Deployment Guide for Microsoft SharePoint 2010

Securing and Accelerating Microsoft SharePoint with Palo Alto Networks Next-Generation Firewall and Citrix NetScaler Joint Solution

Table of Contents

1. Overview

Business productivity hinges on providing users of IT resources secure access to the right applications and the right content – on demand. Enterprise IT strategies are rapidly evolving to support a world in which any user can safely access any application or data, using any device, from any location.

One of the biggest impediments in achieving this degree of flexibility is the enterprise network. Legacy networks were built to provide highly reliable connectivity between users, hosts, and networks, but with no awareness or context of application-layer traffic. This inherently limits the ability of the network to deliver to users the secure and transparent access to apps, data and virtual desktops they need to be productive, and to protect the organization from attack. What is required is a new approach – a next-generation cloud network that safely enables applications with the best-in-class performance and availability.

Palo Alto Networks and Citrix have come together to deliver best-in-class functionality upon which enterprises can build next-generation cloud networks. In addition to sharing a common vision of which networks must evolve, each company is delivering best-in-class solutions that already meet these requirements.

1.1 Best-in-class Solution for Microsoft Sharepoint 2010

Enabling worldwide collaboration, either within the enterprise or over the Internet, Microsoft SharePoint allows people to share ideas and expertise, create custom solutions for specific requirements and find the right information to quickly respond to changing business needs.

With SharePoint 2010, the opportunity to optimize, secure, and maximize SharePoint value has never been greater. This version brings an extensive list of features ranging from business connectivity and Visio services to detailed user profiles and a richer user interface. With these features, however, there is an increase in complexity to the client/server interaction and an increase to overall WAN traffic volume.

Customers have long deployed Citrix NetScaler with SharePoint to reduce processing overhead, accelerate server response times and increase availability and service capacity. Customers have also deployed Palo Alto Networks next-generation firewalls to safely enable SharePoint applications. Both Citrix and Palo Alto Networks have extensive experience working with Microsoft in validating interoperability and verifying benefits of the combined solution.

NetScaler and Palo Alto Networks enhance SharePoint by significantly reducing processing overhead, server response times, and site-wide security. For SharePoint installations, this means an industry-leading solution driving the highest return on investment without sacrificing agility or total cost of ownership (TCO).

To leverage a combined best-in-class solution, this document provides a concise set of step-by-step deployment instructions required to configure a Citrix NetScaler application delivery controller and Palo Alto Networks next-generation firewalls to accelerate and safely enable a Microsoft Office SharePoint 2010 deployment.

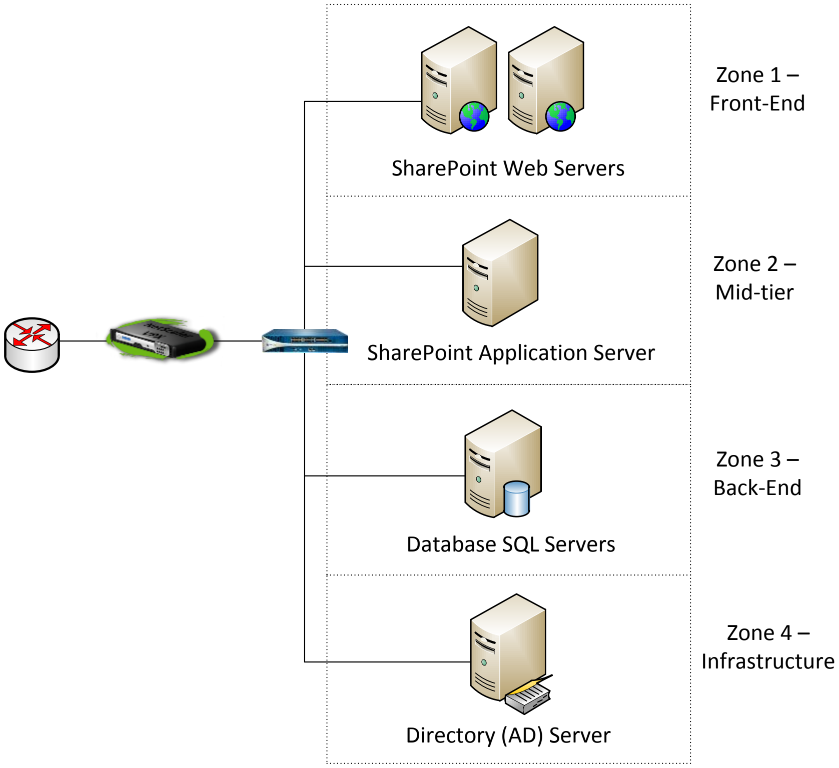
2. Requirements

Required Component	Used in this Document	Note
Citrix NetScaler ADC	NS10.0 VPX Build 69.4.nc with Platinum License	

Palo Alto Networks Next-Generation Firewall	PAN-OS 4.1	
Microsoft SharePoint 2010 Servers	5 Physical/VM servers	2x Web; 1x App; 1x DB; 1x AD
AppExpert SharePoint Template	Template File	http://community.citrix.com/download/attachments/49186776/SharePoint_2010.xml
	Deployment File	http://community.citrix.com/download/attachments/49186776/SharePoint_2010_deployment.xml

3. Microsoft SharePoint Network Topology

3.1 Environment diagram



3.2 IP allocations

The following IP addresses were allocated to this reference environment.

Functional Device	IP	Subnet Mask
NetScaler IP (NSIP)	10.5.172.124	255.255.255.0
NetScaler Subnet IP (SNIP)	10.5.172.126	255.255.255.0

SharePoint Virtual IP (VIP)	10.5.172.156	255.255.255.0
SharePoint Web Server 1	10.5.172.150	255.255.255.0
SharePoint Web Server 2	10.5.172.151	255.255.255.0
SharePoint App Server	10.5.172.153	255.255.255.0
Database SQL Server	10.5.172.152	255.255.255.0
Active Directory Server	10.5.172.155	255.255.255.0

4. SharePoint AppExpert Template Installation and Configuration

Configuring Citrix NetScaler for Microsoft SharePoint 2010 is made up of 5 key steps:

1. Setup the underlying network
2. License the system
3. Configure the policies for Microsoft Sharepoint 2010
4. Setup SSL
5. Setup which servers will receive traffic from the NetScaler

The third step in particular is noteworthy.

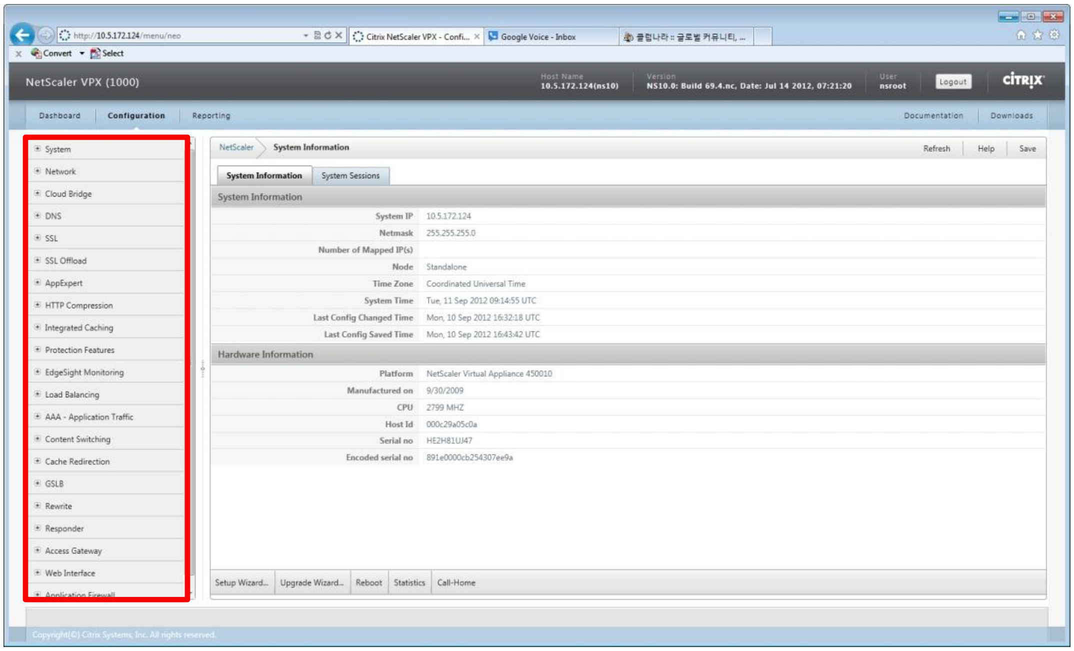
Traditionally, there are numerous policies that must be configured to correctly enable all of the features for optimal traffic management for Microsoft SharePoint. Everything from traffic switching to optimization is affected in this step. With Citrix NetScaler, we are able to leverage the AppExpert AppTemplate for Microsoft SharePoint 2010 which provides a single configuration file to load in order to get all of the correct settings configured.

For additional AppExpert Templates for other applications, visit http://community.citrix.com/display/ns/AppExpert+Templates.

The AppExpert Templates published by Citrix do not contain certain application and custom environment specific parameter settings. Elements which are not predefined include IP addresses, number of servers, SSL parameters and others. The following steps show where and how each custom data will be added.

4.1 NetScaler Configuration

During the installation and configuration process, from the main NetScaler screen, administrators will be able to navigate the menu (in red) panel to configure application specific parameters or to confirm data already populated by the template.



Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

System Information

System IP	10.5.172.124
Netmask	255.255.255.0
Number of Mapped IP(s)	
Node	Standalone
Time Zone	Coordinated Universal Time
System Time	Tue, 11 Sep 2012 09:14:55 UTC
Last Config Changed Time	Mon, 10 Sep 2012 16:32:18 UTC
Last Config Saved Time	Mon, 10 Sep 2012 16:43:42 UTC

Hardware Information

Platform	NetScaler Virtual Appliance 450010
Manufactured on	9/30/2009
CPU	2799 MHZ
Host Id	000c29a05c0a
Serial no	HE2H81UJ47
Encoded serial no	891e0000cb254307ee9a

Copyright(©) Citrix Systems, Inc. All rights reserved.

The table below summarizes the specific menu and actions within NetScaler which need to be configured properly in order to complete the SharePoint configuration:

NetScaler Menu	NetScaler Sub-Menu	Action	Comment
System	Licenses	Manage Licenses	Custom added*
	Settings	Configure basic features	Custom added*
Network	IPs	NetScaler IP, Subnet IP	Custom added*
		Virtual IP	Auto added **
SSL	Certificate	Root-CA, Server	Custom added*
SSL Offload	Servers	Per VM/Physical Server	Auto added
	Service Group	Per Port	Auto added
AppExpert	Applications	Import	Custom added*
		Configure Public Endpoints	Custom added*
		Configure Backend Services	Custom added*
Load Balancing	Servers	Per VM/Physical Server	Auto added
	Service Group	Per Port	Auto added
Content Switching	Virtual Servers	Per VM/Physical Server	Auto added

** Please refer below section 4.2 Step-by-Step Installation for custom environment setup*
*** Auto added –The data will be populated automatically when the template is installed and 'Custom added' data is added (Please do not modify manually 'Auto added' data)*

4.2 Step –by-Step Installation

The following steps are required to get downloaded SharePoint AppExpert template installed and operational.

Step	Action	Detail	Custom Data
1	NetScaler IP, Subnet IP	NetScaler initial Configurations (by Setup Wizard)	NetScaler IP (NSIP), Subnet IP (SNIP)
2	Manage Licenses	NetScaler license installation	.lic license file
3	Configure basic features	NetScaler basic feature settings	Feature settings

4	Import AppExpert Template	Template Import	Template, Deployment files (XML format)
5	Root-CA, Server Certificates	Security Certificate Installation	
6	Configure Public Endpoints	Creating virtual servers (IP) to talk to multiple backend servers	SharePoint Virtual IP (VIP)
7	Configure Backend Services	Creating a Service Group	IPs for Web Server 1 and Web Server 2

5. Deployment Instruction

This section will describe detailed steps from NetScaler VPX installation and initial configuration to SharePoint AppExpert template download to full SharePoint service configuration within NetScaler.

5.1 NetScaler Initial Configurations

Administrators can use the NetScaler command-line to set up the initial NSIP, Mapped IP (MIP), and Subnet IP (SNIP). You can also configure advanced network settings and change the time zone.

For information about MIP, SNIP, other NetScaler-owned IP addresses, and network settings, see the "*Citrix NetScaler Networking Guide"* at http://support.citrix.com/article/CTX132369.

5.1.1 Add NSIP, Subnet Mask, and Default Gateway on NetScaler:

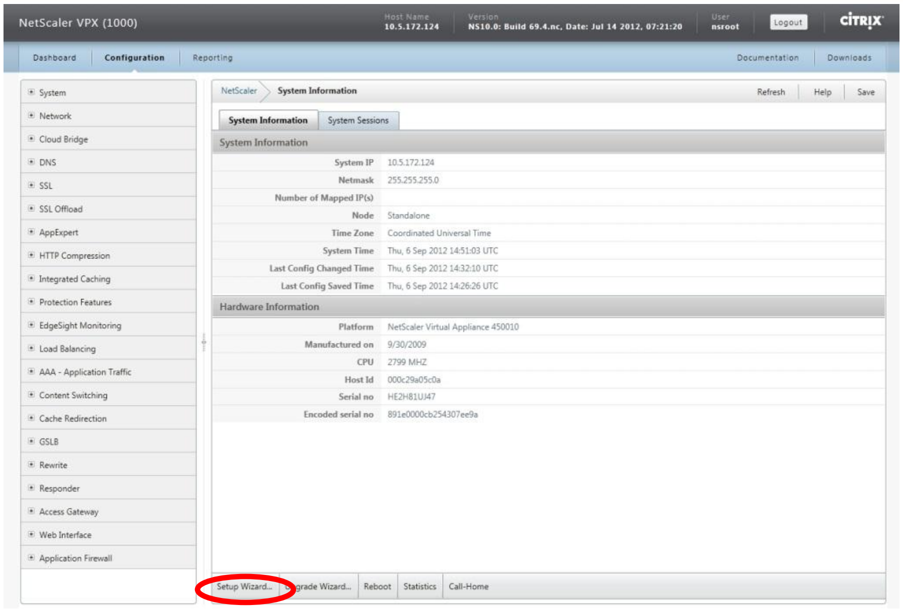
At the Console prompt from XenCenter or xSphere client, enter the NSIP address, subnet mask, and then save the configuration. Use either the SSH client or the NetScaler VPX Console to access the NetScaler command line to complete initial configuration with default gateway.

```
> add route 0.0.0.0 0.0.0.0 <gateway ip>
> show route
> save ns config
```

5.1.2 NetScaler Configuration by Using the Configuration Utility

Once the network connectivity to NetScaler is established, the Configuration Utility can be accessed from a browser to complete the rest of SharePoint configuration.

Connect to NetScaler on a web browser: `http://<NSIP address>`. In **Start in**, select **Configuration**, and then click **Login**. **Setup Wizard** should start up automatically. Otherwise, **Setup Wizard** can be started from menu under **Netscaler>System Information**:



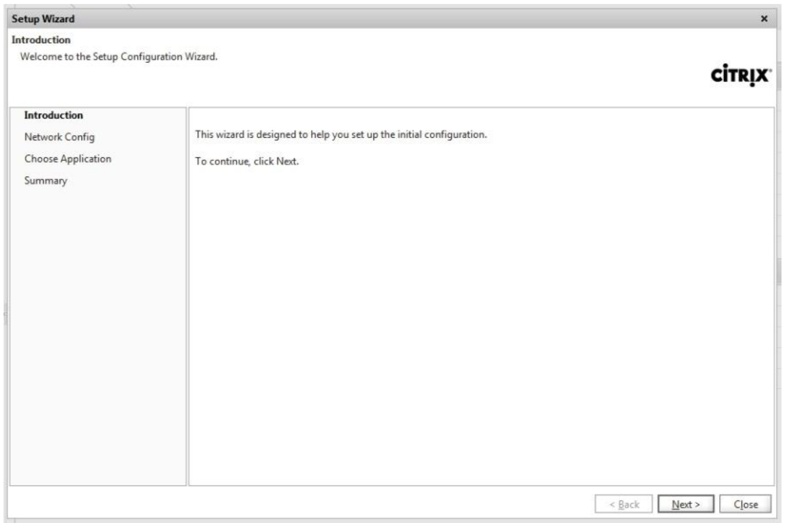
System Information

System IP	10.5.172.124
Netmask	255.255.255.0
Number of Mapped IP(s)	
Node	Standalone
Time Zone	Coordinated Universal Time
System Time	Thu, 6 Sep 2012 14:51:03 UTC
Last Config Changed Time	Thu, 6 Sep 2012 14:32:10 UTC
Last Config Saved Time	Thu, 6 Sep 2012 14:26:26 UTC

Hardware Information

Platform	NetScaler Virtual Appliance 450010
Manufactured on	9/30/2009
CPU	2799 MHZ
Host Id	000c29a05c0a
Serial no	HE2H81UJ47
Encoded serial no	891e0000cb254307ee9a

5.1.3 Setup Wizard

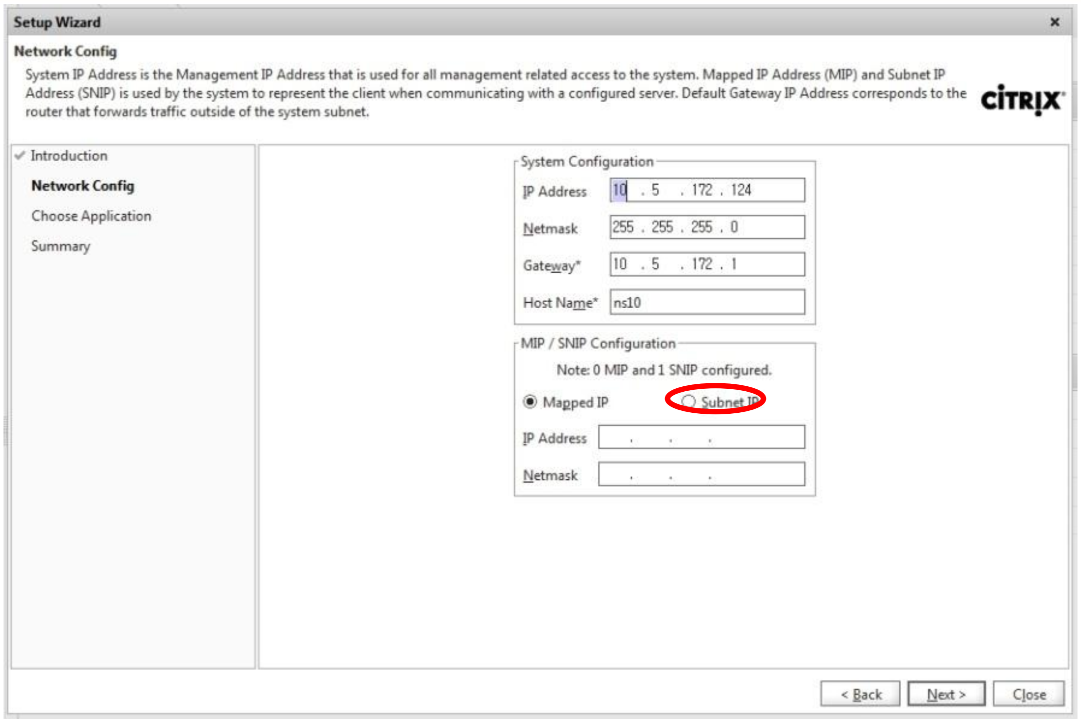


Welcome to the Setup Configuration Wizard.

This wizard is designed to help you set up the initial configuration.

To continue, click Next.

Click **Next** to follow the instructions. Confirm the pre-populated **NSIP**, **Netmask** and **Gateway** addresses.



Setup Wizard

Network Config

System IP Address is the Management IP Address that is used for all management related access to the system. Mapped IP Address (MIP) and Subnet IP Address (SNIP) is used by the system to represent the client when communicating with a configured server. Default Gateway IP Address corresponds to the router that forwards traffic outside of the system subnet.

- ✓ Introduction
- **Network Config**
- Choose Application
- Summary

System Configuration

- IP Address: 10 . 5 . 172 . 124
- Netmask: 255 . 255 . 255 . 0
- Gateway*: 10 . 5 . 172 . 1
- Host Name*: ns10

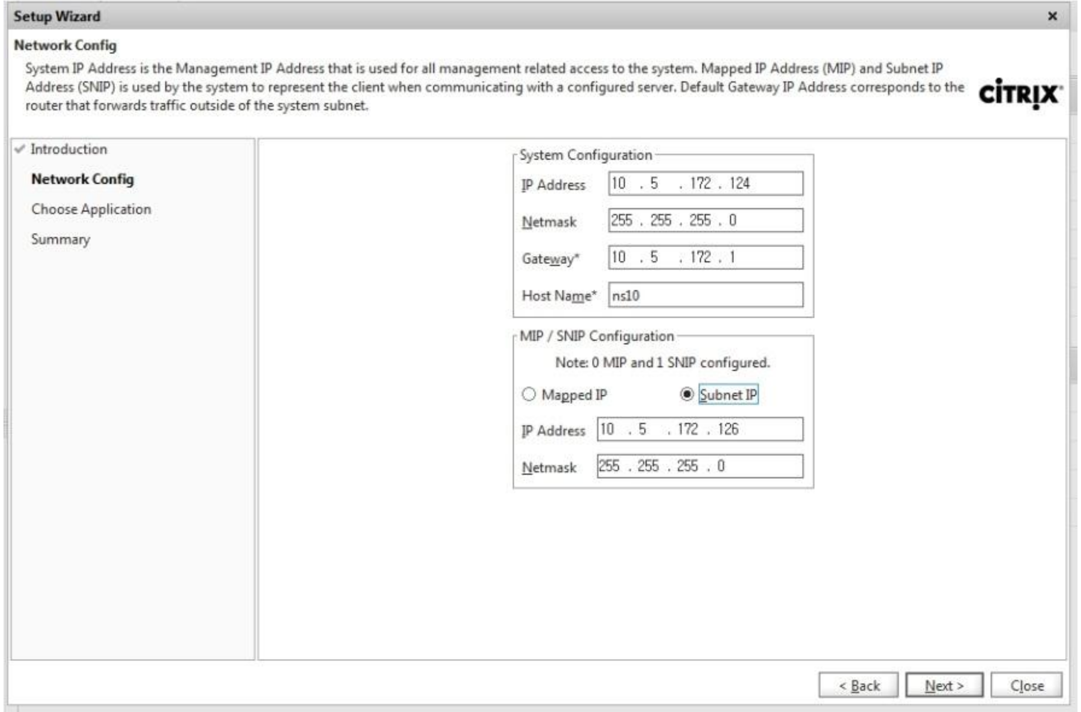
MIP / SNIP Configuration

Note: 0 MIP and 1 SNIP configured.

● Mapped IP ○ Subnet IP

- IP Address: . . .
- Netmask: . . .

Choose **Subnet IP (SNIP)** to add **SNIP** address and its subnet mask (**Netmask**) and Click **Next**.



Setup Wizard

Network Config

System IP Address is the Management IP Address that is used for all management related access to the system. Mapped IP Address (MIP) and Subnet IP Address (SNIP) is used by the system to represent the client when communicating with a configured server. Default Gateway IP Address corresponds to the router that forwards traffic outside of the system subnet.

- ✓ Introduction
- **Network Config**
- Choose Application
- Summary

System Configuration

- IP Address: 10 . 5 . 172 . 124
- Netmask: 255 . 255 . 255 . 0
- Gateway*: 10 . 5 . 172 . 1
- Host Name*: ns10

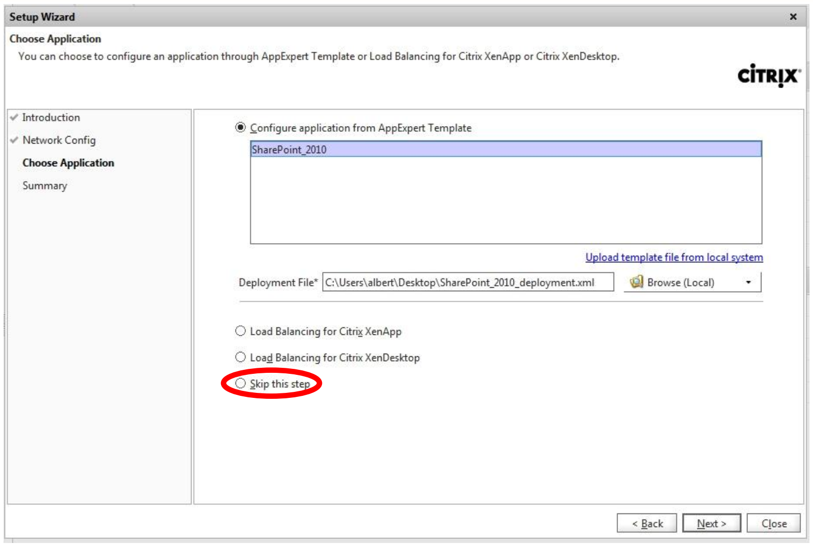
MIP / SNIP Configuration

Note: 0 MIP and 1 SNIP configured.

○ Mapped IP ● Subnet IP

- IP Address: 10 . 5 . 172 . 126
- Netmask: 255 . 255 . 255 . 0

Choose **Skip this Step** for now. AppExpert Template can be added in another step.



Setup Wizard

Choose Application

You can choose to configure an application through AppExpert Template or Load Balancing for Citrix XenApp or Citrix XenDesktop.

● Configure application from AppExpert Template

SharePoint_2010

Upload template file from local system

Deployment File* C:\Users\albert\Desktop\SharePoint_2010_deployment.xml

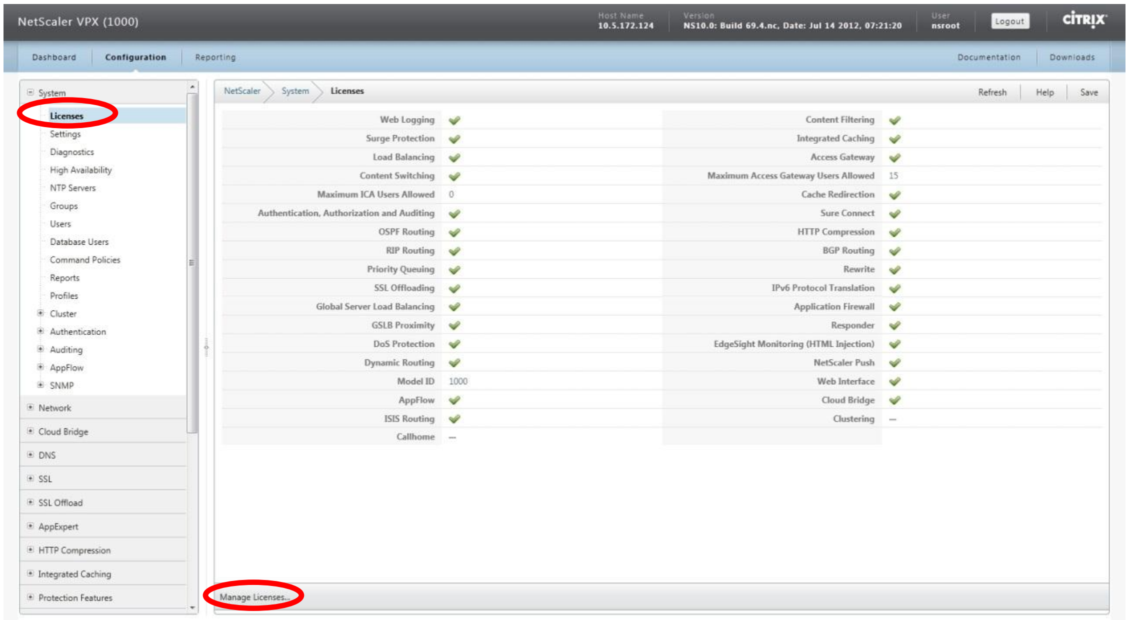
○ Load Balancing for Citrix XenApp

○ Load Balancing for Citrix XenDesktop

○ Skip this step

5.2 NetScaler License installation

Proper license is required in order to enable necessary services for SharePoint configuration. Refer to the “*Citrix NetScaler VPX Licensing Guide”* at http://support.citrix.com/article/CTX122426.



NetScaler VPX (1000)

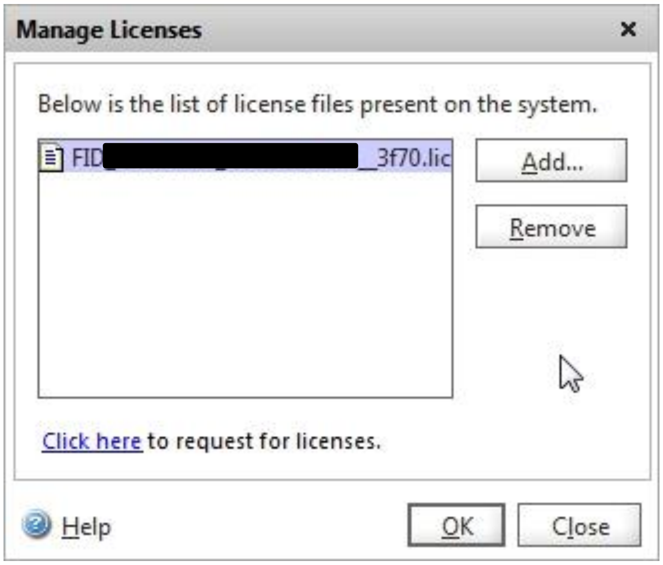
Host Name 10.5.172.124

Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20

User nsroot

Web Logging	✓	Content Filtering	✓
Surge Protection	✓	Integrated Caching	✓
Load Balancing	✓	Access Gateway	✓
Content Switching	✓	Maximum Access Gateway Users Allowed	15
Maximum ICA Users Allowed	0	Cache Redirection	✓
Authentication, Authorization and Auditing	✓	Sure Connect	✓
OSPF Routing	✓	HTTP Compression	✓
RIP Routing	✓	BGP Routing	✓
Priority Queuing	✓	Rewrite	✓
SSL Offloading	✓	IPv6 Protocol Translation	✓
Global Server Load Balancing	✓	Application Firewall	✓
GSLB Proximity	✓	Responder	✓
DoS Protection	✓	EdgeSight Monitoring (HTML Injection)	✓
Dynamic Routing	✓	NetScaler Push	✓
Model ID	1000	Web Interface	✓
AppFlow	✓	Cloud Bridge	✓
ISIS Routing	✓	Clustering	—
Callhome	—		

Click **Manage License** to install the downloaded license.



Manage Licenses

Below is the list of license files present on the system.

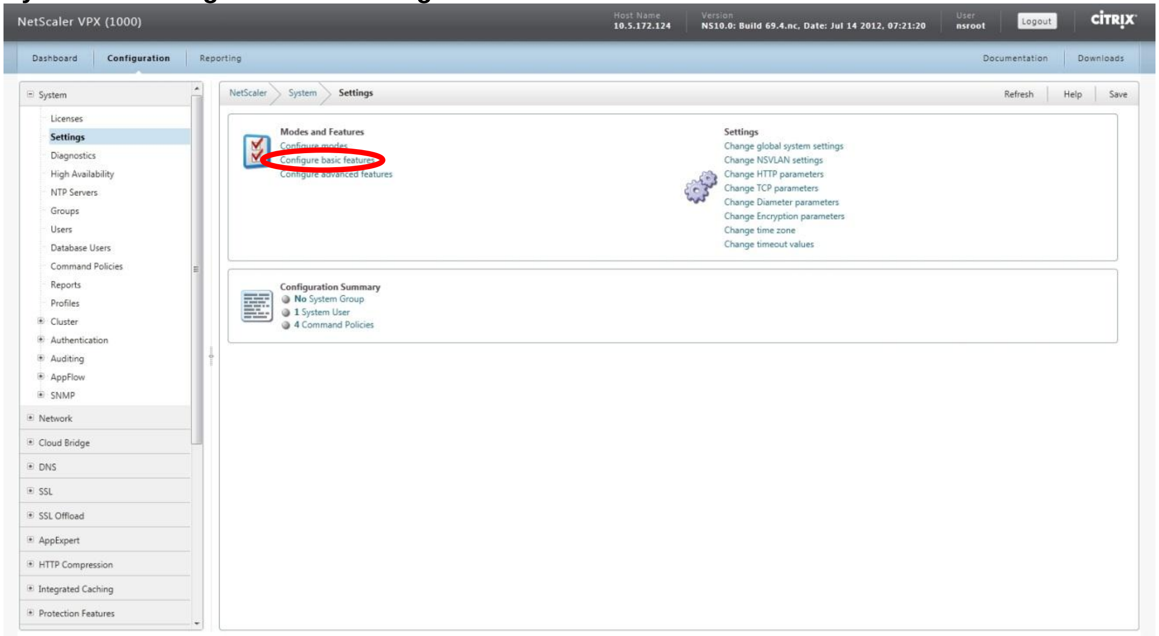
FID[redacted]_3f70.lic

Click here to request for licenses.

5.3 NetScaler Basic Feature Setting

5.3.1 NetScaler Feature Setting

Once a proper license is installed, administrator can select the available features to enable them from **Systems>Settings**. Choose **Configure basic features**.



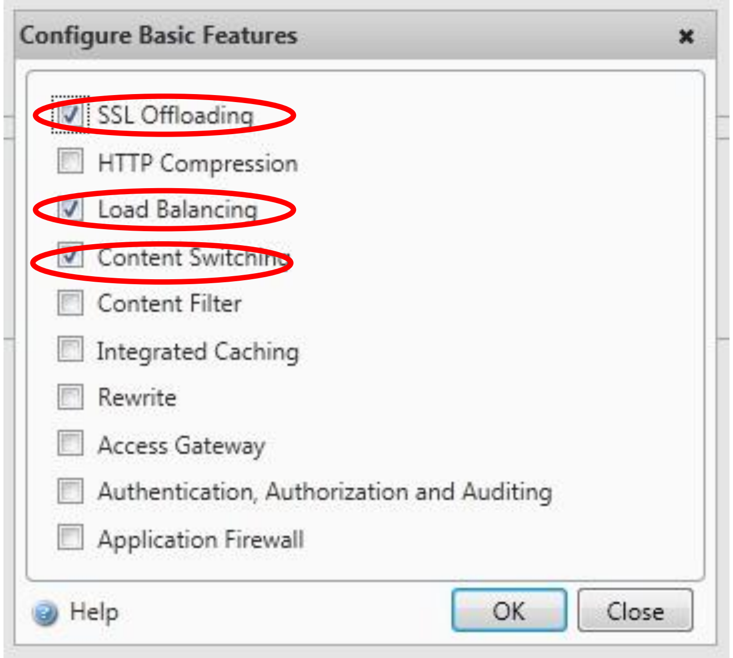
NetScaler VPX (1000)

Host Name 10.5.172.124 | Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20 | User nsroot

Configuration Summary
- No System Group
- 1 System User
- 4 Command Policies

5.3.2 Basic Features

The following services are the minimal services required in order to enable and complete SharePoint configuration.

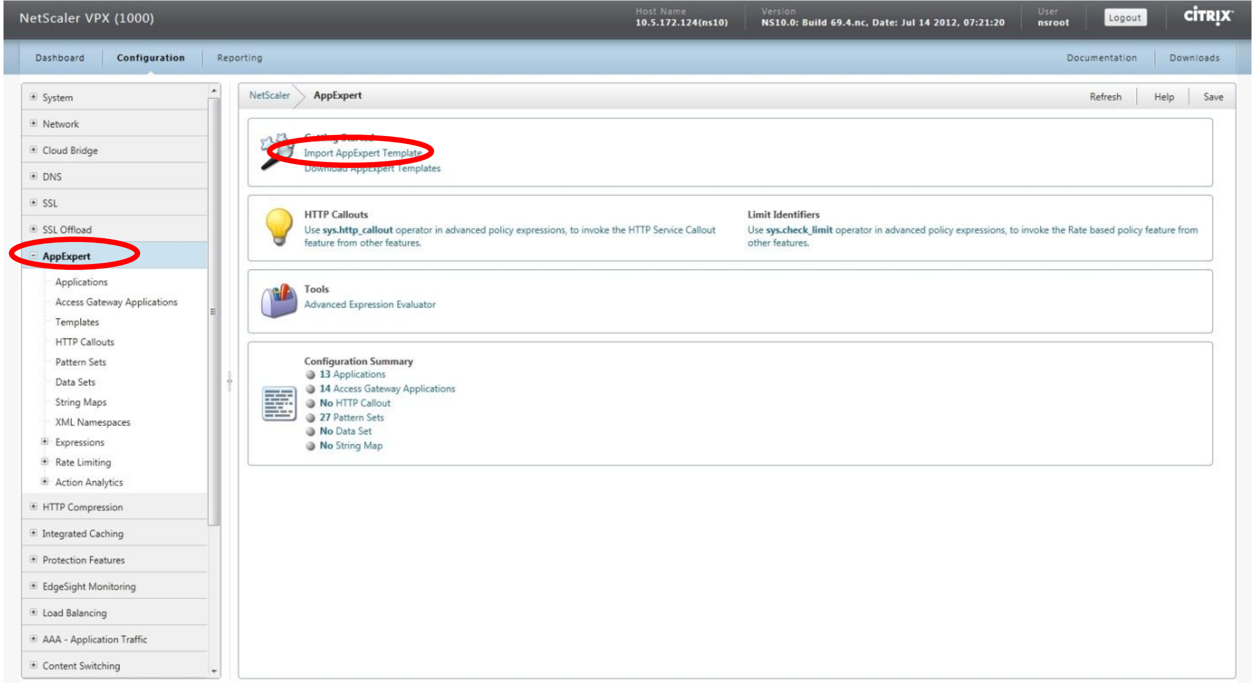


Configure Basic Features

☑ SSL Offloading
□ HTTP Compression
☑ Load Balancing
☑ Content Switching
□ Content Filter
□ Integrated Caching
□ Rewrite
□ Access Gateway
□ Authentication, Authorization and Auditing
□ Application Firewall

5.4 NetScaler AppExpert SharePoint Template Install

AppExpert SharePoint template can be imported under **AppExpert** navigation panel then choose **Import AppExpert Template**.



NetScaler VPX (1000)

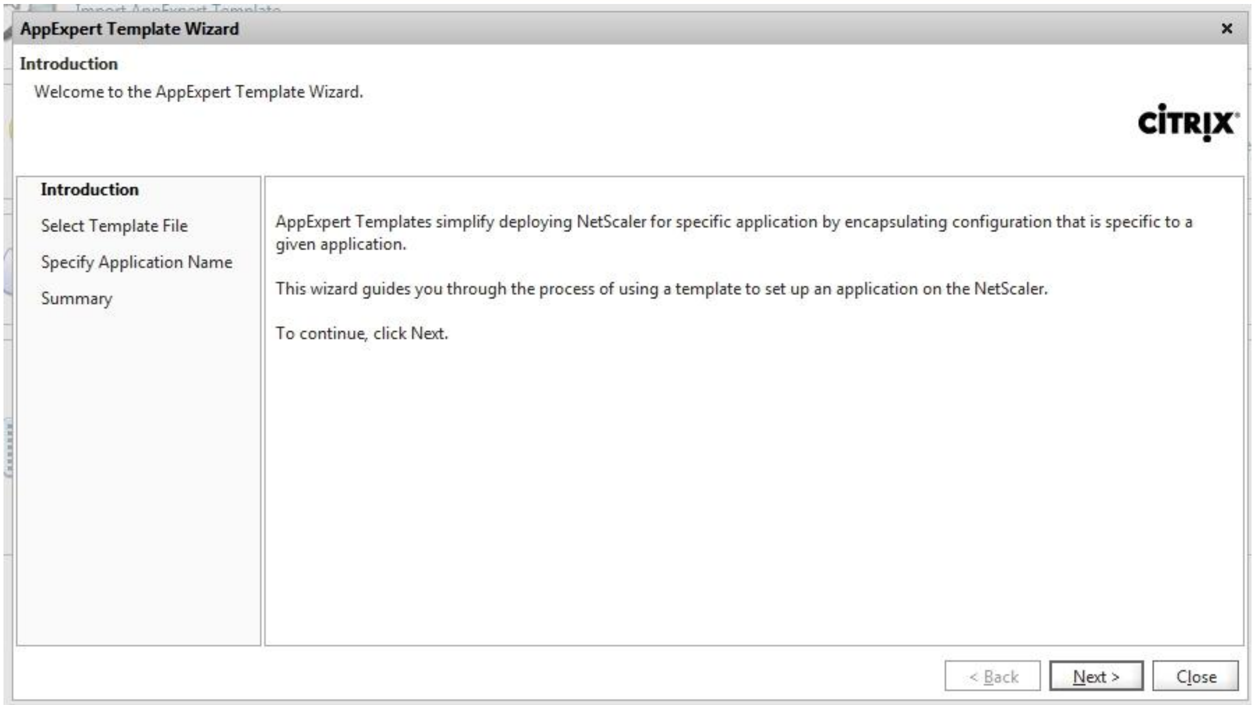
Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

HTTP Callouts
Use sys.http_callout operator in advanced policy expressions, to invoke the HTTP Service Callout feature from other features.

Limit Identifiers
Use sys.check_limit operator in advanced policy expressions, to invoke the Rate based policy feature from other features.

Configuration Summary
- 13 Applications
- 14 Access Gateway Applications
- No HTTP Callout
- 27 Pattern Sets
- No Data Set
- No String Map

Click **Next** to bring **AppExpert Tmplate Wizard** to upload the downloaded templates.



AppExpert Template Wizard

Introduction

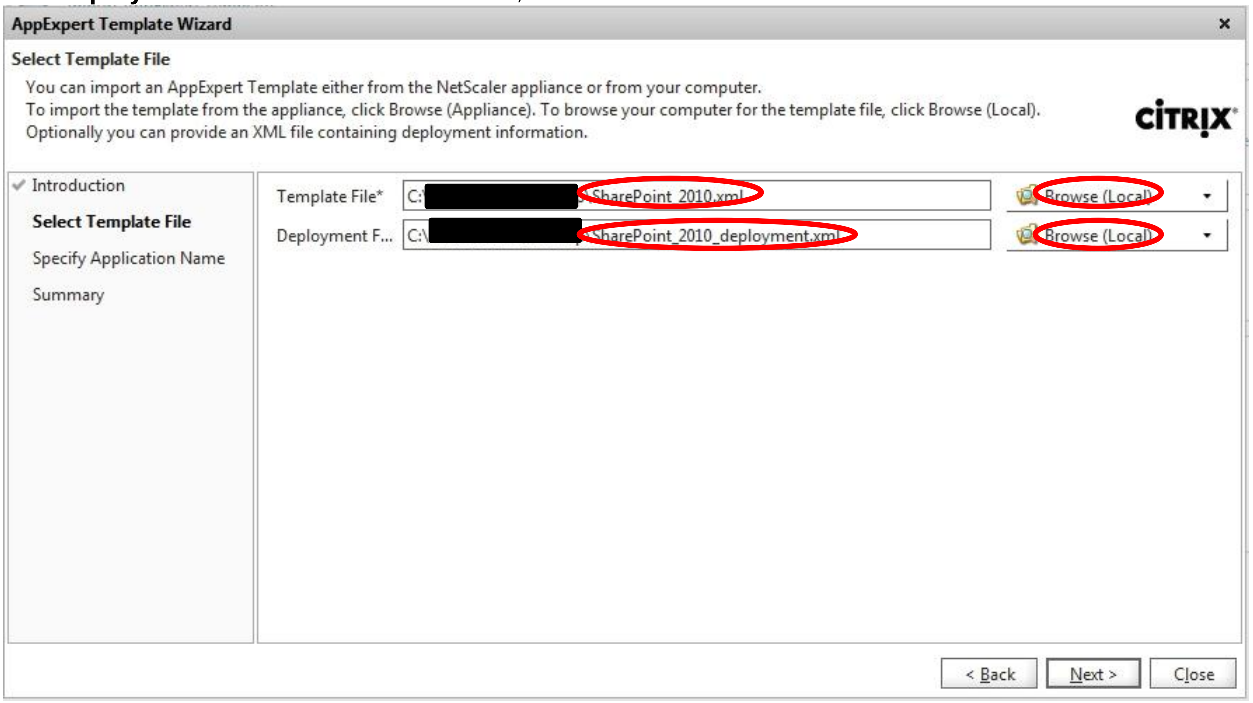
Welcome to the AppExpert Template Wizard.

AppExpert Templates simplify deploying NetScaler for specific application by encapsulating configuration that is specific to a given application.

This wizard guides you through the process of using a template to set up an application on the NetScaler.

To continue, click Next.

Choose **Browse (Local)** if the files were downloaded to local system, then choose the proper **Template** and **Deployment** files for SharePoint. Then, click **Next**.



AppExpert Template Wizard

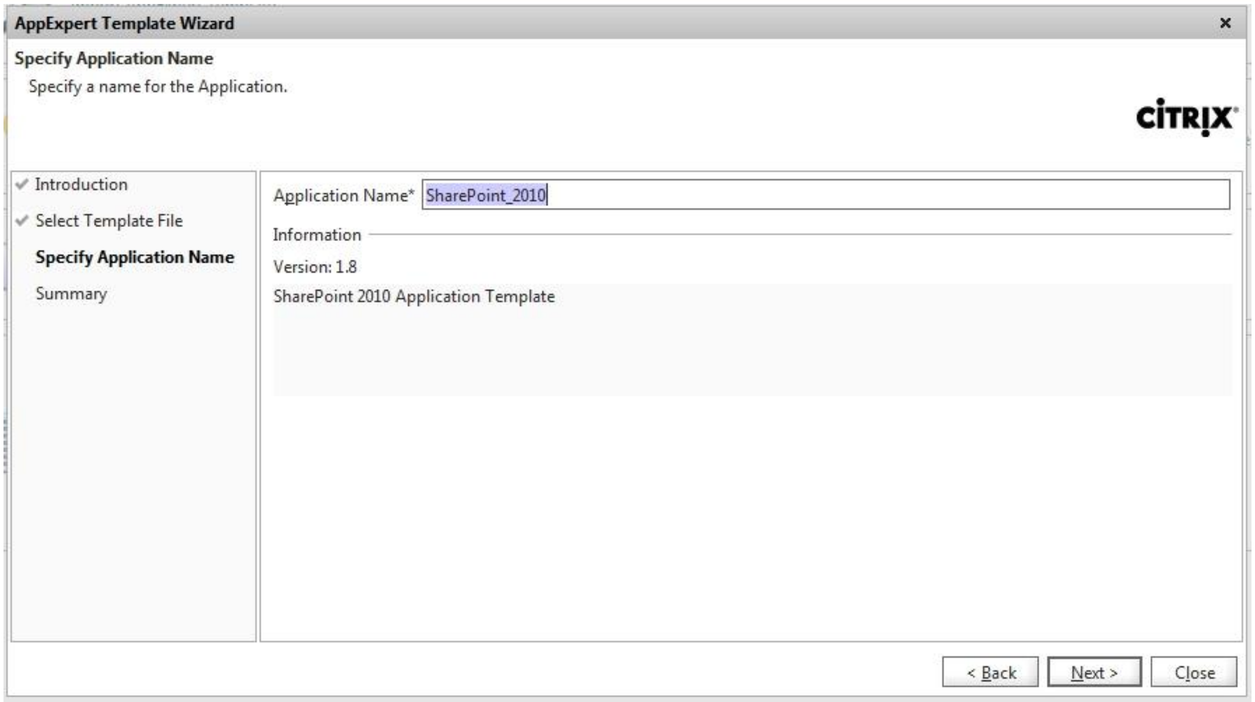
Select Template File

You can import an AppExpert Template either from the NetScaler appliance or from your computer.
To import the template from the appliance, click Browse (Appliance). To browse your computer for the template file, click Browse (Local).
Optionally you can provide an XML file containing deployment information.

Template File* C:[redacted]SharePoint_2010.xml

Deployment F... C:\[redacted]SharePoint_2010_deployment.xml

AppExpert Template Wizard will confirm with the **Application Name** then click **Next** to complete.


AppExpert Template Wizard

Specify Application Name

Specify a name for the Application.

Application Name* SharePoint_2010

Information

Version: 1.8

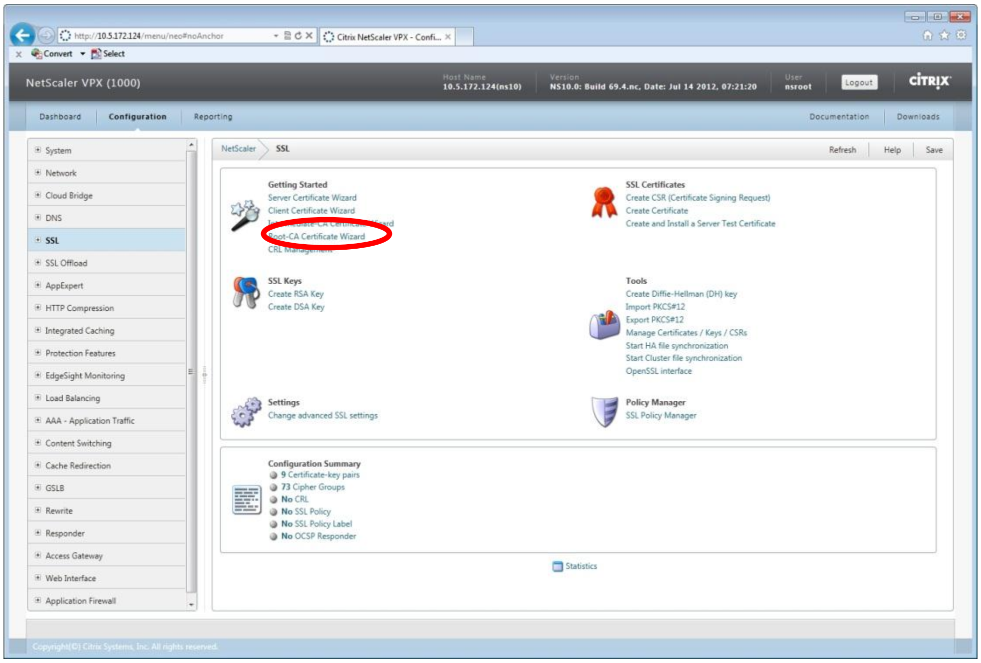
SharePoint 2010 Application Template

5.5 NetScaler SSL Security Certificate installation (Self-Signed Certificate example)

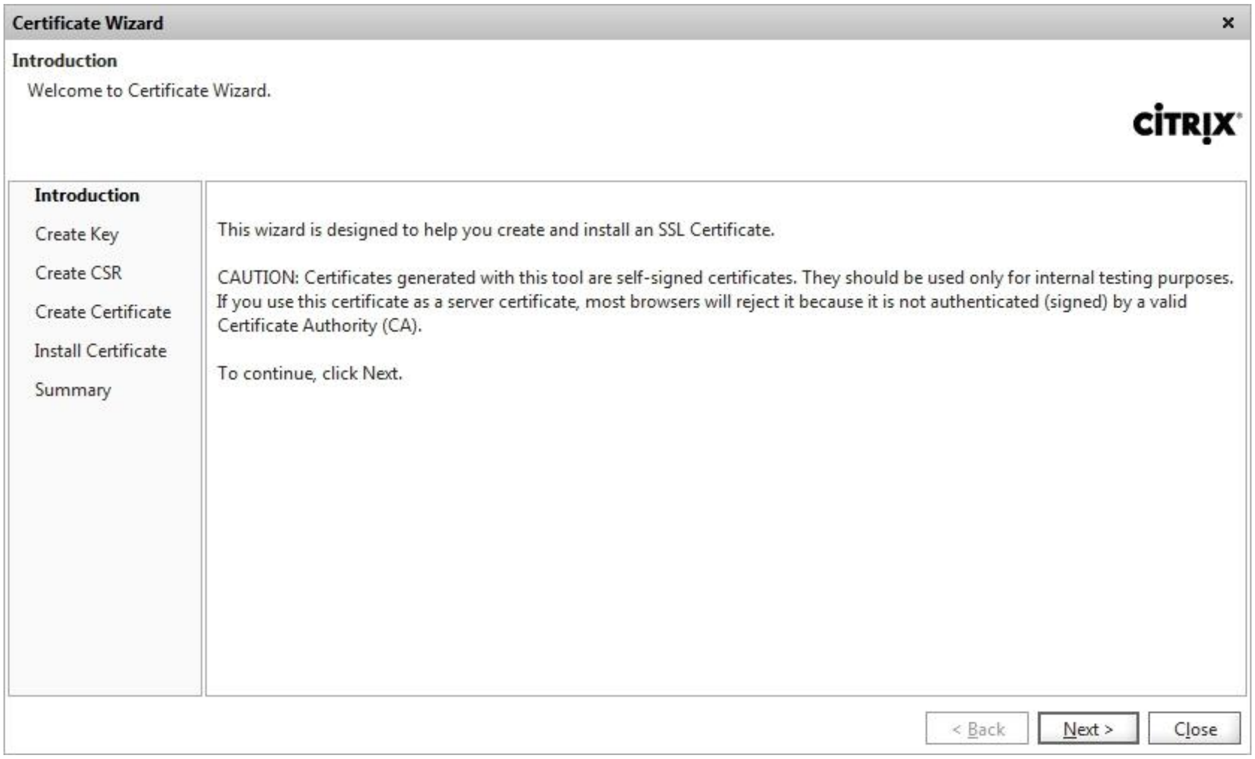
If production certificates are available, these can be imported through the processes within the NetScaler management interface. Consult Chapter 11 , "*Securing Load Balanced Traffic by Using SSL*" of the NetScaler product documentation entitled "*NetScaler VPX Getting Started Guide*" for details pertaining to the user of existing certificate/key pairs.
The following steps were used in this reference environment to create of self-signed certificates used to implement the HTTP to HTTPS rewrite.

5.5.1 Root-CA Certificate

Under **SSL** navigation panel, choose **Root-CA Certificate Wizard**.



Click **Next**.



Certificate Wizard

Introduction

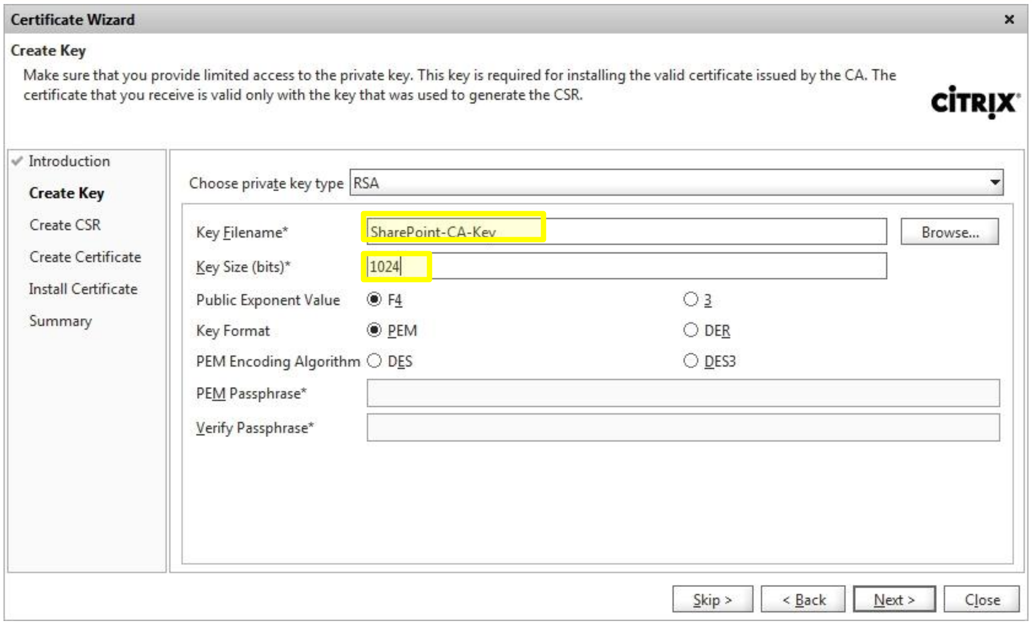
Welcome to Certificate Wizard.

This wizard is designed to help you create and install an SSL Certificate.

CAUTION: Certificates generated with this tool are self-signed certificates. They should be used only for internal testing purposes. If you use this certificate as a server certificate, most browsers will reject it because it is not authenticated (signed) by a valid Certificate Authority (CA).

To continue, click Next.

Set the **Key Filename** to **SharePoint-CA-Key**. And set **Key Size** to **1024** or any value that reflects customized datacenter’s standard. Then click **Next**.



Certificate Wizard

Create Key

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

- ✓ Introduction
- **Create Key**
- Create CSR
- Create Certificate
- Install Certificate
- Summary

Choose private key type: RSA

Key Filename*: SharePoint-CA-Key

Key Size (bits)*: 1024

Public Exponent Value: ● F4 ○ 3

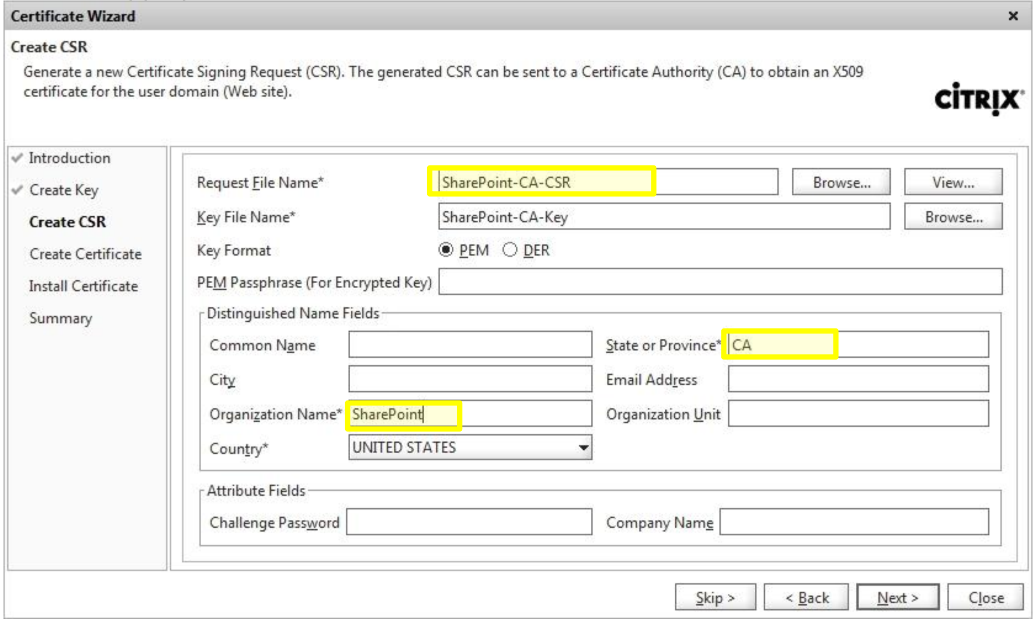
Key Format: ● PEM ○ DER

PEM Encoding Algorithm: ○ DES ○ DES3

PEM Passphrase*:

Verify Passphrase*:

Set the **Request File Name** to **SharePoint-CA-CSR**. And set **City** and **State** or **Province**, **Organization Name** to appropriate values. Then click **Next**.



Certificate Wizard

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).

- ✓ Introduction
- ✓ Create Key
- **Create CSR**
- Create Certificate
- Install Certificate
- Summary

Request File Name*: SharePoint-CA-CSR

Key File Name*: SharePoint-CA-Key

Key Format: ● PEM ○ DER

PEM Passphrase (For Encrypted Key):

Distinguished Name Fields

Common Name:

State or Province*: CA

City:

Email Address:

Organization Name*: SharePoint

Organization Unit:

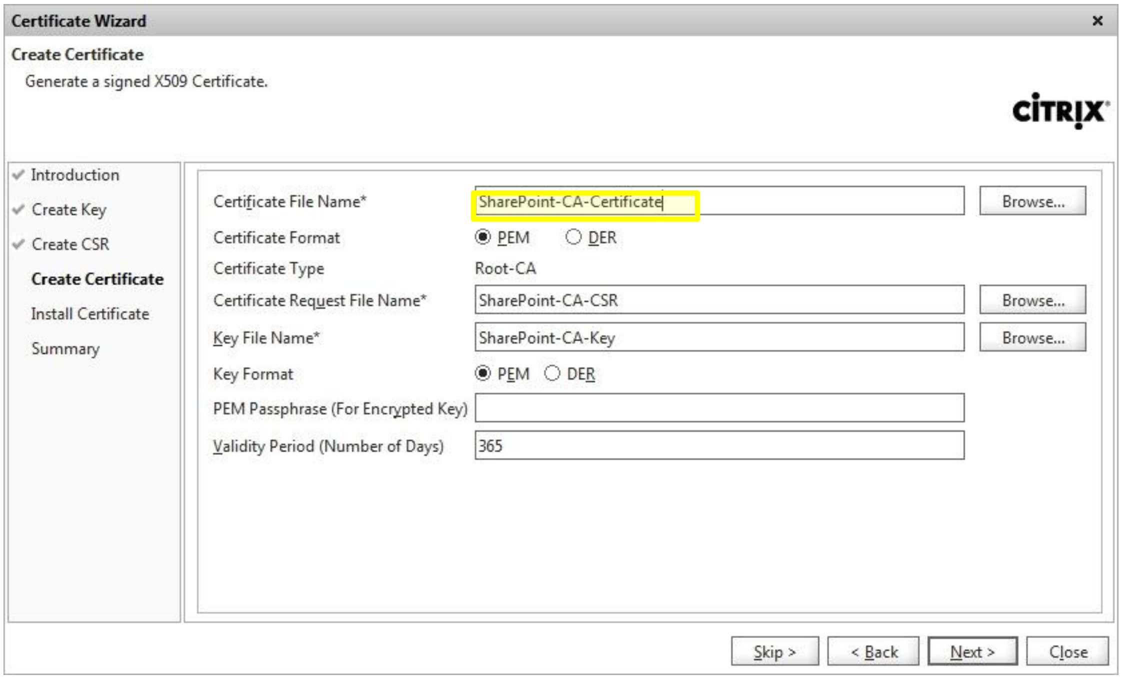
Country*: UNITED STATES

Attribute Fields

Challenge Password:

Company Name:

Set the **Certificate File Name** to **SharePoint-CA-Certificate**. Then click **Next**.



Certificate Wizard

Create Certificate

Generate a signed X509 Certificate.

Certificate File Name* SharePoint-CA-Certificate

Certificate Format ● PEM ○ DER

Certificate Type Root-CA

Certificate Request File Name* SharePoint-CA-CSR

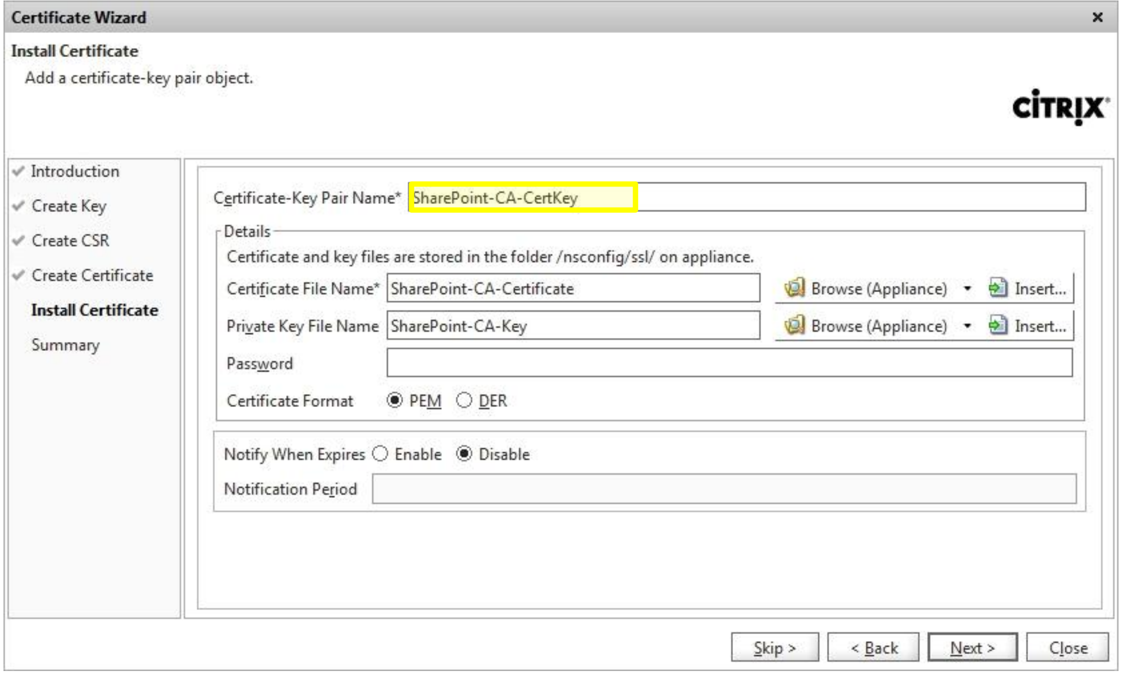
Key File Name* SharePoint-CA-Key

Key Format ● PEM ○ DER

PEM Passphrase (For Encrypted Key)

Validity Period (Number of Days) 365

Set the **Certificate-Key Pair Name** to **SharePoint-CA-CertKey**. Then click **Next**.



Certificate Wizard

Install Certificate

Add a certificate-key pair object.

Certificate-Key Pair Name* SharePoint-CA-CertKey

Details

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

Certificate File Name* SharePoint-CA-Certificate

Private Key File Name SharePoint-CA-Key

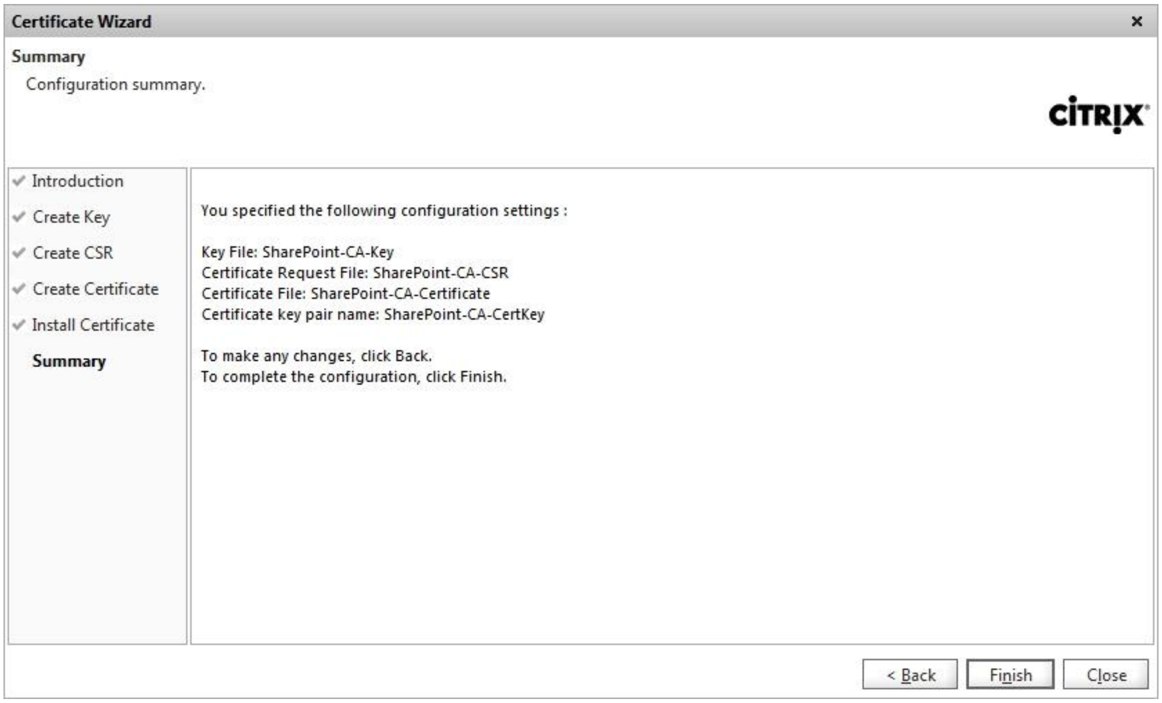
Password

Certificate Format ● PEM ○ DER

Notify When Expires ○ Enable ● Disable

Notification Period

Click **Finish**.

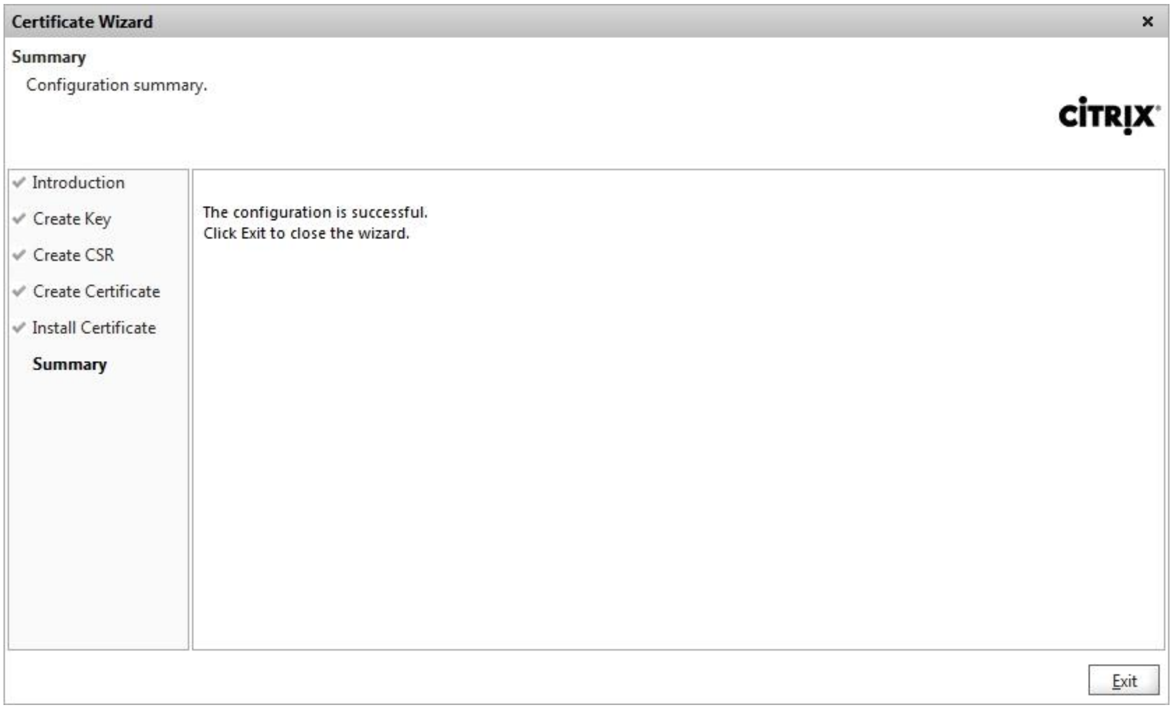


You specified the following configuration settings :

Key File: SharePoint-CA-Key
Certificate Request File: SharePoint-CA-CSR
Certificate File: SharePoint-CA-Certificate
Certificate key pair name: SharePoint-CA-CertKey

To make any changes, click Back.
To complete the configuration, click Finish.

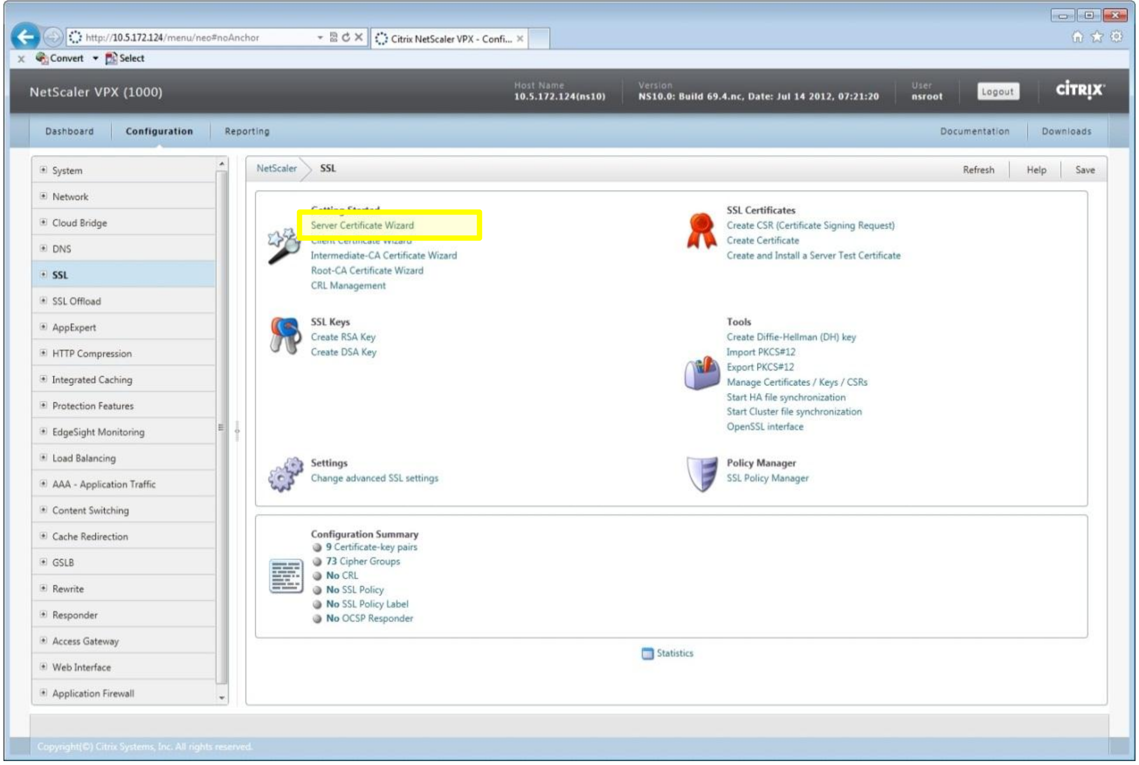
Click **Exit**.



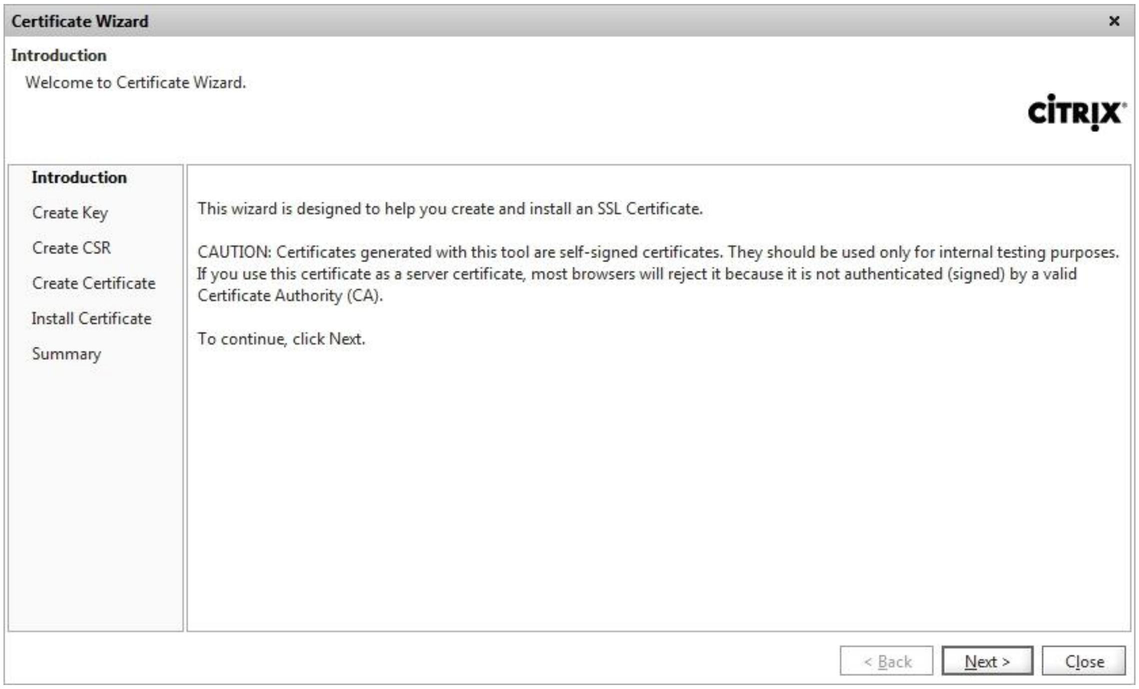
The configuration is successful.
Click Exit to close the wizard.

5.5.2 Server Certificate

Under **SSL** navigation panel, choose **Server Certificate Wizard**.



Click **Next**.



Introduction

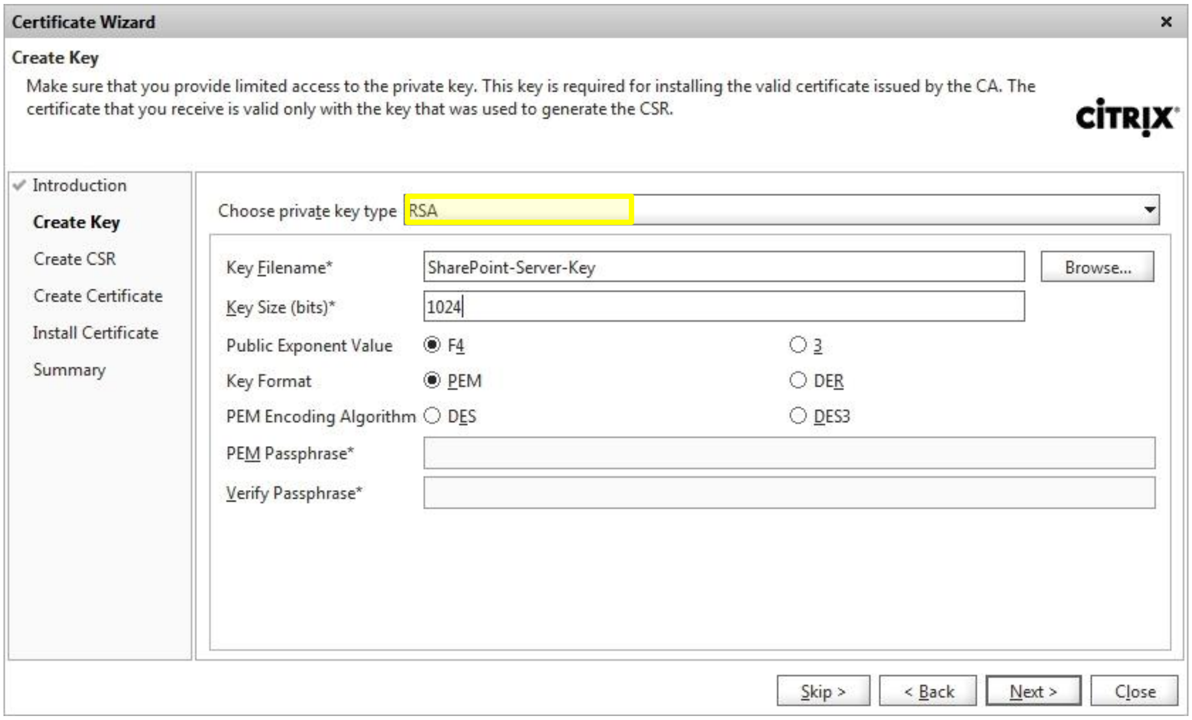
Welcome to Certificate Wizard.

This wizard is designed to help you create and install an SSL Certificate.

CAUTION: Certificates generated with this tool are self-signed certificates. They should be used only for internal testing purposes. If you use this certificate as a server certificate, most browsers will reject it because it is not authenticated (signed) by a valid Certificate Authority (CA).

To continue, click Next.

Set the **Key Filename** to **SharePoint-Server-Key**. And set **Key Size** to **1024** or any value that reflects customized datacenter's standard. Then click **Next**.



Certificate Wizard

Create Key

Make sure that you provide limited access to the private key. This key is required for installing the valid certificate issued by the CA. 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*: SharePoint-Server-Key

Key Size (bits)*: 1024

Public Exponent Value: ● F4 ○ 3

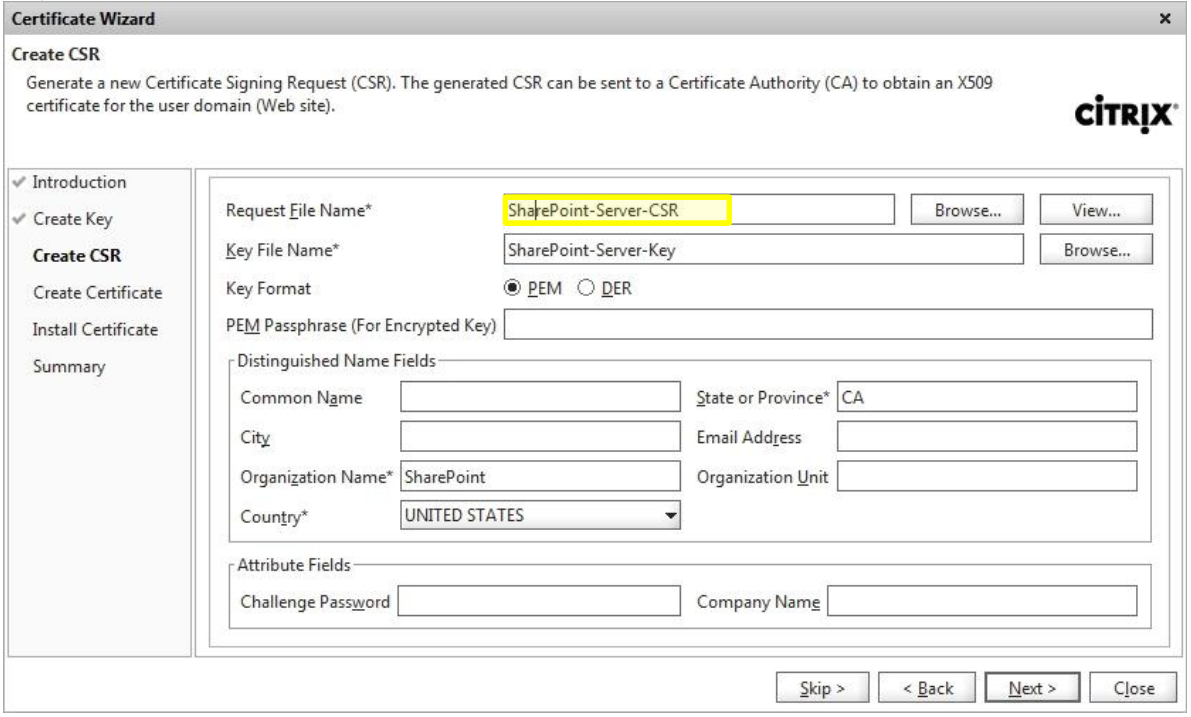
Key Format: ● PEM ○ DER

PEM Encoding Algorithm: ○ DES ○ DES3

PEM Passphrase*:

Verify Passphrase*:

Set the **Request File Name** to **SharePoint-Server-CSR**. And set **City** and **State** or **Province**, **Organization Name** to appropriate values. Then click **Next**.



Certificate Wizard

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*: SharePoint-Server-CSR

Key File Name*: SharePoint-Server-Key

Key Format: ● PEM ○ DER

PEM Passphrase (For Encrypted Key):

Distinguished Name Fields

Common Name:

State or Province*: CA

City:

Email Address:

Organization Name*: SharePoint

Organization Unit:

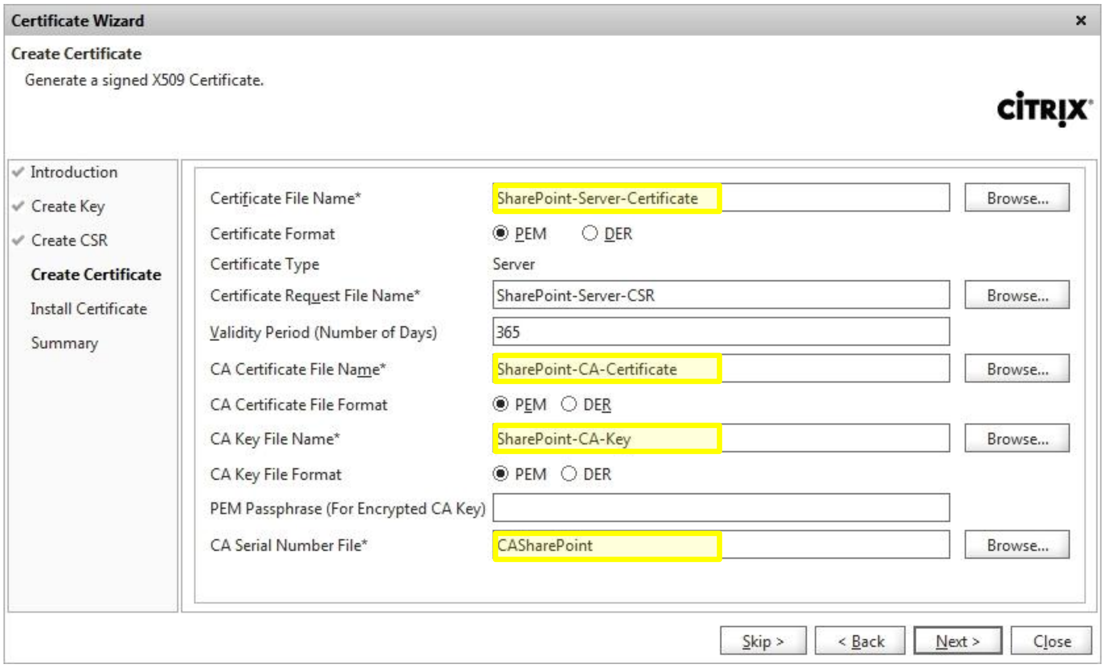
Country*: UNITED STATES

Attribute Fields

Challenge Password:

Company Name:

Set the **Certificate File Name** to **SharePoint-Server-Certificate**. And set **CA Certificate File Name** to **SharePoint-CA-Certificate**. Set **CA Key File Name** to **SharePoint-CA-Key**. And **CA Serial Number File** to **CASharePoint**. Then click **Next**.



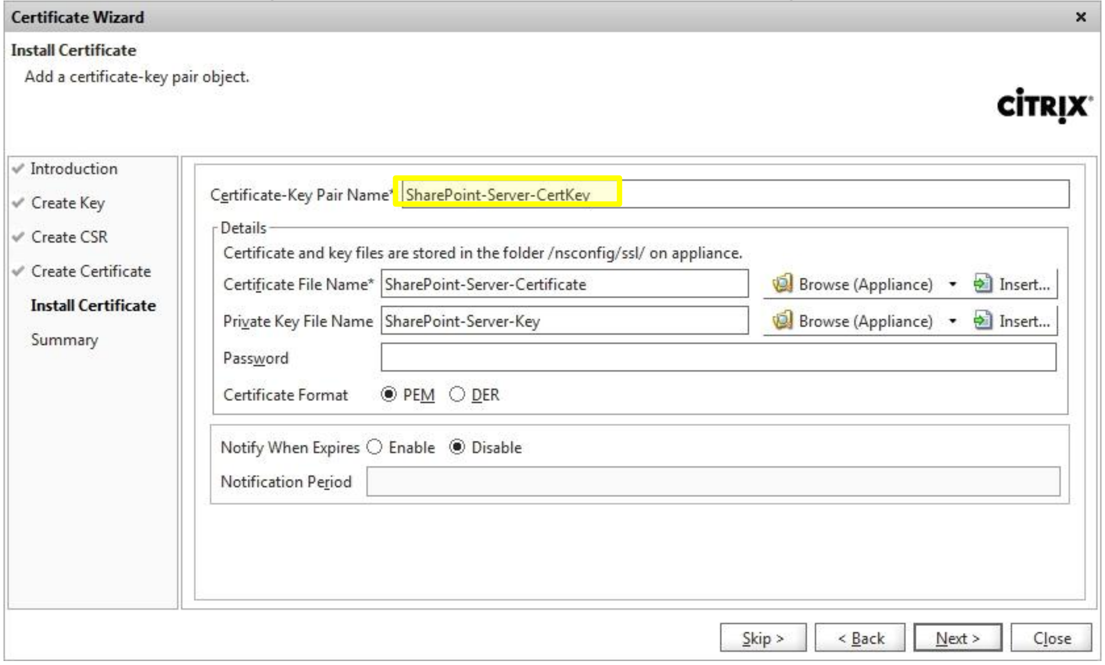
Certificate Wizard ×

Create Certificate

Generate a signed X509 Certificate.

Certificate File Name*	SharePoint-Server-Certificate	Browse...
Certificate Format	● PEM ○ DER	
Certificate Type	Server	
Certificate Request File Name*	SharePoint-Server-CSR	Browse...
Validity Period (Number of Days)	365	
CA Certificate File Name*	SharePoint-CA-Certificate	Browse...
CA Certificate File Format	● PEM ○ DER	
CA Key File Name*	SharePoint-CA-Key	Browse...
CA Key File Format	● PEM ○ DER	
PEM Passphrase (For Encrypted CA Key)		
CA Serial Number File*	CASharePoint	Browse...

Set the **Certificate-Key Pair Name** to **SharePoint-Server-CertKey**. Then click **Next.**



Certificate Wizard ×

Install Certificate

Add a certificate-key pair object.

Certificate-Key Pair Name* SharePoint-Server-CertKey

Details

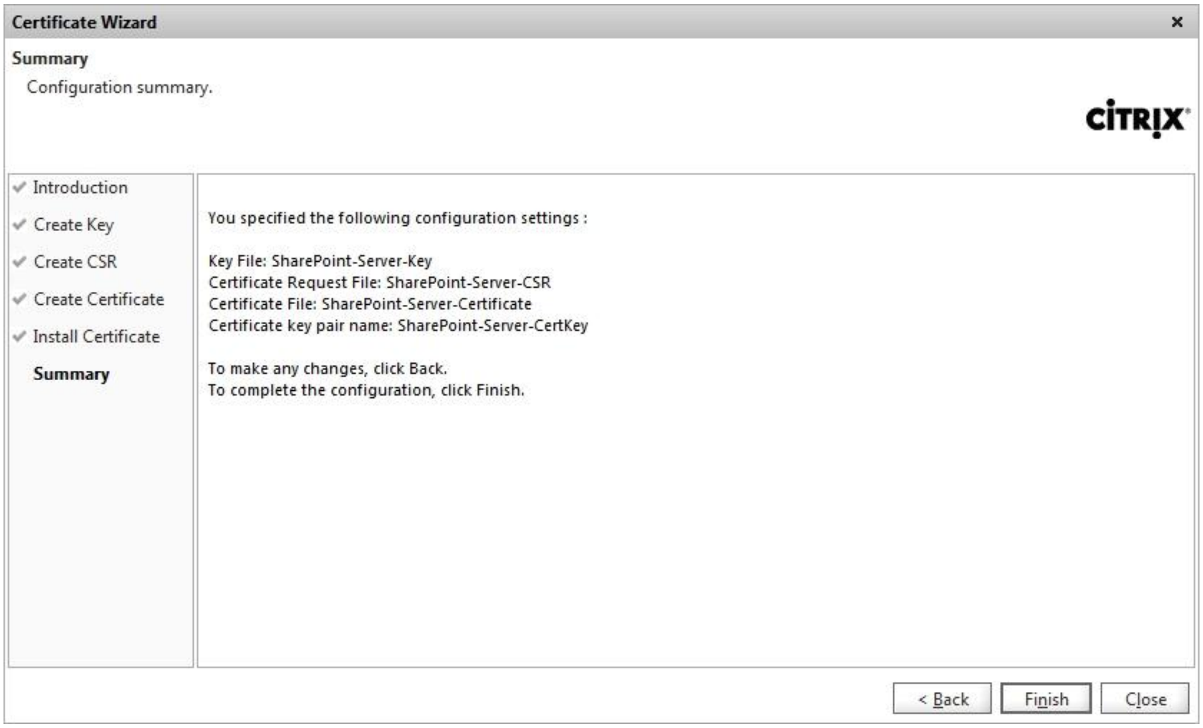
Certificate and key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*	SharePoint-Server-Certificate	Browse (Appliance) ▾ Insert...
Private Key File Name	SharePoint-Server-Key	Browse (Appliance) ▾ Insert...
Password		
Certificate Format	● PEM ○ DER	

Notify When Expires ○ Enable ● Disable

Notification Period

Click **Finish**.

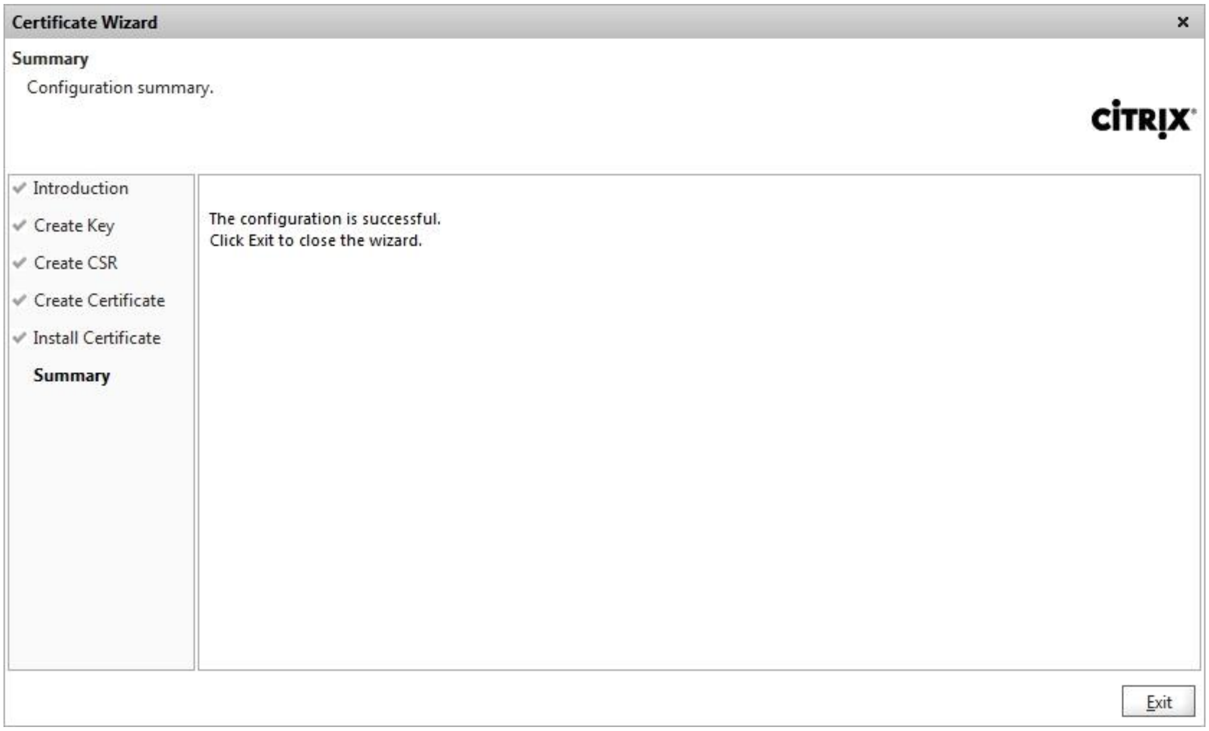


You specified the following configuration settings :

Key File: SharePoint-Server-Key
Certificate Request File: SharePoint-Server-CSR
Certificate File: SharePoint-Server-Certificate
Certificate key pair name: SharePoint-Server-CertKey

To make any changes, click Back.
To complete the configuration, click Finish.

Click **Exit**.



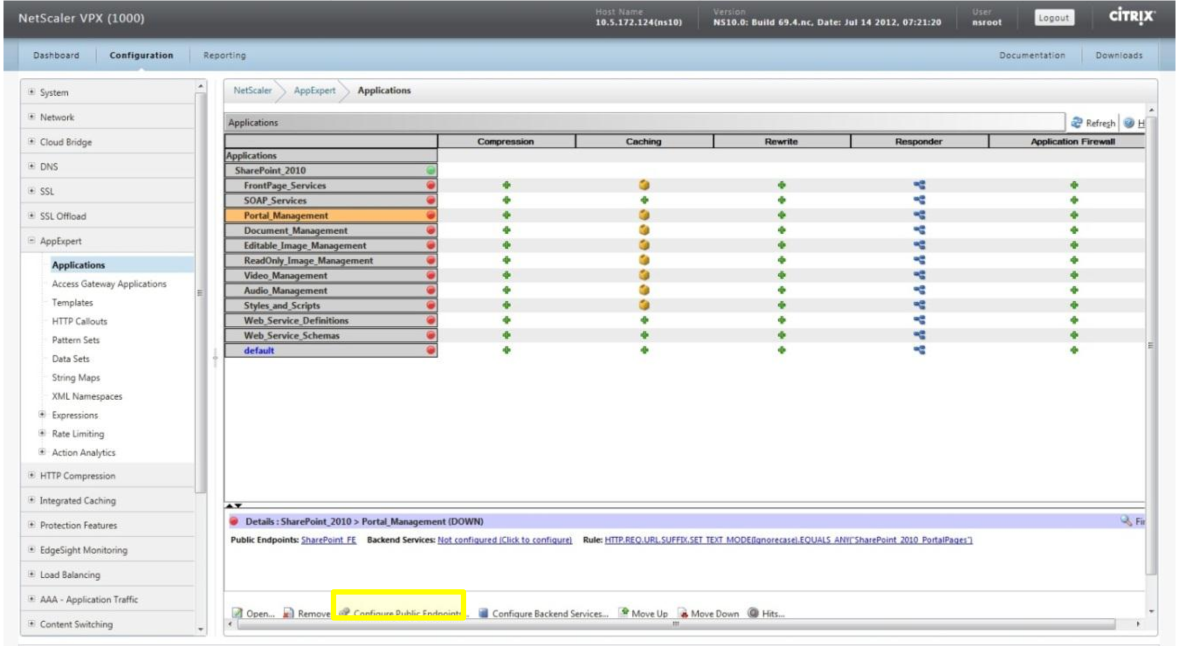
The configuration is successful.
Click Exit to close the wizard.

5.6 Creating virtual servers (VIP)

Virtual servers (or Virtual IP, VIP) will be used for users to connect to SharePoint service. Once completed, users will be able to access their SharePoint environment to `http(s)://<VIP>` or `http(s)://<VIP>/owa` depending on their configuration.

5.6.1 HTTP VIP

Under **AppExpert** navigation panel, choose **Applications** to view those installed templates. Under **SharePoint 2010**, all the pre-defined SharePoint service components will be listed. Choose **Configure Public Endpoints…** to set public virtual server name and ip address according to section 3.2.



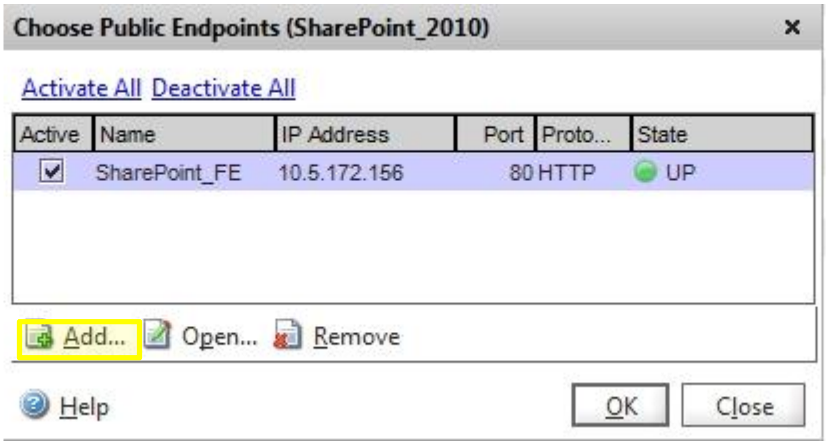
Applications

Applications	Compression	Caching	Rewrite	Responder	Application Firewall
SharePoint_2010 ●					
FrontPage_Services ●	✚	⬢	✚	⋞	✚
SOAP_Services ●	✚	✚	✚	⋞	✚
Portal_Management ●	✚	⬢	✚	⋞	✚
Document_Management ●	✚	⬢	✚	⋞	✚
Editable_Image_Management ●	✚	⬢	✚	⋞	✚
ReadOnly_Image_Management ●	✚	⬢	✚	⋞	✚
Video_Management ●	✚	⬢	✚	⋞	✚
Audio_Management ●	✚	⬢	✚	⋞	✚
Styles_and_Scripts ●	✚	⬢	✚	⋞	✚
Web_Service_Definitions ●	✚	✚	✚	⋞	✚
Web_Service_Schemas ●	✚	✚	✚	⋞	✚
default ●	✚	✚	✚	⋞	✚

Details : SharePoint_2010 > Portal_Management (DOWN)

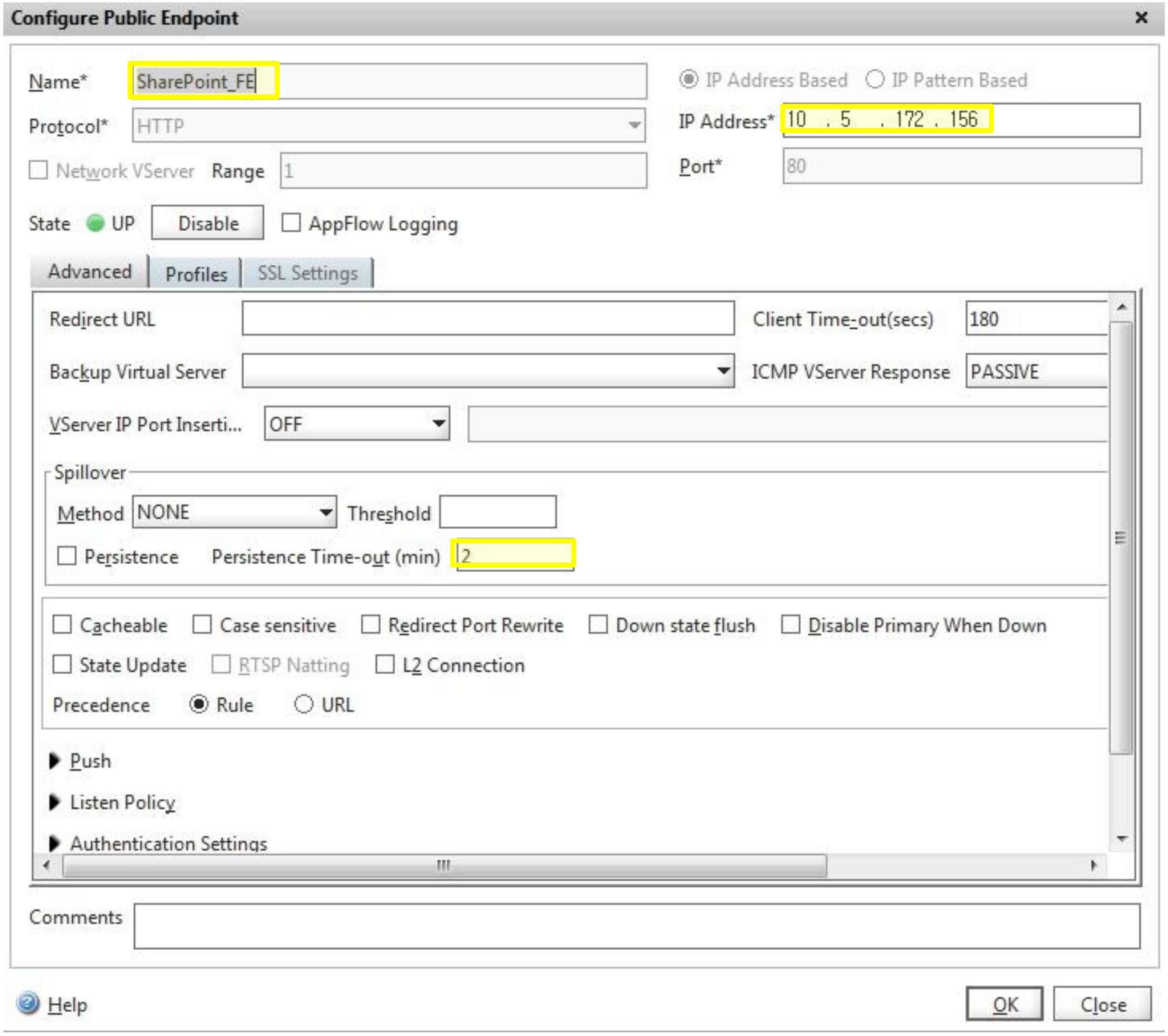
Public Endpoints: SharePoint_FE   Backend Services: Not configured (Click to configure)   Rule: HTTP.REQ.URL.SUFFIX.SET_TEXT_MODE(ignorecase).EQUALS_ANY("SharePoint_2010_PortalPages")

Choose **Add**.



Active	Name	IP Address	Port	Proto...	State
☑	SharePoint_FE	10.5.172.156	80	HTTP	● UP

Set **Name** to **SharePoint_FE** or proper meaningful name. Set **IP Address** (Note. This is not a physical/VM server IP address). **Protocol** to **HTTP** and **Port** number to **80.** Set **Persistence Time-out (min)** to **2.** Then click **OK**.



Configure Public Endpoint

Name* SharePoint_FE

Protocol* HTTP

□ Network VServer Range 1

● IP Address Based ○ IP Pattern Based

IP Address* 10 . 5 . 172 . 156

Port* 80

State ● UP Disable □ AppFlow Logging

Advanced | Profiles | SSL Settings

Redirect URL

Client Time-out(secs) 180

Backup Virtual Server

ICMP VServer Response PASSIVE

VServer IP Port Inserti... OFF

Spillover

Method NONE Threshold

□ Persistence Persistence Time-out (min) 2

□ Cacheable □ Case sensitive □ Redirect Port Rewrite □ Down state flush □ Disable Primary When Down

□ State Update □ RTSP Natting □ L2 Connection

Precedence ● Rule ○ URL

▶ Push

▶ Listen Policy

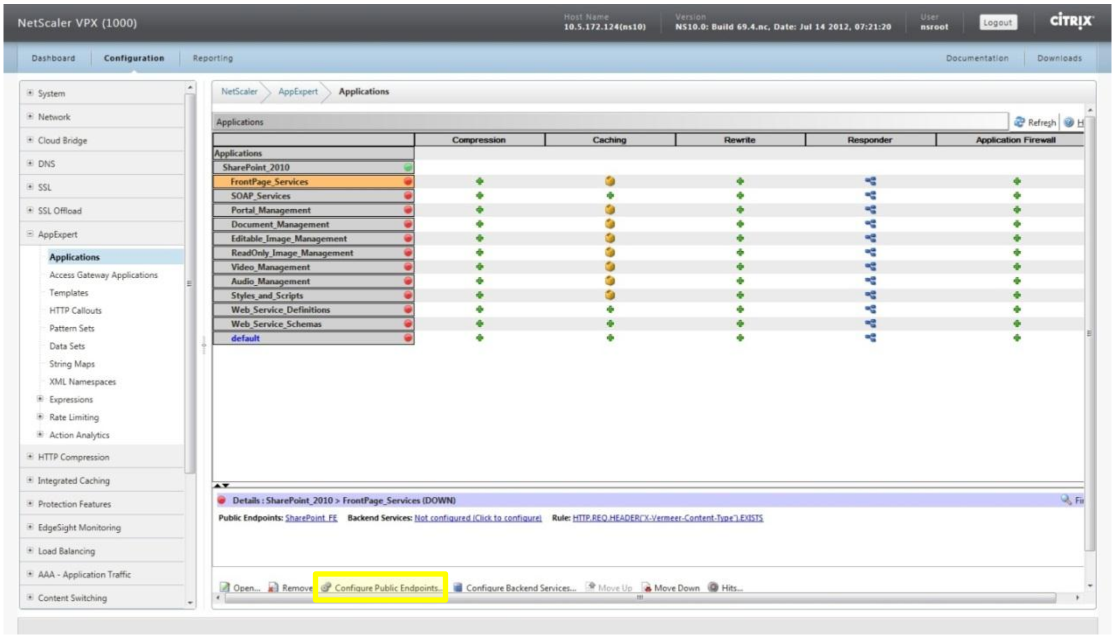
▶ Authentication Settings

Comments

Help OK Close

5.6.1 HTTPS VIP

From the main NetScaler Configuration Utility screen, under **AppExpert** and **Applications**, and **SharePoint 2010**, choose **Configure Public Endpoints** to set public virtual server name and ip address according to section 3.2. (Note. This IP address will be the same as HTTP VIP which was just created in previous section. It will just use a different port.)



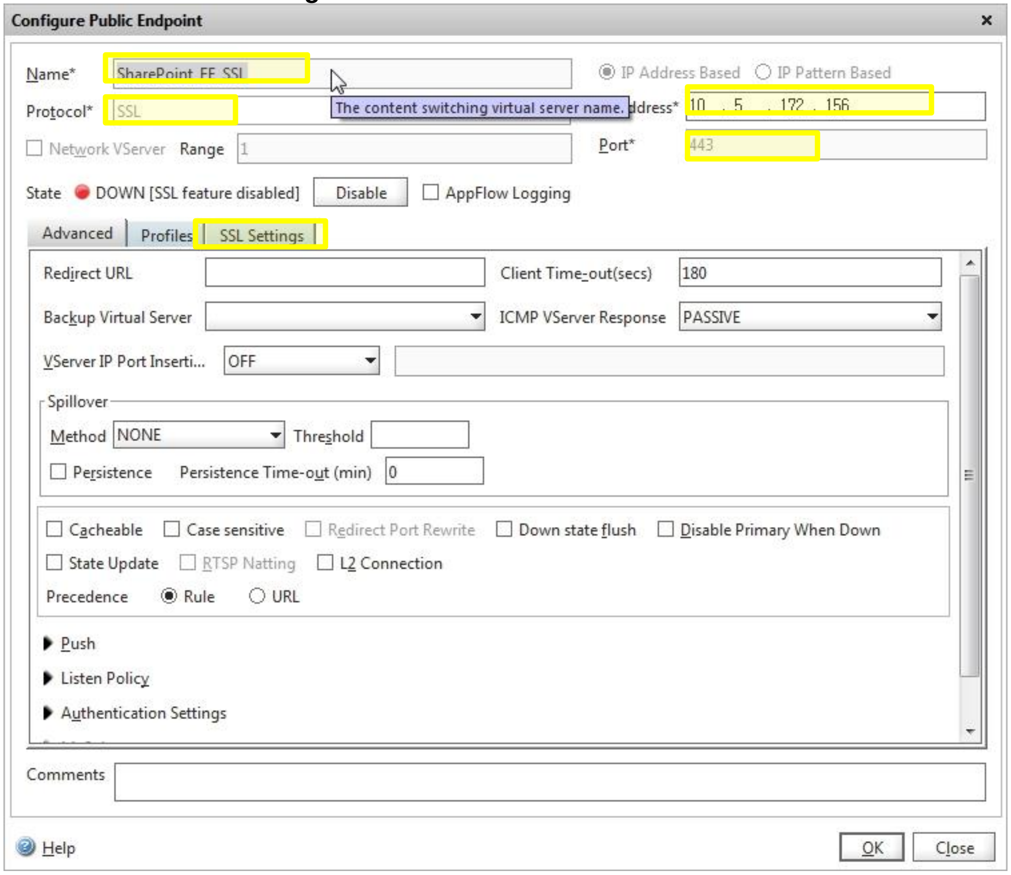
Host Name: 10.5.172.124(ns10) Version: NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20 User: nsroot

Applications	Compression	Caching	Rewrite	Responder	Application Firewall
SharePoint_2010 ●					
FrontPage_Services ●	✚	●	✚	⋖	✚
SOAP_Services ●	✚	✚	✚	⋖	✚
Portal_Management ●	✚	●	✚	⋖	✚
Document_Management ●	✚	●	✚	⋖	✚
Editable_Image_Management ●	✚	●	✚	⋖	✚
ReadOnly_Image_Management ●	✚	●	✚	⋖	✚
Video_Management ●	✚	●	✚	⋖	✚
Audio_Management ●	✚	●	✚	⋖	✚
Styles_and_Scripts ●	✚	●	✚	⋖	✚
Web_Service_Definitions ●	✚	✚	✚	⋖	✚
Web_Service_Schemas ●	✚	✚	✚	⋖	✚
default ●	✚	✚	✚	⋖	✚

Details : SharePoint_2010 > FrontPage_Services (DOWN)

Public Endpoints: SharePoint_FE Backend Services: Not configured (Click to configure) Rule: HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Set **Name** to **SharePoint_FE_SSL** or meaningful name. Set **IP Address** and **Port** to **443**. **Protocol** to **HTTPS**. Click **SSL Settings** tab.



Name* SharePoint_FE_SSL

● IP Address Based ○ IP Pattern Based

Protocol* SSL

The content switching virtual server name.

IP Address* 10 . 5 . 172 . 156

□ Network VServer Range 1

Port* 443

State ● DOWN [SSL feature disabled]

□ AppFlow Logging

Redirect URL

Client Time-out(secs) 180

Backup Virtual Server

ICMP VServer Response PASSIVE

VServer IP Port Inserti... OFF

Spillover

Method NONE Threshold

□ Persistence Persistence Time-out (min) 0

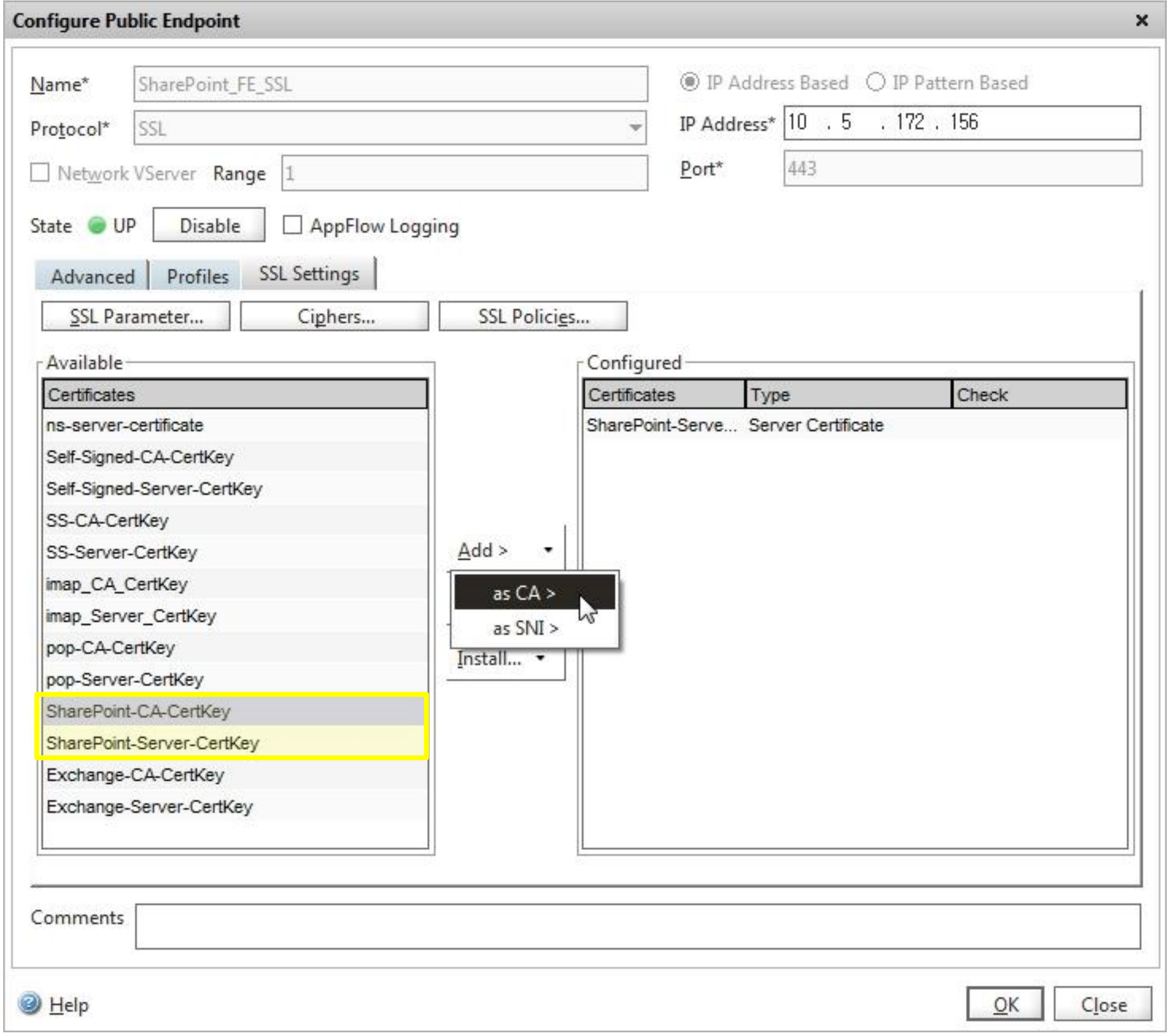
□ Cacheable □ Case sensitive □ Redirect Port Rewrite □ Down state flush □ Disable Primary When Down

□ State Update □ RTSP Natting □ L2 Connection

Precedence ● Rule ○ URL

Comments

Choose the **Certificates** which were created in previous section 5.5. Click the arrow button under **Add>** to choose **as CA>** to add **CA CertKey**.



Configure Public Endpoint

Name* SharePoint_FE_SSL

Protocol* SSL

□ Network VServer Range 1

● IP Address Based ○ IP Pattern Based

IP Address* 10 . 5 . 172 . 156

Port* 443

State ● UP

□ AppFlow Logging

Available

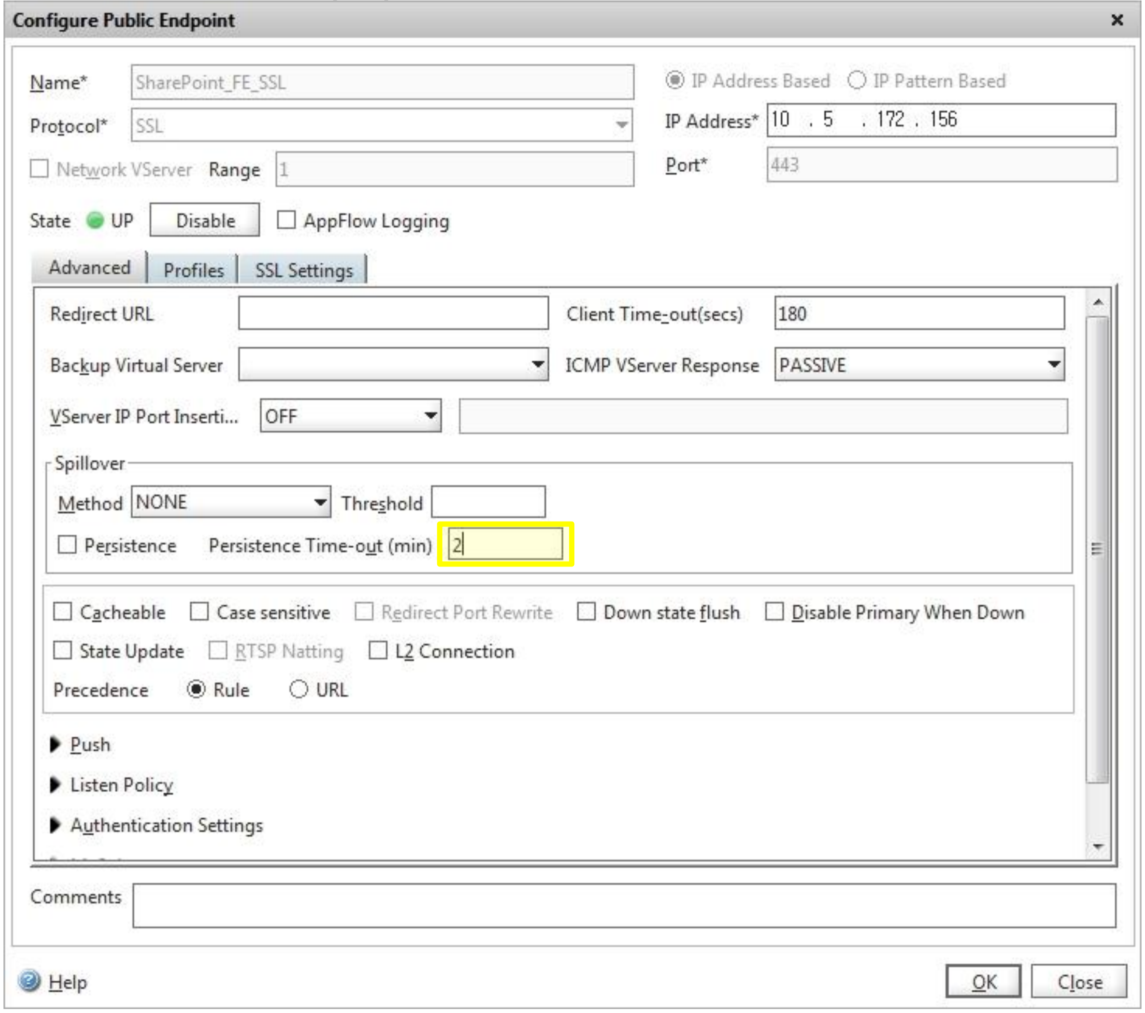
Certificates
ns-server-certificate
Self-Signed-CA-CertKey
Self-Signed-Server-CertKey
SS-CA-CertKey
SS-Server-CertKey
imap_CA_CertKey
imap_Server_CertKey
pop-CA-CertKey
pop-Server-CertKey
SharePoint-CA-CertKey
SharePoint-Server-CertKey
Exchange-CA-CertKey
Exchange-Server-CertKey

Configured

Certificates	Type	Check
SharePoint-Serve...	Server Certificate	

Comments

Set **Persistence Time-out (min)** to **2.** Then click **OK**.



Configure Public Endpoint

Name* SharePoint_FE_SSL

Protocol* SSL

□ Network VServer Range 1

● IP Address Based ○ IP Pattern Based

IP Address* 10 . 5 . 172 . 156

Port* 443

State UP Disable □ AppFlow Logging

Advanced | Profiles | SSL Settings

Redirect URL

Client Time-out(secs) 180

Backup Virtual Server

ICMP VServer Response PASSIVE

VServer IP Port Inserti... OFF

Spillover

Method NONE Threshold

□ Persistence Persistence Time-out (min) 2

□ Cacheable □ Case sensitive □ Redirect Port Rewrite □ Down state flush □ Disable Primary When Down

□ State Update □ RTSP Natting □ L2 Connection

Precedence ● Rule ○ URL

▸ Push

▸ Listen Policy

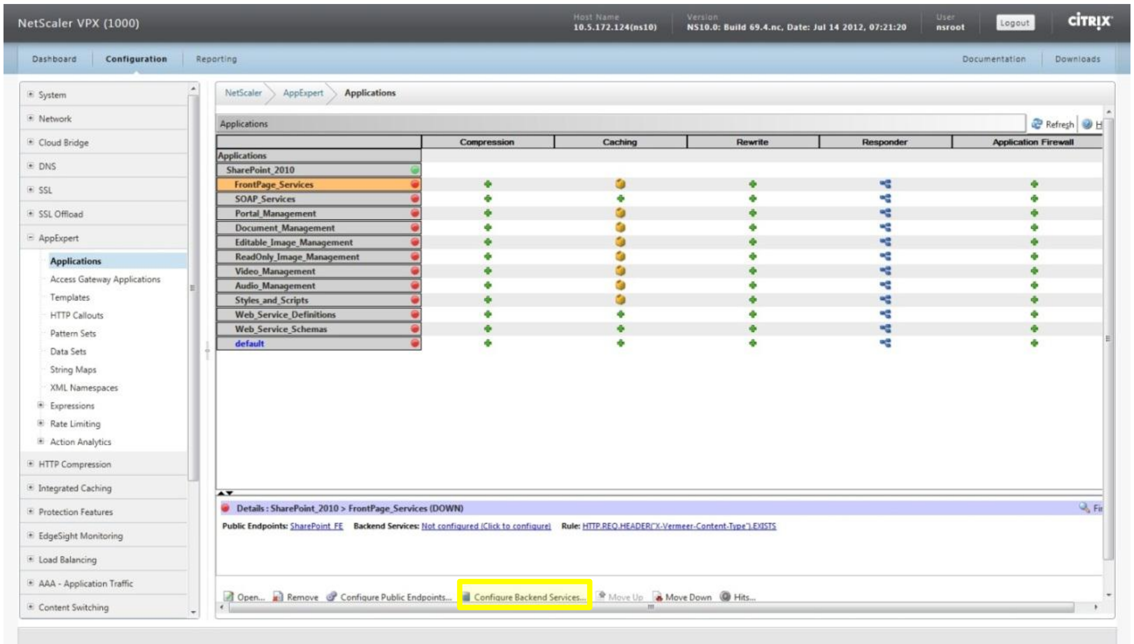
▸ Authentication Settings

Comments

Help OK Close

5.7 Creating a Service Group

From the main NetScaler Configuration Utility screen, under **AppExpert** and **Applications**, and **SharePoint 2010**, choose **Configure Backend Services…** to set **Service Groups** to add physical/VM server IP addresses.

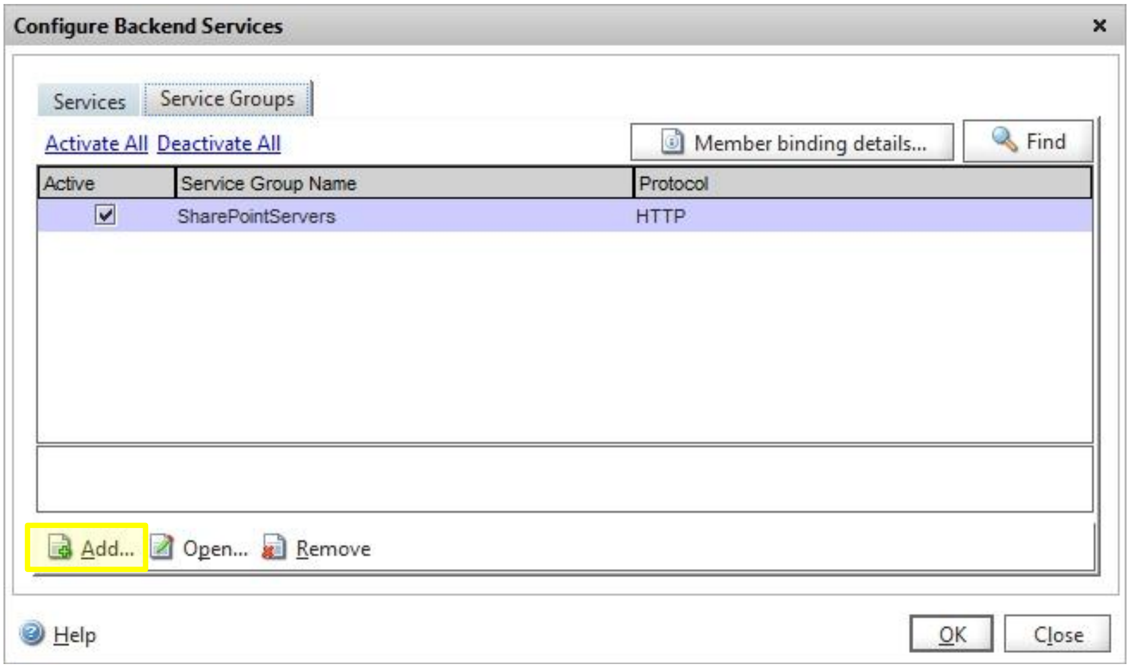


Applications
- SharePoint_2010
  - FrontPage_Services
  - SOAP_Services
  - Portal_Management
  - Document_Management
  - Editable_Image_Management
  - ReadOnly_Image_Management
  - Video_Management
  - Audio_Management
  - Styles_and_Scripts
  - Web_Service_Definitions
  - Web_Service_Schemas
  - default

Details : SharePoint_2010 > FrontPage_Services (DOWN)

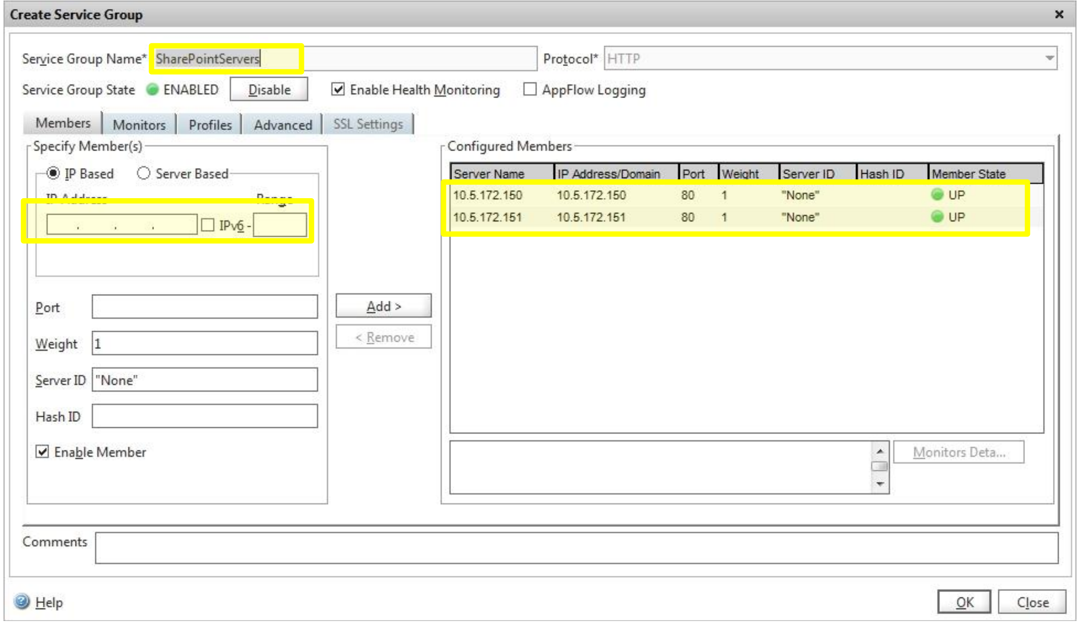
Public Endpoints: SharePoint_FE Backend Services: Not configured (Click to configure) Rule: HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Click **Add**…



Active	Service Group Name	Protocol
☑	SharePointServers	HTTP

Set **Service Group Name** to **SharePointServers** or proper meaningful name. Set **IP address** under **Specify Member(s)**. Then **Add**.



Create Service Group

Service Group Name* SharePointServers

Protocol* HTTP

Service Group State ● ENABLED

☑ Enable Health Monitoring □ AppFlow Logging

Specify Member(s): ● IP Based ○ Server Based

Weight: 1

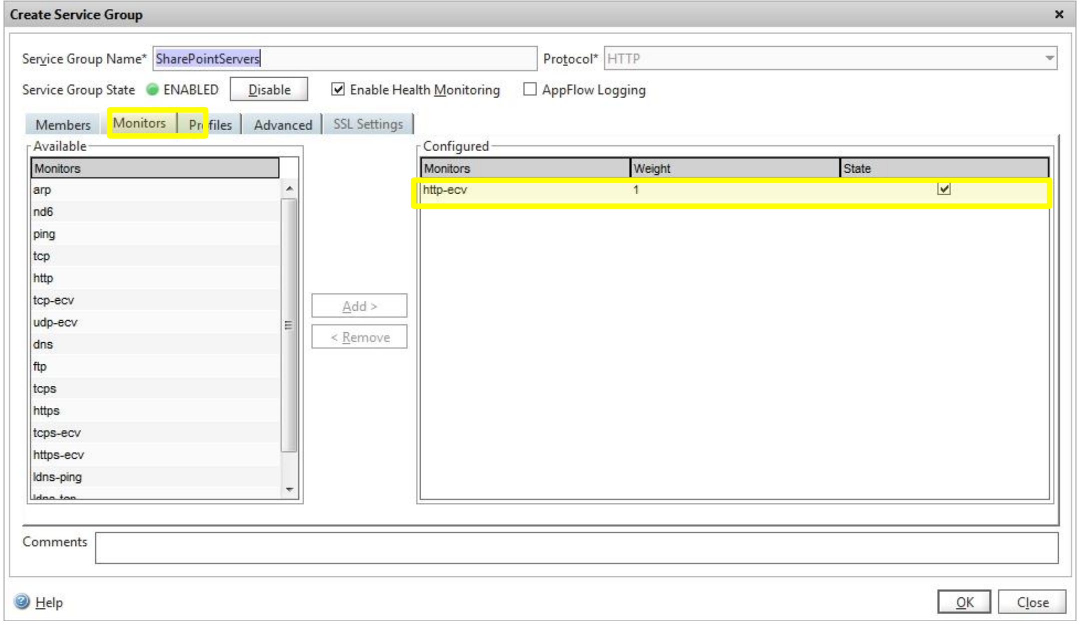
Server ID: "None"

☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.150	10.5.172.150	80	1	"None"		● UP
10.5.172.151	10.5.172.151	80	1	"None"		● UP

Choose **Monitor**. Then add **http-env** .



Create Service Group

Service Group Name* SharePointServers

Protocol* HTTP

Service Group State ● ENABLED

☑ Enable Health Monitoring □ AppFlow Logging

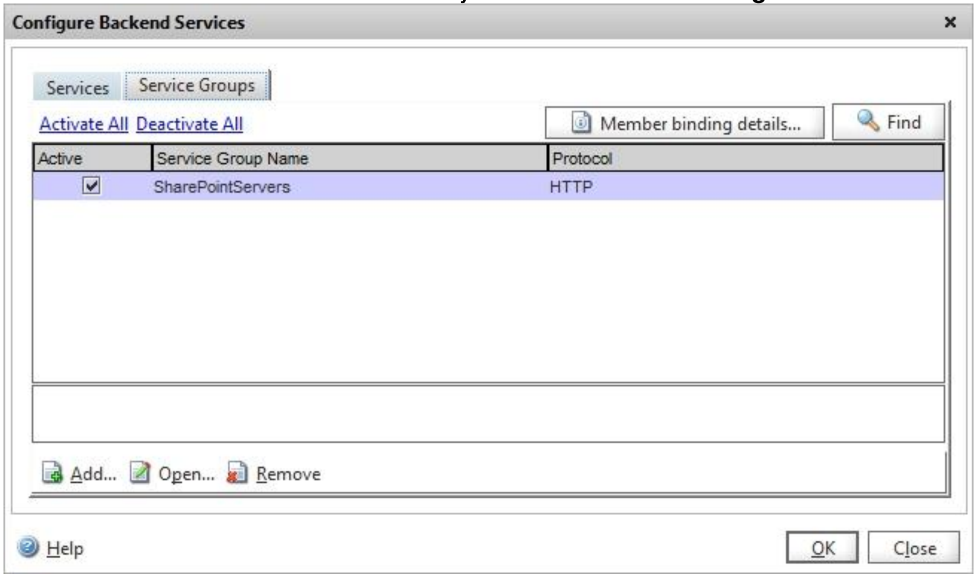
Available

Monitors
arp
nd6
ping
tcp
http
tcp-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping

Configured

Monitors	Weight	State
http-ecv	1	☑

Select **SharePointServers** which was just created under **Configure Backend Services**.



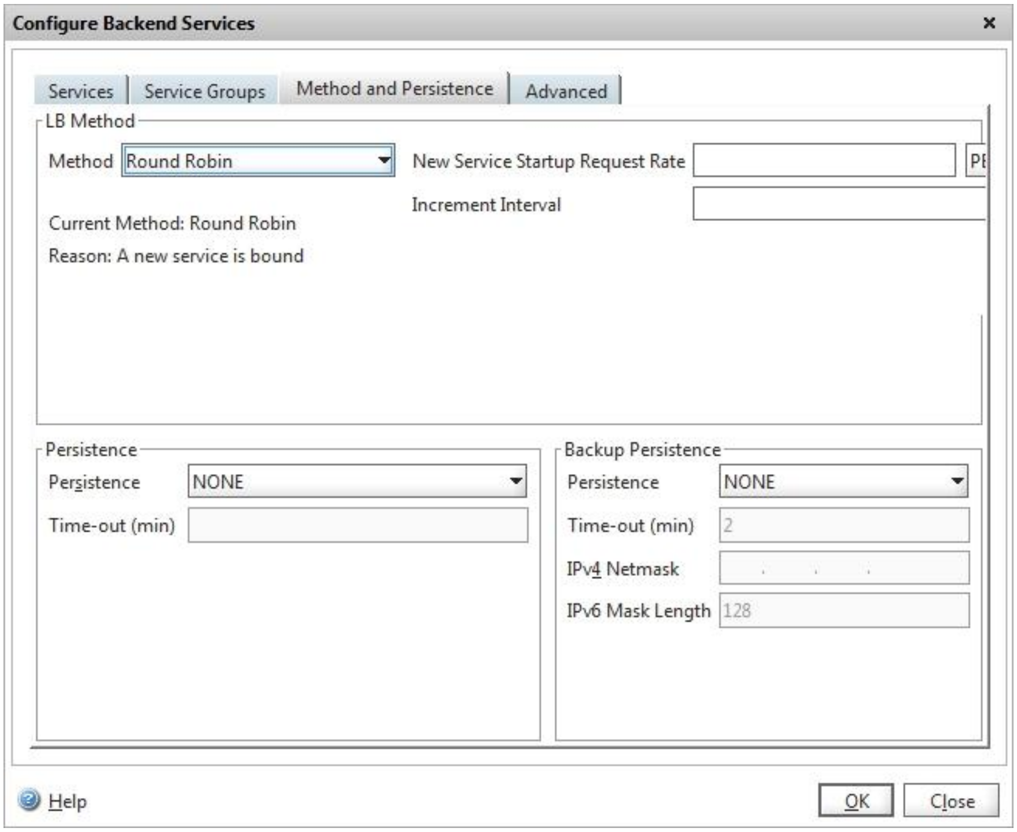
Configure Backend Services

Services | Service Groups

Activate All Deactivate All

Active	Service Group Name	Protocol
☑	SharePointServers	HTTP

Choose **Method and Persistence** to set **Round Robin** under **Method**.



Configure Backend Services

Services | Service Groups | Method and Persistence | Advanced

LB Method

Method: Round Robin

New Service Startup Request Rate:

Increment Interval:

Current Method: Round Robin

Reason: A new service is bound

Persistence

Persistence: NONE

Time-out (min):

Backup Persistence

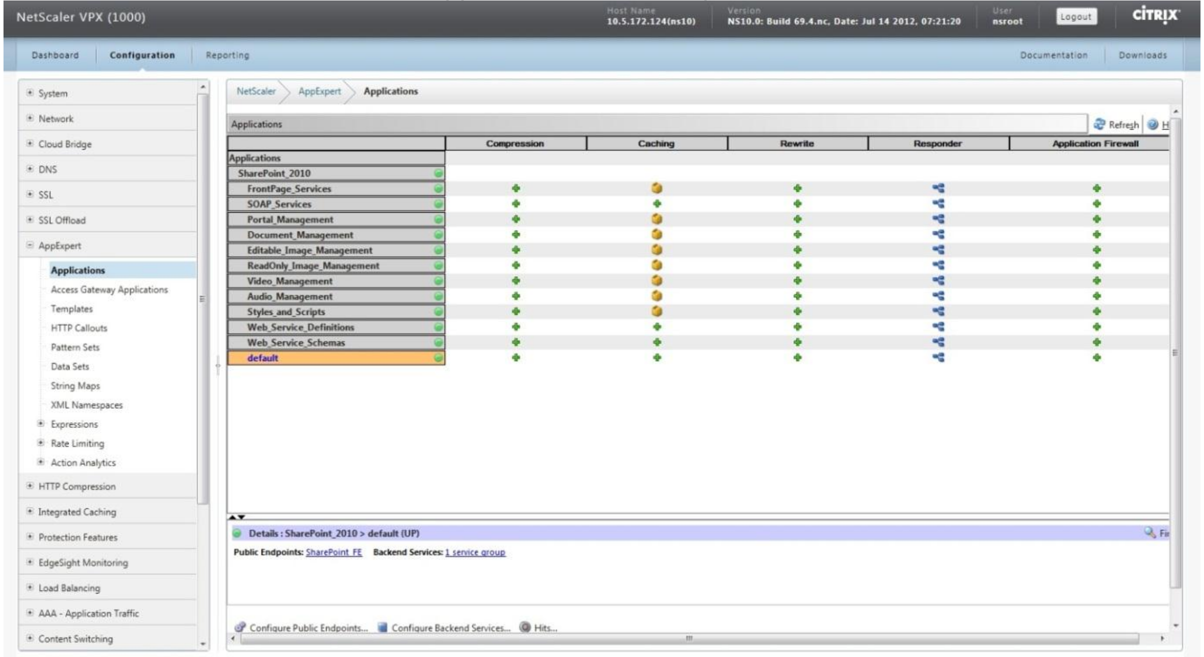
Persistence: NONE

Time-out (min): 2

IPv4 Netmask: . . .

IPv6 Mask Length: 128

All SharePoint 2010 services under Application should be up as shown in **Green** circle.



Applications

Applications	Compression	Caching	Rewrite	Responder	Application Firewall
SharePoint_2010 ●					
FrontPage_Services ●	✚	●	✚	✚	✚
SOAP_Services ●	✚	✚	✚	✚	✚
Portal_Management ●	✚	●	✚	✚	✚
Document_Management ●	✚	●	✚	✚	✚
Editable_Image_Management ●	✚	●	✚	✚	✚
ReadOnly_Image_Management ●	✚	●	✚	✚	✚
Video_Management ●	✚	●	✚	✚	✚
Audio_Management ●	✚	●	✚	✚	✚
Styles_and_Scripts ●	✚	●	✚	✚	✚
Web_Service_Definitions ●	✚	✚	✚	✚	✚
Web_Service_Schemas ●	✚	✚	✚	✚	✚
default ●	✚	✚	✚	✚	✚

Details : SharePoint_2010 > default (UP)

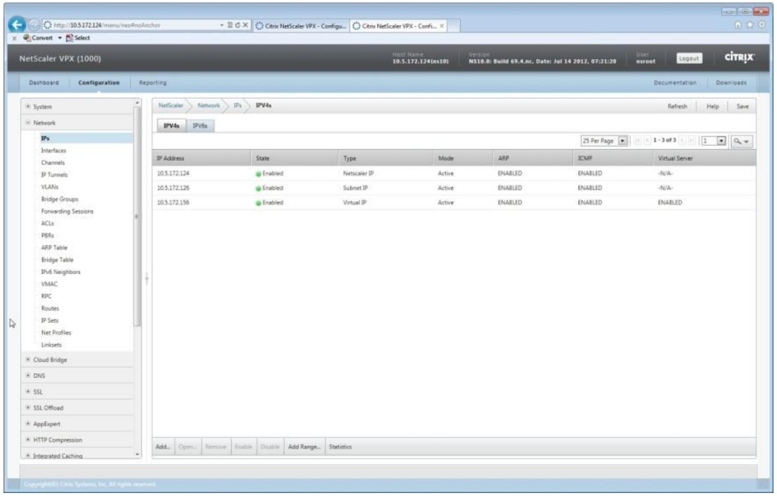
Public Endpoints: SharePoint_FE Backend Services: 1 service group

6. Services Verifications

As described in section 4.1, some required configuration will be added automatically as part of installation and configuration of '*Custom added*' data. Once all the data is installed and configured properly in chapter 5, administrators should be able to confirm and verify other data ('*Auto added'*) which were added automatically.

6.1 Network IPs and Virtual IPs

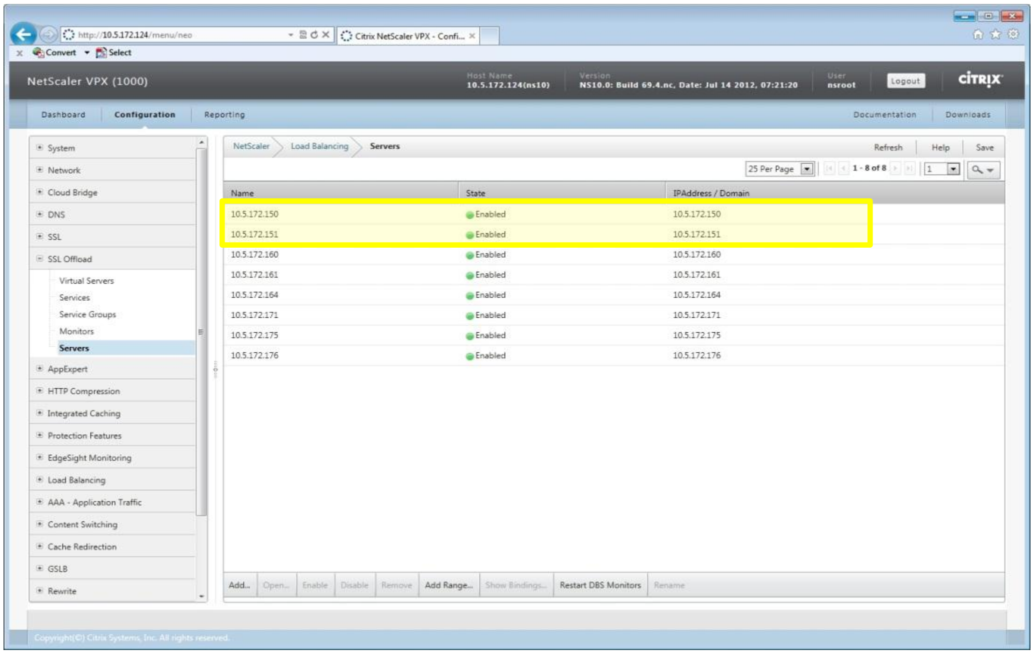
NetScaler IP, **Subnet IP** and **Virtual IP** can be found under **Network>IPs>IPV4s**:



IP Address	State	Type	Mode	ARP	ICMP	Virtual Server
10.5.172.124	● Enabled	Netscaler IP	Active	ENABLED	ENABLED	-N/A-
10.5.172.126	● Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
10.5.172.156	● Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED

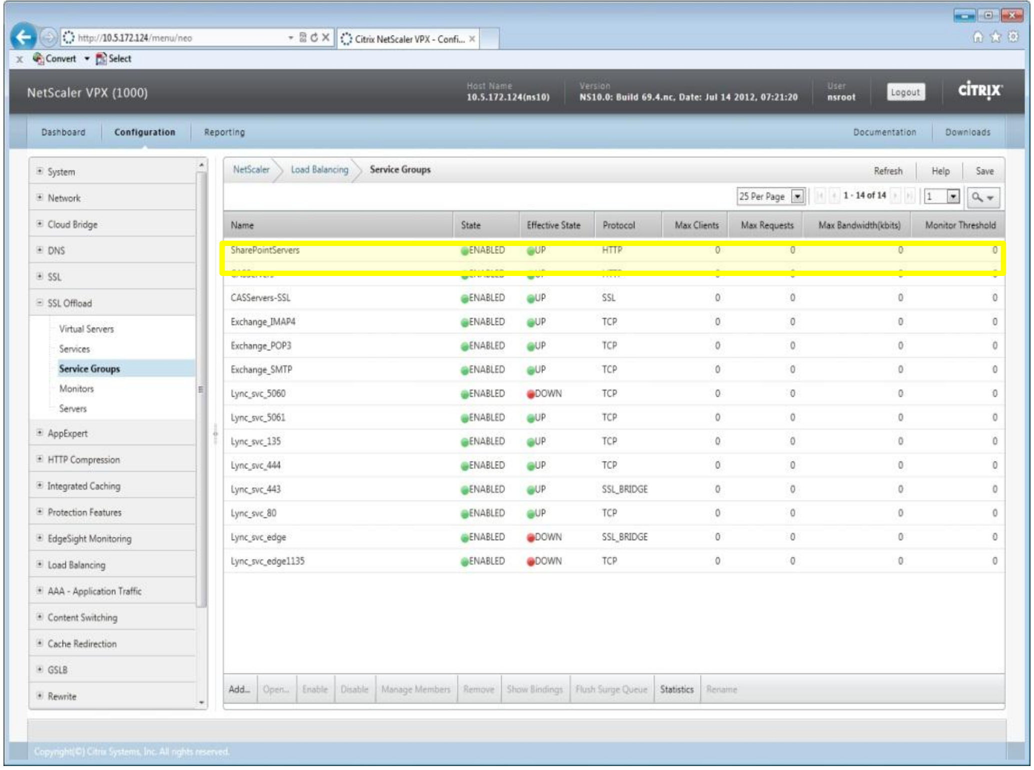
6.2 SSL Offload – Servers, Service Groups

Under **SSL Offload**, *Backend Servers* which were created with *Backend Service Group* can be found under **Servers**:



Name	State	IPAddress / Domain
10.5.172.150	● Enabled	10.5.172.150
10.5.172.151	● Enabled	10.5.172.151
10.5.172.160	● Enabled	10.5.172.160
10.5.172.161	● Enabled	10.5.172.161
10.5.172.164	● Enabled	10.5.172.164
10.5.172.171	● Enabled	10.5.172.171
10.5.172.175	● Enabled	10.5.172.175
10.5.172.176	● Enabled	10.5.172.176

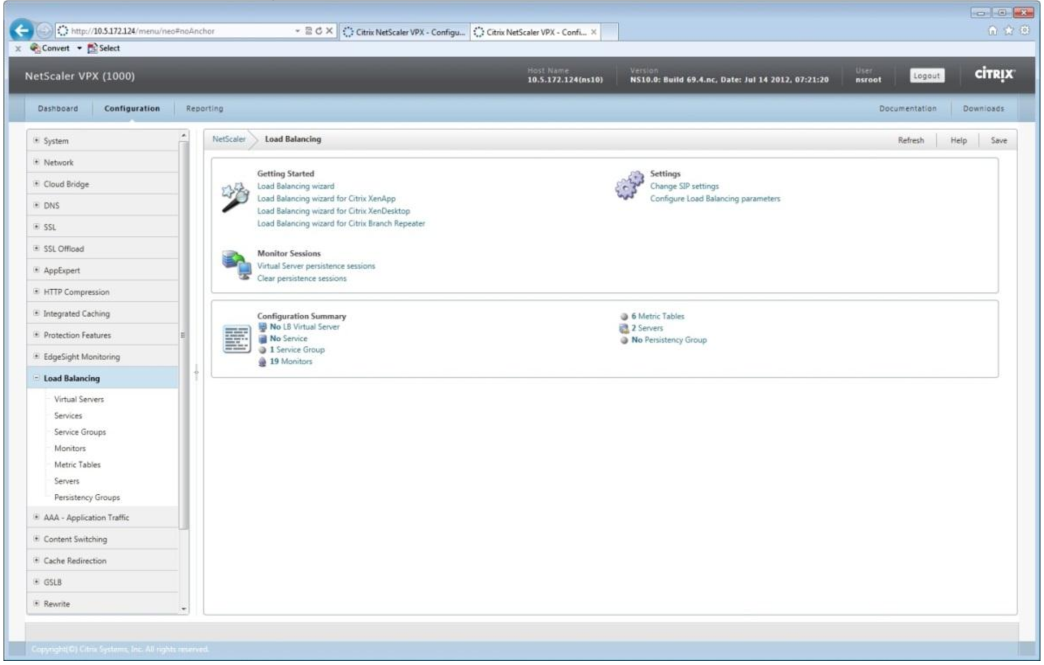
Under **SSL Offload**, *Backend Server Group* which was created can be found under **Service Groups**:



Name	State	Effective State	Protocol	Max Clients	Max Requests	Max Bandwidth(kbits)	Monitor Threshold
SharePointServers	●ENABLED	●UP	HTTP	0	0	0	0
CASServers	●ENABLED	●UP	HTTP	0	0	0	0
CASServers-SSL	●ENABLED	●UP	SSL	0	0	0	0
Exchange_IMAP4	●ENABLED	●UP	TCP	0	0	0	0
Exchange_POP3	●ENABLED	●UP	TCP	0	0	0	0
Exchange_SMTP	●ENABLED	●UP	TCP	0	0	0	0
Lync_svc_5060	●ENABLED	●DOWN	TCP	0	0	0	0
Lync_svc_5061	●ENABLED	●UP	TCP	0	0	0	0
Lync_svc_135	●ENABLED	●UP	TCP	0	0	0	0
Lync_svc_444	●ENABLED	●UP	TCP	0	0	0	0
Lync_svc_443	●ENABLED	●UP	SSL_BRIDGE	0	0	0	0
Lync_svc_80	●ENABLED	●UP	TCP	0	0	0	0
Lync_svc_edge	●ENABLED	●DOWN	SSL_BRIDGE	0	0	0	0
Lync_svc_edge1135	●ENABLED	●DOWN	TCP	0	0	0	0

6.3 Load Balancing – Servers, Service Group

Under **Load Balancing, Servers** and **Service Groups** can be confirmed:



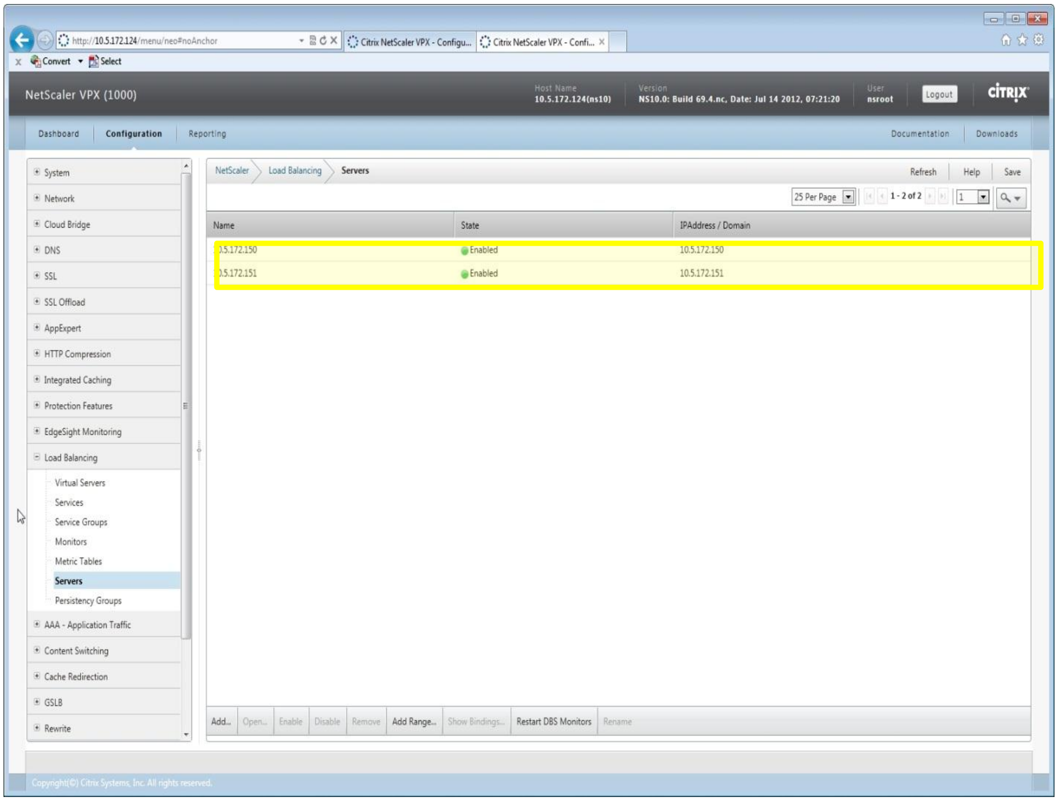
Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

Getting Started
Load Balancing wizard
Load Balancing wizard for Citrix XenApp
Load Balancing wizard for Citrix XenDesktop
Load Balancing wizard for Citrix Branch Repeater

Settings
Change SIP settings
Configure Load Balancing parameters

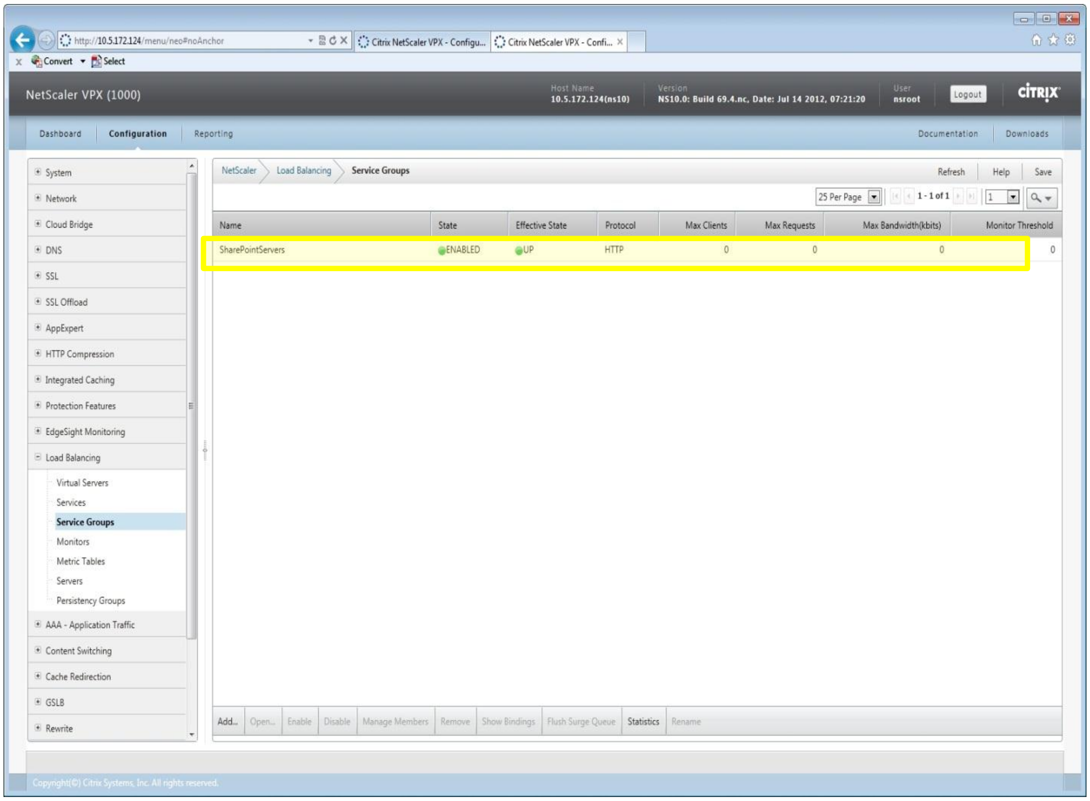
Monitor Sessions
Virtual Server persistence sessions
Clear persistence sessions

Configuration Summary
No LB Virtual Server
No Service
1 Service Group
19 Monitors
6 Metric Tables
2 Servers
No Persistency Group



Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

Name	State	IPAddress / Domain
).5.172.150	● Enabled	10.5.172.150
).5.172.151	● Enabled	10.5.172.151

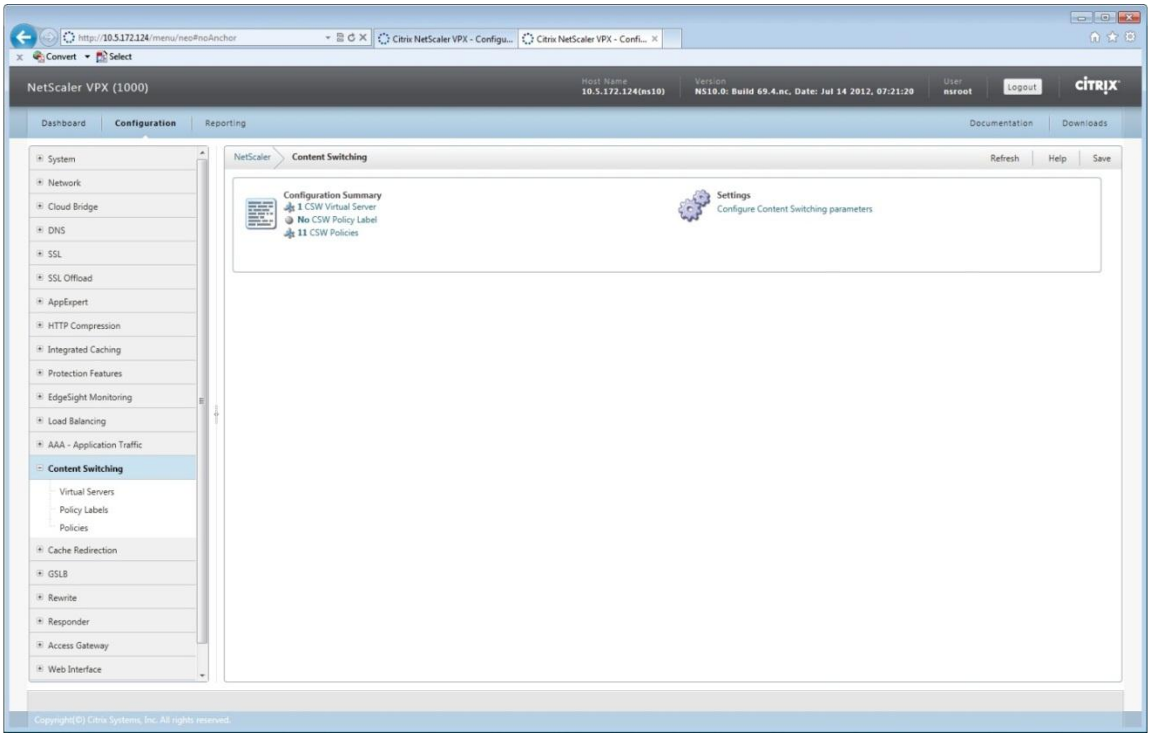


Host Name: 10.5.172.124(ns10)
Version: NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User: nsroot

Name	State	Effective State	Protocol	Max Clients	Max Requests	Max Bandwidth(kbits)	Monitor Threshold
SharePointServers	● ENABLED	● UP	HTTP	0	0	0	0

6.4 Content Switching

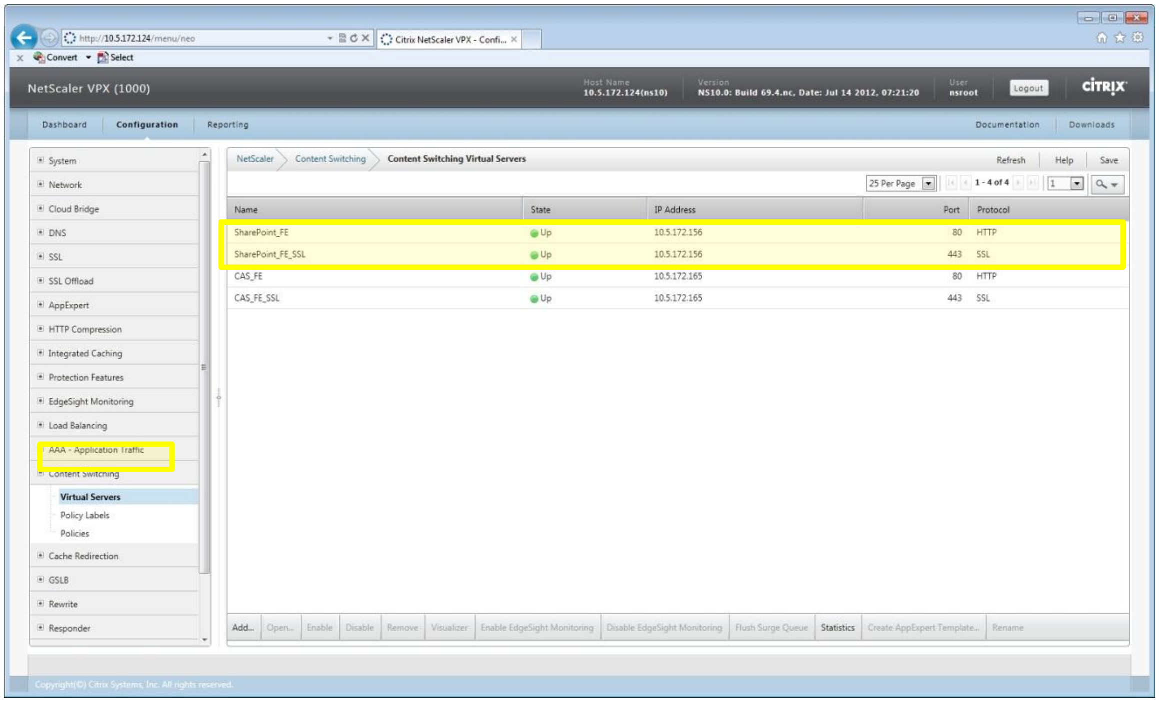
AppExpert Template uses Content Switching to add its virtual server. Under Content Switching, Virtual Servers can be found:



Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

Configuration Summary
1 CSW Virtual Server
No CSW Policy Label
11 CSW Policies

Settings
Configure Content Switching parameters



Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

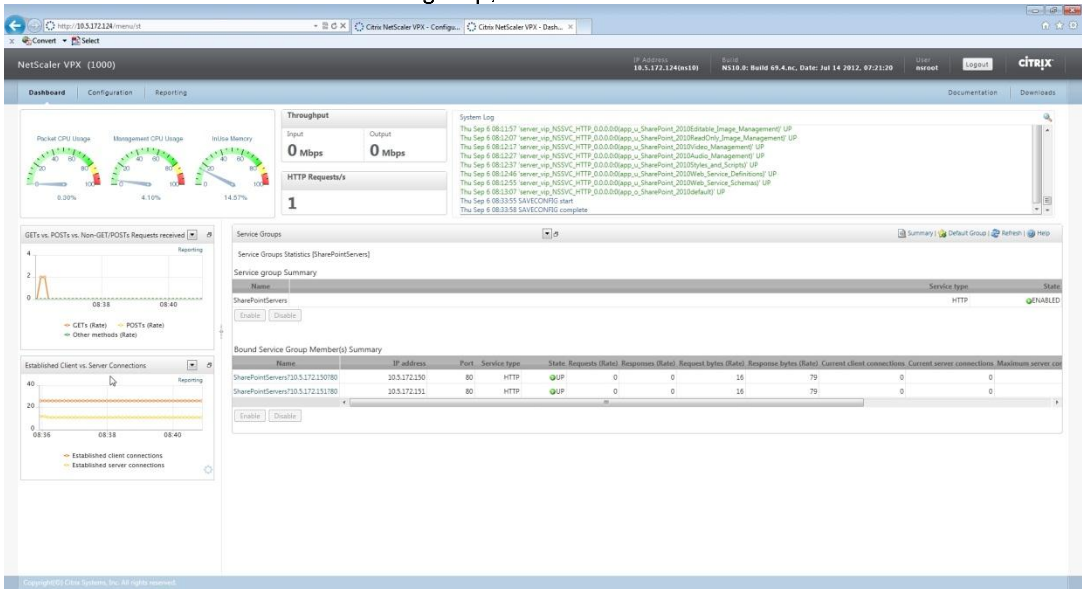
Name	State	IP Address	Port	Protocol
SharePoint_FE	● Up	10.5.172.156	80	HTTP
SharePoint_FE_SSL	● Up	10.5.172.156	443	SSL
CAS_FE	● Up	10.5.172.165	80	HTTP
CAS_FE_SSL	● Up	10.5.172.165	443	SSL

7. Monitoring – NetScaler Dashboard

NetScaler provides **Dashboard** to display System Overviews, Logs, and Service Summary per Service Group(s):

7.1 By Service Groups

Under **SharePointServers** service group, two backend servers can be found for further service details:


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Configu...
Citrix NetScaler VPX - Dash...
Convert
Select
NetScaler VPX (1000)
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
0.30%
Management CPU Usage
4.10%
InUse Memory
14.57%
Throughput
Input
0 Mbps
Output
0 Mbps
HTTP Requests/s
1
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
4
2
0
08:38
08:40
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
08:36
08:38
08:40
Established client connections
Established server connections
Summary | Default Group | Refresh | Help
Enable
Disable
Copyright(C) Citrix Systems, Inc. All rights reserved.

IP Address
10.5.172.124(ns10)
Build
NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User
nsroot

System Log

```
Thu Sep 6 08:11:57 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Editable_Image_Management)' UP
Thu Sep 6 08:12:07 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010ReadOnly_Image_Management)' UP
Thu Sep 6 08:12:17 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Video_Management)' UP
Thu Sep 6 08:12:27 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Audio_Management)' UP
Thu Sep 6 08:12:37 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Styles_and_Scripts)' UP
Thu Sep 6 08:12:46 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Definitions)' UP
Thu Sep 6 08:12:55 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Schemas)' UP
Thu Sep 6 08:13:07 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_o_SharePoint_2010default)' UP
Thu Sep 6 08:33:55 SAVECONFIG start
Thu Sep 6 08:33:58 SAVECONFIG complete
```

Service Groups

Service Groups Statistics [SharePointServers]

Service group Summary

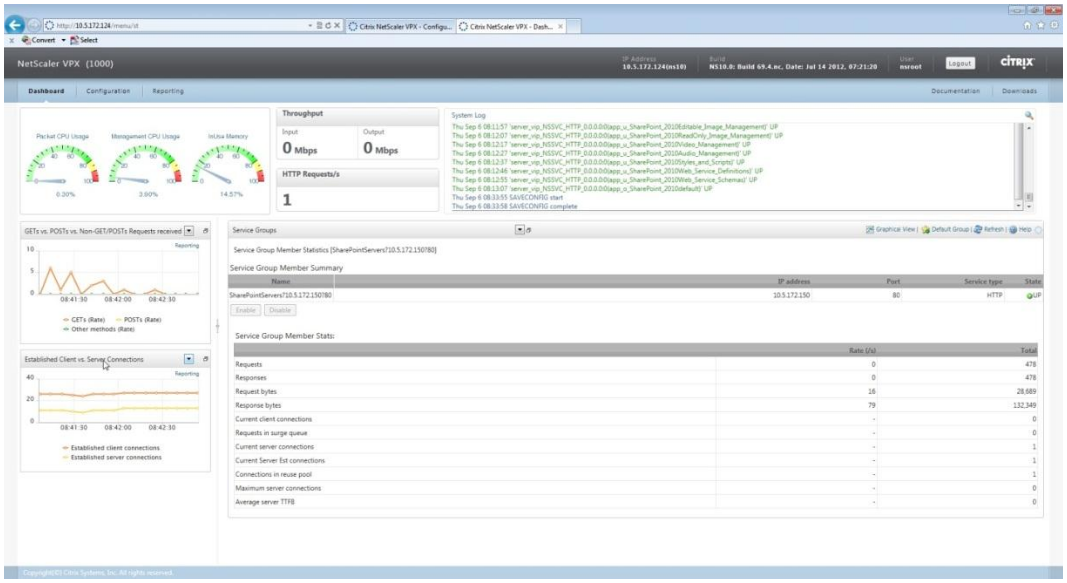
Name	Service type	State
SharePointServers	HTTP	●ENABLED

Bound Service Group Member(s) Summary

Name	IP address	Port	Service type	State	Requests (Rate)	Responses (Rate)	Request bytes (Rate)	Response bytes (Rate)	Current client connections	Current server connections	Maximum server cor
SharePointServers?10.5.172.150?80	10.5.172.150	80	HTTP	●UP	0	0	16	79	0	0	
SharePointServers?10.5.172.151?80	10.5.172.151	80	HTTP	●UP	0	0	16	79	0	0	

7.2 Per Server

Under **SharePointServers Name** service group, service details including # of Requests, Reponses can be found:


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Configu...
Citrix NetScaler VPX - Dash...
Convert
Select
NetScaler VPX (1000)
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
0.30%
Management CPU Usage
3.90%
InUse Memory
14.57%
Throughput
Input
0 Mbps
Output
0 Mbps
HTTP Requests/s
1
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
10
5
0
08:41:30
08:42:00
08:42:30
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
08:41:30
08:42:00
08:42:30
Established client connections
Established server connections
Graphical View | Default Group | Refresh | Help
Enable
Disable
Copyright(C) Citrix Systems, Inc. All rights reserved.

IP Address
10.5.172.124(ns10)
Build
NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User
nsroot

System Log

```
Thu Sep 6 08:11:57 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Editable_Image_Management)' UP
Thu Sep 6 08:12:07 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010ReadOnly_Image_Management)' UP
Thu Sep 6 08:12:17 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Video_Management)' UP
Thu Sep 6 08:12:27 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Audio_Management)' UP
Thu Sep 6 08:12:37 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Styles_and_Scripts)' UP
Thu Sep 6 08:12:46 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Definitions)' UP
Thu Sep 6 08:12:55 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Schemas)' UP
Thu Sep 6 08:13:07 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_o_SharePoint_2010default)' UP
Thu Sep 6 08:33:55 SAVECONFIG start
Thu Sep 6 08:33:58 SAVECONFIG complete
```

Service Groups

Service Group Member Statistics [SharePointServers?10.5.172.150?80]

Service Group Member Summary

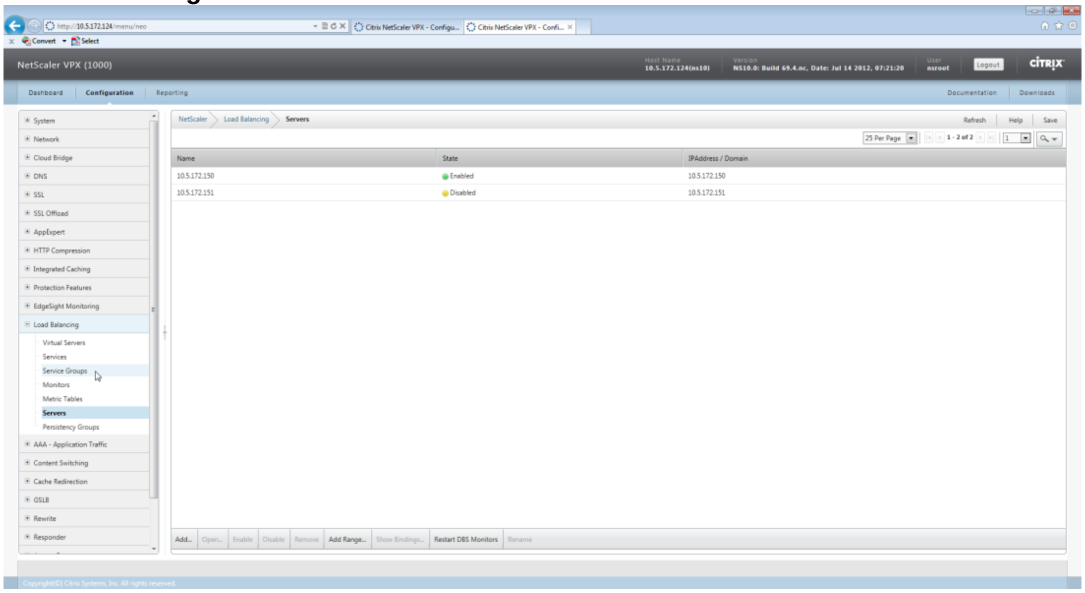
Name	IP address	Port	Service type	State
SharePointServers?10.5.172.150?80	10.5.172.150	80	HTTP	●UP

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	478
Responses	0	478
Request bytes	16	28,689
Response bytes	79	132,349
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	1
Current Server Est connections	-	1
Connections in reuse pool	-	1
Maximum server connections	-	0
Average server TTFB	-	0

7.3 Server Failure Event

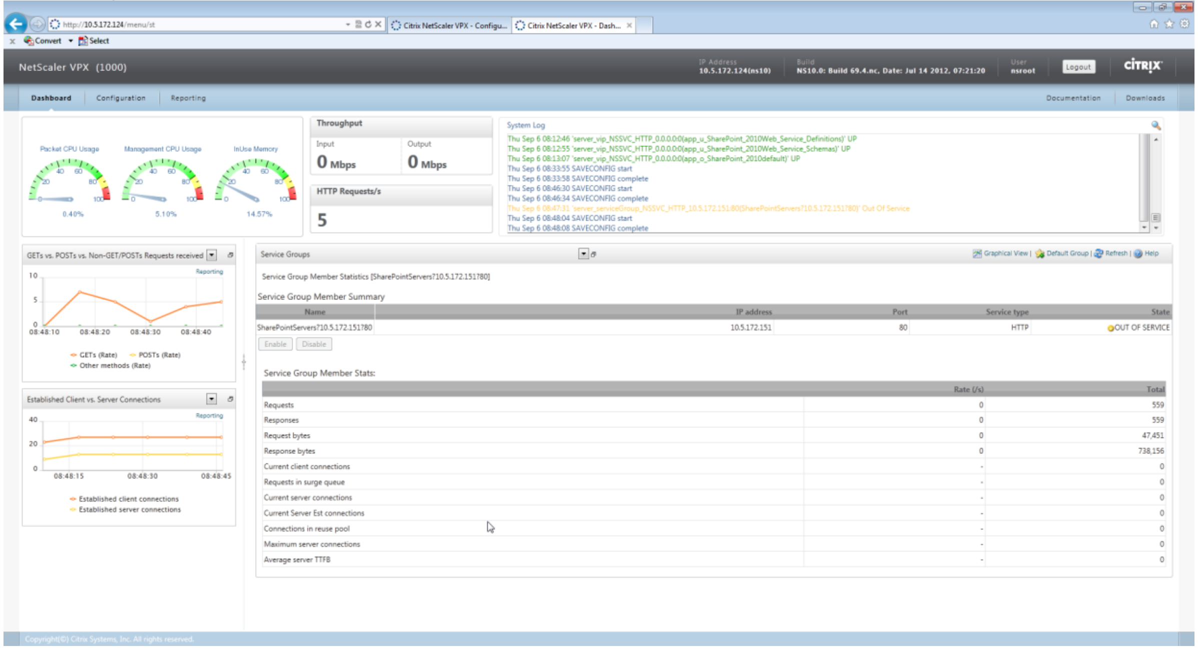
In an event of server failure, the failed server will be **yellow** color-coded and its status can be found in **Load Balancing>Servers:**



Host Name 10.5.172.124(ns10) | Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20 | User nsroot

Name	State	IPAddress / Domain
10.5.172.150	● Enabled	10.5.172.150
10.5.172.151	● Disabled	10.5.172.151

Also the individual server status can be found in **Dashboard>Service Groups>Service Group Member Summary:**



IP Address 10.5.172.124(ns10) | Build NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20 | User nsroot

System Log

```
Thu Sep 6 08:12:46 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Definitions)' UP
Thu Sep 6 08:12:55 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Schemas)' UP
Thu Sep 6 08:13:07 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_o_SharePoint_2010default)' UP
Thu Sep 6 08:33:55 SAVECONFIG start
Thu Sep 6 08:33:58 SAVECONFIG complete
Thu Sep 6 08:46:30 SAVECONFIG start
Thu Sep 6 08:46:34 SAVECONFIG complete
Thu Sep 6 08:47:31 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151?80)' Out Of Service
Thu Sep 6 08:48:04 SAVECONFIG start
Thu Sep 6 08:48:08 SAVECONFIG complete
```

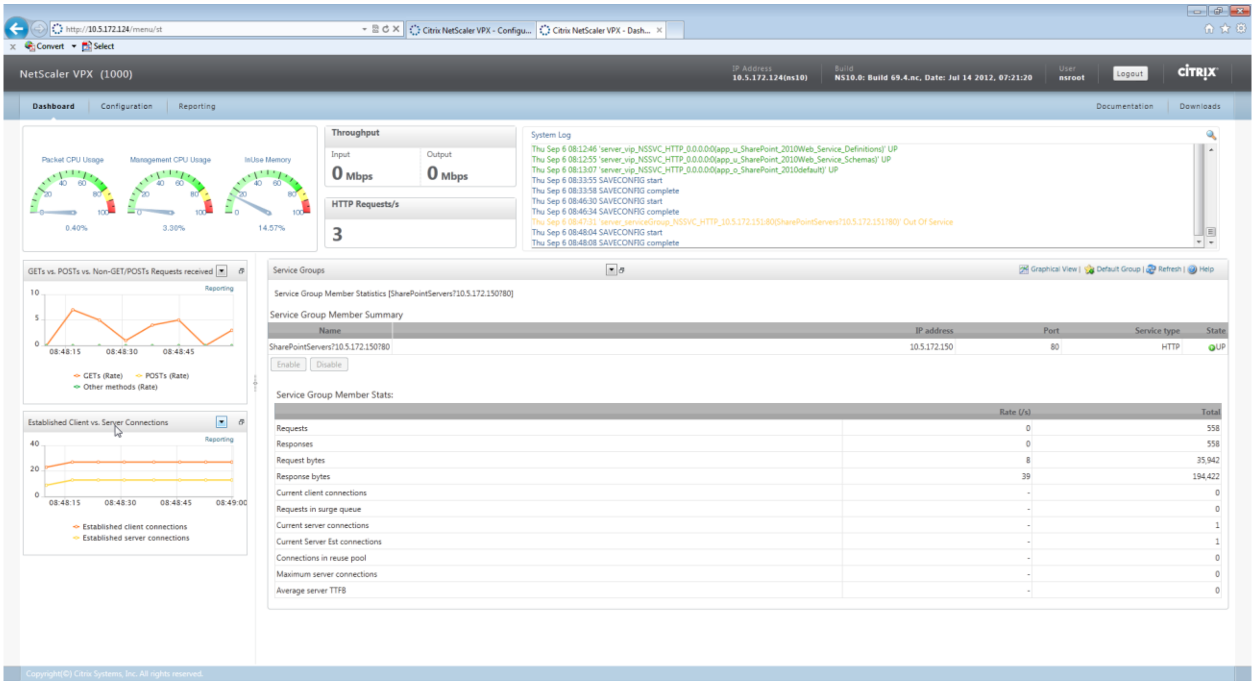
Service Group Member Statistics [SharePointServers?10.5.172.151?80]

Service Group Member Summary

Name	IP address	Port	Service type	State
SharePointServers?10.5.172.151?80	10.5.172.151	80	HTTP	● OUT OF SERVICE

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	559
Responses	0	559
Request bytes	0	47,451
Response bytes	0	738,156
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	0
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0



System Log

```
Thu Sep 6 08:12:46 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Definitions)' UP
Thu Sep 6 08:12:55 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_u_SharePoint_2010Web_Service_Schemas)' UP
Thu Sep 6 08:13:07 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_o_SharePoint_2010default)' UP
Thu Sep 6 08:33:55 SAVECONFIG start
Thu Sep 6 08:33:58 SAVECONFIG complete
Thu Sep 6 08:46:30 SAVECONFIG start
Thu Sep 6 08:46:34 SAVECONFIG complete
Thu Sep 6 08:47:31 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151?80)' Out Of Service
Thu Sep 6 08:48:04 SAVECONFIG start
Thu Sep 6 08:48:08 SAVECONFIG complete
```

Service Group Member Statistics [SharePointServers?10.5.172.150?80]

Service Group Member Summary

Name	IP address	Port	Service type	State
SharePointServers?10.5.172.150?80	10.5.172.150	80	HTTP	●UP

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	558
Responses	0	558
Request bytes	8	35,942
Response bytes	39	194,422
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	1
Current Server Est connections	-	1
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0

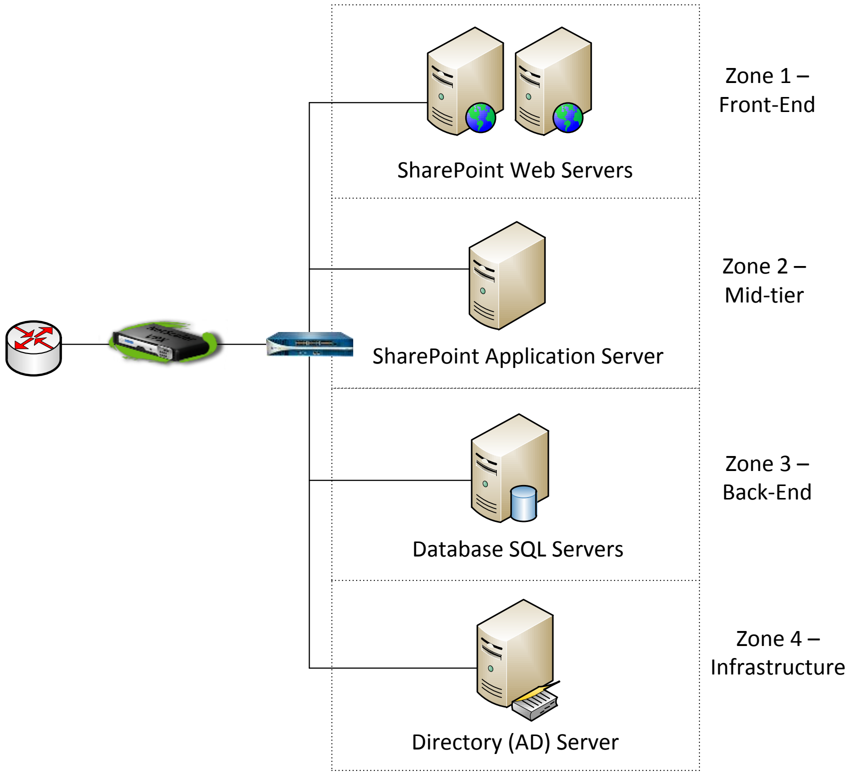
8. Palo Alto Networks Next-Generation Firewall Deployment

The Palo Alto Networks next-generation firewall safely enables enterprise applications in the data center and delivers meaningful segmentation by application, user and content. It identifies all traffic sent to the Microsoft Sharepoint servers, based on actual application, not just port or protocol. Access to the Microsoft Sharepoint servers can be further restricted to only the authorized users or groups. All content is scanned for malicious content - viruses, malware, and spyware – and dropped before they can reach the data center servers.

8.1 Data Center Segmentation

In a standard Sharepoint implementation, there are multiple Sharepoint server roles, including web servers, database servers, search service and other service application roles. In small deployments, some of these services may be combined on a single server, but in large-scale enterprise deployments, there will be multiple servers dedicated to each role. In order to properly segment and secure the Sharepoint implementation, the different server roles will be isolated in dedicated security zones that can only be accessed by authorized users with authorized applications.

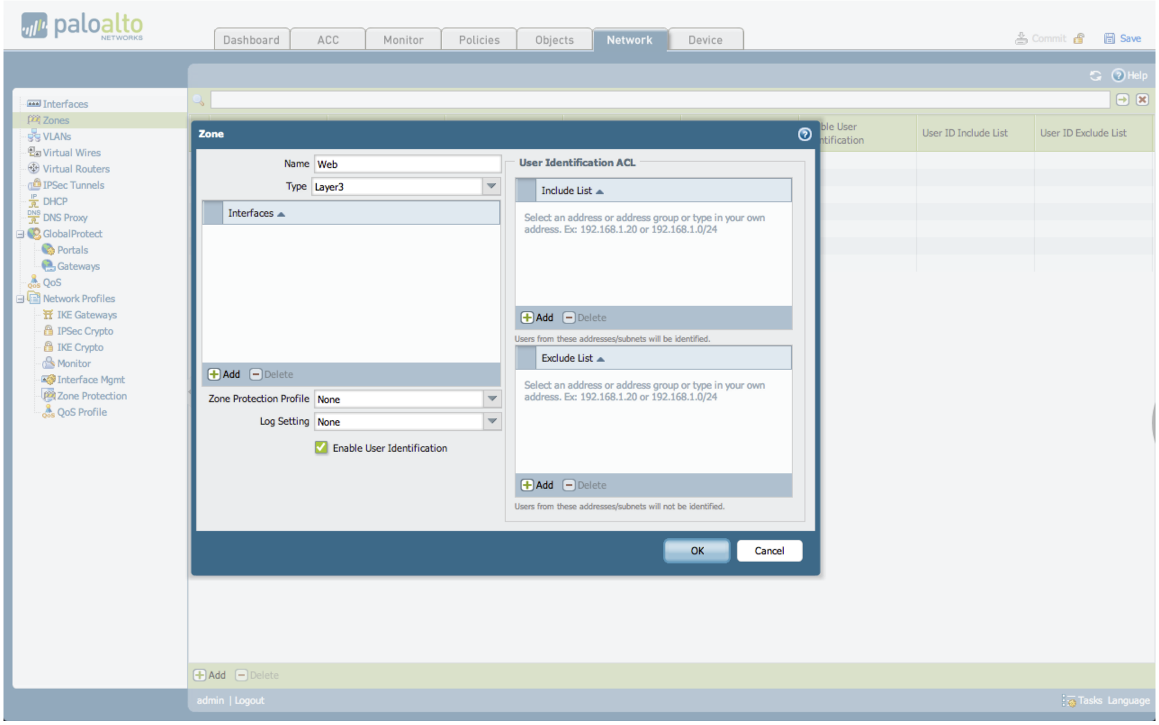
In this reference design, there are three Sharepoint security zones. The Web zone will contain the dedicated web servers. There will be multiple servers, which are load-balanced by the Citrix Netscaler. The Application zone will contain the service application server. This will also be where the Sharepoint Central Administration (SPCA) tool will be run. The SQL servers will be located in the Database zone. Users and administrators from outside the Sharepoint zones will access the servers from the External zone. Finally, the Active Directory domain controller will be used for authentication and will be located in a data center infrastructure zone. All traffic between zones will be specifically enabled by security policy.



To build these segments in the Palo Alto Networks firewall, the following zones will be created:

Web – Sharepoint Web Servers
Application – Sharepoint Application Servers
Database – MS SQL Servers
Active-Directory – Domain controller
External – Users and administrators

For example, to create the Web zone, go to the Network tab, under the Zone section and click Add.



Zone

Name: Web

Type: Layer3

Zone Protection Profile: None

Log Setting: None

☑ Enable User Identification

User Identification ACL

Include List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

Exclude List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Enter the name of the zone, the type – Layer2 or Layer3, and click the check box for Enable User Identification.

Repeat this for each of the required zones.

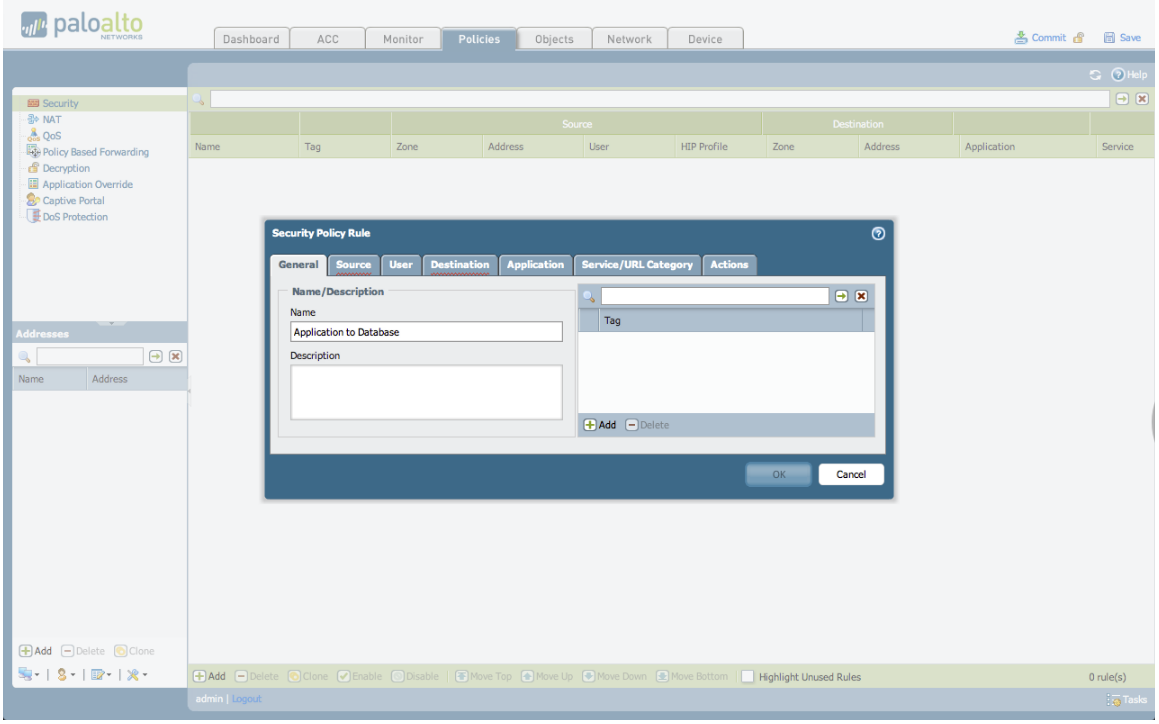
8.2 Security Policy

Palo Alto Networks security policy is zone based. Each segment in a data center deployment will be in a separate zone. Once the traffic flow is understood, the security policy can be written based on actual application, not just ports and port ranges. Allowing the following protocols between the specified zones will enable the Sharepoint application, while restricting non-Sharepoint traffic.

Every Sharepoint implementation is different, and the specific list of applications may vary depending on what services are used, but this will be starting reference for a working Sharepoint security policy.

Source Zone	Destination Zone	Application
Active-Directory	External	Dns
Application	Active-Directory	dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss ntp
Application	Database	mssql-db
Application	External	dns ldap web-browsing
Database	Active-Directory	dns kerberos ldap ms-ds-smb netbios-dg netbios-ss
Database	External	Ldap
External	Active-Directory	active-directory dns ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss ntp
External	Application	sharepoint-admin sharepoint-base web-browsing
External	Web	sharepoint-base sharepoint-calendar web-browsing
Web	Active-Directory	active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss ntp
Web	Database	mssql-db
Web	External	active-directory dns ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss ssl web-browsing

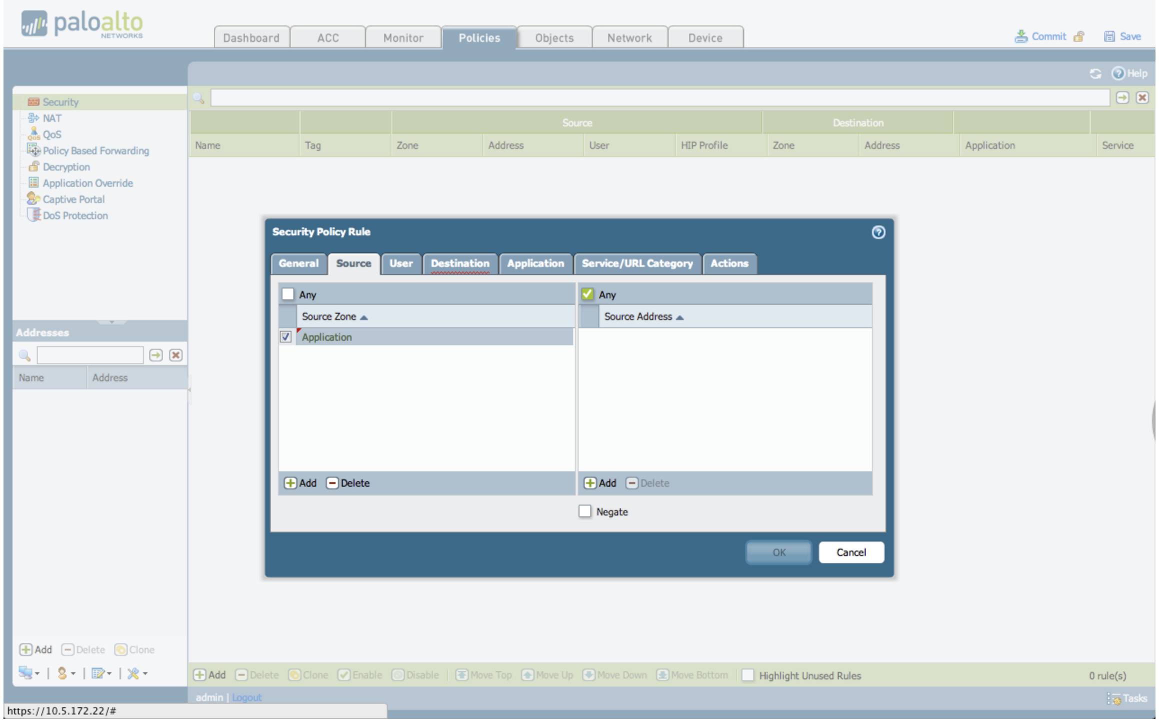
To create the security policy, each of these source and destination zone pairs will represent one line in the security policy. For example, to create the “Application to Database” security policy line on the Palo Alto Networks firewall, go to the Policies tab (on top), and the Security section (on left), and click Add (on bottom). Enter the name of the security policy line.



Name: Application to Database

Description:

Click on the Source tab and click Add. Select the Application zone.



☐ Any

Source Zone ▲

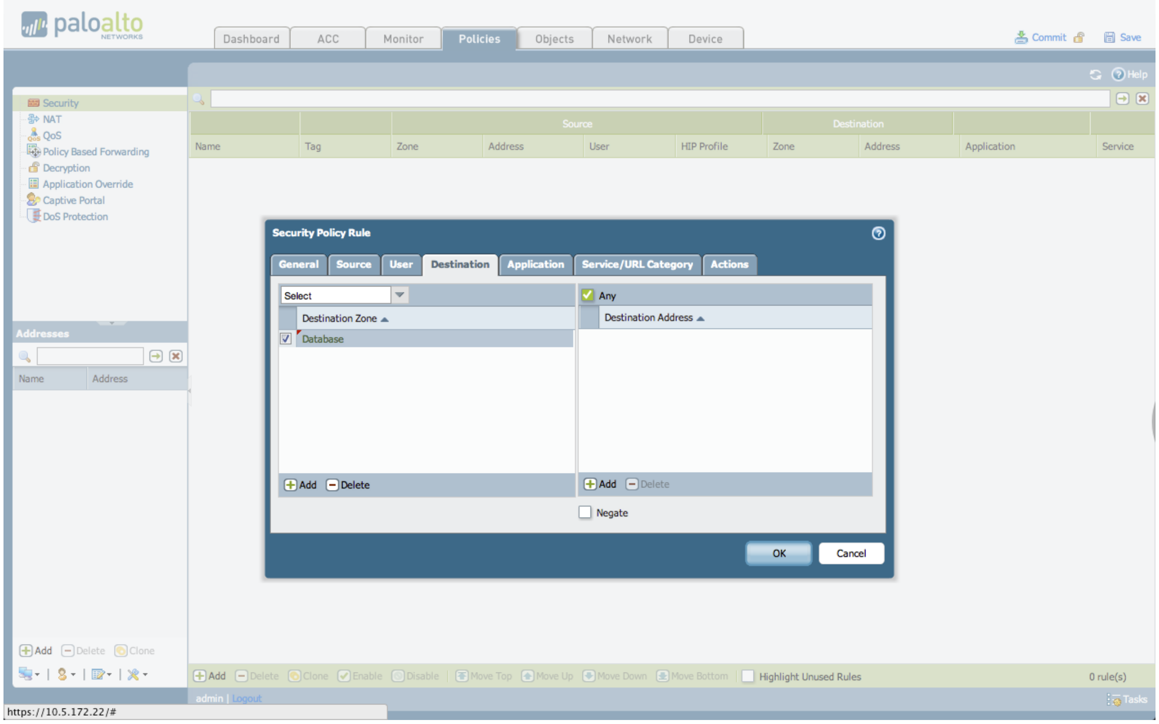
☑ Application

☑ Any

Source Address ▲

☐ Negate

Click on the Destination tab and click Add. Select the Database zone.



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

Select

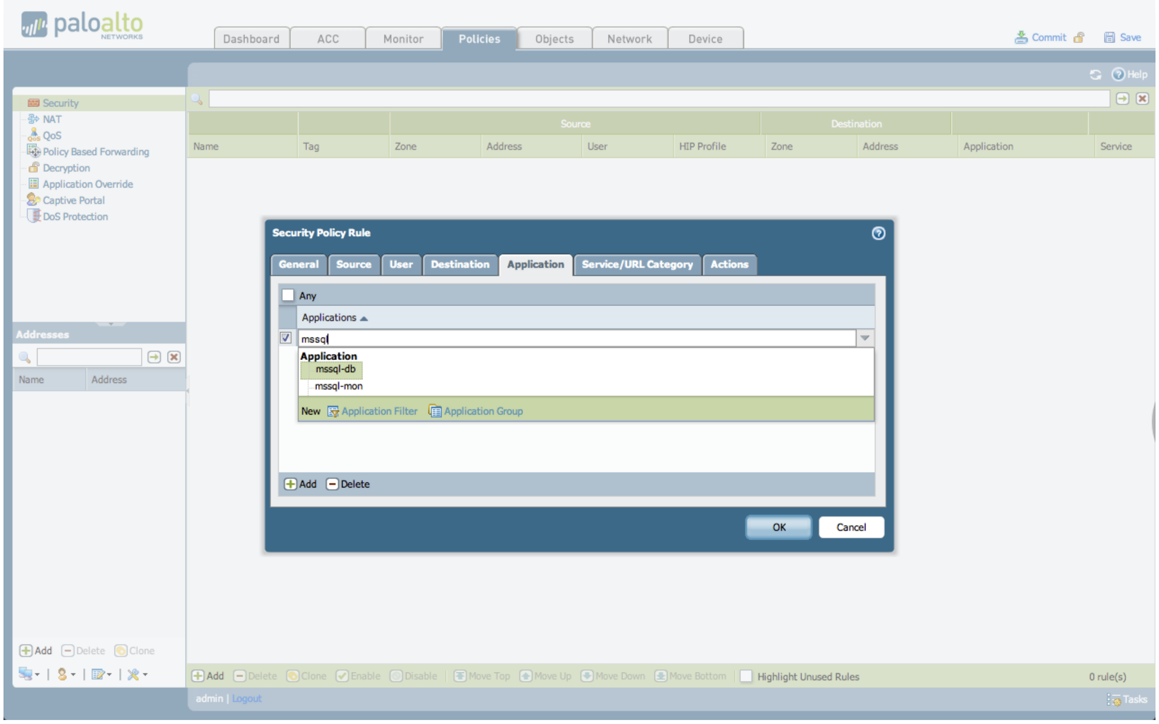
	Destination Zone ▲
☑	Database

☑ Any

Destination Address ▲

☐ Negate

Click on the Application tab and click Add. One application will be added to this rule: mssql-db. Begin typing the first application name and select it when it appears in the list.



Security Policy Rule

General | Source | User | Destination | Application | Service/URL Category | Actions

☐ Any

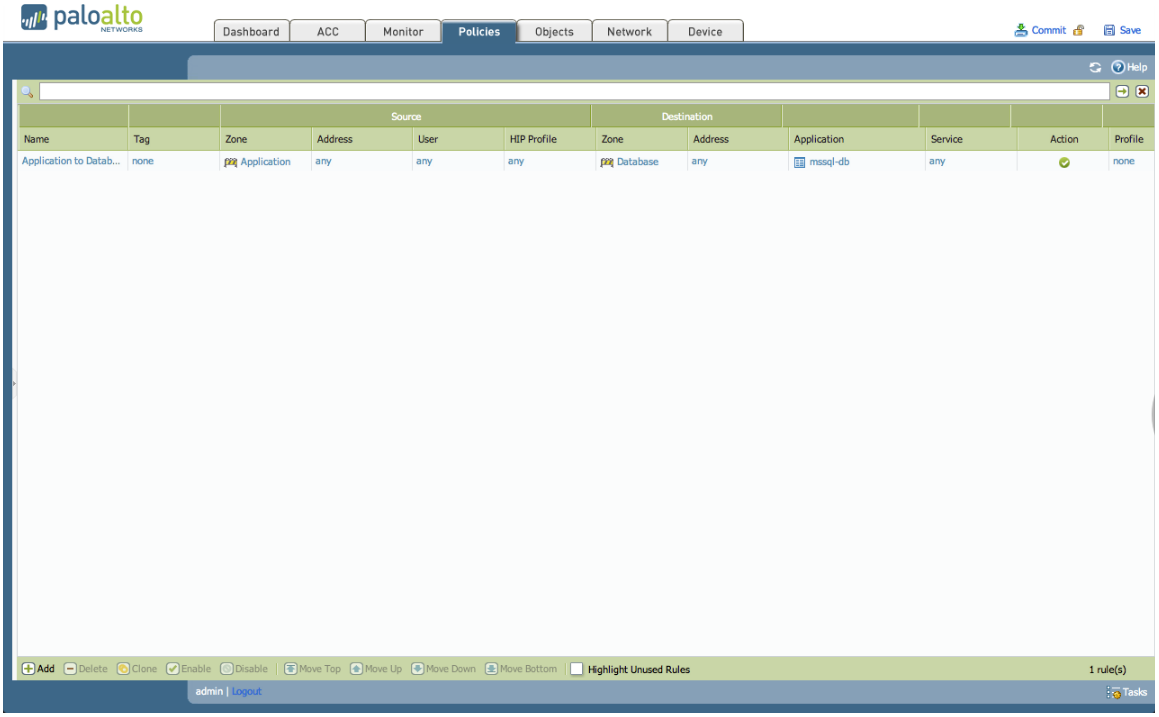
Applications ▲

☑ mssql

Application
mssql-db
mssql-mon

Repeat for any remaining applications in this rule.

Click OK. The rule will be added to the security policy. Repeat this process for each of the source and destination zone pairs listed above.



		Source				Destination					
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
Application to Datab...	none	Application	any	any	any	Database	any	mssql-db	any	✓	none

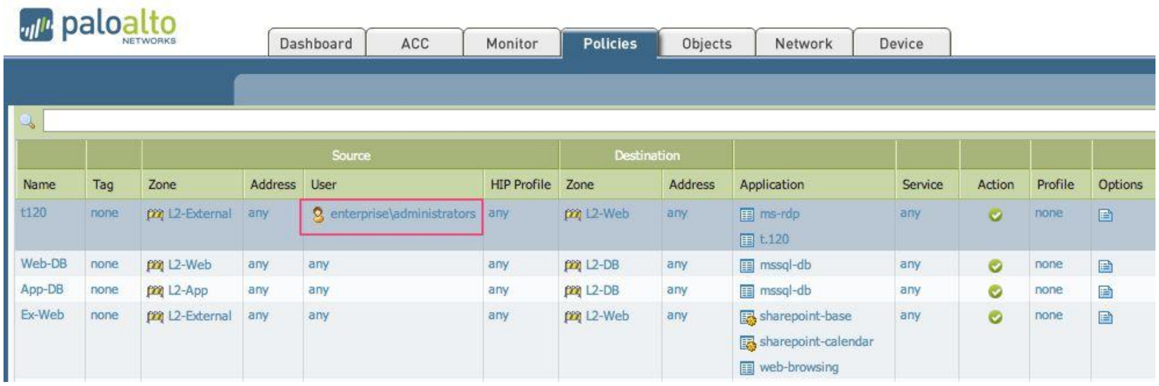
□ Highlight Unused Rules

1 rule(s)

8.3 User Identification

The Palo Alto Networks firewall also allows security policy to be further refined by end user or group, not just source IP. Certain servers, or certain applications in the data center may only need to be accessed by specific people or groups. The next-generation firewall will retrieve user and group information from the local user directory service, and allow that information to be used in security policies.

For example, the Sharepoint servers may need to be accessible by System Administrators with Remote Desktop for management purposes. The rest of the enterprise does not need this access.
The security policy rule allowing the applications, in this case, ms-rdp and t.120, would only be accessible by the administrators group. The Sharepoint applications would be accessible by the entire company via client applications.



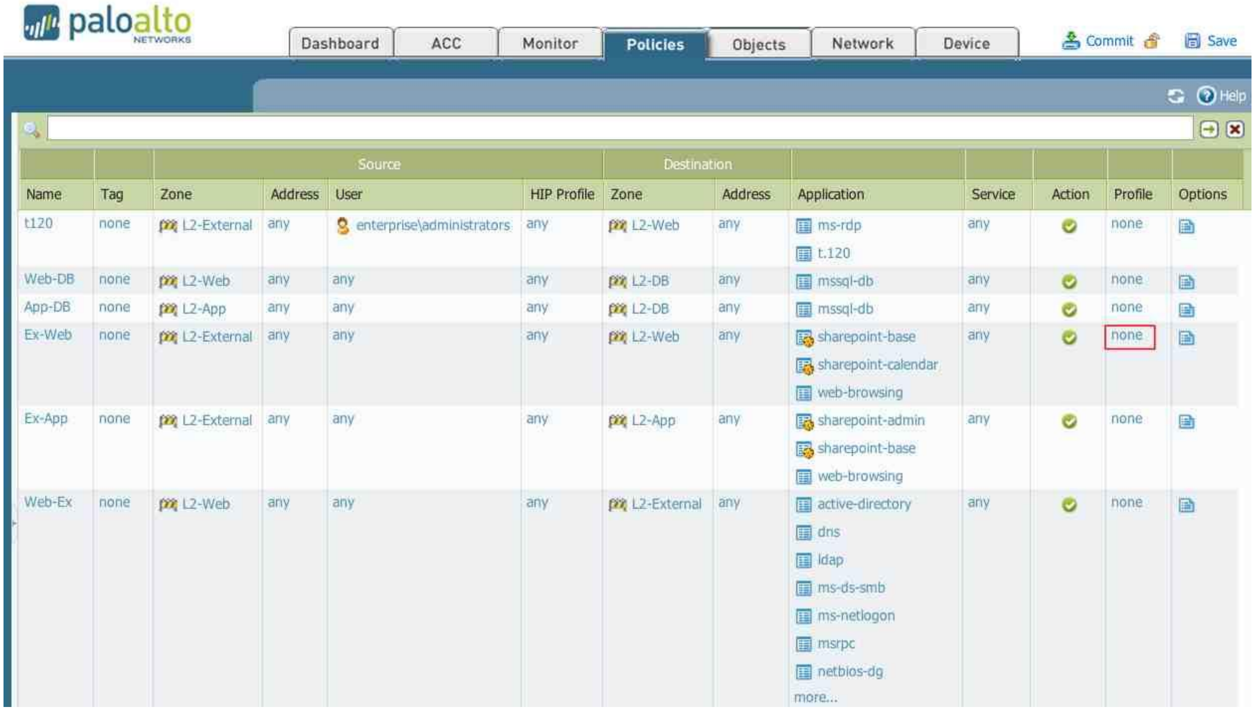
		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
t120	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	
Web-DB	none	L2-Web	any	any	any	L2-DB	any	mssql-db	any	✓	none	
App-DB	none	L2-App	any	any	any	L2-DB	any	mssql-db	any	✓	none	
Ex-Web	none	L2-External	any	any	any	L2-Web	any	sharepoint-base sharepoint-calendar web-browsing	any	✓	none	

8.4 Threat Prevention

In addition to validating the application used to access a security zone and the user initiating the request, the next-generation firewall can scan the network traffic for threats. These include viruses, malware, spyware, or files with confidential data. By creating a security profile that scans traffic into the data center, the firewall can prevent a user from unknowingly infecting data center servers with malware, or getting infected from a compromised server.

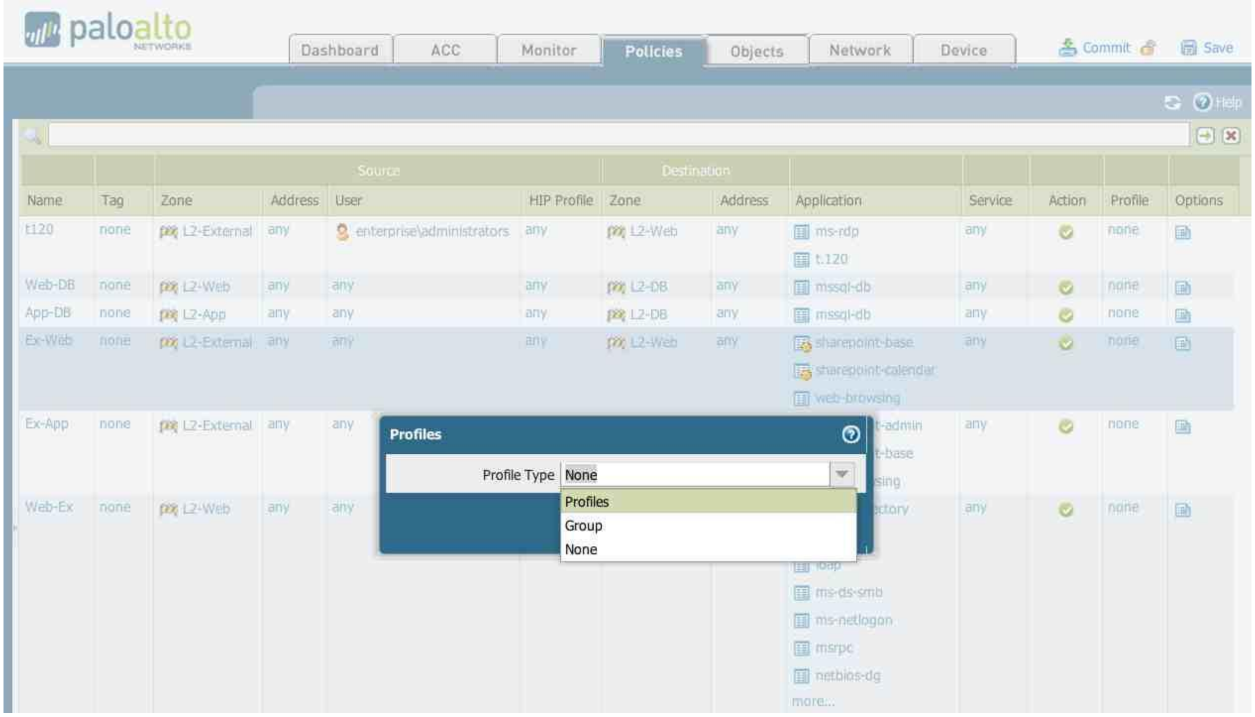
Each rule in the security policy can have its own security profile applied, allowing for the greatest flexibility in setting policy. For example, you may have a strict security profile blocking viruses, malware, and spyware on traffic that originates outside the data center and accesses the front-end servers, but not have any profile on traffic between the application and database servers.

To begin creating the security profile, locate the Profile column in the security policy page. If nothing has been configured there yet, it will indicate "none".



		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
t120	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	📄
Web-DB	none	L2-Web	any	any	any	L2-DB	any	mssql-db	any	✓	none	📄
App-DB	none	L2-App	any	any	any	L2-DB	any	mssql-db	any	✓	none	📄
Ex-Web	none	L2-External	any	any	any	L2-Web	any	sharepoint-base sharepoint-calendar web-browsing	any	✓	none	📄
Ex-App	none	L2-External	any	any	any	L2-App	any	sharepoint-admin sharepoint-base web-browsing	any	✓	none	📄
Web-Ex	none	L2-Web	any	any	any	L2-External	any	active-directory dns ldap ms-ds-smb ms-netlogon msrpc netbios-dg more...	any	✓	none	📄

Click the "none" and a dialog window will open. Choose "Profiles" from this window to configure the security profile.

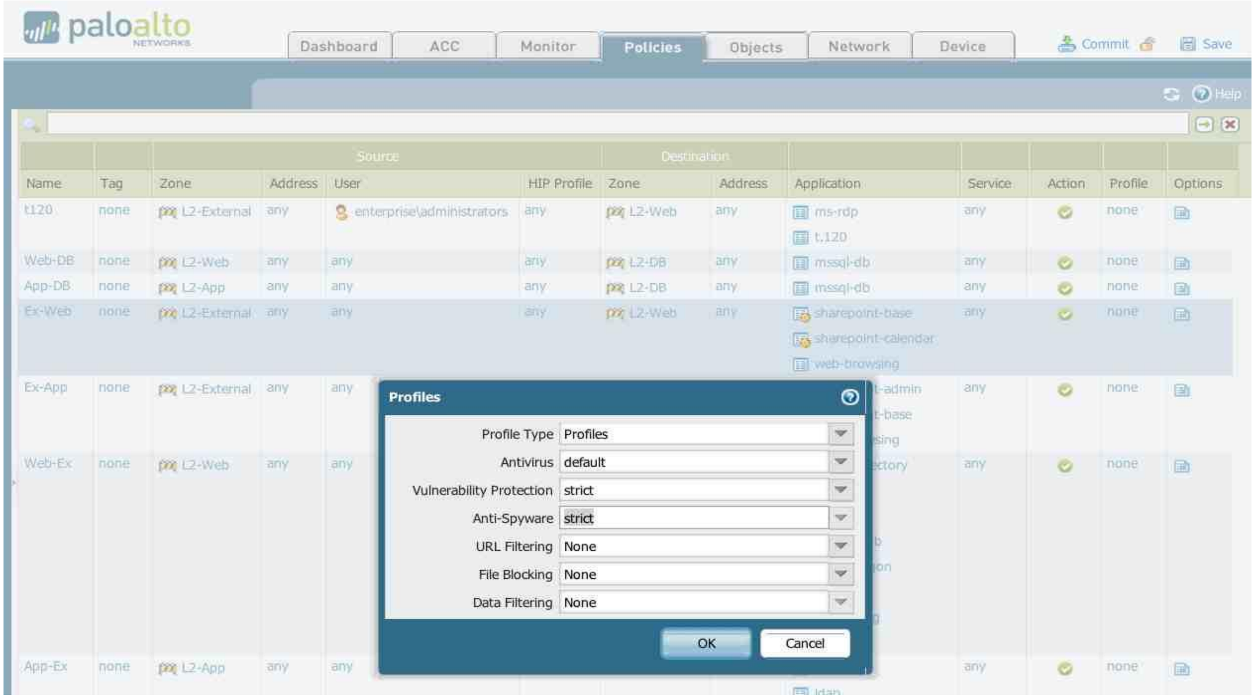


		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
t120	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	
Web-DB	none	L2-Web	any	any	any	L2-DB	any	mssql-db	any	✓	none	
App-DB	none	L2-App	any	any	any	L2-DB	any	mssql-db	any	✓	none	
Ex-Web	none	L2-External	any	any	any	L2-Web	any	sharepoint-base sharepoint-calendar web-browsing	any	✓	none	
Ex-App	none	L2-External	any	any				t-admin t-base sing	any	✓	none	
Web-Ex	none	L2-Web	any	any				ctory ldap ms-ds-smb ms-netlogon msrpc netbios-dg more...	any	✓	none	

Profiles

Profile Type: None

In the security profile window, select the specific profile settings for each of the different areas, Antivirus, Vulnerability Protection, etc. Some of these will have pre-configured profiles, such as “default” or “strict”. These pre-configured options can be chosen, or a customized profile can be created. Please see Palo Alto Networks Administration Guide for details on creating custom profiles.

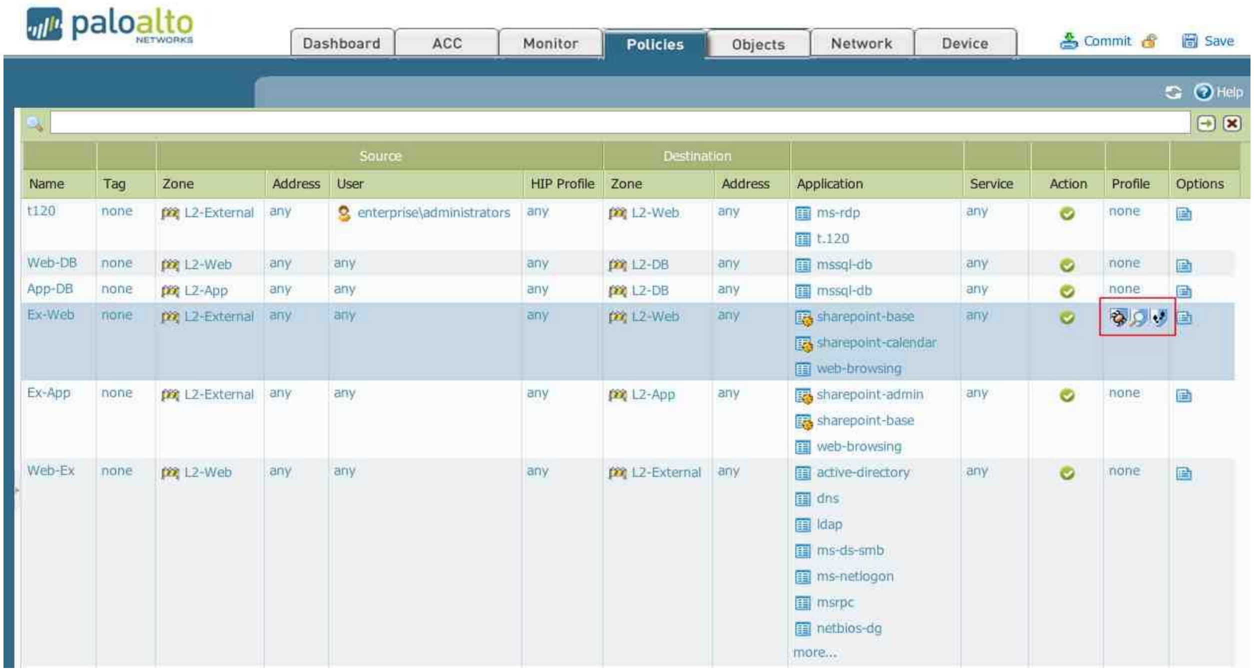


		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
t120	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	
Web-DB	none	L2-Web	any	any	any	L2-DB	any	mssql-db	any	✓	none	
App-DB	none	L2-App	any	any	any	L2-DB	any	mssql-db	any	✓	none	
Ex-Web	none	L2-External	any	any	any	L2-Web	any	sharepoint-base sharepoint-calendar web-browsing	any	✓	none	
Ex-App	none	L2-External	any	any				t-admin t-base sing	any	✓	none	
Web-Ex	none	L2-Web	any	any				ctory b on	any	✓	none	
App-Ex	none	L2-App	any	any				ldap	any	✓	none	

Profiles

Profile Type	Profiles
Antivirus	default
Vulnerability Protection	strict
Anti-Spyware	strict
URL Filtering	None
File Blocking	None
Data Filtering	None

Click OK, and the new security profile should now be part of the security policy rule. This will be displayed with icons for the specific areas that profiles were chosen for.



		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
t120	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	
Web-DB	none	L2-Web	any	any	any	L2-DB	any	mssql-db	any	✓	none	
App-DB	none	L2-App	any	any	any	L2-DB	any	mssql-db	any	✓	none	
Ex-Web	none	L2-External	any	any	any	L2-Web	any	sharepoint-base sharepoint-calendar web-browsing	any	✓		
Ex-App	none	L2-External	any	any	any	L2-App	any	sharepoint-admin sharepoint-base web-browsing	any	✓	none	
Web-Ex	none	L2-Web	any	any	any	L2-External	any	active-directory dns ldap ms-ds-smb ms-netlogon msrpc netbios-dg more...	any	✓	none	

Repeat this process for all of the rules to which a security profile should be applied.

9. References

AppExpert SharePoint Template Quick Start Guide. *AppExpert Quick Start Guide NetScaler 9.0 Consulting Solutions* by Citrix Systems, Inc. 2009
AppExpert Template Deployment Guide. *Microsoft Sharepoint Deployment Guide* by Citrix Systems, Inc. 2009
Deployment Guide for Citrix Application Template for SharePoint 2010. Citrix Systems, Inc. 2009
Microsoft SharePoint Deployment Guide. *Utilizing the Acceleration and Optimization Features of Citrix Netscaler.* Citrix Systems, Inc. 2007

About Palo Alto Networks

Palo Alto Networks™ is the network security company. Its innovative platform allows enterprises, service providers, and government entities to secure their networks and safely enable the increasingly complex and rapidly growing number of applications running on their networks. The core of Palo Alto Networks' platform is its Next-Generation Firewall, which delivers application, user, and content visibility and control integrated within the firewall through its proprietary hardware and software architecture. Palo Alto Networks' products and services can address a broad range of network security requirements, from the data center to the network perimeter, as well as the distributed enterprise, which includes branch offices and a growing number of mobile devices. Palo Alto Networks' products are used by more than 9,000 customers in over 100 countries. For more information, visit www.paloaltonetworks.com.

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.