

Using F5 BIG-IP[®] traffic management and load balancing in a Cisco Unified Customer Voice Portal Solution

Aug 19, 2013

Overview

The Cisco Unified Customer Voice Portal (Unified CVP) leverages a VXML based architecture. The VXML browser can access the VXML server and media servers directly, but for larger deployments it may benefit from leveraging an HTTP load balancer.

Typically in a large Unified CVP solution deployment, Cisco load balancers are used to load-balance incoming http and https traffic. The F5 BIG-IP[®] (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 BIG-IP load balancer in both Standalone and Comprehensive deployment models, where the BIG-IP can perform the following functions:

- HTTP load balancing with CVP VXML Servers
- HTTPS load balancing with CVP VXML Servers
 - SSL offloading at F5-LTM
 - End-to-End HTTPS
- Media server load balancing

To validate the interworking of F5 BIG-IP[®] with the Unified CVP, the parameters can be adjusted based on the physical, virtual, or cloud deployment.

This Application Note details the use for connectivity of F5 BIG-IP[®] 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.

**Note**

The Big-IP load balancer can also be used to load balance requests to enterprise systems (like having the Call Server in IVR mode only). The load balancing of SIP protocol though BIG-IP is not supported for CVP components.

Versions of products used in testing

- Cisco ISR G2 3945E Version 15.3(3)M version of the IOS (gateway).
- Unified Customer Voice Portal 9.0 and 10.0 (CVP)
- Unified Communications Manager 9.0 (CUCM)
- BIG-IP 11.3.0 (F5 Load Balancer)

Tested Features

To validate the interworking of the F5 load balancer with the Cisco Unified CVP, the following functional areas have been tested in the Standalone mode:

- HTTP load balancing with CVP VXML Servers (Refer [Figure 1](#) for the network topology)
- HTTPS load balancing with CVP VXML Servers
 - SSL offloading (Refer [Figure 2](#) for the network topology)
 - End-to-End HTTPS traffic (Refer [Figure 3](#) for the network topology)
- Media server load balancing (Refer [Figure 4](#) for the network topology)

Figure 1

VXML HTTP load balancing with Unified CVP

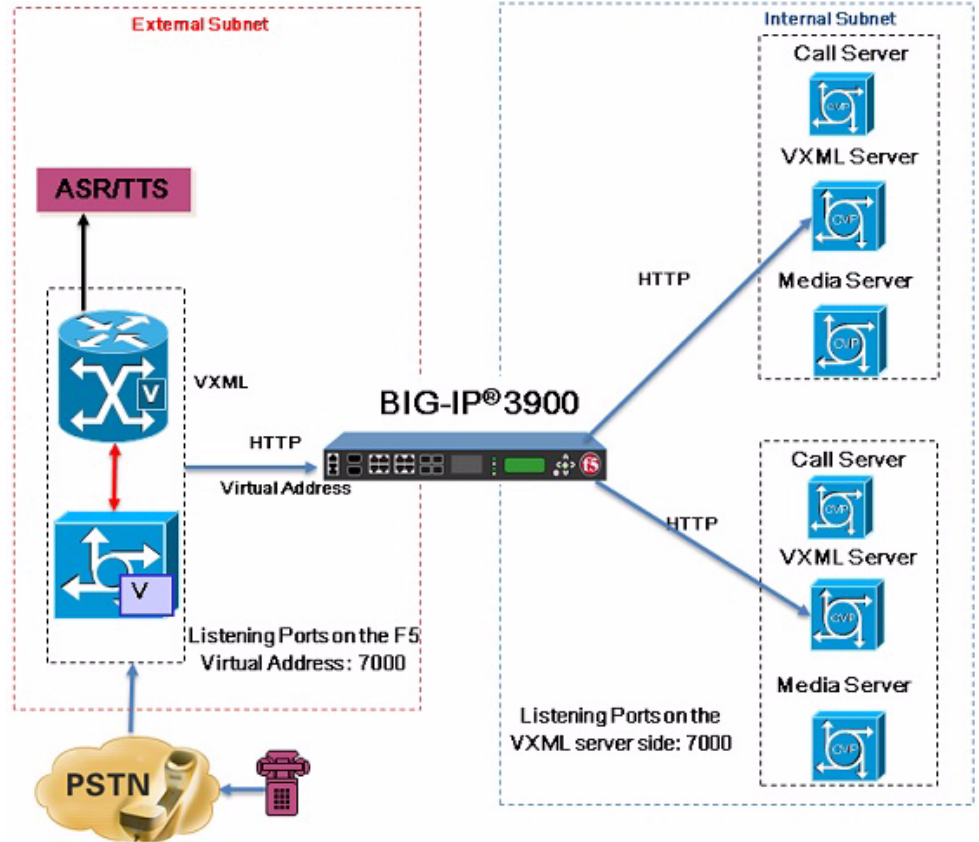


Figure 2 VXML HTTPS load balancing – SSL offload

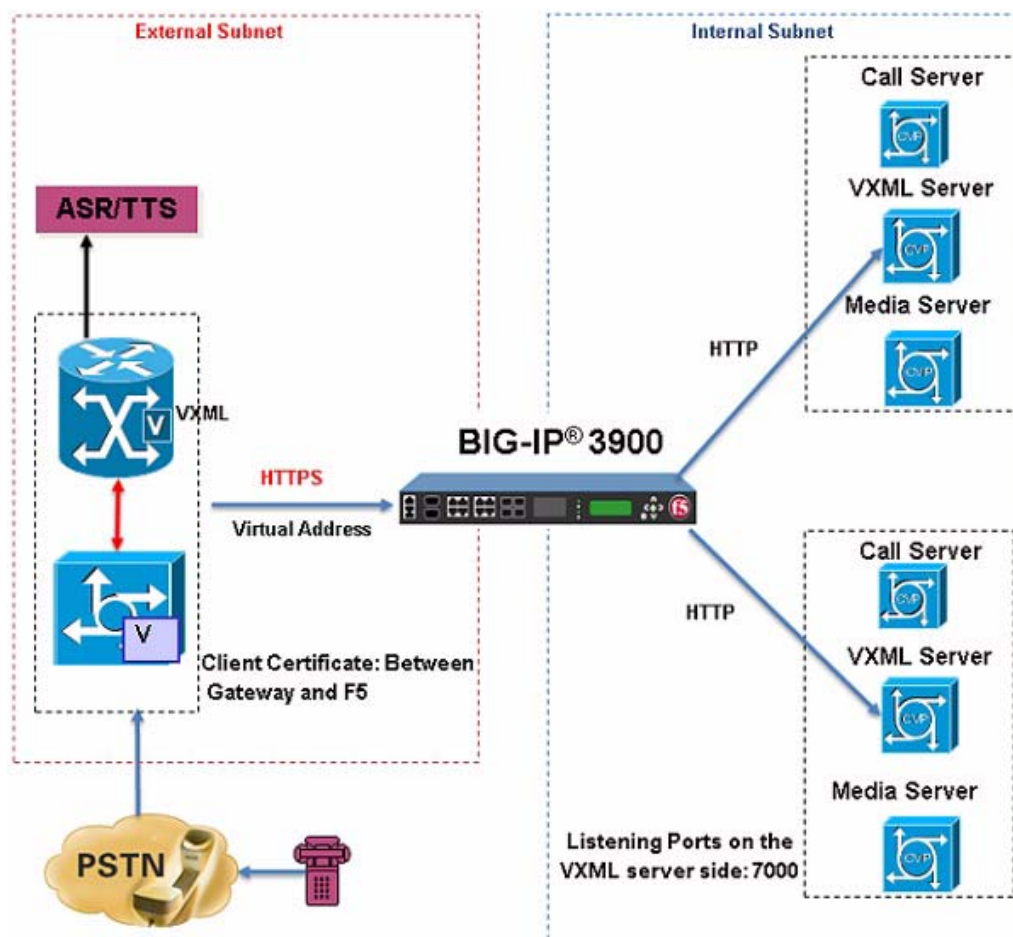


Figure 3 VXML HTTPS load balancing – HTTPS load balancing

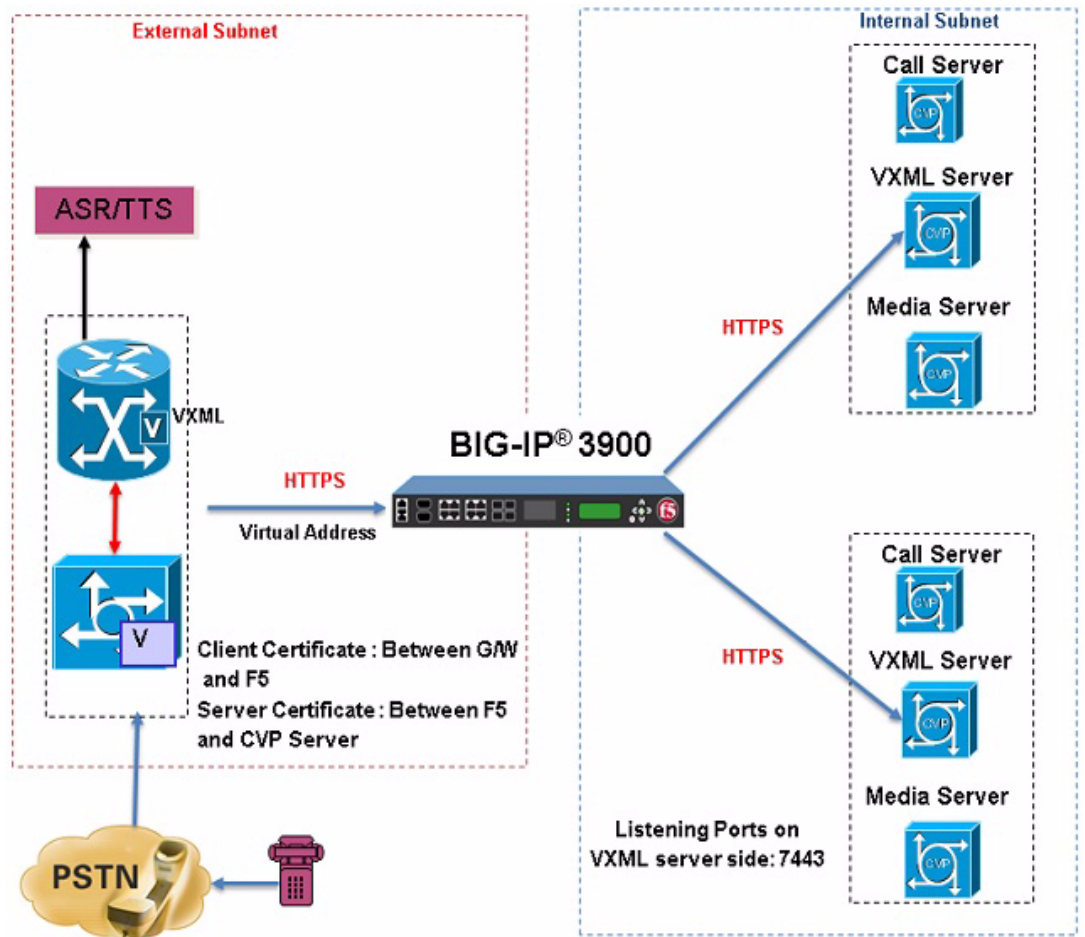
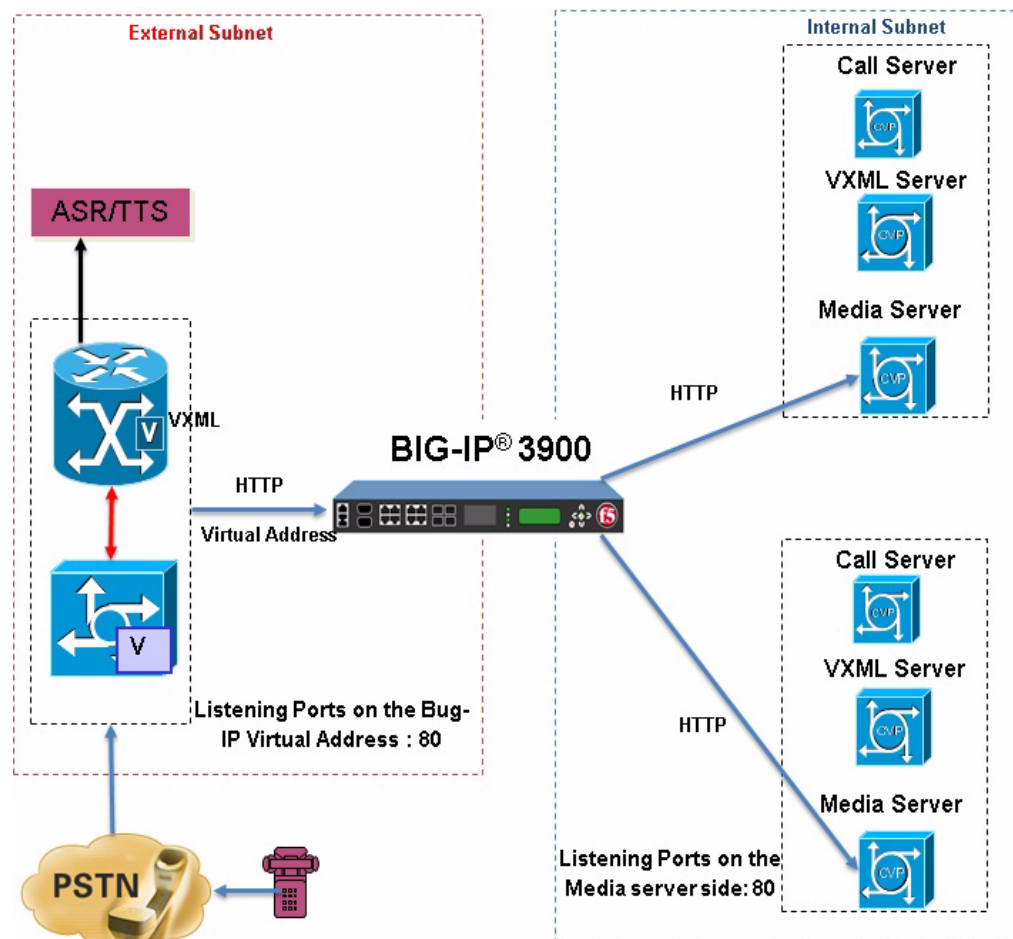


Figure 4 Media server load balancing



Note

All the above features tested with Redirect = true / false in CVP Server (Session Based / Non Session Based)

Table 1 The following table provides information on the load balancing scenarios for http / https protocols that were tested.

Component	Protocol	Port	Configuration of Internal port on F5	Comments
Media Server	TCP 80	HTTP	80	
Voice Gateway to Unified CVP VXML Server	TCP 7000	HTTP	7000	
Voice Gateway to Unified CVP VXML Server	TCP 7443	HTTPS	7443	Both End-to-End HTTPS and SSL off-loading at F5 scenarios have been tested.



Note

The scope of the document is limited for testing HTTP and HTTPS load balancing of CVP VXML Server and CVP Media Server. The load balancing of Speech Servers is not covered as a part of this document. For speech server load balancing, it is recommended to work with the Speech Server vendor and F5 for support.



Note

In the Comprehensive deployment mode, the VXML browser also fetches pages from the IVR Service in the Call Server using ports 8000/8443. This interaction must not be load balanced as the http request must use the same Call server that is handling the SIP signaling for the call.

Caveats

- The Oneconnect feature in the F5 load balancer cannot be used while using load balancing with CVP.
- Only the 7443 port of the F5 load balancer can be used for HTTPS connections.



Note

The OneConnect profile is a configuration tool in F5 to enable connection pooling. By enabling Oneconnect profile, client requests try to utilize existing server-side connections. Since both, Gateway and CVP server prefer "connection = close" header in their http requests /responses, it is recommended to disable the Oneconnect feature in the F5 load balancer. However, session persistence is maintained through HTTP cookies.

Configurations

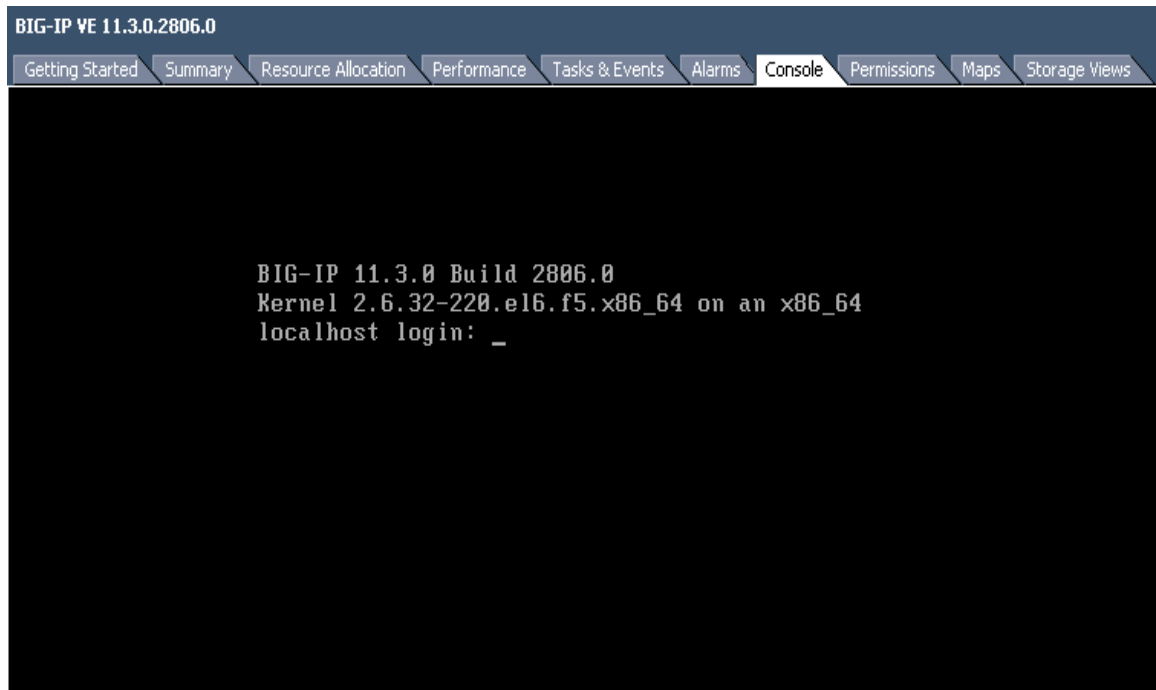
This section provides information on configuration of various components that were used to test the F5 load balancer with the Cisco CVP.

IP Configurations

The BIG-IP® VE virtual machine needs an IP address assigned to its virtual management port.

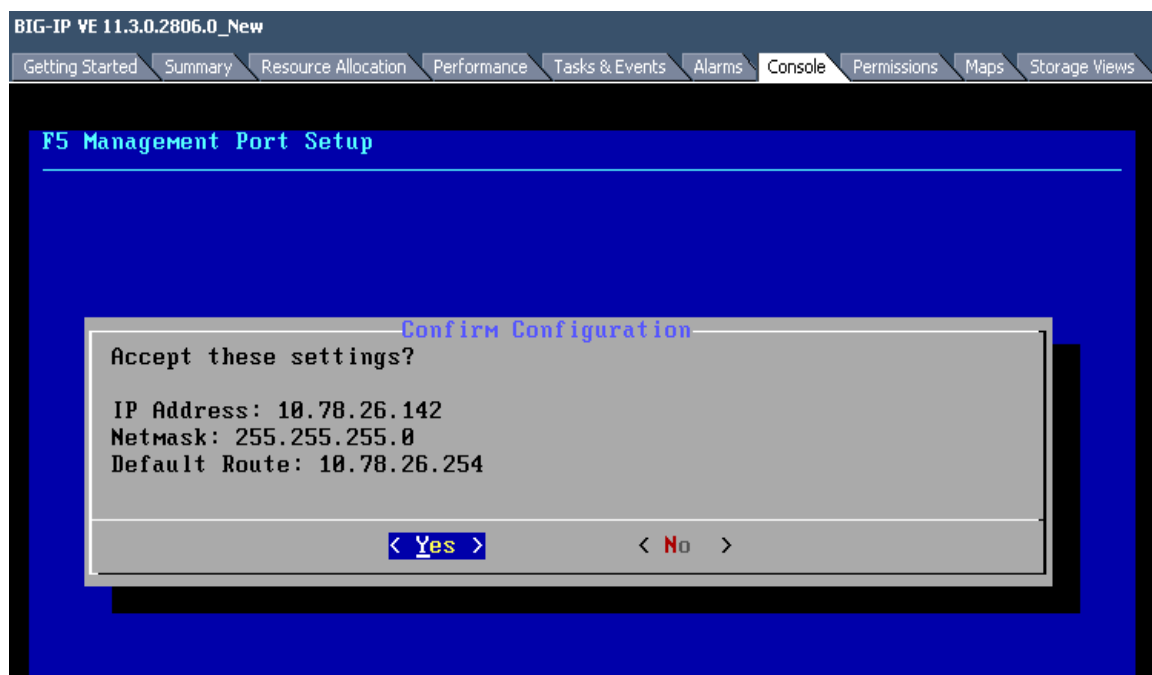
1. From the main vSphere Client screen, click the Administration menu.
2. In the resources pane, select the virtual machine you want to assign the management IP address.
3. Click the Console tab. After a few seconds, the login prompt is displayed.

Figure 5 Login Prompt



4. At the login prompt, type **root** and press Enter.
5. At the Password prompt, type **default.** and press Enter.
6. Type **config** and press Enter. The F5 Management Port Setup screen is displayed.

Figure 6 Management Port Setup screen



7. Click **Yes** if you want DHCP to automatically assign an IP address for the management port, or click **No** to manually assign an IP address and Netmask for the management port.

F5 BIG IP Load Balancer Configuration

1. Open browser and type `https://mgmt-ip` of F5. The F5 Login page is displayed.

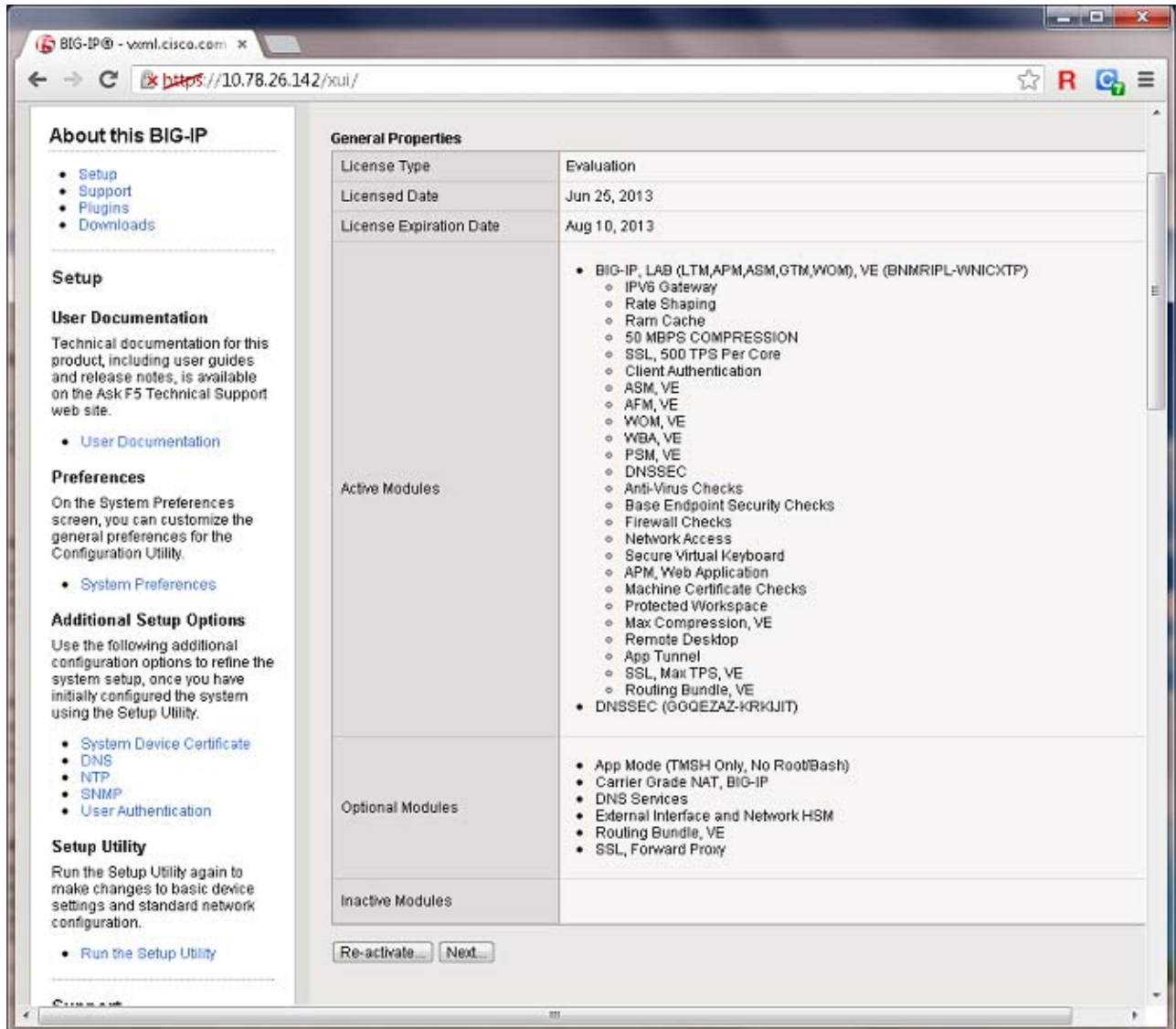
Figure 7 F5 Login page



The image shows the F5 BIG-IP Configuration Utility login page. The header includes the F5 logo, the tagline "IT Agility. Your Way.™", and the text "BIG-IP® Configuration Utility" and "F5 Networks, Inc.". The main content area is divided into two sections. On the left, there are fields for "Hostname" (containing "wml.cisco.com"), "IP Address" (containing "10.78.26.142"), "Username" (with an empty text box), and "Password" (with an empty text box). Below these fields is a "Log in" button. On the right, there is a welcome message: "Welcome to the BIG-IP Configuration Utility." followed by "Log in with your username and password using the fields on the left." The footer contains copyright information: "(c) Copyright 1996-2012, F5 Networks, Inc., Seattle, Washington. All rights reserved." and a link to "F5 Networks, Inc. Legal Notices".

2. Type **admin** in the Username field and **admin** in the Password field.
3. Click Login. The F5 General Properties page is displayed.

Figure 8 General Properties page



4. Click Next. The Current Resource Allocation page is displayed.

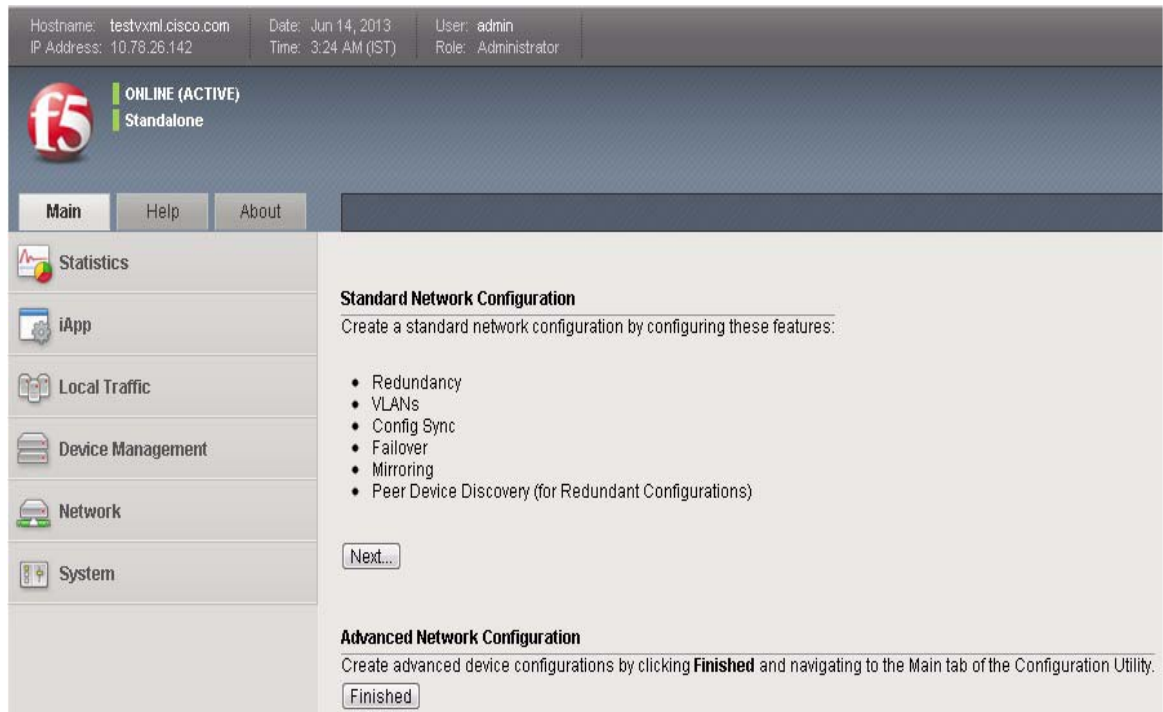
5. Click Next.

Figure 9 The Management IP page

General Properties	
Management Port Configuration	<input type="radio"/> Automatic (DHCP) <input checked="" type="radio"/> Manual
Management Port	IP Address[/prefix]: 10.78.26.142
	Network Mask: 255.255.255.0 255.255.255.0 ▼
	Management Route: 10.78.26.254
Host Name	testxml.cisco.com
Host IP Address	Use Management Port IP Address ▼
Time Zone	Asia/Calcutta ▼
User Administration	
Root Account	Password:
	Confirm:
Admin Account	Password:
	Confirm:
SSH Access	<input checked="" type="checkbox"/> Enabled
SSH IP Allow	* All Addresses ▼
<input type="button" value="Back"/> <input type="button" value="Next..."/>	

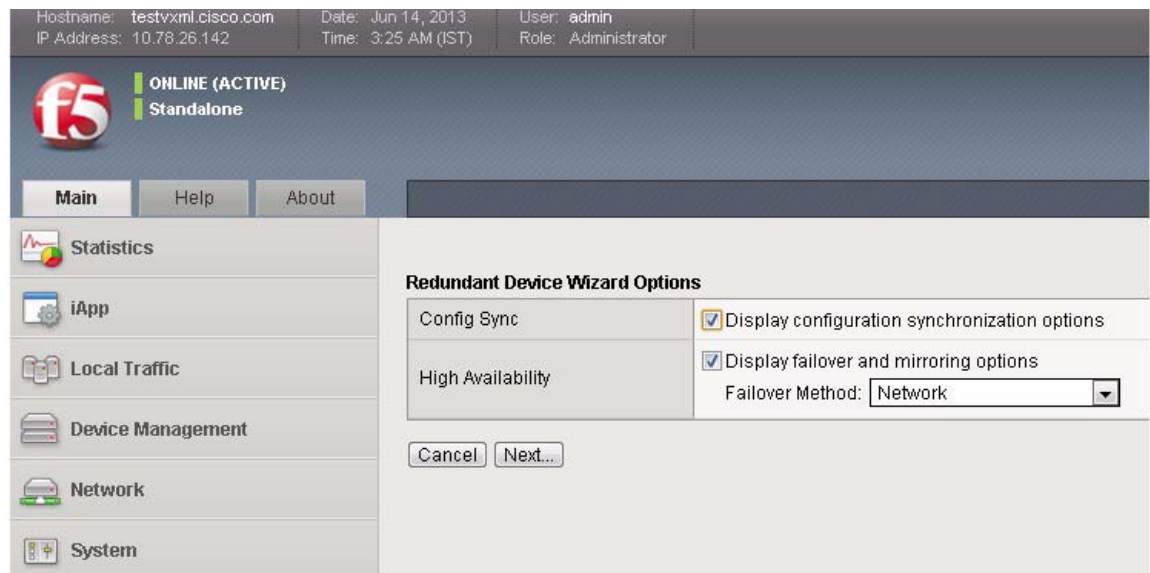
6. Select Manual option, so that big-IP does not reset to default IP address.
7. Type the IP address in the IP Address[/Prefix] field and click Next.
8. The F5 login page is displayed again. After login, the Network Configuration page is displayed.

Figure 10 Network Configuration page



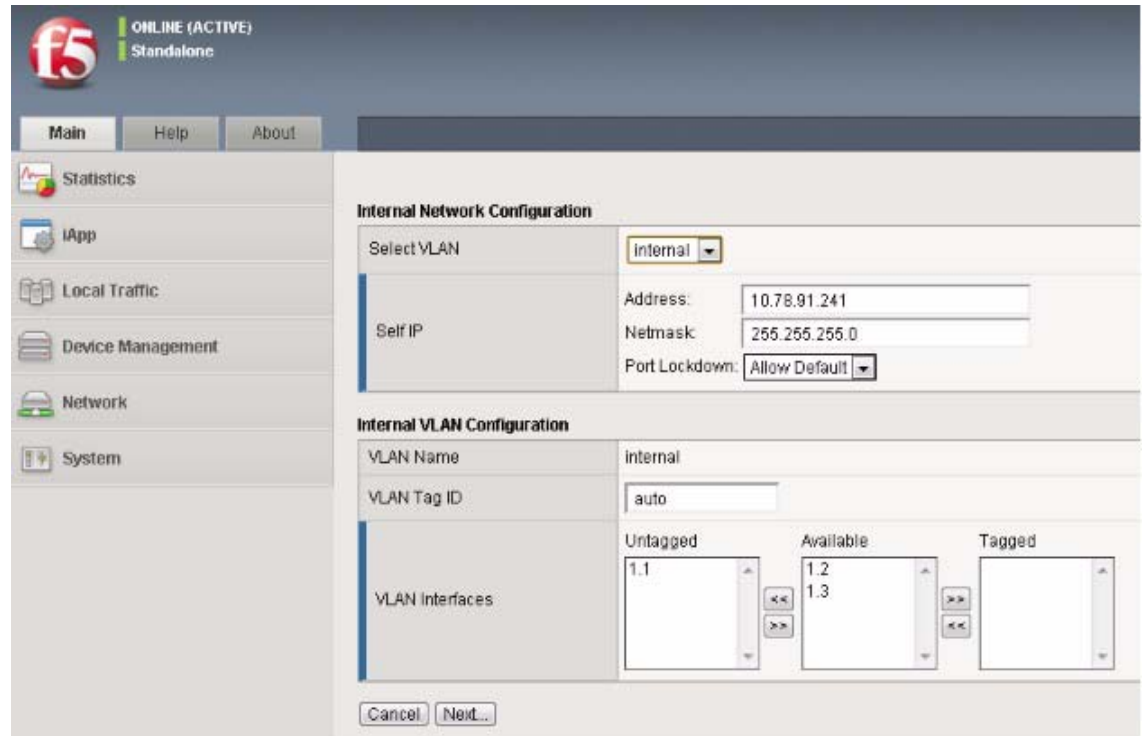
9. Click Next.

Figure 11 The Redundant Device Wizard options



10. Clear the Config Sync option, and click Next. The network configuration page is displayed. You can configure both internal and external IP address.

Figure 12 *Internal Network Configuration*



Internal Network Configuration

Select VLAN: Internal

Self IP

Address: 10.78.91.241

Netmask: 255.255.255.0

Port Lockdown: Allow Default

Internal VLAN Configuration

VLAN Name: Internal

VLAN Tag ID: auto

VLAN Interfaces

Untagged: 1.1

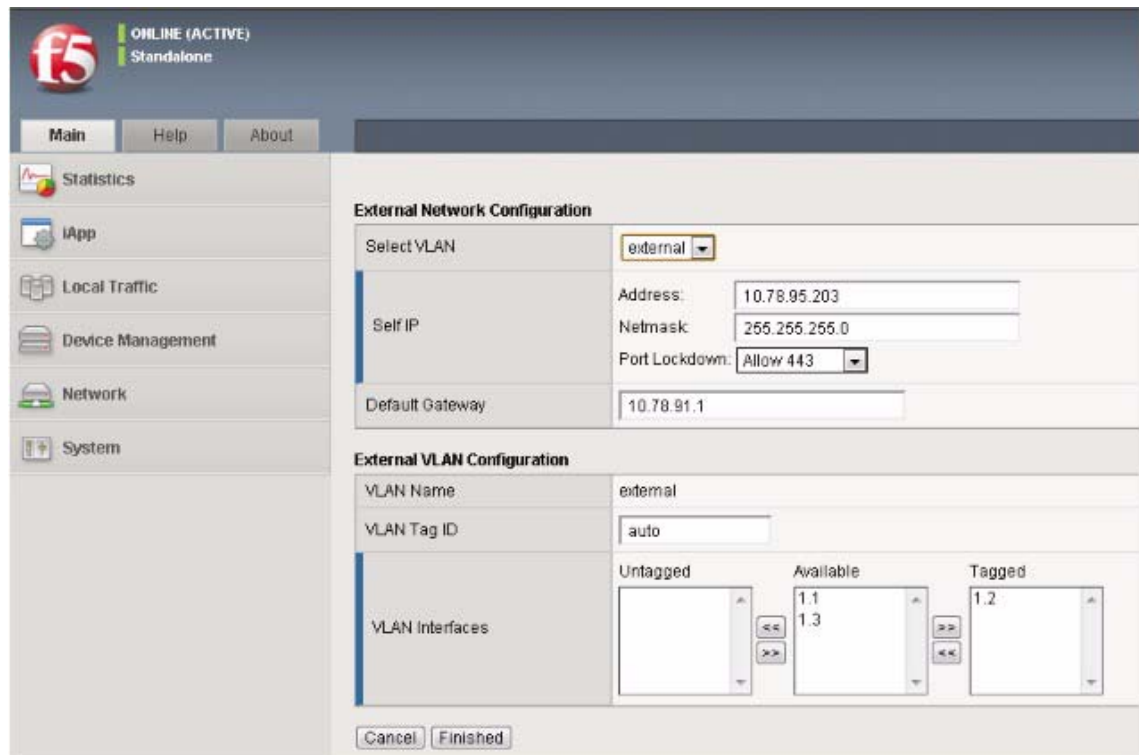
Available: 1.2, 1.3

Tagged:

Cancel Next...

11. In the Self IP, type the IP address and Netmask as mentioned in the [Figure 12](#) for internal configuration.
12. Click Next. The external configuration page is displayed.

Figure 13 *External IP configuration*



The screenshot shows the F5 configuration interface. At the top, it says "f5 ONLINE (ACTIVE) Standalone". Below this are tabs for "Main", "Help", and "About". On the left is a sidebar with icons for "Statistics", "iApp", "Local Traffic", "Device Management", "Network", and "System". The main area is divided into two sections: "External Network Configuration" and "External VLAN Configuration".

External Network Configuration:

- Select VLAN: external (dropdown)
- Self IP:
 - Address: 10.78.95.203
 - Netmask: 255.255.255.0
 - Port Lockdown: Allow 443 (dropdown)
- Default Gateway: 10.78.91.1

External VLAN Configuration:

- VLAN Name: external
- VLAN Tag ID: auto
- VLAN Interfaces:
 - Untagged: (empty list)
 - Available: 1.1, 1.3
 - Tagged: 1.2

At the bottom of the configuration area are "Cancel" and "Finished" buttons.

13. In the Self IP, type the IP address and the Netmask as mentioned in the [Figure 13](#) for internal configuration.
14. Click Finished. The F5 IP configuration is completed.

HTTP Configuration

HTTP Gateway Configuration - Dial-peer configuration at gateway (Standalone configuration)

Application

```
service helloworld flash:CVPSelfService.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  param CVPSelfService-app HelloWorld
  param CVPPrimaryVXMLServer 10.78.91.242 ( F5 Virtual IP Address)
  param CVPSelfService-port 7000
```



```
dial-peer voice 8778778 voip
service helloworld
incoming called-number 8778778
codec g711ulaw
exit
```

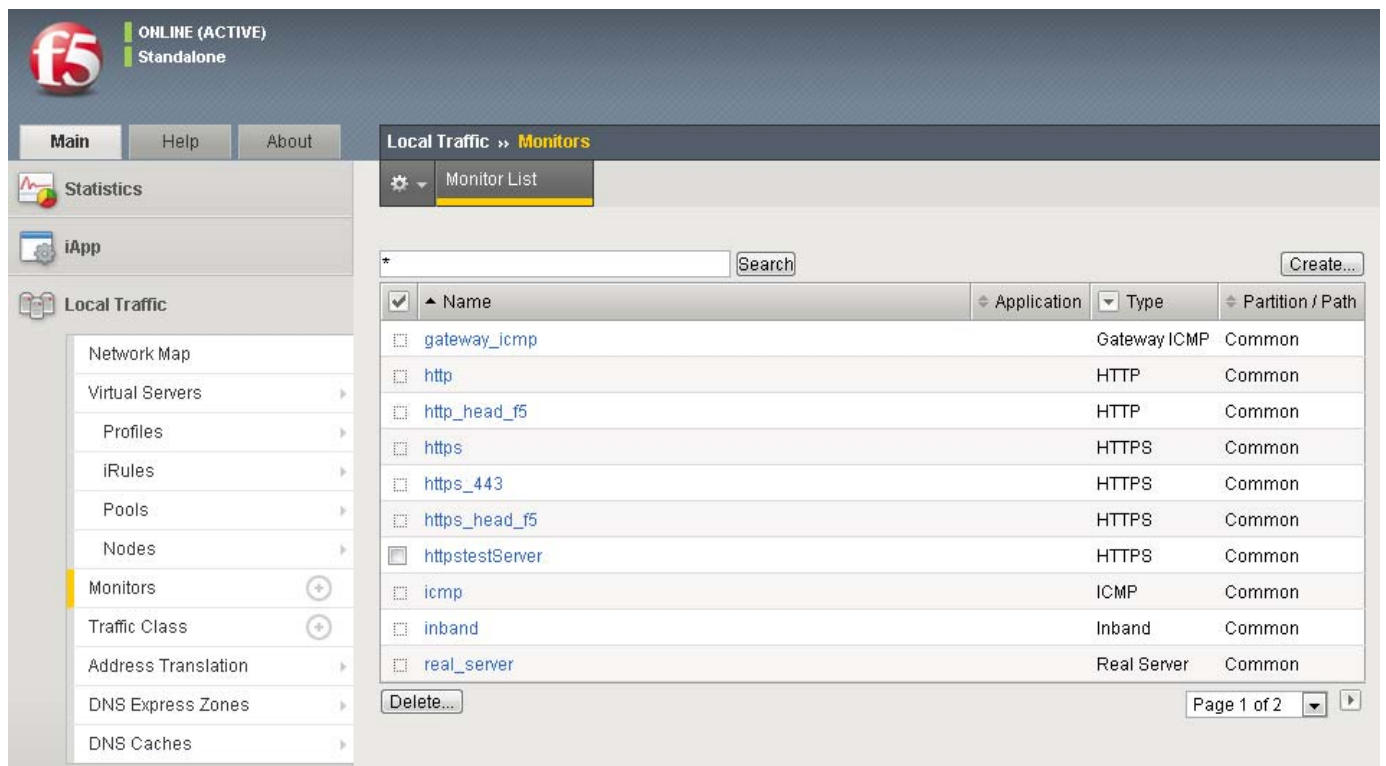
HTTP F5 BIG IP Load Balancer Configuration

The following are the steps to configure F5 for HTTP.

Create a monitor (probe) for CVP

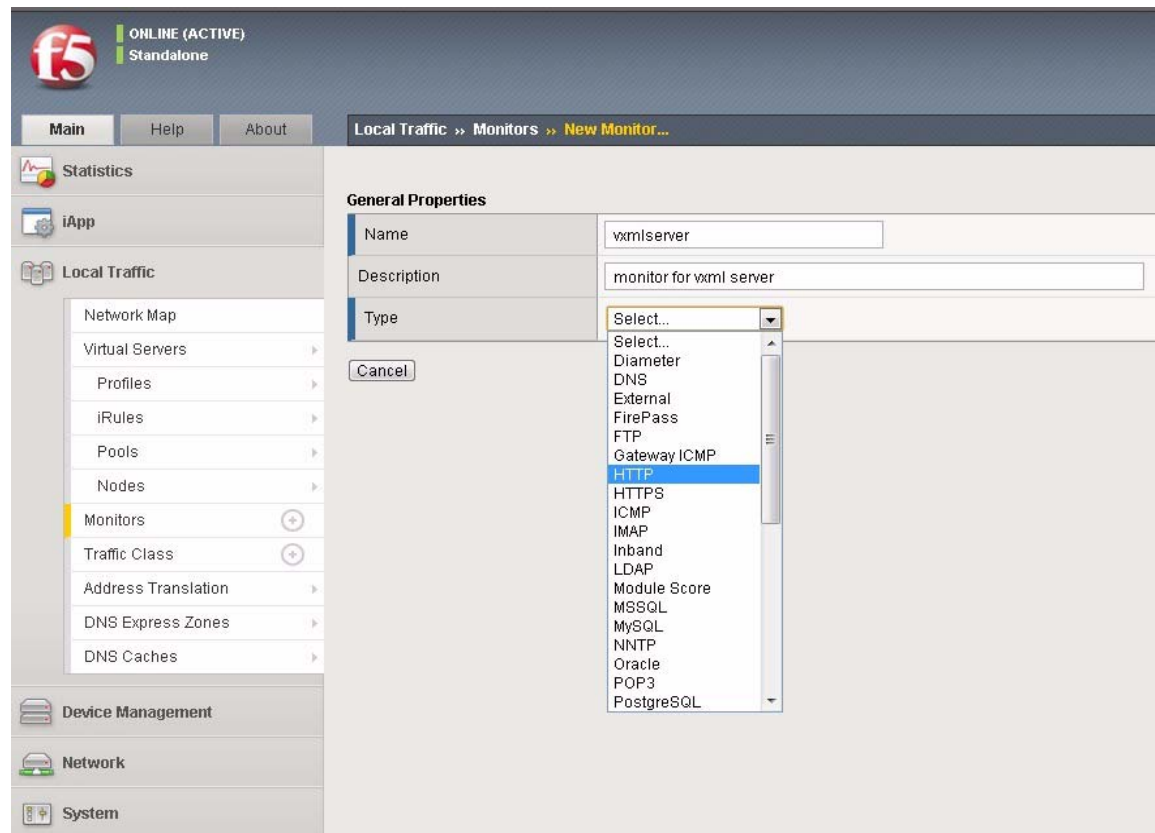
1. Login to the F5 system.
2. Click the Local Traffic tab on left pane and select Monitor from the list. The Monitors page displays the list of monitors in the right pane.

Figure 14 Monitor page



3. Click Create. The New Monitor page is displayed.

Figure 15 New Monitor page



ONLINE (ACTIVE)
Standalone

Main Help About

Local Traffic » Monitors » New Monitor...

Statistics

iApp

Local Traffic

- Network Map
- Virtual Servers
- Profiles
- iRules
- Pools
- Nodes
- Monitors
- Traffic Class
- Address Translation
- DNS Express Zones
- DNS Caches

Device Management

Network

System

General Properties

Name vxmlserver

Description monitor for vxml server

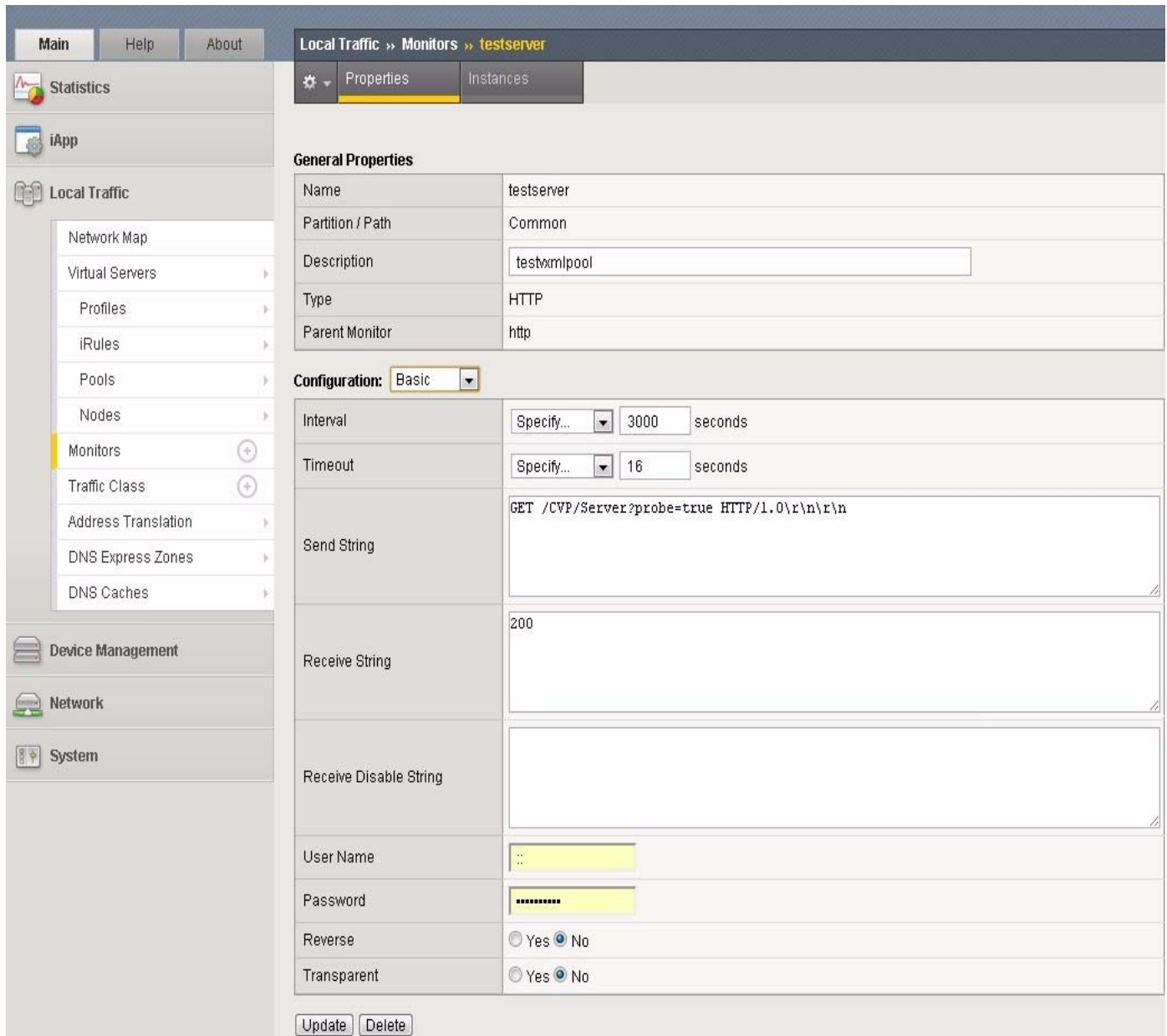
Type Select...

- Select...
- Diameter
- DNS
- External
- FirePass
- FTP
- Gateway ICMP
- HTTP
- HTTPS
- ICMP
- IMAP
- Inband
- LDAP
- Module Score
- MSSQL
- MySQL
- NNTP
- Oracle
- POP3
- PostgreSQL

Cancel

4. Enter a monitor name and description in the respective fields.
5. From the Type drop-down list, select http.

Figure 16 Monitor Configuration page



Local Traffic » Monitors » testserver

General Properties

Name	testserver
Partition / Path	Common
Description	testxmlpool
Type	HTTP
Parent Monitor	http

Configuration: Basic

Interval	Specify... 3000 seconds
Timeout	Specify... 16 seconds
Send String	GET /CVP/Server?probe=true HTTP/1.0\r\n\r\n\r\n
Receive String	200
Receive Disable String	
User Name	::
Password
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No

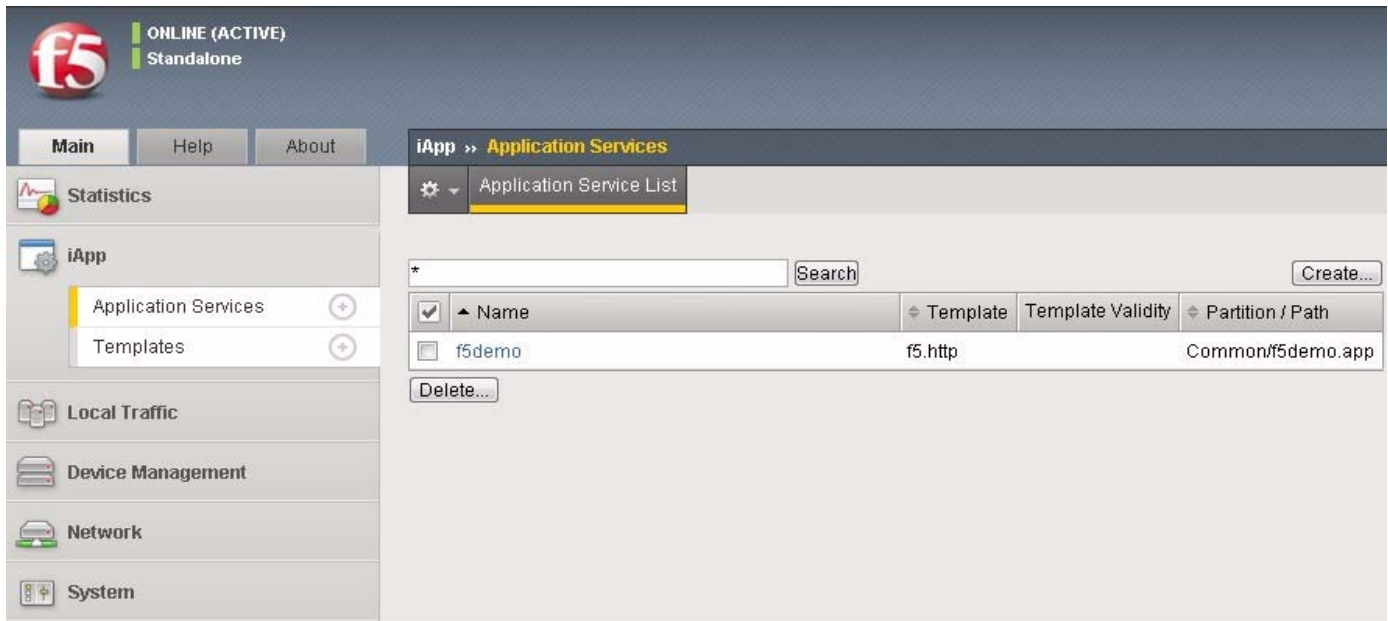
Update Delete

6. Under Configuration section, in the Send String text box, enter **GET /CVP/Server?probe=true HTTP/1.0\r\n\r\n\r\n** command.
7. Click Update. The monitor is created successfully.

Create a virtual server for CVP

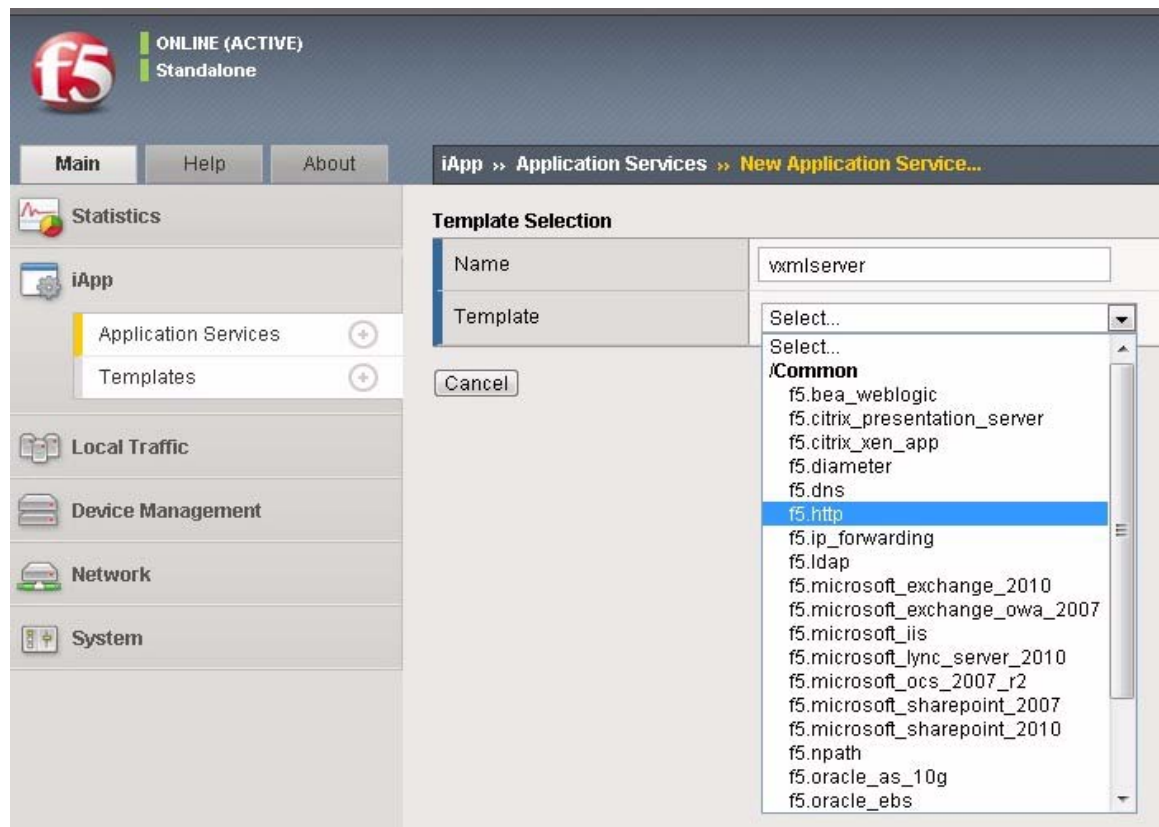
1. Login to the F5 system.
2. In the main page, click iApp tab on the left pane.
3. Select Application servers from the list.

Figure 17 iApp page to create virtual server for CVP



4. Click Create. The new application service page is displayed.

Figure 18 New Application Service page



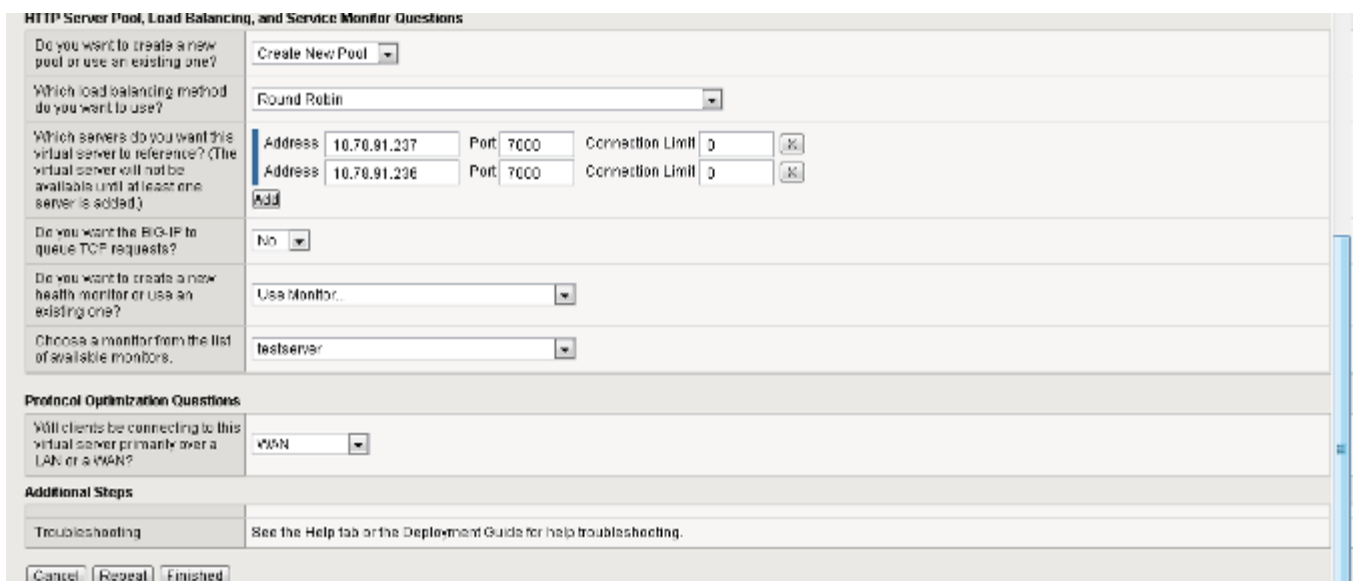
5. Enter the server name in the Name field.
6. From the Template drop-down list, select “f5.http”. The F5 template for HTTP is displayed.

Figure 19 *F5 HTTP Application services page*



7. Under the Virtual Server Creations, type the IP address that you want to use for the virtual server.
8. Enter the port number you want to use for the virtual server.

Figure 20 *F5 HTTP Application services page Cont...*



9. Under HTTP Server Pool, Load Balancing, and Service Monitor Questions section,
 - a. To create a new server pool, select Create New Pool from the “Do you want to create a new pool use an existing one?” drop-down list.
 - b. Enter the CVP server IP address and enter Port number.
10. Click Finished. The HTTP virtual server for CVP is created.

Disable Oneconnect

1. To disable Oneconnect, click Local Traffic tab on the left pane.
2. Select Virtual Machine from the list. The Virtual Machine page displays with the configuration.
3. Under Configuration section, set the Oneconnect option to None. This disables the Oneconnect option.

HTTPS Configuration

HTTPS Configuration for CVP Server

- The following certificates are available for HTTPS configuration with CVP:
 - Call server self-signed certificate (callserver.crt) and keys (callserver.key) located in \$CVP_HOME/conf/security
 - VXML server self-signed certificate (vxml.crt) and key (vxml.key) located in \$CVP_HOME/conf/security
- Call Server running HTTPS listens (accepting connections) on port 8443
- VXML Server running HTTPS listens (accepting connections) on port 7443.



Note

Certificates must be signed by a Certificate Authority (CA) prior to use on the F5 or IOS gateway.

- To request for a certificate enter the following command
openssl req -new -key <keyfile>.key -out <certrequest>.csr
- Certificate is then signed by the CA using the .csr file.
- Signed certificate returned by the CA is put in place of the self-signed .crt file.



Note

The CVP VXML and Call Server must be restarted when signed certificate is installed.

Example,

```
-----BEGIN CERTIFICATE-----
MIIGTzCCBTegAwIBAgIKJozFswAAAAAACjANBgkqhkiG9w0BAQUFADCByDEdMBsG
CSqGSIb3DQEJARYOc3BhbUBjaXNjb3Y5bjB20xCzAJBgNVBAYTAlVTMRYwFAYDVQQI
...
MkYIYifimRdD1U3AH6iPczbi+ryUM5mvcl9fTnq/DiaKqDSAo=
-----END CERTIFICATE-----
```



Note

Certificate file should be in base 64 encoded format, before uploading to F5.

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 F5 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
```

Dial-peer configuration at gateway (Standalone configuration)

Application

```
service Secure flash:CVPSelfService.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  param CVPSelfService-app Test_GD_DTMF
  param CVPPrimaryVXMLServer 10.78.91.242 (F5 Virtual IP)
  param CVPSelfService-port 7443
  param CVPSelfService-SSL 1
```

```
dial-peer voice 4586797 voip
service Secure
incoming called-number 4586797
codec g711ulaw
exit
```

HTTPS F5 BIG IP Configuration

Pre requisites for HTTPS configuration at F5

The following are the steps to configure F5 for HTTPS to create SSL offloading and end to end HTTPS traffic.

1. Import certificates (.Key and .CSR) files using Local Traffic -> SSL Certificates.

Figure 21 *SSL Certificate Loading Page*



ONLINE (ACTIVE)
Standalone

Main Help About

System » Device Certificates : Device Certificate » Device Certificate

Statistics

iApp

Local Traffic

Device Management

Network

System

Configuration

Device Certificates

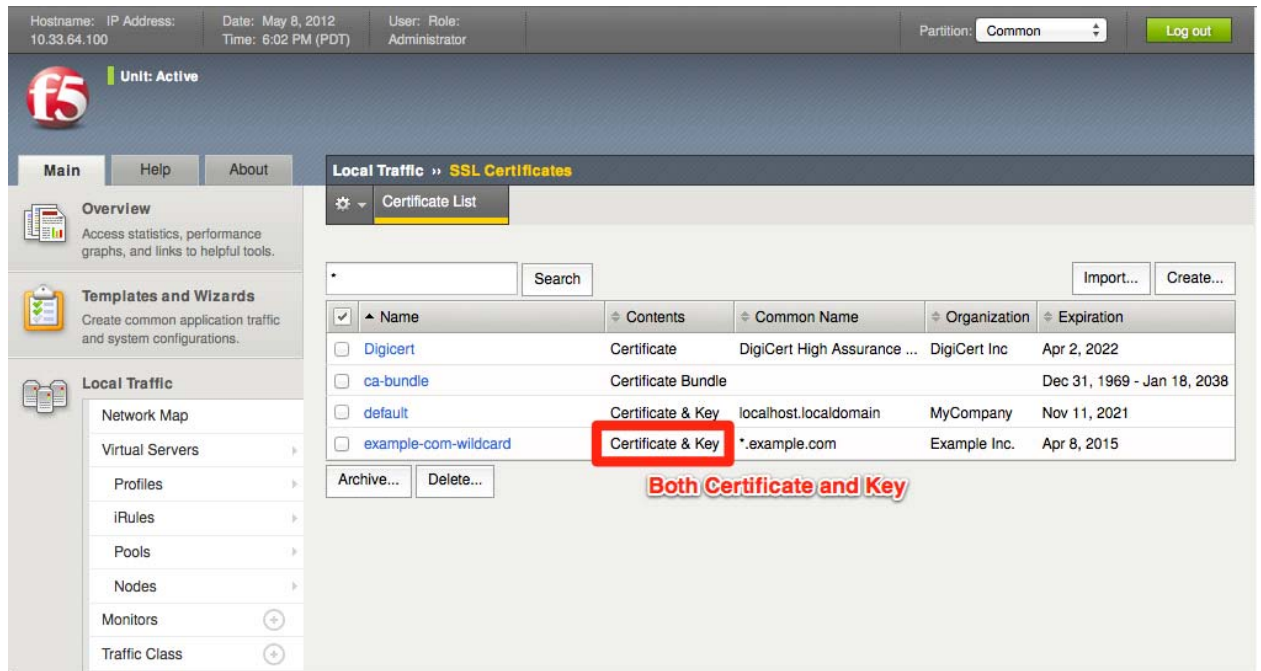
SSL Certificate/Key Source

Import Type	Certificate and Key
Certificate Name	server
Certificate Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text Choose File xml237.csr
Key Source	<input checked="" type="radio"/> Upload File <input type="radio"/> Paste Text Choose File xml.key
Free Space on Disk	84 MB

Cancel Import

2. From the Import Type drop-down list, select Certificate and Key option.
3. To upload a certificate (.csr file), select Upload File and then click Choose File.
4. To upload the Key(.key file), select Upload option and then click Choose File.
5. Click Import.

Figure 22 *SSL Certificate and key is displayed*



Create SSL profile

After the SSL certificate is uploaded to the load balancer, create an SSL profile to use the certificate. The following are the steps to create SSL profile:

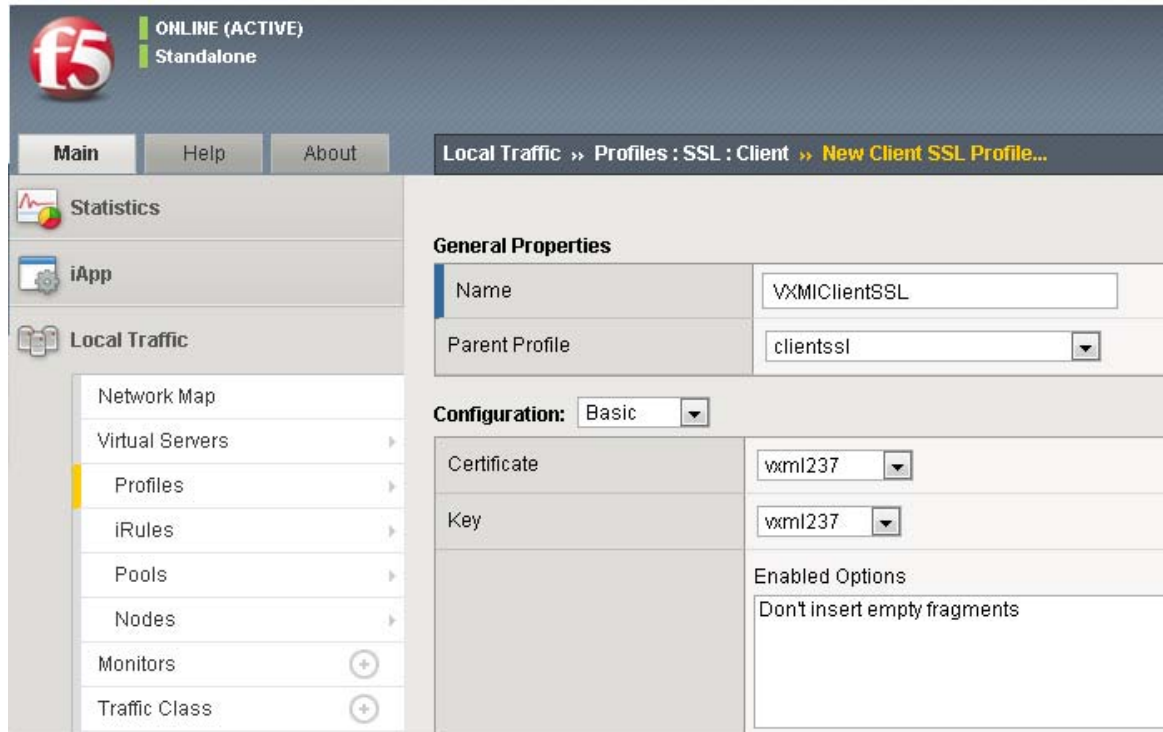
1. Start F5 console.
2. Click Local Traffic in the left pane.
3. Click Profiles, select SSL, and then select Client. The New Client SSL Client page is displayed.



Note

The term "Client" is the traffic between the gateway and the load balancer (conversely "Server" means traffic between your CVP VXML servers and the load balancer).

Figure 23 New SSL Profile Configuration



The screenshot shows the F5 iApp configuration interface. The top status bar indicates 'ONLINE (ACTIVE)' and 'Standalone'. The breadcrumb trail is 'Local Traffic » Profiles : SSL : Client » New Client SSL Profile...'. The left sidebar contains a tree view with 'Local Traffic' expanded, showing options like Network Map, Virtual Servers, Profiles, iRules, Pools, Nodes, Monitors, and Traffic Class. The main configuration area is titled 'General Properties' and includes fields for 'Name' (VXMIclientSSL) and 'Parent Profile' (clientsssl). Below this is a 'Configuration' section with a 'Basic' tab selected. It contains 'Certificate' and 'Key' dropdown menus, both set to 'vxm1237'. An 'Enabled Options' section is also visible, with 'Don't insert empty fragments' checked.

4. From the Certificate and Key fields, select the certificate and key you want to use.
5. Click Finished.

Create Virtual Server for SSL Offloading at F5

1. Open F5 console.
2. Click iAPP in the left pane, and select Application Services.
3. Select Template.
4. In the Application Services page, under SSL Encryption Questions section, set the **Do you want the BIG-IP system to offload SSL processing from the HTTP servers?** option to “Yes”.
5. Select the SSL certificate (.crt file) from the **Which certificate do you want the BIG-IP system to use to authenticate the server? (You may need to import a certificate before deploying this Template.)** option.
6. Select the key from the **Which key do you want the BIG-IP system to use for encryption? (You may need to import a key before deploying this Template.)** option.



Note These certificates can be mapped to the install certificates on the IOS gateway.

Figure 24 Application Services Setting

Main
Help
About
iApp » Application Services » vxmlserver

Statistics
iApp
Application Services
Templates
Local Traffic
Device Management
Network
System

Template Selection: Advanced

Name	https_offloadserver
Template	f5.http
Device Group	<input checked="" type="checkbox"/> Inherit device group from current partition / path None
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating)

Welcome to the HTTP template

Introduction	This template supports most simple web server implementations
Check for updates	Ensure you are using the most recent template before continuing. This template was released on 2012-10-12. Check for newer versions online at the AskF5 Knowledge Base (http://support.f5.com/kb/en-us/solutions/public/13000/400/sol13422.html).
Prerequisites	If you plan on using this template to configure the BIG-IP system for processing encrypted traffic, you need to import an SSL certificate and key that correspond to all fully-qualified DNS names that you are using for the traffic. Importing SSL certificates and keys is not a part of this template; see Local Traffic >> SSL Certificate List.
Additional features available	Provisioning AVR will enable additional options in this template.
Additional features available	Provisioning WAM will enable additional options in this template.

SSL Encryption Questions

Do you want the BIG-IP system to offload SSL processing from the HTTP servers?	Yes
Which certificate do you want the BIG-IP system to use to authenticate the server? (You may need to import a certificate before deploying this Template.)	vxml237.crt
Which key do you want the BIG-IP system to use for encryption? (You may need to import a key before deploying this Template.)	vxml237.key

Figure 25 Application Services Setting Cont...

Virtual Server Questions			
What IP address do you want to use for this virtual server?	<input type="text" value="10.78.91.242"/>		
What port do you want to use for this virtual server?	<input type="text" value="7443"/>		
Do you want to redirect traffic that comes in as HTTP to HTTPS?	<input type="button" value="No"/>		
Do the HTTP servers have a route back to application clients via this BIG-IP system?	<input type="button" value="No"/>		
Will you have more than 64,000 connections at one time? If so, you will need to enter at least one IP address for each 64,000 connections.	<input type="button" value="No"/>		
Are the HTTP servers configured to use NTLM authentication?	<input type="button" value="No"/>		

HTTP Server Pool, Load Balancing, and Service Monitor Questions							
Do you want to create a new pool or use an existing one?	<input type="button" value="Create New Pool"/>						
Which load balancing method do you want to use?	<input type="button" value="Round Robin"/>						
Which servers do you want this virtual server to reference? (The virtual server will not be available until at least one server is added.)	Address	<input type="text" value="10.78.91.237"/>	Port	<input type="text" value="700"/>	Connection Limit	<input type="text" value="0"/>	<input type="button" value="X"/>
	Address	<input type="text" value="10.78.91.236"/>	Port	<input type="text" value="7000"/>	Connection Limit	<input type="text" value="0"/>	<input type="button" value="X"/>
	<input type="button" value="Add"/>						
Do you want the BIG-IP to queue TCP requests?	<input type="button" value="No"/>						
Do you want to create a new health monitor or use an existing one?	<input type="button" value="Use Monitor..."/>						
Choose a monitor from the list of available monitors.	<input type="button" value="httpstestServer"/>						

7. Enter F5 virtual IP address (The same IP address that was configured for Dial-Peer Configure at gateway)
8. Enter the port you want to use the virtual server.
9. Click Finished.



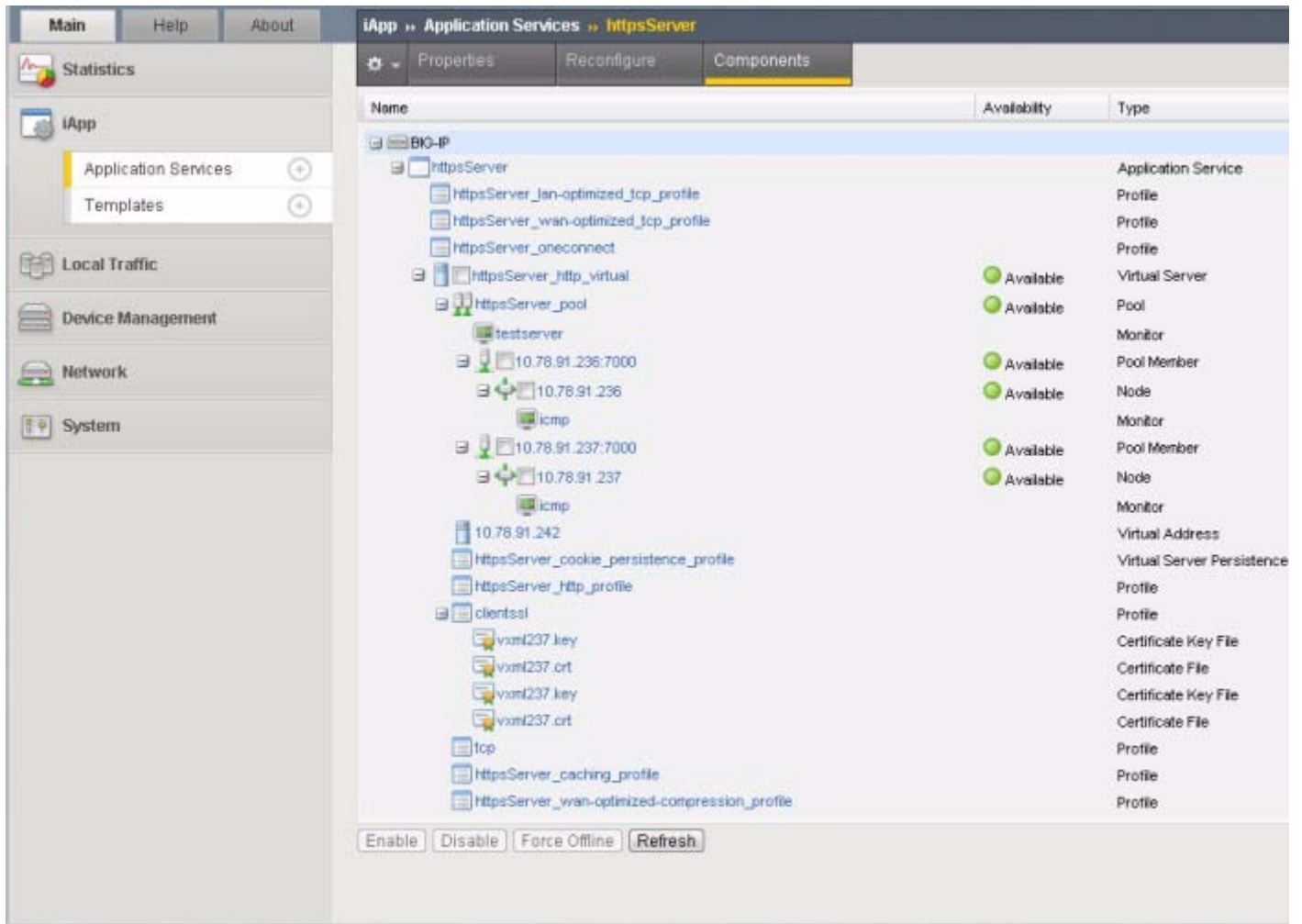
Note

Leave all the other fields in its default values.

After you creating the HTTPS Application Service for SSL Offloading, configure the virtual server by following these steps:

1. From the Local Traffic > Virtual Servers options, select the virtual server that is created.
2. Under Configuration settings, set the **Oneconnect profile** option to None.
3. From SSL Profile (Client) option, select a client profile that is listed and click Add.
4. Click Update. The F5 configuration for HTTPS Application Service - SSL Offloading is completed.

Figure 26 F5 configuration for HTTPS Application Service - SSL Offloading



Name	Availability	Type
BIG-IP		
httpsServer		Application Service
httpsServer_lan-optimized_tcp_profile		Profile
httpsServer_wan-optimized_tcp_profile		Profile
httpsServer_oneconnect		Profile
httpsServer_http_virtual	Available	Virtual Server
httpsServer_pool	Available	Pool
testserver		Monitor
10.78.91.236:7000	Available	Pool Member
10.78.91.236	Available	Node
icmp		Monitor
10.78.91.237:7000	Available	Pool Member
10.78.91.237	Available	Node
icmp		Monitor
10.78.91.242		Virtual Address
httpsServer_cookie_persistence_profile		Virtual Server Persistence
httpsServer_http_profile		Profile
clientssl		Profile
vxm1237.key		Certificate Key File
vxm1237.crt		Certificate File
vxm1237.key		Certificate Key File
vxm1237.crt		Certificate File
tcp		Profile
httpsServer_caching_profile		Profile
httpsServer_wan-optimized-compression_profile		Profile

Enable Disable Force Offline Refresh

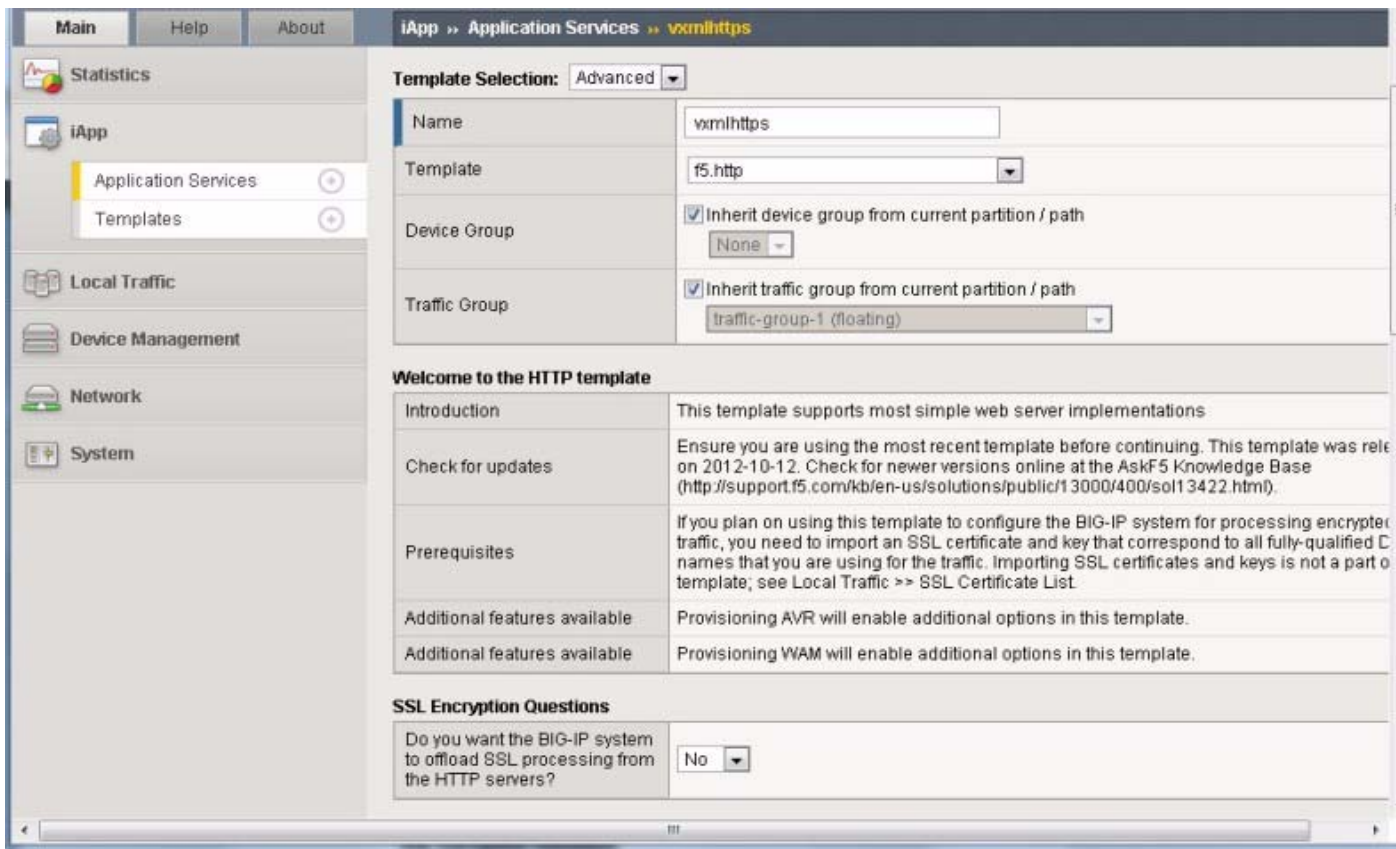
Configuration of End to End HTTPS at F5

The following are the steps to configure end to end HTTPS traffic at F5:

Create Virtual Server for End to End HTTPS Traffic

1. Open F5 console.
2. Click iApp in the left pane, and select Application Services.
3. Select HTTP Template.
4. In the Application Services page, under SSL Encryption Questions section, set the **Do you want the BIG-IP system to offload SSL processing from the HTTP servers?** option to “No”. The default setting of this option is “No”

Figure 27 Application Services configuration for end to end HTTPS traffic



The screenshot shows the F5 iApp Configuration page for Application Services. The left pane shows the navigation menu with options: Main, Help, About, Statistics, iApp, Application Services, Templates, Local Traffic, Device Management, Network, and System. The main pane displays the configuration for the vxm1https virtual server. The Template Selection is set to Advanced. The Name is vxm1https, the Template is f5.http, and the Device Group is None. The Traffic Group is traffic-group-1 (floating). The SSL Encryption Questions section shows the option "Do you want the BIG-IP system to offload SSL processing from the HTTP servers?" set to No.

Template Selection: Advanced	
Name	vxm1https
Template	f5.http
Device Group	<input checked="" type="checkbox"/> Inherit device group from current partition / path None
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from current partition / path traffic-group-1 (floating)

Welcome to the HTTP template

Introduction	This template supports most simple web server implementations
Check for updates	Ensure you are using the most recent template before continuing. This template was released on 2012-10-12. Check for newer versions online at the AskF5 Knowledge Base (http://support.f5.com/kb/en-us/solutions/public/13000/400/sol13422.html).
Prerequisites	If you plan on using this template to configure the BIG-IP system for processing encrypted traffic, you need to import an SSL certificate and key that correspond to all fully-qualified C names that you are using for the traffic. Importing SSL certificates and keys is not a part of this template; see Local Traffic >> SSL Certificate List.
Additional features available	Provisioning AVR will enable additional options in this template.
Additional features available	Provisioning WAM will enable additional options in this template.

SSL Encryption Questions

Do you want the BIG-IP system to offload SSL processing from the HTTP servers?	No
--	----

Figure 28 Application Services configuration for end to end HTTPS traffic Cont...

Virtual Server Questions	
What IP address do you want to use for this virtual server?	10.78.91.242
What port do you want to use for this virtual server?	7443
Do the HTTP servers have a route back to application clients via this BIG-IP system?	No
Will you have more than 64,000 connections at one time? If so, you will need to enter at least one IP address for each 64,000 connections.	No
Are the HTTP servers configured to use NTLM authentication?	No

HTTP Server Pool, Load Balancing, and Service Monitor Questions	
Do you want to create a new pool or use an existing one?	Create New Pool
Which load balancing method do you want to use?	Round Robin
Which servers do you want this virtual server to reference? (The virtual server will not be available until at least one server is added.)	<div>Address 10.78.91.237 Port 7443 Connection Limit 0 X</div> <div>Address 10.78.91.236 Port 7443 Connection Limit 0 X</div> <div>Add</div>
Do you want the BIG-IP to queue TCP requests?	No
Do you want to create a new health monitor or use an existing one?	Use Monitor...
Choose a monitor from the list of available monitors.	httpstestServer

5. Enter F5 virtual IP address (The same IP address that was configured for Dial-Peer Configure at gateway)
6. In the **Which servers do you want this virtual server to reference? (The virtual server will not be available until at least one server is added.)** field, enter the IP address of CVP server. Also, configure the Port to 7443 for virtual server.
7. From the **Do you want to create a new health monitor or use an existing one?** list, select Use Monitor.
8. Click Finished.



Note

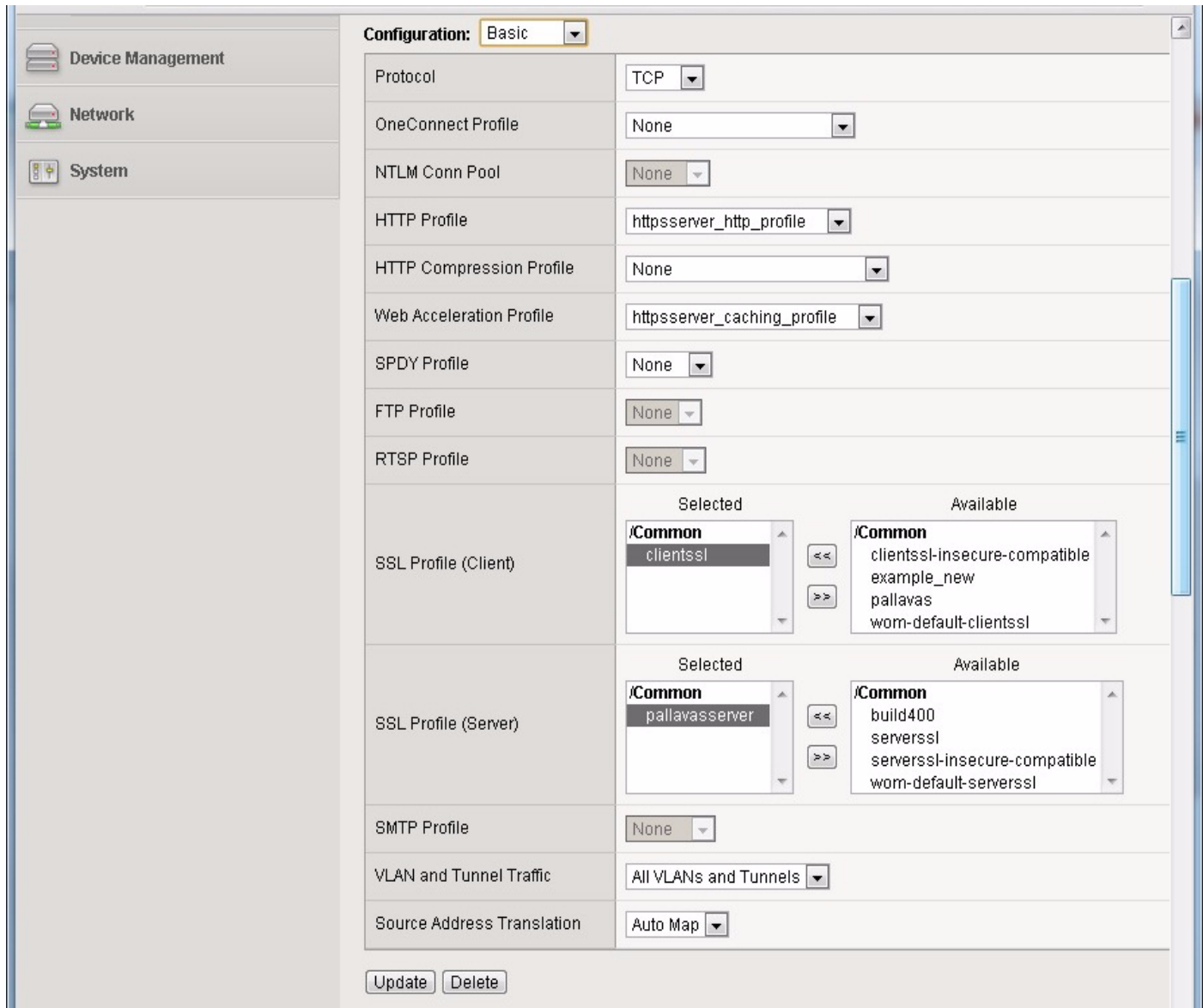
Leave all the other fields in its default values.

After you creating the HTTPS Application Service for end to end traffic , configure the virtual server by following these steps:

1. From the Local Traffic > Virtual Servers options, select the virtual server that is created.

2. Under Configuration settings, set the **Oneconnect profile** option to None.

Figure 29 F5 configuration for HTTPS Application Service - SSL Offloading



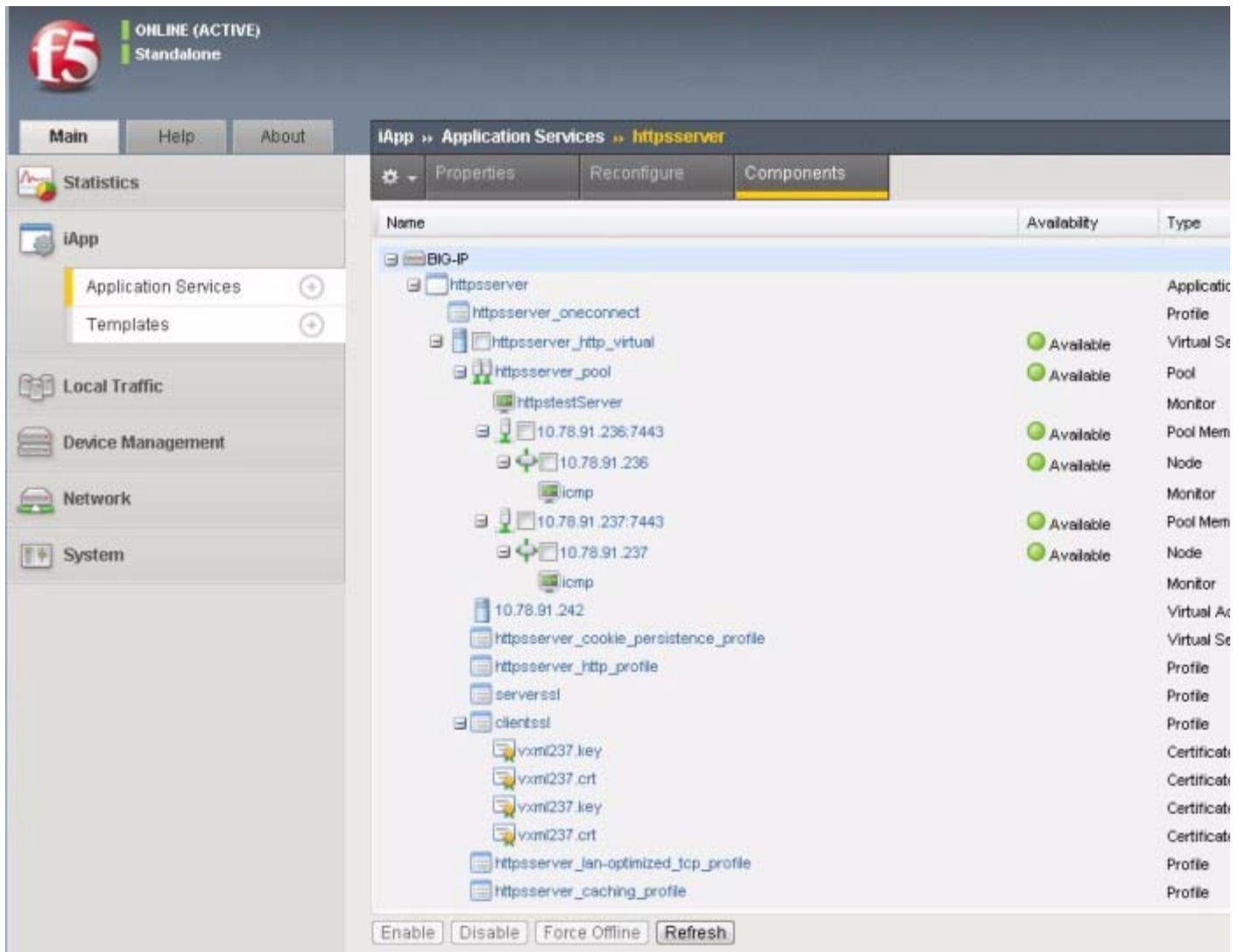
Configuration: Basic

Protocol	TCP
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	httpserver_http_profile
HTTP Compression Profile	None
Web Acceleration Profile	httpserver_caching_profile
SPDY Profile	None
FTP Profile	None
RTSP Profile	None
SSL Profile (Client)	<div> <div>Selected</div> <div> / Common clientssl </div> </div> <div> <div>Available</div> <div> / Common clientssl-insecure-compatible example_new pallavas wom-default-clientssl </div> </div>
SSL Profile (Server)	<div> <div>Selected</div> <div> / Common pallavasserver </div> </div> <div> <div>Available</div> <div> / Common build400 serverssl serverssl-insecure-compatible wom-default-serverssl </div> </div>
SMTP Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Update Delete

3. From SSL Profile (Client) option, select a client profile that is listed and click Add.
4. Click Update. The F5 configuration for HTTPS Application Service end to end traffic is completed.

Figure 30 HTTPS Application Service for end to end traffic



The screenshot displays the Cisco F5 iApp Configuration interface. The top status bar indicates the device is 'ONLINE (ACTIVE)' and in 'Standalone' mode. The left sidebar contains navigation tabs: Main, Help, and About. Below these are icons for Statistics, iApp, Local Traffic, Device Management, Network, and System. The iApp section is expanded, showing 'Application Services' and 'Templates'. The main content area is titled 'iApp » Application Services » httpsserver'. It features three sub-tabs: Properties, Reconfigure, and Components. The 'Components' tab is active, displaying a hierarchical tree of components under the 'BIG-IP' root. The components are listed in a table with columns for Name, Availability, and Type.

Name	Availability	Type
BIG-IP		
httpsserver		Application
httpsserver_oneconnect		Profile
httpsserver_http_virtual	Available	Virtual Server
httpsserver_pool	Available	Pool
httpstestServer		Monitor
10.78.91.236:7443	Available	Pool Member
10.78.91.236	Available	Node
icmp		Monitor
10.78.91.237:7443	Available	Pool Member
10.78.91.237	Available	Node
icmp		Monitor
10.78.91.242		Virtual Address
httpsserver_cookie_persistence_profile		Virtual Server
httpsserver_http_profile		Profile
serverssl		Profile
clientssl		Profile
vxm237.key		Certificate
vxm237.crt		Certificate
vxm237.key		Certificate
vxm237.crt		Certificate
httpsserver_lan-optimized_tcp_profile		Profile
httpsserver_caching_profile		Profile

At the bottom of the components list, there are four buttons: Enable, Disable, Force Offline, and Refresh.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

© 2013 Cisco Systems, Inc. All rights reserved.

CCENT, Cisco Lumin, Cisco Nexus, the Cisco logo and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCVP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Printed in the USA