Securing Oracle E-Business Suite with NetScaler AppFirewall

Solution Guide

This guide focuses on defining the process for securing Oracle E-Business Suite with NetScaler AppFirewall

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 bi-directional traffic, including SSL-encrypted communication, to protect against a broad range of security threats without any modification to applications.

Introduction

NetScaler AppFirewall technology is included in and integrated with Citrix® NetScaler® MPX and 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 via software license to a full NetScaler Application Delivery Controller (ADC).

Oracle E-Business Suite 12c (also known as Applications/Apps or EB-Suite/EBS) consists of a collection of enterprise resource planning (ERP), customer relationship management (CRM), and supply-chain management (SCM) computer applications.

To implement Oracle E-Business Suite security, the Citrix NetScaler application firewall offers an easy-to-configure security solution using the hybrid model. A set of built-in signatures with auto-update support offer protection against web-iis vulnerabilities. Deep protections such as Buffer Overflow, SQL Injection and Cross-Site Scripting security checks can effectively thwart any attempt to exploit application vulnerabilities. Each request is inspected to identify any malicious content, and specified actions are taken to either block such content or render it harmless by transforming it.

This guide focuses on defining the guidelines for securing Oracle E-Business Suite access with Citrix NetScaler AppFirewall.

Recommended Product Versions

Product	Version
Oracle E-Business Suite Server	12.2.x
NetScaler VPX (AppFirewall Integrated Module)	11.0 (Enterprise/Platinum License)

Configuration

Summary of Steps

- Create a service for local virtual server.
- Create load balancing virtual server.
- Create signatures for the application firewall and enable the built-in rules in the web-iis category.
- Create an application-firewall profile.
- Configure the profile's security checks to enable Buffer Overflow, XSS and SQL Injection protections.
- Configure the profile's settings to bind signatures and exclude file uploads from inspection, to prevent false positives.
- Create an application firewall policy with an expression that identifies the traffic flowing to and from the application, and an action that applies the configured profile's protections to the traffic.
- Bind the policy to the load balancing virtual server.
- Monitor logs and tweak the configuration. Deploy relaxation rules to avoid false positives, if needed.

Deployment guidelines

Before beginning this deployment, please test that the Oracle E-Business Suite setup can be accessed at https://<E-Business suite URI>

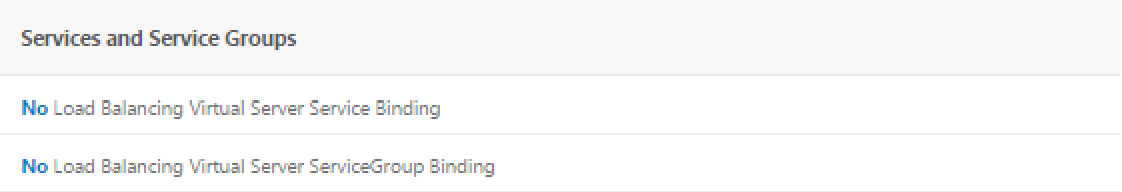
Creating a Service

If it does not already exist, create a service bound to the E-Business service on port 443. Specify the protocol as SSL and the port as 443 (or an alternate port as per your E-Business server configuration)

Create and add a load balancing virtual server

Add a load balancing (LB) virtual server (vserver) that the E-Business service created earlier will be bound to. The protocol should be set as SSL and port should be 443, or any alternate port as per your E-Business server setup.

Bind the service created earlier to the LB along with the required SSL certificates by clicking on the headers in the Services and Service Groups tab section header in the Basic Settings screen for the LB vserver -



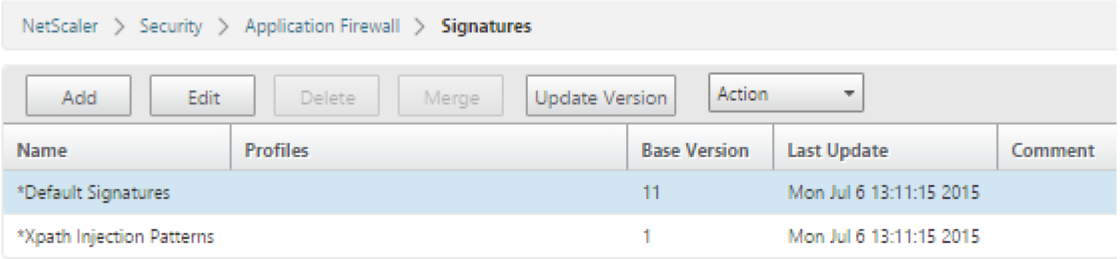
Services and Service Groups

No Load Balancing Virtual Server Service Binding

No Load Balancing Virtual Server ServiceGroup Binding

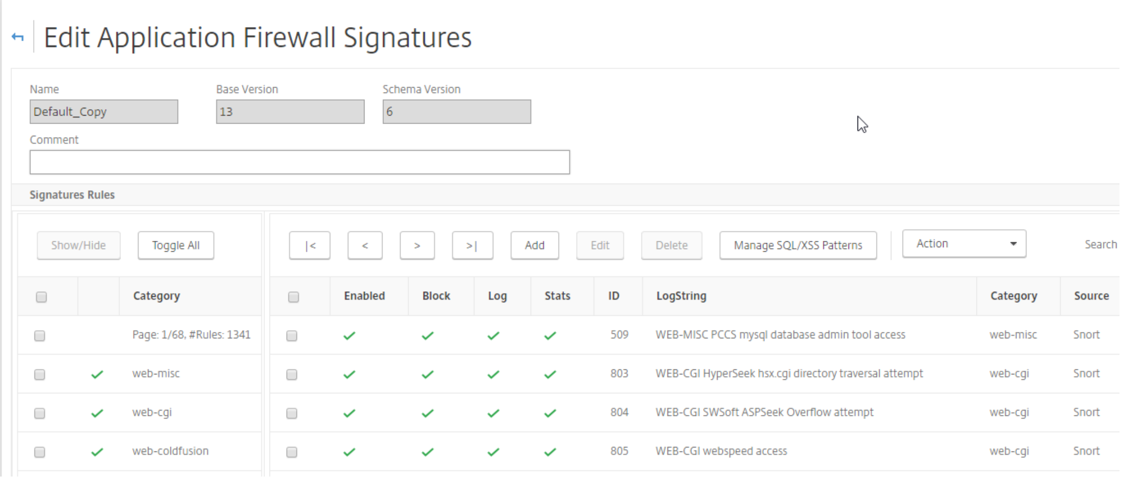
Application Firewall Configuration

Make a copy of the application firewall default signatures by clicking on Export under the Action dropdown on the AppFirewall Signatures screen at Security>AppFirewall>Signatures.



Name	Profiles	Base Version	Last Update	Comment
*Default Signatures		11	Mon Jul 6 13:11:15 2015	
*Xpath Injection Patterns		1	Mon Jul 6 13:11:15 2015	

For this configuration, we will be using the default signatures that are present within the AppFirewall configuration.



Edit Application Firewall Signatures

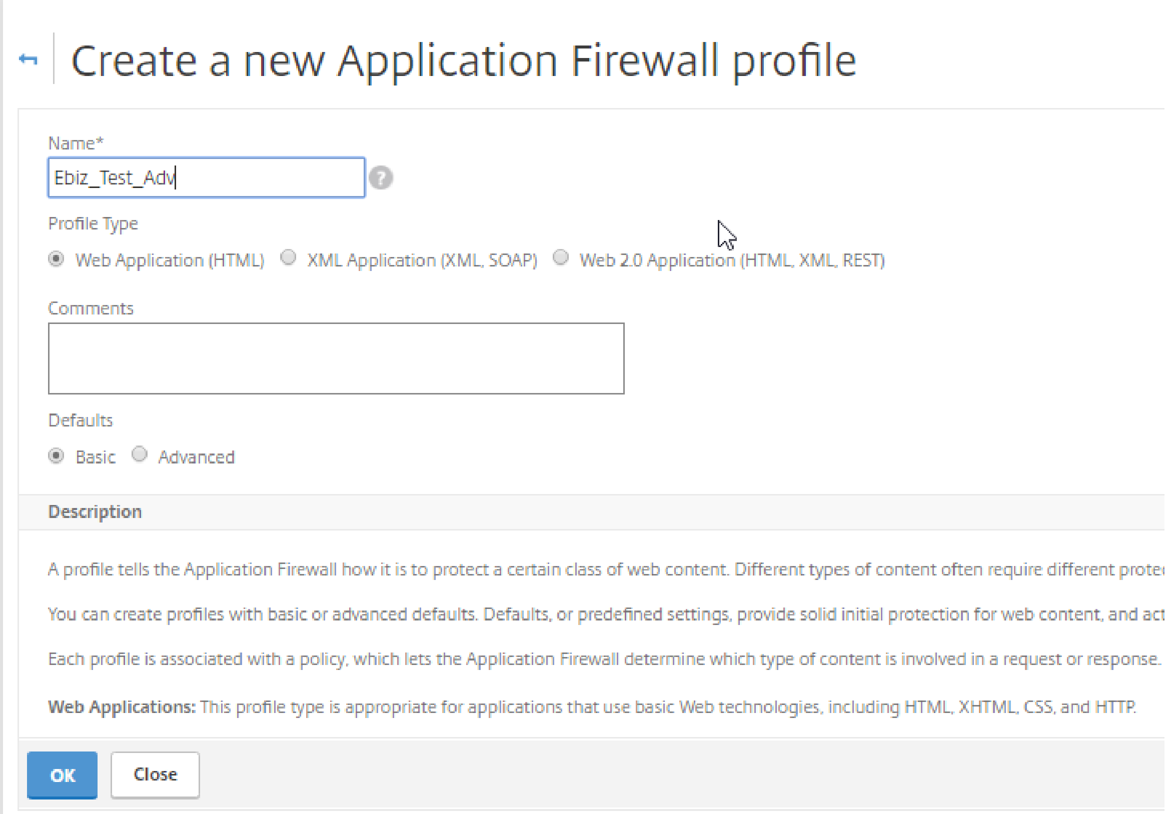
Name: Default_Copy
Base Version: 13
Schema Version: 6
Comment:

Signatures Rules

□		Category
□		Page: 1/68, #Rules: 1341
□	✓	web-misc
□	✓	web-cgi
□	✓	web-coldfusion

□	Enabled	Block	Log	Stats	ID	LogString	Category	Source
□	✓	✓	✓	✓	509	WEB-MISC PCCS mysql database admin tool access	web-misc	Snort
□	✓	✓	✓	✓	803	WEB-CGI HyperSeek hsx.cgi directory traversal attempt	web-cgi	Snort
□	✓	✓	✓	✓	804	WEB-CGI SWSoft ASPSeek Overflow attempt	web-cgi	Snort
□	✓	✓	✓	✓	805	WEB-CGI webspeed access	web-cgi	Snort

Add a basic application firewall profile for the Oracle E-Business application by navigating to Security> Application Firewall> Profiles and clicking on Add. Use a meaningful name to keep track of the purpose of the profile. Set the profile type to Web Application and Defaults to Basic. (The following example shows EBiz_Test_Adv as the profile name. It is recommended for easier manageability, however, that an indicative suffix be added to the name, such as _prof for a profile name)



Create a new Application Firewall profile

Name*: Ebiz_Test_Adv

Profile Type
● Web Application (HTML) ○ XML Application (XML, SOAP) ○ Web 2.0 Application (HTML, XML, REST)

Comments

Defaults
● Basic ○ Advanced

Description

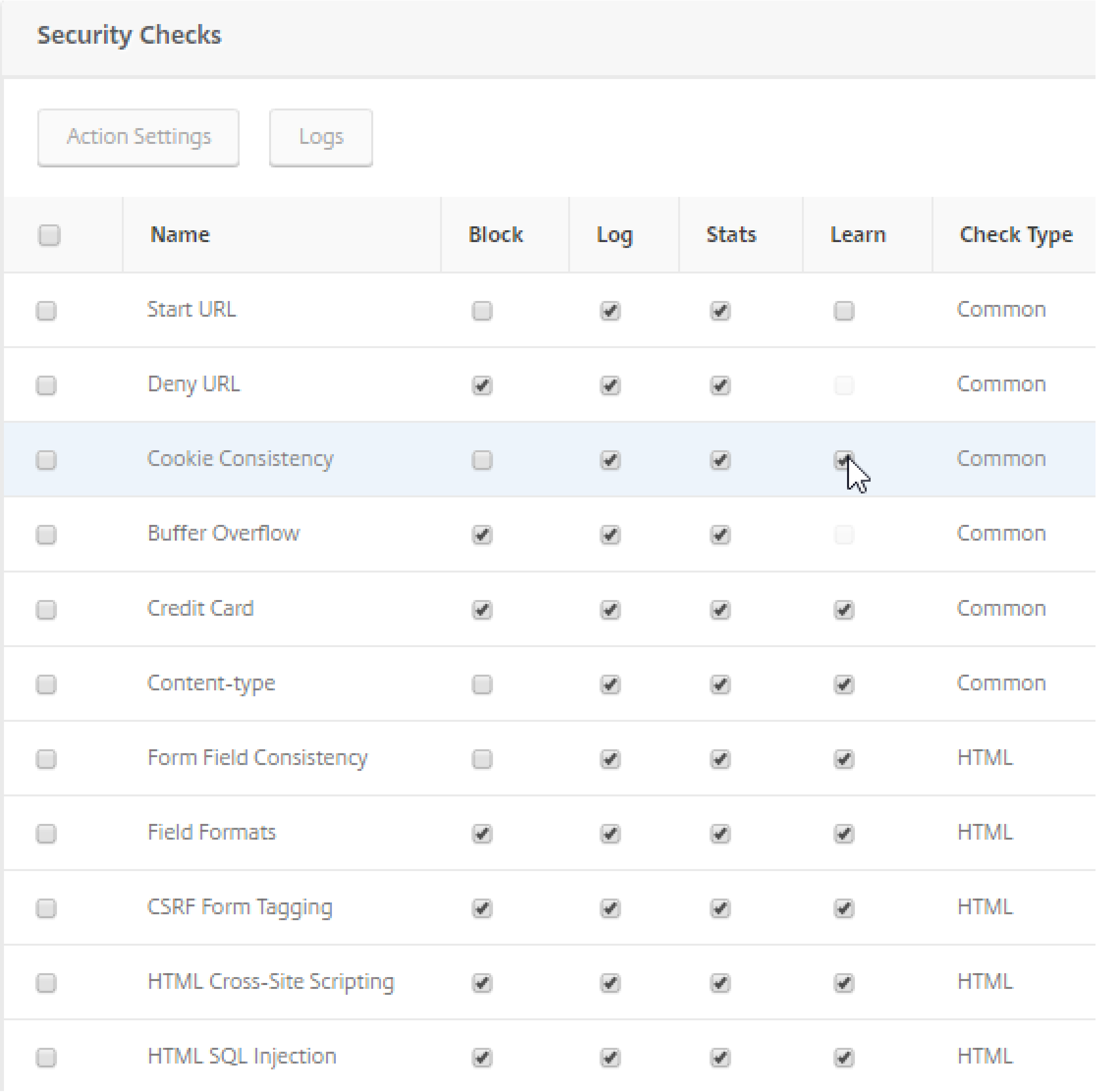
A profile tells the Application Firewall how it is to protect a certain class of web content. Different types of content often require different prote

You can create profiles with basic or advanced defaults. Defaults, or predefined settings, provide solid initial protection for web content, and act

Each profile is associated with a policy, which lets the Application Firewall determine which type of content is involved in a request or response.

Web Applications: This profile type is appropriate for applications that use basic Web technologies, including HTML, XHTML, CSS, and HTTP.

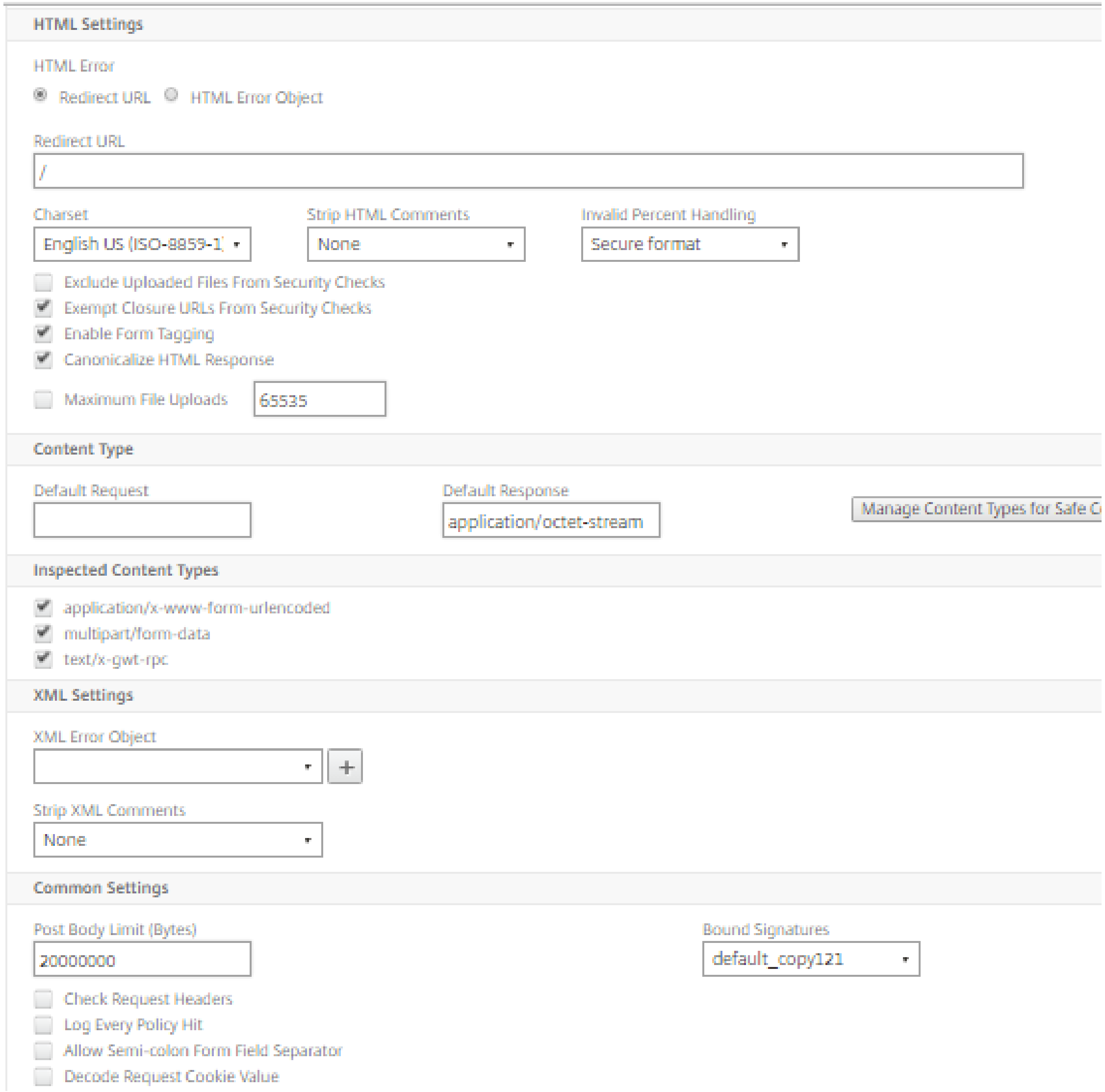
Configure the security checks of the newly added profile by clicking on the profile name and clicking on Edit on the profile list page. Web Applications have two types of checks, one common set and one set for HTML.



Security Checks

□	Name	Block	Log	Stats	Learn	Check Type
□	Start URL	□	☑	☑	□	Common
□	Deny URL	☑	☑	☑	□	Common
□	Cookie Consistency	□	☑	☑	☑	Common
□	Buffer Overflow	☑	☑	☑	□	Common
□	Credit Card	☑	☑	☑	☑	Common
□	Content-type	□	☑	☑	☑	Common
□	Form Field Consistency	□	☑	☑	☑	HTML
□	Field Formats	☑	☑	☑	☑	HTML
□	CSRF Form Tagging	☑	☑	☑	☑	HTML
□	HTML Cross-Site Scripting	☑	☑	☑	☑	HTML
□	HTML SQL Injection	☑	☑	☑	☑	HTML

The screenshot above shows the required settings for Common and HTML checks. Some of the checks are not enabled for blocking, as they check for behaviours that may overlap with the normal behaviour of E-Business Suite, blocking which would interfere with the normal operation of these applications. However, any such instances are logged for later auditing.



HTML Settings

HTML Error

● Redirect URL ○ HTML Error Object

Redirect URL: /

Charset: English US (ISO-8859-1)

Strip HTML Comments: None

Invalid Percent Handling: Secure format

☐ Exclude Uploaded Files From Security Checks
☑ Exempt Closure URLs From Security Checks
☑ Enable Form Tagging
☑ Canonicalize HTML Response
☐ Maximum File Uploads 65535

Content Type

Default Request:

Default Response: application/octet-stream

Inspected Content Types

☑ application/x-www-form-urlencoded
☑ multipart/form-data
☑ text/x-gwt-rpc

XML Settings

XML Error Object:

Strip XML Comments: None

Common Settings

Post Body Limit (Bytes): 20000000

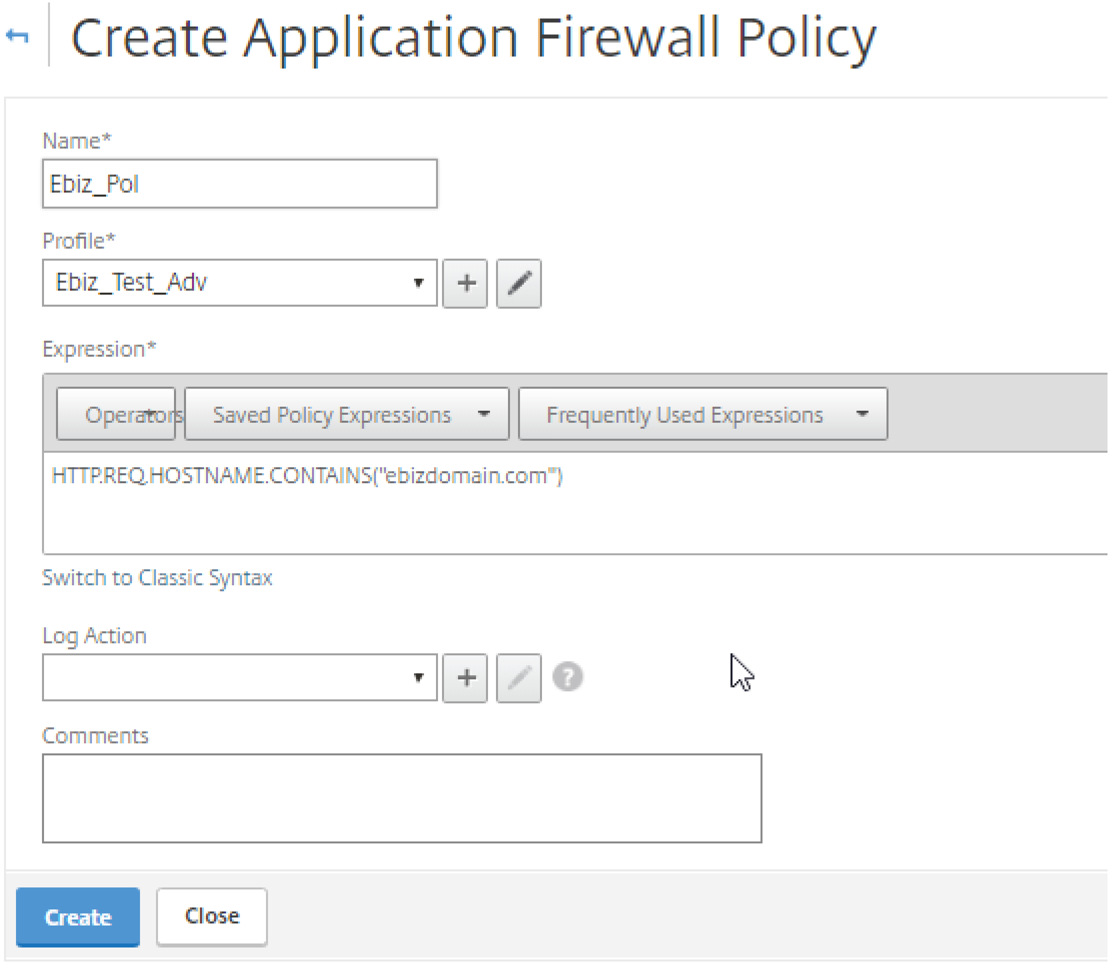
Bound Signatures: default_copy121

☐ Check Request Headers
☐ Log Every Policy Hit
☐ Allow Semi-colon Form Field Separator
☐ Decode Request Cookie Value

Configure the profile's settings as shown above by clicking on the Profile Settings tab. Bind the signatures to the profile in the Bound Signatures drop down (here, we have selected a default copy that was made earlier).

Now, navigate to Security>Application Firewall>Policies> Application Firewall Policies. Create an application firewall policy for the Oracle E-Business profile and bind the policy to the E-Business LB vserver.

The following example uses the expression HTTP.REQ.HOSTNAME.CONTAINS("Ebizdomain.com") to select the target traffic for the policy (replace EBizdomain.com with your Oracle E-Business Suite domain)



Create Application Firewall Policy

Name*: Ebiz_Pol

Profile*: Ebiz_Test_Adv

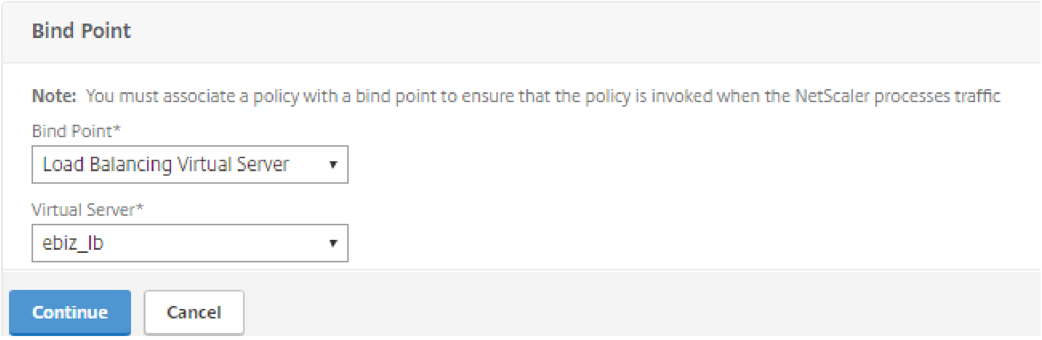
Expression*:

```
HTTP.REQ.HOSTNAME.CONTAINS("ebizdomain.com")
```

Log Action:

Comments:

On the policy listing screen , select the newly added policy and click Policy Manager. From the Bind Point options, select Load Balancing Virtual Server. The Virtual Server field now becomes visible. From this field's drop-down list, select the E-Business virtual server that you created earlier. Click Continue to display the Bind Point pane.

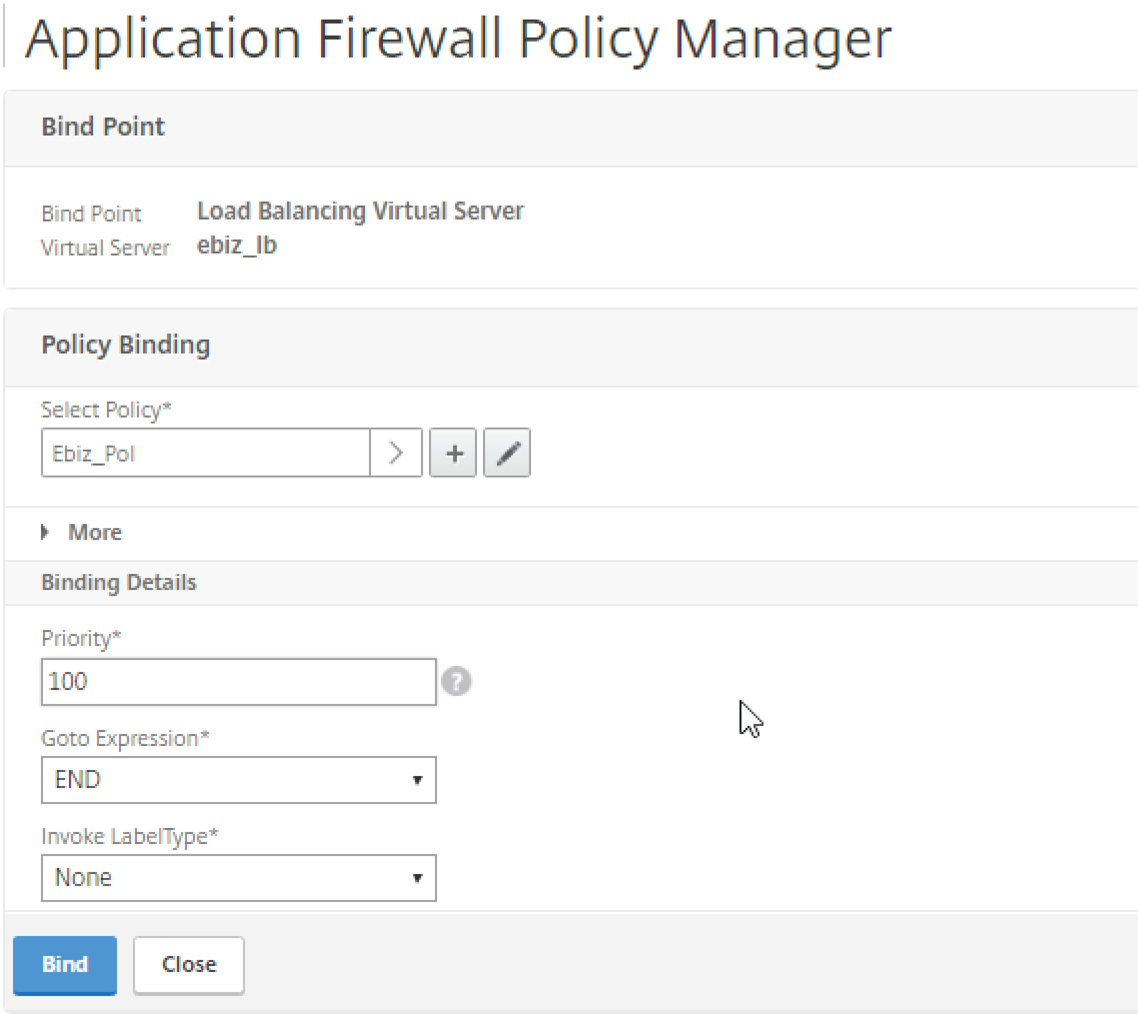


Bind Point

Note: You must associate a policy with a bind point to ensure that the policy is invoked when the NetScaler processes traffic

Bind Point*: Load Balancing Virtual Server

Virtual Server*: ebiz_lb



Application Firewall Policy Manager

Bind Point

Bind Point Load Balancing Virtual Server
Virtual Server ebiz_lb

Policy Binding

Select Policy* Ebiz_Pol

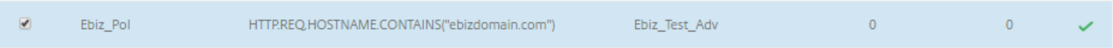
Priority* 100

Goto Expression* END

Invoke LabelType* None

In the Select Policy field, click the arrow to display the policy options. Select the E-Business policy, enter binding details and click Bind. On the next screen, if binding details are correct, click Done.

In the Application Firewall Policies pane, refresh the page. A Green check mark appears in the Active Column to indicate that the policy is now active.

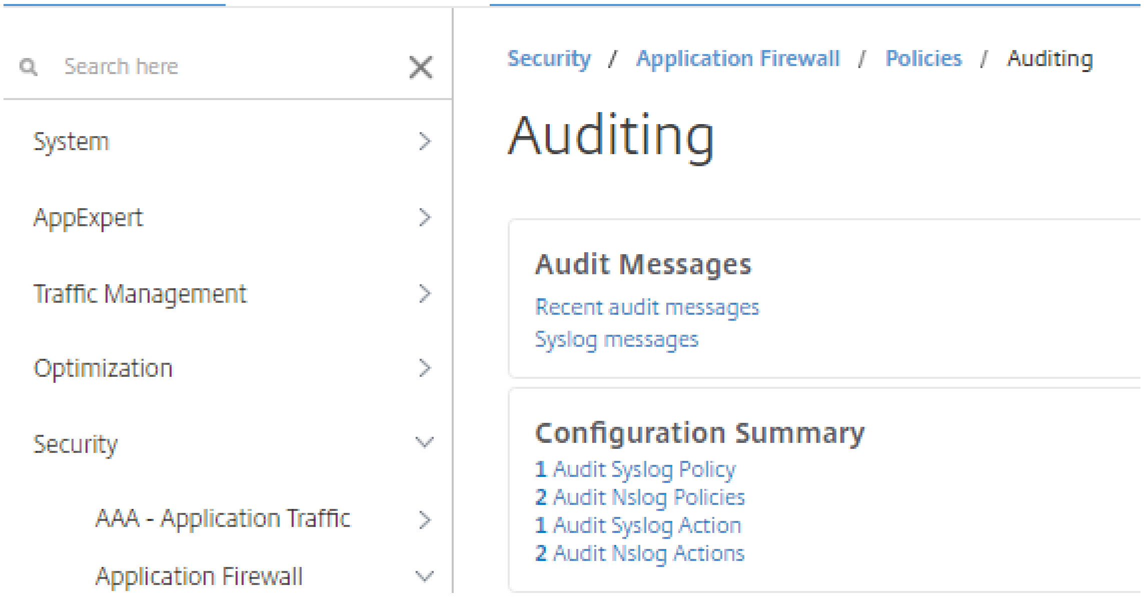


☑	Ebiz_Pol	HTTP.REQ.HOSTNAME.CONTAINS("ebizdomain.com")	Ebiz_Test_Adv	0	0	✓

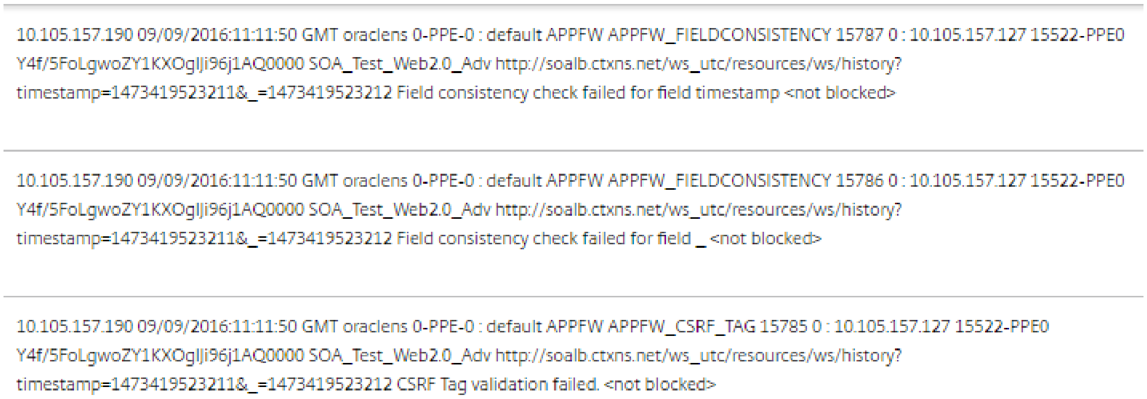
The Oracle E-Business Suite server is now protected by the application firewall. You can monitor the /var/log/ns.log to verify whether any violations are getting triggered, and fine-tune the security check configuration by adding relaxation rules if needed.

Troubleshooting

Violations are noted in the NetScaler Syslog (accessible at Security>Application Firewall>Policies>Auditing as shown below)

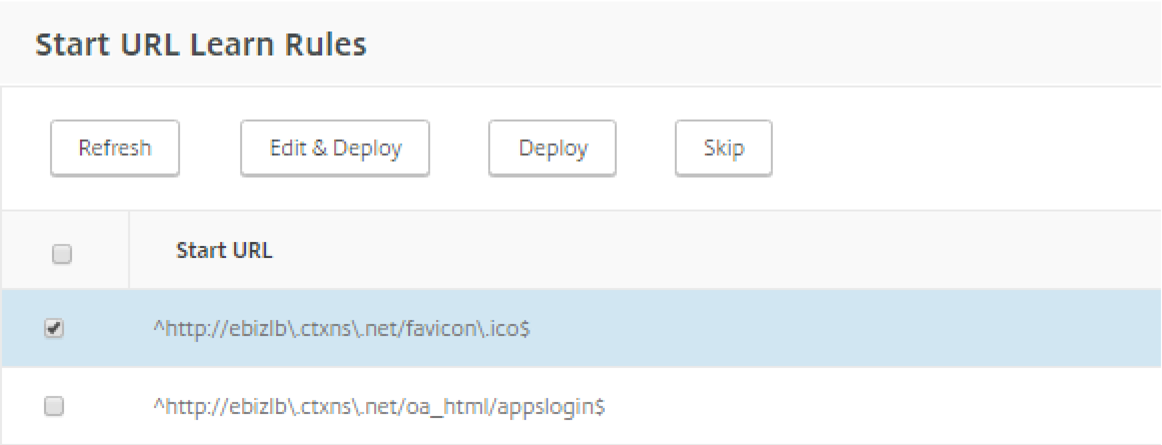


Syslog messages are shown in the GUI unfiltered. Once messages are loaded, it is possible to filter them by module, as the syslog contains messages for all NetScaler modules. To note only Application Firewall messages, choose the APPFW option in the modules dropdown located on the right hand side of the page. Some sample errors:

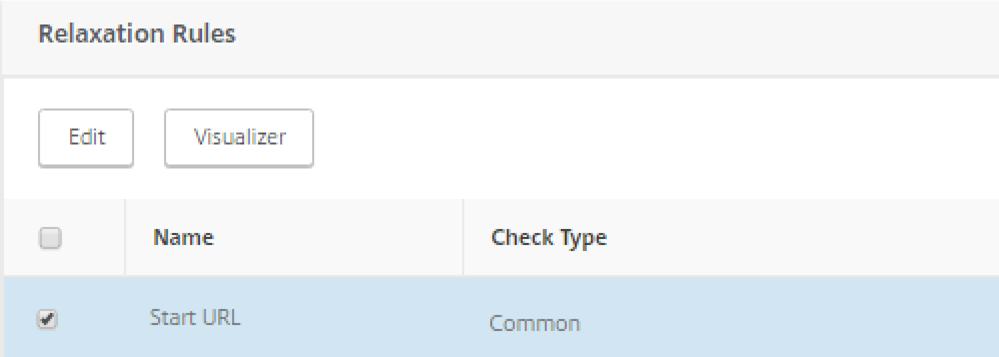


```
10.105.157.190 09/09/2016:11:11:50 GMT oraclens 0-PPE-0 : default APPFW APPFW_FIELDCONSISTENCY 15787 0 : 10.105.157.127 15522-PPE0
Y4f/5FoLgwoZY1KXOgIJi96j1AQ0000 SOA_Test_Web2.0_Adv http://soalb.ctxns.net/ws_utc/resources/ws/history?
timestamp=1473419523211&_=1473419523212 Field consistency check failed for field timestamp <not blocked>

10.105.157.190 09/09/2016:11:11:50 GMT oraclens 0-PPE-0 : default APPFW APPFW_FIELDCONSISTENCY 15786 0 : 10.105.157.127 15522-PPE0
Y4f/5FoLgwoZY1KXOgIJi96j1AQ0000 SOA_Test_Web2.0_Adv http://soalb.ctxns.net/ws_utc/resources/ws/history?
timestamp=1473419523211&_=1473419523212 Field consistency check failed for field _ <not blocked>

10.105.157.190 09/09/2016:11:11:50 GMT oraclens 0-PPE-0 : default APPFW APPFW_CSRF_TAG 15785 0 : 10.105.157.127 15522-PPE0
Y4f/5FoLgwoZY1KXOgIJi96j1AQ0000 SOA_Test_Web2.0_Adv http://soalb.ctxns.net/ws_utc/resources/ws/history?
timestamp=1473419523211&_=1473419523212 CSRF Tag validation failed. <not blocked>
```

When the Learn option is enabled for Application Firewall, the module learns violations that are being repeated, which may indicate that they are potential false positives. These learned rules are generated and maintained in the Learned Rules section within the profile page. These rules can be reviewed and enabled selectively, allowing relaxations for such false positives. These rules can also be created manually using the Relaxation Rules option. The rule editor processes standard regular expressions.



□	Start URL
☑	^http://ebizlb\.ctxns\.net/favicon\.ico$
□	^http://ebizlb\.ctxns\.net/oa_html/appslogin$



□	Name	Check Type
☑	Start URL	Common

Conclusion

Citrix NetScaler AppFirewall enables a completely secured application delivery experience for enterprises with Oracle E-Business Suite by utilizing the right mix of licensing and policy/rule/signature definitions. With the recommendations provided in this guide, enterprises can expect a secure experience while providing continued access to Oracle E-Business Suite to their employees and partners.

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309 United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054 United States