description
Scanning Depth	Levels of web page links to be scanned. The recommended value is 5 .
Scanning Breadth	Keyword in domain names. URLs containing this keyword will be scanned. Enter an IP address here if the Scanning Entrance is set to an IP address.
Scanning Schedule Type	Scanning frequency, which can be Daily , Weekly , or Monthly .
Day/Date	Day/date when the scanning task is conducted if Scanning Schedule Type is set to Weekly or Monthly .
Scheduled Scanning Time	Specific time when the scanning task is conducted.
Whether Policy Applied	Controls whether the setting of the new scanning task takes effect. <ul style="list-style-type: none"> Enable: The setting takes effect immediately and the scanning task is conducted at the scheduled time. Disable: The setting does not take effect till it is enabled.

Step 4 Click **OK** to save the settings.

WAF executes the scanning task at the scheduled time. After the scanning task is completed, the scanning result appears in the area shown in [Figure 7-74](#).

Figure 7-74 Scanning result



----End

7.4.7 Debug Log Tracking

Debug log tracking refers tracking debug logs generated when WAF processes HTTP requests from the source IP address of a specified client. This can be used for engine troubleshooting.

Debug log tracking is applicable for IPv4 and IPv6 addresses, including proxy IP addresses in the HTTP X-forward-for header.

To conduct debug log tracking, perform the following steps:

Step 1 Choose **System Management > Test Tools > Debug Log Tracking**.

Figure 7-75 Debug Log Tracking page

Step 2 Determine whether to enable the debug log tracking function.

Click **Enable** or **Disable** to enable or disable debug log tracking respectively.

Step 3 Configure global settings.

Click **Global Config** to configure global parameters for debug log tracking as listed in [Table 7-13](#).

Table 7-13 Global parameters for debug log tracking

Parameter	Description
Log Level	Specifies the level of debug logs, which can be debug , info , warn , or error . The default value is warn . Change the setting with caution.
Trackings	A tracking refers to following the entire TCP process for a client IP address to access the server, from connection setup to disconnection. When the number of trackings reaches the specified threshold, the tracking stops.
Tracking Duration	Specifies how long a client IP address can be tracked. After a client IP address is added to the tracking list, the tracking stops when the specified duration expires.



The tracking stops when the threshold specified for **Trackings** or **Tracking Duration** is hit.

Step 4 Manage tracked IP addresses.

From the tracked IP address list, you can view the debug logs of HTTP requests from client IP addresses.

- a. Add an IP address for tracking.

Click **Create** in the upper-right corner of the **Tracked IP Addresses** area.

Figure 7-76 Adding an IP address for tracking

Type an IP address and then click **OK** to save the setting.




The IP address is then displayed in the tracked IP address list. **Function Status** is displayed as , indicating that this IP address is not tracked or the tracking is complete. See [Figure 7-77](#).

Figure 7-77 Tracked IP addresses

Tracked IP Addresses ^		
Page Number: 1 / 1 Record Number: 1 First Page Previous Page Next Page Last Page		
<input type="text" value="Enter IP address"/> Create		
IP Address	Function Status	Operation
10.67.1.9		 

- b. Click  in the **Operation** column of an IP address to dispatch or re-dispatch a tracking task of this IP address.

If **Function Status** is displayed as , it indicates that the IP address is under tracking.



- c. (Optional) Click  in the **Operation** column to delete a tracked IP address.

Step 5 Manage tracking logs.

After a tracking is complete, a log is generated and displayed in the **Tracked Logs** area.

Figure 7-78 Tracked logs

Tracked Logs ^			
File	Size (Bytes)	Time	Operation
T_tracelog bin	0	2016-03-17 18:01:28	 

- a. Download tracking logs.
Click  in the **Operation** column of an IP address to download its tracking log to a local disk drive.
- b. Click  in the **Operation** column of an IP address to clear its tracking log.



Currently, tracking logs are only intended for technical support personnel of NSFOCUS. Therefore, tracking logs can only be downloaded and cleared on the web-based manager. You can send downloaded tracking logs to NSFOCUS technical support personnel for troubleshooting.

----End

7.5 Collaboration with ESPC

WAF supports the connection to the NSFOCUS cloud, NSFOCUS security center (ESPC), and NSFOCUS Big Data Security Analysis (BSA).

- **NSFOCUS cloud**
The NSFOCUS cloud, which connects to NSFOCUS products, sends generated enterprise reputation and sample information to NSFOCUS ESPP. Then cloud security experts manually analyze reputation information that needs to be verified. After verification, reputation information is reimported to the global reputation cloud.
- **NSFOCUS ESPC**
NSFOCUS ESPC, a centralized management platform for NSFOCUS products, can conduct monitoring, policy configuration, and report management for multiple NSFOCUS products in a unified manner, greatly improving management efficiency.
- **NSFOCUS BSA**
BSA is a big data analysis platform for NSFOCUS products and third-party applications that meet certain requirements. Used to analyze security threat trends and provide support for customers' decision-making, NSFOCUS BSA incorporates the functions of data collection and storage, indexing, query, report customization, real-time alerting, and basic analysis.

To configure ESPC-related settings on WAF, perform the following steps:

Step 1 Choose **System Management** > **ESPC**.

The **ESPC** page varies with WAF devices in different management modes. [Figure 7-79](#) shows the page on a WAF device under non-centralized management, and [Figure 7-80](#) shows the page on a WAF device under centralized management.

Figure 7-79 ESPC page – under non-centralized management

Network Configuration	System Deployment	System Tools	Test Tools	ESPC	User Management	Traffic Control Mgmt																												
Local IP																																		
Local IP <input type="text" value="10.67.10.94"/>																																		
NSFOCUS Cloud																																		
Device Care Service <input checked="" type="radio"/> Enable <input type="radio"/> Disable Go to Cloud ✓ Connected																																		
<input type="button" value="Apply"/> Terms of Use																																		
ESPC																																		
<table border="1"> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Port</td> <td><input type="text" value="443"/></td> <td>Data transmission</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Port</td> <td><input type="text" value="443"/></td> <td>Data transmission</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Port</td> <td><input type="text" value="443"/></td> <td>Data transmission</td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Port</td> <td><input type="text" value="443"/></td> <td>Data transmission</td> <td><input type="checkbox"/> Enable</td> </tr> </table>							Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable	Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable	Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable	Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable				
Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable																													
Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable																													
Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable																													
Server Address	<input type="text"/>	Port	<input type="text" value="443"/>	Data transmission	<input type="checkbox"/> Enable																													
<input type="button" value="OK"/>																																		
Big Data Security Analysis (BSA)																																		
<table border="1"> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Security Log Interface</td> <td><input type="text" value="5666"/></td> <td>Status Log Interface</td> <td><input type="text" value="5666"/></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Security Log Interface</td> <td><input type="text" value="5666"/></td> <td>Status Log Interface</td> <td><input type="text" value="5666"/></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Security Log Interface</td> <td><input type="text" value="5666"/></td> <td>Status Log Interface</td> <td><input type="text" value="5666"/></td> <td><input type="checkbox"/> Enable</td> </tr> <tr> <td>Server Address</td> <td><input type="text"/></td> <td>Security Log Interface</td> <td><input type="text" value="5666"/></td> <td>Status Log Interface</td> <td><input type="text" value="5666"/></td> <td><input type="checkbox"/> Enable</td> </tr> </table>							Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable	Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable	Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable	Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable
Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable																												
Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable																												
Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable																												
Server Address	<input type="text"/>	Security Log Interface	<input type="text" value="5666"/>	Status Log Interface	<input type="text" value="5666"/>	<input type="checkbox"/> Enable																												
<input type="button" value="OK"/>																																		
Other																																		
Interface Version 3.0.5.37838																																		
Interface Upgrade Time																																		
Interface Update <input type="button" value="Select File"/> No file selected <input type="button" value="Upgrade"/>																																		
Debugging Information <input type="button" value="Click to Obtain"/>																																		

Figure 7-80 ESPC page – under centralized management

The screenshot displays the NSFOCUS WAF V6.0 interface under centralized management. The top navigation bar includes tabs for Network Configuration, System Deployment, System Tools, Test Tools, ESPC (selected), User Management, and Traffic Control Mgmt.

Local IP

Local IP: 10.67.10.25

NSFOCUS Cloud

Device Care Service: ☒ Enable ☐ Disable [Go to Cloud](#) Connected

[Apply](#) [Terms of Use](#)

ESPC

Server Address: 10.67.10.221 Port: 443 Data transmission: ☒ Enable Connected [exit ESPC central manage](#)

Server Address: Port: 443 Data transmission: ☐ Enable

Server Address: Port: 443 Data transmission: ☐ Enable

Server Address: Port: 443 Data transmission: ☐ Enable

[OK](#)

Big Data Security Analysis (BSA)

Server Address: Security Log Interface: 5666 Status Log Interface: 5666 ☐ Enable

Server Address: Security Log Interface: 5666 Status Log Interface: 5666 ☐ Enable

Server Address: Security Log Interface: 5666 Status Log Interface: 5666 ☐ Enable

Server Address: Security Log Interface: 5666 Status Log Interface: 5666 ☐ Enable

[OK](#)

Other

Interface Version: 3.0.5.37838

Interface Upgrade Time

Interface Update: [Select File](#) No file selected [Upgrade](#)

Debugging Information: [Click to Obtain](#)







1. On the web-based manager of WAF under centralized management, **Under centralized management** is displayed in the status bar. Pointing to it will display the following information:



- The device is under centralized management of ESPC.
- WAF in this state has limited functions. To remove such limitations, WAF should exit centralized management.
- The two methods for WAF to exit centralized management.

2. Different authorization methods may also result in slight differences in the **ESPC** page.

Step 2 In the dialog box, set the basic parameters.

Table 7-14 ESPC-related parameters on WAF

Parameter		Description
Local IP	Local IP	<p>IP address of WAF's management interface for the engine for communicating with the NSFOCUS cloud, NSFOCUS ESPC, and NSFOCUS BSA.</p> <p> Note</p> <p>By default, it is the first IP address of the first management interface. The default value is recommended.</p>
NSFOCUS Cloud	Device Care Service	<p>Controls whether to enable device care service.</p> <p>After the device care service is enabled, you can click Go to Cloud to open the homepage of the NSFOCUS cloud. In the dialog box that appears, you can register an account bound to WAF or use the default account to view device status information.</p> <p>An at-one-click account corresponds only to one WAF device and can connect to the NSFOCUS cloud only via WAF. A registered account can be bound to multiple WAF devices and can be used to view information of multiple devices.</p> <p>You can also view device status information on the device care service page on the NSFOCUS cloud.</p> <p> Note</p> <ul style="list-style-type: none"> By default, the device care service is enabled expect the international version. You can click Terms of Use to view the terms for using the device care service. To use WAF, you must log in to NSFOCUS Cloud or download and install a mobile app. You can use the device care service at one click or by registering an account bound to the device. Then you can log in to the NSFOCUS cloud or mobile app by using the account. If the registered account is not bound, cloud-based users cannot view information about WAF after login. If the device care service is disabled, WAF will no longer send any logs to the cloud.
ESPC	Server Address	<p>IP addresses of NSFOCUS ESPCs. WAF can connect to a maximum of four NSFOCUS ESPCs. To connect WAF to an NSFOCUS ESPC, select the Start check box to its right.</p> <p>If centralized management under ESPC is successfully configured, a link saying exit ESPC central manage is displayed. For details, see the <i>NSFOCUS ESPC User Guide - WAF</i>.</p>
	Port	Specifies the port used by ESPC to exchange data with the WAF engine.
	Data Transmission	<p>Controls whether to start connecting WAF to ESPC. Selecting the Start check box enables WAF to connect to ESPC.</p> <p> Note</p> <p>If the icon  is displayed, the connection has been established.</p>

Big Data Security Analysis (BSA)	Server Address	IP address of BSA to which WAF will connect.
	Security Log Interface	Port used by BSA to receive security logs from WAF.
	Status Log Interface	Port used by BSA to receive status logs from WAF.
	Enable	Controls whether to connect WAF to BSA. Selecting the Enable check box enables such connection.  Note When  is displayed, the connection has been established.
Other	Interface Version	Version of the NPAI interface.
	Interface Upgrade Time	Upgrade time of the NPAI interface.
	Interface Upgrade	You need to click Browse to select an interface upgrade file of the local ESPC and click Upgrade to upgrade the interface.
	Debugging Information	Status information about the collaboration (over the NPAI interface) between WAF and NSFOCUS ESPC. The debugging information can be used for fault location if the collaboration failed. You can click Click to Obtain to download the debugging information to a local directory.

Step 3 Click **Apply** to save settings of **Local IP** and **Device care service**. Click **OK** to save ESPC settings.

----End

7.6 User Management

The **User Management** page is used to manage accounts of WAF and related configurations. This section covers the following parts:

- Managing accounts: describes how to create, edit, and delete user accounts of WAF.
- Configuring user security: describes how to configure account security settings, such as password security and login limitations.
- Configuring login control: describes how to enable remote assistance.
- Configuring authentication: describes how to configure user authentication ways.
- Unblocking accounts: describes how the **admin** account unlocks other accounts.

7.6.1 Account Management

There are two default accounts: default administrator account **admin**, default auditor account **auditor**, and default maintenance account **maintainer**.

- The **admin** account has all privileges except managing auditors and viewing audit logs. It can create administrator and common user accounts.

- The **auditor** account has the privileges of viewing audit logs.
- The **maintainer** account has the privileges of managing and configuring system engine parameters.



For details about the privileges of administrator and common user accounts, see section [2.2 System Users](#).

The procedures of creating and editing an account are similar for the **admin**, **auditor**, and **maintainer** accounts. The following uses the **admin** account as an example.

Creating an Account

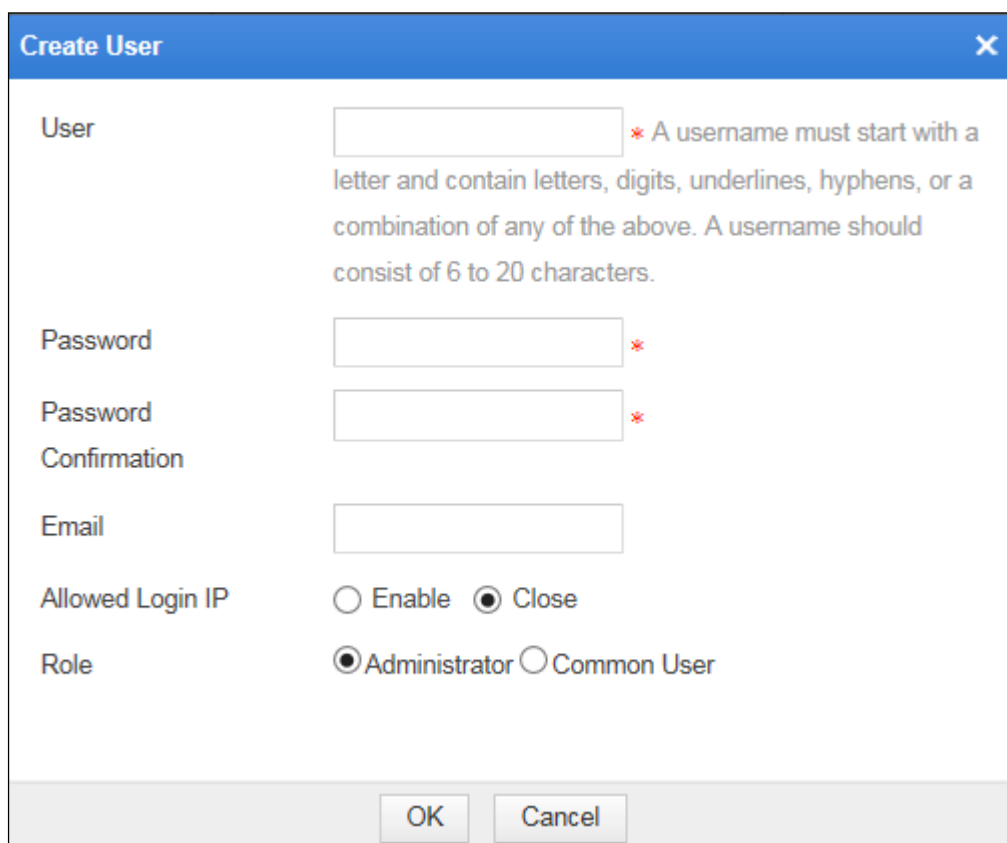
Step 1 Choose **System Management > User Management > User Management**.

Figure 7-81 User Management page

User Management	User Security	Login Control	Authentication Configuration	Account Unlocking	
					Create
Type	User	Status	Role	Email	Operation
	admin		Administrator		

Step 2 Click **Create**.

Figure 7-82 Creating a user



The 'Create User' dialog box contains the following fields and options:

- User:** A text input field with a red asterisk and a note: '* A username must start with a letter and contain letters, digits, underlines, hyphens, or a combination of any of the above. A username should consist of 6 to 20 characters.'
- Password:** A text input field with a red asterisk.
- Password Confirmation:** A text input field with a red asterisk.
- Email:** A text input field.
- Allowed Login IP:** Radio buttons for ☐ Enable and ☒ Close.
- Role:** Radio buttons for ☒ Administrator and ☐ Common User.

At the bottom are 'OK' and 'Cancel' buttons.

Step 3 In the dialog box, set the account parameters.

Table 7-15 Parameters for creating an account

Parameter	Description
User	Login user name of the account. It must be a string of 6 to 20 characters. It can consist of digits, letters, underscores, and/or hyphens, but must start with a letter.
Password	Login password of the account. The password length and complexity are configured by the admin account on the User Security page. For details, see section 7.6.2 User Security . The user name and password of an account must be different.
Password Confirmation	Password reentered for confirmation.
Email	Valid email address for the account.
Allowed Login IP	Controls whether login IP addresses are restricted. <ul style="list-style-type: none"> Enable: Only IP addresses specified in the text box below are allowed to log in to WAF. Both IPv4 and IPv6 addresses are supported. Close: No restriction is imposed on login IP addresses
Role	Role of the account. Different roles have different privileges. Roles include Administrator and Common User .

Step 4 Click **OK** to save the settings.

----End

Editing an Account

The **admin** account can edit an account after it is created. To do that, perform the following steps:

Step 1 In the account list shown in [Figure 7-81](#), click  in the **Operation** column.

The dialog box for editing the account's parameters appears.

- For a created account, all account parameters except **User** can be modified.
- For the default **admin** account, only the password, email, and allowed login IP address can be changed.

Step 2 Edit parameters and click **OK** to save the setting and return to the account list.

----End

Deleting an Account

The default **admin** account cannot be deleted. To delete a created account, perform the following steps:

Step 1 In the account list shown in [Figure 7-81](#), click  in the **Operation** column.





The deletion confirmation dialog box appears.

Step 2 Click **OK**.

----End

Enabling/Disabling Accounts

By default, the default **admin** account is always enabled. You can enable/disable created accounts.

- In the account list shown in [Figure 7-81](#), click  in the **Operation** column to enable an account. After it is enabled, its status turns to .
- In the account list shown in [Figure 7-81](#), click  in the **Operation** column to disable an account. After it is disabled, its status turns to .

7.6.2 User Security

Administrators can configure security settings of WAF accounts. The settings include the password length and complexity, allowed login failures, lockout period, and others. To configure user security, perform the following steps:

Step 1 Choose **System Management > User Management > User Security**.

Figure 7-83 User Security page

Network Configuration	System Deployment	System Tools	Test Tools	ESPC	User Management	Traffic Control Mgmt
<div> User Management User Security Login Control Authentication Configuration Account Unlocking </div>						
<div> <div>Weak Password Checking</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Close </div> </div>						
<div> <div>Password Length</div> <div>8</div> </div>						
<div> <div>Password Complexity</div> <div> <input checked="" type="checkbox"/> Number <input checked="" type="checkbox"/> Lower-case letter <input type="checkbox"/> Upper-case letter <input type="checkbox"/> Symbol </div> </div>						
<div> <div>Login Error Restriction</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Close </div> </div>						
<div> <div> <input checked="" type="radio"/> Account Locking <input type="radio"/> IP Locking </div> </div>						
<div> <div>Allowed Login Failures</div> <div>3</div> </div>						
<div> <div>Lockout Period (minute)</div> <div>30</div> </div>						
<div> <div>Periodical Password Update</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Close </div> </div>						
<div> <div>Update Cycle (day)</div> <div>90</div> </div>						
<div> <div>Timeout Interval Setting</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Close </div> </div>						
<div> <div>Timeout Interval (minute)</div> <div>30</div> </div>						
<div>OK</div>						

Step 2 In the dialog box, set the user security parameters.

Table 7-16 Parameters for configuring user security

Parameter	Description
Weak Password Checking	Controls whether to enable weak password checking. After this parameter is set to Enable , Password Length and Password Complexity appear and need to be specified. A qualified password needs to satisfy the settings of Password Length and Password Complexity .
Password Length	Length of the password used for login. The password should be a string of 6 to 20 characters.
Password Complexity	Complexity of the password used for login. This parameter determines whether passwords must contain digits, lowercase letters, uppercase letters, or special characters. At least two of them should be selected.
Login Error Restriction	Controls whether to enable restrictions to login errors. After this parameter is set to Enable , if the number of an account's consecutive login failures exceeds the number specified by Allowed Login Failures , the account is prohibited from logging in again within the period specified by Lockout Period(minute) .
Allowed Login Failures	For account locking, it indicates the number of consecutive login failures before an account is locked. For IP locking, it indicates the number of consecutive login failures before

Parameter	Description
	an IP address is locked.
Lockout Period (minute)	For account locking, it indicates the period during which an account is locked. For IP locking, it indicates the period during which an IP address is locked.
Periodical Password Update	Controls whether to enable periodical password update. After this parameter is set to Enable , if a password's life time exceeds the period specified by Update Cycle (day) , you need to change the password.
Update Cycle (day)	Cycle for password update.
Timeout Interval Setting	Controls whether to enable timeout interval checking. After this parameter is set to Enable , if a logged-in account's idle period exceeds the period specified by Timeout Interval (minute) , the account automatically logs out.
Timeout Interval (minute)	Maximum idle period before logged-in accounts automatically log out.

Step 3 Click **OK** to save the settings.

----End

7.6.3 Login Control

When WAF fails or has exceptions, you can log in WAF in the way of remote assistance.

Security hazards may arise if the user forgets to disable remote assistance. To prevent this, after remote assistance is enabled, WAF monitors SSH connections of the remote assistance port and automatically disables remote assistance if no connection is detected in consecutive 24 hours.

Choose **System Management > User Management > Login Control**. The **Login Control** page appears, as shown in [Figure 7-84](#). Set **Remote Assistance** to **Enable** to enable the remote assistance function.

Figure 7-84 Login Control page

7.6.4 User Authentication

WAF supports Remote Authentication Dial In User Service (RADIUS) authentication and local authentication.

RADIUS is a standard client/server mode for clients to exchange information with servers containing user authentication and configuration information. The user authentication and

configuration information includes user names, access passwords, and access privileges. Usually, users use RADIUS authentication in remote access to devices.

RADIUS is usually installed on a server (that is, RADIUS authentication server), and the client protocol runs on remotely accessing devices, such as remote accessing servers or routers. RADIUS clients send authentication requests to the RADIUS server and act as instructed by responses from the RADIUS server.


To configure authentication, perform the following steps:

Step 1 Choose **System Management > User Management > Authentication Configuration**.

Figure 7-85 Authentication Configuration page

Step 2 On the **Authentication Configuration** page, set the authentication parameters.

Table 7-17 Parameters for configuring authentication

Parameter	Description
Authentication Way	Way to authenticate accounts. <ul style="list-style-type: none"> RADIUS Authentication: indicates that account authentication is performed via RADIUS. You need to set RADIUS authentication parameters. Local Authentication: indicates that accounts are authenticated only on WAF.
Authentication Server	IP address of a RADIUS authentication server. Both IPv4 and IPv6 addresses are supported.
Authentication Mode	Authentication mode of a RADIUS authentication server, which can be pap , spap , chap , mschapv1 , or mschapv2 .
Authentication Port	Port on which the RADIUS authentication server listens authentication requests. The default RADIUS authentication port is port 1812.
Authentication Shared Key	Authentication shared key of a RADIUS authentication server.  Note The authentication shared key configured on WAF must be consistent with that configured on the RADIUS server. Otherwise, WAF cannot communicate with the RADIUS server.
Authentication Duration (second)	Duration for the authentication server to authenticate a RADIUS client. It is an integer ranging from 5 to 60.

Step 3 Click **OK** to save the settings.

----End

7.6.5 Account Unlocking

After the login attempt restriction function is enabled on the **User Security** page, the user is locked out in a specified period when the maximum number of allowed login attempts is exceeded. Only when the **admin** user unlocks this user account, the user is allowed to log in to the system again.





Choose **System Management > User Management > Account Unlocking**. The **Account Unlocking** page appears, as shown in Figure 7-86. You can click  in the **Operation** column to unlock a user account. To unlock more than one user account, select user accounts and click **Unlock** to unlock them.

Figure 7-86 Account Unlocking page

User Management User Security Login Control Authentication Configuration Account Unlocking					
<input type="checkbox"/>	Type	User	Status	Role	Operation
<input type="checkbox"/>		auditor		Auditor	
					<button>Unlock</button>





7.7 Traffic Control Management

When deployed in in-path, out-of-path, or reverse proxy mode, WAF can restrict the rate of traffic to specified domain names to mitigate or reduce traffic conflicts in the current network.

Enabling/Disabling the Traffic Control Function

Step 1 Choose **System Management > Traffic Control Mgmt.**

Figure 7-87 Traffic Control Mgmt page

Network Configuration System Deployment System Tools Test Tools ESPC User Management Traffic Control Mgmt Online Help					
<input checked="" type="checkbox"/> Enable traffic control <input type="checkbox"/> Close new connection after traffic control					
Page Number: 1 / 1 Record Number: 1 <button>First</button> <button>Previous</button> <button>Next</button> <button>Last</button> <button>Bulk Enable</button> <button>Bulk Disable</button> <button>Bulk Delete</button> <button>Create</button> 					
<input type="checkbox"/>	Object Name	Status	Upper Traffic Limit	Included Domain Name	Operation
<input type="checkbox"/>	test		64MBps	*	  

Step 2 Select the **Enable traffic control** check box, and then click **OK** in the confirmation dialog box to enable the traffic control function.

To disable this function, deselect the check box and click **OK** in the confirmation dialog box.



Note

In the case of either of the following, the traffic control function for these domain names included in traffic control objects loses effect and such domain names disappear from traffic control objects. Also, traffic control logs of such domain names are deleted. If all domain names included in a traffic control object are deleted, this object and traffic control logs relating to this object are also deleted.

The procedure is as follows:

- Websites or website groups using domain names included in traffic control objects are deleted.
- The domain name of the proxied server of an existing website is edited.

----End

Creating a Traffic Control Object

Prior to creating a traffic control object, you need to add websites on domain names for such websites on the **Website Group Mgmt** page. For details, see section [4.3.2.1 Adding Websites](#). Each domain name can be included in one traffic control object. When domain names are used up, you cannot create traffic control objects.

To create a traffic control object, perform the following steps:

Step 1 Click **Create** on the **Traffic Control** page shown in [Figure 7-87](#).

Figure 7-88 Creating a traffic control object

Step 2 In the dialog box, set the traffic control object parameters.


Table 7-18 Parameters for creating a traffic control object

Parameter	Description
Object Name	Name of the new traffic control object. The name must be unique.
Upper Traffic Limit	Upper limit of the traffic rate. It must be an integer.
Description	Brief description of the new traffic control object.
Included Domain Name	Domain name included in the new traffic control object. You can select one or more objects, or select all to include all domain names in the object. The domain name list shows all domain names configured for websites when WAF is in reverse proxy mode.

Step 3 Click **OK** to save the settings.

----End

Editing a Traffic Control Object


Step 1 On the **Traffic Control** page shown in Figure 7-87, click  in the **Operation** column to edit its parameters (including **Object Name**).

Step 2 Click **Save** to save the setting and return to the **Traffic Control** page.

----End

Deleting Traffic Control Objects



You can delete traffic control objects as follows:

- On the **Traffic Control** page shown in Figure 7-87, click  in the **Operation** column and then click **OK** in the confirmation dialog box to delete a traffic control object.
- On the **Traffic Control** page shown in Figure 7-87, select one or more traffic control objects, click **Bulk Delete** to and then click **OK** in the confirmation dialog box to delete the selected traffic control objects.

Enabling Traffic Control Objects



By default, a new traffic control object is enabled.

You can enable traffic control objects as follows:

- On the **Traffic Control** page shown in Figure 7-87, click  in the **Operation** column to enable a traffic control object. After  appears in the **Status** column, this object is enabled.
- On the **Traffic Control** page shown in Figure 7-87, select one or more traffic control objects, click **Bulk Enable** to and then click **OK** in the confirmation dialog box to enable the selected traffic control objects.

Disabling Traffic Control Objects

You can disable traffic control objects as follows:

- On the **Traffic Control** page shown in [Figure 7-87](#), click  in the **Operation** column to disable a traffic control object. After  appears in the **Status** column, this object is disabled.
- On the **Traffic Control** page shown in [Figure 7-87](#), select one or more traffic control objects, click **Bulk Disable** to and then click **OK** in the confirmation dialog box to disable the selected traffic control objects.

----End

Rejecting New Connection Requests After Traffic Control

On the page shown in [Figure 7-87](#), select the **Close new connection after traffic control** check box and click **OK** in the confirmation dialog box. In this case, after the traffic rate of a traffic control object is being restricted to the upper limit, WAF will reject new requests from clients. Also, clients attempting to access websites that use domain names in the traffic control object are rejected

To disable this function, deselect the **Close new connection after traffic control** check box and click **OK** in the confirmation dialog box. In this case, even if the traffic rate of a traffic control object is restricted to the upper limit, new requests from clients will not be dropped, but be saved in WAF and sent after a delay. Such requests will consume some resources on WAF.

7.8 System Parameter Configuration

System parameters include engine parameters, a kernel parameter, an Apache parameter, and other parameters.

7.8.1 Engine Parameter

After a successful login to the system, the **maintainer** user can configure engine parameters. For information about the **maintainer** account, see appendix [A.2 Default Accounts](#).

Step 1 Choose **System Management > System Parameter Configuration > Engine Parameters**.

Figure 7-89 Engine Parameters page

Engine Parameters	Kernel Parameter	Apache Parameter	Other Parameters
Core Parameters			
Max Retransmission Count	15		The default value is 15. Try increasing the value (max: 255) in the case of a low HTTP access speed.
Idle Timeout	5		The default value is 5s. Try decreasing the value (min: 1s) in the case of a low HTTP access speed.
Retransmission Timeout	300		The default value is 300s. Try increasing the value (max: 3600s) in the case of a low HTTP access speed.
Receiving Buffer	4096		The default value is 4 KB. Try increasing the value (max: 10 KB) when the HTTP access page cannot be properly displayed.
Sending Buffer	4096		The default value is 4 KB. Try increasing the value (max: 10 KB) when the HTTP access page cannot be properly displayed.
RST Connection	<input checked="" type="radio"/> Close <input type="radio"/> Enable		By default, it is disabled. In particular circumstances, you can enable it to improve the TCP connection closing speed.
Core Dump	<input type="radio"/> Close <input checked="" type="radio"/> Enable		By default, it is enabled. When an engine exception occurs, a core dump file is generated to collect related information. If this function is not used, disable it.
Auxiliary Request Check Library			By default, it is disabled. When routine checks find suspicious request packets pass through WAF without being detected, first check whether the problem is caused by configurations. If not, consider enabling auxiliary checking. This, however, will slightly degenerate the performance of WAF.
Auxiliary Response Check Library			By default, it is disabled. When routine checks find suspicious response packets pass through WAF without being detected, first check whether the problem is caused by configurations. If not, consider enabling auxiliary checking. This, however, will slightly degenerate the performance of WAF.
CPU Affinity	<input type="radio"/> Close <input checked="" type="radio"/> Enable		Enabled by default to bind the engine to CPU cores.
SSL Negotiation Times	0		The default value is 0, indicating no limit. If SSL renegotiation is disabled, please type 1.
SSL Cache Max Age	300		The default value is 300 seconds.
SSL QAT Delay	10		The default value is 10 milliseconds. This setting is valid only for QAT devices.
SSL QAT Client Sync Mode	<input checked="" type="radio"/> Close <input type="radio"/> Enable		Disabled by default. This setting is valid only for QAT devices.
SSL QAT Server Sync Mode	<input checked="" type="radio"/> Close <input type="radio"/> Enable		Disabled by default. This setting is valid only for QAT devices.
SSL Cache Mode	0		Disabled by default. After this is enabled, the engine will consume more memory space.
SSL Cache Reuse	<input checked="" type="radio"/> Close <input type="radio"/> Enable		Disabled by default. After being enabled, this setting is valid only in the case of HTTPS bidirectional proxy.
SSL Cache Reuse Ticket	<input type="radio"/> Close <input checked="" type="radio"/> Enable		Enabled by default. After being enabled, this setting is valid only in the case of HTTPS bidirectional proxy.
Cyclic Check Mode of Engine	1		The default value is 1, indicating the engine will implement proactive checking and protection. The value 0 indicates no checking and protection. The value 2 indicates the engine will not record real-time performance data. For the value 1, the engine will log real-time performance data every 5 seconds to facilitate analysis of real-time handling performance. For the value 2, the engine records thread-specific data in addition to real-time performance data.
Engine Performance Logging	0		By default, it is disabled, indicating that the engine will record and save real-time performance data for performance analysis. If this function is disabled, the engine will not record real-time performance data.
Engine Performance Monitoring	<input type="radio"/> Close <input checked="" type="radio"/> Enable		The default value is 2, indicating that the engine sets no_delay each time it forwards packets. When this parameter is set to 1, the engine sets no_delay only when it creates a socket. When this parameter is set to 0, the engine does not set no_delay. If all packets are small ones, this parameter should be set to 1.
no_delay	2		By default, it is disabled, indicating that the engine sets tcp_cork for a socket it creates. If it is disabled, the engine does not set tcp_cork.
Smart nagel	<input type="radio"/> Close <input checked="" type="radio"/> Enable		By default, it is disabled, indicating that the engine does not set this parameter for sockets it creates.
Keepalive	<input checked="" type="radio"/> Close <input type="radio"/> Enable		By default, it is disabled, indicating that the engine does not set this parameter for a listening socket.
deferAccept	<input checked="" type="radio"/> Close <input type="radio"/> Enable		
<input type="button" value="OK"/> <input type="button" value="Persist"/>			

Step 2 Configure engine parameters.

For detailed parameter description, please contact technical support personnel of NSFOCUS.

Step 3 Click **OK** to dispatch the engine parameter settings to the engine.

Restarting the engine will restore the engine parameter settings to the defaults.

Step 4 (Optional) Click **Persist** to save engine parameter configuration to the engine configuration file and then dispatch the settings to the engine.

After the engine is restarted, these settings can still take effect.

----End

7.8.2 Kernel Parameter

The kernel parameter is set to **Close** by default. It cannot be enabled in the NAT environment and can be enabled in other environments when the TCP protocol stack needs to be tested.

Step 1 Choose **System Management > System Parameter Configuration > Kernel Parameter**.

Figure 7-90 Kernel Parameter page

Engine Parameters	Kernel Parameter	Apache Parameter	Other Parameters
Core Parameter			
TCP Timestamp		<input checked="" type="radio"/> Close <input type="radio"/> Enable	By default, it is disabled. It cannot be enabled in the NAT environment. In other environments, it can be enabled only when the TCP protocol stack needs to be tested.
<input type="button" value="OK"/> <input type="button" value="Persist"/>			

Step 2 Set **TCP Timestamp** to **Enable**.

- If you click **OK**, the TCP timestamp is enabled but becomes disabled upon the restart of the WAF engine.
- If you click **Persist**, the TCP time stamp is enabled permanently.

----End

7.8.3 Apache Parameter

After a successful login to the system, the **maintainer** user can configure the Apache mode. By default, SSL certificates of weak cryptographic algorithms are used, supporting Internet Explorer 8. You can change the setting to High if SSL certificates of strong cryptographic algorithms are required.

Step 1 Choose **System Management > System Parameter Configuration > Apache Parameter**.

Figure 7-91 Apache Parameter page

Step 2 Set **Apache Mode** to **High**.

- If you click **OK**, the setting will remain valid until the device is restarted.
- If you click **Persist**, the setting remains valid even after the device is restarted.

----End

7.8.4 Other Parameters

After a successful login to the system, the **maintainer** user can choose **System Management > System Parameter Configuration > Other Parameters** to configure the state cryptography mode, which is useful only for customers in China. For information about the **maintainer** account, see appendix [A.2 Default Accounts](#).

The state cryptography mode is disabled by default. Users outside of China are advised to leave this parameter at its default value.

7.9 SSL Acceleration

After a successful login to the system, the **maintainer** user can enable or disable the SSL card. For information about the **maintainer** account, see appendix [A.2 Default Accounts](#).

Step 1 Choose **System Management > SSL Acceleration**.

Figure 7-92 SSL Acceleration page

Step 2 Click **Enable** or **Close** to enable or disable the SSL card.

Step 3 Click **OK** to save the settings.

----End

7.10 System O&M



After a successful login to the system, the **maintainer** user can collect information about the system and restore the system. For information about the **maintainer** account, see appendix [A.2 Default Accounts](#).

Step 1 Choose **System Management > System O&M**.

Figure 7-93 System O&M page

Step 2 Collect information about the system.

When the device fails, you can click **Start** to collect related information for exception cause analysis and troubleshooting.

- You can click  in the **Operation** column of a file to download it to a local disk drive.
- You can click  in the **Operation** column of a file to delete it.

Step 3 Restore the system.

When the system database, process, or engine fails, you can use system restoration functions for emergency restoration.

- Database: Click **Rebuild Database** to rebuild the database.
- Process: Click **Restart Web Service**, **Restart Engine Service**, **Restart Log Service** to restart corresponding services
- Engine: Click **Generate Engine Memory Dump** to generate a memory dump file for the engine. This file can be obtained by using the information collection function.



- Rebuilding the database clears all logs saved on the device.
- Clicking **Generate Engine Memory Dump** will generate a memory dump file for the engine. This file can be obtained by using the information collection function.

----End

7.11 REST API

After a successful login to the system, the **maintainer** user can configure the REST API. For information about the **maintainer** account, see appendix [A.2 Default Accounts](#).

Step 1 Choose **System Management > REST API > Digital Signature Parameters**.

Figure 7-94 Digital Signature Parameters page

Step 2 Configure the timeout.

Step 3 Click **OK** to save the settings.

----End

7.12 Site Control

After a successful login to the system, the **maintainer** user can configure WAF in mirroring mode to support HTTPS websites.

After the HTTPS website switch is turned on, you can create HTTPS websites and manage SSL certificates on WAF in mirroring mode.

Choose **System Management > Site Control**. On the **Site Control** page, click **Enable** to turn on support for HTTPS websites.

Figure 7-95 Site Control page

System Parameter Configuration System O&M REST API Site Control [Online Help](#)

Https site switch

Https site switch ☒ Close ☐ Enable

The default value is closed, only applied to the mirroring mode. Enabled functions: build HTTPS type site; SSL certificate management; Note that switching from Https to Http, the original Https site still exists, please manually modify or delete.

OK

8 Console-based Management

Using console connections, you can access the console of WAF, which provides certain functions such as initial system configuration, status detection, and restoration of the initial configurations. Also, functions and settings that cannot be managed on the web-based manager can be implemented on the console.

This chapter describes how to log in to the console and manage various information of WAF. It covers the following topics:

Topic	Description
Login to the Console	Describes how to log in to the console.
Console Functions	Describes how to manage various initial information of WAF.

8.1 Login to the Console

Before logging in to the console, you need to make the following preparations:

- One computer
- One serial port cable included in the accessory box
- Terminal software that can connect to the serial port (for example, the HyperTerminal software included in Microsoft Windows)
- Proper connection between WAF and the computer

The following uses the HyperTerminal software included in Microsoft Windows XP as an example to describe how to log in to the console:

Step 1 On the computer, choose **Start > Programs > Accessories > Communications > HyperTerminal**.

- If the **Location Information** dialog box shown in [Figure 8-1](#) appears, click **Cancel**. The **Connection Description** dialog box shown in [Figure 8-2](#) appears. Go to [Step 2](#).
- If the **Connection Description** dialog box shown in [Figure 8-2](#) appears, go to [Step 2](#).

Figure 8-1 Location Information dialog box

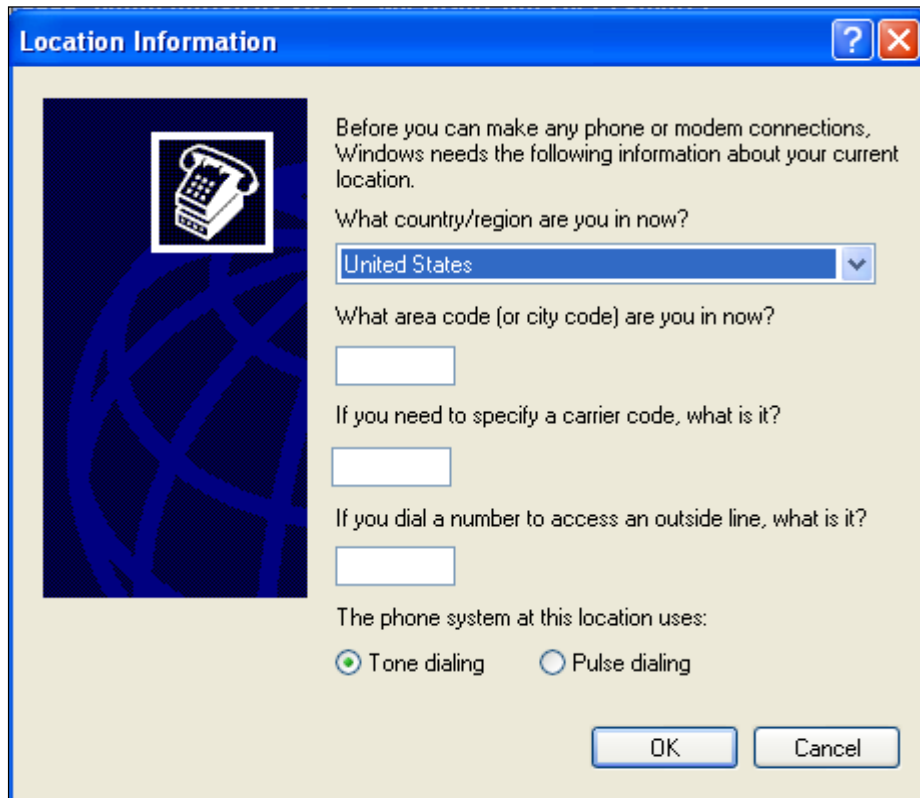


Figure 8-2 Connection Description dialog box



Step 2 Enter the connection name (WAF for example) in the **Name** text box, and click **OK**. The **Location Information** dialog box shown in [Figure 8-1](#) appears. Click **Cancel** and then **OK**. The **Connect to** dialog box appears, as shown in [Figure 8-3](#).

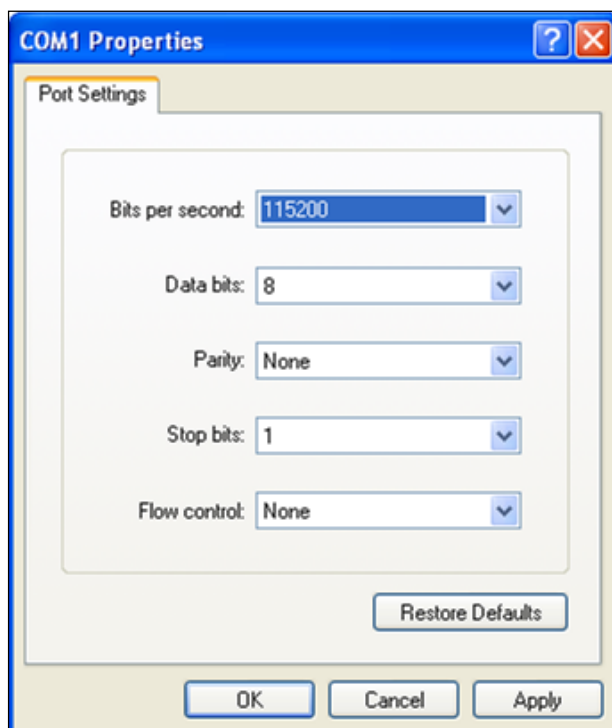
Figure 8-3 Connect to dialog box



Step 3 Select a serial port (**COM1** for example) and click **OK**.

The **COM1 Properties** dialog box appears, as shown in [Figure 8-4](#).

Figure 8-4 COM1 Properties dialog box



Step 4 Set port properties (**Bits per second** to **115200** and **Data bits** to **8**).

Step 5 Click **OK** and press **Enter**. The **login:** prompt appears. Type the user name and password (which are both **nsadmin**) of the console administrator.

If the user name and password are correct, you will log in successfully. (Display effect will be better with terminal ID VT100.)

Figure 8-5 Login page

```
localhost login: nsadmin
Password:
```

After login, the language selection window appears, as shown in [Figure 8-6](#).

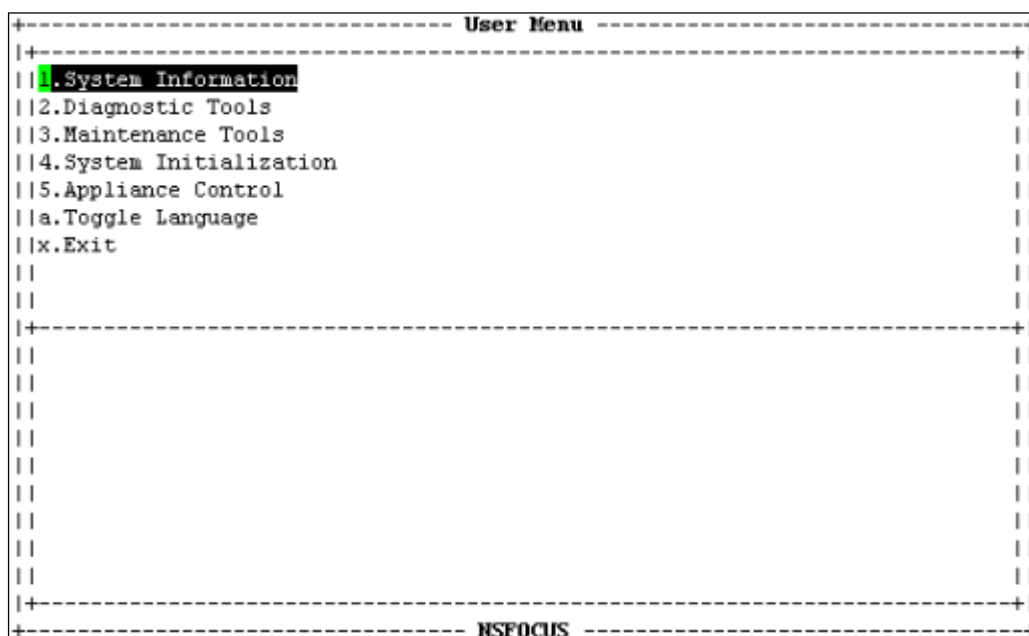
Figure 8-6 Language selection window

```
+----- select Language -----+
| 1. English |
| 2. 中文    |
+-----+
| English Menu |
| WARN:       |
| Please change nsadmin password! |
+-----+
```

Step 6 Select **1. English** and press **Enter**.

The **User Menu** window appears, as shown in [Figure 8-7](#).

Figure 8-7 User Menu window

**Note**

The console menu commands can only be executed using the keyboard. For the meaning of keys, see [Table 8-1](#).

Table 8-1 Meaning of keys

Key	Description
↑	Moves up.
↓	Moves down.
Esc	Cancels a setting.
Enter	Confirms a setting.
Tab	Switches between the input box, OK , and Cancel .
BackSpace	Deletes the character to the left of the cursor.

----End

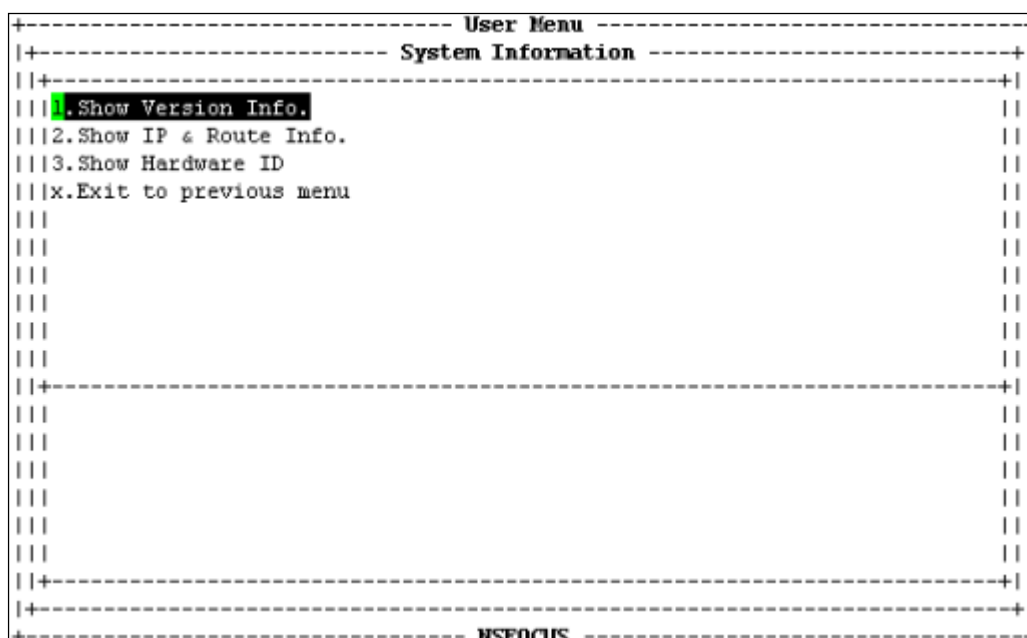
8.2 Console Functions

The following describes functions and operations on the console menu of WAF.

8.2.1 System Information

In the **User Menu** window shown in [Figure 8-7](#), move the cursor to **System Information** and press **Enter**. The **System Information** window appears, as shown in [Figure 8-8](#).

Figure 8-8 System Information window



The **System Information** window provides the following functions:

- **Show Version Info.**
Displays information about the current engine and firmware versions.
- **Show IP & Route Info.**
Displays information about the management IP address and routes.
- **Show Hardware ID**
Displays the hardware ID, which is a unique ID of each WAF engine and required for producing licenses.
- **Exit to previous menu**
Returns to the previous menu.



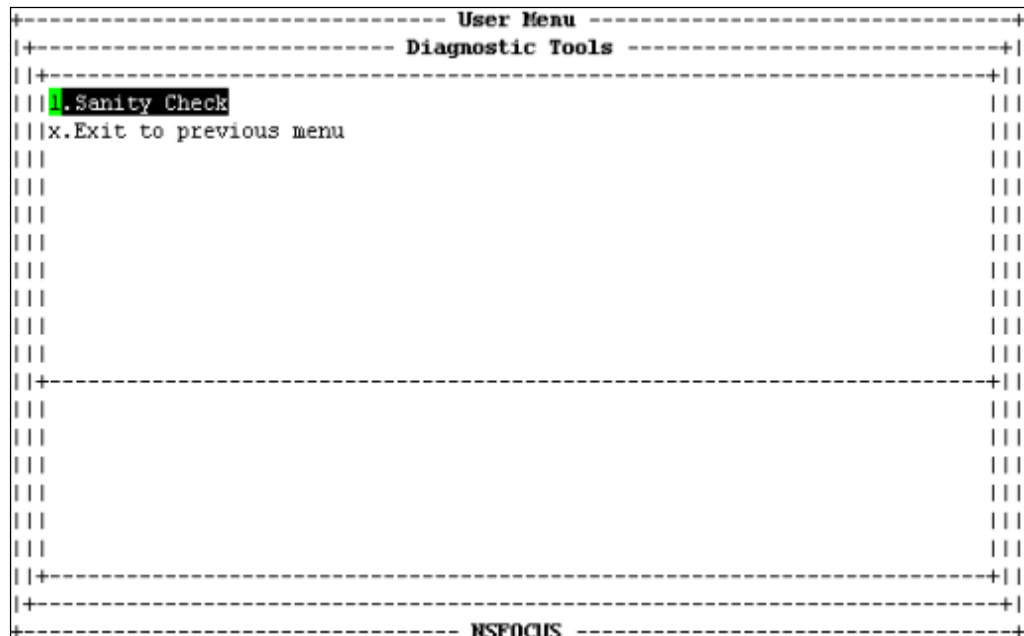
Note

No license is available in WAF when it leaves the factory. You can load a license in the web-based manager of WAF. For details about loading a license, see [section 7.3.5 License](#).

8.2.2 Diagnostic Tools

In the **User Menu** window shown in [Figure 8-7](#), move the cursor to **System Diagnosis** and press **Enter**. The **Diagnostic Tools** window appears, as shown in [Figure 8-9](#).

Figure 8-9 Diagnostic Tools window



The **Diagnostic Tools** window provides the following functions:

- **Sanity Check**
Checks whether hardware and software modules are normal on WAF.
- **Exit to previous menu**
Returns to the previous menu.



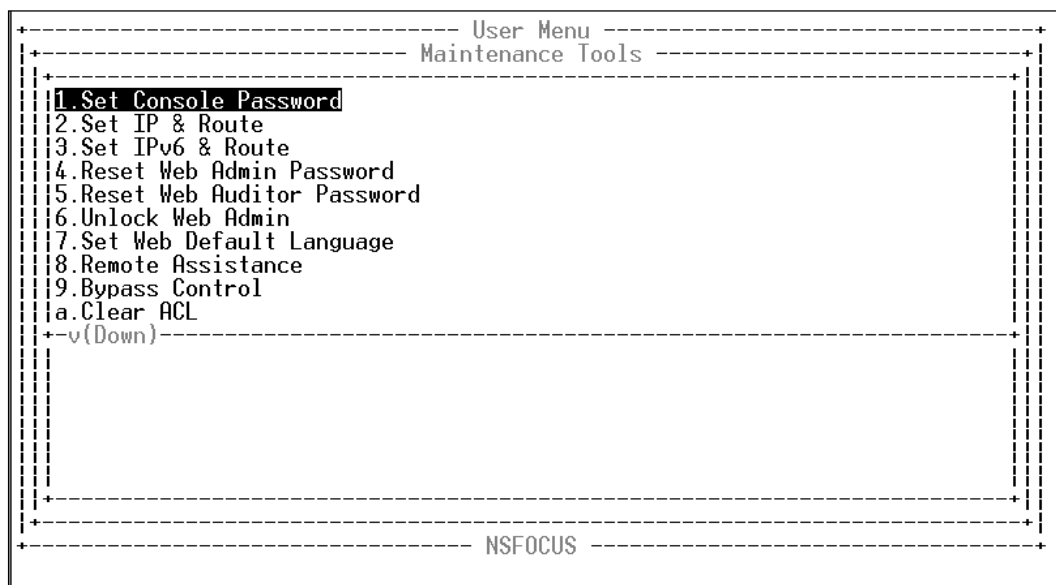
Note

You can also use diagnostic tools in the web-based manager of WAF.

8.2.3 Maintenance Tools

In the **User Menu** window shown in [Figure 8-7](#), move the cursor to **Maintenance Tools** and press **Enter**. The **Maintenance Tools** window appears, as shown in [Figure 8-10](#).

Figure 8-10 Maintenance Tools window



The **Maintenance Tools** window provides the following functions:

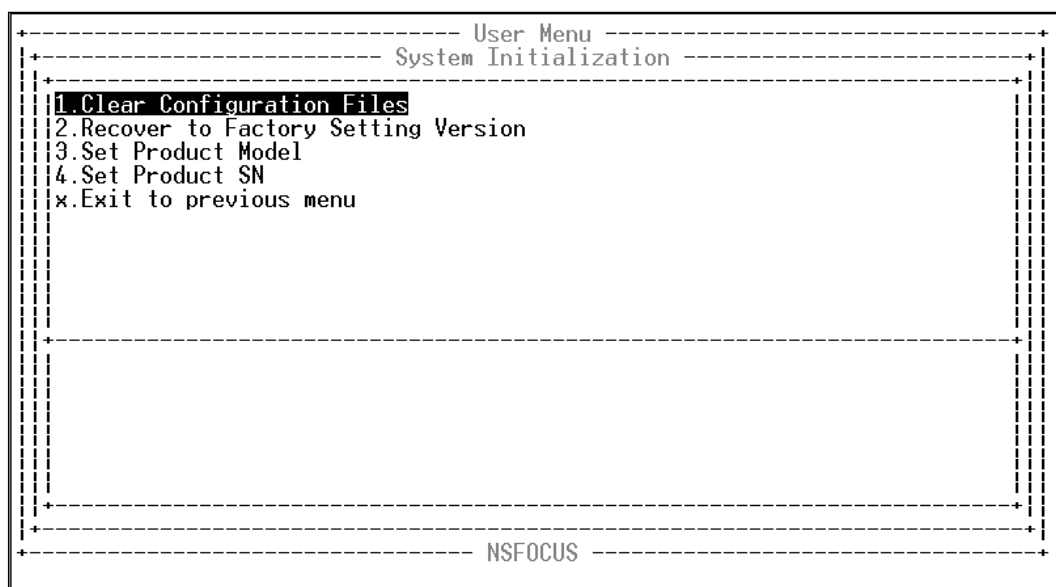
- **Set Console Password**
Sets the login password for the console administrator.
- **Set IP & Route**
Sets IPv4 addresses and routes.
- **Set IPv6 & Route**
Sets IPv6 addresses and routes.
- **Reset Web Admin Password**
Resets the login password for the administrator of the web-based manager to **admin**.
- **Reset Web Auditor Password**
Resets the login password for the auditor of the web-based manager to **auditor**.
- **Unlock Web Admin**
Unlocks the locked web administrator Admin.
- **Set Web Default Language**
Sets the default language of the web-based manager.
- **Remote Assistance**
Specifies whether remote assistance is enabled.
- **Bypass Control**
Specifies whether to enable the bypass function.
- **Clear ACL**
Unblocks all accounts (including **admin**) that are blocked.
- **Apache Management**
Sets the HTTPS port used to log in to the web-based manager. The default port is port 443.
- **Exit to previous menu**

Returns to the previous menu.

8.2.4 System Initialization

In the **User Menu** window shown in [Figure 8-7](#), move the cursor to **System Initialization** and press **Enter**. The **System Initialization** window appears, as shown in [Figure 8-11](#).

Figure 8-11 System Initialization window



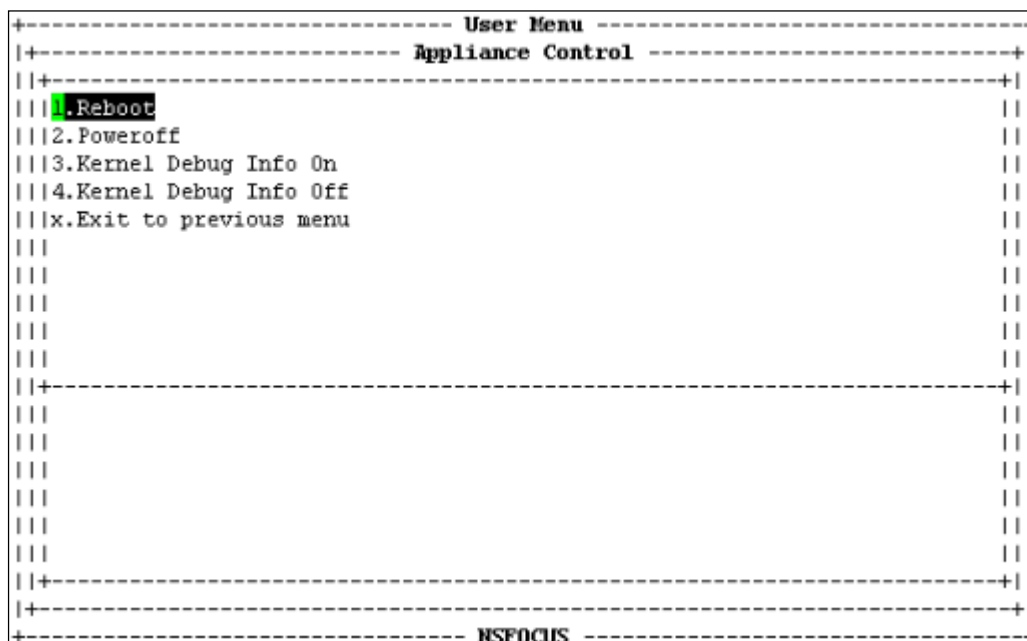
The **System Initialization** window provides the following functions:

- **Restore Factory Settings**
Restores the configurations of the current version. Usually, this operation usually changes configuration files only.
- **Recover**
Restores the version which is used when the device leaves the factory. This operation changes the system software, configuration file, and database, etc.
- **Set Product Model**
Sets the product model. The product model cannot be changed once being set.
- **Set Product SN**
Sets the product serial number. The product serial number cannot be changed once being set.
- **Exit to previous menu**
Returns to the previous menu.

8.2.5 Appliance Control

In the **User Menu** window shown in [Figure 8-7](#), move the cursor to **Appliance Control** and press **Enter**. The **Appliance Control** window appears, as shown in [Figure 8-12](#).

Figure 8-12 Appliance Control window



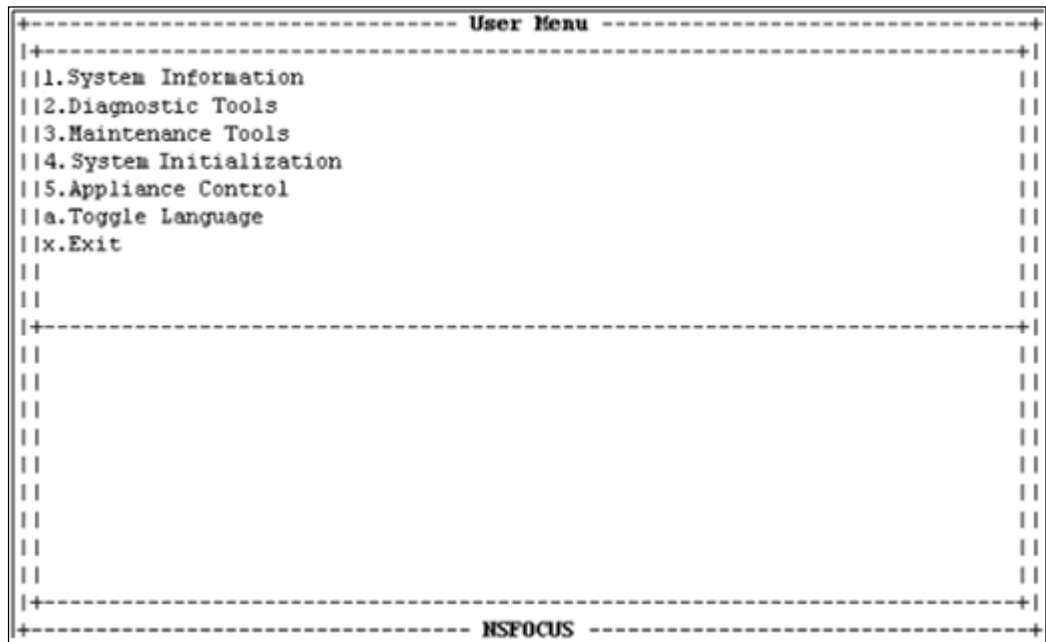
The **Appliance Control** window provides the following functions:

- **Reboot**
Reboots the device.
- **Poweroff**
Powers off the device.
- **Kernel Debug Info On**
Enables kernel debug information.
- **Kernel Debug Info Off**
Disables kernel debug information.
- **Exit to previous menu**
Returns to the previous menu.

8.2.6 Toggle Language

In the **User Menu** window shown in [Figure 8-13](#), move the cursor to **Toggle Language** and press **Enter** to switch the language between Chinese and English.

Figure 8-13 Toggling language



8.2.7 Exit

After configurations are completed, move the cursor to **Exit**, and press **Enter** to log out of the console. The system will prompt you to save the configuration. Select **Yes** to save before exiting, or select **No** to exit directly. If you need to modify the configurations, log in again.

A Default Parameters

A.1 Default Settings of the Management Interface

IP Address	eth0/M: 192.168.0.1
Network Mask	255.255.255.0

A.2 Default Accounts

	User Name	Password
Web Administrator	admin	admin
Web Auditor	auditor	auditor
Console Administrator	nsadmin	nsadmin

A.3 Console Port Communication Settings

Bits per Second	115200
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

B Regular Expressions

B.1 Single Character

Symbol	Description
.	It matches any single character. (By default, the line feed character is not included. If the s flag is on, the line feed character is included.)
[<i>any characters</i>]	It matches any single character specified in []. For example, [xyz] matches the x in axb , y in cya , and z in ucz . You can use a hyphen (-) to specify a range. For example, [a-z] matches any lower-case character, and [0-9] matches any digits ranging from 0 to 9.
[^ <i>any character</i>]	It matches any single character except those specified in [].
\d	It equals [0-9] and matches any single digit.
\D	It equals [^0-9] and matches any single character except digits ranging from 0 to 9.
\w	It equals [a-zA-Z0-9_] and matches any single upper-case letter, lower-case letter, and underline.
\W	It equals [^a-zA-Z0-9_] and matches any single character except upper-case letter, lower-case letter, and underline.
\s	It equals [\t\n\f\r] and matches a null character.
\S	It equals [^\t\n\f\r] and matches a non-null character.

B.2 Escape Character

Symbol	Description
^	Matches the beginning of a line or a text (when multi-line mode is on). For example, ^t matches the first t in test , not the last t .
\$	Matches the end of a line or a text (when multi-line mode is on). For example, t\$ matches the last t in test , not the first t .
\b	Matches a word boundary.
\B	Matches a non-word boundary.
\A	Matches the beginning of an entire paragraph, equaling (?s)^.

Symbol	Description
\Z	Matches the end of an entire paragraph, equaling (?s)\$.
\a	Matches the bell character in ASCII.
\f	Matches a form-feed character.
\t	Matches a tab character.
\n	Matches a newline character.
\r	Matches a carriage return character.
\v	Matches a vertical tab character.
*	Matches the preceding character zero or more times.
\\	\escape.
\123	Octal sign. For example, \011 means horizontal tab.
\x7f	Hex sign. For example, \x0a means a newline character.

B.3 Quantifiers

Symbol	Description
x{n,m}	Matches x at least n and at most m times, with m as the preferred number of matches.
x{n,}	Matches x at least n times until the end.
x{n}	Matches x exactly n times.
x*	Matches x zero or more times until the end. It equals x{0,}.
x+	Matches x one or more times until the end. It equals x{1,}.
x?	Matches x zero or one time. It equals x{0,1}.
?	Non-greedy mode. Appending the question mark (?) to another operator means the minimum number of matches. For example, x{2,4} matches xxxx , but x{2,4}? matches only xx .

B.4 Grouping

Symbol	Description
x y	Matches pattern x or y. For example, ab cd matches ab in tab or cd in pcd .
(x)	x in the brackets is used as a group to separate a pattern string into parts. For example, ab(c d) matches abc and abd , while abc d matches abc and d .
(?flags)	Enabling flags for the following pattern. The flags include the following: <ul style="list-style-type: none"> i: case-insensitive (off by default) m: multi-line mode (off by default)

Symbol	Description
	<ul style="list-style-type: none"> • s: line feed included (off by default) • U: non-greedy mode for all quantifiers (off by default) • Examples: • (?i) means case-insensitive. • (?-i) means case-sensitive. • (?i)a(?-i)a means that the first a is case-insensitive and the second a is case-sensitive.

B.5 Examples

- Matching any IPv4 address:
`(\d{1,3}\.){3}\d{1,3}`
- Matching all hosts in the **nsfocus.com** domain:
`([\\w-]+\\.)+nsfocus\\.com`
- Matching all .txt files in the **log** sub-directory of the root directory:
`^/log/[^\\"*\\?:"<>|]+\\.txt$`
- Matching all URL paths containing **.svn**:
`^\\.*/\\.svn/.*$`
- Matching jpg and jpeg files:
`^\\.*/ [^\\"*\\?:"<>|]+\\. (jpeg|jpg)$`