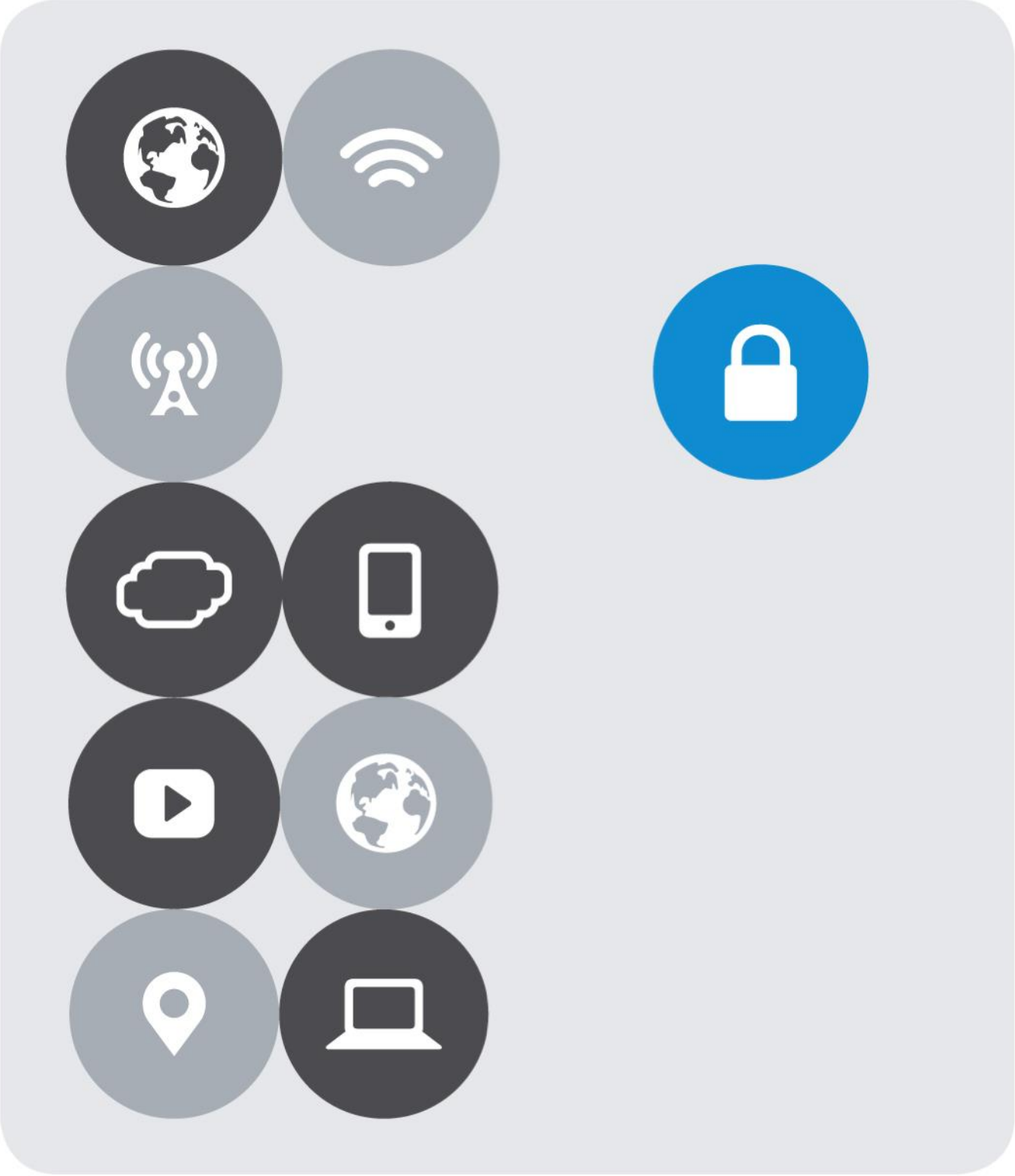
INTEGRATION GUIDE

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



Version History

Date	Version	Author	Description	Compatible Versions
April 2020	2.0	Matt Mabis Paul Pindell	Updated Documentation (Pictures and Re-Validation on Newest Versions of NSX-V)	VMware NSX Data Center for vSphere 6.4.x (1)
????	1.0	Paul Pindell Justin Venezia	Initial Document	

(1) This is confirmed working for NSX Datacenter for vSphere 6.4.x but could work on earlier editions.

Contents

Introduction

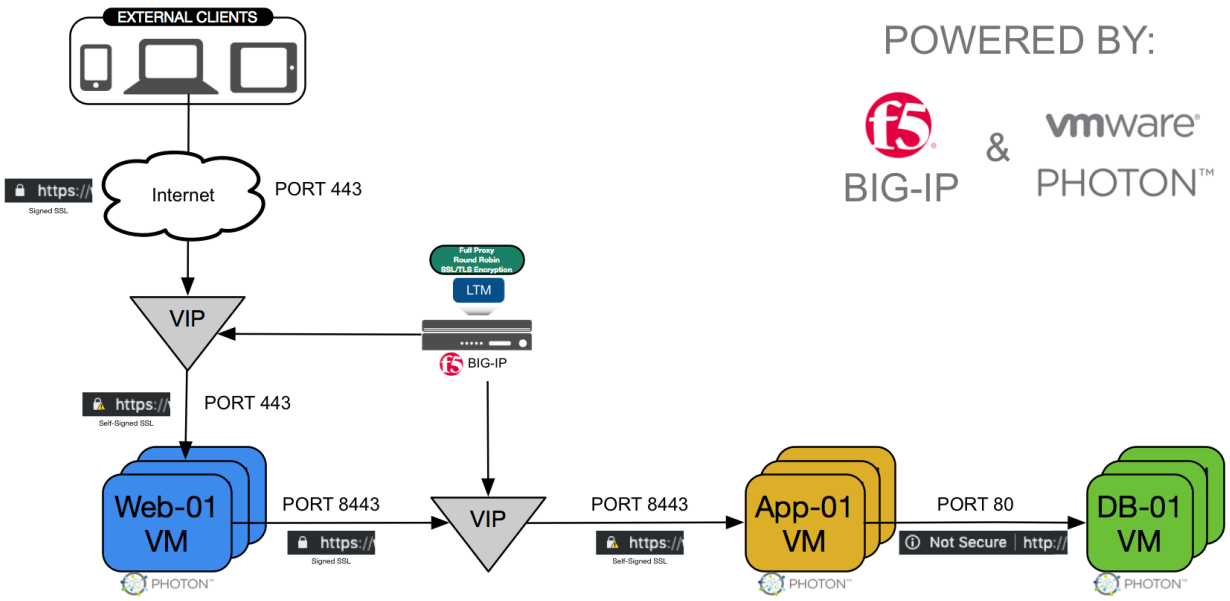
The Software-Defined Data Center (SDDC) is characterized by server virtualization, storage virtualization, and network virtualization. Server virtualization has already proved the value of SDDC architectures in reducing costs and complexity of the compute infrastructure. VMware NSX network virtualization 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, workflows and best practices for the topologies to optimize interoperability between the NSX platform and F5 BIG-IP physical and/or virtual appliances. This guide is intended for customers who would like to adopt the SDDC while ensuring compatibility and minimal disruption to their existing BIG-IP environment.

The Multi-tiered Application

The multi-tiered application consists of 3 instances that are independent of each other. Each instance has a specific role/task and has its own OS/Firewall Protections on them. Here is a diagram of how the information is accessed from an external client.



1) WebTier – Web Server(s) are providing secure access to the backend application, these servers are internet facing typically and have load balancing to allow servers to distribute loads appropriately.

2) AppTier – Application Server(s) access the backend database(s) and execute the code and provide that data to the Web Server(s) sitting in front of them. These Applications are not internet facing and are protected by the LAN.

3) DBTier – Database Server(s) that house the information that the application servers execute against, these servers these servers are also not internet facing and are protected by the LAN.

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

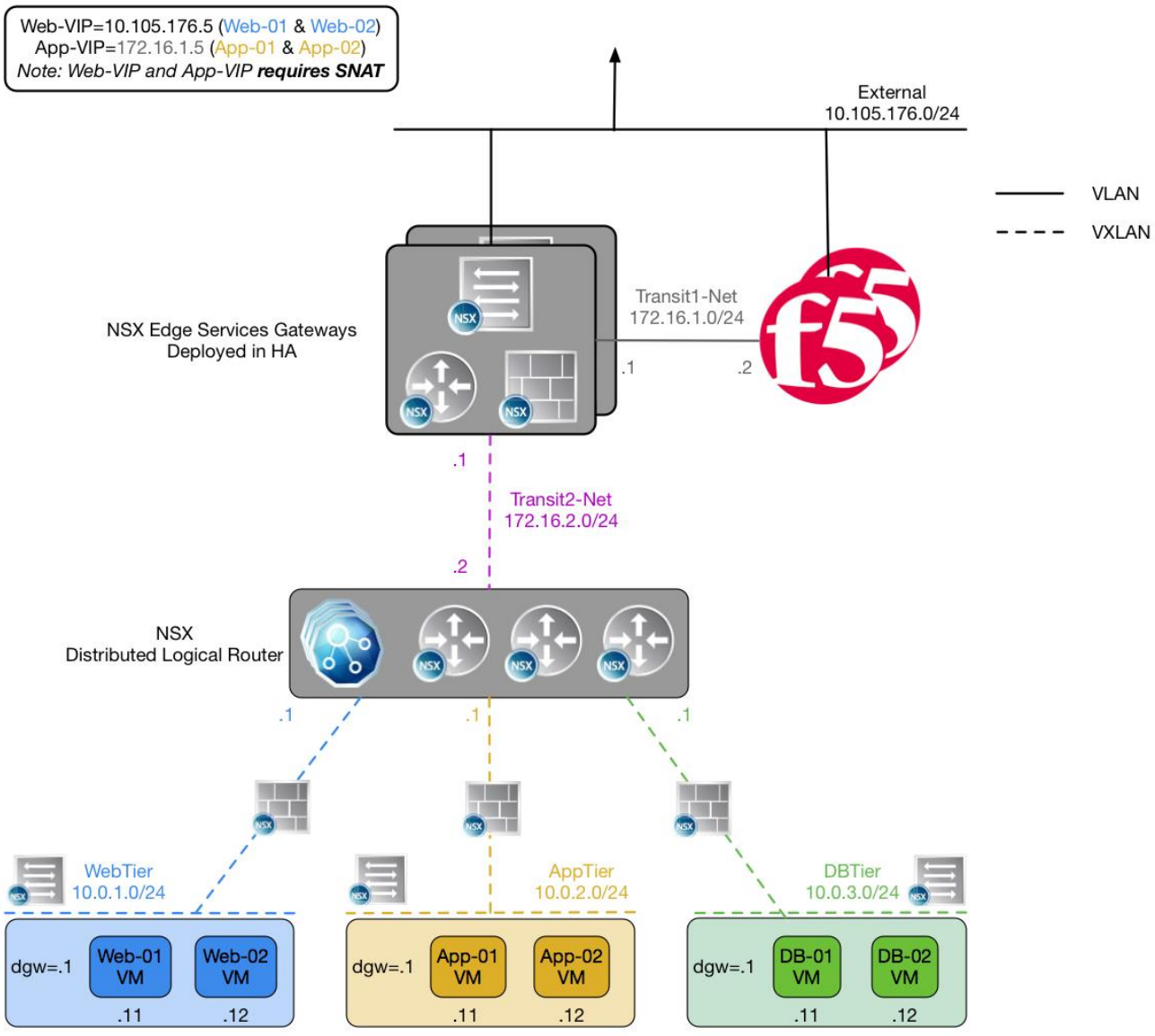


Figure 1 BIG-IP appliance parallel to NSX Edge Services Gateway

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.

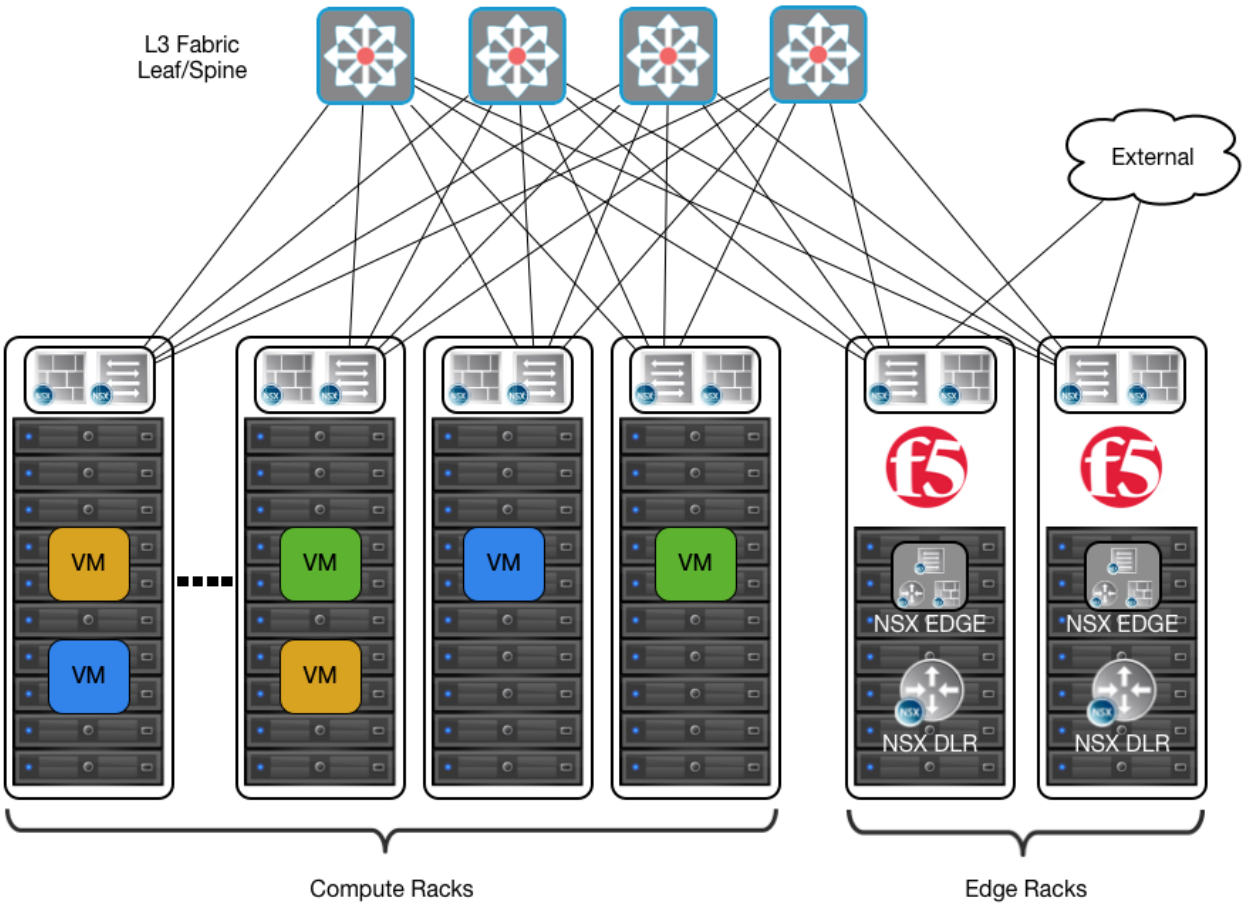


Figure 2 Leaf/spine physical rack infrastructure

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 placement of the BIG-IP appliances (physical or virtual) should be in the same infrastructure racks as those reserved for the NSX Edge Services Gateway deployments.

Traffic Flows

North-South Traffic - Logical Traffic Flows as Follows

1. From Client (External) to BIG-IP WebTier VIP (Web-VIP)
2. From BIG-IP Appliance to NSX Edge to DLR to WebTier Servers
3. From WebTier Servers to DLR to NSX Edge to BIG-IP AppTier VIP (App-VIP)
4. From BIG-IP Appliance to NSX Edge to DLR to AppTier Servers
5. From AppTier Servers to DLR to DB-Tier Servers

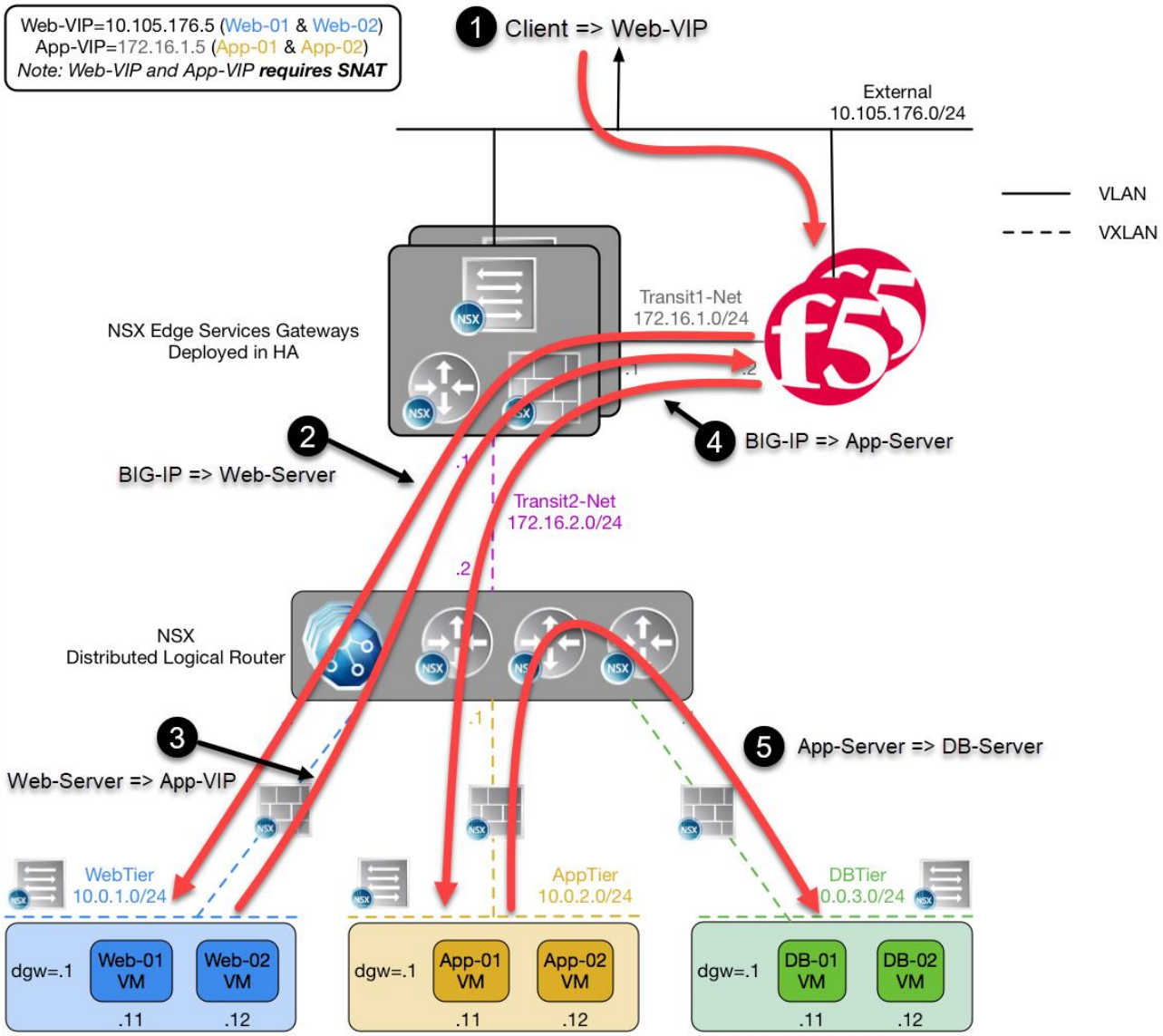


Figure 3 North-South Logical Traffic Flow "Parallel to NSX Edge" with BIG-IP Appliances

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 4: the Cluster1-VDC (Edge Rack) and Cluster3-Compute-NSX (Compute Rack). 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 4 vSphere Console

In accordance with best practices, edge and compute ESXi hosts are physically and logically separated from one another. In our configuration BIG-IP's are installed in dedicated edge racks, along with vCenter, NSX manager, and the NSX Edge Services Gateways, which also will be installed in the edge rack ESXi hosts.

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, look at Figure 3 above.

Prerequisites

Referencing the diagram in Figure 1, the BIG-IP requires connectivity to at minimum two of its 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 BIG-IP will need to be installed and connected (physically or virtually) to the edge rack. Each BIG-IP management interface will need to be connected and configured with an IP address in the management segment.
- The BIG-IP interface 1.1 will need to be connected to a switch port either in ESXi (trunked port group) or on the edge rack top-of-rack switch that 802.1Q tags the VLANs used in this environment. In the example, VLANs 102, 176 and 177 are used.
- Physical network infrastructure switches connected to the ESXi servers and BIG-IP appliances (if not virtual) 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	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176	176
Internal	DVS-VLAN-102	102
TransitNet-1	DVS-VLAN-177	177

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

Name	Transport Zone	Segment ID	Control Plane Mode
AppTier	TransportZone1	5002	Unicast
DBTier	TransportZone1	5003	Unicast
Transit2-Net	TransportZone1	5005	Unicast
WebTier	TransportZone1	5001	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, IP Pools are created that will be used by the Web, App, and DB virtual machines.

802.1Q VLAN segments

- **VLAN 176 (External)** is the VLAN used for external client to Web-VIP connectivity. The 10.105.176.0/24 IP subnet range is configured on this VLAN.
- **VLAN 102 (Internal)** (not shown) is for management connectivity. The 192.168.14.0/24 IP subnet range is configured on this VLAN.
- **VLAN 177 (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.

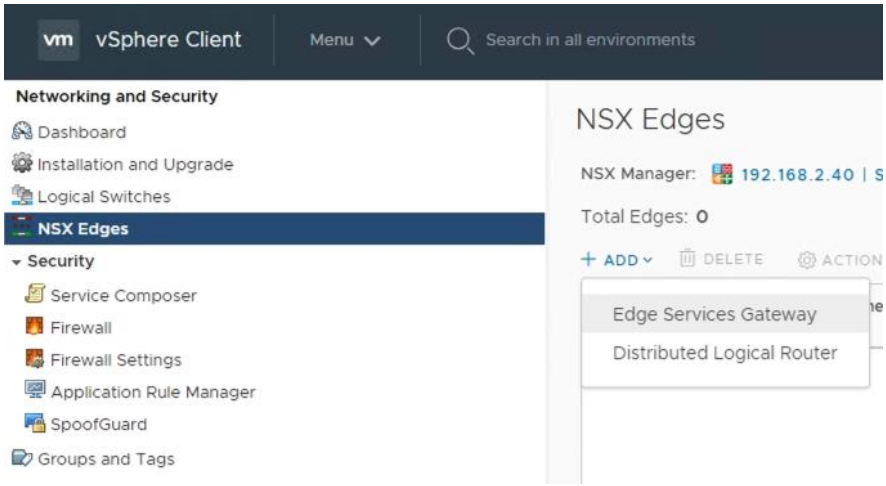
VXLAN Segments

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

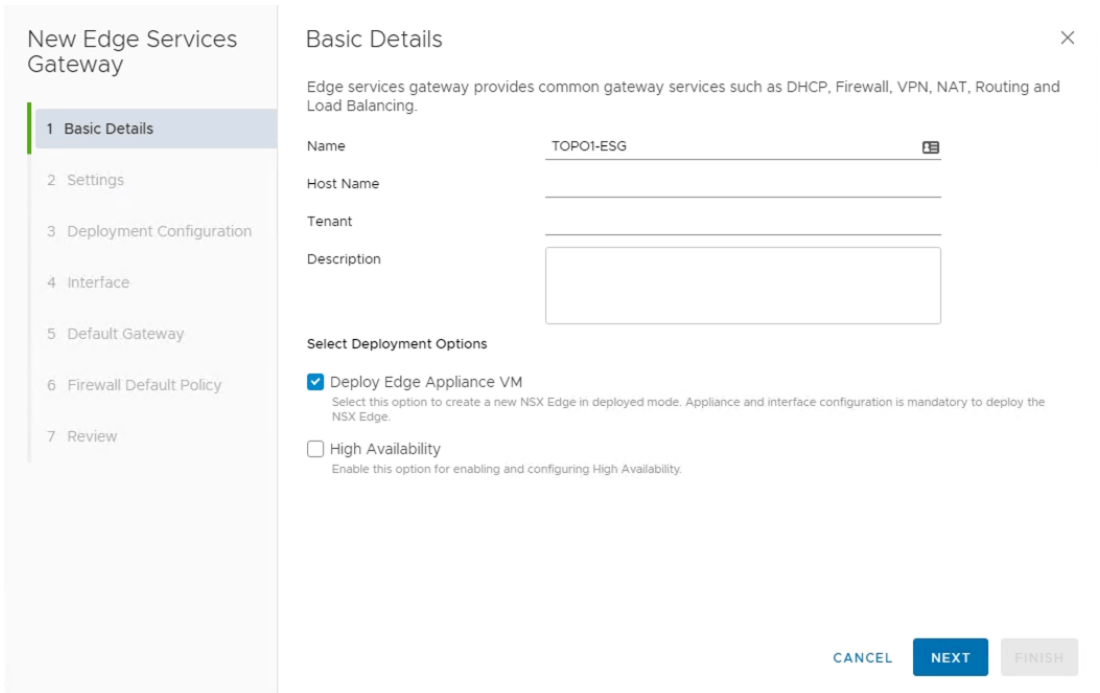
- VXLAN 5001 WebTier is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5002 AppTier is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5003 DBTier is the segment ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5005 TransitNet-2 is the VXLAN segment ID used for the transport zone between the DLR and the NSX Edge.

NSX Edge Configuration

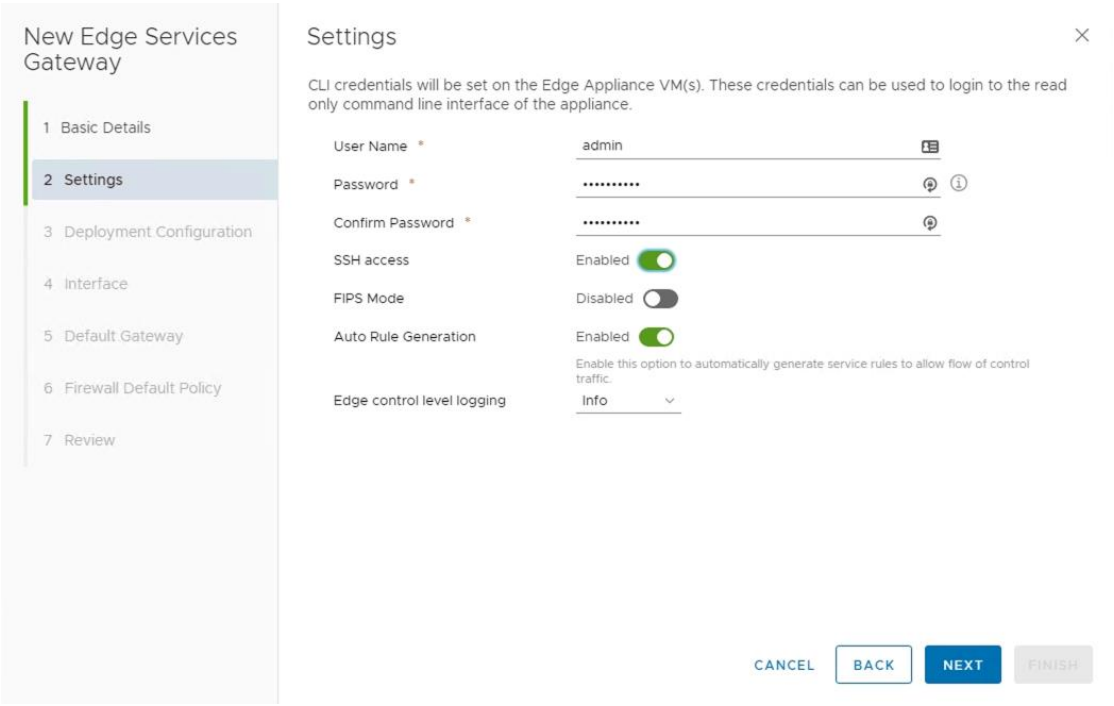
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then click (+ Add) hyperlink → Click on “Edge Services Gateway”.



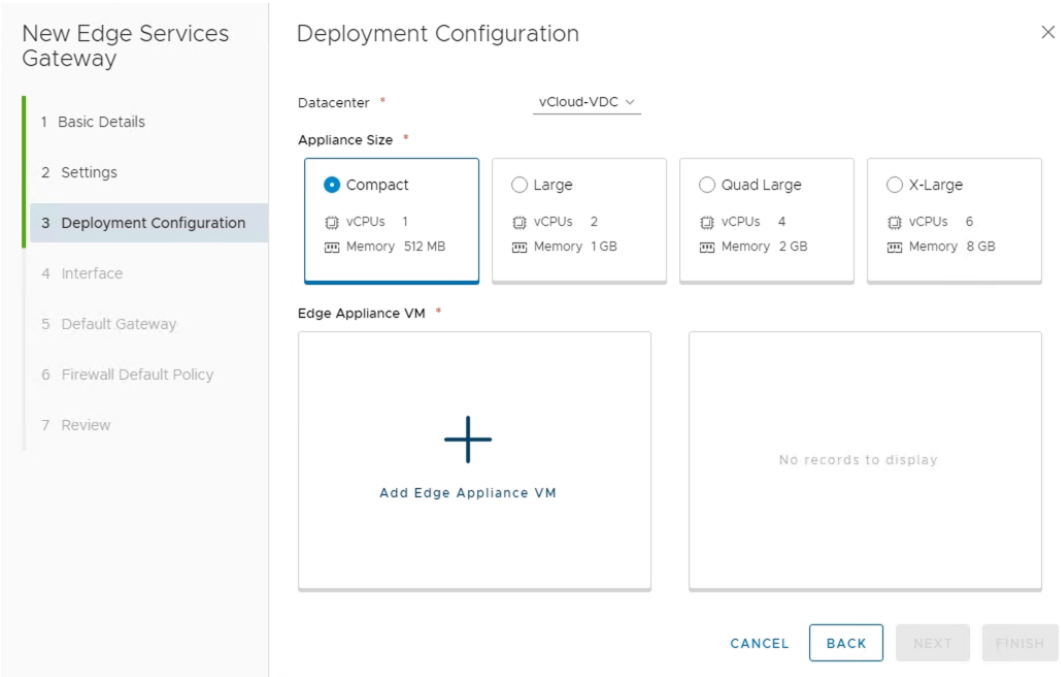
2. Provide a name for the device, then click next.



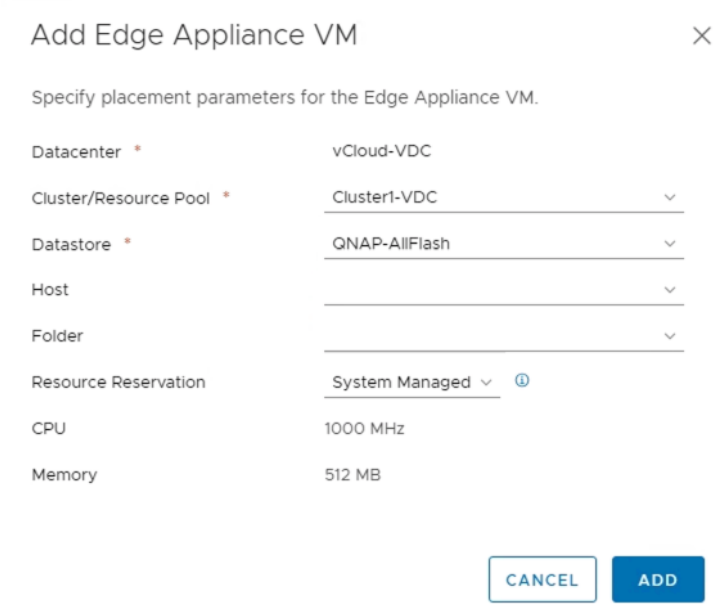
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.



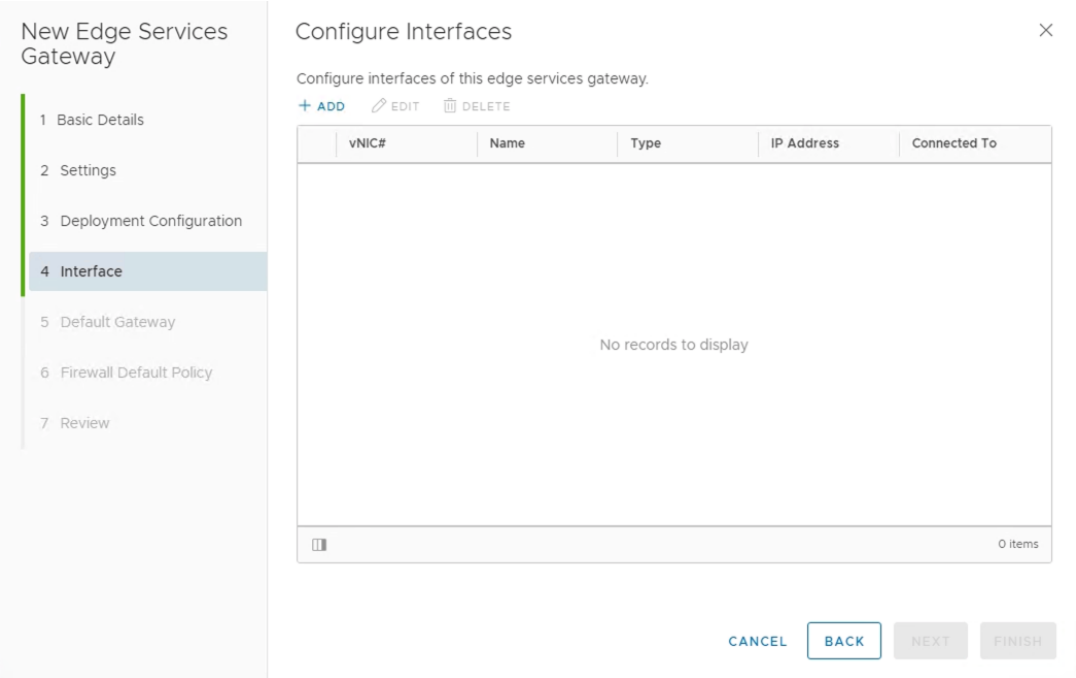
4. Under Configure deployment, select the Datacenter and Appliance Size appropriate for your deployment. Then click on the plus symbol (+) to Add Edge Appliance VM.



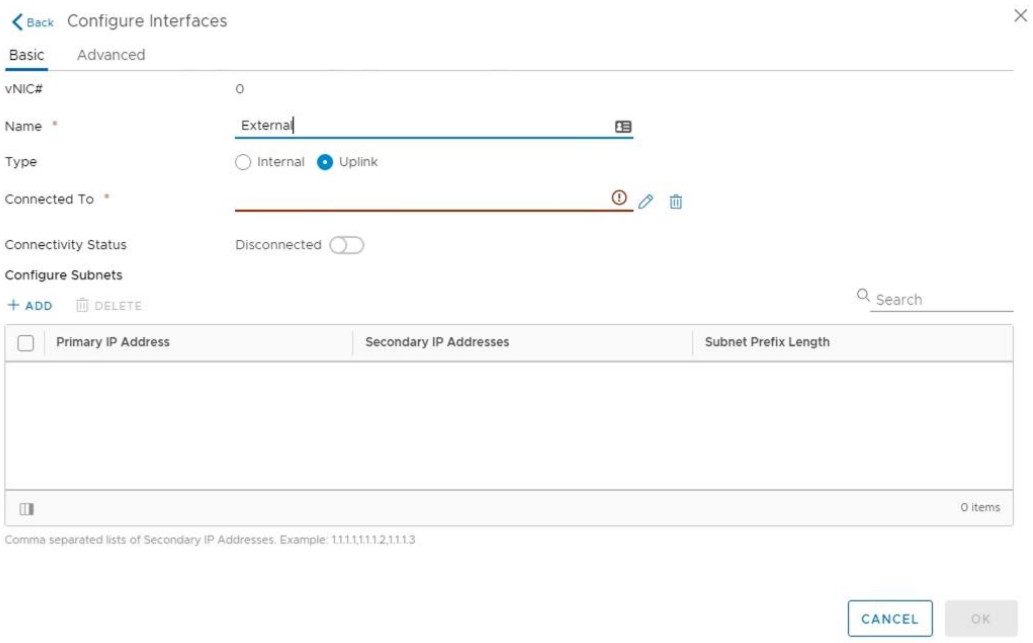
5. Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete. This will return you to the configure deployment screen shown in step 4 with the Edge Appliance VM filled out. Click **Next** to continue.



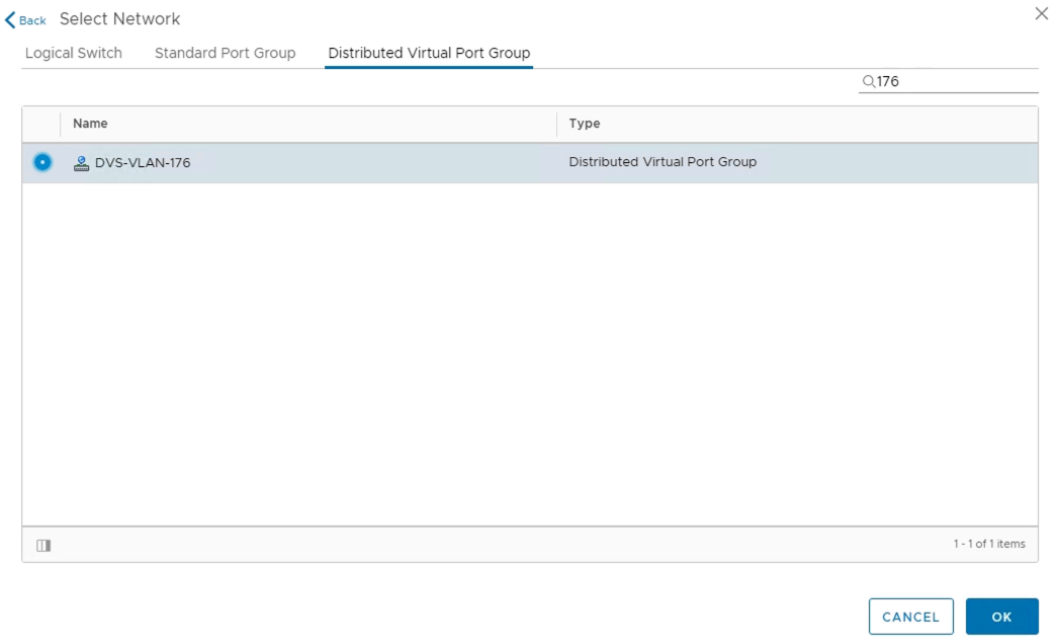
6. In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX Edge Interface dialog box.



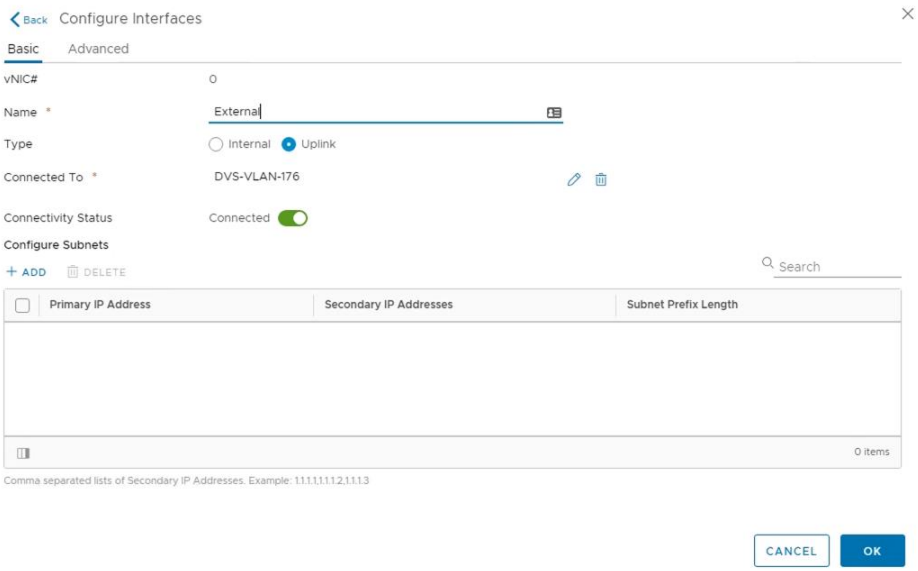
7. Provide a name and click the edit icon next to the “Connected To” field.



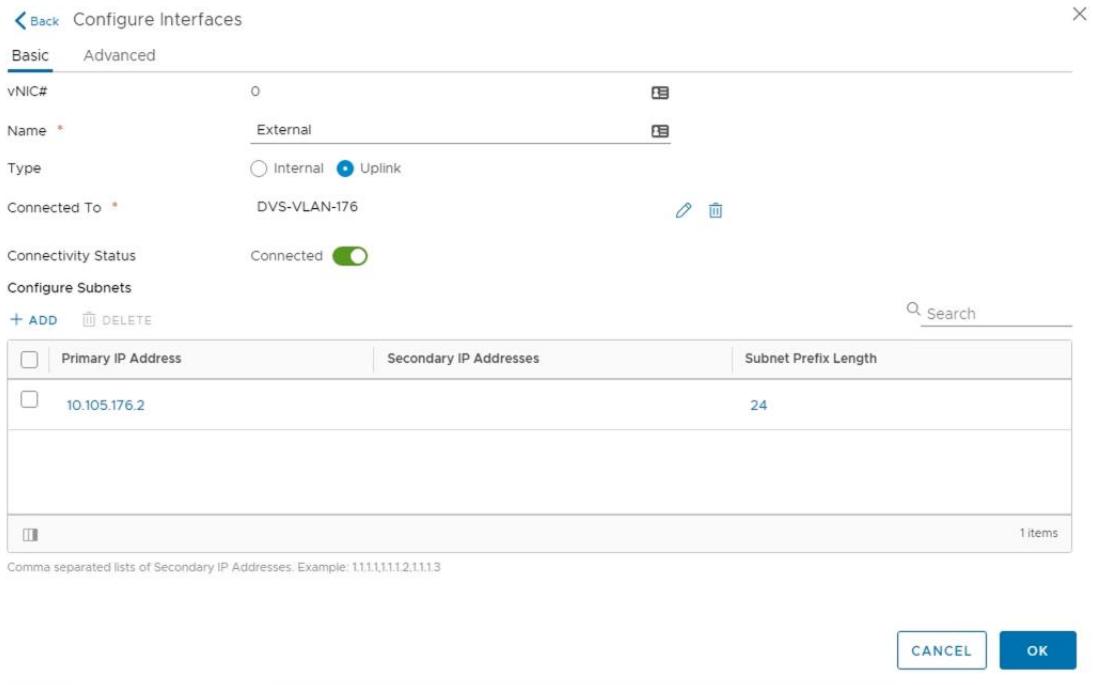
8. For the External network, click on the Distributed Virtual Port Group tab and then selecting the port group used for external access. Click OK.



9. Once the network is chosen, select the (+ Add) hyperlink under Configure Subnets to add the appropriate IP address and subnet configuration to the interface.



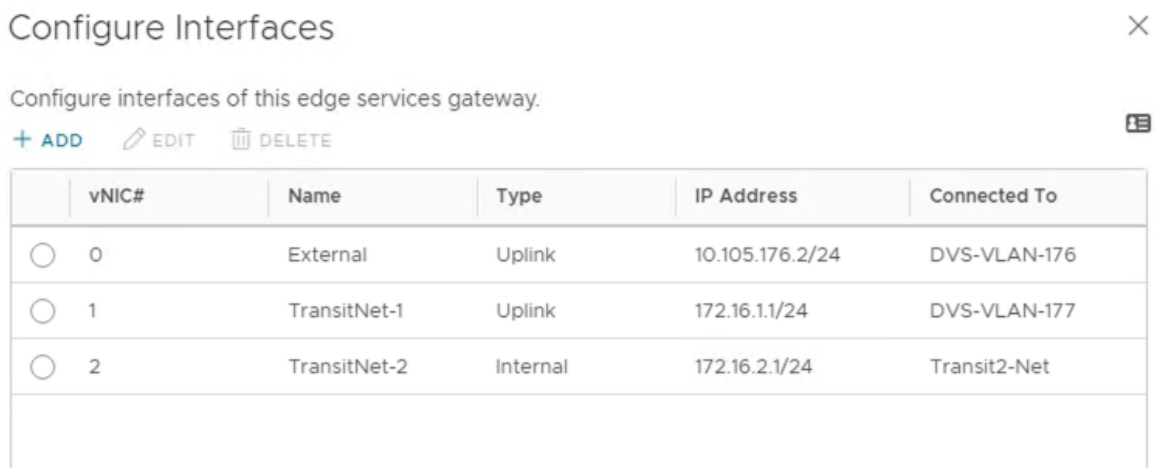
10. In the Add Subnet dialog box, enter the appropriate IP address and Subnet prefix length, and click OK.



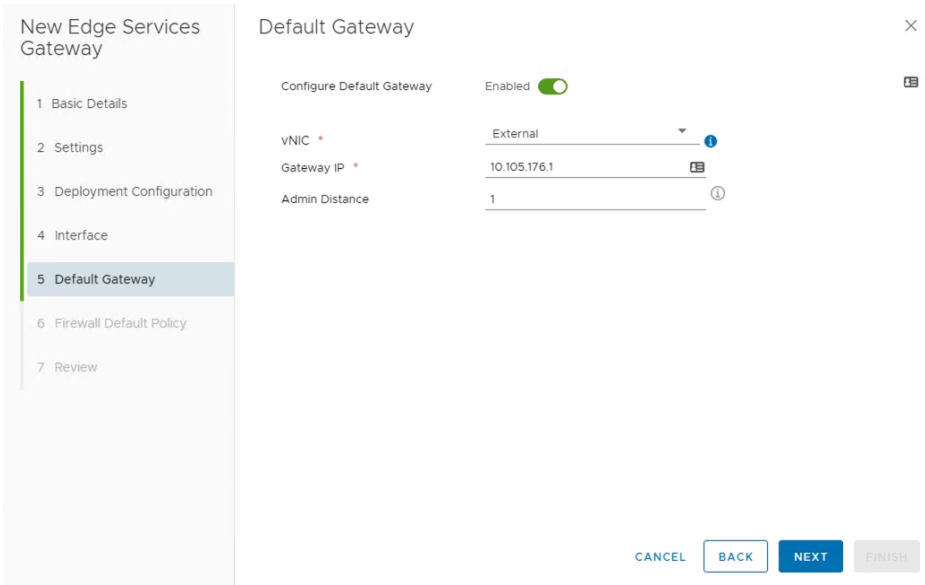
11. This will bring you back to the Configure interfaces dialog box. For each of the three interfaces required for this deployment scenario, add and configure the appropriate subnets and switch type, according to the table below and look like the final picture below with your datacenter information.

Network Name	Type	Network Type	IP Address	Connected To
External	Uplink	Distributed Virtual Port Group	10.105.176.2/24	DVS-VLAN-176
TransitNet-1	Uplink	Distributed Virtual Port Group	172.16.1.1/24	DVS-VLAN-177
TransitNet-2	Internal	Logical Switch	172.16.2.1/24	Transit2-Net

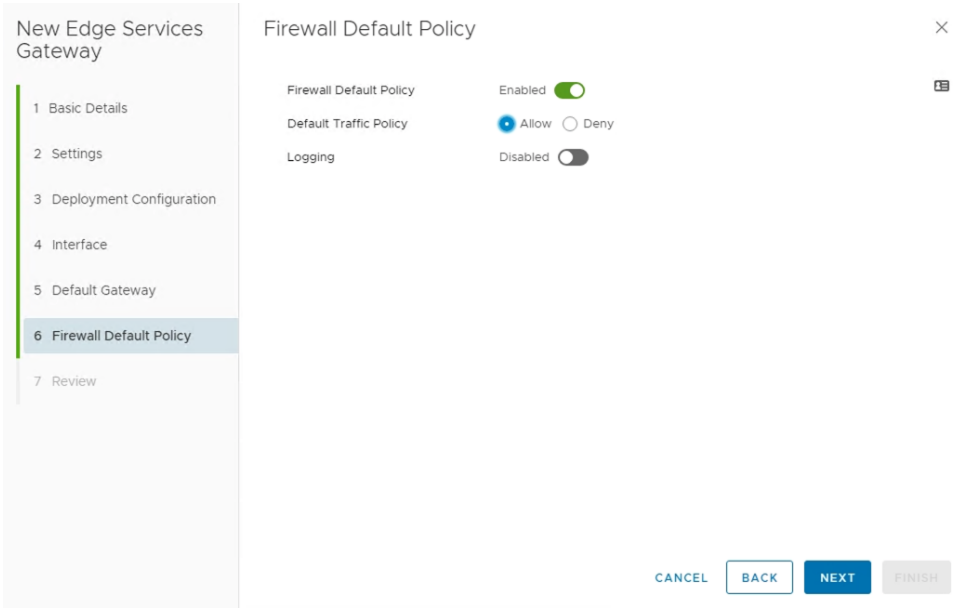
Table 3 NSX Edge network interfaces



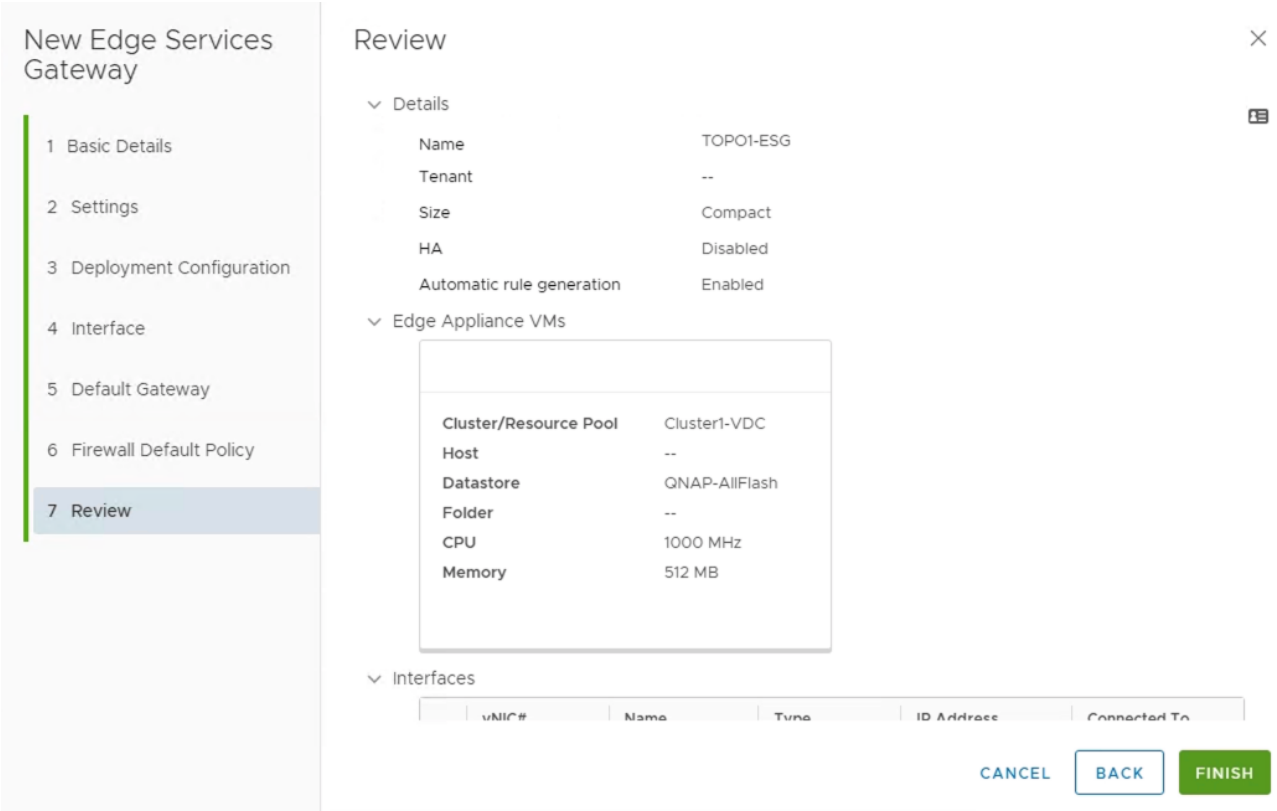
12. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway is our data center backbone router with the IP address of 10.105.176.1 on External vNIC that we configured under the interface settings. If asked, use the default MTU parameter 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. Enable the “Firewall Default Policy” and check Allow for the Default Traffic Policy. (This is for validation testing; firewall can be set to Deny instead however firewall rules will be required on ESG to allow for traffic to flow to/from ESG/DLR and F5).

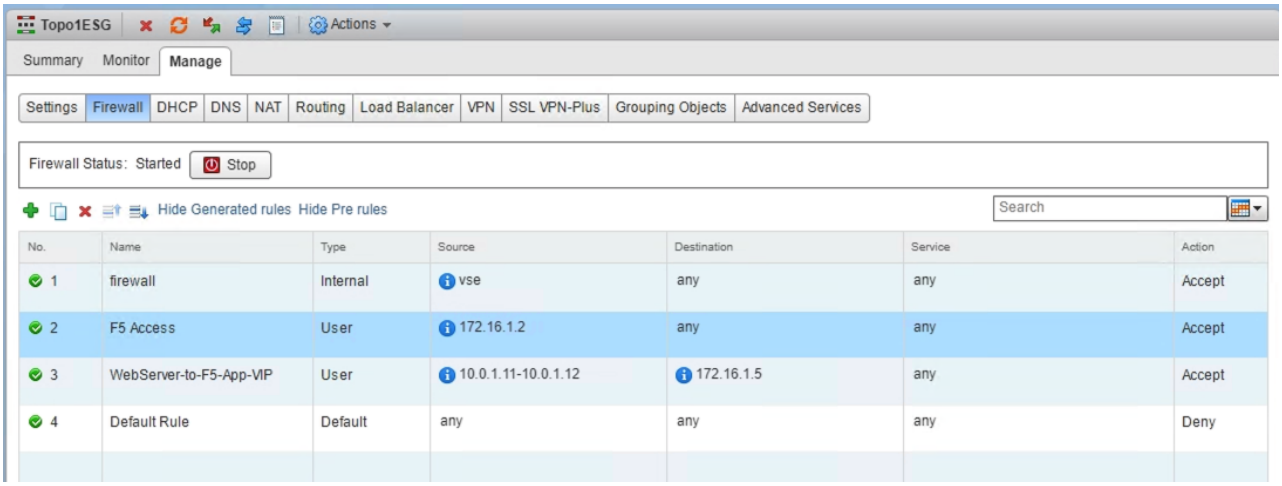


14. Review and click finish to complete the deployment of the NSX Edge.



15. If the Firewall was set to Deny (Currently can only be configured via vSphere Flex [FLASH] client) To configure firewall rules Home → Network and Security → NSX Edges → Double Click on Edge (Topo1ESG) → Firewall Tab.

    Adding Rules Click the (+) button and add appropriate firewall rules to allow Transits (Transit-1 and Transit-2) to communicate and the Networks for the F5 to access (Web Servers 10.0.1.11 & 10.0.1.12 in this use case).

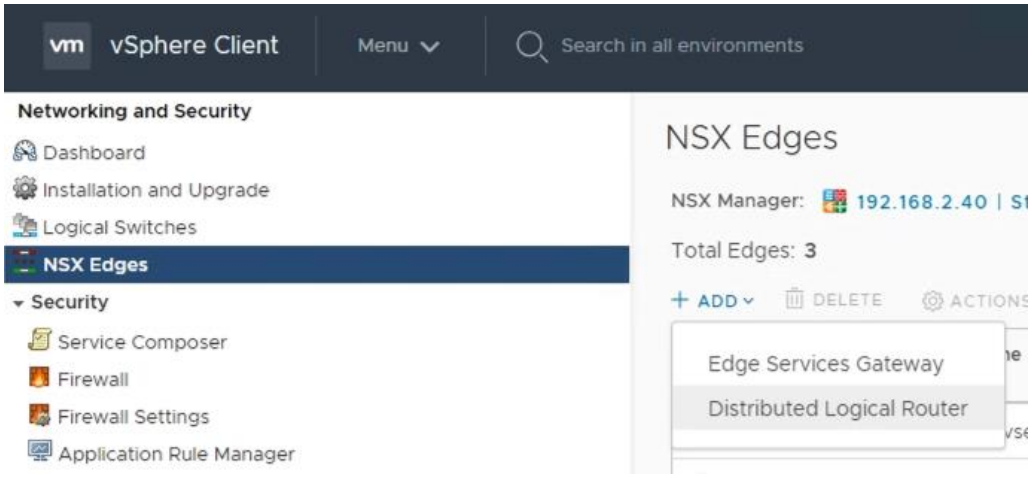


Create and Deploy DLR

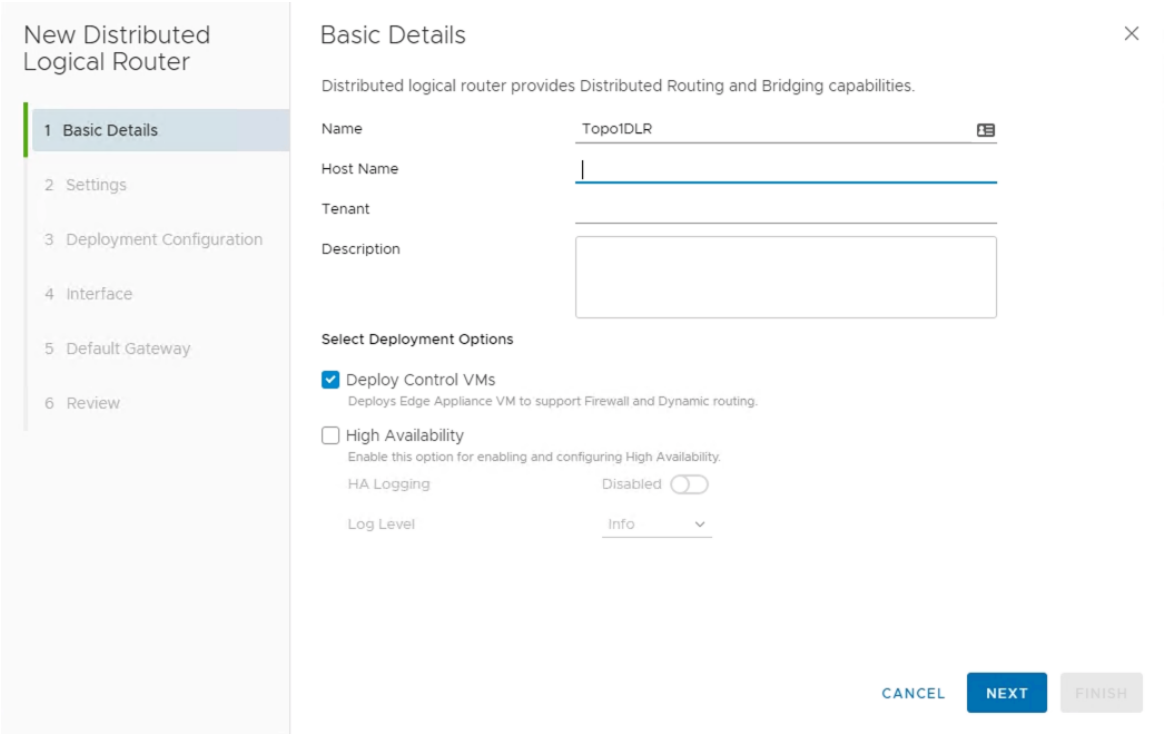
Within VMWare NSX, the Distributed Logical Router (DLR) provides an optimized way of handling east-west traffic within the data center. East-west traffic consists of communication between virtual machines or other resources on different subnets within a data center. As east-west traffic demand increases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

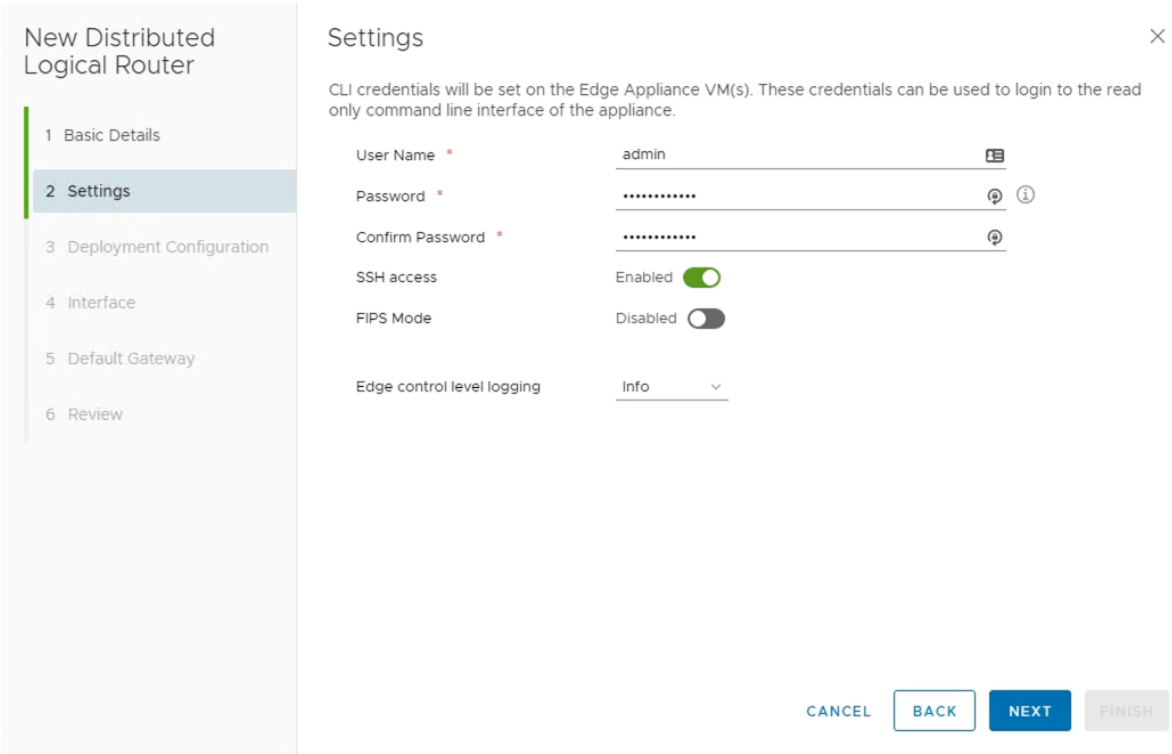
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection. Under Networking and Security, choose NSX Edges and then click (+ Add) hyperlink → Click on “Distributed Logical Router”.



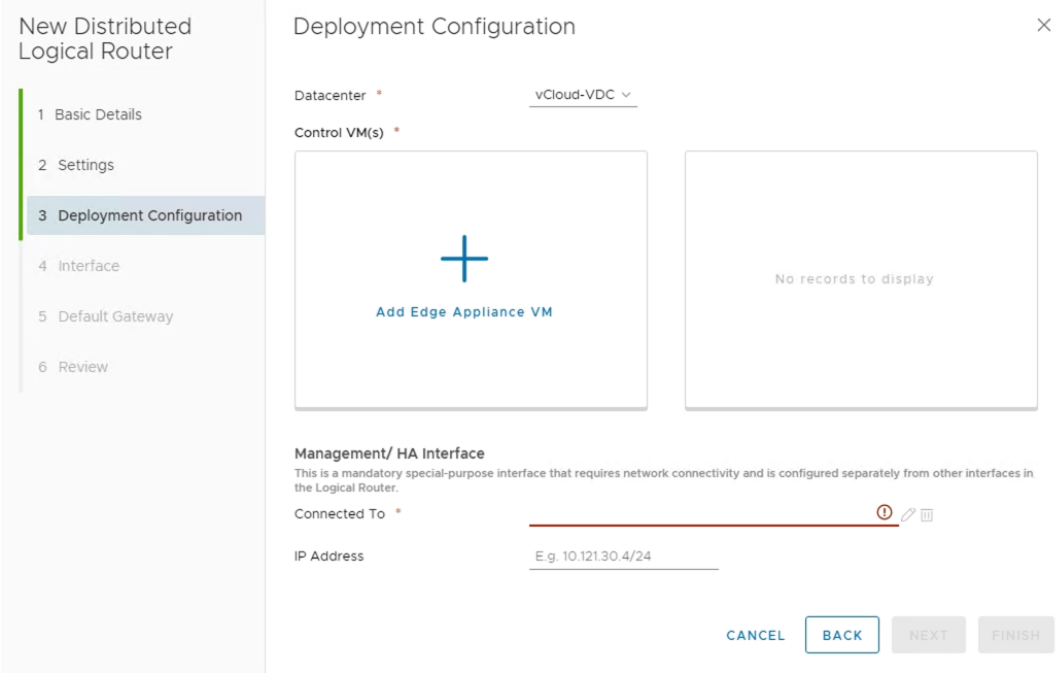
2. Provide a name for the device, then click next.



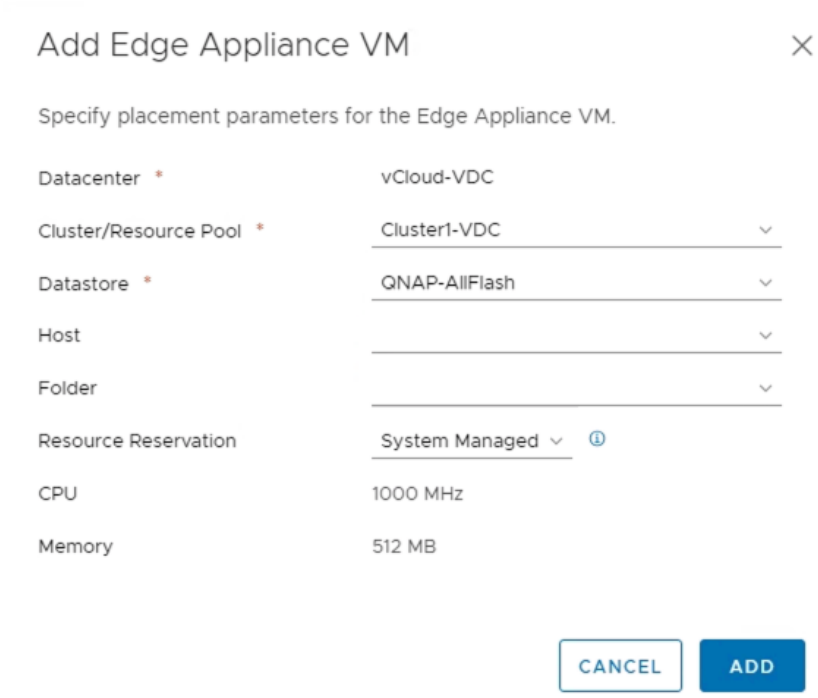
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.



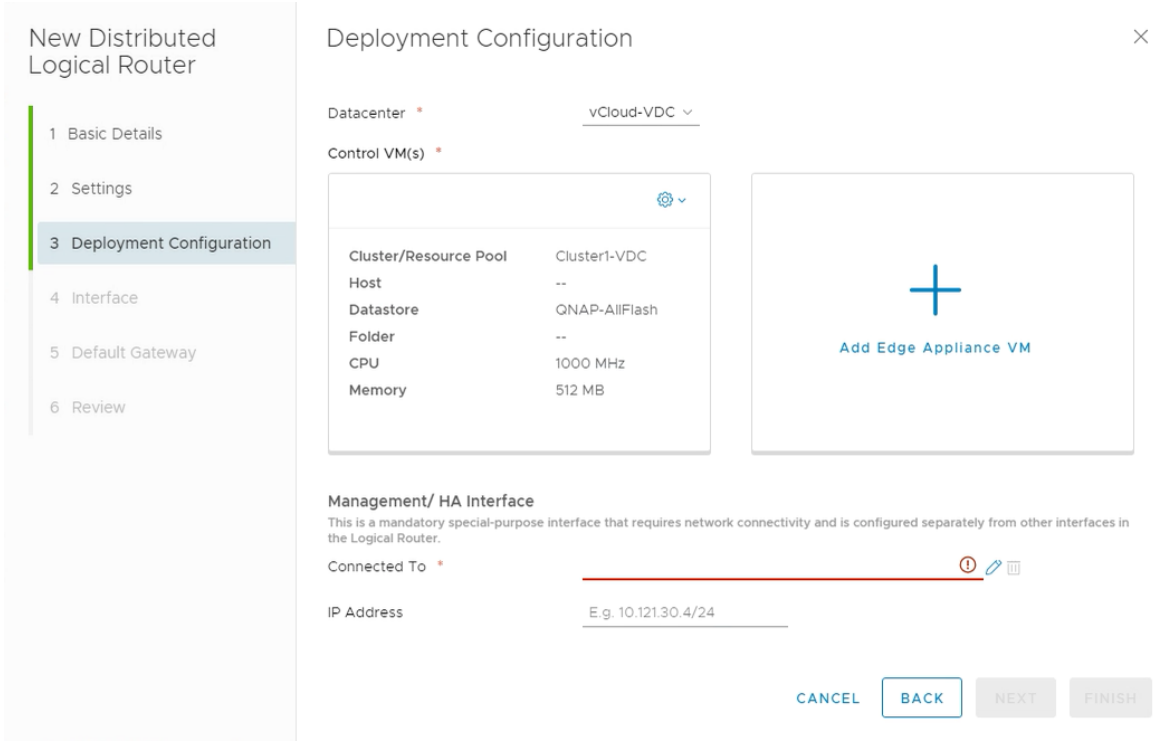
4. Under Configure deployment, select the Datacenter and Appliance Size appropriate for your deployment. Then click on the plus symbol (+) to Add Edge Appliance VM.



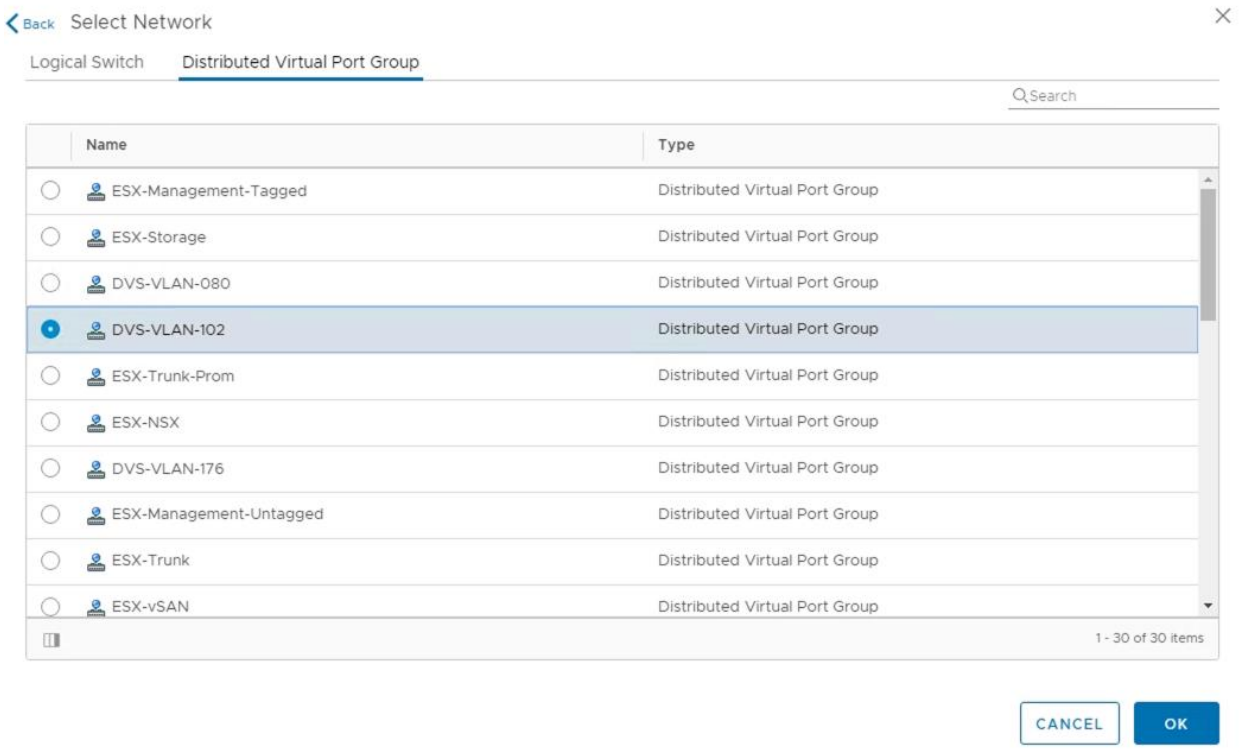
5. Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete.



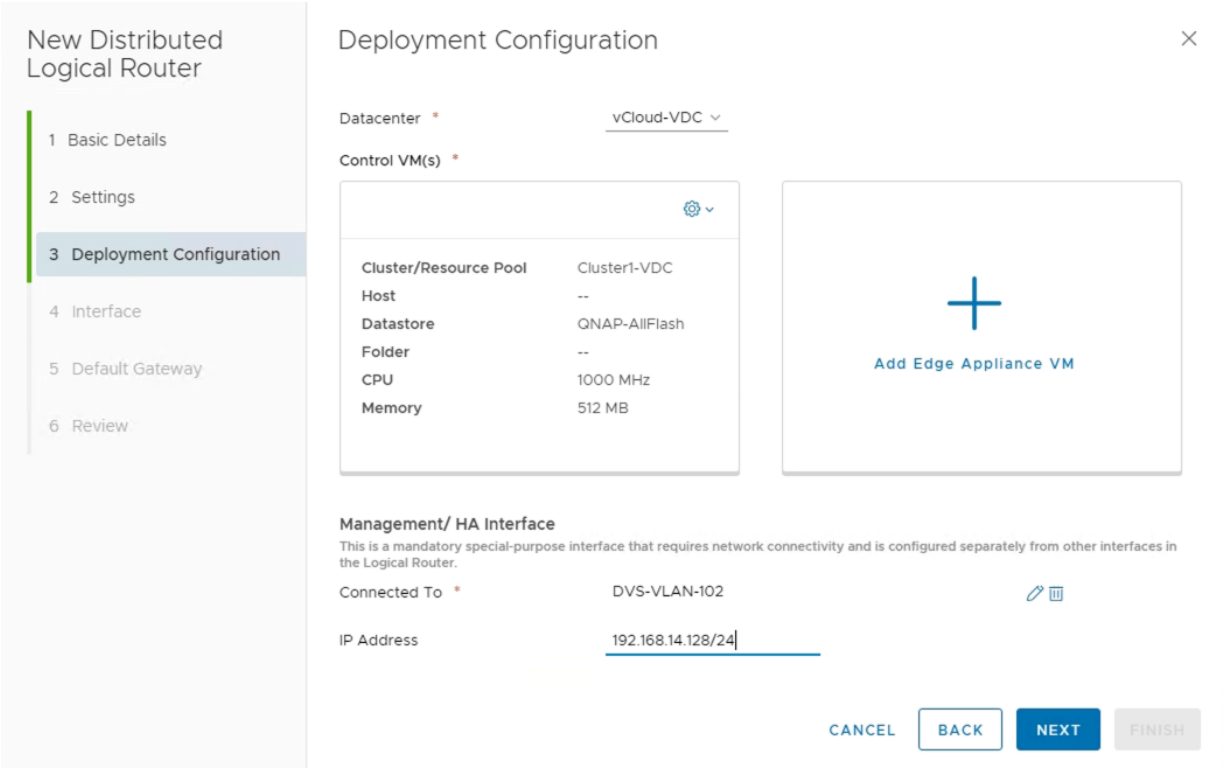
6. Click the Edit icon in the “Connected To” section of the Management/HA Interface.



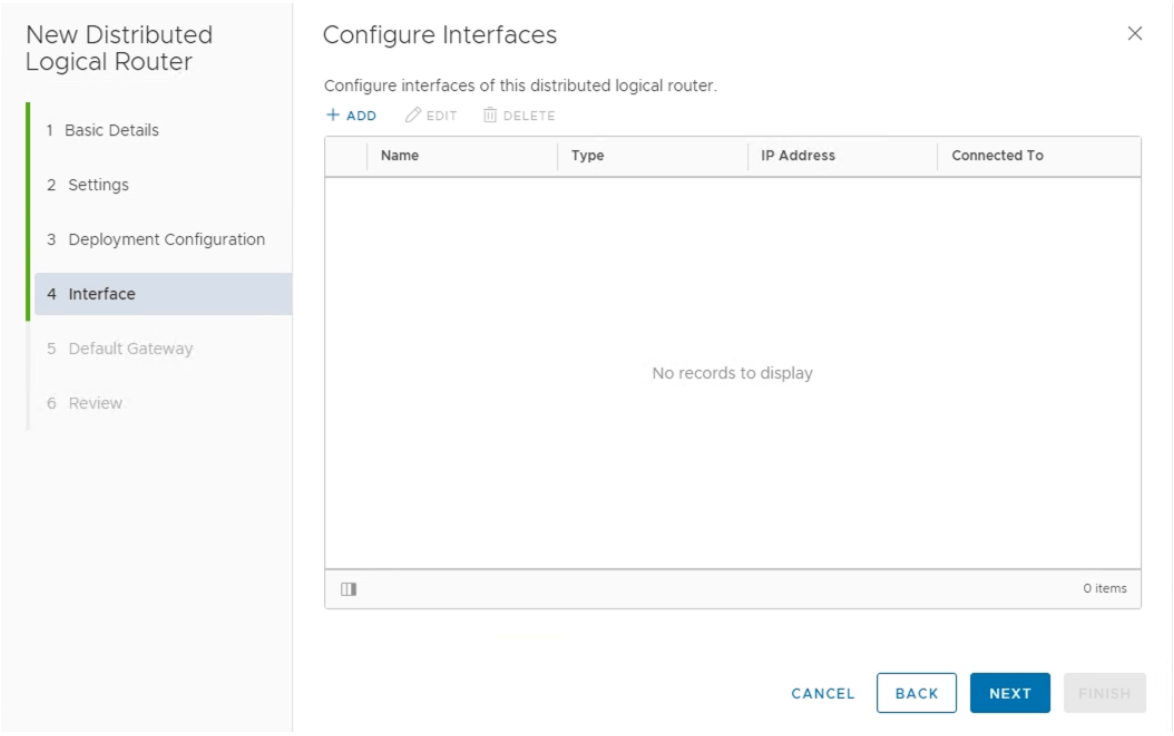
7. Select an appropriate Management Network (Distributed Virtual Port Group) to manage the DLR then Click OK.



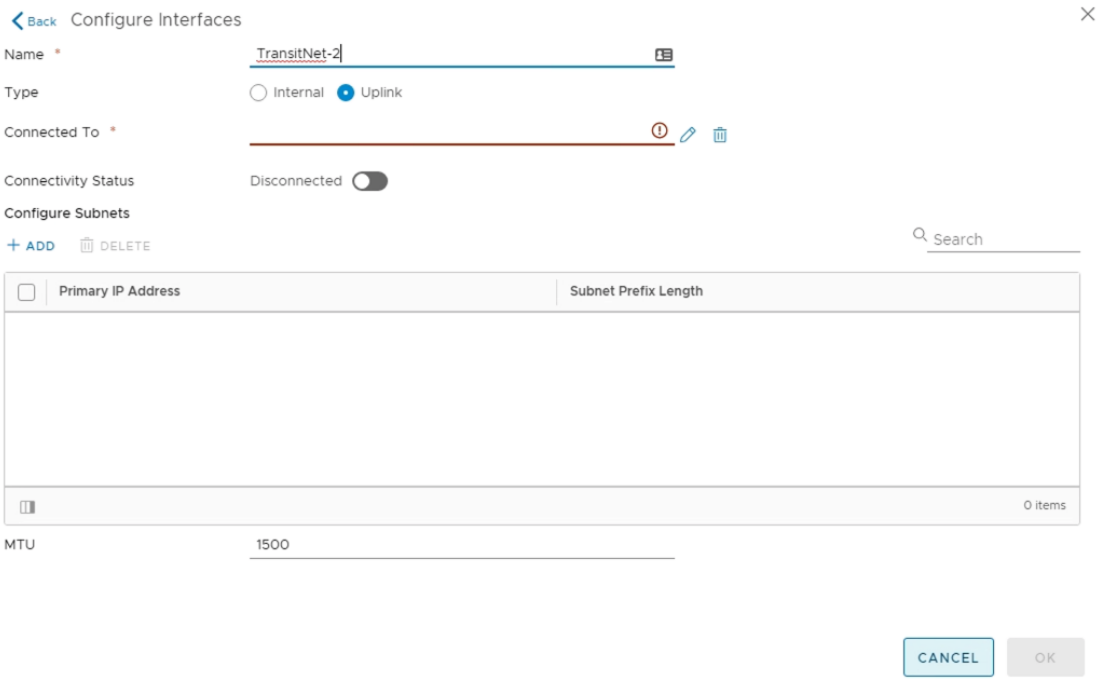
8. Fill out the IP/Subnet Field for the Management IP of the DLR then Click Next.



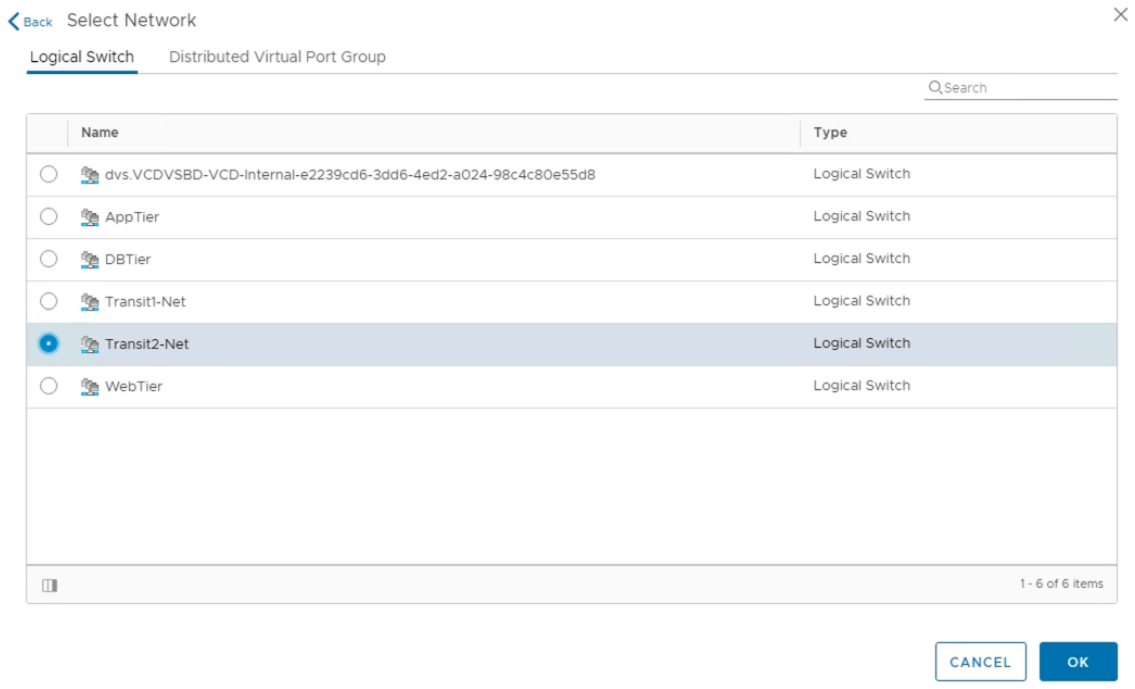
9. In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX DLR Interface dialog box.



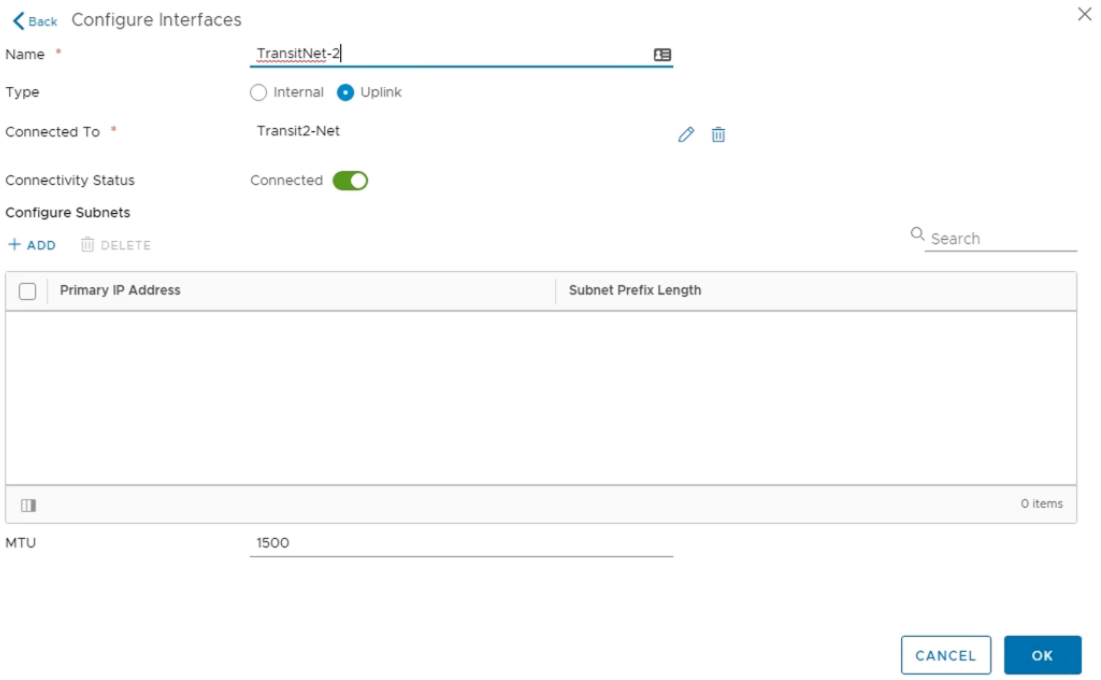
10. Provide a name and click the edit icon next to the “Connected To” field



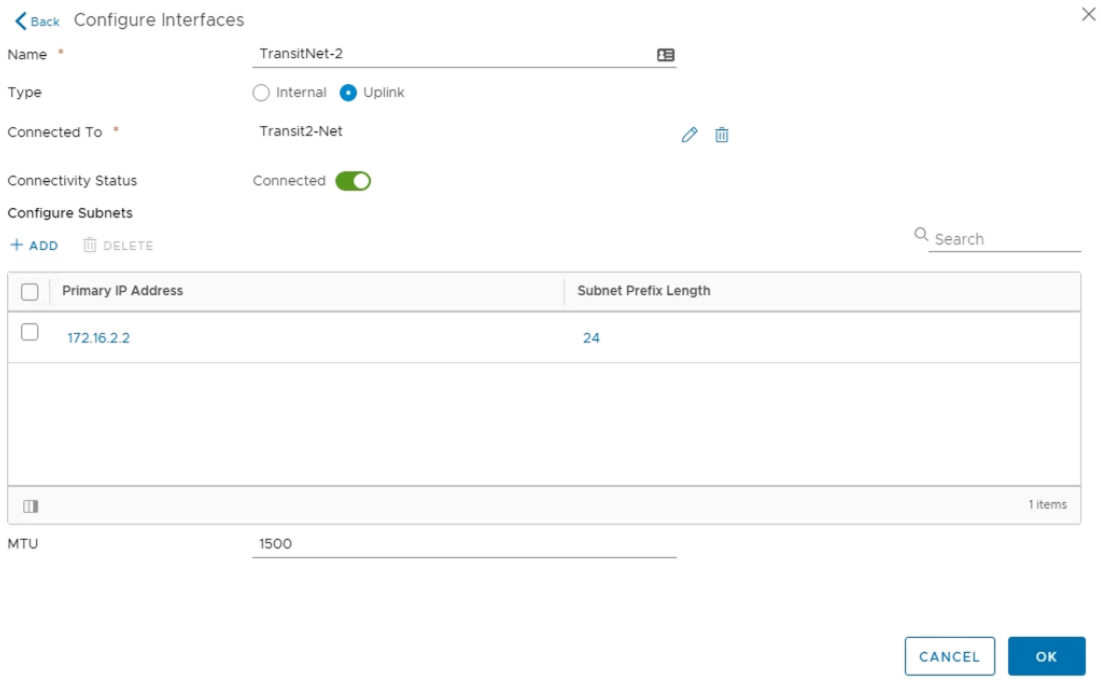
11. For the TransitNet-2 network, click on the Logical Switch tab and then selecting the TransitNet-2 Logical Switch. Click OK.



12. Once the network is chosen, select the (+ Add) hyperlink under Configure subnets to add the appropriate IP address and subnet configuration to the interface.



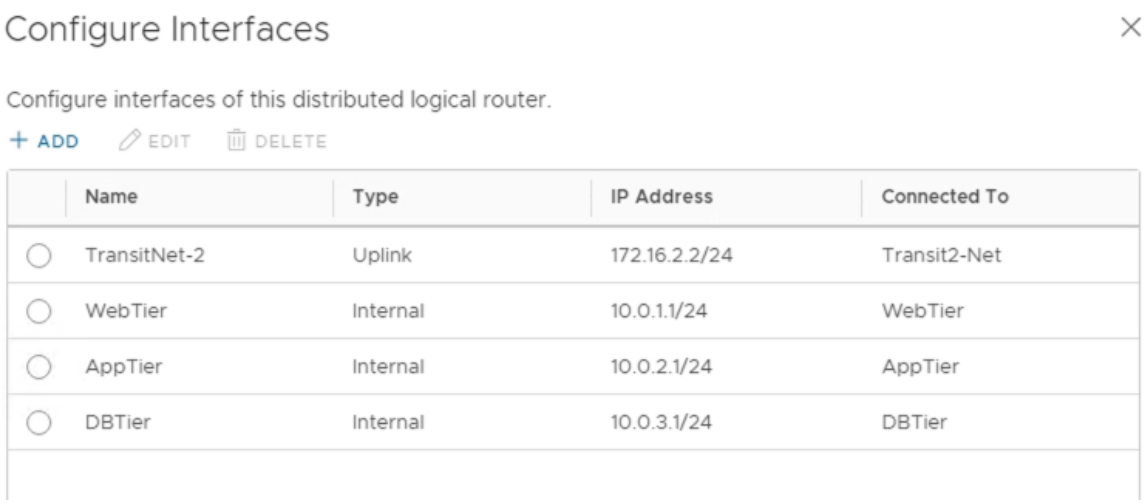
13. In the Add Subnet dialog box, enter the appropriate IP address and Subnet prefix length, and click OK.



14. This will bring you back to the Configure interfaces dialog box. For each of the four interfaces required for this deployment scenario, add and configure the appropriate subnets and switch type, according to the table below and look like the final picture below with your datacenter information.

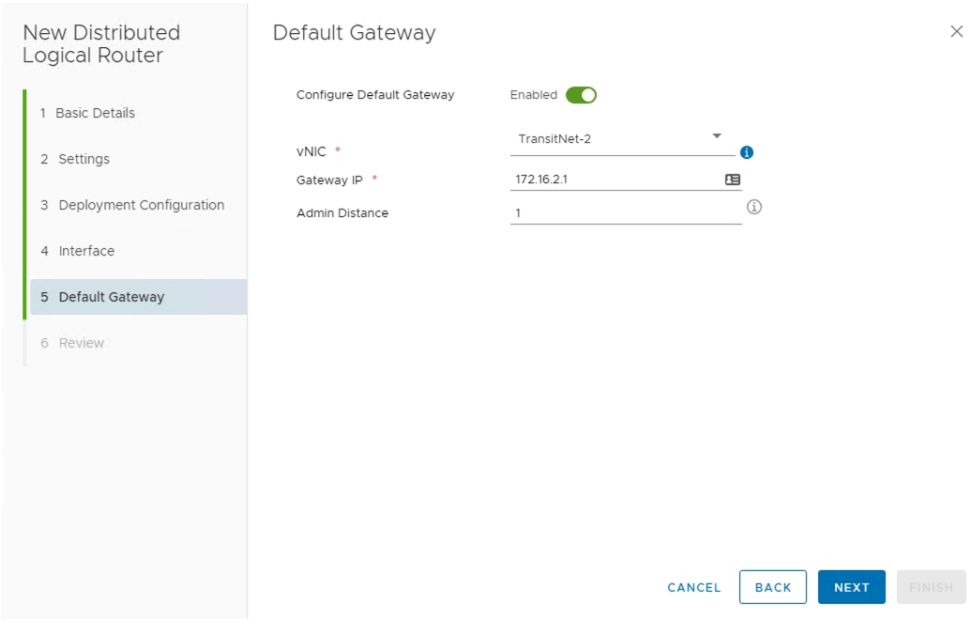
Network Name	Type	Network Type	IP Address	Connected To
TransitNet-2	Uplink	Logical Switch	10.105.176.2/24	Transit2-Net
WebTier	Internal	Logical Switch	10.0.1.1/24	WebTier
AppTier	Internal	Logical Switch	10.0.2.1/24	AppTier
DBTier	Internal	Logical Switch	10.0.3.1/24	DBTier

Table 4 NSX distributed logical router network interfaces

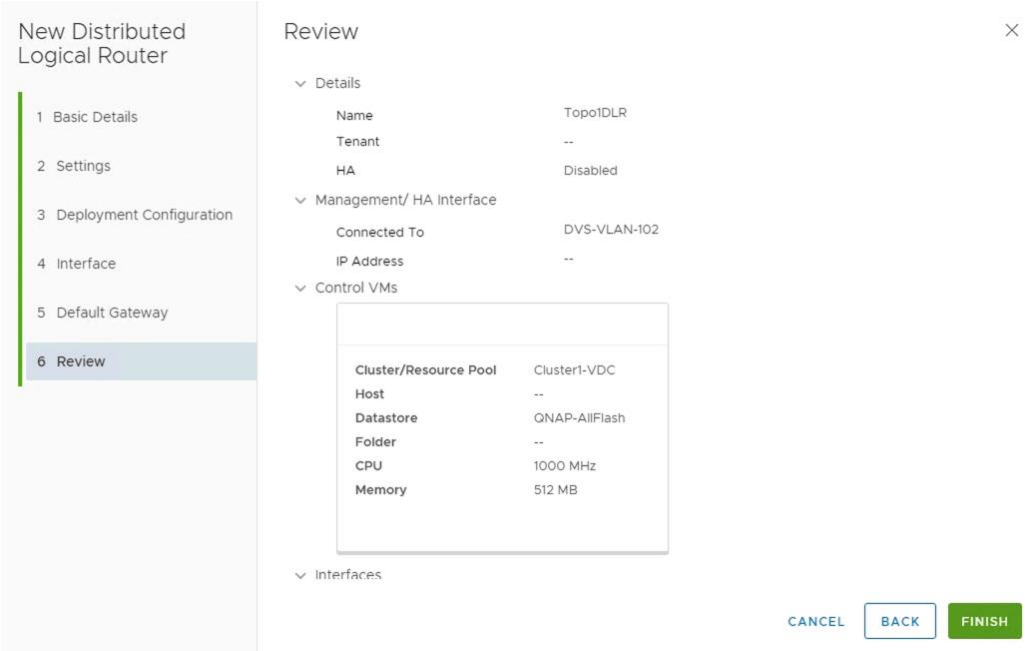


15. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway for the DLR is the data center core router that we configured in the previous section across the transit segment TransitNet-2.

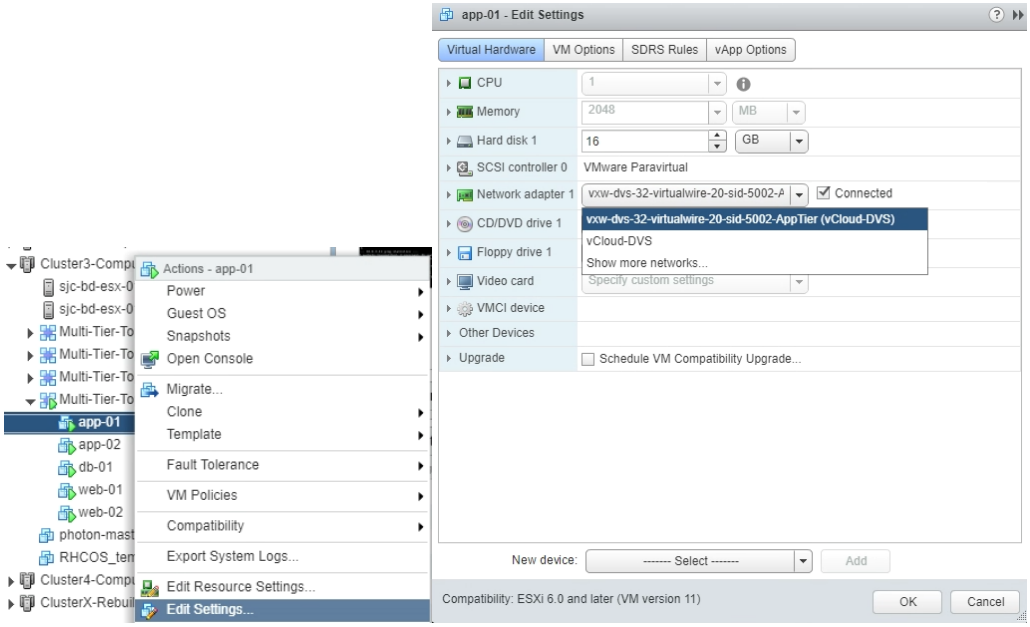
    For the vNIC select TransitNet-2 and provide the Gateway IP address of the NSX Edge.
    In this example, its 172.16.2.1 and (Admin Distance is Default at 1). Click Next to proceed.



16. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



17. After the Creation of the DLR and the logical switches within vSphere, attach the Virtual Machines for each tier to their logical switches for network traffic. (This is an example of one of our AppTier VM's attached to the AppTier Logical Switch.



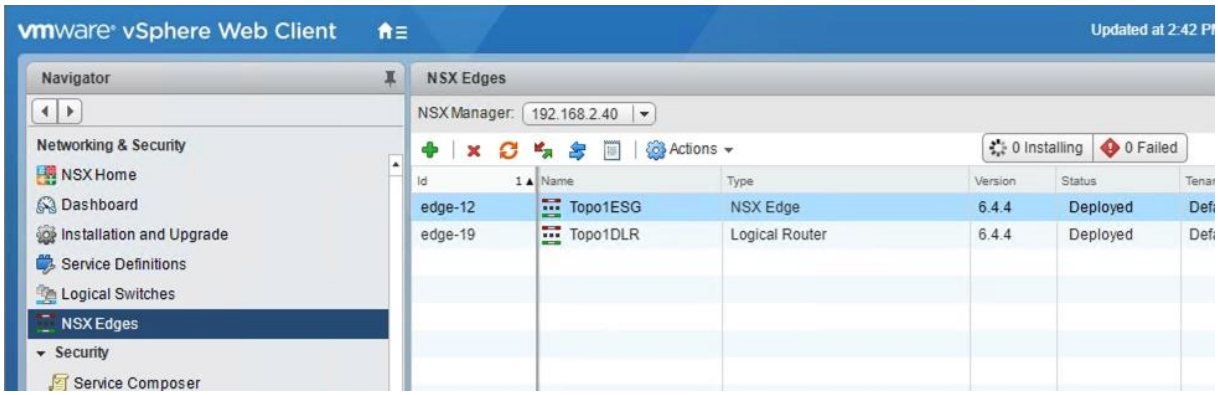
NSX Edge Static Routing Configuration

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.

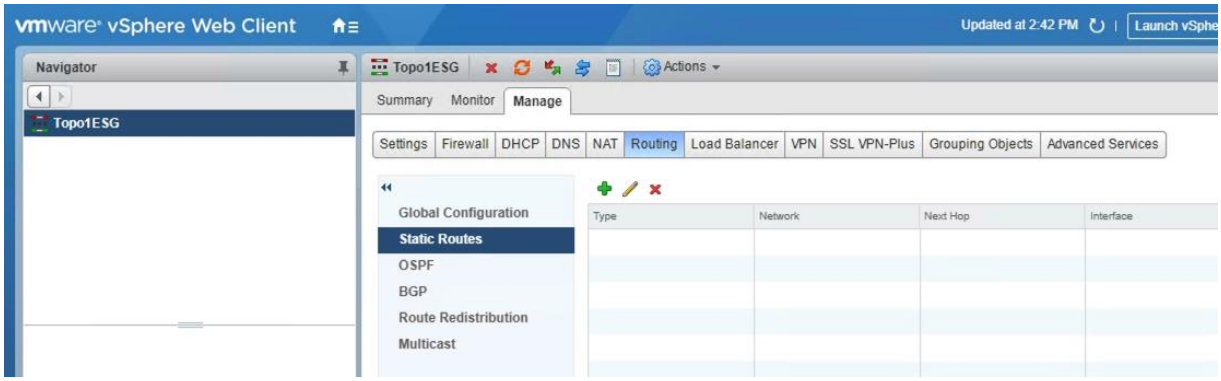
This configuration is also required to ensure that traffic coming from the external networks finds its way in.

1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then Double-click on the NSX Edge you configured in the first section. (In our use case this was named Topo1ESG).

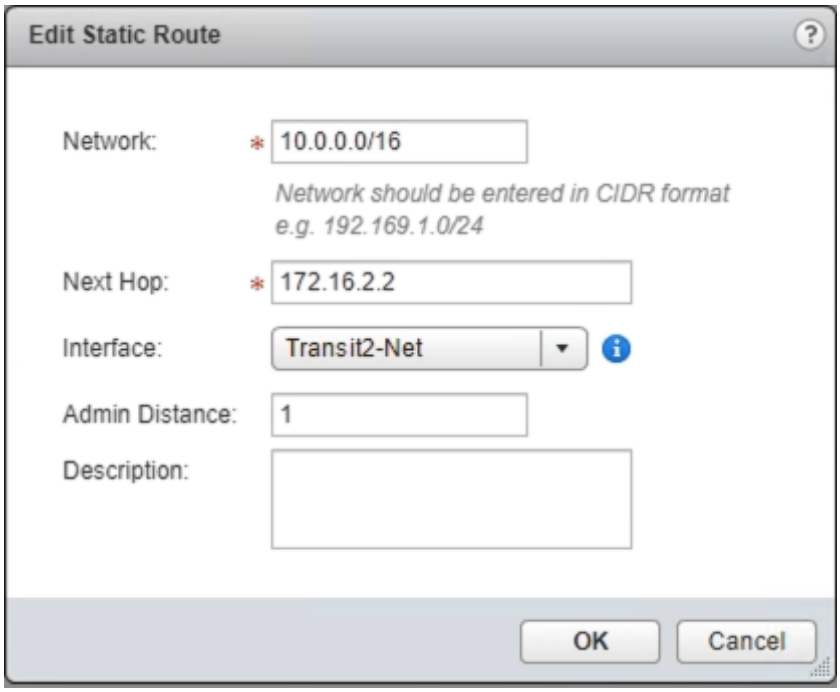
   Currently this must be done in the vSphere Web Client (FLEX) [Flash Based] as the functionality hasn’t been ported to the HTML5 Client.



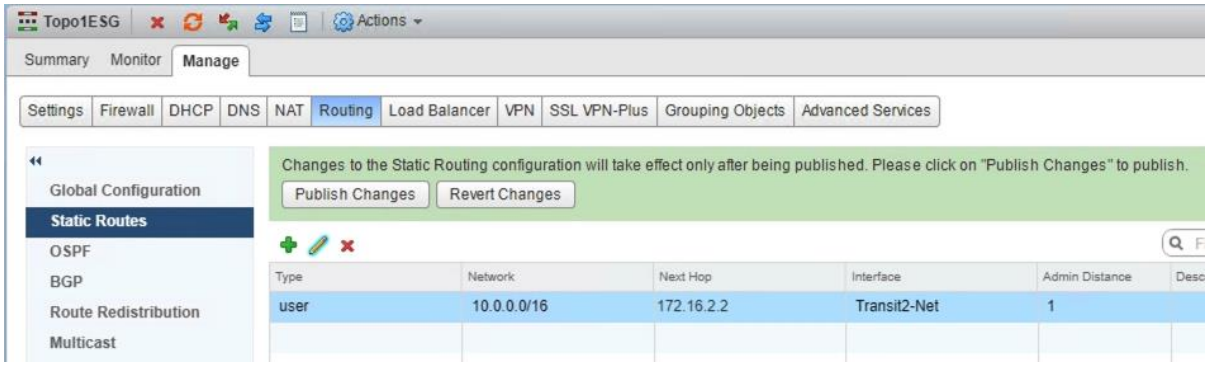
2. In the NSX Edge select the Manage Tab and the Routing sub-tab, then select Static Routes from the menus. Click on the (+) plus symbol to add a Static Route.



3. Provide an internal summary route that points the NSX Edge to the Transit2-Net 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.



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



BIG-IP 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.

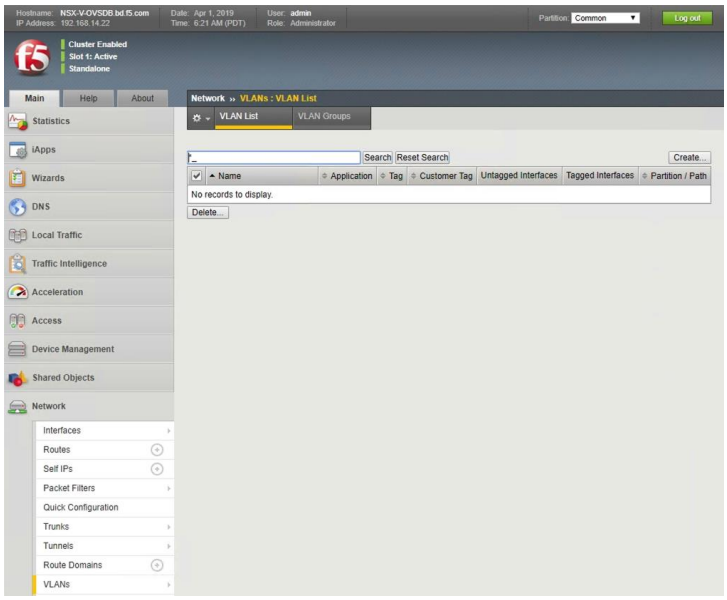
Prerequisites

- The BIG-IP is configured with a management IP address in the proper subnet on the management interface. In our specific use case this is VLAN 102.
- Licenses have been applied and activated.
- Appropriate provisioning of resources is complete.
- Base configuration of services DNS, NTP, SYSLOG, etc. are configured.
- BIG-IP Interface 1.1 or an available interface that is connected is wired to a physical or virtual switch (trunk) configured to support 802.1Q tagging of traffic. In our specific use case this is VLANs 176 and 177.

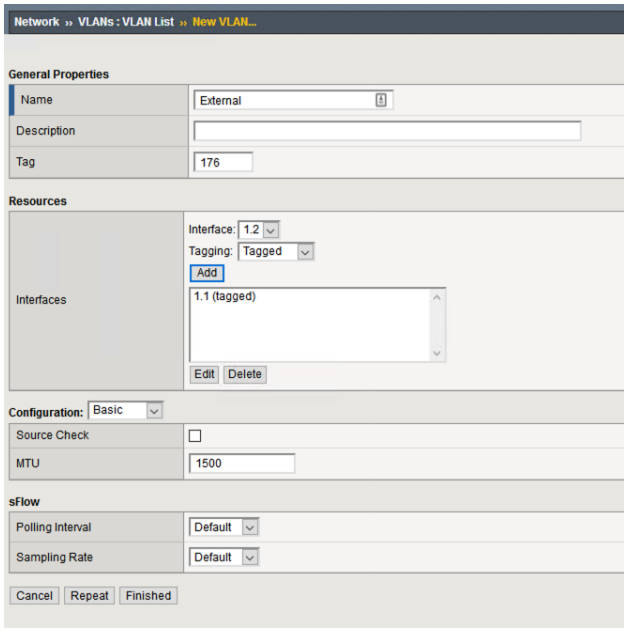
  For info on how to perform these installation and basic setup steps, refer to http://support.f5.com and consult the appropriate implementation guide for your version and device.

Create VLANs

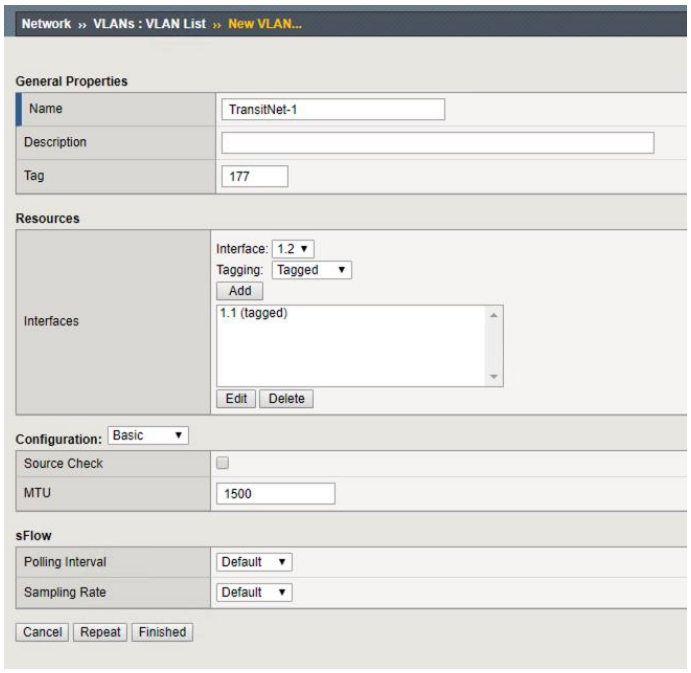
1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select VLANs.
2. In the upper right corner, click Create.



3. In the New VLAN menus.
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used External.
   b. In the Tag field, enter the External VLAN ID in this example, our VLAN is 176.
   c. Under Resources, for Interface, select 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and then click the Add button below it.
   e. Select Repeat to proceed with the creating of the transit network VLAN



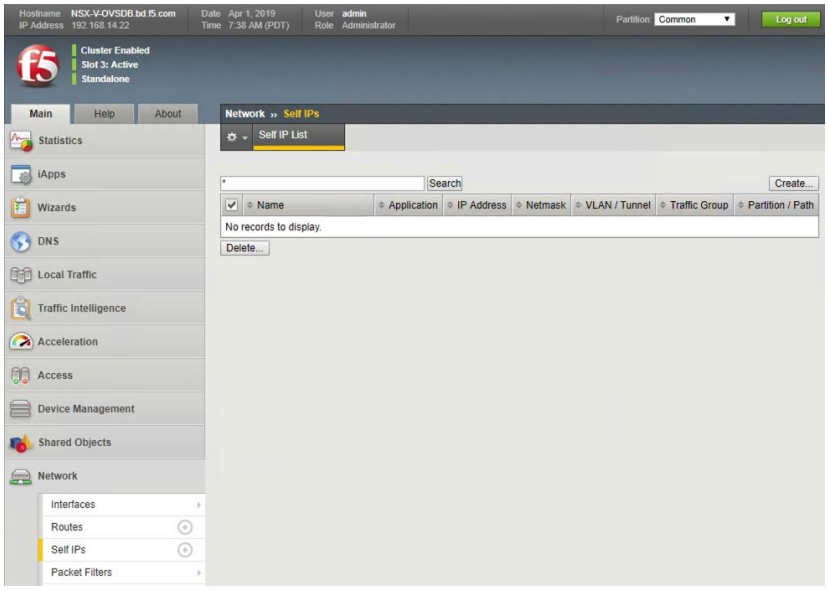
4. In the New VLAN Menus
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used TransitNet1.
   b. For the Tag, enter the TransitNet-1 VLAN ID in this example, our VLAN is 177.
   c. Under Resources, select the Interface 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and click the Add button below it.
   e. Select Finished to complete the VLAN creation.



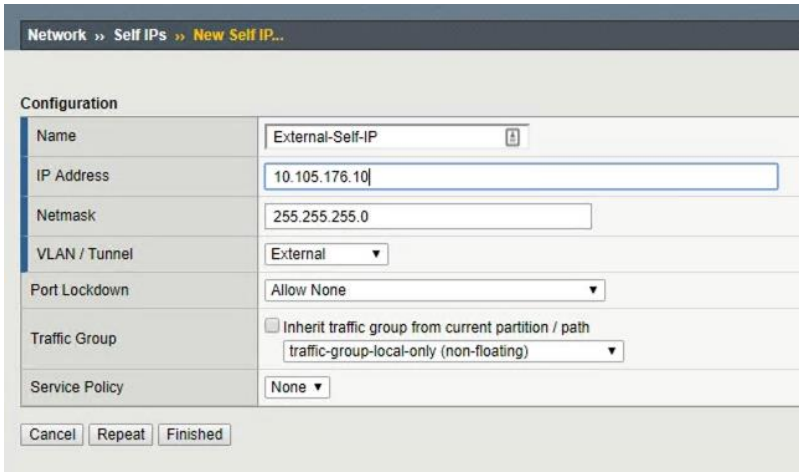
Configure Self IP Addresses

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.

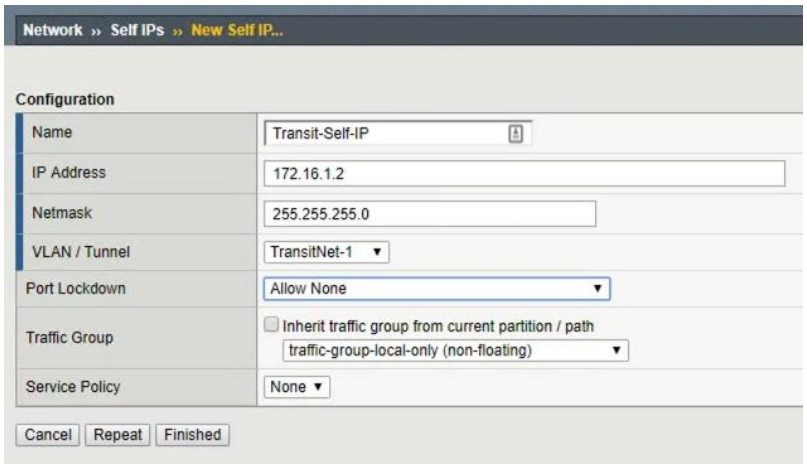
1. On the Main tab of the BIG-IP navigation pane, click Network and then click Self IPs.
2. In the upper right corner of the screen, click the Create button.

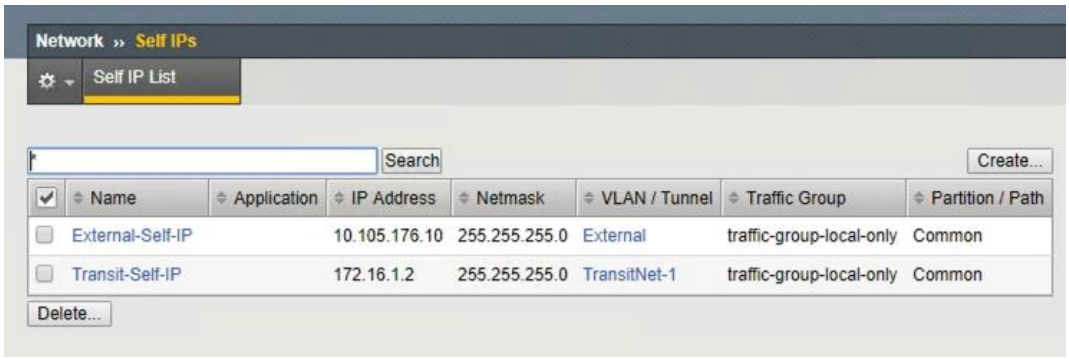


3. In New Self IP Menus
   a. Type a unique name in the Name box. In this example, we used “External-Self-IP” (without double quotes).
   b. In the IP address box, provide the IP address for the External network, in our example, we used 10.105.176.10.
   c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
   d. For the VLAN/Tunnel, select External from the dropdown box.
   e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
   f. Click the Repeat button to continue



4. In New Self IP Menus
   a. Type a unique name in the Name box. In this example, we used “Transit-Self-IP” (without double quotes).
   b. In the IP address box, provide the IP address for the External network, in our example, we used 172.16.1.2.
   c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
   d. For the VLAN/Tunnel, select TransitNet-1 from the dropdown box.
   e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
   f. Click the Finished to validate the completed self IP configurations.

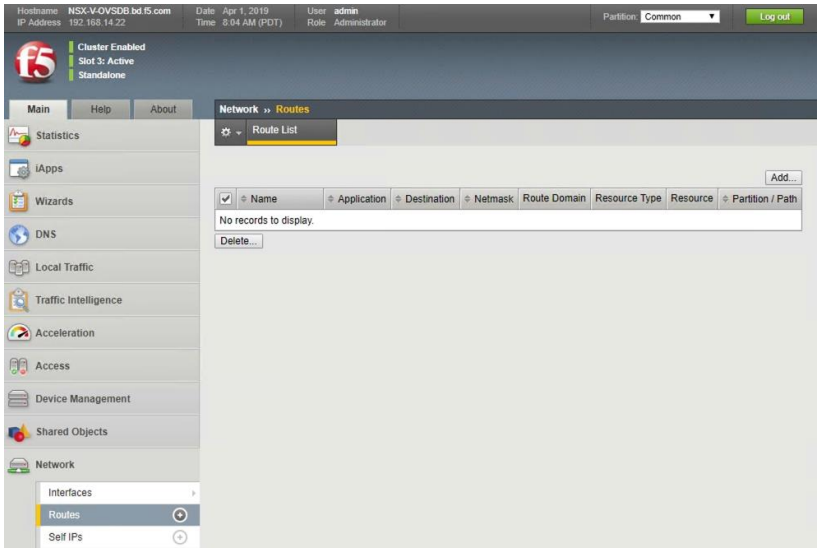




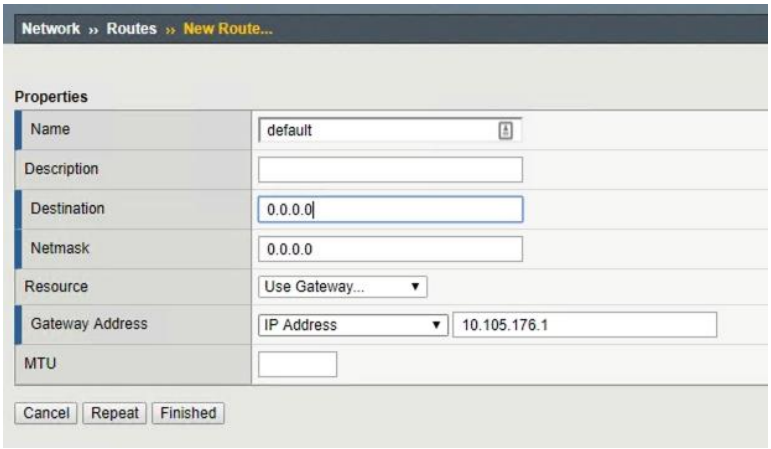
Configure Static Routes

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.

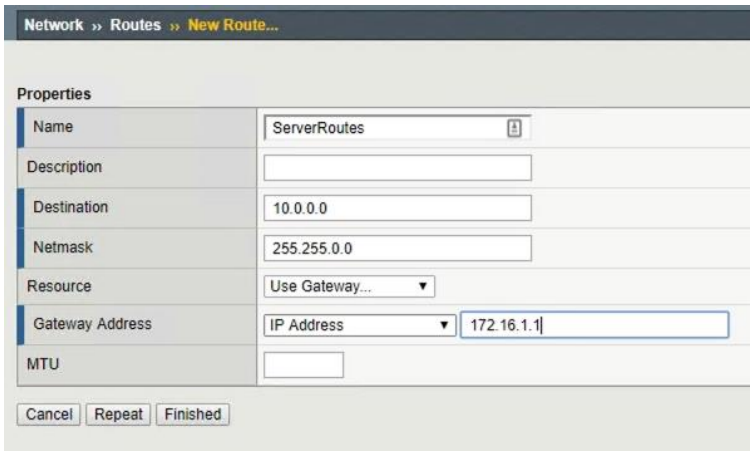
1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select Routes.
2. In the upper right corner of the screen, click the Ad button.

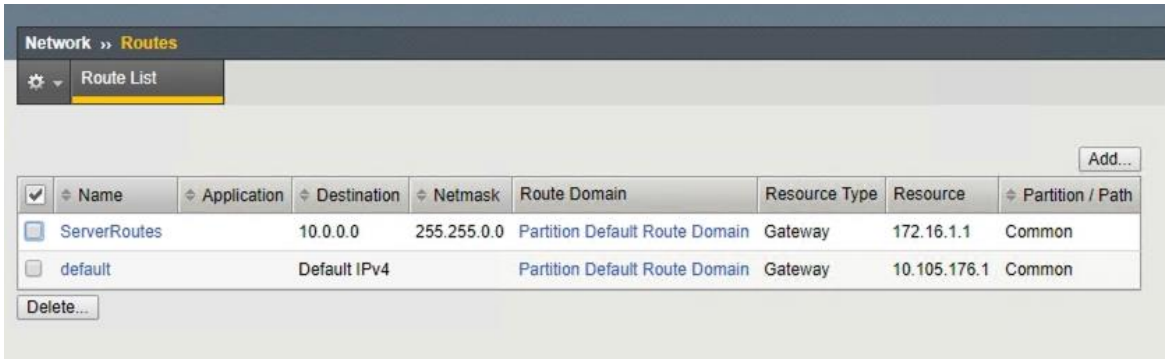


3. In the New Route menus
   a. For the Name, use the keyword default.
   b. The default route for both Destination and Netmask is 0.0.0.0.
   c. The Gateway Address is the address of the core router, in our example the core router's IP address is 10.105.176.1
   d. Click Repeat to complete and add the second router



4. In the New Route menus
   a. For the Name, in our example we used ServerRoutes.
   b. The Destination is 10.0.0.0.
   c. The Netmask is 255.255.0.0.
   d. The Gateway Address is the address of the core router, in our example the core router's IP address is 172.16.1.1
   e. Click the Finished to validate the created Static Routes.





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.

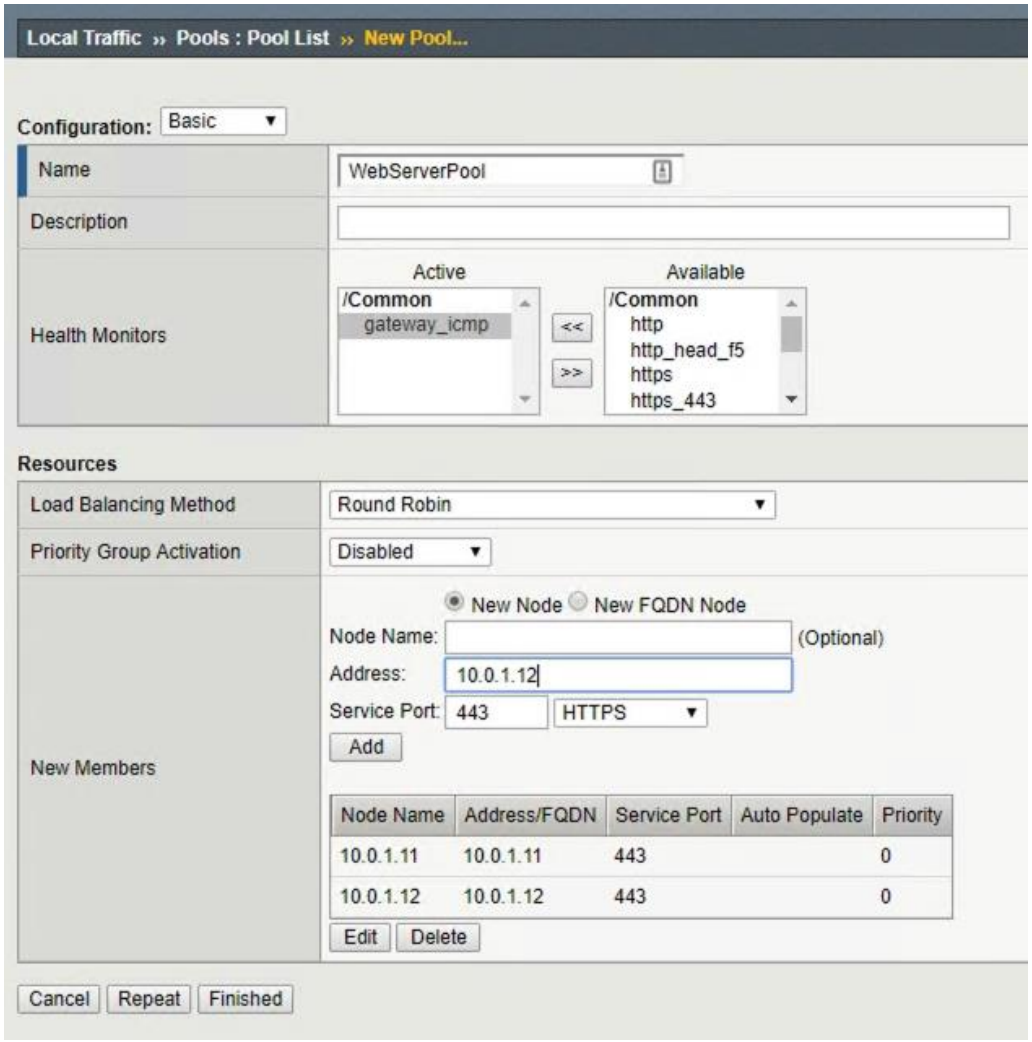
Create Application Pools

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 New Pool menus
    a. In the Name field, type a unique name for the web pool. For this validation, we used WebServerPool.
    b. 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.
    c. Under Resources, select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
    d. 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.
    e. Click Repeat to continue and enter the application tier information,

Name (Optional)	Address	Service Port
web-01	10.0.1.11	443 (HTTPS)
web-02	10.0.1.12	443 (HTTPS)

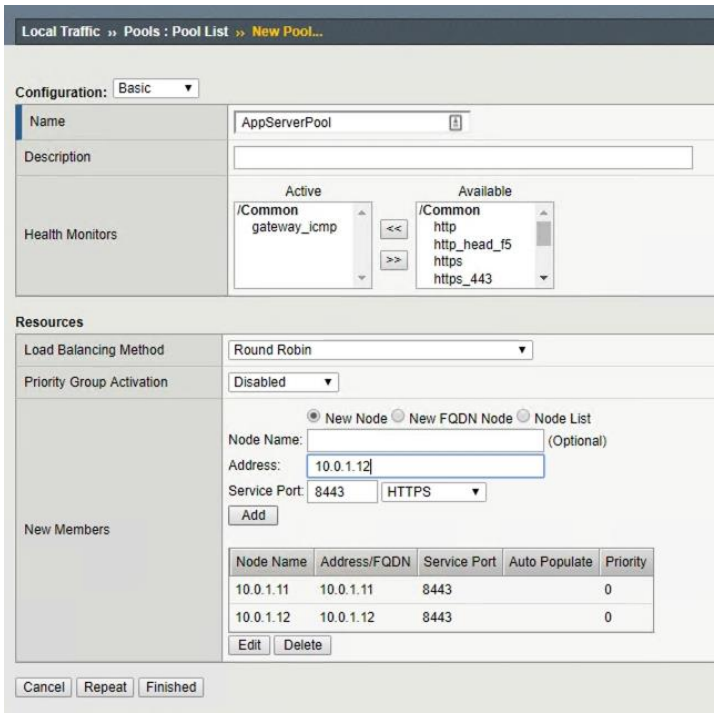
Table 5 BIG-IP web tier pool members


Local Traffic ›› Pools : Pool List ›› New Pool...
Configuration: Basic
Name
WebServerPool
Description
Health Monitors
Active
/Common
gateway_icmp
<<
>>
Available
/Common
http
http_head_f5
https
https_443
Resources
Load Balancing Method
Round Robin
Priority Group Activation
Disabled
New Members
New Node
New FQDN Node
Node Name:
(Optional)
Address:
10.0.1.12
Service Port:
443
HTTPS
Add
Node Name
Address/FQDN
Service Port
Auto Populate
Priority
10.0.1.11
10.0.1.11
443
0
10.0.1.12
10.0.1.12
443
0
Edit
Delete
Cancel
Repeat
Finished

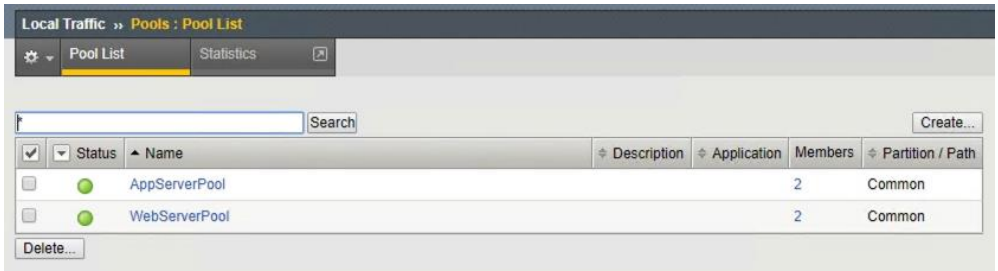
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
   a. In the Name field, type a unique name for the web pool. For this validation AppServerPool was used.
   b. In the Health Monitors section, select an appropriate monitor for your application. 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.
   c. In the Resources section of the screen, select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
   d. 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.
   e. Click Finished to complete the pool creation.

Name (Optional)	Address	Service Port
app-01	10.0.2.11	8443
app-02	10.0.2.12	8443

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.

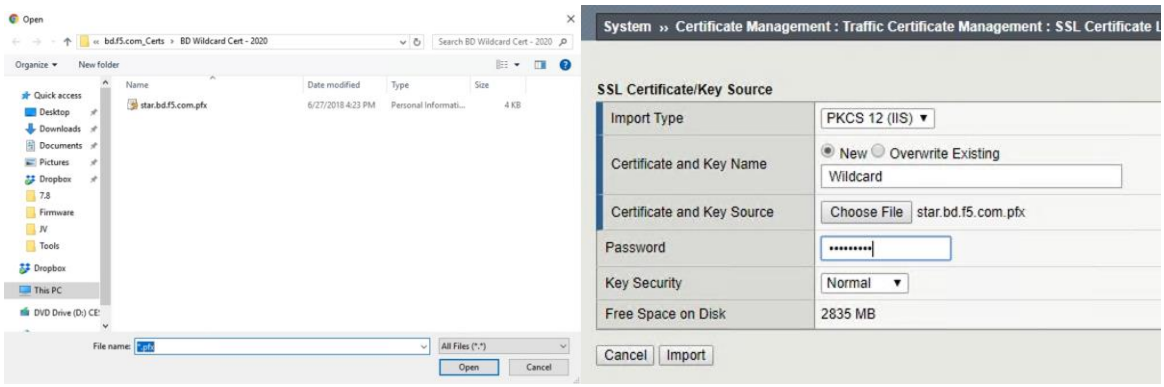


Import SSL Certificate

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

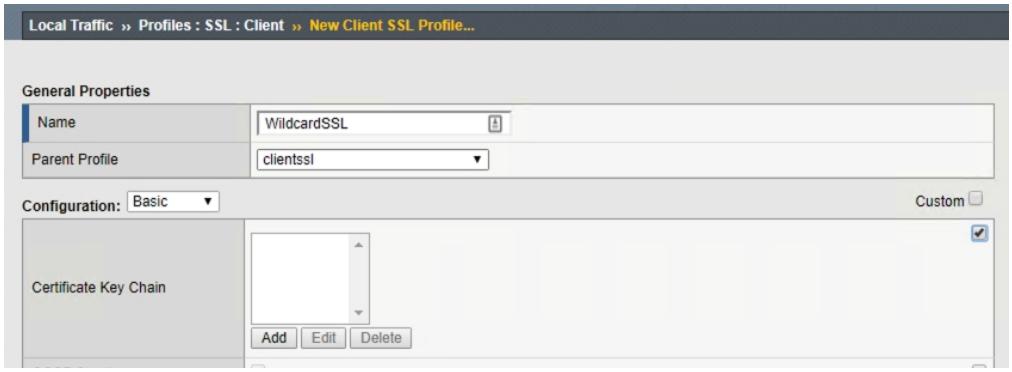
As a prerequisite to completing this task you must have a Certificate with a Private Key (Exportable) available to install this could be in Certificate/Key format or PKCS12 (PFX) format. In our test case, we will be using a public PKCS12 certificate (PFX) wildcard certificate "*.bd.f5.com" that will allow any DNS name in front of bd.f5.com to be accepted as valid name in a web browser.

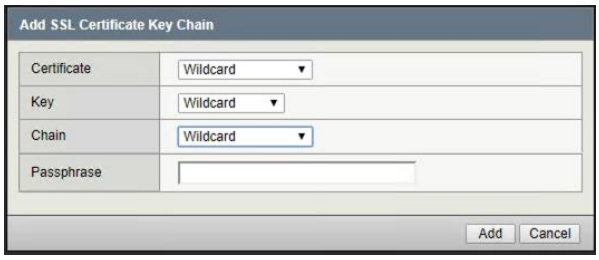
1. On the Main tab, select System → Traffic Certificate Management → SSL Certificate List
2. In the upper right corner of the screen, click the Import button.
3. Enter the following in the Import SSL Certificate and Keys menu
    a. In the Import Type field, in our example we select "PKCS 12 (IIS)"
    b. In the Certificate and Key Name field, in our example we entered "Wildcard" without quotes
    c. In the Certificate and Key Source field, select the "Choose File" button
    d. In the pop out menus browse and select the file, in our example star.bd.f5.com.pfx
    e. In the password field, enter the password to decrypt the pfx file.
    f. Click the Import button

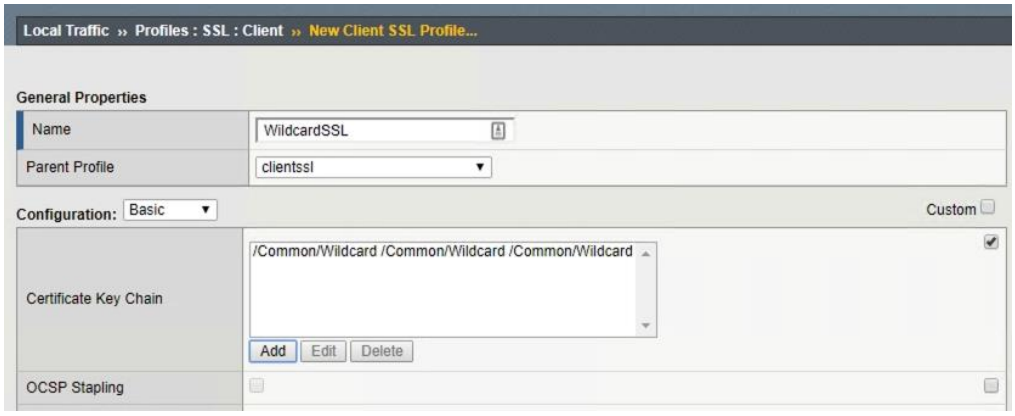


Create ClientSSL Profile

1. On the Main tab, select Local Traffic → Profiles → SSL → Client
2. In the upper right corner of the screen, click the Create button.
3. In the New Client SSL Profile menus
    a. In the Name field, type a unique name for the profile, for this validation WildcardSSL was used.
    b. In the Certificate Key Chain field, check the custom box and click the Add button
    c. In the Certificate, Key and Chain pulldown menus, select the previously imported Certificate chain, in this validation it was named Wildcard. Then click the Add button.
    d. Once added, scroll to the bottom and click the finished button.



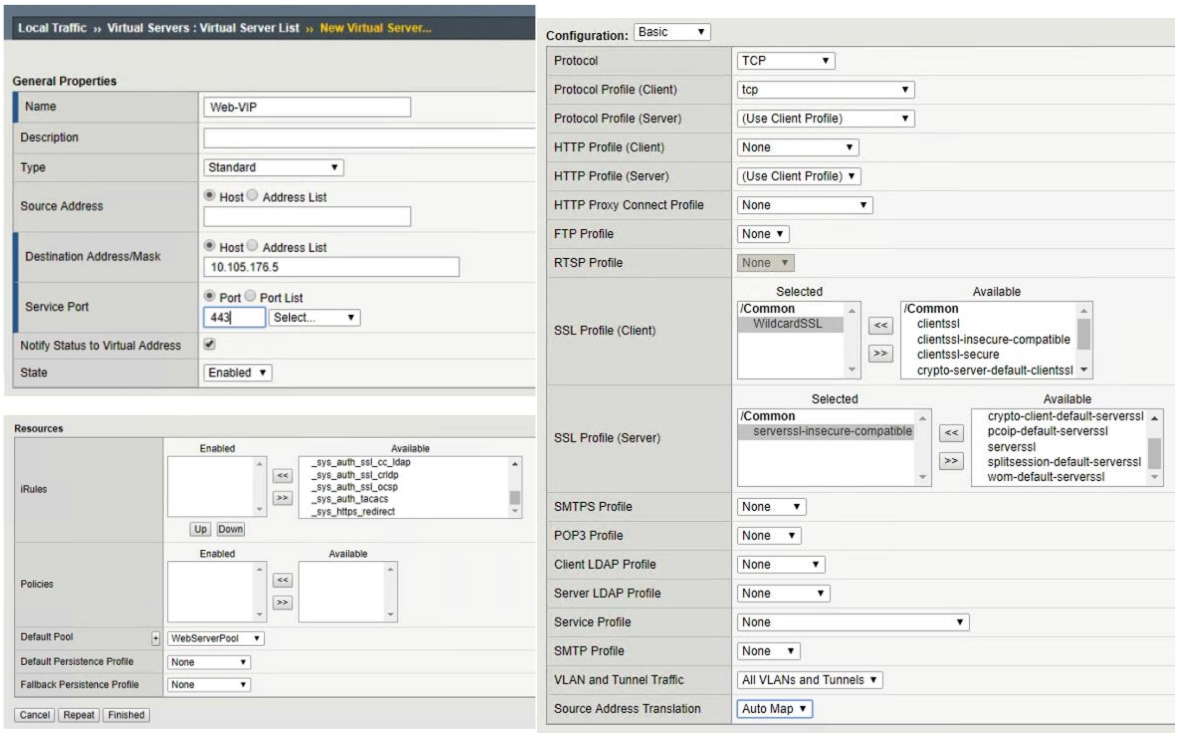




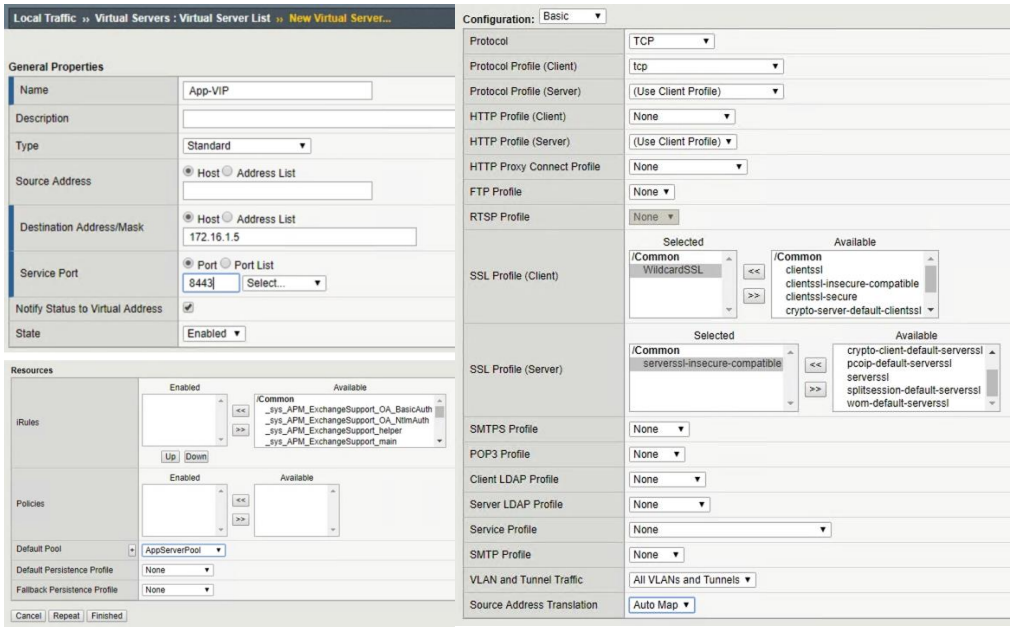
Create Application Virtual Servers

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 10.105.176.0/24 segment, and the other for the application tier, available on the TransitNet-1 segment (172.16.1.0/24).

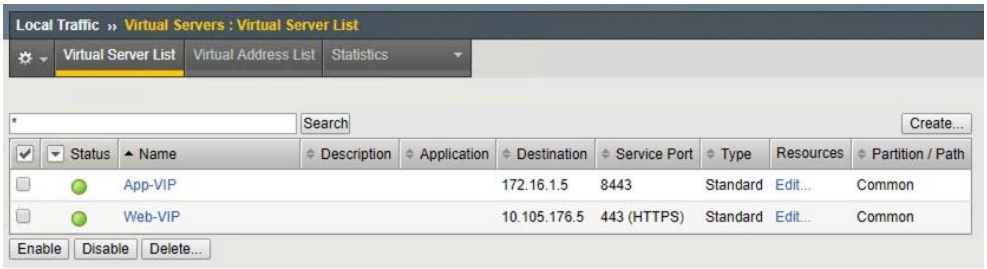
1. On the Main tab, select Local Traffic and then click Virtual Servers. The Virtual Server List screen is displayed.
2. In the upper right corner of the screen, click the Create button.
3. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the web application. In this case, we used Web-VIP.
    b. In the Destination Address field, enter 10.105.176.5
    c. For Service Port use the standard HTTPS port 443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the WebServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Repeat to continue configuring the application tier virtual server



4. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the web application. In this case, we used App-VIP.
    b. In the Destination Address field, enter 172.16.1.5
    c. For Service Port use the standard HTTPS port 8443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the AppServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Finished to continue configuring the application tier virtual server



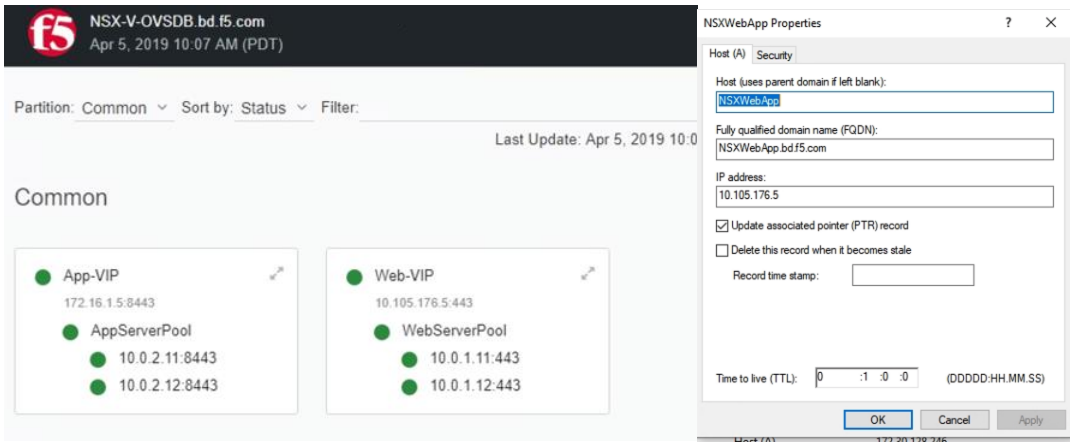
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.



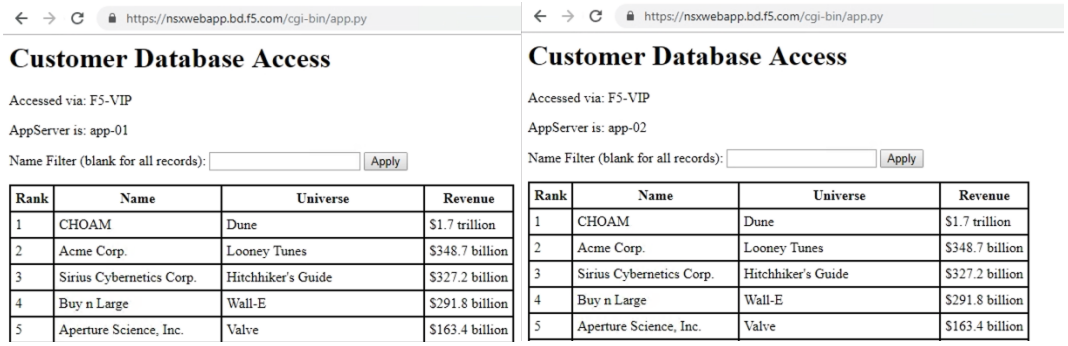
Validation

The web tier virtual server should now be available and accepting application traffic on port 443 (HTTPS).

On the Main tab, expand Local Traffic and then click Network Map to display the overall health of the applications and their associated resources. Due to also this traffic being HTTPS rather than HTTP we created a DNS A record using the FQDN of NSXWebApp.bd.f5.com to allow our wildcard certificate to be validated when connecting to the site.



Any web browser can be used to test by typing https://NSXWebApp.bd.f5.com/cgi-bin/app.py to send a request to the virtual server. Our 3-tier application will appear and show data within the database validating that the connection works, to further validate which application server you can refresh the page and see the AppServer changes. To further validate which Web server is being used we run a curl command “curl -kv “https://nsxwebapp.bd.f5.com” in the web server we injected a header in the web server configuration (not shown in this guide) called X-Upstream-Server to show which web server was being accessed.



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

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

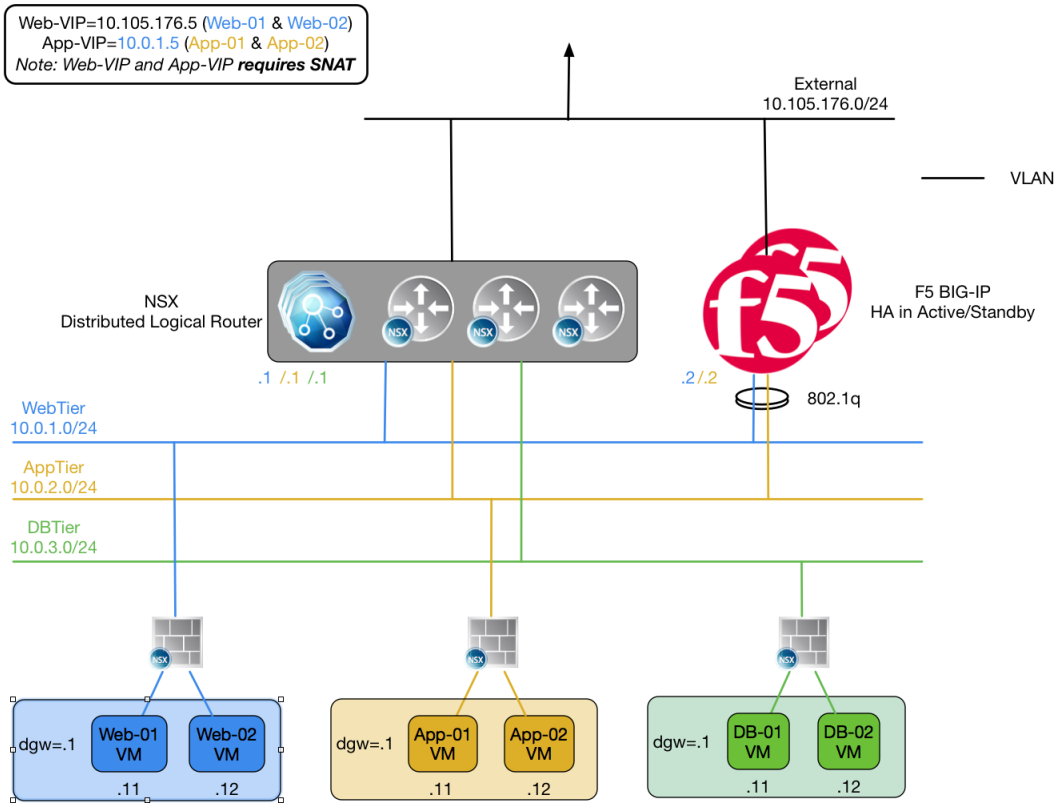


Figure 5 BIG-IP appliance parallel to NSX Distributed Logical Router

The second deployment scenario also utilizes a topology with a second data path for application delivery traffic. BIG-IP's 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 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.

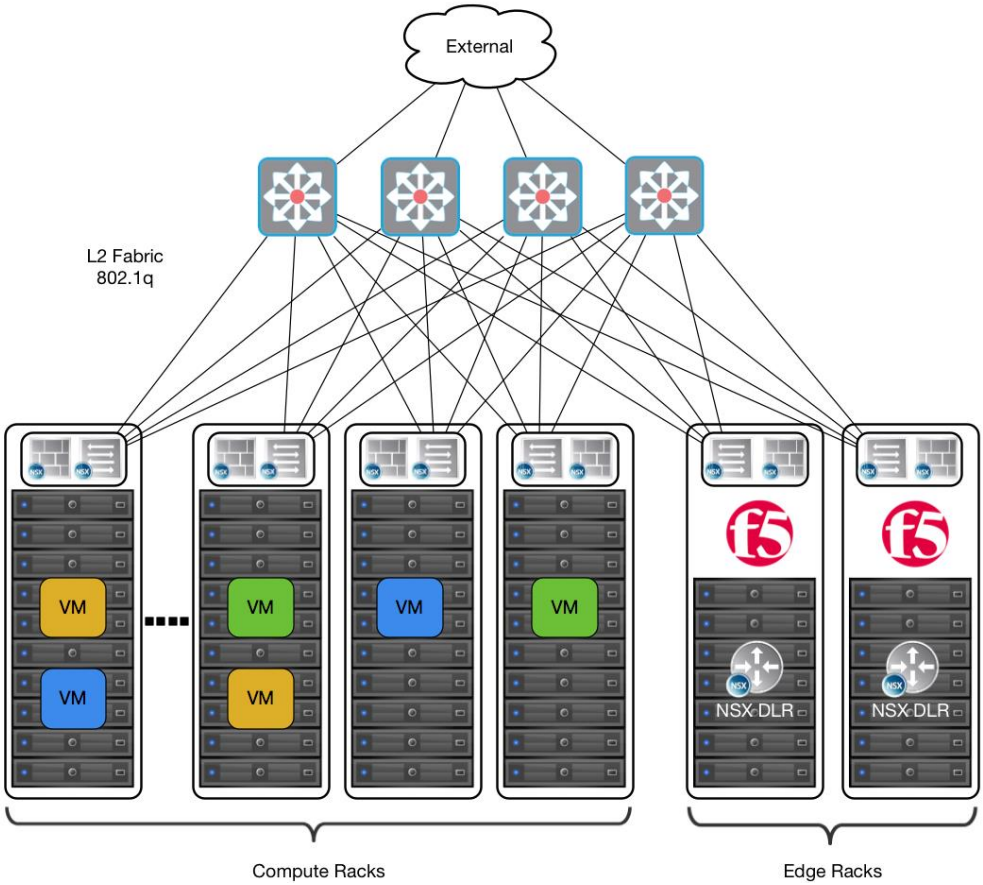


Figure 6 Leaf/spine physical rack infrastructure

The topology in this deployment scenario still isolates infrastructure vs compute racks however in this case the Edge services are not being used. The placement of the BIG-IP appliances (physical or virtual) should provide an optimal layer 2 path for application traffic. The DLR instances provide an optimal east-west path between tiers and to external networks.

Traffic Flows

North-South Traffic - Logical Traffic Flows as Follows

1. From Client (External) to BIG-IP WebTier VIP (Web-VIP)
2. From BIG-IP Appliance to WebTier Servers
3. From WebTier Servers to BIG-IP AppTier VIP (App-VIP)
4. From BIG-IP Appliance to AppTier Servers
5. From AppTier Servers to DLR to DB-Tier Servers

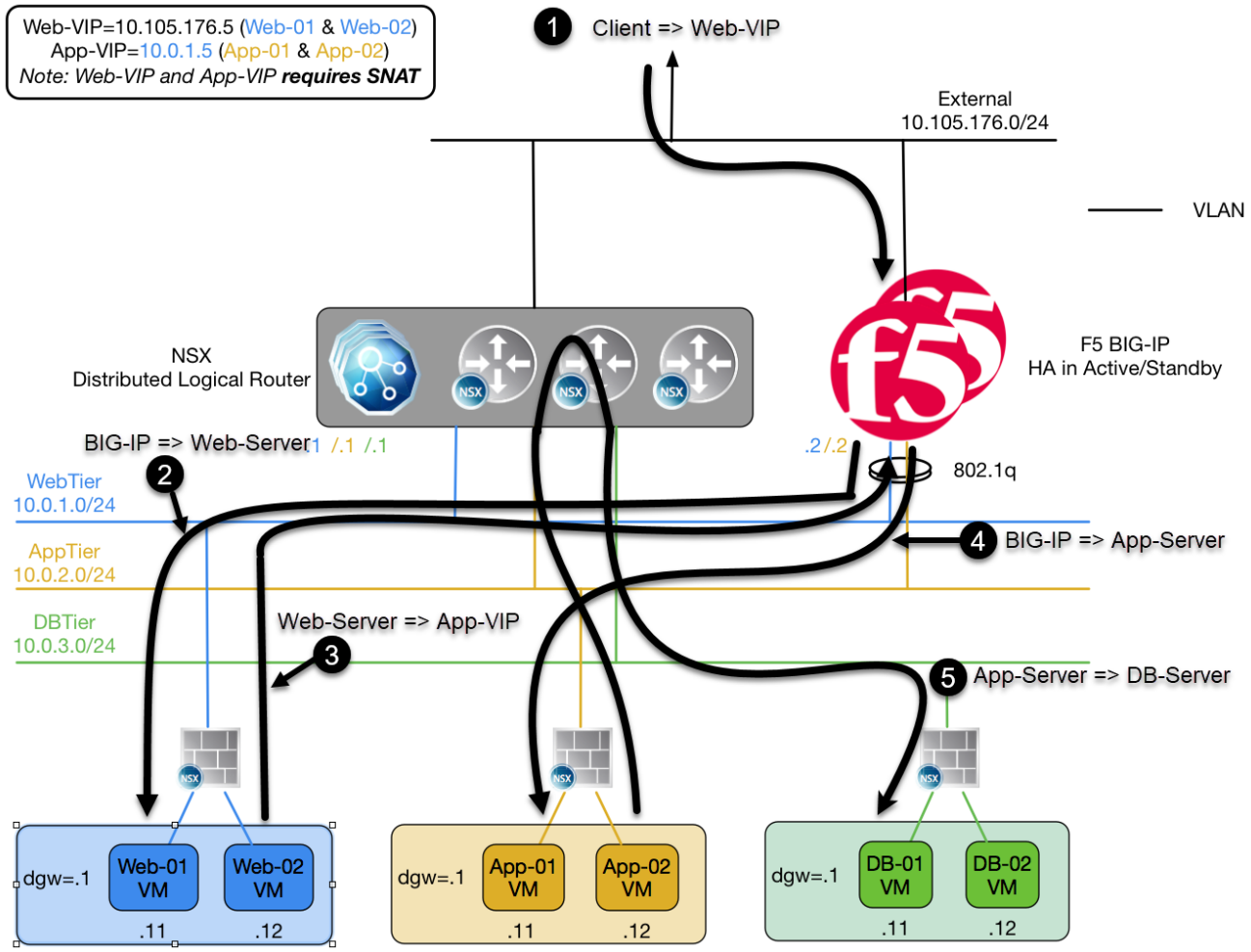


Figure 7 North-South Logical Traffic Flow "Parallel to DLR" with BIG-IP Appliances

Implementation Infrastructure

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

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 8: the Cluster1-VDC (Edge Rack) and Cluster3-Compute-NSX (Compute Rack). 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 6.

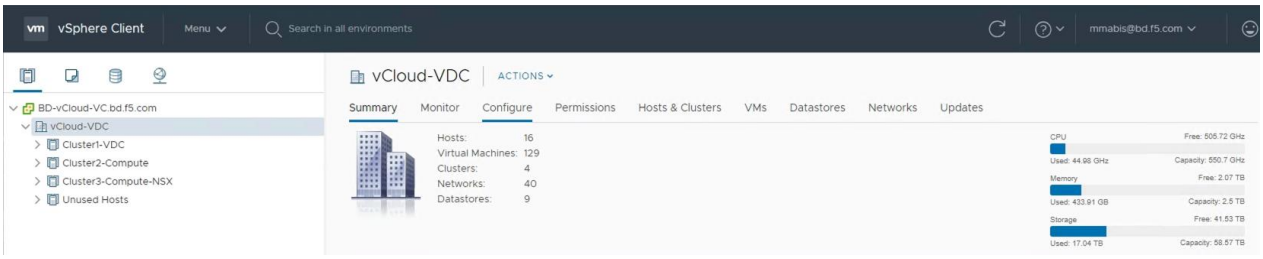


Figure 8 vSphere Console

In accordance with best practices, edge and compute ESXi hosts are physically and logically separated from one another. BIG-IP's are installed in dedicated edge racks, along with vCenter, NSX manager, and the NSX Distributed Logical Router, which also will be installed in the edge racks.

The virtual machines used as Web (Web), Application (App), and Database (DB) servers will be running on ESXi hosts in the compute cluster.

Prerequisites

Referencing the diagram in Figure 5, the BIG-IP requires connectivity to at minimum two of its 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 BIG-IP will need to be installed and connected (physically or virtually) to the infrastructure rack which is connected to L2 Fabric (802.1q). Each BIG-IP management interface will need to be connected and configured with an IP address in the management segment.
- The BIG-IP interface 1.1 will need to be connected to a switch port either in ESXi (trunked port group) or on the edge rack top-of-rack switch that 802.1Q tags the VLANs used in this environment. In the example, VLANs 102, 176, 177, 178 and 179 are used.
- Physical network infrastructure switches connected to the ESXi servers and BIG-IP appliances (if not virtual) 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	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176-External	176
Internal	DVS-VLAN-102	102
WebTier	DVS-VLAN-177-WebTier	177
AppTier	DVS-VLAN-178-AppTier	178
DBTier	DVS-VLAN-179-DBTier	179

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

Network Segments

Traditional 802.1Q VLAN network segments are utilized in this topology.

802.1Q VLAN segments

- **VLAN 176 (External)** is the VLAN used for external connectivity. The 10.105.176.0/24 IP subnet range is configured on this VLAN.
- **VLAN 102 (Internal)** (not shown) is for management connectivity. The 192.168.14.0/24 IP subnet range is configured on this VLAN
- VLAN 177 WebTier 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 178 AppTier is the VLAN ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VLAN.
- VLAN 179 DBTier is the VLAN ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VLAN.

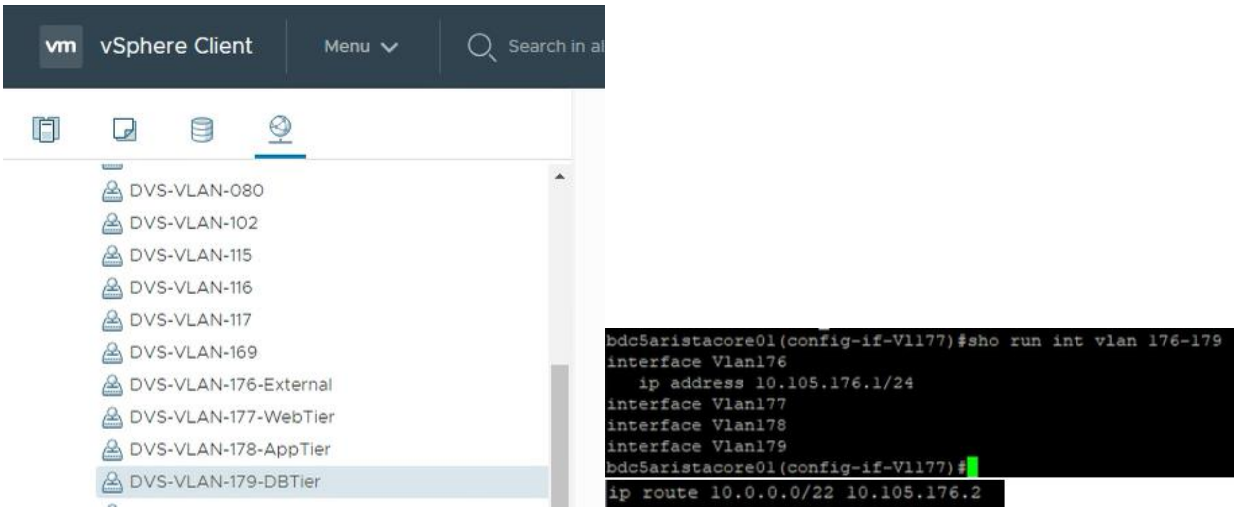


Figure 9 vSphere Client (HTML5) Console & Core Switch VLAN Gateways and IP Route for 10.0.0.0 segment

Port groups are created in vSphere that are tagged with the VLANs 102, 176-179. A DV uplink that is 802.1Q tagging with VLANs 0-4094 connected to the top-of-rack switches. Note in the Core Switch configurations that VLAN 177-179 have no gateway IP addresses associated to ensure the NSX DLR does that work. Also on the core switch a static route was put in to let traffic know that the DLR is the Gateway for the 10.0.0.0/22 network segment we created for (Web/App/DB)

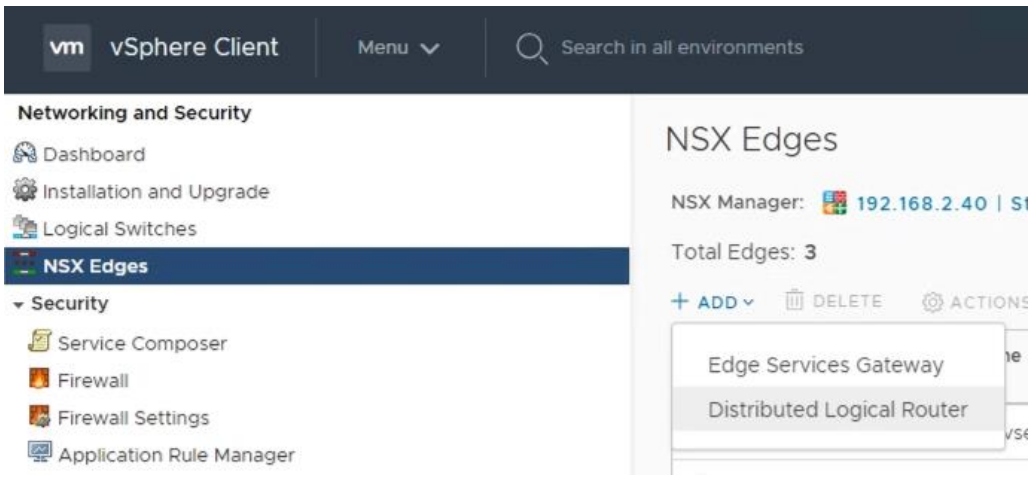
The top-of-rack switches must have at least these four VLANs tagged up to the L2 Fabric (802.1q)

Create and Deploy DLR

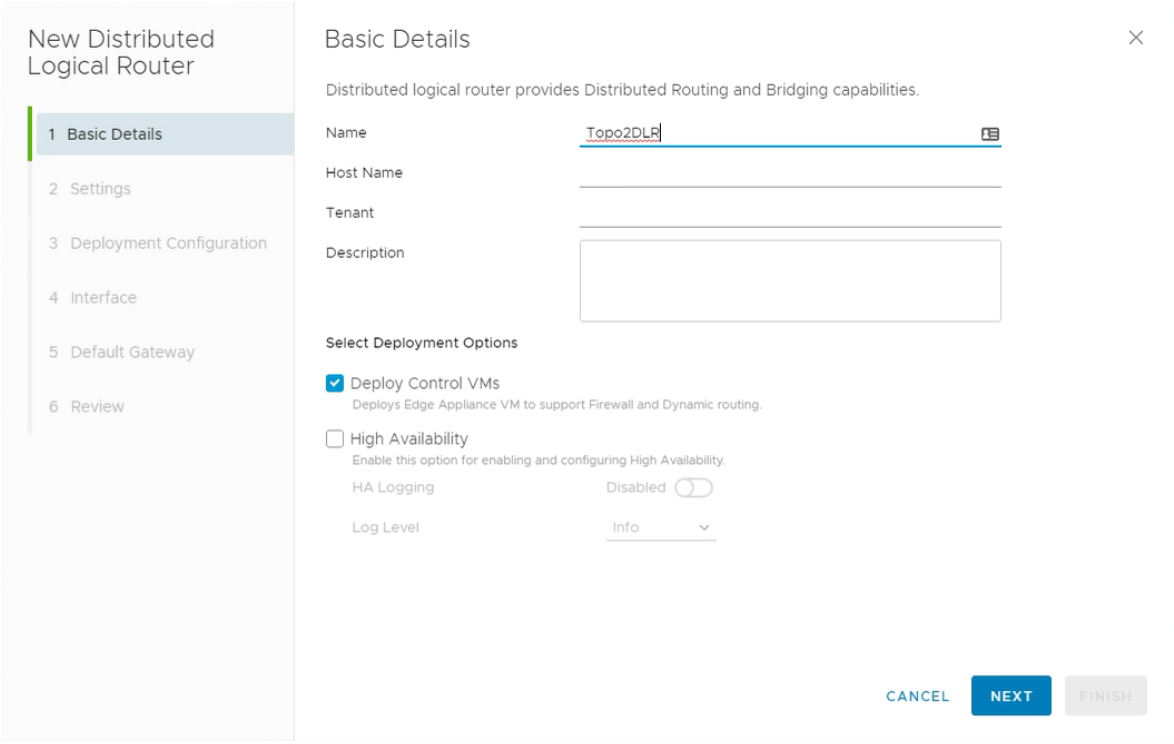
Within VMWare NSX, the Distributed Logical Router (DLR) provides an optimized way of handling east-west traffic within the data center. East-west traffic consists of communication between virtual machines or other resources on different subnets within a data center.

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

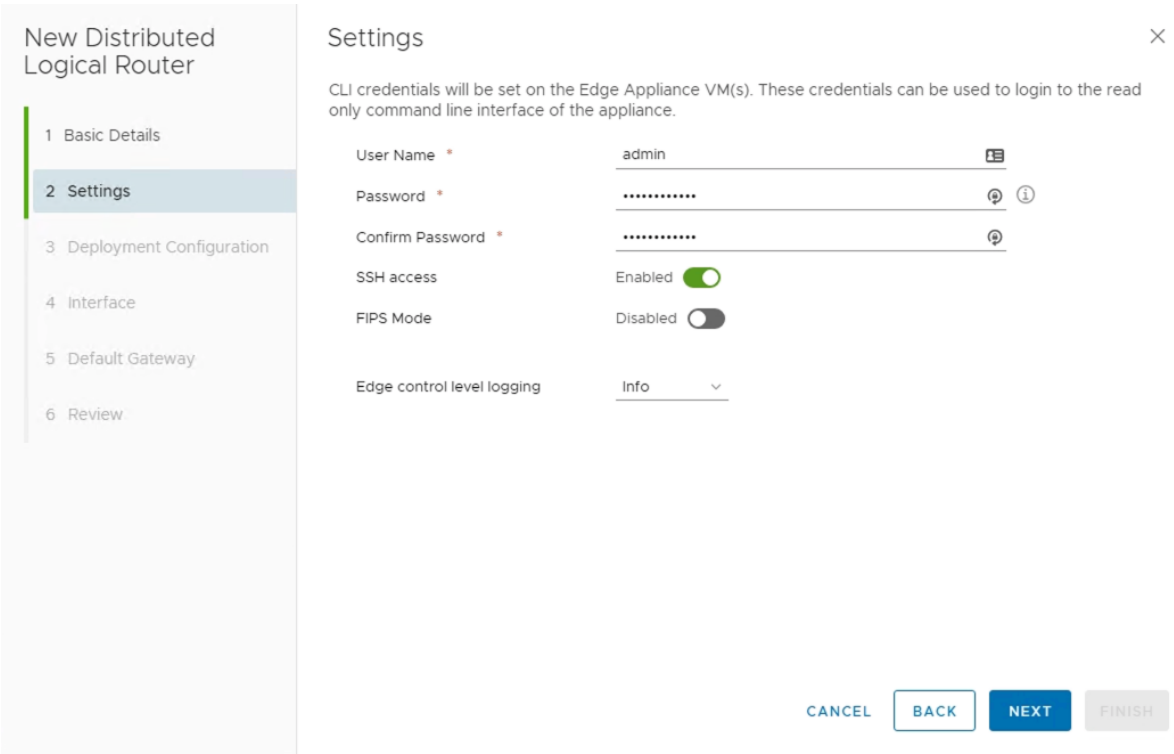
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection. Under Networking and Security, choose NSX Edges and then click (+ Add) hyperlink → Click on “Distributed Logical Router”



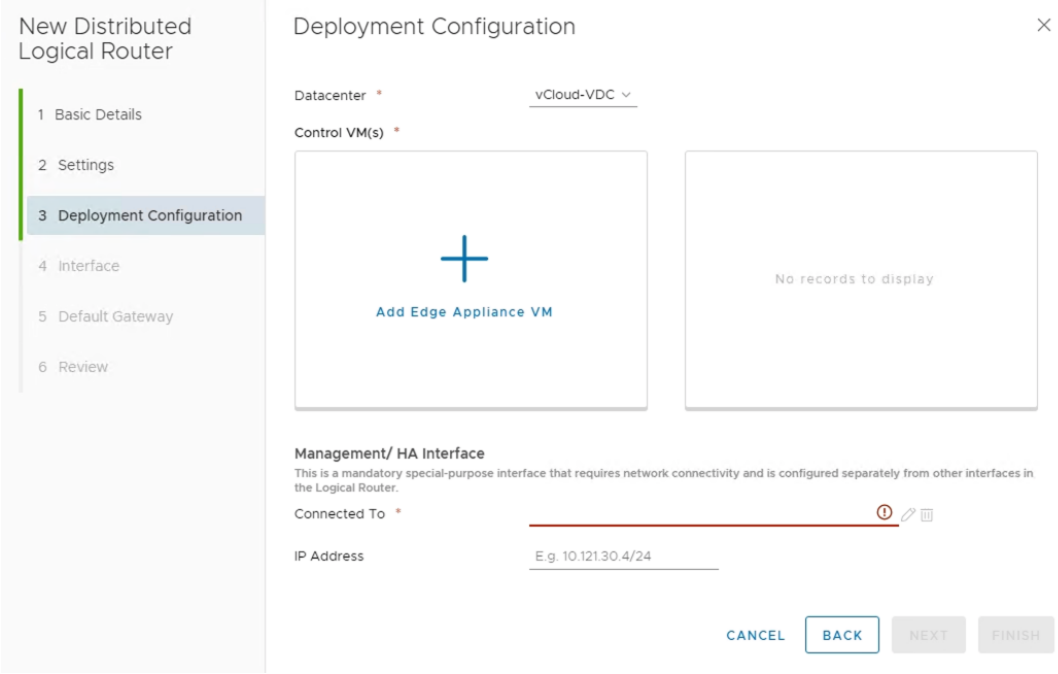
2. Provide a name for the device, then click next.



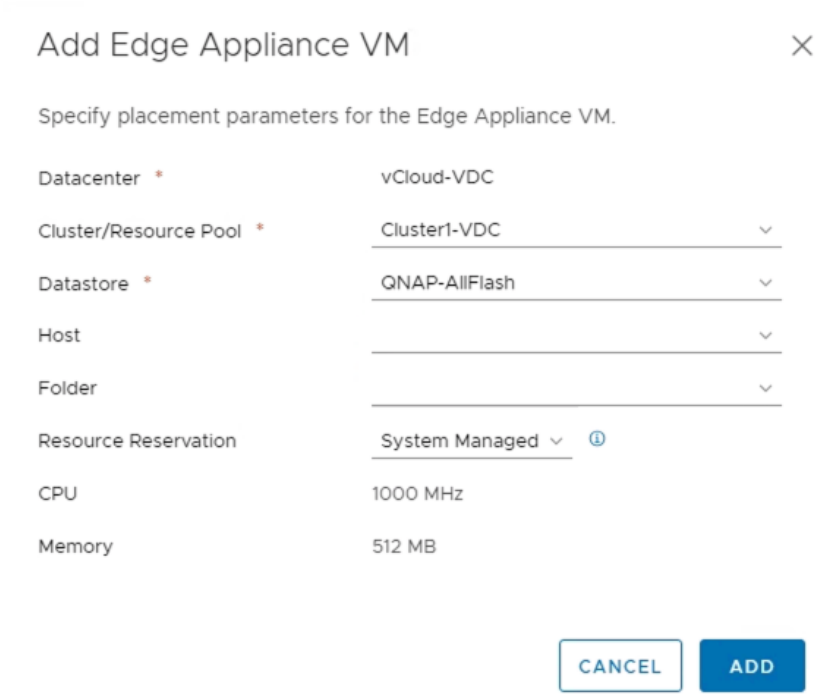
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Distributed Logical Router. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.



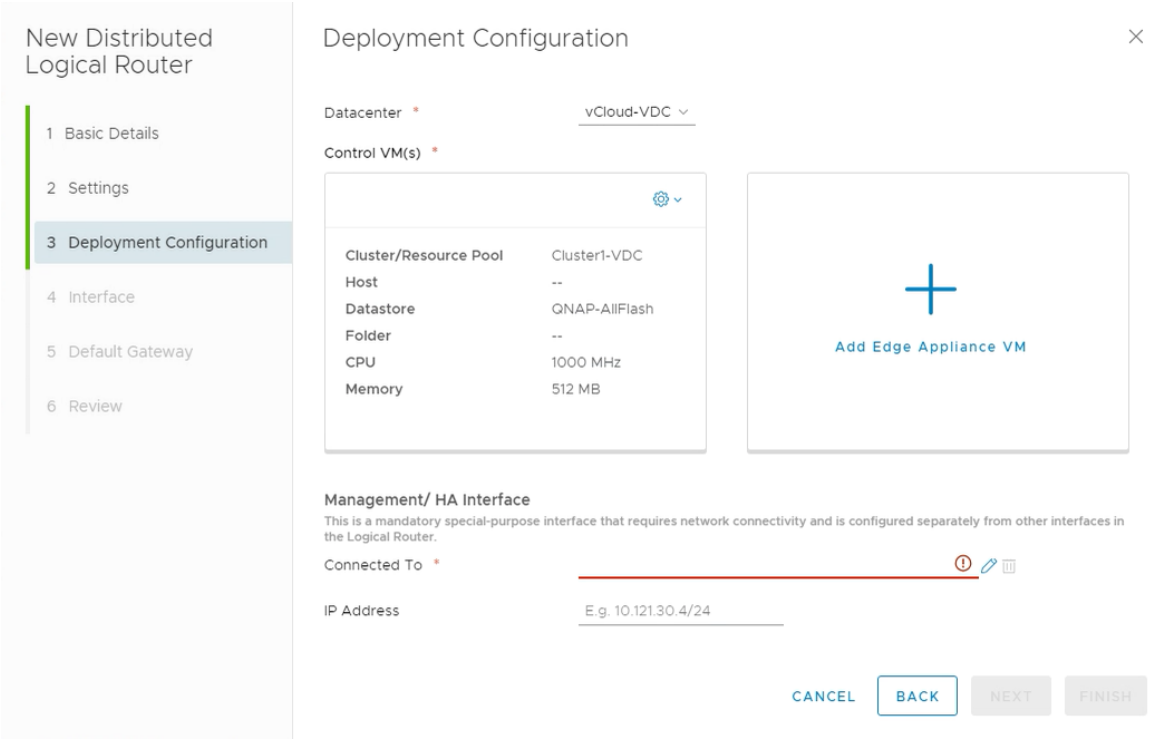
4. Under Configure deployment, select the Datacenter and Appliance Size appropriate for your deployment. Then click on the plus symbol (+) to Add Edge Appliance VM.



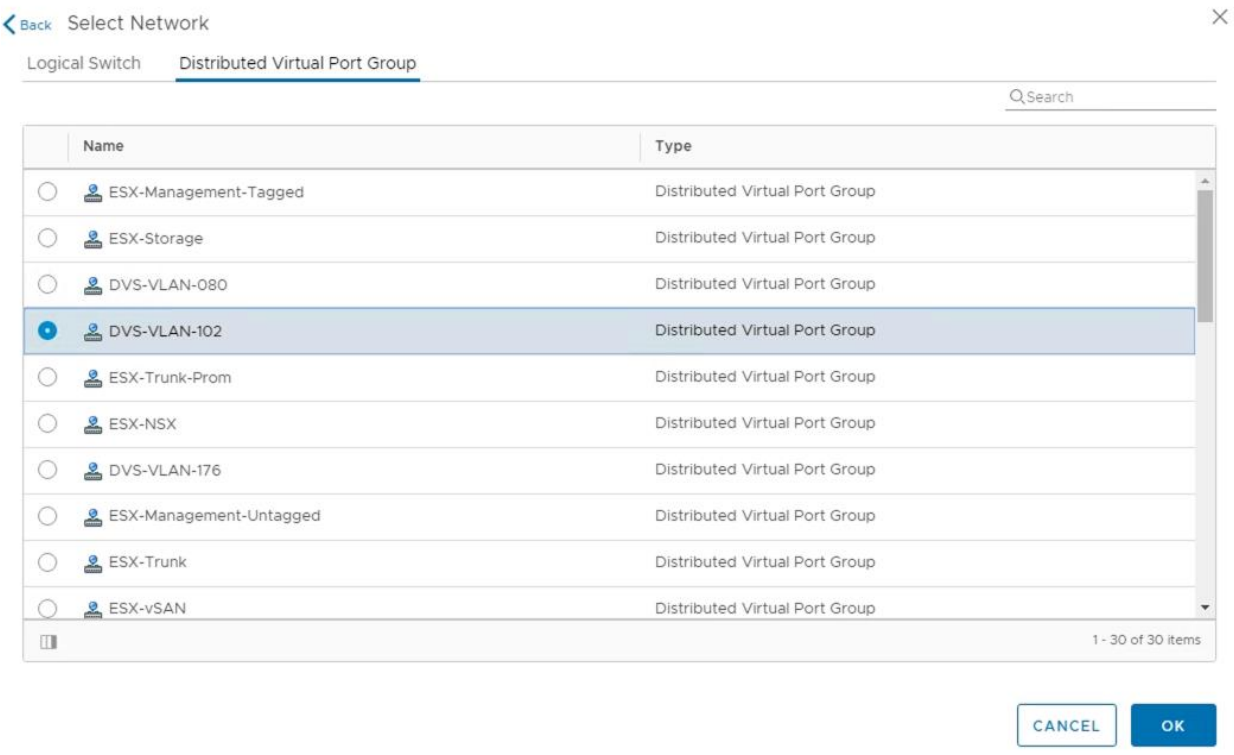
5. Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete.



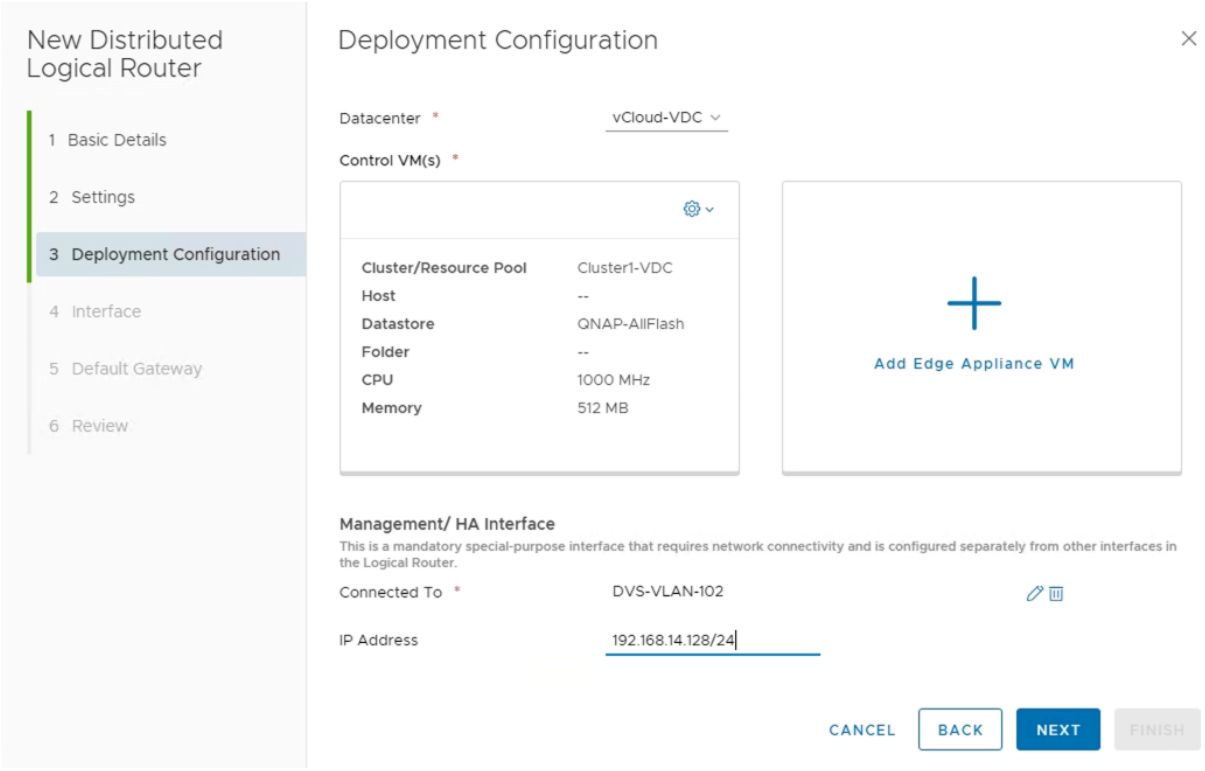
6. Click the Edit icon in the “Connected To” section of the Management/HA Interface



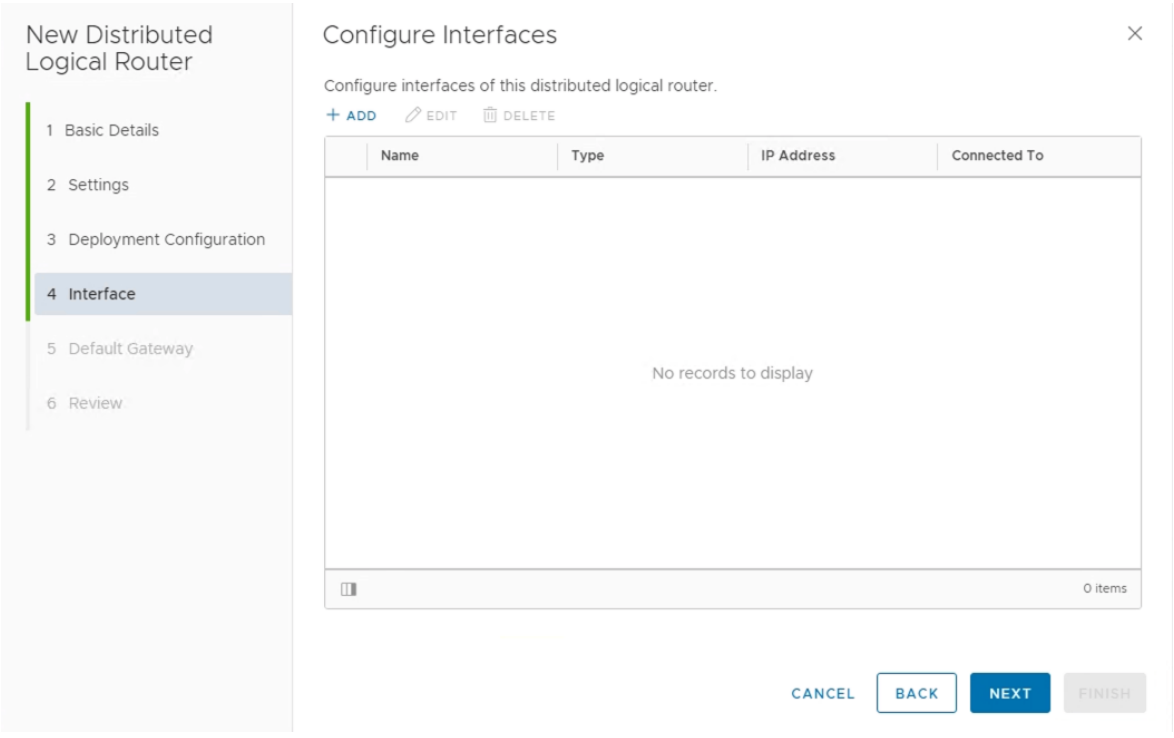
7. Select an appropriate Management Network (Distributed Virtual Port Group) to manage the DLR then Click OK



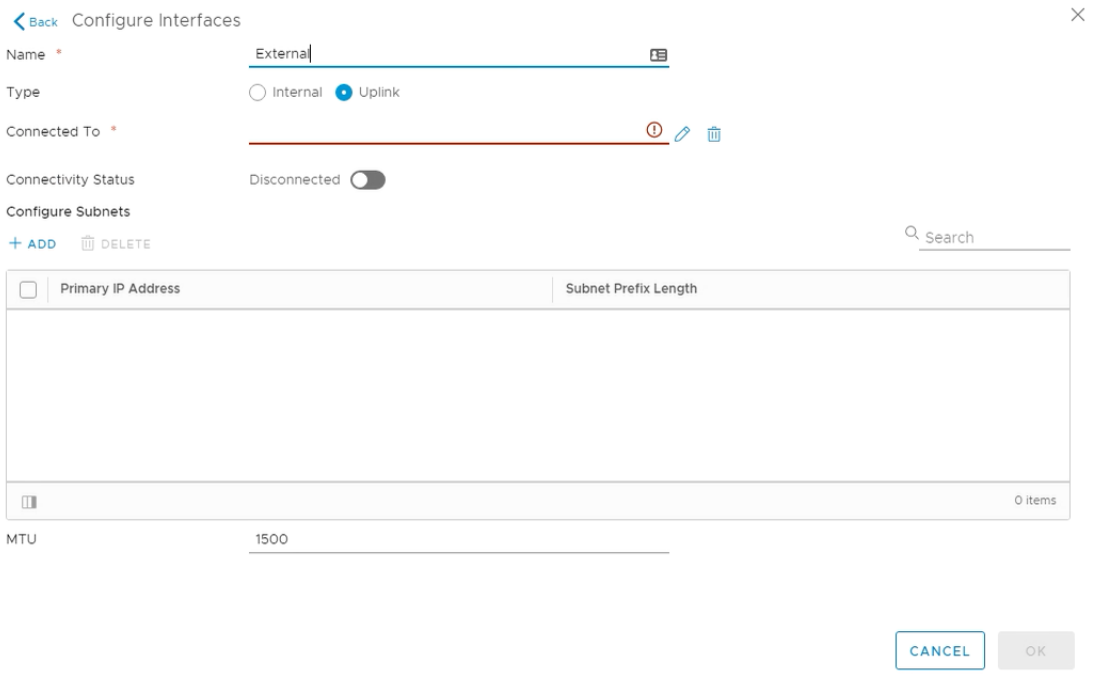
8. Fill out the IP/Subnet Field for the Management IP of the DLR then Click Next



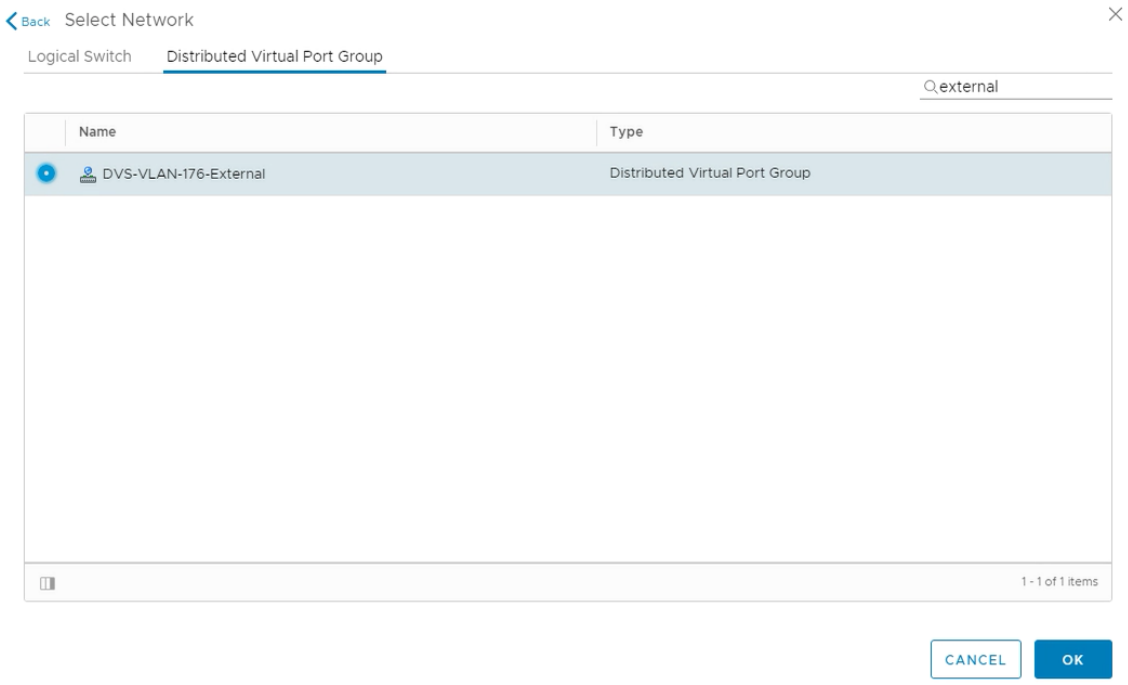
9. In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX DLR Interface dialog box.



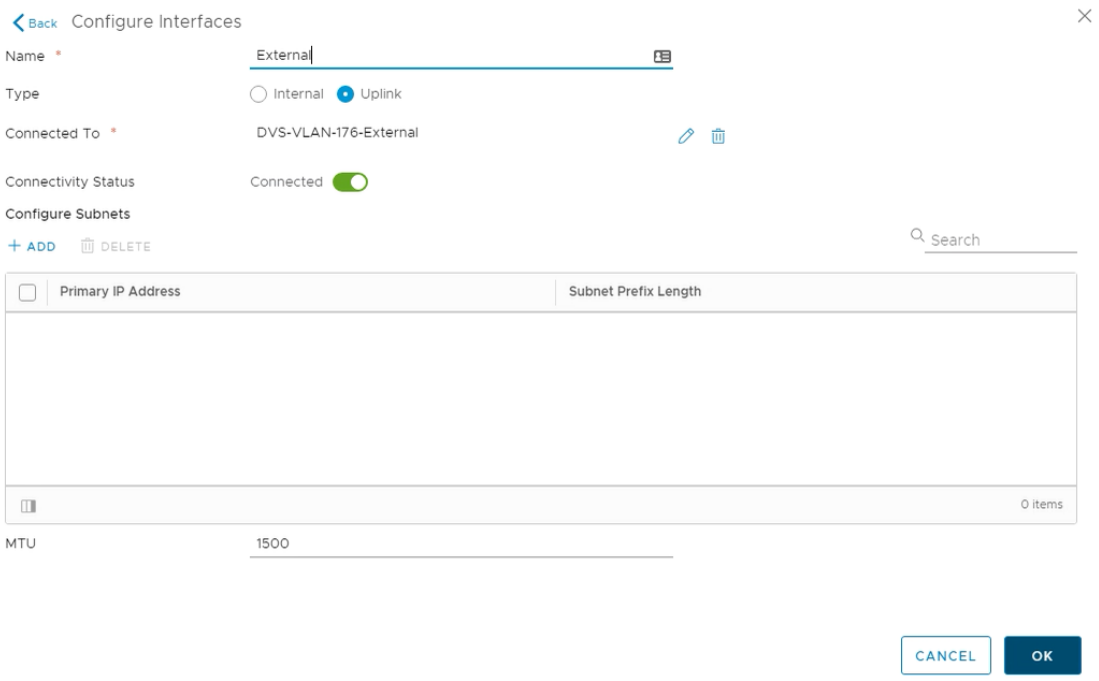
10. Provide a name and click the edit icon next to the “Connected To” field



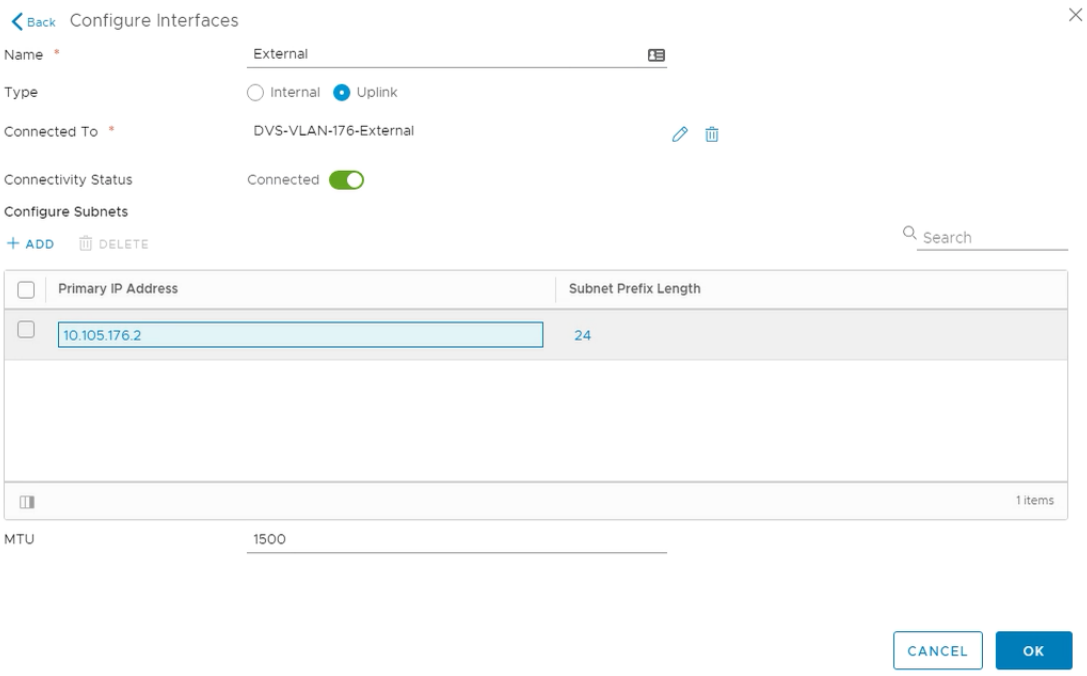
11. For the External network, click on the Distributed Virtual Port Group tab and then selecting the correct VLAN associated to the External Network. Click OK.



12. Once the network is chosen, select the (+ Add) hyperlink under Configure subnets.



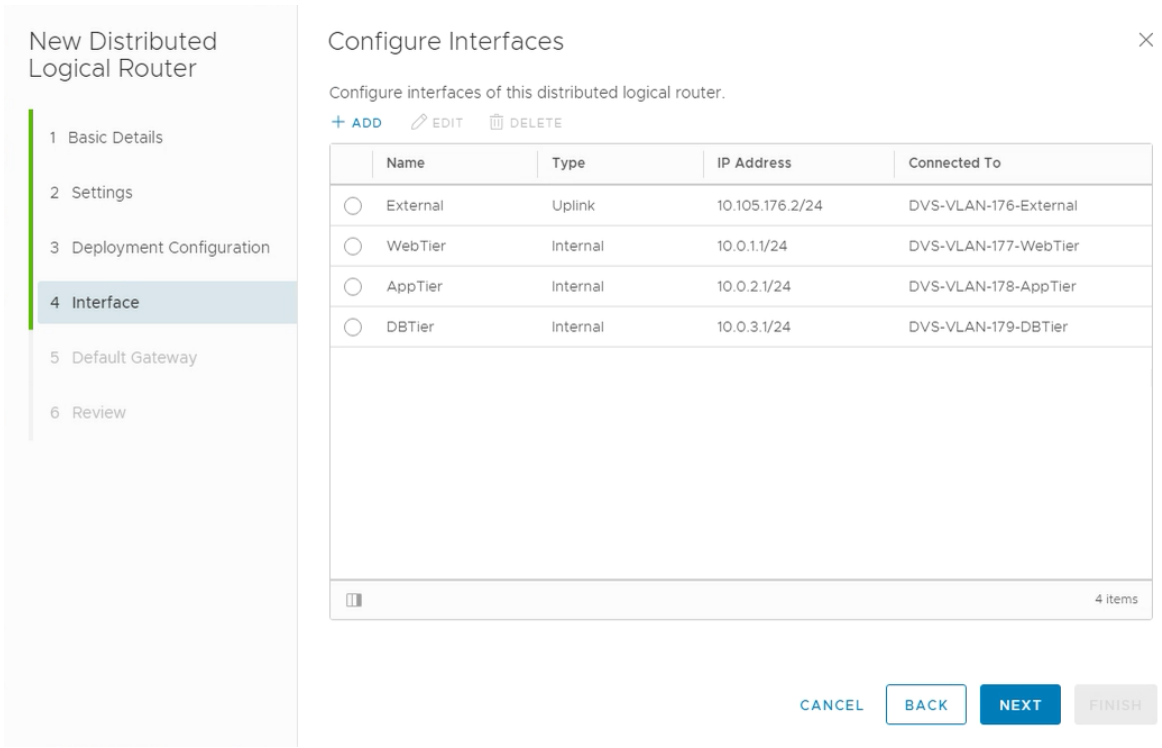
13. In the Configure Subnet dialog box, enter the appropriate IP address and Subnet prefix length, and click OK.



14. This will bring you back to the Configure interfaces dialog box. For each of the four interfaces required for this deployment scenario, add and configure the appropriate subnets and switch type, according to the table below and look like the final picture below with your datacenter information. Click Next to continue.

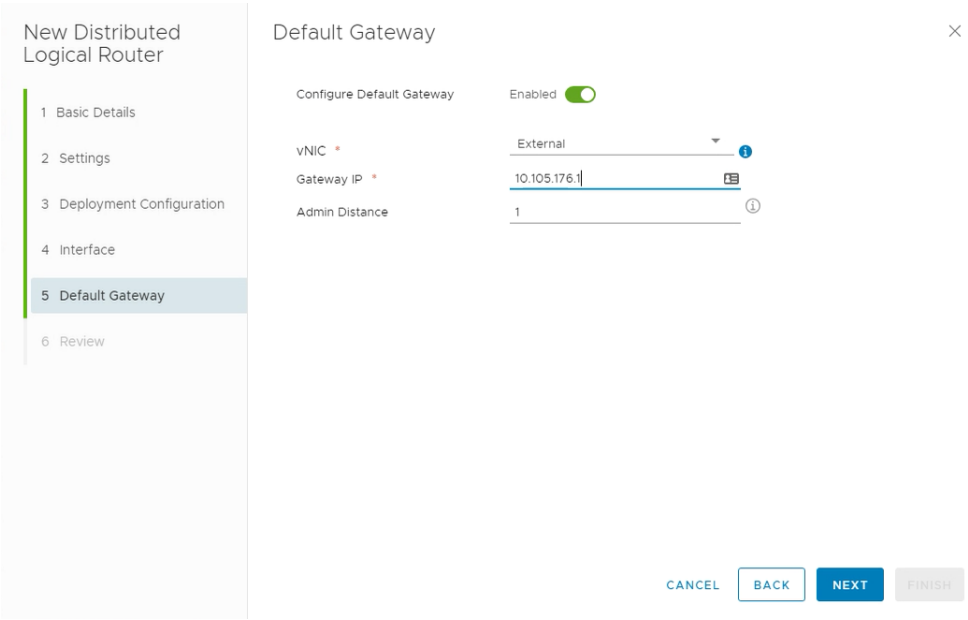
Network Name	Type	Network Type	IP Address	Connected To
External	Uplink	Distributed Virtual Port Group	10.105.176.2/24	DVS-VLAN-176-External
WebTier	Internal	Distributed Virtual Port Group	10.0.1.1/24	DVS-VLAN-177-WebTier
AppTier	Internal	Distributed Virtual Port Group	10.0.2.1/24	DVS-VLAN-178-AppTier
DBTier	Internal	Distributed Virtual Port Group	10.0.3.1/24	DVS-VLAN-179-DBTier

Table 8 NSX distributed logical router network interfaces

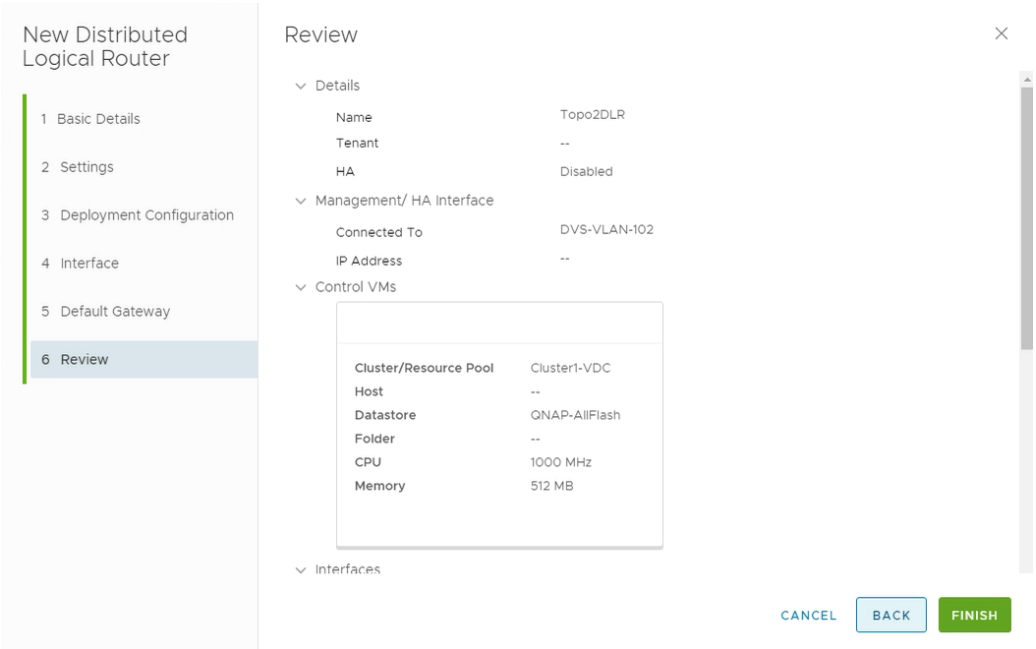


15. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway for the DLR is the data center core router that we configured in the previous section for the external network

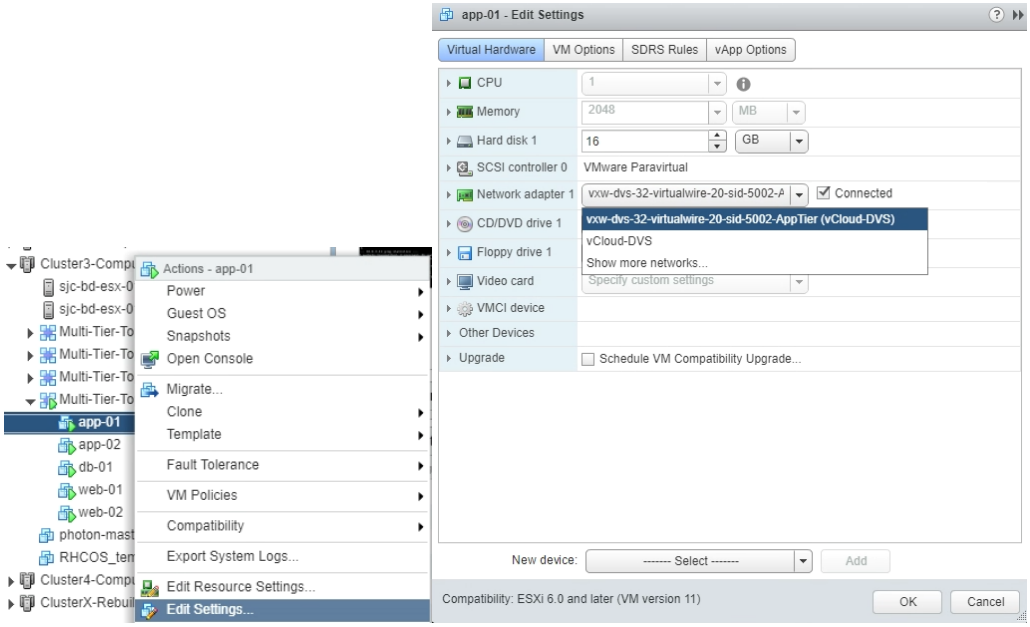
    For the vNIC select External and provide the Gateway IP address of the External Network.
    In this example, it is 10.105.176.1 Click Next to proceed.



18. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



19. After the Creation of the DLR and the logical switches within vSphere, attach the Virtual Machines for each tier to their logical switches for network traffic. (This is an example of one of our AppTier VM's attached to the AppTier Logical Switch.



BIG-IP 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.

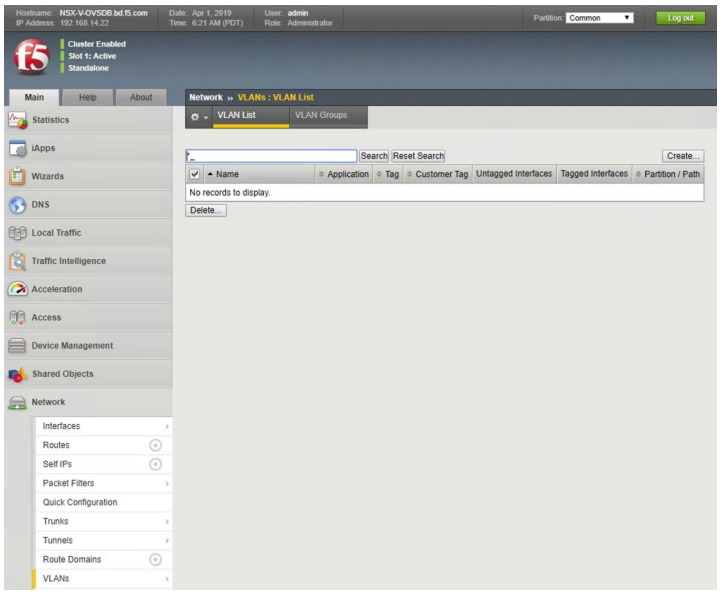
Prerequisites

- The BIG-IP 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 or an available interface that is connected to a physical or virtual switch (trunk) configured to support 802.1Q tagging of traffic. In our specific use case we use VLANs 176-179.

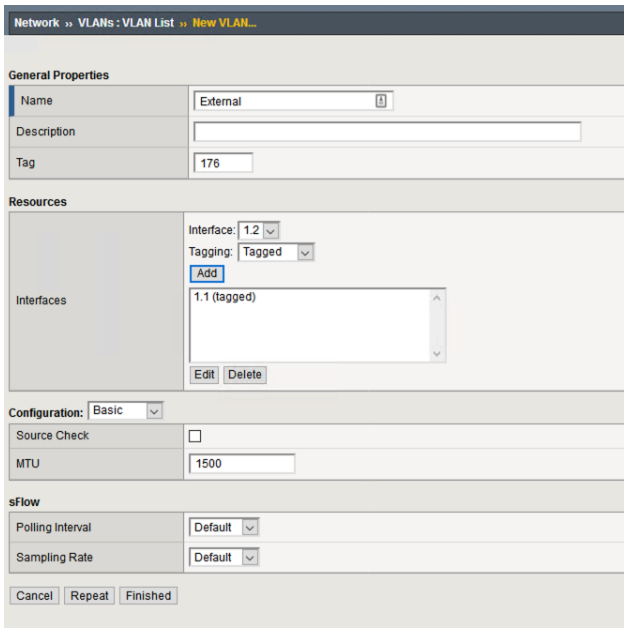
  For info on how to perform these installation and basic setup steps, refer to http://support.f5.com and consult the appropriate implementation guide for your version and device.

Create VLANs

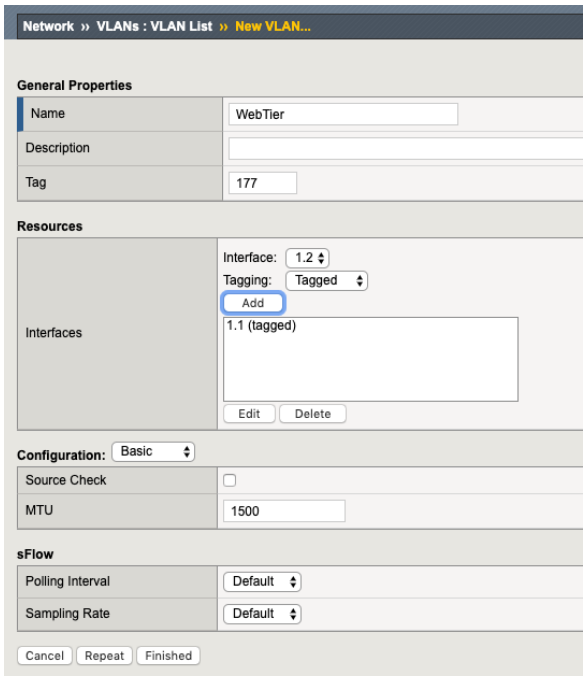
1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select VLANs.
2. In the upper right corner, click Create.

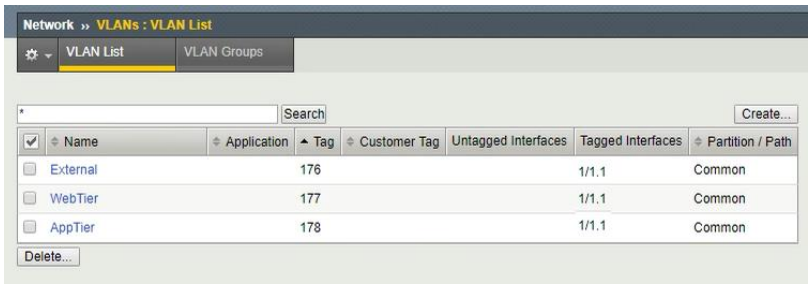


3. In the New VLAN menus.
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used External.
   b. In the Tag field, enter the External VLAN ID in this example, our VLAN is 176.
   c. Under Resources, for Interface, select 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and then click the Add button below it.
   e. Select Repeat to continue.



4. In the New VLAN Menus
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used WebTier.
   b. For the Tag, enter the WebTier VLAN ID in this example, our VLAN is 177.
   c. Under Resources, select the Interface 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and click the Add button below it.
   e. Select Repeat and return to step (a) for VLAN 178 AppTier to complete the VLAN creation. Click Finished to proceed.
   f. Validate the VLAN configuration against the image below.

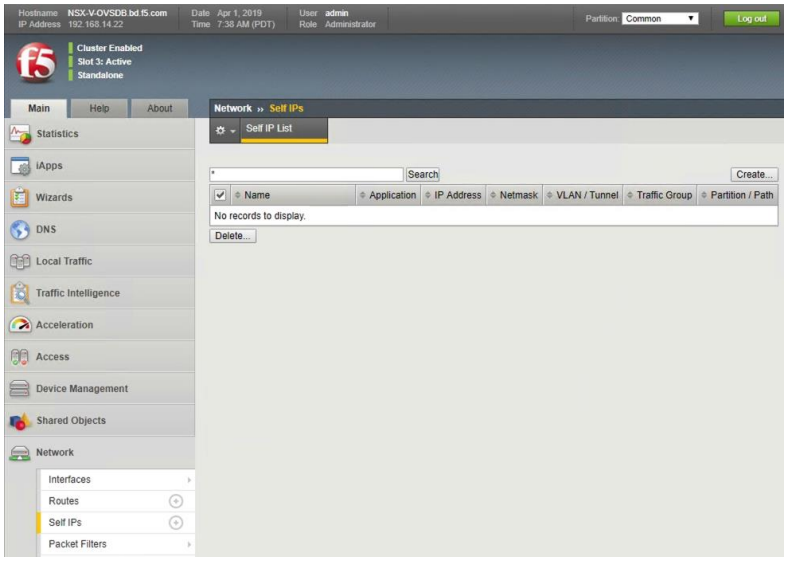




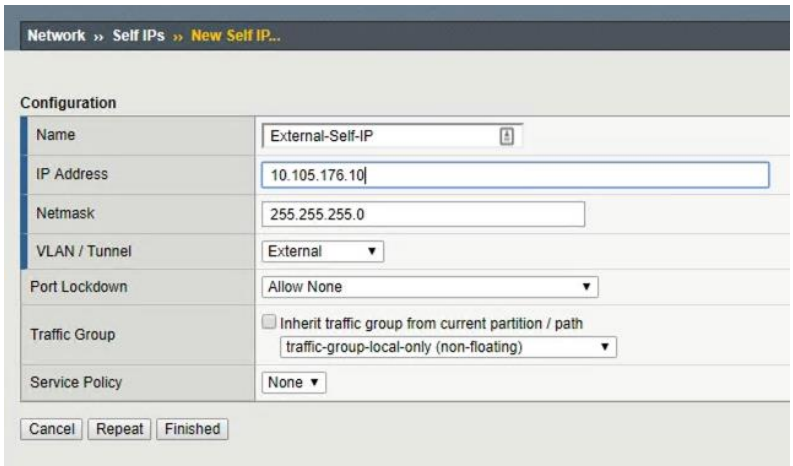
Configure Self IP Addresses

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.

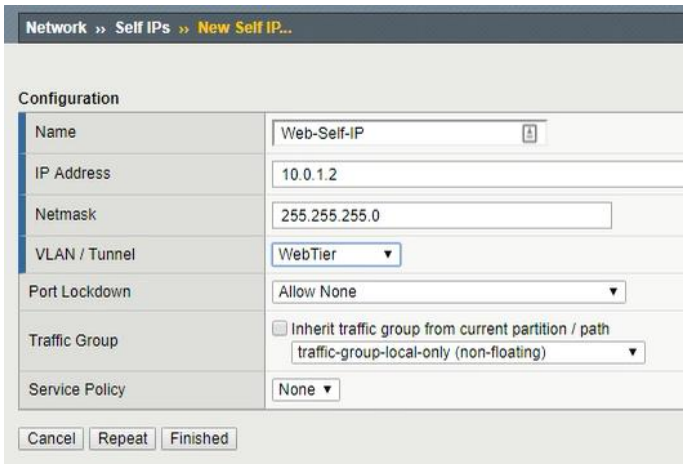
1. On the Main tab of the BIG-IP navigation pane, click Network and then click Self IPs.
2. In the upper right corner of the screen, click the Create button.

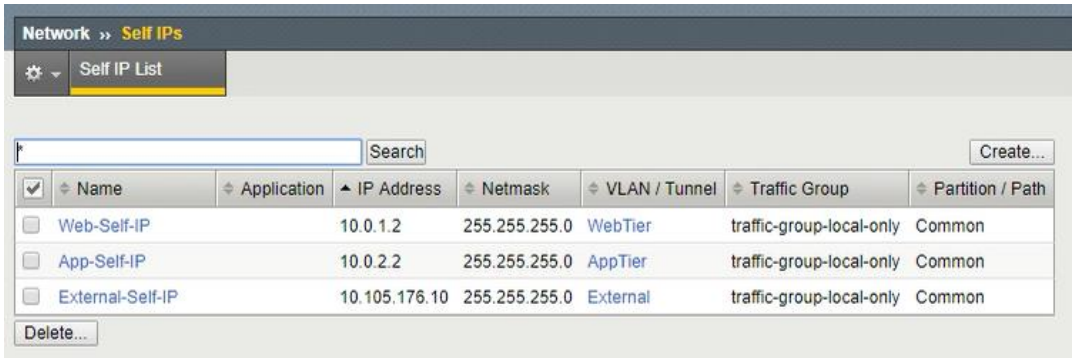


3. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “External-Self-IP” (without double quotes).
    b. In the IP address box, provide the IP address for the External network, in our example, we used 10.105.176.10.
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select External from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Repeat button to continue



4. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “Web-Self-IP” (without double quotes).
    b. In the IP address box, provide the IP address for the WebTier network, in our example, we used 10.0.1.2
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select WebTier from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Select Repeat and return to step (a) for the “App-Self-IP” to complete the Self IP Creation then click Finished to proceed.
    g. Validate the VLAN configuration against the image below.

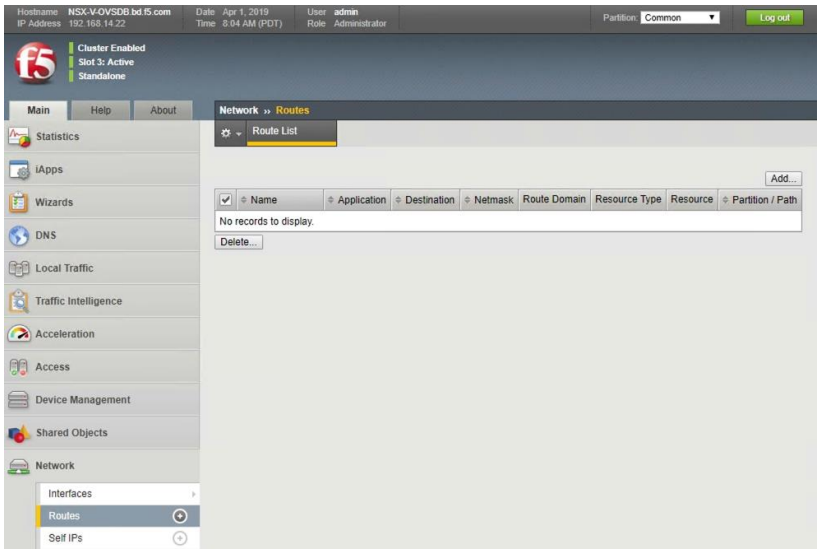




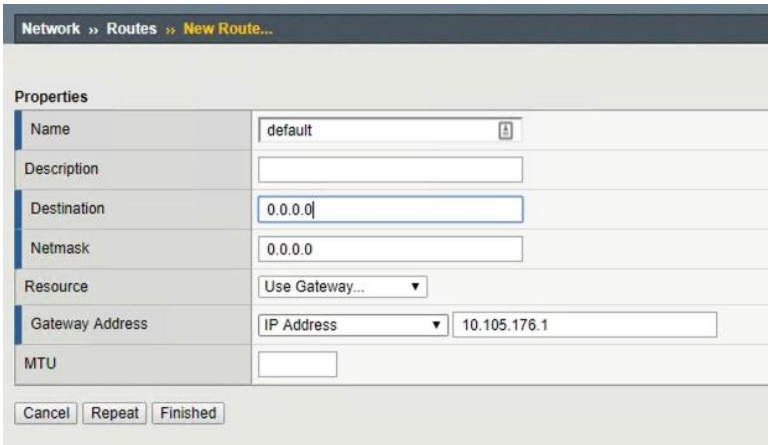
Configure Static Routes

To ensure the BIG-IP can properly forward requests to all of the VIPs and application servers, static routing is used to provide a discreet path for traffic.

1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select Routes.
2. In the upper right corner of the screen, click the Ad button.



3. In the New Route menus
   a. For the Name, use the keyword default.
   b. The default route for both Destination and Netmask is 0.0.0.0.
   c. The Gateway Address is the address of the core router, in our example the core router's IP address is 10.105.176.1
   d. Click Finished to complete.



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.

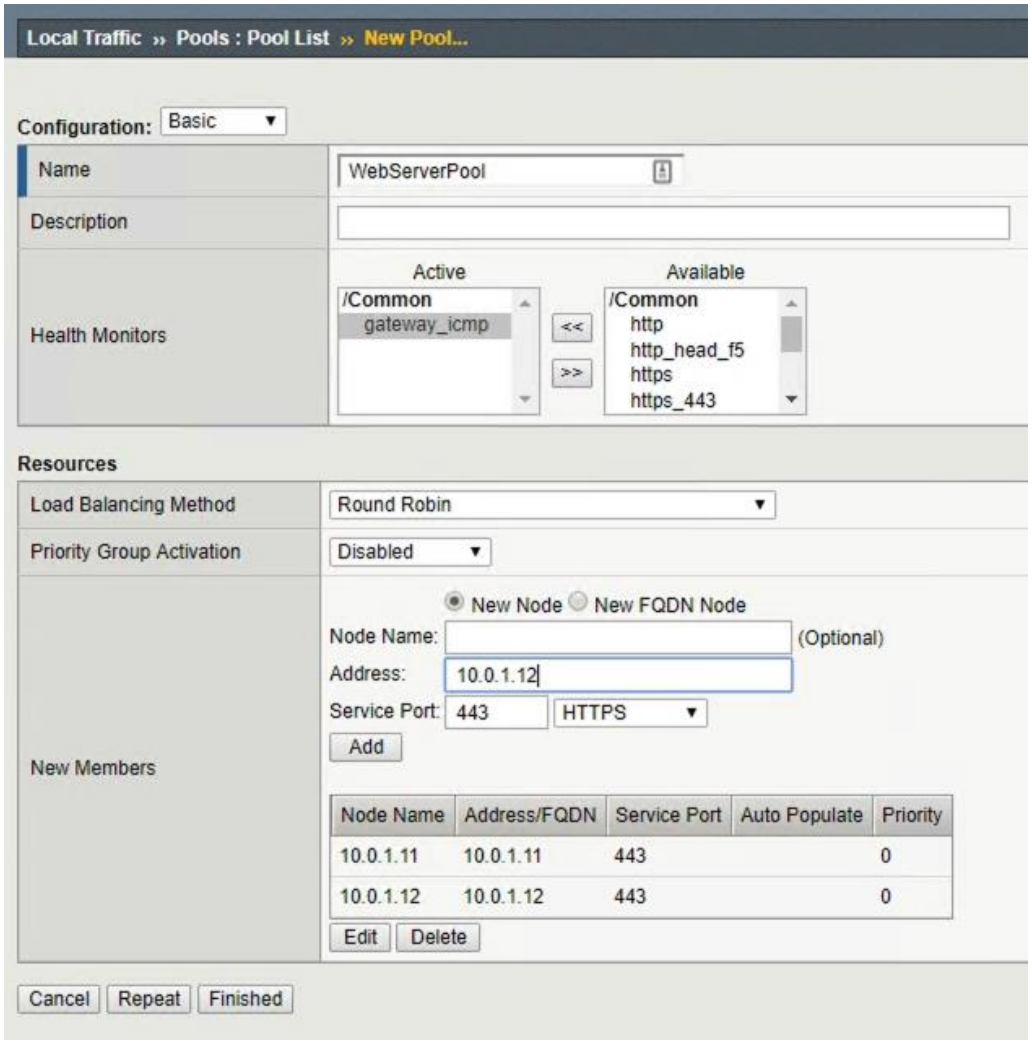
Create Application Pools

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 New Pool menus
    a. In the Name field, type a unique name for the web pool. For this validation, we used WebServerPool.
    b. 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.
    c. Under Resources, select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
    d. 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.
    e. Click Repeat to continue and enter the application tier information,

Name (Optional)	Address	Service Port
web-01	10.0.1.11	443 (HTTPS)
web-02	10.0.1.12	443 (HTTPS)

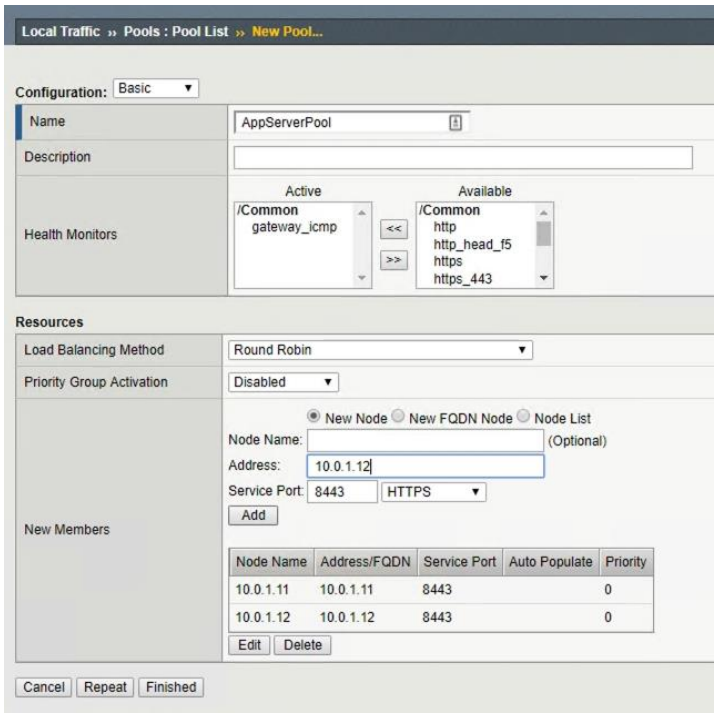
Table 9 BIG-IP web tier pool members


Local Traffic ›› Pools : Pool List ›› New Pool...
Configuration: Basic
Name
WebServerPool
Description
Health Monitors
Active
/Common
gateway_icmp
<<
>>
Available
/Common
http
http_head_f5
https
https_443
Resources
Load Balancing Method
Round Robin
Priority Group Activation
Disabled
New Members
New Node
New FQDN Node
Node Name:
(Optional)
Address:
10.0.1.12
Service Port:
443
HTTPS
Add
Node Name
Address/FQDN
Service Port
Auto Populate
Priority
10.0.1.11
10.0.1.11
443
0
10.0.1.12
10.0.1.12
443
0
Edit
Delete
Cancel
Repeat
Finished

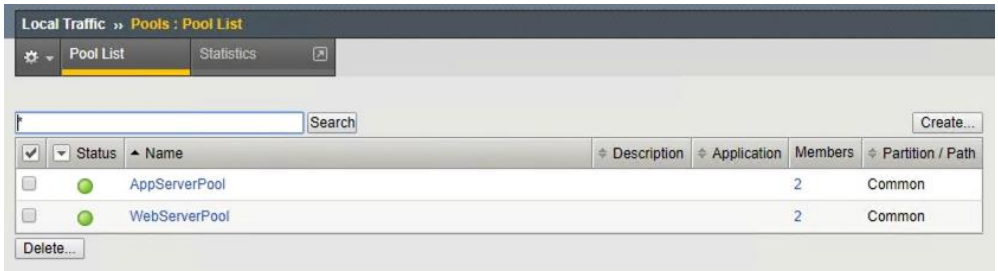
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
   a. In the Name field, type a unique name for the app pool. For this validation AppServerPool was used.
   b. In the Health Monitors section select an appropriate monitor for your application. 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.
   c. In the Resources section of the screen select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
   d. 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 10). Select the Add button for each pool member.
   e. Click Finished to complete the pool creation.

Name (Optional)	Address	Service Port
app-01	10.0.2.11	8443
app-02	10.0.2.12	8443

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.

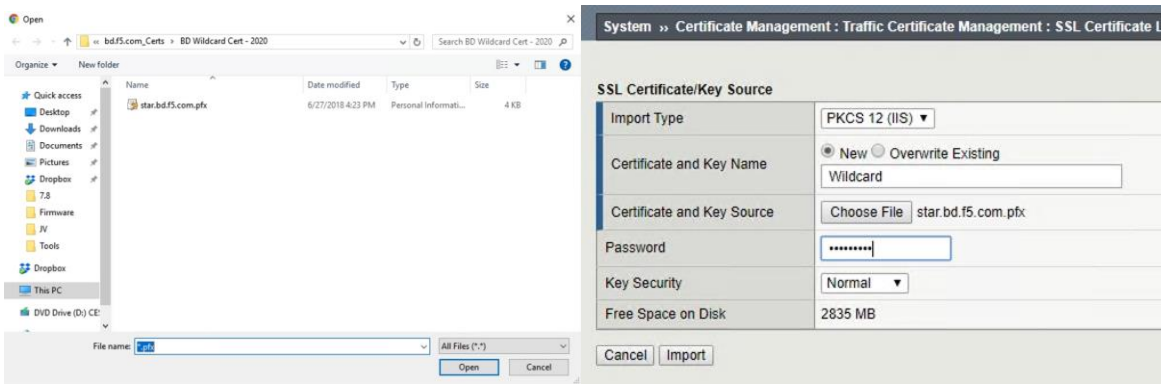


Import SSL Certificate

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

As a prerequisite to completing this task you must have a Certificate with a Private Key (Exportable) available to install this could be in Certificate/Key format or PKCS12 (PFX) format. In our test case we will be using a public PKCS12 certificate (PFX) wildcard certificate "*.bd.f5.com" that will allow any DNS name in front of bd.f5.com will be an accepted as valid name in a web browser.

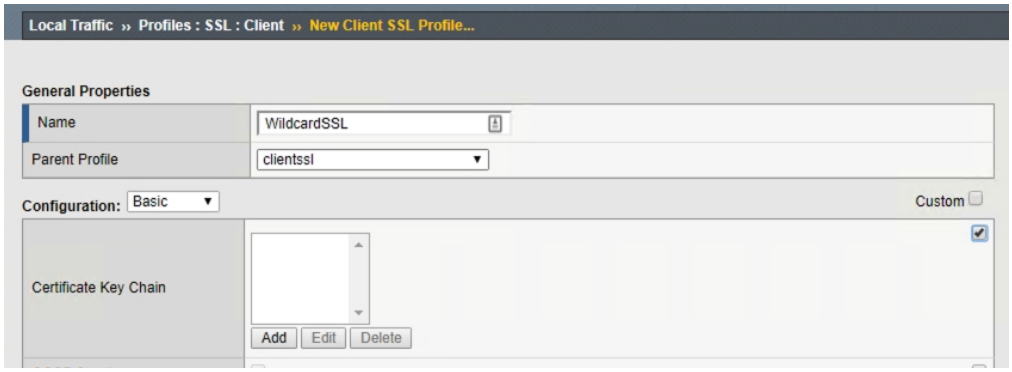
1. On the Main tab, select System → Traffic Certificate Management → SSL Certificate List
2. In the upper right corner of the screen, click the Import button.
3. In the Import SSL Certificate and Keys menus
    a. In the Import Type field, in our example we select "PKCS 12 (IIS)"
    b. In the Certificate and Key Name field, in our example we entered "Wildcard" without quotes
    c. In the Certificate and Key Source field, select the "Choose File" button
    d. In the pop out menus browse and select the file, in our example star.bd.f5.com.pfx
    e. In the password field, enter the password to decrypt the pfx file.
    f. Click the Import button

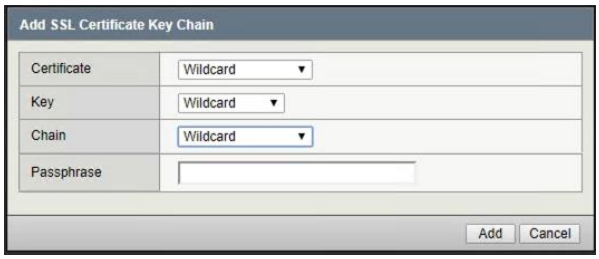


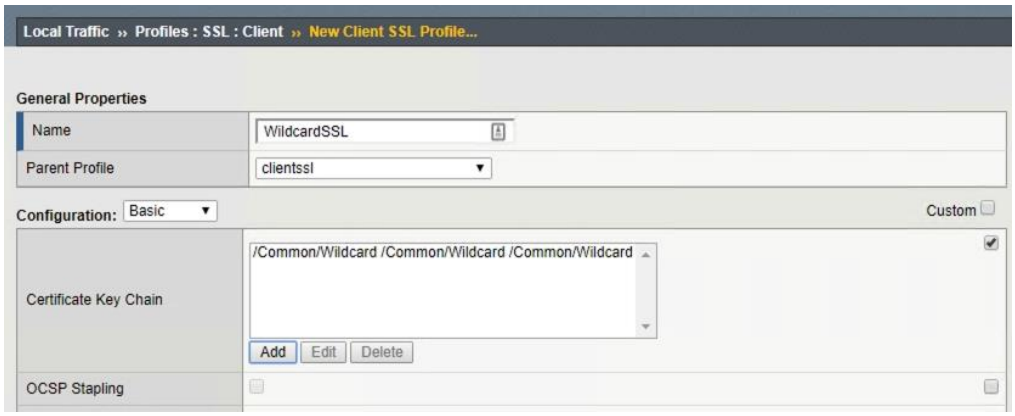
Create ClientSSL Profile

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

1. On the Main tab, select Local Traffic → Profiles → SSL → Client
2. In the upper right corner of the screen, click the Create button.
3. In the New Client SSL Profile menus
    a. In the Name field, type a unique name for the profile, for this validation WildcardSSL was used.
    b. In the Certificate Key Chain field, check the custom box and click the Add button
    c. In the Certificate, Key and Chain pulldown menus, select the previously imported Certificate chain, in this validation it was named Wildcard. Then click the Add button.
    d. Once added, scroll to the bottom and click the finished button.



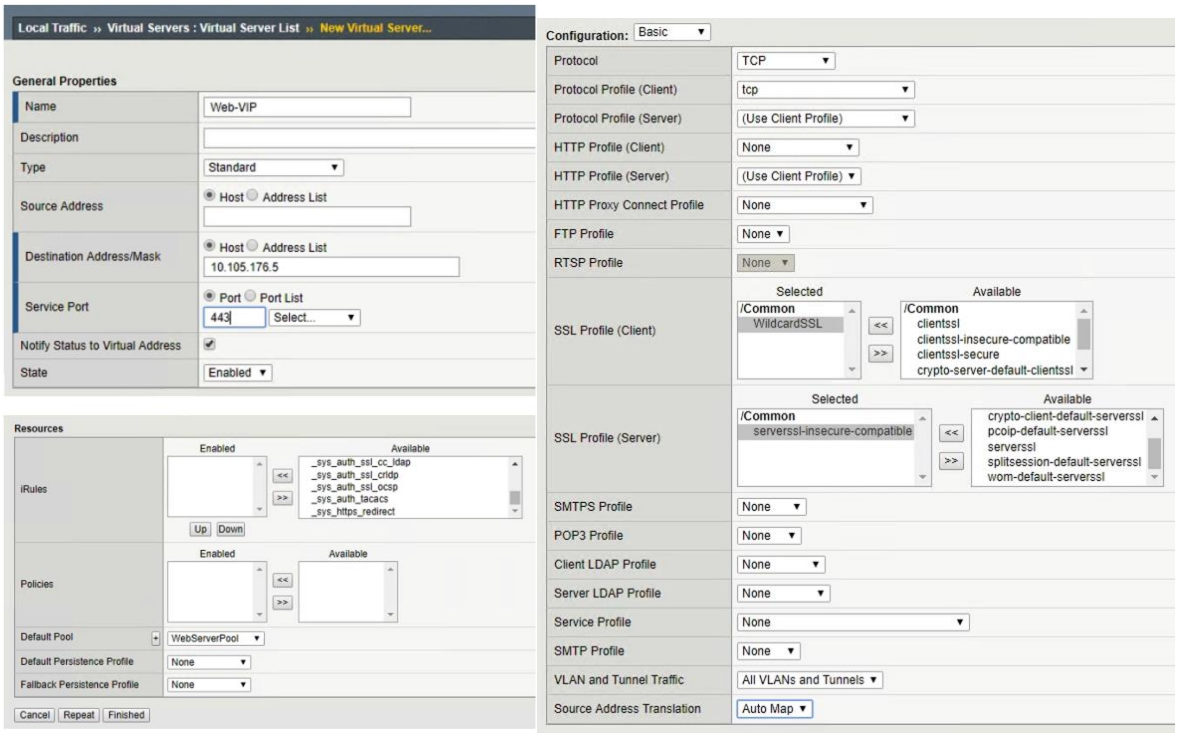




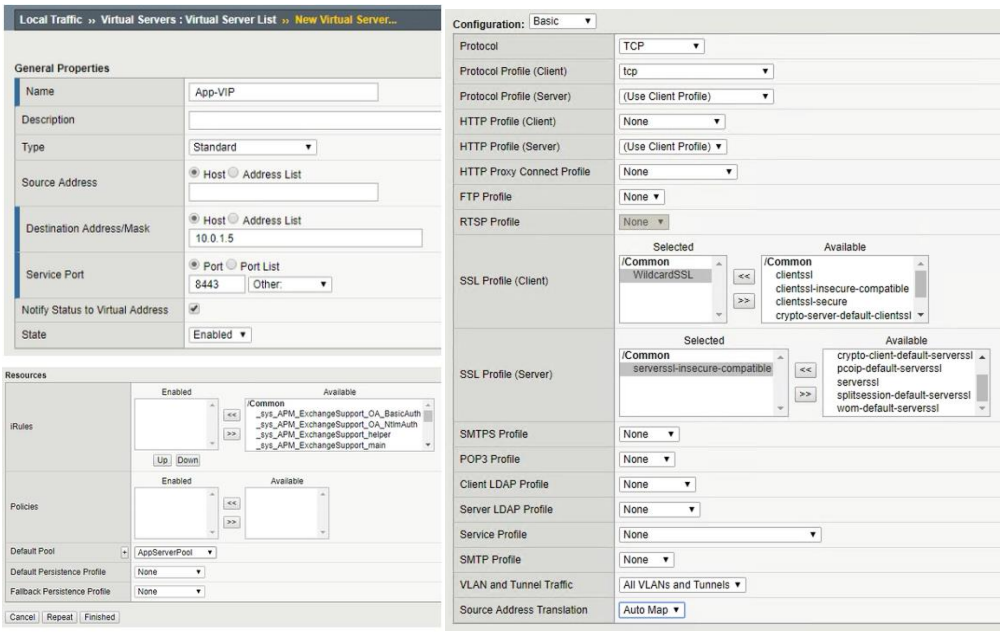
Create Application Virtual Servers

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 10.105.176.0/24 segment, and the other for the application tier, available on the TransitNet-1 segment (172.16.1.0/24).

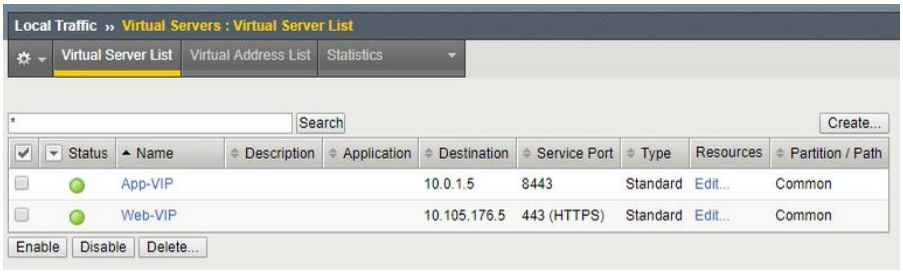
1. On the Main tab, select Local Traffic and then click Virtual Servers. The Virtual Server List screen is displayed.
2. In the upper right corner of the screen, click the Create button.
3. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the web application. In this case, we used Web-VIP.
    b. In the Destination Address field, enter 10.105.176.5
    c. For Service Port use the standard HTTPS port 443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the WebServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Repeat to continue to configure the application tier virtual server



4. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the app application. In this case, we used App-VIP.
    b. In the Destination Address field, enter 172.16.1.5
    c. For Service Port use the standard HTTPS port 8443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the AppServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Finished to continue to configure the application tier virtual server



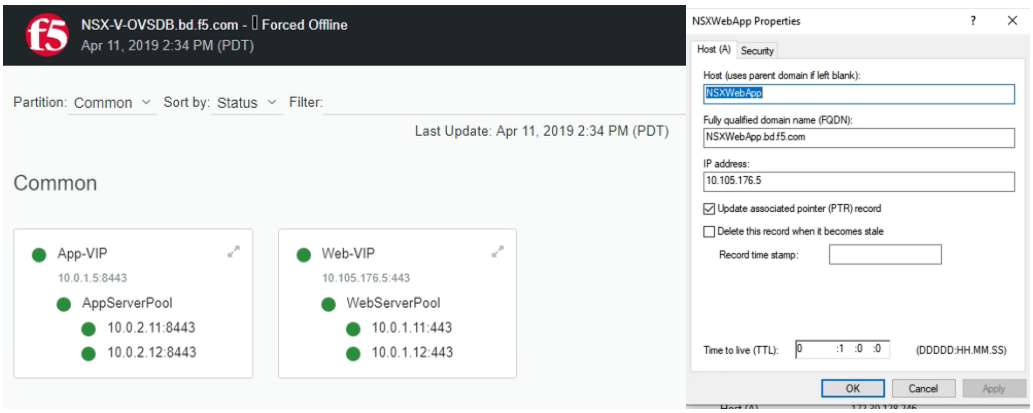
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.



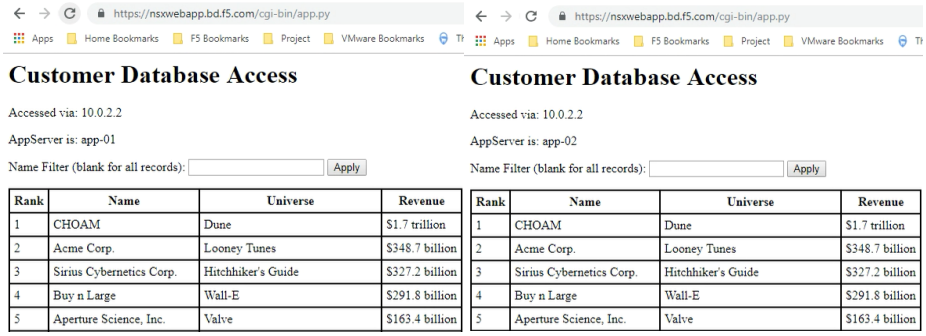
Validation

The web tier virtual server should now be available and accepting application traffic on port 443 (HTTPS).

On the Main tab, expand Local Traffic and then click Network Map to display the overall health of the applications and their associated resources. Due to also this traffic being HTTPS rather than HTTP we setup a FQDN of NSXWebApp.bd.f5.com to allow our wildcard certificate to be validated when connecting to the site.



Any web browser can be used to test by typing https://NSXWebApp.bd.f5.com/cgi-bin/app.py to send a request to the virtual server. Our 3-tier application will appear and show data within the database validating that the connection works, to further validate which application server you can refresh the page and see the AppServer changes. To further validate which Web server is being used we run a curl command “curl -kv “https://nsxwebapp.bd.f5.com” in the web server we injected a header in the web server configuration (not shown in this guide) called X-Upstream-Server to show which web server was being accessed.



This concludes the validation of the *Parallel to NSX DLR Using VLANs Overlays with BIG-IP* deployment scenario.

Topology 3: One-Arm connected using VXLAN Overlays with BIG-IP Virtual Edition

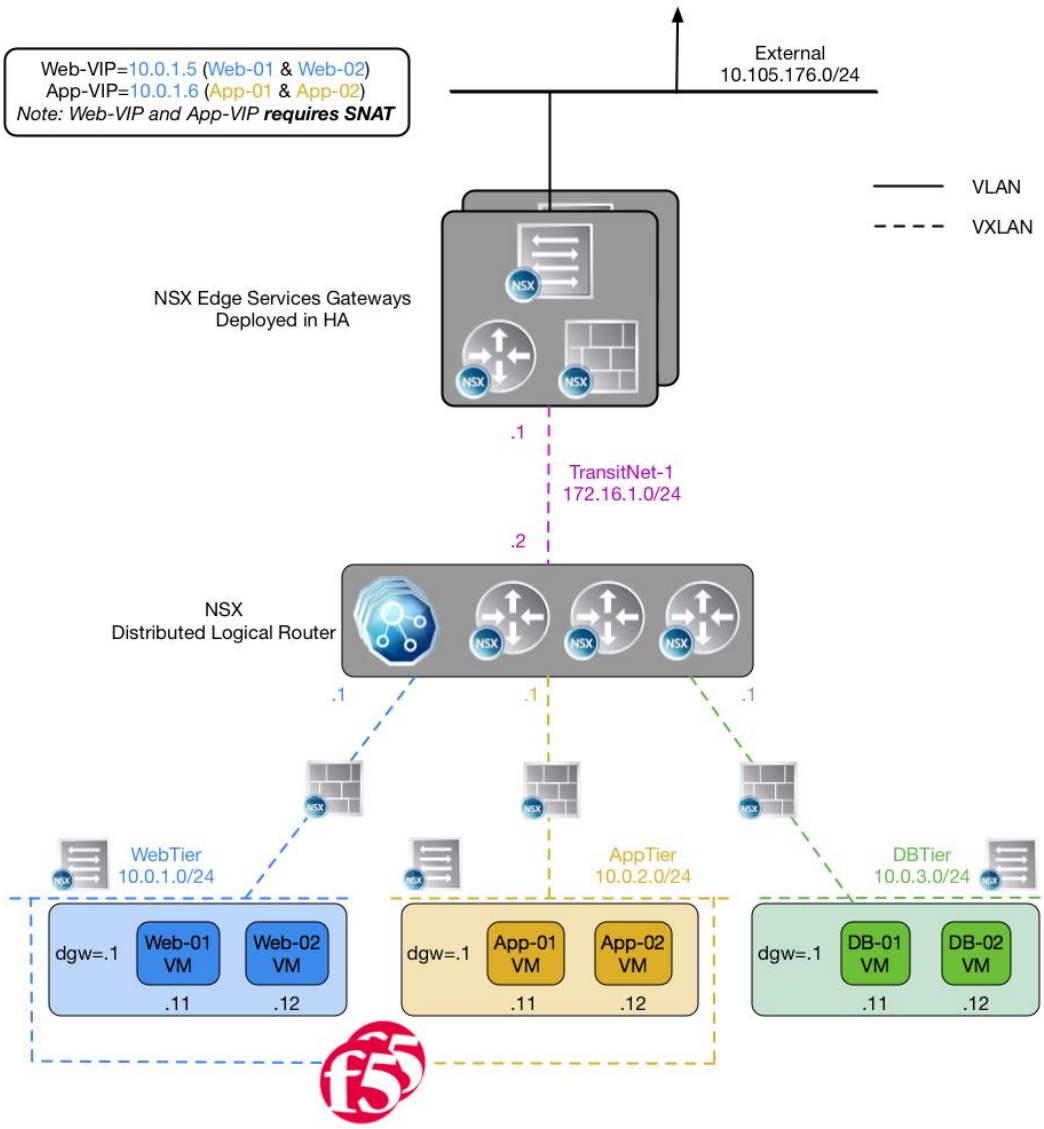


Figure 10 BIG-IP Virtual Edition in one-arm topology within VXLAN environment

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.

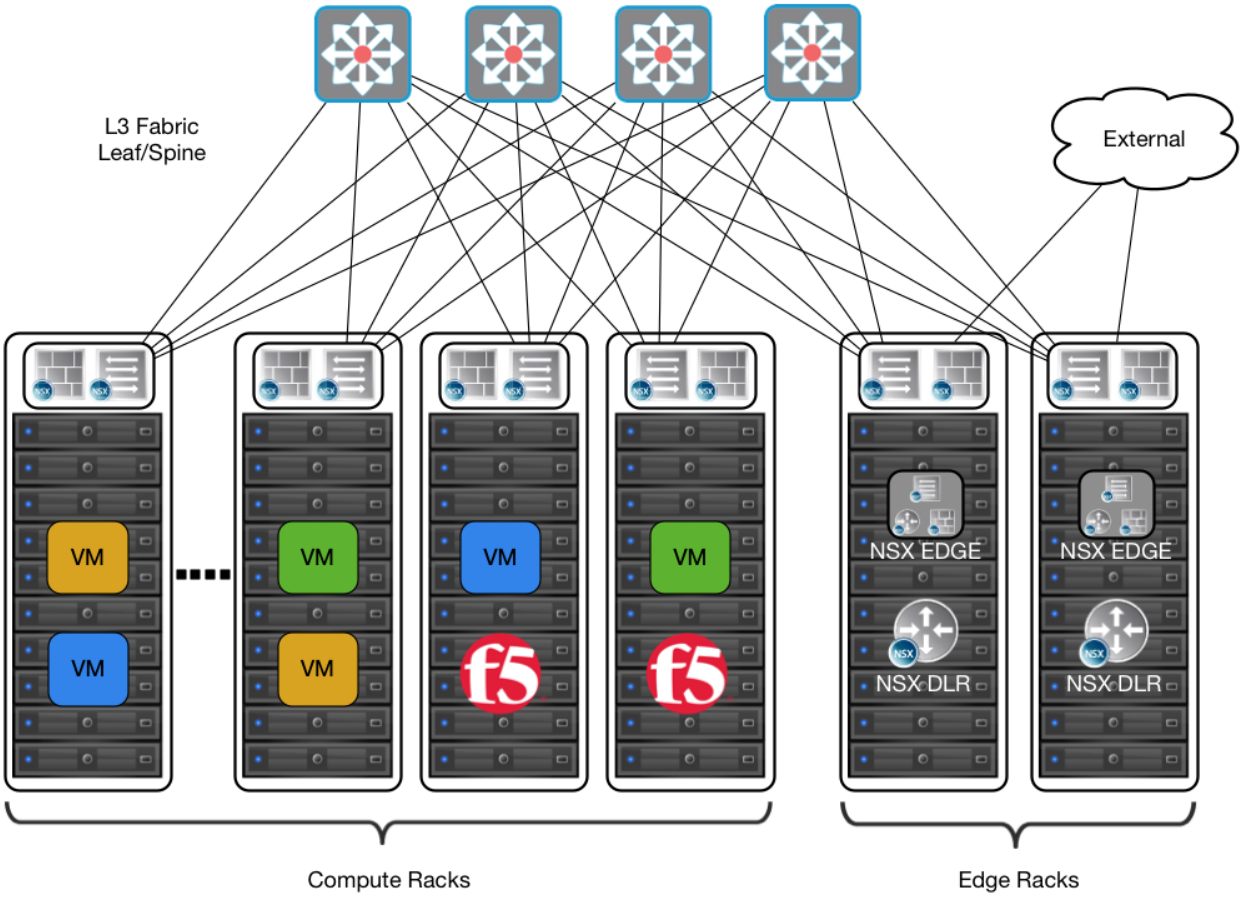


Figure 11 Leaf/spine physical rack infrastructure

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. In this scenario the BIG-IP virtual appliances should be allowed to connect to the logical switches that are connected to the VM's acting as part of the internal network. The BIG-IPs are located in the Compute racks with the workload VMs to emulate this scenario.

Note: This can be done with physical boxes however requires access to the OVSDB to access the VXLAN and we will go over that scenario in topology 4.

Traffic Flows

North-South Traffic - Logical Traffic Flows as Follows

1. From Client (External) to NSX Edges to NSX DLR to BIG-IP WebTier VIP (Web-VIP)
2. From BIG-IP VE to WebTier Servers
3. From WebTier Servers to NSX DLR to BIG-IP AppTier VIP (App-VIP)
4. From BIG-IP VE to AppTier Servers
5. From AppTier Servers to DLR to DB-Tier Servers

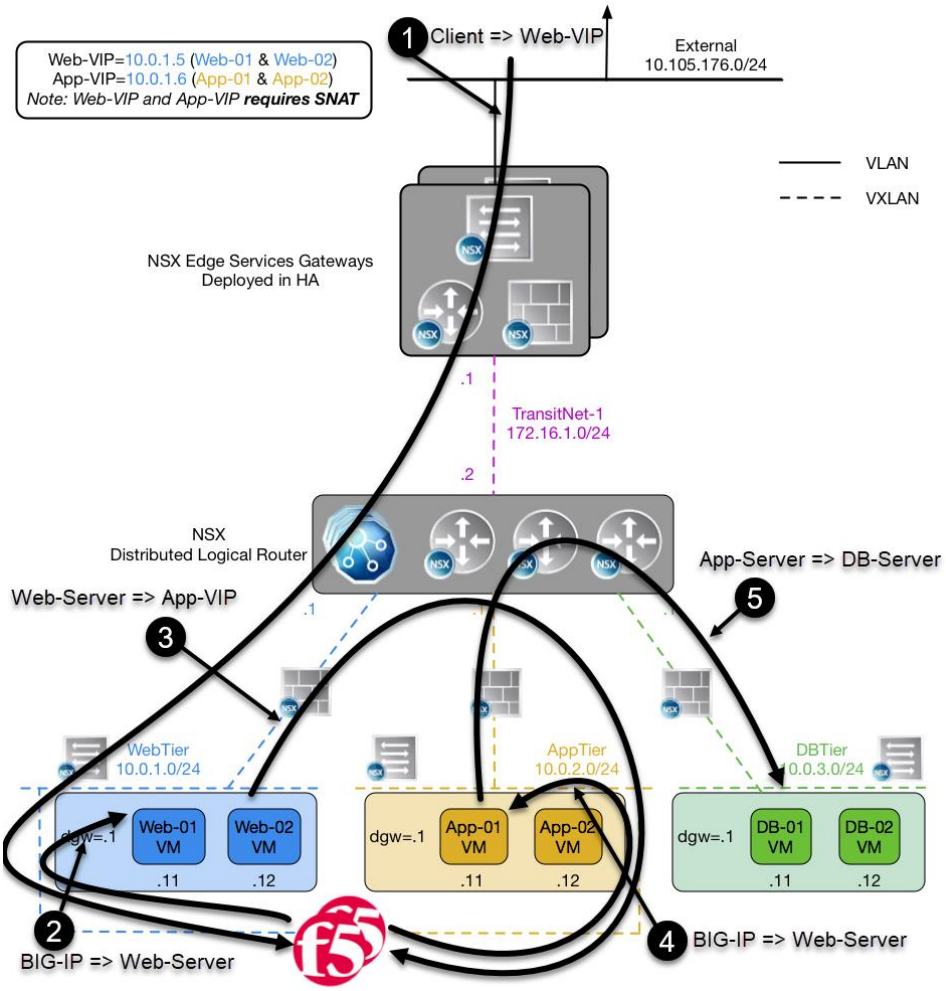


Figure 12 North-South Logical Traffic Flow "One-arm Connected" with BIG-IP Virtual Edition

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 13: the Cluster1-VDC (Edge Racks) and Cluster3-Compute-NSX (Compute Racks). 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 10.

Figure 13 vSphere Console

In accordance with best practices, edge and compute ESXi hosts are physically and logically separated from one another. BIG-IP Virtual Editions are installed in the compute cluster for this scenario that is consistent with Figure 11

The virtual machines used as Web (Web), Application (App), and Database (DB) servers will be running on ESXi hosts in the compute cluster.

Prerequisites

Referencing the diagram in Figure 10, 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, WebTier and AppTier, 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	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176	176
Internal	DVS-VLAN-102	102

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

Name	Transport Zone	Segment ID	Control Plane Mode
WebTier	TransportZone1	5001	Unicast
AppTier	TransportZone1	5002	Unicast
DBTier	TransportZone1	5003	Unicast
TransitNet-1	TransportZone1	5004	Unicast

Table 12 Logical switch configuration

Note: In our environment, we put the F5 BIG-IP management interface on the DVS-VLAN-102 network so that we could obtain clear web GUI screenshots from our web browser client on that network.

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 176 (External)** is the VLAN used for external connectivity. The 10.105.176.0/24 IP subnet range is configured on this VLAN.
- **VLAN 102 (Internal)** (not shown) is for management connectivity. The 192.168.14.0/24 IP subnet range is configured on this VLAN

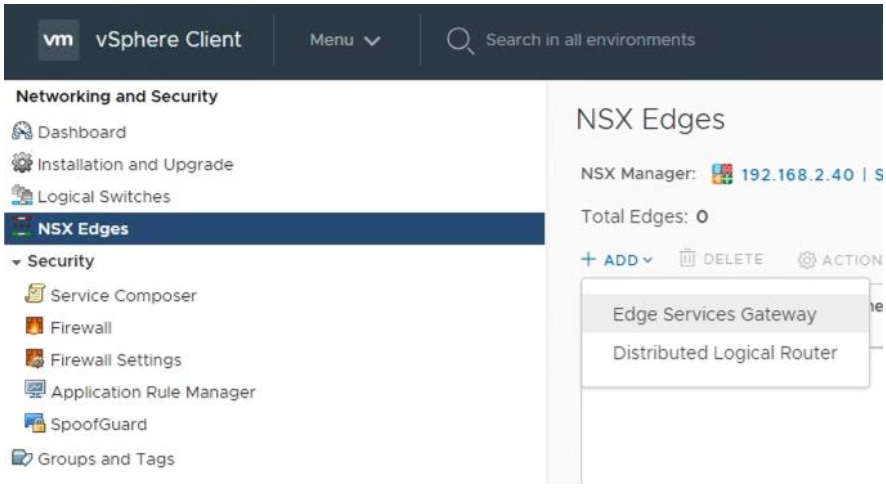
VXLAN Segments

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

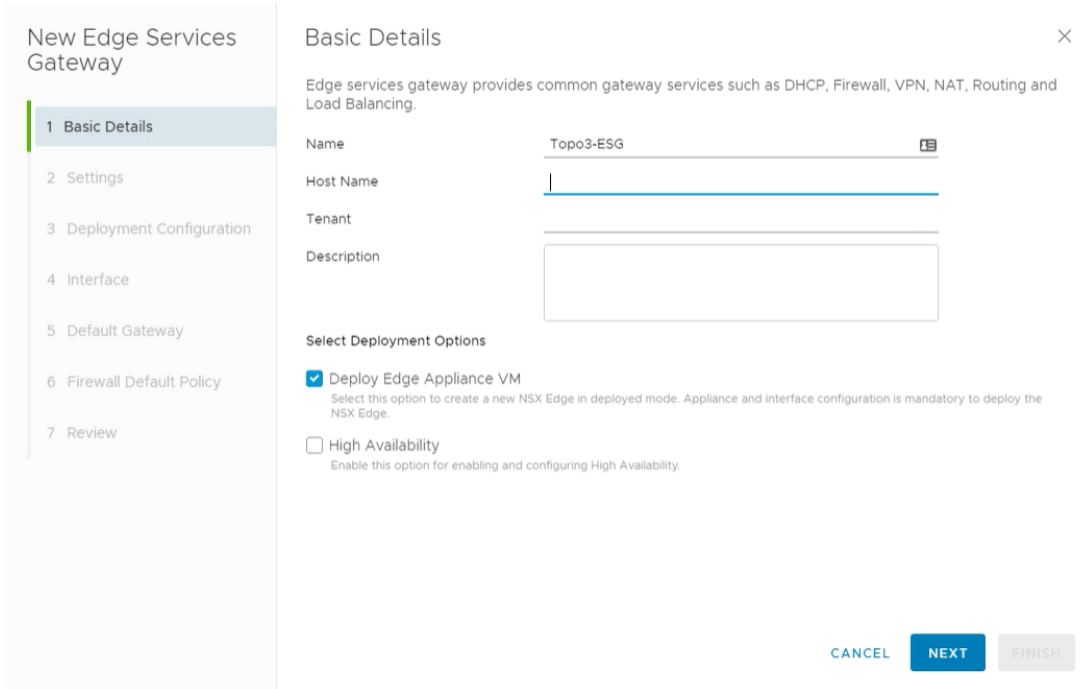
- VXLAN 5001 WebTier is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5002 AppTier is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5003 DBTier is the segment ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5004 TransitNet-1 is the VXLAN segment ID used for the transport zone between the DLR and the NSX Edge.

NSX Edge Configuration

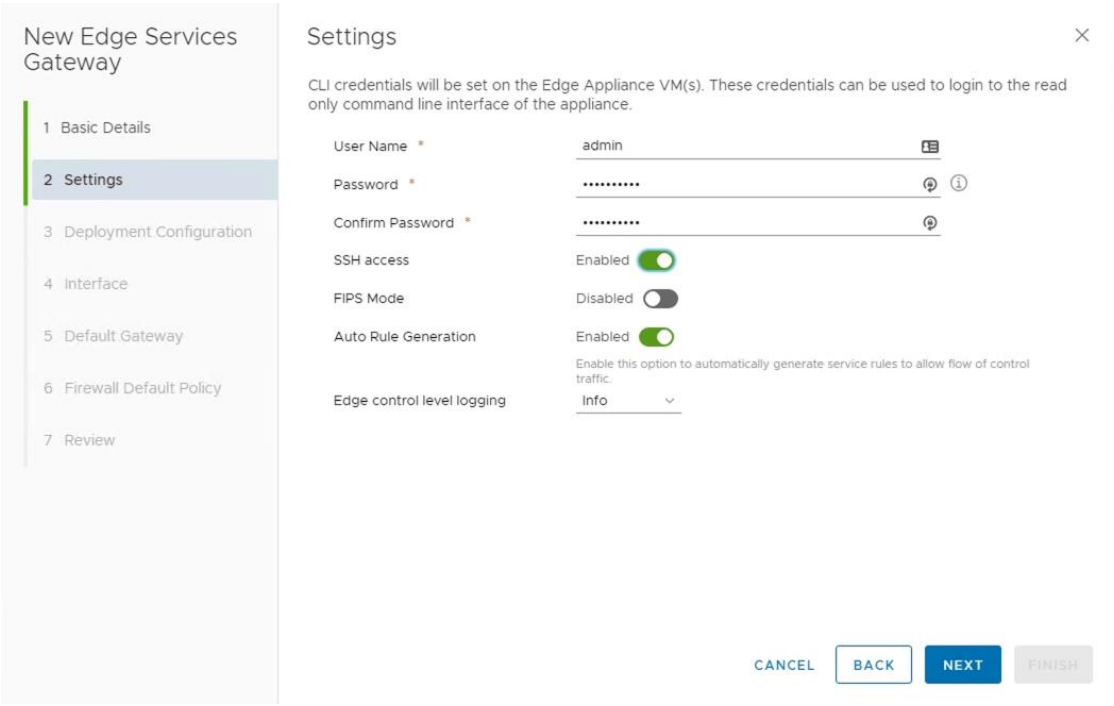
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then click (+ Add) hyperlink → Click on “Edge Services Gateway”.



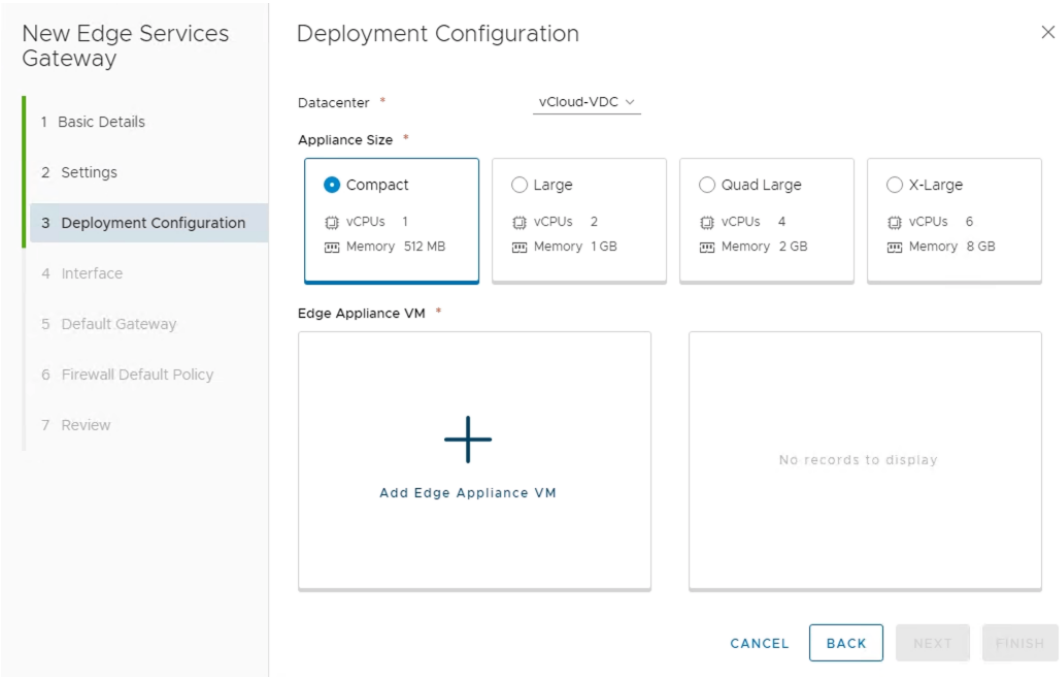
2. Provide a name for the device, then click next.



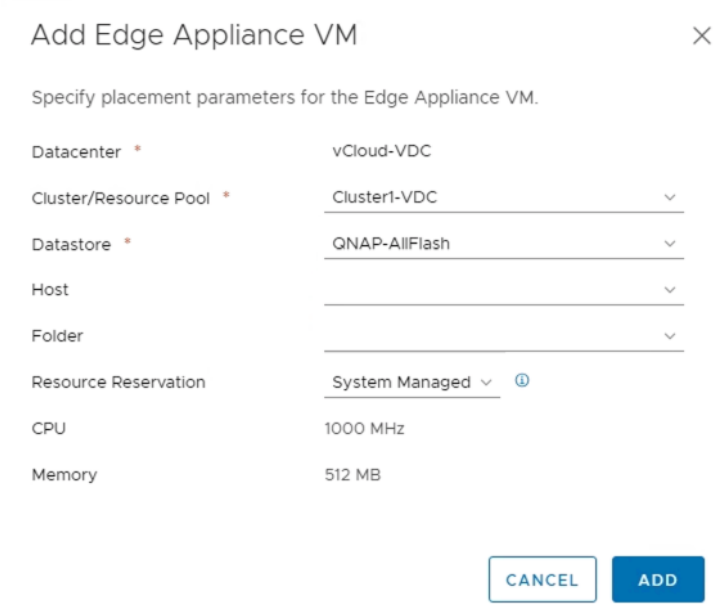
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.



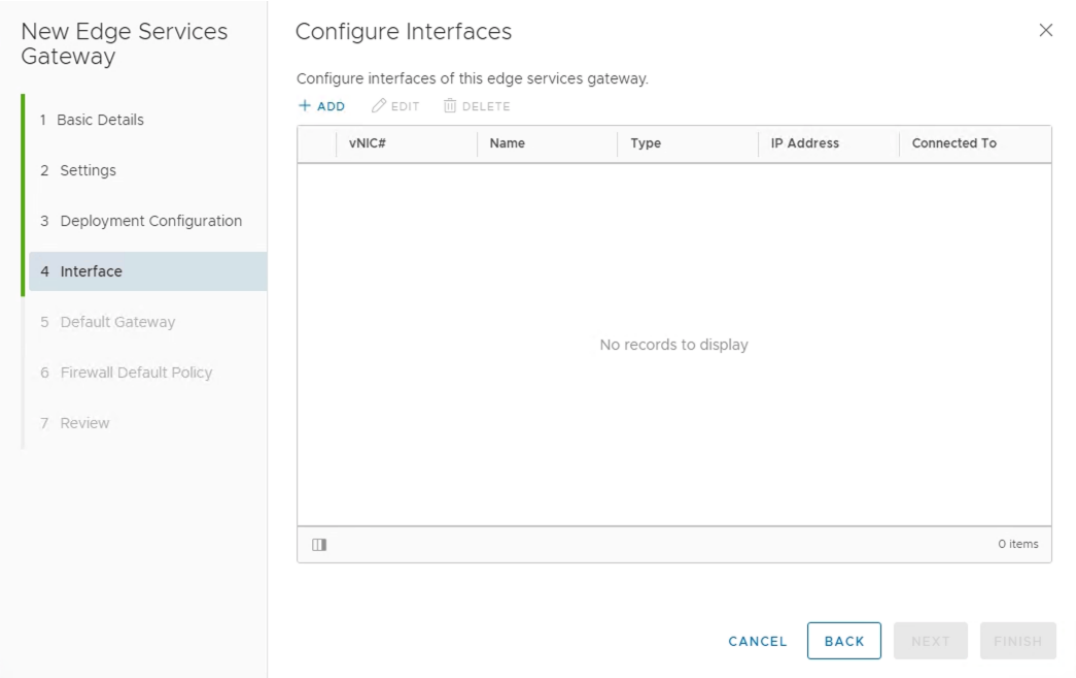
4. Under Configure deployment, select the Datacenter and Appliance Size appropriate for your deployment. Then click on the plus symbol (+) to Add Edge Appliance VM.



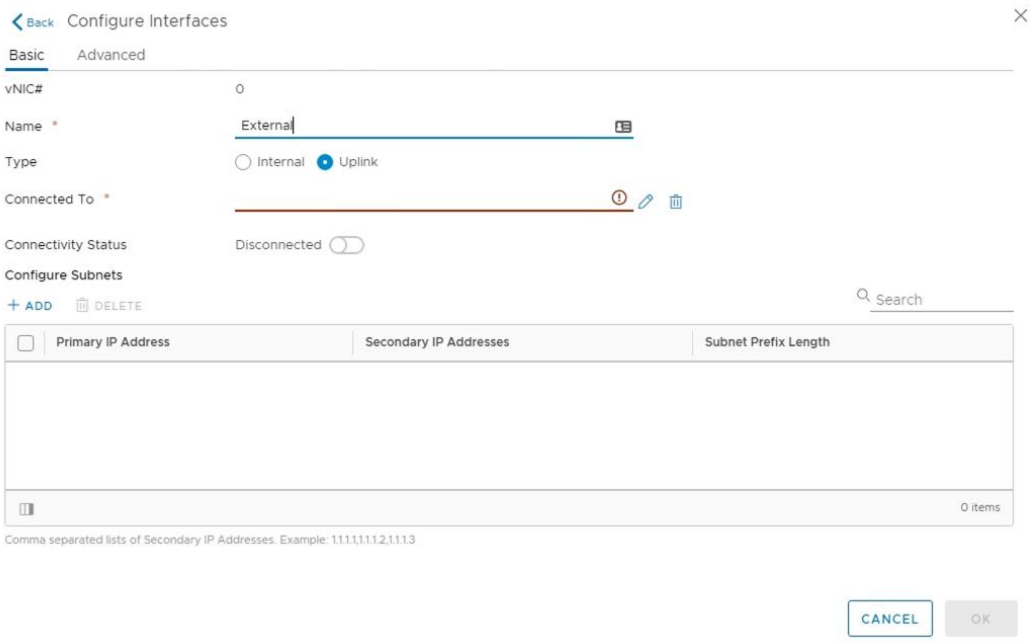
5. Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete. This will return you to the configure deployment screen shown in step 4 with the Edge Appliance VM filled out. Click **Next** to continue.



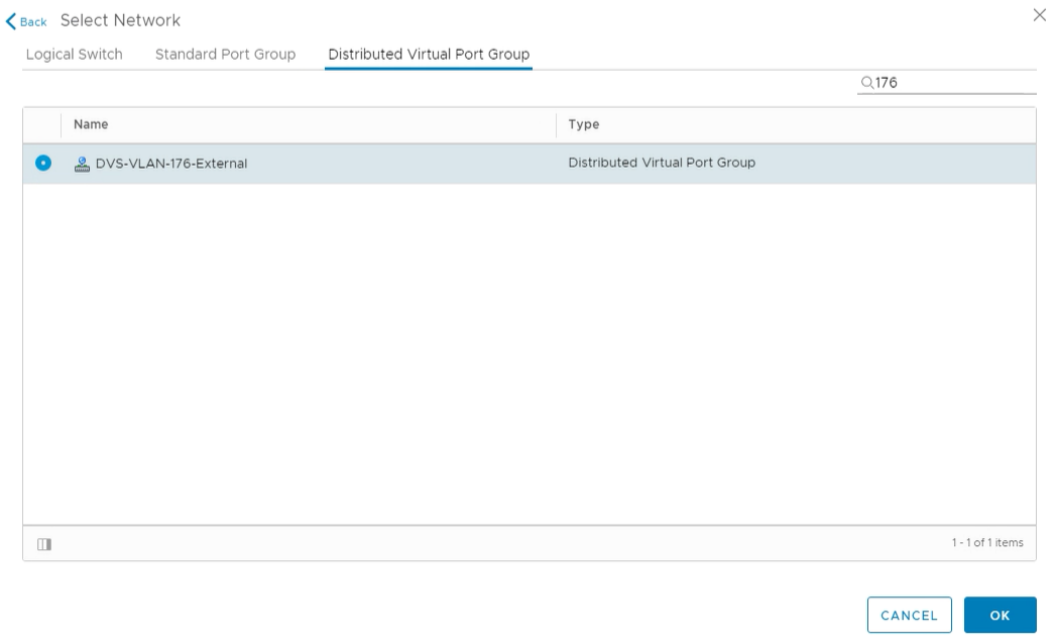
6. In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX Edge Interface dialog box.



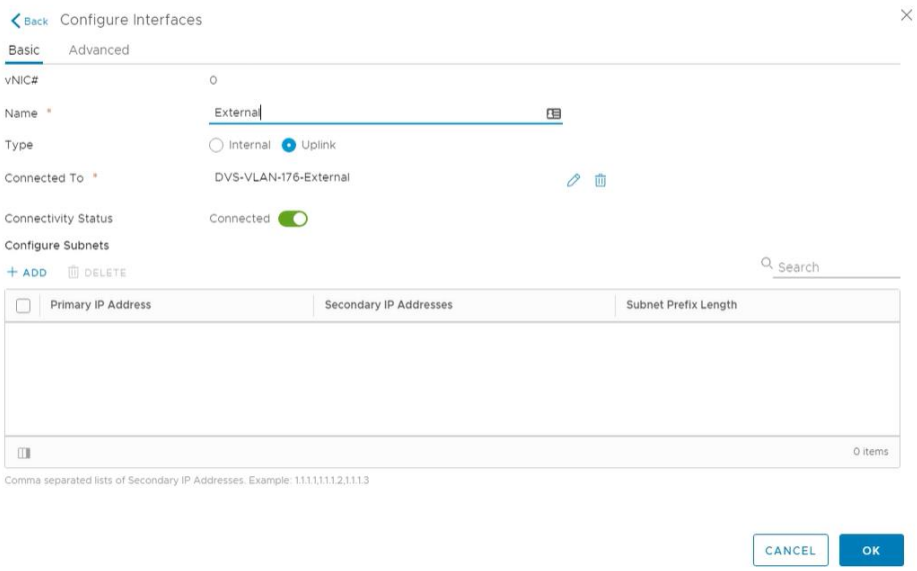
7. Provide a name and click the edit icon next to the “Connected To” field



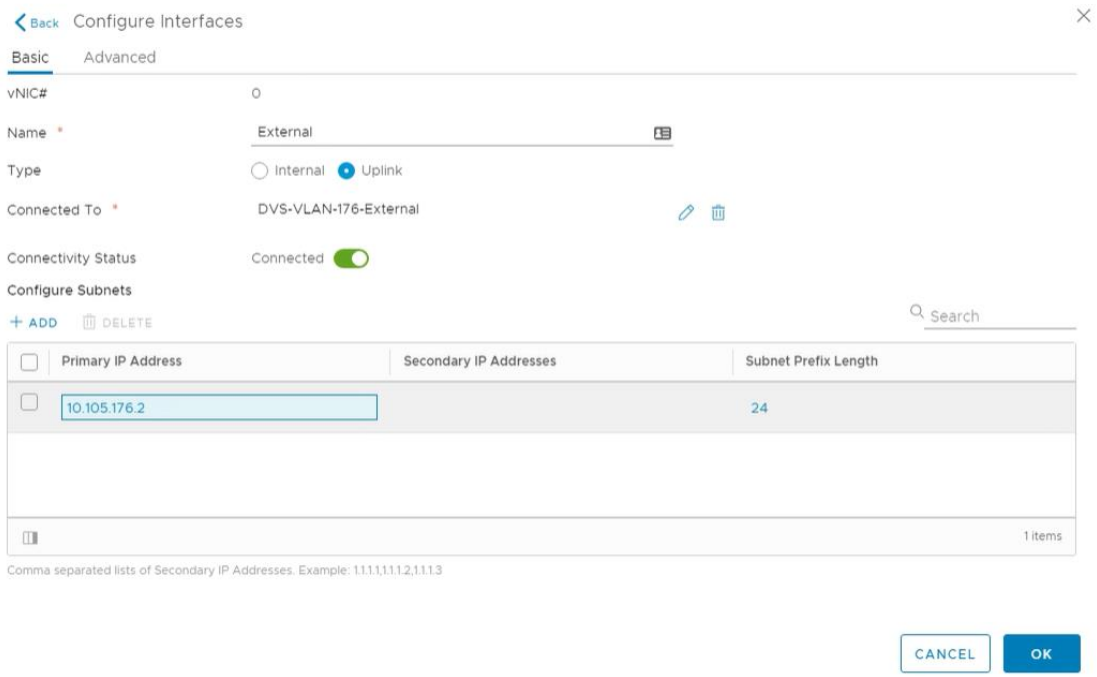
8. For the External network, click on the Distributed Virtual Port Group tab and then selecting the port group used for external access. Click OK.



9. Once the network is chosen, select the (+ Add) hyperlink 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.

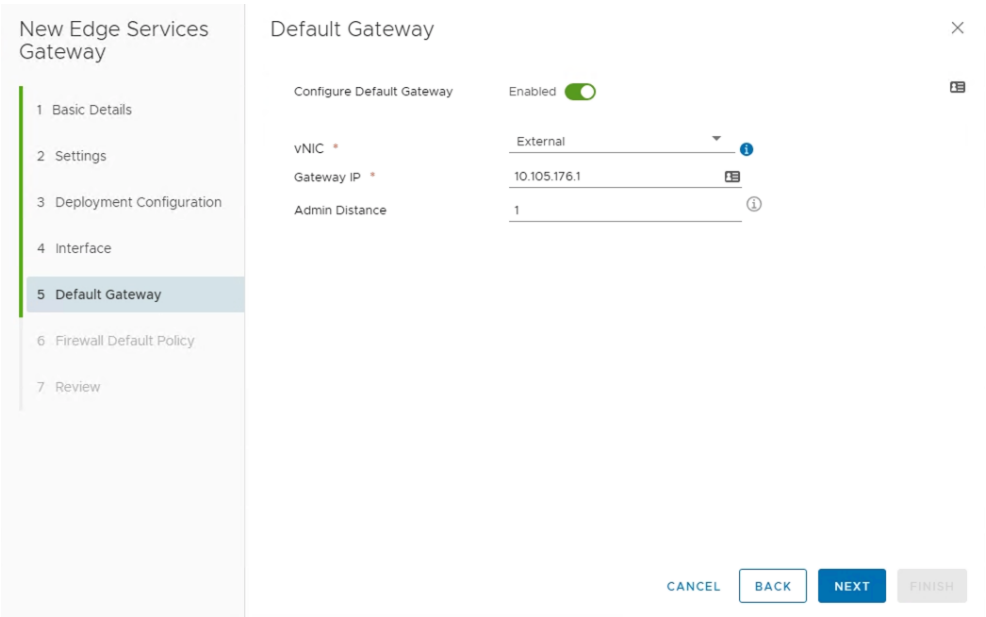


11. This will bring you back to the Configure interfaces dialog box. For each of the three interfaces required for this deployment scenario, add and configure the appropriate subnets and switch type, according to the table below and look like the final picture below with your datacenter information.

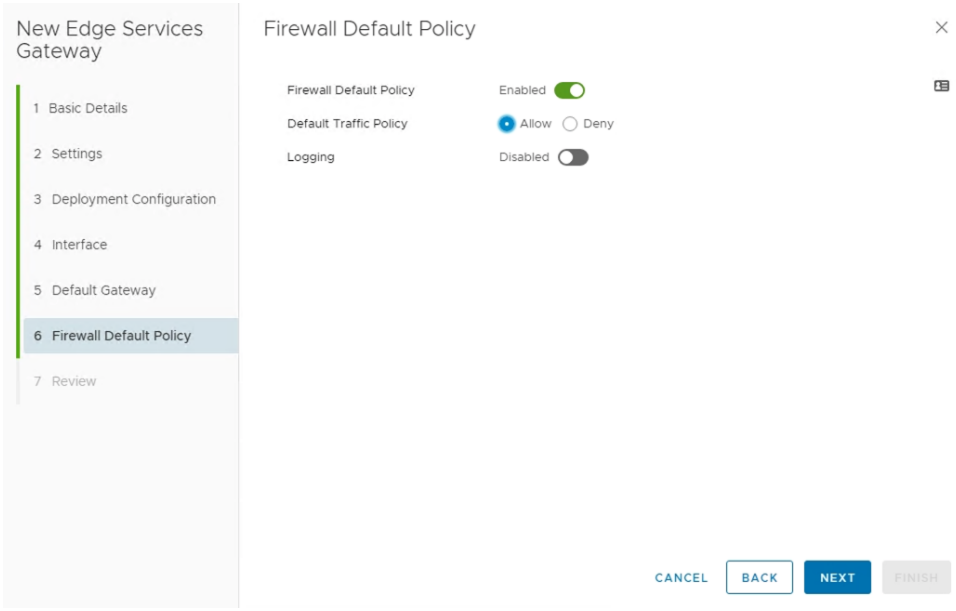
Network Name	Type	Network Type	IP Address	Connected To
External	Uplink	Distributed Virtual Port Group	10.105.176.2/24	DVS-VLAN-176-External
TransitNet-1	Internal	Logical Switch	172.16.1.1/24	TransitNet-1

Table 13 NSX Edge network interfaces

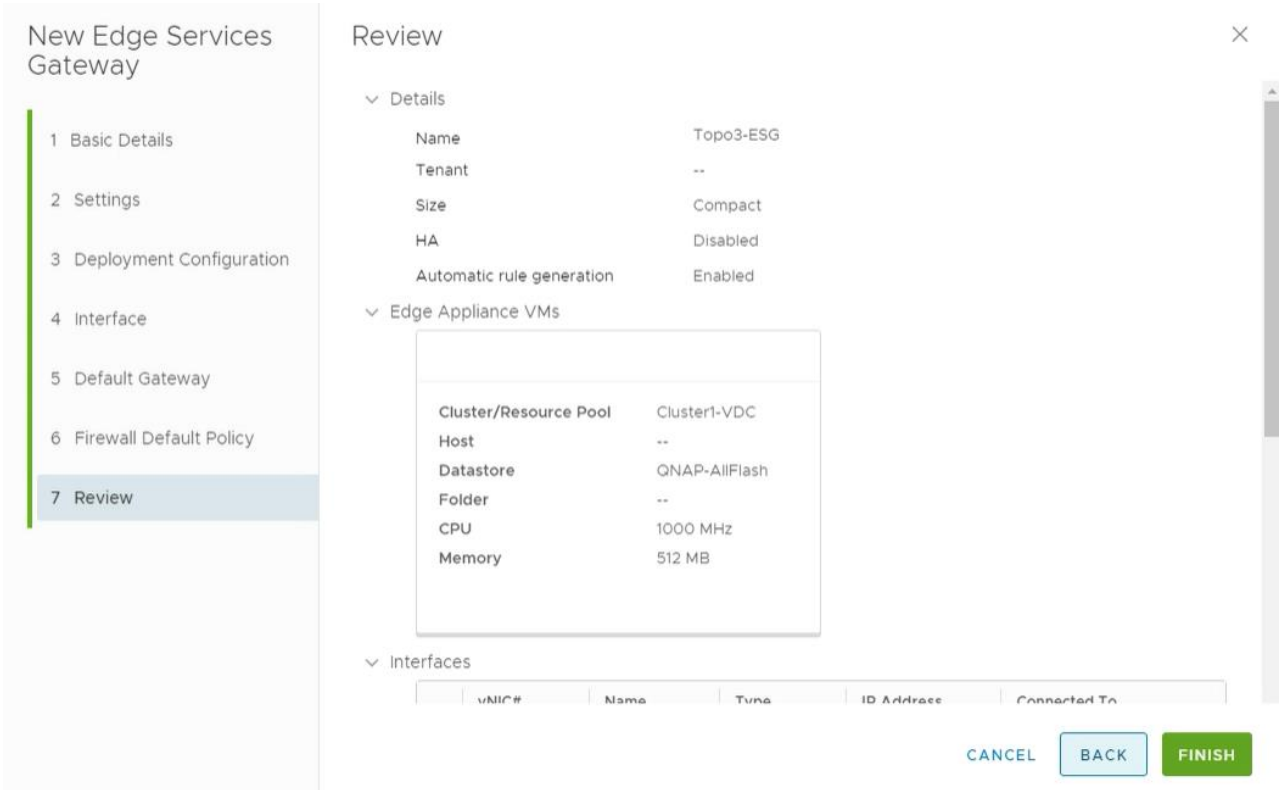
12. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway is our data center backbone router with the IP address of 10.105.176.1 on External vNIC that we configured under the interface settings. If asked use the default MTU parameter 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. Enable the “Firewall Default Policy” and check Allow for the Default Traffic Policy. (This is for validation testing; firewall can be set to Deny instead however firewall rules will be required on ESG to allow for traffic to flow from ESG/DLR and F5)

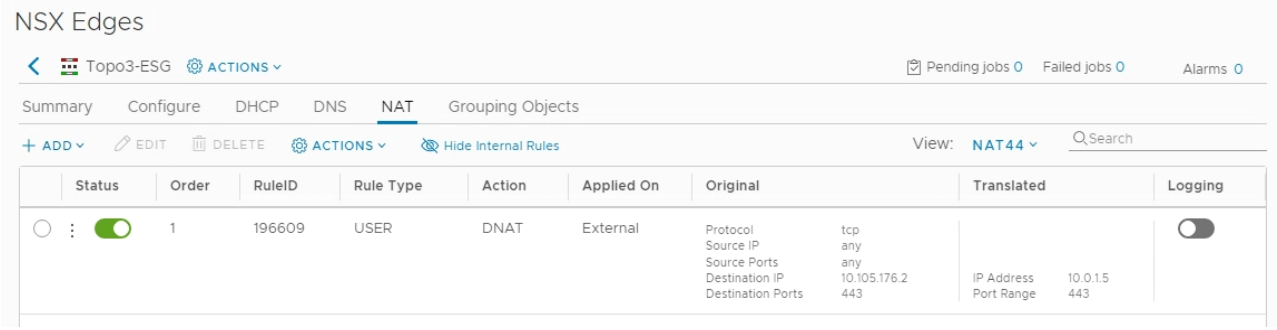


14. Review and click finish to complete the deployment of the NSX Edge.



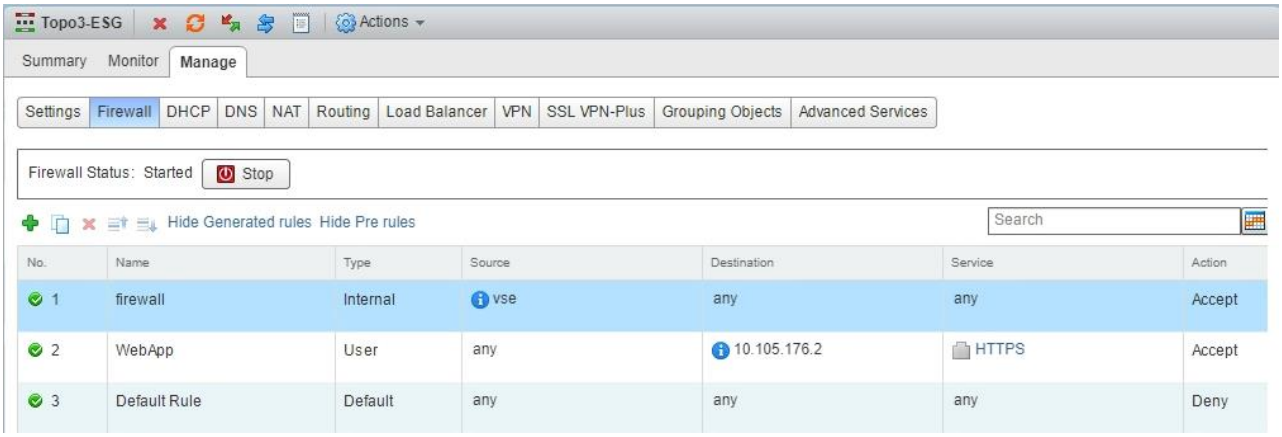
15. Create a NAT configuration to access the BIG-IP through the VXLAN from an external interface. To configure NAT rules Home → Network and Security → NSX Edges → Double Click on Edge (Topo3-ESG) → NAT Tab.

    Adding Rules Click the (+ Add) hyperlink → Add DNAT Rule. In our configuration we will use External Interface and allow port 443 TCP via the DNAT to the External Interface IP (10.105.176.2) and forward 443 TCP traffic to our BIG-IP VIP (10.0.1.5).



16. If the "Firewall Default Policy" was set to Deny traffic in earlier configuration, a firewall rule must be created to allow traffic to access the environment. (Currently, these can only be configured via vSphere Flex [FLASH] client) To configure firewall rules Home → Network and Security → NSX Edges → Double Click on Edge (Topo3-ESG) → Firewall Tab.

    Adding Rules Click the (+) button and add appropriate firewall rule to allow External Traffic talk to the 10.105.176.2 address over HTTPS, the 10.105.176.2 address is the External Interface on the ESG that we will use to NAT to the backend BIG-IP VIP 10.0.1.5 (in the one-armed configuration)

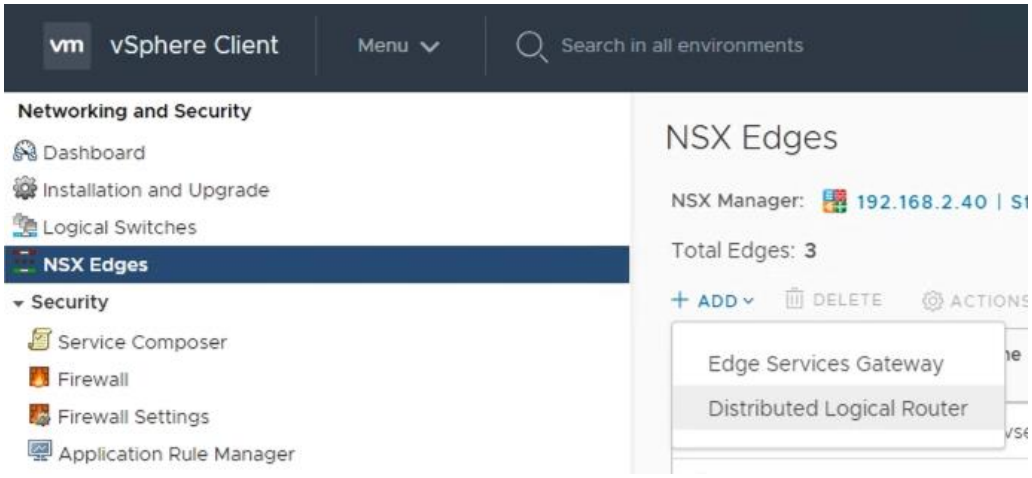


Create and Deploy DLR

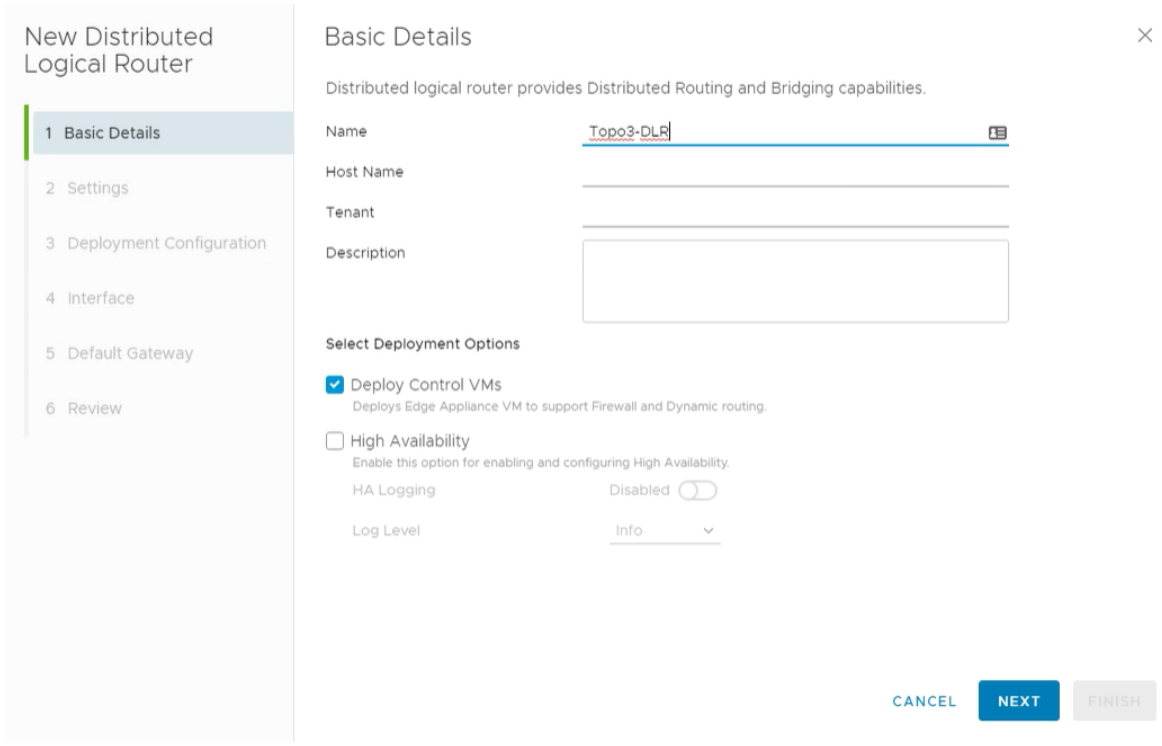
Within VMWare NSX, the Distributed Logical Router (DLR) provides an optimized way of handling east-west traffic within the data center. East-west traffic consists of communication between virtual machines or other resources on different subnets within a data center. As east-west traffic demand increases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

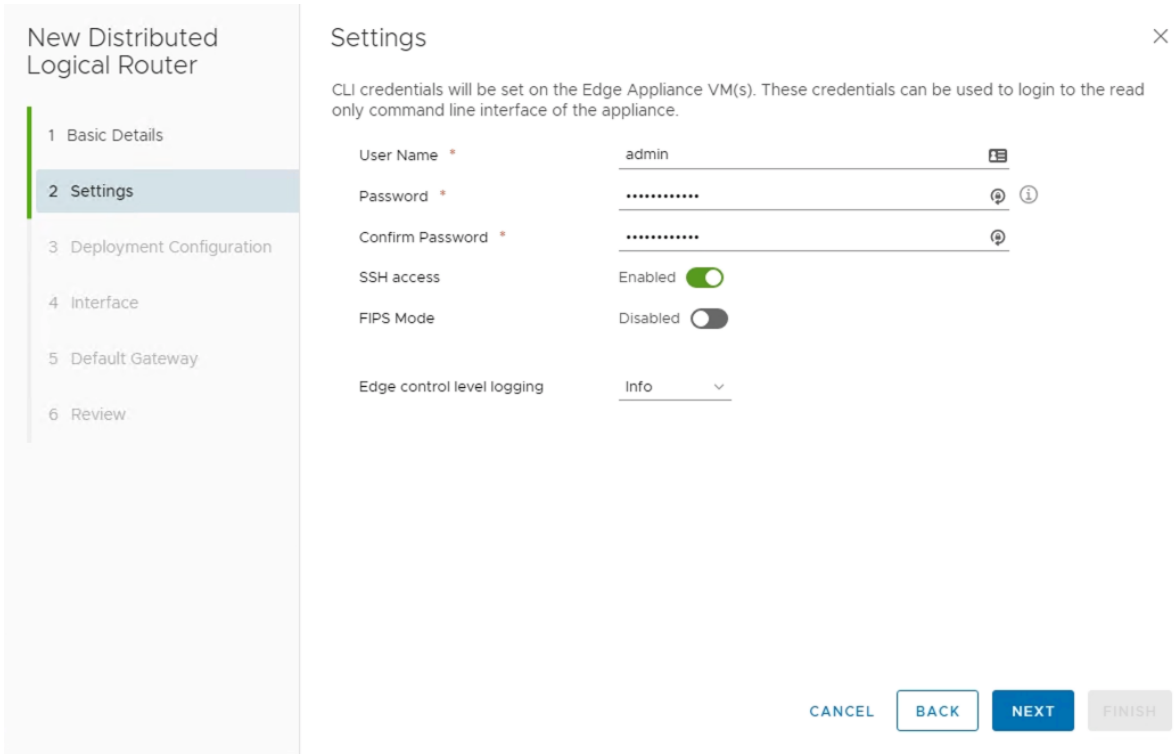
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then click (+ Add) hyperlink → Click on “Distributed Logical Router”



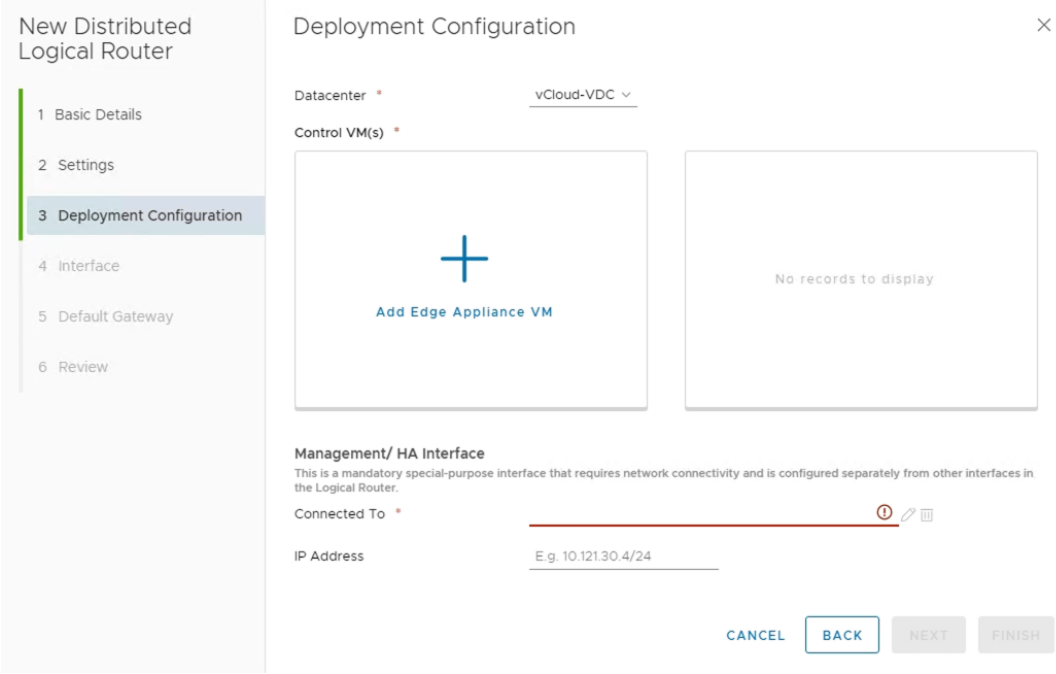
2. Provide a name for the device, then click next.



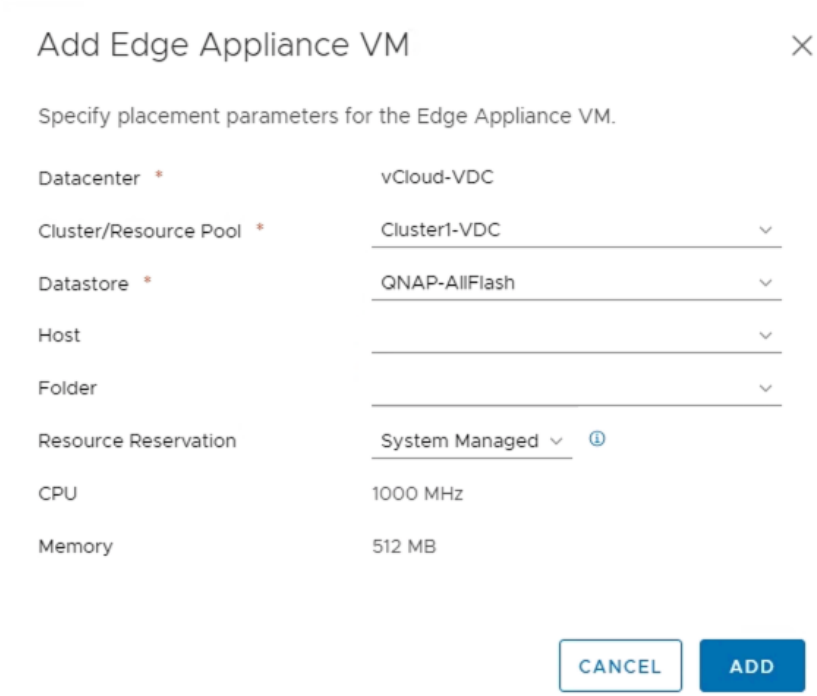
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.



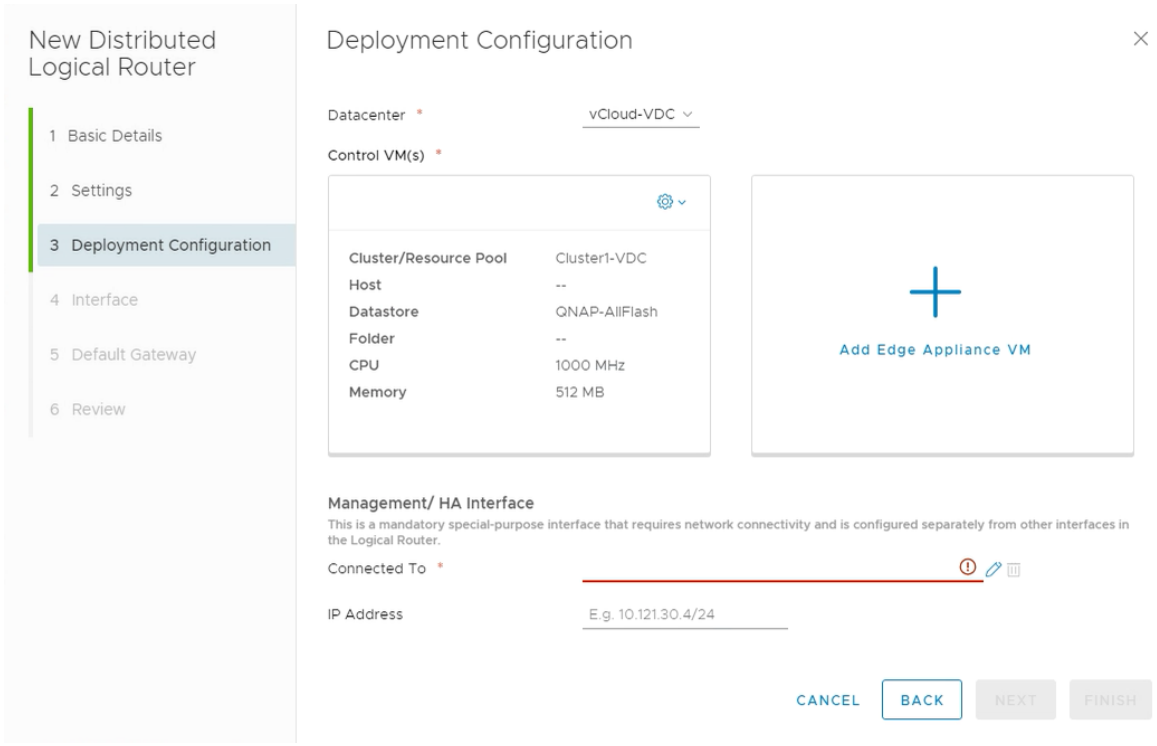
4. Under Configure deployment, select the Datacenter and Appliance Size appropriate for your deployment. Then click on the plus symbol (+) to Add Edge Appliance VM.



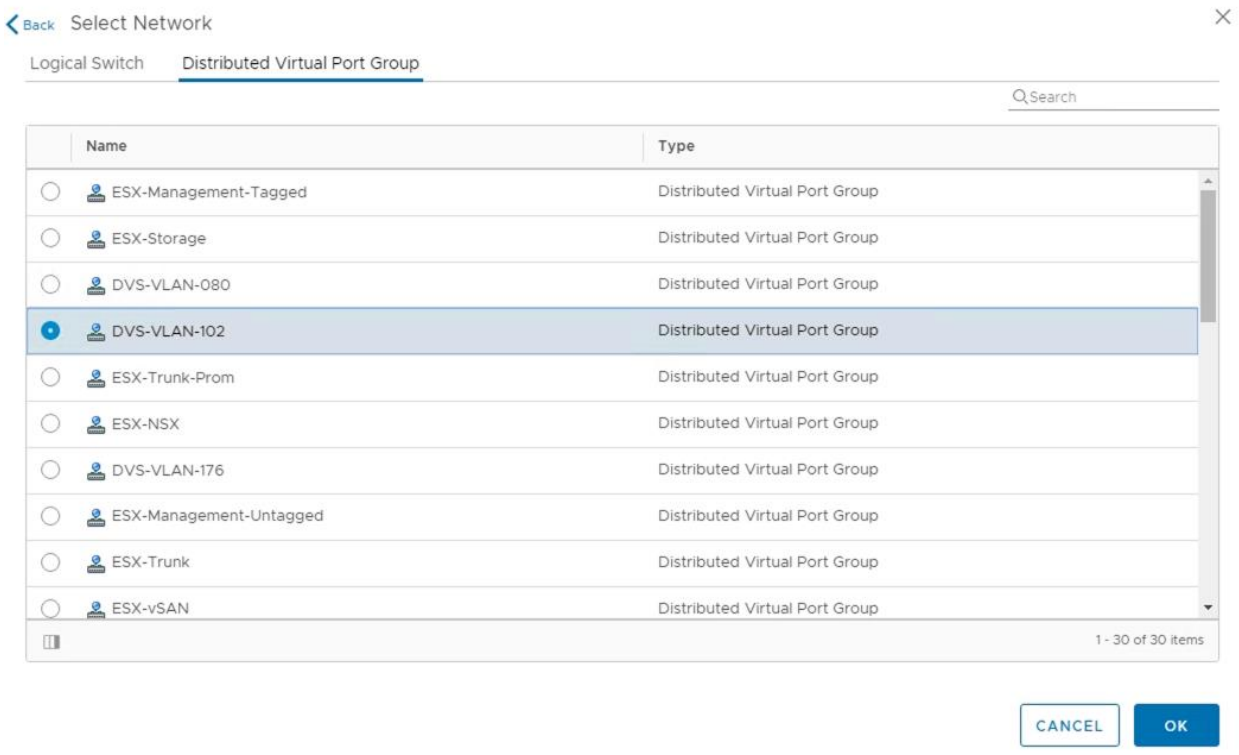
5. Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete.



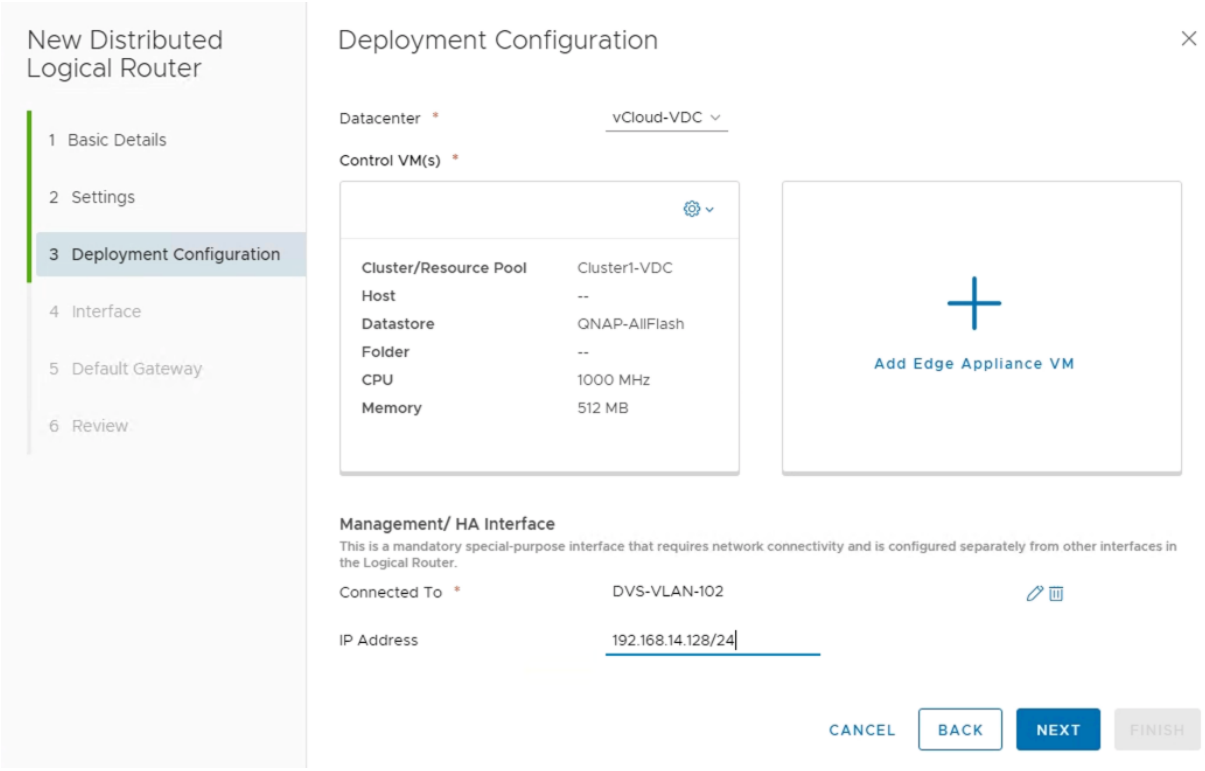
6. Click the Edit icon in the “Connected To” section of the Management/HA Interface



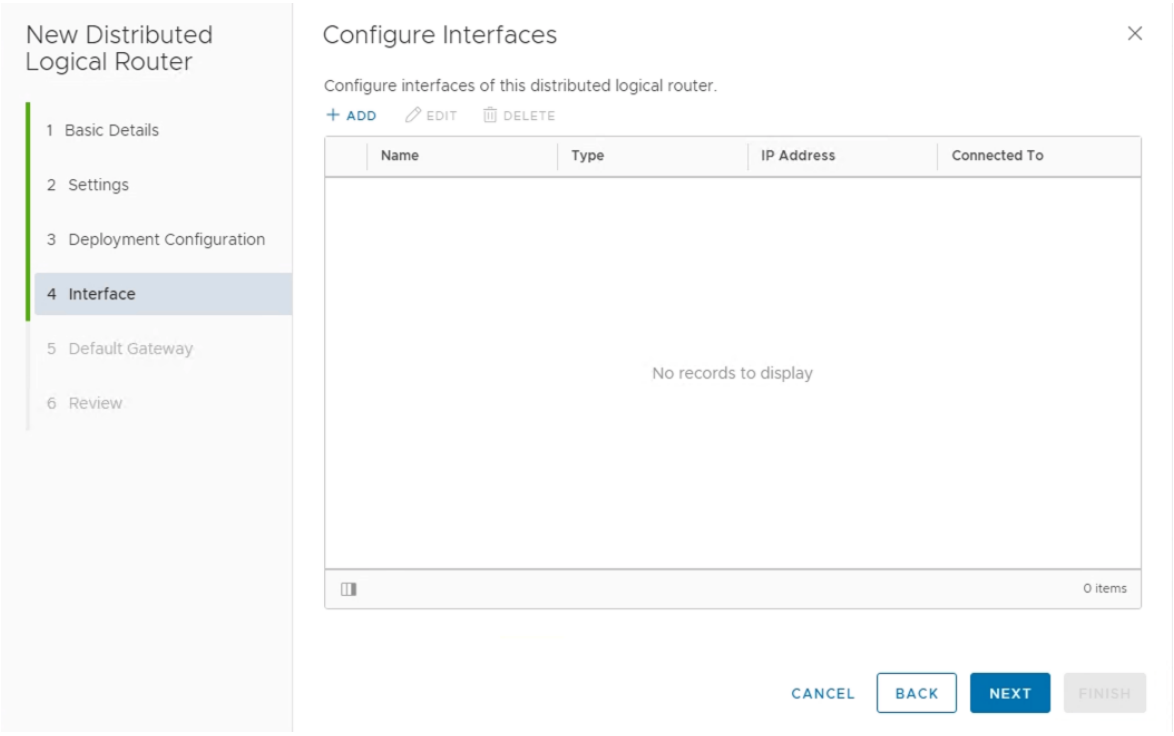
7. Select an appropriate Management Network (Distributed Virtual Port Group) to manage the DLR then Click OK



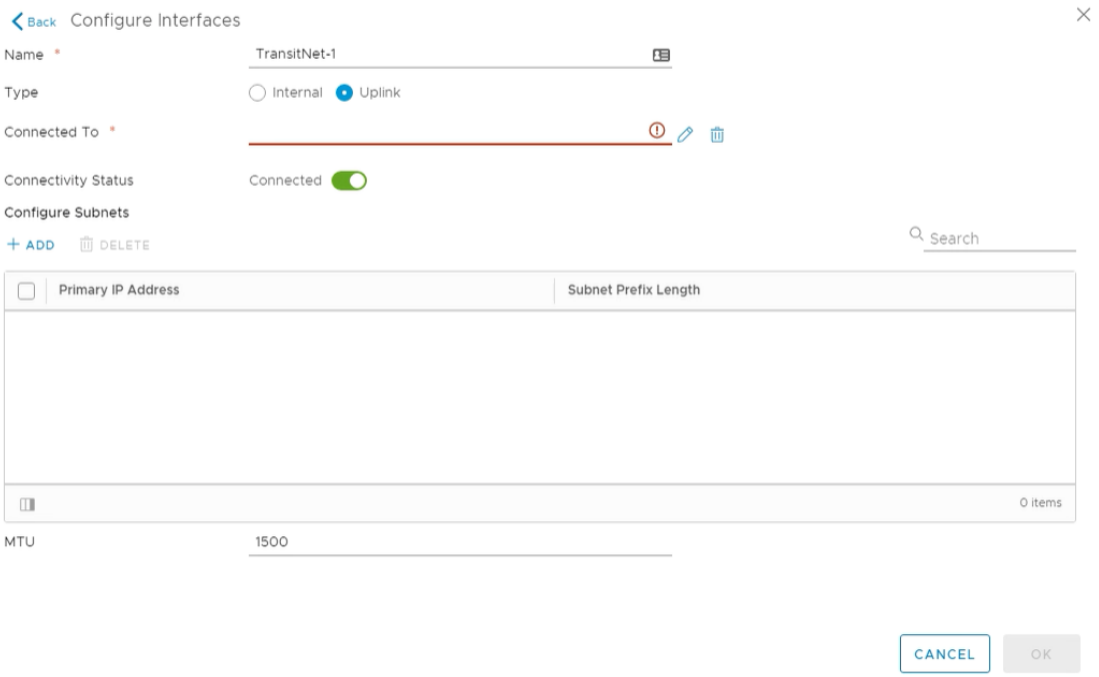
8. Fill out the IP/Subnet Field for the Management IP of the DLR then Click Next



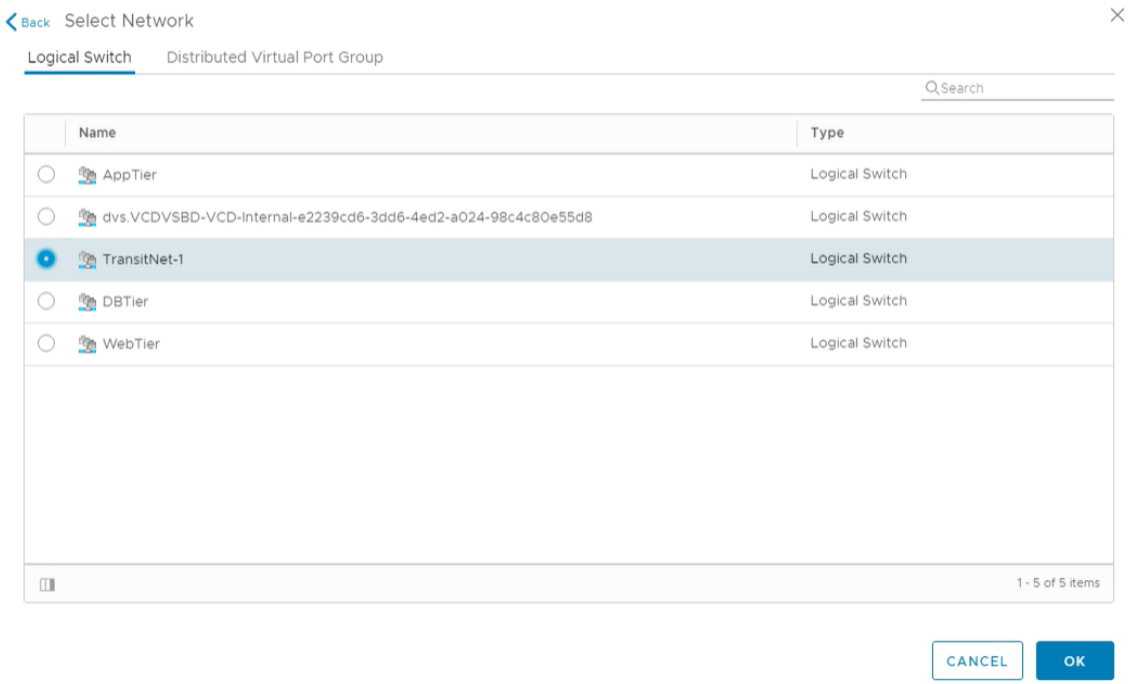
9. In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX DLR Interface dialog box.



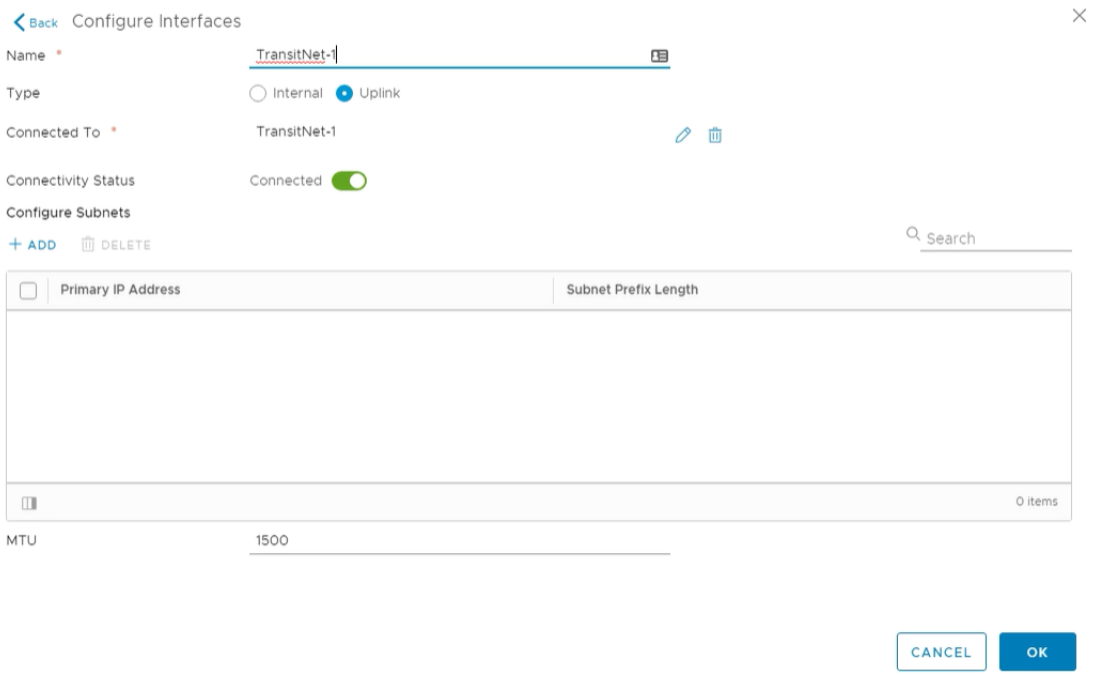
10. Provide a name and click the edit icon next to the “Connected To” field



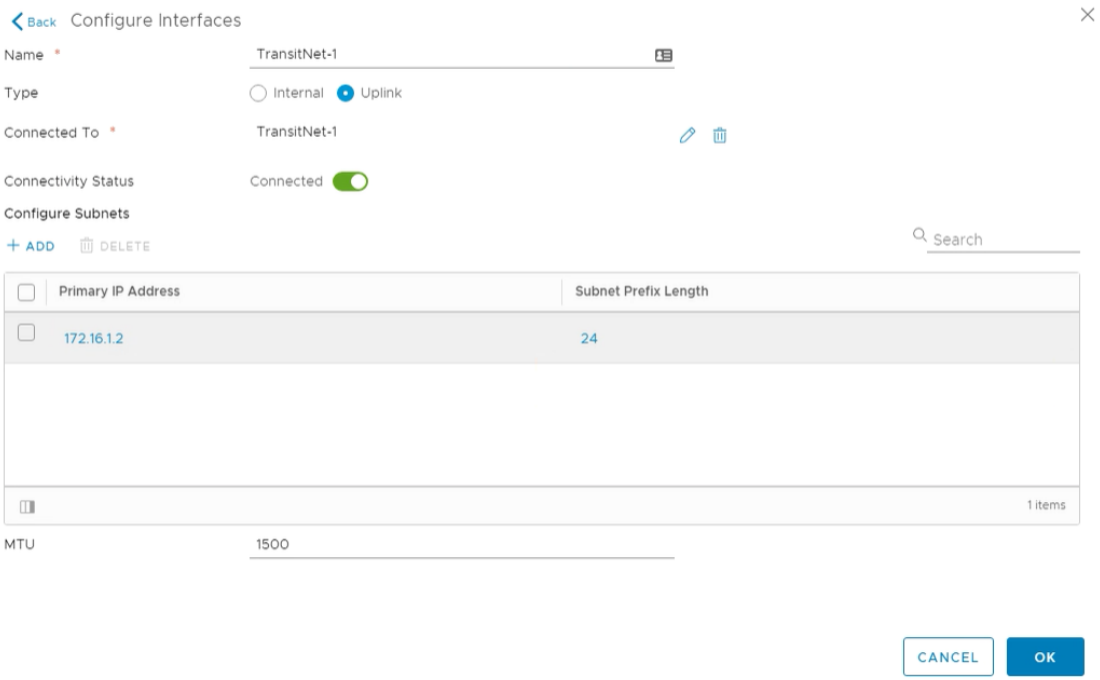
11. For the TransitNet-1 network, click on the Logical Switch tab and then selecting the TransitNet-1 Logical Switch. Click OK.



12. Once the network is chosen, select the (+ Add) hyperlink under Configure subnets to add the appropriate IP address and subnet configuration to the interface.



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



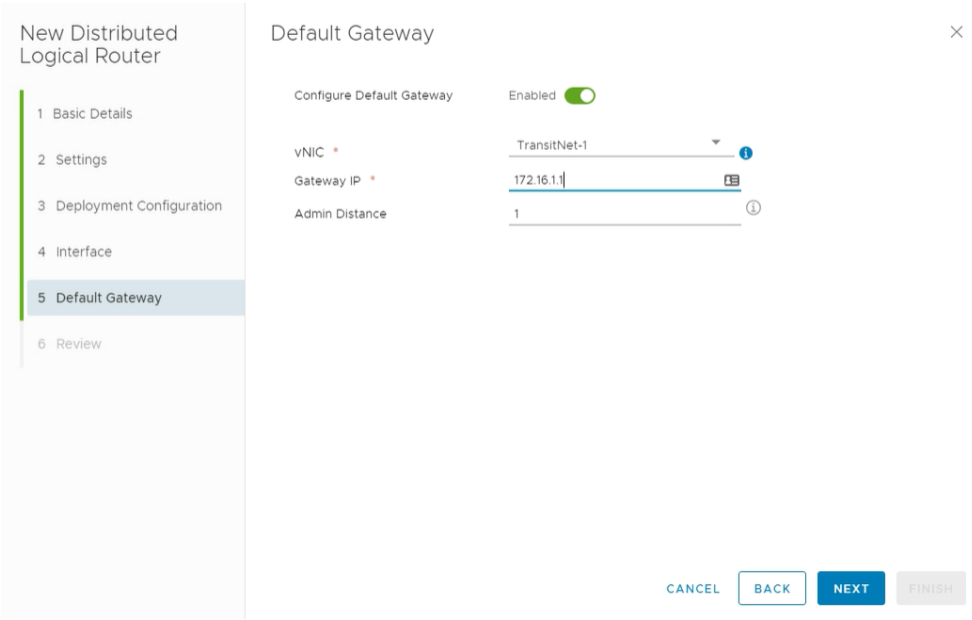
14. This will bring you back to the Configure interfaces dialog box. For each of the four interfaces required for this deployment scenario, add and configure the appropriate subnets and switch type, according to the table below and look like the final picture below with your datacenter information.

Network Name	Type	Network Type	IP Address	Connected To
TransitNet-1	Uplink	Logical Switch	172.16.1.2/24	TransitNet-1
WebTier	Internal	Logical Switch	10.0.1.1/24	WebTier
AppTier	Internal	Logical Switch	10.0.2.1/24	AppTier
DBTier	Internal	Logical Switch	10.0.3.1/24	DBTier

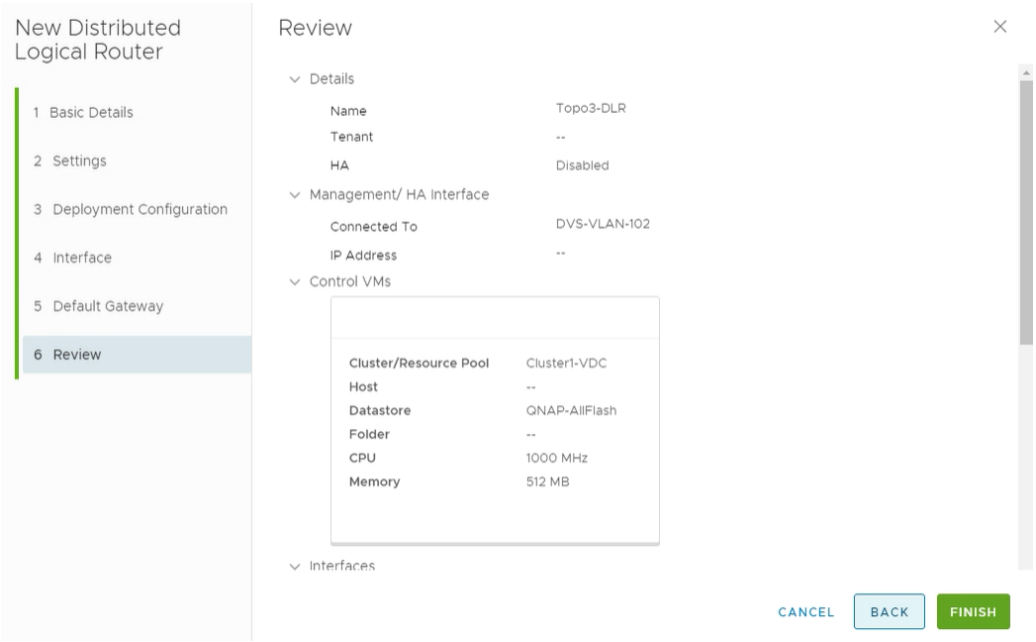
Table 14 NSX distributed logical router network interfaces

15. Once the interface settings are completed, 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 TransitNet-1.

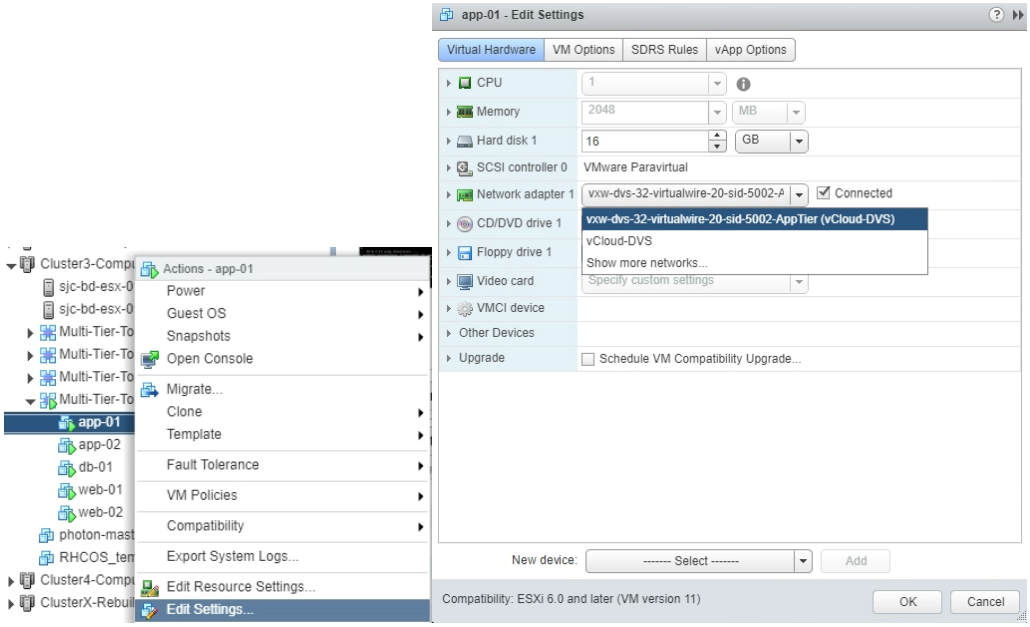
    For the vNIC select TransitNet-1 and provide the Gateway IP address of the NSX Edge.
    In this example, its 172.16.1.1. Click Next to proceed.



17. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



18. After the Creation of the DLR and the logical switches within vSphere, attach the Virtual Machines for each tier to their logical switches for network traffic. (This is an example of one of our AppTier VM's attached to the AppTier Logical Switch.



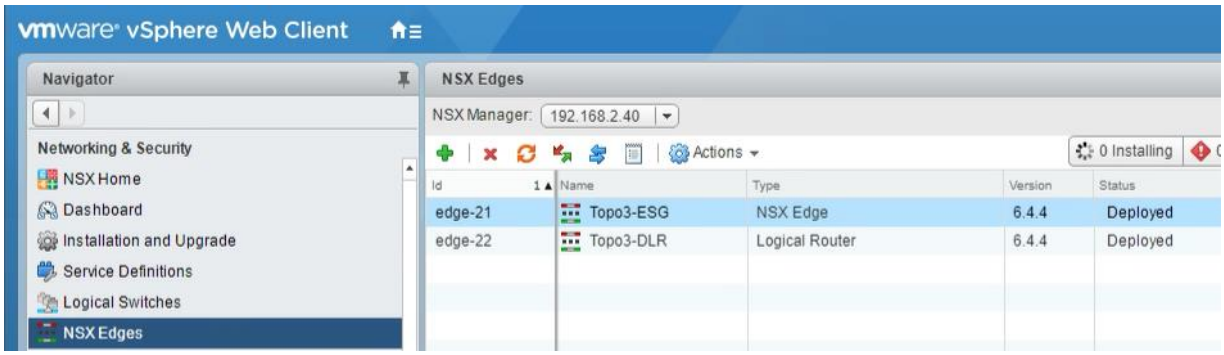
NSX Edge Static Routing Configuration

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.

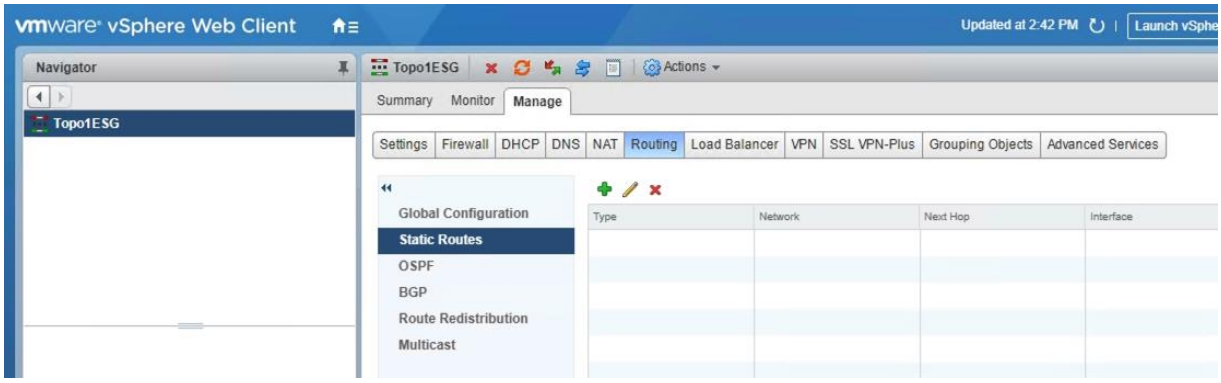
This configuration is also required to ensure that traffic coming from the external networks finds its way in.

5. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then Double-click on the NSX Edge you configured in the first section. (in our use case this was named Topo3-ESG)

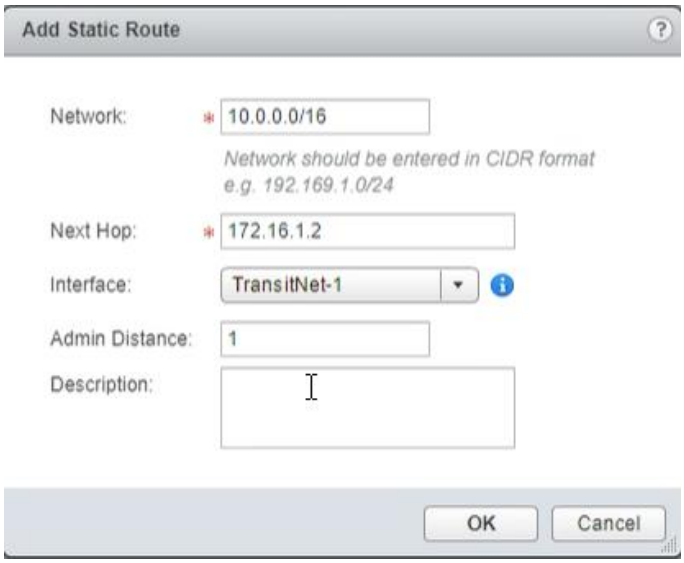
   Currently this must be done in the vSphere Web Client (FLEX) [Flash Based] as the functionality hasn’t been ported to the HTML5 Client.



6. In the NSX Edge select the Manage Tab and the Routing sub-tab, then select Static Routes from the menus. Click on the (+) plus symbol to add a Static Route.



7. Provide an internal summary route that points the NSX Edge to the TransitNet-1 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 172.16.1.2. Click OK.



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

BIG-IP Configuration

The validation of this topology is currently configured on a single device. The base network configuration consists of configuring the Management Interface (VLAN) and the Logical Switches (VXLAN) and assigning them to interfaces 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.

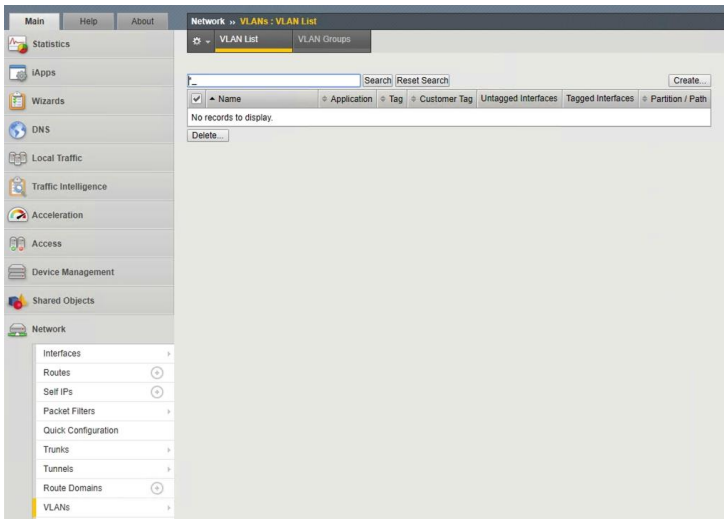
Prerequisites

- The BIG-IP 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 Interfaces 1.1 and 1.2 are connected and configured to the Logical Switches for AppTier and WebTier.

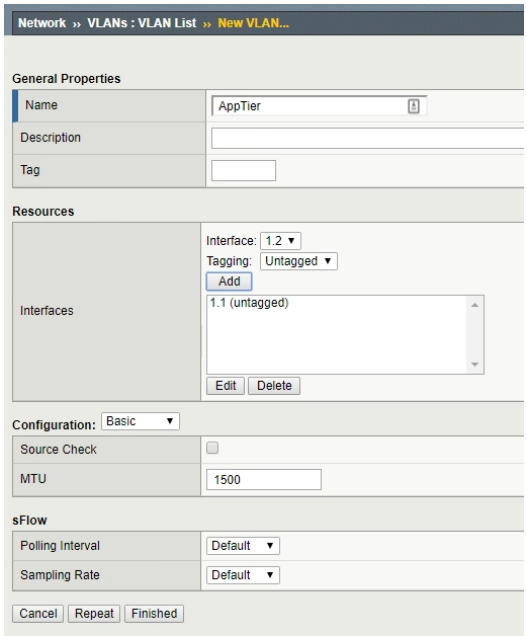
  For info on how to perform these installation and basic setup steps, refer to http://support.f5.com and consult the appropriate implementation guide for your version and device.

Create VLANs

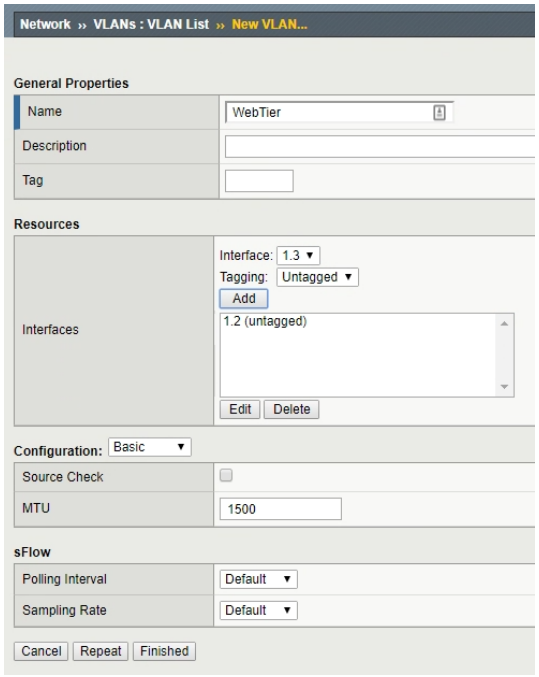
1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select VLANs.
2. In the upper right corner, click Create.



5. In the New VLAN menus.
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used AppTier.
   b. Under Resources, for Interface, select 1.1 (or use interface that is connected to the App Network 10.0.2.x)
   c. Select Untagged and then click the Add button below it.
   d. Select Repeat to proceed with the creating of the WebTier network VLAN



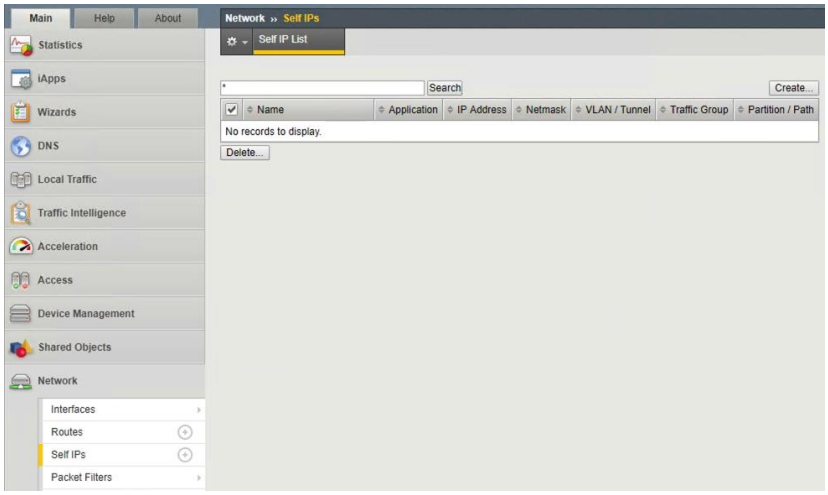
6. In the New VLAN Menus
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used WebTier.
   b. Under Resources, select the Interface 1.2 (or use interface that is connected to the App Network 10.0.1.x)
   c. Select Tagged and click the Add button below it.
   d. Select Finished to complete the VLAN creation.



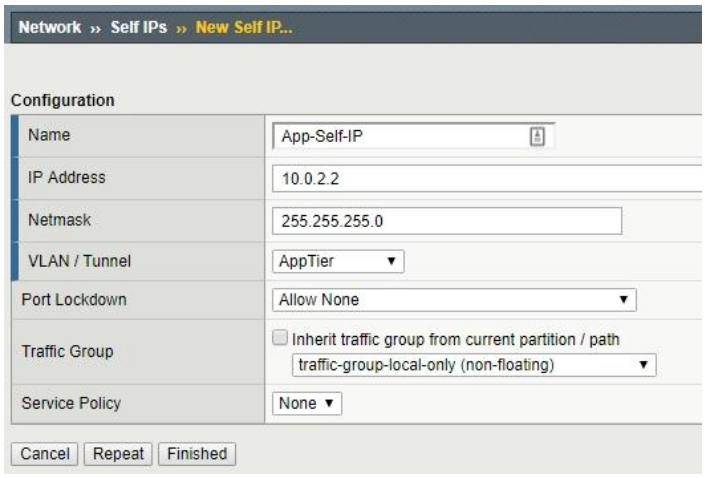
Configure Self IP Addresses

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.

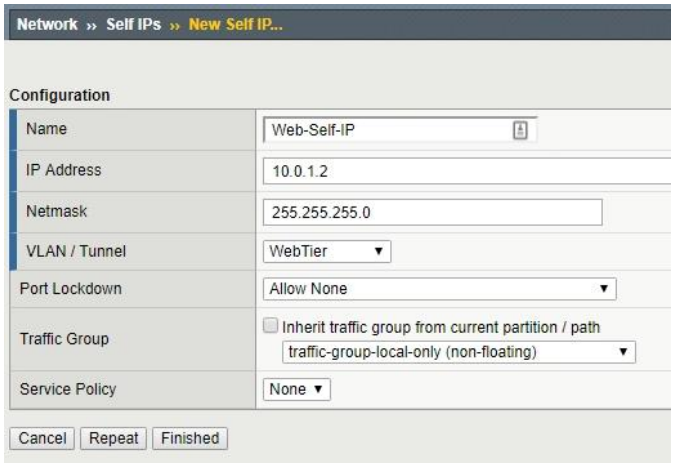
1. On the Main tab of the BIG-IP navigation pane, click Network and then click Self IPs.
2. In the upper right corner of the screen, click the Create button.

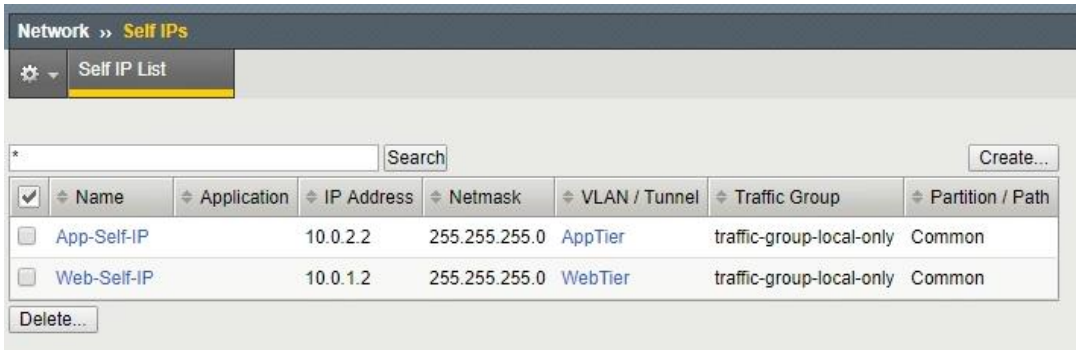


3. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “App-Self-IP” (without double quotes).
    b. In the IP address box, provide the IP address for the AppTier network, in our example, we used 10.0.2.2
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select AppTier from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Repeat button to continue



4. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “Web-Self-IP” (without double quotes).
    b. In the IP address box, provide the IP address for the External network, in our example, we used 10.0.1.2
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select WebTier from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Finished to validate the completed self IP configurations.



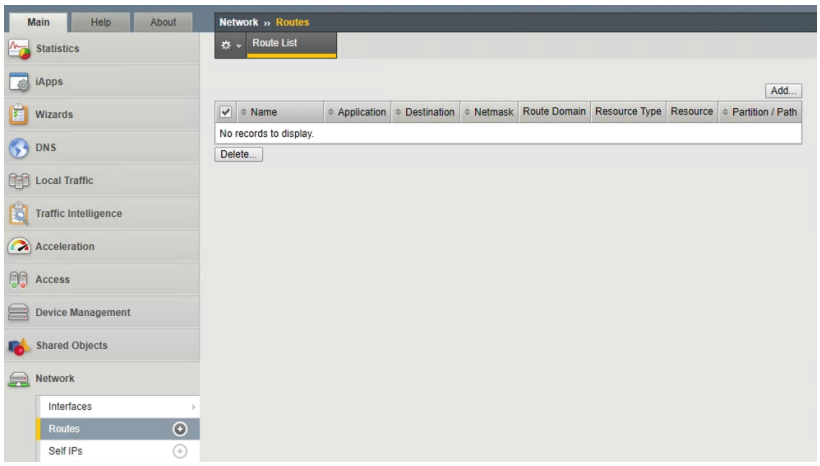


Configure Static Routes

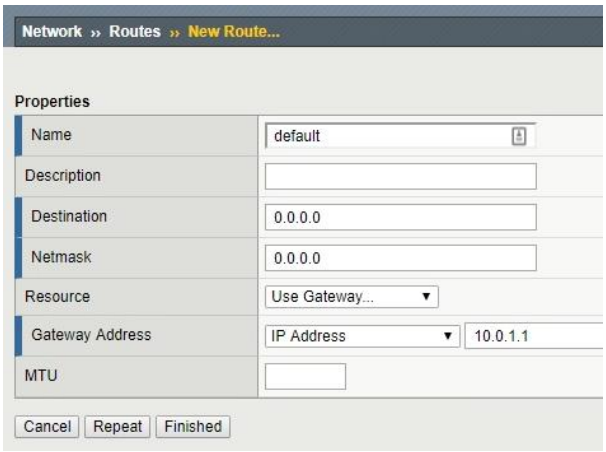
To ensure the BIG-IP can properly forward requests to the application servers within the overlay network.

From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select Routes.

1. In the upper right corner of the screen, click the Ad button.



2. In the New Route menus
   a. For the Name, use the keyword default.
   b. The default route for both Destination and Netmask is 0.0.0.0.
   c. The Gateway Address is the WebTier Gateway Address which is 10.0.1.1
   d. Click Finished to complete static route creation



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.

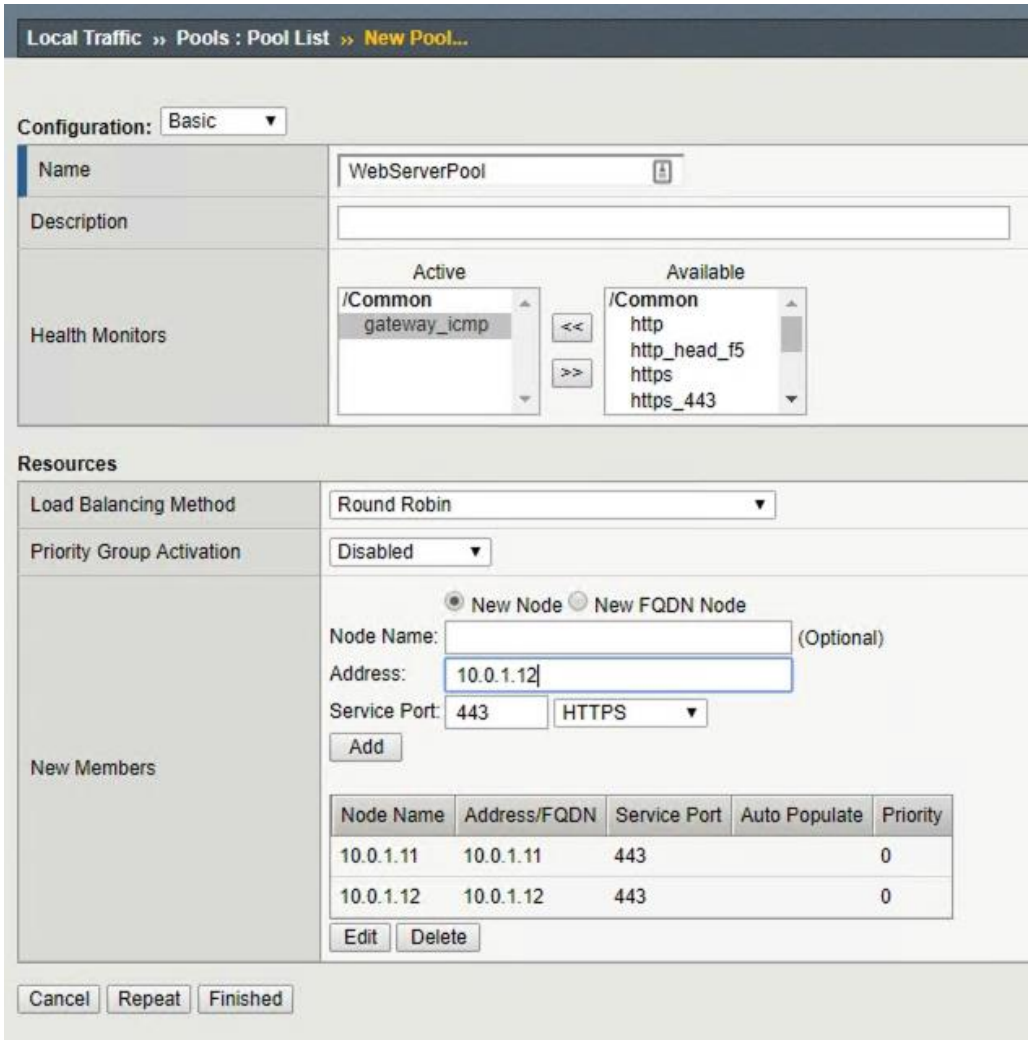
Create Application Pools

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 New Pool menus
    a. In the Name field, type a unique name for the web pool. For this validation, we used WebServerPool.
    b. 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.
    c. Under Resources, select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
    d. Under Resources, use the New Members setting to add the IP address and port of the web servers (refer to Table 15 below). Click the Add button for each pool member.
    e. Click Repeat to continue and enter the application tier information,

Name (Optional)	Address	Service Port
web-01	10.0.1.11	443 (HTTPS)
web-02	10.0.1.12	443 (HTTPS)

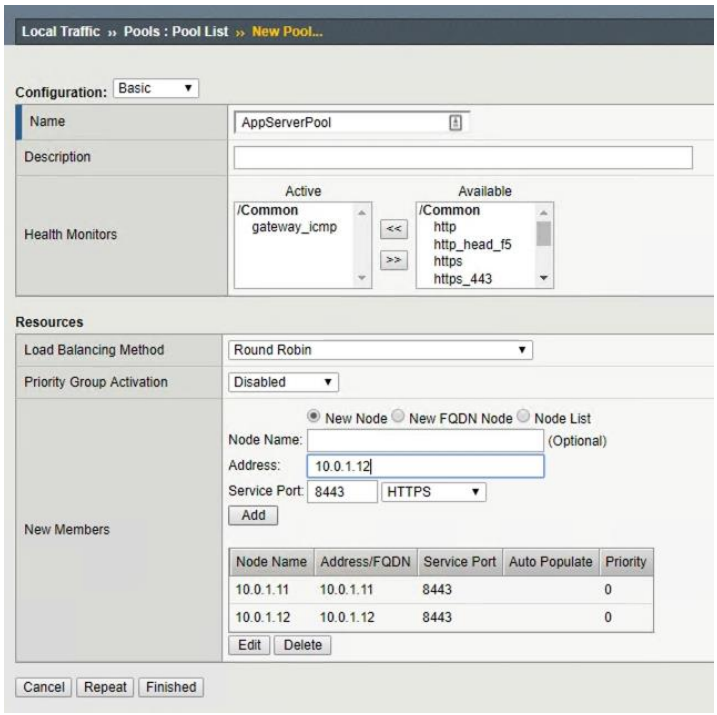
Table 15 BIG-IP web tier pool members


Local Traffic ›› Pools : Pool List ›› New Pool...
Configuration: Basic
Name
WebServerPool
Description
Health Monitors
Active
/Common
gateway_icmp
<<
>>
Available
/Common
http
http_head_f5
https
https_443
Resources
Load Balancing Method
Round Robin
Priority Group Activation
Disabled
New Members
New Node
New FQDN Node
Node Name:
(Optional)
Address:
10.0.1.12
Service Port:
443
HTTPS
Add
Node Name
Address/FQDN
Service Port
Auto Populate
Priority
10.0.1.11
10.0.1.11
443
0
10.0.1.12
10.0.1.12
443
0
Edit
Delete
Cancel
Repeat
Finished

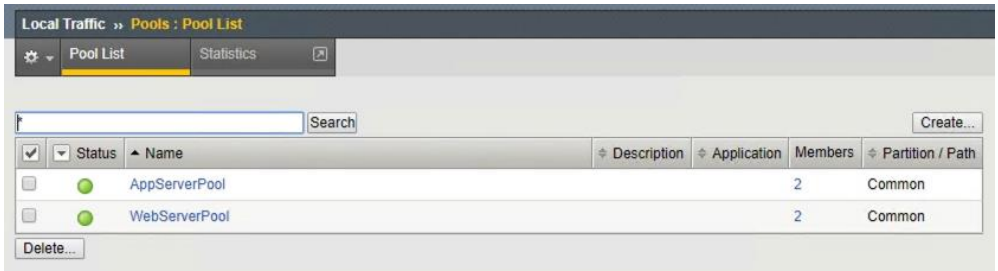
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
   a. In the Name field, type a unique name for the app pool. For this validation AppServerPool was used.
   b. In the Health Monitors section select an appropriate monitor for your application. 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.
   c. In the Resources section of the screen select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
   d. 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 16). Select the Add button for each pool member.
   e. Click Finished to complete the pool creation.

Name (Optional)	Address	Service Port
app-01	10.0.2.11	8443
app-02	10.0.2.12	8443

Table 16 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.

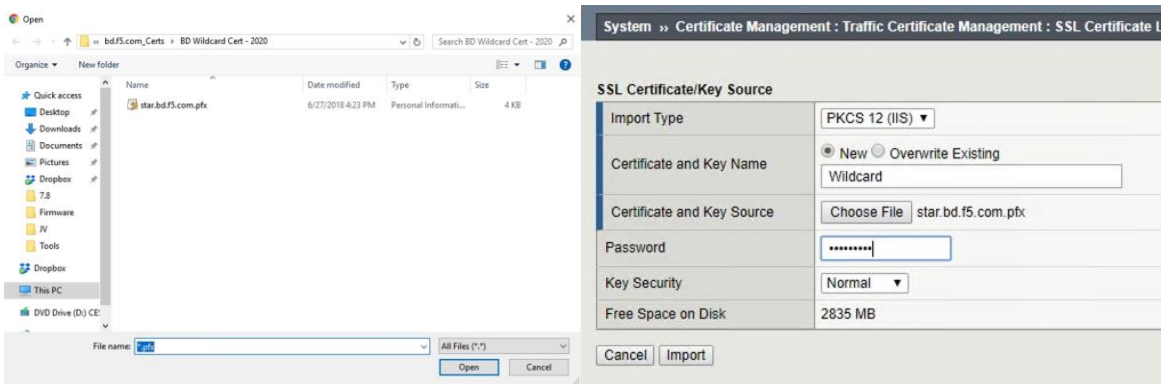


Import SSL Certificate

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

As a prerequisite to completing this task you must have a Certificate with a Private Key (Exportable) available to install this could be in Certificate/Key format or PKCS12 (PFX) format. In our test case we will be using a public PKCS12 certificate (PFX) wildcard certificate "*.bd.f5.com" that will allow any DNS name in front of bd.f5.com will be an accepted as valid name in a web browser.

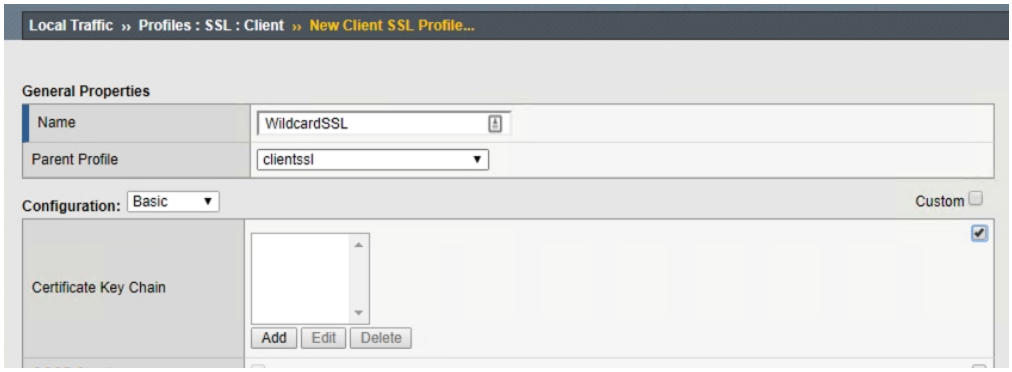
4. On the Main tab, select System → Traffic Certificate Management → SSL Certificate List
5. In the upper right corner of the screen, click the Import button.
6. In the Import SSL Certificate and Keys menus
    a. In the Import Type field, in our example we select "PKCS 12 (IIS)"
    b. In the Certificate and Key Name field, in our example we entered "Wildcard" without quotes
    c. In the Certificate and Key Source field, select the "Choose File" button
    d. In the pop out menus browse and select the file, in our example star.bd.f5.com.pfx
    e. In the password field, enter the password to decrypt the pfx file.
    f. Click the Import button

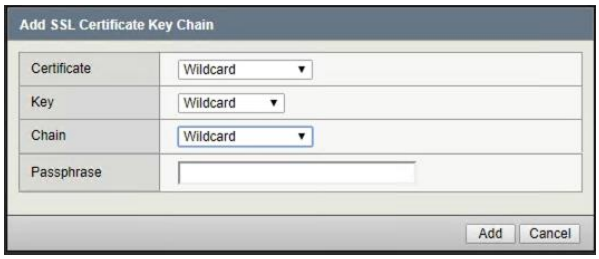


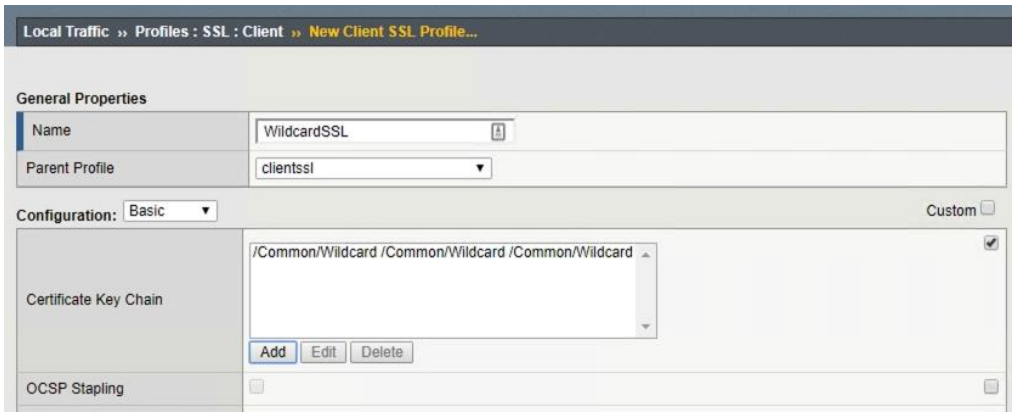
Create ClientSSL Profile

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

4. On the Main tab, select Local Traffic → Profiles → SSL → Client
5. In the upper right corner of the screen, click the Create button.
6. In the New Client SSL Profile menus
    a. In the Name field, type a unique name for the profile, for this validation WildcardSSL was used.
    b. In the Certificate Key Chain field, check the custom box and click the Add button
    c. In the Certificate, Key and Chain pulldown menus, select the previously imported Certificate chain, in this validation it was named Wildcard. Then click the Add button.
    d. Once added, scroll to the bottom and click the finished button.



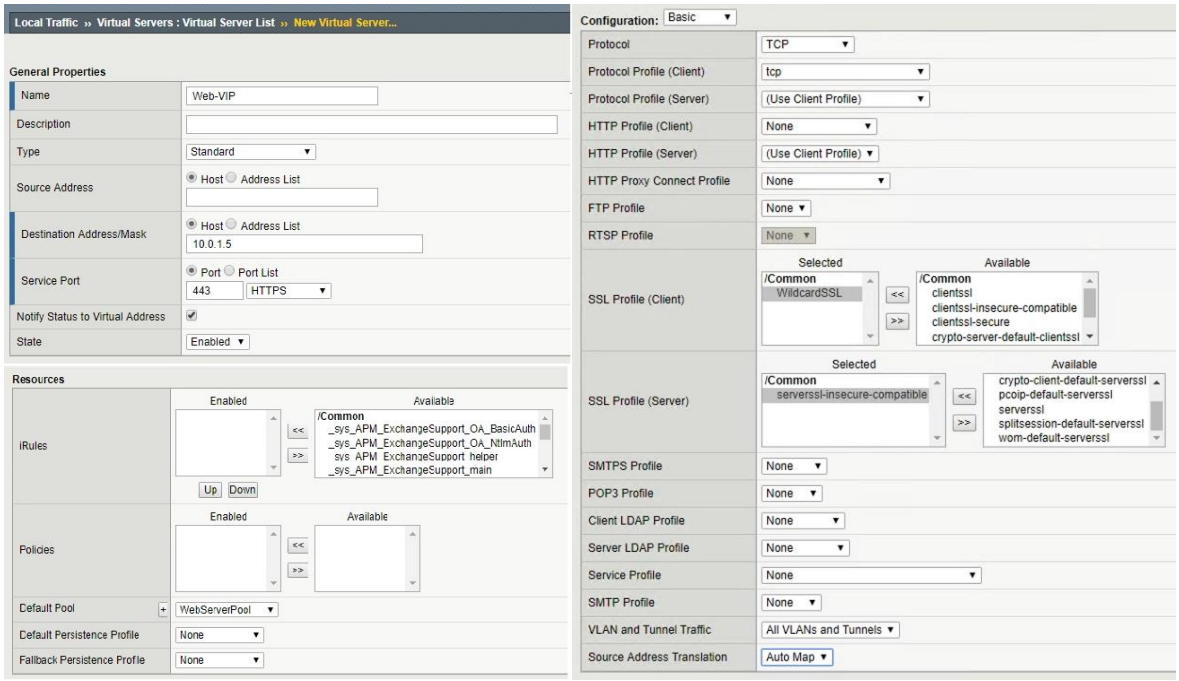




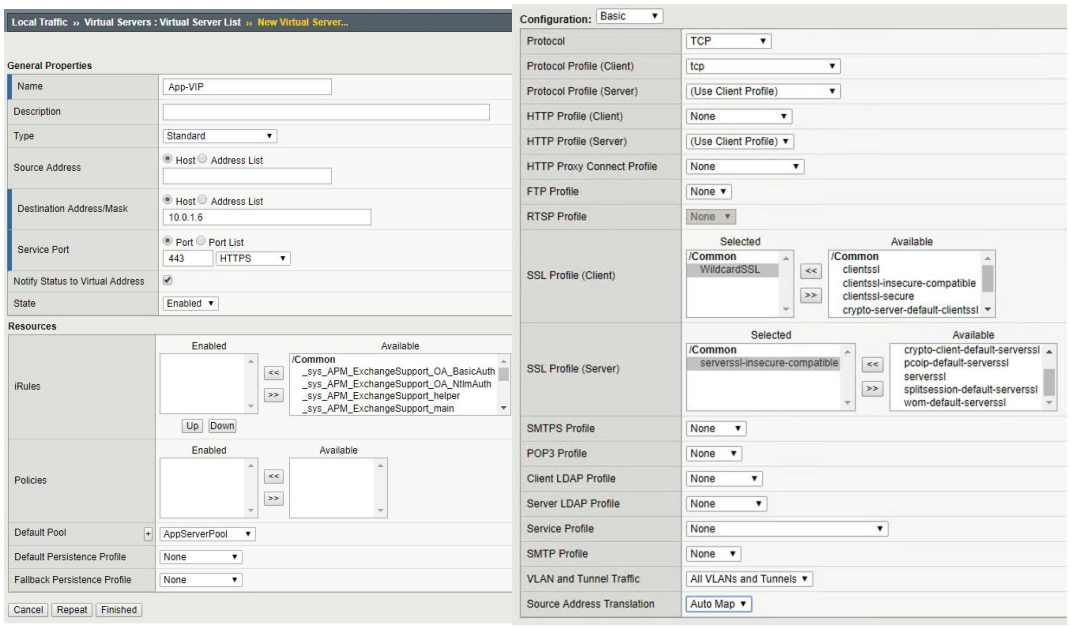
Create Application Virtual Servers

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 in the WebTier network on the 10.0.1.0/24 segment and accessed via NAT from 10.105.176.2, and the other for the AppTier on the same WebTier Network only accessible for the WebTier Network (10.0.1.0/24).

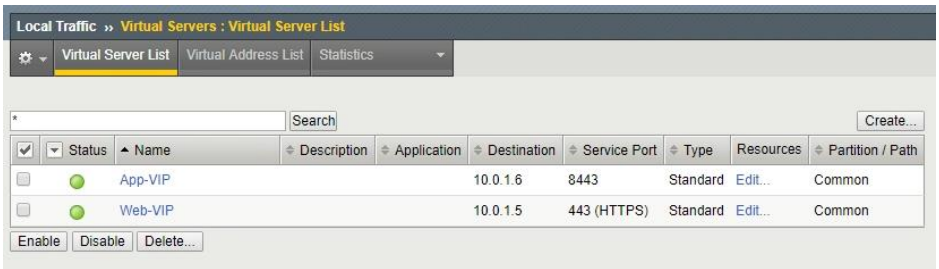
1. On the Main tab, select Local Traffic and then click Virtual Servers. The Virtual Server List screen is displayed.
2. In the upper right corner of the screen, click the Create button.
3. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the web application. In this case, we used Web-VIP.
    b. In the Destination Address field, enter 10.0.1.5
    c. For Service Port use the standard HTTPS port 443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the WebServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Repeat to continue to configure the application tier virtual server



4. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the app application. In this case, we used App-VIP.
    b. In the Destination Address field, enter 10.0.1.6
    c. For Service Port use the standard HTTPS port 8443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the AppServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Finished to continue to configure the application tier virtual server



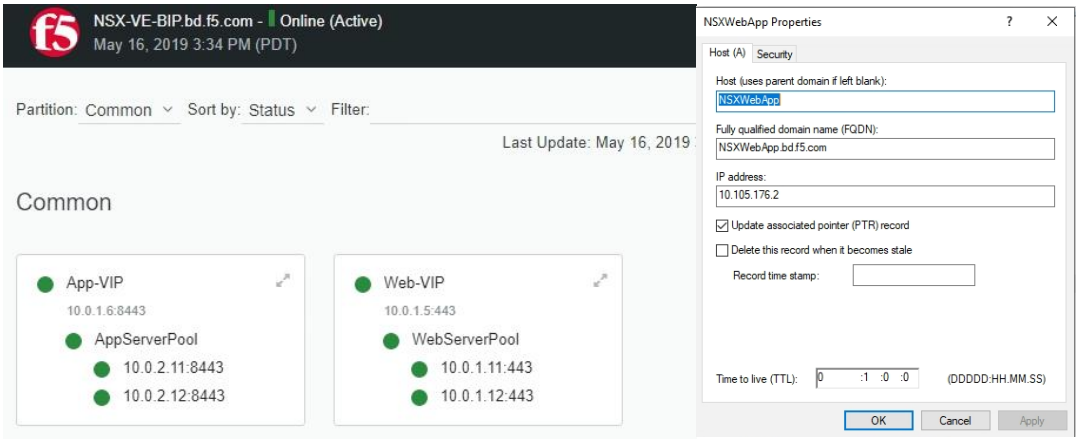
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.



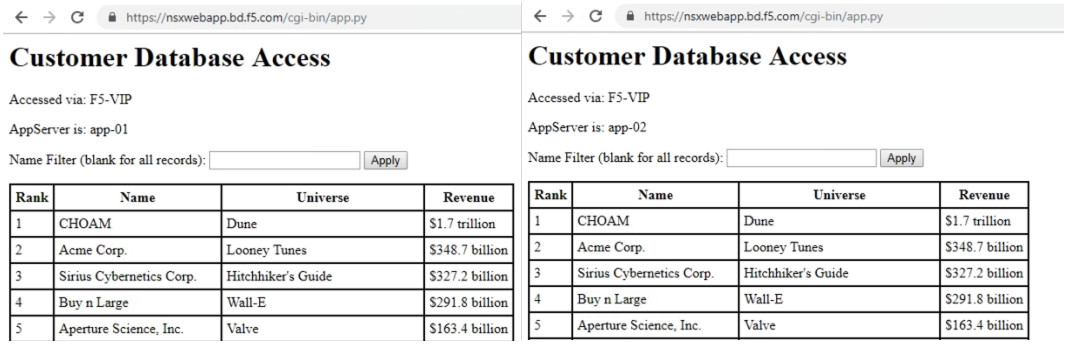
Validation

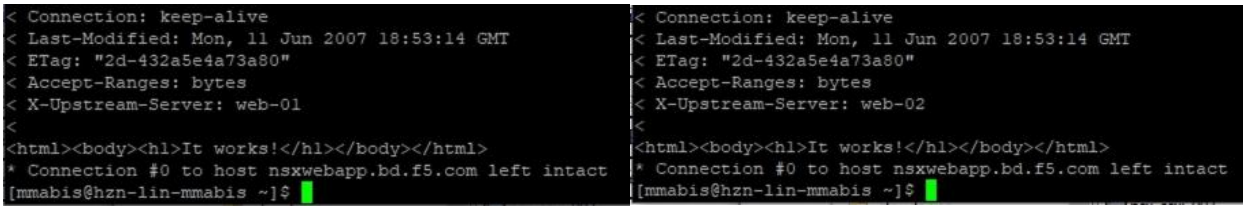
The web tier virtual server should now be available and accepting application traffic on port 443 (HTTPS).

On the Main tab, expand Local Traffic and then click Network Map to display the overall health of the applications and their associated resources. Due to also this traffic being HTTPS rather than HTTP we setup a FQDN of NSXWebApp.bd.f5.com to allow our wildcard certificate to be validated when connecting to the site.



Any web browser can be used to test by typing https://NSXWebApp.bd.f5.com/cgi-bin/app.py to send a request to the virtual server. Our 3-tier application will appear and show data within the database validating that the connection works, to further validate which application server you can refresh the page and see the AppServer changes. To further validate which Web server is being used we run a curl command “curl -kv “https://nsxwebapp.bd.f5.com” in the web server we injected a header in the web server configuration (not shown in this guide) called X-Upstream-Server to show which web server was being accessed.





This concludes the validation of the *One-Arm Connected using VXLAN Overlays with BIG-IP Virtual Edition*.

Topology 4: OVSDB Integration with NSX-V

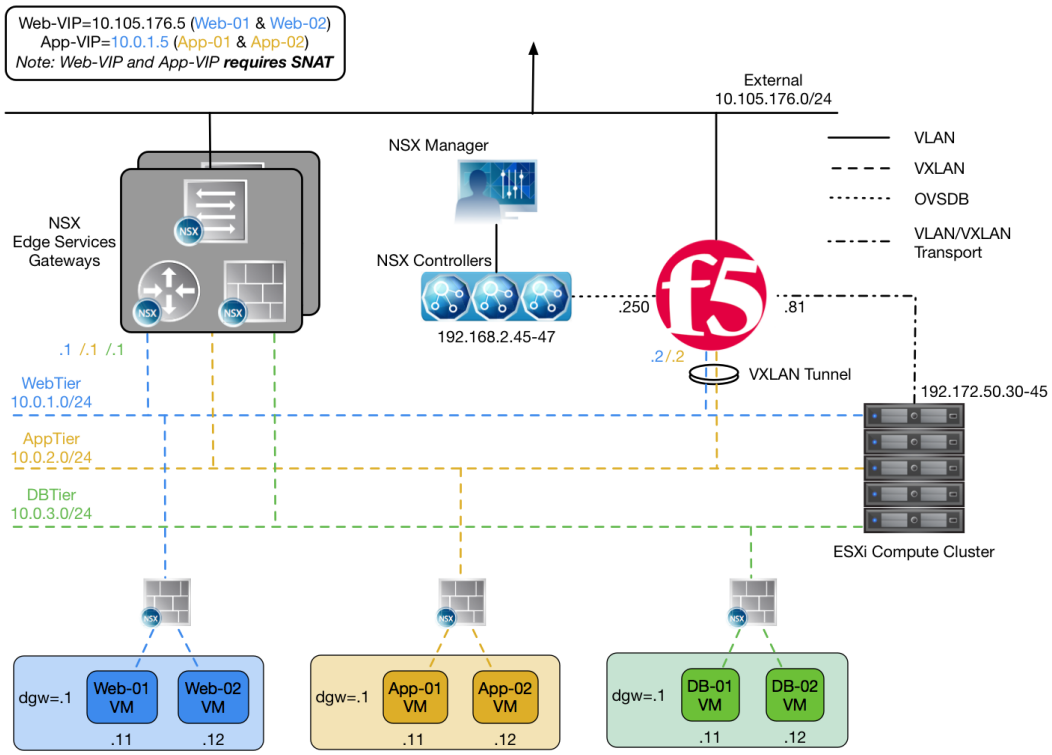


Figure 14 OVSDB Integration with NSX-V

The fourth deployment scenario utilizes a topology with a second data path for application delivery traffic. BIG-IP's are arranged logically parallel to the Edge Services Gateway (ESG). This deployment method is not compatible with a Distributed Logical Router (DLR) as logical switches cannot be mapped to both DLR and hardware interfaces.

The BIG-IP has 802.1Q tagged interfaces for external traffic, OVSDB connectivity via NSX controllers, and VTEP communications between endpoints. Once the OVSDB is configured on BIG-IP and vSphere, VXLAN tunnels will be automatically created by vSphere when mapping logical switches to hardware devices (BIG-IP). From there a Self IP can be created for that tunnel and communication to the underlay devices within NSX-V is now accessible via the BIG-IP.

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.

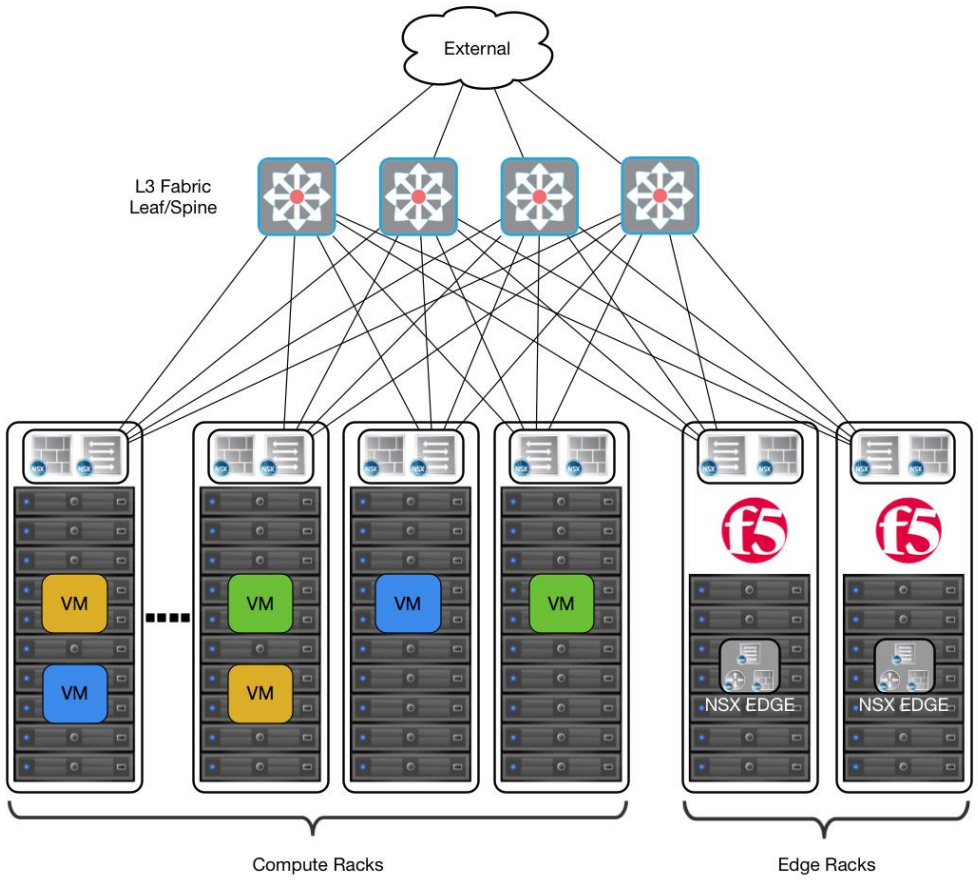


Figure 15 Leaf/spine physical rack infrastructure

The topology in this deployment scenario isolates infrastructure vs compute racks however in this case the Logical Routing services aren't being used. The placement of the BIG-IP appliances (physical or virtual) provides an optimal layer 2 path for application traffic.

Important Notes:

- **BIG-IP Version 13.1 or higher required**
- **When using a F5 Virtual Appliance, the VE cannot be placed in a cluster managed by NSX-V. The traffic will not pass from the VE to Controllers correctly.**
- **The OVSDB connectivity requires the use of a NSX Edge and not a DLR, Logical Switches cannot be mapped to both DLR and Hardware at the same time. This is an NSX-V Limitation.**
- **When mapping logical switches to the BIG-IP, a VLAN must be specified when connecting to the Local0, Local1, Local2, and Local3 interfaces. These VLANs have no effect on connectivity. This is a limitation based on VMware assumptions that traffic wouldn't be terminated.**

Traffic Flows

North-South Traffic - Logical Traffic Flows as Follows

1. From Client (External) to BIG-IP WebTier VIP (Web-VIP)
2. From BIG-IP Appliance to WebTier Servers
3. From WebTier to BIG-IP AppTier VIP (App-VIP)
4. From BIG-IP Appliance to AppTier Servers
5. From AppTier Servers to NSX Edge to DB-Tier Servers

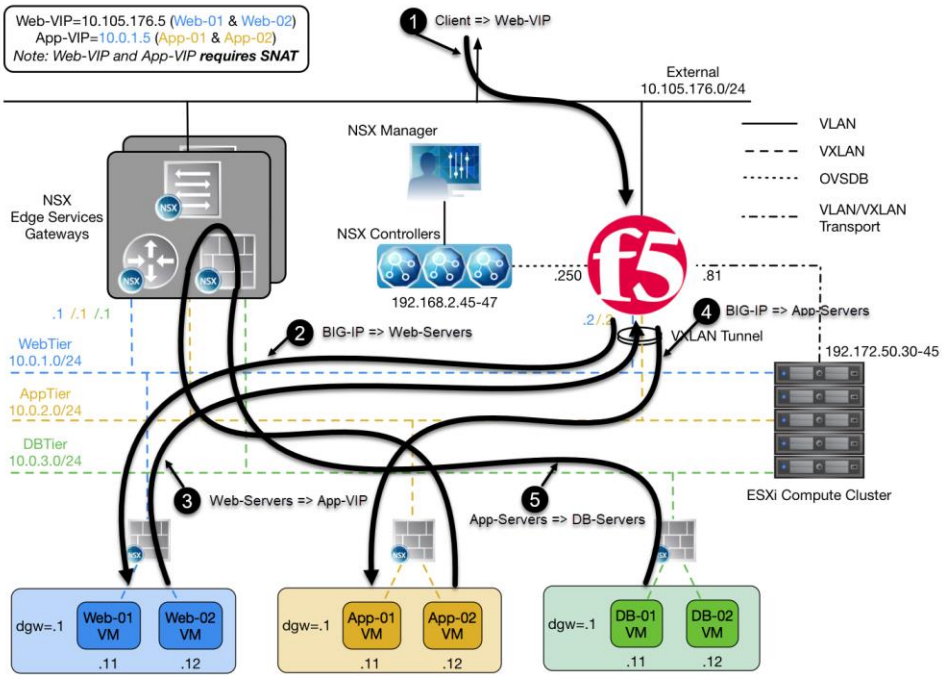


Figure 16 North-South Logical Traffic Flow "OVSDB Integration with NSX-T" with BIG-IP Appliance

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 17: the Cluster1-VDC (Edge Rack) and Cluster3-Compute-NSX (Compute Rack). 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 15.

Figure 17 vSphere Console

In accordance with best practices, edge and compute ESXi hosts are physically and logically separated from one another. BIG-IP's are installed in dedicated edge racks, along with vCenter, NSX manager, and the NSX Edge Services Gateways, which also will be installed in the edge racks.

The virtual machines used as Web (Web), Application (App), and Database (DB) servers will be running on ESXi hosts in the compute cluster.

Prerequisites

Referencing the diagram in Figure 14, the BIG-IP requires connectivity to at minimum two of its 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.

- BIG-IP Version 13.1 and above is required.
- The BIG-IP will need to be installed and connected (physically or virtually) to the edge rack which is connected to the distribution switches. Each BIG-IP management interface will need to be connected and configured with an IP address in the management segment.
- The BIG-IP interface 1.1 will need to be connected to a switch port either in ESXi (trunked port group) or on the edge rack top-of-rack switch that 802.1Q tags the VLANs used in this environment. VLANs 102, 176 and 50 are used in this example.
- Physical network infrastructure switches connected to the ESXi servers and BIG-IP appliances (if not virtual) are configured to support 802.1Q tagging and allow the appropriate VLANs.
- Ensure that the Physical or Virtual BIG-IP is configured for NTP and DNS to ensure time sync with NSX Controllers.
- ESXi hosts will need to be configured with the appropriate distributed port groups and virtual switches.

Name	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176-External	176
NSX-CTRL	DVS-VLAN-102	102
VTEP	DVS-VLAN-50	50

Table 17 VLAN tags for configuration on distributed virtual switch and physical switches

Name	Transport Zone	Segment ID	Control Plane Mode
AppTier	TransportZone1	5002	Unicast or Hybrid
DBTier	TransportZone1	5003	Unicast or Hybrid
WebTier	TransportZone1	5001	Unicast or Hybrid

Table 18 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 50 (VTEP/Transport)** is for management connectivity. The 192.172.50.0/24 IP subnet range is configured on this VLAN.
- **VLAN 102 (NSX Controller Network)** is the VLAN used to communicate. The 192.168.2.0/16 IP subnet range is configured on this VLAN.
- **VLAN 176 (External)** is the VLAN used for external connectivity. The 10.105.176.0/24 IP subnet range is configured on this VLAN.

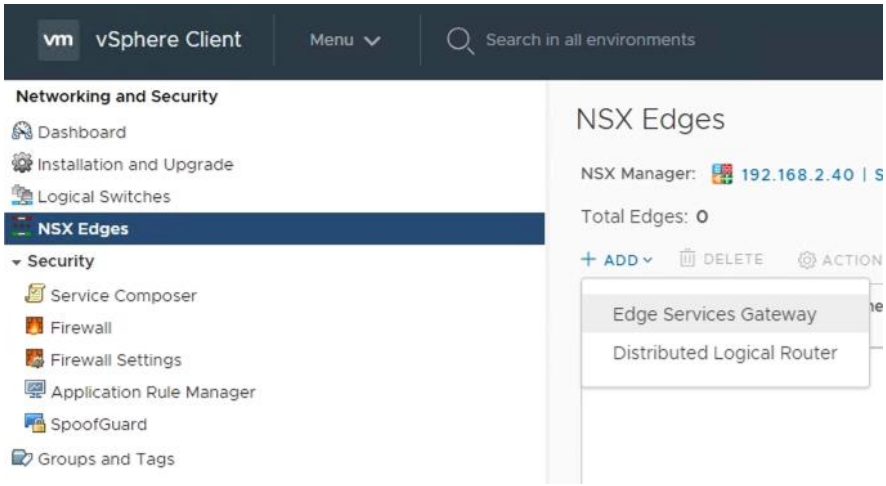
VXLAN Segments

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

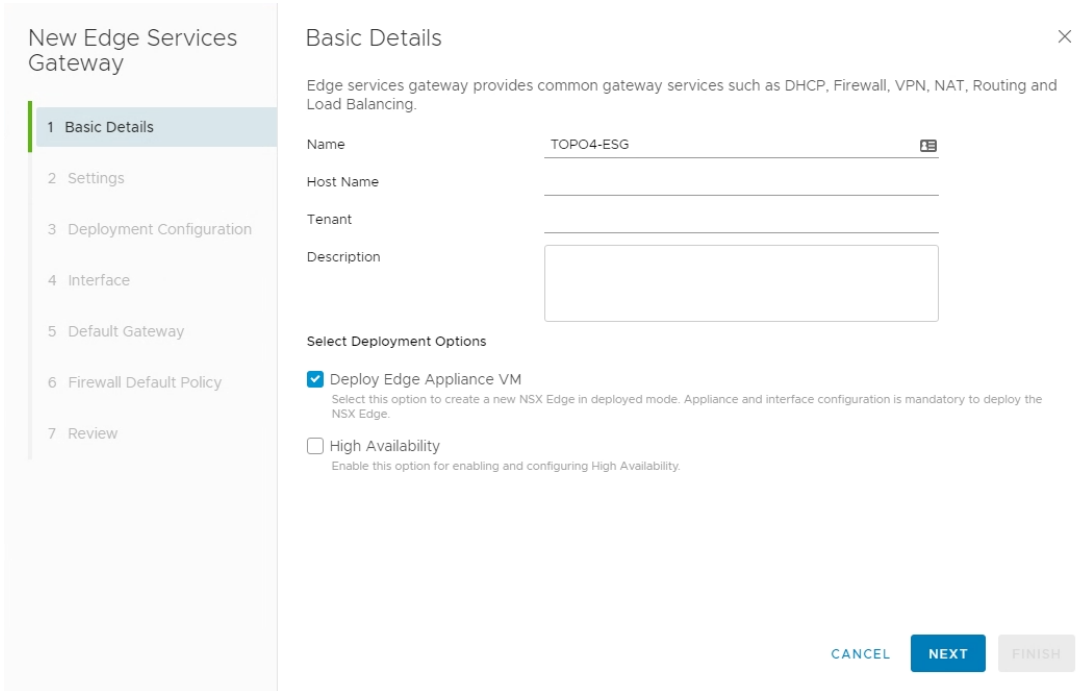
- VXLAN 5001 WebTier is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5002 AppTier is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- VXLAN 5003 DBTier is the segment ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VXLAN.

NSX Edge Configuration

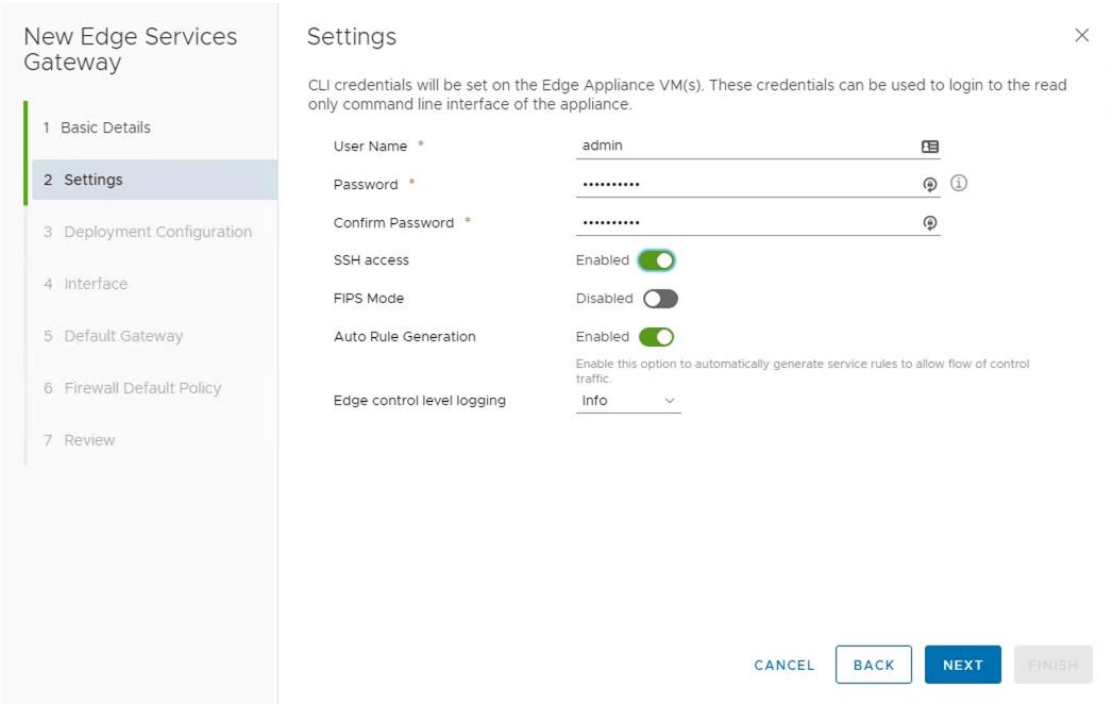
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then click (+ Add) hyperlink → Click on “Edge Services Gateway”



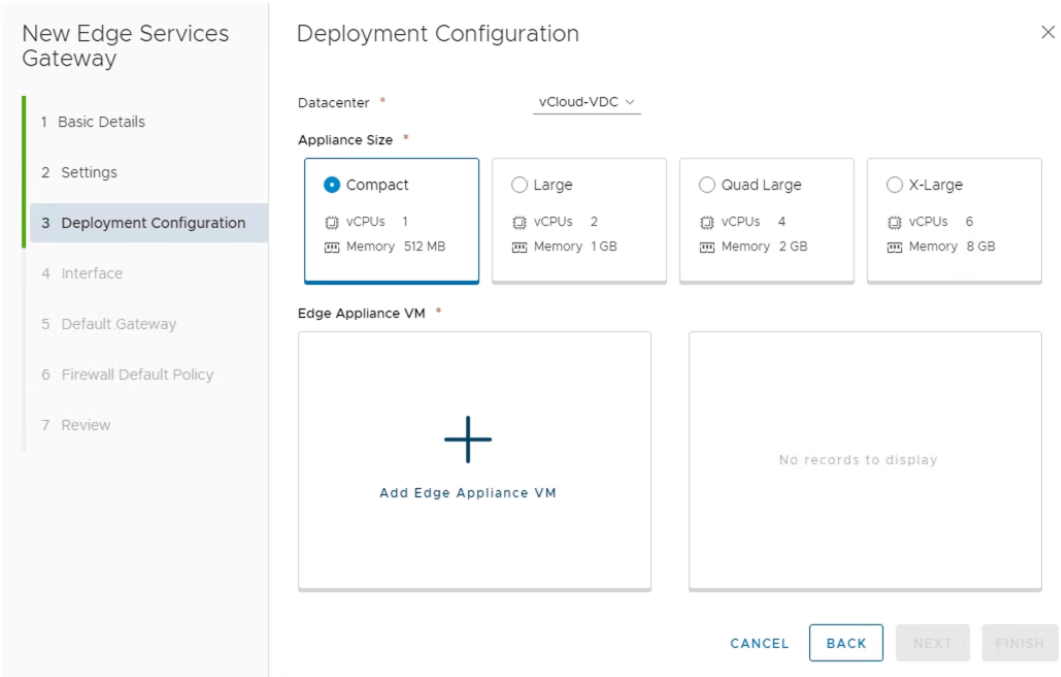
2. Provide a name for the device, then click Next.



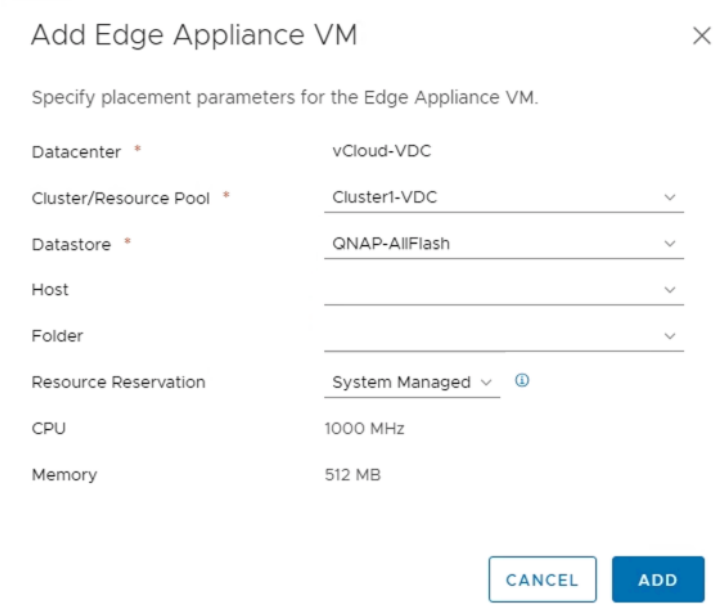
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.



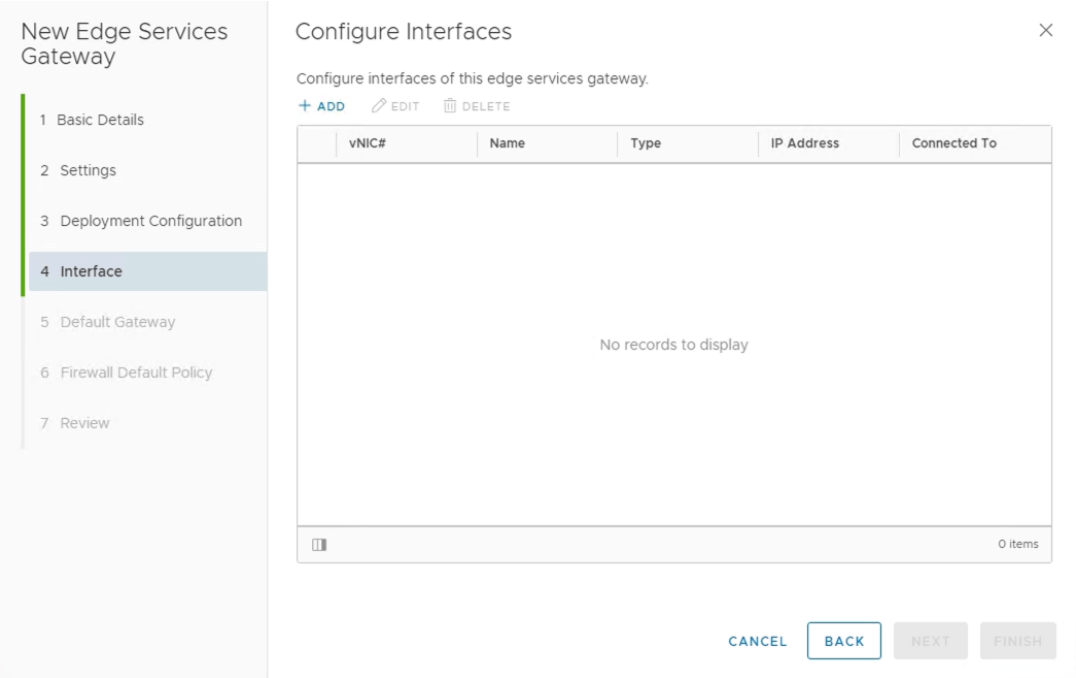
4. Under Configure deployment, select the Datacenter and Appliance Size appropriate for your deployment. Then click on the plus symbol (+) to Add Edge Appliance VM.



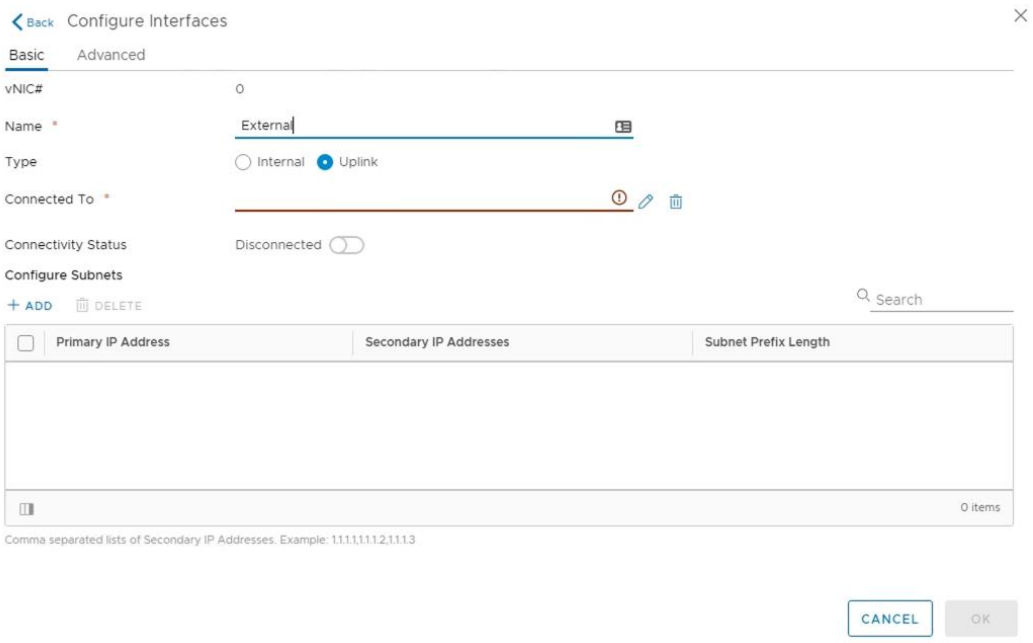
5. Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete. This will return you to the configure deployment screen shown in step 4 with the Edge Appliance VM filled out. Click **Next** to continue.



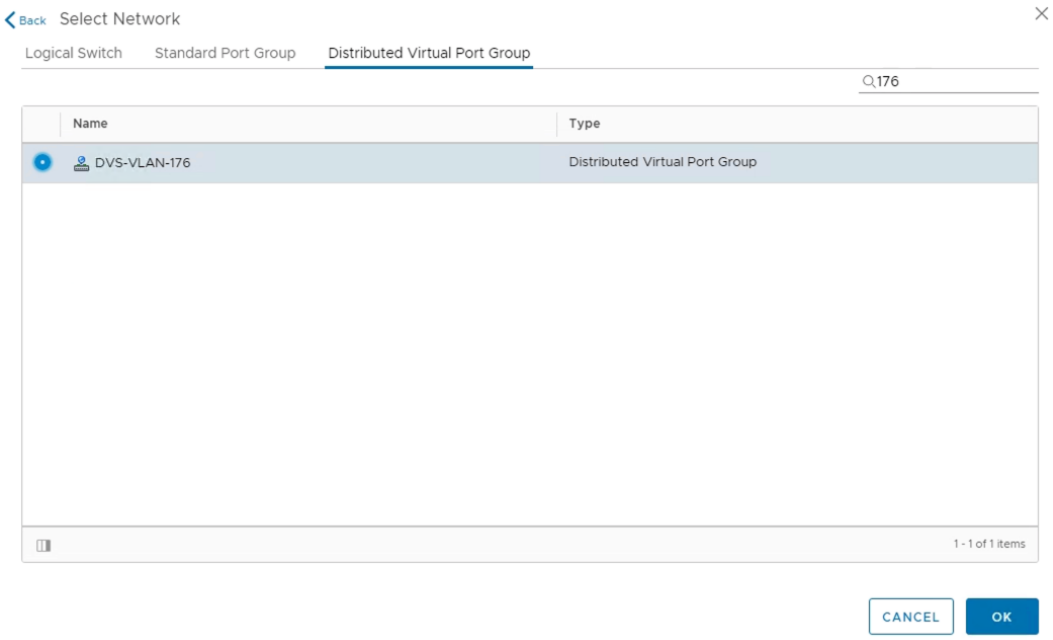
6. In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX Edge Interface dialog box.



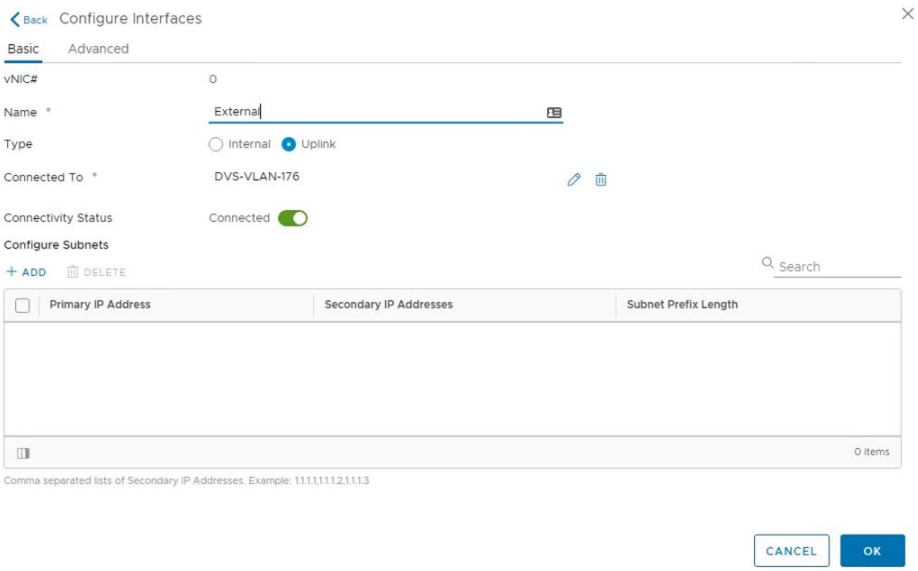
7. Provide a name and click the edit icon next to the “Connected To” field



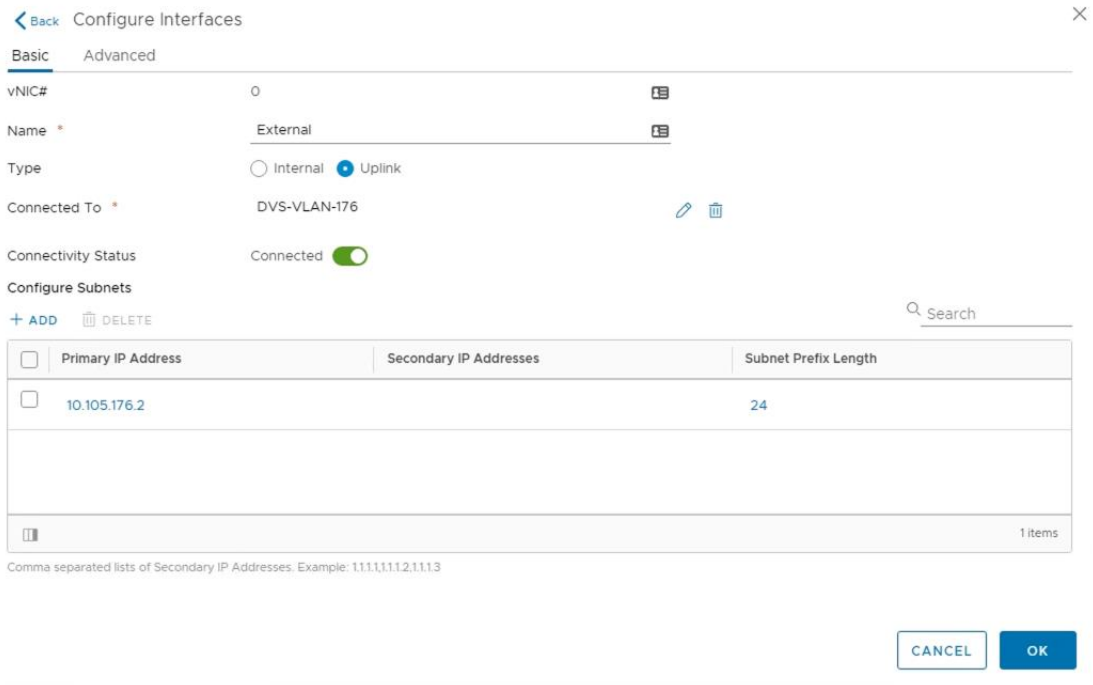
8. For the External network, click on the Distributed Virtual Port Group tab and then selecting the port group used for external access. Click OK.



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



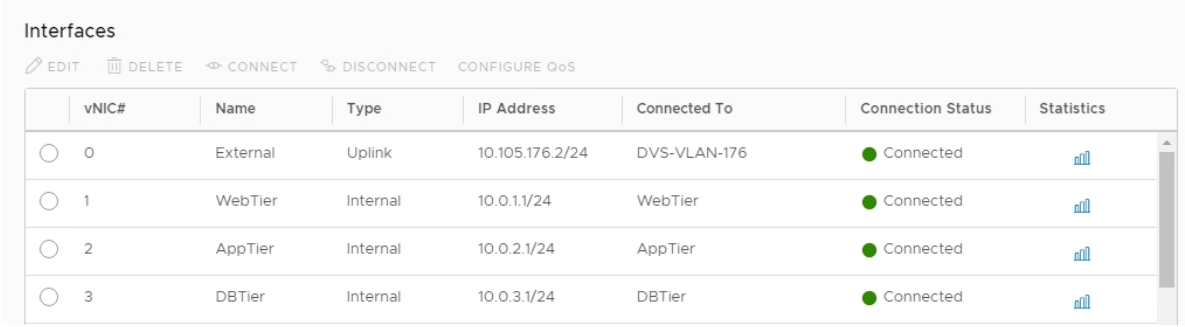
10. In the Add Subnet dialog box, enter the appropriate IP address and Subnet prefix length, and click OK.



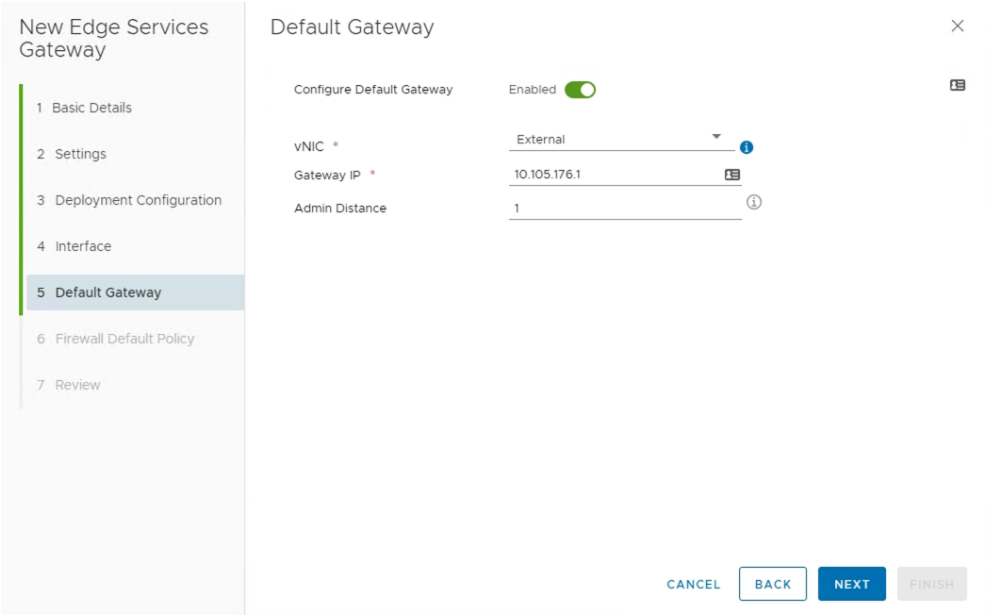
11. This will bring you back to the Configure interfaces dialog box. For each of the three interfaces required for this deployment scenario, add and configure the appropriate subnets and switch type, according to the table below and look like the final picture below with your datacenter information.

Network Name	Type	Network Type	IP Address	Connected To
External	Uplink	Distributed Virtual Port Group	10.105.176.2/24	DVS-VLAN-176
WebTier	Internal	Logical Switch	10.0.1.1/24	WebTier
AppTier	Internal	Logical Switch	10.0.2.1/24	AppTier
DBTier	Internal	Logical Switch	10.0.3.1/24	DBTier

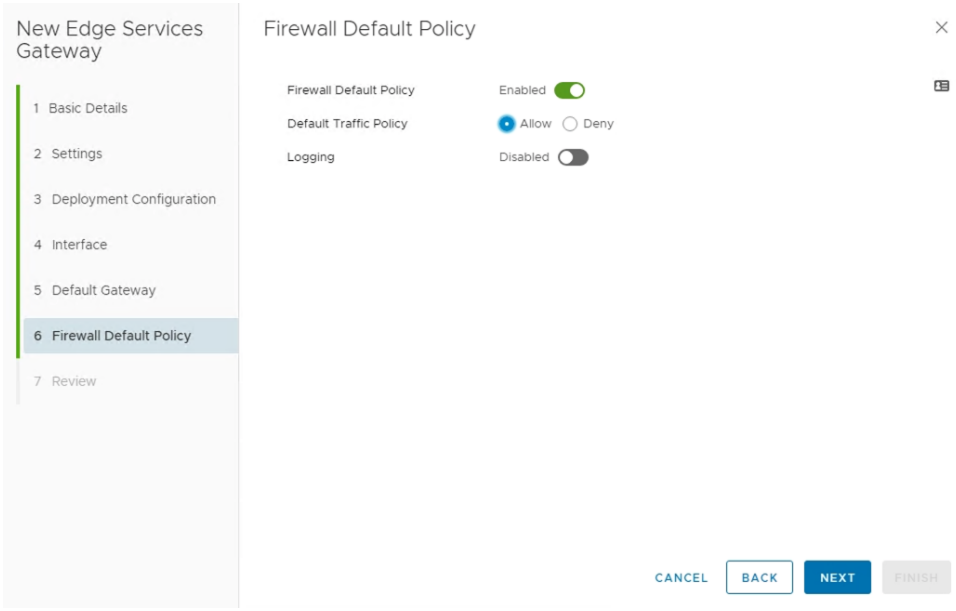
Table 19 NSX Edge network interfaces



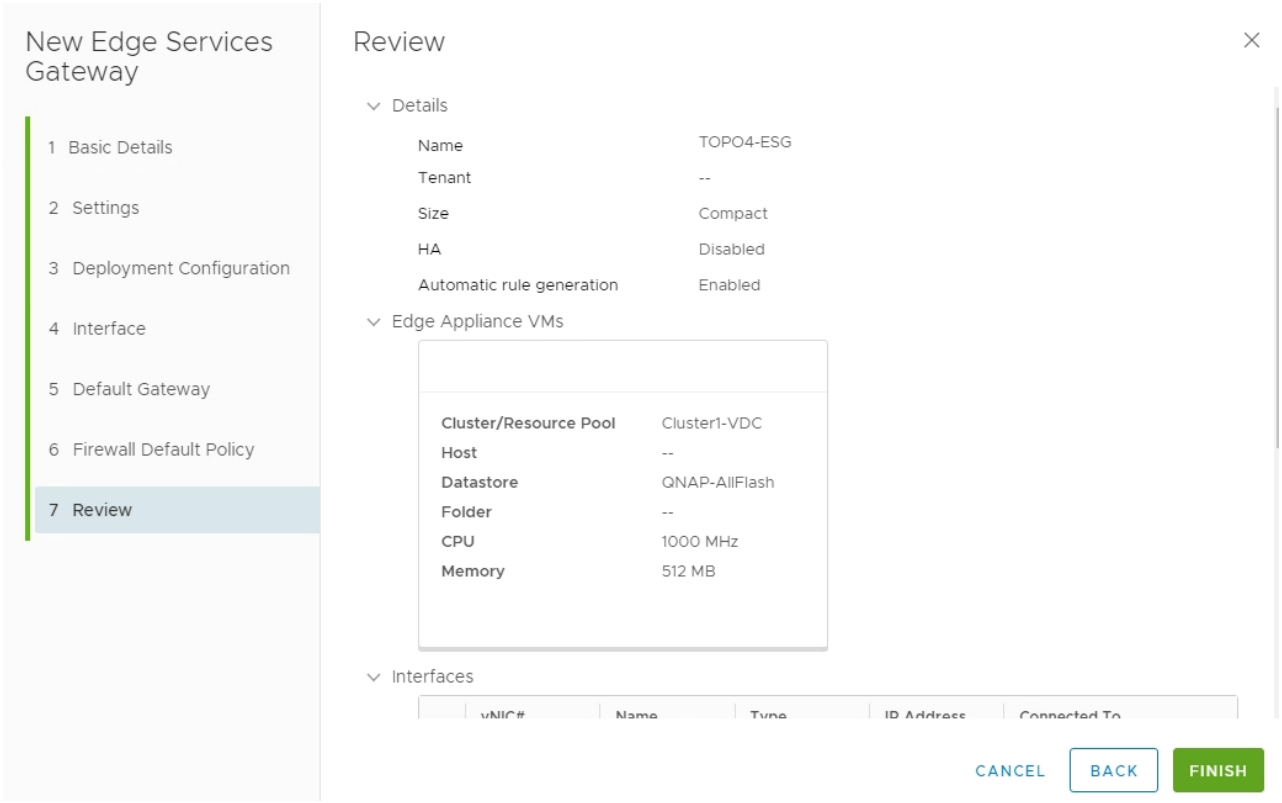
12. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway is our data center backbone router with the IP address of 10.105.176.1 on External vNIC that we configured under the interface settings. If asked use the default MTU parameter 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.



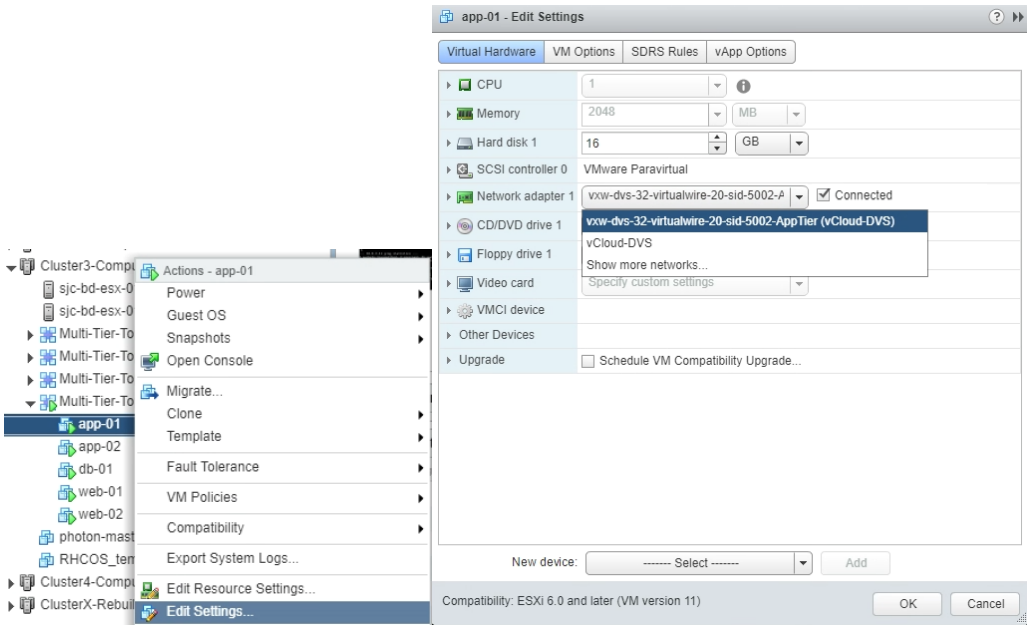
13. HA settings can be left as default. Enable the “Firewall Default Policy” and check Allow for the Default Traffic Policy. (This is for validation testing; firewall can be set to Deny instead however firewall rules will be required on ESG to allow for traffic to flow from ESG/DLR and F5)



14. Review and click Finish to complete the deployment of the NSX Edge.

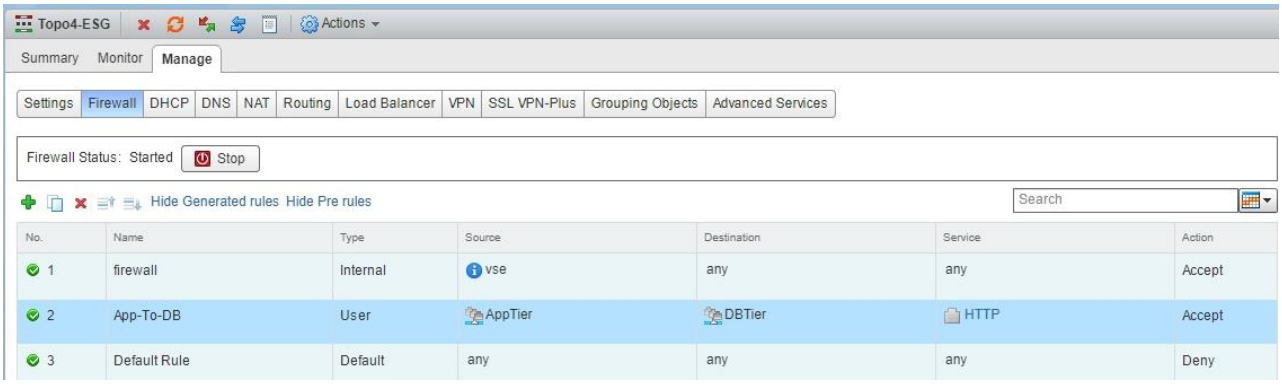


15. After the Creation of the ESG and the logical switches within vSphere, attach the Virtual Machines for each tier to their logical switches for network traffic. (This is an example of one of our AppTier VM's attached to the AppTier Logical Switch.



16. If the "Firewall Default Policy" was set to Deny traffic in earlier configuration, a firewall rule must be created to allow traffic to access the environment. (Currently can only be configured via vSphere Flex [FLASH] client) To configure firewall rules Home → Network and Security → NSX Edges → Double Click on Edge (Topo4-ESG) → Firewall Tab.

    Adding Rules Click the (+) button and add appropriate firewall rule to allow the AppTier network talk to the DBTier network over HTTP.



BIG-IP 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.

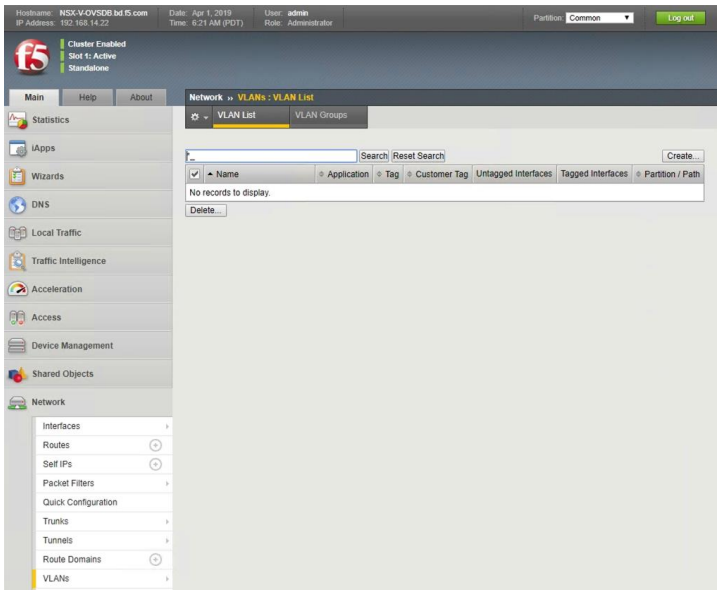
Prerequisites

- BIG-IP Version 13.1 and above.
- The BIG-IP 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 or an available interface that is connected is wired to a physical or virtual switch (trunk) configured to support 802.1Q tagging of traffic. In our specific use case this is VLANs 50, 102 and 176.

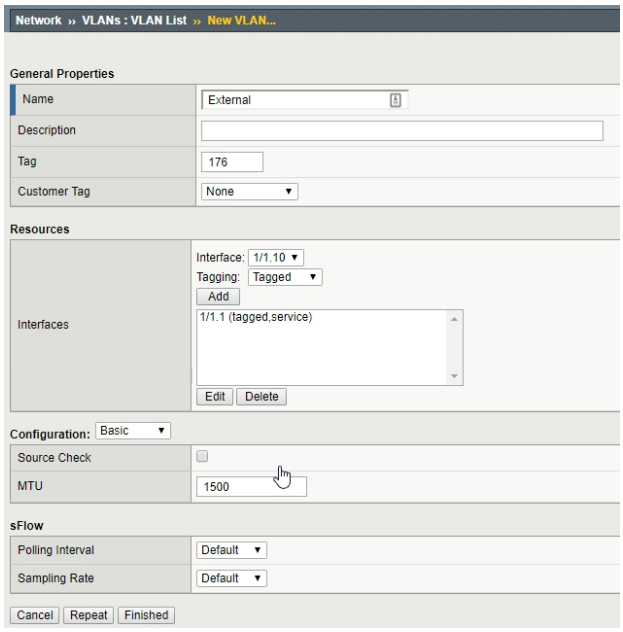
  For info on how to perform these installation and basic setup steps, refer to http://support.f5.com and consult the appropriate implementation guide for your version and device.

Create VLANs

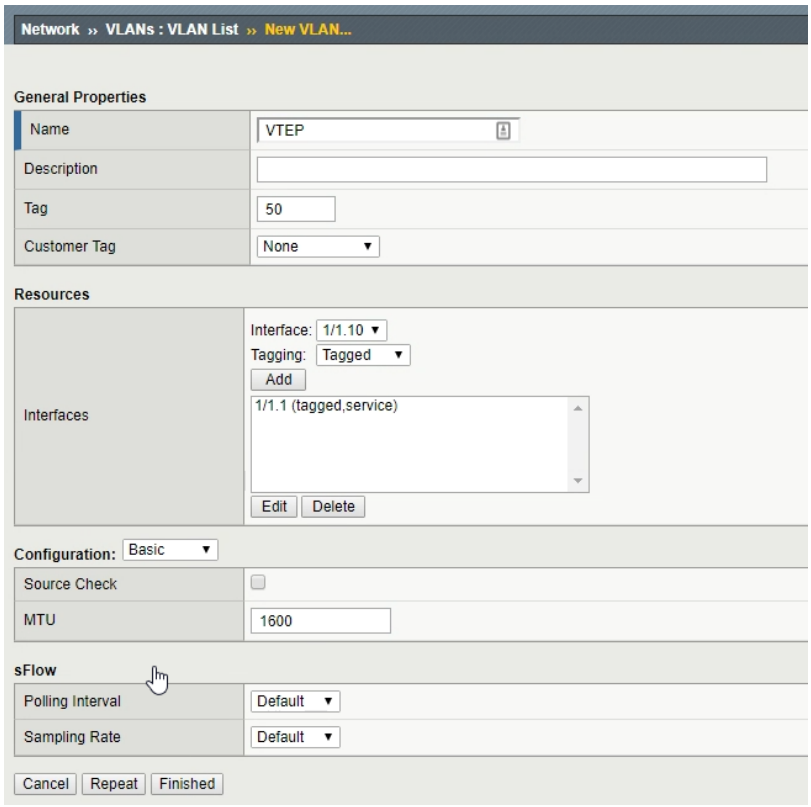
1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select VLANs.
2. In the upper right corner, click Create.



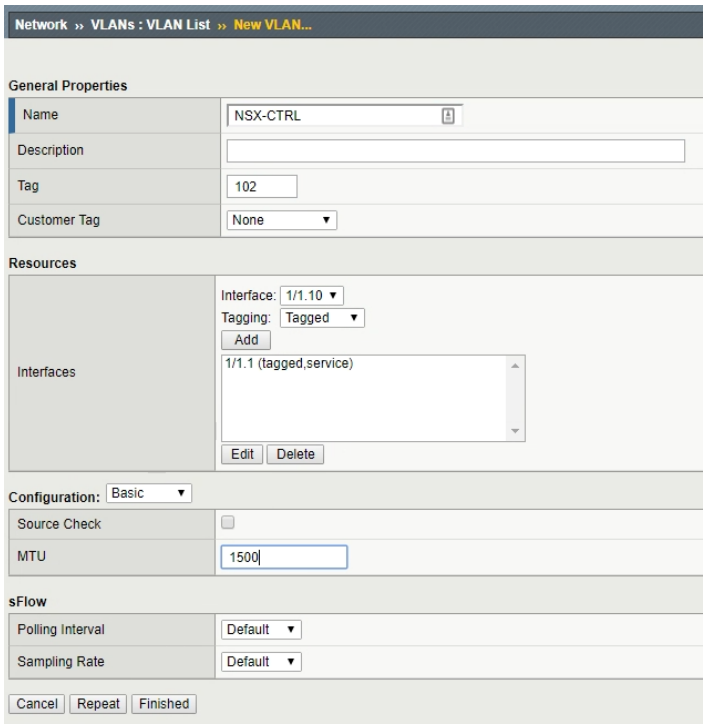
3. In the New VLAN menus,
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used External.
   b. In the Tag field, enter the External VLAN ID in this example, our VLAN is 176.
   c. Under Resources, for Interface, select 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and then click the Add button below it.
   e. Select Repeat to continue.

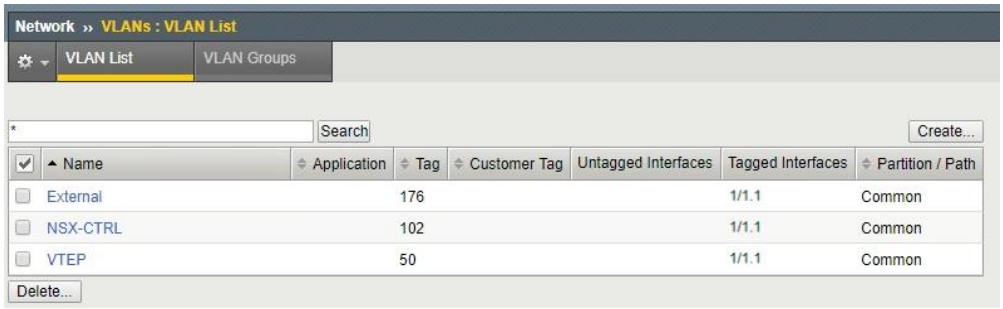


4. In the New VLAN Menus
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used VTEP.
   b. For the Tag, enter the VTEP VLAN ID in this example, our VLAN is 50.
   c. Under Resources, select the Interface 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and click the Add button below it.
   e. In the MTU Field make sure to enter the MTU of your VTEP Network in our use case it is 1600
      This is the network that the ESXi vmkernel and Overlay uses to communicate over VXLAN
   f. Select Repeat to continue.



3. In the New VLAN Menus
   a. Under General Properties, enter a unique name for the VLAN. In this example, we used NSX-CTRL.
   b. For the Tag, enter the NSX-CTRL VLAN ID in this example, our VLAN is 102.
   c. Under Resources, select the Interface 1.1 (or use interface that allows 802.1q tagging)
   d. Select Tagged and click the Add button below it.
   e. Click Finished to proceed.
   f. Validate the VLAN configuration against the image below.

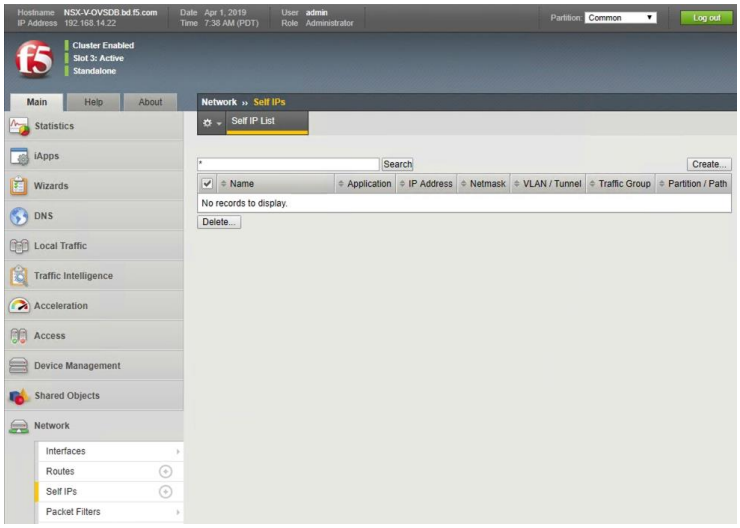




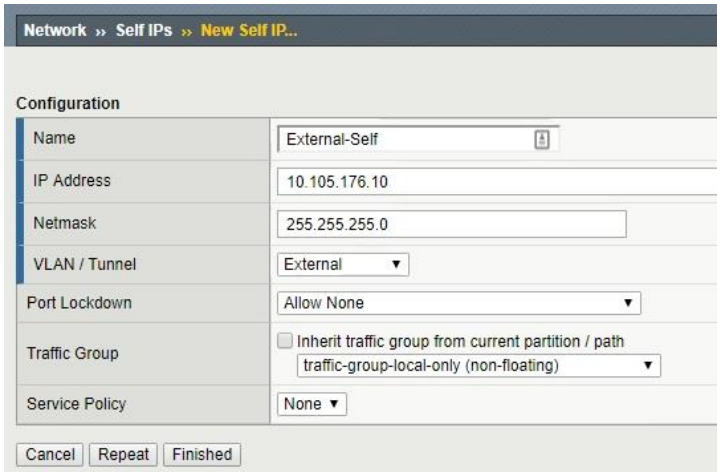
Configure Self IP Addresses

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.

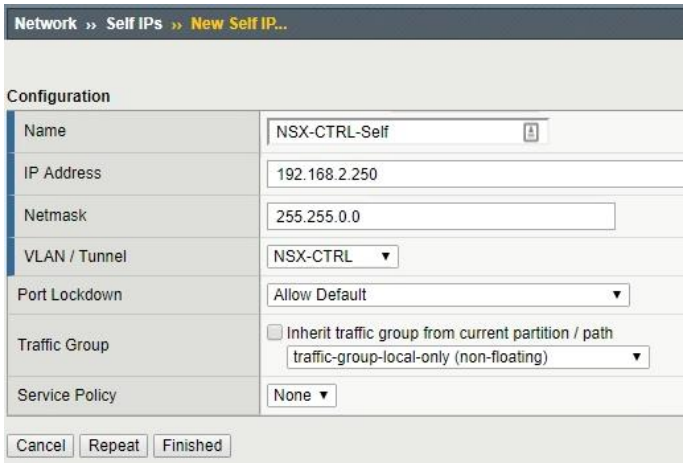
1. On the Main tab of the BIG-IP navigation pane, click Network and then click Self IPs.
2. In the upper right corner of the screen, click the Create button.



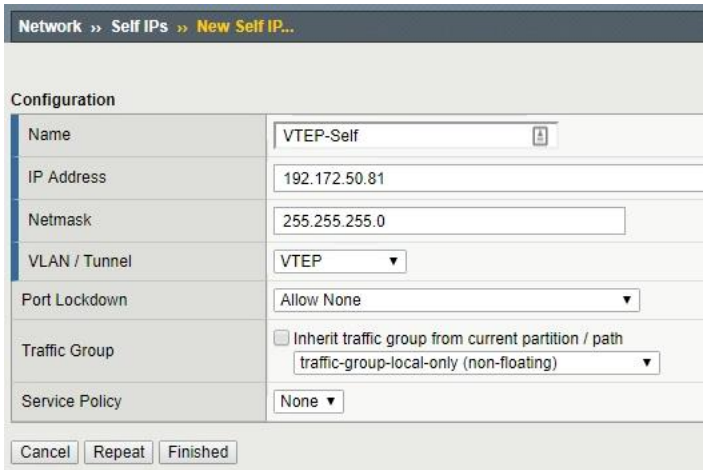
3. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “External-Self” (without double quotes).
    b. In the IP address box, provide the IP address for the External network, in our example, we used 10.105.176.10.
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select External from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Repeat button to continue



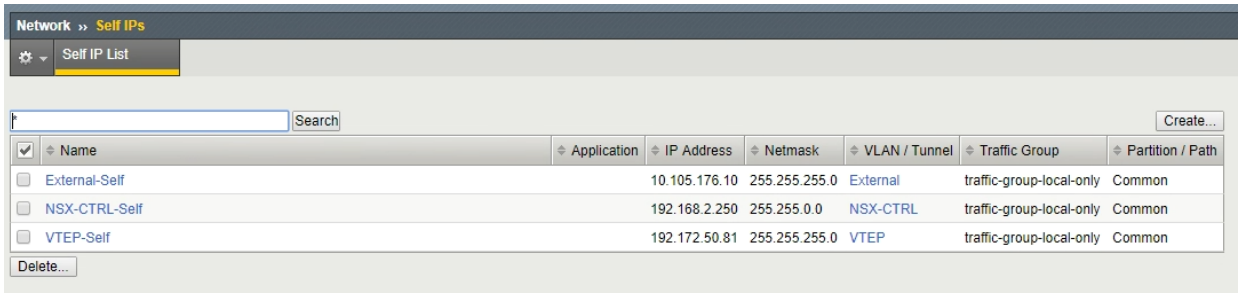
4. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “NSX-CTRL-IP” (without double quotes).
    b. In the IP address box, provide the IP address for the WebTier network, in our example, we used 192.168.2.250
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.0.0
    d. For the VLAN/Tunnel, select NSX-CTRL from the dropdown box.
    e. Use the setting (Allow Default) for Port Lockdown and the default setting for Traffic Group.
    f. Click the Repeat button to continue



5. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “VTEP-Self” (without double quotes).
    b. In the IP address box, provide the IP address for the External network, in our example, we used 192.172.50.81
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0
    d. For the VLAN/Tunnel, select External from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Finished Button to complete the configuration



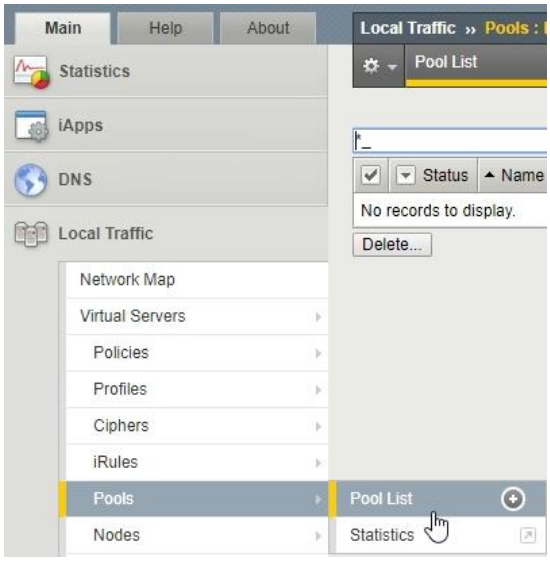
6. Validate the VLAN configuration against the image below.

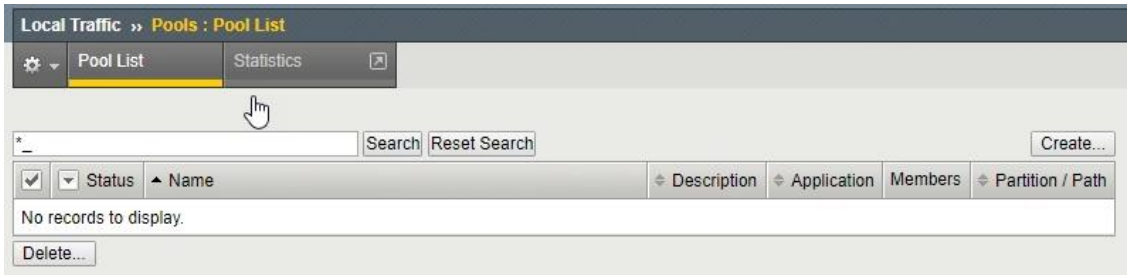


Create Pools

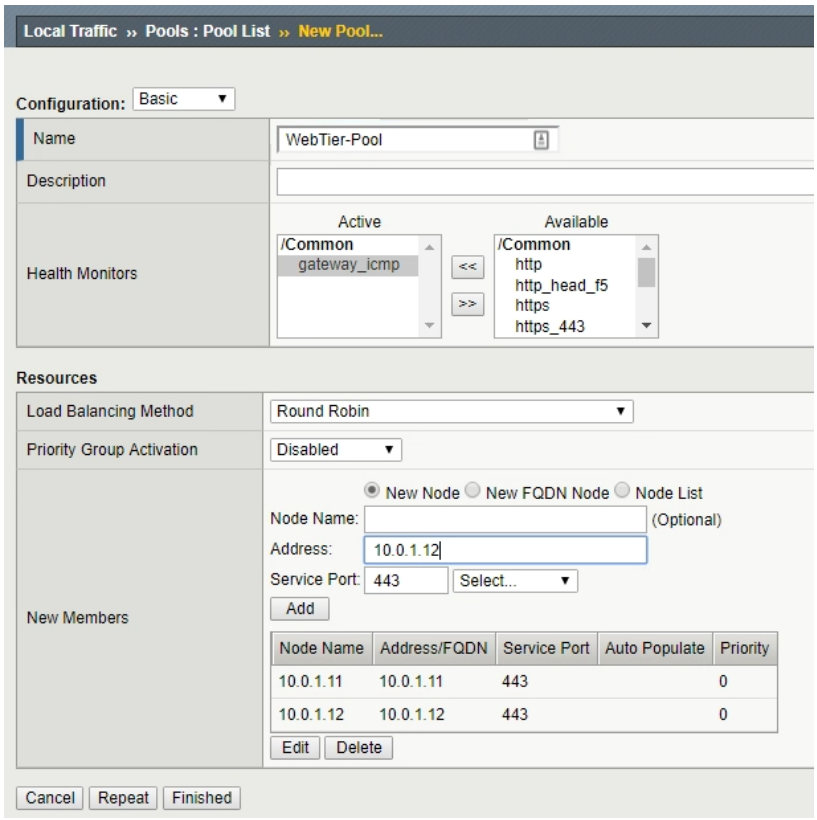
Prior to creating the OVSDB connection, we will create the pools for the App and Web Tier machines to validate that there is no connectivity to them prior to the configuration.

1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Local Traffic and select Pools → Pool List.
2. In the upper right corner of the screen, click the Create button.

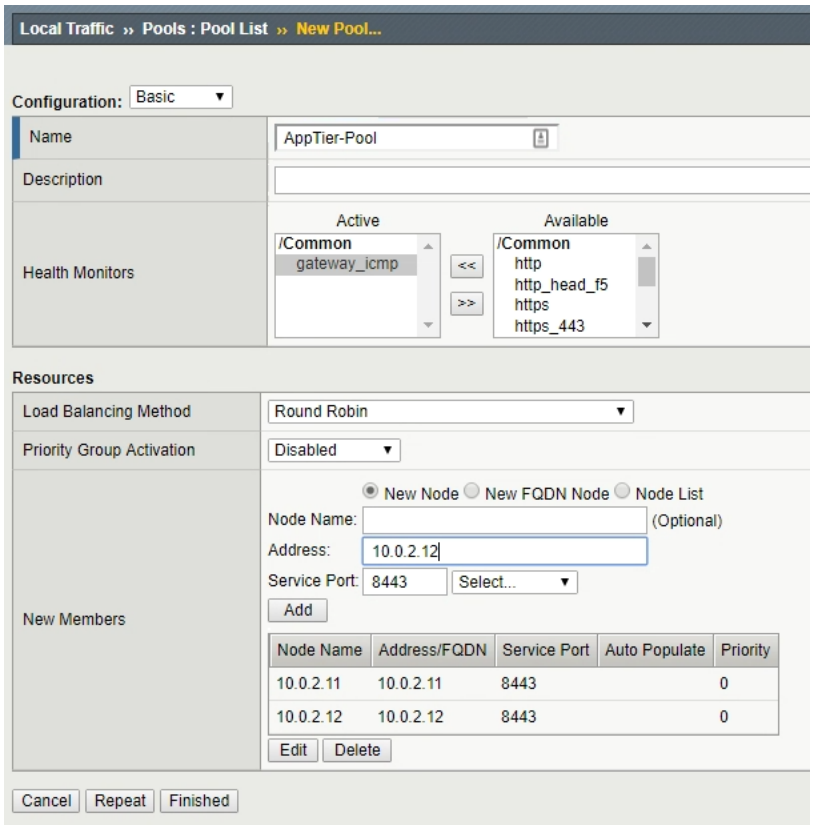




3. In the New Pool menus
   a. Type a unique name in the Name box. In this example, we used “WebTier-Pool” (without double quotes).
   b. In the Health Monitors select gateway_icmp from the Available slot and move it into the Active slot.
   c. In the Load Balancing Method select Round Robin
   d. In the New Members Field
      i. (Optional) Enter a Unique Node name for the Web Server.
      ii. Enter the Address for one of the Web Servers. In this example we used 10.0.1.11
      iii. Enter the Port for the same Web Server. In this example we used 443
      iv. Click the Add Button
      v. Repeat steps (i-iv) for any additional Web Servers. In this example we had 10.0.1.12 as well
   e. Click Finished to complete.



4. In the New Pool menus
   a. Type a unique name in the Name box. In this example, we used “AppTier-Pool” (without double quotes).
   b. In the Health Monitors select gateway_icmp from the Available slot and move it into the Active slot.
   c. In the Load Balancing Method select Round Robin
   d. In the New Members Field
      i. (Optional) Enter a Unique Node name for the App Server.
      ii. Enter the Address for one of the App Servers. In this example we used 10.0.2.11
      iii. Enter the Port for the same App Server. In this example we used 8443
      iv. Click the Add Button
      v. Repeat steps (i-iv) for any additional App Servers. In this example we had 10.0.2.12 as well
   e. Click Finished to complete.



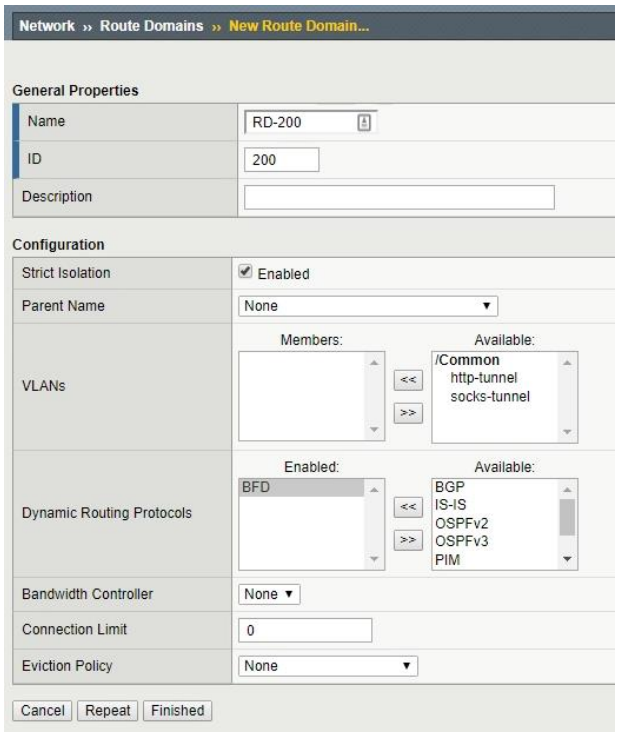
5. Validate the Pool configuration against the image below. (The Pools should be in an Offline (Enabled) state – Red Diamond). This is due to pool members not being able to communicate via the F5 until the remainder of the configuration is completed.

Create Route Domain

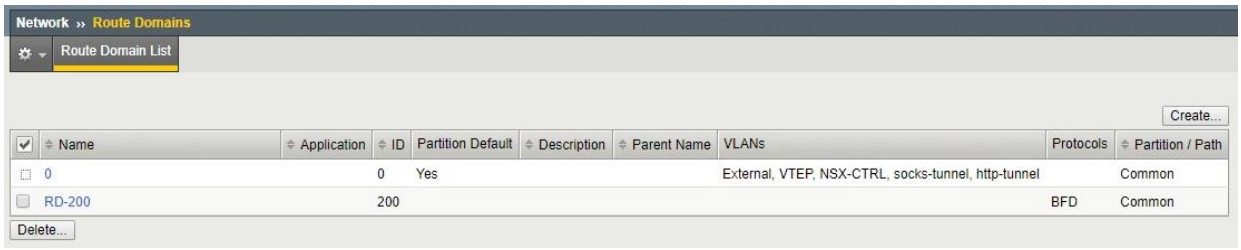
Prior to creating the OVSDB connection we will create a route domain for the VXLAN Traffic, this is required prior to creating an OVSDB connection using BFD.

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

3. In the New Route Domain menus
   a. Type a unique name in the Name box. In this example, we used “RD-200” (without double quotes).
   b. Enter the route domain number in the ID box. In this example, we used “200” (without double quotes).
   c. In the Dynamic Routing Protocols Field. Select BFD from the available menus and move to the Enabled menus.
   d. Click the Finished button.



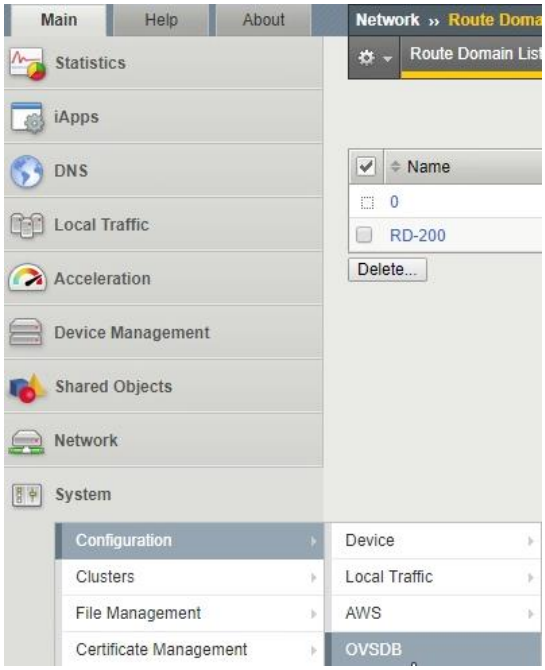
4. Validate the Route Domain configuration against the image below.



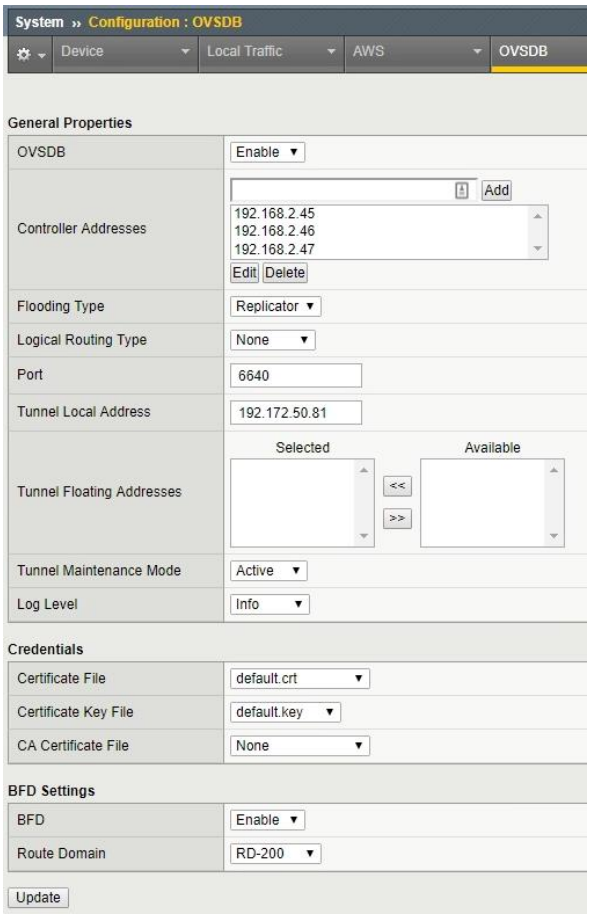
Create OVSDB Configuration

This section goes through enabling the OVSDB connection from the F5 to NSX-V and vSphere.

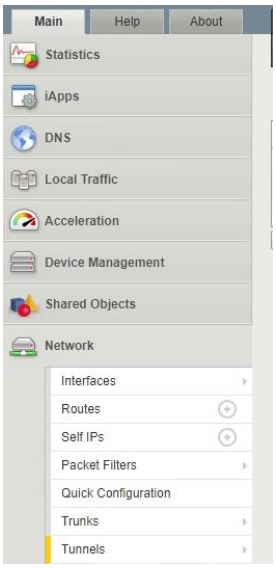
1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Configuration and select OVSDB.

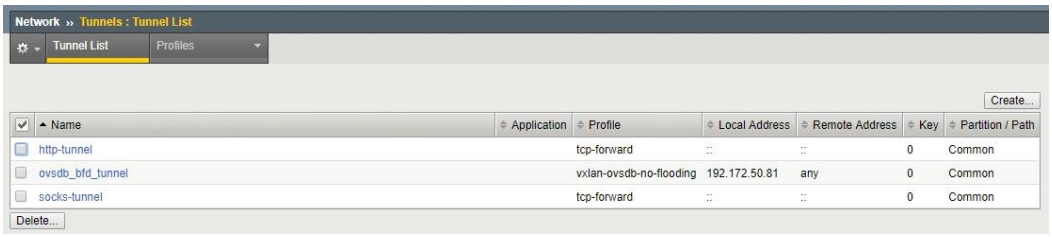


2. In the OVSDB Configuration menus
   a. In the General Properties section
      i. OVSDB – Select Enable
      ii. Controller Addresses – Enter the Addresses of the NSX Controllers clicking add after entering each one. In this example we used 192.168.2.45, 192.168.2.46, 192.168.2.47
      iii. Tunnel Local Address – This is the VTEP-Self IP address used to communicate to the Overlay and VTEPs to the other ESXi Hosts. in this example we used 192.172.50.81
      iv. Leave all other defaults in General Properties Menus.
   b. In the Credentials section
      i. Certificate File – Select Certificate used to communicate to NSX Controllers. In this example we used the default certificate deployed with the F5 BIG-IP (default.crt).
      ii. Certificate Key File – Select the Key used for the certificate listed in Certificate File. In this example we used the default certificate key deployed with the F5-BIG-IP (default.key)
      iii. CA Certificate File – Select NONE
   c. In the BFD Settings section.
      i. BFD – Select Enable
      ii. Route Domain – Select the Route Domain previously created
   d. Click the Update Button.

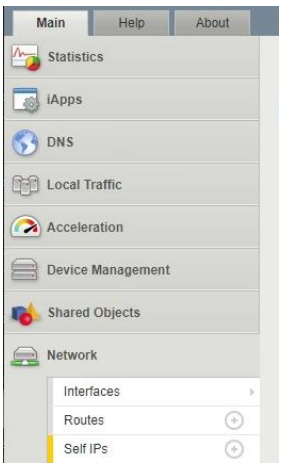


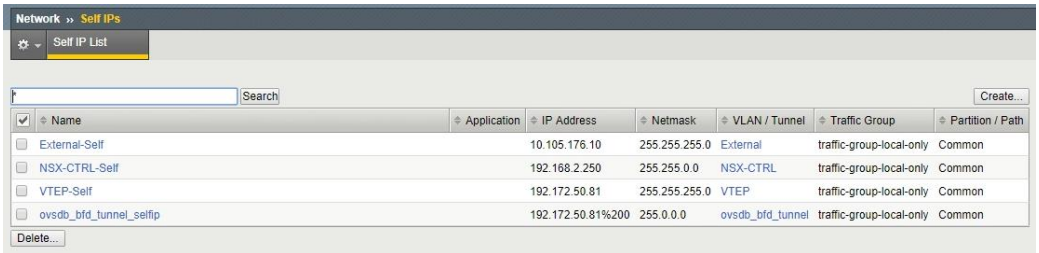
3. Validate the creation of the Tunnels and Self IP for the OVSDB configuration.
   a. In the Main menus, expand Network and select Tunnels.





   b. In the Main menus, expand Network and select Self IPs.

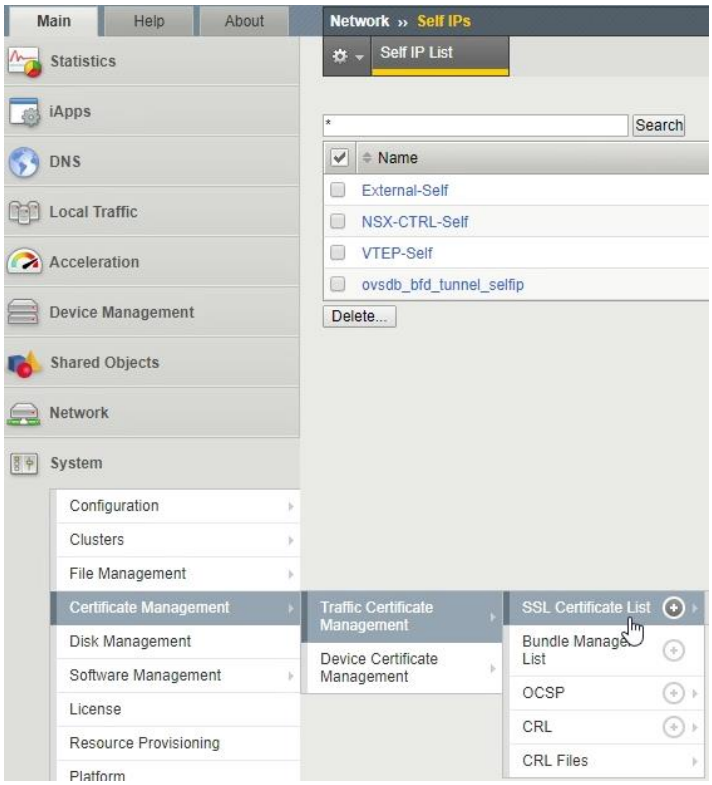




Export Certificate

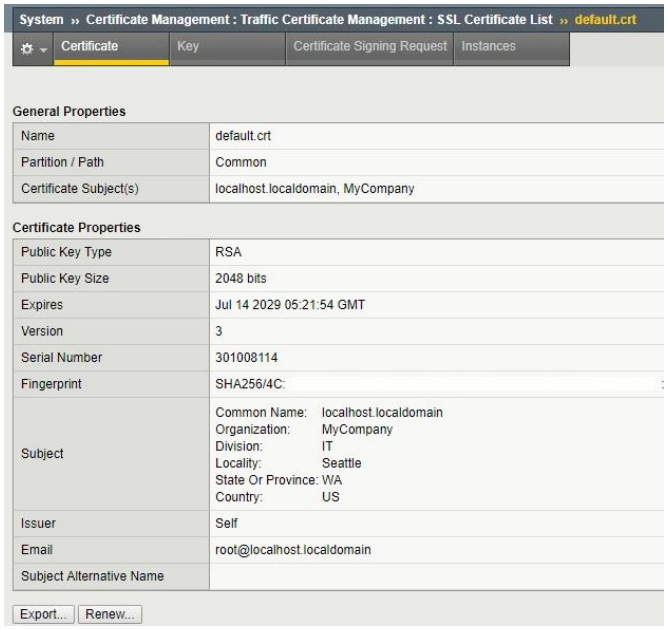
Next we will need to export the certificate used in the previous section for the vSphere NSX and BIG-IP OVSDB communication to work correctly.

1. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand System then go to Certificate Management → Traffic Certificate Management → and select SSL Certificate List.

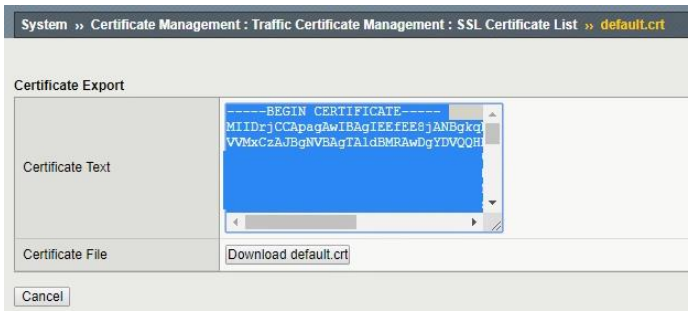


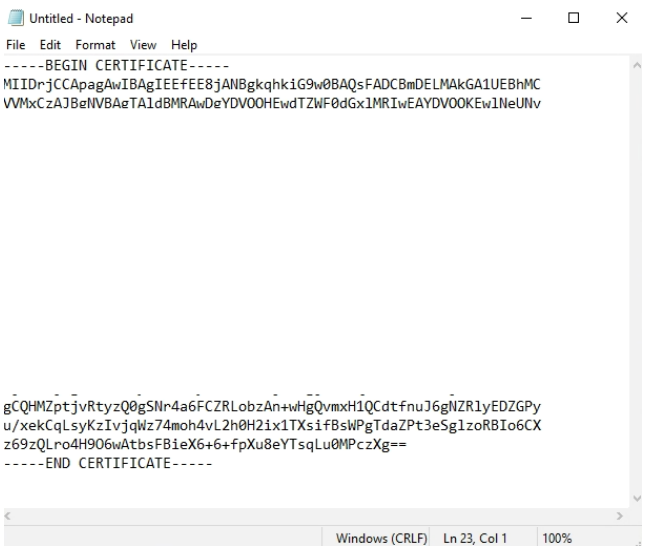
2. Select the certificate used in previous section for configuring OVSDB. In our example we used default.

3. In the selected certificate's Certificate sub-menus, click the Export button. **(Edited for data protection)**



4. In the Certificate Text field, copy the entire string and paste into a notepad or text editor application file for later configuration. **(Edited for data protection)**

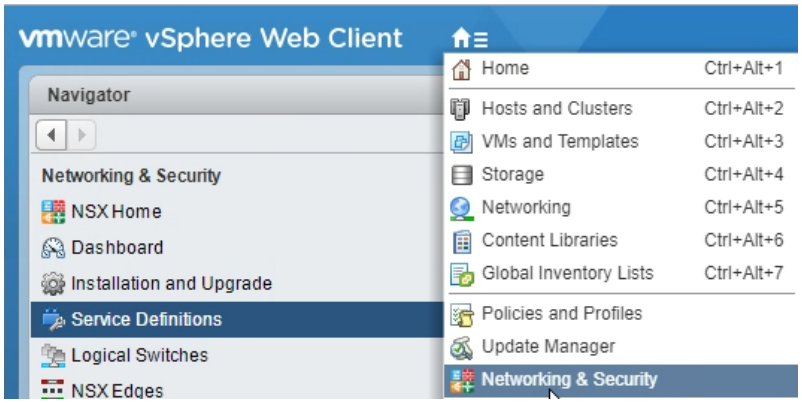


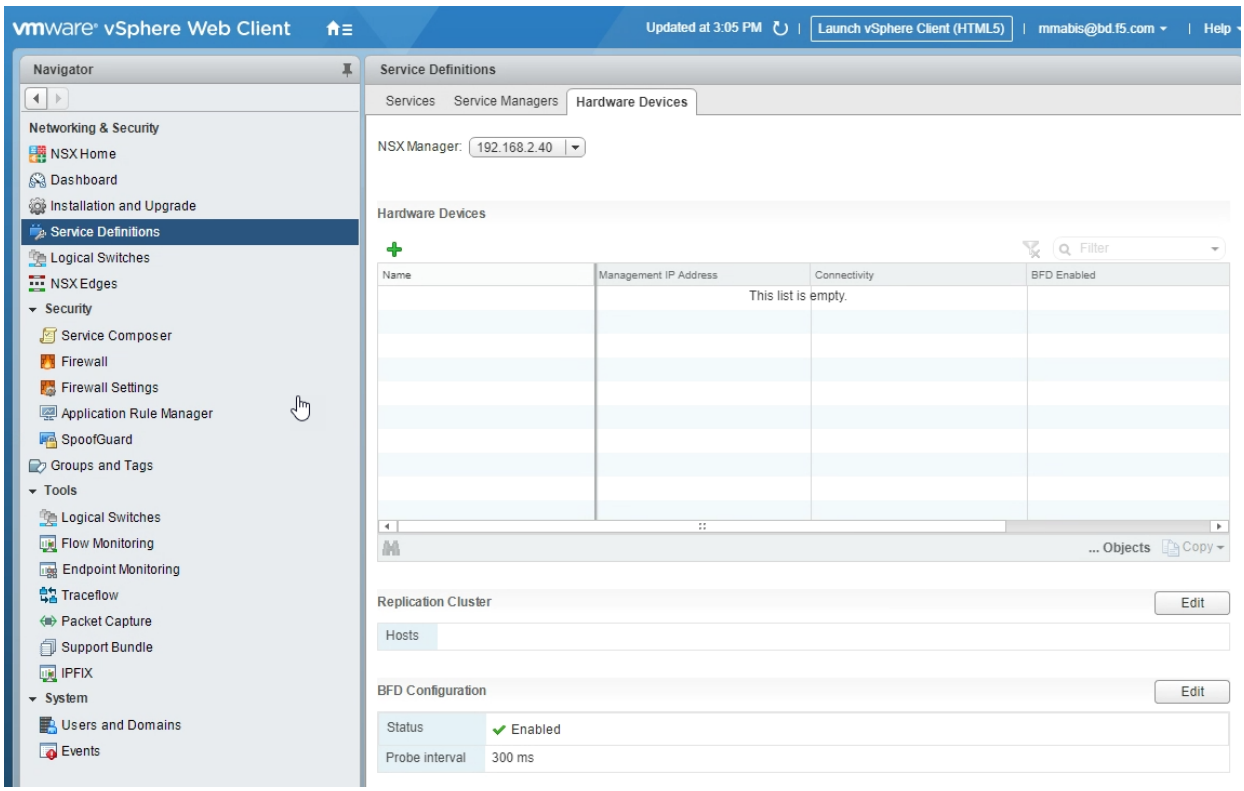


Configure NSX-V Hardware Device in vSphere

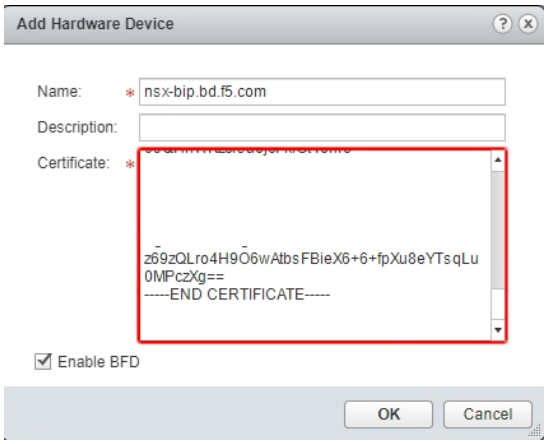
Next we will need to configure the Hardware VTEP within vSphere (Currently this configuration can only be found in the Flash Client).

1. From the Main Menus of the vSphere Web Client (Flash) console, select the Home Icon and select Networking and Security.
2. In the left-hand menus, select Service Definitions → Hardware Devices and click on the Green Plus (+) under Hardware Devices.

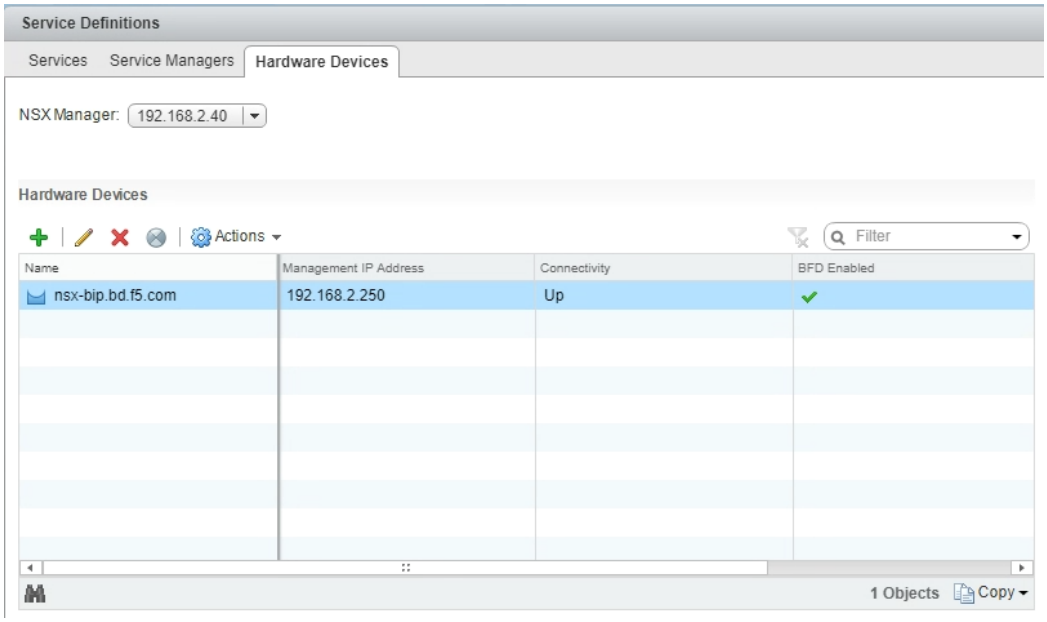




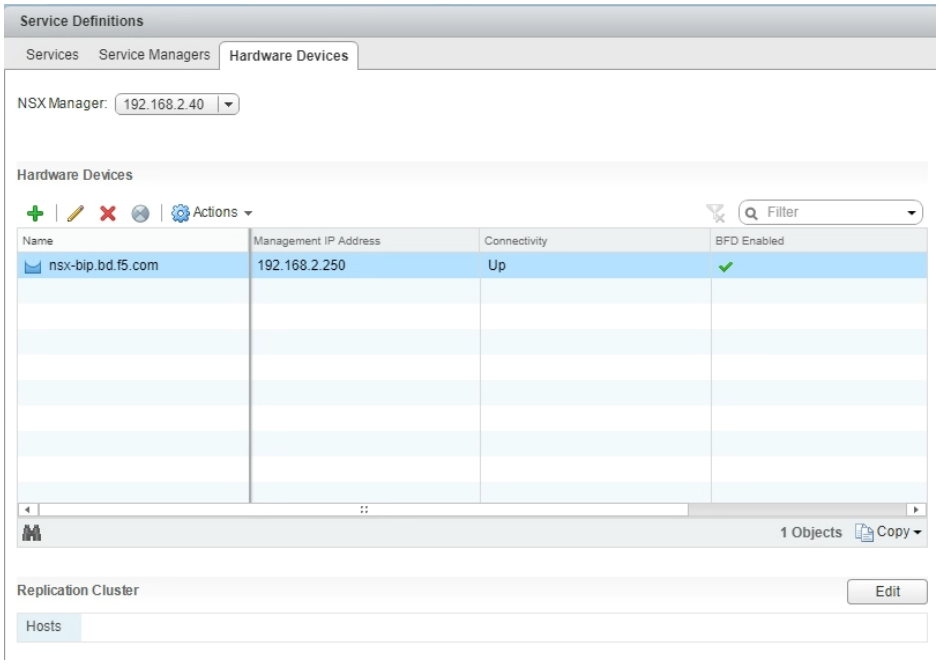
3. In the Hardware Device menus
   a. Enter a unique name for the hardware device. In our example, we used the FQDN of the BIG-IP nsx-bip.bd.f5.com.
   b. (Optional) enter a description for the device.
   c. In the Certificate field, paste the certificate data that was copied from the previous section in the notepad or text editor file.
   d. Ensure that Enable BFD checkbox is checked.
   e. Click the OK button when completed.



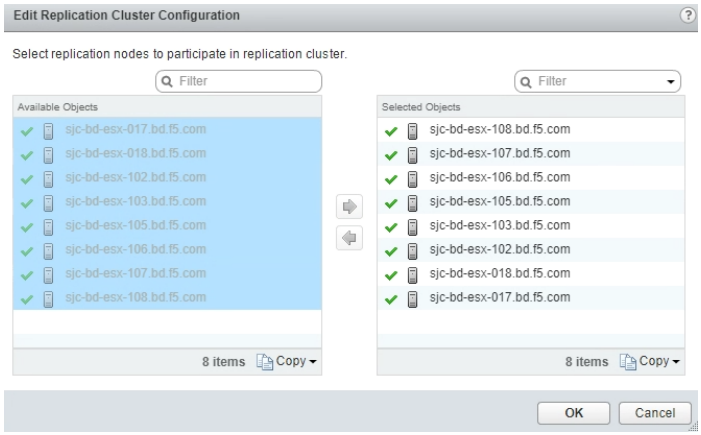
4. Validate that the Hardware device connectivity is Up
   NOTE: If connectivity is not up refresh page, and if still not up go to Troubleshooting section at the end of this document.



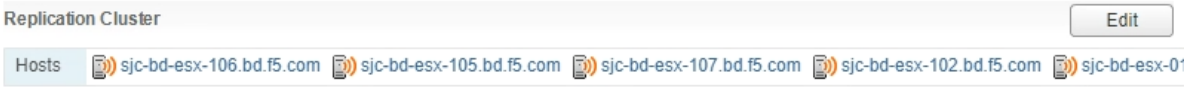
5. In the Replication Cluster section, click the Edit button.



6. Select the replication nodes to participate in the replication cluster. In our example we selected all of the hosts and moved them from Available Objects to Selected Objects and clicked the OK button.



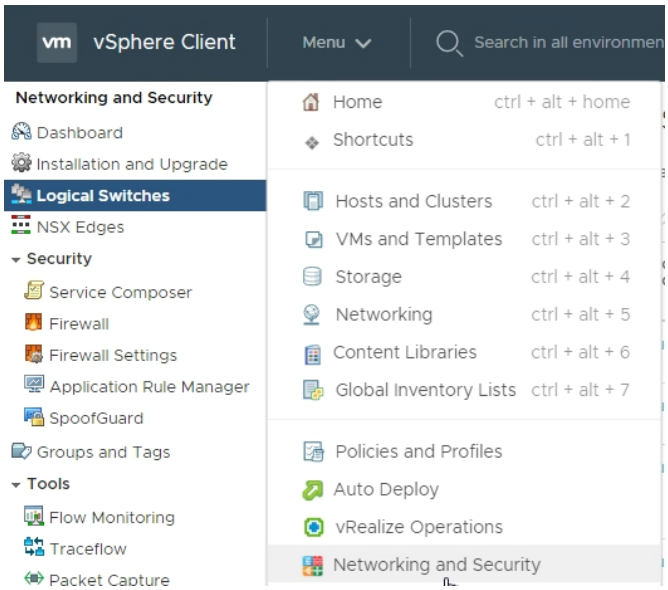
7. Once completed the Replication Cluster hosts will be populated.

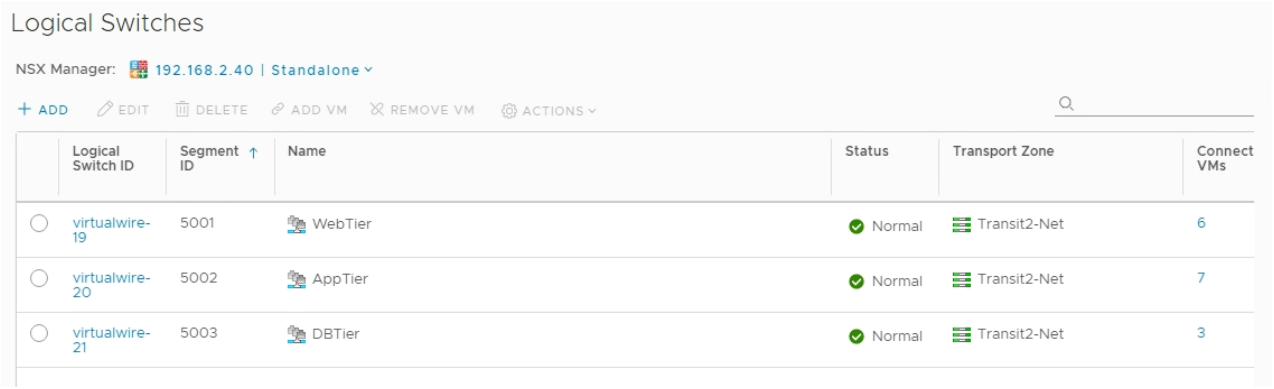


Configure NSX-V Logical Switch to Hardware VTEP.

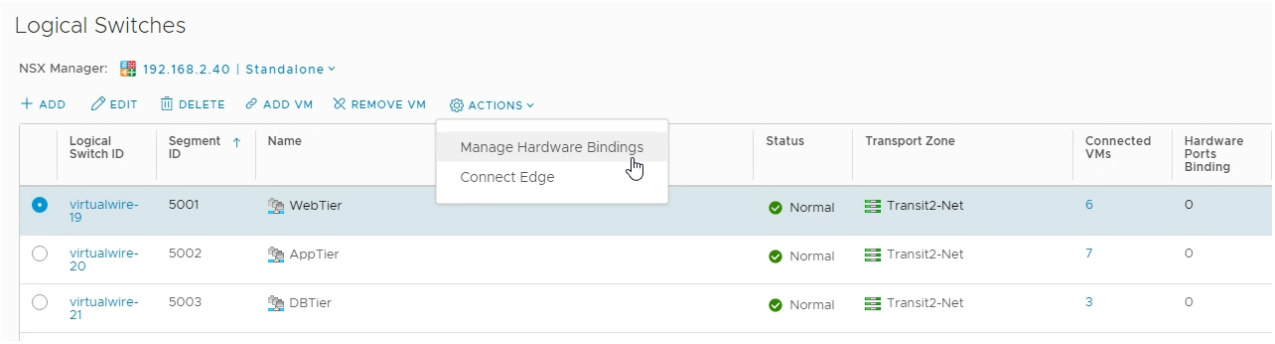
Next we will need to configure the Logical Switches within vSphere, this allows there to be a mapping and tunnel creation from the NSX Nodes to the Hardware VTEP. In this scenario, we will be binding the Web and App Tier networks to the BIG-IP,

1. From the Main Menus of the vSphere HTML5 Client console select the Menu dropdown and select Networking and Security.
2. In the left hand menus select Logical Switches.

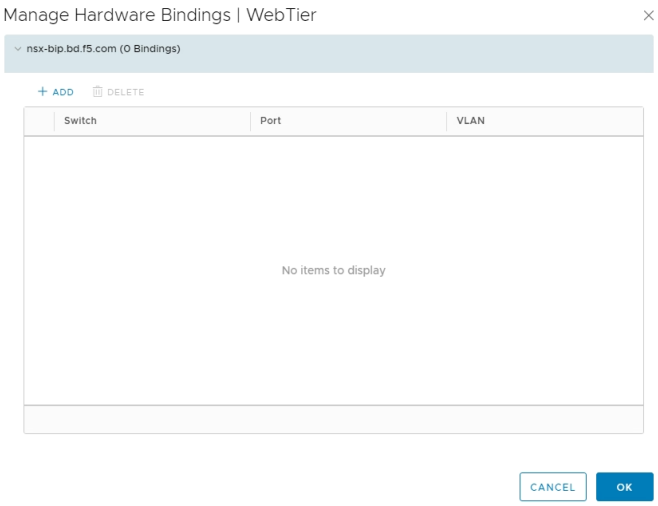




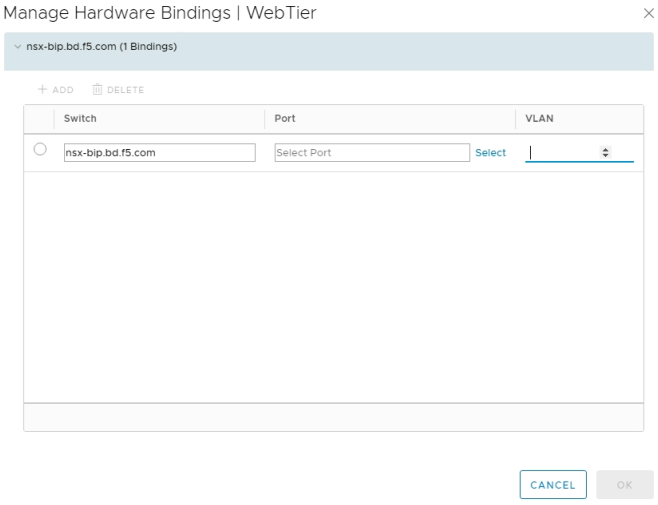
3. Select the WebTier Logical switch go to the Actions pull down and select Manage Hardware Bindings.



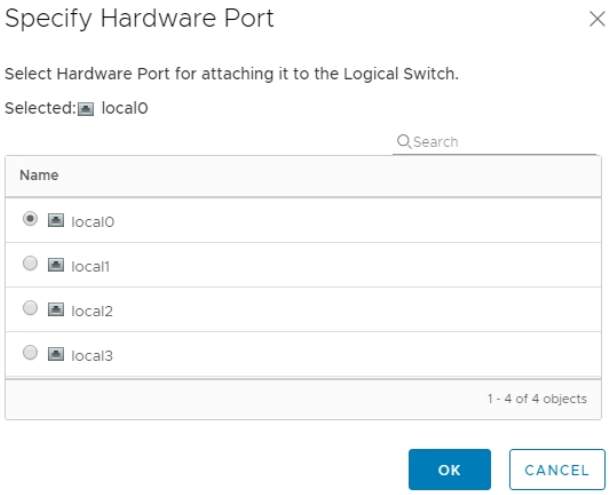
4. In the Manage Hardware Bindings menu for the WebTier Logical switch, expand the BIG-IP and click the (+ Add) link



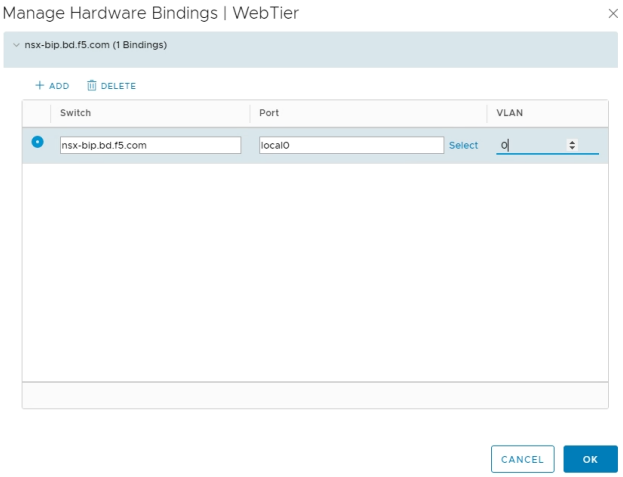
5. Click the Select link in the Port section



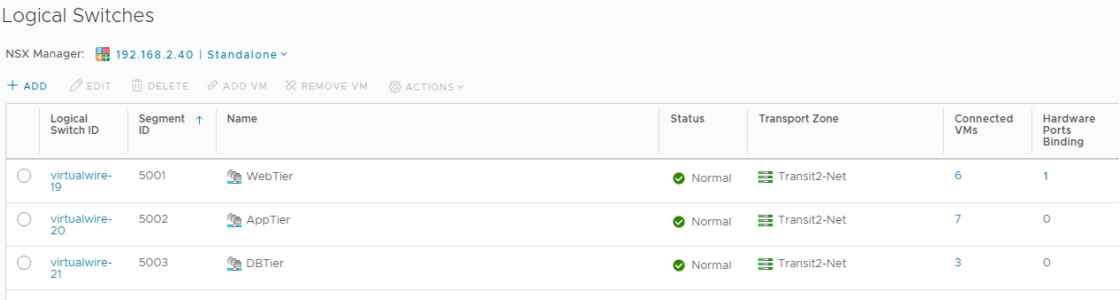
6. Depending on the device used (Physical or VE) there could be Physical links (1/1.1, 1/1.2, etc.) and logical local networks (local0, local1, local2, local3). In our example we will be using Local logical networks, Select local0 and click OK



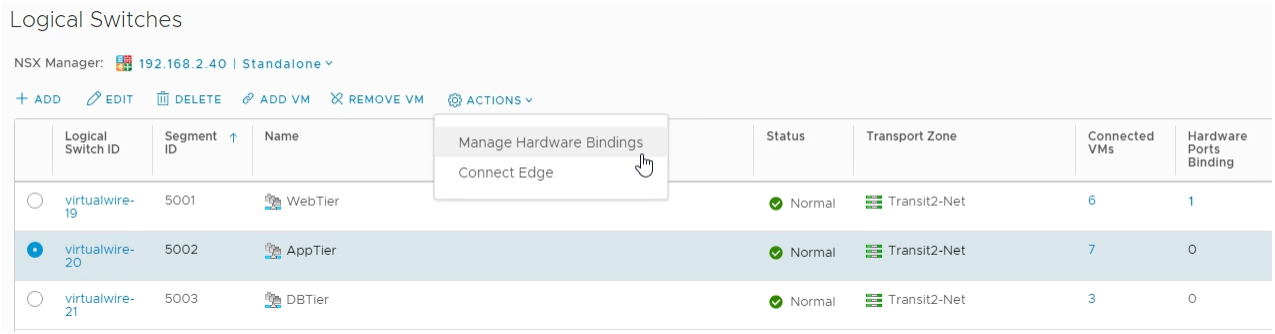
7. In the VLAN section enter a normal VLAN Number (0-4095), this has to be a unique number for each logical switch due to a VMware limitation requiring a VLAN. **The BIG-IP will ignore the VLAN as it does termination of the VXLAN.**
   In our example we entered VLAN 0 for Local0 Port for WebTier and click OK.



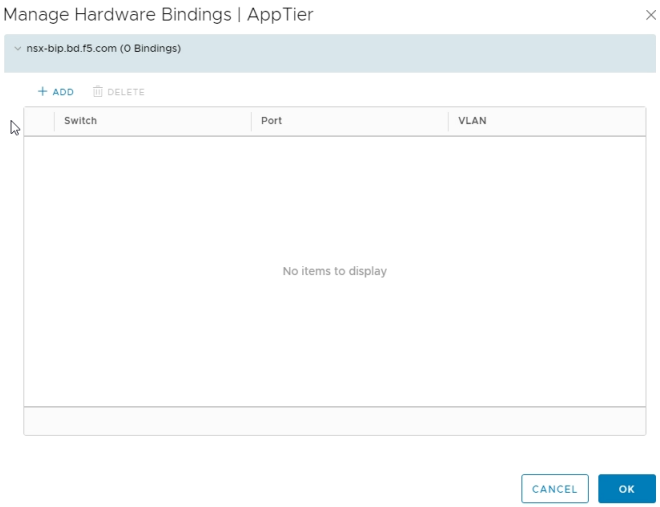
8. Back in the Logical Switches menus, the Hardware Ports Binding column for the selected logical switch will have increased to 1 or by 1. See picture below for WebTier shows 1 binding before it said 0.



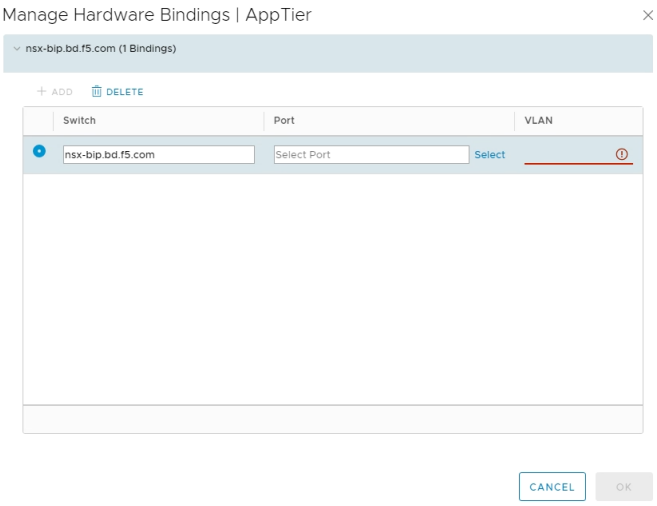
9. Select the AppTier Logical switch go to the Actions pull down and select Manage Hardware Bindings.



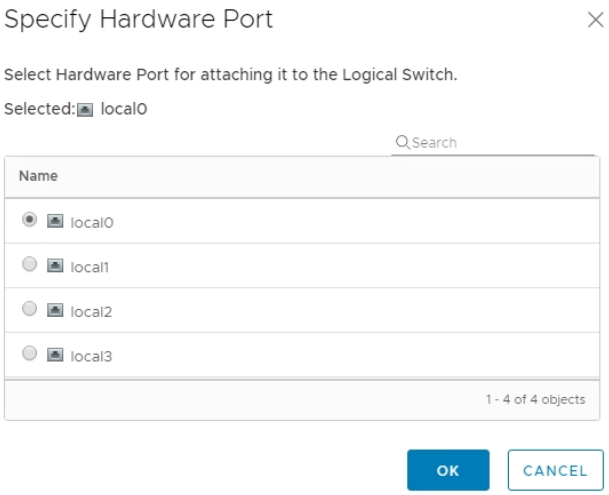
10. In the Manage Hardware Bindings menus for the AppTier Logical switch, expand the BIG-IP and click the (+ Add) link



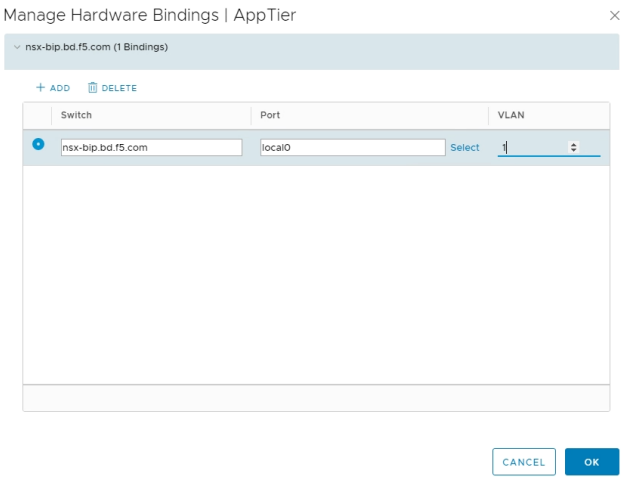
11. Click the Select link in the Port section



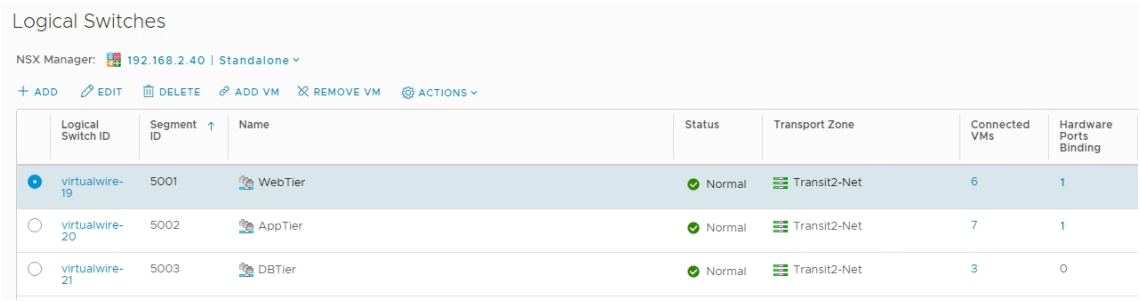
12. Depending on the device used (Physical or VE) there could be Physical links (1/1.1, 1/1.2, etc.) and logical local networks (local0, local1, local2, local3). In our example we will be using Local logical networks, Select local0 and click OK



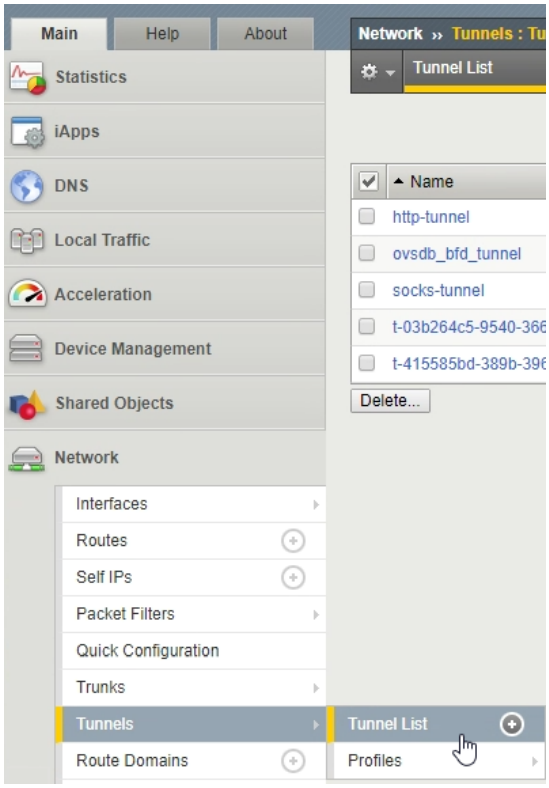
13. In the VLAN section enter a normal VLAN Number (0-4095), this has to be a unique number for each logical switch due to a VMware limitation requiring a VLAN. **The BIG-IP will ignore the VLAN as it does termination of the VXLAN.**
In our example we entered VLAN 1 for Local0 Port for WebTier and click OK.



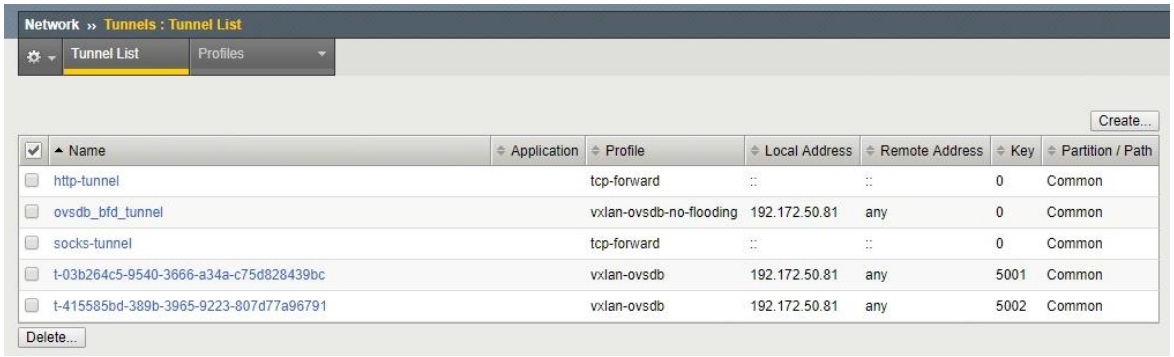
14. Back in the Logical Switches menus, the Hardware Ports Binding column for the selected logical switch will have increased to 1 or by 1. See picture below for WebTier shows 1 binding before it said 0.



5. Once completed, validate that the tunnels are created on the BIG-IP. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network then go to Tunnels → and select Tunnel List.



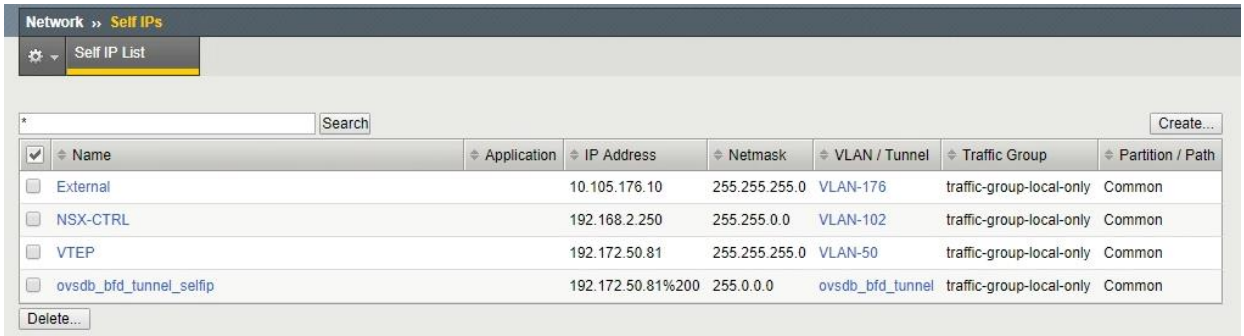
15. Each NSX vxlan-ovsdb tunnel will have a unique GUID for each Segment ID (This GUID is generated by NSX and cannot be changed or controlled). To verify which Segment ID is associated to which GUID look at the Key Section in the Tunnel List. In this example Key 5001 and Tunnel (t-03b26…) is for WebTier and Key 5002 and Tunnel (t-41558…) is for AppTier



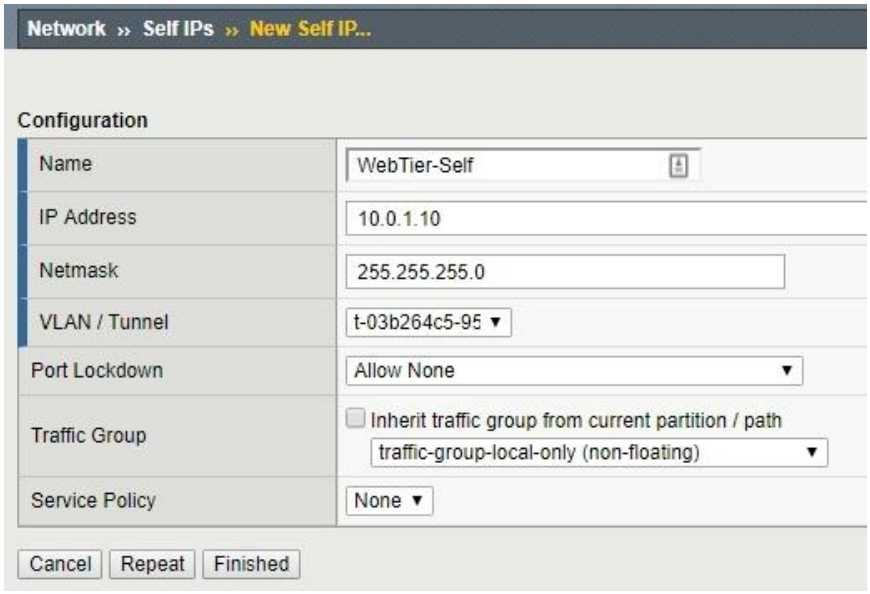
Create Self-IP for OVSDB Tunnels

Next we will need to configure the Self IPs for the OVSDB Tunnels to allow direct communication between the BIG-IP and the WebTier and AppTier via L2.

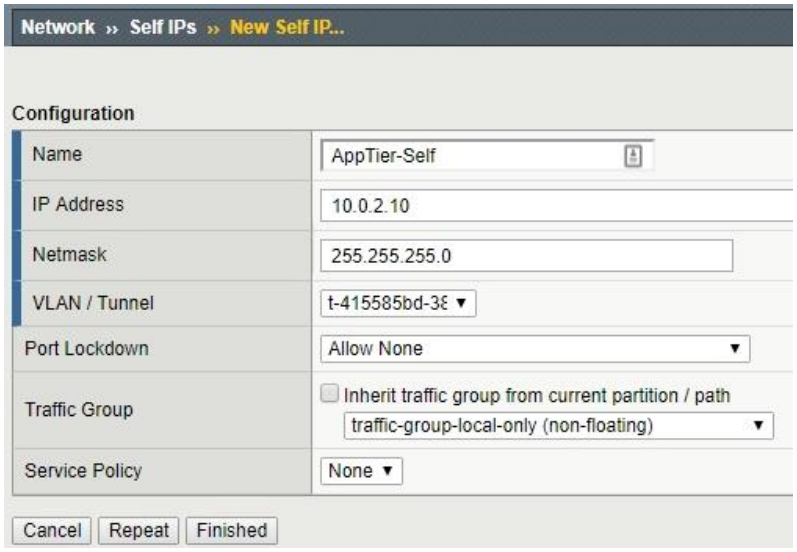
1. Once completed, validate that the tunnels are created on the BIG-IP. From the Main tab of the BIG-IP Configuration Utility navigation pane, expand Network and select Self IPs.
2. In the upper right corner of the screen, click the Create button.

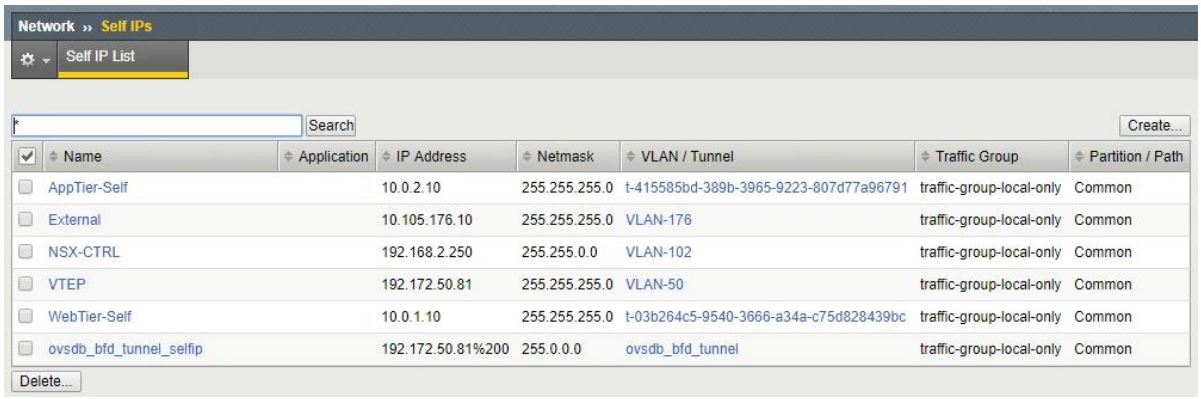


3. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “WebTier-Self” (without double quotes).
    b. In the IP address box, provide the IP address for the External network, in our example, we used 10.0.1.10
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select Tunnel (t-03b26…) from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Repeat button to continue



4. In New Self IP Menus
    a. Type a unique name in the Name box. In this example, we used “AppTier-Self” (without double quotes).
    b. In the IP address box, provide the IP address for the External network, in our example, we used 10.0.2.10
    c. Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
    d. For the VLAN/Tunnel, select Tunnel (t-41558…) from the dropdown box.
    e. Use the default settings (Allow None) for Port Lockdown and Traffic Group.
    f. Click the Finished to validate the completed self IP configurations.





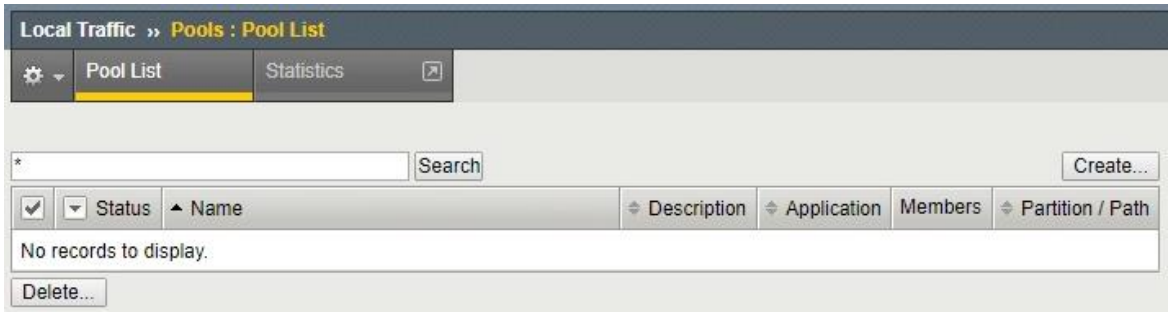
Application Configuration

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.

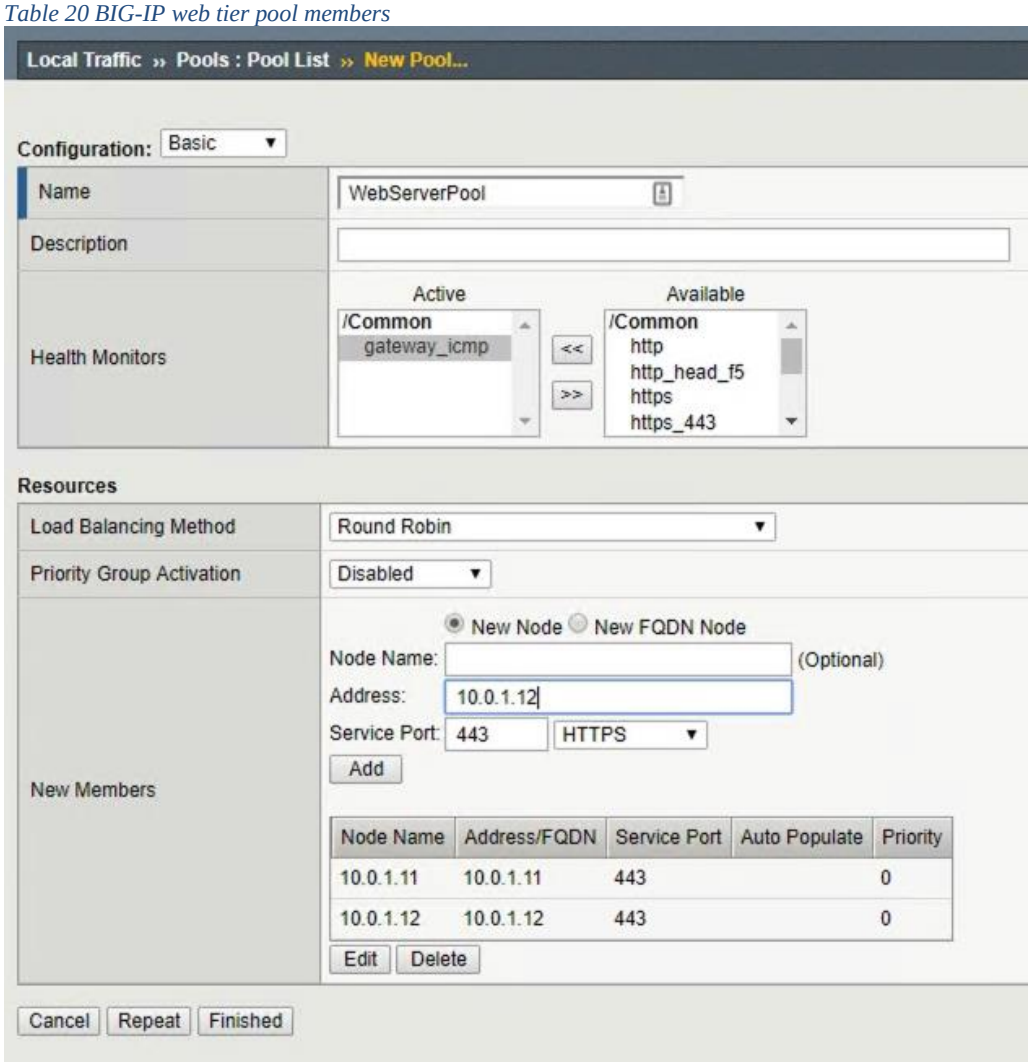


3. In the New Pool menus

   a. In the Name field, type a unique name for the web pool. For this validation, we used WebServerPool.
   b. 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.
   c. Under Resources, select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
   d. Under Resources, use the New Members setting to add the IP address and port of the web servers (refer to Table 20 below). Click the Add button for each pool member.
   e. Click Repeat to continue and enter the application tier information,

Name (Optional)	Address	Service Port
web-01	10.0.1.11	443 (HTTPS)
web-02	10.0.1.12	443 (HTTPS)

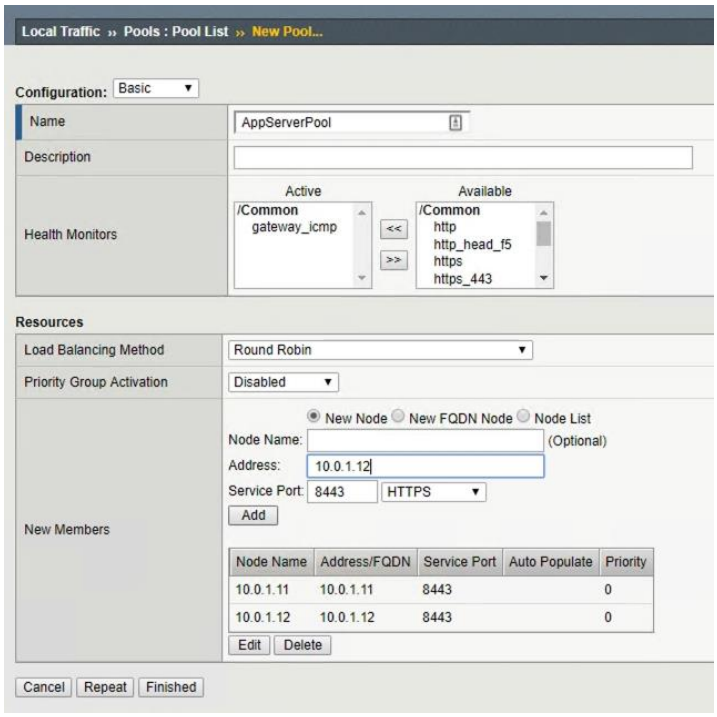
Table 20 BIG-IP web tier pool members



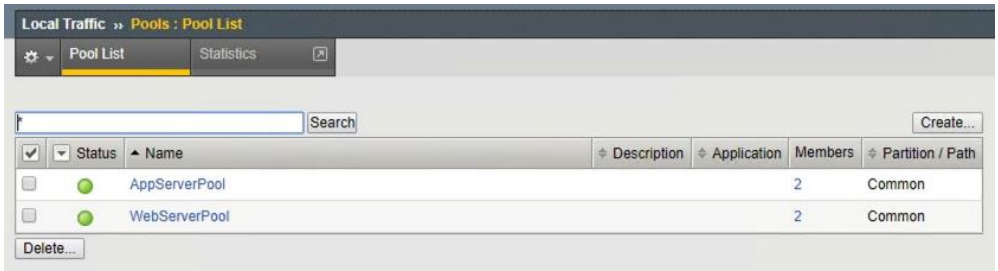
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
   a. In the Name field, type a unique name for the App pool. For this validation AppServerPool was used.
   b. In the Health Monitors section select an appropriate monitor for your application. 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.
   c. In the Resources section of the screen select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
   d. 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 21). Select the Add button for each pool member.
   e. Click Finished to complete the pool creation.

Name (Optional)	Address	Service Port
app-01	10.0.2.11	8443
app-02	10.0.2.12	8443

Table 21 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 from the ovsdb-tunnel VXLAN network.

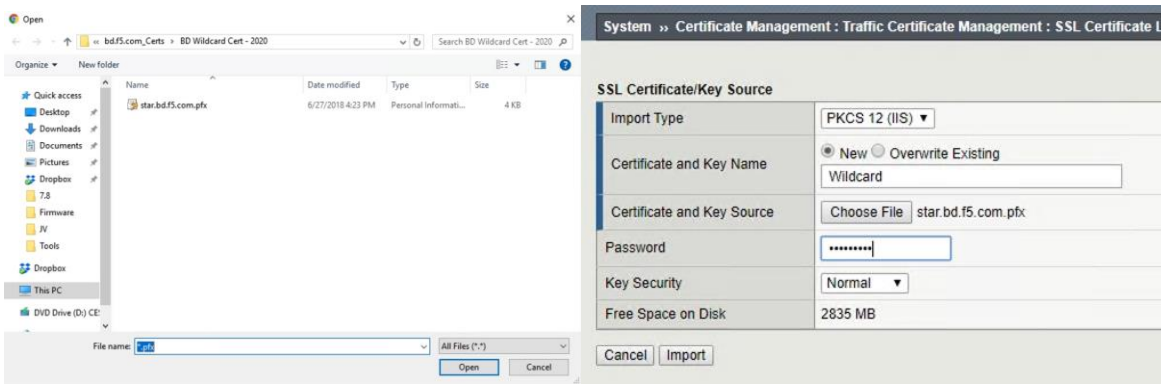


Import SSL Certificate

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

As a prerequisite to completing this task you must have a Certificate with a Private Key (Exportable) available to install this could be in Certificate/Key format or PKCS12 (PFX) format. In our test case we will be using a public PKCS12 certificate (PFX) wildcard certificate "*.bd.f5.com" that will allow any DNS name in front of bd.f5.com to be accepted as a valid name in a web browser.

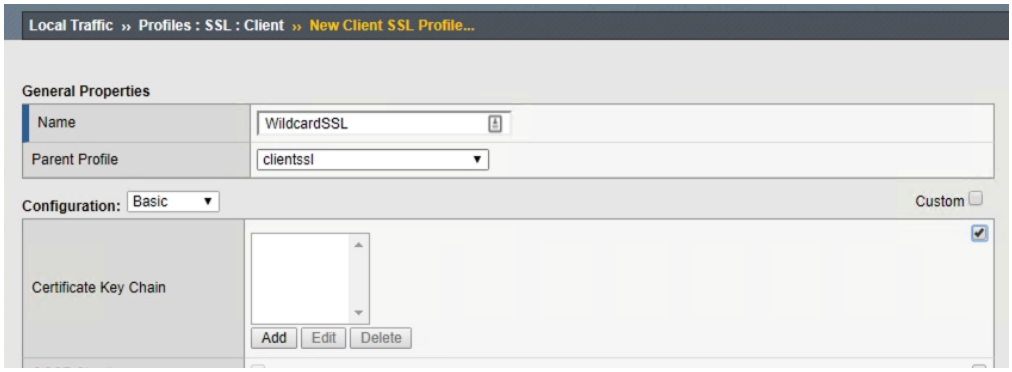
1. On the Main tab, select System → Traffic Certificate Management → SSL Certificate List
2. In the upper right corner of the screen, click the Import button.
3. In the Import SSL Certificate and Keys menus
    a. In the Import Type field, in our example we select "PKCS 12 (IIS)"
    b. In the Certificate and Key Name field, in our example we entered "Wildcard" without quotes
    c. In the Certificate and Key Source field, select the "Choose File" button
    d. In the pop out menus browse and select the file, in our example star.bd.f5.com.pfx
    e. In the password field, enter the password to decrypt the pfx file.
    f. Click the Import button

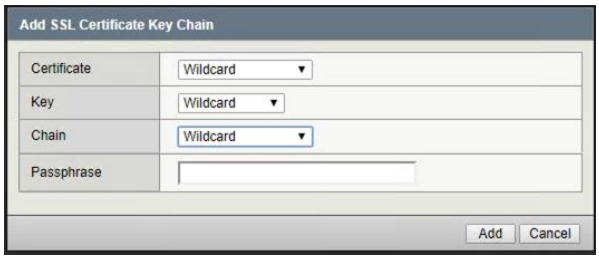


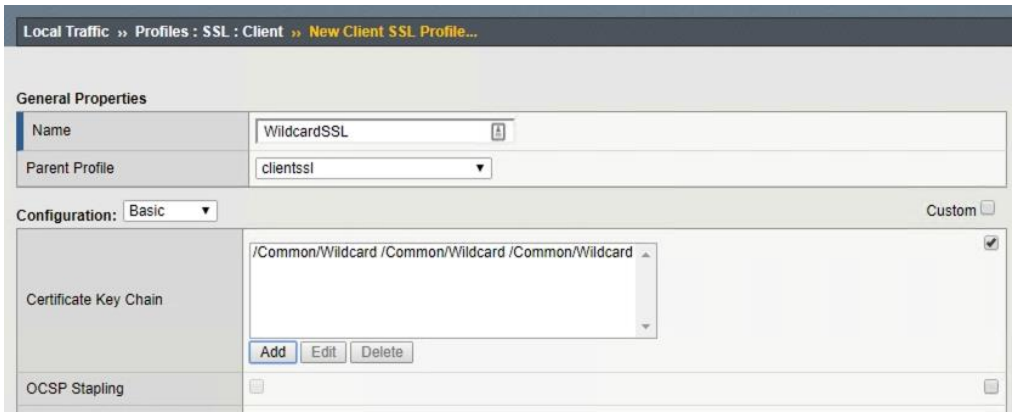
Create ClientSSL Profile

Prior to creating a virtual server for our implementation, a certificate must be imported, and a ClientSSL Profile must be created to ensure a seamless HTTPS connection to the Web Server. With F5's full proxy the backend web server certificate could be self-signed and the F5 could present a fully validated certificate to the clients (users) allowing a secure transaction throughout the web call.

1. On the Main tab, select Local Traffic → Profiles → SSL → Client
2. In the upper right corner of the screen, click the Create button.
3. In the New Client SSL Profile menus
    a. In the Name field, type a unique name for the profile, for this validation WildcardSSL was used.
    b. In the Certificate Key Chain field, check the custom box and click the Add button
    c. In the Certificate, Key and Chain pulldown menus, select the previously imported Certificate chain, in this validation it was named Wildcard. Then click the Add button.
    d. Once added, scroll to the bottom and click the Finished button.



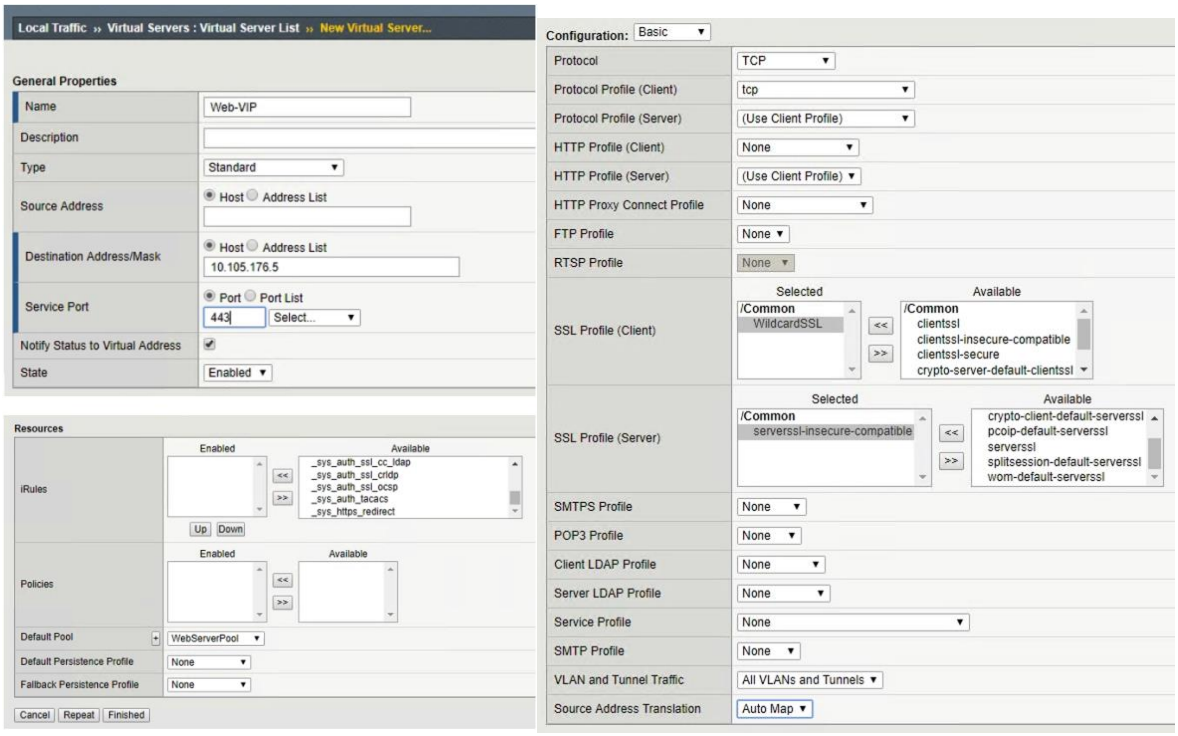




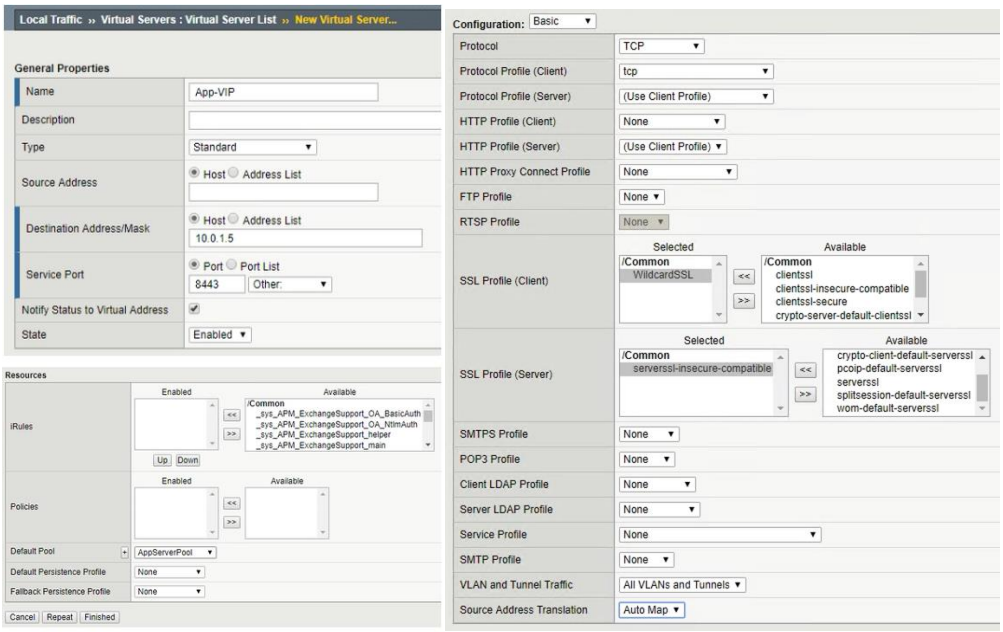
Create Application Virtual Servers

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 WebTier, which will be available to the external network on the 10.105.176.0/24 segment, and the other for the AppTier, available on the WebTier logical network.

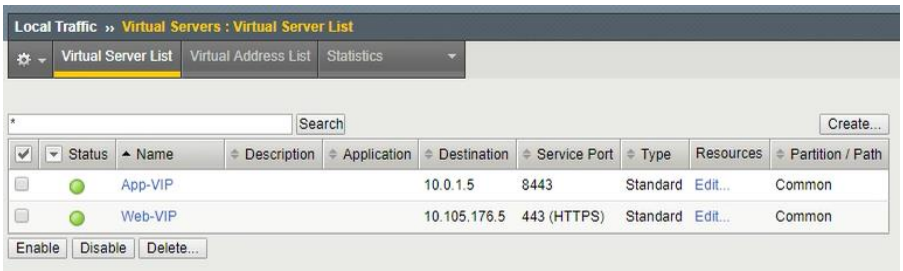
1. On the Main tab, select Local Traffic and then click Virtual Servers. The Virtual Server List screen is displayed.
2. In the upper right corner of the screen, click the Create button.
3. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the web application. In this case, we used Web-VIP.
    b. In the Destination Address field, enter 10.105.176.5
    c. For Service Port use the standard HTTPS port 443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the WebServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Repeat to continue to configure the application tier virtual server



4. In the New Virtual Server menus
    a. In the Name field, provide a unique name for the App tier application. In this case, we used App-VIP.
    b. In the Destination Address field, enter 10.0.1.5
    c. For Service Port use the standard HTTPS port 8443.
    d. In the Configuration section
        I. Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
        II. Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
        III. Select Auto Map from the pull-down menus for the Source Address Translation.
    e. In the Resources section
        I. Select the AppServerPool from the Default Pool dropdown box.
        II. Typically, a persistence profile would be used in a real-world case but to validate that the servers are changing (round-robin) we have omitted it currently.
    f. Click Finished to continue to configure the application tier virtual server



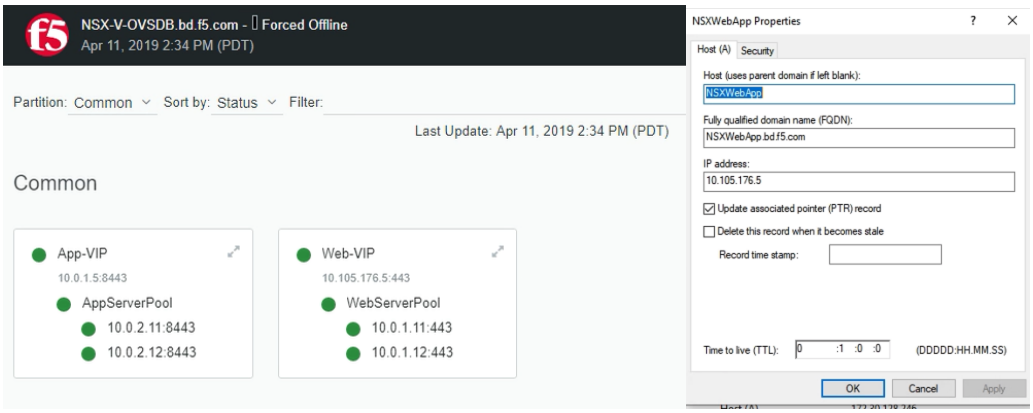
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.



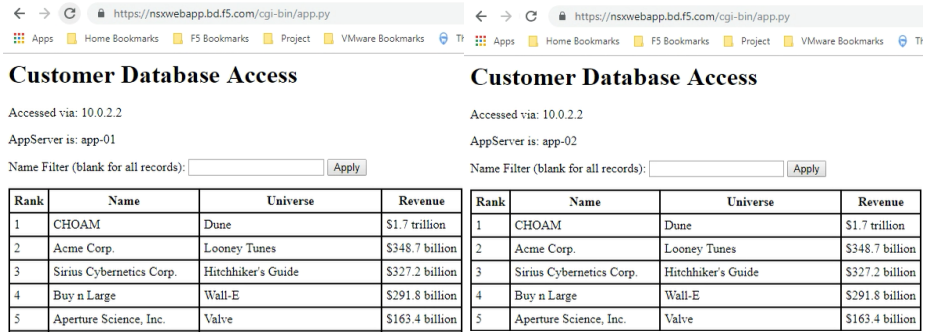
Validation

The web tier virtual server should now be available and accepting application traffic on port 443 (HTTPS).

On the Main tab, expand Local Traffic and then click Network Map to display the overall health of the applications and their associated resources. Due to also this traffic being HTTPS rather than HTTP we setup a FQDN of NSXWebApp.bd.f5.com to allow our wildcard certificate to be validated when connecting to the site.



Any web browser can be used to test by typing https://NSXWebApp.bd.f5.com/cgi-bin/app.py to send a request to the virtual server. Our 3-tier application will appear and show data within the database validating that the connection works, to further validate which application server you can refresh the page and see the AppServer changes. To further validate which Web server is being used we run a curl command “curl -kv “https://nsxwebapp.bd.f5.com” in the web server we injected a header in the web server configuration (not shown in this guide) called X-Upstream-Server to show which web server was being accessed.



This concludes the validation of the *OVSDB Integration with NSX-V* deployment scenario.

Troubleshooting

This section accounts for some of the troubleshooting that can be done on the F5 to determine where issues might arise.

Commands in the F5 console that can be used to examine connectivity.

BIG-IP OVSDB Troubleshooting

- **TMSH:**

tmsh list net tunnels tunnel <tunnel-name>
tmsh list net fdb tunnel <tunnel-name>
tmsh list net self
tmsh list net arp
tmsh list net route
tmsh show net tunnels endpoint tunnel-name <tunnel-name>
tmsh show net tunnels tunnel <tunnel-name>
tmsh show net fdb tunnel <tunnel-name>

- **ZebOS:**

imish -r <route-domain-id> -e 'show running-config'
imish -r <route-domain-id> -e 'show running-config interface ovsdb_bfd_tunnel'
imish -r <route-domain-id> -e 'show bfd session'

- **OVSDB:**

ovsdb-client dump
vtep-ctl list manager
vtep-ctl list physical_switch
vtep-ctl list physical_port
vtep-ctl list logical_switch
vtep-ctl list tunnel
vtep-ctl list ucast_macs_local
vtep-ctl list ucast_macs_remote
vtep-ctl list mcast_macs_local
vtep-ctl list mcast_macs_remote
vtep-ctl list physical_locator_set
vtep-ctl list physical_locator

Example of ovsdb-client command to validate connectivity.

- ovsdb-client dump

Areas in the dump that are of significance (Manager Table which is NSX Controllers) and (Tunnel Tables which is VXLAN connectivity to ESXi Hosts over VTEP Network) will determine if connectivity is Active/Up or not Backoff/Down

```
Manager table
_uuid                                inactivity_probe is_connected max_backoff other_config status                                                               target
------------------------------------ ---------------- ------------ ----------- ------------ -------------------------------------------------------------------- ----------------------
9c579b5d-fc0c-4159-bc1f-d4b696a3ba01 []               true         []          {}           {sec_since_connect="118", sec_since_disconnect="140", state=ACTIVE} "ssl:192.168.2.45:6640"
f5a7c0a6-181d-4e0c-94d1-bd66e997d2cf []               true         []          {}           {sec_since_connect="200", sec_since_disconnect="222", state=ACTIVE} "ssl:192.168.2.46:6640"
d12940b6-2512-4dde-b583-5908618f21c8 []               true         []          {}           {sec_since_connect="273", sec_since_disconnect="295", state=ACTIVE} "ssl:192.168.2.47:6640"
```

```
Tunnel table
_uuid                                bfd_config_local                                                   bfd_config_remote                                                   bfd_params
                              bfd_status                                                            local                                remote
------------------------------------ ------------------------------------------------------------------ ------------------------------------------------------------------- ------------------------
------------------------------ -------------------------------------------------------------------- ------------------------------------ ------------------------------------
2892ef1a-c942-4b98-9413-ed7ff2f6fdda {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.30", bfd_dst_mac="00:50:56:6f:3d:f0"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 f62d06e4-9c45-4525-8701-278c9e5ac816
bf209194-740e-4652-85bd-b804a330139b {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.31", bfd_dst_mac="00:50:56:61:b7:e0"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 556dc505-a969-49e6-8763-b43706843d60
46ad8429-d166-40e6-aaeb-e28f77ea3345 {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.32", bfd_dst_mac="00:50:56:60:e7:8e"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 0c5d2d41-a56b-45e0-906d-0a9ef16159bc
4ecf69de-37be-4499-908a-1d03924daea5 {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.33", bfd_dst_mac="00:50:56:68:40:1c"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 6c415526-2dab-46a5-8473-4a9e2fea0e2f
919aeecd-8ca1-40ef-ae50-9ffd5350f3d9 {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.34", bfd_dst_mac="00:50:56:60:12:b5"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 b68a61bb-21f7-4087-a26c-a7a22e28e84d
14e66503-b683-4886-a413-e7ecd93ef2e9 {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.39", bfd_dst_mac="00:50:56:64:ae:a6"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 f7700709-fa0a-4141-9254-183060563b96
30c74575-201e-426d-afd9-e65199cd9b02 {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.40", bfd_dst_mac="00:50:56:66:a7:ea"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 45c93b54-a3ea-4d49-9221-4a3ee792c776
54013507-5b76-4a16-b71f-4b8cb71a61b8 {bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c3"} {bfd_dst_ip="192.172.50.41", bfd_dst_mac="00:50:56:66:58:d4"} {enable="true", forwardi
ng_if_rx="true", min_rx="300"} {enabled="true", forwarding="true", remote_state=up, state=up} ef35d1ad-33cb-407f-bee1-1145745e24a4 aa42e10e-0e54-429f-988d-c7afcf51eb27
```

Logs in the F5 console that can be used to examine connectivity.

- /var/log/openvswitch/ovsdb-server.log
- /var/log/vxland.log