
NSFOCUS WAF V6.0

Configuration Guide



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

© 2020 NSFOCUS

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

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

Contents

Preface	1
Scope.....	1
Audience	1
Organization.....	1
Conventions	2
Customer Support.....	2
1 Configuring Websites	3
1.1 Quick Mode.....	3
1.2 Guide Mode.....	7
1.2.1 Configuring an HTTP Website	7
1.2.2 Configuring an HTTPS Website.....	12
1.3 Creating a Virtual Website.....	15
2 Configuring Policies.....	18
2.1 Configuration Example of Auto-Learning Policies	18
2.2 Configuration Examples of Web Security Protection Policies	21
2.2.1 Whitelist Policy	21
2.2.2 CSRF Protection Policy	23
2.2.3 Leech Protection Policy	31
2.2.4 Cookie Security Protection Policy	34
2.2.5 Brute Force Protection Policy	38
2.2.6 XML Attack Protection Policy	46
2.2.7 Smart Engine Inspection Policy	49
2.2.8 IP Reputation Policy	52
2.3 Configuration Example of Smart Patches	55
3 Connecting to Other NSFOCUS Devices	61
3.1 Connecting to NSFOCUS ESPC.....	61
3.2 Connecting to NSFOCUS ADS.....	64
A Exporting the HTTPS Certificate	70
B Default Parameters.....	72
B.1 Default Settings of the Management Interface	72
B.2 Default Accounts	72
B.3 Communication Parameters of the Console Port	72

Figures

Figure 1-1 Quick mode — typical deployment topology	3
Figure 1-2 Quick mode — Website Group Mgmt page.....	4
Figure 1-3 Quick mode — creating a website group.....	4
Figure 1-4 Quick mode — entering the website group name	5
Figure 1-5 Quick mode — viewing web security protection policies	6
Figure 1-6 Quick mode — Website Group Mgmt tab page of group1	6
Figure 1-7 Quick mode — adding a website.....	7
Figure 1-8 Configuring an HTTP website — creating a website group	8
Figure 1-9 Configuring an HTTP website — entering the website group name	8
Figure 1-10 Configuring an HTTP website — Website List dialog box	9
Figure 1-11 Configuring an HTTP website — adding an HTTP website.....	10
Figure 1-12 Configuring an HTTP website — selecting protection items	11
Figure 1-13 Configuring an HTTP website — web security protection policy configuration	11
Figure 1-14 Configuring an HTTPS website — creating a website group.....	12
Figure 1-15 Configuring an HTTPS website — entering the website group name	13
Figure 1-16 Configuring an HTTPS website — Website List dialog box	13
Figure 1-17 Configuring an HTTPS website — creating an HTTPS website.....	14
Figure 1-18 Configuring an HTTPS website — selecting protection items	15
Figure 1-19 Creating a virtual website	16
Figure 1-20 Virtual Website page	16
Figure 1-21 Policy Configuration page	17
Figure 2-1 Typical deployment topology	18
Figure 2-2 Website Group Mgmt page of group1	19
Figure 2-3 Auto-Learning Policies page	19
Figure 2-4 Creating an auto-learning policy	20
Figure 2-5 Auto-learning results	20
Figure 2-6 Creating a whitelist policy	22

Figure 2-7 Referencing a whitelist policy	23
Figure 2-8 Typical network topology	24
Figure 2-9 Creating a CSRF protection policy — URI to submit	25
Figure 2-10 Viewing the HTTP request method on the form page.....	25
Figure 2-11 Checking packet capture data for the HTTP request method.....	26
Figure 2-12 Checking the target URI on the form page	26
Figure 2-13 Checking packet capture data for the target URI	26
Figure 2-14 Creating a CSRF protection policy — URI containing the form.....	27
Figure 2-15 Checking packet capture data for the HTTP request method	28
Figure 2-16 Attribute tab linked to the form page	28
Figure 2-17 Checking the URL of the HTTP request.....	29
Figure 2-18 Referencing a CSRF policy	30
Figure 2-19 Web security logs for CSRF protection	31
Figure 2-20 Creating a leech protection policy	32
Figure 2-21 Referencing a leech protection policy	33
Figure 2-22 Leech alert logs.....	34
Figure 2-23 Creating a cookie security protection policy	35
Figure 2-24 Referencing a cookie security protection policy	37
Figure 2-25 Failure to obtain the cookie value.....	38
Figure 2-26 Cookie security protection result in packet capture data	38
Figure 2-27 Creating a brute force protection policy (form authentication)	39
Figure 2-28 Referer	40
Figure 2-29 Creating a brute force protection policy (Ajax authentication)	41
Figure 2-30 Example of embedded code (Ajax authentication).....	42
Figure 2-31 Creating a brute force protection policy (Jsonp authentication)	43
Figure 2-32 Example of embedded code (Jsonp authentication).....	44
Figure 2-33 Referencing a brute force protection policy	45
Figure 2-34 Brute force alert logs	46
Figure 2-35 Creating an XML attack protection policy	47
Figure 2-36 Referencing this XML attack protection policy.....	48
Figure 2-37 XML attack alert logs	49
Figure 2-38 Creating a smart engine inspection policy	50
Figure 2-39 Referencing this smart engine inspection policy	51

Figure 2-40 Smart engine inspection logs	52
Figure 2-41 Creating an IP reputation policy	53
Figure 2-42 Referencing an IP reputation policy	54
Figure 2-43 IP reputation logs	55
Figure 2-44 Smart patch deployment topology	55
Figure 2-45 Configuring the scanning service	56
Figure 2-46 Configuring the DNS client	57
Figure 2-47 Configuring communication interfaces for scan	57
Figure 2-48 Configuring access control policies on the network layer	57
Figure 2-49 Viewing scanning files	58
Figure 2-50 Viewing scanning results	58
Figure 2-51 Configuring smart patches	59
Figure 3-1 Topology for the connection between WAF and ESPC	62
Figure 3-2 Connecting to ESPC	63
Figure 3-3 Configuration success message	64
Figure 3-4 Topology for the connection between WAF and ADS	65
Figure 3-5 Enabling ADS collaboration on the ADS device	65
Figure 3-6 Collaboration Configuration page after ADS collaboration is enabled	66
Figure 3-7 Viewing the list of IP addresses from which traffic is diverted	66
Figure 3-8 Adding WAF	66
Figure 3-9 Enabling ADS collaboration on WAF	67
Figure 3-10 Editing ADS coordination settings	68
Figure 3-11 Verifying the configuration result	69

Preface

Scope

This document describes typical configuration examples of NSFOCUS Web Application Firewall (WAF) V6.0 on the web-based manager.

The product information involved in this document may slightly differ from your product to be installed, because of version upgrades or other reasons.

Audience

This document is intended for the following users:

- Users who want to know how to configure typical policies on WAF
- System administrator
- Network administrator





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

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

Organization

Chapter	Description
1 Configuring Websites	Describes how to configure a website on WAF.
2 Configuring Policies	Describes how to configure typical policies on WAF.
3 Connecting to Other NSFOCUS Devices	Describes how to configure WAF-ESPC and WAF-ADS connections.
A Exporting the HTTPS Certificate	Describes how to export the HTTPS certificate.
B Default Parameters	Describes default parameters of WAF.

Conventions

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

Customer Support

Email: support@nsfocusglobal.com

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

Contacts:

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

1 Configuring Websites

WAF applies policies to websites in terms of website groups. Website groups can be configured in quick mode or guide mode.

- Quick mode

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

- Guide mode

When you configure a website group in guide mode, the system asks you to configure basic information about websites to be protected and related servers, and automatically generates a set of security solutions. The set of solutions take effect and protect the websites immediately when the website group configuration is completed.

1.1 Quick Mode

Scenario

A set of security solutions is created to protect specified servers in the network environment shown in [Figure 1-1](#).

Figure 1-1 Quick mode — typical deployment topology



Configuration Roadmap

1. Create a website group in quick mode.

2. Add websites to the website group.

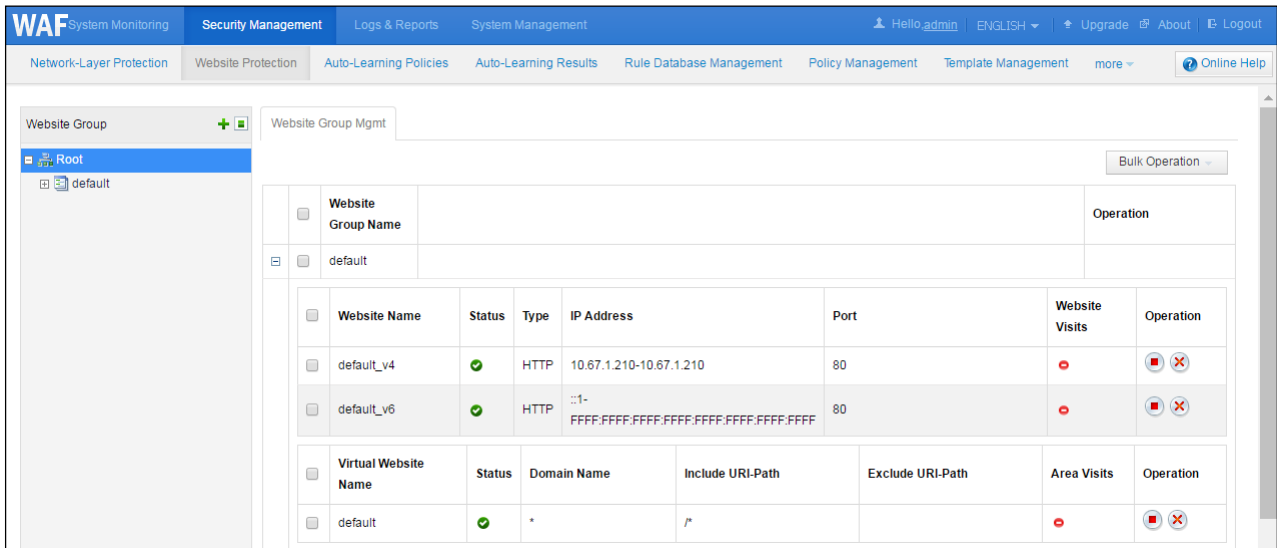
Configuration Procedure

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

Step 1 Create a website group.

- a. Choose **Security Management > Website Protection**.

Figure 1-2 Quick mode — Website Group Mgmt page




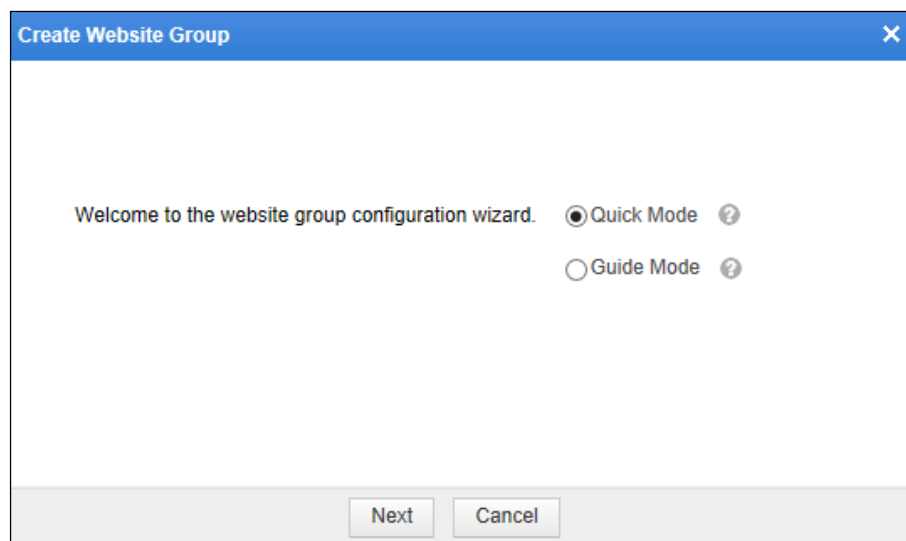
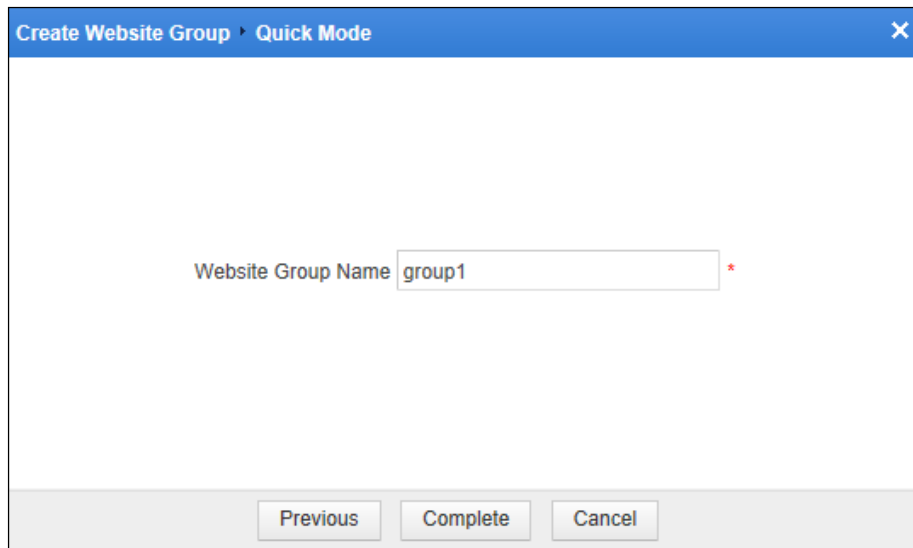
- b. In the **Website Group** pane, click  in the upper-right corner.
The **Create Website Group** dialog box appears, as shown [Figure 1-3](#).

Figure 1-3 Quick mode — creating a website group



- c. Click **Quick Mode** and then click **Next**.

Figure 1-4 Quick mode — entering the website group name



The screenshot shows a dialog box titled "Create Website Group - Quick Mode". Inside the dialog, there is a label "Website Group Name" followed by a text input field containing the text "group1". A red asterisk is positioned to the right of the input field. At the bottom of the dialog, there are three buttons: "Previous", "Complete", and "Cancel".

- d. In the dialog box, type the website group name, for example, **group1**, and then click **Complete**.
The **group1** website group is created and displayed in the **Website Group** navigation tree.
- e. Click **group1** in the navigation tree and view its web security protection policies on the **Web Security Protection** page.
The system's default protection policies have been loaded, as shown in [Figure 1-5](#).

Figure 1-5 Quick mode — viewing web security protection policies

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

Policy Template

Fast Config Use templates to configure the following policies.

Protocol Validation

HTTP Validation

Basic Protection

HTTP Access Control

Web Server/Plug-in Protection

Crawler Protection

Common Web Protection

Illegal Upload Restriction

Illegal Download Restriction

Information Disclosure Protection

Advanced Protection

Leech Protection

CSRF Protection

Scanning Protection

Cookie Security

Content Filtering

Sensitive Information Filtering

Brute Force Protection

XML Attack Protection

Smart Engine Inspection

IP Reputation

Precise Protection

Whitelist

Smart Patch

Others

Custom Policy

Step 2 Add a website.

- a. Click the **Website Group Mgmt** tab.


Figure 1-6 Quick mode — Website Group Mgmt tab page of group1

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

Policy Control

Accept

Website Group Basic Information

Website Group Name	Operating System	Database	Web Server	Language	Operation
group1	Linux/Unix Windows Others	SQL Server Access MySQL Postgres Oracle DB2 Others	IIS Apache Tomcat Nginx Weblogic Lighttpd Others	PHP ASP .Net Java Python Perl Others	

Website

Website Name	Type	IP Address	Port	Certificate	Web Access Logs	Website Visits	Status	Operation
No protected website								

Virtual Website

Virtual Website Name	Domain Name	Include URI-Path	Exclude URI-Path	Area Visits	Status	Operation
No virtual website.						

- b. Click **Add Website** to add a website (that is, object protected by policies) to this group.

Figure 1-7 Quick mode — adding a website

Add Website

Server Name *

Server Type ☒ HTTP ☐ HTTPS

Server IP Address - * ?

Server Port *

Enable Web Access Log ☐ Yes ☒ No

Enable Website Access Statistics ☐ Yes ☒ No

HTTP decode failure alert ☒ Yes ☐ No

Action upon HTTP Decode Failure ☒ Block for all ☐ Pass for all ☐ Custom ?

Enable Gzip ☐ Yes ☒ No

- c. In the dialog box, set parameters and click **Complete** to complete the configuration. Then WAF can protect the new website with default policies.

----End

1.2 Guide Mode

You can configure HTTP websites and HTTPS websites in guide mode.

1.2.1 Configuring an HTTP Website

Scenario

A set of security solutions is created for a specified HTTP server in the network environment shown in [Figure 1-1](#).

Configuration Roadmap

1. Create a website group in guide mode.
2. Configure an HTTP website.
3. Generate default policies in guide mode.

Configuration Procedure

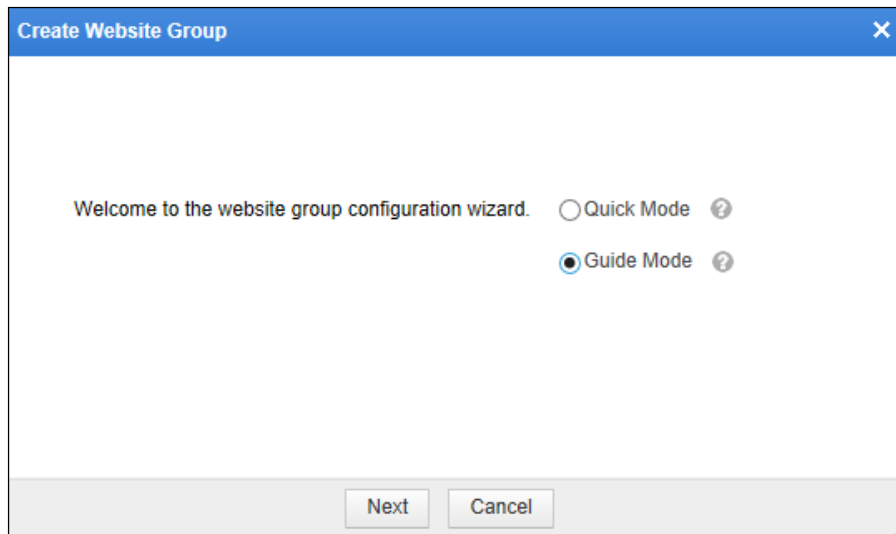
To configure an HTTP website in guide mode, perform the following steps:

Step 1 Create a website group.

- a. Choose **Security Management > Website Protection**.
- b. In the **Website Group** pane, click in the upper-right corner.

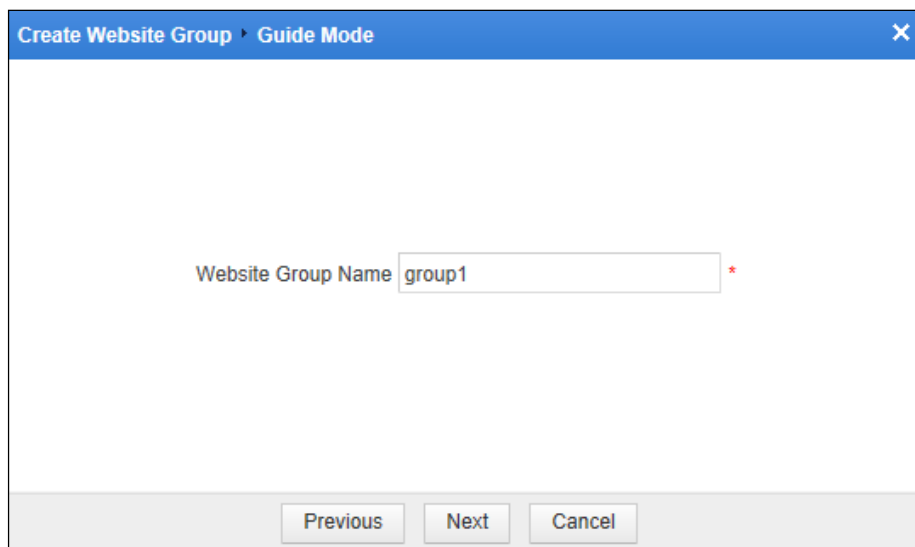
The **Create Website Group** dialog box appears, as shown in [Figure 1-8](#).

Figure 1-8 Configuring an HTTP website — creating a website group



- c. Click **Guide Mode** and then click **Next**.

Figure 1-9 Configuring an HTTP website — entering the website group name




- d. In the dialog box, type the website group name, for example, **group1**. Click **Next**.

Figure 1-10 Configuring an HTTP website — Website List dialog box

Create Website Group > Guide Mode > Website List

Website List

Create

Name	Type	Address	Port	Certificate	Operation
 No Data					

Previous Next

Step 2 Add an HTTP website.

- a. In the dialog box, click **Create** in the upper-right corner.

Figure 1-11 Configuring an HTTP website — adding an HTTP website

- b. In the dialog box, set HTTP website parameters.
- c. Click **OK** to complete the configuration and return to the **Website List** dialog box.

Step 3 Generate default policies for the website group in guide mode.

- a. Click **Next**.

The **Service System Information** dialog box appears, as shown in [Figure 1-12](#).

By default, all items are selected. You can make your own selections as required to create protection policies for your website.



Note

If you are sure about the specific operating system, web server, database, and programming language used by the server to be protected, you are advised to select the specific values so that WAF can create protection policies specific to the server.

If **Action upon HTTP Decode Failure** is set to **Pass**, when HTTP decoding fails for a connection, all subsequent requests and responses of the connection will be directly forwarded by WAF, without going through security protection policies. If **Action upon HTTP Decode Failure** is set to **Block**, when HTTP decoding fails for a connection, all subsequent requests and responses of the connection will be directly blocked by WAF.

Figure 1-12 Configuring an HTTP website — selecting protection items

Create Website Group > Guide Mode > Service System Information

Operating System

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

Web Server

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

Database

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

Programming Language

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

Previous **Complete**

b. Click **Complete** to complete the configuration.

Step 4 Click **group1** in the **Website Group** navigation tree and click **Web Security Protection** to view the website's web security protection policies, as shown in [Figure 1-13](#).

Figure 1-13 Configuring an HTTP website — web security protection policy configuration

Policy Template

Fast Config Use templates to configure the following policies.

Protocol Validation

HTTP Validation

Basic Protection

HTTP Access Control

Web Server/Plug-in Protection

Crawler Protection

Common Web Protection

Illegal Upload Restriction

Illegal Download Restriction

Information Disclosure Protection

Advanced Protection

Leech Protection

CSRF Protection

Scanning Protection

Cookie Security

Content Filtering

Sensitive Information Filtering

Brute Force Protection

XML Attack Protection

Smart Engine Inspection

IP Reputation

Precise Protection

Whitelist

Smart Patch

Others

Custom Policy

----End

1.2.2 Configuring an HTTPS Website

Scenario

A set of security solutions is created for a specified HTTPS server in the network environment as shown in [Figure 1-1](#).

Configuration Roadmap

1. Create a website group in guide mode.
2. Configure an HTTPS website.
3. Generate default policies in guide mode.

Configuration Procedure

To configure an HTTPS website in guide mode, perform the following steps:

Step 1 Create a website group.


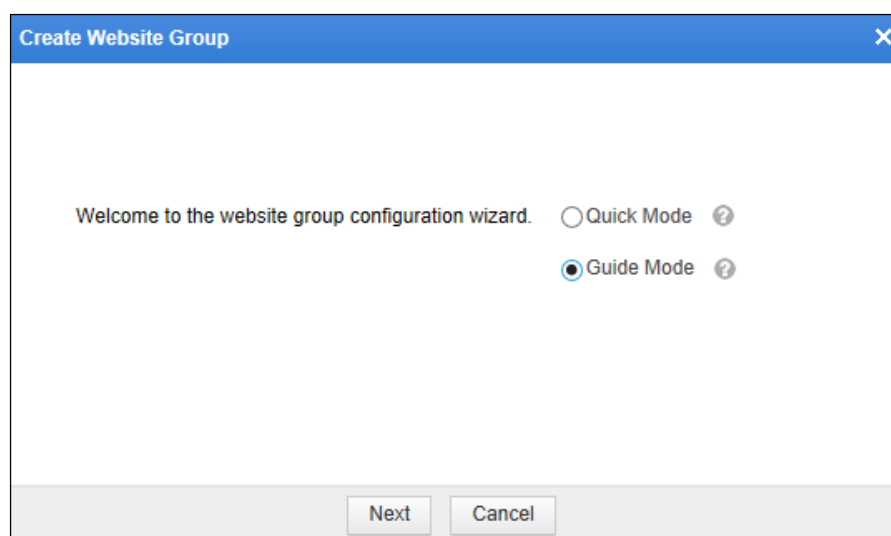
- a. Choose **Security Management > Website Protection**.
- b. In the **Website Group** pane, click  in the upper-right corner.
The **Create Website Group** dialog box appears, as shown in [Figure 1-14](#).

Figure 1-14 Configuring an HTTPS website — creating a website group



- c. Click **Guide Mode** and then click **Next**.

Figure 1-15 Configuring an HTTPS website — entering the website group name

Create Website Group ▸ Guide Mode

Website Group Name *

Previous Next Cancel


- d. In the dialog box, type the website group name, for example, **group1**. Click **Next**.

Figure 1-16 Configuring an HTTPS website — Website List dialog box

Create Website Group ▸ Guide Mode ▸ Website List

Website List

Create

Name	Type	Address	Port	Certificate	Operation
 No Data					

Previous Next

Step 2 Add an HTTPS website.

- a. In the dialog box, click **Create** in the upper-right corner, and select **HTTPS** for **Server Type**, as shown in [Figure 1-17](#).

Figure 1-17 Configuring an HTTPS website — creating an HTTPS website

- b. Set HTTPS website parameters and upload the HTTPS certificate file for the server.



Note

The HTTPS certificate file you import should match the specified server. For details on how to export common HTTPS certificate files, see [appendix A Exporting the HTTPS Certificate](#).

You are advised to select one or more SSL cipher algorithms for WAF communication.

- c. Click **OK** to complete the configuration and return to the **Website List** dialog box.

Step 3 Generate default policies for the website group in guide mode.

- a. Click **Next**.

The **Service System Information** dialog box appears, as shown in [Figure 1-18](#).

By default, all items are selected. You can make your own selections as required to create protection policies for your website.

Figure 1-18 Configuring an HTTPS website — selecting protection items

Create Website Group > Guide Mode > Service System Information

Operating System ^

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

Web Server ^

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

Database ^

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

Programming Language ^

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

Previous Complete

b. Click **Complete** to complete the configuration.

----End

1.3 Creating a Virtual Website

Scenario

For the website group of a specified HTTPS server in the network environment as shown in [Figure 1-1](#), create a virtual website and then configure protection policies for this website.

Configuration Roadmap

4. Create a virtual website for an existing website group.
5. Configure policies for the new virtual website.

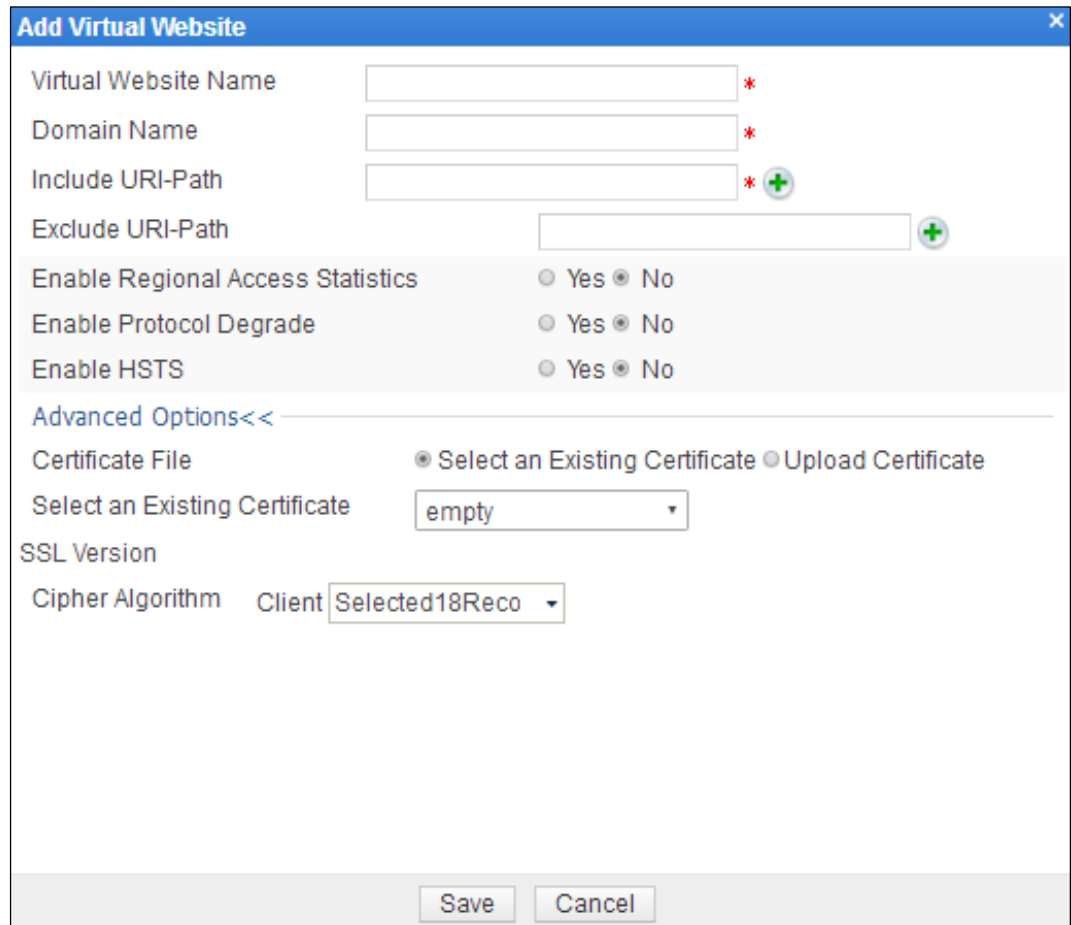
Configuration Procedure

To create a virtual website, perform the following steps:

Step 1 Create a virtual website.

- a. Choose **Security Management > Website Protection**.
- b. Point to a website group and then click **+**.

Figure 1-19 Creating a virtual website



Add Virtual Website

Virtual Website Name *

Domain Name *

Include URI-Path * +

Exclude URI-Path +

Enable Regional Access Statistics ☐ Yes ☒ No

Enable Protocol Degrade ☐ Yes ☒ No

Enable HSTS ☐ Yes ☒ No

Advanced Options << —

Certificate File ☒ Select an Existing Certificate ☐ Upload Certificate

Select an Existing Certificate ▼

SSL Version

Cipher Algorithm Client ▼

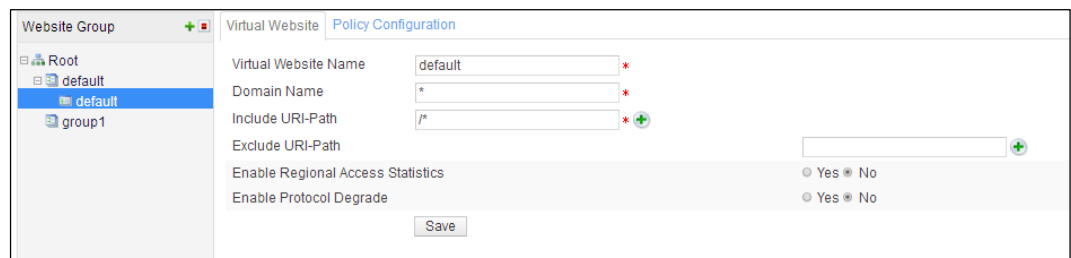
Save Cancel

- c. In the dialog box, configure parameters.
- d. Click **Save** to complete the configuration.

Step 2 Configure policies for the new virtual website.

- a. Click **default** in the website tree to open the **Virtual Website** page of this website.

Figure 1-20 Virtual Website page



Website Group + - Virtual Website Policy Configuration

Root

default

group1

Virtual Website Name *

Domain Name *

Include URI-Path * +

Exclude URI-Path +

Enable Regional Access Statistics ☐ Yes ☒ No

Enable Protocol Degrade ☐ Yes ☒ No

Save

- b. Click the **Policy Configuration** tab.

Figure 1-21 Policy Configuration page

Virtual Website Policy Configuration		
Policy Template		
Fast Config	<input type="button" value="Select Virtual Website Template"/>	Use templates to configure the following policies.
Protocol Validation		
HTTP Validation	<input checked="" type="checkbox"/> Use corresponding policy of its website group	default_medium
Basic Protection		
Web Server/Plug-in Protection	<input checked="" type="checkbox"/> Use corresponding policy of its website group	default_medium
Crawler Protection	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
Common Web Protection	<input checked="" type="checkbox"/> Use corresponding policy of its website group	default_medium
Illegal Upload Restriction	<input checked="" type="checkbox"/> Use corresponding policy of its website group	default_medium
Illegal Download Restriction	<input checked="" type="checkbox"/> Use corresponding policy of its website group	default_medium
Information Disclosure Protection	<input checked="" type="checkbox"/> Use corresponding policy of its website group	default_medium
Advanced Protection		
Content Filtering	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
Sensitive Information Filtering	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
Brute Force Protection	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
XML Attack Protection	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
Smart Engine Inspection	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
Others		
Custom Policy	<input type="checkbox"/> Use corresponding policy of its website group	Select a policy.
<input type="button" value="OK"/> <input type="button" value="Export as Virtual Website Template"/>		

c. Configure policy parameters.

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

----End

2 Configuring Policies

This chapter describes how to configure the following types of policies:

- Auto-learning policy
- Web security protection policy
- Smart patch

2.1 Configuration Example of Auto-Learning Policies

Scenario

You can configure a server-specific (for example, `www.example.com`) auto-learning policy on WAF in the network environment as shown in [Figure 2-1](#). Then WAF automatically learns traffic data of this specified URL and generates auto-learning results based on the learned traffic statistics. Note that WAF only learns traffic statistics of `www.example.com`, but excludes statistics of other expanded URLs, for example, `www.example.com/ex/` (such as `www.example.com/ex/` or `www.example.com/ex/xxx.jsp`).

Figure 2-1 Typical deployment topology



Preparation

Configure the server site `10.24.37.99:80`.

For configuration details, see chapter [1 Configuring Websites](#).

Configuration Roadmap

1. Configure an auto-learning policy.
2. Generate auto-learning results.

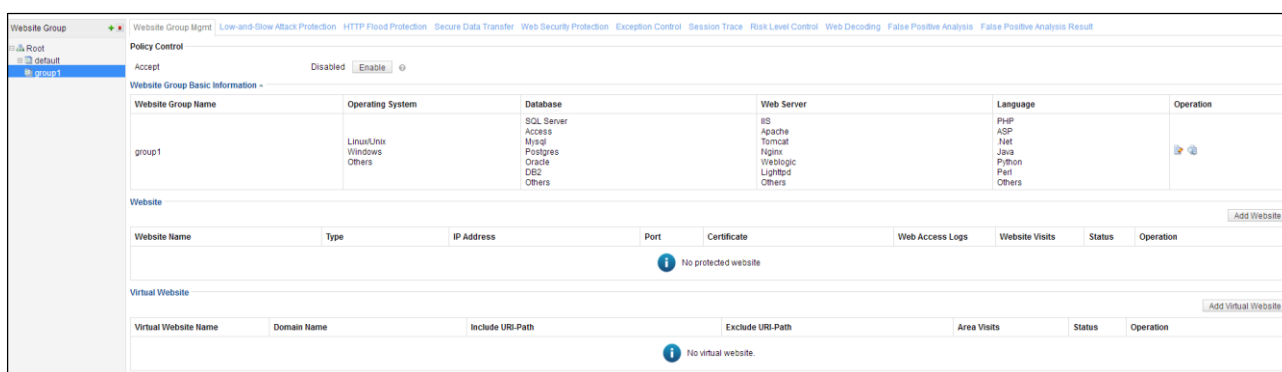
Configuration Procedure

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

Step 1 Choose **Security Management > Website Protection**.

Step 2 Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of **group1**, as shown in [Figure 2-2](#).

Figure 2-2 Website Group Mgmt page of group1




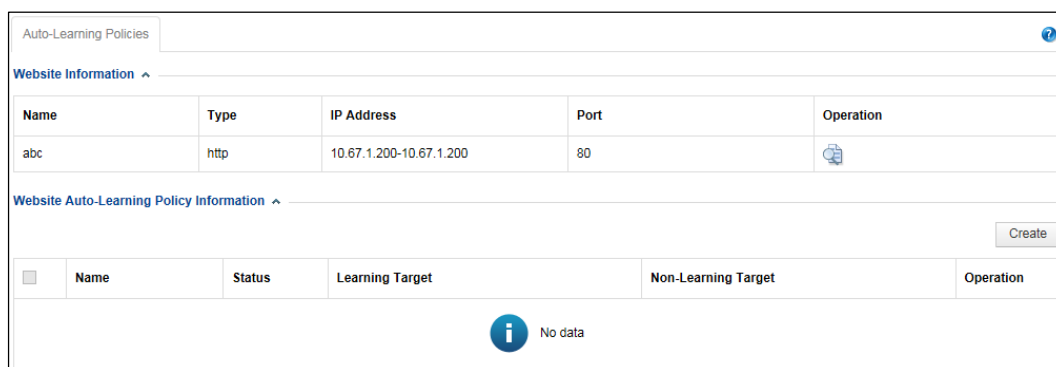
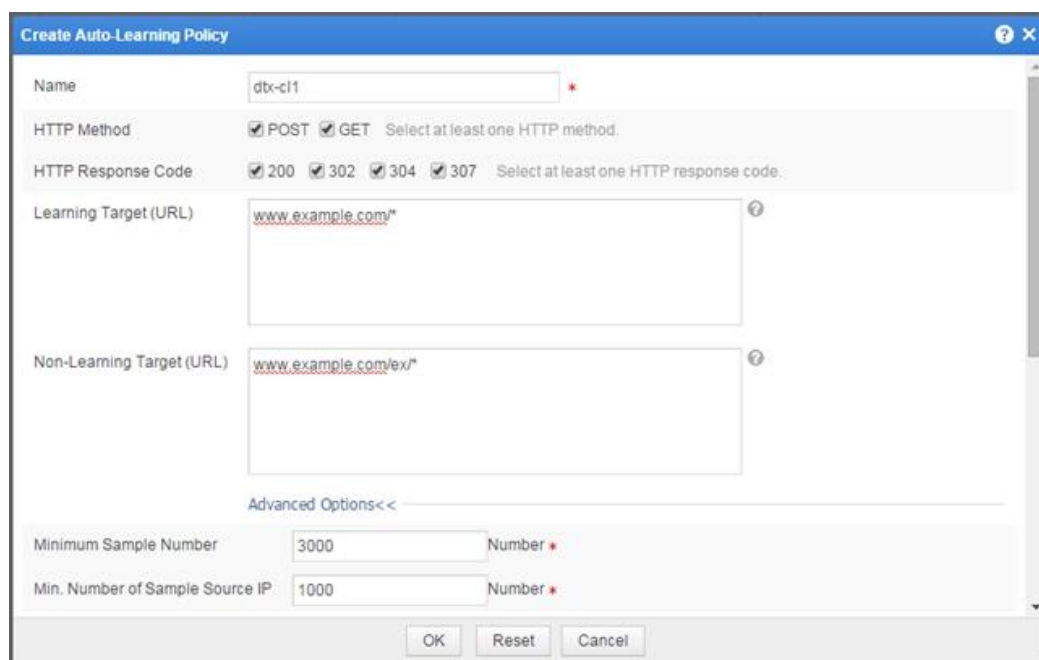
Step 3 Click  in the row of **group1** to open the **Auto-Learning Policies** page, as shown in [Figure 2-3](#).

Figure 2-3 Auto-Learning Policies page



Step 4 Click **Create** in the upper-right corner of the **Website Auto-Learning Policy Information** area.

Figure 2-4 Creating an auto-learning policy



The 'Create Auto-Learning Policy' dialog box contains the following fields and options:

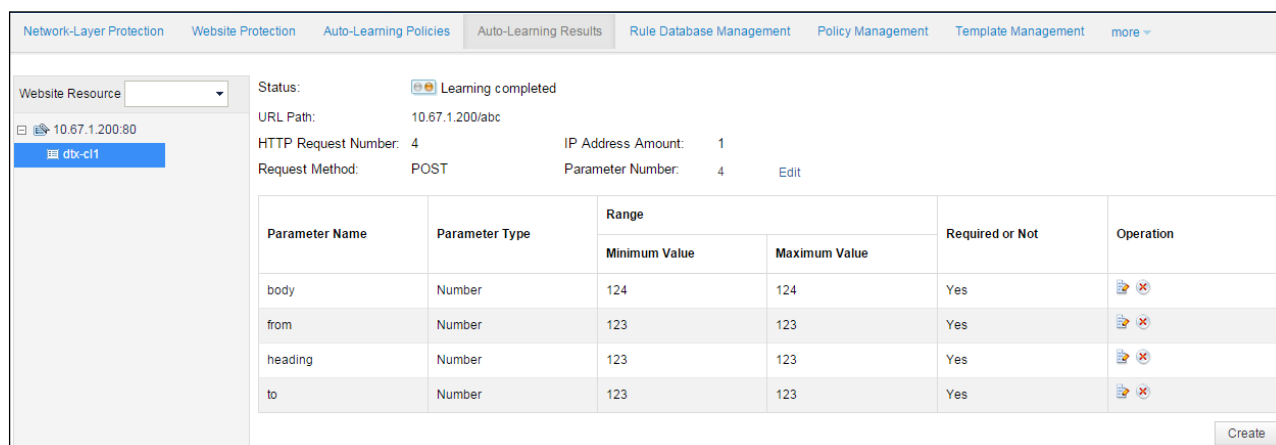
- Name:** dtx-cl1
- HTTP Method:** ☒ POST ☒ GET (Select at least one HTTP method.)
- HTTP Response Code:** ☒ 200 ☒ 302 ☒ 304 ☒ 307 (Select at least one HTTP response code.)
- Learning Target (URL):** www.example.com/*
- Non-Learning Target (URL):** www.example.com/lex/*
- Advanced Options <<**
 - Minimum Sample Number:** 3000 (Number)
 - Min. Number of Sample Source IP:** 1000 (Number)

Buttons: OK, Reset, Cancel

Step 5 Set parameters in the dialog box and click **OK** to save the settings and return to the **Auto-Learning Policies** page.

Step 6 Wait until the specified learning time elapses, and view the learning results on the **Auto-Learning Results** page (**Security Management > Auto-Learning Results**), as shown in Figure 2-5.

Figure 2-5 Auto-learning results



The 'Auto-Learning Results' page displays the following information:

- Website Resource:** 10.67.1.200:80
- Status:** Learning completed
- URL Path:** 10.67.1.200/abc
- HTTP Request Number:** 4
- IP Address Amount:** 1
- Request Method:** POST
- Parameter Number:** 4

Parameter Name	Parameter Type	Range		Required or Not	Operation
		Minimum Value	Maximum Value		
body	Number	124	124	Yes	
from	Number	123	123	Yes	
heading	Number	123	123	Yes	
to	Number	123	123	Yes	

Buttons: Create

Step 7 (Optional) Alter auto-learning results that do not fit in with the actual network environment.

----End

2.2 Configuration Examples of Web Security Protection Policies

This section mainly describes configuration examples of the following types of web security protection policies:

- [Whitelist Policy](#)
- [CSRF Protection Policy](#)
- [Leech Protection Policy](#)
- [Cookie Security Protection Policy](#)
- [Brute Force Protection Policy](#)
- [XML Attack Protection Policy](#)
- [Smart Engine Inspection Policy](#)
- [IP Reputation Policy](#)

2.2.1 Whitelist Policy

Scenario

You can configure whitelist policies on WAF based on its auto-learning results in the network environment as shown in [Figure 2-1](#). WAF handles requests by matching them against whitelist policies you configure. If a request matches a whitelist policy, WAF handles it as directed in the matching policy; otherwise, WAF does not perform whitelist protection on it.

Preparation

Configure an auto-learning policy. For details, see section [2.1 Configuration Example of Auto-Learning Policies](#).

Configuration Roadmap

1. Create a whitelist policy.
2. Reference this policy.

Configuration Procedure

Perform the following steps:

Step 1 Create a whitelist policy.

- a. Choose **Security Management > Policy Management > Precise Protection > Whitelist**.
- b. Click **Create**.

Figure 2-6 Creating a whitelist policy

Create Whitelist

Basic Information

Name:
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: ?

Response Code:

Response File: ☒ Select an Existing Response File ☐ Upload Response File

Optional Learning Result Object ?

- ☐ ☐ 10.71.1.22:82
- ☐ ☐ 188.1.1.107:82

Submit Reset Cancel

- c. In the **Create Whitelist** dialog box, configure parameters and click **Submit** to save the settings.

Step 2 Specify a website group to reference this whitelist policy.

- a. Choose **Security Management > Website Protection**
- b. Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- c. Click **Web Security Protection**, and select **Test** from the **Whitelist** drop-down box in the **Precise Protection** area, as shown in [Figure 2-7](#).

Figure 2-7 Referencing a whitelist policy

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

d. Click **OK** to complete the configuration.

----End

2.2.2 CSRF Protection Policy

Scenario

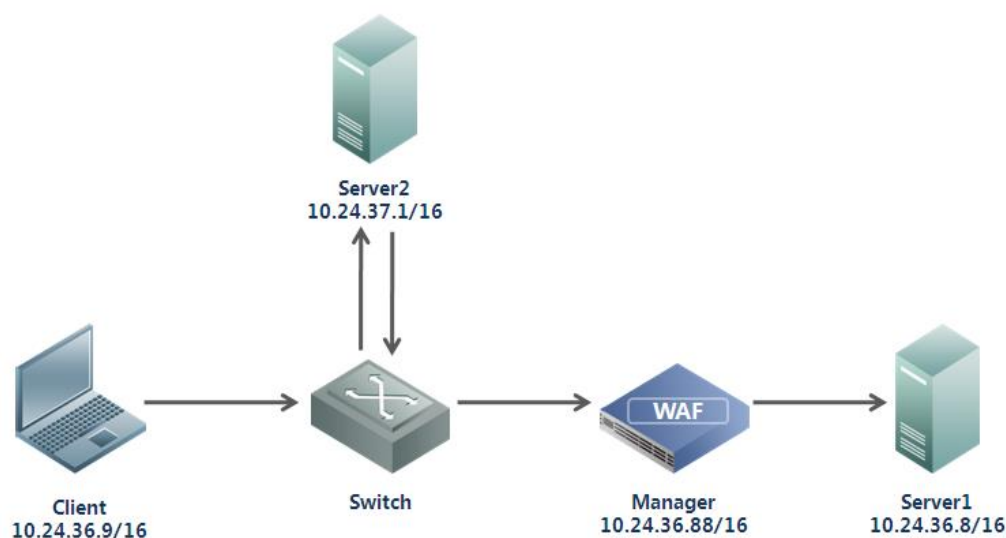
WAF can protect against cross-site request forgery (CSRF) attacks. A CSRF attack in a network environment shown in [Figure 2-8](#) is conducted as follows:

(Prerequisite: The client has access to server1 and has the privilege to change its password for logging in to server1.)

1. The client logs in to server1 and continues to access server2 without logging out of server1.
2. Server2 contains malicious code and induces the client to send server 1 a request for changing the client's login password for server1 without the client's knowing it.
3. The password changing request contains the identity information of the client. Server1 approves the request because the client has the privilege of changing its login password.

In this way, the client's password for logging in to server1 is maliciously changed.

Figure 2-8 Typical network topology



Preparation

Configure a website group to be protected.

Configuration Roadmap

1. Create a CSRF protection policy.
2. Reference this policy.

Configuration Procedure

Perform the following steps:

Step 1 Create a CSRF protection policy.

- a. Choose **Security Management > Policy Management > Advanced Protection > CSRF Protection**.
- b. Click **Create** in the upper-right corner of the page.
- c. In the **Create CSRF Protection** dialog box, configure a CSRF protection policy named **CSRF**, as shown in [Figure 2-9](#).

Figure 2-9 Creating a CSRF protection policy — URI to submit

Create CSRF Protection

Basic Information

Name:
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: ?

Source IP Blocking:

Protection Information

URI to Submit:

URI Containing the Form: [Web 2.0 Config](#)

Destination Host Name:

URI ?

Request Method: ☐ GET ☒ POST

URI Matching: ?

☐ Case-Sensitive ☒

OK Reset Cancel

You can obtain **Request Method** and **URI Matching** before configuring them.

- Obtaining the HTTP request method of the target URI

The request method of **URI to Submit** is a method used to submit forms to the server. Generally, the request method is POST. You can obtain it in one of the following ways:

- Check the **method** attribute included in the `<form>` tag in HTML code of the form page, as shown in Figure 2-10.

Figure 2-10 Viewing the HTTP request method on the form page

```
<form method="POST" action="/admin/adminpwd.asp?act=modify">
old password <input name="oldpasswd" type="password" /><br/>
```

- Capture packets to analyze the HTTP request method for form submitting. See Figure 2-11.

Figure 2-11 Checking packet capture data for the HTTP request method

```

Hypertext Transfer Protocol
+ POST /admin/adminpwd.asp?act=modify HTTP/1.1\r\n
  Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x
  Referer: http://10.24.36.8/admin/adminpwd.asp\r\n
  Accept-Language: zh-cn\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; Trident
  Content-Type: application/x-www-form-urlencoded\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: 10.24.36.8\r\n
+ Content-Length: 50\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  [truncated] Cookie: __utma=27290431.1202772552.1357643872.1357643872.1
  \r\n
Line-based text data: application/x-www-form-urlencoded
oldpasswd=██&newpasswd=██&newpasswd1=██

```

- Obtaining the target URI

The target URI is the URL to which forms are submitted for handling. You can obtain the target URI in one of the following ways:

- Check the **action** attribute included in the <form> tag in HTML code of the form page, as shown in Figure 2-12.

Figure 2-12 Checking the target URI on the form page

```

<form method="POST" action="/admin/adminpwd.asp?act=modify">
old password <input name="oldpasswd" type="password" /><br/>

```

- Capture packets to analyze the HTTP request URL for form submitting, as shown in Figure 2-13.

Figure 2-13 Checking packet capture data for the target URI

```

Hypertext Transfer Protocol
+ POST /admin/adminpwd.asp?act=modify HTTP/1.1\r\n
  Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x
  Referer: http://10.24.36.8/admin/adminpwd.asp\r\n
  Accept-Language: zh-cn\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT 5.2; Trident
  Content-Type: application/x-www-form-urlencoded\r\n
  Accept-Encoding: gzip, deflate\r\n
  Host: 10.24.36.8\r\n
+ Content-Length: 50\r\n
  Connection: Keep-Alive\r\n
  Cache-Control: no-cache\r\n
  [truncated] Cookie: __utma=27290431.1202772552.1357643872.1357643872.1
  \r\n
Line-based text data: application/x-www-form-urlencoded
oldpasswd=██&newpasswd=██&newpasswd1=██

```




- To obtain the target URI of the HTTP request, you need to first open the form page, fill in the form, start packet capture, and submit the form. In the packet capture data, the URL of the first HTTP request is the URL on which the form is handled.
- If the form is submitted via an HTTP GET request, the URI of the request contains parameters to be submitted, for example, /admin/adminpwd.asp?act=modify&oldpasswd=xxx&newpasswd=yyy&newpasswd1=yyy. To match these parameters to be submitted, when you configure the target URI in a CSRF protection policy, suffix a wildcard (asterisk) to the path specified by the **action** attribute of the form, for example, /admin/adminpwd.asp?act=modify&*.

- d. On the page shown in [Figure 2-9](#), click **URI Containing the Form**.
The **URI Containing the Form** area appears, as shown in [Figure 2-14](#).

Figure 2-14 Creating a CSRF protection policy — URI containing the form

Create CSRF Protection

Basic Information

Name:
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: ?

Source IP Blocking:

Protection Information

URI to Submit

URI Containing the Form

Web 2.0 Config

Referrer Host Name:

URI: ?

Request Method: ☒ GET ☐ POST

URI Matching: ?

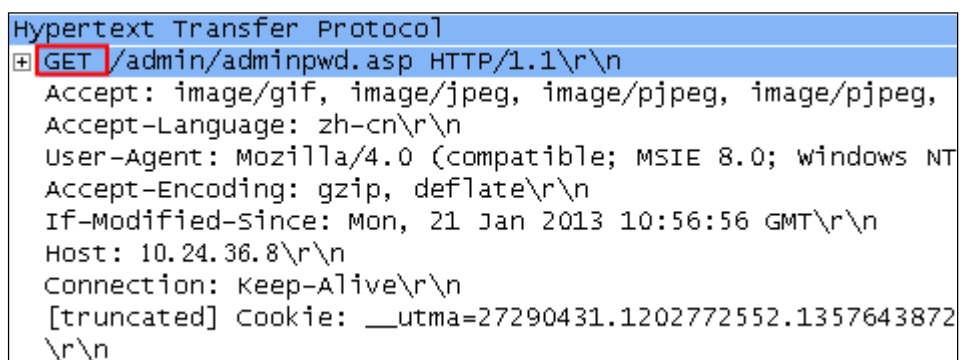
☐ Case-Sensitive +

OK Reset Cancel

You can obtain **Request Method** and **URI Matching** before configuring them.

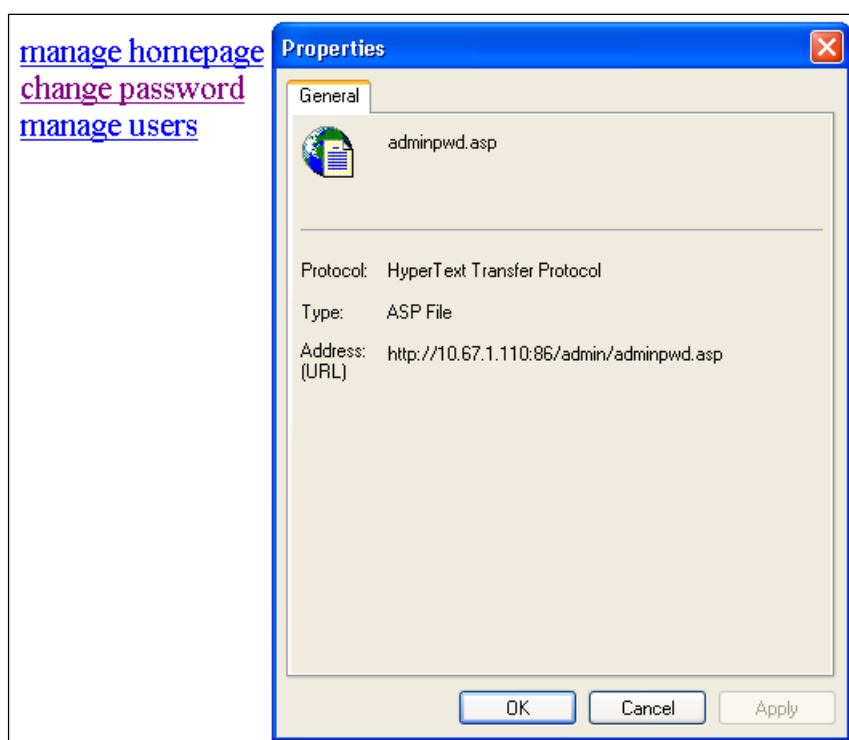
- **Obtaining the request method of URI Containing the Form**
The request method of **URI Containing the Form** is the HTTP method used to open the form page. Usually, the request method is GET. You can obtain the request method from the packet capture data. See [Figure 2-15](#).

Figure 2-15 Checking packet capture data for the HTTP request method



- **URI Containing the Form** — URI matching
URI Containing the Form is the URL of the page that includes the form. You can obtain the referrer URI in one of the following ways:
 - View the referrer URI in the **Attribute** tab of the link on the form page, as shown in Figure 2-16.

Figure 2-16 Attribute tab linked to the form page



- Capture packets to analyze the referrer of the HTTP request when the form is submitted or the URL of the HTTP request when the form page is open. See Figure 2-17.

Figure 2-17 Checking the URL of the HTTP request

```

Hypertext Transfer Protocol
+ GET /admin/adminpwd.asp HTTP/1.1\r\n
  Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg,
  Accept-Language: zh-cn\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; windows NT
  Accept-Encoding: gzip, deflate\r\n
  If-Modified-Since: Mon, 21 Jan 2013 10:56:56 GMT\r\n
  Host: 10.24.36.8\r\n
  Connection: Keep-Alive\r\n
  [truncated] Cookie: __utma=27290431.1202772552.1357643872
\r\n

```

**Note**

When you configure a CSRF protection policy, WAF asks you to type the verification code on the website entry page. Therefore, the website entry page must be protected and proxied by WAF. Otherwise, WAF cannot protect the website.

- e. After configuring parameters, click **OK** to save the settings.

Step 2 Specify a website group to reference this CSRF protection policy.

- a. Choose **Security Management > Website Protection**.
- b. Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- c. Click **Web Security Protection**, and select **CSRF** from the **CSRF Protection** drop-down box in the **Advanced Protection** area, as shown in [Figure 2-18](#).

Figure 2-18 Referencing a CSRF policy

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

Step 3 Click **OK** to complete the configuration.

----End

Protection Effect

Based on the preceding configuration, WAF will block CSRF attacks that target the server and generate alert logs about the attacks. You can view attack alert logs on the **Web Security Logs** page (**Logs & Reports > Security Protection Logs**), as shown in [Figure 2-19](#).

Figure 2-19 Web security logs for CSRF protection

Web Security Logs [Network-Layer Access Control Logs](#) [DDoS Protection Logs](#) [High-Risk IP Blocking Logs](#) [Web Anti-Defacement Logs](#) [ARP Protection Logs](#) [Web Access Logs](#) [Session Track Logs](#)

Q Conditions ▲

☐ Date 2016-11-23 15:27 - 2016-11-23 15:27

☐ Event Type

☐ Risk Level

☐ Domain Name

☐ URI

☐ Method

☐ Action

☐ Protocol Type

☐ Server IP Address

☐ Client Location

☐ Client IP Address

☐ Server Port

☐ Client Port

☐ Proxy Information

Page Number: 1 / 1 Query Result: 5 ?

Local Time	Event Type	Domain Name	Client IP Address	Protocol Type	URI	Risk Level	Method	Matching Policy	Matching Rule	Action	IP Address Block	Operation
2016-11-17 17:17:06	Cross-Site Request Forgery	10.68.2.204	10.68.2.53(Local area network)	HTTP	/content/content/21757980.php		GET	CSRF		Block	Disable	

2.2.3 Leech Protection Policy

Scenario

In the network environment shown in [Figure 2-8](#), the website on server2 can reference resources (for example, a picture, <http://www.xxx.com/A.jpg>) on server1 and provide them for users to seek illegal benefits. To prevent unauthorized use of resources on server1, WAF is configured to stop server2 from obtaining resources from server1, but allow normal access to other websites (for example, www.yyy.com).

Preparation

Configure a website group to be protected.

Configuration Roadmap

1. Create a leech protection policy.
2. Reference this policy.

Configuration Procedure

Perform the following steps:

Step 1 Configure a leech protection policy.

- a. Choose **Security Management > Policy Management > Advanced Protection > Leech Protection**.
- b. Click **Create** in the lower-right corner of the page.
- c. In the **Create Leech Protection** dialog box, configure parameters to create a leech protection policy named **LeechProtection**, as shown in [Figure 2-20](#).

Figure 2-20 Creating a leech protection policy

Create Leech Protection

Basic Information

Name: LeechProtection
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: Block

Source IP Blocking: Unblock

Policy Inspection: Referer Inspection

Mode:
Mode

Trusted Websites

Allow Null Referer: ☒ Yes ☐ No

URI-Path Allowing Null Referer

OK Reset Cancel



Note

- In the **URI-Path Allowing Null Referer** area, you can add URLs (for example, the homepage) exempted from leech protection.
- In the **URI-Path Allowing Null Referer** area, the symbol "*" indicates that users can access the sites specified in the **Trusted Websites** area as well as default web pages of these sites, for example, `http://www.xxx.com/` or `http://www.xxx.com/bbs/`.

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

Step 2 Specify a website group to reference this leech protection policy.

- Choose **Security Management > Website Protection**.
- Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- Click **Web Security Protection**, and select **LeechProtection** from the **Leech Protection** drop-down box in the **Advanced Protection** area, as shown in [Figure 2-21](#).

Figure 2-21 Referencing a leech protection policy

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

Step 3 Click **OK** to complete the configuration.

----End

Protection Effect

Based on the preceding configuration, WAF will block leech attacks targeting <http://www.xxx.com/A.jpg> and generate related alert logs. You can view alert logs on the **Web Security Logs** page (**Logs & Reports > Security Protection Logs**), as shown in [Figure 2-22](#).

Figure 2-22 Leech alert logs

Web Security Logs [DDoS Protection Logs](#) [High-Risk IP Blocking Logs](#) [Web Anti-Defacement Logs](#) [Web Access Logs](#) [Session Track Logs](#)

Conditions

☐ Date 2017-08-06 13:39 - 2017-08-06 13:39

☐ Event Type

☐ Risk Level

☐ Domain Name

☐ URI

☐ Method

☐ Action

☐ Protocol Type

☐ Server IP Address

☐ Client Location

☐ Client IP Address

☐ Server Port

☐ Client Port

☐ Proxy Information

Query

Page Number: 1 / 2 Query Result: 27

Local Time	Event Type	Domain Name	Client IP Address	Protocol Type	URI	Risk Level	Method	Matching Policy	Matching Rule	Action	IP Address Block	Operation
2017-08-06 13:38:24	Resource Leech	10.71.1.97	10.71.1.53(Local area Network)	HTTP	/py/download/123.jpg		GET	LeechProtection		Block	Disable	

2.2.4 Cookie Security Protection Policy

Scenario

In the network environment shown in [Figure 2-1](#), WAF protects cookie information (for example, plaintext password) delivered by the server to the client from being defaced, obtained, or stolen for a malicious purpose. In this example, WAF protects cookie information based on cookie encryption and HTTPOnly.

Preparation

Configure a website group to be protected.

Configuration Roadmap

1. Create a cookie security protection policy.
2. Reference this policy.

Configuration Procedure

Perform the following steps:

Step 1 Create a cookie security protection policy.

- a. Choose **Security Management > Policy Management > Advanced Protection > Cookie Security** to open the **Cookie Security** page.
- b. Click **Create** in the lower-right corner of the page.
- c. In the **Create Cookie Security** dialog box, configure parameters to create a cookie protection policy named **CookieSecurityProtection**, as shown in [Figure 2-23](#).

Figure 2-23 Creating a cookie security protection policy

Recommendations for selecting the protection algorithm:

- The cookie signature algorithm has no impact on the existing cooking contents of user services. This applies when you are not sure if certain cookie values are used by client scripts.
- The cookie encryption algorithm can be used to protect cookies (such as ASPSESSIONID, PHPSESSID, and JSESSIONID) that identify sessions, as these cookies usually should not be used by client scripts.

HTTP requests from the same user may have different source IP addresses in one of the following cases:

- A reverse proxy exists on the server side.
- A forward proxy exists on the user side.

As each HTTP request corresponds to a source IP address, the client sending these requests fails to pass the verification by the cookie security algorithm on WAF. To allow the client to pass the verification, you need to turn off the source IP address check.

For better user experience, you are advised to set **Action** to **Clear**, that is, making WAF clear illegal cookies during protection. For example, WAF deletes detected illegal cookies from a request and delivers the handled request to the server. Then the server resets cookies for the request and WAF encrypts or signs cookies before delivering the request to the client.

If you are sure that the client scripts need to use cookies, turn off the HttpOnly protection switch and apply the cookie signature algorithm for protection. If cookies include confidential information (for example, password or IDs), you can apply the cookie encryption algorithm.



Note

	If you want the cookie protection policy to take effect immediately, you can set Cookie Compatibility Time to past time. To minimize impacts on user operations, you can set it to noon or evening when the traffic is relatively small. Note that the cookie protection policy does not take effect during the time specified by Cookie Compatibility Time .
--	---

- d. Click **OK** to save the settings.

Step 2 Specify a website to reference this cookie security protection policy.

- a. Choose **Security Management > Website Protection**.
- b. Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- c. Click **Web Security Protection**, and select **CookieSecurityProtection** from the **Cookie Security** drop-down box in the **Advanced Protection** area, as shown in [Figure 2-24](#).

Figure 2-24 Referencing a cookie security protection policy

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

Step 3 Click **OK** to complete the configuration.

----End

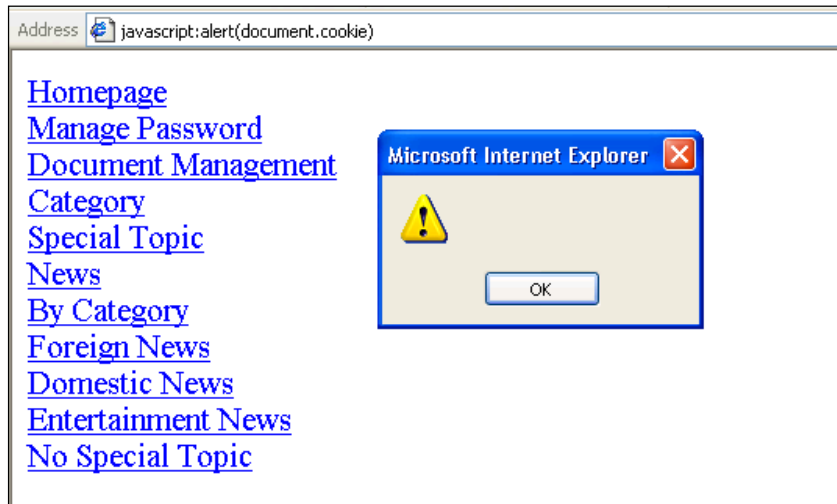
Protection Effect

You can verify the protection effect of the cookie security protection policy by using one of the following methods:

Method 1

After completing the preceding configuration, use a client to revisit a website and run the **javascript:alert(document.cookie)** command in the address bar. It turns out that you fail to obtain the cookie value, as shown in Figure 2-25.

Figure 2-25 Failure to obtain the cookie value



Method 2

Perform packet capture. The packet capture data shows that the cookie value delivered to the client is already encrypted and the HTTPOnly attribute is added.

Figure 2-26 Cookie security protection result in packet capture data

```
Content-Type: text/html\r\n
Transfer-Encoding: chunked\r\n
Connection: keep-alive\r\n
X-Powered-By: PHP/5.3.10\r\n
Set-Cookie: osCsid=pcp3nd2h0fkrq7tg8hc5utgdc0; path=/; HttpOnly\r\n
Set-Cookie: osCsid_NS_Sig=R0zoR4zoCSQpK9n7; path=/; HttpOnly\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
\r\n
```

2.2.5 Brute Force Protection Policy

Scenario

In the network environment shown in Figure 2-1, WAF is required to identify brute-force packets from login requests initiated on the client side, thereby preventing brute-force attacks targeting servers.

Preparation

Configure a website group to be protected.

Configuration Roadmap

1. Create a brute force protection policy.
2. Reference this policy.

Configuration Procedure

Step 1 Create a brute force protection policy.

The method for creating such a policy varies with the login authentication method (form, Ajax, and Jsonp).

Form authentication:

- a. Choose **Security Management > Policy Management > Advanced Protection > Brute Force Protection**.
- b. Click **Create** in the upper-right corner of the page.

In the **Create Brute Force Protection** dialog box, configure parameters to create a brute force protection policy named **form_verify**, as shown in [Figure 2-27](#).

Figure 2-27 Creating a brute force protection policy (form authentication)

Create Brute Force Protection

Basic Information

Name: form_verify * The name length should not exceed 50 characters

Description: The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: Verification Code ?

Protection Information

Protected URL * ?	Request Threshold *	Detection Cycle (min) *	
	30	5	+

Login Verification Mode: Form

Login Referer:

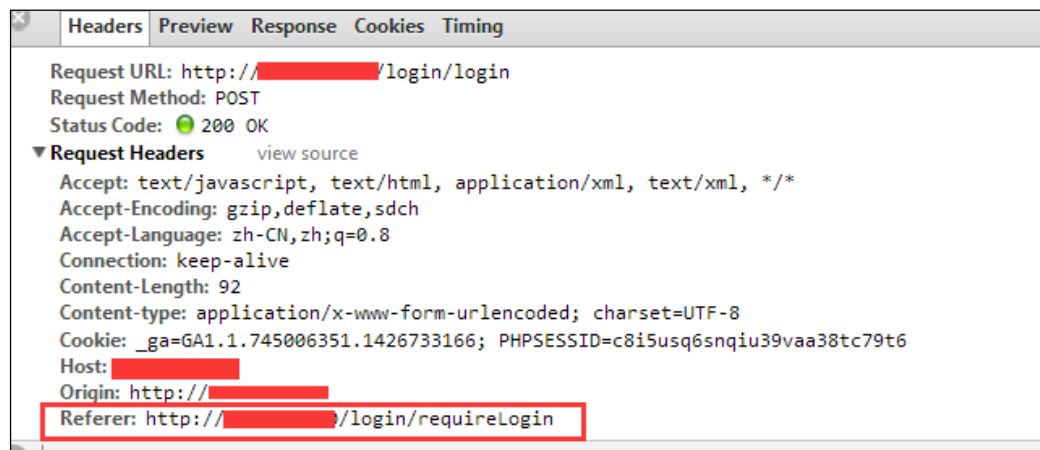
OK Reset Cancel

[Table 2-1](#) describes parameters for creating a brute force protection policy when form authentication is used.

Table 2-1 Parameters for creating a brute force protection policy (form authentication)

Parameter		Description
Basic Information	Name	Specifies the name the new policy, which is form_verify here.
	Description	Brief description of this 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. In this example, Action is set to Verification Code .
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 number of login attempts allowed within a single inspection cycle. The value range is 1–300, with 30 as the default. You can change the value according to business characteristics.
	Detection Cycle (min)	Specifies the detection cycle. The value range is 1–360 minutes, with 5 as the default. You can change the value according to business characteristics.
	Login Verification Mode	Specifies the login method. In this example, Form is selected.
	Login Referer	Specifies the referer URL carried in the request submitted via the browser. Figure 2-28 shows an example of the referer URL.

Figure 2-28 Referer



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

Ajax authentication:

- a. Choose **Security Management > Policy Management > Advanced Protection > Brute Force Protection**.

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

In the **Create Brute Force Protection** dialog box, configure parameters to create a brute force protection policy named **ajax_verify**, as shown in [Figure 2-29](#).

Figure 2-29 Creating a brute force protection policy (Ajax authentication)

The screenshot shows a 'Create Brute Force Protection' dialog box with two main sections: 'Basic Information' and 'Protection Information'. In the 'Basic Information' section, the 'Name' field is filled with 'ajax_verify', the 'Description' field is empty, the 'Alert or Not' radio buttons have 'Yes' selected, and the 'Action' dropdown is set to 'Verification Code'. In the 'Protection Information' section, the 'Protected URL' field is empty, the 'Request Threshold' is set to '30', the 'Detection Cycle (min)' is set to '5', the 'Login Verification Mode' dropdown is set to 'Ajax', and the 'Login Referer' field is empty. The dialog box has 'OK', 'Reset', and 'Cancel' buttons at the bottom.

[Table 2-2](#) describes parameters for creating a brute force protection policy when Ajax authentication is used.

Table 2-2 Parameters for creating a brute force protection policy (Ajax authentication)

Parameter		Description
Basic Information	Name	Specifies the name of the new policy, which is ajax_verify here.
	Description	Brief description of this 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. In this example, Action is set to Verification Code .
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 number of login attempts allowed within a single inspection cycle. The value range is 1–300, with 30 as the default. You can change the value according to business characteristics.
	Detection Cycle (min)	Specifies the detection cycle. The value range is 1–360 minutes, with 5 as the default. You can change the value according to business characteristics.
	Login Verification Mode	Specifies the login method. In this example, Ajax is selected.

Parameter	Description
Login Referer	Specifies the referer URL carried in the request submitted via the browser. Figure 2-28 shows an example of the referer URL.

Figure 2-30 Example of embedded code (Ajax authentication)

```

<? include "/menu.php"?>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=gb2312" />
<title>ajax</title>
<script type="text/javascript" src="../../js/jquery-1.4.1.min.js"></script>
<script type="text/javascript">
function testjquery()
{
    var uname=$('#username').val();
    var password=$('#pswd').val();
    var method = $("input[name='method']:checked").val();
    var wcp=$('#ns_wcp_5f').val();
    var dataString = 'username=' + uname + '&pswd=' + password + '&ns_wcp_5f=' + wcp;

    $.ajax({
        type: method,
        url: "/py/login/check.php",
        data: dataString,
        cache: false,
        success: function(result){
            document.getElementById("ajaxdiv").innerHTML=result;
        }
    });
}
</script>
</head>
<body>
<h1>login</h1>
Username: <input type="text" id="username" cols="20" rows="1"><br/>
Password: <input type="password" id="pswd" cols="20" rows="1"><br/>
Method: <input name="method" value="GET" checked="" type="radio">GET
       <input name="method" value="POST" type="radio">POST
</body>
</html>

```

Embedded JS function, used for submitting verification codes to WAF

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

Jsonp authentication:

Jsonp authentication involves two websites A and B with different origins. Website A is the object of protection, responsible for managing account information. Website B is responsible for actual business handling. The following configuration method is applicable provided that:

Users authenticated by the web server of website B are from a different domain, that is, user information is stored on website A (for example, a major Internet portal provides user authentication for third-party small- and medium-sized websites).

Jsonp is used for user authentication.

WAF is required to provide the verification code function.

- a. Choose **Security Management > Policy Management > Advanced Protection > Brute Force Protection**.
- b. Click **Create** in the upper-right corner of the page.

In the **Create Brute Force Protection** dialog box, configure parameters to create a brute force protection policy named **jsonp_verify**, as shown in [Figure 2-31](#).

Figure 2-31 Creating a brute force protection policy (Jsonp authentication)

Create Brute Force Protection

Basic Information

Name: jsonp_verify * The name length should not exceed 50 characters

Description: The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: Verification Code

Protection Information

Protected URL *	Request Threshold *	Detection Cycle (min) *
	30	5

Login Verification Mode: Jsonp

Login Referer:

OK Reset Cancel

Table 2-3 describes parameters for creating a brute force protection policy when Jsonp authentication is used.

Table 2-3 Parameters for creating a brute force protection policy (Jsonp authentication)

Parameter		Description
Basic Information	Name	Specifies the name of the new policy, which is jsonp_verify here.
	Description	Brief description of this 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. In this example, Action is set to Verification Code .
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 number of login attempts allowed within a single inspection cycle. The value range is 1–300, with 30 as the default. You can change the value according to business characteristics.
	Detection Cycle (min)	Specifies the detection cycle. The value range is 1–360 minutes, with 5 as the default. You can change the value according to business characteristics.
	Login Verification Mode	Specifies the login method. In this example, Jsonp is selected.
	Login Referer	Specifies the referer URL carried in the request submitted via the browser. Figure 2-28 shows an example of the referer URL.

Figure 2-32 Example of embedded code (Jsonp authentication)

```

<title>ajax</title>
<script type="text/javascript" src="../../js/jquery-1.4.1.min.js"></script>
<script type="text/javascript">

    function login()
    {
        var uname=$('#username').val();
        var password=$('#pswd').val();
        var _wcp=$('#nS_wcp_5f').val();
        var dataString = '?username=' + uname + '&pswd=' + password + '&nS_wcp_5f=' + _wcp;
        var verifyUrl = 'http://' + document.getElementById('host').value + '/py/login/checkjsonp.php';

        $.ajax({
            type: "GET",
            async:false,
            url: verifyUrl+dataString,
            dataType: 'jsonp',
            jsonp: 'callback',
            success: function(result) {
                document.getElementById("ajaxdiv").innerHTML=result.msg;
            }
        });
    }

</script>
</head>
<body>
<h1>Login</h1>
Username: <input type="text" id="username" cols="20" rows="1" /><br />
Password: <input type="password" id="pswd" cols="20" rows="1" /><br />
host: <input type="text" id="host" cols="20" rows="1" /> <br />
</body>
</html>

```

Embedded JS code used for initiating Jsonp-based cross-domain access

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

Step 2 Specify a website group to reference this brute force protection policy.

The following uses ajax_verify as an example.

- a. Choose **Security Management > Website Protection**.
Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- b. Click **Website Security Protection**, and select **ajax_verify** from the **Brute Force Protection** drop-down list in the **Advanced Protection** area, as shown in [Figure 2-33](#).

Figure 2-33 Referencing a brute force protection policy

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

c. Click **OK** to complete the configuration.

----End

Protection Effect

Based on the preceding configuration, WAF will block brute force attacks targeting the server and generate related alert logs. Simulate a brute force attack and view the attack alert logs on the **Web Security Logs** page (**Logs & Reports > Security Protection Logs**).

Figure 2-34 Brute force alert logs

Web Security Logs
Network-Layer Access Control Logs
DDoS Protection Logs
High-Risk IP Blocking Logs
Web Anti-Defacement Logs
ARP Protection Logs
Web Access Logs
Session Track Logs

Q Conditions

☐ Date

between

2017-06-28 16:28

-

2017-06-28 16:28

☐ Event Type

Not selected

☐ Risk Level

High

☐ Server IP Address

☐ Domain Name

=

☐ Client Location

CN, China

☐ URI

=

☐ Client IP Address

☐ Method

UNKNOWN

☐ Server Port

☐ Action

Pass

☐ Client Port

☐ Protocol Type





HTTP

☐ Proxy Information

Query

Page Number: 1 / 50
Query Result: 1000

First
Previous
Next
Last
Query

Local Time	Event Type	Domain Name	Client IP Address	Protocol Type	URI	Risk Level	Method	Matching Policy	Matching Rule	Action	IP Address Block	Operation
2017-06-28 16:11:50	Cookie Defacement	10.67.10.96	10.67.9.69(Local area Network)	HTTPS	/utils/sysinfo		POST	default_medium		Clear	Disable	 
2017-06-28 16:11:20	Cookie Defacement	10.67.10.96	10.67.9.69(Local area Network)	HTTPS	/utils/sysinfo		POST	default_medium		Clear	Disable	 

2.2.6 XML Attack Protection Policy

Scenario

In the network environment shown in [Figure 2-1](#), WAF needs to identify XML attack behaviors to protect the server from such attacks.

Preparation

Complete configuration of a website group named **group1** prior to XML attack protection configuration.

Configuration Roadmap

1. Create an XML attack protection policy.
2. Reference this policy.

Configuration Procedure

Step 1 Create an XML attack protection policy.

- Choose **Security Management > Policy Management > Advanced Protection > XML Attack Protection**.
- Click **Create** in the upper-right corner of the page.

In the **Create XML Attack Protection** dialog box, configure parameters to create an XML attack protection policy named **XMLAttackProtection**, as shown in [Figure 2-35](#).

Figure 2-35 Creating an XML attack protection policy

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

Step 2 Reference this XML attack protection policy.

- a. Choose **Security Management > Website Protection**.
Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- b. Click **Website Security Protection**, and select **XMLAttackProtection** from the **XML Attack Protection** drop-down list in the **Advanced Protection** area, as shown in [Figure 2-36](#).

Figure 2-36 Referencing this XML attack protection policy

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

c. Click **OK** to complete the configuration.

----End

Protection Effect

Based on the above configuration, WAF will block XML attacks that target at the server and generate alerts about the attacks. Choose **Logs & Reports > Security Protection Logs > Web Access Logs** to view XML attack alert logs.

Figure 2-37 XML attack alert logs

Web Security Logs Network-Layer Access Control Logs DDoS Protection Logs High-Risk IP Blocking Logs Web Anti-Defacement Logs ARP Protection Logs Web Access Logs Session Track Logs

Conditions

☐ Date between 2016-11-17 17:19 - 2016-11-17 17:19

☐ Event Type XML Attack

☐ Risk Level High

☐ Domain Name =

☐ URI =

☐ Method UNKNOWN

☐ Action Pass

☐ Protocol Type HTTP

☐ Server IP Address

☐ Client Location CN, China

☐ Client IP Address

☐ Server Port

☐ Client Port

☐ Proxy Information

Query

Page Number: 1 / 1 Query Result: 3 First Previous Next Last Query ?

Local Time	Event Type	Domain Name	Client IP Address	Protocol Type	URI	Risk Level	Method	Matching Policy	Matching Rule	Action	IP Address Block	Operation
2016-11-17 17:14:55	XML Attack	10.68.2.204	10.68.2.53(Local area Network)	HTTP	/content	▲	POST	XMLAttackProtection		Block	Disable	

2.2.7 Smart Engine Inspection Policy

Scenario

In the network environment shown in [Figure 2-1](#), WAF needs to detect SQL injection, cross-site scripting, command line injection, and path traversal attacks based on common web protection policies. In addition, WAF can perform more precise protection against these attacks by conducting semantic analysis of and using statistical algorithms for URI contents. In this manner, WAF will deliver a higher detection rate and a lower false positive rate.

Preparation

Complete configuration of a website group named **group1** prior to configuration of the smart engine inspection policy.

Configuration Roadmap

1. Create a smart engine inspection policy.
2. Reference this policy.

Configuration Procedure

Step 1 Create a smart engine inspection policy.

- a. Choose **Security Management > Policy Management > Advanced Protection > Smart Engine Inspection**.
- b. Click **Create** in the upper-right corner of the page.

In the **Create Smart Engine Inspection** dialog box, configure parameters to create a smart engine inspection policy named **SEaaa**, as shown in [Figure 2-38](#).

Figure 2-38 Creating a smart engine inspection policy

Create Smart Engine Inspection

Basic Information

Name: SEaaa
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: Block

Source IP Blocking: Unblock

Inspection Item

Attack: ☒ Cross-Site Scripting Attack ☒ SQL Injection Attack ☒ Command Line Injection Attack ☒ Path Traversal Attack

Content: ☒ URI ☐ Parameter ☐ Cookie

OK Reset Cancel

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

Step 2 Reference this smart engine inspection policy.

- Choose **Security Management > Website Protection**.
- Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- Click **Website Security Protection**, and select **SEaaa** from the **Smart Engine Inspection** drop-down list in the **Advanced Protection** area, as shown in [Figure 2-39](#).

Figure 2-39 Referencing this smart engine inspection policy

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

d. Click **OK** to complete the configuration.

----End

Protection Effect

After the preceding configuration is complete, WAF will detect SQL injection, cross-site scripting, command line injection, and path traversal attacks against the configured policy and generate alert logs after detecting such an attack. Choose **Logs & Reports > Security Protection Logs > Web Security Logs** to view smart engine inspection logs.

Figure 2-40 Smart engine inspection logs

Web Security Logs Network-Layer Access Control Logs DDoS Protection Logs High-Risk IP Blocking Logs Web Anti-Defacement Logs ARP Protection Logs Web Access Logs Session Track Logs

Q Conditions

☐ Date between 2016-11-17 17:57 - 2016-11-17 17:57

☐ Event Type Not selected

☐ Risk Level High

☐ Domain Name =

☐ URI =

☐ Method UNKNOWN

☐ Action Pass

☐ Protocol Type HTTP

☐ Server IP Address

☐ Client Location CN, China

☐ Client IP Address



☐ Server Port

☐ Client Port

☐ Proxy Information

Query

Page Number: 1 / 26 Query Result: 515 First Previous Next Last Query

Local Time	Event Type	Domain Name	Client IP Address	Protocol Type	URI	Risk Level	Method	Matching Policy	Matching Rule	Action	IP Address Block	Operation
2016-11-17 18:00:54	SQL Injection Attack	10.68.2.204	10.68.2.53(Local area Network)	HTTP	/py/sqlResponse.php?testid=123...	▲	GET	SEaaa	Smart engine inspection rule	Block	Disable	 

2.2.8 IP Reputation Policy

Scenario

In the network environment shown in [Figure 2-1](#), WAF can identify geographical locations of source IP addresses and then block accesses from a specific region (for example, Japan) according to the configured IP reputation policy.

Preparation

Complete configurations relating to the website group named **group1** prior to the IP reputation policy.

Configuration Roadmap

1. Create an IP reputation policy.
2. Reference this policy.

Configuration Procedure

Step 1 Create an IP reputation policy.

- a. Choose **Security Management > IP Reputation > IP Reputation Configuration**.
- b. Click **Create** in the upper-right corner of the **Advanced Protection** area.

In the **Create IP Reputation Policy** dialog box, configure parameters to create an IP reputation policy named **IPR1**, as shown in [Figure 2-41](#).

Figure 2-41 Creating an IP reputation policy

Create IP Reputation Policy

Basic Information

Name: IPR1
* The name length should not exceed 50 characters

Description:
The description content should not exceed 200 characters.

Alert or Not: ☒ Yes ☐ No

Action: Block ?

Source IP Blocking: Unblock

Inspection Item

Area: Include

OK Reset Cancel

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

Step 2 Reference this IP reputation policy.

- a. Choose **Security Management > Website Protection**.
Click **group1** in the **Website Group** navigation tree to open the **Website Group Mgmt** page of group1, as shown in [Figure 2-2](#).
- b. Click **Website Security Protection**, and select **IPR1** from the **IP Reputation** drop-down list in the **Advanced Protection** area, as shown in [Figure 2-42](#).

Figure 2-42 Referencing an IP reputation policy

Website Group Mgmt Low-and-Slow Attack Protection HTTP Flood Protection Secure Data Transfer Web Security Protection Exception Control Session Trace Risk Level Control	
Policy Template	
Fast Config	<input type="button" value="Select Website Template"/> Use templates to configure the following policies.
Protocol Validation	
HTTP Validation	default_medium
Basic Protection	
HTTP Access Control	default_medium
Web Server/Plug-in Protection	default_medium
Crawler Protection	Select a policy.
Common Web Protection	default_medium
Illegal Upload Restriction	default_medium
Illegal Download Restriction	default_medium
Information Disclosure Protection	default_medium
Advanced Protection	
Leech Protection	default_medium
CSRF Protection	Select a policy.
Scanning Protection	default_medium
Cookie Security	default_medium ?
Content Filtering	Select a policy.
Sensitive Information Filtering	Select a policy.
Brute Force Protection	Select a policy.
XML Attack Protection	Select a policy.
Smart Engine Inspection	Select a policy.
IP Reputation	IPR1
Precise Protection	
Whitelist	Select a policy.
Smart Patch	Smart Patch Configuration
Others	
Custom Policy	Select a policy.
<input type="button" value="OK"/> <input type="button" value="Export as Website Template"/>	

c. Click **OK** to complete the configuration.

----End

Protection Effect

After the preceding configuration is complete, WAF will detect IP requests in the specified region against the configured policy and generate IP reputation logs. Choose **Logs & Reports > Security Protection Logs > Web Security Logs** to view IP reputation alert logs.

Figure 2-43 IP reputation logs

Web Security Logs [DDoS Protection Logs](#) [High-Risk IP Blocking Logs](#) [Web Anti-Defacement Logs](#) [Web Access Logs](#) [Session Track Logs](#)

Conditions

☐ Date: between 2017-08-05 19:05 - 2017-08-05 19:05

☐ Event Type: Not selected

☐ Risk Level: High

☐ Domain Name: =

☐ URI: =

☐ Method: UNKNOWN

☐ Action: Pass

☐ Protocol Type: HTTP

☐ Server IP Address:

☐ Client Location: CN, China

☐ Client IP Address:

☐ Server Port:

☐ Client Port:

☐ Proxy Information:

Query

Page Number: 1 / 2 Query Result: 23 First Previous Next Last Query

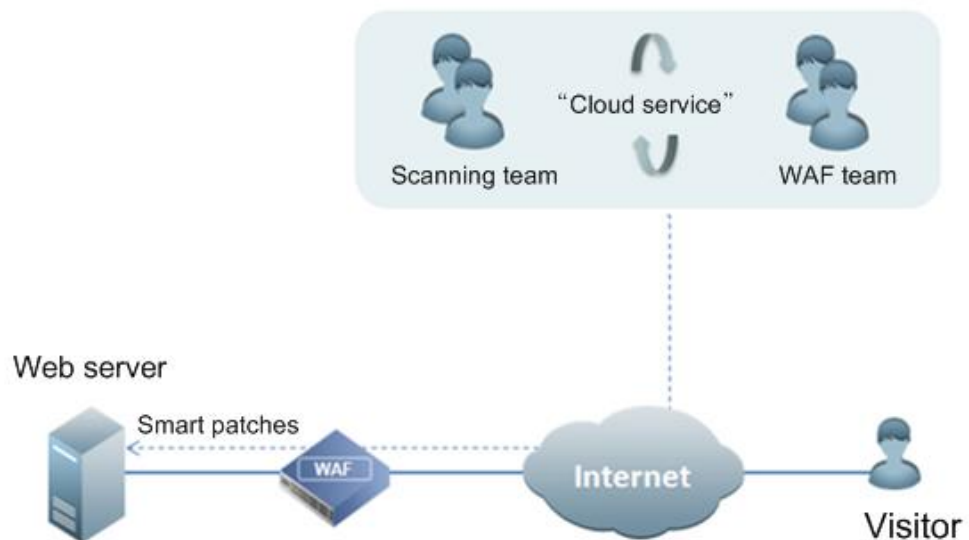
Local Time	Event Type	Domain Name	Client IP Address	Protocol Type	URI	Risk Level	Method	Matching Policy	Matching Rule	Action	IP Address Block	Operation
2017-08-05 19:05:12	IP Reputation Control	10.71.1.97	1.1.1.1(Australia)	HTTP	/scripts/test.pl%3F+.htr		GET	IPR1		Block	Disable	

2.3 Configuration Example of Smart Patches

Scenario

In the deployment topology as shown in [Figure 2-44](#), WAF performs remote penetration scan for the server to be protected and promptly applies smart patches to fix vulnerabilities.

Figure 2-44 Smart patch deployment topology



Preparation

Prior to configuration, make a call to the scanning team of NSFOCUS to confirm that the IP address for performing transmission scanning is 211.99.227.140, and the domain name and IP address for receiving scanning reports are respectively waf.api.nsfocus.net and 211.99.227.132.

Configuration Roadmap

1. Perform scanning configuration.
2. Configure communication interfaces for scanning.
3. Configure access control policies on the network layer.
4. View scanning results.
5. Generate patches.
6. Apply patches.

Configuration Procedure

Perform the following steps:

Step 1 Configure scanning.

Choose **Security Management > Smart Patch > SAAS Scan Config**. On the **SAAS Scan Config** page, enable the SAAS scanning service.

Figure 2-45 Configuring the scanning service

SAAS Scan Config WVSS Scan Config Scanning File Management Patch Management	
Authorization Information	Valid license Details
Service Running Status	Disabled
Communication with the SAAS Scanning Service	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Penetration Scanning IP	211.99.227.140
Protection Scanning IP	211.99.227.138
OK Reset	

Step 2 Configure communication interfaces for scanning.

- Choose **System Management > Network Configuration > DNS Configuration**. The **DNS Configuration** page appears, as shown in [Figure 2-46](#).

Figure 2-46 Configuring the DNS client

- b. Click **Add** and type the domain name and IP address for receiving scanning reports in the **Create** dialog box, as shown in [Figure 2-47](#).

Figure 2-47 Configuring communication interfaces for scan

- Step 3** Configure access control policies at the network layer to allow the penetration scanning IP address to directly access the customer's system.

Choose **Security Management > Network-Layer Protection > Network-Layer Access Control**. On the **Network-Layer Access Control** page that appears, click **Create** and configure two access control policies, as shown in [Figure 2-48](#).

Figure 2-48 Configuring access control policies on the network layer

Policy Enable-Disable										
Network-Layer Access Control										
TCP Flood Protection ARP Spoofing Protection ADS Collaboration Config										
Name	Status	Destination Network		Source Network		Protocol	Network Interface	Action	Alert or Not	Operation
		Network Address/Mask	Port Range	Network Address/Mask	Port Range					
test	✓	0.0.0.0/0.0.0.0		211.99.227.0/255.255.255.0		Unlimited	G1/1	Forward	Yes	
Create										

Step 4 After the scanning is completed, view the scanning results.

- a. Choose **Security Management > Smart Patch > Scanning File Management**.
The **Scanning File Management** page appears, as shown in [Figure 2-49](#).

Figure 2-49 Viewing scanning files

SAAS Scan Config WVSS Scan Config Scanning File Management Patch Management			
<input checked="" type="radio"/> SAAS <input type="radio"/> WVSS			
Scanning Domain Name	Latest Scanning Time	Scanning Status	Scanning File
zhuti.dianxinos.com	2012-12-26 17:29:09	Scanning completed.	Related Scanning File
theme01.dianxinos.com	2012-12-26 17:29:09	Scanning completed.	No scanning file
browser.dianxinos.com	2012-12-26 17:29:09	Scanning completed.	No scanning file
qianbian.dianxinos.com	2012-12-26 17:29:10	Scanning completed.	No scanning file
donut.dianxinos.com	2012-12-26 17:29:11	Scanning completed.	No scanning file
daohang.dianxinos.com	2012-12-26 17:29:11	Scanning completed.	No scanning file
widgetapi.dianxinos.com	2012-12-26 17:29:08	Scanning completed.	No scanning file

- b. In the **Scanning File** column, click **Related Scanning File** to open the online scanning report of this scanning task.

Figure 2-50 Viewing scanning results

SaaS Scanning File					
Web Vulnerability Information (Complete Time:2012-12-26 17:32:10 Detected 7 types of vulnerabilities)					
<input type="checkbox"/> Selection	No.	Vulnerability Name	Vulnerability ID	Vulnerable URL Amount	View
<input type="checkbox"/>	1	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q
<input type="checkbox"/>	2	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q
<input type="checkbox"/>	3	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q
<input type="checkbox"/>	4	Invalid Links Detected on Target Network	1000013	1	Q
<input type="checkbox"/>	5	Unsafe HTTP Method Enabled on Target URL	1000063	1	Q
<input type="checkbox"/>	6	robots File Network Architecture Information Disclosure on Target Network	1200035	1	Q
<input type="checkbox"/>	7	CRLF Injection Vulnerability in Target Website	1000061	1	Q

Step 5 Generate patches.

- a. Click **Generate Patch** in the lower-right corner of the dialog box shown in [Figure 2-50](#).

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?"

- b. Click **OK** to generate patches.



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** page shown in [Figure 2-50](#). You are advised to regenerate smart patches a moment later.

After patches are generated, The **Smart Patch Configuration** page appears, as shown in [Figure 2-51](#).

Figure 2-51 Configuring smart patches

<input type="checkbox"/> Selection	No.	Website Name
<input type="checkbox"/>	1	default
<input type="checkbox"/>	2	test



Smart patches that are not selected in [Figure 2-51](#) 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 the *NSFOCUS WAF V6.0 User Guide*.

Step 6 Apply patches.

- a. On the smart patch list shown in [Figure 2-51](#), 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?"

- b. Click **OK** to apply patches.



If smart patches fail to be applied, a red message saying "Failed to apply the smart patch(es), please retry later." appears in the lower-right corner of the **Smart Patch Configuration** dialog box shown in [Figure 2-51](#). You are advised to reapply smart patches a moment later.

----End

3

Connecting to Other NSFOCUS Devices

This chapter describes how to connect WAF to other devices for collaboration:

- [Connecting to NSFOCUS ESPC](#)
- [Connecting to NSFOCUS ADS](#)

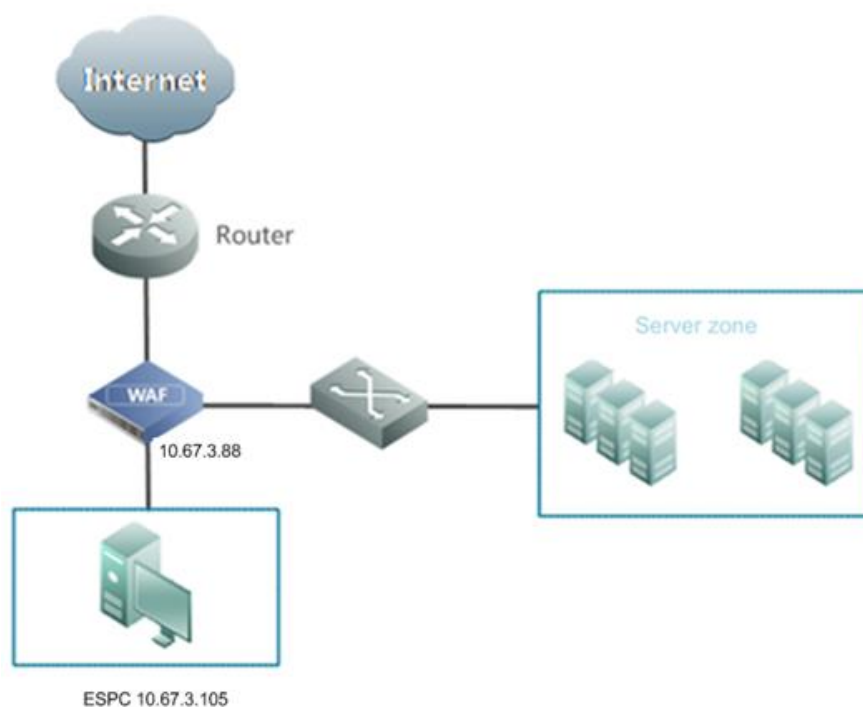
3.1 Connecting to NSFOCUS ESPC

WAF can proactively connect to ESPC or accept a connection request from ESPC. This section describes how to configure a connection from WAF to ESPC. For how to initiate a connection to WAF from ESPC, see the *NSFOCUS ESPC User Guide*.

Scenario

In the network environment shown in [Figure 3-1](#), WAF is connected to and collaborates with ESPC to receive detailed logs and keep them for a specified period of time.

Figure 3-1 Topology for the connection between WAF and ESPC



Preparation

Set the IP address of ESPC to 10.67.3.105 and the data transmission address of WAF to 10.67.3.88.

Configuration Roadmap

1. Configure WAF's registration with ESPC.
2. Verify the configuration result.

Configuration Procedure

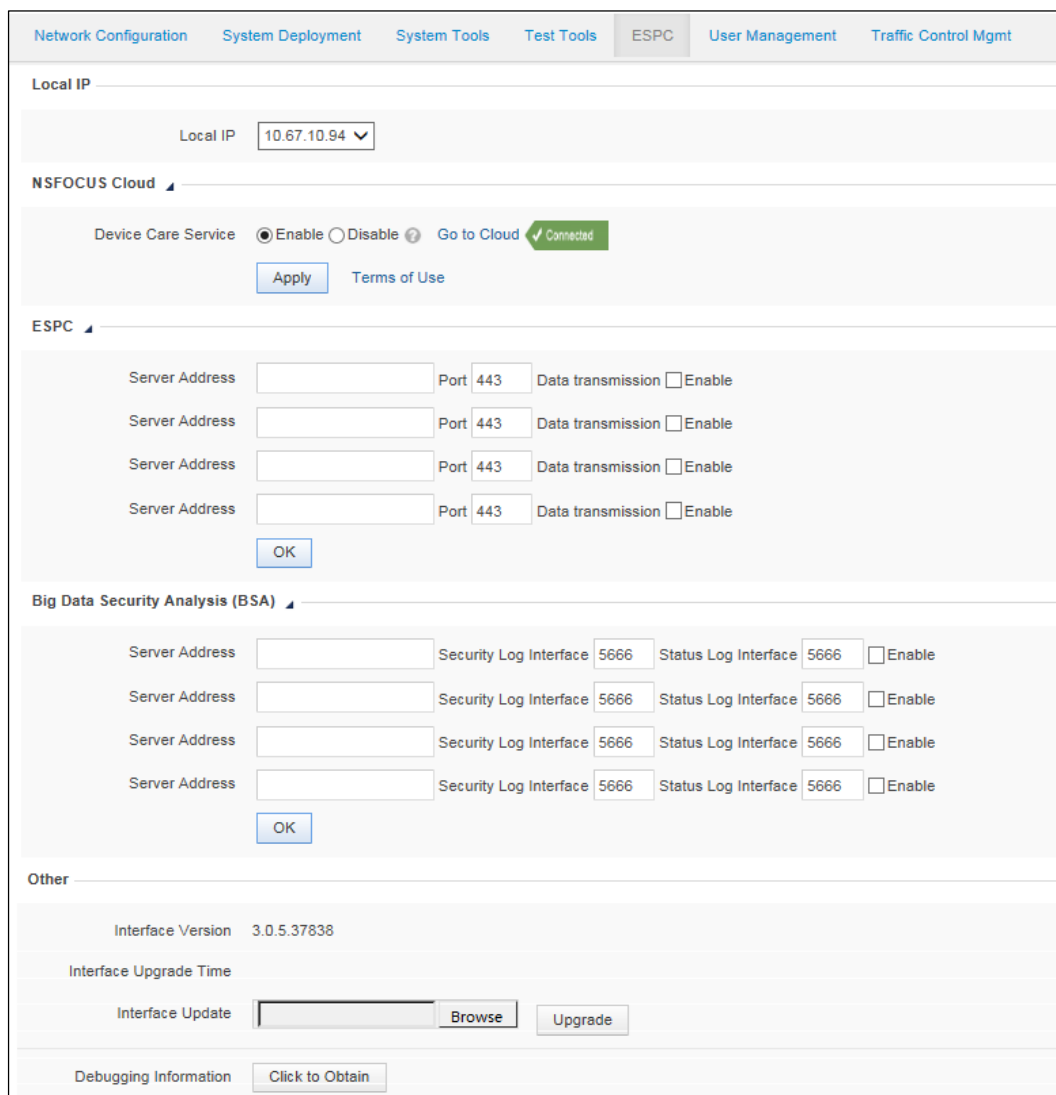
To configure the connection from WAF to ESPC, perform the following step on WAF:

Step 1 Choose **System Management > ESPC**.



Before ESPC detects WAF and adds it, the status of ESPC is displayed as **Connecting**.

Figure 3-2 Connecting to ESPC



The screenshot shows the NSFOCUS WAF configuration interface. The top navigation bar includes tabs for Network Configuration, System Deployment, System Tools, Test Tools, ESPC, User Management, and Traffic Control Mgmt. The ESPC tab is selected.

Local IP

Local IP: 10.67.10.94

NSFOCUS Cloud

Device Care Service: ☒ Enable ☐ Disable [Go to Cloud](#) Connected

[Apply](#) [Terms of Use](#)

ESPC

Four rows of configuration for ESPC:

Server Address	Port	Data transmission
<input type="text"/>	443	<input type="checkbox"/> Enable
<input type="text"/>	443	<input type="checkbox"/> Enable
<input type="text"/>	443	<input type="checkbox"/> Enable
<input type="text"/>	443	<input type="checkbox"/> Enable

[OK](#)

Big Data Security Analysis (BSA)

Four rows of configuration for BSA:

Server Address	Security Log Interface	Status Log Interface	Enable
<input type="text"/>	5666	5666	<input type="checkbox"/> Enable
<input type="text"/>	5666	5666	<input type="checkbox"/> Enable
<input type="text"/>	5666	5666	<input type="checkbox"/> Enable
<input type="text"/>	5666	5666	<input type="checkbox"/> Enable

[OK](#)

Other

Interface Version: 3.0.5.37838

Interface Upgrade Time:

Interface Update: [Browse](#) [Upgrade](#)

Debugging Information: [Click to Obtain](#)

Step 2 Configure parameters.

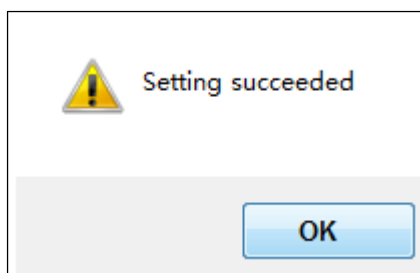
Table 3-1 Parameters for configuring WAF to connect to ESPC

Parameter		Description
WAF	Local IP	Specifies the IP address of WAF.
ESPC	You can select any line to configure an ESPC.	
	Server Address/Port	IP address and port of ESPC.
	Data Transmission	After the Enable check box is selected, WAF connects to ESPC and can send data to the latter.

Step 3 Click **OK**.

A dialog box appears, indicating the configuration success.


Figure 3-3 Configuration success message



Step 4 Click **OK**.

Then WAF is registered with ESPC.

You can also manually review a device for registration with ESPC. For details, see section "Device Review" in the *NSFOCUS ESPC User Guide – Device Management*.

 <p>Note</p>	<p>After ESPC detects WAF and adds it, the status of ESPC is displayed as Connected.</p>
--	---

----End

Verification

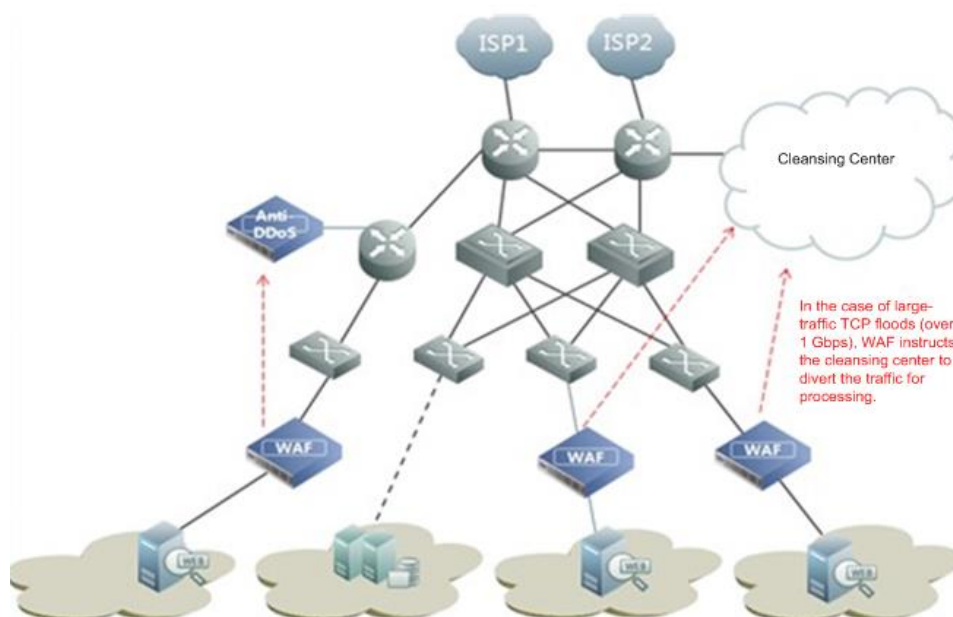
After WAF is successfully identified by ESPC, you can see the information about the device on the **Status List** page under **Device Management > Device List**. This means WAF will upload log information to ESPC in real time.

3.2 Connecting to NSFOCUS ADS

Scenario

In the network environment shown in [Figure 3-4](#), if a server behind WAF suffers super large-volume distributed denial-of-service (DDoS) attacks, the uplink of WAF will be congested. To solve this issue, an NSFOCUS ADS is deployed upstream to collaborate with WAF. In this case, once traffic thresholds specified on WAF are exceeded, WAF sends a notification to ADS which will then divert the traffic for cleansing. This section describes how to configure the connection between WAF and ADS.

Figure 3-4 Topology for the connection between WAF and ADS



Preparation

Set the IP address of ADS to 10.30.2.115 and the management IP address of WAF to 10.30.29.1.

Configuration Roadmap

1. Configure the connection from ADS to WAF.
2. Configure the connection from WAF to ADS.
3. Verify the configuration result.

Configuration Procedure

Step 1 Configure the connection from ADS to WAF.

Perform the following steps on ADS:

- a. Choose **System > Local Settings > Collaboration Configuration**. On the **Collaboration Configuration** page that appears, click **Edit** and enable the ADS collaboration function.

Figure 3-5 Enabling ADS collaboration on the ADS device

System > Local Settings > Collaboration Configuration	
Collaboration Configuration ?	
Item	Value
Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Role	Upper-Level Device v
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- b. Click **OK** to return to the **Collaboration Configuration** page, as shown in Figure 3-6.

Figure 3-6 Collaboration Configuration page after ADS collaboration is enabled

Item	Value
Enable	Yes
Role	Upper-Level Device

Diverted IP Status List Lower-Level Device IP List Edit

- c. Click **Lower-Level Device IP List**.

The list of IP addresses from which traffic is diverted appears, as shown in Figure 3-7.

Figure 3-7 Viewing the list of IP addresses from which traffic is diverted

IP Address	Device ID	Expand to /24 Subnet Diversion	Status	Operation
10.30.2.235	EE4E-0475-A333-4096	No	Enable	

Add Back

- d. Click **Add** and set **IP Address** to the management IP address of WAF and **HASH** to the WAF hash, as shown in Figure 3-8.

Figure 3-8 Adding WAF

IP Address 10.67.3.87

HASH 7B13-8725-30B8-14DD

Expand to /24 Subnet Diversion ☐ Yes ☒ No

Server Status Enable

OK Cancel

- e. Click **OK** to complete the configuration.



In addition to the preceding basic settings, to enable an ADS device to coordinate with WAF, you need to configure the related routing protocols, injection interfaces, and injection routes as required. For details, see the related ADS device user guide.

After completing the configuration, click **Apply** in the upper-right corner of the page to commit the settings. Then click **Save** in the upper-right corner of the page to permanently save the settings; otherwise, the settings may be lost after the device is restarted.

Step 2 Configure the connection from WAF to ADS.

Perform the following steps:

- a. Enable ADS collaboration.

Choose **Security Management > Network-Layer Protection > Policy Enable-Disable**.


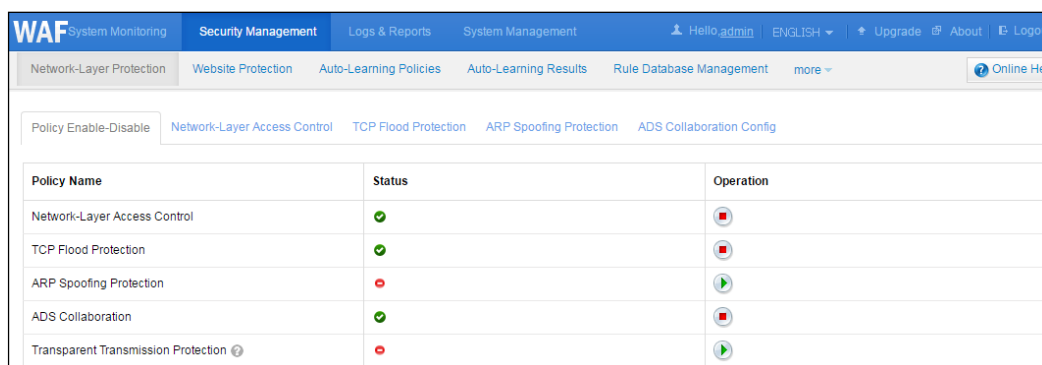





On the **Policy Enable-Disable** page that appears, click  to enable the ADS collaboration function, as shown in [Figure 3-9](#).

Figure 3-9 Enabling ADS collaboration on WAF



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

- b. Configure ADS collaboration parameters.

- Choose **Security Management > Network-Layer Protection > ADS Collaboration Config**.
- On the **ADS Coordination Config** page that appears, set the parameters, with **IP Address** of ADS set to the management IP address of the ADS device.

Figure 3-10 Editing ADS coordination settings

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

Diverged IP Status List

Basic Configuration

Collaboration with ADS ☒ Yes ☐ No

Running Mode Overall-Traffic Diversion ?

ADS IP and Port IP Address 10.30.2.72 Port 443 + Test

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

Overall Traffic ?

Statistic Dimension ☐ pps ☒ bps ☐ pps and bps

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

Advanced Options>>

OK

Diversion-Allowed IPs

Diversion-Allowed IPs 0.0.0.0-255.255.255.255 ?

OK

Diversion-Forbidden IPs

Diversion-Forbidden IPs ?

OK

Running Mode can be set to **Single-IP Diversion**, **Overall-Traffic Diversion**, or **Hybrid Diversion** as required.

Traffic Rate (pps) Notification Threshold must be set to a value that is greater than values of both **SYN Flood Notification Threshold** and **ACK Flood Notification Threshold**.

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

----End

Verification

Choose **Security Management > Network-Layer Protection > ADS Coordination Config**. Then, click **Test** on the **ADS Coordination Config** page that appears. If WAF successfully connects to the ADS device, **Connected** is displayed, as shown in [Figure 3-11](#).

Figure 3-11 Verifying the configuration result

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

Basic Configuration

Collaboration with ADS ☐ Yes ☒ No

Running Mode Overall-Traffic Diversion ?

ADS IP and Port IP Address 10.30.2.72 Port 443 + Test ✓ Connected

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

Overall Traffic ?

Statistic Dimension ☐ pps ☒ bps ☐ pps and bps

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

Advanced Options>>

OK

Diversion-Allowed IPs

Diversion-Allowed IPs 0.0.0.0-255.255.255.255 ?

OK

Diversion-Forbidden IPs

A Exporting the HTTPS Certificate

WAF supports the import of website certificates in PEM and PFX formats. As certificates cannot be encrypted by private keys or protected by passwords, different certificates are exported in different ways. The following describes how to export common web server certificates.

IIS

Select the virtual sites to be protected in Internet Information Services (IIS). Choose **Site Properties > Directory Security > View certificate > Detailed information** and click **Copy to File** to export the certificate. In the export wizard, select **Export the private key**, set the type of the certificate you want to export to **PKCS#12**, deselect **Enable strong protection**, and leave the private key blank.

Apache

To export an Apache certificate in the Linux system via OpenSSL, you can first obtain the certificate file path and the private key file path from the website configuration file or in the **ssl-mod** configuration file, and then export the certificate using one of the following methods:

Method 1

Run the following command to generate **server-key.pem**:

```
openssl rsa -in <SSLCertificateKeyFile-path> -out ./server-key.pem
```

Combine the generated **server-key.pem** and the file in the path specified by **<SSLCertificateFile-path>** file into a new file named **server.pem**. You can import this new file as a certificate to WAF.



You need to edit **server.pem** using UltraEdit or Notepad++ and save the edited file in a Linux-recognizable format. Otherwise, WAF considers this certificate invalid.

Method 2

Run the following command to export the Apache certificate:

```
openssl pkcs12 -export -inkey < SSLCertificateKeyFile-path> -in <
SSLCertificateFile-path> -out ./server.pfx
```

Where:

SSLCertificateKeyFile-path: indicates the path to the private key file of the certificate.

SSLCertificateFile-path: indicates the path to the certificate file.

You can import **server.pfx** as a new certificate to WAF.

WebLogic

The WebLogic server can use a PFX certificate or a PEM certificate.

- Exporting a PFX certificate

You can run the following command to remove private key protection:

```
openssl pkcs12 -nodes -in <CertificateFile-PFX> -out ./server.pem
```

- Exporting a PEM certificate

Make a PEM certificate following method 1 of Apache.

If the certificate chain (SSLCertificateChainFile of Apache) is configured, you only need to append the content in the certificate chain file to **server.pem**. That is, run the **openssl pkcs12 -export -inkey < SSLCertificateKeyFile-path> -in < SSLCertificateFile-path> -out ./server.pfx** command (in Method II of Apache) appended with **-chain <SSLCertificateChainFile>**.

B Default Parameters

B.1 Default Settings of the Management Interface

IP Address	eth0/M:192.168.0.1
Subnet Mask	255.255.255.0

B.2 Default Accounts

	User Name	Password
Web Administrator	admin	admin
Web Auditor	auditor	auditor
System Maintainer	maintainer	maintainer
Console Administrator	nsadmin	nsadmin

B.3 Communication Parameters of the Console Port

Baud Rate	115200
Data Bit	8
Parity Check	None
Stop Bit	1
Data Flow Control	None