Enabling EPA and Access Control with NetScaler Gateway for ADFS and other applications

Enterprise Use Case Guidelines
Table of Contents

Introduction 3
Solution Description 3
NetScaler Configuration 5
Conclusion 13
Introduction
Overview
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications. It provides availability, scalability, optimization and security for enterprise application deployments.

The Citrix NetScaler Gateway enables a large set of client end point management capabilities. A key enterprise use case that is enabled by the gateway is the ability to perform end point analysis on client machines looking to connect to enterprise services hosted on the NetScaler. This can range from simple checks such as IP-based filtering to more advanced client side checks such as the presence of an antivirus program.

Solution Description

Solution Workflow

The following steps describe the workflow for this solution:

1. The user attempts to log on to a secured enterprise application, either on the cloud or on the internal network. (In this example, we are using Office 365, configured for ADFS based SSO authentication)
2. The user is redirected to the NetScaler Gateway, which prompts for an EPA check.

   The EPA check feature allows for a large number of checks to be run on the client. These can be explored using the OPSWAT editor (described later in the document). More details on NetScaler’s EPA engine is available at https://www.citrix.com/blogs/2013/12/10/netscaler-gateway-advanced-end-point-analysis/

   Note: The EPA feature set has a number of possible applications for applications that are hosted and made available using the NetScaler Gateway. Although this solution only utilizes the Gateway to enable pre-authentication EPA, other possibilities are described at https://www.citrix.com/blogs/2014/09/26/how-to-securing-the-netscaler-gateway-using-opswat/

3. When the EPA check is successful, the user is redirected to the application for authentication. If the check fails, an error message is presented with details about the check that has failed. For the purpose of this guide, we are running a simple EPA check – verifying whether the client machine is running Notepad. (a common Windows application)
NetScaler Configuration
To enable this solution, the following configuration should be completed on the NetScaler.

Step 1: Configure Content Switching (CS) Virtual Server (Vserver)
To configure the content switching virtual server, navigate to Traffic Management>Content Switching>Virtual Servers and click on Add.

Create a new content switching vserver, by giving it an appropriate name (such as vs_https_adfs as shown above). Enter other details such as the IP address that the virtual server should use. This IP address should be the IP address that is bound to the public FQDN that is registered in Office 365 for authentication. The protocol used should be SSL.
Note: In this deployment, ADFS has been used as the backend authentication system for Office 365.

After creating the content switching virtual server, we will now configure the content switching policies to be configured on this virtual server. There are two key policies that should be configured that we will describe here.

To configure the policies, navigate to Traffic Management>Content Switching>Policies and click on Add. Alternatively, navigate to the Basic Settings window for the CS vserver you have just created by selecting the vserver in the list at Traffic Management>Content Switching>Virtual Servers. Here, scroll to the Policies section (if it isn’t seen, enable it in the menu to the right) and click on the + icon in the title bar (or on the Content Switching Policies entry in this section).

Policy 1 – EPA

With both methods described above, a screen similar to the following one will be shown for adding a policy –

![Policy 1 - EPA Configuration](image-url)
In the last screen shown on the earlier page, provide a name for the policy (the option is greyed out in this screenshot as this policy is already configured. It will be enabled and required when adding a new policy). The Action field specifies the action to be taken when the policy expression is matched. Defining this action will be described later in the document.

The Expression field specifies the condition that must be matched for the policy action to be triggered. Use the following expression to initiate the EPA check upon redirection from Office 365 –

```plaintext
http.req.url.contains("username") || is_vpn_url
```

This expression is triggered whenever the incoming request contains the term “username” (as it does for an Office 365 redirection) or when the request is for a VPN url. This second expression is a special predefined expression that is built into the NetScaler appliance.

To define the action for the policy, click on the + next to the Action field. Perform this step after completing the setup of the VPN virtual server.

Here, define the Gateway virtual server as the target virtual server and select NetScaler Gateway Virtual Server in the Choose Virtual Server or Expression field.
Policy 2 – Redirecting requests from invalid IP addresses

The second policy to be defined is for redirecting requests from invalid IP addresses. This policy can be used to filter requests from different geolocations, departments etc. Follow the same process as described earlier to define the following policy –

For this policy, use the following Expression –

```
Client.IP.SRC.IN_SUBNET(x.x.x.x/s).NOT
```

where x.x.x.x is the IP for the network subnet you would like to allow access to. Requests coming from any other IP subnet will be blocked.

For the action, select Load Balancing Virtual Server in the Choose Virtual Server or Expression field and specify a load balancing virtual server that can redirect the user to an appropriate alternate page. (Such as an Access Error webpage)
Step 2: Configuring the VPN Virtual Server

Now, we shall configure the NetScaler Gateway VPN virtual server. Navigate to NetScaler Gateway>Virtual Servers, then click on Add above the list shown in the main window.

After clicking on Add, the VPN Virtual Server settings screen is shown as below -

Configure the VPN virtual server with an available IP address (this need not be a publicly addressable IP address).

Once the VPN virtual server has been setup, you will be shown the Basic Settings screen for the virtual server as shown below. Here, apply an appropriate SSL server certificate. After applying the certificate, you should now configure the pre-authentication policy that will drive the EPA check.
Enabling EPA and Access Control with NetScaler Gateway for ADFS and other applications

Configuring the AAA Pre-authentication policy

Scroll to the Policies section in the Basic Settings screen for the VPN virtual server and click on the + icon to add a new pre-authentication policy and configure it.
The expression used here defines the pre-authorization checks to be carried out. In this example, we have used the following expression:

\texttt{CLIENT.APPLICATION.PROCESS\,(notepad) \ EXIST\,}

This expression checks to see whether the Notepad application is running on the client machine. In addition to simple checks such as this, a wide variety of other checks may also be configured. To configure more advanced checks, you can use the OPSWAT editor link at the top right of the Expression field. This opens up the Expression Editor window shown below.

It is possible to configure thousands of unique EPA check expressions using the editor. For the purpose of this deployment, however, we will be using the simpler expression that will check whether Notepad is running on the client machine.
Configuring the pre-authentication action/profile

To add and configure the pre-authentication action, click on the + button next to the Request Action field, which will give the following window:

Provide an appropriate name for the action, then set the Action drop down field to ALLOW. Leave the other settings as they are.
This completes the required configurations for this scenario.
**Conclusion**

A leading application delivery solution, Citrix NetScaler provides much more than application load balancing with an enhanced feature set that includes SSL VPN and authentication capabilities along with end point analysis. This enables enterprise solutions such as the one described in this document.

To learn more about how NetScaler can bring these benefits to enterprise requirements, please visit [http://www.citrix.com](http://www.citrix.com).