SSL VPN
Deployment Guide

A Step-by-Step Technical Guide

Notice:

The information in this publication is subject to change without notice.

THIS PUBLICATION IS PROVIDED “AS IS” WITHOUT WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. CITRIX SYSTEMS, INC. (“CITRIX”), SHALL NOT BE LIABLE FOR TECHNICAL OR EDITORIAL ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR DIRECT, INCIDENTAL, CONSEQUENTIAL OR ANY OTHER DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION, EVEN IF CITRIX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

The exclusive warranty for Citrix products, if any, is stated in the product documentation accompanying such products. Citrix does not warrant products other than its own.

Table of Contents

Introduction 4

Solution Requirements....5

Prerequisites....5

Network Diagram 6

First time connectivity 7

- Serial Connection 7
- Ethernet Connection....7

NetScaler Configuration....8

- Deployment Model: Netscaler High Availability, Two-Arm Mode, SSL VPN 8
- Important Considerations for NetScaler High Availability....9
- High Availability Command Synchronization 12
- Important NetScaler IP Addresses 13
- IP Addresses, Interfaces and VLANs....14

SSL Keys & Certificates 16

- Obtaining Keys and Certificates 16
- Using the SSL Certificate Wizard 16

SSL VPN Configuration 20

- SSL VPN Wizard....20

Accessing the SSL VPN 23

- Importing SSL Certificates 23
- Testing the SSL VPN....23

Things you need to know 25

SSL VPN Polices 26

- Step-by-Step SSL VPN policy creation 27

Appendix A - NetScaler Application Switch Configuration....32

Introduction

Citrix® NetScaler® optimizes the delivery of web applications— increasing security and improving performance and Web server capacity. This approach ensures the best total cost of ownership (TCO), security, availability, and performance for Web applications. The Citrix NetScaler solution is a comprehensive network system that combines high-speed load balancing and content switching with state-of-the-art application acceleration, layer 4-7 traffic management, data compression, dynamic content caching, SSL acceleration, network optimization, and robust application security into a single, tightly integrated solution. Deployed in front of application servers, the system significantly reduces processing overhead on application and database servers, reducing hardware and bandwidth costs.

Citrix Access Gateway™ is the only SSL VPN to securely deliver any application with policy-based SmartAccess control. Users will have easy-to-use secure access to all of the enterprise applications and data they need to be productive and IT can cost effectively extend access to applications while maintaining security through SmartAccess application-level policies. With Access Gateway organizations are empowered to cost effectively meet the anywhere access demands of all workers – enabling flexible work options, easier outsourcing and non-employee access, and business continuity readiness – while ensuring the highest-level of information security.

This deployment guide walks through the step-by-step configuration details of how to configure the Citrix NetScaler for use as a SSL VPN gateway.

Solution Requirements

- SSL VPN for all applications
- Agentless connectivity, and Agent based connectivity
- Split-Tunneling without network conflicts
- User/Group Restrictions to specific VLANs and IP Addresses

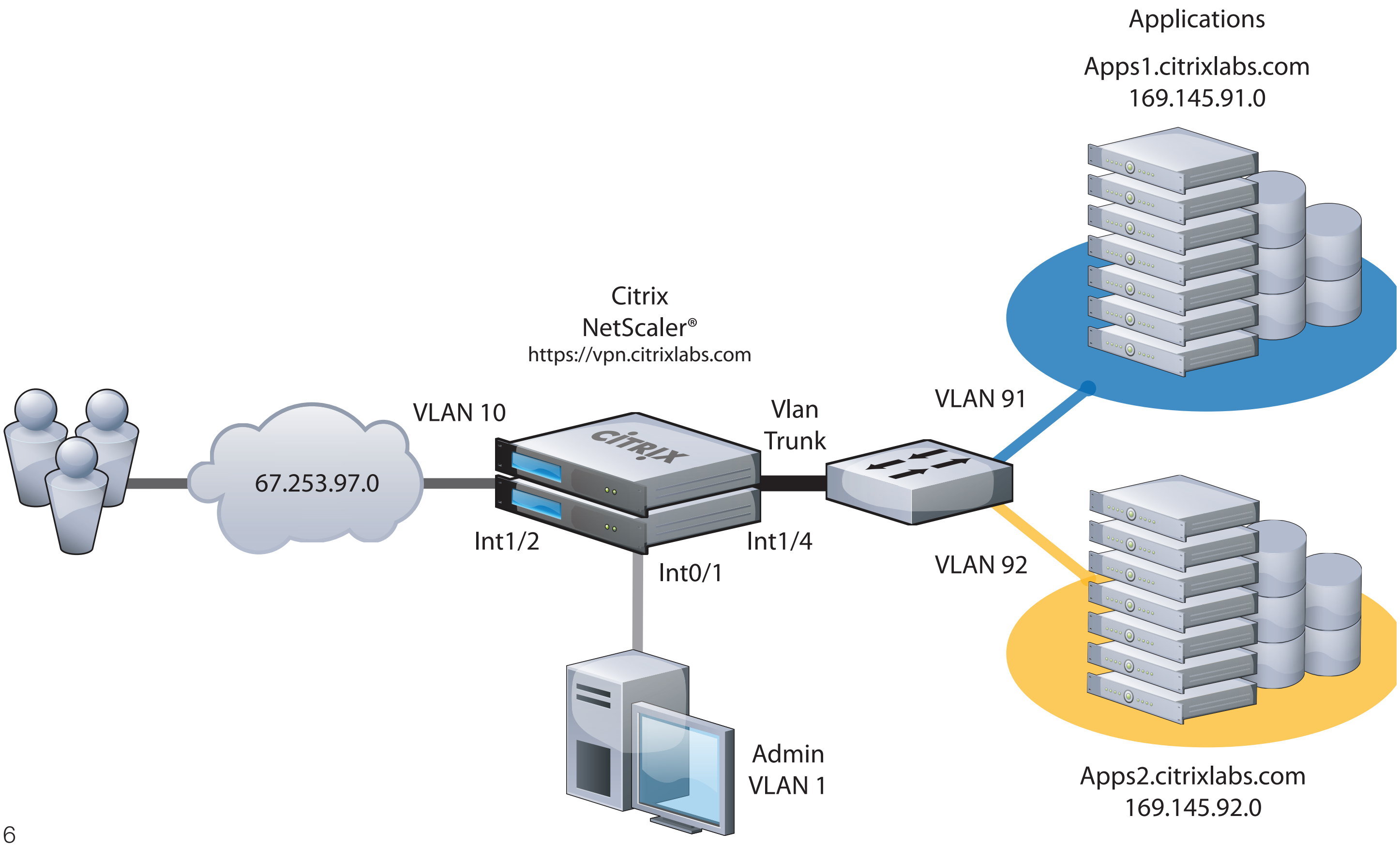
Prerequisites

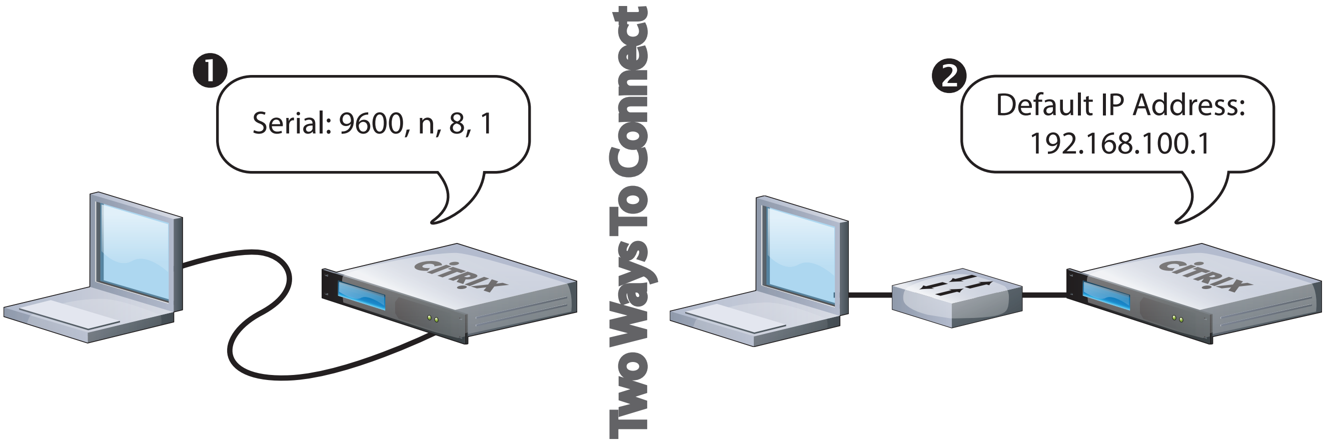
- Citrix NetScaler L4/7 Application Switch, running version 8.0+, (Quantity x 1 for single deployment, Quantity x 2 for HA deployment).
- Layer 2/3 switches, w/support for 802.1q Tagging & Trunking, (Quantity x 1)
- Client laptop/workstation running Internet Explorer 6.0+.

Network Diagram

The following is the Network that was used to develop this deployment guide, and is representative of a solution implemented at a customer site.

VLAN Legend	Primary NetScaler	Primary/Secondary NetScaler	Secondary NetScaler
◻ VLAN 1 ◼ VLAN 10 🟦 VLAN 91 🟨 VLAN 92 ⬛ TRUNK	IP Addresses: NSIP: 10.217.104.51 SNIP: 10.217.104.53	Shared IP Addresses: VIP: 67.97.253.92 SNIP: 169.145.91.239 SNIP: 169.145.92.239 VLAN 10: Interface 1/2, Untagged SNIP: 67.97.253.91 VLAN 91: Interface 1/4, Tagged MIP: 169.145.91.240 VLAN 92: Interface 1/4, Tagged MIP: 169.145.92.240 VLAN 4: Interface 1/4, Untagged Trunking ON VLAN 1: (Mgmt) Interface 0/1, Untagged MIP: 10.217.104.50	IP Addresses: NSIP: 10.217.104.52 SNIP: 10.217.104.54





First time connectivity

Serial Connection

The NetScaler can be accessed by the serial port through any terminal emulation program. Windows Hyperterm is commonly used on a laptop or workstation. Connect a 9-pin Null Modem cable from the computer to the NetScaler's console port. In the terminal emulation program configure the settings for 9600 baud, No stop bits, 8 data bits, and 1 parity bit. The login prompt should appear. The default login is nsroot, nsroot. It is advisable to change the nsroot password once connected.

Once connected type in the CLI command 'configns' ('nsconfig' if at the shell prompt). Select option 1 to change the NetScaler IP Address and Network Mask. Exit, save and reboot.

Ethernet Connection

The NetScaler can also be accessed by the default IP Address of 192.168.100.1, either through an http, https, telnet or ssh connection. Once connected, the login prompt should appear. The default login is nsroot, nsroot. It is advisable to change the nsroot password once connected.

Type in the CLI command 'configns' ('nsconfig' if at the shell prompt). Select option 1 to change the NetScaler IP Address and Network Mask. Exit, save and reboot.

Note: Changing the NetScaler IP Address always requires a reboot.

NetScaler Configuration

Deployment Model: Netscaler High Availability, Two-Arm Mode, SSL VPN

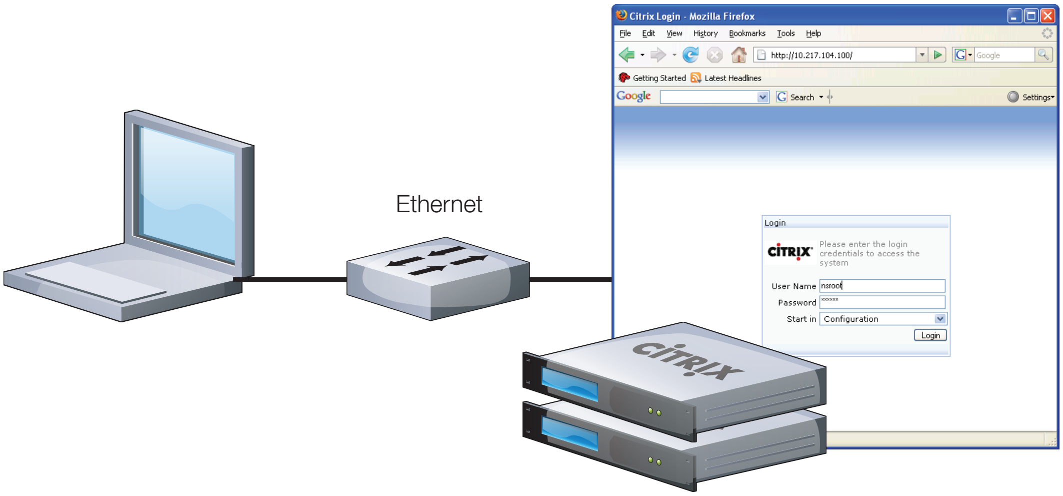
The NetScaler SSL VPNs in this example will be deployed as a high availability pair, in two-arm mode. Always start with the first NetScaler. The NetScalers in Two-Arm mode provide the utmost is site security, as they provide a full reverse-proxy gateway to intercept incoming traffic before it is sent to the Applications on the backend. Once the initial NetScaler IP Address (NSIP) has been configured, you can connect to both the Primary and Secondary NetScalers via a http or https web browser connection.

1. Connect to the NetScaler via the NSIP using a web browser.

   In this example:
   NS1: http://10.217.104.51
   NS2: http://10.217.104.52

   Note: Java will be installed.

   Default login is: nsroot, nsroot.


Ethernet
File Edit View History Bookmarks Tools Help
Getting Started Latest Headlines
Google Search Settings
Login
CITRIX

Citrix Login - Mozilla Firefox

http://10.217.104.100/

Login

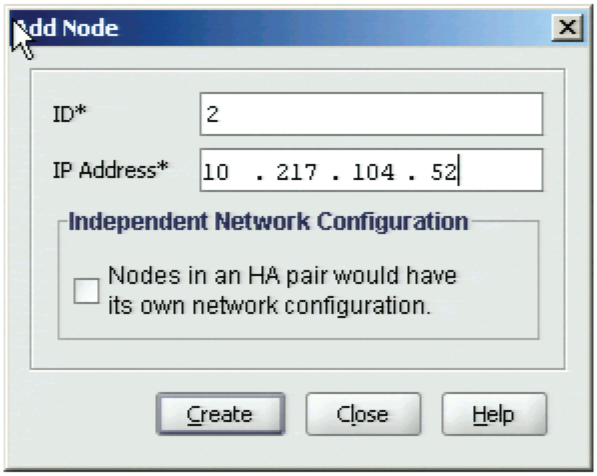
Please enter the login credentials to access the system

User Name: nsroot
Password: ******
Start in: Configuration

In a High Availability deployment, one Application Switch actively accepts connections and manages servers, while the second monitors the first. If the first Application Switch quits accepting connections for any reason, the second Application Switch takes over and begins actively accepting connections. This prevents downtime and ensures that the services provided by the Application Switch will remain available even if one Application Switch ceases to function.

Important Considerations for NetScaler High Availability

- The passwords for both NetScalers 'nsroot' account must match. You must change these manually on the switches, they are not synchronized.
- The maximum node ID for Application Switches in an HA pair is 64.
- Both NetScaler HA peers must be running the same version of code.
- The configuration files in 'ns.conf' must match on both NetScalers. For this to happen, the following must occur:
    - » The primary and secondary NetScaler Application switches must be configured with their own unique NSIP's.
    - » The 'node id' and 'IP Address' of one Application switch must point to the other Application switch (it's HA peer).
    - » You must configure RPC node passwords onto both Applicaiton switches. Initially, all Application Switches are configured with the same RPC node password. To enhance security, you should change these default RPC node passwords.



Add Node

ID* 2

IP Address* 10 . 217 . 104 . 52

Independent Network Configuration

□ Nodes in an HA pair would have its own network configuration.

2. While connected to the Primary NetScaler, add the Secondary node.

In the NetScaler GUI, navigate to: NetScaler ➥ System ➥ High Availability ➥ Add.

Enter the Node ID and IP address for the Secondary HA peer.

In this example:
'2', and 10.217.104.52.

Note:

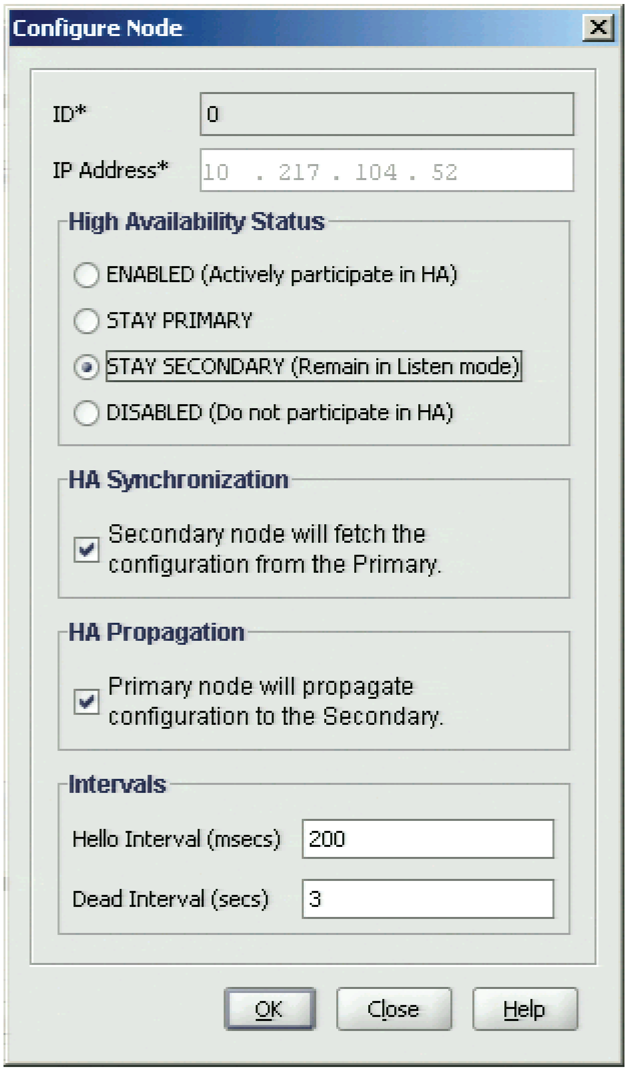
It is important to turn 'Off' HA Monitoring on interfaces that it is not intended for, otherwise HA Node Synchronization will not be successful.

In the NetScaler GUI: Navigate to NetScaler > Network > Interfaces.

Double-click the interface number(s), and turn 'Off' HA Monitoring.

4a. Connect to the Secondary NetScaler and tell it to take the Secondary role.

Navigate to NetScaler ➥ System ➥ High Availability ➥ Open ➥ "Stay Secondary".



Configure Node

ID* 0

IP Address* 10 . 217 . 104 . 52

High Availability Status

○ ENABLED (Actively participate in HA)

○ STAY PRIMARY

● STAY SECONDARY (Remain in Listen mode)

○ DISABLED (Do not participate in HA)

HA Synchronization

☑ Secondary node will fetch the configuration from the Primary.

HA Propagation

☑ Primary node will propagate configuration to the Secondary.

Intervals

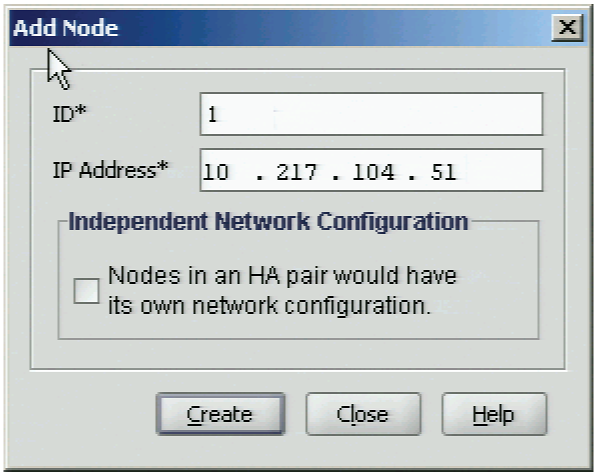
Hello Interval (msecs) 200

Dead Interval (secs) 3

4b. Connect to the Secondary NetScaler and add the Primary node.

Enter the Node ID and IP address for the Primary HA peer.

In this example:
'1', and 10.217.104.1.



Add Node

ID* 1

IP Address* 10 . 217 . 104 . 51

Independent Network Configuration

□ Nodes in an HA pair would have its own network configuration.

4c. Both Primary and Secondary must be configured to Actively participate in HA.

In the NetScaler GUI on the Primary: Navigate to NetScaler ➥ System ➥ High Availability ➥ ID 0 ➥ Open.

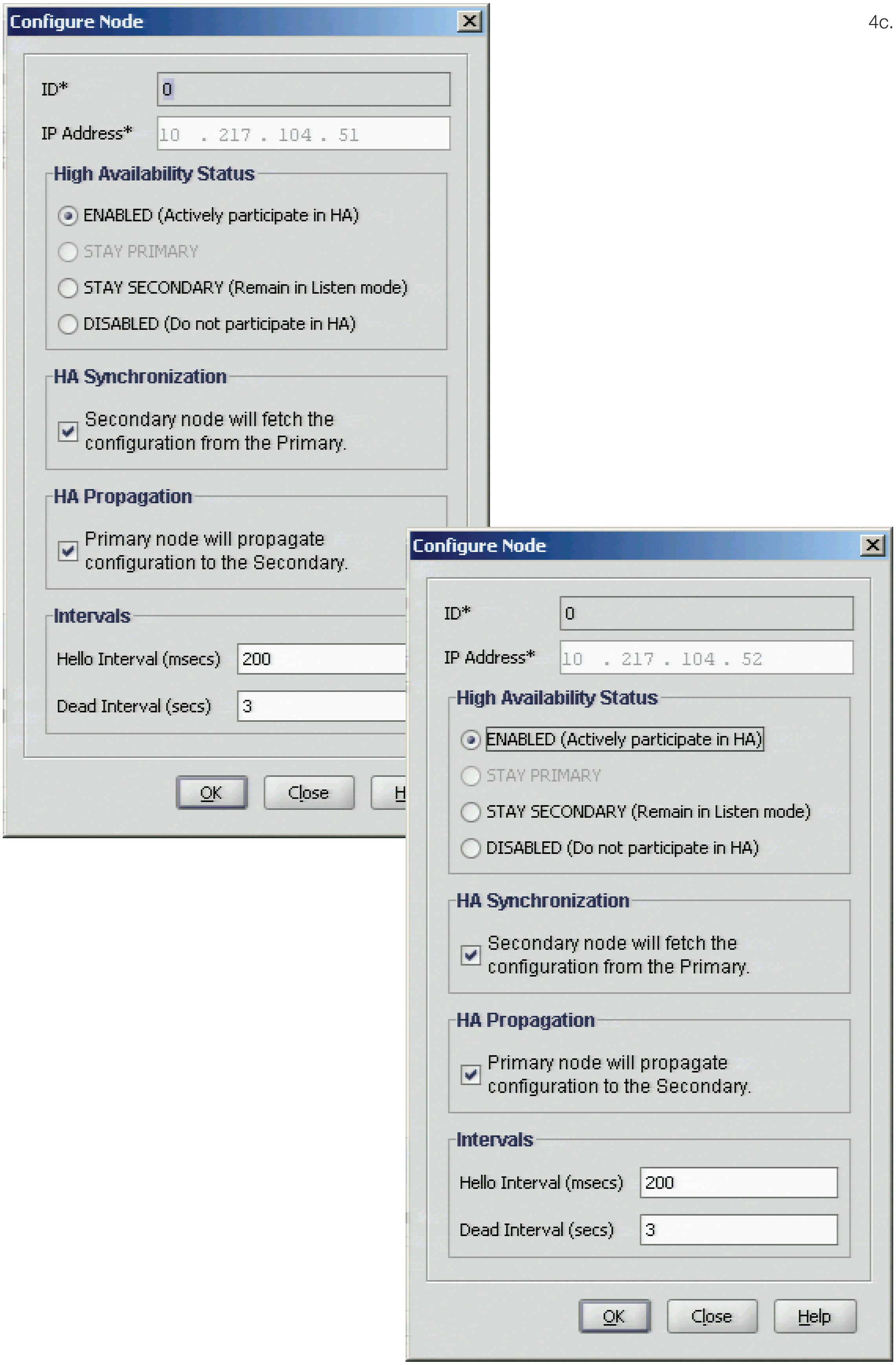
Select HA Status ‘Enabled’.

Enable HA Synchronization.

Enable HA Propagation.

Click ‘Ok’.

Repeat for Secondary.



Configure Node

ID* 0

IP Address* 10 . 217 . 104 . 51

High Availability Status

● ENABLED (Actively participate in HA)

○ STAY PRIMARY

○ STAY SECONDARY (Remain in Listen mode)

○ DISABLED (Do not participate in HA)

HA Synchronization

☑ Secondary node will fetch the configuration from the Primary.

HA Propagation

☑ Primary node will propagate configuration to the Secondary.

Intervals

Hello Interval (msecs) 200

Dead Interval (secs) 3

Configure Node

ID* 0

IP Address* 10 . 217 . 104 . 52

High Availability Status

● ENABLED (Actively participate in HA)

○ STAY PRIMARY

○ STAY SECONDARY (Remain in Listen mode)

○ DISABLED (Do not participate in HA)

HA Synchronization

☑ Secondary node will fetch the configuration from the Primary.

HA Propagation

☑ Primary node will propagate configuration to the Secondary.

Intervals

Hello Interval (msecs) 200

Dead Interval (secs) 3

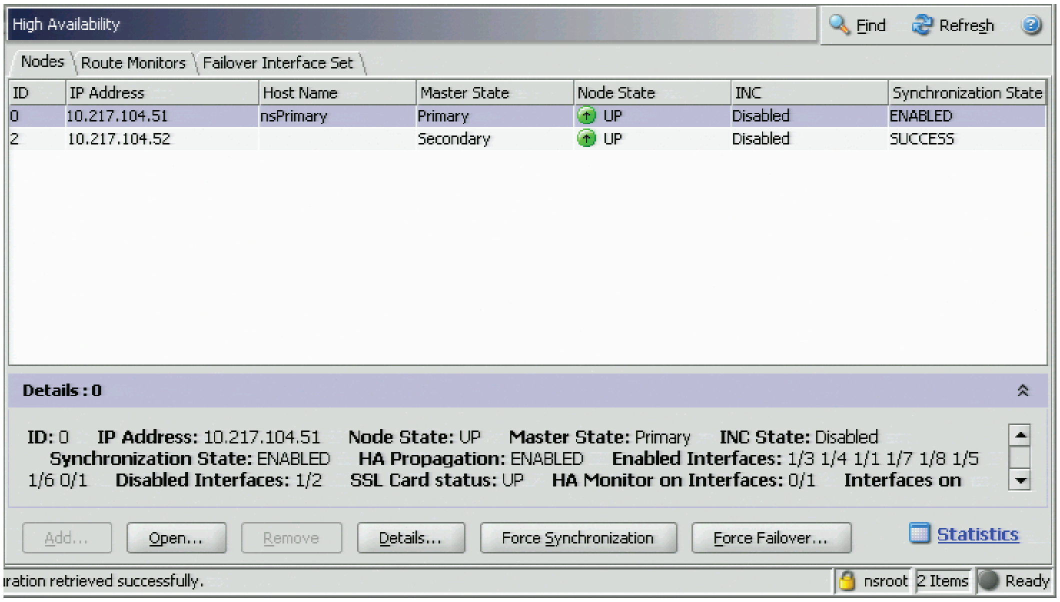
5. A successful HA Synchronization can be viewed from the High Availability screen on either the Primary or Secondary node's GUI.

   From the same screen you can 'Force Synchronization' or 'Force Failover'.

High Availability Command Synchronization

In a correct HA setup, any command issued on the primary Application Switch will propagate automatically to the secondary Application Switch. Some reasons why command synchronization may not work:

- Network connectivity is down
- Resources are not available on the Secondary Application switch
- Authentication failure, (nsroot and/or rpc node)
- HA Monitoring is not turned 'On', 'Off' on same interfaces for both nodes



ID	IP Address	Host Name	Master State	Node State	INC	Synchronization State
0	10.217.104.51	nsPrimary	Primary	UP	Disabled	ENABLED
2	10.217.104.52		Secondary	UP	Disabled	SUCCESS

Details : 0

ID: 0 **IP Address:** 10.217.104.51 **Node State:** UP **Master State:** Primary **INC State:** Disabled **Synchronization State:** ENABLED **HA Propagation:** ENABLED **Enabled Interfaces:** 1/3 1/4 1/1 1/7 1/8 1/5 1/6 0/1 **Disabled Interfaces:** 1/2 **SSL Card status:** UP **HA Monitor on Interfaces:** 0/1 **Interfaces on**

ration retrieved successfully. nsroot 2 Items Ready

TIP: Disabling the blinking LCD Panel

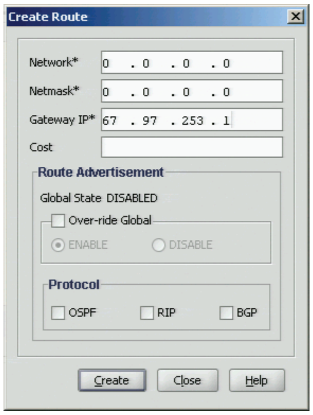
The LCD panel on the front of the NetScaler will flash intermittently until the unused interfaces are disabled and HA monitoring is turned off on them. In the GUI, Navigate to NetScaler > Network > Interfaces. Select an interface, right-click to disable. Right-click to Open, and disable HA monitoring.

Add a Default Route

6. Add a default route.

   NetScaler ➥ Network ➥ Route ➥ Add

   In this example,
   Network 0.0.0.0,
   Netmask 0.0.0.0,
   Gateway 67.97.253.1.



Network* 0 . 0 . 0 . 0
Netmask* 0 . 0 . 0 . 0
Gateway IP* 67 . 97 . 253 . 1
Cost

Route Advertisement
Global State DISABLED
□ Over-ride Global
● ENABLE ○ DISABLE

Protocol
□ OSPF □ RIP □ BGP

Optional:

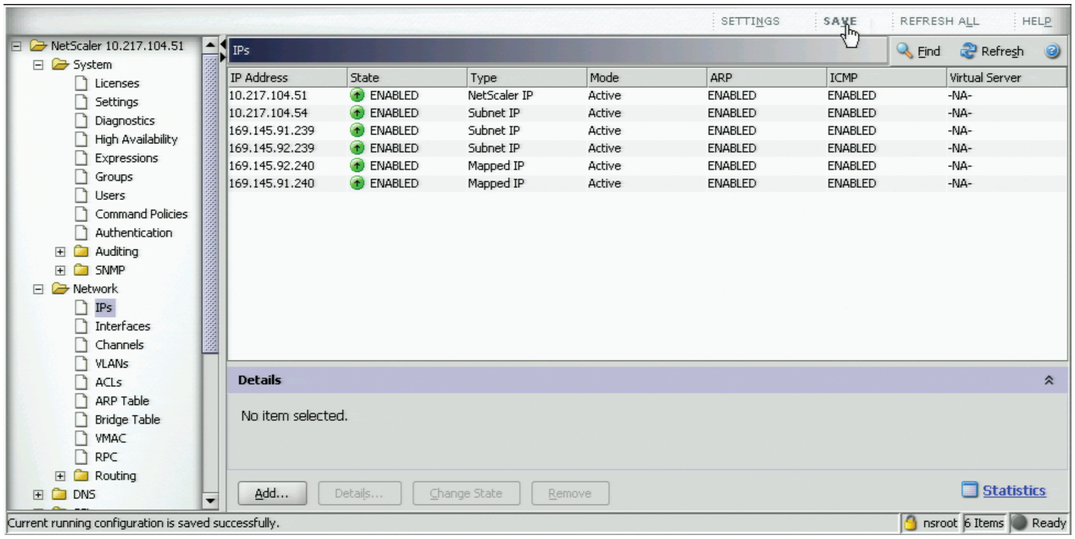
Because we have a Subnet IP Address (SNIP) on the Public Interface 1/2, this isn't really necessary.

Important NetScaler IP Addresses

Acronym	Description	Usage
Note: NSIP is Mandatory and requires a reboot.		
NSIP	NetScaler IP Address	The NetScaler IP (NSIP) is the management IP address for the appliance, and is used for all management related access to the appliance. There can only be one NSIP.
MIP	Mapped IP Address	The mapped IP address (MIP) is used by the Application Switch to represent the client when communicating with the backend managed server. Mapped IP addresses (MIP) are used for server-side connections and Reverse NAT. Think of this as the client's source address on the server-side of the Application Switch, assuming a two-arm proxy deployment. In this example you can think of it as the Tagged VLAN IP.
SNIP	Subnet IP Address	The Subnet IP address (SNIP) allows the user to access an Application Switch from an external host that is residing on another subnet. When a subnet IP address is added, a corresponding route entry is made in the route table. Only one such entry is made per subnet. The route entry corresponds to the first IP address added in the subnet.
VIP	Virtual IP Address	The Virtual Server IP address (VIP) is used by the Application Switch to represent the public facing ip address of the managed services. ARP and ICMP attributes on this IP address allow users to host the same vserver on multiple Application Switches residing on the same broadcast domain.
DFG	Default Gateway	IP Address of the router that forwards traffic outside of the subnet where the appliance is installed.

Add the remaining IP Addresses

IP Addresses that are added after HA Synchronization is complete, will be replicated on both Primary and Secondary NetScalers.



IP Address	State	Type	Mode	ARP	ICMP	Virtual Server
10.217.104.51	ENABLED	NetScaler IP	Active	ENABLED	ENABLED	-NA-
10.217.104.54	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-NA-
169.145.91.239	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-NA-
169.145.92.239	ENABLED	Subnet IP	Active	ENABLED	ENABLED	-NA-
169.145.92.240	ENABLED	Mapped IP	Active	ENABLED	ENABLED	-NA-
169.145.91.240	ENABLED	Mapped IP	Active	ENABLED	ENABLED	-NA-

No item selected.

Current running configuration is saved successfully.

7. Add the remaining IP Addresses.

NetScaler ➥ Network ➥ IPs ➥ Add.

⚠ Make sure you take this opportunity to “Save” the configuraiton on both the Primary and Secondary NetScalers.

IP Addresses, Interfaces and VLANs

Assigning IP Addresses to Interfaces is done ‘virtually’ through the use of port based VLANs.

By default, all the interfaces on the system are in a single port-based VLAN as untagged interfaces. This VLAN is the default VLAN with a VID equal to 1.

When an interface is added to a new VLAN as an untagged member, the interface is automatically removed from the default VLAN and placed in the new VLAN. This becomes a convenient feature, such that when we plug the Netscaler into a Switch that is using VLANs with tagging, we only need to check the box, to turn on tagging. VLANs are typically used to separate subnet traffic.

If Trunking is turned On, you will see an interface as a member of more than one VLAN.

8. Create VLANs and Assign Mapped IP Addresses to them.

   NetScaler ➥ Network ➥ VLANs ➥ Add.

Note: For this example: We create VLANs 4, 10, 91, 92. Only VLANs 91 and 92 are tagged.

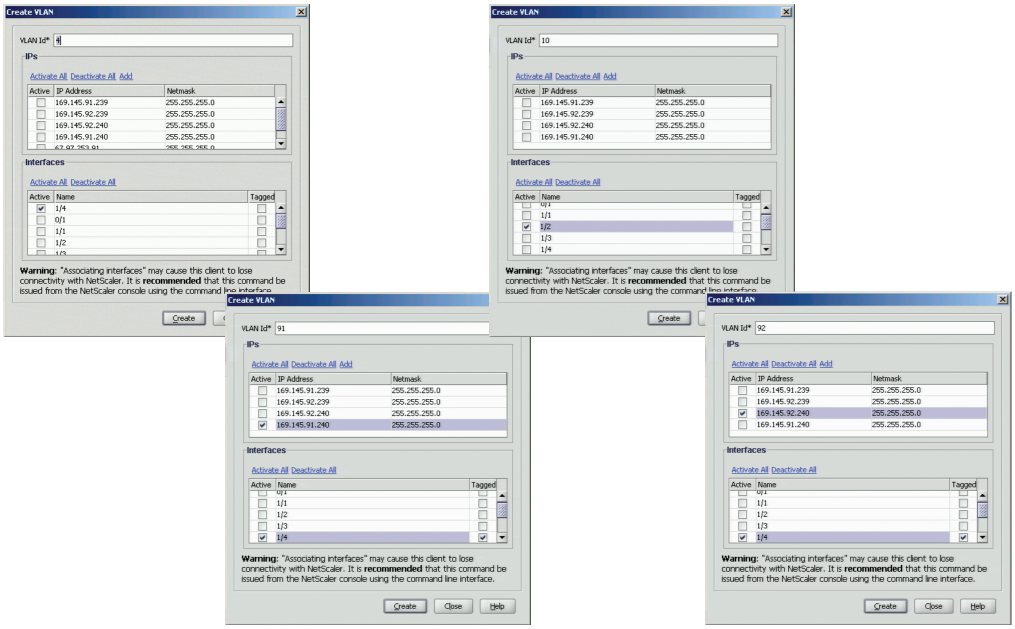
Interface 0/1 is our management interface, in VLAN 1.

Interface 1/2 is our public interface, in VLAN 10.

Interface 1/4 is the server side interface, and will be used as our 802.1q VLAN Trunk.

The corresponding port on the Layer 2 switch will be configured for 802.1q Trunking.

NetScaler ➥ Network ➥ VLANs, to view VLAN and Interface assignments on the Application switch.



Create VLAN — VLAN Id* 4

Active	IP Address	Netmask
☐	169.145.91.239	255.255.255.0
☐	169.145.92.239	255.255.255.0
☐	169.145.92.240	255.255.255.0
☐	169.145.91.240	255.255.255.0
☐	67.97.253.91	255.255.255.0

Active	Name	Tagged
☑	1/4	☐
☐	0/1	☐
☐	1/1	☐
☐	1/2	☐
☐	1/3	☐

Create VLAN — VLAN Id* 10

Active	IP Address	Netmask
☐	169.145.91.239	255.255.255.0
☐	169.145.92.239	255.255.255.0
☐	169.145.92.240	255.255.255.0
☐	169.145.91.240	255.255.255.0

Active	Name	Tagged
☐	0/1	☐
☐	1/1	☐
☑	1/2	☐
☐	1/3	☐
☐	1/4	☐

Create VLAN — VLAN Id* 91

Active	IP Address	Netmask
☐	169.145.91.239	255.255.255.0
☐	169.145.92.239	255.255.255.0
☐	169.145.92.240	255.255.255.0
☑	169.145.91.240	255.255.255.0

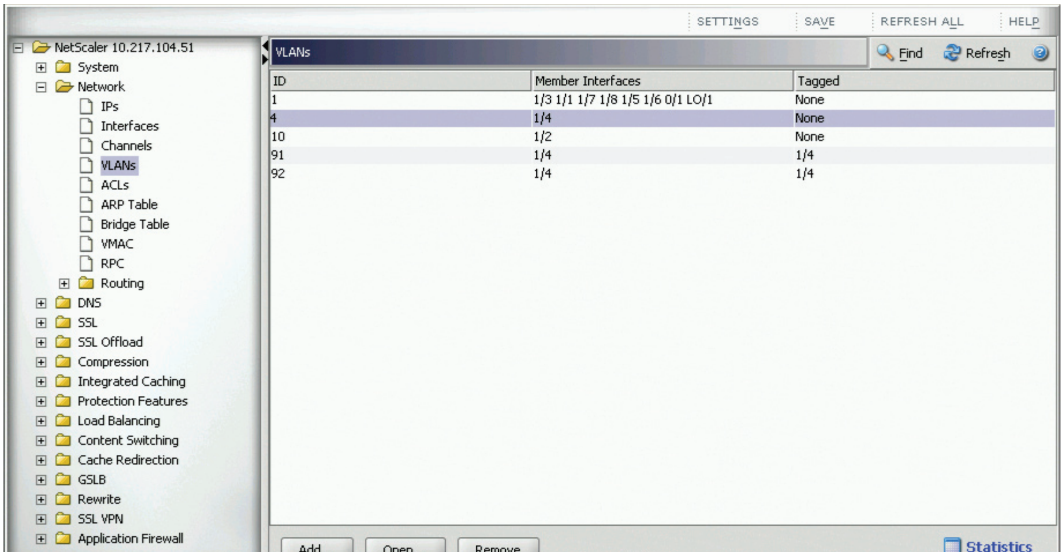
Active	Name	Tagged
☐	0/1	☐
☐	1/1	☐
☐	1/2	☐
☐	1/3	☐
☑	1/4	☑

Create VLAN — VLAN Id* 92

Active	IP Address	Netmask
☐	169.145.91.239	255.255.255.0
☐	169.145.92.239	255.255.255.0
☑	169.145.92.240	255.255.255.0
☐	169.145.91.240	255.255.255.0

Active	Name	Tagged
☐	0/1	☐
☐	1/1	☐
☐	1/2	☐
☐	1/3	☐
☑	1/4	☑

Warning: "Associating interfaces" may cause this client to lose connectivity with NetScaler. It is **recommended** that this command be issued from the NetScaler console using the command line interface.



ID	Member Interfaces	Tagged
1	1/3 1/1 1/7 1/8 1/5 1/6 0/1 LO/1	None
4	1/4	None
10	1/2	None
91	1/4	1/4
92	1/4	1/4

Configuring the Virtual MAC

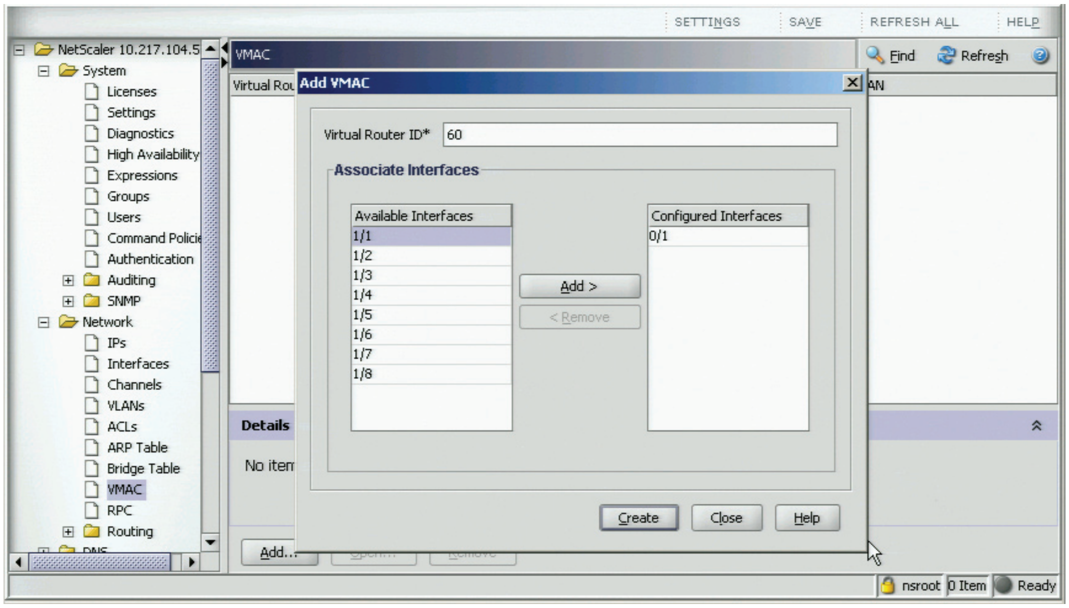
The Virtual MAC address (VMAC) is a floating entity shared by the primary and secondary nodes in an HA setup.

In an HA setup, the primary node owns all of the floating IP addresses such as MIP, SNIP, VIP, etc. It responds to ARP requests for these IP addresses with its own MAC address. As a result, the ARP table of an external device (for example, upstream router) is updated with the floating IP address and the primary node's MAC address.

When a failover occurs, the secondary node takes over as the new primary node. It then uses Gratuitous ARP to advertise the floating IP addresses that it acquired from the primary. The MAC address that the new primary advertises is that of its own interface.

Some devices do not accept Gratuitous ARP messages. You can overcome this problem by configuring a VMAC on both nodes of an HA pair. This implies that both the nodes possess identical MAC addresses. As a result, when failover occurs, the MAC address of the secondary node remains unchanged and ARP tables on the external devices do not need to be updated.

To create a VMAC, you need to create a VRID and bind it to an interface. In an HA setup, you need to bind it to the interfaces on both the primary and secondary nodes. When the VRID is bound to an interface, the system generates a VMAC with the VRID as the last octet. The generic VMAC is of the form 00:00:5e:00:01:<VRID>.



Virtual Router ID* 60

Configured Interfaces: 0/1

9. Assign a VMAC.

   Navigate to NetScaler ➥ Network ➥ VMAC ➥ Add.

   Add a Virtual Router ID to the Interface that HA Monitoring is enabled on.

SSL Keys & Certificates

Obtaining Keys and Certificates

Note: The Application Switch supports a certificate key size of up to 2048 bits (RSA/DSA).

All generated keys and certificates are created under directory /nsconfig/ssl on the Application Switch.

To get to this directory, login, and type the 'shell' CLI command.

Using any of the SSL features on the NetScaler requires that you obtain a certificate and private key for the NetScaler. An SSL certificate is a digital data form (X509) that identifies a particular company (domain) or an individual. An SSL key is the private component of the public-private key pair used in asymmetric key encryption (public key encryption).

Note: The Application Switch supports a certificate key size of up to 2,048 bits (RSA/DSA).

There are three ways to obtain keys and certificates for use with the Application Switch.

1) Create a self-signed certificate using the SSL certificate wizard.

2) Use an existing one, either root or intermediary, from an existing web server.

3) Obtain one from a public CA-Certificate Authority, such as Verisign.

In this guide we will use the Application Switch to generate a self-signed certificate. Refer to the Installation and Configuration Guide, NS_ICG_V1.pdf, for instructions on how to use an existing certificate or obtain one from a CA. NS_ICG_V2.pdf provides more detail surrounding SSL VPN configuration and should be used as another reference.

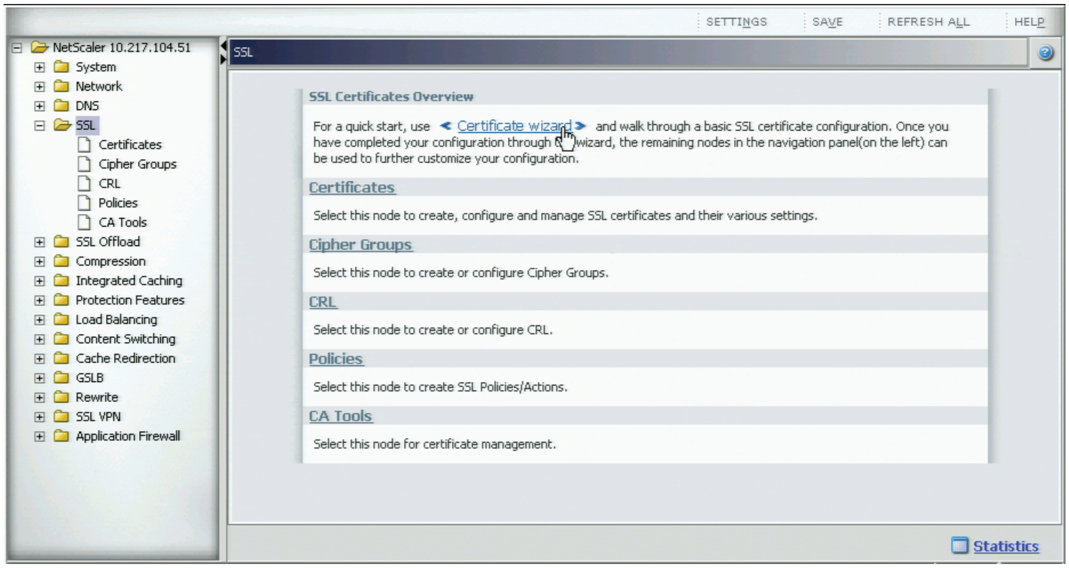
Using the SSL Certificate Wizard

Tip:

If you are in a rush to complete a proof of concept or a test environment, skip this section and use the Certificate creation tool inside of the SSL VPN Wizard in the next section, it is much easier.

10. To launch the SSL Certificate Wizard, from the GUI, navigate to NetScaler ➥ SSL.

Click on the <Certificate Wizard>.



SSL Certificates Overview

For a quick start, use < Certificate wizard > and walk through a basic SSL certificate configuration. Once you have completed your configuration through the wizard, the remaining nodes in the navigation panel(on the left) can be used to further customize your configuration.

Certificates

Select this node to create, configure and manage SSL certificates and their various settings.

Cipher Groups

Select this node to create or configure Cipher Groups.

CRL

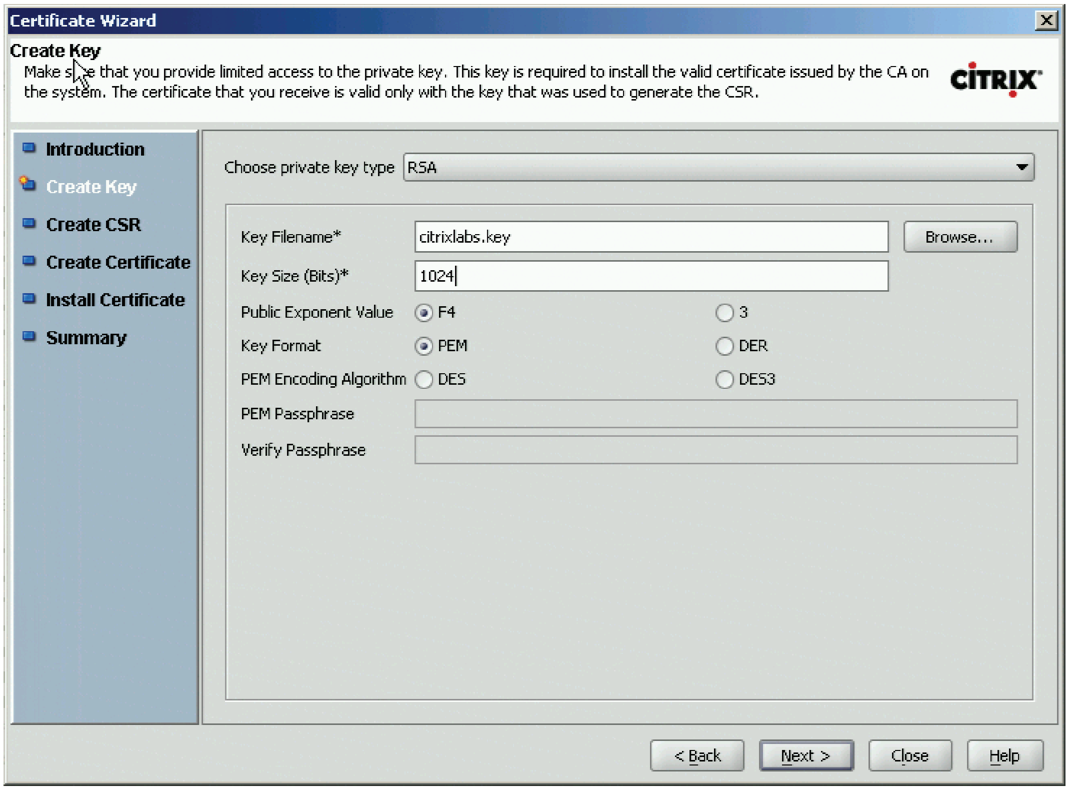
Select this node to create or configure CRL.

Policies

Select this node to create SSL Policies/Actions.

CA Tools

Select this node for certificate management.



Create Key

Make sure that you provide limited access to the private key. This key is required to install the valid certificate issued by the CA on the system. The certificate that you receive is valid only with the key that was used to generate the CSR.

Choose private key type: RSA

Key Filename*: citrixlabs.key

Key Size (Bits)*: 1024

Public Exponent Value: ● F4 ○ 3

Key Format: ● PEM ○ DER

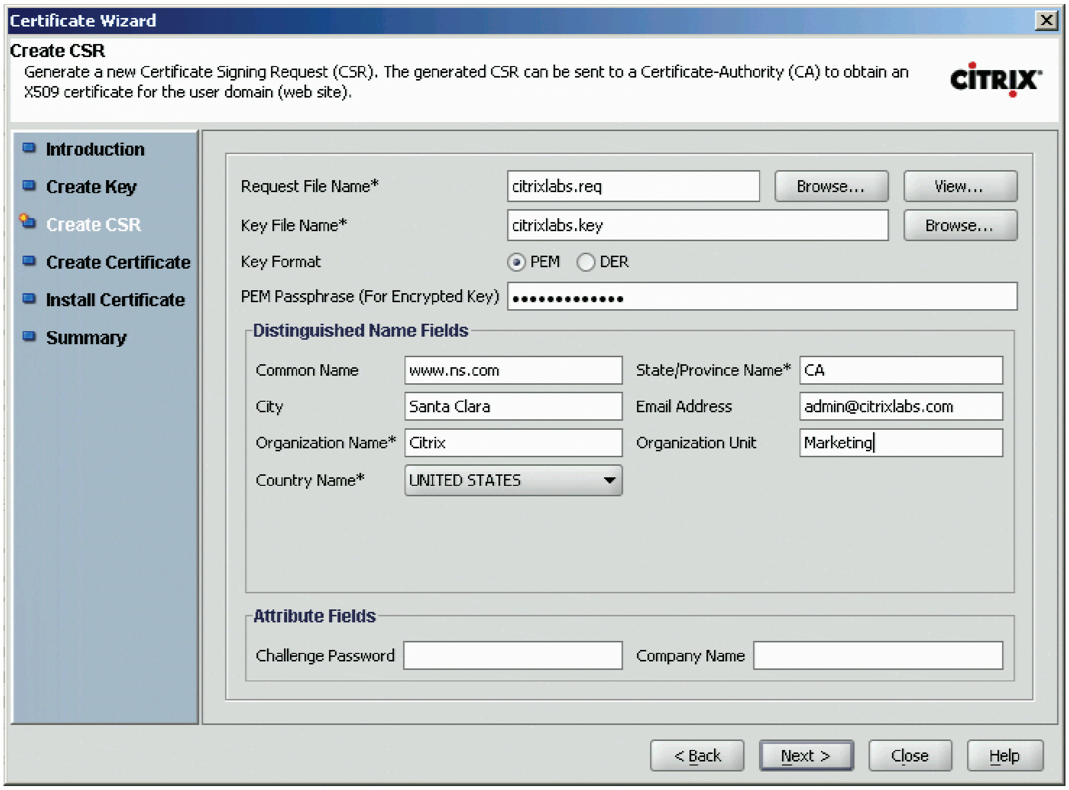
PEM Encoding Algorithm: ○ DES ○ DES3

PEM Passphrase:

Verify Passphrase:

11. Once past the introduction screen, enter the name for the file to store the ssl keys in.

    Common key strength values: 512, 1024, 2048.



Create CSR

Generate a new Certificate Signing Request (CSR). The generated CSR can be sent to a Certificate-Authority (CA) to obtain an X509 certificate for the user domain (web site).

Request File Name*: citrixlabs.req

Key File Name*: citrixlabs.key

Key Format: ● PEM ○ DER

PEM Passphrase (For Encrypted Key): ••••••••••••••

Distinguished Name Fields

Common Name	www.ns.com	State/Province Name*	CA
City	Santa Clara	Email Address	admin@citrixlabs.com
Organization Name*	Citrix	Organization Unit	Marketing
Country Name*	UNITED STATES		

Attribute Fields

Challenge Password: Company Name:

12. Enter a filename to store the request.

    Select the PEM format for CA. Enter a passphrase.

    Enter the X509 fields.

TIP:

Common Name:

The common name should match the name used by DNS servers during a DNS lookup of your virtual server (for example, vpn.citrixlabs.com). Most browsers use this information for authenticating the virtual server's certificate during the SSL handshake. If the virtual server DNS name does not match the common name as given in the server certificate, the browsers will terminate the SSL handshake or prompt the user with a warning message. Do not use wildcard characters such as * or ? and do not use an IP address as a common name. The common name should be without the protocol specifier http:// or https://.

Organization Name:

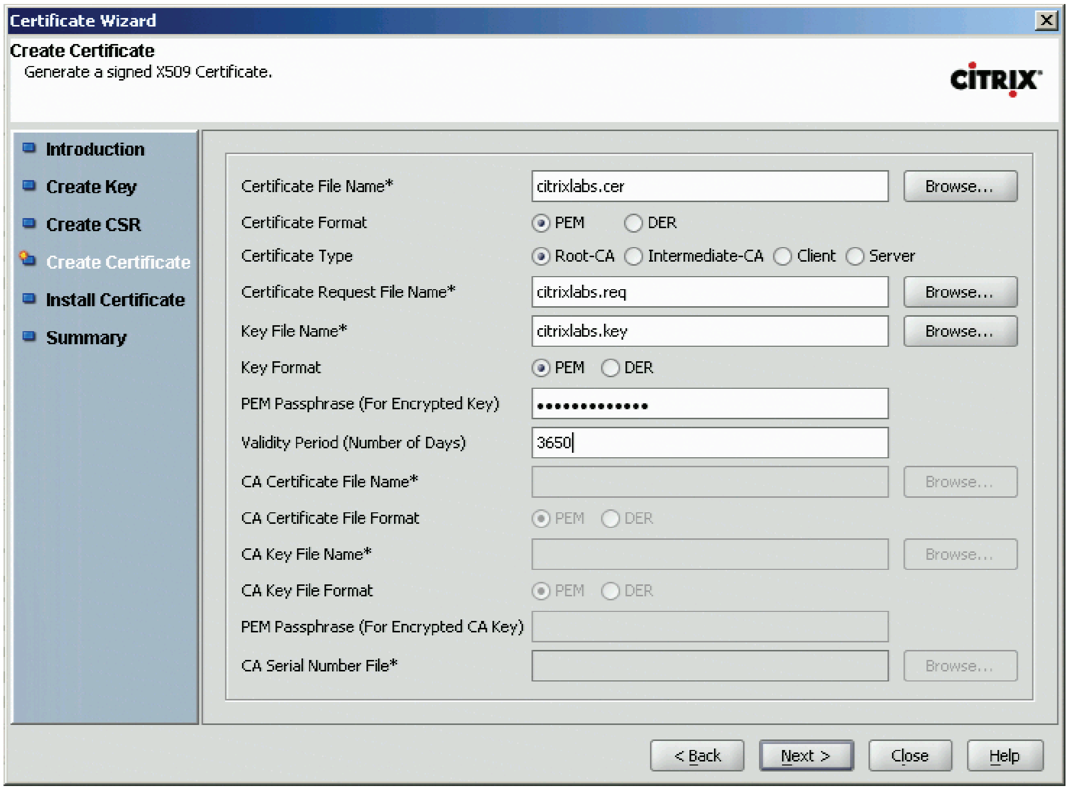
The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Do not abbreviate the organization name and do not use the following characters in the name: < > ~ ! @ # $ % ^ * / \ ( )?. For example, Citrix Systems, Inc.

13. Enter the filename for the SSL Certificate. You will need to find this one later.

    Make sure you select Root CA certificate, as this is a self-signed root certificate.

    Enter a passphrase.

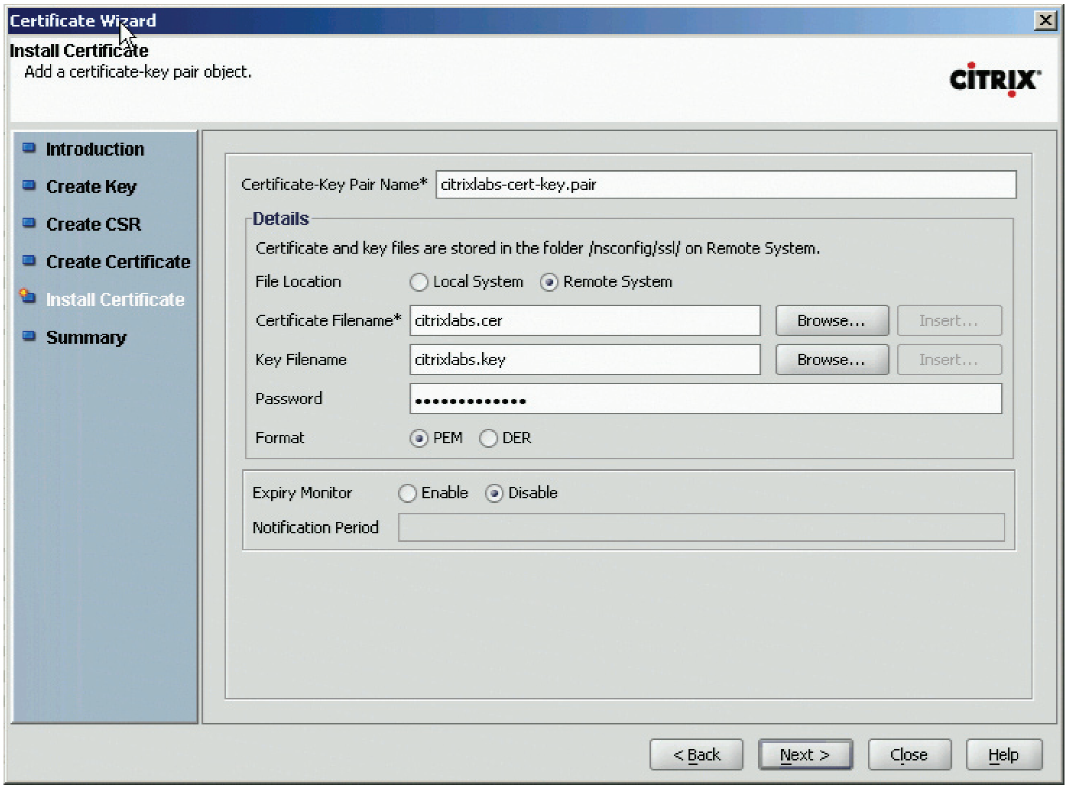
    Enter a time period this certificate is valid for. 3650 is equivalent to 10 years. More stringent security rules would dictate shorter time periods.



Create Certificate

Generate a signed X509 Certificate.

Certificate File Name*	citrixlabs.cer
Certificate Format	● PEM ○ DER
Certificate Type	● Root-CA ○ Intermediate-CA ○ Client ○ Server
Certificate Request File Name*	citrixlabs.req
Key File Name*	citrixlabs.key
Key Format	● PEM ○ DER
PEM Passphrase (For Encrypted Key)	•••••••••••••
Validity Period (Number of Days)	3650
CA Certificate File Name*	
CA Certificate File Format	● PEM ○ DER
CA Key File Name*	
CA Key File Format	● PEM ○ DER
PEM Passphrase (For Encrypted CA Key)	
CA Serial Number File*	



Certificate Wizard

Install Certificate

Add a certificate-key pair object.

Certificate-Key Pair Name* citrixlabs-cert-key.pair

Details

Certificate and key files are stored in the folder /nsconfig/ssl/ on Remote System.

File Location ○ Local System ● Remote System

Certificate Filename* citrixlabs.cer

Key Filename citrixlabs.key

Password •••••••••••••

Format ● PEM ○ DER

Expiry Monitor ○ Enable ● Disable

Notification Period

14. Enter a kay pair filename and passphrase.

    Then select Finish.

TIP:

Now is a good time to log into the GUI on both the Primary and Seconary NetScaler and make sure the SSL Certificate exists on both systems. If the certificate files (request, key, certificate) did not get replicated from the Primary to the Secondary HA unit, then creating the SSL VPN will be difficult.

Make sure the SSL Certificate files exist on both the Primary and Secondary. The most efficient way to do this is to SSH into the Primary node, and enter the ‘sync HA files all’ command.

You can also download / upload certificate files using a tool called WinSCP. http://winscp.net/.

The certificate files are stored in the /nsconfig/ssl directory.

This is also a good time for Force Synchronization and save configuraitons.

Once the SSL VPN is completely configured, you will want to perform a ‘Force Failover’ to make sure the VPN comes up on the Secondary unit to ensure the certificates have been replicated across the HA systems.

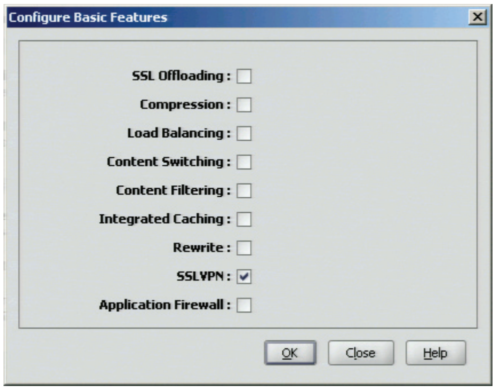
SSL VPN Configuration

SSL VPN Wizard

This section walks through the steps to configure a basic SSL VPN using the SSL VPN Wizard. The basic configuration steps are: Enable the SSL VPN feature, Create an SSL VPN virtual server, Configure name resolution for VPN clients, and Configure the VPN's SSL certificate(s).

15. First the SSL VPN feature needs to be enabled.

    From the GUI, navigate to NetScaler ➥ System ➥ Settings ➥ Basic Features. Cllick on <basic features> and check the SSL VPN box.



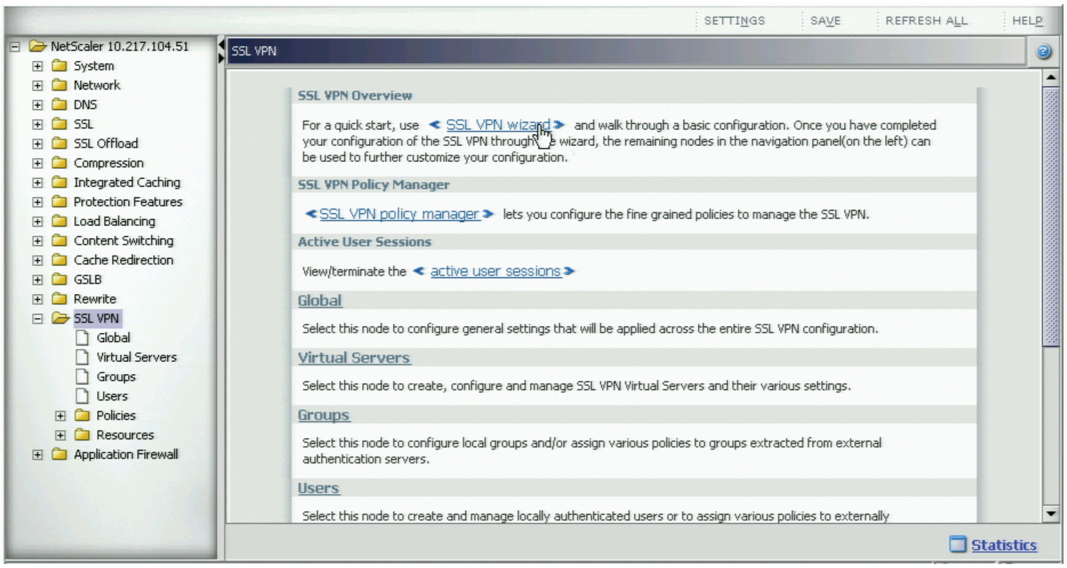
Configure Basic Features

SSL Offloading : □
Compression : □
Load Balancing : □
Content Switching : □
Content Filtering : □
Integrated Caching : □
Rewrite : □
SSLVPN : ☑
Application Firewall : □

16. The SSL VPN Wizard simplifies the process of creating the SSL VPN configuration.

    From the GUI, navigate to NetScaler ➥ SSL VPN.

    In the right-hand frame, select <SSL VPN Wizard>.



SSL VPN Overview

For a quick start, use < SSL VPN wizard > and walk through a basic configuration. Once you have completed your configuration of the SSL VPN through the wizard, the remaining nodes in the navigation panel(on the left) can be used to further customize your configuration.

SSL VPN Policy Manager

< SSL VPN policy manager > lets you configure the fine grained policies to manage the SSL VPN.

Active User Sessions

View/terminate the < active user sessions >

Global

Select this node to configure general settings that will be applied across the entire SSL VPN configuration.

Virtual Servers

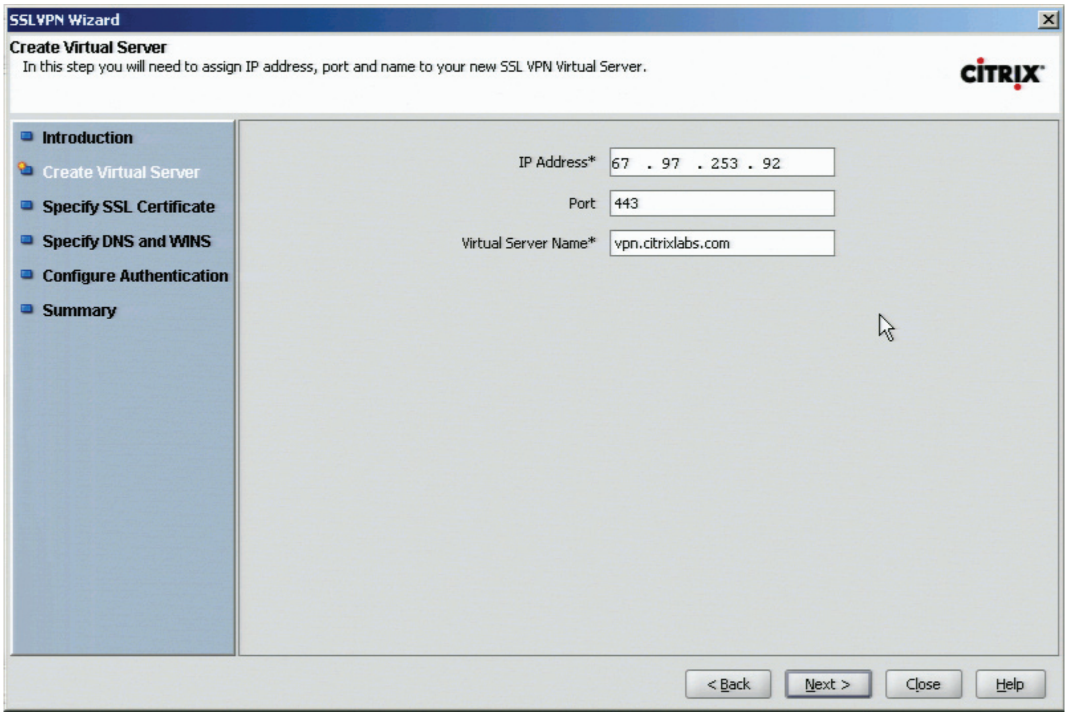
Select this node to create, configure and manage SSL VPN Virtual Servers and their various settings.

Groups

Select this node to configure local groups and/or assign various policies to groups extracted from external authentication servers.

Users

Select this node to create and manage locally authenticated users or to assign various policies to externally



SSLVPN Wizard

Create Virtual Server

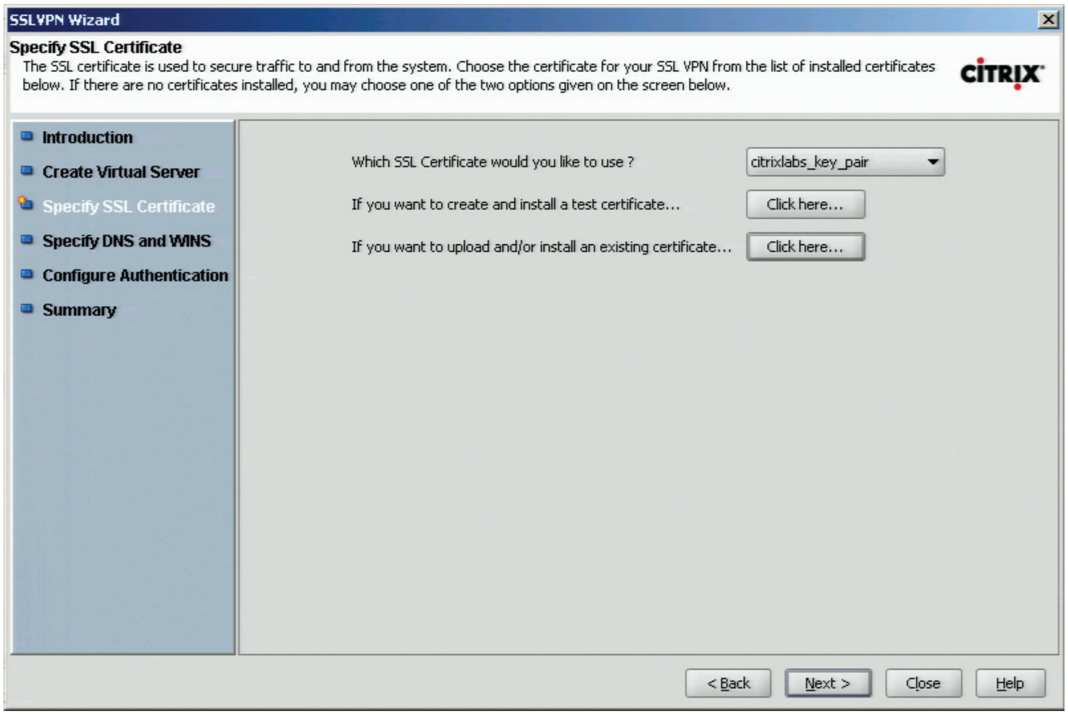
In this step you will need to assign IP address, port and name to your new SSL VPN Virtual Server.

IP Address* 67 . 97 . 253 . 92

Port 443

Virtual Server Name* vpn.citrixlabs.com

17. After the Introduction, create the Virtual Server for the SSL VPN by entering the Public IP Address that users will access the SSL VPN by. Also enter the port and FQDN.



SSLVPN Wizard

Specify SSL Certificate

The SSL certificate is used to secure traffic to and from the system. Choose the certificate for your SSL VPN from the list of installed certificates below. If there are no certificates installed, you may choose one of the two options given on the screen below.

Which SSL Certificate would you like to use ? citrixlabs_key_pair

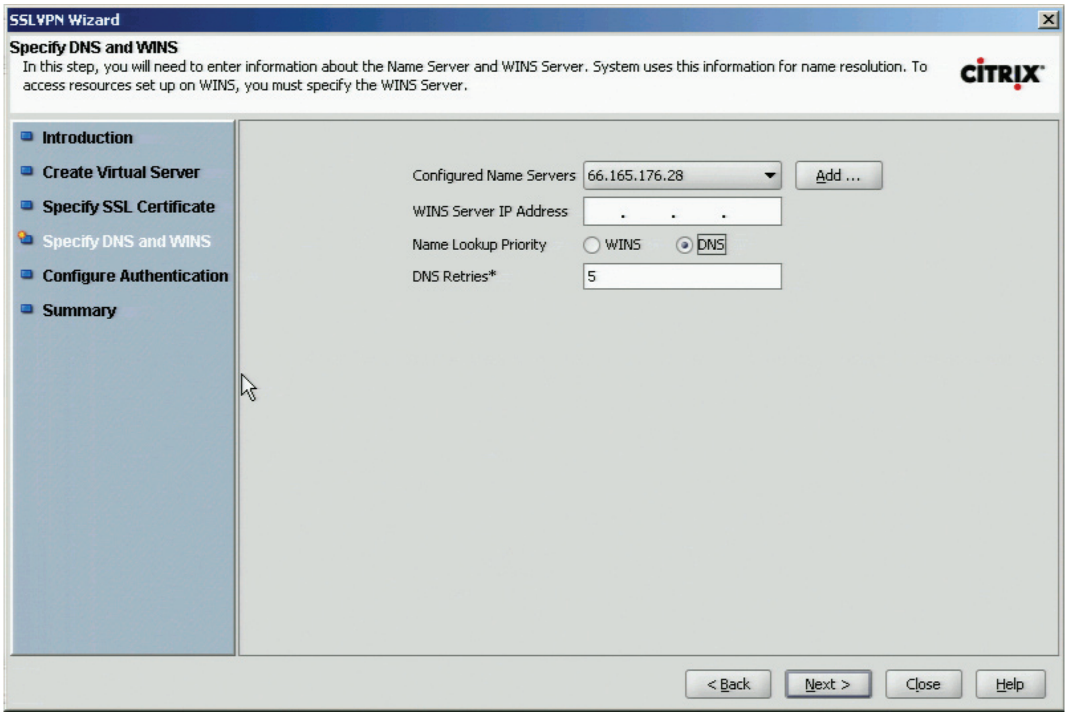
If you want to create and install a test certificate... Click here...

If you want to upload and/or install an existing certificate... Click here...

18. Specify the SSL Certificate. Click on the first drop down menu on the right-hand frame, and select the name of the certificate created earlier in the exercise.

If you skipped the certificate creation in the previous section, you can create one quickly for testing by clicking on the second button.

19. Add the Domain Name Server and select DNS.



Specify DNS and WINS

In this step, you will need to enter information about the Name Server and WINS Server. System uses this information for name resolution. To access resources set up on WINS, you must specify the WINS Server.

Configured Name Servers: 66.165.176.28

WINS Server IP Address: . . .

Name Lookup Priority: ○ WINS ● DNS

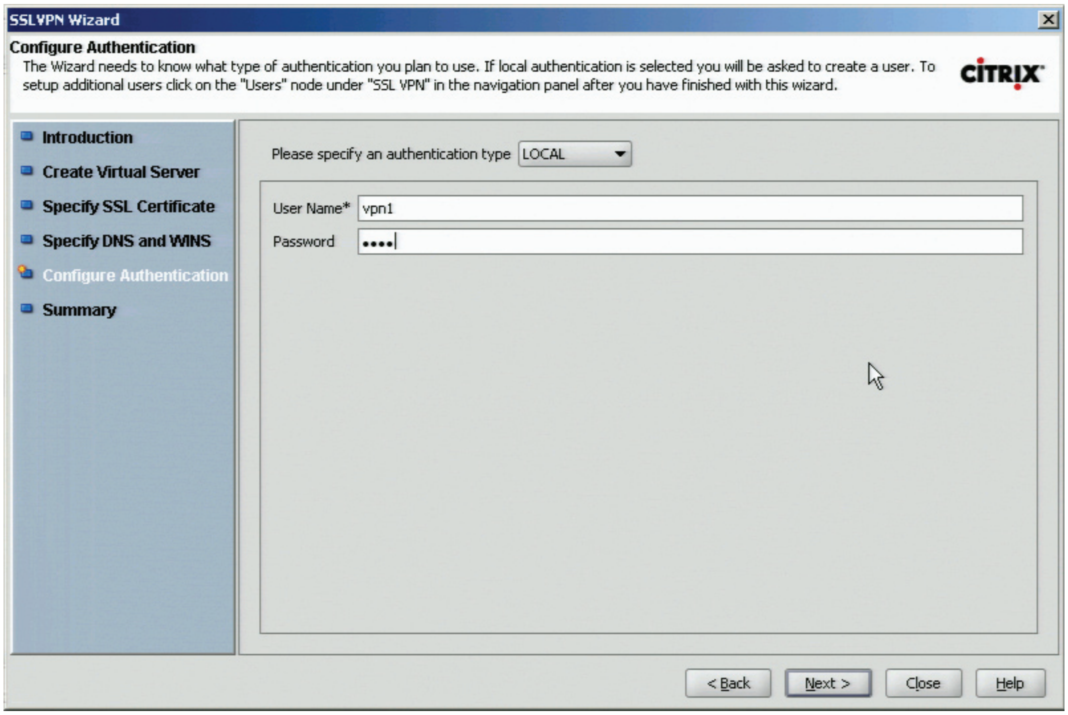
DNS Retries*: 5

20. Enter a local username and password for authentication.

Later on, you can configure other types of authentication using external resources, such as LDAP, RADIUS, Client Certificate, Active Directory and TACACS.

Review and select Finish.

Note: If the Virtual Server does not come up, make sure the licenses match on the Primary and Secondary devices.



Configure Authentication

The Wizard needs to know what type of authentication you plan to use. If local authentication is selected you will be asked to create a user. To setup additional users click on the "Users" node under "SSL VPN" in the navigation panel after you have finished with this wizard.

Please specify an authentication type: LOCAL

User Name*: vpn1

Password: ••••

Accessing the SSL VPN

Importing SSL Certificates

If you followed the tip in the previous section on the use of Common Name and Organization Name, then there is one more step to enable your clients. Download the SSL Certificate from the Primary or Secondary Applicaiton Switch and Import the certificate into the web browser as a 'Trusted Root Certificate Authority".

Internet Explorer: Navigate to Tools ➥ Internet Options ➥ Content. Certificates ➥ Trusted Root Certificate Authorities ➥ Import.

Firefox: Navigate to Tools ➥ Options ➥ View Certificates. Select the Authorities Tab ➥ Import.

Testing the SSL VPN

To access the SSL VPN, you need to launch a browser and point it to the Virtual Server IP Address (VIP) created in the previous section. This is the public facing IP Address. For example, in the lab used in this guide, https://67.97.253.92 ~or~ https://vpn.citrixlabs.com.

At the logon screen, enter the username and password of the user account you created earlier. If the user authenticates correctly, you will see the window shown on the next page.

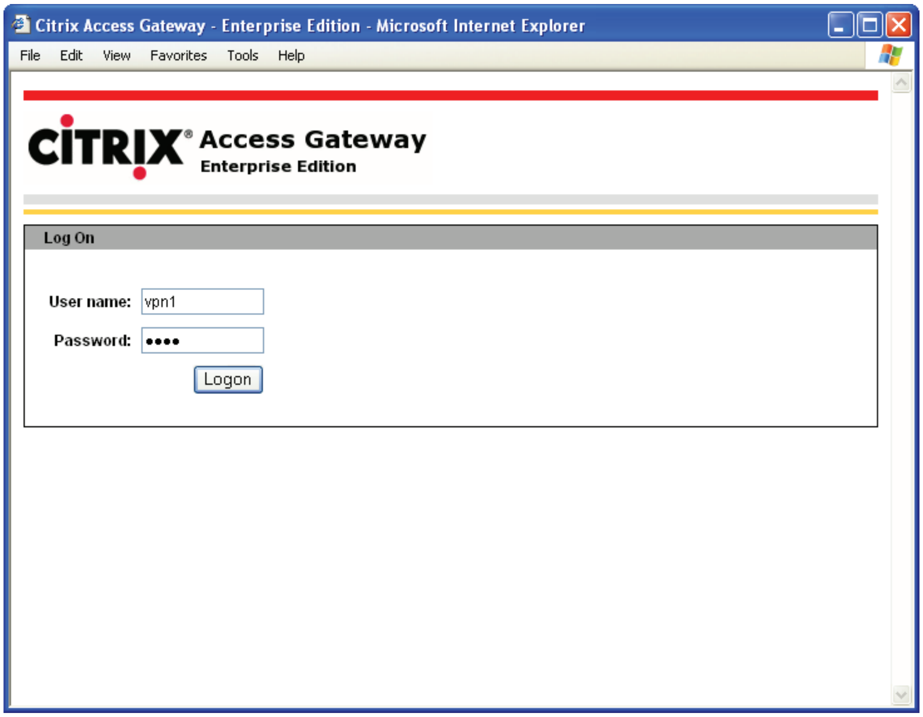
Note:

If you see a certificate warning before the login window appears, this may be because the VPN is using a self-signed certificate or an invalid certificate. If you used a self-signed certificate, you can ignore this warning.

If you used a certificate signed by a CA, however, there is a problem with the certificate, so close the warning by clicking the "No" button. Verify that you generated the site certificate correctly if you used a signed CSR, and that the distinguished name data entered in the CSR is accurate. Check that the configured certificate's common name corresponds to the configured virtual server IP information.

If the login screen does not appear, or if you received a different error, review the setup process and confirm that all steps were performed correctly and that all parameters were entered accurately.

21. Enter the username and password created earlier.



Citrix Access Gateway - Enterprise Edition - Microsoft Internet Explorer

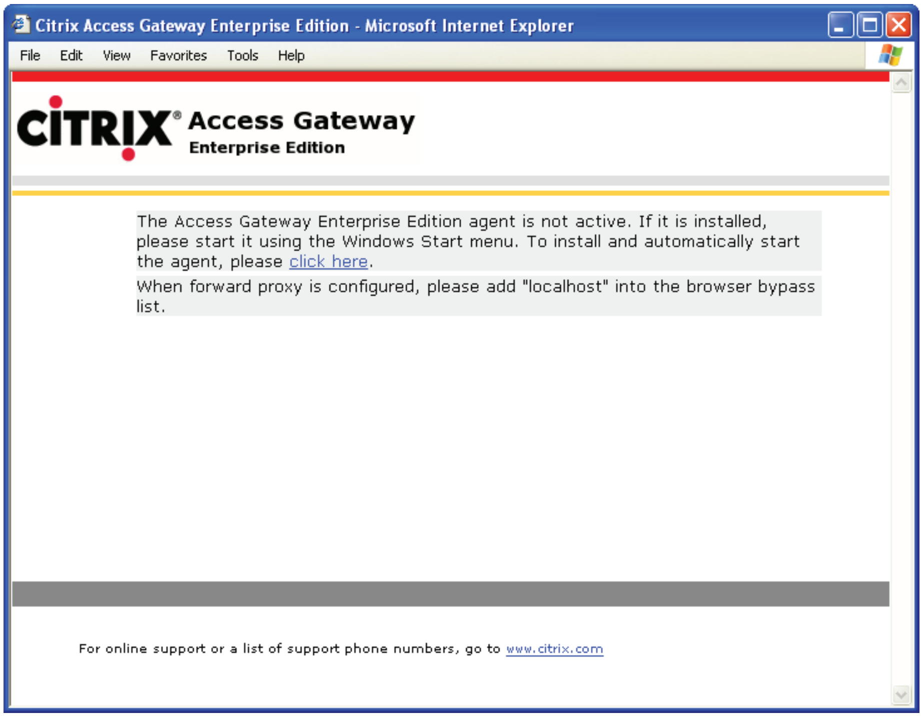
Log On

User name: vpn1

Password: ••••

When authentication is successful, the following screen appears.

You have the option of downloading the SSL VPN Agent.



Citrix Access Gateway Enterprise Edition - Microsoft Internet Explorer

The Access Gateway Enterprise Edition agent is not active. If it is installed, please start it using the Windows Start menu. To install and automatically start the agent, please click here.

When forward proxy is configured, please add "localhost" into the browser bypass list.

For online support or a list of support phone numbers, go to www.citrix.com

Things you need to know

There are two ways to access the SSL VPN

1) Agentless (using a web browser plug-in)
The SSL VPN does not need a client or agent, which is what makes SSL VPN so attractive, affordable and efficient. You can require all users to access the SSL VPN by only using the web browser.

2) Agent Login (using an agent installed on the users computer)
When you configure the SSL VPN Policies you will notice under the VPN Global Settings, Client Experience, Windows Client Type, there are two types of clients. Agent and Plugin. Agent=Windows Agent Client, Plugin=Active-X client ~or~ Java applet client.

Windows users will use either the Agent (Agent login) or Active-X client or Java applet client (Agentless login), while other OS's will use the Java applet client. The Transparent Inspection setting determines which Client gets downloaded. Also keep in mind the ActiveX and Java clients behave differently and have differing depths of features.

The Windows Active-X plug-in intelligently intercepts traffic to be tunneled to the private intranet. Alternatively, the Java applet plug-in, available for both Windows and non-Windows operating systems, does not intercept traffic transparently and hence native client/server applications need to be specifically configured on the system. Once these applications are configured on a port basis, the Java applet plug-in listens on those pre-configuredapplication ports via the client's loopback interface in order to manage the client's connections.

Split Tunneling

Split tunneling allows an ActiveX client to distinguish between SSL VPN traffic and other traffic based on destination IP, and direct only SSL VPN traffic through the SSL VPN tunnel. However, setting Split Tunnel to ON, will enable the traffic to bypass the secure Netscaler VPN tunnel.

With split tunnel set to OFF, all user traffic is tunneled through the secure NetScaler SSL VPN tunnel.

Setting split tunnel to Reverse will enable all traffic except Traffic directed to IP addresses belonging to the intranet network domains configured on the SSL VPN to pass through the secure NetScaler VPN tunnel.

Cleanup

The Client Cleanup Prompt controls the display of the Client Cleanup pop-up window that appears on Windows client machines on exiting the SSL VPN session. If prompted, the user can select the data that needs to be removed. However, certain types of data can be automatically removed by configuring the force cleanup option.

Client Cleanup can be automatically performed, by turning OFF the Client Cleanup Prompt and setting the Cleanup options in advanced settings.

Home Page

When a VPN user logs in, the default SSL VPN portal page is presented to the user. On configuring the home page URL option, the system will redirect the VPN user's browser to the URL specified in the Home Page field. If the option is unchecked, no homepage will be displayed after the SSL VPN user logs in.

SSL VPN Polices

Evaluated in the following order, these policies give you control over clients as they access the resources within the Intranet. If none of the policies match those bound to users or groups, then global policies will be evaluated and applied.

Authentication policy

In the SSL VPN, there are five types of policies available for managing your configuration dynamically. Authentication policies are used to define what type of authentication method to ascribe to users. These policies are applied first by the system in order to determine who is allowed to log in to the SSL VPN.

Session policy

The VPN Session Policy regulates how clients are configured. With VPN session policies, you may define policies to set various client Agent (ActiveX) or Plug-in (Java) parameters such as client security checks and proxy configurations. VPN session policies are evaluated based on client source network after user authentication has been performed. VPN Session policies are useful for directing clients to specific home pages or CPS Server farms, and setting ICA Proxy ON or OFF.

Authorization policy

The Authorization policy is used to control which resources SSL VPN clients may access. Each time a client attempts to access an intranet resource through the SSL VPN, all the authorization policies for that user are evaluated to determine whether the user is allowed to access that resource before the user is given access to the resource.

Traffic policy

VPN Trafic policies further refine how clients are to access resources. With VPN traffic policies, you can customize VPN session traffic parameters such as what application timeout interval to apply to client sessions. These policies can be evaluated based on requested resource location data such as an IP address, port number, or a URL.

Tunnel policy

Tunnel trafic policy is used to control available traffic acceleration services including compression. Tunnel traffic policies evaluate what services to apply based on requested resource destination IP address, port, or URL.

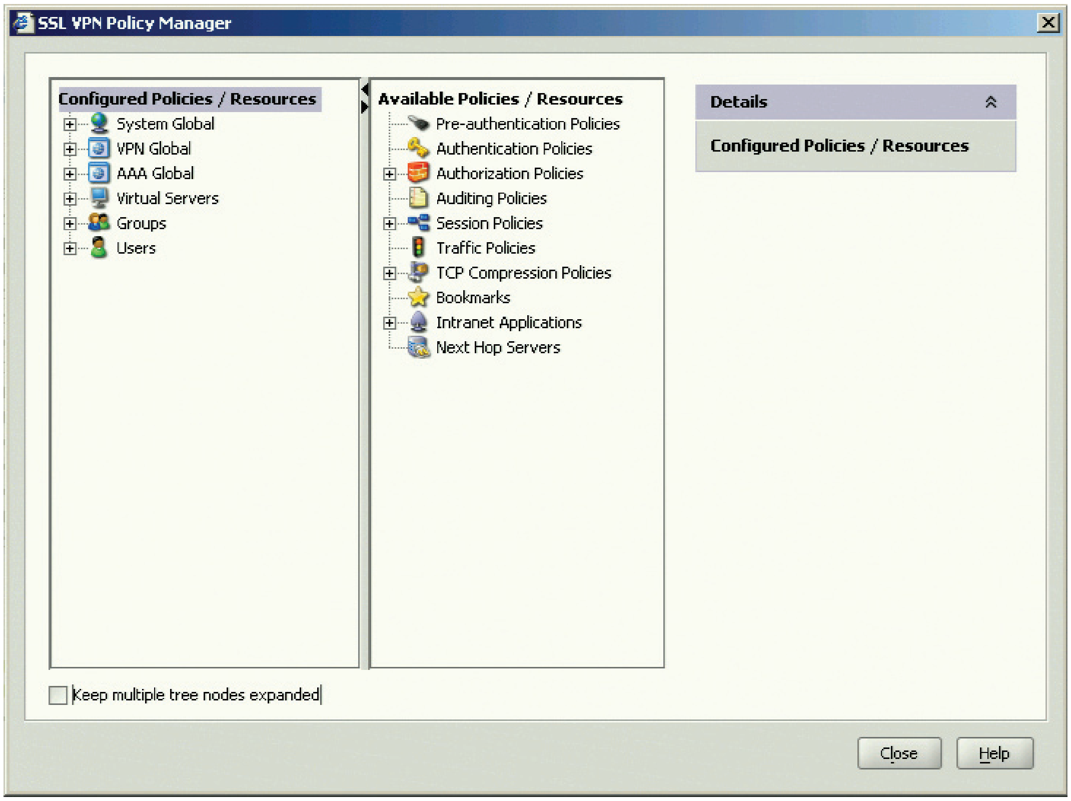
Intranet Applications policy

Intranet Applications are applications which can be accessed through the VPN. When split tunneling in ON, only traffic to the configured intranet applications are tunnelled through the VPN.

Intranet IPs policy

Intranet IP Addresses allow you to provide a range of IP Addresses to be used as a resource for a defined group of users. Think of it as a built-in DHCP server. it works off of the CIDR principle, so you will need to break out your subnet calculator.

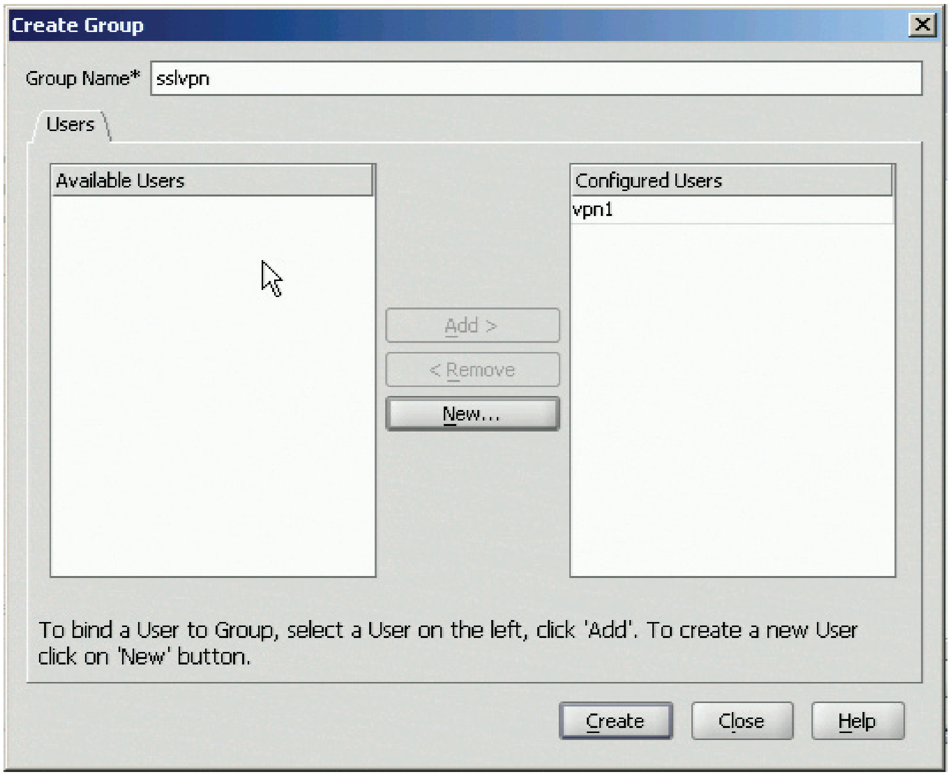
Step-by-Step SSL VPN policy creation



22. The first thing to do is launch the SSL VPN Policy Manager.

From the GUI, navigate to NetScaler ➥ SSL VPN. In the right-side frame, second from the top, click on <SSL VPN Manager>

Up pops the SSL VPN Manager GUI.



Group Name* sslvpn

Configured Users: vpn1

To bind a User to Group, select a User on the left, click 'Add'. To create a new User click on 'New' button.

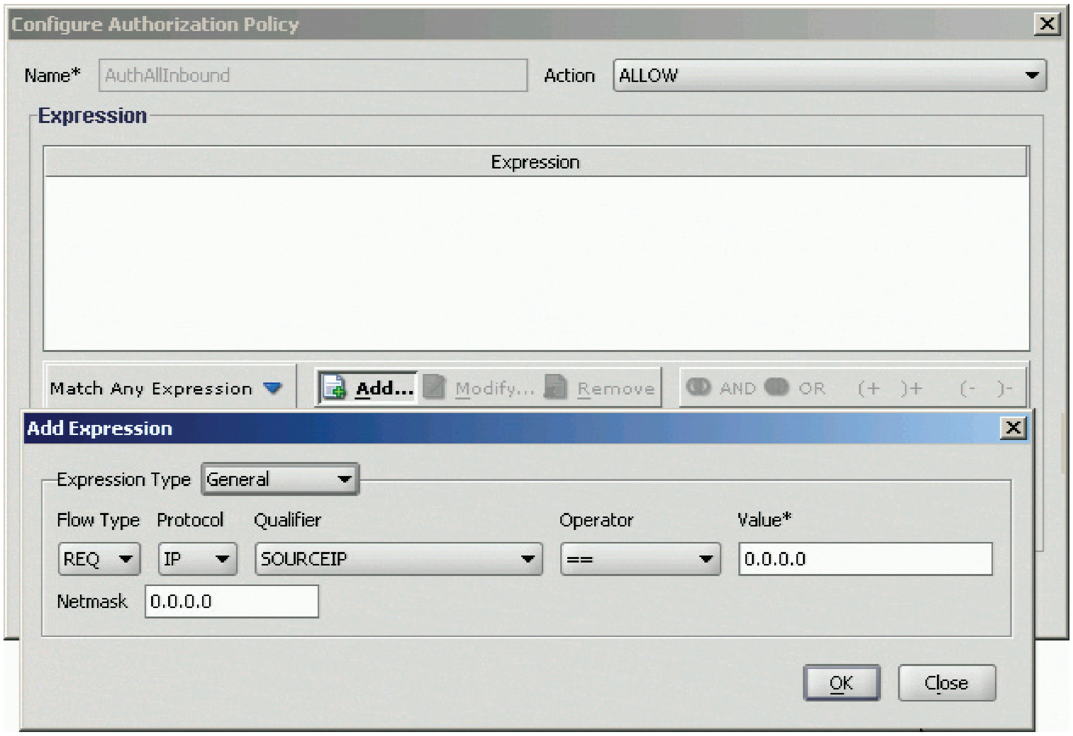
23. Create a new group to assign our policies to.

In this example, we create a group called 'sslvpn'.

We add our vpn user 'vpn1' to this group.

24. The first Authorization policy we create is to allow anyone to come into the VPN.

    So our first Auth policy is REQ.IP.SOURCEIP == 0.0.0.0 -netmask 0.0.0.0.



Configure Authorization Policy

Name* AuthAllInbound Action ALLOW

Add Expression

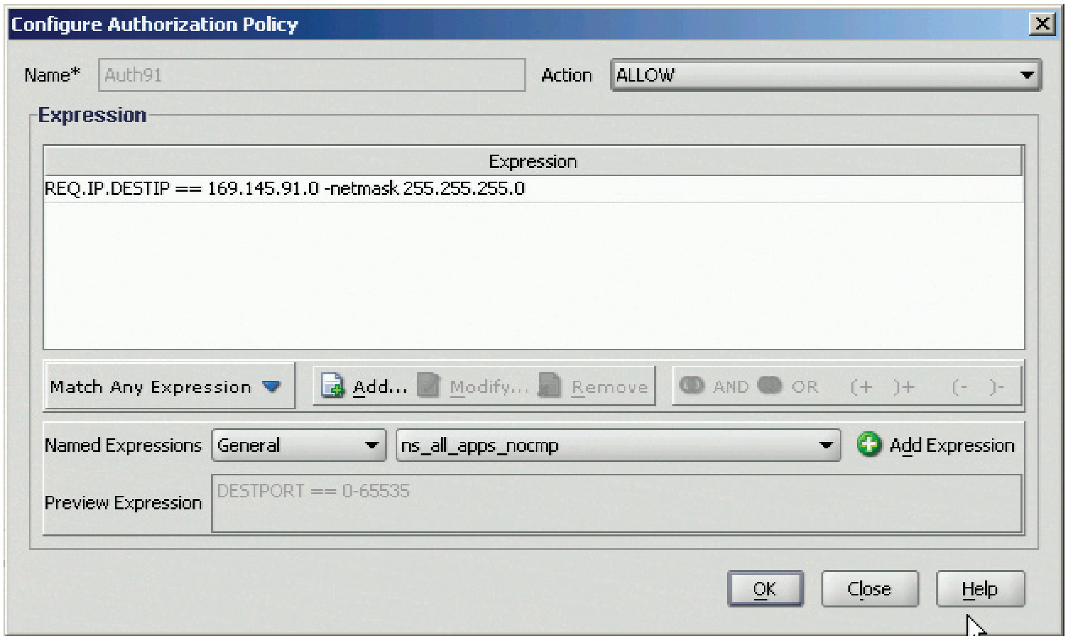
Expression Type: General

Flow Type: REQ Protocol: IP Qualifier: SOURCEIP Operator: == Value*: 0.0.0.0

Netmask: 0.0.0.0

25. The second Authorization policy we create is to only allow users who are destined for the 91 Subnet which is also VLAN 91.

    So our second Auth policy is REQ.IP.DESTIP == 169.145.91.0 -netmask 255.255.255.0.



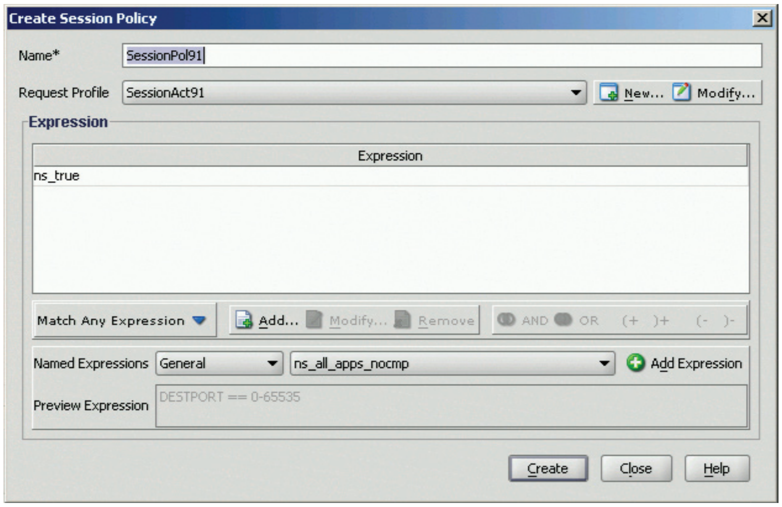
Configure Authorization Policy

Name* Auth91 Action ALLOW

Expression: REQ.IP.DESTIP == 169.145.91.0 -netmask 255.255.255.0

Named Expressions: General ns_all_apps_nocmp

Preview Expression: DESTPORT == 0-65535



Create Session Policy

Name* SessionPol91

Request Profile SessionAct91

Expression

ns_true

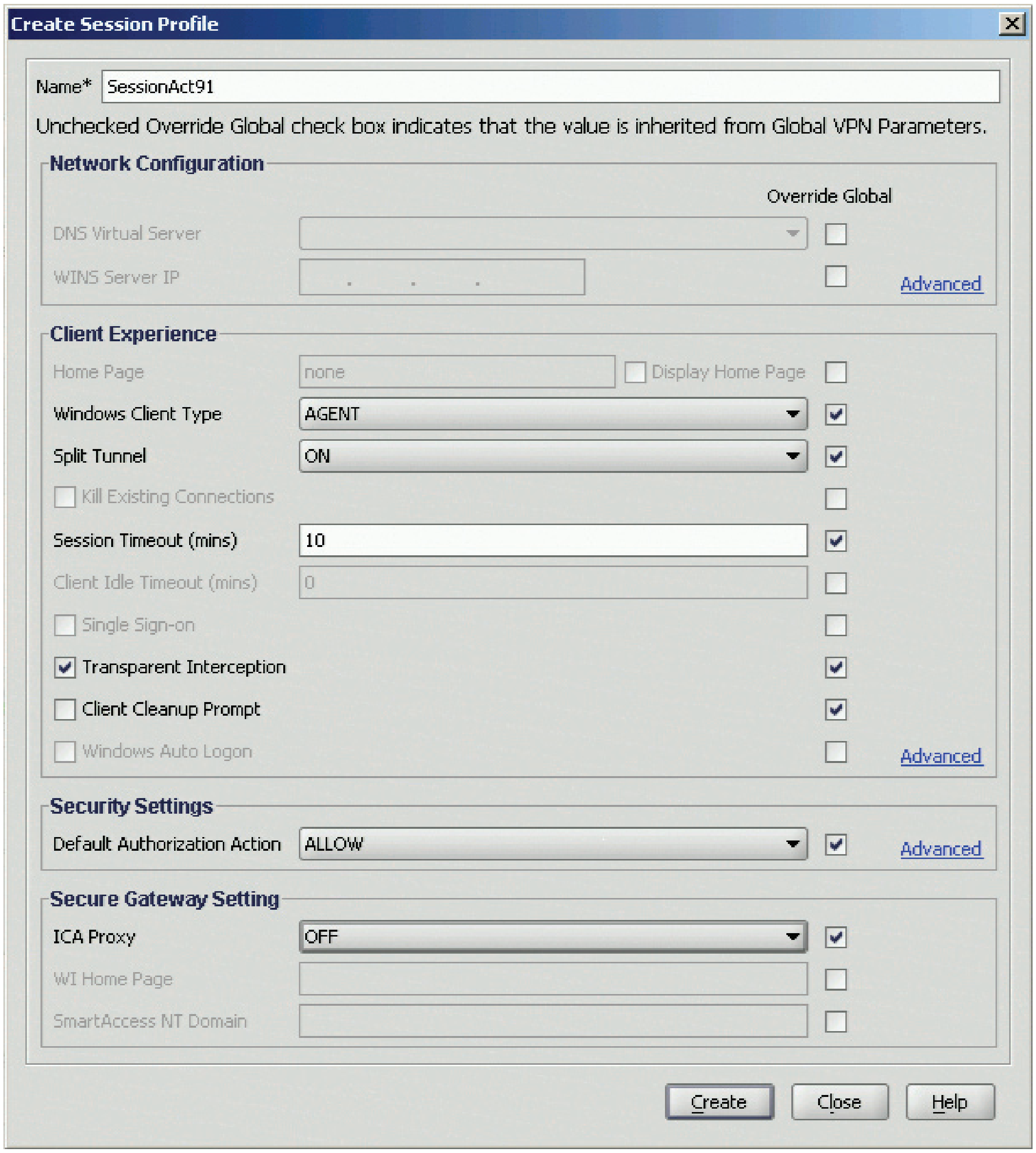
Match Any Expression

Named Expressions General ns_all_apps_nocmp

Preview Expression DESTPORT == 0-65535

26. The next step is to Create a New Session Policy.

Add an expression to match 'ns_true' so the policy evaluates to true.



Create Session Profile

Name* SessionAct91

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

Network Configuration

Override Global

DNS Virtual Server □

WINS Server IP . . . □

Client Experience

Home Page none □ Display Home Page □

Windows Client Type AGENT ☑

Split Tunnel ON ☑

□ Kill Existing Connections □

Session Timeout (mins) 10 ☑

Client Idle Timeout (mins) 0 □

□ Single Sign-on □

☑ Transparent Interception ☑

□ Client Cleanup Prompt ☑

□ Windows Auto Logon □

Security Settings

Default Authorization Action ALLOW ☑

Secure Gateway Setting

ICA Proxy OFF ☑

WI Home Page □

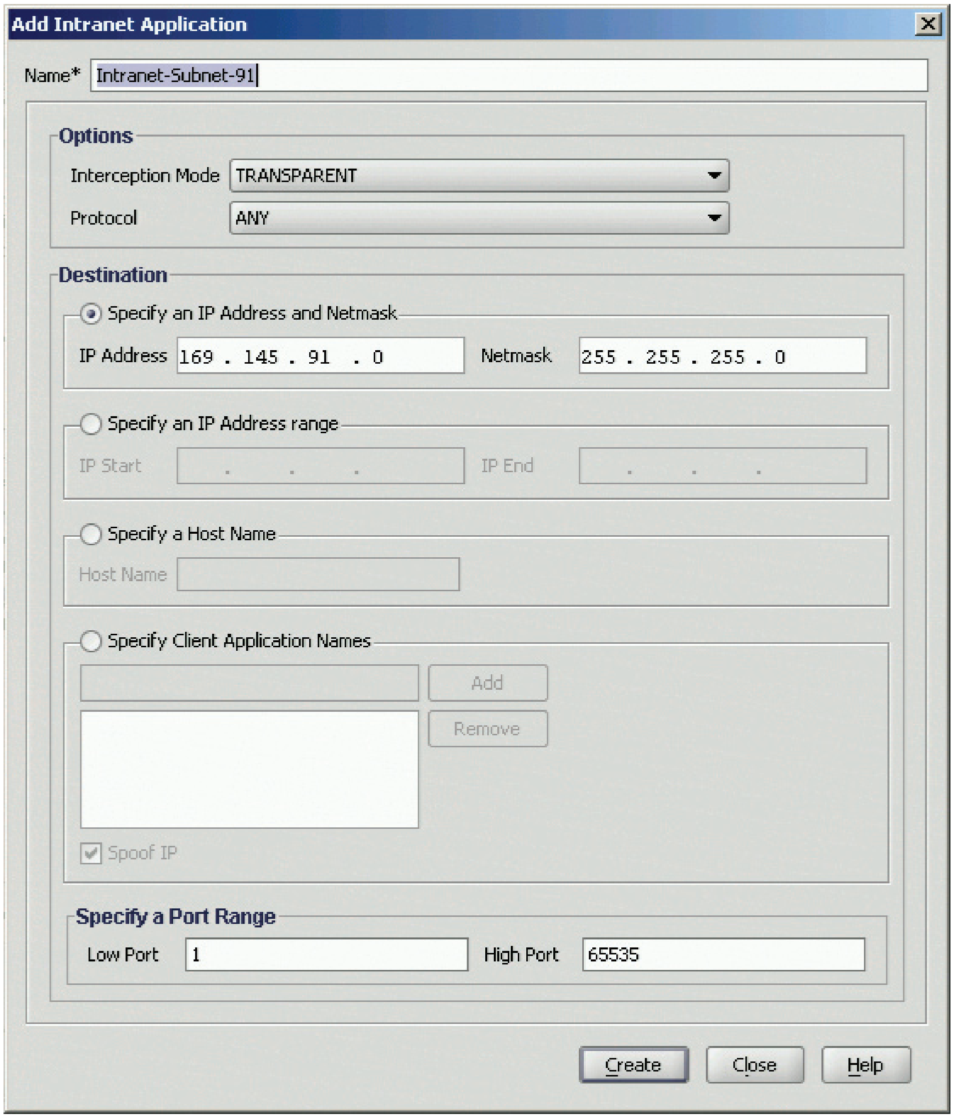
SmartAccess NT Domain □

27. And the Session Action which dictates all of the end user 'Client' behavior.

Here we are configuring Windows clients to use the Agent client with Split Tunneling, a session timeout and transparent inspection.

We selected Advanced settings and configured the VPN to automatically cleanup the clients files when they logout of the VPN.

28. Create an Intranet policy to allow users access to Subnet 91 (Vlan 91).



Add Intranet Application

Name* Intranet-Subnet-91

Options

Interception Mode TRANSPARENT

Protocol ANY

Destination

● Specify an IP Address and Netmask

IP Address 169 . 145 . 91 . 0   Netmask 255 . 255 . 255 . 0

○ Specify an IP Address range

IP Start . . .   IP End . . .

○ Specify a Host Name

Host Name

○ Specify Client Application Names

☑ Spoof IP

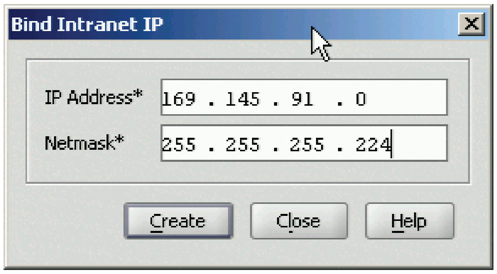
Specify a Port Range

Low Port 1   High Port 65535

29. Finally bind an IP Subnet range for users to be assigned IP Addresses from. This can only done directly to the resources in the left-side frame of the SSL VPN Policy Manager.

Open up the ‘sslvpn’ group created earlier, under ‘Intranet IPs’, bind new intranet ip.

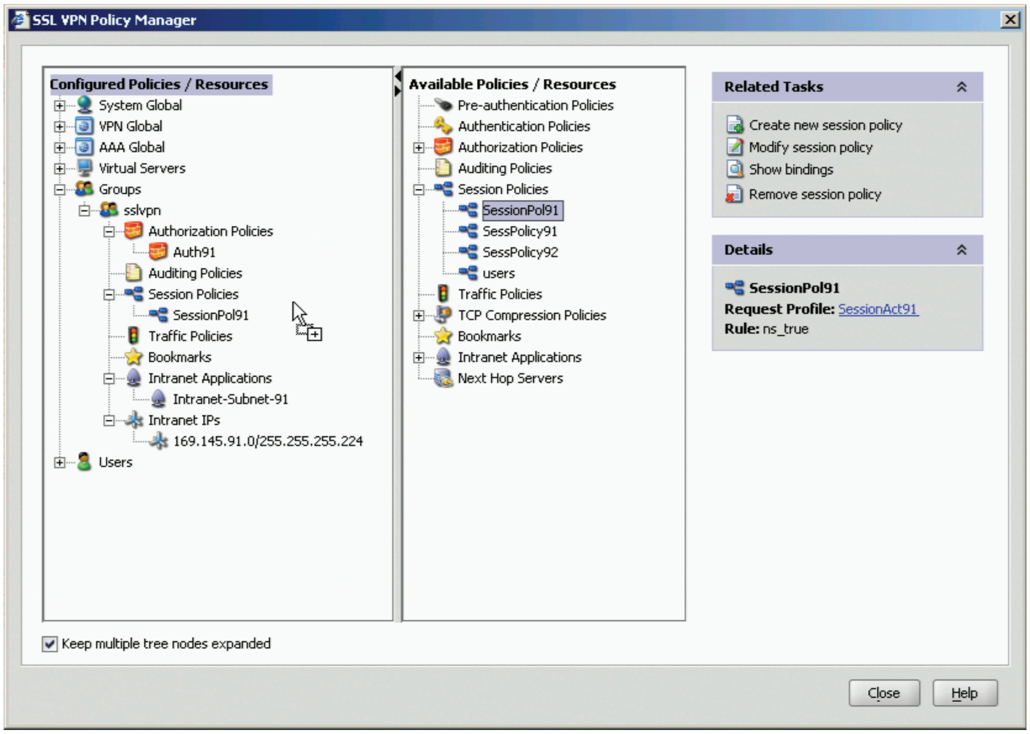
Think of this as a built-in DHCP server that assigns IP Addresses.



Bind Intranet IP

IP Address* 169 . 145 . 91 . 0

Netmask* 255 . 255 . 255 . 224

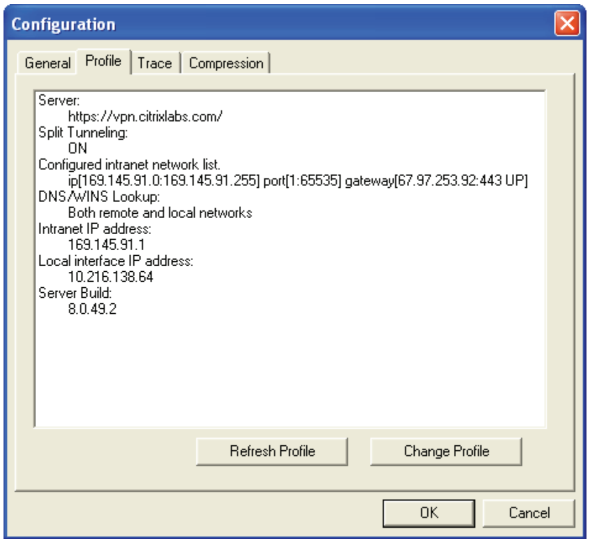


SessionPol91
Request Profile: SessionAct91
Rule: ns_true

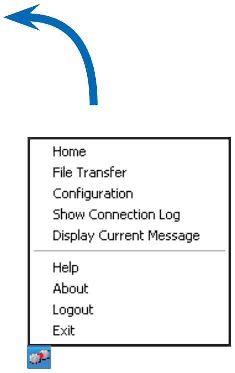
☑ Keep multiple tree nodes expanded

30. Finally, bind all of these policies together to the 'sslvpn' group, so that when the user 'vpn1' logs in, they are bound to those policies.

    Do this by click-hold and drag from the Available Policies frame in the center of the SSL VPN Policy Manager, to the Configured Policies in the left-side frame, under groups, 'sslvpn'.



```
Server:
     https://vpn.citrixlabs.com/
Split Tunneling:
     ON
Configured intranet network list:
     ip[169.145.91.0:169.145.91.255] port[1:65535] gateway[67.97.253.92:443 UP]
DNS/WINS Lookup:
     Both remote and local networks
Intranet IP address:
     169.145.91.1
Local interface IP address:
     10.216.138.64
Server Build:
     8.0.49.2
```



31. Test the connection from a client machine.

    After logging into the SSL VPN, do a right-click on the ActiveX client in the system trap, and select Configure.

    Here you can view the configuration details for the client to see if the policies were correctly pushed down to the client.

    From the same client, right-click to logout of the SSL VPN.

Appendix A - NetScaler Application Switch Configuration

Primary NetScaler

```
#NS8.0 Build 49.2

# Last modified by `save config`, Sun Dec 23 23:21:57 2007

set ns config -IPAddress 10.217.104.51 -netmask 255.255.255.0

enable ns feature CMP SSLVPN SSL

set lacp -sysPriority 32768

set system user nsroot 1b8c0fd3800004c04ecd8f170ec96e3d2c597e739e223fced -encrypted

set interface 0/1 -speed AUTO -duplex AUTO -autoneg ENABLED -haMonitor ON -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/1 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/2 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/3 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/4 -speed 1000 -duplex FULL -flowControl RX -autoneg DISABLED -haMonitor OFF -trunk ON -lacpMode DISABLED -throughput 0

set interface 1/5 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/6 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/7 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/8 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

add HA node 2 10.217.104.52

add ns ip 10.217.104.54 255.255.255.0 -vServer DISABLED -gui SECUREONLY -mgmtAccess ENABLED

add ns ip 169.145.91.239 255.255.255.0 -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add ns ip 169.145.92.239 255.255.255.0 -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add ns ip 169.145.92.240 255.255.255.0 -type MIP -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED
add ns ip 169.145.91.240 255.255.255.0 -type MIP -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add ns ip 10.217.104.50 255.255.255.0 -type MIP -vServer DISABLED -gui SECUREONLY -mgmtAccess ENABLED

add ns ip 67.97.253.91 255.255.255.0 -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add vlan 4

add vlan 10

add vlan 91

add vlan 92

bind vlan 4 -ifnum 1/4

bind vlan 10 -ifnum 1/2

bind vlan 10 -IPAddress 67.97.253.91 255.255.255.0

bind vlan 91 -ifnum 1/4 -tagged

bind vlan 91 -IPAddress 169.145.91.239 255.255.255.0

bind vlan 92 -ifnum 1/4 -tagged

bind vlan 92 -IPAddress 169.145.92.240 255.255.255.0

add vrID 60

bind vrID 60 -ifnum 0/1

set locationParameter -context geographic -q1label Continent -q2label Country -q3label Region -q4label City -q5label ISP -q6label Organization

add policy expression users “SOURCEIP == 0.0.0.0 -netmask 0.0.0.0”

add aaa user vpn1 -password c83f1e11 -encrypted

add aaa group sslvpn

add vpn intranetApplication Intranet-Subnet-91 ANY 169.145.91.0 -netmask 255.255.255.0 -destPort 1-65535 -interception TRANSPARENT

add authorization policy Auth91 “REQ.IP.DESTIP == 169.145.91.0 -netmask 255.255.255.0” ALLOW

add authorization policy AuthAllInbound “REQ.IP.SOURCEIP == 0.0.0.0 -netmask 0.0.0.0” ALLOW

add vpn vserver vpn.citrixlabs.com SSL 67.97.253.92 443 -maxAAAUsers 5 -downStateFlush DISABLED

set ns rpcNode 10.217.104.51 -password 8a7b474124957776a0cd31b862cbe4d72b5cbd59868a136d4bdeb56cf03b28 -encrypted -srcIP 10.217.104.51

set ns rpcNode 10.217.104.52 -password 8a7b474124957776a0cd31b862cbe4d72b5cbd59868a136d4bdeb56cf03b28 -encrypted -srcIP 10.217.104.51

set responder param -undefAction NOOP

set rewrite param -undefAction NOREWRITE
```

```
add dns nameServer 66.165.176.28 -state DISABLED

set dns parameter -nameLookupPriority DNS

add ssl certKey ns-server-certificate -cert ns-server.cert -key ns-server.key

add ssl certKey citrixlabs.keypair -cert citrixlabs.cer -key citrixlabs.key -inform DER

set ssl service nshttps-67.97.253.91-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-67.97.253.91-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-10.217.104.50-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-10.217.104.50-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.91.240-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.91.240-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.92.240-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.92.240-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.92.239-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.92.239-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.91.239-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.91.239-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-10.217.104.54-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-10.217.104.54-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nskrpcs-127.0.0.1-3009 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-127.0.0.1-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-127.0.0.1-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set cache parameter -memLimit 0 -via “NS-CACHE-8.0:    1” -verifyUsing HOSTNAME_AND_IP -maxPostLen 0 -prefetchMaxPending 4294967294 -enableBypass YES

set cache contentGroup BASEFILE -relExpiry 86000 -maxResSize 256 -memLimit 2

set cache contentGroup DELTAJS -relExpiry 86000 -insertAge NO -maxResSize 256 -memLimit 1 -pinned YES

set aaa parameter -maxAAAUsers 5

add vpn sessionAction SessAction91 -windowsClientType AGENT -defaultAuthorizationAction ALLOW -homePage http://169.145.91.151/Citrix/AccessPlatform/ -icaProxy ON -ntDomain Srv1

add vpn sessionAction SessAction92 -homePage http://169.145.92.152/Citrix/AccessPlatform/ -icaProxy ON -ntDomain Srv2

add vpn sessionAction userAction -sessTimeout 20 -windowsClientType AGENT
add vpn sessionAction SessionAct91 -sessTimeout 10 -splitTunnel ON -transparentInterception ON -windowsClientType AGENT -defaultAuthorizationAction ALLOW -clientCleanupPrompt OFF -forceCleanup all -homePage none -icaProxy OFF

add vpn sessionPolicy SessPolicy91 ns_true SessAction91

add vpn sessionPolicy SessPolicy92 ns_true SessAction92

add vpn sessionPolicy users “REQ.IP.SOURCEIP == 0.0.0.0 -netmask 0.0.0.0” userAction

add vpn sessionPolicy SessionPol91 ns_true SessionAct91

set aaa preauthenticationparameter -preauthenticationaction ALLOW -rule ns_true

set vpn parameter -splitDns BOTH -splitTunnel ON -killConnections OFF -defaultAuthorizationAction DENY -proxy OFF -proxyLocalBypass DISABLED -forceCleanup all -clientOptions all -clientConfiguration all -SSO OFF -windowsAutoLogon OFF -clientDebug OFF -homePage none -icaProxy OFF -ClientChoices OFF -epaClientType PLUGIN

bind aaa group sslvpn -userName vpn1

bind aaa group sslvpn -intranetIP 169.145.91.0 255.255.255.224

bind aaa group sslvpn -policy Auth91

bind aaa group sslvpn -policy SessionPol91

bind aaa group sslvpn -intranetApplication Intranet-Subnet-91

bind tunnel global ns_tunnel_cmpall_gzip

set lb sipParameters -addRportVip ENABLED

bind ssl service nshttps-67.97.253.91-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-67.97.253.91-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-10.217.104.50-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-10.217.104.50-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.91.240-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.91.240-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.92.240-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.92.240-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.92.239-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.92.239-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.91.239-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.91.239-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-10.217.104.54-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-10.217.104.54-3008 -certkeyName ns-server-certificate

bind ssl service nskrpcs-127.0.0.1-3009 -certkeyName ns-server-certificate
bind ssl service nshttps-127.0.0.1-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-127.0.0.1-3008 -certkeyName ns-server-certificate

bind ssl vserver vpn.citrixlabs.com -certkeyName citrixlabs.keypair

set ns hostName nsPrimary
```

Secondary NetScaler

```
#NS8.0 Build 49.2

# Last modified by `save config`, Fri Dec 21 22:27:18 2007

set ns config -IPAddress 10.217.104.52 -netmask 255.255.255.0

enable ns feature CMP SSLVPN SSL

set lacp -sysPriority 32768

set system user nsroot 1b8c0fd3800004c04ecd8f170ec96e3d2c597e739e223fced -encrypted

set interface 0/1 -speed AUTO -duplex AUTO -autoneg ENABLED -haMonitor ON -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/1 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/2 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -state DISABLED -lacpMode DISABLED -throughput 0

set interface 1/3 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/4 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk ON -lacpMode DISABLED -throughput 0

set interface 1/5 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/6 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/7 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

set interface 1/8 -speed AUTO -duplex AUTO -flowControl RX -autoneg ENABLED -haMonitor OFF -trunk OFF -lacpMode DISABLED -throughput 0

add HA node 1 10.217.104.51

add ns ip 10.217.104.54 255.255.255.0 -vServer DISABLED -gui SECUREONLY -mgmtAccess ENABLED

add ns ip 169.145.91.239 255.255.255.0 -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add ns ip 169.145.92.239 255.255.255.0 -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add ns ip 169.145.92.240 255.255.255.0 -type MIP -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED
```

```
-snmp DISABLED

add ns ip 169.145.91.240 255.255.255.0 -type MIP -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add ns ip 10.217.104.50 255.255.255.0 -type MIP -vServer DISABLED -gui SECUREONLY -mgmtAccess ENABLED

add ns ip 67.97.253.91 255.255.255.0 -vServer DISABLED -telnet DISABLED -ftp DISABLED -gui DISABLED -ssh DISABLED -snmp DISABLED

add vlan 4

add vlan 10

add vlan 91

add vlan 92

bind vlan 4 -ifnum 1/4

bind vlan 10 -ifnum 1/2

bind vlan 10 -IPAddress 67.97.253.91 255.255.255.0

bind vlan 91 -ifnum 1/4 -tagged

bind vlan 91 -IPAddress 169.145.91.239 255.255.255.0

bind vlan 92 -ifnum 1/4 -tagged

bind vlan 92 -IPAddress 169.145.92.240 255.255.255.0

add vrID 60

bind vrID 60 -ifnum 0/1

set locationParameter -context geographic -q1label Continent -q2label Country -q3label Region -q4label City -q5label ISP -q6label Organization

add policy expression users “SOURCEIP == 0.0.0.0 -netmask 0.0.0.0”

add aaa user vpn1 -password c83f1e11 -encrypted

add aaa group sslvpn

add vpn intranetApplication Intranet-Subnet-91 ANY 169.145.91.0 -netmask 255.255.255.0 -destPort 1-65535 -interception TRANSPARENT

add authorization policy Auth91 “REQ.IP.DESTIP == 169.145.91.0 -netmask 255.255.255.0” ALLOW

add authorization policy AuthAllInbound “REQ.IP.SOURCEIP == 0.0.0.0 -netmask 0.0.0.0” ALLOW

add vpn vserver vpn.citrixlabs.com SSL 67.97.253.92 443 -maxAAAUsers 5 -downStateFlush DISABLED

set ns rpcNode 10.217.104.52 -password 8a7b474124957776a0cd31b862cbe4d72b5cbd59868a136d4bdeb56cf03b28 -encrypted -srcIP 10.217.104.52

set ns rpcNode 10.217.104.51 -password 8a7b474124957776a0cd31b862cbe4d72b5cbd59868a136d4bdeb56cf03b28 -encrypted -srcIP 10.217.104.52

set responder param -undefAction NOOP
set rewrite param -undefAction NOREWRITE

add dns nameServer 66.165.176.28 -state DISABLED

set dns parameter -nameLookupPriority DNS

add ssl certKey ns-server-certificate -cert ns-server.cert -key ns-server.key

add ssl certKey citrixlabs.keypair -cert citrixlabs.cer -key citrixlabs.key -inform DER

set ssl service nshttps-67.97.253.91-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-67.97.253.91-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-10.217.104.50-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-10.217.104.50-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.91.240-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.91.240-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.92.240-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.92.240-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.92.239-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.92.239-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-169.145.91.239-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-169.145.91.239-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-10.217.104.54-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-10.217.104.54-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nskrpcs-127.0.0.1-3009 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nshttps-127.0.0.1-443 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set ssl service nsrpcs-127.0.0.1-3008 -sessReuse ENABLED -sessTimeout 120 -cipherRedirect DISABLED -sslv2Redirect DISABLED

set cache parameter -memLimit 0 -via “NS-CACHE-8.0:    1” -verifyUsing HOSTNAME_AND_IP -maxPostLen 0 -prefetchMaxPending 4294967294 -enableBypass YES

set cache contentGroup BASEFILE -relExpiry 86000 -maxResSize 256 -memLimit 2

set cache contentGroup DELTAJS -relExpiry 86000 -insertAge NO -maxResSize 256 -memLimit 1 -pinned YES

set aaa parameter -maxAAAUsers 5

add vpn sessionAction SessAction91 -windowsClientType AGENT -defaultAuthorizationAction ALLOW -homePage http://169.145.91.151/Citrix/AccessPlatform/ -icaProxy ON -ntDomain Srv1

add vpn sessionAction SessAction92 -homePage http://169.145.92.152/Citrix/AccessPlatform/ -icaProxy ON -ntDomain Srv2
add vpn sessionAction userAction -sessTimeout 20 -windowsClientType AGENT

add vpn sessionAction SessionAct91 -sessTimeout 10 -splitTunnel ON -transparentInterception ON -windowsClientType AGENT -defaultAuthorizationAction ALLOW -clientCleanupPrompt OFF -forceCleanup all -homePage none -icaProxy OFF

add vpn sessionPolicy SessPolicy91 ns_true SessAction91

add vpn sessionPolicy SessPolicy92 ns_true SessAction92

add vpn sessionPolicy users “REQ.IP.SOURCEIP == 0.0.0.0 -netmask 0.0.0.0” userAction

add vpn sessionPolicy SessionPol91 ns_true SessionAct91

set aaa preauthenticationparameter -preauthenticationaction ALLOW -rule ns_true

set vpn parameter -splitDns BOTH -splitTunnel ON -killConnections OFF -defaultAuthorizationAction DENY -proxy OFF -proxyLocalBypass DISABLED -forceCleanup all -clientOptions all -clientConfiguration all -SSO OFF -windowsAutoLogon OFF -clientDebug OFF -homePage none -icaProxy OFF -ClientChoices OFF -epaClientType PLUGIN

bind aaa group sslvpn -userName vpn1

bind aaa group sslvpn -intranetIP 169.145.91.0 255.255.255.224

bind aaa group sslvpn -policy Auth91

bind aaa group sslvpn -policy SessionPol91

bind aaa group sslvpn -intranetApplication Intranet-Subnet-91

bind tunnel global ns_tunnel_cmpall_gzip

set lb sipParameters -addRportVip ENABLED

bind ssl service nshttps-67.97.253.91-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-67.97.253.91-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-10.217.104.50-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-10.217.104.50-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.91.240-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.91.240-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.92.240-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.92.240-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.92.239-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.92.239-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-169.145.91.239-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-169.145.91.239-3008 -certkeyName ns-server-certificate

bind ssl service nshttps-10.217.104.54-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-10.217.104.54-3008 -certkeyName ns-server-certificate
bind ssl service nskrpcs-127.0.0.1-3009 -certkeyName ns-server-certificate

bind ssl service nshttps-127.0.0.1-443 -certkeyName ns-server-certificate

bind ssl service nsrpcs-127.0.0.1-3008 -certkeyName ns-server-certificate

bind ssl vserver vpn.citrixlabs.com -certkeyName citrixlabs.keypair

set ns hostName nsSecondary
```

Citrix Worldwide

Worldwide headquarters

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA
T +1 800 393 1888
T +1 954 267 3000

Regional headquarters

Americas
Citrix Silicon Valley
4988 Great America Parkway
Santa Clara, CA 95054
USA
T +1 408 790 8000

Europe
Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen
Switzerland
T +41 52 635 7700

Asia Pacific
Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central
Hong Kong
T +852 2100 5000

Citrix Online division
5385 Hollister Avenue
Santa Barbara, CA 93111
USA
T +1 805 690 6400

www.citrix.com

About Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) is the global leader and the most trusted name in application delivery infrastructure. More than 200,000 organizations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost. Citrix customers include 100% of the Fortune 100 companies and 98% of the Fortune Global 500, as well as hundreds of thousands of small businesses and prosumers. Citrix has approximately 6,200 channel and alliance partners in more than 100 countries. Annual revenue in 2006 was $1.1 billion.

www.citrix.com