Application Note

Using Citrix NetScaler 1000v® traffic management and load balancing in a Cisco Unified Customer Voice Portal Solution

April 21, 2014

Overview

Typically in a large Unified CVP solution deployment, Cisco load balancers are used to load-balance incoming http and https traffic. The Citrix NetScaler 1000v (Load Balancer) can also provide the functionality required to load balance the Unified CVP http and https traffic. The Unified CVP solution can be deployed with the NetScaler Load Balancer in both Standalone and Comprehensive deployment models, where it can perform the following functions:

- HTTP load balancing with CVP VXML Servers
- HTTPS load balancing with CVP VXML Servers
  - SSL offloading at NetScaler
  - End-to-End HTTPS
- Media server load balancing

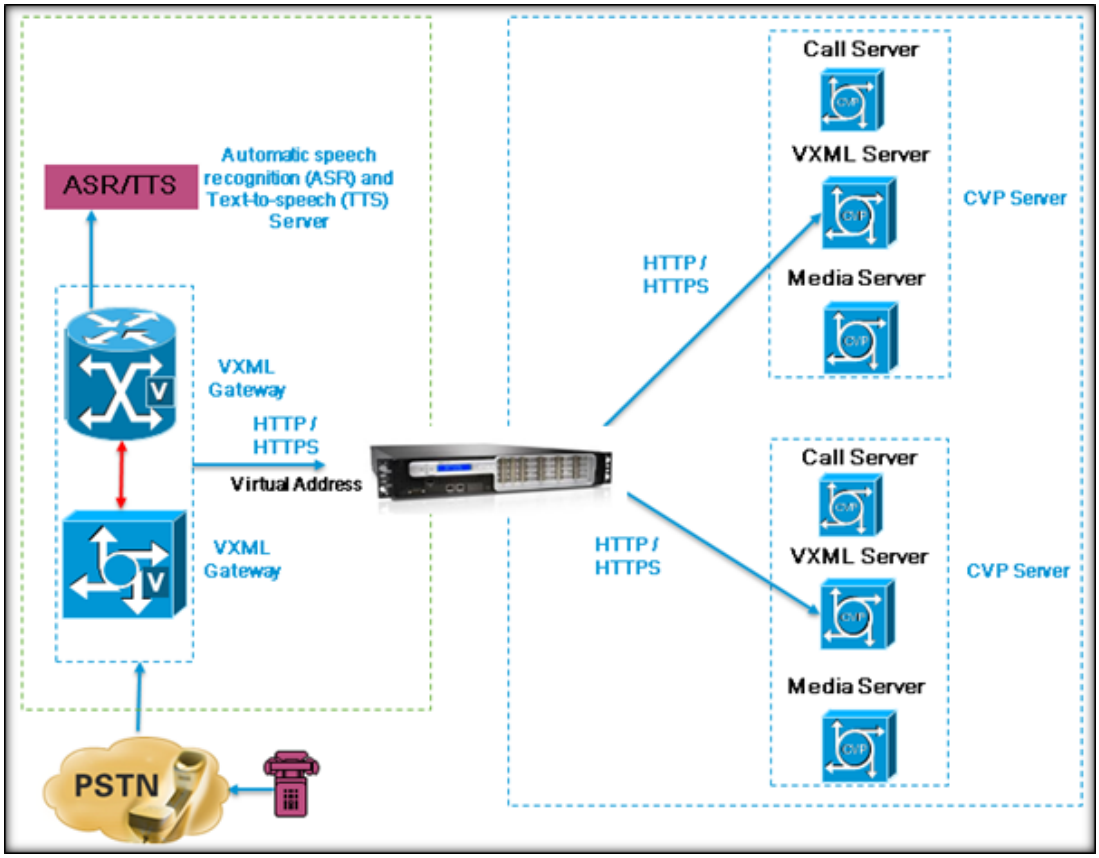
This Interoperability note details the use for connectivity of Citrix NetScaler 1000v with CVP. It serves as guidance for integration. However, it does not guarantee interoperability for every use case. Under the same conditions, this document may also be leveraged with different component versions and different service providers. As in any third-party interoperability, Cisco provides support for its own components, but may not be able to fully assist in end-to-end troubleshooting or provide timely diagnostics and fixes.

Versions of products used in testing

- IOS 15.3.3M1 (VXML Browser)
- Unified Customer Voice Portal (CVP) 8.5(1), 9.0(1), 10.(1)
- Citrix NS : Virtual Edition : Citrix NetScaler 1000v (10.1)

Network Topology

Figure 1 VXML HTTP load balancing with Unified CVP



Caveats

It is recommended to use7443 as the server port at Citrix NS for HTTPS connection and 7000 as Server port for the Cirtix NS when the redirect is set to true (redirect=true). Only the 7443 port of the NetScaler load balancer can be used for HTTPS connections. The supported features listed in this document are tested with Redirect = true / false in CVP Server (Session Based / Non Session Based)

Configurations

This section provides information on configuration of various components that were used to test the Citrix NetScaler load balancer with the Cisco Unified CVP.

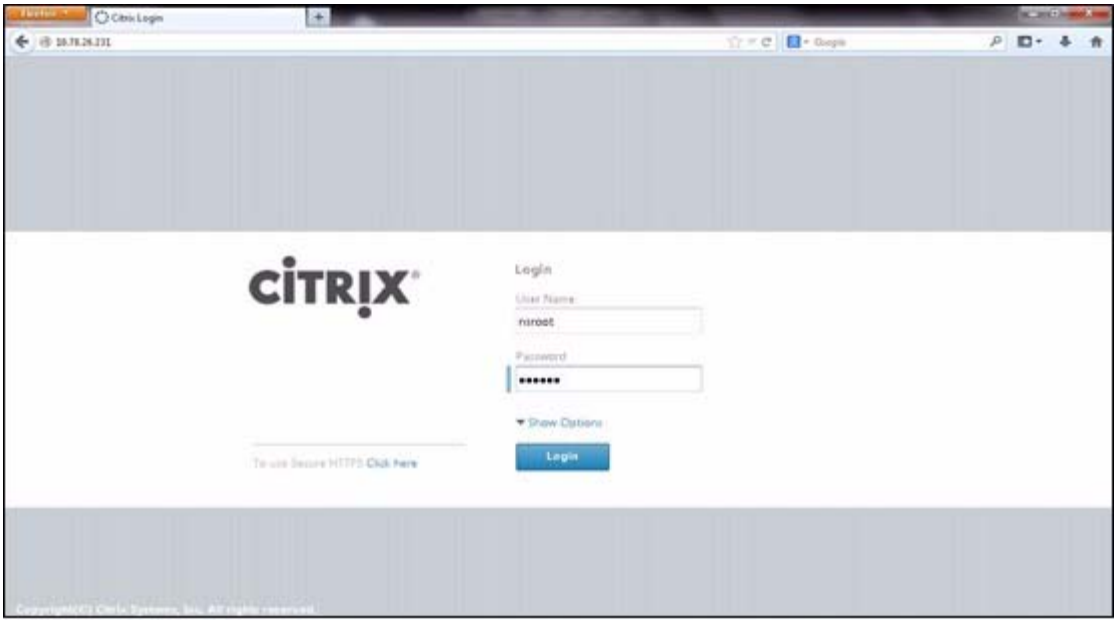
HTTP Load Balancing

NetScaler Web Interface

The NetScaler 1000v virtual machine needs an IP address assigned to its virtual management port. Following are the steps to configure:

1. Enter a NetScaler IP in the web browser, (for example, 10.78.26.231) to start the NetScaler Web Interface.
2. Enter the Username and the Password and then click Login.

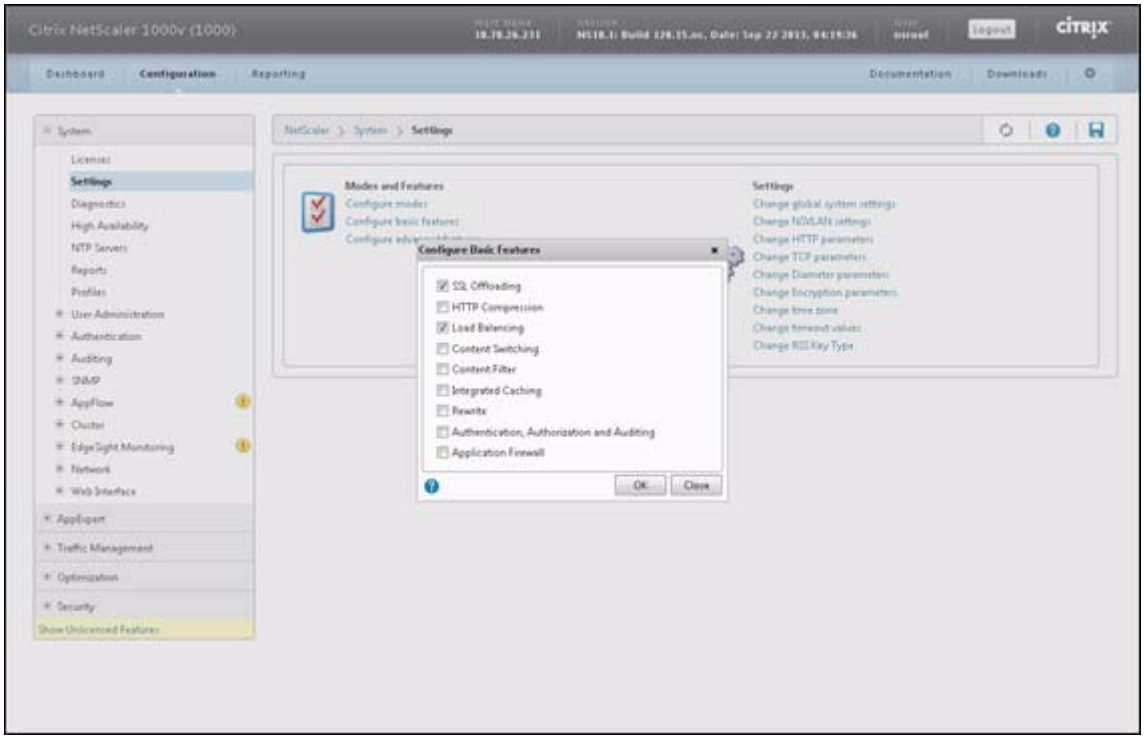
Figure 2 Login Prompt



System Settings

For system setings follow the these steps:

Figure 3 Settings page

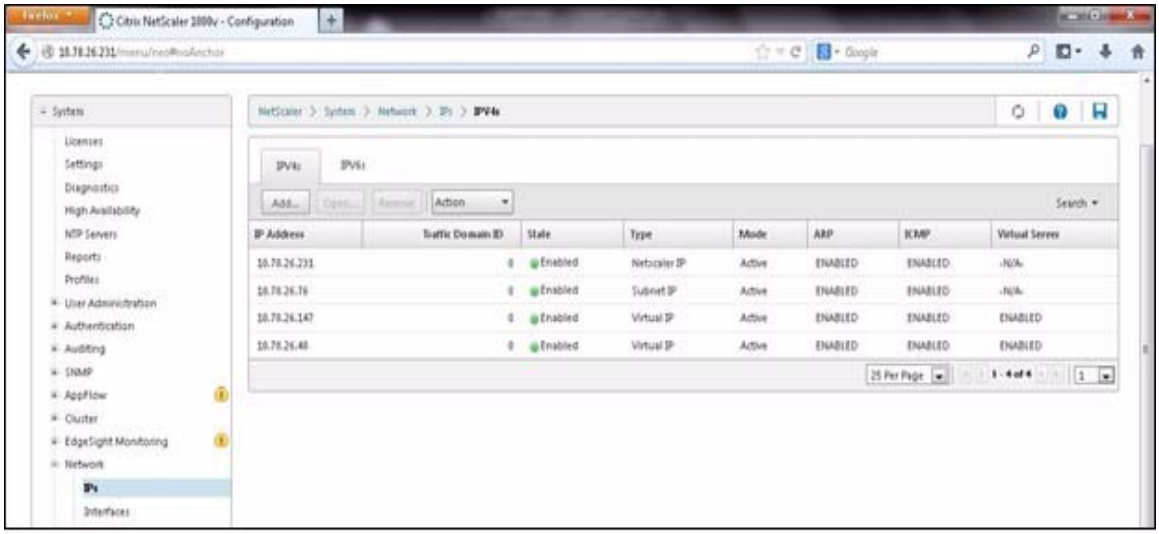


3. Select Configure basic features option from the list to configure NetScaler features.

IP Address Configuration

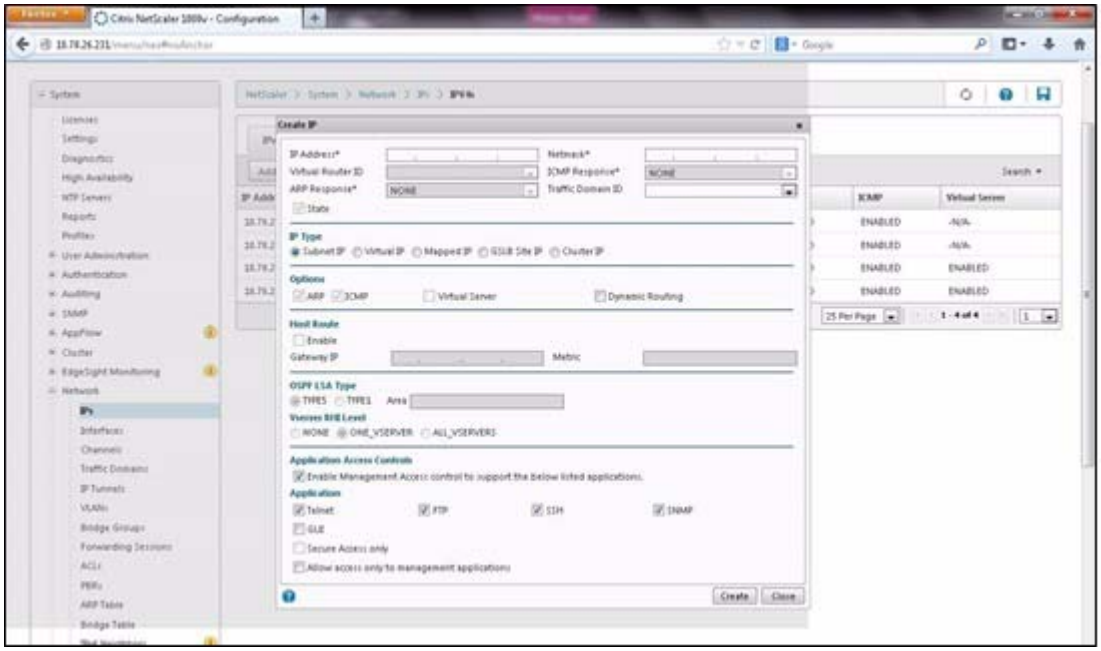
1. Under System dropdown list, select Network and then select IPs

Figure 4 System IP Page



2. Click on the Add button to add IP address.

Figure 5 Create IP page

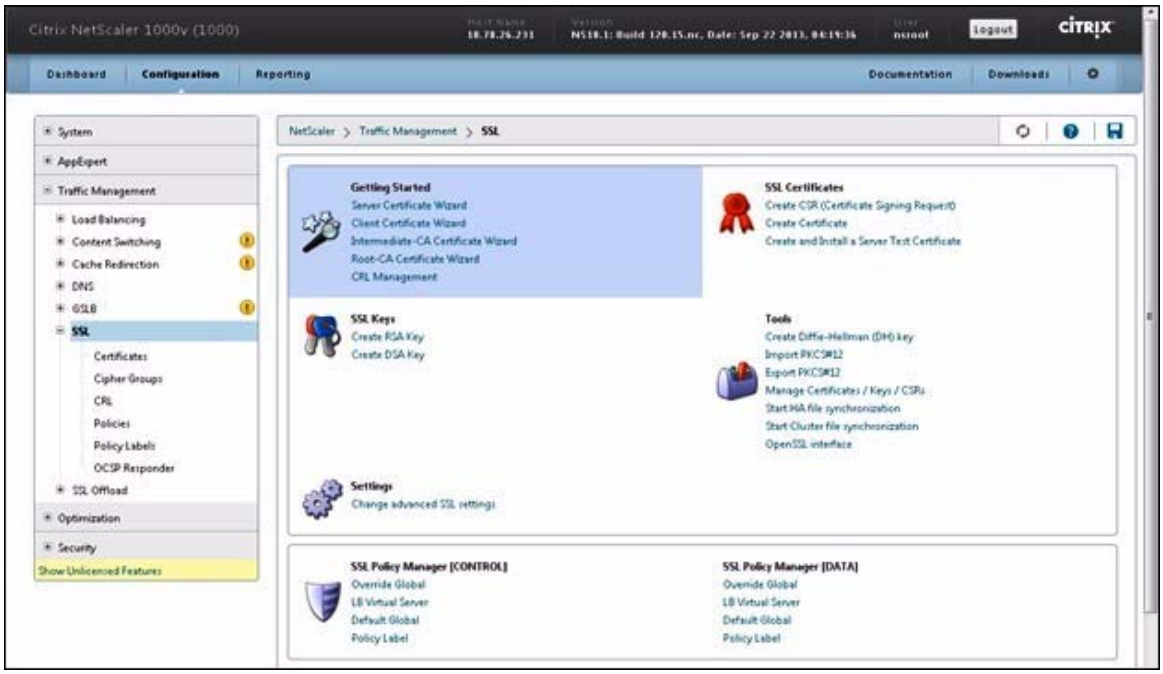


3. To add the Subnet IP, select Subnet IP under IP Type.
4. Similarly select Virtual IP for Virtual Servers.
5. Click Create to create the desired IP address.

SSL and HTTPS Load Balancing Configuration

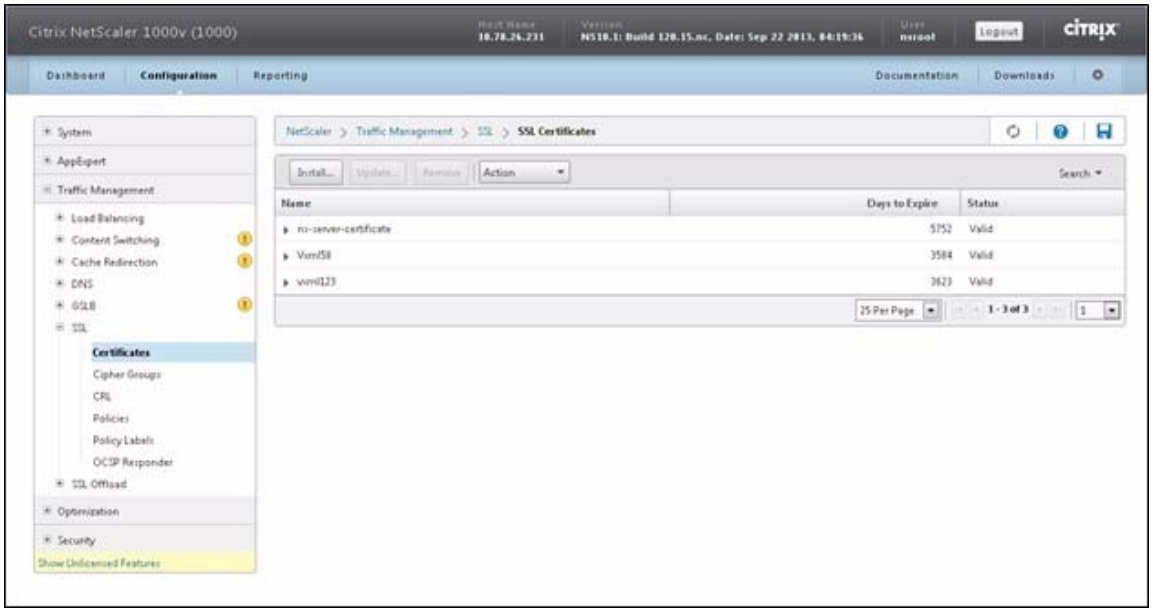
1. Upload VXML Server certificates to NetScaler.
2. To add a SSL certificate, from Configuration tab, expand Traffic Management and then select SSL.

Figure 6 SSL certificate page



3. Click on the certificates under SSL.

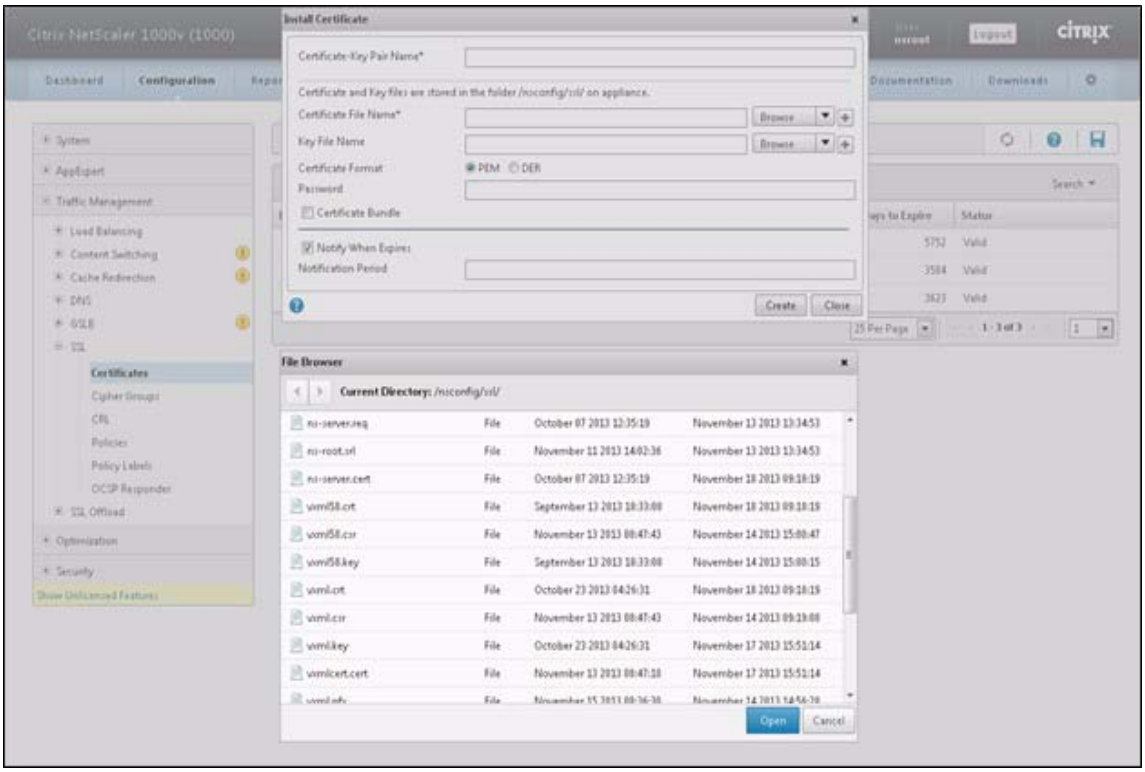
Figure 7 SSL Certificates page



4. Select the certificate from the list and follow the steps to install the certificate as illustrated in the following images.

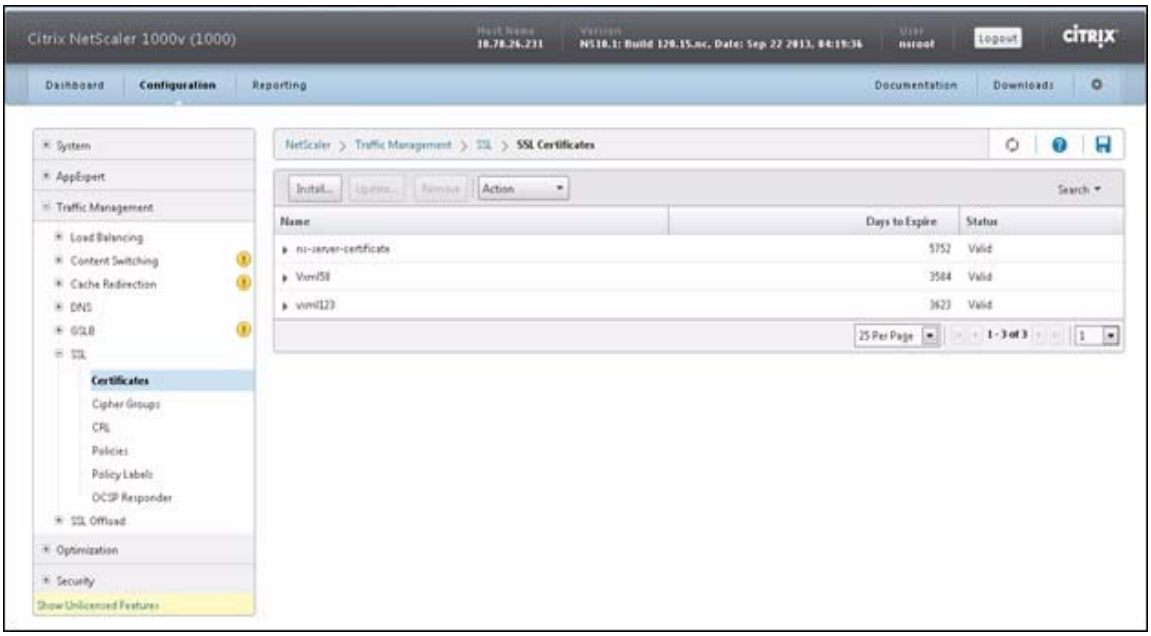
Note Before installing, certificates must be copied into the NetScaler machine using winscp (/nsconfig/ssl).

Figure 8 File Browser page



After the successful installation, the installed certificates are displayed as shown in the following illustration.

Figure 9 External IP configuration

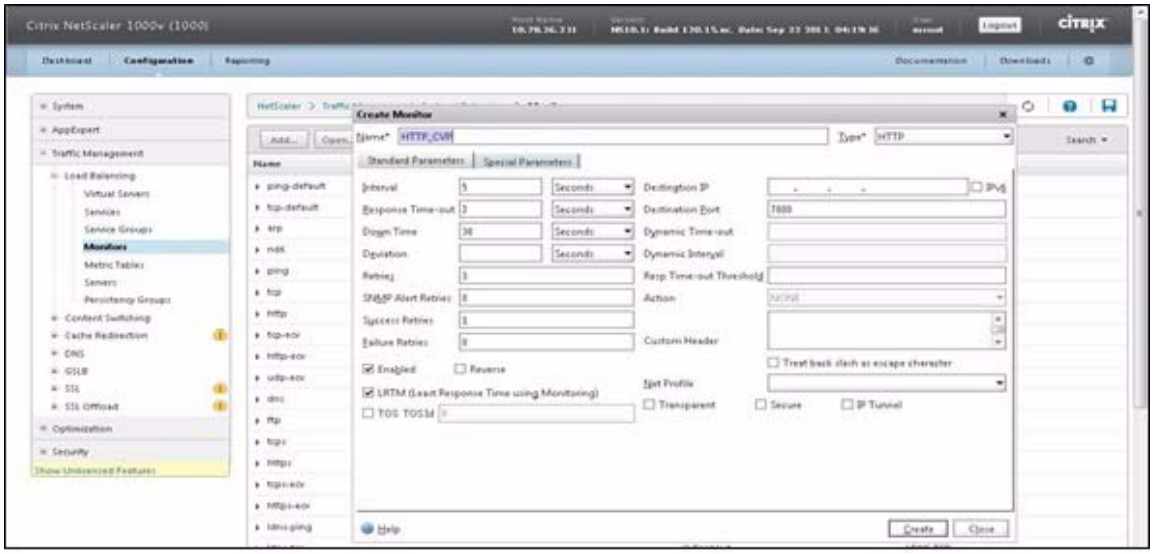


HTTPS Citrix Load Balancer

To create the HTTPS Citrix Load Balancer, follow these steps:

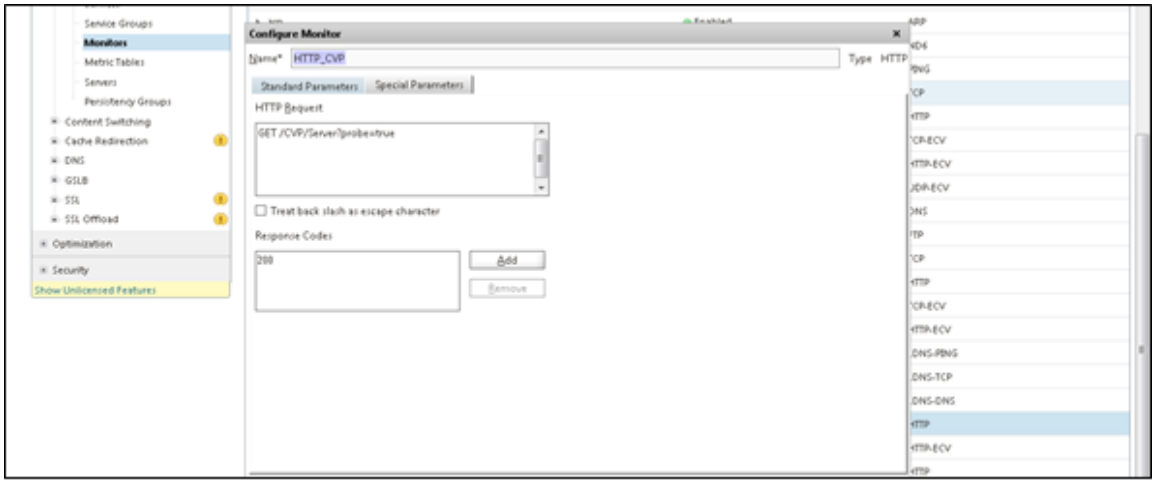
1. To create monitors, click the Traffic Management tab select SSL and then select Monitors.
2. Click the Add button and enter the name.

Figure 10 Create Monitor page



3. Select the Type of protocol in the Standard Parameters and click on the Special Parameters option.

Figure 11 Configure Monitor page

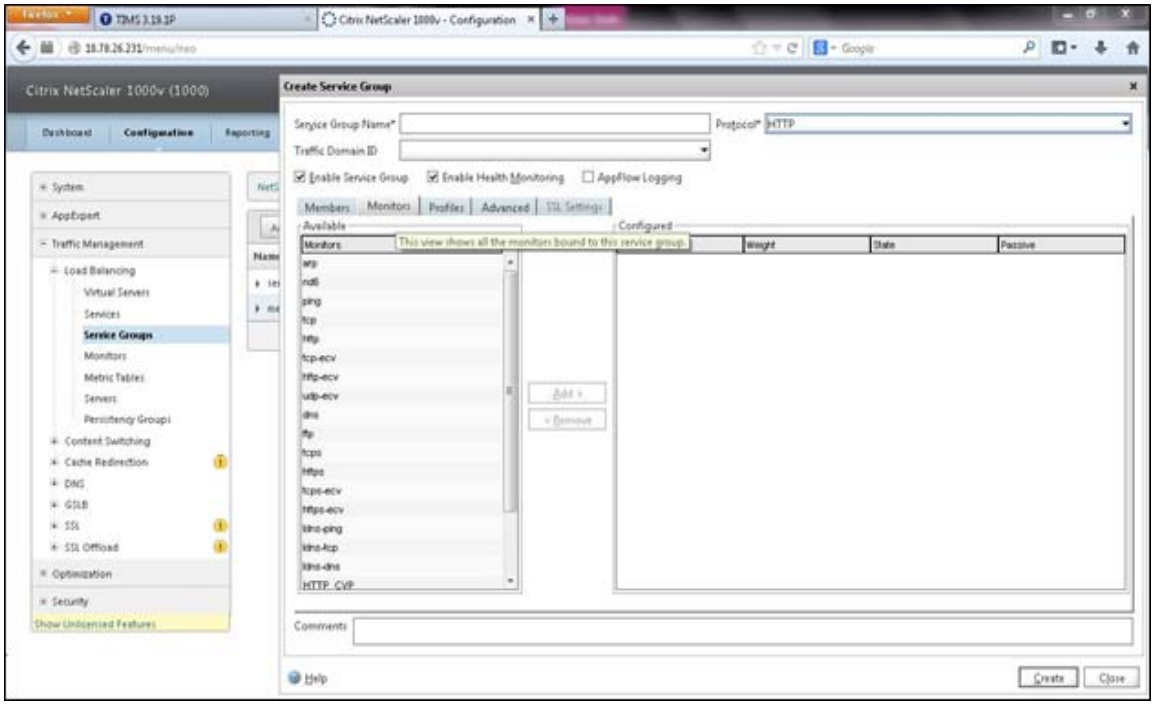


Note You can enter the HTTP request (Example, GET /CVP/Server?probe=true) and Response codes manually.

1. Click Create button to create the monitor with port as 7443

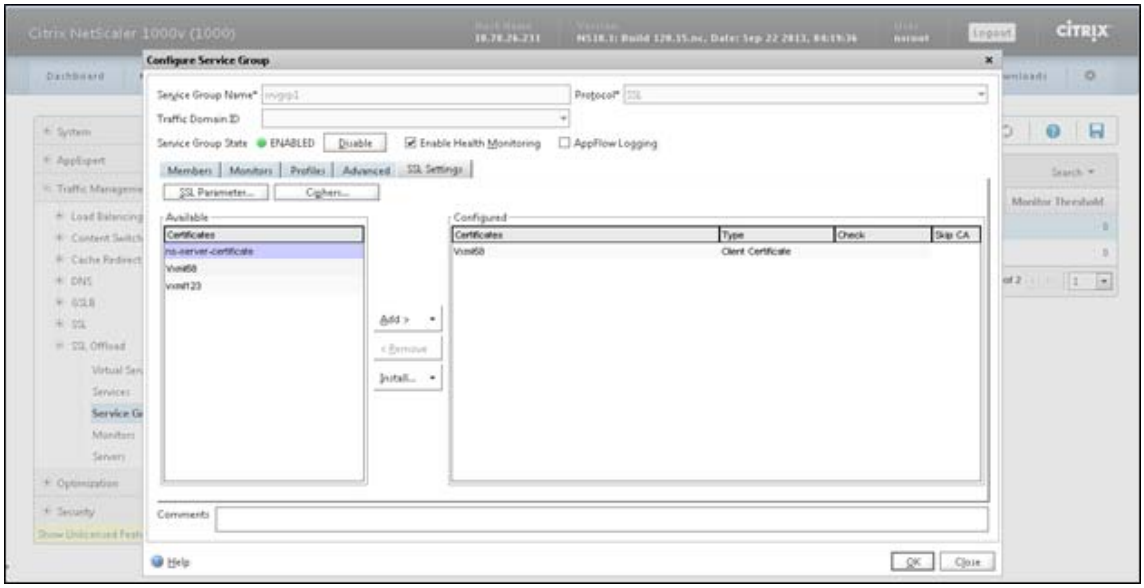
2. Create Service Groups, under Traffic Management > SSL Service Groups.
3. Click on the Add button and provide a service group name with Protocol type.
4. Under the Members Tab, add members to the group (CVP Servers).
5. Under the Monitors Tab add the Monitors.
6. Click Create.

Figure 12 Create Service Group page



10.Select the certificate to communicate with VXML Server.

Figure 13 Certificate Service Group page

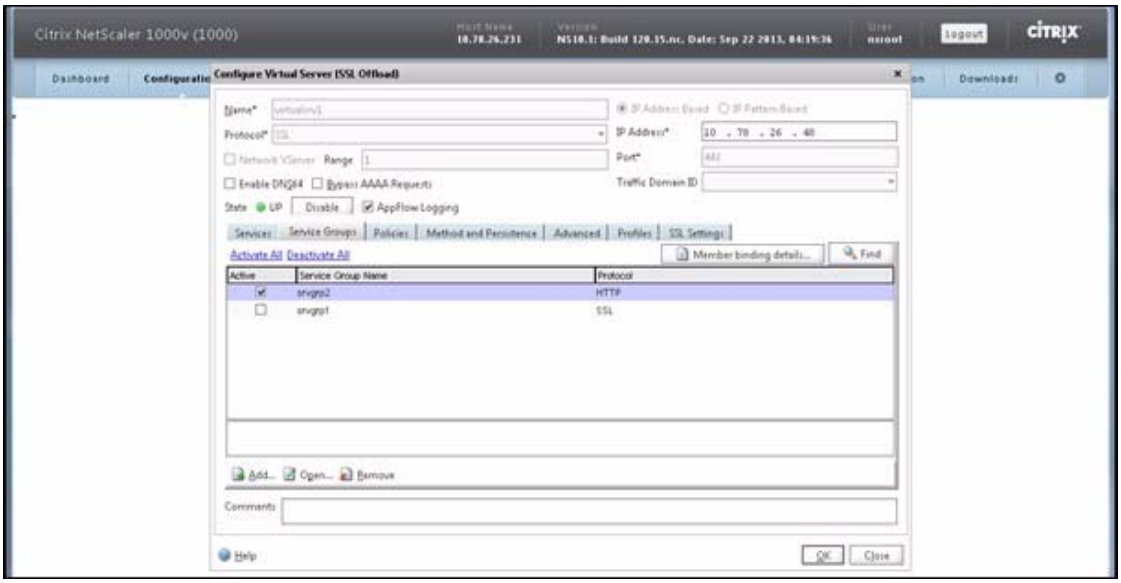


Virtual Server Configuration

To configure virtual server, follow these steps:

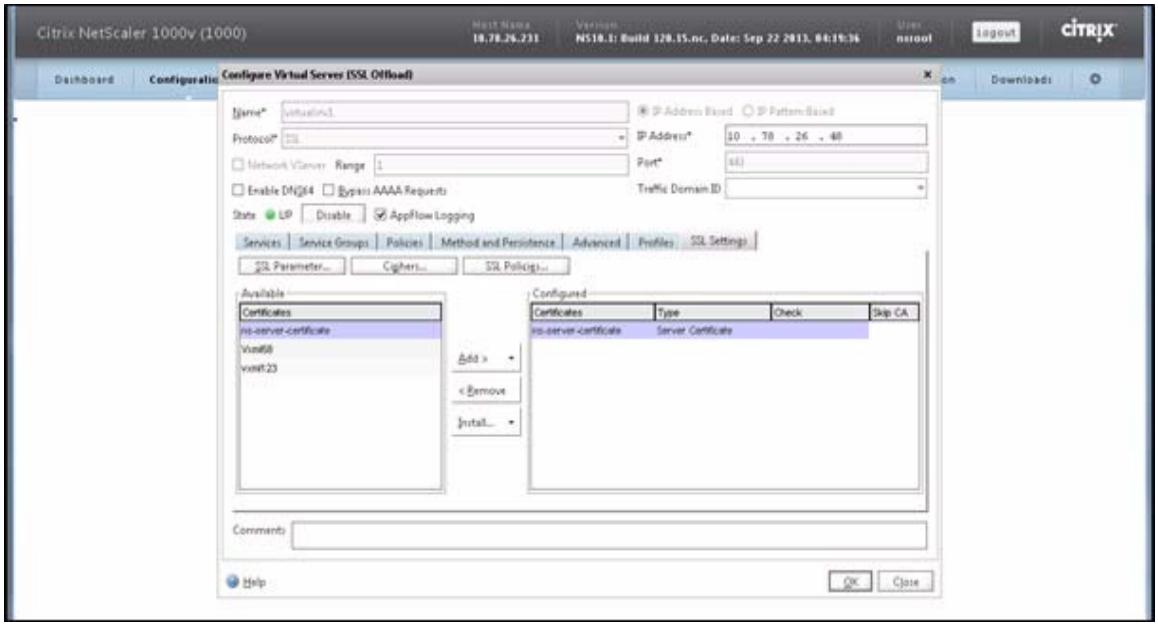
1. Select SSL in the Protocol tab to create HTTPS virtual server.

Figure 14 Virtual Server configuration page



2. Select certificate for this SSL virtual server (Imported / Installed Certificate)

Figure 15 Certificates list



Note The same certificate should be exported from NetScaler and has to be installed in the gateway. Follow below steps to install certificate in gateway.

```
Example Certificate file (content trimmed due to size, typically about
30 lines in length):
-----BEGIN CERTIFICATE-----
MIIGTzCCBTegAwIBAgIKJozFswAAAAAACjANBgkqhkiG9w0BAQUFADCBvDEdMBsG
CSqGSIb3DQEJARYOc3BhbUBjaXNjby5jb20xCzAJBgNVBAYTAlVTMRYwFAYDVQQI...
MkYIfimRdD1U3AH6iPczbi+ryUM5mvcl9fTnq/DiaKqDSAo=
----END CERTIFICATE-----
For SSL offload, create a service group with HTTP as protocol.
```

Gateway Configuration for HTTPS

To apply certificates to the IOS gateway use the following command:

```
crypto pki trustpoint <name>
enroll terminal
exit
crypto pki authenticate <name>
 <paste in contents of the previously copied cert file>
```

Note Certificates must be applied to the IOS gateway for NetScaler load balancer system using HTTPS.

To display certificates configured on a gateway use the following command:

```
show crypto pki certificates
```

For better performance, it is recommended to use the following configuration on the Cisco IOS VoiceXML Gateway with HTTPS option:

```
http client connection persistent
http client cache memory pool 15000
http client cache memory file 1000
```