Deployment Guide for Microsoft Exchange 2010

Securing and Accelerating Microsoft Exchange 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 Exchange 2010

Citrix® NetScaler® and Palo Alto Networks take a best-in-class approach to optimizing and securing applications. This approach ensures the best total cost of ownership (TCO), security, availability, and performance for enterprise applications. The combined solution is a comprehensive network system that takes the best of high-speed load balancing, content switching, state-of-the-art application acceleration, layer 4-7 traffic management, data compression, dynamic content caching, SSL acceleration, network optimization, deep packet inspection, and next-generation network security to provide a robust, tightly integrated solution. Deployed in front of application servers, the NetScaler and Palo Alto Networks firewalls significantly reduce processing overhead on application and database servers and improves security

The purpose of this guide is to help organizations deploy NetScaler and Palo Alto Networks next-generation firewalls for securing and load balancing Microsoft® Exchange 2010 Client Access servers. Inside this guide you will find a concise set of step-by-step deployment instructions required to configure both devices to accelerate and safely enable a Microsoft Exchange 2010 OWA application.

Within the Exchange 2010 server architecture, a NetScaler and next generation firewall is located in front of the Client Access Servers (CAS) with one single Virtual IP (VIP) address. The next-generation firewall secures the CAS systems and the NetScaler provides load balancing and traffic optimization. Exchange client traffic is bound to a Client Access Server through NetScaler. Each CAS system within the server pool handles the server applications, security, authentication, and connection and protocol processing. The Mailbox server at the back end handles the mailbox data, such as mail and contacts.

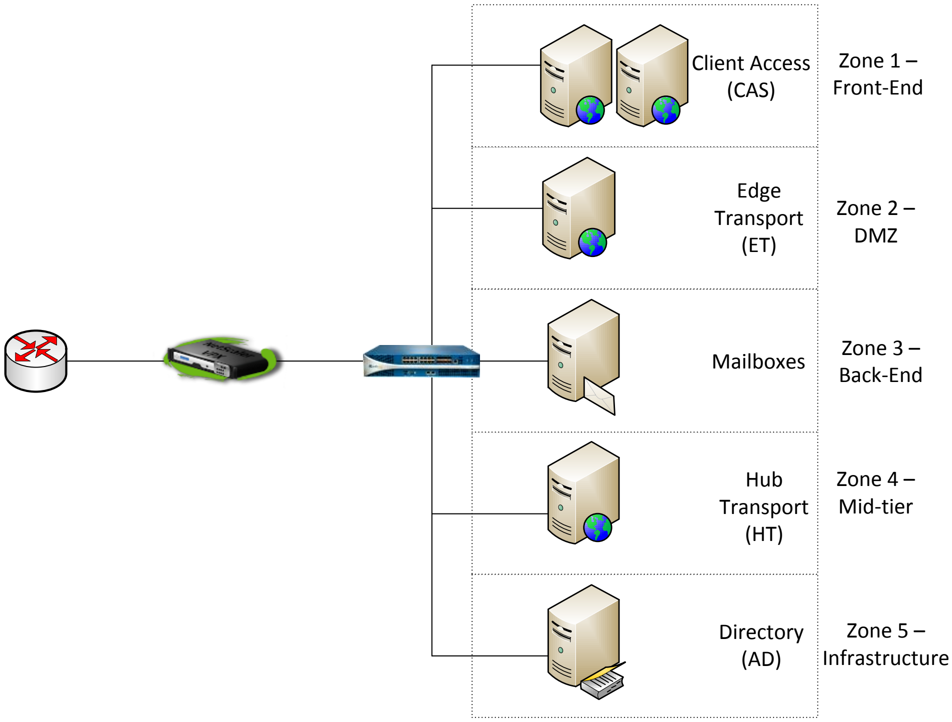
For readers less familiar with the architecture of Exchange 2010, Microsoft provides a useful overview at http://technet.microsoft.com/en-us/video/microsoft-exchange-server-2010-architecture.aspx.

2. Requirements

Required Component	Used in this Document	Note
Citrix NetScaler	NS 10.0 VPX Build 69.4.nc with Platinum License	
Palo Alto Networks Next-Generation Firewall	PAN-OS 4.1	
Microsoft Exchange 2010 Servers	6 Physical/VM servers	2x CAS (Web); 1x Edge Transport; 1x Mailboxes; 1x Hub Transport; 1x AD
AppExpert Microsoft Outlook Web Access Template	Template File	http://community.citrix.com/download/attachments/49186776/OWA.xml
	Deployment File	http://community.citrix.com/download/attachments/49186776/OWA_deployment.xml

3. Microsoft Exchange Server Network Topology

3.1 Environment diagram



3.2 IP allocations

Functional Device	IP:Port	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
Exchange OWA (VIP) – Web	10.5.172.165:443	255.255.255.0
Exchange OA (VIP) – Outlook	10.5.172.165:443	255.255.255.0
Exchange AS (VIP) – Mobile	10.5.172.165:443	255.255.255.0
Exchange IMAP4 – IMAP Client	10.5.172.165:993	255.255.255.0
Exchange POP3 – POP Client	10.5.172.165:995	255.255.255.0
Exchange SMAP Relay	10.5.172.166:25	255.255.255.0
Exchange CAS Server 1	10.5.172.160	255.255.255.0
Exchange CAS Server 2	10.5.172.161	255.255.255.0
Exchange ET Server	10.5.172.162	255.255.255.0
Exchange Mailbox Server	10.5.172.163	255.255.255.0
Exchange HT Server	10.5.172.164	255.255.255.0
Active Directory Server	10.5.172.155	255.255.255.0

4. Microsoft Exchange Installation and Configurations

The configuration of Citrix NetScaler for Microsoft Exchange 2010 is made up of 5 key steps:

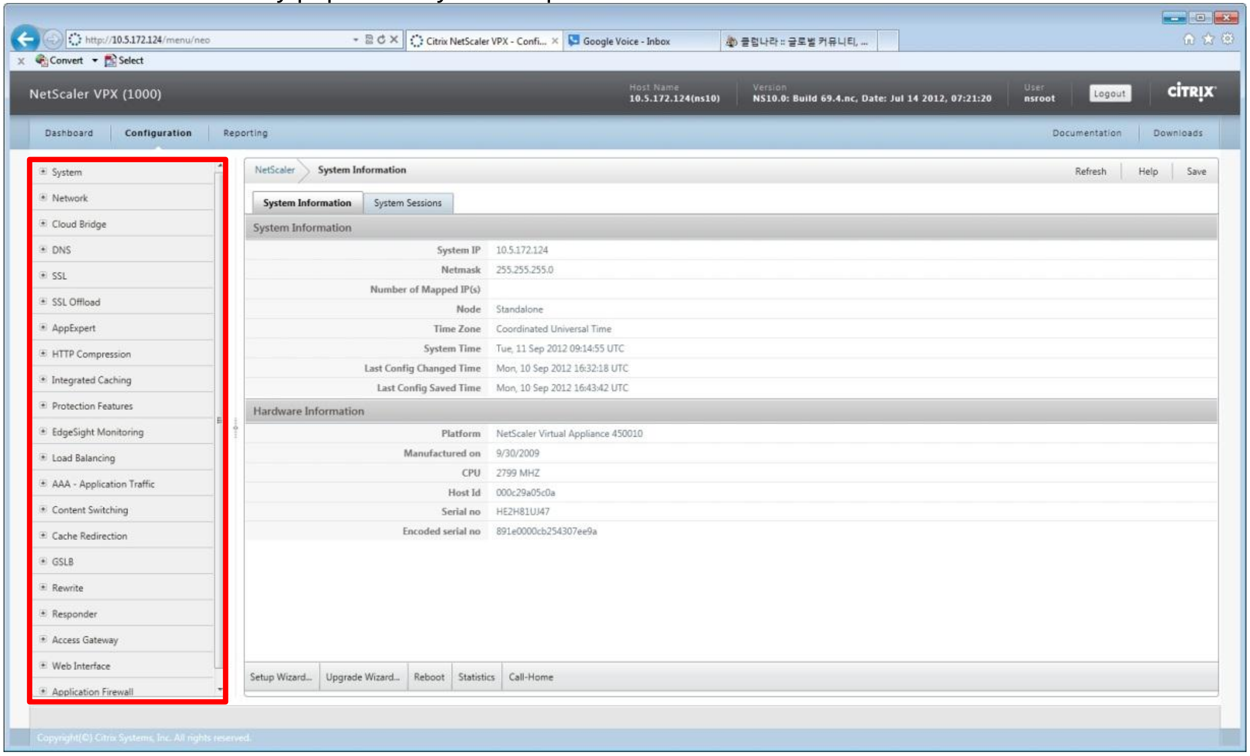
1. Setup the underlying network
2. License the system
3. Configure the policies for Microsoft Exchange 2010
4. Setup SSL
5. Setup which servers will receive traffic from the NetScaler

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 Exchange. Everything from traffic switching to optimization is affected in this step. With Citrix NetScaler, we are able to leverage the AppExpert AppTemplate for Microsoft Exchange 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. Since the AppExpert Template for Exchange 2010 only supports Microsoft Outlook Web Access (OWA), there will be separate steps to manually configure the rest of Exchange services such as Outlook Anywhere (OA, i.e., Outlook client), ActiveSync (AS, i.e., mobile client), IMAP4, POP3 and external SMTP relay services. The following steps guide 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 the 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

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

Service	NetScaler Menu	NetScaler Sub-Menu	Action	Comment
All	System	Licenses	Manage Licenses	Custom added*
		Settings	Configure basic features	Custom added*
All	Network	IPs	NetScaler IP, Subnet IP	Custom added*
			Virtual IP	Auto added **
All	SSL	Certificate	Root-CA, Server	Custom added*
All	SSL Offload	Servers	Per VM/Physical Server	Auto added
		Service Group	Per Port	Auto added
		Virtual Servers	VIP per Port	Auto added
OWA	AppExpert	Applications	Import	Custom added*
			Configure Public	Custom

			Endpoints	added*
			Configure Backend Services	Custom added*
OWA	Load Balancing	Servers	Per VM/Physical Server	Auto added
		Service Groups	Per Port	Auto added
IMAP4	Load Balancing	Service Groups	Per Port	Custom added*
		Virtual Servers	VIP per Port	Custom added*
		Servers	Per VM/Physical Server	Auto added
POP3	Load Balancing	Service Groups	Per Port	Custom added*
		Virtual Servers	VIP per Port	Custom added*
		Servers	Per VM/Physical Server	Auto added
SMTP	Load Balancing	Service Groups	Per Port	Custom added*
		Virtual Servers	VIP per Port	Custom added*
		Servers	Per VM/Physical Server	Auto added
OWA	Content Switching	Virtual Servers	Per VM/Physical Server	Auto added
OA/AS	AppExpert	Applications	Service confirmation	Auto added***

** Please refer below 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)*

**** Auto added – The Exchange environment in this deployment doc shares the same CAS servers for OA/AS services with OWA, and sharing same port numbers. Therefore, no additional service configuration is required.*

4.2 Step –by-Step Installation

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

Step	Action	Detail	Custom Data
1	NetScaler IP, Subnet IP	NetScaler initial Configuration (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	Template Import	Template, Deployment files (XML format)
5	Root-CA, Server	Security Certificate Installation	
6	Configure Public Endpoints	Creating virtual servers (IP) to talk to multiple backend servers	OWA Virtual IP (VIP)
7	Configure Backend Services	Creating a Service Group	IPs for Web Server 1 and Web Server 2
8	Per Port, VIP/Port	IMAP4 Service Installation	IMAP4 port

9	Per Port, VIP/Port	POP3 Service Installation	POP3 port
10	Per Port, VIP/Port	SMTP Service Installation	SMTP VIP and Port
11	Service confirmation	OA/AS service confirmation	OWA data

5. Deployment Instructions

This section will describe details of the NetScaler VPX installation and initial configuration, Exchange AppExpert template download, and full SharePoint service configuration within NetScaler.
Administrators can use the NetScaler command-line to set up the initial NSIP, Mapped IP (MIP), and Subnet IP (SNIP). Administrators 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.

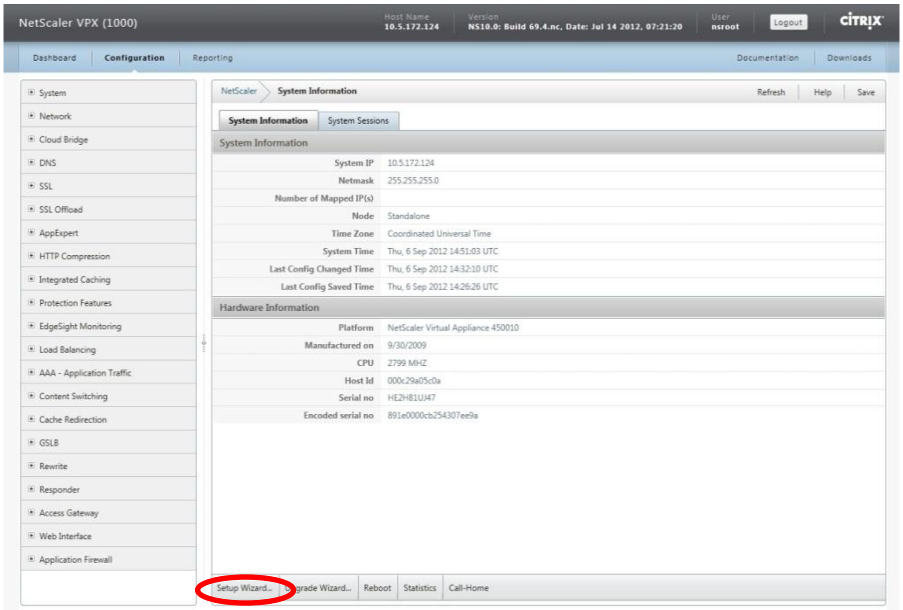
5.1.1 Add NSIP, Subnet Mask, and Default Gateway on NetScaler:

At the Console prompt from XenCenter or vSphere 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 the Microsoft Exchange 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**:



Host Name 10.5.172.124

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

User nsroot

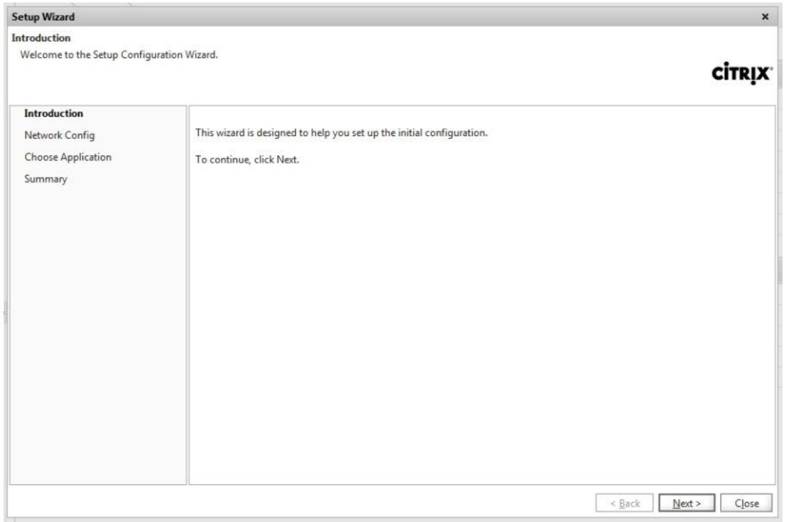
System Information

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	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

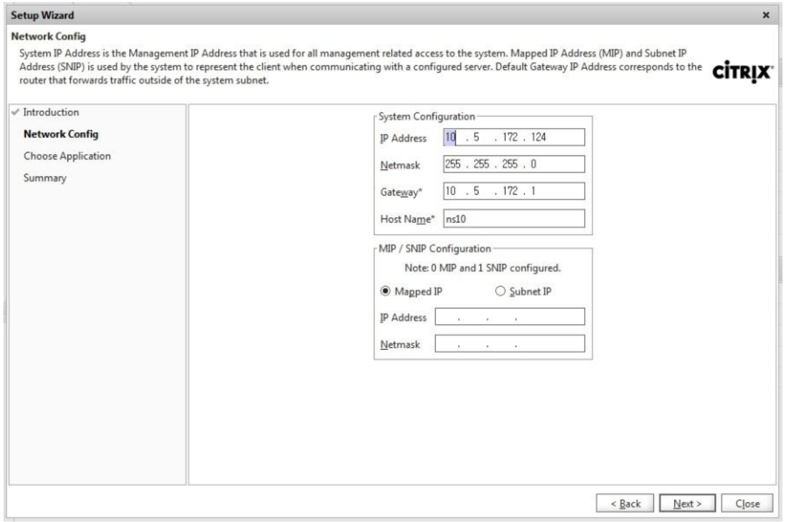


Welcome to the Setup Configuration Wizard.

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

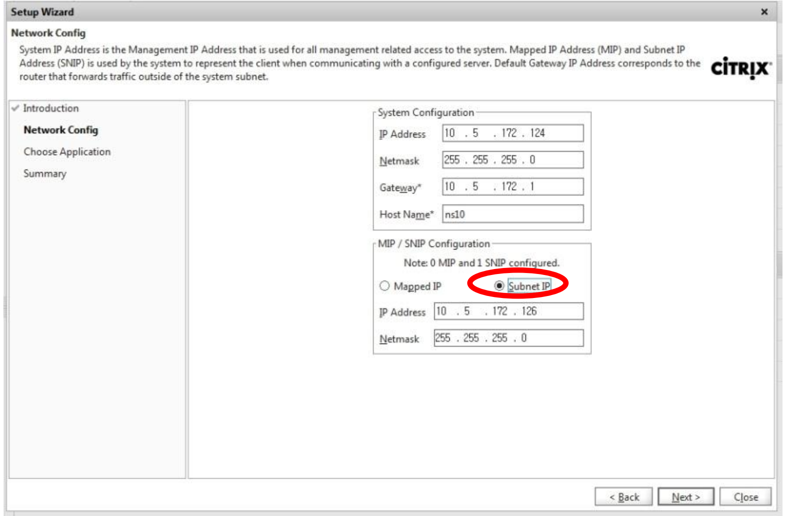
MIP / SNIP Configuration

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

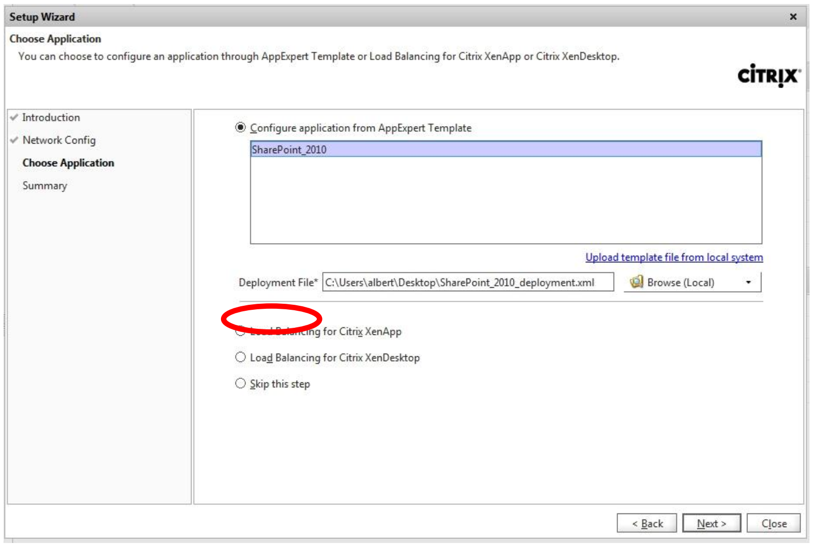
MIP / SNIP Configuration

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.

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

● Configure application from AppExpert Template

SharePoint_2010

Upload template file from local system

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

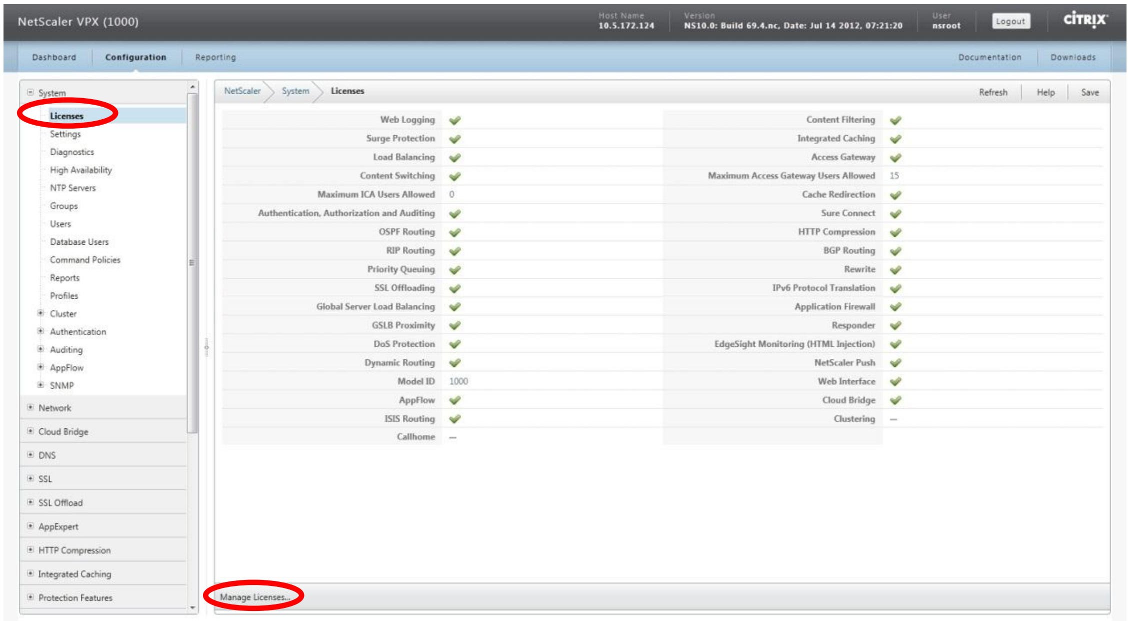
○ Load Balancing for Citrix XenApp

○ Load Balancing for Citrix XenDesktop

○ Skip this step

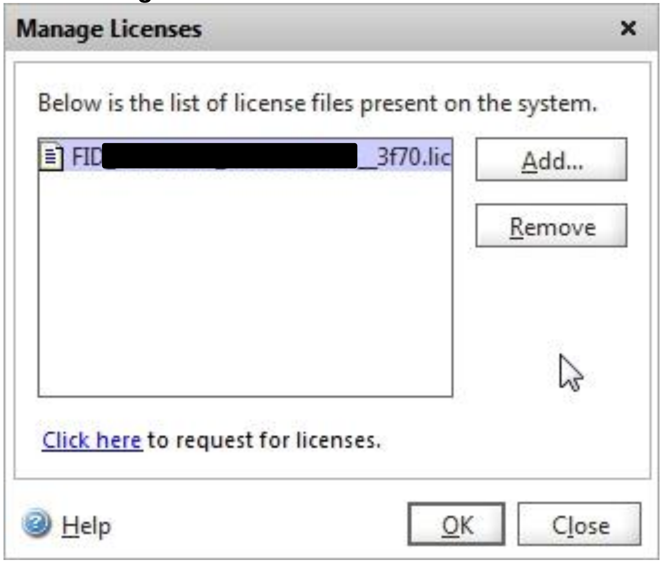
5.2 NetScaler License installation

Proper licenses are required in order to enable necessary services for the Exchange configuration. Refer to the "*Citrix NetScaler VPX Licensing Guide"* at http://support.citrix.com/article/CTX122426.



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.



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

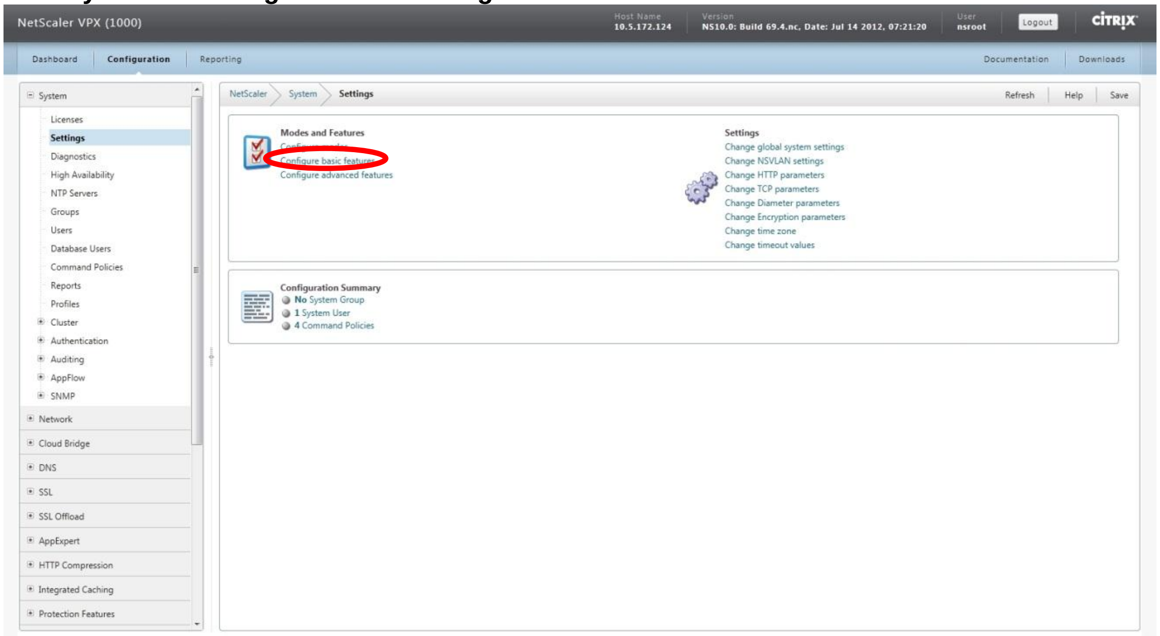
FID[redacted]_3f70.lic

Click here to request for licenses.

5.3 NetScaler Basic Feature Setting

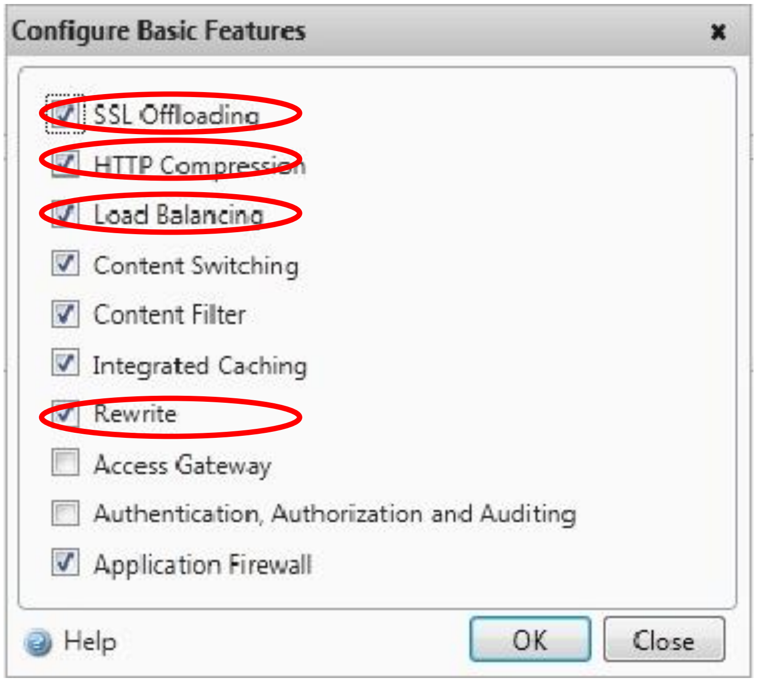
5.3.1 Systems Settings

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



5.3.2 Basic Features

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



Configure Basic Features

☑ SSL Offloading

☑ HTTP Compression

☑ Load Balancing

☑ Content Switching

☑ Content Filter

☑ Integrated Caching

☑ Rewrite

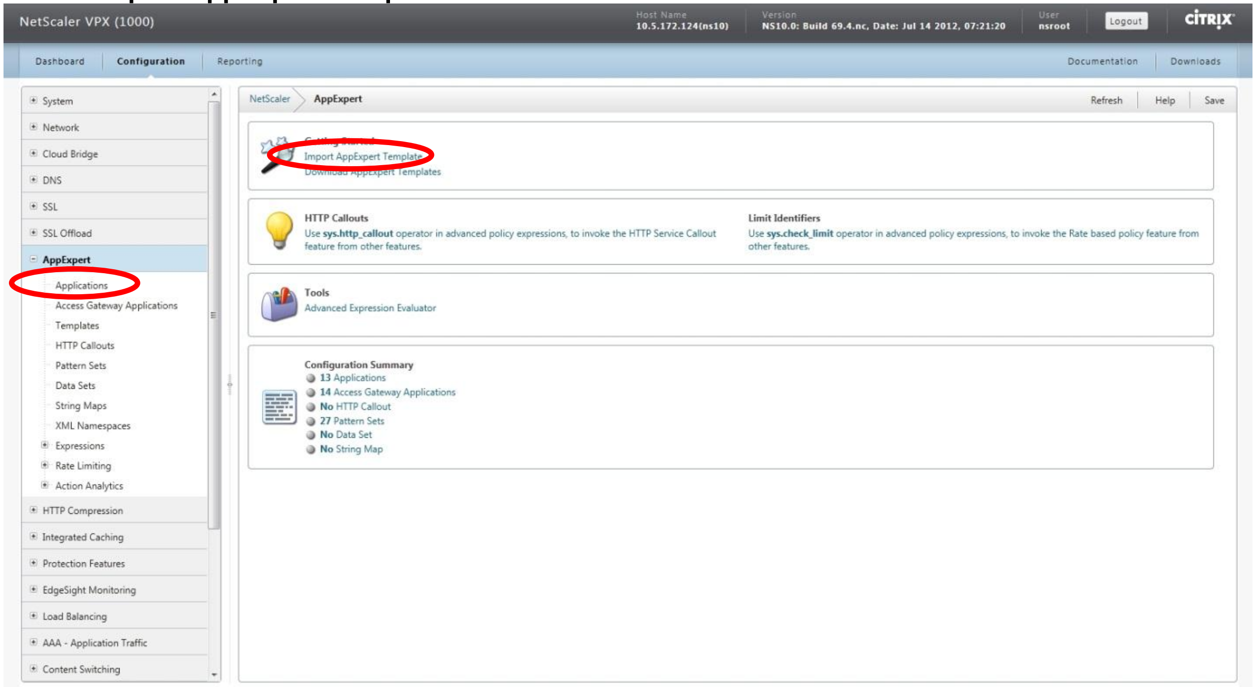
□ Access Gateway

□ Authentication, Authorization and Auditing

☑ Application Firewall

5.4 NetScaler AppExpert Outlook Web Access Template Install

AppExpert Outlook Web Access 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

Getting Started
Import AppExpert Template
Download AppExpert Templates

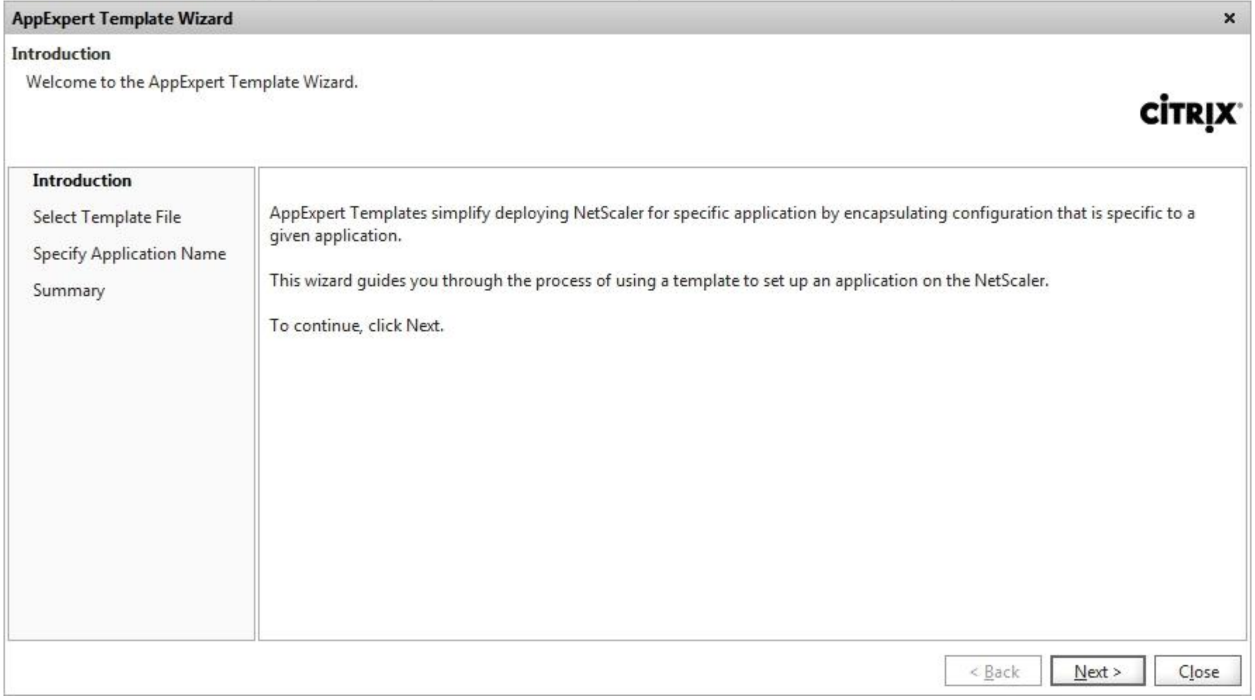
HTTP Callouts
Use **sys.http_callout** operator in advanced policy expressions, to invoke the HTTP Service Callout feature from other features.

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

Tools
Advanced Expression Evaluator

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 Template Wizard** to upload the downloaded templates.



AppExpert Template Wizard

Introduction

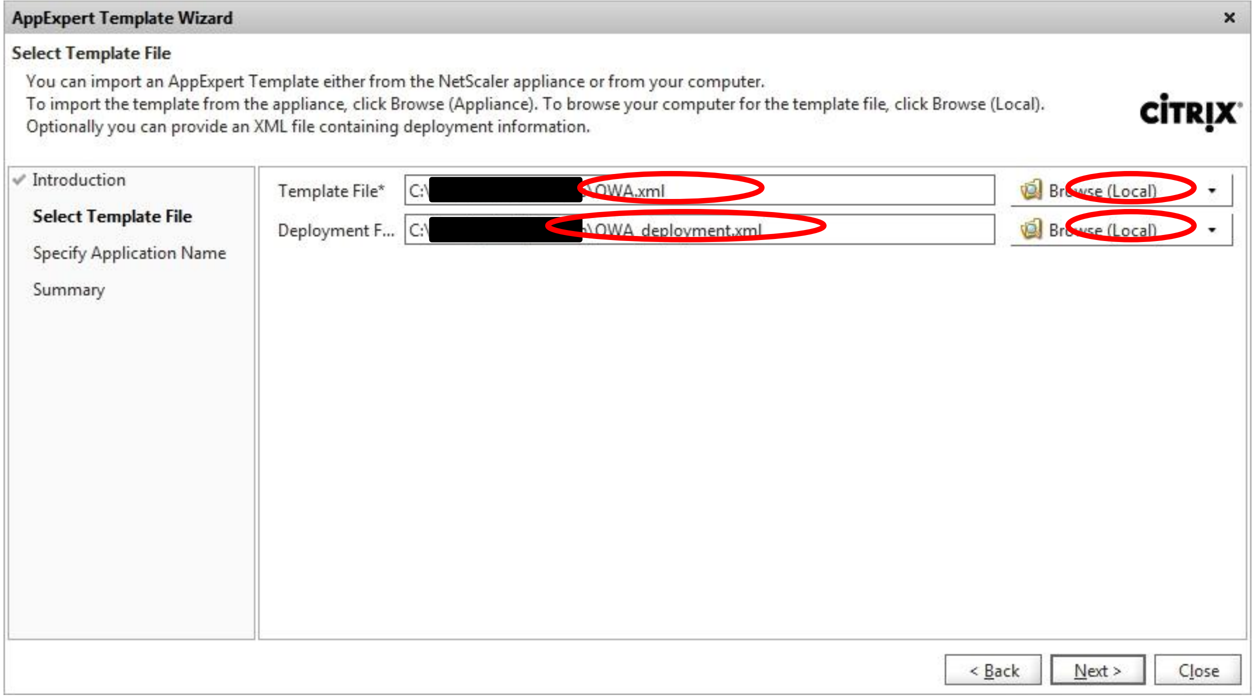
Welcome to the AppExpert Template Wizard.

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 Exchange. Then, click **Next**.



AppExpert Template Wizard

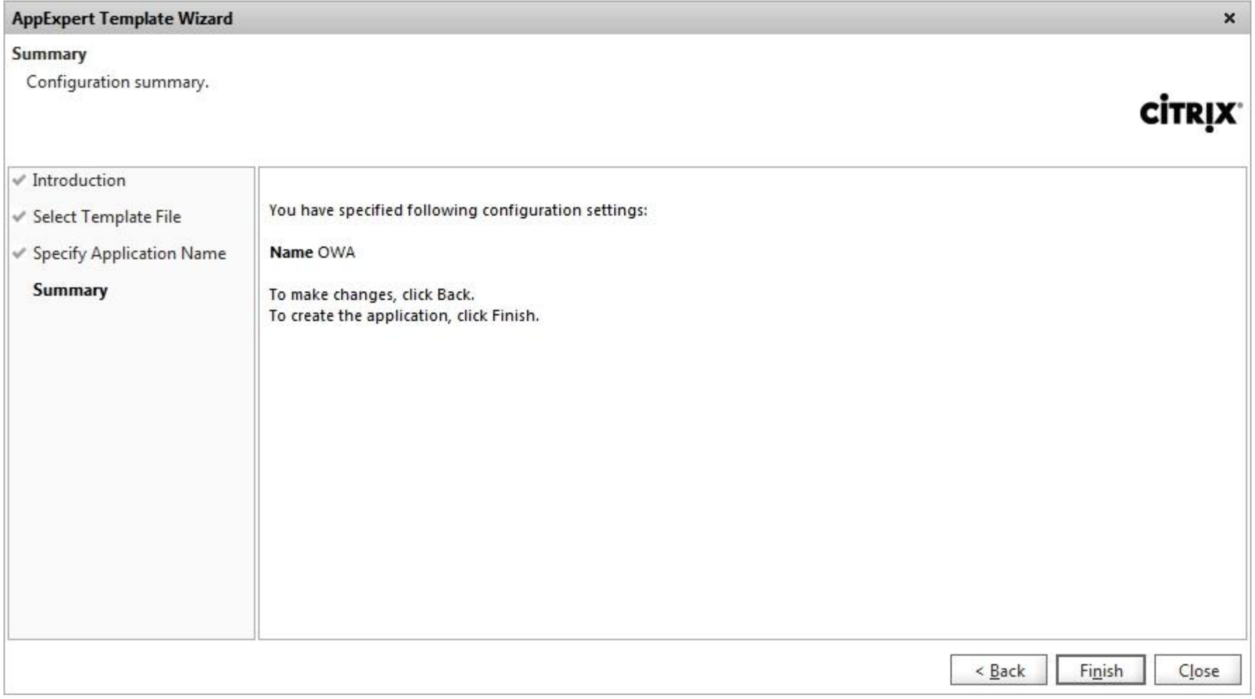
Select Template File

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]\OWA.xml Browse (Local)

Deployment F... C:\[redacted]\OWA_deployment.xml Browse (Local)

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



AppExpert Template Wizard

Summary

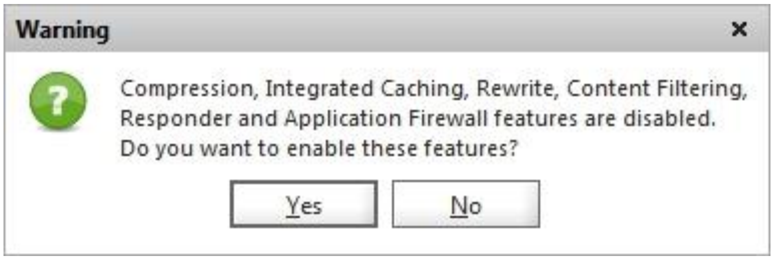
Configuration summary.

You have specified following configuration settings:

Name OWA

To make changes, click Back.
To create the application, click Finish.

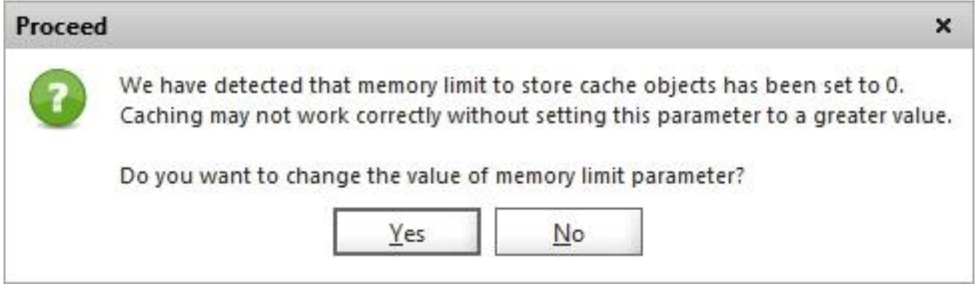
If any of required services for OWA were not enabled, the following **Warning** will guide through to enable those features. Click **Yes**.



Warning

Compression, Integrated Caching, Rewrite, Content Filtering, Responder and Application Firewall features are disabled. Do you want to enable these features?

By default, the memory usage limit was set to 0. **Proceed** message will prompt to change the value of memory limit parameter. Click **Yes.**

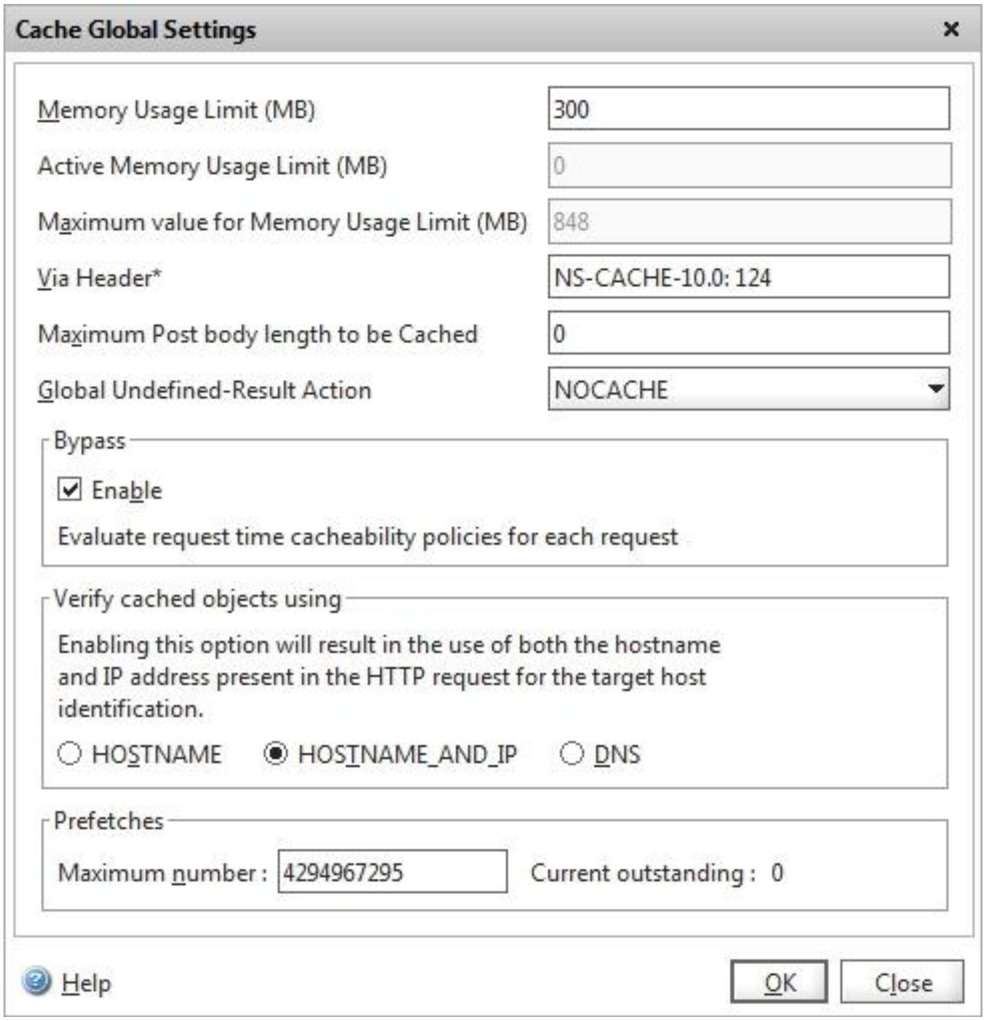


Proceed

We have detected that memory limit to store cache objects has been set to 0. Caching may not work correctly without setting this parameter to a greater value.

Do you want to change the value of memory limit parameter?

Set **Memory Usage Limit (MB)** to **300**. Then click **OK**.



Cache Global Settings

Memory Usage Limit (MB): 300

Active Memory Usage Limit (MB): 0

Maximum value for Memory Usage Limit (MB): 848

Via Header*: NS-CACHE-10.0: 124

Maximum Post body length to be Cached: 0

Global Undefined-Result Action: NOCACHE

Bypass

☑ Enable

Evaluate request time cacheability policies for each request

Verify cached objects using

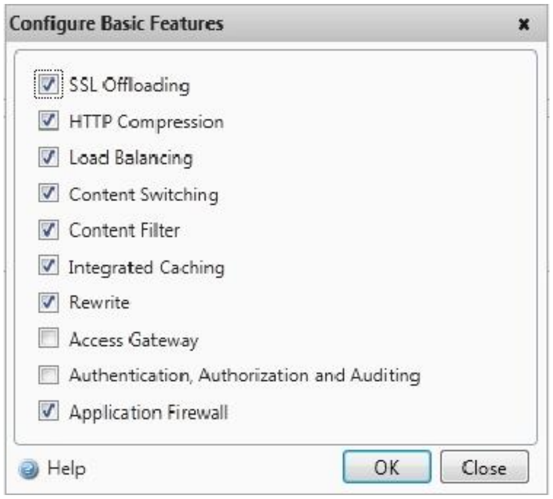
Enabling this option will result in the use of both the hostname and IP address present in the HTTP request for the target host identification.

○ HOSTNAME ● HOSTNAME_AND_IP ○ DNS

Prefetches

Maximum number : 4294967295 Current outstanding : 0

Confirm enabled **Basic Features**. Click **OK**.



Configure Basic Features

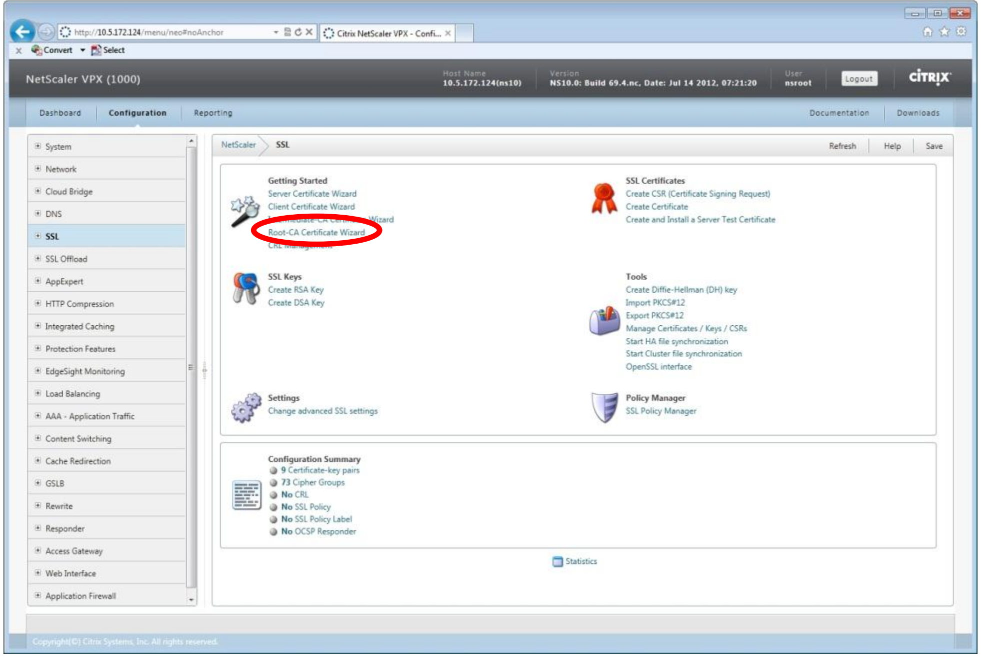
☑ SSL Offloading
☑ HTTP Compression
☑ Load Balancing
☑ Content Switching
☑ Content Filter
☑ Integrated Caching
☑ Rewrite
□ Access Gateway
□ Authentication, Authorization and Auditing
☑ Application Firewall

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

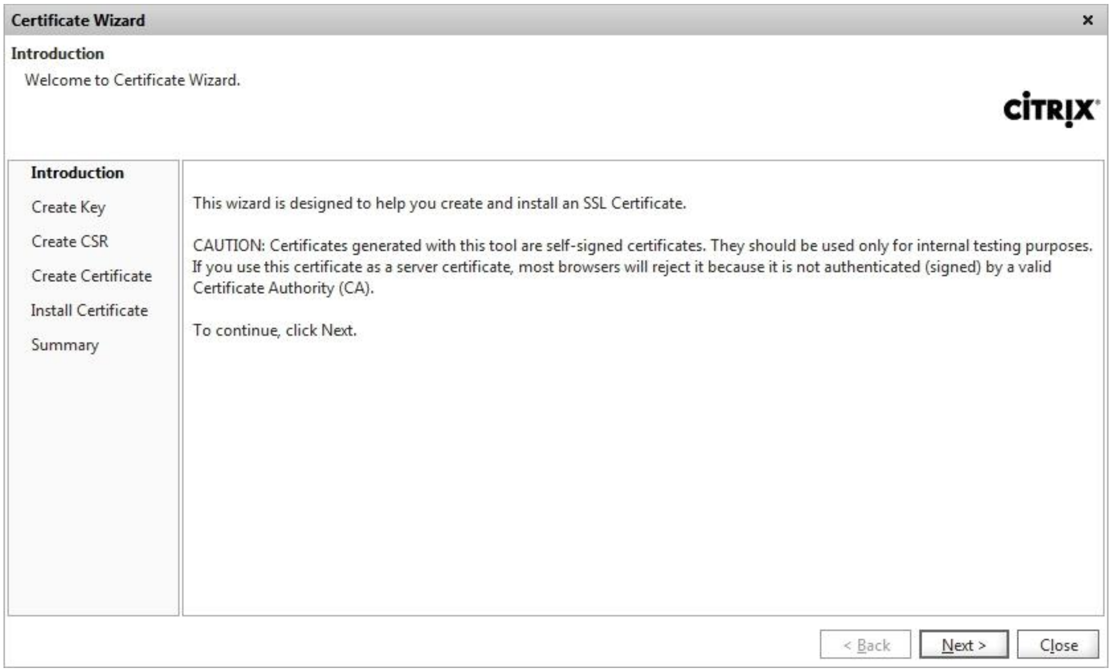
If production certificates are available, these can be imported through the processes within the NetScaler management interface. Consult Chapter 11 , "*Securing Load Balanced Traffic by Using SSL*" of the NetScaler product documentation entitled "*NetScaler VPX Getting Started Guide*" for details pertaining 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.

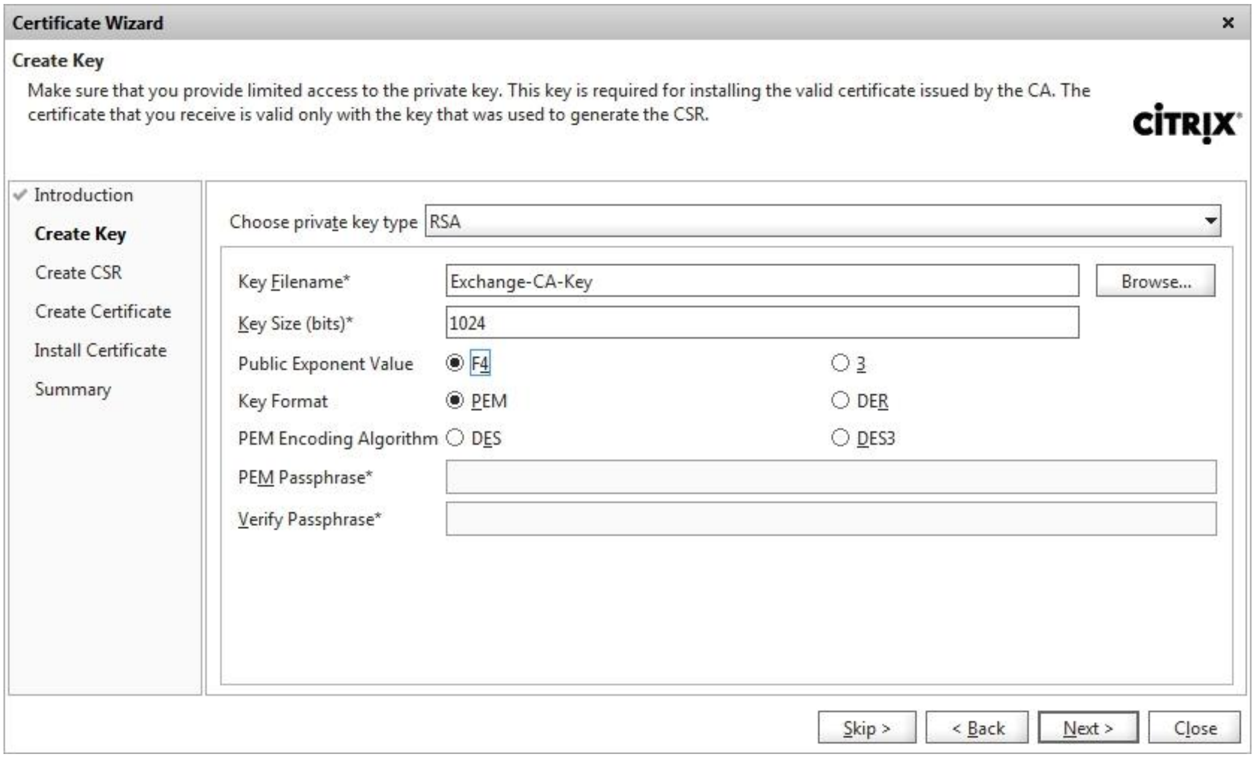
- **Introduction**
- Create Key
- Create CSR
- Create Certificate
- Install Certificate
- Summary

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 **Exchange-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*: Exchange-CA-Key

Key Size (bits)*: 1024

Public Exponent Value: ● F4 ○ 3

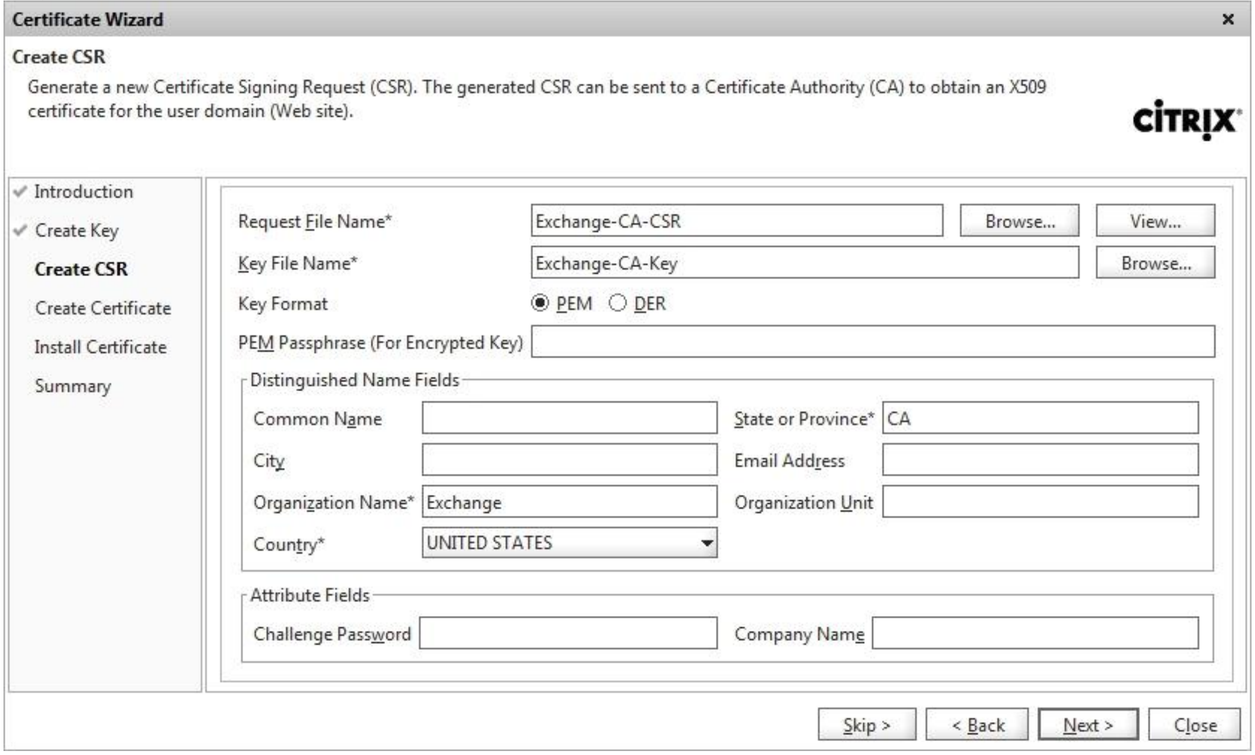
Key Format: ● PEM ○ DER

PEM Encoding Algorithm: ○ DES ○ DES3

PEM Passphrase*:

Verify Passphrase*:

Set the **Request File Name** to **Exchange-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).

Request File Name*: Exchange-CA-CSR

Key File Name*: Exchange-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*: Exchange

Organization Unit:

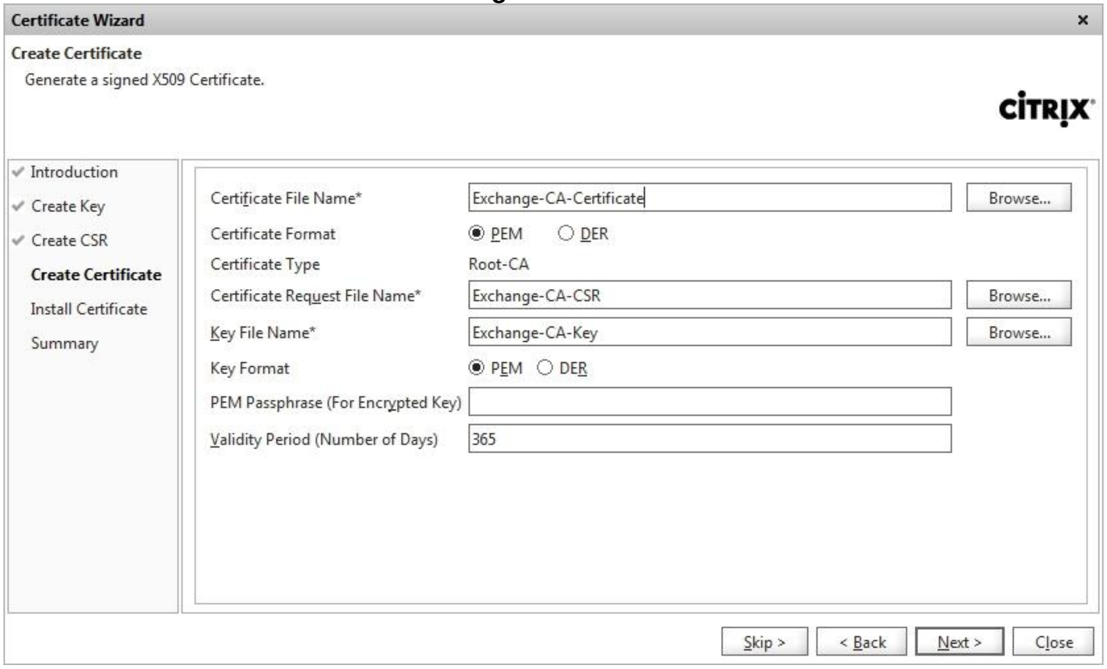
Country*: UNITED STATES

Attribute Fields

Challenge Password:

Company Name:

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



Certificate Wizard

Create Certificate

Generate a signed X509 Certificate.

Certificate File Name*: Exchange-CA-Certificate

Certificate Format: ● PEM ○ DER

Certificate Type: Root-CA

Certificate Request File Name*: Exchange-CA-CSR

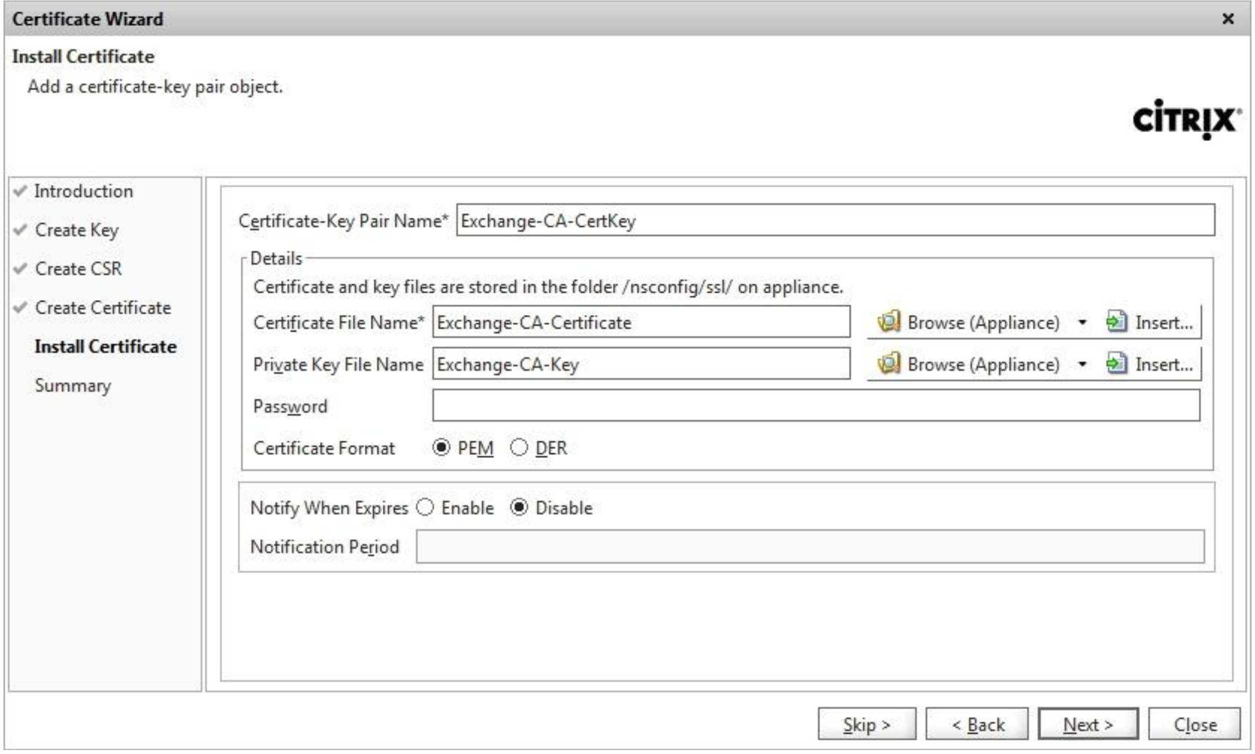
Key File Name*: Exchange-CA-Key

Key Format: ● PEM ○ DER

PEM Passphrase (For Encrypted Key):

Validity Period (Number of Days): 365

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



Certificate Wizard

Install Certificate

Add a certificate-key pair object.

Certificate-Key Pair Name* Exchange-CA-CertKey

Details

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

Certificate File Name* Exchange-CA-Certificate

Private Key File Name Exchange-CA-Key

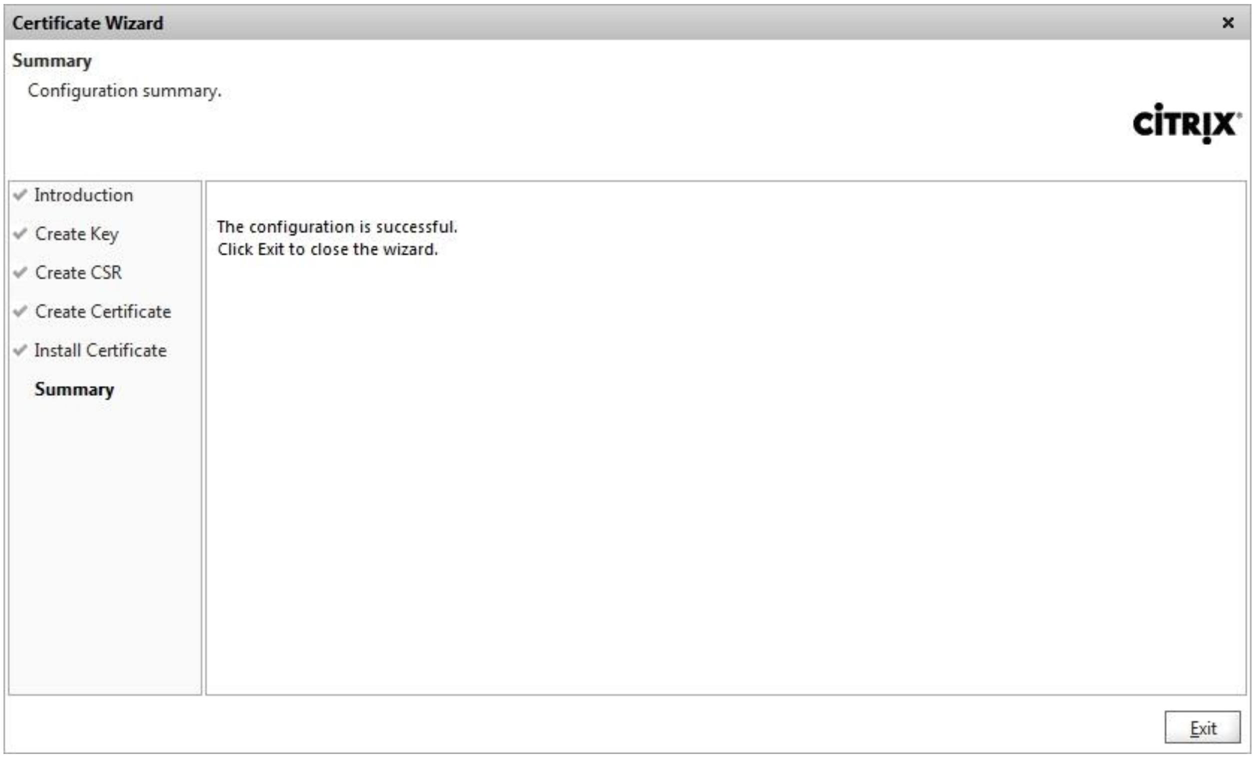
Password

Certificate Format ● PEM ○ DER

Notify When Expires ○ Enable ● Disable

Notification Period

Click **Finish** then **Exit**.



Certificate Wizard

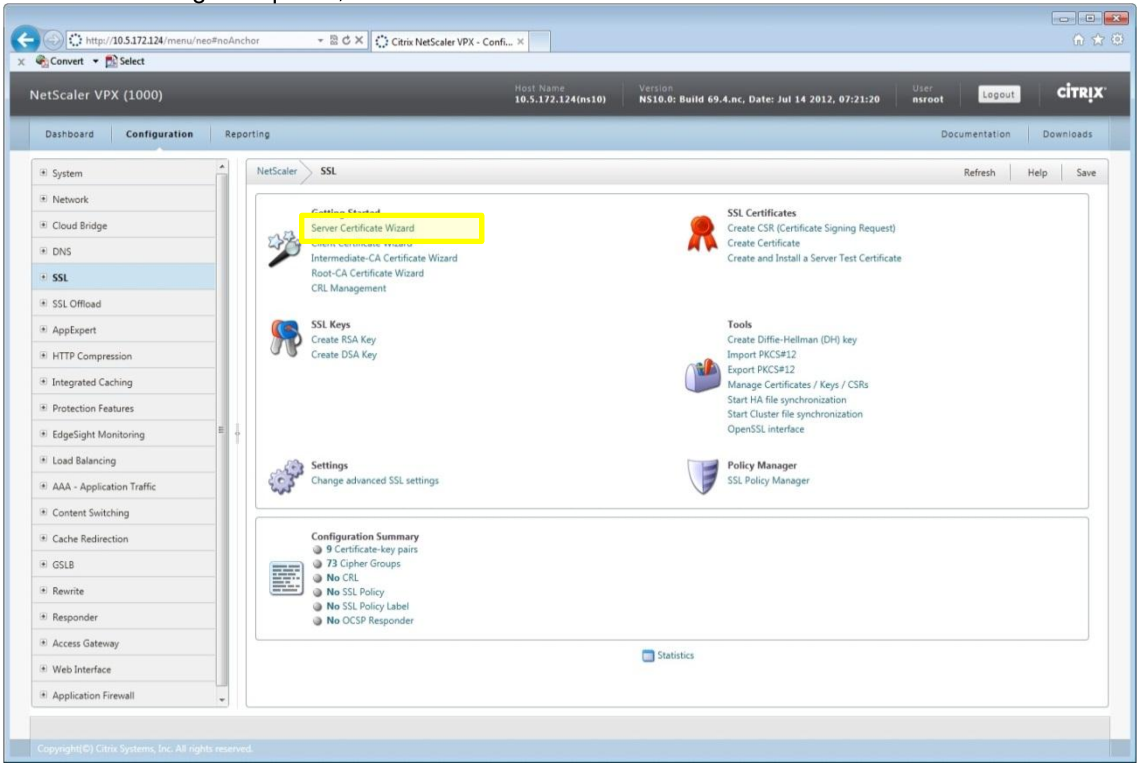
Summary

Configuration summary.

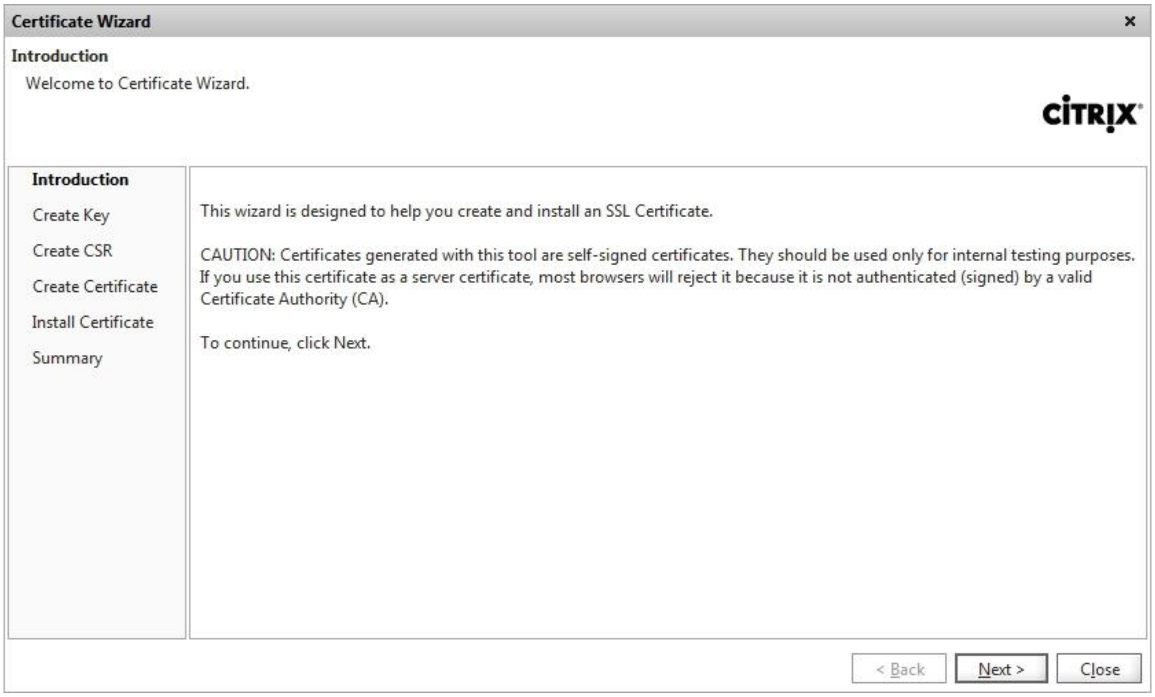
The configuration is successful.
Click Exit to close the wizard.

5.5.2 Server Certificate

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



Click **Next**.


Certificate Wizard

Introduction

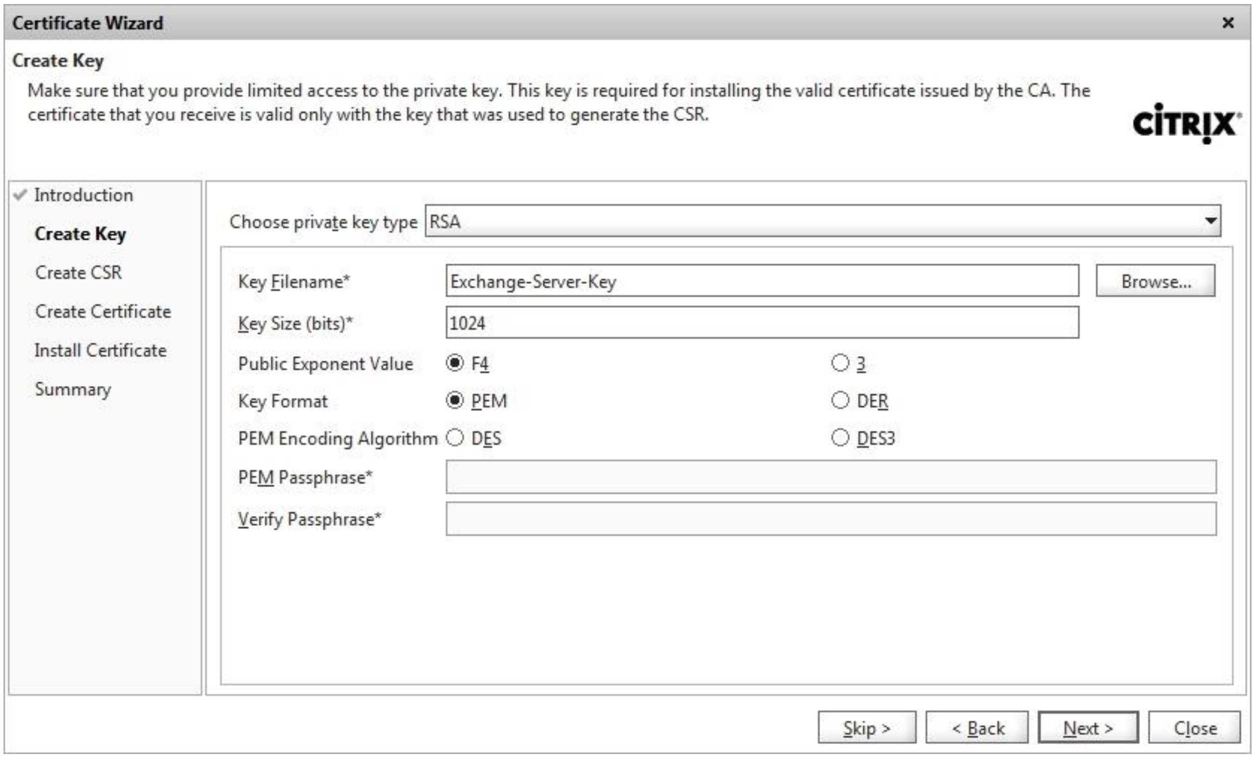
Welcome to Certificate Wizard.

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 **Exchange-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*: Exchange-Server-Key

Key Size (bits)*: 1024

Public Exponent Value: ● F4 ○ 3

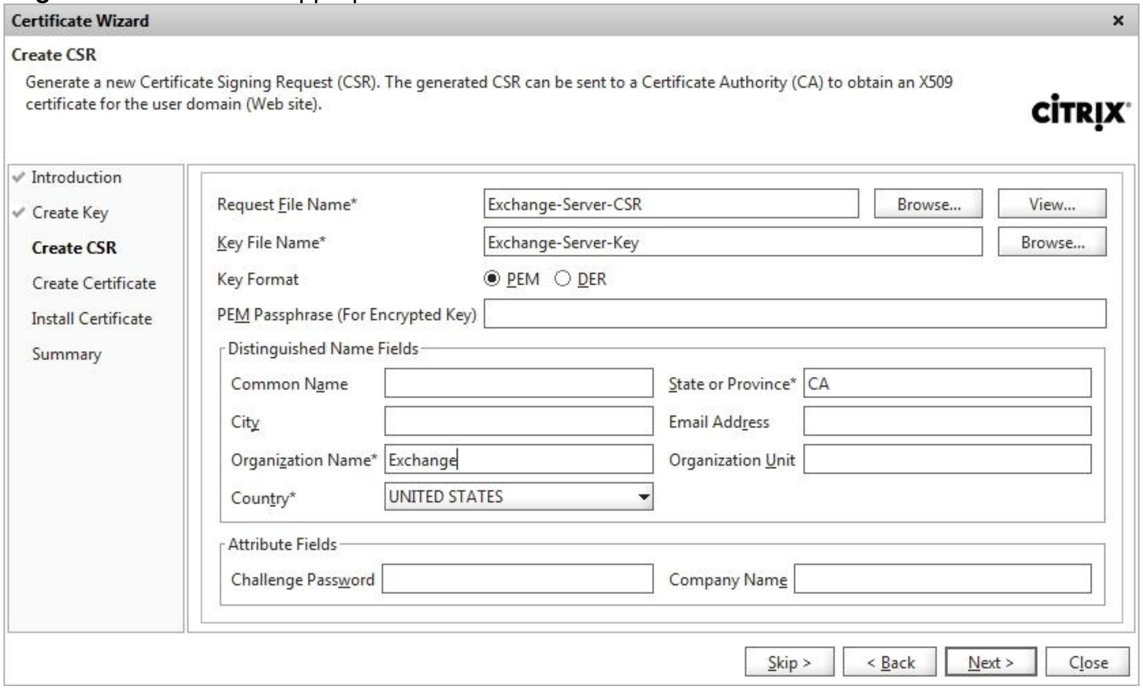
Key Format: ● PEM ○ DER

PEM Encoding Algorithm: ○ DES ○ DES3

PEM Passphrase*:

Verify Passphrase*:

Set the **Request File Name** to **Exchange-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*: Exchange-Server-CSR

Key File Name*: Exchange-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*: Exchange

Organization Unit:

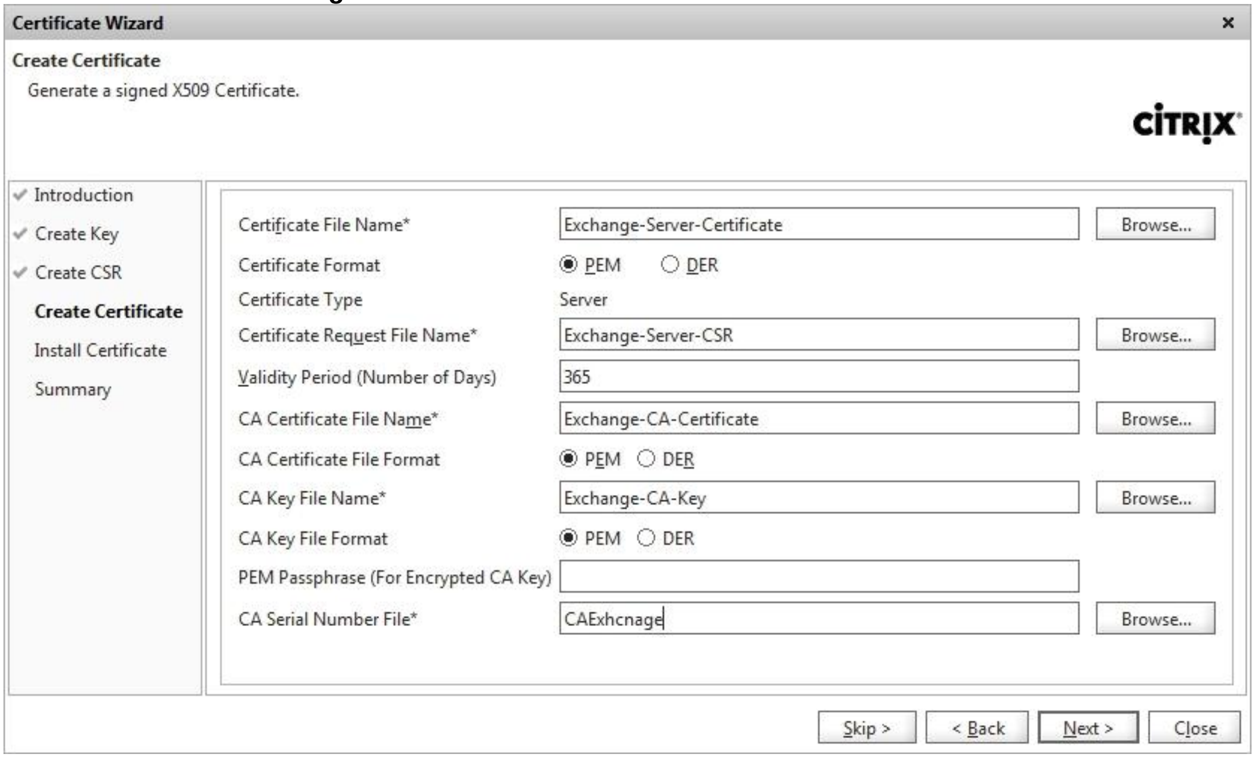
Country*: UNITED STATES

Attribute Fields

Challenge Password:

Company Name:

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



Certificate Wizard

Create Certificate

Generate a signed X509 Certificate.

Certificate File Name*: Exchange-Server-Certificate

Certificate Format: ● PEM ○ DER

Certificate Type: Server

Certificate Request File Name*: Exchange-Server-CSR

Validity Period (Number of Days): 365

CA Certificate File Name*: Exchange-CA-Certificate

CA Certificate File Format: ● PEM ○ DER

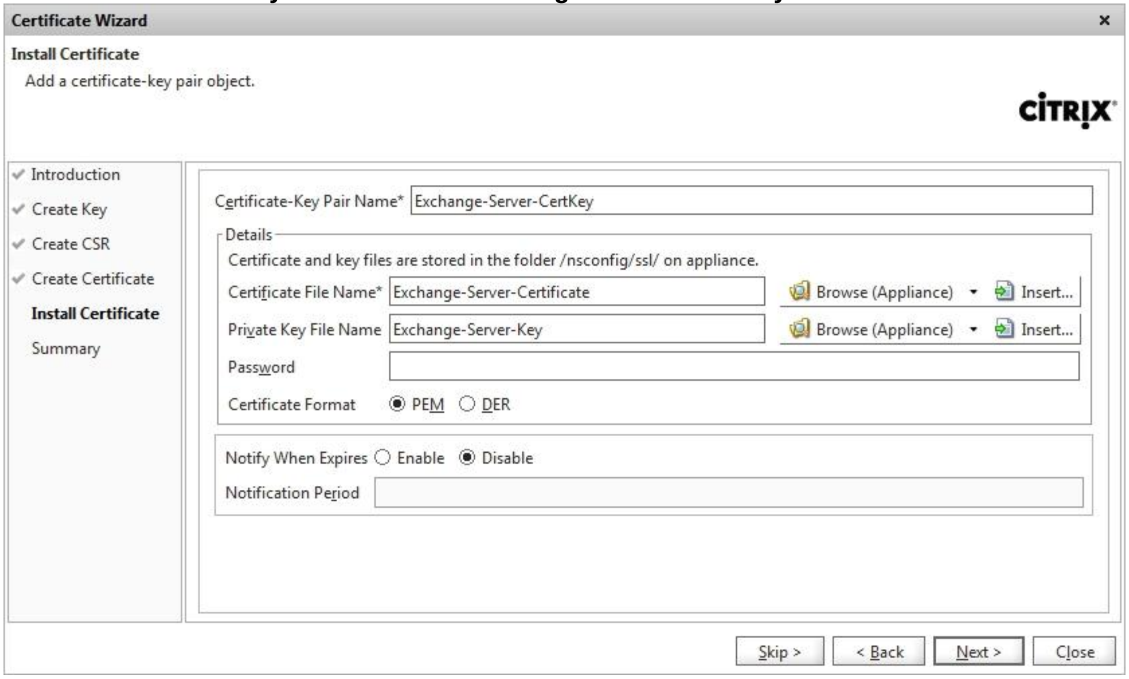
CA Key File Name*: Exchange-CA-Key

CA Key File Format: ● PEM ○ DER

PEM Passphrase (For Encrypted CA Key):

CA Serial Number File*: CAExhcnage

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



Certificate Wizard

Install Certificate

Add a certificate-key pair object.

Certificate-Key Pair Name*: Exchange-Server-CertKey

Details

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

Certificate File Name*: Exchange-Server-Certificate

Private Key File Name: Exchange-Server-Key

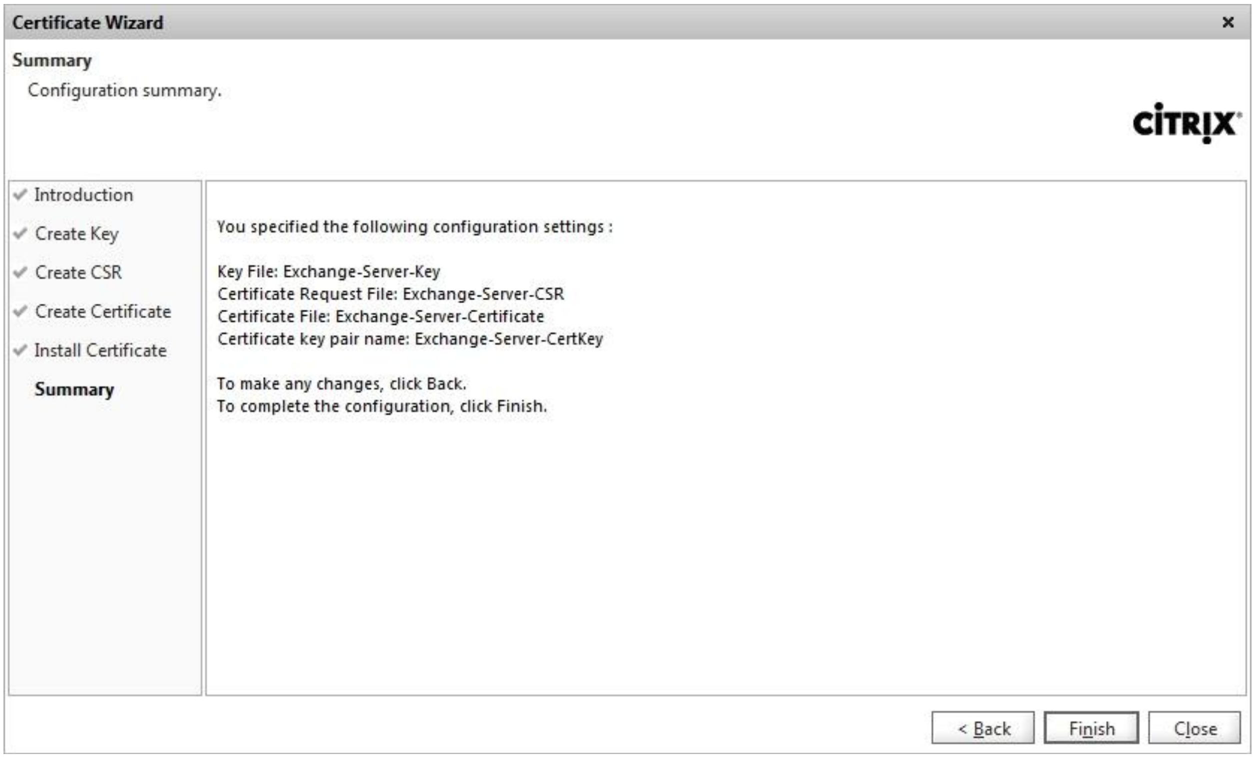
Password:

Certificate Format: ● PEM ○ DER

Notify When Expires: ○ Enable ● Disable

Notification Period:

Click **Finish**.

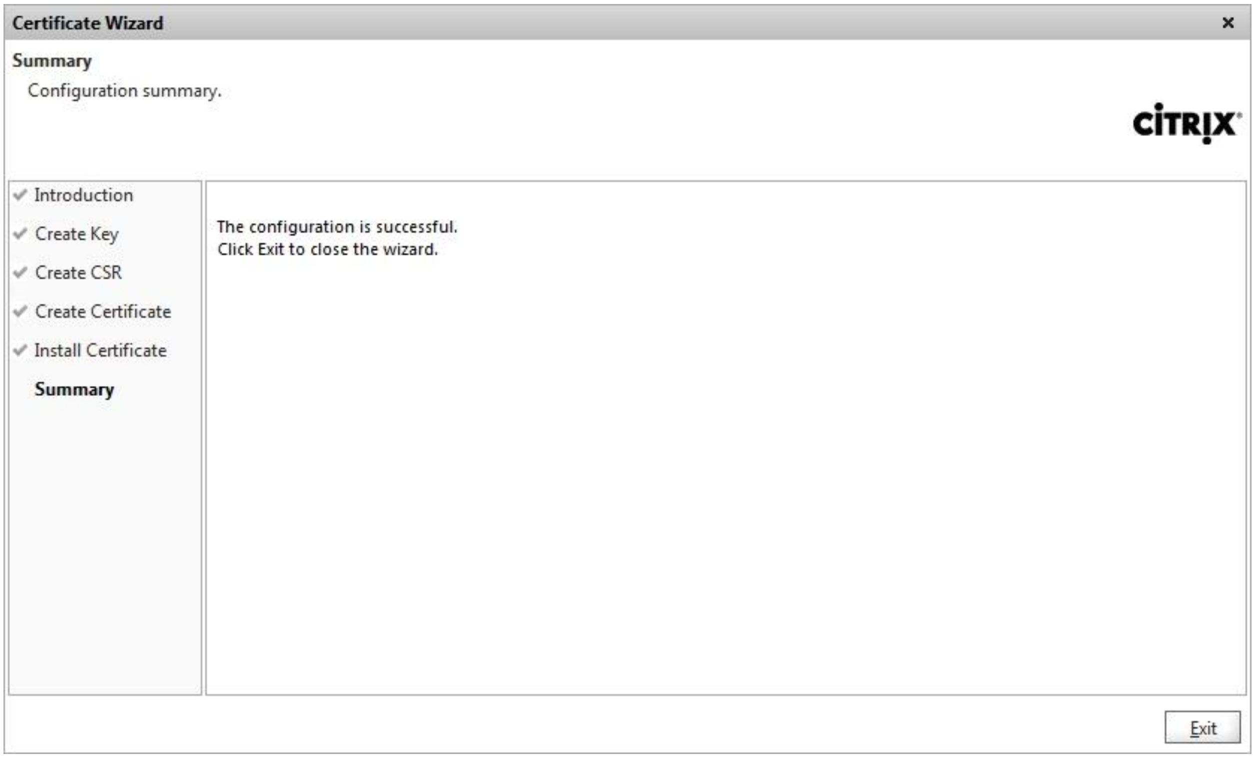


You specified the following configuration settings :

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

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

Click **Exit**.



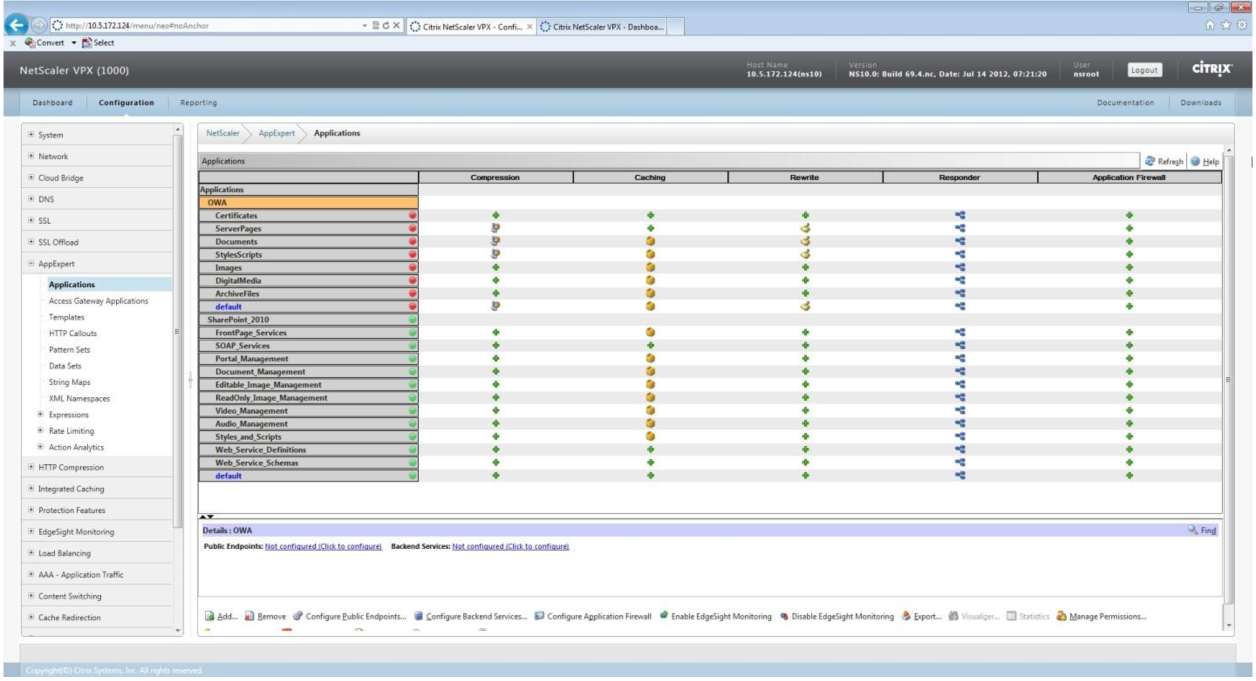
The configuration is successful.
Click Exit to close the wizard.

5.6 Creating virtual servers (VIP)

Virtual servers (or Virtual IP, VIP) will be used for users to connect to Exchange 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

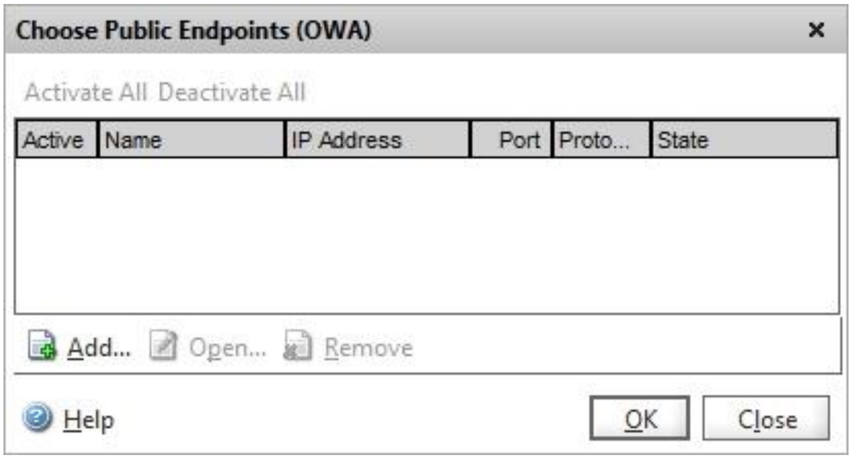
Under **AppExpert** navigation panel, choose **Applications** to view those installed templates. Under **OWA**, all the pre-defined Exchange service components will be listed. Choose **Configure Public Endpoints…** to set public virtual server name and ip address according to section 3.2.



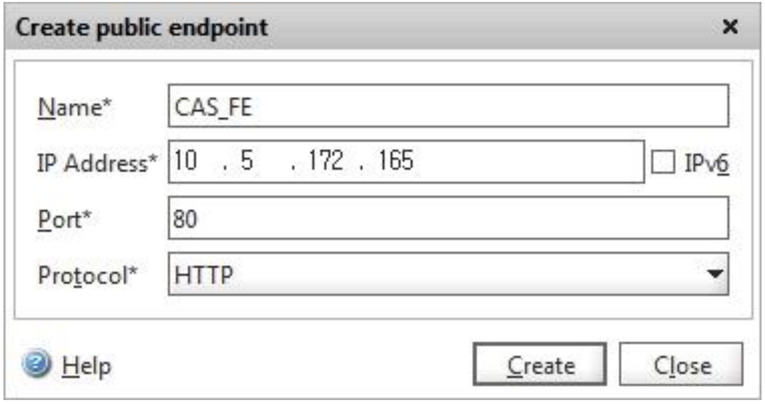
Details : OWA

Public Endpoints: Not configured (Click to configure) Backend Services: Not configured (Click to configure)

Choose **Add**.



Set **Name, IP Address**, **Port,** and **Protocol**. Click **Create**.



Create public endpoint

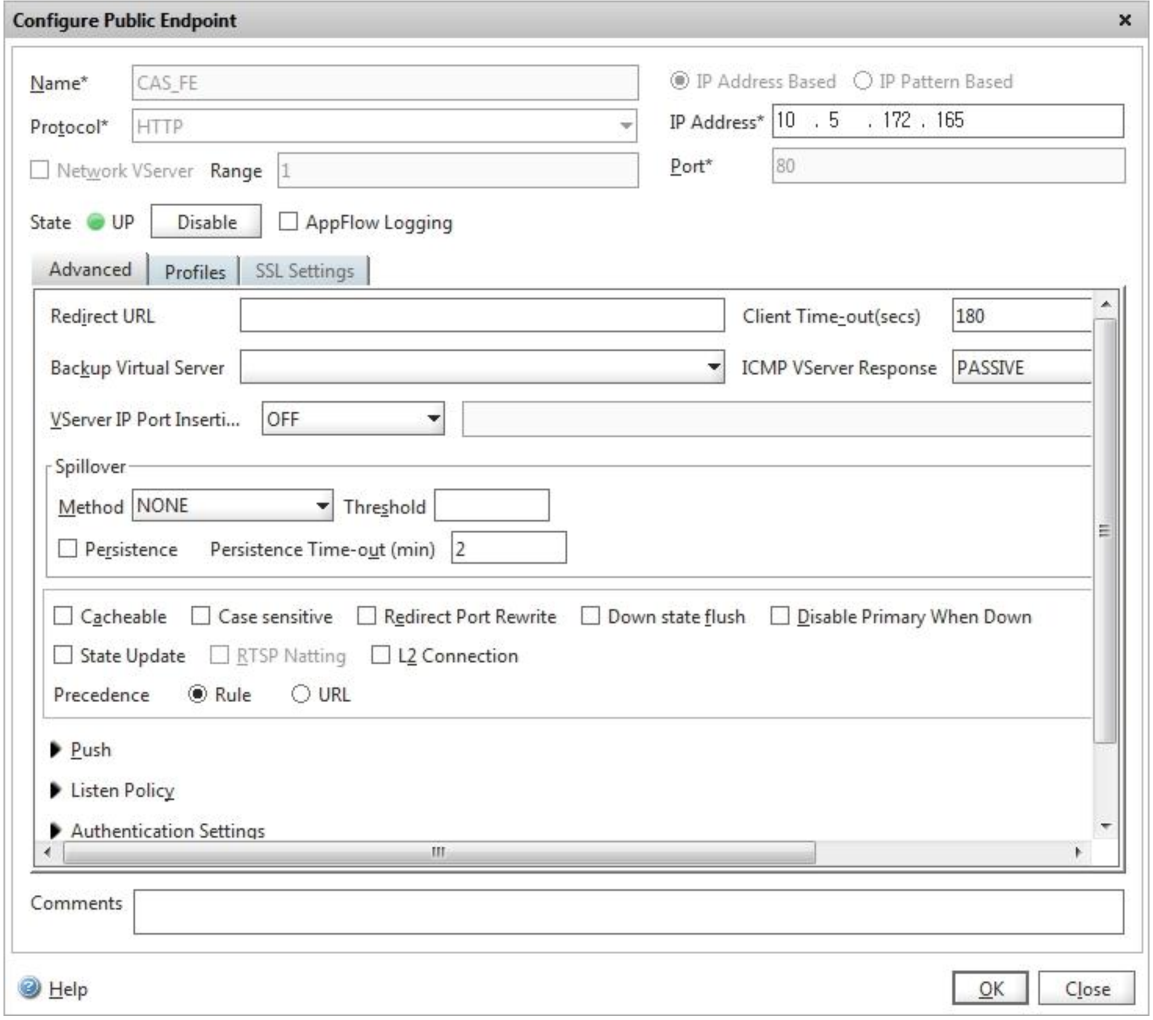
Name*: CAS_FE

IP Address*: 10 . 5 . 172 . 165 □ IPv6

Port*: 80

Protocol*: HTTP

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



Configure Public Endpoint

Name*: CAS_FE

Protocol*: HTTP

□ Network VServer Range: 1

● IP Address Based ○ IP Pattern Based

IP Address*: 10 . 5 . 172 . 165

Port*: 80

State ● UP Disable □ AppFlow Logging

Advanced | Profiles | SSL Settings

Redirect URL:

Backup Virtual Server:

VServer IP Port Inserti...: OFF

Client Time-out(secs): 180

ICMP VServer Response: PASSIVE

Spillover

Method: NONE Threshold:

□ Persistence Persistence Time-out (min): 2

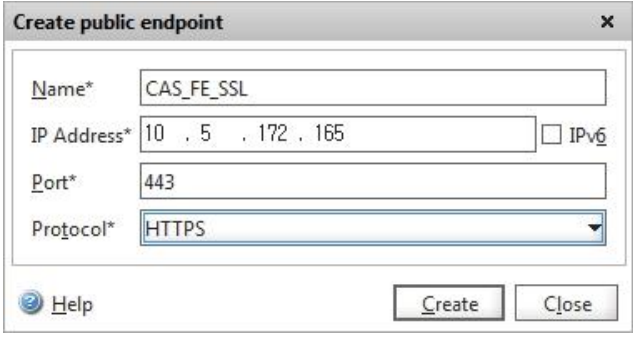
□ Cacheable □ Case sensitive □ Redirect Port Rewrite □ Down state flush □ Disable Primary When Down

□ State Update □ RTSP Natting □ L2 Connection

Precedence ● Rule ○ URL

5.6.2 HTTPS VIP

From the main NetScaler Configuration Utility screen, under **AppExpert** and **Applications**, and **OWA**, 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.). Set **Name** to **CASSe_FE_SSL** or meaningful name. Set **IP Address**, **Port 443** and **Protocal** as **HTTPS**. Then click **Create**.



Create public endpoint

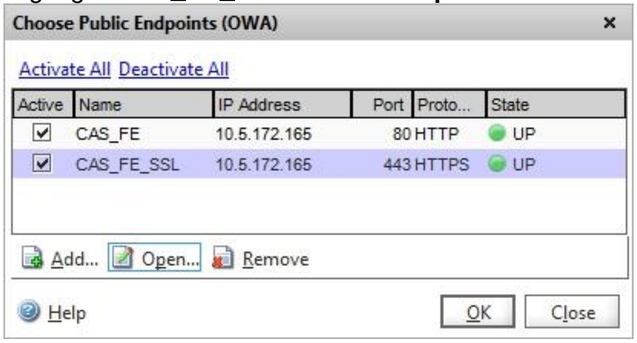
Name* CAS_FE_SSL

IP Address* 10 . 5 . 172 . 165 □ IPv6

Port* 443

Protocol* HTTPS

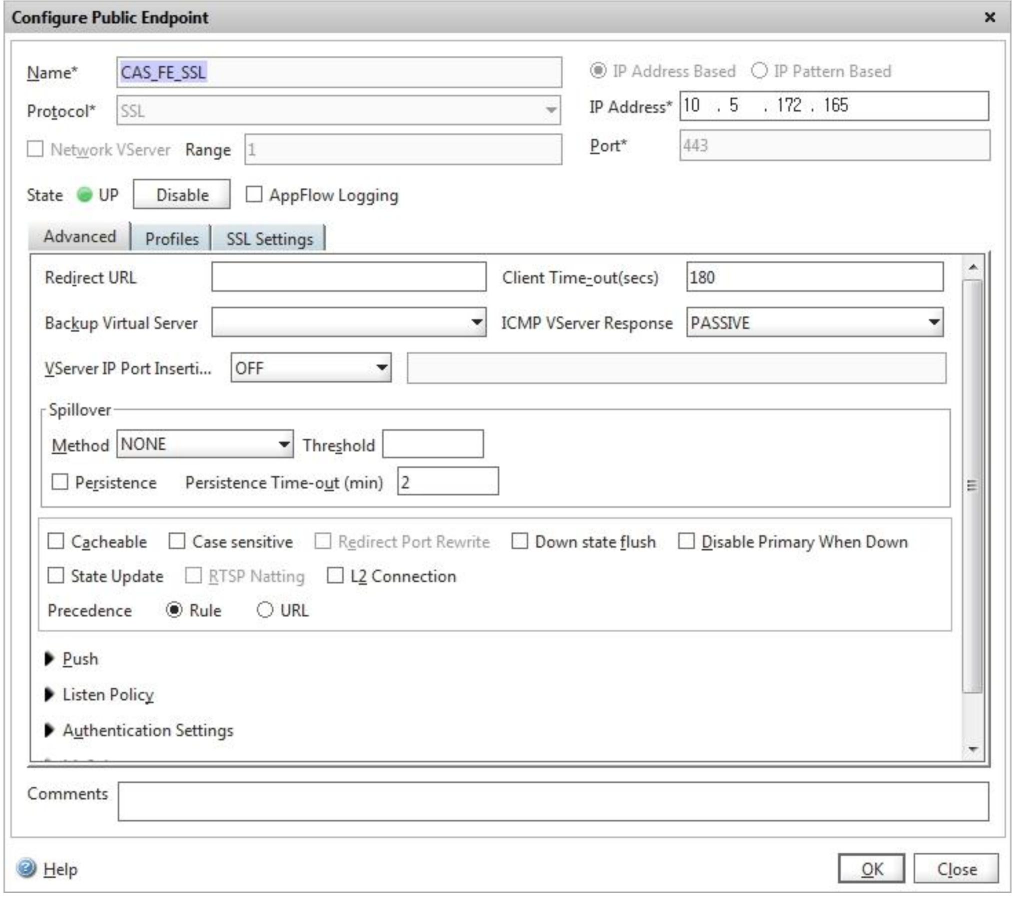
Highlight **CAS_FE_SSL** then click **Open…**



Choose Public Endpoints (OWA)

Active	Name	IP Address	Port	Proto...	State
☑	CAS_FE	10.5.172.165	80	HTTP	● UP
☑	CAS_FE_SSL	10.5.172.165	443	HTTPS	● UP

Set **Persistence Time-out (min)** to **2**. Click **SSL Settings**.



Configure Public Endpoint

Name* CAS_FE_SSL

Protocol* SSL

□ Network VServer Range 1

● IP Address Based ○ IP Pattern Based

IP Address* 10 . 5 . 172 . 165

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

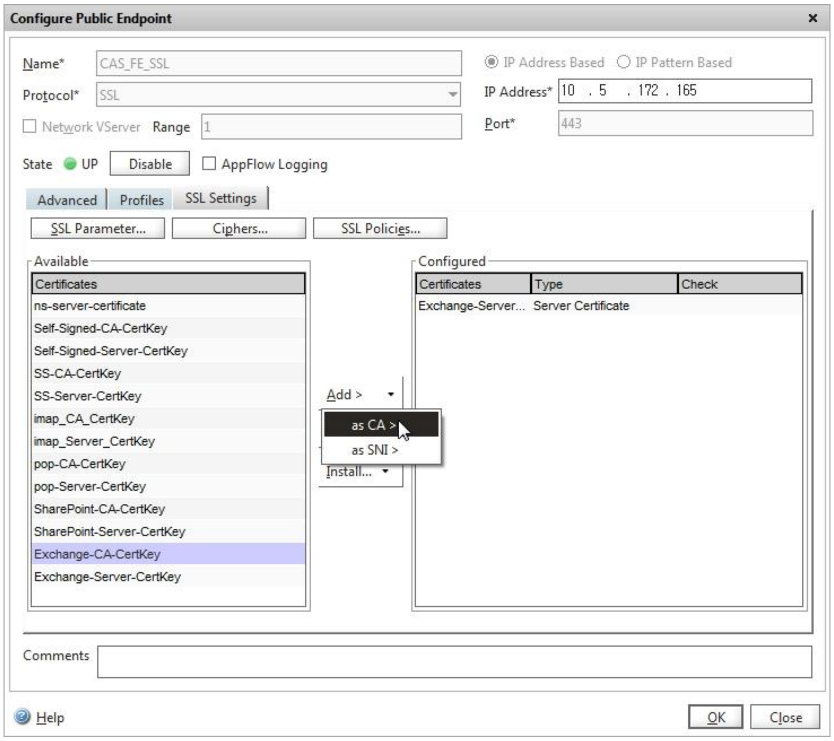
Listen Policy

Authentication Settings

Comments

Help OK Close

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*: CAS_FE_SSL

Protocol*: SSL

□ Network VServer Range: 1

● IP Address Based ○ IP Pattern Based

IP Address*: 10 . 5 . 172 . 165

Port*: 443

State: UP

□ AppFlow Logging

Available

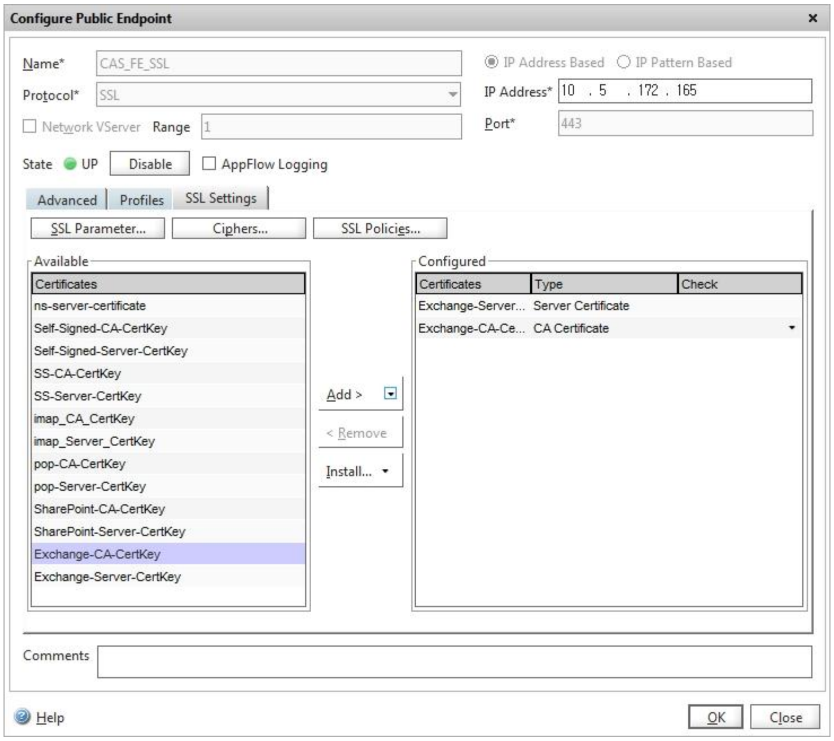
Certificates
ns-server-certificate
Self-Signed-CA-CertKey
Self-Signed-Server-CertKey
SS-CA-CertKey
SS-Server-CertKey
imap_CA_CertKey
imap_Server_CertKey
pop-CA-CertKey
pop-Server-CertKey
SharePoint-CA-CertKey
SharePoint-Server-CertKey
Exchange-CA-CertKey
Exchange-Server-CertKey

Configured

Certificates	Type	Check
Exchange-Server...	Server Certificate	

Comments:

Click **OK**.



Configure Public Endpoint

Name*: CAS_FE_SSL

Protocol*: SSL

□ Network VServer Range: 1

● IP Address Based ○ IP Pattern Based

IP Address*: 10 . 5 . 172 . 165

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

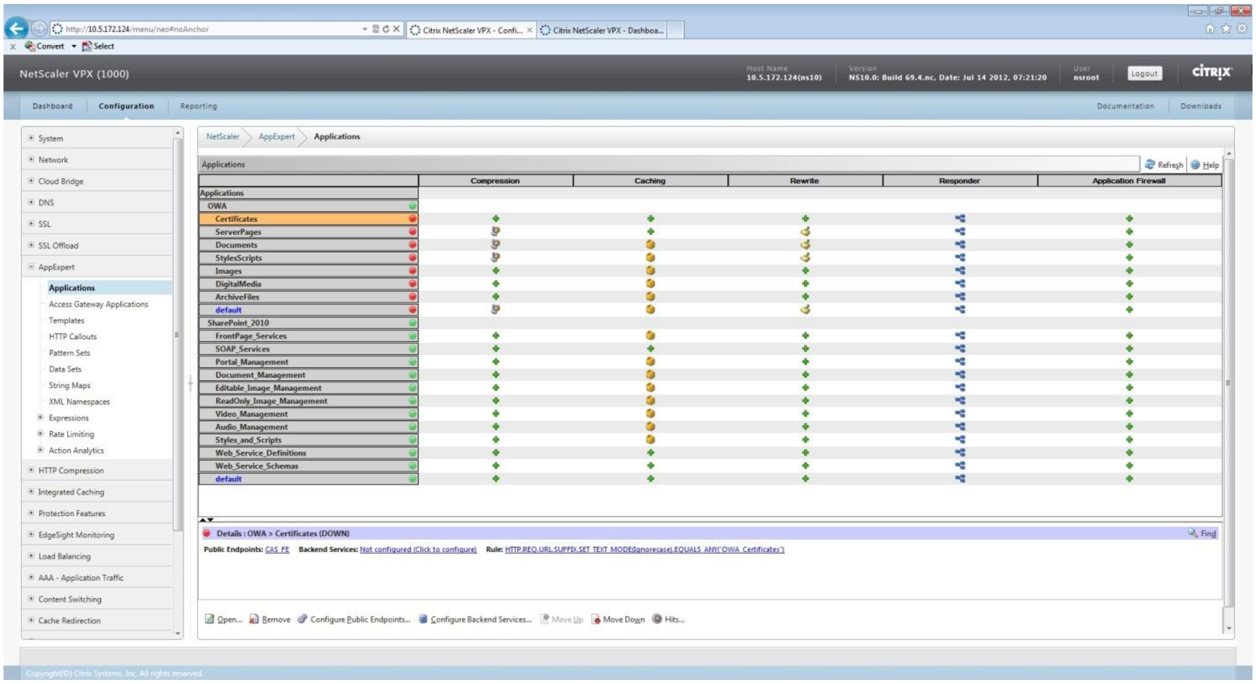
Configured

Certificates	Type	Check
Exchange-Server...	Server Certificate	
Exchange-CA-Ce...	CA Certificate	

Comments:

5.7 Creating a Service Group

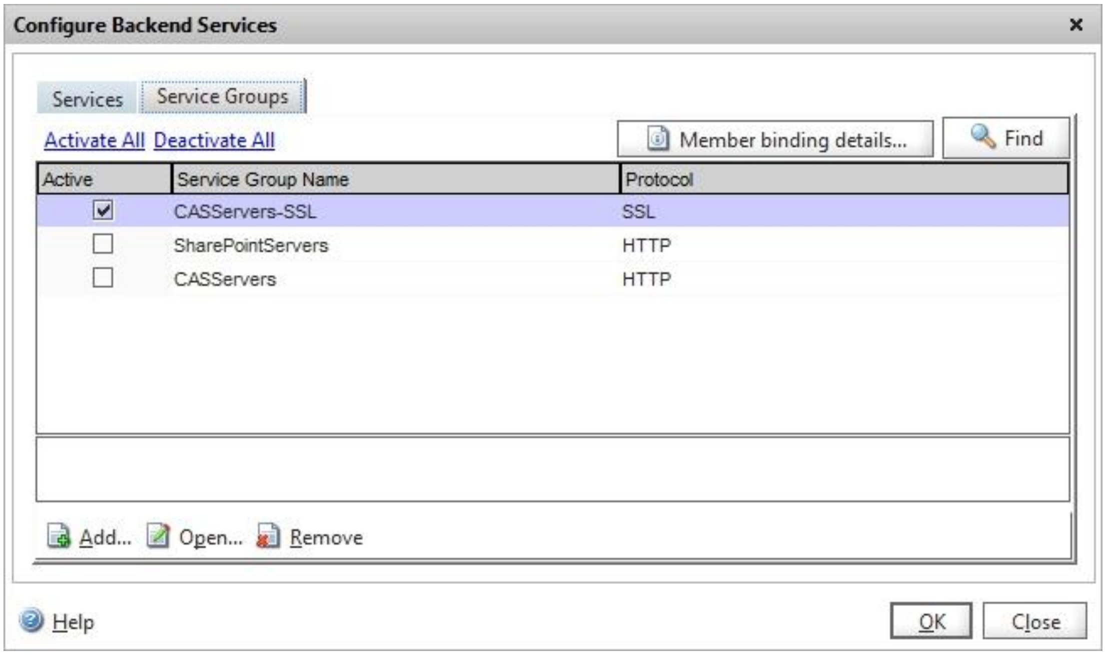
From the main NetScaler Configuration Utility screen, under **AppExpert** and **Applications**, and **OWA**, choose **Configure Backend Services…** to set **Service Groups** to add physical/VM server IP addresses.



Details : OWA > Certificates (DOWN)

Public Endpoints: CAS_FE Backend Services: Not configured (Click to configure) Rule: HTTP.REQ.URL.SUFFIX.SET_TEXT_MODE(Ignorecase).EQUALS_ANY("OWA_Certificates")

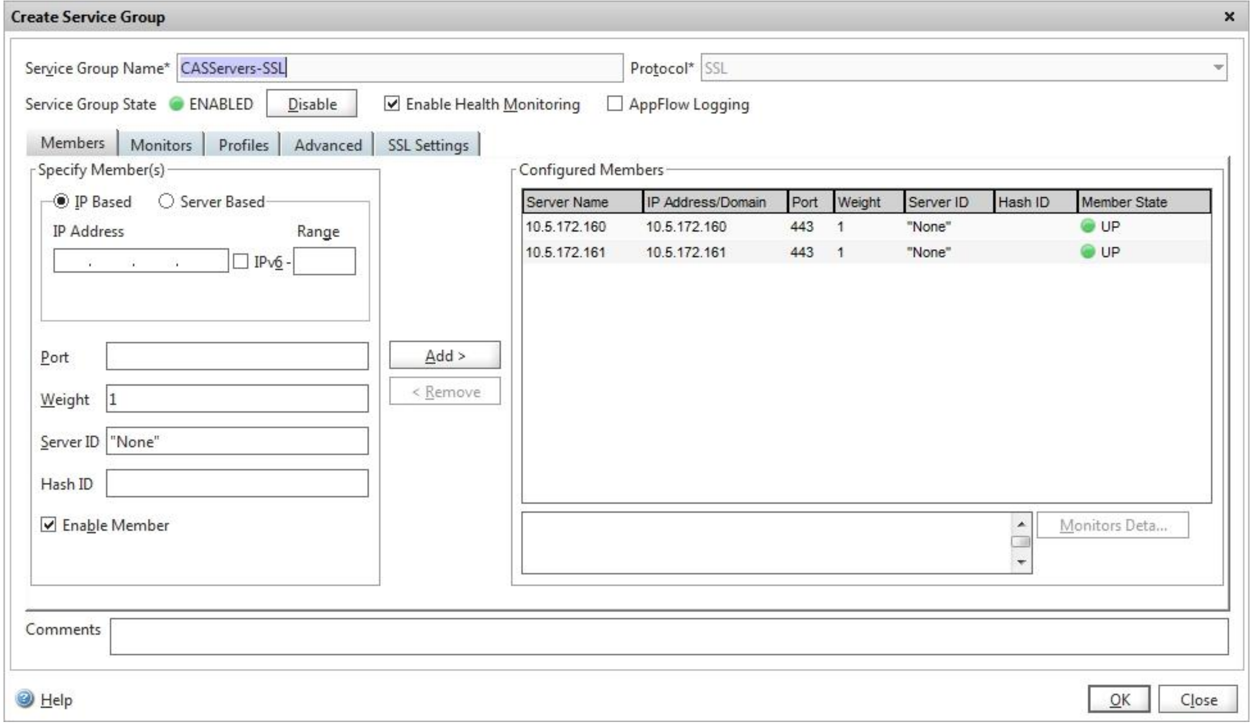
Click **Add…**



Configure Backend Services

Active	Service Group Name	Protocol
☑	CASServers-SSL	SSL
□	SharePointServers	HTTP
□	CASServers	HTTP

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



Service Group Name* CASServers-SSL   Protocol* SSL

Service Group State ● ENABLED   ☑ Enable Health Monitoring   ☐ AppFlow Logging

Specify Member(s)

● IP Based   ○ Server Based

IP Address . . .   ☐ IPv6 -   Range

Port

Weight 1

Server ID "None"

Hash ID

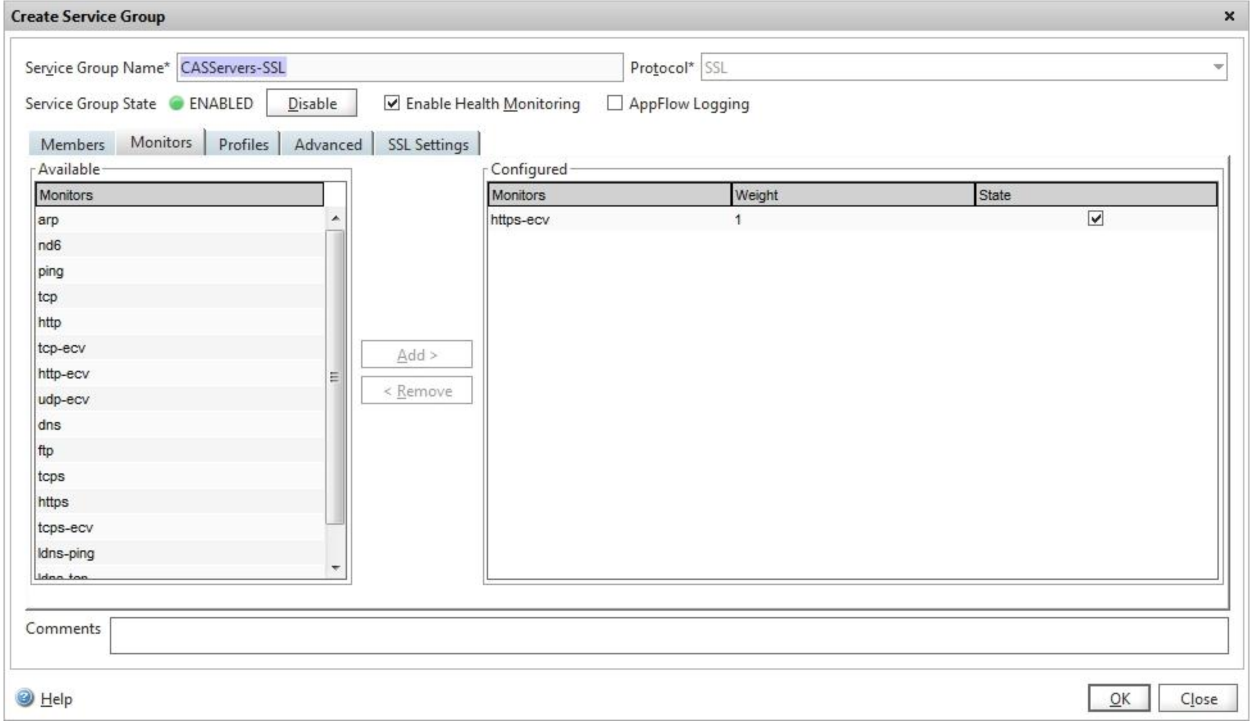
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.160	10.5.172.160	443	1	"None"		● UP
10.5.172.161	10.5.172.161	443	1	"None"		● UP

Comments

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



Service Group Name* CASServers-SSL   Protocol* SSL

Service Group State ● ENABLED   ☑ Enable Health Monitoring   ☐ AppFlow Logging

Available

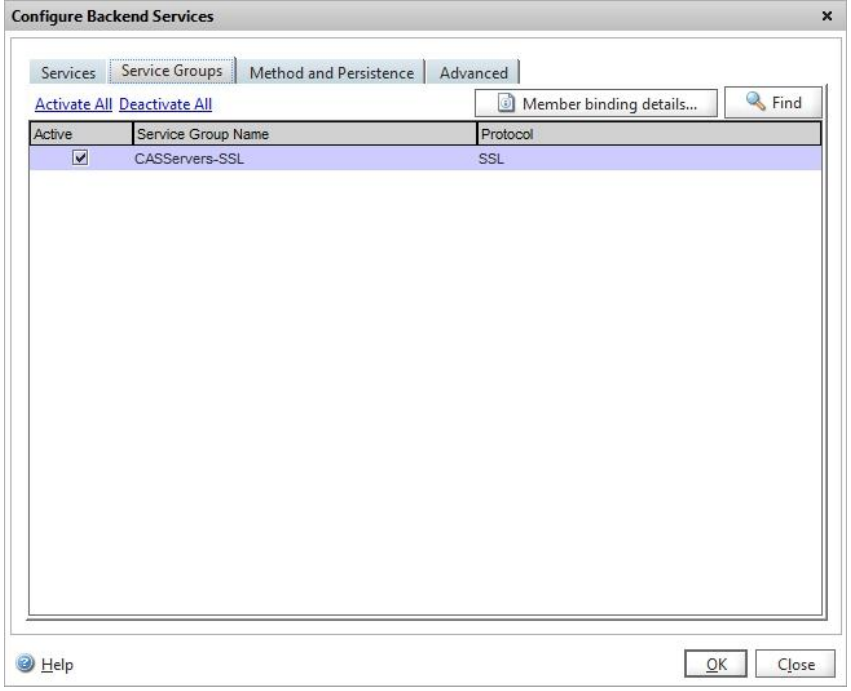
Monitors
arp
nd6
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
ldns-ping
ldns-tcp

Configured

Monitors	Weight	State
https-ecv	1	☑

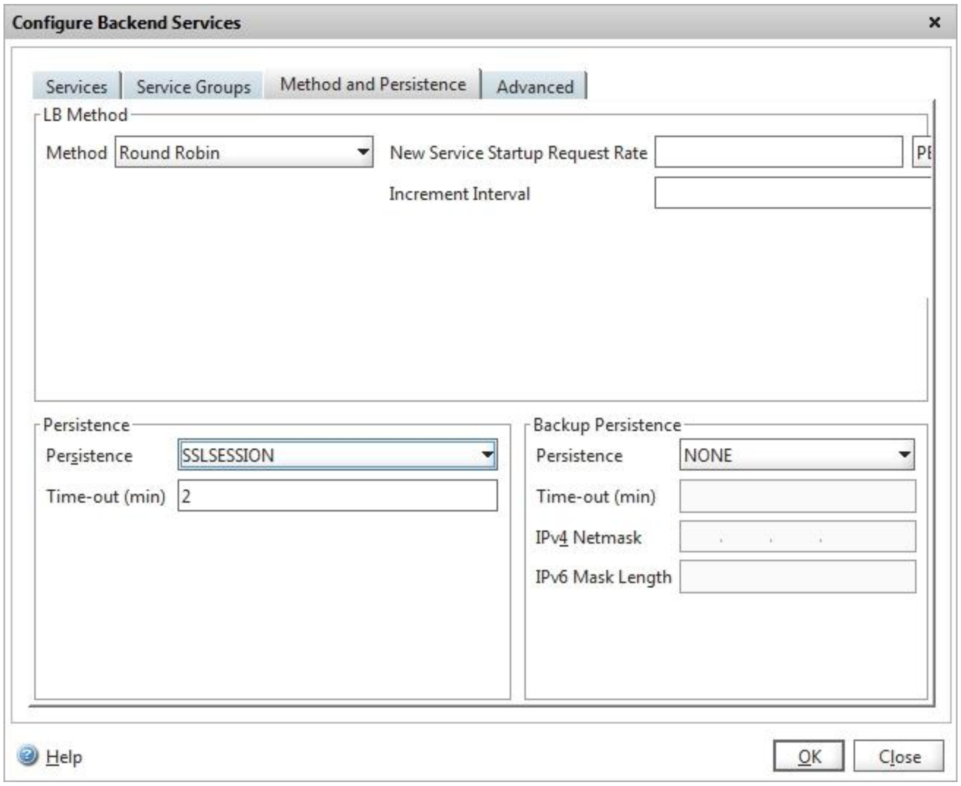
Comments

Select **CASServers-SSL** which was just created under **Configure Backend Services**.



Active	Service Group Name	Protocol
☑	CASServers-SSL	SSL

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



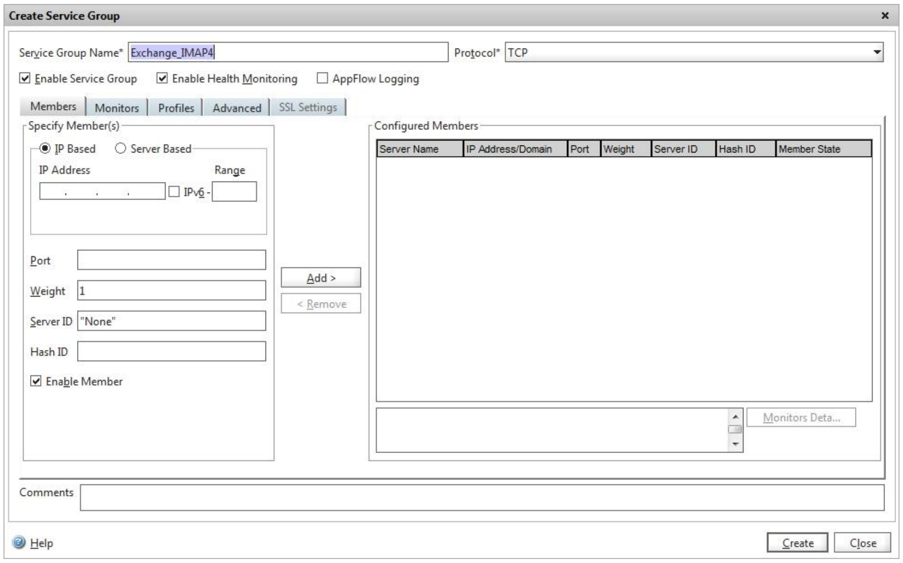
Method: Round Robin
New Service Startup Request Rate:
Increment Interval:

Persistence: SSLSESSION
Time-out (min): 2

Backup Persistence
Persistence: NONE
Time-out (min):
IPv4 Netmask:
IPv6 Mask Length:

5.8 IMAP4 installation

IMAP4 service was not added as part of Exchange (OWA) AppExpert Template. In order to install and configure the service, a *service group* needs to be created with physical/VM servers to be load balanced. Then a *virtual server* will be created using the service group.
From main NetScaler navigation panel, choose **Service Groups** under **Load Balancing**. Click **Add…**



Create Service Group

Service Group Name* Exchange_IMAP4

Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring ☐ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address . . . ☐ IPv6 - Range

Port

Weight 1

Server ID "None"

Hash ID

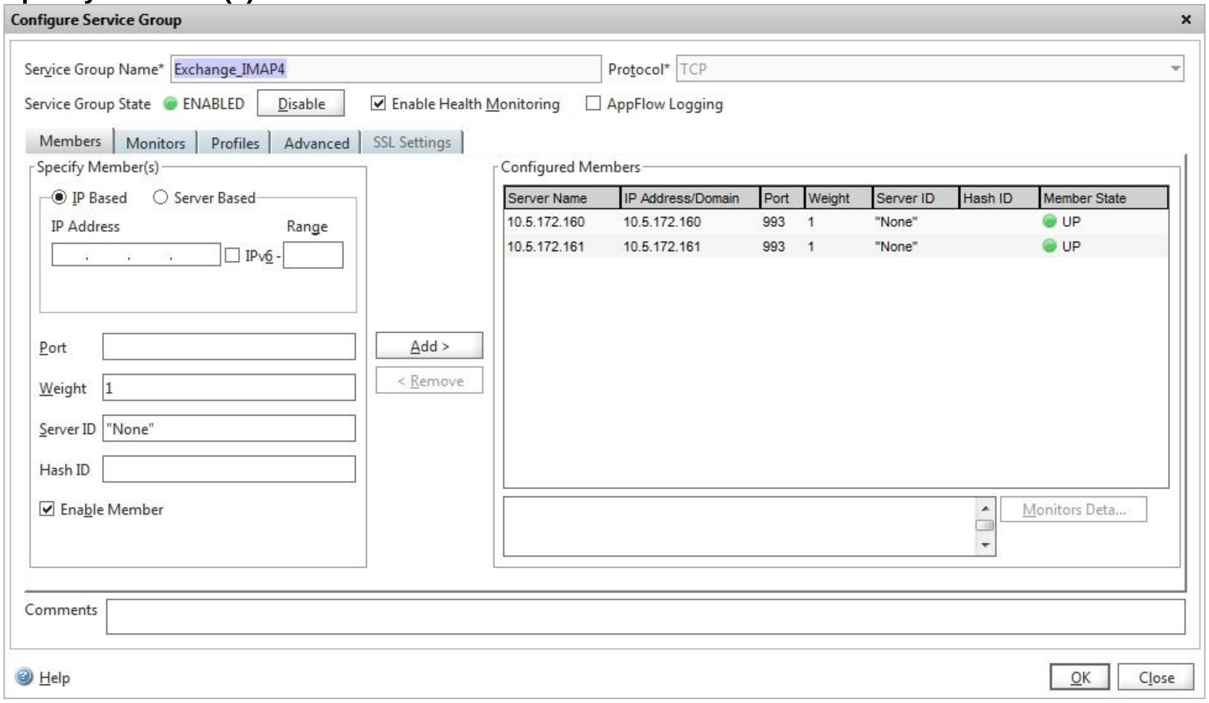
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State

Comments

Set **Service Group Name** to **Exchange_IMAP4** and add designated physical/VM servers under **Specify Members(s)** with **993 Port**. Click **Create**.



Configure Service Group

Service Group Name* Exchange_IMAP4

Protocol* TCP

Service Group State ● ENABLED

☑ Enable Health Monitoring ☐ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address . . . ☐ IPv6 - Range

Port

Weight 1

Server ID "None"

Hash ID

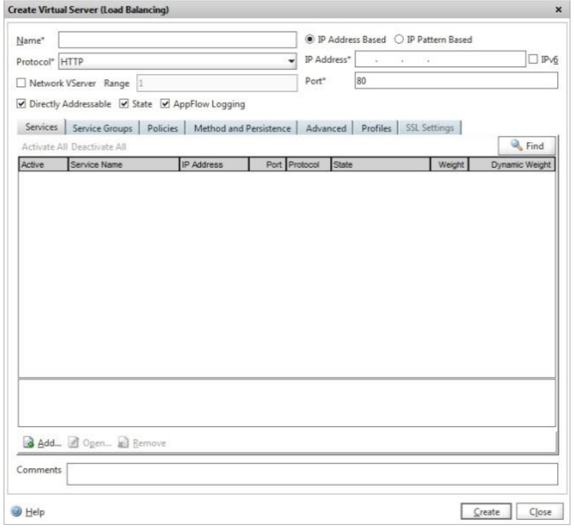
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.160	10.5.172.160	993	1	"None"		● UP
10.5.172.161	10.5.172.161	993	1	"None"		● UP

Comments

Under **Load Balancing** navigation panel, choose **Virtual Servers**. Click **Add…**



Create Virtual Server (Load Balancing)

Name*

● IP Address Based ○ IP Pattern Based

Protocol* HTTP

IP Address* . . .

□ IPv6

□ Network VServer Range 1

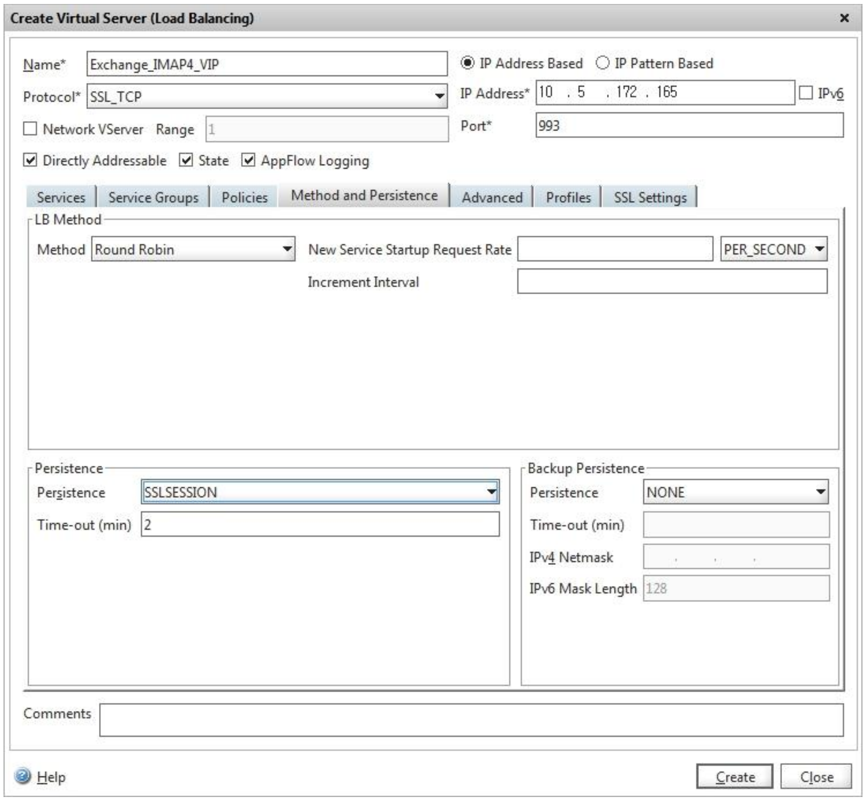
Port* 80

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight

Comments

Set **Name** to **Exchange_IMAP4_VIP** and **IP Address**. **Protocol** to **SSL_TCP**. Choose **Method and Persistence** tab. Set **Round Robin** Method and **SSLSESSION** Persistence.



Create Virtual Server (Load Balancing)

Name* Exchange_IMAP4_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_TCP

IP Address* 10 . 5 . 172 . 165

□ IPv6

□ Network VServer Range 1

Port* 993

☑ Directly Addressable ☑ State ☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SSLSESSION

Time-out (min) 2

Backup Persistence

Persistence NONE

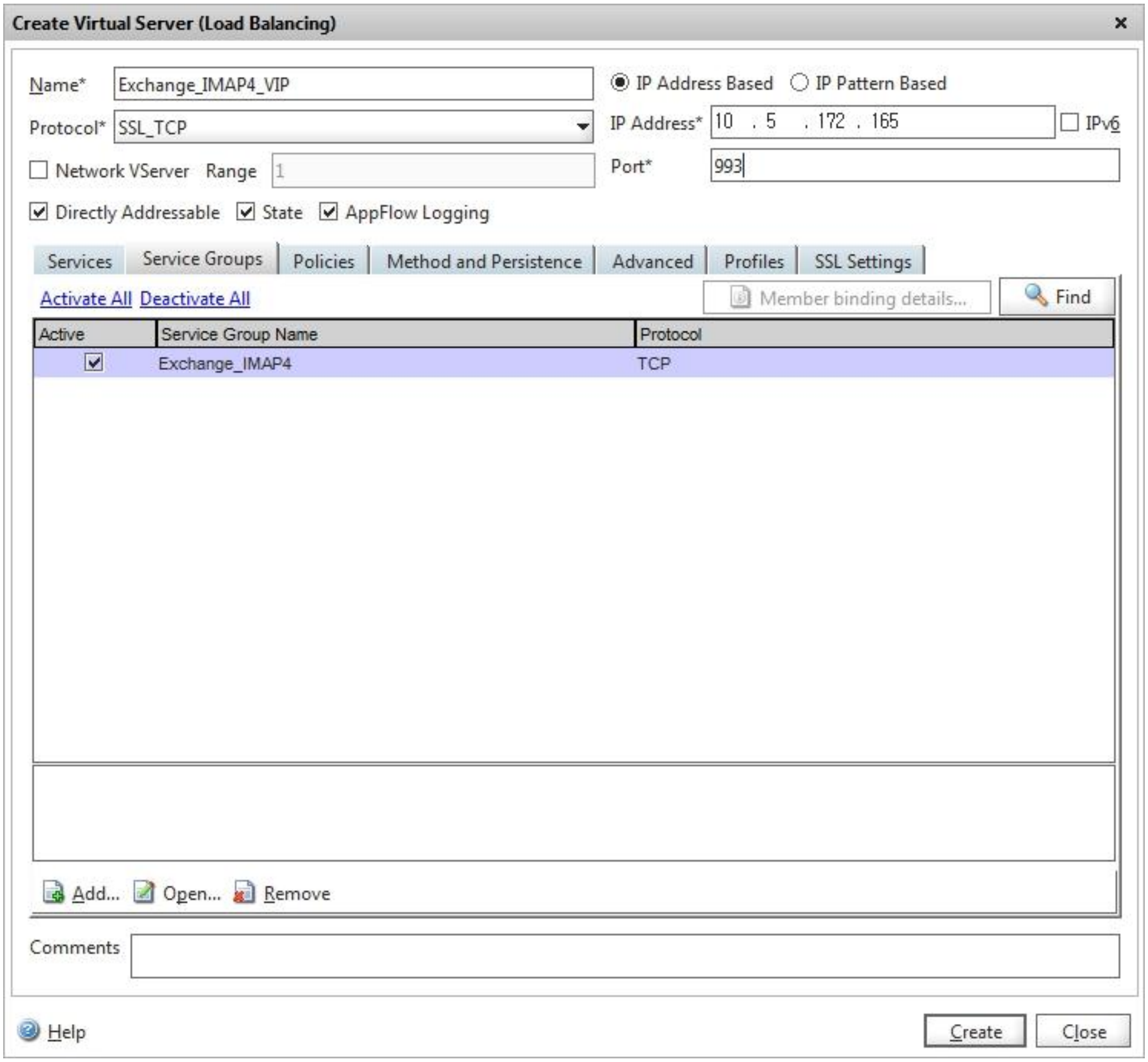
Time-out (min)

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Binding **Exchange_IMAP4** service group under **Service Groups** tab.



Create Virtual Server (Load Balancing)

Name* Exchange_IMAP4_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_TCP

IP Address* 10 . 5 . 172 . 165 □ IPv6

□ Network VServer Range 1

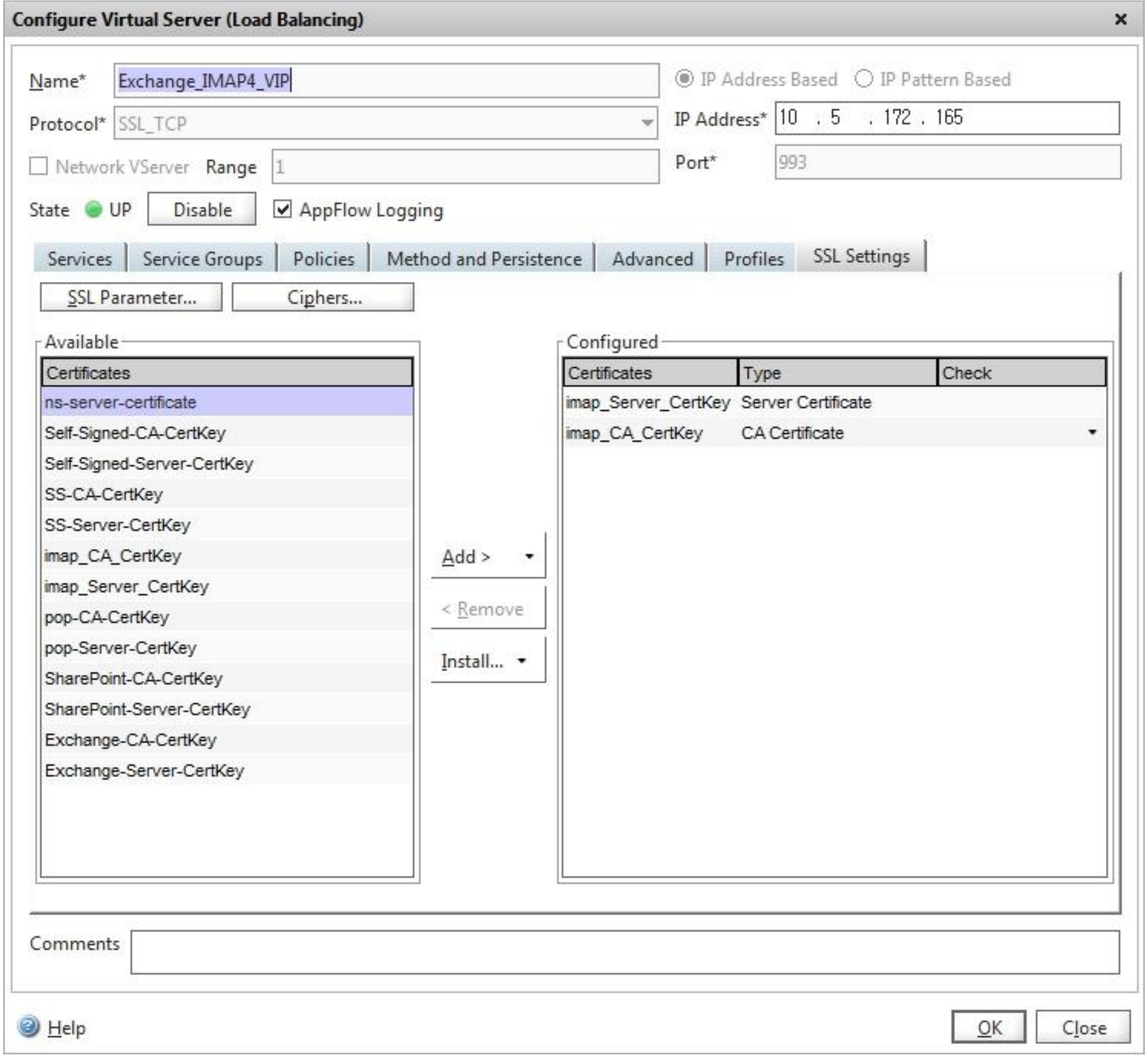
Port* 993

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Active	Service Group Name	Protocol
☑	Exchange_IMAP4	TCP

Comments

Add **Certificates** under **SSL Settings**. Then click **Create**.



Name* Exchange_IMAP4_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_TCP

IP Address* 10 . 5 . 172 . 165

□ Network VServer Range 1

Port* 993

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

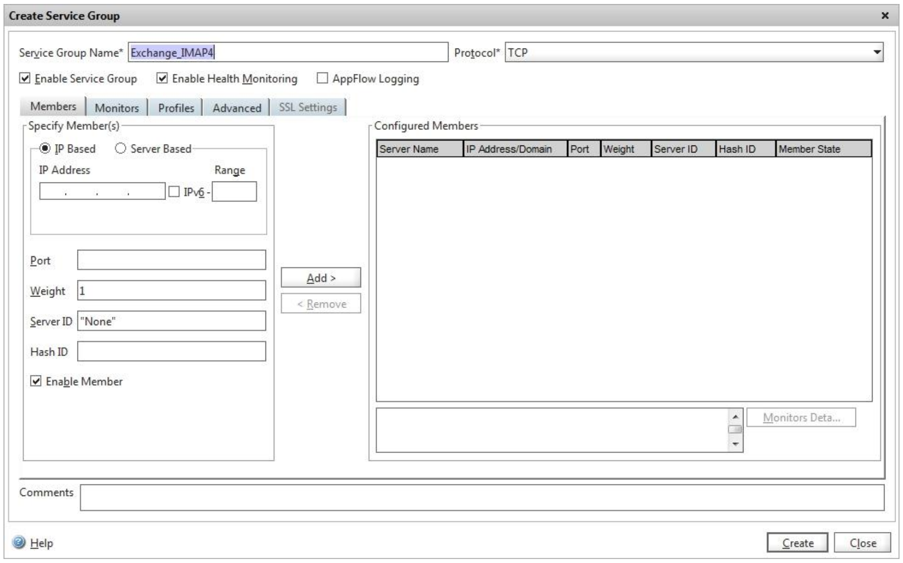
Certificates	Type	Check
imap_Server_CertKey	Server Certificate	
imap_CA_CertKey	CA Certificate	

Comments

5.9 POP3 installation

POP3 service was not added as part of Exchange (OWA) AppExpert Template. In order to install and configure the service, a *service group* needs to be created with physical/VM servers to be load balanced. Then a *virtual server* will be created using the service group.

From main NetScaler navigation panel, choose **Service Groups** under **Load Balancing**. Click **Add…**



Service Group Name* Exchange_IMAP4

Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring ☐ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address Range ☐ IPv6

Port

Weight 1

Server ID "None"

Hash ID

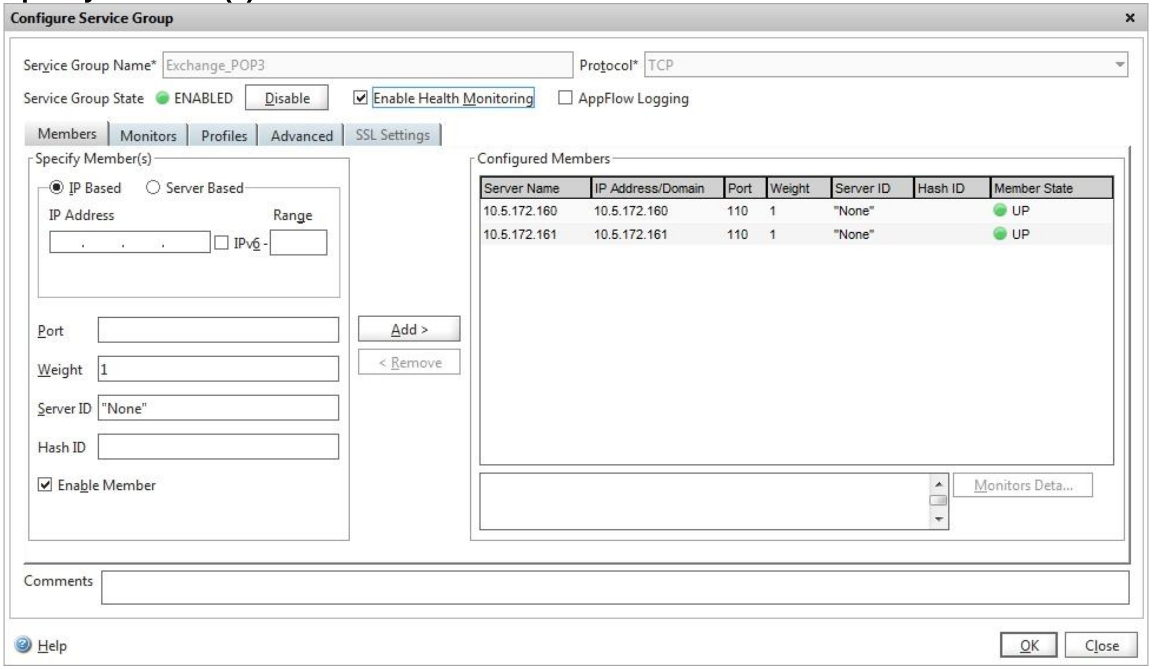
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State

Comments

Set **Service Group Name** to **Exchange_POP3** and add designated physical/VM servers under **Specify Members(s)** with **110 Port**. Click **Create**.



Service Group Name* Exchange_POP3

Protocol* TCP

Service Group State ● ENABLED

☑ Enable Health Monitoring ☐ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address Range ☐ IPv6

Port

Weight 1

Server ID "None"

Hash ID

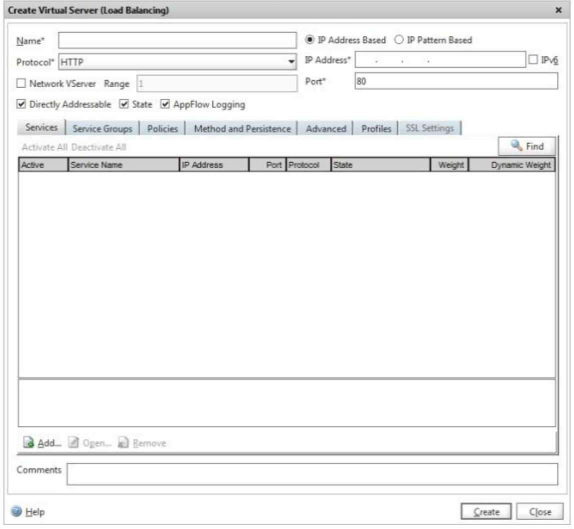
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.160	10.5.172.160	110	1	"None"		● UP
10.5.172.161	10.5.172.161	110	1	"None"		● UP

Comments

Under **Load Balancing** navigation panel, choose **Virtual Servers**. Click **Add…**


Create Virtual Server (Load Balancing)

Name*

● IP Address Based ○ IP Pattern Based

Protocol* HTTP

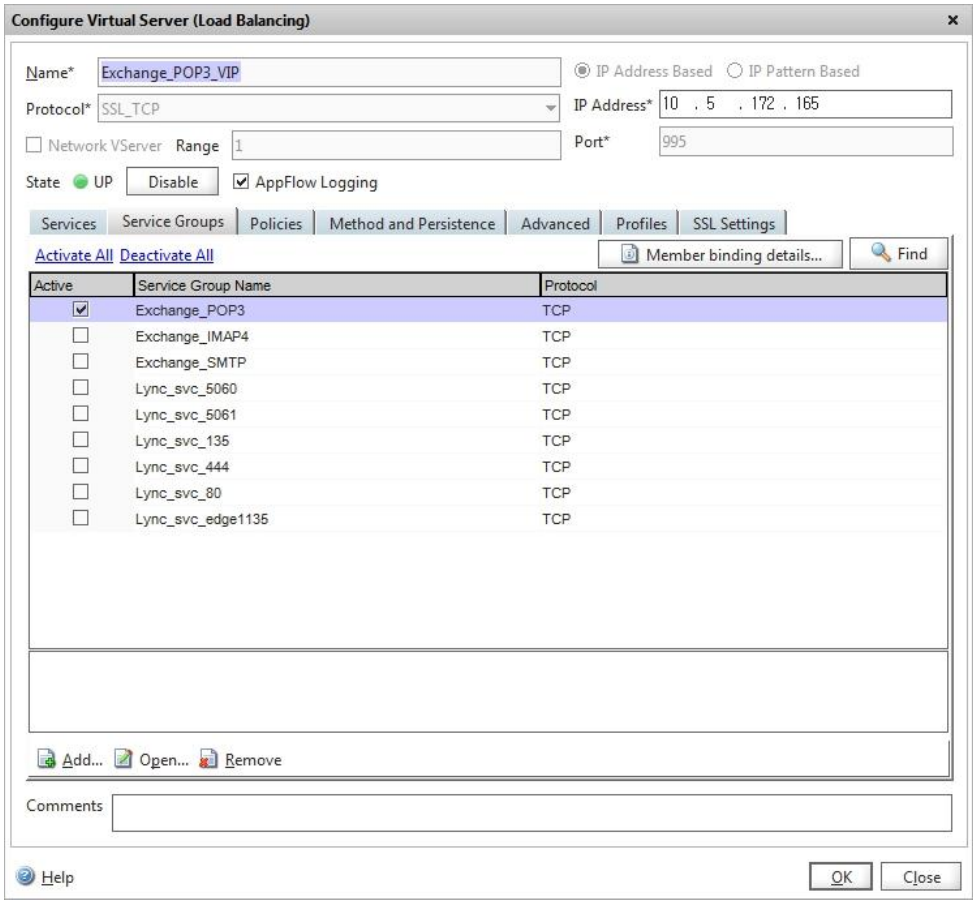
IP Address* . . . □ IPv6

□ Network VServer Range 1

Port* 80

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Set **Name** to **Exchange_POP3_VIP** and **IP Address**. **Protocol** to **SSL_TCP**. Choose **Method and Persistence** tab. Set **Round Robin** Method and **SSLSESSION** Persistence. Binding **Exchange_POP3** service group under **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Exchange_POP3_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_TCP

IP Address* 10 . 5 . 172 . 165

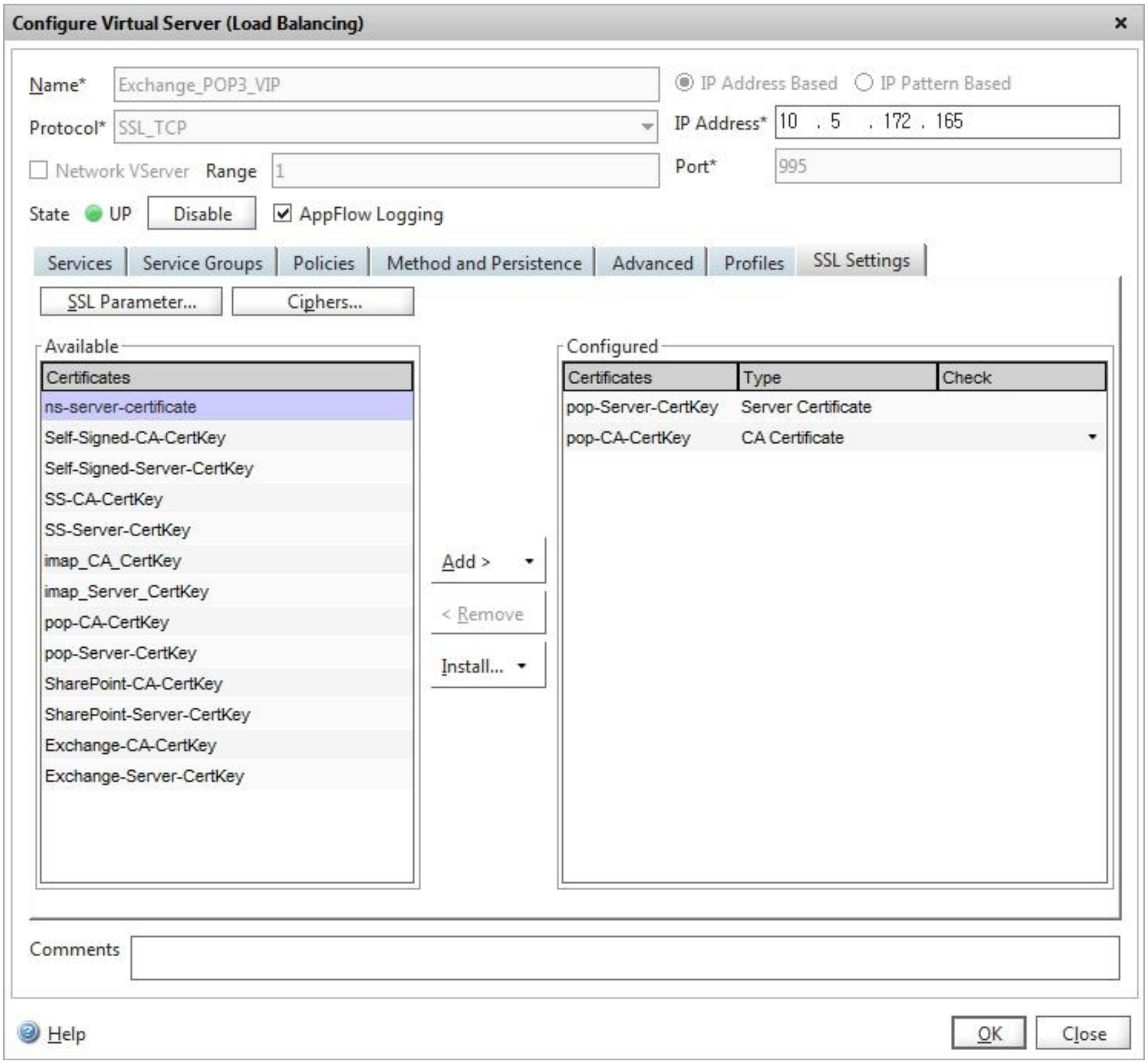
□ Network VServer Range 1

Port* 995

State UP Disable ☑ AppFlow Logging

Active	Service Group Name	Protocol
☑	Exchange_POP3	TCP
□	Exchange_IMAP4	TCP
□	Exchange_SMTP	TCP
□	Lync_svc_5060	TCP
□	Lync_svc_5061	TCP
□	Lync_svc_135	TCP
□	Lync_svc_444	TCP
□	Lync_svc_80	TCP
□	Lync_svc_edge1135	TCP

Add **Certificates** under **SSL Settings**. Then click **Create**.



Configure Virtual Server (Load Balancing)

Name* Exchange_POP3_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_TCP

IP Address* 10 . 5 . 172 . 165

□ Network VServer Range 1

Port* 995

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

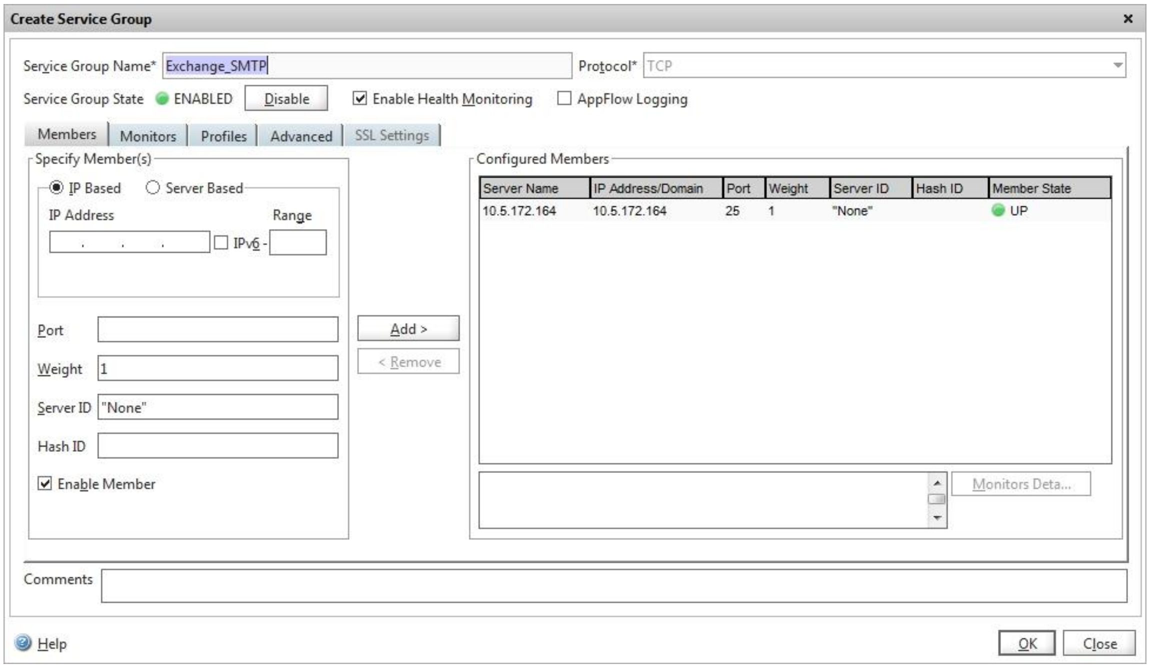
Configured

Certificates	Type	Check
pop-Server-CertKey	Server Certificate	
pop-CA-CertKey	CA Certificate	

Comments

5.10 SMTP installation

SMTP service was not added as part of Exchange (OWA) AppExpert Template. In order to install and configure the service, a *service group* needs to be created with physical/VM servers to be load balanced. Then a *virtual server* will be created using the service group.
From main NetScaler navigation panel, choose **Service Groups** under **Load Balancing**. Click **Add…**


Create Service Group

Service Group Name* Exchange_SMTP Protocol* TCP

Service Group State ● ENABLED Disable ☑ Enable Health Monitoring □ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address Range

□ IPv6

Port

Weight 1

Server ID "None"

Hash ID

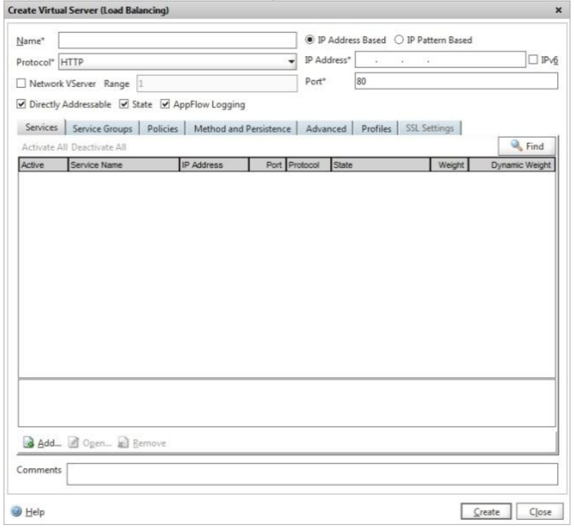
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.164	10.5.172.164	25	1	"None"		● UP

Comments

Set **Service Group Name** to **Exchange_SMTP** and add designated physical/VM servers under **Specify Members(s)** with **25 Port**. Click **Create**.
Under **Load Balancing** navigation panel, choose **Virtual Servers**. Click **Add…**


Create Virtual Server (Load Balancing)

Name* ● IP Address Based ○ IP Pattern Based

Protocol* HTTP IP Address* □ IPv6

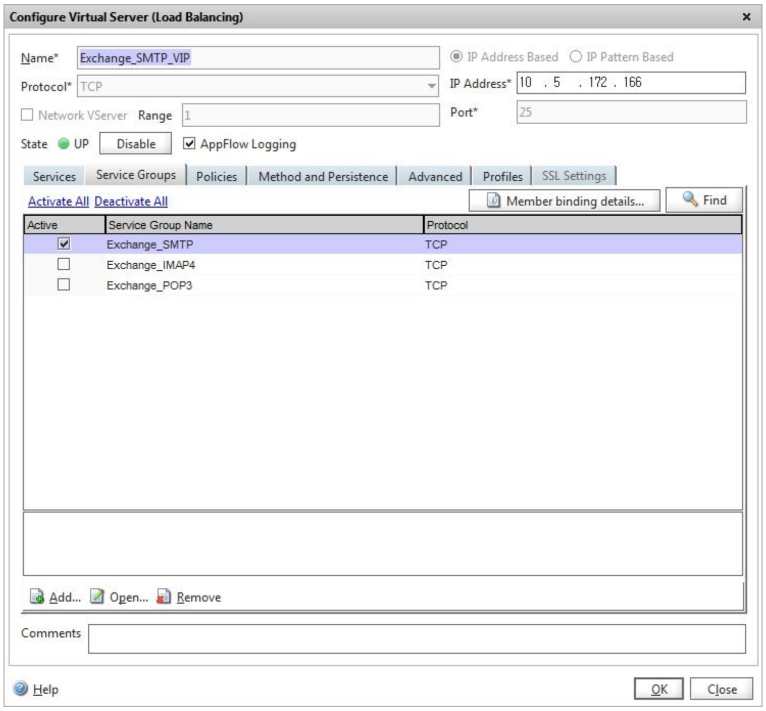
□ Network VServer Range 1 Port* 80

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight

Comments

Set **Name** to **Exchange_SMTP_VIP** and **IP Address**. **Protocol** to **TCP**. Choose **Method and Persistence** tab. Set **Round Robin** Method and **SSLSESSION** Persistence. Binding **Exchange_SMTP** service group under **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Exchange_SMTP_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 166

□ Network VServer Range 1

Port* 25

State ● UP

☑ AppFlow Logging

Active	Service Group Name	Protocol
☑	Exchange_SMTP	TCP
□	Exchange_IMAP4	TCP
□	Exchange_POP3	TCP

Comments

5.11 Outlook Anywhere, ActiveSync confirmation

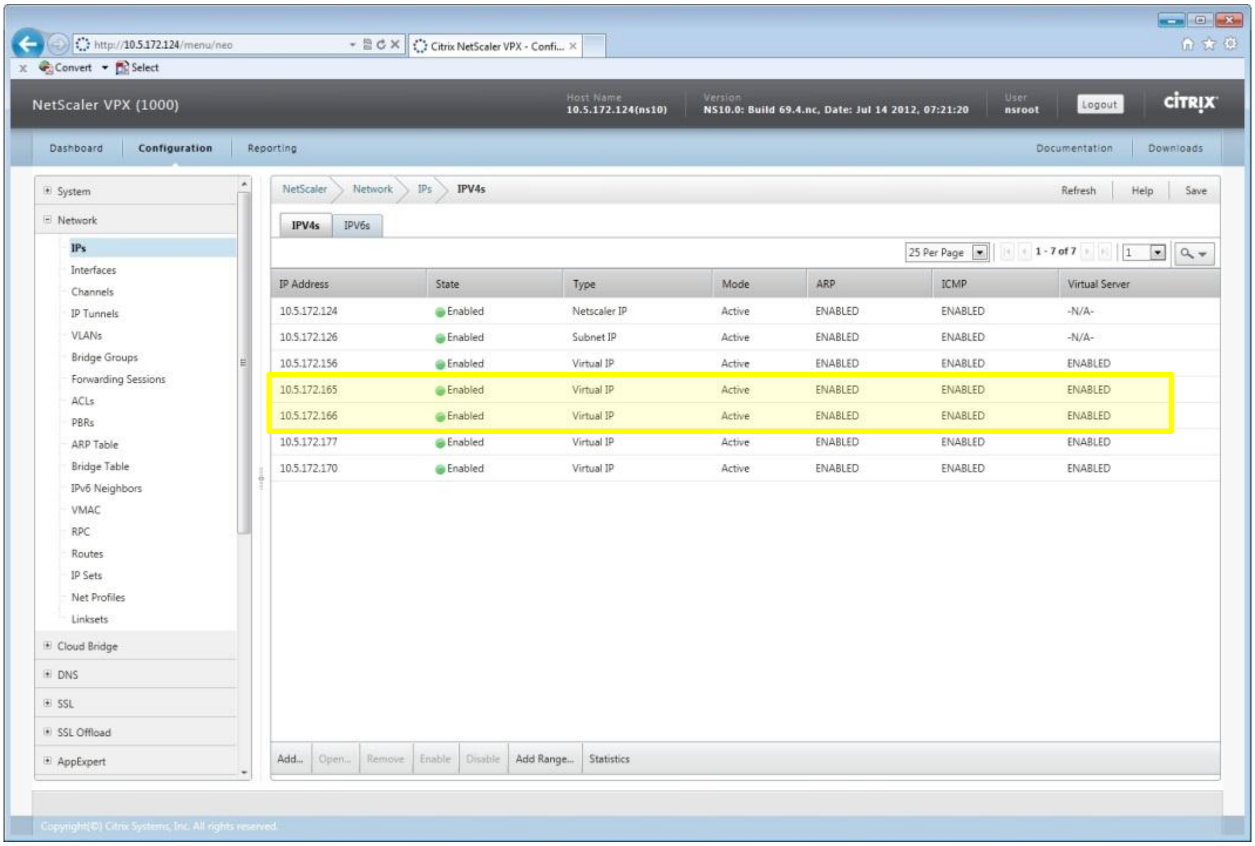
Microsoft Outlook Anywhere (OA) allows Exchange access through the Microsoft Outlook client by tunneling Outlook's MAPI protocol over an HTTP connection.
Microsoft Exchange ActiveSync (AS) client synchronizes data between mobile devices and Exchange 2010. E-mail, contacts, calendar information, and tasks can be synchronized over an HTTP connection.
Since OA and AS services are connecting to Exchange servers over secured SSL (443) tunneling to an HTTP (80) connection which is the same way Outlook Web App (OWA) does, if Client Access Server (CAS) was set up as a multi-mode service including OWA, OA and AS, then there won't be any necessary service configuration for OA and AS. If OA and AS are serviced in a separated server from OWA, the configuration steps will be the same as OWA in previous chapter 5.

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**:

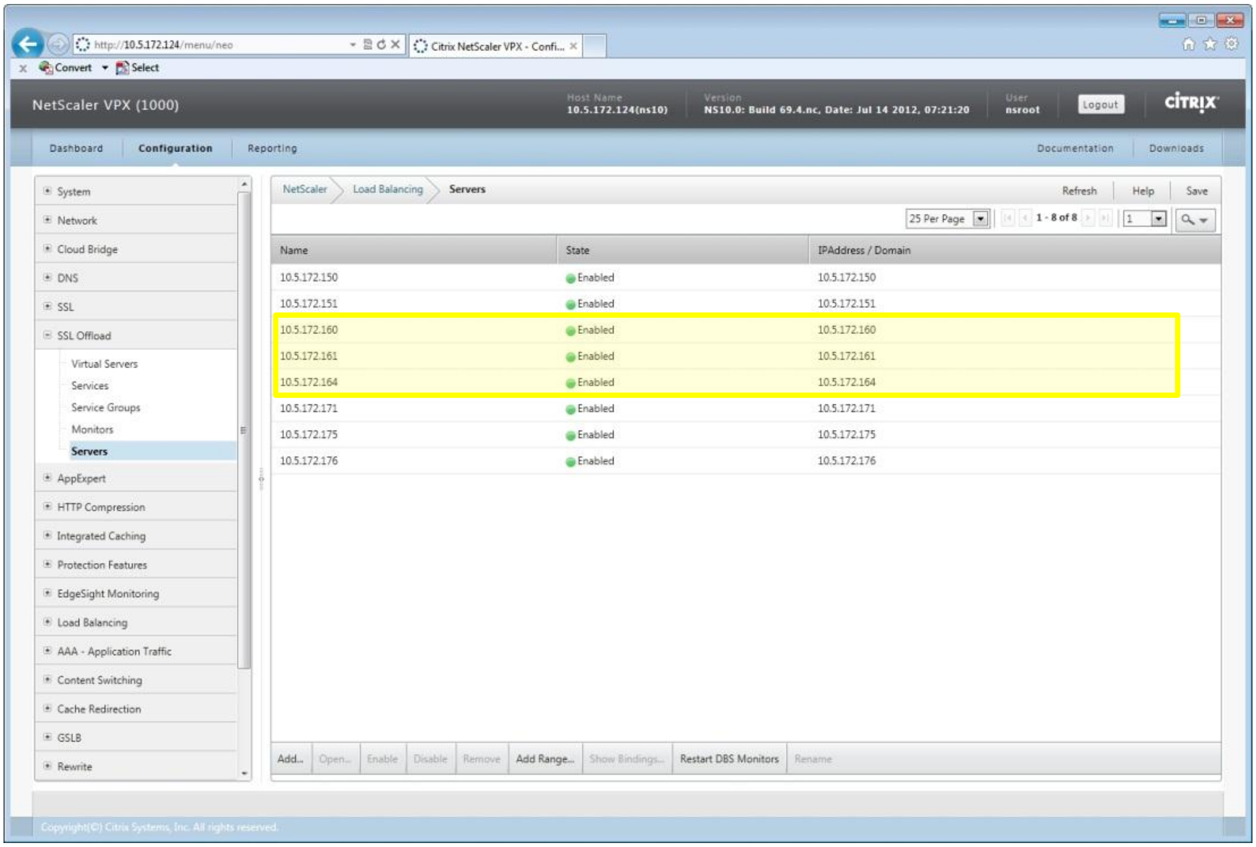


Host Name: 10.5.172.124(ns10)
Version: NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User: nsroot

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
10.5.172.165	● Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED
10.5.172.166	● Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED
10.5.172.177	● Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED
10.5.172.170	● 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**:



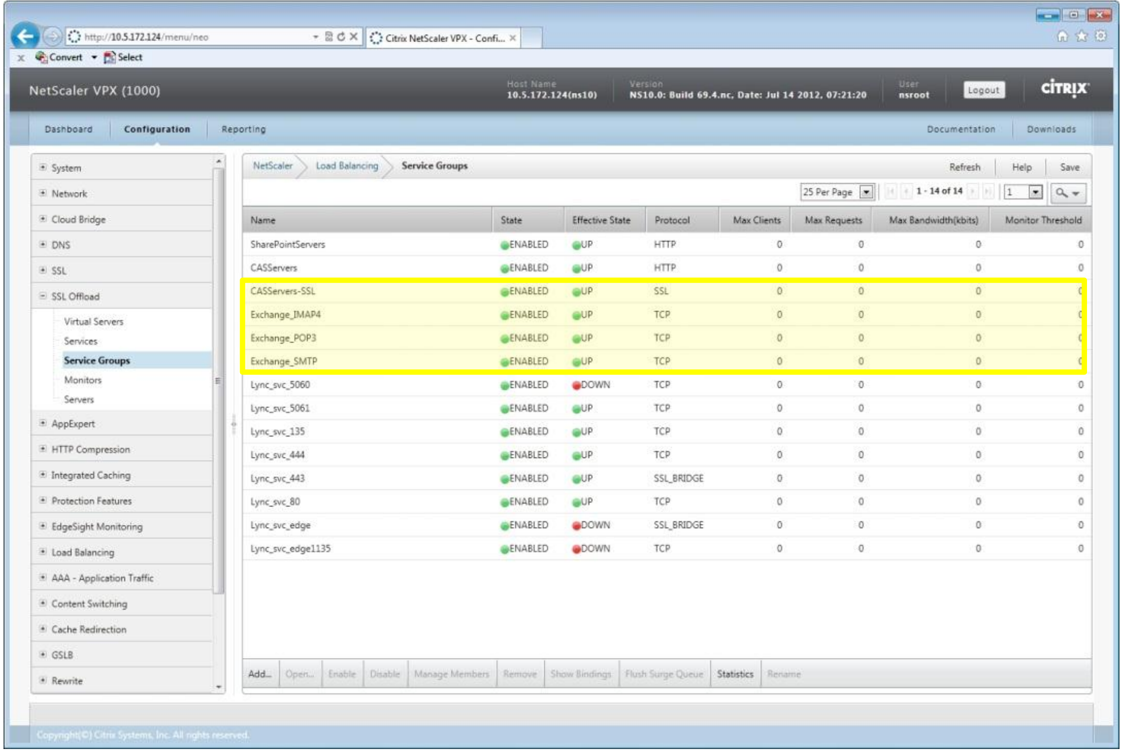
Host Name: 10.5.172.124(ns10)

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

User: nsroot

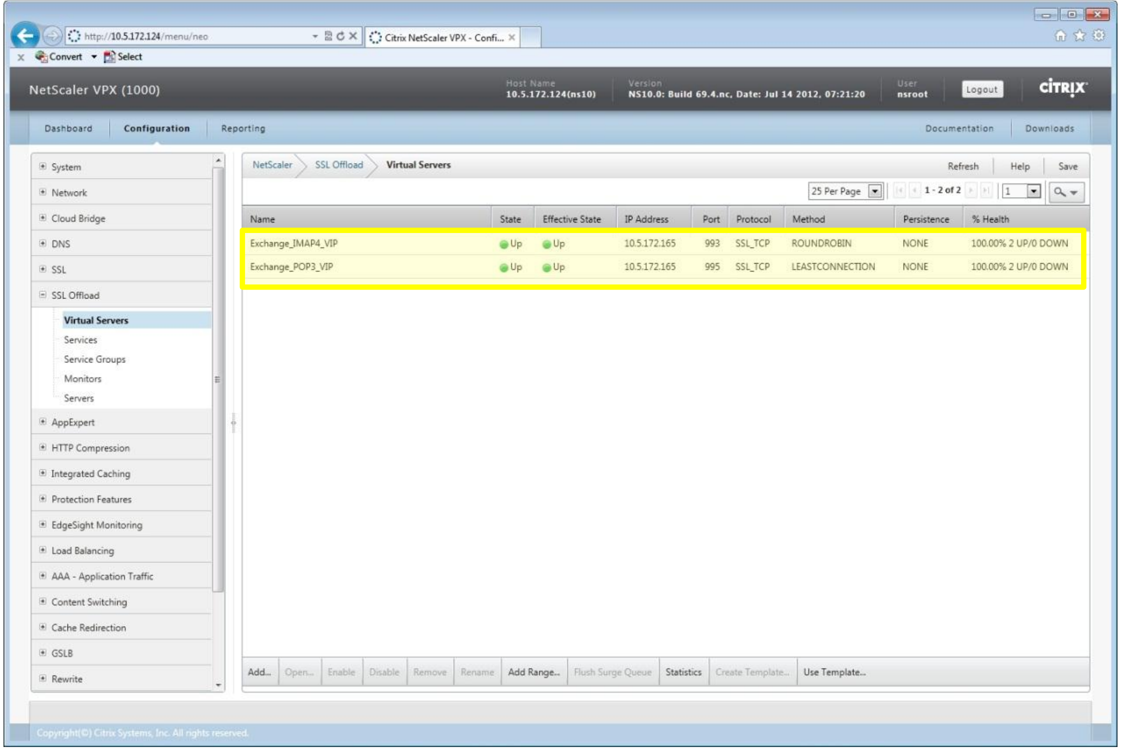
Name	State	IPAddress / Domain
10.5.172.150	● Enabled	10.5.172.150
10.5.172.151	● Enabled	10.5.172.151
10.5.172.160	● Enabled	10.5.172.160
10.5.172.161	● Enabled	10.5.172.161
10.5.172.164	● Enabled	10.5.172.164
10.5.172.171	● Enabled	10.5.172.171
10.5.172.175	● Enabled	10.5.172.175
10.5.172.176	● Enabled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

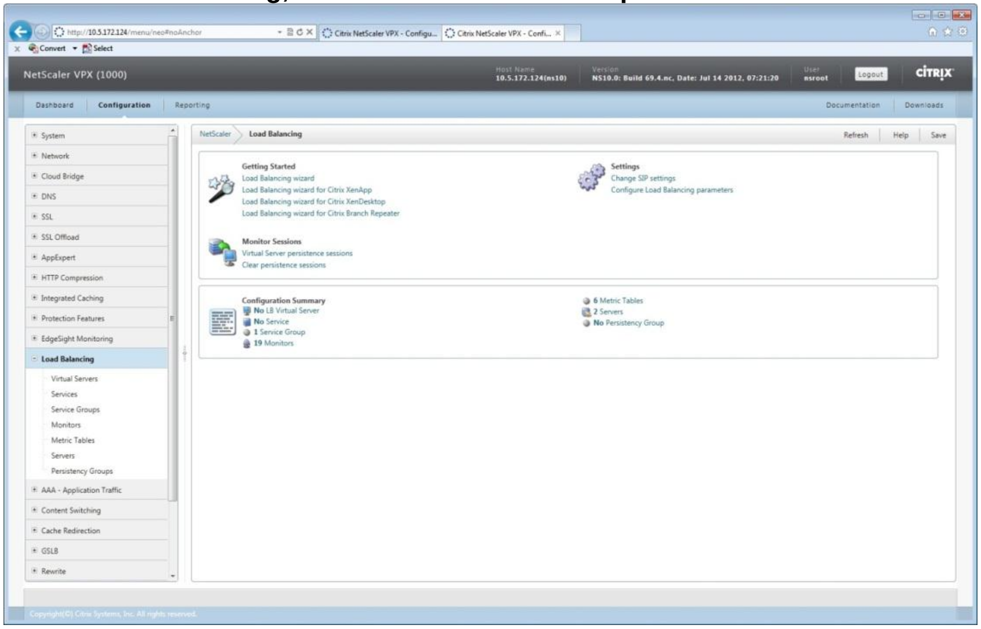
Under **SSL Offload**, *public endpoints* which were created can be found under **Virtual Servers**:



Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
Exchange_IMAP4_VIP	Up	Up	10.5.172.165	993	SSL_TCP	ROUNDROBIN	NONE	100.00% 2 UP/0 DOWN
Exchange_POP3_VIP	Up	Up	10.5.172.165	995	SSL_TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN

6.3 Load Balancing – Servers, Service Group

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



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

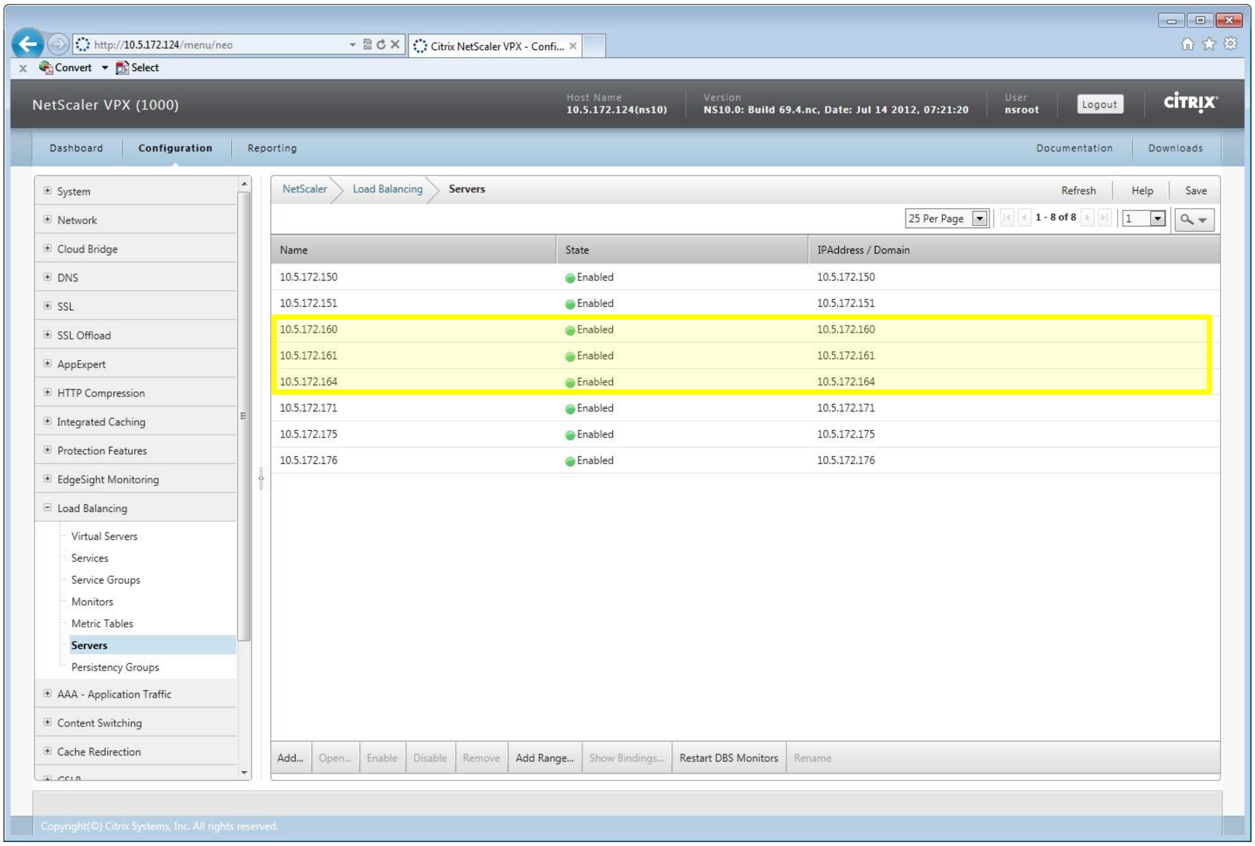
NetScaler > Load Balancing

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

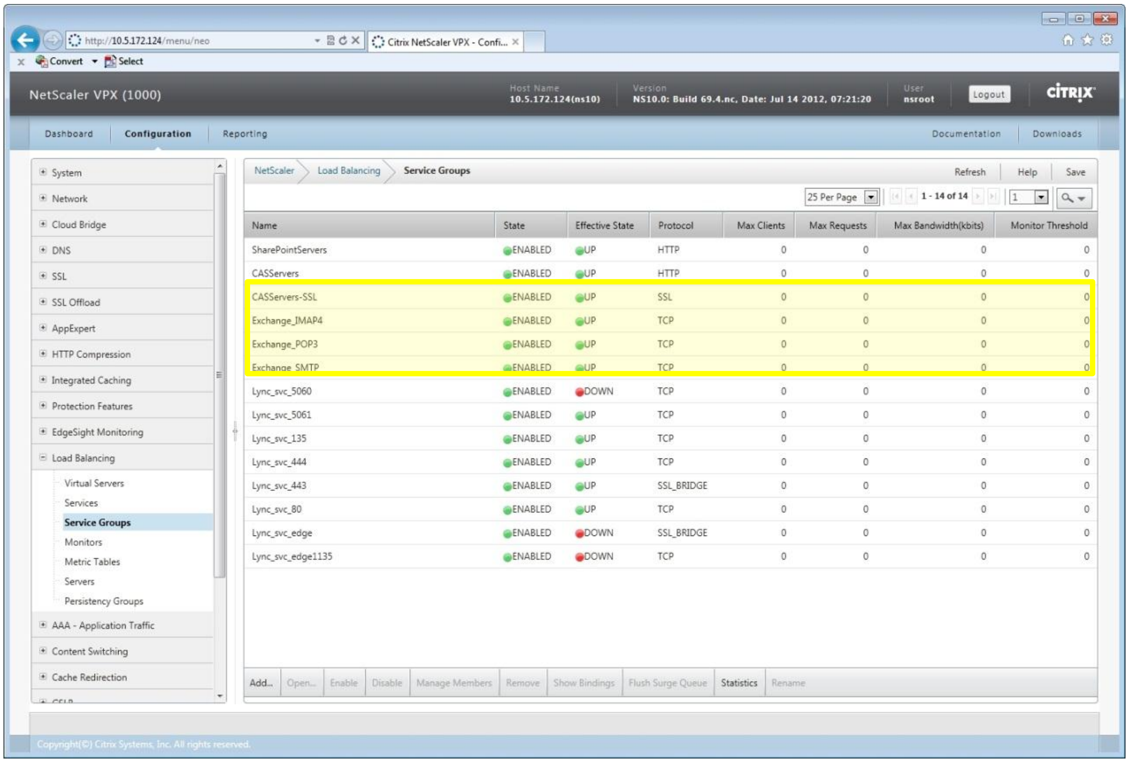
Settings
Change SIP settings
Configure Load Balancing parameters

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



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

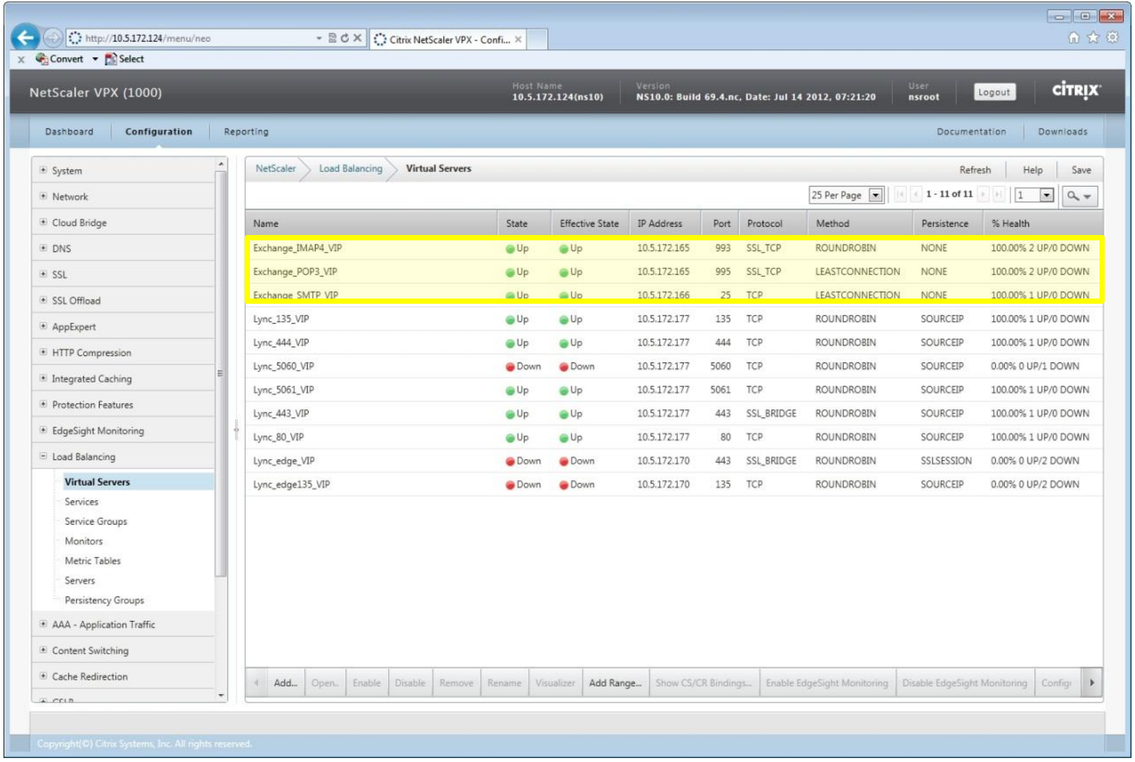


Host Name 10.5.172.124(ns10)
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20
User nsroot

NetScaler > Load Balancing > 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

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



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

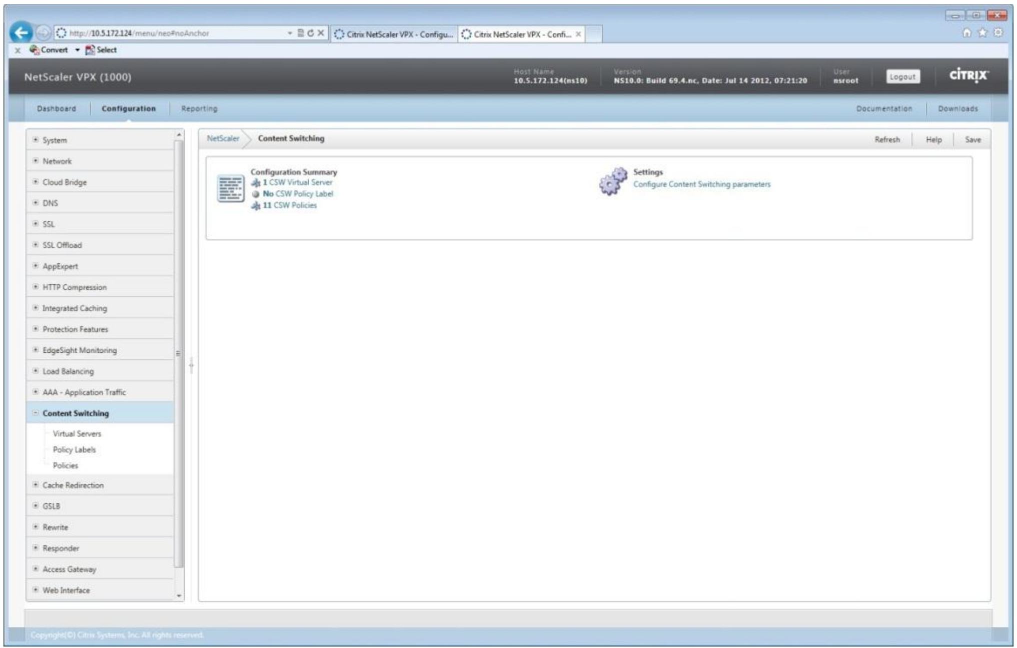
NetScaler > Load Balancing > Virtual Servers

Name	State	Effective State	IP Address	Port	Protocol	Method	Persistence	% Health
Exchange_IMAP4_VIP	● Up	● Up	10.5.172.165	993	SSL_TCP	ROUNDROBIN	NONE	100.00% 2 UP/0 DOWN
Exchange_POP3_VIP	● Up	● Up	10.5.172.165	995	SSL_TCP	LEASTCONNECTION	NONE	100.00% 2 UP/0 DOWN
Exchange_SMTP_VIP	● Up	● Up	10.5.172.166	25	TCP	LEASTCONNECTION	NONE	100.00% 1 UP/0 DOWN
Lync_135_VIP	● Up	● Up	10.5.172.177	135	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_444_VIP	● Up	● Up	10.5.172.177	444	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_5060_VIP	● Down	● Down	10.5.172.177	5060	TCP	ROUNDROBIN	SOURCEIP	0.00% 0 UP/1 DOWN
Lync_5061_VIP	● Up	● Up	10.5.172.177	5061	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_443_VIP	● Up	● Up	10.5.172.177	443	SSL_BRIDGE	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_80_VIP	● Up	● Up	10.5.172.177	80	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_edge_VIP	● Down	● Down	10.5.172.170	443	SSL_BRIDGE	ROUNDROBIN	SSLSESSION	0.00% 0 UP/2 DOWN
Lync_edge135_VIP	● Down	● Down	10.5.172.170	135	TCP	ROUNDROBIN	SOURCEIP	0.00% 0 UP/2 DOWN

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

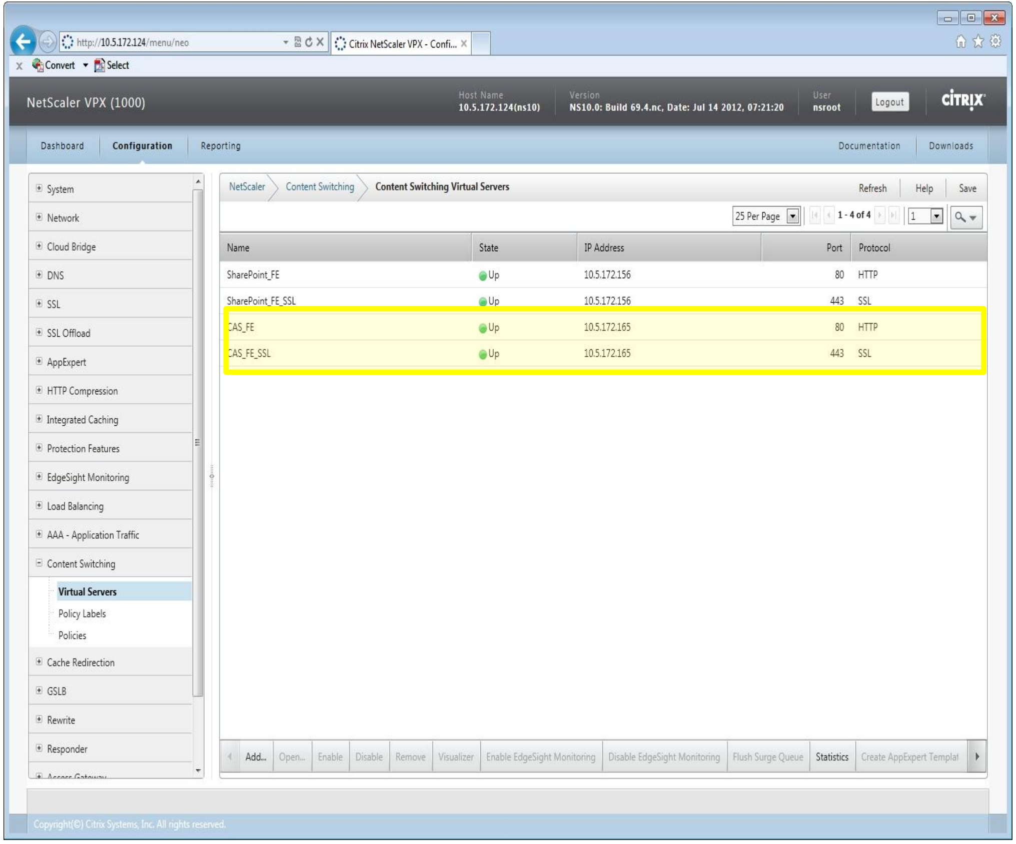
6.4 Content Switching

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



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

Settings
Configure Content Switching parameters



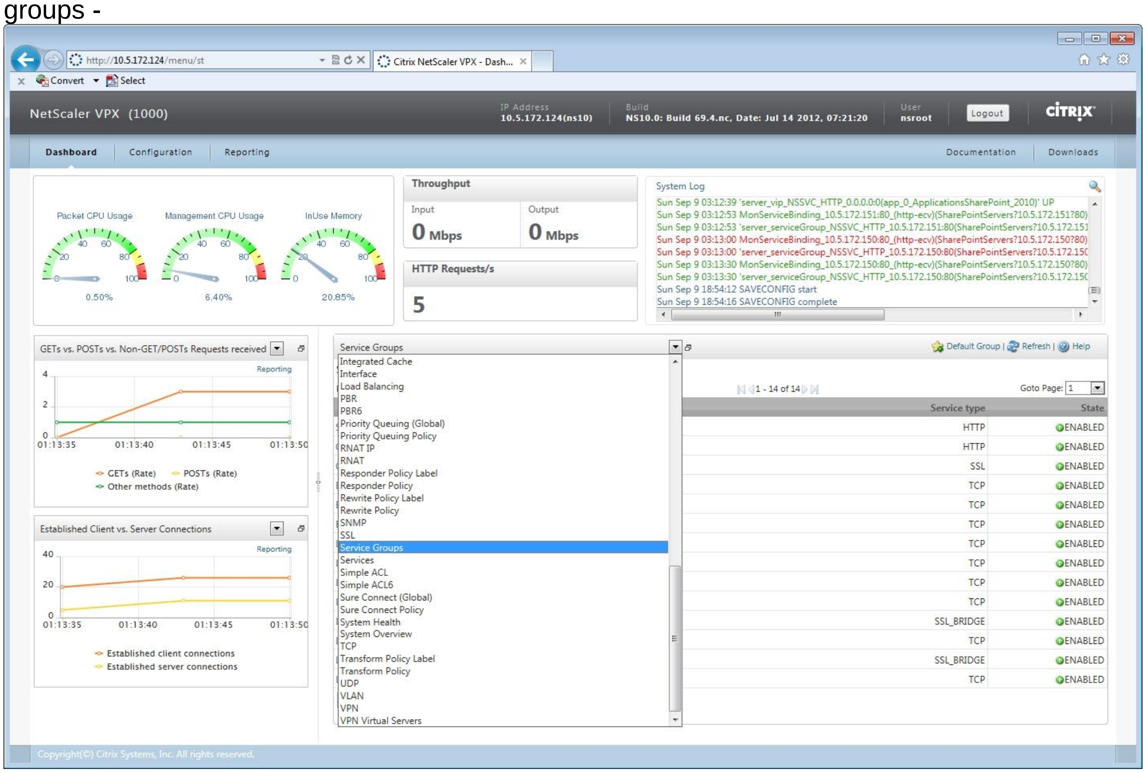
Name	State	IP Address	Port	Protocol
SharePoint_FE	Up	10.5.172.156	80	HTTP
SharePoint_FE_SSL	Up	10.5.172.156	443	SSL
CAS_FE	Up	10.5.172.165	80	HTTP
CAS_FE_SSL	Up	10.5.172.165	443	SSL

7. Monitoring – NetScaler Dashboard

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

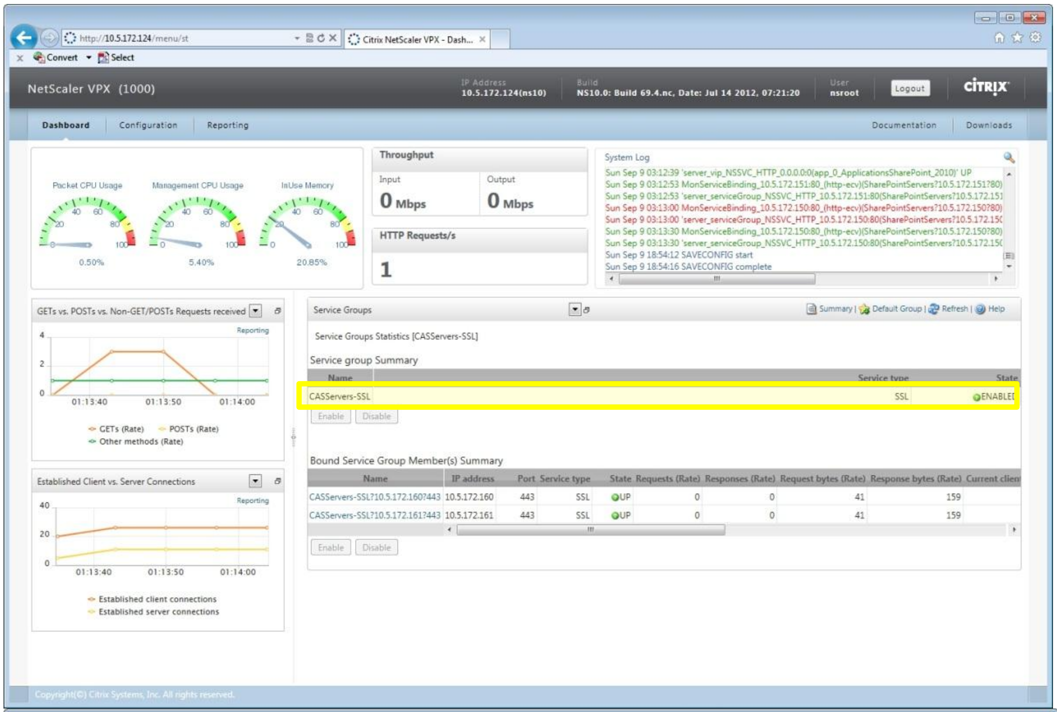
7.1 By Service Groups

Under **CASServers-SSL** , **Exchange_IMAP4**, **Exchange_POP3**, and **Exchange_SMTP** service groups -



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?80)
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.15(
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.15(
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

Service type	State
HTTP	ENABLED
HTTP	ENABLED
SSL	ENABLED
TCP	ENABLED
TCP	ENABLED
TCP	ENABLED
TCP	ENABLED
TCP	ENABLED
TCP	ENABLED
TCP	ENABLED
SSL_BRIDGE	ENABLED
TCP	ENABLED
SSL_BRIDGE	ENABLED
TCP	ENABLED


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Dash...
Convert
Select
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
Management CPU Usage
InUse Memory
0
20
40
60
80
100
0.50%
5.40%
20.85%
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
4
2
0
01:13:40
01:13:50
01:14:00
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
01:13:40
01:13:50
01:14:00
Established client connections
Established server connections
Summary | Default Group | Refresh | Help
Enable
Disable
Copyright(©) Citrix Systems, Inc. All rights reserved.

NetScaler VPX (1000)

IP Address 10.5.172.124(ns10)

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

User nsroot

Throughput

Input 0 Mbps

Output 0 Mbps

HTTP Requests/s 1

System Log

```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?80)
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.150
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.150
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

Service Groups

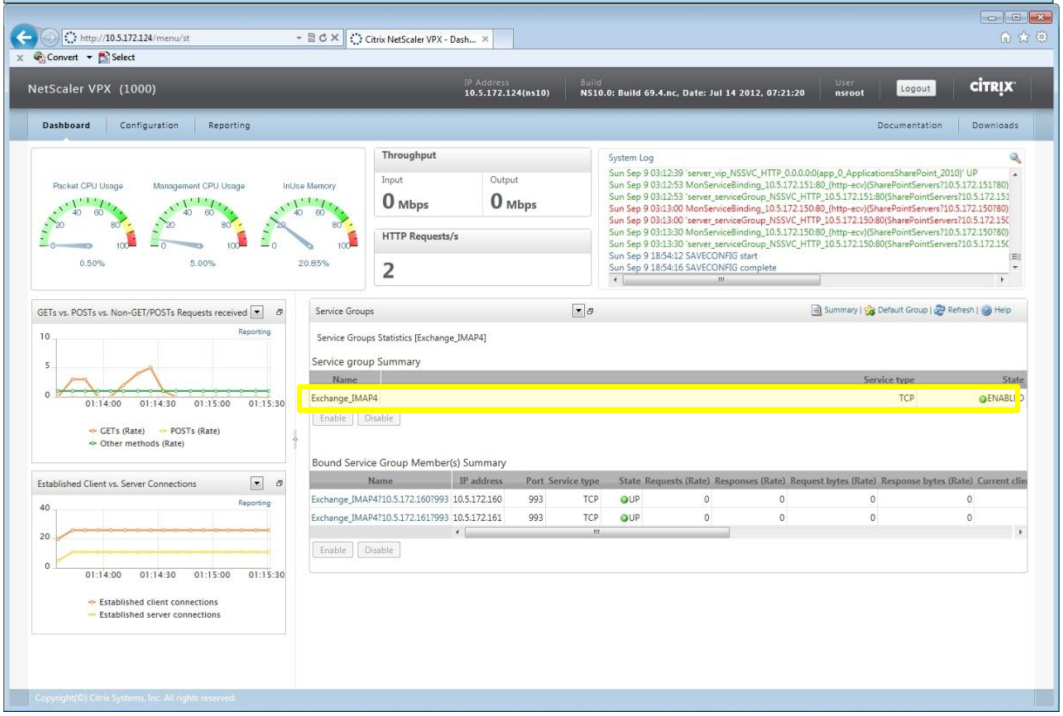
Service Groups Statistics [CASServers-SSL]

Service group Summary

Name	Service type	State
CASServers-SSL	SSL	● 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 clien
CASServers-SSL?10.5.172.160?443	10.5.172.160	443	SSL	● UP	0	0	41	159	
CASServers-SSL?10.5.172.161?443	10.5.172.161	443	SSL	● UP	0	0	41	159	


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Dash...
Convert
Select
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
Management CPU Usage
InUse Memory
0
20
40
60
80
100
0.50%
5.00%
20.85%
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
10
5
0
01:14:00
01:14:30
01:15:00
01:15:30
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
01:14:00
01:14:30
01:15:00
01:15:30
Established client connections
Established server connections
Summary | Default Group | Refresh | Help
Enable
Disable
Copyright(©) Citrix Systems, Inc. All rights reserved.

NetScaler VPX (1000)

IP Address 10.5.172.124(ns10)

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

User nsroot

Throughput

Input 0 Mbps

Output 0 Mbps

HTTP Requests/s 2

System Log

```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?80)
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.150
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.150
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

Service Groups

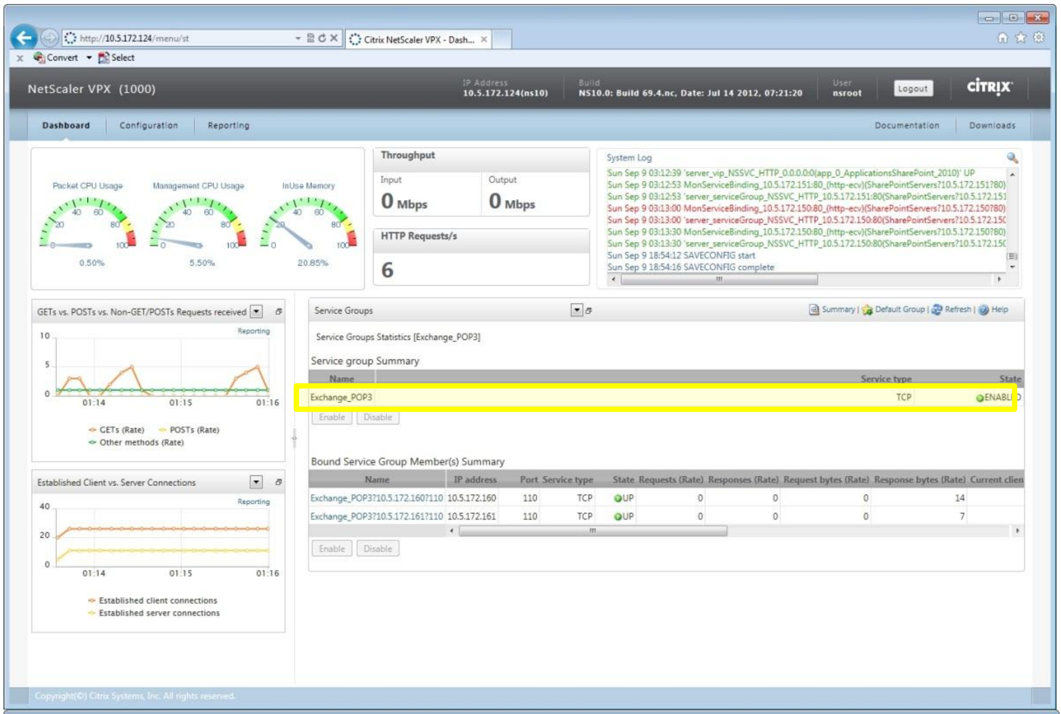
Service Groups Statistics [Exchange_IMAP4]

Service group Summary

Name	Service type	State
Exchange_IMAP4	TCP	● 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 clie
Exchange_IMAP4?10.5.172.160?993	10.5.172.160	993	TCP	● UP	0	0	0	0	
Exchange_IMAP4?10.5.172.161?993	10.5.172.161	993	TCP	● UP	0	0	0	0	



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?80)
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.15(
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.15(
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

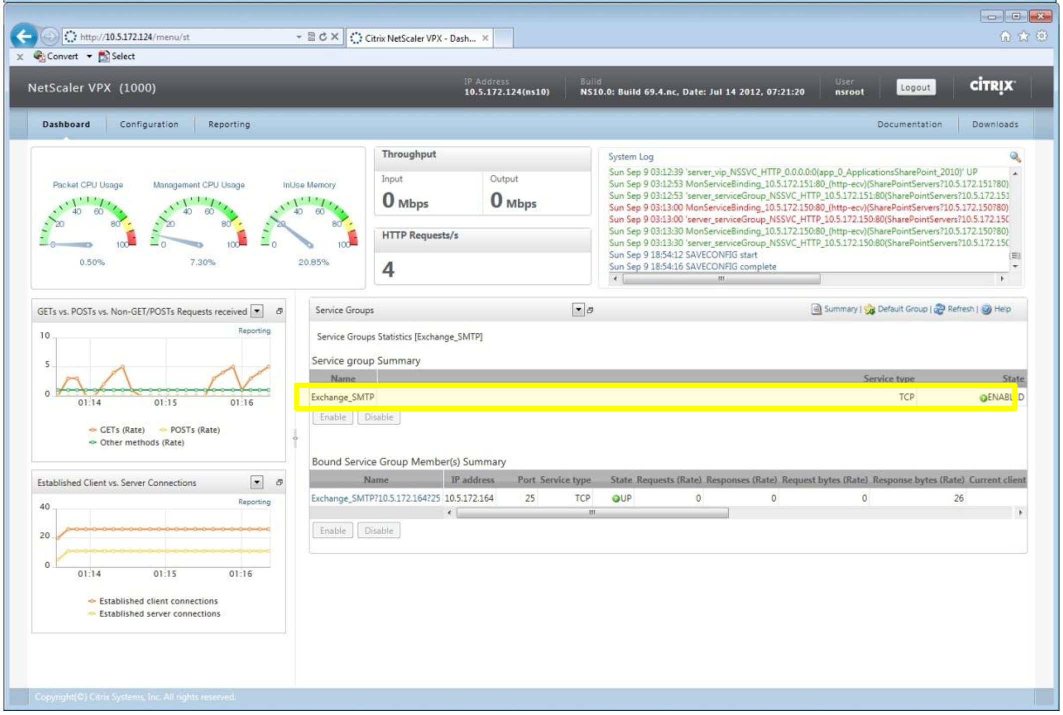
Service Groups Statistics [Exchange_POP3]

Service group Summary

Name	Service type	State
Exchange_POP3	TCP	● 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 clien
Exchange_POP3?10.5.172.160?110	10.5.172.160	110	TCP	● UP	0	0	0	14	
Exchange_POP3?10.5.172.161?110	10.5.172.161	110	TCP	● UP	0	0	0	7	



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?80)
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.151
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.15(
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?80)
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.15(
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

Service Groups Statistics [Exchange_SMTP]

Service group Summary

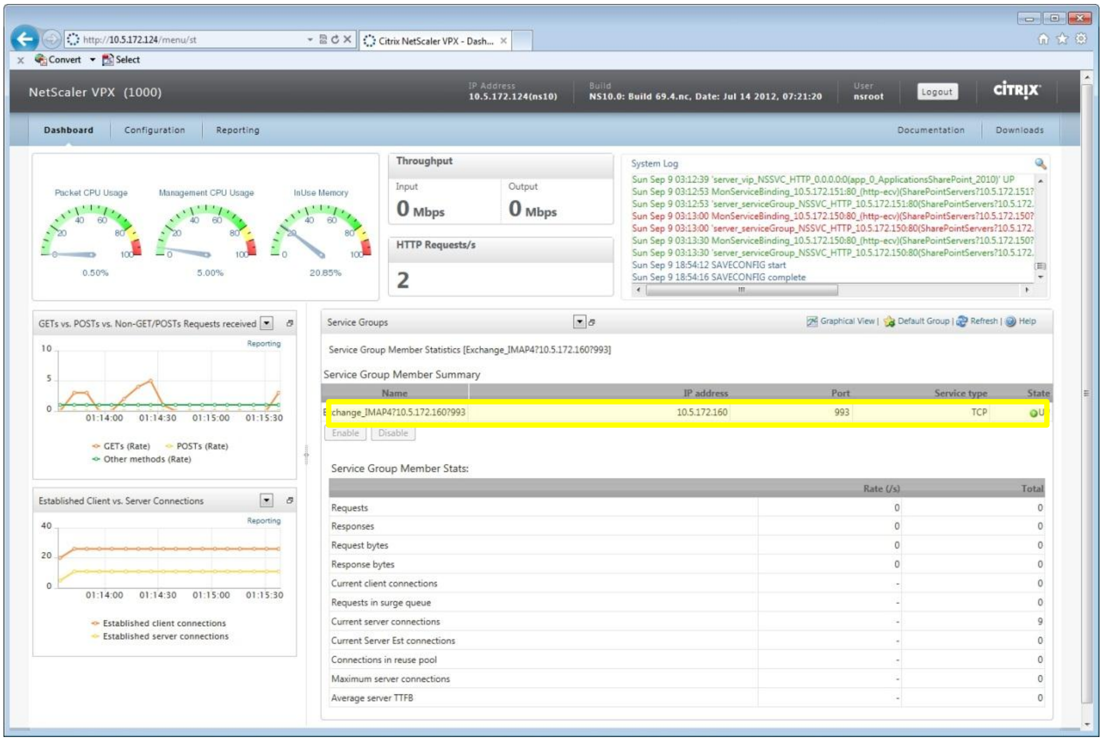
Name	Service type	State
Exchange_SMTP	TCP	● ENABLED

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
Exchange_SMTP?10.5.172.164?25	10.5.172.164	25	TCP	● UP	0	0	0	26	

7.2 Per Server

Under **Service Group Member Summary**, service details including # of Requests, Reponses can be found:



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

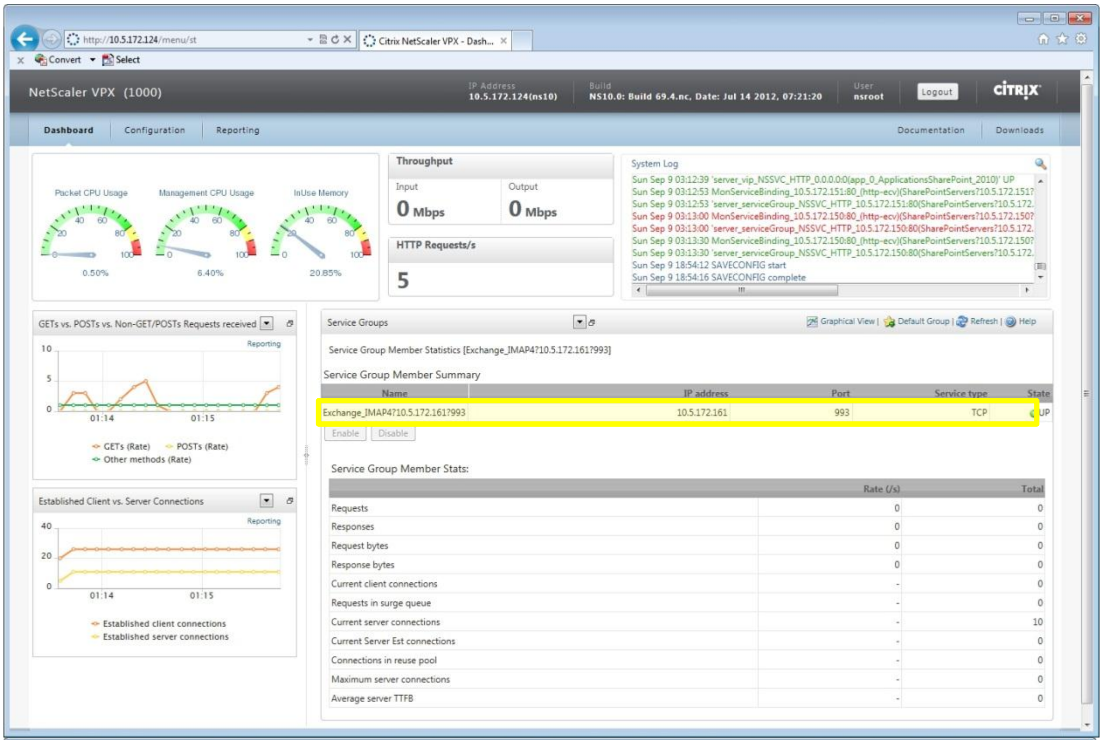
Service Group Member Statistics [Exchange_IMAP4?10.5.172.160?993]

Service Group Member Summary

Name	IP address	Port	Service type	State
Exchange_IMAP4?10.5.172.160?993	10.5.172.160	993	TCP	● U

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	0
Responses	0	0
Request bytes	0	0
Response bytes	0	0
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	9
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

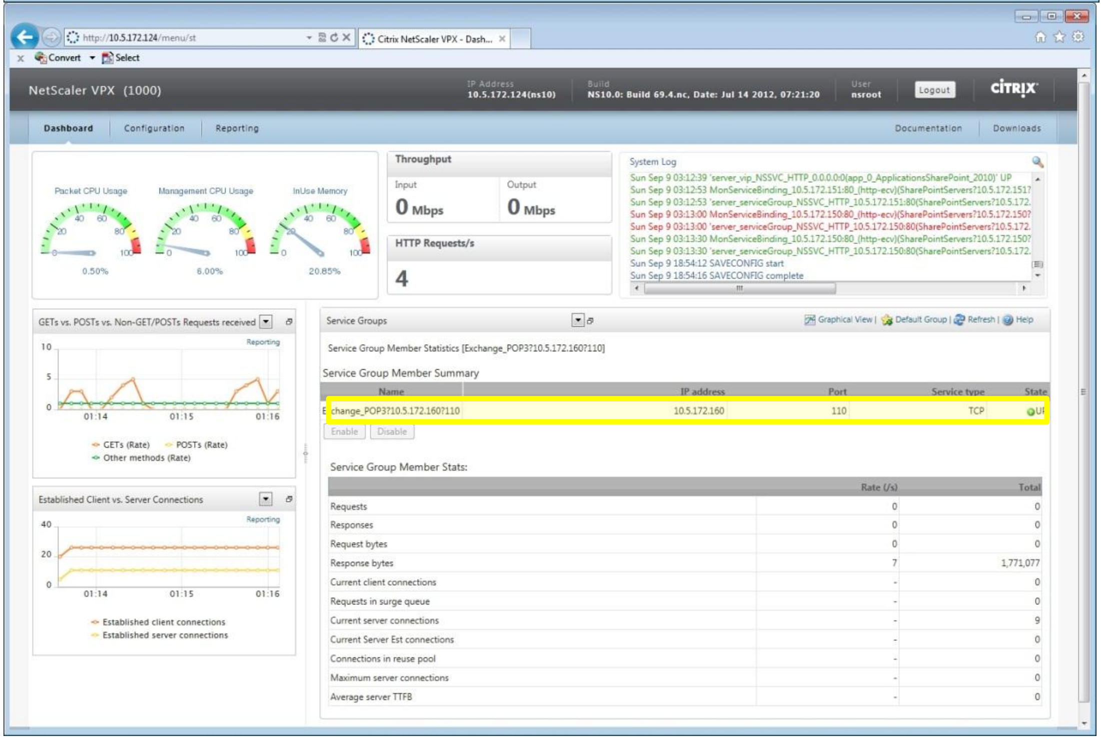
Service Group Member Statistics [Exchange_IMAP4?10.5.172.161?993]

Service Group Member Summary

Name	IP address	Port	Service type	State
Exchange_IMAP4?10.5.172.161?993	10.5.172.161	993	TCP	● UP

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	0
Responses	0	0
Request bytes	0	0
Response bytes	0	0
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	10
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

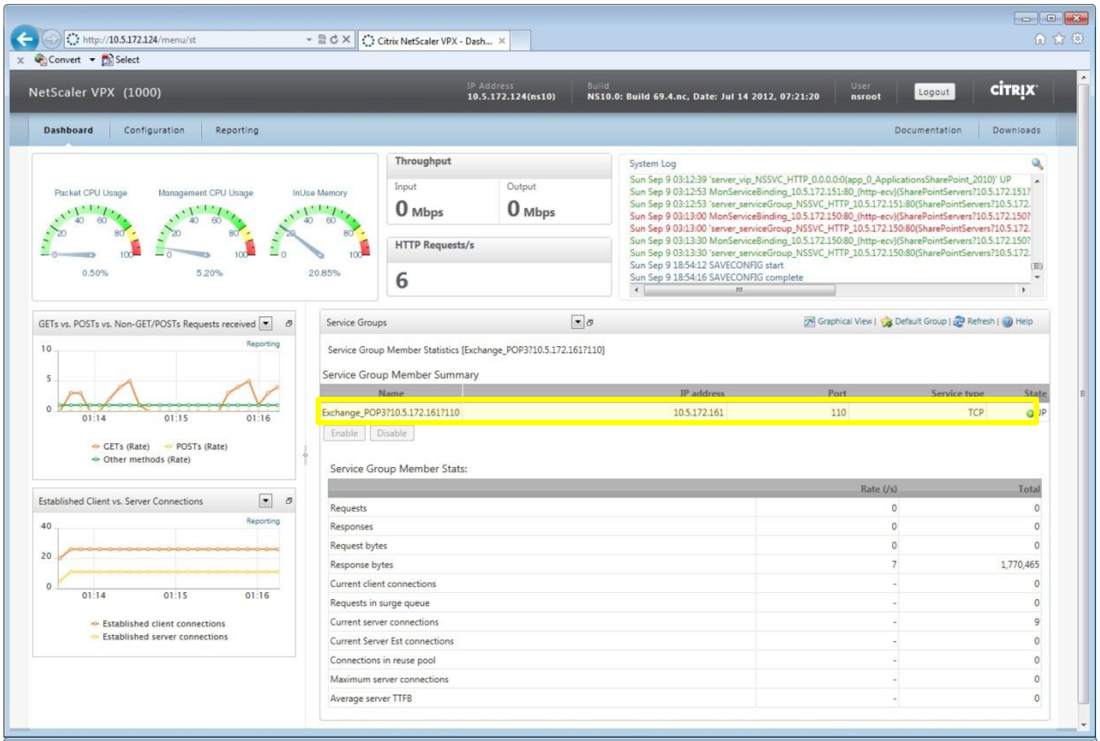
Service Group Member Statistics [Exchange_POP3?10.5.172.160?110]

Service Group Member Summary

Name	IP address	Port	Service type	State
E change_POP3?10.5.172.160?110	10.5.172.160	110	TCP	● UI

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	0
Responses	0	0
Request bytes	0	0
Response bytes	7	1,771,077
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	9
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

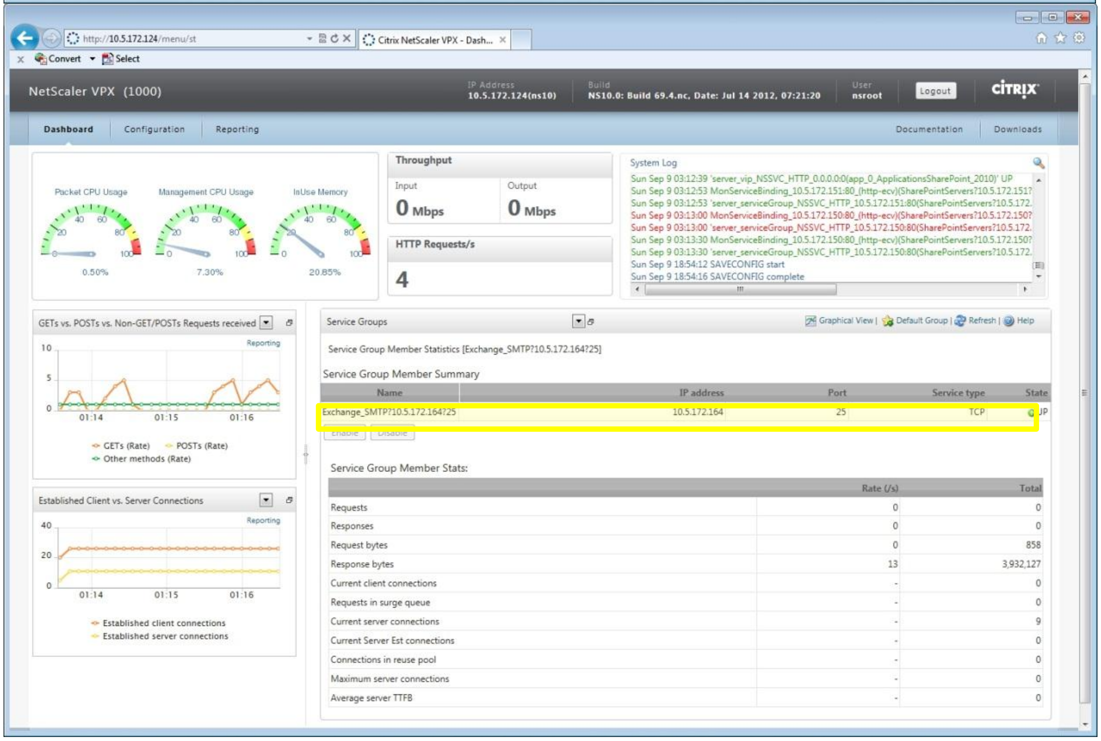
Service Group Member Statistics [Exchange_POP3?10.5.172.161?110]

Service Group Member Summary

Name	IP address	Port	Service type	State
Exchange_POP3?10.5.172.161?110	10.5.172.161	110	TCP	● UP

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	0
Responses	0	0
Request bytes	0	0
Response bytes	7	1,770,465
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	9
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0



```
Sun Sep 9 03:12:39 'server_vip_NSSVC_HTTP_0.0.0.0:0(app_0_ApplicationsSharePoint_2010)' UP
Sun Sep 9 03:12:53 MonServiceBinding_10.5.172.151:80_(http-ecv)(SharePointServers?10.5.172.151?
Sun Sep 9 03:12:53 'server_serviceGroup_NSSVC_HTTP_10.5.172.151:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:00 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:00 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 03:13:30 MonServiceBinding_10.5.172.150:80_(http-ecv)(SharePointServers?10.5.172.150?
Sun Sep 9 03:13:30 'server_serviceGroup_NSSVC_HTTP_10.5.172.150:80(SharePointServers?10.5.172.
Sun Sep 9 18:54:12 SAVECONFIG start
Sun Sep 9 18:54:16 SAVECONFIG complete
```

Service Group Member Statistics [Exchange_SMTP?10.5.172.164?25]

Service Group Member Summary

Name	IP address	Port	Service type	State
Exchange_SMTP?10.5.172.164?25	10.5.172.164	25	TCP	● UP

Service Group Member Stats:

	Rate (/s)	Total
Requests	0	0
Responses	0	0
Request bytes	0	858
Response bytes	13	3,932,127
Current client connections	-	0
Requests in surge queue	-	0
Current server connections	-	9
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0

8. Palo Alto Networks Next-Generation Firewall Deployment

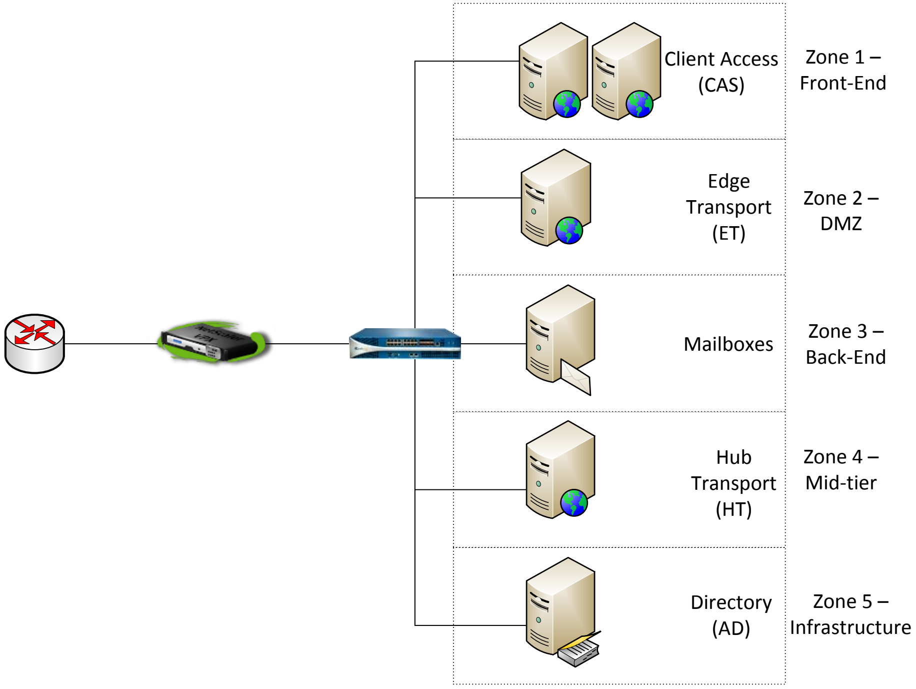
The Palo Alto Networks next-generation firewall safely enables enterprise applications in the data center and delivers meaningful segmentation by application, user and content. It identifies all traffic sent to the Microsoft Exchange servers, based on actual application, not just port or protocol. Access to the Microsoft Exchange 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 an Exchange data center implementation, there will be several different roles performed by the servers. In smaller implementations, some of these roles can be combined in a single server. For large Exchange installations, the different server roles will be deployed on dedicated physical or virtual servers.

In order to properly segment and secure a large Exchange 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 will be segments for the Exchange Client Access Servers, Edge Transport Servers, Hub Transport Servers, and Mailbox Servers. Users and administrators accessing the Exchange servers will come from the External zone, and there will be an infrastructure segment in which the Active Directory Domain Controllers reside.

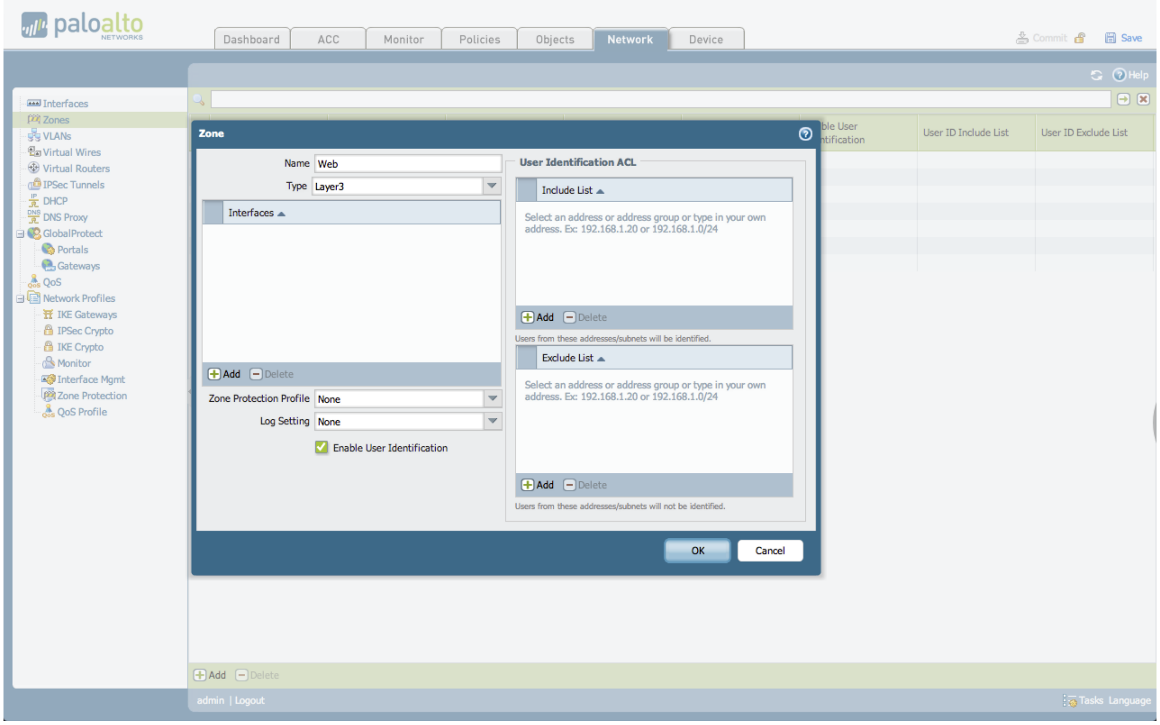


To build these segments in the Palo Alto Networks firewall, the following zones will be created:

Web – Exchange Client Access Servers
DMZ – Edge Transport Servers

Application – Hub Transport Servers
Database – Mailbox 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.



Name: Web
Type: Layer3
Zone Protection Profile: None
Log Setting: None
☑ Enable User Identification

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

The Palo Alto Networks next-generation firewall 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 Exchange, while restricting non-Exchange traffic.

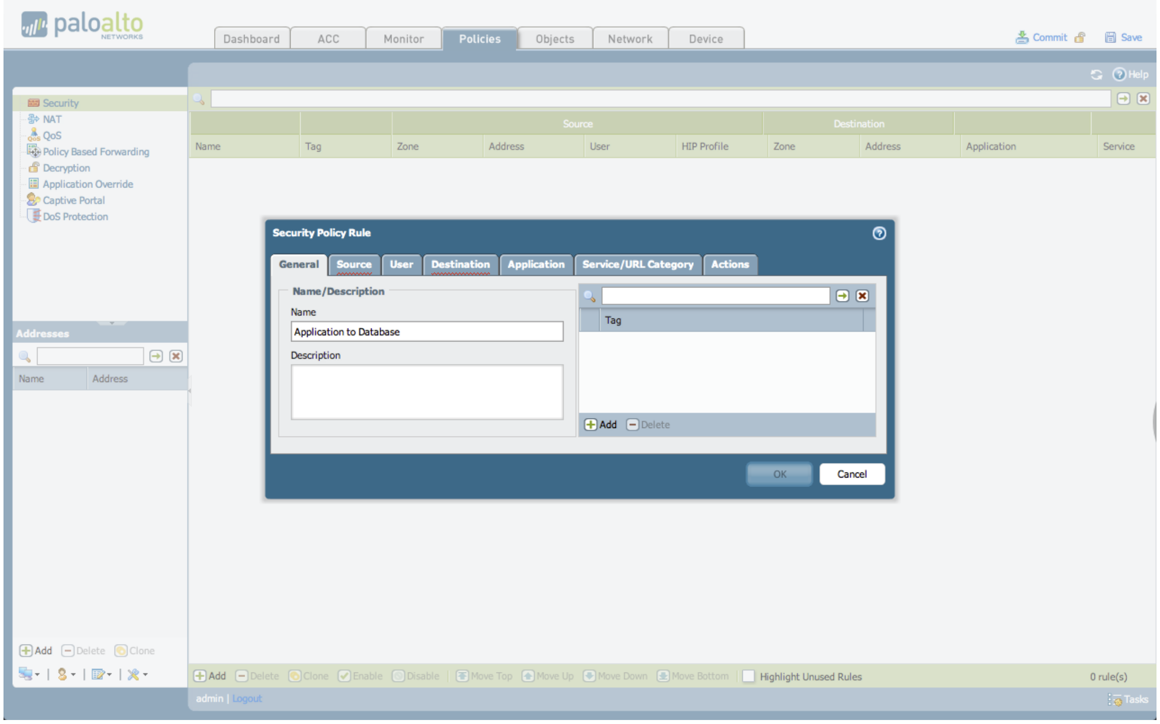
Every Exchange implementation is different, and depending on the features and services enabled, the specific applications between zones, as well as the required zones, may vary. This will serve as a starting reference for a working Exchange security policy.

Source Zone	Destination Zone	Application
Active-Directory	DMZ	netbios-ns

Active-Directory	External	dns
Active-Directory	Web	ms-ds-smb msrpc netbios-dg netbios-ns netbios-ss
Application	Active-Directory	dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc
Application	Database	ms-ds-smb msrpc netbios-dg netbios-ss
Application	External	dns kerberos rpc
Database	Active-Directory	active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc
Database	Application	ms-ds-smb msrpc netbios-dg netbios-ss
Database	External	web-browsing
DMZ	Active-Directory	dns ldap ms-ds-smb netbios-dg netbios-ss
DMZ	External	web-browsing
External	Active-Directory	active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc
External	Application	smtp

External	Web	imap ms-ds-smb ms-exchange msrpc netbios-dg netbios-ss outlook-web pop3 rpc-over-http ssl web-browsing
Web	Active-Directory	active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc
Web	Application	ms-ds-smb msrpc netbios-dg netbios-ss
Web	Database	ms-ds-smb msrpc ms-exchange netbios-dg netbios-ss rpc-over-http ssl web-browsing
Web	External	active-directory dns kerberos ldap ms-ds-smb ms-netlogon msrpc netbios-dg netbios-ss rpc web-browsing

To create the security policy, each of these source and destination zone pairs will represent one rule in the security policy. For example, to create the “Application to Database” security policy, 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 rule.



Security Policy Rule

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

Name/Description

Name: Application to Database

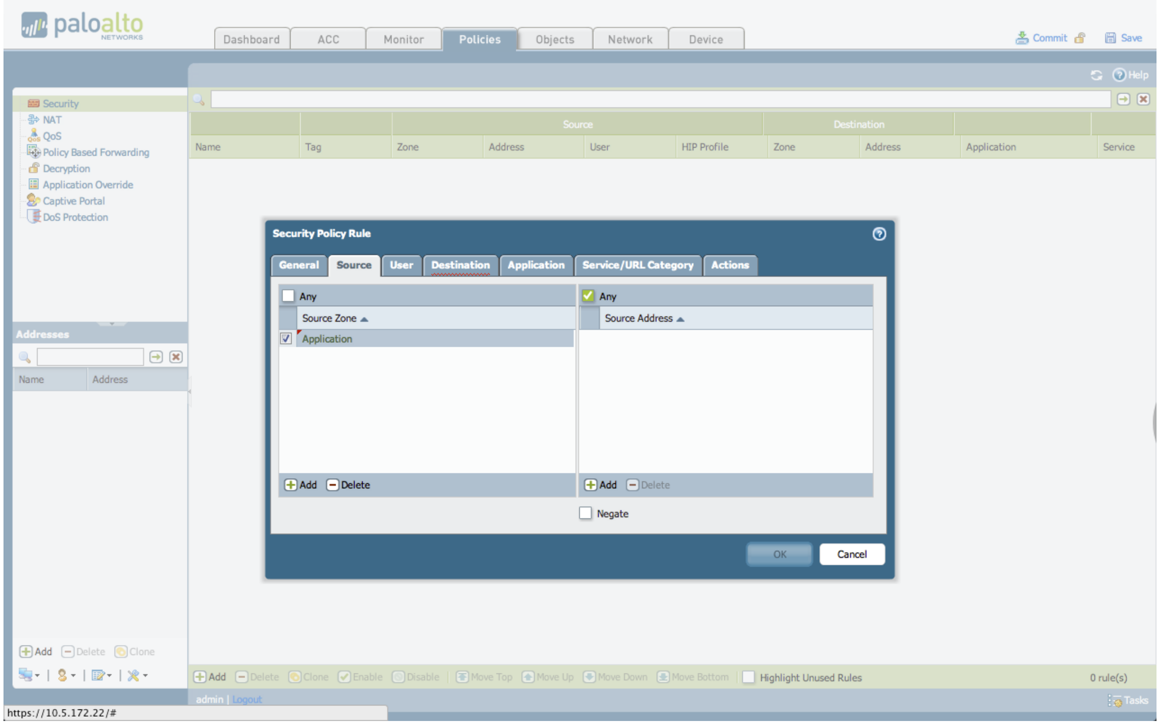
Description:

Tag

Add | Delete

OK | Cancel

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



Security Policy Rule

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

☐ Any

Source Zone

☑ Application

Add | Delete

☑ Any

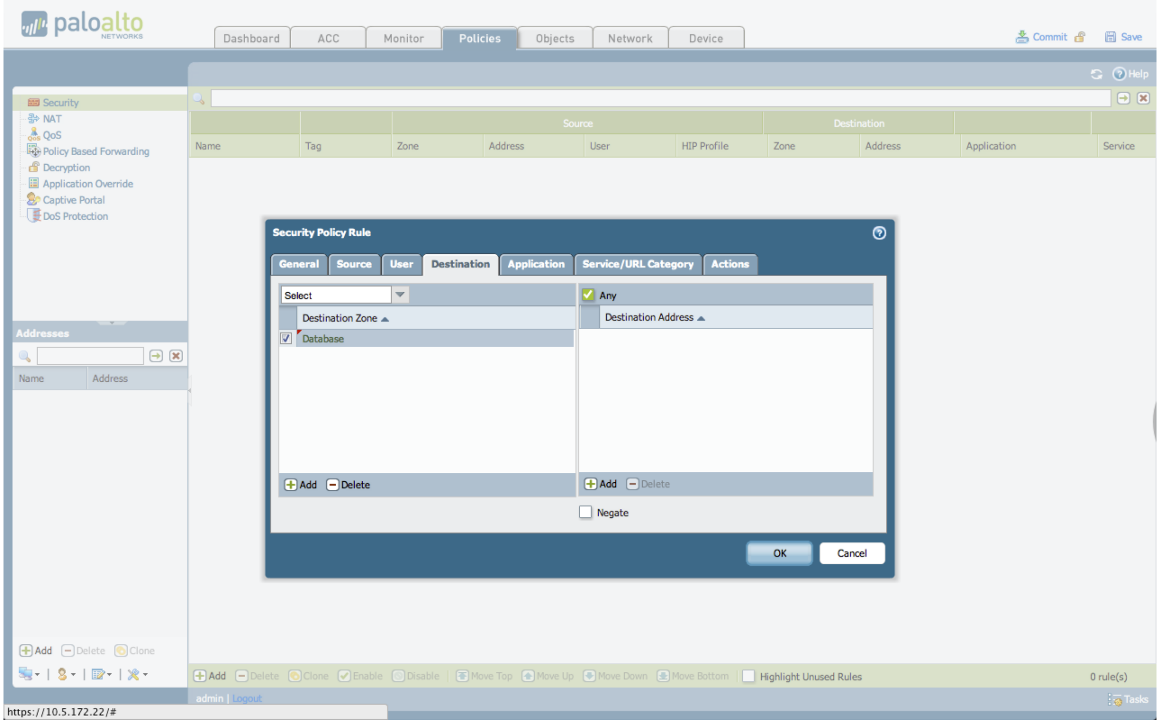
Source Address

Add | Delete

☐ Negate

OK | Cancel

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

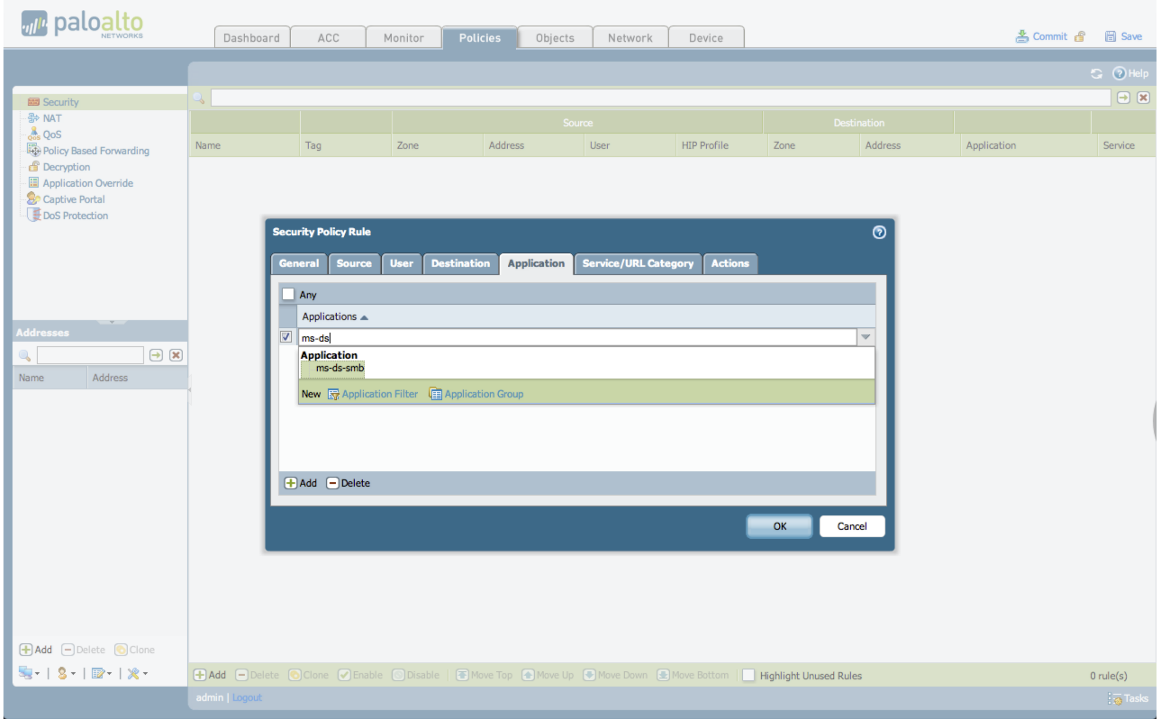
Destination Address ▲

Add Delete

□ Negate

OK Cancel

Click on the Application tab and click Add. Four applications will be added to this rule: ms-ds-smb, msrpc, netbios-dg, and netbios-ss. 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 ▲

☑ ms-ds

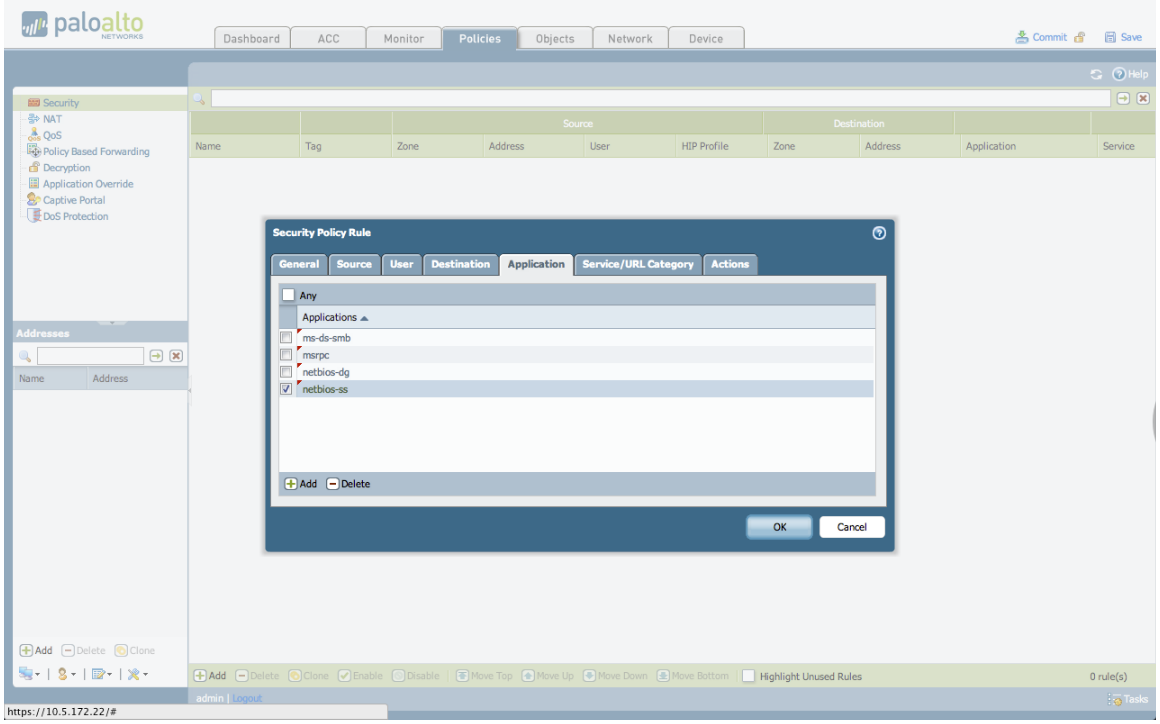
Application
ms-ds-smb

New Application Filter Application Group

Add Delete

OK Cancel

Repeat for the remaining applications in this rule.



Security Policy Rule

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

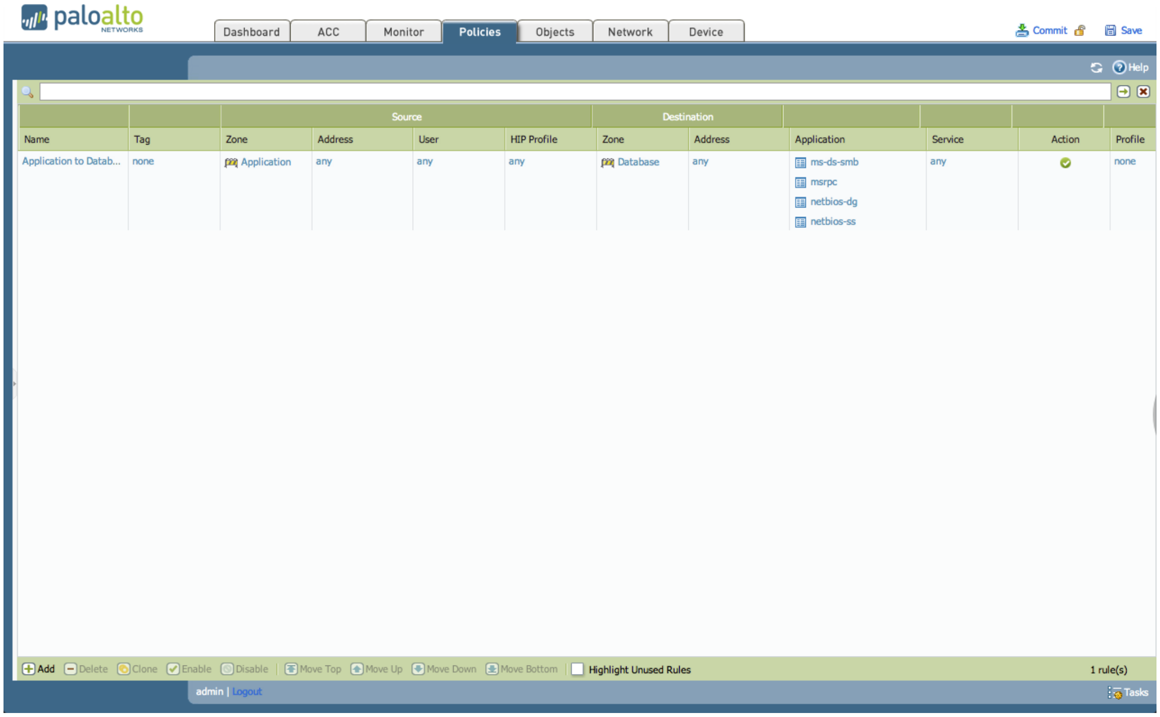
☐ Any

	Applications ▲
☐	ms-ds-smb
☐	msrpc
☐	netbios-dg
☑	netbios-ss

Add | Delete

OK | Cancel

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.



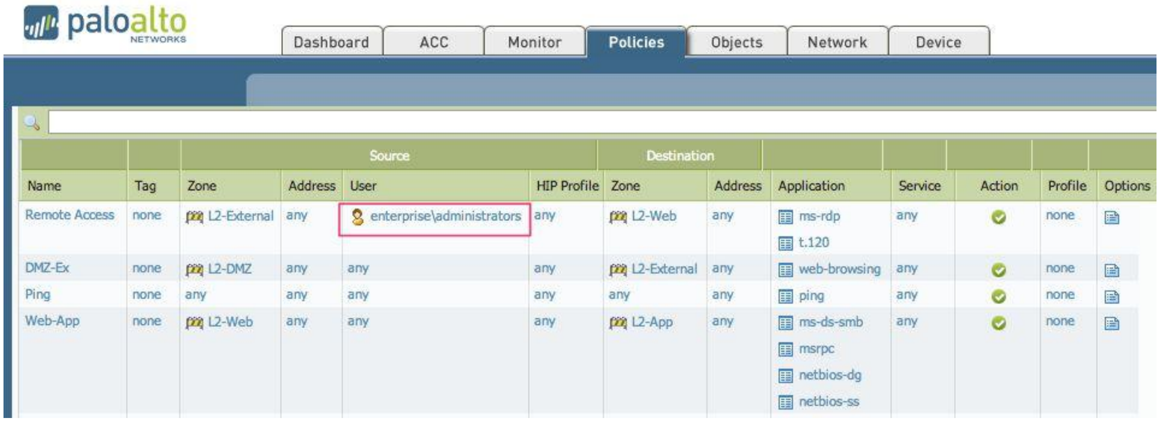
		Source				Destination					
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
Application to Datab...	none	Application	any	any	any	Database	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none

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 Exchange servers may need to be accessible by system administrators with Remote Desktop for management purposes. But, other users do 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. Exchange would be accessible by other users using the client applications.



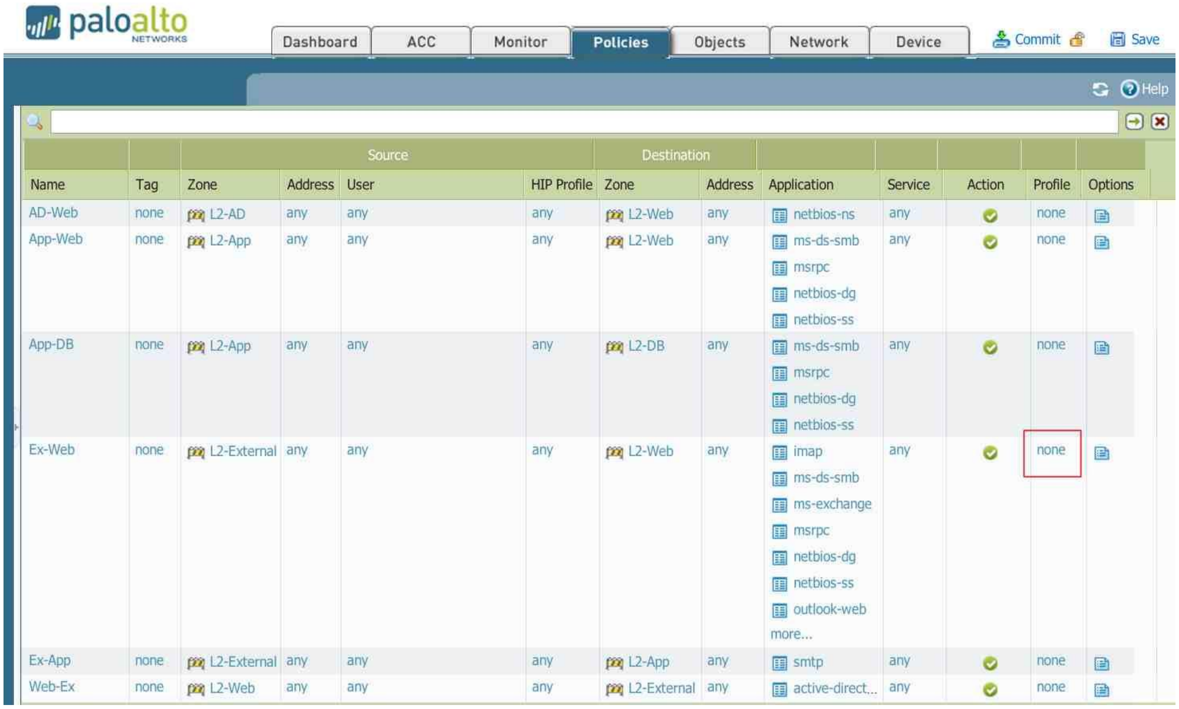
		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Remote Access	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	▤
DMZ-Ex	none	L2-DMZ	any	any	any	L2-External	any	web-browsing	any	✓	none	▤
Ping	none	any	any	any	any	any	any	ping	any	✓	none	▤
Web-App	none	L2-Web	any	any	any	L2-App	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	▤

8.4 Threat Protection

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 known and unknown 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.

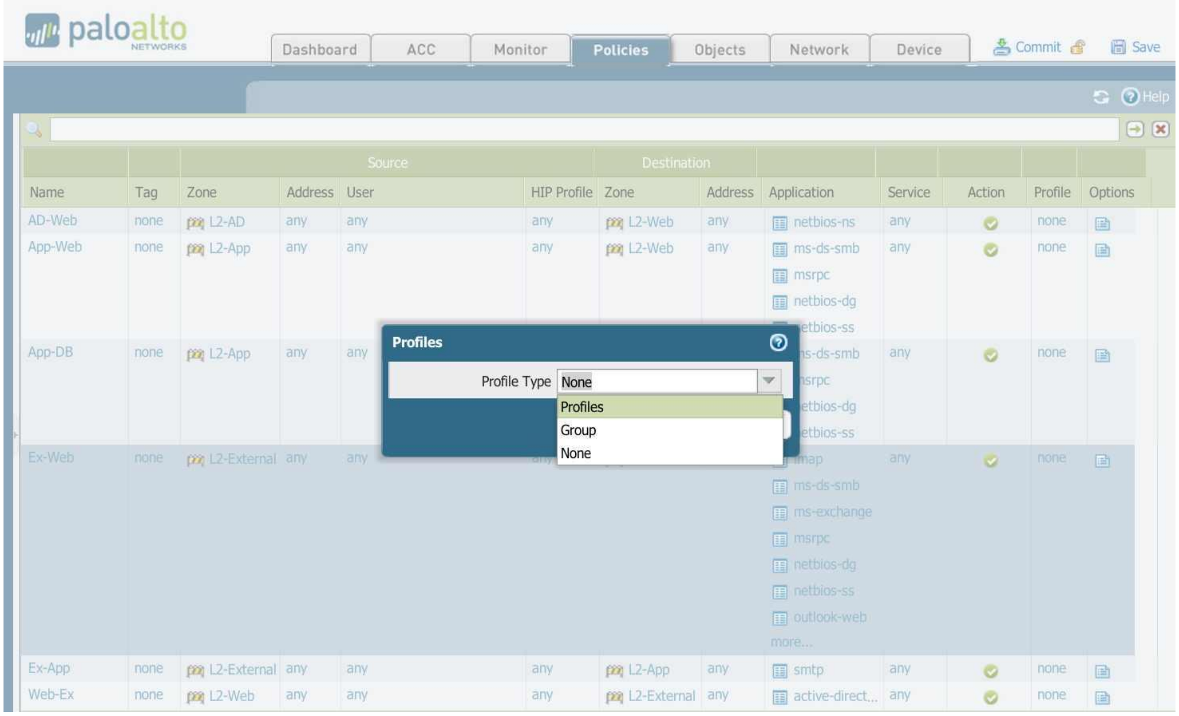
Each rule in the security policy can have its own security profile applied, allowing for the greatest flexibility in setting policy. For example, you may have a strict security profile blocking viruses, malware, and spyware on traffic that originates outside the data center and accesses the front-end servers, but not have any inspection 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
AD-Web	none	L2-AD	any	any	any	L2-Web	any	netbios-ns	any	✓	none	
App-Web	none	L2-App	any	any	any	L2-Web	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	
App-DB	none	L2-App	any	any	any	L2-DB	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	
Ex-Web	none	L2-External	any	any	any	L2-Web	any	imap ms-ds-smb ms-exchange msrpc netbios-dg netbios-ss outlook-web more...	any	✓	none	
Ex-App	none	L2-External	any	any	any	L2-App	any	smtp	any	✓	none	
Web-Ex	none	L2-Web	any	any	any	L2-External	any	active-direct...	any	✓	none	

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

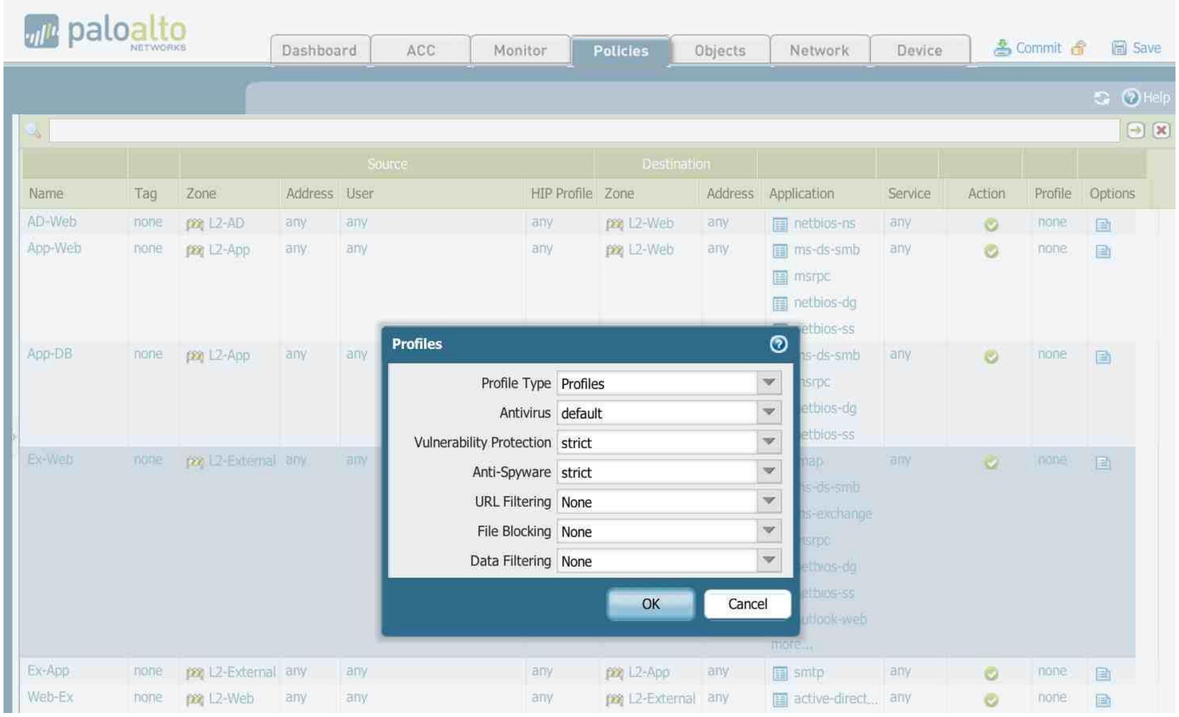


Profiles

Profile Type: None

		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
AD-Web	none	L2-AD	any	any	any	L2-Web	any	netbios-ns	any	✓	none	
App-Web	none	L2-App	any	any	any	L2-Web	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	
App-DB	none	L2-App	any	any				ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	
Ex-Web	none	L2-External	any	any				imap ms-ds-smb ms-exchange msrpc netbios-dg netbios-ss outlook-web more...	any	✓	none	
Ex-App	none	L2-External	any	any	any	L2-App	any	smtp	any	✓	none	
Web-Ex	none	L2-Web	any	any	any	L2-External	any	active-direct...	any	✓	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.

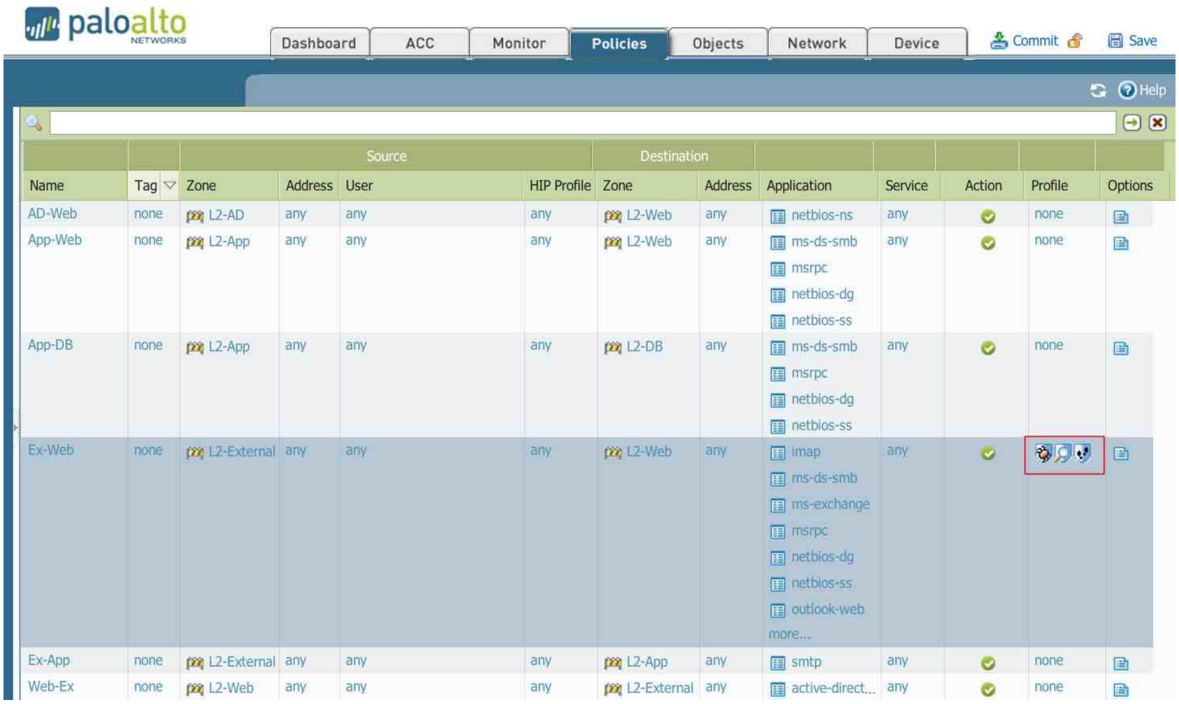


		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
AD-Web	none	L2-AD	any	any	any	L2-Web	any	netbios-ns	any	✓	none	
App-Web	none	L2-App	any	any	any	L2-Web	any	ms-ds-smb msrpc netbios-dg etbios-ss	any	✓	none	
App-DB	none	L2-App	any	any				ns-ds-smb nsrpc etbios-dg etbios-ss	any	✓	none	
Ex-Web	none	L2-External	any	any				map s-ds-smb s-exchange srpc etbios-dg etbios-ss utlook-web more...	any	✓	none	
Ex-App	none	L2-External	any	any	any	L2-App	any	smtp	any	✓	none	
Web-Ex	none	L2-Web	any	any	any	L2-External	any	active-direct...	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
AD-Web	none	L2-AD	any	any	any	L2-Web	any	netbios-ns	any	✓	none	
App-Web	none	L2-App	any	any	any	L2-Web	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	
App-DB	none	L2-App	any	any	any	L2-DB	any	ms-ds-smb msrpc netbios-dg netbios-ss	any	✓	none	
Ex-Web	none	L2-External	any	any	any	L2-Web	any	imap ms-ds-smb ms-exchange msrpc netbios-dg netbios-ss outlook-web more...	any	✓		
Ex-App	none	L2-External	any	any	any	L2-App	any	smtp	any	✓	none	
Web-Ex	none	L2-Web	any	any	any	L2-External	any	active-direct...	any	✓	none	

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

9. References

Citrix NetScaler Deployment Guide for Microsoft Exchange 2010. Citrix Systems, Inc. 2009
Application Template Deployment Guide. *Microsoft OWA*. Citrix Systems, Inc. 2008
NetScaler: Load Balancing Exchange 2010 http://www.cb-net.co.uk/citrix-articles/2013-netscaler-load-balancing-exchange-2010

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.