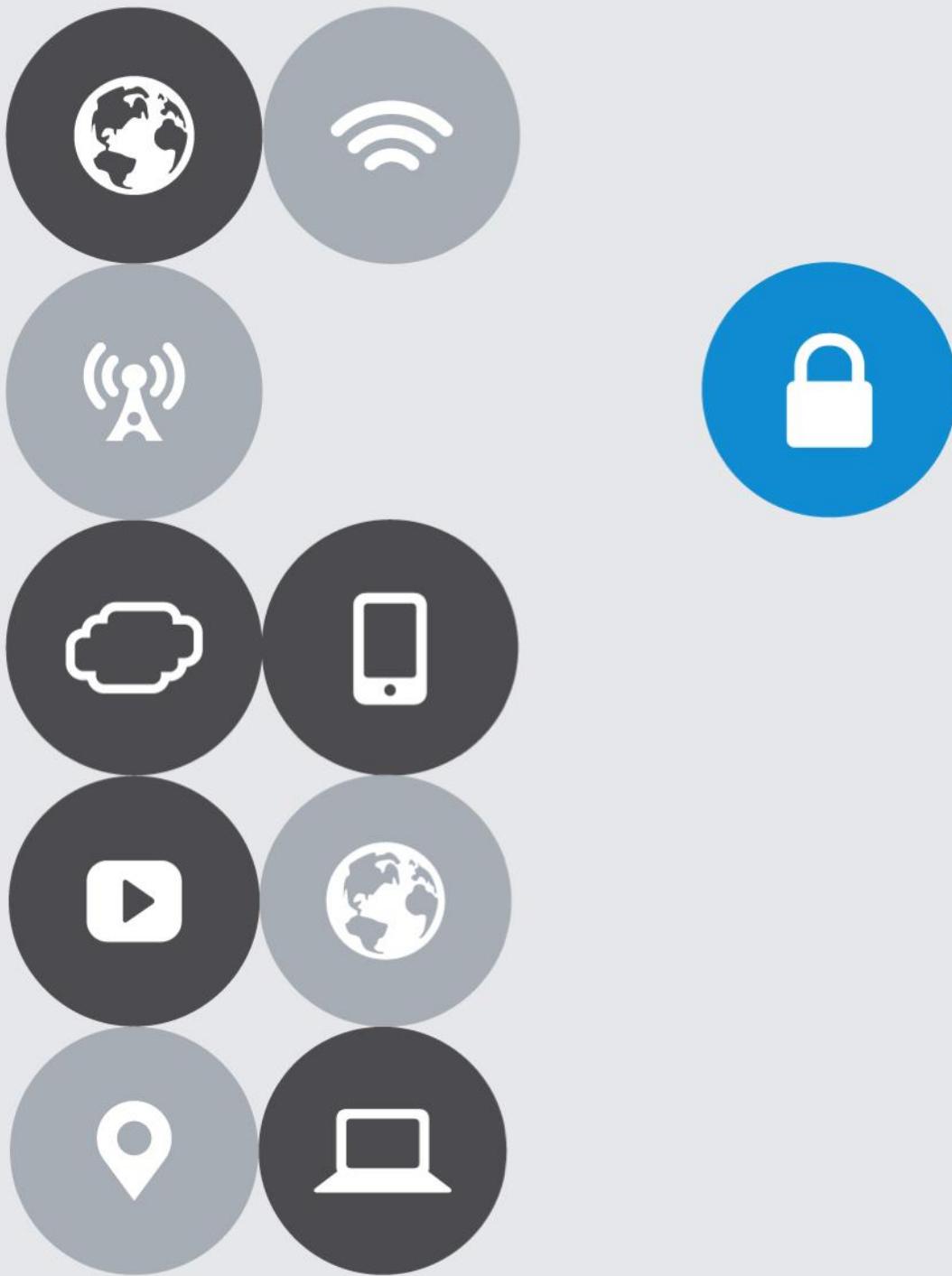




INTEGRATION GUIDE

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

vmware®





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

Version History	2
Introduction.....	5
The Multi-tiered Application	6
Topology 1: Parallel to NSX Edge Using VXLAN Overlays with BIG-IP	7
Traffic Flows	9
Implementation Infrastructure.....	10
Prerequisites	11
Network Segments	12
NSX Edge Configuration	13
Create and Deploy DLR	21
NSX Edge Static Routing Configuration	31
BIG-IP Configuration.....	33
Application Configuration.....	40
Validation	47
Topology 2: Parallel to DLR Using VLANs with BIG-IP	48
Traffic Flows	50
Implementation Infrastructure.....	51
Prerequisites	52
Network Segments	53
Create and Deploy DLR	54
BIG-IP Configuration.....	64
Application Configuration.....	70
Validation	77
Topology 3: One-Arm Connected using VXLAN Overlays with BIG-IP Virtual Edition	78
Traffic Flows	80
Implementation Infrastructure.....	81
Prerequisites	82
Network Segments	83
NSX Edge Configuration	84
Create and Deploy DLR	92
NSX Edge Static Routing Configuration	102
BIG-IP Configuration.....	104
Application Configuration.....	110
Validation	117
Topology 4: OVSDB Integration with NSX-V	118
Traffic Flows	120
Implementation Infrastructure.....	121
Prerequisites	122
Network Segments	123
NSX Edge Configuration	124
BIG-IP Configuration.....	132



Application Configuration.....	161
Validation	168
Troubleshooting	169

INTEGRATION GUIDE

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

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.

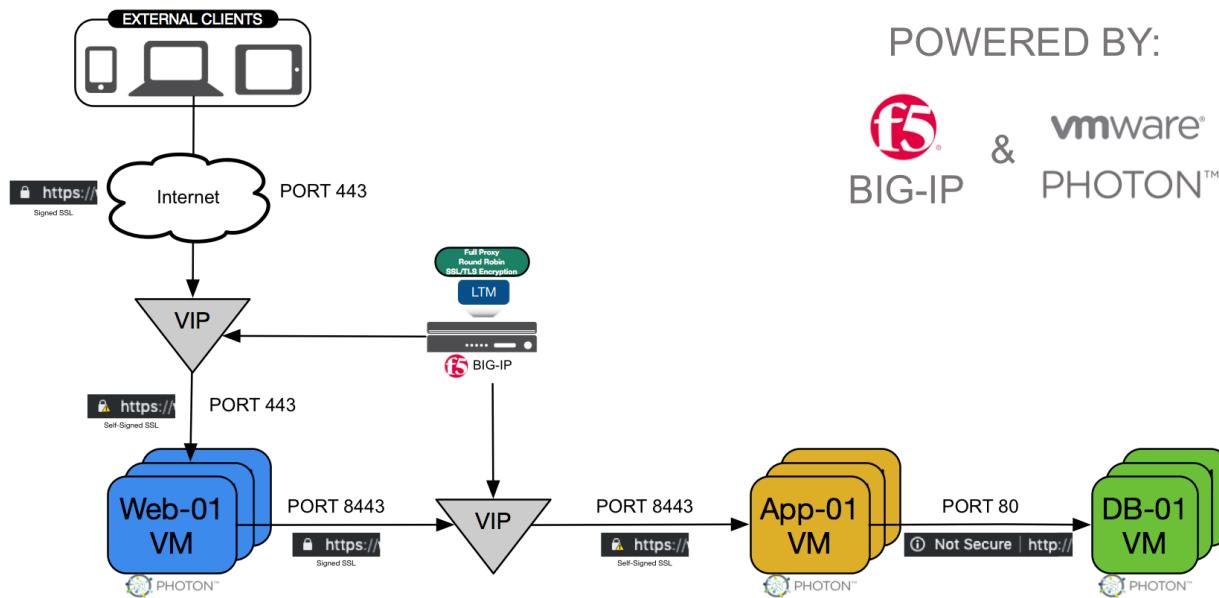
This guide provides configuration guidance, workflows and best practices for the topologies to optimize interoperability between the NSX platform and F5 BIG-IP physical and/or virtual appliances. This guide is intended for customers who would like to adopt the SDDC while ensuring compatibility and minimal disruption to their existing BIG-IP environment.

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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

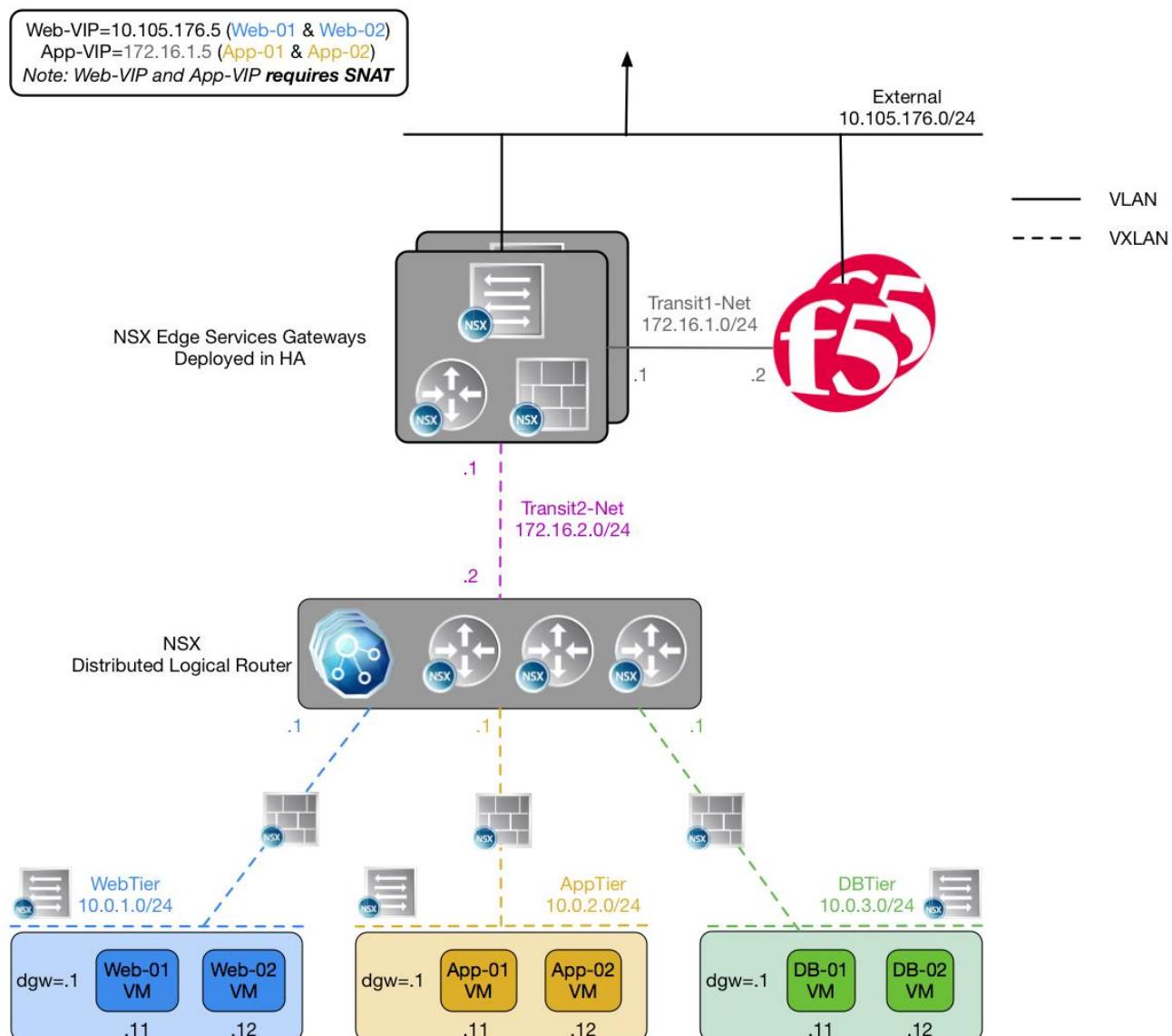


Figure 1 BIG-IP appliance parallel to NSX Edge Services Gateway

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.

INTEGRATION GUIDE

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

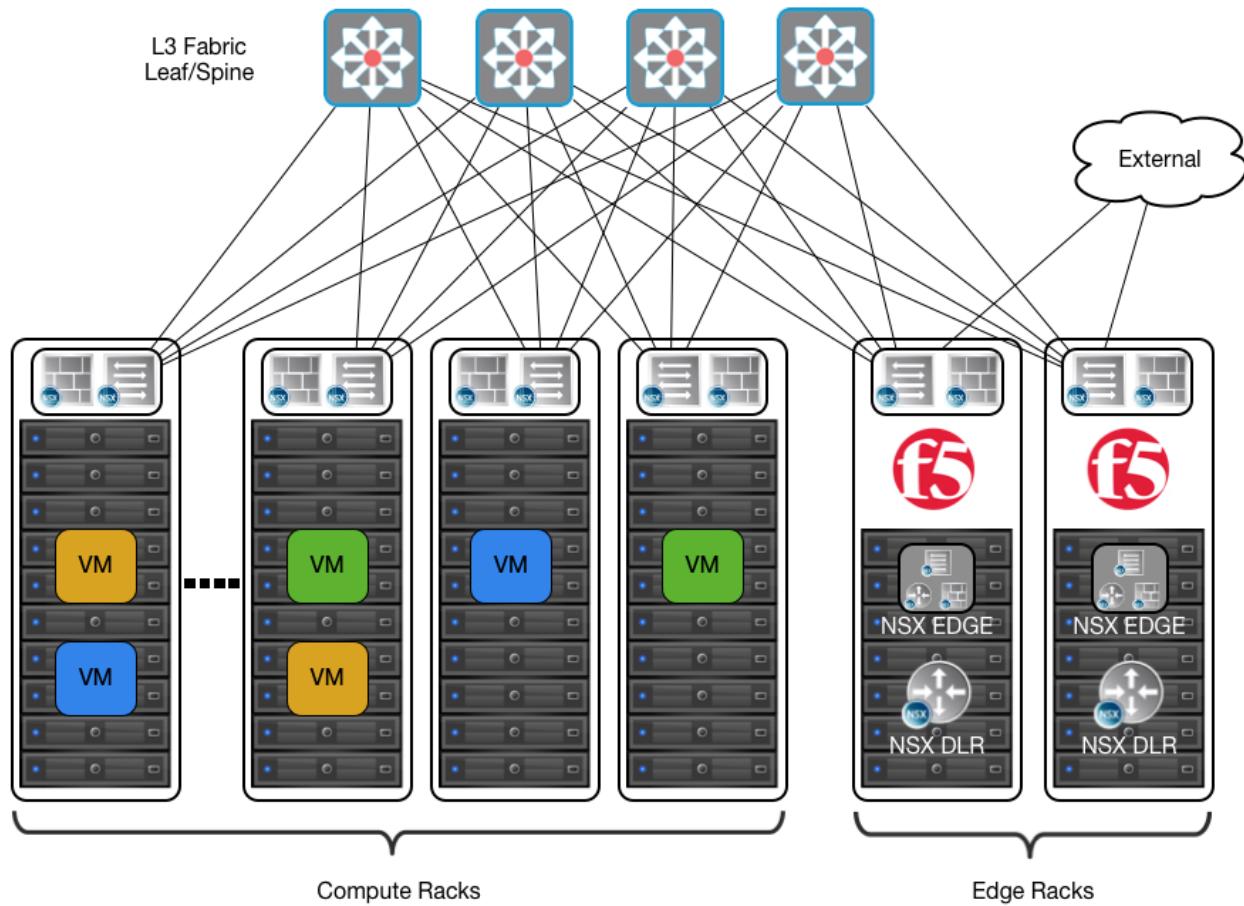


Figure 2 Leaf/spine physical rack infrastructure

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.

INTEGRATION GUIDE

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

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

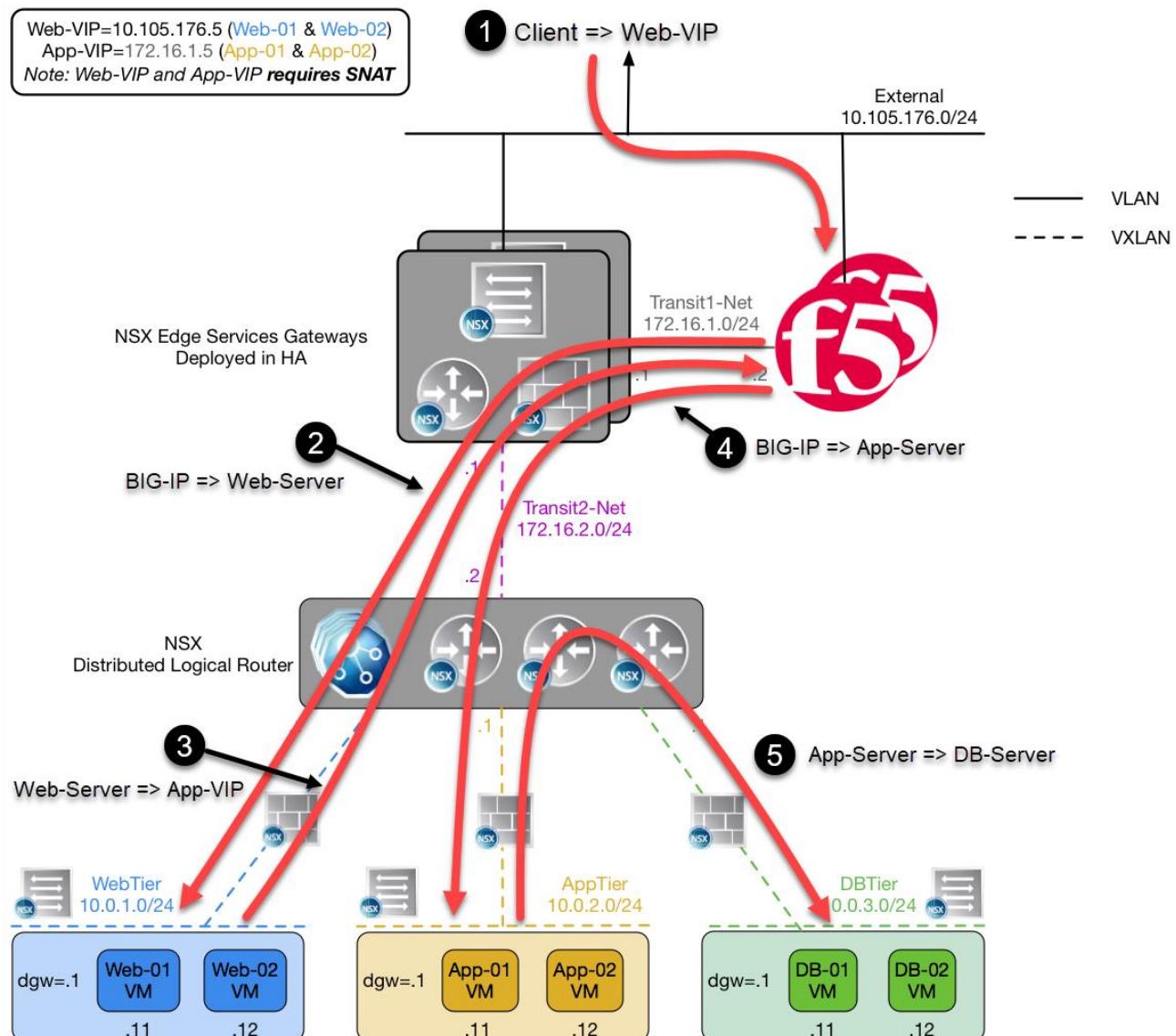


Figure 3 North-South Logical Traffic Flow “Parallel to NSX Edge” with BIG-IP Appliances

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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

INTEGRATION GUIDE

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

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.

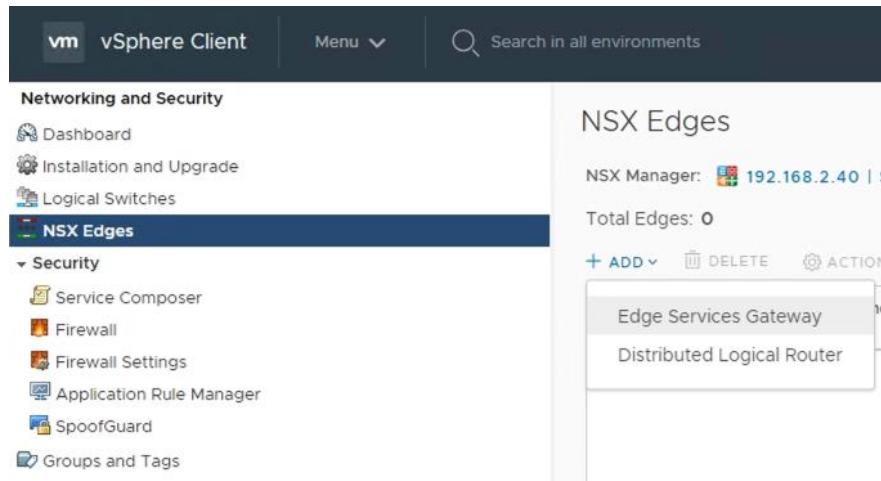
- **VXLAN 5001 WebTier** is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5002 AppTier** is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5003 DBTier**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

INTEGRATION GUIDE

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

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.

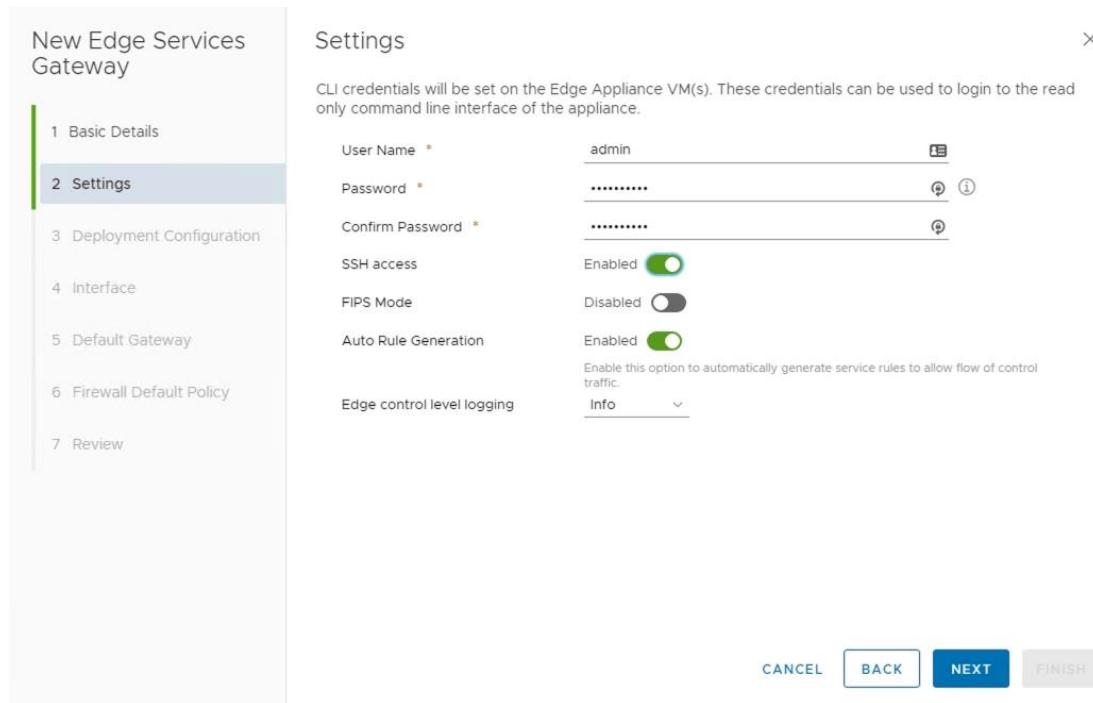
The screenshot shows the "New Edge Services Gateway" configuration wizard with the following steps:

- Left Sidebar:** New Edge Services Gateway, 1 Basic Details (selected), 2 Settings, 3 Deployment Configuration, 4 Interface, 5 Default Gateway, 6 Firewall Default Policy, 7 Review.
- Right Panel (Basic Details):** Title: Basic Details. Description: Edge services gateway provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing. Fields: Name (TOPO1-ESG), Host Name, Tenant, Description.
- Right Panel (Select Deployment Options):** Deploy Edge Appliance VM (checked), Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge. High Availability (unchecked), Enable this option for enabling and configuring High Availability.
- Bottom Buttons:** CANCEL, NEXT (highlighted in blue), FINISH.

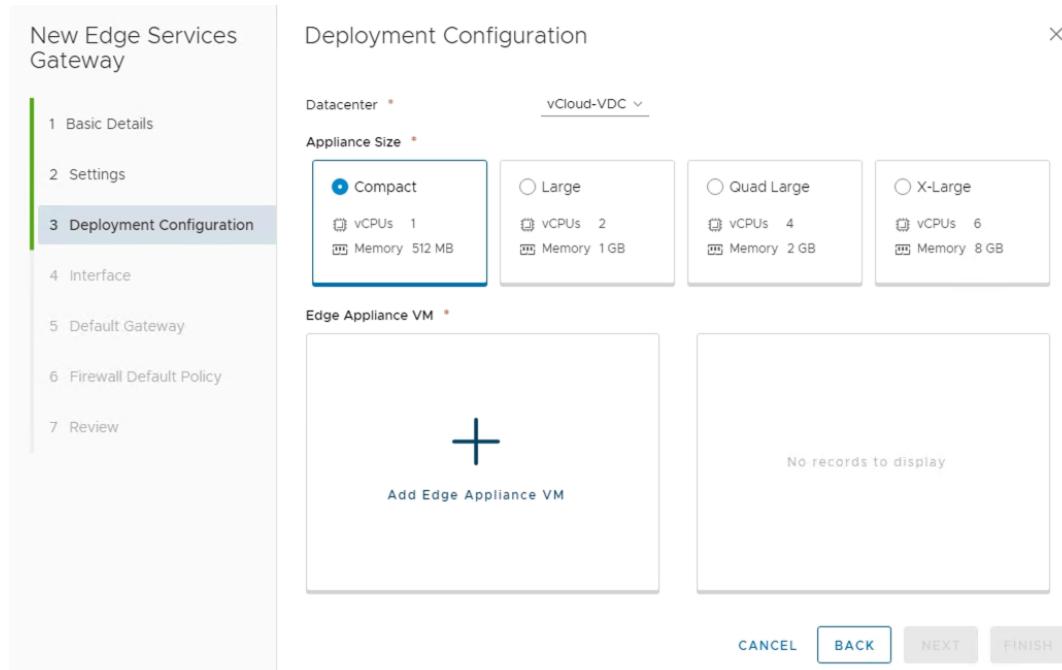
INTEGRATION GUIDE

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

- 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.



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



INTEGRATION GUIDE

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

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.

Add Edge Appliance VM X

Specify placement parameters for the Edge Appliance VM.

Datacenter *	vCloud-VDC
Cluster/Resource Pool *	Cluster1-VDC
Datastore *	QNAP>AllFlash
Host	
Folder	
Resource Reservation	System Managed ①
CPU	1000 MHz
Memory	512 MB

CANCEL ADD

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

New Edge Services Gateway

Configure Interfaces

Configure interfaces of this edge services gateway.

+ ADD EDIT DELETE

vNIC#	Name	Type	IP Address	Connected To
No records to display				

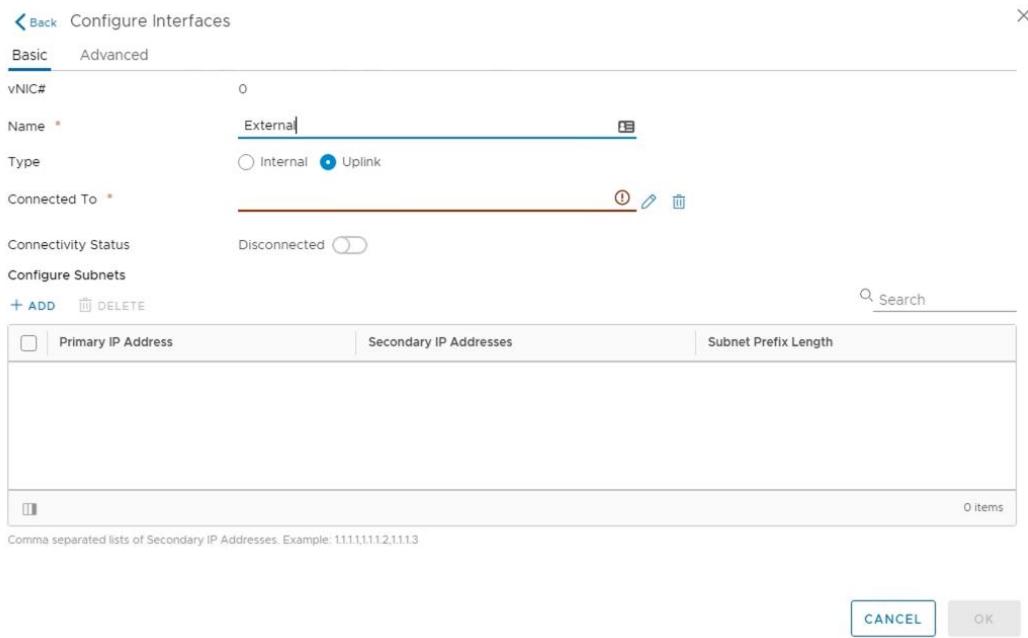
0 items

CANCEL BACK NEXT FINISH

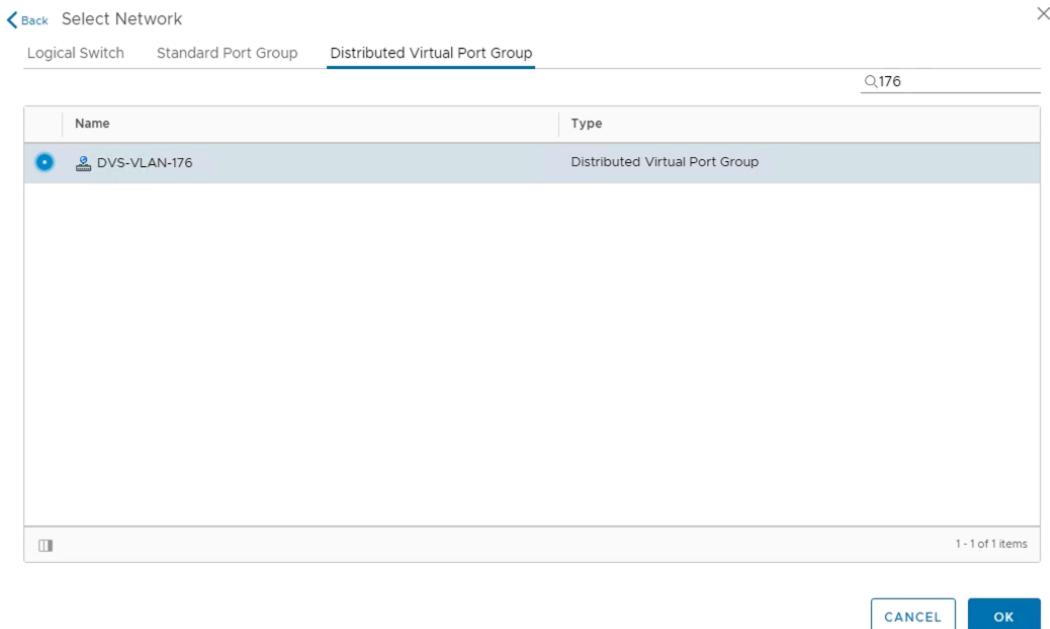
INTEGRATION GUIDE

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

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



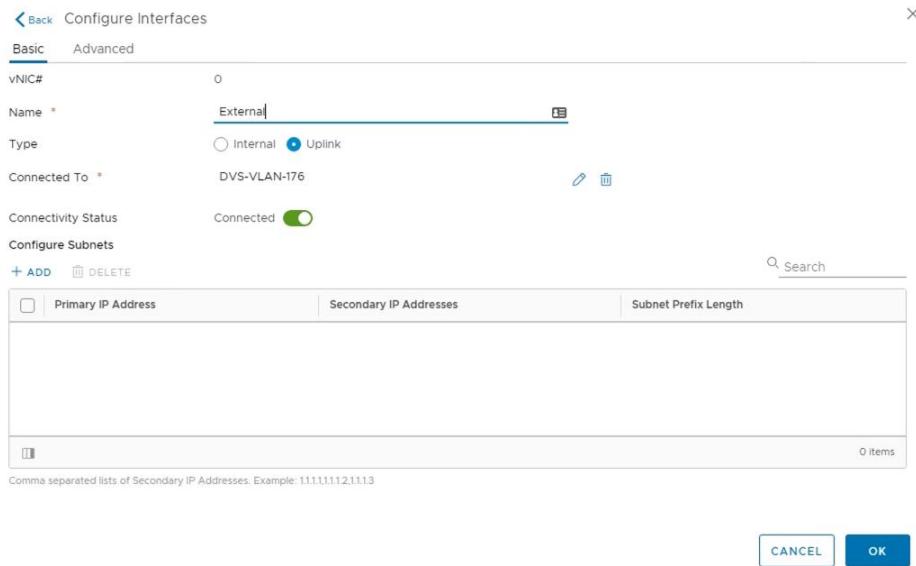
8. For the External network, click on the Distributed Virtual Port Group tab and then selecting the port group used for external access. Click OK.



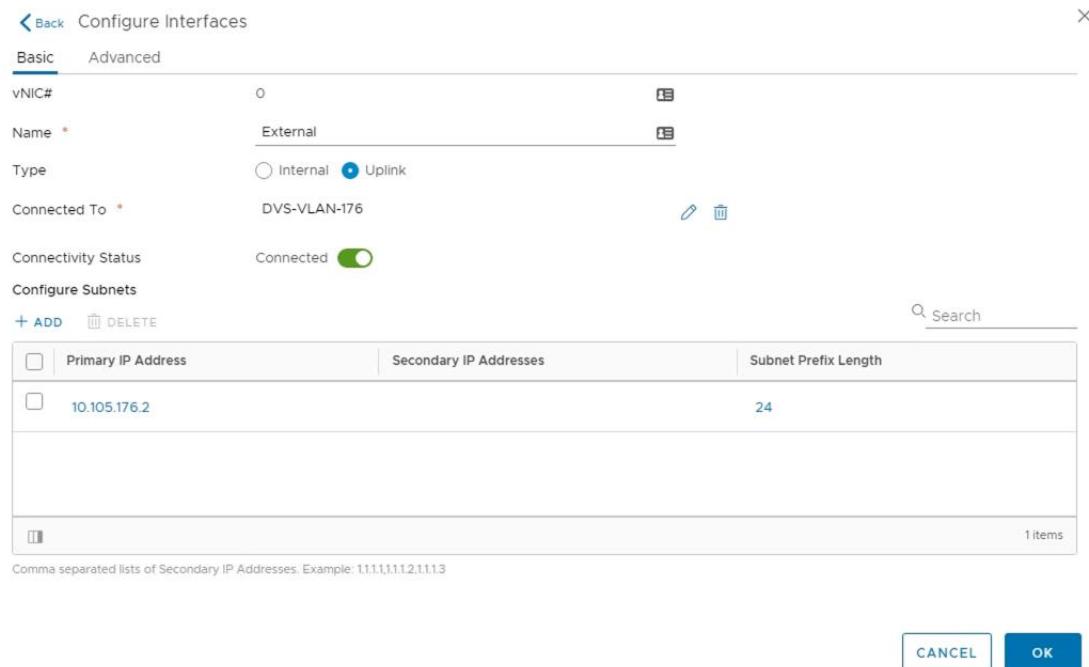
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

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

Configure Interfaces



Configure interfaces of this edge services gateway.

+ ADD EDIT DELETE



vNIC#	Name	Type	IP Address	Connected To
0	External	Uplink	10.105.176.2/24	DVS-VLAN-176
1	TransitNet-1	Uplink	172.16.1.1/24	DVS-VLAN-177
2	TransitNet-2	Internal	172.16.2.1/24	Transit2-Net

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.

New Edge Services Gateway

1 Basic Details

2 Settings

3 Deployment Configuration

4 Interface

5 Default Gateway

6 Firewall Default Policy

7 Review

Default Gateway

Configure Default Gateway

Enabled

vNIC *

Gateway IP *

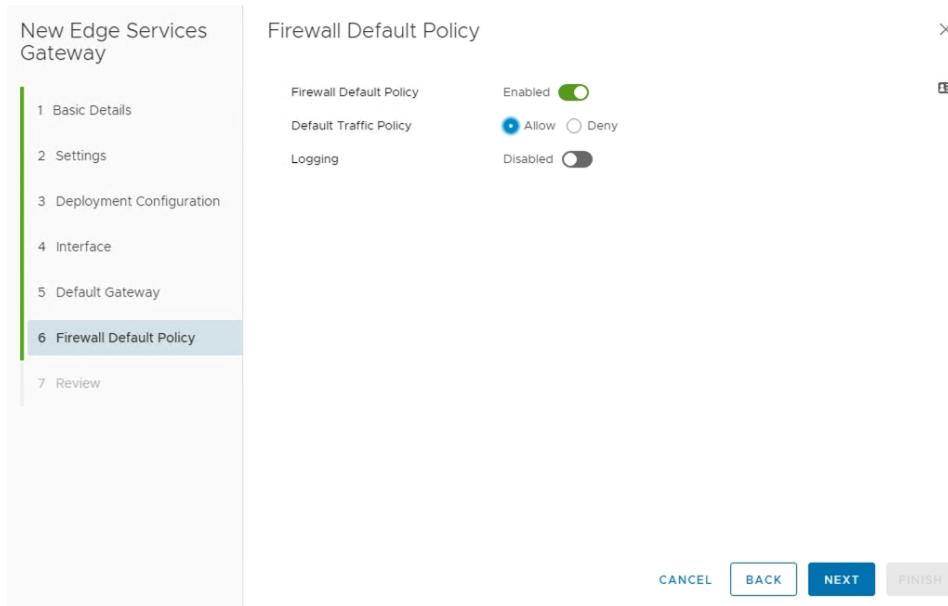
Admin Distance

CANCEL BACK NEXT FINISH

INTEGRATION GUIDE

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

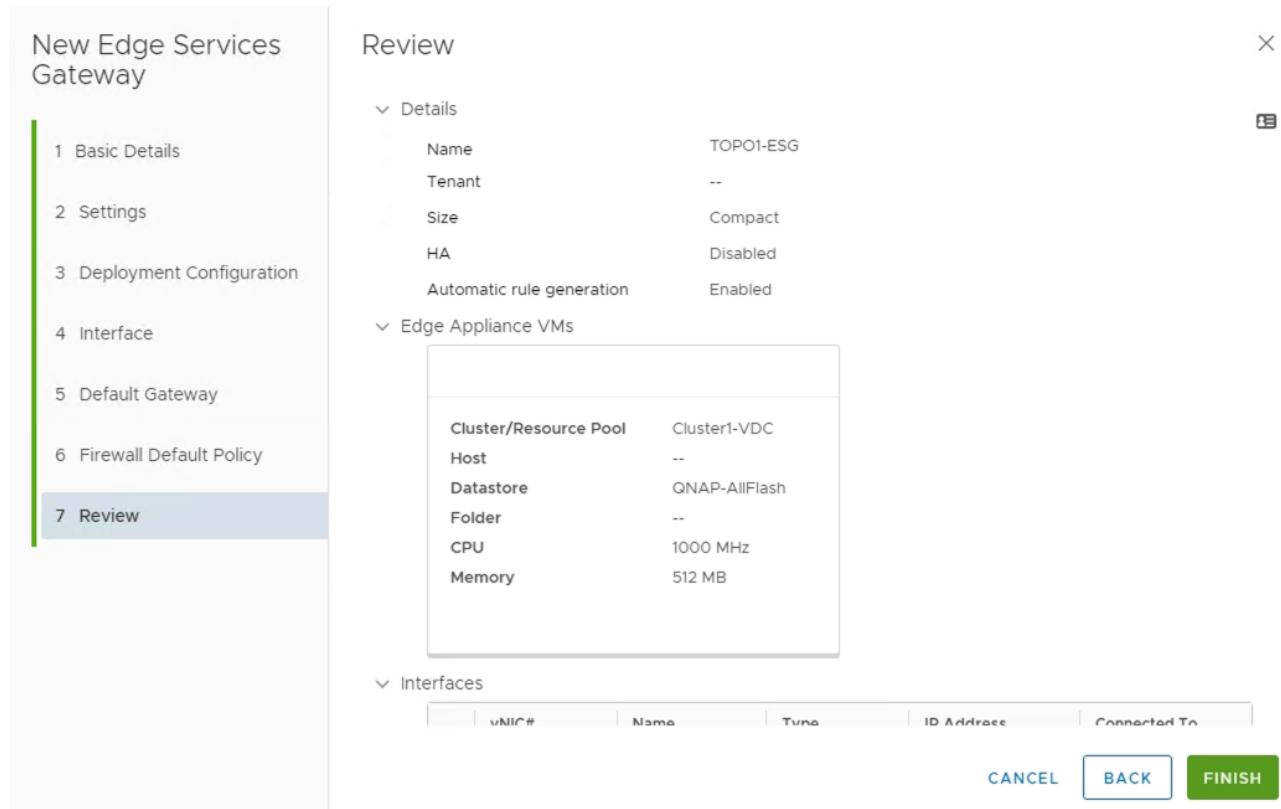
13. HA settings can be left as default. Enable the “Firewall Default Policy” and check Allow for the Default Traffic Policy. (This is for validation testing; firewall can be set to Deny instead however firewall rules will be required on ESG to allow for traffic to flow to/from ESG/DLR and F5).



INTEGRATION GUIDE

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

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).

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	F5 Access	User	172.16.1.2	any	any	Accept
3	WebServer-to-F5-App-VIP	User	10.0.1.11-10.0.1.12	172.16.1.5	any	Accept
4	Default Rule	Default	any	any	any	Deny

INTEGRATION GUIDE

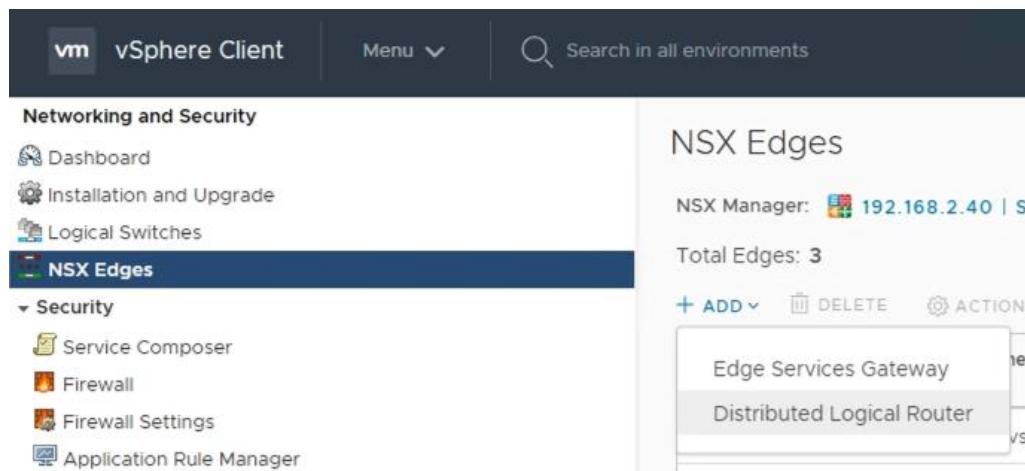
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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”.



INTEGRATION GUIDE

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

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

The screenshot shows the 'Basic Details' step of a wizard titled 'New Distributed Logical Router'. On the left, a vertical navigation bar lists steps 1 through 6. Step 1, 'Basic Details', is selected and highlighted in blue. The main panel displays 'Basic Details' with a descriptive text: 'Distributed logical router provides Distributed Routing and Bridging capabilities.' Below this, there are input fields for 'Name' (set to 'Topo1DLR'), 'Host Name' (empty), 'Tenant' (empty), and 'Description' (empty). A section titled 'Select Deployment Options' contains two checkboxes: 'Deploy Control VMs' (checked) and 'High Availability' (unchecked). Under 'High Availability', there are options for 'HA Logging' (set to 'Disabled') and 'Log Level' (set to 'Info'). At the bottom right are buttons for 'CANCEL', 'NEXT' (highlighted in blue), and 'FINISH'.

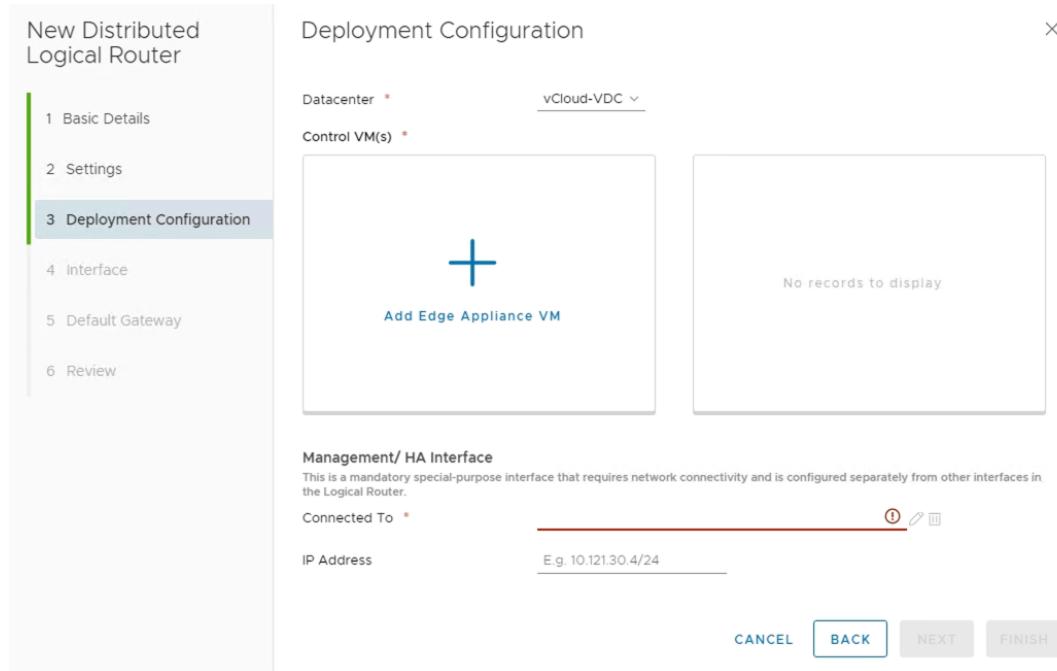
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.

The screenshot shows the 'Settings' step of the wizard. The left navigation bar shows step 2, 'Settings', is selected. The main panel displays settings for the Edge Appliance VM(s). It includes fields for 'User Name' (set to 'admin'), 'Password' (redacted), 'Confirm Password' (redacted), 'SSH access' (set to 'Enabled'), and 'FIPS Mode' (set to 'Disabled'). Below these, there is a dropdown for 'Edge control level logging' set to 'Info'. At the bottom right are buttons for 'CANCEL', 'BACK' (highlighted in blue), 'NEXT', and 'FINISH'.

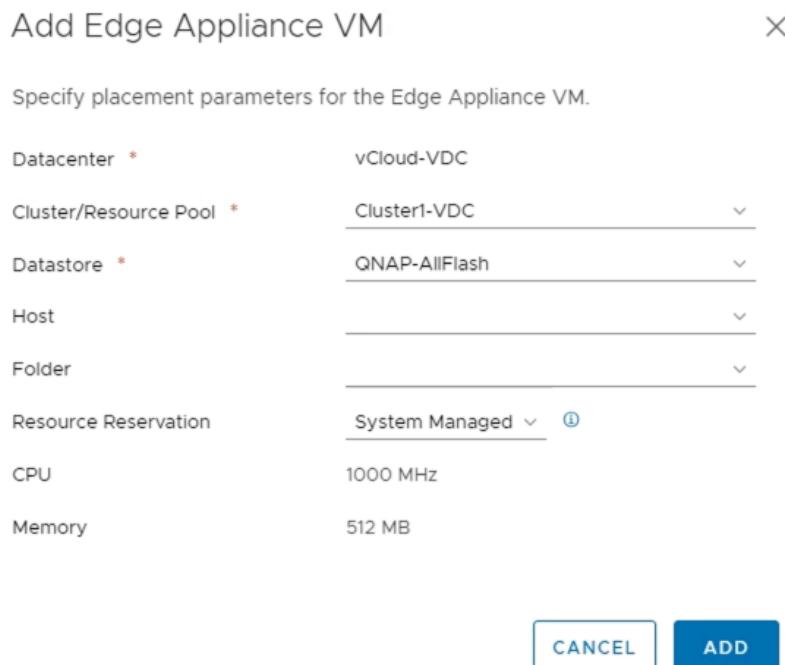
INTEGRATION GUIDE

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

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



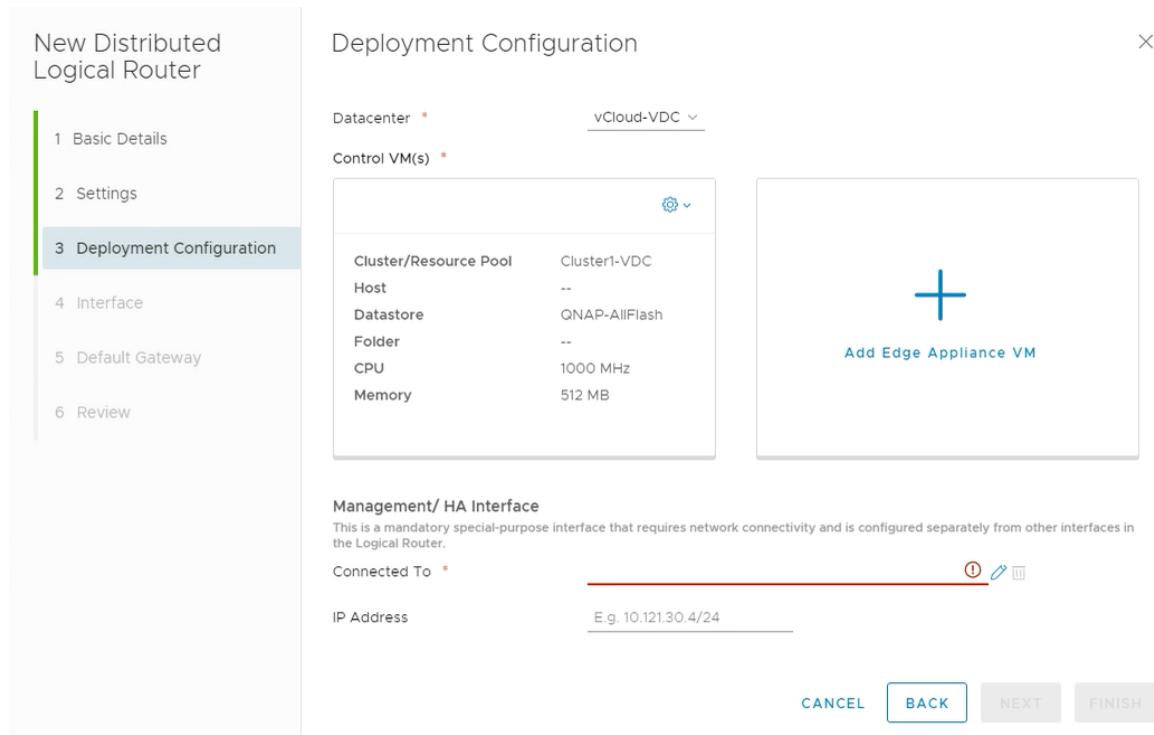
- Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete.



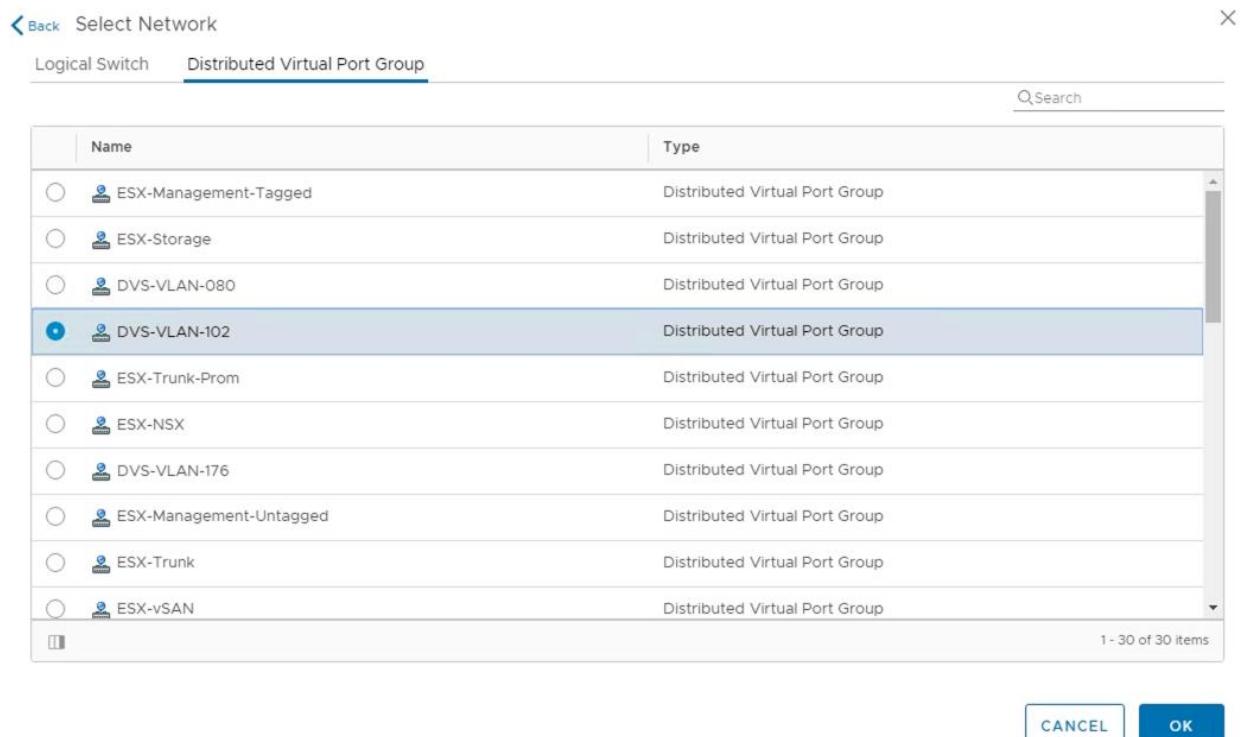
INTEGRATION GUIDE

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

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



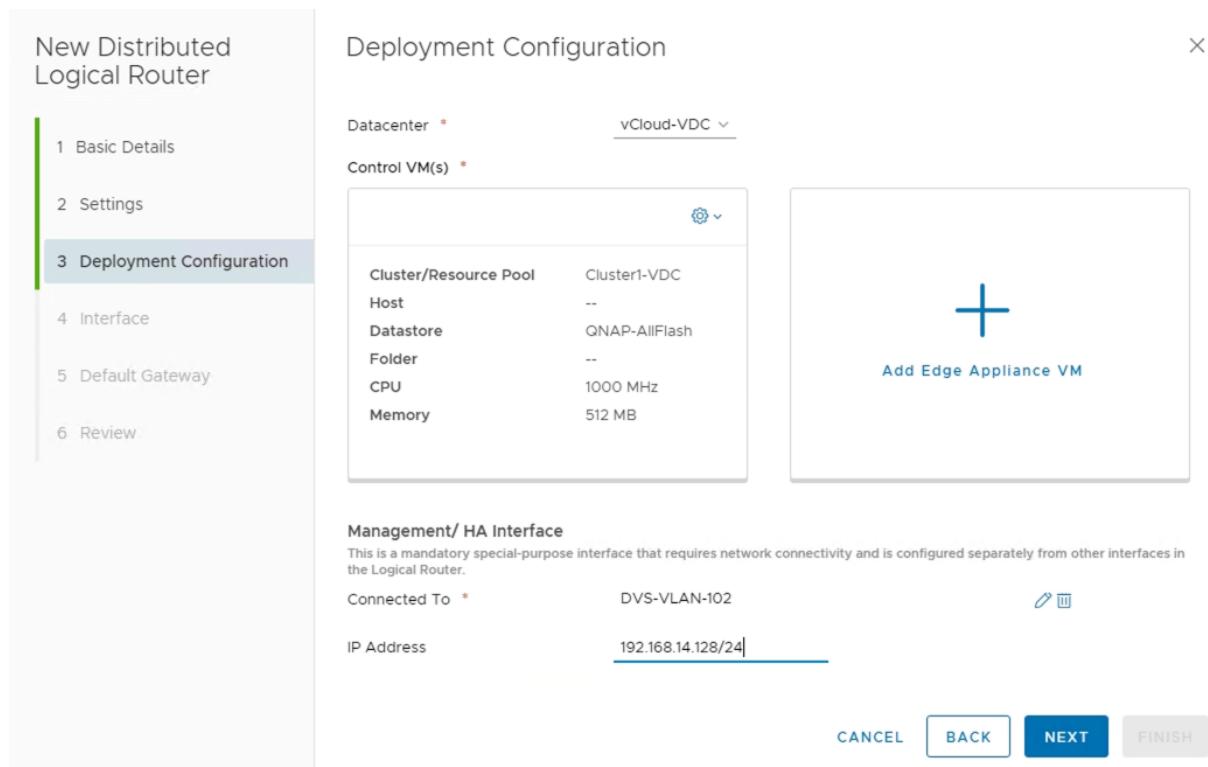
- Select an appropriate Management Network (Distributed Virtual Port Group) to manage the DLR then Click OK.



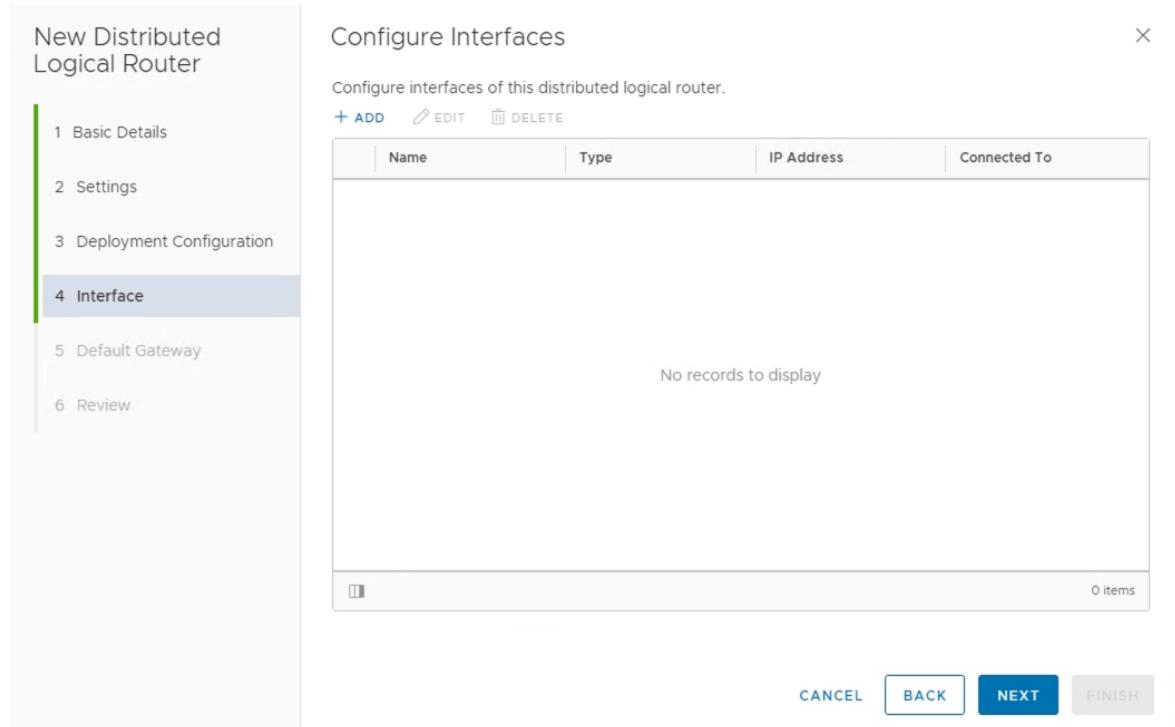
INTEGRATION GUIDE

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

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



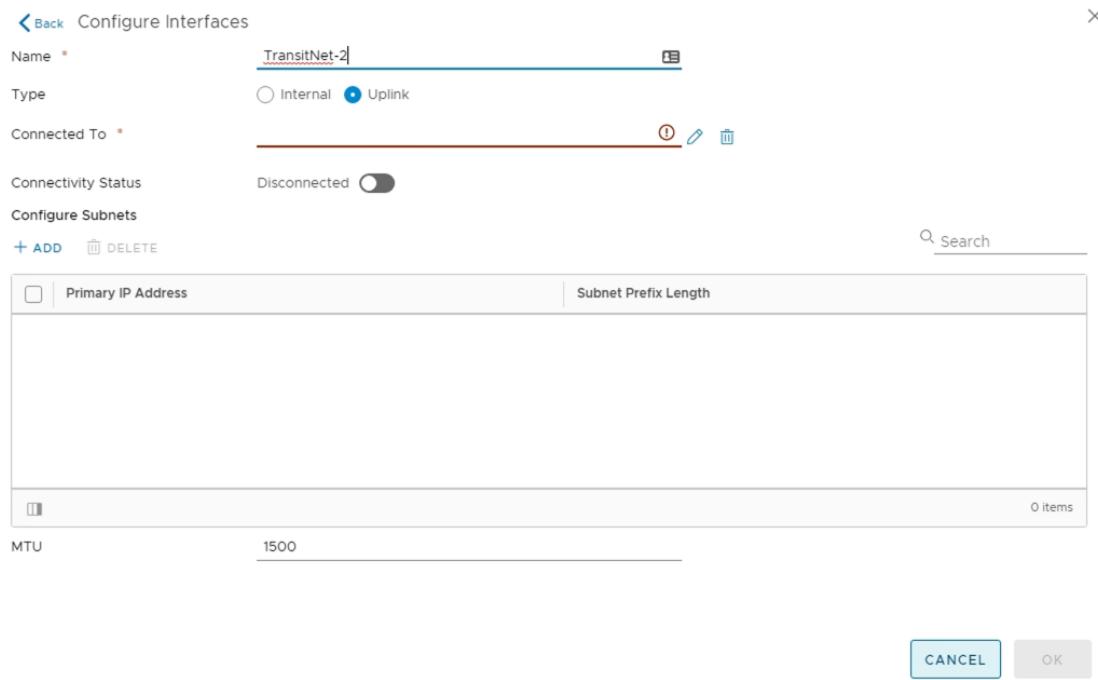
- In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX DLR Interface dialog box.



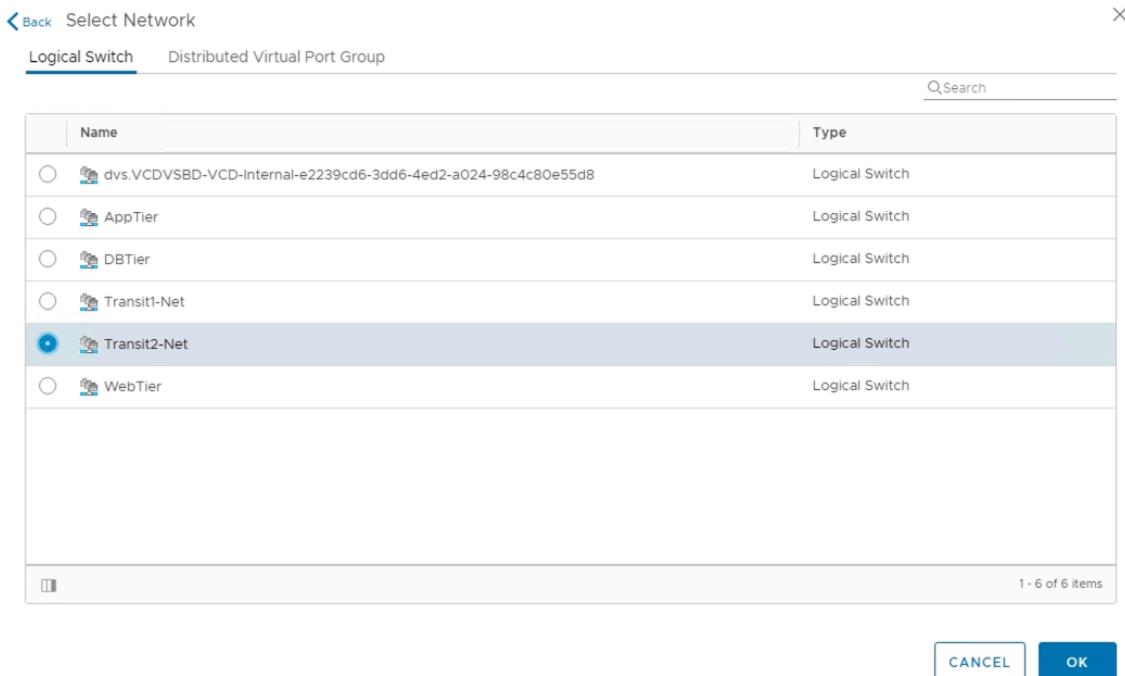
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

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

Configure Interfaces

Name *

Type Internal Uplink

Connected To *

Connectivity Status

Configure Subnets

+ ADD

Search

Primary IP Address	Subnet Prefix Length

MTU

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

Configure Interfaces

Name *

Type Internal Uplink

Connected To *

Connectivity Status

Configure Subnets

+ ADD

Search

Primary IP Address	Subnet Prefix Length
172.16.2.2	24

MTU

INTEGRATION GUIDE

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

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

Configure Interfaces



Configure interfaces of this distributed logical router.

+ ADD **EDIT** **DELETE**

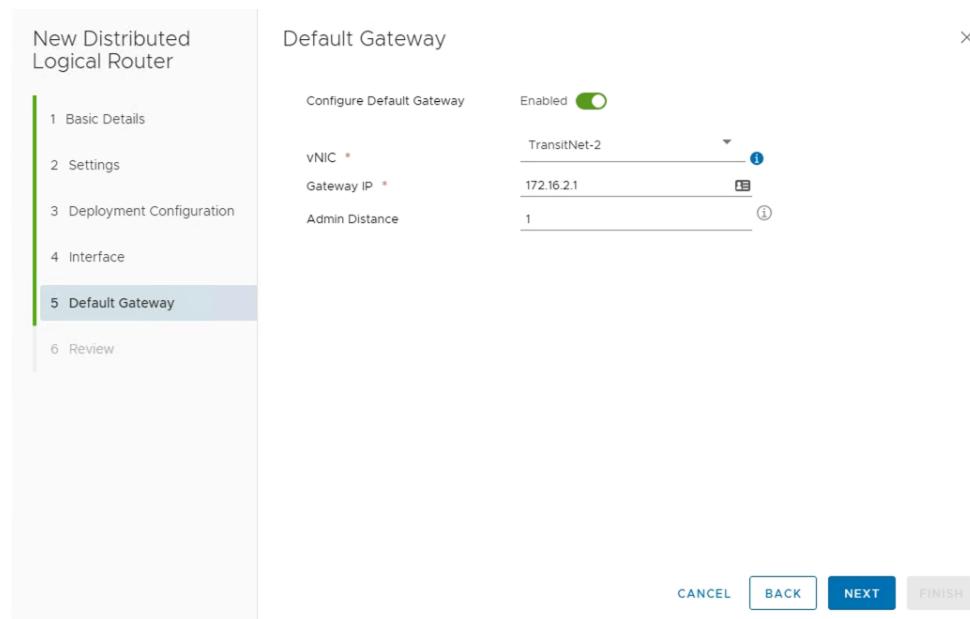
	Name	Type	IP Address	Connected To
<input type="radio"/>	TransitNet-2	Uplink	172.16.2.2/24	Transit2-Net
<input type="radio"/>	WebTier	Internal	10.0.1.1/24	WebTier
<input type="radio"/>	AppTier	Internal	10.0.2.1/24	AppTier
<input type="radio"/>	DBTier	Internal	10.0.3.1/24	DBTier

INTEGRATION GUIDE

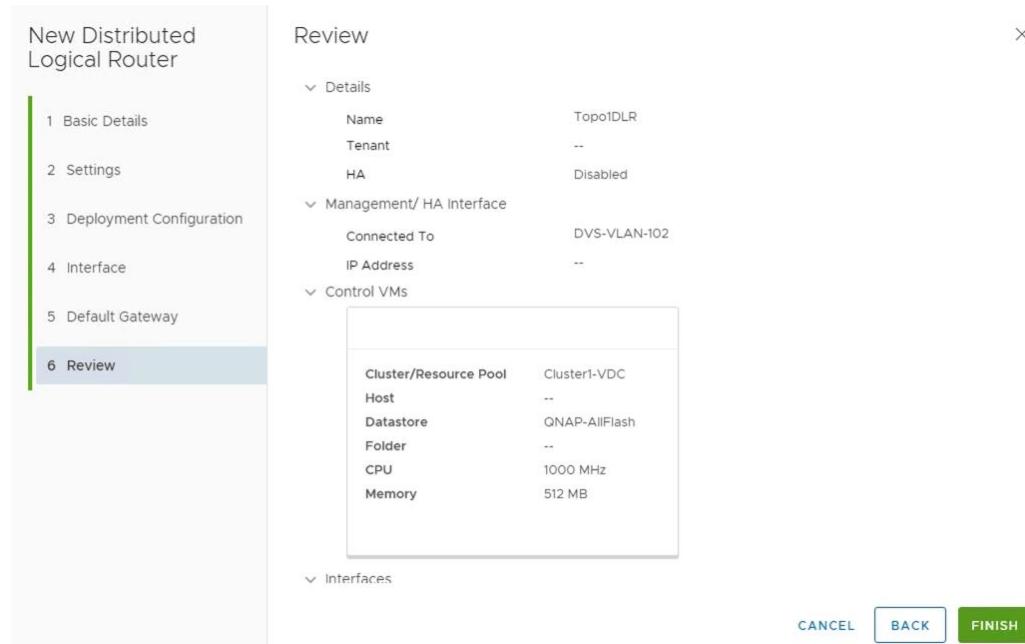
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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.



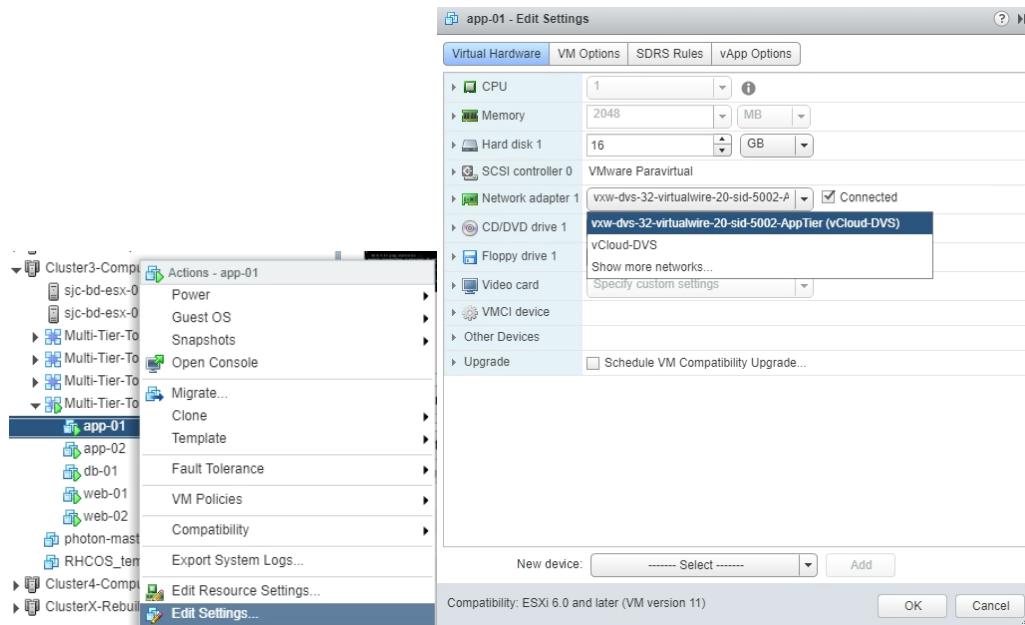
16. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

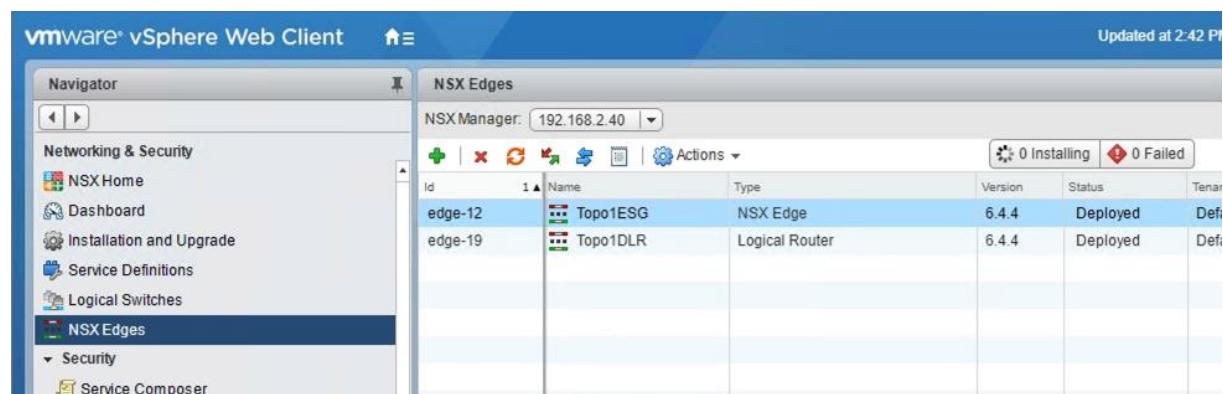
NSX Edge Static Routing Configuration

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.

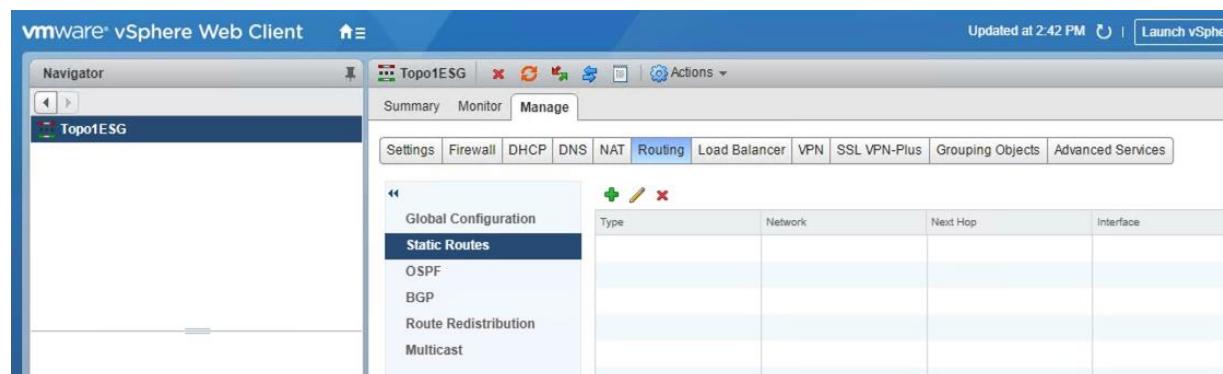
1. In the vSphere Client console, begin by navigating to Networking & Security in the “Menu” selection under Networking and Security, choose NSX Edges and then Double-click on the NSX Edge you configured in the first section. (In our use case this was named Topo1ESG).

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



The screenshot shows the vSphere Web Client interface. The left sidebar has a 'Navigator' section with links like NSX Home, Dashboard, Installation and Upgrade, Service Definitions, Logical Switches, NSX Edges (which is selected and highlighted in blue), and Security. The main content area is titled 'NSX Edges' and shows a table of edges. The table has columns for Id, Name, Type, Version, Status, and Tenant. There are two entries: 'edge-12' (Type: NSX Edge, Name: Topo1ESG, Version: 6.4.4, Status: Deployed, Tenant: Default) and 'edge-19' (Type: Logical Router, Name: Topo1DLR, Version: 6.4.4, Status: Deployed, Tenant: Default). A toolbar at the top of the table includes icons for add, delete, search, and actions.

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.

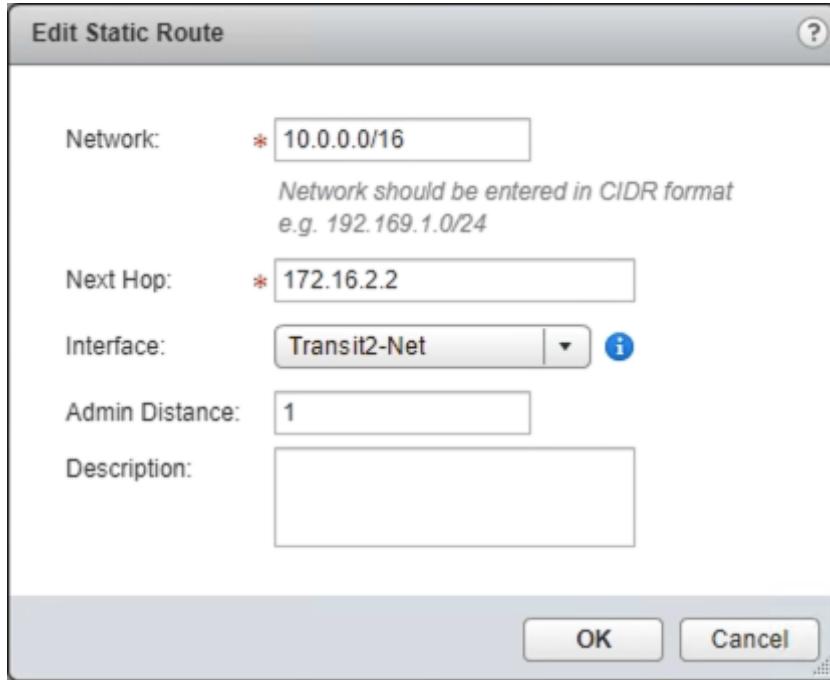


The screenshot shows the configuration screen for the 'Topo1ESG' NSX Edge. The left sidebar shows 'Topo1ESG'. The main navigation tabs are Summary, Monitor, and Manage (which is selected). Under Manage, there are sub-tabs: Settings, Firewall, DHCP, DNS, NAT, Routing (which is selected and highlighted in blue), Load Balancer, VPN, SSL VPN-Plus, Grouping Objects, and Advanced Services. On the left, a sidebar lists Global Configuration options: OSPF, BGP, Route Redistribution, and Multicast. The main content area is titled 'Static Routes' and contains a table with columns: Type, Network, Next Hop, and Interface. There are four empty rows in the table.

INTEGRATION GUIDE

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

- 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.



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

The screenshot shows the F5 BIG-IP Management Interface under the 'Manage' tab. The 'Routing' tab is selected. On the left, the 'Static Routes' section is highlighted. A message at the top right says: "Changes to the Static Routing configuration will take effect only after being published. Please click on 'Publish Changes' to publish." Below this are 'Publish Changes' and 'Revert Changes' buttons. The main pane displays a table of static routes:

Type	Network	Next Hop	Interface	Admin Distance	Desc
user	10.0.0.0/16	172.16.2.2	Transit2-Net	1	

INTEGRATION GUIDE

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

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.

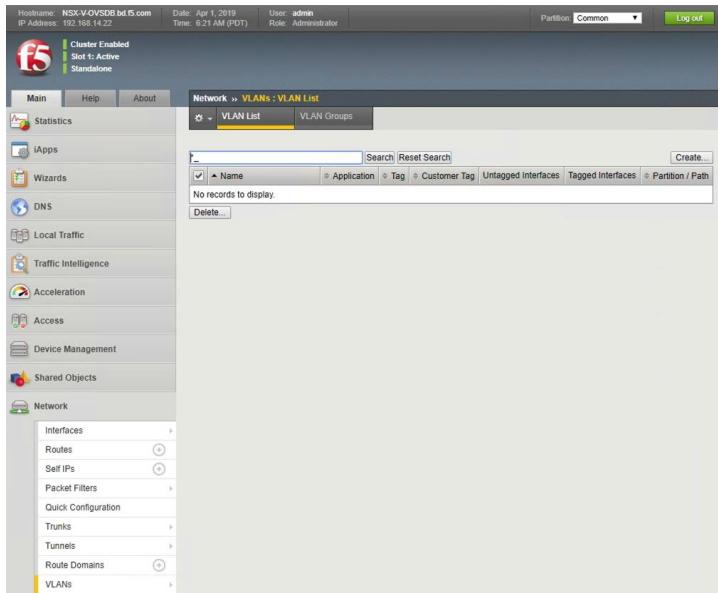
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

INTEGRATION GUIDE

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

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

A screenshot of the 'New VLAN...' configuration dialog. The dialog is divided into several sections:

- General Properties:** Name is set to 'External', Description is empty, and Tag is set to '176'.
- Resources:** Under 'Interfaces', Interface is set to '1.2' and Tagging is set to 'Tagged'. An 'Add' button is visible, and the list shows '1.1 (tagged)'.
- Configuration:** Configuration mode is set to 'Basic'. Source Check is unchecked, and MTU is set to '1500'.
- sFlow:** Polling Interval and Sampling Rate are both set to 'Default'.

At the bottom of the dialog are three buttons: 'Cancel', 'Repeat', and 'Finished'.

INTEGRATION GUIDE

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

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.

The screenshot shows the 'New VLAN...' configuration dialog box. It has several sections:

- General Properties:** Name: TransitNet-1, Description: (empty), Tag: 177.
- Resources:** Interfaces: A list box containing '1.1 (tagged)' with an 'Add' button above it. Below the list box are 'Edit' and 'Delete' buttons.
- Configuration:** Configuration dropdown set to 'Basic'. Source Check: checked, MTU: 1500.
- sFlow:** Polling Interval: Default, Sampling Rate: Default.
- Buttons:** Cancel, Repeat, Finished.

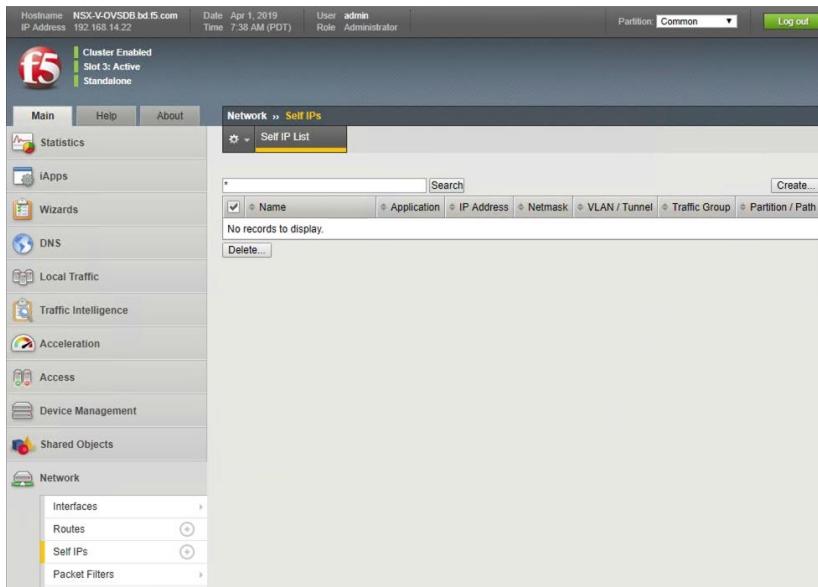
INTEGRATION GUIDE

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

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

Network > Self IPs > New Self IP...

Configuration	
Name	External-Self-IP <input style="width: 20px; height: 20px;" type="button" value="..."/>
IP Address	10.105.176.10
Netmask	255.255.255.0
VLAN / Tunnel	External <input style="width: 20px; height: 20px;" type="button" value="..."/>
Port Lockdown	Allow None <input style="width: 20px; height: 20px;" type="button" value="..."/>
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating) <input style="width: 20px; height: 20px;" type="button" value="..."/>
Service Policy	None <input style="width: 20px; height: 20px;" type="button" value="..."/>

INTEGRATION GUIDE

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

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.

The screenshot shows the 'New Self IP...' configuration dialog. It has a title bar 'Network > Self IPs > New Self IP...'. The main area is titled 'Configuration' and contains the following fields:

Name	Transit-Self-IP
IP Address	172.16.1.2
Netmask	255.255.255.0
VLAN / Tunnel	TransitNet-1
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

At the bottom are three buttons: 'Cancel', 'Repeat', and 'Finished'.

The screenshot shows the 'Self IP List' table. The title bar is 'Network > Self IPs' with a 'Self IP List' tab selected. The table has columns: Name, Application, IP Address, Netmask, VLAN / Tunnel, Traffic Group, and Partition / Path. There are two entries:

Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
External-Self-IP		10.105.176.10	255.255.255.0	External	traffic-group-local-only	Common
Transit-Self-IP		172.16.1.2	255.255.255.0	TransitNet-1	traffic-group-local-only	Common

At the bottom left is a 'Delete...' button.

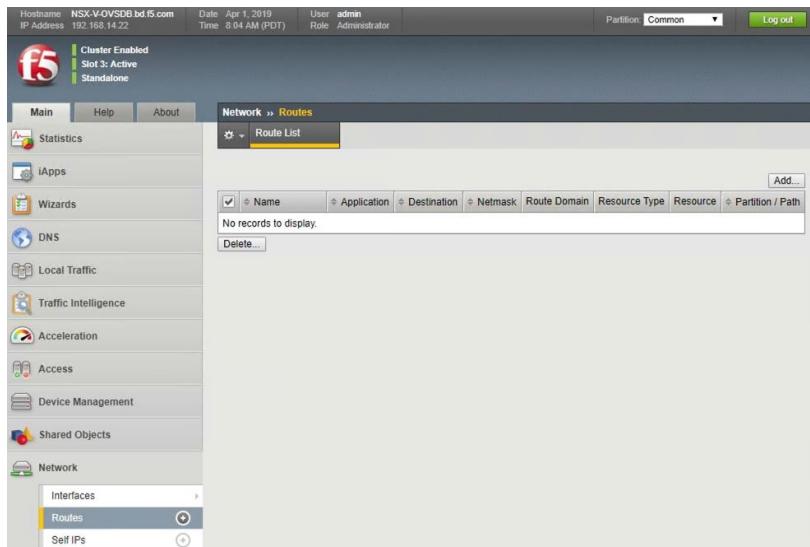
INTEGRATION GUIDE

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

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

A screenshot of the 'New Route...' configuration dialog. The title bar says 'Network > Routes > New Route...'. The main area is titled 'Properties' and contains the following fields:

Name	default
Description	(empty)
Destination	0.0.0.0
Netmask	0.0.0.0
Resource	Use Gateway...
Gateway Address	IP Address: 10.105.176.1
MTU	(empty)

At the bottom of the dialog are three buttons: 'Cancel', 'Repeat', and 'Finished'.

INTEGRATION GUIDE

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

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.

The screenshot displays two windows from the VMware NSX interface:

New Route... Properties

Properties	
Name	ServerRoutes
Description	(empty)
Destination	10.0.0.0
Netmask	255.255.0.0
Resource	Use Gateway...
Gateway Address	IP Address 172.16.1.1
MTU	(empty)

Route List

<input checked="" type="checkbox"/>	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
<input checked="" type="checkbox"/>	ServerRoutes		10.0.0.0	255.255.0.0	Partition Default Route Domain	Gateway	172.16.1.1	Common
<input type="checkbox"/>	default		Default IPv4		Partition Default Route Domain	Gateway	10.105.176.1	Common

INTEGRATION GUIDE

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

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

INTEGRATION GUIDE

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

Local Traffic > Pools : Pool List > New Pool...

Configuration: Basic ▾

Name	WebServerPool				
Description					
Health Monitors	<table border="1"><tr><td>Active</td><td>Available</td></tr><tr><td>/Common gateway_icmp</td><td>/Common http http_head_f5 https https_443</td></tr></table>	Active	Available	/Common gateway_icmp	/Common http http_head_f5 https https_443
Active	Available				
/Common gateway_icmp	/Common http http_head_f5 https https_443				

Resources

Load Balancing Method	Round Robin															
Priority Group Activation	Disabled															
New Members	<p><input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node</p> <p>Node Name: <input type="text"/> (Optional)</p> <p>Address: <input type="text" value="10.0.1.12"/></p> <p>Service Port: <input type="text" value="443"/> <input type="button" value="HTTPS"/></p> <p><input type="button" value="Add"/></p> <table border="1"><thead><tr><th>Node Name</th><th>Address/FQDN</th><th>Service Port</th><th>Auto Populate</th><th>Priority</th></tr></thead><tbody><tr><td>10.0.1.11</td><td>10.0.1.11</td><td>443</td><td></td><td>0</td></tr><tr><td>10.0.1.12</td><td>10.0.1.12</td><td>443</td><td></td><td>0</td></tr></tbody></table> <p><input type="button" value="Edit"/> <input type="button" value="Delete"/></p>	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
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												

INTEGRATION GUIDE

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

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

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.0.1.11	10.0.1.11	8443	0	0
10.0.1.12	10.0.1.12	8443	0	0

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.

Local Traffic > Pools : Pool List					
Status		Name	Description	Application	Members
<input checked="" type="checkbox"/>	AppServerPool				2 Common
<input checked="" type="checkbox"/>	WebServerPool				2 Common

INTEGRATION GUIDE

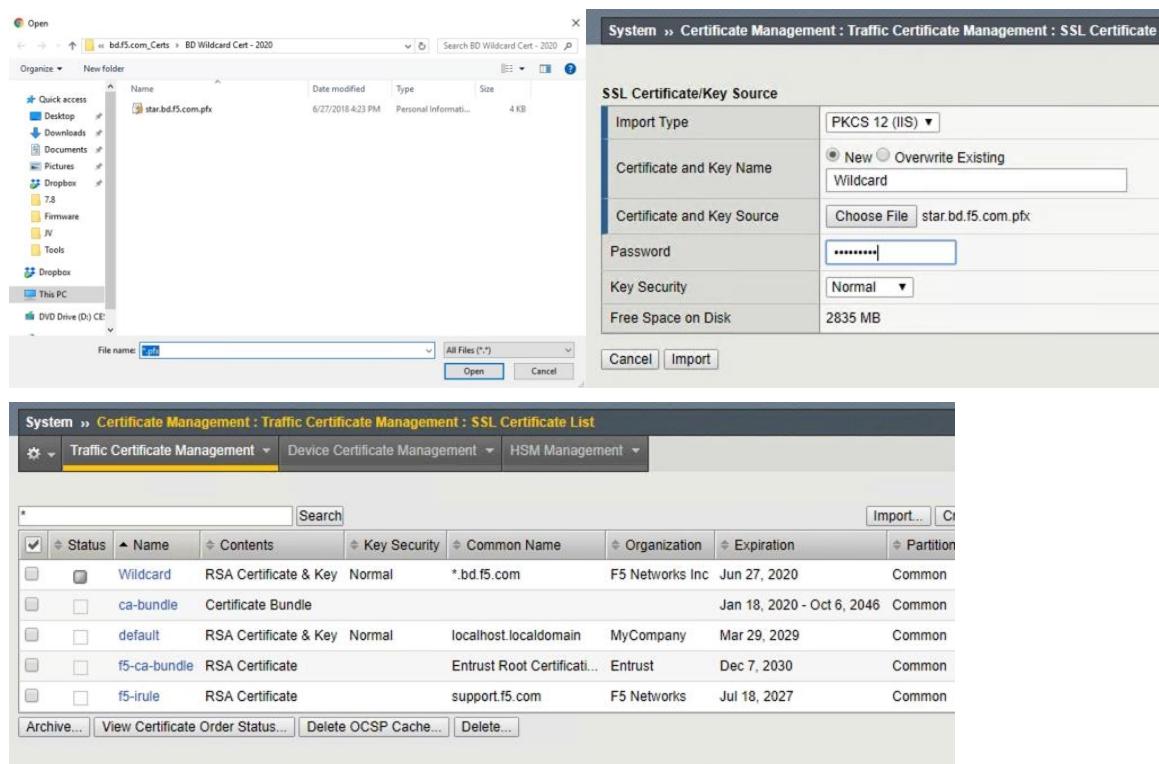
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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



INTEGRATION GUIDE

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

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.

The screenshot shows three windows related to creating a ClientSSL profile:

- Top Window: General Properties**

Name	WildcardSSL
Parent Profile	clientssl

Configuration: Basic Custom

Certificate Key Chain (List View):

 - Add
 - Edit
 - Delete
- Middle Window: Add SSL Certificate Key Chain**

Certificate	Wildcard
Key	Wildcard
Chain	Wildcard
Passphrase	<input type="text"/>

Add Cancel
- Bottom Window: General Properties (Final State)**

Name	WildcardSSL
Parent Profile	clientssl

Configuration: Basic Custom

Certificate Key Chain (List View): /Common/Wildcard /Common/Wildcard /Common/Wildcard

OCSP Stapling

INTEGRATION GUIDE

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

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

The screenshot shows the configuration interface for creating a new virtual server. The General Properties tab is active, showing the basic settings for the virtual server. The Resources tab is also visible, showing the assigned iRules and policies. The main configuration pane on the right lists various protocol and SSL profiles, with specific ones selected for the client and server sides. The SSL Profile (Client) section shows 'WildcardSSL' selected, and the SSL Profile (Server) section shows 'serverssl-insecure-compatible' selected. Other configuration options like HTTP, FTP, and RTSP profiles are also listed.

INTEGRATION GUIDE

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

4. In the New Virtual Server menus

- In the Name field, provide a unique name for the web application. In this case, we used App-VIP.
- In the Destination Address field, enter 172.16.1.5
- For Service Port use the standard HTTPS port 8443.
- In the Configuration section
 - Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
 - Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
 - Select Auto Map from the pull-down menus for the Source Address Translation.
- In the Resources section
 - Select the AppServerPool from the Default Pool dropdown box.
 - 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.
- 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.

	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input checked="" type="checkbox"/>	●	App-VIP			172.16.1.5	8443	Standard	Edit...	Common
<input type="checkbox"/>	●	Web-VIP			10.105.176.5	443 (HTTPS)	Standard	Edit...	Common

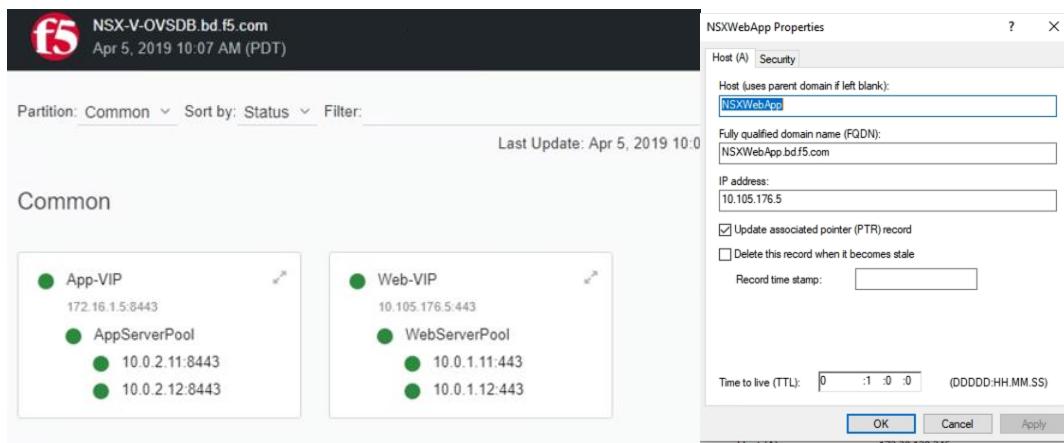
INTEGRATION GUIDE

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

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.

The screenshot shows a web browser displaying the 'Customer Database Access' page from the F5 BIG-IP. The page lists companies and their revenue. Below the browser is a terminal window showing the results of a curl command. The curl command output shows the response headers and body, including the 'X-Upstream-Server' header which indicates the web server used for the request.

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

```
< Connection: keep-alive
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< X-Upstream-Server: web-01
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host nsxwebapp.bd.f5.com left intact
[mmabis@hzn-lin-mmabis ~]$ 
```

```
< Connection: keep-alive
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< X-Upstream-Server: web-02
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host nsxwebapp.bd.f5.com left intact
[mmabis@hzn-lin-mmabis ~]$ 
```

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

INTEGRATION GUIDE

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

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

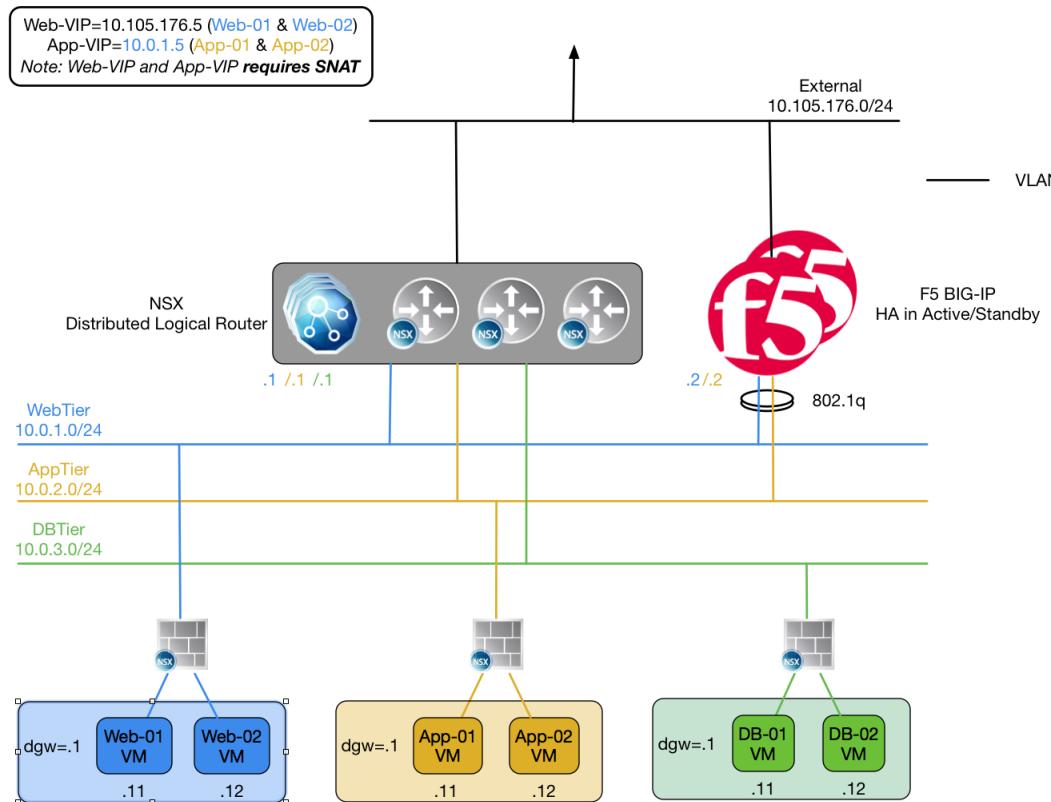


Figure 5 BIG-IP appliance parallel to NSX Distributed Logical Router

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.

INTEGRATION GUIDE

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

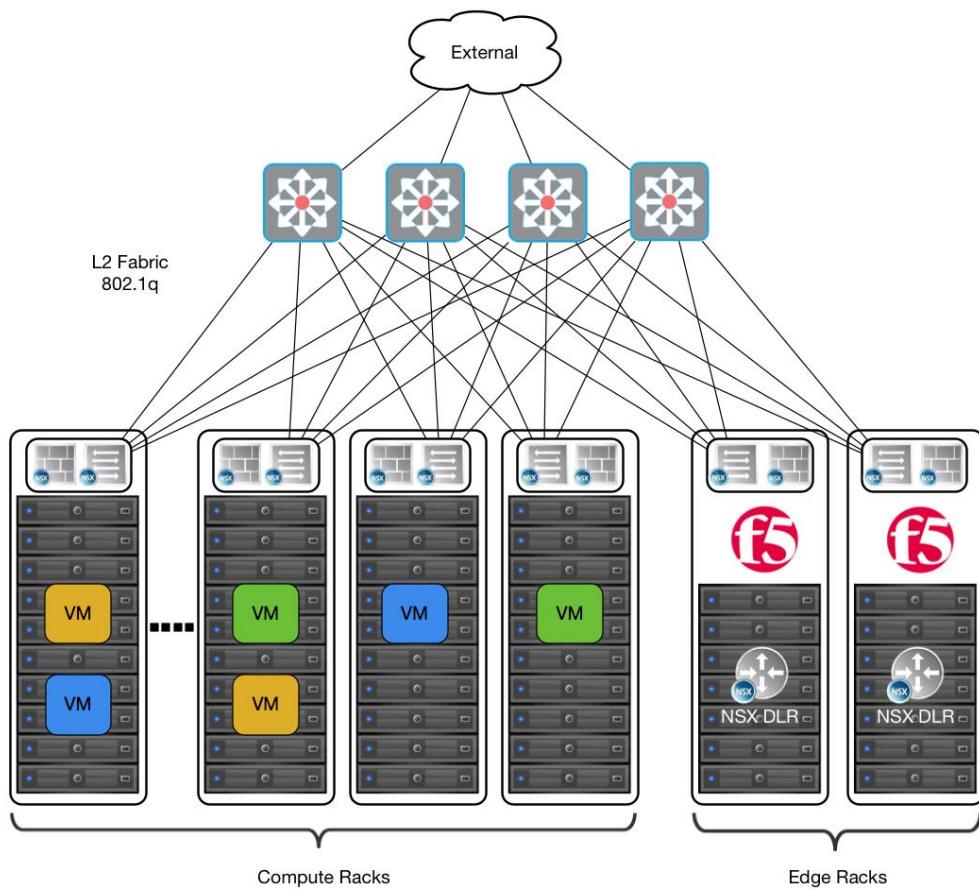


Figure 6 Leaf/spine physical rack infrastructure

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.

INTEGRATION GUIDE

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

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

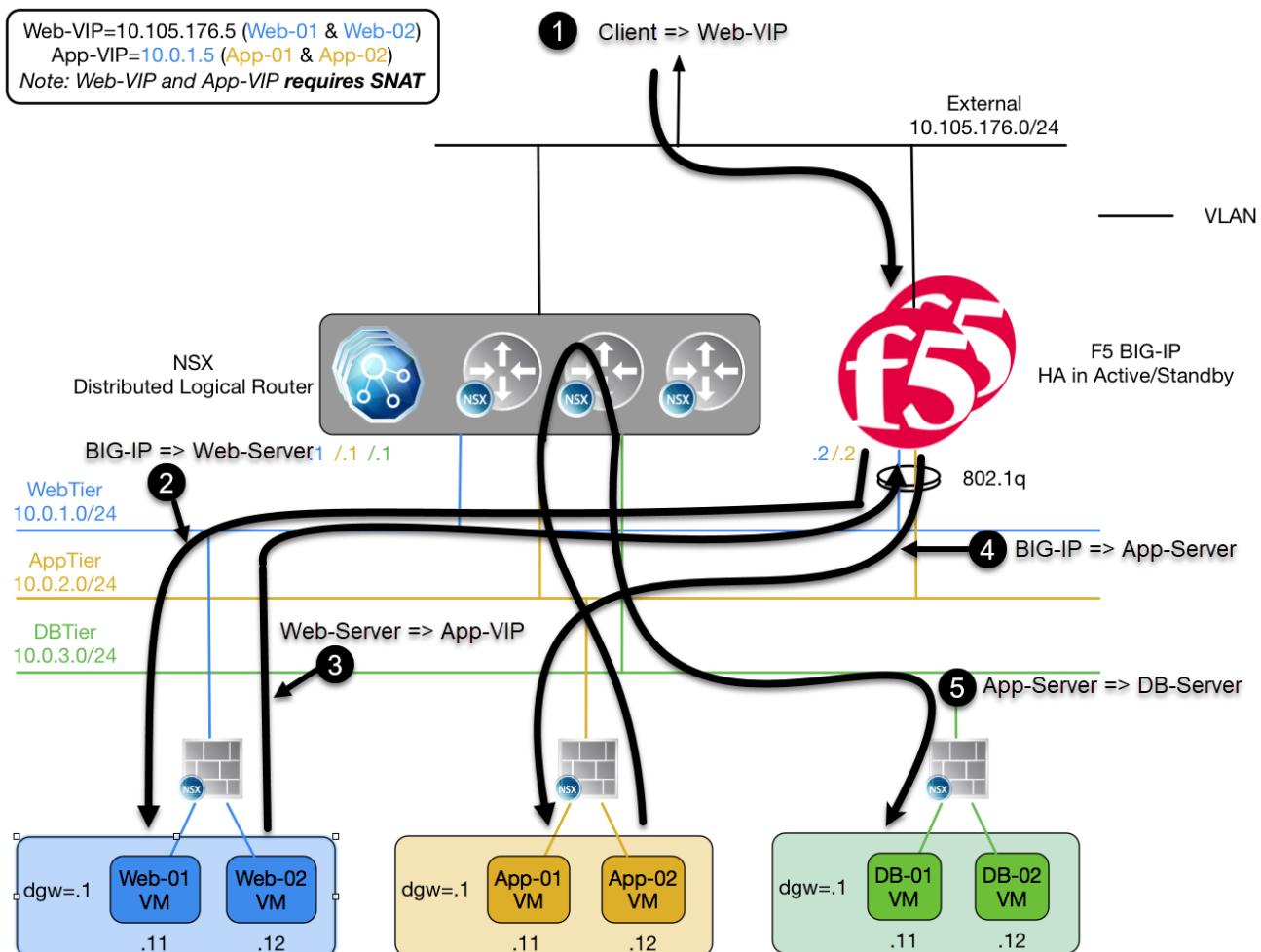


Figure 7 North-South Logical Traffic Flow “Parallel to DLR” with BIG-IP Appliances

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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

INTEGRATION GUIDE

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

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.

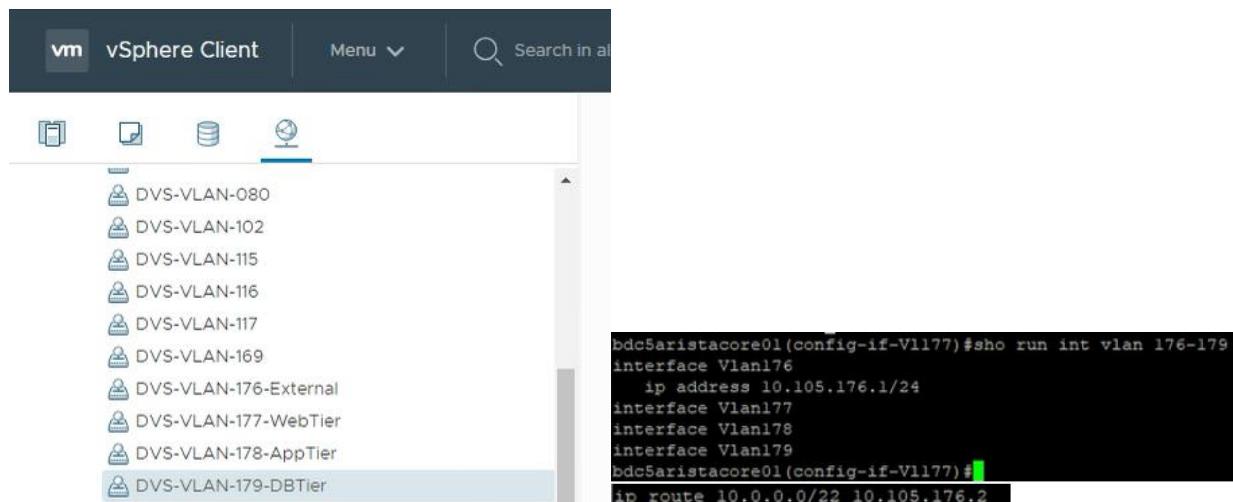


Figure 9 vSphere Client (HTML5) Console & Core Switch VLAN Gateways and IP Route for 10.0.0.0 segment

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)

INTEGRATION GUIDE

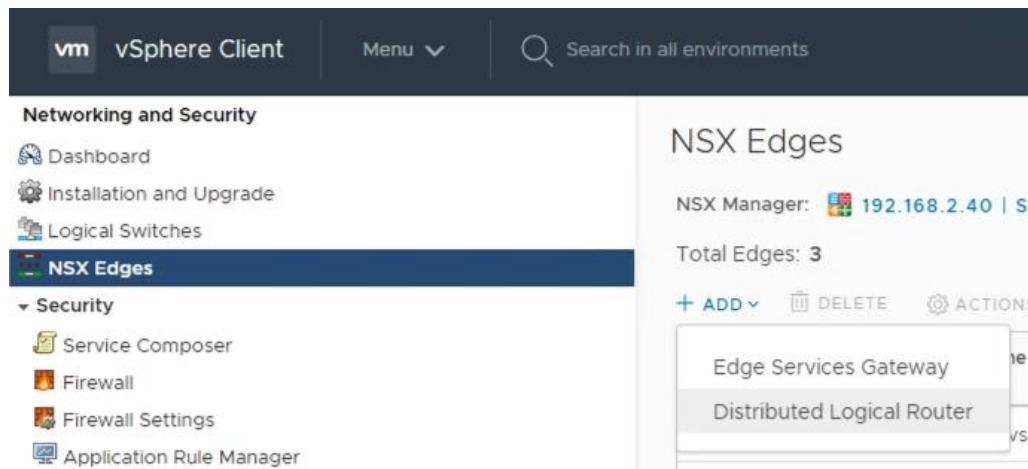
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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”



INTEGRATION GUIDE

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

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

The screenshot shows the 'Basic Details' step of a 'New Distributed Logical Router' wizard. On the left, a vertical navigation bar lists steps 1 through 6. Step 1, 'Basic Details', is highlighted with a teal background. The main panel displays the 'Basic Details' configuration. It includes fields for 'Name' (set to 'Topo2DLR'), 'Host Name', 'Tenant', and 'Description'. Below these, under 'Select Deployment Options', there are two checkboxes: 'Deploy Control VMs' (checked) and 'High Availability' (unchecked). The 'High Availability' section contains 'HA Logging' (disabled) and 'Log Level' (Info). At the bottom right are 'CANCEL', 'NEXT' (highlighted in blue), and 'FINISH' buttons.

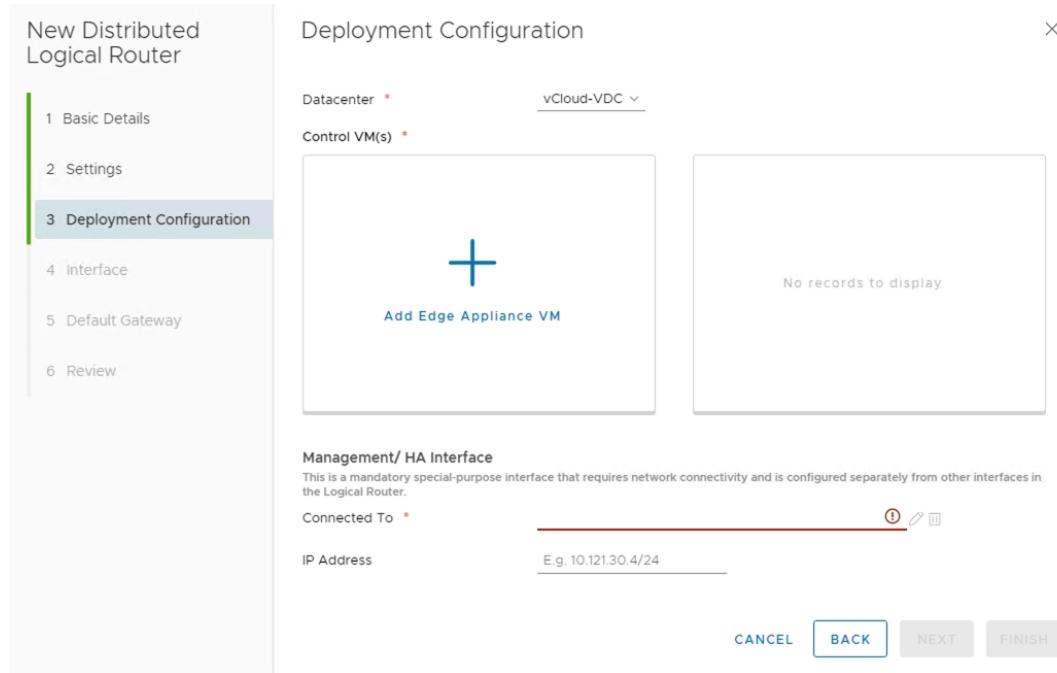
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Distributed Logical Router. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.

The screenshot shows the 'Settings' step of the 'New Distributed Logical Router' wizard. The left navigation bar highlights step 2, 'Settings'. The main panel shows settings for the Edge Appliance VM(s). It includes fields for 'User Name' (admin), 'Password' (redacted), 'Confirm Password' (redacted), 'SSH access' (Enabled), and 'FIPS Mode' (Disabled). Below these is a 'Edge control level logging' dropdown set to 'Info'. At the bottom right are 'CANCEL', 'BACK', 'NEXT' (highlighted in blue), and 'FINISH' buttons.

INTEGRATION GUIDE

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

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



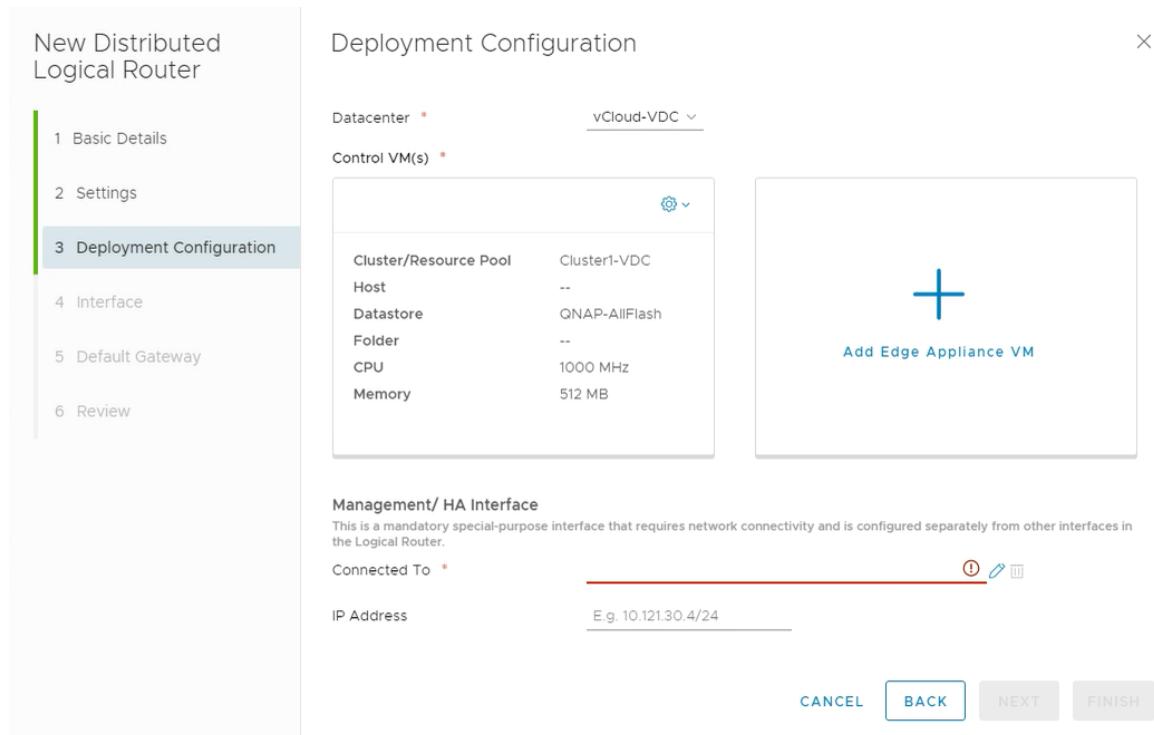
- Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete.

The screenshot shows the 'Add Edge Appliance VM' configuration dialog. It asks to 'Specify placement parameters for the Edge Appliance VM.' The form includes fields for 'Datacenter' (set to 'vCloud-VDC'), 'Cluster/Resource Pool' (set to 'Cluster1-VDC'), 'Datastore' (set to 'QNAP-AllFlash'), 'Host' (empty), 'Folder' (empty), 'Resource Reservation' (set to 'System Managed'), 'CPU' (set to '1000 MHz'), and 'Memory' (set to '512 MB'). At the bottom are 'CANCEL' and 'ADD' buttons.

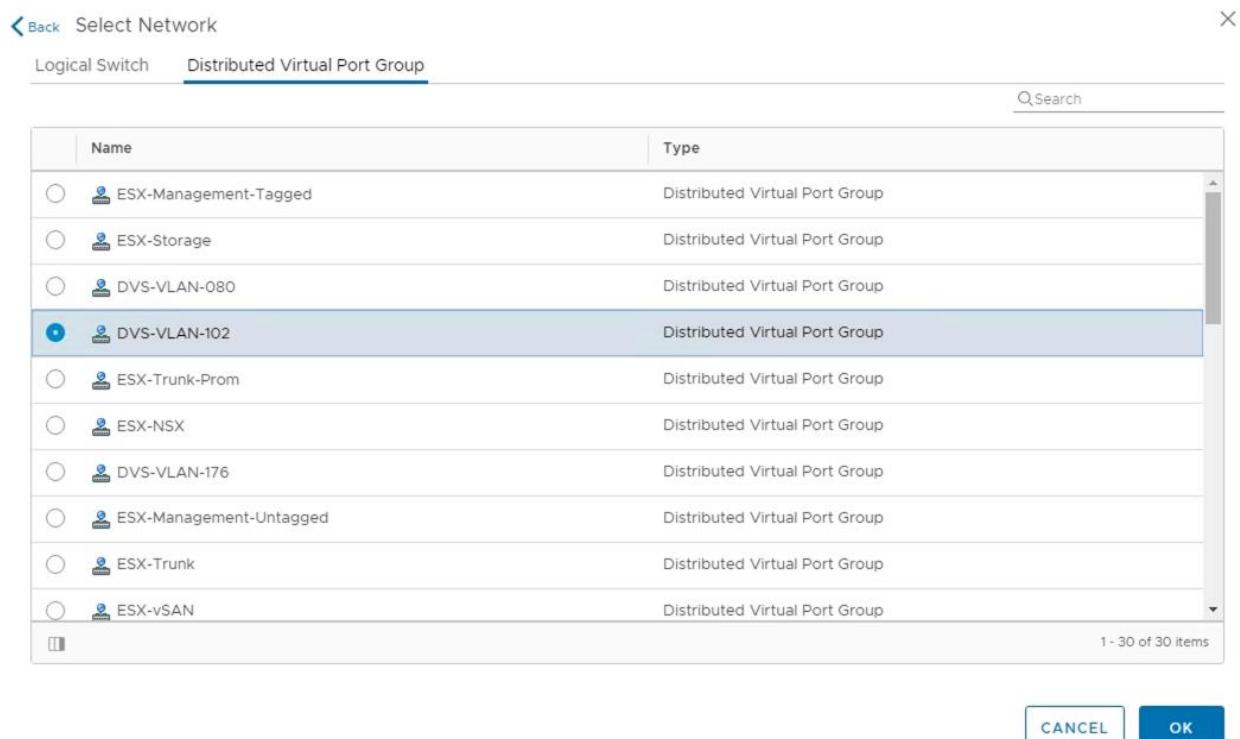
INTEGRATION GUIDE

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

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



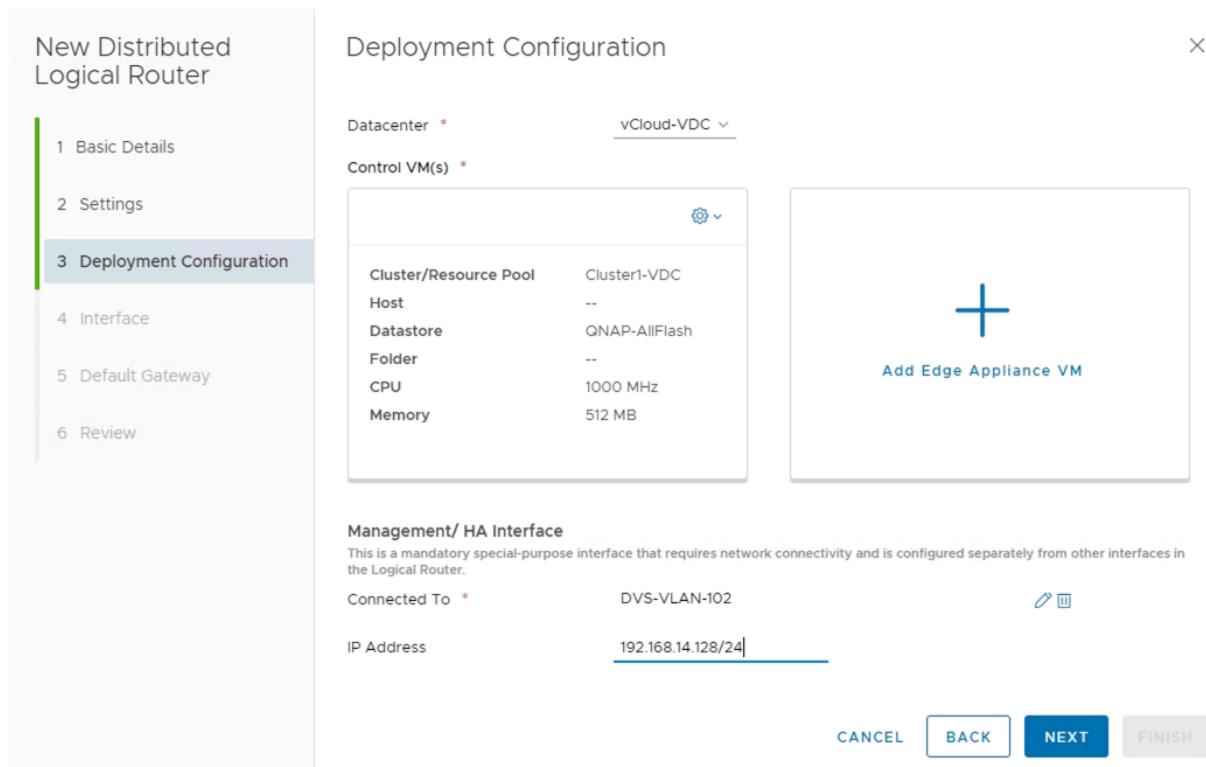
- Select an appropriate Management Network (Distributed Virtual Port Group) to manage the DLR then Click OK



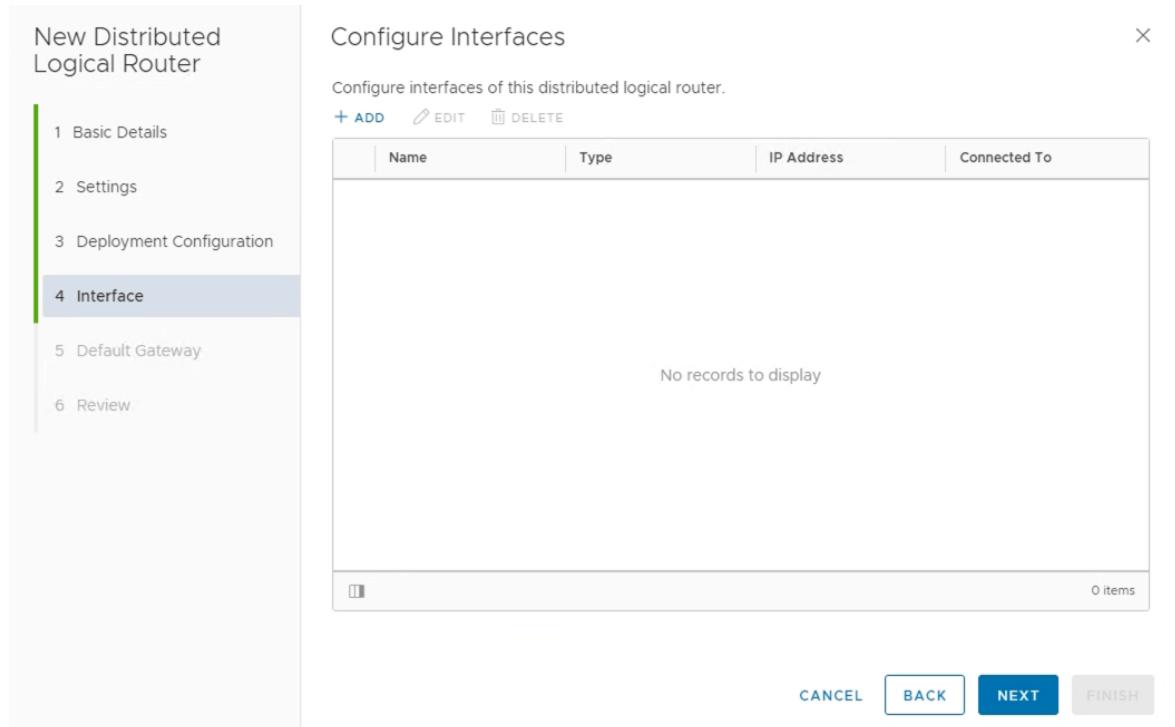
INTEGRATION GUIDE

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

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



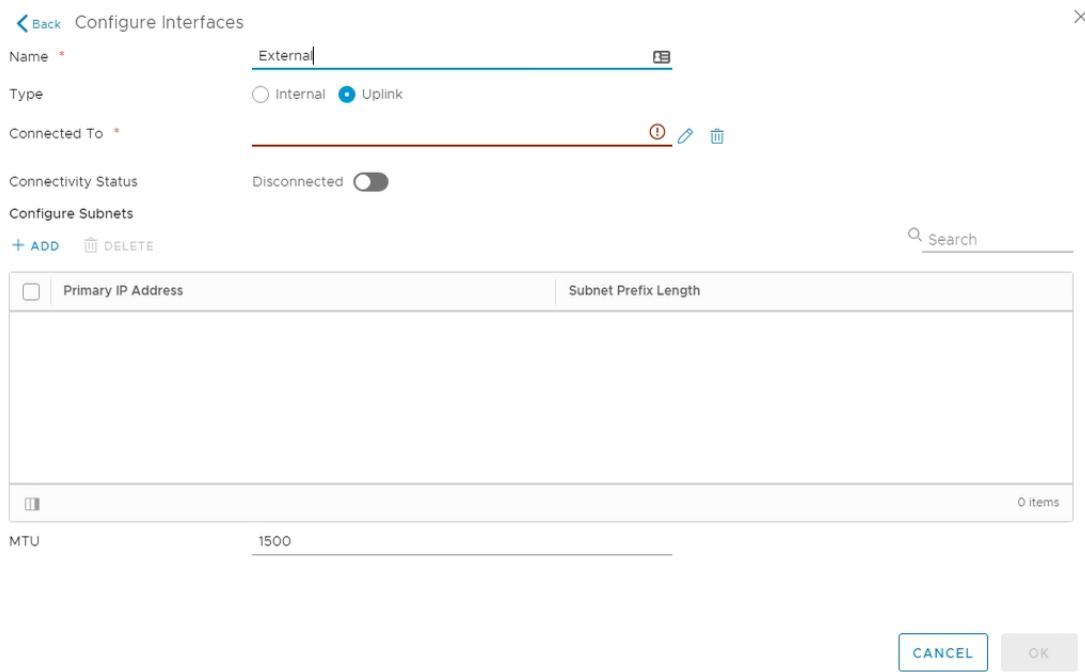
- In the Configure interfaces dialog box, select the (+ Add) hyperlink to display the Add NSX DLR Interface dialog box.



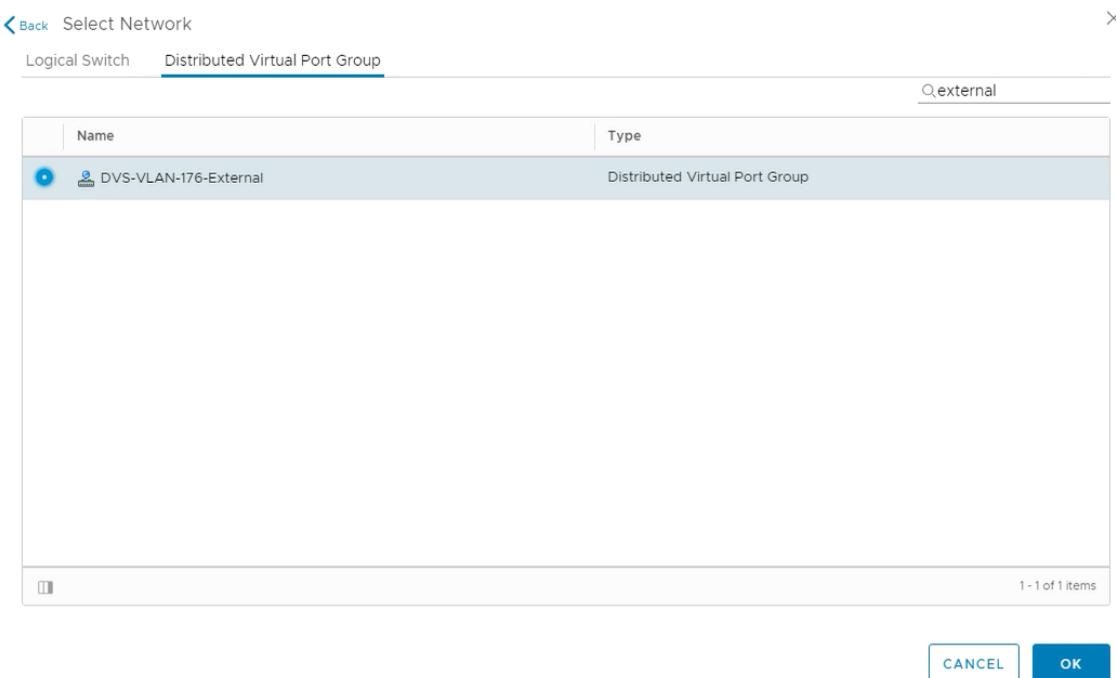
INTEGRATION GUIDE

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

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



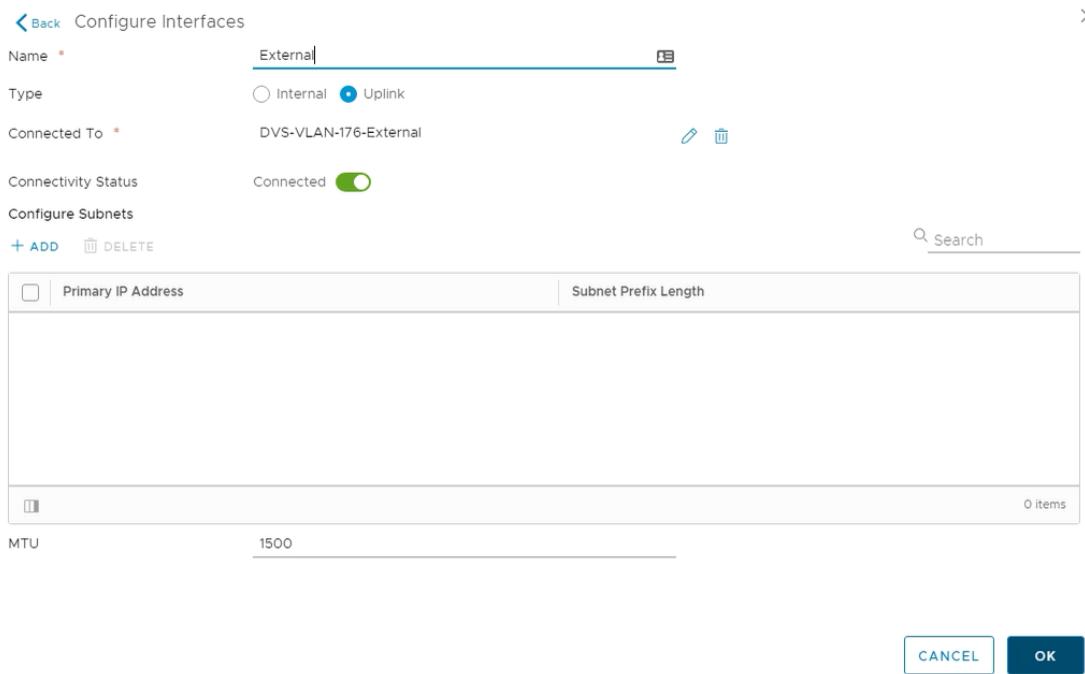
- For the External network, click on the Distributed Virtual Port Group tab and then selecting the correct VLAN associated to the External Network. Click OK.



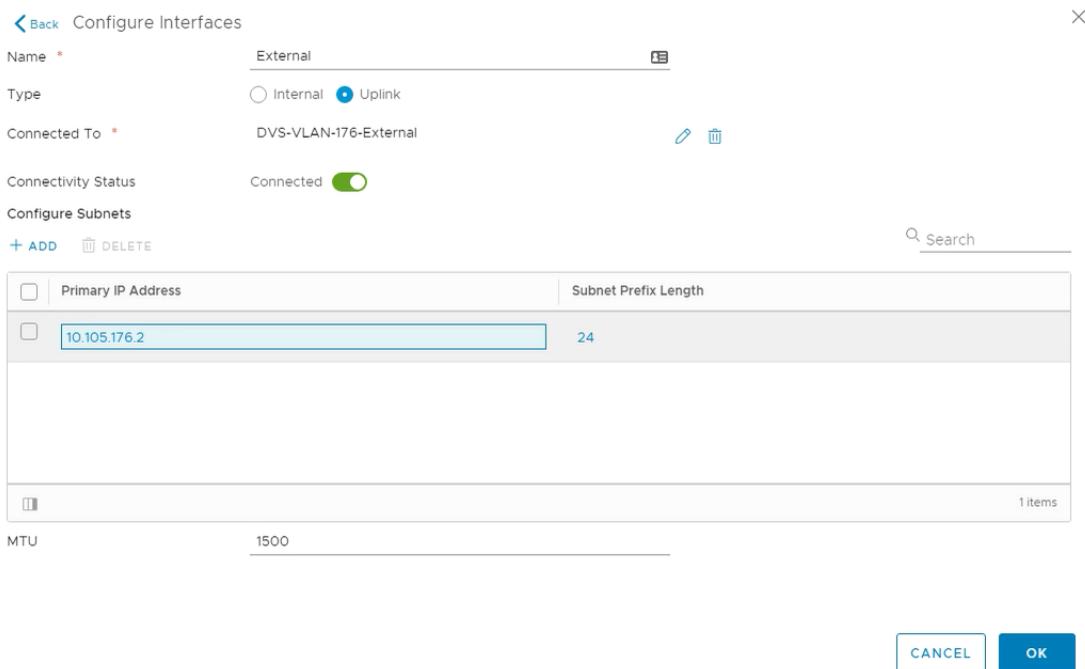
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

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

New Distributed Logical Router

Configure Interfaces

Configure interfaces of this distributed logical router.

+ ADD EDIT DELETE

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

4 items

CANCEL BACK NEXT FINISH

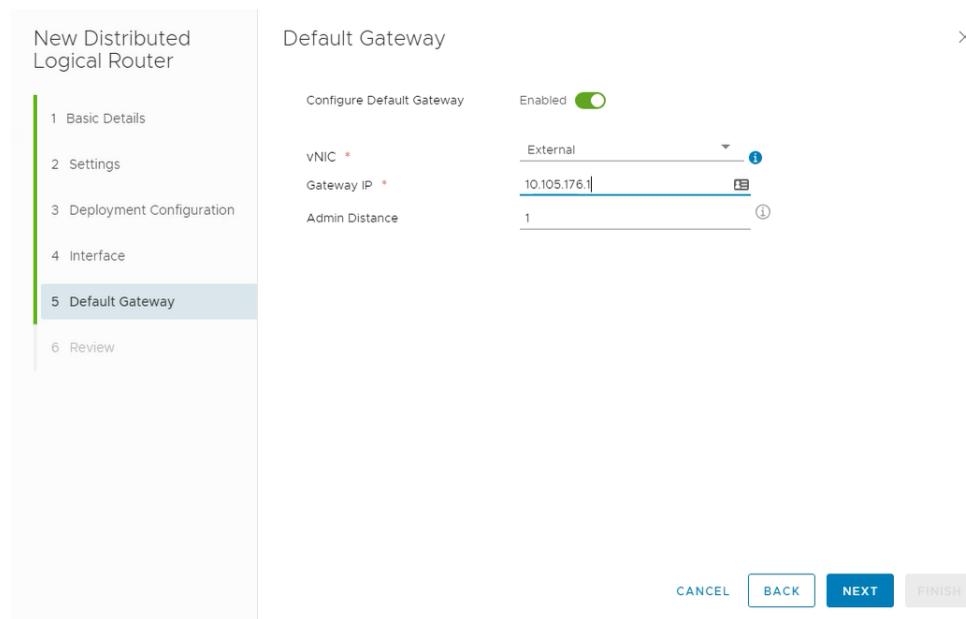
INTEGRATION GUIDE

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

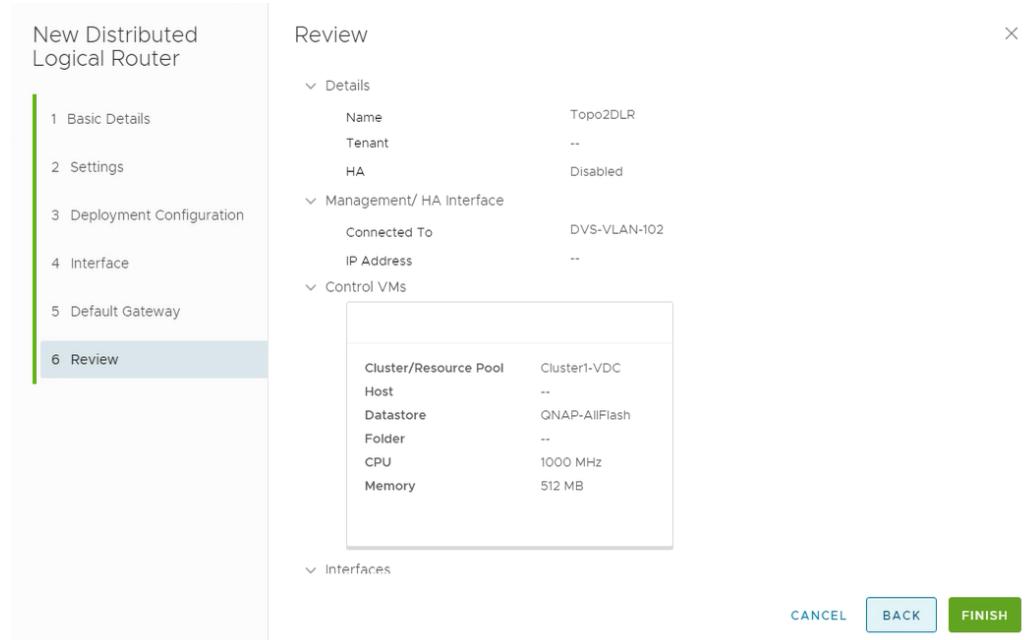
15. Once the interface settings are completed, the next step is to configure the default gateway settings. The default gateway for the DLR is the data center core router that we configured in the previous section for the external network

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.



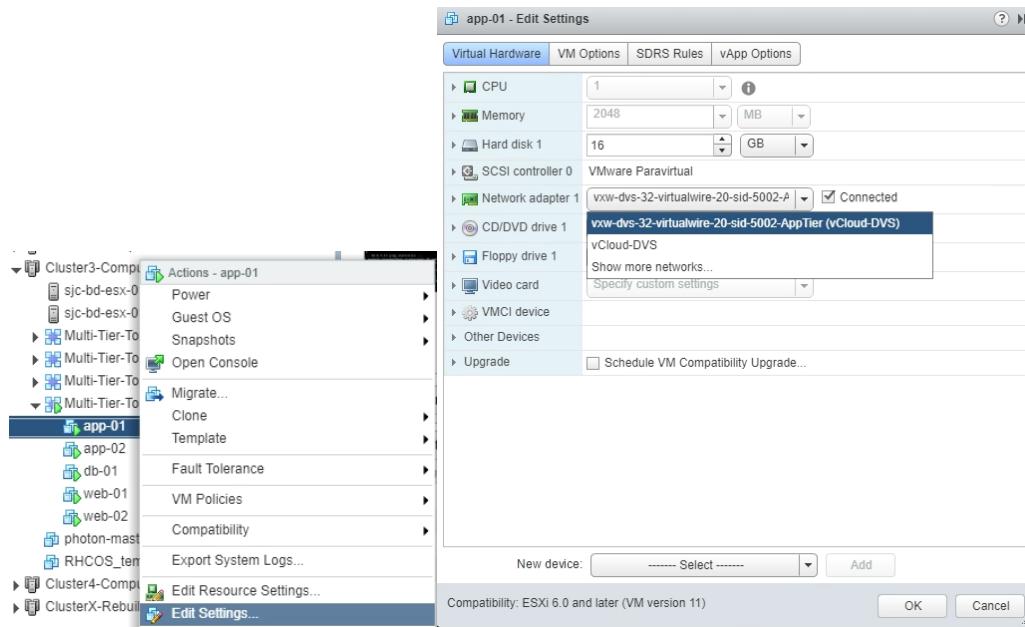
18. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

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.

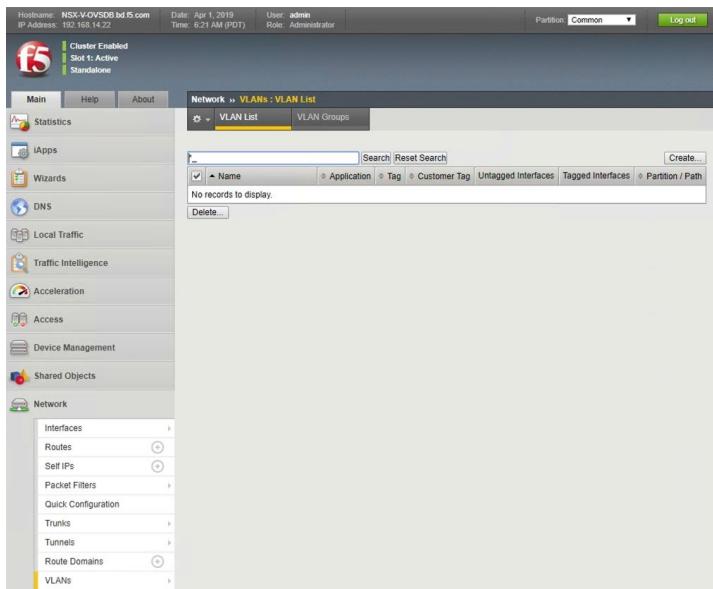
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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.

Network > VLANs : VLAN List > New VLAN...

General Properties

Name	WebTier
Description	
Tag	177

Resources

Interfaces	Interface: 1.2 Tagging: Tagged Add
1.1 (tagged)	
<input type="button" value="Edit"/> <input type="button" value="Delete"/>	

Configuration: Basic

Source Check	<input type="checkbox"/>
MTU	1500

sFlow

Polling Interval	Default
Sampling Rate	Default

Network > VLANs : VLAN List

VLAN List

Name	Application	Tag	Customer Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
External		176		1/1.1		Common
WebTier		177		1/1.1		Common
AppTier		178		1/1.1		Common

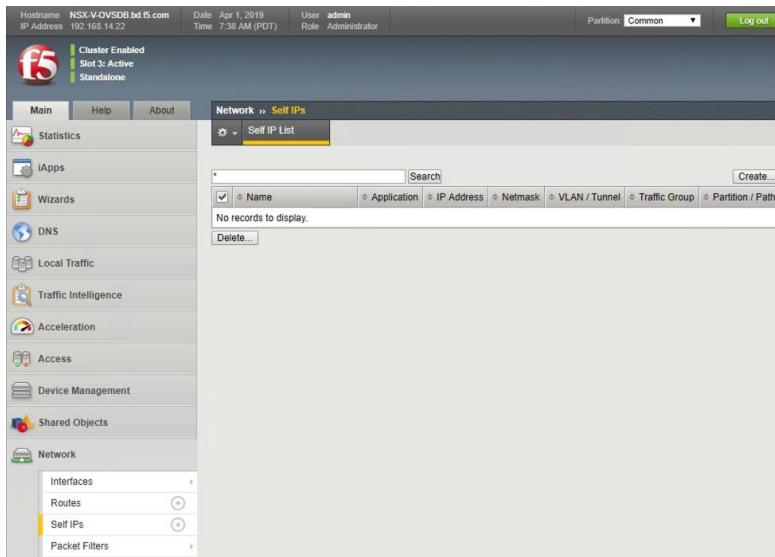
INTEGRATION GUIDE

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

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

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

Configuration	
Name	External-Self-IP
IP Address	10.105.176.10
Netmask	255.255.255.0
VLAN / Tunnel	External
Port Lockdown	Allow None
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Cancel Repeat Finished

INTEGRATION GUIDE

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

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.

Network >> Self IPs >> New Self IP...

Configuration	
Name	Web-Self-IP
IP Address	10.0.1.2
Netmask	255.255.255.0
VLAN / Tunnel	WebTier
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Network >> Self IPs

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	Web-Self-IP		10.0.1.2	255.255.255.0	WebTier	traffic-group-local-only	Common
<input type="checkbox"/>	App-Self-IP		10.0.2.2	255.255.255.0	AppTier	traffic-group-local-only	Common
<input type="checkbox"/>	External-Self-IP		10.105.176.10	255.255.255.0	External	traffic-group-local-only	Common

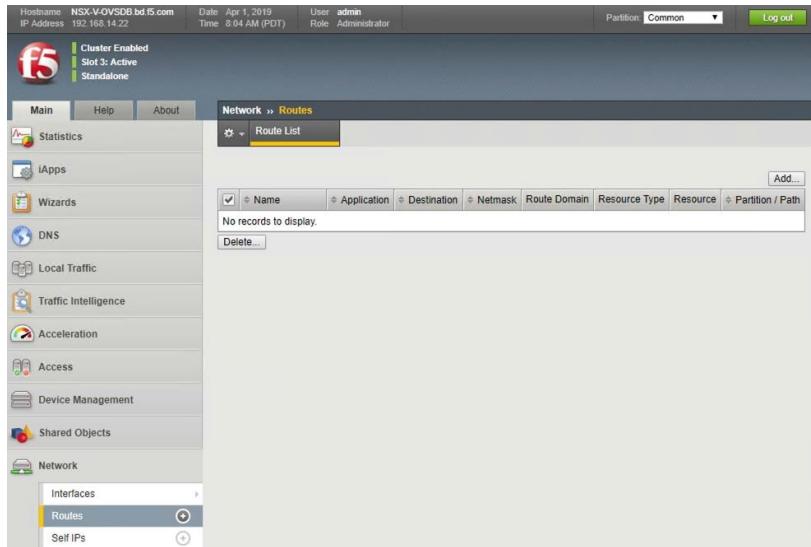
INTEGRATION GUIDE

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

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.

A screenshot of the 'New Route...' configuration dialog. The title bar says 'Network > Routes > New Route...'. The main area is titled 'Properties' and contains the following fields:

Name	default
Description	(empty)
Destination	0.0.0.0
Netmask	0.0.0.0
Resource	Use Gateway...
Gateway Address	IP Address: 10.105.176.1
MTU	(empty)

At the bottom are three buttons: 'Cancel', 'Repeat', and 'Finished'.

INTEGRATION GUIDE

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

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

INTEGRATION GUIDE

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

Local Traffic > Pools : Pool List > New Pool...

Configuration: Basic ▾

Name	WebServerPool				
Description					
Health Monitors	<table border="1"><tr><td>Active</td><td>Available</td></tr><tr><td>/Common gateway_icmp</td><td>/Common http http_head_f5 https https_443</td></tr></table>	Active	Available	/Common gateway_icmp	/Common http http_head_f5 https https_443
Active	Available				
/Common gateway_icmp	/Common http http_head_f5 https https_443				

Resources

Load Balancing Method	Round Robin															
Priority Group Activation	Disabled															
New Members	<p><input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node</p> <p>Node Name: <input type="text"/> (Optional)</p> <p>Address: <input type="text" value="10.0.1.12"/></p> <p>Service Port: <input type="text" value="443"/> <input type="button" value="HTTPS"/></p> <p><input type="button" value="Add"/></p> <table border="1"><thead><tr><th>Node Name</th><th>Address/FQDN</th><th>Service Port</th><th>Auto Populate</th><th>Priority</th></tr></thead><tbody><tr><td>10.0.1.11</td><td>10.0.1.11</td><td>443</td><td></td><td>0</td></tr><tr><td>10.0.1.12</td><td>10.0.1.12</td><td>443</td><td></td><td>0</td></tr></tbody></table> <p><input type="button" value="Edit"/> <input type="button" value="Delete"/></p>	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
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												

INTEGRATION GUIDE

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

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.

Status	Name	Description	Application	Members	Partition / Path
Green Circle	AppServerPool			2	Common
Green Circle	WebServerPool			2	Common

INTEGRATION GUIDE

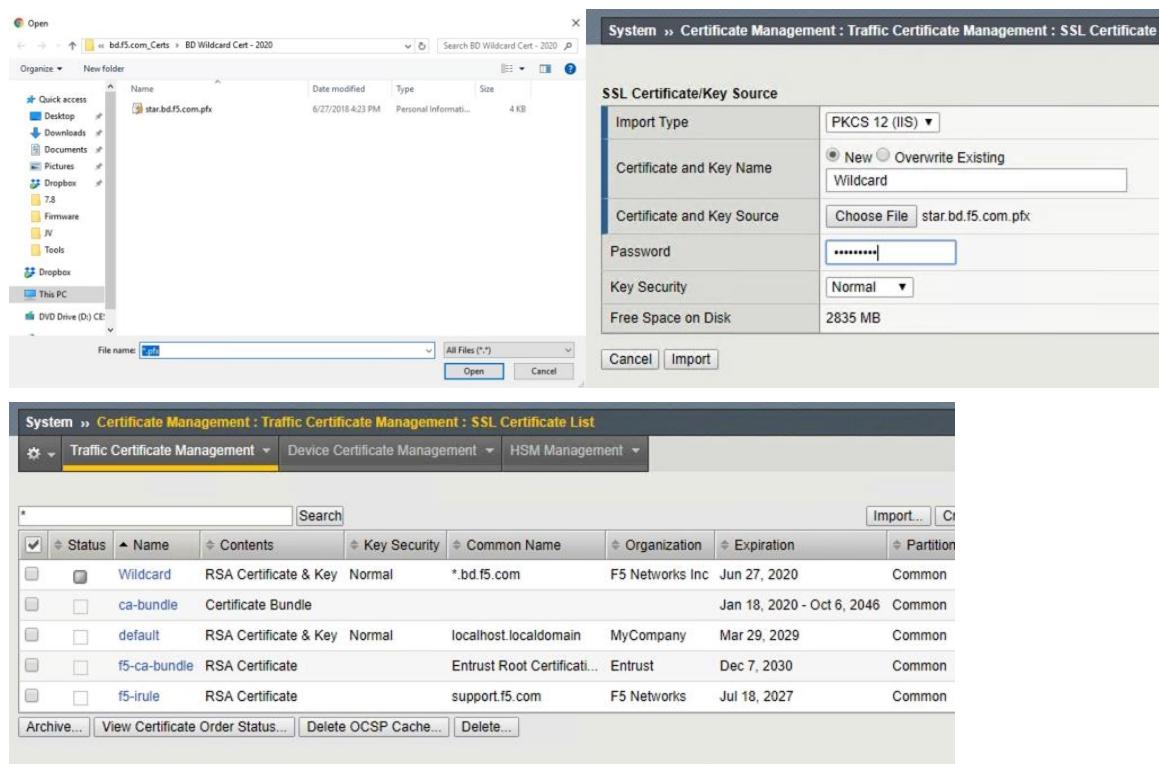
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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



INTEGRATION GUIDE

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

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.

The screenshot shows the F5 Management Interface for creating a new Client SSL Profile. It consists of three main windows:

- New Client SSL Profile...** (Top Window):
 - General Properties:** Name is set to "WildcardSSL" and Parent Profile is "clientssl".
 - Configuration:** Set to "Basic".
 - Certificate Key Chain:** A list box containing "Wildcard" with an "Add" button below it.
 - Custom:** An unchecked checkbox.
- Add SSL Certificate Key Chain...** (Middle Window):
 - Fields:** Certificate, Key, Chain, and Passphrase, all currently set to "Wildcard".
 - Buttons:** Add and Cancel.
- New Client SSL Profile...** (Bottom Window):
 - General Properties:** Same as the top window.
 - Configuration:** Set to "Basic".
 - Certificate Key Chain:** Now lists "/Common/Wildcard /Common/Wildcard /Common/Wildcard" with an "Add" button below it.
 - OCSP Stapling:** An empty section.

INTEGRATION GUIDE

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

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

The screenshot displays the F5 BIG-IP configuration interface for creating a new virtual server. The main window title is "Local Traffic > Virtual Servers : Virtual Server List > New Virtual Server...".

General Properties:

- Name: Web-VIP
- Description: (empty)
- Type: Standard
- Source Address: Host (10.105.176.5)
- Destination Address/Mask: Host (10.105.176.5)
- Service Port: Port (443)
- Notify Status to Virtual Address: checked
- State: Enabled

Resources:

- iRules: A list of available iRules including _sys_auth_ssl_cc_idap, _sys_auth_ssl_crldp, _sys_ssl_ocsp, _sys_auth_tacacs, and _sys_https_redirect. One iRule (_sys_auth_ssl_cc_idap) is selected.
- Policies: A list of available policies.
- Default Pool: WebServerPool is selected.
- Default Persistence Profile: None
- Fallback Persistence Profile: None

Configuration:

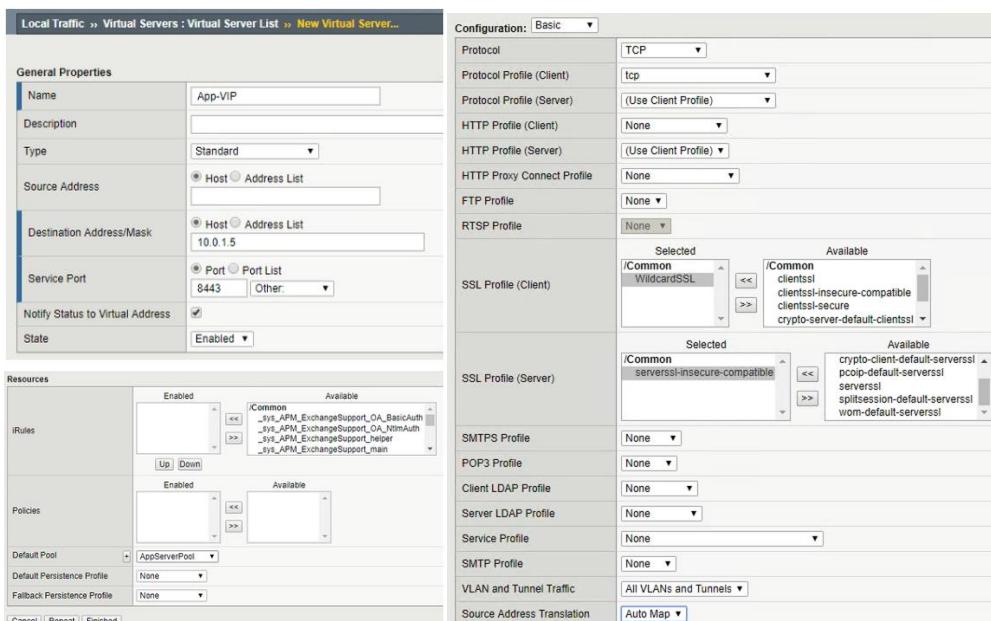
- Protocol: TCP
- Protocol Profile (Client): tcp
- Protocol Profile (Server): (Use Client Profile)
- HTTP Profile (Client): None
- HTTP Profile (Server): (Use Client Profile)
- HTTP Proxy Connect Profile: None
- FTP Profile: None
- RTSP Profile: None
- SSL Profile (Client): /Common WildcardSSL (Selected)
- SSL Profile (Server): /Common serverssl-insecure-compatible (Selected)
- SMTPS Profile: None
- POP3 Profile: None
- Client LDAP Profile: None
- Server LDAP Profile: None
- Service Profile: None
- Source Address Translation: Auto Map

INTEGRATION GUIDE

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

4. In the New Virtual Server menus

- In the Name field, provide a unique name for the app application. In this case, we used App-VIP.
- In the Destination Address field, enter 172.16.1.5
- For Service Port use the standard HTTPS port 8443.
- In the Configuration section
 - Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
 - Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
 - Select Auto Map from the pull-down menus for the Source Address Translation.
- In the Resources section
 - Select the AppServerPool from the Default Pool dropdown box.
 - 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.
- 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.

Local Traffic > Virtual Servers : Virtual Server List						
		Virtual Server List		Virtual Address List Statistics		
<input checked="" type="checkbox"/> Status		Name	Description	Application	Destination	Service Port
Type	Resources	Partition / Path	Created	Last Modified	Last Accessed	Last Used
Standard		Common	2023-09-12 10:30:00	2023-09-12 10:30:00	2023-09-12 10:30:00	2023-09-12 10:30:00
App-VIP	AppServerPool	Common	2023-09-12 10:30:00	2023-09-12 10:30:00	2023-09-12 10:30:00	2023-09-12 10:30:00
Web-VIP	AppServerPool	Common	2023-09-12 10:30:00	2023-09-12 10:30:00	2023-09-12 10:30:00	2023-09-12 10:30:00

INTEGRATION GUIDE

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

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.

The screenshot shows the F5 BIG-IP Local Traffic interface. On the left, there's a tree view under 'Common' with two main nodes: 'App-VIP' (IP 10.0.1.5:8443) and 'Web-VIP' (IP 10.0.1.76.5:443). The 'Web-VIP' node has two child nodes: 'WebServerPool' (IP 10.0.1.11:443) and 'WebServerPool' (IP 10.0.1.12:443). On the right, a 'NSXWebApp Properties' dialog box is open. It shows the 'Host (A)' tab selected. The 'Host' field contains 'NSXWebApp'. The 'Fully qualified domain name (FQDN)' field contains 'NSXWebApp.bd.f5.com'. The 'IP address' field contains '10.105.176.5'. There are checkboxes for 'Update associated pointer (PTR) record' and 'Delete this record when it becomes stale'. A 'Record time stamp' field is present. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons. The status bar at the bottom of the interface shows 'Last Update: Apr 11, 2019 2:34 PM (PDT)'.

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.

The screenshot shows two browser tabs. Both tabs are displaying the same page: 'Customer Database Access'. The left tab shows 'Accessed via: 10.0.2.2' and 'AppServer is: app-01'. The right tab shows 'Accessed via: 10.0.2.2' and 'AppServer is: app-02'. Below the tabs, there are two tables. The left table is for 'app-01' and the right table is for 'app-02'. Both tables have columns: Rank, Name, Universe, and Revenue. The data for both tables is identical:

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

The screenshot shows a terminal window with two panes. Both panes show the output of a curl command. The curl command is: curl -kv "https://nsxwebapp.bd.f5.com". The output shows the connection details and the response body, which contains the text "It works!". The terminal prompt is '[mmabis@hzn-lin-mmabis ~]\$'.

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

INTEGRATION GUIDE

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

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

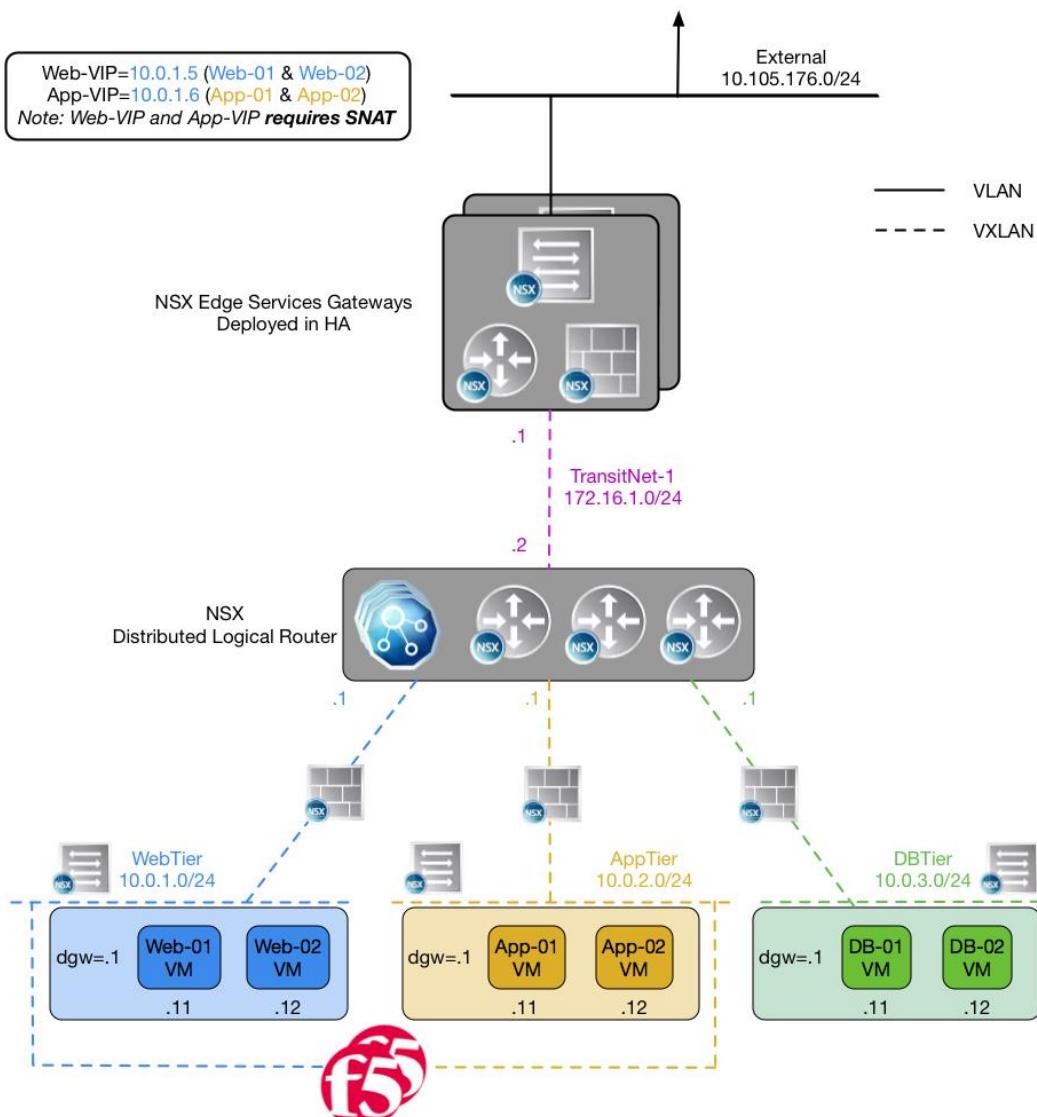


Figure 10 BIG-IP Virtual Edition in one-arm topology within VXLAN environment

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.

INTEGRATION GUIDE

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

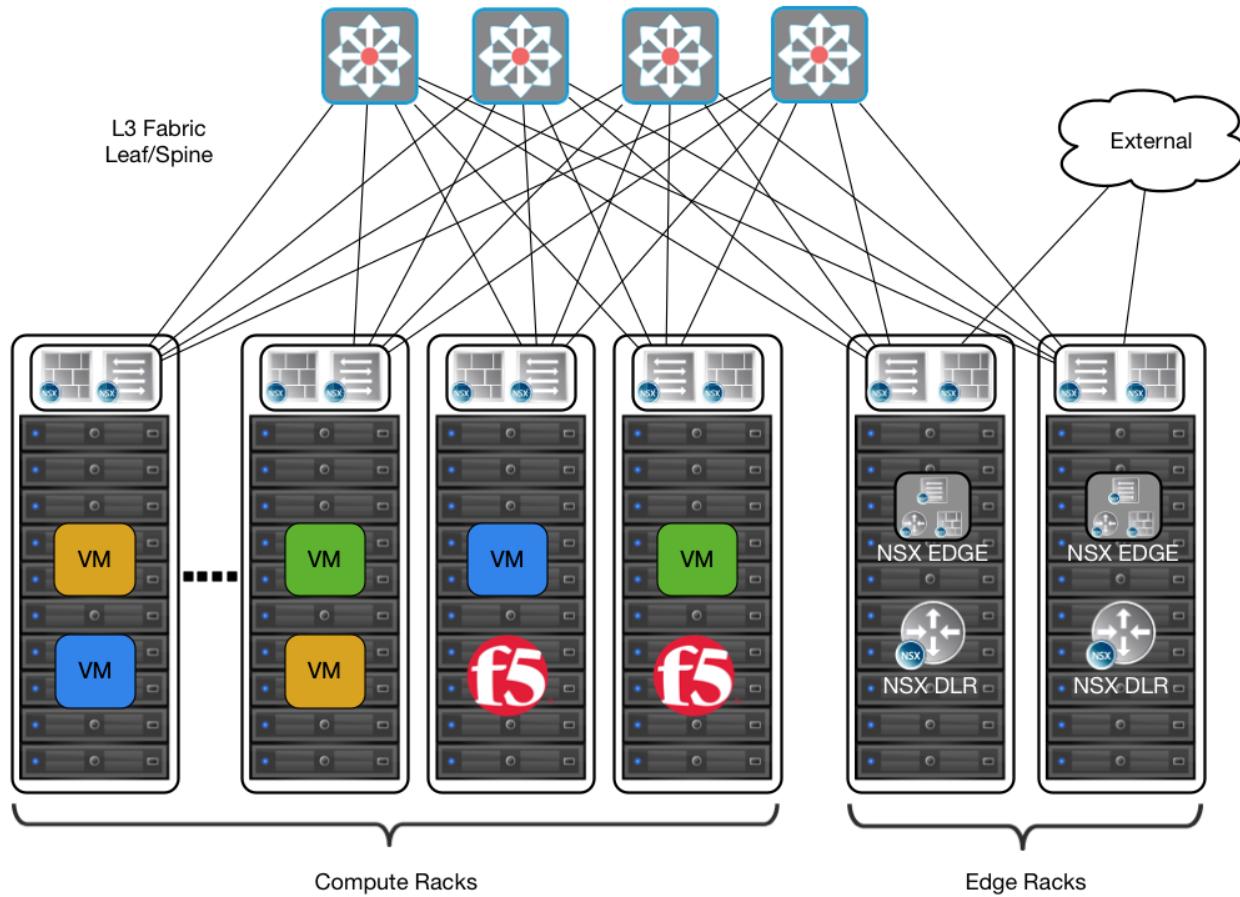


Figure 11 Leaf/spine physical rack infrastructure

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.

INTEGRATION GUIDE

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

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

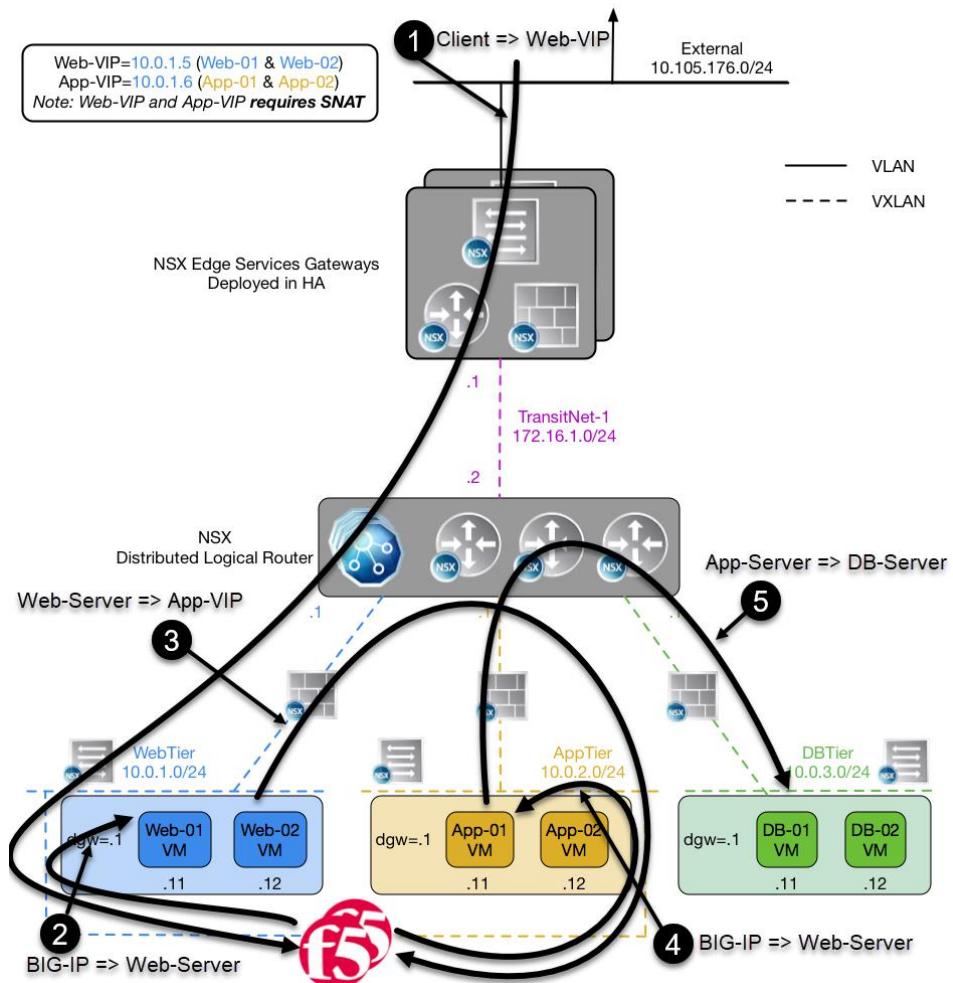


Figure 12 North-South Logical Traffic Flow “One-arm Connected” with BIG-IP Virtual Edition

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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.

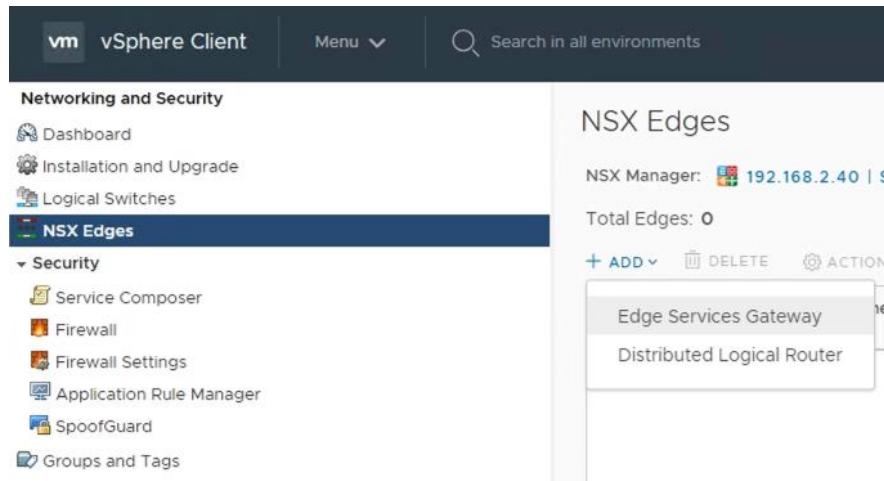
- **VXLAN 5001 WebTier** is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5002 AppTier** is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5003 DBTier**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

INTEGRATION GUIDE

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

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.

The screenshot shows the "New Edge Services Gateway" wizard with the following steps:

- Step 1: Basic Details** (selected)
- Step 2: Settings**
- Step 3: Deployment Configuration**
- Step 4: Interface**
- Step 5: Default Gateway**
- Step 6: Firewall Default Policy**
- Step 7: Review**

Basic Details:

Edge services gateway provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.

Name	Topo3-ESG
Host Name	[Empty]
Tenant	[Empty]
Description	[Empty]

Select Deployment Options:

Deploy Edge Appliance VM
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.

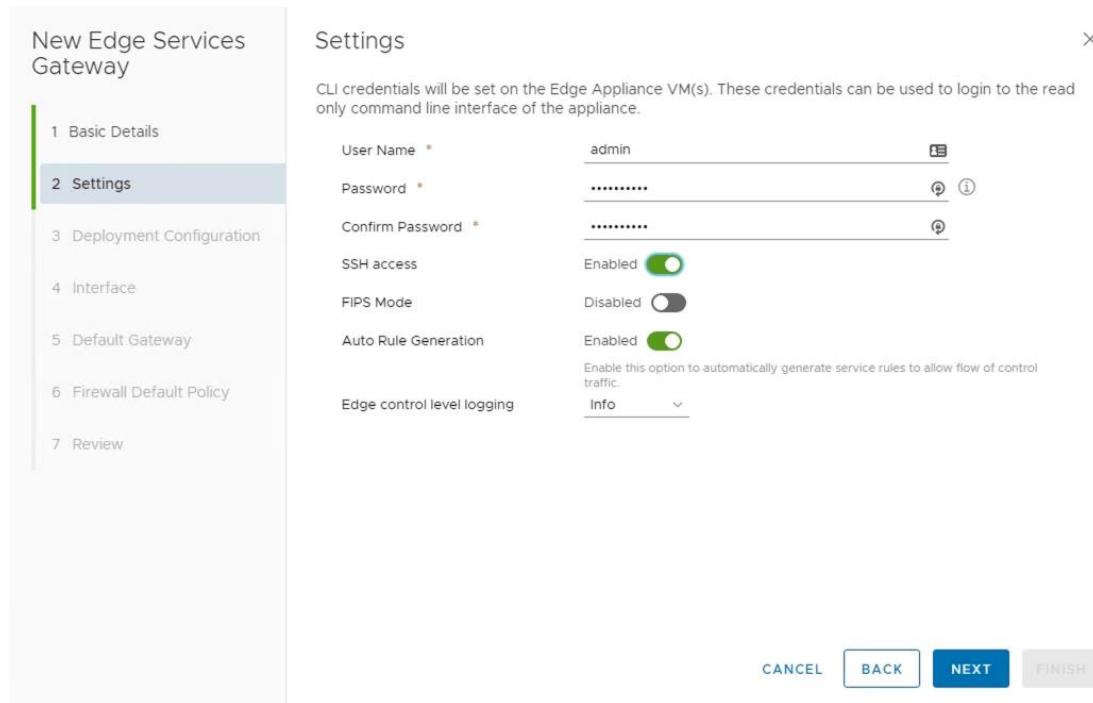
High Availability
Enable this option for enabling and configuring High Availability.

Buttons: CANCEL, NEXT, FINISH

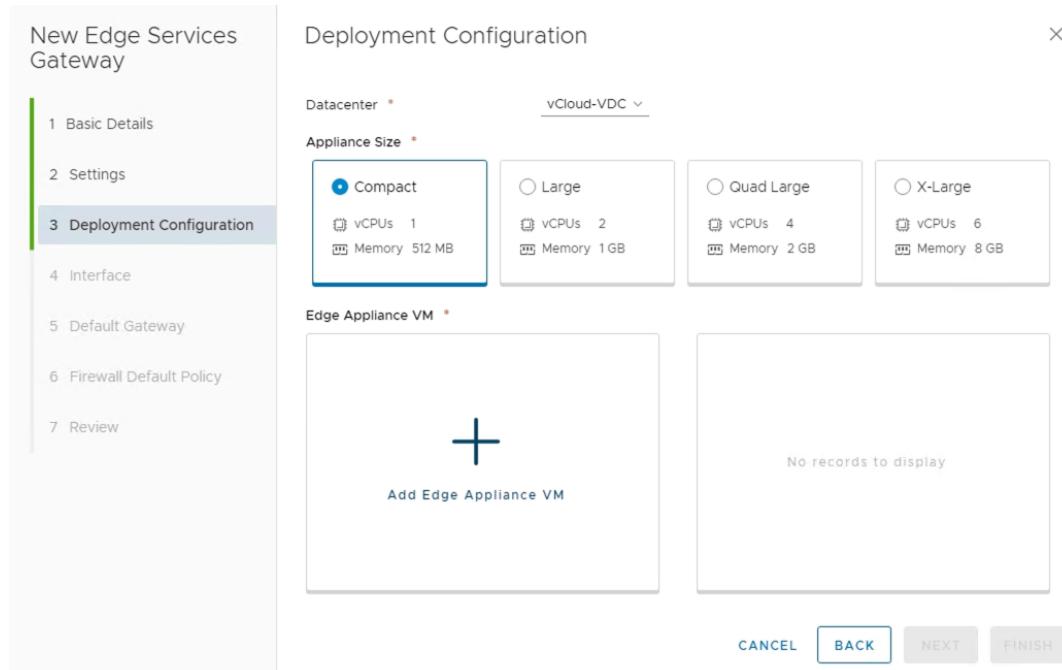
INTEGRATION GUIDE

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

- 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.



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



INTEGRATION GUIDE

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

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.

Add Edge Appliance VM X

Specify placement parameters for the Edge Appliance VM.

Datacenter *	vCloud-VDC
Cluster/Resource Pool *	Cluster1-VDC
Datastore *	QNAP>AllFlash
Host	
Folder	
Resource Reservation	System Managed ①
CPU	1000 MHz
Memory	512 MB

CANCEL ADD

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

New Edge Services Gateway

Configure Interfaces

Configure interfaces of this edge services gateway.

+ ADD EDIT DELETE

vNIC#	Name	Type	IP Address	Connected To
No records to display				

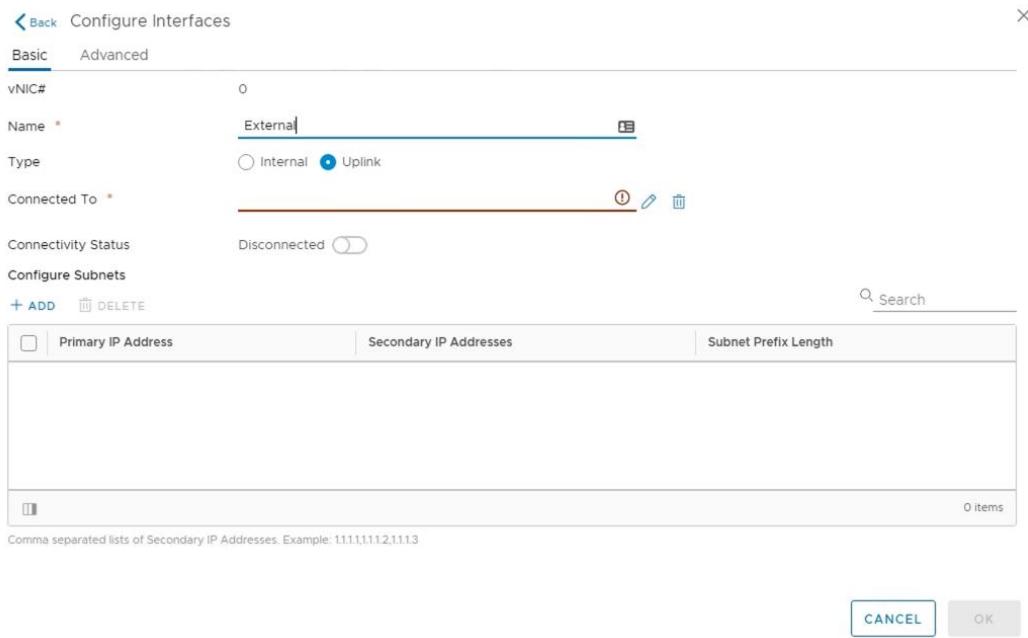
NEXT FINISH

1 Basic Details
2 Settings
3 Deployment Configuration
4 Interface
5 Default Gateway
6 Firewall Default Policy
7 Review

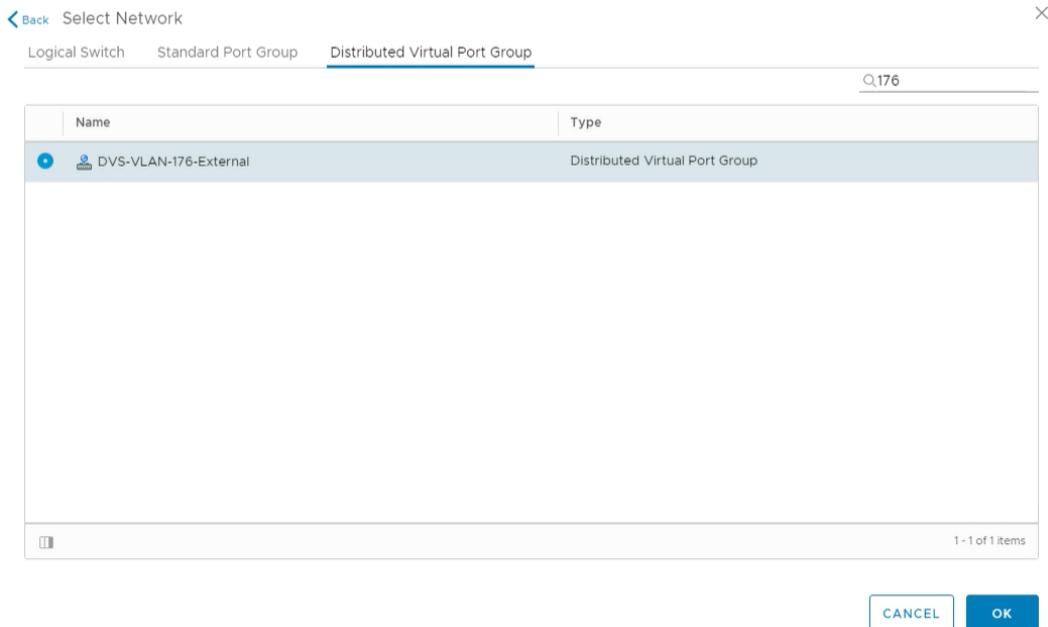
INTEGRATION GUIDE

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

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



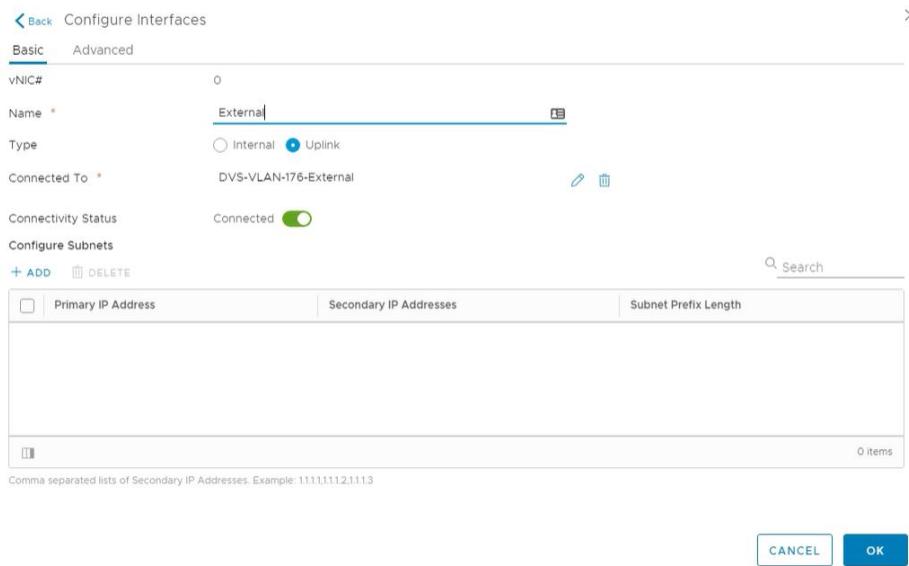
8. For the External network, click on the Distributed Virtual Port Group tab and then selecting the port group used for external access. Click OK.



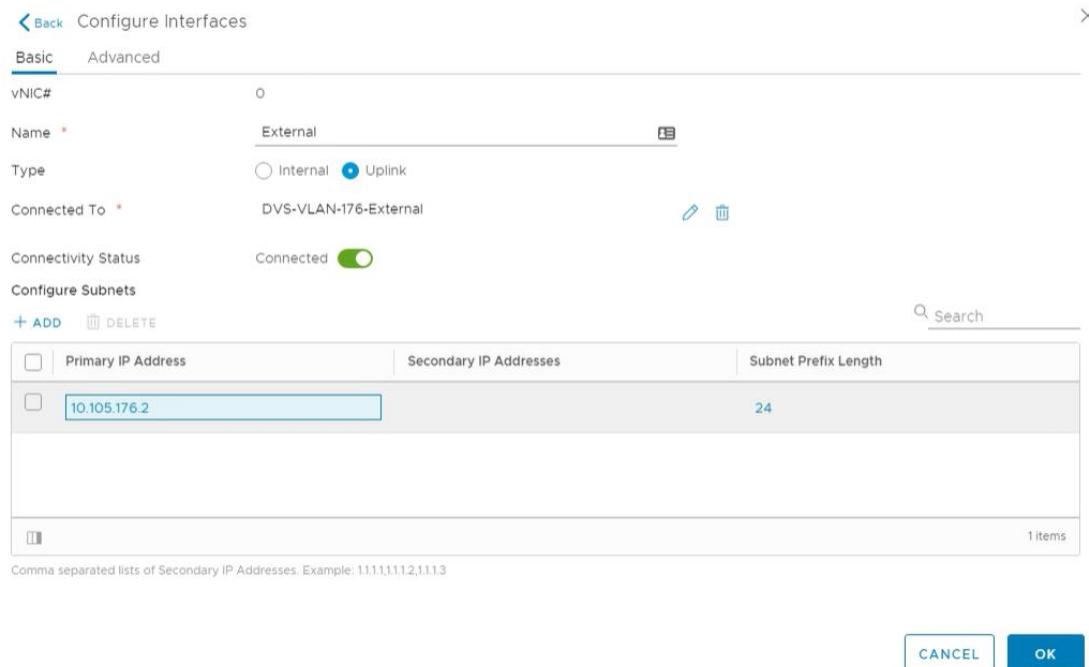
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

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

Configure Interfaces

Configure interfaces of this edge services gateway.

+ ADD EDIT DELETE

vNIC#	Name	Type	IP Address	Connected To
0	External	Uplink	10.105.176.2/24	DVS-VLAN-176-External
1	TransitNet-1	Internal	172.16.1.1/24	TransitNet-1

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.

New Edge Services Gateway

1 Basic Details

2 Settings

3 Deployment Configuration

4 Interface

5 Default Gateway

6 Firewall Default Policy

7 Review

Default Gateway

Configure Default Gateway

Enabled

vNIC *

Gateway IP *

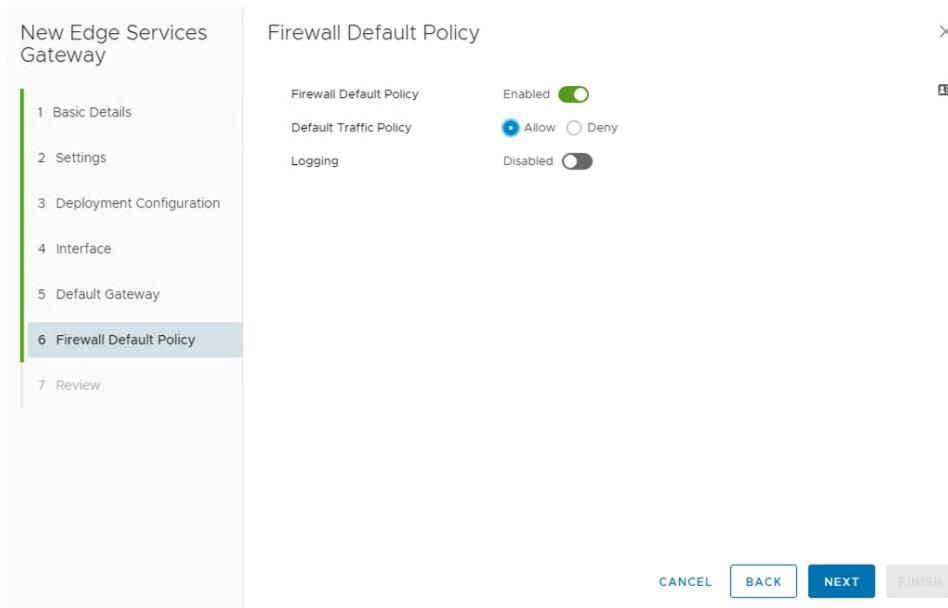
Admin Distance

CANCEL BACK NEXT FINISH

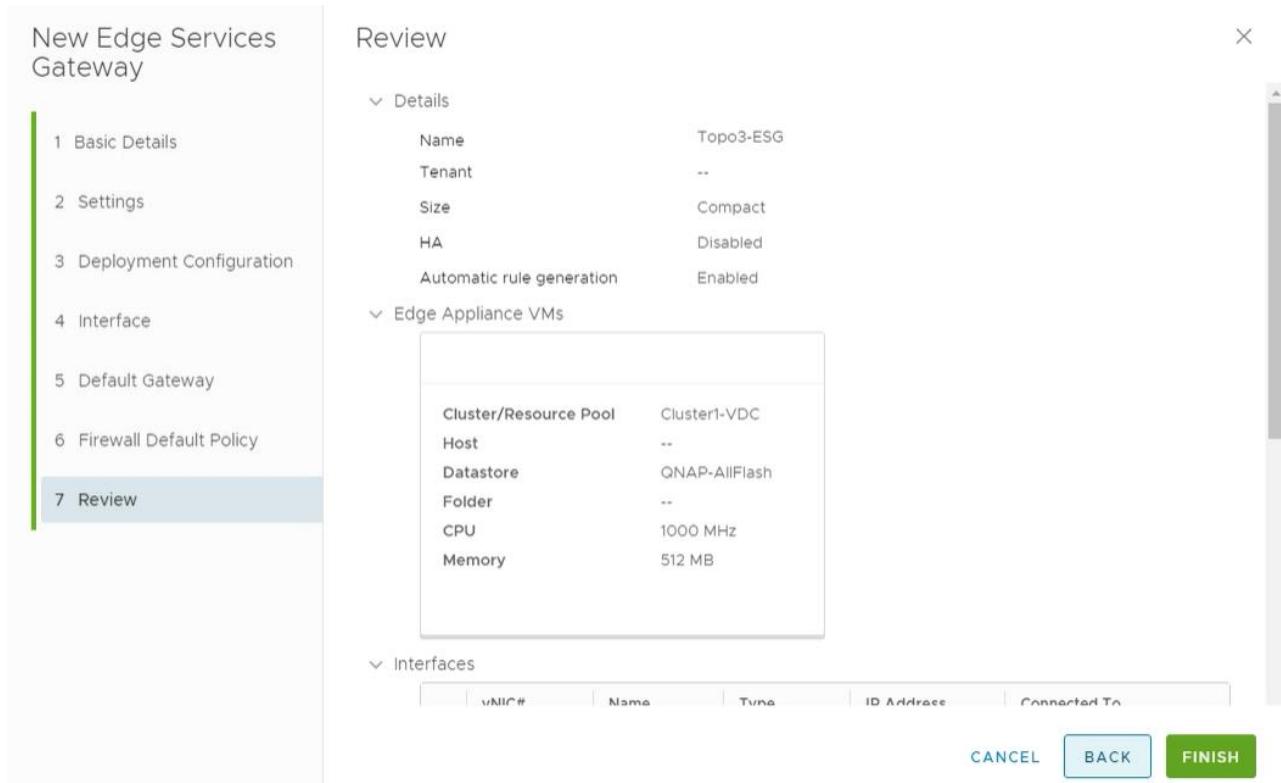
INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

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).

The screenshot shows the NSX Edges interface for the Topo3-ESG edge device. The NAT tab is selected. A single DNAT rule is listed in the table:

Status	Order	RuleID	Rule Type	Action	Applied On	Original	Translated	Logging
<input type="radio"/>	1	196609	USER	DNAT	External	Protocol: tcp Source IP: any Source Ports: any Destination IP: 10.105.176.2 Destination Ports: 443	IP Address: 10.0.1.5 Port Range: 443	<input checked="" type="checkbox"/>

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)

The screenshot shows the NSX Edges interface for the Topo3-ESG edge device. The Firewall tab is selected. Three firewall rules are listed in the table:

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	WebApp	User	any	10.105.176.2	HTTPS	Accept
3	Default Rule	Default	any	any	any	Deny

INTEGRATION GUIDE

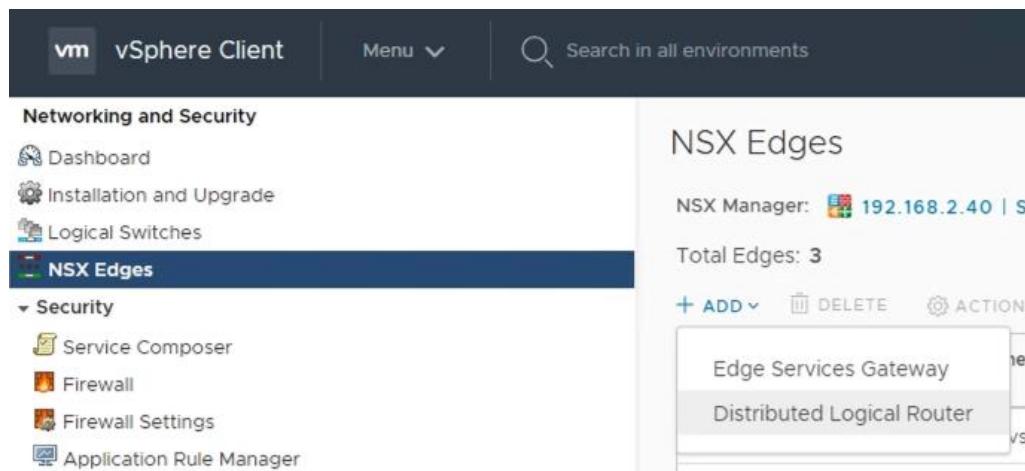
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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”



INTEGRATION GUIDE

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

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

The screenshot shows the 'Basic Details' step of a wizard titled 'New Distributed Logical Router'. On the left, a vertical navigation bar lists steps 1 through 6. Step 1, 'Basic Details', is highlighted. The main panel displays the 'Basic Details' configuration. It includes fields for Name (set to 'Topo3-DLR'), Host Name, Tenant, and Description. Below these are 'Select Deployment Options' with two checkboxes: 'Deploy Control VMs' (checked) and 'High Availability' (unchecked). Under 'High Availability', there are options for HA Logging (set to 'Disabled') and Log Level (set to 'Info'). At the bottom right are 'CANCEL', 'NEXT' (highlighted in blue), and 'FINISH' buttons.

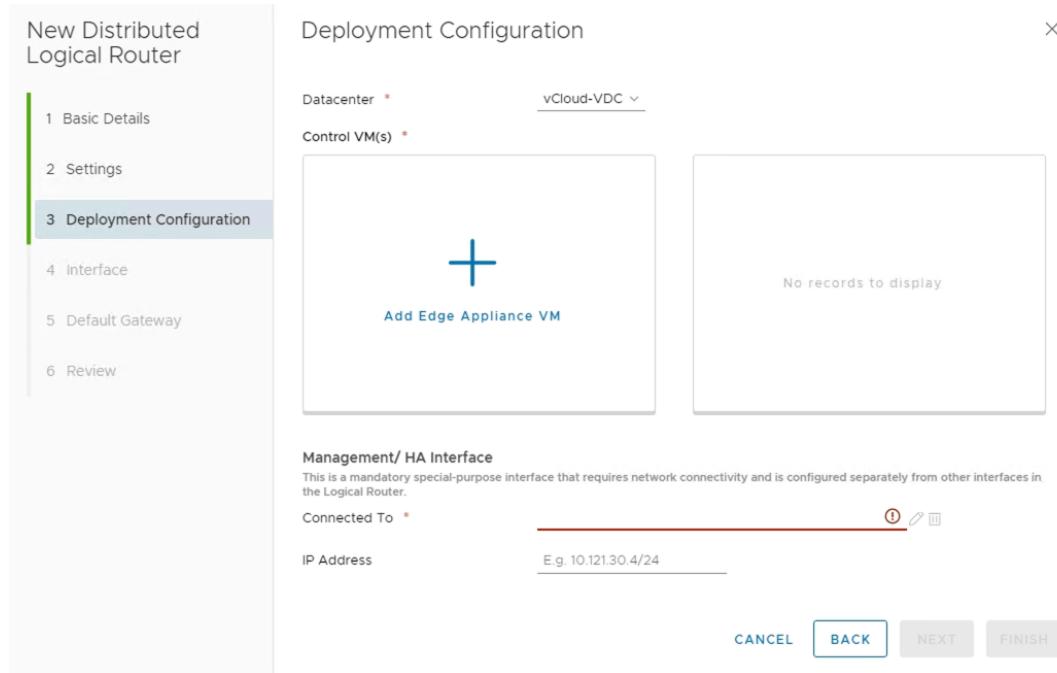
3. Under Settings, select the slider to **enable** SSH access and provide a username and password for the Edge Services Gateway. Click Next. Enabling SSH is for troubleshooting and tcpdump capabilities, if you do not want these features leave SSH disabled.

The screenshot shows the 'Settings' step of the wizard. The left navigation bar highlights step 2, 'Settings'. The main panel shows settings for the Edge Appliance VM(s). It includes fields for User Name (set to 'admin'), Password (set to '*****'), Confirm Password (set to '*****'), SSH access (set to 'Enabled'), and FIPS Mode (set to 'Disabled'). Below these is an 'Edge control level logging' dropdown set to 'Info'. At the bottom right are 'CANCEL', 'BACK', 'NEXT' (highlighted in blue), and 'FINISH' buttons.

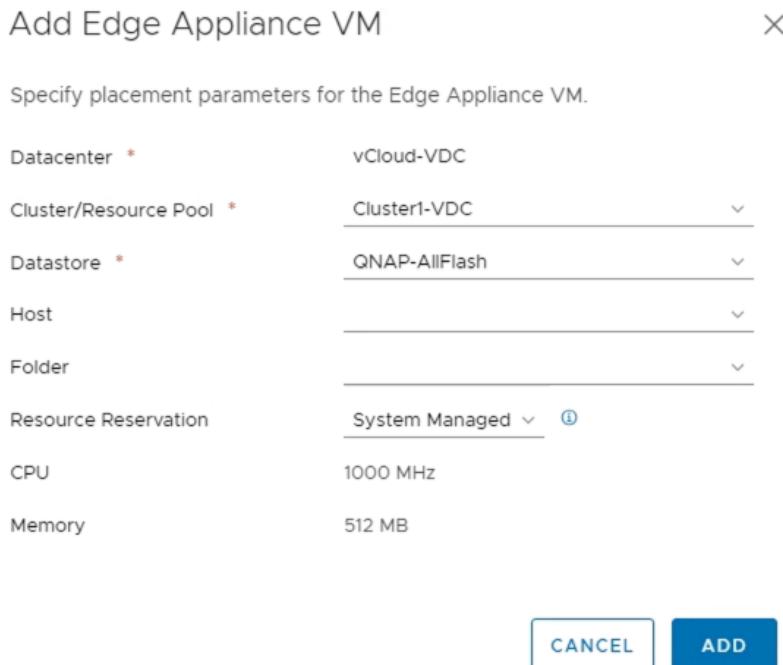
INTEGRATION GUIDE

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

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



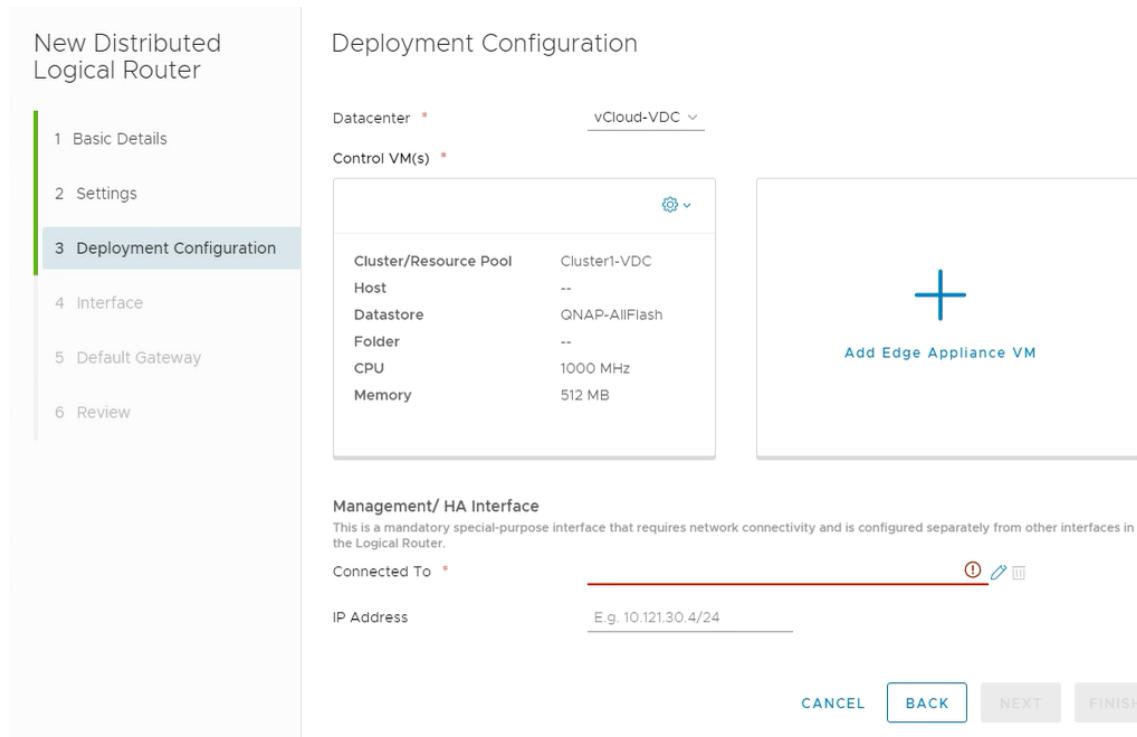
- Selecting plus symbol will display the options in the screenshot below. Choose the appropriate Cluster/resource pool and datastore (for this example, the Cluster1-VDC and the QNAP-AllFlash datastore). The host and folder selection are optional. Click **Add** to complete.



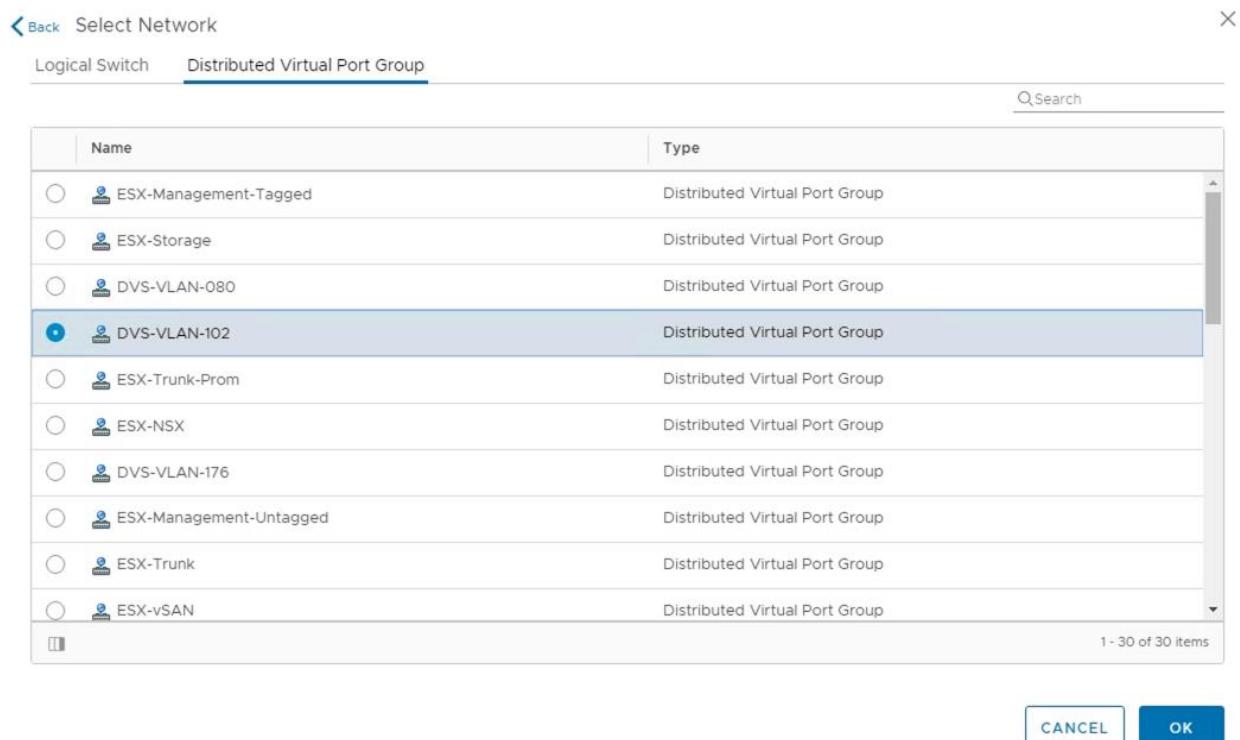
INTEGRATION GUIDE

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

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



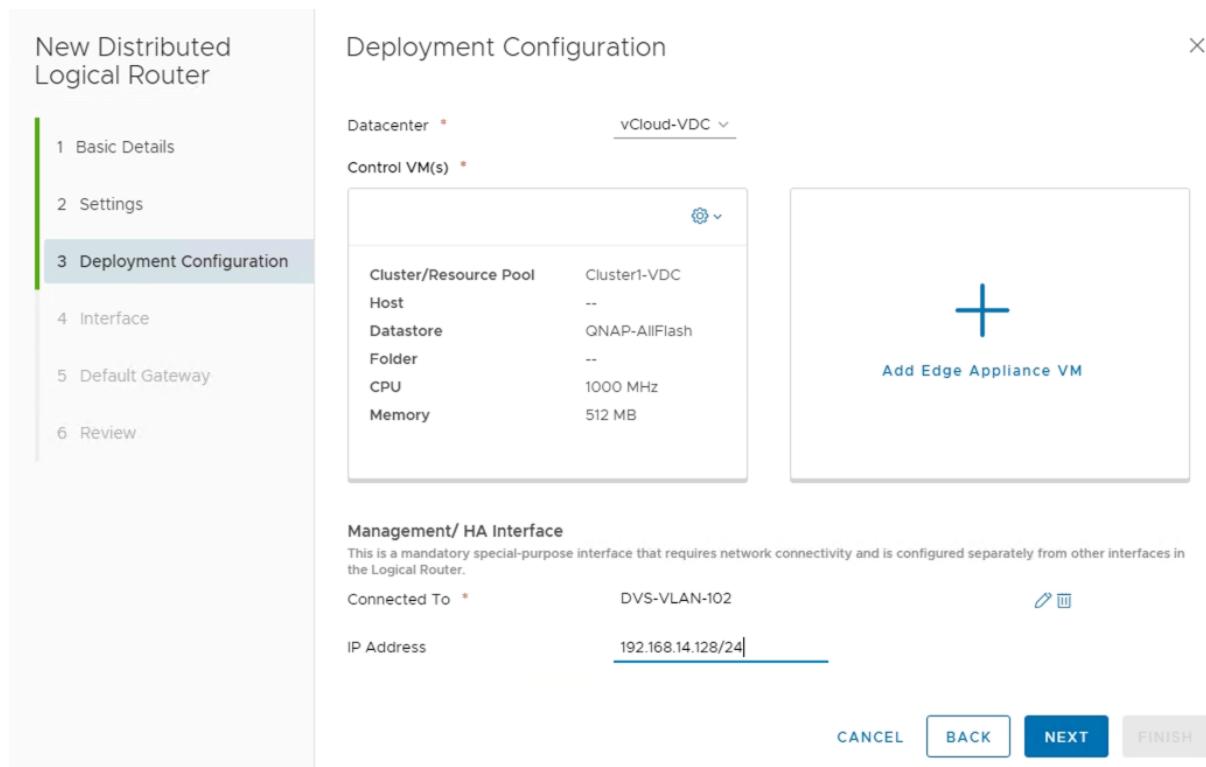
- Select an appropriate Management Network (Distributed Virtual Port Group) to manage the DLR then Click OK



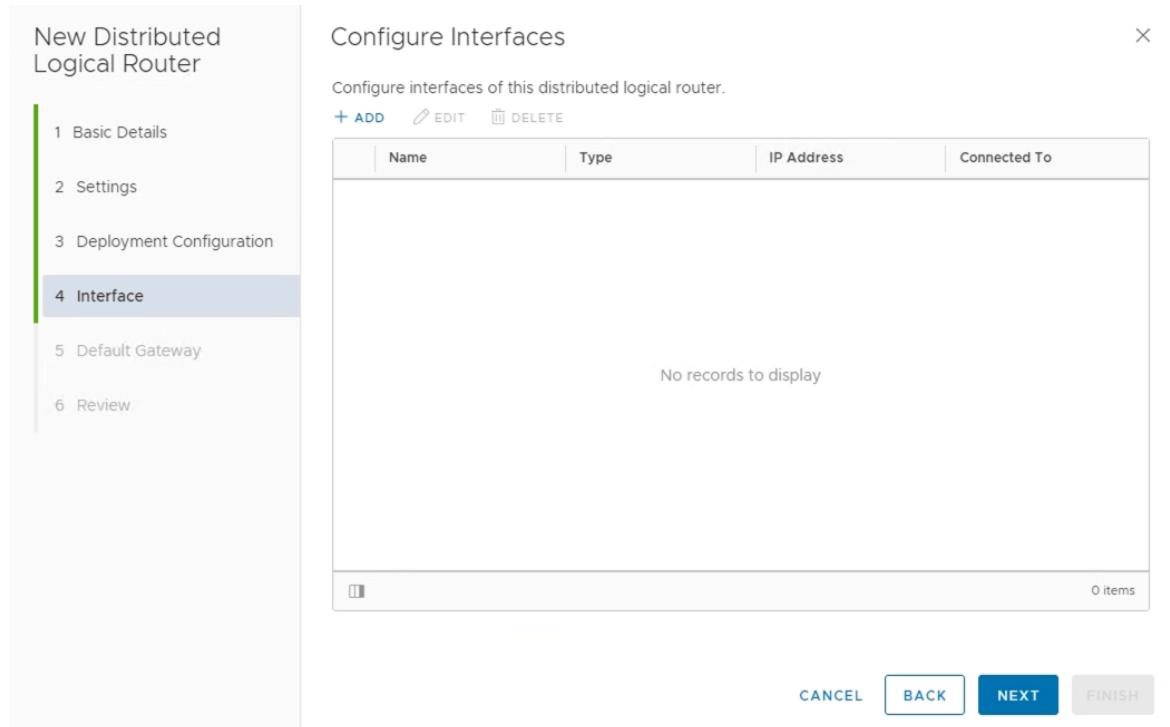
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

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

The screenshot shows the 'Configure Interfaces' dialog box. The 'Name' field is set to 'TransitNet-1'. The 'Type' field is set to 'Uplink'. The 'Connected To' field is highlighted with a red border and contains an edit icon (pencil). The 'Connectivity Status' field is set to 'Connected'. Below these fields are 'Configure Subnets' buttons for '+ ADD' and 'DELETE'. A search bar labeled 'Search' is also present. The main area displays a table for subnet configuration, showing columns for 'Primary IP Address' and 'Subnet Prefix Length'. At the bottom, the 'MTU' value is set to '1500'. In the bottom right corner, there are 'CANCEL' and 'OK' buttons.

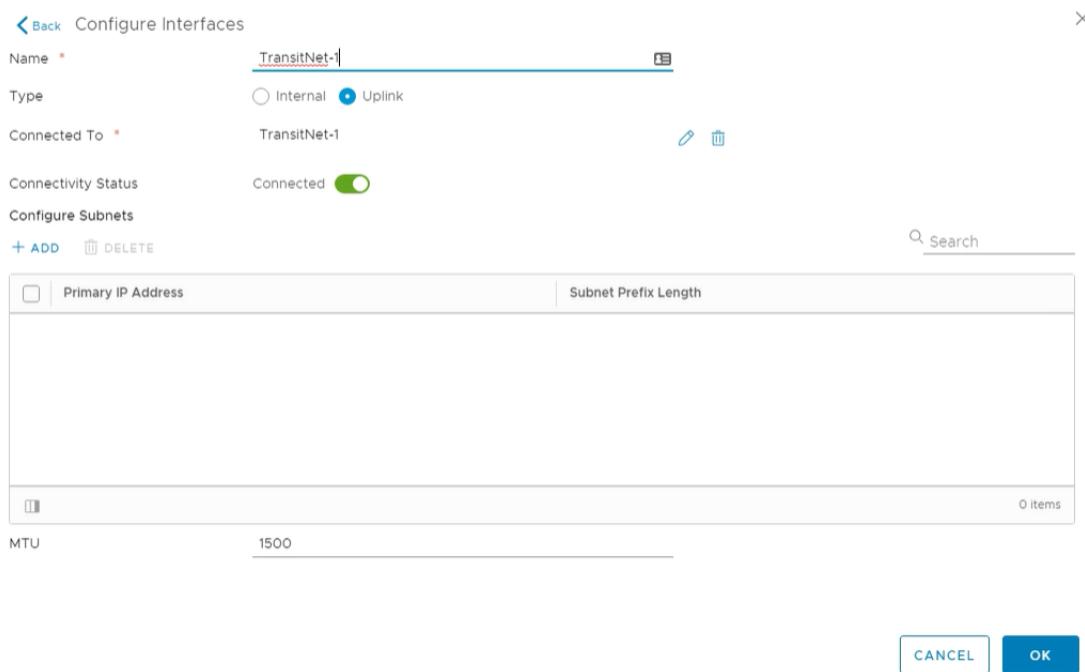
11. For the TransitNet-1 network, click on the Logical Switch tab and then selecting the TransitNet-1 Logical Switch. Click OK.

The screenshot shows the 'Select Network' dialog box with the 'Logical Switch' tab selected. The table lists several logical switches: AppTier, dvs.VCDVSBD-VCD-Internal-e2239cd6-3dd6-4ed2-a024-98c4c80e55d8, TransitNet-1, DBTier, and WebTier. The 'TransitNet-1' row is selected and highlighted with a blue background. The table has columns for 'Name' and 'Type'. A search bar labeled 'Search' is located at the top right. In the bottom right corner, there are 'CANCEL' and 'OK' buttons.

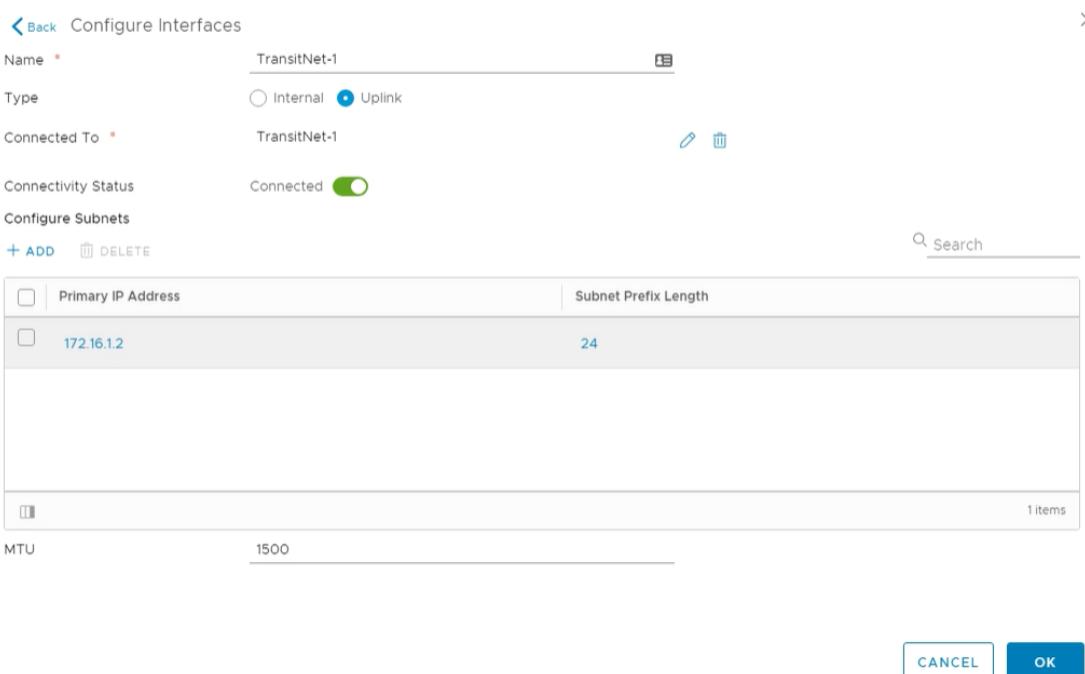
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

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

Configure Interfaces



Configure interfaces of this distributed logical router.

+ ADD EDIT DELETE

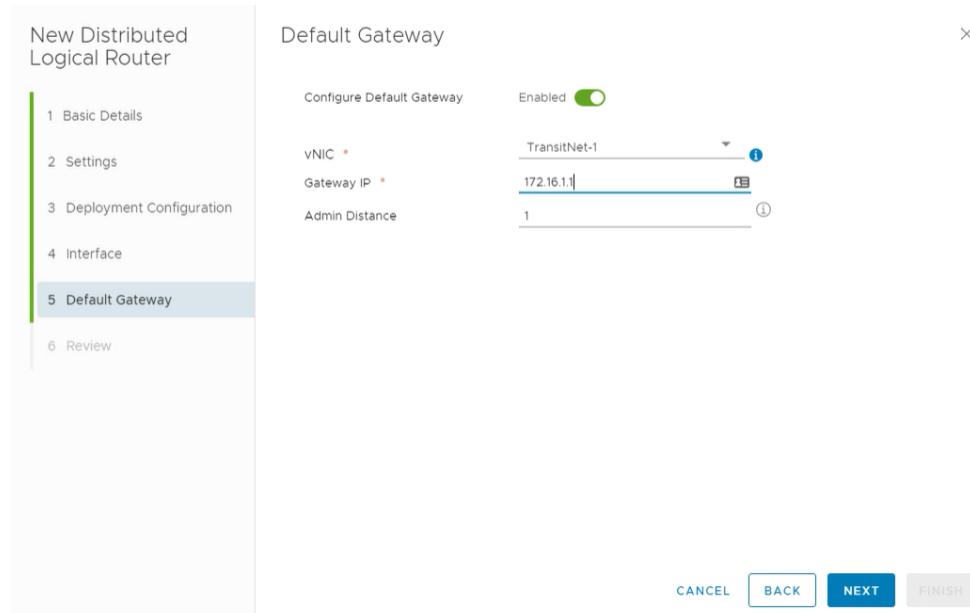
	Name	Type	IP Address	Connected To
<input type="radio"/>	TransitNet-1	Uplink	172.16.1.2/24	TransitNet-1
<input type="radio"/>	WebTier	Internal	10.0.1.1/24	WebTier
<input type="radio"/>	AppTier	Internal	10.0.2.1/24	AppTier
<input type="radio"/>	DBTier	Internal	10.0.3.1/24	DBTier

INTEGRATION GUIDE

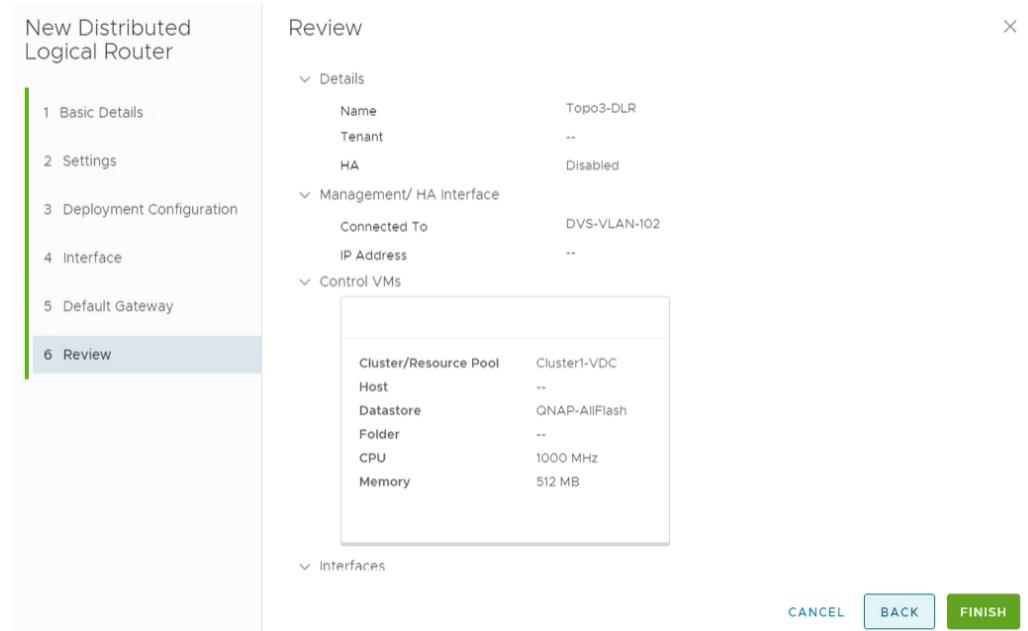
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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.



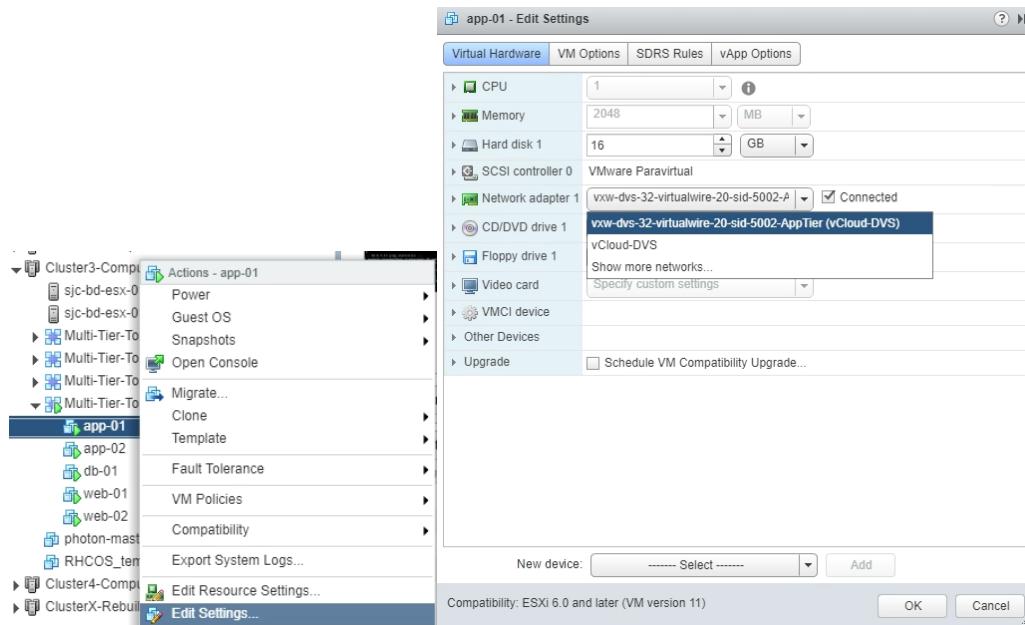
17. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

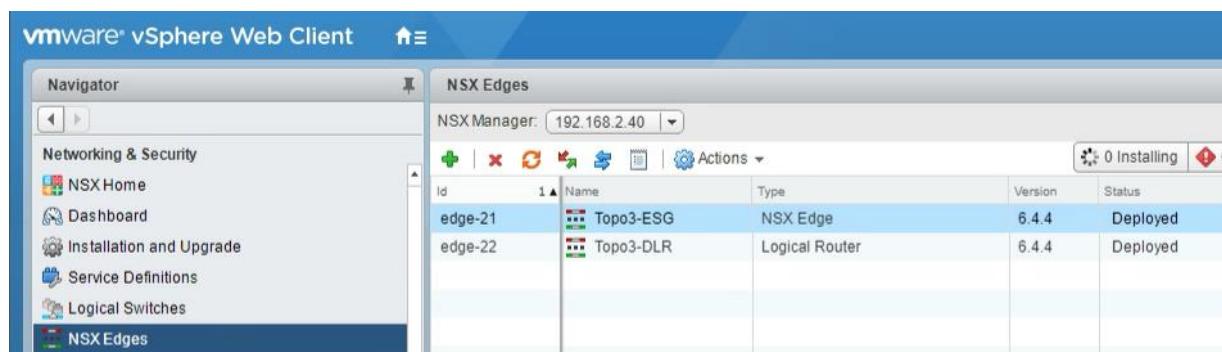
NSX Edge Static Routing Configuration

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)

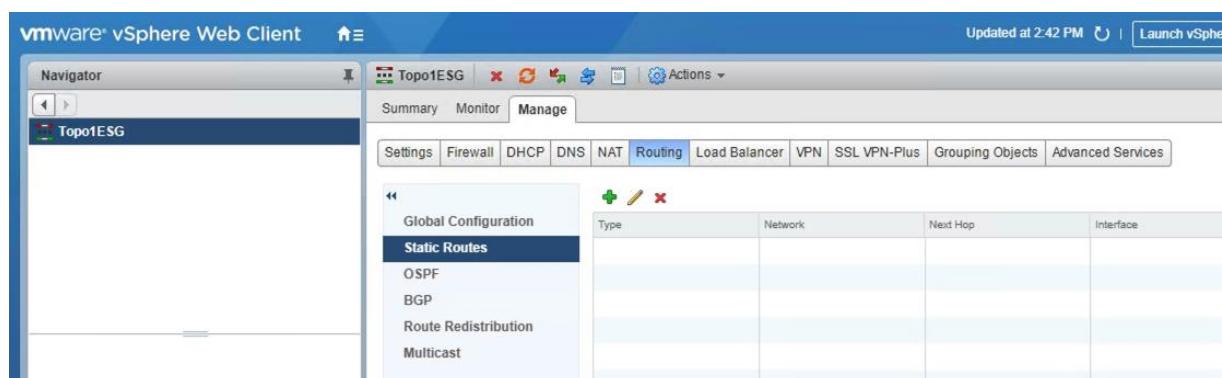
Currently this must be done in the vSphere Web Client (FLEX) [Flash Based] as the functionality hasn't been ported to the HTML5 Client.



The screenshot shows the vSphere Web Client interface. The left sidebar has a 'Navigator' section with 'Networking & Security' expanded, showing 'NSX Home', 'Dashboard', 'Installation and Upgrade', 'Service Definitions', 'Logical Switches', and 'NSX Edges'. The 'NSX Edges' item is selected. The main panel is titled 'NSX Edges' and shows a table with two entries:

ID	Name	Type	Version	Status
edge-21	Topo3-ESG	NSX Edge	6.4.4	Deployed
edge-22	Topo3-DLR	Logical Router	6.4.4	Deployed

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.



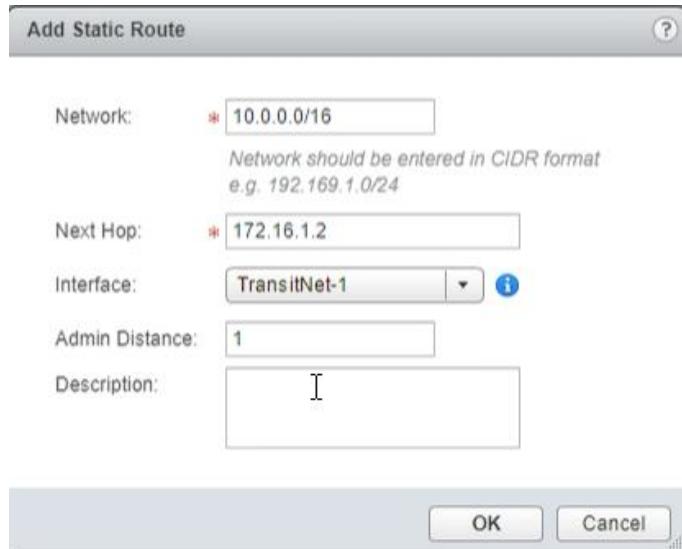
The screenshot shows the vSphere Web Client interface for the 'Topo1ESG' NSX Edge. The left sidebar shows 'Topo1ESG' selected. The main panel has tabs: 'Summary', 'Monitor', and 'Manage'. Under 'Manage', the 'Routing' tab is selected. On the left, there's a sidebar with 'Global Configuration' and 'Static Routes' selected. The main area shows a table for 'Static Routes':

Type	Network	Next Hop	Interface

INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

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.

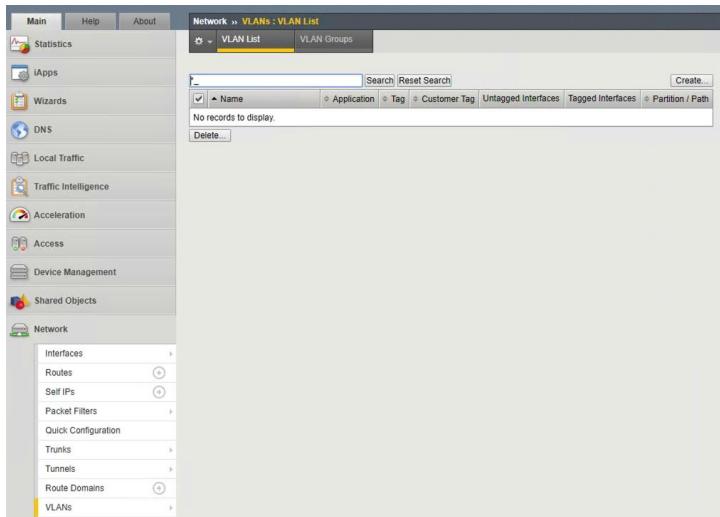
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

INTEGRATION GUIDE

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

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

Name:	AppTier
Description:	(empty)
Tag:	(empty)
Interface:	1.2
Tagging:	Untagged
Interfaces	
1.1 (untagged)	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Configuration:	Basic
Source Check	<input type="checkbox"/>
MTU	1500
sFlow	
Polling Interval	Default
Sampling Rate	Default
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

INTEGRATION GUIDE

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

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.

The screenshot shows the 'New VLAN...' configuration dialog box. It is divided into several sections:

- General Properties:** Contains fields for Name (WebTier), Description, and Tag.
- Resources:** Contains a table for defining interfaces. The 'Interfaces' column lists '1.3' and '1.2 (untagged)'. The 'Tagging' dropdown is set to 'Untagged'. An 'Add' button is available to add more interfaces.
- Configuration:** Contains fields for Source Check (unchecked) and MTU (1500).
- sFlow:** Contains fields for Polling Interval (Default) and Sampling Rate (Default).
- Buttons:** At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

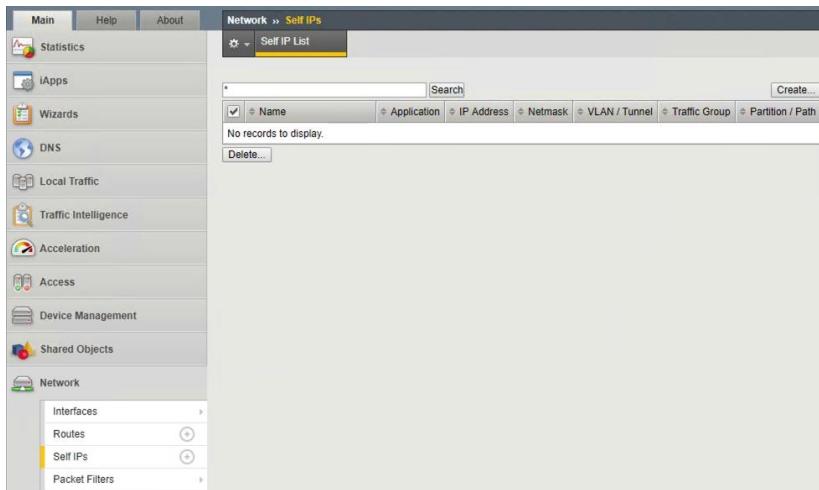
INTEGRATION GUIDE

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

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

Name	App-Self-IP
IP Address	10.0.2.2
Netmask	255.255.255.0
VLAN / Tunnel	AppTier
Port Lockdown	Allow None
Traffic Group	Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

INTEGRATION GUIDE

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

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.

Network >> Self IPs >> New Self IP...

Configuration	
Name	Web-Self-IP
IP Address	10.0.1.2
Netmask	255.255.255.0
VLAN / Tunnel	WebTier
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Network >> Self IPs

*	Search						
<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	App-Self-IP		10.0.2.2	255.255.255.0	AppTier	traffic-group-local-only	Common
<input type="checkbox"/>	Web-Self-IP		10.0.1.2	255.255.255.0	WebTier	traffic-group-local-only	Common

INTEGRATION GUIDE

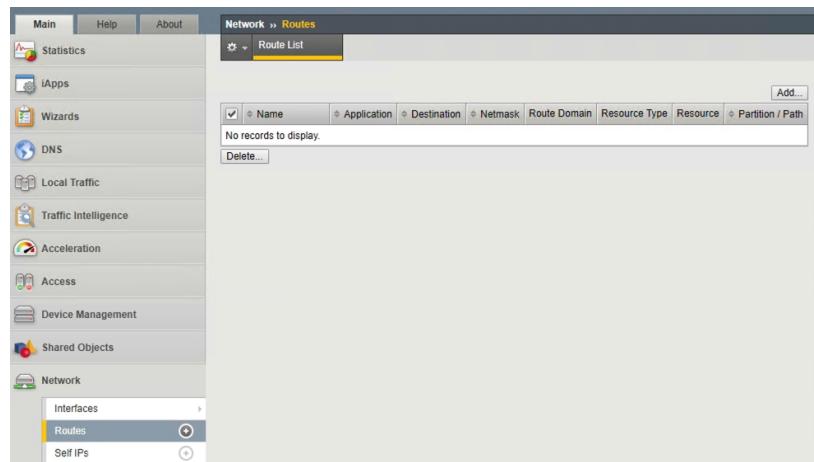
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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

Name	default
Description	(empty)
Destination	0.0.0.0
Netmask	0.0.0.0
Resource	Use Gateway...
Gateway Address	IP Address: 10.0.1.1
MTU	(empty)

At the bottom are three buttons: Cancel, Repeat, and Finished.

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

INTEGRATION GUIDE

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

Local Traffic > Pools : Pool List > New Pool...

Configuration: Basic ▾

Name	WebServerPool				
Description					
Health Monitors	<table border="1"><tr><td>Active</td><td>Available</td></tr><tr><td>/Common gateway_icmp</td><td>/Common http http_head_f5 https https_443</td></tr></table>	Active	Available	/Common gateway_icmp	/Common http http_head_f5 https https_443
Active	Available				
/Common gateway_icmp	/Common http http_head_f5 https https_443				

Resources

Load Balancing Method	Round Robin															
Priority Group Activation	Disabled															
New Members	<p><input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node</p> <p>Node Name: <input type="text"/> (Optional)</p> <p>Address: <input type="text" value="10.0.1.12"/></p> <p>Service Port: <input type="text" value="443"/> <input type="button" value="HTTPS"/></p> <p><input type="button" value="Add"/></p> <table border="1"><thead><tr><th>Node Name</th><th>Address/FQDN</th><th>Service Port</th><th>Auto Populate</th><th>Priority</th></tr></thead><tbody><tr><td>10.0.1.11</td><td>10.0.1.11</td><td>443</td><td></td><td>0</td></tr><tr><td>10.0.1.12</td><td>10.0.1.12</td><td>443</td><td></td><td>0</td></tr></tbody></table> <p><input type="button" value="Edit"/> <input type="button" value="Delete"/></p>	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
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												

INTEGRATION GUIDE

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

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

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.0.1.11	10.0.1.11	8443	0	0
10.0.1.12	10.0.1.12	8443	0	0

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.

Status	Name	Description	Application	Members	Partition / Path
Green Circle	AppServerPool			2	Common
Green Circle	WebServerPool			2	Common

INTEGRATION GUIDE

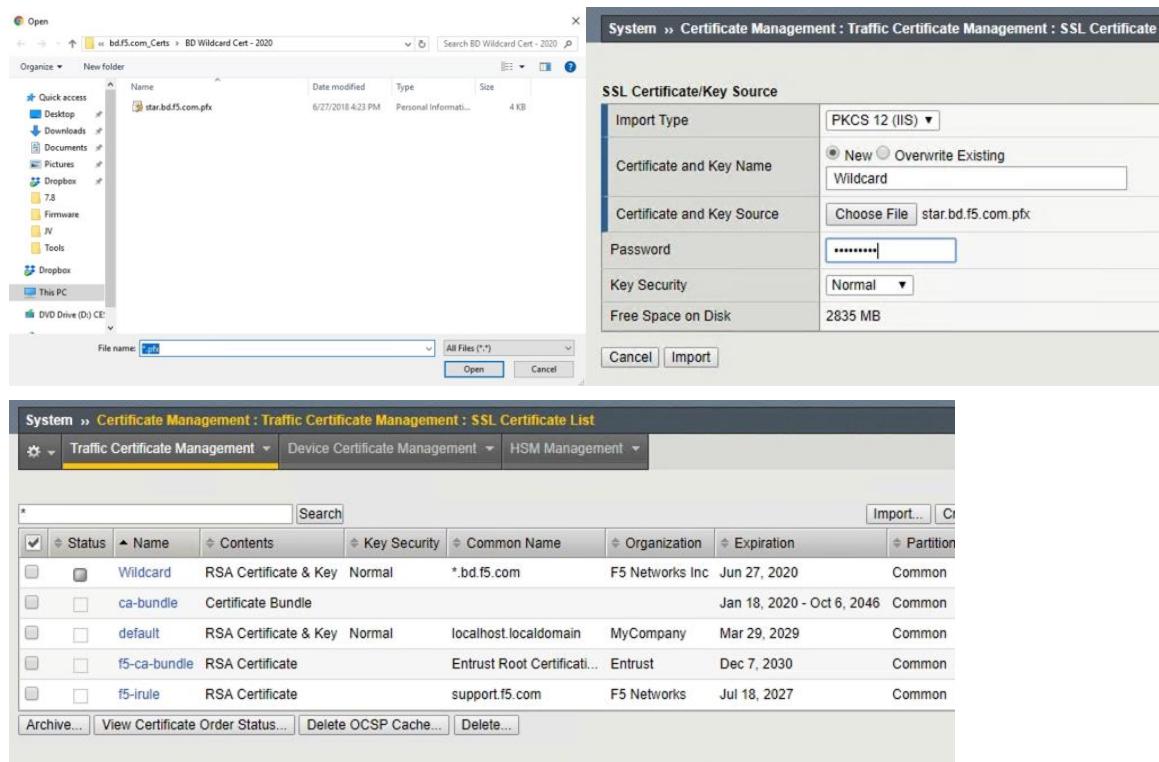
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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



INTEGRATION GUIDE

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

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.

The screenshot shows the F5 Management Interface for creating a new Client SSL Profile. It consists of three main windows:

- Top Window (New Client SSL Profile...):** Shows the "General Properties" section with "Name" set to "WildcardSSL" and "Parent Profile" set to "clientssl". The "Configuration" dropdown is set to "Basic". A "Custom" checkbox is checked. Below this is a "Certificate Key Chain" section with an empty list and "Add", "Edit", and "Delete" buttons.
- Middle Window (Add SSL Certificate Key Chain):** A modal dialog with fields for "Certificate" (set to "Wildcard"), "Key" (set to "Wildcard"), "Chain" (set to "Wildcard"), and "Passphrase" (empty). It has "Add" and "Cancel" buttons.
- Bottom Window (New Client SSL Profile...):** Shows the updated "General Properties" section with the "Certificate Key Chain" field now containing the entry "/Common/Wildcard /Common/Wildcard /Common/Wildcard". The "Custom" checkbox is still checked.

INTEGRATION GUIDE

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

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

The screenshot displays the configuration interface for creating a new Virtual Server. The General Properties tab is active, showing the following details:

- Name: Web-VIP
- Description: (empty)
- Type: Standard
- Source Address: Host Address List (selected), Address: 10.0.1.5
- Destination Address/Mask: Host Address List (selected), Address: 10.0.1.5
- Service Port: Port List (selected), Port: 443 / HTTPS
- Notify Status to Virtual Address: checked
- State: Enabled

The Resources tab shows the following configurations:

- iRules: A list of available profiles including _sys_APM_ExchangeSupport_OA_BasicAuth, _sys_APM_ExchangeSupport_OA_NtlmAuth, _sys_APM_ExchangeSupport_helper, and _sys_APM_ExchangeSupport_main. One profile is enabled.
- Policies: A list of available profiles including _Common_. One profile is enabled.
- Default Pool: WebServerPool (selected)
- Default Persistence Profile: None
- Fallback Persistence Profile: None

The Configuration tab shows the following settings:

- Protocol: TCP (selected)
- Protocol Profile (Client): tcp (selected)
- Protocol Profile (Server): (Use Client Profile) (selected)
- HTTP Profile (Client): None (selected)
- HTTP Profile (Server): (Use Client Profile) (selected)
- HTTP Proxy Connect Profile: None (selected)
- FTP Profile: None (selected)
- RTSP Profile: None (selected)
- SSL Profile (Client): Selected: /Common/WildcardSSL (moved from Available)
- SSL Profile (Server): Selected: /Common/serverssl-insecure-compatible (moved from Available)
- SMTPS Profile: None (selected)
- POP3 Profile: None (selected)
- Client LDAP Profile: None (selected)
- Server LDAP Profile: None (selected)
- Service Profile: None (selected)
- Source Address Translation: Auto Map (selected)

INTEGRATION GUIDE

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

4. In the New Virtual Server menus

- In the Name field, provide a unique name for the app application. In this case, we used App-VIP.
- In the Destination Address field, enter 10.0.1.6
- For Service Port use the standard HTTPS port 8443.
- In the Configuration section
 - Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
 - Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
 - Select Auto Map from the pull-down menus for the Source Address Translation.
- In the Resources section
 - Select the AppServerPool from the Default Pool dropdown box.
 - 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.
- 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.

	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
<input checked="" type="checkbox"/>		App-VIP			10.0.1.6	8443	Standard	Edit...	Common
<input checked="" type="checkbox"/>		Web-VIP			10.0.1.5	443 (HTTPS)	Standard	Edit...	Common

INTEGRATION GUIDE

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

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.

The screenshot shows the F5 BIG-IP Local Traffic - Network Map interface. On the left, there are two main nodes: 'App-VIP' (status green) and 'Web-VIP' (status green). Under 'App-VIP', there are three sub-nodes: '10.0.1.6:8443', '10.0.2.11:8443', and '10.0.2.12:8443'. Under 'Web-VIP', there are three sub-nodes: '10.0.1.5:443', 'WebServerPool' (status green), and '10.0.1.11:443' and '10.0.1.12:443' (status green). On the right, a 'NSXWebApp Properties' dialog box is open. It shows the host name as 'NSXWebApp' and the fully qualified domain name as 'NSXWebApp.bd.f5.com'. The IP address is listed as '10.105.176.2'. There are checkboxes for 'Update associated pointer (PTR) record' and 'Delete this record when it becomes stale'. A 'Record time stamp' field is present. The 'Time to live (TTL)' is set to '0 : 1 : 0 : 0'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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.

The screenshot shows two browser tabs. Both tabs have the URL <https://nsxwebapp.bd.f5.com/cgi-bin/app.py>. The left tab is titled 'Customer Database Access' and shows 'Accessed via: F5-VIP', 'AppServer is: app-01', and a 'Name Filter' input field. The right tab is also titled 'Customer Database Access' and shows 'Accessed via: F5-VIP', 'AppServer is: app-02', and a 'Name Filter' input field. Below each tab is a table with columns 'Rank', 'Name', 'Universe', and 'Revenue'. The left table's data is:

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

The right table's data is:

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

The screenshot shows a terminal session with two curl commands. The first command, run on the left, connects to 'app-01' and shows the response: 'It works!' and 'Connection #0 to host nsxwebapp.bd.f5.com left intact'. The second command, run on the right, connects to 'app-02' and shows the same response. The prompt at the bottom is '[mmabis@hnz-lin-mmabis ~]\$'.

```
< Connection: keep-alive
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< X-Upstream-Server: web-01
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host nsxwebapp.bd.f5.com left intact
[mmabis@hnz-lin-mmabis ~]$ 
[mmabis@hnz-lin-mmabis ~]$ 
< Connection: keep-alive
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< X-Upstream-Server: web-02
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host nsxwebapp.bd.f5.com left intact
[mmabis@hnz-lin-mmabis ~]$ 
```

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

INTEGRATION GUIDE

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

Topology 4: OVSDB Integration with NSX-V

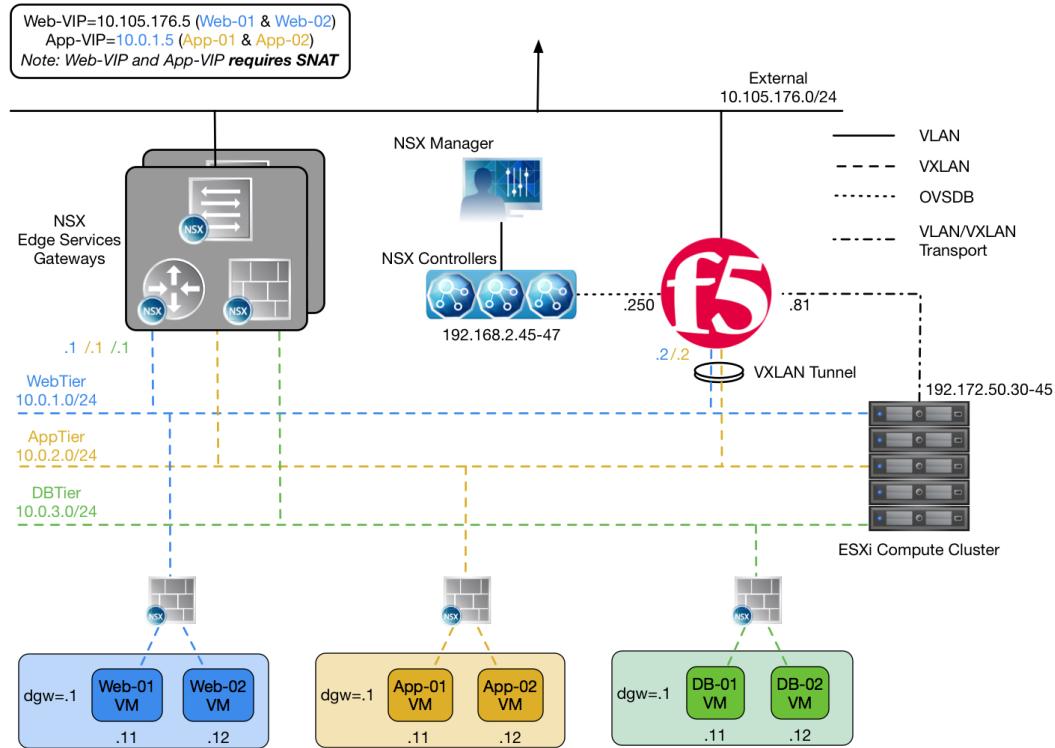


Figure 14 OVSDB Integration with NSX-V

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.

INTEGRATION GUIDE

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

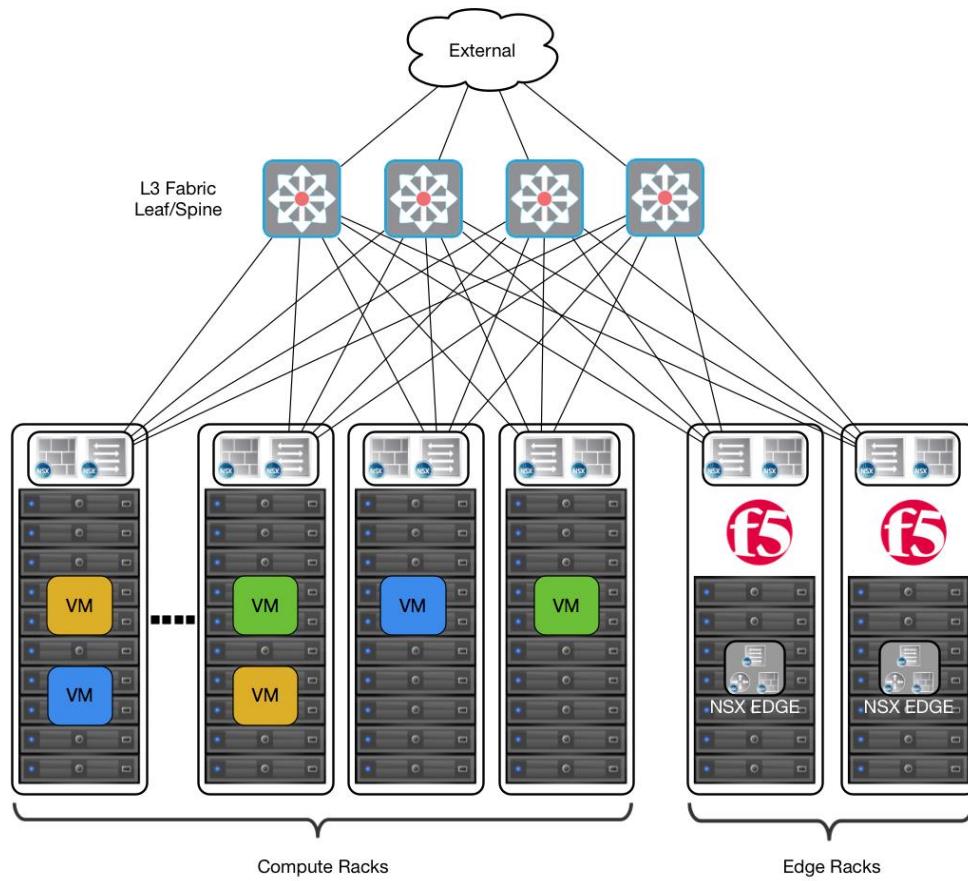


Figure 15 Leaf/spine physical rack infrastructure

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.**

INTEGRATION GUIDE

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

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

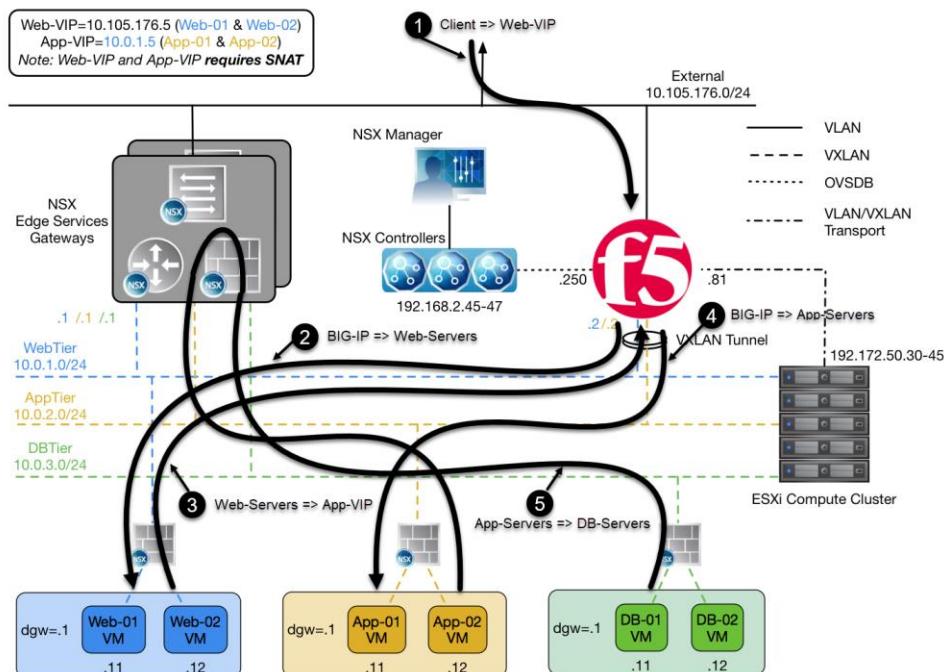


Figure 16 North-South Logical Traffic Flow “OVSDB Integration with NSX-T” with BIG-IP Appliance

INTEGRATION GUIDE

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

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.

INTEGRATION GUIDE

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

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

INTEGRATION GUIDE

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

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.

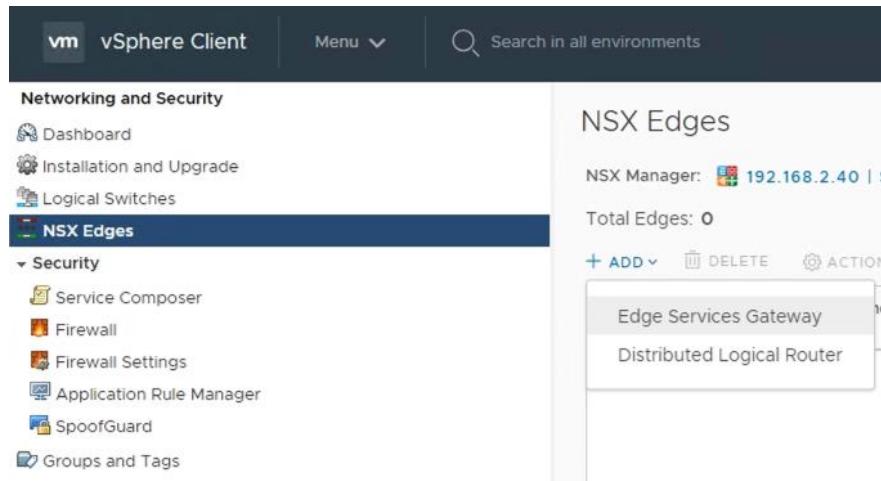
- **VXLAN 5001 WebTier** is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5002 AppTier** is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5003 DBTier**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

INTEGRATION GUIDE

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

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.

The screenshot shows the "New Edge Services Gateway" wizard with the following steps listed on the left:

- 1 Basic Details
- 2 Settings
- 3 Deployment Configuration
- 4 Interface
- 5 Default Gateway
- 6 Firewall Default Policy
- 7 Review

The "Basic Details" step is active, showing the following fields:

Name	TOPO4-ESG
Host Name	
Tenant	
Description	

Below the fields, there is a section titled "Select Deployment Options" with two checkboxes:

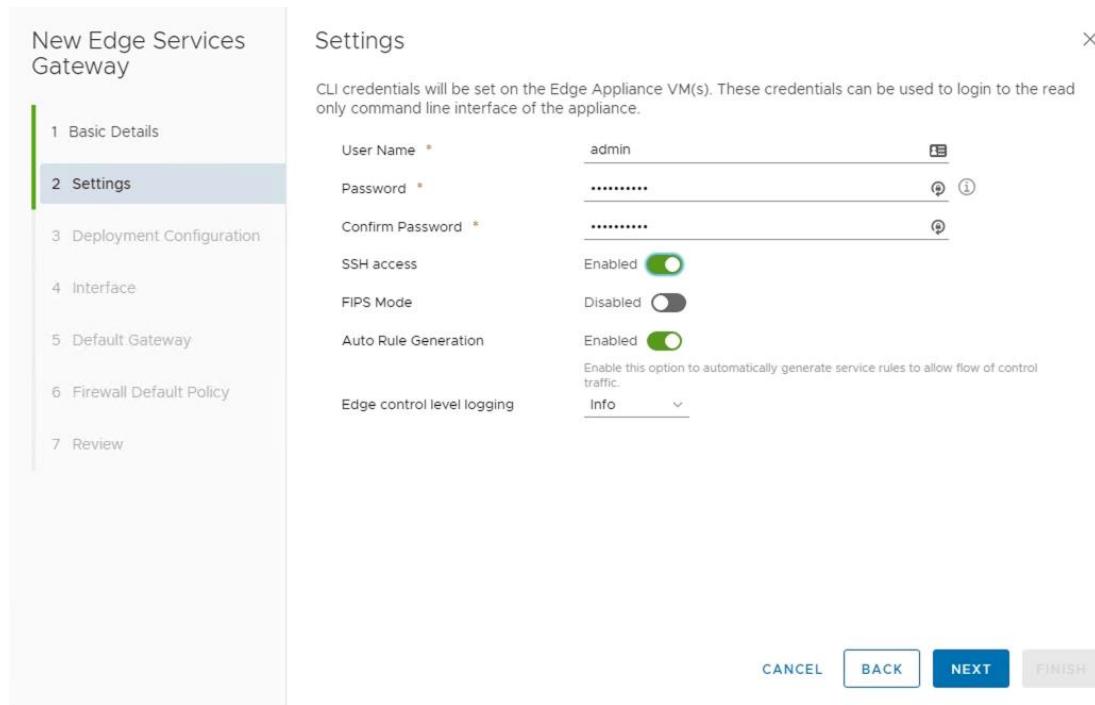
- Deploy Edge Appliance VM
Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.
- High Availability
Enable this option for enabling and configuring High Availability.

At the bottom right are buttons: CANCEL, NEXT (highlighted in blue), and FINISH.

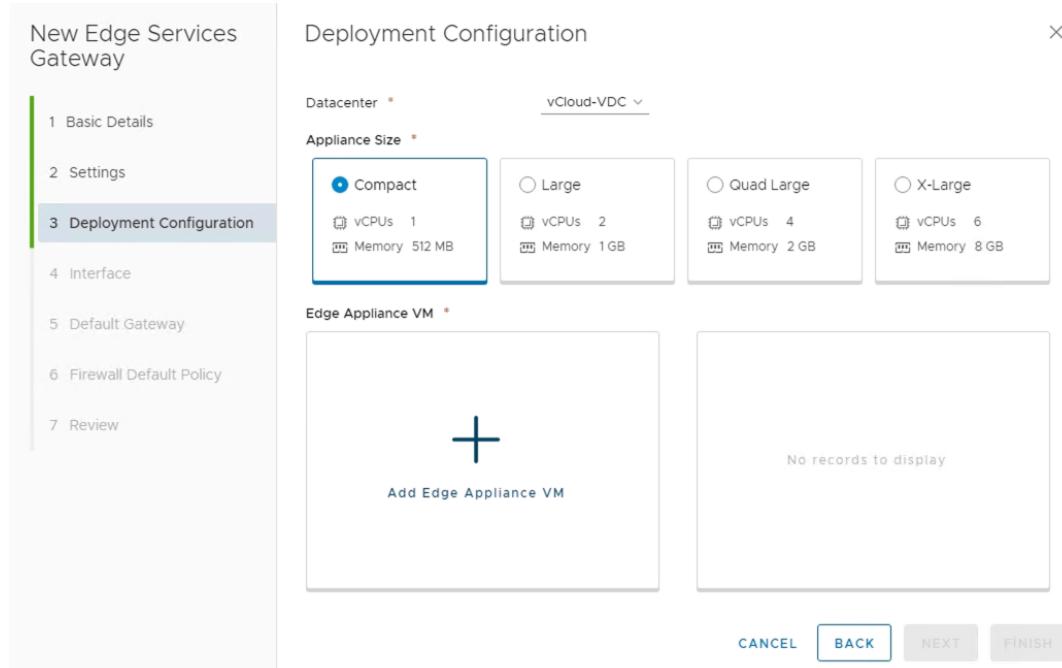
INTEGRATION GUIDE

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

- 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.



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



INTEGRATION GUIDE

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

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.

Add Edge Appliance VM X

Specify placement parameters for the Edge Appliance VM.

Datacenter *	vCloud-VDC
Cluster/Resource Pool *	Cluster1-VDC
Datastore *	QNAP>AllFlash
Host	
Folder	
Resource Reservation	System Managed ①
CPU	1000 MHz
Memory	512 MB

CANCEL ADD

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

New Edge Services Gateway

Configure Interfaces

Configure interfaces of this edge services gateway.

+ ADD EDIT DELETE

vNIC#	Name	Type	IP Address	Connected To
No records to display				

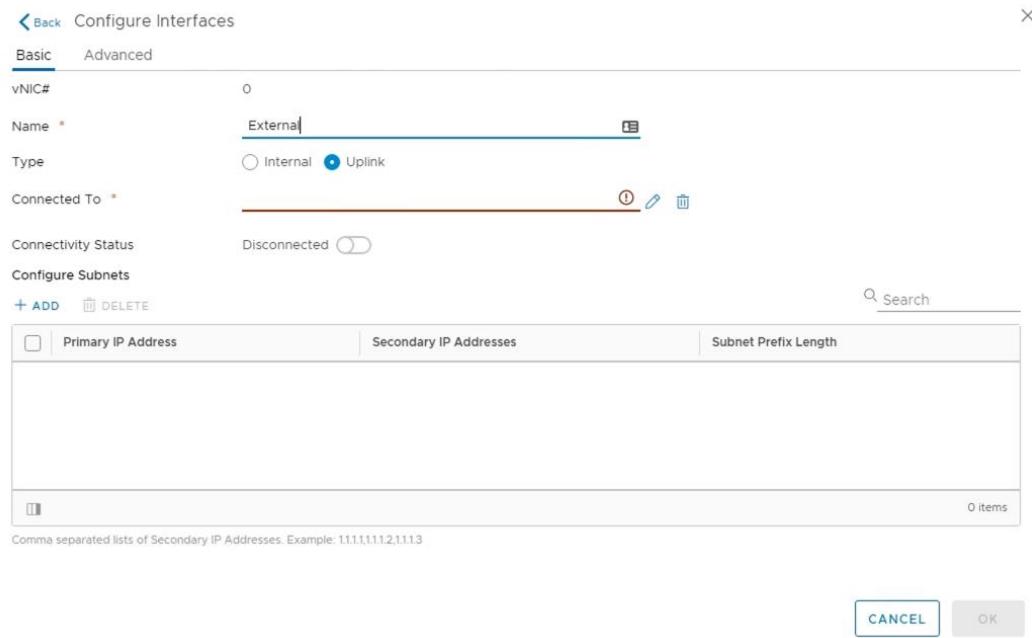
NEXT FINISH

1 Basic Details
2 Settings
3 Deployment Configuration
4 Interface
5 Default Gateway
6 Firewall Default Policy
7 Review

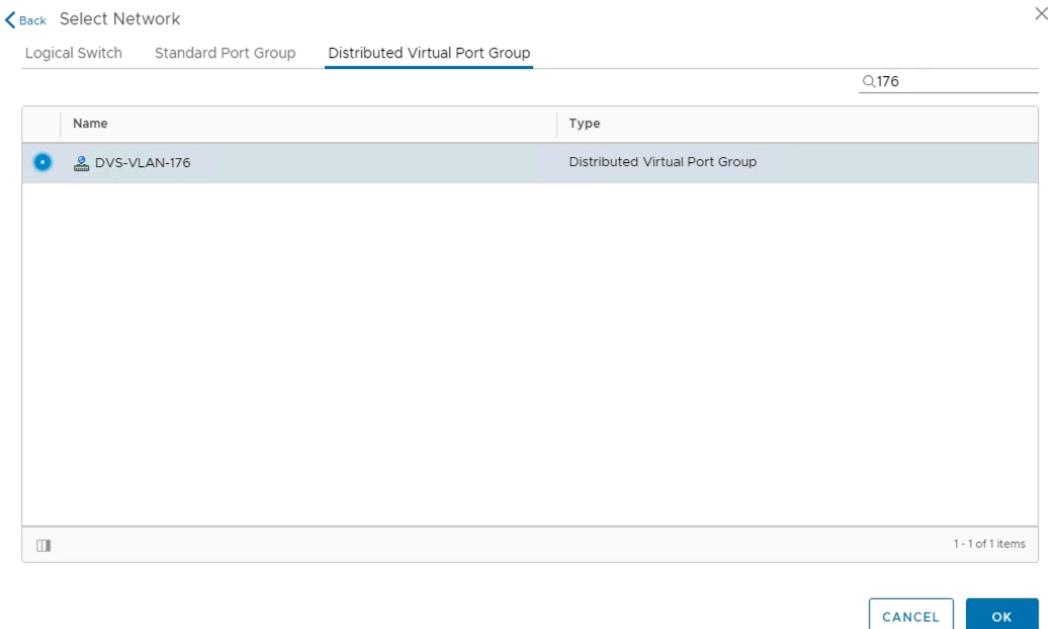
INTEGRATION GUIDE

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

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



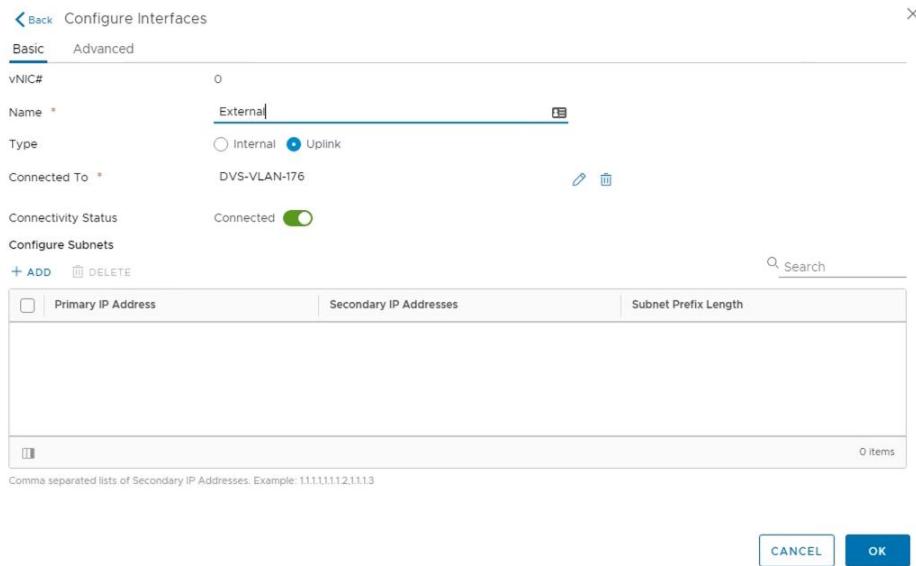
8. For the External network, click on the Distributed Virtual Port Group tab and then selecting the port group used for external access. Click OK.



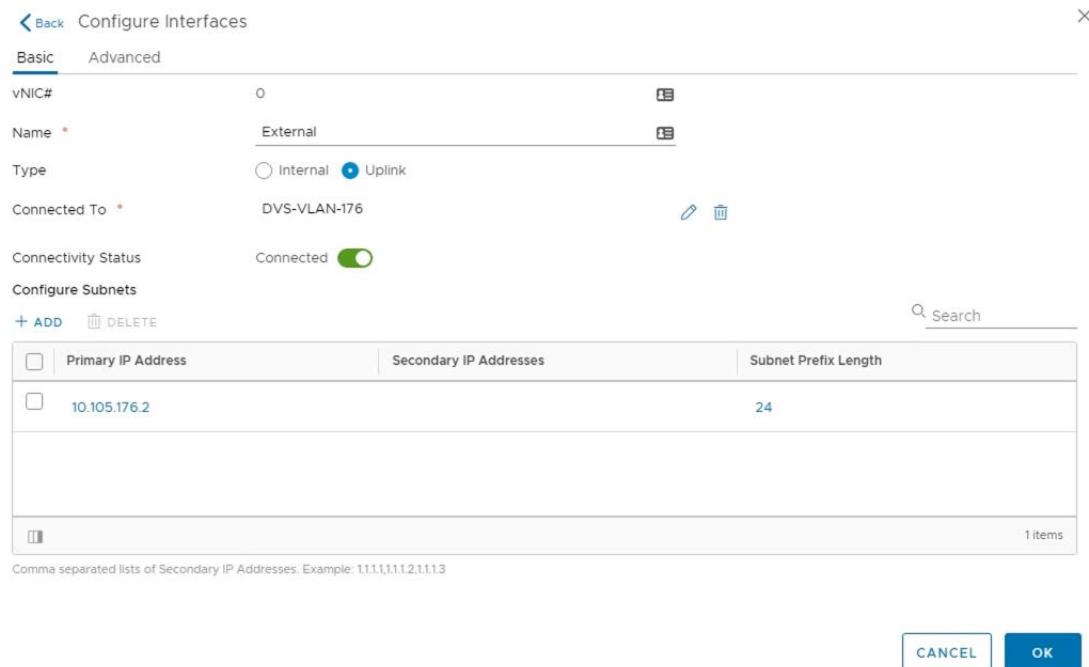
INTEGRATION GUIDE

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

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



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



INTEGRATION GUIDE

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

- 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

vNIC#	Name	Type	IP Address	Connected To	Connection Status	Statistics
0	External	Uplink	10.105.176.2/24	DVS-VLAN-176	Connected	
1	WebTier	Internal	10.0.1.1/24	WebTier	Connected	
2	AppTier	Internal	10.0.2.1/24	AppTier	Connected	
3	DBTier	Internal	10.0.3.1/24	DBTier	Connected	

- 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.

New Edge Services Gateway

Default Gateway

Configure Default Gateway

Enabled

vNIC *

Gateway IP *

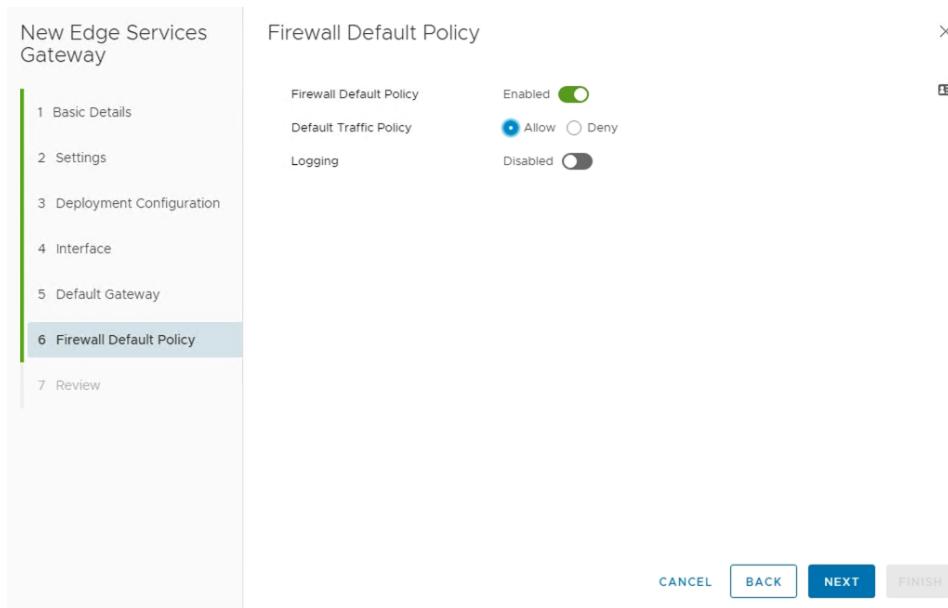
Admin Distance

NEXT FINISH

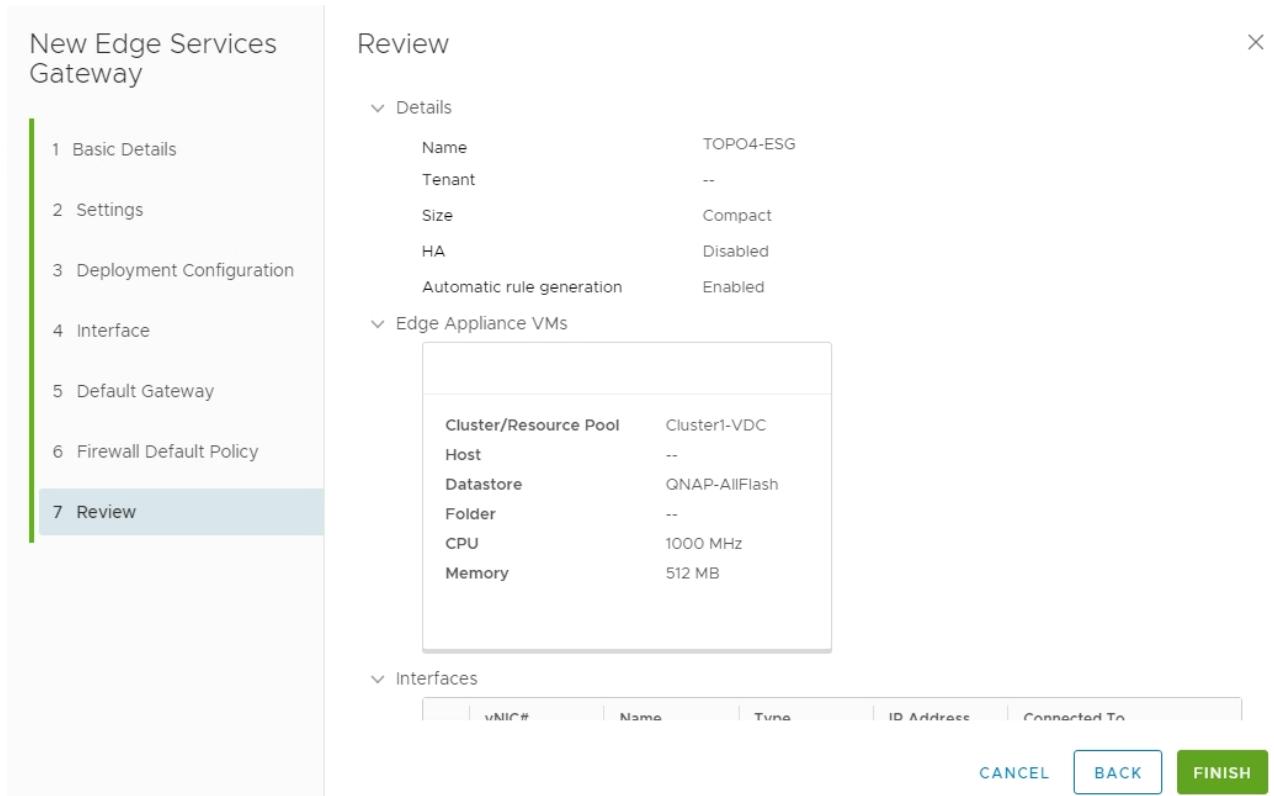
INTEGRATION GUIDE

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

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)



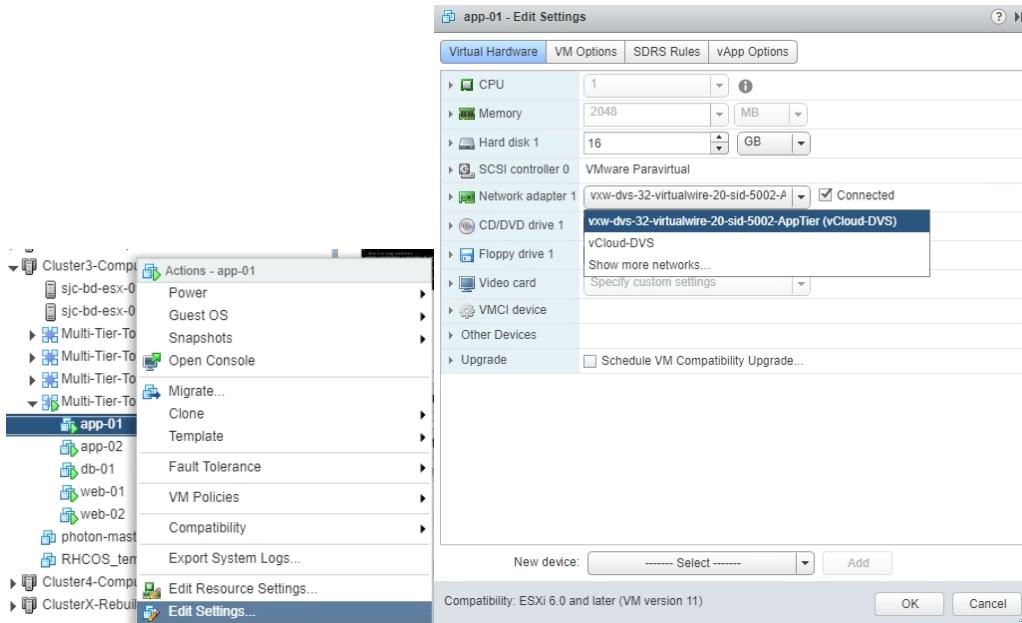
14. Review and click Finish to complete the deployment of the NSX Edge.



INTEGRATION GUIDE

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

- 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.



- 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.

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	App-To-DB	User	AppTier	DBTier	HTTP	Accept
3	Default Rule	Default	any	any	any	Deny

INTEGRATION GUIDE

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

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.

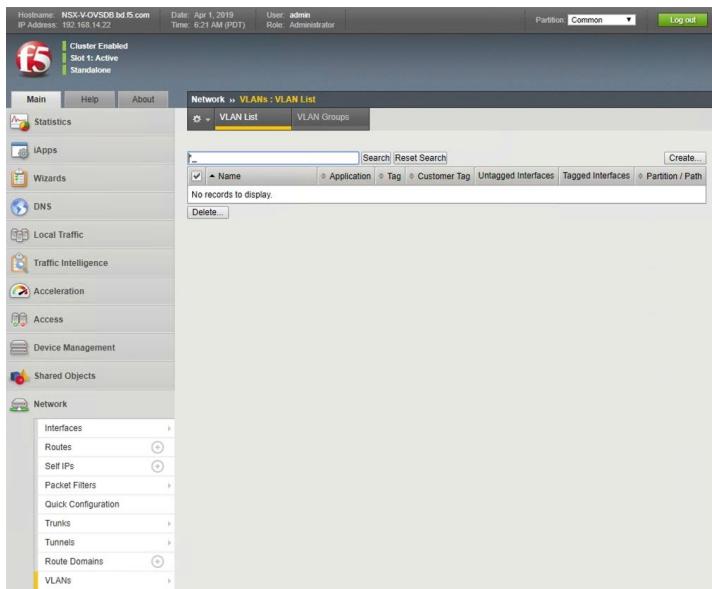
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

INTEGRATION GUIDE

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

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.

Name	External
Description	
Tag	176
Customer Tag	None

Interface:	1/1.10
Tagging:	Tagged
Add	
1/1.1 (tagged,service)	
Edit	Delete

Source Check	<input type="checkbox"/>
MTU	1500

Polling Interval	Default
Sampling Rate	Default

Buttons: Cancel, Repeat, Finished

INTEGRATION GUIDE

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

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.

Network > VLANs : VLAN List > New VLAN...

General Properties

Name	VTEP
Description	
Tag	50
Customer Tag	None

Resources

Interfaces	Interface: 1/1.10 Tagging: Tagged Add 1/1.1 (tagged.service) Edit Delete
------------	--

Configuration: Basic

Source Check	<input type="checkbox"/>
MTU	1600

sFlow

Polling Interval	Default
Sampling Rate	Default

Buttons: Cancel | Repeat | Finished

INTEGRATION GUIDE

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

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.

Network > VLANs : VLAN List > New VLAN...

General Properties

Name	NSX-CTRL
Description	
Tag	102
Customer Tag	None

Resources

Interfaces	Interface: 1/1.10 Tagging: Tagged <input type="button" value="Add"/> 1/1.1 (tagged,service) <input type="button" value="Edit"/> <input type="button" value="Delete"/>
------------	---

Configuration: Basic

Source Check	<input type="checkbox"/>
MTU	1500

sFlow

Polling Interval	Default
Sampling Rate	Default

Network > VLANs : VLAN List

VLAN List

*	Name	Application	Tag	Customer Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input checked="" type="checkbox"/>	External	176			1/1.1		Common
<input checked="" type="checkbox"/>	NSX-CTRL	102			1/1.1		Common
<input checked="" type="checkbox"/>	VTEP	50			1/1.1		Common

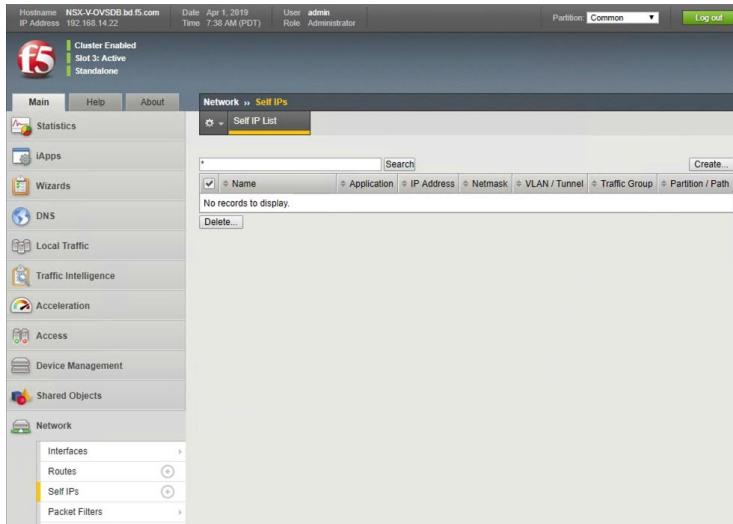
INTEGRATION GUIDE

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

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

Network » Self IPs » New Self IP...

Configuration	
Name	External-Self <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/>
IP Address	10.105.176.10
Netmask	255.255.255.0
VLAN / Tunnel	External <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/>
Port Lockdown	Allow None <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/>
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating) <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/>
Service Policy	None <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/>

INTEGRATION GUIDE

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

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

The screenshot shows the 'Network > Self IPs > New Self IP...' configuration dialog. The 'Name' field is set to 'NSX-CTRL-Self'. The 'IP Address' is '192.168.2.250'. The 'Netmask' is '255.255.0.0'. The 'VLAN / Tunnel' dropdown is set to 'NSX-CTRL'. The 'Port Lockdown' dropdown is set to 'Allow Default'. The 'Traffic Group' section contains a checked checkbox 'Inherit traffic group from current partition / path' with a dropdown menu showing 'traffic-group-local-only (non-floating)'. The 'Service Policy' dropdown is set to 'None'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

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

The screenshot shows the 'Network > Self IPs > New Self IP...' configuration dialog. The 'Name' field is set to 'VTEP-Self'. The 'IP Address' is '192.172.50.81'. The 'Netmask' is '255.255.255.0'. The 'VLAN / Tunnel' dropdown is set to 'VTEP'. The 'Port Lockdown' dropdown is set to 'Allow None'. The 'Traffic Group' section contains a checked checkbox 'Inherit traffic group from current partition / path' with a dropdown menu showing 'traffic-group-local-only (non-floating)'. The 'Service Policy' dropdown is set to 'None'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

INTEGRATION GUIDE

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

6. Validate the VLAN configuration against the image below.

Network > Self IPs						
Self IP List		Create...				
<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group
<input type="checkbox"/>	External-Self		10.105.176.10	255.255.255.0	External	traffic-group-local-only Common
<input type="checkbox"/>	NSX-CTRL-Self		192.168.2.250	255.255.0.0	NSX-CTRL	traffic-group-local-only Common
<input type="checkbox"/>	VTEP-Self		192.172.50.81	255.255.255.0	VTEP	traffic-group-local-only Common

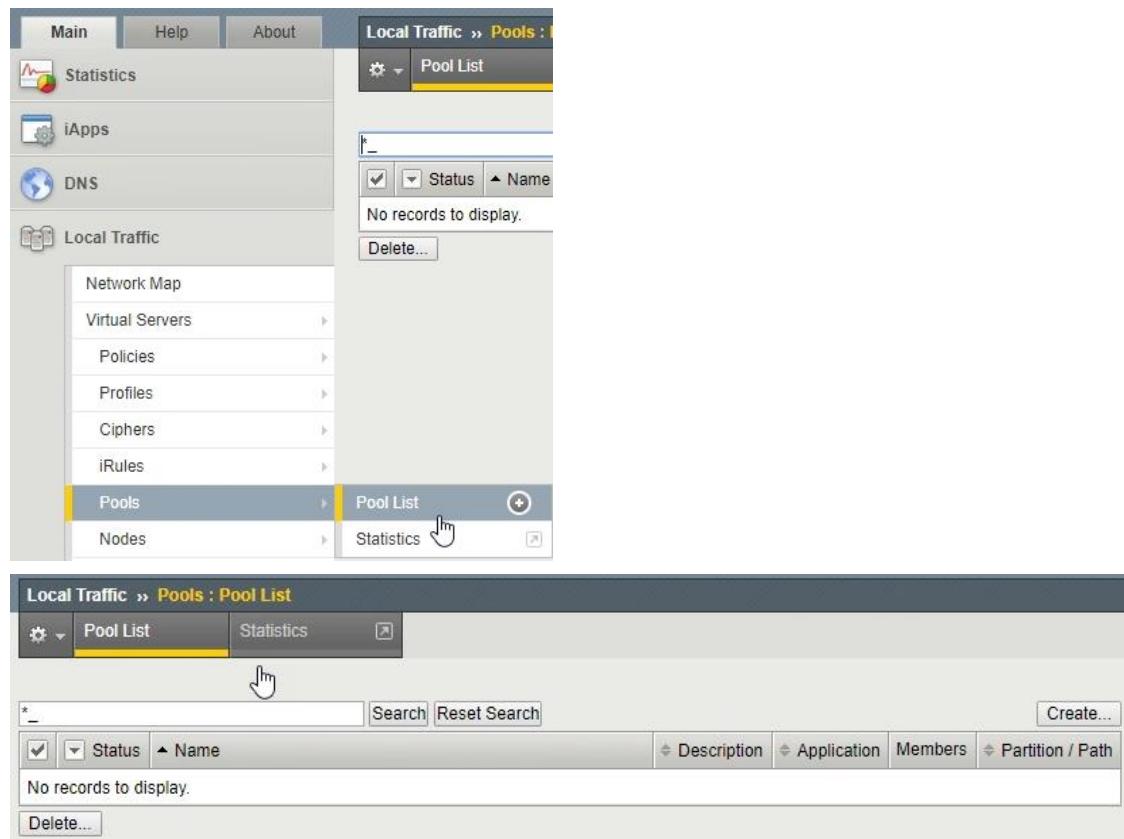
INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

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.

The screenshot shows the configuration screen for creating a new pool named "WebTier-Pool".

Configuration: Basic

Name: WebTier-Pool

Description: (empty)

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:** A table showing two members:

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.0.1.11	10.0.1.11	443	0	0
10.0.1.12	10.0.1.12	443	0	0

Buttons at the bottom: Cancel, Repeat, Finished

INTEGRATION GUIDE

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

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.

The screenshot shows the configuration of a new pool named "AppTier-Pool". The "Health Monitors" section shows "gateway_icmp" moved to the "Active" list. The "Resources" section shows "Round Robin" as the load balancing method. In the "New Members" section, two members are added: "10.0.2.11" and "10.0.2.12", both assigned to service port 8443. The "Finished" button is highlighted.

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.

Name	Description	Application	Members	Partition / Path
AppTier-Pool			2	Common
WebTier-Pool			2	Common

INTEGRATION GUIDE

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

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.



Network > Route Domains								
Route Domain List								
Create...								
Name	Application	ID	Partition Default	Description	Parent Name	VLANs	Protocols	Partition / Path
0	External, VTEP, NSX-CTRL, socks-tunnel, http-tunnel	0	Yes					Common

INTEGRATION GUIDE

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

3. In the New Route Domain menus

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

The screenshot shows the 'New Route Domain...' configuration dialog. It has two main sections: 'General Properties' and 'Configuration'. In 'General Properties', the 'Name' field is set to 'RD-200' and the 'ID' field is set to '200'. In 'Configuration', under 'VLANs', the 'Members' list contains '/Common http-tunnel' and 'socks-tunnel', with a 'BFD' checkbox selected in the 'Available' list. Under 'Dynamic Routing Protocols', 'BFD' is selected in the 'Enabled' list, while 'BGP', 'IS-IS', 'OSPFv2', 'OSPFv3', and 'PIM' are listed in the 'Available' list. Other fields like 'Bandwidth Controller', 'Connection Limit', and 'Eviction Policy' are set to 'None'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

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

The screenshot shows the 'Route Domains' list view. A table displays route domains with columns for Name, Application, ID, Partition Default, Description, Parent Name, VLANs, Protocols, and Partition / Path. Two rows are present: one for '0' (Application: External, VTEP, NSX-CTRL, socks-tunnel, http-tunnel, Protocols: Common) and one for 'RD-200' (ID: 200, Protocols: BFD, Partition / Path: Common). A 'Create...' button is visible at the top right of the table area.

Name	Application	ID	Partition Default	Description	Parent Name	VLANs	Protocols	Partition / Path
0	External, VTEP, NSX-CTRL, socks-tunnel, http-tunnel	0	Yes				Common	
RD-200		200					BFD	Common

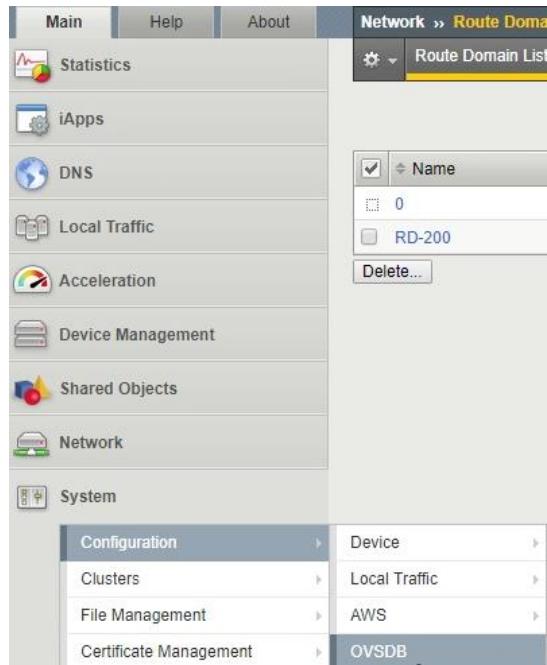
INTEGRATION GUIDE

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

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.



INTEGRATION GUIDE

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

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.

The screenshot shows the configuration interface for the OVSDB module. The top navigation bar includes tabs for System, Configuration, and OVSDB, with OVSDB selected. Below the navigation is a toolbar with Device, Local Traffic, AWS, and OVSDB buttons. The main area is divided into several sections:

- General Properties:** Contains fields for OVSDB (Enable dropdown), Controller Addresses (list box with entries 192.168.2.45, 192.168.2.46, 192.168.2.47, with Add, Edit, and Delete buttons), Flooding Type (Replicator dropdown), Logical Routing Type (None dropdown), Port (6640 input), Tunnel Local Address (192.172.50.81 input), and Tunnel Floating Addresses (a list box with Selected and Available sections and transfer buttons).

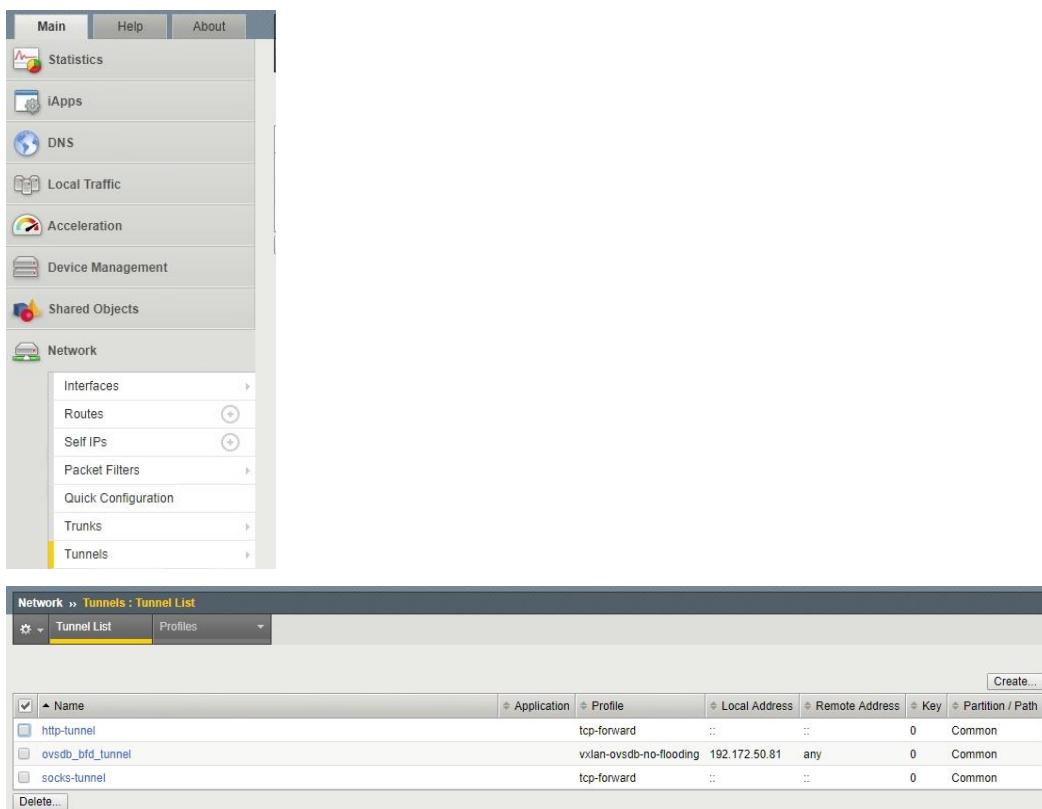
Controller Addresses	<input type="text" value="192.168.2.45"/> <input type="text" value="192.168.2.46"/> <input type="text" value="192.168.2.47"/>						
Tunnel Floating Addresses	<table border="1"><tr><td>Selected</td><td>Available</td></tr><tr><td>[List of addresses]</td><td>[Empty list]</td></tr><tr><td>[Transfer buttons: <<, >>, <>]</td><td></td></tr></table>	Selected	Available	[List of addresses]	[Empty list]	[Transfer buttons: <<, >>, <>]	
Selected	Available						
[List of addresses]	[Empty list]						
[Transfer buttons: <<, >>, <>]							
- Credentials:** Contains fields for Certificate File (default.crt dropdown), Certificate Key File (default.key dropdown), and CA Certificate File (None dropdown).
- BFD Settings:** Contains fields for BFD (Enable dropdown) and Route Domain (RD-200 dropdown).

At the bottom right is a large **Update** button.

INTEGRATION GUIDE

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

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

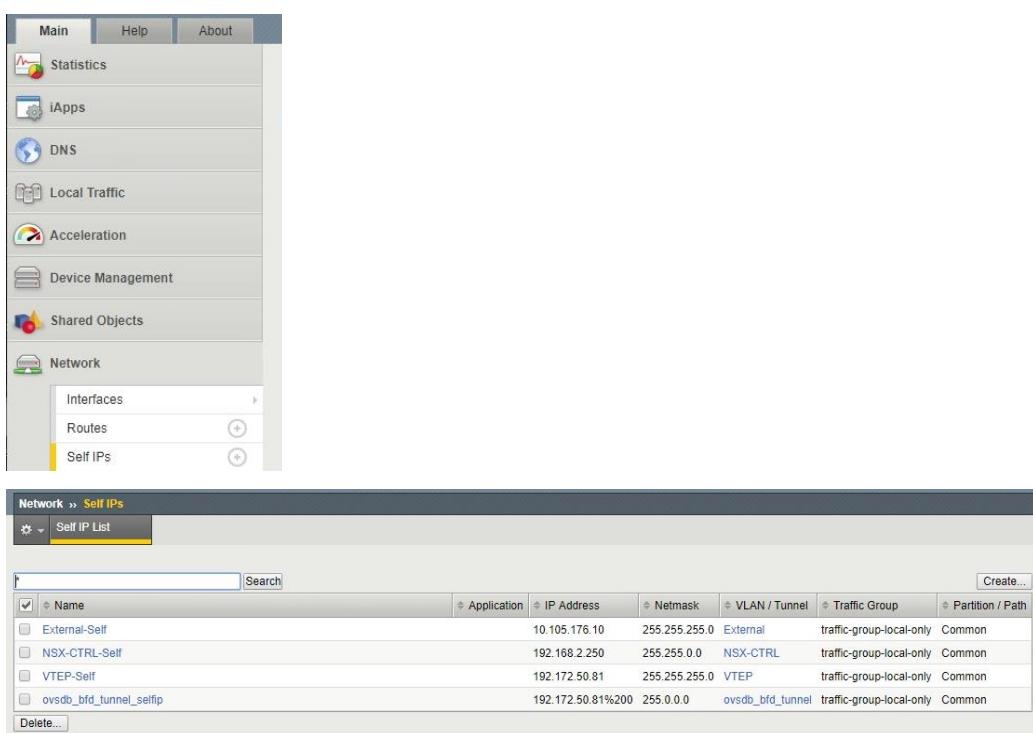


The screenshot shows the F5 BIG-IP management interface. The left sidebar is titled 'Network' and contains links for Interfaces, Routes, Self IPs, Packet Filters, Quick Configuration, Trunks, and Tunnels. The 'Tunnels' link is highlighted with a yellow bar. The main window title is 'Network > Tunnels : Tunnel List'. It has tabs for 'Tunnel List' (which is selected) and 'Profiles'. A 'Create...' button is at the top right. A table lists three tunnels:

Name	Application	Profile	Local Address	Remote Address	Key	Partition / Path
http-tunnel	tcp-forward	0	Common
ovsdb_bfd_tunnel	vxlan-ovsdb-no-flooding	192.172.50.81	any	..	0	Common
socks-tunnel	tcp-forward	0	Common

A 'Delete...' button is at the bottom left of the table.

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



The screenshot shows the F5 BIG-IP management interface. The left sidebar is titled 'Network' and contains links for Interfaces, Routes, and Self IPs. The 'Self IPs' link is highlighted with a yellow bar. The main window title is 'Network > Self IPs : Self IP List'. It has tabs for 'Self IP List' (selected) and 'Profiles'. A 'Create...' button is at the top right. A table lists four self IPs:

Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
External-Self	10.105.176.10	255.255.255.0	External	..	traffic-group-local-only	Common
NSX-CTRL-Self	192.168.2.250	255.255.0.0	NSX-CTRL	..	traffic-group-local-only	Common
VTEP-Self	192.172.50.81	255.255.255.0	VTEP	..	traffic-group-local-only	Common
ovsdb_bfd_tunnel_selfip	192.172.50.81%200	255.0.0.0	ovsdb_bfd_tunnel	..	traffic-group-local-only	Common

A 'Delete...' button is at the bottom left of the table.

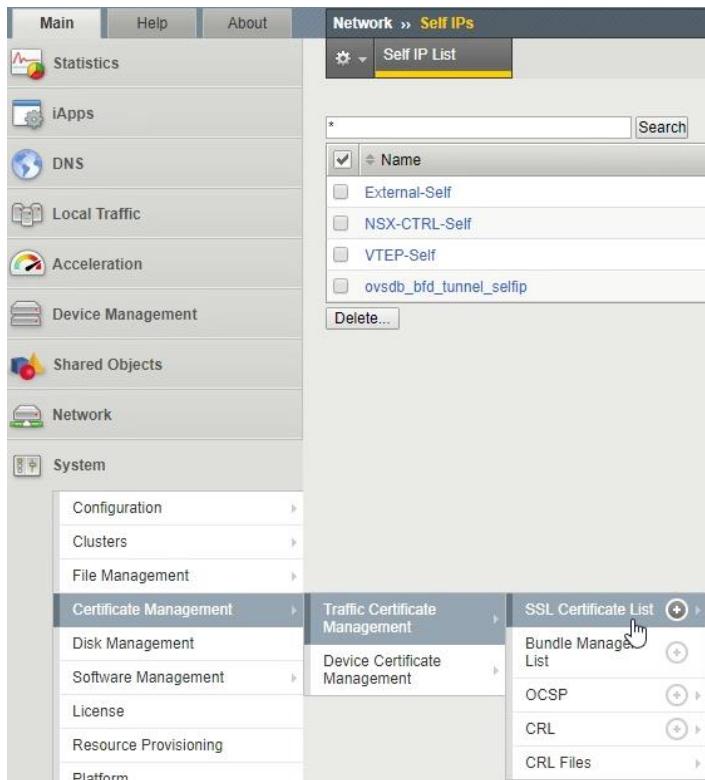
INTEGRATION GUIDE

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

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.



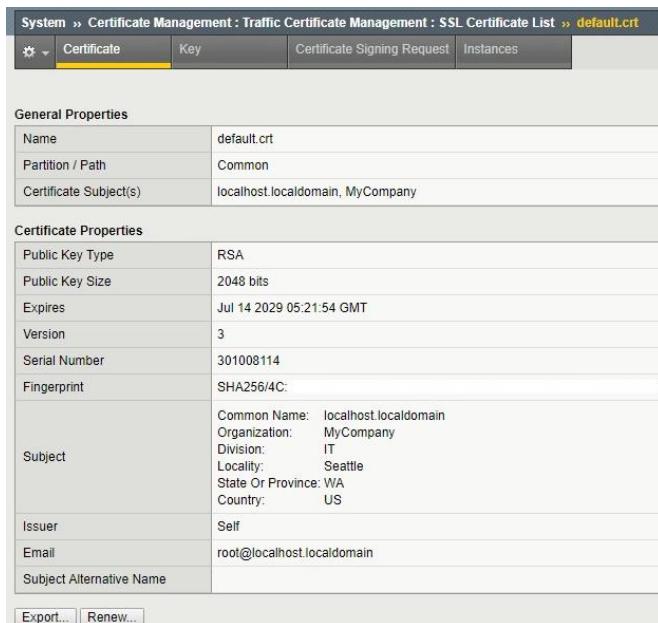
2. Select the certificate used in previous section for configuring OVSDB. In our example we used default.

System > Certificate Management : Traffic Certificate Management : SSL Certificate List						
Traffic Certificate Management		Device Certificate Management				
SSL Certificate List		Bundle Manager		Import... Create...		
Status	Name	Contents	Key Security	Common Name	Organization	Expiration
						Partition / Path
<input type="checkbox"/>	ca-bundle	Certificate Bundle			Dec 31, 2029 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost localdomain	MyCompany	Jul 13, 2029
<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust, Inc.	Dec 7, 2030
<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 18, 2027

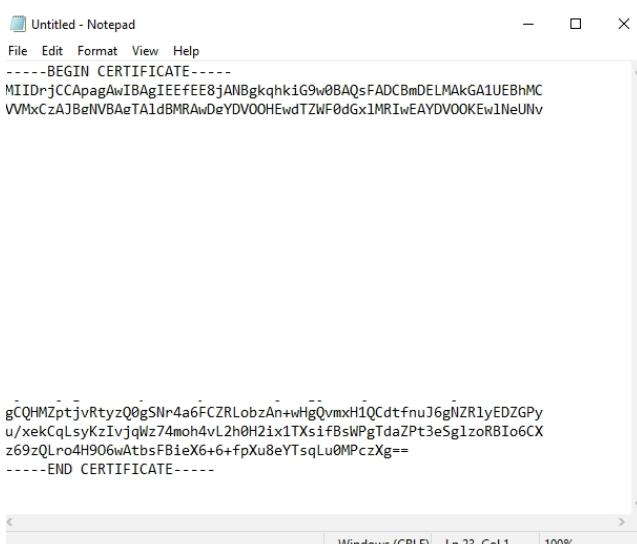
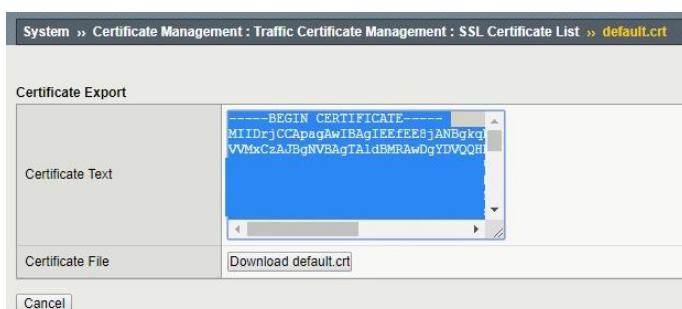
INTEGRATION GUIDE

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

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)**



INTEGRATION GUIDE

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

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.

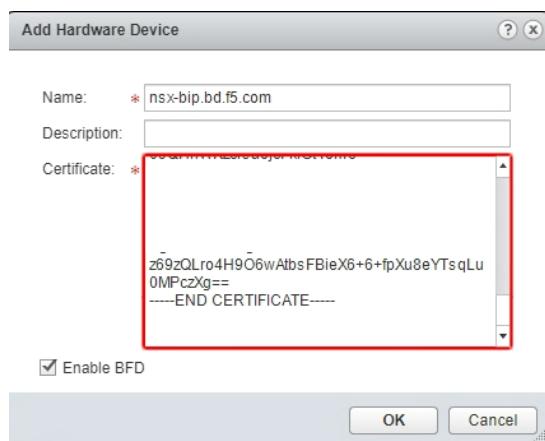
The screenshot shows the VMware vSphere Web Client (Flash) interface. The top navigation bar includes links for Home, Hosts and Clusters, VMs and Templates, Storage, Networking, Content Libraries, Global Inventory Lists, Policies and Profiles, Update Manager, and Networking & Security. The left sidebar has sections for NSX Home, Dashboard, Installation and Upgrade, Service Definitions (selected), Logical Switches, and NSX Edges. The main content area is titled "Service Definitions" and shows tabs for Services, Service Managers, and Hardware Devices (selected). It displays a table for "Hardware Devices" with columns for Name, Management IP Address, Connectivity, and BFD Enabled. A message states "This list is empty." Below this is a "Replication Cluster" section with an "Edit" button and a table for "Hosts". At the bottom is a "BFD Configuration" section with "Status" set to "Enabled" and "Probe interval" set to "300 ms".

INTEGRATION GUIDE

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

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.

The screenshot shows the 'Service Definitions' interface with the 'Hardware Devices' tab selected. A dropdown menu for the 'NSX Manager' is set to '192.168.2.40'. The 'Hardware Devices' table lists one entry:

Name	Management IP Address	Connectivity	BFD Enabled
nsx-bip.bd.f5.com	192.168.2.250	Up	✓

At the bottom right of the table, it says '1 Objects' and has a 'Copy' button.

INTEGRATION GUIDE

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

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

The screenshot shows the Service Definitions interface. At the top, there are tabs for Services, Service Managers, and Hardware Devices. The Hardware Devices tab is selected. It displays a table with one row for the device 'nsx-bip.bd.f5.com'. The columns are Name, Management IP Address, Connectivity, and BFD Enabled. The device name is highlighted in blue. The Management IP Address is 192.168.2.250, Connectivity is Up, and BFD Enabled is checked. Below the table, there is a toolbar with icons for add, edit, delete, and actions, followed by a 'Filter' search bar. At the bottom right of the table area, it says '1 Objects' and has a 'Copy' button. Below the hardware devices section, there is a 'Replication Cluster' section with a 'Hosts' tab and an '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.

The screenshot shows the 'Edit Replication Cluster Configuration' dialog. It has two main sections: 'Available Objects' on the left and 'Selected Objects' on the right. Both sections have a 'Filter' search bar at the top. Under 'Available Objects', there are eight items: sjc-bd-esx-017.bd.f5.com, sjc-bd-esx-018.bd.f5.com, sjc-bd-esx-102.bd.f5.com, sjc-bd-esx-103.bd.f5.com, sjc-bd-esx-105.bd.f5.com, sjc-bd-esx-106.bd.f5.com, sjc-bd-esx-107.bd.f5.com, and sjc-bd-esx-108.bd.f5.com. All items have a green checkmark next to them. Under 'Selected Objects', there are also eight items: sjc-bd-esx-108.bd.f5.com, sjc-bd-esx-107.bd.f5.com, sjc-bd-esx-106.bd.f5.com, sjc-bd-esx-105.bd.f5.com, sjc-bd-esx-103.bd.f5.com, sjc-bd-esx-102.bd.f5.com, sjc-bd-esx-018.bd.f5.com, and sjc-bd-esx-017.bd.f5.com. All items have a green checkmark next to them. Between the two sections are two buttons: a double-left arrow and a double-right arrow. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

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

The screenshot shows the 'Replication Cluster' configuration page. At the top right is an 'Edit' button. Below it, there is a 'Hosts' tab which is currently selected. The host list contains several entries, each preceded by an orange icon: sjc-bd-esx-106.bd.f5.com, sjc-bd-esx-105.bd.f5.com, sjc-bd-esx-107.bd.f5.com, sjc-bd-esx-102.bd.f5.com, sjc-bd-esx-018.bd.f5.com, sjc-bd-esx-017.bd.f5.com, sjc-bd-esx-016.bd.f5.com, and sjc-bd-esx-015.bd.f5.com.

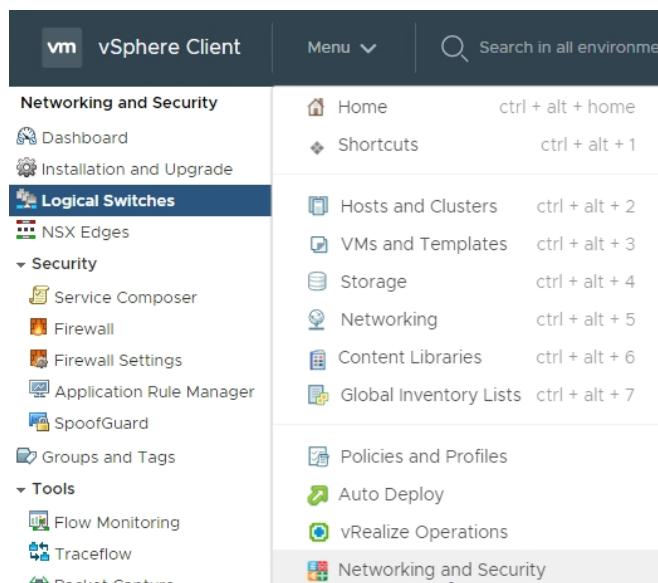
INTEGRATION GUIDE

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

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.



The screenshot shows the vSphere Client interface. The top navigation bar includes 'vm', 'vSphere Client', 'Menu', and a search bar. The left sidebar has a 'Networking and Security' section with various icons and links. The 'Logical Switches' link is highlighted with a blue background. Below it are 'NSX Edges', 'Security' (with sub-links like Service Composer, Firewall, etc.), 'Groups and Tags', 'Tools' (Flow Monitoring, Traceflow, Packet Capture), and 'Networking and Security'. The main content area is titled 'Logical Switches' and shows a table of three logical switches: 'virtualwire-19' (Segment ID 5001, Name WebTier, Status Normal, Transport Zone Transit2-Net, Connect VMs 6), 'virtualwire-20' (Segment ID 5002, Name AppTier, Status Normal, Transport Zone Transit2-Net, Connect VMs 7), and 'virtualwire-21' (Segment ID 5003, Name DBTier, Status Normal, Transport Zone Transit2-Net, Connect VMs 3). Action buttons for ADD, EDIT, DELETE, ADD VM, REMOVE VM, and ACTIONS are at the top of the table.

Logical Switch ID	Segment ID	Name	Status	Transport Zone	Connect VMs
virtualwire-19	5001	WebTier	Normal	Transit2-Net	6
virtualwire-20	5002	AppTier	Normal	Transit2-Net	7
virtualwire-21	5003	DBTier	Normal	Transit2-Net	3

INTEGRATION GUIDE

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

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

Logical Switches

NSX Manager: 192.168.2.40 | Standalone

+ ADD EDIT DELETE ADD VM REMOVE VM ACTIONS

Logical Switch ID	Segment ID	Name	Manage Hardware Bindings
virtualwire-19	5001	WebTier	Connect Edge
virtualwire-20	5002	AppTier	
virtualwire-21	5003	DBTier	

Status Transport Zone Connected VMs Hardware Ports Binding

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

Manage Hardware Bindings | WebTier

nsx-bip.bd.f5.com (0 Bindings)

+ ADD DELETE

Switch	Port	VLAN
No items to display		

CANCEL OK

5. Click the Select link in the Port section

Manage Hardware Bindings | WebTier

nsx-bip.bd.f5.com (1 Bindings)

+ ADD DELETE

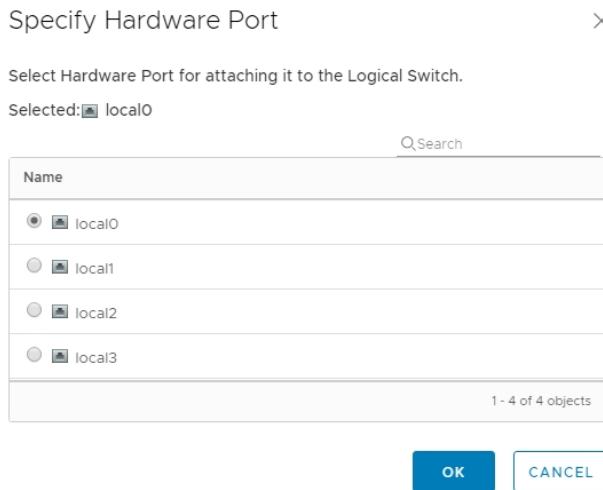
Switch	Port	VLAN
nsx-bip.bd.f5.com	Select Port	Select

CANCEL OK

INTEGRATION GUIDE

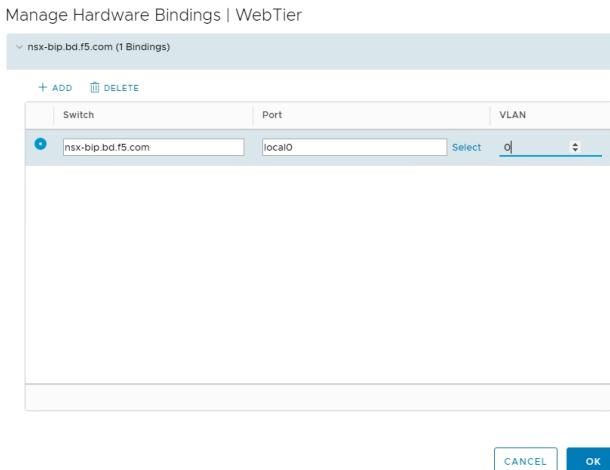
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

- 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



- 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.



- Back in the Logical Switches menu, 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.

Logical Switches						
NSX Manager: 192.168.2.40 Standalone			Actions			
Logical Switch ID	Segment ID	Name	Status	Transport Zone	Connected VMs	Hardware Ports Binding
virtualwire-19	5001	WebTier	Normal	Transit2-Net	6	1
virtualwire-20	5002	AppTier	Normal	Transit2-Net	7	0
virtualwire-21	5003	DBTier	Normal	Transit2-Net	3	0

INTEGRATION GUIDE

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

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

Logical Switch ID	Segment ID	Name	Status	Transport Zone	Connected VMs	Hardware Ports Binding
virtualwire-19	5001	WebTier	Normal	Transit2-Net	6	1
virtualwire-20	5002	AppTier	Normal	Transit2-Net	7	0
virtualwire-21	5003	DBTier	Normal	Transit2-Net	3	0

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

Switch	Port	VLAN
No items to display		

CANCEL OK

11. Click the Select link in the Port section

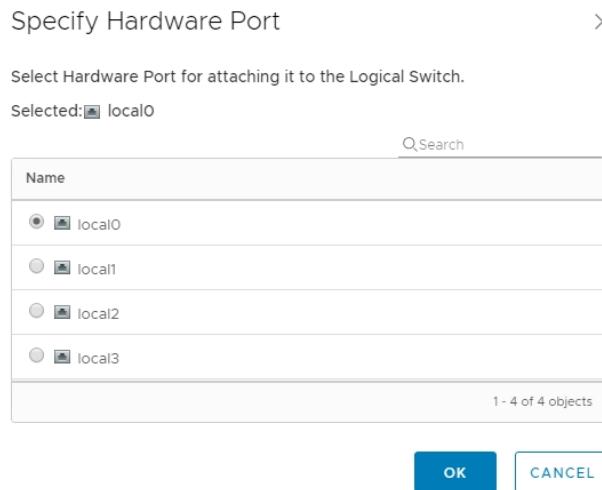
Switch	Port	VLAN
nsx-bip.bd.f5.com	Select Port	Select

CANCEL OK

INTEGRATION GUIDE

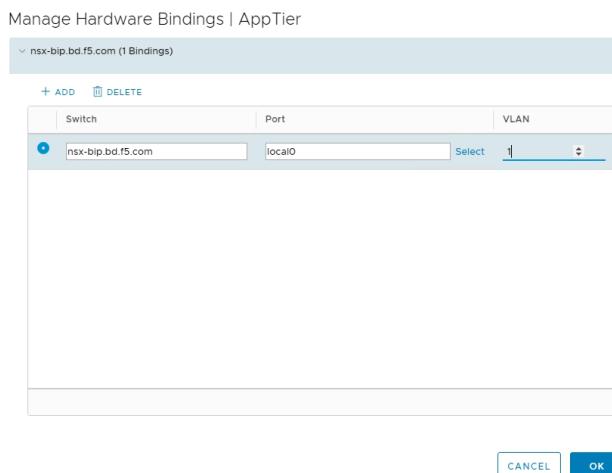
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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.

Logical Switches

NSX Manager: 192.168.2.40 | Standalone

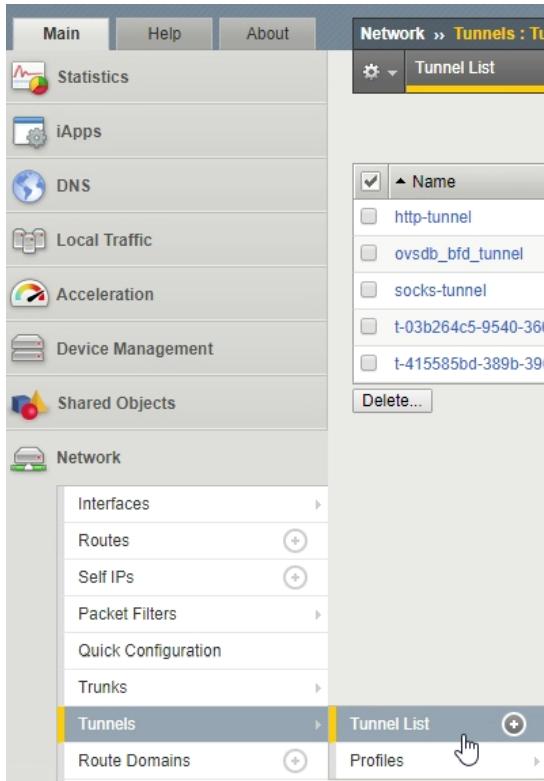
+ ADD EDIT DELETE ADD VM REMOVE VM ACTIONS

Logical Switch ID	Segment ID	Name	Status	Transport Zone	Connected VMs	Hardware Ports Binding
virtualwire-19	5001	WebTier	Normal	Transit2-Net	6	1
virtualwire-20	5002	AppTier	Normal	Transit2-Net	7	1
virtualwire-21	5003	DBTier	Normal	Transit2-Net	3	0

INTEGRATION GUIDE

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

- 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.



- 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

This screenshot shows a detailed view of the Tunnel List table from the previous screenshot. The table includes columns for Name, Application, Profile, Local Address, Remote Address, Key, and Partition / Path. The data is identical to the summary table above, listing five tunnels: http-tunnel, ovldb_bfd_tunnel, socks-tunnel, t-03b264c5-9540-366, and t-415585bd-389b-396. The 'Create...' button is visible at the top right of the table area.

Name	Application	Profile	Local Address	Remote Address	Key	Partition / Path
http-tunnel	tcp-forward		::	::	0	Common
ovldb_bfd_tunnel		vxlan-ovsdb-no-flooding	192.172.50.81	any	0	Common
socks-tunnel	tcp-forward		::	::	0	Common
t-03b264c5-9540-3666-a34a-c75d828439bc		vxlan-ovsdb	192.172.50.81	any	5001	Common
t-415585bd-389b-3965-9223-807d77a96791		vxlan-ovsdb	192.172.50.81	any	5002	Common

INTEGRATION GUIDE

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

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.

The screenshot shows the F5 BIG-IP Configuration Utility interface. The main window title is "Network > Self IPs". The left sidebar has tabs for Main, Help, and About, and a navigation pane with icons for Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, Shared Objects, and Network. Under Network, there are sub-options for Interfaces, Routes, and Self IPs, with the "Self IPs" option highlighted. The main content area displays a table titled "Self IP List" with the following data:

Name	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
External	10.105.176.10	255.255.255.0	VLAN-176	traffic-group-local-only	Common
NSX-CTRL	192.168.2.250	255.255.0.0	VLAN-102	traffic-group-local-only	Common
VTEP	192.172.50.81	255.255.255.0	VLAN-50	traffic-group-local-only	Common
ovsdb_bfd_tunnel_selfip	192.172.50.81%200	255.0.0.0	ovsdb_bfd_tunnel	traffic-group-local-only	Common

INTEGRATION GUIDE

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

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

Network » Self IPs » **New Self IP...**

Configuration	
Name	WebTier-Self
IP Address	10.0.1.10
Netmask	255.255.255.0
VLAN / Tunnel	t-03b264c5-95 ▼
Port Lockdown	Allow None ▼
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating) ▼
Service Policy	None ▼

Cancel **Repeat** **Finished**

INTEGRATION GUIDE

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

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.

Network » Self IPs » New Self IP...

Configuration

Name	AppTier-Self
IP Address	10.0.2.10
Netmask	255.255.255.0
VLAN / Tunnel	t-415585bd-3E ▾
Port Lockdown	Allow None ▾
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating) ▾
Service Policy	None ▾

Network » Self IPs

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	AppTier-Self		10.0.2.10	255.255.255.0	t-415585bd-389b-3965-9223-807d77a96791	traffic-group-local-only	Common
<input type="checkbox"/>	External		10.105.176.10	255.255.255.0	VLAN-176	traffic-group-local-only	Common
<input type="checkbox"/>	NSX-CTRL		192.168.2.250	255.255.0.0	VLAN-102	traffic-group-local-only	Common
<input type="checkbox"/>	VTEP		192.172.50.81	255.255.255.0	VLAN-50	traffic-group-local-only	Common
<input type="checkbox"/>	WebTier-Self		10.0.1.10	255.255.255.0	t-03b264c5-9540-3666-a34a-c75d828439bc	traffic-group-local-only	Common
<input type="checkbox"/>	ovsdb_bfd_tunnel_selfip		192.172.50.81%200	255.0.0.0	ovsdb_bfd_tunnel	traffic-group-local-only	Common

INTEGRATION GUIDE

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

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.

The screenshot shows the F5 Management Interface. The top navigation bar includes Main, Help, About, Network, and Self IPs. The left sidebar under Local Traffic lists Network Map, Virtual Servers, Policies, Profiles, Ciphers, iRules, Pools (which is selected), and Nodes. The main content area is titled "Network > Self IPs" and "Self IP List". It shows a table with columns for Name, Status, Description, Application, Members, and Partition / Path. A row for "AppTier-Self" is selected. Below this is a "Pool List" section with tabs for Pool List (selected), Statistics, and Create. A message says "No records to display." A "Create..." button is visible in the top right of the Pool List tab.

INTEGRATION GUIDE

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

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

Local Traffic » Pools : Pool List » **New Pool...**

Configuration: Basic ▾

Name	WebServerPool				
Description					
Health Monitors	<table border="1"><tr><td>Active</td><td>Available</td></tr><tr><td>/Common gateway_icmp</td><td>/Common http http_head_f5 https https_443</td></tr></table>	Active	Available	/Common gateway_icmp	/Common http http_head_f5 https https_443
Active	Available				
/Common gateway_icmp	/Common http http_head_f5 https https_443				

Resources

Load Balancing Method	Round Robin															
Priority Group Activation	Disabled															
New Members	<p><input checked="" type="radio"/> New Node <input type="radio"/> New FQDN Node</p> <p>Node Name: <input type="text"/> (Optional)</p> <p>Address: <input type="text" value="10.0.1.12"/></p> <p>Service Port: <input type="text" value="443"/> <input type="button" value="HTTPS"/></p> <p>Add</p> <table border="1"><thead><tr><th>Node Name</th><th>Address/FQDN</th><th>Service Port</th><th>Auto Populate</th><th>Priority</th></tr></thead><tbody><tr><td>10.0.1.11</td><td>10.0.1.11</td><td>443</td><td></td><td>0</td></tr><tr><td>10.0.1.12</td><td>10.0.1.12</td><td>443</td><td></td><td>0</td></tr></tbody></table> <p>Edit Delete</p>	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
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												

INTEGRATION GUIDE

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

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.

Status	Name	Description	Application	Members	Partition / Path
●	AppServerPool			2	Common
●	WebServerPool			2	Common

INTEGRATION GUIDE

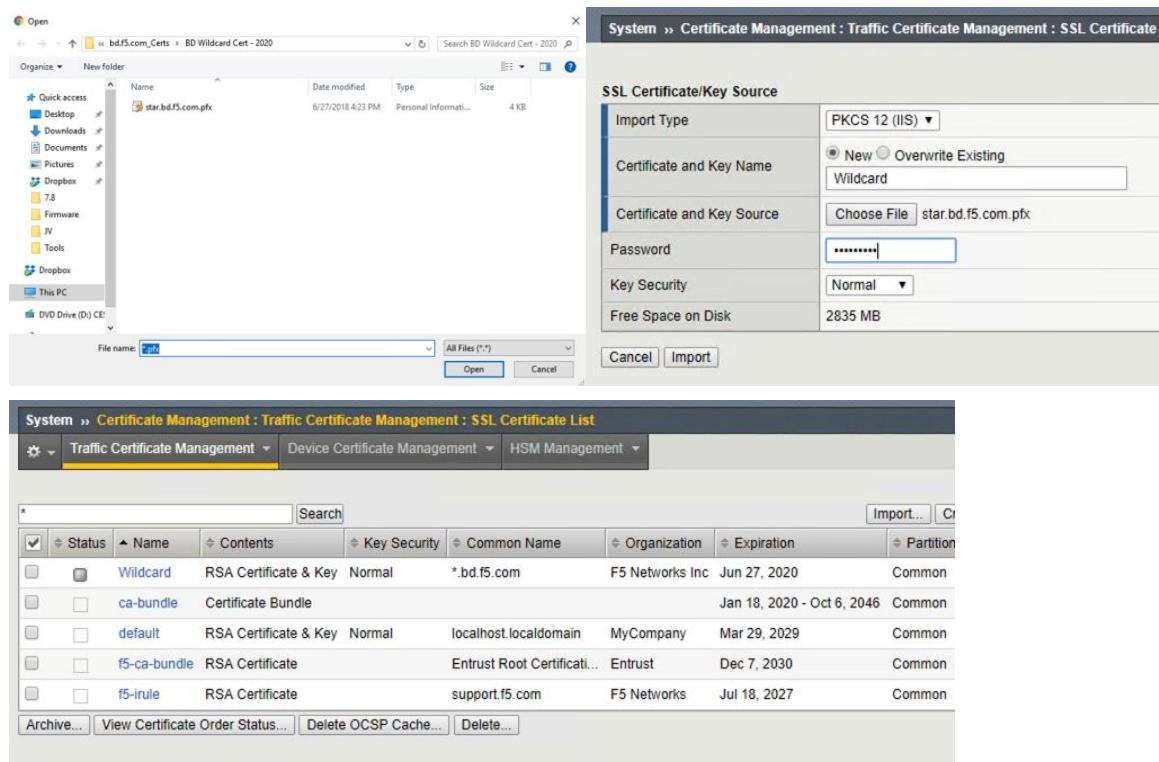
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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



INTEGRATION GUIDE

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

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.

The screenshot shows the F5 Management Interface for creating a new Client SSL Profile. It consists of three main windows:

- Top Window (Main View):** Shows the "General Properties" section with "Name" set to "WildcardSSL" and "Parent Profile" set to "clientssl". The "Configuration" dropdown is set to "Basic". A "Custom" checkbox is checked. Below this is a "Certificate Key Chain" section with an empty list and "Add", "Edit", and "Delete" buttons.
- Middle Window (Modal):** Titled "Add SSL Certificate Key Chain", it contains four dropdown fields: "Certificate" (set to "Wildcard"), "Key" (set to "Wildcard"), "Chain" (set to "Wildcard"), and "Passphrase" (empty). At the bottom are "Add" and "Cancel" buttons.
- Bottom Window (Main View):** Shows the updated "General Properties" section where the "Certificate Key Chain" dropdown now lists "/Common/Wildcard /Common/Wildcard /Common/Wildcard". The "Custom" checkbox is still checked.

INTEGRATION GUIDE

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

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

The screenshot shows the configuration interface for creating a new virtual server. The General Properties tab is active, showing the following details:

- Name: Web-VIP
- Description: (empty)
- Type: Standard
- Source Address: Host
- Destination Address/Mask: 10.105.176.5
- Service Port: 443
- Notify Status to Virtual Address: checked
- State: Enabled

The Resources tab shows:

- iRules: A list of available iRules including _sys_auth_ssl_cc_idap, _sys_auth_ssl_crldp, _sys_ssl_ocsp, _sys_auth_tacacs, and _sys_https_redirect. One is selected: _sys_auth_ssl_cc_idap.
- Policies: A list of available policies.
- Default Pool: Set to WebServerPool.
- Default Persistence Profile: None
- Fallback Persistence Profile: None

The main configuration pane shows the following settings:

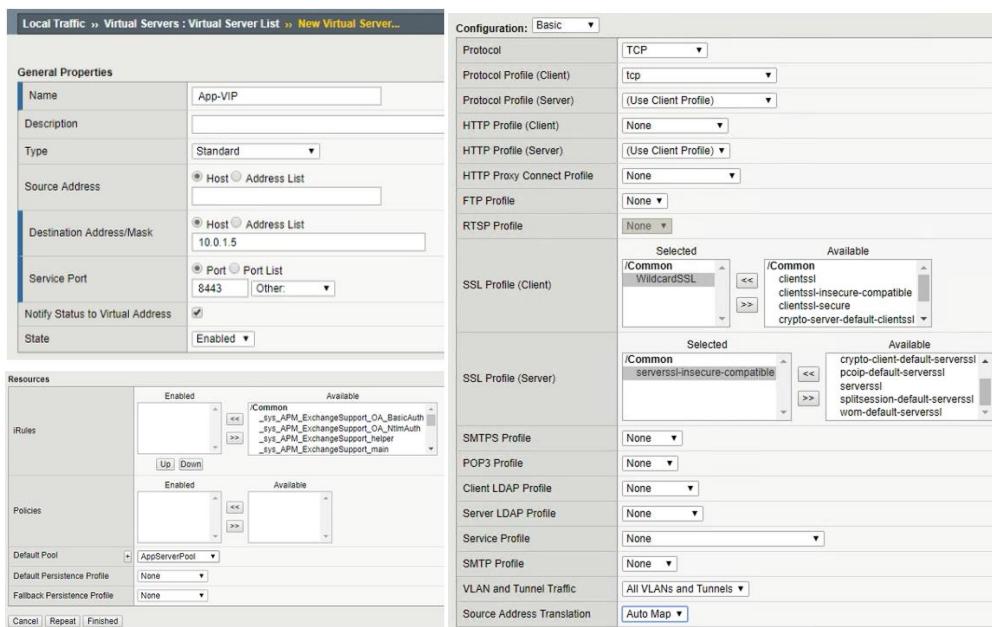
- Protocol: TCP
- Protocol Profile (Client): tcp
- Protocol Profile (Server): (Use Client Profile)
- HTTP Profile (Client): None
- HTTP Profile (Server): (Use Client Profile)
- HTTP Proxy Connect Profile: None
- FTP Profile: None
- RTSP Profile: None
- SSL Profile (Client): Selected: /Common/WildcardSSL (from Available: /Common/clientssl, clientsl-insecure-compatible, clientsl-secure, crypto-server-default-clientsl)
- SSL Profile (Server): Selected: /Common/serverssl-insecure-compatible (from Available: /Common/crypto-client-default-serverssl, pcip-default-serverssl, serverssl, splitsession-default-serverssl, wom-default-serverssl)
- SMTPS Profile: None
- POP3 Profile: None
- Client LDAP Profile: None
- Server LDAP Profile: None
- Service Profile: None
- SMTP Profile: None
- VLAN and Tunnel Traffic: All VLANs and Tunnels
- Source Address Translation: Auto Map

INTEGRATION GUIDE

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

4. In the New Virtual Server menus

- In the Name field, provide a unique name for the App tier application. In this case, we used App-VIP.
- In the Destination Address field, enter 10.0.1.5
- For Service Port use the standard HTTPS port 8443.
- In the Configuration section
 - Move WildcardSSL from Available to Selected in the SSL Profile (Client) field.
 - Move serverssl-insecure-compatible from Available to Selected in the SSL Profile (Server) field.
 - Select Auto Map from the pull-down menus for the Source Address Translation.
- In the Resources section
 - Select the AppServerPool from the Default Pool dropdown box.
 - 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.
- 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.

Local Traffic > Virtual Servers : Virtual Server List					
Virtual Server List		Virtual Address List		Statistics	
	Name	Description	Application	Destination	Type
<input checked="" type="checkbox"/>	App-VIP			10.0.1.5	8443 Standard
<input checked="" type="checkbox"/>	Web-VIP			10.105.176.5	443 (HTTPS) Standard

INTEGRATION GUIDE

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

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.

The screenshot shows the F5 BIG-IP Local Traffic interface. On the left, there's a tree view under 'Common' with two main nodes: 'App-VIP' and 'Web-VIP'. 'App-VIP' has three children: '10.0.1.5:8443', 'AppServerPool' (which has two children: '10.0.2.11:8443' and '10.0.2.12:8443'), and another '10.0.1.5:8443'. 'Web-VIP' has two children: 'WebServerPool' (which has two children: '10.0.1.11:443' and '10.0.1.12:443') and another '10.0.1.5:443'. On the right, a 'NSXWebApp Properties' dialog box is open. It shows the 'Host (A)' tab selected. The 'Host' field contains 'NSXWebApp'. The 'Fully qualified domain name (FQDN)' field contains 'NSXWebApp.bd.f5.com'. The 'IP address' field contains '10.105.176.5'. There are checkboxes for 'Update associated pointer (PTR) record' and 'Delete this record when it becomes stale'. A 'Record time stamp' field is present. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons. The status bar at the bottom of the interface shows 'Last Update: Apr 11, 2019 2:34 PM (PDT)'.

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.

The screenshot shows a web browser with two tabs both displaying the URL <https://nsxwebapp.bd.f5.com/cgi-bin/app.py>. Both tabs show the same content: 'Customer Database Access'. The left tab has the 'Accessed via: 10.0.2.2' and 'AppServer is: app-01' information. The right tab has the 'Accessed via: 10.0.2.2' and 'AppServer is: app-02' information. Below the tabs, there are two search bars labeled 'Name Filter (blank for all records)' and 'Apply'. Underneath each search bar is a table showing company data:

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

Rank	Name	Universe	Revenue
1	CHOAM	Dune	\$1.7 trillion
2	Acme Corp.	Looney Tunes	\$348.7 billion
3	Sirius Cybernetics Corp.	Hitchhiker's Guide	\$327.2 billion
4	Buy n Large	Wall-E	\$291.8 billion
5	Aperture Science, Inc.	Valve	\$163.4 billion

The screenshot shows a terminal window with two separate curl commands. The left command is for host 'nsxwebapp.bd.f5.com' and the right command is for host 'nsxwebapp.bd.f5.com'. Both commands include the '-kv' option and show the response from the web server. The responses are identical, showing the 'Customer Database Access' page with the same data as the browser screenshot above. The terminal prompt is '[mmabis@hzn-lin-mmabis ~]\$'.

```
< Connection: keep-alive
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< X-Upstream-Server: web-01
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host nsxwebapp.bd.f5.com left intact
[mmabis@hzn-lin-mmabis ~]$ [mmabis@hzn-lin-mmabis ~]$ < Connection: keep-alive
< Last-Modified: Mon, 11 Jun 2007 18:53:14 GMT
< ETag: "2d-432a5e4a73a80"
< Accept-Ranges: bytes
< X-Upstream-Server: web-02
<
<html><body><h1>It works!</h1></body></html>
* Connection #0 to host nsxwebapp.bd.f5.com left intact
[mmabis@hzn-lin-mmabis ~]$
```

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

INTEGRATION GUIDE

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

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-bclf-d4bf696a3ba01	[]	true	[]	()	{sec since connect="118", sec since disconnect="140", state=ACTIVE}	"ssl:192.168.2.45:6640"
f5a7caef-181d-4e0c-94d1-bd66e997d2cf	[]	true	[]	()	{sec since connect="200", sec since disconnect="222", state=ACTIVE}	"ssl:192.168.2.46:6640"
d12940be-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	local	remote	bfd_params	
2952ef1a-c942-4b98-9413-edf7f2f5fd0	[bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c5"]	[bfd_dst_ip="192.172.50.30", bfd_dst_mac="00:50:56:ff:3d:f0"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	fc2d04e1-5c45-4525-8701-278ce5ac816	
02094194-740e-4e52-05bd-b804a330139b	[bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c5"]	[bfd_dst_ip="192.172.50.31", bfd_dst_mac="00:50:56:e1:b7:e0"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	556dc505-a869-49e6-8763-b43706843d60	
#ead8429-d166-40e6-aaeb-e2877ea3345	[bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c5"]	[bfd_dst_ip="192.172.50.32", bfd_dst_mac="00:50:56:ff:3d:f0"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	0c5d2441-a86b-40e0-904d-0a9e416159bc	
nu_1f_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	0c5d2441-a86b-40e0-904d-0a9e416159bc	
ng_1f_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	66415526-2ddc-420d-8473-4a9e2fea0e2f	
ng_1f_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	66415526-2ddc-420d-8473-4a9e2fea0e2f	
913494cc-8ca1-4fe1-aef0-fd350406	[bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c5"]	[bfd_dst_ip="192.172.50.30", bfd_dst_mac="00:50:56:ff:3d:f0"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	d686161b-21f7-407f-a26c-a7a2e28e3d	
ng_1f_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	556dc505-a869-49e6-8763-b43706843d60	
ng_1f_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	556dc505-a869-49e6-8763-b43706843d60	
90c74575-201e-426d-af51-99cd9b02	[bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c5"]	[bfd_dst_ip="192.172.50.40", bfd_dst_mac="00:50:56:ff:3d:f0"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	f770c709-7a0a-4141-8254-43060a3b96	
ng_if_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	45cb3541-3a2a-4449-9221-4a3e7e92c776	
54013507-5b76-4a16-b71f-4b8c871a1b18	[bfd_dst_ip="192.172.50.81", bfd_dst_mac="00:23:e9:fc:f9:c5"]	[bfd_dst_ip="192.172.50.41", bfd_dst_mac="00:50:56:66:58:d4"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	a442e10e-0e54-429e-980d-c7afcf51eb27	
ng_if_rx="true", min_rx="300"	[enabled="true"]	[enabled="true"]	{enable="true", forwarding="true", remote_state="up", state=up}	eif35d1ad-33cb-407f-beel-1145745e4a4	a442e10e-0e54-429e-980d-c7afcf51eb27	

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

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