Citrix ADC Web App Firewall Service
## Contents

**Getting started** 3  
- Step 1: Sign Up for Citrix Cloud 3  
- Step 2: Request for Citrix Web App Firewall service trial 3  
- Log into the Citrix Web App Firewall service 5  

**Service level goal** 6  

**Multi-Geo regions** 7  
- Limitations 7  

**Configure Multi-Geo Regions** 9  

**Configure domains for WAF service** 11  
- Upload SSL certificate 12  
- Configure Security service application 17  
- Manage Web App Security service applications 20  

**Web App Firewall service actions** 28  
- Security Insight 28  
- SSL certificate and keys 31  
- HTML error pages 31  
- Signatures 32  

**Manage Citrix Web App Firewall service profiles** 33
Getting started

June 5, 2019
Contributed by: C

This section below walks you through how to get started with onboarding and setting up Citrix Web App Firewall Service for the first time. These instructions are intended for network and application administrators who manage Citrix network devices (Citrix ADC, SD-WAN WANOP, Citrix Gateway, Citrix Secure Web Gateway, and so on).

The following image illustrates the steps you have to perform to get started.

**Step 1: Sign Up for Citrix Cloud**

To start using Citrix Web App Firewall Service, you must first create a Citrix Cloud service account or join an existing one that has been created by someone else in your company. For detailed processes and instructions on how to proceed, see Signing Up for Citrix Cloud.

**Step 2: Request for Citrix Web App Firewall service trial**

After you log on to Citrix Cloud, the list of available services within the Citrix Cloud environment is displayed. You can add web application firewall service to existing services, when it is not available. In the Available Services section, on the Citrix Web App Firewall service tile, click Request Trial.
The **Citrix Web App Firewall Service** tile moves to the **My Services** section, and the button then changes to **View Trial Status**. You will receive an email to notify you when your trial becomes available with the sign in information. It might take a few minutes.

To get started, sign in to Citrix Cloud and click on **Manage** or select **Web App Security Service** from the menu.

The **Web App Security Service** service trial will be active for 60 days. After that, we'll archive your data and configuration for 90 days. You can convert your service from trial to production at any time during or before the 90-day period.

After you are authorized to access the trial, the button on the tile changes to **Manage**. Click **Manage** to log on to the **Citrix Web App Firewall Service** GUI.
Citrix assigns permissions to you to access the Citrix Web App Firewall service for a 60-day trial period. For information about trial subscriptions and how to buy, see https://www.citrix.com/products/citrix-cloud/subscriptions.html.

Log into the Citrix Web App Firewall service

If you have purchased a license to use the service, the Citrix Web App Firewall Service page is displayed as shown below. Click Get Started to begin setting up the service for the first time.
The POP expansion and performance package pages are displayed. If this is the first time you are accessing the Citrix Web App Firewall service and want to configure domains, you must have a Basic SKU Package.

The Citrix Web App Firewall service web management interface allows you to select regions based on the POP and Performance package you have. Read the following information about multi-geo regions and how you can use the web application firewall service product SKUs before proceeding with configuring domains.

**Set Default Region**

Thank you for using the Web App Security Service. To get started, you must set the Default Region for your base package before any configuration.

<table>
<thead>
<tr>
<th>Enlistment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Package Performance (Mbps)</td>
</tr>
<tr>
<td>Total number of POP Expansion</td>
</tr>
<tr>
<td>Total Performance Packages (Mbps)</td>
</tr>
<tr>
<td>select the default region for your base package</td>
</tr>
<tr>
<td>✔ US East</td>
</tr>
<tr>
<td>✔ US West</td>
</tr>
<tr>
<td>Asia Pacific (APAC)</td>
</tr>
<tr>
<td>Europe, Middle East &amp; Africa (EMEA)</td>
</tr>
</tbody>
</table>

**OK**

**Note**

The Getting Started page is displayed, when there are no domains configured/available.

1.  
2. Citrix ADC Web App Firewall Service

**Service level goal**

June 5, 2019

Contributed by:
C

Citrix Web App Firewall service is a cloud-based web application service that protects customer’s web applications and their infrastructure from cyber security attacks.
The Service Level Agreement (SLA) describes Citrix’s commitment for Citrix Cloud Service availability. This SLA is part of the Citrix end user service agreement (EUSA) for covered services (“Services”). For complete details about Citrix’s commitment for availability of Citrix Cloud services, see the Service Level Agreement.

1. 
   2. Citrix ADC Web App Firewall Service

Multi-Geo regions

June 5, 2019
Contributed by: C

The multi-geo feature allows you to choose the location/region for the server. For example; US East, US West, EMEA, or APAC. To use the Citrix Web App Firewall service for multi-geo functionality, there is a Base Package SKU called Basic, which can be purchased that is available with 25 Mbps and 200 Mbps performance. You can choose only one bandwidth option at a time and not both.

Limitations

Currently, Citrix Web App Firewall service has the following set of limitations:

- Rules can operate only on URLs.
- Default geolocation is mandatory and cannot be changed.
- Currently, the allowed geo locations are US-West and EMEA. In addition, you can select a geo location only after you select the default location.
- Signature editor is not supported. WAF supports only signature files upload.

Resource Limitation

The following table gives a list of resource limitation when selecting multi-geo regions.

<table>
<thead>
<tr>
<th>Entity</th>
<th>Max Limits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domains</td>
<td>5</td>
</tr>
<tr>
<td>Profiles</td>
<td>5</td>
</tr>
<tr>
<td>Per-entity binding</td>
<td>25</td>
</tr>
</tbody>
</table>
Following are the WAF service product SKUs available when selecting multi-geo regions for a server:

**BASIC**: This product SKU is required for service to be configured. This is not only a prerequisite for any configuration to be accepted by WAF-service but also for other SKUs. You cannot have other SKU unless the basic SKU is available. Basic SKUs have the following bandwidth and transmission data limits:

- Bandwidth: 25 Mbps or 200 Mbps
- Transmission Data: 2 TB

There might be only one entitlement corresponding to BASIC SKU.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The BASIC package can only be assigned once, and only to one geo location. Unless this default geo location is selected, you cannot perform any configuration.</td>
</tr>
</tbody>
</table>

Once the geo location of the Base Package is decided and selected, you cannot change it.

1. **PERF-EXPANSION**: This product SKU allows you to increase the performance bandwidth. Quantity mentioned in the entitlements corresponding to this SKU is always an integer. Each unit of quantity corresponds to 25 Mbps. There can be multiple entitlements of this type.

You can assign the quantity in integer units to multiple geolocations.

For example, you can buy a PERF-PACKAGE with a quantity of 4 and can assign 2 units to the US EAST region, 1 unit to US WEST and remaining 1 unit to EMEA, which means you intend to have 50 Mbps for US EAST, 25 Mbps to US WEST, and 25 Mbps to the EMEA region.

1. **POP-EXPANSION**: This product SKU can be bought to expand POP presence. Quantity mentioned in the entitlements corresponding to this SKU should always be an integer. Each unit of quantity corresponds to one region and default bandwidth of 25 Mbps. There can be multiple entitlements of this type.

For example: You can buy a POP-EXPANSION with a quantity of 3 and can expand the service presence to three regions each with default capacity of 25 Mbps.

1. **Data**: This product SKU can be bought to store total bytes processed in the service. This SKU is integrated with MAS storage licenses/SKUs.

Also, you can purchase more POP-Expansion packages that allow you to add different geo location for the server. This expansion package comes with 25 Mbps performance.

To speed up the service, you can purchase more “Performance Packages” to add on to the existing locations (including the Base region).

The Performance Package is 25 Mbps per unit. You can purchase units in the range of 25, 50, 75, 100, and 125 … Mbps. You can change the assignment of “POP-Expansion” and “Performance Packages” after they have been configured and assigned.
Proceed with configuring multi-geo regions.

1. Select a region and allocate bandwidth and performance capacity based on the WAF service multi-geo feature package that you have purchased. The Set Default Region page is displayed. The default region is **US East**.

2. Select the POP expansion and performance package bandwidth and click **OK**.
Ensure that you do not allocate additional POP or performance packages other than your entitlement allocation capacity for bandwidth. The WAF service web interface will generate allocation errors as shown below. Errors are displayed if entry is invalid. For example; Invalid Integer, -ve value and not multiple of 25.

1. After you have successfully configured regions and the required assigned bandwidth capacity, the **Web App Security Service Domains** page is displayed.

   1.
   2. **Citrix ADC Web App Firewall Service**
Configure domains for WAF service

June 5, 2019

Contributed by:
C

Domains are a way to segment network traffic for different applications. You can use traffic domains to create multiple isolated environments within a Citrix ADC appliance network. An application belonging to a specific traffic domain communicates with entities and processes traffic within that domain. The traffic belonging to one traffic domain cannot cross the boundary of another traffic domain.

Use the following steps to add security service domains by using specific application firewall functionality.

1. On the **Web App Security Service Domains** page, click the **Action** tab to select desired Application Firewall features.

![Web App Security Service Domains](image)

The stand-alone objects to be created in order to construct a Domain, Application and Profile are:

- **SSL Cert Key**: Created with SSL certificate and key in addition to the pass phrase. This object is required to create a domain.
- **Profile**: This object is required to create a domain. An application is equivalent to a policy which is bound to a domain. Each domain contains a list of applications with priorities assigned to each one of them. In addition, an application consists of a flag for turning on the IP Reputation feature.
- **HTML Error Page and Signatures**: These objects are optional if creating a profile.

These objects can be reused and shared between domains and applications and are available under the **Action** menu.
1. Click **Add**. The **Add Web App Security Service Domain** page is displayed. Type the Name, Description, and Domain. Upload the SSL Certificate and SSL key files, for example; waf.cert and waf.key. Enter an SSL Pass Phrase and then click **Create**. The domain is added to the list of domains as shown below. If you want to add multiple domains, click **Add**, and specify the same SSL CertKey.

**Upload SSL certificate**

1. To upload SSL certificate and key, you can click the “+” sign in the **SSL Cert Keys Name** field. The **Add SSL Cert Keys** page is displayed.

**Note:**

Web Application Firewall service currently supports certificates in PEM format and SSL passphrase is not mandatory.
1. After a certificate is uploaded, select the SSL Cert Key when adding a new domain.

1. Create a Domain. Type Name, Domain name, and description for the domain. Click Create.
Add Web App Security Service Domain

Name
D1

Description
Domain 1

Domain
www.google.com

SSL Certkey Name
SSL1

Please remember to add the CNAME to the DNS after the domain has been created.

Cancel  Create

A confirmation page is displayed.
1. Select the newly created domain and click **Edit** to edit it. If you hover over the row of a domain, a circle with three dots icon appears on the left-most column where you can directly select an action to click.
Edit Web App Security Service Domain

Name:
D1

Description:
Domain 1

Domain:
www.google.com

CNAME:
78fc1acfc.dns.appfwsvc.net

Server IP:
74.125.28.104

SSL CertKey Name:
SSL1

Cancel  OK
Citrix ADC Web App Firewall Service

Note
You should allow traffic only from the NetScaler IP address to the back end server and block traffic from all other IP addresses.

Configure Security service application

1. Click Add to add an application. Add profile name, description, and URL for the Application. Click Create and Close.

2. After you have finished editing the domain information, click OK. A confirmation page displaying the edited information for the domain is displayed. Click Close.

3. You can also choose the newly added Domain and click Manage Applications. Ensure that you change the CNAME provided by the WAF service for newly created domain. This changes the DNS record address for the CNAME. The IP address of the back-end server is populated as shown below. Click Close. You can copy “CNAME to clipboard” to setup DNS.
1. Select a profile name. You would need to add a profile name by adding it from the Applications page as shown below.

You can also perform more actions using the **Action** tab on the **Manage application service** page.
1. To edit a profile, select it and click **Edit**.
Manage Web App Security service applications

1. Choose an application, and click Manage Security Profile, the following Application Firewall profile information is displayed as shown below.

![Application Firewall profile](image1)

**Application Security service profile:**

![Application Security service profile](image2)

1. On the Security Checks page, create security profiles. This page displays the Application Firewall standard GUI interface options for you to add security profiles. Add Application Name, URL, and Priority.
2. Choose the security profile which you want to edit.
3. Edit the White List URLs and click OK.

**Security check actions views:** URL Whitelist Settings and URL Blacklist Settings.

Use the check box to uncheck “Block” and “Log” settings for whitelist and blacklist URL settings.
Buffer overflow settings:

Content-type Settings: Use the check box to deselect “Block” and “Log” settings.

HTML cross-site scripting settings:
HTML Cross-Site Scripting Settings

Actions:
- Block
- Log
- Transform cross-site scripts

Parameters:
- Check complete URLs for cross-site scripting

[OK] [Close]

HTML SQL Injection Settings:

Actions:
- Block
- Log
- Transform SQL special characters

Parameters:
- Check for SQL Wildcard Characters

[Cancel] [OK]

Save & Close your changes for Security checks.

Profile settings page:
Profile Signatures page:

Add Signatures

Name*

☐ Text Input

Signareus File*  Choose File

Cancel  OK

Relaxation rules page: All relaxation rules are enabled by default when you add them. When you
need to delete a relaxation rule, you disable it first and then remove it.

**URL whitelist relaxation rules:**

**URL Blacklist Relaxation Rules:**
Content-type Relaxation Rules:
Add Content-type Relaxation Rule

- Content Type
  - RegEx Editor
- Comments

Create

HTML cross-Site scripting relaxation rules:

<table>
<thead>
<tr>
<th>Name</th>
<th>URL</th>
<th>Location</th>
<th>Value Type</th>
<th>Value Expression</th>
</tr>
</thead>
</table>

No items

Close
HTML Cross-Site Scripting Relaxation Rules

Add HTML Cross-Site Scripting Relaxation Rule

- Is Name Regex
  - Name
    - RegExp Editor
- URL
  - RegExp Editor
- Location
  - FORMFIELD
- Value Type
- Comments

[Cancel] [Create]

HTML SQL injection relaxation rules:

- Add
- Edit
- Delete
- Clone

<table>
<thead>
<tr>
<th>Name</th>
<th>URL</th>
<th>Location</th>
<th>Value Type</th>
<th>Value Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Close]
Web and web service applications that are exposed to the Internet have become increasingly vulnerable to attacks. To protect applications from attack, you need visibility into the nature and extent of past, present, and impending threats, real-time actionable data on attacks, and recommendations on countermeasures. Security Insight provides a single-pane solution to help you assess your application
security status and take corrective actions to secure your applications. Security Insight is an intuitive dashboard-based security analytics solution that gives you full visibility into the threat environment associated with your applications. You can view reports based on Application Firewall profile settings by using the Security Insight option in the Action menu of the WAF service GUI.
SSL certificate and keys

An SSL certificate, which is an integral part of any SSL transaction, is a digital data form (X509) that identifies a company (domain) or an individual. The certificate has a public key component that is visible to any client that wants to initiate a secure transaction with the server. The corresponding private key, which resides securely on the Citrix ADC appliance, is used to complete asymmetric key (or public key) encryption and decryption.

You can obtain an SSL certificate and key in either of the following ways:

- From an authorized certificate authority (CA), such as VeriSign
- By generating a new SSL certificate and key on the Citrix ADC appliance

Alternately, you can use an existing SSL certificate on the appliance.

Note

Citrix recommends that you use certificates obtained from authorized CAs, such as VeriSign, for all your SSL transactions. Certificates generated on the Citrix ADC appliance should be used for testing purposes only, not in any live deployment.

HTML error pages

You can import HTML error objects to the application firewall by using the configuration utility. You can edit these files in a web-based text area after importing them, to make small changes directly on the Citrix ADC appliance instead of having to make them on your computer and then reimport them. Finally, you can export any of these files to your computer, or delete any of these files, by using the configuration utility.

To add HTML error pages:
Signatures

The application firewall signatures function provides specific, configurable rules to simplify the task of protecting your web sites against known attacks. A signature represents a pattern that is a component of a known attack on an operating system, web server, website, XML-based web service, or other resource. You can create your own signatures by following these steps below:
The Citrix Web App Firewall service allows you to add, edit, and delete required profiles using the GUI.

1. Click **Add** to add new profile.
2. Enter profile name and click **Create**.
Add Web App Security Service Profile

Profile Name*

Comments

* A default setting will be created after this operation. Please edit this profile for more detail afterward.

Cancel  Create