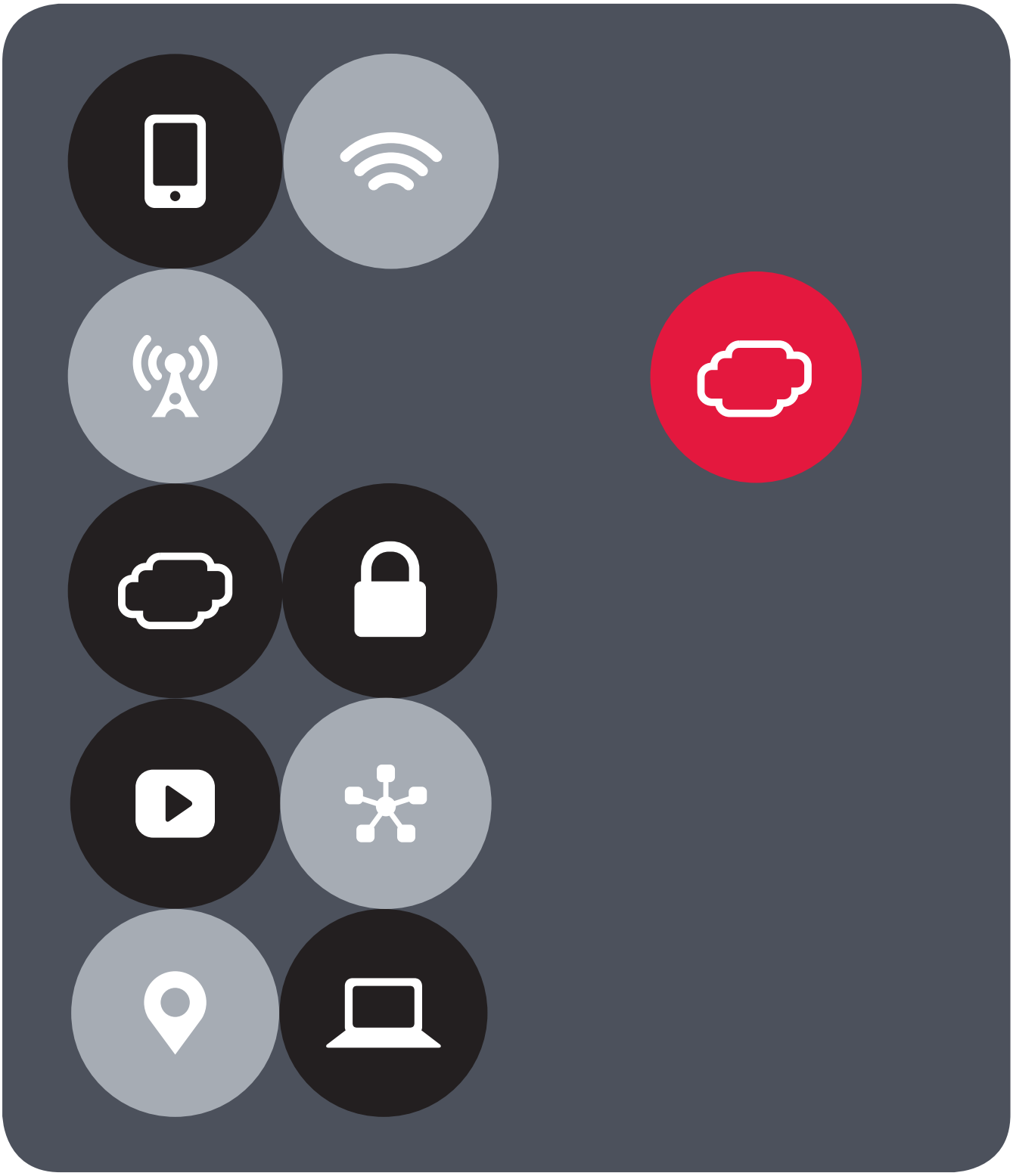
BEST PRACTICES

VMware NSX for vSphere (NSX-v) and F5 BIG-IP Best Practices Guide



Contents

Introduction

The Software-Defined Data Center (SDDC) is characterized by server virtualization, storage virtualization, and network virtualization. Server virtualization has already proved the value of SDDC architectures in reducing costs and complexity of the compute infrastructure. VMware NSX network virtualization provides the third critical pillar of the SDDC. It extends the same benefits to the data center network to accelerate network service provisioning, simplify network operations, and improve network economics.

By deploying F5 BIG-IP and NSX together, organizations are able to achieve service provisioning automation and agility enabled by the SDDC. This is combined with the richness of the F5 application delivery services they have come to expect.

This guide provides configuration guidance and best practices for the topologies articulated in the *NSX F5 Design Guide* to optimize interoperability between the NSX platform and F5 BIG-IP physical and virtual appliances. It is designed to validate and complement the scenarios described in the *NSX F5 Design Guide* and is intended for customers who would like to adopt the SDDC while ensuring compatibility and minimal disruption to their existing BIG-IP environment.

Topology 1: Parallel to NSX Edge Using VXLAN Overlays with BIG-IP Physical Appliances

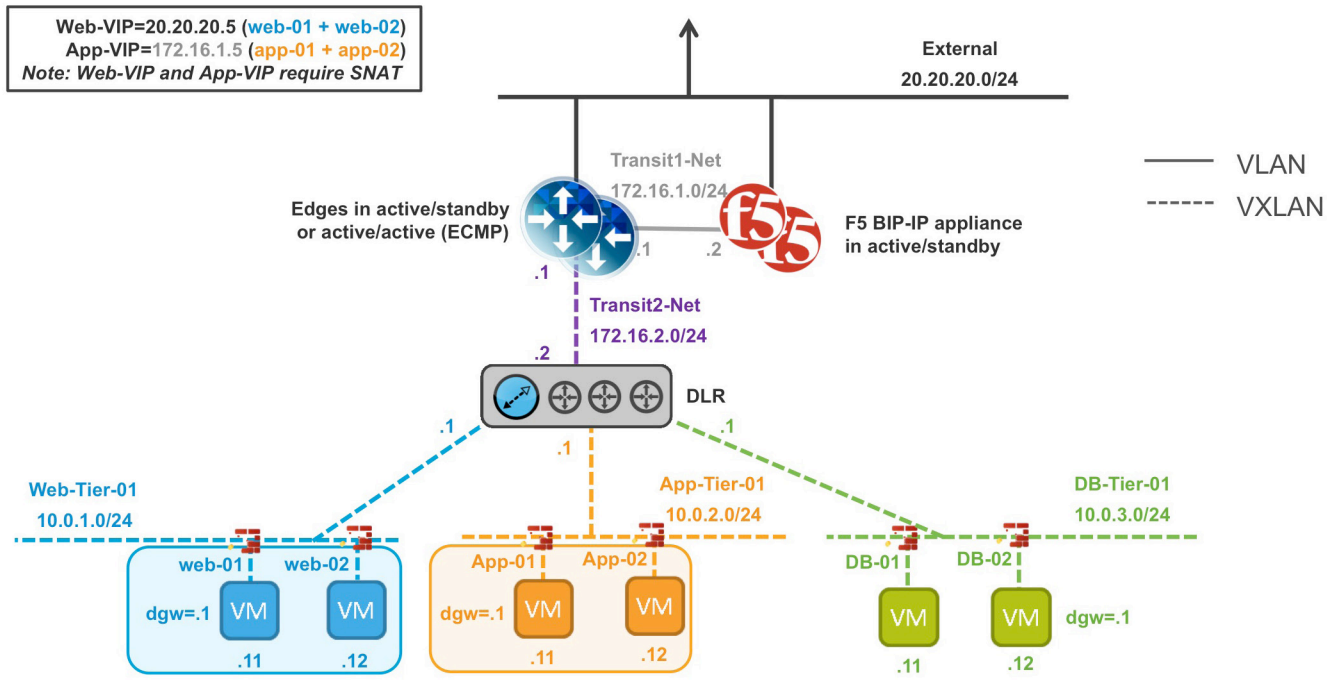


Figure 1. BIG-IP appliance parallel to NSX Edge Services Gateway

The first deployment scenario utilizes a topology that creates a second data path for application delivery traffic with BIG-IP appliances arranged logically adjacent to the NSX Edge Services Gateway. This allows application specific optimizations and load balancing decisions to take place before traversing the overlay network. It is also a key enforcement point for application specific security policies to be built, from layer 4 through layer 7, outside the flow and policy enforcement for traditional east-west traffic. This design also provides a range of isolated private address space in the transit segment to be used for application VIPs and SNATs for inter-tier load balancing.

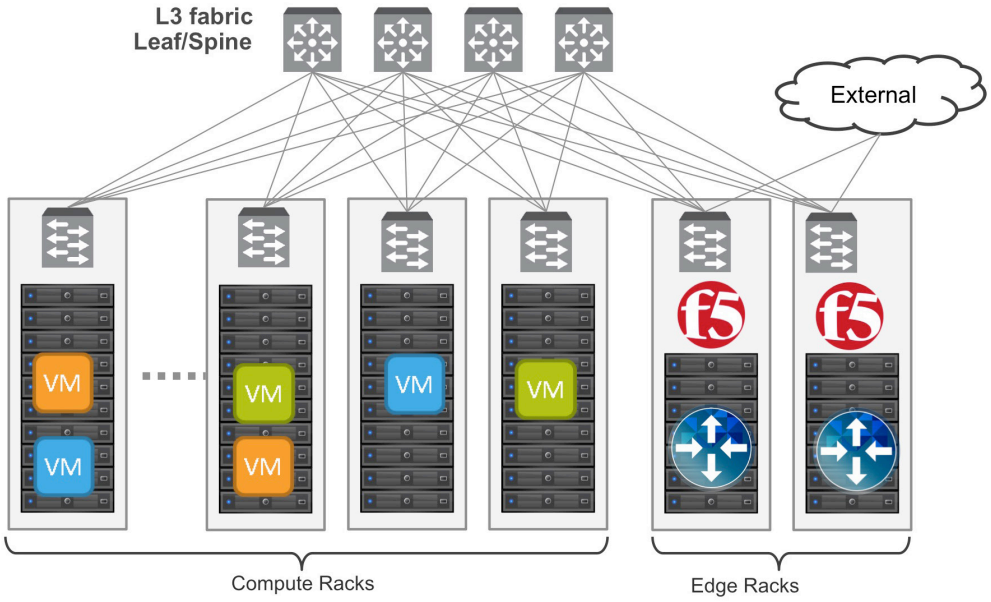


Figure 2. Leaf/spine physical rack infrastructure

This topology is popular on standard layer 3 physical fabrics as seen in a leaf/spine topology but is equally applicable to a flat layer 2 infrastructure. The physical placement of the BIG-IP appliances should be in the same infrastructure racks as those reserved for the NSX Edge Services Gateway deployments.

Implementation Infrastructure

In the validation environment, several ESXi clusters are in use. Some of the clusters are NSX-enabled clusters and some are not.

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 3: the USSJ-55-Management Cluster and the USSJ-55-Computer Cluster. While this is a smaller representation of a typical data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 2.

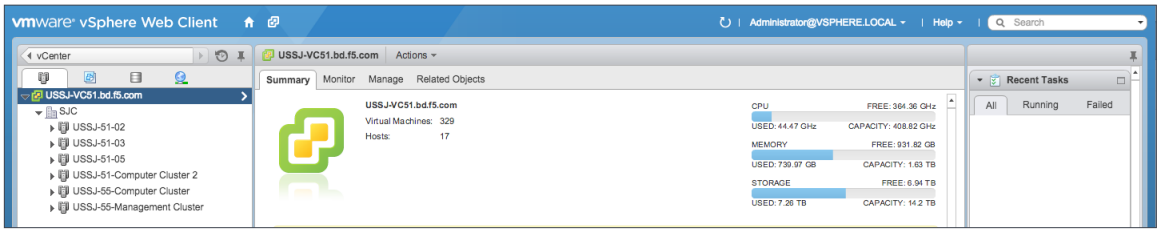


Figure 3. vSphere console

In accordance with best practices, edge and compute ESXi hosts are physically and logically separated from one another. Physical F5 devices are installed in dedicated edge racks, along with vCenter, NSX manager, and the NSX Edge Services Gateways, which also will be installed in the management racks.

The virtual machines used as Web (Web), Application (App), and Database (DB) servers will be running on ESXi hosts in the compute cluster. To better understand data traffic flows for this deployment scenario topology, examine the *VMWare NSX for vSphere (NSX-V) and BIG-IP Design Guide*.

Prerequisites

Referencing the diagram in Figure 1, the BIG-IP appliance requires connectivity for two physical interfaces. One interface is used for management of the device and the other is used for all production traffic. The VLAN numbers, the VXLAN segment IDs and the IP addressing scheme can be tailored to your environment.

- The physical BIG-IP appliances will need to be installed and connected to the edge rack top-of-rack switches. Each BIG-IP appliance's management interface will need to be connected to a switchport on a top-of-rack management switch and configured with an IP address in the management segment.
- For this environment, a BIG-IP interface 1.1 will need to be connected to a switchport on the edge rack top-of-rack switch that 802.1Q tags the VLANs used in this environment. In the example, VLANs 20 and 159 are used.
- Physical network infrastructure switches connected to the ESXi servers and BIG-IP appliance are configured to support 802.1Q tagging and allow the appropriate VLANs.
- ESXi hosts will need to be configured with the appropriate distributed port groups and virtual switches.

Name	802.1Q VLAN ID
External	20
dvs_VL155_NSXIPPool	155
TransitNet-1	159

Table 1. VLAN tags for configuration on distributed virtual switch and physical switches

Name	Transport Zone	Segment ID	Control Plane Mode
App-Tier-01	TransportZone1	7001	Unicast
DB-Tier-01	TransportZone1	7002	Unicast
TransitNet-2	TransportZone1	7003	Unicast
Web-Tier-01	TransportZone1	7000	Unicast

Table 2. Logical switch configuration

Network Segments

Two types of network segments are utilized in this topology: traditional 802.1Q VLAN network segments and VXLAN overlay segments. Within NSX, we created IP Pools that will be used by the Web, App, and DB virtual machines.

802.1Q VLAN segments

VLAN 20 External is the VLAN used for external connectivity. The 20.20.20.0/24 IP subnet range is configured on this VLAN.

VLAN 155 dvs_VL155_NSXIPPool (not shown) is for management connectivity. The 10.105.155.0/24 IP subnet range is configured on this VLAN

VLAN 159 TransitNet-1 is the VLAN used as the transit VLAN between the BIG-IP appliance and the NSX Edge for application traffic. The 172.16.1.0/24 IP subnet range is configured on this VLAN.

VXLAN Segments

The Web, App, and DB tier virtual machines are all provisioned and connected to VXLANs.

VXLAN 7000 Web-Tier-01 is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.

VXLAN 7001 App-Tier-01 is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.

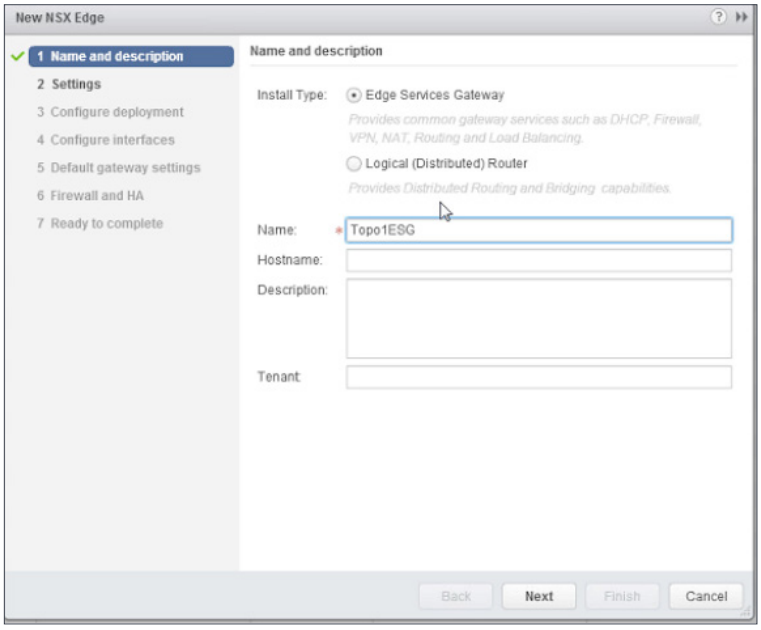
VXLAN 7002 DB-Tier-01 is the segment ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VXLAN.

VXLAN 7003 TransitNet-2 is the VXLAN segment ID used for the transport zone between the DLR and the NSX Edge.

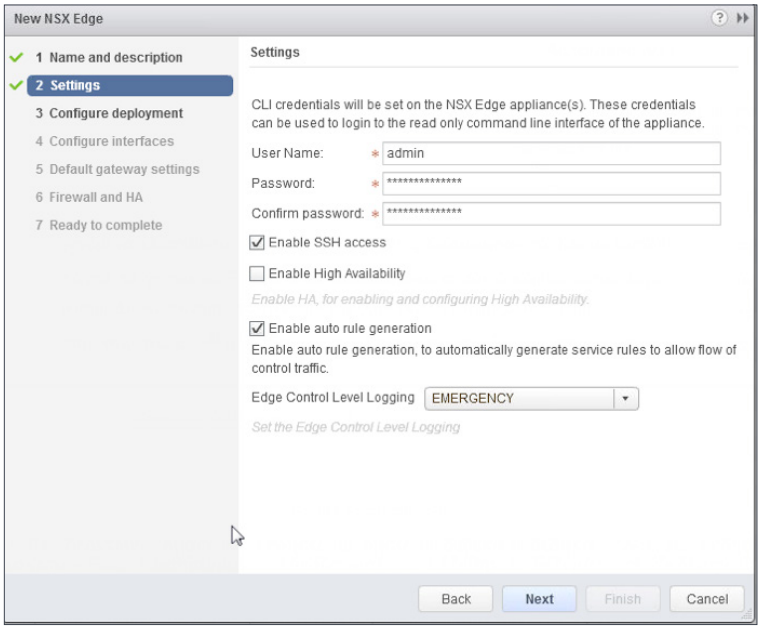
NSX Edge Configuration

1. In the vSphere Web Client console, begin by navigating to **Networking & Security** in the left column. Under Networking and Security, choose **NSX Edges** and then click the green plus symbol (+).

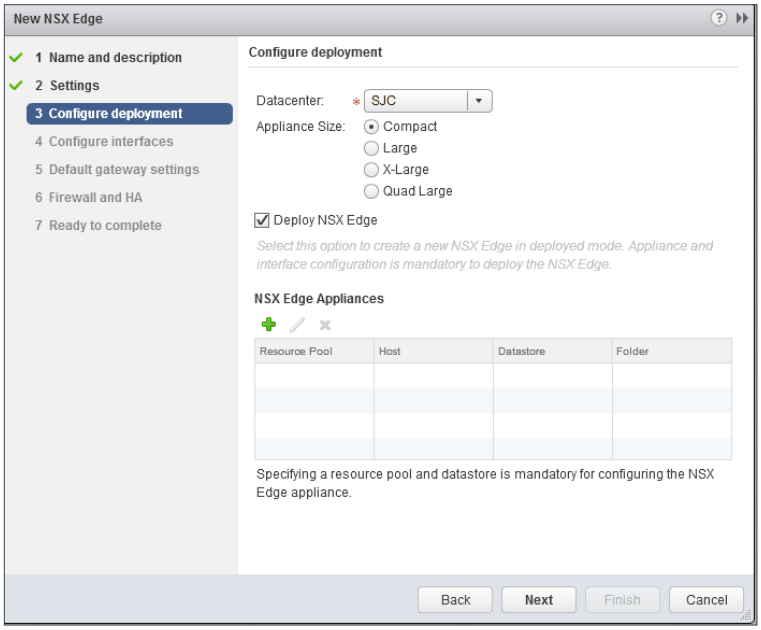
2. Select Edge Services Gateway as the Install Type and provide a name for the device, then click **Next**.



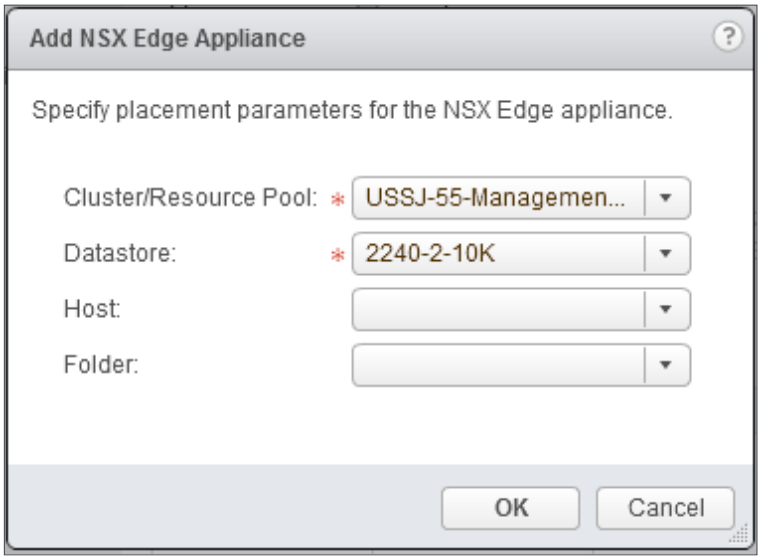
3. Under **Settings**, select **Enable SSH access** and provide a username and password for the Edge Services Gateway. Click **Next**.



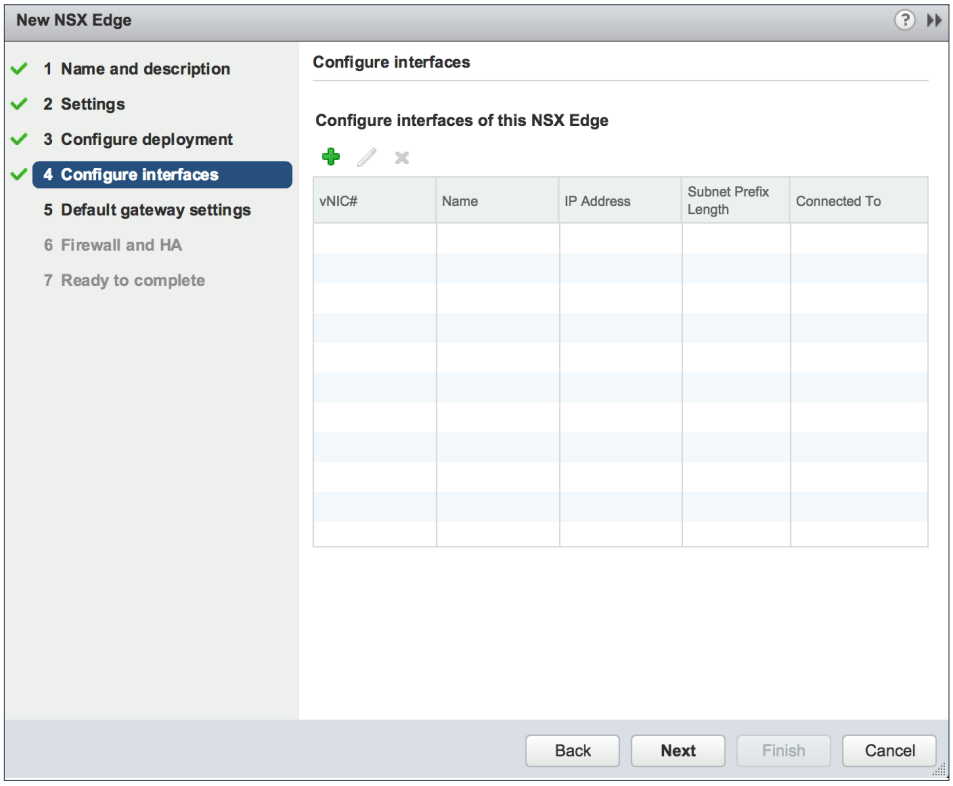
4. Under **Configure deployment**, select the **Datacenter** and **Appliance Size** appropriate for your deployment, and check the **Deploy NSX Edge** checkbox. Then click on the green plus symbol (+) under NSX Edge Appliances.



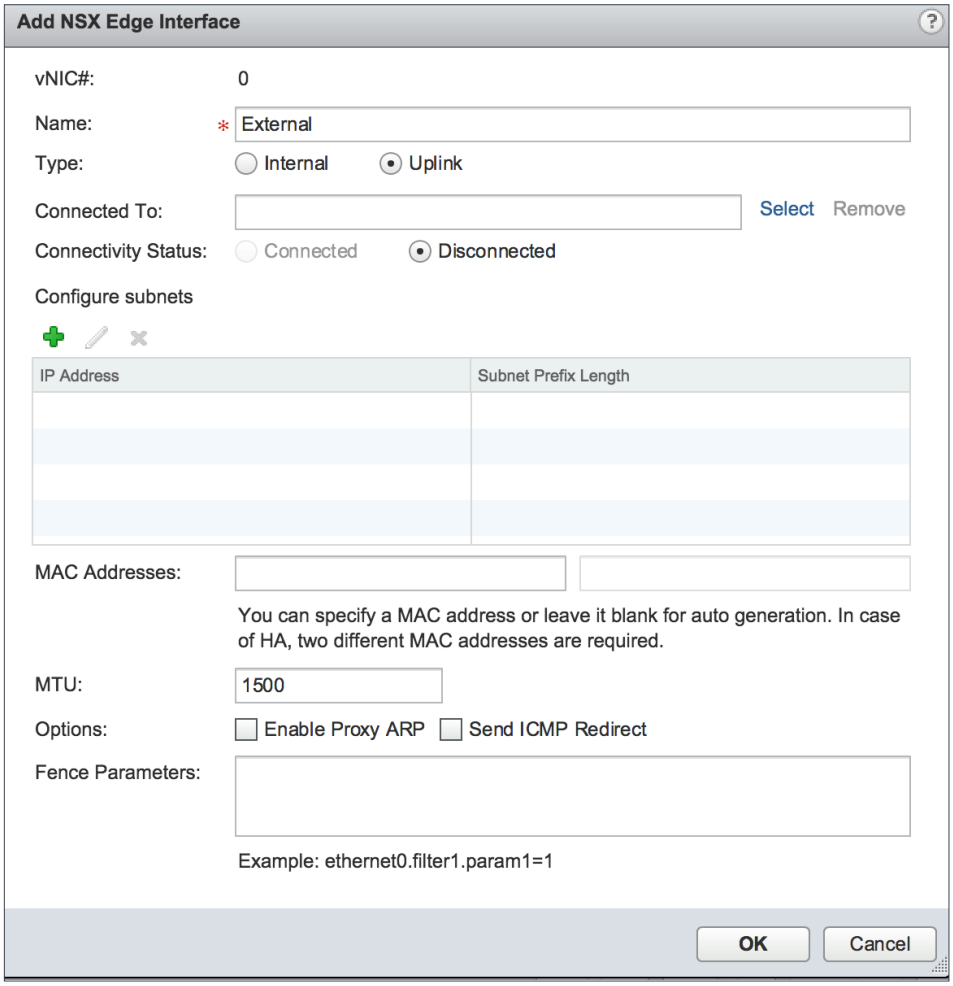
5. Selecting the green plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and Datastore (for this example, the USSJ-55-Management Cluster and the 2240-2-10K datastore). The host selection is optional. Click OK to complete. This will return you to the configure deployment screen shown in step 4. Click Next to continue.



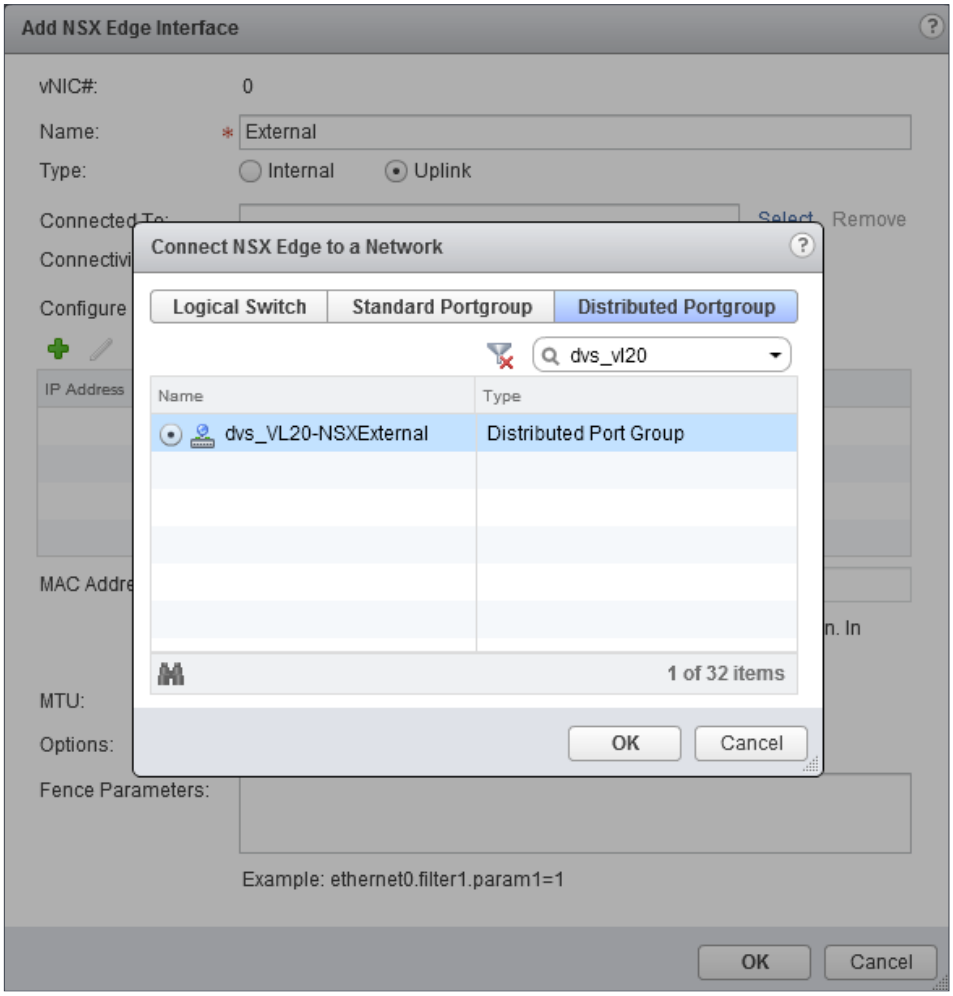
6. In the Configure interfaces dialog box, select the green plus symbol to display the Add NSX Edge Interface dialog box.



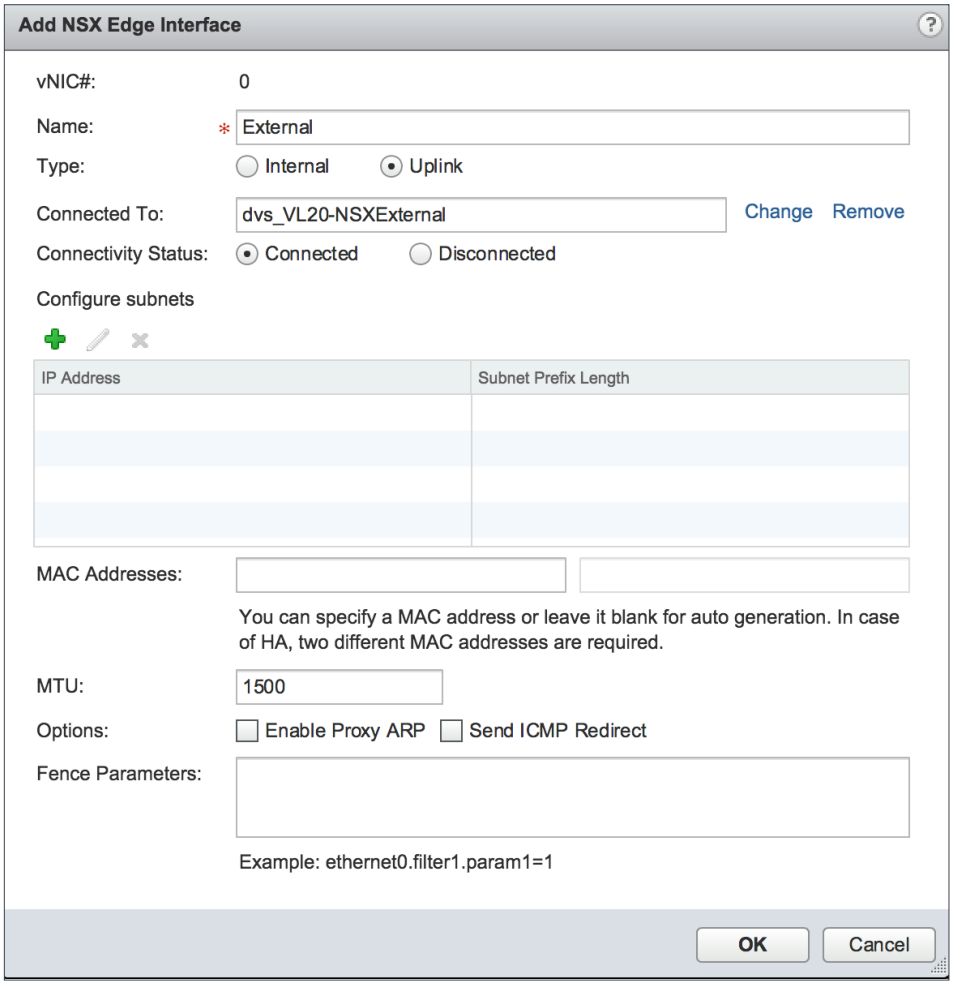
7. Provide a name and click **Select** next to the **Connected To** field.



8. For the External network, click on the **Distributed Portgroup** tab and then selecting the Portgroup used for external access. Click **OK**.



9. Once the network is chosen, select the green plus symbol (+) under **Configure subnets** to add the appropriate IP address and subnet configuration to the interface.



10. In the **Add Subnet** dialog box, enter the appropriate **IP address** and **Subnet prefix length**, and click OK.

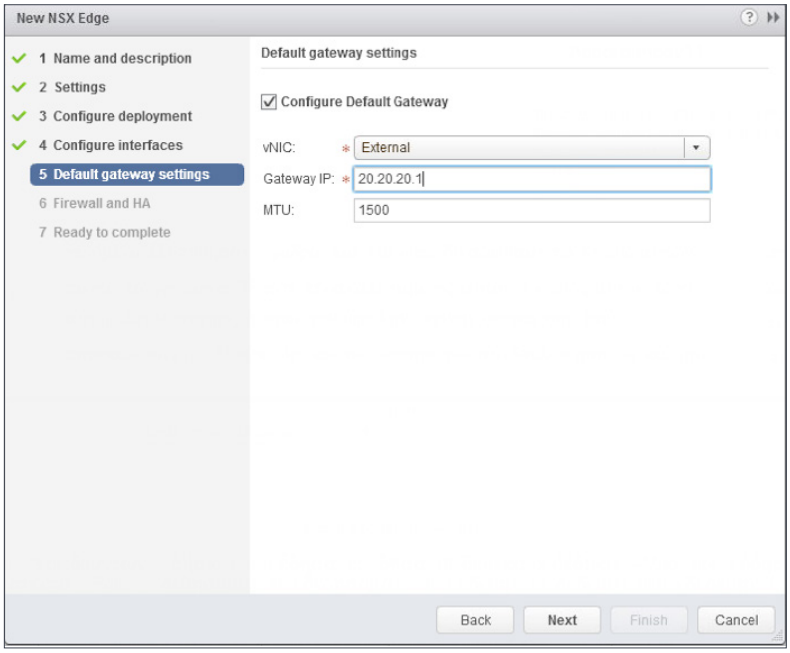
11. This will bring you back to the **Configure interfaces** dialog box. For each of the three interfaces required for this deployment scenario, configure the appropriate subnets and switch type, according to the table below.

Network Name	Type	Network	Interface IP /Subnet Prefix
External	Uplink	Distributed Port Group	20.20.20.2/24
TransitNet-1	Uplink	Distributed Port Group	17.16.1.1/24
TransitNet-2	Internal	Logical Switch	172.16.2.1/24

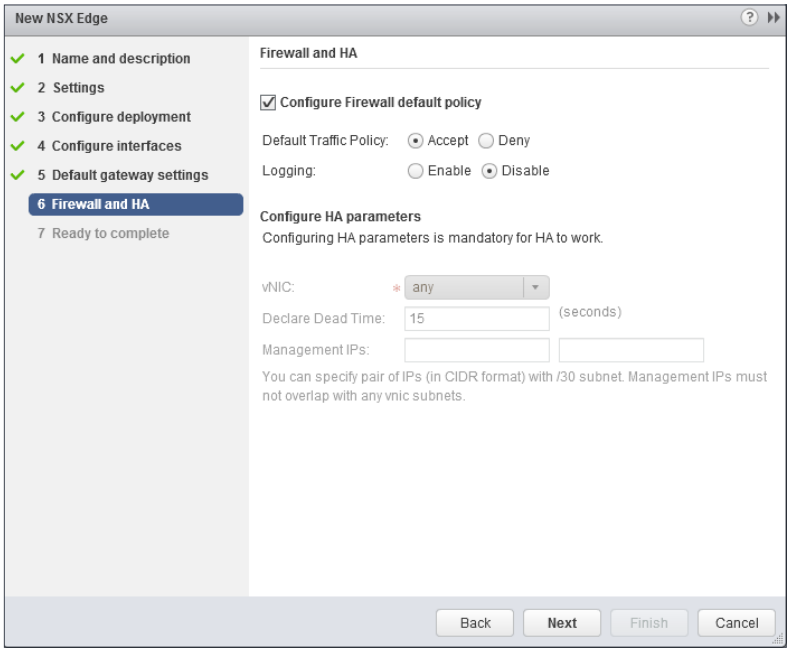
Table 3. NSX Edge network interfaces

12. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway is our data center backbone router with the IP address of 20.20.20.1 on External vNIC that we configured under the interface settings.

    Use the default MTU parameter unless the network is using an MTU of a different size, such as jumbo frames. (Configuring a non-standard MTU that is inconsistent can lead to unnecessary fragmentation of packets or black-holing of some traffic.) Click **Next** to continue.



13. HA settings can be left as default. Check **Configure firewall default policy** and check **Accept** for the **Default Traffic Policy.**



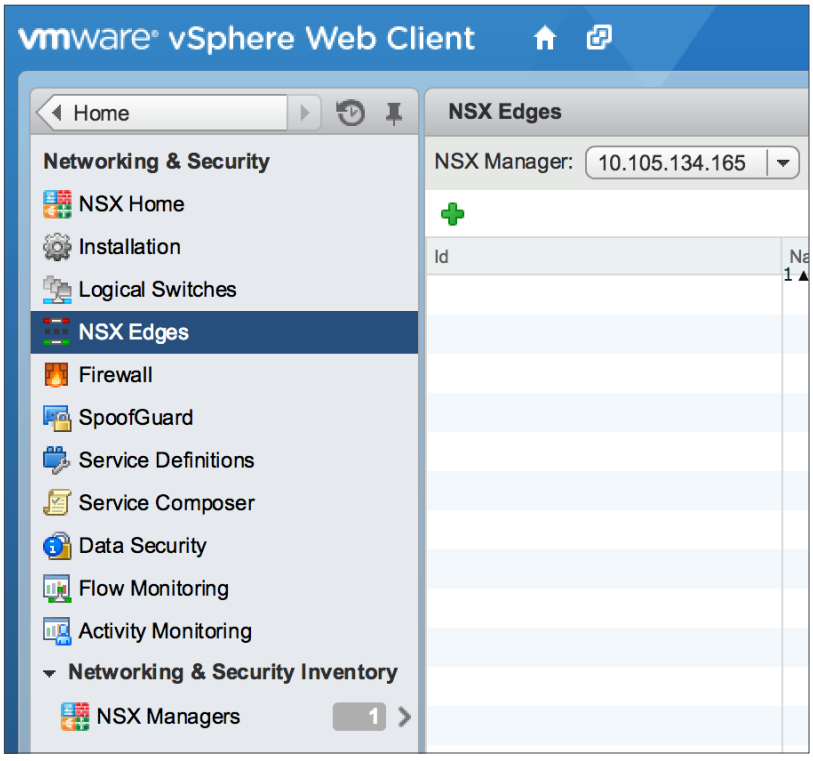
14. Select **Finish** to complete the deployment of the NSX Edge.

Create and Deploy DLR

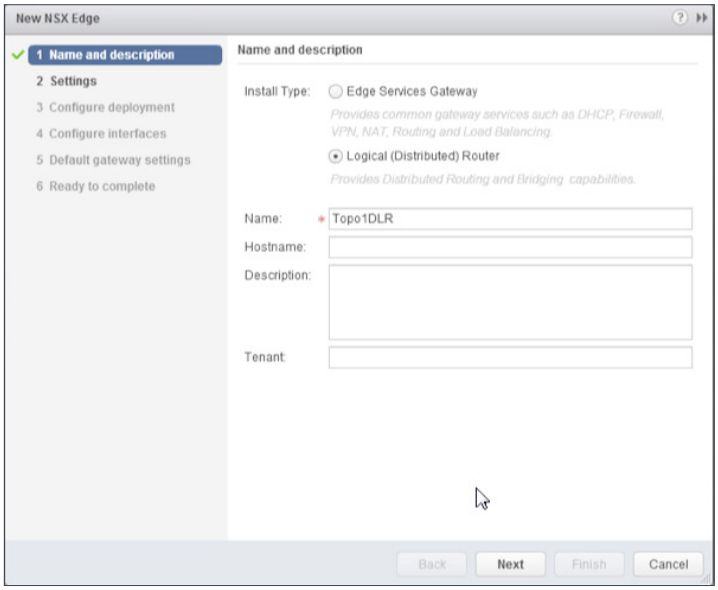
Within VMWare NSX, the Distributed Logical Router (DLR) provides an optimized way of handling east-west traffic within the data center. East-west traffic consists of communication between virtual machines or other resources on different subnets within a data center. As east-west traffic demand increases within the data center, the distributed architecture allows for optimized routing between VXLAN segments.

(Note that DLR and LDR—Logical (Distributed) Router—are used synonymously by VMware.)

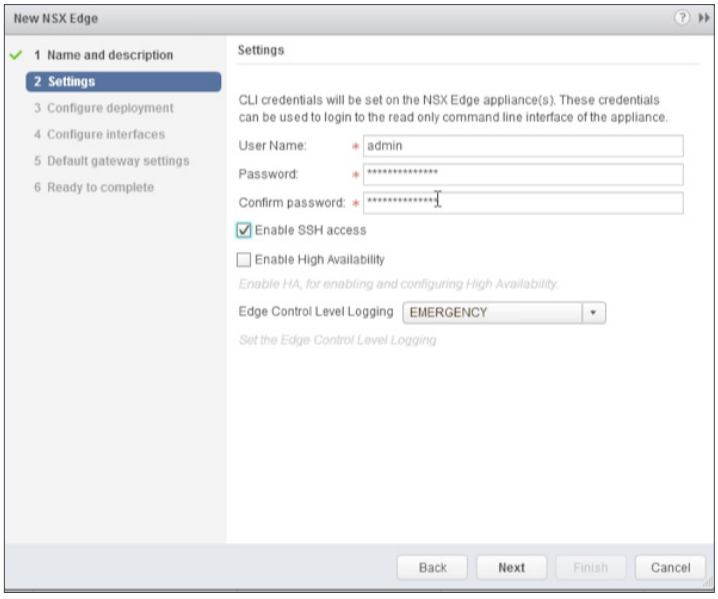
1. Return to the **vSphere Web Client** console and choose **Networking & Security** in the left column. Under **Networking and Security**, choose **NSX Edges** and then click the green plus symbol (+).



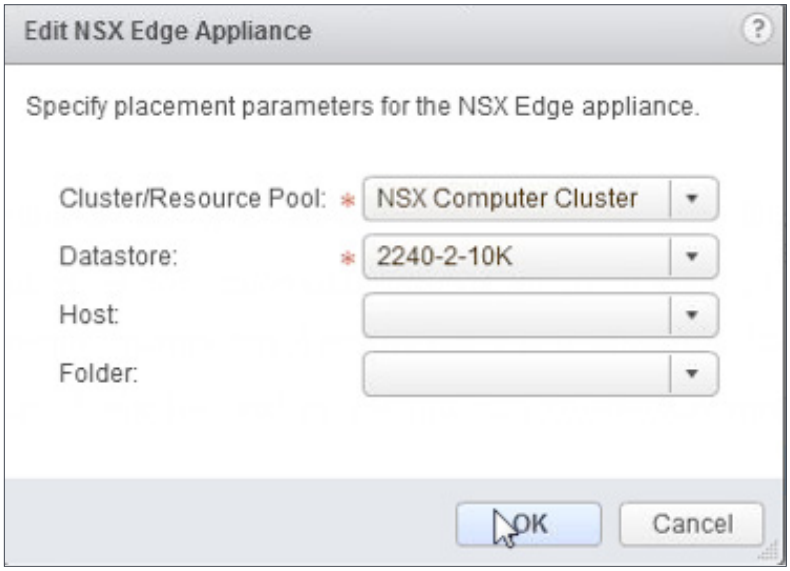
2. Select **Logical (Distributed) Router** as the **Install Type** and provide a name for the device, then click **Next**.



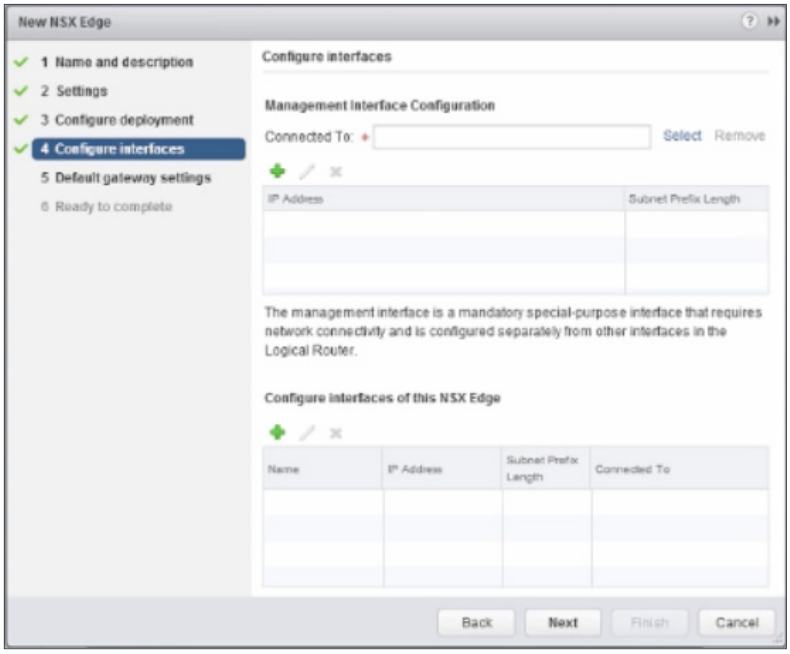
3. Under **Settings**, check **Enable SSH access** and provide a username and password for the Edge Services Gateway. Select **Next**.



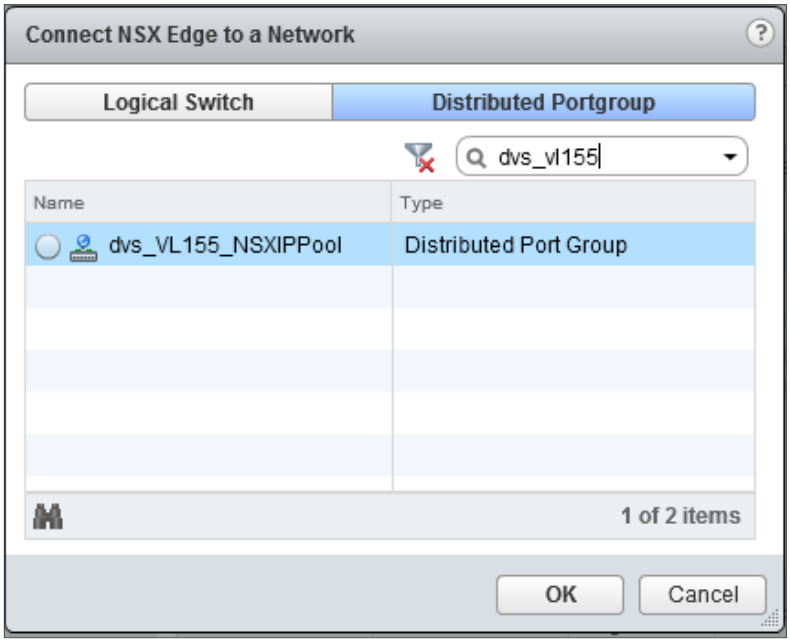
4. Selecting the green plus symbol (+) in the Configure Deployment section will display the options in the figure below. Choose the appropriate Cluster/resource pool and Datastore (for this example, the **NSX Computer Cluster** and the **2240-2-10K** datastore). The **Host** is optional. Click **OK** to complete and **Next** to continue. This will return you to the screen shown in step 2.



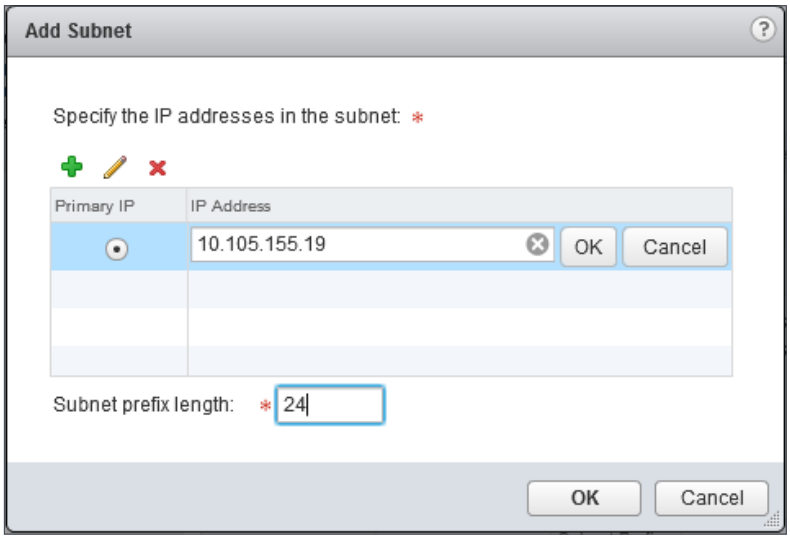
5. Select **Configure Interfaces**, and then click **Select** to the right of the **Connected To** text box.



   a. In this case, the management interface should be connected to a distributed port group that is connected to the shared management VLAN.



b. Click the green plus symbol (+) to specify a fixed **IP address** and **Subnet prefix length** in the management network. Click **OK** to complete.

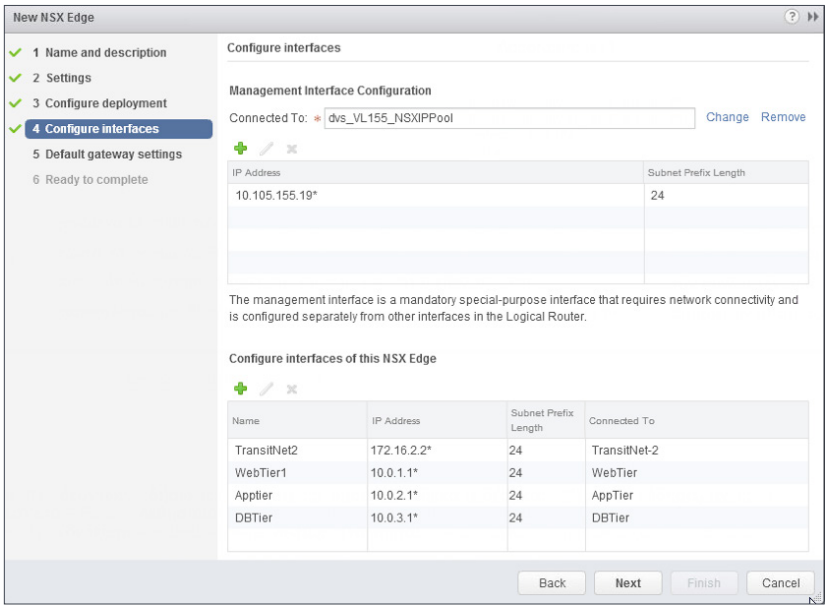


6. For each of the four interfaces required for this topology, configure the appropriate subnets and switch type according to the table below. Select the green plus symbol (+) under Configure Interfaces of this NSX Edge to bring up the Add Interface dialog box.

Network Name	Connected To	Type	Network	Interface IP/Subnet Prefix
TransitNet2	TransitNet-2	Uplink	Logical Switch	172.16.2.2/24
WebTier	WebTier	Internal	Logical Switch	10.0.1.1/24
AppTier	AppTier	Internal	Logical Switch	10.0.2.1/24
DBTier	DBTier	Internal	Logical Switch	10.0.3.1/24

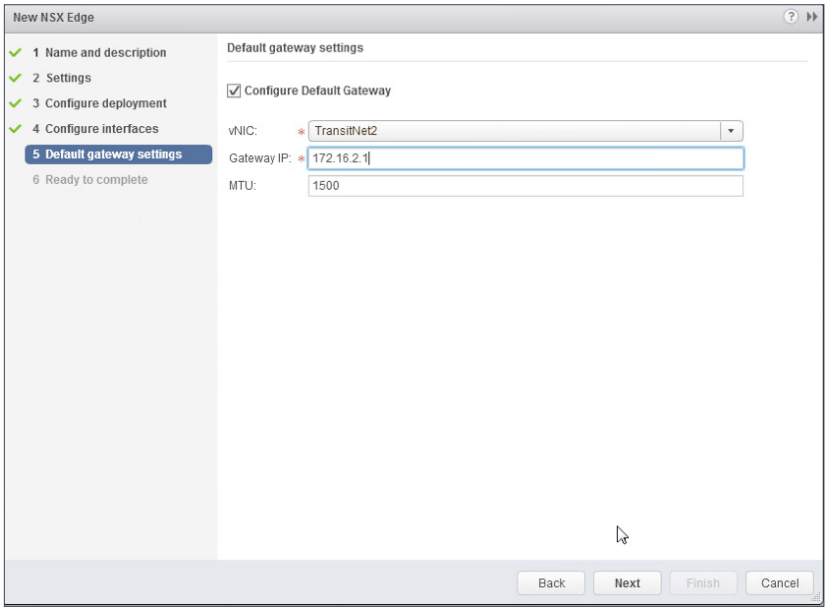
Table 4. NSX distributed logical router network interfaces

The DLR interface configuration, once completed, should resemble the dialog box below. Click **Next** to continue.

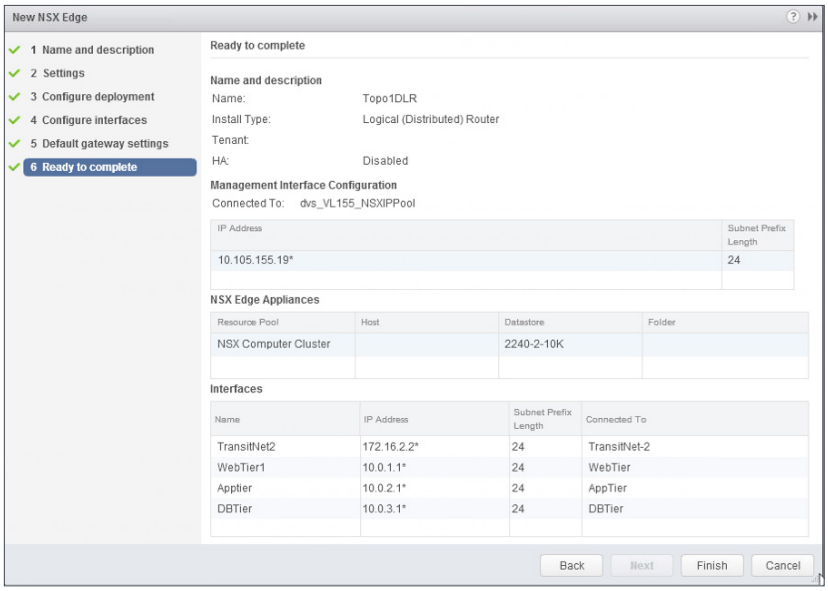


7. With the interface settings complete, the next step is to configure the default gateway settings. The default gateway for the DLR is the data center core router that we configured in the previous section across the transit segment TransitNet2.

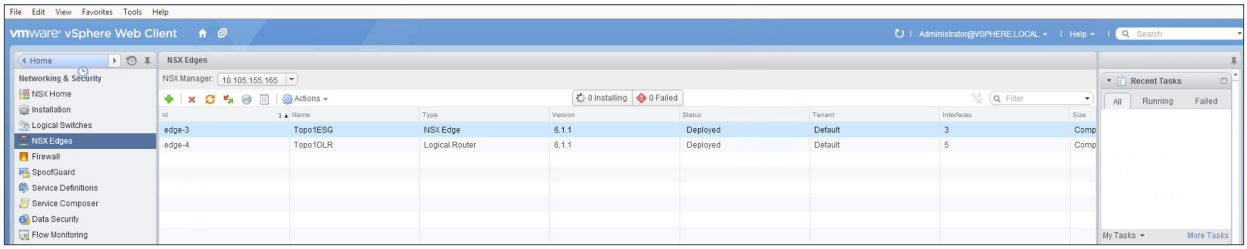
   For the **vNIC**, select **TransitNet2** and provide the **Gateway IP** address of the NSX Edge. In this example, it is **172.16.2.1**. Click Next to proceed.



8. Click **Ready to complete** to review your configuration and then click **Finish** to deploy the DLR. Depending on the number of ESXi hosts, it may take some time for the DLR deployment to complete.



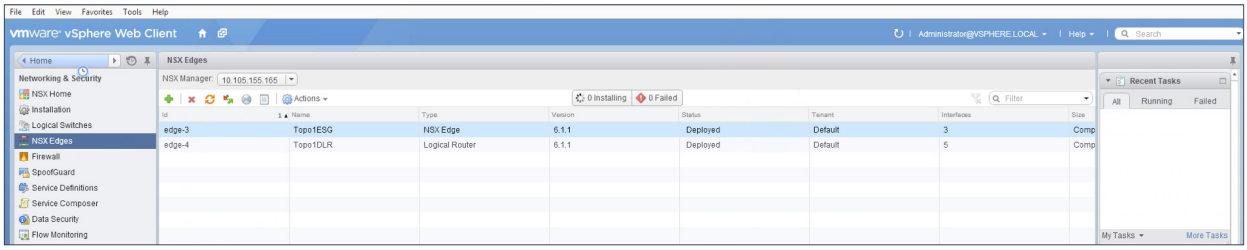
9. Once complete, the vSphere NSX Edges configuration should resemble the image below.



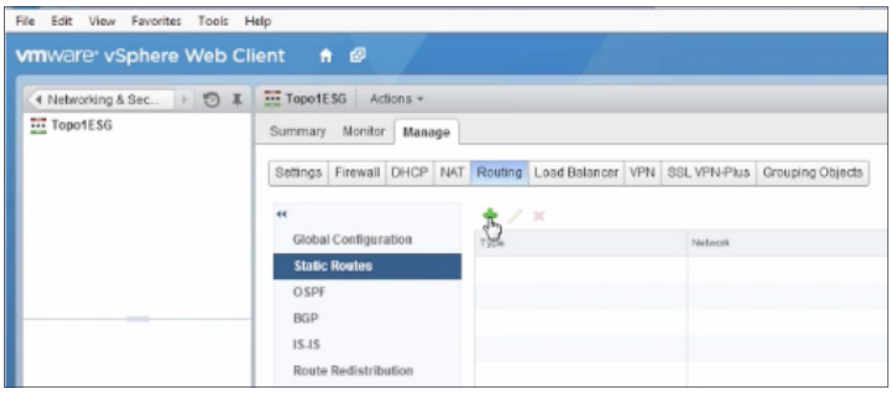
NSX Edge Static Routing Configuration

For this deployment scenario, static routing is configured to allow the NSX Edge to forward packets into the different tiered networks via the DLR. The default gateway configuration on both the NSX Edge and the DLR ensures packets find their way out to external networks. This configuration is also required to ensure that traffic coming from the external networks finds its way in.

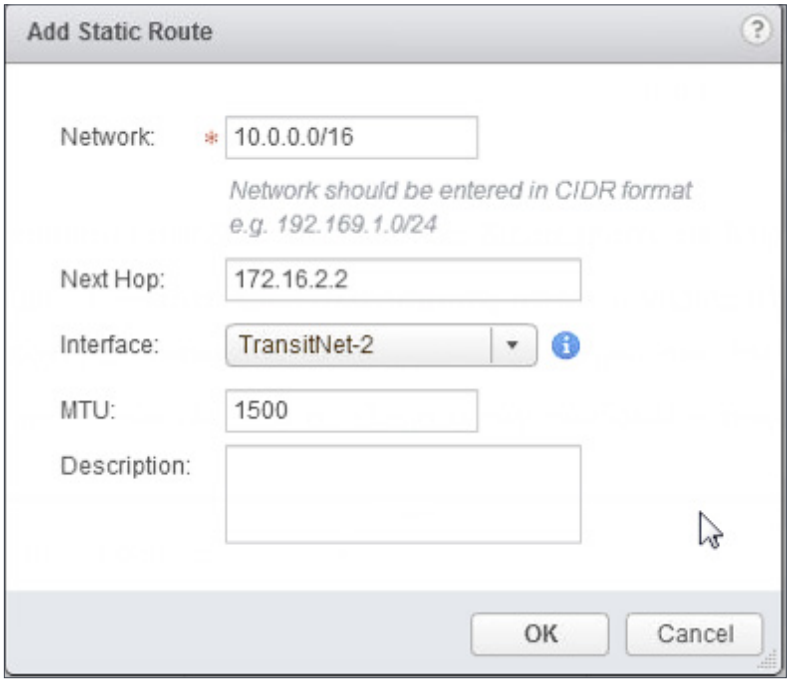
1. Double-click on the NSX Edge you configured in the first section.



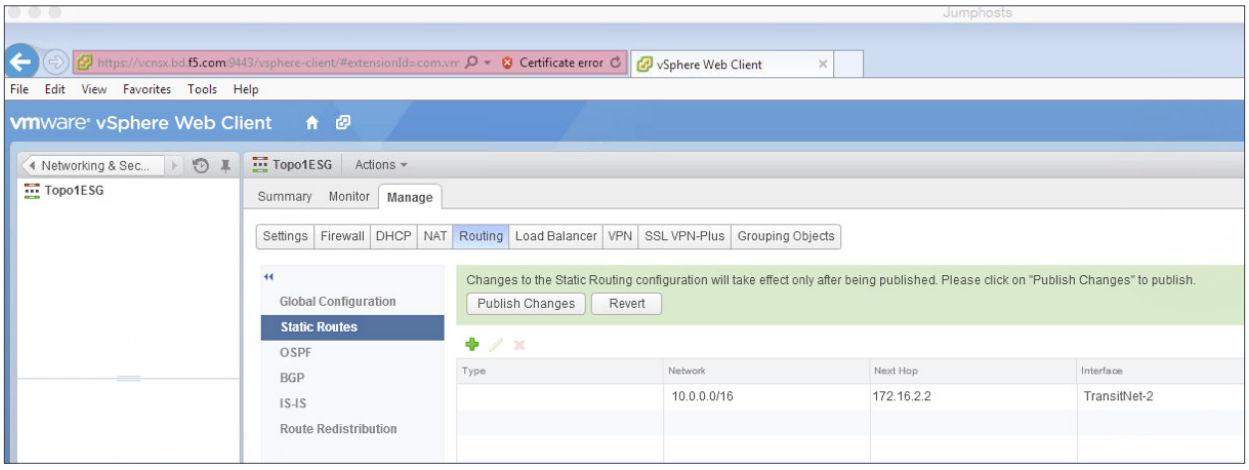
2. The configuration screen below should now be displayed. Click on the **Manage** tab and then select the **Routing** sub-tab. In the left-hand column, click **Static Routes**, and then click the green plus symbol (+) to bring up the **Add Static Route** configuration dialog box.



1. Provide an internal summary route that points the NSX Edge to the TransitNet-2 IP Address of the DLR interface. In this case, a summary of **10.0.0.0/16** is pointed internally to the DLR IP address of **172.16.2.2**. Click OK.



2. Click **Publish Changes** to push the updated routing information to the NSX Edge.



BIG-IP Appliance Configuration

The validation of this topology is currently configured on a single device. The base network configuration consists of configuring the VLANs and assigning them to an interface as well as creating the appropriate self IP addresses for each of the network segments. For production deployments, F5 recommends that two BIG-IP devices be configured in an HA configuration.

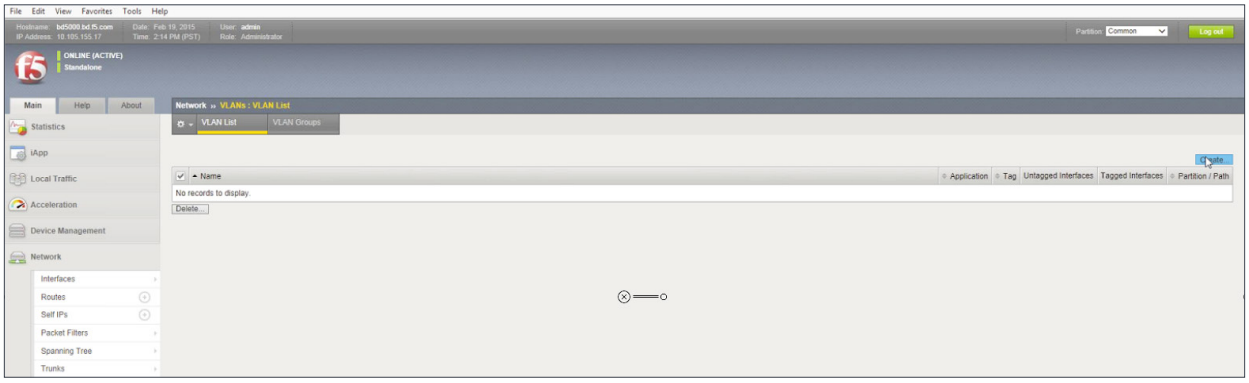
Prerequisites

- The BIG-IP appliance is configured with a management IP address in the proper subnet.
- Licenses have been applied and activated.
- Appropriate provisioning of resources is complete.
- Base configuration of services DNS, NTP, SYSLOG are configured.
- BIG-IP Interface 1.1 is physically wired to a switch configured to support 802.1Q tagging of traffic on VLANs 20 and 159.

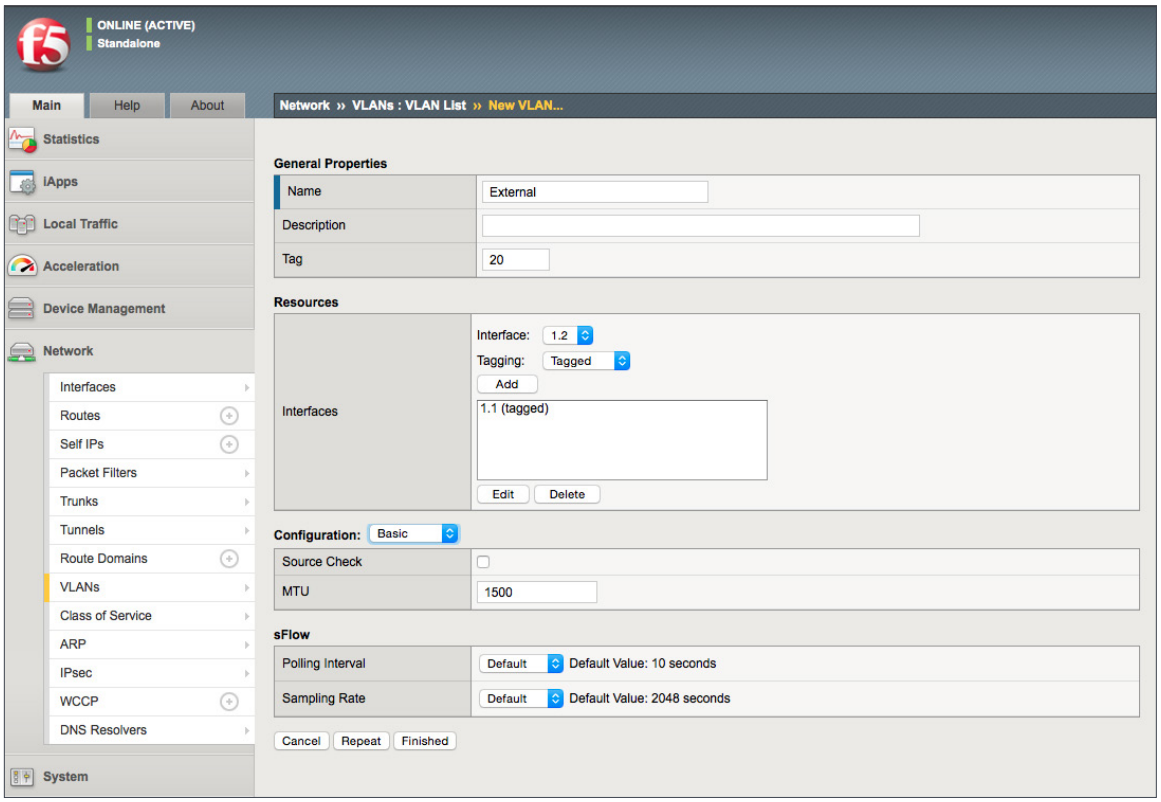
For info on how to perform these installation and basic setup steps, refer to http://support.f5.com and consult the appropriate implementation guide for your version and device.

Create VLANs

1. From the Main tab of the **BIG-IP Configuration Utility** navigation pane, expand **Network** and select **VLANs**.
2. In the upper right corner, click **Create**.



3. Under **General Properties**, enter a unique name for the VLAN. In this example, we used **External**.
4. In the **Tag** field, enter the External VLAN ID of **20**.
5. Under Resources, for **Interface**, select 1.1.
6. Select **Tagged** and then click the **Add** button below it.

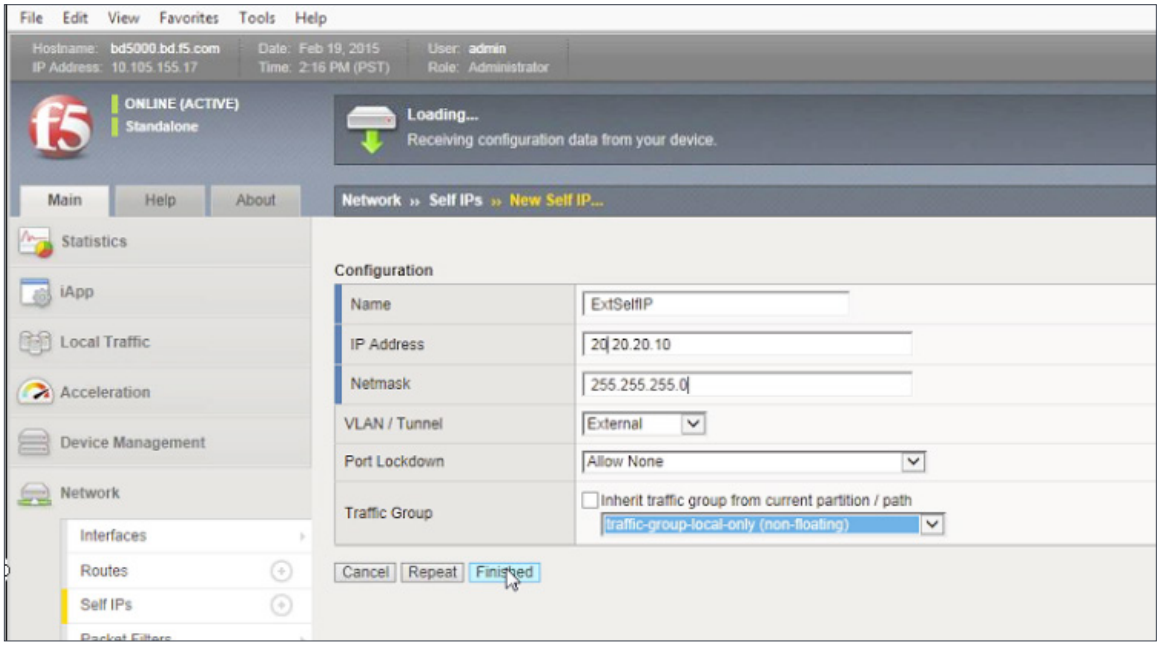


7. Select **Repeat** to proceed with creating the transit network.
8. Under **General Properties**, enter a unique name for the VLAN. In this example, we used **TransitNet1**.
9. For the **Tag**, enter the TransitNet-1 VLAN ID of **159**.
10. Under **Resources**, select the **Interface 1.1**.
11. Select **Tagged** and click the **Add** button below it.
12. Select **Finished** to complete the VLAN creation.

Configure Self IP Addresses

Self IP addresses are logical interfaces that allow the BIG-IP to participate in the networks for which they are configured. They also are useful for functions such as SNAT to ensure symmetric traffic patterns.

1. On the **Main** tab of the BIG-IP navigation pane, click **Network** and then click **Self IPs**.
2. In the upper right corner of the screen, click the **Create** button.
3. Type a unique name in the Name box. In this example, we used **Extself IP**.
4. In the IP address box, type the IP address you want to assign to a VLAN. For the External network, use **20.20.20.10**.
5. Provide the appropriate subnet mask in the Netmask box. In this example, we used **255.255.255.0**.
6. For the VLAN/Tunnel, select **External** from the dropdown box.
7. Use the default settings for Port Lockdown and Traffic Group.
8. Click the **Repeat** button to continue.



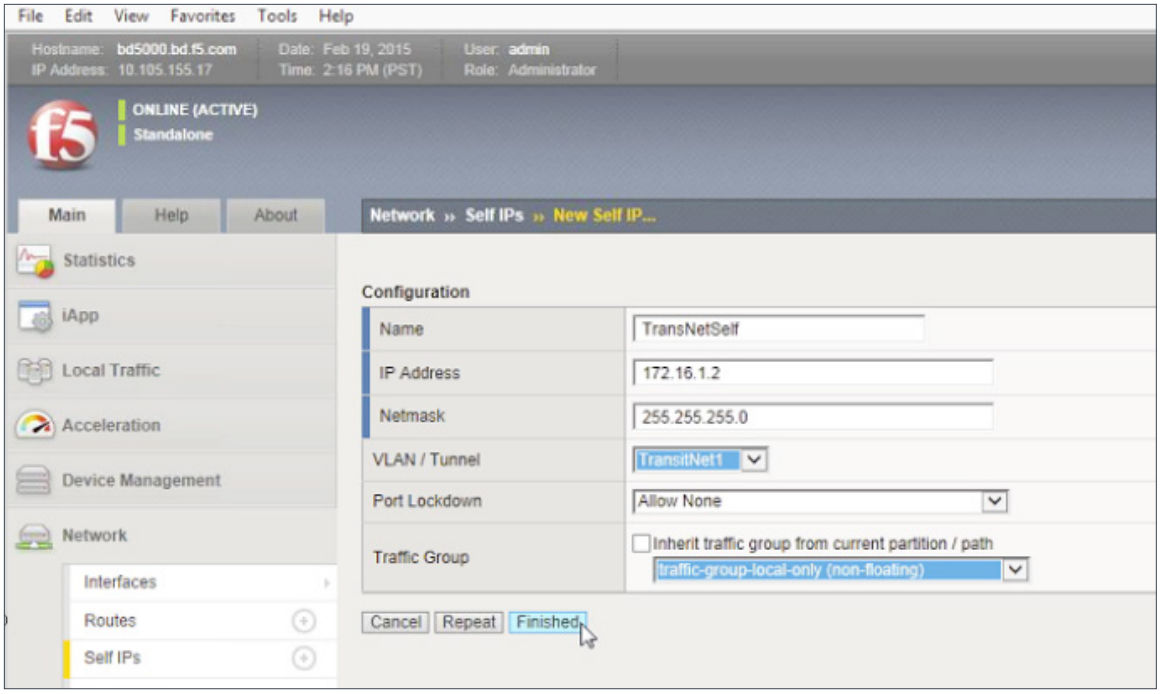
9. Complete the configuration for the **TransitNetSelf** self IP using the following settings:

   a. Name: **TransitNetSelf**

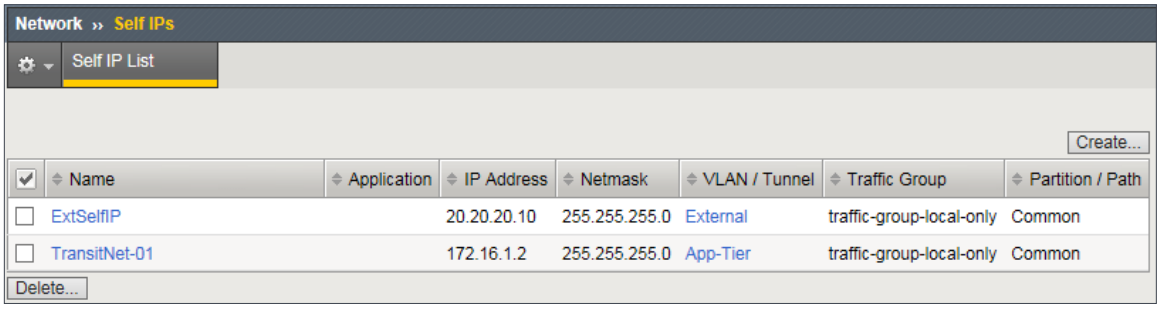
   b. IP Address: **172.16.1.2**

   c. Netmask: **255.255.255.0**

   d. VLAN/Tunnel: **TransitNet1**



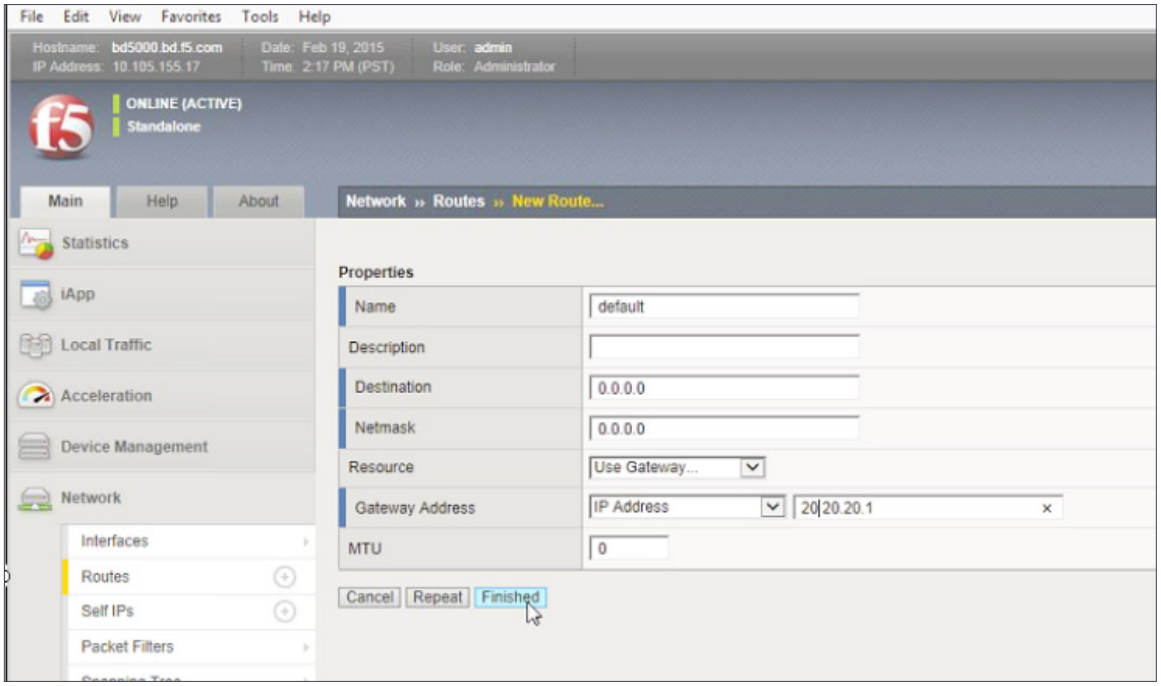
10. Click **Finished** to validate the completed self IP configuration.



Configure Static Routes

To ensure the BIG-IP can properly forward requests to the application servers within the overlay network and also communicate with all external networks, static routing is used to provide two discreet paths for traffic. The External VLAN will be used for web tier application traffic VIPs; TransitNet-1 will be used for application tier VIPs as well as the source IP for SNAT traffic.

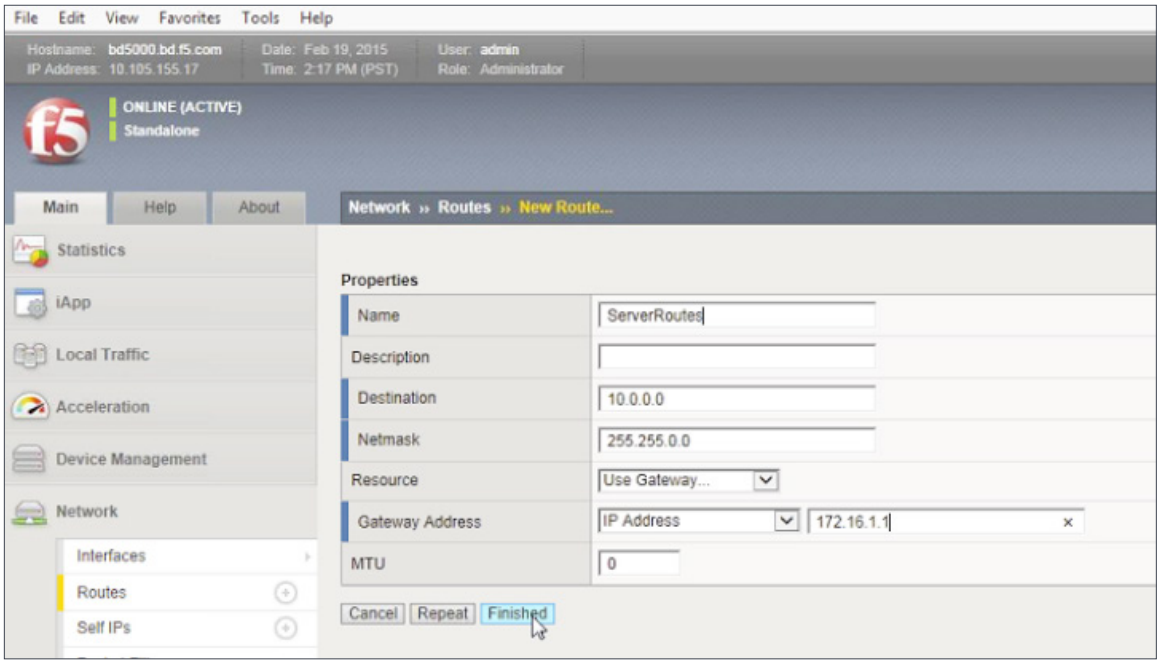
1. From the Main tab of the **BIG-IP Configuration Utility** navigation pane, expand **Network** and select **Routes**.
2. For the **Name**, use the keyword **default**.
3. The default route for both **Destination** and **Netmask** is **0.0.0.0**.
4. The **Gateway Address** is the address of the core router, **20.20.20.1**.
5. Click **Repeat** to complete and add the second route.



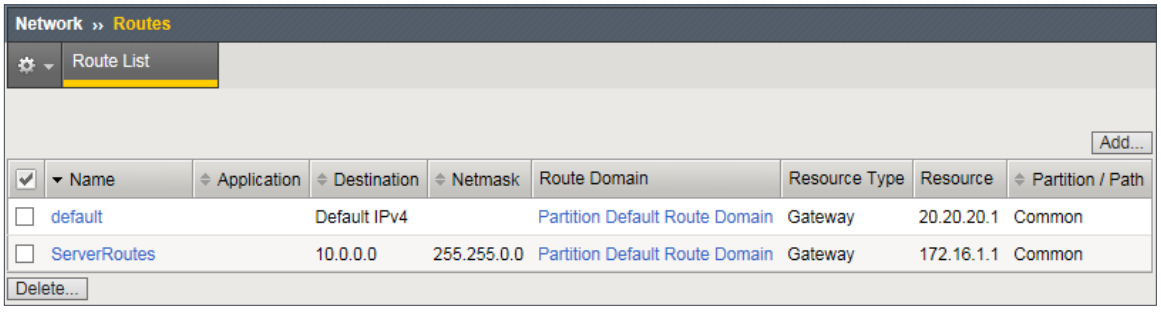
6. For the network route pointing internally to the application servers, use the Name **ServerRoutes**.
7. The **Destination** and **Netmask** for ServerRoutes is **10.0.0.0** and **255.255.0.0** respectively.

8. The **Gateway Address** is the address of the NSX Edge Service Gateway on the transit segment TransitNet1: **172.16.1.1**.

9. Click **Finished** to continue.



10. The completed routing configuration should resemble the configuration below.



Application Configuration

Application configuration typically consists of a base configuration of pool members that are contained within the pool object. The virtual server references the pool to make a load balancing decision among the available pool members. Additional application delivery functionality such as SSL termination, more flexible load balancing algorithm selection,

and layer 7 data plane programmability via iRules can be leveraged but are outside the scope of this validation.

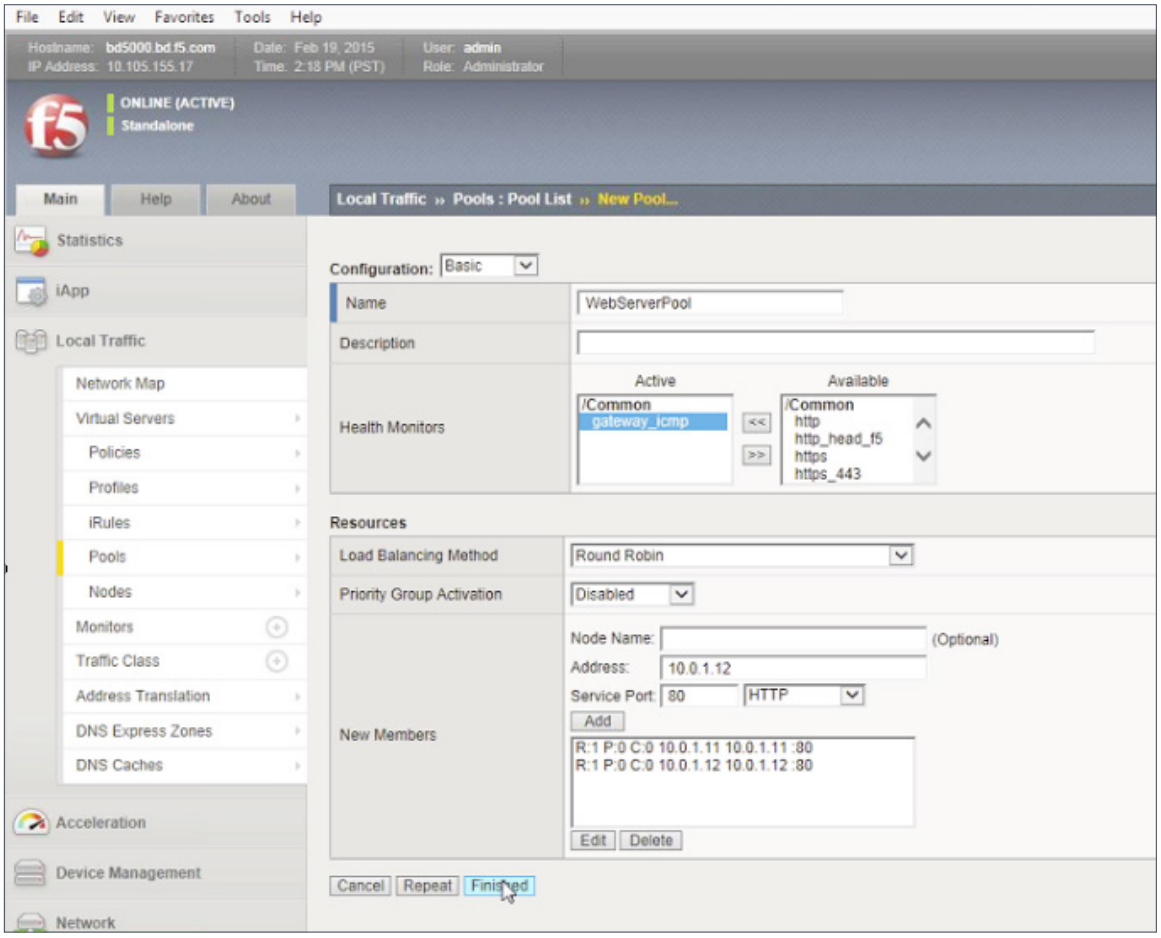
Create application pools

In the following examples, we are creating the most basic of pools for our web and app servers to show the minimum configuration that's required in order for the F5 appliance to load balance the two tiers (web and app). The F5 device will not be load balancing the DB tier traffic, so we are not creating a pool of the DB servers.

1. On the **Main** tab, click **Local Traffic** and then click **Pools** to display the Pool List screen.
2. In the upper right corner of the screen, click the **Create** button.
3. In the **Name** field, type a unique name for the web pool. For this validation, we used **WebServerPool**.
4. In the **Health Monitors** section, select an appropriate monitor for your application. In this case, we chose a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.
5. Under Resources, select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.
6. Under Resources, use the **New Members** setting to add the IP address and port of the web servers (refer to Table 5 below). Click the **Add** button for each pool member.
7. Click **Repeat** to continue and enter the application tier information.

Name (Optional)	Address	Service Port
web-01	10.0.1.11	80 (HTTP)
web-02	10.0.1.12	80 (HTTP)

Table 5. BIG-IP web tier pool members



8. In the **Name** field, type a unique name for the web pool. For this validation **AppServerPool** was used.

9. In the **Health Monitors** section select an appropriate monitor for your application. In this case, we are choosing a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.

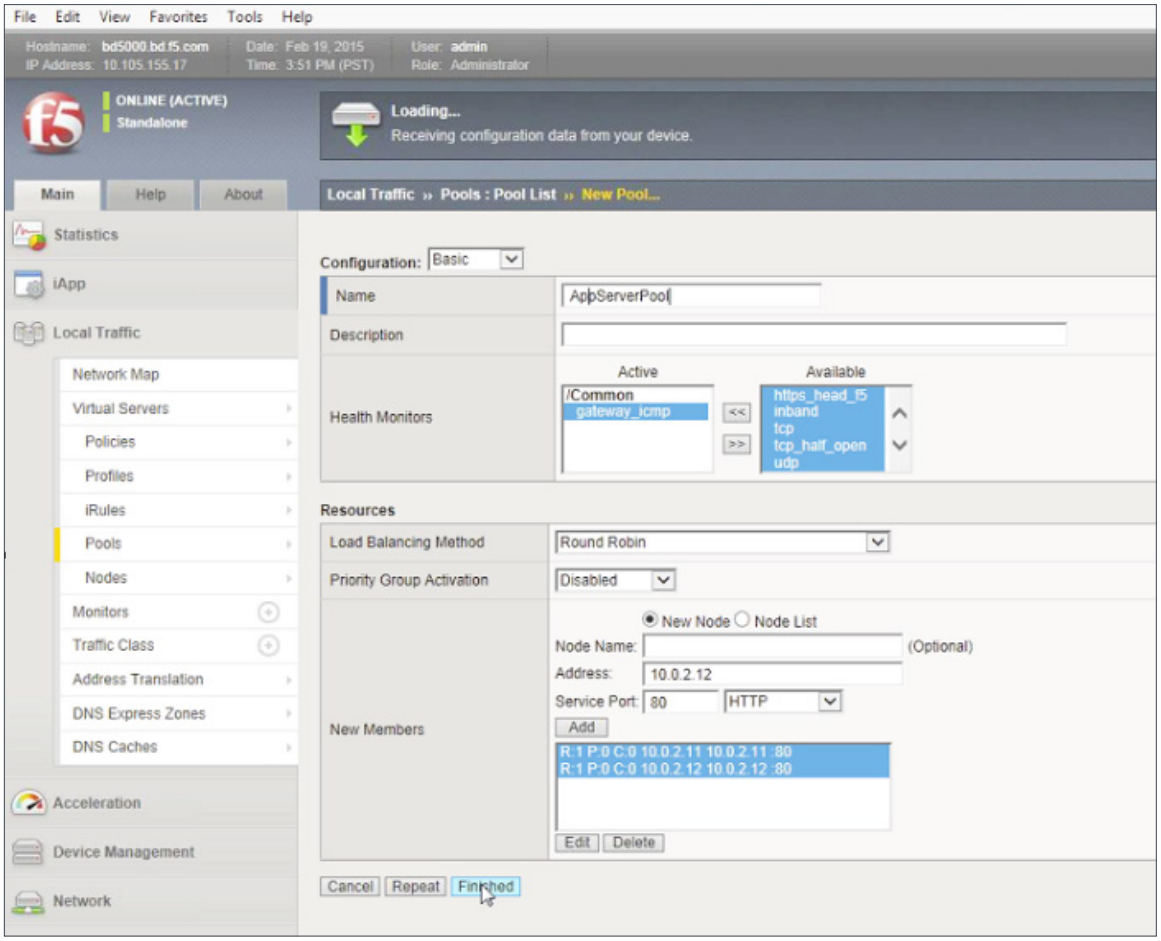
10. In the **Resources** section of the screen select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.

11. In the **Resources** section of the screen, use the New Members setting to add the IP address and port of the web servers (refer to Table 6). Select the **Add** button for each pool member.

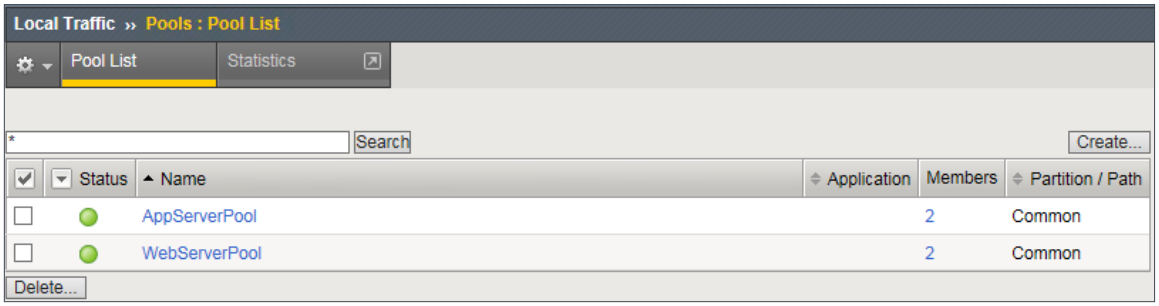
12. Click **Finished** to complete the pool creation.

Name (Optional)	Address	Service Port
App-01	10.0.2.11	80 (HTTP)
App-02	10.0.2.12	80 (HTTP)

Table 6. BIG-IP application tier pool members



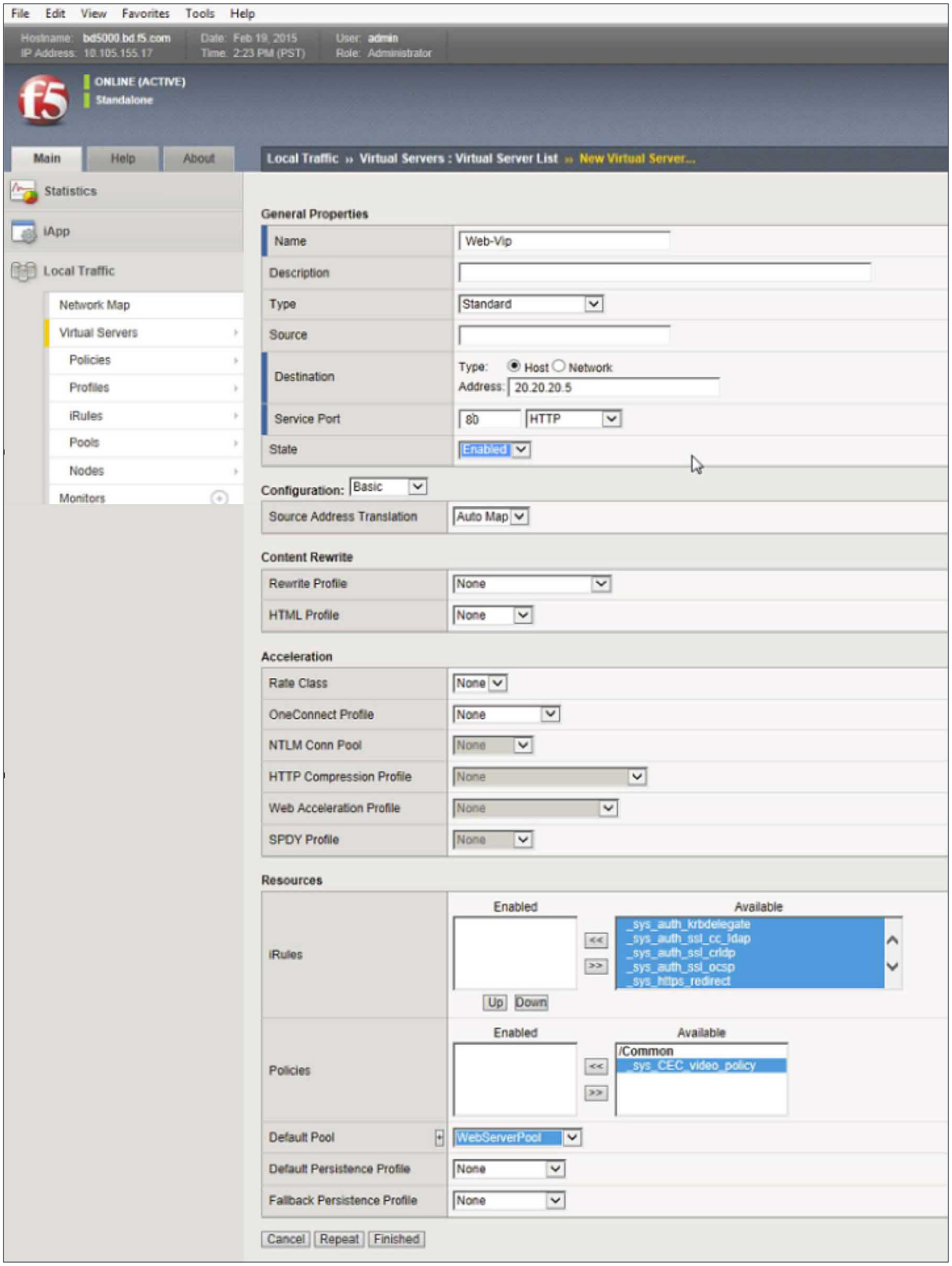
The completed configuration for the web and application tier pools should look similar to the image below. Note that the green circles demonstrate that the health monitor, in this case, ICMP, is able to successfully monitor the servers in the overlay networks.



Create application virtual server

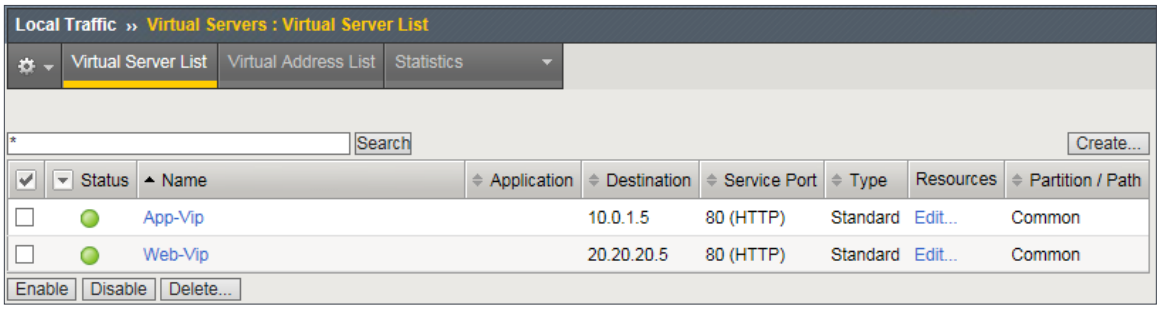
In creating a virtual server, you specify a destination IP address and service port on which the BIG-IP appliance is listening for application traffic to be load balanced to the appropriate application pool members. In this validation, we have two virtual servers (VIPs) to create: one for the web tier, which will be available to the external network on the 20.20.20.0/24 segment, and the other for the application tier, available on the TransitNet-1 segment.

1. On the **Main** tab, select **Local Traffic** and then click **Pools**. The Pool List screen is displayed.
2. In the upper right corner of the screen, click the **Create** button.
3. In the **Name** field, provide a unique name for the web application. In this case, we used **Web-Vip**.
4. In the **Destination Address** field, enter **20.20.20.5**.
5. For **Service Port** use the standard HTTP port **80**.
6. In the **Configuration** section, select **Auto Map** for the **Source Address Translation**.
7. Under Resources, select the **WebServerPool** from the **Default Pool** dropdown box.
8. Click **Repeat** to continue to configure the application tier virtual server.


File Edit View Favorites Tools Help
Hostname: bd5000.bd.f5.com
IP Address: 10.105.155.17
Date: Feb 19, 2015
Time: 2:23 PM (PST)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Main Help About
Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...
Statistics
iApp
Local Traffic
Network Map
Virtual Servers
Policies
Profiles
iRules
Pools
Nodes
Monitors
General Properties
Name
Web-Vip
Description
Type
Standard
Source
Destination
Type: Host Network
Address: 20.20.20.5
Service Port
80
HTTP
State
Enabled
Configuration: Basic
Source Address Translation
Auto Map
Content Rewrite
Rewrite Profile
None
HTML Profile
None
Acceleration
Rate Class
None
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Compression Profile
None
Web Acceleration Profile
None
SPDY Profile
None
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
_sys_auth_ssl_crldp
_sys_auth_ssl_ocsp
_sys_https_redirect
Up
Down
Policies
Enabled
Available
/Common
_sys_CEC_video_policy
Default Pool
WebServerPool
Default Persistence Profile
None
Fallback Persistence Profile
None
Cancel
Repeat
Finished

1. In the upper right corner of the screen, click the **Create** button.
2. In the **Name** field, provide a unique name for the web application. In this case, we used **App-Vip**.
3. In the **Destination Address** field, enter the IP address **10.0.1.5**.
4. For **Service Port**, use the standard HTTP port **80**.
5. In the **Configuration** section, select **Auto Map** for the **Source Address Translation** field.
6. Under Resources, select **AppServerPool** from the dropdown box.
7. Again, click **Finished** to continue to configure the application tier virtual server.

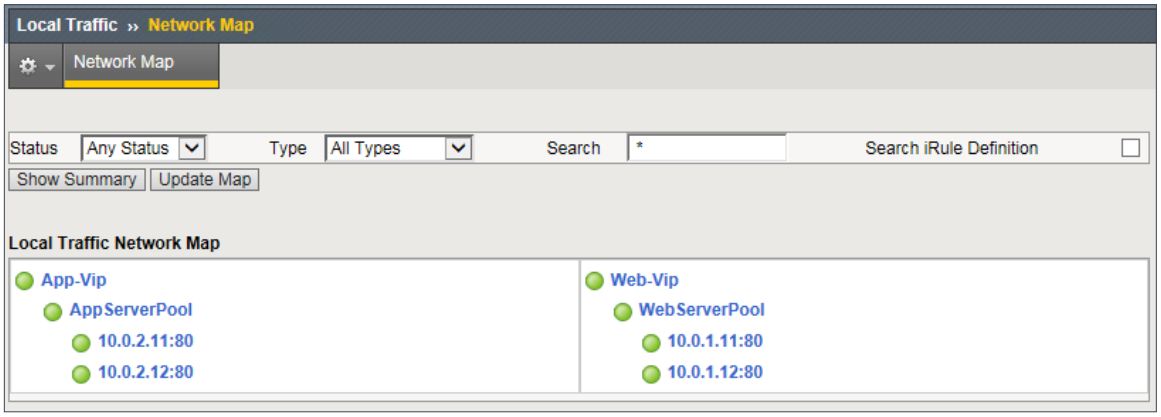
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.



Validation

The web tier virtual server should now be available and accepting application traffic on port 80 (HTTP).

On the **Main** tab, expand **Local Traffic** and then click **Network Map** to display the overall health of the applications and their associated resources.



Any web browser can be used to test by typing http://20.20.20.5 to send a request to the virtual server. A simple Apache web server can be installed on the web tier to validate.

This concludes the validation of the *Adjacent to NSX Edge Using VXLAN Overlays with BIG-IP Physical Appliances* deployment scenario.

Topology 2: Parallel to DLR Using VLANs with BIG-IP Physical Appliances

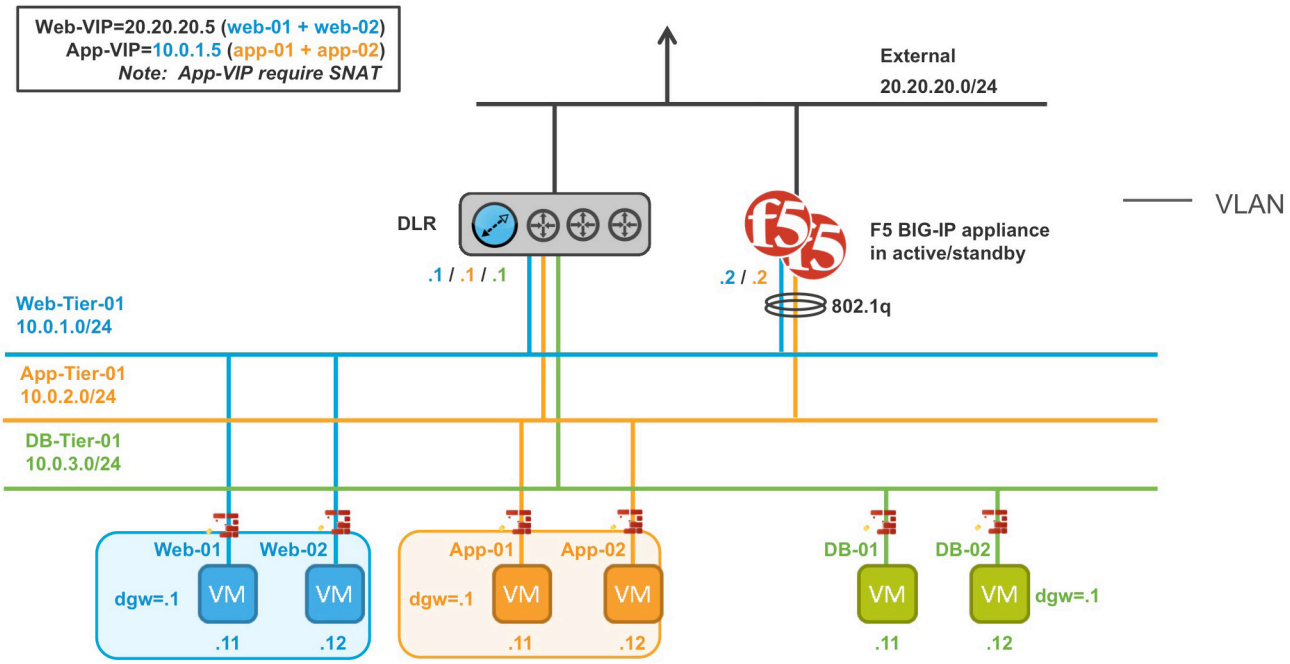


Figure 4. BIG-IP appliances parallel to DLR

The second deployment scenario also utilizes a topology with a second data path for application delivery traffic. BIG-IP appliances are arranged logically parallel to the Distributed Logical Router (DLR). There is no requirement in this scenario for an NSX Edge Services Gateway.

The BIG-IP appliance has 802.1Q tagged interfaces directly into the web and application tiers. This allows application-specific optimizations and load balancing decisions to take place, and the BIG-IP appliance will let the layer 2 network determine the optimal path between the BIG-IP appliance and the application servers. It is also a key enforcement point for application-specific security policies to be built from layer 4 through layer 7 outside the flow and policy enforcement for traditional east-west traffic. Since the BIG-IP appliance is directly connected to the application networks, address space for application VIPs and SNATs for inter-tier load balancing can be utilized from those individual networks and do not need to traverse a transit network.

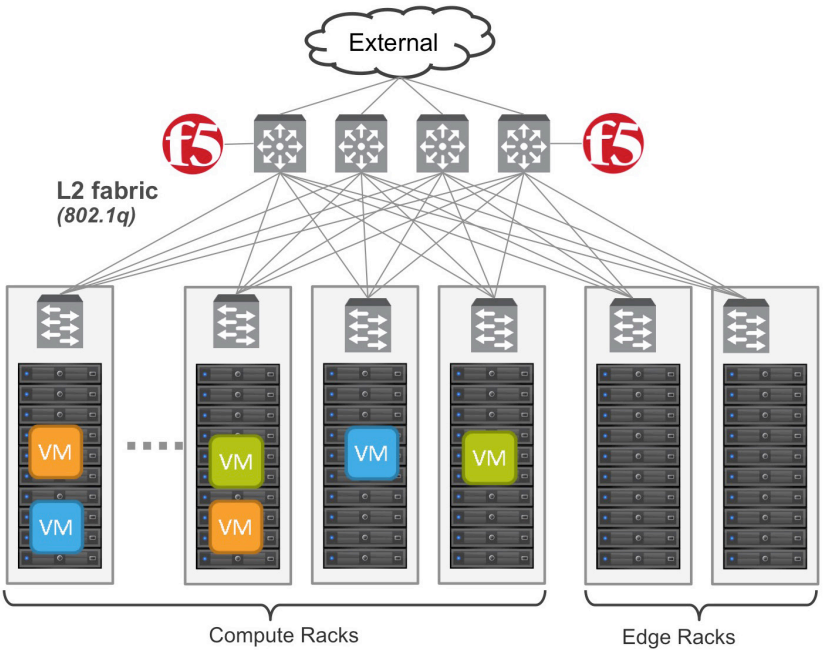


Figure 5. Traditional layer 2 topology with BIG-IP in distribution layer

The physical topology in this deployment scenario connects the BIG-IP appliance in the traditional distribution tier to provide an optimal layer 2 path for application traffic. The DLR instances provide an optimal east-west path between tiers and to external networks.

Implementation Infrastructure

In the validation environment, the same ESXi clusters are in use.

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 6: USSJ-55-Management Cluster and the USSJ-55-Compute Cluster. While this is a smaller representation of a data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 5.

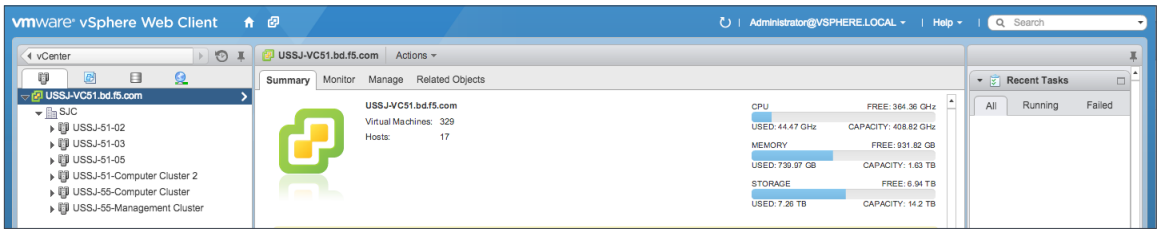


Figure 6. vSphere console

In accordance with best practices, management and compute ESXi hosts are physically and logically separated from one another. Physical BIG-IP devices are installed in distribution racks, and vCenter and NSX manager will be installed in the management racks.

The virtual machines used as Web (web), Application (app), and Database (DB) servers will be running on ESXi hosts in the compute cluster. To better understand data traffic flows for this deployment scenario topology, examine the *VMWare NSX for vSphere (NSX-V) and BIG-IP Design Guide*.

Prerequisites

Referencing the diagram in Figure 4, the BIG-IP appliance requires connectivity for two physical interfaces. One interface is used for management of the device and the other is used for all production traffic. The VLAN numbers, and the IP addressing scheme can be tailored to your environment.

- The physical BIG-IP appliances will need to be installed and connected to the distribution switches. Each BIG-IP appliance's management interface will need to be connected to a switchport on a top-of-rack management switch that has the management VLAN extended to it, and configured with an IP address in the management segment.
- For this environment, a BIG-IP interface 1.1 will need to be connected to a switchport on the distribution switch that 802.1Q tags the VLANs used in this environment. In the example, VLANs 20, 160, 161, and 162 are used.
- Physical network infrastructure switches connected to the ESXi servers are configured to support 802.1Q tagging and allow the appropriate VLANs.
- ESXi hosts will need to be configured with the appropriate distributed port groups and virtual switches.

Name	802.1Q VLAN ID
External	20
dvs_VL155_NSXIPPool	155
Web-Tier-01	160
App-Tier-01	161
DB-Tier-01	162

Table 7. VLAN tags for configuration on distributed virtual switch and physical switches

Network Segments

Two types of network segments are utilized in this topology: traditional 802.1Q VLAN network segments and VXLAN overlay segments. Within NSX, we created IP pools that will be used by the Web, App, and DB virtual machines.

802.1Q VLAN segments

VLAN 20 External is the VLAN used for external connectivity. The 20.20.20.0/24 IP subnet range is configured on this VLAN.

VLAN 155 dvs_VL155_NSXIPPool *(not shown)* is for management connectivity. The 10.105.155.0/24 IP subnet range is configured on this VLAN.

VLAN 160 Web-Tier-01 is the VLAN ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VLAN.

VLAN 161 App-Tier-01 is the VLAN ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VLAN.

VXLAN 162 DB-Tier-01 is the VLAN ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VLAN.

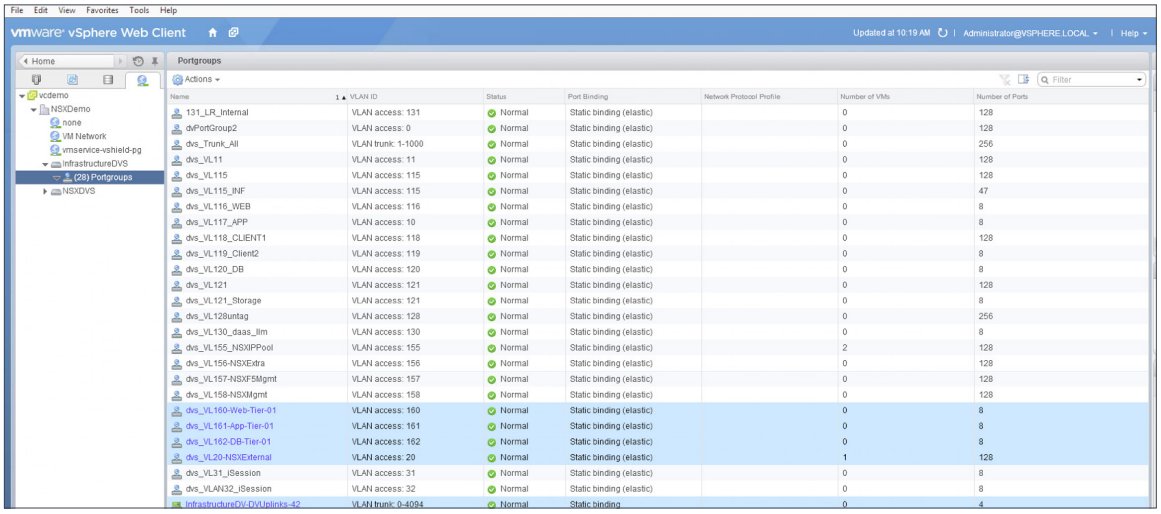


Figure 7. vSphere DVS VLAN configuration example

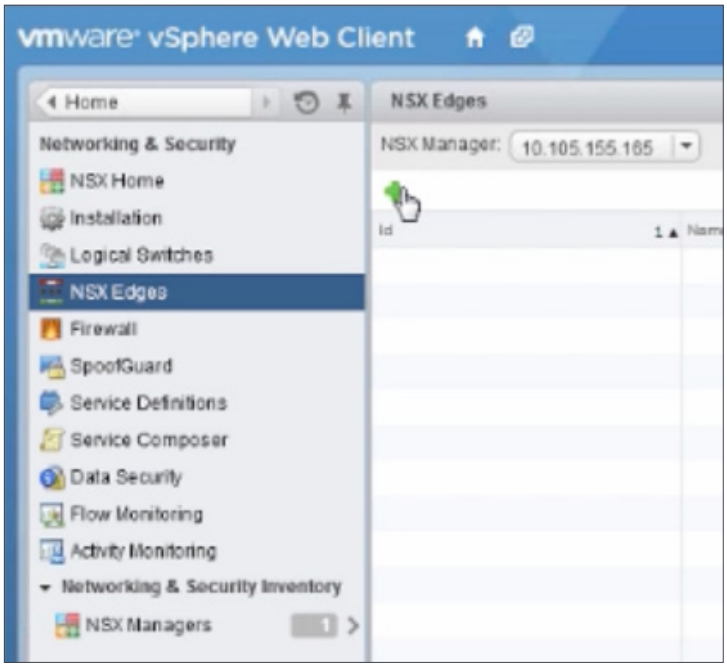
PortGroups are created in vSphere that are tagged with the VLANs 20, 155, 160-162. A DV uplink that is 802.1Q tagging with VLANs 0-4094 connected to the top-of-rack switches. The top-of-rack switches must have at least these four VLANs tagged up to the distribution switches.

Create and Deploy DLR

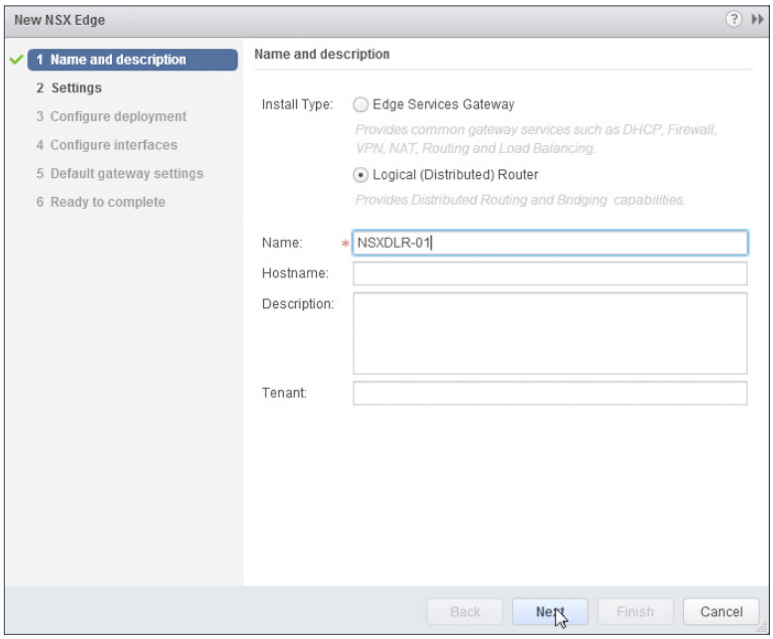
Within VMWare NSX the Distributed Logical Router (DLR) provides an optimized way of handling east-west traffic within the data center. East-west traffic is communication between virtual machines or other resources on different subnets within a data center. As east-west traffic needs increase within the data center, the distributed architecture allows for optimized routing between VXLAN segments.

(Note that DLR and LDR—Logical (Distributed) Router—are used synonymously by VMware.)

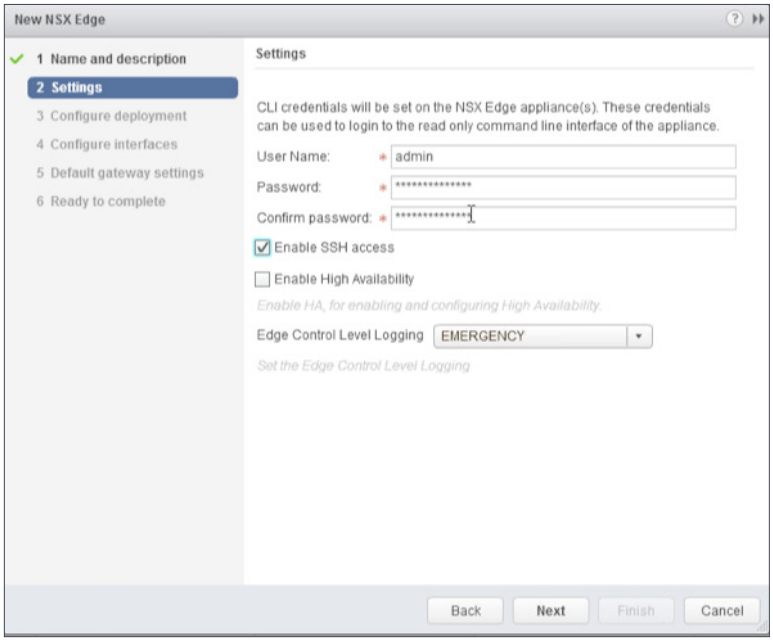
1. Return to the **vSphere Web Client** console and choose **Networking & Security** in the left column. Under **Networking and Security**, choose **NSX Edges** and then click the green plus symbol (+).



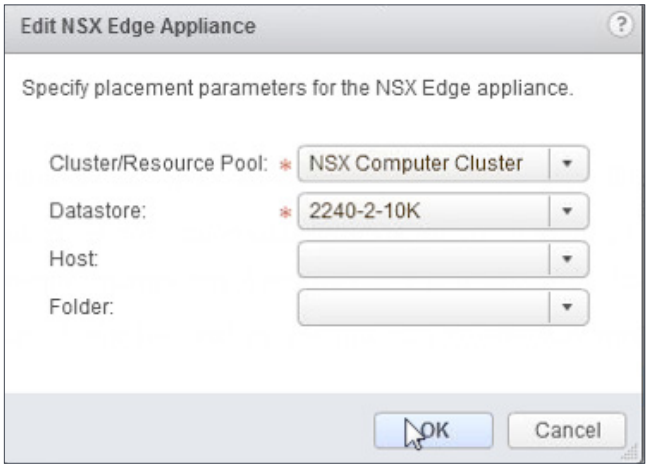
2. Select the **Logical (Distributed) Router** as the **Install Type** and provide a name for the device, then click **Next**.



3. Under **Settings**, check the **Enable SSH access** check box and provide a username and password for the Edge Services Gateway. Click **Next** to proceed.

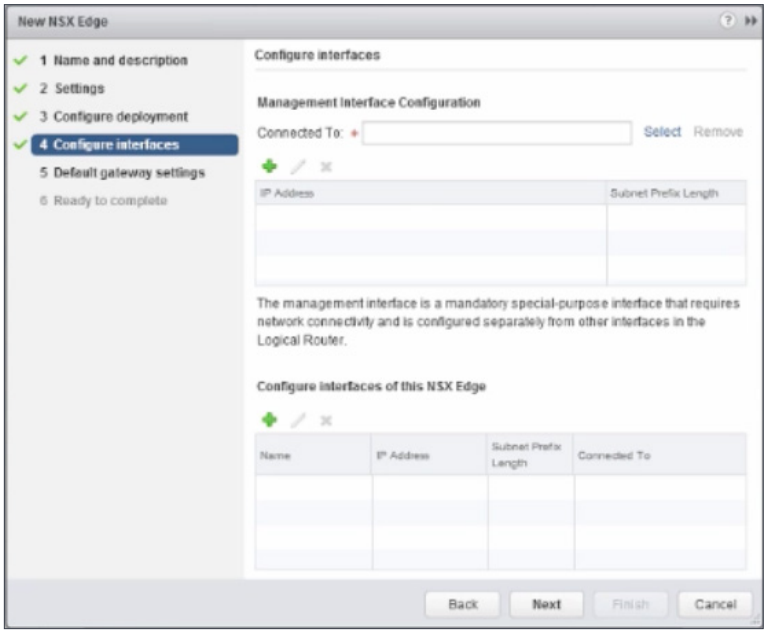


4. Selecting the green plus symbol in the **Configure deployment** section will display the options in the dialog box below. Choose the appropriate Cluster/resource pool **(NSX Computer Cluster)**, and Datastore (**2240-2-10K**). The host selection is optional. Ensure the NSX DLR is deployed in the NSX Computer Cluster. Click **OK** to complete, and **Next** to continue.

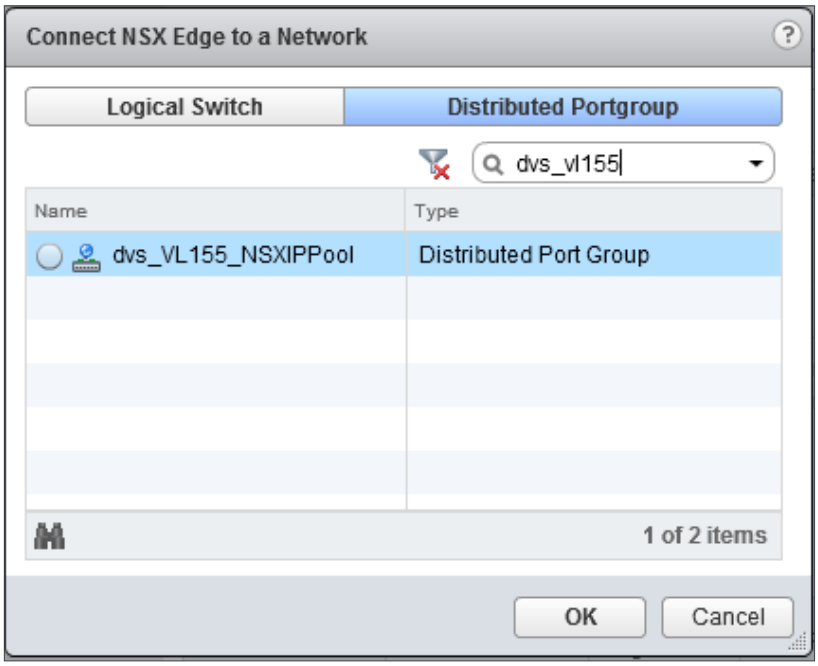


5. Configure Interfaces for the DLR.

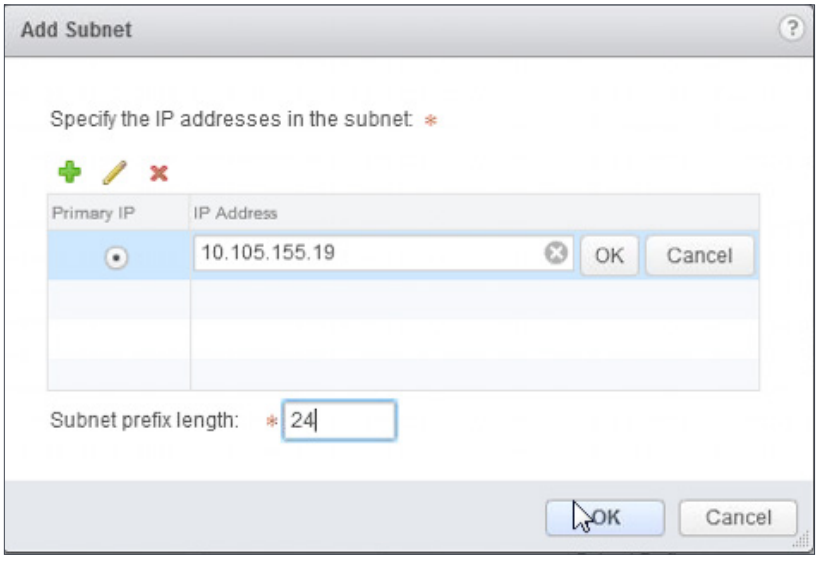
   a. First configure the management interface for the DLR. Click **Select** to the right of the **Connected To** field under **Management Interface Configuration**.



b. In this case, the management interface should be connected to a distributed port group that is connected to the shared management VLAN.



c. Click the green plus symbol (+) to specify a fixed **IP Address** and **Subnet prefix length** in the management network.

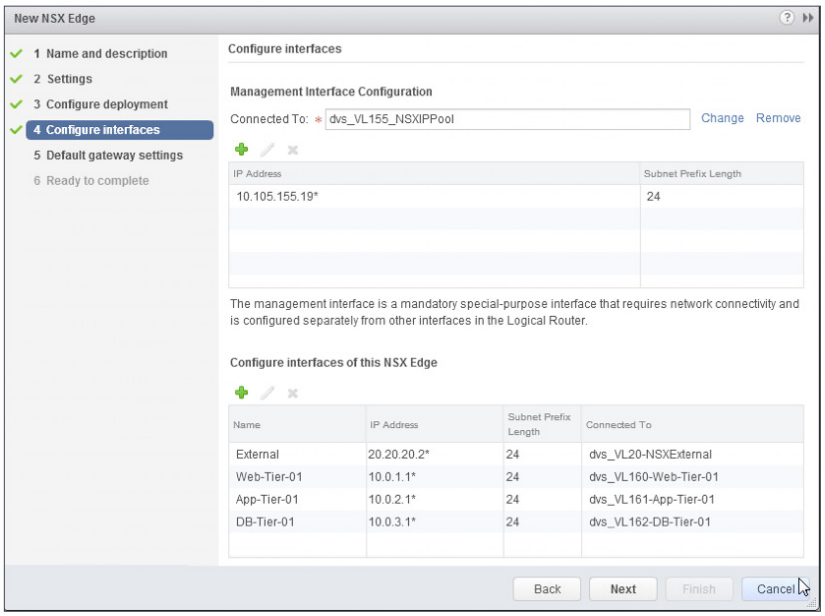


6. For each of the four interfaces required for this deployment scenario, configure the appropriate subnets and switch type according to the table below. Select the green plus symbol under Configure Interfaces of this NSX Edge to bring up the Add Interface dialog box.

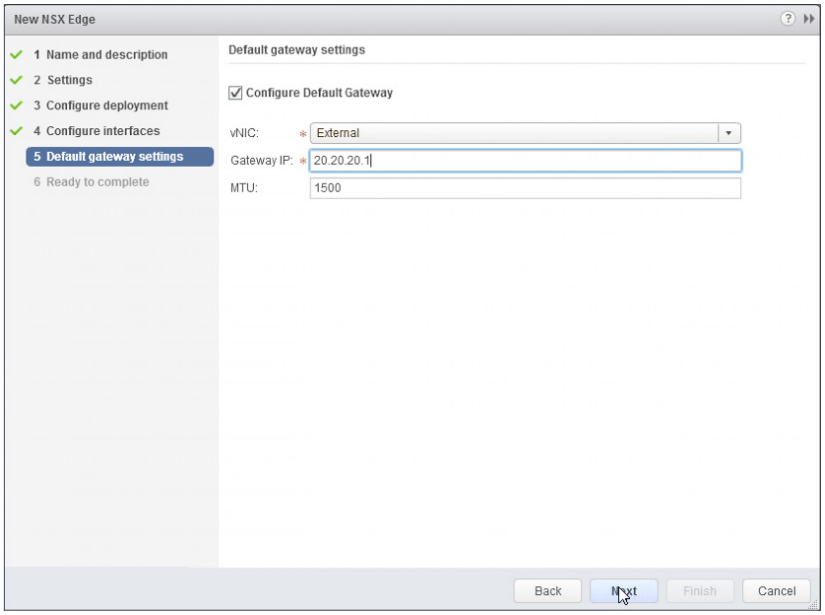
Network Name	Connected To	Interface IP/Subnet Prefix
External	dvs_VL20-NSXExternal	20.20.20.2/24
Web-Tier-01	dvs_VL160-Web-Tier-01	10.0.1.1/24
App-Tier-01	dvs_VL161-App-Tier-01	10.0.2.1/24
DBTier	dvs-VL162-DB-Tier-01	10.0.3.1/24

Table 8. NSX distributed logical router network interfaces

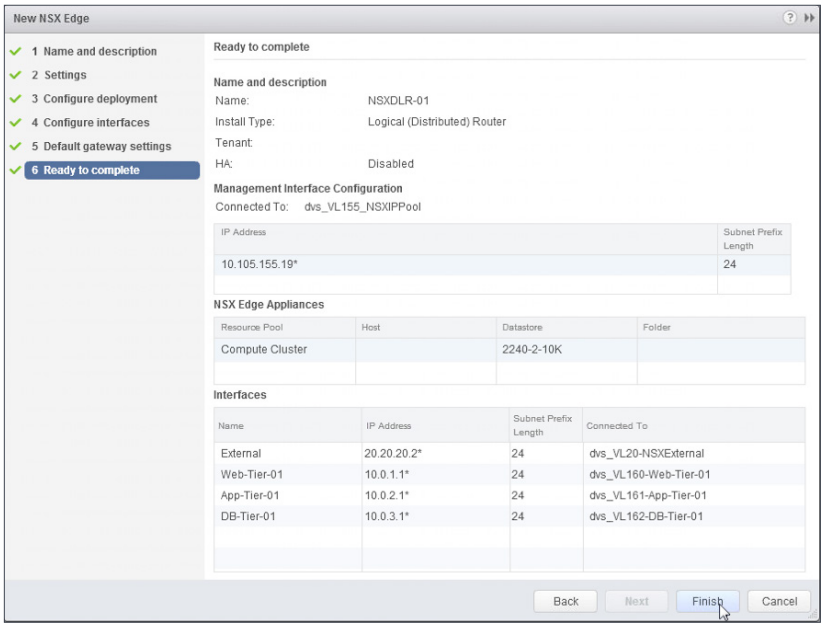
The complete DLR interface configuration, once complete should resemble the diagram below. Click **Next** to continue.



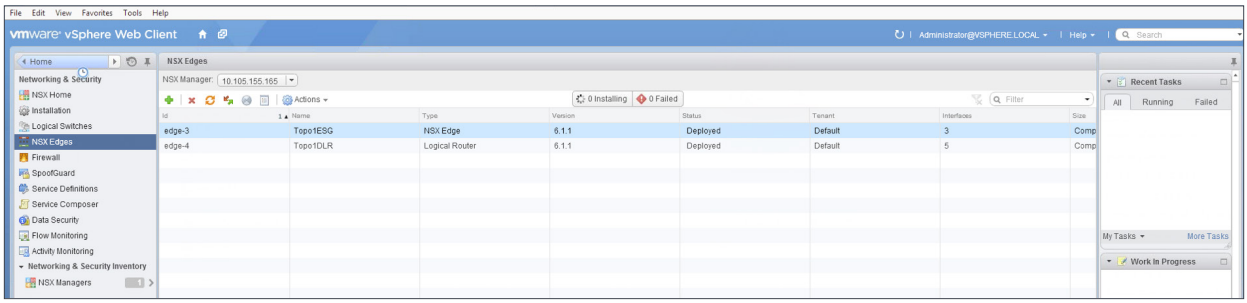
7. With the interface settings complete, the next step is to configure the Default gateway settings. The default gateway for the DLR is our data center backbone router with the IP address of **20.20.20.1**. Use the default MTU parameter unless the network is using an MTU of a different size, such as jumbo frames. Configuring a non-standard MTU that is inconsistent can lead to unnecessary fragmentation of packets or black-holing of some traffic. Click **Next** to proceed.



8. Review your configuration under **Ready to complete** and then click **Finish** to deploy the DLR. Depending on the number of ESXi hosts, it may take some time for the DLR deployment to complete.



9. Once complete, the vSphere NSX Edges configuration should resemble the image below.



BIG-IP Appliance Configuration

The validation of this topology is currently configured on a single device. The base network configuration consists of configuring the VLANs and assigning them to an interface and creating the appropriate self IP for each of the network segments. For production deployments, F5 recommends that two BIG-IP devices are configured in an HA configuration.

Prerequisites

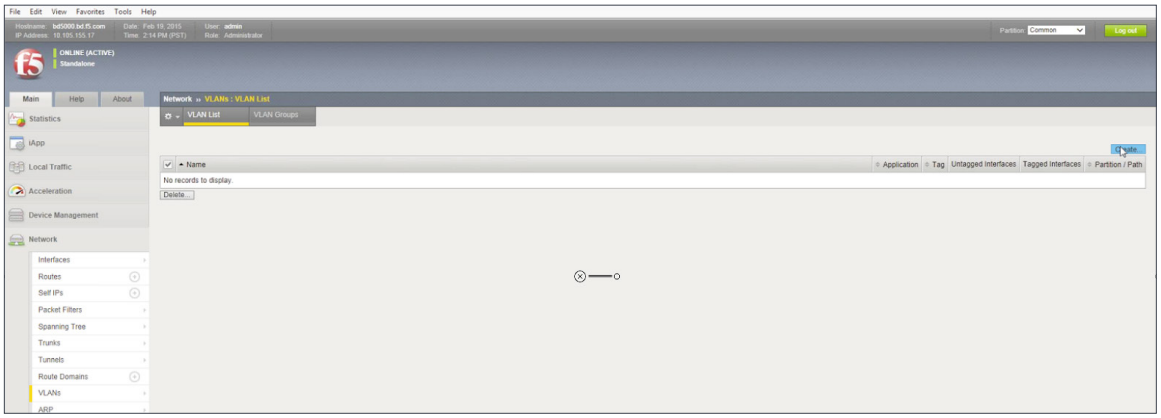
- The BIG-IP appliance is configured with a management IP address in the proper subnet.
- Licenses have been applied and activated.
- Appropriate provisioning of resources is complete.
- Base configuration of services DNS, NTP, SYSLOG are configured.
- BIG-IP Interface 1.1 is physically wired to a distribution switch configured to support 802.1Q tagging of traffic on VLANs 20, 160 and 161.

For info on how to perform these Installation and basic set up steps refer to http://support.f5.com and consult the appropriate Implementation guide for your version and device.

Create VLANs

1. From the **Main** tab of the **BIG-IP Configuration Utility** navigation pane, select **Network** and then click **VLANs**.

2. In the upper right corner, click the **Create** button.

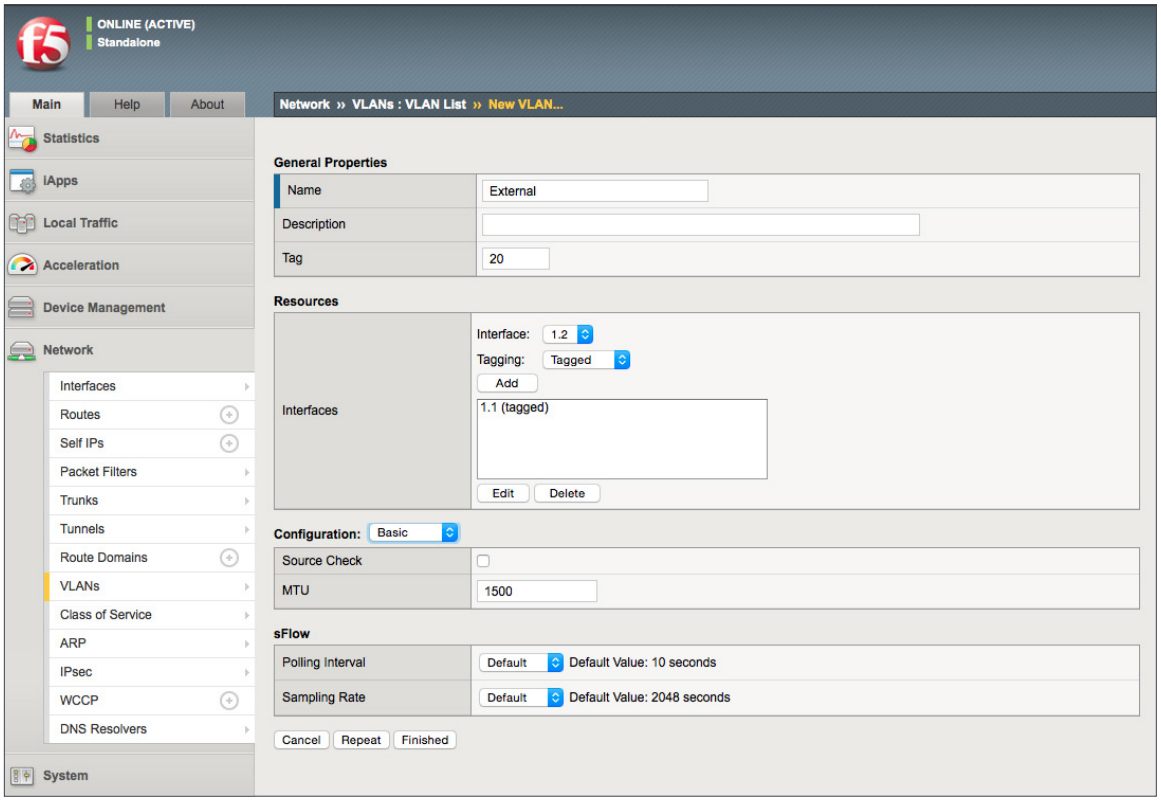


3. Under **General Properties**, type a unique name for the VLAN. In this case, we used **External**.

4. For the **Tag**, enter the External VLAN ID of **20**.

5. Under **Resources**, select **Interface 1.1**.

6. Select **Tagged** from the dropdown box and click the **Add** button below it.



7. Click **Repeat** to continue.

8. Proceed with creating the web tier network. Under **General Properties**, type a unique name for the VLAN. In this case, we used **Web-Tier**.

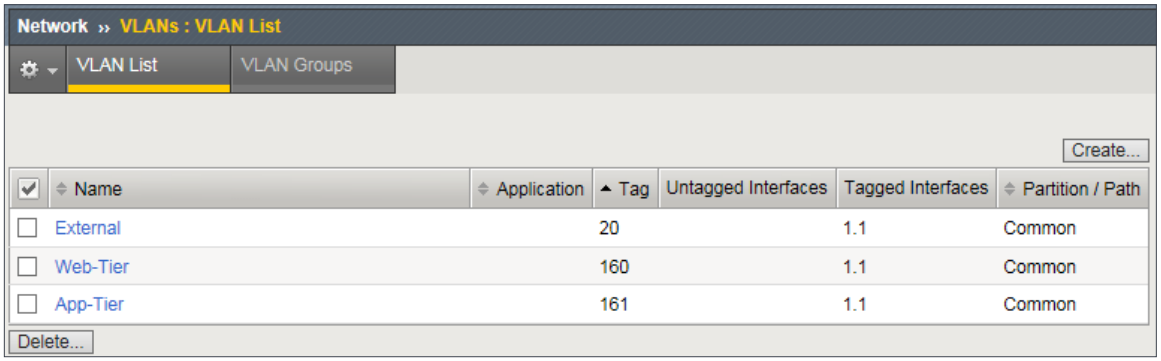
9. For the **Tag**, enter the TransitNet-1 VLAN ID of **160**.

10. Under **Resources**, select Interface 1.1.

11. Select **Tagged** from the dropdown box and click the **Add** button below it.

12. Click **Repeat** and return to step 8 for **VLAN 161 App-Tier** to complete the VLAN creation. Click **Finished** to proceed.

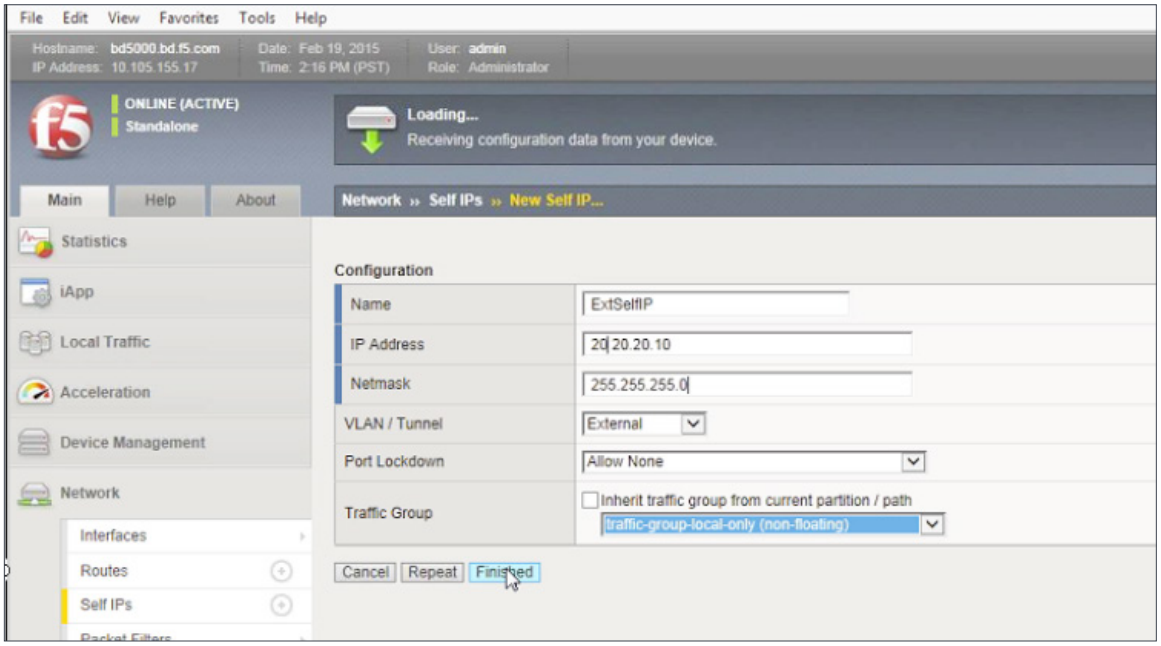
13. Validate the VLAN configuration against the image below.



Configure Self IP Addresses

Self IP addresses are logical interfaces that allow the BIG-IP to participate in the networks for which they are configured. They also are useful for functions such as SNAT to ensure symmetric traffic patterns.

1. From the **Main** tab of the BIG-IP navigation pane, click **Network** and then select **Self IPs**.
2. In the upper right corner of the screen, click the **Create** button.
3. Provide a unique name in the Name box. In this example, we used **ExtselfIP**.
4. For the **IP Address**, enter the IP address you want to assign to a VLAN. For the External network, use **20.20.20.10**.
5. For **Netmask**, provide the appropriate subnet mask. In this example, we used **255.255.255.0**.
6. For the **VLAN/Tunnel**, select **External** from the dropdown box.
7. Use the default settings for both **Port Lockdown** and **Traffic Group**.
8. Click the **Repeat** button to continue.



9. Complete the configuration for the **WebSelf** self IP using the following settings:

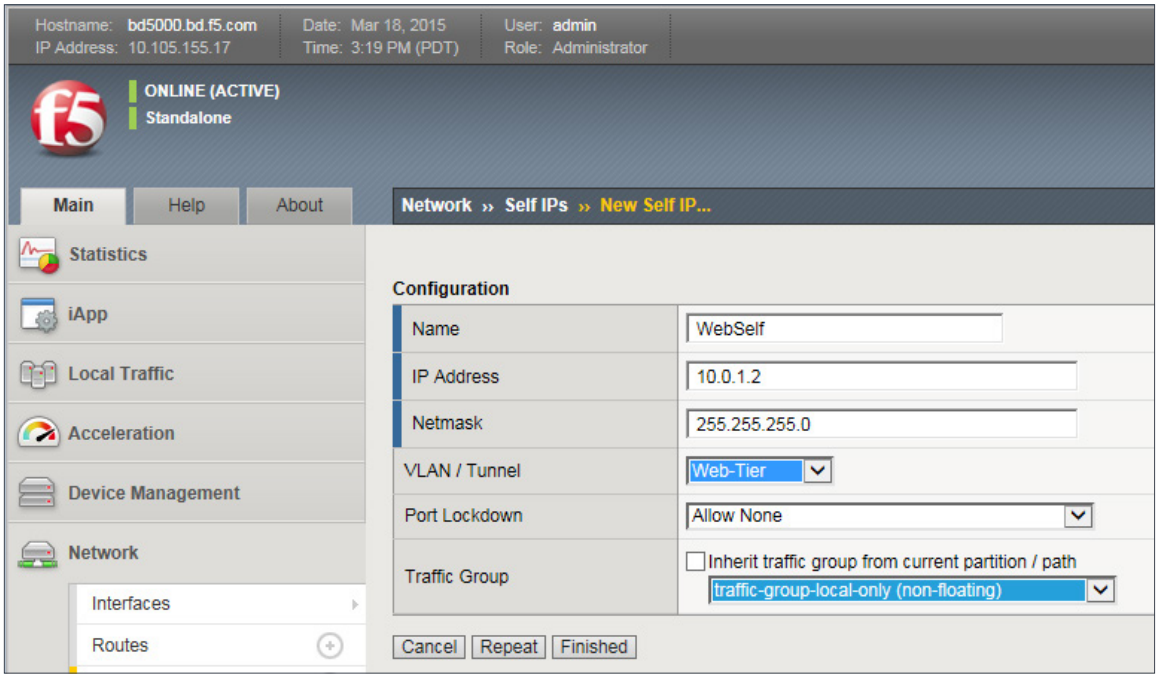
    a. Name: **WebSelf**

    b. IP Address: **10.0.1.2**

    c. Netmask: **255.255.255.0**

    d. VLAN/Tunnel: **Web-Tier**

10. Click the **Repeat** button to continue.



11. Complete the configuration for the **AppSelf** self IP using the following settings:

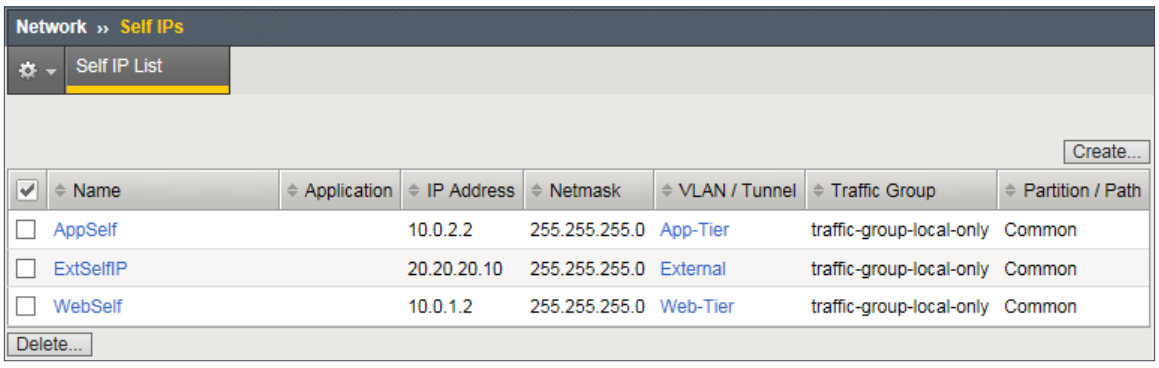
    a. Name: **AppSelf**

    b. IP Address: **10.0.2.2**

    c. Netmask: **255.255.255.0**

    d. VLAN/Tunnel: **App-Tier**

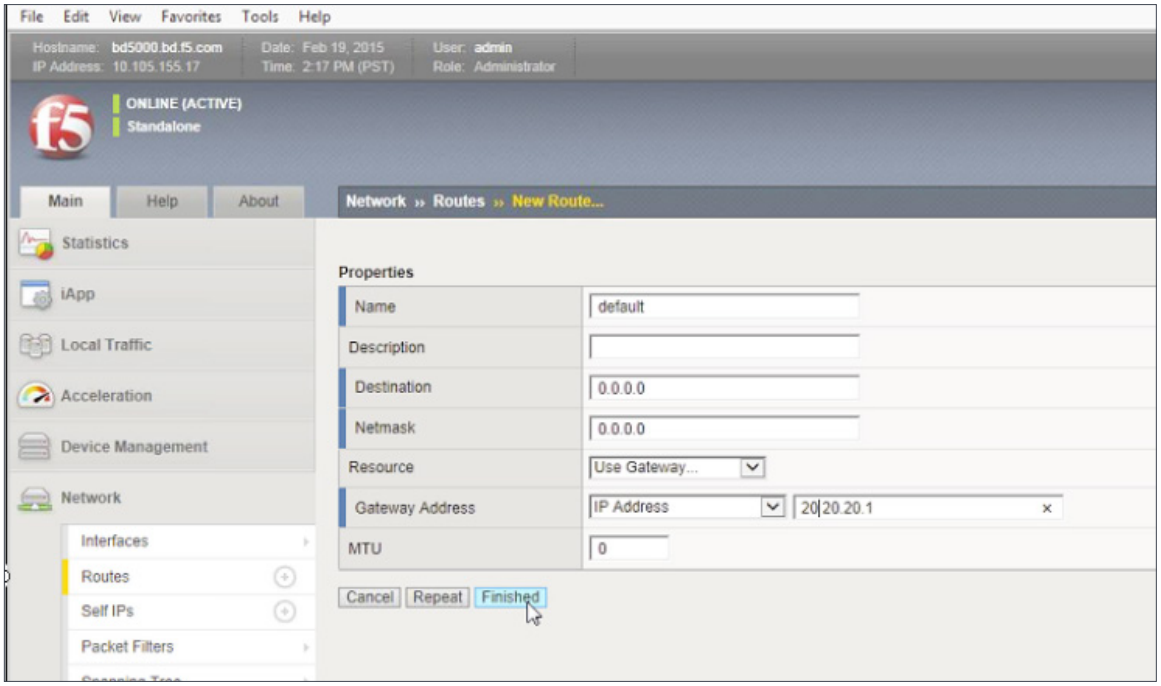
12. Click **Finished** and validate the completed self IP configuration.



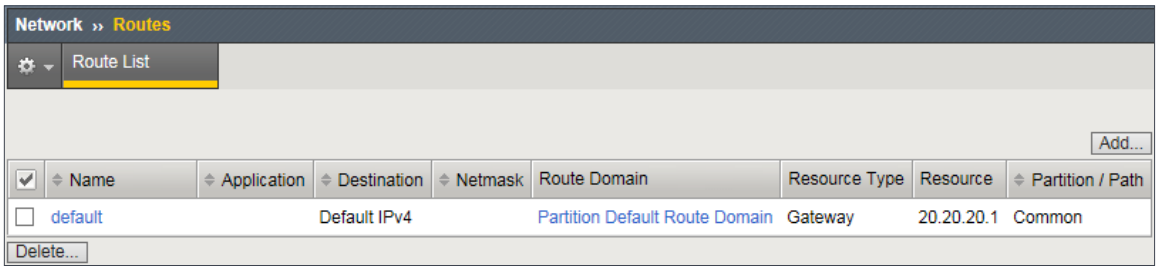
Configure a Default Static Route

The External VLAN will be used for web tier application traffic VIPs, and a default static route is configured to ensure external traffic is routed to the core router. Since the BIG-IP already has interfaces in the Web-Tier and Application-Tier networks, it does not need a route to participate in those segments.

1. From the Main tab of the **BIG-IP Configuration Utility** navigation pane, expand **Network** and select **Routes**.
2. Use the keyword **default** for the Name.
3. The default route for both Destination and Netmask is **0.0.0.0**.
4. The Gateway Address is the address of the core router **20.20.20.1**.
5. Click **Finished** to continue.



The completed routing configuration should resemble the configuration below.



Application Configuration

Application configuration typically consists of a base configuration of pool members that are contained by the pool object. The virtual server references the pool to make a load balancing decision amongst the available pool members. Additional application delivery functionality such as SSL termination, more flexible load balancing algorithm selection, and layer 7 data plane programmability via iRules can be leveraged but are outside the scope of this validation.

Create application pools

In the following examples, we are creating the most basic of pools for our web and app servers, to show the minimum configuration that needs to be done for the BIG-IP appliance to load balance the two tiers (web and app). The F5 device will not be load balancing the DB tier traffic, so we are not creating a pool of the DB servers.

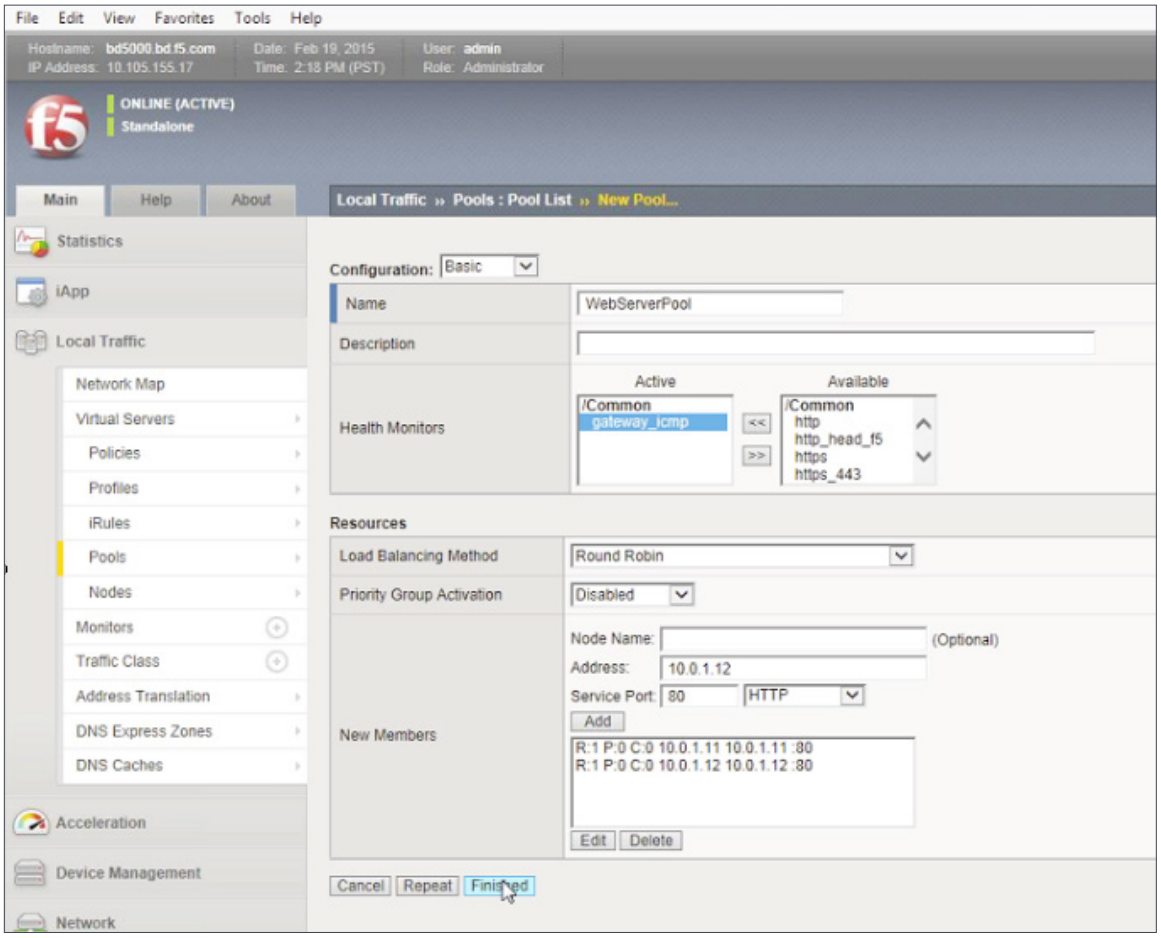
1. From the **Main** tab, expand **Local Traffic** and then click **Pools** to display the Pool List screen.
2. In the upper right corner of the screen, click the **Create** button.
3. In the **Name** field, type a unique name for the web pool. For this validation, we used **WebServerPool**.
4. Under **Health Monitors**, select an appropriate monitor for your application. In this case, we chose a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.
5. Under **Resources**, select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.

6. Under Resources, use the **New Members** setting to add the IP address and port of the web servers (refer to table 9 below). Click the **Add** button for each pool member.

7. Click **Repeat** to continue and enter the Application Tier information.

Name (Optional)	Address	Service Port
web-01	10.0.1.11	80 (HTTP)
web-02	10.0.1.12	80 (HTTP)

Table 9. BIG-IP web tier pool members



8. In the **Name** field, type a unique name for the web pool. For this validation AppServerPool was used.

9. Under **Health Monitors**, select an appropriate monitor for your application. In this case we are choosing a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.

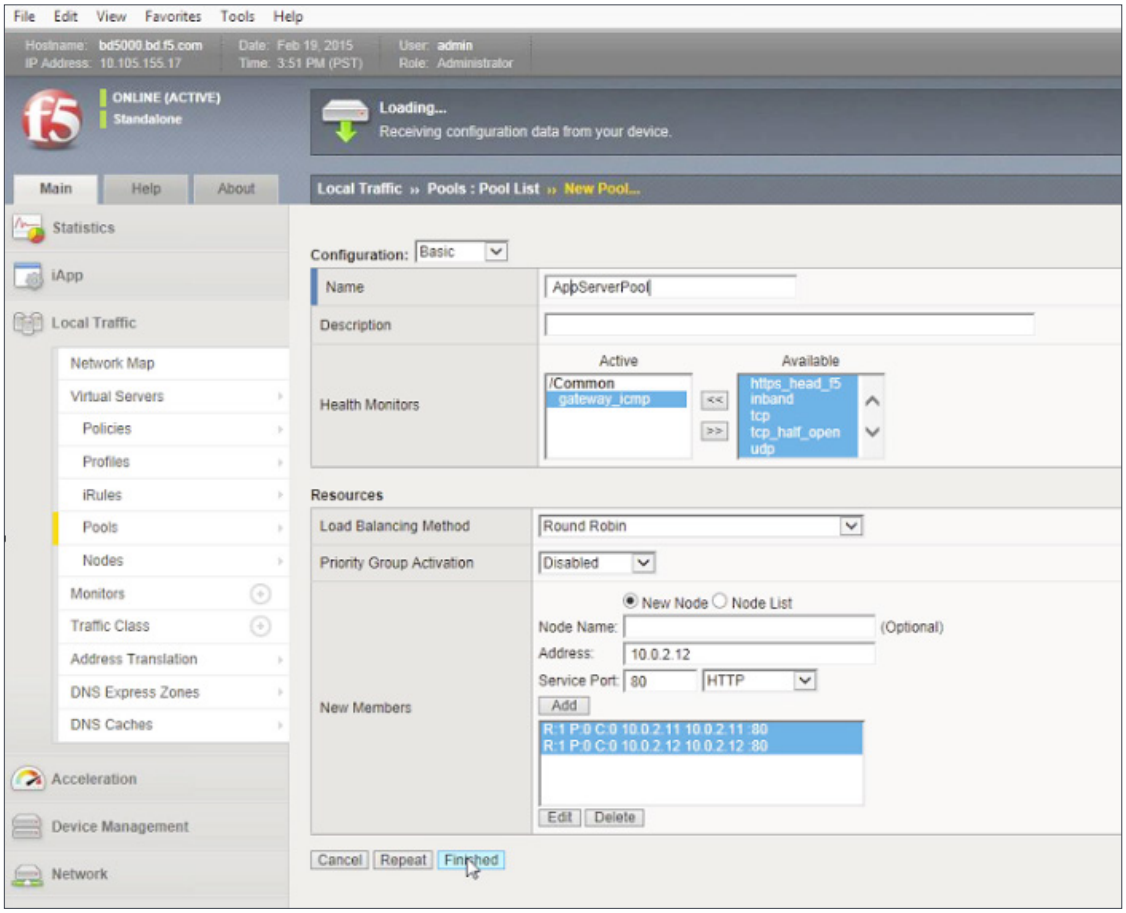
10. Under **Resources**, select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.

11. Under **Resources**, use the **New Members** setting to add the IP address and port of the web servers (refer to Table 10). Click the **Add** button for each pool member.

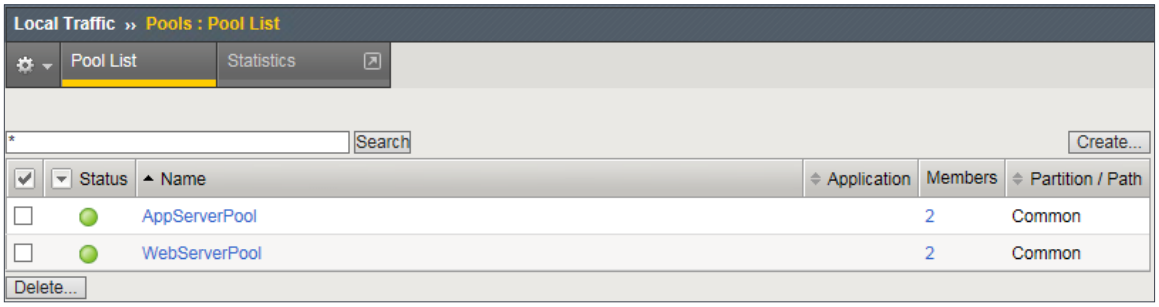
12. Click **Finished** to complete the pool creation.

Name (Optional)	Address	Service Port
App-01	10.0.2.11	80 (HTTP)
App-02	10.0.2.12	80 (HTTP)

Table 10. BIG-IP application tier pool members



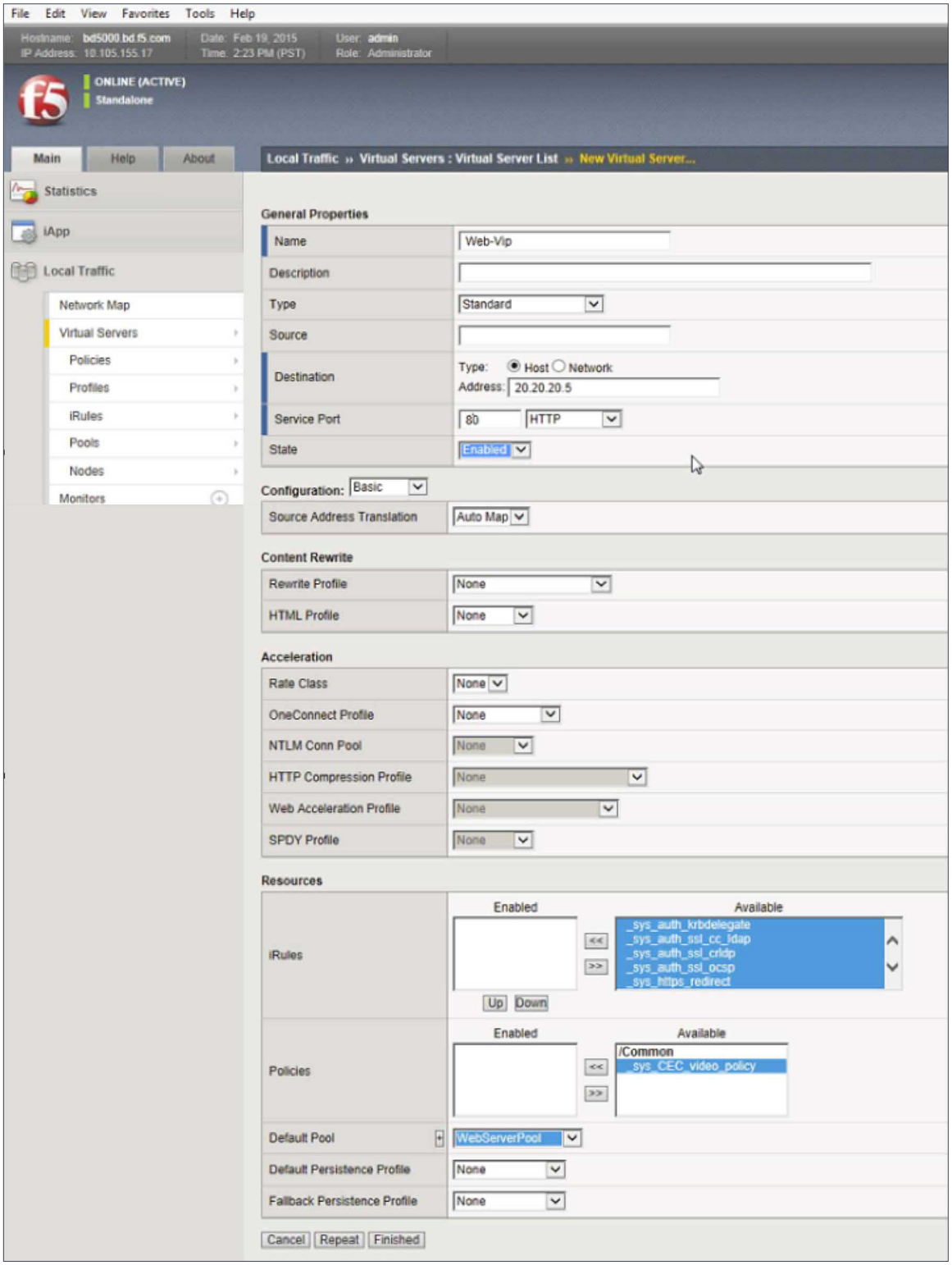
The completed configuration for the web and application tier pools should look similar to the image below. Note that the green circles demonstrate that the health monitor, in this case, ICMP, is able to successfully monitor the servers in the overlay networks.



Create application virtual server

In creating a virtual server, you specify a destination IP address and service port on which the BIG-IP appliance is listening for application traffic to be load balanced to the appropriate application pool members. In this validation, we have two virtual servers (VIPs) to create: one for the web tier, which will be available to the external network on the 20.20.20.0/24 segment, and the other for the application tier, available on the TransitNet-1 segment.

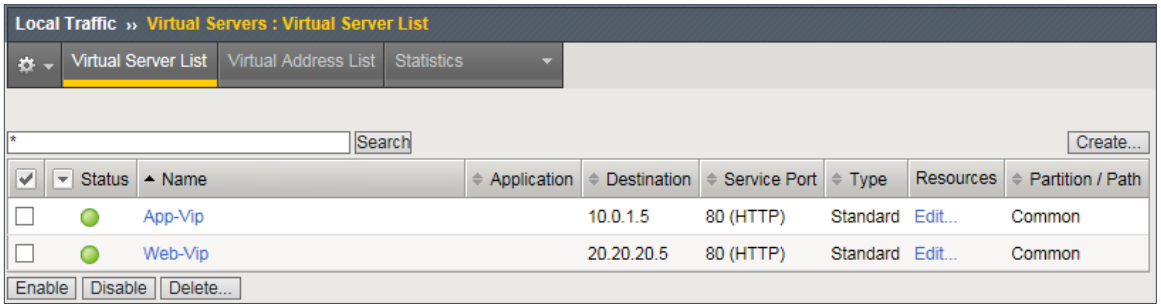
1. On the **Main** tab, expand **Local Traffic** and then click **Pools**. The Pool List screen is displayed.
2. In the upper right corner of the screen, click the **Create** button.
3. Under **General Properties** in the **Name** field, provide a unique name for the web application. In this case, we used **Web-Vip**.
4. In the **Destination Address** field, enter **20.20.20.5**.
5. For **Service Port** use the standard HTTP port **80**.
6. Under **Configuration**, select **Auto Map** for the **Source Address Translation**.
7. Under **Resources**, select the **WebServerPool** from the Default Pool dropdown box.
8. Click **Repeat** to continue to configure the application tier virtual server.


File Edit View Favorites Tools Help
Hostname: bd5000.bd.f5.com
IP Address: 10.105.155.17
Date: Feb 19, 2015
Time: 2:23 PM (PST)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Main Help About
Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...
Statistics
iApp
Local Traffic
Network Map
Virtual Servers
Policies
Profiles
iRules
Pools
Nodes
Monitors
General Properties
Name
Web-Vip
Description
Type
Standard
Source
Destination
Type: Host Network
Address: 20.20.20.5
Service Port
80
HTTP
State
Enabled
Configuration: Basic
Source Address Translation
Auto Map
Content Rewrite
Rewrite Profile
None
HTML Profile
None
Acceleration
Rate Class
None
OneConnect Profile
None
NTLM Conn Pool
None
HTTP Compression Profile
None
Web Acceleration Profile
None
SPDY Profile
None
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
_sys_auth_ssl_crldp
_sys_auth_ssl_ocsp
_sys_https_redirect
Up
Down
Policies
Enabled
Available
/Common
_sys_CEC_video_policy
Default Pool
WebServerPool
Default Persistence Profile
None
Fallback Persistence Profile
None
Cancel
Repeat
Finished

The image has been cropped to highlight the specific configuration.

1. In the upper-right corner of the screen, click the **Create** button.
2. Under **General Properties** in the **Name** field, we will provide a unique name for the web application. In this case, we used **App-Vip**.
3. In the **Destination Address** field, enter the IP Address **172.16.1.5**.
4. For **Service Port** use the HTTP standard port **80**.
5. Under **Configuration**, select **Auto Map** for the **Source Address Translation**.
6. Under **Resources**, Select **AppServerPool** from the dropdown box.
7. Again, click **Finished** to continue to configure the application tier Virtual Server.

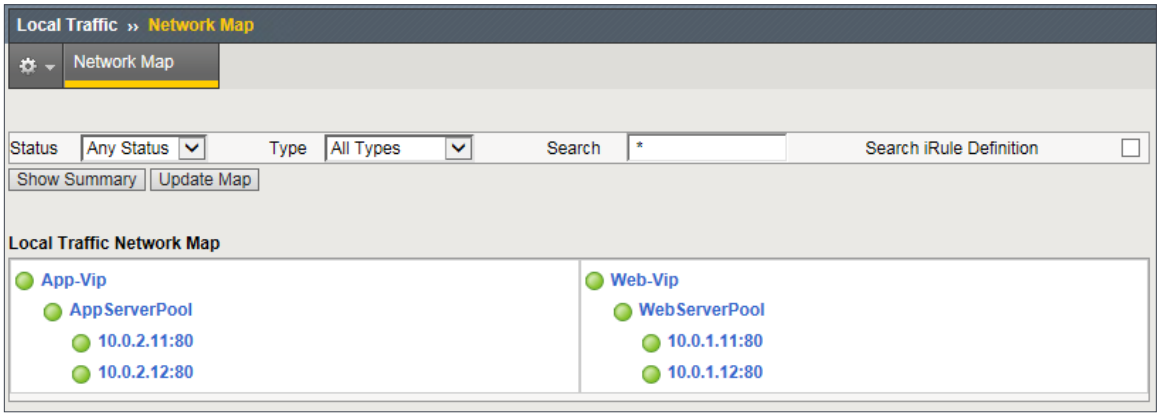
When finished, the virtual server list ought to look similar to the one shown below. The green status icons indicating that all systems are go with the validation application and the virtual servers and the associated pools are reachable and healthy.



Validation

The web tier virtual server should now be available and accepting application traffic on port 80 (HTTP).

On the Main tab, expand **Local Traffic** and then click **Network Map** to display the overall health of the applications and their associated resources.



Any web browser can be used to test the application itself by typing **http://20.20.20.5** to send a request to the virtual server. A simple Apache web server can be installed on the Web Tier to validate.

This concludes the validation of the *Parallel to DLR using VLANs with BIG-IP Physical Appliances* deployment scenario.

Topology 3: One-Arm Connected Using VXLAN Overlays with BIG-IP Virtual Edition

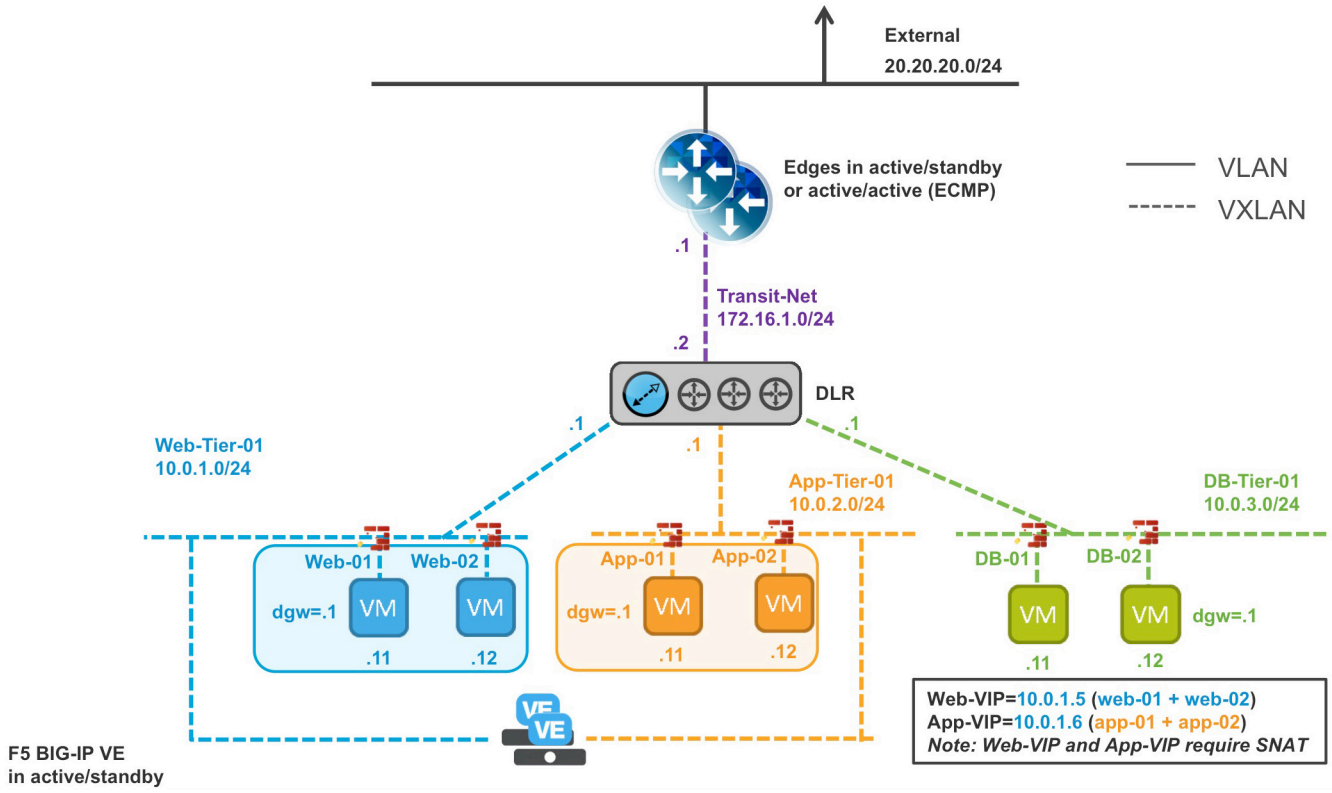


Figure 8. BIG-IP Virtual Edition in one-arm topology within VXLAN environment

The third deployment scenario utilizes a topology that connects a BIG-IP virtual edition's interfaces into the local overlay networks. This allows application-specific optimizations and load balancing decisions to take place within the local overlay network segment. Application specific security policies are applied, from layer 4 through layer 7, within the overlay networks. Traditional east-west traffic between tiers traverses the BIG-IP device for highly available application services.

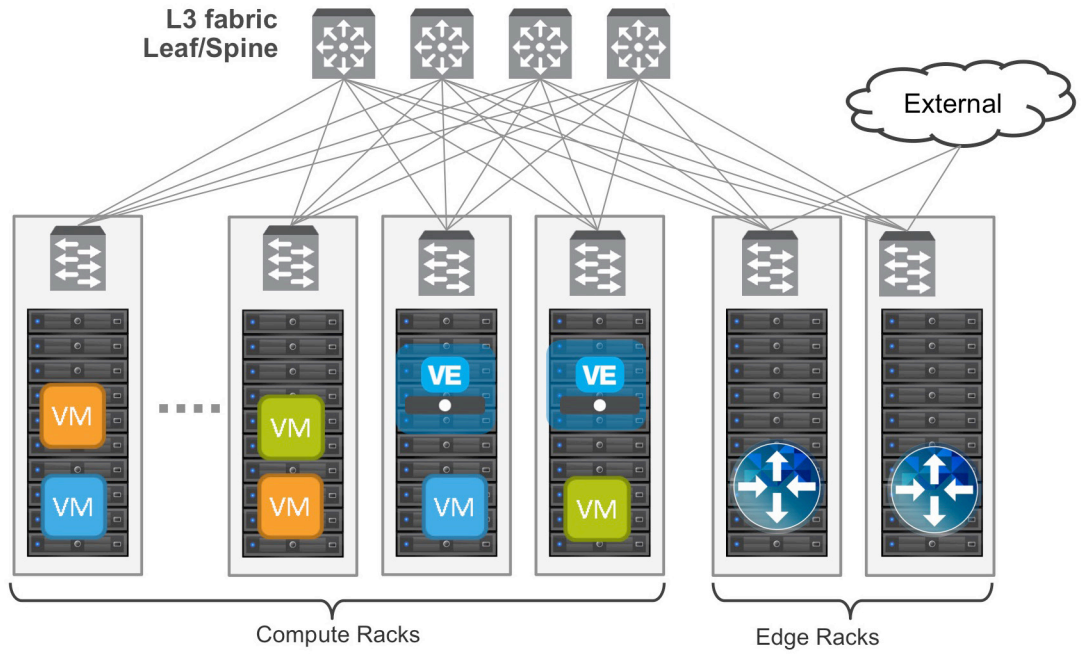


Figure 9. add caption

Implementation Infrastructure

In the validation environment, several ESXi clusters are in use. Some of the clusters are NSX-enabled clusters and some are not.

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 10: the USSJ-55-Management Cluster and the USSJ-55-Computer Cluster. While this is a smaller representation of a typical data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 9.

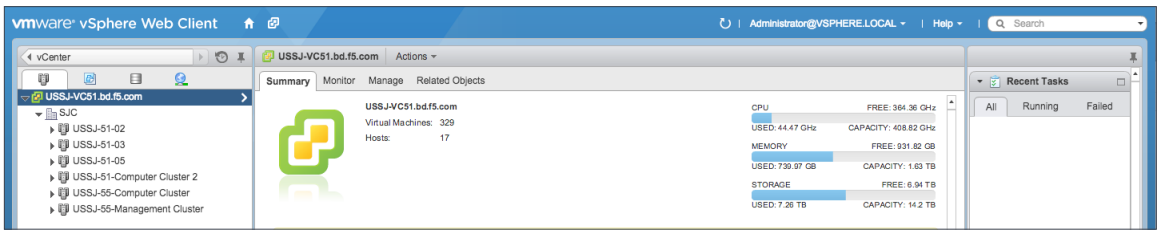


Figure 10. vSphere console

In accordance with best practices, edge and compute ESXi hosts are physically and logically separated from one another. Virtual BIG-IP devices will be deployed within the virtual environment while the VMware infrastructure consisting of vCenter, NSX manager, and the NSX Edge Services Gateways will be installed in the management racks.

The virtual machines used as Web (Web), Application (App), and Database (DB) servers will be running on ESXi hosts in the compute cluster. To better understand data traffic flows for this deployment scenario topology, examine the *VMWare NSX for vSphere (NSX-V) and BIG-IP Design Guide*.

Prerequisites

Referencing the diagram in Figure 8, the BIG-IP Virtual Edition requires connectivity for three logical interfaces. One interface is used for management of the device and the other two are used for all production traffic. The two VLANs, Web-Tier-01 and App-Tier-01, each have one of the logical interfaces in a one-arm configuration attached to the segment. The VLAN numbers, the VXLAN Segment IDs, and the IP addressing scheme can be tailored to your environment.

- Physical network infrastructure switches connected to the ESXi servers and are configured to support 802.1Q tagging and allow the appropriate VLANs.
- ESXi hosts will need to be configured with the appropriate distributed port groups and virtual switches.

Name	802.1Q VLAN ID
External	20
VLAN128-untagged	128
dvs_VL155_NSXIPPool	155

Table 11. VLAN tags for configuration on distributed virtual switch and physical switches

Note: *In our environment, we put the F5 BIG-IP management interface on the VLAN128-untaggd network so that we could obtain clear web GUI screenshots from our web browser client on that network. Generally, you would want to put the management interface on the same network as the NSX manager and other management components, which happens to be the dvs_VL155_NSXIPPool PortGroup network in our environment.*

Name	Transport Zone	Segment ID	Control Plane Mode
App-Tier-01	TransportZone1	5000	Unicast
DB-Tier-01	TransportZone1	5002	Unicast
Web-Tier-01	TransportZone1	5003	Unicast
TransitNet-1	TransportZone1	5013	Unicast

Table 12. Logical switch configuration

Network Segments

Two types of network segments are utilized in this topology. Traditional 802.1Q VLAN network segments and VXLAN overlay segments. Within NSX we Created IP pools that will be used by the web, app, and DB virtual machines.

802.1Q VLAN segments

VLAN 20 External is the VLAN used for external connectivity. The 20.20.20.0/24 IP subnet range is configured on this VLAN.

VLAN128-untagged is the VLAN used as for out-of-band management of the virtual BIG-IP appliances. The 172.16.1.0/24 IP subnet range is configured on this VLAN.

VLAN 155 dvs_VL155_NSXIPPool *(not shown)* is for management connectivity. The 10.105.155.0/24 IP subnet range is configured on this VLAN.

VXLAN segments

The web, app, and DB tier virtual machines are all provisioned and connected to VXLANs.

VXLAN 5000 App-Tier-01 is the Segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.

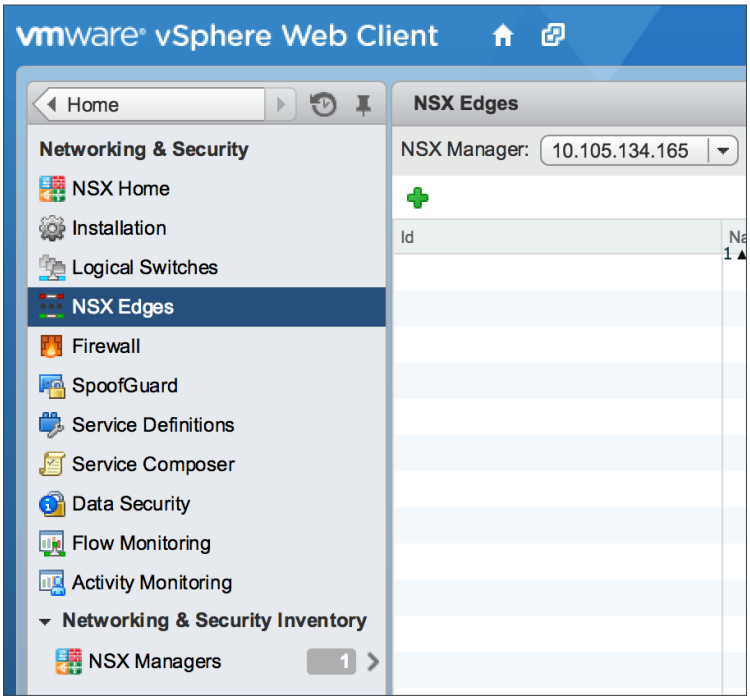
VXLAN 5002 DB-Tier-01 is the Segment ID used for the green DB Connectivity. The 10.0.3.0/24 IP subnet range is configured on this VXLAN.

VXLAN 5003 Web-Tier-01 is the Segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.

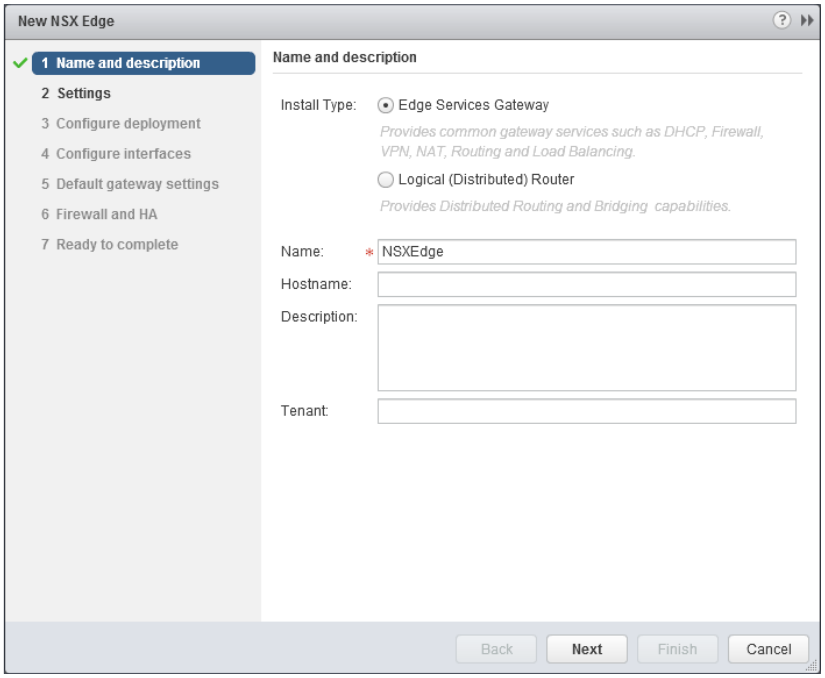
VXLAN 5013 TransitNet-1 is the VXLAN Segment ID used for the transport zone between the DLR and the NSX Edge.

NSX Edge Configuration

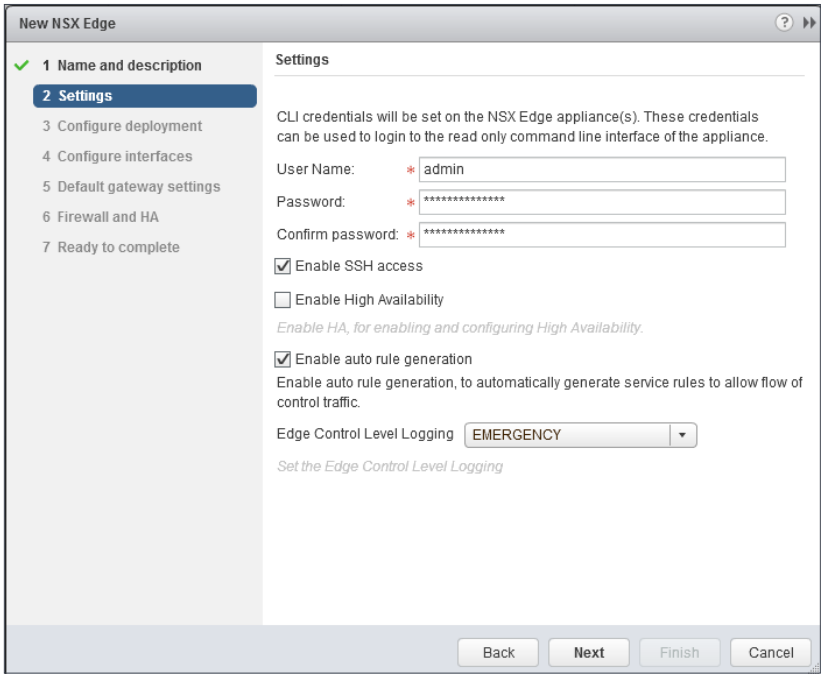
In the **vSphere Web Client** console, begin by navigating to **Networking & Security** in the left column. Under **Networking and Security**, choose **NSX Edges** and then click the green plus symbol (+).



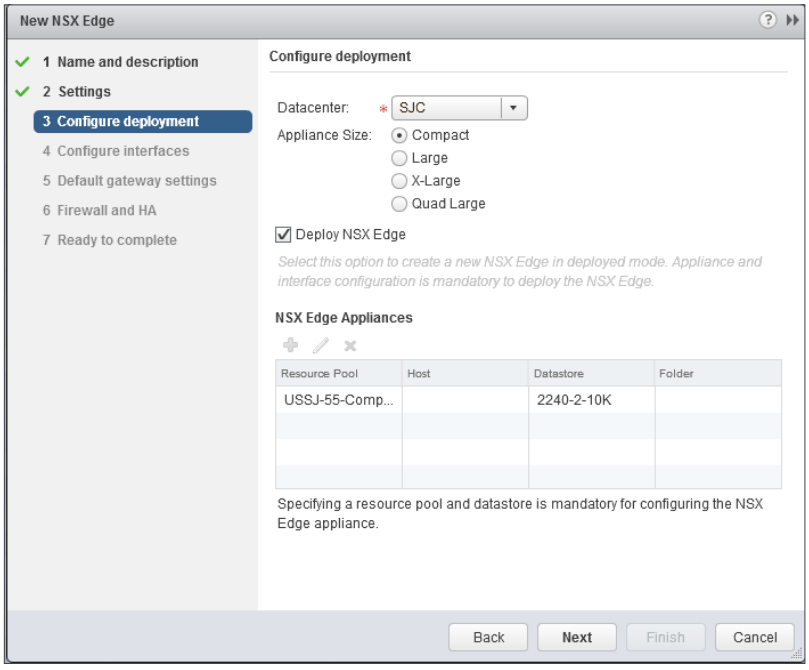
2. Select **Edge Services Gateway** as the **Install Type** and provide a name for the device, then click **Next**.



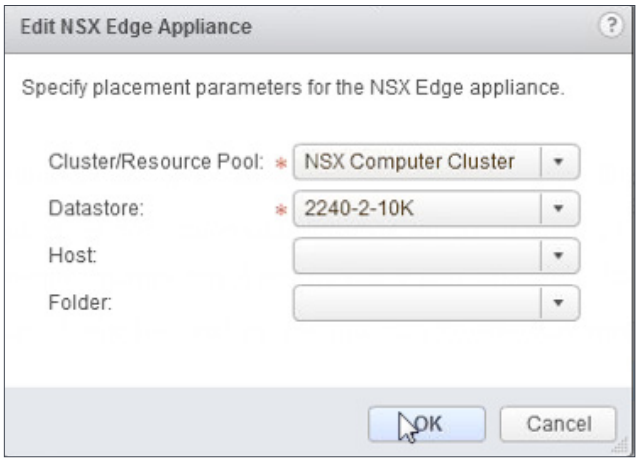
3. Under **Settings**, click **Enable SSH access** and provide a username and password for the Edge Services Gateway. Click **Next** to proceed.



4. Select the **Datacenter** and **Appliance Size** appropriate for your deployment, and check the **Deploy NSX Edge** checkbox. Then click the green plus symbol (+) under NSX Edge Appliances.



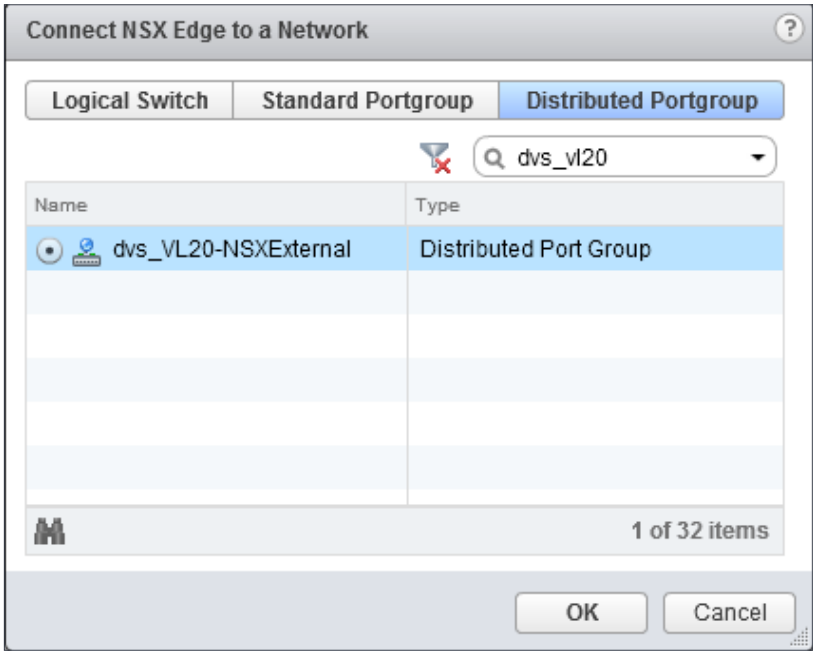
5. Selecting the green plus symbol in the **Configure deployment** section will display the options in the screenshot below. Choose the appropriate Cluster/resource pool (**NSX Computer Cluster**), and Datastore (**2240-2-10K**). The host selection is optional. Ensure the NSX Edge is deployed in the Management cluster. Click **OK** to complete and **Next** to continue.



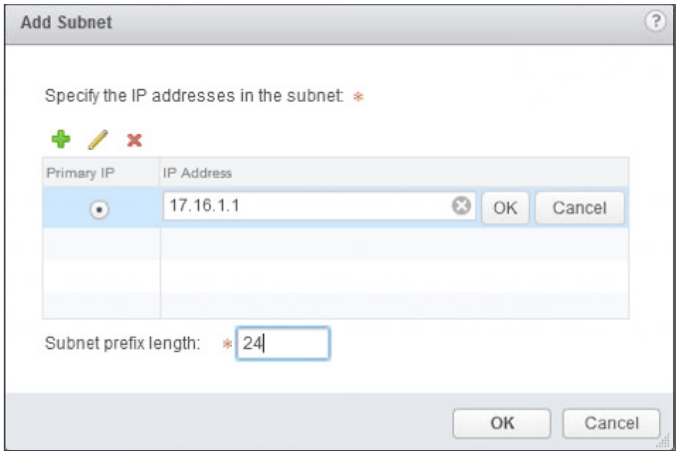
6. Configure Interfaces for the NSX Edge. For each of the three interfaces required for this deployment scenario, configure the appropriate subnets and switch type according to the settings shown in Table 13. Click the green plus symbol (+) to display the Add NSX Edge Interface dialog box.

Network Name	Type	Network	Interface IP /Subnet Prefix
External	Uplink	Distributed Port Group	20.20.20.2/24
TransitNet-1	Internal	Logical Switch	172.16.1.1/24

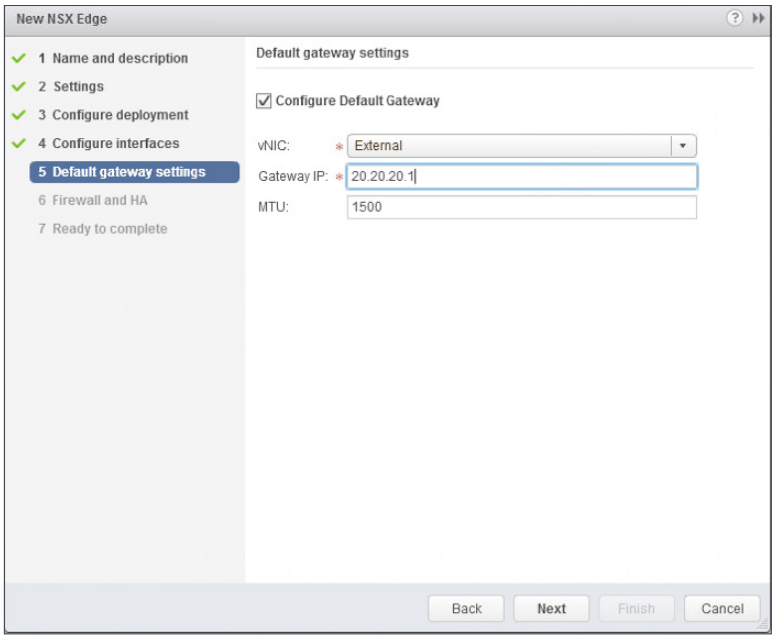
Table 13. NSX Edge network interfaces



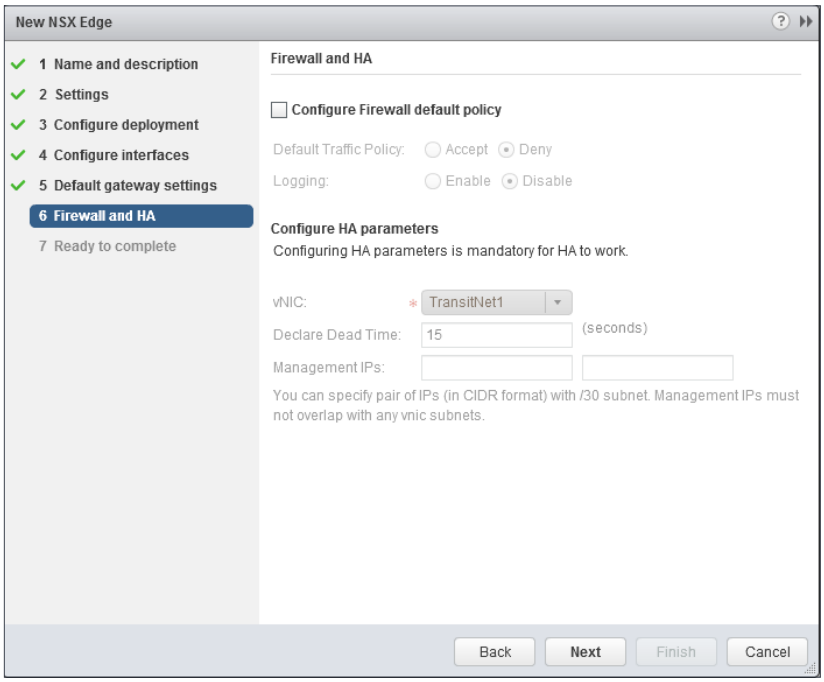
7. Once the network is chosen, select the green plus symbol (+) under **Configure Subnets** in order to add the appropriate **IP address** and **subnet prefix length** to the interface.



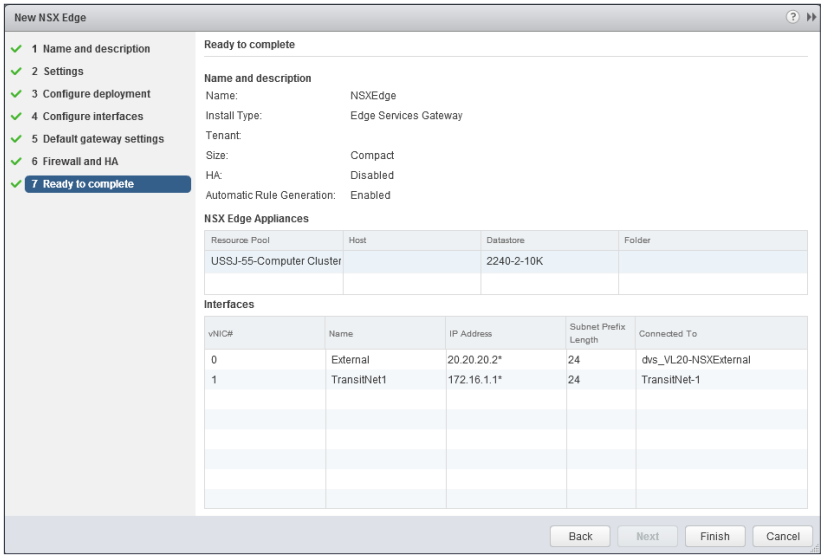
8. Once the interface settings are completed, the next step is to configure the Default gateway settings. The default gateway is our data center backbone router with the IP address of 20.20.20.1 on External vNIC we configured under the interface settings. Use the default MTU parameter unless the network is using an MTU of a different size, such as jumbo frames. Configuring a non-standard MTU that is inconsistent can lead to unnecessary fragmentation of packets or black-holing of some traffic. Select **Next** to proceed.



9. Firewall and HA settings can be left as default.



10. Select **Finish** to complete the deployment of the NSX Edge.



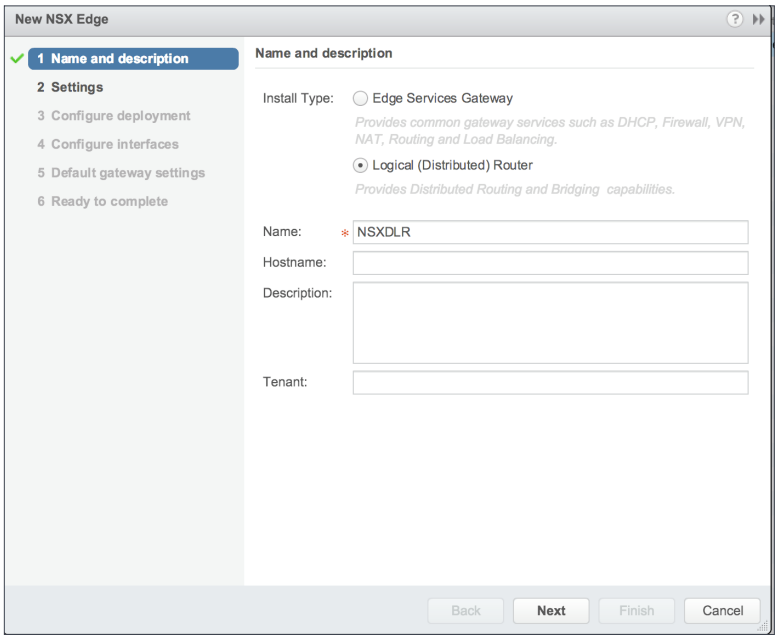
Create and Deploy DLR

Within VMWare NSX the Distributed Logical Router (DLR) provides an optimized way of handling east-west traffic within the data center. East-west traffic is communication between virtual machines or other resources on different subnets within a data center. As east-west traffic demand increases within the data center, the distributed architecture allows for optimized routing between VXLAN segments.

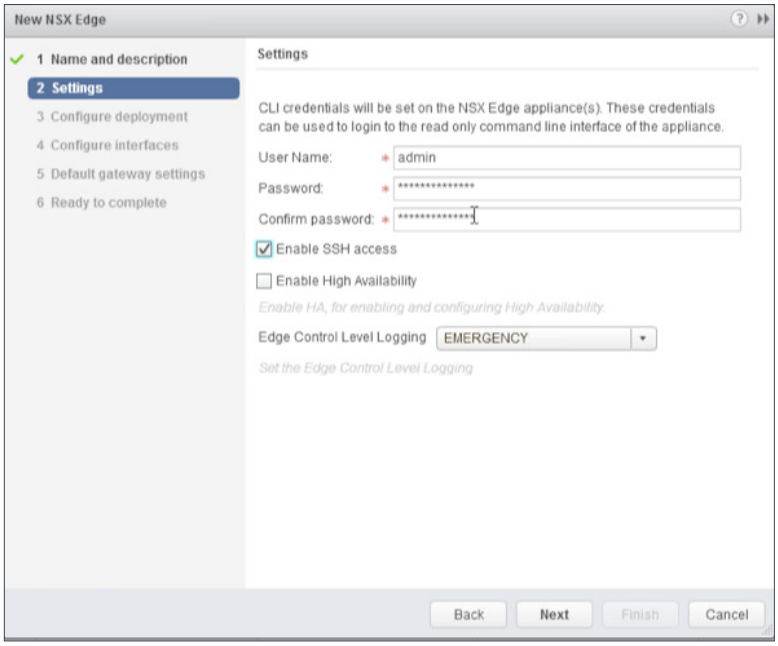
(Note that VMware uses DLR and LDR—Logical (Distributed) Router—synonymously.)

1. Return to the **vSphere Web Client** console and choose **Networking & Security** in the left column, then choose **NSX Edges** and click the green plus symbol (+).

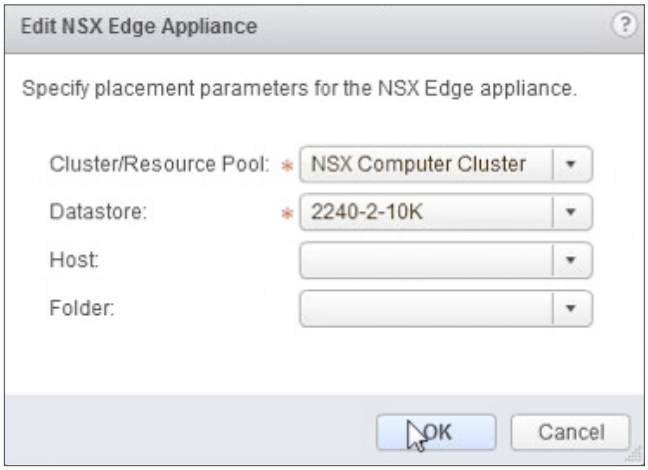
2. Select **Logical (Distributed) Router** as the **Install Type** and provide a name for the device and then click **Next**.



3. Under **Settings**, select **Enable SSH access** and provide a username and password for the Edge Services Gateway. Select **Next**.

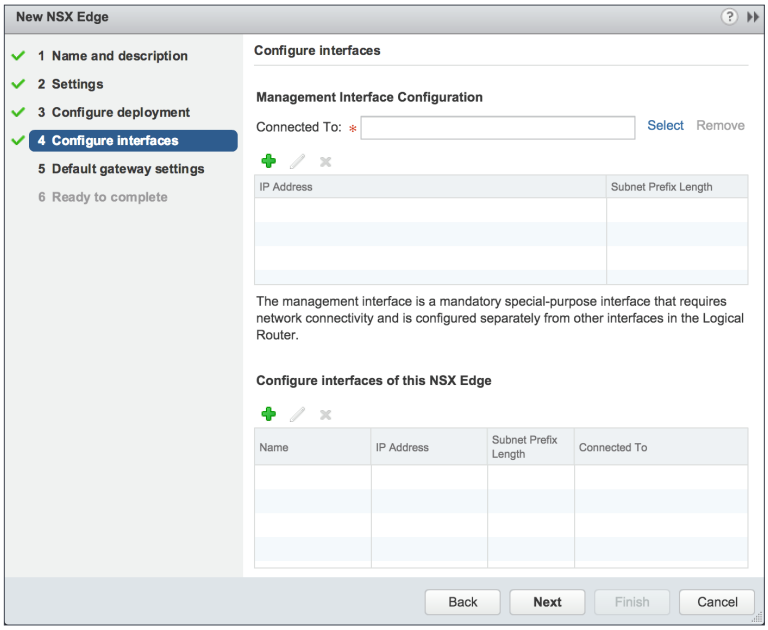


4. Selecting the green plus symbol in the Configure Deployment will provide you with the options in the screenshot below. Choose the appropriate Cluster/resource pool (**NSX Computer Cluster**), and Datastore (**2240-2-10K**). The host selection is optional. Ensure the NSX DLR is deployed in the NSX Computer Cluster. Select **OK** to complete and **Next** to continue.

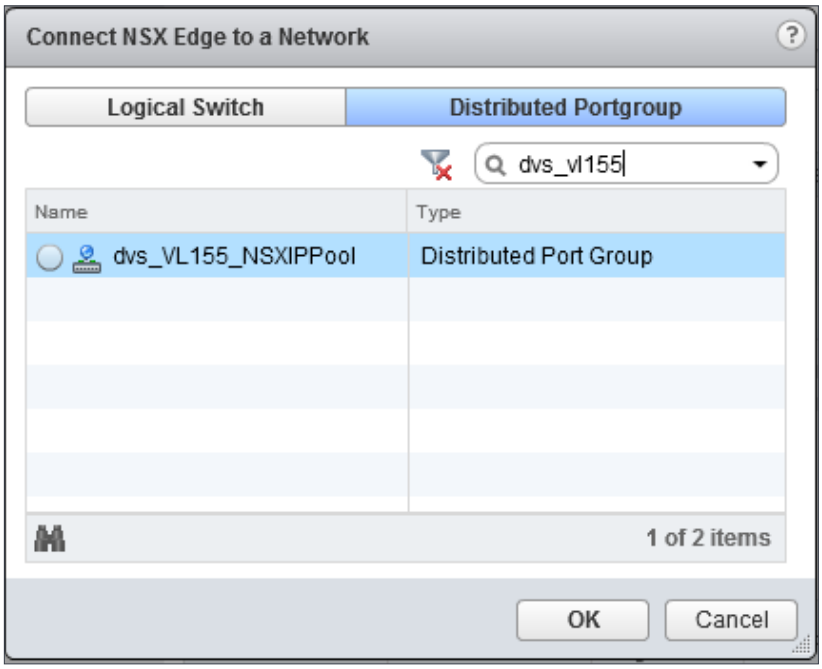


5. Configure Interfaces for the DLR.

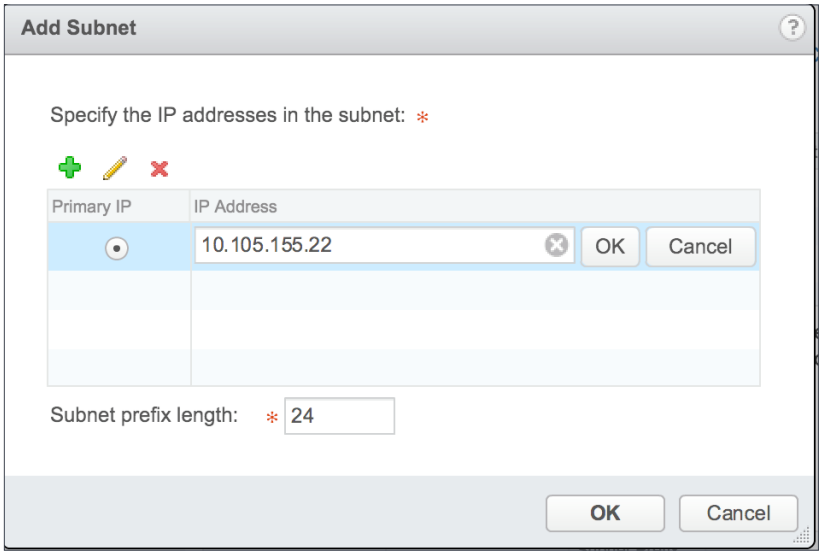
   a. First configure the management interface for the DLR. Under **Management Interface Configuration**, Click **Select** to the right of the **Connected To** field.



b. In this case, the management interface should be connected to a distributed port group that is connected to the shared management VLAN.



c. Click the green plus symbol (+) to specify a fixed IP Address and subnet prefix length in the management network.

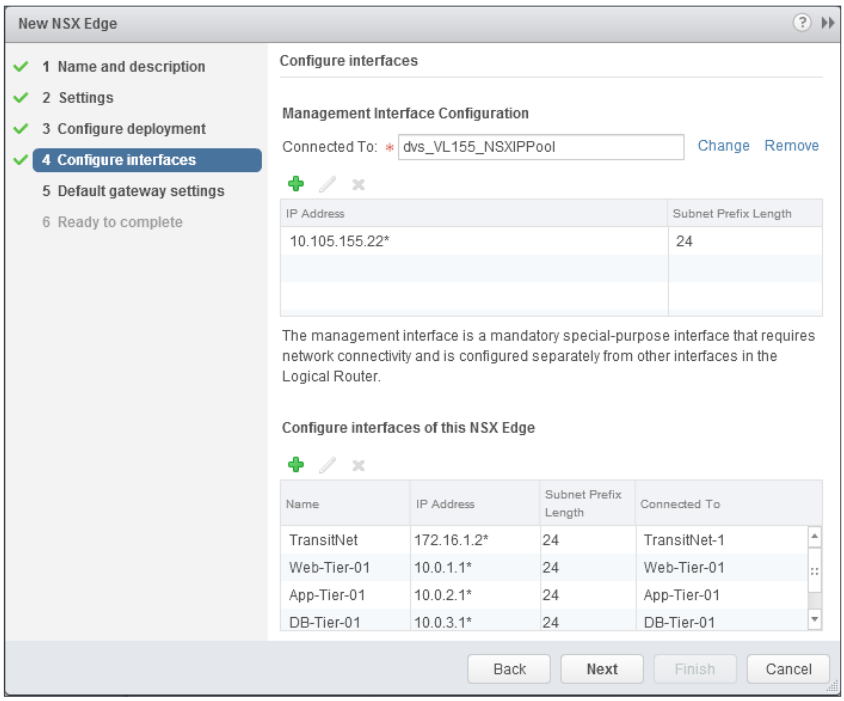


6. For each of the four interfaces required for this deployment scenario, configure the appropriate subnets and switch type according to the table below. Select the green plus symbol under Configure Interfaces of this NSX Edge to display the Add Interface dialog box.

Network Name	Connected To	Type	Network	Interface IP /Subnet Prefix
TransitNet	TransitNet-1	Uplink	Logical Switch	172.16.1.2/24
Web-Tier-01	Web-Tier-01	Internal	Logical Switch	10.0.1.1/24
App-Tier-01	App-Tier-01	Internal	Logical Switch	10.0.2.1/24
DB-Tier-01	DB-Tier-01	Internal	Logical Switch	10.0.3.1/24

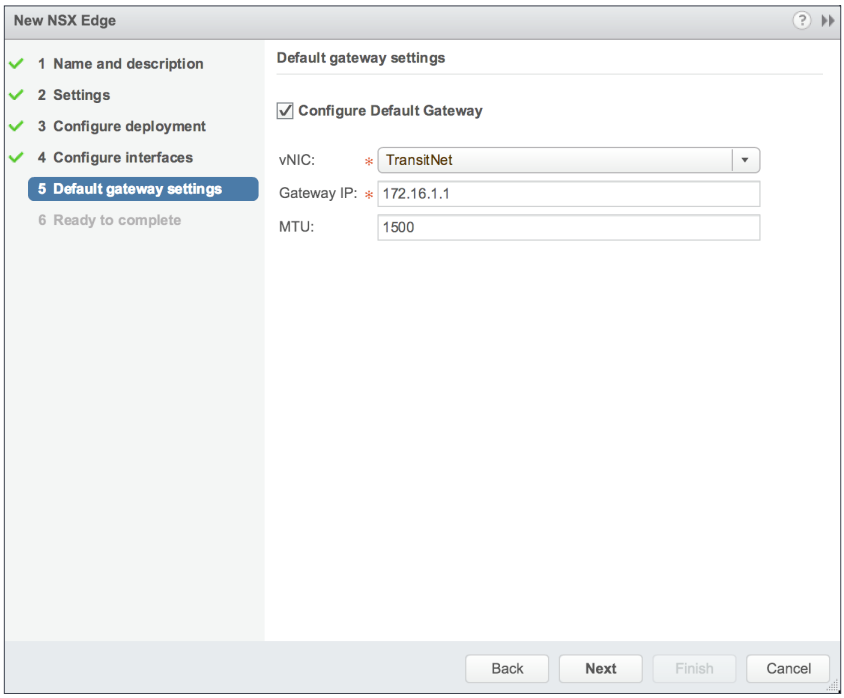
Table 14. NSX distributed logical router Network interfaces

The DLR interface configuration, once complete, should resemble the diagram below. Click Next to continue.

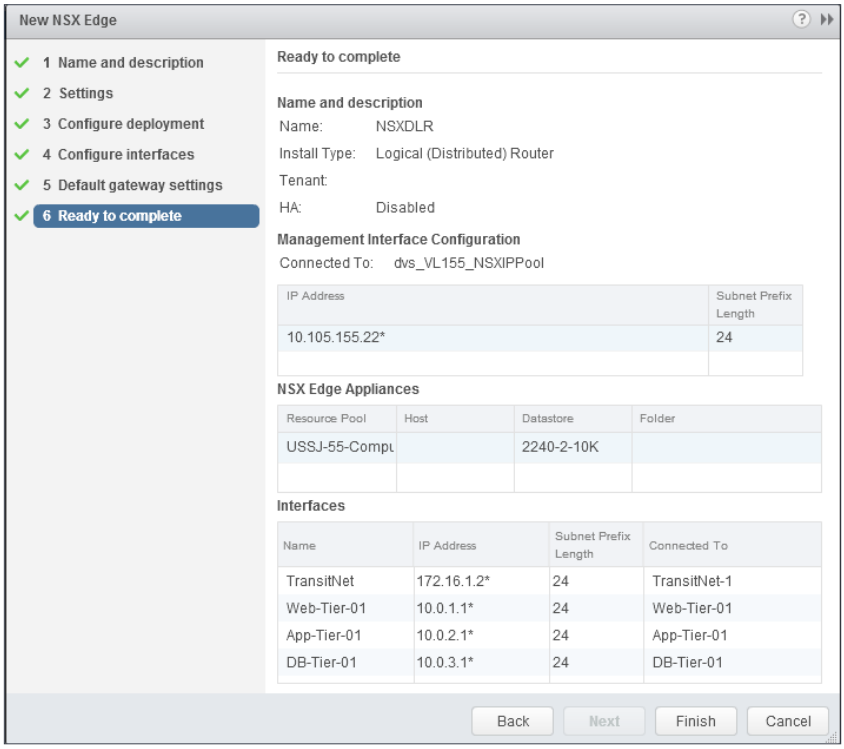


7. With the interface settings complete, the next step is to configure the default gateway settings. The default gateway for the DLR is the data center core router we configured in the previous section across the transit segment Transit-Net.

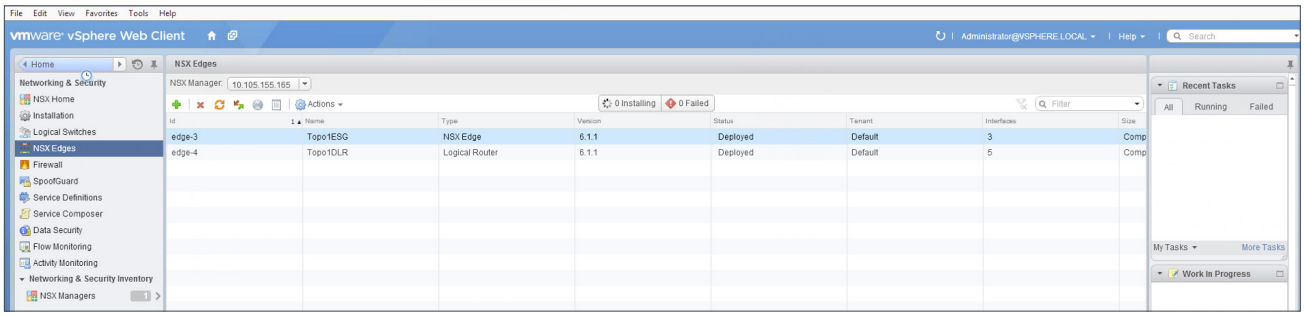
Select the **TransitNet** vNIC and provide the Gateway IP address of the NSX Edge. In this configuration, it is **172.16.1.1**. Click **Next** to proceed.



8. Click **Ready** to complete to view the configuration and then click **Finish** to deploy the DLR. Depending on the number of ESXi hosts, it may take some time for the DLR deployment to complete.



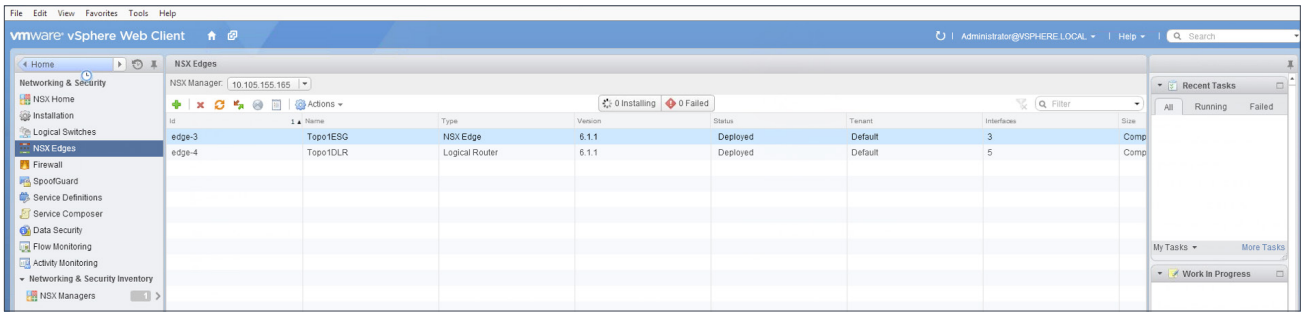
9. Once complete, the vSphere NSX Edges configuration should resemble the image below.



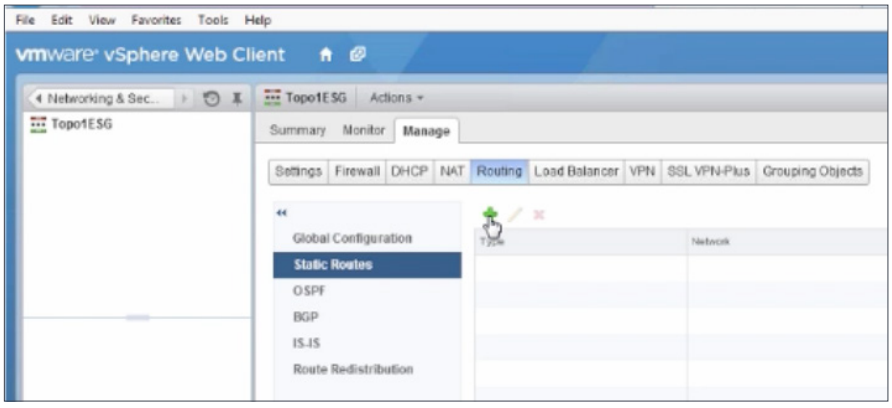
NSX Edge Static Routing Configuration

For this deployment scenario, static routing is configured to allow the NSX Edge to forward packets into the different tiered networks via the DLR. The default gateway configuration on both the NSX Edge and the DLR ensures packets find their way out to external networks. This configuration is also required to ensure that traffic coming from the external networks finds its way into the networks.

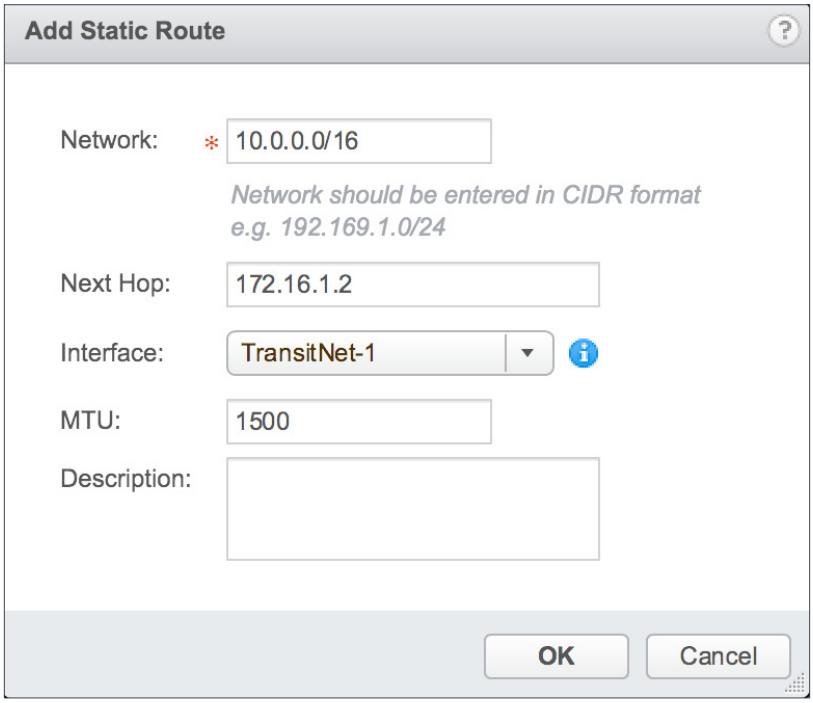
1. Double-click on the NSX Edge you configured in the first section.



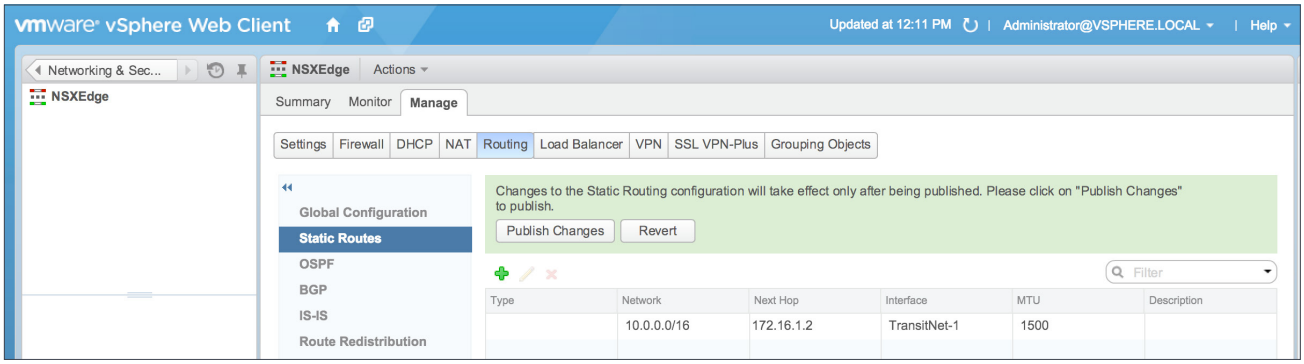
2. The configuration screen below should now be displayed. Click the **Manage** tab and then click the **Routing** sub-tab. Click **Static Routes**, and then click the green plus symbol (+) to display the Add Static Route configuration dialog box.



3. Provide an internal summary route that points the NSX Edge to the TransitNet-2 IP Address of the DLR interface. In this case, a summary of 10.0.0.0/16 is pointed internally to the DLR IP address of **172.16.2.2**.



4. Once complete, select **OK** to continue.



5. Click **Publish Changes** to push the updated routing information to the NSX Edge.

BIG-IP Appliance Configuration

The validation of this topology includes a pair of BIG-IP Virtual Edition appliances deployed in the same vSphere cluster. For more information on deploying a BIG-IP Virtual Edition through vSphere, F5 provides the *BIG-IP Virtual Edition Setup Guide for VMWare ESXi*, located at the following link.

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-setup-vmware-esxi-11-5-0.html

For production deployments, F5 recommends that two BIG-IP devices be configured in an HA configuration. For additional information on high-availability configurations, consult the *BIG-IP Device Service Clustering: Administration* manual for the appliance version you are using.

The manual for BIG-IP version 11.6, can be found here.

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-device-service-clustering-admin-11-6-0.html

The base network configuration consists of provisioning the proper port group to the management interface's network adapter and VXLAN virtual switches to the BIG-IP virtual appliances' network adapters for the data interfaces. Next, you'll configure the appropriate VLANs and assign them to the BIG-IP interfaces. And last, you'll create the appropriate self IP addresses for each of the network segments.

Prerequisites

- BIG-IP Virtual Editions have been deployed in the same ESXi cluster on separate hosts with appropriate anti-affinity DRS rules in place.
- Licenses have been applied and activated.
- Appropriate provisioning of resources is complete.

For information on how to perform these installation and basic setup steps, refer to http://support.f5.com and consult the appropriate implementation guide for your version and model.

For this validation, we've labeled the BIG-IP Virtual Edition appliances as NSXBigIP and NSXBigIP2.

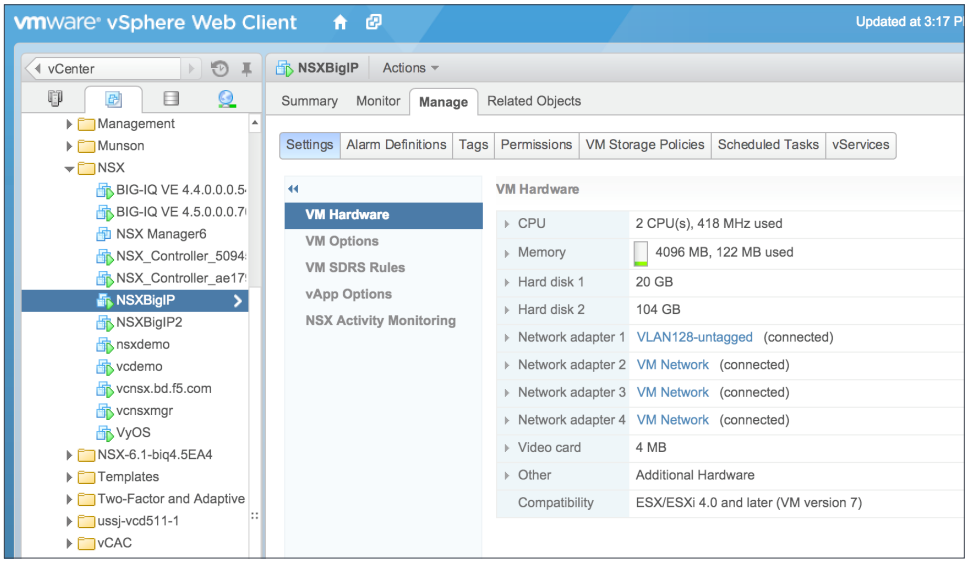
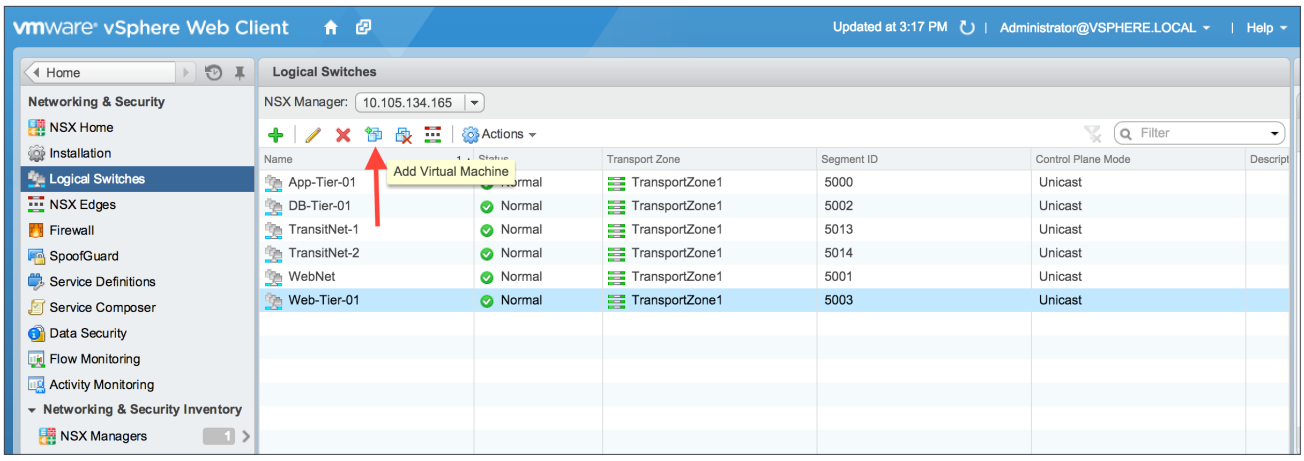


Figure 11. vSphere display of deployed BIG-IP Virtual Edition

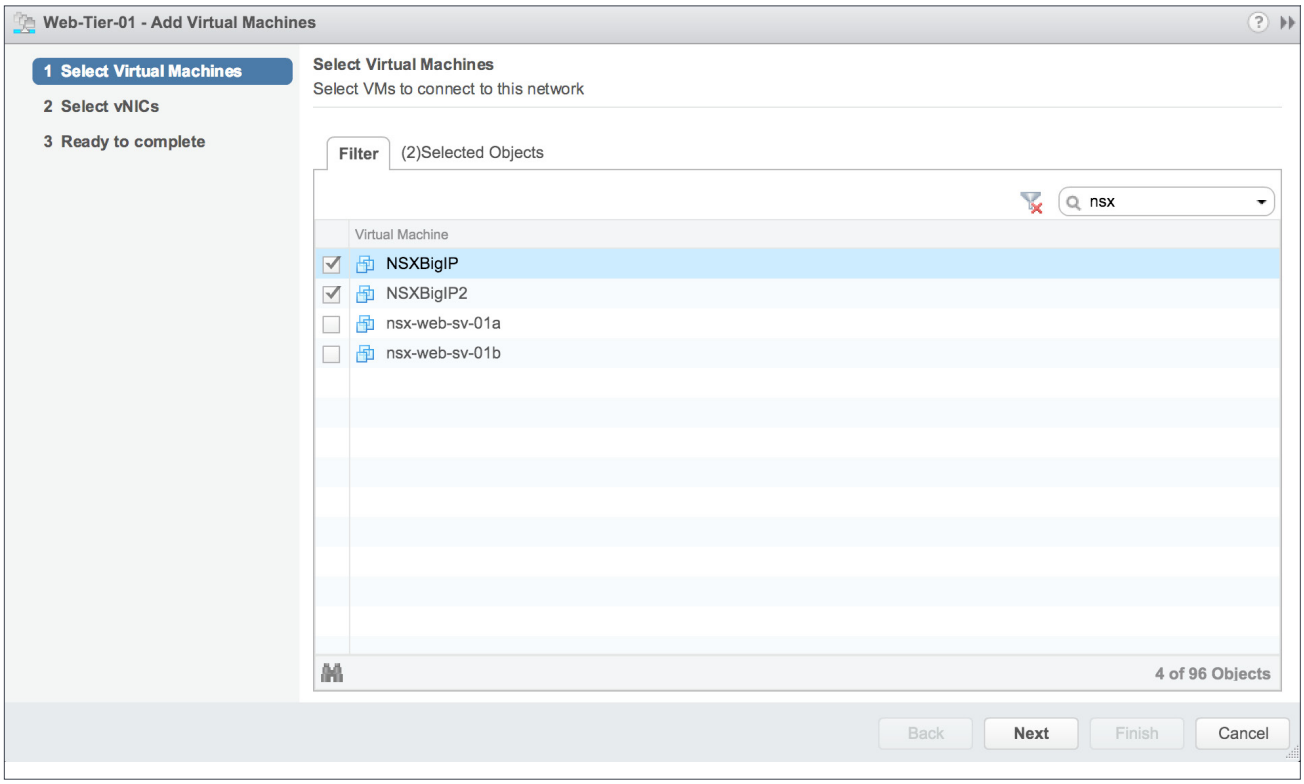
Provision BIG-IP Network Adapters in vSphere

For this topology, the BIG-IP requires four network adapters. The first is for management of the devices, the second two are for data traffic, and the fourth is for HA information and configuration syncing between the two BIG-IP virtual appliances.

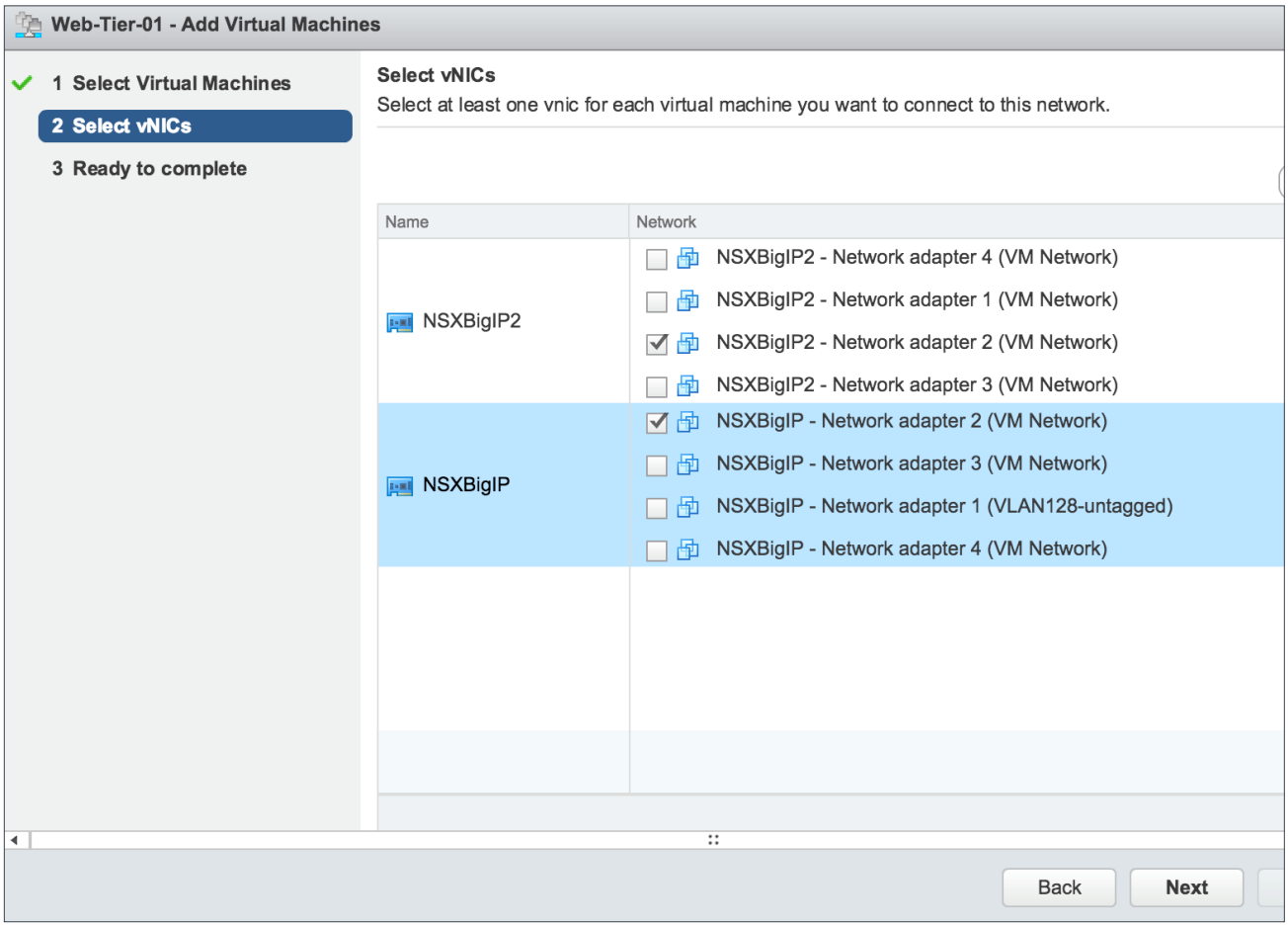
1. Return to the **vSphere Web Client** console and choose to **Networking & Security** in the left column. Under **Networking and Security**, choose **Logical Switches**. Highlight the **Web-Tier-01** logical switch, and then click the **Add Virtual Machine** icon (indicated by the red arrow in the figure below).



2. Select the two BIG-IP virtual appliances **NSXBigIP** and **NSXBigIP2**. Click **Next** to continue.



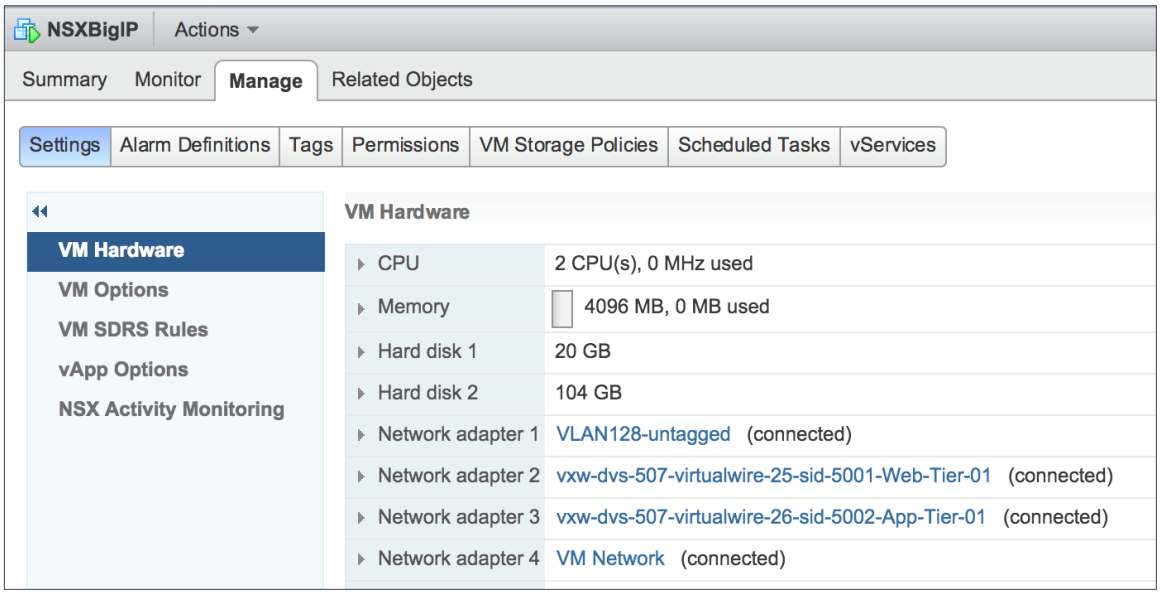
3. Select vNICs. For Web-Tier-01, makes sure to check the checkbox for Network adapter 2 for each of the virtual editions. Click Next to continue, and then click Finish.



4. For the App-Tier-01 logical switch, repeat the same steps, making sure to choose Network adapter 3.

5. In our environment we are using the VM Network PortGroup as the HANet PortGroup and leaving the Network adapter 4 associated with the VM Network PortGroup.

6. When complete, the settings shown under the **Manage** tab for the HA pair of BIG-IP VEs ought to look similar to this.

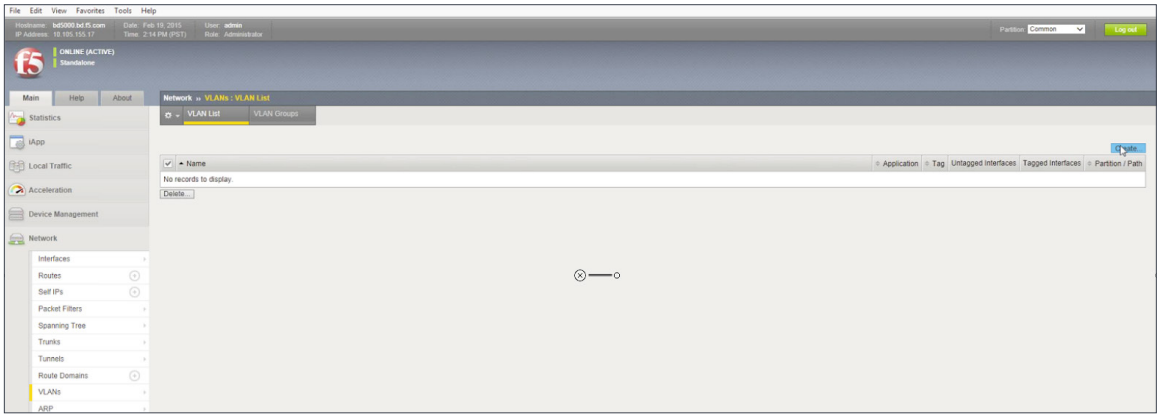


Provision BIG-IP Networking

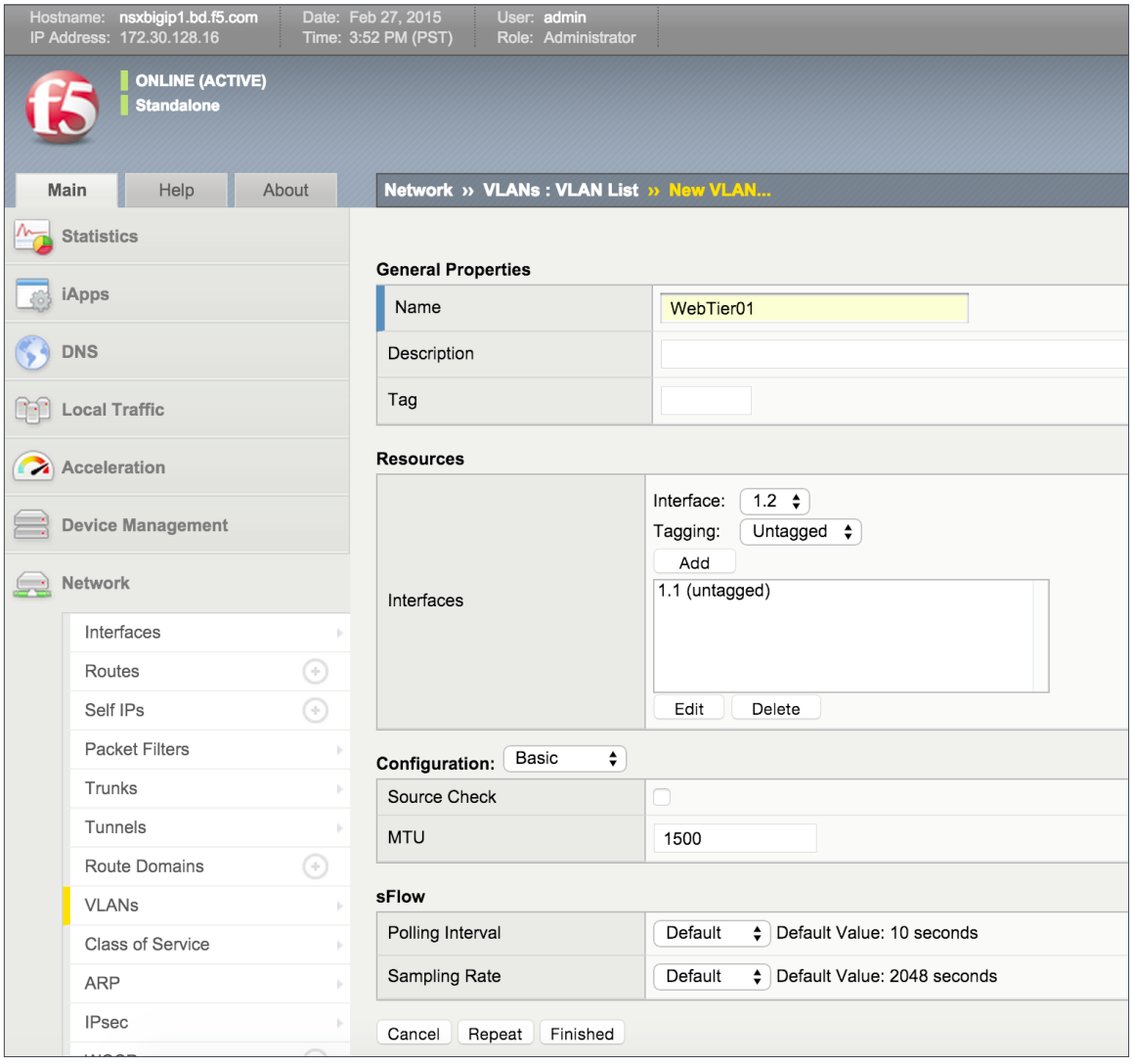
Create VLANs

1. From the **Main** tab of the **BIG-IP Configuration Utility** navigation pane, expand **Network** and then select **VLANs**.

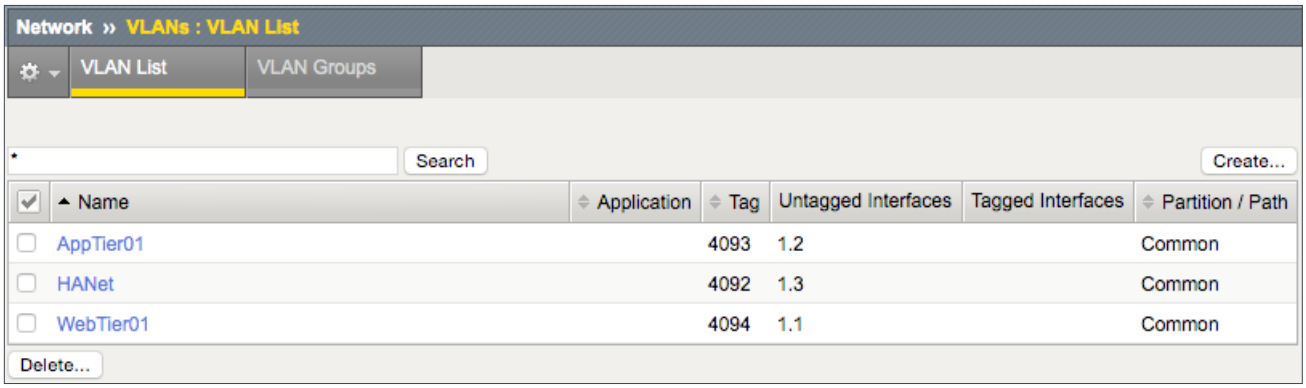
2. In the upper right corner, click the **Create** button.



3. Under **General Properties**, enter a unique name for the VLAN. In this case, we used **WebTier01**.
4. In this scenario, 802.1Q VLAN tagging is not required so no tag value is needed.
5. Under **Resources**, choose **1.1** for the Interface.
6. For **Tagging**, select **Untagged** and then click the **Add** button below it. The screenshot below is what you ought to see after clicking **Add**. Notice that in the **Interfaces** field **1.1(untagged)** is entered.



7. Click **Repeat** to continue.
8. Proceed with creating the application tier network. Type a unique name for the VLAN. In this case, we used **AppTier01**.
9. Tagging is not required, so no Tag value is needed.
10. Select Interface **1.1**.
11. For **Tagging**, select **untagged** and then click the **Add** button below it.
12. Select **Repeat** and return to step 8 for **HANet** to complete the VLAN creation.
13. Click **Finished** to proceed.
14. Validate the VLAN configuration against the image below. The BIG-IP device will use self-generated tags for internal tracking of the VLANs.



Repeat steps 1-13 to create the VLANs on the second appliance, NSXBigIP2.

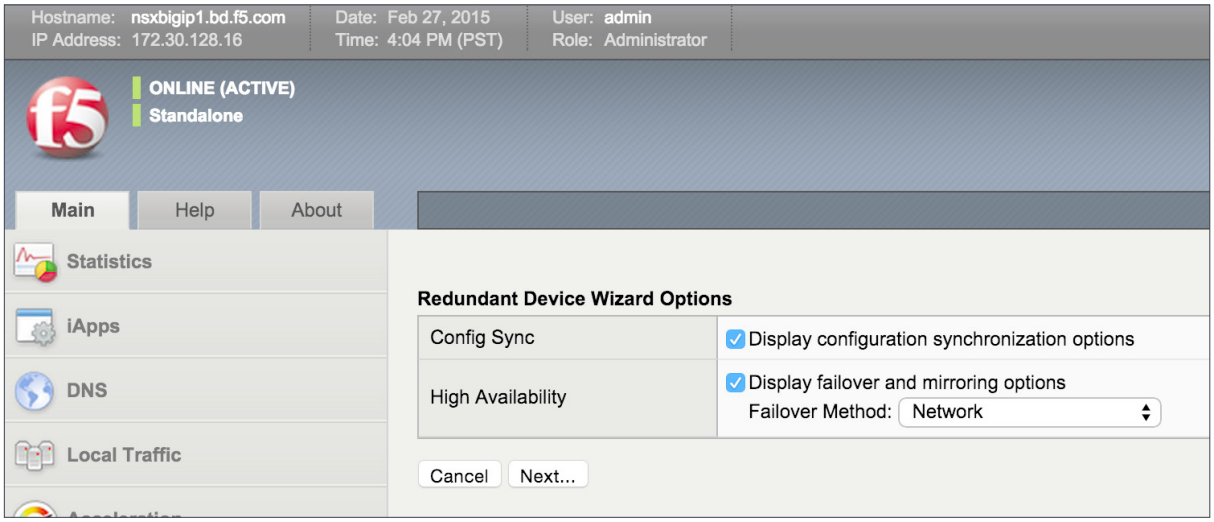
Run Config Sync/HA Utility To Set Up a High Availability Cluster

The Config Sync/HA Utility simplifies the setup of high availability between the two BIG-IP devices. It walks through the configuration of the logical interfaces and other configuration parameters that are required for proper operation.

In an HA configuration, a floating self IP address is created (in addition to the local self IPs) as a shared address that “floats” on whichever device in the cluster is active. This needs to be done for both of the data VLANs WebTier01 and AppTier01, but not for HANet.

1. From the **Main** tab, click **Statistics** and then click **Module Statistics**.
2. Under **Setup Utility**, click **Run Configure Sync/HA Utility**.

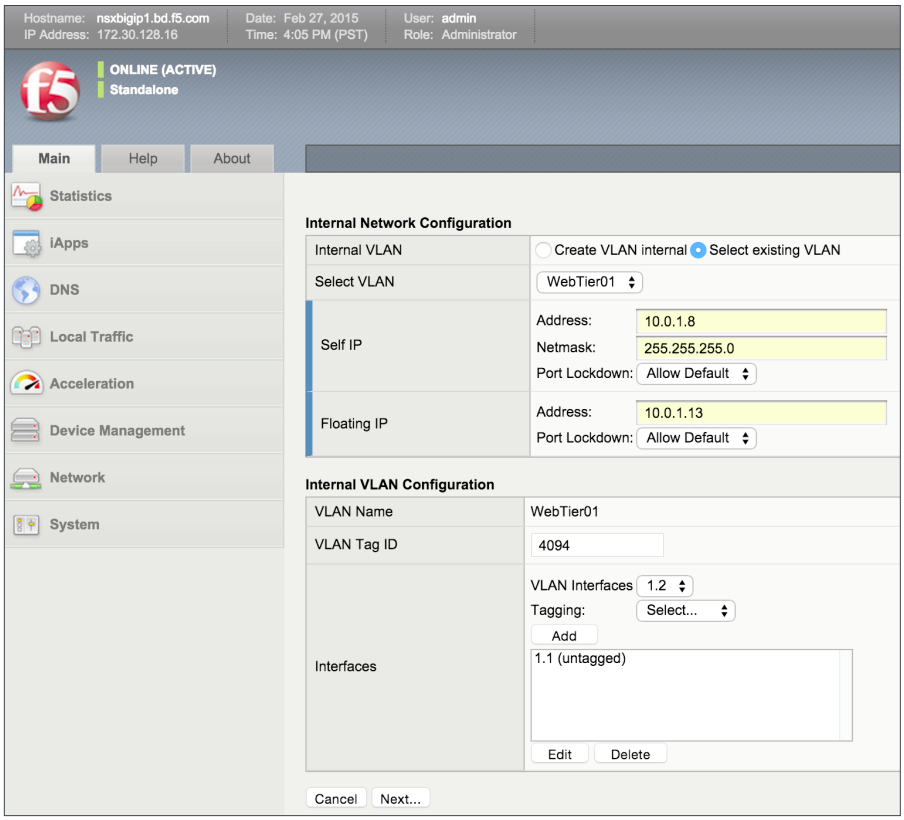
3. Under **Redundant Device Wizard Options**, the default configuration options can be left as shown. Click **Next** to continue.



4. Under **Internal Network Configuration**, choose the following settings

   - Internal VLAN: Select **Existing VLAN**
   - Select VLAN: **WebTier01**
   - Self IP
     - Address: **10.0.1.8**
     - Netmask: **255.255.255.0**
     - Port Lockdown: **Allow Default**
   - Floating IP
     - Address: **10.0.1.13**
     - Port Lockdown: **Allow Default**

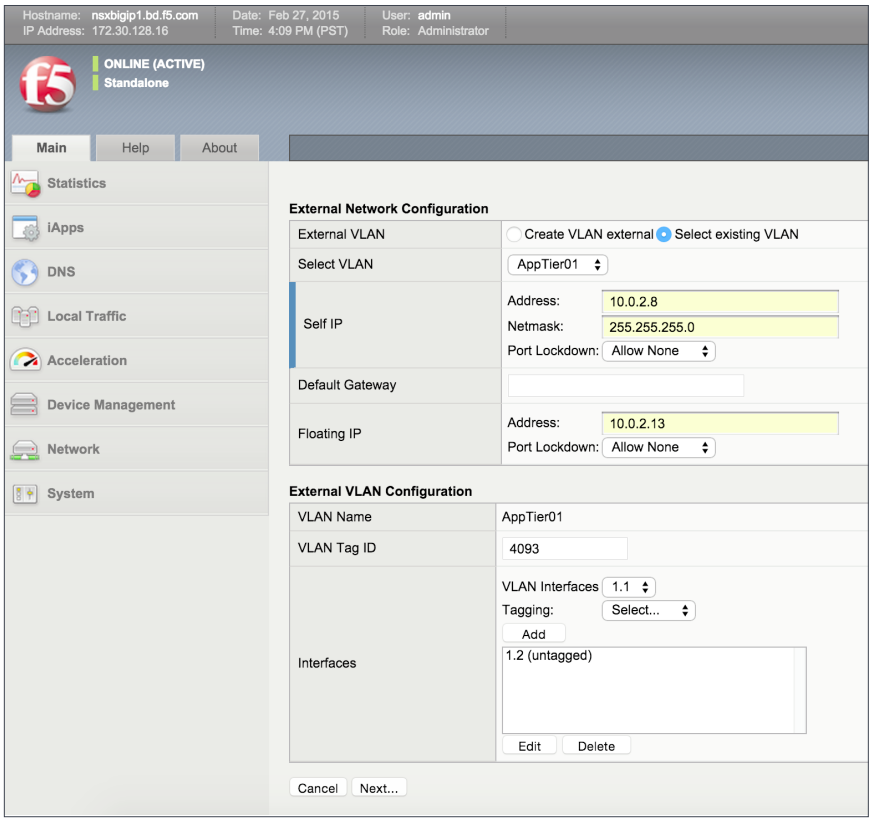
5. Click **Next** to continue.



6. Under **External Network Configuration**, choose the following settings:

   - Internal VLAN: Select **Existing VLAN**
   - Select VLAN: **AppTier01**
   - Self IP
     - Address: **10.0.2.8**
     - Netmask: **255.255.255.0**
     - Port Lockdown: **Allow Default**
   - Floating IP
     - Address **10.0.2.13**
     - Port Lockdown: **Allow Default**

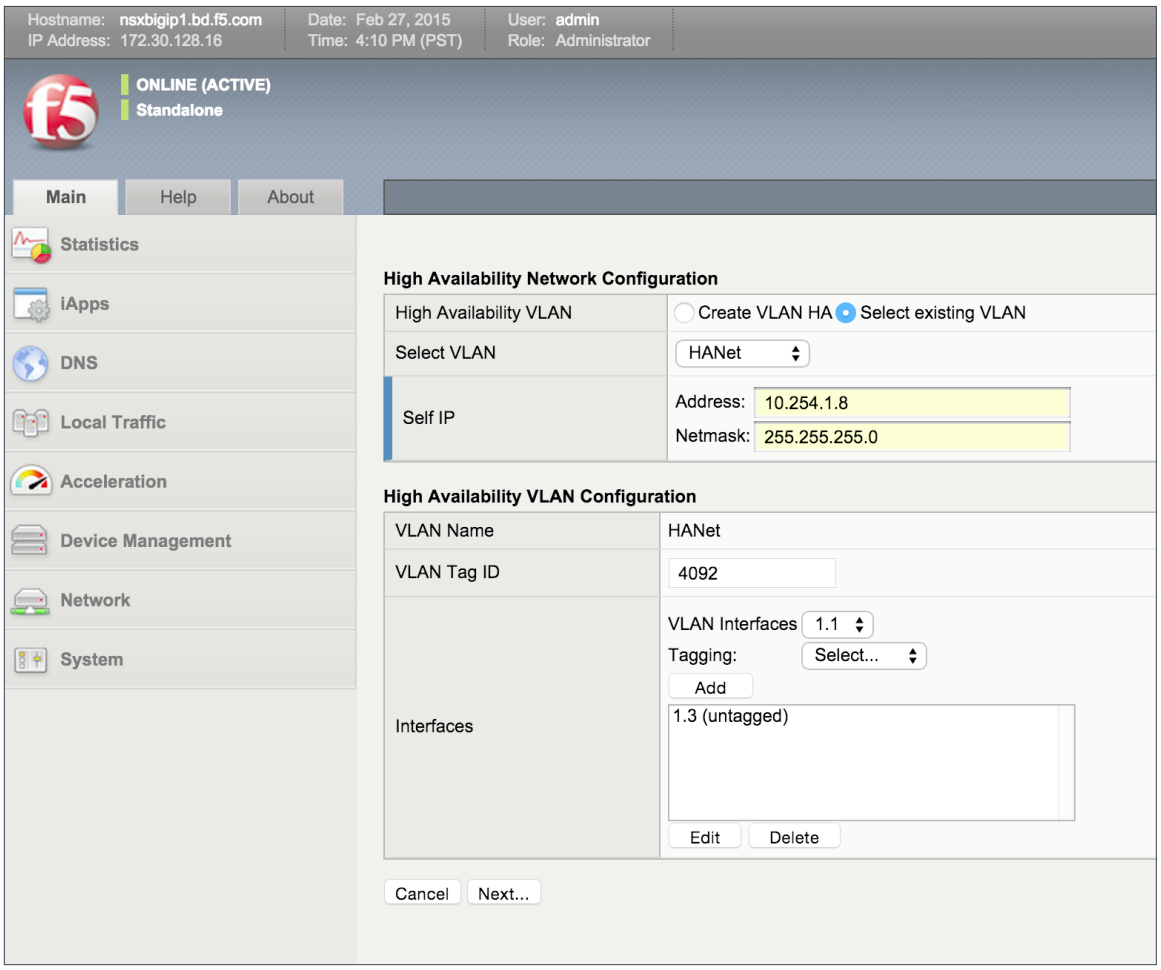
7. Click **Next** to continue.



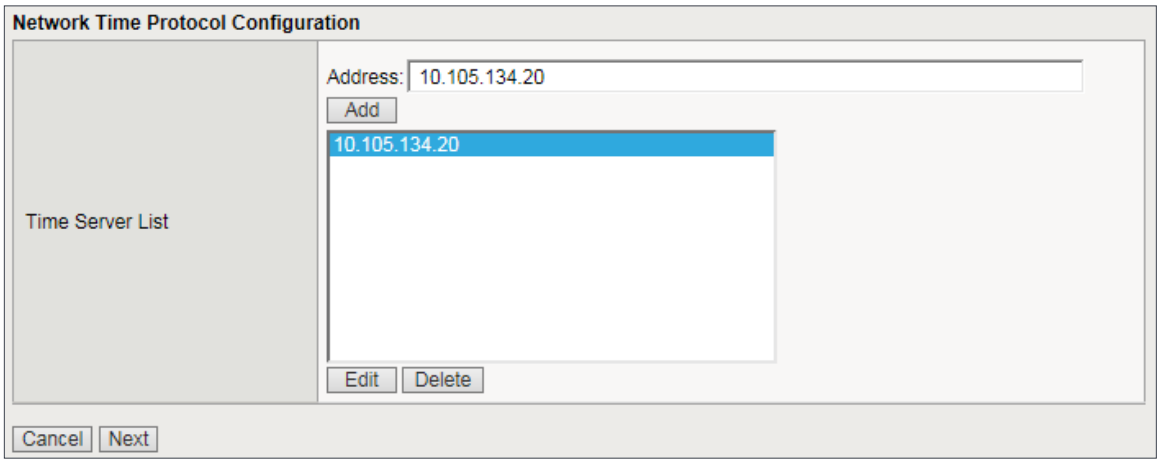
8. Under **High Availability Network Configuration**, choose the following settings:

   - Internal VLAN: **Select Existing VLAN**
   - Select VLAN: **HANet**
   - Self IP
     - Address: **10.254.1.8**
     - Netmask: **255.255.255.0**
     - Port Lockdown: **Allow Default**

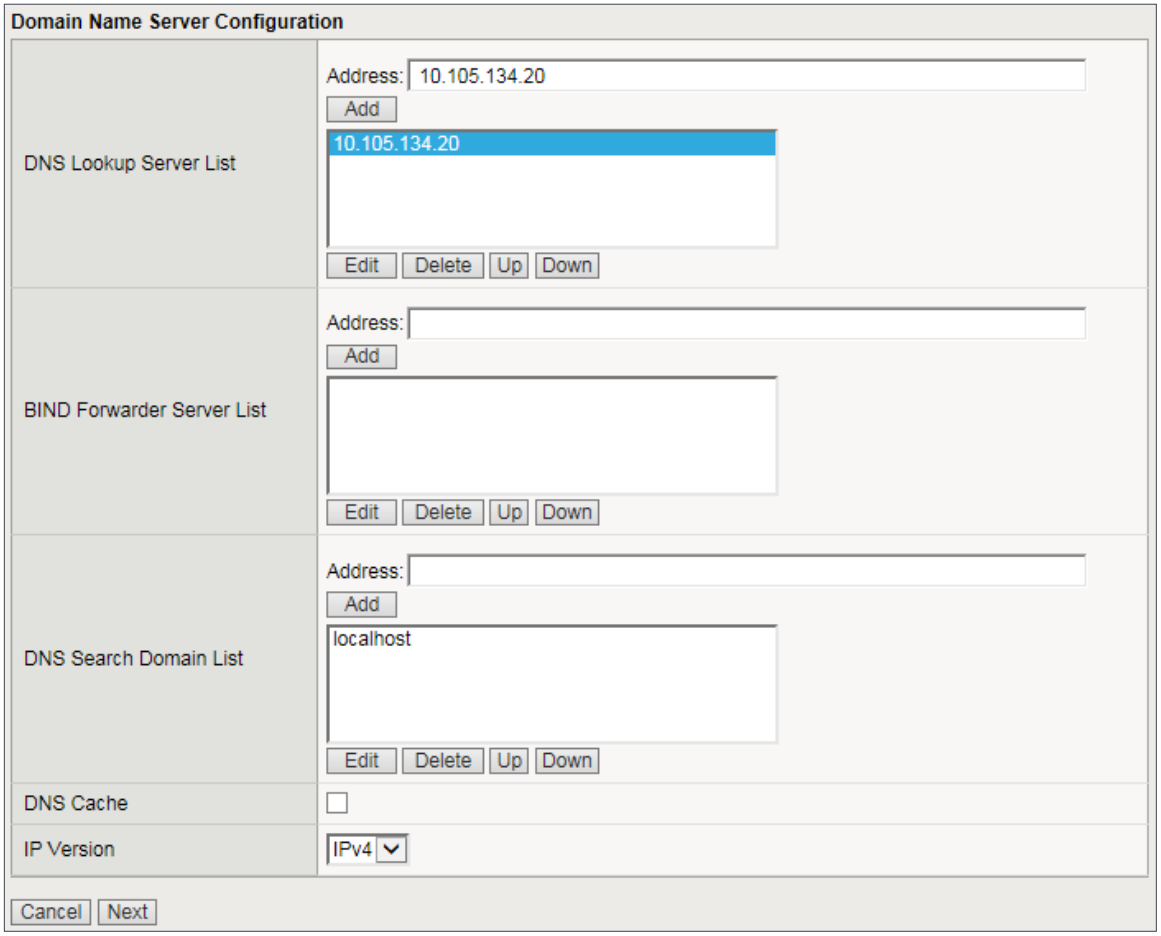
9. Click **Next** to continue.



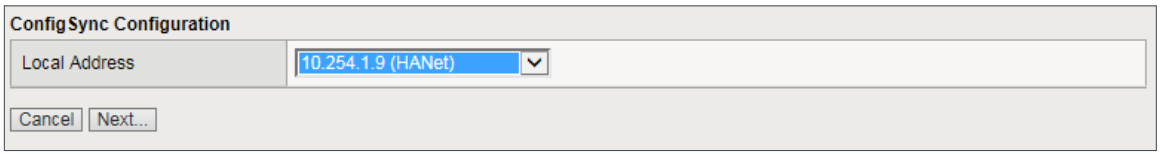
10. Under **Network Time Protocol Configuration**, enter the NTP server **10.105.134.20** and then click **Next**.



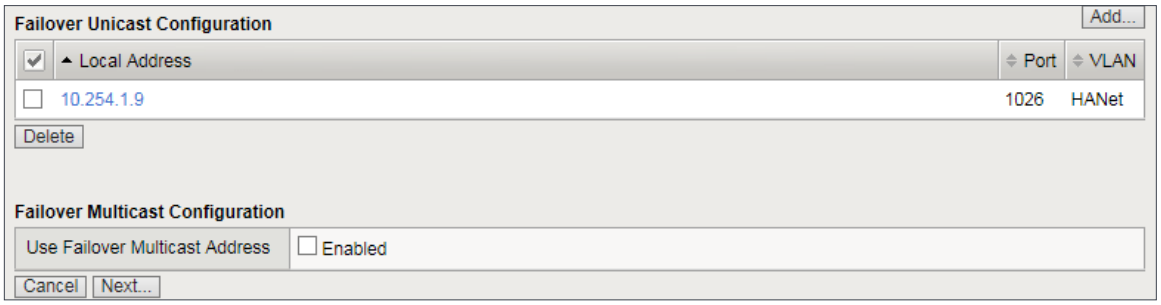
11. In the **DNS Lookup Server List**, enter the appropriate DNS server, in this case, **10.105.134.20**, and then click **Next**.



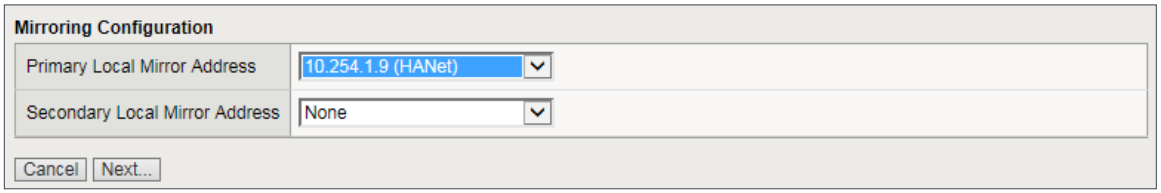
12. For **ConfigSync Configuration**, select the Local address **HANet** VLAN and then click **Next**.



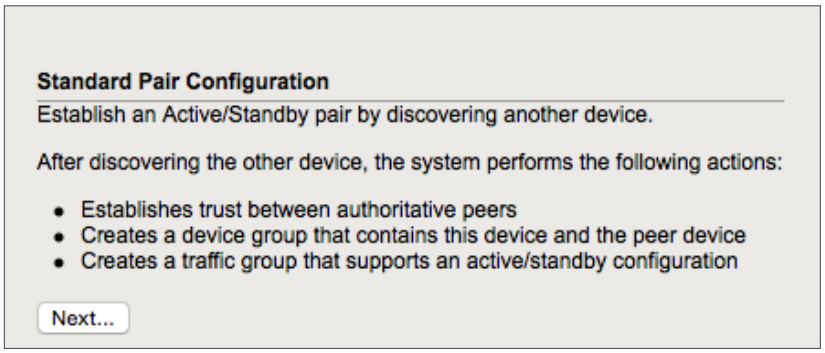
13. Under the **Failover Unicast Configuration**, validate the unicast IP address and select **Next**.



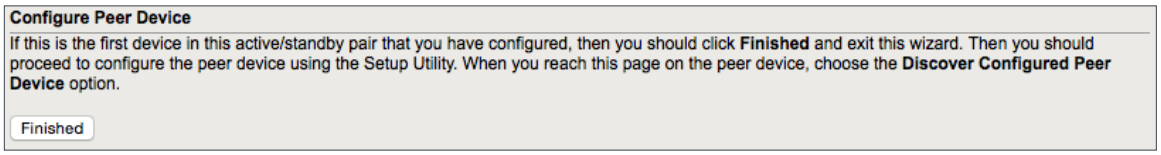
14. Under **Mirroring Configuration**, select the **HANet** as the Primary Local Mirror Address.



15. Select **Next** to continue to **Standard Pair Configuration**.



16. Complete the configuration of NSXBigIP by clicking **Finished**.

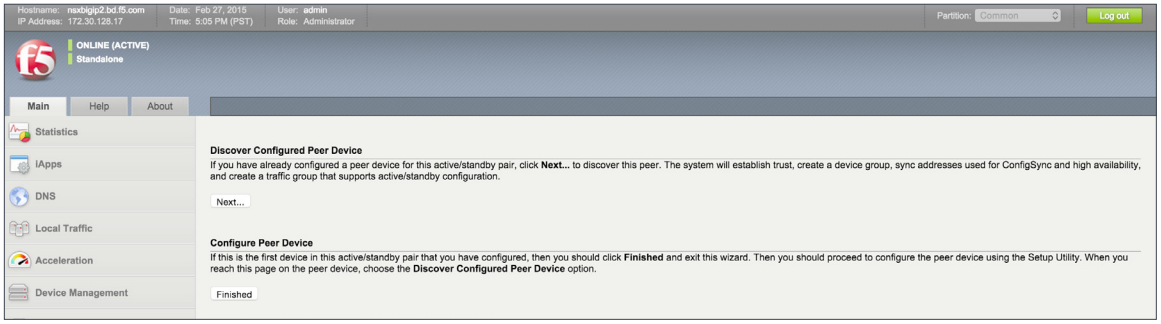


Proceed to configuring NSXBigIP2.

1. For **Internal Network Configuration**, use the following settings:
   - Internal VLAN: **Select Existing VLAN**
   - Select VLAN: **WebTier01**
   - self IP
     - Address: **10.0.1.9**
     - Netmask: **255.255.255.0**
     - Port Lockdown: **Allow Default**
   - Floating IP
     - Address: **10.0.1.13**
     - Port Lockdown: **Allow Default**
2. Select **Next** to continue.
3. For **External Network Configuration**, use the following settings:
   - Internal VLAN: **Select Existing VLAN**
   - Select VLAN: **AppTier01**
   - Self IP
     - Address: **10.0.2.9**
     - Netmask: **255.255.255.0**
     - Port Lockdown: **Allow Default**

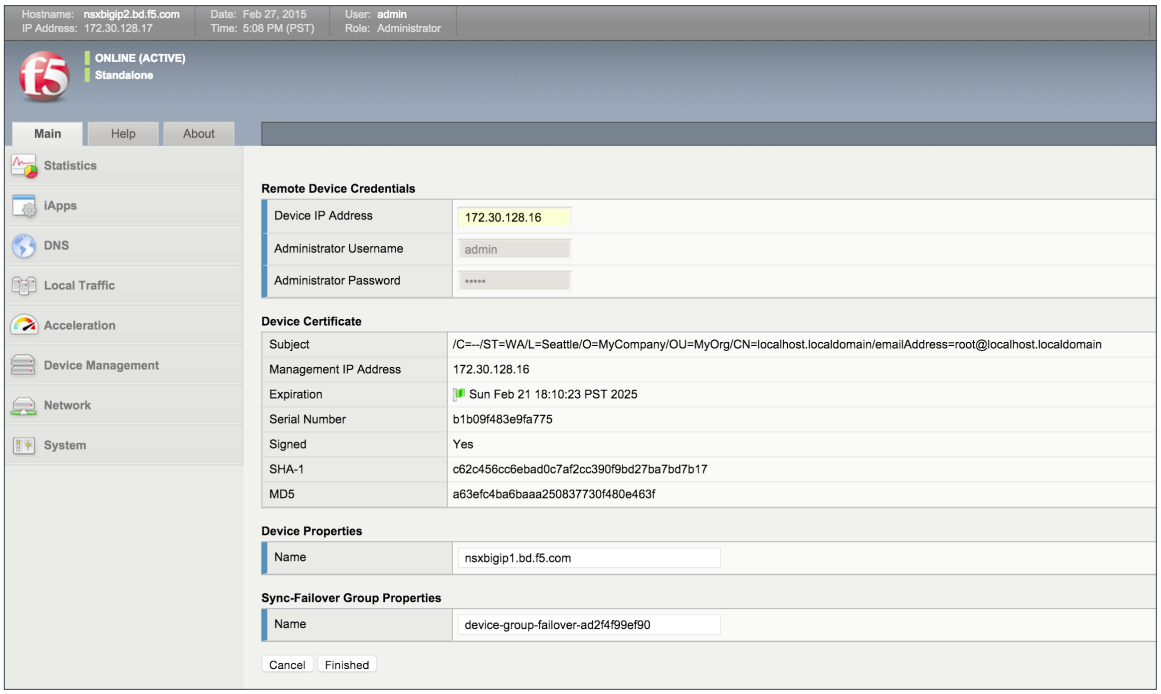
- Floating IP
  - Address: **10.0.2.13**
  - Port Lockdown: **Allow Default**

4. Select **Next** to continue.
5. For **High Availability Network Configuration**, use the following settings:
   - Internal VLAN: **Select Existing VLAN**
   - Select VLAN: **HANet**
   - Self IP
     - Address: **10.254.1.9**
     - Netmask: **255.255.255.0**
     - Port Lockdown: **Allow Default**
6. Select **Next** to continue.
7. To create trust between the two devices and establish a high availability cluster, select **Discover Configured Peer Device**.

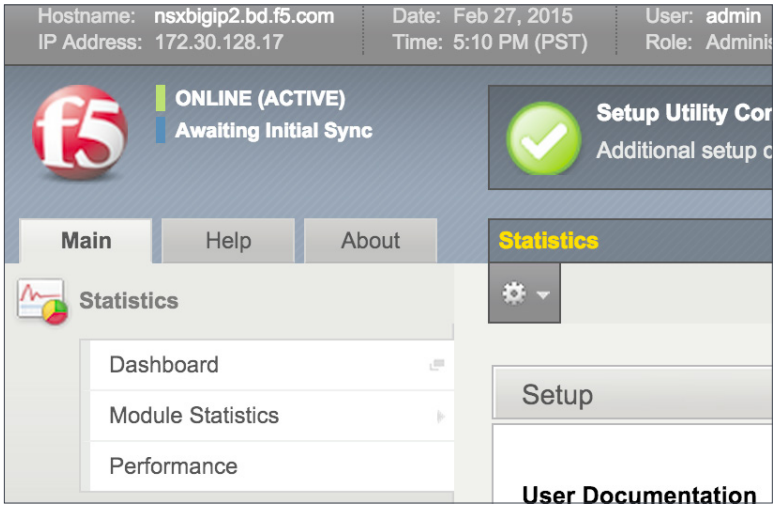


8. Enter the appropriate Device IP Address and administrative username and password combination for your peer device. If you are using the same IP addressing scheme as this validation, use **172.30.128.16**. Click **Retrieve Device Information** to continue.

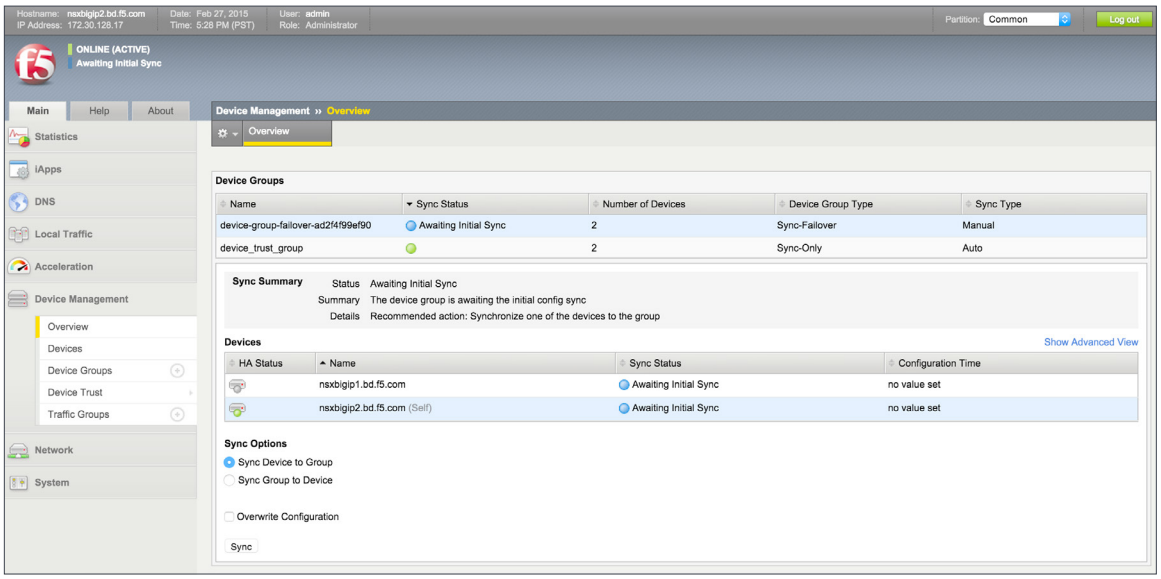
9. The process will return the device certificate for the peer BIG-IP. Validate the name in the Device Properties section and click **Finished** to continue.



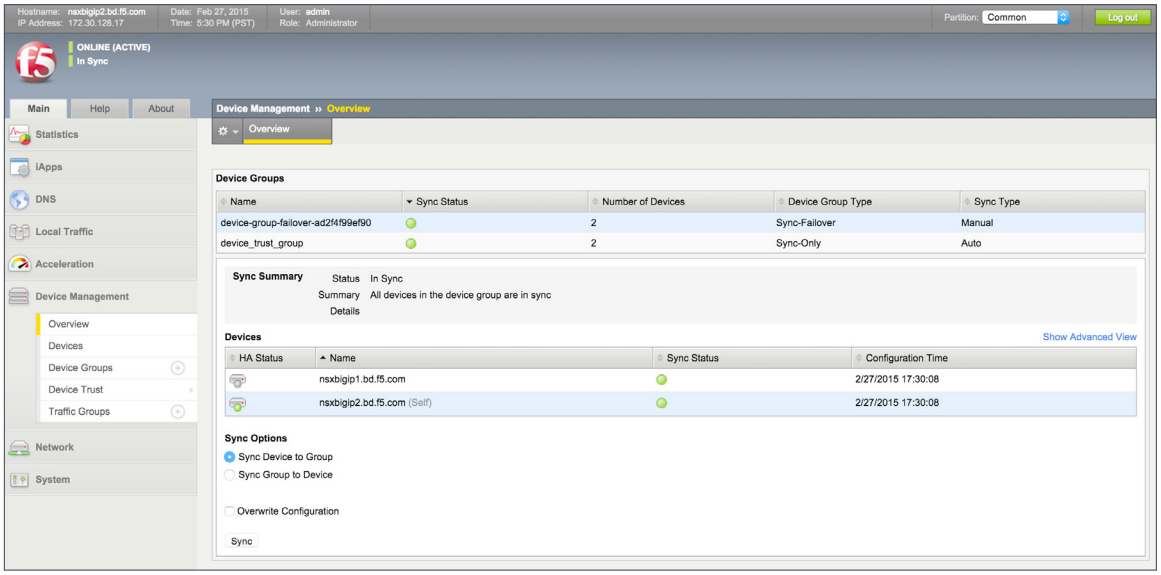
10. The devices should now display Awaiting Initial Sync in the upper left corner. Click on the **Awaiting Initial Sync** link to initiate the initial sync. This will bring up the Device Management >> Overview page.



11. Select and highlight the device you are working from, in this case, **NSXBigIP2**, and click **Sync Device to Group**. Lastly, click **Sync** to initiate the process.



12. Once the sync process completes, the sync status for all Devices Groups and Devices should be green.



Application Configuration

Application configuration typically consists of a base configuration of pool members that are contained by the pool object. The virtual server references the pool to make a load balancing decision among the available pool members. Additional application delivery functionality such as SSL termination, more flexible load balancing algorithm selection, and layer 7 data plane programmability via iRules can be leveraged but are outside the scope of this validation.

Create application pools

We are creating the most basic of pools for our web and app servers, to show the minimum configuration that needs to be done for F5 to load balance the two tiers (web and app). The BIG-IP device will not be load balancing the DB tier traffic, so we are not creating a pool of the DB servers.

1. On the **Main** tab, expand **Local Traffic** and then click **Pools**. The Pool List screen opens.
2. In the upper right corner of the screen, click **Create**.
3. In the **Name** field, type a unique name for the web pool. For this validation, we used **WebServerPool**.

4. Under **Health Monitors**, select an appropriate monitor for your application. In this case we chose a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.

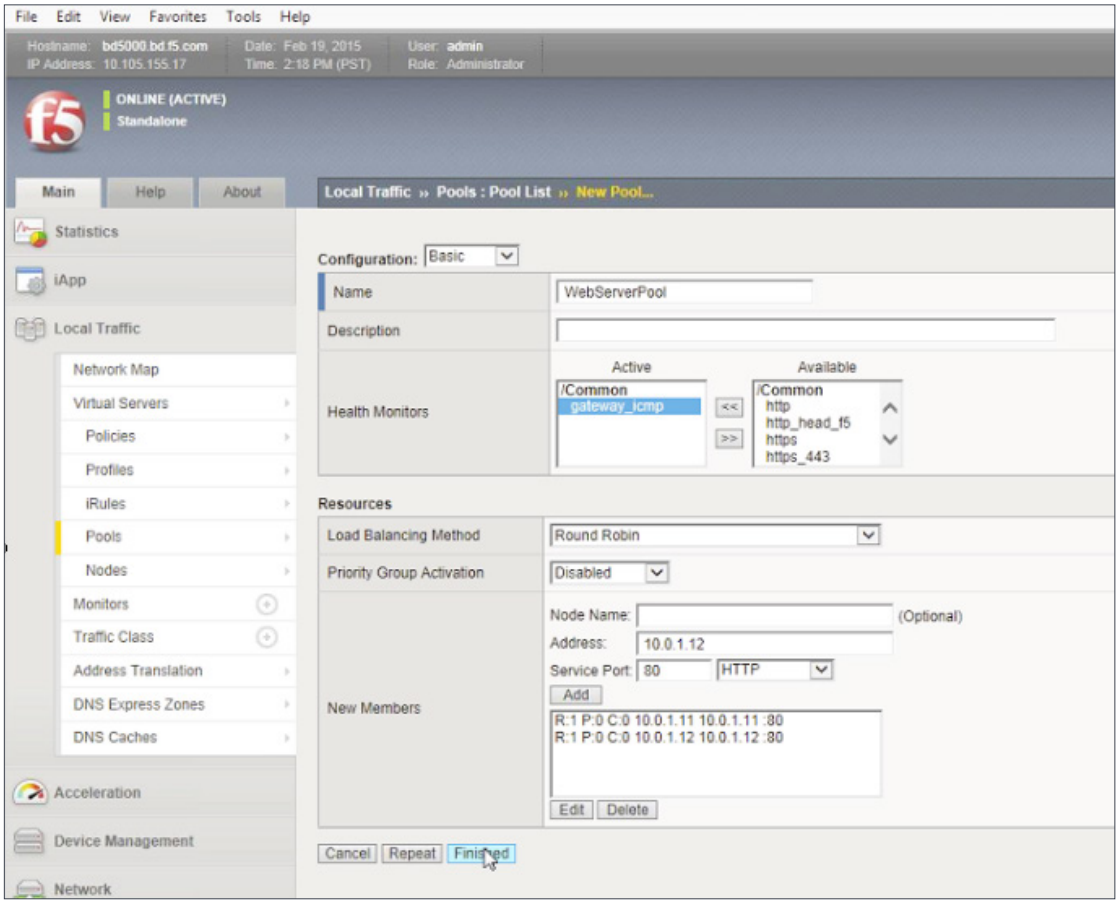
5. Under **Resources**, select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.

6. Under **Resources**, use the **New Members** setting to add the IP address and port of the web servers. Click the **Add** button for each pool member.

7. Select **Repeat** to continue and input the application tier information.

Name (Optional)	Address	Service Port
web-01	10.0.1.11	80 (HTTP)
web-02	10.0.1.12	80 (HTTP)

Table 15. BIG-IP web tier pool members



13. In the **Name** field, type a unique name for the web pool. For this validation, **AppServerPool** was used.

14. Under **Health Monitors**, select an appropriate monitor for your application. In this case, we are choosing a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.

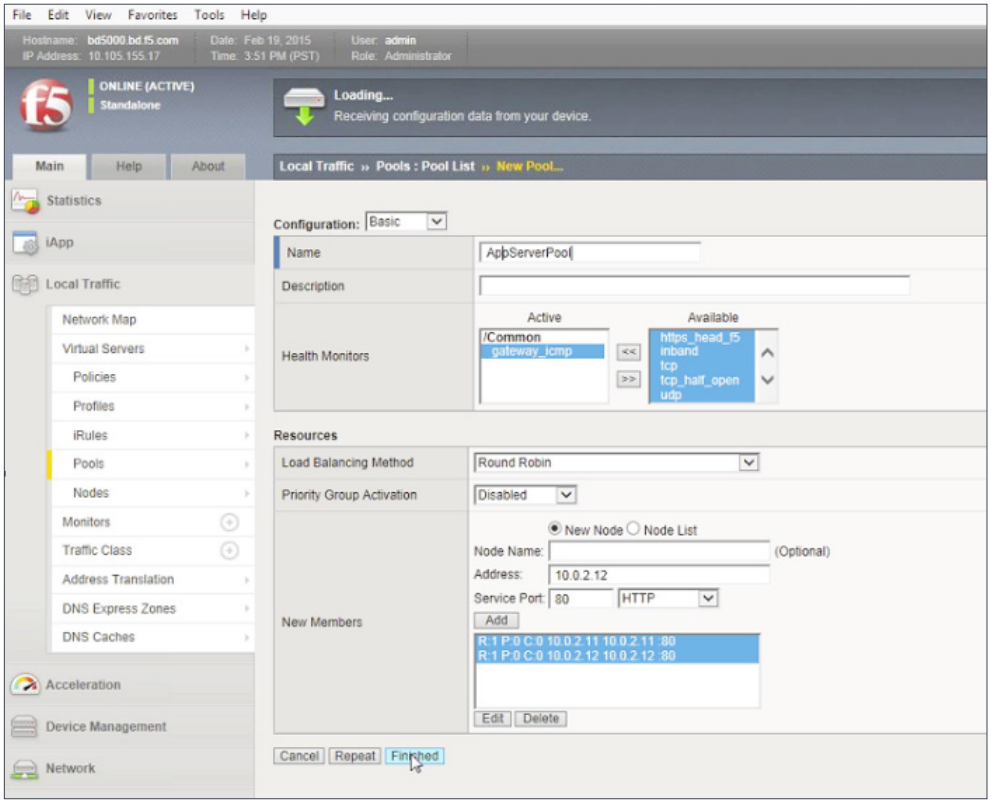
15. Under **Resources**, select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.

16. Under **Resources**, use the **New Members** setting to add the IP address and port of the web servers. Click **Add** for each pool member.

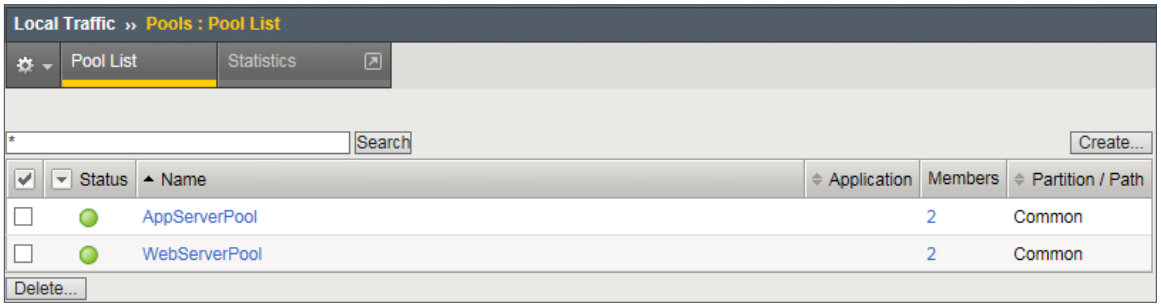
17. Click **Finished** to complete the pool creation.

Name (Optional)	Address	Service Port
App-01	10.0.2.11	80 (HTTP)
App-02	10.0.2.12	80 (HTTP)

Table 16. BIG-IP application tier pool members



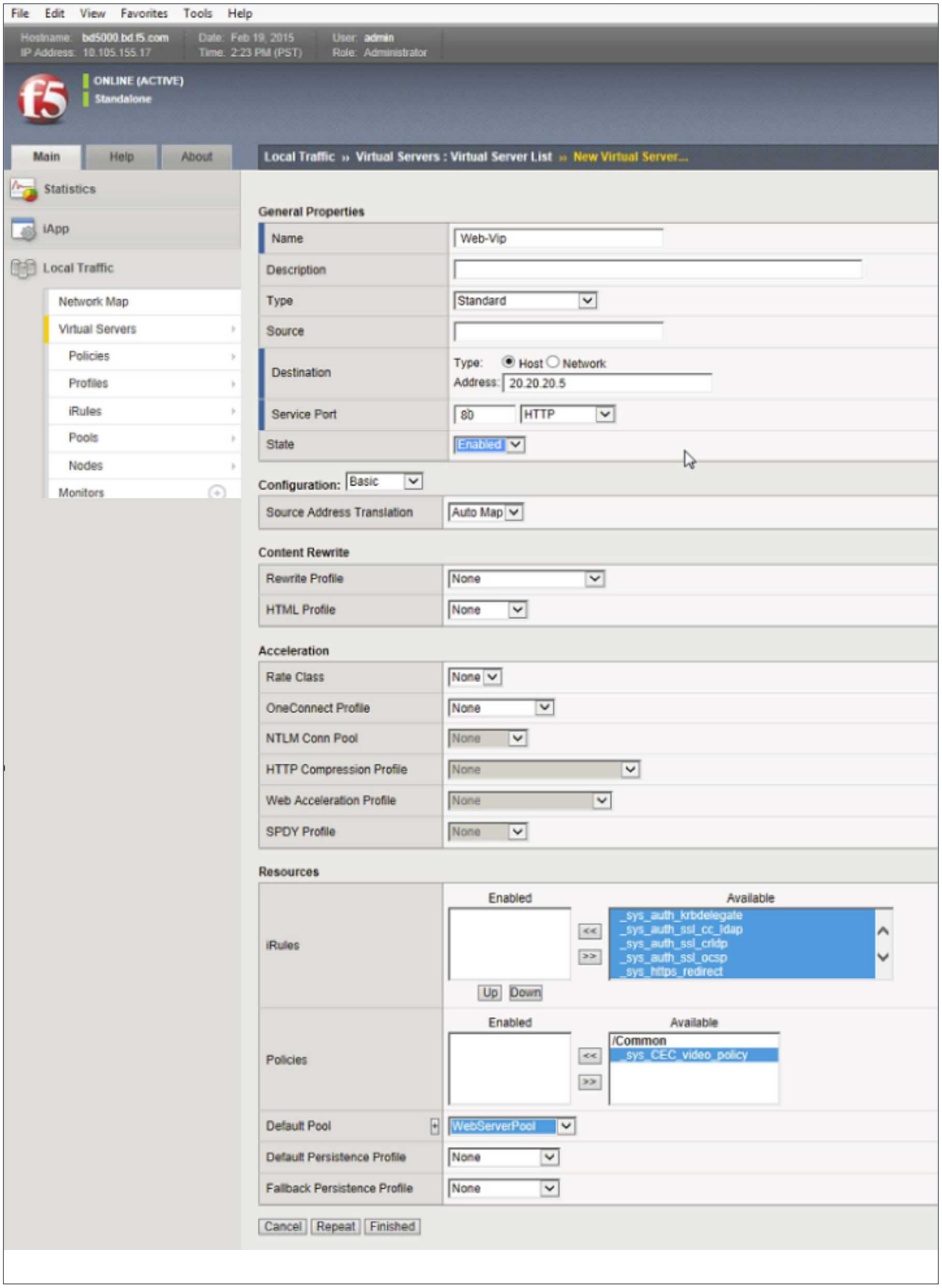
18. The completed configuration for the web and application tier pools should look similar to the image below. Note that the green circles demonstrate that the health monitor, in this case, ICMP, is able to successfully monitor the servers in the overlay networks.



Create application virtual server

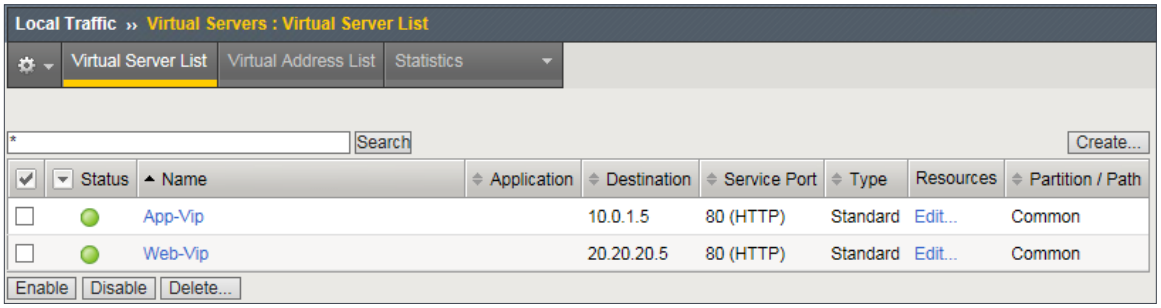
In creating a virtual server, you specify a destination IP address and service port on which the BIG-IP appliance is listening for application traffic to be load balanced to the appropriate application pool members. In this validation we have two virtual servers (VIPs) to create: one for the web tier, which will be available to the external network on the 20.20.20.0/24 segment, and the other for the application tier, available on the TransitNet-1 segment.

1. On the **Main** tab, expand **Local Traffic** and then select **Pools**. The Pool List screen opens.
2. In the upper right corner of the screen, click **Create**.
3. In the **Name** field, enter a unique name for the web application. In this case, we used **Web-Vip**.
4. In the **Destination Address** field, enter the IP Address **20.20.20.5**.
5. For **Service Port** use the HTTP standard port **80**.
6. Under **Configuration**, select **Auto Map** from the Source Address Translation dropdown box.
7. Under **Resources** at the bottom of the New Virtual Server configuration page, select the **WebServerPool** from the dropdown box.
8. Again, select **Repeat** to continue to configure the application tier virtual server.


File Edit View Favorites Tools Help
Hostname: bd5000.bd.f5.com
IP Address: 10.105.155.17
Date: Feb 19, 2015
Time: 2:23 PM (PST)
User: admin
Role: Administrator
ONLINE (ACTIVE)
Standalone
Main Help About
Local Traffic » Virtual Servers : Virtual Server List » New Virtual Server...
Statistics
iApp
Local Traffic
Network Map
Virtual Servers
Policies
Profiles
iRules
Pools
Nodes
Monitors
General Properties
Name Web-Vip
Description
Type Standard
Source
Destination Type: Host Network Address: 20.20.20.5
Service Port 80 HTTP
State Enabled
Configuration: Basic
Source Address Translation Auto Map
Content Rewrite
Rewrite Profile None
HTML Profile None
Acceleration
Rate Class None
OneConnect Profile None
NTLM Conn Pool None
HTTP Compression Profile None
Web Acceleration Profile None
SPDY Profile None
Resources
iRules
Enabled
Available
_sys_auth_krbdelegate
_sys_auth_ssl_cc_ldap
_sys_auth_ssl_crldp
_sys_auth_ssl_ocsp
_sys_https_redirect
Up Down
Policies
Enabled
Available
/Common
_sys_CEC_video_policy
Default Pool WebServerPool
Default Persistence Profile None
Fallback Persistence Profile None
Cancel Repeat Finished

9. The image has been cropped to highlight the specific configuration.
10. In the upper right corner of the screen, click **Create**.
11. In the **Name** field, enter a unique name for the web application. In this case, use used **App-Vip**.
12. In the **Destination** address field, enter the IP address **172.16.1.5**.
13. For **Service Port**, use the HTTP standard port **80**.
14. Under **Configuration**, select **Auto Map** from the Source Address Translation dropdown box.
15. Under **Resources**, select **AppServerPool** from the dropdown box.
16. Again, select **Finished** to continue to configure the application tier virtual server.

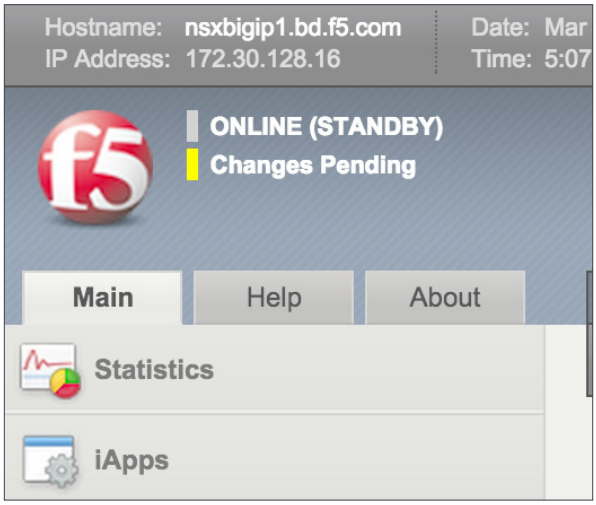
When complete, the virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application, and the virtual servers and the associated pools are reachable and healthy.



Synchronize Changes across the Cluster

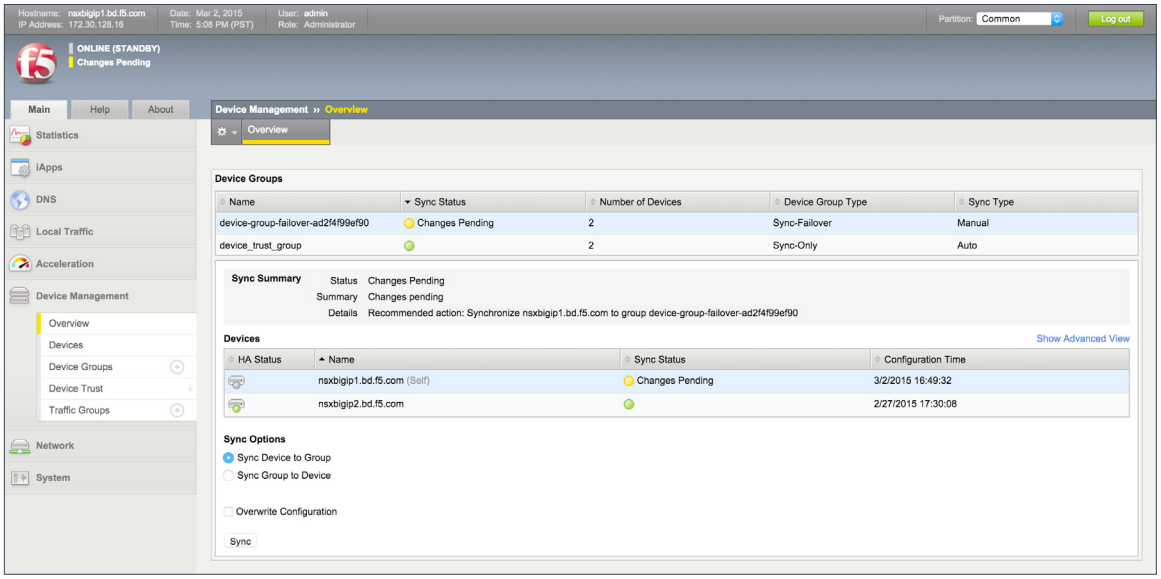
When working with a device cluster, we must initiate the sync process from the device cluster we are making changes to on the peer BIG-IP.

1. In the upper left of the browser window, click the **Changes Pending** link.

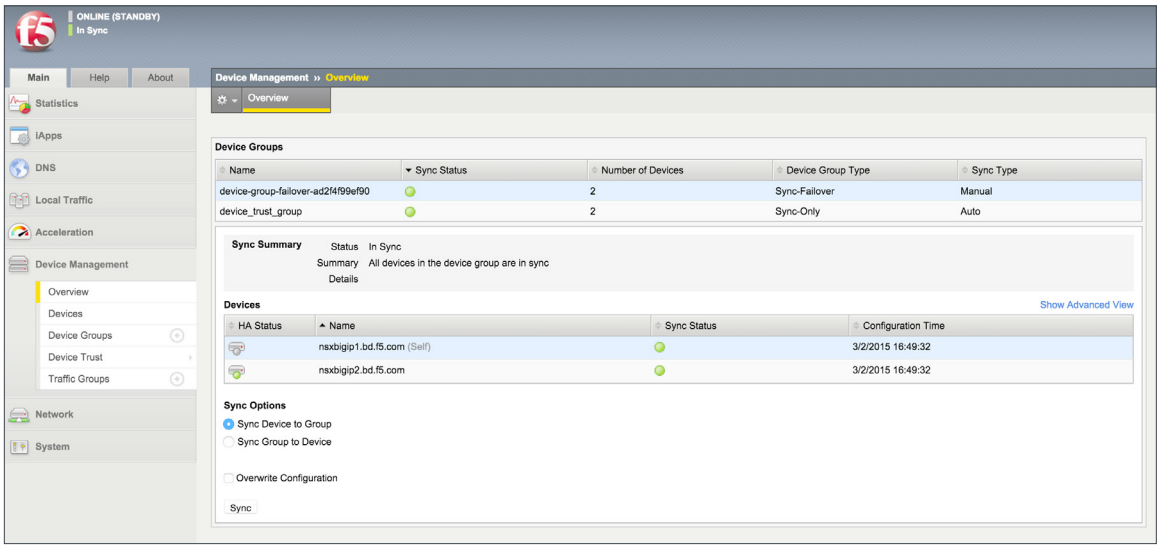


Pay careful attention to the **Recommended Action** in the **Sync Summary** section. In this case, we made changes on NSXBigIP, which need to be synchronized to other device in the group NSXBigIP2.

2. Select and highlight the device you are working from, in this case, **NSXBigIP1**, and then click **Sync Device to Group**. Lastly, click **Sync** to initiate the process.



3. Validate that the synchronization process completed successfully and that all devices in the group are in sync. All sync status buttons should be green, as shown below.

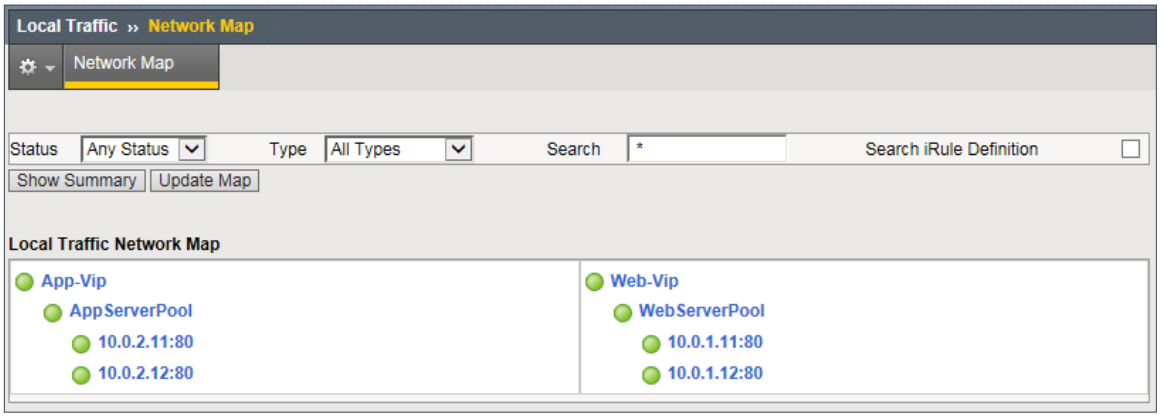


4. This completes the configuration portion for the topology.

Validation

The web tier virtual server should now be available and accepting application traffic on port 80 (HTTP).

From the Main tab, expand **Local Traffic**, and then click **Network Map** to display the overall health of the applications and their associated resources.



Any web browser can be used to test the application itself by typing http://20.20.20.5 to send a request to the virtual server. A simple Apache web server can be installed on the web tier to validate.

This concludes the validation of the *Parallel to DLR using VLANs with BIG-IP Physical Appliances* deployment scenario.

Conclusion

This document validates and walks through the implementation of several possible NSX and BIG-IP interoperability scenarios and the network topologies to accomplish those scenarios.

F5 and VMware are working on a jointly developed API integration between NSX and the F5 BIG-IQ management and orchestration platform. This will enable IT organizations to fully leverage the combined strengths of NSX virtualization and automation with richer application delivery services enabled by F5 BIG-IP.

This planned NSX/F5 integration will allow users to configure BIG-IP settings (for example, pools, VIPs, iApps) from NSX. The integration will also allow for automated BIG-IP virtual edition deployment, licensing, and configuration. Many of the scenarios described in this document will be deployable using this upcoming integration. For more information about these solutions, please contact your local F5 or VMware representative.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan K.K. f5j-info@f5.com

Solutions for an application world.