Microsoft Exchange 2013 with NetScaler: Authentication and Optimization

Deployment Guide

This deployment guide focuses on enabling authentication and optimization with NetScaler for Exchange 2013 deployments.
Table of Contents

Introduction 3
Configuration Details 4
NetScaler features to be enabled 4
Steps for authentication and optimization configuration 5
Enabling authentication to Exchange 2013 with NetScaler 6
Creating the AAA vserver 6
  RADIUS authentication 8
  LDAP authentication 9
  Client certificate authentication 10
  Session policy configuration 11
  Traffic policies and form-based SSO profiles (for Exchange OWA logins) 12
  Two-factor authentication with NetScaler and Exchange 2013 15
  Setting up front-end authentication 16
Optimizing Exchange 2013 with NetScaler 19
  HTTP compression 19
  Integrated caching 22
  Front-end optimization 27
  Content filtering on NetScaler with Responder and Rewrite 29
Conclusion 33
NetScaler is a world-class application delivery controller (ADC) with the proven ability to load balance, accelerate, optimize and secure enterprise applications. Microsoft Exchange 2013 is an industry-leading enterprise email and personal information management solution developed by Microsoft. Out of the box, the product provides enterprises with an easily deployed enterprise email, calendar, task and other enterprise information management solution with a massive and ever-evolving set of features.

**Introduction**

Enterprises today use various authentication schemas to give internal and external users reliable and secure access to their corporate Microsoft Exchange servers. With NetScaler application delivery controllers (ADCs) serving as the preferred platform for enhancing enterprise application performance at many organizations worldwide, it is important to understand how the security requirements of these enterprises can also be served by NetScaler.

This guide focuses on using the authentication and optimization capabilities of NetScaler with Microsoft Exchange 2013 to enable enterprises to use more secure authentication systems while reducing the network load experienced due to Exchange email traffic.
**Configuration Details**

![Citrix NetScaler Architecture Diagram](image)

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange Server</td>
<td>2013 SP1</td>
</tr>
<tr>
<td>NetScaler VPX</td>
<td>10.5 (Enterprise License)</td>
</tr>
</tbody>
</table>

**NetScaler features to be enabled**

The following NetScaler features are necessary for authentication with Exchange 2013. Please ensure they are enabled.

- Content switching
- Load balancing
- Rewrite
- Responder
- SSL offload
- AAA (authentication, authorization and auditing)

**Other considerations**

- Make sure you have installed, at a minimum, one license for NetScaler Enterprise Edition.
- Set the time zone and a NTP (Network Time Protocol) server, and check the date and time on the NetScaler virtual appliance, as Exchange server connections can be very sensitive to time differences.
**Steps for authentication and optimization configuration**

Broadly, the steps to configure an Exchange server with authentication are as follows:

**Set up load balancing virtual servers**

i) Complete initial setup for the Exchange server; create a server object for each Exchange server and a custom monitor for each individual Exchange service, listed here:

1. /owa (Outlook Web Access)
2. /ecp (Exchange Control Panel)
3. /ews (Exchange Web Service)
4. /Microsoft-Server-ActiveSync (ActiveSync Service for mobile mail clients)
5. /oab (Offline Address Book)
6. /rpc (Outlook Anywhere or RPC over HTTPS)
7. /Autodiscover (Autodiscover Service)

ii) Create a service group object for each Exchange service and bind the server objects and appropriate monitors to it.

iii) Now, create a load balancing virtual server (load balancing vserver) for each Exchange service and bind the appropriate service group and certificate to it. For this deployment, we have used a self-signed certificate; however you may use any valid server certificate.

   1. When defining the load balancing vservers, select Not Directly Addressable, as these vservers will later be bound to a content switching virtual server. (content switching vserver)
   2. Set an appropriate load balancing method (such as LEASTCONNECTION) and a persistence method such as SSLSESSION.

iv) Now, configure the content switching vserver and relevant policies for switching to the appropriate backend load balancing vserver based on user request.

**Set up authentication and AAA-TM policies**

i) Create an AAA vserver with an externally accessible IP address (over HTTPS) and bind the required certificate to it. This vserver is the authentication server that will handle the two-factor authentication requirement.

ii) Define and bind relevant authentication policies.

iii) Define the session policy for configuring login to Exchange, and bind it to the AAA vserver.

iv) Define traffic policies and a form-based SSO policy, then bind the traffic policies to the OWA (Outlook Web Access) load balancing vserver

v) Bind the authentication policy to the content switching vserver. Multiple configurations, defined later in the guide, can be made here.

**Set up optimization policies**

i) Create the FEO, compression and caching policies and attach them to the content switching vserver.

This guide covers sections (b) and (c) above. Detailed guidelines for section (a) can be found in the basic deployment guide for Exchange 2013 with NetScaler at https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/microsoft-exchange-2013-citrix-netscaler-deployment-guide.pdf
Enabling authentication to Exchange 2013 with NetScaler

Creating the AAA vserver
The AAA vserver on NetScaler handles authentication requirements. This versatile feature allows a combination of multiple authentication factors in a primary/secondary prioritized setup and policy-driven authentication mechanisms to be used from a single interface. For this deployment, the Exchange_2013_401_Auth_vserver AAA vserver was created. To create a new AAA vserver, navigate to Security>AAA Application Traffic>Virtual Servers and click the Add button.

Upon clicking the Add button, the following screen is presented, where settings for the AAA vserver (IP address, authentication domain, etc.) can be entered. Context-sensitive help is provided (a small question mark shows up next to each text field) if you need assistance with providing details.

Authentication Virtual Server

Once created, the AAA vserver shows up on the Authentication Virtual Servers listing screen (where the Add button was clicked earlier) as shown below. As noted above, the AAA vserver we will be using is Exchange_2013_401_Auth_vserver.
Upon selecting the AAA vserver and clicking Edit, the configuration screen for the virtual server is presented, as shown below. It allows exhaustive changes to the vserver configuration.

**Authentication Virtual Server**

### Basic Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange_2013_401_Auth_Vserver</td>
<td>10.105.157.94</td>
<td>443</td>
</tr>
</tbody>
</table>

### Certificates

- **1 Server Certificate**
- **No CA Certificate**

### Advanced Authentication Policies

- **No Authentication Policy**

### Basic Authentication Policies

This screen can be used for defining backend (NetScaler to Exchange servers) authentication settings, which is described later in this guide.
RADIUS authentication

To add a new RADIUS authentication policy, in the navigation menu on the left, click through to AAA Application Traffic>Policies>Authentication>Basic Policies>RADIUS. Click Add in the pane on the right to add a new policy.

Before creating a policy, ensure you have defined the settings for your RADIUS server in the Servers tab. If you haven’t, click on the Servers tab and then click Add to create a new RADIUS server definition.

You will see the following window. Enter the appropriate settings for your RADIUS server. (The Details pane is minimized by default; you can expand it when needed, for example, to connect to RSA SecurID, as NetScaler connectivity to SecurID works over RADIUS.)
After creating a new server, you can add it to your RADIUS authentication policy; go back to the Policies tab and click Add. On the prompt that follows, add the necessary details with the name of the server you have just created.

The Expression section shown below lets you add an expression that determines whether or not the user should be authenticated with the server, using parameters such as the certificate issuer or source IP address.

**LDAP authentication**

To add a new LDAP authentication policy, in the navigation menu on the left of the screen below, click through to AAA Application Traffic>Policies>Authentication>Basic Policies>LDAP. Here, click Add in the pane on the right to add a new policy.

Again, make sure the server is defined first. To do so, go to the Servers tab as described earlier, then click Add.

This screen will allow you to configure your LDAP server. It also provides other capabilities, such as extracting a field other than the user’s SAN (for example, the UPN). These capabilities can be defined in the Other Settings section under Server Logon Name Attribute (for server login) and SSO Name Attribute (for an alternate username).

After adding the server, you can go back to policies and add the LDAP policy, similar to the RADIUS policy. The Expression section also holds similar functionality.
Client certificate authentication

To enable client certificate authentication with Exchange on NetScaler, you may choose one of two options. If you would like to enable client certificate authentication without needing to set up an authentication (AAA) virtual server, you can enable Client Authentication in the SSL Parameters section of the Exchange CS vserver basic settings window. Here, you also have the option of setting client authentication as Optional or Mandatory; if you choose the latter, NetScaler will terminate the request if the user presents an invalid certificate or does not submit one. If you select Optional, the user will be allowed to proceed further without authentication. Therefore, for enabling certificate-based authentication, the recommended setting here is Mandatory. The validity of the certificate is verified by matching the root CA for the certificate with the one registered on the Exchange content switching vserver.

Alternatively, you can configure a CERT policy and link it to an AAA vserver, then add it to your content switching vserver definitions (as with the LDAP and RADIUS policies).
Session Policy Configuration

After completing configuration of the AAA vserver and relevant authentication policies, you should next create a session policy that allows NetScaler to initiate and maintain an authenticated session with the Exchange server.

To begin creating the session policy, navigate to Security>AAA Application Traffic>Policies>Session. Alternatively, you can do the same by going to the basic settings screen for your AAA vserver and adding a policy.

Here, after clicking on the Add button, you can configure a new session policy.

Alternatively, you can use ns_true for the expression. To edit or create a new request profile, click on either the pencil icon (for editing an existing policy) or the plus icon (for creating a new one). This action launches the session profile definition screen, shown below.
Here, fill the text box titled Single Sign-on Domain with the SSO domain for your environment. In some instances, the HTTPOnly cookie setting may cause synchronization issues with some Android native email clients. If this is an issue in your environment, change the setting (enable the check mark next to the setting to edit it; when unchecked, the setting is inherited from the global settings).

Traffic policies and form-based SSO profiles (for Exchange OWA logins)

Now, to enable OWA functionality, you should configure traffic policies and form-based SSO profiles. The Form SSO profile definition can be done at Security>AAA-Application Traffic>Policies>Traffic as shown below.

The profile configuration required is shown below.
The traffic policy definition can be done at Security>AAA-Application Traffic>Policies>Traffic as shown below.

Here, we create two policies (Exchange_2013_owa_sso_policy and Exchange_2013_owa_logout_policy), one to enable SSO and the other for clean logout. The configurations for the two policies are shown below.

**Exchange_2013_owa_sso_policy**

A. Configuring the traffic policy

The expression added here is HTTP.REQ.URL.CONTAINS("/owa/auth/logon.asp")

B. Configuring the traffic profile

Here, set AppTimeout to 1 minute, Single Sign-on to ON and for the Form SSO profile, use the profile created earlier. Leave the other settings as is.
Exchange_2013_owa_logout_policy

A. Configuring the traffic policy

The expression added here is HTTP.REQ.URL.CONTAINS('logoff.owa')
B. Configuring the traffic profile

Here, select the check mark next to Initiate Logout. These configured traffic policies should be bound to the OWA load balancing vserver v_cas_owa.

Two-factor authentication with NetScaler and Exchange 2013

When two-factor authentication is required, you can add a second primary authentication policy to the content switching vserver. If the first factor configured is CERT authentication, the policy will then pass the credentials pulled from the certificate to the form. On the form, the username will be locked and a password for the username corresponding to the one present in the certificate provided will be requested.

For the purposes of illustrating this capability and describing the solution, we will be using the following test configuration:

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange Server version</td>
<td>2013</td>
</tr>
<tr>
<td>NetScaler version</td>
<td>10.5</td>
</tr>
<tr>
<td>Primary authentication factor</td>
<td>LDAP/Active Directory</td>
</tr>
<tr>
<td>Secondary authentication factor</td>
<td>RADIUS</td>
</tr>
</tbody>
</table>

The reason for the selection of RADIUS as the secondary factor is that the RADIUS authentication system connects quite easily with popular enterprise second-factor authentication systems such as RSA SecurID, SafeWord and Gemalto Protiva.

To enable two-factor authentication, complete configuration of the LDAP and RADIUS servers as described earlier in the guide. Then, navigate to the Basic Settings page for the AAA vserver configured earlier (Security>AAA – Application Traffic>Virtual Servers) and then, click on the plus sign (+) next to Basic Authentication Policies.
Here, you will see the following screen:

In the Choose Type dropdown, select Secondary. After clicking Continue, you are taken to the following screen where you can select or add a new authentication policy.

After selecting/adding a new policy (the process for adding a new RADIUS policy is the same as described earlier), click on Bind. This completes the configuration for two-factor authentication.

**Setting up front-end authentication**

At the content switching vserver

To enable authentication on NetScaler for the front end (client-to-NetScaler authentication), click on the Authentication subsection on the cs_cas_443 content switching vserver Basic Settings page. Note that this action has to be performed on the settings screen for the content switching vserver, not the AAA vserver.
To get to the Authentication section, scroll down on the Basic Settings page or, if you don’t see the section, look on the right-hand side of the page for the Authentication link and click it.

In this section, you have two options: enable 401-based authentication, in which case users will be presented with a standard authentication popup prompt; or enable Form-based authentication, in which case NetScaler will present an authentication form to the user. In the second case, you will also have to provide the authentication FQDN (Fully Qualified Domain Name), which is the domain name for the AAA vserver. This is the host domain for the form that will be presented to the user.

Note that if form-based authentication is enabled at the content switching vserver, only OWA and ECP (Exchange Control Panel) will be accessible. The other services cannot work with form-based authentication. If all services are required to be functional with this setup, use 401-based basic authentication as the setup option.

At the individual load balancing vservers
In a similar fashion, the authentication can be enabled at the load balancing vserver level as well. In this case, the OWA and ECP load balancing vservers should be configured with form-based authentication, while all other load balancing vservers are configured with 401-based authentication, all linked to the same AAA vserver (Exchange_2013_401_Auth_vserver).
To have this profile functioning with Outlook clients, you should enable Outlook Anywhere. (located in File>Account Settings>More Settings>Connection>Connect to Microsoft Exchange using HTTP). Here, to use the settings above (LDAP server), you must configure the mail server address as the FQDN for the CS vserver, and the authentication type as Basic. This should be configured at the Exchange server as well.

To be able to use NTLM authentication, use a Negotiate Action policy with the AAA vserver instead of the LDAP policy bound currently.

Note: Please ensure that Edgesight Monitoring/HTML Injection is disabled in the feature list (Located at System>Advanced Settings) on the NetScaler device for Exchange connectivity to function properly with NetScaler.
Other settings

The authentication profile defines settings such as the authentication domain and level. The authentication level is important, as it defines the vserver levels that authentication with this profile will allow the user to access. A user authenticated with an authentication vserver at a certain level cannot access a vserver running at a higher level. The level setting for load balancing or content switching vservers is an optional parameter when access restriction is required.

If dual-factor authentication is set up as described earlier, when the AAA vserver is bound to the Exchange vserver(s), the login screen shown will ask for two passwords – one each for LDAP (first authentication factor) and RADIUS (second authentication factor). Note that the username for both factors should be the same.

![Login Prompt](image)

The screen above shows the login prompt users will see if dual factor authentication is enabled.

Optimizing Exchange 2013 with NetScaler

NetScaler offers a suite of optimization features in these categories:
- HTTP compression
- Integrated caching
- Front-end optimization (FEO)
- Responder and Rewrite

To configure HTTP compression, integrated caching and FEO, expand the Optimization tab in the NetScaler GUI's left-hand navigation panel.

HTTP compression

The NetScaler optimization suite is, like other NetScaler features, driven by a policy-action architecture.
To enable HTTP compression for the Exchange 2013 content switching vserver, you should:
- Define the HTTP Compression Policies and Actions relevant to the service
- Bind the service to the Exchange 2013 CS vserver.

To define the Compression Policy and Action, click on the Policies option under HTTP Compression, shown above. This gives you the following screen -

To add a new compression policy, click the Add button. This will give you the following screen.

Here, you can define a name for the policy and an expression that defines when this policy is triggered (for example, when a particular URL is encountered.) To make the policy apply to all content, use true in the Expression window. For assistance here, click on the Frequently Used Expressions dropdown and the Response Action that should be taken. Here, the actions available are COMPRESS (GZIP or DEFLATE compression, with GZIP given priority), GZIP (GZIP standard compression), DEFLATE (DEFLATE compression) and NOCOMPRESS.

Note that you should use true and not ns_true for the expression, as ns_true will make the compression policy a classic policy, which will not allow proper binding to the content switching vserver. If you have difficulties with binding the policy, please verify this setting.

You can either add a new action or reconfigure the existing ones. You can add using the plus button, or edit/configure using the pencil-shaped button. Either option gives you a screen similar to the one shown below.
To offload all compression to NetScaler (and thus save CPU cycles on the server) you can disable server-side compression. By default, NetScaler will disable server-side compression, but in case it is enabled you can disable it by navigating to Optimization>HTTP Compression and clicking Change compression settings.

Here, clear the check box for Allow Server-side compression if it is enabled.
Compression should be enabled on the service groups as well. To do this using the GUI, navigate to Traffic Management>Load Balancing>Service Groups. Here, you will see the individual service groups listed for each Exchange service (created using the base deployment guide listed earlier).

Here, select each service group and click the edit button. This takes you to the Basic Settings screen for the service group, shown below.

Here, click on the edit (pencil icon) next to the Settings section and then enable HTTP compression (already enabled in the screenshot above).

Vary Header Insertion is an option that is relevant for caching; the value of the vary header allows different cache results to be returned for similar requests. For now, we are not changing the options presented here. You can add a new action that uses a compression type of your choice.

Integrated caching
After you enable the integrated cache feature and perform basic setup (for example, determining the amount of NetScaler appliance memory the cache is permitted to use), the integrated cache
uses built-in policies to store and serve specific types of static content, including simple web pages and image files. You can also configure the integrated cache to store and serve dynamic content that is usually marked as non-cacheable by web and application servers (for example, database records and stock quotes).

To configure caching, you can use the integrated wizard that makes configuration very straightforward. To initiate the wizard, navigate to Optimization>Integrated Caching as shown below.

You can initiate the Caching Wizard under Getting Started.

The first step requires you to specify the content type. This can be either static (examples given) or dynamic. Helpful hints are provided as shown above to help determine which type of content is relevant for you.
The next step involves defining which content should be cached. The Frequently Used Expressions dropdown helps you define the correct expression; however, if you want the caching policy to run for all content, you can use ns_true as the expression, as shown below.

The next screen allows you to define when content expires. This can be custom (a defined interval) or heuristic (NetScaler makes the determination based on a guideline percentage of the time since the object was last modified, with a pre-set deadline that is used in case the heuristic measurement cannot be made).
The next step involves definition of the caching space to be used on NetScaler and the minimum size of objects to be cached. Here, you should increase the setting for Do not cache if size exceeds (default set to 80KB) as relevant to your environment. If your deployment uses a large number of image/audio/video files or large documents, this size should be increased to a higher number so that caching performance is improved. Note, however, that the cache has a limit, and caching large objects will result in reaching this limit much faster.

Finally, the cache policy should be bound to the Exchange content switching vserver cs_cas_443. These definitions can be made under Cache Policies as shown in the next screenshot.
With respect to dynamic caching, NetScaler allows configuration of selectors and content groups.

**Selectors and content groups**

A content group is a container for cached objects that can be served in a response. When you first enable the integrated cache, cacheable objects are stored in a content group named Default. You can create new content groups that have unique properties. For example, you can define separate content groups for image data, bug reports and stock quotes, and you can configure the stock quote content group to be refreshed more often than the other groups.

You can configure expiration of an entire content group or selected entries in a content group.

The data in a content group can be static or dynamic:

- **Static content groups.** Find an exact match between the URL stem and host name on the request and the URL stem and host name of the response.
- **Dynamic content groups.** Look for objects that contain particular parameter-value pairs, arbitrary strings or string patterns. Dynamic content groups are useful when caching data that is updated frequently (for example, a bug report or a stock quote).

When you add a selector to one or more content groups, you specify whether the selector is to be used for identifying cache hits or identifying cached objects to be invalidated (expired). Selectors are optional. Alternatively, you can configure content groups to use hit parameters and invalidation parameters. However, Citrix recommends that you configure selectors.

Both of these features can be accessed using the navigation menu in the NetScaler GUI.
For more detailed information on integrated caching and the features described above, please refer to http://support.citrix.com/proddocs/topic/ns-optimization-10-5-map/ns-IC-gen-wrapper-10-con.html

Front-end optimization

The FEO feature set makes NetScaler an extremely capable optimization device by implementing enhanced optimization routines for specific front-end entities such as images, JavaScript, etc. These improve optimization performance by enabling compression and caching.

FEO capabilities can be activated by navigating to Optimization>Front End Optimization. As with all NetScaler features, FEO capabilities are implemented using a policy-action mechanism.

To add a new policy, click on Policies, then click Add in the section displayed to the right of the navigation menu.

This will give you the following screen for definition of a new FEO policy.
The expression here works much on the same lines as expressed for the earlier features; the Frequently Used Expressions dropdown can be used for assistance. Certain predefined actions can be assigned here, all of which have different configurations for the same settings; you can also either edit or create a custom action using the plus or pencil buttons next to the Action name. Upon clicking either of these buttons, the following screen (or a similar one) is shown.

This screen presents all the various FEO options available; NetScaler can help to optimize web traffic with JavaScript, image, cascading style sheets (CSS), HTML and miscellaneous optimization. This last section also allows for domain sharding, which splits resources across subdomains to improve optimization and page load times. (The profile shown above is for the Basic default setting, however the recommended setting here is Moderate.)
For FEO implementation, the profile to be used will vary significantly for each individual deployment, depending upon the mix of data that is being sent over email in your organization. Therefore, it is recommended that you try out different built-in profiles/create custom profiles to see which of the available optimization options provides the best performance. Begin with the BASIC profile, evaluate performance and then move on to MODERATE/AGGRESSIVE to find the profile that gives you best performance improvements. Alternatively, you may configure your own custom FEO action.

In our test deployment, primarily running text and basic HTML email, we have used the following settings.

**Optimization Policy Name:** Exchange_Optimization_Test  
**Default Optimization Action:** MODERATE (Preconfigured)  
**Expression:** HTTP.REQ.HEADER("Accept").CONTAINS("html")

**Alternate Configuration (Custom Policy)**  
**Optimization Policy Name:** Exchange_Optimization_TestCustom  
**Optimization Action:** Exchange_Optimization_custom  
**Expression:** HTTP.REQ.HEADER("Accept").CONTAINS("html")

**Exchange_Optimization_TestCustom Configuration:**  
Enabled Settings: JavaScript/Make Inline, JavaScript/Minify, Image/Optimize, Image/Convert GIF to PNG, Image/Make Inline, Image/Optimize, Image/Convert to WEBP, Image/Convert to JXR format, CSS/Make Inline, CSS/Move to Head Tag, CSS/Minify, CSS/Combine, CSS/Convert Imports to Links, HTML/Remove Comments from HTML

You may use the default optimization action (Moderate) if you do not want to configure your own custom optimization action. The alternate configuration provides the recommended settings in case you do choose to create it.

In the lab environment, these settings provide up to a 60 percent reduction in page load times and up to a 36 percent reduction in the amount of data transferred. This may vary significantly for your deployment based on the profile of data being transferred; therefore, it is recommended that you test multiple settings.

**Content filtering on NetScaler with Responder and Rewrite**

Note: the use of Responder and Rewrite is optional and allows administrators to configure several usage improvements for the deployment, such as making it easier to access URLs.

The URL filtering capability with NetScaler can be found under AppExpert>Responder on the left-hand navigation menu in the NetScaler GUI.

With the Responder feature, responses can be based on who sends the request, where it is sent from and other criteria with security and system management implications. The feature is simple and quick to use. By avoiding the invocation of more-complex features, it reduces CPU cycles and time spent in handling requests that do not require complex processing.
For example, for handling sensitive data such as financial information, if you want to ensure that the client uses a secure connection to browse a site, you can redirect the request to a secure connection by using https:// instead of http://.

To use the Responder feature, first enable it on NetScaler from System>Settings>Configure Advanced Features. Then, navigate to AppExpert>Responder and click Policies to add a new policy. After clicking Add, the next screen allows you to configure the policy as well as the action bound to it.

The policy determines the requests (traffic) for which an action has to be taken. This determination is made using the expression provided by the administrator. Multiple Frequently Used Expressions are available for use, as shown below.
To configure the action bound to this policy, click the pencil icon next to the action name indicated. Note that you will not be able to edit the default policies, only custom ones that you have created. To add a new policy, click the plus icon.

The action can be to generate a custom response or redirect a request to a different, custom web page. The policy must be bound to a bind point put it into effect. A bind point refers to an entity where NetScaler examines the traffic to see if it matches a policy. For example, a bind point can be a load balancing vserver.

You can specify a default action for requests that do not match any policy, and you can bypass the safety check for actions that would otherwise generate error messages.

The Rewrite feature helps in rewriting some information in the requests or responses handled by NetScaler. For example, the following Rewrite action adds the “/owa” string to any user URL when it contains the organization’s email domain.
The policy that enables this action to be performed when the URL contains the organization’s mail domain is defined as follows (again, these are configurable in the AppExpert>Rewrite section under Policies and Actions).

Here, replace_host_name is the policy name, and replace_host_name is the action we defined earlier.

There are differences between the Rewrite and Responder features. Responder cannot be used for response- or server-based expressions. Responder can be used only for the following scenarios, depending upon client parameters:

- Redirecting an HTTP request to new websites or web pages
- Responding with a custom response
- Dropping or resetting a connection at the request level
For a Rewrite policy, the NetScaler device examines the request from the client or response from the server, takes action according to the applicable policies and forwards the traffic to the client or the server.

In general, it is recommended to use Responder if you want NetScaler to reset or drop a connection based on a client- or request-based parameter. Use Responder to redirect traffic or respond with custom messages. Use Rewrite for manipulating data on HTTP requests and responses.

Conclusion
NetScaler enables a secure and optimized experience with Microsoft Exchange 2013 through a superior set of optimization and authentication capabilities. NetScaler not only helps deliver a load balanced and responsive Exchange system, but also provides several additional capabilities such as two-factor authentication and front-end optimization.