SANGFOR

NGAF

Web Application Protection - Best Practice

Version 8.0.8

Change Log

Date	Change Description
July 2, 2019	Version 8.0.8 document release.

CONTENT

Chapter 1 Function Description

Web Application Protection (WAF) is a set of protection policies designed for Web servers in the local area network (LAN) of customers. It prevents Web application attacks including operating system (OS) command injections, Structured Query Language (SQL) injections, cross-site scripting (XSS) attacks and so forth, and configures Web servers to prevent data leakage.

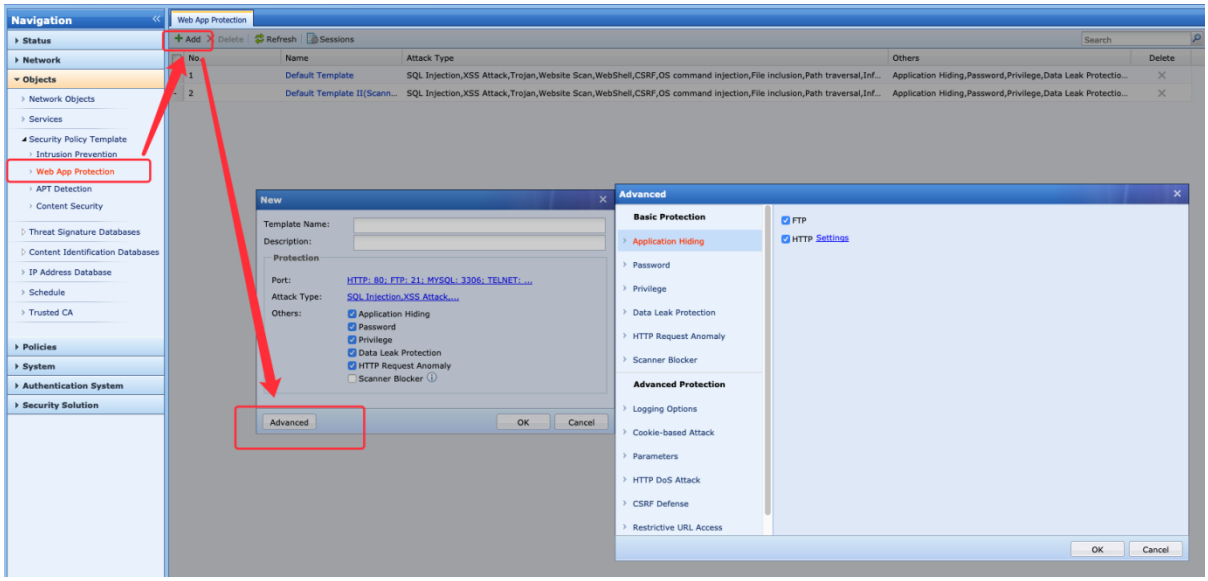
Chapter 2 Best Practices

Collect the detailed information of users' Web servers in advance, and customize protection policies for each Web according to their features. It is recommended that each Web business should have its own policy for ease of management and customization.

Note: To identify and protect an HTTPS-encrypted Web protocol, you need to decrypt the protocol first, instead of adding the port 433 or other HTTPS ports into the Web Application Protection policies.

1 Web Application Protection Policy Templates

Select "Web App Protection" under "Objects". In the right pane, click "Add" to create a new policy template. An example configuration is as follows:

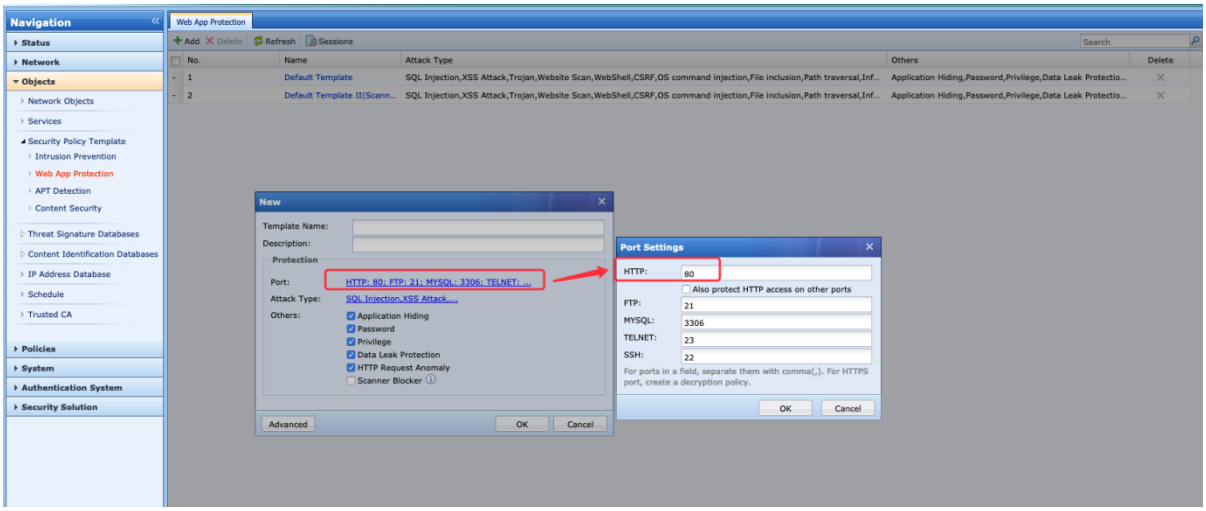


Note: It must be configured as follows to take effect. Choose "Policies" > "Network Security" > "Policies" to use the policy template you just created.

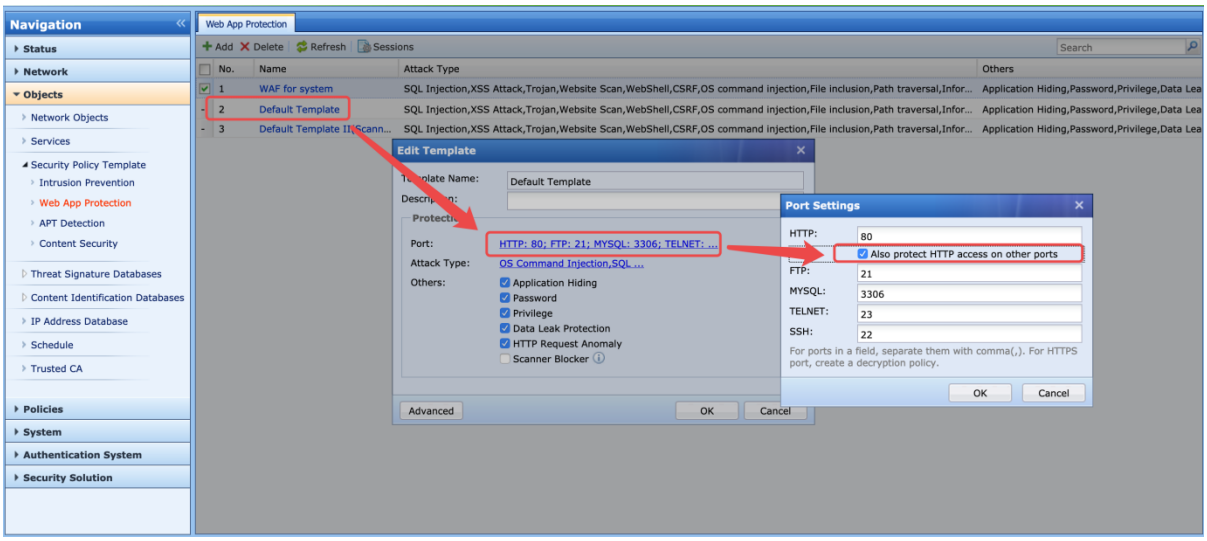
1.1 Identifying Web Ports

Web Application Protection policies by default take effect only for the standard HTTP port 80, while users often use non-standard HTTP ports. Therefore, the ports users actually use require attention during the delivery. If users use non-standard ports, there are two solutions:

- Add Web server ports that users actually use into Web Application Protection policies. This solution applies to the scenario where each Web server has a Web Application Protection policy. For example, if users use the port 8080 in a Web order system, you should configure a policy as follows:



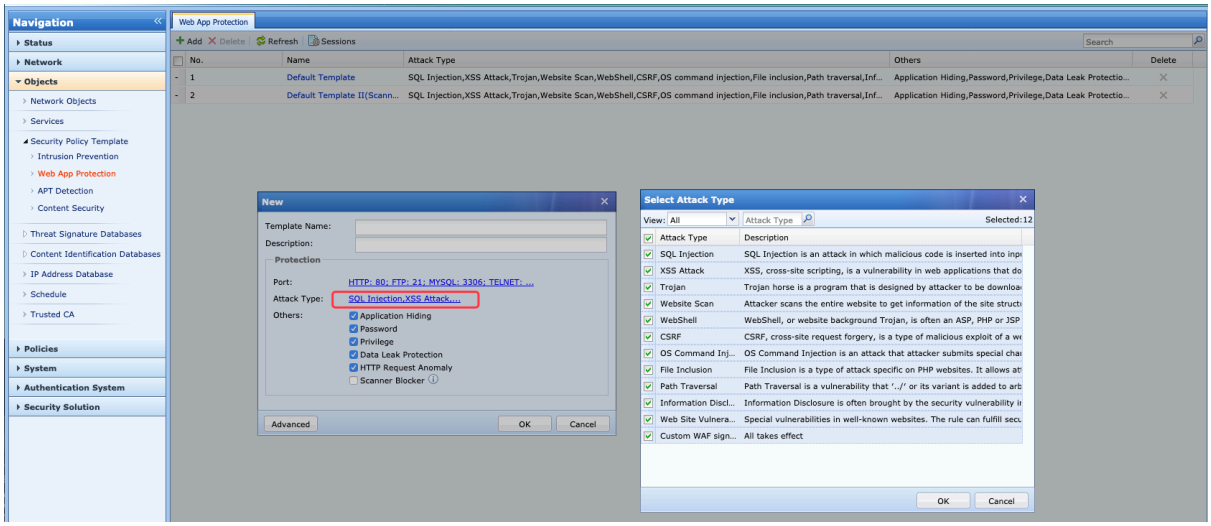
- Select the check box before "Also protect HTTP access on other ports". This solution applies to the scenario where a policy template is associated with and protects more than one Web server, and you cannot determine whether all Web servers use standard ports, or the port numbers each Web server actually uses. (This solution is recommended in version 7.2 or later. In earlier versions, this solution has flaws in identifying ports.) An example configuration is as follows:



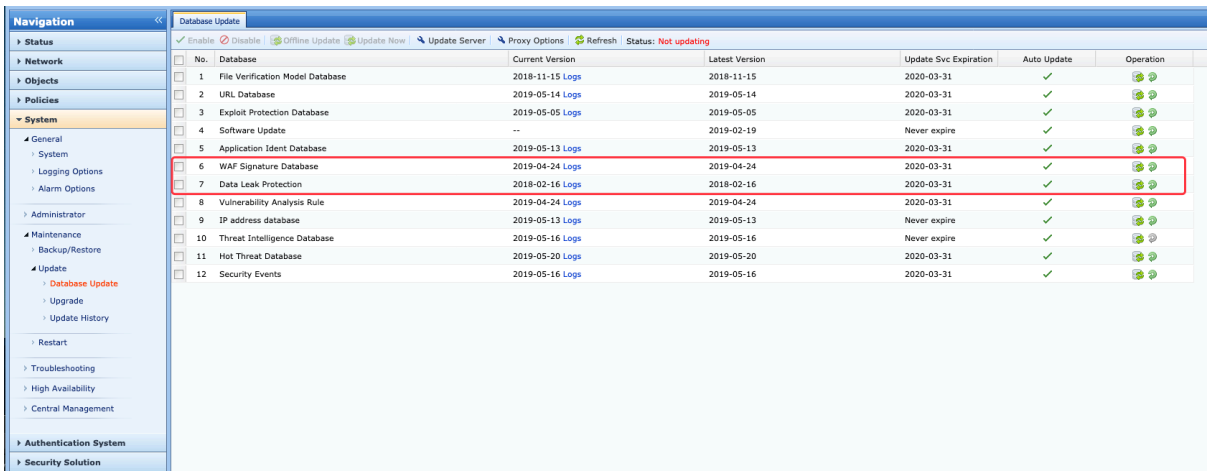
1.2 Selecting Attack Types

Web Application Protection guards against 11 types of common attacks, and provides protection based on one custom rule and one rule issued from cloud.

- You are recommended to select all attack types by default. Under special circumstances such as false identification, you are recommended to adjust the rules related to the problem rather than deselect all attack types. An example configuration is as follows:



- Based on the rules in the databases, Web Application Protection identifies and guards against all the types of attacks listed in the preceding figure. Each attack type covers several same type attacks. Therefore, the function of Web Application Protection is strongly associated with the rule databases of the device itself. You are recommended to check regularly for updates to the rule databases, as shown in the following figure:



1.3 Selecting Protection Types

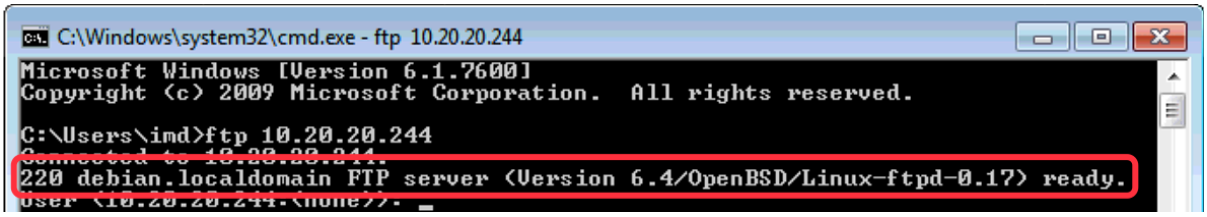
Attack protection based on behavioral characteristics currently includes application hiding, password protection, privilege control, data leak protection, HTTP request anomaly detection, and the scanner blocker. The behaviors of these types of protection need to be configured in the Advanced settings.

1.4 Advanced Settings - Application Hiding

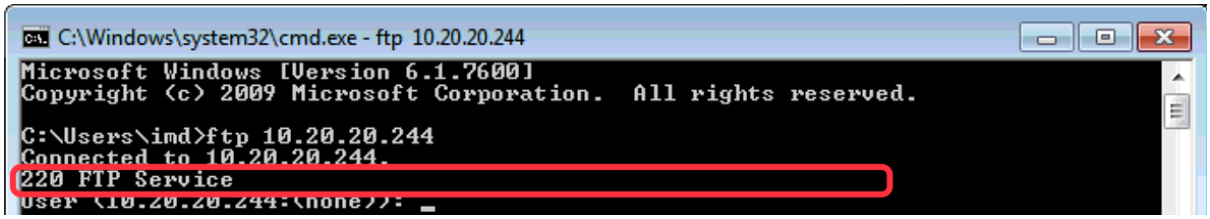
Application Hiding includes three functions: hiding the version information of FTP servers, hiding HTTP header fields, and replacing HTTP 4XX and 5XX error pages. The functions are explained as follows.

a) Select “FTP” to enable FTP application hiding, with no configuration parameters required, as shown in the following figure:

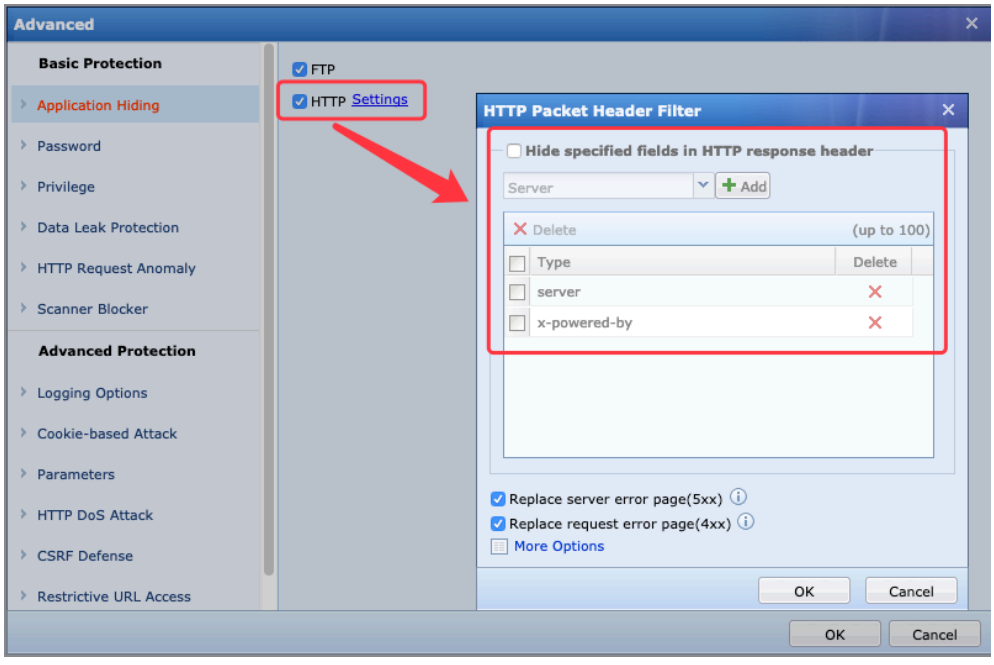
When FTP application hiding is **disabled**, the information of FTP servers is displayed as follows:



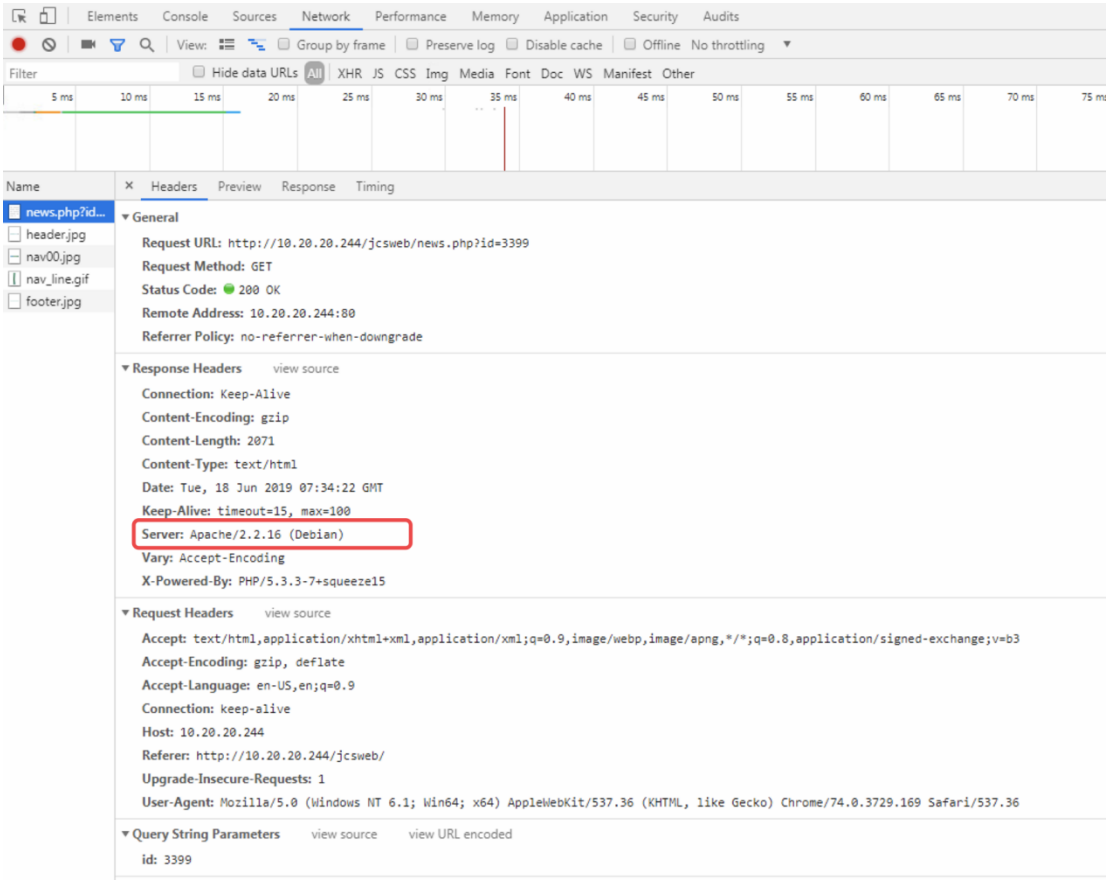
When FTP application hiding is **enabled**, the information of FTP servers is displayed as follows:



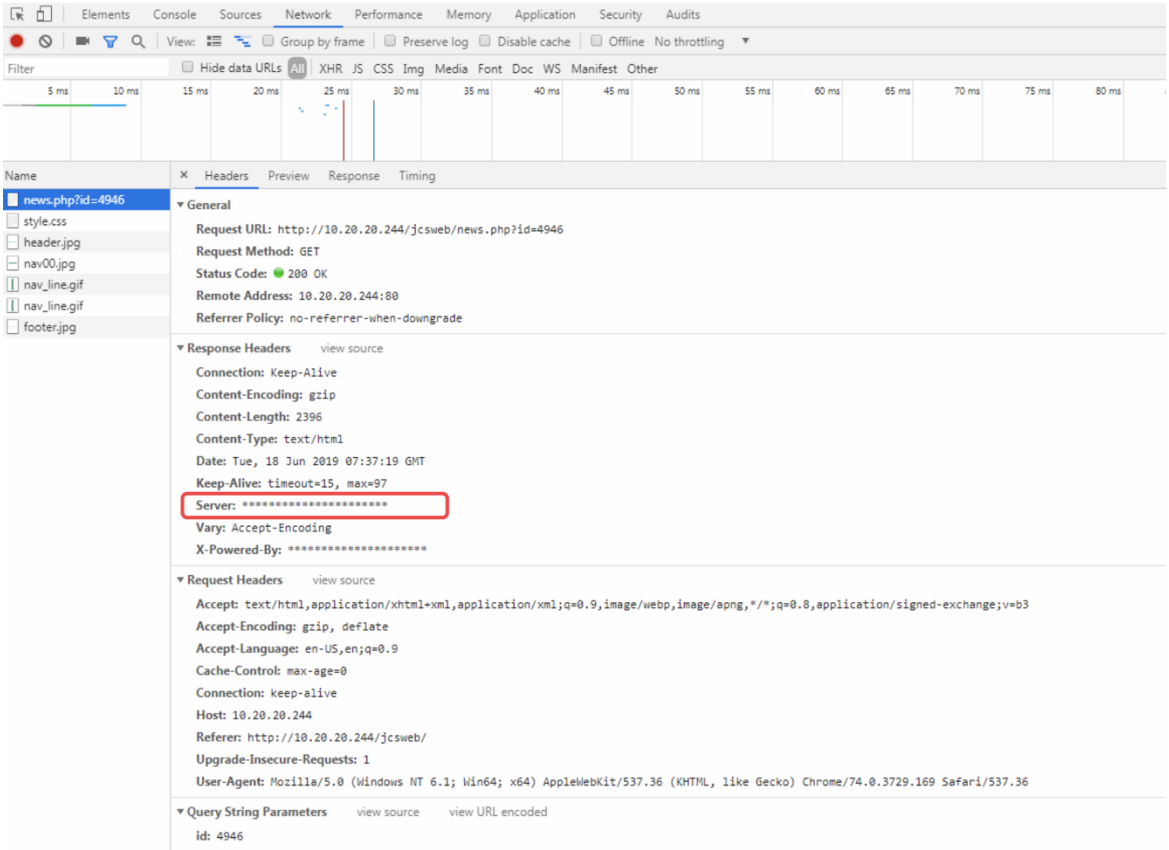
b) HTTP application hiding requires you to define HTTP header fields in advance. You are recommended to hide the "server" field and the "x-powered-by" field, and take caution in handling other fields to avoid interrupting business communications. An example configuration is as follows:



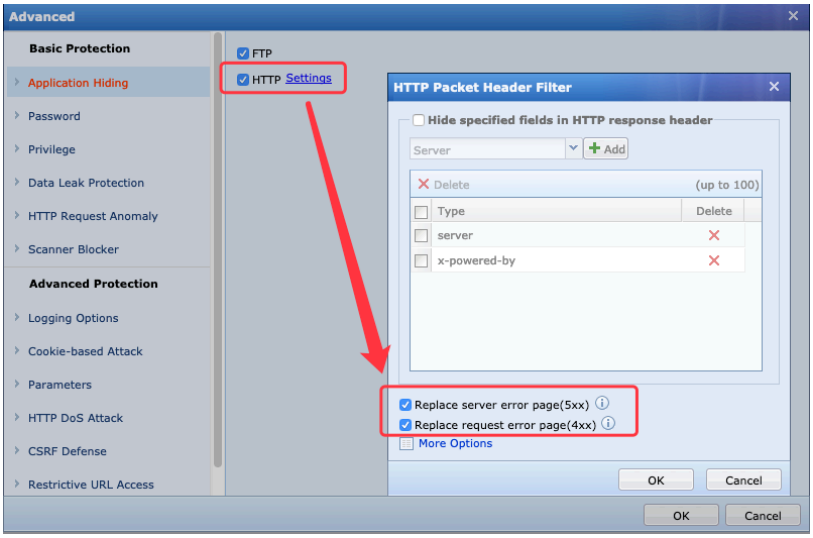
When HTTP application hiding is **disabled**, the information of response headers is displayed as follows:



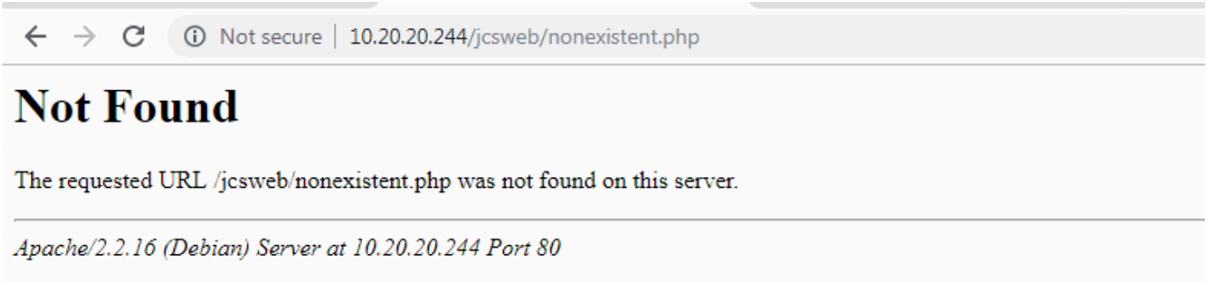
When HTTP application hiding is **enabled**, the information of response headers is displayed as follows:



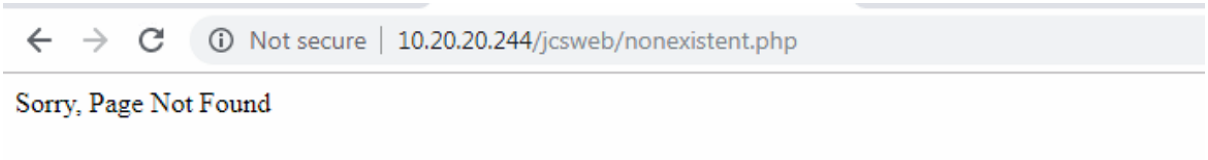
c) Enable the function of replacing the HTTP 4XX and 5XX error pages, as shown in the following figure:



When HTTP error page replacement is **disabled**, the error page is displayed as follows:



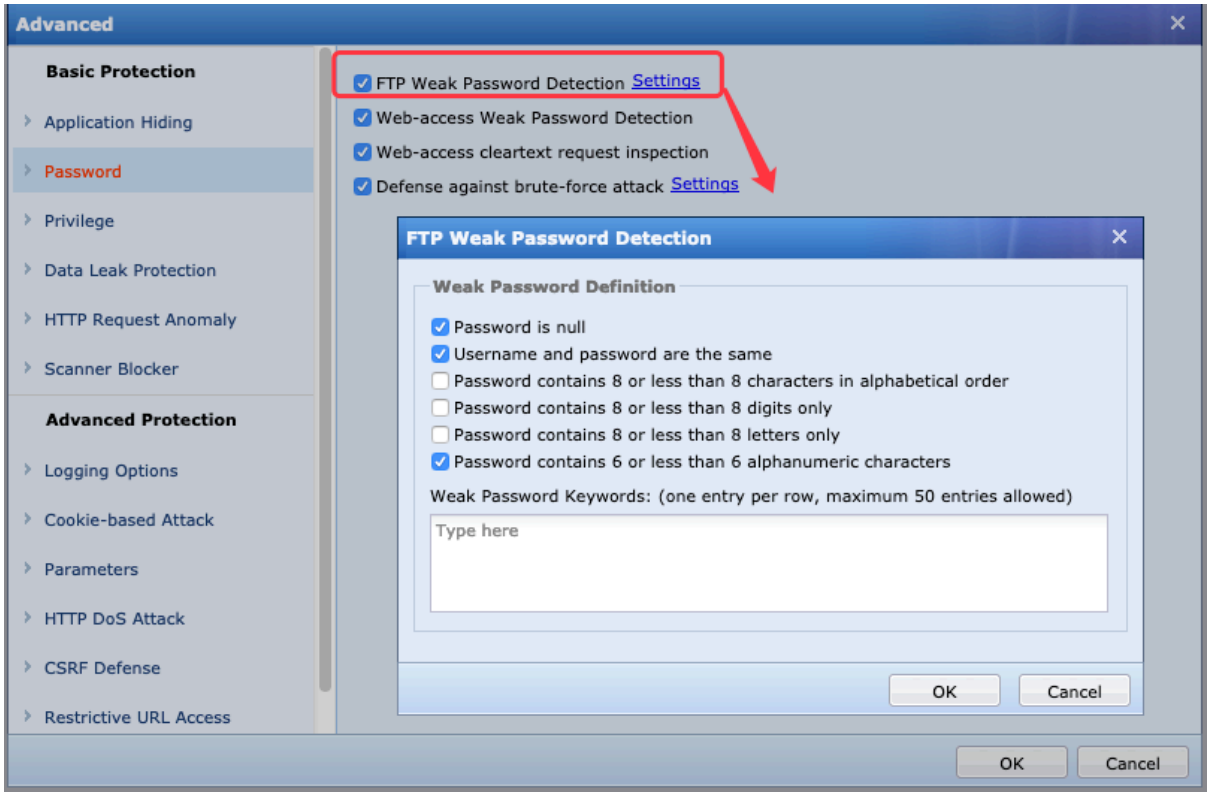
When the HTTP error page replacement is **enabled**, the error page is displayed as follows:



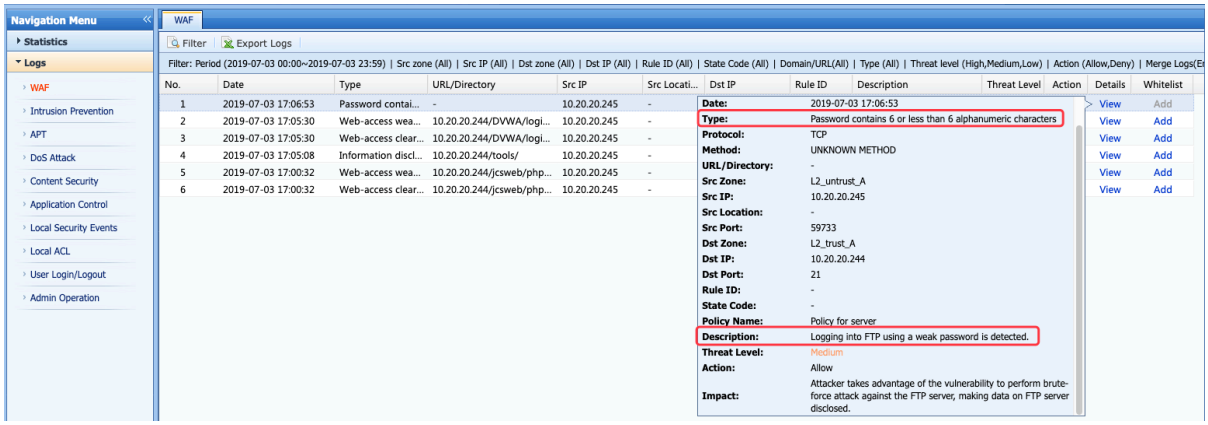
1.5 Advanced Settings - Password Protection

Password protection includes four functions: **FTP Weak Password Detection, Web-access Weak Password Detection, Web-access cleartext request inspection,** and **Defense against brute-force attacks**. The first three only have the function of detection instead of blocking. The functions are explained as follows.

a) **FTP Weak Password Detection** detects weak passwords used in FTP login. You can define rules of weak passwords in advance, as shown in the following figure:

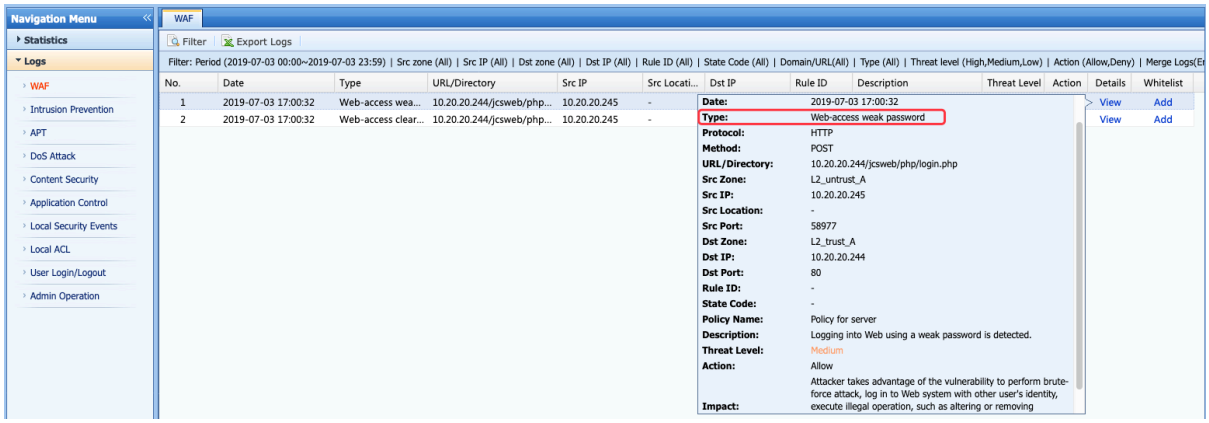


When **FTP weak password** detection is **enabled**, a log is displayed as follows:

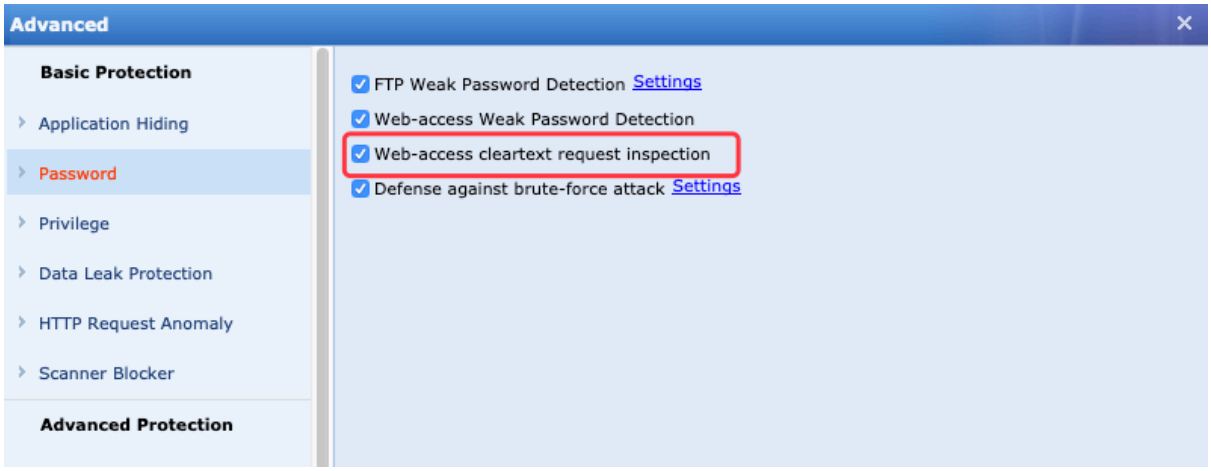


b) Web-access weak password detection has built-in weak password rules, so you do not need to configure any parameters. Select the check box before "Web-access Weak Password Detection" to enable the function, as shown in the following figure:

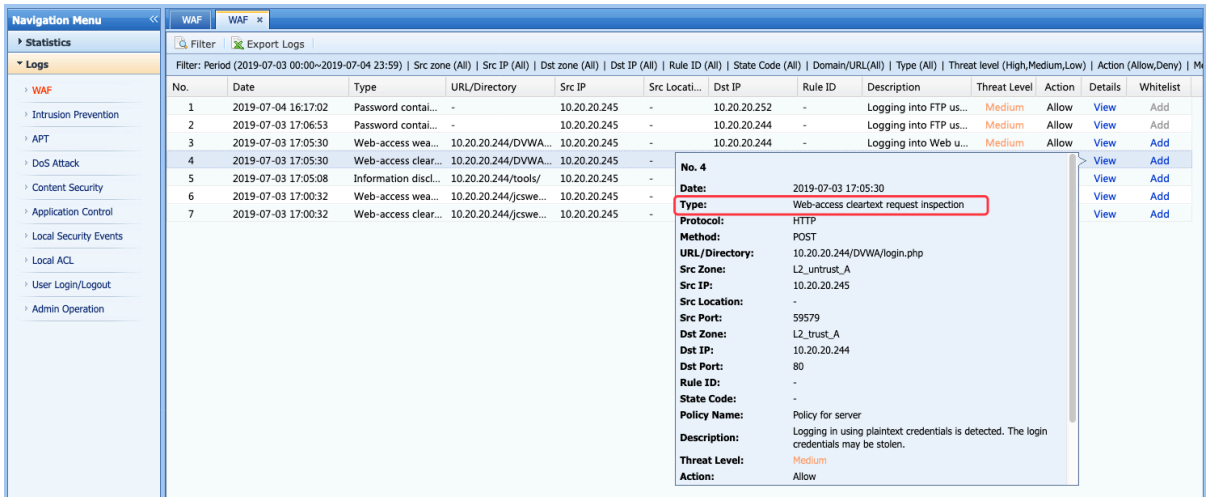
When **Web-access weak password detection** is **enabled**, a log is displayed as follows:



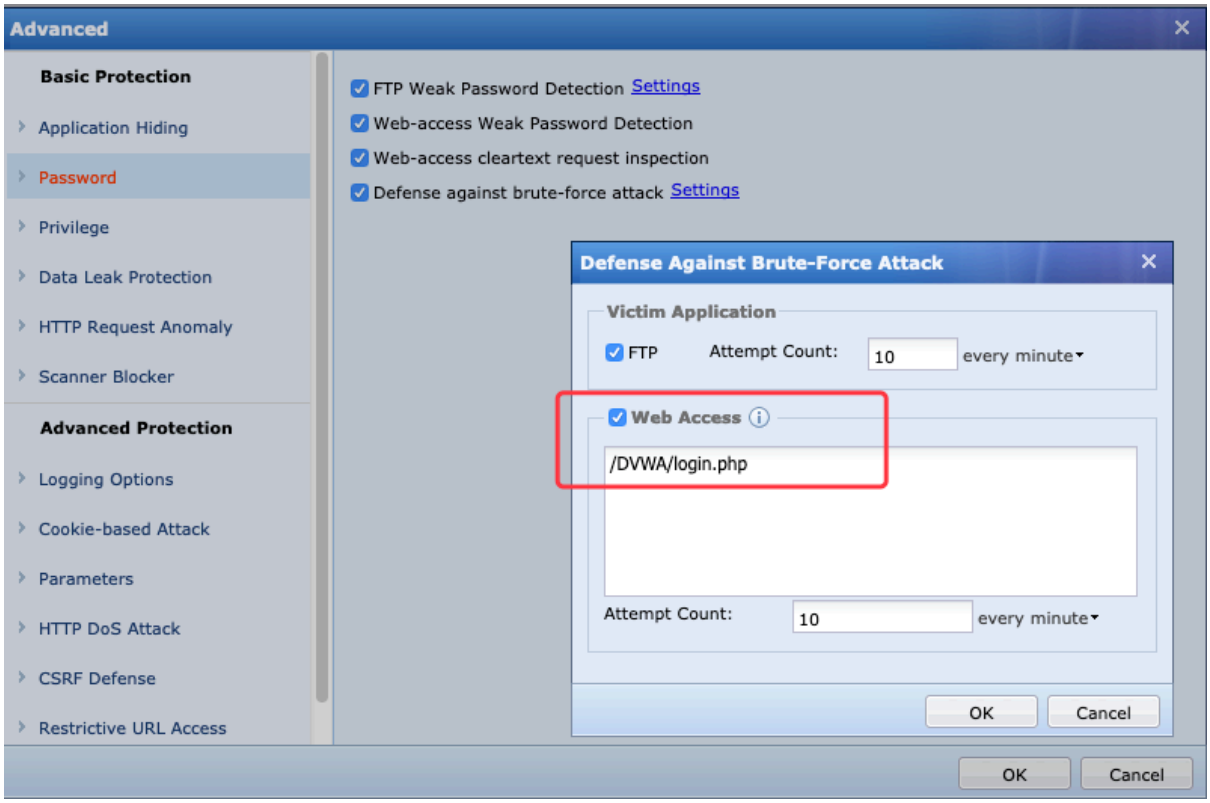
c) Select the check box before "Web-access cleartext request inspection" to enable the function, with no configuration parameters required, as shown in the following figure:



When **Web-access cleartext request inspection** is **enabled**, a log is displayed as follows:



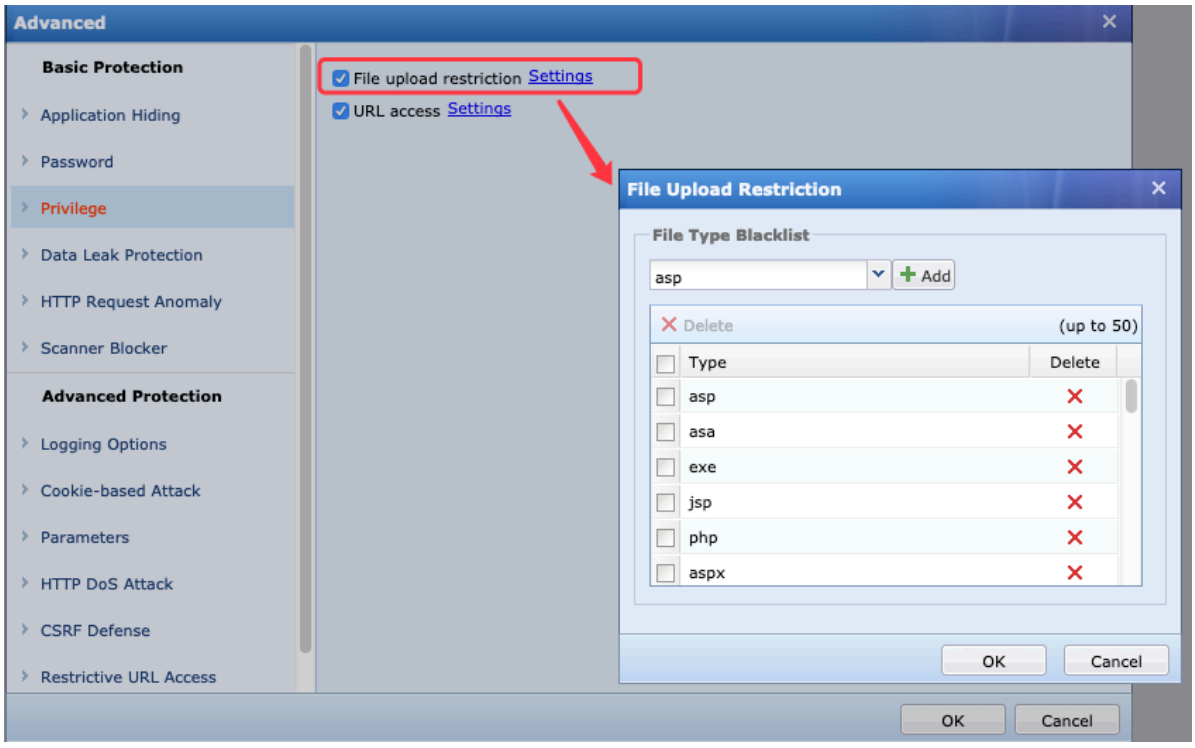
d) Defense against brute force attacks takes effect only for FTP and HTTP. When "FTP" is selected for "Victim Application", the default value of "Attempt Count" is "10" times per minute, which requires no modification except under special circumstances. When "Web Access" is selected, you need to configure the HTTP access address that requires protection. For example, if you need to protect the address "http://10.20.20.244/dvwa/login.php" from brute force attacks, do not change the default value of "Attempt Count", which is "10" times per minute. An example configuration is as follows:



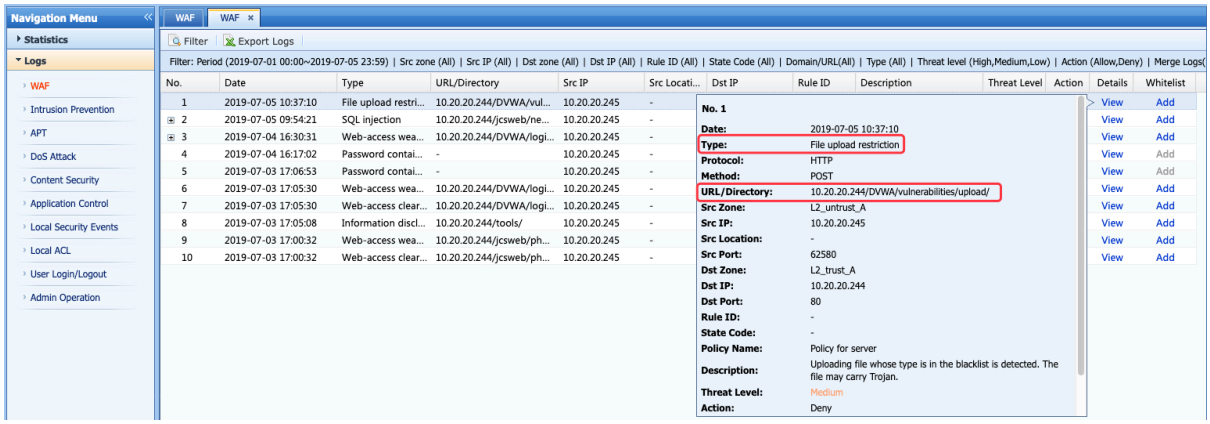
1.6 Advanced Settings - Privilege Control

Privilege control manages the privileges of specific files and URLs, including two functions: File upload restriction and URL access. The functions are explained as follows.

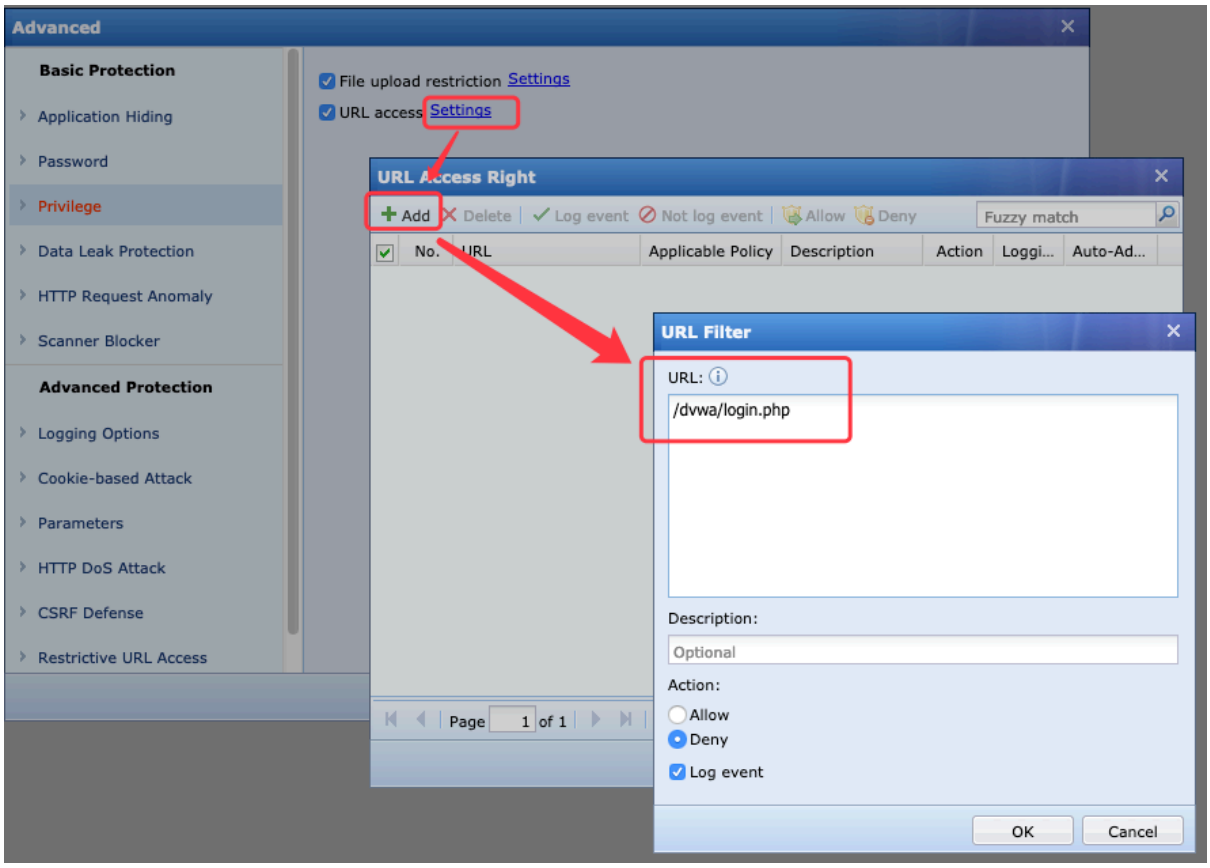
a) File upload restriction filters risky files by filename extensions and prevents them from being uploaded to servers. The blacklist contains several file types by default. If you need to add a new file type, enter the corresponding filename extension in the input box and click "Add", as shown in the following figure:



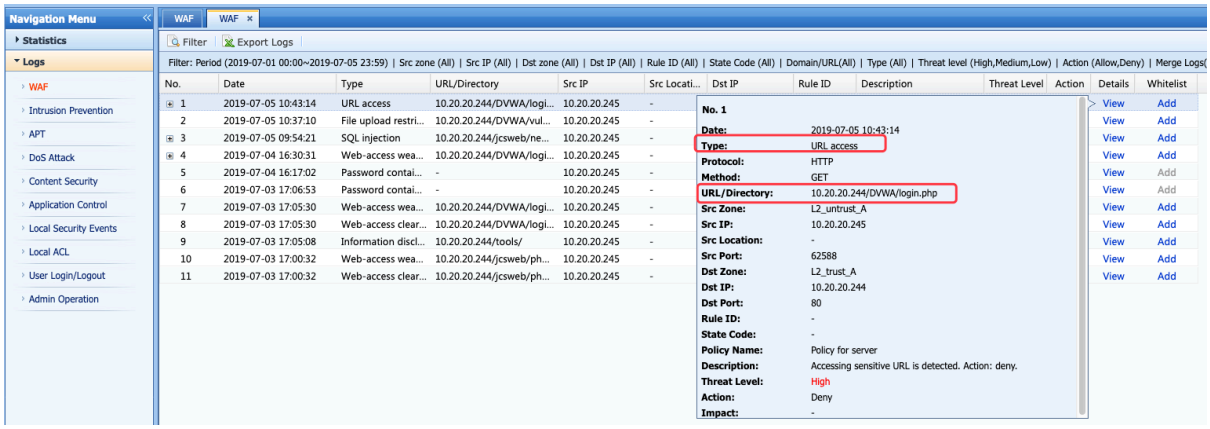
When **file upload restriction** is **enabled**, a log is displayed as follows:



b) URL access controls specific URLs. If you select "Allow" for "Action", the URL can be accessed, which is not affected by the Web Application Firewall (WAF); if you select "Deny" for "Action", any requests for access to the URL will be intercepted, which is also not affected by WAF, as shown in the following figure:

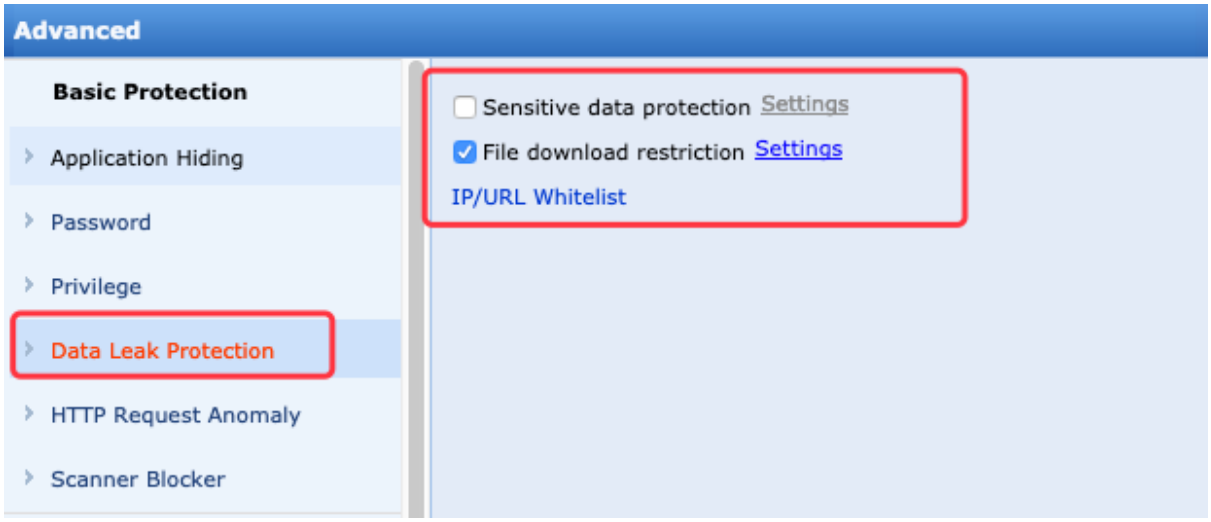


When **URL access** is **enabled**, a log is displayed as follows:

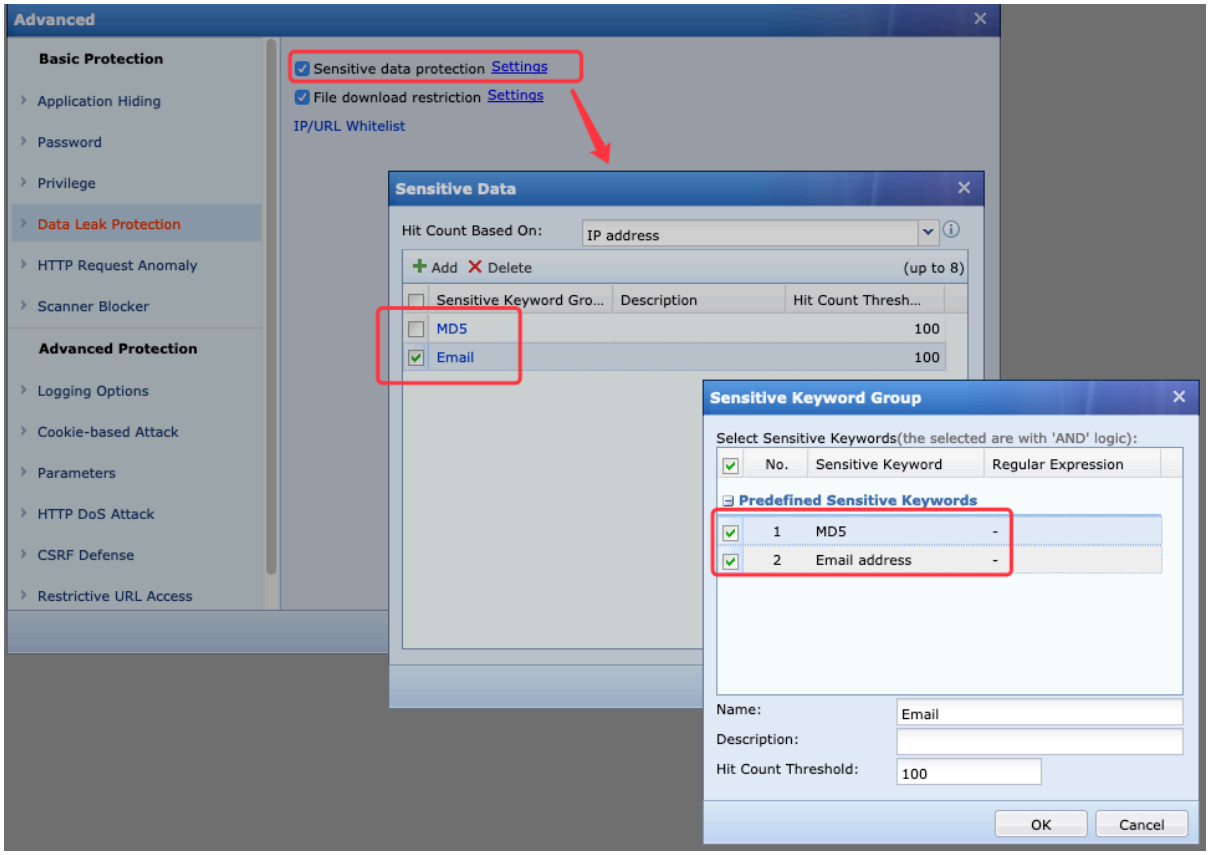


1.7 Advanced Settings - Data Leak Protection

Data leak protection controls sensitive data and downloaded files, including two functions: sensitive data protection and file download restriction. The functions are explained as follows.

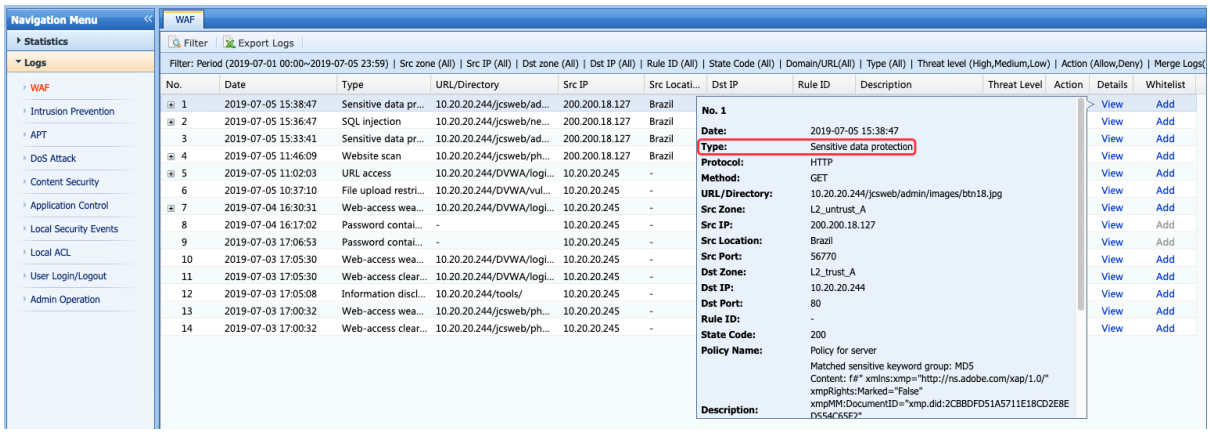


a) Sensitive data protection logs or intercepts the data packets that match with predefined sensitive keywords or sensitive keyword groups. An example configuration is as follows:

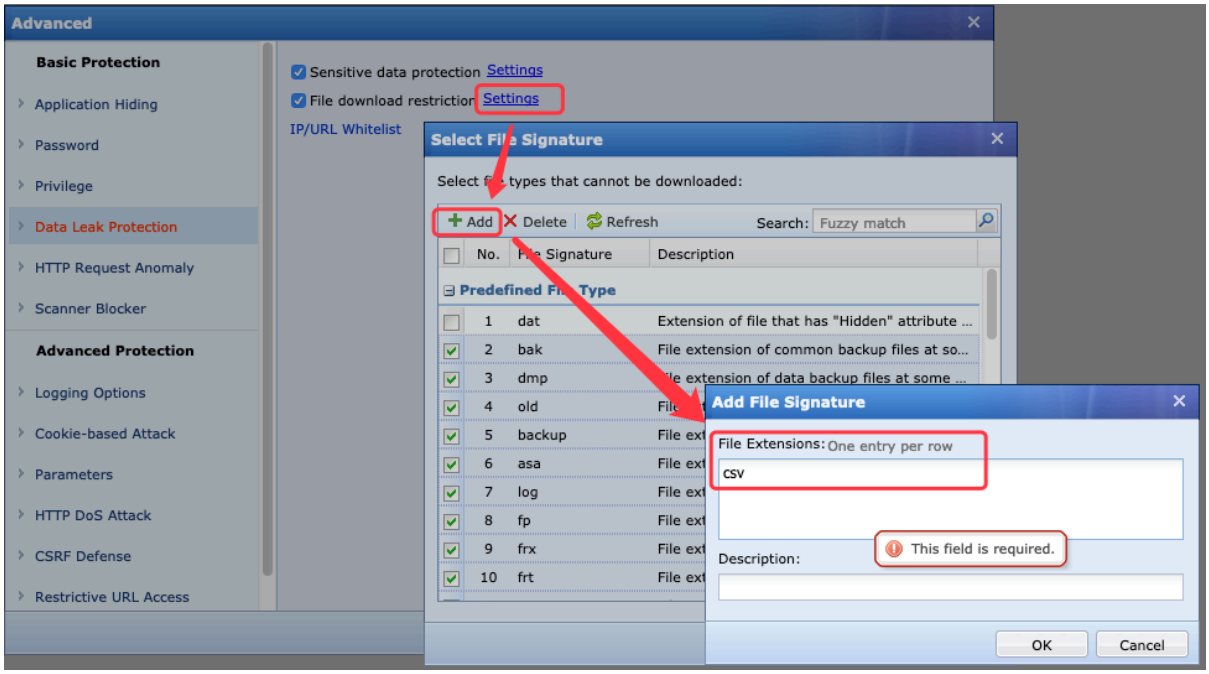


Note: A sensitive keyword group can be identified only when all the predefined sensitive keywords you have selected are matched. A piece of sensitive data can be identified when any one of the selected sensitive keyword groups is matched.

When **sensitive data protection** is **enabled**, a log is displayed as follows:

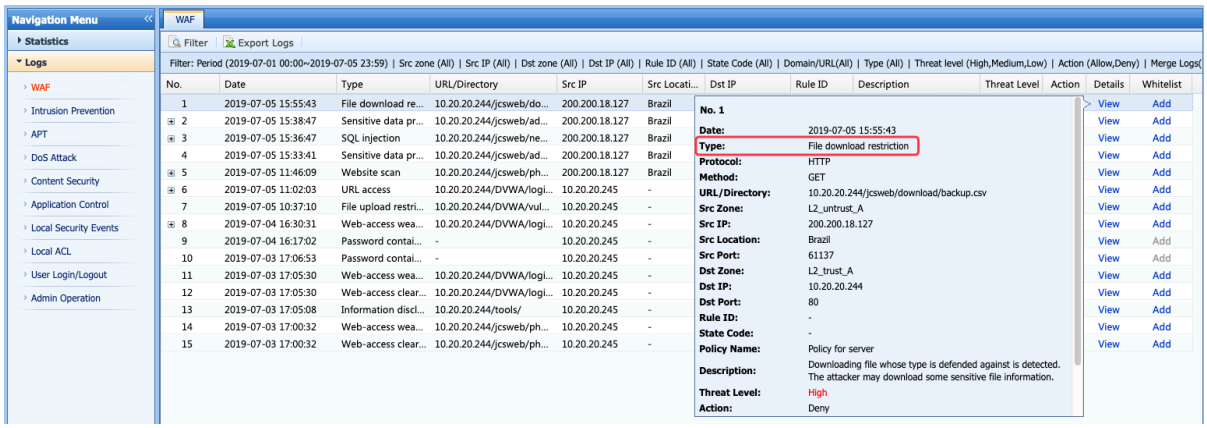


b) File download restriction filters risky files by filename extensions and prevents them from being downloaded. The blacklist contains several file types by default. If you need to add a new file type, click "Add" and enter the corresponding filename extension in the popped-up window, as shown in the following figure:



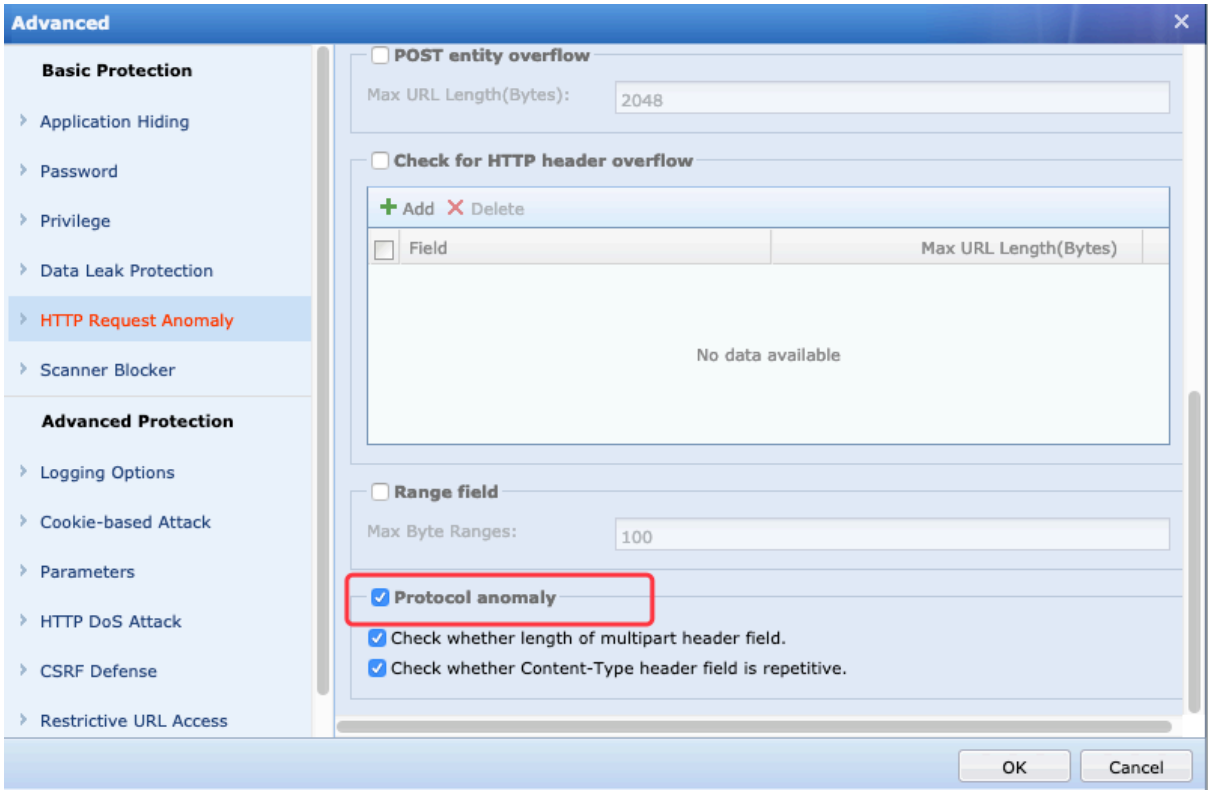
Note: To filter a specific type of files, you need to select the corresponding check box; otherwise, deselect it.

When **file download restriction** is **enabled**, a log is displayed as follows:



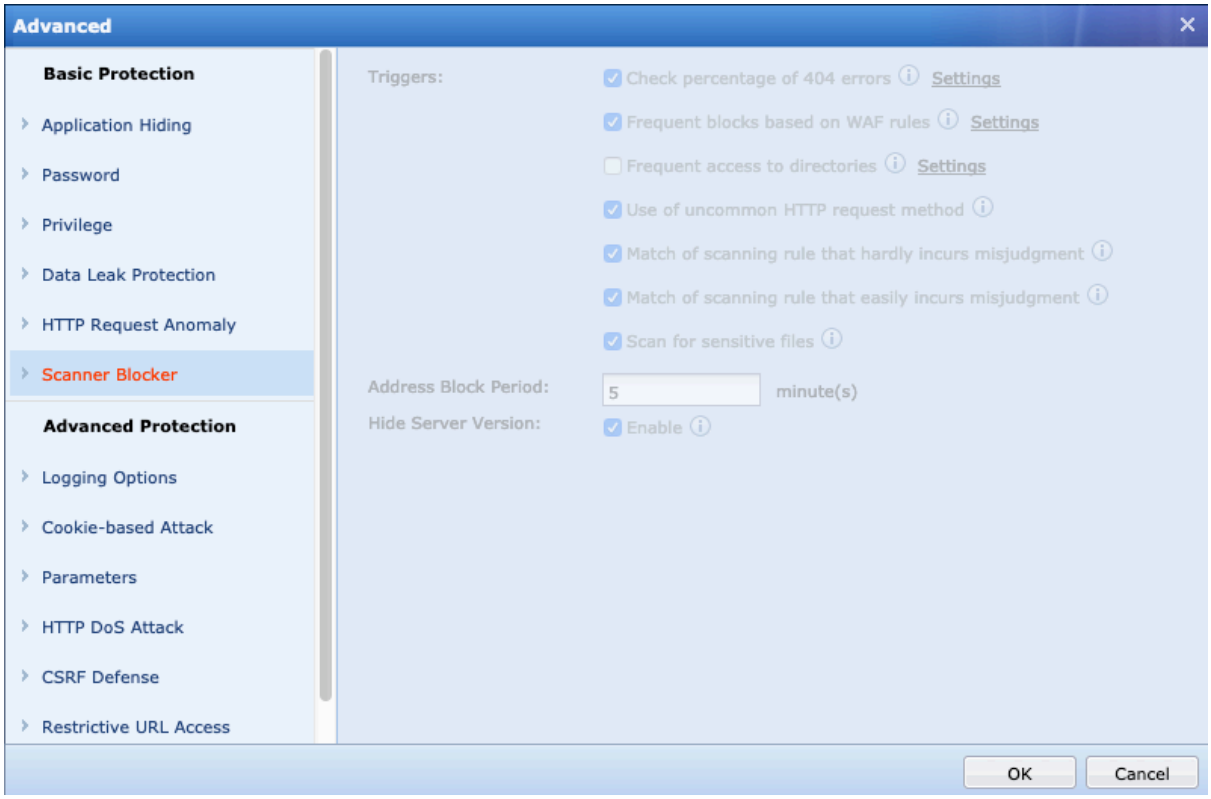
1.8 Advanced Settings - HTTP Request Anomaly Detection

HTTP request anomaly detection includes seven functions: request method, SQL injection through HTTP header, URL length detection, POST entity overflow detection, check for HTTP header overflow, range field, and protocol anomaly. "Protocol anomaly" detection is enabled by default. You are recommended to disable the function due to the frequent occurrence of false detection. You can remain default options unchanged for other functions, except under special circumstances.



1.9 Advanced Settings - Scanner Blocker

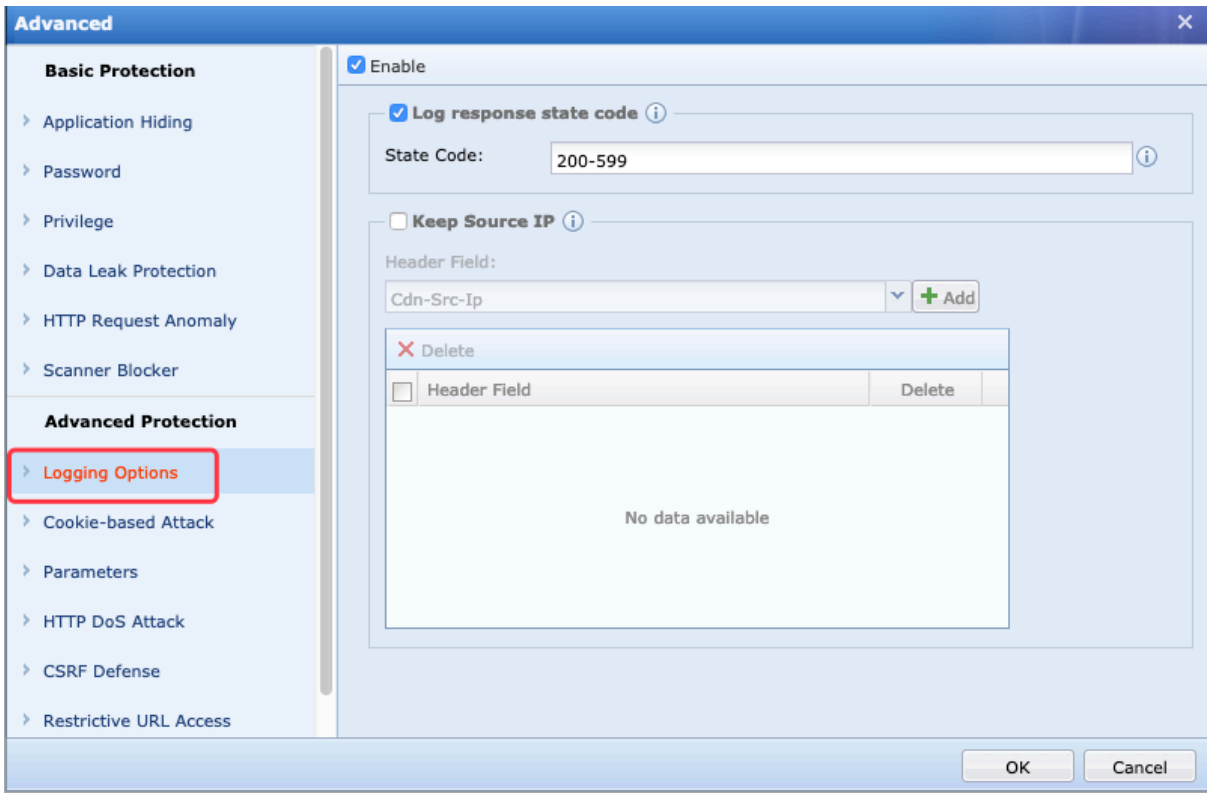
The scanner blocker blocks scanning operations of Web servers performed by external sources. The scanner blocker identifies an external source based on page threshold values, scanning rules, or scanning behavior characteristics. After identified, the IP address of the external source will be blocked for five minutes by default. During the block period, any requests from the IP address will be intercepted.



Note: When you need to block the notifications from a supervision and administration department, you must enable the function and remain the default threshold values unchanged.

1.10 Advanced Settings - Logging Options

Configure logging options for the logs that match with WAF policies, including logging response state codes and keeping source IP addresses. An example configuration is as follows:

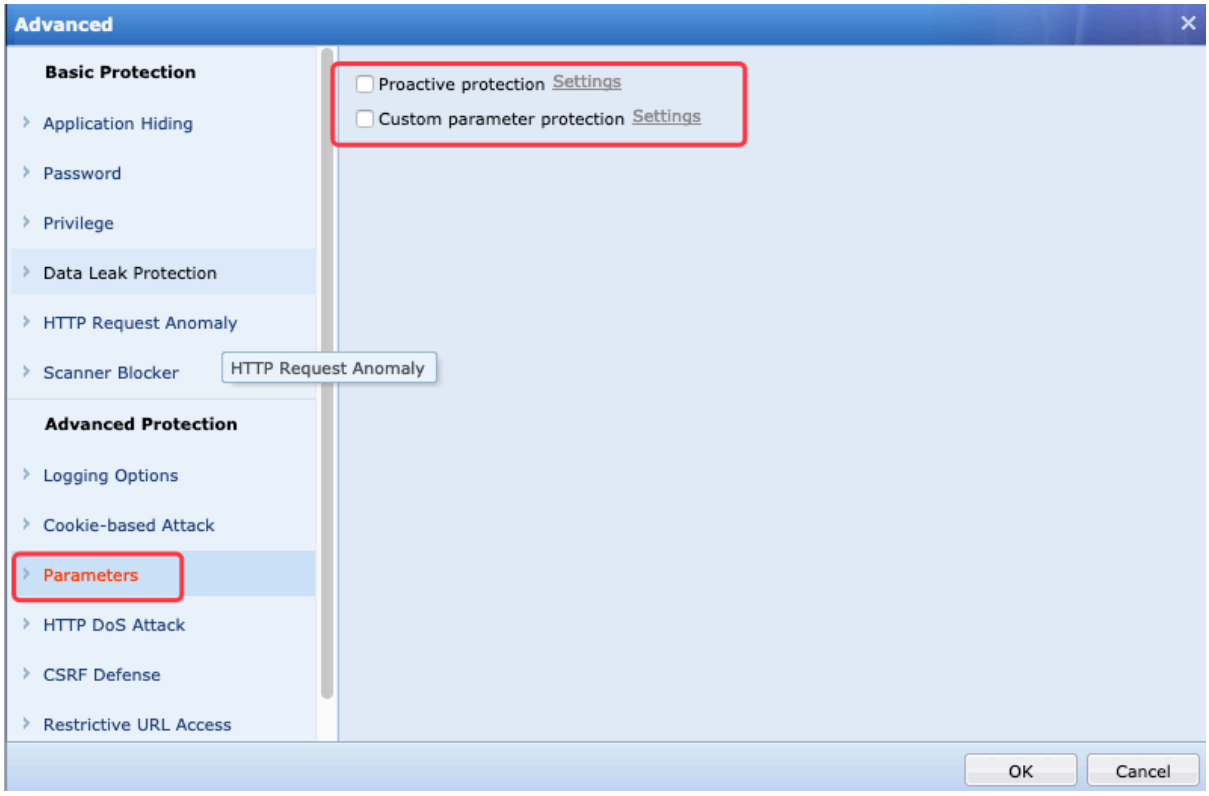


a) Configure the "Log response state code" option to specify the HTTP response state codes to be logged. You are recommended to remain the default settings unchanged.

b) Configure the "Keep Source IP" option to log the true source IP address by specifying the field of the true source IP address in the current session, when the source IP address does not change, and a proxy or SNAT is used.

1.11 Advanced Settings - Parameter

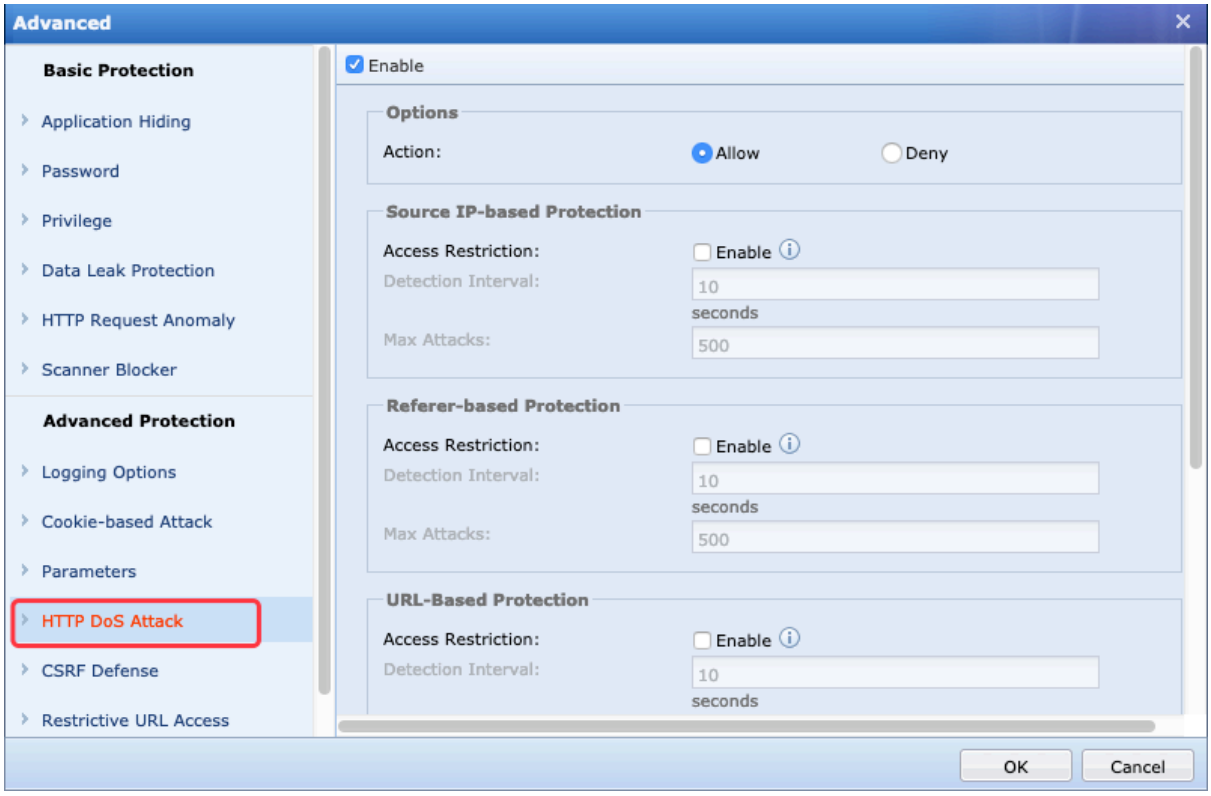
Parameter protection guards Web servers through device learning or custom parameter protection. Parameters that do no match with the criteria of protected fields are intercepted.



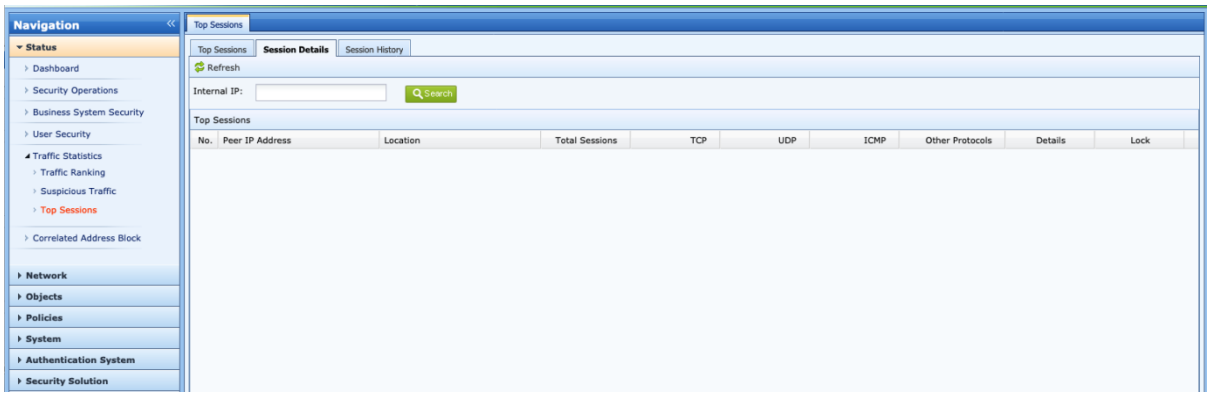
Note: You are not recommended to enable this function, except under special circumstances. Proactive protection takes effect for devices that have a CPU with more than four cores and more than four GB of memory.

1.12 Advanced Settings - HTTP DoS Attack

HTTP DoS attack protection guards websites from HTTP DoS attacks (Challenge Collapsar attacks). It includes four protection methods: source IP-based protection, referer-based protection, URL-based protection, and custom rule protection. An example configuration is as follows:



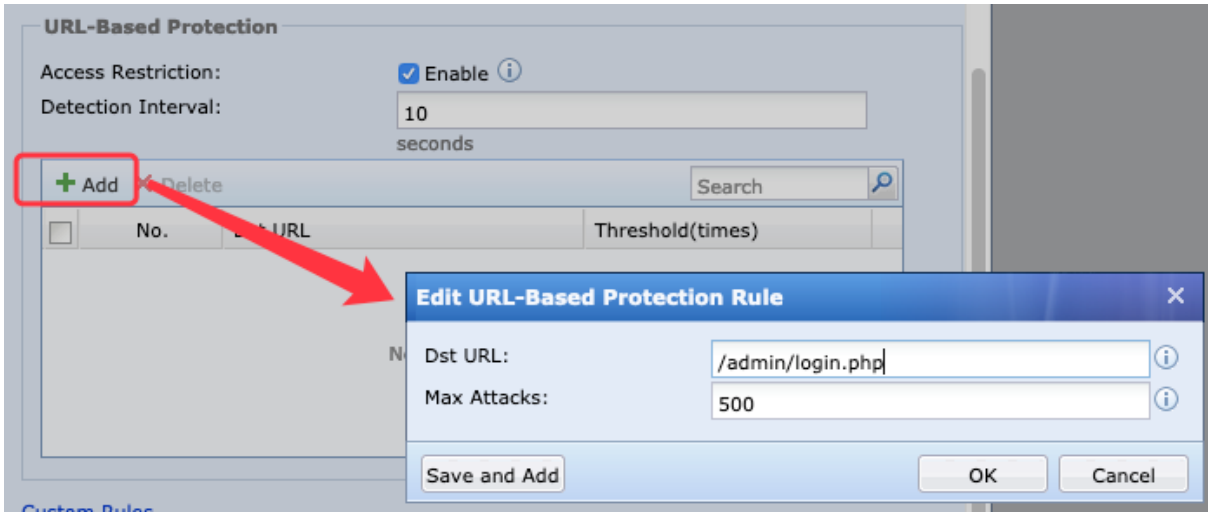
a) Source IP-based protection counts the number of access of a source IP address. If the number exceeds a threshold value, the source IP address will be added to a blacklist and its requests will be intercepted.



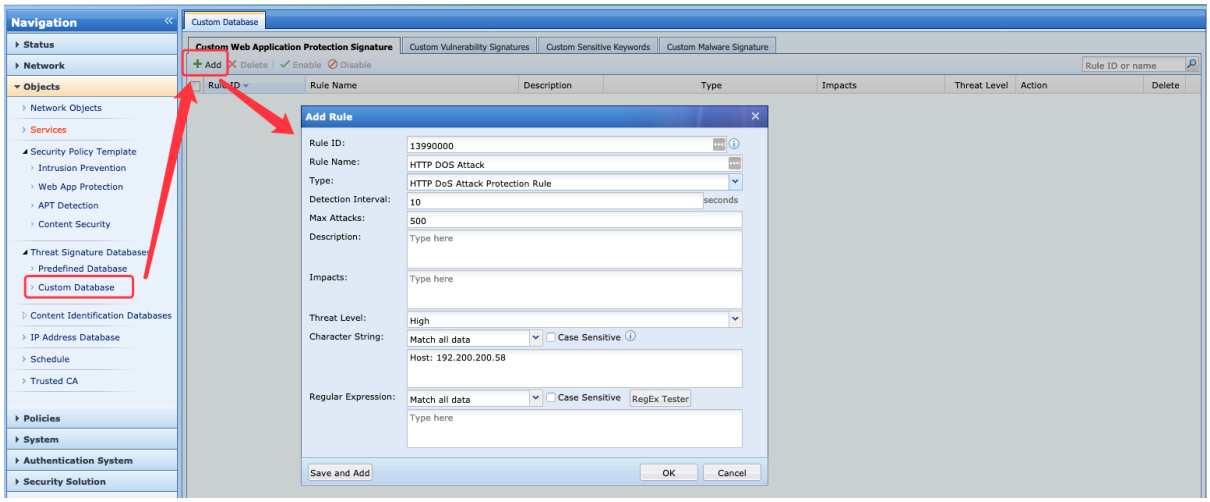
You should set the threshold value after consulting with customers. If customers cannot determine the threshold value, you can search the peak value of the busiest sessions of Web servers in customers' LAN in the right pane of session ranking as shown in the above figure. Then, you can set the threshold to a value higher than the peak value. You can also remain the default value unchanged.

b) Referer-based protection counts the number of access of HTTP addresses that contain the same URL in the referer field. If the number exceeds a threshold value, requests from any HTTP addresses that contain the same URL in the referer field will be denied.

c) URL-based protection protects a URL by counting the number of access of a source IP address to the URL. If the number exceeds a threshold value, the source IP address will be added to a blacklist and its requests will be intercepted.

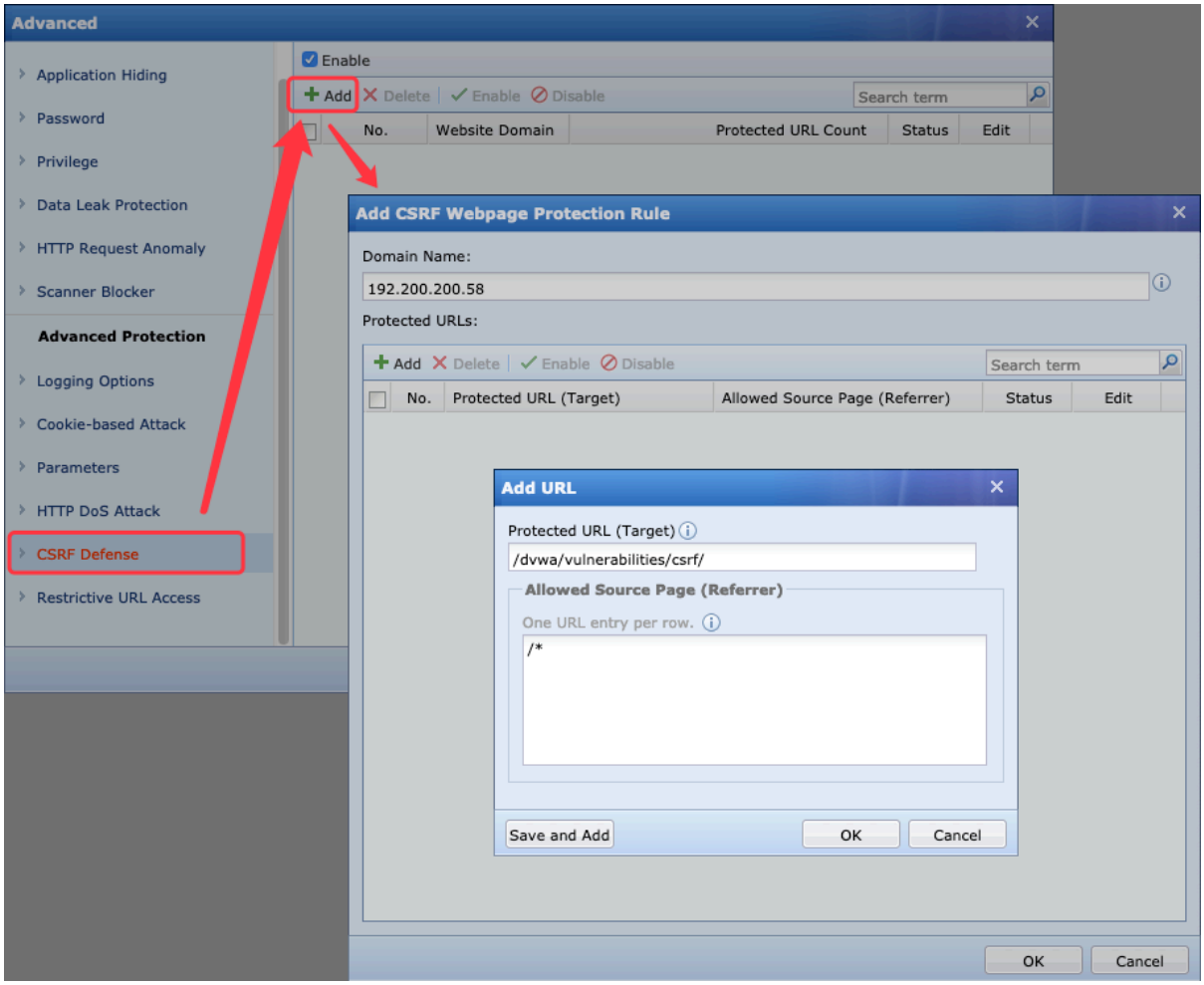


d) Custom rule protection allows you to define rules of HTTP DoS attacks in advance. A source IP address that matches with the rules will be added to a blacklist and its requests will be intercepted.



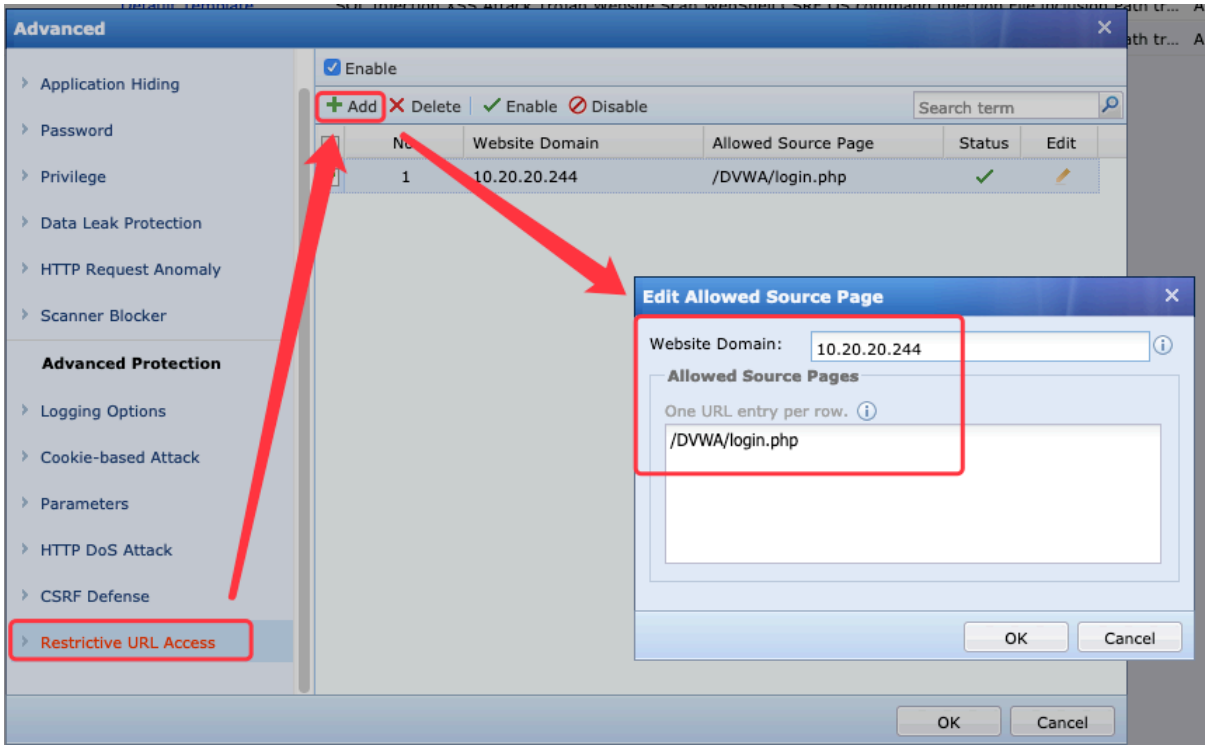
1.13 Advanced Settings - User Login Privilege Protection

If users want to access some specific Web pages, such as background login pages, they need to pass the short message service (SMS) authentication, which means that the page can be accessed after users provide a phone number and a correct verification code sent to the phone. User access privilege control manages Web-access privileges and other access privileges. An example configuration is as follows:

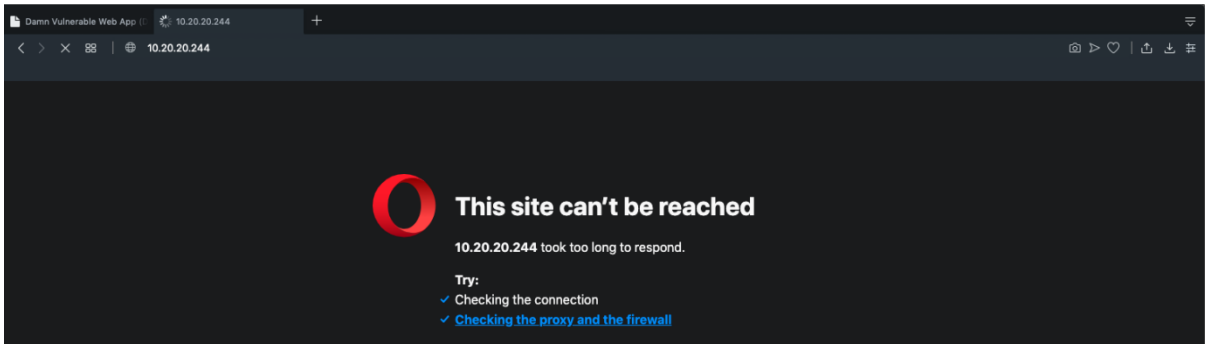


1.14 Advanced Settings - Restrictive URL Access

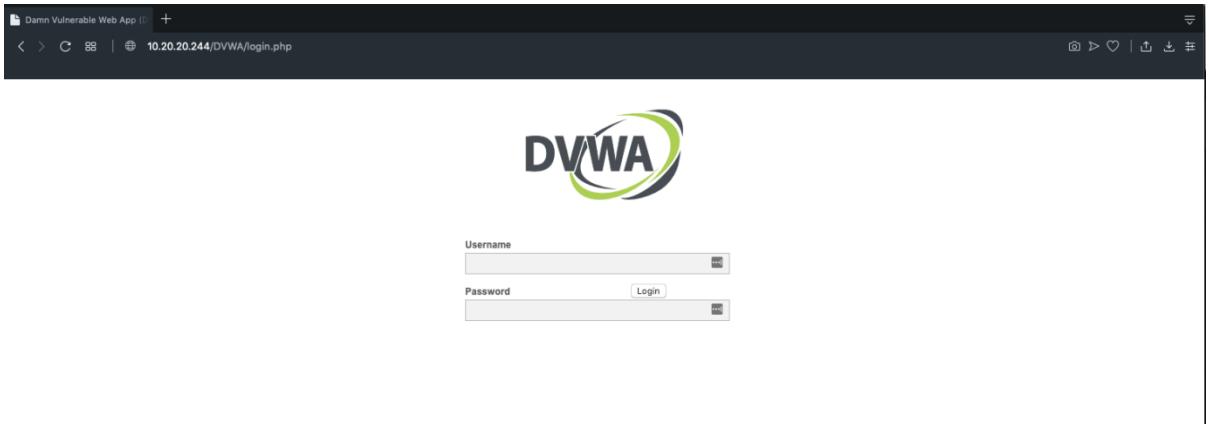
Restrictive URL access protects key addresses of a website from being directly accessed by external sources. For example, the website address "http://10.20.20.244" only allows direct access from the page "/DVWA/login.php", so external sources cannot directly access it, as shown in the following figure:



When **restrictive URL access** is **enabled**, if you access http://10.20.20.244, the response is displayed as follows:



If you access http://10.20.20.244/DVWA/login.php, the response is as follows:

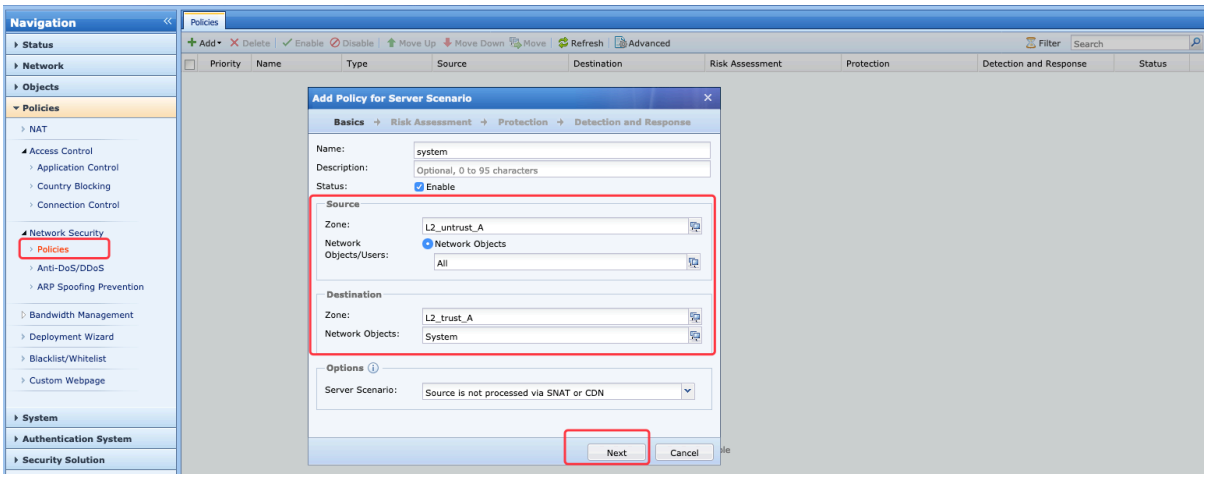


2 Using Template in Policies

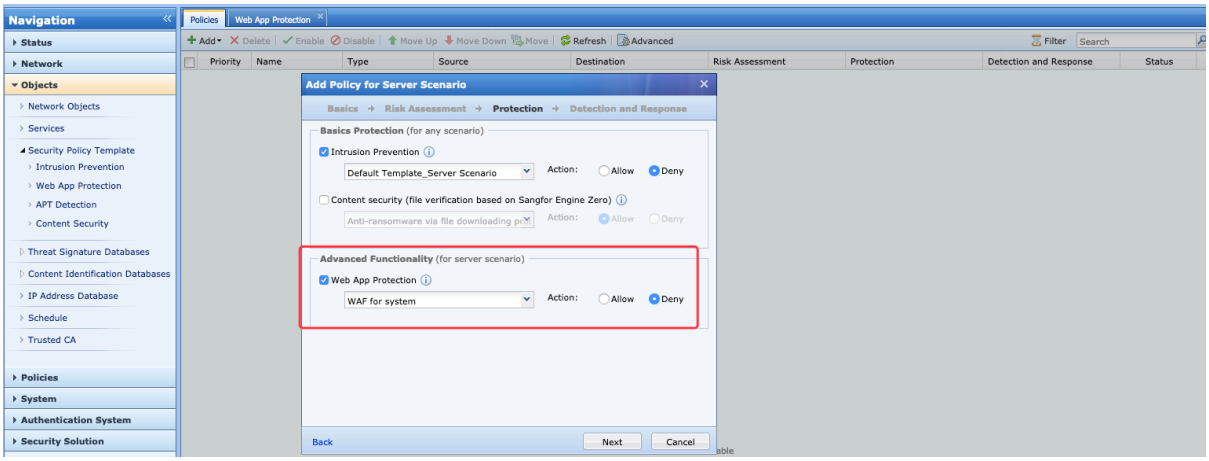
In the left pane, choose "Policies" > "Network Security" > "Policies". In the displayed right pane, click "Add". In the popped up window of "Add Policy for Server Scenario", specify the objects that require

protection and associate them with a template. For example, if you need to protect an order system and you have created a WAF template for the system according to the instructions in Chapter 2.1, you can perform the following steps:

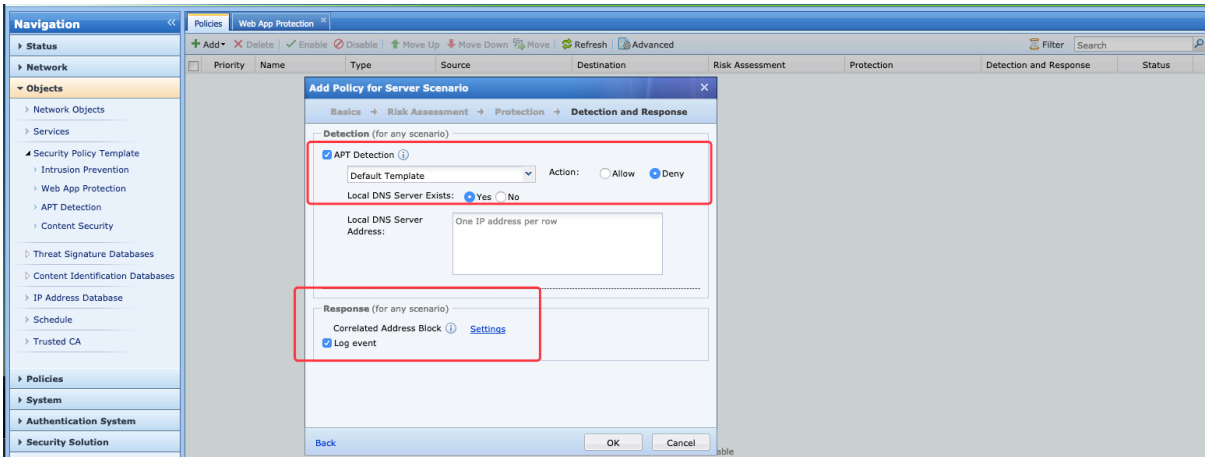
a) In the popped up window of "Add Policy for Server Scenario", specify the required information of the order system in the "Source" and "Destination" fields, as shown in the following figure:



b) Remain the default options unchanged for "Intrusion Prevention" and select the WAF template that you created for the order system for "Web App Protection", as shown in the following figure:



c) Select "Allow" or "Deny" for "Action" in the field of "APT Detection" according to the requirements of customers. Select "Log event" in the field of "Response". Then, click "OK", as shown in the following figure:



Chapter 3 Precautions

- The port numbers must be correct in a WAF template. If the port numbers are not correct and you have not enabled the automatic identification, the Web Application Protection functions defined by the template will become invalid.
- It is recommended that each of users' key services should have a template and a policy for ease of management and customization.

Chapter 4 Contact Us

Technical Support Email:	tech.support@sangfor.com
Technical Support Hotline:	International Service Centre: +60 12711 7129 (7511) Malaysia: 1700 81 7071 Hong Kong: +852 81257201 Singapore: +65 3152 9370 Other Regions: +60-12-7117511 (7129)
Technical Support Community:	http://community.sangfor.com
Official Website:	http://www.sangfor.com