Deployment Guide for Microsoft Lync 2010

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

Table of Contents

1. Overview

Microsoft Lync Server 2010 is a real-time enterprise communications server providing instant messaging (IM), presence, file transfer, peer-to-peer and multi-party voice and video calling, as well as ad-hoc and structured conferences (audio, video, web, and shared whiteboard). These features are available within an organization, between separate organizations, with outside users on the Internet, on standard telephones (mobile or fixed-line).

As with any sophisticated application, a best-in-class firewall and application delivery controller are recommended for providing appropriate security, scalability, and optimization. The combination of Citrix NetScaler® and Palo Alto Networks PA Series addresses these requirements and go on to deliver 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 identity based security to provide a robust, tightly integrated solution. Deployed in front of application servers, the NetScaler and Palo Alto Networks next-generation firewalls significantly reduce processing overhead on application and database servers and improves security thereby reducing hardware and bandwidth costs.

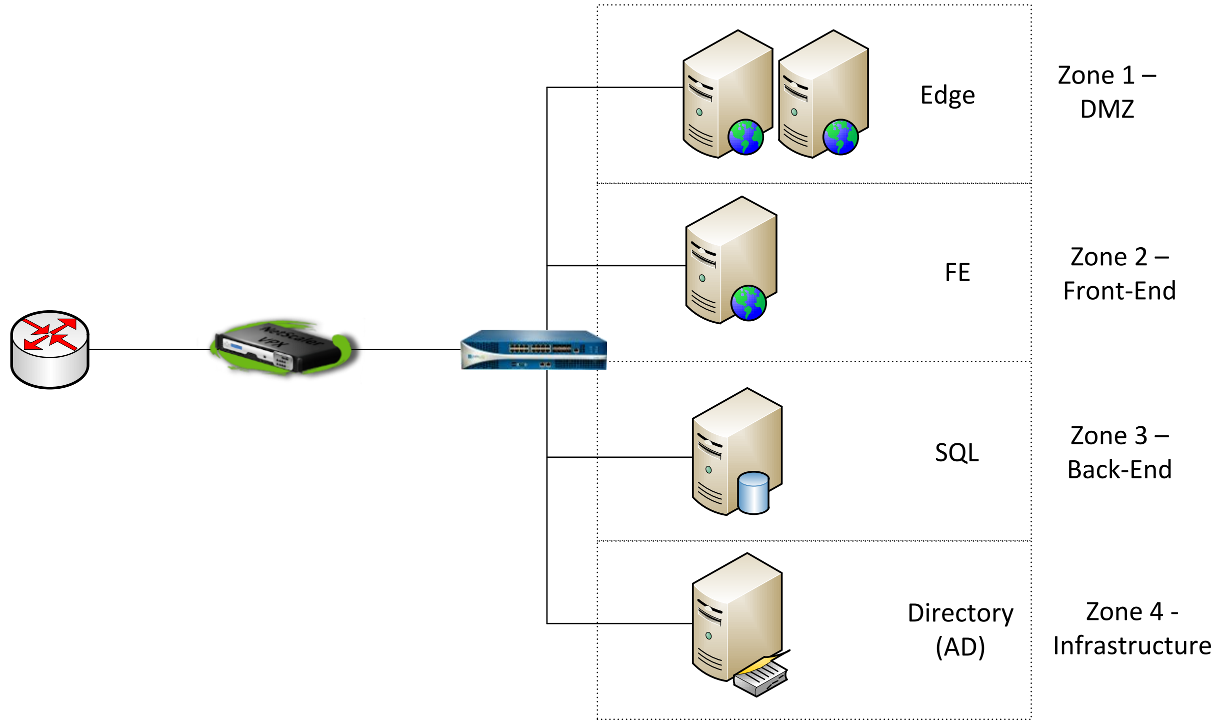
In this deployment guide, step-by-step instructions are provided on how to deploy Citrix NetScaler and the Palo Alto Networks next-generation firewalls to improve the security and performance of Microsoft Lync 2010.

2. Requirements

Required Component	Used in this Document	Note
NetScaler ADC	NS10.0 VPX Build 69.4.nc with Platinum License	
Palo Alto Networks Firewall	PAN-OS 4.1	
Lync 2010 Servers	4 Physical/VM servers	2x Edge; 1x Internal Front-end; 1x DB; 1x AD

3. Microsoft Lync Network Topology

3.1 Environment diagram



3.2 IP allocations

The following IP addresses were allocated in this reference environment.

Functional Device	IP	Subnet Mask
NetScaler IP (NSIP)	10.5.172.124	255.255.255.0
NetScaler Subnet IP (SNIP)	10.5.172.126	255.255.255.0
Lync External Edge (VIP)	10.5.172.170	255.255.255.0
Lync Edge Server 1	10.5.172.175	255.255.255.0
Lync Edge Server 2	10.5.172.176	255.255.255.0
Lync Internal Front-End (VIP)	10.5.172.177	255.255.255.0
Lync Front-End Server	10.5.172.171	255.255.255.0
Database SQL Server	10.5.172.152	255.255.255.0
Active Directory Server	10.5.172.155	255.255.255.0

3.3 Lync Protocol/Port Requirements

The following protocols and ports were used in this reference environment.

Virtual Server	Protocol	Load-Balanced Lync Server	Port	Services
Edge VIP	SSL_BRIDGE*	Edge Server1 Edge Server2	443 443	
Edge VIP	TCP	Edge Server1	135	

		Edge Server2	135	
Front-End VIP	TCP	Front-End Server**	135	
Front-End VIP	TCP	Front-End Server	444	
Front-End VIP	TCP	Front-End Server	5060	
Front-End VIP	TCP	Front-End Server	5061	
Front-End VIP	SSL_BRIDGE	Front-End Server	443	
Front-End VIP	TCP	Front-End Server	80	

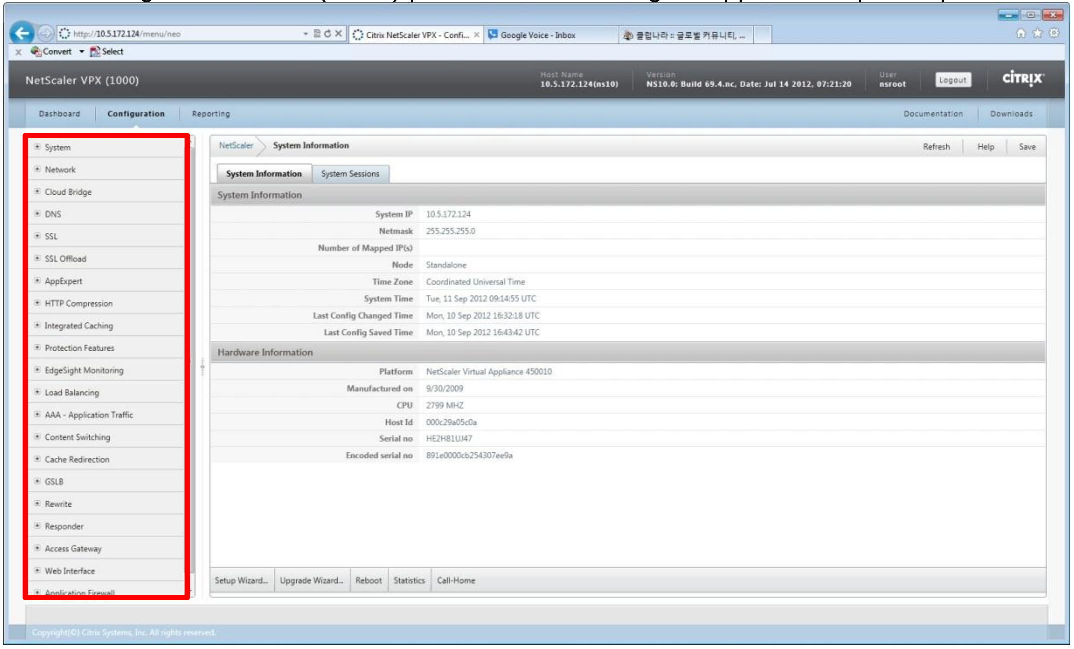
** SSL Offload is not supported on Lync by Microsoft. NetScaler will act as a bridge to pass the security certificate authentication to Lync servers.*

*** Although there is only one Front-End Server in this reference environment, this document will use a virtual server to communicate from NetScaler to Front-End Server.*

4. Overview of NetScaler Installation and Configuration for Lync

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 where to configure application specific parameters.



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 Lync configuration:

NetScaler Menu	NetScaler Sub-Menu	Action
System	Licenses	Manage Licenses
	Settings	Configure basic features
Network	IPs	NetScaler IP, Subnet IP
		Virtual IP
Load Balancing	Monitoring	Per Port
	Service Group	Per Port
	Servers	Per Physical/VM server

4.2 Step –by-Step Installation

The following is an overview of steps which are required to configure Lync services within NetScaler..

Step	Action	Detail	Custom Data
1	NetScaler IP, Subnet IP	NetScaler initial Configurations (by Setup Wizard)	NetScaler IP (NSIP), Subnet IP (SNIP)
2	Manage Licenses	NetScaler license installation	.lic license file
3	Configure basic features	NetScaler basic feature settings	Feature settings
4	Configure Lync Custom Monitoring	Creating Load Balancing Monitoring	TCP Port 80, 443, 50601 and 5061
5	Configure Backend Services	Creating a Service Group	IPs for Edge Server 1 and Edge Server 2; IP for Front-end Server
6	Configure Public Endpoint Services	Creating virtual servers (IP) to talk to multiple backend servers	Lync Virtual IPs (VIP)

5. Deployment Instruction

This section will describe detail steps from NetScaler VPX installation and initial configuration to Lync service configuration within NetScaler.

5.1 NetScaler Initial Configurations

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

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

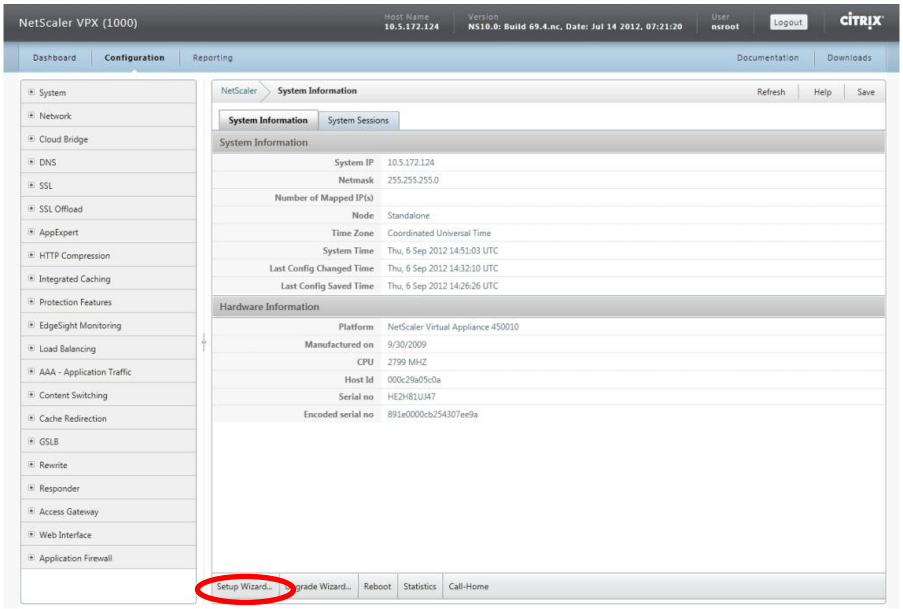
5.1.1 Add NSIP, Subnet Mask, and Default Gateway on NetScaler:

At the Console prompt from XenCenter or 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 Lync 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

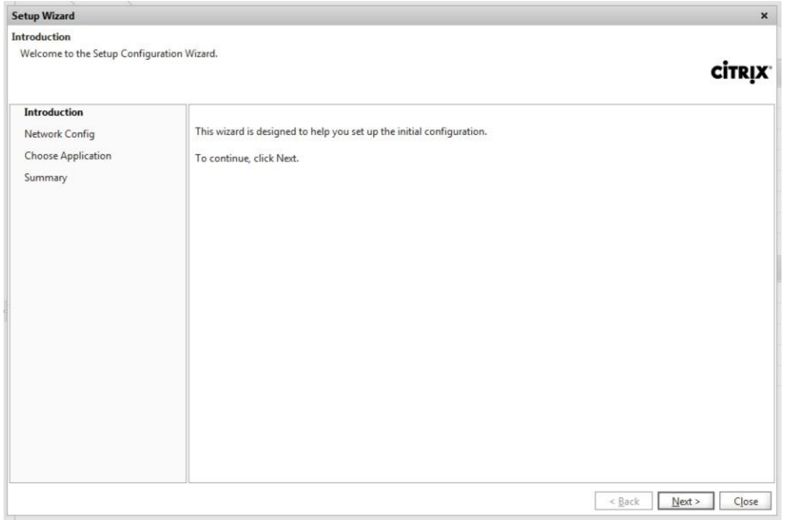
System Information

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



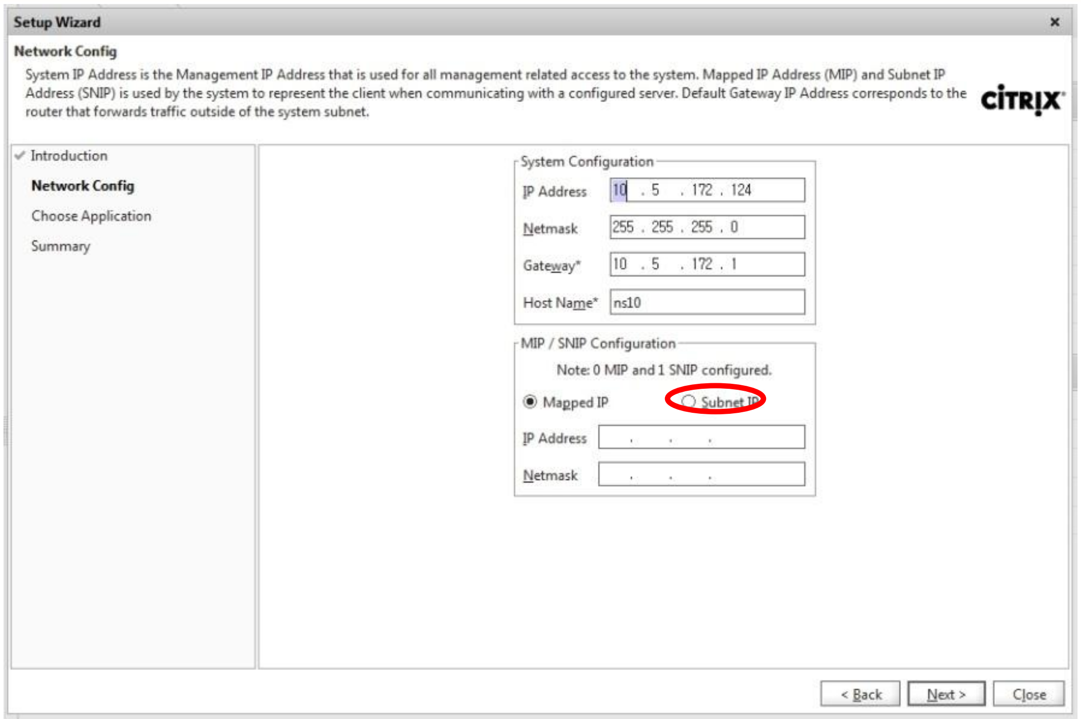
Introduction

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.

System Configuration

IP Address: 10 . 5 . 172 . 124

Netmask: 255 . 255 . 255 . 0

Gateway*: 10 . 5 . 172 . 1

Host Name*: ns10

MIP / SNIP Configuration

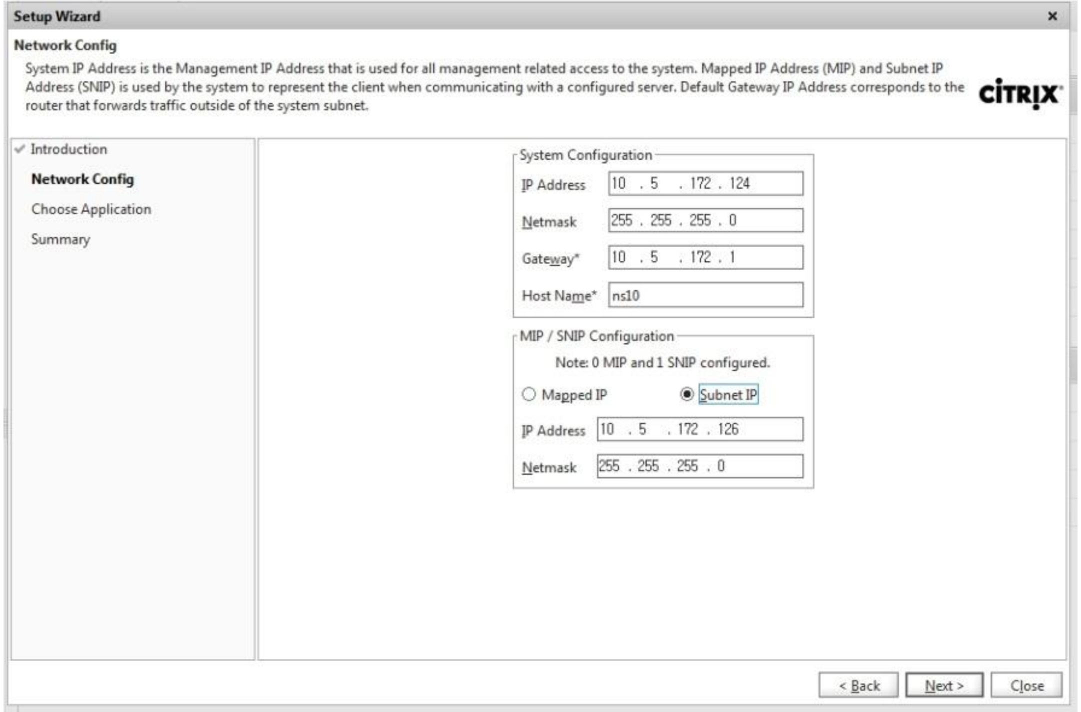
Note: 0 MIP and 1 SNIP configured.

● 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.

System Configuration

IP Address: 10 . 5 . 172 . 124

Netmask: 255 . 255 . 255 . 0

Gateway*: 10 . 5 . 172 . 1

Host Name*: ns10

MIP / SNIP Configuration

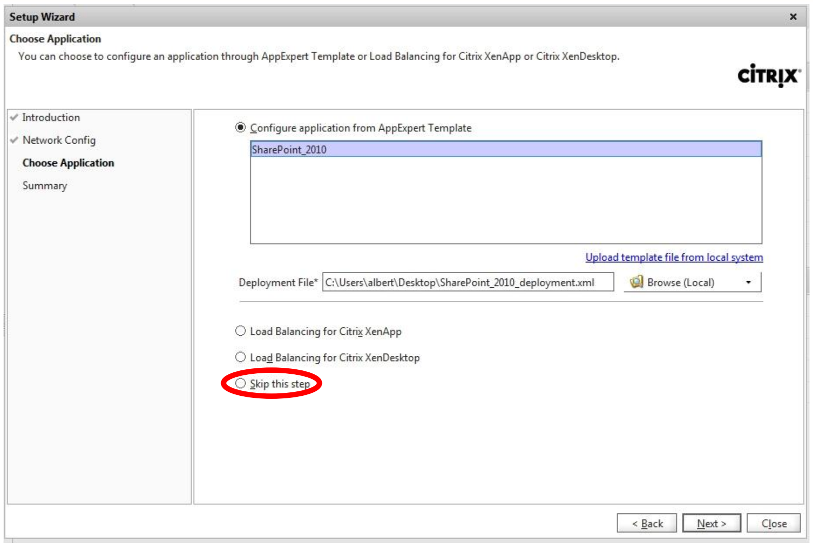
Note: 0 MIP and 1 SNIP configured.

○ Mapped IP ● Subnet IP

IP Address: 10 . 5 . 172 . 126

Netmask: 255 . 255 . 255 . 0

Choose **Skip this Step**. Lync configuration data will be added manually.



Choose Application

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

● Configure application from AppExpert Template

SharePoint_2010

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

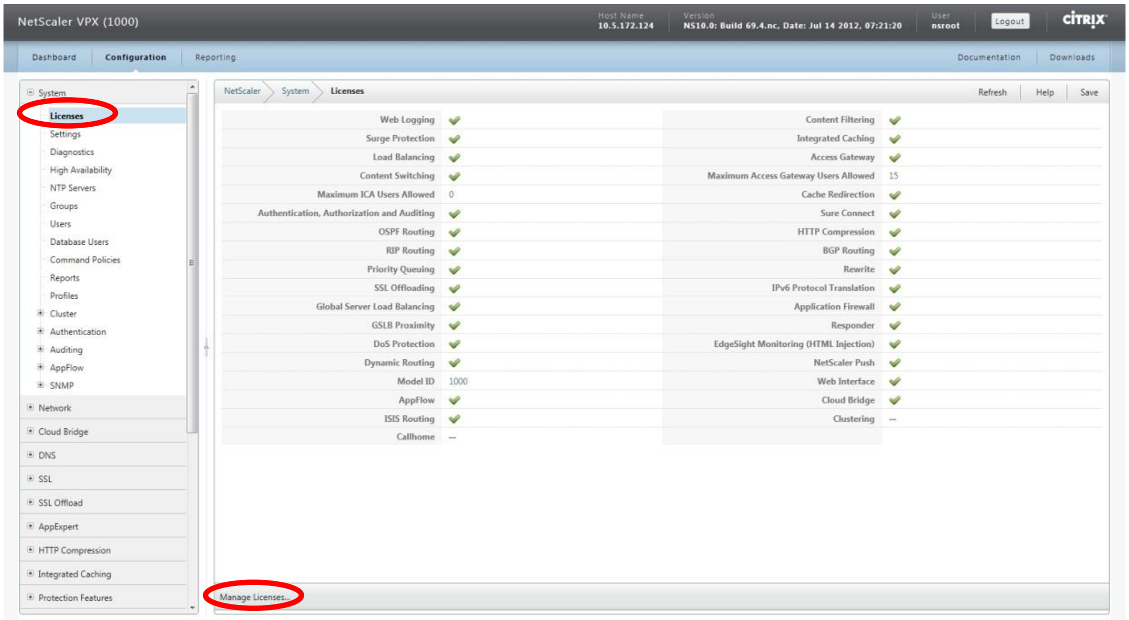
○ Load Balancing for Citrix XenApp

○ Load Balancing for Citrix XenDesktop

○ Skip this step

5.2 NetScaler License installation

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



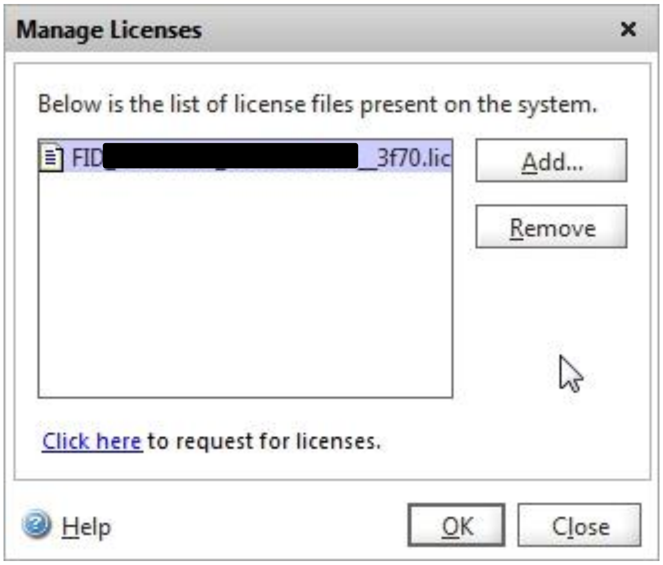
Host Name 10.5.172.124

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

User nsroot

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

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



Manage Licenses

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

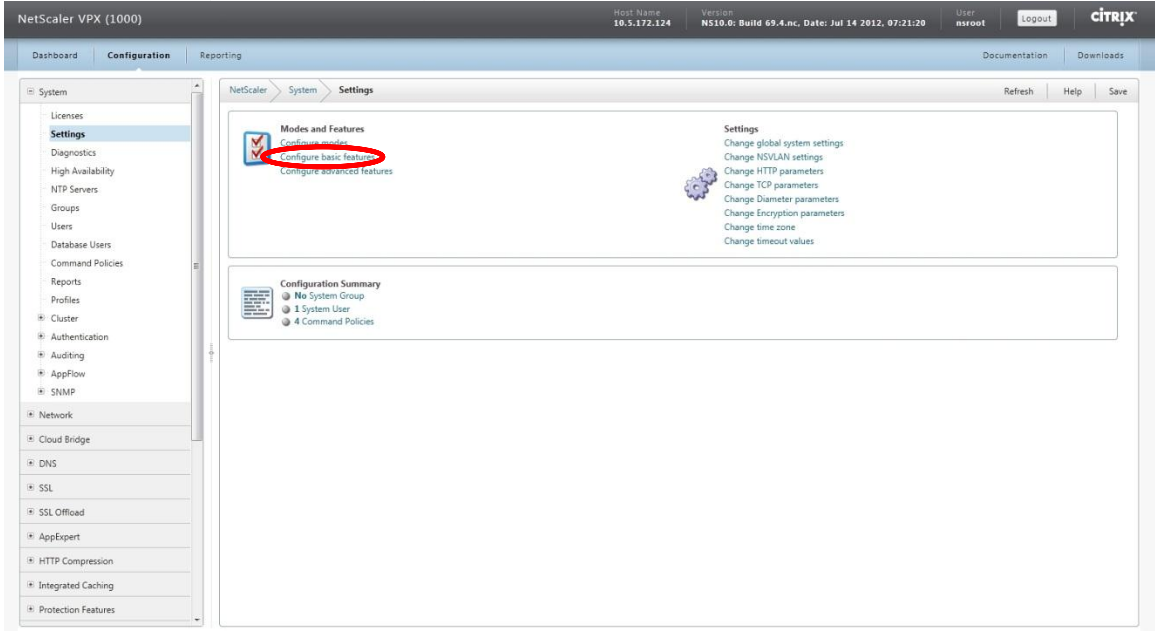
FID[redacted]_3f70.lic

Click here to request for licenses.

5.3 NetScaler Basic Feature Setting

5.3.1 NetScaler Feature Setting

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



NetScaler VPX (1000)

Host Name 10.5.172.124

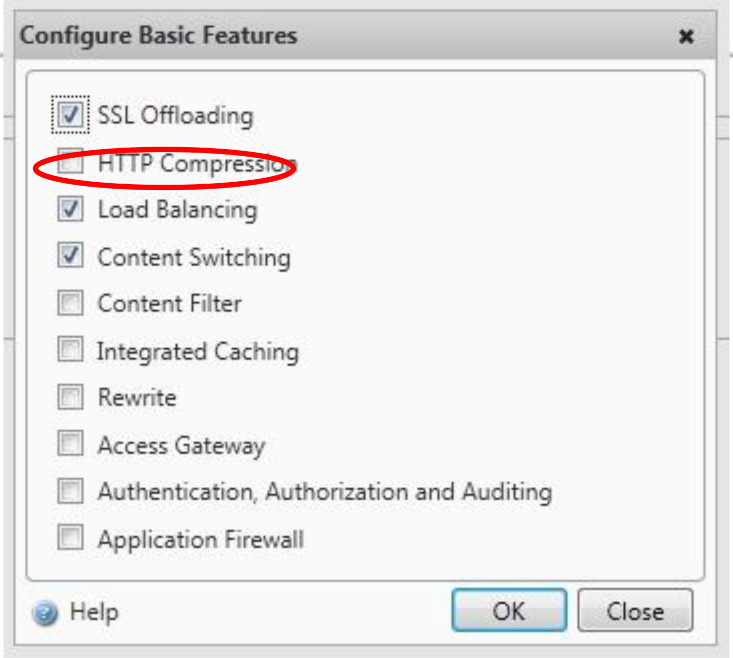
Version NS10.0: Build 69.4.nc, Date: Jul 14 2012, 07:21:20

User nsroot

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

5.3.2 Basic Features

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

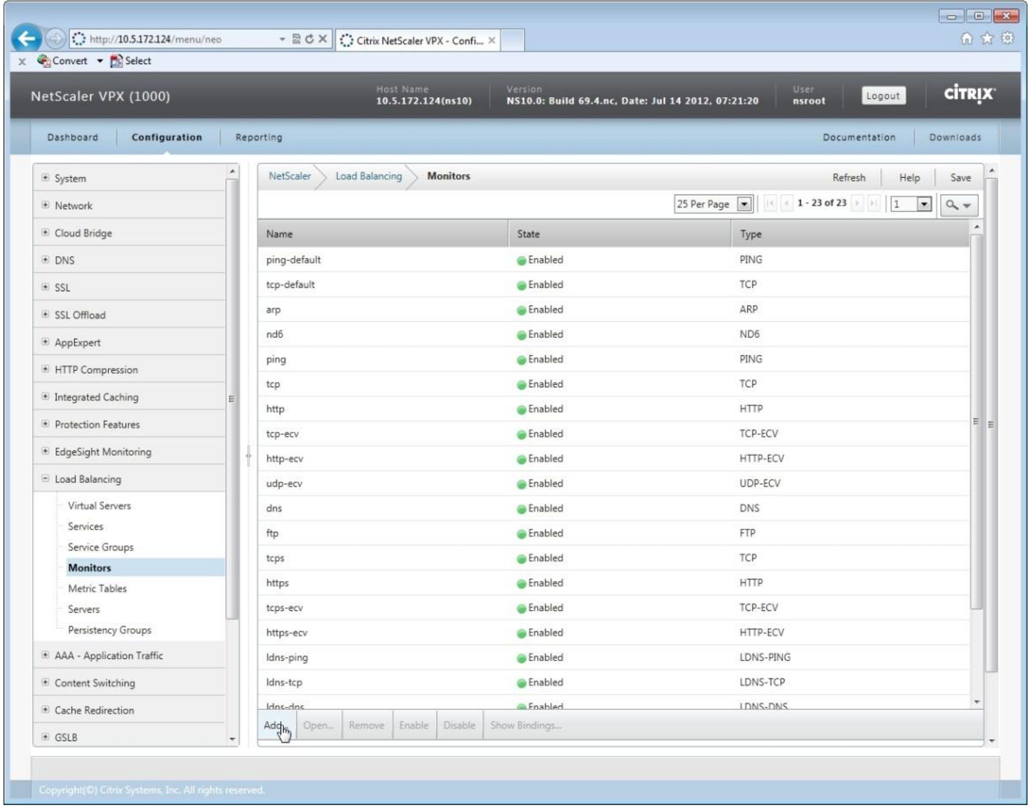


Configure Basic Features

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

5.4 Creating Lync Load Balancing Custom Monitoring

Based on protocol/port requirements in Section 3.3, the following custom monitoring will be created – Port 80, 443, 5060 and 5061. The rest of ports 135, 444 will be monitored with port 5061.
Under **Load Balancing** navigation menu, choose **Monitor** and **Add**.



NetScaler VPX (1000)

Host Name 10.5.172.124(ns10)

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

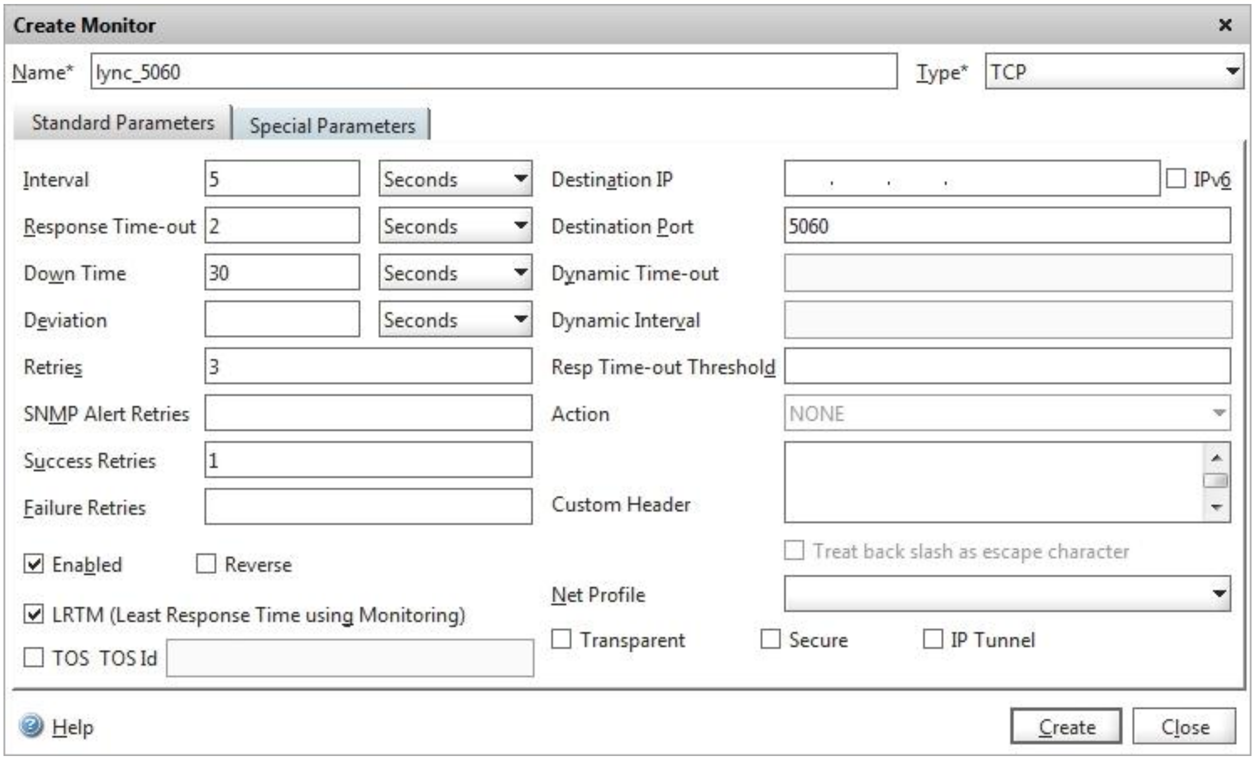
User nsroot

NetScaler > Load Balancing > Monitors

25 Per Page | 1 - 23 of 23

Name	State	Type
ping-default	Enabled	PING
tcp-default	Enabled	TCP
arp	Enabled	ARP
nd6	Enabled	ND6
ping	Enabled	PING
tcp	Enabled	TCP
http	Enabled	HTTP
tcp-ecv	Enabled	TCP-ECV
http-ecv	Enabled	HTTP-ECV
udp-ecv	Enabled	UDP-ECV
dns	Enabled	DNS
ftp	Enabled	FTP
tcps	Enabled	TCP
https	Enabled	HTTP
tcps-ecv	Enabled	TCP-ECV
https-ecv	Enabled	HTTP-ECV
ldns-ping	Enabled	LDNS-PING
ldns-tcp	Enabled	LDNS-TCP
ldns-dns	Enabled	LDNS-DNS

Select **Name** to **lync_5060** and **Type** to **TCP**. **Destination Port** to **5060**. Then, **Create**.



Create Monitor ×

Name* lync_5060 Type* TCP

Standard Parameters | Special Parameters

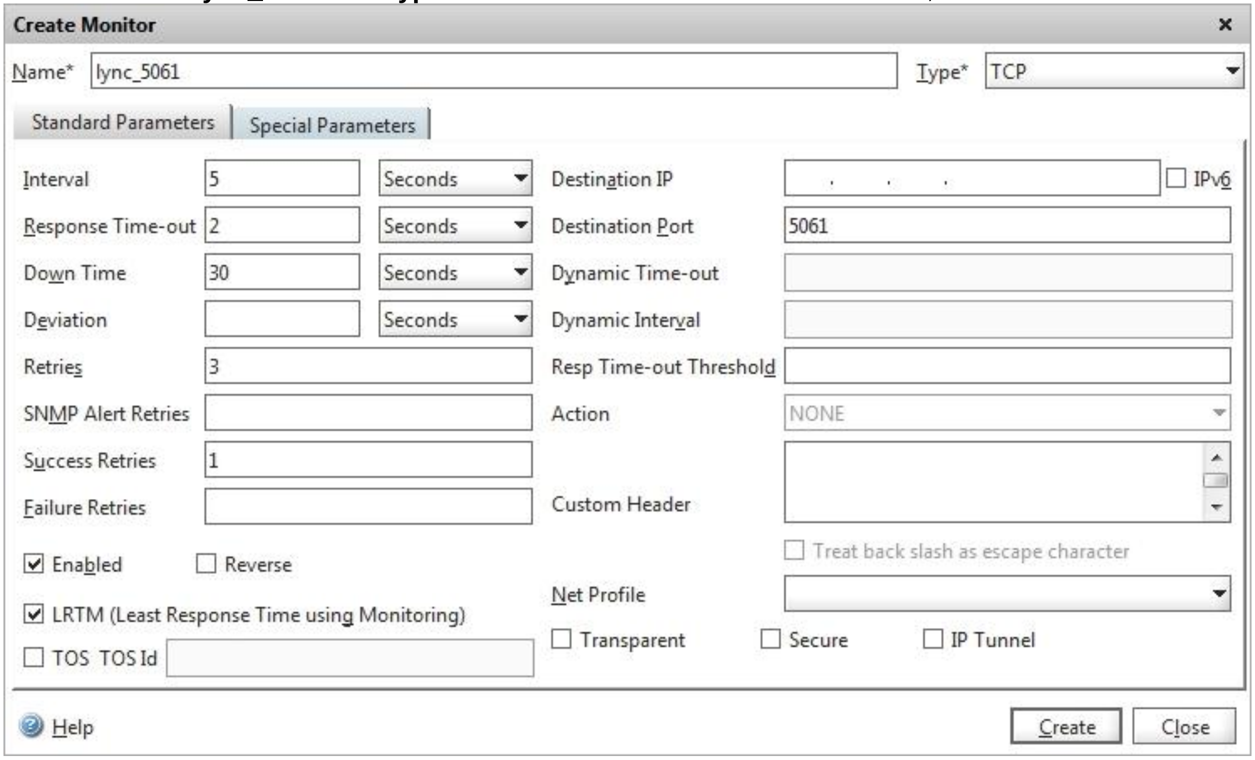
Interval 5 Seconds
Response Time-out 2 Seconds
Down Time 30 Seconds
Deviation Seconds
Retries 3
SNMP Alert Retries
Success Retries 1
Failure Retries

☑ Enabled □ Reverse
☑ LRTM (Least Response Time using Monitoring)
□ TOS TOS Id

Destination IP . . . □ IPv6
Destination Port 5060
Dynamic Time-out
Dynamic Interval
Resp Time-out Threshold
Action NONE
Custom Header
□ Treat back slash as escape character
Net Profile
□ Transparent □ Secure □ IP Tunnel

Help Create Close

Select **Name** to **lync_5061** and **Type** to **TCP**. **Destination Port** to **5061**. Then, **Create**.



Create Monitor ×

Name* lync_5061 Type* TCP

Standard Parameters | Special Parameters

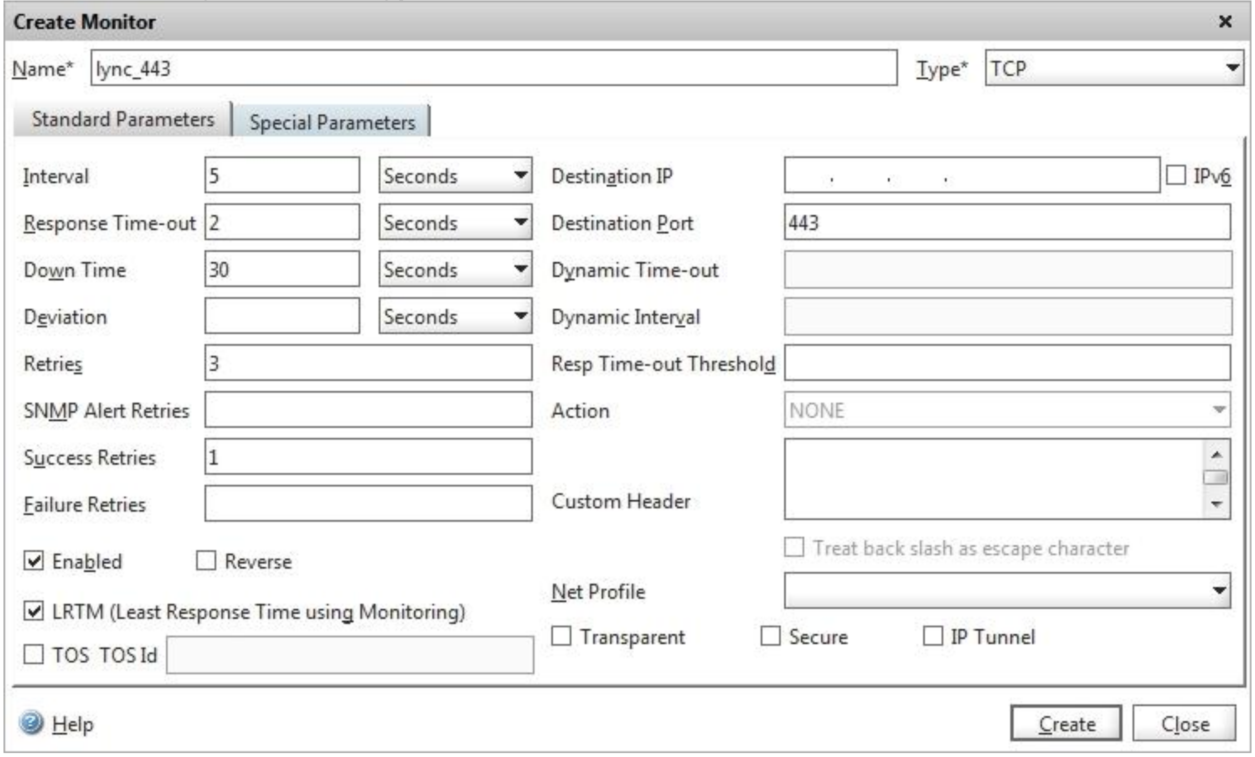
Interval 5 Seconds
Response Time-out 2 Seconds
Down Time 30 Seconds
Deviation Seconds
Retries 3
SNMP Alert Retries
Success Retries 1
Failure Retries

☑ Enabled □ Reverse
☑ LRTM (Least Response Time using Monitoring)
□ TOS TOS Id

Destination IP . . . □ IPv6
Destination Port 5061
Dynamic Time-out
Dynamic Interval
Resp Time-out Threshold
Action NONE
Custom Header
□ Treat back slash as escape character
Net Profile
□ Transparent □ Secure □ IP Tunnel

Help Create Close

Select **Name** to **lync_443** and **Type** to **TCP**. **Destination Port** to **443**. Then, **Create**.



Create Monitor

Name* lync_443 Type* TCP

Standard Parameters | Special Parameters

Interval	5	Seconds	Destination IP	. . . □ IPv6
Response Time-out	2	Seconds	Destination Port	443
Down Time	30	Seconds	Dynamic Time-out	
Deviation		Seconds	Dynamic Interval	
Retries	3		Resp Time-out Threshold	
SNMP Alert Retries			Action	NONE
Success Retries	1		Custom Header	
Failure Retries				

☑ Enabled □ Reverse

□ Treat back slash as escape character

☑ LRTM (Least Response Time using Monitoring)

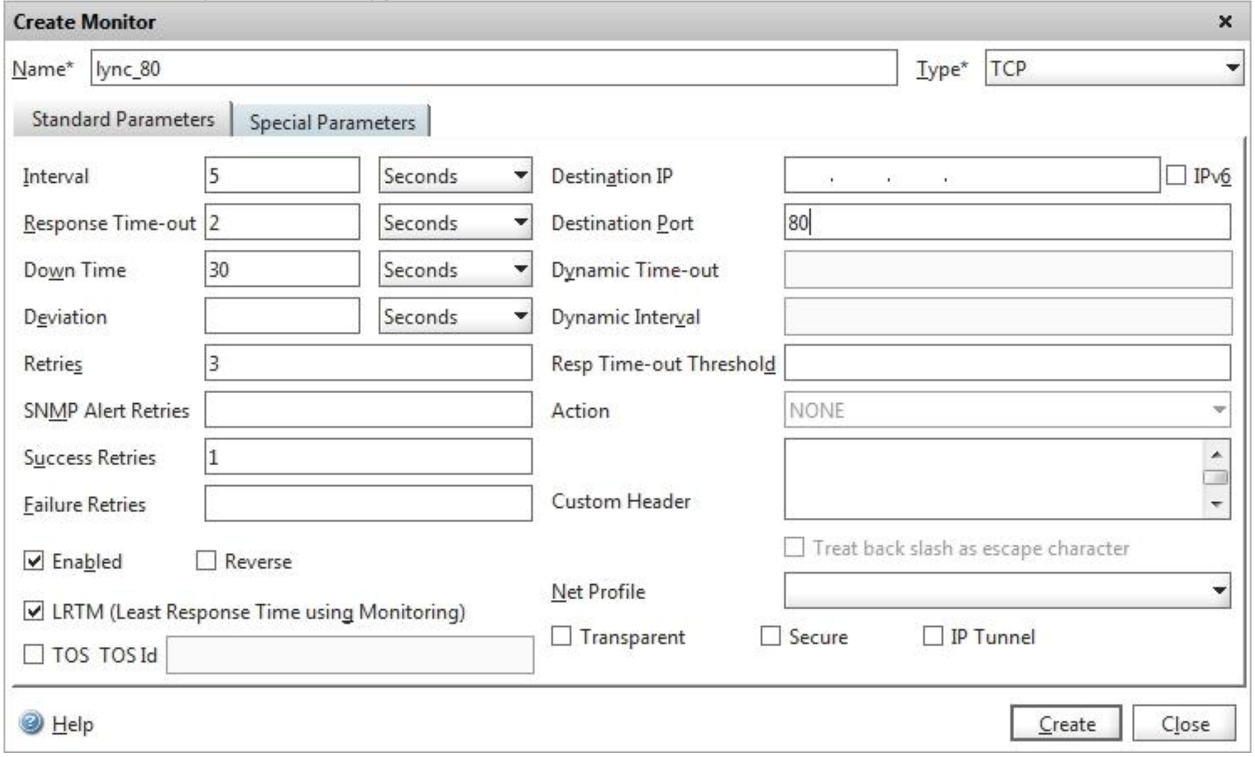
Net Profile

□ TOS TOS Id

□ Transparent □ Secure □ IP Tunnel

Help

Select **Name** to **lync_80** and **Type** to **TCP**. **Destination Port** to **80**. Then, **create**.



Create Monitor

Name* lync_80 Type* TCP

Standard Parameters | Special Parameters

Interval	5	Seconds	Destination IP	. . . □ IPv6
Response Time-out	2	Seconds	Destination Port	80
Down Time	30	Seconds	Dynamic Time-out	
Deviation		Seconds	Dynamic Interval	
Retries	3		Resp Time-out Threshold	
SNMP Alert Retries			Action	NONE
Success Retries	1		Custom Header	
Failure Retries				

☑ Enabled □ Reverse

□ Treat back slash as escape character

☑ LRTM (Least Response Time using Monitoring)

Net Profile

□ TOS TOS Id

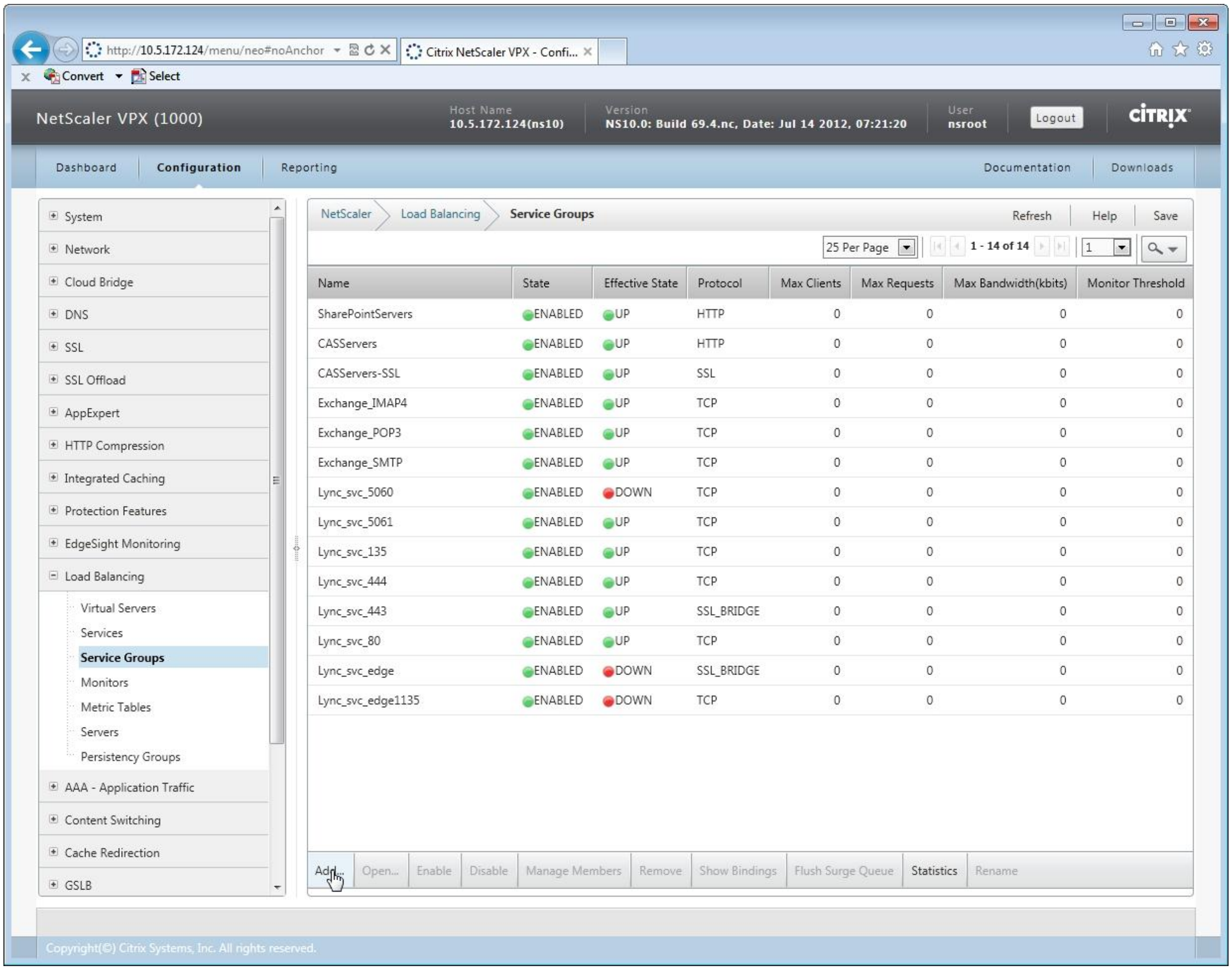
□ Transparent □ Secure □ IP Tunnel

Help

5.5 Creating Load Balancing Service Groups

Each service port which communicates between backend physical/VM servers and public endpoint virtual server needs to be configured as a service group.

From NetScsaler Configuration Utility navigation menu, choose **Service Groups** under **Load Balancing** menu. Click **Add**.



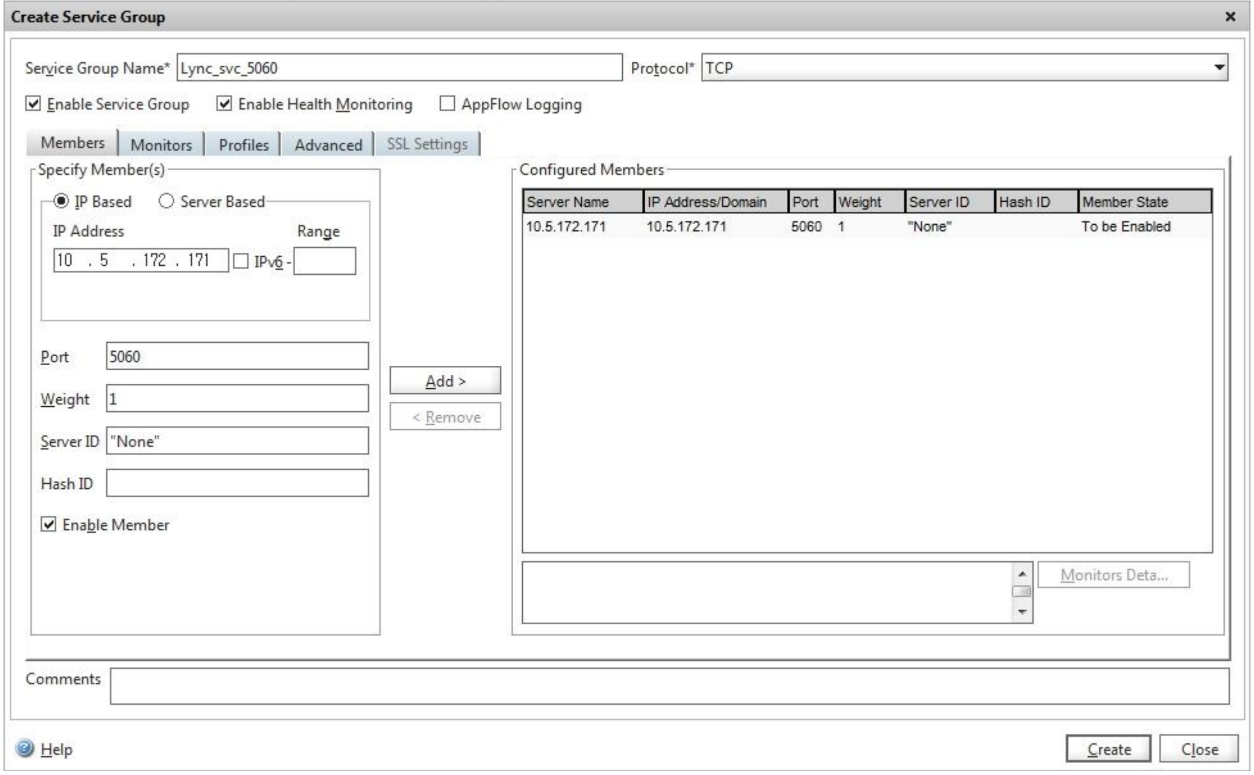
Host Name 10.5.172.124(ns10)

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

User nsroot

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

Set **Service Group Name** to **Lync_svc_5060**, **Protocol** to **TCP**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group

Service Group Name* Lync_svc_5060 Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring □ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address 10 . 5 . 172 . 171 □ IPv6 - Range

Port 5060

Weight 1

Server ID "None"

Hash ID

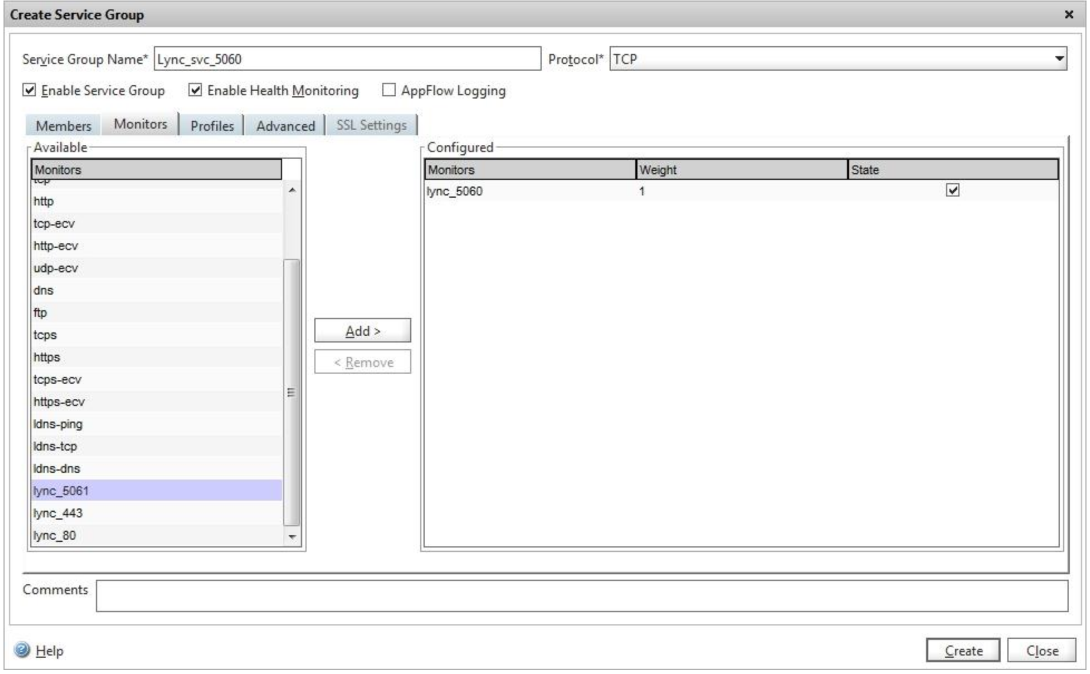
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.171	10.5.172.171	5060	1	"None"		To be Enabled

Comments

Choose **lync_5060** from **Monitors** tab. Then **Create**.



Create Service Group

Service Group Name* Lync_svc_5060 Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring □ AppFlow Logging

Available

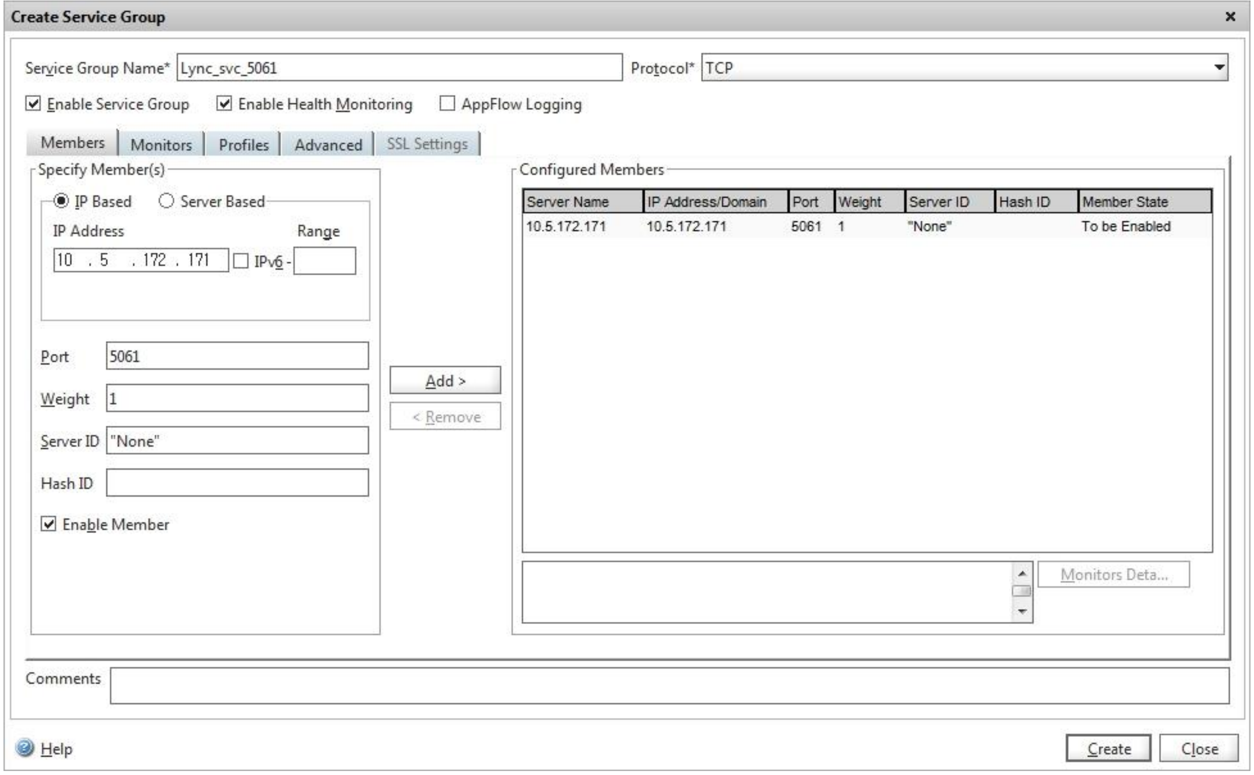
Monitors
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_5061
lync_443
lync_80

Configured

Monitors	Weight	State
lync_5060	1	☑

Comments

Set **Service Group Name** to **Lync_svc_5061**, **Protocol** to **TCP**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group

Service Group Name* Lync_svc_5061

Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring ☐ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address: 10 . 5 . 172 . 171 ☐ IPv6 - Range:

Port: 5061

Weight: 1

Server ID: "None"

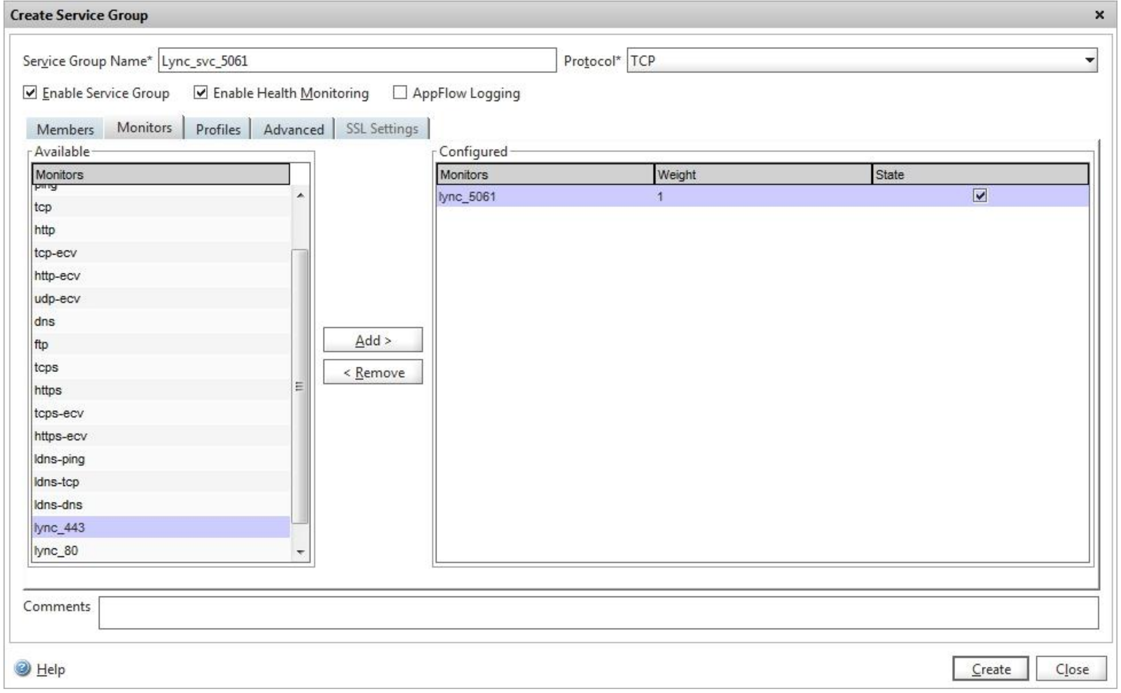
Hash ID:

☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.171	10.5.172.171	5061	1	"None"		To be Enabled

Choose **lync_5061** from **Monitors** tab. Then **Create**.



Create Service Group

Service Group Name* Lync_svc_5061

Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring ☐ AppFlow Logging

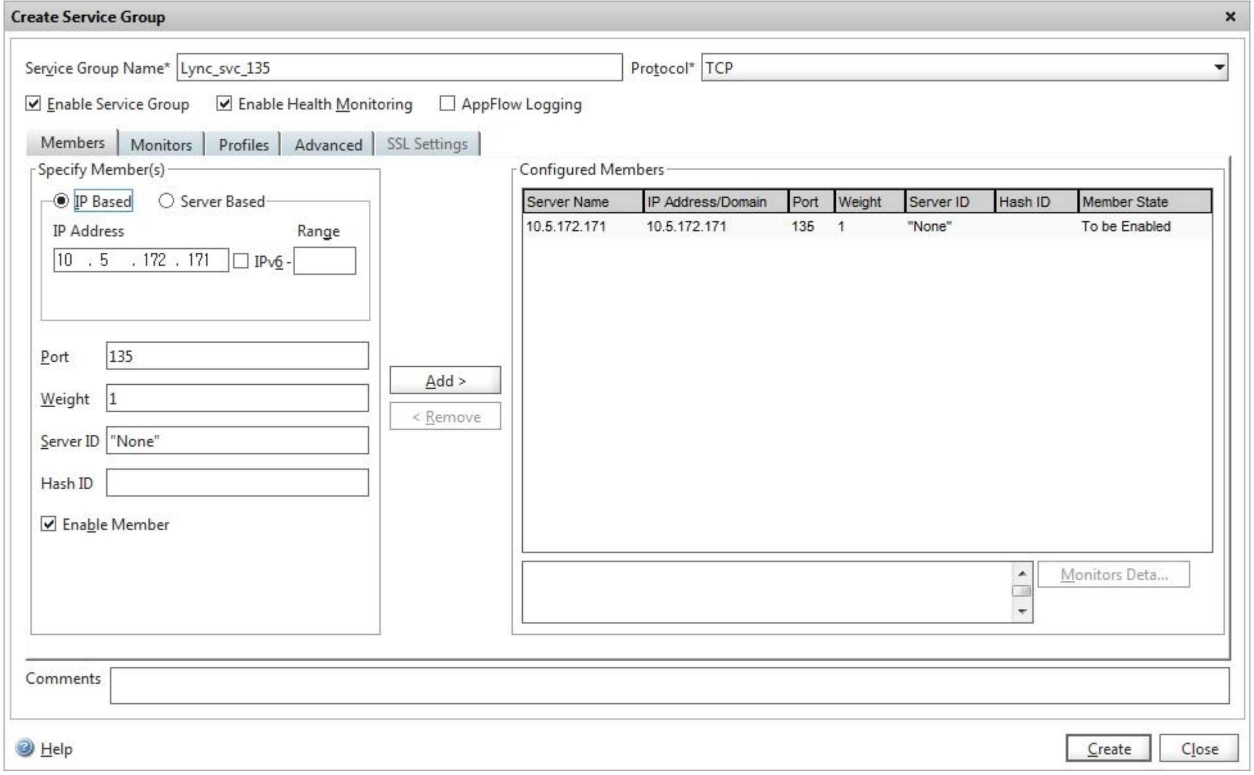
Available

Monitors
ping
tcp
http
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_443
lync_80

Configured

Monitors	Weight	State
lync_5061	1	☑

Set **Service Group Name** to **Lync_svc_135**, **Protocol** to **TCP**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Service Group Name* Lync_svc_135 Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring ☐ AppFlow Logging

● IP Based ○ Server Based

IP Address 10 . 5 . 172 . 171 ☐ IPv6 - Range

Port 135

Weight 1

Server ID "None"

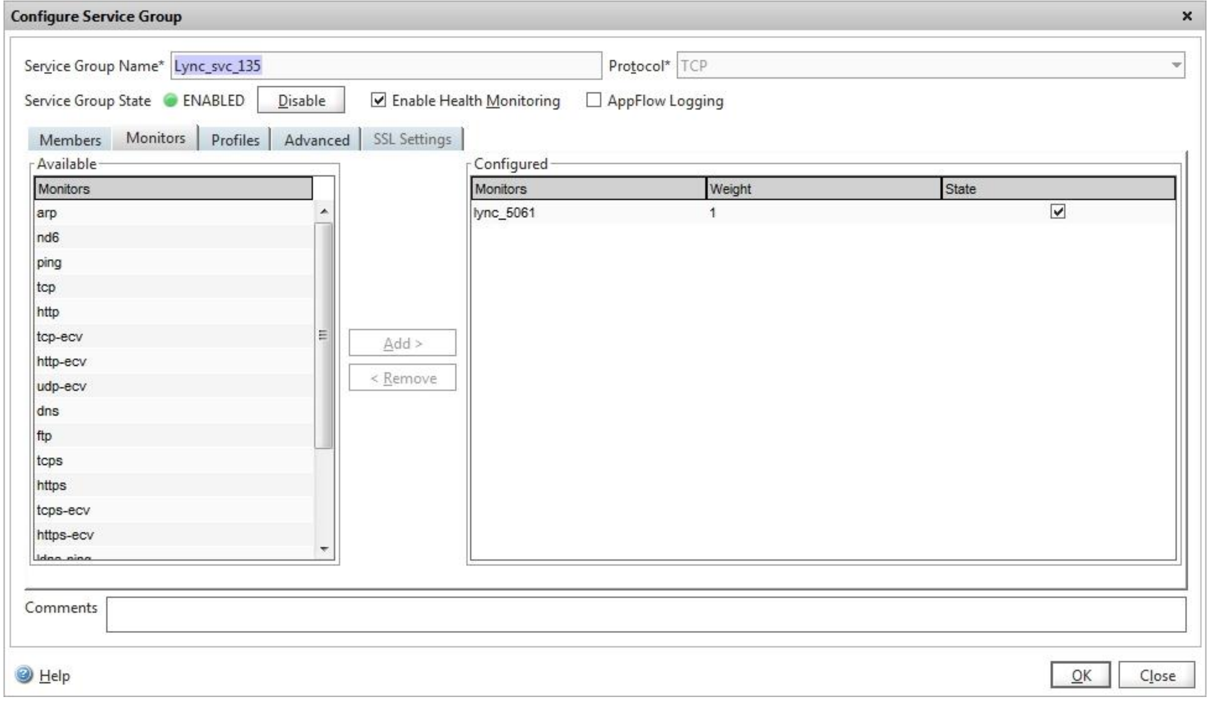
Hash ID

☑ Enable Member

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.171	10.5.172.171	135	1	"None"		To be Enabled

Comments

Choose **lync_5060** from **Monitors** tab. Then **Create**.



Service Group Name* Lync_svc_135 Protocol* TCP

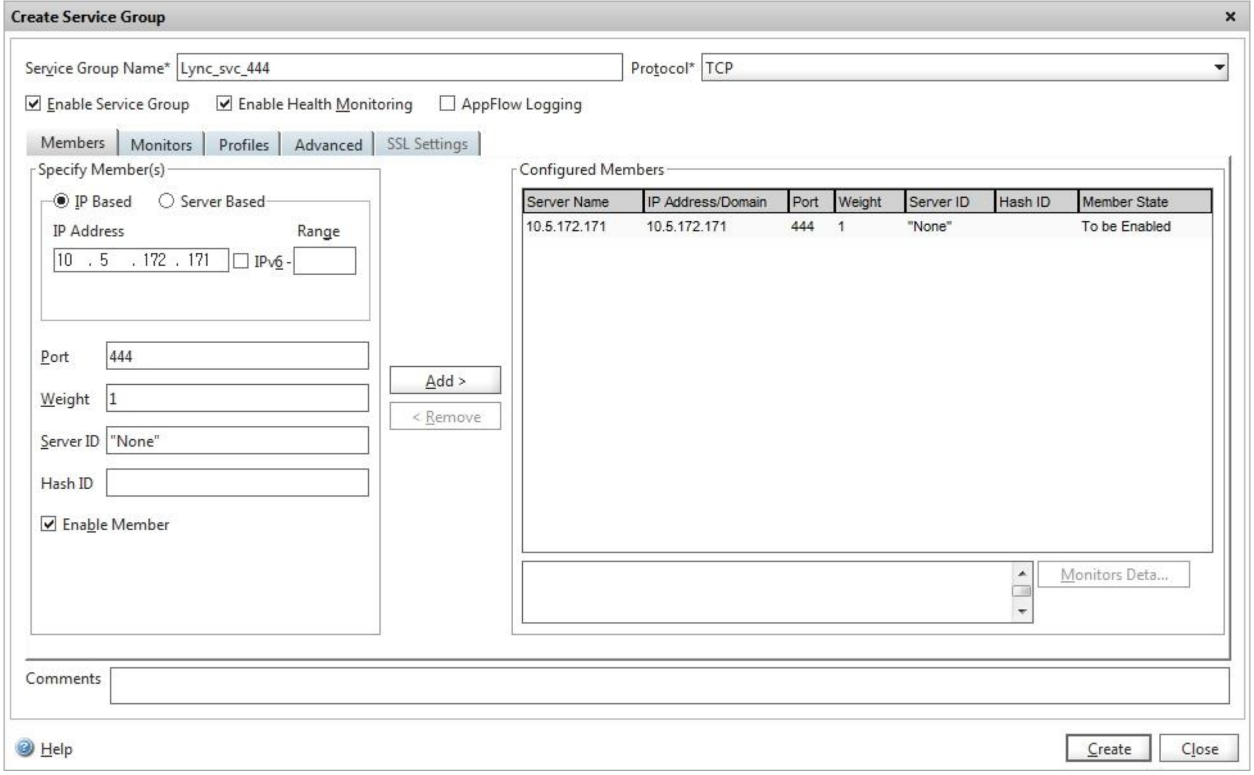
Service Group State ● ENABLED ☑ Enable Health Monitoring ☐ AppFlow Logging

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

Monitors	Weight	State
lync_5061	1	☑

Comments

Set **Service Group Name** to **Lync_svc_444**, **Protocol** to **TCP**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group

Service Group Name* Lync_svc_444 Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring ☐ AppFlow Logging

Specify Member(s)

● IP Based ○ Server Based

IP Address 10 . 5 . 172 . 171 ☐ IPv6 - Range

Port 444

Weight 1

Server ID "None"

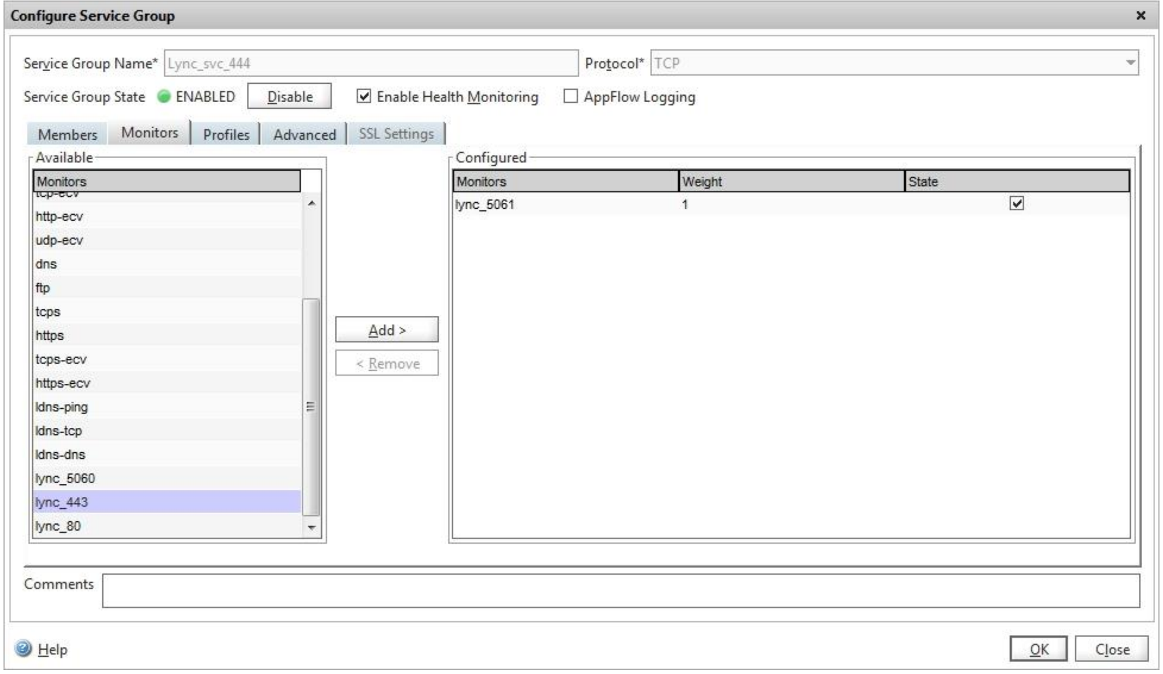
Hash ID

☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.171	10.5.172.171	444	1	"None"		To be Enabled

Choose **lync_443** from **Monitors** tab. Then **Create**.



Configure Service Group

Service Group Name* Lync_svc_444 Protocol* TCP

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

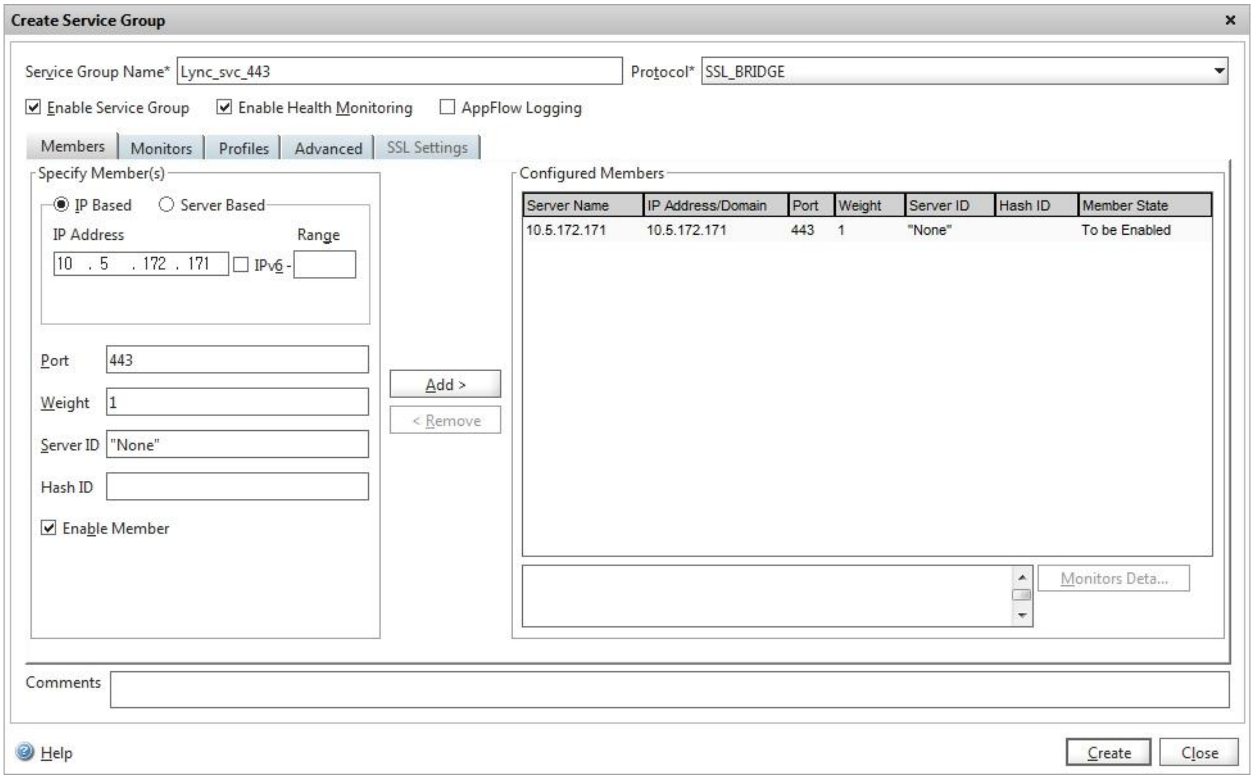
Available

Monitors
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_5060
lync_443
lync_80

Configured

Monitors	Weight	State
lync_5061	1	☑

Set **Service Group Name** to **Lync_svc_443**, **Protocol** to **SSL_BRIDGE**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group

Service Group Name* Lync_svc_443 Protocol* SSL_BRIDGE

☑ Enable Service Group ☑ Enable Health Monitoring □ AppFlow Logging

Members | Monitors | Profiles | Advanced | SSL Settings

Specify Member(s)

● IP Based ○ Server Based

IP Address 10 . 5 . 172 . 171 □ IPv6 - Range

Port 443

Weight 1

Server ID "None"

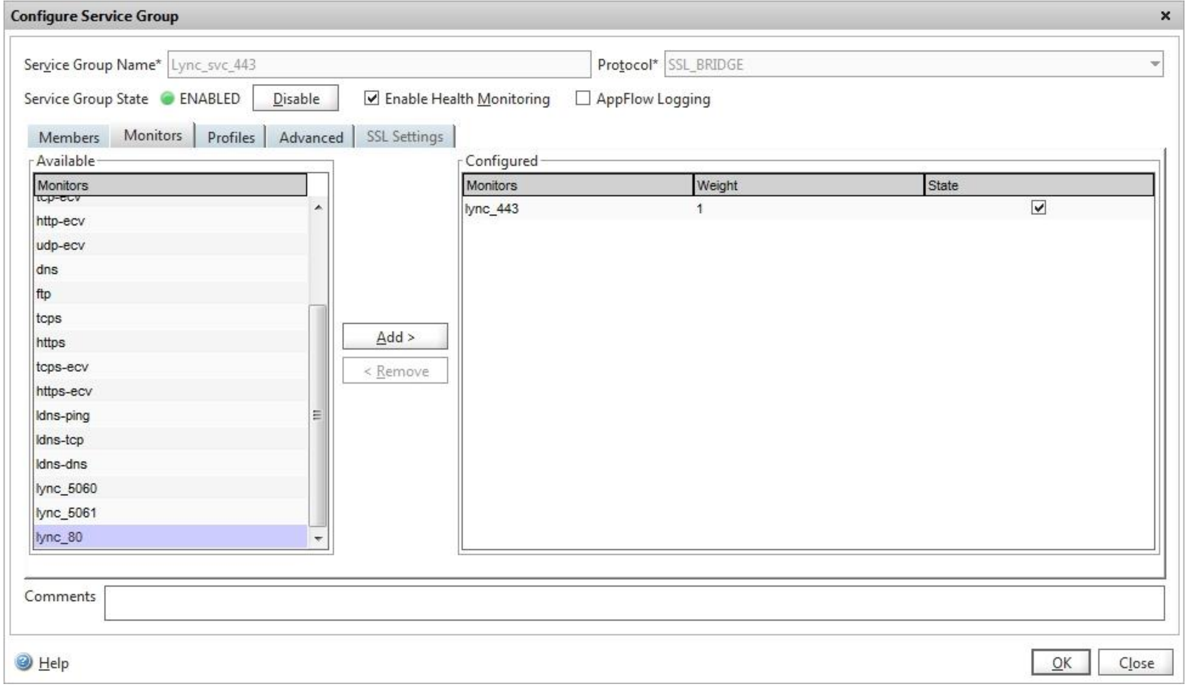
Hash ID

☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.171	10.5.172.171	443	1	"None"		To be Enabled

Choose **lync_443** from **Monitors** tab. Then **Create**.



Configure Service Group

Service Group Name* Lync_svc_443 Protocol* SSL_BRIDGE

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

Members | Monitors | Profiles | Advanced | SSL Settings

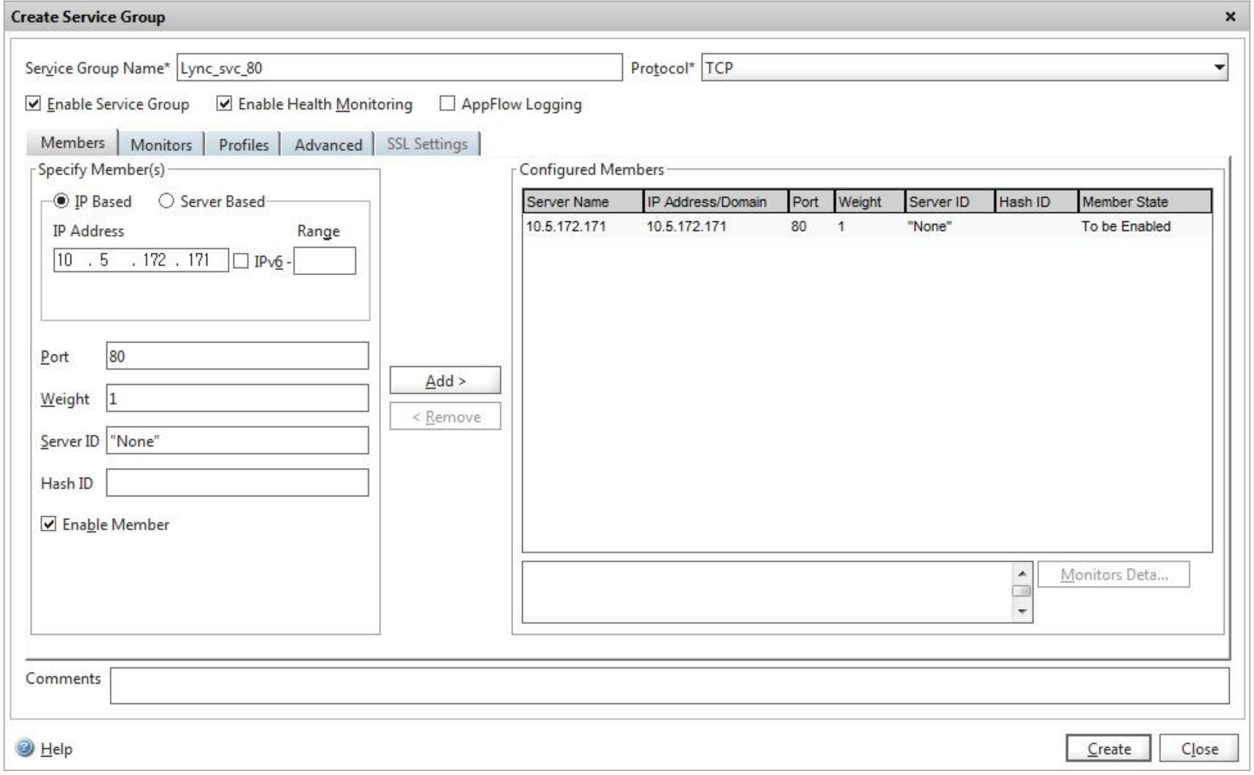
Available

Monitors
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_5060
lync_5061
lync_80

Configured

Monitors	Weight	State
lync_443	1	☑

Set **Service Group Name** to **Lync_svc_80**, **Protocol** to **TCP**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group

Service Group Name* Lync_svc_80 Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring □ AppFlow Logging

Members | Monitors | Profiles | Advanced | SSL Settings

Specify Member(s)

● IP Based ○ Server Based

IP Address: 10 . 5 . 172 . 171 □ IPv6 - Range:

Port: 80

Weight: 1

Server ID: "None"

Hash ID:

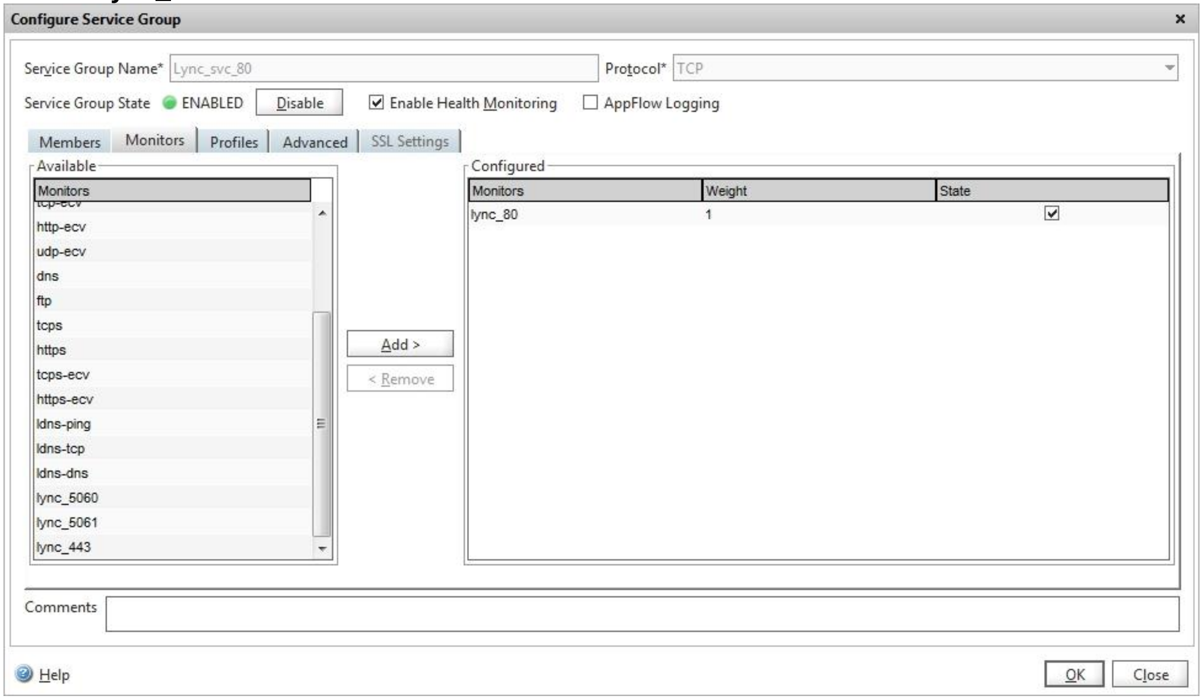
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.171	10.5.172.171	80	1	"None"		To be Enabled

Comments:

Choose **lync_80** from **Monitors** tab. Then **Create**.



Configure Service Group

Service Group Name* Lync_svc_80 Protocol* TCP

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

Members | Monitors | Profiles | Advanced | SSL Settings

Available

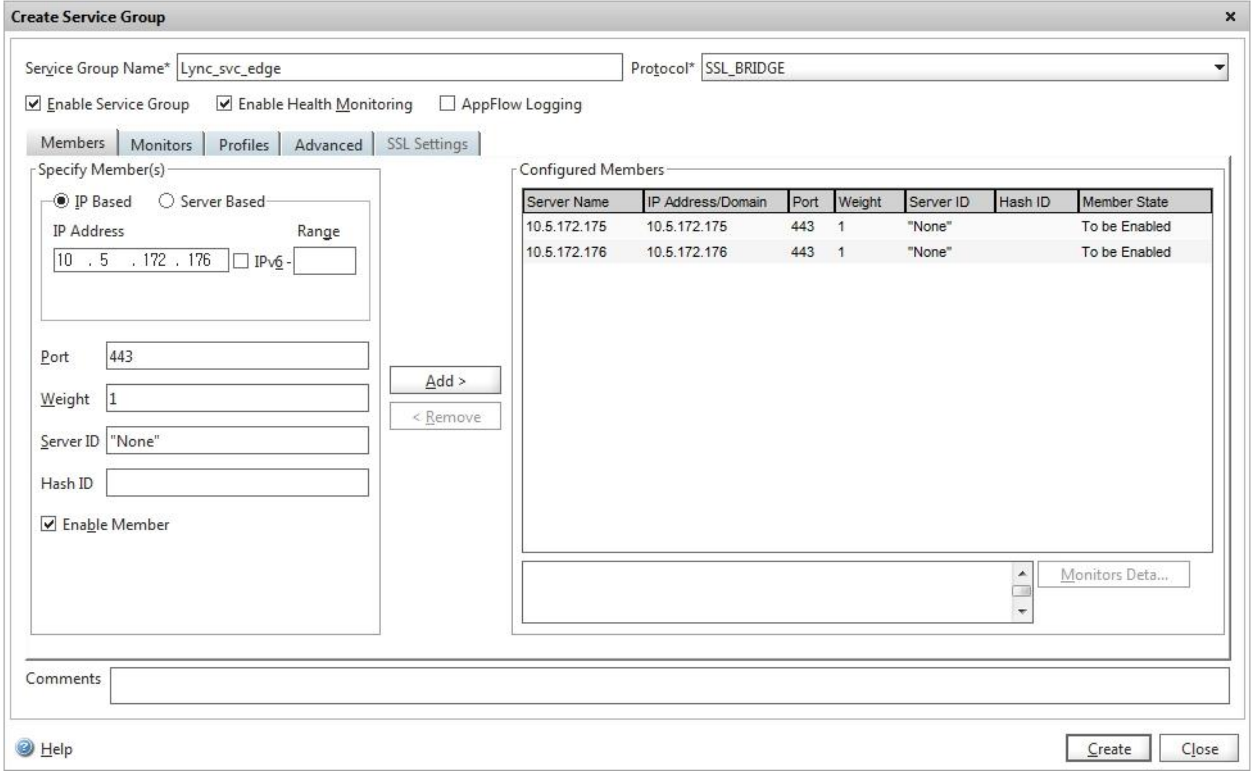
Monitors
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_5060
lync_5061
lync_443

Configured

Monitors	Weight	State
lync_80	1	☑

Comments:

Set **Service Group Name** to **Lync_svc_edge**, **Protocol** to **SSL_BRIDGE**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group

Service Group Name* Lync_svc_edge   Protocol* SSL_BRIDGE

☑ Enable Service Group   ☑ Enable Health Monitoring   □ AppFlow Logging

Specify Member(s)

● IP Based   ○ Server Based

IP Address 10 . 5 . 172 . 176   □ IPv6 -   Range

Port 443

Weight 1

Server ID "None"

Hash ID

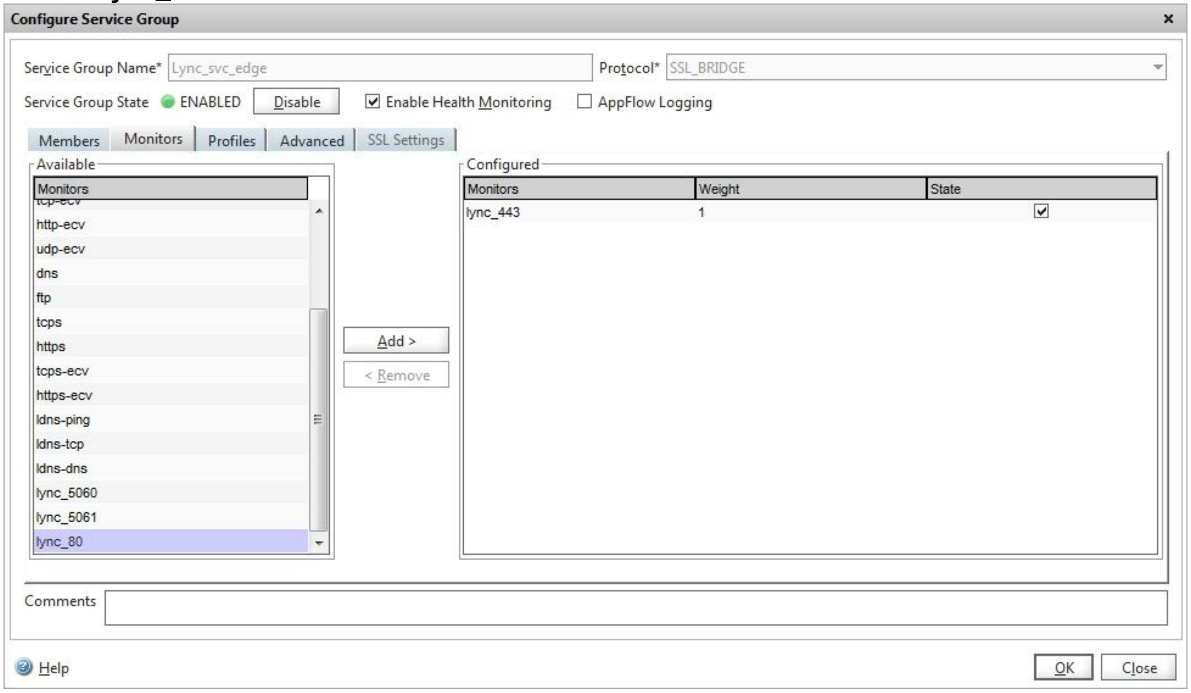
☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.175	10.5.172.175	443	1	"None"		To be Enabled
10.5.172.176	10.5.172.176	443	1	"None"		To be Enabled

Comments

Choose **lync_443** from **Monitors** tab. Then **Create**.



Configure Service Group

Service Group Name* Lync_svc_edge   Protocol* SSL_BRIDGE

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

Available

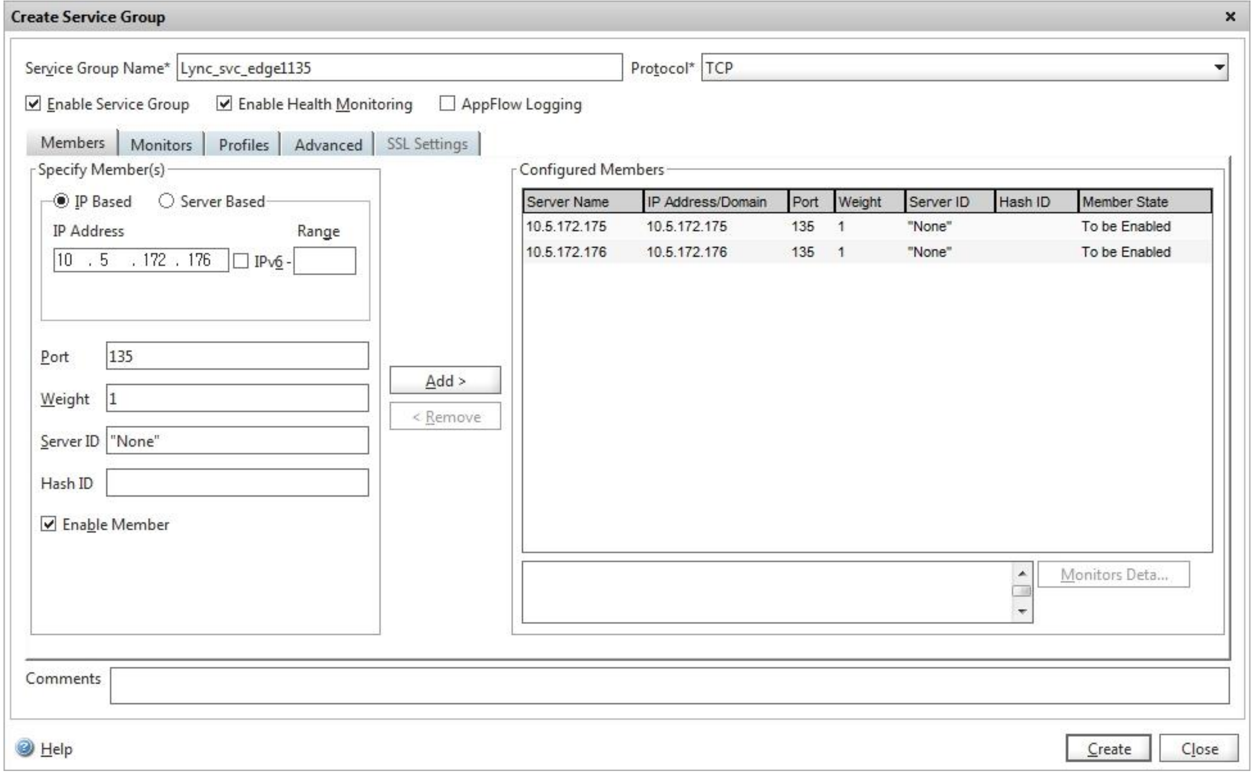
Monitors
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_5060
lync_5061
lync_80

Configured

Monitors	Weight	State
lync_443	1	☑

Comments

Set **Service Group Name** to **Lync_svc_edge1135**, **Protocol** to **TCP**. Add a physical or VM server one at a time under **Members>Specify Member(s).**



Create Service Group ×

Service Group Name* Lync_svc_edge1135 Protocol* TCP

☑ Enable Service Group ☑ Enable Health Monitoring □ AppFlow Logging

Members | Monitors | Profiles | Advanced | SSL Settings

Specify Member(s)

● IP Based ○ Server Based

IP Address 10 . 5 . 172 . 176 □ IPv6 - Range

Port 135

Weight 1

Server ID "None"

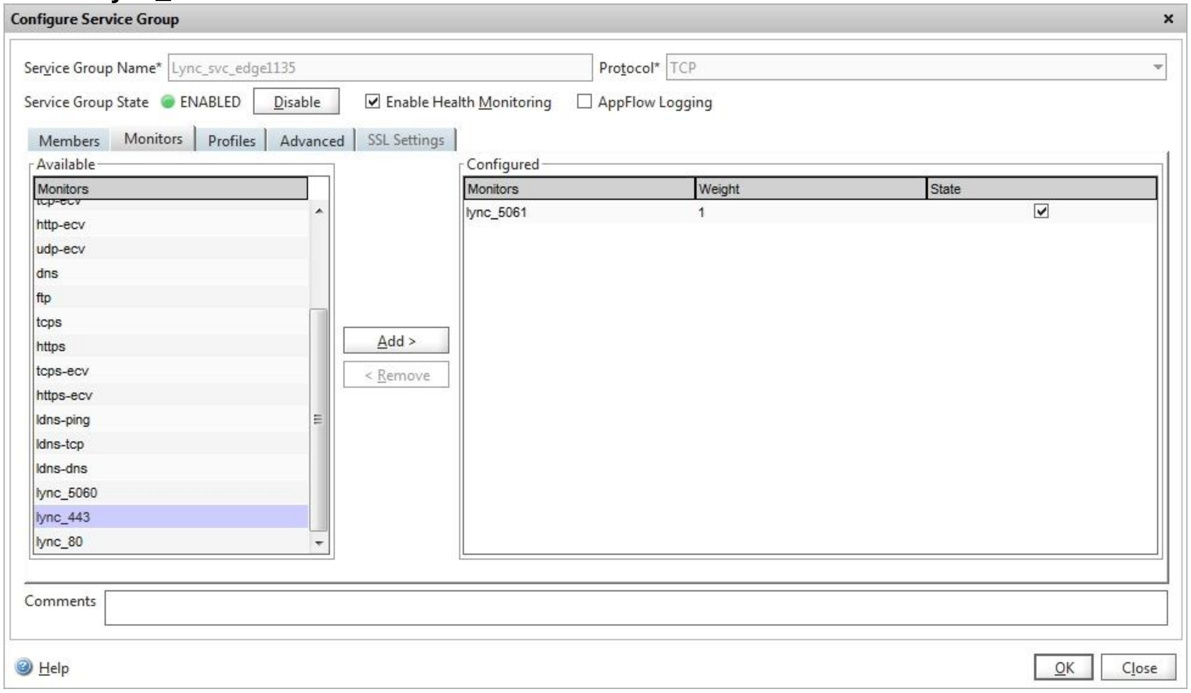
Hash ID

☑ Enable Member

Configured Members

Server Name	IP Address/Domain	Port	Weight	Server ID	Hash ID	Member State
10.5.172.175	10.5.172.175	135	1	"None"		To be Enabled
10.5.172.176	10.5.172.176	135	1	"None"		To be Enabled

Choose **lync_443** from **Monitors** tab. Then **Create**.



Configure Service Group ×

Service Group Name* Lync_svc_edge1135 Protocol* TCP

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

Members | Monitors | Profiles | Advanced | SSL Settings

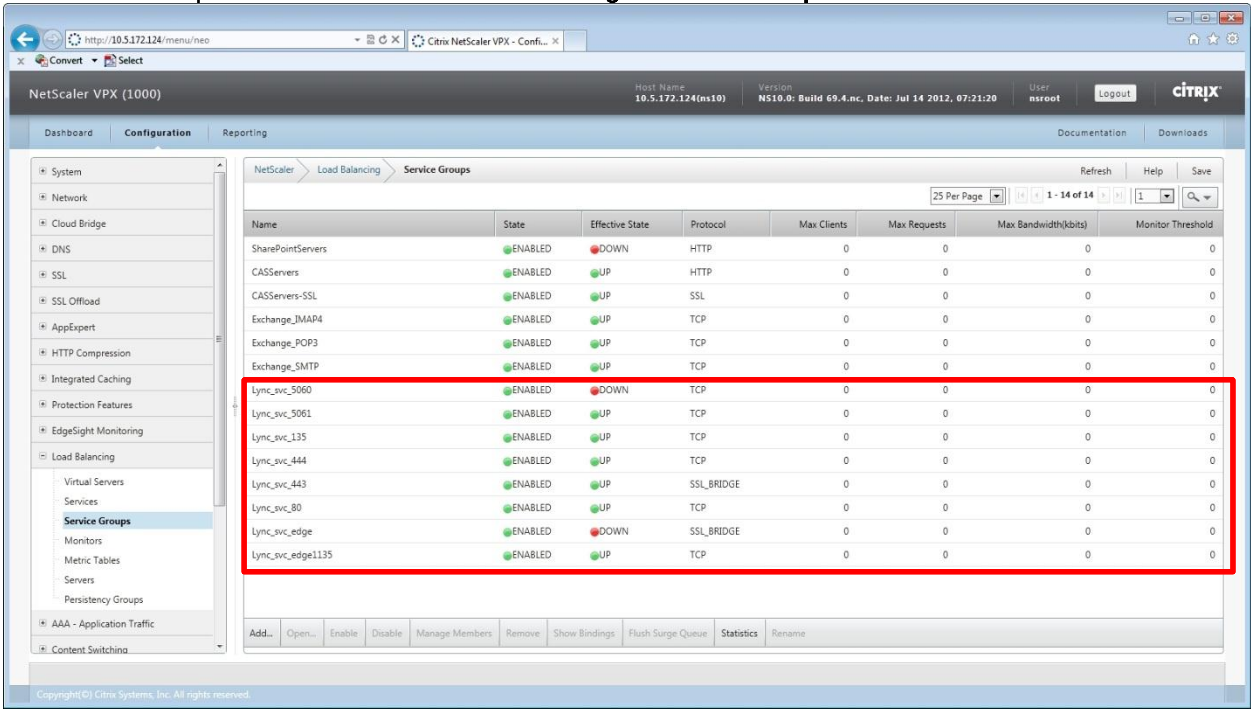
Available

Monitors
tcp-ecv
http-ecv
udp-ecv
dns
ftp
tcps
https
tcps-ecv
https-ecv
ldns-ping
ldns-tcp
ldns-dns
lync_5060
lync_443
lync_80

Configured

Monitors	Weight	State
lync_5061	1	☑

All Service Groups are listed under **Load Balancing>Service Groups**.

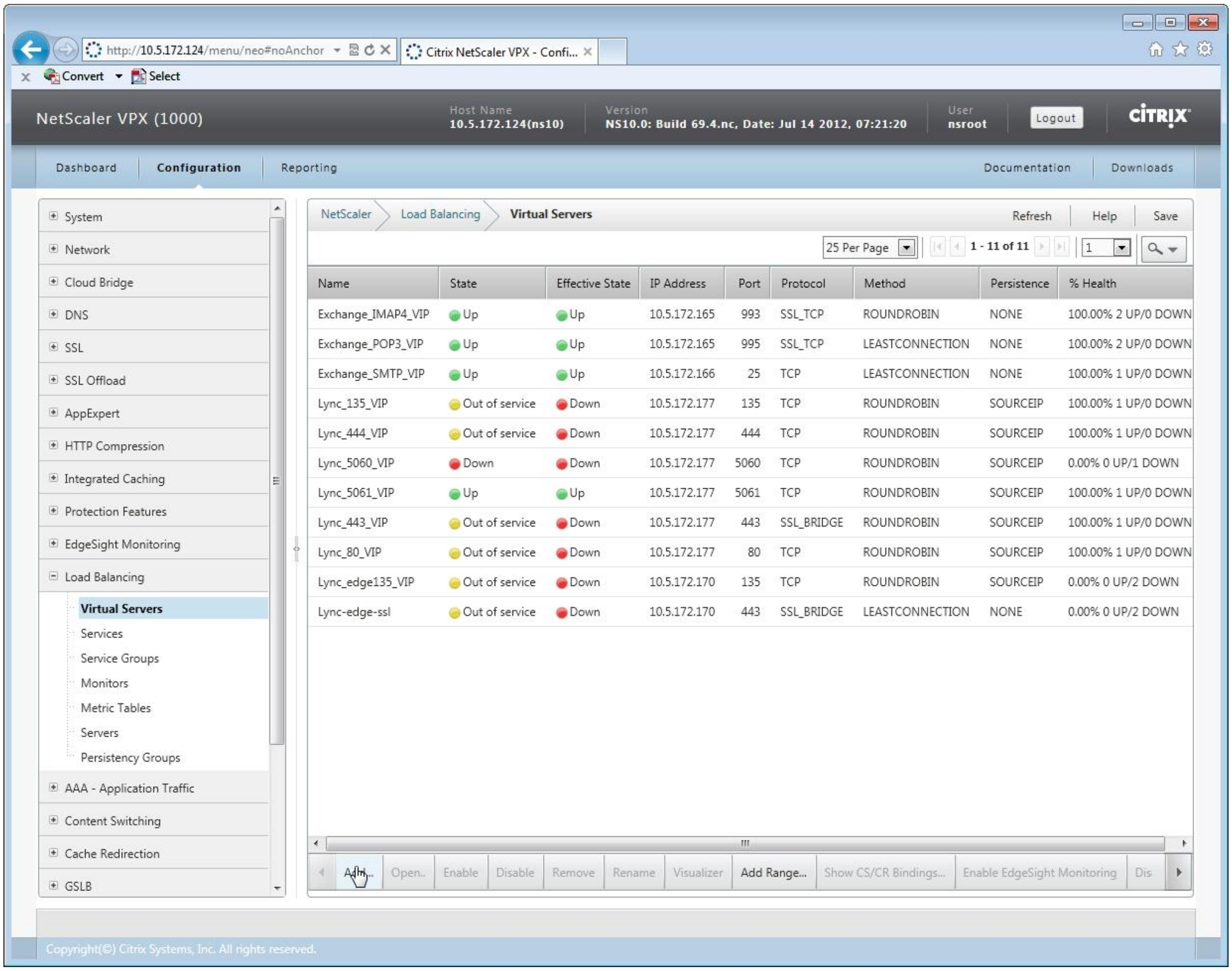


NetScaler > Load Balancing > Service Groups

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

5.6 Creating Virtual Server

Each public endpoint server using a specific service port needs to be configured as a virtual server and to bind a service group along with backend physical/VM server(s).
From NetScsaler Configuration Utility navigation menu, choose **Virtual Servers** under **Load Balancing** menu. Click **Add**.



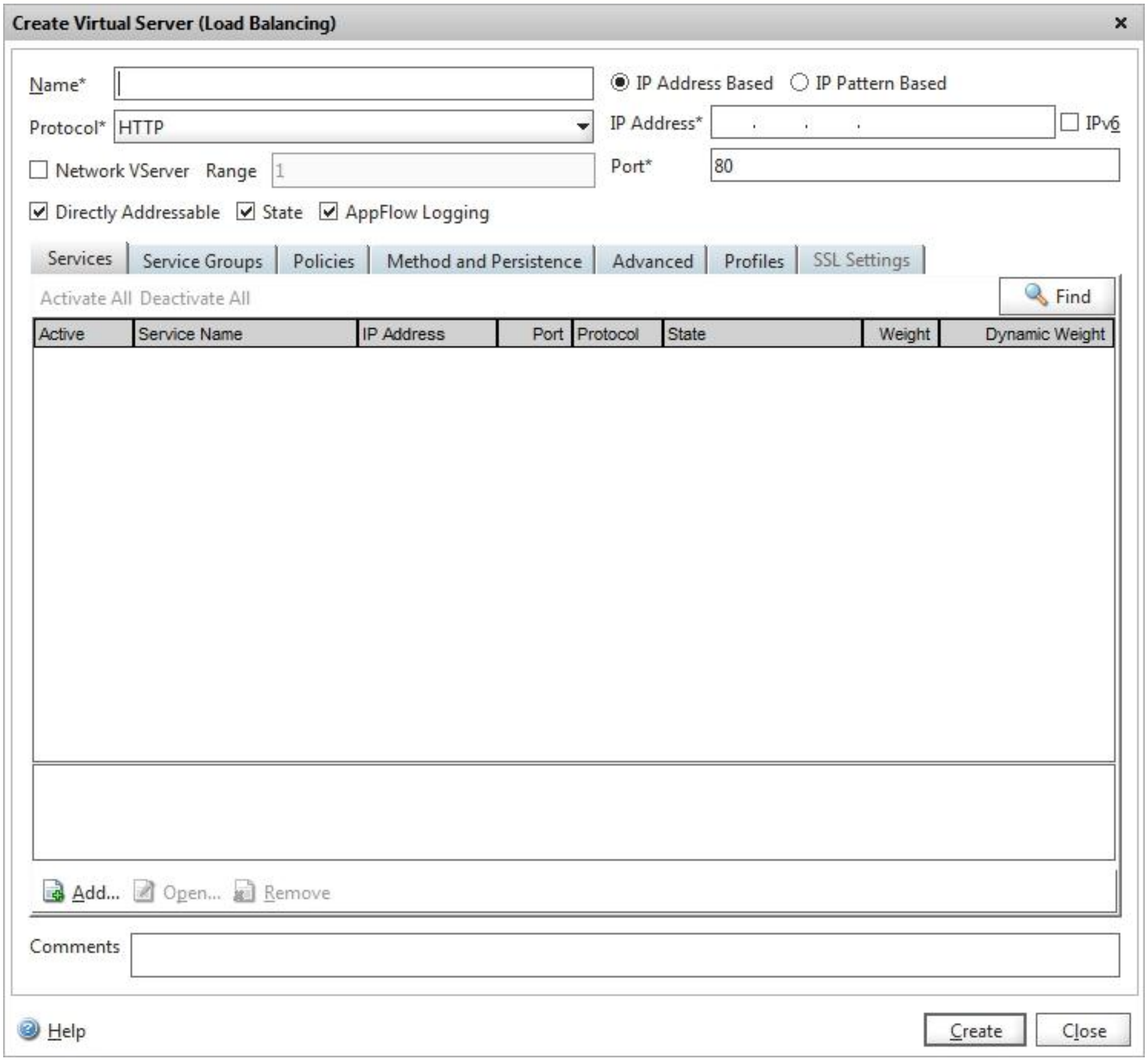
Host Name
10.5.172.124(ns10)

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

User
nsroot

Name	State	Effective State	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	● Out of service	● Down	10.5.172.177	135	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_444_VIP	● Out of service	● Down	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	● Out of service	● Down	10.5.172.177	443	SSL_BRIDGE	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_80_VIP	● Out of service	● Down	10.5.172.177	80	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_edge135_VIP	● Out of service	● Down	10.5.172.170	135	TCP	ROUNDROBIN	SOURCEIP	0.00% 0 UP/2 DOWN
Lync-edge-ssl	● Out of service	● Down	10.5.172.170	443	SSL_BRIDGE	LEASTCONNECTION	NONE	0.00% 0 UP/2 DOWN

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



Create Virtual Server (Load Balancing)

Name*

Protocol* HTTP

□ Network VServer Range 1

☑ Directly Addressable ☑ State ☑ AppFlow Logging

● IP Address Based ○ IP Pattern Based

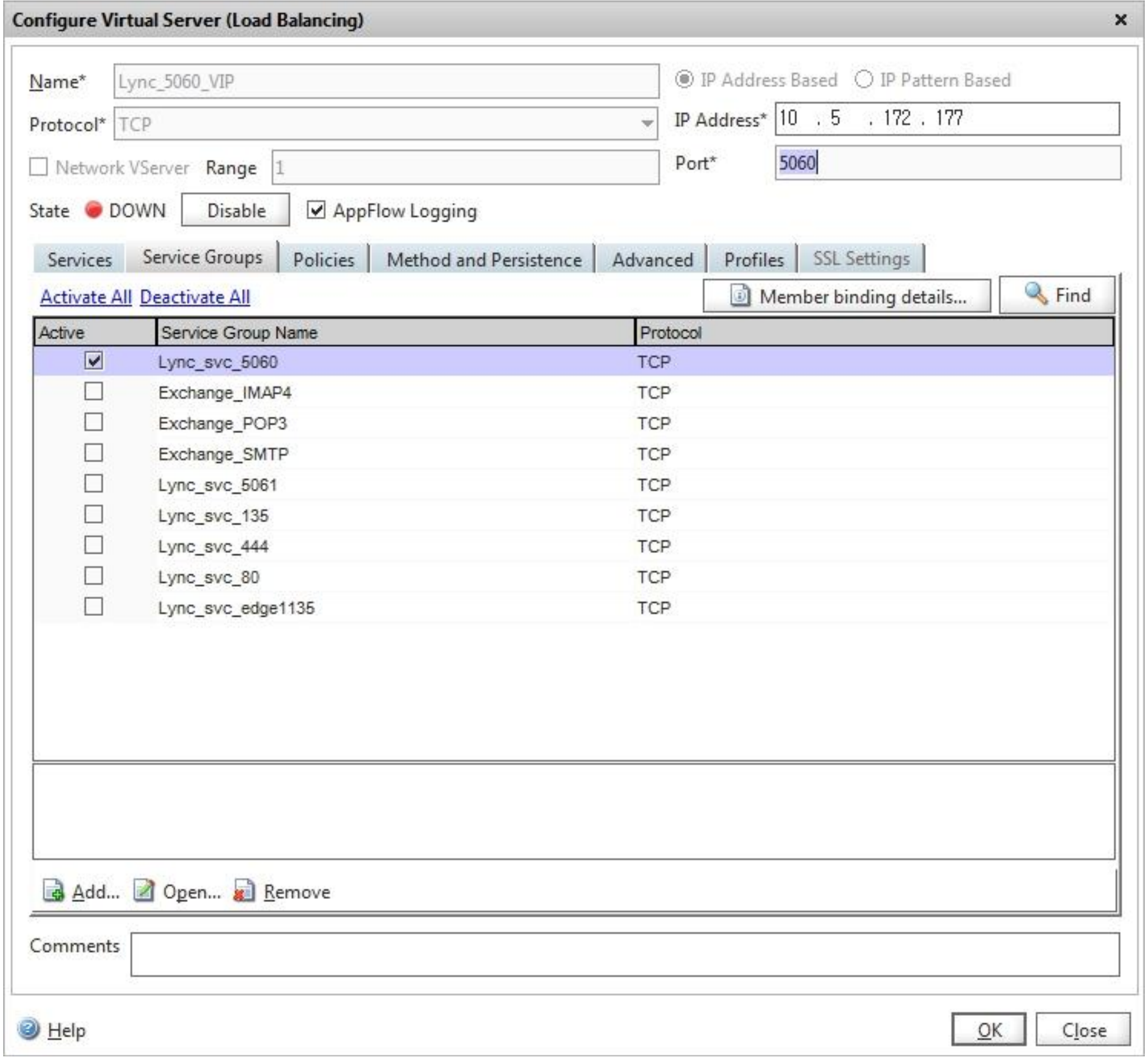
IP Address* . . . □ IPv6

Port* 80

Active	Service Name	IP Address	Port	Protocol	State	Weight	Dynamic Weight

Comments

Set **Name** to **Lync_5060_VIP**. **IP Address** to **10.5.172.177**. **Port** to **5060**. Choose **Lync_svc_5060** service group from **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Lync_5060_VIP

Protocol* TCP

● IP Address Based ○ IP Pattern Based

IP Address* 10 . 5 . 172 . 177

Port* 5060

□ Network VServer Range 1

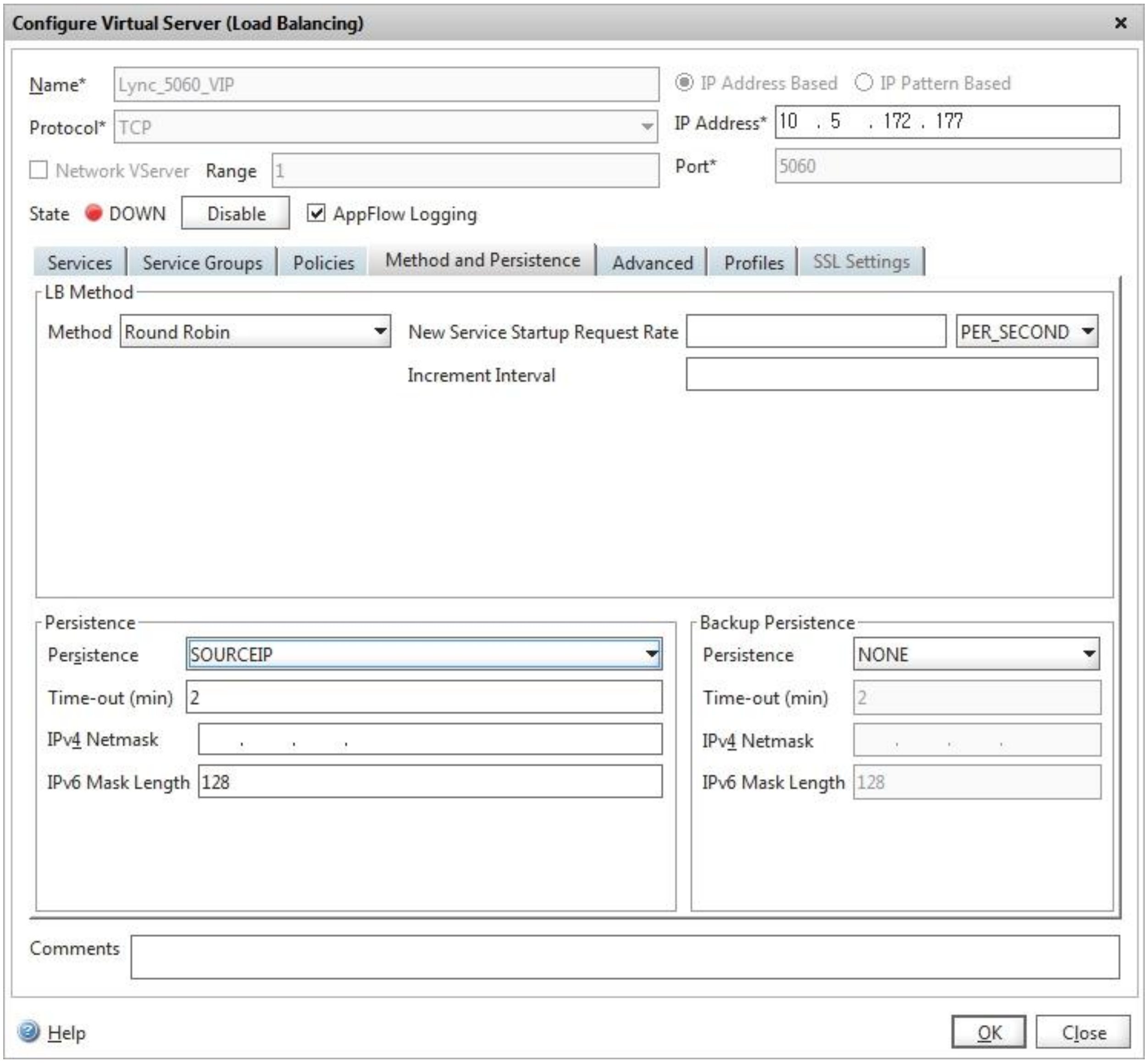
State ● DOWN

☑ AppFlow Logging

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

Comments

Set **Persistence** to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_5060_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

□ Network VServer Range 1

Port* 5060

State ● DOWN Disable ☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

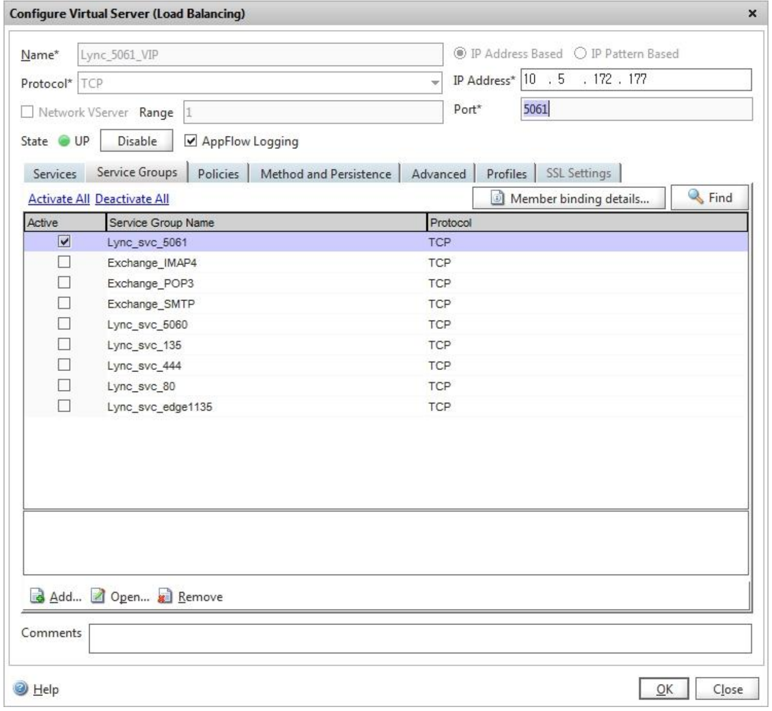
Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Set **Name** to **Lync_5061_VIP**. **IP Address** to **10.5.172.177**. **Port** to **5061**. Choose **Lync_svc_5061** service group from **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Lync_5061_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

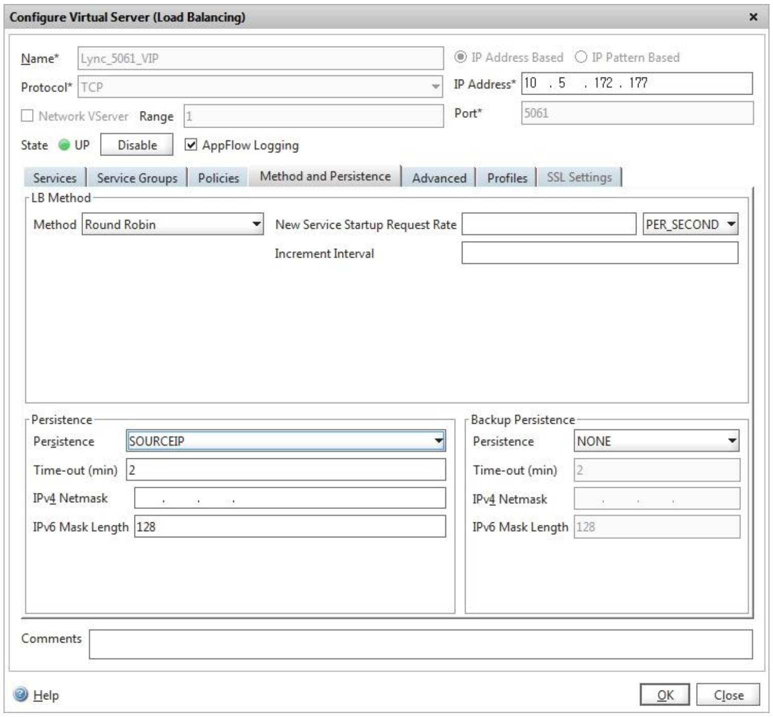
□ Network VServer Range 1

Port* 5061

State ● UP Disable ☑ AppFlow Logging

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

Set **Persistence** to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_5061_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

□ Network VServer Range 1

Port* 5061

State ● UP Disable ☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

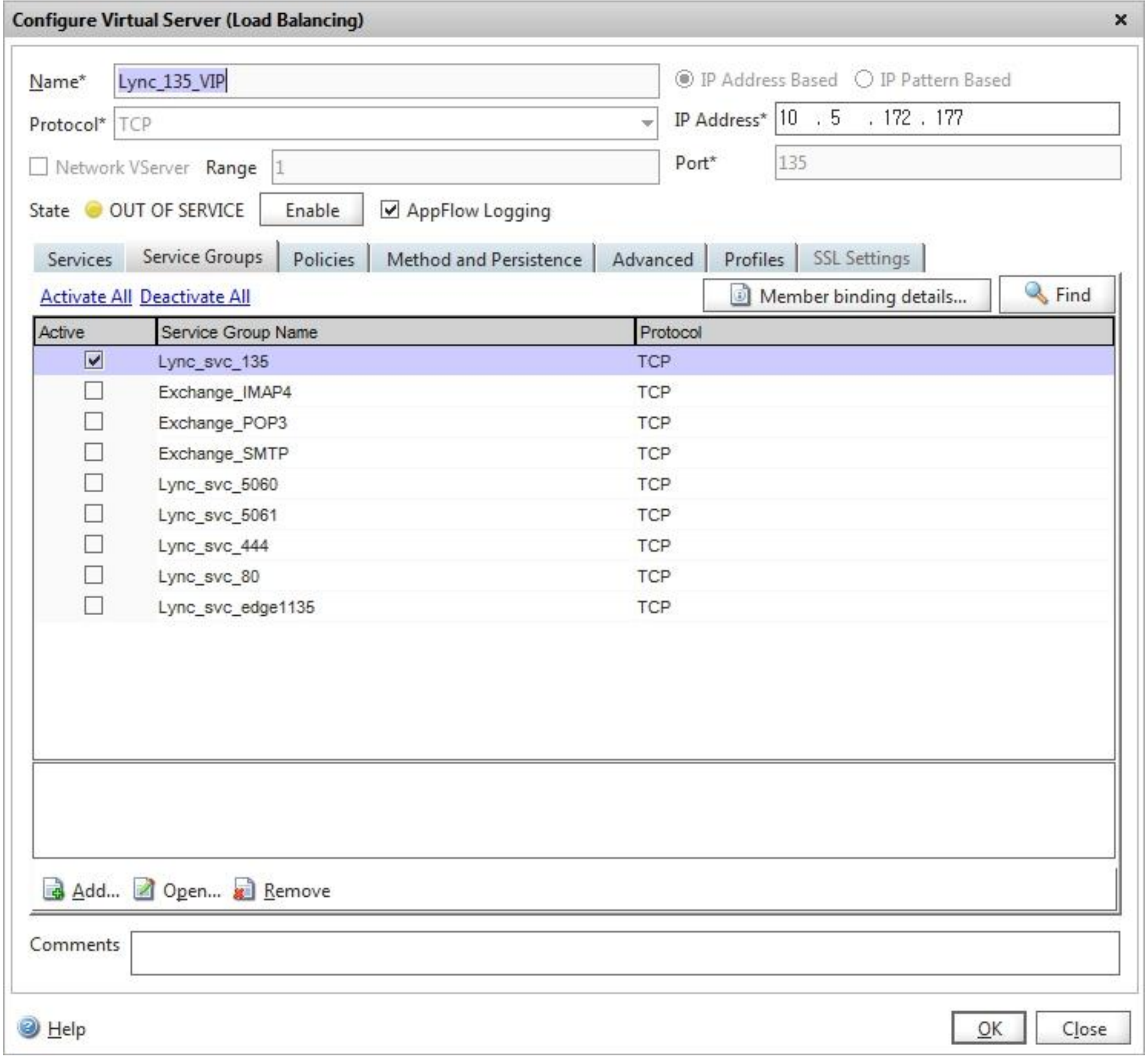
Persistence NONE

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Set **Name** to **Lync_135_VIP**. **IP Address** to **10.5.172.177**. **Port** to **135**. Choose **Lync_svc_135** service group from **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Lync_135_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

☐ Network VServer Range 1

Port* 135

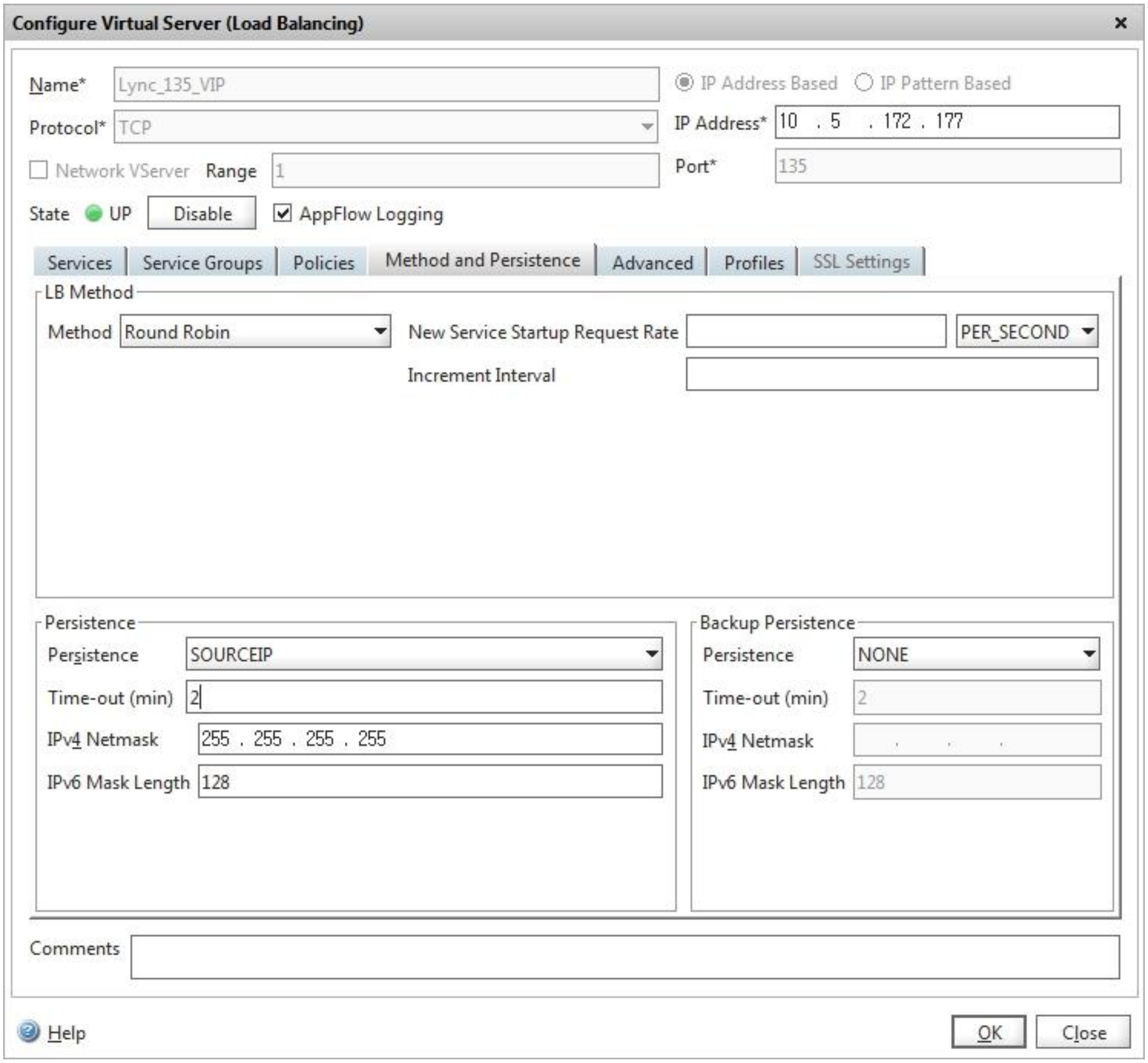
State OUT OF SERVICE

☑ AppFlow Logging

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

Comments

Set **Persistence** to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_135_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

□ Network VServer Range 1

Port* 135

State UP Disable

☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask 255 . 255 . 255 . 255

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

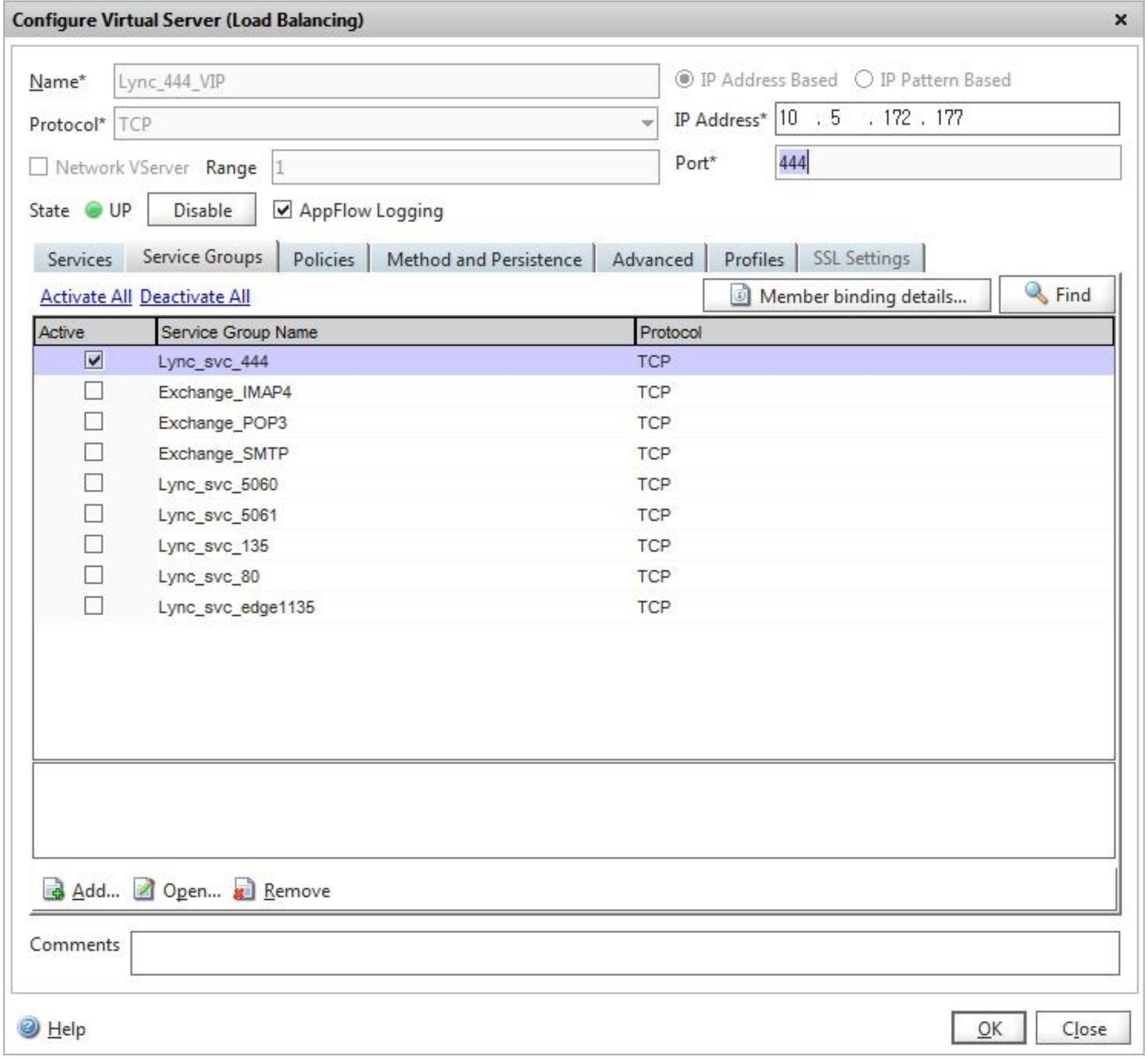
Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Set **Name** to **Lync_444_VIP**. **IP Address** to **10.5.172.177**. **Port** to **444**. Choose **Lync_svc_444** service group from **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Lync_444_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

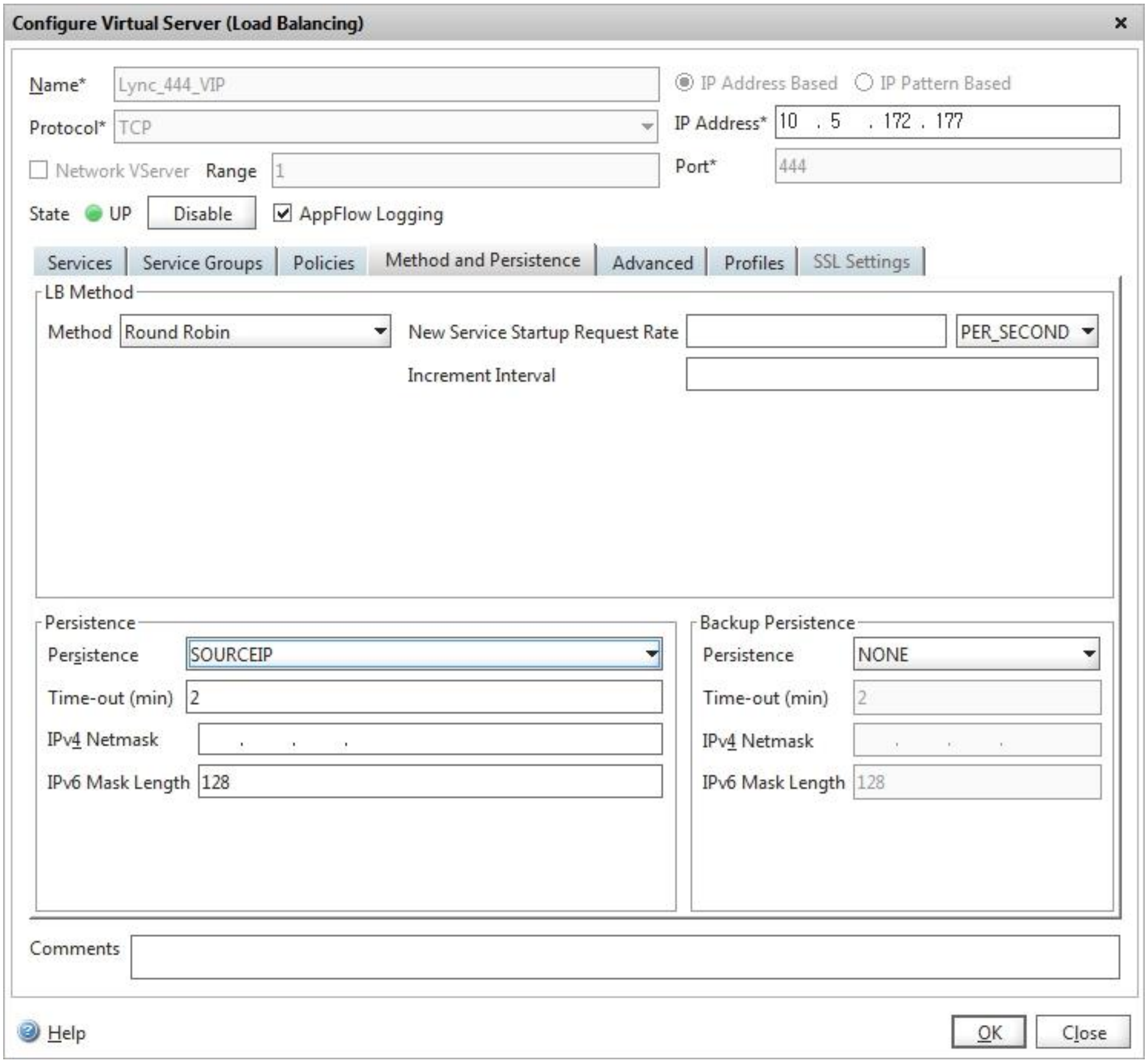
□ Network VServer Range 1

Port* 444

State UP Disable ☑ AppFlow Logging

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

Persistence to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_444_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

□ Network VServer Range 1

Port* 444

State UP

☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

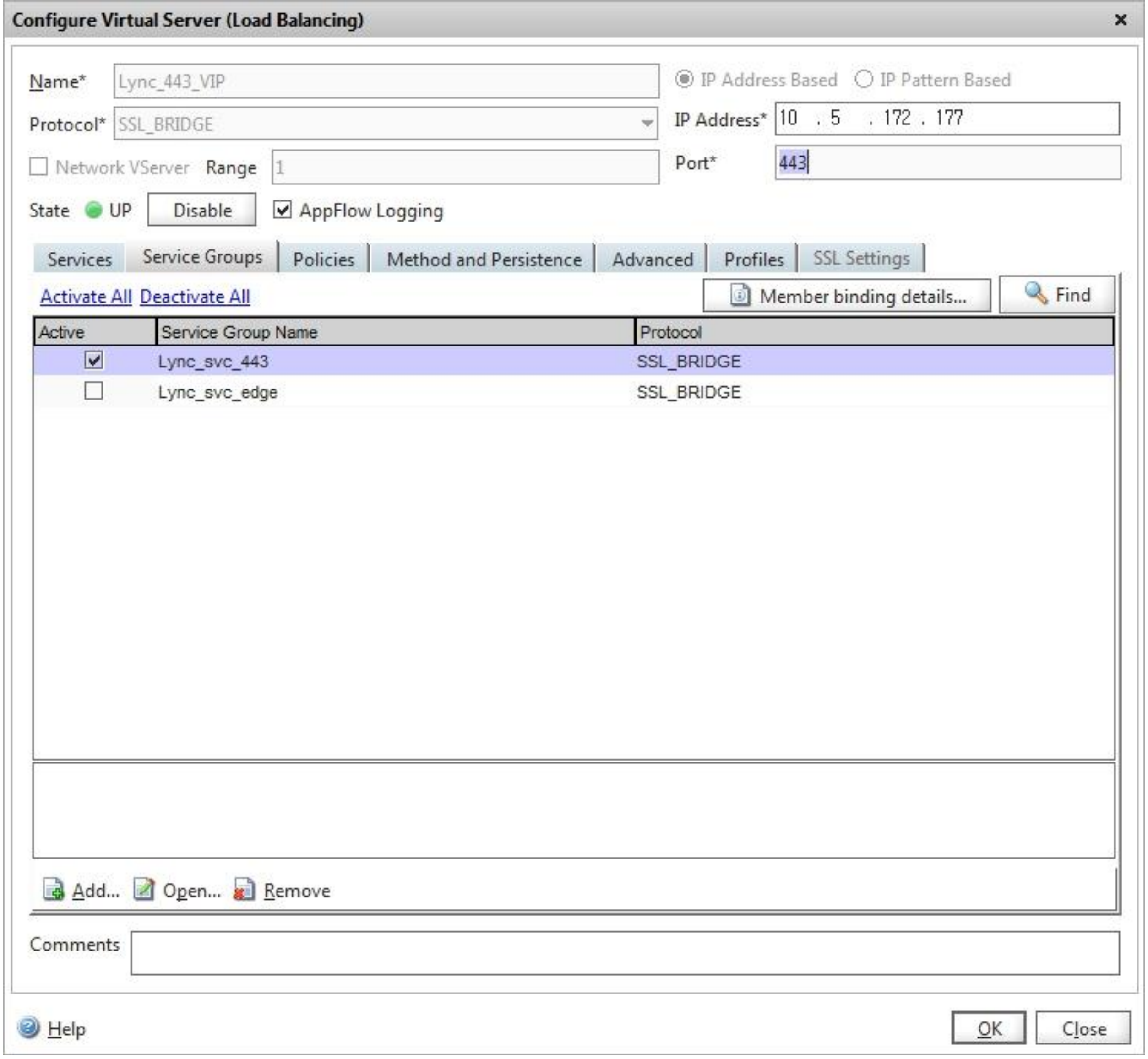
Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Set **Name** to **Lync_443_VIP**. **IP Address** to **10.5.172.177**. **Port** to **443**. Choose **Lync_svc_444** service group from **Service Groups** tab.



Configure Virtual Server (Load Balancing)

Name* Lync_443_VIP

Protocol* SSL_BRIDGE

● IP Address Based ○ IP Pattern Based

IP Address* 10 . 5 . 172 . 177

Port* 443

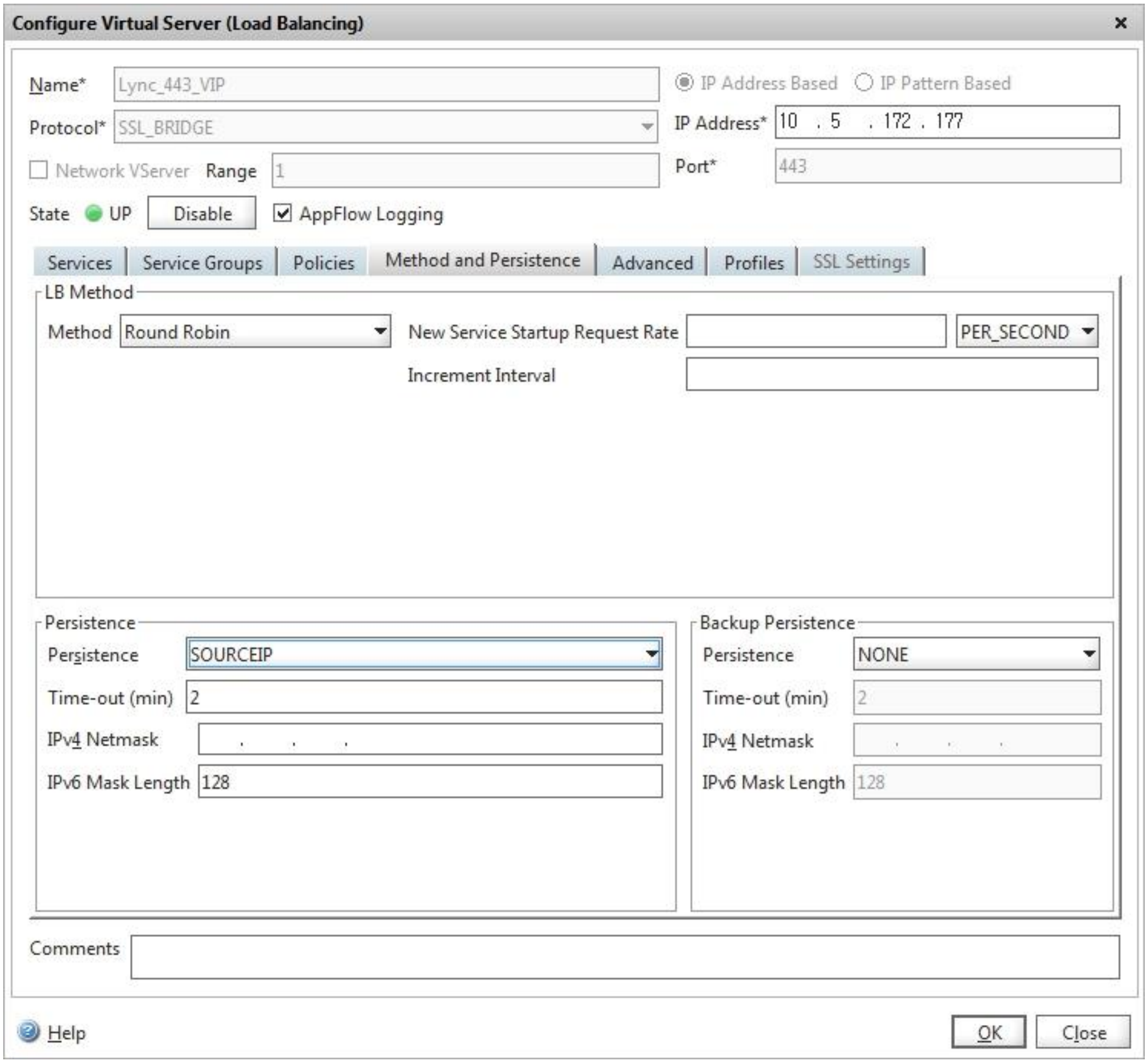
□ Network VServer Range 1

State ● UP Disable ☑ AppFlow Logging

Active	Service Group Name	Protocol
☑	Lync_svc_443	SSL_BRIDGE
□	Lync_svc_edge	SSL_BRIDGE

Comments

Persistence to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_443_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_BRIDGE

IP Address* 10 . 5 . 172 . 177

□ Network VServer Range 1

Port* 443

State UP Disable

☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

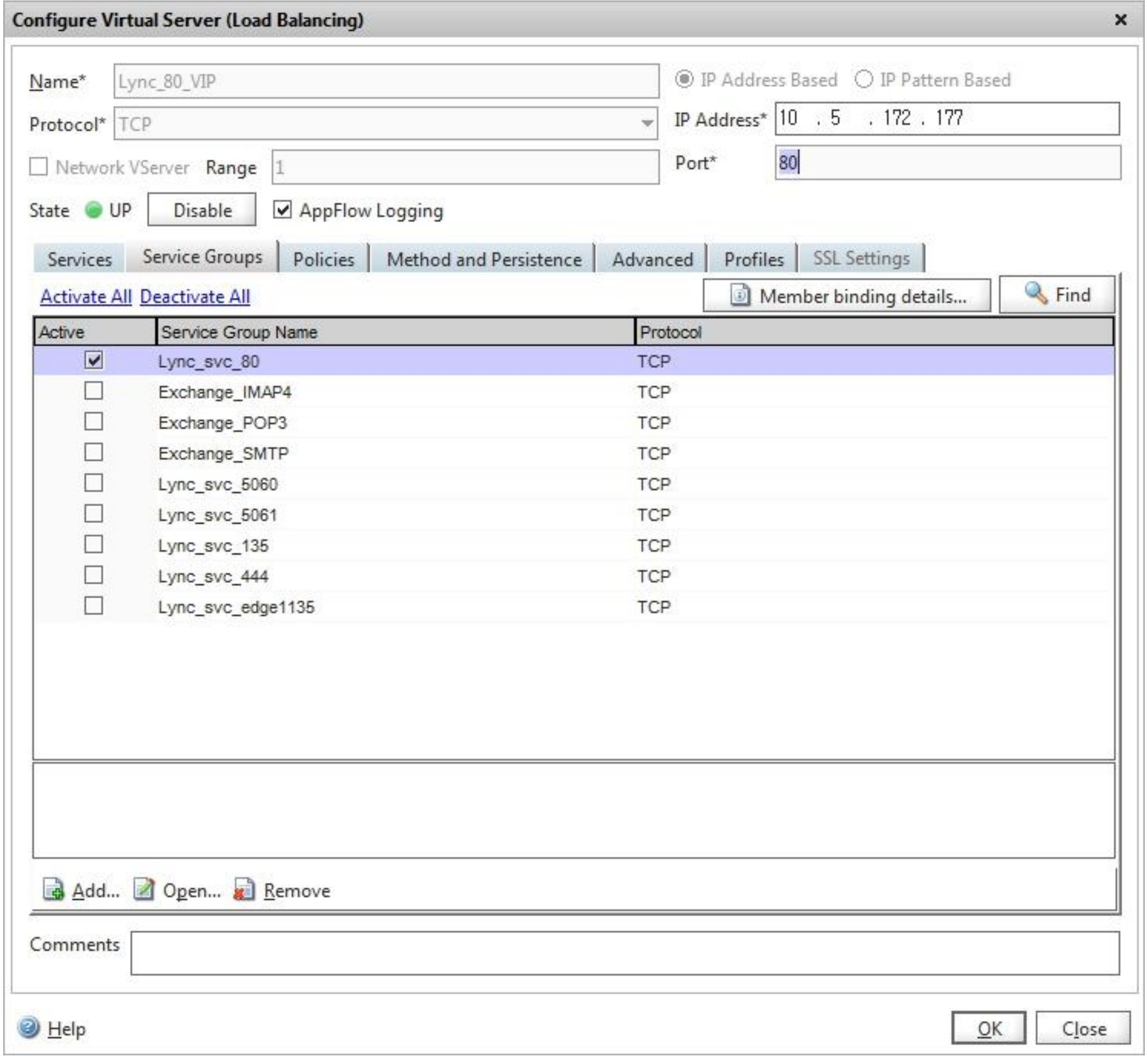
Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Set **Name** to **Lync_80_VIP**. **IP Address** to **10.5.172.177**. **Port** to **80**. Choose **Lync_svc_80** service group from **Service Groups** tab.



Name* Lync_80_VIP

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

Port* 80

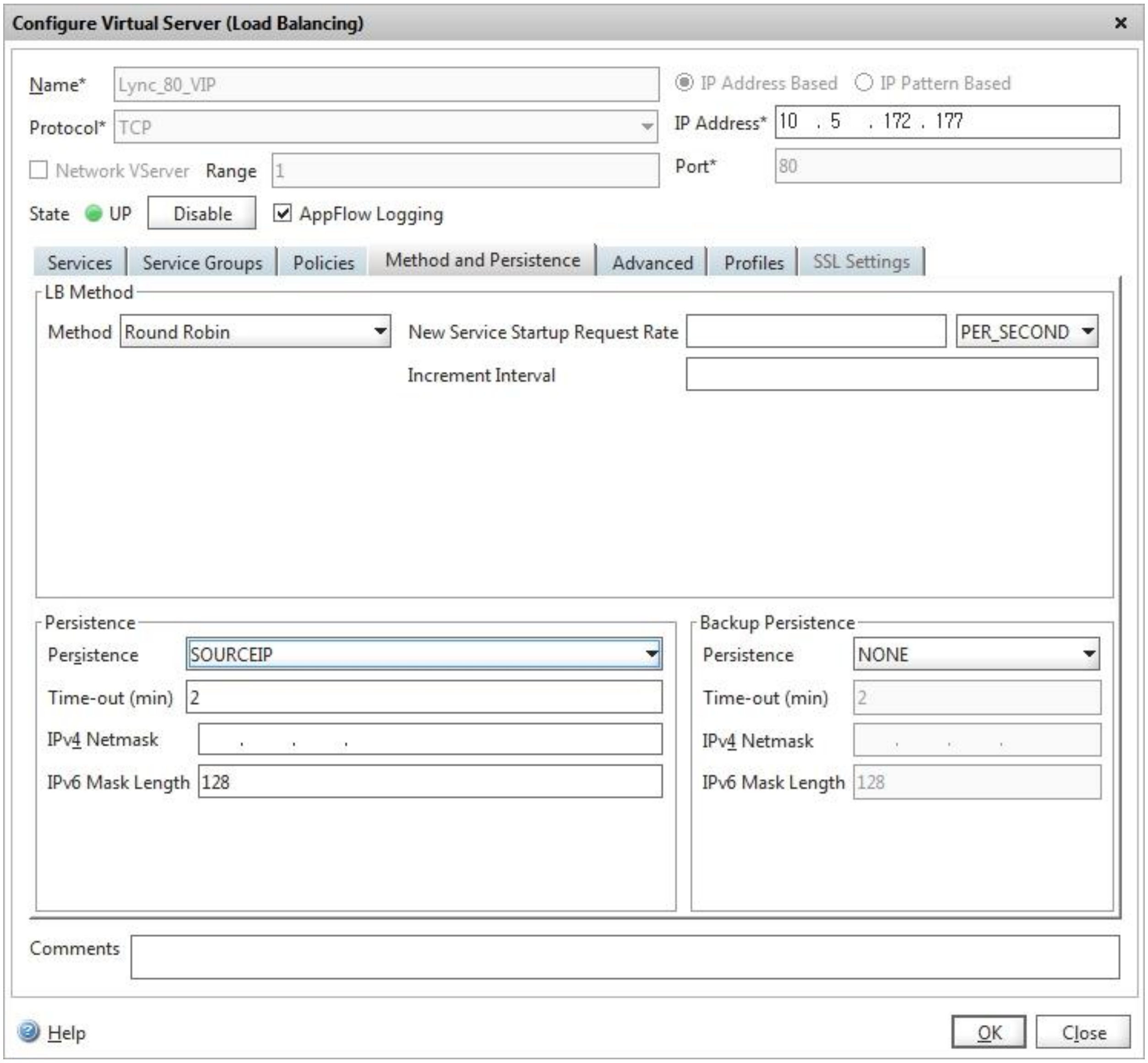
Range 1

State UP

☑ AppFlow Logging

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

Persistence to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_80_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 177

□ Network VServer Range 1

Port* 80

State UP Disable ☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

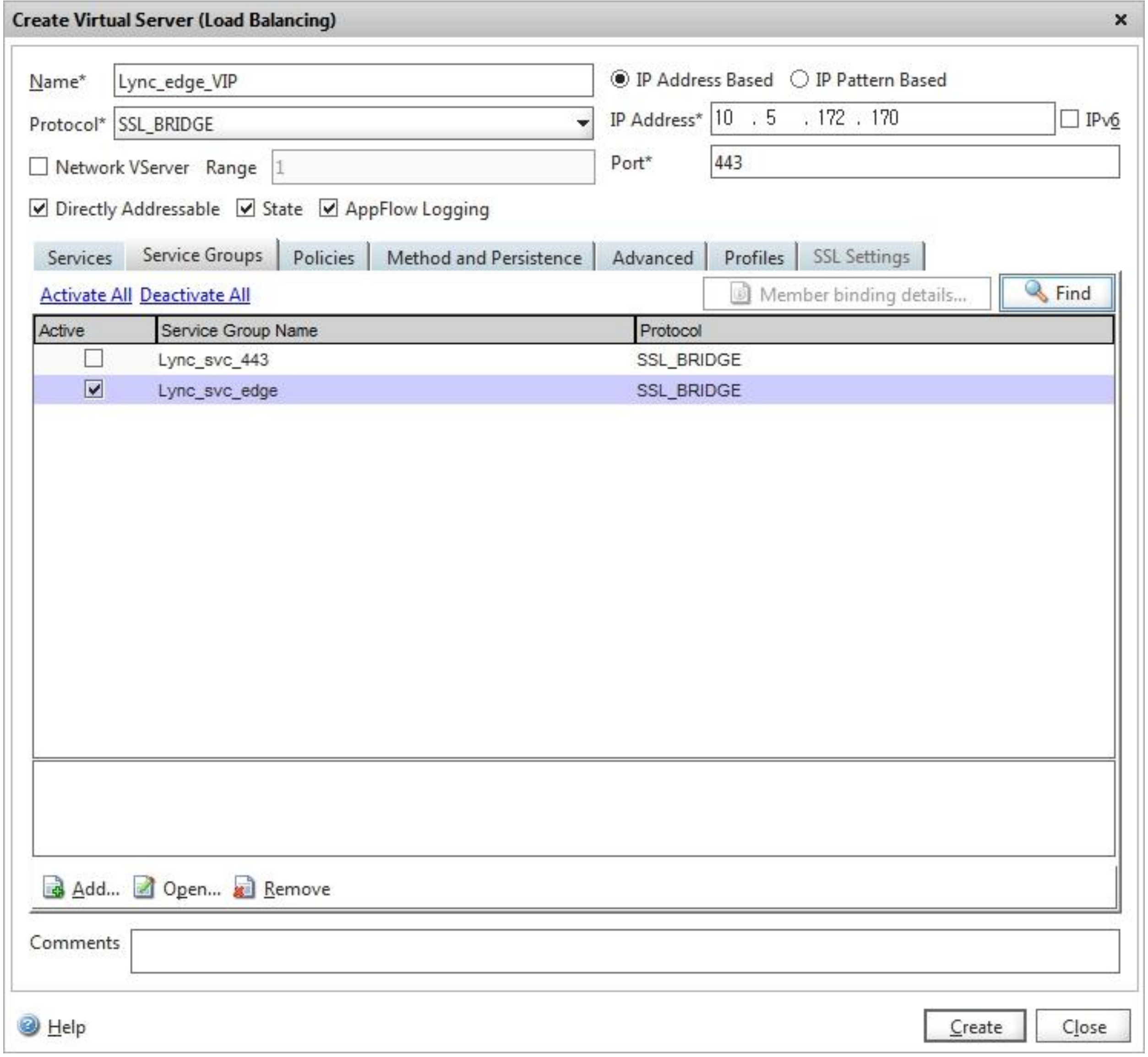
Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Set **Name** to **Lync_edge_VIP**. **IP Address** to **10.5.172.170**. **Port** to **443**. Choose **Lync_svc_edge** service group from **Service Groups** tab.



Create Virtual Server (Load Balancing)

Name* Lync_edge_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_BRIDGE

IP Address* 10 . 5 . 172 . 170 □ IPv6

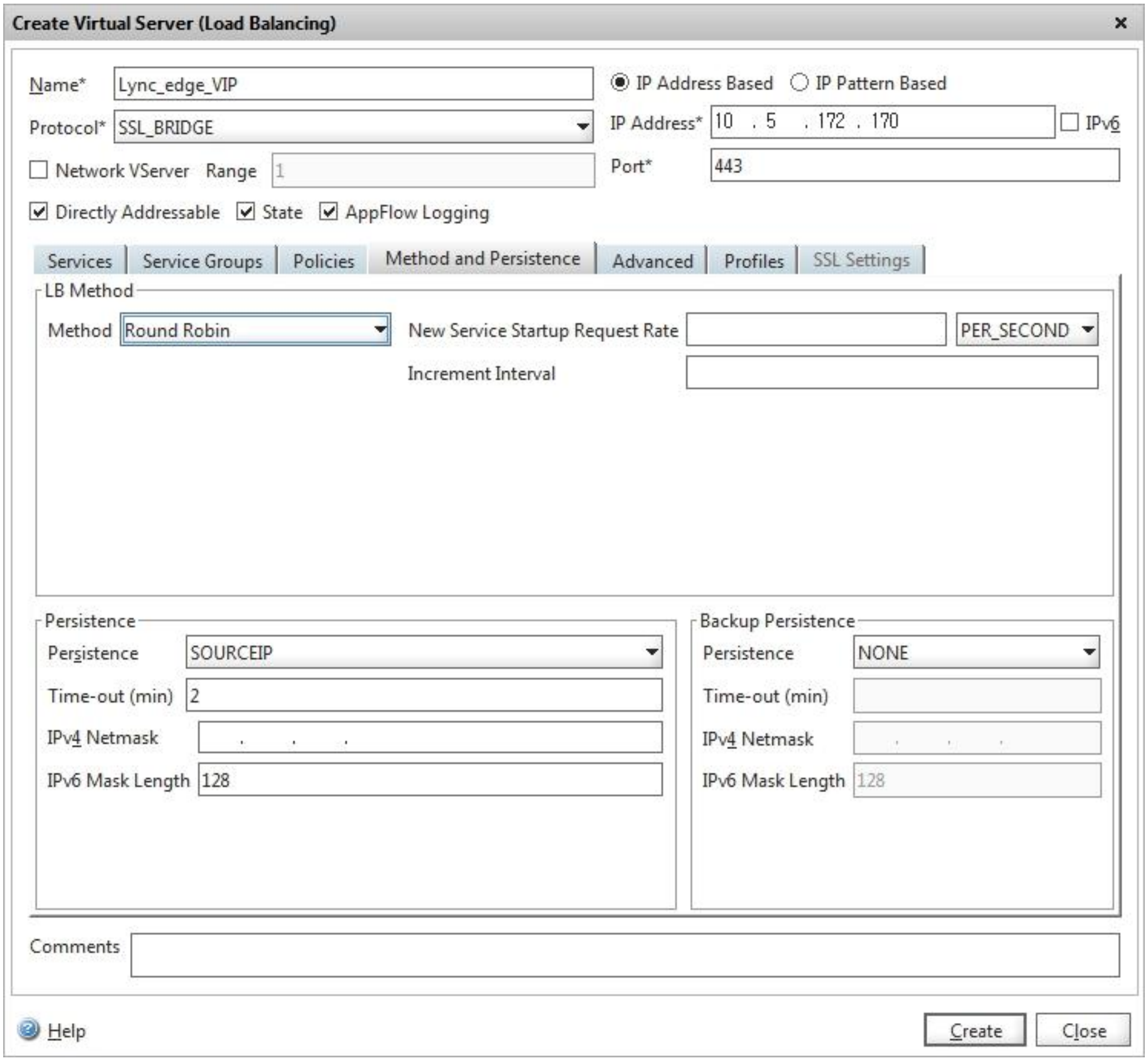
□ Network VServer Range 1

Port* 443

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Active	Service Group Name	Protocol
□	Lync_svc_443	SSL_BRIDGE
☑	Lync_svc_edge	SSL_BRIDGE

Persistence to **SOURCEIP** under **Method and Persistence** tab



Create Virtual Server (Load Balancing)

Name* Lync_edge_VIP

● IP Address Based ○ IP Pattern Based

Protocol* SSL_BRIDGE

IP Address* 10 . 5 . 172 . 170 □ IPv6

□ Network VServer Range 1

Port* 443

☑ Directly Addressable ☑ State ☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

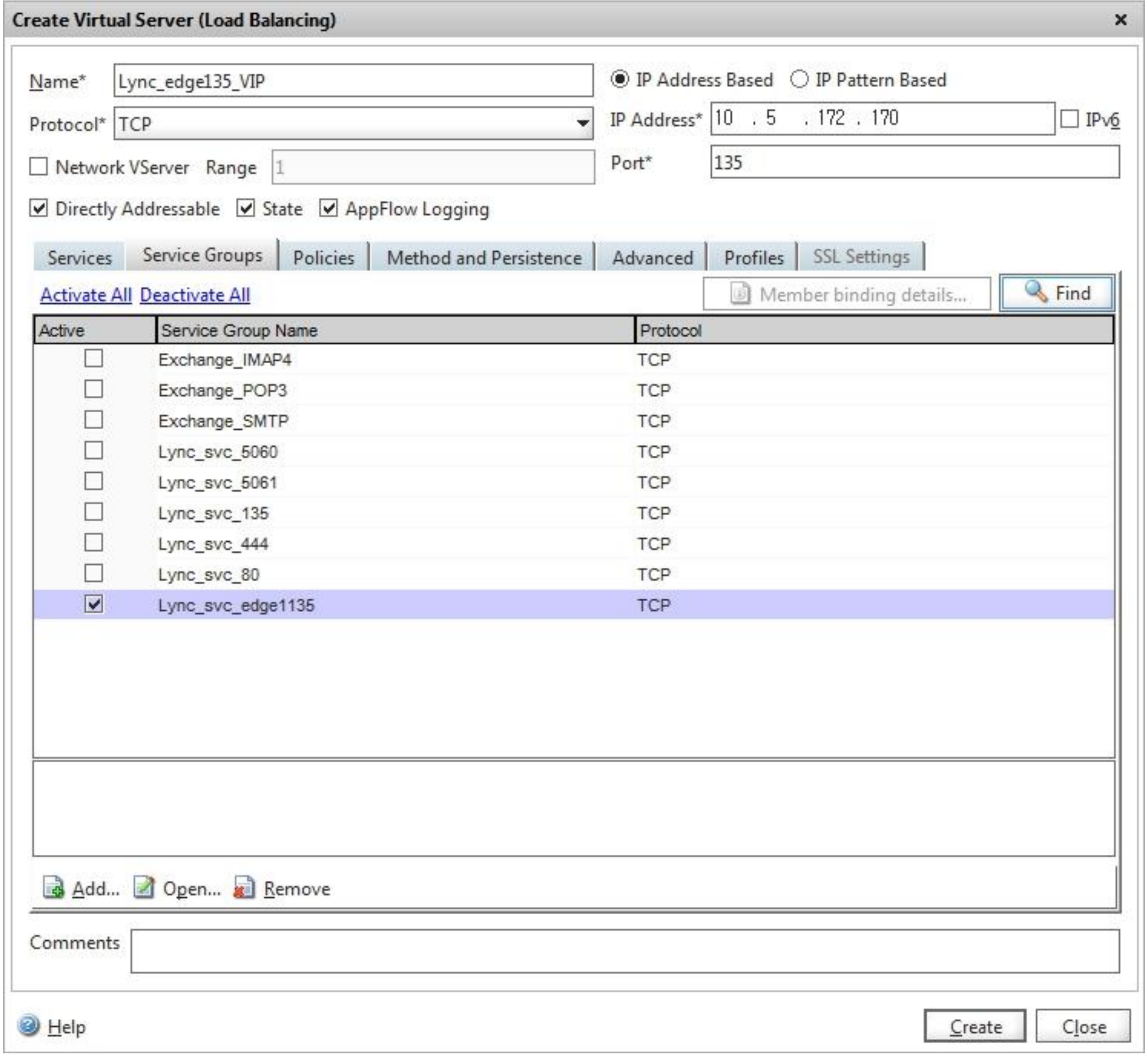
Time-out (min)

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

Set **Name** to **Lync_edge135_VIP**. **IP Address** to **10.5.172.170**. **Port** to **135**. Choose **Lync_svc_edge1135** service group from **Service Groups** tab.



Create Virtual Server (Load Balancing)

Name* Lync_edge135_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 170 □ IPv6

□ Network VServer Range 1

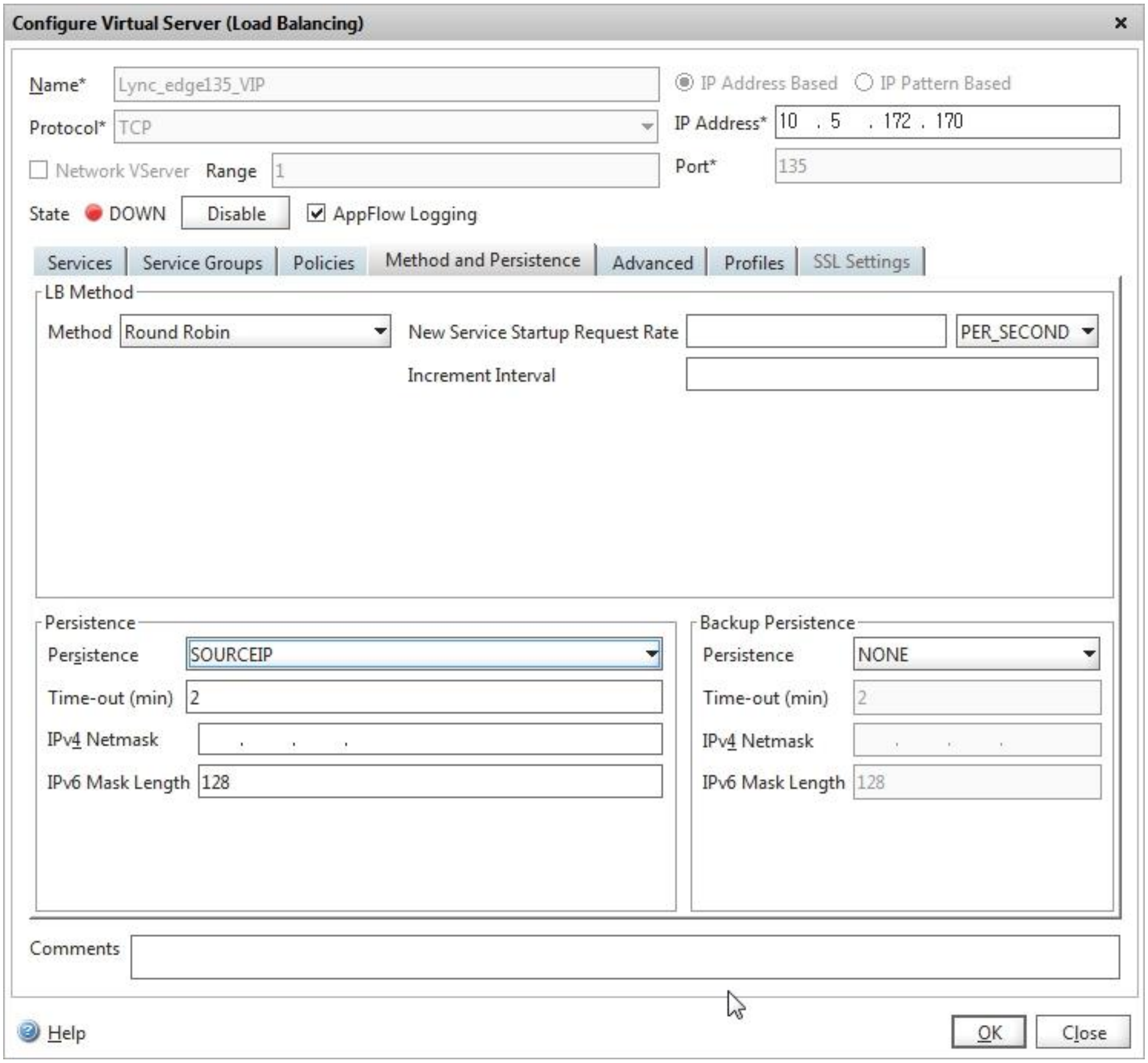
Port* 135

☑ Directly Addressable ☑ State ☑ AppFlow Logging

Active	Service Group Name	Protocol
□	Exchange_IMAP4	TCP
□	Exchange_POP3	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

Comments

Persistence to **SOURCEIP** under **Method and Persistence** tab



Configure Virtual Server (Load Balancing)

Name* Lync_edge135_VIP

● IP Address Based ○ IP Pattern Based

Protocol* TCP

IP Address* 10 . 5 . 172 . 170

□ Network VServer Range 1

Port* 135

State DOWN Disable ☑ AppFlow Logging

LB Method

Method Round Robin

New Service Startup Request Rate PER_SECOND

Increment Interval

Persistence

Persistence SOURCEIP

Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Backup Persistence

Persistence NONE

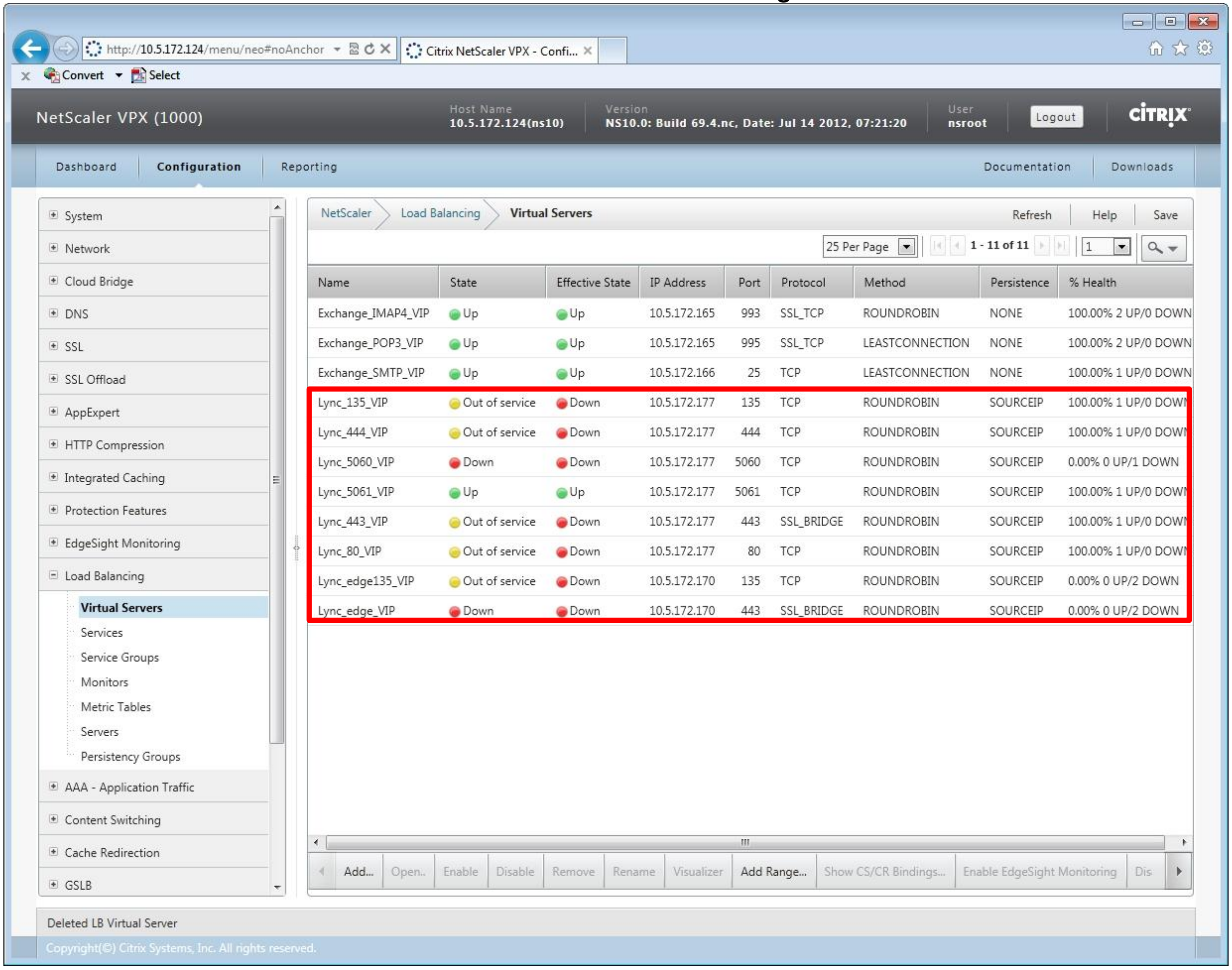
Time-out (min) 2

IPv4 Netmask . . .

IPv6 Mask Length 128

Comments

All the virtual servers created can be viewed under **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	🟡 Out of service	🔴 Down	10.5.172.177	135	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_444_VIP	🟡 Out of service	🔴 Down	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	🟡 Out of service	🔴 Down	10.5.172.177	443	SSL_BRIDGE	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_80_VIP	🟡 Out of service	🔴 Down	10.5.172.177	80	TCP	ROUNDROBIN	SOURCEIP	100.00% 1 UP/0 DOWN
Lync_edge135_VIP	🟡 Out of service	🔴 Down	10.5.172.170	135	TCP	ROUNDROBIN	SOURCEIP	0.00% 0 UP/2 DOWN
Lync_edge_VIP	🔴 Down	🔴 Down	10.5.172.170	443	SSL_BRIDGE	ROUNDROBIN	SOURCEIP	0.00% 0 UP/2 DOWN

Deleted LB Virtual Server

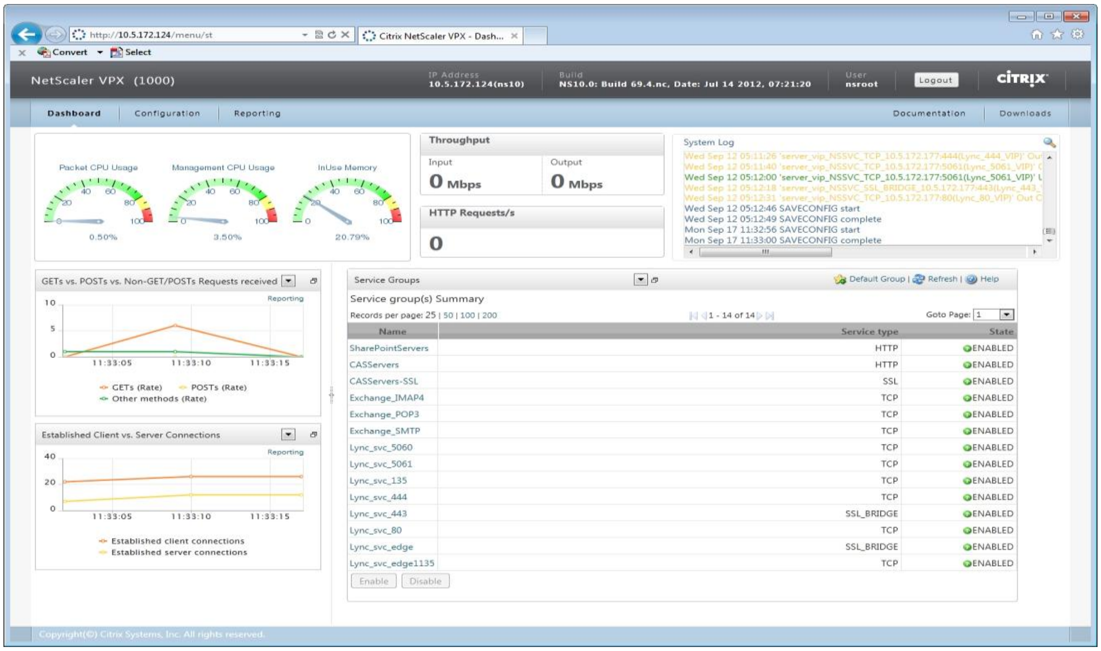
Copyright(©) Citrix Systems, Inc. All rights reserved.

6. Monitoring – NetScaler Dashboard

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

6.1 By Service Groups

Under **Service group(s) Summary**, all Lync services can be found:


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Dash...
Convert
Select
NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
Management CPU Usage
InUse Memory
0.50%
3.50%
20.79%
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
10
5
0
11:33:05
11:33:10
11:33:15
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
11:33:05
11:33:10
11:33:15
Established client connections
Established server connections
Default Group | Refresh | Help
Enable
Disable
Copyright(©) Citrix Systems, Inc. All rights reserved.

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

Throughput
Input 0 Mbps
Output 0 Mbps

HTTP Requests/s
0

System Log

```
Wed Sep 12 05:11:26 'server_vip_NSSVC_TCP_10.5.172.177:444(Lync_444_VIP)' Out
Wed Sep 12 05:11:40 'server_vip_NSSVC_TCP_10.5.172.177:5061(Lync_5061_VIP)' C
Wed Sep 12 05:12:00 'server_vip_NSSVC_TCP_10.5.172.177:5061(Lync_5061_VIP)' U
Wed Sep 12 05:12:18 'server_vip_NSSVC_SSL_BRIDGE_10.5.172.177:443(Lync_443_'
Wed Sep 12 05:12:31 'server_vip_NSSVC_TCP_10.5.172.177:80(Lync_80_VIP)' Out C
Wed Sep 12 05:12:46 SAVECONFIG start
Wed Sep 12 05:12:49 SAVECONFIG complete
Mon Sep 17 11:32:56 SAVECONFIG start
Mon Sep 17 11:33:00 SAVECONFIG complete
```

Service Groups

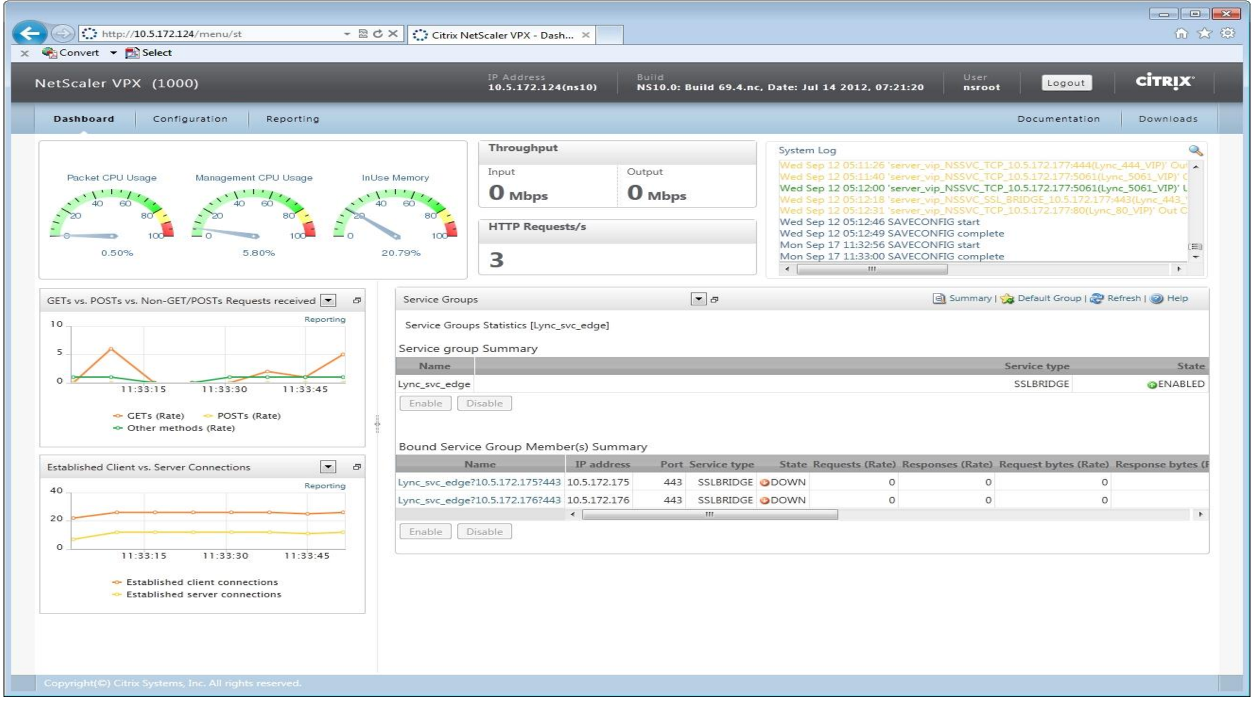
Service group(s) Summary

Records per page: 25 | 50 | 100 | 200 1 - 14 of 14 Goto Page: 1

Name	Service type	State
SharePointServers	HTTP	●ENABLED
CASServers	HTTP	●ENABLED
CASServers-SSL	SSL	●ENABLED
Exchange_IMAP4	TCP	●ENABLED
Exchange_POP3	TCP	●ENABLED
Exchange_SMTP	TCP	●ENABLED
Lync_svc_5060	TCP	●ENABLED
Lync_svc_5061	TCP	●ENABLED
Lync_svc_135	TCP	●ENABLED
Lync_svc_444	TCP	●ENABLED
Lync_svc_443	SSL_BRIDGE	●ENABLED
Lync_svc_80	TCP	●ENABLED
Lync_svc_edge	SSL_BRIDGE	●ENABLED
Lync_svc_edge1135	TCP	●ENABLED

6.2 Per Service Group Member

Under Service group **Name**, service backend servers are listed:


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Dash...
Convert
Select
NetScaler VPX (1000)
Logout
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
Management CPU Usage
InUse Memory
0.50%
5.80%
20.79%
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
10
5
0
11:33:15
11:33:30
11:33:45
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
11:33:15
11:33:30
11:33:45
Established client connections
Established server connections
Summary | Default Group | Refresh | Help
Enable
Disable
Copyright(©) Citrix Systems, Inc. All rights reserved.

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

Throughput
Input 0 Mbps
Output 0 Mbps

HTTP Requests/s
3

System Log

```
Wed Sep 12 05:11:26 'server_vip_NSSVC_TCP_10.5.172.177:444(Lync_444_VIP)' Out
Wed Sep 12 05:11:40 'server_vip_NSSVC_TCP_10.5.172.177:5061(Lync_5061_VIP)' C
Wed Sep 12 05:12:00 'server_vip_NSSVC_TCP_10.5.172.177:5061(Lync_5061_VIP)' U
Wed Sep 12 05:12:18 'server_vip_NSSVC_SSL_BRIDGE_10.5.172.177:443(Lync_443_'
Wed Sep 12 05:12:31 'server_vip_NSSVC_TCP_10.5.172.177:80(Lync_80_VIP)' Out C
Wed Sep 12 05:12:46 SAVECONFIG start
Wed Sep 12 05:12:49 SAVECONFIG complete
Mon Sep 17 11:32:56 SAVECONFIG start
Mon Sep 17 11:33:00 SAVECONFIG complete
```

Service Groups

Service Groups Statistics [Lync_svc_edge]

Service group Summary

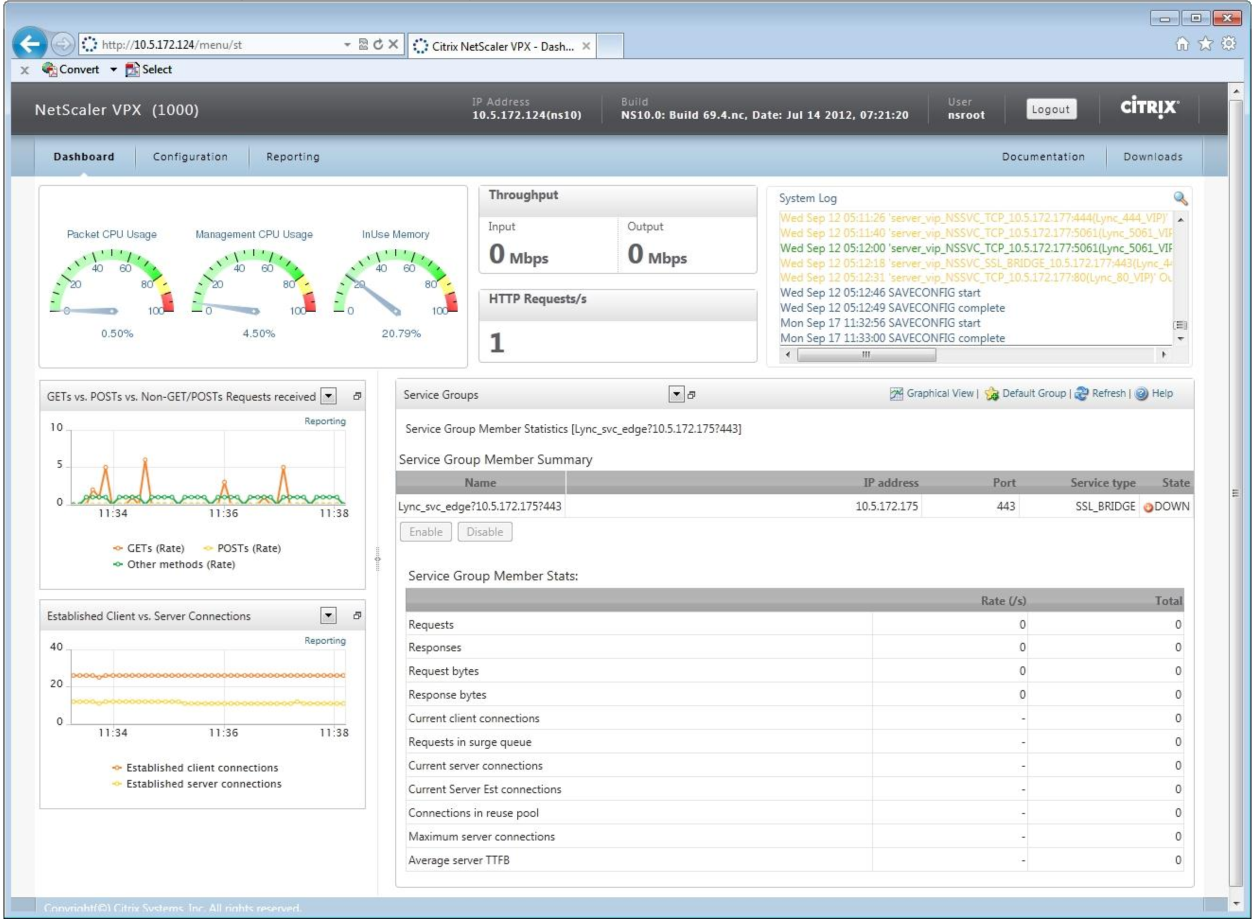
Name	Service type	State
Lync_svc_edge	SSLBRIDGE	●ENABLED

Bound Service Group Member(s) Summary

Name	IP address	Port	Service type	State	Requests (Rate)	Responses (Rate)	Request bytes (Rate)	Response bytes (F
Lync_svc_edge?10.5.172.175?443	10.5.172.175	443	SSLBRIDGE	●DOWN	0	0	0	
Lync_svc_edge?10.5.172.176?443	10.5.172.176	443	SSLBRIDGE	●DOWN	0	0	0	

6.3 Per Server

Under Service Group Member Summary, each member server stats are listed:


http://10.5.172.124/menu/st
Citrix NetScaler VPX - Dash...
Convert
Select
NetScaler VPX (1000)
Logout
CITRIX
Dashboard
Configuration
Reporting
Documentation
Downloads
Packet CPU Usage
Management CPU Usage
InUse Memory
0.50%
4.50%
20.79%
GETs vs. POSTs vs. Non-GET/POSTs Requests received
Reporting
10
5
0
11:34
11:36
11:38
GETs (Rate)
POSTs (Rate)
Other methods (Rate)
Established Client vs. Server Connections
Reporting
40
20
0
11:34
11:36
11:38
Established client connections
Established server connections
Service Groups
Graphical View | Default Group | Refresh | Help
Enable
Disable
Copyright(C) Citrix Systems, Inc. All rights reserved.

IP Address: 10.5.172.124(ns10)

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

User: nsroot

Throughput

Input: 0 Mbps

Output: 0 Mbps

HTTP Requests/s: 1

System Log

```
Wed Sep 12 05:11:26 'server_vip_NSSVC_TCP_10.5.172.177:444(Lync_444_VIP)'
Wed Sep 12 05:11:40 'server_vip_NSSVC_TCP_10.5.172.177:5061(Lync_5061_VIP
Wed Sep 12 05:12:00 'server_vip_NSSVC_TCP_10.5.172.177:5061(Lync_5061_VIP
Wed Sep 12 05:12:18 'server_vip_NSSVC_SSL_BRIDGE_10.5.172.177:443(Lync_4
Wed Sep 12 05:12:31 'server_vip_NSSVC_TCP_10.5.172.177:80(Lync_80_VIP)' Ou
Wed Sep 12 05:12:46 SAVECONFIG start
Wed Sep 12 05:12:49 SAVECONFIG complete
Mon Sep 17 11:32:56 SAVECONFIG start
Mon Sep 17 11:33:00 SAVECONFIG complete
```

Service Group Member Statistics [Lync_svc_edge?10.5.172.175?443]

Service Group Member Summary

Name	IP address	Port	Service type	State
Lync_svc_edge?10.5.172.175?443	10.5.172.175	443	SSL_BRIDGE	DOWN

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	-	0
Current Server Est connections	-	0
Connections in reuse pool	-	0
Maximum server connections	-	0
Average server TTFB	-	0

7. Palo Alto Networks Next-Generation Firewall Deployment

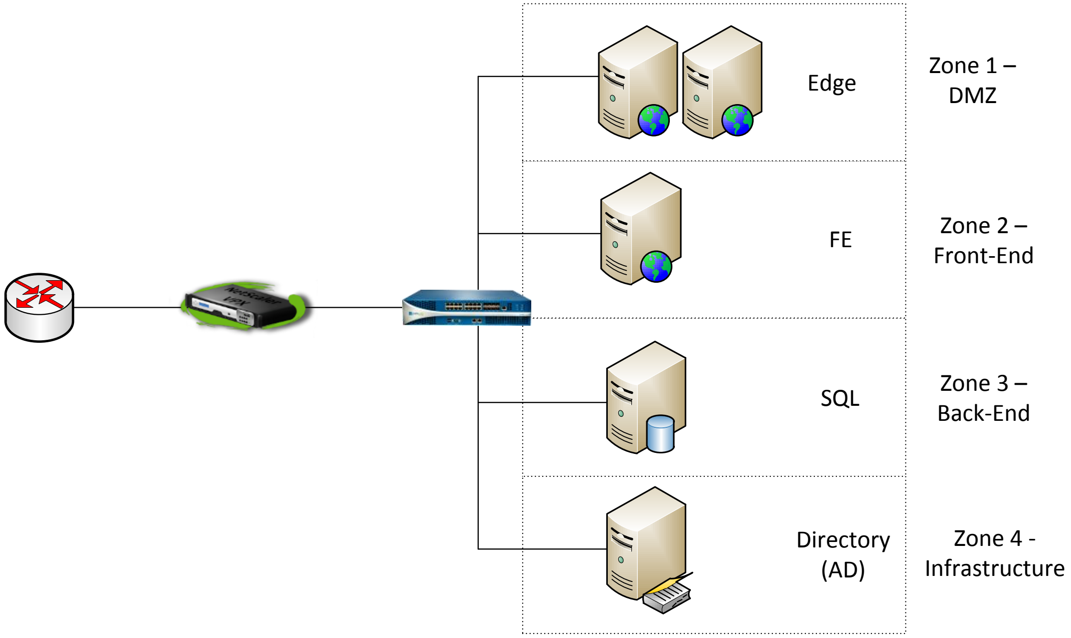
The Palo Alto Networks next-generation firewall safely enables enterprise applications in the data center and delivers meaningful segmentation by application, user and content. It identifies all traffic sent to the Microsoft Lync servers, based on actual application, not just port or protocol. Access to the Microsoft Lync 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.

7.1 Data Center Segmentation

In a Lync 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 Lync installations, the different server roles will be deployed on dedicated physical or virtual servers.

In order to properly segment and secure a large Lync implementation, the different server roles will be isolated in dedicated security zones that can only be accessed by authorized users with authorized applications.

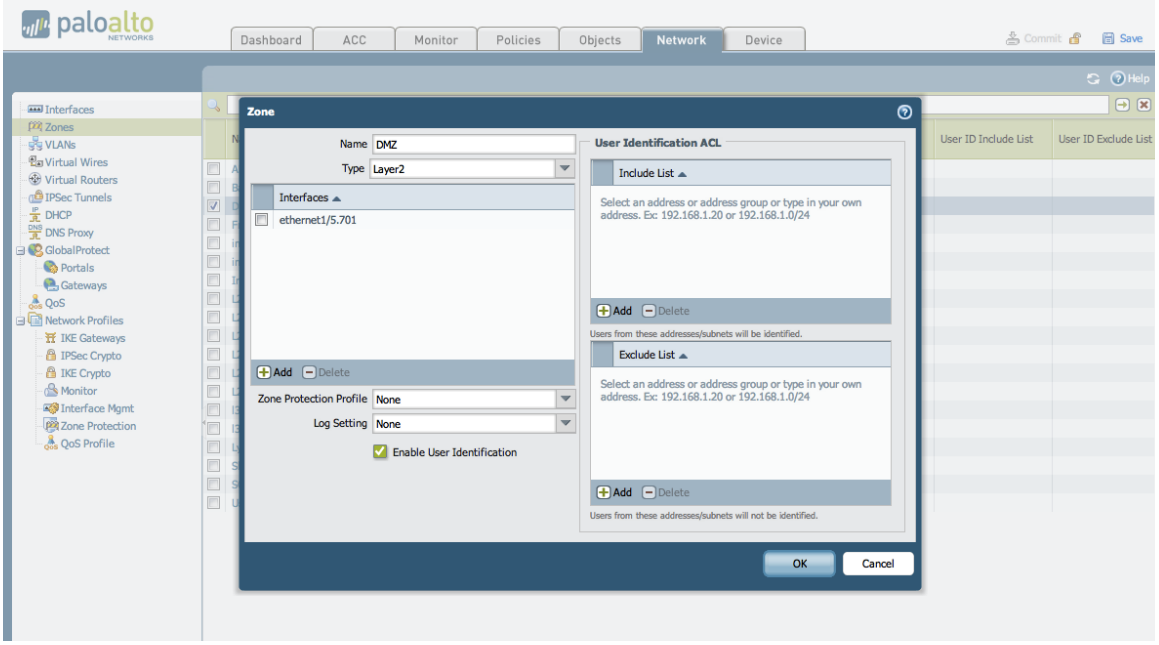
In this reference design, there will be segments for the Lync Front End Servers, Edge Servers, SQL Servers, and Active Directory Servers. Users and administrators accessing the Lync servers will come from the External zone, and there will be an infrastructure segment in which the Active Directory Domain Controllers reside. It is also important to note that Lync has a dependency on MS Exchange communications. To simplify this design and focus on the Lync components, all MS Exchange services will reside in the Active Directory zone.



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

- **DMZ** – Lync Edge Servers
- **Front-End** – Lync Front End Servers
- **Back-End** – SQL Server
- **Infrastructure** – Domain controller
- **External** – Users and administrators

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



Name DMZ

Type Layer2

Interfaces

□ ethernet1/5.701

Zone Protection Profile None

Log Setting None

☑ Enable User Identification

User Identification ACL

Include List

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

Users from these addresses/subnets will be identified.

Exclude List

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

Users from these addresses/subnets will not be identified.

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

Repeat this for each of the required zones.

7.2 Security Policy

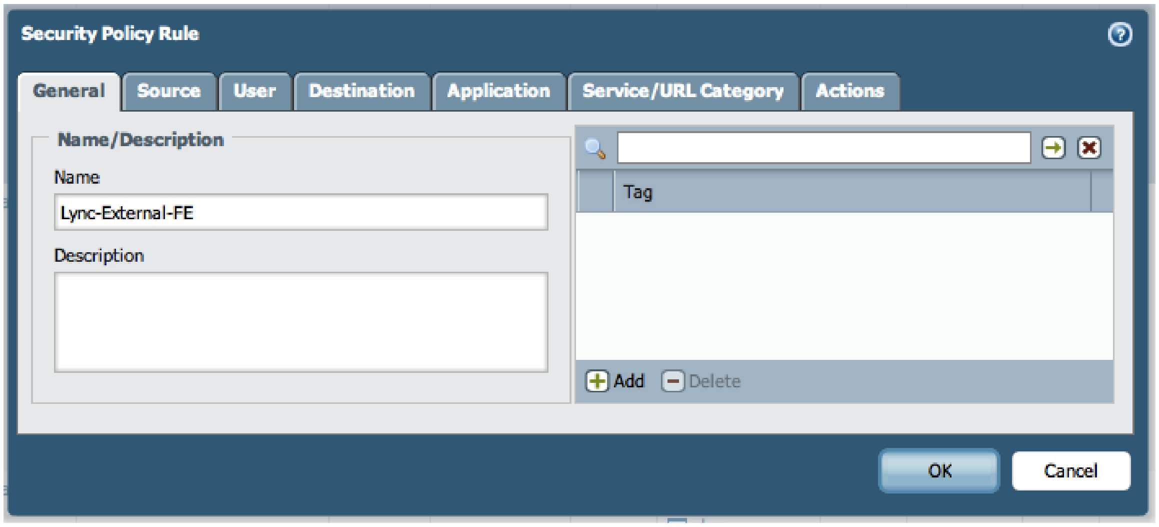
Palo Alto Networks security policy is zone based. Each segment in a data center deployment will be in a separate zone. Once the traffic flow is understood, the security policy can be written based on actual application, not just ports and port ranges. Allowing the following protocols between the specified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

Every Lync 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 Lync security policy.

Source Zone	Destination Zone	Application
External	Front-End	kerberos ms-lync rpc sip soap ssl stun web-browsing
External	DMZ	kerberos ms-lync rpc sip soap

		ssl stun
External	Infrastructure (AD/Exchange)	active-directory dns kerberos ldap ms-ds-smb ms-exchange ms-netlogon msrpc netbios-dg netbios-ss pop3 rpc rpc-over-http smtp ssl web-browsing
External	Back-End (Database)	mssql-db
Infrastructure (AD/Exchange)	External	active-directory ms-ds-smb msrpc netbios-dg netbios-ss
Infrastructure (AD/Exchange)	DMZ	active-directory ms-ds-smb msrpc netbios-dg netbios-ss
Infrastructure (AD/Exchange)	Front-End	active-directory ms-ds-smb msrpc netbios-dg netbios-ss
DMZ	Infrastructure (AD/Exchange)	dns ms-ds-smb msrpc netbios-dg netbios-ss
Front-End	Infrastructure (AD/Exchange)	dns ms-ds-smb msrpc netbios-dg netbios-ss
Front-End	DMZ	ssl

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



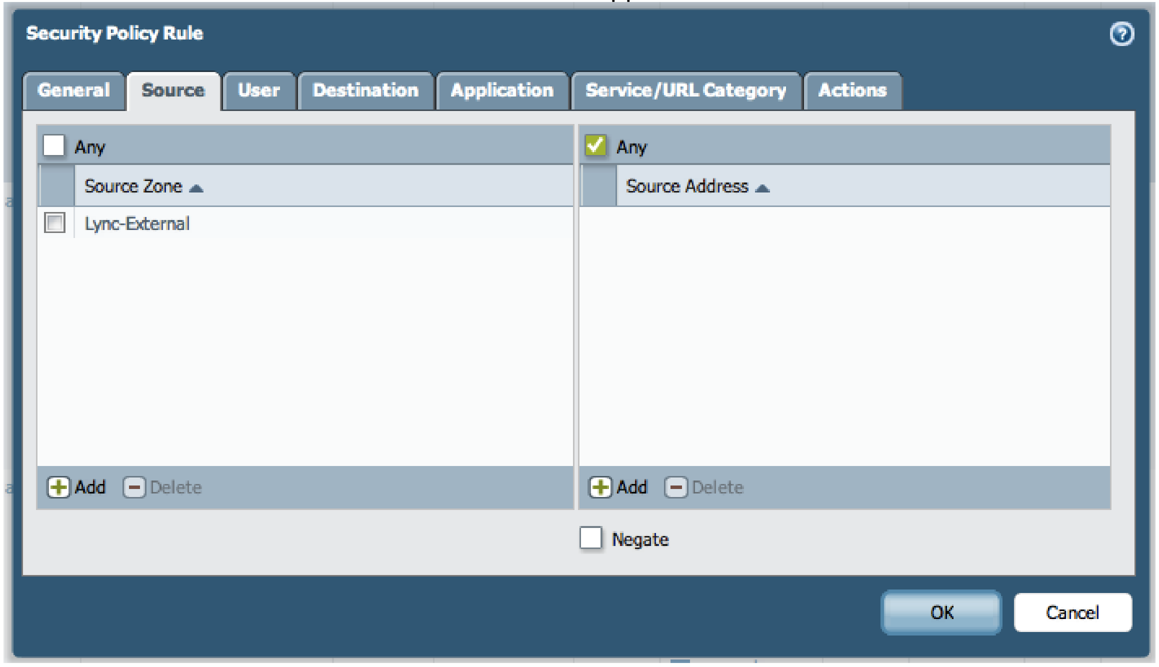
Security Policy Rule

Name/Description

Name: Lync-External-FE

Description:

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



Security Policy Rule

□ Any

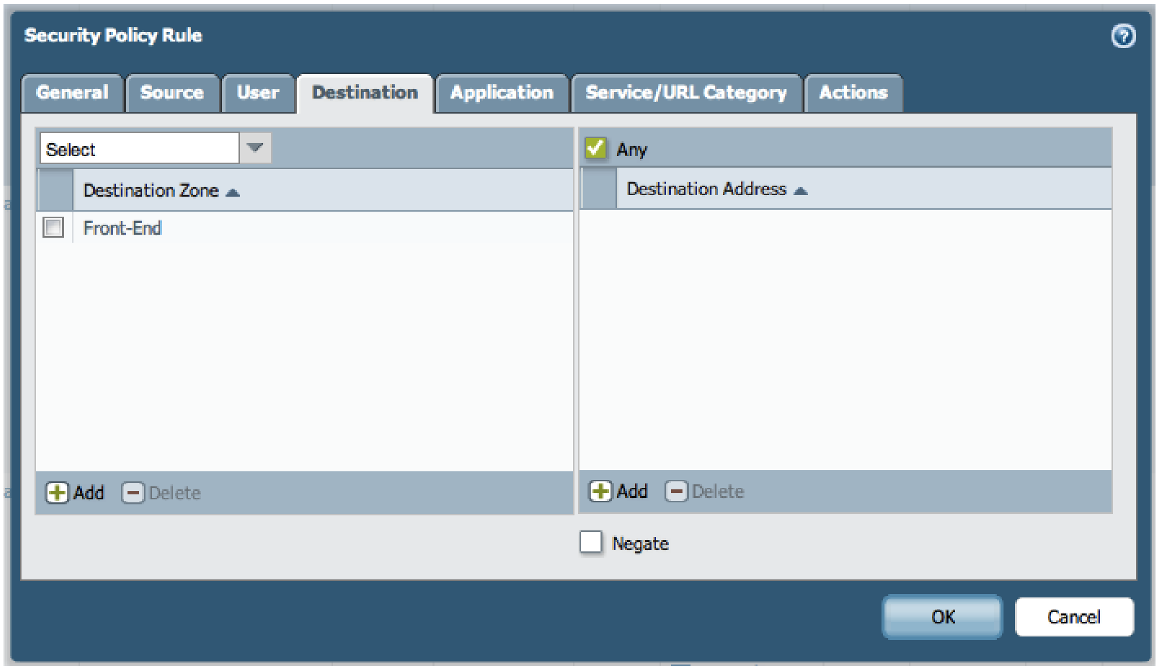
	Source Zone
□	Lync-External

☑ Any

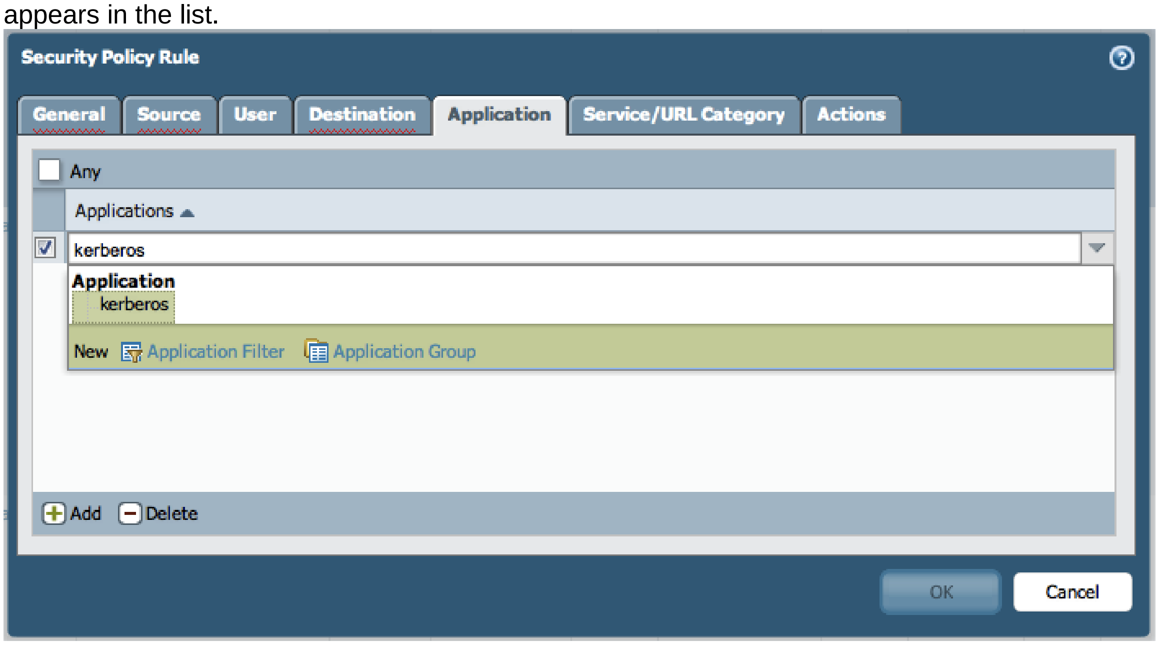
	Source Address

□ Negate

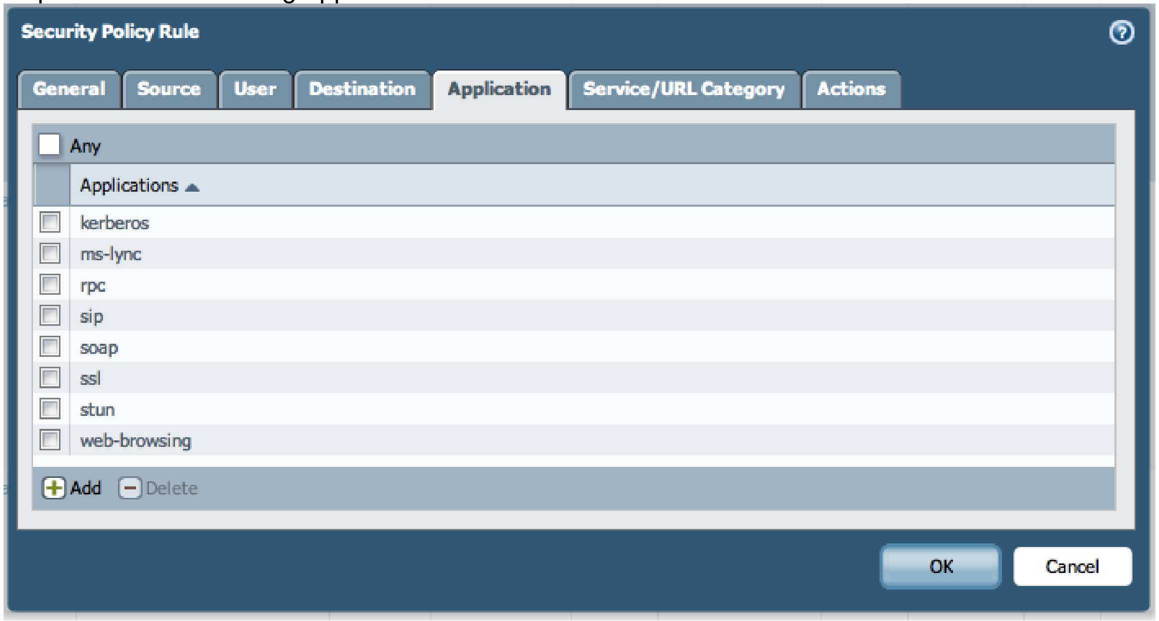
Click on the Destination tab and click Add. Select the Database zone.



Click on the Application tab and click Add. Eight applications will be added to this rule: kerberos, ms-lync, rpc, sip, soap, ssl, stun, web-browsing. Begin typing the first application name and select it when it appears in the list.



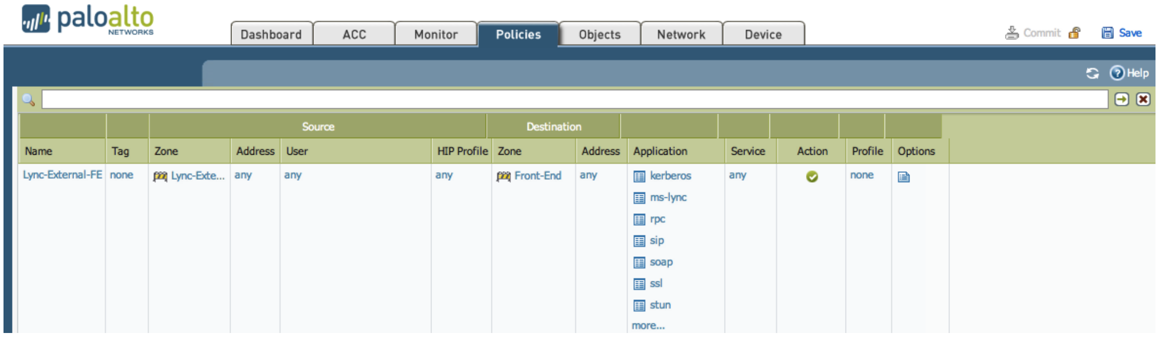
Repeat for the remaining applications in this rule.



□ Any

	Applications
□	kerberos
□	ms-lync
□	rpc
□	sip
□	soap
□	ssl
□	stun
□	web-browsing

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.



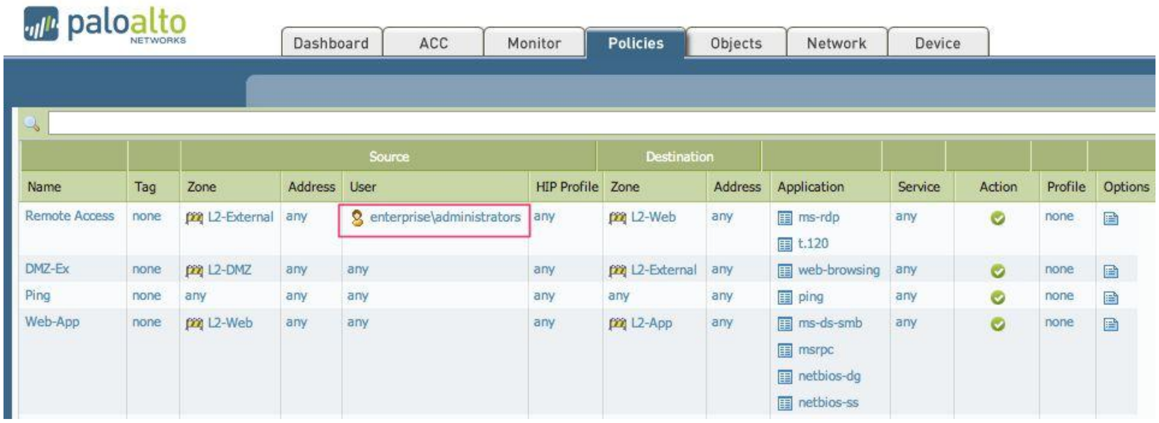
		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Lync-External-FE	none	Lync-Exte...	any	any	any	Front-End	any	kerberos ms-lync rpc sip soap ssl stun more...	any	✓	none	

7.3 User Identification

The Palo Alto Networks firewall also allows security policy to be further refined by end user, 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 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, say that the Lync servers need to be accessible by the System Administrators with Remote Desktop for management purposes. The rest of the enterprise does not need this access.

The security policy rule allowing the applications, in this case, ms-rdp and t.120, would only be accessible by the administrators group. Lync would be accessible by the entire company using the client applications.



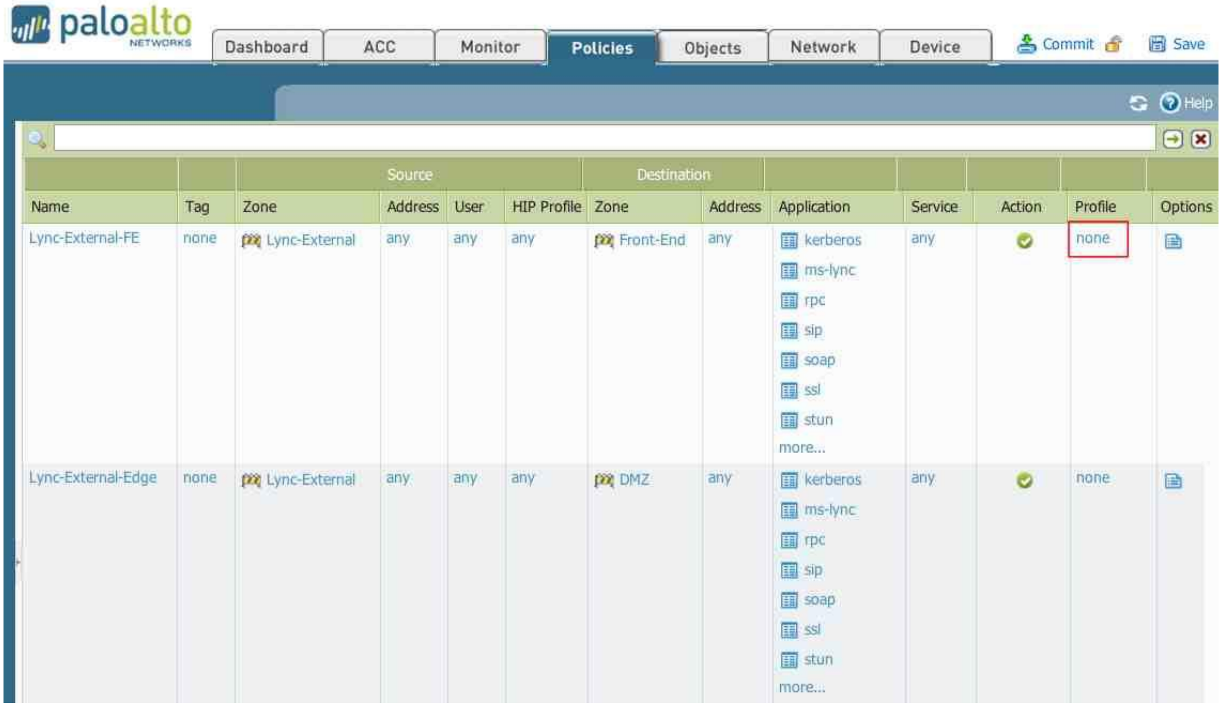
		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Remote Access	none	L2-External	any	enterprise\administrators	any	L2-Web	any	ms-rdp t.120	any	✓	none	
DMZ-Ex	none	L2-DMZ	any	any	any	L2-External	any	web-browsing	any	✓	none	
Ping	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	

7.4 Threat Prevention

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

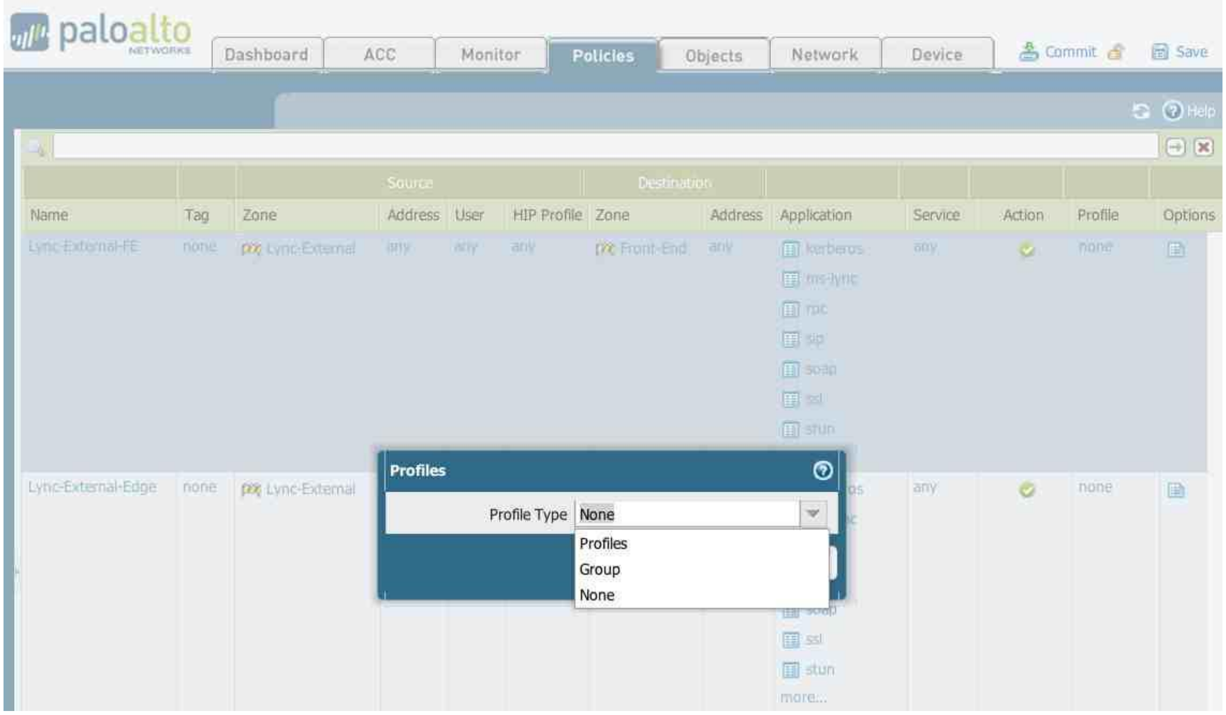
Each rule in the security policy can have its own security profile applied, allowing for the greatest flexibility in setting policy. For example, you may have a strict security profile blocking viruses, malware, and spyware on traffic that originates outside the data center and accesses the front-end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

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



		Source				Destination						
Name	Tag	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Lync-External-FE	none	Lync-External	any	any	any	Front-End	any	kerberos ms-lync rpc sip soap ssl stun more...	any	✓	none	
Lync-External-Edge	none	Lync-External	any	any	any	DMZ	any	kerberos ms-lync rpc sip soap ssl stun more...	any	✓	none	

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

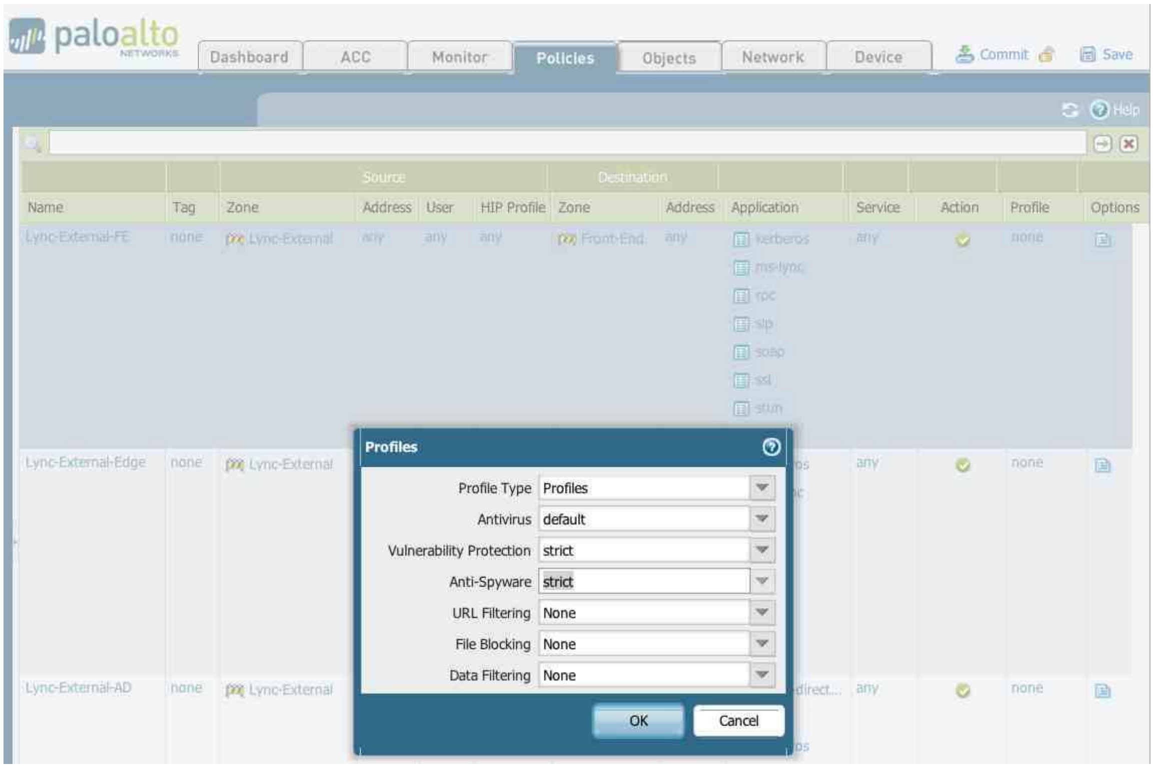


Profiles

Profile Type: None

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”.

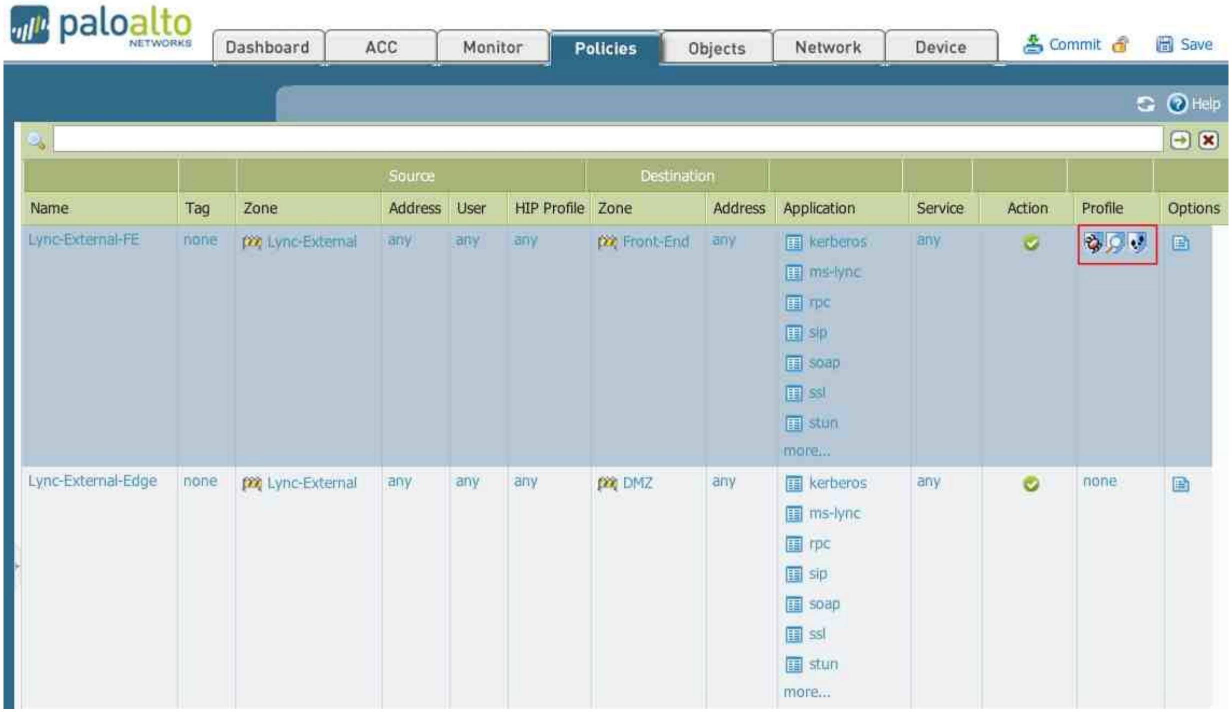
These pre-configured options can be chosen, or a customized profile can be created. Please see Palo Alto Networks Administration Guide for details on creating custom profiles.



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
Lync-External-FE	none	Lync-External	any	any	any	Front-End	any	kerberos ms-lync rpc sip soap ssl stun more...	any	✓		
Lync-External-Edge	none	Lync-External	any	any	any	DMZ	any	kerberos ms-lync rpc sip soap ssl stun more...	any	✓	none	

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

8. References

Citrix Deployment Guide: Citrix NetScaler for Microsoft Lync. Citrix Systems, Inc. 2010
Citrix NetScaler Networking Guide – Release 10. Citrix Systems, Inc. 2012
Microsoft Lync: Determining External A/V Firewall and Port Requirements http://technet.microsoft.com/en-us/library/gg425882.aspx
Microsoft Lync: Ports and Protocols for Internal Servers http://technet.microsoft.com/en-us/library/gg398833(d=printer).aspx

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.