# FortiADC - WAF Deployment Guide

Version 5.4.0

**FORTINET DOCUMENT LIBRARY**
https://docs.fortinet.com

**FORTINET VIDEO GUIDE**
https://video.fortinet.com

**FORTINET BLOG**
https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**
https://support.fortinet.com

**FORTINET TRAINING & CERTIFICATION PROGRAM**
https://www.fortinet.com/support-and-training/training.html

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://fortiguard.com/

**END USER LICENSE AGREEMENT**
https://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**
Email: techdoc@fortinet.com

February 4, 2020
FortiADC 5.4.0 WAF Deployment Guide
00-540-000000-20200204

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2019-09-04 | Initial release. |

# Introduction

To increase security in FortiADC, the following features have been added since the v5.3.0 release:

**CSRF protection**

Cross-site request forgery (CSRF) is an attack that exploits the trust that a site has in a user's browser to transmit unauthorized commands.

**Input validation**

Input validation can prevent suspicious HTTP requests, which include parameter validation, hidden fields, and file security.

**Brute force attack detection**

A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until the attacker discover the correct combination.

**Page anti-defacement**

The anti-defacement features monitors your web sites for defacement attacks. If it detects a change, it can automatically reverse the damage. The anti-defacement feature examines a website's files for changes at specified time intervals. If it detects a change that could indicate a defacement attack, the FortiADC appliance can notify you and quickly react by automatically restoring the website contents to the previous backup.

**Cookie security**

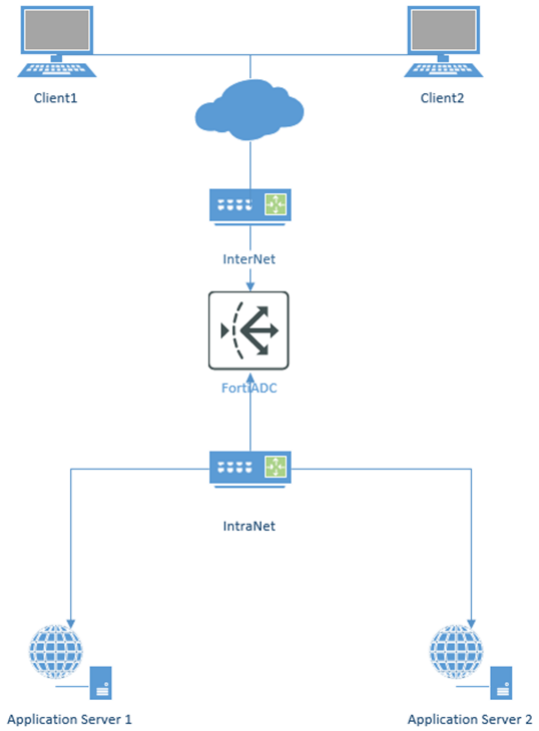
A cookie security policy allows you to configure FortiADC features that prevent cookie-based attacks and to apply them in a protection profile. For example, a policy can enable cookie poisoning detection, encrypt the cookies issued by a back-end server, and add security attributes to cookies.

**Data leak prevention**

The FortiADC data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. When you define sensitive data patterns, data matching these patterns will be blocked, or logged and allowed, when passing through the FortiADC unit.

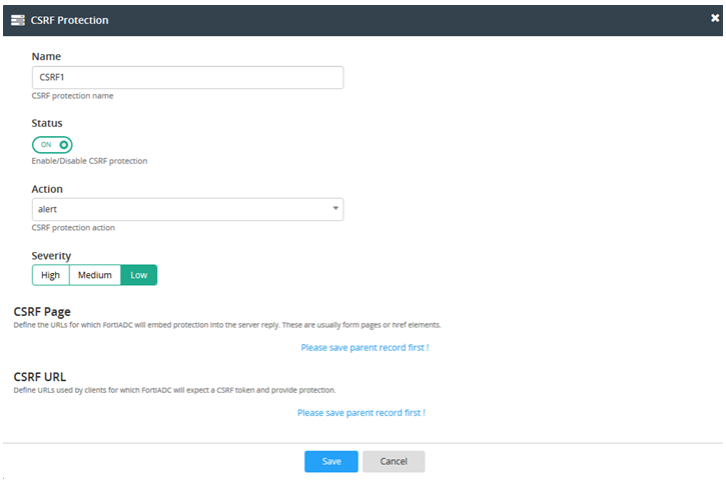
# Configurations

**Topology**

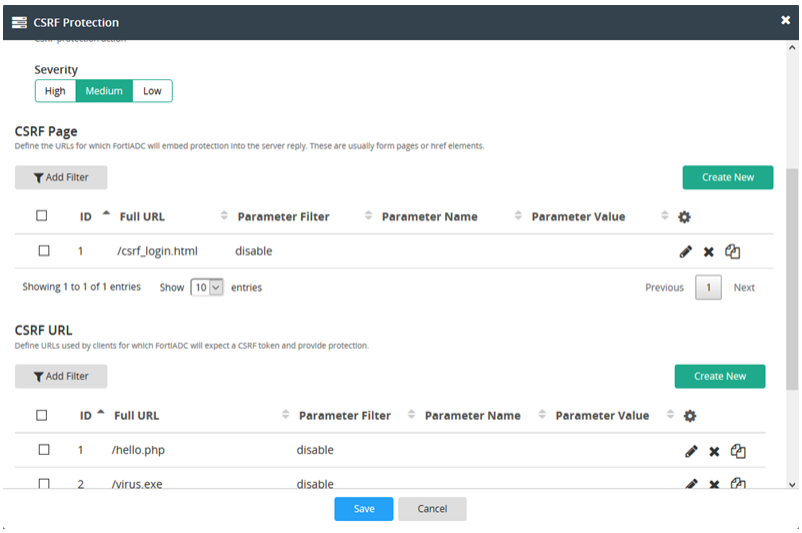



## To configure a CSRF Protection policy:

1. Go to **Web Application Firewall.**
2. Click the **Common Attacks Detection** tab.
3. Click the **CSRF Protection** tab
4. Click **Create New** to display the configuration editor.
5. Fill in the Name as “CSRF1”.
6. **Enable** the Status.
7. Modify the **Action** or **Severity** based on your requirements.
8. Click **Save** to save the configuration.




9. Click **Edit** to display the CSRF Protection.
10. Click **Create New** in CSRF Page to display the configuration editor and fill the Full URL Pattern and enable or disable Parameter Filter based on your security requirements.
11. Click **Create New** in CSRF URL to display the configuration editor and fill the Full URL Pattern and enable or disable Parameter Filter based on your security requirements.
12. Click **Save** to save the configuration.




13. To apply the CSRF Protection policy, select it in a WAF profile.

# Examples of requests with the anti-CSRF parameter

For example, a web page in the list of pages contains the following `<a href>` element:

```
<a href=/csrf_test.php>test</a>
```

This link generates the following request, which includes the parameter that the javascript has added:

http://example.com/csrf_test1.php?tknfv=3DF5BDCCIG3DCXNTE3RUNCTKRS3E36AD

Therefore, to make the feature work for this web page, you add /csrf_test.php to the list of URLs.

For an example using an HTML form element, the web page csrf_login.html contains the following form:

```
<form name="do_some_action" id="form1" action="hello.php" method="GET">
<input type="text" name="username" value=""/>
<Input type="text" name="password" value=""/>
<input type="submit" value="do Action"/>
</form>
```

This form generates the following request when the page is added to the list of pages protected by a CSRF protection policy:

http://target-site.com/hello.php?username=test&password=123&tknfv=3DF5BDCCIG3DCXNTE3RUNCTKRS3E36AD

In this case, you add csrf_login.html to the list of pages and /hello.php to the list of URLs.

# Troubleshooting

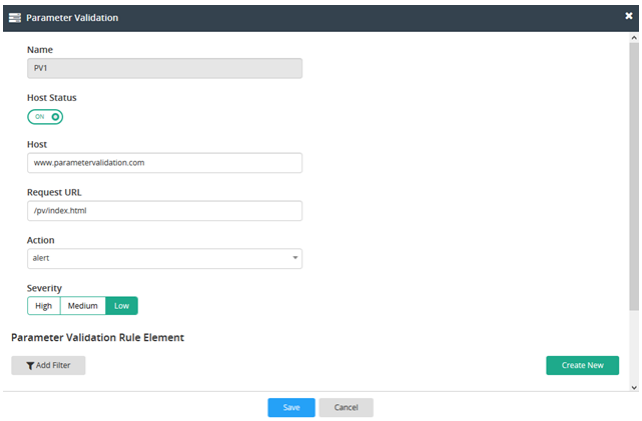
If the feature is not working properly, ensure the following:

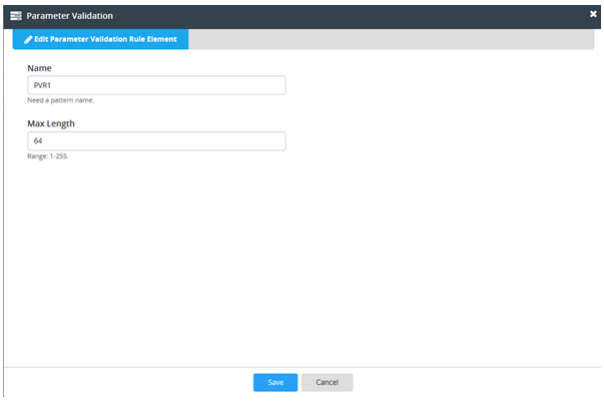
- The type of the web page to protect is HTML and contains the <html> and </html> tags.
- The HTTP response code for the page is 200 OK.
- If the page is compressed, a corresponding uncompressing policy is configured
- The Maximum Body Cache Size value is larger than the size of the web page.

# To configure an Input Validation policy

## To configure a Parameter Validation rule

1. Go to **Web Application Firewall**.
2. Click the **Input Validation** tab.
3. Click the **Parameter Validation** tab.
4. Click **Create New** to display the configuration editor and fill the Name, Host Status, Host, Request URL, Action, Severity, and Parameter Validation Rule Element based on your security requirements.
5. Click **Save** to save the configuration.



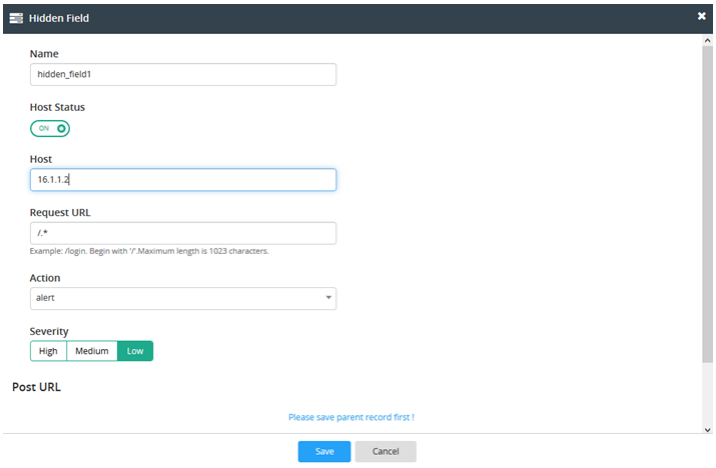

**Notes:** FortiADC checks the Host and Request URL by simple string or regular express matching.

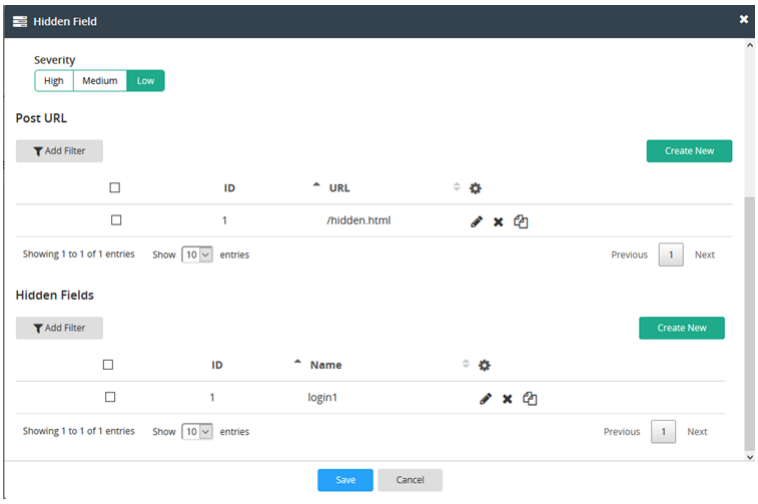
| | |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |
| Host Status | Enable to apply this input rule only to HTTP requests for specific web hosts. Also, configure Host.<br>Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the Host: field. |
| Host | Select which protected host names entry (either a web host name or IP address) that the Host: field of the HTTP request must be in to match the signature exception.<br>This option is available only if Host Status is enabled. |
| Request URL | Depending on your selection in Request URL Type, type either:<br>• the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash ( / ).<br>• a regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash ( / ).; however, it must at least match URLs that begin with a slash, such as /index.html. |
| Action | Select which action FortiADC takes when the conditions are fulfilled for File Restriction.<br>• Alert—Accept the request and generate an alert email, log message, or both.<br>• Deny—Block the request (or reset the connection).<br>• Block—Block subsequent requests from the client for a number of seconds. Also configure Block Period. |

| | |
|---|---|
| | • Silent-deny—Deny without log.<br>The default value is Alert. |
| Severity | When FortiADC records violations of this rule in the attack log, each log message contains a **Severity Level** (severity_level) field. Select which severity level FortiADC uses when using Input Validation:<br>• Low<br>• Medium<br>• High<br>The default value is **Low**. |
| Max Length | The maximum string length of the string that is the input's value. The default value is 64 characters. |

## To configure a Hidden Field rule

1. Go to **Web Application Firewall**.
2. Click the **Input Validation** tab.
3. Click the **Hidden Field** tab.
4. Click **Create New** to display the configuration editor and fill the Name, Host Status, Host, Request URL, Action, Severity, Post URL, and Hidden Fields based on your security requirements.
5. Click **Save** to save the configuration.



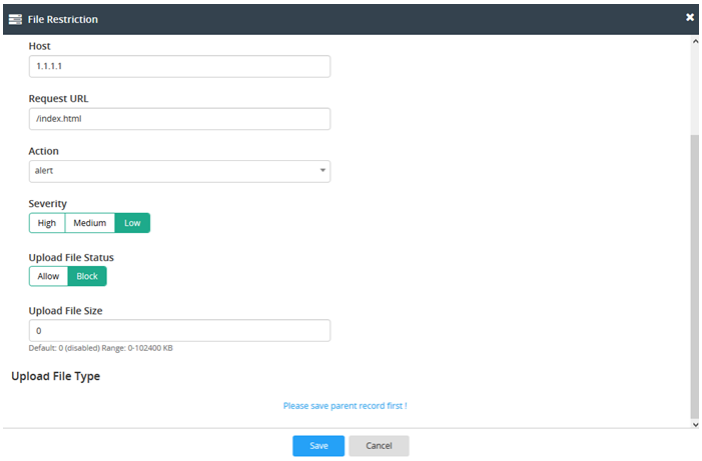


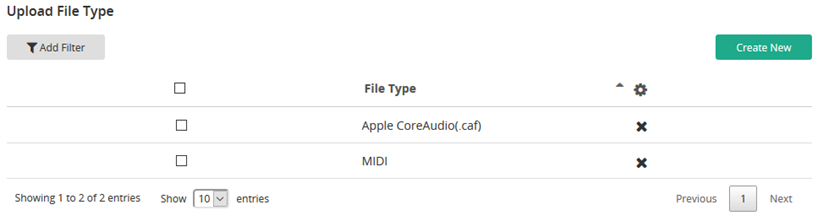

| | |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |
| Host Status | Enable to apply this input rule only to HTTP requests for specific web hosts. Also, configure Host.<br>Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the Host: field. |
| Host | Select which protected host names entry (either a web host name or IP address) that the Host: field of the HTTP request must be in to match the signature exception.<br>This option is available only if Host Status is enabled. |
| Request URL | Depending on your selection in Request URL Type, type either:<br>• the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash ( / ).<br>• a regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash ( / ).; however, it must at least match URLs that begin with a slash, such as /index.html. |
| Action | Select which action FortiADC takes when the conditions are fulfilled for File Restriction.<br>• Alert—Accept the request and generate an alert email, log message, or both.<br>• Deny—Block the request (or reset the connection).<br>• Block—Block subsequent requests from the client for a number of seconds. Also configure Block Period.<br>• Silent-deny—Deny without log.<br>The default value is Alert. |
| Severity | When FortiADC records violations of this rule in the attack log, each log message contains a **Severity Level** (severity_level) field. Select which severity level FortiADC uses when using Input Validation:<br>• Low<br>• Medium<br>• High<br>The default value is **Low**. |

| | |
|---|---|
| Post URL | Check URL by simple string or regular express matching. |
| Hidden Fields | The “Hidden Fields ” rules are for hidden parameters only, from <input type="hidden"> HTML tags. |

## To configure a File Restriction rule

1. Go to **Web Application Firewall.**
2. Click the **Input Validation** tab.
3. Click the **File Restriction** tab.
4. Click **Create New** in File Restriction Rule part to display the configuration editor and fill the Name, Host Status, Request URL, Action, Severity, Upload File Size, and Upload File Type, based on your security requirements.
5. Click **Save** to save the configuration

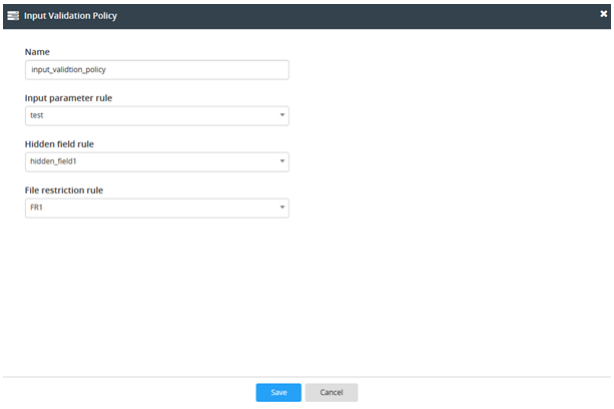



| | |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |
| Host Status | Enable to apply this input rule only to HTTP requests for specific web hosts. Also, configure Host.<br>Disable to match the input rule based upon the other criteria, such as the URL, but regardless of the Host: field. |
| Host | Select which protected host names entry (either a web host name or IP address) that the Host: field of the HTTP request must be in to match the signature exception.<br>This option is available only if Host Status is enabled. |

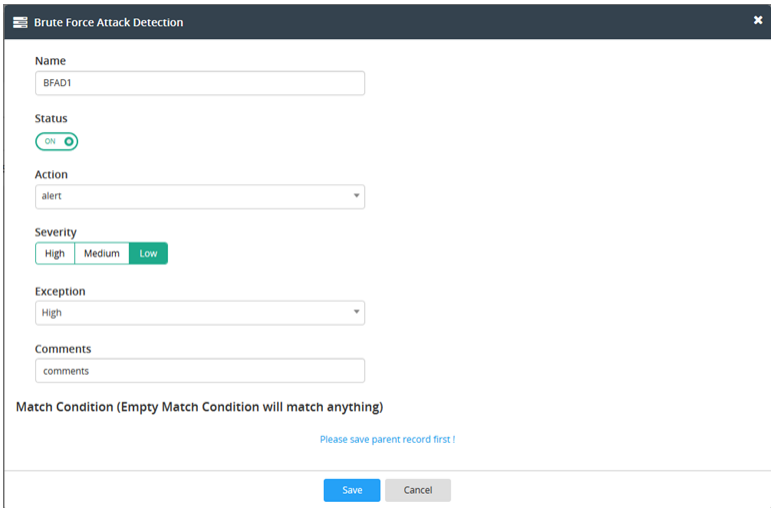
| | |
|---|---|
| Request URL | Depending on your selection in Request URL Type, type either:<br>• the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash ( / ).<br>• a regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash ( / ).; however, it must at least match URLs that begin with a slash, such as /index.html. |
| Action | Select which action FortiADC takes when the conditions are fulfilled for File Restriction.<br>• Alert—Accept the request and generate an alert email, log message, or both.<br>• Deny—Block the request (or reset the connection).<br>• Block—Block subsequent requests from the client for a number of seconds. Also configure Block Period.<br>• Silent-deny—Deny without log.<br>The default value is Alert. |
| Severity | When FortiADC records violations of this rule in the attack log, each log message contains a **Severity Level** (severity_level) field. Select which severity level FortiADC uses when using Input Validation:<br>• Low<br>• Medium<br>• High<br>The default value is **Low**. |
| Upload File Status | Allow or block the file type. The default value is allow. |
| Upload File Size | The maximum size of uploading file. |
| Upload File Type | Select a predefined file type. |

To apply the input validation policy, you can add any rule or all those three rules into input validation policy and then select the input policy in a WAF profile.

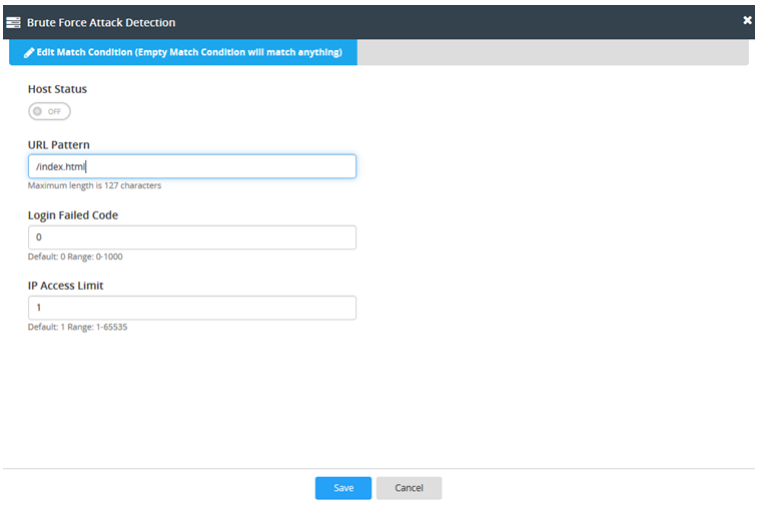


# To configure a brute force attack detection policy

1. Go to **Web Application Firewall**.
2. Click the **Common Attacks Detection** tab.
3. Click the **Brute Force Attack Detection** tab.
4. Click **Create New** to display the configuration editor and fill the Name, Status, Action, Severity, Exception, and Comments based on your security requirements.




5. Click **Save** to save the configuration.
6. Click **Edit** to display the configuration editor and click Create New in Match Condition part to display the configuration editor and fill the Host Status, URL Pattern, Login Failed Code, and IP Access Limit based on your security requirements.




7. **Save** the configuration.

| | |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |

| | |
|---|---|
| Status | Enable or disable this function. |
| Action | Select which action FortiADC takes when the conditions are fulfilled for File Restriction.<br>• Alert—Accept the request and generate an alert email, log message, or both.<br>• Deny—Block the request (or reset the connection).<br>• Block—Block subsequent requests from the client for a number of seconds. Also configure Block Period.<br>• Silent-deny—Deny without log.<br>The default value is Alert. |
| Severity | When FortiADC records violations of this rule in the attack log, each log message contains a **Severity Level** (severity_level) field. Select which severity level FortiADC uses when using Input Validation:<br>• Low<br>• Medium<br>• High<br>The default value is **Low**. |
| Exception | Exception policy. |
| Host Status | Enable to apply this input rule only to HTTP requests for specific web hosts. |
| URL Pattern | Depending on your selection in Request URL Type, type either:<br>• the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash ( / ).<br>• a regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash ( / ).; however, it must at least match URLs that begin with a slash, such as /index.html. |
| Login Failed Code | The response code which used to judge the login is failed or not. The default is 0, which means will not match any status code. |
| IP Access Limit | The threshold for source IP address that is single client's login. If login failed count exceeded the threshold, FortiADC will perform the corresponding WAF action.<br>The default is 1. |

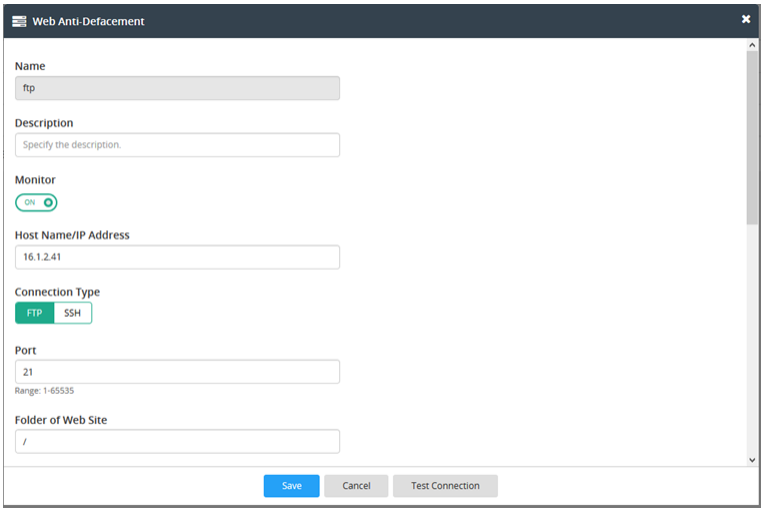
8. To apply the brute force detection policy, select it in a WAF profile.

## To configure an anti-defacement policy

1. Go to **Web Application Firewall**.
2. Click the **Web Anti-Defacement** tab.
3. Click **Create New** to display the configuration editor and fill or change the configurations based on your security requirements.
4. Click **Test Connection** to test the connection between the FortiADC appliance and the web server. During the next interval, FortiADC should connect to download its first backup. You should notice that Total Files and Total Files would increment.If not, first verify the login and IP address that you provided.

Also, on the web server, check the file system permissions for the account that FortiADC is using to connect.

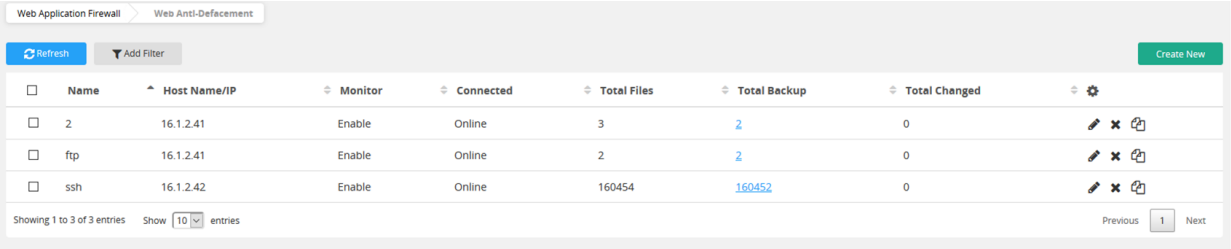
5. **Save** the configuration.




| | |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |
| Description | Enter a comment. up to 63 characters long. This field is optional. |
| Monitor | Enable to monitor the web site's files for changes. |
| Host Name/IP Address | Type the IP address or FQDN of the web server on which the web site is hosted. |
| Connection Type | Select which protocol (FTP, SSH) to use when connecting to the web site in order to monitor its contents and download web site backups. |
| Port | Enter the TCP port number on which the web site's real server listens. The standard port number for FTP is 21; the standard port number for SSH is 22. |
| Folder of Web Site | Type the path to the web site's folder, such as public_html or wwwroot, on the real server. The path is relative to the initial location when logging in with the user name that you specify in User Name. |
| Username | Enter the user name that the FortiADC appliance will use to log in to the web site's real server. |
| Password | Enter the password for the user name you entered in User Name. |
| Monitor Interval for Root Folder | Enter the time interval in seconds between each monitoring connection from the FortiADC appliance to the web server. During this connection, the FortiADC appliance examines Folder of Web Site (but not its subfolders) to see if any files have changed by comparing the files with the latest backup. |
| Monitor Interval for other Folder | Enter the time interval in seconds between each monitoring connection from the FortiADC appliance to the web server. During this connection, the FortiADC appliance examines subfolders to see if any files have been changed by comparing the files with the latest backup. |

| | |
|---|---|
| Maximum Depth of Monitored Folders | Type how many folder levels deep to monitor for changes to the web site's files. |
| Skip Files Larger Than | Type a file size limit in kilobytes (KB) to indicate which files will be included in the web site backup. Files exceeding this size will not be backed up. The default file size limit is 10240 KB. |
| Skip Files with These Extensions | Type zero or more file extensions, such as iso, avi, to exclude from the web site backup. Separate each file extension with a comma. |
| Automatic Action | Enable to automatically restore the web site to the previous revision number when it detects that the web site has been changed.<br>• Disable<br>• Acknowledge<br>• Restore |

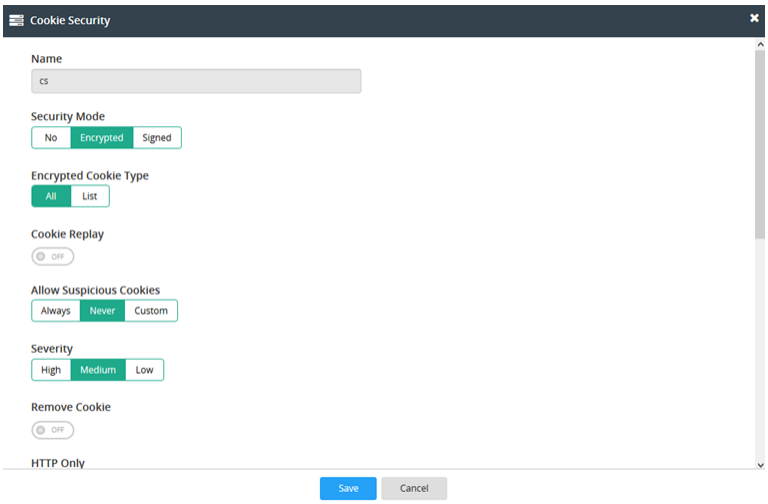
From the Web Anti-Defacement page, you can check the status of each web site that FortiADC is monitoring.




| | |
|---|---|
| Monitor | Indicates whether or not anti-defacement is currently enabled for the web site. |

## To configure a cookie security policy

1. Go to **Web Application Firewall**.
2. Click the **Sensitive Data Protection** tab.
3. Click **Cookie Security** tab.
4. Click **Create New** to display the configuration editor and fill or change the configurations based on your security requirements.



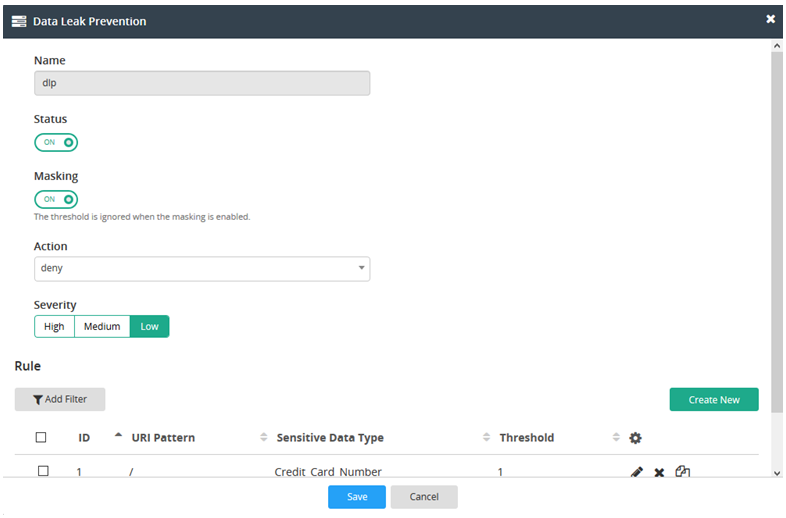

| | |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |
| Security Mode | • No — FortiADC does not apply cookie tampering protection or encrypt cookie values.<br>• Encrypted — Encrypts cookie values the back-end web server sends to clients. Clients see only encrypted cookies. FortiADC decrypts cookies submitted by clients before it sends them to the back-end server. No back-end server configuration changes are required.<br>• Signed — Prevents tampering (cookie poisoning) by tracking the cookie value. |
| HTTP Only | Enable--add "HTTPOnly" flag to cookies. HttpOnly attribute limits the scope of the cookie to HTTP requests. In particular, the attribute instructs the user agent to omit the cookie when providing access to cookies via "non-HTTP" APIs (such as a web browser API that exposes cookies to scripts). |
| Secure | Enable--add the secure flag to cookies. The Secure attribute limits the scope of the cookie to "secure" channels (where "secure" is defined by the user agent). When a cookie has the Secure attribute, the user agent will include the cookie in an HTTP request only if the request is transmitted over a secure channel (typically HTTP over Transport Layer Security (TLS) |
| Encrypted Cookie Type | When security-mode is selected to encrypted:<br>• All—will encrypt all the cookies<br>• List—will encrypt the cookie that match with the cookie-list |
| Cookie Replay | Optionally, select whether FortiADC uses the IP address of a request to determine the owner of the cookie. |
| Allow Suspicious Cookies | Note: only for security-mode encrypted<br>Whether allows requests that contain cookies ADC does not recognize by encrypted cookie function or with missing cookies.<br>When cookie-replay enable, the suspicious cookie is a missing cookie that tracks the client IP address. |

| | |
|---|---|
| | In many cases, when you first introduce the cookie security features, cookies that client browsers have cached earlier generate false positives. To avoid this problem, either select Never, or select Custom and enter an appropriate date on which to start taking the specified action against suspicious cookies.<br>• Never—never allow suspicious cookies.<br>• Always—always allow suspicious cookies.<br>• Custom—Don't Block suspicious cookies Until dont_block_until specified date. |
| Severity | When FortiADC records violations of this rule in the attack log, each log message contains a **Severity Level** (severity_level) field. Select which severity level FortiADC uses when using Input Validation:<br>• Low<br>• Medium<br>• High<br>The default value is **Low**. |
| Remove Cookie | Enable this option to accept the request, but remove the cookie before send it to the web server. |
| Action | Select which action FortiADC takes when the conditions are fulfilled for File Restriction.<br>• Alert—Accept the request and generate an alert email, log message, or both.<br>• Deny—Block the request (or reset the connection).<br>• Block—Block subsequent requests from the client for a number of seconds. Also configure Block Period.<br>• Silent-deny—Deny without log.<br>The default value is Alert. |
| Max Age | Enter the maximum age (in minutes) permitted for cookies that do not have an “Expires” or “Max-Age” attribute.<br>To configure no expiry age for cookies, enter 0. |
| Exception | Exception list for encrypted/ signed. |

5. **Save** the configuration.
6. To apply the cookie security policy, select in a WAF profile.

## To configure a data leak prevention policy

1. Go to **Web Application Firewall**.
2. Click the **Sensitive Data Protection** tab.
3. Click the **Data Leak Prevention** tab.
4. Click **Create New** to display the configuration editor and fill or change the configurations based on your security requirements.




| Setting name | Description |
|---|---|
| Name | Type a unique name that can be referenced in other parts of the configuration. Do not use spaces or special characters. |
| Status | Click to enable or disable this policy. |
| Masking | To replace sensitive data with asterisks (*) by enabling it. The default is disable.<br>It only works with alert action. |
| Action | Select which action FortiADC takes when the conditions are fulfilled for File Restriction.<br>• Alert—Accept the request and generate an alert email, log message, or both.<br>• Deny—Block the request (or reset the connection).<br>• Block—Block subsequent requests from the client for a number of seconds. Also configure Block Period.<br>• Silent-deny—Deny without log.<br>The default value is Alert. |
| Severity | When FortiADC records violations of this rule in the attack log, each log message contains a **Severity Level** (severity_level) field. Select which severity level FortiADC uses when using Input Validation:<br>• Low<br>• Medium<br>• High<br>The default value is **Low**. |
| URL Pattern | Depending on your selection in Request URL Type, type either:<br>• the literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash ( / ).<br>• a regular expression, such as ^/*.php, matching all and only the URLs to which the input rule should apply. The pattern does not require a slash ( / ).; however, it must at least match URLs that begin with a slash, such as /index.html.<br>Note: Rule will not work when URL Pattern is empty. |

| | |
|---|---|
| Sensitive Data Type | The specified data type that created in Web Application Firewall à Sensitive Data Type. |
| Threshold | The rule will take effect when the threshold is hit. The default value is 1.<br>Note: It will not take effect when the masking is enabled. |

5. **Save** the configuration.
6. To apply DLP, select it in a WAF profile.