NSFOCUS WAF

User Guide

Version: V6.0R08F01 (2024-08-20)

Confidentiality: RESTRICTED

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

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

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

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.
8 API Protection	Describes how configure API protection.
9 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.

Change History

Version	Description
V6.0R08F01	Added support for source IP proxy in reverse proxy mode, port aggregation, and mirroring mode.
V6.0R08F00	Added support for transparent bridge mode, API security, dynamic protection, API compliance, and TLS 1.3.
V6.0R07F03	Initial release.

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.
Italic font	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.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- 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

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Product Introduction

This chapter describes customer values, advantages, and functions of WAF as well as its typical usage scenarios and deployment modes, providing users with a general idea of WAF.

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, a variety of web applications and APIs are prone to security vulnerabilities and protection measures are far behind attack methods.

NSFOCUS Web Application Firewall (WAF) is designed to protect web applications and APIs from online attacks. With a constantly updated vulnerability database, WAF enables security professionals, network administrators, and application developers to mitigate security risks and threats against web applications and APIs, therefore ensuring their availability and continuity.

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 multiple out-of-path deployment modes
- Support for traffic controls based on domain names
- Support for fine-grained application programming interfaces (APIs)
- Support for API security protection
- Support for dynamic protection
- Support for TLS 1.3
- Support for source IP proxy in reverse proxy mode
- Support for centralized management

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
- API security
  - API asset identification
  - API attack prevention
- Dynamic protection
  - Bot recognition
  - Token authentication
  - Web page element obfuscation
  - Data obfuscation

Customer Values

- 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 precision protection 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.

- API security

  Adopts active and passive approaches to assist customers in sorting out API assets and uses automatically generated API baselines and imported OAS files for API compliance check. It parses multiprotocol traffic to filter out attack traffic and analyzes malicious attack behaviors to ensure normal access of legitimate users.

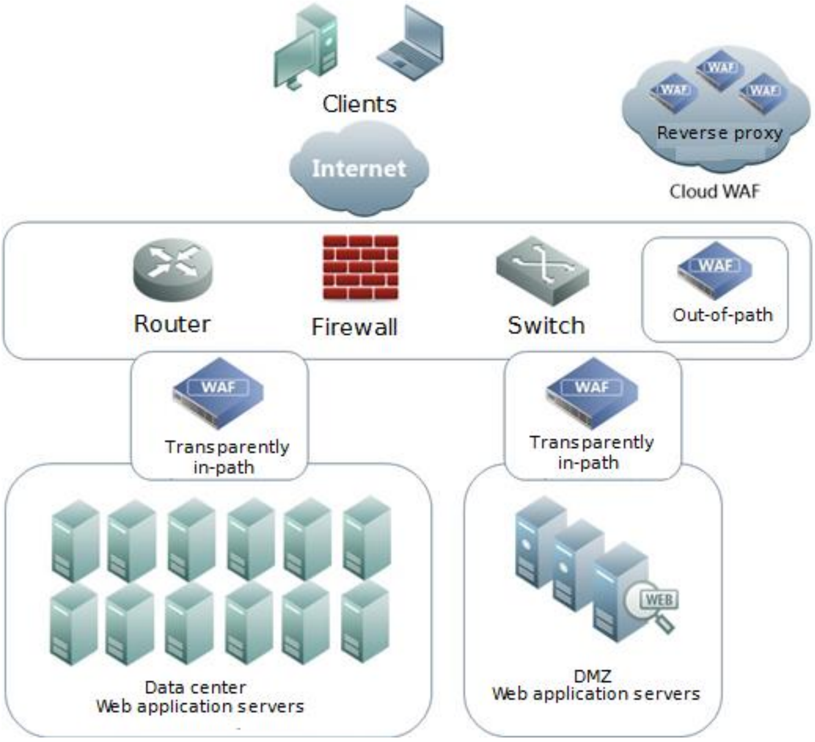
- Dynamic protection

  Dynamically implements and updates protection policies based on the network security situation, without needing manual update of signatures and protection rules, achieving the shift from passive protection to active security protection. Dynamic protection can effectively defend against known, unknown, and emerging security threats, implementing real-time dynamic protection. By using machine learning and big data technologies, WAF can comprehensively detect and analyze various abnormal requests, analyze user behaviors, and trace the source of attacks. This helps achieve efficient protection of web applications and reduce O&M pressure.

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 in-path mode, transparent bridge mode, mirroring mode, reverse proxy mode, plugin-enabled mode, and multiple route-based out-of-path modes, providing high software- and hardware-based availability.

Figure 1-1 Typical WAF application

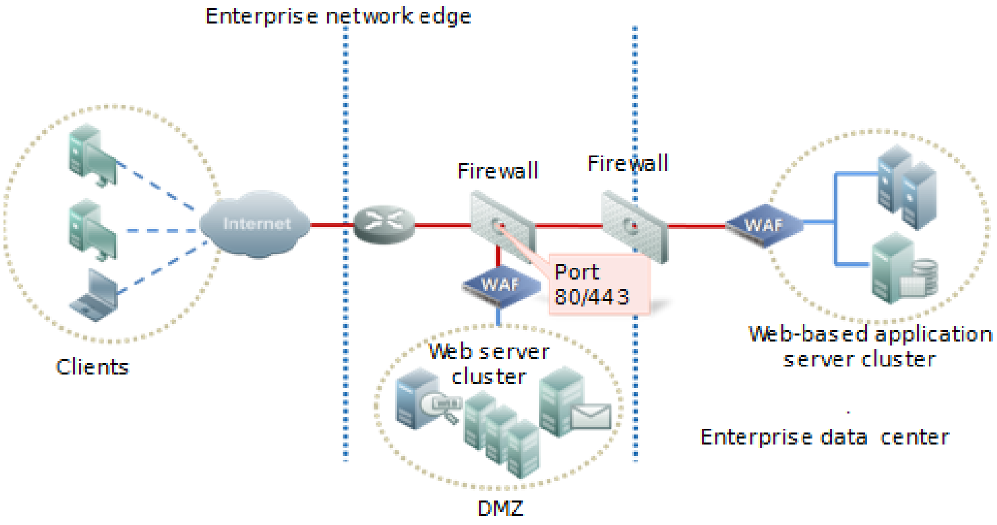


1.3 Typical Deployment

Usually, WAF operates in the DMZ. It is deployed in 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 an intuitive man-machine interaction interface 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

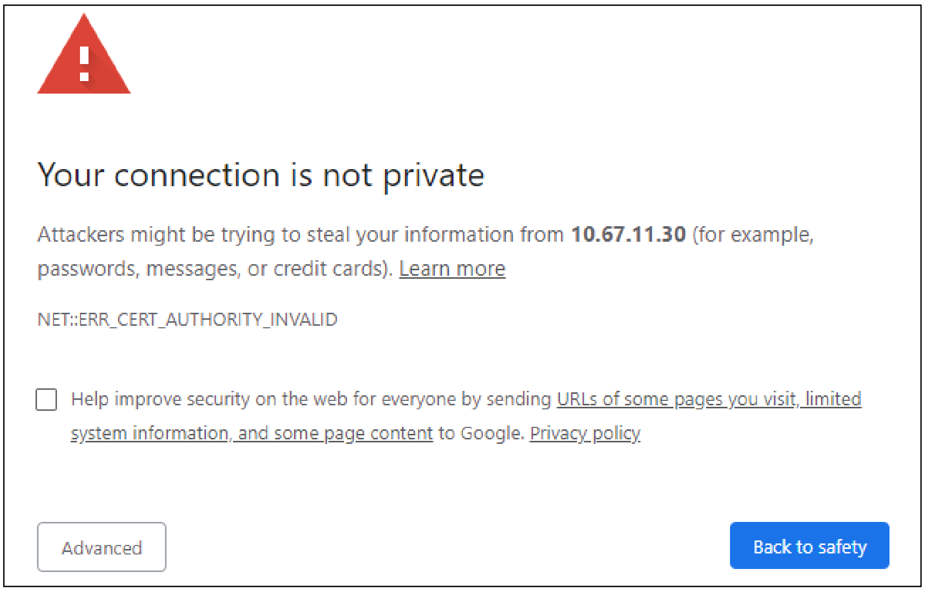
Before login, make sure that the client communicates properly with WAF. Open port 443 if the communication goes through a firewall.

To log in to the web-based manager, perform the following steps. Take Chrome as an example.

Step 1 Open Chrome and access the web-based manager of WAF via HTTPS by typing, for example, **https://192.168.1.1**, in the address bar and pressing **Enter**.

A security alert page appears, as shown in Figure 2-1.

Figure 2-1 Security alert prompt



Your connection is not private

Attackers might be trying to steal your information from **10.67.11.30** (for example, passwords, messages, or credit cards). Learn more

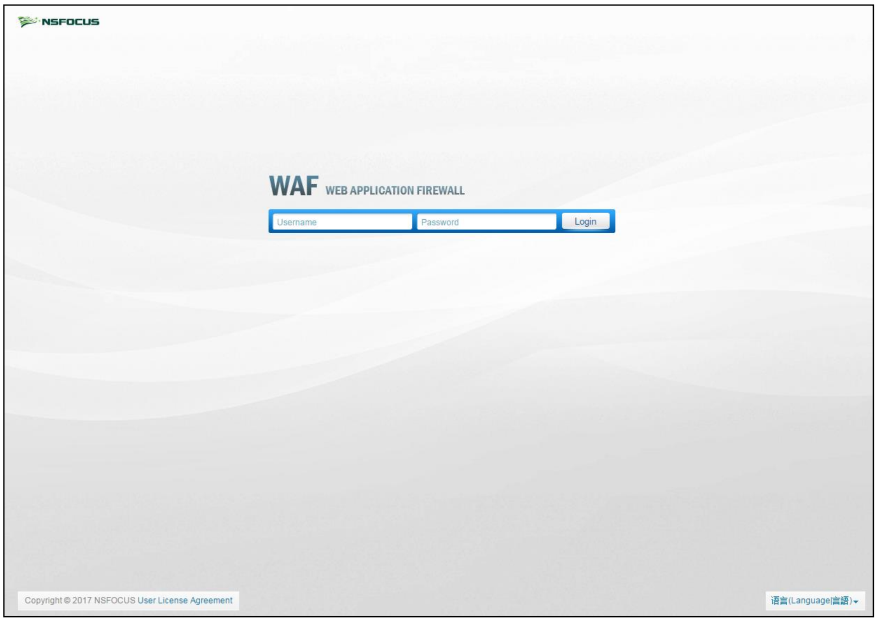
NET::ERR_CERT_AUTHORITY_INVALID

☐ Help improve security on the web for everyone by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

Step 2 Click **Advanced** and then **Proceed to xxxx (unsafe)**.

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



NSFOCUS
WAF WEB APPLICATION FIREWALL
Username
Password
Login
Copyright © 2017 NSFOCUS User License Agreement
语言(Language|言語)

----End

> **Note**
>
> Note the following when logging in to the web-based manager:
>
> - You are advised to use the Internet Explorer 10 or later, Firefox 3.6 or later, or Chrome browser and set the display resolution to 1024 x 768 or higher.
> - Before login, check whether **Turn on Pop-up Blocker** is selected in the browser. If yes, deselect it.
> - The first time that you log in to WAF ', you have to use the default username and password. Then you will be prompted to configure and enter a new password for your WAF account. For details about default accounts, see Default Parameters.
> - Possible causes for login failures are incorrect user name, incorrect password, or upper/lower case confusion of the user name or password.

2.2 System Users

WAF users fall into four 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	Privileges of editing information about the current

User		Privilege
	(created by administrators)	common user account and managing and configuring the web-based manager.

Note

For more details about system users, see 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.

Note

The layout varies with user privileges.

Figure 2-3 Layout of the web-based manager

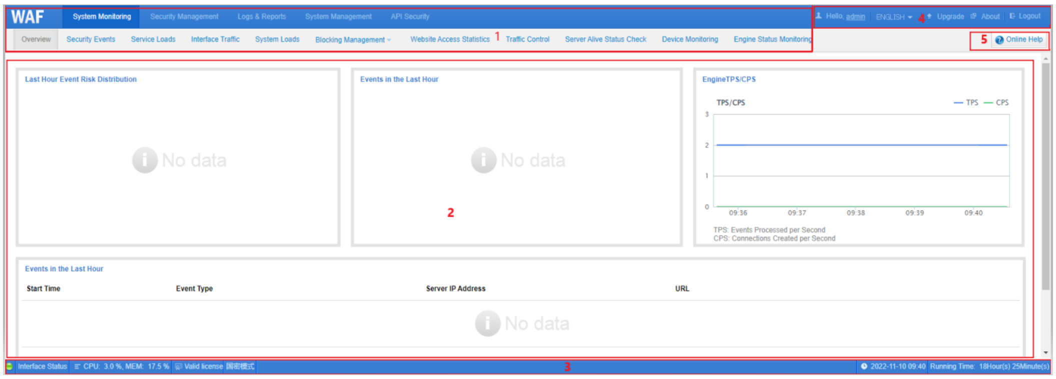


Table 2-2 describes the layout of the web-based manager.

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 System Information.

No.	Area	Description
4	Quick access bar	Area providing several buttons for quick access and operations. • 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

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

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.
Save	Saves a configuration.
Reset	Restores a configuration.

3 System Monitoring

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

This chapter covers the following topics:

Topic	Description
Overview	Describes how to view the risk distribution of last-hour security events, types and numbers of last-hour security events, and engine TPS/CPS.
Security Events	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	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).
Blocking Management	Describes how to view and manage blocked IP addresses, sessions, and UA blocking status.
Website Access Statistics	Describes how to view access statistics of a specified website.
Traffic Control	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.
Engine Status Monitoring	Describes how to view real-time and historical data concerning the engine status, and how to configure custom inspection items.
System Information	Describes how to view system information in the status bar.

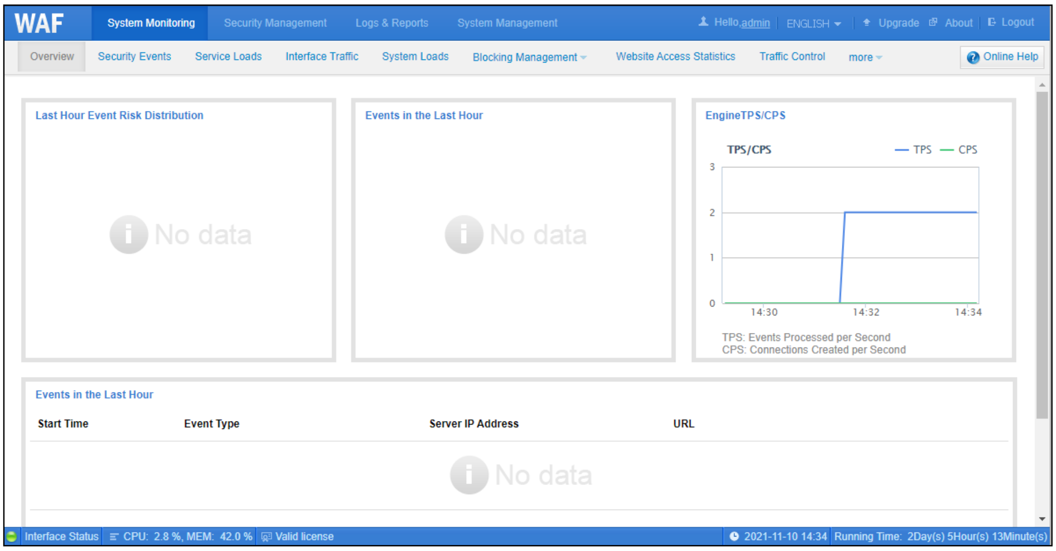
3.1 Overview

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 describes the risk level of various security events.

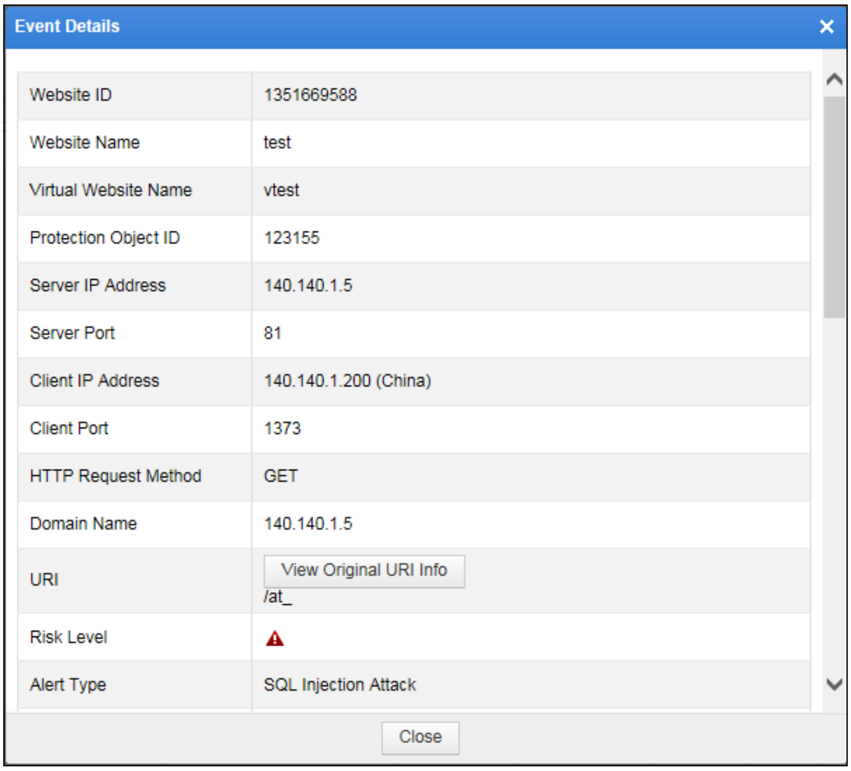
Table 3-1 Risk level of security events

Security Event Type	Risk Level
HTTP violation	Medium
Web server vulnerability attack	Depending on the triggered rule
Web plugin vulnerability attack	Depending on the triggered rule
Secure data transfer	Low
HTTP access control event	Low
Crawler event	Low
XSS attack	Depending on the triggered rule
SQL injection	Depending on the triggered rule
LDAP injection	Depending on the triggered rule

Security Event Type	Risk Level
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
Web shell 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
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 Querying Security Protection Logs.

Figure 3-2 Details of a security event



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	/at_
Risk Level	⚠
Alert Type	SQL Injection Attack

3.2 Security Events

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. After real-time data is generated, you can query it on the **Historical Data** page in about 1–2 minutes.

3.2.1 Viewing Real-Time Data

Choose **System Monitoring** > **Security Events** to view real-time security event data. Similar to the **Overview** page, the **Realtime Data** 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

3.2.2 Querying Historical Data

Choose **System Monitoring** > **Security Events** > **Historical Data** to view historical security event data. You can query a specific range of security events by setting query conditions.

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. After real-time data is generated, you can query it on the **Historical Data** page in about 1–2 minutes.

Website traffic statistics are available only for websites for which the website traffic statistics function is enabled. For details on how to enable website traffic statistics, see Creating a Website Group.

Note

Website traffic statistics are unavailable in transparent bridge mode.

3.3.1 Viewing Real-Time Data

Choose **System Monitoring** > **Service Loads** to view real-time service load data.

The **Realtime Data** 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** to view historical service load data.

The **Historical Data** 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. The statistics are displayed in a trend graph and a table.

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

The **Interface Traffic** page shows real-time and historical data on traffic transmitted and received by each interface on WAF. After real-time data is generated, you can query it on the **Historical Data** page in about 1–2 minutes.

3.4.1 Viewing Real-Time Data

Choose **System Monitoring** > **Interface Traffic** to view real-time interface traffic data.

The **Realtime Data** page shows the received and transmitted traffic (in bps and pps) trends of specified interfaces 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.

3.4.2 Querying Historical Data

Choose **System Monitoring** > **Interface Traffic** > **Historical Data** to view historical interface traffic 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 the traffic (in bps and pps) trend of specified interfaces in a specified period.

- Interface traffic table

  The table lists the maximum and average traffic (in bps and pps) of specified interfaces 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 period	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. After real-time data is generated, you can query it on the **Historical Data** page in about 1–2 minutes.

3.5.1 Viewing Real-Time Data

Choose **System Monitoring** > **System Loads** to view real-time system load 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** to view historical system load data.

The **Historical Data** page shows the CPU or memory usage trend in a specific period.

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 Blocking Management

The blocking management module consists of IP block management, session block management, and UA block management.

3.6.1 IP Block Management

The **IP Block Management** page lists all source IP addresses that are blocked because of triggering related policies. 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.

> **Note**
>
> 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 Block** is set to **Block as customized** or **Permanently block**.
> - The policy is triggered.

Choose **System Monitoring > Blocking Management > IP Management**. Click a website group name in the left pane and all blocked IP block events related to the websites in this group are listed in the right pane.

- Enabling IP block management

  Click **Yes** or **No** for **Enable** to enable or disable IP block management.

> **Note**
>
> If IP block management is not enabled here, the IP block function in policies will not work.

- Unblocking source IP addresses

  In the blocked IP list, select one or more source IP addresses, and click **Unblock IP** to unblock the IP address(es).

- Querying block events by source IP address

  Set the **Source IP Address** parameter to a desired IP address, and click **Query** to view block events of the specified IP address.

3.6.2 Session Block Management

The **Session Block Management** page lists all HTTP sessions blocked because of triggering related policies. Blocked sessions are managed through website groups. Administrators can unblock sessions manually.

> **Note**
>
> Blocked sessions can be managed only after the following conditions are met:
>
> - A website group references a policy, in which **Action** is set to **Block** and **Session Block** is set to **Block as customized** or **Permanently block**.
> - The policy is triggered.

Choose **System Monitoring** > **Blocking Management > Session Management**. Click a website group in the website group tree. Then all session block events related to the websites in this group are listed in the right pane.

- Enabling/Disabling session block management

  Click **Yes** or **No** for **Enable** to enable or disable session block management.

Note	If session block management is not enabled here, the session block function in policies will not work.

- Unblocking sessions

  In the blocked session list, select one or more sessions, and click **Unblock Session** to unblock the session(s).

- Querying block events by session

  Set the **Blocked Session** parameter to a desired session, and click **Query** to view block events of the specified session.

3.6.3 UA Block Management

The **UA Block Management** page lists all UAs (user-agent) blocked because of triggering related policies. Blocked UAs are managed through website groups. Administrators can unblock UAs manually.

Note	Blocked UAs can be managed only after the following conditions are met: • A website group references a policy, in which **Action** is set to **Block** and **UA Block** is set to **Block as customized** or **Permanently block**. • The policy is triggered.

Choose **System Monitoring** > **Blocking Management > UA Management**. Click a website group name in the left pane and all UA block events related to the websites in this group are listed in the right pane.

- Enabling/Disabling UA block management

  Click **Yes** or **No** for **Enable** to enable or disable UA block management.

Note	If UA block management is not enabled here, the UA block function in policies will not work.

- Unblocking UAs

In the blocked session list, select one or more UAs, and click **Unblock UA** to unblock the UA(s).

- Querying block events by UA

  Set the **Blocked UA** parameter to a desired session, and click **Query** to view block events of the specified UA.

3.7 Website Access Statistics

The **Website Access Statistics** module shows the real-time and historical access statistics of a specified website. After real-time data is generated, you can query it on the **Historical Data** page in about 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 Creating a Website Group.

Note

Website access statistics are unavailable in transparent bridge mode.

3.7.1 Viewing Real-Time Data

Choose **System Monitoring** > **Website Access Statistics** to view real-time access statistics.

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** to view historical access statistics.

The **Historical Data** page shows the total access statistics and access trends in a specific period.

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**.
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 periods	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

The traffic control function is unavailable on WAF deployed in plugin-enabled mode. For details, see 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. After real-time data is generated, you can query it on the **Historical Data** page in about 1–2 minutes.

Note	Traffic control is unavailable on WAF deployed in transparent bridge mode or plugin-enabled mode.

3.8.1 Viewing Real-Time Data

Choose **System Monitoring** > **Traffic Control** to view real-time traffic control data.

The **Realtime Data** 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** to view historical traffic control 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. Also, you can add, edit, enable, disable, reset, or delete a server.

Enabling Server Status Check

Choose **System Monitoring** > **Server Alive Status Check**. Click **Enable** or **Disable** to enable the server status check function. After that, you can view real-time server status.

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.

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

Adding a Server

Click **Create** in the upper right half of the server list. In the **Create Server** dialog box, set server parameters and click **OK** to save the settings.

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**.

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

In 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**. Then click the **Inspection Configuration** tab to configure parameters for the server status check function.

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 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

Device monitoring includes the following:

- 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.

Parameter	Description
Critical Threshold	If the usage of a critical partition exceeds the specified critical threshold, WAF 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.

To configure device monitoring, choose **System Monitoring** > **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.

3.11 Engine Status Monitoring

The Engine Status Monitoring module provides real-time and historical delay data of the system engine's threads executing tasks. After real-time data is generated, you can query it on the **Historical Data** page in about 1 minute.

Note	The Engine Status Monitoring module is unavailable on WAF deployed in transparent bridge mode.

3.11.1 Viewing Real-Time Data

Choose **System Monitoring** > **Engine Status Monitoring** > **Realtime Data** to view real-time engine status.

By default, the **Realtime Data** page displays the delay trends of threads 1–4 executing tasks in the last 5 minutes.

3.11.2 Querying Historical Data

The **Historical Data** page displays delay trends of threads executing tasks in a specified period and provides the average and maximum delay values of each thread.

Choose **System Monitoring** > **Engine Status Monitoring** > **Historical Data** to view historical engine status. You can set query conditions (time and threads) to show delay data of the specified threads in the specified period.

3.11.3 Inspection Configuration

Choose **System Monitoring** > **Engine Status Monitoring** > **Inspection Configuration** to configure inspection.

Table 3-10 describes engine status inspection parameters.

Table 3-10 Parameters for engine status inspections

Parameter	Description
Timeout (seconds)	Timeout of the engine. The value range is 0–300 seconds.
Action upon timeout	Controls whether to perform any action when the engine's response time is longer than the timeout value. For the selection of **Yes**, you need to further set **Option** and **Collect core**.
Option	Actions upon timeout include **Restart engine** and **Forward**. For the selection of **Forward**, if you want the engine to resume protection after performing the action upon timeout, choose **System Management** > **System Deployment** > **Running Mode** and select **Protection Mode** for **Mode Configuration**. **Note** The **Forward** action cannot work on WAF in reverse proxy or plugin-enabled deployment mode.
Collect core	Controls whether to collect core file information.

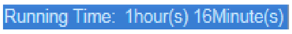
3.12 System Information

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.

Table 3-11 describes details about items in the status bar.

Table 3-11 Status bar information

Item	Description
●	Indicates the engine status. - ●: debugging state - ●: abnormal state - ●: normal state
Interface Status	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**.
CPU: 3.8 %, MEM: 2.7 %	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**.
Valid license	Provides a shortcut for viewing the license status. Clicking **Valid license** displays the **License** page under **System Management** > **License**.
2021-11-12 17:48	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
Overview	Describes the protection idea, system, and procedure of WAF.
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 Information Configuration	Describes how to configure a proxy.
Uploaded File Management	Describes how to manage uploaded files, including 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 provides all-around protection for a website:

- Prevention in advance
  - Web vulnerability scanning: With the built-in scanner, WAF can detect vulnerabilities in websites and fix them before websites are attacked.

  - Smart patching: With 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: With various custom policies, WAF can perform real-time protection on website servers under attack.
  - Auto-learning policy configuration: With custom auto-learning policies, WAF automatically learns about the data and traffic patterns of websites. WAF supports precise whitelist policies. This can offer 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.

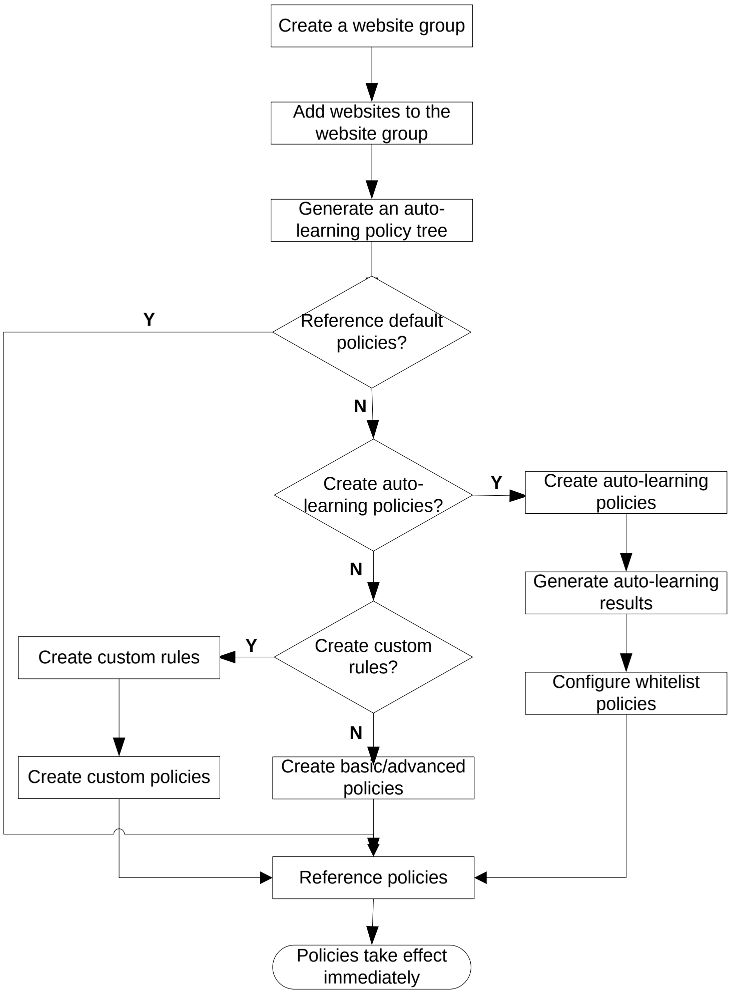
Protection System

Attacks or defacements against websites will bring reputational damage and cause financial losses. WAF, deployed between clients and web servers, effectively blocks or mitigates attacks against servers via multi-layer protection.

Protection Procedure

Generally, servers protected by WAF are referred to 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


Create a website group
Add websites to the website group
Generate an auto-learning policy tree
Reference default policies?
Y
N
Create auto-learning policies?
Y
Create auto-learning policies
Generate auto-learning results
Configure whitelist policies
N
Create custom rules?
Y
Create custom rules
Create custom policies
N
Create basic/advanced policies
Reference policies
Policies take effect immediately

4.2 Network-Layer Protection

This section describes network-layer protection in different deployment modes.

Note	Network-layer protection is unavailable on WAF deployed in mirroring mode.

4.2.1 Network-Layer Protection (in Transparent Bridge Mode)

When WAF is deployed in transparent bridge mode, the following network-layer protection functions are supported:

- ACL protection
- Anti-DDoS protection

4.2.1.1 Configuring ACL Protection

WAF supports data packets filtering based on IP addresses, ports, and protocols.

Choose **Security Management > Network-Layer Protection > ACL Rule** to enable or disable ACL.

Creating an ACL

Step 1 Choose **Security Management** > **Network-Layer Protection** > **Network Object**, and click **Create** to create a network object. Then specify a name and an IP address for the new network object, and click **OK**.

Step 2 Choose **Security Management** > **Network-Layer Protection** > **Service Object**, and click **Create** to create a service object. Then select a protocol, specify a name, a source port, and a destination port, and click **OK**.

Step 3 Choose **Security Management** > **Network-Layer Protection** > **ACL Rule**, and click **Create** to create an ACL. Specify a name, select source and destination address objects and service, and click **Yes** to enable blocking and logging. Then click **OK**.

Table 4-1 Parameters for configuring an ACL rule

Parameter	Description
Name	Specifies the ACL name.
Src Addr Object	Specifies the source address of packets that pass through WAF.
Dst Addr Object	Specifies the destination address of packets that pass through WAF.
Service	Specifies the protocol protection service. The value can be **TCP-All-Ports**, **UDP-All-Ports**, **HTTP**, or others.
Block	Controls whether to block packets.
Log	Controls whether to record a log.

----End

4.2.1.2 Configuring Anti-DDoS Protection

The anti-DDoS 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 anti-DDoS protection, choose **Security Management > Network-Layer Protection > Anti-DDoS**. Then enable SYN flood and ACK flood protection and set the detection thresholds for them respectively. Click **OK**.

Table 4-2 Parameters for configuring an anti-DDoS protection policy

Parameter	Description
SYN Flood	Controls whether to enable SYN flood attack protection.

Parameter	Description
ACK Flood	Controls whether to enable ACK flood attack protection.
Detection Threshold (packets)	Specifies the flood attack threshold in pps. - The default value is **60000** for the SYN flood attack. - The default value is **5** for the ACK flood attack.

4.2.2 Network-Layer Protection (in In-Path, Out-of-Path, Reverse Proxy, Mirroring, or Plugin-enabled 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
- Transparent transmission protection
- Reuse of TCP sequence number of clients

4.2.2.1 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, transparent transmission protection, and reuse of TCP sequence number of clients. Only WAF in in-path mode can provide ARP spoofing protection and reuse of TCP sequence number of clients. 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.

By default, the network-layer access control and TCP flood protection are enabled (✓), and the ARP spoofing protection, ADS collaboration, transparent transmission protection, and reuse of TCP sequence number of clients are disabled (⛔).

- Enabling a policy

  In the policy list, 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, click ■ in the **Operation** column to disable a policy. After a policy is disabled, its status turns to ⛔.

4.2.2.2 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 when WAF is deployed in in-path mode, out-of-path mode, reverse proxy mode, and plugin-enabled mode. However, only the block and accept actions are supported when WAF is deployed in reverse proxy mode and plugin-enabled mode.

Note

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

Choose **Security Management** > **Network-Layer Protection** > **Network-Layer Access Control**. Then click **Create** and set the parameters in the displayed dialog box. Click **OK** to save the settings.

Table 4-3 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/mask and source IP address/mask, for example, 2.2.2.1/255.255.255.0 - 1.1.1.1/255.255.255.0. Both IPv4 and IPv6 addresses are allowed here. You can click ⊕ to add multiple pairs of destination IP address/mask and source IP address/mask. A maximum of 50 entries can be specified for either address type. Note • A maximum of 10 entries can be specified in a text box for each 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/mask text box but multiple entries in the source IP address/mask text box, and vice versa. • If the same address pair exists in more than one policy, it should be handled according to the policy matched first.
Protocol	Specifies the protocol of matching packets. The value can be **ICMP**, **ICMPV6**, **TCP**, **UDP**, or **Unlimited**. **Unlimited** specifies that all protocols are included. If **TCP** or **UDP** is selected, you also need to configure the source port range and destination port range of the target traffic.
Network Interface	Specifies the interface from which WAF receives packets.
Action	Specifies the action on a packet that matches this new policy: • **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.

Parameter	Description
Enable or Not	Controls whether to enable the policy.

Note

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.

Editing a Network-Layer Access Control Policy

You can edit the parameter settings of a network-layer access control policy after it is configured.

In the policy list, click ✎ in the **Operation** column. In the displayed dialog box, edit parameters of the policy and click **OK** to save settings and return to the policy list.

Deleting a Network-Layer Access Control Policy

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

In the policy list, 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

Perform the following step to enable or disable a network-layer access control policy:

- In the policy list, click ▶ in the **Operation** column to enable a policy. After a policy is enabled, the policy status turns to ✓.
- In the policy list, click ■ in the **Operation** column to disable a policy. After a policy is disabled, the policy status turns to ⊖.

4.2.2.3 Configuring TCP Flood Protection

Note

TCP flood protection is available only when WAF works in in-path mode, out-of-path mode, and reverse proxy mode, and is unavailable in plugin-enabled mode or 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 fall 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, choose **Security Management > Network-Layer Protection > TCP Flood Protection**. Then edit TCP flood protection parameters and click **OK** to save the settings. After that, enable this policy on the **Policy Enable-Disable** page.

Table 4-4 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.

4.2.2.4 Configuring ARP Spoofing Protection

Note	Only WAF in in-path mode can provide ARP spoofing protection.

Common Address Resolution Protocol (ARP) attacks are classified 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:

  - The communication between the victim and the real gateway may be broken, and the victim's responses cannot reach the real gateway, causing a denial of service.
  - The victim's response may be sent to the host with the MAC address specified by the attacker. Once the attacker obtains the data, or even worse, alters data and then forwards it to the real gateway, data theft and tampering can be caused.
- False end user/server

- Gateway spoofing

  A false IP-MAC address binding 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 address bindings. When receiving the first ARP packet (query or response) from a server whose IP address is specified in "Proxy Service", WAF will record the IP-MAC binding and take it as the standard IP-MAC address binding of the server.

After the **Auto-Learning MAC Address Table** is established, WAF performs ARP protection based on the standard IP-MAC address bindings 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 address binding in the **MAC Binding Configuration** list.

The following describes how to view auto-learned IP-MAC bindings and create an IP-MAC address binding. The operations of editing, deleting, enabling, and disabling an IP-MAP binding relationship are the same as those for network-layer access control policies.

Viewing the Auto-Learning MAC Address Table

Choose **Security Management > Network-Layer Protection > ARP Spoofing Protection**. The **ARP Spoofing Protection** page appears. You can view auto-learned IP-MAC bindings in the **Auto-Learning MAC Address Table**.

Creating an IP-MAC Address Binding

In the **MAC Binding Configuration** list, click **Create**. Then set parameters in the **Create** dialog box to create an IP-MAC address binding.

Table 4-5 Parameters for creating an IP-MAC address binding

Parameter	Description
Name	Name of the new IP-MAC binding.
IP Address	IP address in the new IP-MAC binding. 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 in the new IP-MAC binding. This parameter can be set only to the MAC address of a proxied server or gateway.
Network Interface	Interface over which WAF detects the new IP-MAC binding. 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.

Note

- After being established, the **Auto-Learning MAC Address Table** cannot be automatically refreshed. You need to add new IP-MAC bindings manually.
- After the system restarts, WAF automatically learns IP-MAC bindings 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.

4.2.2.5 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.

Note

Collaboration with ADS is not supported when WAF is deployed in mirroring mode or plugin-enabled mode.

Usually, WAF protects against TCP flood attacks. 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.

The following WAF-ADS collaboration modes are supported:

- 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 must be performed on both WAF and ADS to implement their collaboration. This section describes the related configurations on WAF.

Note

Before configuring WAF-ADS collaboration, choose **Security Management** > **Network-Layer Protection** > **Policy Enable-Disable** and enable **ADS Collaboration**. For details, see Enabling/Disabling Policies.

To configure WAF-ADS collaboration on WAF, choose **Security Management > Network-Layer Protection > ADS Collaboration Config**. Then configure basic information under **Basic Configuration**.

The running mode can be single-IP diversion, overall-traffic diversion, or hybrid diversion. The configuration parameters vary with the running mode.

Table 4-6 Parameters for configuring WAF-ADS collaboration

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		Specifies how to stop traffic diversion. It has the following values: • **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. Note 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	Threshold for SYN flood traffic. When the number of SYN packets reaches the threshold, WAF instructs ADS to divert the traffic. Note When TCP flood protection is enabled on WAF, this threshold must be greater than that specified in the TCP flood protection policy.
	ACK Flood Notification Threshold	Threshold for ACK flood traffic. When the number of ACK packets reaches the threshold, WAF instructs ADS to divert the traffic. Note When TCP flood protection is enabled on WAF, this threshold must be greater than that specified in the TCP flood protection policy.
	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 for traffic expressed in pps. When the total traffic of the network exceeds the threshold, WAF notifies ADS of the IP

Parameter		Description
	Threshold	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	Specifies the maximum number of allowed queries per traffic diversion. 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 until the maximum number of allowed queries is reached. If there is still no response returned, WAF cancels the diversion for the traffic of the protected IP address.
	Maximum Number of Notification	Specifies the maximum number of allowed notifications. 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, WAF keeps sending such a notification at intervals (specified with **Query Interval**) until the specified maximum number is reached. If there is still no diversion success response, WAF will delete the notification record of this IP address from the notification list.

After that, click **Test** on the page to verify the collaboration status. If the system displays "Connected", the communication link between WAF and ADS is successfully established.

You can also specify IP addresses that allow traffic diversion and those that do not allow traffic diversion as required.

- Specify IP addresses that allow traffic diversion

  Type IP addresses that allow traffic diversion in the text box below **Diversion-Allowed IPs**, 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.

- 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**, 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.

Note

When configuring diversion-allowed or diversion-forbidden IP addresses, note the following:

- If an IP address is specified for both **Diversion-Allowed IPs** and **Diversion-Forbidden IPs**, traffic to this IP address will not be diverted.
- If an IP address is neither specified for **Diversion-Allowed IPs** nor **Diversion-Forbidden IPs**, traffic to this IP address will not be diverted.
- 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.

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, click **Diverted IP Status List** to view IP addresses whose traffic is diverted, their traffic information, and the status of collaboration with ADS.

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.

4.2.2.1 Transparent Transmission Protection

When transparent transmission protection is enabled, ACK packets from the response end that does not establish a connection with the request end are discarded in the traffic of the protected website. When this function is disabled, such ACK packets are forwarded. If there are status detection packets in the network, they are forwarded through the WAN and LAN interfaces.

Transparent transmission protection is available on WAF deployed in in-path mode or out-of-path mode.

Choose **Security Management** > **Network-Layer Protection** > **Policy Enable-Disable**, and click ▶ in the **Operation** column in the policy list to enable **Transparent Transmission Protection**.

4.2.2.2 Reuse of TCP Sequence Number of Client

When functioning as a proxy, WAF proxies TCP sessions and modifies their TCP sequence numbers. If the client's TCP sequence number reuse protection is enabled, the sequence number of the client's TCP session cannot be modified.

The client's TCP sequence number reuse protection is available on WAF deployed in in-path mode.

Choose **Security Management** > **Network-Layer Protection** > **Policy Enable-Disable**, and click ▶ in the **Operation** column in the policy list to enable **Reuse of TCP Sequence Number of Client**.

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**. 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.

4.3.1 Managing Website Groups

On the **Website Group Management** 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
- Quickly Invalidating Policies
- Deleting a Website Group

4.3.1.1 Creating a Website Group

A website group can be created in quick mode. When you configure a website group in quick mode, a set of security solutions containing system-defined policies are generated automatically. After the website group is created, you must add servers to the website group, so that the servers can be protected by the set of security solutions.

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

Step 1 On the **Website Protection** page, 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).

Step 2 In the displayed **Create Website Group** dialog box, click **Next**.

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

The new website group appears on the **Website Group Management** page. At this time, this new website group contains no website, and can be used only after websites and policies are configured.

----End

The parameters for creating a website vary with the deployment mode. For more information, see Adding a Website.

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

Website Group Basic Information

Click a website group in the website group tree, and the **Website Group Management** page is displayed.

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

Website

Click a website group in the website group tree, and the **Website Group Management** page is displayed.

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

Virtual Website

Click a website group in the website group tree, and the **Website Group Management** page is displayed.

- Click **Add Virtual Website** to add a virtual website to the website group.
- Click ✎ in the **Operation** column of the **Virtual Website** section 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 Management** page appears. In the website group list, click ⬆ or ⬇ to move a website group up or down to alter website group priorities.

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.

Use either of the following methods to enable or disable quickly accepting packet function:

- In the website group tree, click **Root**. On the **Website Group Management** page, 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. On the **Website Group Management** page, click **Enable** or **Close** for **Accept** in the **Policy Control** section to enable or disable the quick packet accepting function.

4.3.1.6 Quickly Invalidating Policies

The quick policy invalidation function works for both the website group and virtual websites, covering web security policies (built-in HTTP validation excluded). After this is enabled, traffic to the website group and virtual websites will not be checked against any of the current policies.

In the website group tree, click a website group, and then in the **Policy Control** section in the right pane, click **Enable** or **Close** for **Invalidate** to enable or disable policy invalidation.

4.3.1.7 Deleting a Website Group

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

- In the website group tree, point to a website group and the deleting icon ✖ appears. Click the icon and then click **OK** in the displayed dialog box.
- Click **Root** in the website group tree. On the **Website Group Management** page, select a website, click ⊗ in the **Operation** column, and then click **OK** in the confirmation dialog box.

4.3.2 Website Group Health Check

Choose **Security Management** > **Website Protection** > **Website Group Health Check**, and click **One-Click Check** to scan website groups for compilation errors.

4.3.3 Managing Websites

On the **Website Group Management** page, you can perform the following configuration:

- Adding a Website
- Enabling/Disabling a Website

- Bulk Operations
- Configuring Website Security Policies
- Deleting a Website

4.3.3.1 Adding a Website

WAF in different modes requires different parameters for adding a website.

Adding a Website (in In-Path, Out-of-Path, or Transparent Bridge Mode)

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. On the displayed **Website Group Management** page, click **Add Website** in the upper-right corner of the **Website** section, set parameters, and click **Complete**. To add more websites, click **Add More**.

Table 4-7 describes parameters for adding a website.

Table 4-7 Parameters for adding a website in in-path, out-of-path, or transparent bridge mode

Parameter	Description
Server Name	Website name. The value is at most 50-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. **Note** The **HTTPS** type is unavailable on WAF deployed in transparent bridge mode.
Server IP Address	Specifies the IP addresses of protected servers. The value can be an IP address segment or a single IP address. You can click + to add IP addresses. **Note** • Multiple server IP addresses are supported only in in-path mode and out-of-path mode. • IPv4 and IPv6 addresses are supported. • Once an address segment is matched, WAF will not match its repetitive address segments specified for the same website.
Server Port	Specifies the communication port of the protected server. For an HTTP server, you can enter multiple port numbers, separated by commas. **Note** Full port detection is supported in transparent bridge mode. The value of 0 indicates all ports. For an HTTPS server, you can enter only one port number.
Backend IP	When multiple IP addresses are configured for interfaces, you can specify

Parameter	Description
	the desired IP addresses from the drop-down list as the backend IP. Note This parameter is available on WAF deployed in out-of-path mode or reverse proxy mode.
Enable Web Access Log	Specifies whether WAF records access requests in web access logs. The value can be **Yes** or **No**.
Enable Website Access Statistics	Controls whether to enable website access statistics. The value can be **Yes** or **No**. Note This function is unavailable on WAF deployed in transparent bridge mode.
Enable Website Traffic Statistics	Controls whether to enable website traffic statistics. The value can be **Yes** or **No**. Note This function is unavailable on WAF deployed in transparent bridge mode.
Action upon HTTP Decode Failure	Specifies the action to be performed by WAF after failing to decode a request. By default, **Custom** is selected.
Inspection Item	Specifies what WAF will do and whether it will generate an alert following a request decoding failure. You can set these one by one or in batches. Actions include the following: • **Pass**: WAF will directly forward the request without checking it against any policies. • **Block**: WAF will directly tear down the current connection. • **Accept**: WAF will continue to check the request against other policies. Alert values include the following: • **Yes**: WAF will generate an alert upon a decoding failure. • **No**: WAF will not generate an alert upon a decoding failure.
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: 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. Note This function is unavailable on WAF deployed in transparent bridge mode.

Parameter	Description
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. This parameter is available only when Gzip is enabled. 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.
SSL Protocol	Specifies the SSL protocol. Note This parameter is available only when the following conditions are met: - WAF is deployed in in-path or out-of-path mode. - **Server Type** is set to **HTTPS**. - After login as a **maintainer** user, choose **System Management** > **System Parameter Configuration** > **Other Parameters** to enable the state cryptography mode.
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: - **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 Uploaded File Management. - **Upload Certificate**: Uploads a certificate to WAF. Note This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.
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	- **SSL Version**: specifies one or more SSL protocol versions for the client. Supported SSL versions include SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. - **Cipher Algorithm**: specifies one or more built-in cipher algorithms used for communication between WAF and the client. Note This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.

Parameter	Description
Server	• **SSL Version**: specifies one or more SSL protocol versions for the server. Supported SSL versions include SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • **Cipher Algorithm**: specifies one or more built-in cipher algorithms used for communication between WAF and the server. Note This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.

Adding a Website (in Mirroring Mode)

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. On the displayed **Website Group Management** page, click **Add Website** in the upper-right corner of the **Website** section, set parameters, and click **Complete**. To add more websites, click **Add More**.

Table 4-8 describes parameters for adding a website.

Table 4-8 Parameters for adding a website in mirroring mode

Parameter	Description
Server Name	Website name. The value is at most 50-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.
Server IP Address	Specifies the IP addresses of protected servers. Note • Both IPv4 and IPv6 addresses are supported.
Server Port	Specifies the communication port of the protected server. For an HTTP server, you can enter up to 128 port numbers, separated by commas.
Enable Web Access Log	Specifies whether WAF records access requests in web access logs. The value can be **Yes** or **No**.
Enable Website Access Statistics	Controls whether to enable website access statistics. The value can be **Yes** or **No**.
Action upon HTTP Decode Failure	Specifies the action to be performed by WAF after failing to decode a request. By default, **Custom** is selected.
Inspection Item	Specifies what WAF will do and whether it will generate an alert following a request decoding failure. You can set these one by one or in batches. Actions include the following:

Parameter	Description
	• **Pass**: WAF will directly forward the request without checking it against any policies. • **Accept**: WAF will continue to check the request against other policies. Alert values include the following: • **Yes**: WAF will generate an alert upon a decoding failure. • **No**: WAF will not generate an alert upon a decoding failure.
Certificate File	Specifies the certificate file if **Server Type** is set to **HTTPS**. You can upload a certificate file to WAF.
Client	• **SSL Version**: specifies one or more SSL protocol versions for the client. Supported SSL versions include SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • **Cipher Algorithm**: specifies one or more built-in cipher algorithms used for communication between WAF and the client. Note This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.
Server	• **SSL Version**: specifies one or more SSL protocol versions for the server. Supported SSL versions include SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • **Cipher Algorithm**: specifies one or more built-in cipher algorithms used for communication between WAF and the server. Note This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.

Adding a Website (in Reverse Proxy or Plugin-enabled Mode)

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. On the displayed **Website Group Management** page, click **Add Website** in the upper-right corner of the **Website** section, set parameters, and click **Complete**. To add more websites, click **Continue Creating**.

Table 4-9 describes parameters for adding a website in reverse proxy or plugin-enabled mode.

Table 4-9 Parameters for adding a website in reverse proxy or plugin-enabled mode

Parameter	Description
Server Name	Website name. The value is at most 50-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.

Parameter	Description
	Note The HTTPS website is not supported on WAF deployed in transparent bridge mode.
Proxy Interface	Specifies the interface for proxy access. Only a WAN interface can be selected. For the configuration of working interfaces, see Editing Work Groups in 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 Work Group Management. Both IPv4 and IPv6 addresses are supported. An interface can have a maximum of 253 IP addresses.
Proxy Port	Specifies the communication port of the proxy. For an HTTP or HTTPS server, you can enter only one port.
Backend IP	When multiple IP addresses are configured for interfaces, you can specify the desired IP addresses from the drop-down list as the backend IP. Note This field is unavailable on WAF deployed in plugin-enabled mode.
Enable Web Access Log	Specifies whether WAF records access requests in web access logs. The value can be **Yes** or **No**.
Enable Website Access Statistics	Controls whether to enable website access statistics. The value can be **Yes** or **No**.
Enable Website Traffic Statistics	Controls whether to enable website traffic statistics. The value can be **Yes** or **No**. Note This function is unavailable on WAF deployed in transparent bridge mode.
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: • 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. Note This field is unavailable on WAF deployed in transparent bridge mode.
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. This parameter is available only when Gzip is enabled. By default, WAF supports Gzip compression for the following file types: text,

Parameter	**Description**
	application/x-javascript, application/json, and application/javascript. Also, you can type other file types.
Action upon HTTP Decode Failure	Specifies the action to be performed by WAF after failing to decode a request. By default, **Custom** is selected.
Inspection Item	Specifies what WAF will do and whether it will generate an alert following a request decoding failure. You can set these one by one or in batches. Actions include the following: • **Pass**: WAF will directly forward the request without checking it against any policies. • **Block**: WAF will directly tear down the current connection. • **Accept**: WAF will continue to check the request against other policies. Alert values include the following: • **Yes**: WAF will generate an alert upon a decoding failure. • **No**: WAF will not generate an alert upon a decoding failure.
SSL Protocol	Specifies the SSL protocol. **Note** This parameter is available only when **Server Type** is set to **HTTPS**.
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: • **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 Uploaded File Management. • **Upload Certificate**: uploads a certificate to WAF. **Note** This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.
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	• **SSL Version**: Specifies one or more SSL versions for the client. SSL versions include SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. • **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	• **SSL Version**: specifies one or more SSL versions for the server.

Parameter	Description
	• **Cipher Algorithm**: specifies one or more built-in SSL encryption algorithms that WAF will use for communication with the server. ✎ Note This parameter is an advanced option available only when **Server Type** is set to **HTTPS**.

4.3.3.2 Enabling/Disabling a Website

By default, a website is automatically 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 Management** page.

- Click ▶ in the row of a disabled website to enable a website. After it is enabled, its status turns to ✓.
- Click ■ in the row of an enabled website to disable a website. After it is disabled, its status turns to ⛔.

4.3.3.3 Editing a Website

Click **Root** or a specific website group in the website group tree. On the **Website Group Management** page that appears, click ✎ in the **Operation** column and then edit parameters in the dialog box to edit a website.

4.3.3.4 Deleting a Website

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

4.3.3.5 Bulk Operations

Administrators can perform bulk operations on multiple website groups and websites, including enabling and disabling regional access statistics, enabling and disabling website access statistics, enabling, disabling and deleting websites, enabling and disabling API protection, and so on. Website access statistics refer to access data of all websites other than virtual websites.

To perform bulk operations, click **Root** in the website group tree to open the **Website Group Management** page. Select multiple websites or website groups and click **Bulk Operation**. Then select the desired operation from the drop-down list.

4.3.4 Configuring Website Security Policies

Website security policies vary with the deployment mode of WAF.

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
- Session Blocking

4.3.4.1 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 tailing \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.

Note	WAF does not provide low-and-slow attack protection when deployed in plugin-enabled and transparent bridge modes.

To configure the low-and-slow attack protection policy, choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **Low-and-Slow Attack Protection** tab in the right pane, enable the low-and-slow attack protection policy, and configure parameters.

By default, the low-and-slow attack protection policy is disabled.

Table 4-10 Parameters for configuring the low-and-slow attack protection policy

Parameter	Description
Source IP Block	Controls whether to block the detected source IP addresses of low-and-slow attacks. • **Never**: 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.

4.3.4.2 HTTP Flood Protection Policy

Upon the detection of an HTTP 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.

Note	WAF does not provide HTTP flood protection when deployed in plugin-enabled and transparent bridge modes.

After HTTP flood protection is enabled, you can configure HTTP flood protection. HTTP flood protection configuration includes three parts: global configurations, HTTP flood protection policies, and custom protection policies.

Enabling HTTP Flood Protection

To enable HTTP flood protection, choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **HTTP Flood Protection** tab in the right pane. On the **HTTP Flood Protection** page, click **Enable** in the **Protection Control** section.

By default, **HTTP Flood Protection Status** is **Enabled**. To disable it, click **Close** in the **Protection Control** section.

Setting Global Parameters

Set parameters in the **Global Configuration** section.

Table 4-11 describes parameters for global configuration.

Table 4-11 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**.

Creating an HTTP Flood Protection Policy

Click **Create** in the **HTTP Flood Protection Policy** section, and set parameters.

Table 4-12 describes parameters for creating an HTTP flood protection policy.

Table 4-12 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	Specifies the authentication algorithm used in the new policy. The value can be one of the following: • **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.

Parameter	Description
	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.
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.

Creating a Custom Protection Policy

Click **Create** in the **Custom Protection Policy** section, and set parameters.

Table 4-13 describes parameters for configuring a custom protection policy.

Table 4-13 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.
Domain Name	Domain name of the protected website
Where to Obtain	Specifies the URLs that are not protected by the new policy.
Algorithm	Specifies the authentication algorithm used in the new policy. The value can be one of the following: - **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.

4.3.4.3 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.

Note	WAF does not support secure data transfer when deployed in plugin-enabled and transparent bridge modes.

Creating a Secure Data Transfer Policy

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **Secure Data Transfer** tab, and click **Create** to configure a secure data transfer policy.

Table 4-14 describes parameters for configuring a secure data transfer policy

Table 4-14 Parameters for configuring a secure data transfer policy

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	Specifies WAF's action on requests matching this policy, which can be one of the following: • **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.
Source IP Block	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**. • **Never**: 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.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**.

Parameter	Description
	• **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
Redirection Path	Specifies the redirection URL. This parameter is required if **Action** is set to **Redirection**. • **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. **Note** • 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**.

Other Operations for Secure Data Transfer

On the **Secure Data Transfer** page, 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 Management** page

  Click ↗ in the **Operation** column to return to the **Website Group Management** page.

4.3.4.4 Web Security Protection Policy

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 Policy Management.

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. This saves you from the trouble of selecting child policies from different policy categories one by one. For details about website templates, see Website Template.

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **Web Security Protection** tab in the right pane, click **Select Website Template** in the **Policy Template** section, and select a website template, for example **Frequent, risky event policy template for cyber exercises_rules**.

The website templates are described as follows:

- 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.
- Frequent, risky event policy template for cyber exercises_rules + semantics: enables most of frequent and risky event policies, with a low probability of false positives and good protection effect. It should be used with the semantic engine inspection policy.
- Frequent, risky event policy template for cyber exercises_rules: enables most of frequent and risky event policies, with a low probability of false positives and good protection effect. This template can be used when the semantic engine inspection policy is not enabled.

In this way, **Frequent, risky event policy template for cyber exercises_rules** is selected for all protection policies by default.

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.

Loading Existing Policies

On the **Web Security Protection** page, click the drop-down arrow in the **Protocol Validation** section, select an HTTP validation type, and 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.

Canceling Selected Policies

On the **Web Security Protection** page, click the drop-down arrow of a policy, and select one or more policies. Then click **Cancel Selected Policy** and click **OK** to save the settings.

Creating a Policy

On the **Web Security Protection** page, click the drop-down arrow of a policy, and click **Create Policy** from the drop-down list.

For information on how to create a policy, see Policy Management.

Exporting as Website Templates

At the bottom of the **Web Security Protection** page, click **Export as Website Template**, and click **OK**. Enter the website template name in **Website Template** dialog box and 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 Website Template.

Configuring Smart Patches

Step 1 Click **Smart Patch Configuration** in the **Precise Protection** section. The **Smart Patch Configuration** dialog box appears.

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.

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 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

4.3.4.5 Exception Control Policy

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **Exception Control** tab in the right pane. The **Exception Control** page appears.

Loading Exception Policies

On the **Exception Control** tab page, click the drop-down arrow to the right of **Exception Policy**, and select desired policies from the drop-down list. Click **OK** to complete the configuration.

Canceling Selected Exception Policies

On the **Exception Control** page, click the drop-down arrow to the right of **Exception Policy**, and click **Cancel Selected Exception Policy**. Click **OK** to complete the settings.

Creating Exception Policies

On the **Exception Control** page, click the drop-down arrow, and select **Create Policy** from the drop-down list. The **Create Exception Policy** dialog box appears. For information on how to create exception policies, see Policy Management.

4.3.4.6 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.

Note	WAF does not provide session tracking when deployed in plugin-enabled and transparent bridge modes.

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **Session Trace** tab in the right pane. Click **Yes** to enable the session tracking function and configure session tracking parameters.

By default, the session tracking function is disabled.

Table 4-15 describes parameters for configuring the session tracking policy

Table 4-15 Parameters for configuring the session tracking policy

Parameter	Description
Enable Session Trace	Controls whether to enable or the session tracking function.
Session ID Name	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. WAF supports the following session ID names: • ASP-DOT-NET-session • ASPSESSIONID-session • ColdFusion-session • J2EE-JSESSIONID-Cookie-session • J2EE-JSESSIONID-URL-session • J2EE-session • JWS-ID-session • PHP-BB-MYSQL-session • PHPSESSID-session • PHPSESSIONID-session • SAP-session **Note** You can customize session ID names by modifying the configuration file on the background.
Custom Session ID Name	Specifies custom session ID names. Multiple values must be separated by the semicolon, like PHPSESSID;SAP.
Resources to Trace	Specifies which resources can be tracked. • **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	Specifies file name extensions that are tracked. Multiple file name extensions must be separated by semicolons. This parameter is mandatory when **Resources to Trace** is set to **Only specified resources** or **Specified resources excluded**.
Trace Username	Specifies whether the user name is specified. If you select **Yes**, all logs triggered for individual sessions can be associated with the user name during the user's access period.

Parameter	Description
Login Parameters	Login parameters of the traced user name. • **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.

4.3.4.7 Risk Level Control Policy

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Then click the **Risk Level Control** tab in the right pane. The **Risk Level Control** page appears.

Loading Risk Level Control Policies

On the **Risk Level Control** page, click the drop-down arrow to the right of **Risk Level Policy**. Select one or more policies and click **OK** to save the setting.

Cancelling Selected Risk Level Control Policies

On the **Risk Level Control** page, click the drop-down arrow to the right of **Risk Level Policy**. Select one or more policies and click **Cancel Selected Policy** to deselect risk level control policies that you have selected.

Creating a Risk Level Control Policy

On the **Risk Level Control** page, click the drop-down arrow, and click **Create Policy** to create a risk level control policy. For details, see Risk Level Policy.

4.3.4.8 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.

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Click the **Web Decoding** tab in the right pane. The **Web Decoding** page appears.

Creating a Web Decoding Policy

Click **Create** in the upper right corner. In the **Create Policy** dialog box, configure parameters.

Table 4-16 describes parameters for configuring a web decoding policy.

Table 4-16 Parameters for configuring a web decoding policy

Parameter	Description
Policy Name	Name of the new web decoding policy.
Decoding Mode	Specifies the decoding scheme and level.

Parameter	Description
	You can select a decoding scheme from the drop-down list. You can also click ✚ or ✖ to add or delete decoding levels. The decoding sequence is from left to right and then from top to bottom.
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.

Other Operations

You can also perform the following operations on the **Web Decoding** page:

- 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.

4.3.4.9 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** section.

Manual Analysis

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Click the **False Positive Analysis** tab in the right pane, and configure analysis conditions in the **Manual Analysis** section, and then click **Analyze**. After a dialog box appears prompting successful execution, click **OK** to issue the false positive analysis task.

- 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** section will be directly called for use.

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

Automatic Analysis

Choose **Security Management** > **Website Protection**, click a website group in the website group tree, and click the **False Positive Analysis** tab in the right pane. In the **Auto Analysis** section, set **Enable** to **Yes** and configure analysis conditions:

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

After that, 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.

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.

To configure automatic adjustment, perform the following steps:

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).

Note

- 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

4.3.4.10 False Positive Analysis Result

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

Viewing the False Positive Analysis Result

Choose **Security Management** > **Website Protection**, click a website group in the website group tree, and then click the **False Positive Analysis Result** tab in the right pane. On the displayed **False Positive Analysis Result** page, click 🔍 in the **Operation** column of a result. Then details of the result are displayed.

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

In the **Analysis Result** list, click **Details** in the **Auto Adjust** column. Then details about the adjustment are displayed in a new dialog box.

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.

4.3.4.11 Session Blocking

The web-based manager supports session blocking for each website. You can specify session ID names (cookies) by selecting one or more existing session ID names from the drop-down list or typing custom ones. After session blocking is enabled and cookie-key is configured, if an HTTP session hits the policy, the cookie field of the HTTP header is automatically added to the blocked session list. Upon receipt of a subsequent HTTP request, WAF will obtain the cookie field in the session and match it with the existing blocked sessions one by one. If finding a match, WAF will block the current session. If not, the request is passed for subsequent checks against other policies.

Choose **Security Management** > **Website Protection**, and click a website group in the website group tree. Click the **Session Block** tab in the right pane and configure parameters on the **Session Block Configuration** page.

4.3.5 Managing Virtual Websites

On WAF in other modes, you can do as follows on virtual websites:

- Creating a Virtual Website
- Enabling/Disabling a Virtual Website
- Configuring a Virtual Website
- Editing a Virtual Website
- Bulk Operations

4.3.5.1 Creating a Virtual Website

Choose **Security Management** > **Website Protection**. In the website group tree, point to a desired website group, and click +. In the displayed dialog box, set parameters.

WAF in different modes requires different parameters for adding a virtual website. Table 4-17 describes parameters for creating a virtual website.

Table 4-17 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.

Parameter	Description
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. **Note** This field is unavailable on WAF deployed in plugin-enabled and transparent bridge modes.
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. **Note** This field is available only on WAF deployed in in-path and reverse proxy modes.
Server	Specifies the real server. This parameter is required only in reverse proxy mode. • If you select **IP Address**, you need to enter the IP address and port number of the real 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 real server and click **Gain IP Address** to obtain the IP address of the server. Both IPv4 and IPv6 addresses are supported. **Note** This parameter is required only in reverse proxy mode.
Enable Load Balancing	Controls whether to enable the load balancing function. This parameter is required only in reverse proxy mode. After **Enable Load Balancing** is set to **Yes**, you need to set **IP Address** and **Port**. **Note** This parameter is required only in reverse proxy mode.
Advanced Options	If the website group contains websites with HTTPS servers, you can configure advanced options for the virtual website: • **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. **Note** This parameter is unavailable in transparent bridge mode.

4.3.5.2 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 Management** 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 ⊖.

4.3.5.3 Configuring a Virtual Website

In the website group tree, click a virtual website. The **Virtual Website** page appears. Set parameters in the dialog boxes, and then click **Save** to save the settings.

Note that the **Virtual Website** page in different modes may have different parameters.

4.3.5.4 Configuring Virtual Website Policies

Click **Policy Configuration**, and 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 group 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.

Creating Policies

On the **Policy Configuration** page, click the **Create Policy** link. The dialog box for creating a policy of this type appears. For how to create policies, see Policy Management.

Exporting as Virtual Website Templates

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 Virtual Website Template.

4.3.5.5 Editing a Virtual Website

Click **Root** or a specific website group in the website group tree. On the **Website Group Management** page that appears, click ✎ in the **Operation** column of the Virtual Website table and then edit parameters in the dialog box to edit a virtual website.

4.3.5.6 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 Management** page that appears, click ⊗ in the **Operation** column and then click **OK** in the confirmation dialog box to delete a virtual website.

4.3.5.7 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 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

Note

WAF does not support auto-learning policies when deployed in plugin-enabled mode and transparent bridge mode.

4.4.1 Creating an Auto-Learning Policy

Choose **Security Management > Auto-Learning Policies**, and click a website group in the auto-learning policy tree. On the **Auto-Learning Policies** page, click **Create**. Alternatively, point to a website group in the auto-learning policy tree, and click +. Then set parameters in the displayed dialog box. Click **OK** to save the settings.

4.4.2 Editing an Auto-Learning Policy

Click a website group in the auto-learning policy tree. On the **Auto-Learning Policies** page, click ✎ in the **Operation** column in the **Website Auto-Learning Policy Information** section. Alternatively, click an auto-learning policy in the auto-learning policy tree. Then Set parameters in this dialog box. Click **OK** to save the settings.

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

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, 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 ⊖.

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, 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, 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 **Auto-Learning Policies** page, you can do as follows:

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

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

  The **Website Group Management** page appears.
- Switching to the **View Learning Result** Page

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

  The **View Learning Result** page appears.

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

4.5 Auto-Learning Results

Choose **Security Management** > **Auto-Learning Results**. The **Auto-Learning Results** page appears. In the website group tree, select a website to view auto-learning results. The icon ☰ indicates the auto-learning results of the website.

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 built-in protection rules are used to defend against known vulnerabilities. Users can only query them, but cannot edit them.

Choose **Security Management** > **Rule Database Management** > **Common Protection** > **Web Server Vulnerability**. The **Web Server Vulnerability** page appears. Then specify parameters and click **Query**. Then click 🔍 to query details of a rule.

Table 4-18 describes parameters for querying a rule.

Table 4-18 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.

4.6.2 Configuring Custom Rules

As many web applications are customized, built-in protection rules are insufficient to cover all web applications. WAF supports custom protection rules. You can customize rules and make them take effect by referencing them in policies.

Alert types of the custom rules can be predefined ones (such as **Web Server Vulnerability** and **Web Plug-in Vulnerability**) and **Custom**. Note that a custom rule can be referenced only by a custom policy no matter whether the alert type is set to **Custom** or not.

4.6.2.1 Creating Custom Rules

Choose **Security Management** > **Rule Database Management** > **Custom Rules** > **Custom**. Click **Create** to the upper right of the custom rule list. Then set the parameters and click **OK** to save the settings.

4.6.2.2 Editing Custom Rules

You can edit the parameter settings of a custom rule after it is configured.

On the **Custom** page, click ✎ in the **Operation** column of a rule and edit it. Then click **OK** to save settings and return to the **Custom** page.

4.6.2.3 Deleting Custom Rules

You can delete custom rules one by one.

In the custom rule list of the **Custom** page, 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: includes HTTP validation policies.
- Basic protection: includes common protection policies in ordinary network environment.
- Advanced protection: includes protection policies specific to network environment.
- Precise protection: includes protection policies applied through smart patches and based on auto-learning results.
- Others: includes custom policies, exception policies, and risk level policies that are defined according to 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 Policyin section 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.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

4.7.1 HTTP Validation Policies

Hypertext Transfer Protocol (HTTP) 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

Choose **Security Management** > **Policy Management**. The **HTTP Validation** page appears. Click **Create**. In the displayed dialog box, set the parameters.

Table 4-19 describes parameters for creating an HTTP validation policy.

Table 4-19 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. Note This parameter is unavailable on WAF deployed in mirroring mode.
Inspection Item	Specifies items to be checked, such as abnormal headers, abnormal parameters, abnormal encodings, and abnormal upload. • 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. • 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. Note WAF deployed in mirroring mode does not support the blocking action.

Parameter	Description
	And both the **Block or Not** option and the **Block for all** option are unavailable.
HTTP Decoding Control	Controls whether WAF removes percent signs (%) or null characters in HTTP decoding. **Note** This parameter is unavailable on WAF deployed in mirroring mode.

Editing an HTTP Validation Policy

You can edit an HTTP validation policy after it is configured.

In the HTTP validation policy list of the **HTTP Validation** page, click ✎ in the **Operation** column of an HTTP validation policy. Then edit parameters of the HTTP validation policy, click **OK** to save settings, and return to the **HTTP Validation** page.

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.

On the **HTTP Validation** page, click ⧉ in the **Operation** column to modify parameters. For details, see Table 4-19.

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, 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/Plugin Protection Policy
- HTTP Access Control Policy
- Crawler Protection Policy
- Common Web Protection Policy
- Illegal Upload Restriction Policy
- Illegal Download Restriction Policy (unavailable in plugin-enabled mode)
- Information Disclosure Protection Policy (unavailable in transparent bridge mode, mirroring mode, and plugin-enabled mode)

4.7.2.1 Web Server/Plugin Protection Policy

"Web server/plugin" 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/plugin protection mainly detects and defends against illegal requests and responses. WAF's web server/plugin 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/plugin protection policies. The following describes how to create a web server/plugin protection policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a web server/plugin protection policy, choose **Security Management** > **Policy Management** > **Basic Protection** > **Web Server/Plug-in Protection**. Click **Create** and set the parameters. Click **OK** to save the settings.

Table 4-20 describes parameters for creating a web server/plugin protection policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-20 Parameters for creating a web server/plugin 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: • **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 Block**, **Session Block**, and **UA Block**. • **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. **Note** Actions cannot be configured when WAF is deployed in mirroring mode.
Source IP Block	Specifies whether and how to block the source IP address of packets that match

Parameter	Description
	this new policy. This parameter is mandatory when **Action** is set to **Block**. • **Never**: 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, which can be set to a value in seconds, minutes, or hours. Note This parameter is unavailable when WAF is deployed in mirroring mode.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination. Note This parameter is unavailable when WAF is deployed in mirroring mode.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination. Note This parameter is unavailable when WAF is deployed in mirroring mode.
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. • **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**

Parameter	Description
	Vulnerability), just select the check box of the rule. At least one rule should be selected.

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.

On the **HTTP Access Control** page, you can create, edit, delete, and duplicate HTTP access control policies. The following describes how to create an HTTP access control policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create an HTTP access control policy, choose **Security Management > Policy Management > Basic Protection > HTTP Access Control**. Click **Create** and then set the parameters. Click **OK** to save the settings.

Table 4-21 describes parameters for creating HTTP access control policies.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-21 Parameters for creating HTTP access control policies

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: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match

Parameter	Description
	this new policy. This parameter is mandatory when **Action** is set to **Block**. • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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.

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 describes how to create a crawler protection policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a crawler protection policy, choose **Security Management > Policy Management > Basic Protection > Crawler Protection**. Click **Create** and then set the parameters. Click **OK** to save the settings.

Table 4-22 describes parameters for creating a crawler protection policy.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-22 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	Specifies the action WAF will take on a matched request. Actions include the following: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.

Parameter	Description
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. - **Never**: WAF does not block the UA. - **Permanently block**: WAF permanently blocks the UA. - **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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. - **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. By default, all rules are listed. After you filter rules, only rules that meet filtering conditions are displayed. 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.

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 that will 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 describes how to create a common web protection policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a common web protection policy, choose **Security Management > Policy Management > Basic Protection > Common Web Protection**. Then click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-23 describes parameters for creating a common web protection policy.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-23 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: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the

Parameter	Description
	specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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. The value can be: • **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. By default, all rules are listed. After you filter rules, only rules that meet filtering conditions are displayed. 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.

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 describes how to create an illegal upload restriction policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create an illegal upload restriction policy, choose **Security Management > Policy Management > Basic Protection > Illegal Upload Restriction**, and click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-24 describes parameters for creating an illegal upload restriction policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-24 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	Specifies the action WAF will take on a matched request. Actions include the following: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be:

Parameter	Description
	- **Never**: WAF does not block the UA. - **Permanently block**: WAF permanently blocks the UA. - **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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.

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 describes how to create an illegal file download restriction policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create an illegal file download restriction policy, choose **Security Management > Policy Management > Basic Protection > Illegal Download Restriction**, and Click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-25 describes parameters for creating an illegal download restriction policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-25 Parameters for creating an illegal download restriction policy

Parameter	Description
Name	Name of the new policy.

Parameter	Description
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: • **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 Block** and **Session Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
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**. 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.
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.

Parameter	Description
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.

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.

On the **Information Disclosure** page, you can create, edit, delete, and duplicate information disclosure protection policies. The following describes how to create an information disclosure protection policy. The editing, deleting, and duplicating operations are similar to those on information disclosure protection policies. For details, see HTTP Validation Policies.

To create an information disclosure protection policy, choose Security Management > Policy Management > **Basic Protection > Information Disclosure Protection**. Then click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-26 describes parameters for creating an information disclosure protection policy, and Table 4-27 describes common status codes.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-26 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.

Parameter	Description
Action	Specifies the action WAF will take on a matched request. Actions include the following: - **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. - **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 the rule. For descriptions about status codes, see Table 4-27.
Redirection Path/Response Replacement Content	Redirection path or response replacement content. - 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 4-27 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

Status Code	Description
	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)	The resource has not been modified since last requested. The server does not return resource content. If the resource has not been modified since last requested, set the server to respond this code (called the If-Modified-Since header).
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.
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.

Status Code	Description
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.
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.

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
- Semantic Engine Inspection
- Dynamic Protection

Note

WAF deployed in plugin-enabled mode does not support cookie security, content filtering, sensitive information filtering, and dynamic protection.

WAF deployed in transparent bridge mode and mirroring mode does not support cookie security, dynamic protection, CSRF protection, or sensitive information filtering.

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 describes how to create a leech protection policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a leech protection policy, choose **Security Management** > **Policy Management** > **Advanced Protection** > **Leech Protection**. Then click **Create**. In the dialog box, set the parameters and click **OK** to save the settings.

Table 4-28 describes parameters for creating a leech protection policy.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-28 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: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**.

Parameter	Description
	- **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. - **Never**: WAF does not block the session ID (cookie). - **Permanently block**: WAF permanently blocks the session ID. - **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. - **Never**: WAF does not block the UA. - **Permanently block**: WAF permanently blocks the UA. - **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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	Policy inspection mode, which can be either of the following: - **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. Note **Referer+Cookie Inspection** does not work on WAF in plugin-enabled mode and mirroring mode.
Trusted Websites	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. The value is URLs starting with **http://** or **https://**. The wildcard * is

Parameter	Description
	supported, but this does not indicate that any URL parameters are allowed. For example, the format is **http://*.example.com**. 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.

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 describes how to create a CSRF protection policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a CSRF protection policy, choose **Security Management > Policy Management > Advanced Protection > CSRF Protection**. Then click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-29 describes parameters for creating a CSRF protection policy.

Table 4-29 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: • **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 Block**, **Session Block**, and **UA Block**.

Parameter	Description
	- **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: - **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: - **Never**: WAF does not block the session ID (cookie). - **Permanently block**: WAF permanently blocks the session ID. - **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: - **Never**: WAF does not block the UA. - **Permanently block**: WAF permanently blocks the UA. - **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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	Controls whether to enable web 2.0 protection. 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.

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 describes how to create a scanning protection policy. The editing, deleting, and duplicating operations are similar to those in HTTP validation policies. For details, see HTTP Validation Policies.

To create a scanning protection policy, choose **Security Management > Policy Management > Advanced Protection > Scanning Protection**. Then click **Create**. In the displayed dialog box, set the parameters and click **OK** to save the settings.

Table 4-30 describes parameters for creating a scanning protection policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-30 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 the following: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The

Parameter	Description
	value can be: - **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: - **Never**: WAF does not block the session ID (cookie). - **Permanently block**: WAF permanently blocks the session ID. - **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: - **Never**: WAF does not block the UA. - **Permanently block**: WAF permanently blocks the UA. - **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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 Amount Measurement	Controls whether to count HTTP requests in a given measurement period.
Request Amount Measurement	- **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. Note

Parameter	Description
	At least one of **Request Discrete Rate** and **Maximum Request Amount** should be specified. If only **Maximum Request Amount** is specified, **Request Discrete Rate** is 0 by default.
Response Distribution Measurement	• **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. Note 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. • **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	• **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.

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 describes how to create a cookie security policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a cookie security policy, choose **Security Management** > **Policy Management** > **Advanced Protection** > **Cookie Security**. The click **Create**. In the displayed dialog box, set the parameters. Click **OK** to save the settings.

Table 4-31 describes parameters for creating a cookie security policy.

Table 4-31 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	Specifies the action WAF will take on a matched request. Actions include the following: • **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 Block**, **Session Block**, and **UA Block**. • **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. • **Clear**: Upon detection of illegal cookies, WAF removes them and then sends data to servers, instead of blocking the HTTP sessions.
Source IP Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the

Parameter	Description
	specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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	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: • 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.

4.7.3.5 Content Filtering Policy

On the **Content Filtering** page, you can create, edit, delete, and duplicate content filtering policies. The following describes how to create a content filtering policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a content filtering policy, choose **Security Management** > **Policy Management** > **Advanced Protection** > **Content Filtering**. Click **Create**. In the displayed dialog box, set the parameters. Click **OK** to save the settings.

Table 4-32 describes parameters for creating a content filtering policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-32 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: • **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. • **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. The value can be: • **Stop upon a match**: WAF stops matching the packet against other rules in the policy.

Parameter	Description
	- **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.

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 a sensitive information filtering policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a sensitive information policy, choose **Security Management** > **Policy Management** > **Advanced Protection** > **Sensitive Information Filtering**. Click **Create** in the lower-right corner. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-33 describes parameters for creating a sensitive information filtering policy.

Table 4-33 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: - **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	This parameter has the following values:

Parameter	Description.
Principle	• **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.

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.

On the **Brute Force Filtering** page, you can create, edit, delete, and duplicate brute force filtering policies. The following describes how to create a brute force filtering policy. The editing, deleting, and duplicating operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

Note	Only HTTP traffic detection instead of HTTPS traffic detection is supported in a brute force protection policy on WAF deployed in mirroring mode.

To create a brute force protection policy, choose **Security Management > Policy Management > Advanced Protection > Brute Force Protection**. Click **Create** in the upper-right corner. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-34 describes parameters for creating a brute force protection policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-34 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.
	Action	Specifies the action that WAF will take on a matched request. Actions include the following: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. • **Never**: 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, which can be set to a value in seconds, minutes, or hours.

Parameter		Description
	Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
	UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
	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	Specifies the method by which the server verifies login requests from clients. Options include **Form**, **Ajax**, and **Jsonp**. This parameter is required when **Action** is set to **Verification Code**.
	Login Referer	Specifies the referer URL carried in the request submitted. This parameter is required when **Action** is set to **Verification Code**.

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 are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create an XML attack protection policy, choose **Security Management > Policy Management > Advanced Protection > XML Attack Protection**. Click **Create** in the upper-right corner. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-35 describes parameters for creating an XML attack protection policy.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-35 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: • **Pass**: WAF directly forwards such request to the server without any more security checks.

Parameter		Description
		- **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 Block**, **Session Block**, and **UA Block**. - **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**. For the latter, you can select an existing response file or upload a response file.
	Source IP Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. - **Never**: 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, which can be set to a value in seconds, minutes, or hours.
	Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. - **Never**: WAF does not block the session ID (cookie). - **Permanently block**: WAF permanently blocks the session ID. - **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
	UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. - **Never**: WAF does not block the UA. - **Permanently block**: WAF permanently blocks the UA. - **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in

Parameter			Description
			seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
	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 Processing Directives	Controls whether to forbid XML documents to contain processing directives. By default, this option 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

Parameter			Description
			parameters, you can select or upload only one schema file. Different groups must use different schema files. For how to manage XSD files, see 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: • 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 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.

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 are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a smart engine inspection policy, choose **Security Management > Policy Management > Advanced Protection > Smart Engine Inspection**. Then click **Create** in the upper-right corner of the page. Configure parameters in the dialog box and click **OK** to save the settings.

Table 4-36 describes parameters for configuring a smart engine inspection policy.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-36 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: • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period

Parameter	Description
	expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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**.

4.7.3.10 Semantic Engine Inspection

Semantic engine policies can be configured for semantic analysis only after the **admin** user enables the semantic engine policy function.

The semantic engine detects attacks in a finer-grained manner based on lexical and semantic analysis of target strings. Despite the linear time complexity, the engine manages to be as approximate as possible to the target language and uses signature-based scoring or policy-based determination algorithms to judge whether some input is part of an attack.

On the **Semantic Engine Inspection** page, you can create, edit, duplicate, and delete semantic engine inspection policies. The following describes how to create a semantic engine inspection policy. Other operations are similar to those on HTTP validation policies. For details, see HTTP Validation Policies.

To create a semantic engine inspection policy, choose **Security Management > Policy Management > Advanced Protection > Semantic Engine Inspection**. Then click **Create** in the upper-right corner of the page. Configure parameters in the dialog box and click **OK** to save the settings.

Table 4-37 describes parameters for configuring a semantic engine inspection policy.

Note

When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-37 Parameters for configuring a semantic engine inspection policy

Parameter	Description
Name	Name of the semantic engine inspection policy.
Description	Brief description of the semantic engine inspection policy.

Parameter	Description
Alert or Not	Controls whether to generate alert messages. Options include **Yes** and **No**.
Action	Specifies the action that WAF will take on a matched request. Actions include the following: • **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 Block**, **Session Block**, and **UA Block**. • **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**. For the latter, you can select an existing response file or upload a response file.
Source IP Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
Inspection Item	The semantic engine can decode URLs, JSON data, Base64 strings, and Unicode, convert hexadecimal characters, parse PHP serialized objects, remove leading and trailing spaces, and unescape slashes. The semantic engine can detect SQL injection, command line injection, PHP code injection, Java code injection, PHP deserialization, and Java deserialization provided that such protections are enabled. After enabling a protection type, you need to further configure the alert threshold and inspection items (URI, parameters, HTTP headers,

Parameter	Description
	and cookie).

4.7.3.11 Dynamic Protection

Dynamic protection can identify automated attacks in various business scenarios, such as crawlers, promotion abuse, and vulnerability scan. It can accurately identify and block bot traffic, effectively reducing website vulnerability exposure and business congestion and helping businesses improve O&M efficiency.

WAF supports script running environment inspection and browser environment inspection.

Note

After login using a **maintainer** account, choose **System Management** > **System Parameter Configuration** > **Other Parameters** to enable the dynamic protection policy function.

Dynamic protection is unavailable on WAF deployed in plugin-enabled mode, mirroring mode, and transparent bridge mode.

Choose **Security Management** > **Policy Management** > **Advanced Protection** > **Dynamic Protection**, and then click **Create** to configure a dynamic protection policy.

Table 4-38 describes parameters for configuring dynamic protection.

Table 4-38 Parameters for configuring a dynamic protection policy

Parameter	Subitem	Description
Name	/	Name of the policy.
Description	/	Brief description of the dynamic protection policy.
Alert or Not	/	Controls whether an alert is generated when the dynamic protection policy is triggered.
Action	/	Specifies the action WAF will take on a matched request. Actions include the following: • **Pass**: WAF directly forwards such request to the server without any more security checks. • **Block**: WAF directly closes the current connection request and ends the policy detection. • **Accept**: WAF ends the check against the current policy but will still check such request against other policies. • **Redirection**: WAF constructs a 302 redirect page to respond to the client and tears down the current TCP connection. After selecting this action, you also need to specify the redirection path. • **Disguise**: WAF responds to the client with a customized HTTP/HTTPS response code and response file contents, and tears down the current TCP connection. If this action is specified, you also need to set the response code and response file. You can use the existing response file or upload a response file.

Parameter	Subitem	Description
Source IP Blocking	/	Specifies whether to block the source IP address of HTTP/HTTPS requests that match this policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: - **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 a specified period, which can be set to a value in seconds, minutes, or hours.
Session Block	/	Specifies whether to block the session of HTTP/HTTPS requests that match the policy. This parameter is mandatory only when **Action** is set to **Block**. The value can be: - **Unblock**: WAF does not block the session ID (cookie) of HTTP/HTTPS requests that match the policy. - **Permanently block**: WAF permanently blocks the session ID. - **Block as customized**: WAF blocks the session ID in the specified period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP/HTTPS requests are allowed to reach the destination.
UA Block	/	Specifies whether to block the User-Agent (UA) of HTTP requests that match the policy. This parameter is mandatory only when **Action** is set to **Block**. The value can be: - **Unblock**: WAF does not block the UA of HTTP requests. - **Permanently block**: WAF blocks the UA. - **Block as customized**: WAF blocks the UA in the specified period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
Inspection Item	Bot Recognition	Determines whether the request client is a bot. After bot recognition is enabled, set the following parameters: - **Max Pass Times**: indicates the maximum allowed requests without containing bot recognition marks. - **Strict Mode**: indicates that any requests that do not contain bot recognition marks will be blocked in this mode. Note that this mode will result in a high false positive rate in blocking. - **Browser Environment Inspection**: selects environment attributes that are not inspected.
	Token Authentication	WAF validates tokens to prevent replay attacks. After token authentication is enabled, set the following parameters: - **Max POST Pass Times**: indicates the maximum pass times of POST requests that do not contain tokens. - **Verify URL**: verifies whether the token of one request is reused by another request. - **Strict Mode**: indicates that any requests that do not contain tokens will trigger the policy in this mode.

Parameter	Subitem	Description
	Script Configuration	Specifies the JS request path. If not specified, /ng_dynamic_defend is used by default.
	Submitted Data Obfuscation	Encrypts the submitted data to prevent man-in-the-middle attacks and protect against privacy data disclosure. By default, data obfuscation is disabled. After it is enabled, add the full URL and specify the data submission method of the protected object. A maximum of 10 pieces of data can be obfuscated at one time.
	Web Page Element Obfuscation	HTML elements are dynamically processed to hide contents from crawlers, thus stopping the crawling of web pages. By default, page element obfuscation is disabled. After it is enabled, specify an obfuscated object. It can be a tag, Form, or Javascript.
	Allowlist Configuration	Configures the allowlist for requests. Any requests that match the allowlist will be directly accepted and continue to match the next protection policy. The allowlist takes effect only in the current policy. There are two types of allowlists: • Domain allowlist: indicates the allowlist that contains domain name entries or IP address entries, separated by line breaks. A domain allowlist has no more than 10 entries. • URI-path allowlist: indicates the allowlist that contains URI path entries, separated by line breaks. A URI-path allowlist has no more than 10 entries. URIs in regular expression are supported.

4.7.4 Precise Protection Policy

WAF features allowlist 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 **Allowlist** page, you can create, edit, delete, and duplicate allowlist policies. The following only describes how to create allowlist policies. The editing, deleting, and duplicating operations for whitelist policies are the same as those for HTTP validation policies. For details, see HTTP Validation Policies.

Note	WAF does not support allowlist precise protection when deployed in plugin-enabled mode, mirroring mode, or transparent bridge mode.

To create an allowlist policy, choose **Security Management** > **Policy Management** > **Precise Protection** > **Allowlist**. Click **Create**. In the dialog box, set the parameters. Click **Submit** to save the settings.

Table 4-39 Parameters for creating an allowlist 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: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
Redirection Path	Redirection URL. This parameter needs to be set only when **Action** is set to **Redirection**.
Optional Learning	Auto-learning objects that can be selected. Optional learning result objects are

Parameter	Description
Result Object	URLs for whom the auto learning process is completed 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.

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 HTTP Validation Policies.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

To create an exception policy, choose **Security Management** > **Policy Management** > **Others** > **Exception Policy**. Click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

You can configure exception policies for multiple policies at the same time.

Note	You can create and edit exception policies on the **Website Protection** page. For details, see Exception Control Policy in Configuring Website Security Policies.

Table 4-40 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.

Parameter	Description
Policy Instance	Target policy instance.
Rule	Target rule instance. Note - 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: 1. If no rule is selected, WAF also adds the selected policy instance to the new risk level policy. 2. If a rule is selected, WAF adds only this rule to the new rule level policy.
Exception Source IPs	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). Leaving it empty means that the new policy applies to all IP addresses.
Exception URLs	Specifies URLs to which the new policy applies. 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. Examples: - www.example1.com:8080/login.jsp - $www\.example2\.com:80/.* Leaving it empty means that the new policy applies to all URLs.

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 HTTP Validation Policies.

To create a custom policy, choose **Security Management** > **Policy Management** > **Others** > **Custom Policy**. Click **Create**. In the dialog box, set the parameters. Click **OK** to save the settings.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-41 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: • **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 Block**, **Session Block**, and **UA Block**. • **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 Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. The value can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. The value can be: • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
Redirection Path	Redirection URL. This parameter is required if **Action** is set to **Redirection**.
Matching Principle	Controls whether WAF continues to match a packet that has matched a rule in a policy against other rules in the policy. The value can be:

Parameter	Description
	- **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.

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 HTTP Validation Policies.

To create a risk level policy, choose **Security Management** > **Policy Management** > **Others** > **Risk Level Policy**. Click **Create** in the upper-right corner. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-42 Parameters for creating a risk level policy

Parameter	Description
Name	Name of the new policy.
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	Specifies the type, instance, and rules of the new policy. You can click ⊕ to create more policies or click ⊗ to delete policies. - **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.

Parameter	Description
	Note • 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: 1. If no rule is selected, WAF also adds the selected policy instance to the new risk level policy. 2. If a rule is selected, WAF adds only this rule to the new rule level policy.
Source IP	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). Leaving it empty means that the new policy applies to all IP addresses.
URL	Specifies URLs to which this new policy applies. 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. Examples: www.example1.com:8080/login.jsp, $www.example2.com:80/.* Leaving it empty indicates that the policy applies to all URLs.

4.7.5.4 API Compliance Policy

The API compliance policy is used to verify and manage API requests to ensure API compliance. The API compliance policy verifies the following contents:

- Content of the request direction
- Request parameter name
- Request parameter type
- Request method

Choose **Security Management** > **Policy Management** > **Others** > **API Compliance Policy**, click **Create** to configure an API compliance policy.

Table 4-43 describes parameters for configuring an API compliance policy.

Note	When WAF is deployed in mirroring mode, no actions including various blocking functionalities can be configured in a protection policy.

Table 4-43 Parameters for configuring an API compliance policy

Parameter	Description
Name	API compliance policy name.

Parameter	Description
Description	Brief description of the API compliance policy.
Alert or Not	Controls whether an alert is generated when the API compliance policy is triggered.
Action	Specifies the action WAF will take on a matched request. Actions include the following: • **Pass**: WAF directly forwards the request to the server without further security checks. • **Block**: WAF directly blocks the request and ends the security check against the policy. • **Accept**: WAF accepts the request but will check it against other policies. • **Redirect**: 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 a customized HTTP response code and a response file and tears down the current TCP connection.
Source IP Blocking	Specifies whether to block the source IP address of HTTP request packets that match the policy. This parameter is mandatory when **Action** is set to **Block.** The value can be: • **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 a specified period, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether to block the session of HTTP requests that match the policy. This parameter is mandatory only when **Action** is set to **Block**. The value can be: • **Unblock**: WAF does not block the session ID (cookie) of HTTP/HTTPS requests that match the policy. • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the specified period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether to block the UA of HTTP/HTTPS requests that match the policy. This parameter is mandatory only when **Action** is set to **Block**. The value can be: • **Unblock**: WAF does not block the UA of HTTP requests. • **Permanently block**: WAF blocks the UA. • **Block as customized**: WAF blocks the UA in the specified period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
OAS File	Selects an OAS file for compliance verification.

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.
- Frequent, risky event policy template for cyber exercises_rules + semantics: enables most of frequent and risky event policies, with a low probability of false positives and good protection effect. It should be used with the semantic engine inspection policy.
- Frequent, risky event policy template for cyber exercises_rules: enables most of frequent and risky event policies, with a low probability of false positives and good protection effect. This template can be used when the semantic engine inspection policy is not enabled.

Templates can be divided into website templates and virtual website templates.

4.8.1 Website Template

You can create, edit, delete, view, and download website templates.

4.8.1.1 Creating a Website Template

Choose **Security Management > Template Management**. The **Website Template** page appears. Click **Create** in the lower-right corner of the **Website Template** page. In the dialog box, set the parameters. Click **OK** to commit the configuration.

Table 4-44 describes parameters for creating a website template.

Table 4-44 Parameters for creating a website template

Parameter	Description.
Name	Name of the website template.
Description.	Brief description of the website template.
Selecting Policy	Specifies policies for website protection. You can select a policy from the drop-down list. Note • 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.

4.8.1.2 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 Configuring Website Security Policies.

On the **Website Template** page, 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.
- Downloading templates: You can click to download a template to a local disk drive. Only the website templates created by the administrator can be downloaded.

4.8.2 Virtual Website Template

You can create, edit, delete, view, and download website templates. However, WAF deployed in plugin-enabled mode does not support template configuration for virtual websites.

4.8.2.1 Creating a Virtual Website Template

To create a virtual website template, choose **Security Management > Template Management > Virtual Website Template**. Click **Create** in the lower-right corner of the **Website Management** page. In the dialog box, set the parameters and click **OK** to complete the settings.

Table 4-45 Parameters for creating a virtual website template

Parameter	**Description.**
Name	Name of the new template.
Description.	Brief description of the new template.
Selecting Policy	Specifies policies for protection. You can select a policy from the drop-down list. **Note** • 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.

4.8.2.2 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 Configuring a Virtual Website.

On the **Virtual Website Template** page, you can also perform the following operations:

- Viewing templates: Click 🔍 to display template details. Template details are available only for built-in virtual website templates.
- Editing templates: Click ✎ to edit a virtual website template. Only the virtual website templates created by the administrator can be edited.
- Deleting templates: Click ✖ to delete a virtual website template. Only the website virtual templates created by the administrator can be deleted.
- Downloading templates: Click ⬇ to download a template to a local disk drive. Only the website templates created by the administrator can be downloaded.

4.9 Smart Patching

Note

Only users who have purchased the smart patch module can use this function.

Smart patching is unavailable on WAF deployed in transparent bridge mode or mirroring mode.

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 4-2, 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 4-2 Deployment topology — smart patching function via cloud-based scanning

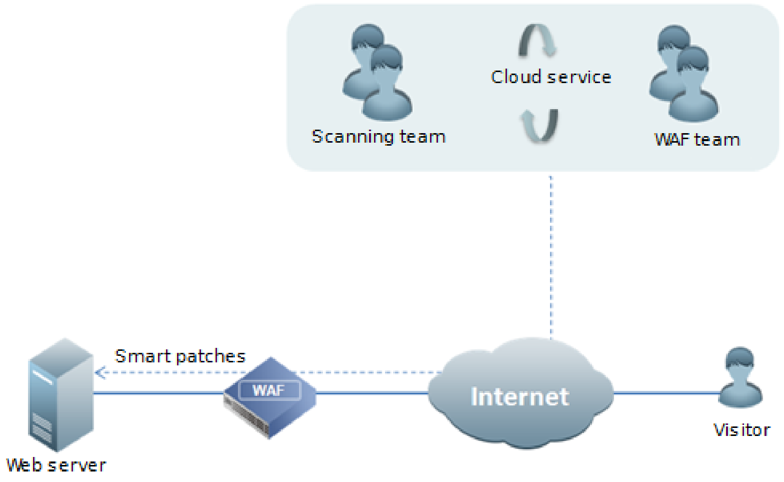
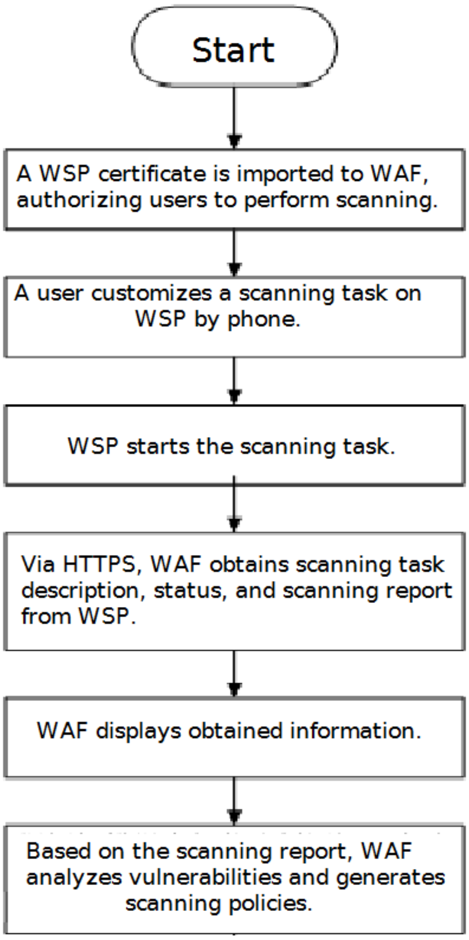


Figure 4-3 shows the procedure of smart patching via cloud-based scanning.

Figure 4-3 Procedure of smart patching via cloud-based scanning



A WSP certificate is imported to WAF, authorizing users to perform scanning.

A user customizes a scanning task on WSP by phone.

WSP starts the scanning task.

Via HTTPS, WAF obtains scanning task description, status, and scanning report from WSP.

WAF displays obtained information.

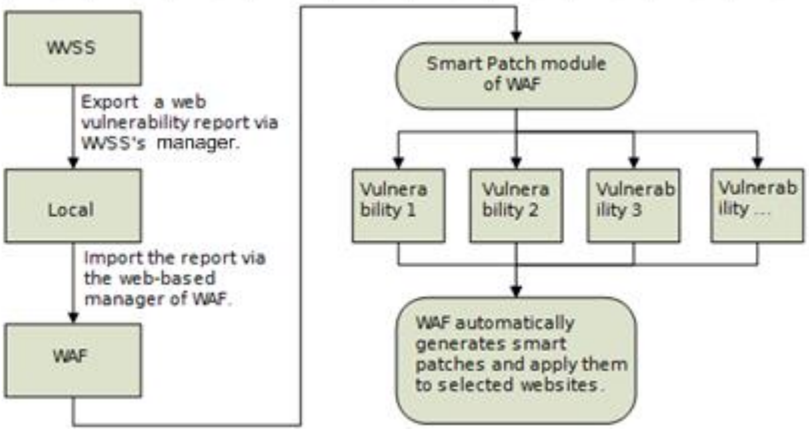
Based on the scanning report, WAF analyzes vulnerabilities and generates scanning policies.

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 4-4 shows the procedure of the smart patching function via imported vulnerability scanning report.

Figure 4-4 Procedure of the smart patching function via imported vulnerability scanning report


WVSS
Export a web vulnerability report via WVSS's manager.
Local
Import the report via the web-based manager of WAF.
WAF
Smart Patch module of WAF
Vulnerability 1
Vulnerability 2
Vulnerability 3
Vulnerability ...
WAF automatically generates smart patches and apply them to selected websites.

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**.

b. Set the parameters.

Table 4-46 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**.
Penetration Scanning IP	IP address of penetration scanning. WAF does not perform protection against penetration scanning. Penetration scanning penetrates WAF to detect web

Parameter	Description
	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**.

b. Click **Add**.

c. Type a domain name for cloud-based scanning and an IP address for receiving scanning reports.

Note	**Domain Name** must be set to **waf.api.nsfocus.net**, and **IP Address** must be set to **211.99.227.132**.

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.

----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.

Configuring Collaboration with WVSS Device

Choose **Security Management** > **Smart Patch** > **WVSS Scan Config**. On the **WVSS Scan Config** page, set WVSS device parameters. Then click **Connect** to connect WAF to WVSS.

Table 4-47 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.

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

Click **Create** to the upper right of the task list. In the dialog box, set the parameters. Click **OK** to save the settings and dispatch the task.

Table 4-48 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

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. To switch to the page for managing web vulnerability scanning reports (WVSS reports), click **WVSS** in the upper-left corner of the page.

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:

On the **Scanning File Management** page, click **Related Scanning File**. Then click **View**.

Click 🔍 in the **View** column to view details of a vulnerability.

Generating Patches

Click **Generate Patch** in the lower-right corner of the **SaaS Scanning File** dialog box. 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.

Tip	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. You are advised to regenerate smart patches a moment later.

If WAF successfully generates smart patches based on detected web vulnerabilities, the **Smart Patch Configuration** page appears.

Applying Patches

On the **Smart Patch Configuration** page, 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.

Note

- 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. 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 Configuring Website Security Policies.

Deleting Cloud-based Scanning Reports

In the **Related Scanning File** dialog box, 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

You can import, view, and download WVSS scanning reports, and delete imported reports. Based on vulnerabilities in the reports, you can generate and apply smart patches.

Tip

You can click **File Size** or **Upload Time** to rank WVSS scanning files by file size or upload time.

Importing a Report

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. On the page, click **Browse**, select a desired WVSS scanning report, and click **Import**.

The imported scanning report is displayed in the **WVSS Scanning File Management** list.

Viewing Report Details

On the **WVSS Scanning File Management** list, click 🔍 in the **Operation** column. Click 🔍 in the **View** column to view its details.

Generating Patches

On the displayed **WVSS Scanning File** page, 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?" Click **OK** to generate patches.

> **Note**
>
> 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. You are advised to regenerate smart patches a moment later.

After patches are generated for the report, ↳ appears in the **Operation** column in the **WVSS Scanning File Management** list. 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.

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. A patch application dialog box appears.

> **Note**
>
> - 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. 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 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 Select desired smart patches, and click **Apply to Website**.

Step 3 In the **Apply to Website** dialog box, 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.

Tip

- Smart patches that are not selected 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 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. You are advised to reapply smart patches a moment later.

----End

Downloading a Report

On the **WVSS Scanning File Management** list, 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

On the **WVSS Scanning File Management** list, 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.

To switch to the page for managing patches generated for imported web vulnerability scanning reports, click **WVSS**.

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, click 🔍 in the **Operation** column of a patch package on the **Patch Management** page. Then contents of the patch package are displayed. Click 🔍 in the **Operation** column of the item to view details.

Note

- 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 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.

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 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

Secure delivery 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

Note

Secure delivery is unavailable on WAF deployed in plugin-enabled mode, transparent bridge mode, and mirroring mode.

4.10.1 Viewing Page Caches

To view page caches, choose **Security Management** > **Secure Delivery** > **Page Cache**. Click a cache in the cache tree in the left pane. The URL update information of the cache is displayed. 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.

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 4-49 describes common MIME types.

Table 4-49 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, choose **Security Management** > **Secure Delivery** > **Cache File Types**. On the displayed page, click **Create**. In the **Create MIME Type** dialog box, set the parameters. Click **OK** to save the settings.

Table 4-50 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.

Editing a Custom MIME Type

You can edit a custom MIME type after it is configured.

To edit a custom MIME type, click ✎ in the **Operation** column in the MIME type list. In the displayed 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.

Deleting a Custom MIME Type

You can delete MIME types one by one.

In the MIME type list, 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** > **Secure Delivery** > **Cache File Types** > **Built-in MIME Types** to view built-in MIME types.

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, choose **Security Management** > **Secure Delivery** > **Anti-Defacement Configuration**. Click **Edit**. In the dialog box, set the parameters. Click **OK** to save the settings.

Table 4-51 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.

Parameter	Description
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 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**.

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, choose **Security Management > Secure Delivery > Anti-Defacement Configuration > URL Exception List**. Click **Create**. In the dialog box, set the parameters and then click **OK** to save the settings.

Tip	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/**.

Editing a URL Exception

You can edit an excluded URL after it is configured.

In the URL exception list, click 📝 in the **Operation** column and edit parameters in the dialog box. After that, click **OK** to save the settings.

Deleting Excluded URLs

In the URL exception list, 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, 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, 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 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** > **Secure Delivery** > **Page Prefetch Management**.

Enabling/Disabling Page Prefetch Management

WAF can prefetch web page contents only after this function is enabled.

- On the **Page Prefetch Management** page, select **Enable Page Prefetch Management** to enable the page prefetch management function.
- On the **Page Prefetch Management** page, 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.

On the **Page Prefetch Management** page, click the **Update Cycle (second)** text box and change the value. Click **OK** to save the settings.

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.

On the **Page Prefetch Management** page, click **Create** to the lower right of the **Prefetch Task List**. In the dialog box, set the parameters to create a page prefetch task.

Table 4-52 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.

Editing a Page Prefetch Task

You can edit a page prefetch task after it is configured.

In the **Prefetch Task List**, click ✎ in the **Operation** column. 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.

Deleting a Page Prefetch Task

You can delete page prefetch tasks one by one.

In the **Prefetch Task List**, click ✖ in the **Operation** column and click **OK** in the confirmation dialog box, to delete a page prefetch task.

Enabling/Disabling a Page Prefetch Task

In the **Prefetch Task List**, click ▶ in the **Operation** column to enable a page prefetch task. After it is enabled, its status turns to ✓.

In the **Prefetch Task List**, 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.

Note	Before clearing the cache, you must disable the page prefetch management function.

To clear the cache of WAF, choose **Security Management** > **Secure Delivery** > **Clear Cache**. Click **Clear Cache** and then click **OK** in the confirmation dialog box.

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** > **Secure Delivery** > **Server Offline Takeover** to configure server offline takeover.

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.

Note

WAF does not support proxy information configuration when deployed in plugin-enabled mode.

If the source IP proxy is not enabled in reverse proxy mode, the client IP address seen by the server is actually the interface IP address of WAF. To obtain the real client IP address, you must configure the proxy information to enable the X-Forwarded-For feature.

To configure proxy information, choose **Security Management > Proxy Information Configuration**. Then set proxy parameters and click **OK** to save the settings.

Table 4-53 Proxy parameters

Parameter	Description
Proxy Mode	Proxy mode. WAF supports the following proxy modes: • **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

Parameter	Description
	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	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. 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. **Note** • 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.
Proxy Field Index in Headers	Specifies a proxy field to be selected as the real source IP address. When multiple proxy fields exist in a header in a top-down manner, WAF will select the specified one as the real source IP address. By default, WAF selects the first proxy field.
IP Field Index	Specifies an IP address to be selected as the real source IP address. By default, WAF selects the first one. • If no IP address is added as a trusted one, the addresses are indexed from left to right and WAF will select the specified one as the real source IP address. When no IP address of the specified index is found, WAF will use the network-layer IP address as the source IP address. The last IP address refers to the rightmost one. • If trusted IP addresses are configured, the addresses are indexed from right to left and WAF will select the specified one as the source IP address. When trusted IP addresses do exist, but no IP address of the specifies index is found, WAF will use the leftmost IP address as the source IP address. When no trusted IP address exists, WAF deems the current proxy field untrusted and continues to check the next proxy field for trusted IP addresses. If no desired IP address is found ultimately, it will use the network-layer IP address as the source IP address. The last IP address refers to the leftmost one.
Max Proxy Depth	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. The value range is 0–10. The value **0** indicates that WAF will not check the header depth of proxy information.
Server Trusted IP	IPv4 and/or IPv6 addresses trusted by the server. 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.

4.12 Uploaded File Management

This section involves SSL certificate management, XSD/WSDL file management, disguised response file management, GmSSL certificate management, and IP access control.

4.12.1 SSL Certificate Management

To create an HTTPS website, an SSL certificate must be uploaded. You can upload, view, or delete the SSL certificate.

Note	SSL certificate management is unavailable on WAF deployed in transparent bridge mode.

4.12.1.1 Importing an SSL Certificate

To import an SSL certificate, choose **Security Management** > **Uploaded File Management** > **SSL Certificate Management**. Then click **Import** on the page. Click **Choose File**, select the desired SSL certificate, and then click **OK**.

You can also view or delete SSL certificates.

4.12.1.2 Viewing an SSL Certificate

Click 🔍 in the **Operation** column of the certificate list to view 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

Choose **Security Management** > **Uploaded File Management** > **XSD/WSDL File Management**. Click **Upload** in the upper-right corner of the page, and browse to an XSD or WSDL file in a local disk drive. Then click **OK** to upload the file.

Note	Pay attention to the following when uploading an XSD or WSDL file: • 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.

4.12.2.2 Downloading a File

Choose **Security Management** > **Uploaded File Management** > **XSD/WSDL File Management**. On the displayed page, 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.

Note	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 Management** page. You can upload or delete files on this page.

Note

WAF does not support disguised response file management when deployed in plugin-enabled mode and transparent bridge mode.

4.12.3.1 Uploading a Disguised Response File

Choose **Security Management > Uploaded File Management > Disguised Response File Management**. On the displayed page, click **Upload** to open the file upload dialog box. Browse to a disguised response file in the GIF or HTML format and click **OK** to upload this file.

Note

A disguised response file in the GIF format to upload cannot exceed 20 KB.

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.

4.12.4 IP Access Control

The IP Access Control module allows you to create or import a blacklist to effectively prevent malicious attacks or deny access from a certain IP address.

Note

IP access control is unavailable when WAF is deployed in transparent bridge mode.

4.12.4.1 Creating an IP Blacklist

To create a blacklist, choose **Security Management > Uploaded File Management > IP Access Control**. In the **IP Access Control Blacklist** list, click **New Blacklist**. Type the file name and an IP address to be added to the blacklist and click **OK**.

To add more IP addresses, click ➕ in the **Operation** column.

4.12.4.2 Importing a File

On the **IP Access Control Blacklist** page, click **Import File**, select a local blacklist, and click **OK**. In the blacklist file, multiple IP addresses must be separated by the comma.

4.12.4.3 Editing an IP Blacklist

On the IP blacklist file list, click ✎ in the **Operation** column of a file and then you can edit this file. WAF allows you to add or delete IP addresses. Multiple IP addresses must be separated by the comma, like 178.1.1.1,179.1.1.1.

4.12.4.4 Other Operations

On the **IP Access Control Blacklist** page, you can perform the following operations:

- Query an IP address.

  Type an IP address in the text box and click **Query** to check whether it is included in any blacklist file.
- Download an IP blacklist file.

  Click ⬇ in the **Operation** column of a blacklist file to download it to a local disk drive.
- Preview an IP blacklist file.

  Click 🔍 in the **Operation** column of a blacklist file to view IP addresses in the file.
- Delete an IP blacklist file.

  Click ✖ in the **Operation** column of a blacklist file and click **OK** in the confirmation dialog box that appears to delete this file.

4.12.5 GmSSL Certificate Management

When a new HTTPS website is created, the GmSSL certificate must be uploaded or selected if the SSL protocol is set to **GmSSL**. The **admin** user can import and delete the state cryptography SSL certificate on the **GmSSL Certificate Management** page.

Note	GmSSL certificate management is unavailable when WAF is deployed in transparent bridge mode.

4.12.5.1 Importing an GmSSL Certificate

Choose **Security Management** > **Uploaded File Management** > **GmSSL Certificate Management**, and click **Import**. In the **Import GmSSL Certificate** dialog box, click **Choose File** to select the state cryptography SSL certificate and click **OK**.

Deleting a GmSSL Certificate

Choose **Security Management** > **Uploaded File Management** > **GmSSL Certificate Management**, select a specified certificate in the table, and click ⊗ to delete the certificate. Or select multiple certificates and click **Bulk Delete** to delete them.

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 Configuring Website Security Policies.

4.13.1 IP Reputation Overview

To implement IP reputation protection, WAF connects to the NSFOCUS reputation cloud to obtain IP reputation data. Then WAF checks these IP addresses, thus providing more convenient and accurate IP protection services.

Note

IP reputation is not supported on WAF deployed in plugin-enabled or transparent bridge mode.

When WAF is deployed in mirroring mode, common IP reputation protection is unavailable while advanced IP reputation protection is available.

To view the IP reputation overview, choose **Security Management > IP Reputation > IP Reputation Overview**. On the **IP Reputation Overview** page, view IP reputation information.

Table 4-54 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: • DDoS attack • Vulnerability • Spam • Web attack • Scan source • Botnet client
Reputation Match Count in the Last One Week	Indicates the numbers of attacks triggering common protection and advanced protection for IP reputation in the past 7 days.

4.13.2 IP Reputation Configuration

WAF supports IP reputation protection, including common protection and advanced protection.

4.13.2.1 Reputation Cloud Connectivity Test

On the **IP Reputation Configuration** page, the last synchronization time is displayed.

To test the reputation cloud connectivity, choose **Security Management > IP Reputation > IP Reputation Configuration**, and click **Test**.

If WAF properly connects to the NSFOCUS reputation cloud, a dialog box indicating the connection success appears. Then click **OK** to complete the connectivity test.

4.13.2.2 Common Protection

Common protection indicates the application of IP reputation protection at the network layer.

On the **IP Reputation Configuration** page, you can click **Enable** or **Disable** in the **Common Protection** section 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 database, 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:

On the **IP Reputation Configuration** page, click **Create** in the **Advanced Protection** section. In the dialog box, set parameters and click **OK** to save the settings.

Table 4-55 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. Option can be: • **Pass**: WAF directly forwards the matching packet without any more security detection. • **Block**: WAF blocks matching packets and tears down the current TCP connection. After selecting this action, you need to further set **Source IP Block**, **Session Block**, and **UA Block**. • **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.

Parameter	**Description**
Source IP Block	Specifies whether and how to block the source IP address of packets that match this new policy. This parameter is mandatory when **Action** is set to **Block**. Option can be: • **Never**: 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, which can be set to a value in seconds, minutes, or hours.
Session Block	Specifies whether and how to block the session ID of HTTP requests that match this policy. This parameter is required when **Action** is set to **Block**. Option can be: • **Never**: WAF does not block the session ID (cookie). • **Permanently block**: WAF permanently blocks the session ID. • **Block as customized**: WAF blocks the session ID in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the session ID is deleted from the blocked session list and related HTTP requests are allowed to reach the destination.
UA Block	Specifies whether and how to block the UA of HTTP sessions that match this policy. This parameter is required when **Action** is set to **Block**. Option can be: • **Never**: WAF does not block the UA. • **Permanently block**: WAF permanently blocks the UA. • **Block as customized**: WAF blocks the UA in the customized period, which can be set to a value in seconds, minutes, or hours. When the specified period expires, the UA is deleted from the blocked UA list and related HTTP requests are allowed to reach the destination.
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.

5 Reports

This chapter 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**.

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 Website Protection. If you select no website, but select the **Global policies** check box, an alert report on events triggering network-layer access control policies will be generated.
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.

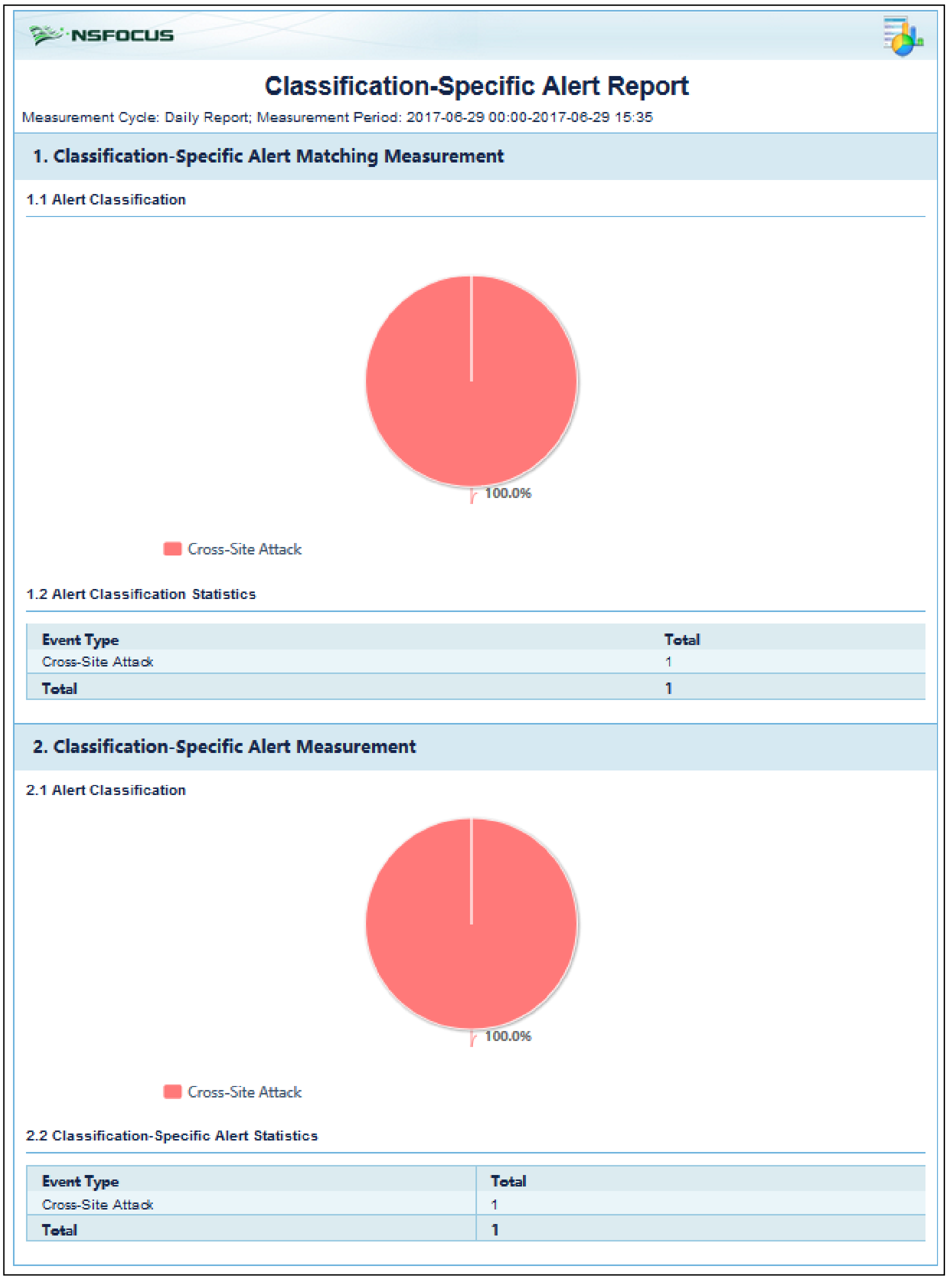
Step 3 Click **Generate**.

You can view statistics about web security events of the specified websites within the statistic collection period.

Figure 5-1 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 5-1 Classification-specific alert report



Classification-Specific Alert Report

Measurement Cycle: Daily Report; Measurement Period: 2017-06-29 00:00-2017-06-29 15:35

1. Classification-Specific Alert Matching Measurement

1.1 Alert Classification

1.2 Alert Classification Statistics

Event Type	Total
Cross-Site Attack	1
Total	**1**

2. Classification-Specific Alert Measurement

2.1 Alert Classification

2.2 Classification-Specific Alert Statistics

Event Type	Total
Cross-Site Attack	1
Total	**1**

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**.

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

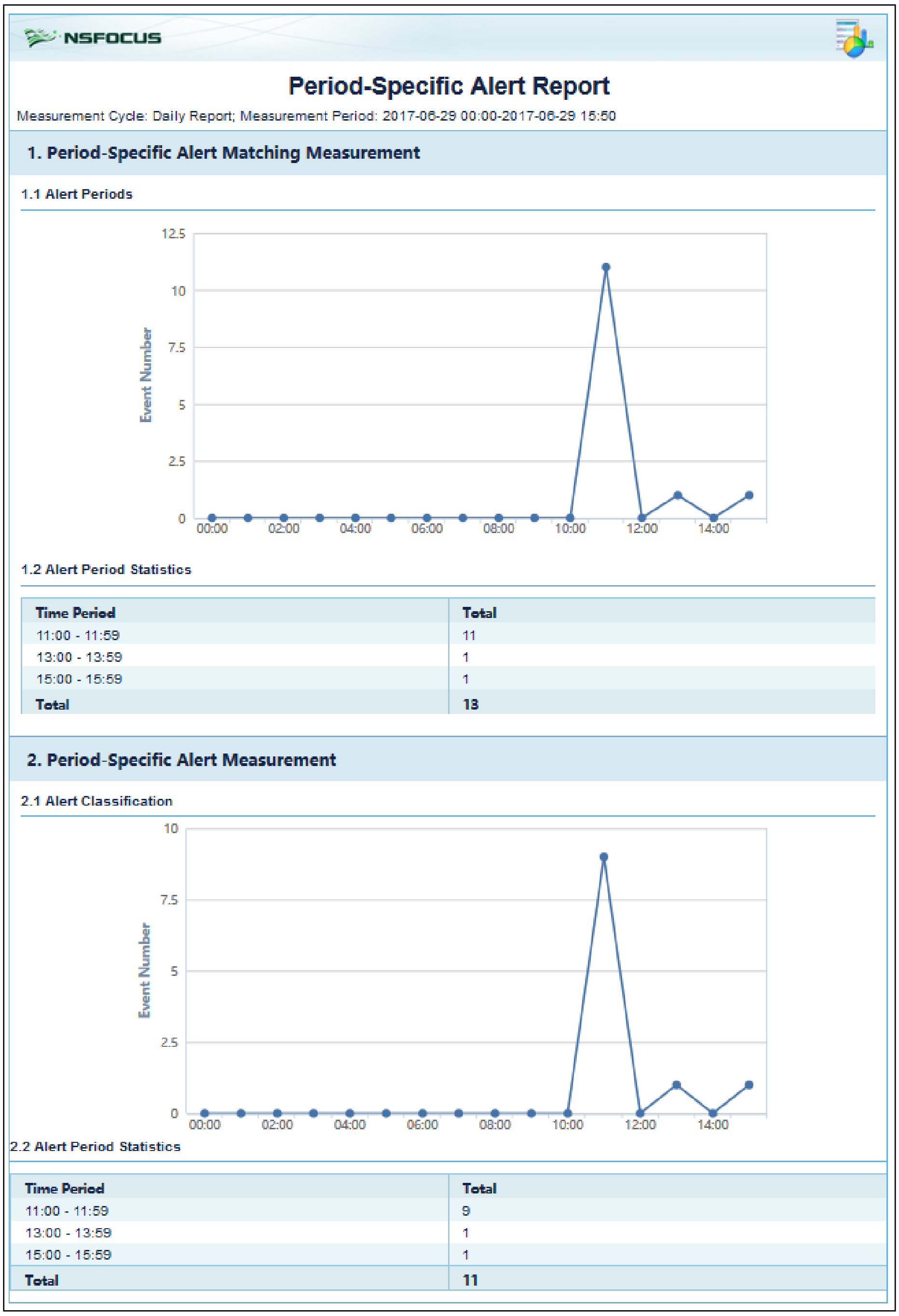
Step 3 Click **Generate**.

You can view statistics about various web security events in different time periods.

Figure 5-2 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 5-2 Period-specific alert report



Period-Specific Alert Report

Measurement Cycle: Daily Report; Measurement Period: 2017-06-29 00:00-2017-06-29 15:50

1. Period-Specific Alert Matching Measurement

1.1 Alert Periods

1.2 Alert Period Statistics

Time Period	Total
11:00 - 11:59	11
13:00 - 13:59	1
15:00 - 15:59	1
Total	**13**

2. Period-Specific Alert Measurement

2.1 Alert Classification

2.2 Alert Period Statistics

Time Period	Total
11:00 - 11:59	9
13:00 - 13:59	1
15:00 - 15:59	1
Total	**11**

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

5.1.3 IP Statistics Report

The IP statistics report displays the security events detected when a client accesses a specified website during a specified time period.

Choose **Logs & Reports** > **Security Reports** > **IP Statistics Report** and configure the IP statistics report parameters. Click **Generate**. The security event statistics report is generated.

Table 5-3 describes the IP statistics report parameters.

Table 5-3 Parameters for configuring the IP statistics report

Item	Description
Client IP	IP address of the client.
Website	Website the client accesses.
Client Location	Specifies the client's location.
Risk Level	Risk level of a security event. The options are **High**, **Medium**, and **Low**.
Date	Time range the statistics are collected.

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**.

Table 5-4 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: • **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**.

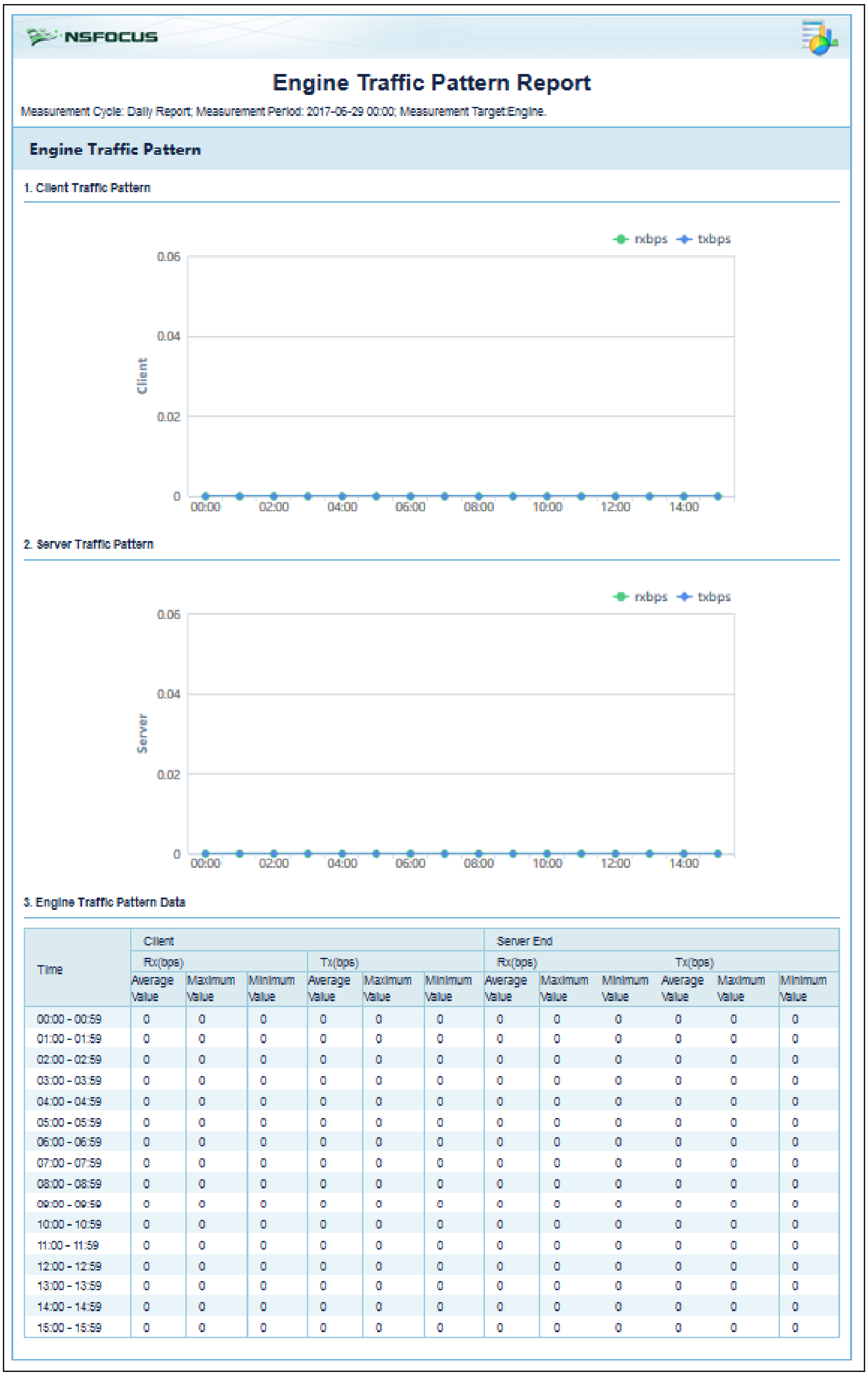
You can view traffic statistics of the measurement target within the specified period.

WAF provides two types of traffic statistics: engine traffic statistics and interface traffic statistics.

- Figure 5-3 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 5-3 Engine traffic pattern report



Engine Traffic Pattern Report

Measurement Cycle: Daily Report; Measurement Period: 2017-06-29 00:00; Measurement Target:Engine.

Engine Traffic Pattern

1. Client Traffic Pattern

2. Server Traffic Pattern

3. Engine Traffic Pattern Data

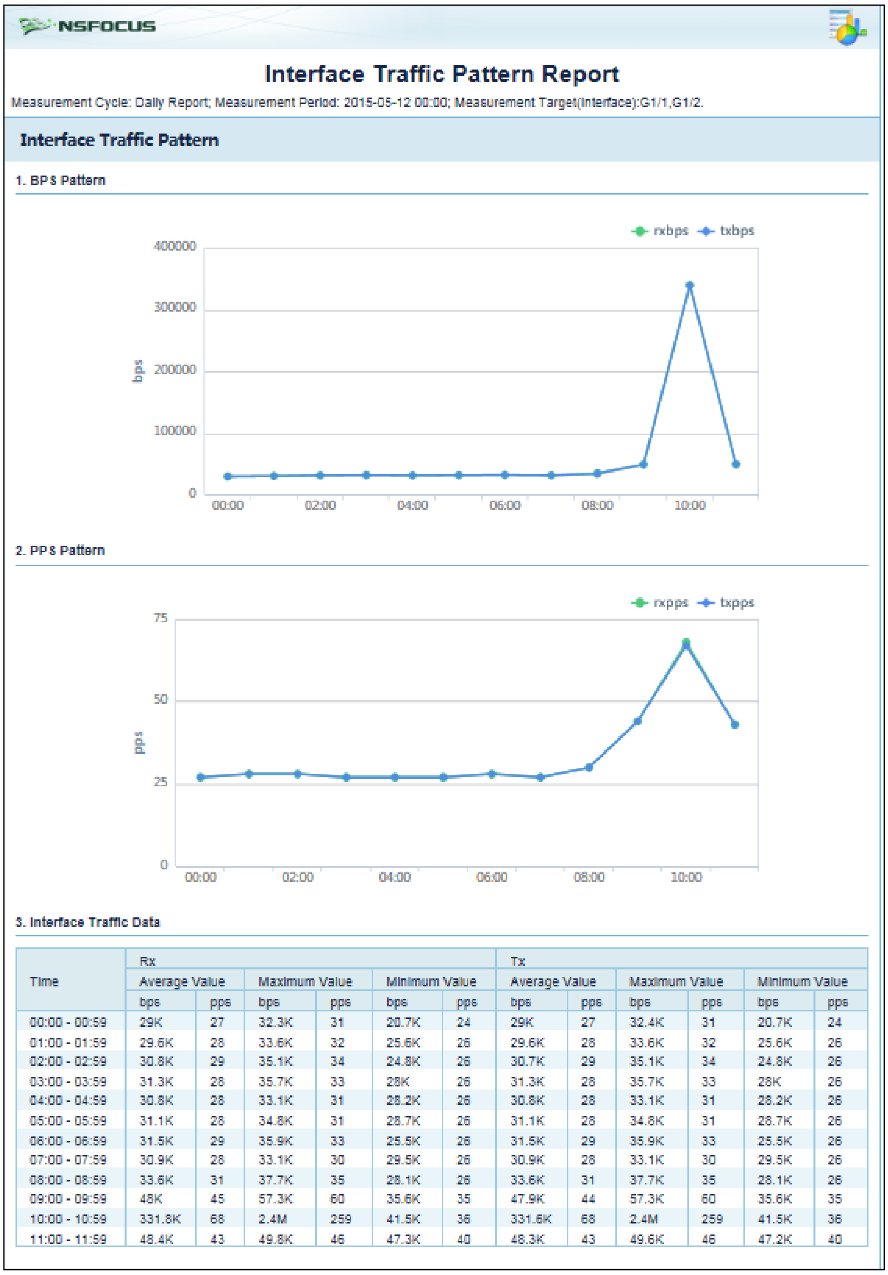
Time	Client						Server End					
	Rx(bps)			Tx(bps)			Rx(bps)			Tx(bps)		
	Average Value	Maximum Value	Minimum Value	Average Value	Maximum Value	Minimum Value	Average Value	Maximum Value	Minimum Value	Average Value	Maximum Value	Minimum Value
00:00 - 00:59	0	0	0	0	0	0	0	0	0	0	0	0
01:00 - 01:59	0	0	0	0	0	0	0	0	0	0	0	0
02:00 - 02:59	0	0	0	0	0	0	0	0	0	0	0	0
03:00 - 03:59	0	0	0	0	0	0	0	0	0	0	0	0
04:00 - 04:59	0	0	0	0	0	0	0	0	0	0	0	0
05:00 - 05:59	0	0	0	0	0	0	0	0	0	0	0	0
06:00 - 06:59	0	0	0	0	0	0	0	0	0	0	0	0
07:00 - 07:59	0	0	0	0	0	0	0	0	0	0	0	0
08:00 - 08:59	0	0	0	0	0	0	0	0	0	0	0	0
09:00 - 09:59	0	0	0	0	0	0	0	0	0	0	0	0
10:00 - 10:59	0	0	0	0	0	0	0	0	0	0	0	0
11:00 - 11:59	0	0	0	0	0	0	0	0	0	0	0	0
12:00 - 12:59	0	0	0	0	0	0	0	0	0	0	0	0
13:00 - 13:59	0	0	0	0	0	0	0	0	0	0	0	0
14:00 - 14:59	0	0	0	0	0	0	0	0	0	0	0	0
15:00 - 15:59	0	0	0	0	0	0	0	0	0	0	0	0

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 5-4 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 5-4 Interface traffic pattern report



Interface Traffic Pattern Report

Measurement Cycle: Daily Report; Measurement Period: 2015-05-12 00:00; Measurement Target(Interface):G1/1,G1/2.

Interface Traffic Pattern

1. BPS Pattern

2. PPS Pattern

3. Interface Traffic Data

Time	Rx						Tx					
	Average Value		Maximum Value		Minimum Value		Average Value		Maximum Value		Minimum Value	
	bps	pps	bps	pps	bps	pps	bps	pps	bps	pps	bps	pps
00:00 - 00:59	29K	27	32.3K	31	20.7K	24	29K	27	32.4K	31	20.7K	24
01:00 - 01:59	29.6K	28	33.6K	32	25.6K	26	29.6K	28	33.6K	32	25.6K	26
02:00 - 02:59	30.8K	29	35.1K	34	24.8K	26	30.7K	29	35.1K	34	24.8K	26
03:00 - 03:59	31.3K	28	35.7K	33	28K	26	31.3K	28	35.7K	33	28K	26
04:00 - 04:59	30.8K	28	33.1K	31	28.2K	26	30.8K	28	33.1K	31	28.2K	26
05:00 - 05:59	31.1K	28	34.8K	31	28.7K	26	31.1K	28	34.8K	31	28.7K	26
06:00 - 06:59	31.5K	29	35.9K	33	25.5K	26	31.5K	29	35.9K	33	25.5K	26
07:00 - 07:59	30.9K	28	33.1K	30	29.5K	26	30.9K	28	33.1K	30	29.5K	26
08:00 - 08:59	33.6K	31	37.7K	35	28.1K	26	33.6K	31	37.7K	35	28.1K	26
09:00 - 09:59	48K	45	57.3K	60	35.6K	35	47.9K	44	57.3K	60	35.6K	35
10:00 - 10:59	331.8K	68	2.4M	259	41.5K	36	331.6K	68	2.4M	259	41.5K	36
11:00 - 11:59	48.4K	43	49.8K	46	47.3K	40	48.3K	43	49.6K	46	47.2K	40

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 Managing Virtual Websites.

Step 1 Choose **Logs & Reports** > **Regional Access Statistical Report**.

Step 2 Set the query conditions.

Table 5-5 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.

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

Based on the Payment Card Industry Security Standards (PCI-DSS), WAF performs a PCD-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.

Note	The PCI-DSS compliance report function is unavailable on WAF deployed in mirroring mode.

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, choose **Logs & Reports** > **PCI-DSS Compliance Report**. Set the query conditions, and click **Generate**.

Table 5-6 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.

WAF generates the report in background and adds information about the generated report to the report list.

Downloading a Report

In the PCI-DSS compliance report list, 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. 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.

Deleting Reports

In the PCI-DSS compliance report list, 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

This chapter describes detailed information about each type of logs. Login logs, operation logs, export logs, and access 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 Default Parameters.

The default log retention period is 180 days, indicating that you can query logs of the last 180 days. The log retention period is configurable.

This chapter 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.
Exporting Logs	Describes how to export, download, and clear logs.
Auditing URL and File Access Logs	Describes how to view access logs and access statistics.
Managing Logs	Describes how to configure log management parameters, such as parameters for backing up, sending, and retaining 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**.

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: • <= 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: • = indicates precise query. • >= indicates fuzzy query. • != indicates contents excluded in the query.
URI	URI of web security events to be queried. NSFOCUS WAF support both precise query and fuzzy query based on URIs: • = 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.

Parameter	Description
Proxy Information	Proxy information. For details, see 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 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 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 Risk Level Policy.

----End

6.1.2 Network-Layer Access Control Logs

To view network-layer access control logs, choose **Logs & Reports** > **Security Protection Logs** > **Network-Layer Access Control Logs**. Set the query conditions and click **Query**.

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: • <= 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.

Parameter	Description
Action	WAF's actions in network-layer access control events to be queried, including: • **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**.

6.1.3 DDoS Protection Logs

To view DDoS protection logs, choose **Logs & Reports > Security Protection Logs > DDoS Protection Logs**. Set the query conditions and click **Query**.

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: • <= 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: • 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.

6.1.4 High-Risk IP Blocking Logs

To view high-risk IP blocking logs, choose **Logs & Reports > Security Protection Logs > High-Risk IP Blocking Logs**. Set query conditions and click **Query.**

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: • <= 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.

6.1.5 Web Anti-Defacement Logs

To view web anti-defacement logs, choose **Logs & Reports** > **Security Protection Logs** > **Web Anti-Defacement Logs**. Set the query conditions and click **Query**.

Table 6-5 Parameters for querying web anti-defacement logs

Parameter	Description
Date	Period when web anti-defacement logs to be queried are generated. The value can be one of the following: • <= 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	URLs of web anti-defacement logs to be queried. WAF supports both precise query and fuzzy query based on URLs: • = indicates precise query. • >= indicates fuzzy query. • != indicates contents excluded in the query.
Server IP Address/Port	Server IP addresses and ports of web anti-defacement logs to be queried. Both IPv4 and IPv6 addresses are supported.

6.1.6 ARP Protection Logs

To view ARP protection logs, choose **Logs & Reports** > **Security Protection Logs** > **ARP Protection Logs**. Set the query conditions, and click **Query**.

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: • <= 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 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**.

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 Creating a Website Group.

To view web access logs, choose **Logs & Reports** > **Security Protection Logs** > **Web Access Logs**. Set the query conditions and click **Query**.

By default, the latest 1000 logs that meet query conditions are displayed. To view all logs, click **Query** to the right of **Last**.

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: • <= 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.

Parameter	Description
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: • = 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.

Operations on logs are as follows:

- 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 Session Track Logs.

6.1.8 Session Track Logs

To view session tracing logs, choose **Logs & Reports** > **Security Protection Logs** > **Session Track Logs**. Set the query conditions and click **Query**.

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: • <= 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: • = indicates exact query.

Parameter	Description
	- >= 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 IP Address	Server/client IP addresses of session tracing logs to be queried. Both IPv4 and IPv6 addresses are supported.
Server Port	Server port number.
Client Location	Geographical location of session tracing events to be queried.

6.1.9 API Protection Logs

To view API protection logs, choose **API Security** > **API Protection Log**. Set query conditions and click **Query**.

Table 6-9 describes parameters for querying API protection logs.

Table 6-9 Parameters for querying API protection logs

Parameter	Description
Date	Species a period when API protection logs to be queried are generated. The value can be one of the following: - <= 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 API protection logs to be queried.
Website Group	Website group to be queried.
Risk Level	Risk level of API alerts to be queried. It can be **High**, **Medium**, or **Low**.
Server IP Address	IP address of the server in the API protection logs to be queried.
Domain Name	Domain name to be queried. WAF supports both exact query and fuzzy query based on domain names. - = indicates exact query. - >= indicates fuzzy query. - != indicates contents excluded in the query.
URI	URI of API protection logs to be queried. WAF supports both exact query and

Parameter	Description
	fuzzy query based on URLs: • = indicates exact query. • >= indicates fuzzy query. • != indicates contents excluded in the query.
Client Location	Geographical location of the client in API protection logs to be queried.
Client IP Address	Client IP address of API protection logs to be queried. Both IPv4 and IPv6 addresses are supported.
Server Port	Server port number.
Client Port	Client port number.
Protocol Type	Protocol types of API protection logs to be queried, which can be **HTTP** or **HTTPS**.
Method	HTTP request method.
Action	Specifies the action in the policy. It can be **Pass**, **Block**, **Accept**, **Redirect**, **Disguise**, **Clear**, **Replace**, and **Verification Code**.
Agent Info	User agent of API protection logs to be queried.
Local Time	Time when the API alert was generated.
Matching Policy	Name of the matching policy.
Matching Rule	Matching protection rule.
IP Address Block	Controls whether to enable IP block.
Operation	• Click 🔍 to view API protection log details. • Click ⊕ to add policy to **Exception Policy**.

6.2 Querying Traffic Control Logs

Traffic control logs are available when WAF is deployed in in-path, out-of-path, or reverse proxy mode.

To view traffic control logs, choose **Logs & Reports > Traffic Control Logs**. Set the query conditions and click **Query**.

Table 6-10 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.

Parameter	Description
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: • <= 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.

6.3 Querying System Running Logs

To view system running logs, choose **Logs & Reports** > **System Running Logs** > **Running Logs**. Set the query conditions and click **Query**.

Table 6-11 Parameters for querying system running logs

Parameter	Description
Date	Period when system running logs to be queried are queried. The value can be one of the following: • <= 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	Running status change type of system running logs to be queried, which can be one of the following: • 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 • Policy Compilation • Website Group Compilation
Source	Specific operation that triggers the log to be queried, which can be **Interface Open-Close**, **Normal System Startup-Shutdown**, **Engine Startup-Shutdown Control**, or **System Monitoring**.
Description	Brief description of system running logs to be queried.

6.4 Querying Login Logs

After login, an auditor can view login logs of various accounts on the **Login Logs** page.

To view login logs, choose **Audit Logs** > **Login Logs** > **Login Logs**. Set the query conditions. Click **Query**.

Table 6-12 Parameters for querying login logs

Parameter	Description
Date	Period when login logs are generated. The value can be one of the following: • <= 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.

6.5 Querying Operation Logs

After login, an auditor can view WAF operation logs of various accounts on the **Operation Logs** page.

To view operation logs, choose **Audit Logs** > **Operation Logs** > **Operation Logs**. Set the query conditions and click **Query**.

Table 6-13 Parameters for querying operation logs

Parameter	Description
Date	Period when operation logs are generated. The value can be one of the following: • <= 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	Operation type of operation logs to be queried, which can be one of the following:

Parameter	Description
	• 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.

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.

Exporting Logs

Exporting logs means saving logs as files in other storage media. Periodical log export is a good way to clear storage space.

To export logs, choose **Audit Logs** > **Export Logs** > **Export Logs**. On the **Export Logs** page, 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, click a desired log file, and save the log file to a local disk drive.

Clearing Log Files

On the **Export Logs** page, click **Clear Files** in the **Operation** column to clear a type of exported log files appearing in the **Download** column.

Note

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 Auditing URL and File Access Logs

URLs and files accessed by administrators, maintainers, auditors, and other users authorized by administrators on the WAF web-based manager are logged.

After login to WAF, the auditor can view access logs of various users as well as the statistics of accessed URLs and files.

Access Logs

Choose **Audit Logs** > **Access Audit** > **Access Logs**, and type query conditions to view access logs of various users on WAF. This can help auditors to check whether the access information is correct.

Table 6-14 Parameters for querying access logs

Parameter	Description
Date	Period when access logs to be queried are generated. The value can be one of the following: • <= plus a specific date: indicates the specific date and prior dates. • >= plus a specific date: indicates the period from the specific date to today. • Between plus two specific dates: indicates the period between the two specific dates.
Client IP Address	Specifies the client IP address of access logs to be queried. Both IPv4 and IPv6 addresses are allowed.
User	User account of access logs to be queried.
Access Type	Access type, including URL access, report downloading, and log downloading Note Only the report downloading conducted by the **admin** user is logged. Only the log downloading conducted by the **admin** user is logged.

Access Statistics

Access statistics helps the auditor to learn about the percentages of specific URLs and files accessed by various users on the WAF web-based manager. URL access statistics and file access statistics are collected separately.Choose **Audit Logs** > **Access Audit** > **Access Statistics**, and type query conditions to view the graph of access statistics in a specified period.

Table 6-15 Parameters for querying access statistics

Parameter	Description
Time	Period when access statistics to be queried are generated.
Accessed URLs	URLs accessed by various users on the WAF web-based manager.
Accessed Files	Files accessed by the **admin** user on the WAF web-based manager, including traffic

Parameter	Description
	reports and log files.

6.8 Managing Logs

You can export and back up system logs in the following ways:

- Direct export and backup
- Via syslog
- Via SNMP

6.8.1 Log Export and Backup

You can export, download, and clear various web security logs.

Exporting Logs

Exporting logs means saving logs as files in other storage media. Periodical log export is a good way to release storage space.

To export logs, choose **Logs & Reports** > **Log Management** > **Log Export & Backup**. On the **Log Export & Backup** page, 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

On the **Log Export & Backup** page, click a desired exported log file in the **Download** column to save the log file to a local disk drive.

Clearing Log Files

On the **Log Export & Backup** page, click **Clear Files** in the **Operation** column to clear a type of exported log files appearing in the **Download** column.

Note	Clicking **Clear Files** only clears exported log files appearing in the **Download** column, and has no impact on original log information in the database.

Clearing the Database

On the **Log Export & Backup** page, click **Clear Database** in the row of a log type to clear the type's original log information from the database.

Caution	Log information in the database cannot be recovered once being deleting. Perform deletion only when necessary.

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

Caution	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.

6.8.2 Syslog

WAF can send logs to a syslog server for storage. 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.

Note	The syslog configuration needs to be used in conjunction with log sending parameters. For details about log sending parameters, see Log Sending Parameters.

Adding a Syslog Server

Choose **Logs & Reports** > **Log Management** > **Syslog Configuration**. Click **Add** in the lower-right corner of the **Server IP Address** list. Set the server IP address and port, and click **Save**.

Deleting a Syslog Server

In the **Server IP Address** list, click ✖ in the **Operation** column and click **OK** in the confirmation dialog box.

Enabling or Disabling the Syslog Service

On the **Syslog Configuration** page, select **Yes** for **Enable Syslog**, and configure the method for saving the log content to the syslog server, which can be **Plaintext** or **Base64 encoding**. Then click **OK** to enable the syslog service.

To disable the syslog service, select **No** for **Enable Syslog**.

6.8.3 SNMP

WAF can send logs to an SNMP server for storage.

Note	The SNMP configuration needs to be used in conjunction with log sending parameters. For details about log sending parameters, see Log Sending Parameters.

6.8.3.1 Downloading the Management Information Base

Choose **Logs & Reports** > **Log Management** > **SNMP Configuration**. On the **SNMP Configuration** page, click **Download** 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.

6.8.3.2 Configuring an SNMP Agent

WAF supports SNMPv1, v2c, and v3. This section describes how to configure SNMP agents of the three versions.

Configuring an SNMPv1/v2c Agent

Choose **Logs & Reports** > **Log Management** > **SNMP Configuration**. On the **SNMP Configuration** page, select **Yes** for **Enable SNMP v1/v2c** and set **Community** in the **v1/v2c** section under **Agent Configuration**. Click **OK** to save the settings.

Configuring an SNMPv3 Agent

Before configuring an SNMPv3 agent, you must enable SNMP.

On the **SNMP Configuration** page, select **Yes** for **Enable SNMP v3** in the **v3** section under **Agent Configuration**. In the **v3** section, click **Create** to the upper right of the SNMP agent table. Set parameters in the **Add** dialog box and click **OK** to save the settings.

Table 6-16 Parameters for creating an SNMPv3 agent

Parameter	Description
User Name	Specifies the SNMPv3 user name.

Parameter	Description
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**.

6.8.3.3 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 Trap

Choose **Logs & Reports** > **Log Management** > **SNMP Configuration**. On the **SNMP Configuration** page, select **Yes** for **Enable Snmp Trap** and click **Create** in the **v1/v2c** section under **Trap Configuration** to add an SNMPv1/v2c server. Then set the server IP address, port, and community, and click **Save**.

Configuring an SNMPv3 Trap

Choose **Logs & Reports** > **Log Management** > **SNMP Configuration**. On the **SNMP Configuration** page, select **Yes** for **Enable Snmp Trap** and click **Create** in the **v3** section under **Trap Configuration**. Set parameters in the **Add** dialog box and click **OK** to save the settings.

Table 6-17 Parameters for configuring an SNMPv3 trap

Parameter	Description
Destination Host	Specifies the host that receives SNMP trap notifications 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 notifications.
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.

Parameter	Description
	The ID is a 16-bit hexadecimal digit without starting with 0x.

6.8.4 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 (that is, NPAI) parameters.

Choose **Logs & Reports > Log Management > Log Sending Parameter Configuration**. Set the log sending parameters. Click **OK** to save the settings.

Table 6-18 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. **Severity**: risk level of logs. There are eight levels, which are listed as follows in a low-to-high order: • Debugging message • Notification message • Common but important • Warning • Error • Critical • Immediate measure required • System unavailable
SNMP Parameters	Parameters for exporting logs via SNMP. **Enable**: controls whether to enable the SNMP service for the specified log type.
A Interface Parameters	Parameters for exporting logs to NSFOCUS ESPC over the A interface. **Enable**: controls whether to enable the A interface service for the specified log type.
Kafka Parameters	Parameters for exporting logs to the Kafka server. **Enable**: controls whether to send logs to the Kafka server.

You can click **Reset** to cancel your setting.

You can click **Display default settings** to reset log sending parameters to the default setting.

6.8.5 A Interface Configuration

WAF uploads data to NSFOCUS Cloud or ESPC only via the A interface (that is, NPAI). In this case, you need to enable the A interface. This interface is enabled by default.

To enable A interface, choose **Logs & Reports > Log Management > A Interface Configuration**. Select **Enable**. Click **OK** to save the settings.

6.8.6 Kafka Configuration

WAF can save logs to a Kafka server. This requires that related settings be configured on the Kafka side to receive logs in real time.

To configure a Kafka server on WAF, follow these steps:

Step 1 Choose **Logs & Reports** > **Log Management** > **Kafka Configuration**.

By default, the **Kafka Configuration** page lists previously configured Kafka clusters. You can add or delete a server as required.

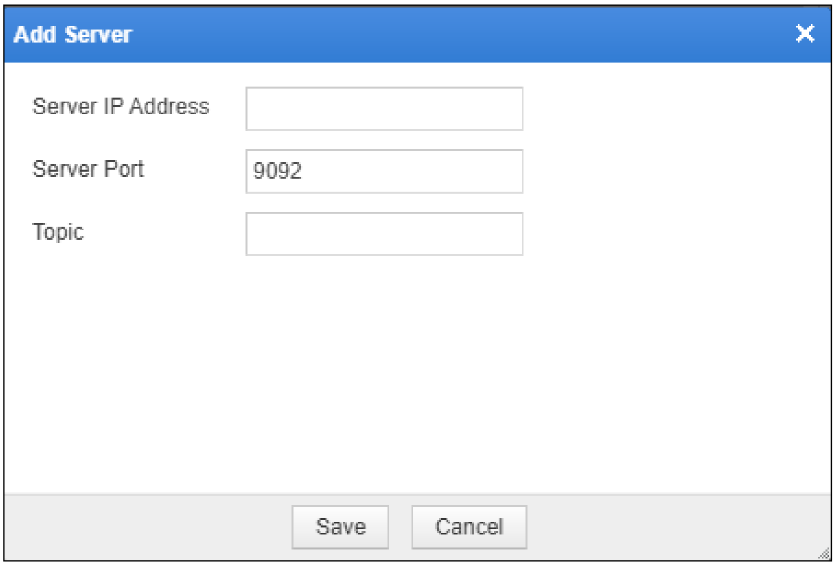
Table 6-19 Kafka configuration parameters

Parameter	**Description**
Enable Kafka	Controls whether to use Kafka to save logs. Options include **Yes** and **No**.
Log Content	Specifies the format of logs to be sent. Options include **Plaintext** and **Base64 encoding**. When **Enable Kafka** is set to **No**, the log content can only be Base64-encoded, which cannot be modified.
Device Location	Specifies the device location with a code like sz to be sent with logs.
IP Address	Specifies an IP address matching the URL to which statistics and signature database information will be sent.
Port	Specifies a port number matching the URL to which statistics and signature database information will be sent.

Step 2 In the **Cluster Configuration** section, click ⊕ to add one entry.

Step 3 Click **Add Server**.

Figure 6-1 Adding a server



Server Port: 9092

Step 4 In the **Add Server** dialog box, type the IP address, port, and topic, and click **Save**.

For a cluster, you can configure multiple servers.

----End

Deleting Cluster Configuration

On the **Kafka Configuration** page, you can delete clusters or servers as follows:

- Click ☒ to delete a cluster.
- Click **Delete** to delete a server.

6.8.7 Sensitive Parameter Configuration

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+&amp;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=[******]".

Caution	If the parameter content contains both sensitive information and an attack signature, the content will not be shielded.

Choose **Logs & Reports** > **Log Management** > **Sensitive Parameter Config**. Select **Enable** for **Sensitive Data Masking** and type sensitive parameters in the text box. Click **OK** to save the settings.

Note that multiple sensitive parameters should be separated by semicolons.

6.8.8 Scheduled Report

The scheduled report function allows to schedule the sending of a log report through a specific mailbox server to the user.

Table 6-20 Parameters for configuring a scheduled report

Parameter	Description
Enable scheduled report	Controls whether to enable or disable the scheduled report function. Options include **Yes** and **No**.
Sending time	Specifies the time to send a scheduled report.
Report frequency	Specifies the report frequency, which can be **Daily**, **Weekly**, or **Monthly**.
Recipient	Specifies the recipient email. Multiple recipients can be added and must be separated by commas.

6.8.9 Log Retention Configuration

Logs can be retained for 7 days to 3 years. By default, logs can be retained for 180 days.

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 Other Platforms	Describes how to connect WAF to ESPC.
User Management	Describes how to manage users.
User Management	Describes how to conduct traffic control.
Traffic Control Management	Describes how to configure system engine parameters as a maintainer.
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. WAF can be deployed in in-path, out-of-path, reverse proxy, plugin-enabled, mirroring, or transparent bridge mode. For the setting of system deployment mode, see Running Mode Configuration.

Note	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, eth0 and eth1). 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. On this page, you can view available interfaces in the system, and manage management interfaces and work groups.

Adding Management Interfaces

Click **Add** in the upper-right corner of the **Management Interfaces** list. In the **Add Management Interface** dialog box that shows available interfaces, select desired interfaces and click **OK**.

Note	• 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".

Note	• 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 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.

Editing Management Interfaces

In the **Management Interfaces** list, click ✎ in the **Operation** column. In the dialog box, edit the interface parameters. Click **OK** to save the settings.

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**.

Parameter	Description
IP Address	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. Note You can add, delete, or clear a pair of the IP address and subnet mask: • Click **Clear** to clear the first pair. • Click **Add** to set more pairs. • Click **Delete** to delete a pair.
Rate	Traffic rate of the interface, which can be one of the following: • **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)	Maximum transmission unit (MTU) of this interface in bytes. 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.

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, 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.

On the **Work Group Management**, click **Add** in the lower-right corner of the **Work Group** list to create a work group. In the **Create Work Group** dialog box, edit the work group parameters and click **OK** to save the settings.

Interfaces available in the system are automatically displayed in the **Available Interfaces** list.

Note

- 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.

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.

Editing Working Interfaces

In the **Work Group** list, click ✎ in the **Operation** column. In the dialog box, edit the interface parameters. Click **OK** to save the settings.

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: • 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	Traffic rate of the interface, which can be one of the following: • **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 (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	Controls whether the source MAC address of packets transmitting from this interface is replaced with the MAC address of this interface. • **Yes**: indicates that the source MAC address is replaced. • **No**: indicates that the source MAC address is not replaced. Usually, this option is configured for a WAN interface.

Editing Work Groups

In the **Work Group** list, click **Edit** in the upper-right corner of a work group. In the **Edit Interface** dialog box, set the parameters. Click **OK** to save the settings.

In the dialog box that appears, you can edit the basic information and VLAN subinterface of the work group.

Deleting a Work Groups

In the **Work Group** list, 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. In the dialog box, set the parameters. Click **OK** to save the settings.

The area for creating a VLAN appears in the red frame.

Note	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**.

7.1.1.2 Work Group Management in Out-of-Path Mode

On the **Work Group Management** 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

Creating Work Groups

There is one default work group on WAF.

Click **Add** in the lower-right corner of the **Work Group** list. In the **Create Work Group** dialog box, set the parameters. Click **OK** to save the settings.

Interfaces available in the system are displayed in the **Available Interfaces** section.

Note	In out-of-path mode, you can create a work group if there is any available interface.

Note	In the **Create Work Group** dialog box, physical interfaces are selected as working interfaces only. They can function as working interfaces only after being edited and configured with some properties.

Creating Subinterfaces

In the **Work Group** list, click ✎ in the **Operation** column to edit a working interface. In the **Edit Interface** dialog box, click **Add Subinteface** ⊕ to create a subinterface. In the displayed dialog box, set the paraemeters, and click **OK** to save the settings.

Viewing the Forwarding Table

In the **Work Group** list, 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.

Viewing the Forwarding Routing Table

In the **Work Group** list, 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.

Configuring Injection Routes

You can use either of the following two methods to configure an injection route for a work group.

- In the **Work Group** list, click **Edit** in the upper-right corner of a work group. In the displayed Work Group Configuration dialog box, click **Add Route**. Set the parameters, click **OK,** and return to the **Route Injection Configuration** list. Click **Apply All** in the lower-right corner.

- In the **View Forwarding Routing Table** dialog box, click **Route Injection Configuration**. Click **Add Route**, set the parameters, and click **Apply All** to make the settings take effect.

7.1.1.3 Work Group Management in Reverse Proxy Mode

On the **Work Group Management** page, you can view available interfaces in the system and manage management interfaces and work groups.

On WAF deployed 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. The method of managing work groups in reverse proxy mode is similar to that for work groups in in-path mode. For details, see Work Group Management in In-Path Mode.

7.1.1.4 Work Group Management in Mirroring Mode

On the **Work Group Management** page, you can view available interfaces in the system and configure management interfaces and work groups.

On WAF deployed in mirroring mode, you cannot add or delete management interfaces.

IP addresses cannot be configured for interfaces in work groups and VLANs cannot be configured. The method of managing work groups in mirroring mode is similar to that for work groups in in-path mode. For details, see Work Group Management in In-Path Mode.

7.1.1.5 Work Group Management in Plugin-enabled Mode

On the **Work Group Management** page, you can view available interfaces in the system and configure management interfaces and work groups.

On WAF deployed in plugin-enabled mode, you can manage configured IP addresses in batches. The method of managing work groups in plugin-enabled mode is similar to that for work groups in in-path mode. For details, see Work Group Management in In-Path Mode.

7.1.1.6 Work Group Management in Transparent Bridge Mode

On the **Work Group Management** page, you can view available interfaces in the system and configure management interfaces and work groups. You cannot add or delete management interfaces. Interfaces in a work group cannot be configured with IP addresses and VLANs cannot be configured.

On WAF deployed in transparent bridge mode, you can use multiple physical interfaces to create an aggregation interface and use the aggregation interface in a work group to improve traffic transmission bandwidth and increase network availability. There are two types of aggregation interfaces: manual aggregation and dynamic LACP.

The method of managing work groups in transparent bridge mode is similar to that for work groups in in-path mode. For details, see Work Group Management in In-Path Mode.The following describes how to create an aggregation interface and create a work group that uses aggregation interfaces.

Creating an Aggregation Interface

Choose **System Management** > **Network Configuration** > **Work Group Management**. In the aggregation interface list, click **Add** to configure an aggregation interface.

Table 7-4 describes the parameters for configuring an aggregation interface.Parameters for configuring an aggregation interface

Parameter	Description
Name	Name of the aggregation interface.
Member Interfaces	Member interfaces of the aggregation interface. The number of member interfaces in an aggregation interface ranges from 2 to 8.
Type	Specifies the type of the aggregation interface. Option can be: • **Manual aggregation**: Traffic is distributed among all member interfaces. • **Dynamic LACP**: Traffic is distributed among LACP-negotiated member interfaces.
Load Balancing Method	Specifies the distribution policy type. Options include: • **Round robin**: distributes traffic to the member interfaces of the aggregation interface through a polling mechanism. • **src-mac**: distributes traffic to the matched member interfaces of the aggregation interface based on the source MAC address calculation result. • **dst-mac**: distributes traffic to the matched member interfaces of the aggregation interface based on the destination MAC address calculation result. • **src-dst-mac**: distributes traffic to the matched member interfaces of the aggregation interface based on the source and destination MAC address calculation result. • **src-dst-mac + src-dst-ip**: distributes traffic to the matched member interfaces of the aggregation interface based on the bidirectional MAC and bidirectional IP address calculation result. • **src-dst-mac + src-dst-port**: distributes traffic to the matched member interfaces of the aggregation interface based on the bidirectional MAC and bidirectional port calculation result.

Creating a Work Group that Uses Aggregation Interfaces

After configuring aggregation interfaces, you can create a work group that uses aggregation interfaces.

Choose **System Management** > **Network Configuration** > **Work Group Management**. In the work group list, click **Add** to configure a work group that uses aggregation interfaces.

Table 7-5 describes the parameters for configuring a work group that uses aggregation interfaces.

Table 7-5 Parameters for configuring a work group that uses aggregation interfaces

Parameter	Description
Name	Name of the work group.
Description	Description of the work group.
WAN Interface	Specifies a WAN interface.
LAN Interface	Specifies a LAN interface.

Parameter	Description
Type	Specifies an interface type. The options include **Available Interfaces** and **Aggregation Interfaces**.
Interface Name	Specifies an interface.
Bound Interfaces	Bound interfaces of the specified interface. • When **Available Interfaces** is selected, the specified physical interface is displayed by default. • When **Aggregation Interfaces** is selected, the member interfaces of the specified aggregation interface are displayed.

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 for small networks rarely changing. As static routes cannot automatically adapt to network changes, if a network fails or a topology changes, the static route configuration needs to be manually modified.

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

Choose **System Management** > **Network Configuration** > **Route Configuration**. Type the IP address of the desired gateway in the **Default Gateway** text box and click **OK** to save the settings.

Creating a Static Route

Click **Add** in the upper-right corner of the **Static Route** list. In the **Add** dialog box, set the static route parameters. Click **OK** to save the settings.

Table 7-6 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.

Deleting a Static Route

In the **Static Route** list, 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

Choose **System Management** > **Network Configuration** > **DNS Configuration**. Specifies IPv4 or IPv6 addresses for the preferred and alternate DNS servers. Click **OK** to save the settings.

7.1.3.2 Managing Custom Domain Names

You can create, edit, and delete custom domain names.

Creating Custom Domain Names

Choose **System Management** > **Network Configuration** > **DNS Configuration**. In the **Customized Domain Name** list, click **Add** in the upper-right corner. In the **Create** dialog box, set the parameters. Click **OK** to save the settings.

Editing Custom Domain Names

In the **Customized Domain Name** list, click ✎ in the **Operation** column. In the dialog box that appears, edit the parameters and click **OK** to save the settings.

Deleting Custom Domain Names

In the **Customized Domain Name** list, 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 plugin-enabled mode)
- Bypass Configuration (unavailable in mirroring, reverse proxy, and plugin-enabled modes)
- VRRP Configuration (unavailable in in-path, plugin-enabled, and transparent bridge modes)

7.2.1 Running Mode Configuration

Choose **System Management** > **System Deployment** > **Running Mode** to open the **Running Mode** page.

- **Deployment Topology** can be set to **In-Path**, **Out-of-Path**, **Reverse Proxy**, **Plugin-enabled, Mirroring,** or **Transparent Bridge**.
- **Mode Configuration** can be set to one of the following values. Note that the emergency mode is available only in in-path mode and in out-of-path mode:
  - **Forwarding Mode**: In this mode, the engine forwards traffic without processing, and thus has no protection effect. This mode is unavailable for reverse proxy and plugin-enabled deployment.
  - **Protection Mode**: In this mode, WAF implements protection for servers.
  - **Debugging Mode**: In this mode, WAF provides the same protection for servers as it functions in protection mode, and more debugging information is available on the background. This mode is usually used for WAF debugging. The debug level options are **debug**, **info**, **warn**, and **alert**. By default, it is **warn**. You are recommended not to change the setting. The debugging mode is not available on WAF deployed in transparent bridge mode.
  - **Emergency Mode**: After entering the emergency mode, WAF continues handling traffic on established TCP connections, but directly forwards new requests. The emerency mode is available on WAF deployed in in-path and out-of-path modes.

    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.

Choose **System Management** > **System Deployment** > **Running Mode** to select a deployment topology and mode.

Table 7-7 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

Parameter		Description
		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.

WAF deployed in in-path mode supports both master/slave HA and active-active HA. In transparent bridge, out-of-path, or reverse proxy mode, WAF supports master/slave HA only. HA is used to implement 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 salve device does not. If the number of consecutive lost heartbeats detected by the slave device reaches the specified threshold, the slave device immediately enables working interfaces and takes over services, to ensure service continuity. If the slave device fails to receive heartbeat messages from the master device for a specified number of consecutive times, it considers that the master device has lost its heartbeat. The slave device will then decide whether to start its work interfaces, depending on the configuration.

To configure HA, choose **System Management > System Deployment > HA Configuration**. Set the HA parameters and click **OK** to save the settings.

Table 7-8 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: • **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. After HA is enabled, WAF's status will be displayed. Note Working modes vary with deployment modes.
Work Group	Work group for which HA is enabled. One or more work groups can be selected for link status monitoring.
Heartbeat Port	Interface over which the current WAF exchanges heartbeat signals with the peer WAF. It is a management interface. Up to two heartbeat ports can be added.
Peer IP Address	IP address of the peer heartbeat interface. Both IPv4 and IPv6 addresses are supported.
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)	Interval for sending heartbeat messages.
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.
Gateway Info	You can add gateway information of the peer device if it is needed.

7.2.3 Bypass Configuration

WAF provides built-in bypass and external bypass functions.

- Built-in bypass

Built-in bypass can be configured on the NIC that supports bypass.

- External bypass

  External bypass can be configured on the NIC that does not support bypass. You can connect this type of NIC to a bypass switch to implement the bypass function.

Note

Bypass configuration is available only on WAF deployed in in-path, out-of-path, or transparent bridge mode.

The external bypass function is not available on WAF deployed in transparent bridge mode.

7.2.3.1 Built-in Bypass

Built-in bypass is implemented by software.

Enabling Built-in Bypass Groups

You can enable built-in bypass groups by using one of the following methods:

- Enabling built-in bypass via **Watchdog Heartbeat Process**

  Choose **System Management** > **System Deployment** > **Built-in Bypass Configuration**. On the **Built-in Bypass Configuration** page, set **Watchdog Heartbeat Process** 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, set **Watchdog Heartbeat Process** to **Disable**.

  In the **Manual Bypass Enable-Disable Control** list, click ▶ in the **Operation** column to enable built-in bypass. After it is enabled, its status turns to ✓.

Disabling Built-in Bypass Groups

You can disable built-in bypass groups by using one of the following methods:

- Disabling built-in bypass via **Watchdog Heartbeat Process**

  Note that 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, 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

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.

Note	- 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 7-1 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 7-1 External bypass topology

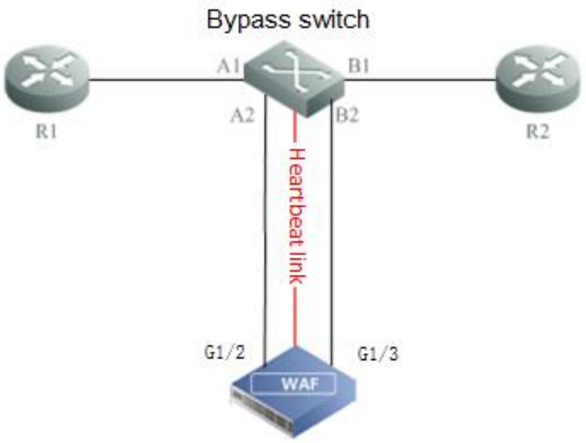
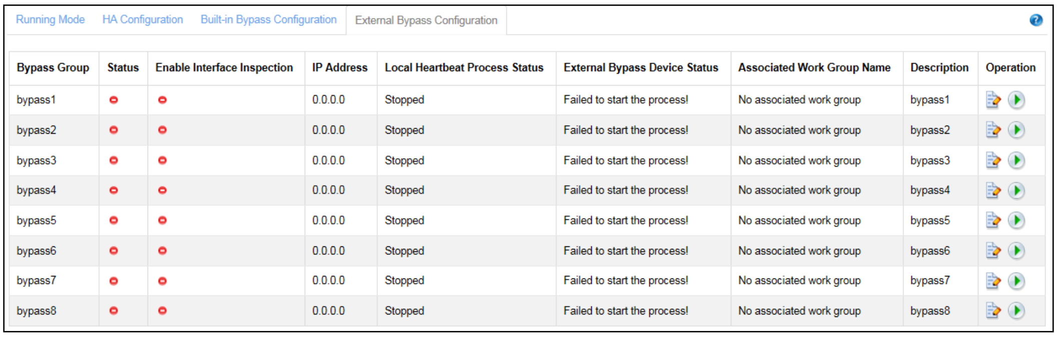


Figure 7-2 External Bypass Configuration page



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

Choose **System Management > System Deployment > External Bypass Configuration**. The **External Bypass Configuration** page appears. In the external bypass configuration list, click ✎ in the **Operation** column. In the **Edit** dialog box, edit the external bypass parameters. Click **OK** to save the settings.

Table 7-9 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.

Enabling External Bypass Groups

In the external bypass configuration list, click ▶ in the **Operation** column to enable a bypass group. After it is enabled, its status turns to ✓.

Disabling External Bypass Groups

In the external bypass configuration list, click ■ in the **Operation** column to disable a bypass group. After it is disabled, its status turns to ⊖.

7.2.4 VRRP Configuration

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, 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.

> **Note**
>
> Virtual Router Redundancy Protocol (VRRP) configuration is only available in out-of-path and reverse proxy deployment modes.

Perform the following steps to configure VRRP in reverse proxy mode:

Step 1 Choose **System Management** > **System Deployment** > **VRRP Configuration.**

> **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. Click **OK**.

The **VRRP Configuration** page appears.

Step 3 Click the VRRP instance management icon ▣ in the **Operation** column of interface G1/1.

The **G1/1 Instance Management** page appears.

Step 4 Click **Add** in the lower-right corner of the page.

> **Note**
>
> 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.

Step 5 In the dialog box, set the VRRP instance parameters.

Table 7-10 Parameters for creating a VRRP instance

Parameter	Description
Group ID	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. **Note**

Parameter	Description
	The master WAF and backup WAF must have the same group ID.
Priority	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.
Virtual IP Addresses	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.
Enable or Not	Controls whether to enable the VRRP instance, which can be either of the following: • **Yes**: The VRRP instance is enabled. • **No**: The VRRP instance is disabled. This parameter is mandatory.
Allow Preemption	Working mode of the master WAF and backup WAF, which can be either of the following: • **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 mater 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	Initial state of WAFs in this instance, which can be either of the following: • **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	First IP address configured for the interface with the VRRP instance. 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.
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 6 Click **Save** to save the settings.

----End

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

7.3.1 System Information

Choose **System Management** > **System Tools** > **System Information**. If no SSL card is loaded in WAF, the **System Information** page 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 value.

The **System Information** page varies with whether an SSL card is loaded in WAF. If an SSL card is loaded in WAF, an extra **SSL Card** column will appear in the list.

7.3.2 System Upgrade

For a licensed WAF, users can always conduct system upgrade before the license expires, to enhance system functions.

To perform system upgrade, choose **System Management** > **System Tools** > **System Upgrade**. Click **Browse** and select the desired upgrade file with the extension of .bin. 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.

Tip

- If **Disable auto update** is set for **Installation Method** in the **Scheduled Upgrade** section 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.

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.

7.3.3.1 Viewing the Current Version Information

Choose **System Management** > **System Tools** > **Rule Upgrade**. On the **Rule Upgrade** page**, you can view t**he current version information, including the current rule database version and dependency system version in the **Current Version Info** section.

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

Choose **System Management** > **System Tools** > **Rule Upgrade**. On the **Rule Upgrade** page, configure parameters in the **Scheduled Upgrade** section. Click **OK** to save the settings.

Table 7-11 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.

Parameter	Description
	The format should be in the format of 12:38.
Installation Method	Specifies how the new rule upgrade package is installed after download. • **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. • 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.

Manual Upgrade

Choose **System Management** > **System Tools** > **Rule Upgrade**. On the **Rule Upgrade** page, click **Choose File** in the **Manual Upgrade** section, and select the desired upgrade file with the extension of .bin. Then 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.

7.3.3.3 Checking Updates

In the **Check Update** section on the **Rule Upgrade** page, you can check updates and view historical updates.

Checking Updates

Choose **System Management** > **System Tools** > **Rule Upgrade**. On the **Rule Upgrade** page, click **Check Update** in the **Check Update** section. 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.
- 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

Choose **System Management** > **System Tools** > **Rule Upgrade**. On the **Rule Upgrade** page, click **Historical Updates** in the **Check Update** section. The **Historical updates** dialog box appears.

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.

Viewing Rule Upgrade Packages

Choose **System Management** > **System Tools** > **Rule Upgrade**. You can view rule upgrade packages in the **Auto-Backup of Rule Database** section.

Downloaded rule upgrade packages are displayed in the rule upgrade package 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

Click **Restore** in the **Operation** column in the rule upgrade package list to 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.

7.3.4 Configuration Synchronization

WAF provides the configuration synchronization function. If configuration files (such as system configuration and policy configuration) are damaged because of WAF exceptions, you can restore the configuration files in either of the following ways:

- Offline synchronization: backs up and restores configuration files via a restore point.
- Online synchronization: synchronizes selected configuration files to another device.
- Scheduled online synchronization: synchronizes the configuration to another device at the scheduled start time and at a specified interval.

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**.

Step 2 Create restore point.

a. Specify the synchronization scope.

Table 7-12 Synchronization scope

Parameter	Description
All	The scope covers the customer's assets, protection policies, network interfaces, APIs, and new rule bases.
Assets and policies	The scope covers: • The following configurations under **Security Management**: **Website Protection**, **Custom Rules**, **Policy Management**, **Template Management**, **Smart Patch**, **Secure Delivery**, **Proxy Information Configuration**, **XSD/WSDL File Management**, **Rule Database Management**, and **IP Reputation**. • **Server Alive Status Check** under **System Monitoring**. • **API Management** and **OAS File Management** under **API Security**.
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, 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 the **Import Backup File** section, 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:

- Click to download it for local backup.
- Click to delete it.
- Click to view its details.

7.3.4.2 Online Synchronization

Choose **System Management** > **System Tools** > **Synchronize Configuration**. Enable the rsync-606 service, specify the synchronization scope, set the synchronization mode to **Online**, and type the IP address of the desired peer device and the service password. 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.

You can click in the row of an online synchronization record to view its details.

7.3.4.3 Scheduled Online Synchronization

Choose **System Management** > **System Tools** > **Synchronize Configuration**. Enable the rsync-606 service, set the synchronization mode to **Scheduled online**, and enable it. Type the IP address of the desired peer device and the peer service password. Specify the synchronization start time and the synchronization interval, and then click **OK**.

The configuration will be synchronized to the desired peer device starting at the scheduled start time and at the specified interval.

Table 7-13 Scheduled online synchronization parameters

Parameter	Description
Enable or Not	Controls whether to enable scheduled online synchronization.
Peer IP	Specifies the IP address of the peer device.
Peer Service Password	Specifies the peer service password.
Start Time	Specifies the scheduled synchronization start time.
Synchronization Interval	Sets the synchronization interval. The value ranges from 1 to 60. The unit can be minutes, hours, days, or weeks.

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 license

  After a trial license expires:

  - System upgrade cannot be performed.

- The **Submit** button is dimmed.
- The engine stops running.
- The system automatically enters the forwarding mode.
- Protection functions of the system lose effect.

Note	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, but the system cannot be upgraded.

7.3.5.1 Viewing License Information

Choose **System Management** > **System Tools** > **License**. The **License** page appears.

After importing a license, you can view license information and authorized registration information. When the remaining period is less than 90 days for a paid license or less than 7 days for a trial license, the system prompts a message indicating that the license is about to expire.

7.3.5.2 Importing a License

Step 1 Choose **System Management** > **System Tools** > **License**. On the **License** page, 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.

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.

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

7.3.5.3 License Expiration Warning

A license expiration warning appears for the first time when the paid license expires in 90 days and the trial license expires in 7 days. When you log in to WAF, a pop-up window prompts the details of the license expiration. The reminder frequency is configurable.

When the license expires, a pop-up window will appear, prompting that the license has expired in red text. You can also set the reminder frequency.

To reduce the exposure to risk and avoid unnecessary financial and data losses, we recommend that the paid license user purchase the warranty service as soon as possible.

Contact your NSFOCUS sales account manager or NSFOCUS technical support to learn more about purchasing service.

To ensure that the device functions properly, we recommend that the trial license user contact NSFOCUS technical support in time to obtain a new license.

7.3.5.4 License Expiration Email Notification

A license expiration email notification is sent for the first time when the paid license expires in 90 days and the trial license expires in 7 days. The email notification frequency is configurable.

Choose **System Management** > **System Tools** > **License**. In the **Trial License Expiration Email Notification** area or **Paid License Expiration Email Notification** area, set the recipients and the reminder frequency. Multiple email addresses should be separated by a comma, for example, xxx@xx.com,xxx@xx.cn.

Note	Before using the license expiration email notification service, choose **System Management** > **Email Sending Configuration** to configure the email sending service.

7.3.6 System Time and Language

Choose **System Management** > **System Tools** > **Time & Language**. The **Time & Language** page appears. You can set the system time, time server, and system language.

7.3.7 System Control

Choose **System Management** > **System Tools** > **System Control**. The **System Control** page appears.

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.

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.

7.4 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 connectivity between the system and a destination host, response time, and whether a domain name is correctly parsed.

Choose **System Management** > **Test Tools** > **Ping**. The **Ping** page appears. Type the IP address of a target host in the **Destination IP Address** text box and click **Ping**. The ping result appears.

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.

7.4.3 Traceroute

Traceroute is used to trace the path that an IP packet takes to its destination and display the time the packet reaches each node.

Choose **System Management** > **Test Tools** > **Trace Route**. The **Trace Route** page appears. Type the IP address of a target host in the **Destination IP Address** text box and click **Traceroute**. The trace result appears.

7.4.4 Packet Capture

The **admin** user can use the packet capture tool to capture packets transferred through an interface on WAF. The packet capture file can be used to analyze whether the device sends and receives packets as expected, or analyze alert details, facilitating 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:

Choose **System Management** > **Test Tools** > **Capture Packets**, and click **Capture Packets**. In the dialog box, set the packet capture parameters and click **OK** to start capturing packets.

Note that if you want to reset the parameters, click **Reset** to restore the default settings of the parameters.

Table 7-14 Parameters for capturing packets (in-path, out-of-path, reverse proxy, and plugin-enabled modes)

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**. • **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.
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.

Table 7-15 Parameters for capturing packets (transparent bridge and mirroring modes)

Parameter	Description
Interface	Interface where packet capture is conducted. The default value **any** indicates all logical interfaces.
Protocol	Protocol of packets to be captuered. The default value **any** indicates all protocols.
Packet Direction	Direction of packets to be captured. Option can be **All**, **Rx**, or **Tx**. • **Rx**: indicates the system captures packets that are received.

Parameter	Description
	• **Tx**: indicates that the system captures packets that are sent. • **All**: indicates that the system captures packets that are sent and that are received.
Source IP/Netmask	Source IP address and net mask of packets to be captured. The default value **0** indicates all IP addresses and netmasks.
Source Port	Source port of packets to be captured. The default value **0** indicates all ports.
Destination IP/Netmask	Destination IP address and net mask of packets to be captured. The default value **0** indicates all IP addresses and netmasks.
Destination Port	Destination port of packets to be captured. The default value **0** indicates all ports.
Capture Time (sec)	Duration of capturing PCAP packets. When the specified duration expires, packet capture will stop. The default value **0** indicates no limit to the capture duration.
Packet Count	Upper limit of captured PCAP packets.
PACP File Capacity	Size of the PCAP file in MB. The default value is **16**.

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.

To download a packet capture file, click it listed in the **File Name** column or click ⬇ in the **Operation** column to download it to a local directory. You can delete a packet capture file by clicking ✖ in the **Operation** column.

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. You can click listed buttons to perform corresponding operations.

7.4.6 Scanner

A scanner is built in WAF to scan protected servers for website vulnerabilities.

Choose **System Management** > **Test Tools** > **Scanner**. Click **Create**. In the **Create Scanner** dialog box, set the scanning parameters. Click **OK** to save the settings.

Table 7-16 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: • SQL Injection and XSS Vulnerability Scanning • Trojan scanning

Parameter	Description
Entrance URL	Starting URL to be scanned, for example, http:192.168.1.100/index.html. **Note** An HTTPS URL is not supported.
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. • **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.

WAF executes the scanning task at the scheduled time. After the scanning task is completed, the scanning result appears in the area.

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**.

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 7-17.

Table 7-17 Global parameters for debug log tracking

Parameter	Description
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

Parameter	Description
	to the tracking list, the tracking stops when the specified duration expires.

Note	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** section.

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.

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** section.

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.

Note	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 Other Platforms

WAF supports the connection to the NSFOCUS cloud, NSFOCUS Enterprise Security Platform (ESP-C), NSFOCUS Big Data Security Analysis (BSA), and NSFOCUS T-ONE CLOUD.

- 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 ESP-C

  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. For more information on centralized management, see *NSFOCUS ESP-C User Guide-WAF*.

- 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.

- NSFOCUS T-ONE CLOUD

  NSFOCUS T-ONE CLOUD is a security operations center for managing NSFOCUS security series products and third-party security products. It provides one-click online and offline operations for WAF-protected websites.

  After downloading the T-ONE CLOUD Security Manager app and connecting your WAF to T-ONE CLOUD, you can bring WAF-protected websites online or offline as needed.

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. The page on a WAF device under non-centralized management is different from that on a WAF device under centralized management.

Step 2 In the dialog box, set the basic parameters.

Table 7-18 ESPC-related parameters on WAF

Parameter		Description
Local IP	Local IP	IP address of WAF's management interface for the engine for communicating with the NSFOCUS cloud, NSFOCUS ESPC, and NSFOCUS BSA. Note By default, it is the first IP address of the first management interface. The default value is recommended.
NSFOCUS Cloud	Device Care Service	Controls whether to enable device care service. 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. 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. You can also view device status information on the device care service page on the NSFOCUS cloud. Note • 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	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. If centralized management under ESPC is successfully configured, a link saying **exit ESPC central manage** is displayed. For details, see *NSFOCUS ESPC User Guide - WAF.*
	Port	Specifies the port used by ESPC to exchange data with the WAF engine.
	Data Transmission	Controls whether to start connecting WAF to ESPC. Selecting the Start check box enables WAF to connect to ESPC. Note When ✓ Connected is displayed, the connection has been established.
Big-data Security Analytics Platform (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 ✓ Connected is displayed, the connection has been established.

NSFOCUS T-ONE CLOUD	Server Address	IP address of the T-ONE CLOUD portal to which WAF is connected.
	Port	Port number of the T-ONE CLOUD portal.
	T-ONE User Name	User name for T-ONE CLOUD portal login.
	Password	Password for T-ONE CLOUD portal login. Note When ✓ Connected is displayed, the connection has been established.
Other	Interface Version	Version of the A interface.
	Interface Upgrade Time	Upgrade time of the A interface.
	Interface Upgrade	You need to click **Choose File** to select the A interface upgrade file of the local ESP-C and click **Upgrade** to upgrade the interface. Note The A interface can be upgraded together with the system version upgrade. Therefore, this function is not used in practice.
	Debugging Information	Status information about the collaboration (over the A interface) between WAF and NSFOCUS ESP-C. 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. Note This function is not used in practice.

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, enable, 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 the RADIUS server: describes how to configure RADIUS authentication.

- Unblocking accounts: describes how to unlock other accounts as an **admin** user.
- IP unlocking: describes how to unlock IPs as an **admin** user.
- Two-factor authentication: describes how to configure two-factor authentication.

7.6.1 Account Management

There are three default accounts: default administrator account **admin**, default auditor account **auditor**, and default maintenance account **maintainer**. They are described as follows:

- 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 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

Choose **System Management > User Management > User Management**. Click **Create**. In the **Create User** dialog box, set the account parameters and click **OK** to save the settings.

Table 7-19 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.
Authentication Mode	Login authentication mode of the account. • **Local**: indicates that accounts are authenticated only on WAF. • **RADIUS**: indicates that account authentication is performed via the RADIUS server. You must set RADIUS authentication parameters. For details, see RADIUS Server.
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 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. • **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**.

Editing an Account

The **admin** account can edit an account after it is created.

In the account list, click ✎ in the **Operation** column. In the dialog box, edit parameters and click **OK** to save the setting and return to the account list.

Note

- 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.

Deleting an Account

In the account list shown, click ⊗ in the **Operation** column. In the deletion confirmation dialog box, click **OK**.

The default **admin** account cannot be deleted.

Enabling/Disabling Accounts

By default, the default **admin** account is always enabled. You can enable/disabled created accounts.

- In the account list, click ▶ in the **Operation** column to enable an ccount. After it is enabled, its status turns to ✓.
- In the account list, click ■ in the **Operation** column to disable an account. After it is disabled, its status turns to ⛔.

Note

After first login as an **admin** account, **auditor** account, or **maintainer** account, users are required to change the default password.

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.

Choose **System Management** > **User Management** > **User Security**. In the dialog box, set the user security parameters. Click **OK** to save the settings.

Table 7-20 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.
Max Password Reuse Count	Specifies the maximum number of previous passwords that can be reused. By default, it is **2**.
Login Error Restriction	Controls whether to enable restrictions to login errors. After this parameter is set to **Enable**, you can choose account locking or IP locking. 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	Specifies the allowed login failures of login error restriction. • For account locking, specifies the number of consecutive login failures before an account is locked. • For IP locking, specifies the number of consecutive login failures before an IP address is locked.
Lockout Period (minute)	Specifies the lockout period of login error restriction. • For account locking: specifies the period during which an account is locked. • For IP locking: specifies 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.
Password Expiration Notification (day)	Specifies the number of days before password expiration when the system will start to send notifications.
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.

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. Set **Remote Assistance** to **Enable**, and configure up to three allowed IP addresses. Click **OK**. Then generate a password based on the displayed QR code and login key. Use the password to remotely log in to WAF and perform remote assistance.

7.6.4 RADIUS Server

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:

Choose **System Management** > **User Management** > **RADIUS Server**. On the **RADIUS Server** page, set the authentication parameters. Click **OK** to save the settings.

Table 7-21 Parameters for configuring authentication

Parameter	**Description**
Authentication Server	IP address of a RADIUS authentication server. Both IPv4 and IPv6 addresses are supported.
Authentication Method	Authentication method of a RADIUS authentication server, which can be **pap**, **spap**, **chap**, **mschapv1**, or **mschapv2**.
Authentication Port	Port on which the RADIUS authentication server listens for authentication requests. The default RADIUS authentication port is **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.

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. You can click 🔧 in the **Operation** column to unlock a user account. To unlock more than one user account, selectuser accounts and click **Unlock** to unlock them.

7.6.6 IP Unlocking

When the login error restriction is enabled, if an allowed IP is locked after too many login attempt failures, only an **admin** user can unlock the IP within the lockout period.

Choose **System Management** > **User Management** > **IP Unlocking**. Select one or more IP addresses and click **Unlock** to unlock them.

7.6.7 Two-Factor Authentication

WAF supports two-factor authentication which uses both the web login password and the certificate to authenticate user identities, thereby increasing the security of user authentication.

To configure two-factor authentication, perform the following steps:

Step 1 Choose **System Management** > **User Management** > **Two-Factor Authentication** and click **Download License** to download the certificate file **client.pfx**.

Step 2 Set **Enable Two-Factor Authentication** to **Yes** and click **OK**.

Step 3 After the web service is restarted, click ··· in the upper-right corner of the browser. Then click **Settings**. Then type **Certificate** in the search text box.

Step 4 Click **Security**. On the **Security** page, click the **Manage Certificates** area. On the displayed **Certificate** page, click **Import** to import the downloaded certificate file **client.pfx**. Then click **Next**.

Step 5 On the **Certificate Import Wizard** page, type the private key protection password (**123456** by default), and click **Next**. Then click **Next** and **Finish**.

Step 6 Log in to WAF again, and click **OK** in the **Select a Certificate for Authentication** dialog box. Then type your login user name and password to log in to WAF.

----End

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 the Traffic Control Function

Choose **System Management** > **Traffic Control Management**. 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.

Creating a Traffic Control Object

Prior to creating a traffic control object, you need to add websites or domain names for such websites on the **Website Group Management** page. For details, see Adding a Website. Traffic control objects include domain names and websites. A domain name or website can be included only in one traffic control object. When available domain names or websites are used up, you cannot create more traffic control objects. The following describes how to create a traffic control object of domain names. The method of creating a traffic control object of websites is similar and is omitted.

To create a traffic control object of domain names, follow these steps:

Click **New (domains)** on the **Traffic Control Management** page. In the dialog box, set the traffic control object parameters. Click **Save** to save the settings.

Table 7-22 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 in-path, out-of-path, or reverse proxy mode.

Editing a Traffic Control Object

On the **Traffic Control Management** page, click ✎ in the **Operation** column to edit its parameters (including **Object Name**). Click **Save** to save the setting and return to the **Traffic Control Management** page.

Deleting Traffic Control Objects

You can delete traffic control objects as follows:

- On the **Traffic Control Management** page, click ✖ in the **Operation** column and then click **OK** in the confirmation dialog box to delete a traffic control object.
- On the **Traffic Control Management** page, 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 Management** page, 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 Management** page, 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 Management** page, 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 Management** page, 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.

Rejecting New Connection Requests After Traffic Control

On the **Traffic Control Management** page, select the **Close new connection after traffic control** check box and click **OK** in the confirmation dialog box to enable this function.

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 Email Sending Configuration

Before using scheduled reports and the license expiration email notification service, you need to perform email sending configuration.

Choose **System Management** > **Email Sending Configuration** and configure email sending settings. Then click **OK**.

Table 7-23 describes parameters for configuring the email sending service.

Table 7-23 Parameters for configuring the email sending service

Parameter	Description
Server IP Address	Email server address, which can be an IPv4 address, an IPv6 address, or a domain name. The email server only supports SMTP for sending emails.
Server Port	Email server port, ranging from 1 to 65535.
Sender Email	Email address that sends reports or notifications.
Authorization Code	A special password used to log in to third-party email clients, which is used for authentication and is not the sender's login password.

7.9 System Parameter Configuration

System parameters include engine parameters, a kernel parameter, bridge mode parameters, and other parameters.

7.9.1 Engine Parameter

After a successful login to WAF, the **maintainer** user can configure engine parameters. For information about the **maintainer** account, see Default Accounts.

To configure the engine parameters, perform the following steps:

Choose **System Management** > **System Parameter Configuration** > **Engine Parameters**. Configure engine parameters which are presented and described on the **Engine Parameters** page. Then commit the settings.

- Click **OK** to dispatch the engine parameter settings to the engine. Note that restarting the engine will restore the engine parameter settings to the defaults.
- Click **Persist** to the save engine parameter configuration to the engine configuration file and then dispatch the settings to the engine. In this case, these settings can still take effect after the engine is restarted.

For detailed parameter description, please contact technical support personnel of NSFOCUS.

7.9.2 Kernel Parameter

After a successful login to WAF, the **maintainer** user can configure kernel parameters. 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.

Choose **System Management > System Parameter Configuration > Kernel Parameter**. Set **TCP Timestamp** to **Enable**. Commit the settings.

- 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 timestamp is enabled permanently.

7.9.3 Other Parameters

After a successful login to the system, the **maintainer** user can configure China's state cryptography mode (only available for customers in China), NIC multi-queue, and dynamic protection policy.

For information about the **maintainer** account, see Default Accounts.

> **Note**
>
> You can enable either state cryptography or SSL acceleration, but cannot enable both. To use state cryptography, you must disable SSL acceleration if it is already enabled.

7.9.3.1 State Cryptography Mode

Choose **System Management** > **System Parameter Configuration** > **Other Parameters**. Then enable or disable the state cryptography mode as required. Click **OK** to save the settings.

The state cryptography mode is disabled by default. Users outside China are advised to leave this parameter at its default value.

> **Note**
>
> The certificate and the protocol of websites must be configured again once the WAF deployment mode is changed.
>
> For a website that uses China's state cryptography only, disabling the state cryptography mode will make the website unavailable, affecting service continuity.

7.9.3.2 NIC Multi-Queue

Choose **System Management** > **System Parameter Configuration** > **Other Parameters**. Then enable or disable the NIC multi-queue as required. Click **OK** to save the settings.

7.9.3.3 Dynamic Protection Policy

Choose **System Management** > **System Parameter Configuration** > **Other Parameters**. Then enable or disable the dynamic protection policy as required. Click **OK** to save the settings.

7.9.3.4 Memory Optimization

After login to WAF as a **maintainer** account, choose **System Management** > **System Parameter Configuration** > **Other Parameters** to enable memory optimization. You can set the maximum number of connections handled each time.

Memory optimization is enabled by default. After it is enabled, the engine enters memory acceleration mode, which significantly improves processing performance and stability.

7.9.4 Bridge Mode Parameter

Bridge mode parameters are available only on WAF deployed in transparent bridge mode. After login to WAF as a **maintainer** user, you can configure bridge mode parameters.

Choose **System Management** > **System Parameter Configuration** > **Bridge Mode Parameters** to configure bridge mode parameters.

Table 7-24 Parameters for configuring the transparent bridge mode

Parameter	**Description**
max_tcpsession_single_class	Specifies the maximum number of TCP sessions supported by a single client.
flow_hash_buckets_num	Specifies the concurrent TCP session threshold of the server. The default value is **4000000**. The number of entries in the server's flow table must not be smaller than the threshold.
tcpsession_prune_quanta	Sets the timeout value for a TCP session.
tcpsessionest_prune_quanta	Sets the timeout value for an established TCP session.
Tcp_stream_reass_max_queued_sessions	Specifies the maximum number of TCP sessions that can be converged. 0 indicates that there is no limit. The default value is **100000**.

7.10 System O&M

After a successful login to the system, the **maintainer** account can collect information about the system and restore the system. For information about the **maintainer** account, see Default Accounts.

Information Collection

To collect information about the system, choose **System Management > System O&M**. Click **Start** to collect device-related information for exception cause analysis and troubleshooting.

- Click ⬇ in the **Operation** column of a file to download it to a local disk drive.
- Click ✖ in the **Operation** column of a file to delete it.

System Restoration

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.
- **Datacom engine:** Click **Restart Datacom Engine** to restart the datacom engine.
- **Console password:** Click **Reset Console Port Password** to reset the console port password.

Note	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.

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 Default Accounts.

7.11.1 Digital Signature Parameters

Choose **System Management** > **REST API** > **Digital Signature Parameters**. Then enable digital signature V1 and/or V3, and set the API request timeout. Click **OK** to save the settings.

7.11.2 REST Listening Port

Choose **System Management** > **REST API** > **REST Listening Port**. Then type the listening port number or use the default port number of **8443**. Click **OK** to save the settings.

7.11.3 API Service Control

API service control indicates whether to enable the API service. After enabling the API service, you need to change the default API password.

Note	API service control is disabled by default. You need to change the default API password before enabling API service control.

7.11.4 API Password Change

The maintainer can change the password for use of the API service.

Choose **System Management** > **REST API** > **REST API Change Password**. Type a new password in the **Reset Password** text box. Click **OK** to save the settings.

Note that the password must consist of eight or more characters of at least three of the following types: special characters, uppercase letters, lowercase letters, and digits.

7.12 Site Control

After successful login to the system, the **maintainer** user can configure WAF to support HTTPS websites.

After the HTTPS website switch is turned on, you can create HTTPS websites and manage SSL certificates on WAF.

Choose **System Management** > **Site Control**. On the **Site Control** page, click **Enable** to turn on support for HTTPS websites.

8 API Protection

WAF provides protection for third-party API assets. The API security protection feature helps customers sort out API assets more efficiently and conduct API security compliance checks based on automatically generated API baselines and imported OAS files. WAF can parse multiprotocol traffic, filter attack traffic, and correlate malicious attack behavior analysis to ensure normal access of legitimate users.

This chapter describes how to configure API security protection, covering the following topics:

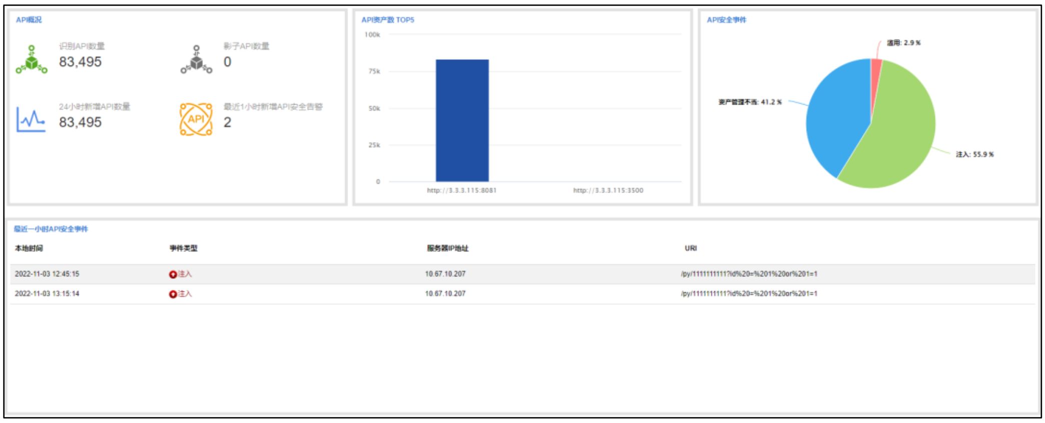
Topic	Description
API Overview Page	Introduces the API overview page.
API Management	Describes how to import and learn API assets, manage API lists, and configure allowlists and suspicious lists.
OAS File Management	Describes how to import OAS files.
API Protection Logs	Describes how to view API protection logs.

8.1 API Overview Page

The **API Overview** page visualizes the overall security situation of third-party APIs, including the statistics of identified APIs, shadow APIs, new APIs in the last 24 hours, top 5 API assets, API security events, and API security events in the last 1 hour. This provides customers intuitive and comprehensive insight into the API security situation.

Choose **API Security** > **Overview** to view the overall API security situation.

Figure 8-1 API overview page



本地时间	事件类型	服务器IP地址	URI
2022-11-03 12:45:15	注入	10.67.10.207	/py/1111111111?id%20=%201%20or%201=1
2022-11-03 13:15:14	注入	10.67.10.207	/py/1111111111?id%20=%201%20or%201=1

API security events are classified into the following risk levels:

- : indicates low-risk events.
- : indicates medium-risk events.
- : indicates high-risk events.

Click a real-time event in the **Event Type** column of the API security event list in the latest 1 hour to view the details of event alerts. The log details are the same as those displayed in the security protection logs.

Table 8-1 describes the API security event types.

Table 8-1 API security event types

Event Type	Description
Abuse	Includes JS related, account takeover, and CSRF.
Sensitive data exposure	Includes sensitive information disclosure, crawler protection, information leak protection, and illegal download.
No rate limiting	Includes brute-force cracking and scanning protection.
API protocol violation	Includes HTTP protocol validation and XML protocol validation.
Security misconfiguration	Includes web server/plug-in protection.
Injection	Includes web universal protection, semantic analysis engine, and star absorption.
Improper asset management	Includes shadow APIs.
Custom policy	Includes custom policies.
Compliance verification	Includes compliance policies.

8.2 API Management

API management includes API learning, managing API lists and shadow lists, and configuring allowlists and suspicious lists.

8.2.1 API Assets

Users can manually import APIs in bulk, or enable the API learning function to learn APIs, thus generating an API asset baseline. After API learning is enabled, WAF will automatically learn new APIs and update the API asset baseline.

API Learning Control

Note

Before using API learning, you need to enable API security for a website group first.

Choose **Security Management** > **Website Protection**, and click ▶ in the **Operation** column of a website group to enable API security.

Choose **API Security**> **API Management**, and select a website group. On the **API Asset** tab page, click **Yes** or **No** in the **API learning control** section to enable or disable API learning.

After being enabled, API learning will be automatically disabled after 7x24 hours by default.

Importing APIs for the Root Website Group

Choose **API Security** > **API Management**. Then click ⬆ in the upper-right of the website group tree and select a desired API import file to bulk import APIs for the **Root** website group.

APIs imported in bulk automatically fall into the corresponding website groups. The import result takes effect after the confirmation.

Note

- If an allowlist is configured, only imported API assets that do not match the API allowlist are added to the API list.
- If a suspicious list is configured, only imported API assets that match the suspicious list are added to the API list.
- If the allowlist and the suspicious list are both configured, the allowlist takes precedence over the suspicious list, and only imported APIs that match the suspicious list and do not match the allowlist at the same time are added to the API list.

Note

On the **Import APIs** page, click the **example_en.xlsx** file to download the import template and manually fill in API information.

Table 8-2 describes parameters for creating an API import file.

Table 8-2 Parameters for creating an API import file

Parameter	Description
Website Group ID	Website group ID.
Learning Time	Time the API is learned.
Protocol Type	Protocol used by the API. It can be HTTP or HTTPS.
Domain Name	API domain name.
URI	API URI path.
Learning Mode	API learning mode. It can be auto or manual import.
CONTENT_TYPE	Type of data content sent by the API request.
Method	Request method.
Website Group Name	Name of the website group to which the API belongs.
Website ID	ID of the website to which the API belongs.
Website Name	Name of the website to which the API belongs.
Server IP	Server IP address.
Service Port	Service port number.

Importing APIs for a Website Group

Choose **API Security** > **API Management**, select a website group in the website group tree, and click **API Asset**. In the **API Import** section, click **API Import** to select a desired API asset file for importing new APIs.

Note

- If an allowlist is configured, only imported APIs that do not match the allowlist are added to the API list.
- If a suspicious list is configured, only imported APIs that matches the suspicious list are added to the API list.

Viewing APIs

Choose **API Security** > **API Management**, select a website group, and click the **API Asset** tab. In the **API asset** list, type query conditions to query the matched APIs.

The API asset list is displayed by website group. In each website group, the API list is organized by domain name. WAF offers statistics on APIs of each website group and on APIs under each domain name in a website group.

8.2.2 API List

Choose **API Security** > **API Management**, select a website group, click **API List**, and then type query conditions to view the matched APIs.

Table 8-3 describes the API parameters in the API list.

Table 8-3 API parameters in the API list

Parameter	**Description**
Learning Time	Time an API is learned.
Protocol Type	Protocol used by the API.
Domain Name	API domain name.
URI	API URI path.
CONTENT_TYPE	Type of data content sent by the API request.
Learning Mode	API learning mode. It can be **Auto** or **Manual import**.
Method	Request method.

You can perform the following operations on APIs in the API list.

- Click 📤 to export the API query result, which is a CSV file in .xlsx format.
- Click 🗑 to bulk delete selected APIs in the API list.
- Click 🔍 to view the API details.
- Click ✖ to delete the API.
- Click ↗ to jump to the API protection log.
- Click ➕ to add the API to the allowlist.
  Note: After being added to the allowlist, the API will not be automatically deleted from the API list. You need to manually delete it.

8.2.3 Shadow API List

Shadow APIs refer to those that are used by enterprises, but live outside the normal IT governance management and security processes. When API security is enabled for a website group, but API learning control is disabled, the APIs learned by WAF are added to the shadow list.

Choose **API Security** > **API Management**, select a website group, click the **Shadow API List** tab, and then type query conditions to view the matched API assets.

Table 8-4 describes shadow API parameters.

Table 8-4 Shadow API asset parameters

Parameter	Description
Learning Time	Time an API is learned.
Protocol Type	Protocol used by the API. It can be HTTP or HTTPS.
Domain Name	API domain name.
URI	API URI path.
CONTENT_TYPE	Type of data content sent by the API request.
Learning Mode	API learning mode. It can be auto or manual import.
Method	Request method.

You can perform the following operations on shadow APIs in the shadow API list.

- Click 🔍 to view the API details.
- Click ⊗ to delete the shadow API.
- Click ⊕ and click **Add to allowlist** to add the API to the allowlist.
  After being added, the API is automatically deleted from the shadow list.
- Click ⊕ and click **Add to API list** to add the API to the API list.
  After being added, the API is automatically deleted from the shadow list.
- Choose one or more shadow APIs and click **Bulk Add to Allowlist** to add them to the allowlist.
- Choose one or more shadow APIs and click **Bulk Add to API List** to add them to the API list.
- Choose one or more shadow APIs and click **Bulk Delete** to delete them.

8.2.4 Allowlist

The allowlist is configured by website group. APIs that match the allowlist of a website group are not added to the API list and will not be managed.

Choose **API Security** > **API Management**, select a website group, click the **Allowlist** tab, and click **Add** to create a new allowlist.

Table 8-5 describes parameters for creating an allowlist.

Table 8-5 Parameters for creating an allowlist

Parameter	Description
Domain Name	API domain name.
URI	API URI path.

You can perform the following operations on APIs in the allowlist.

- Click ✎ to edit the API in the allowlist.
- Click ✖ to delete the API in the allowlist.

8.2.5 Suspicious List

The suspicious list determines what API assets are to be learned by WAF. The suspicious list is configured by website group. Allowlists take precedence over suspicious lists.

If a website group is configured with a suspicious list, WAF identifies APIs only against the suspicious list. Identified APIs that do not match the allowlist are added to the API list.

If the website group is configured with an allowlist and not configured with a suspicious list, WAF will identify all API requests and add those that do not match the allowlist to the API list.

Choose **API Security** > **API Management**, select a website group, then click the **Suspicious List** tab, and click **Add** to create a new suspicious list.

Table 8-6 describes parameters for creating a suspicious list.

Table 8-6 Parameters for creating a suspicious list

Parameter	**Description**
Domain Name	API domain name.
URI	API URI path.

You can perform the following operations on APIs in the suspicious list.

- Click ✎ to edit the API in the suspicious list.
- Click ✖ to delete the API in the suspicious list.

8.3 OAS File Management

Open API Specification (OAS) files are used for API compliance verification. After an imported OAS file is associated with API compliance policies and applied to a website, API compliance verification takes effect. WAF supports custom OAS files in .yaml format. You can download the sample OAS file and edit it for use.

8.3.1 Downloading the Sample OAS File

Choose **API Security** > **OAS File Management**. In the OAS file list, click **Sample File** to download the sample file.

8.3.2 Uploading the OAS File

Choose **API Security** > **OAS File Management**, click **Upload OAS File**, and select the desired OAS file. Click **OK**.

In the OAS file list, you can download and delete uploaded OAS files.

Select multiple OAS files, click **Bulk Delete**, and after confirmation you can delete the OAS files in bulk.

8.4 API Protection Logs

Choose **API Security** > **API Protection Log**, and you can view the list of API protection logs. Type query conditions to view matched API protection logs. For more information about security logs, see API Protection Logs.

9 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.

9.1 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)

Note There are certain requirements for the encryption algorithm used in the terminal software. In case of connection failure, a later version of the terminal software is required.

- Proper connection between WAF and the computer

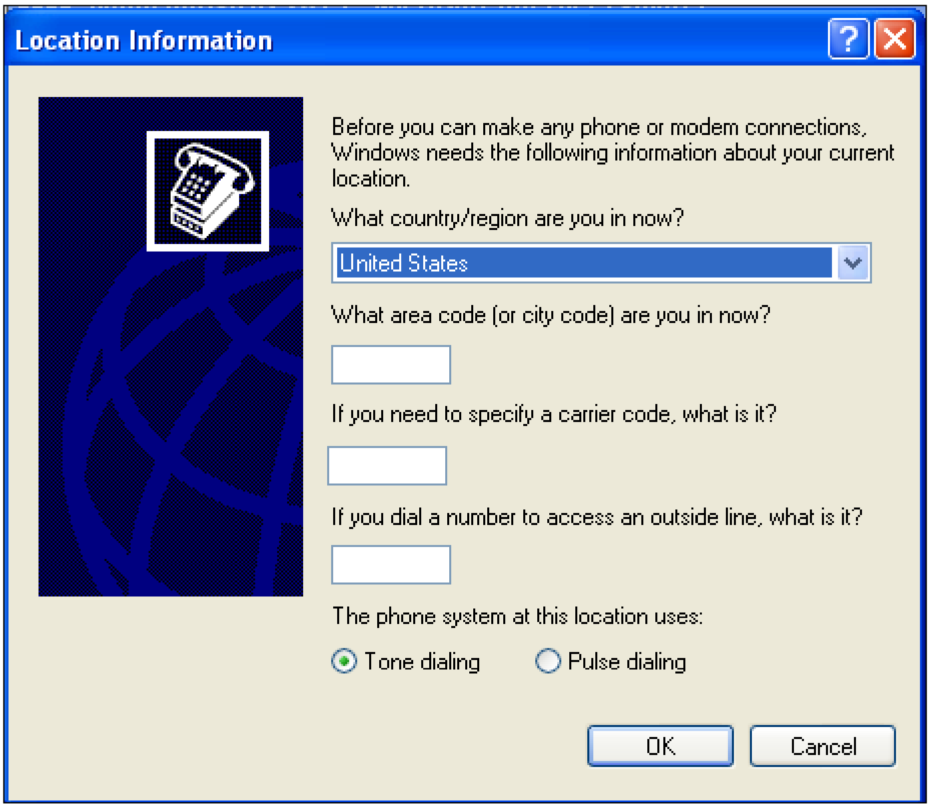
The following uses the HyperTerminal software included in Microsoft Windows XP as an example to describe how to log in to the console:

Step 1 On the computer, choose **Start** > **Programs** > **Accessories** > **Communications** > **Hyper Terminal**.

- If the **Location Information** dialog box shown in Figure 9-1 appears, click **Cancel**. The **Connection Description** dialog box shown in Figure 9-2 appears. Go to Step 2.

- If the **Connection Description** dialog box shown in Figure 9-2 appears, go to Step 2.

Figure 9-1 Location Information dialog box



Location Information

Before you can make any phone or modem connections, Windows needs the following information about your current location.

What country/region are you in now?

United States

What area code (or city code) are you in now?

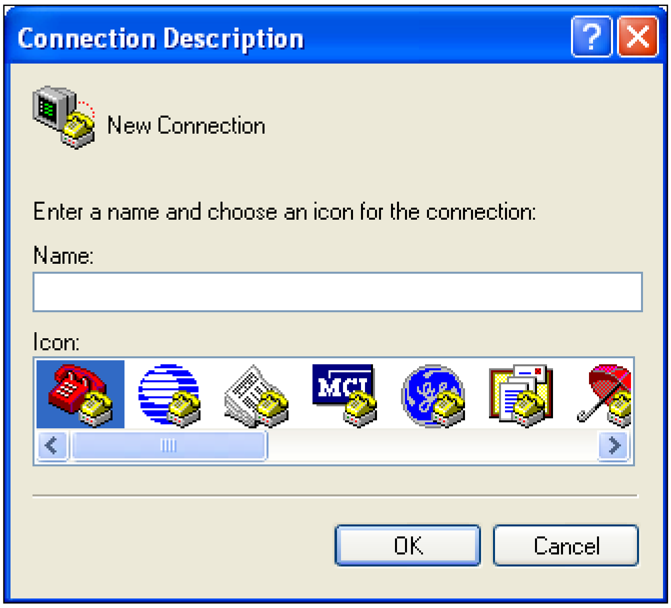
If you need to specify a carrier code, what is it?

If you dial a number to access an outside line, what is it?

The phone system at this location uses:

● Tone dialing ○ Pulse dialing

Figure 9-2 Connection Description dialog box



Connection Description

New Connection

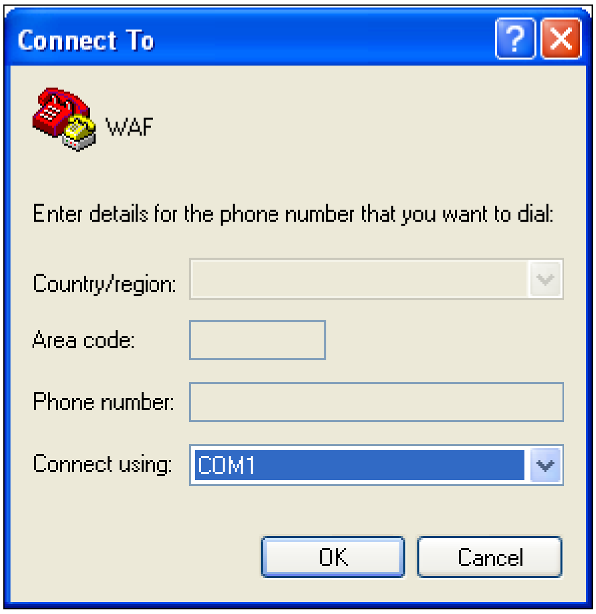
Enter a name and choose an icon for the connection:

Name:

Icon:

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 9-1 appears. Click **Cancel** and then **OK**. The **Connect to** dialog box appears, as shown in Figure 9-3.

Figure 9-3 Connect to dialog box



Enter details for the phone number that you want to dial:

Country/region:

Area code:

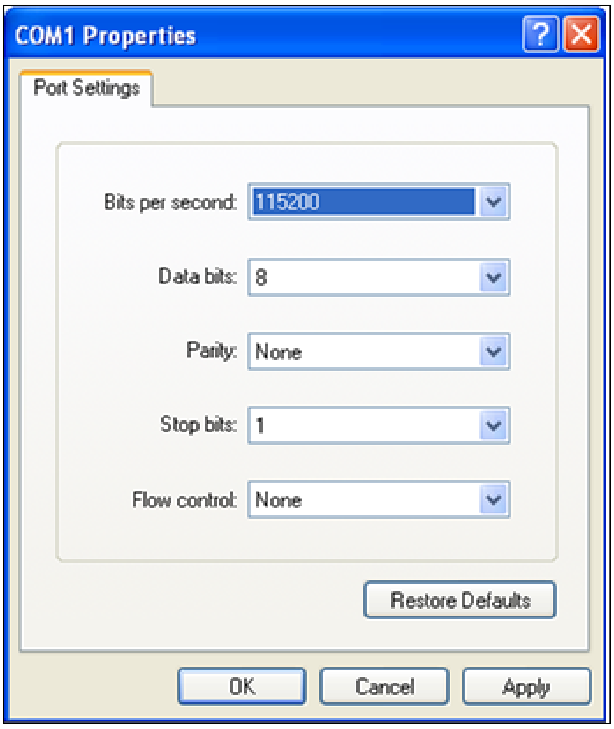
Phone number:

Connect using: COM1

Step 3 Select a serial port (**COM1** for example) and click **OK**.

The **COM1 Properties** dialog box appears, as shown in Figure 9-4.

Figure 9-4 COM1 Properties dialog box



Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

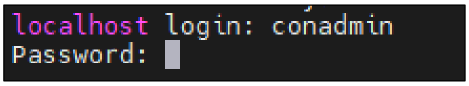
Flow control: None

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 **conadmin**) 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 9-5 Login page



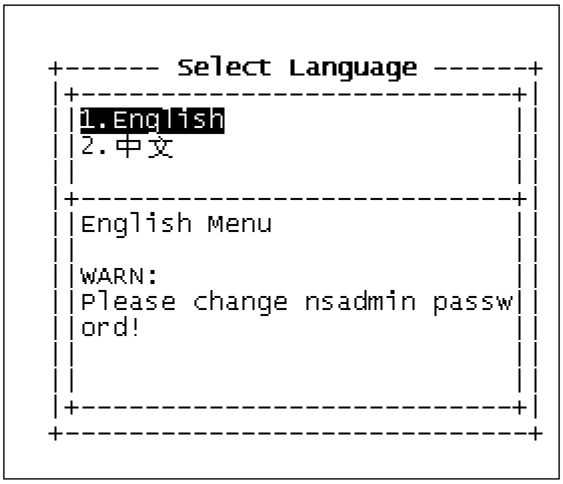
```
localhost login: conadmin
Password:
```

Note

Upon first login through the console port, users are required to change the default password. The new password must be at least eight characters in length and contain only upper-case letters, lower-case letters, and digits, and cannot contain special characters.

After login, the language selection window appears, as shown in Figure 9-6.

Figure 9-6 Language selection window

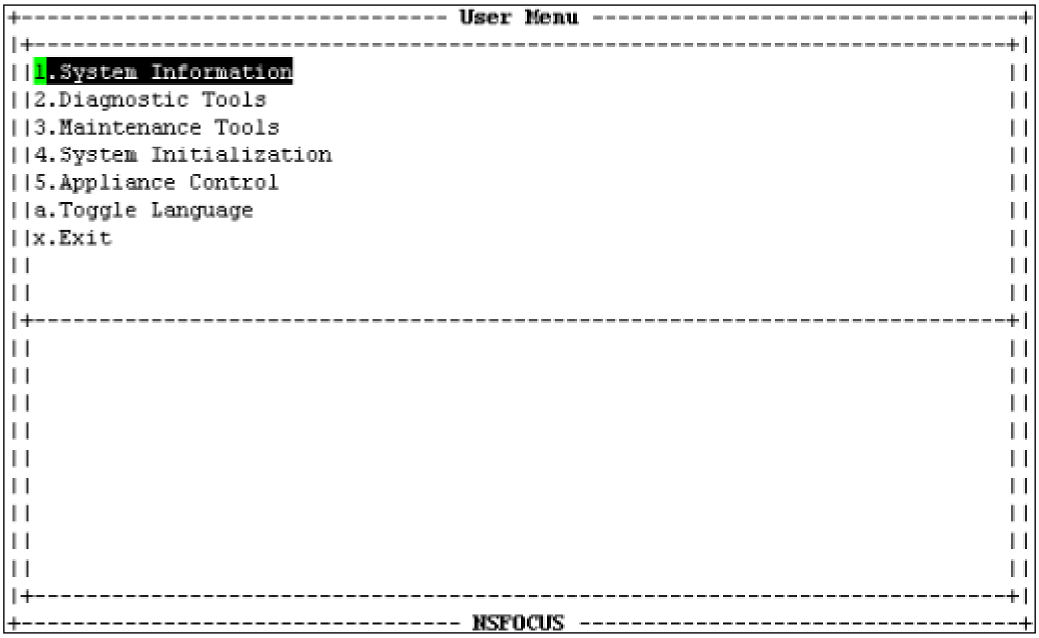


```
+------ Select Language ------+
|+---------------------------+|
||1.English                  ||
||2.中文                     ||
||                           ||
|+---------------------------+|
||English Menu               ||
||                           ||
||WARN:                      ||
||Please change nsadmin passw||
||ord!                       ||
||                           ||
||                           ||
|+---------------------------+|
+-----------------------------+
```

Step 6 Select **1. English** and press **Enter**.

The **User Menu** window appears, as shown in Figure 9-7.

Figure 9-7 User Menu window



```
+-------------------------------- User Menu --------------------------------+
|+-------------------------------------------------------------------------+|
||1.System Information                                                     ||
||2.Diagnostic Tools                                                       ||
||3.Maintenance Tools                                                      ||
||4.System Initialization                                                  ||
||5.Appliance Control                                                      ||
||a.Toggle Language                                                        ||
||x.Exit                                                                   ||
||                                                                         ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
+--------------------------------- NSFOCUS ---------------------------------+
```

Note	The console menu commands can only be executed using the keyboard. For the meaning of keys, see Table 9-1.

Table 9-1 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

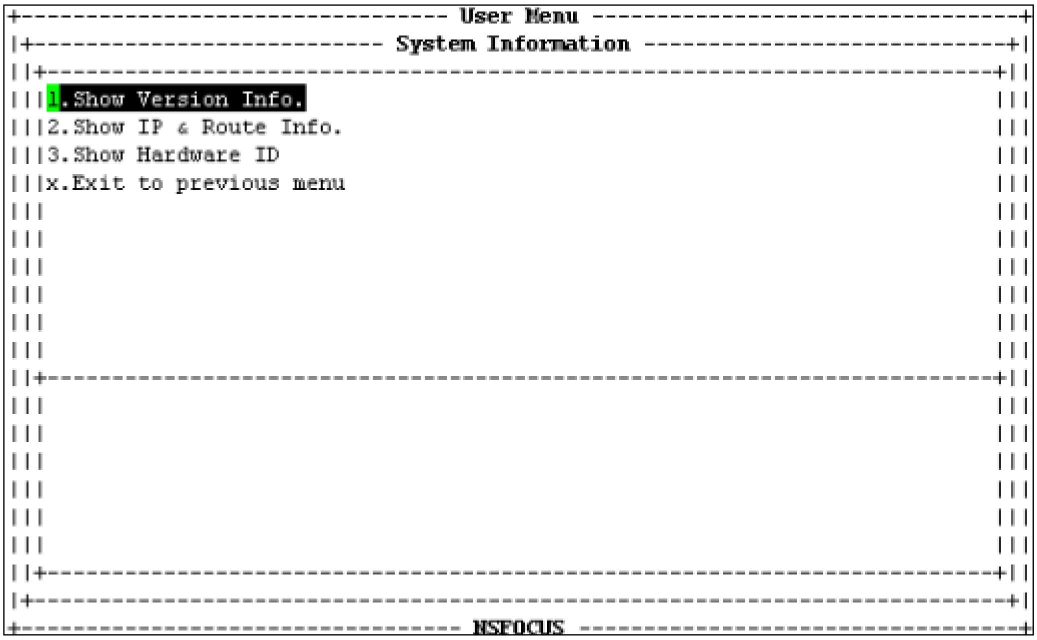
9.2 Console Functions

The following describes functions and operations on the console menu of WAF.

9.2.1 System Information

In the **User Menu** window shown in Figure 9-7, move the cursor to **System Information** and press **Enter**. The **System Information** window appears, as shown in Figure 9-8.

Figure 9-8 System Information window



```
+-------------------------------- User Menu --------------------------------+
|+--------------------------- System Information ---------------------------+|
||+----------------------------------------------------------------------+||
|||1.Show Version Info.                                                  |||
|||2.Show IP & Route Info.                                               |||
|||3.Show Hardware ID                                                    |||
|||x.Exit to previous menu                                               |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
||+----------------------------------------------------------------------+||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
||+----------------------------------------------------------------------+||
|+------------------------------------------------------------------------+|
+--------------------------------- NSFOCUS ---------------------------------+
```

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.

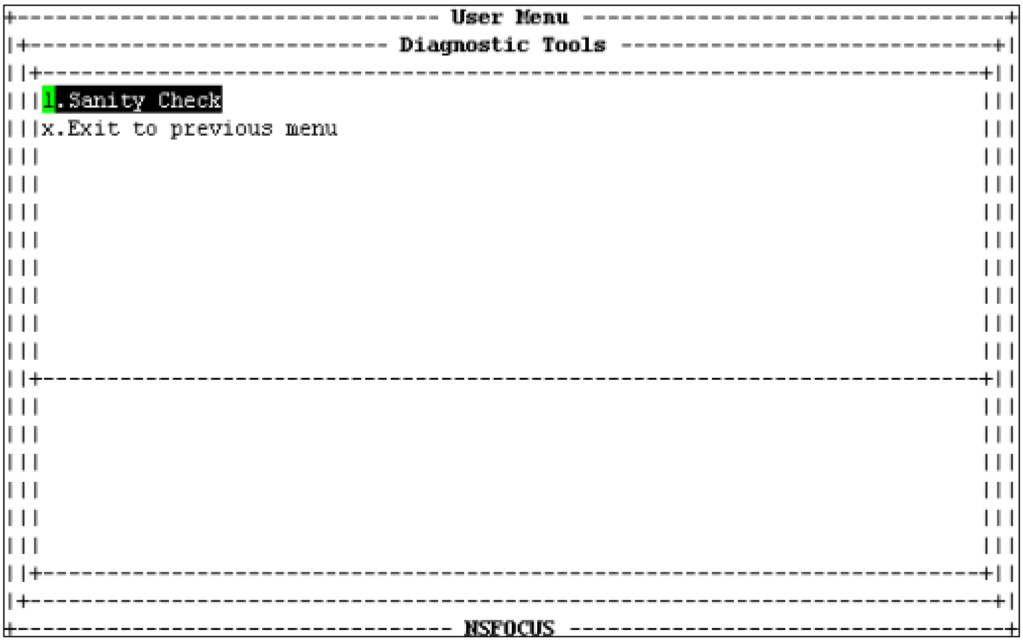
Note

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 License.

9.2.2 Diagnostic Tools

In the **User Menu** window shown in Figure 9-7, move the cursor to **System Diagnosis** and press **Enter**. The **Diagnostic Tools** window appears, as shown in Figure 9-9.

Figure 9-9 Diagnostic Tools window



```
+---------------------------------- User Menu ---------------------------------+
|+---------------------------- Diagnostic Tools -----------------------------+|
||+-----------------------------------------------------------------------+||
|||1.Sanity Check                                                         |||
|||x.Exit to previous menu                                                |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
||+-----------------------------------------------------------------------+||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
||+-----------------------------------------------------------------------+||
|+-------------------------------------------------------------------------+|
+----------------------------------- NSFOCUS ----------------------------------+
```

The **Diagnostic Tools** window provides the following functions:

- Sanity Check

  Checks whether hardware and software modules are normal on WAF.

- Exit to previous menu

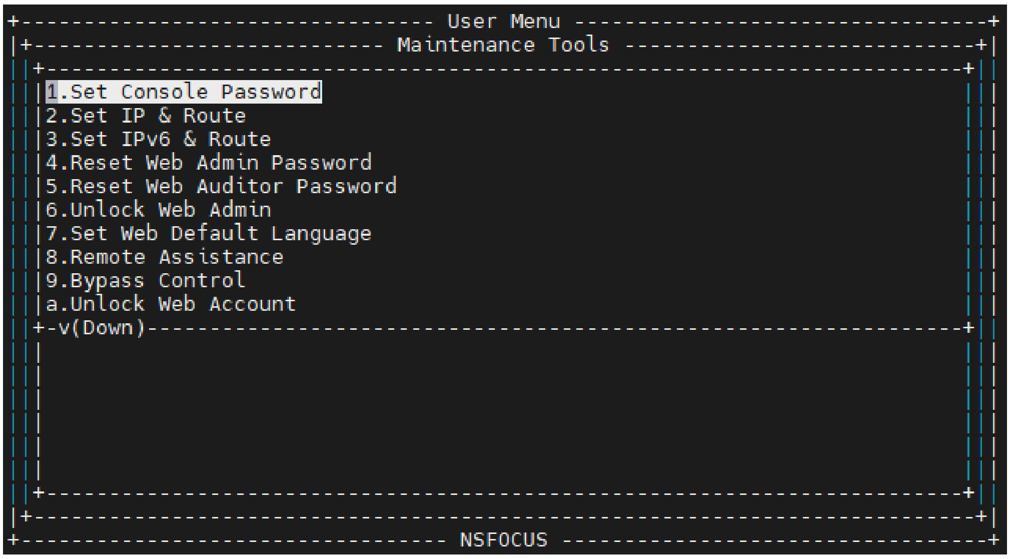
  Returns to the previous menu.

Note	You can also use diagnostic tools in the web-based manager of WAF.

9.2.3 Maintenance Tools

In the **User Menu** window shown in Figure 9-7, move the cursor to **Maintenance Tools** and press **Enter**. The **Maintenance Tools** window appears, as shown in Figure 9-10.

Figure 9-10 Maintenance Tools window



```
+-------------------------------- User Menu --------------------------------+
|+--------------------------- Maintenance Tools ---------------------------+|
||+---------------------------------------------------------------------+||
|||1.Set Console Password                                                |||
|||2.Set IP & Route                                                      |||
|||3.Set IPv6 & Route                                                    |||
|||4.Reset Web Admin Password                                            |||
|||5.Reset Web Auditor Password                                          |||
|||6.Unlock Web Admin                                                    |||
|||7.Set Web Default Language                                            |||
|||8.Remote Assistance                                                   |||
|||9.Bypass Control                                                      |||
|||a.Unlock Web Account                                                  |||
||+-v(Down)-------------------------------------------------------------+||
|||                                                                     |||
|||                                                                     |||
|||                                                                     |||
|||                                                                     |||
|||                                                                     |||
|||                                                                     |||
||+---------------------------------------------------------------------+||
|+-------------------------------------------------------------------------+|
+--------------------------------- NSFOCUS ---------------------------------+
```

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.
- Unlock Web Account

  Unblocks all accounts (including **admin**) that are blocked.
- Apache Management

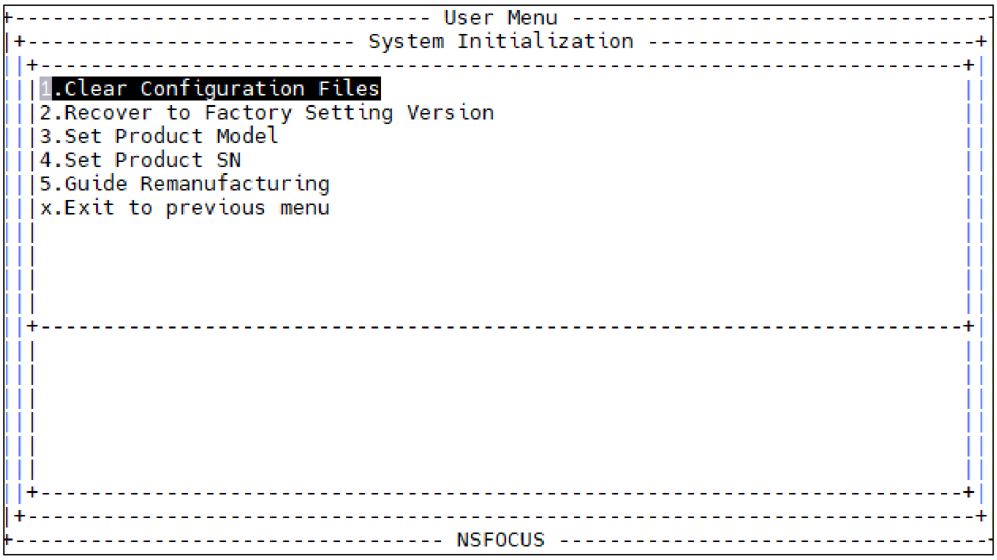
  Sets the HTTPS port used to log in to the web-based manager. The default port is port 443.
- Exit to previous menu

  Returns to the previous menu.

9.2.4 System Initialization

In the **User Menu** window shown in Figure 9-7, move the cursor to **System Initialization** and press **Enter**. The **System Initialization** window appears, as shown in Figure 9-11.

Figure 9-11 System Initialization window



```
+--------------------------------- User Menu ---------------------------------+
|+------------------------- System Initialization --------------------------+|
||+----------------------------------------------------------------------+||
|||1.Clear Configuration Files                                           |||
|||2.Recover to Factory Setting Version                                  |||
|||3.Set Product Model                                                   |||
|||4.Set Product SN                                                      |||
|||5.Guide Remanufacturing                                               |||
|||x.Exit to previous menu                                               |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
||+----------------------------------------------------------------------+||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
|||                                                                      |||
||+----------------------------------------------------------------------+||
|+--------------------------------------------------------------------------+|
+---------------------------------- NSFOCUS ----------------------------------+
```

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.

- Guide Remanufacturing

  Guides device remanufacturing through the console interface in DHCP, ST, or USB manufacturing mode.

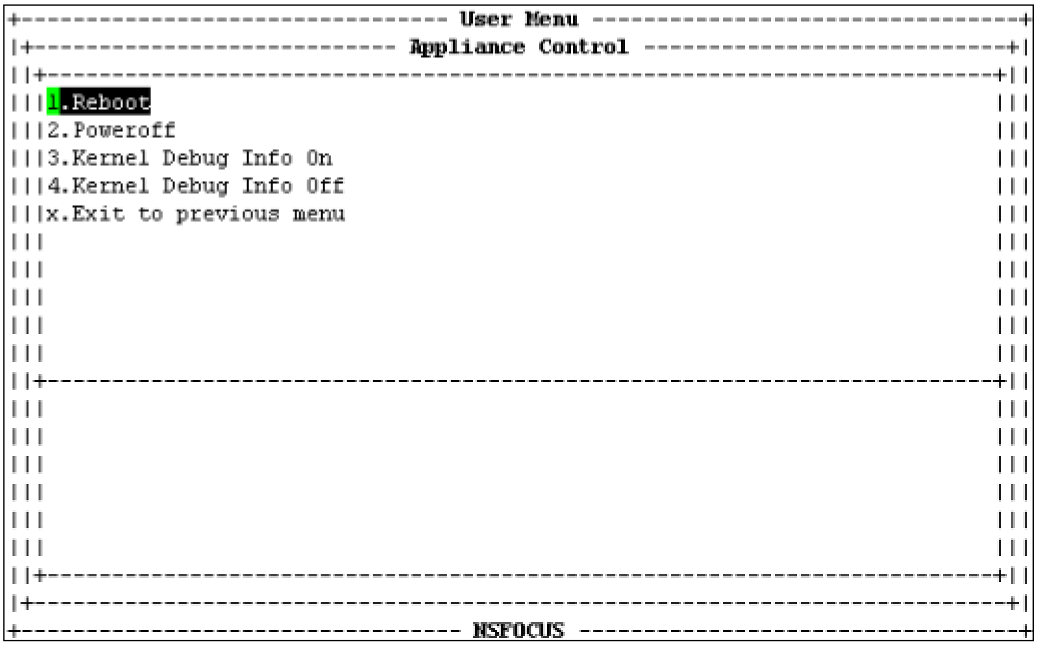
- Exit to previous menu

  Returns to the previous menu.

9.2.5 Appliance Control

In the **User Menu** window shown in Figure 9-7, move the cursor to Appliance Control and press **Enter**. The **Appliance Control** window appears, as shown in Figure 9-12.

Figure 9-12 Appliance Control window



```
+-------------------------------- User Menu --------------------------------+
|+--------------------------- Appliance Control ---------------------------+|
||+-----------------------------------------------------------------------+||
|||1.Reboot                                                               |||
|||2.Poweroff                                                             |||
|||3.Kernel Debug Info On                                                 |||
|||4.Kernel Debug Info Off                                                |||
|||x.Exit to previous menu                                                |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
||+-----------------------------------------------------------------------+||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
|||                                                                       |||
||+-----------------------------------------------------------------------+||
|+-------------------------------------------------------------------------+|
+--------------------------------- NSFOCUS ---------------------------------+
```

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.

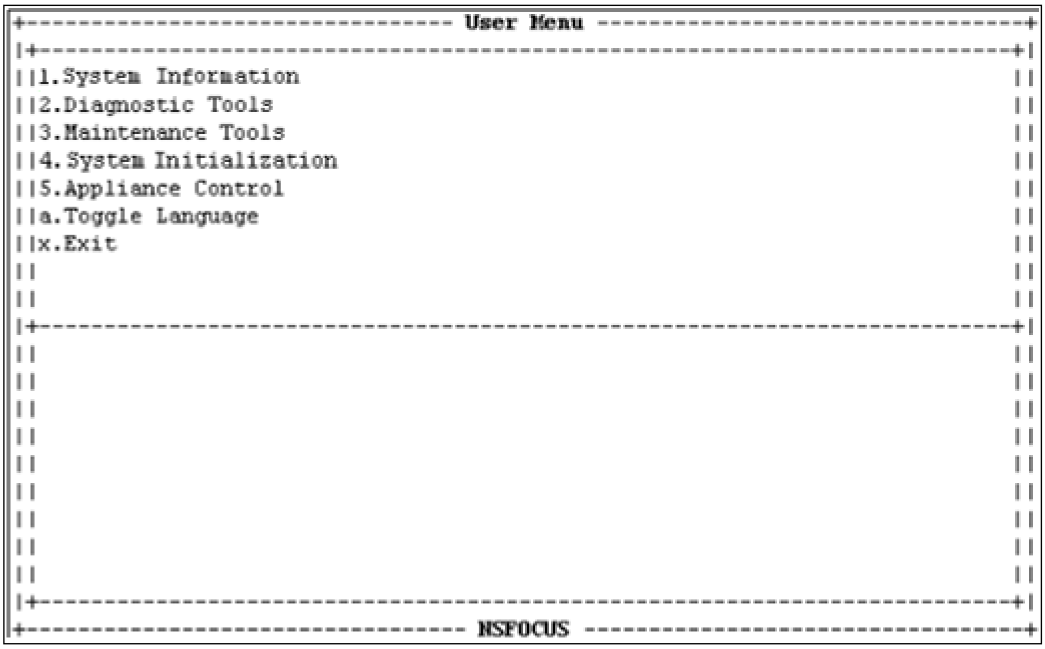
- Exit to previous menu

  Returns to the previous menu.

9.2.6 **Toggle Language**

In the **User Menu** window shown in Figure 9-13, move the cursor to **Toggle Language** and press **Enter** to switch the language between Chinese and English.

Figure 9-13 Toggling language



```
+-------------------------------- User Menu --------------------------------+
|+-------------------------------------------------------------------------+|
||1.System Information                                                      ||
||2.Diagnostic Tools                                                        ||
||3.Maintenance Tools                                                       ||
||4.System Initialization                                                   ||
||5.Appliance Control                                                       ||
||a.Toggle Language                                                         ||
||x.Exit                                                                    ||
||                                                                          ||
||                                                                          ||
|+-------------------------------------------------------------------------+|
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
|+-------------------------------------------------------------------------+|
+--------------------------------- NSFOCUS ---------------------------------+
```

9.2.7 **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	Admin123!@#
Web Auditor	auditor	Auditor123!@#
System Maintainer	maintainer	Maintainer123!@#
Console Administrator	conadmin	conadmin

A.3 Console Port Communication Settings

Bits per Second	115200
Data Bits	8
Parity	None
Stop Bits	1
Data 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.)
[*any characters***]**	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.
[^*any character***]**	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: • **i**: case-insensitive (off by default) • **m**: multi-line mode (off by default) • **s**: line feed included (off by default)

Symbol	Description
	• **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)$