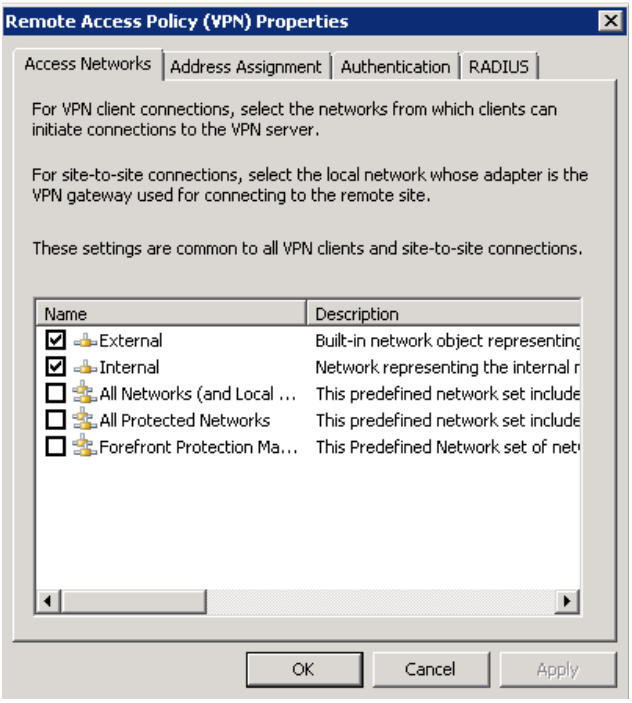
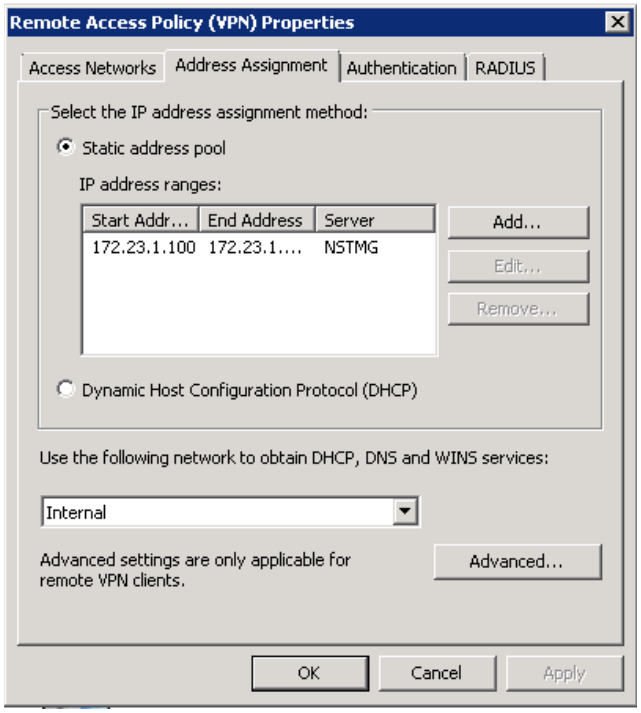
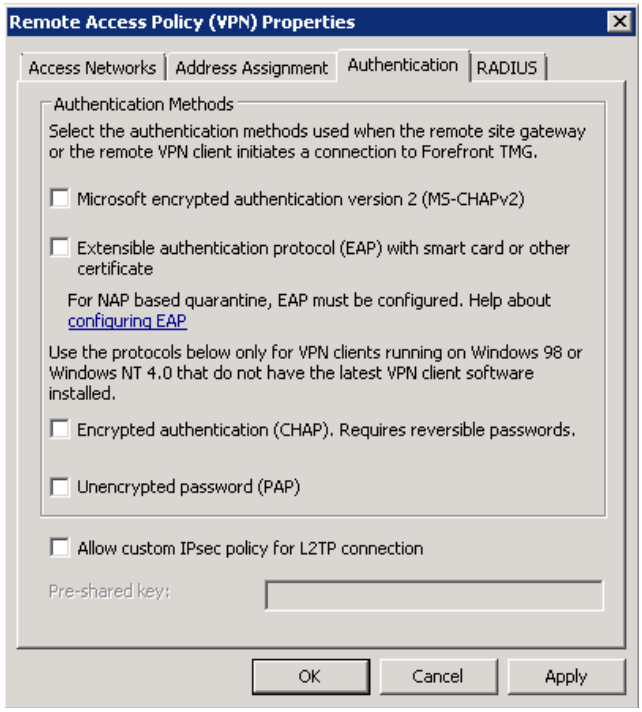
Here, select **Configure VPN Properties**.



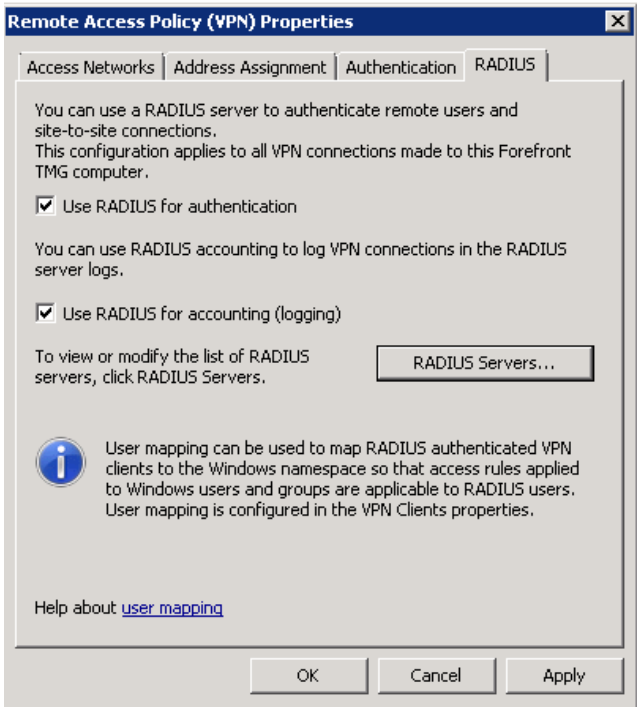
In the window that pops up, select the **Address Assignments** tab. You will see what appears in the figure below. Choose the **Dynamic Host Configuration Protocols (DHCP)** option or the **Static Address Pool** option. Be sure that the addresses you put in the pool are not part of any other network definition or the setup will fail and you will see an error in the Alerts section of the TMG console.



Click the **Authentication** tab to choose how the client will authenticate to the **TMG server**.



Also, you can use a RADIUS server to perform authentication by clicking the **RADIUS** tab; here, the list of RADIUS servers used is the same as the list created during configuration of user authentication to applications using a listener.

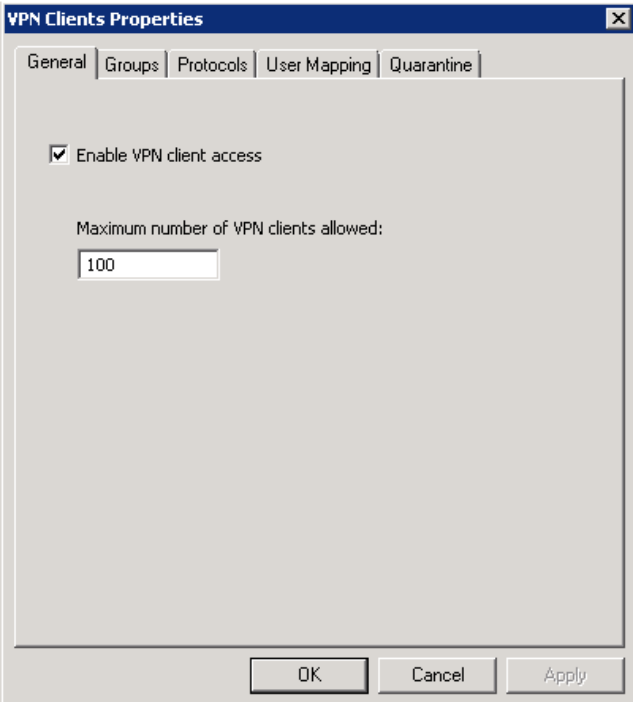


Click **Ok** to complete VPN configuration on TMG.

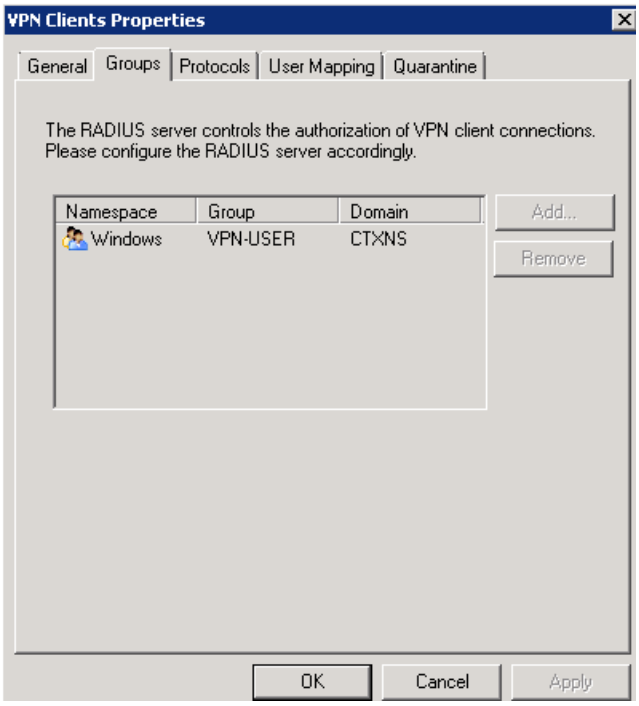
Enable VPN access

Click the **Enable VPN Client Access** link in the **Task** tab of the Task Pane in TMG. This page also presents various other relevant VPN options.

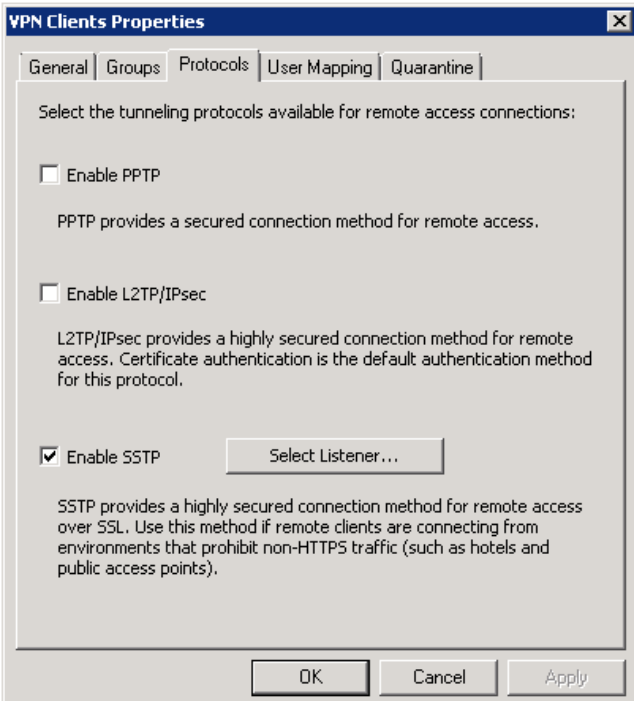
To enable VPN access, click **Configure VPN Client Access**. Here, in the **General** tab, you can disable or enable VPN client access and specify the number of connections and other relevant settings.



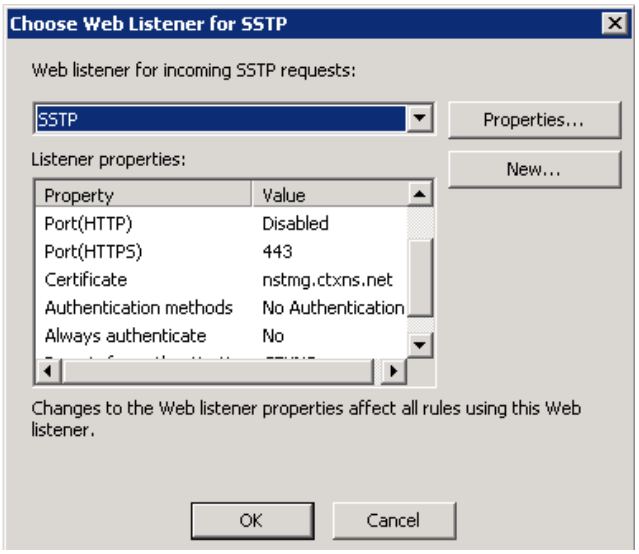
In the **Groups** tab, you can define the Active Directory or local groups that are allowed to connect using VPN.



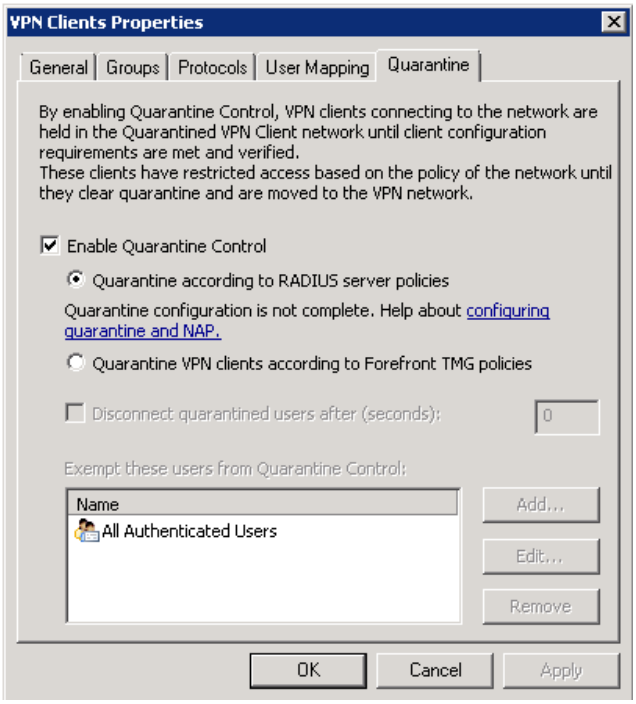
In the **Protocols** tab, you can define the various protocols to be made available for VPN access. For this use case, we are setting up SSTP, so we will choose the **SSTP** option. For the SSTP proxy, you will be required to choose an appropriate listener.



In the **Choose Web Listener for SSTP** dialog box, you will see a list of potential web listeners that can be used for SSTP connections. As there are no SSL-enabled listeners on this TMG firewall yet, we will have to create one. To begin doing so, click on the **New** button. This will take you back to the **New Web Listener Wizard**, which will lead you through the creation of an SSTP listener.



The **Quarantine** tab lets you configure TMG to place VPN remote access clients in quarantine using the remote access quarantine service (RQS) and remote access quarantine client (RQC). Quarantine control provides phased network access for remote clients by restricting them to a quarantine mode before allowing them to access the network.



The two options available here are:

- **Quarantine according to RADIUS server policies.** When a VPN client attempts to connect, routing and remote access policy determines whether the connection request is passed to Forefront TMG. After compliance with policy has been verified, the client joins the VPN clients' network.
- **Quarantine VPN clients according to Forefront TMG policies.** When a VPN client attempts to connect to the Forefront TMG computer, routing and remote access unconditionally passes the request to Forefront TMG. Forefront TMG places the connecting client in the quarantined VPN clients' network, subjecting the client to the firewall policy defined for that network. When the client clears quarantine, it moves into the VPN clients' network. When you select this option, you must disable the routing and remote access quarantine feature so the VPN connection can be established.

When you select the second option, you must configure quarantine control on the Forefront TMG computer, and on the remote VPN clients that are attempting to connect to the corporate network. Otherwise, remote VPN clients will remain in quarantine mode until the specified time passes and they are disconnected from Forefront TMG.

Part 2: Configuring secure VPN access on NetScaler

To configure SSL VPN access on NetScaler VPX, you must complete the actions below. –

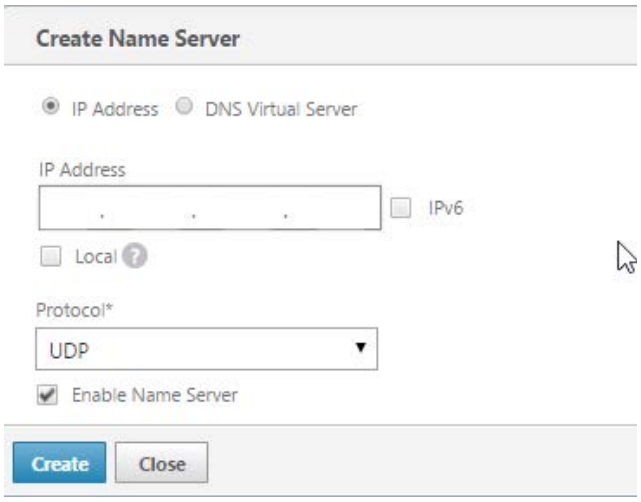
Note: This process requires installation of SSL certificates for the VPN server along with the necessary authentication profile configuration that will be used to authenticate users for the VPN setup. For more information on this process, check the requirements section at http://support.citrix.com/article/CTX127044

Enabling the SSL VPN feature

To enable SSL VPN, navigate to **System>Settings>Configure Basic Features** and enable NetScaler Gateway, if it is not enabled already.

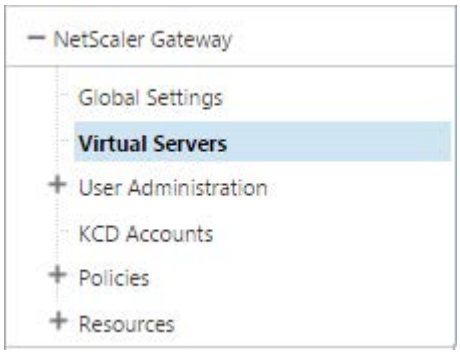
Create entries for DNS name servers

Navigate to the name server definition node at **Traffic Management>DNS>Name Servers**. If your name server is not listed here, add it to the existing list, if any.

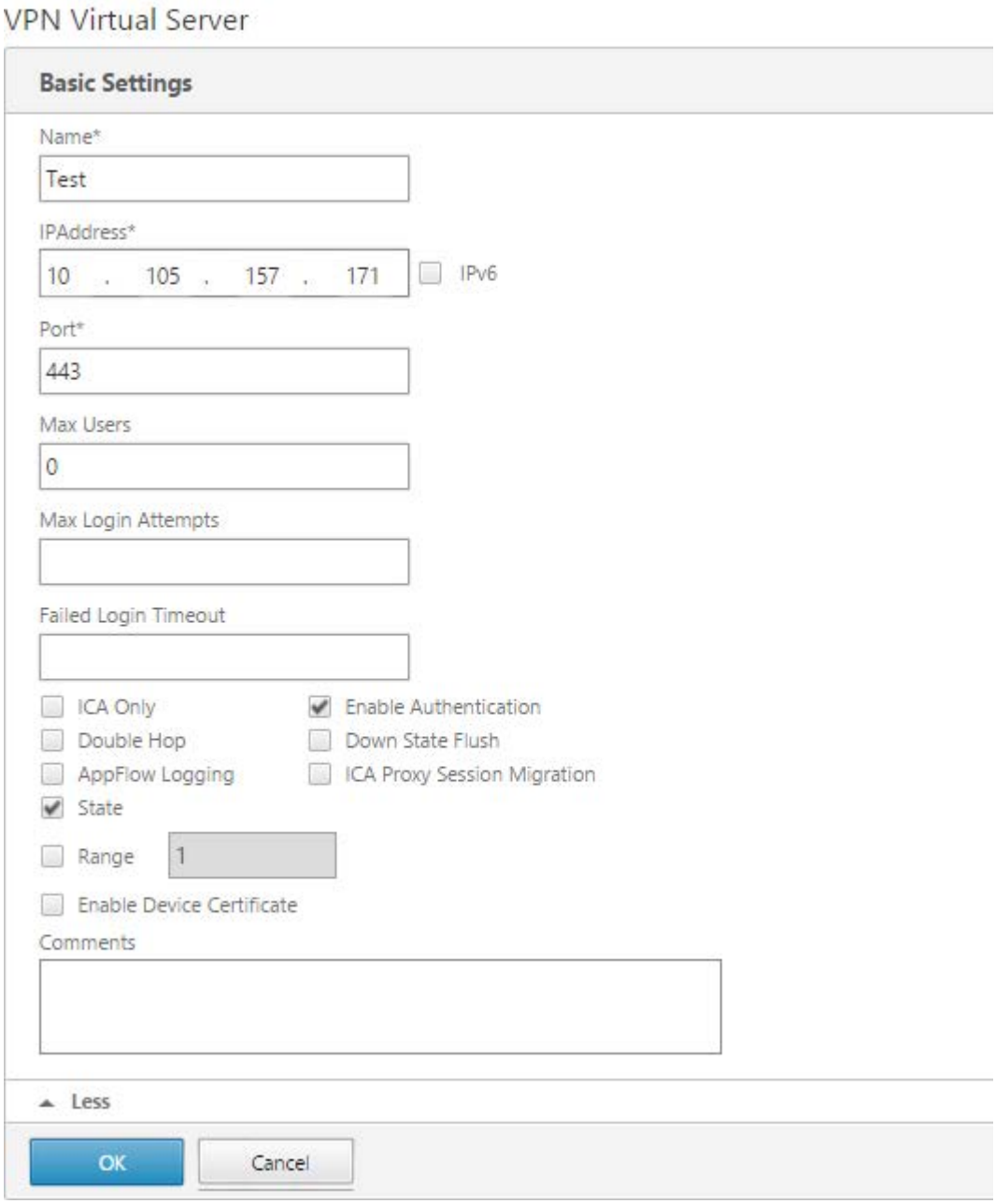


Create an SSL VPN virtual server

After enabling NetScaler Gateway, navigate to **NetScaler Gateway>Virtual Servers** and click **Add** above the list of servers shown to the right of the navigation menu.

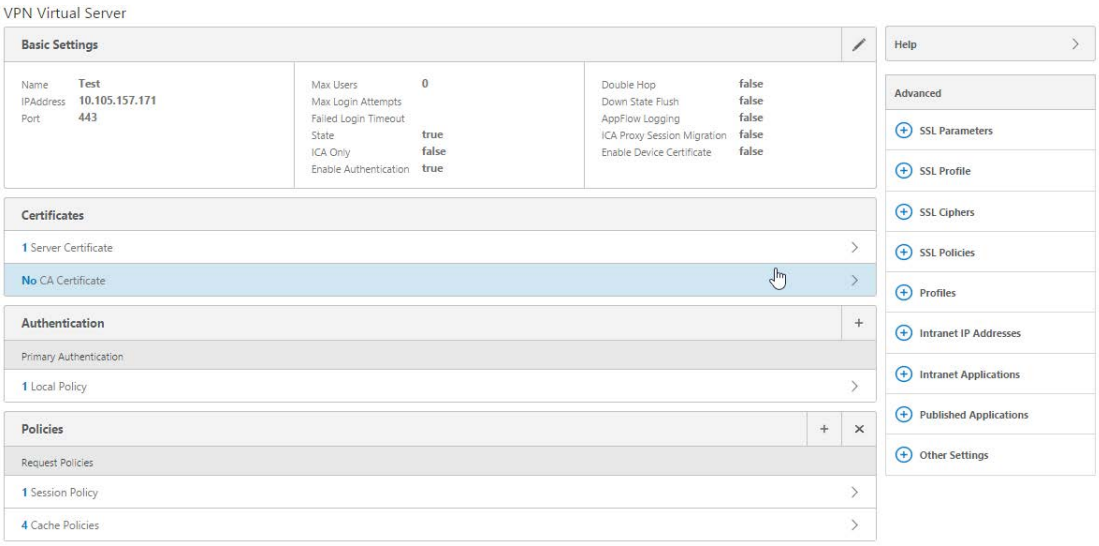


The screen that is presented allows you to configure the new virtual server.



Here, you can specify the name, IP address and port (443 for an SSL virtual server). You can also define the maximum number of users the VPN server will support, as with TMG. If you click **More**, you will be presented with additional settings as shown in the screen above.

Complete configuration per your requirements and click **OK**.

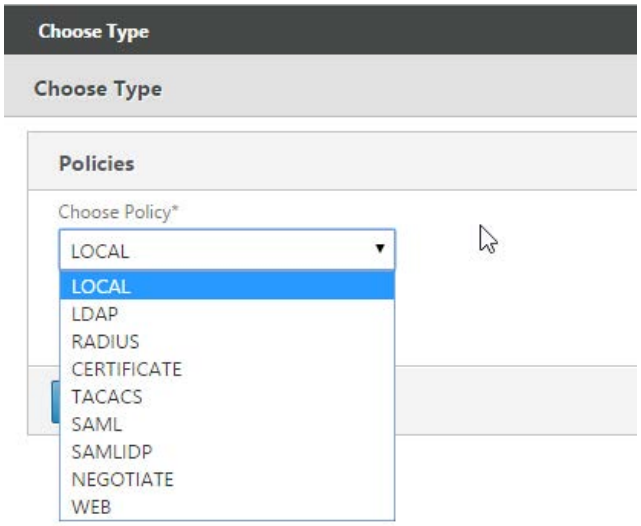


Here, bind the server certificate (listed as a prerequisite).

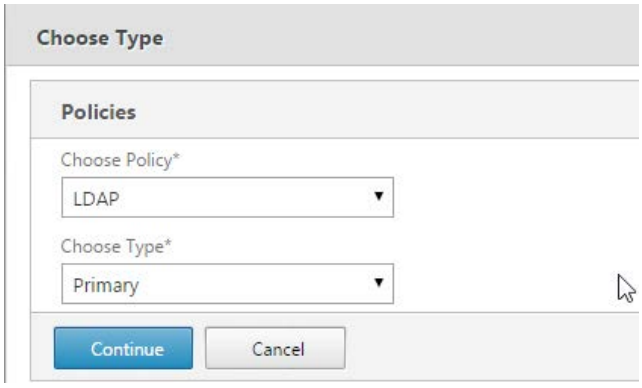
Binding the authentication policy to the VPN virtual server

After binding the server certificate, the next step is to bind the authentication policy that this VPN virtual server will use. To do this, click on the **+** icon next to the Authentication header as shown in the screenshot above. If the Authentication panel is not seen, look for the Authentication option in the panel to the right of the main settings area and click on it to see it in the main settings area.

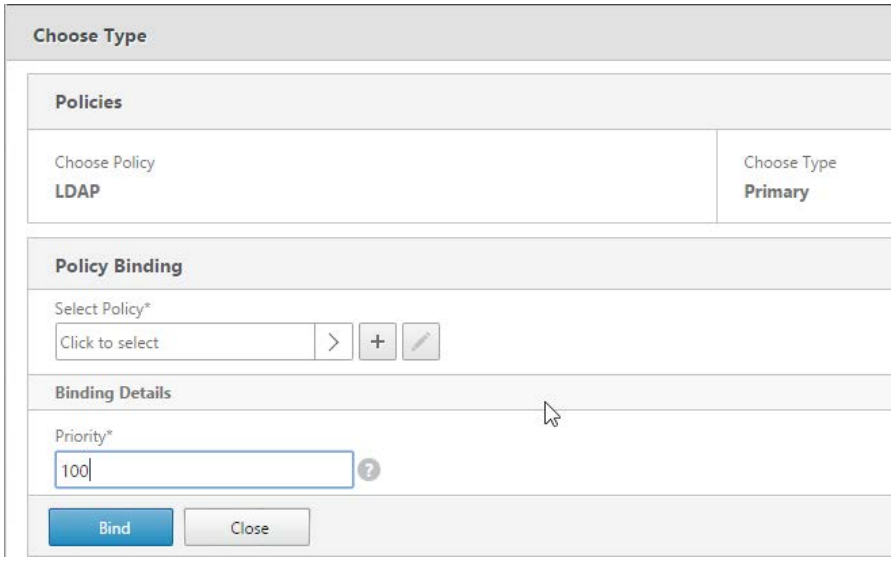
After you click**+**, the screen below is presented –



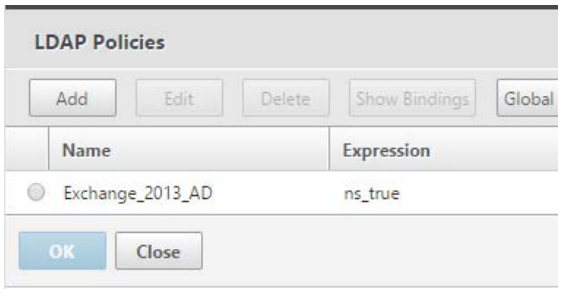
This screen shows the available policy options for configuring authentication on the VPN vserver. You may also classify them as primary or secondary (for two-factor authentication) as shown below.



Upon clicking **next**, you will be provided with an option to add an existing policy or create a new one. After you click **Continue**, the screen below is shown (when LDAP is selected in the **Choose Policy** drop down above).



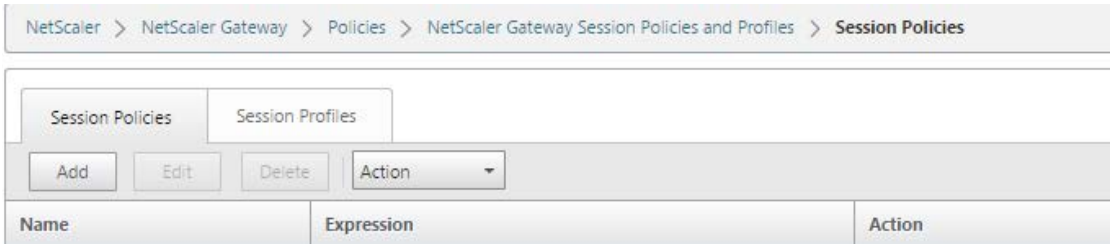
The next screen allows you to add/use an existing policy. This screen is reached by clicking on the **Click to select** option under **Select Policy** shown above.



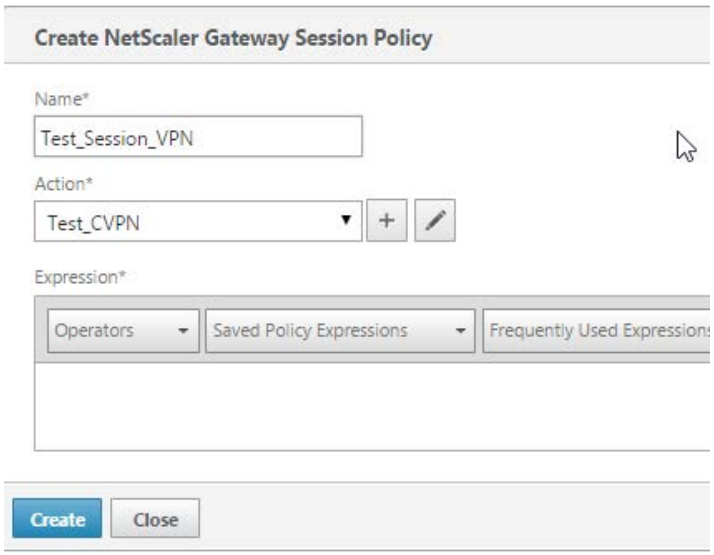
Select the appropriate policy or add a new one by clicking **Add** above, then click **OK** to bind it to the VPN vserver.

Create the session policy for the VPN virtual server

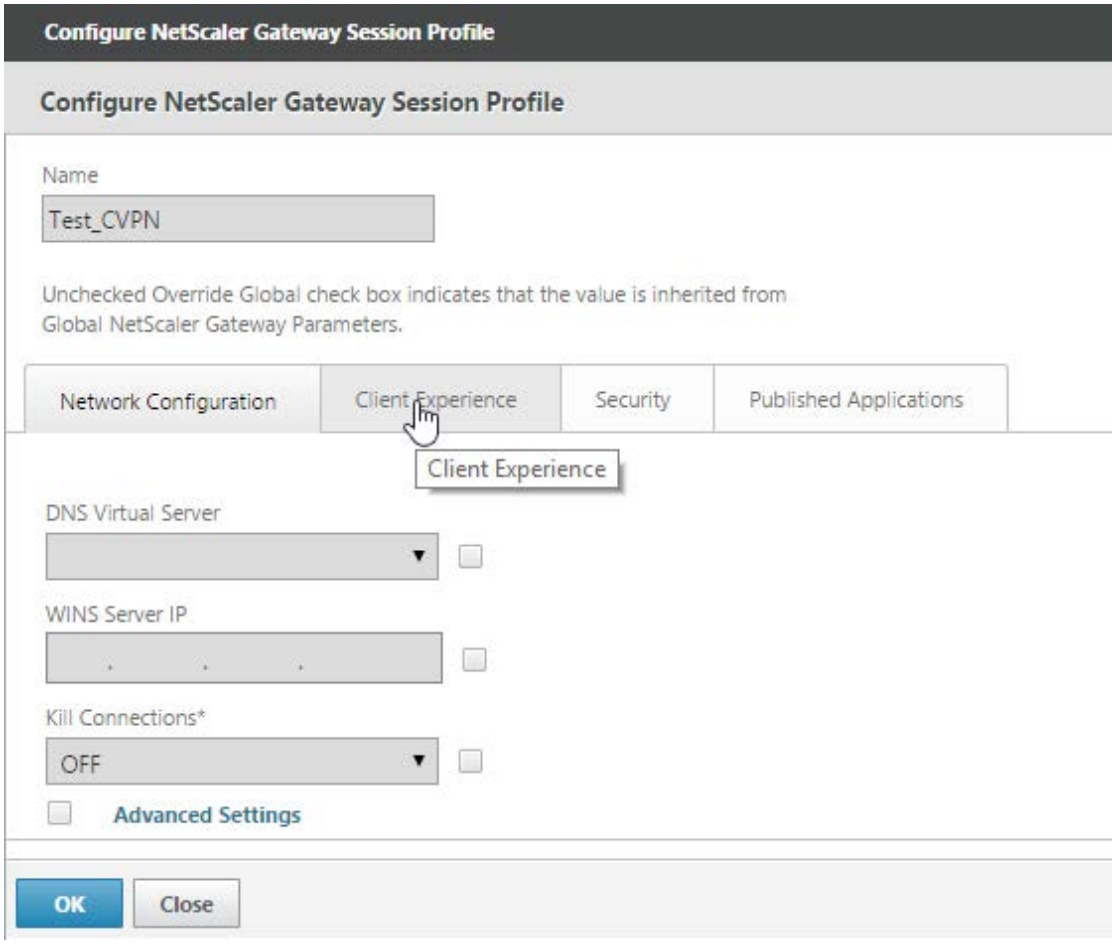
Navigate to **NetScaler Gateway>Policies>Session** and click **Add** to create a new session policy when presented with the Session Policies screen.



Note: For each component you configure in the Configure Session Profile dialog box, ensure that you select the **Override Global** option for the respective component.



Give an appropriate name to the policy, then click on the pencil-shaped icon (to edit an existing action) or the plus button (to add a new one) to define the session profile for this policy.

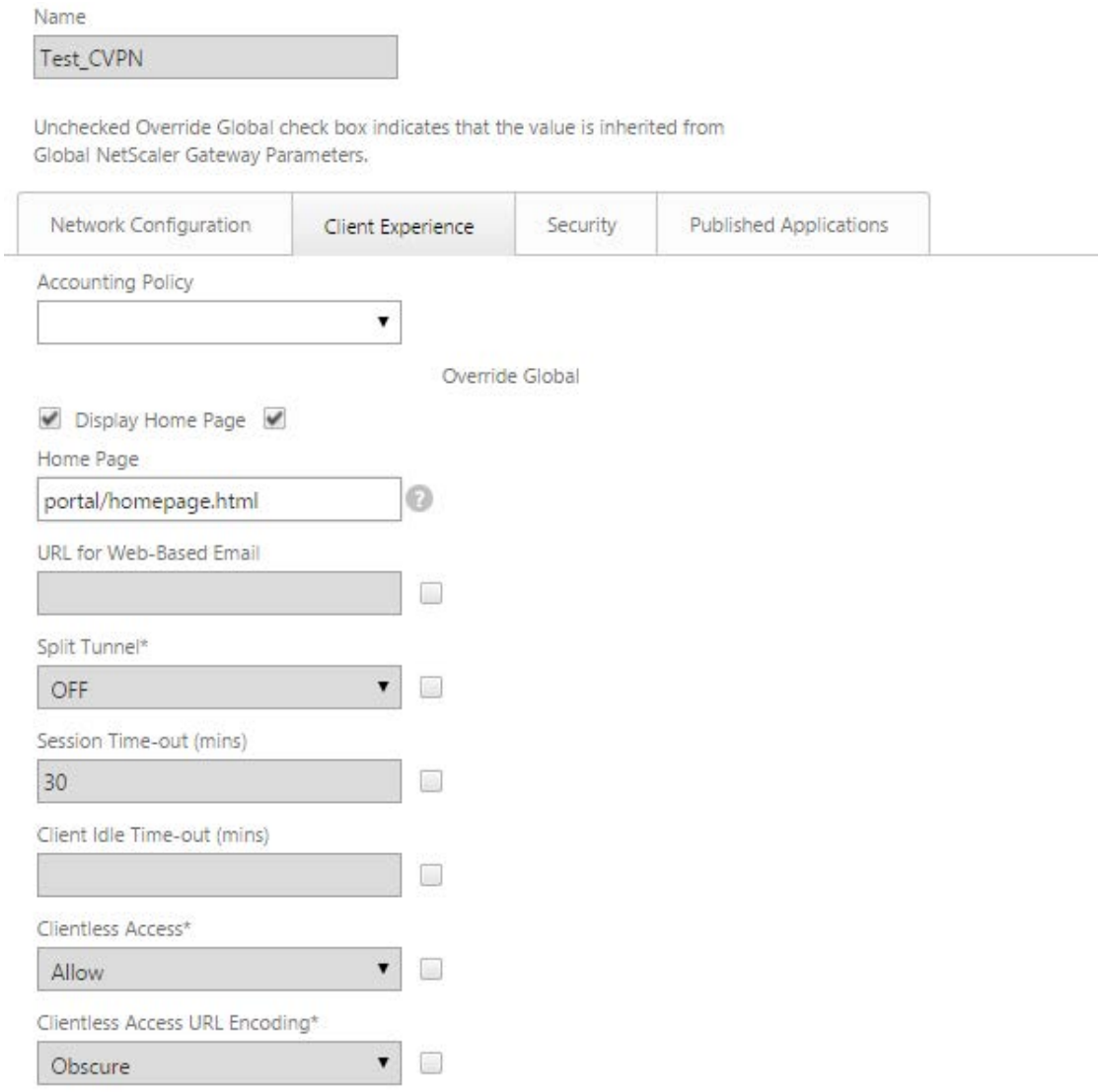


First, move to the **Client Experience** tab after ensuring the **Network Configuration** (DNS nameserver, etc.) is configured properly. To change the settings in the Network Configuration tab, check the box next to each setting (this will override the globally set values) and provide the appropriate values.

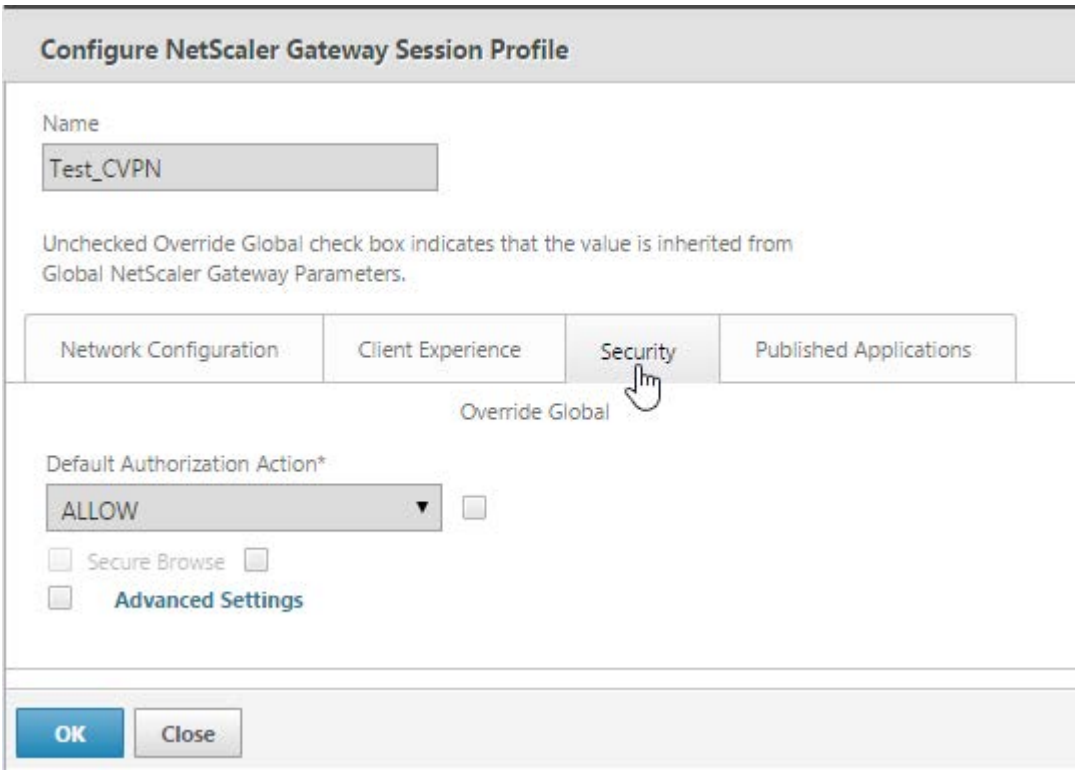
On the **Client Experience** tab, make the following changes: (to set these values, enable the check box next to the setting as described earlier)

- Type the intranet portal URL in the Home Page field.
- Ensure **OFF** is selected in the Split Tunnel list.
- Select **OFF** in the Clientless Access list (or allow this if appropriate for your environment)
- Ensure that Windows/Mac OS X is selected from the **Plug-in Type** list.
- Select the **Single Sign-on to Web Applications** option.
- Ensure that the **Client Cleanup Prompt** option is selected}

You can also define the credential to be used (primary/secondary) and add a KCD account for SSO if necessary. Most of these values are inherited globally, and may not need configuration. A partial snapshot of the page is shown below: all the settings above can be found on this page.

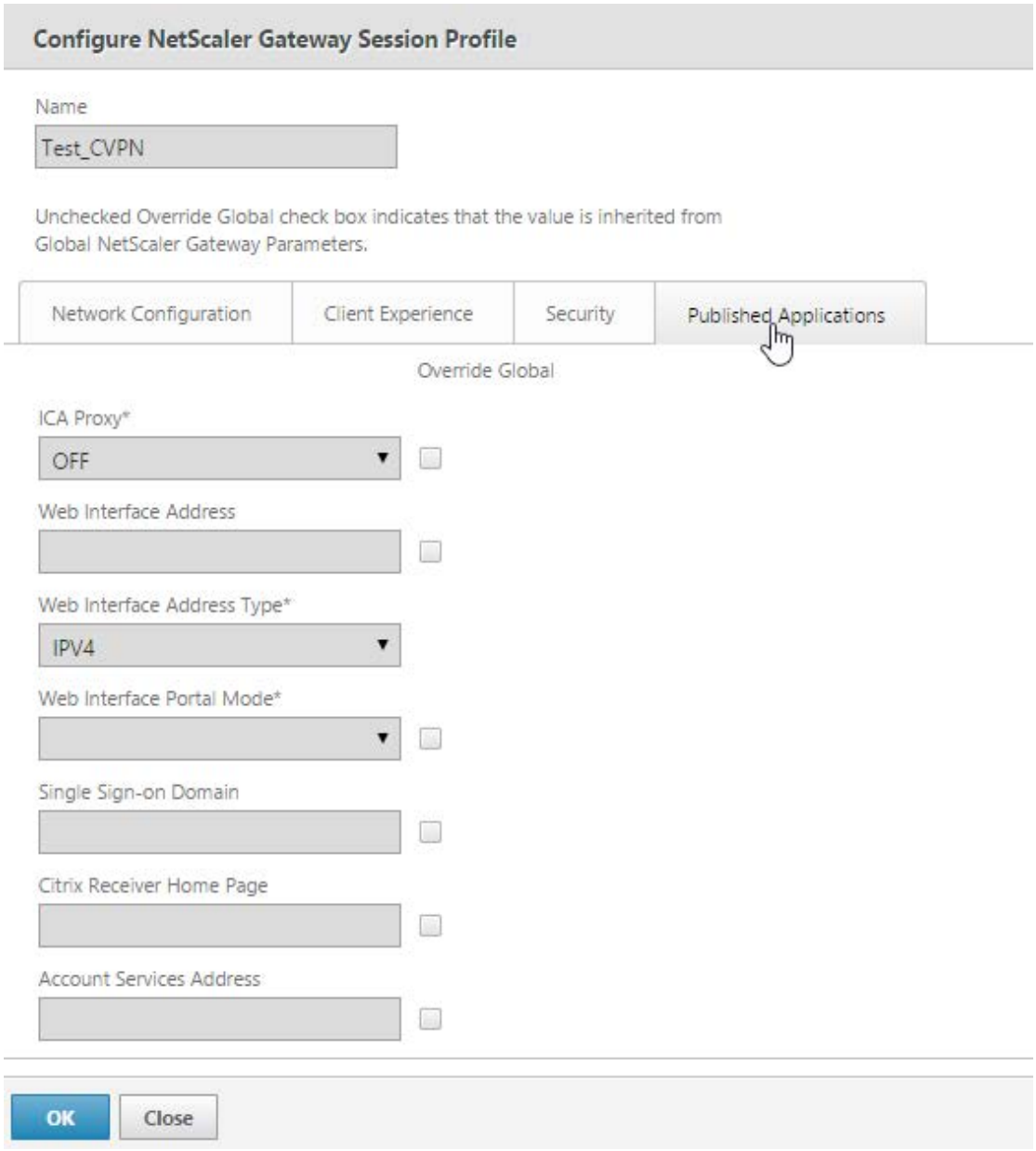


Now, activate the **Security** tab.

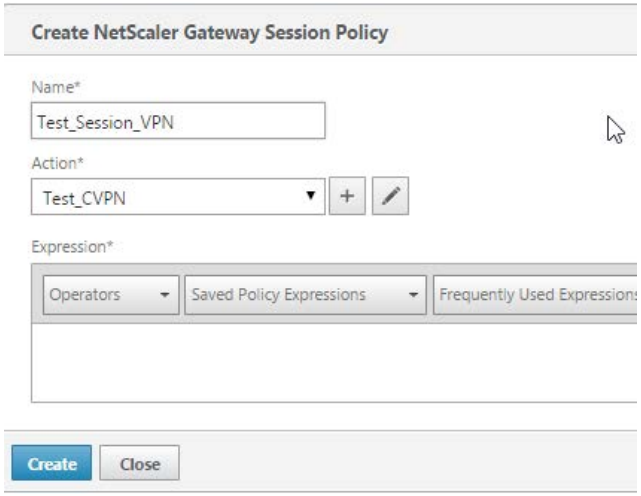


Ensure that **ALLOW** is selected in the default authorization list.

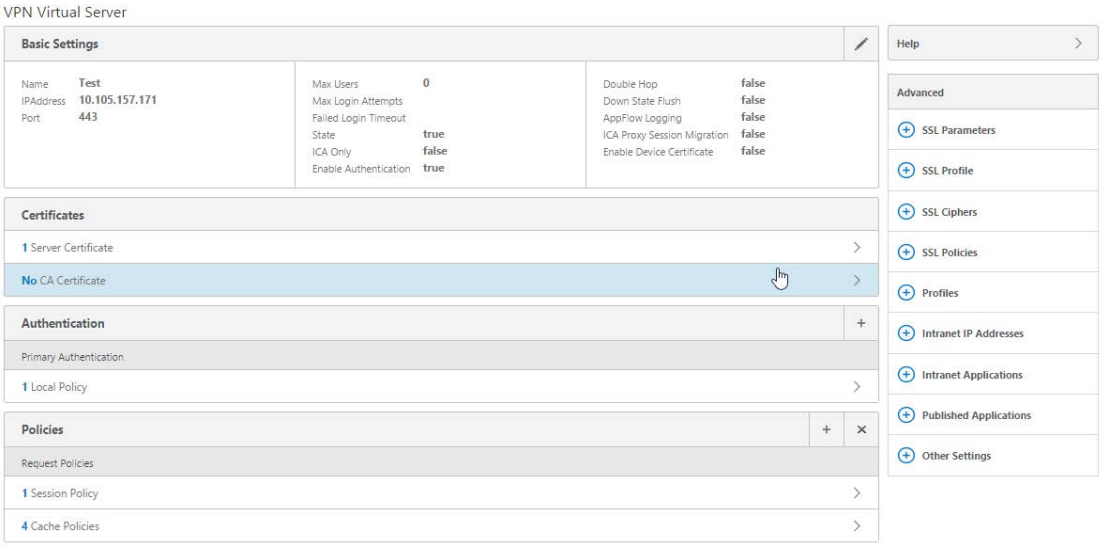
Now, activate the **Published Applications** tab.


Configure NetScaler Gateway Session Profile
Name
Test_CVPN
Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.
Network Configuration
Client Experience
Security
Published Applications
Override Global
ICA Proxy*
OFF
Web Interface Address
Web Interface Address Type*
IPV4
Web Interface Portal Mode*
Single Sign-on Domain
Citrix Receiver Home Page
Account Services Address
OK
Close

Ensure that OFF is selected under the options for ICA Proxy. Click **OK**. In the screen now presented for the Session Policy, put **ns_true** as the expression and click **Create**.



Now bind the session policy to the VPN server created earlier in the **Policies** section on the **Basic Settings** screen shown below:



Conclusion

NetScaler provides a complete replacement of Microsoft Forefront TMG for organizations that want to securely host multiple, load balanced services over a secure SSL VPN connection. NetScaler offers comprehensive SSL VPN capability for enterprise users and a wide range of authentication options.

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

CITRIX®

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

Copyright © 2015 Citrix Systems, Inc. All rights reserved. Citrix, NetScaler, NetScaler VPX and NetScaler Gateway are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.