NetScaler deployment guide

Replacing Microsoft Forefront TMG with Citrix NetScaler for enterprise authentication
Authors

The following authors contributed to the creation of this deliverable.

Citrix

Abhishek RVRK Sharma
#33, Ulsoor Road
Bangalore, Karnataka 560042
India
Phone: +91 80 39541000 Extension 78219
Abhishek.sharma@citrix.com

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Change Description</th>
<th>Updated By</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Initial Draft</td>
<td>Abhishek RVRK Sharma</td>
<td>6th May 2015</td>
</tr>
</tbody>
</table>
Table of Contents

Introduction ................................................................................................................. 4
Configuration details ................................................................................................. 5
Solution description ..................................................................................................... 7
  Section 1: Initial preparation ..................................................................................... 7
  Section 2: Frontend authentication .......................................................................... 12
  Section 3: Enabling authentication delegation to the backend enterprise service ..... 16
  Section 3: Setting up individual authentication schemes ........................................ 23
  Section 4: Enabling single sign-on (SSO) .............................................................. 34
  Section 5: SSO with Kerberos Constrained Delegation (KCD) .............................. 37
Conclusion .................................................................................................................. 48
## Introduction

This deployment guide focuses on defining solutions for replacing Microsoft Forefront Threat Management Gateway (TMG) with Citrix® NetScaler® for various enterprise authentication scenarios. NetScaler is a world-class application delivery controller (ADC) with the proven ability to load balance, accelerate, optimize and secure enterprise applications.

Forefront TMG offers some useful authentication features:

- **User authentication**: TMG supports user authentication (both 401 and form based) with LDAP, RADIUS, RADIUS-OTP and RSA SecurID. It also allows for two-factor authentication.
- **Authentication delegation and SSO**: TMG offers authentication delegation so it can authenticate with services on behalf of the user. Delegated SSO with Kerberos Constrained Delegation (KCD) is also possible.

In this guide, we describe replicating TMG functionality for various authentication scenarios with NetScaler, and then highlight the additional possibilities that NetScaler enables.

The following TMG features will be replicated with NetScaler in this guide:

<table>
<thead>
<tr>
<th>Secure Application Publishing</th>
<th>Secure publishing of web and internal servers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SSO (single sign-on)</td>
</tr>
<tr>
<td></td>
<td>Delegation of basic authentication</td>
</tr>
<tr>
<td></td>
<td>SSL bridging</td>
</tr>
<tr>
<td></td>
<td>SSL tunneling</td>
</tr>
</tbody>
</table>
Configuration details

To show Forefront TMG administrators the equivalent steps for configuring NetScaler for enterprise authentication, this guide presents step-by-step details for some sample use case. Figure 1 below depicts the setup of the test deployment.

![Diagram of test setup](image)

**Figure 1. Diagram of test setup**

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Forefront TMG</td>
<td>2010 SP1</td>
</tr>
<tr>
<td>NetScaler VPX™</td>
<td>10.5 (enterprise license)</td>
</tr>
</tbody>
</table>

**NetScaler features to be enabled**

The essential NetScaler features that need to be enabled are load balancing, content switching, SSL offloading and AAA authentication, authorization and auditing (AAA).

The following NetScaler features are used in this deployment. Please ensure these features are enabled in the NetScaler system.

- Content switching
- Load balancing
- SSL offloading
- AAA (Authentication, Authorization and Auditing)
Here is a quick explanation of how these features work.

**Content switching**

The content switching module directs incoming traffic to a matching load balancing virtual server. This logical switching of incoming traffic based on content type allows configuration of specific optimization policies.

**Load balancing**

NetScaler load balancing evenly distributes requests to backend servers. Multiple algorithms (such as LEASTCONNECTION, ROUNDROBIN, etc.) are supported to provide efficient load balancing logic for every application server.

**SSL offloading**

SSL connections are terminated at the NetScaler appliance, thus allowing NetScaler to conduct advanced traffic monitoring. Additionally, SSL offloading can significantly reduce the computational overhead of offloading encrypted user connections on backend servers.

**AAA**

The AAA feature set controls authentication, authorization and auditing policies for NetScaler. These policies include definition and management of various authentication schemas. NetScaler supports a wide range of authentication protocols and a strong, policy-driven application firewall capability.

Several additional features can help improve the enterprise user experience. Rewrite, responder, HTTP compression, DoS protection and integrated caching can be enabled. However, the use case described here can be deployed using the four features described above; this guide will not describe the benefits that can be achieved with these additional features.
Solution description

Section 1: Initial preparation

Part 1: Forefront TMG

TMG can be set up as described in the earlier guide, “Replacing Microsoft Forefront TMG with Citrix NetScaler for website publishing.”

Since this guide describes a deployment using two different servers, we run the website publishing server as described in Guide 1 for the load balanced websites mailmg.ctxns.net and sp.ctxns.net.

All settings will remain the same as in Guide 1, except for changes that will need to be made from Step 11 in Section 3 of the earlier guide. Step 11 from that guide is repeated below for convenience.

Note: If your web listener is already configured (if you previously set up a non-authenticated web listener) you must use an alternate path to change these settings.

Step 11 – Client authentication method definition

On the next screen, you can define how clients are authenticated with TMG. TMG supports LDAP/Active Directory, RADIUS, client certificates or RSA SecurID-based authentication.
NetScaler advantage
NetScaler supports several other alternative authentication mechanisms as well. In addition to Basic/Local, NTLM/AD and RADIUS that are supported by TMG, NetScaler supports CERT (certificate based), TACACS, web and SAML/SAML IDP-based authentication, thus providing significantly improved functionality.

Assuming that a web listener has already been configured with the earlier guide but has no authentication defined, you can change the authentication parameters for the web listener by navigating to Toolbox>Network Objects>Web Listeners.

Part 2: Initial preparation - NetScaler
Configuring the content switching policy
In the last guide (Steps 6 and 7), we configured the content switching virtual server (CS vserver) to switch between different load balancing virtual servers based upon the requested URL.

For this deployment, we will be using the following websites:
mailtmg.ctxns.net – Exchange server
sp.ctxns.net – SharePoint server

The content switching policy defines how a request will be evaluated based on whether the host name in the request contains mailtmg.ctxns.net for the Exchange server or contains sp.ctxns.net for the SharePoint server.

(To reach this prompt, navigate to Traffic Management>Content Switching>Virtual Servers. Then select the appropriate CS vserver and click Edit. On the screen that follows, click Content Switching Policies under CS Policy Binding.)
The content switching action essentially delegates the request to the appropriate load balancing virtual server (which hosts the Exchange and SharePoint portal per the client request).

The figure above is the prompt shown for configuring the content switching action. (To reach this screen, click on the Edit dropdown, then select Edit Action.)

Creating the AAA Virtual Server

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 **TMG_authvserver** 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 on 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.
Once created, the AAA vserver shows up on the Authentication Virtual Servers listing screen (where the Add button was clicked earlier) as shown below. The AAA vserver we will be using is TMG_authvserver.

Upon selecting the AAA vserver and clicking **Edit**, the following screen is displayed. This is the configuration screen for the virtual server. It allows exhaustive changes to the vserver configuration.
This is the screen that can be used for defining backend (NetScaler to backend service) authentication settings as described in Section 2.
Section 2: Frontend authentication

Part 1: Enabling authentication on the front end with TMG

The authentication settings for TMG show up on the Authentication tab in the Properties window for the appropriate listener. In this case, it is the Outlook Web Access (OWA)-https listener, as shown above. To get to this prompt, go to **Firewall Policy>Find the appropriate rule** and right-click on the listener listed as part of the rule. From the menu then presented, choose **Properties**.
Here, you are presented with the following options. Choose the setting that is appropriate for your environment.

For Client Authentication Method –

**HTML Form Authentication**: TMG will present an HTML form to collect credentials from the client.

**HTTP Authentication**: TMG will present a standard 401-based authentication prompt (a popup message requesting a username and password).

**SSL Client Certificate Authentication**: TMG will request the user to present a valid client certificate, which will then be verified by TMG.

**No Authentication**: TMG will not request any authentication and will pass traffic through, allowing the backend service to handle authentication.

**NOTE**: These settings work in tandem with the Authentication Delegation settings presented in the Properties window for the individual rules in the Firewall Policy window.

For Authentication validation method, the options available are Windows and LDAP (both authenticating with Active Directory), RADIUS and RADIUS-OTP, and RSA SecurID.

When the **Collect additional delegation credentials** option in the Client Authentication section is enabled, the only two options available are RSA SecurID and RADIUS-OTP.

The **Configure Validation Servers** option is available for LDAP, RADIUS and RADIUS-OTP. For RSA SecurID and Windows Authentication, no server settings are required as they are picked up automatically by TMG. When this option is clicked, the following window pops up, which allows you to configure LDAP and RADIUS servers.
Define the sets of LDAP servers Forefront TMG will query to validate user credentials:

<table>
<thead>
<tr>
<th>LDAP Server Set</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxns</td>
<td>dc.ctxns.net</td>
</tr>
</tbody>
</table>

Define the login expressions Forefront TMG will use to match the user login strings:

<table>
<thead>
<tr>
<th>Login Expression</th>
<th>LDAP Server Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxns*</td>
<td>ctxns</td>
</tr>
</tbody>
</table>

Forefront TMG will query the servers in the matching LDAP server set to validate user credentials.

Help about [LDAP authentication settings](#)
Part 2: Enabling authentication on the front end with NetScaler

For NetScaler, frontend authentication is set at the LB/CS (traffic management) vserver level.

To enable authentication on the NetScaler for the front end (Client to NetScaler authentication), click on the Authentication subsection on the LB vserver Basic Settings page. Note that this action has to be performed on the settings screen for the LB 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 – to enable either 401-based authentication, in which case users will be presented with a standard authentication popup prompt, or 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.

<table>
<thead>
<tr>
<th>Basic Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>Traffic Domain</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Services and Service Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Load Balancing Virtual Server Service Binding</td>
</tr>
<tr>
<td>No Load Balancing Virtual Server ServiceGroup Binding</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Form Based Authentication</td>
</tr>
<tr>
<td>Authentication FQDN</td>
</tr>
<tr>
<td>Authentication Virtual Server</td>
</tr>
<tr>
<td>Authentication Profile</td>
</tr>
</tbody>
</table>

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 LB or CS vservers is an optional parameter when access restriction is required.
Section 3: Enabling authentication delegation to the backend enterprise service

Part 1: Backend authentication with TMG authentication delegation

The rules for authentication with the backend service are set in the Properties>Authentication Delegation section in the properties window for the relevant firewall rule. These rules are listed in the Firewall Policy subsection.

Note the options available in the screenshot above: they depend upon the settings in the listener that were set in Part 1. When selecting Kerberos constrained delegation, you will be required to present the subject principal name (SPN) to be used by TMG (this is the Kerberos-enabled service that the firewall rule applies to). We will discuss more about SSO methods in a separate section.

Examples: Basic and NTLM delegation

Two of the more popular delegation schemes are Basic (401-based) and NTLM (Active Directory) authentication delegation. Either defines how TMG will interact with the backend service. The Description section under the dropdown menu for selection of delegation methods provides details on the chosen method.
Part 2: Backend authentication with NetScaler

Note: For NetScaler, the backend authentication is set at the AAA vserver level.

Authentication Virtual Server

<table>
<thead>
<tr>
<th>Basic Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>TMG_authvserver</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Server Certificate</td>
</tr>
<tr>
<td>No CA Certificate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advanced Authentication Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Authentication Policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Basic Authentication Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Authentication</td>
</tr>
<tr>
<td>1 LDAP Policy</td>
</tr>
</tbody>
</table>

401 Based Virtual Servers

2 Load Balancing Virtual Servers

As shown above, we are using an LDAP policy for authenticating users to this AAA vserver as an illustration. You can choose another authentication factor such as Local, LDAP, RADIUS, CERT (certificate based), Negotiate (for
Negotiate method authentication), etc. NetScaler supports both single- and two-factor authentication; a second factor can be declared as a **Secondary Authentication Policy** in the panel above.

**Note:** The AAA vserver can only be defined over SSL; therefore, you will be required to add a server certificate to the AAA vserver. This can be self-signed or a purchased certificate, depending upon the security level required. A purchased certificate allows verification with a certified, recognized certificate authority. A self-signed certificate may be adequate and easier to obtain, but will not be verifiable and most browsers will present errors with such a certificate.

To add the LDAP policy as indicated in the AAA vserver configuration snapshot above, the policy needs to be bound to the server by clicking on the + icon next to the **Basic Authentication Policies** section header.

After clicking on this button, the following screen is shown:

Here, you can select the type of authentication policy you would like to add. The **Type** parameter defines whether the authentication policy defined is primary or secondary. This is useful during dual-factor authentication scenarios. As we are only defining a single authentication policy here, we will keep the **Type** parameter set as **Primary**.

Upon clicking **Continue**, you will be presented with the following screen:

Here, you can either add a new LDAP policy or select a pre-existing policy.
When you click on **Policy binding>Select Policy>Click to Select**, the following screen is displayed:

![LDAP Policies](image_url)

This screen will present a list of all LDAP policies defined on the NetScaler box. You can choose the appropriate policy and then click **OK**. Alternatively, you can choose to add a new LDAP policy here by clicking **Add**. This leads to the add new LDAP policy screen, shown below. The screen prompt is similar to other authentication mechanisms, which provide for adding settings that are appropriate for those schemes.

![Create Authentication LDAP Policy](image_url)

This LDAP policy needs to be bound to an LDAP server; similar to the policy addition, here a server may be chosen from a dropdown menu or a new one may be added. The new server prompt will request the settings that are necessary for the LDAP server, as shown below. The right-hand and left-hand fields must be filled in completely to facilitate LDAP authentication. Context-sensitive help (indicated by a question mark icon next to the field) is available to assist with identifying the values needed.
Left-hand side of the LDAP server configuration screen
Right-hand side of the LDAP server configuration screen
Upon creation of the LDAP policy, the screen below will allow you to bind the policy to the authentication vserver with the newly created policy already selected.

This AAA vserver is bound to the load balancing virtual servers (LB vservers) defined for the SharePoint and Outlook Web Access servers (as described in the first guide). While the AAA vserver can be bound to the CS vserver as well, because each of these services presents individual authentication mechanisms, we will implement authentication at the LB vserver level.

When you look at the basic settings screen for the AAA vserver, it will show the LB or CS vservers in the **401-based Virtual Servers** or **Form-based Virtual Servers** section, according to the type of frontend authentication chosen by you in Step 1.

When you click on one of the options in these sections, the following screen is presented. This is a screenshot of the 401-based LB vservers. The screen for the form-based vservers is similar; however, it includes information about the authentication domain.

**NOTE:** Make sure the FQDNs (fully qualified domain names) for all the vservers and services in use are added into the DNS records located at **Traffic Management>DNS>Records>Address Records**.
At this point, we have configured the AAA vserver **TMG_authvserver**.

This AAA vserver is bound to the LB vservers defined for SharePoint and OWA mail servers. Alternatively, you can use a CS vserver for enabling authentication, and use content switching policies to switch between SharePoint and OWA if both of them use the same authentication mechanism.

## Section 3: Setting up individual authentication schemes

### Part 1: Implementing authentication on Forefront TMG

**RADIUS authentication**

In the *Client Authentication Method* page shown below, set the authentication method for the listener to **HTTP Authentication>Basic**. This will enable the **RADIUS** option in the *Authentication Validation Method* Section.
After selecting RADIUS as the authentication validation method, click **Configure Validation Servers** and add the configuration settings for your RADIUS server.
Whether you choose to **Edit** or **Add** a new server, you will be asked to provide the details shown below:

![Edit RADIUS Server](image)

**LDAP authentication**

On the **Listener Settings>Authentication** tab (as for RADIUS authentication), select **HTTP Authentication** and select **Basic** in the **Client Authentication Method** section. For the **Validation Method**, select **LDAP (Active Directory)**. Now click on **Configure Validation Servers**.

First, click **Add** next to the **LDAP Server Set** section. Here, you can add your LDAP server details. TMG can query multiple LDAP servers to verify authentication; enter the list in order of priority. You will also be required to enter the Active Directory domain name and, optionally, provide a username and password for verification of users.
Authentication Servers

RADIUS Servers
LDAP Servers

Define the sets of LDAP servers Forefront TMG will query to validate user credentials:

<table>
<thead>
<tr>
<th>LDAP Server Set</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxns</td>
<td>dc.ctxns.net</td>
</tr>
</tbody>
</table>

Add... Edit... Remove

Define the login expressions Forefront TMG will use to match the user login strings:

<table>
<thead>
<tr>
<th>Login Expression</th>
<th>LDAP Server Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctxns^1</td>
<td>ctxns</td>
</tr>
</tbody>
</table>

New... Remove

↑  ↓

Forefront TMG will query the servers in the matching LDAP server set to validate user credentials.

Help about LDAP authentication settings

OK Cancel Apply
After this, you will be required to define a new LDAP server mapping by clicking **Add** next to the Define Login expression section in the first dialog box in this section. This defines the login expression for users as well as the linked LDAP server set.

**Client certificate authentication**

TMG can also use client certificates to authenticate users. To enable client certificate authentication, go to the **Authentication** panel in the OWAPP Properties section for your listener and choose **SSL Client Certificate authentication**.
Note that the only authentication method enabled here is Windows (Active Directory). TMG will verify the certificate provided with the client certificate stored in the Active Directory and confirm access. You can provide a fallback authentication method for users in case certificate authentication fails.

**Part 2: Implementing authentication with NetScaler**

**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.

Here, 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 the connectivity to SecurID for NetScaler works over RADIUS.)
After adding a new server, you can add the same 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 here 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.
To add a new LDAP authentication policy, in the navigation menu on the left, 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). This is defined under 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.
The screen prompt for LDAP authentication servers (left and right halves of the screen)

**Client certificate authentication**

To enable client certificate authentication with 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 your LB or 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 set to 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 NetScaler LB or CS vserver.
Alternatively, you can configure a CERT policy and link it to an AAA vserver, then add it to your LB or CS vserver definitions (as with the LDAP and RADIUS policies).

The prompt for creating a new CERT authentication policy has the same options as the LDAP and RADIUS policies. As with the earlier schemes, you should define a CERT server to enable authentication. The server settings allow you to define the fields that contain user details such as username, and group name that are relevant for authentication. These fields can then be extracted by NetScaler and submitted to an authentication form (when two-factor authentication is enabled).
When two-factor authentication is enabled, you can add a second primary authentication policy to the LB or CS vserver in addition to the cert policy. 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.

**NetScaler advantage**

TMG will accept any certificate from any certificate provider that is linked to the user in Active Directory. TMG performs no independent verification on the certificate; this can be a security risk when an attacker has gained access to Active Directory and managed to insert a certificate. NetScaler will only accept a certificate that it can independently verify; however, NetScaler will not match the same with the bound certificate in Active Directory.

---

**Section 4: Enabling single sign-on (SSO)**

**Part 1: SSO with Forefront TMG**

You can enable SSO for multiple websites in the **Listener Properties** panel under the **SSO** tab. Click the check box for **Enable Single Sign On**, then specify the domains that will use the SSO mechanism. This SSO mechanism will use the authentication parameters specified under the **Authentication** tab.
Part 2: SSO with NetScaler

To enable SSO to multiple applications with NetScaler, create a session policy, defined here as TMG_SP_SSO. This session policy defines the SSO parameters and needs to be bound to an AAA vserver.

This policy definition process will also allow you to define which authentication parameter to use (primary or secondary) for enabling SSO. You can create and configure this session profile and session policy by navigating to AAA Application Traffic>Policies>Session.
When you click Add in the Session Policies tab, the panel shown above will pop up. Enter an appropriate name for the policy, then add or create a new request profile. You can either edit an existing profile using the pencil-shaped icon or add a new one. In either case, the same screen is presented. This is shown below:

When you choose to add a profile, the name will be blank. This profile inherits a set of global parameters that you can override individually using the Override Global option next to each parameter. To enable SSO, set the Single Sign-on to Web Applications drop down to ON.
Section 5: SSO with Kerberos Constrained Delegation (KCD)

KCD enables your users to access multiple internal services without needing to log in multiple times with client certificates or enterprise username and password. KCD offers both security as well as flexibility with respect to user authentication and is supported by both TMG and NetScaler. We will now describe how to achieve KCD with both TMG and NetScaler.

Part 1: KCD with TMG

To enable KCD on TMG, go to the authentication delegation settings in the TMG rule properties window and select Kerberos constrained delegation.

Note: To view a list of delegation options available with different authentication methods, go to https://technet.microsoft.com/en-us/library/cc995215.aspx

Here, you will have to make sure the SPN that you have provided in the window above is added to Active Directory. You have the option to test the rule using the Test Rule button.

Your Active Directory should be configured to trust the computers used.

Part 2: KCD with NetScaler

There are two processes needed for the configuration of KCD on NetScaler – one on Active Directory and the second on the NetScaler appliance itself.

The steps on the Active Directory Server are as follows –
Create a KCD user account

To enable KCD on NetScaler, you need to create a user account on Active Directory for the NetScaler device to use.

This account must have the rights to do protocol transition and delegation. This account also needs rights to request a Kerberos ticket on behalf of a user logging into the NetScaler appliance.

Start by creating a new user in Active Directory. In this example, create kcdtest as the account to provide constrained delegation access to the web server.

Enable the Delegation tab for the created user

The Delegation tab is not enabled by default for a user account, so you may need to enable it. This involves the use of the SETSPN command-line tool. A standard Windows 2003 installation does not include this tool. However, this tool is available in Windows 2008 Server.

Check Active Directory user properties to see if the delegation tab is available; if not, install Windows Server 2003 support tools from the product CD or from the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=100114).

For more information about how to install Windows support tools from the product CD, see Install Windows Support Tools (http://go.microsoft.com/fwlink/?LinkId=62270). If these are installed on Windows 2003 Server, they can be found in the C:\Program Files\Support Tools folder. To get the latest version of the SETSPN tool visit http://support.microsoft.com/kb/970536.

Use the following command to run the SETSPN tool:

```
setspn -A host/kcdvserver.example.com example\kcdtest
```

Note: In the command above, example is the placeholder for the user domain (CTXNS in our example) and kcdtest is the user account (the same is used in our example). In this command, the kcdtest user has the subject principal name SPN: host/kcdvserver.example.com, and kcdvserver.example.com is the fully qualified domain name (FQDN) of the LB or CS vserver (test.ctxns.net in our example).

So, for our example, the command would look like:

```
setspn -A host/test.ctxns.net CTXNS\kcdtest
```
This command enables the **Delegation** tab in the **[User Account] Properties** window for the user account *kcdtest*.

If the Delegation Tab does not appear, Active Directory is probably running in mixed or native mode and you should raise it to the Windows 2003 functional level.

**NOTE** that the following steps change Active Directory behavior and alter support for older Windows clients. If you are uncertain, you should not raise the domain functional level without verifying any impact to the environment, because this step cannot be reversed.

After Active Directory is at Windows 2003 functional level you can continue with the configuration.

The **Delegation** tab should now be visible. Be sure to enable these options: **Trust this user for delegation to specified services only** and **Use any Authentication protocol**.
Even though other options might seem more accurate, the Kerberos-only options do not work because they do not enable protocol transition and constrained delegation.

### kcdtest Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

- [ ] Do not trust this user for delegation
- [ ] Trust this user for delegation to any service (Kerberos only)
- [ ] Trust this user for delegation to specified services only
- [ ] Use Kerberos only
- [x] Use any authentication protocol

**Services to which this account can present delegated credentials:**

<table>
<thead>
<tr>
<th>Service Type</th>
<th>User or Computer</th>
<th>Port</th>
<th>Service Name</th>
<th>Domain</th>
</tr>
</thead>
</table>

- [ ] Expanded

[Add...][Remove]

**Add the services**

You must specify the services this applies to, as constrained delegation applies only to specific services. Select **Add**.

Click **Users or Computers** to select the computer hosting these services.
In this example, mail.ctxns.net hosts the Exchange service and sp.ctxns.net hosts the SharePoint web service. Therefore, in the preceding window both these machines need to be selected. These can be any other servers in the domain. Note that for Kerberos to be enabled, these servers should have Negotiate authentication enabled in the IIS configuration settings for the relevant websites they are publishing.

Also, constrained delegation does not support services hosted in other domains even though there is a trust relationship with those domains.
Add the services on the selected server.
The http service is selected because this example is about setting up constrained delegation to web-based servers (Exchange OWA and SharePoint). This is the same for any other web-based applications running on this server. Review the settings and click Apply/OK.

Generate Keytab file (Optional, only necessary if the NetScaler account is configured using the Keytab file)
The keytab file contains an encrypted password for the user. For KCD, this is only necessary if KCD Account (configured in NetScaler, explained below) is configured using a keytab file.

If the configured KCD Account does not use a keytab file, this step can be skipped.
Create the keytab file for the kcdtest user with SPN: host/kcdvserver.example.com@example.COM
You can select any of the following two options to generate a keytab file:
The NetScaler GUI has a utility that helps in creating a batch file, which can be run on the domain controller server to generate a keytab file. Select AAA Application Traffic > Batch file to generate keytab to open this utility. Copy the generated script and run it from a command prompt window on the domain controller server.
Run the following command to generate a keytab file:
```
ktpass /princ host/kcdvserver.example.com@example.COM /ptype KRB5_NT_PRINCIPAL /mapuser example\kcdtest /pass freebsd -out C:\kcdvserver.keytab
```

**Note:** host/kcdvserver.example.com@example.COM is case sensitive.

Copy the kcdvserver.keytab file to the `nsconfig/krb` directory on the NetScaler appliance.

**KCD configuration for AAA-TM**

The backend services we will use here are already configured; if they are not, please refer to earlier sections and the first guide for information on addition of servers, services and LB, CS and AAA vservers. We will include the CLI (command line interface) commands here for additional reference.

**Create the TM and authentication virtual server**

New commands introduced for the NetScaler appliance specify domain or realm for an LB or CS vserver when you define the virtual server. These parameters are optional.

For example, `add lb vserver accesslb1 HTTP 10.217.28.20 80`

(here, an LB vserver serves as the TM vserver)

**Create the authentication virtual server**

Here, we are providing sample CLI commands. For our deployment, CTXNS.NET corresponds to Example.COM and auth.example.com corresponds to clientcert.ctxnhs.net – the FQDN for the AAA vserver.

- `add authentication vserver auth1 SSL <IP address for AAA vserver> 443`
- `set authentication vserver auth1 -authenticationdomain Example.COM`
- `set lb vserver accesslb1 -authentication ON -authenticationHost auth.example.com`

**Create the KCD account**

The KCD Account is an entity consisting of the configuration necessary for delegation or impersonation. With delegation, the configured user would get tickets for a service on behalf of the actual user. The Delegated User string/setting which is specified in the KCD account should be the same user for which delegation is enabled on Active Directory.

There are multiple ways to create a KCD account in NetScaler.

**Create the KCD account using the keytab file**

To extract the SPN from the keytab file, use the KCD account. The NetScaler appliance reads the keytab file and extracts the SPN listed in the file. To see this prompt, navigate to **AAA Application Traffic>KCD Account>Add** and enable the **Use Keytab File** option.
On the CLI (NetScaler shell) you can use the following commands:

```
add kcdaccount <kcdaccount name> -keytab <keytab filename>.keytab
```

Or

```
add kcdaccount <kcd account name> -keytab /nsconfig/krb/<keytab file name>.keytab
```

**Note**: You must copy the keytab file to the /nsconfig/krb/ directory. If the file is not found in the /nsconfig/krb directory, the NetScaler appliance will reject it. For simplicity, it is best practice to use the FQDN of the LB or CServer as the keytab file name.

**Create the KCD account manually with a password**

Alternatively, the KCD account can be created by giving the delegated username and password.

Here, **Delegated User** is the user account to which services/users are delegated. **Password** is the password for this Delegated User account. **Realm** is the realm of the delegated user, and can be omitted if the delegated user’s name is in UPN (user@domain) format. If UPN is given, the realm is taken from the domain portion of the delegated user name.

NetScaler uses configured delegated users to get ticket granting tickets (TGTs). Active Directory accepts both ways of specifying names (UPN or SPN formats).

**Create the KCD account manually with a certificate**

Instead of specifying the delegated user’s password, you can use a client certificate, which is mapped to this user in Active Directory. A CA certificate is also required in this approach.

NetScaler uses the client certificate to obtain a TGT. This approach is highly secure as it does not involve specifying user’s password, and hence avoids password expiry problems.
To do this, either provide the client and CA certificates in the prompt shown earlier or use the following on the CLI:

```
add aaa kcdAccount <kcd account name> -realmStr <domain> -delegatedUser "host/<delegated user name>.<domain>" -usercert <string> -cacert <string>
```

where `usercert` is the path to the user’s certificate file stored on NetScaler, and `cacert` is the path to the issuing authority’s certificate.

**Create the traffic/session Profile**

You can provide the KCD account details in the session action or the traffic action. Different rules can be attached to the policies that use these actions. Rules are combinations of expressions. Expressions are simple conditions, such as a test for equality, which are applied to operands such as a URL string or an IP address.

**Note**: When you specify the KCD account in the traffic/session profile with SSO set to On, the NetScaler appliance completes KCD to the backend servers. If the KCD account is set to None, the NetScaler appliance performs standard NTLM SSO (SSO with standard Windows NT credentials, as KCD credentials are not available).

All of the following commands need to be entered on a shell window connected to the NetScaler CLI in the order specified below.

**Settings in Session Profile**

```
add tm sessionAction <session action name> -SSO ON -kcdaccount <kcd account name>
add tm sessionPolicy <session policy name> ns_true <session action name>
bind authentication vserver auth1 -policy <session policy name>
```

**Settings in Traffic Profile**

```
add tm trafficAction <traffic action name> -SSO ON -kcdAccount <kcd account name>
add tm trafficPolicy <traffic policy name> TRUE <traffic action name>
bind lb vserver accesslb1 -policy mysso1 -priority 100
```

**Setting at Global Level**

```
set tm sessionparameter -sso on -kcdaccount kcdaccount1
```
Alternatively, you can do these steps using the GUI. Navigate to **AAA Application Traffic > Authentication** and choose **Session** or **Traffic** policies.

Session policy definition
Configure Session Profile

Name

KCD_CC_SSO1

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

Session Time-out (mins)

30

Default Authorization Action*

ALLOW

Override Glo

Single Sign-on to Web Applications*

ON

Credntial Index*

PRIMARY

Single Sign-on Domain

HTTPOnly Cookie*

YES

Enable Persistent Cookie*

OFF

Persistent Cookie Validity

KCD Account

KCD_ClientCert

Home Page

OK  Close

Session profile definition

This completes the deployment guidelines for configuration of authentication settings on the NetScaler appliance.
Conclusion

Citrix NetScaler provides a complete replacement for Microsoft Forefront TMG for organizations seeking to securely host multiple, load balanced websites. As has been indicated through various NetScaler advantage callouts, this solution presents benefits over TMG for end users and provides for a wide range of authentication options.

About Citrix

Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler and NetScaler VPX are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.
<table>
<thead>
<tr>
<th>Location</th>
<th>Headquarters</th>
<th>City, Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Headquarters</td>
<td></td>
<td>Fort Lauderdale, FL, USA</td>
</tr>
<tr>
<td>Silicon Valley Headquarters</td>
<td></td>
<td>Santa Clara, CA, USA</td>
</tr>
<tr>
<td>EMEA Headquarters</td>
<td></td>
<td>Schaffhausen, Switzerland</td>
</tr>
<tr>
<td>India Development Center</td>
<td></td>
<td>Bangalore, India</td>
</tr>
<tr>
<td>Online Division Headquarters</td>
<td></td>
<td>Santa Barbara, CA, USA</td>
</tr>
<tr>
<td>Pacific Headquarters</td>
<td></td>
<td>Hong Kong, China</td>
</tr>
<tr>
<td>Latin America Headquarters</td>
<td></td>
<td>Coral Gables, FL, USA</td>
</tr>
<tr>
<td>UK Development Center</td>
<td></td>
<td>Chalfont, United Kingdom</td>
</tr>
</tbody>
</table>