Education

CNS-221-2i
Citrix NetScaler Unified
Gateway

Lab Guide Version 1.0

PUBLISHED BY
Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, Florida 33309 USA
http://www.citrix.com

Citrix Systems, Inc. (Citrix) makes no representations or warranties with respect to the content or use of this publication. Citrix specifically disclaims any expressed or implied warranties, merchantability or fitness for any particular purpose. Citrix reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

Credits Page

Title	Name
Architects	Howard Weise Jesse Wilson
Product Manager	Lissette Jimenez Matt Brooks
Technical Solutions Developer	Aman Sharma Anton Mayers Layna Hurst Rhonda Rowland Shruti Dhamale
Instructional Designer	Elizabeth Diaz
Graphics Designer	Ryan Flowers Veronica Fuentes
Publication Services	Rahul Mohandas Akhilesh Karanth Nicole Tacher Zahid Baig
Special Thanks	Layer 8 Training

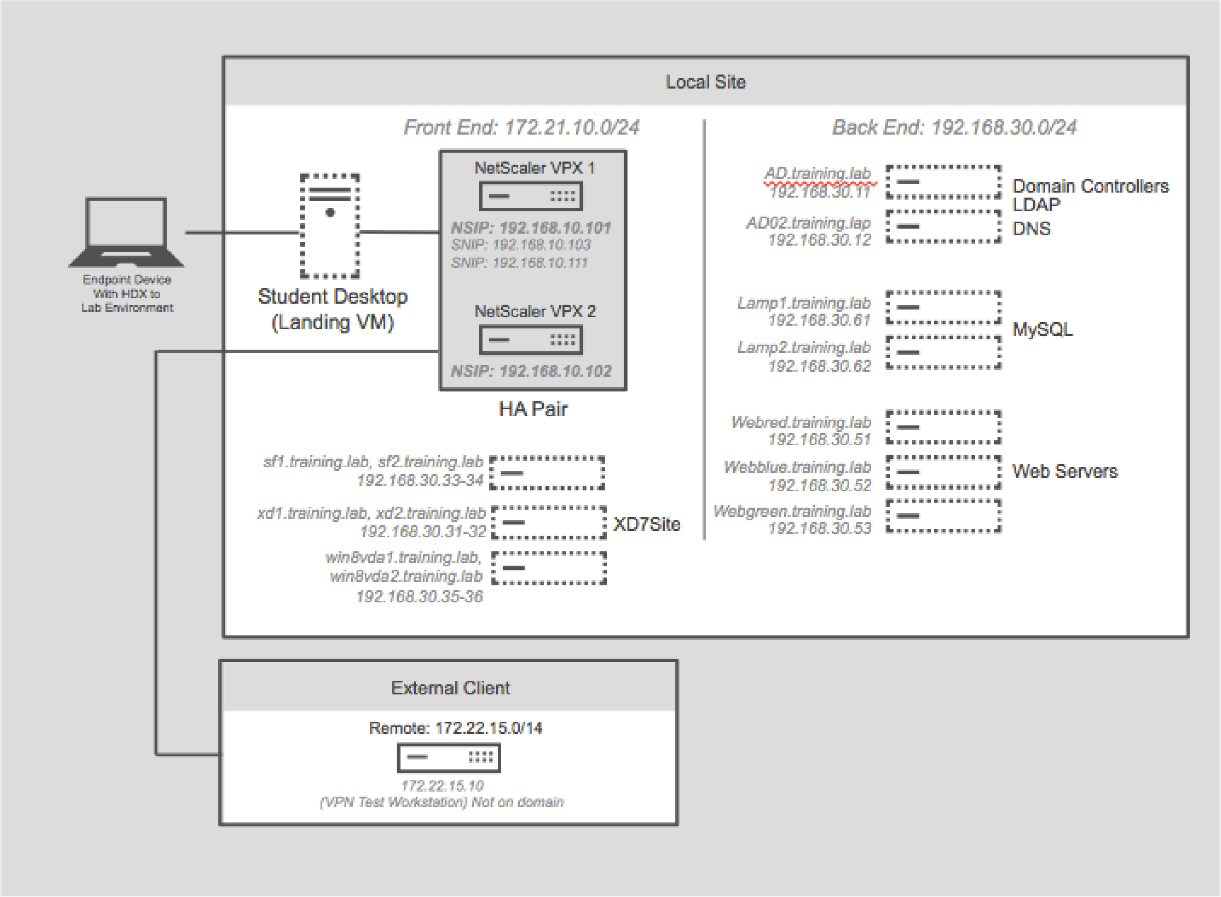
Contents

Lab Guide Overview

In this lab guide, you will get valuable hands-on experience with NetScaler Gateway and its features. This lab guide will enable you to work with product components and perform required steps for configuration of the NetScaler Gateway as an SSL VPN and for integration with XenApp/XenDesktop environments.

Lab Environment Overview

Lab Diagram



Local Site
Front End: 172.21.10.0/24
Back End: 192.168.30.0/24
Endpoint Device With HDX to Lab Environment
Student Desktop (Landing VM)
NetScaler VPX 1
NSIP: 192.168.10.101
SNIP: 192.168.10.103
SNIP: 192.168.10.111
NetScaler VPX 2
NSIP: 192.168.10.102
HA Pair
sf1.training.lab, sf2.training.lab 192.168.30.33-34
xd1.training.lab, xd2.training.lab 192.168.30.31-32
win8vda1.training.lab, win8vda2.training.lab 192.168.30.35-36
XD7Site
AD.training.lab 192.168.30.11
AD02.training.lap 192.168.30.12
Domain Controllers
LDAP
DNS
Lamp1.training.lab 192.168.30.61
Lamp2.training.lab 192.168.30.62
MySQL
Webred.training.lab 192.168.30.51
Webblue.training.lab 192.168.30.52
Webgreen.training.lab 192.168.30.53
Web Servers
External Client
Remote: 172.22.15.0/14
172.22.15.10
(VPN Test Workstation) Not on domain

SERVER LIST

Virtual Machine Name	Domain FQDN	IP Address	Description
AD.training.lab	ad.training.lab	192.168.30.11	Domain Controller (training.lab)
AD02.training.lab	ad02.training.lab	192.168.30.12	Domain Controller 2 (training.lab)
LAMP_1	lamp1.training.lab	192.168.30.61	MYSQL Database server
LAMP_2	lamp2.training.lab	192.168.30.62	MYSQL Database server
WebRed	webred.training.lab	192.168.30.51	Web Server
WebBlue	webblue.training.lab	192.168.30.52	Web Server
WebGreen	webgreen.training.lab	192.168.30.53	Web Server
Exchange	mail.training.lab	192.168.30.40	Exchange Server with OWA
ExternalClient	externalclient.training.lab	172.22.15.10	Windows 8; not a domain member.
RADIUS	radius.training.lab	192.168.30.15	Not a domain member; Radius services use TekRadius.
XD1	xd1.training.lab	192.168.30.31	XenDesktop 7.6 Controller and SQLExpress database.

XD2	xd2.training.lab	192.168.30.32	XenDesktop 7.6 Controller
SF1	sf1.training.lab	192.168.30.33	StoreFront 3.0.1
SF2	sf2.training.lab	192.168.30.34	StoreFront 3.0.1
Win8VDA1	win8vda1.training.lab	192.168.30.35	Win 8.1 - XenDesktop 7.6 VDA
Win8VDA2	win8vda2.training.lab	192.168.30.36	Win 8.1 - XenDesktop 7.6 VDA
Student Desktop	--	192.168.10.10	Student lab workstation; landing workstation. All labs performed from this system.

NetScaler List

Virtual Machine Name	NSIP Address	Subnet IP (SNIP) Address	Description
NS_VPX_01	192.168.10.101	SNIP1: 192.168.10.111 (traffic) SNIP2: 192.168.10.103 (mgmt.)	NS_VPX_01 is the principal NetScaler for most exercises. It will be in an HA Pair with NS_VPX_02 and they will be managed via the shared SNIP 192.168.10.103.
NS_VPX_02	192.168.10.102	HA Pair: shared configuration with NS_VPX_01.	Secondary member of HA Pair with NS_VPX_01.
NS_InsightCenter	192.168.30.13		Initially not configured.

CREDENTIALS LIST (1): Training Domain Users and Groups for NetScaler Administration

User Name	Groups	Password	Description
administrator	Domain Admins	Password1	Domain administrator account which can be used to access domain controllers. Otherwise, not needed in class.
trainNSAdmin	Training_NSAdmins	Password1	Domain account used in NetScaler delegated administration exercise.
trainNSOperator	Training_NSOperators	Password1	Domain account used in NetScaler delegated administration exercise.
trainADUser	Domain Users	Password1	Domain account used as LDAP BindDN service account.
Contractor	Contractors	Password1	Domain account available for NetScaler demonstrations.

CREDENTIALS LIST (2): Training Domain Users and Groups for NetScaler Gateway Testing

User Name	Groups	Password	Description
itadmin1	ITAdmins	Password1	ITAdmins usually will be granted full VPN access.
hruser1	HRUsers	Password1	Human Resources users.
sales1	Sales	Password1	Sales users.
contractor	Contractors	Password1	Contractors usually will be granted limited VPN access.

CREDENTIALS LIST (3): Training Domain Users and Groups with RADIUS accounts

User Name	Groups	Password	RADIUS Password
user1-user5	RADIUS (AD group) HRUsers (AD group)	Citrix123	Citrix456

CREDENTIALS LIST (4): Training Domain Users and Groups (Bonus Accounts not used in Labs)

User Name	Groups	Password	Description
icauser1	ICAUsers	Password1	Extra account that can be used for demos.
vpnuser1	VPNUsers	Password1	Extra account that can be used for demos.
ruser1	RestrictedUsers	Password1	Extra account that can be used for demos.
nsroot	Domain Users	Password1	Can be used to demonstrate need to disable external authentication on nsroot user on NetScaler.

CREDENTIALS LIST: NetScaler Local Accounts

User Name	Delegated Admin Role	Password	Description
nsroot	superuser	nsroot	Built-in NetScaler account; will be used for all exercises.
testuser	custom	Password1	Test account for delegated administration.
padmin1	Partition Admin	Password1	Test account for Admin Partitions exercise.
padmin2	Partition Admin	Password1	Test account for Admin partitions exercise.

Virtual Servers, FQDNs, and VIPs - (NetScaler Gateway)

FQDN	VIPs	Description
gateway.training.lab	172.21.10.150	Unified Gateway Virtual IP Address
storefront.training.lab	172.21.10.110	StoreFront Load Balancing VIP for (SF1 and SF2).
xdxml.training.lab	172.21.10.115	XenDesktop XML load balancing VIP (for XD1 and XD2)

Citrix Hands-On Labs

What are Hands-On Labs?

Hands-On Labs from Citrix Education allows you to revisit, relearn, and master the lab exercises covered during the course. This offer gives you 25 days of unlimited lab access to continue your learning experience outside of the classroom.

Claim introductory pricing of $500 for 25 days of access.

Contact your Citrix Education representative or **purchase online here**.

Why Hands-On Labs?

Practice outside of the classroom	You'll receive a fresh set of labs, giving you the opportunity to recreate and master each step in the lab exercises.
Test before implementing	Whether you're migrating to a new version of a product or discovered a product feature you previously didn't know about, you can test it out in a safe sandbox environment before putting in live production.
25 days of access	Get unlimited access to the labs for 25 days after you launch, giving you plenty of time to sharpen your skills.
Certification exam preparation	Get ready for your Citrix certification exam by practicing test materials covered by lab exercises.

Module 1: Introducing NetScaler Gateway

Overview:

Company ABC wants you to implement the NetScaler Gateway. Eventually, the NetScaler Gateway configuration will allow both SSL VPN and ICA Proxy connections. However, this initial configuration will begin with the SSL VPN deployment. In order to allow future expansion to support additional resources, the company has also asked that you begin with the Unified Gateway configuration.

In this module, you will perform hands-on exercises to create and configure the initial Unified Gateway to support SSL VPN access.

After completing this lab module, you will be able to:

- Import and convert a certificate in .pfx format into a certificate file the NetScaler can use.
- Use the Unified Gateway wizard to create the necessary content switching and SSL VPN virtual servers on the NetScaler.

This module contains the following exercises using the NetScaler Configuration Utility GUI:

- Exercise: Import SSL Certificate
- Exercise: Create NetScaler Unified Gateway
- Exercise: Test Unified Gateway Default Access

Before you begin:

Estimated time to complete this lab module: 20 minutes

Make Sure the following VMs are on.

AD.training.lab	SF1	XD2
AD02.training.lab	SF2	Win8VDA1
ExternalClient	WebBlue	Win8VDA2
NS_VPX_01	WebGreen	Exchange
NS_VPX_02	WebRed	
RADIUS	XD1	

Shutdown the following VMs:

Docker (won’t be needed)	LAMP_2 (won't be needed)
HTTP_Callout (won’t be needed)	NS_VPX_03 (won’t be needed)
LAMP_1 (won’t be needed)	WebRemote (won’t be needed)

Exercise 1-1: Import SSL Certificate (GUI)

In this exercise, you will import a domain-signed SSL certificate in .pfx format for with the Unified Gateway. You will use the Configuration Utility to perform this exercise.

When the .pfx certificate is imported, the NetScaler will convert it to a PEM format based certificate file. The converted certificate file will contain the server certificate issued to the wildcard FQDN *.training.lab and the associated private key. This certificate will then be used to create an SSL certkey for use with the Unified Gateway and any other SSL virtual server that needs to be accessed in the training.lab domain. This exercise builds on previous SSL exercises and shows how to import a certificate for use.

In this exercise, you will perform the following tasks:

- Import and convert a PFX wildcard certificate into NetScaler:

Import SSL Certificate

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Import the SSL Certificate PFX bundle • Navigate to **Traffic Management > SSL**. • Click **Import PKCS#12** in the right pane. Import PKCS12 File: • Enter **wc-training.cer** in the Output File Name field. • Click on Choose File drop down and click Local. • Browse to **C:\Resources\SSL Certificates\** and select **wc-training.pfx** and click **Open**. • Enter **Password1** in the Import Password field. • Select **DES3** in the Encoding Format. • Enter **Password1** in the PEM Passphrase and Confirm PEM Passphrase fields. Click **OK**.

3.	View certificate file after import: • Click **Manage Certificates / Keys / CSRs**. • Select **wc-training.cer** and click **View**. View the certificate details. • Verify the file contains a Begin Certificate…End Certificate block. • Verify the file also contains a Begin RSA Private Key…End RSA Private Key block. Note: This certificate contains both the certificate file and private key file. When creating the certkey object on the NetScaler it will point to this one file for both objects. Click **Close** to close the certificate details. Click **Close** to close the Manage Certificates dialog.
4.	Create an SSL certkey for the imported wildcard certificate file: • Navigate to **Traffic Management > SSL > Certificates > Server Certificates**. • Click **Install**. Install Certificate (Create SSL Certkey) • Enter **wc-training-certkey** in the Certificate-Key Pair Name field. • Enter **wc-training.cer** in the Certificate File Name field (or browse appliance for file). • Enter **Password1** in the Password field. Click **Install**. **Note :** In case you get a message command failed on Secondary node Kindly go to System>High Availability and do the force synchronization manually.
5.	Save the NetScaler configuration by clicking on the Floppy Icon on top right hand side and confirm.

Key Takeaways:

- Connections to the NetScaler Gateway must be made using SSL and require a trusted connection.
- Certificates signed by public CA's should be used in production deployments; otherwise root certificates will have to be distributed.
- SSL Certificate Requests can be generated on the NetScaler and submitted to a Certificate Authority.
- If the certificate was generated by some other device, the PFX format which contains the Certificate and associated private key can be imported onto the NetScaler for use.
- Wildcard certificates may be convenient to provide SSL functionality for multiple virtual servers.

Exercise 1-2: Create NetScaler Unified Gateway (GUI)

In this exercise, you will configure the NetScaler Unified Gateway using the wizard. You will use the Configuration Utility to perform this exercise.

The Unified Gateway wizard streamlines the process of configuring Content Switching and the VPN Virtual Server into one task. The Unified Gateway Wizard completes the essential configuration of the VPN Virtual server including SSL certificate binding, single-factor or two-factor authentication, and integration with XenApp/XenDesktop and other applications.

In this exercise, the basic Unified Gateway configuration will be performed to enable SSL VPN access. Integration with other applications and XenApp/XenDesktop will be added in later exercises.

Once the wizard has completed the VPN virtual server configuration, the initial VPN configuration will be modified to include settings required for the lab environment such as Split Tunnel. Later exercises will then continue to extend the configuration of the initial Unified Gateway.

In this exercise, you will perform the following tasks:

- Configure Unified Gateway with Wizard
- View and Modify Unified Gateway Settings
- Configure Initial Split Tunnel Settings
- Create an HTTP to HTTPS Redirect for the Unified Gateway

Configure Unified Gateway with Wizard

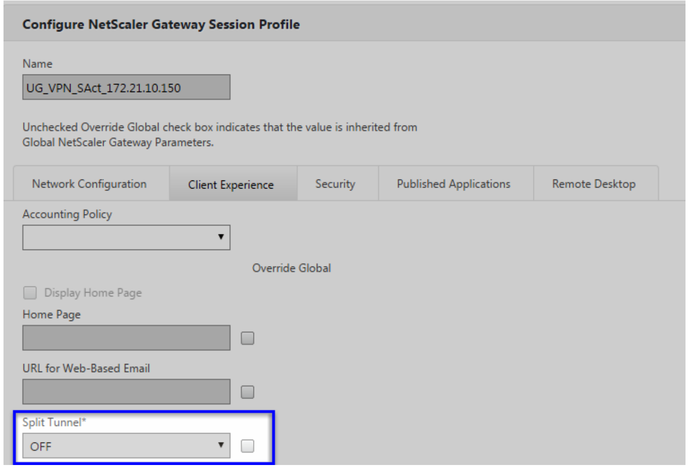
Step	Action
1.	Enable NetScaler features for Gateway: • Navigate to **System > Settings**. • Click **Configure Basic Features**. • Enable (check) **NetScaler Gateway**. Verify the following features are already enabled, if not Enable the features: • SSL Offloading • Load Balancing • Content Filter • HTTP Compression • Content Switching • Rewrite Click **OK**.

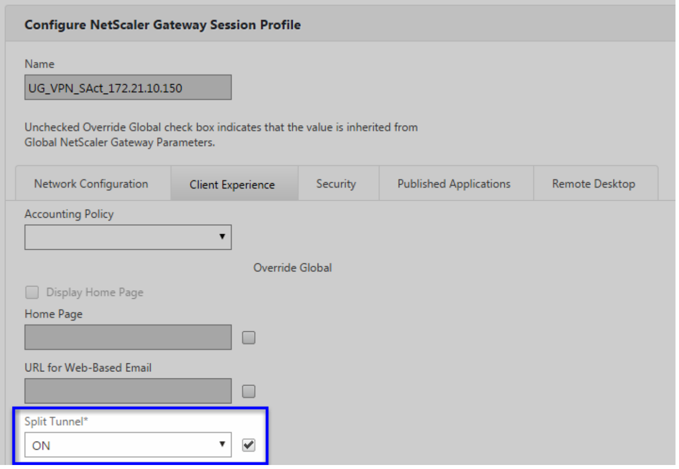
2.	Enable Advanced Features for Gateway: • Click **Configure Advanced Features**. Enable the following Advanced Features: • RDP Proxy. Verify Responder is already enabled, if not Enable it. Click **OK**.
3.	Start Unified Gateway Wizard: • Click **Unified Gateway** under Integrate with Citrix Products section in the Navigation Pane (left pane). • Click **Get Started** to begin the wizard. • Click **Continue** on Single Public Access Point.
4.	Unified Gateway Configuration: Virtual Server Enter the details necessary to create the unified gateway content switching virtual server. • Enter **ugw_gateway** in the Name field. • Enter **172.21.10.150** in the Unified Gateway IP Address field. • Verify Port is 443. Click **Continue**.
5.	Unified Gateway Configuration: Server Certificate Enter the details necessary to configure the wildcard SSL certificate. • Select **Use Existing certificate**. • Select **wc-training-certkey** from the Server Certificate drop-down list. • Click **Continue** to configure the certificate. Click **Continue** again.
6.	Unified Gateway Configuration: Authentication • Select **Active Directory/LDAP** under Primary Authentication Method. • Select **auth_ldap_policy** under Use Existing Server. • Leave Secondary Authentication Method set to None. • Click **Continue**. This configures the unified gateway to use the existing LDAP authentication policy against the training.lab domain.
7.	Unified Gateway Configuration: Portal Theme • Leave Portal Theme set to Default. • Click **Continue**.
8.	Unified Gateway Configuration: Applications • No applications will be configured at this time. • Click **Continue**. Click **Done** to end the Unified Gateway Configuration wizard. The Unified Gateway Dashboard is displayed.

View and Modify Unified Gateway Settings

Step	Action
1.	View Content Switching virtual server for the Unified Gateway: • Navigate to **Traffic Management > Content Switching > Virtual Servers**. • Verify the ugw_gateway virtual server is in an UP state.
2.	Update the Content Switching Virtual Server properties to disable SSLv3: • Select **ugw_gateway** and click **Edit**. • Click **Edit** (pencil icon) next to **SSL Parameters**. • Uncheck **SSLv3**. • Click **OK** to apply changes. Click **Done**.
3.	View VPN virtual server for the Unified Gateway status: • Navigate to **NetScaler Gateway > Virtual Servers**. • Verify the VPN virtual server is in an UP state.
4.	View the VPN virtual server for the Unified Gateway settings: • Select **UG_VPN_ugw_gateway** and click **Edit**. Verify the following settings that were configured by the Unified Gateway wizard: • The IP Address (VIP) is set to 0.0.0.0. • The wc-training-certkey is bound to the VPN virtual server. • The LDAP authentication policy (auth_ldap_policy) is bound to the primary authentication bank.
5.	Update the VPN virtual server properties to disable SSLv3: • Click the **Edit** icon next to **SSL Parameters**. • Uncheck **SSLv3**. • Click **OK** to apply changes. Click **Done**.
6.	Save the NetScaler configuration and confirm.

Configure Initial Split Tunnel Settings

Step	Action
1.	Edit Session Policy created by Unified Gateway wizard: • Navigate to **NetScaler Gateway > Policies > Session**. • Click the **Session Profiles** tab. • Select **UG_VPN_SAct_172.21.10.150** and click **Edit**.
2.	Update Profile settings to enable Split Tunnel: • Click the **Client Experience** tab. • Check the **Override Global** box for the Split Tunnel setting. (See Note below). • Set Split Tunnel to **ON.** **NOTE**: Anytime you need to edit a Session Policy setting, the Override Global checkbox must be enabled to make the setting active. When the Override Global is unchecked, the setting is not configured and can be inherited from the global parameters or lower-priority policies. This step explicitly referenced clicking the checkbox for Override Global. Future steps will not include this exact step as it is a requirement to configure the specified settings; the step will be implied from this point on.
	Override Global not checked; default policy setting applies.  **Configure NetScaler Gateway Session Profile** Name UG_VPN_SAct_172.21.10.150 Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters. Network Configuration | Client Experience | Security | Published Applications | Remote Desktop Accounting Policy Override Global □ Display Home Page Home Page □ URL for Web-Based Email □ Split Tunnel* OFF □

	Override Global checked; modified policy setting applies.  Configure NetScaler Gateway Session Profile Name UG_VPN_SAct_172.21.10.150 Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters. Network Configuration | Client Experience | Security | Published Applications | Remote Desktop Accounting Policy Override Global ☐ Display Home Page Home Page ☐ URL for Web-Based Email ☐ Split Tunnel* ON ☑
3.	Update profile with setting to force Gateway Plug-In icon to be displayed separately from Citrix Receiver icon: • Check **Advanced Settings**. • Remain on the **General** tab under **Advanced settings** and scroll to the bottom. • Enable (check) **Override Global** option for the **Show VPN Plugin icon with Receiver**. settings Click **OK** to close the profile.
4.	Create an Intranet App for the Internal (Server) network: • Navigate to **NetScaler Gateway > Resources > Intranet Applications**. • Click **Add**. • Enter **network_internal_192.168.30.0** in the Name field. • Select **TRANSPARENT**. This is the intercept type. • Enter **192.168.30.0** in the IP Address field. • Enter **255.255.255.0** in the Netmask field. (You need to clear the fourth octet for the Netmask.) • Click **Create**.
5.	Create an Intranet App for the External (Frontend) network: • Click **Add**. • Enter **network_external_172.21.10.0** in the Name field. • Select **TRANSPARENT**. This is the intercept type. • Enter **172.21.10.0** in the IP Address field. • Enter **255.255.255.0** in the Netmask field. • Click **Create**.
6.	Edit the Unified Gateway VPN virtual server: • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**.

7.	Bind the Intranet Application network_internal_192.168.30.0 to the Unified Gateway VPN virtual server: • Click **Intranet Applications** under Advanced Settings in the right-pane to add the category to the configuration pane (left pane). • Click **Intranet Application** under the Intranet Applications category. • Click **Click to Select** under Select Intranet Application. • Select **network_internal_192.168.30.0** and click **Select**. • Click **Bind**.
8.	Bind the Intranet Application network_external_172.21.10.0 to the Unified Gateway VPN virtual server: • Click **Intranet Application** under the Intranet Applications category. • Click **Add Binding**. • Click **Click to Select** under Select Intranet Application. • Select **network_external_172.21.10.0** and click **Select**. • Click **Bind**. • Click **Close** to close the VPN Virtual Server Intranet Application Binding dialog. Click **Done**.
9.	Save the NetScaler configuration and confirm.

Create an HTTP to HTPS Redirect for the Unified Gateway

Step	Action
1.	Create an HTTP load balancing virtual server to redirect to HTTPS: • Navigate to **Traffic Management > Load Balancing > Virtual Servers**. • Click **Add**. • Enter **lb_vsrv_ugw_sslredirect** in the Name field. • Verify **Protocol** is **HTTP** and **Port** is **80**. • Enter **172.21.10.150** in the IP Address field. • Click **OK**. Leave Services and Service Groups unbound: • Click **Continue**.
2.	Configure redirect URL setting: • Click **Protection** under the Advanced Settings. • Enter **https://gateway.training.lab** in the Redirect URL field. • Click **OK**. Click **Done**.
3.	Verify the virtual server lb_vsrv_ugw_ssl redirect is in a DOWN state.
4.	Save the NetScaler configuration and confirm.

Key Takeaways:

- The NetScaler Unified Gateway integrates Content Switching with the SSL VPN virtual server.
- The Unified Gateway wizard automates the configuration of the Content Switching virtual server and Content Switching policies, the VPN Virtual Server configuration, Certificate management, authentication policies. This simplifies implementing a complex configuration across multiple features by using the wizard.
- The Unified Gateway wizard creates a default Session Policy for the VPN virtual server.

Exercise 1-3: Test Unified Gateway Default Access (GUI)

In this exercise, you will test the Unified Gateway based on its initial settings. You will use the Configuration Utility to perform this exercise.

Now that the Unified Gateway has been configured, the initial connection will be used to download the NetScaler Gateway Plug-in and test SSL VPN connection. This will confirm the initial settings are correctly configured and establish a baseline for the VPN connection experience. Later exercises will demonstrate how to modify the user experience and control access to resources using the NetScaler Gateway policies.

This exercise will validate the NetScaler Gateway can successfully authenticate users and connect to internal network resources. The NetScaler Gateway is currently configured with default authorization settings (Allow).

During this exercise, you will install the NetScaler Gateway Plug-in on the test system (ExternalClient). During installation, the plug-in will cause a momentary interruption of the networking stack which may cause the RDP session to disconnect and then reconnect. In most cases, the session pauses for a second and then reconnects automatically without issue. If necessary, you can manually reconnect to the ExternalClient.

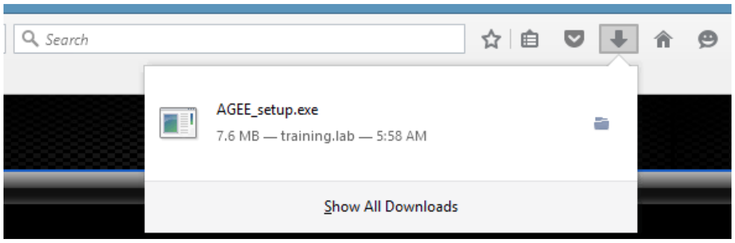
When establishing an SSL VPN connection, if the split tunnel settings are incorrect you could lose access to the test system. As a result, the NetScaler Gateway will be tested from the ExternalClient virtual machine only. If you lose access to the ExternalClient virtual machine, use XenCenter to connect to the ExternalClient console and end the VPN session. Do not connect to the NetScaler Gateway from the Student Desktop; instead the Student Desktop will be used to make configuration changes to the NetScaler.

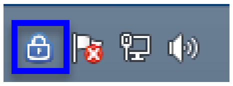
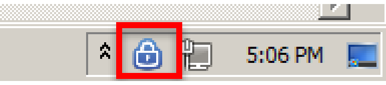
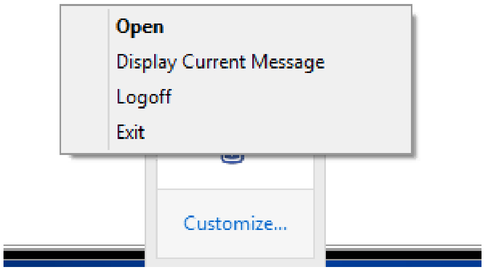
In this exercise, you will perform the following tasks:

- Test Unified Gateway and Install Gateway Plug-In

Test Unified Gateway and Install Gateway Plug-In

Step	Action
1.	Connect to the ExternalClient virtual machine (172.22.15.10) using the RDP Connections shortcuts on the desktop of the Student Management workstation. **NOTE**: The following credentials are used to make the connection: username: **externalclient\citrix with Password1** as the password. **IMPORTANT: Do Not** connect to the Unified Gateway from the Student Management workstation as you could lose access to your lab environment. All VPN connection tests should be performed from the ExternalClient.
2.	Test the connection to the Unified Gateway at https://gateway.training.lab: • Open Firefox and browse to https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1** Note : Open the connection using Firefox only .

3.	Verify the VPN client choices page is displayed with an option to connect over SSLVPN using the Network Access or to connect using Clientless Access. Click **Network Access** to connect using the SSLVPN.
4.	Install NetScaler Gateway Plugin. - Click Download - Save AGEWW_setup.exe - Click **AGEE_setup.exe** in the chrome downloads bar (bottom of browser).  Search AGEE_setup.exe 7.6 MB — training.lab — 5:58 AM Show All Downloads - Click Install - Click Yes on User access control. - The NetScaler Gateway Plug-in Setup wizard launches: - Click **Install** and click **Yes** to confirm. - Click **Finish**. - If the connection to ExternalClient is interrupted, reconnect to complete the install. - Check Remember my choice of Citrixing links and Click OK. Note : It will take around 2 minutes to install the NetScaler Gateway Plug-in.
5.	Log off the VPN Session using Browser and Close the Browser. Click **Exit** on the Citrix Windows Cleanup prompt.
6.	Reconnect to the NetScaler Gateway: - Browse to https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1**

7.	Click **Network Access** to connect using the SSLVPN. This time the NetScaler Gateway Plug-in icon is displayed in the Notification Area. If the icon does not auto display, drag the icon to the visible area.  **NOTE**: The Session Policy with the option to keep the NetScaler Gateway Plug-in Icon separate from the Citrix Receiver didn't apply until after the first logon to the Gateway. Now, the Gateway icon will be displayed separately from the Citrix Receiver on this system. If the Citrix Receiver is started the icons will appear side-by-side. Prior to 11.0 build we used to decouple using the registry keys . In case the Icon is not showing after the above mentioned steps try editing the following Registry values. To show the NetScaler Gateway plug-in icon, edit the following registry values: Run: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client Name: DisableIconHide Type: REG_DWORD Data: 1
8.	Log off the VPN Session: • Right-click the NetScaler Gateway Plug-in icon in the Notification Area and click **Log off**. • Click **Yes** to confirm. • Click **Exit** to cancel the Citrix Windows Cleanup option for the NetScaler Gateway Plug-in.   Open Display Current Message Logoff Exit Customize...
9.	Close the browser connected to https://gateway.training.lab.
10.	Note: Ignore the certificate warning in Chrome or use Firefox or internet Explorer .

Key Takeaways:

- Users connect to the NetScaler Gateway via a web browser using the Gateway FQDN. If the NetScaler Gateway plug-in is not installed, the Gateway will provide the user with the installation file. Upgrades to the NetScaler firmware may require an upgrade of the plug-in.
- The NetScaler Gateway Plug-in (VPN client) is required to make an SSL VPN connection. It is not required when using ICA Proxy or Clientless Access connections.
- The NetScaler Gateway Plug-in is a separate installation from the Citrix Receiver, but by default, once the NetScaler Gateway Plug-in is installed its interface will integrate with the Citrix Receiver interface.
- NetScaler 12 introduces a Session Policy setting that allows the NetScaler Gateway Plug-in interface to display and run separately from the Citrix Receiver interface for end-user convenience when the VPN is a primary connection method.

Module 3: Authentication and Authorization

Overview:

Company ABC wants to require two-factor authentication for users of the NetScaler Gateway in order to access the SSL VPN and other resources. As part of the initial SSL VPN configuration, you are also asked to configure different levels of access for different user groups in order to manage which users can access which resources over the SSL VPN.

In this module, you will perform hands-on exercises that will configure the NetScaler Gateway authorization and authentication policies.

After completing this lab module, you will be able to:

- Configure single-factor and two-factor authentication for a VPN virtual server.
- Create and manage AAA groups.
- Change default authorization settings from Allow to Deny.
- Use authorization policies to manage resources accessible using the VPN.
- Manage access to resources per group.

This module contains the following exercises using the NetScaler Configuration Utility GUI:

- Exercise: Configure Radius and Two-factor Authentication
- Exercise: Configure AAA Groups
- Exercise: Configure Authorization Policies

Before you begin:

Estimated time to complete this lab module: 30 minutes

RADIUS Authentication Infrastructure

Active Directory	Value
RADIUS.training.lab	192.168.30.15
RADIUS User accounts	User Name: user1-user5 Password: Citrix456 Radius accounts only exist for these 5 user accounts; no other LDAP account is currently configured on the Radius server.
LDAP User accounts	User Name: user1-user5 Password: Citrix123

LDAP Active Directory Authentication Infrastructure

Active Directory	Value
AD Domain Controller	192.168.30.11
AD2 Domain Controller	129.168.30.12
Administrator BindDN	trainaduser@training.lab
BindDN Account Password	Password1

LDAP Active Directory Groups and Accounts for NetScaler Gateway

USER	GROUP	PASSWORD
itadmin1	ITAdmins	Password1
contractor	Contractors	Password1
hruser1	HRUsers	Password1
sales1	Sales	Password1

Exercise 3-1: Configure Radius and Two-factor Authentication (GUI)

In this exercise, you will configure two-factor authentication using Radius and LDAP. You will use the Configuration Utility to perform this exercise.

Company ABC plans to require two-factor authentication for access to remote resources using the NetScaler Gateway SSL VPN or ICA Proxy connections. RADIUS authentication has not been fully deployed throughout the environment, but the company wants to do an initial test to confirm two-factor authentication works.

You will configure two-factor authentication using a new radius authentication policy and the existing LDAP authentication policy. The only accounts currently configured for both radius and LDAP authentication are the user1-5 accounts. After the two-factor authentication has been confirmed, reset the NetScaler Gateway to single-factor authentication using LDAP to continue with the rest of the exercises.

In this exercise, you will perform the following tasks:

- Configure Radius Authentication Policy
- Test Two Factor Authentication
- Restore Single Factor Authentication with LDAP

Configure Radius Authentication Policy

Step	Action
1.	Return to the Student Desktop.
2.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
3.	Create a Radius server (Policy Action): • Navigate to **NetScaler Gateway > Policies > Authentication > RADIUS**. • Click **Servers**. • Click **Add**.
4.	Configure the Radius authentication settings in the Create Authentication RADIUS Server dialog: • Enter **auth_radius_srv**. • Select **Server IP**. • Enter **192.168.30.15** in the IP Address field. • Verify **Port** is set to **1812**. Enter **Citrix456** in the Secret Key and Confirm Secret Key fields. Click **Create**. **Note**: We can test the connections as well by clicking on Test Connection. In case the test result show the Radius server port or service is not working reboot the Radius Server using Xencenter and build the Radius server again on NetScaler.

5.	Create a Radius authentication policy. • Click the **Policies** tab. • Click **Add**. Configure the policy: • Enter **auth_radius_policy** in the Name field. • Select **auth_radius_srv** in the Server field. • Enter **ns_true** in the Expression field. (Classic policy syntax.) • Click ok on the warning. Click **Create**.
6.	Edit the Unified Gateway VPN virtual server properties: • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**.
7.	Unbind the LDAP policy from the Primary Authentication bank: • Click **LDAP Policy** under the Authentication category for the Primary Authentication settings. • Select **auth_ldap_policy** and click **Unbind**. • Click **Yes** to confirm to unbind the entity. • Click **Close** to close the **Policy Binding** dialog box.
8.	Bind the RADIUS policy to the Primary Authentication bank: Choose the policy bind point (Radius: Primary Authentication) • Click "**+**" next to Authentication to bind a new policy. • Select **RADIUS** under Choose Policy. • Select **Primary** under Choose Type. • Click **Continue**. Bind the policy: • Click **Click to select** under Select Policy. • Select **auth_radius_policy** and click **Select**. • Leave priority set to 100. • Click **Bind**.
9.	Bind the LDAP policy to the Secondary Authentication bank: Choose the policy bind point (LDAP: Secondary Authentication) • Click "**+**" next to Authentication to bind a new policy. • Select **LDAP** under Choose Policy. • Select **Secondary** under Choose Type. • Click **Continue**. Bind the policy: • Click **Click to Select** under Select Policy. • Select **auth_ldap_policy** and click **Select**. • Leave **Priority** set to **100**. • Click **Bind**.

10.	Verify Authentication bindings display: • Primary Authentication: RADIUS Policy • Secondary Authentication: LDAP Policy Click **Done**.
11.	Save the NetScaler configuration and confirm.

Test Two Factor Authentication

Step	Action
1.	Connect to the ExternalClient virtual machine (172.22.15.10) using the RDP shortcuts on the desktop of the Student Management workstation. **Note**: The following credentials are used to make the connection: user name: **citrix with Password1 as the password.**
2.	Test the connection to the Unified Gateway at https://gateway.training.lab: • Open Chrome and browse to https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **user1** Password: **Citrix456** Password 2: **Citrix123** In this case the RADIUS credentials are in the first field (Password) and the LDAP Domain credentials are in the second field (Password 2).
3.	Click **Network Access** on the VPN Client Choices page.
4.	Log off the VPN session: • Click **Logoff** in the web browser. • Click **Exit** to cancel the Citrix Windows Cleanup option for the NetScaler Gateway Plug-in.
5.	Minimize the ExternalClient RDP session. Return to the Student Desktop.

Restore Single Factor Authentication with LDAP

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Edit Unified Gateway properties using the Unified Gateway Wizard: • Navigate to **Integrate with Citrix Products > Unified Gateway**. • Click **Authentication** on the right side. • Click **Edit** (pencil icon) next to Authentication. **NOTE:** This time the Unified Gateway wizard will be used to adjust the authentication policies. The Unified Gateway Wizard manages the same settings as the VPN Virtual Server properties (but there are some options the Unified Gateway does not support, that the VPN Virtual Server authentication policies can.
3.	Change Primary Authentication from RADIUS to LDAP: • Select **Active Directory/LDAP** from the Primary Authentication method drop down menu. • Verify **auth_ldap_policy** is automatically selected. • Verify the Secondary Authentication method is set to None. (It will say Not Configured on the Unified Gateway Configuration page.) • Click **Continue** to apply changes.
4.	Click **Back** at top of wizard to bypass rest of the configuration prompts. The wizard automatically saved the NetScaler configuration.

Key Takeaways:

- The NetScaler Gateway can support two-factor authentication by binding different authentication policies to the primary and the secondary authentication banks. If a policy is present in both banks, then users must authenticate successfully using both criteria.
- By configuring LDAP in the secondary authentication bank, user must pass the first authentication requirement before LDAP authentication is even attempted. This can help prevent repeated login attempts against LDAP and Active Directory.

Exercise 3-2: Configure AAA Groups (GUI)

In this exercise, you will configure AAA groups for NetScaler Gateway access. You will use the Configuration Utility to perform this exercise.

With the NetScaler Gateway, policies can be applied to the AAA Groups, allowing different users to be managed with different access permissions, connection types, and connection settings.

The AAA Group names must exactly match the corresponding Active Directory group names. The LDAP user authentication policy is configured for group extraction. Later exercises will bind authorization and session policies to the AAA Groups to manage each group's settings.

In this exercise, you will perform the following tasks:

- Configure AAA Groups

Configure AAA Groups

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Create AAA Group: ITAdmins • Navigate to **NetScaler Gateway > User Administration > AAA Groups**. • Click **Add**. • Enter **ITAdmins** in the Group Name field. • Click **OK**. Click **Done**. **NOTE**: Group Name is case-sensitive.
3.	Create AAA Group: HRUsers • Click **Add**. • Enter **HRUsers** in the Group Name field. • Click **OK**. Click **Done**.
4.	Create AAA Group: Contractors • Click **Add**. • Enter **Contractors** in the Group Name field. • Click **OK**. Click **Done**.
5.	Save the NetScaler configuration and confirm.

Key Takeaways:

- Group extraction can be used with both AAA authentication policies and system authentication policies for LDAP and RADIUS.
- AAA Group names must match the group names in the LDAP or RADIUS authentication service.
- NetScaler Gateway behavior can be managed by binding policies to the VPN virtual server or to the AAA groups. Policies bound to the AAA groups allow settings to be managed based on which user account connects.

Exercise 3-3: Configure Authorization Policies (GUI)

In this exercise, you will configure NetScaler Gateway Authorization Policies. You will use the Configuration Utility to perform this exercise.

The default NetScaler Gateway configuration sets the default authorization action to ALLOW. Once a user account has successfully authenticated, the user has access to any resource available over the SSL VPN connection. In order to manage the accessibility of resources over the SSL VPN, the default authorization can be set to DENY and then explicit authorization permissions can be granted to individual groups (or other criteria).

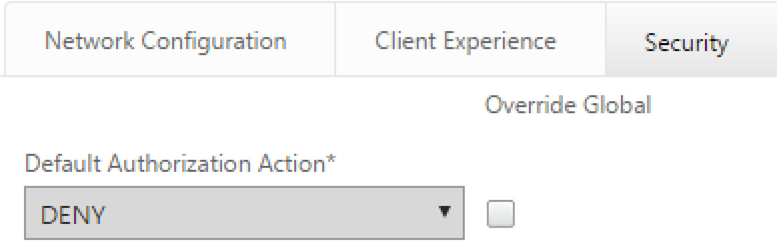
The following are requirements that must be met by the end of this exercise:

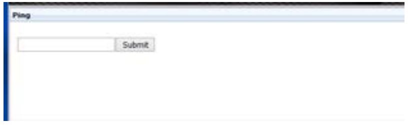
- Change the default authorization action for the NetScaler Gateway virtual server to DENY. Ensure that authenticated users that are not explicitly granted permissions are denied access to resources.
- ITAdmins will have full access to the internal resources over the SSL VPN. This includes access to all internal IP Address over any port.
- Contractors will have limited access to internal resources over the SSL VPN. The Contractors group should be able to access all internal IP Addresses but are limited to web connections only (HTTP:80 or HTTPS:443).

In this exercise, you will perform the following tasks:

- Change Default Authorization to DENY and test access
- Configure Authorization Policies
- Test the Authorization Policies

Change Default Authorization to Deny and Test Access

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Change default authorization setting in current Session Profile: - Navigate to **NetScaler Gateway > Policies > Session**. - Click **Session Profiles** tab. - Select **UG_VPN_SAct_172.21.10.150** and click **Edit**. Make the following changes to the Session Profile: UG_VPN_SAct_172.21.10.150. Security Tab: - Default Authorization Action: <not configured> **Override Global: Unchecked** (Deselect Override global to leave a non-configured Authorization Action value.)  Override Global Default Authorization Action* DENY ☐ Explanation: The wizard creates a profile with a default authorization action set to ALLOW which overrides the global parameter. By deselecting the Override Global, the Authorization Action is not configured by the policy, allowing global setting to take effect. The action will then reflect this inherited value from the system parameter. In this case, it is inheriting the global authorization action which is now set to DENY. Click **OK**. **NOTE**: To streamline Session Profile configuration, settings that need to be changed will be identified by the tab they are located on and the <Field Name>:<NEW Value>. Unless noted otherwise, assume override global will be enabled on any modified setting. Also, only modify values specified unless instructions note otherwise. Profiles may be modified multiple times to manage different settings in different exercises.
3.	Return to ExternalClient. Remain logged on as citrix.

4.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1** NOTE: Login is successful.
5.	Click **Network Access** to connect with the VPN.
6.	Attempt to ping a backend resource: • Open a CMD prompt: Start > Run > CMD. • Run command: **ping 192.168.30.11**. Expected Result: • The ping test fails. Use the Ping utility.  Expected Result : • Error: Not a privileged User.
7.	Open a web browser and attempt to connect to a backend resource: http://webblue.training.lab/. Expected Result: • The page fails to display in the browser.
8.	In the browser, return to https://gateway.training.lab. • Click **Logoff** in the portal page to end the VPN session. • Click **Exit** in the Citrix Windows Cleanup prompt.

Configure Authorization Policies

Step	Action
1.	Return to the Student Management workstation and access the NetScaler Configuration Utility: • Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103.

2.	Create Authorization Policy: autho_allowall • Navigate to **NetScaler Gateway > Policies > Authorization**. • Click **Add**. Configure Authorization Policy: • Enter **autho_allowall** in the Name field. • Select **Allow** in the Action field. • Click **Switch to Classic syntax**. • Enter **ns_true** in the Expression field. Click **Create**.
3.	Create Authorization Policy: autho_denyall • Click **Add**. Configure Authorization Policy: • Enter **autho_denyall** in the Name field. • Select **Deny** in the Action field. • Click **Switch to Classic syntax**. • Enter **ns_true** in the Expression field. Click **Create**.
4.	Create Authorization Policy: autho_allow_backendweb • Click **Add**. Configure Authorization Policy: • Enter **autho_allow_backendweb** in the Name field. • Select **Allow** in the Action field. • Click **Switch to Classic syntax**. • Enter the following expression or use the Expression Editor to build the expression: **`REQ.IP.DESTIP == 192.168.30.0 -netmask 255.255.255.0 && (REQ.TCP.DESTPORT == 80 || REQ.TCP.DESTPORT == 443)`** Click **Create**.
5.	Open the NetScaler Gateway Policy Manager: • Navigate to **NetScaler Gateway**. • Click **NetScaler Gateway Policy Manager**.

6.	Bind the autho_allowall policy to the ITAdmins group. Open the ITAdmins group: • Click the **"+"** sign next to AAA Groups to expand the AAA Groups node. • Select **ITAdmins** and click **Edit**. • Click **Authorization Policies** under Advanced Settings to add the category to the configuration pane. Bind the policy: • Click **Authorization Policy** under Authorization Policies. • Click **Click to Select** under Select Policy. • Select **autho_allowall** and click **Select**. • Enter Priority to **10**. • Click **Bind**. • Click **Done** to close the AAA Group properties.
7.	Bind the autho_allow_backendweb policy to the Contractors group. Open the Contractors group: • Select **Contractors** and click **Edit**. • Click **Authorization Policies** under Advanced Settings to add the category to the configuration pane. Bind the policy: • Click **Authorization Policy** under Authorization Policies. • Click **Click to Select** under Select Policy. • Select **autho_allow_backendweb** and click **Select**. • Enter Priority to **100**. • Click **Bind**. • Click **Done** to close the AAA Group properties.
8.	Close the Policy Manager: • Click **OK** on AAA Groups. • Click **Done** to close the Policy Manager.
9.	Save the NetScaler configuration and confirm.

Test the Authorization Policies

Step	Action
1.	Return to ExternalClient. Remain logged on as citrix.
2.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **ITAdmin1** Password: **Password1**

3.	Click **Network Access** to connect with the VPN.
4.	Attempt to connect using RDP to the Domain Controller (192.168.30.11): • Run the **RDP Test.cmd** shortcut on the desktop of ExternalClient. This will auto-launch a connection to ad.training.lab and authenticate as training\administrator without requiring a prompt for credentials. Expected Result: Verify the RDP connection is successful. Close (disconnect) the RDP session to ad.training.lab when done.
5.	Attempt to connect to a backend web server. Open a new tab in the web browser and browse to http://webblue.training.lab. Expected Result: The WebBlue server webpage loads successfully. **NOTE**: Members of the ITAdmins group are allowed access to all VPN resources due to the "allow all" authorization policy.
6.	Log off the NetScaler Gateway VPN connection: • Click **Log Off** on the https://gateway.training.lab page. • Click **Exit** in the Citrix Windows Cleanup dialog.
7.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **Contractor** Password: **Password1**
8.	Click **Network Access** to connect with the VPN.
9.	Attempt to connect using RDP to the Domain Controller (192.168.30.11): • Run the **RDP Test.cmd** shortcut on the desktop of ExternalClient. Expected Result: • RDP Connection will fail. Click **OK** to close the Remote Desktop Connection error dialog.
10.	Attempt to connect to a backend web server. Open a new tab in the web browser and browse to http://webblue.training.lab. Expected Result: The WebBlue server webpage loads successfully. **NOTE**: Members of the Contractors group are allowed access to web resources on the backend, but not other protocols. The web connection will succeed, while the RDP connection failed.
11.	Log off the NetScaler Gateway VPN connection: • Click **Log Off** on the https://gateway.training.lab page. • Click **Exit** in the Citrix Windows Cleanup dialog.

Key Takeaways:

- Authenticated users must still be authorized to access resources.
- Session and Authorization policies can be used to specify authorization actions ALLOW or DENY.
- Authorization Policies bind exclusively to AAA Groups or AAA users.
- Authorization Policies can be used to manage level of access to resources over the SSL VPN connection.

Exercise 3-4: Configure NetScaler as SAML SP and IDP

In this exercise, You will configure NetScaler as SAML Service provider and SAML Identity provider. You will use the Configuration Utility to perform this exercise.

Before we start with the exercise let us discuss the connection flow with SAML

- The SP trusts the IdP (trust relationship)
- The user connects to service, protected by SP. (In this scenario NetScaler Gateway)
- The user is redirected by SP to IdP to authenticate (SAML Request signed by SP)
- user brings SAML Request to IdP and authenticates (In this scenario AAA Vserver with LDAP bound to check the AD database)
- IdP creates SAML assertion after successful authentication and redirects back to SP (SAML assertion signed by IdP).
- SP validates SAML assertion and uses values for authorization.

In this exercise, you will perform the following tasks:

- Configure SAML IDP Policy.
- Configure AAA Vserver and bind the SAML IDP Policy to the vserver.
- Configure SAML SP Policy and bind it to the NetScaler Gateway Vserver.

Configure NetScaler as IDP

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Enable AAA Application Traffic • Navigate to **Security> AAA- Application Traffic.** • If you observe a yellow **(!)** icon, right click on it. • Click **Enable Feature**

3.	Configure AAA Vserver • Navigate to **Security > AAA - Application Traffic >Authentication Virtual Servers** • Click **Add** • Enter Name as **vsrv_aaa** • Confirm if in the IP Address Type field **IP Address** is selected • Enter IP Address as **172.21.10.108** • Observe that the port and protocol are selected as **443** and **SSL** respectively • Click OK
4.	Bind Certificate to the AAA Vserver • In the Certificate section, Click **No Server Certificate** • Click **Click to select** • Select **wc.training-certkey** • Click **Bind** • Click **Continue**
5.	Bind LDAP Policy to the AAA Vserver • Click **No Authentication Policy** • In the Select Policy file, Click **Click to select** • Select the **LDAP** policy • Click **Select** • Click **Bind** • Click **Continue** • Click **Done**
6.	Configure SAML IDP Profile • Navigate to **Security>AAA - Application Traffic>Policies>Authentication>Advanced Policies>SAML IDP** • Click **Profiles** • Click **Add** • Enter Name as **SAML_IDP_Prof** • Enter Assertion Consumer Service Url as **https://gateway.training.lab/cgi/samlauth** • Select IDP Certificate Name as **wc-training-certkey** • Select SP Certificate Name as **wc-training-certkey** • Select **Encrypt Assertion** • Select Encryption Algorithm as **AES256** • Enter Issuer Name as **https://gateway.training.lab** • Let the other settings be default • Click **Create** **Note:** in this scenario we have a wildcard certificate in the lab so we will be using the same certificate on IDP and SP. However, in the production you may use separate certificates

7.	Configure SAML IDP Policy • Navigate to **Security>AAA - Application Traffic>Policies>Authentication>Advanced Policies>SAML IDP** • Click **Policies** • Click **Add** • Enter Name as **SAML_IDP_Pol** • Select Action as **SAML_IDP_Prof** • Enter Expression as **true** • Click **Create**.
8.	Bind SAML IDP Policy to the AAA Vserver • Navigate to **Security>AAA - Application Traffic>Authentication Virtual Servers** • Select **vsrv_aaa** and click **Edit** • In Advanced Authentication Policies field, click **No SAML IDP Policy** • Click **Add Binding** • In Select Policy field, Click **Click to select** • Select the **SAML_IDP_Pol** • Click **Bind** • Click **Close** • Click **Done**

Configure NetScaler SP

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**

2.	Configure SAML SP Server • Navigate to **Security > AAA - Application Traffic > Policies > Authentication > Basic Policies>SAML** • Click **Servers** • Click **Add** • Enter Name as **SAML_SP_Server** • Select IDP Certificate Name as **wc-training-certkey** • Enter Redirect URL as **https://idp.training.lab/saml/login** • Enter User Field as **Name ID** • Select Signing Certificate Name as **wc-training-certkey** • (This is the SP certificate) • Enter Issuer Name as **https://gateway.training.lab** • Let the other settings be default • Click **Create**
3.	Configure SAML Policy • Navigate to **Security > AAA - Application Traffic > Policies > Authentication > Basic Policies>SAML** • Click **Policies** • Click **Add** • Enter Name as **SAML_SP_Pol** • Select Server as **SAML_SP_Server** • Enter Expression as **ns_true** • Click **Create**
4.	Bind policy to the NetScaler Gateway Virtual Server • Navigate to **NetScaler Gateway >NetScaler Gateway Virtual Servers** • In the Basic Authentication field, Click **+** icon • In the Choose Policy drop-down select **SAML** • In the Choose Type drop-down select **Primary** • Click **Continue** • In the Select Policy field, Click **Click to select** • Select **SAML_SP_Pol** • Click **Bind** • Click **Done**.

5.	Perform Test • Open a new browser window (Google Chrome) • Click **F12** • Click **SAML** • Browse for **https://gateway.training.lab** • Observe that you are being redirected to **https://idp.training.lab/logon/LogonPoint/tmindex.html** •Enter credential as **itadmin1/Passowrd1** We can observer the SAML authentication request either by Installing SAML Tracer in the browser or it can be confirmed using Ns.log. **Output from SAML Tracer.** SAML Tracer output with SAML authentication request The AssertionConsumerServiceURL=https://gateway.training.lab/cgi/samlauth The Destination="https://idp.training.lab/saml/login" • Enter credential as itadmin1/Passowrd1 • In the SAML tracer output it indicates the successful authentication. • samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode>

Key Takeaways:

- The Trust between the Service provider and Identity provider should be configured.
- In the SP in initiated authentication process the SP generates an AuthnRequest that is sent to the IDP as the first step in the process and the IDP then responds with a SAML Response.

Module 4: Session Policies

Overview:

Now that the initial VPN has been deployed, several settings need to be adjusted to manage the user experience. The Session Policy contains a wide range of settings that determine the type of connection end users receive (VPN, ICA Proxy, or Clientless Access). This module will use session policies to manage VPN and Clientless Access settings.

In this module, you will perform hands-on exercises that will configure additional VPN settings. The policies will modify the experience for the user group from full VPN access to Clientless Access with various levels of restrictions being applied to tune the behavior.

After completing this lab module, you will be able to:

- Create bookmarks and configure Clientless Access to internal web resources using the VPN virtual server.
- Manage VPN settings and advanced options available to the end user configuration.
- Configure and adjust the NetScaler Gateway Plug-in cleanup requirements.
- Configure EPA Scans and enable Pre-authentication policies to ensure users meet minimum requirements before authenticating to the NetScaler Gateway.

This module contains the following exercises using the NetScaler Configuration Utility GUI:

- Exercise: VPN Session Policies
- Exercise: VPN Clientless Access and Bookmarks
- Exercise: Client Configuration and Client Cleanup
- Exercise: EPA Scans and Preauthentication Policies

Before you begin:

Estimated time to complete this lab module: 30-45 minutes

Exercise 4-1 : VPN Session Policies (GUI)

In this exercise, you will configure a new Session Policy to modify the HRUsers group connection experience. You will use the Configuration Utility to perform this exercise.

Create a new Session Policy that will be applied to the HRUsers group. The policy profile will then be used to apply different VPN configuration settings to the HRUsers group. The HRUsers group will be used to test different policy configurations ranging from full VPN access to Clientless Access only.

This exercise you will just create and bind the new baseline policy for HRUsers. Future exercises will adjust and test the different configurations.

The following are requirements that must be met by the end of this exercise:

- Create a new Session Policy and bind to HRUsers.
- Ensure the Session Policy grants HRUsers unrestricted VPN access to backend IP addresses over all protocols. The policy will ensure authorization is allowed and override the global parameter default authorization action.
  - Access to internal web sites such http://blue.training.lab will succeed.
  - Access to any backend IP address over non-web protocols will also succeed, such as an RDP connection to AD.training.lab.

In this exercise, you will perform the following tasks:

- Create a new Session Policy and bind to HRUsers.
- Test the new Session Policy and confirm full VPN access is granted.

Create new Session Policy and Bind to HRUsers

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Create new Session Profile: • Navigate to **NetScaler Gateway > Policies > Session**. • Click on **Session Profiles** tab. • Click **Add**. • Enter **session_prof_hrusers_baseline**.

3.	Configure initial session profile settings: • Click **Security** tab. • Select the Override Global and then select **ALLOW** under Default Authorization Action. Click **Create**. **NOTE**: • This is essentially an empty profile with the exception of the Authorization Action set to ALLOW. This will serve the same purpose as the authorization policy when bound to the AAA Group. • Once it is bound it will be modified multiple times over the next several exercises to demonstrate different VPN settings and behaviors.
4.	Create Session Policy: • Click **Session Policies** tab. • Click **Add**. • Enter **session_pol_hrusers_baseline** in the Name field. • Select **session_prof_hrusers_baseline** in the Profile field. • Enter **ns_true** in the Expression field. • Click **Create**.
5.	Bind the policy session_pol_hrusers_baseline to HRUsers AAA group. Use the policy manager to access the AAA Groups: • Navigate to **NetScaler Gateway** • Click **NetScaler Gateway Policy Manager**. • Click **AAA Groups** to expand. • Click **AAA groups** under AAA Groups to view the list of groups. Bind the policy to the HRUsers: • Select **HRUsers** and click **Edit**. • Click **Policies** under Advanced Settings to add the category to the configuration pane. • Click the **"+"** sign to bind policies. • Select **Session** under Choose Policy and click **Continue**. • Click **Click to Select** under Select Policy. • Select **session_pol_hrusers_baseline** and click **Select**. • Leave **Priority** set to **100**. • Click **Bind**. • Click **Done** to close the HRUsers properties dialog. Exit Policy Manager: • Click **OK** to close AAA Groups. • Click **Done** to close Policy Manager.
6.	Save the NetScaler configuration and confirm.
7.	Return to ExternalClient. Remain logged on as citrix.

8.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1**
9.	Click **Network Access** to connect with the VPN.
10.	Attempt to connect using RDP to the Domain Controller (192.168.30.11): • Run the **RDP Test.cmd** shortcut on the desktop of ExternalClient. Expected Result: • RDP Connection will succeed. Close (disconnect) the RDP session to ad.training.lab when done.
11.	Log off the NetScaler Gateway VPN connection: • Click **Log Off** on the https://gateway.training.lab page. • Click **Exit** in the Citrix Windows Cleanup dialog.

Key Takeaways:

- Without priorities, Session Policies bound to AAA groups can override Session Policies bound to VPN virtual servers.
- With priorities, then the priorities determine the precedence of policies instead of the bind points.
- To continue using policies bound to AAA groups to override policies bound to virtual servers, apply higher priority (lower indexes) to the AAA group policies (such as priorities 1-3000) and apply lower priorities (higher indexes) to the VPN virtual servers (such as priority 6000-9000).

Exercise 4-2: VPN Clientless Access and Bookmarks (GUI)

In this exercise, you will configure Clientless Access for the HRUsers group. You will use the Configuration Utility to perform this exercise.

Modify the HRUsers baseline Session Policy to test Clientless Access to internal web servers (blue.training.lab and red.training.lab). Clientless Access will be tested in two scenarios. The first is a client choices configuration that allows HRUsers to switch between VPN access or Clientless Access. The second will force Clientless Access as the only connection option.

The following are requirements that must be met for the Clientless Access Scenario 1:

- Only HRUsers should be affected.
- Configure the policy to allow users switch between Clientless Access or SSL VPN connections.
- Configure Clientless Access to use no URL encoding and display the Clientless Access URLs in clear text.
- Create Clientless Access URLs to the internal web servers (http://red.training.lab and http://blue.training.lab). Assign the RED resource to all users of the VPN vserver. Assign the BLUE resource to only the HRUsers group.

The following are requirements that must be met for the Clientless Access Scenario 2:

- Update the Clientless configuration so that only Clientless Access is available to HRUsers. The Client Choices page should not be displayed.
- Change the Clientless URL encoding to Obscure instead of Clear text and notice how this affects the URL.
- Updated configuration will only apply to HRUsers.

In this exercise, you will perform the following tasks:

- Configure Clientless Access with Client Choices (Scenario 1)
- Test Client Choices and Clientless Access (Scenario 1)
- Configure and Test Clientless Access without Choices (Scenario 2)
- Restore Settings

Configure Clientless Access with Client Choices (Scenario 1)

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Open Session Profile session_prof_hrusers_baseline for editing: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Select **session_prof_hrusers_baseline** and click **Edit**.

3.	Configure Clientless Access and VPN Access: Configure the following settings on the Client Experience tab: Client Experience (Basic): • Clientless Access: **ON** (Override global: Enabled) • Clientless Access URL Encoding: **Clear** (Override global: Enabled) • Plug-in Type: **Windows/Mac OS X** (Override global: Enabled) Client Experience (Advanced Settings): General Tab • Client Choices: **Enabled** (Override global: Enabled) Click **OK**. **NOTE**: Even if the values specified match the default in the above settings, you should check the Override global box to treat these settings as configured settings instead of inherited settings.
4.	Create Bookmarks to web content for use with Clientless Access: • Navigate to **NetScaler Gateway > Resources > Bookmarks**. • Click **Add**. Configure Bookmark for the Red server: • Enter **web_red** in the Name field. • Enter **Red Server** in the Text to Display field. • Enter **http://webred.training.lab** in the Bookmark field. • Select **CVPN** in the Application Type field. • Check **Use NetScaler Gateway as a Reverse Proxy**. Click **Create**.
5.	Configure Bookmark for the Blue server: • Click **Add**. • Enter **web_blue** in the Name field. • Enter **Blue Server** in the Text to Display field. • Enter **http://webblue.training.lab** in the Bookmark field. • Select **CVPN** in the Application Type field. • Check **Use NetScaler Gateway as a Reverse Proxy**. Click **Create**.
6.	Open the NetScaler Gateway Policy Manager: • Navigate to **NetScaler Gateway**. • Click **NetScaler Gateway Policy Manager**.

7.	Bind bookmark web_red to NetScaler Gateway VPN Virtual Server. This will apply to all users connecting to this VPN virtual server. • Click **"+"** next to NetScaler Gateway Virtual Server to display a list of all VPN virtual servers. • Select **UG_VPN_ugw_gateway** and click **Edit**. Bind Bookmark web_red: • Click **Published Applications** under Advanced Settings (right-pane) to add the category to the configuration pane (left pane). • Click **URL** under Published Applications to bind bookmarks. • Click **Click to Select** under Select URL. • Click **web_red** and click **Select**. • Click **Bind**. • Click **Done** to close the VPN virtual server properties. Click **OK** to return to the Policy Manager.
8.	Bind bookmark web_blue to the AAA Group HRUsers: • Click **“+"** next to AAA Groups to display a list of all AAA groups. • Select **HRUsers** and click **Edit**. • Click **Bookmarks** under Advanced Settings (right pane) to add the category to the configuration pane (left pane). • Click **URL** under Published Applications to bind bookmarks. (The Bookmarks category changes name when added to the configuration pane.) • Click **Click to Select** under Select URL. • Click **web_blue** and click **Select**. • Click **Bind**. • Click **Done** to close the HRUsers properties. Click **OK** to close the AAA groups and return to the Policy Manager.
9.	Click **Done** to close the Policy Manager.
10.	Save the NetScaler configuration and confirm.

Test Client Choices and Clientless Access (Scenario 1)

Step	Action
1.	Return to ExternalClient. Remain logged on as citrix.
2.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1**
3.	Connect using the full VPN: • Click **Network Access**. • Verify the NetScaler Gateway Plug-in is "blue", indicating the VPN connection is active. With Client Choices enabled, the user has a choice between Network Access and Clientless Access.
4.	Test the VPN Connection: • Run the **RDP Test.cmd** shortcut on the desktop of ExternalClient. Confirm the connection is successful. • Logout of the VPN connection. • Click Exit on the NetScaler Gateway Windows Cleanup
5.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1**
6.	Make a Clientless Access connection: • Click **Clientless Access**. • Verify the NetScaler Gateway Plug-In is gray, indicating that a full VPN connection is not in use. Test the Clientless Access connection: • Verify both Blue Server and Red Server bookmarks are displayed. • Click **Blue Server**. • Verify BLUE Server content is displayed via the gateway URL: https://gateway.training.lab/cvpn/http/webblue.training.lab/ **NOTE**: The NetScaler Gateway Plug-in is gray instead of blue, indicating an SSL VPN connection has not been established.
7.	Return to https://gateway.training.lab and click **Log Off**.

Configure Clientless Access without Choices (Scenario 2)

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Open Session Profile session_prof_hrusers_baseline for editing: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Select **session_prof_hrusers_baseline** and click **Edit**.
3.	Configure Clientless Access only: Configure the following settings on the Client Experience tab: Client Experience (Basic): • Clientless Access: **ON** (Override global: Enabled) • Clientless Access URL Encoding: **Obscure** (Override global: Enabled) Client Experience (Advanced): • Client Choices: **Disabled** (Override global: Enabled) Due to a GUI bug, after enabling Override global, you must first check Client Choices to explicitly enable then uncheck Client Choices to clear the value. Otherwise, setting will still be ON. Click **OK**.
4.	Verify the Client Choices setting after creating the profile and verify it is disabled: • Select **session_prof_hrusers_baseline** and click **Edit**. • Click on the **Client Experience** tab. • Check **Advanced Settings**. • Verify Client Choices is explicitly disabled (unchecked) while the Override global is enabled (checked). • Correct the value if necessary at this time. Click **OK**.

5.	From the External Client, connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1** **NOTE**: No client choices page is presented; user is automatically connected to clientless VPN connection only.
6.	Test the Clientless Access connection: • Verify both Blue Server and Red Server bookmarks are displayed. • Click **Blue Server**. • Verify BLUE Server content is displayed via the gateway URL: https://gateway.training.lab/cvpn/<obscured URL strings>
7.	Return to https://gateway.training.lab and click **Log Off**.

Restore Settings

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Open Session Profile session_prof_hrusers_baseline for editing: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Select **session_prof_hrusers_baseline** and click **Edit**.

3.	Return configuration to allow Clientless Access or other connection types, if available: Configure the following settings on the Client Experience tab: Client Experience (Basic): • Clientless Access: **ON** (Override global: Enabled) Client Experience (Advanced): • Client Choices: **Enabled** (Override global: Enabled) Click **OK**.
4.	Save the NetScaler configuration and confirm.

Key Takeaways:

- Clientless Access does not require the NetScaler Gateway Plug-in to be installed. If it is installed, it is not engaged and a SSL VPN Tunnel is not established.
- All Clientless Access directs the client side request to the NetScaler Gateway VPN virtual server over SSL and then the VPN virtual server acts as a web proxy to the destination web server on the internal network.
- To obscure and protect the identity of the internal resources fulfilling the requests, the Clientless Access URLs can be rewritten as obscure or encrypted text instead of clear text.
- The client choices option can be used to determine whether user's have the option of choosing the connection type after log on to the NetScaler Gateway. Even if Client Choices is enabled, the client choices page will only be displayed if users have more than one connection method available.
- Disabling client choices will result in users being forced into one specific type of connection: SSL VPN, ICA Proxy, or Clientless Access only. The final result depends on the other configured Session Policy settings. When client choices are disabled:
- ON - Allow only clientless access.
- OFF - Allow clientless access after users log on with the NetScaler Gateway Plug-in.
- DISABLED - Do not allow clientless access.

Exercise 4-3: Client Configuration and Client Cleanup (GUI)

In this exercise, you will configure session policies to manage NetScaler Gateway Plug-in configuration and clean-up options for the HRUsers group. You will use the Configuration Utility to perform this exercise.

The NetScaler Gateway Plug-in provides a number of client-side tools and utilities that can be used to provide additional information for troubleshooting or diagnosing the SSL VPN connection and tools that can be used to change the SSL VPN behavior. For advanced VPN users, such as administrators or roaming engineers, these settings could allow a user to manually adjust split tunnel, split DNS, and network intercept settings as they move between networks. For other users, the administrator may want to prevent access to these advanced tools and settings.

Administrators may also want to force the NetScaler Gateway plug-in to clean up after itself when a user ends an SSL VPN session. This is especially useful if users connect in from shared, kiosk, or public workstations. The cleanup settings can be used to force removal of local instances of data referring to internal server names and IPs that are created during the session while using local resources like web browsers and other applications. Some of the data included in the cleanup list is session specific and will result in only data created during the VPN session log on and log off events being removed (such as cookies and auto-complete entries). Other data is non-selective and will be removed from the system regardless of when it was created such as address bar history. Using the cleanup settings, the administrator can determine what level of items to include in the cleanup and whether the cleanup action is optional or forced.

The following are requirements that must be met by the end of this exercise:

- Use the Session Policy to restrict access to the NetScaler Gateway Plug-in NetScaler Configuration menu. Only configuration menu options allowed should be General and Compression. The ability to change the VPN split tunnel and network intercept behavior should be disabled. Apply settings to HRUsers only.
- Ensure Client Cleanup is required with no option for users to bypass or to skip the cleanup action. Remove all settings; however, do not require the NetScaler Gateway plugin to be uninstalled. Apply settings to HRUsers only.

In this exercise, you will perform the following tasks:

- Configure and Test NetScaler Gateway Plug-in Configuration Options
- Configure and Test Client-Clean up Options

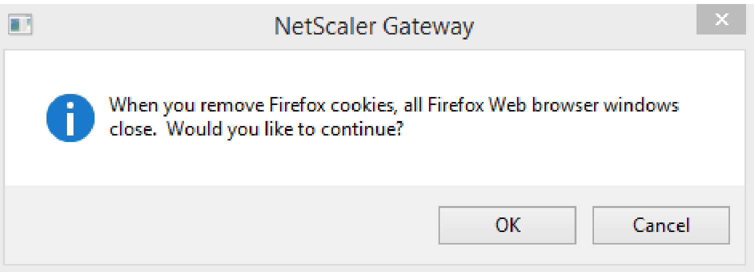
Configure and Test NetScaler Gateway Plug-in Configuration Options

Step	Action
1.	Return to ExternalClient. Remain logged on as citrix.
2.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1**
3.	Click **Network Access** to connect using the full VPN.
4.	Run the **RDP Test.cmd** shortcut on the desktop to establish an RDP connection over the VPN tunnel.

5.	Right-click the NetScaler Gateway Plug-in in the Notification area and click open. Click on Status and verify the following menu options are displayed: • Home • Tunneled Applications • Connection • Configuration • Logging • Additional Items: About, Logoff, Home page
6.	View client-side configuration options by clicking on Configuration: Notice the tabs available in the NetScaler Gateway Configuration window: Click on Status and select Configuration • Language • Enable debug Logging • Open homepage Automatically • Local LAN access
7.	Disconnect the RDP session to ad.training.lab (on ExternalClient).
8.	Right-click the NetScaler Gateway Plug-in and click **Logoff**. Click **Yes** to confirm logoff. Click **Exit** to cancel the Windows Cleanup.

Configure and Test Client-Clean up Options

Step	Action
1.	Demonstrate default Client Clean-up settings. • Return to ExternalClient. Remain logged on as citrix. • Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1** • Click **Network Access** to connect using the full VPN. • Right-click the NetScaler Gateway Plug-in and click **Logoff** and click **yes** to confirm. In the Citrix Windows Cleanup dialog, view the default checked clean up options: • Remove passwords and automatic completion data. • Clear Internet Explorer history. • Remove Internet Explorer Cookies. • Remove temporary Internet files. The unchecked boxes represent items not included in the cleanup process based on the selected cleanup level. The checked boxes represent items that will be removed by default, but for which the user could deselect to prevent cleanup. Switch to Student desktop and connect to NetScaler . Open Session Profile session_prof_hrusers_baseline for editing: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Select **session_prof_hrusers_baseline** and click **Edit**. • Click on Client Experience and select Client Cleanup under Advanced Settings Change the cleanup level to None and view cleanup settings: • Set cleanup level to **None**. • Click ok • Verify all items are deselected and unavailable for cleanup. Return to ExternalClient. Remain logged on as citrix. Log into the Unified Gateway VPN portal page using Firefox and the following credentials: User Name: **hruser1** Password: **Password1** • Click **Network Access** to connect using the full VPN. • Right-click the NetScaler Gateway Plug-in and click **Logoff** and click **yes** to confirm. • By default no cleanup is performed. Note: As the Client Clean up prompt is set to default user will get an option to select the cleanup level at his end , This is explained later in the exercise.

2.	Change the cleanup level to All Items and view cleanup settings: • Set cleanup level to **All items**. **NOTE**: Including cleanup of the NetScaler Gateway Plugin uninstall the plugin. The plugin removal is included in the All items cleanup level and optional in the Web browser cleanup level. Return to ExternalClient. Remain logged on as citrix. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1** • Click **Network Access** to connect using the full VPN. • Right-click the NetScaler Gateway Plug-in and click **Logoff** and click **yes** to confirm. It automatically performs the cleanup.  NetScaler Gateway When you remove Firefox cookies, all Firefox Web browser windows close. Would you like to continue? Click Ok on the warning. Click Exit on the Cleanup Prompt
3.	Open Session Profile session_prof_hrusers_baseline for editing: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Select **session_prof_hrusers_baseline** and click **Edit**.
4.	Configure client clean up options. Client Experience (Basic Settings) • Client Cleanup Prompt: **ON** (Override global: Enabled) Client Experience (Advanced Settings): • Click **Client Clean up** tab. • Force Cleanup: **Custom** Enable all cleanup options except for Plug-in; leave Plug-in deselected (disabled). • Cookie AddressBar • File System Application Application Application Data • Client Certificate Auto-Complete Cache Click **OK**.
5.	Return to ExternalClient. Remain logged on as citrix.

6.	Connect to the Unified Gateway at https://gateway.training.lab using Firefox. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1**
7.	Click **Network Access** to connect with the VPN.
8.	Click **Log off** in the web browser.
9.	Click ok on the firefox warning. It automatically did a cleanup of the used options.
10.	Click **Exit** to skip cleanup.
11.	Return to the Student Desktop.
12.	Client cleanup without Client Cleanup Prompt: Open Session Profile session_prof_hrusers_baseline for editing: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Select **session_prof_hrusers_baseline** and click **Edit**.
13.	Configure client clean up options. Client Experience (Basic Settings) • Client Cleanup Prompt: OFF (Override global: Enabled) • Click **OK**. This will force cleanup to occur based on previous options under Advanced Settings, without allowing the user a chance to bypass the cleanup or change the cleanup level.
14.	Return to ExternalClient. Remain logged on as citrix.
15.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **hruser1** Password: **Password1**
16.	Click **Network Access** to connect with the VPN.
17.	Click **Log off** in the web browser. • Verify the cleanup prompt is not displayed. • Cleanup options were forcibly applied at logoff.
18.	Return to Student Desktop.
19.	Save the NetScaler configuration and confirm.

Key Takeaways:

- The NetScaler Gateway Plug-in has a number of client-side options that are useful for diagnostics, troubleshooting, or advanced user VPN configurations. Session Policies can disable settings that administrators do not want users to adjust or have access to.
- Client clean-up is used to remove sensitive information left behind after the NetScaler Gateway Plug-in logs off an SSL VPN session.
- If the Client Clean-up prompt is presented to users, users can skip the recommended or required clean-up options.
- If the Client Clean-up prompt is disabled, then the configured clean-up options are required.
- If the Client Clean-up options include removing the NetScaler Gateway Plug-in, then the Gateway Plug-in is automatically uninstalled at the end of the VPN session (and must be reinstalled on next connection attempt). All clean-up options are then required and the client clean-up prompt is ignored.

Exercise 4-4: EPA Scans and Preauthentication Policies (GUI)

In this exercise, you will configure Endpoint Analysis scans and Preauthentication Policy requirements. You will use the Configuration Utility to perform this exercise.

Preauthentication Policies use EPA or OPSWAT scans to ensure that user devices meet minimum requirements in order to even access the authentication page. This scenario examines both EPA scan configuration and the Preauthentication Policy requirements.

Preauthentication Policies must be bound to the AAA Global or to the VPN virtual server. Since these policies are processed before authentication occurs, Preauthentication Policies cannot be bound to AAA groups or users. This configuration will affect all users of the NetScaler Gateway VPN virtual server in this configuration and not just select users.

The following are requirements that must be met by the end of this exercise:

- Configure a Preauthentication Policy that requires that a specific application is running on the client device to simulate antivirus detection. If the application (NotePad) is not running, access to the authentication page is denied. If the application (NotePad) is running, the user can attempt to authentication to the NetScaler Gateway VPN.
- To avoid having to run the scan for all subsequent tasks, the Preauthentication Policy will be unbound at the end of this exercise.

In this exercise, you will perform the following tasks:

- Configure and Test Preauthentication Policies
- Unbind Preauthentication Policies

Configure and Test Preauthentication Policies

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Configure global preauthentication settings to Deny: • Navigate to **NetScaler Gateway > Global Settings**. • Click **Change Preauthentication Settings** in the right-pane. • Select **DENY** from the Action drop-down list. Click **OK**. This configures a default deny preauthentication setting that applies to all virtual servers. This will deny access to the logon page unless an allow preauthentication condition is met.

3.	Create a new Preauthentication Profile to allow logons: • Navigate to **NetScaler Gateway > Policies > Preauthentication**. • Click **Preauthentication Profiles** tab. • Click **Add**. • Enter **preauth_prof_allowlogon_notepad** in the Name field. • Verify action is set to ALLOW. Click **Create**.
4.	Create a Preauthentication Policy that uses an EPA scan to detect that notepad.exe is running before it will allow access to the log on page: • Click **Preauthentication Policies** tab. • Click **Add**. • Enter **preauth_pol_allowlogon_notepad** in the Name field. • Select **preauth_prof_allowlogon_notepad** in the Request Action field. Use the Expression Editor to build the expression: • Click **Expression Editor**. • Select **Client Security** in the Select Expression Type drop-down list. • Select **Process** in the Component field. • Enter **notepad.exe** in the Name field. • Leave Operator set to EXISTS. Click **Done**. Verify the final expression is: **`CLIENT.APPLICATION.PROCESS(notepad.exe) EXISTS`** Click **Create**.
5.	Bind the policy to the NetScaler Gateway VPN virtual server: Open the NetScaler Gateway Policy Manager and edit the VPN virtual server: • Navigate to **NetScaler Gateway**. • Click **NetScaler Gateway Policy Manager**. • Click **"+"** next to NetScaler Gateway Virtual Server. • Select **UG_VPN_ugw_gateway** and click **Edit**. Bind the Preauthentication Policy to the virtual server: • Click **"+"** next to Policies. • Select **Preauthentication** under Choose Policy and click **Continue**. • Click **Click to Select** under Select Policy. • Select **preauth_pol_allowlogon_notepad** and click **Select**. • Click **Bind**. • Click **Done** to close the VPN Virtual Server properties. • Click **OK** to close the NetScaler Gateway Virtual Server list. Click **Done** to close NetScaler Gateway Policy Manager.
6.	Return to ExternalClient. Remain logged on as citrix.

7.	Connect to the Unified Gateway at https://gateway.training.lab. • To standardize steps, use Chrome to connect to the Gateway. **NOTE**: The EPA download screen is displayed before the logon screen.Ignore the certificate warning.
8.	The web browser displays a notice that your computer needs to be checked before you can be allowed to connect and an instruction to "download the software that handles this check". If you connect with Chrome: • There is no download button in the page. A separate window opens prompting to run the scan. It may open behind the browser, so look in the taskbar for a NetScaler Gateway icon. • Click **Yes** to allow the scan to occur. (This is a one-time authorization and will be repeated each time you access the page and the EPA scan requests to run.) • If you click Always the scan can run automatically without this extra prompt. However, for this lab exercise, click Yes each time. Expected Result: Access is denied since the EPA scan requirement failed since NotePad is not running. If you connect with Firefox (or IE), you will be prompted to download the EPA plug-in. Due to the self-signed certificate in use in the lab, Firefox may not perform the scan. This exercise assumes Chrome is in use.
9.	Start NotePad: **Start > Run > notepad.exe**.
10.	Repeat the test: • In the current Access Denied page (/epa/errorpage.html), click **Back** to repeat the scan. • Click **Yes** in the NetScaler Gateway Endpoint Analysis window to allow the scan to run. (Window may be behind browser windows.) Expected Result: Access to the logon page is allowed when notepad.exe is running.

Unbind the Preauthentication Policy

Step	Action
1.	Return to the Student Desktop.
2.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
3.	Change the global settings for preauthentication to allow: • Navigate to **NetScaler Gateway > Global Settings**. • Click **Change Preauthentication Settings**. • Select **ALLOW** under Action. • Click **OK**.

4.	Unbind Preauthentication Policy from VPN virtual server: • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**. • Click **AAA Preauthentication Policy** under the Policies category (at bottom of properties list). • Select **preauth_pol_allowlogon_notepad** and click **Unbind**. • Click **Yes** to confirm. • Click **Close** to close the policy binding dialog. • Click **Done** to close the VPN virtual server properties.
5.	Save the NetScaler configuration and confirm.

Key Takeaways:

- EPA scans are based on the classic policy engine's client security syntax and can look at a basic set of criteria to determine operating system, registry keys, files, and specific processes are present and/or running. The EPA scans can also detect various antivirus, firewall, and other security programs on the endpoint device.
- OPSWAT scans can be used in place of EPA policies and can provide more granular inspection on a wider range of criteria for enhanced security.
- Preauthentication Policies determine whether the users are allowed or denied access to the authentication page.

Module 5: XenDesktop Integration (ICA/HDX Proxy)

Overview:

Company ABC wants to enable secure, external remote access to the XenDesktop 7 environment using the NetScaler Unified Gateway in ICA Proxy mode.

In this module, you will perform hands-on exercises that will configure StoreFront and the NetScaler Gateway for ICA Proxy mode. Once ICA Proxy is implemented, configure session policies to enforce fallback to ICA for VPN users who fail to meet minimum requirements. Finally, configure SmartAccess integration between NetScaler Gateway and the XenDesktop site.

After completing this lab module, you will be able to:

- Configure StoreFront and NetScaler Gateway for ICA Proxy configuration.
- Use session policies bound to VPN virtual servers and groups to determine whether users get VPN only, ICA Proxy, or a choice in connection types.
- Use EPA scans to enforce connection fallback.
- Configure XenDesktop and NetScaler Gateway for SmartAccess filters.

This module contains the following exercises using the NetScaler Configuration Utility GUI:

- Exercise: Configuring StoreFront for Integration with NetScaler Gateway
- Exercise: Configuring NetScaler Gateway for ICA Proxy
- Exercise: Session Policy for ICA Proxy and ICA Proxy fallback
- Exercise: Test ICA Proxy
- Exercise: NetScaler Gateway SmartAccess with XenDesktop

Before you begin:

Estimated time to complete this lab module: 45-60 minutes

Exercise 5-1: Configuring StoreFront for Integration with NetScaler Gateway (GUI)

In this exercise, you will configure StoreFront for integration with NetScaler Gateway. You will use the Configuration Utility to perform this exercise.

In order to configure ICA Proxy, the StoreFront configuration needs to be updated with the NetScaler Gateway and remote access configuration details.

The following are requirements that must be met by the end of this exercise:

- Configure StoreFront with Pass through Authentication from NetScaler Gateway.
- Integrate the NetScaler Unified Gateway virtual server with StoreFront.
- Configure the necessary STA servers using HTTPS.
- And update the StoreFront XML Brokers to use the load balanced XML vServer (using HTTP:80)
- Propagate changes to StoreFront SF2.

In this exercise, you will perform the following tasks:

- Configure StoreFront Authentication, Beacons, and Remote Access

Configure StoreFront Authentication, Beacons, and Remote Access

Step	Action
1.	Connect to the SF1 virtual machine to access the StoreFront Management Console: • Use the RDP shortcut on the Student Desktop to connect to SF1. **Note**: The following credentials are used to make the connection: user name: **training\administrator** with **Password1** as the password.
2.	Open the StoreFront Management Console: • Click **Citrix StoreFront** icon in the taskbar (or use the Windows Search to search for Citrix StoreFront).
3.	Update the Base URL for StoreFront to match the FQDN used for the load balancing virtual server: • Navigate to **Server Group**. • Click **Change Base URL** in the Actions pane (right-pane). • Enter **https://storefront.training.lab/** in the Base URL field. Click **OK**.

4.	Enable Authentication to support Pass-through from Gateway: • Navigate to **Authentication**. Click **Add/Remove Methods** in the Actions pane. • Keep User name and Password enabled. • Select **Pass-through from NetScaler Gateway** to enable. Click **OK**.
5.	Create a NetScaler Gateway object on StoreFront: • Navigate to **NetScaler Gateway**. • Click **Add NetScaler Gateway Appliance** in the Actions pane. Complete Add NetScaler Gateway Appliance details: • Enter **UGW** in the Display Name field. Enter **https://gateway.training.lab** in the NetScaler Gateway URL field.Enter **https://gateway.training.lab in Callback URL.** Click **Next**.
6.	Configure Secure Ticket Authority URLs: Add XD1 as the first STA URL: • Click **Add**. • Enter **https://xd1.training.lab** in the STA URL field. • Click **OK**. Add XD2 as the second STA URL: • Click **Add**. • Enter **https://xd2.training.lab** in the STA URL field. • Click **Next**. Enter **https://gateway.training.lab under Callback URL** Click **Create** and click **Finish**. Click Close Refresh and ensure there are no warning messages.
7.	Configure Remote Access for the StoreFront store using the NetScaler Gateway object: • Navigate to **Stores**. • Select **Store-1** in the configuration pane (https://storefront.training.lab/Citrix/Store-1). • Click **Enable Remote Access** in the Actions pane. • Select **No VPN tunnel** for Remote Access. • Select **UGW** for NetScaler Gateway appliances to enable. Click **OK**.

8.	Update StoreFront list of XML brokers with the XDXML Load Balancing virtual server: • Select **Store-1**. • Click **Manage Delivery Controllers** in the Actions pane. • Select **XD7Site** and click **Edit**. Remove the individual Controllers from the Servers list: • Select **xd1.training.lab** and click **Remove**. • Select **xd2.training.lab** and click **Remove**. • Click **Add**. • Enter **xdxml.training.lab** in the Server Name field and click **OK**. • Select **HTTP** in the Transport Type field. • Select **80** in the **Port** field. • Click **OK** to close the Edit Delivery Controller dialog. Click **OK** to close the Manage Delivery Controllers dialog. **NOTE**: The load balancing virtual server will be created in the next exercise.
9.	Confirm Beacon settings: • Navigate to **Beacons**. • Verify the internal beacon contact point is https://storefront.training.lab/ • Verify the external beacon contact points are: https://gateway.training.lab and http://www.citrix.com.
10.	Propagate configuration changes from SF1 to SF2 in the StoreFront server group: • Navigate to **Server Group**. • Click **Propagate Changes** and click **Yes** to confirm. • Click **OK** when propagation completes. **NOTE**: If you make any additional changes to the StoreFront configuration on SF1 (or need to correct a misconfiguration), you must repeat the configuration propagation to ensure that SF2 is also updated. Otherwise, you may experience inconsistent results when load balancing StoreFront communication.
11.	Minimize the RDP session for SF1 and return to the Student Desktop.

Key Takeaways:

- StoreFront must be configured with the NetScaler Gateway FQDN and the callback address to support the ICA Proxy.
- Different Stores can be integrated with different NetScaler Gateways. A single store can also integrate with multiple NetScaler Gateways, though this may require additional steps to configure optimal gateway routing.
- The NetScaler Gateway must be configured with the identical list of STA's that StoreFront uses to request tickets.

Exercise 5-2: Configuring NetScaler Gateway for ICA Proxy (GUI)

In this exercise, you will configure the NetScaler Unified Gateway for the ICA Proxy integration using the Unified Gateway wizard. You will use the Configuration Utility to perform this exercise.

The Unified Gateway's XenApp/XenDesktop integration wizard will configure the necessary NetScaler Gateway policies and virtual server settings to integrate with XenApp/XenDesktop, such as StoreFront or Web Interface path, single-sign on integration, and list of STA's. In addition, the wizard can also automate the load balancing configuration for the StoreFront or Web Interface components and the XML brokers for new XenDesktop/XenApp 7.x infrastructure or classic XenApp 6.5 and earlier infrastructure.

Once the session policies for the ICA Proxy configuration have been defined, they can be modified to support client choices to allow for users to connect with VPN, ICA Proxy, or Clientless Access options as permitted. Or the policies can be used for ICA Proxy-only configurations.

The following are requirements that must be met by the end of this exercise:

- Use the Unified Gateway XenApp/XenDesktop wizard to configure the ICA Proxy settings.
- Integrate with StoreFront using SF1 and SF2. Configure load balancing using SSL:443 and VIP 172.21.10.110.
- Integrate with the XenDesktop XML Brokers using XD1 and XD2. Configure load balancing using HTTP:80 and VIP 172.21.10.115. Note: This wizard can change the port but cannot create the XML services with SSL. This will be updated later.
- Specify the list of individual STA's. These cannot refer to the load balanced virtual server for the XML services.
- Review the settings configured by the Unified Gateway wizard under Load Balancing and the updates to the VPN virtual server configuration regarding VPN virtual server properties and Session Policies.
- Update the wizard generated policies to disable Client Choices in order to use an ICA Proxy only configuration. Other policies can be used to override this setting to allow some users VPN and ICA Proxy configurations.
- Update VPN Authorization Policies to allow access to the necessary VIPs on the NetScaler; backend IP's may not be required for ICA Proxy only configuration. This step is for the combination of VPN connection policies and existing Authorization Policies already in place in the environment. An ICA Proxy only configuration may not require this adjustment.

In this exercise, you will perform the following tasks:

- Configure ICA Proxy with the Unified Gateway Wizard
- Review Settings Configured by the Unified Gateway Wizard
- Update Session and Authorization Policies

Configure ICA Proxy with the Unified Gateway Wizard

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Update the Unified Gateway configuration using the Unified Gateway Wizard: • Navigate to **Integrate with Citrix Products > Unified Gateway**. • Click **ugw_gateway** in the right-pane to edit its properties using the wizard. • Click **Edit** (pencil icon) next to Applications. • Click **"+"** sign next to Applications to create additional applications.
3.	Configure Unified Gateway for XenApp/XenDesktop integration using the wizard: • Select **XenApp & XenDesktop** under Type. • Select **StoreFront** under Choose Integration Point. • Click **Continue**. NOTE: This wizard can also configure integration with legacy Web Interface and Web Interface on NetScaler configurations.
4.	Configure integration settings: StoreFront • Enter https://**storefront.training.lab** in the StoreFront URL field. (This will be the FQDN of the load balanced StoreFront server configuration.) • Enter **training** in the Default Active Directory Domain field.
5.	Configure list of STA servers: • Click **"+"** next to the Secure Ticket Authority field to create a second entry. • Enter **https://xd1.training.lab** in the first Secure Ticket Authority field. • Enter **https://xd2.training.lab** in the second Secure Ticket Authority field. • Click on Retrieve stores (It will fail for now as we don’t have all the necessary configuration in place for now. • Enter **/Citrix/Store-1Web** in the Receiver for Web Path field. • Click Continue and then Done • Click back (Left arrow on the top) to avoid running through any additional tasks. **NOTE**: Secure Ticket Authorities cannot be load balanced; the NetScaler Gateway must point to each individual STA used by the associated StoreFront servers.

6.	Configure StoreFront Load Balancing configuration details: • Click on Traffic Management and select Load Balancing • Click Services and Add • Enter **svc_ sf1** under the Service name • Enter **192.168.30.33** under the IP Address • Select **SSL** from Protocol Drop down • Enter 443 under Port • Click Ok • Edit SSL parameter and uncheck **SSLV3** Click ok and Done • Configure Second service **svc_sf2** with IP **192.168.30.34** , Port 443 and **SSL** as protocol . • Disable SSLV3 Click ok and Done . Configure Load balanced Virtual Server • Click on Virtual Servers and Add. • Enter **lb_vsrv_sf** under the Name. • Select **SSL** under the Protocol • Enter **172.21.10.110** in the Virtual Server field. (This is the VIP for the load balancing virtual server for StoreFront.) • Click on **No Load balancing Virtual server** binding and click on **Click to Slect** select svc_sf1 and svc_sf2 and click bind Click **Continue**. • Click on No Server certificate and click on **Click to Select** select wc-training-certkey and click bind • Click Continue and uncheck the SSLv3 after editing SSL parameters. • Click on Persistence and select SOURCEIP from the Dropdown. • Click OK • Click Done

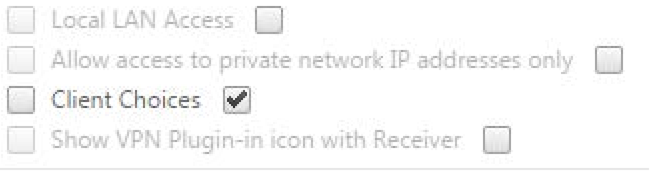
7.	Configure XenDesktop XML Broker Load Balancing: Configure XML broker services • Click on Traffic Management and select Load Balancing • Click Services and Add • Enter **svc_xml1** under Service Name. • Enter **192.168.30.31** (This is XD1.) • click ok . • Click Done • Add the second service • Enter **Svc_xml2** under Service Name. • Enter **192.168.30.32**. (This is XD2.)click ok and Done. • Click ok • Click Done. Configure Load balancing Virtual server • Click on **Virtual Servers** and click Add. • Enter **lb_vsrv_xml** under Name. • Enter **172.21.10.115** under IP address. (This is the VIP for the load balancing virtual server for the XenDesktop Controller XML Broker communication.) • Click on **No Load balancing Server Binding** and click **Click to Select** select **svc1_xml, svc2_xml2** and click Bind. • Click continue. • Click on Persistence and select SOURCEIP . • Click ok and Done.
8.	Add SNIP in Subnet of Load Balancing VIP. • Navigate to **System>Network>IPs** and click Add. • Enter **172.21.10.119** under IP Address • Enter **255.255.255.**0 under Netmask. • Select SNIP under the dropdown. • Uncheck Enable Management Access Control to support the below listed applications and confirm. • Click Create **Note**: There is a design change from NetScaler 11.0-67+ builds, where when you add StoreFront URL in NetScaler Gateway session profile, NetScaler will internally try to probe the load balancing VIP that is added. In order to counter this we need to configure SNIP in subnet of Load balancing VIP.
9.	Save NetScaler Configuration and Confirm.

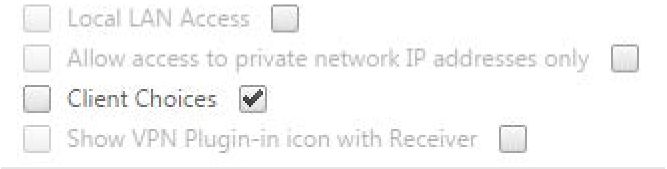
Review Settings

1.	View the NetScaler Gateway Virtual Server configuration: • Navigate to **NetScaler Gateway > Virtual Servers**. • Click **UG_VPN_ugw_gateway** and click **Edit**. View STA Configuration: • Click **STA Servers** under the Published Applications category. • Verify the STA Servers are configured using https://. • Verify both STA Servers are in an UP state and an STA ID (Auth ID) is displayed. • Click **Close**.
2.	View Session Policies bound to the NetScaler Gateway Virtual Server: • Click **Session Policies** under the Policies category. • Verify two new policies generated by the wizard are bound: PL_OS_172.21.10.150 and PL_WB_172.21.10.150. Click **Close** to close the policy binding list. Click **Done** to close the virtual server properties. These policies will be explored and updated in the next task.

Update Session and Authorization Policies

Step	Action
1.	Remain connected to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103.

2.	Edit Session Profile for ICA Proxy only configuration (without Client Choices): • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles**. • Select **AC_WB_172.21.10.150** and click **Edit**. Update the following settings: Published Applications: • Web Interface Address: **https://storefront.training.lab/Citrix/Store-1Web/** Client Experience (Advanced Settings): General • Client Choices: **Disabled** (Unchecked) (Override global: Enabled) Remember: After enabling Override global, check then uncheck the Client Choices option to clear the value.  □ Local LAN Access □ □ Allow access to private network IP addresses only □ □ Client Choices ☑ □ Show VPN Plugin-in icon with Receiver □ Click **OK**. **NOTE**: About the changes to the policy: • Due to our existing policies enabling VPN and Clientless Access options, users connecting will generally get presented with a Client Choices prompt. To make this an ICA Proxy only connection, the Client Choices option is being disabled as an override setting.
3.	Verify the Client Choices setting after creating the profile and verify it is disabled: • Select **AC_WB_172.21.10.150** and click **Edit**. • Click on the **Client Experience** tab. • Check **Advanced Settings**. • Verify Client Choices is explicitly disabled (unchecked) while the Override global is enabled (checked). • Correct the value if necessary at this time. Click **OK**.

4.	Edit session profile for ICA Proxy only configuration (without client choices): • Select **AC_OS_172.21.10.150** and click **Edit**. Update the following settings: Published Applications: • Web Interface Address: https://storefront.training.lab/Citrix/Store-1Web/ • Client Experience (Advanced Settings): General • Client Choices: **Disabled** (Unchecked) (Override global: Enabled) Remember: After enabling Override global, check then uncheck the Client Choices option to  ☐ Local LAN Access ☐ ☐ Allow access to private network IP addresses only ☐ ☐ Client Choices ☑ ☐ Show VPN Plugin-in icon with Receiver ☐ clear the value. Click **OK**.
5.	Create an Authorization Policy to allow access to VIPs hosted on NetScaler: • Navigate to **NetScaler Gateway > Policies > Authorization**. • Click **Add**. • Enter **autho_allow_frontend** in the Name field. • Keep Action set to ALLOW. Configure the expression: • Click **Switch to Classic Syntax**. • Enter the following expression or use the **Expression Editor** to build the expression: **`REQ.IP.DESTIP == 172.21.10.0 -netmask 255.255.255.0`** Click **Create**. Note: This policy will be bound later in the exercise.
6.	Return to ExternalClient. Remain logged on as Citrix.
7.	Connect to the Unified Gateway at https://gateway.training.lab. (Use Chrome.) Log into the Unified Gateway VPN portal page using the following credentials: User Name: **ITAdmin1** Password: **Password1** **NOTE:** ITAdmin1 is sent directly to StoreFront instead of the client choices page.

8.	Test connection to published resources using ICA Proxy. In Chrome: • The Welcome to Receiver page is displayed requesting to install the Citrix Receiver. • Click **Install**. • Check **Remember my choice for all links of this type** and click Launch Application (in the External Protocol Request field. • If the client is not detected as installed, click **Already Installed**. In Firefox: • The Install Citrix Receiver page is present. • Check **I agree with the Citrix License Agreement.** • Check **Skip to Logon**.
9.	Launch an application: • Click **Notepad** in the published list of resources in StoreFront. • Verify the application launches successfully. • Close the application.
10.	Log out of StoreFront: • Click the **drop-down arrow** next to the logged on user's name itadmin1 in the upper-right hand corner of StoreFront. • Click **Log Off**. This will log the user out of StoreFront and the gateway session. If you click "Log On" in the StoreFront page you will be directed to the NetScaler Gateway logon page.
11.	Connect to the Unified Gateway at https://gateway.training.lab. (Use Firefox.) Log into the Unified Gateway VPN portal page using the following credentials: User Name: **Contractor** Password: **Password1** Expected Result: Contractor receives a message: "Error: Not a privileged User". This is the message associated with an authorization DENY message. The contractor is configured to allow access to backend network resources using the VPN. The ICA Proxy connection only requires the contractor to access frontend network resources (specifically the NetScaler Gateway). The Authorization Policies will be updated.
12.	Minimize the ExternalClient RDP session and return to the Student Desktop.
13.	Remain connected to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103.

14.	Bind new Authorization Policy to Contractors group: • Navigate to **NetScaler Gateway > User Administration > AAA Groups**. • Select **Contractors** and click **Edit**. • Click **Authorization Policy** under Authorization Policies category. • Click **Add Binding**. • Click **Click to Select**. • Select **autho_allow_frontend** and click **Select**. • Click **Bind** and Click **Close**. • Unbind any other policy that is bind to the Group. • Click Close Click **Done**. **NOTE:** If Contractors will be used for ICA Proxy only, then no authorization policies are explicitly required if an Allow authorization is included in the Session Policy for ICA Proxy. If the group will be allowed to do VPN or ICA Proxy, then Authorization Policies may be required to limit types of resources allowed over the VPN connection.
15.	Save the NetScaler configuration and confirm.
16.	Switch to ExternalClient.
17.	Connect to the Unified Gateway at https://gateway.training.lab. (Use Chrome.) Log into the Unified Gateway VPN portal page using the following credentials: User Name: **Contractor** Password: **Password1** Expected Result: This time the log on succeeds and the user can access StoreFront and published resources.
18.	Launch an application: • Click **NotePad** in the published list of resources in StoreFront. • Verify the application launches successfully. • Close the application.
19.	Log out of StoreFront: • Click the **drop-down arrow** next to the logged on user's name contractor in the upper-right hand corner of StoreFront. • Click **Log Off**.

Key Takeaways:

- NetScaler Gateway configuration for ICA Proxy requires defining a Session Policy that identifies the StoreFront server and Store path to use, configuring the required Authentication Policies, and configuring the list of STA's for the NetScaler Gateway to use to redeem tickets. The Session Policy can be configured manually or using the XenApp/XenDesktop integration wizard that is part of the Unified Gateway.
- Configure StoreFront load balancing using either HTTP:80 or HTTPS:443 (or other ports specified). Load Balancing method is LeastConnections with SourceIP persistence.
- The Unified Gateway XenApp/XenDesktop wizard also generates the default session policies for ICA Proxy integration. In some scenarios, the default policies may need to be modified.
- The Session Policy/action PL_WB_<VIP> and AC_WB_<VIP> are for all web browser based connections.

- The Session Policy/action PL_OS_<VIP> and AC_OS_<VIP> are for connections made by the native Citrix Receiver that may require access to the Account Services path.

Exercise 5-3: Session Policy for ICA Proxy and ICA Proxy fallback (GUI)

In this exercise, you will configure ICA Proxy fallback to downgrade a user connection from full SSL VPN to ICA Proxy only in the event the user fails to meet EPA requirements. You will use the Configuration Utility to perform this exercise.

ICA Proxy fallback (or Session Policy fallback) allows and administrator to configure a security requirement within a Session Policy (such as minimum antivirus requirements). If the user or endpoint device fails to meet the requirement, the Session Policy will treat the user as a member of an alternate group known as a Quarantine Group instead of as a member of their regular directory service based group membership. The user can then receive the policies applied to the quarantine group when this fallback or quarantine mode is triggered. When the security requirements are met, the Quarantine Group is not in effect and the user receives their normal policies based on their regular AAA group membership.

The Quarantine Group is then usually a local group created on the NetScaler to manage these types of accounts and is not an actual group in the external directory service. Users become temporary members of this group when they fail the security requirement and they avoid becoming members when the security requirement is met.

The following are requirements that must be met by the end of this exercise:

- Create a AAA group that is local to the NetScaler (does not overlap with actual external directory services groups): ns_quarantine.
- Configure the necessary Session Policies to restrict access to ICA Proxy only and bind to the ns_quarantine group.
- Configure the fallback Session Policy that detects whether users meet the minimum requirements expected for VPN Access, if not quarantine the users by treating them as members in the ns_quarantine group. In this case, the criterion is dependent on whether WordPad is running or not. And bind this policy to the VPN virtual server.
- Test with users who normally receive Client Choices options and are allowed to connect using the SSL VPN or other options such as Contractors. Depending on whether WordPad is or isn't running will determine whether they receive a client choices connection page or whether it automatically connects as ICA Proxy only.

In this exercise, you will perform the following tasks:

- Configure and Test ICA Proxy Fallback

Configure and Test ICA Proxy Fallback

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**

2.	Create AAA Group for ICA Fallback scenario: • Navigate to **NetScaler Gateway > User Administration > AAA Groups**. • Click **Add**. • Enter **ns_quarantine** in the Group Name field. • Click **OK** and click **Done**. NOTE: This group is a local group on the NetScaler and is not a group in Active Directory.
3.	Create and configure Session Policy to allow VPN, Clientless Access, and Client Choices: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Click **Add**. • Enter **session_prof_dovpn_withchoices** in the Name field. Configure the following settings: Client Experience: Advanced Settings: General tab • Client Choices: **Enabled (**checked**)** **(**Override global: Enabled) Click **Create**.
4.	Create a Session Policy: • Click **Session Policies** tab. • Click **Add**. • Enter **session_pol_dovpn_withchoices** in the Name field. • Select **session_prof_dovpn_withchoices** in the Profile field. • Enter **ns_true** in the expression field. Click **Create**.

5.	Create and configure Session Policy to do ICA Proxy only: • Click **Session Profiles** tab. • Click **Add**. • Enter **session_prof_doicaproxy** in the Name field. Configure the following settings: Published Applications: (Override global: Enabled) • ICA Proxy: **ON** • Web Interface Address: **https://storefront.training.lab/Citrix/Store-1Web/** • Single Sign-On Domain: **training** Security: • Default Authorization Action: **ALLOW** (Override global: Enabled) Client Experience (Basic): • Clientless Access: **ON** (Override global: Enabled) • Plug-in Type: **Windows/MAC OS X** (Override global: Enabled) • Single Sign-on to Web Applications: **Enabled** (checked) (Override global: Enabled) Client Experience (Advanced Settings): General tab • Client Choices: **Disabled** (unchecked) (Override global: Enabled) Remember: After enabling Override global, check then uncheck the Client choices option to clear the value. Click **Create**. **NOTE:** The existing ICA Proxy policy generated by the Unified Gateway wizard could have been used with the modifications made earlier; but a new policy was created so you have the experience of which settings are required. That and its bind points can be tailored for this specific use-case.
6.	Verify the Client Choices setting after creating the profile and verify it is disabled: • Select **session_prof_doicaproxy** and click **Edit**. • Click on the **Client Experience** tab. • Check **Advanced Settings**. • Verify Client Choices is explicitly disabled (unchecked) while the Override global is enabled (checked). • Correct the value if necessary at this time. Click **OK**.
7.	Create a Session Policy: • Click **Session Policies** tab. • Click **Add**. • Enter **session_pol_doicaproxy** in the Name field. • Select **session_prof_doicaproxy** in the Profile field. • Enter **ns_true** in the expression field. Click **Create**.

8.	Create and configure Session Policy to do ICA Fallback, if a condition is not met. This will quarantine a user who would normally receive VPN access and limit them to ICA Proxy only. • Click **Session Profiles** tab. • Click **Add**. • Enter **session_prof_fallback** in the Name field. Configure the following settings: Security (Advanced Settings): • Client Security Check String: `CLIENT.APPLICATION.PROCESS(wordpad.exe) EXISTS` • Quarantine Group: **ns_quarantine** (Override global: Enabled) Click **Create**. Click OK on the warning. Detailed steps to configure the expression for the Client Security Check String, using the Expression Editor: • Click **Override Global** next to Client Security Check String. • Click **Expression Editor** to build the expression. • Expression Type: **Client Security** • Component: **Process** • Name: **wordpad.exe** • Operator: **Exists**. • Click **Done**.
9.	Create a Session Policy: • Click **Session Policies** tab. • Click **Add**. • Enter **session_pol_fallback** in the Name field. • Select **session_prof_fallback** in the Profile field. • Enter **ns_true** in the expression field. Click **Create**.
10.	Use the Policy Manager to bind the policies to AAA Groups. • Navigate to **NetScaler Gateway**. • Click **NetScaler Gateway Policy Manager**. • Click **"+"** next to AAA Groups.

11.	Bind VPN policy to ITAdmins group: • Select **ITAdmins** and click **Edit**. • Click **Policies** under Advanced Settings to add the category to the configuration pane. • Click **"+"** next to Policies. • Select **Session** under Choose Policy and click **Continue**. • Click **Click to Select** under Select Policy. • Select **session_pol_dovpn_withchoices** and click **Select**. • Click **Bind**. • Click Done and OK Click **Done** to close the ITAdmins group properties and.
12.	Bind the VPN Policy and the Fallback policy to Contractors group: Bind the Fallback Policy with Priority 10 to Contractors: • Click on User Administration and Click on AAA Group. • Select **Contractors** and click **Edit**. • Click **Policies** under Advanced Settings to add the category to the configuration pane. • Click **"+"** next to Policies. • Select **Session** under Choose Policy and click **Continue**. • Click **Click to Select** under Select Policy. • Select **session_pol_fallback** and click **Select**. • Enter **10** in the Priority field. • Click **Bind** . Bind the VPN Policy with Priority 100 to Contractors: • Click **Session Policy** under the Policies category. • Click **Add Binding**. • Click **Click to Select** under Select Policy. • Select **session_pol_dovpn_withchoices** and click **Select**. • Enter **100** in the Priority field. • Click **Bind**. • Click **Close** to close the Session Policy list. Click **Done** to close the Contractors group properties.

13.	Bind the ICA Proxy policy to the ns_quarantine group: • Select **ns_quarantine** and click **Edit**. • Click **Policies** under Advanced Settings to add the category to the configuration pane. • Click **"+"** next to Policies. • Select **Session** under Choose Policy and click **Continue**. • Click **Click to Select** under Select Policy. • Select **session_pol_doicaproxy** and click **Select**. • Enter **10** in the Priority field. • Click **Bind**. Click **Done** to close the ns_quarantine group properties. Click **OK** to close the AAA groups list. Click **Done** to close the Policy Manager.
14.	Save the NetScaler configuration and confirm.

Key Takeaways:

- Session Policy client security check settings are used to implement Session Policy fallback and connection quarantines. This can be used to conditionally override normal access permissions if a user (or endpoint device) fails to meet required security configurations.
- The fallback configuration can be used to downgrade SSL VPN connections to ICA Proxy or Clientless connections or to deny access.
- The Quarantine Group is a local group on the NetScaler that users receive temporary membership in by failing the client security check.

Exercise 5-4: Test ICA Proxy Connection and Fallback Policy (GUI)

In this exercise, you will test the ICA Proxy configurations and launch XenApp/XenDesktop resources using the Citrix Receiver and the NetScaler Gateway. You will use the Configuration Utility to perform this exercise.

With all the policies configured, test the ICA Proxy connection to XenApp and XenDesktop resources. Using the Contractor account will test the previously configured ICA Fallback policies.

This exercise tests with the following users only, but based on the policy configuration, the following results should be received for different accounts:

- ITAdmin1:
  - During Unified Gateway logon, user should receive the client choices page. Choice between: VPN, Clientless, and ICA Proxy
  - When connecting using the VPN: all backend resources area available over all ports; so both RDP and WEB connections will succeed (along with anything else).
- Sales1:
  - The Sales group was not defined as a AAA group on the VPN vServer. So after authentication, the sales1 account will only receive policies applied to the VPN virtual server. The current configuration, should result in an ICAProxy only connection (with no Choices page)
- Contractor:
  - Contractor is receiving the fallback policy.
  - With WordPad running: Client Choices page will be displayed. Contractor will have a choice of VPN, Clientless, and ICA Proxy connections. However, due to the Authorization Policies, the VPN connection will only access to WEB content (HTTP/HTTPS) to the backend network and no RDP (or anything else). the WEB test will succeed; the RDP test will fail.
  - Without WordPad running: the fallback policy is in effect and the Contractor user receives an ICAProxy only connection via the ns_quarantine group policies.

In this exercise, you will perform the following tasks:

- Test ICA Proxy Connections with Unified Gateway

NOTE: The Win8VDA's in the lab are not configured with Power Management in the XenDesktop site. If you log on with multiple users without logging off the existing sessions (such as by disconnecting instead), you may run out of resources to connect to. If the StoreFront displays a no resources available message, try rebooting the Win8VDA1 and Win8VDA2 systems using XenCenter as a quick way of freeing up resources.

Test ICA Proxy Connections and Fallback Policy with Unified Gateway

Step	Action
1.	Return to ExternalClient. Remain logged on as citrix.
2.	Open WordPad (local to ExternalClient): **Start > Run > wordpad.exe**.(Launch it from Desktop)
3.	Connect to the Unified Gateway at https://gateway.training.lab. (Use Chrome). Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1** **(Note:** The web browser displays a notice that your computer needs to be checked before you can be allowed to connect and an instruction to "download the software that handles this check". Click on Download)
4.	The EPA scan will be performed The Client choices page is displayed and the Contractor can either connect as a VPN user with web access to backend resources or can manually choose to make a clientless or ICA Proxy connection. Log off the VPN: • Click **Network Access** then click **Logoff**. • Click **Cleanup** and then click **Exit** in the Citrix Windows Cleanup prompt.
5.	Close WordPad.
6.	Reconnect to the Unified Gateway at https://gateway.training.lab. (Use Chrome). Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1**
7.	Expected Result: User connects using ICA Proxy only without a Client Choices page. ICA resources will launch successfully. Log off of StoreFront: • Click the drop-down arrow next to Contractor and click **Log Off**.

Key Takeaways:

- The ICA Proxy connection only requires the Citrix Receiver; no NetScaler Gateway Plugin (SSL VPN client) is needed nor is it engaged.

- All client communication is from the client to the NetScaler Gateway VIP over SSL:443. The gateway proxies the rest of the communication to StoreFront (or Web Interface) and the ICA/HDX connection to the VDA (or legacy XenApp servers).
- The NetScaler Gateway policies bound to the VPN virtual server and AAA groups largely determine the type of connections and the connection experience that users have.

Exercise 5-5: NetScaler Gateway SmartAccess with XenDesktop (GUI)

In this exercise, you will configure SmartAccess policies on the NetScaler Gateway and integrate these with the XenDesktop delivery groups to control resource availability. You will use the Configuration Utility to perform this exercise.

The following are requirements that must be met by the end of this exercise:

- Configure a NetScaler Gateway Session Profile with an EPA scan requirement that notepad.exe must be running. This Session Policy will point to a null profile and it sole purpose is to pass the result of the EPA scan (true or false) to the XenDesktop environment.
- Update the XenDesktop configuration to support SmartAccess by enabling XML Service Trust.
- Configure a SmartAccess requirement on the delivery group to require that the NetScaler Gateway policy returned true (NotePad is running) in order to access the published apps and desktop resources.

In this exercise, you will perform the following tasks:

- Configure SmartAccess Session Policies on the NetScaler Gateway
- Enable XML Service Trust on the XenDesktop Site and Update Delivery Group (with the SmartAccess setting).
- Test SmartAccess Policy

Configure SmartAccess Session Policies on the NetScaler Gateway

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Create a NULL Session Profile. • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Make sure no existing profiles are highlighted and click **Add**. • Enter **session_prof_null** in the Name field. Click **Create**. **NOTE**: A NULL profile contains no settings. It is used as a placeholder so that a Session Policy expression can be used to run an EPA scan. The policy expression result will be passed to the XenApp/XenDesktop environment. The settings for this session will be inherited from other Session Policies that go into effect.

3.	Create a Session Policy for SmartAccess. The policy expression will perform a test to see if the device meets requirements for corporate antivirus. For this exercise, notepad.exe will be used as a stand-in. • Click **Session Policies** tab. • Click **Add**. • Enter **session_pol_antivirus_good** in the Name field. • Select **session_prof_null** from the Profile drop-down list. • Enter the following in the Expression field: `CLIENT.APPLICATION.PROCESS(notepad.exe) EXISTS` Click **Create**.
4.	Bind the policy to the VPN virtual server to affect all ICA connections through Gateway. • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**. • Click **Session Policies** under the Policies category (at bottom of the configuration pane). • Click **Add Binding**. • Click **Click to Select** under Select Policy. • Select **session_pol_antivirus_good** and click **Select**. • Enter **10** in the Priority field. • Click **Bind**. • Click **Close** to close the policy Binding list. Click **Done** to close the VPN virtual server properties.
5.	Save the NetScaler configuration and confirm.

Enable XML Service Trust on XenDesktop Site and Update Delivery Group

Step	Action
1.	Use RDP shortcut on desktop to connect to XD1. Log into the utility using the following credentials: User Name: **training\Administrator** Password: **Password1**
2.	Open PowerShell • Click the **PowerShell** icon in the taskbar or **Start > Run > PowerShell.exe**.

3.	Run the following PowerShell commands to view and update the property: Add PowerShell Snap-in: **`add-pssnapin citrix*`** View current site settings to verify PowerShell snap-in loaded: **`get-brokersite`** Notice that the TrustRequestsSentToTheXMLServicePort property is False by default. Update XML Service Trust setting to $TRUE: **`set-BrokerSite -TrustRequestsSentToTheXMLServicePort $True`** The parameter supports tab-completion.
4.	Open Citrix Studio: • Click **Citrix Studio** shortcut in Taskbar or use Windows Search.
5.	Update the Delivery Group with the SmartAccess filter. Connections meeting the requirement (notepad running) will receive the published apps and desktop. Connections failing the requirement will have no access to this delivery group. • Navigate to **Delivery Groups**. • Select **Win8Desktop** and click **Edit Delivery Group**. • Click **Access Policy** (left pane). Configure the Access Policy settings: • All connections not through NetScaler Gateway: **Enabled**. • Connections through NetScaler Gateway: **Enabled**. • Connections meeting any of the following filters: **Enabled**. Configure the SmartAccess Filter: • Click **Add**. • Site or Farm Name: **UG_VPN_ugw_gateway** This is the name of the VPN virtual server configured on the NetScaler Gateway. • Filter: **session_pol_antivirus_good** This is the name of the Session Policy configured on the NetScaler Gateway. • Click **OK** twice to apply changes. **NOTE**: Names in use in the filter must match the names on the NetScaler. The values are not case-sensitive, but typos would be invalid. If necessary, copy the VPN virtual server name and the Session Policy name from the NetScaler Gateway to Studio on XD1. Also note this is the name of the VPN virtual server and not the Unified Gateway object which is actually a CS virtual server.

Test SmartAccess Policy

Step	Action
1.	Return to ExternalClient. Remain logged on as citrix.
2.	Prepare applications for test: • Close any existing instances of WordPad. • Open an instance of NotePad.
3.	Connect to the Unified Gateway at https://gateway.training.lab. (Use Chrome). Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1**
4.	Verify Contractor is connected to StoreFront and all published resources are displayed.
5.	Log off of StoreFront: • Click the drop-down arrow next to Contractor and click **Log Off**.
6.	Close notepad.exe.
7.	Reconnect to the Unified Gateway at https://gateway.training.lab. (Use Chrome). Log into the Unified Gateway VPN portal page using the following credentials: User Name: **contractor** Password: **Password1**
8.	User connects successfully to StoreFront, but StoreFront displays a message that there are no apps or desktops available to you at this time. Log off of StoreFront: • Click the drop-down arrow next to Contractor and click **Log Off**. **NOTE**: The SmartAccess test would also apply to ICA Proxy connections for other user groups such as: ITAdmins, Sales, and HRUsers.
9.	Remember to keep NotePad running to access XenDesktop resources in later exercises.

Key Takeaways:

- SmartAccess allows the NetScaler to pass results of EPA scans to the XenApp/XenDesktop environment in order to trigger specific types of functionality.
  - SmartAccess can be used to control whether delivery groups are or aren't available when users log on to StoreFront. Certain published applications or desktops (delivery groups) may be only available to internal users or gateway users meeting these security requirements. If the SmartAccess policy fails, the resource is not displayed.

  - SmartAccess can also be used to trigger XenApp/XenDesktop policies based. The SmartAccess policy from the Gateway can then be used to trigger XenDesktop user policies and can be used to turn on or off various virtual channels.
- SmartAccess requires the XenDesktop XML Brokers are configured with the trust requests sent to XML Service setting. This is configured via PowerShell at the XenDesktop Site-level on XenDesktop 7.
- In addition, SmartAccess requires users to consume a Universal License (SSL VPN concurrent user license) instead of the unlimited ICA Proxy licenses.
- SmartControl is a new feature in NetScaler 12 that allows the ICA virtual channels to be controller at the NetScaler without needing to pass SmartAccess policy results to the XenDesktop environment.

Module 6: Unified Gateway

Overview:

Now that the SSL VPN and ICA Proxy configurations have been deployed with the Unified Gateway, this module will enhance the user experience with the Unified Gateway by configuring additional settings such as Exchange integration and RDP Proxy configurations.

In this module, you will perform hands-on exercises that will customize the Unified Gateway configuration. You will customize the NetScaler Unified Gateway portal them to match the StoreFront deployment and look at basic customizations such as changing the background image Header and Footer customization and including a custom EULA requirement.

After completing this lab module, you will be able to:

- Configure additional applications for integration with the Unified Gateway.
- Configure RDP Proxy settings for the Unified Gateway and integrate RDP Proxy connections with the end user resources.
- Change and customize the Unified Gateway portal theme.
- Integrate a custom EULA message and require end user acceptance of requirements prior to accessing corporate resources.

This module contains the following exercises using the NetScaler Configuration Utility GUI:

- Exercise: Add Application: Exchange Integration
- Exercise: RDP Proxy
- Exercise: Portal Themes and Customizations
- Exercise: Apply an End User License Agreement

Before you begin:

Estimated time to complete this lab module: 40-55 minutes

Exercise 6-1: Add Application: Exchange Integration (GUI)

In this exercise, you will configure OWA Exchange integration with the Unified Gateway. You will use the Configuration Utility to perform this exercise.

Outlook Web Access (OWA) allows for web-based access to Exchange. OWA utilizes either Kerberos or NTLM authentication. In this exercise, OWA is configured with NTLM authentication. OWA will be integrated with the list of additional applications available with the Unified Gateway as a Clientless application. Single sign on will pass through from the NetScaler Gateway logon to the OWA website during the user connection.

Only user1-user5 are configured with Exchange inboxes. These accounts are also members of the HRUsers group. The current Session Policy provides the client choices option during login, so these users can select Clientless Access to perform the OWA demo. Be sure to test OWA with these accounts only.

In this exercise, you will perform the following tasks:

- Configure OWA Integration with the Unified Gateway using Clientless Access.
- Test OWA access using the Unified Gateway.

Configure OWA Integration with the Unified Gateway

Step	Action
1.	Return to the StudentDesktop.
2.	Open XenCenter: • Right-click **Exchange** and select **Start(In case it's not on)**. • Wait for exchange to boot. It may take a few minutes. If there are not enough resources to boot Exchange, shutdown LAMP_1, and LAMP_2 servers.
3.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
4.	Update the Unified Gateway configuration using the Unified Gateway Wizard: • Navigate to **Integrate with Citrix Products > Unified Gateway**. • Click **STA** in the right-pane to edit its properties using the wizard. • Click **Edit** (pencil icon) next to Applications. • Click **"+"** sign next to Applications to create additional applications.
5.	Configure OWA Integration as a Web Application: • Enter **OWA** in the Name field. • Select **Clientless Access** from the Application Type drop-down list. • Enter **https://mail.training.lab/owa** in the Enter URL field. • Click **Continue** and click **Done** to close the Application wizard. Click **Continue** and click **Done** to end the Unified Gateway Wizard. Click Back arrow on the top left hand side of Unified Gateway to exit the setup.

Test OWA

Step	Action
1.	Connect to ExternalClient using the RDP shortcut.
2.	Verify WordPad is running.
3.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **user1** Password: **Citrix123**
4.	Click **Clientless Access** to connect using the gateway web proxy.
5.	Click **OWA** link under Web Sites. OWA is being access via the web proxy function. • Wait for OWA to connect. The first launch after booting exchange may take up to 6-8 minutes to display the user's inbox. Additional launches will be much faster. (The exchange server is low on memory.) • Verify OWA connection for user1. • Notice that the user was not prompted for authentication to access OWA. Existing policies enabled Single Sign On to Web Applications.
6.	Close OWA and log off of the NetScaler Gateway: • Close the OWA tab. • Return to the NetScaler Gateway tab at https://gateway.training.lab and click **Log off**.

Key Takeaways:

- The Unified Gateway wizard makes it easy to add additional resources of various types to the existing Unified Gateway configuration. These resources can include additional web application accessible using Clientless Access, additional web application accessible via the content switching virtual server, or direct integration with XenApp/XenDesktop environments.
- The NetScaler Gateway SSL VPN connection can support single sign on to OWA if the authentication is based on NTLM.

Exercise 6-2: RDP Proxy (GUI)

In this exercise, you will configure RDP Proxy integration with the Unified Gateway. You will use the Configuration Utility to perform this exercise.

While the ITAdmins have full VPN connection privileges and access to all internal network resources. ITAdmins want to request access to RDP shortcuts using the NetScaler Gateway RDP Proxy configuration for frequently accessed resources. An initial pilot will grant access to a limited number of resources to the ITAdmins group only.

The following are requirements that must be met by the end of this exercise:

- Configure RDP Proxy client and server profiles that designate the NetScaler Gateway virtual server as the proxy.
- Ensure only the ITAdmins receive the proxy resources.

In this exercise, you will perform the following tasks:

- Configure RDP Proxy
- Test RDP Proxy

Configure RDP Proxy

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Create RDP Server Profile: • Navigate to **NetScaler Gateway > Policies > RDP**. • Click the **Server Profiles** tab. • Click **Add**. Configure RDP Server Profile settings: • Enter **rdpserver_prof_gateway** in the Name field. • Enter **172.21.10.150** in the RDP IP address field. • Verify **RDP** Port is **3389**. • Enter **Password1** in the Pre Shared Key field. Click **Create**.

3.	Create RDP Client Profile: • Click **Client Profiles** tab. • Click **Add**. Configure RDP Client Profile settings: • Enter **rdpclient_prof_gateway** in the Name field. • Scroll down and enter **gateway.training.lab** in the RDP Host field. • Enter **Password1** in the Pre Shared Key field. Click **Create**. **NOTE**: The Pre-shared key must match between the RDP Client and RDP Server profiles. The NetScaler Gateway will act as the RDP host when it proxies the connection.
4.	Create session profile for the RDP Proxy settings: • Navigate to **NetScaler Gateway > Policies > Session**. • Click **Session Profiles** tab. • Click **Add**.
5.	Configure the Session Profile with the following settings: • Enter **session_prof_rdpproxy** in the Name field. Client Experience: • Click the **Client Experience** tab. • Clientless Access: **ON**. (Override global: Enabled) Security: • Click the **Security** tab. • Default Authorization Action: **Allow** (Override global: Enabled) Published Applications: • Click the **Published Applications** tab. • ICA Proxy: **OFF** (Override global: Enabled) Remote Desktop: • Click the **Remote Desktop** tab. • RDP Client Profile Name: **rdpclient_prof_gateway** (Override global: Enabled) Click **Create**.
6.	Create a Session Policy for the RDP Proxy settings: • Click **Session Policies** tab. • Click **Add**. • Enter **session_pol_rdpproxy** in the Name field. • Select **session_prof_rdpproxy** in the Profile field. • Enter **ns_true** in the Expression field. Click **Create**.

7.	Create an RDP Bookmark: • Navigate to **NetScaler Gateway > Resources > Bookmarks**. • Click **Add**. • Enter **RDP AD02** in the Name field. • Enter **MGMT RDP AD02** in the Text to Display field. • Enter **rdp://ad02.training.lab** as the Bookmark • Enable (Check) **Use NetScaler Gateway as a Reverse Proxy**. • Click **Create**.
8.	Edit NetScaler Gateway VPN virtual server properties with the RDP Server settings: • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**. Update VPN Virtual Server basic settings with the RDP server details: • Click **Edit** (pencil icon) next to Basic Settings in the VPN virtual server properties. • Click **More** (below the IP Address Type field) to display the editable properties. • Select **rdpserver_prof_gateway** in the RDP Server Profile field. • Uncheck **ICA only**, if enabled. • Click **OK** to apply the changes to the Basic Settings. Click **Back** to exit the VPN virtual server properties.
9.	Bind the policy to the ITAdmins Group. Open the NetScaler Gateway Policy Manager: • Navigate to **NetScaler Gateway**. • Click **NetScaler Gateway Policy Manager** in the right-pane. • Click **"+"** next to AAA Groups to display the group list. Edit the ITAdmins group properties: • Select **ITAdmins** and click **Edit**. • Click **Session Policy** under the Policies category. • Click **Add Binding**. • Click **Click to Select** under Select Policy. • Select **session_pol_rdpproxy** and click **Select**. • Keep **Priority** at **110**. • Click **Bind**. • Click **Close** to close the Session Policy list. Keep the ITAdmins properties open.

10.	Bind an RDP Bookmark to the ITAdmins group: • Click **Bookmarks** under Advanced Settings to add the category to the configuration pane. • Click **URL** under Published Applications to edit the bindings. (This is the Bookmarks category.) • Click **Click to Select** under Select URL. • Select **RDP AD02** and click **Select**. • Click **Bind**. • Click **Done** to close the ITAdmins group properties. Click **OK** to close the AAA groups list. Click **Done** to close the NetScaler Gateway Policy Manager.
11.	Save the NetScaler configuration and confirm.

Test RDP Proxy

Step	Action
1.	Connect to ExternalClient using the RDP shortcut.
2.	Verify the local WordPad is running.
3.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **itadmin1** Password: **Password1**
4.	Click **Clientless Access** to connect using the Gateway proxy.
5.	Connect using the RDP proxy link to AD02.training.lab: • Click **MGMT RDP AD02**. • Click to open the **app.rdp** download in the browser downloads bar. • Click **Connect** in the Remote Desktop Connection security prompt. Expected Results: • The RDP connection should connect successfully. • Notice that the user was not prompted for credentials when establishing the connection. Existing session policies in the configuration enabled Single Sign On to Web Applications.
6.	Close the RDP Proxy session and log off the VPN: RDP Session for AD02.training.lab • Log off of the RDP session (instead of disconnecting). • Right-click **Start > Shut down or sign out > Sign out**. Log off NetScaler Gateway • Return to the NetScaler Gateway tab at https://gateway.training.lab and click **Log off**.

Key Takeaways:

- The RDP Proxy configuration allows the NetScaler Gateway VPN vServer to proxy RDP connections, such that the client to NetScaler communication is tunneled to the VPN vServer over SSL:443 while the NetScaler then proxies the RDP connection to the intended destination server on the internal network.
- RDP Proxy resources act as shortcuts to establish an RDP connection to specific backend components. These resources can be bound to the virtual server to specific AAA groups/users. Binding the resource to AAA groups, limits access to the RDP shortcuts to only the intended users.
- In order for the RDP Proxy connection to be supported the NetScaler Gateway VPN virtual server must not be restricted to ICA Proxy only connections and must be able to perform VPN connections as well.

Exercise 6-3: Portal Themes and Customizations (GUI)

In this exercise, you will configure custom Portal theme settings. You will use the Configuration Utility to perform this exercise.

The unified gateway simplifies customizing the NetScaler Gateway logon and portal pages to more closely match the StoreFront appearance. If additional customizations to the look-and-feel and style of the theme, a custom theme can be created and a GUI-based editor is provided for common web elements. This integrated portal theme editor should allow most environment to avoid having to directly modify the web content on the NetScaler manually.

In this exercise, you will perform the following tasks:

- Compare the Default, GreenBubble, and X1 themes.
- Create and configure a custom theme with a new background image.

Test Default Portal Themes and Configure Custom Theme Settings

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Change the NetScaler Gateway portal using the Unified Gateway wizard: • Navigate to **Integrate with Citrix Products > Unified Gateway**. • Click **STA**. Change Portal Theme: • Click **Edit** next to Portal Theme. • Select **X1** from the Portal Theme. • Click **Continue** to apply change to Portal Theme. • Click **Continue** under Applications to skip. Click **Done**.
3.	Connect to ExternalClient using the RDP shortcut.
4.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **itadmin1** Password: **Password1**

5.	Click **Network Access** to connect using the full VPN. Notice how the NetScaler Gateway appearance approximates the look-and-feel of the StoreFront 3.x appearance. (The GreenBubble theme matches the StoreFront 2.x appearance.)
6.	Log off the NetScaler Gateway. • Click itadmin1 and click **Log Off**.
7.	Return to the Student Desktop access the NetScaler configuration utility.
8.	Create a custom portal theme: • Navigate to **NetScaler Gateway > Portal Themes**. • Click **Add**. • Enter **Custom X1** in the Theme Name field. • Select **X1** in the Template theme field. Click **OK**. This will create a new theme based on the existing theme that can be customized.
9.	Customize a few of the portal them properties: • Scroll down to the Common Attributes section. • Select **Edit** under Background Image. • Click **Browse**. • Browse to C:\Resources\Portal Images\ and select an image to apply as the background image and click **Open**. Click **OK** to close the portal them attributes and return to the Portal Theme properties summary view.
10.	Update the Portal Theme: • Click **Click to bind and view configured theme** at top of page. • Verify **UG_VPN_ugw_gateway** vpn virtual server is select in the Name field. • Click **OK** and **Done.**
11.	Connect to ExternalClient using the RDP shortcut.
12.	Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **itadmin1** Password: **Password1**
13.	Click **Network Access** to connect using the full VPN. The custom portal theme is now displayed.
14.	Log off the NetScaler Gateway. • Click itadmin1 and click **Log Off**.
15.	Switch to the Student Desktop.

16.	Return the portal theme to the default theme: • Navigate to **Integrate with Citrix Products > Unified Gateway**. • Click **STA**. Change Portal Theme: • Click **Edit** next to Portal Theme. • Select **Default** from the Portal Theme. • Click **Continue** to apply change to Portal Theme. • Click **Continue** to skip Applications. Click **Done** to exit the Unified Gateway configuration tool.
17.	Save the NetScaler configuration and confirm.

Key Takeaways:

- NetScaler 12.0 has improved the ability to make changes to the look-and-feel by integrating default and custom themes and by allowing GUI-based configuration of basic appearance settings.
- The NetScaler VPN logon page can be adjusted to more closely resemble the look and feel of StoreFront. The GreenBubbles theme corresponds to StoreFront 2.x deployments (and 3.x deployments running in classic mode). The X1 them corresponds to StoreFront 3.x deployments.
- Custom themes can be created from any of the default themes making it easier for an administrator to modify just the settings they are interested while still preserving the overall look and feel of the original themes where desired.

Exercise 6-4 Customize Header and Footer (GUI)

In this exercise, you will configure custom Portal theme settings. You will use the Configuration Utility to perform this exercise.

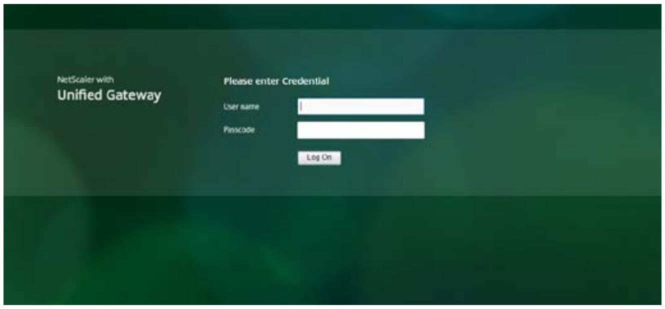
The unified gateway simplifies customizing the NetScaler Gateway logon and portal pages, We can customize the entire page to ensure we provide all the necessary information to users on the Logon page itself.

In this exercise you will perform following tasks.

- Customize Footer for Green bubble theme using rewrite policies.

Configure Custom Green Bubble theme with Footer Customization.

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Create a custom portal theme: • Navigate to **NetScaler Gateway > Portal Themes**. • Click **Add**. • Enter **Custom Green Bubble** in the Theme Name field. • Select **Green Bubble** in the Template theme field. Click **OK**. This will create a new theme based on the existing theme that can be customized.
3.	Create Custom Login Page Click on Login page • Enter **Please enter credential** under Form Title. • Enter **Passcode** under Password Field Title. • Click OK and Done
4.	Update the Portal Theme: • Click on NetScaler Gateway • Select UG_VPN_ugw_gateway under Virtual servers and click Edit • Edit Portal Theme and Select Custom Green Bubble under the drop down. • Click OK and Done

5.	Connect to ExternalClient using the RDP shortcut. Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **itadmin1** Password: **Password1**
6.	Click **Network Access** to connect using the full VPN. The custom portal theme is now displayed.
7.	We can Customize the Footer and Header of NetScaler Gateway page to add necessary information.  NetScaler with Unified Gateway Please enter Credential User name Passcode Log On

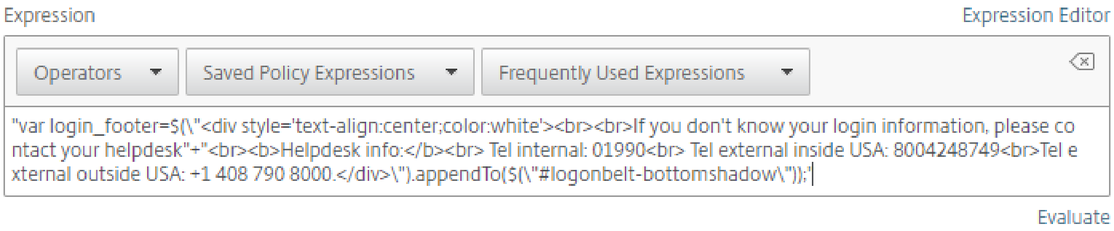
8. Create Rewrite Policy for Footer Customization.

- Click on **Appexpert** and Navigate to Rewrite .
- Select **Rewrite Polices** and Click **Add**.
- Enter **rw_pol_insert_belowloginbtn** under Name.

- Add **HTTP.REQ.URL.CONTAINS("gateway_login_form_view.js")** under Expression.

Configure Action

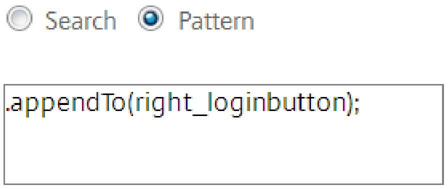
- Click + at Action
- Enter **rw_act_insert_belowloginbtn** under Name.
- Select **INSERT_AFTER_ALL** under Type
- Enter **HTTP.RES.BODY(120000).SET_TEXT_MODE(IGNORECASE)** under Expression to Choose target location.
- Enter **"var login_footer=$(\"<div style='text-align:center;color:white'><br><br>If you don't know your login information, please contact your helpdesk"+"<br><b>Helpdesk info:</b><br> Tel internal: 01990<br> Tel external inside USA: 8004248749<br>Tel external outside USA: +1 408 790 8000.</div>\").appendTo($(\"#logonbelt-bottomshadow\"));"** under Expression.



```
"var login_footer=$(\"<div style='text-align:center;color:white'><br><br>If you don't know your login information, please co
ntact your helpdesk"+"<br><b>Helpdesk info:</b><br> Tel internal: 01990<br> Tel external inside USA: 8004248749<br>Tel e
xternal outside USA: +1 408 790 8000.</div>\").appendTo($(\"#logonbelt-bottomshadow\"));'
```

Note: Ensure that you are entering the expression as it displayed in the screenshot.

- Select **Pattern** and Enter .appendTo(right_loginbutton);


○ Search ● Pattern

```
.appendTo(right_loginbutton);
```

- Click Create twice to close the Policy .

9. Apply the rewrite to NetScaler Gateway.

- Navigate to NetScaler Gateway>Virtual Servers> UG_VPN_ugw_gateway and Click Edit.

- Click + on Policies and Select **Rewrite** and **Response** from Dropdowns , Click Continue.
- Click Click to select and choose rw_pol_insert_belowloginbtn
- Click Bind and Done

10

Connect to ExternalClient using the RDP shortcut.

Connect to the Unified Gateway at https://gateway.training.lab.

Log into the Unified Gateway VPN portal page using the following credentials:

User Name: **itadmin1**
Password: **Password1**

Note: The change might not take effect straightaway since Apache server might send 304 (Not modified), instead of a 200 OK to the client for this file and hence the rewrite action would not take effect. If that happens, then edit the **vpn/gateway_login_view.js file**. You need not make any changes, just adding a space anywhere in the file and saving it would do the trick.

Make sure to clean all the cached objects on the browser and on the NetScaler under Integrated Caching when switching from one theme to another.

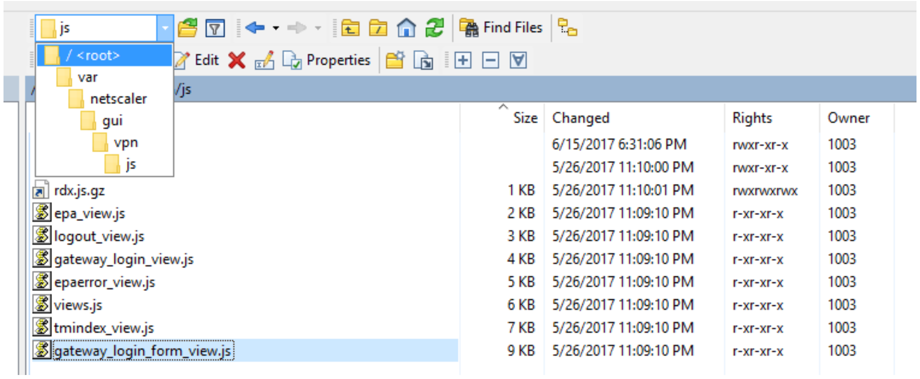
11.

Make changes to gateway_login_view.js file.

Open Winscp utility from Student Desktop and connect to NS_VPX_01

User Name: nsroot
Password: nsroot

Navigate to **var/netscaler/gui/vpn/js** and select **gateway_login_from_view.js**



	Size	Changed	Rights	Owner
		6/15/2017 6:31:06 PM	rwxr-xr-x	1003
		5/26/2017 11:10:00 PM	rwxr-xr-x	1003
rdx.js.gz	1 KB	5/26/2017 11:10:01 PM	rwxrwxrwx	1003
epa_view.js	2 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003
logout_view.js	3 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003
gateway_login_view.js	4 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003
epaerror_view.js	5 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003
views.js	6 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003
tmindex_view.js	7 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003
gateway_login_form_view.js	9 KB	5/26/2017 11:09:10 PM	r-xr-xr-x	1003

Open **gateway_login_from_view.js** add space at the end of first line and hit save.
Enter **nsroot** when prompted for password.

Close the Editior and end the Winscp session.

Note: Don’t make any changes to **gateway_login_from_view.js** file apart from adding space at the end of the first line , Making any changes part from that may corrupt the file.

12.	Connect to ExternalClient using the RDP shortcut. Connect to the Unified Gateway at https://gateway.training.lab. Log into the Unified Gateway VPN portal page using the following credentials: User Name: **itadmin1** Password: **Password1** We can see the customized information at the footer of NetScaler Gateway login page. Note : Make sure all the browser cache is cleared.

Key Takeaways:

- NetScaler 12.0 has improved the ability to make changes to the look-and-feel of the NetScaler gateway login Page.
- With use of responder and rewrite policies we can make granular changes to NetScaler gateway Login page and can ensure all the necessary information is delivered on the Login page itself.

Exercise 6-5: Apply an End User License Agreement (GUI)

In this exercise, you will configure a custom End User License Agreement for integration with the NetScaler Gateway. You will use the Configuration Utility to perform this exercise.

Some environment require users explicitly accept and agree to specific terms and conditions prior to accessing corporate resources using the NetScaler Gateway. In the past, integrating a EULA would require manually customizing the NetScaler Gateway logon page to implement this type of functionality. NetScaler 12 allows administrators to import a predefined EULA message in HTML format and link it to a NetScaler Gateway VPN virtual server. The EULA is then presented to users as an option that users must agree to prior to being allowed to attempt authentication to the NetScaler VPN virtual server. Users can also view the content of the EULA prior to accepting it.

You will integrate the predefined EULA text with the existing VPN virtual server and enable the EULA requirement.

In this exercise, you will perform the following tasks:

- Configure and Test Custom EULA integration

Configure and Test Custom EULA Integration

Step	Action
1.	Connect to the NetScaler configuration utility for the HA Pair using the NSMGMT SNIP at http://192.168.10.103. Log into the utility using the following credentials: User Name: **nsroot** Password: **nsroot**
2.	Open the custom EULA file on the Student Desktop: • Browse to **C:\Resources\Portal Images** and open the **Eula.txt**. • Copy the contents of EULA.txt to the clipboard.
3.	Create a custom EULA agreement: • Navigate to **NetScaler Gateway > Resources > EULA**. • Click **Add**. • Enter **custom_eula** in the Name field. • Paste the contents from the Eula.txt file (C:\resources\Portal Images\) to the End User License Agreement in English field. • Click **Create**.

4.	Configure the EULA to display with the Unified Gateway: • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**. • Click **EULA** under Advanced Settings in the right-pane. • Click **EULA** under the EULA category. • Click **Click to Select** under Select EULA. • Select **custom_eula** and click **Select**. • Click **Bind**. Click **Done**.
5.	Connect to ExternalClient using the RDP shortcut.
6.	Connect to the Unified Gateway at https://gateway.training.lab. Notice the "I accept Terms and Conditions" checkbox is displayed and the agreement must be accepted before logging on to the NetScaler Gateway. Click **Terms and Conditions** to view the EULA. • Click **Back** to exit the EULA.
7.	Return to the Student Desktop.
8.	Unbind the EULA form the Unified Gateway VPN Virtual Server: • Navigate to **NetScaler Gateway > Virtual Servers**. • Select **UG_VPN_ugw_gateway** and click **Edit**. • Click **EULA** under the EULA category. • Select **custom_eula** and click **Unbind**. • Click **Yes** to confirm. • Click **Close** to close the EULA properties. Click **Done**.
9.	Save the NetScaler configuration and confirm.

Note: Please Shutdown the Exchange Server before starting new Module.

Key Takeaways:

- Previously, incorporating a custom EULA with a terms and conditions acceptance requirement would have required manual customizations to the NetScaler VPN virtual server portal pages. Now the customization is easy to integrate or remove as part of the NetScaler Gateway configuration.