Deploying NetScaler AppFirewall

Deployment Guide

This deployment guide provides general guidelines for deploying the NetScaler Application Firewall.
# Table of Contents

- Introduction 3
- AppFirewall Features 3
- Rules and Signatures 7
- Integrating with other NetScaler features 8
- Packet Processing with NetScaler and AppFirewall 8
- Standard Workflow for Deploying AppFirewall 9
- Deploying the AppFirewall 11
  - Basic and Advanced Policies 12
  - Custom Policy Bindings 16
- Conclusion 18
Citrix NetScaler AppFirewall is a comprehensive ICSA certified web application security solution that blocks known and unknown attacks against web and web services applications. NetScaler AppFirewall enforces a hybrid security model that permits only correct application behaviour and efficiently scans and protects against known application vulnerabilities. It analyzes all bidirectional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications.

**Introduction**

NetScaler AppFirewall (also referred to as AppFirewall, Web Application Firewall or WAF) technology is included in and integrated with Citrix NetScaler MPX and NetScaler VPX, Platinum Edition, and is available as an optional module that can be added to NetScaler MPX appliances running NetScaler Enterprise Edition. NetScaler AppFirewall is also available as a stand-alone solution on some NetScaler MPX appliances. The stand-alone NetScaler AppFirewall models can be upgraded through software licensing to full NetScaler Application Delivery Controllers (ADCs).

This guide focuses on defining the general deployment guidelines for Citrix NetScaler AppFirewall. The product versions described here are -

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler (AppFirewall Integrated Module)</td>
<td>10.5 (Enterprise/Platinum License)</td>
</tr>
</tbody>
</table>

**AppFirewall Features**

**Hybrid security model**

The NetScaler hybrid security model allows you to take advantage of both a positive security model and a negative security model to come up with a configuration ideally suited for your applications.

The positive security model protects against Buffer Overflow, CGI-BIN Parameter Manipulation, Form/Hidden Field Manipulation, Forceful Browsing, Cookie or Session Poisoning, Broken ACLs, Cross-Site Scripting (XSS), Command Injection, SQL Injection, Error Triggering Sensitive Information Leak, Insecure Use of Cryptography, Server Misconfiguration, Back Doors and Debug Options, Rate-Based Policy Enforcement, Well Known Platform Vulnerabilities, Zero-Day Exploits, Cross Site Request Forgery (CSRF), and leakage of Credit Card and other sensitive data.

The negative security model uses a rich set signatures to protect against L7 and HTTP application vulnerabilities. The application firewall is integrated with several third party scanning tools, such as those offered by Cenzic, Qualys, Whitehat, and IBM. The built-in XSLT files allow easy importation...
of rules, which can be used in conjunction with the native-format Snort based rules. An auto-update feature gets the latest updates for new vulnerabilities.

The positive security model might be the preferred choice for protecting applications that have a high need for security, because it gives you the option to fully control who can access what data. You allow only what you want and block the rest. This model includes a built-in security check configuration, which is deployable with a few clicks. However, keep in mind that the tighter the security, the greater the processing overhead.

The negative security model might be preferable for customized applications. The signatures allow you to combine multiple conditions, and a match and the corresponding action are triggered only when all the conditions are satisfied. You block only what you don’t want and allow the rest. A specific fast-match pattern in a specified location can significantly reduce processing overhead to optimize performance. The option to add your own signature rules, based on the specific security needs of your applications, gives you the flexibility to design your own customized security solutions.

Request as well as response side detection and protection
You can inspect the incoming requests to detect any suspicious behavior and take appropriate actions, and you can check the responses to detect and protect against leakage of sensitive data.

Rich set of built-in protections for HTML, XML and JSON payloads
The application firewall offers 19 different security checks. Six of them (such as Start URL and Deny URL) apply to both HTML and XML data. Five checks (such as Field Consistency and Field Format) are specific to HTML, and eight (such as XML Format and Web Service Interoperability) are specific to XML payloads. This feature includes a rich set of actions and options. For example, URL Closure enables you to control and optimize the navigation through your website, to safeguard against forceful browsing without having to configure relaxation rules to allow each and every legitimate URL. You have the option to remove or x-out the sensitive data, such as credit-card numbers, in the response. Be it SOAP array attack protection, XML denial of service (XDoS), WSDL scan prevention, attachment check, or any number of other XML attacks, you have the comfort of knowing that you have an ironclad shield protecting your data when your applications are protected by the application firewall. The signatures allow you to configure rules using XPATH-Expressions to detect violations in the body as well as the header of a JSON payload.

GWT
Support for protecting Google Web Toolkit applications to safeguard against SQL, XSS and Form Field Consistency check violations.

Java-free, user friendly graphical user interface (GUI)
An intuitive GUI and preconfigured security checks make it easy to deploy security by clicking a few buttons. A wizard prompts and guides you to create the required elements, such as profiles, policies, signatures, and bindings. The HTML5 based GUI is free of any Java dependency. It’s performance is significantly better than that of the older, Java based versions.
Easy to Use and automatable CLI
Most of the configuration options that are available in GUI are also available in the command line interface (CLI). The CLI commands can be executed by a batch file and are easy to automate.

Support for REST API
The NetScaler NITRO protocol supports a rich set of REST API’s to automate application firewall configuration and collect pertinent statistics for ongoing monitoring of security violations.

Learning
The application firewall’s ability to learn by monitoring traffic to fine tune security is very user friendly. The learning engine recommends rules, which makes it easy to deploy relaxations without proficiency in regular expressions.

RegEx editor support
Regular expression offer an elegant solution to the dilemma of wanting to consolidate rules and yet optimize search. You can capitalize on the power of regular expressions to configure URLs, field names, signature patterns, and so on. The rich built-in GUI RegEx editor offers you a quick reference for the expressions and provides a convenient way to validate and test your RegEx for accuracy.

Customized error page
Blocked requests can be redirected to an error URL. You also have the option to display a customized error object that uses supported variables and Citrix default syntax (advanced PI expressions) to embed troubleshooting information for the client.

PCI-DSS, stats, and other violation reports
The rich set of reports makes it easy to meet the PCI-DSS compliance requirement, gather stats about traffic counters, and view violation reports for all profiles or just one profile.

Logging and click-to-rule from log
Detailed logging is supported for native as well as CEF format. The application firewall offers you the ability to filter targeted log messages in the syslog viewer. You can select a log message and deploy a corresponding relaxation rule by a simple click of a button. You have the flexibility to customize log messages and also have support for generating web logs. For additional details, see http://docs.citrix.com/en-us/netscaler/11/security/application-firewall/logs.html.

Include violation logs in trace records
The ability to include log messages in the trace records makes it very easy to debug unexpected behavior such as reset and block.

Cloning
The useful Import/Export profile option allows you to clone the security configuration from one NetScaler appliance to others. Export learned data options make it easy to export the learned rules to an Excel file. You can then get them reviewed and approved by the application owner before applying them.
AppExpert Templates
An AppExpert template (a set of configuration settings) can be designed to provide appropriate protection for your websites. You can simplify and expedite the process of deploying similar protection on other appliances by exporting these cookie-cutter templates to a template file. For additional details, see http://docs.citrix.com/en-us/netscaler/10-5/ns-appexpert-con-10/ns-aapexpert-apptemp-wrapper-con.html

Sessionless security checks
Deploying sessionless security checks can help you reduce the memory footprint and expedite the processing.

Interoperability with other NetScaler features
The application firewall works seamlessly with other NetScaler features, such as rewrite, URL transformation, integrated caching, CVPN, and rate limiting.

Support of PI expressions in policies
You can leverage the power of advanced PI expressions to design policies to implement different levels of security for different parts of your application.

Support for IPv6
The application firewall supports both IPv4 and IPv6 protocols.

Geolocation based security protection:
You have the flexibility of using Citrix default syntax (PI Expressions) for configuring location based policies, which can be used in conjunction with a built-in location database to customize firewall protection. You can identify the locations from which malicious requests originate, and enforce the desired level of security-check inspections for requests that originate from a specific geographical location.

Performance
Request-side streaming significantly improves performance. As soon as a field is processed, the resulting data is forwarded to the back end while evaluation continues for the remaining fields. The improvement in processing time is especially significant when handling large posts.

Other security features
The application firewall has several other security knobs that can help ensure the security of your data. For example, the Confidential Field lets you block leakage of sensitive information in the log messages, and Strip HTML Comment allows you to remove the HTML comments from the response before forwarding it to the client. Field Types can be used to specify what inputs are allowed in the forms submitted to your application.
Rules and Signatures

The application firewall makes it very easy to design the right level of security for your applications. You can have multiple application firewall policies, bound to different application firewall profiles, to implement different levels of security-check inspections for your applications. You can initially monitor the logs to observe what security threats are being detected and which violations are being triggered. Rule creation is made straightforward with the application firewall’s rule engine, which supports two types of rules – learned rules and relaxation rules. You can either manually add relaxation rules or take advantage of the application firewall’s recommended learned rules to deploy the required relaxations to avoid false positives.

The Citrix application firewall offers visualizer support in the GUI, which makes rule management very easy. You can easily view all the data on one screen, and take action on several rules with one click. The biggest advantage of the visualizer is that it recommends regular expressions to consolidate several rules. You can select a subset of the rules, basing your selection on the delimiter and Action URL. Visualizer support is available for viewing 1) learned rules and 2) relaxation rules.

1) The visualizer for learned rules offers the option to edit the rules and deploy them as relaxations. You can also skip (ignore) rules.

2) The visualizer for deployed relaxations offers you the option to add a new rule or edit an existing one. You can also enable or disable a group of rules by selecting a node and clicking the Enable or Disable button in the relaxation visualizer.

A signature is an object that can have multiple rules. Each rule consists of one or more patterns that can be associated with a specified set of actions. The application firewall has a built-in default signature object consisting of more than 1,300 signature rules, with an option to get the latest rules by using the auto-update feature to get protection against new vulnerabilities. Rules created by other scan tools can also be imported.

Signatures are very powerful because they use pattern matching to detect malicious attacks and can be configured to check both the request and the response of a transaction. They are a preferred option when a customizable security solution is needed. Multiple action choices (for example, block, log, learn, and transform) are available for when a signature match is detected. The default signatures, such as web-cgi, web-coldfusion, web-frontpage, web-iis, web-php, web-client, web-activex, web-shell-shock, and web-struts, cover rules to protect different types of applications. To match the needs of your application, you can select and deploy the rules belonging to a specific category.
Signature usage tips:

• You can just make a copy of the default signature object and modify it to enable the rules you need and configure the actions you want.
• The signature object can be customized by adding new rules, which can work in conjunction with other signature rules.
• The signature rules can also be configured to work in conjunction with the security checks specified in the application firewall profile. If a match indicating a violation is detected by a signature as well as a security check, the more restrictive action is the one that gets enforced.
• A signature rule can have multiple patterns and be configured to flag a violation only when all the patterns are matched, thereby avoiding false positives.
• Careful selection of a literal fast-match pattern for a rule can significantly optimize processing time.

Integrating with other NetScaler features
The application firewall is fully integrated into the NetScaler appliance and works seamlessly with other features. You can configure maximum security for your application by using other NetScaler security features in conjunction with the application firewall. For example, AAA-TM can be used to authenticate the user, check the user’s authorization to access the content, and log the accesses, including invalid login attempts. Rewrite can be used to modify the URL or to add, modify or delete headers, and responder can be used to deliver customized content to different users. You can define the maximum load for your website by using rate limiting to monitor the traffic and throttle the rate if it is too high. HTTP Denial-of-Service (DoS) protection can help distinguish between real HTTP clients and malicious DoS clients. You can narrow the scope of security-check inspection by binding the application firewall policies to virtual servers, while still optimizing the user experience by using the load balancing feature to manage heavily used applications. Requests for static objects such as images or text can bypass security check inspection, taking advantage of integrated caching or compression to optimize the bandwidth usage for such content.

Packet Processing with NetScaler and AppFirewall
The flow of a packet in the NetScaler appliance is shown in the diagram below. This diagram is also available in the Processing Order of Features section at http://docs.citrix.com/en-us/netscaler/11/getting-started-with-netscaler.html.
Standard Workflow for Deploying AppFirewall

**Know your environment:** Knowing your environment will help you to identify the best security protection solution (signatures, security checks, or both) for your needs. Before you begin configuration, you should gather the following information.

- **OS:** What kind of OS (MS Windows, Linux, BSD, Unix, others) do you have?
- **Web Server:** What web server (IIS, Apache or NetScaler Enterprise Server) are you running?
- **Application:** What type of applications are running on your application server (for example, ASP.NET, PHP, Cold Fusion, ActiveX, FrontPage, Struts, CGI, Apache Tomcat, Domino, and WebLogic)?
- **Do you have customized applications or off-the-shelf (for example, Oracle, SAP) applications? What version you are using?**
- **SSL:** Do you require SSL? If so, what key size (512, 1024, 2048, 4096) is used for signing certificates?
- **Traffic Volume:** What is the average traffic rate through your applications? Do you have seasonal or time-specific spikes in the traffic?
- **Server Farm:** How many servers do you have? Do you need to use load balancing?
- **Database:** What type of database (MS-SQL, MySQL, Oracle, Postgres, SQLite, nosql, Sybase,
• DB Connectivity: What kind of data base connectivity do you have (DSN, per-file connection string, single file connection string) and what drivers are used?

**Identify your security needs:** You might want to evaluate which applications or specific data need maximum security protection, which ones are less vulnerable, and the ones for which security inspection can safely be bypassed. This will help you in coming up with an optimal configuration, and in designing appropriate policies and bind points to segregate the traffic. For example, you might want to configure a policy to bypass security inspection of requests for static web content, such as images, MP3 files, and movies, and configure another policy to apply advanced security checks to requests for dynamic content. You can use multiple policies and profiles to protect different contents of the same application.

**License requirement:** Citrix offers a unified solution to optimize the performance of your application by taking advantage of a rich set of features such as load balancing, content switching, caching, compression, responder, rewrite, and content filtering, to name a few. Identifying the features that you want can help you decide which license you need.

**Install and baseline a NetScaler appliance:** Create a virtual server and run test traffic through it to get an idea of the rate and amount of traffic flowing through your system. This information will help you to identify your capacity requirement and select the right appliance (VPX, MPX, or SDX). For a detailed description of various available platforms and their throughput capabilities, see the following data sheet: https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/netscaler-data-sheet.pdf?accessmode=direct

**Deploy the application firewall:** Use the application firewall wizard to proceed with a simple security configuration. The wizard walks you through several screens and prompts you to add a profile, policy, signature, and security checks.

  • **Profile:** Select a meaningful name and the appropriate type (HTML, XML or WEB 2.0) for your profile. The default policy and signatures will be auto-generated using the same name.
  • **Policy:** The auto-generated policy has the default expression (true), which selects all traffic and is bound globally. This is a good starting point unless you have in mind a specific policy that you want to use.
  • **Protections:** The wizard helps you take advantage of the hybrid security model, in which you can use the default signatures offering a rich set of rules to protect different types of applications. Simple edit mode allows you to view the various categories (CGI, Cold Fusion, PHP, etc.). You can select one or more categories to identify a specific set of rules applicable to your application. Use the Action option to enable all the signature rules in the selected categories. Make sure that blocking is disabled, so that you can monitor the traffic before tightening the security. Click Continue. In the Specify Deep protections pane, you can make changes as needed to deploy the security check protections. In most cases, basic protections are sufficient for initial security configuration. Run the traffic for a while to collect a representative sample of the security-inspection data.
Tightening the security: After deploying the application firewall and observing the traffic for a while, you can start tightening the security of your applications by deploying relaxations and then enabling blocking. Learning, visualizer, and click-to-deploy rules are useful features that make it very easy to tweak your configuration to come up with just the right level of relaxation. At this point, you can also change the policy expression and/or configure additional policies and profiles to implement desired levels of security for different types of content.

Debugging: If you see unexpected behavior of your application, the application firewall offers various options for easy debugging:

- Log: If legitimate requests are getting blocked, your first step is to check the ns.log file to see if any unexpected security-check violation is being triggered.
- Disable feature: If you do not see any violations but are still seeing unexpected behavior, such as an application resetting or sending partial responses, you can temporarily disable the application firewall feature. If the issue persists, it rules out the application firewall as a suspect.
- Trace records with log messages: If the issue appears to be application firewall related and needs closer inspection, you have the option to include security violation messages in an nstrace. You can use “Follow TCP stream” in the trace to view the details of the individual transaction, including headers, payload, and the corresponding log message, together on the same screen. Details of how to use this functionality are available at http://docs.citrix.com/en-us/netscaler/11/security/application-firewall/appendixes/nstrace-with-violation-logs.html.

Deploying the AppFirewall

Initiate the WAF wizard by navigating to Security > Application Firewall and clicking the Application Firewall Wizard link in the Getting Started section. This will give you the screen shown below –

Add an application firewall profile and select the appropriate type (htmlHTML, xmlXML, wWeb2.0) for the security requirements of the application.

Choosing the right profile - The application firewall profile offers protection for both HTML and XML payloads. Depending on the need of your application, you can choose either a an HTML profile or an XML profile. If your application supports both HTML and XML data, you can choose a Web 2.0 profile. Select an appropriate profile at the next screen (screenshot on the next page).
Basic and Advanced Profiles

When you choose to add a new profile by navigating to Security > Application Firewall > Profiles through the NetScaler GUI, you will get a screen similar to the one above, but with the additional option of choosing between a basic and an advanced profile, as shown below.

The decision to use a basic or an advanced profile depends on the security need of your application. A basic profile includes a preconfigured set of Start URL and Deny URL relaxation rules. These relaxation rules determine which requests are allowed and which are denied. Incoming requests are matched with the preconfigured rules, and the configured actions are applied. The user can secure applications with minimal configuration of relaxation rules. The Start URL rules protect against forceful browsing. Known web server vulnerabilities that are exploited by hackers can be detected and blocked by enabling a set of default Deny URL rules. Commonly launched attacks, such as Buffer Overflow, SQL, or Cross-Site Scripting can also be easily detected.
As the name indicates, advanced protections are for applications that have higher security requirements. Relaxation rules are configured to allow access to only specific data and block the rest. This positive security model mitigates unknown attacks, which might not be detected by basic security checks. In addition to all the basic protections, an advanced profile keeps track of a user session by controlling the browsing, checking for cookies, specifying input requirements for various form fields, and protecting against tampering of forms or Cross-Site Request Forgery attacks. Learning, which observes the traffic and recommends the appropriate relaxations, is enabled by default for many security checks. Although easy to use, advanced protections require due consideration, because they offer tighter security but also require more processing. Some advance security checks do not allow use of caching, which can affect performance.

Keep the following points in mind when deciding whether to use basic or advanced profiles:

- Basic and advanced profiles are just starting templates. You can always modify the basic profile to deploy advanced security features, or change an advanced profile to use basic features.
- Advanced security checks require more processing and can affect performance. Unless your application needs advanced security, you might want to start with a basic profile and tighten the security as required for your application.
- You do not want to enable all security checks unless your application needs them.

Next, a rule must be specified that defines what type of traffic is evaluated by the current configuration. The rule is defined by an expression as shown below.

To have this policy evaluate all traffic, set the expression to true. To specify the type of traffic to evaluate, use the Frequently Used Expressions drop-down list and the expression editor to create a custom expression.

To have this policy evaluate all traffic, set the expression to true. To specify the type of traffic to evaluate, use the Frequently Used Expressions drop-down list and the expression editor to create a custom expression. Click Continue, and then add or select an existing signature on the screen shown in the next screenshot.

Note: AppFirewall also supports WSDL, which is applicable for XML or Web 2.0 profiles but is not part of the standard wizard workflow. WSDL files have to be imported separately at Security > Application Firewall > Imports > WSDL in the NetScaler GUI.
In the screen above, you can either create a new signature or select a pre-existing signature. After selection, to edit the signature you can use the simple or the advanced edit mode. The simple mode allows for easy configuration of the signature, with a preset list of protection definitions for common applications such as IIS (Internet Information Server), PHP and ActiveX. The advanced mode allows for more granular control over the signature definitions and provides significantly more information. Use the advanced mode if you want complete control over signature definition. The screen for simple configuration is as shown below -

Advanced mode presents a lot more options, as shown in the screenshot on the next page -
Next, after selecting the appropriate signatures and clicking continue, you will be shown the screen below. Here, you can configure the deep protections that this profile should support, as determined by the specific attack types that the protected application might be vulnerable to. Each application will have an appropriate profile that will allow it to function optimally.

![Specify Deep Protections](image-url)

<table>
<thead>
<tr>
<th>Name</th>
<th>Block</th>
<th>Log</th>
<th>Stats</th>
<th>Learn</th>
<th>Check Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start URL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>Common</td>
</tr>
<tr>
<td>Deny URL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>Common</td>
</tr>
<tr>
<td>Cookie Consistency</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td></td>
<td>Common</td>
</tr>
<tr>
<td>Buffer Overflow</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>Common</td>
</tr>
<tr>
<td>Credit Card</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>Common</td>
</tr>
<tr>
<td>Content-type</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td>Common</td>
</tr>
<tr>
<td>Form Field Consistency</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>HTML</td>
</tr>
<tr>
<td>Field Formats</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>CSRF Form Tagging</td>
<td>✗</td>
<td>✓</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>HTML Cross-Site Scripting</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>HTML SQL Injection</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
</tbody>
</table>

[Continue] [Cancel]
When you click Continue, the wizard ends and completes creation of the configuration profile. The default policy created by the wizard is bound globally.

**Custom Policy Bindings**
To bind a policy to a particular target bind point (for example, bind globally or to a specific LB vserver. Other options are available as well) and specify the priority, go to Security > Application Firewall and click on the link for Application Firewall Policy Manager under Policy Manager. On the screen that appears, select the bind point, which can be global (Override Global) or a specific load balancing virtual server. The following example shows the selection of a load balancing virtual server as the bind point.

![Application Firewall Policy Manager](image)

After selecting the bind point, choose the policy that you would like to bind on the next screen, shown below -

![Application Firewall Policy Manager](image)
Choosing a policy and bind point

Application firewall policies can help sort your traffic into logical groups for configuring different levels of security implementation. Carefully select the bind points for the policies to determine which traffic is matched against which policy. For example, if you want every incoming request to be checked for SQL/XSS attacks, you can create a generic policy and bind it globally. Or, if you want to apply more stringent security checks to the traffic of a virtual server hosting applications that contain sensitive data, you can bind a policy to that virtual server.

Careful assignment of priorities can enhance the traffic processing. You want to assign higher priorities to more specific policies and lower priorities to generic policies. Note that the higher the number, the lower the priority. A policy with a priority of 10 is evaluated before a policy that has a priority of 15.

You can apply different levels of security for different kinds of contents, e.g. requests for static objects like images and text can be bypassed by using one policy and requests for other sensitive contents can be subjected to a much stringent check by using a second policy.

After you bind the policy to the correct bind point, the application firewall begins applying the policy to filter traffic arriving at the bind point.

Conclusion

Citrix NetScaler AppFirewall enables a completely secured application delivery experience for enterprises. A winner in the Best of Application Firewalls category in TechTarget’s Reader’s Choice awards, recommended by NSS Labs and ICSA certified after stringent testing, NetScaler AppFirewall ticks all the boxes for enterprise application security requirements and is ideal for deployments in enterprise environments of all sizes. By utilizing the right mix of licensing and policy/rule/signature definition, AppFirewall can secure any enterprise environment.