This solution guide provides guidelines for securing Exchange 2013 Outlook Web Access (OWA) with NetScaler Application Firewall.
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).

Microsoft OWA 2013 is a web-based email client that enables users to access emails and contacts, and to share a web calendar. It is supported by all major browsers. To implement OWA 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 the 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 OWA 2013 access with 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>
<tr>
<td>Microsoft Exchange Server/OWA</td>
<td>2013</td>
</tr>
</tbody>
</table>
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

Creating a Service

If it does not already exist, create a service bound to the OWA service on port 443 (the IP provided will normally be that of the client access server (CAS) in your Exchange 2013 setup). Specify the protocol as SSL and the port as 443 (or an alternate port as per your Exchange server configuration).
Create and add a load balancing virtual server

Add a load balancing (LB) virtual server (vserver) that the OWA 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 Exchange server setup.

![Load Balancing Virtual Server](image)

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

![Services and Service Groups](image)
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.

Now, add a signature by clicking on Add above, then edit the name and add comments so that the rule is distinguishable. Use the Show/Hide button to select web-iis to isolate all the rules for this Category. By default the signature rules are disabled. Click the down-arrow on the Action button, and select Enable All Searched Rules to enable all the selected rules. (The following example shows owa_sig as the signature name.)
Add a basic application firewall profile for the OWA 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 owa_profile as the profile name.)

Configure the security checks of the newly added profile by clicking on the profile name and clicking on Edit on the profile list page. Enable the Block, Log, Learn, and Stats actions for the SQL Injection and Cross-Site Scripting checks. Enable the Block, Log and Stats actions for the Buffer Overflow check. Disable all actions for the rest of the security checks.
Configure the profile's settings. Bind the signatures to the profile and select the check box for Exclude Uploaded Files from Security Checks.

Now, navigate to Security>Application Firewall>Policies> Application Firewall Policies. Create an application firewall policy for the OWA profile and bind the policy to the LB vserver.
The following example uses the expression HTTP.REQ.HOSTNAME.EQ("www.mail.com") to select the target traffic. (replace www.mail.com with your email domain)

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 OWA virtual server that you created earlier. Click Continue to display the Bind Point pane.
In the Select Policy field, click the arrow to display the policy options. Select the OWA policy and click Select. Click Bind.

Now, in the Bind Point pane, 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.

The Microsoft OWA application is now protected by the application firewall. You can monitor the /var/log/ns.log to verify whether any violations are being detected, and fine-tune the security check configuration by adding relaxation rules if needed.

**Conclusion**

Citrix NetScaler AppFirewall enables a completely secured application delivery experience for enterprises with Outlook Web Access 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 email, calendar, tasks and other essential business information to their employees and partners.