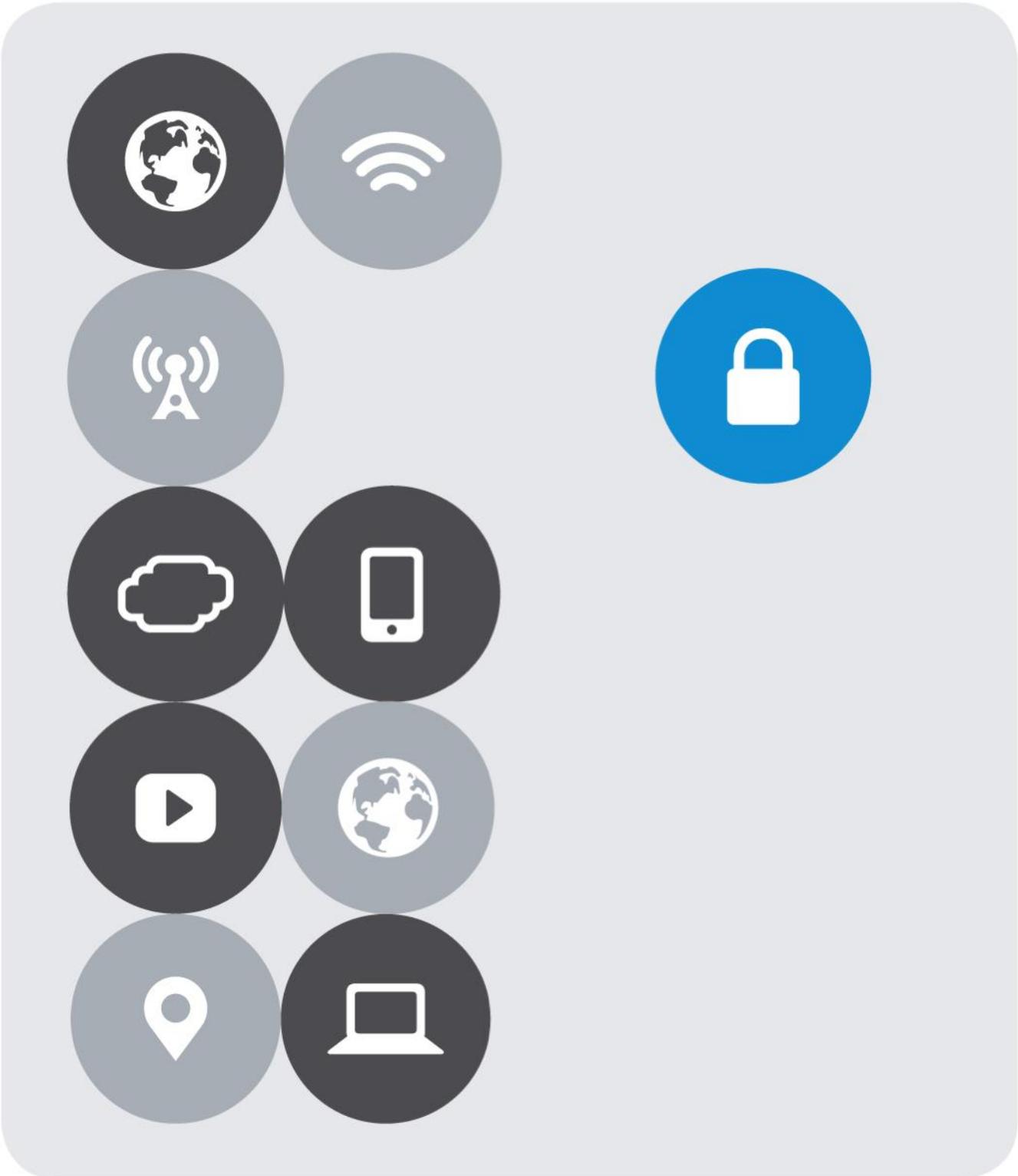




INTEGRATION GUIDE

vmware®

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





## Version History

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

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



# Contents

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

# Introduction

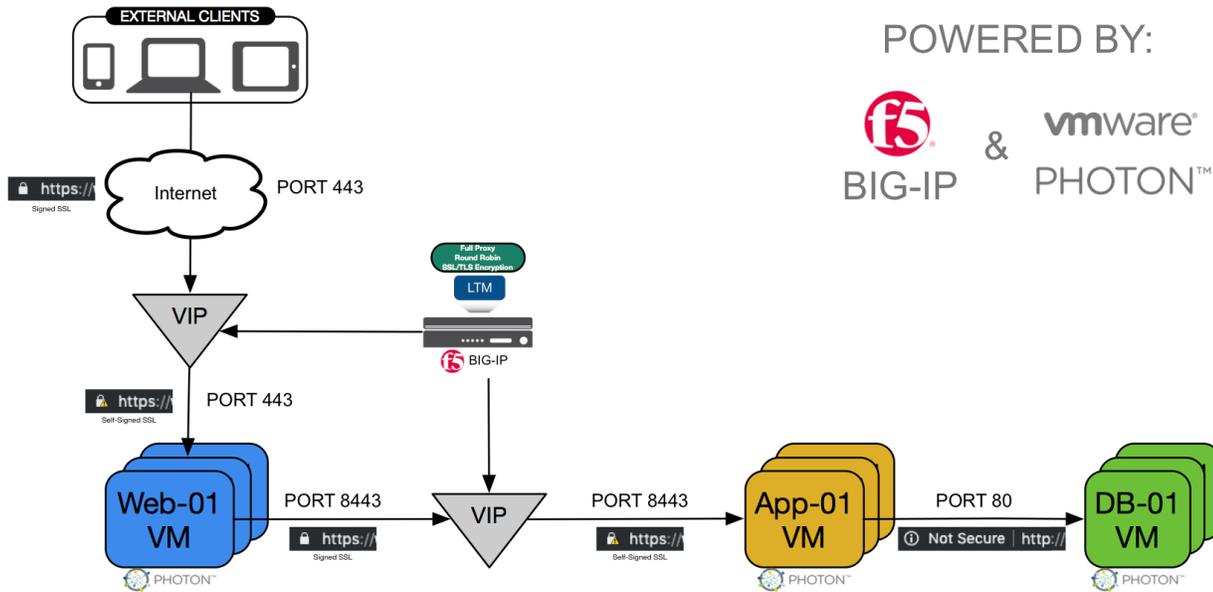
The Software-Defined Data Center (SDDC) is characterized by server virtualization, storage virtualization, and network virtualization. Server virtualization has already proved the value of SDDC architectures in reducing costs and complexity of the compute infrastructure. VMware NSX network virtualization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

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

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

# The Multi-tiered Application

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



POWERED BY:



- 1) WebTier – Web Server(s) are providing secure access to the backend application, these servers are internet facing typically and have load balancing to allow servers to distribute loads appropriately.
- 2) AppTier – Application Server(s) access the backend database(s) and execute the code and provide that data to the Web Server(s) sitting in front of them. These Applications are not internet facing and are protected by the LAN.
- 3) DBTier – Database Server(s) that house the information that the application servers execute against, these servers these servers are also not internet facing and are protected by the LAN.

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

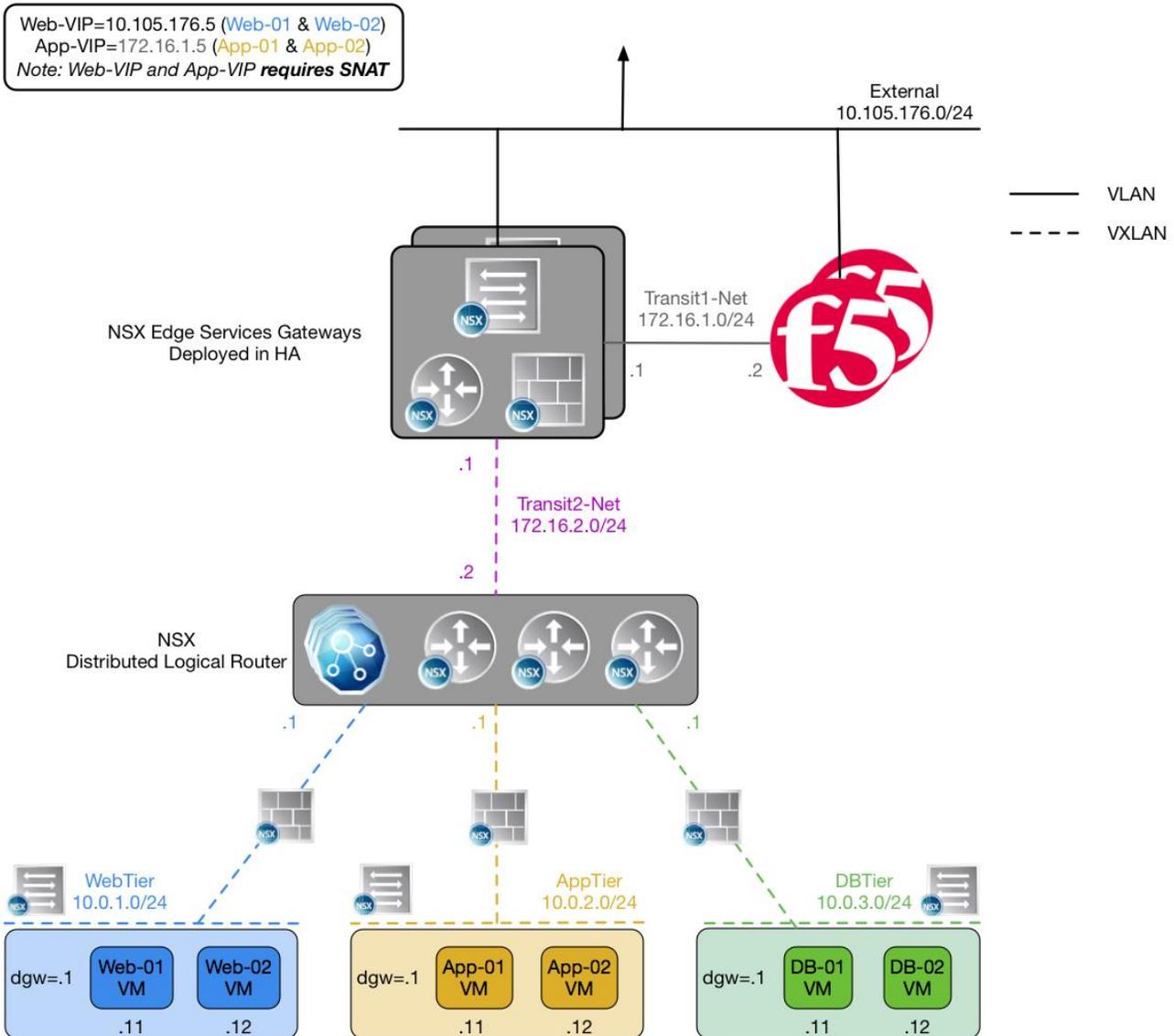
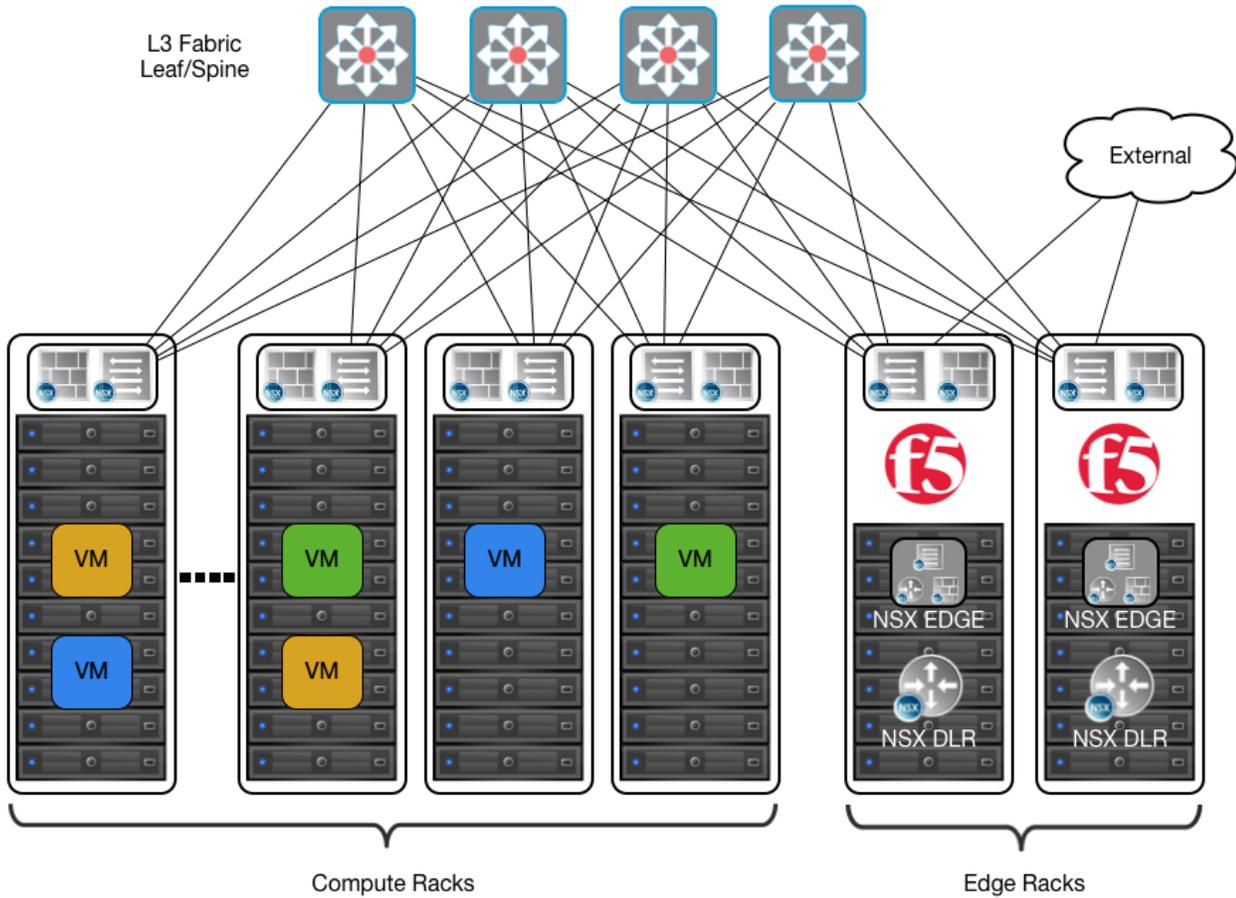


Figure 1 BIG-IP appliance parallel to NSX Edge Services Gateway

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

**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

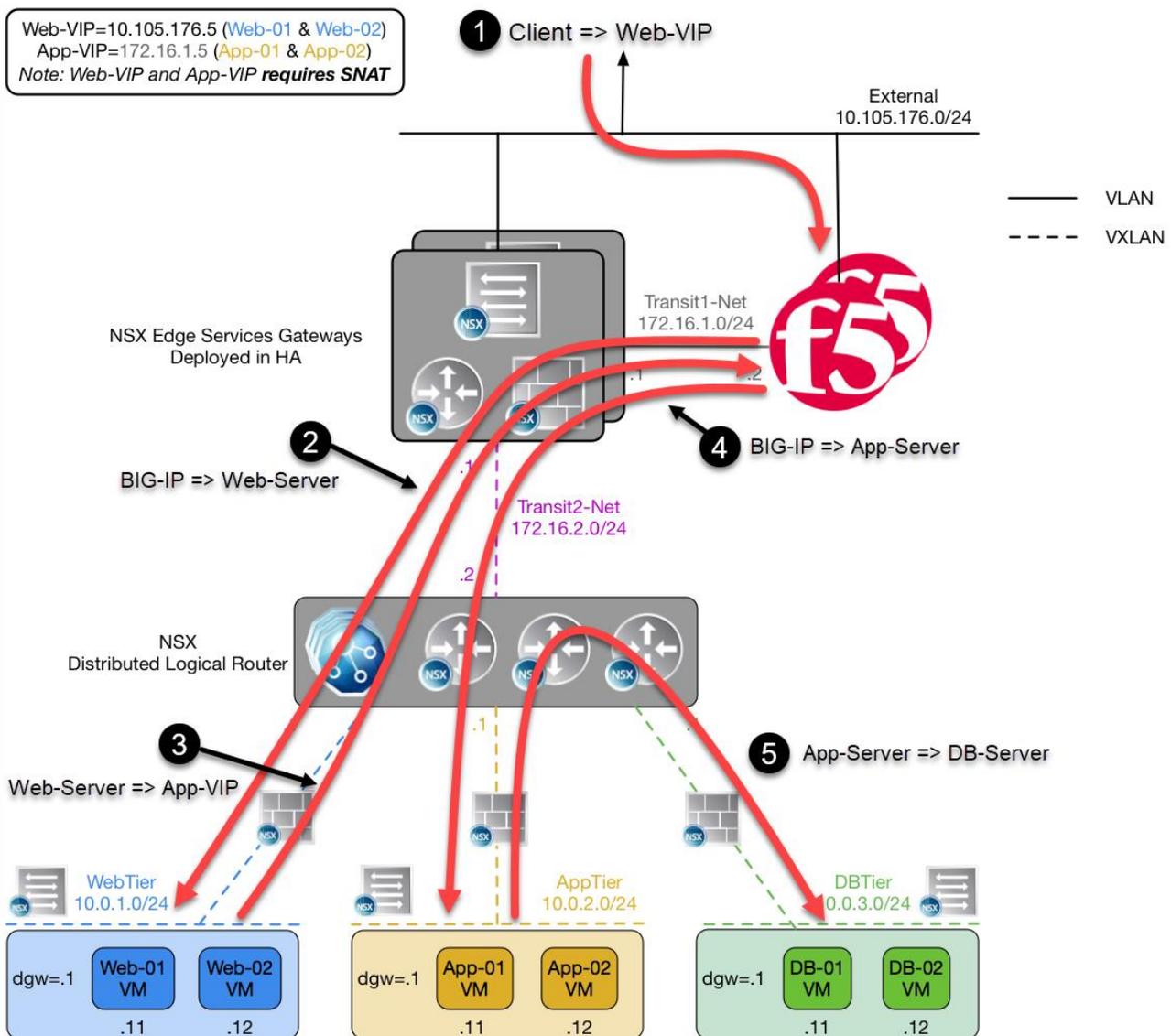


Figure 3 North-South Logical Traffic Flow "Parallel to NSX Edge" with BIG-IP Appliances

## Implementation Infrastructure

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

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 4: the Cluster1-VDC (Edge Rack) and Cluster3-Compute-NSX (Compute Rack). While this is a smaller representation of a typical data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 2.



Figure 4 vSphere Console

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

The virtual machines used as Web (Web), Application (App), and Database (DB) servers will be running on ESXi hosts in the compute cluster. To better understand data traffic flows for this deployment scenario topology, look at Figure 3 above.

## Prerequisites

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

- The BIG-IP will need to be installed and connected (physically or virtually) to the edge rack. Each BIG-IP management interface will need to be connected and configured with an IP address in the management segment.
- The BIG-IP interface 1.1 will need to be connected to a switch port either in ESXi (trunked port group) or on the edge rack top-of-rack switch that 802.1Q tags the VLANs used in this environment. In the example, VLANs 102, 176 and 177 are used.
- Physical network infrastructure switches connected to the ESXi servers and BIG-IP appliances (if not virtual) are configured to support 802.1Q tagging and allow the appropriate VLANs.
- ESXi hosts will need to be configured with the appropriate distributed port groups and virtual switches.

Name	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176	176
Internal	DVS-VLAN-102	102
TransitNet-1	DVS-VLAN-177	177

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

Name	Transport Zone	Segment ID	Control Plane Mode
AppTier	TransportZone1	5002	Unicast
DBTier	TransportZone1	5003	Unicast
Transit2-Net	TransportZone1	5005	Unicast
WebTier	TransportZone1	5001	Unicast

Table 2 Logical switch configuration

## Network Segments

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

### 802.1Q VLAN segments

- **VLAN 176 (External)** is the VLAN used for external client to Web-VIP connectivity. The 10.105.176.0/24 IP subnet range is configured on this VLAN.
- **VLAN 102 (Internal)** (not shown) is for management connectivity. The 192.168.14.0/24 IP subnet range is configured on this VLAN.
- **VLAN 177 (TransitNet-1)** is the VLAN used as the transit VLAN between the BIG-IP appliance and the NSX Edge for application traffic. The 172.16.1.0/24 IP subnet range is configured on this VLAN.

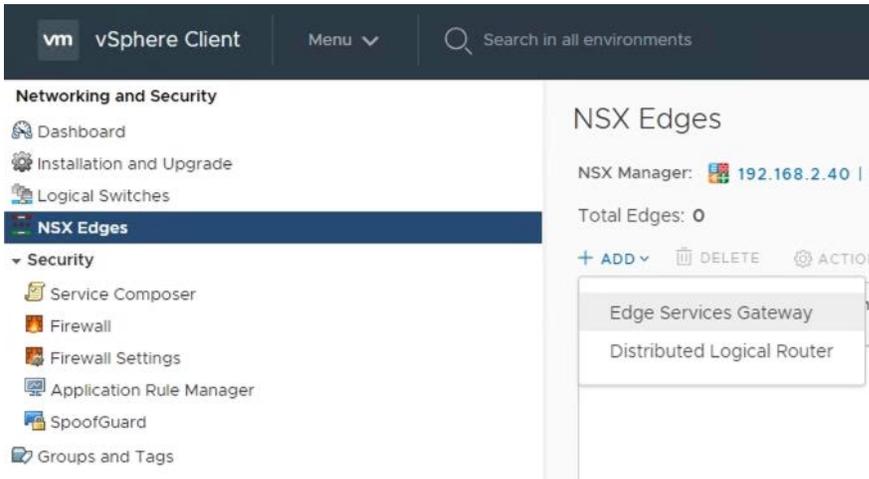
### VXLAN Segments

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

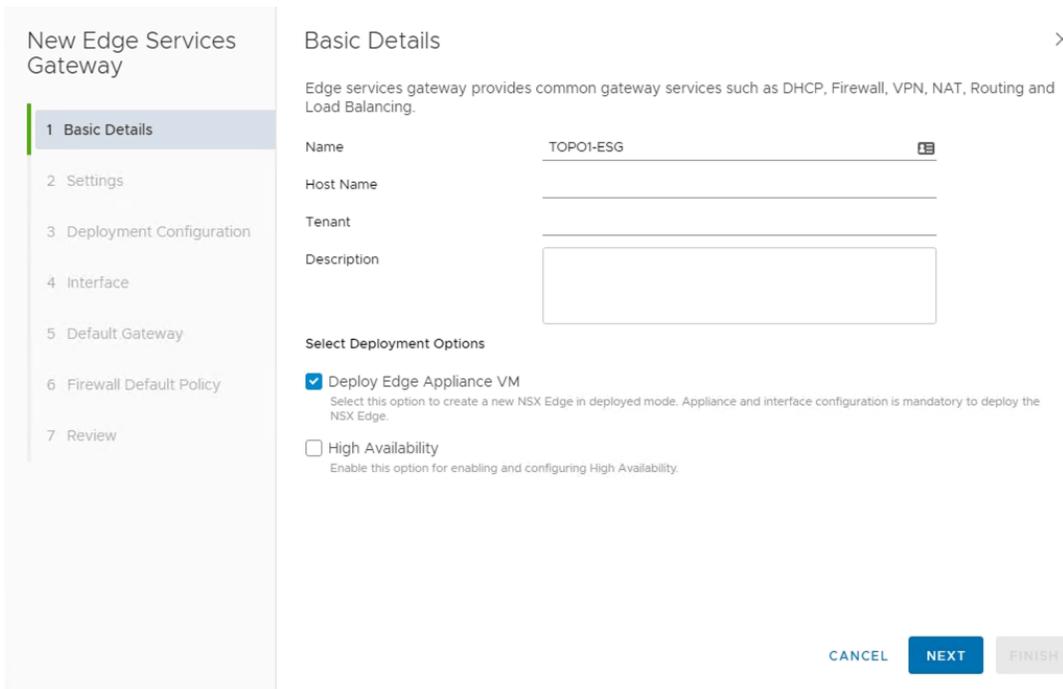
- **VXLAN 5001 WebTier** is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5002 AppTier** is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5003 DBTier**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

# NSX Edge Configuration

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



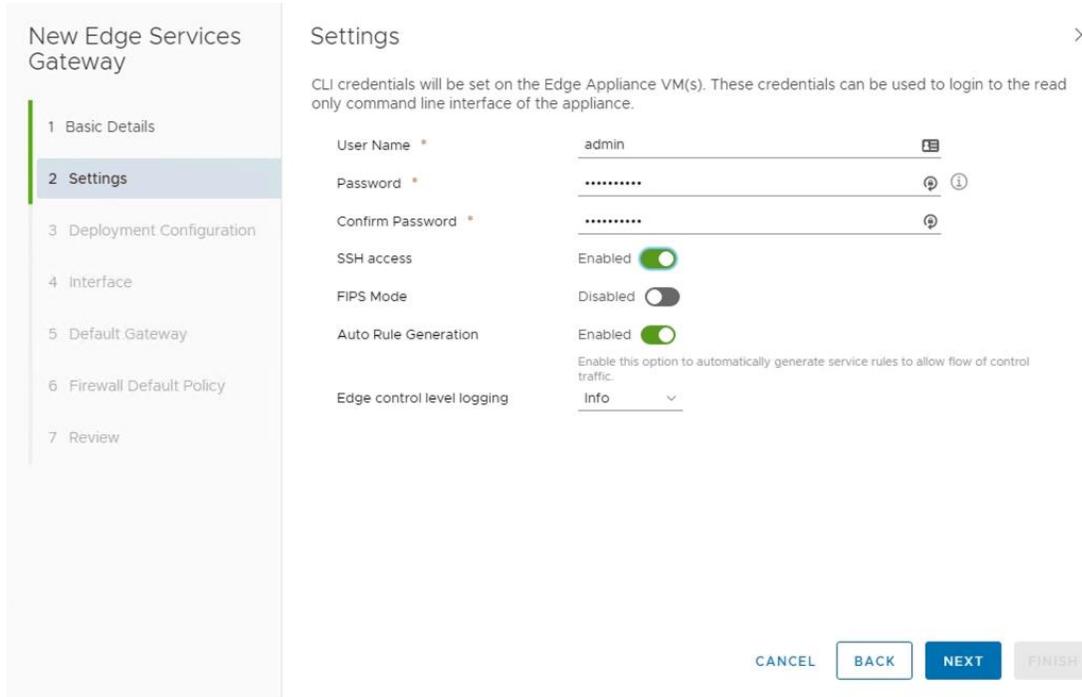
2. Provide a name for the device, then click next.



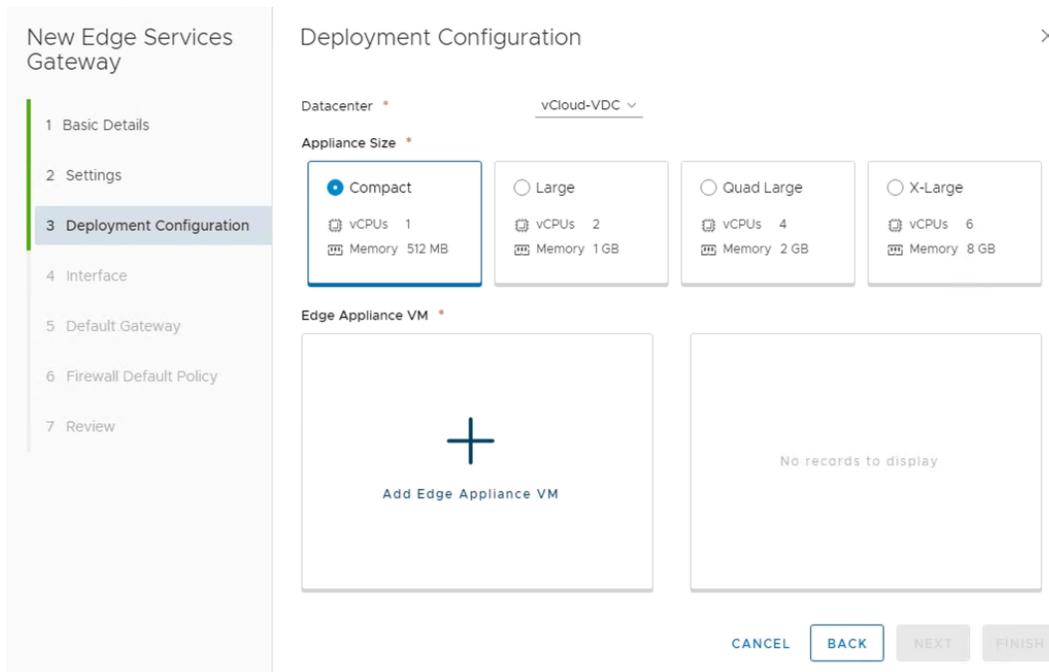
**INTEGRATION GUIDE**

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

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



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



## 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 ×

Specify placement parameters for the Edge Appliance VM.

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

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

### New Edge Services Gateway

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

### 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

## 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.

Configure Interfaces

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \*

Connectivity Status Disconnected

Configure Subnets

+ ADD DELETE Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
--------------------------	--------------------	------------------------	----------------------

0 Items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL OK

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.

Select Network

Logical Switch Standard Port Group Distributed Virtual Port Group

176

Name	Type
<input checked="" type="radio"/> DVS-VLAN-176	Distributed Virtual Port Group

1 - 1 of 1 items

CANCEL 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

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \* DVS-VLAN-176

Connectivity Status Connected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
--------------------	------------------------	----------------------

0 items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL OK

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

Configure Interfaces

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \* DVS-VLAN-176

Connectivity Status Connected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/> 10.105.176.2		24

1 items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL 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

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.

Configure Default Gateway: Enabled

vNIC: External

Gateway IP: 10.105.176.1

Admin Distance: 1

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).

The screenshot shows the configuration interface for a new Edge Services Gateway. On the left, a vertical navigation pane lists seven steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration, 4 Interface, 5 Default Gateway, 6 Firewall Default Policy (highlighted), and 7 Review. The main area is titled 'Firewall Default Policy' and contains three settings:

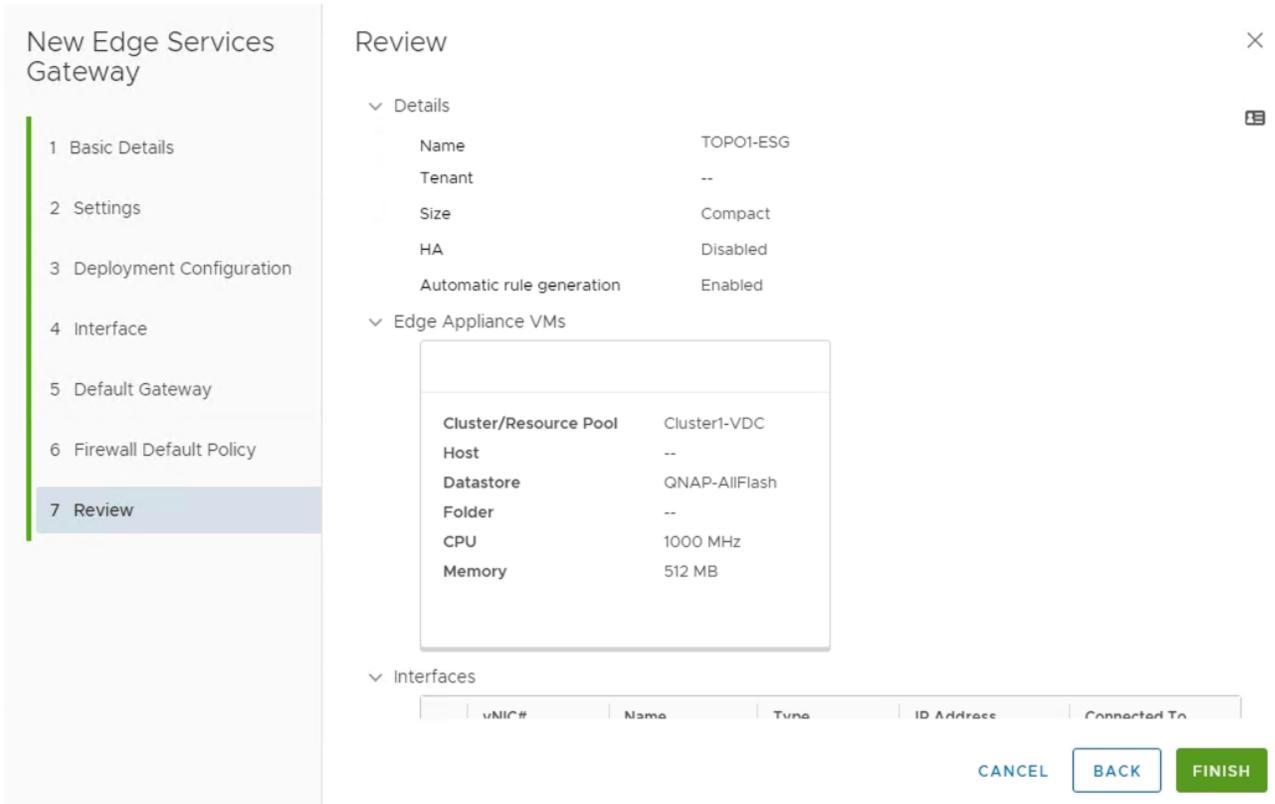
- Firewall Default Policy: Enabled (toggle switch is turned on)
- Default Traffic Policy: Allow (radio button selected), Deny (radio button unselected)
- Logging: Disabled (toggle switch is turned off)

At the bottom right, there are four buttons: CANCEL, BACK, NEXT, and FINISH. The NEXT button is highlighted in blue.

**INTEGRATION GUIDE**

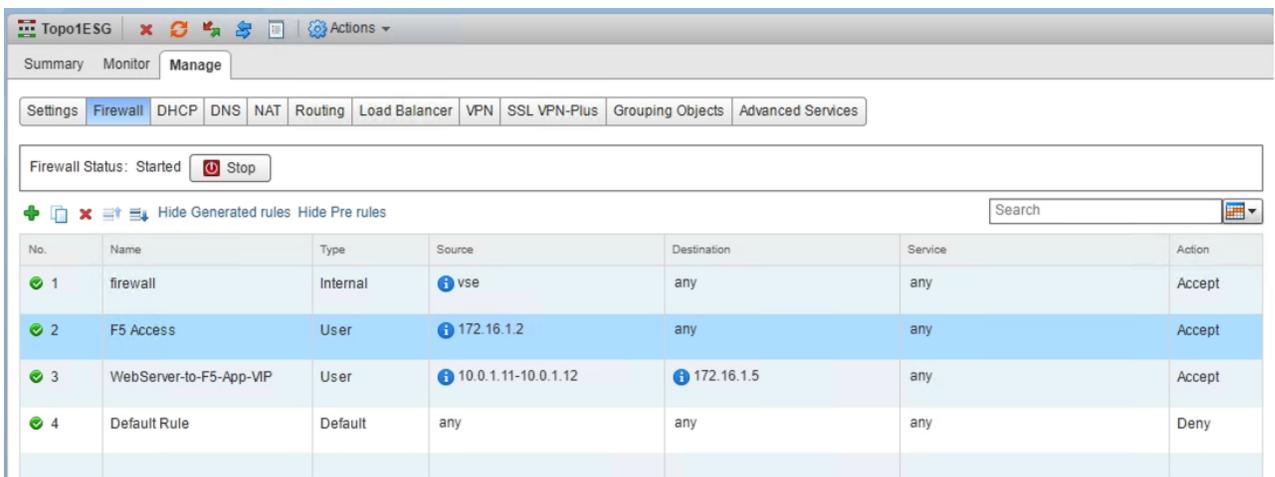
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

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).

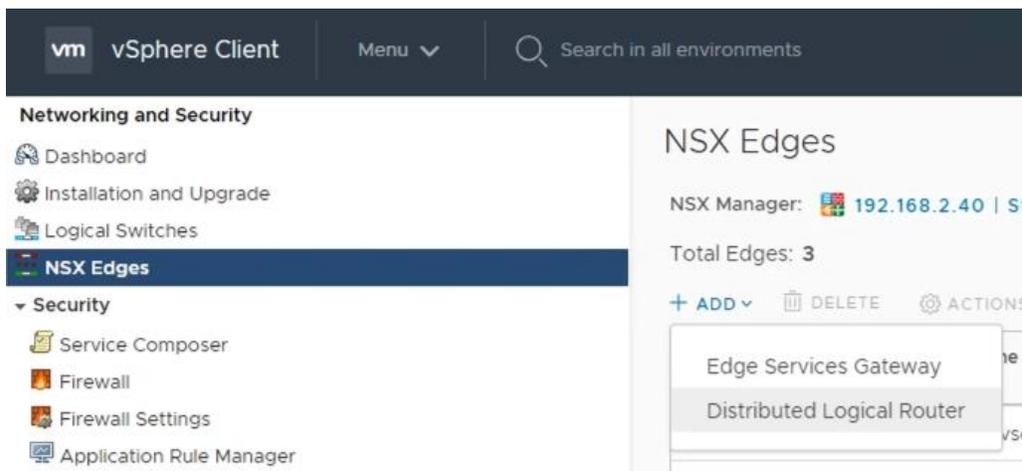


## Create and Deploy DLR

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.

### New Distributed Logical Router

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

#### Basic Details

Distributed logical router provides Distributed Routing and Bridging capabilities.

Name

Host Name

Tenant

Description

**Select Deployment Options**

**Deploy Control VMs**  
Deploys Edge Appliance VM to support Firewall and Dynamic routing.

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

HA Logging  Disabled

Log Level

**CANCEL** **NEXT** **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 topdump capabilities, if you do not want these features leave SSH disabled.

### New Distributed Logical Router

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

#### Settings

CLI credentials will be set on the Edge Appliance VM(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name \*

Password \*

Confirm Password \*

SSH access  Enabled

FIPS Mode  Disabled

Edge control level logging

**CANCEL** **BACK** **NEXT** **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.

New Distributed Logical Router

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

### Deployment Configuration

Datacenter \* vCloud-VDC

Control VM(s) \*

+ Add Edge Appliance VM

No records to display

**Management/ HA Interface**  
This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To \*

IP Address E.g. 10.121.30.4/24

CANCEL BACK NEXT FINISH

- 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.

### Add Edge Appliance VM

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

CPU 1000 MHz

Memory 512 MB

CANCEL ADD

## 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.

New Distributed Logical Router

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

### Deployment Configuration

Datacenter <sup>\*</sup> vCloud-VDC

Control VM(s) <sup>\*</sup>

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB

Management/ HA Interface

This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To <sup>\*</sup> \_\_\_\_\_ ⓘ 🗑️

IP Address \_\_\_\_\_  
E.g. 10.121.30.4/24

CANCEL BACK NEXT FINISH

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

< Back Select Network

Logical Switch Distributed Virtual Port Group

Q Search

Name	Type
<input type="radio"/> ESX-Management-Tagged	Distributed Virtual Port Group
<input type="radio"/> ESX-Storage	Distributed Virtual Port Group
<input type="radio"/> DVS-VLAN-080	Distributed Virtual Port Group
<input checked="" type="radio"/> DVS-VLAN-102	Distributed Virtual Port Group
<input type="radio"/> ESX-Trunk-Prom	Distributed Virtual Port Group
<input type="radio"/> ESX-NSX	Distributed Virtual Port Group
<input type="radio"/> DVS-VLAN-176	Distributed Virtual Port Group
<input type="radio"/> ESX-Management-Untagged	Distributed Virtual Port Group
<input type="radio"/> ESX-Trunk	Distributed Virtual Port Group
<input type="radio"/> ESX-vSAN	Distributed Virtual Port Group

1 - 30 of 30 items

CANCEL OK

## INTEGRATION GUIDE

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

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

### New Distributed Logical Router

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

### Deployment Configuration

Datacenter \* vCloud-VDC

Control VM(s) \*

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB

**Management/ HA Interface**  
This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To \* DVS-VLAN-102

IP Address 192.168.14.128/24

CANCEL BACK NEXT FINISH

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

### New Distributed Logical Router

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

### Configure Interfaces

Configure interfaces of this distributed logical router.

[+ ADD](#) [EDIT](#) [DELETE](#)

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

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

< Back Configure Interfaces

Name

Type  Internal  Uplink

Connected To

Connectivity Status Disconnected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Subnet Prefix Length
--------------------	----------------------

0 items

MTU

CANCEL OK

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

< Back Select Network

Logical Switch Distributed Virtual Port Group

Search

Name	Type
<input type="radio"/> dvs.VCDVSD-VCD-Internal-e2239cd6-3dd6-4ed2-a024-98c4c80e55d8	Logical Switch
<input type="radio"/> AppTier	Logical Switch
<input type="radio"/> DBTier	Logical Switch
<input type="radio"/> Transit1-Net	Logical Switch
<input checked="" type="radio"/> Transit2-Net	Logical Switch
<input type="radio"/> WebTier	Logical Switch

1 - 6 of 6 items

CANCEL 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.

The screenshot shows the 'Configure Interfaces' dialog box for the interface 'TransitNet-2'. The 'Type' is set to 'Uplink' and it is connected to 'Transit2-Net'. The 'Connectivity Status' is 'Connected'. The 'Configure Subnets' section is active, showing a table with two columns: 'Primary IP Address' and 'Subnet Prefix Length'. The table is currently empty, with a search bar and '+ ADD' and 'DELETE' buttons above it. The 'MTU' is set to 1500. 'CANCEL' and 'OK' buttons are at the bottom right.

Primary IP Address	Subnet Prefix Length
--------------------	----------------------

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

The screenshot shows the 'Configure Interfaces' dialog box for the interface 'TransitNet-2'. The 'Type' is set to 'Uplink' and it is connected to 'Transit2-Net'. The 'Connectivity Status' is 'Connected'. The 'Configure Subnets' section is active, showing a table with two columns: 'Primary IP Address' and 'Subnet Prefix Length'. One subnet is added: '172.16.2.2' with a 'Subnet Prefix Length' of '24'. The table has a search bar and '+ ADD' and 'DELETE' buttons above it. The 'MTU' is set to 1500. 'CANCEL' and 'OK' buttons are at the bottom right.

Primary IP Address	Subnet Prefix Length
172.16.2.2	24

## 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 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

- 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.

The screenshot shows the 'Default Gateway' configuration window for a 'New Distributed Logical Router'. On the left, a navigation pane lists steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration, 4 Interface, 5 Default Gateway (highlighted), and 6 Review. The main area is titled 'Default Gateway' and contains the following settings:

- Configure Default Gateway: Enabled (toggle switch)
- vNIC: TransitNet-2 (dropdown menu)
- Gateway IP: 172.16.2.1 (text input)
- Admin Distance: 1 (text input)

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

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

The screenshot shows the 'Review' screen for the 'New Distributed Logical Router'. The navigation pane on the left highlights step 6 Review. The main area is titled 'Review' and displays a summary of the configuration:

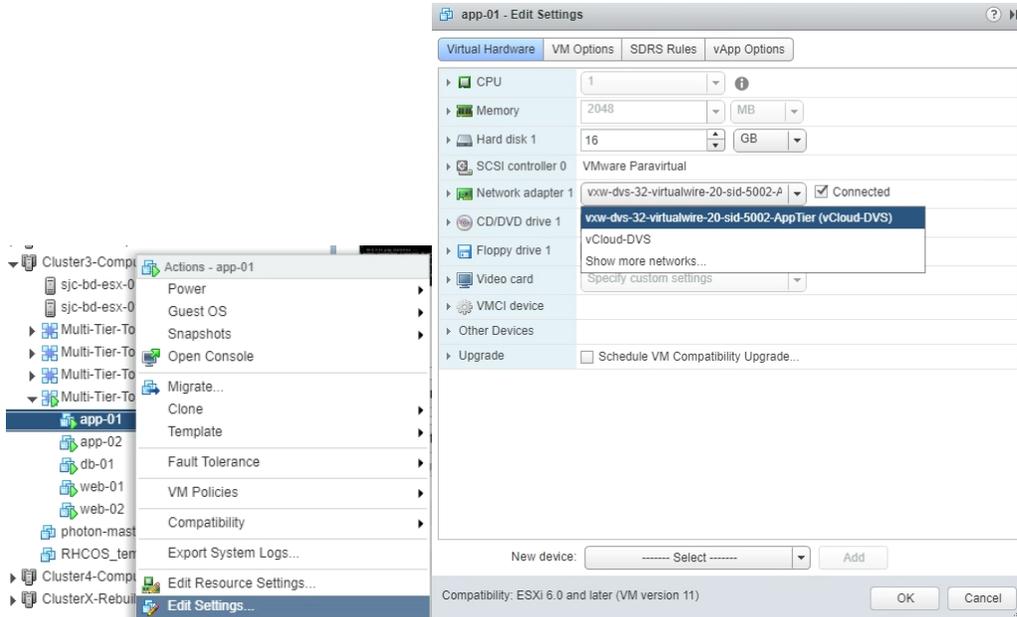
- Details
  - Name: TopoIDLR
  - Tenant: --
  - HA: Disabled
- Management/ HA Interface
  - Connected To: DVS-VLAN-102
  - IP Address: --
- Control VMs
  - Cluster/Resource Pool: Cluster1-VDC
  - Host: --
  - Datastore: QNAP-AllFlash
  - Folder: --
  - CPU: 1000 MHz
  - Memory: 512 MB
- Interfaces (partially visible)

At the bottom right, there are four buttons: CANCEL, BACK, FINISH (highlighted in green), and NEXT.

## 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.



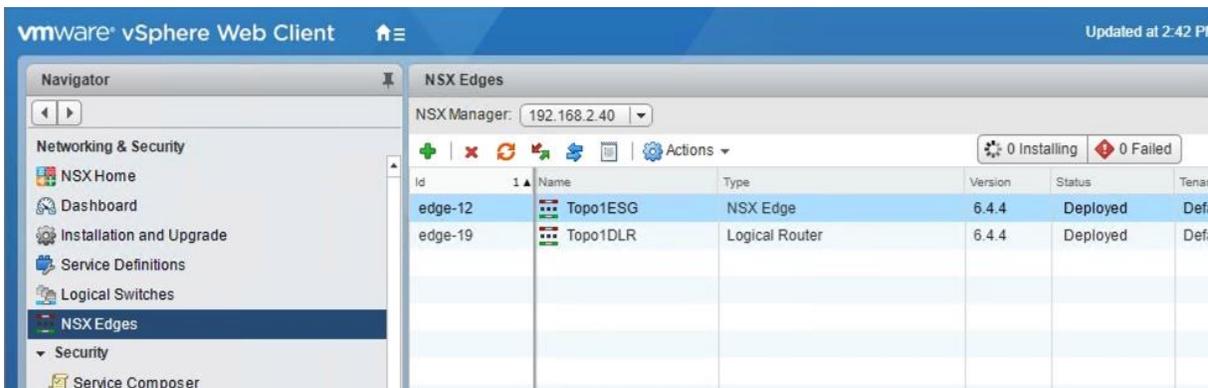
## NSX Edge Static Routing Configuration

For this deployment scenario, static routing is configured to allow the NSX Edge to forward packets into the different tiered networks via the DLR. The default gateway configuration on both the NSX Edge and the DLR ensures packets find their way out to external networks.

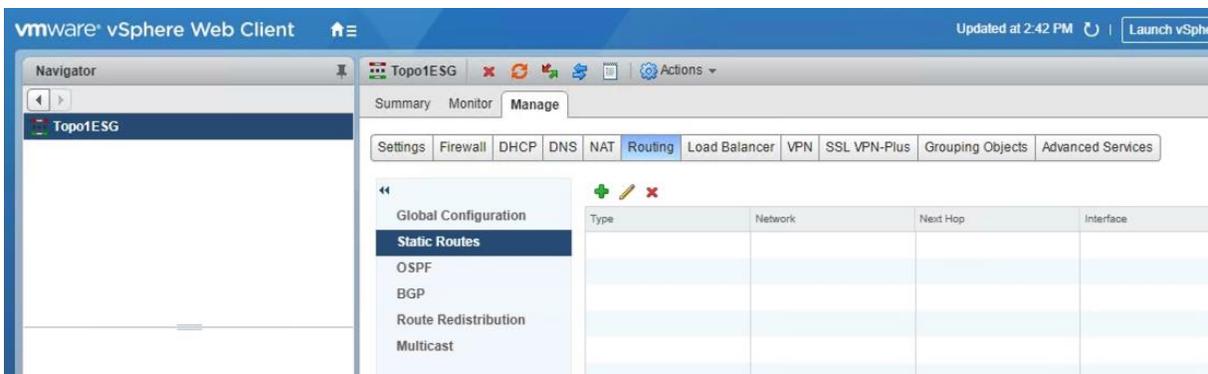
This configuration is also required to ensure that traffic coming from the external networks finds its way in.

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

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



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



## INTEGRATION GUIDE

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

3. Provide an internal summary route that points the NSX Edge to the Transit2-Net IP Address of the DLR interface. In this case, a summary of 10.0.0.0/16 is pointed internally to the DLR IP address of 172.16.2.2. Click OK.

**Edit Static Route**

Network: \* 10.0.0.0/16  
*Network should be entered in CIDR format  
e.g. 192.169.1.0/24*

Next Hop: \* 172.16.2.2

Interface: Transit2-Net

Admin Distance: 1

Description:

OK Cancel

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

Topo1ESG

Summary Monitor Manage

Settings Firewall DHCP DNS NAT Routing Load Balancer VPN SSL VPN-Plus Grouping Objects Advanced Services

Global Configuration  
Static Routes  
OSPF  
BGP  
Route Redistribution  
Multicast

Changes to the Static Routing configuration will take effect only after being published. Please click on "Publish Changes" to publish.  
Publish Changes Revert Changes

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

## 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.

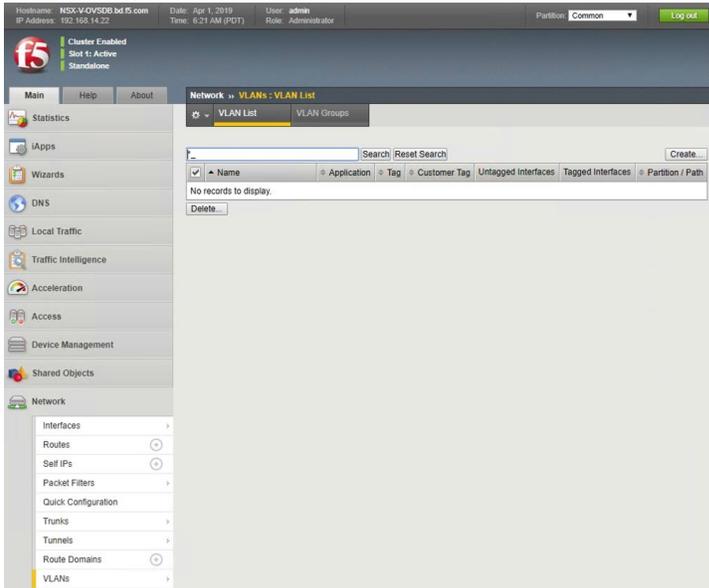
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

## INTEGRATION GUIDE

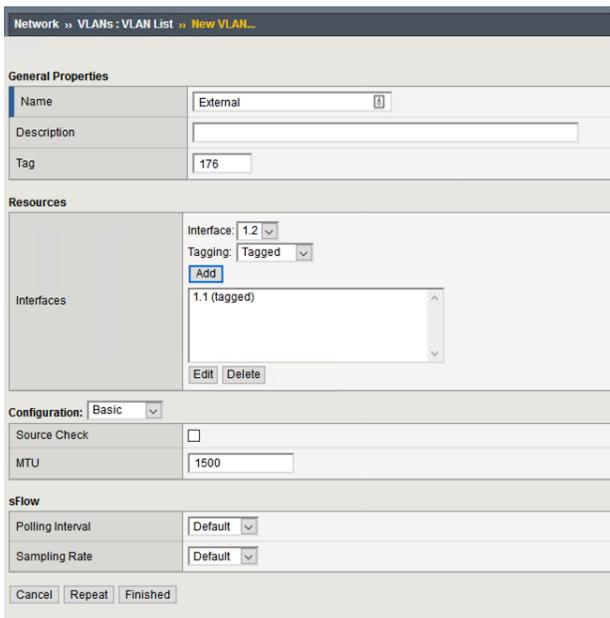
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

### 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 menu.
  - 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

The screenshot shows the 'New VLAN...' configuration form. The breadcrumb path is 'Network > VLANs > VLAN List > New VLAN...'. The form is organized into several sections:

- General Properties:** Includes fields for 'Name' (set to 'External'), 'Description', and 'Tag' (set to '176').
- Resources:** Includes a dropdown for 'Interface' (set to '1.2'), a dropdown for 'Tagging' (set to 'Tagged'), an 'Add' button, and a list of interfaces (currently showing '1.1 (tagged)'). There are 'Edit' and 'Delete' buttons below the list.
- Configuration:** Includes a 'Configuration' dropdown (set to 'Basic'), a 'Source Check' checkbox (unchecked), and an 'MTU' field (set to '1500').
- sFlow:** Includes 'Polling Interval' and 'Sampling Rate' dropdowns (both set to 'Default').

At the bottom of the form are 'Cancel', 'Repeat', and 'Finished' buttons.

## INTEGRATION GUIDE

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

4. In the New VLAN Menu
  - 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.

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

**General Properties**

Name	TransitNet-1
Description	
Tag	177

**Resources**

Interfaces	Interface: 1.2
	Tagging: Tagged
	Add
	1.1 (tagged)
	Edit Delete

**Configuration:** Basic

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

**sFlow**

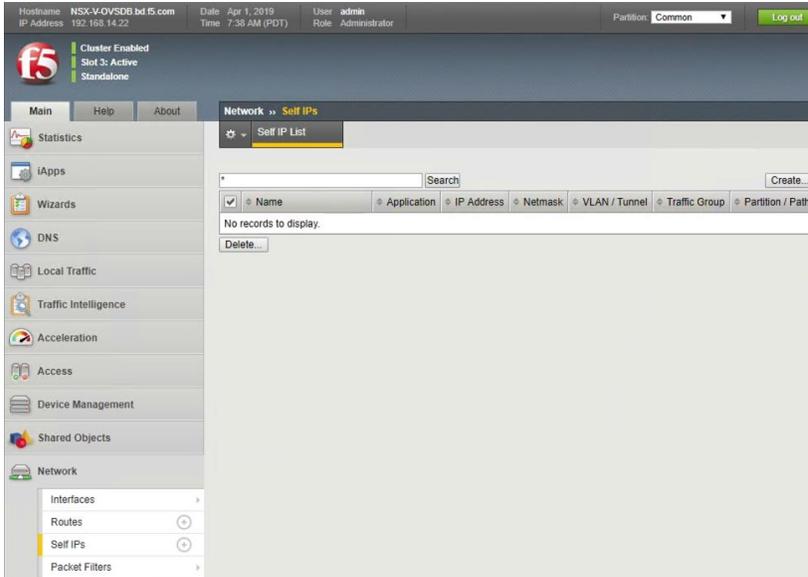
Polling Interval	Default
Sampling Rate	Default

Cancel Repeat Finished

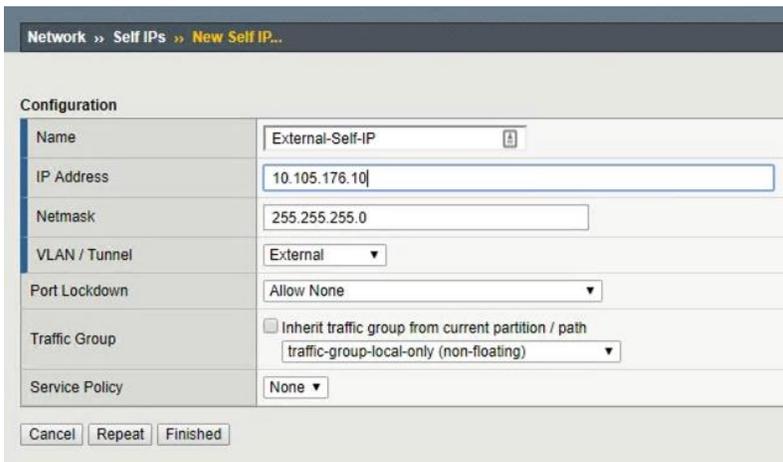
## Configure Self IP Addresses

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



## 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 form. The breadcrumb navigation is 'Network >> Self IPs >> New Self IP...'. The form fields are as follows:

Configuration	
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

Buttons: Cancel, Repeat, Finished

The screenshot shows the 'Self IP List' table. The breadcrumb navigation is 'Network >> Self IPs'. The table has columns for Name, Application, IP Address, Netmask, VLAN / Tunnel, Traffic Group, and Partition / Path. There are two entries: 'External-Self-IP' and 'Transit-Self-IP'.

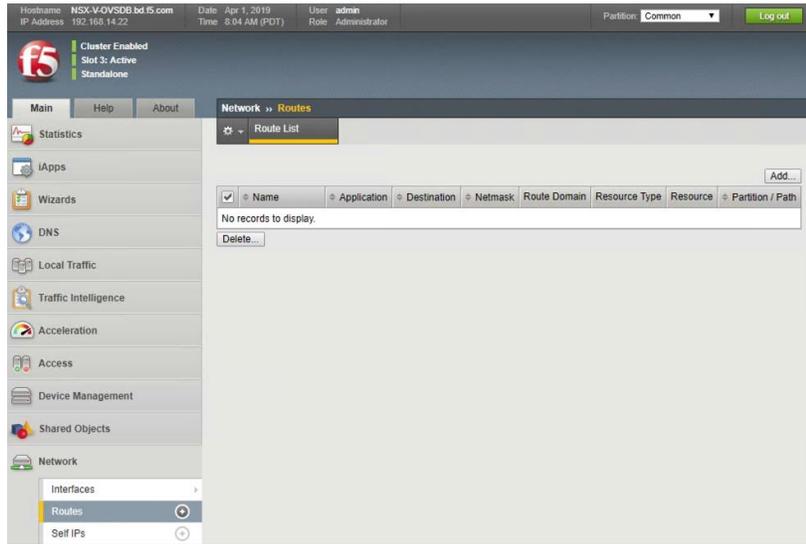
	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	External-Self-IP		10.105.176.10	255.255.255.0	External	traffic-group-local-only	Common
<input type="checkbox"/>	Transit-Self-IP		172.16.1.2	255.255.255.0	TransitNet-1	traffic-group-local-only	Common

Buttons: Search, Create..., Delete...

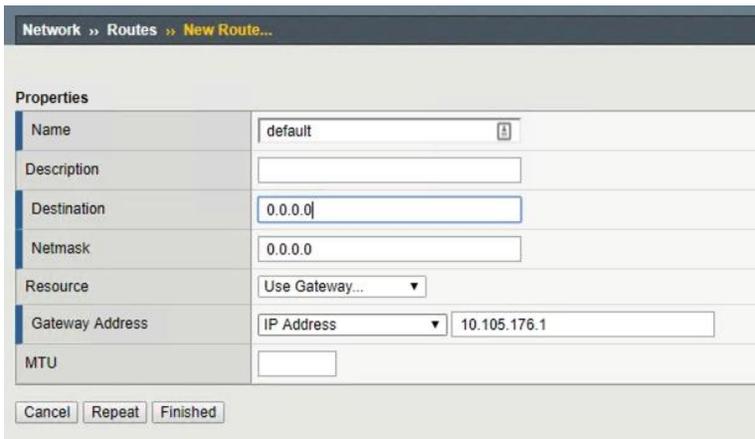
## Configure Static Routes

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 Add 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



## 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 shows the 'New Route...' configuration form. The breadcrumb navigation is 'Network >> Routes >> New Route...'. The form has a 'Properties' section with the following fields:

Name	ServerRoutes
Description	
Destination	10.0.0.0
Netmask	255.255.0.0
Resource	Use Gateway...
Gateway Address	IP Address   172.16.1.1
MTU	

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

The screenshot shows the 'Route List' table in the NSX management console. The breadcrumb navigation is 'Network >> Routes'. The table has the following columns: Name, Application, Destination, Netmask, Route Domain, Resource Type, Resource, and Partition / Path. There are two rows of data.

<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

Buttons 'Add...' and 'Delete...' are visible at the top right and bottom left of the table area, respectively.

# 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: (Optional)</p> <p>Address: 10.0.1.12</p> <p>Service Port: 443 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												

Cancel Repeat Finished

## 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

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

Configuration: Basic

Name: AppServerPool

Description:

Health Monitors: /Common gateway\_icmp (Active), /Common http, http\_head\_f5, https, https\_443 (Available)

Resources

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members

Node Name: (Optional)

Address: 10.0.1.12

Service Port: 8443

Protocol: HTTPS

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

Buttons: Add, Edit, Delete, Cancel, Repeat, Finished

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

Pool List | Statistics

Search

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

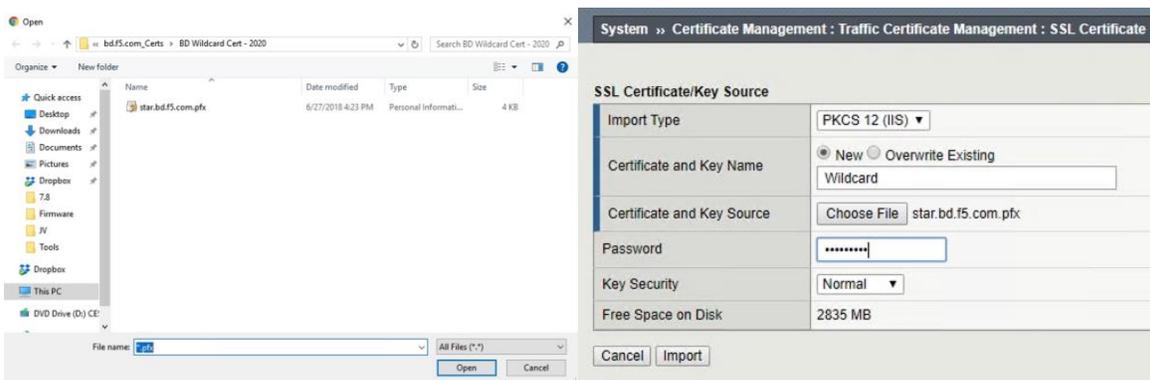
Buttons: Delete...

## 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



The image shows the 'System >> Certificate Management : Traffic Certificate Management : SSL Certificate List' page. It features a search bar and an 'Import...' button. Below is a table listing installed certificates.

Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition
<input checked="" type="checkbox"/>	Wildcard	RSA Certificate & Key	Normal	*.bd.f5.com	F5 Networks Inc	Jun 27, 2020	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle				Jan 18, 2020 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	Mar 29, 2029	Common
<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust	Dec 7, 2030	Common
<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 18, 2027	Common

Buttons at the bottom: Archive..., View Certificate Order Status..., Delete OCSP Cache..., Delete...

## 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.

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

**General Properties**

Name: WildcardSSL

Parent Profile: clientssl

Configuration: Basic Custom

Certificate Key Chain:  Add Edit Delete

**Add SSL Certificate Key Chain**

Certificate: Wildcard

Key: Wildcard

Chain: Wildcard

Passphrase:

Add Cancel

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

**General Properties**

Name: WildcardSSL

Parent Profile: clientssl

Configuration: Basic Custom

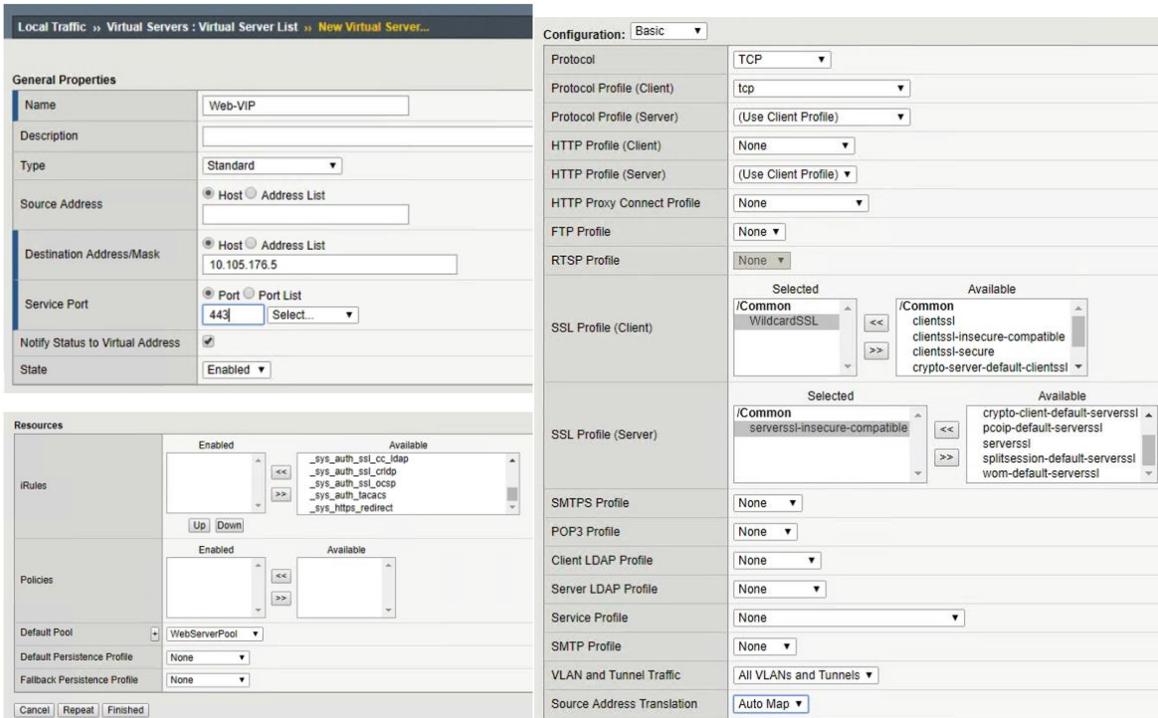
Certificate Key Chain: /Common/Wildcard /Common/Wildcard /Common/Wildcard Add Edit Delete

OCSP Stapling:

## 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).

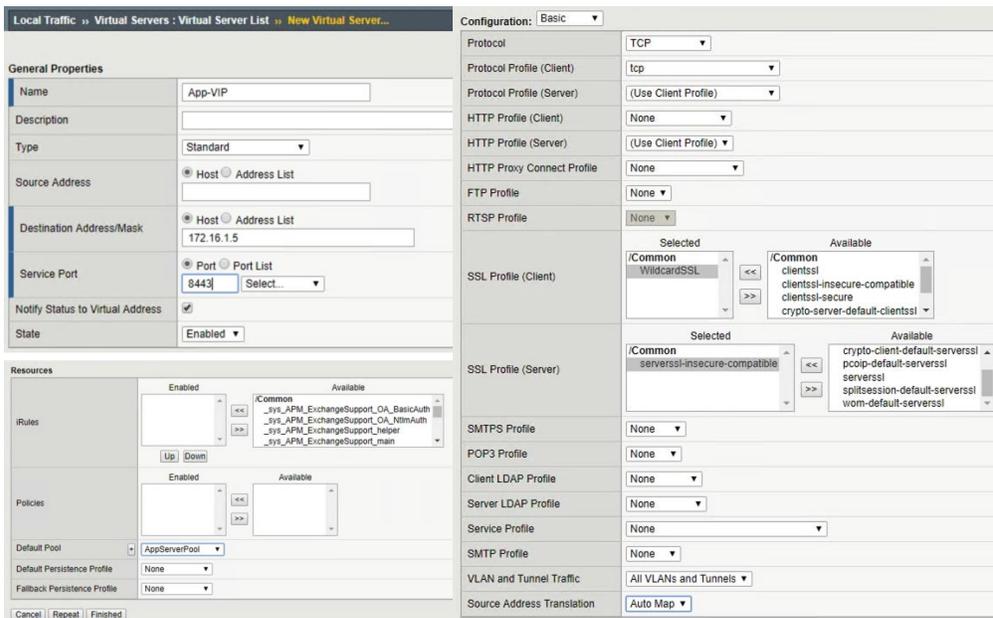
1. On the Main tab, select Local Traffic and then click Virtual Servers. The Virtual Server List screen is displayed.
2. In the upper right corner of the screen, click the Create button.
3. In the New Virtual Server menus
  - a. In the Name field, provide a unique name for the web application. In this 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



**INTEGRATION GUIDE**

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

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



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

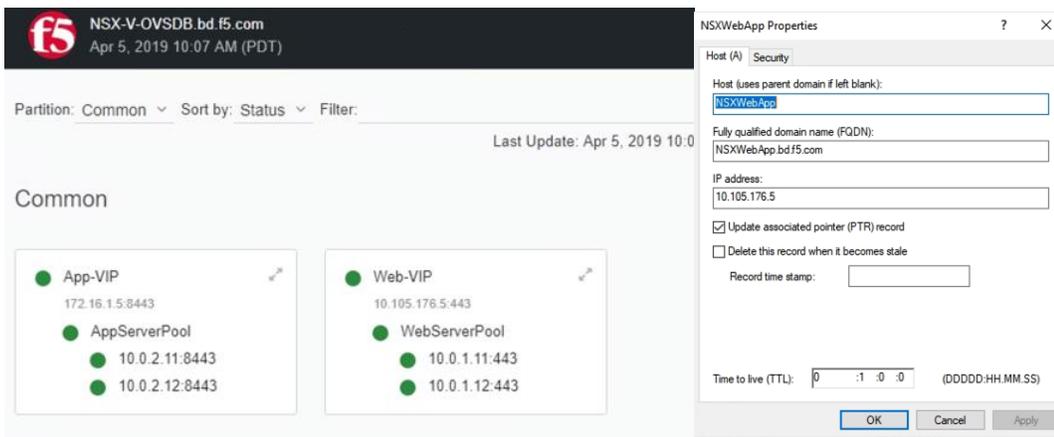
Local Traffic >> Virtual Servers : Virtual Server List									
Virtual Server List   Virtual Address List   Statistics									
* Search [ ] Create...									
✓	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
	●	App-VIP			172.16.1.5	8443	Standard	Edit...	Common
	●	Web-VIP			10.105.176.5	443 (HTTPS)	Standard	Edit...	Common

Enable | Disable | Delete...

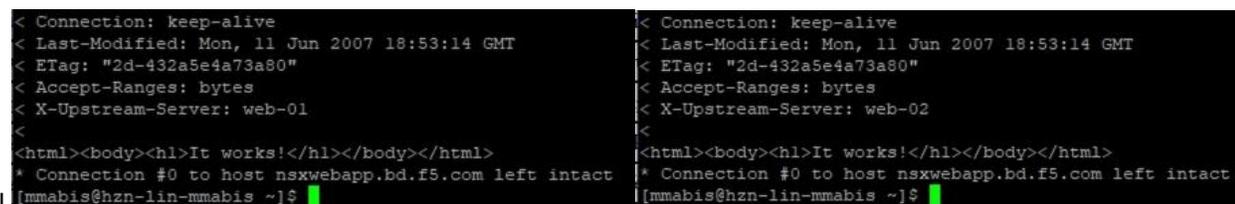
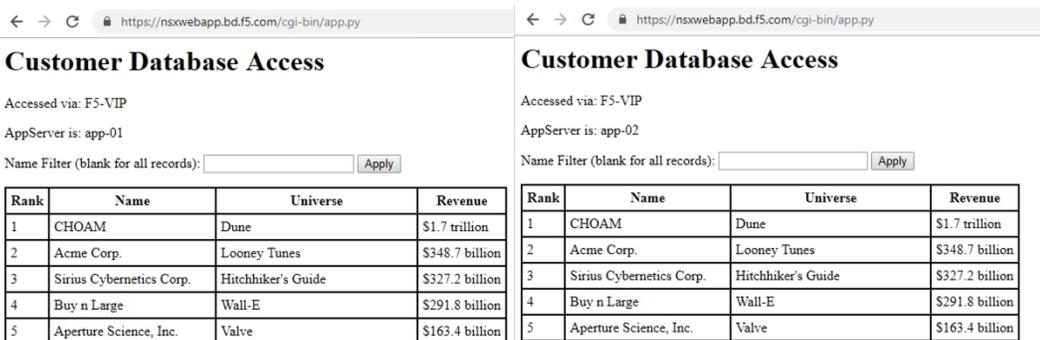
## Validation

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

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



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



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

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

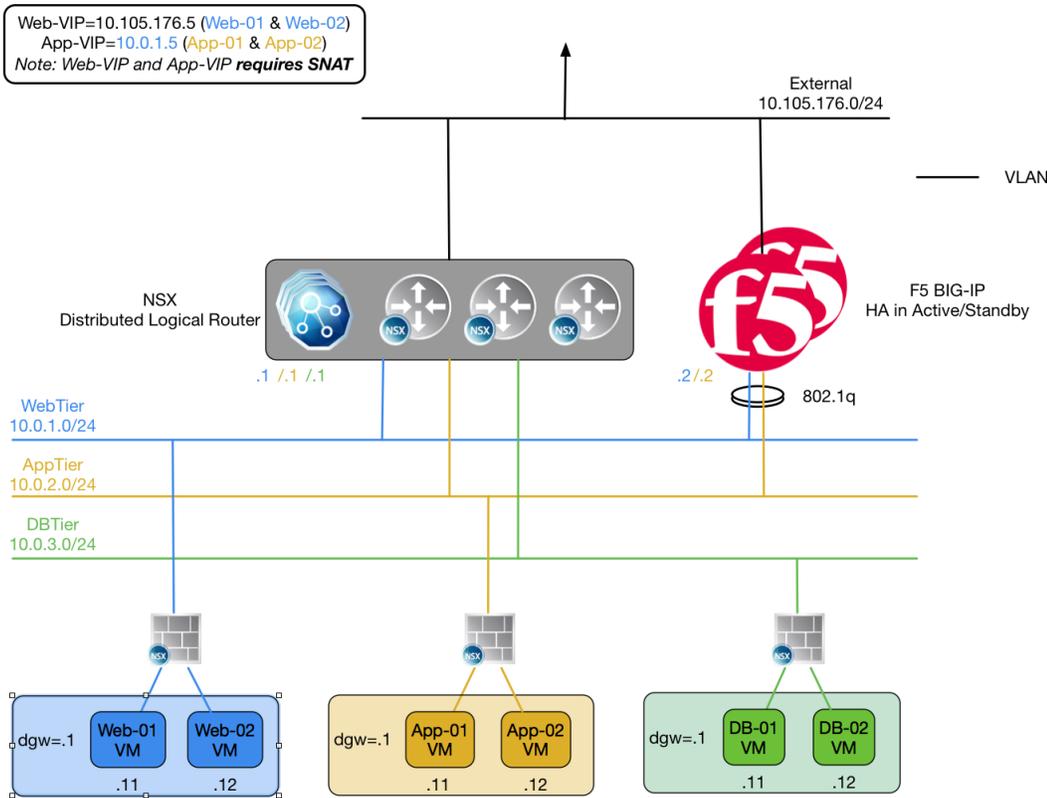


Figure 5 BIG-IP appliance parallel to NSX Distributed Logical Router

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

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

## INTEGRATION GUIDE

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

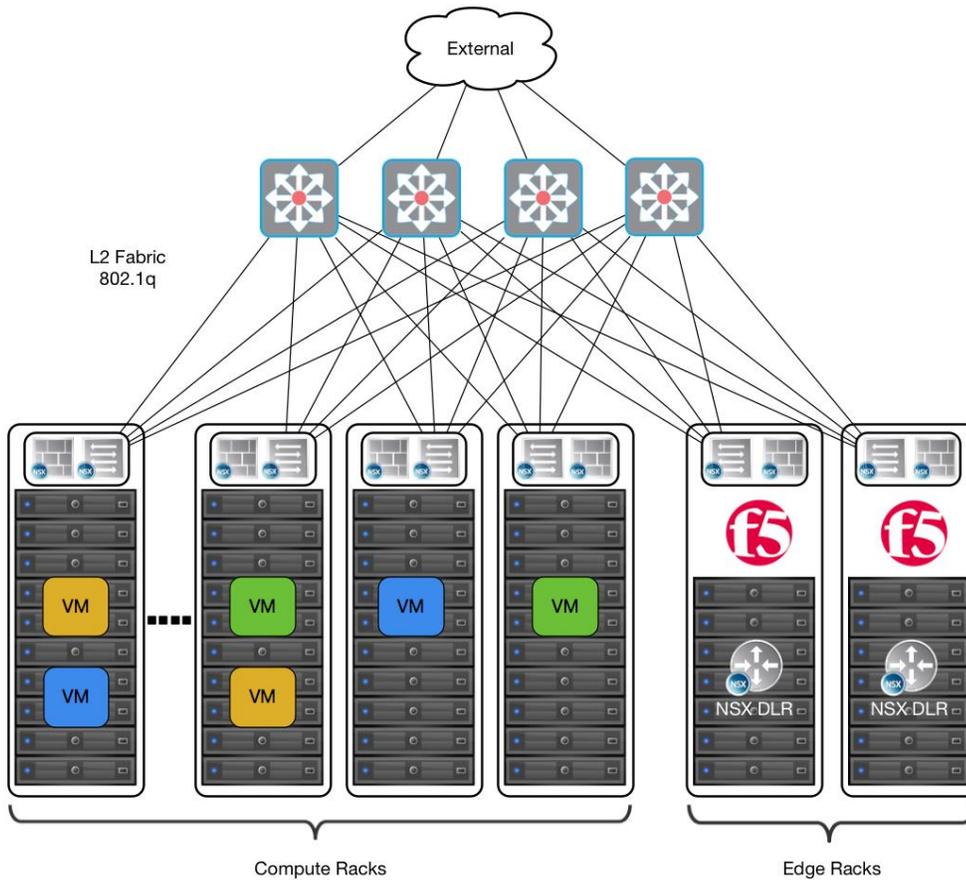


Figure 6 Leaf/spine physical rack infrastructure

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.

# Traffic Flows

## North-South Traffic - Logical Traffic Flows as Follows

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

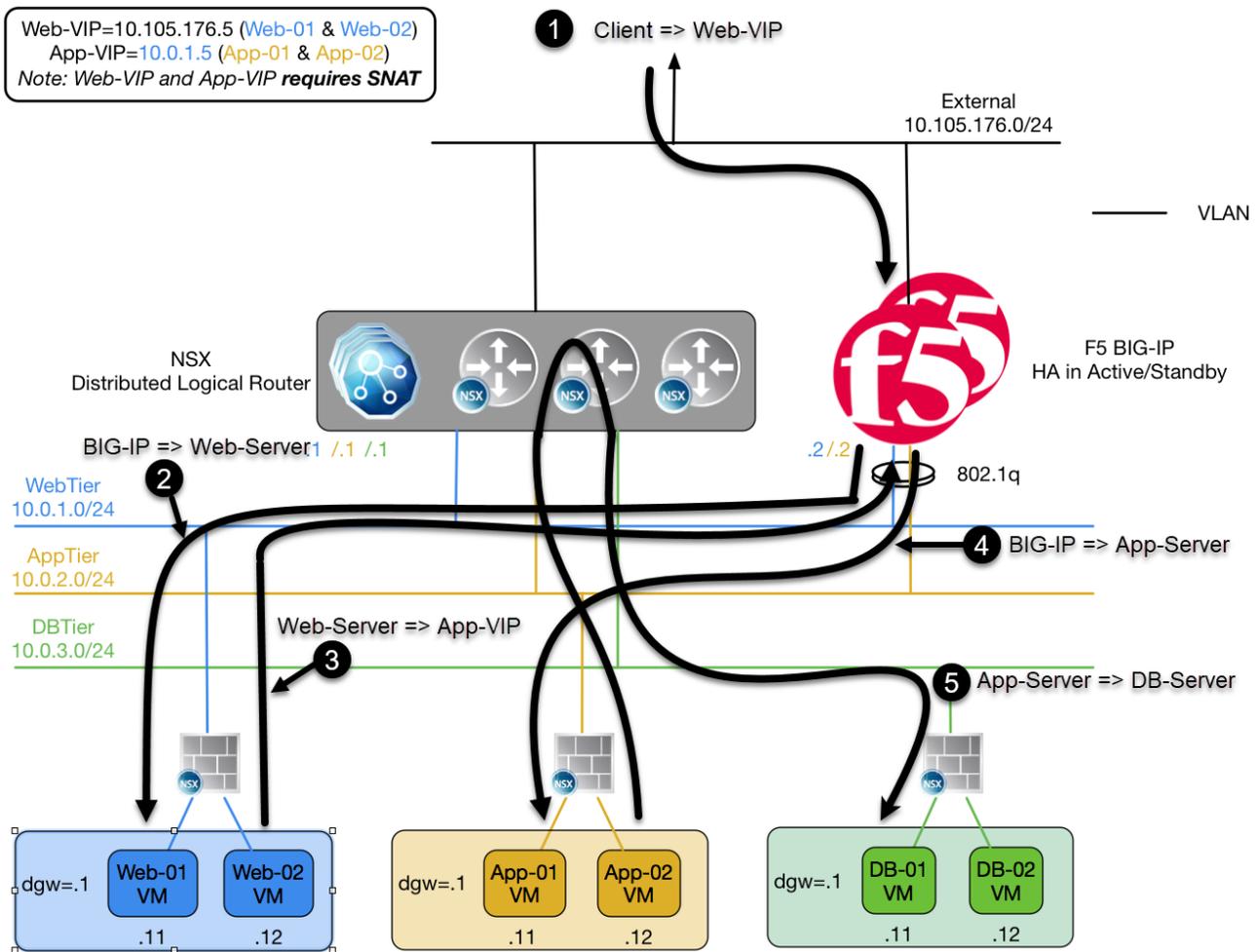


Figure 7 North-South Logical Traffic Flow "Parallel to DLR" with BIG-IP Appliances

## Implementation Infrastructure

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

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 8: the Cluster1-VDC (Edge Rack) and Cluster3-Compute-NSX (Compute Rack). While this is a smaller representation of a typical data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 6.



Figure 8 vSphere Console

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

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

## Prerequisites

Referencing the diagram in Figure 5, the BIG-IP requires connectivity to at minimum two of its interfaces. One interface is used for management of the device and the other is used for all production traffic. The VLAN numbers and the IP addressing scheme can be tailored to your environment.

- The BIG-IP will need to be installed and connected (physically or virtually) to the infrastructure rack which is connected to L2 Fabric (802.1q). Each BIG-IP management interface will need to be connected and configured with an IP address in the management segment.
- The BIG-IP interface 1.1 will need to be connected to a switch port either in ESXi (trunked port group) or on the edge rack top-of-rack switch that 802.1Q tags the VLANs used in this environment. In the example, VLANs 102, 176, 177, 178 and 179 are used.
- Physical network infrastructure switches connected to the ESXi servers and BIG-IP appliances (if not virtual) are configured to support 802.1Q tagging and allow the appropriate VLANs.
- ESXi hosts will need to be configured with the appropriate distributed port groups and virtual switches.

Name	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176-External	176
Internal	DVS-VLAN-102	102
WebTier	DVS-VLAN-177-WebTier	177
AppTier	DVS-VLAN-178-AppTier	178
DBTier	DVS-VLAN-179-DBTier	179

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

# Network Segments

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

## 802.1Q VLAN segments

- **VLAN 176 (External)** is the VLAN used for external connectivity. The 10.105.176.0/24 IP subnet range is configured on this VLAN.
- **VLAN 102 (Internal)** (not shown) is for management connectivity. The 192.168.14.0/24 IP subnet range is configured on this VLAN
- **VLAN 177 WebTier** is the VLAN ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VLAN.
- **VLAN 178 AppTier** is the VLAN ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VLAN.
- **VLAN 179 DBTier** is the VLAN ID used for the green DB connectivity. The 10.0.3.0/24 IP subnet range is configured on this VLAN.

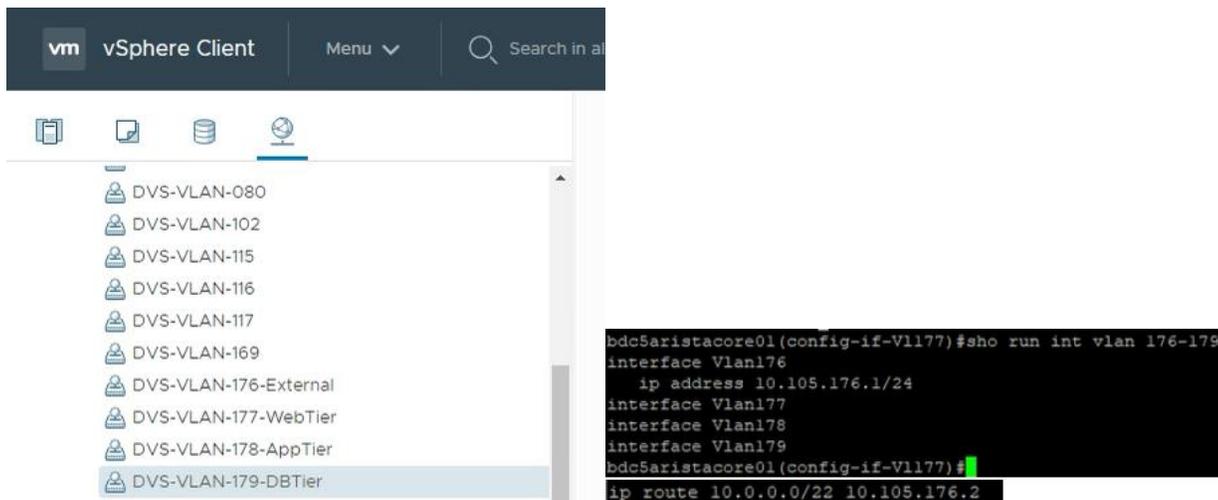


Figure 9 vSphere Client (HTML5) Console & Core Switch VLAN Gateways and IP Route for 10.0.0.0 segment

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

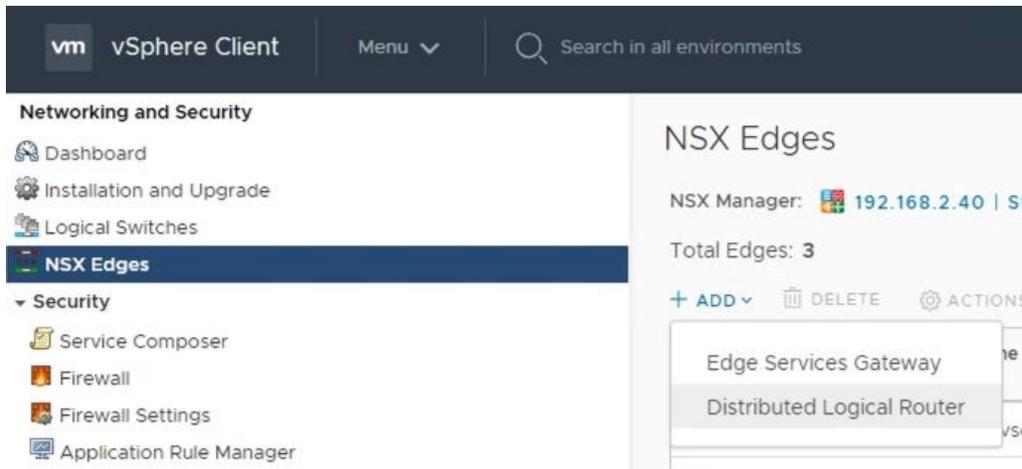
The top-of-rack switches must have at least these four VLANs tagged up to the L2 Fabric (802.1q)

## Create and Deploy DLR

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

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

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



## INTEGRATION GUIDE

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

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

### New Distributed Logical Router

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

#### Basic Details

Distributed logical router provides Distributed Routing and Bridging capabilities.

Name

Host Name

Tenant

Description

Select Deployment Options

Deploy Control VMs  
Deploys Edge Appliance VM to support Firewall and Dynamic routing.

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

HA Logging Disabled

Log Level

CANCEL NEXT FINISH

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.

### New Distributed Logical Router

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

#### Settings

CLI credentials will be set on the Edge Appliance VM(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name \*

Password \*

Confirm Password \*

SSH access Enabled

FIPS Mode Disabled

Edge control level logging

CANCEL BACK NEXT 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.

New Distributed Logical Router

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

### Deployment Configuration

Datacenter \* vCloud-VDC

Control VM(s) \*

+  
Add Edge Appliance VM

No records to display

**Management/ HA Interface**  
This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To \*

IP Address E.g. 10.121.30.4/24

CANCEL BACK NEXT FINISH

- 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.

### Add Edge Appliance VM

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

CPU 1000 MHz

Memory 512 MB

CANCEL ADD

## 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

New Distributed Logical Router

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

### Deployment Configuration

Datacenter **\*** vCloud-VDC

Control VM(s) **\***

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB

**Management/ HA interface**  
This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To **\***

IP Address

**Buttons:** CANCEL, BACK, NEXT, FINISH

**Visuals:** A large blue plus sign and the text "Add Edge Appliance VM" are displayed in a box on the right side of the configuration area.

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

Back Select Network

Logical Switch Distributed Virtual Port Group

Search

Name	Type
<input type="radio"/> ESX-Management-Tagged	Distributed Virtual Port Group
<input type="radio"/> ESX-Storage	Distributed Virtual Port Group
<input type="radio"/> DVS-VLAN-080	Distributed Virtual Port Group
<input checked="" type="radio"/> DVS-VLAN-102	Distributed Virtual Port Group
<input type="radio"/> ESX-Trunk-Prom	Distributed Virtual Port Group
<input type="radio"/> ESX-NSX	Distributed Virtual Port Group
<input type="radio"/> DVS-VLAN-176	Distributed Virtual Port Group
<input type="radio"/> ESX-Management-Untagged	Distributed Virtual Port Group
<input type="radio"/> ESX-Trunk	Distributed Virtual Port Group
<input type="radio"/> ESX-vSAN	Distributed Virtual Port Group

1 - 30 of 30 items

**Buttons:** CANCEL, 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

The screenshot shows the 'Deployment Configuration' dialog for a 'New Distributed Logical Router'. The left sidebar lists steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration (selected), 4 Interface, 5 Default Gateway, and 6 Review. The main area is titled 'Deployment Configuration' and includes the following fields:

- Datacenter**: vCloud-VDC
- Control VM(s)**: A table with the following details:

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB
- Management/ HA Interface**: A note states, 'This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.' Below this, the **Connected To** field is set to 'DVS-VLAN-102' and the **IP Address** field is set to '192.168.14.128/24'.

At the bottom right, there are buttons for CANCEL, BACK, NEXT (highlighted), and FINISH. A large blue plus sign and the text 'Add Edge Appliance VM' are visible in a separate box on the right side of the dialog.

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

The screenshot shows the 'Configure Interfaces' dialog for a 'New Distributed Logical Router'. The left sidebar lists steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration, 4 Interface (selected), 5 Default Gateway, and 6 Review. The main area is titled 'Configure Interfaces' and includes the following elements:

- A heading: 'Configure interfaces of this distributed logical router.'
- Buttons: + ADD, EDIT, and DELETE.
- A table with columns: Name, Type, IP Address, and Connected To.
- The table is currently empty, displaying the message 'No records to display'.
- At the bottom right, there are buttons for CANCEL, BACK, NEXT (highlighted), and FINISH.

## 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

< Back Configure Interfaces

Name \* External

Type  Internal  Uplink

Connected To \*

Connectivity Status Disconnected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Subnet Prefix Length
--------------------	----------------------

0 items

MTU 1500

CANCEL OK

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

< Back Select Network

Logical Switch Distributed Virtual Port Group

external

Name	Type
DVS-VLAN-176-External	Distributed Virtual Port Group

1 - 1 of 1 items

CANCEL 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.

The screenshot shows the 'Configure Interfaces' dialog box. The 'Name' field is 'External'. The 'Type' is 'Uplink'. The 'Connected To' field is 'DVS-VLAN-176-External'. The 'Connectivity Status' is 'Connected'. The 'Configure Subnets' section has a '+ ADD' button and a 'DELETE' button. Below this is a table with two columns: 'Primary IP Address' and 'Subnet Prefix Length'. The table is currently empty. The 'MTU' field is set to '1500'. At the bottom right, there are 'CANCEL' and 'OK' buttons.

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

The screenshot shows the 'Configure Interfaces' dialog box. The 'Name' field is 'External'. The 'Type' is 'Uplink'. The 'Connected To' field is 'DVS-VLAN-176-External'. The 'Connectivity Status' is 'Connected'. The 'Configure Subnets' section has a '+ ADD' button and a 'DELETE' button. Below this is a table with two columns: 'Primary IP Address' and 'Subnet Prefix Length'. The table now contains one row with the IP address '10.105.176.2' and a Subnet Prefix Length of '24'. The 'MTU' field is set to '1500'. At the bottom right, there are 'CANCEL' and 'OK' buttons.

## 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

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

### Configure Interfaces

Configure interfaces of this distributed logical router.

[+ ADD](#) [EDIT](#) [DELETE](#)

Name	Type	IP Address	Connected To
<input type="radio"/> External	Uplink	10.105.176.2/24	DVS-VLAN-176-External
<input type="radio"/> WebTier	Internal	10.0.1.1/24	DVS-VLAN-177-WebTier
<input type="radio"/> AppTier	Internal	10.0.2.1/24	DVS-VLAN-178-AppTier
<input type="radio"/> DBTier	Internal	10.0.3.1/24	DVS-VLAN-179-DBTier

4 items

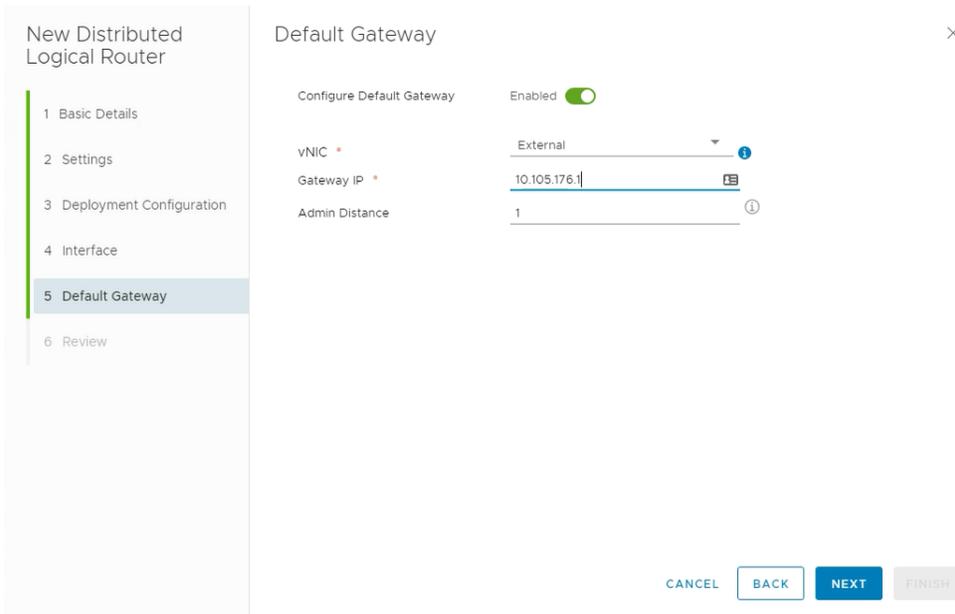
[CANCEL](#) [BACK](#) [NEXT](#) [FINISH](#)

**INTEGRATION GUIDE**

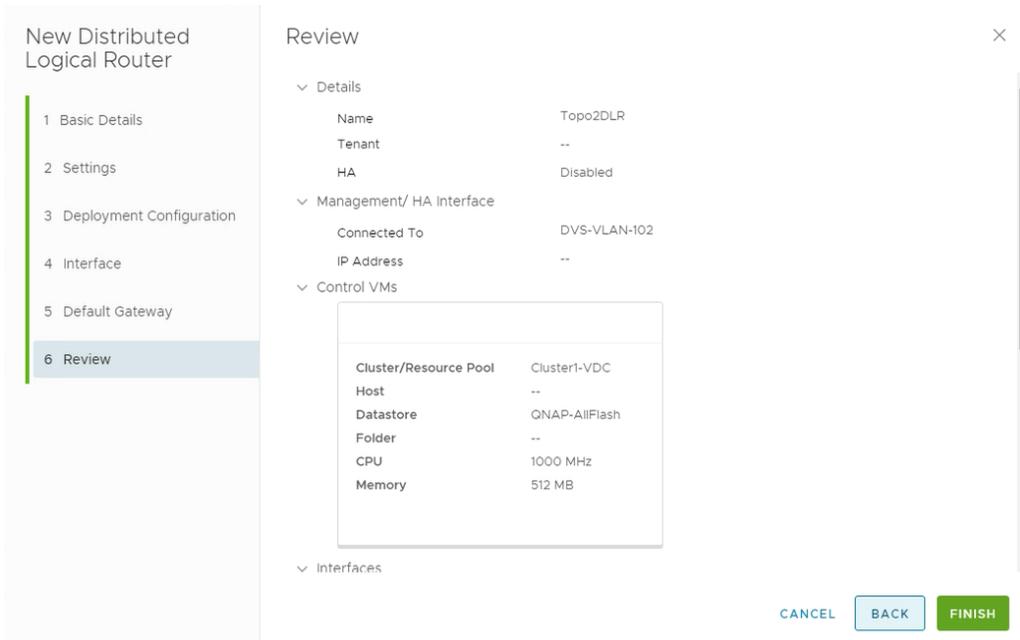
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

- 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.



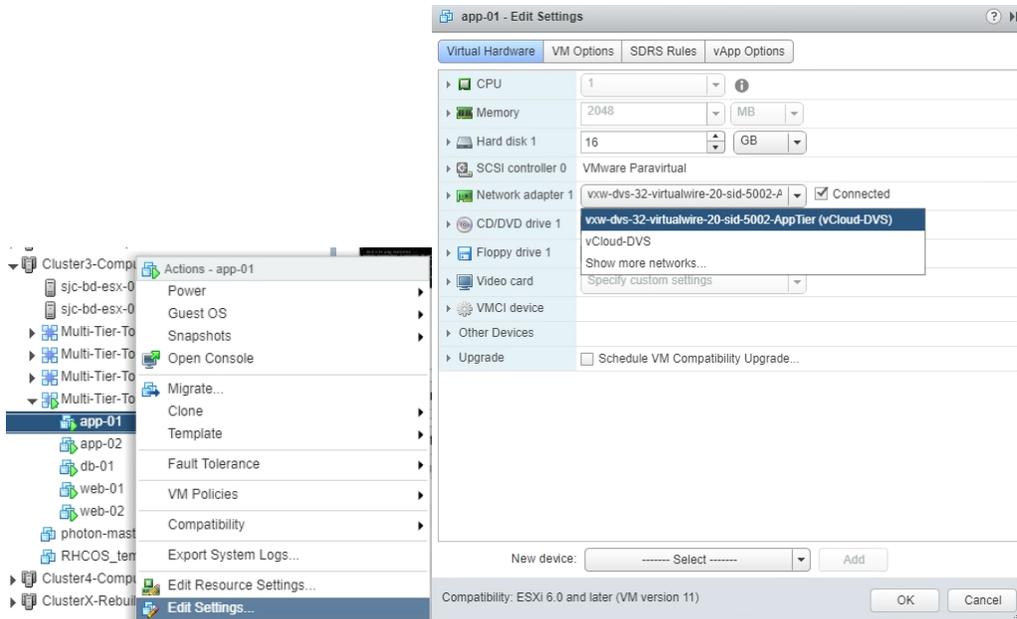
- 18. Review and click finish to complete the deployment of the NSX Distributed Logical Router.



## 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.



## BIG-IP Configuration

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

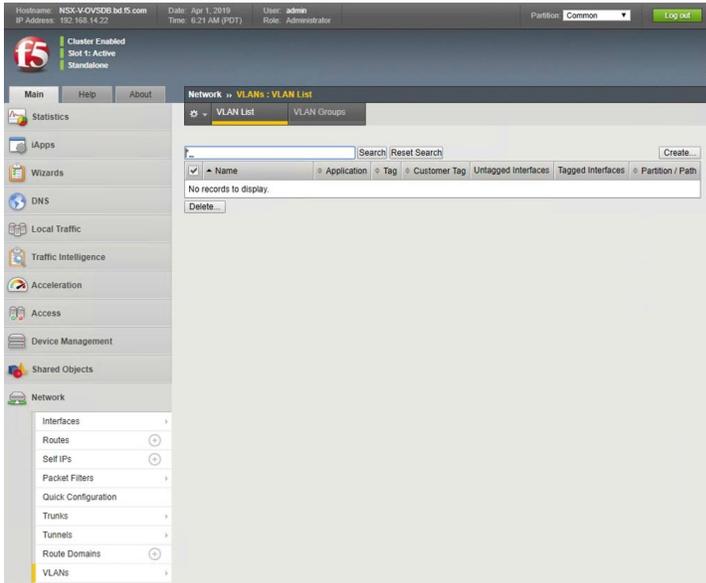
### Prerequisites

- The BIG-IP is configured with a management IP address in the proper subnet.
- Licenses have been applied and activated.
- Appropriate provisioning of resources is complete.
- Base configuration of services DNS, NTP, SYSLOG are configured.
- BIG-IP Interface 1.1 or an available interface that is connected to a physical or virtual switch (trunk) configured to support 802.1Q tagging of traffic. In our specific use case we use VLANs 176-179.

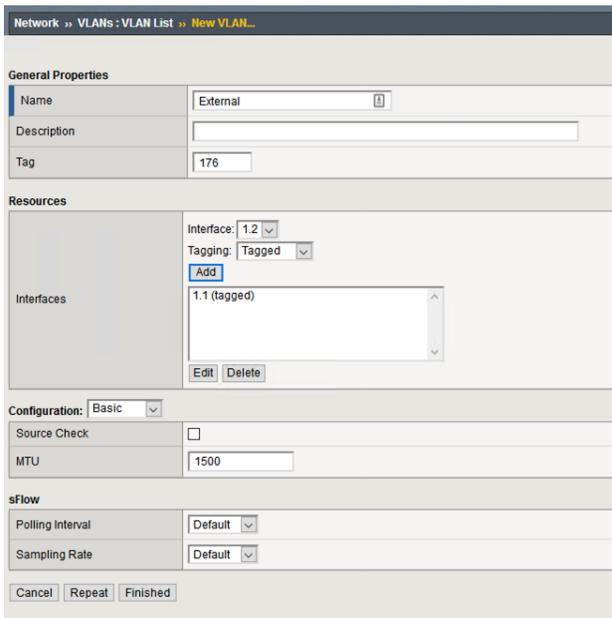
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

## Create VLANs

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



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



## INTEGRATION GUIDE

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

4. In the New VLAN Menu
  - 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**

Interface: 1.2  
Tagging: Tagged  
**Add**  
1.1 (tagged)  
Edit Delete

**Configuration:** Basic

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

**sFlow**

Polling Interval	Default
Sampling Rate	Default

Cancel Repeat Finished

Network » VLANs : VLAN List

VLAN List VLAN Groups

\* Search Create...

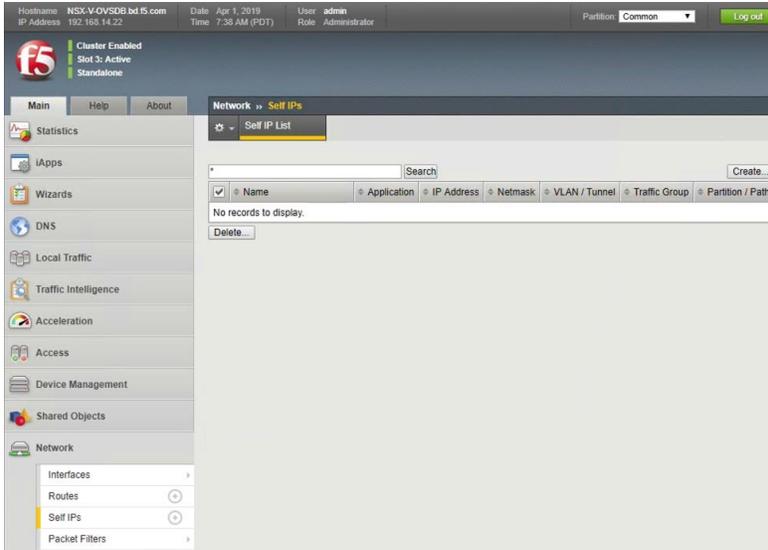
<input checked="" type="checkbox"/>	Name	Application	Tag	Customer Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	External		176			1/1,1	Common
<input type="checkbox"/>	WebTier		177			1/1,1	Common
<input type="checkbox"/>	AppTier		178			1/1,1	Common

Delete...

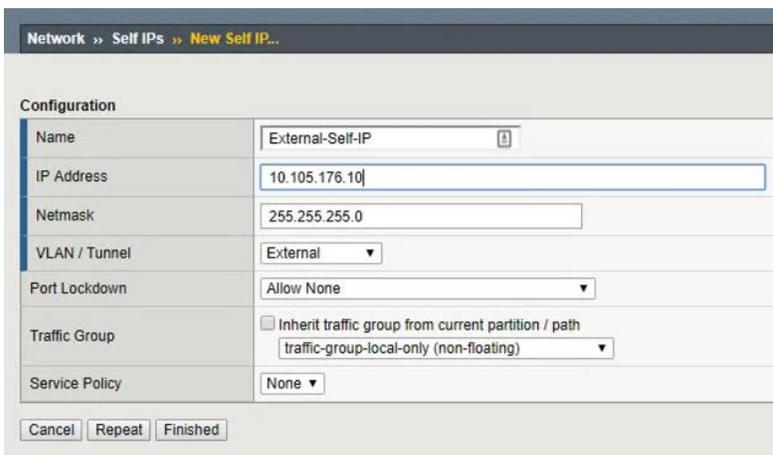
## Configure Self IP Addresses

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 Menu
  - 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



## 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

Cancel Repeat Finished

Network >> Self IPs

Self IP List

Search Create...

<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

Delete...

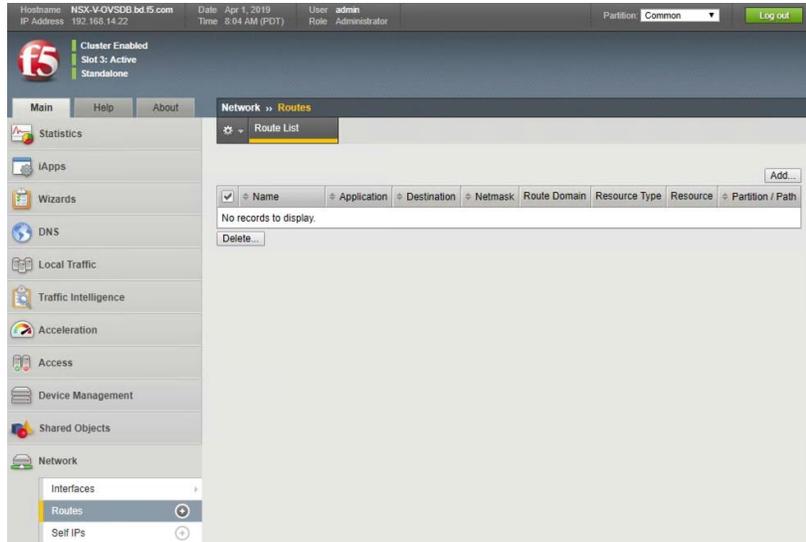
## INTEGRATION GUIDE

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 Add button.



3. In the New Route menu
  - 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.

The screenshot shows the 'New Route...' configuration dialog box. The title bar reads 'Network >> Routes >> New Route...'. The 'Properties' section 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 (dropdown), 10.105.176.1
- MTU: (empty)

At the bottom, there 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 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: (Optional)</p> <p>Address: 10.0.1.12</p> <p>Service Port: 443 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												

Cancel Repeat Finished

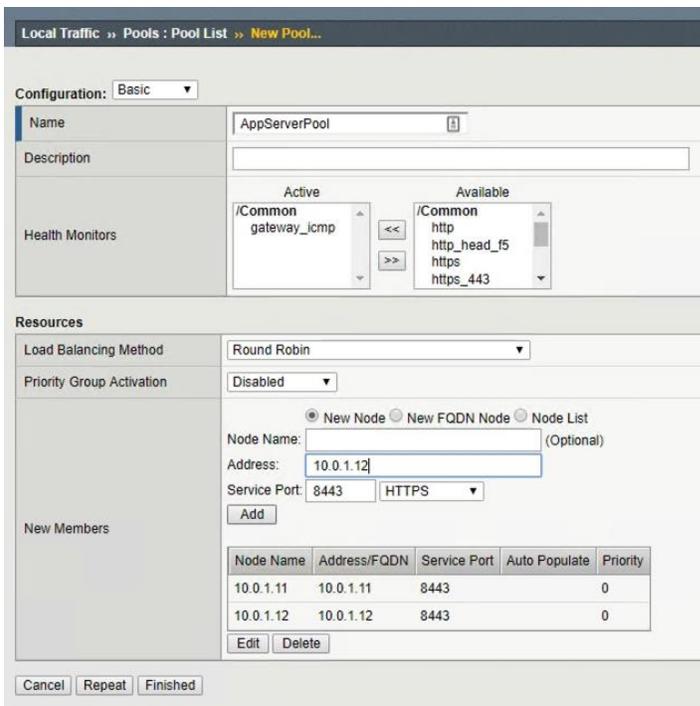
**INTEGRATION GUIDE**

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

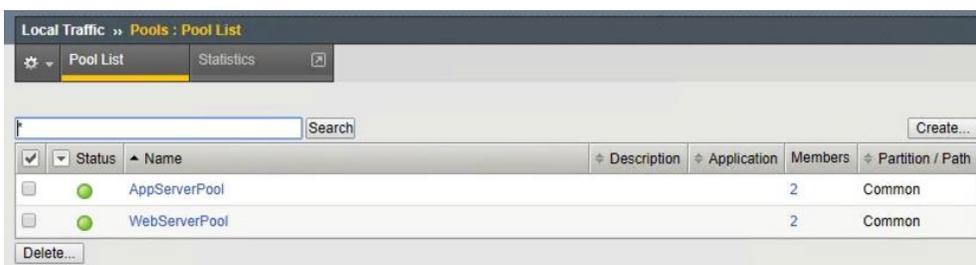
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
  - a. In the Name field, type a unique name for the app pool. For this validation AppServerPool was used.
  - b. In the Health Monitors section select an appropriate monitor for your application. 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.

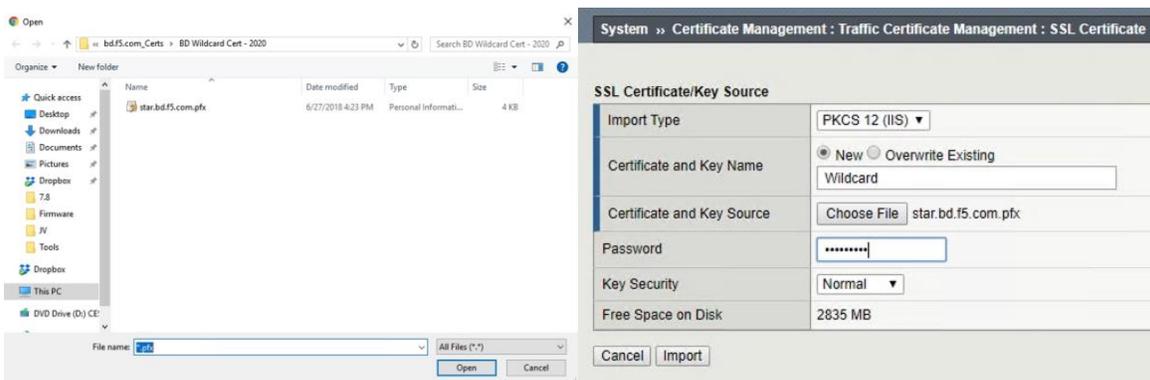


## Import SSL Certificate

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

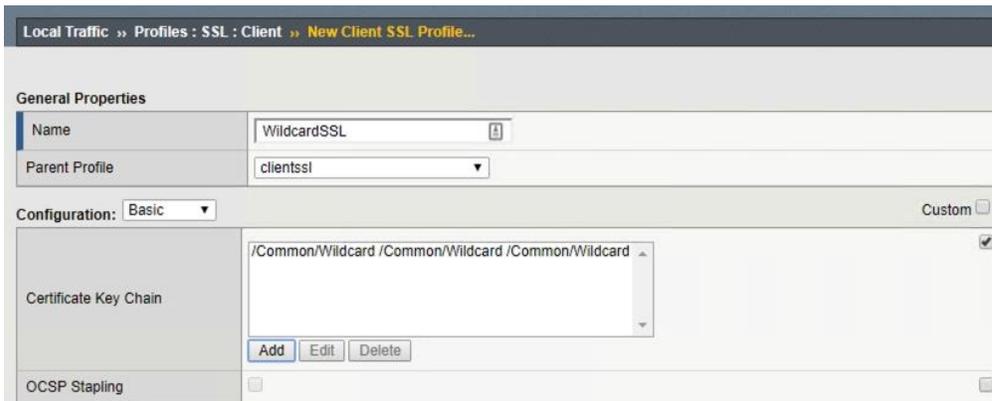
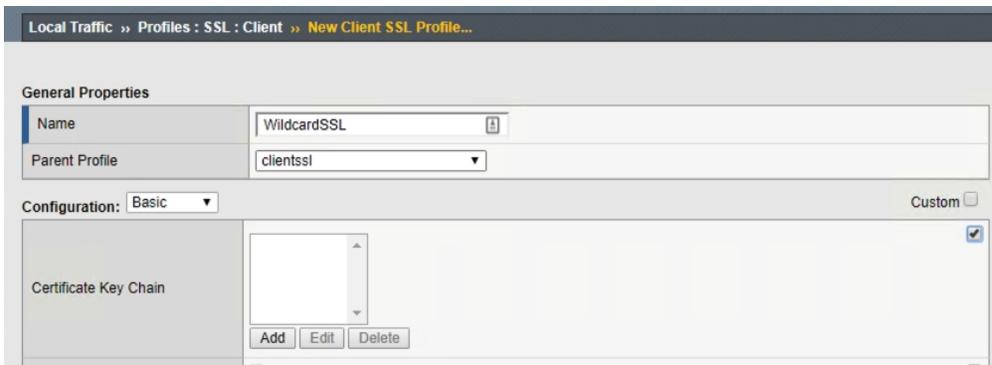


Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition
<input checked="" type="checkbox"/>	Wildcard	RSA Certificate & Key	Normal	*.bd.f5.com	F5 Networks Inc	Jun 27, 2020	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle				Jan 18, 2020 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	Mar 29, 2029	Common
<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust	Dec 7, 2030	Common
<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 18, 2027	Common

## Create ClientSSL Profile

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

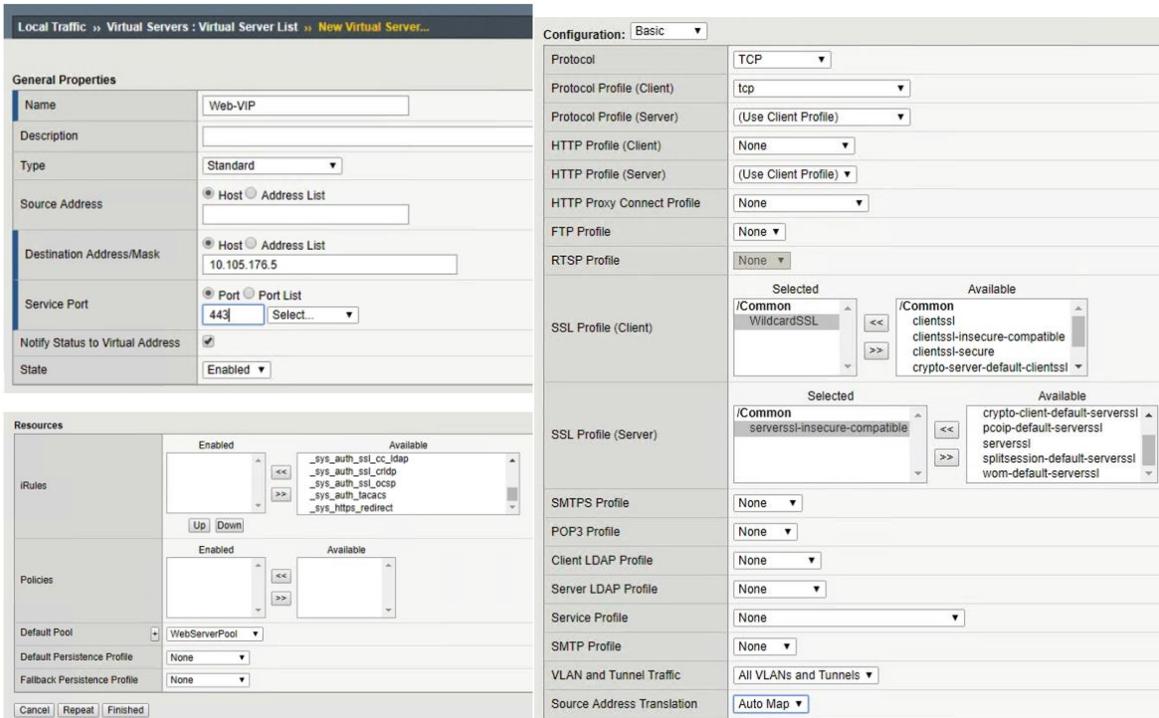
1. On the Main tab, select Local Traffic → Profiles → SSL → Client
2. In the upper right corner of the screen, click the Create button.
3. In the New Client SSL Profile menus
  - a. In the Name field, type a unique name for the profile, for this validation WildcardSSL was used.
  - b. In the Certificate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



## Create Application Virtual Servers

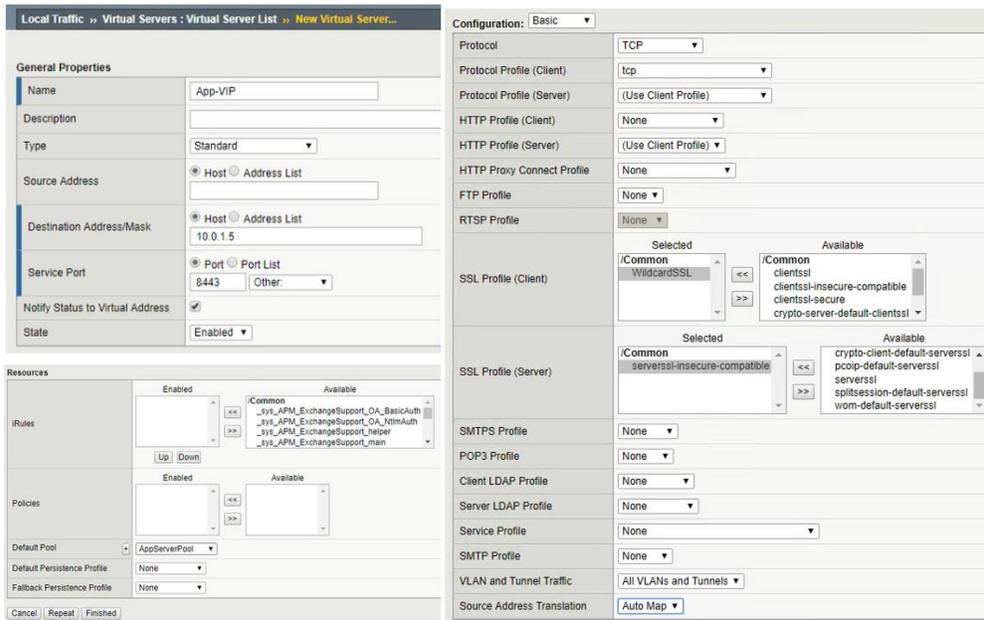
In creating a virtual server, you specify a destination IP address and service port on which the BIG-IP appliance is listening for application traffic to be load balanced to the appropriate application pool members. In this validation, we have two virtual servers (VIPs) to create: one for the web tier, which will be available to the external network on the 10.105.176.0/24 segment, and the other for the application tier, available on the TransitNet-1 segment (172.16.1.0/24).

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



4. In the New Virtual Server menus

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



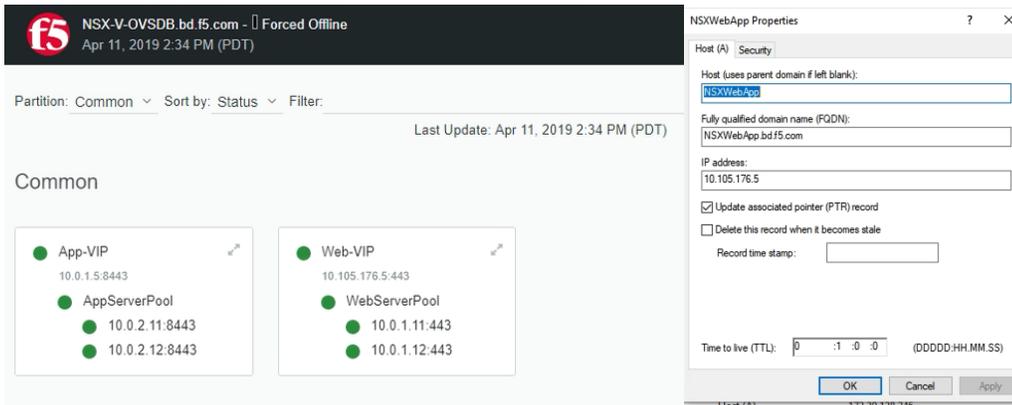
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.

Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
	App-VIP			10.0.1.5	8443	Standard	Common	
	Web-VIP			10.105.176.5	443 (HTTPS)	Standard	Common	

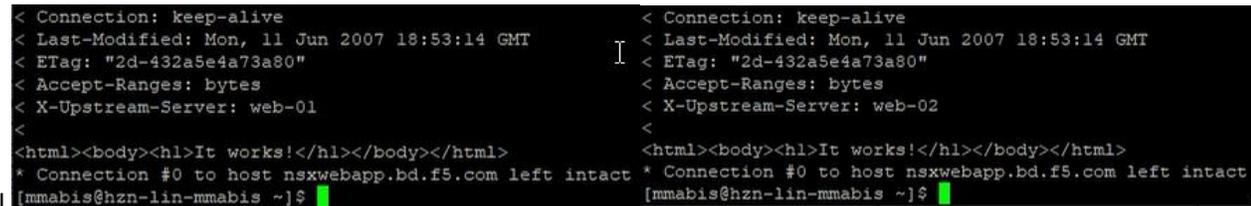
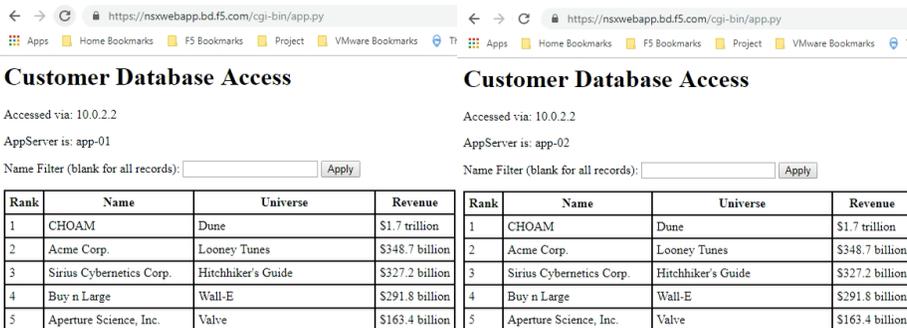
# Validation

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

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



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



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

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

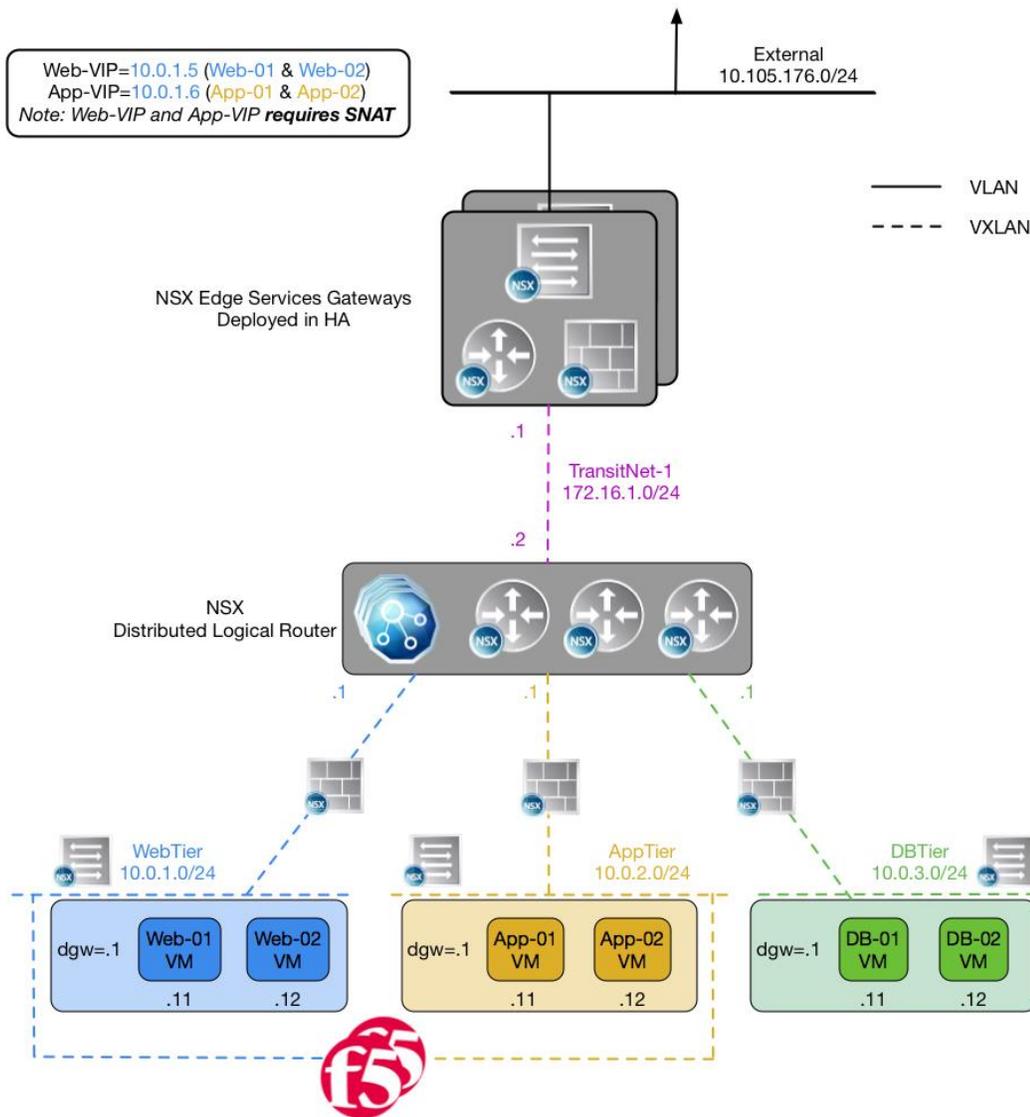


Figure 10 BIG-IP Virtual Edition in one-arm topology within VXLAN environment

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

## INTEGRATION GUIDE

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

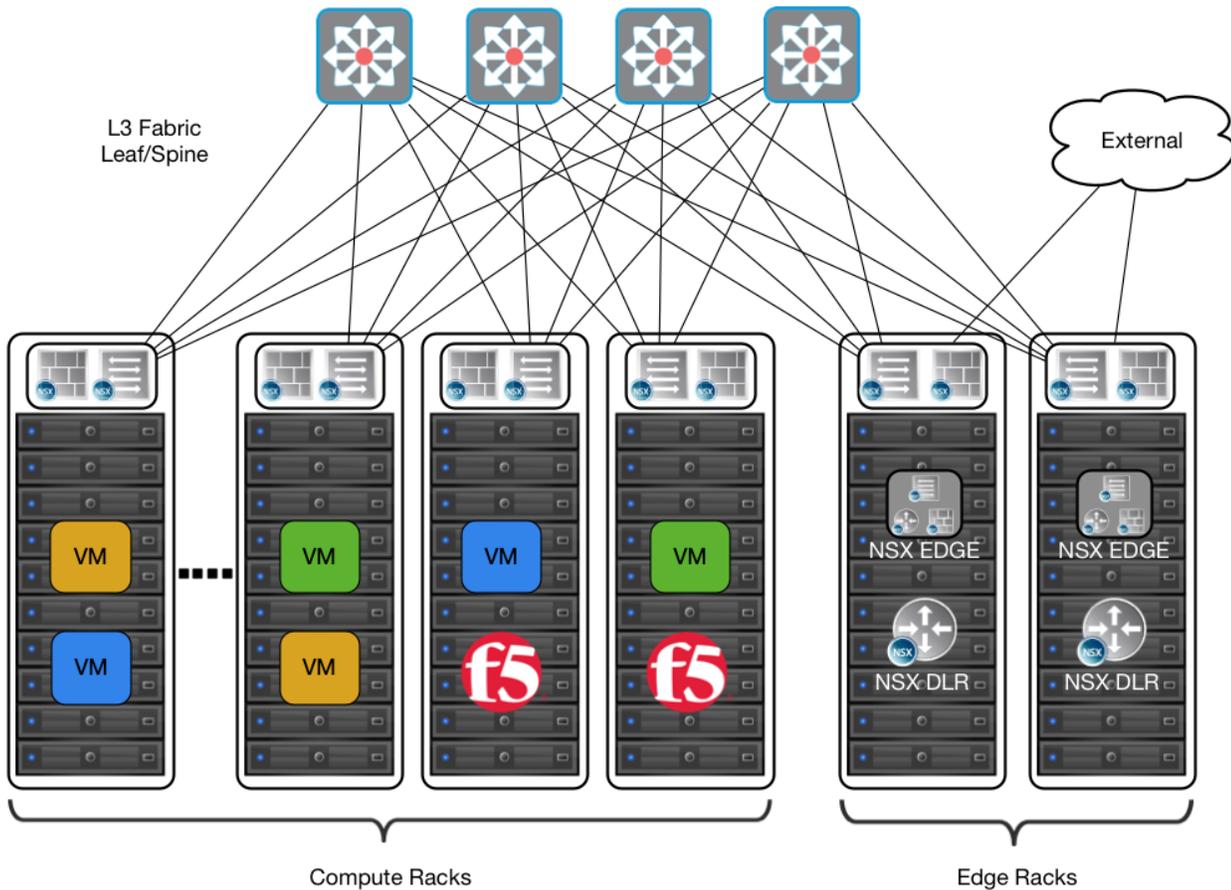


Figure 11 Leaf/spine physical rack infrastructure

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

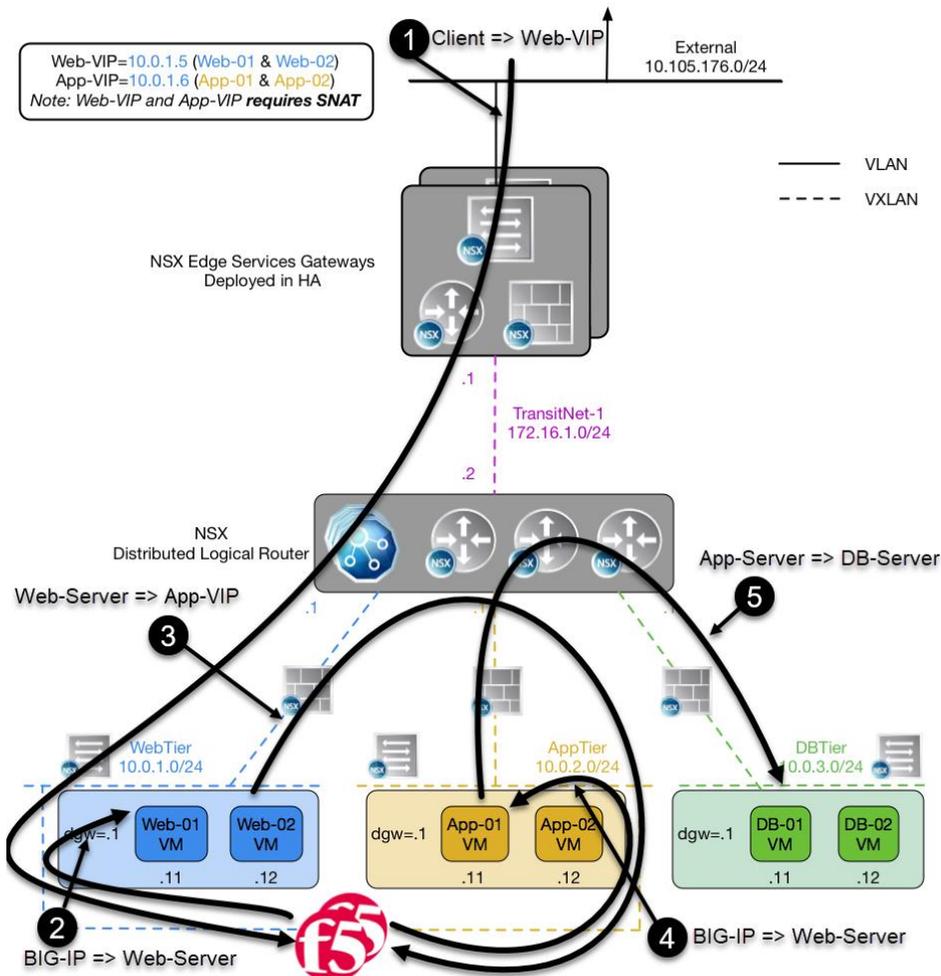


Figure 12 North-South Logical Traffic Flow "One-arm Connected" with BIG-IP Virtual Edition

## Implementation Infrastructure

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

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 13: the Cluster1-VDC (Edge Racks) and Cluster3-Compute-NSX (Compute Racks). While this is a smaller representation of a typical data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 10.



Figure 13 vSphere Console

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

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

## Prerequisites

Referencing the diagram in Figure 10, the BIG-IP Virtual Edition requires connectivity for three logical interfaces. One interface is used for management of the device and the other two are used for all production traffic. The two VLANs, WebTier and AppTier, each have one of the logical interfaces in a one-arm configuration attached to the segment. The VLAN numbers, the VXLAN Segment IDs, and the IP addressing scheme can be tailored to your environment.

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

Name	Port Group Name	802.1Q VLAN ID
External	DVS-VLAN-176	176
Internal	DVS-VLAN-102	102

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

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

Table 12 Logical switch configuration

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

# Network Segments

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

## 802.1Q VLAN segments

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

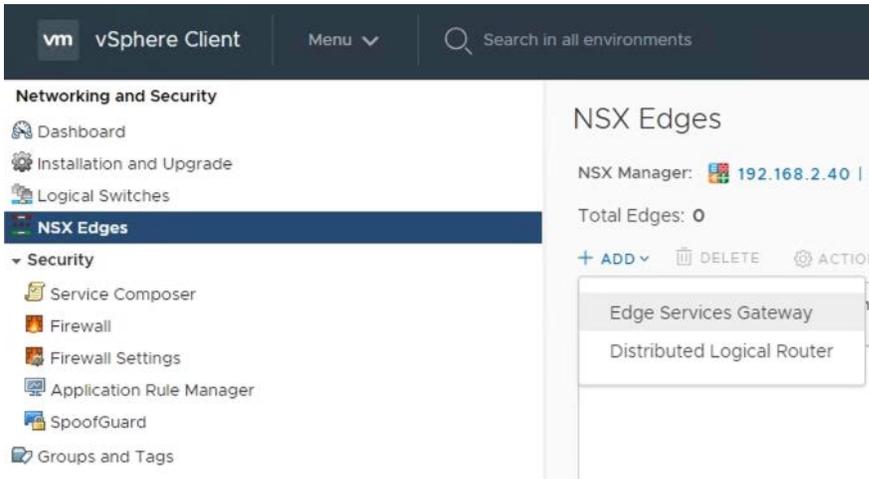
## VXLAN Segments

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

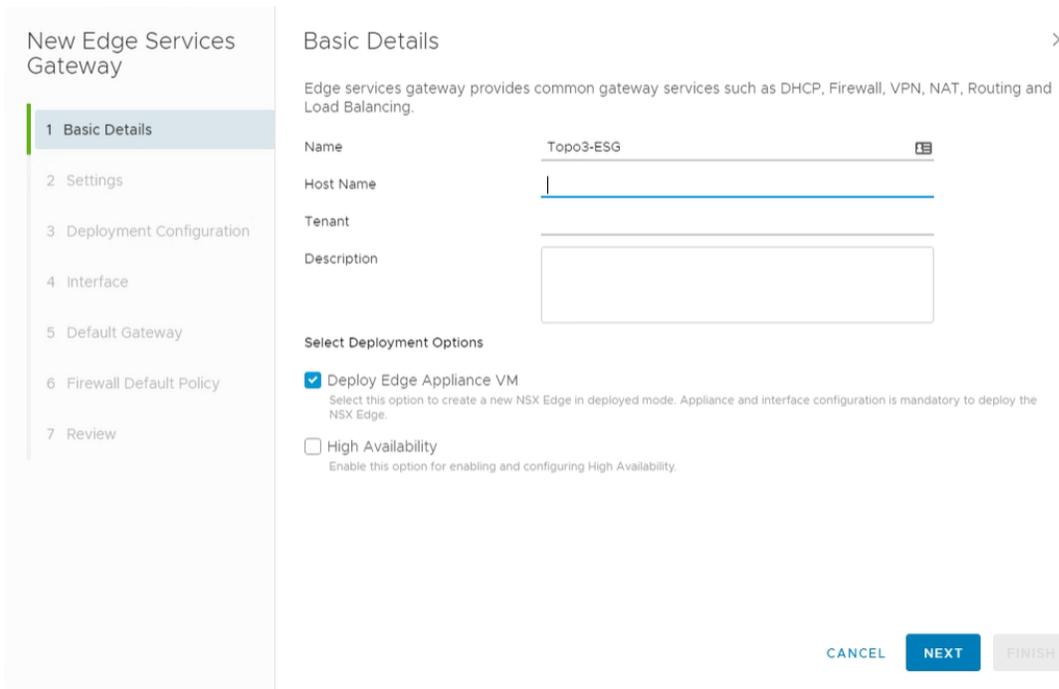
- **VXLAN 5001 WebTier** is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5002 AppTier** is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5003 DBTier**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

# NSX Edge Configuration

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



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



## 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 topdump capabilities, if you do not want these features leave SSH disabled.

New Edge Services Gateway

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

### Settings

CLI credentials will be set on the Edge Appliance VM(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name *	admin
Password *	.....
Confirm Password *	.....
SSH access	Enabled <input checked="" type="checkbox"/>
FIPS Mode	Disabled <input type="checkbox"/>
Auto Rule Generation	Enabled <input checked="" type="checkbox"/>
Edge control level logging	Info

Enable this option to automatically generate service rules to allow flow of control traffic.

CANCEL BACK NEXT FINISH

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

New Edge Services Gateway

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

### Deployment Configuration

Datacenter \* vCloud-VDC

Appliance Size \*

<input checked="" type="radio"/> Compact vCPUs 1 Memory 512 MB	<input type="radio"/> Large vCPUs 2 Memory 1 GB	<input type="radio"/> Quad Large vCPUs 4 Memory 2 GB	<input type="radio"/> X-Large vCPUs 6 Memory 8 GB
--	---	--	---

Edge Appliance VM \*

+  
Add Edge Appliance VM

No records to display

CANCEL BACK NEXT FINISH

## 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 ×

Specify placement parameters for the Edge Appliance VM.

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

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

### New Edge Services Gateway

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

### 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

## 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

Configure Interfaces

Basic | Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \*

Connectivity Status Disconnected

Configure Subnets

+ ADD DELETE Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
--------------------------	--------------------	------------------------	----------------------

0 Items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL OK

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.

Select Network

Logical Switch | Standard Port Group | Distributed Virtual Port Group

176

Name	Type
DVS-VLAN-176-External	Distributed Virtual Port Group

1 - 1 of 1 items

CANCEL 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

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \* DVS-VLAN-176-External

Connectivity Status Connected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
0 items		

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.2.1.1,1.3

CANCEL OK

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

Configure Interfaces

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \* DVS-VLAN-176-External

Connectivity Status Connected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/> 10.105.176.2		24

1 items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.2.1.1,1.3

CANCEL 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

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.

Configure Default Gateway  Enabled

vNIC \* External

Gateway IP \* 10.105.176.1

Admin Distance 1

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)

The screenshot shows the 'New Edge Services Gateway' configuration wizard at step 6, 'Firewall Default Policy'. The left sidebar lists the steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration, 4 Interface, 5 Default Gateway, 6 Firewall Default Policy (highlighted), and 7 Review. The main area shows the following settings:

- Firewall Default Policy: Enabled (toggle switch)
- Default Traffic Policy: Allow (radio button selected), Deny (radio button)
- Logging: Disabled (toggle switch)

At the bottom, there are four buttons: CANCEL, BACK, NEXT, and FINISH.

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

The screenshot shows the 'New Edge Services Gateway' configuration wizard at step 7, 'Review'. The left sidebar lists the steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration, 4 Interface, 5 Default Gateway, 6 Firewall Default Policy, and 7 Review (highlighted). The main area shows the following details:

- Details**
  - Name: Topo3-ESG
  - Tenant: --
  - Size: Compact
  - HA: Disabled
  - Automatic rule generation: Enabled
- Edge Appliance VMs**

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB
- Interfaces**

vNIC#	Name	Type	ID Address	Connected To
-------	------	------	------------	--------------

At the bottom, there are four buttons: CANCEL, BACK, and FINISH (highlighted in green).

**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 configuration page for Topo3-ESG, specifically the NAT tab. A single DNAT rule is visible with the following details:

Status	Order	RuleID	Rule Type	Action	Applied On	Original	Translated	Logging
<input checked="" type="checkbox"/>	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 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 configuration page for Topo3-ESG, specifically the Firewall tab. The Firewall Status is 'Started'. Three firewall rules are listed:

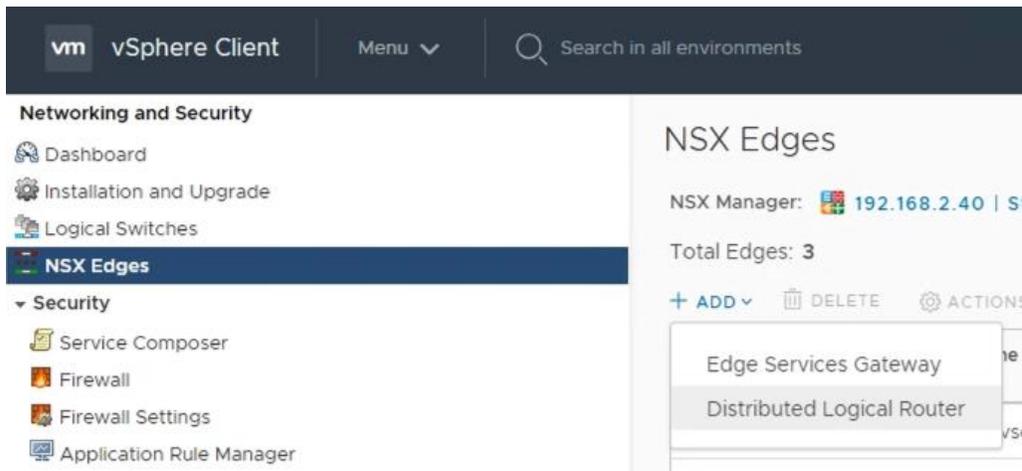
No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	WebApp	User	any	10.105.176.2	HTTPS	Accept
3	Default Rule	Default	any	any	any	Deny

## 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.

### New Distributed Logical Router

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

#### Basic Details

Distributed logical router provides Distributed Routing and Bridging capabilities.

Name

Host Name

Tenant

Description

**Select Deployment Options**

Deploy Control VMs  
Deploys Edge Appliance VM to support Firewall and Dynamic routing.

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

HA Logging Disabled

Log Level

CANCEL NEXT 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.

### New Distributed Logical Router

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

#### Settings

CLI credentials will be set on the Edge Appliance VM(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name \*

Password \*

Confirm Password \*

SSH access Enabled

FIPS Mode Disabled

Edge control level logging

CANCEL BACK NEXT 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.

New Distributed Logical Router

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

### Deployment Configuration

Datacenter \* vCloud-VDC

Control VM(s) \*

Management/ HA Interface

This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To \*

IP Address E.g. 10.121.30.4/24

CANCEL BACK NEXT FINISH

- 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.

### Add Edge Appliance VM

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

CPU 1000 MHz

Memory 512 MB

CANCEL ADD

**INTEGRATION GUIDE**

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

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

The screenshot shows the 'New Distributed Logical Router' configuration wizard. The left sidebar lists steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration (selected), 4 Interface, 5 Default Gateway, and 6 Review. The main area is titled 'Deployment Configuration' and includes a close button (X) in the top right. It shows 'Datacenter' set to 'vCloud-VDC' and 'Control VM(s)' with a gear icon. A table lists VM specifications: Cluster/Resource Pool (Cluster1-VDC), Host (--), Datastore (QNAP-AllFlash), Folder (--), CPU (1000 MHz), and Memory (512 MB). To the right is a box with a plus sign and the text 'Add Edge Appliance VM'. Below this is the 'Management/ HA Interface' section, which includes a description: 'This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.' It has a 'Connected To' field with an edit icon (pencil) and a delete icon (trash), and an 'IP Address' field with the example 'E.g. 10.121.30.4/24'. At the bottom right are buttons for 'CANCEL', 'BACK', 'NEXT', and 'FINISH'.

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

The screenshot shows the 'Select Network' dialog box with a 'Back' button and a close button (X) in the top right. It has two tabs: 'Logical Switch' and 'Distributed Virtual Port Group' (selected). A search bar is located in the top right. Below is a table with two columns: 'Name' and 'Type'. The table lists several Distributed Virtual Port Groups, with 'DVS-VLAN-102' selected. At the bottom right are 'CANCEL' and 'OK' buttons.

Name	Type
<input type="radio"/> ESX-Management-Tagged	Distributed Virtual Port Group
<input type="radio"/> ESX-Storage	Distributed Virtual Port Group
<input type="radio"/> DVS-VLAN-080	Distributed Virtual Port Group
<input checked="" type="radio"/> DVS-VLAN-102	Distributed Virtual Port Group
<input type="radio"/> ESX-Trunk-Prom	Distributed Virtual Port Group
<input type="radio"/> ESX-NSX	Distributed Virtual Port Group
<input type="radio"/> DVS-VLAN-176	Distributed Virtual Port Group
<input type="radio"/> ESX-Management-Untagged	Distributed Virtual Port Group
<input type="radio"/> ESX-Trunk	Distributed Virtual Port Group
<input type="radio"/> ESX-vSAN	Distributed Virtual Port Group

**INTEGRATION GUIDE**

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

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

**New Distributed Logical Router**

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

**Deployment Configuration**

Datacenter \* vCloud-VDC

Control VM(s) \*

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB

**Management/ HA Interface**

This is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Connected To \* DVS-VLAN-102

IP Address 192.168.14.128/24

CANCEL BACK NEXT FINISH

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

**New Distributed Logical Router**

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

**Configure Interfaces**

Configure interfaces of this distributed logical router.

+ ADD EDIT DELETE

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

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

< Back Configure Interfaces

Name

Type  Internal  Uplink

Connected To

Connectivity Status  Connected

Configure Subnets

+ ADD DELETE

Primary IP Address	Subnet Prefix Length
--------------------	----------------------

0 items

MTU

CANCEL OK

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

< Back Select Network

Logical Switch Distributed Virtual Port Group

Search

Name	Type
<input type="radio"/> AppTier	Logical Switch
<input type="radio"/> dvs.VCDVSBDD-VCD-Internal-e2239cd6-3dd6-4ed2-a024-98c4c80e55d8	Logical Switch
<input checked="" type="radio"/> TransitNet-1	Logical Switch
<input type="radio"/> DBTier	Logical Switch
<input type="radio"/> WebTier	Logical Switch

1 - 5 of 5 items

CANCEL 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.

The screenshot shows the 'Configure Interfaces' dialog box for an interface named 'TransitNet-1'. The interface type is 'Uplink' and it is connected to 'TransitNet-1'. The connectivity status is 'Connected'. The 'Configure Subnets' section is currently empty, with a table header showing 'Primary IP Address' and 'Subnet Prefix Length'. Below the table, the MTU is set to 1500. There are '+ ADD' and 'DELETE' buttons, a search bar, and 'CANCEL' and 'OK' buttons at the bottom.

Primary IP Address	Subnet Prefix Length
--------------------	----------------------

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

The screenshot shows the 'Configure Interfaces' dialog box for an interface named 'TransitNet-1'. The interface type is 'Uplink' and it is connected to 'TransitNet-1'. The connectivity status is 'Connected'. The 'Configure Subnets' section now contains one subnet entry in the table: '172.16.1.2' with a 'Subnet Prefix Length' of '24'. Below the table, the MTU is set to 1500. There are '+ ADD' and 'DELETE' buttons, a search bar, and 'CANCEL' and 'OK' buttons at the bottom.

Primary IP Address	Subnet Prefix Length
172.16.1.2	24

## 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

- 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.

New Distributed Logical Router

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

### Default Gateway

Configure Default Gateway Enabled

vNIC \* TransitNet-1

Gateway IP \* 172.16.1.1

Admin Distance 1

CANCEL BACK NEXT FINISH

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

New Distributed Logical Router

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

### Review

Details

Name Topo3-DLR

Tenant --

HA Disabled

Management/ HA Interface

Connected To DVS-VLAN-102

IP Address --

Control VMs

Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AiiFlash
Folder	--
CPU	1000 MHz
Memory	512 MB

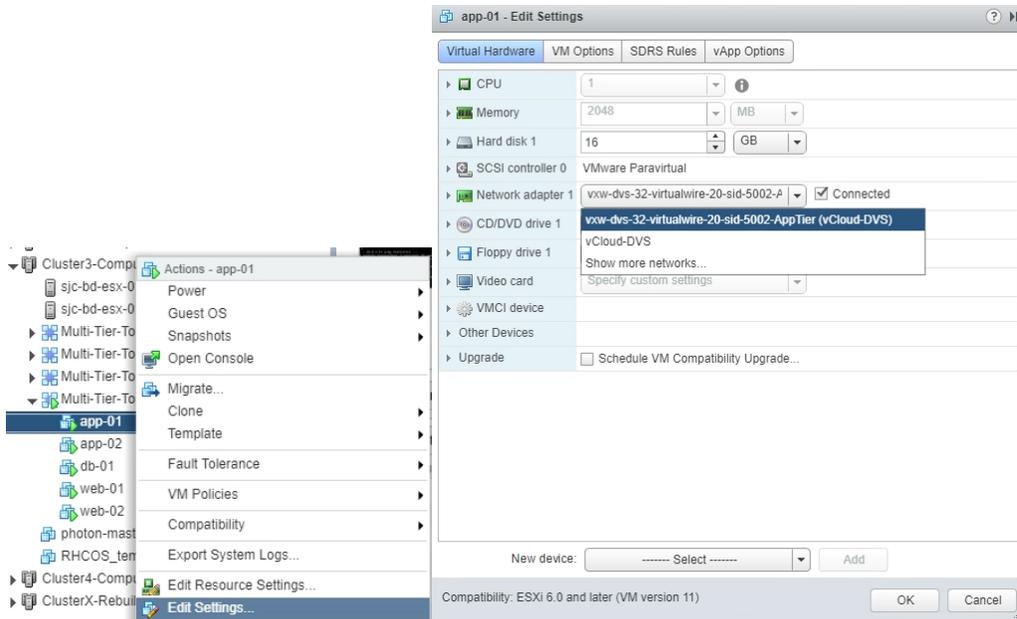
Interfaces

CANCEL BACK FINISH

## 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.



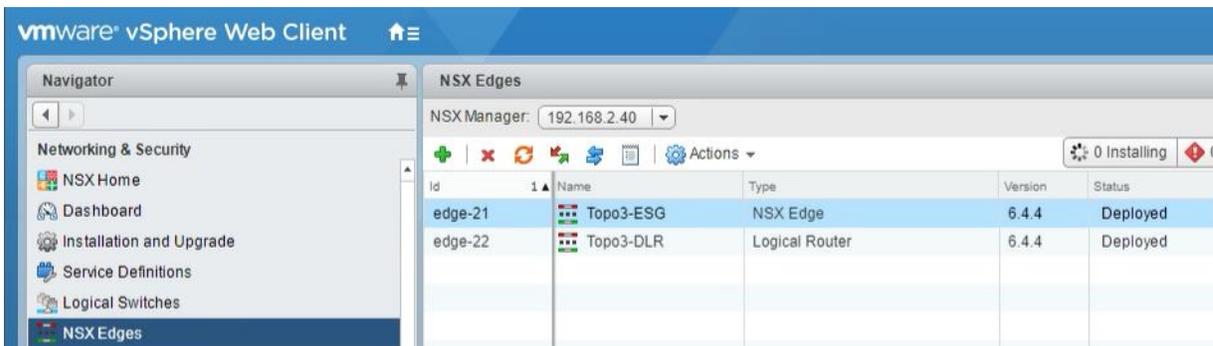
## NSX Edge Static Routing Configuration

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.

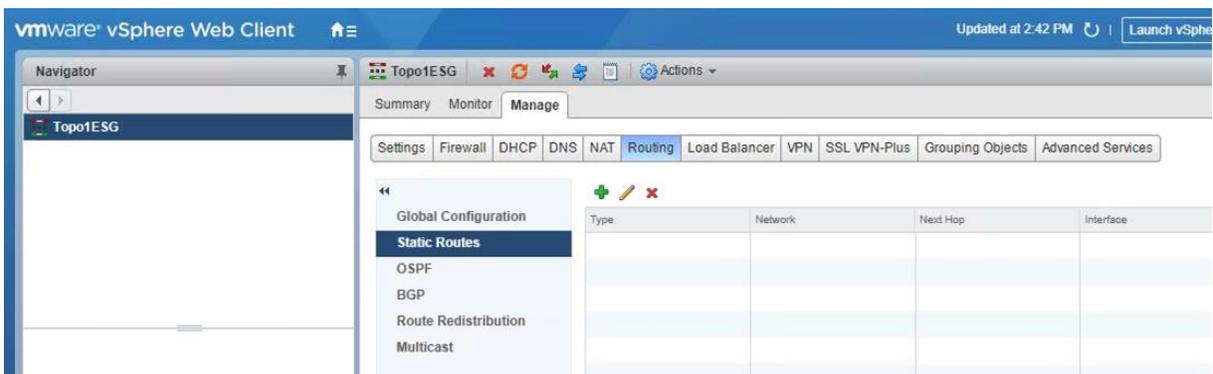
This configuration is also required to ensure that traffic coming from the external networks finds its way in.

- 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.



- 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.



## 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.

**Add Static Route** ?

Network: \* 10.0.0.0/16  
*Network should be entered in CIDR format  
e.g. 192.169.1.0/24*

Next Hop: \* 172.16.1.2

Interface: TransitNet-1 ⓘ

Admin Distance: 1

Description: I

OK Cancel

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

Topo3-ESG [Icons] Actions

Summary Monitor **Manage**

Settings Firewall DHCP DNS NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects Advanced Services

Global Configuration  
**Static Routes**  
OSPF  
BGP  
Route Redistribution  
Multicast

Changes to the Static Routing configuration will take effect only after being published. Please click on "Publish Changes" to publish.

Publish Changes Revert Changes

Type	Network	Next Hop	Interface	Admin Distance
	10.0.0.0/16	172.16.1.2	TransitNet-1	1

## 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.

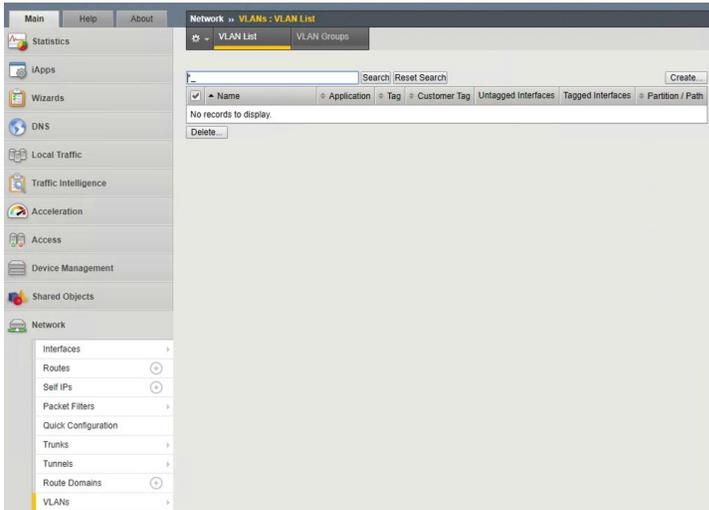
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

## INTEGRATION GUIDE

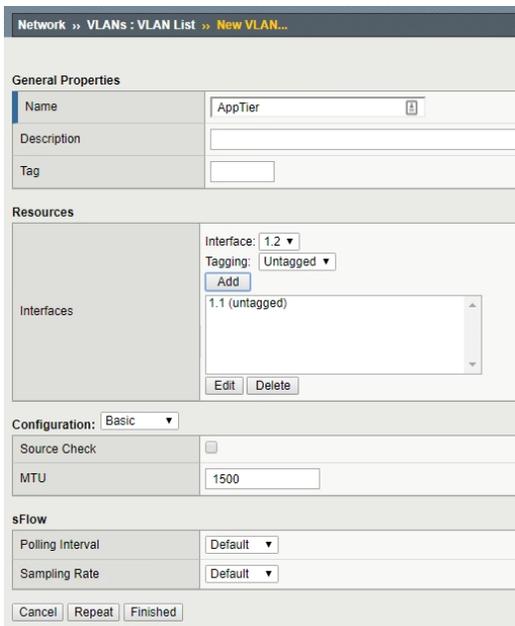
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

### 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



## INTEGRATION GUIDE

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

6. In the New VLAN Menu
  - 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.

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

**General Properties**

Name	WebTier
Description	
Tag	

**Resources**

Interface: 1.3  
Tagging: Untagged

Add

Interfaces

- 1.2 (untagged)

Edit Delete

**Configuration:** Basic

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

**sFlow**

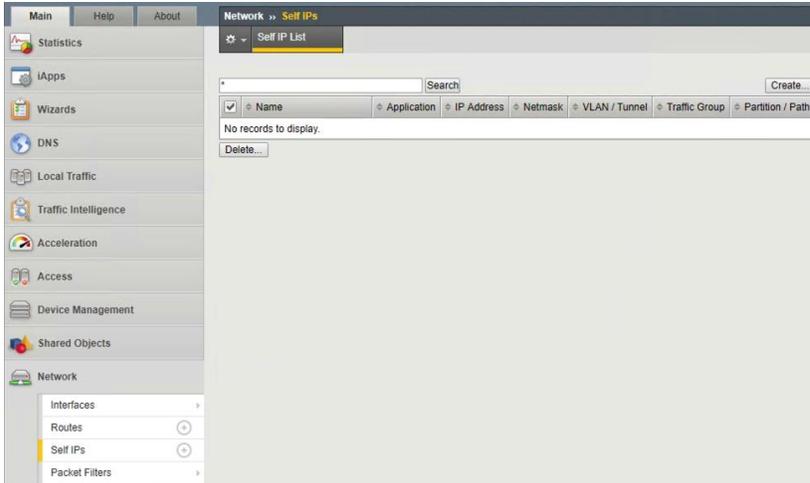
Polling Interval	Default
Sampling Rate	Default

Cancel Repeat Finished

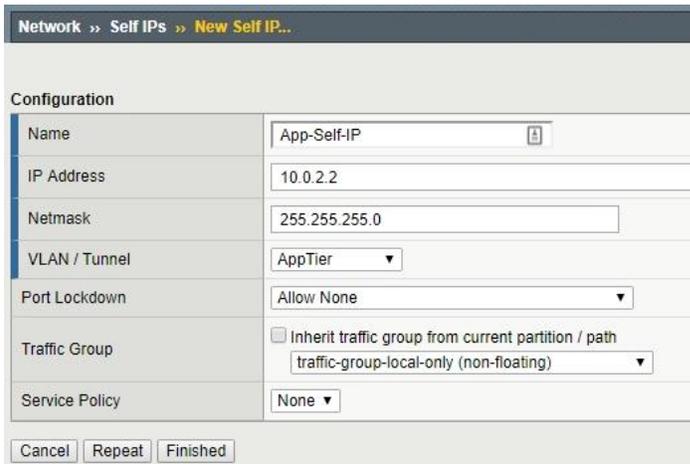
## Configure Self IP Addresses

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



## 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.

The screenshot shows the 'New Self IP' configuration form. The breadcrumb path is 'Network >> Self IPs >> New Self IP...'. The form fields are as follows:

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

Buttons: Cancel, Repeat, Finished

The screenshot shows the 'Self IP List' table. The breadcrumb path is 'Network >> Self IPs'. The table contains the following data:

	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

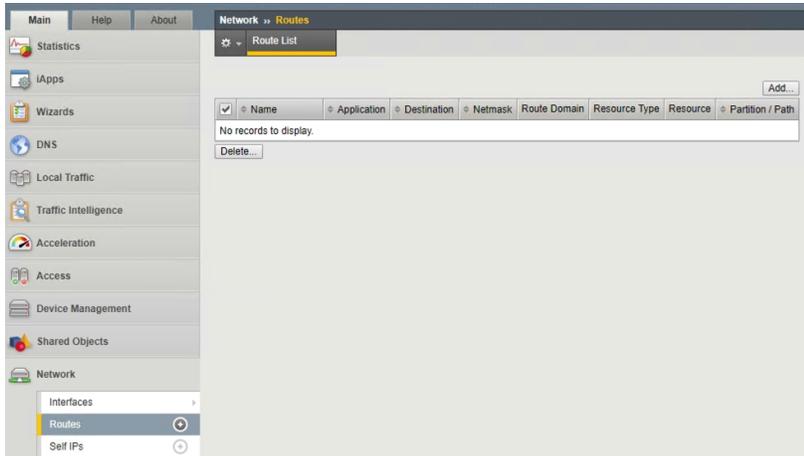
Buttons: Search, Create..., Delete...

## Configure Static Routes

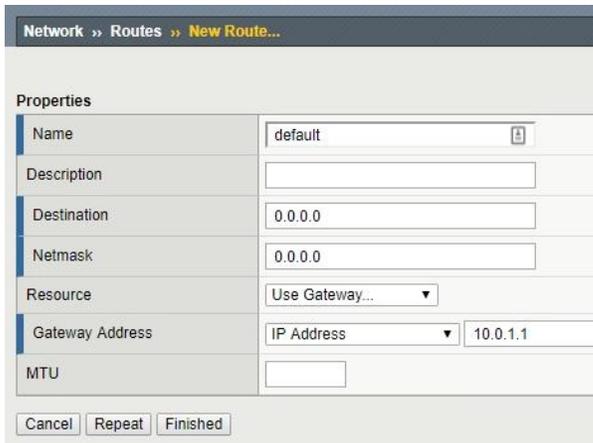
To ensure the BIG-IP can properly forward requests to the application servers within the overlay network.

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 Add button.



2. In the New Route menu
  - 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

A screenshot of the 'New Route...' dialog box in the BIG-IP Configuration Utility. The dialog has a title bar that reads 'Network >> Routes >> New Route...'. Below the title bar is a 'Properties' section with several fields: 'Name' (text box with 'default'), 'Description' (empty text box), 'Destination' (text box with '0.0.0.0'), 'Netmask' (text box with '0.0.0.0'), 'Resource' (dropdown menu with 'Use Gateway...'), 'Gateway Address' (dropdown menu with 'IP Address' and a text box with '10.0.1.1'), and 'MTU' (empty text box). At the bottom of the dialog 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: (Optional)</p> <p>Address: 10.0.1.12</p> <p>Service Port: 443 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												

Cancel Repeat Finished

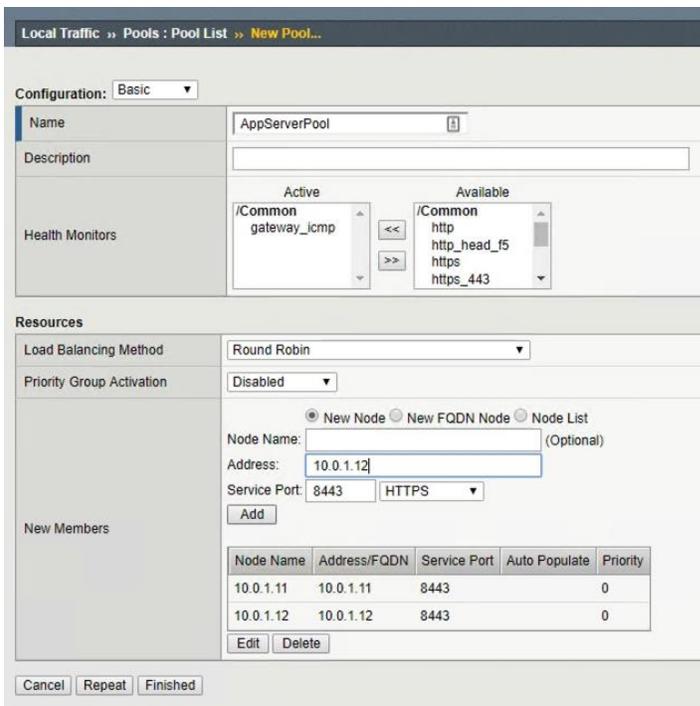
**INTEGRATION GUIDE**

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

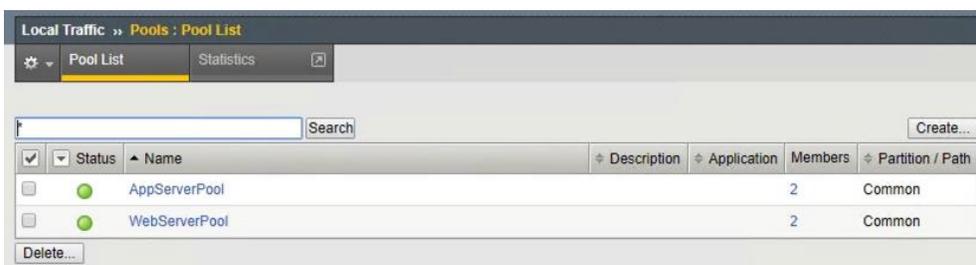
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
  - a. In the Name field, type a unique name for the app pool. For this validation AppServerPool was used.
  - b. In the Health Monitors section select an appropriate monitor for your application. 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



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

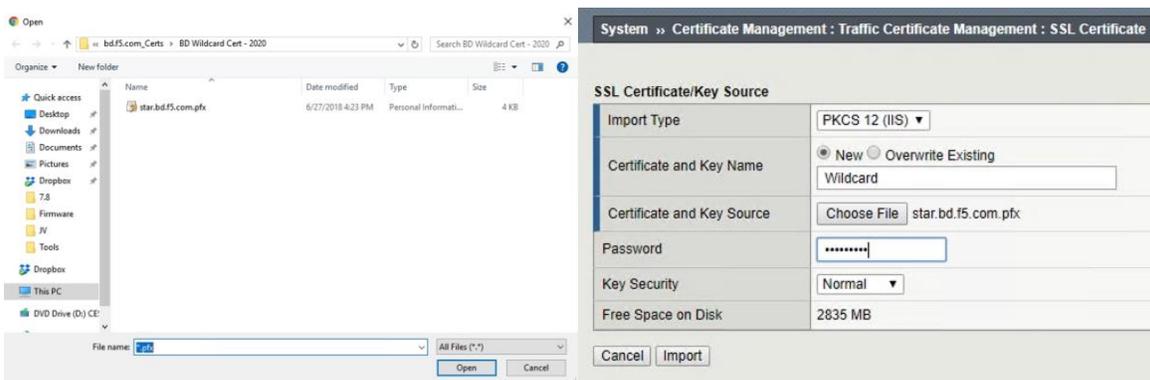


## Import SSL Certificate

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

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

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



The image shows the 'SSL Certificate List' interface with a table of certificates. The table has columns for Status, Name, Contents, Key Security, Common Name, Organization, Expiration, and Partition. Below the table are buttons for 'Archive...', 'View Certificate Order Status...', 'Delete OCSP Cache...', and 'Delete...'.

Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition
<input checked="" type="checkbox"/>	Wildcard	RSA Certificate & Key	Normal	*.bd.f5.com	F5 Networks Inc	Jun 27, 2020	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle				Jan 18, 2020 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	Mar 29, 2029	Common
<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust	Dec 7, 2030	Common
<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 18, 2027	Common

## 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.

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

General Properties

Name: WildcardSSL

Parent Profile: clientssl

Configuration: Basic

Certificate Key Chain: [Empty list]

Custom:

Buttons: Add, Edit, Delete

Add SSL Certificate Key Chain

Certificate: Wildcard

Key: Wildcard

Chain: Wildcard

Passphrase: [Empty text box]

Buttons: Add, Cancel

Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

General Properties

Name: WildcardSSL

Parent Profile: clientssl

Configuration: Basic

Certificate Key Chain: /Common/Wildcard /Common/Wildcard /Common/Wildcard

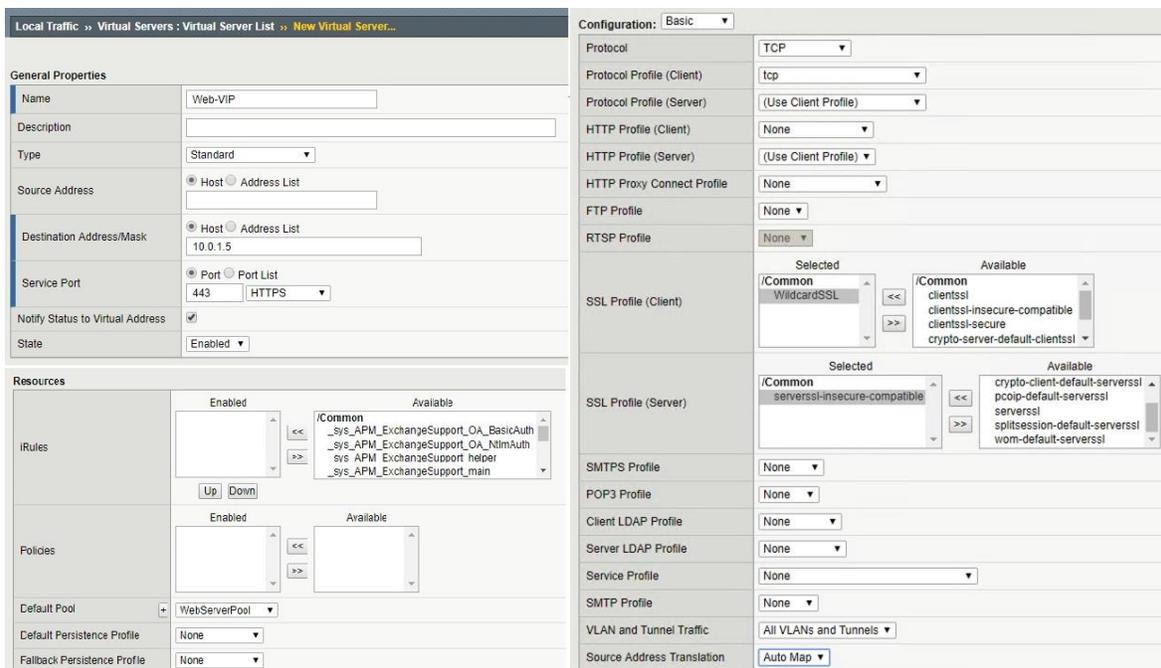
OCSP Stapling:

Buttons: Add, Edit, Delete

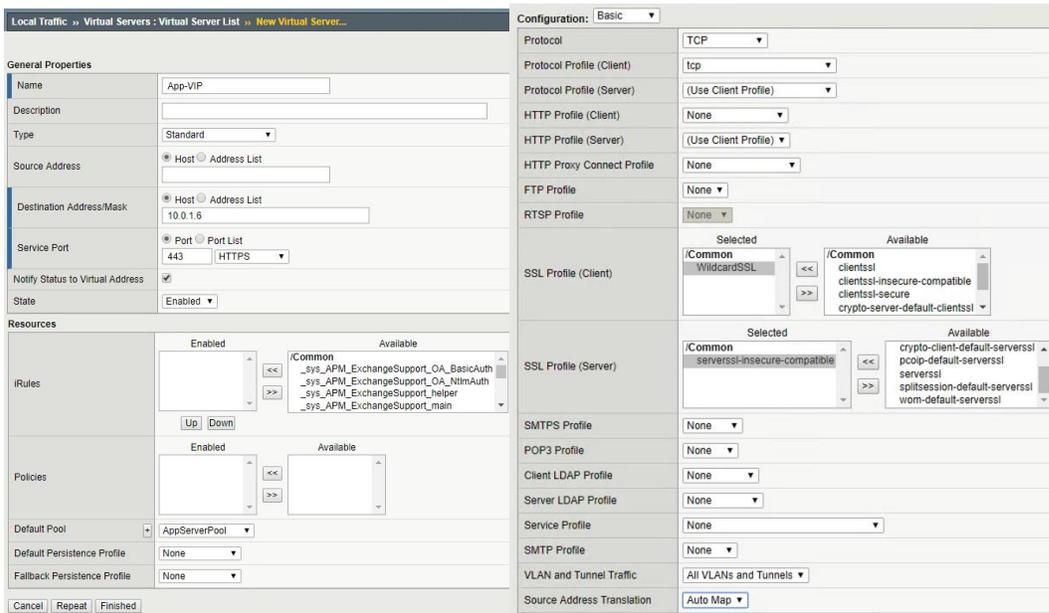
## Create Application Virtual Servers

In creating a virtual server, you specify a destination IP address and service port on which the BIG-IP appliance is listening for application traffic to be load balanced to the appropriate application pool members. In this validation, we have two virtual servers (VIPs) to create: one for the web tier, which will be available in the WebTier network on the 10.0.1.0/24 segment and accessed via NAT from 10.105.176.2, and the other for the AppTier on the same WebTier Network only accessible for the WebTier Network (10.0.1.0/24).

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



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



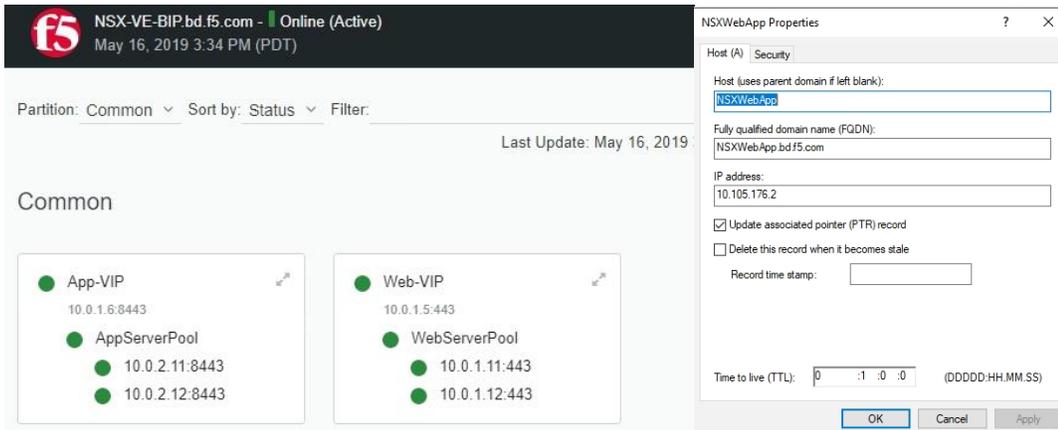
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are go with the validation application. The virtual servers and the associated pools are reachable and healthy.

Local Traffic >> Virtual Servers : Virtual Server List							
Virtual Server List							
Status	Name	Description	Application	Destination	Service Port	Type	Resources
	App-VIP			10.0.1.6	8443	Standard	Common
	Web-VIP			10.0.1.5	443 (HTTPS)	Standard	Common

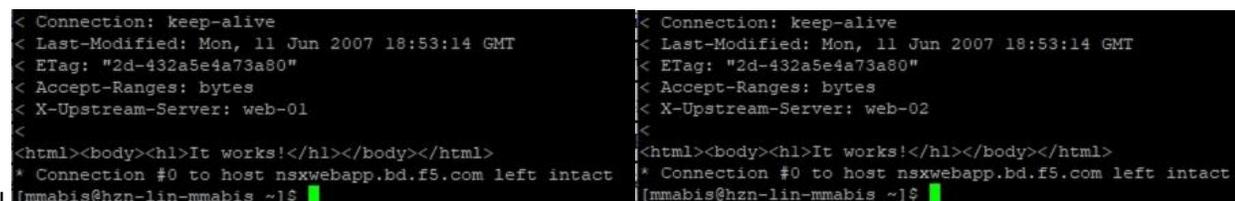
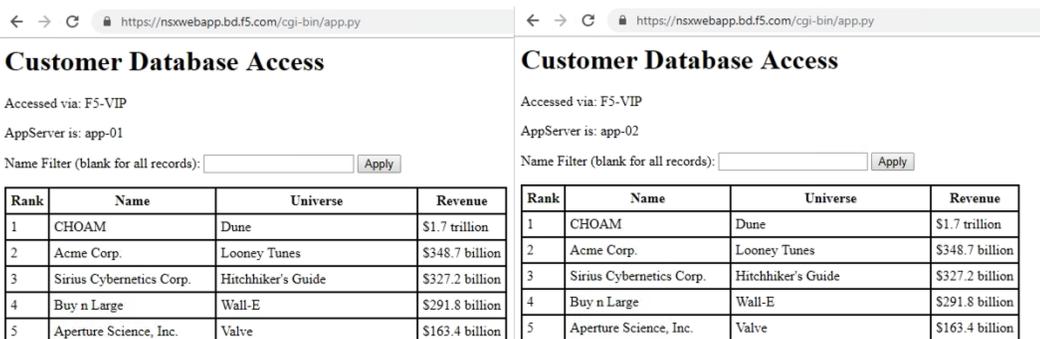
## Validation

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

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



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



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

# Topology 4: OVSDB Integration with NSX-V

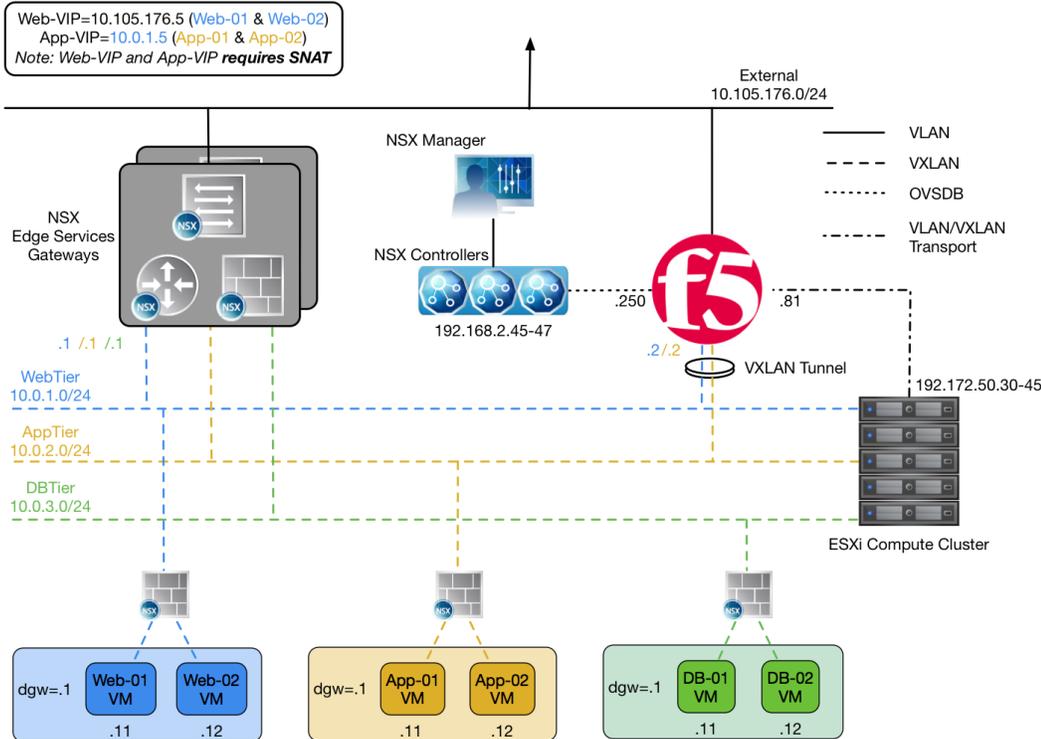


Figure 14 OVSDB Integration with NSX-V

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

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

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

## INTEGRATION GUIDE

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

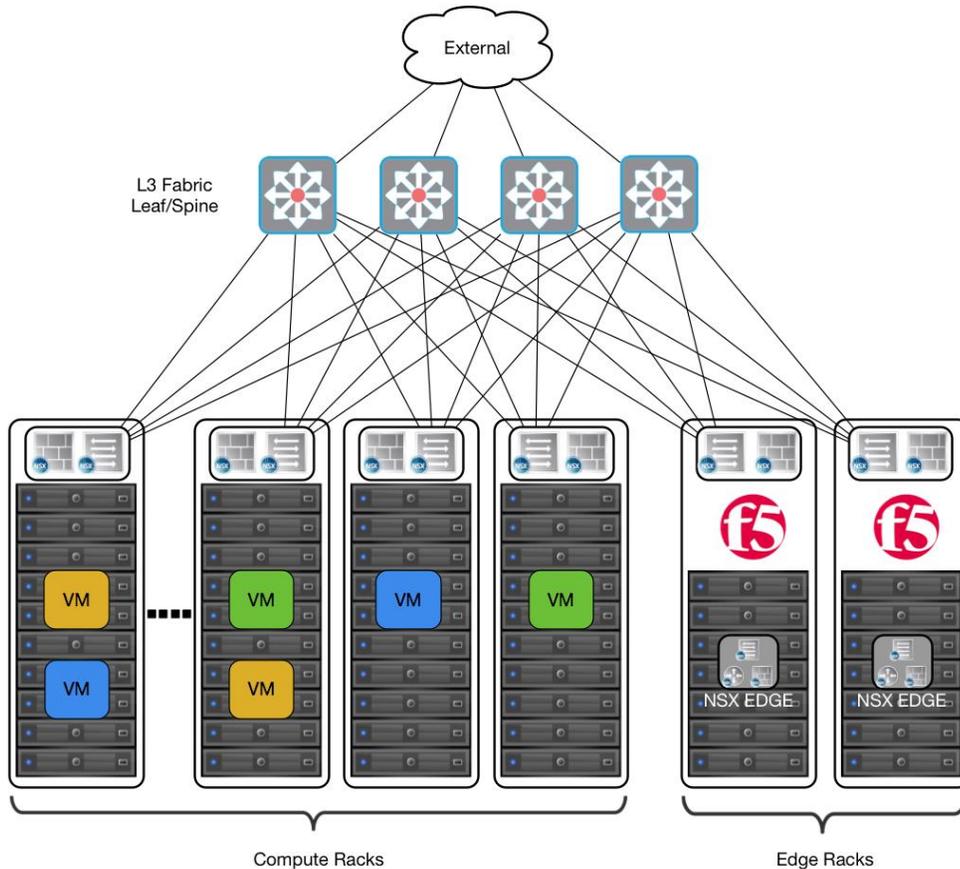


Figure 15 Leaf/spine physical rack infrastructure

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.**



## Implementation Infrastructure

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

For the purposes of explaining and building the validation infrastructure, we will be using two of the clusters listed in Figure 17: the Cluster1-VDC (Edge Rack) and Cluster3-Compute-NSX (Compute Rack). While this is a smaller representation of a typical data center deployment, the hardware is segregated in a manner consistent with that shown in Figure 15.

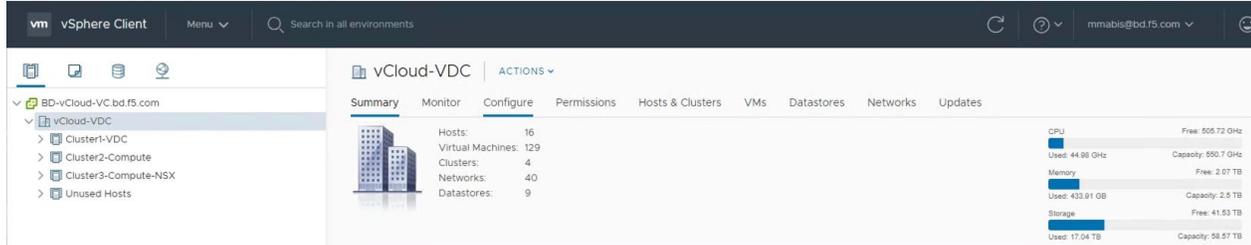


Figure 17 vSphere Console

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

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

## Prerequisites

Referencing the diagram in Figure 14, the BIG-IP requires connectivity to at minimum two of its interfaces. One interface is used for management of the device and the other is used for all production traffic. The VLAN numbers and the IP addressing scheme can be tailored to your environment.

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

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

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

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

Table 18 Logical switch configuration

## Network Segments

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

### 802.1Q VLAN segments

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

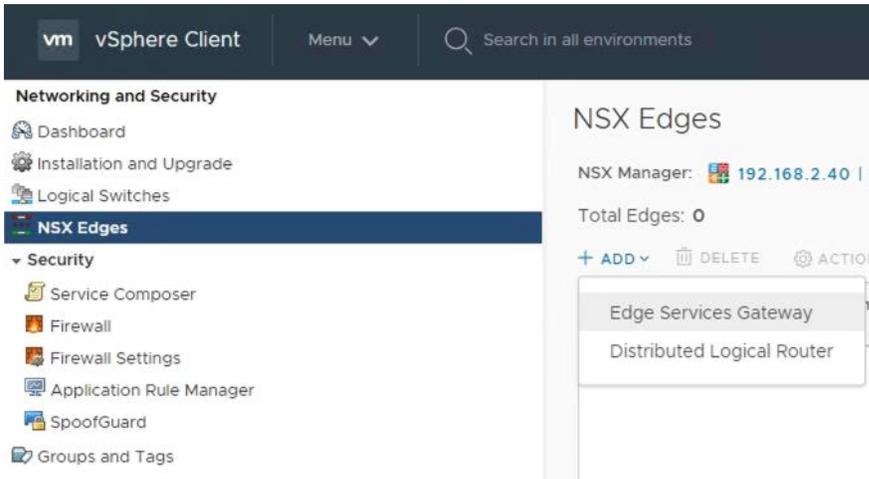
### VXLAN Segments

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

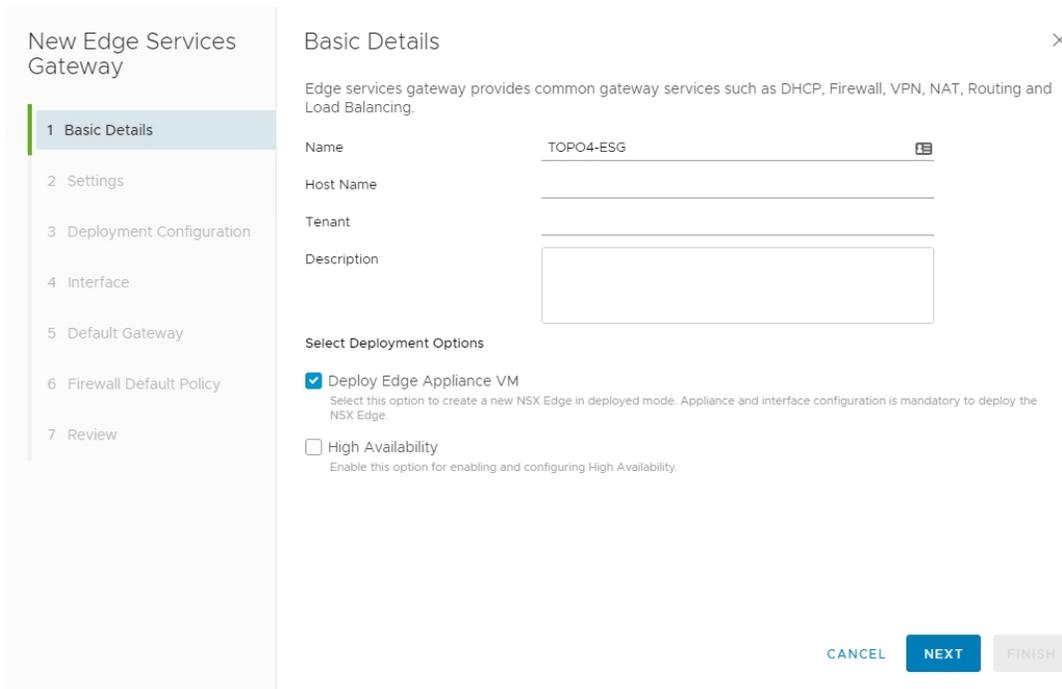
- **VXLAN 5001 WebTier** is the segment ID used for the blue web connectivity. The 10.0.1.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5002 AppTier** is the segment ID used for the yellow app connectivity. The 10.0.2.0/24 IP subnet range is configured on this VXLAN.
- **VXLAN 5003 DBTier**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

# NSX Edge Configuration

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



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



## 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 topdump capabilities, if you do not want these features leave SSH disabled.

**New Edge Services Gateway**

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

**Settings**

CLI credentials will be set on the Edge Appliance VM(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name *	admin
Password *	.....
Confirm Password *	.....
SSH access	Enabled <input checked="" type="checkbox"/>
FIPS Mode	Disabled <input type="checkbox"/>
Auto Rule Generation	Enabled <input checked="" type="checkbox"/>
Edge control level logging	Info

Enable this option to automatically generate service rules to allow flow of control traffic.

CANCEL BACK NEXT FINISH

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

**New Edge Services Gateway**

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

**Deployment Configuration**

Datacenter \* vCloud-VDC

Appliance Size \*

<input checked="" type="radio"/> Compact vCPUs 1 Memory 512 MB	<input type="radio"/> Large vCPUs 2 Memory 1 GB	<input type="radio"/> Quad Large vCPUs 4 Memory 2 GB	<input type="radio"/> X-Large vCPUs 6 Memory 8 GB
--	---	--	---

Edge Appliance VM \*

+  
Add Edge Appliance VM

No records to display

CANCEL BACK NEXT FINISH

## 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 ×

Specify placement parameters for the Edge Appliance VM.

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

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

### New Edge Services Gateway

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

### 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

## 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

Configure Interfaces

Basic | Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \*

Connectivity Status Disconnected

Configure Subnets

+ ADD DELETE Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
--------------------------	--------------------	------------------------	----------------------

0 Items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL OK

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.

Select Network

Logical Switch | Standard Port Group | Distributed Virtual Port Group

176

Name	Type
DVS-VLAN-176	Distributed Virtual Port Group

1 - 1 of 1 items

CANCEL 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

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \* DVS-VLAN-176

Connectivity Status Connected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
--------------------	------------------------	----------------------

0 items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL OK

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

Configure Interfaces

Basic Advanced

vNIC# 0

Name \* External

Type  Internal  Uplink

Connected To \* DVS-VLAN-176

Connectivity Status Connected

Configure Subnets

+ ADD DELETE Search

Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/> 10.105.176.2		24

1 items

Comma separated lists of Secondary IP Addresses. Example: 1.1.1.1,1.1.2.1,1.1.3

CANCEL 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

- 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 \* External

Gateway IP \* 10.105.176.1

Admin Distance 1

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)

The screenshot shows the 'New Edge Services Gateway' configuration wizard. On the left, a sidebar lists the steps: 1 Basic Details, 2 Settings, 3 Deployment Configuration, 4 Interface, 5 Default Gateway, 6 Firewall Default Policy (highlighted), and 7 Review. The main area is titled 'Firewall Default Policy' and contains three settings: 'Firewall Default Policy' is set to 'Enabled' with a green toggle; 'Default Traffic Policy' is set to 'Allow' with a selected radio button; and 'Logging' is set to 'Disabled' with a grey toggle. At the bottom right, there are four buttons: 'CANCEL', 'BACK', 'NEXT', and 'FINISH'.

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

The screenshot shows the 'New Edge Services Gateway' configuration wizard at the 'Review' step. The sidebar on the left highlights step 7 'Review'. The main area is titled 'Review' and contains two sections: 'Details' and 'Edge Appliance VMs'. The 'Details' section shows: Name: TOPO4-ESG, Tenant: --, Size: Compact, HA: Disabled, Automatic rule generation: Enabled. The 'Edge Appliance VMs' section shows a table with the following data:

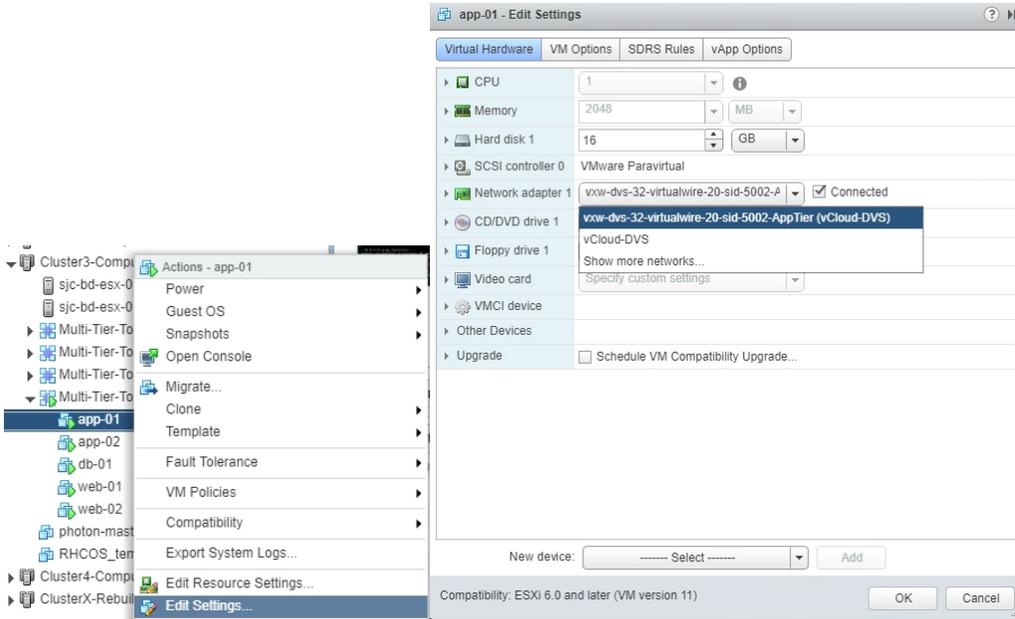
Cluster/Resource Pool	Cluster1-VDC
Host	--
Datastore	QNAP-AllFlash
Folder	--
CPU	1000 MHz
Memory	512 MB

Below the VMs section is the 'Interfaces' section, which is partially visible as a table with columns: vNIC#, Name, Type, IP Address, Connected To. At the bottom right, there are four buttons: 'CANCEL', 'BACK', 'FINISH' (highlighted in green), and 'NEXT'.

**INTEGRATION GUIDE**

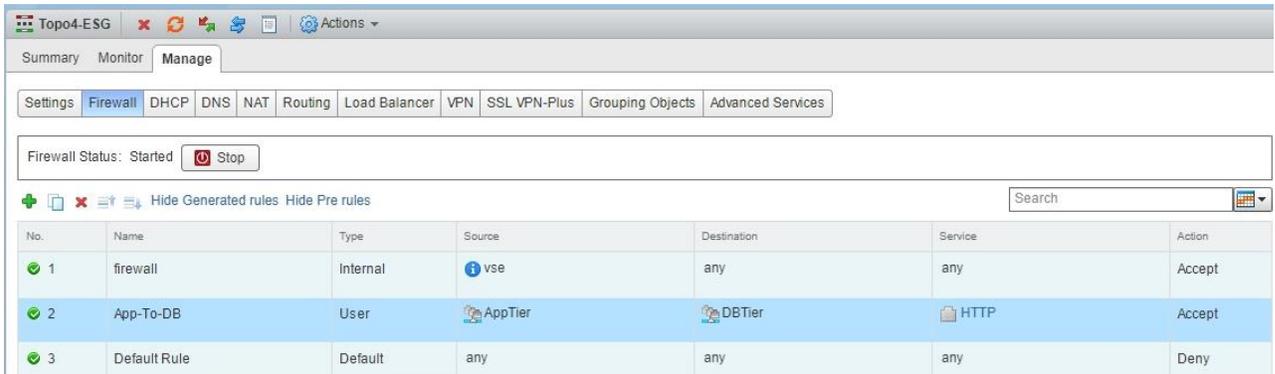
VMware NSX for vSphere (NSX-V) and F5 BIG-IP

- 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.



## BIG-IP Configuration

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

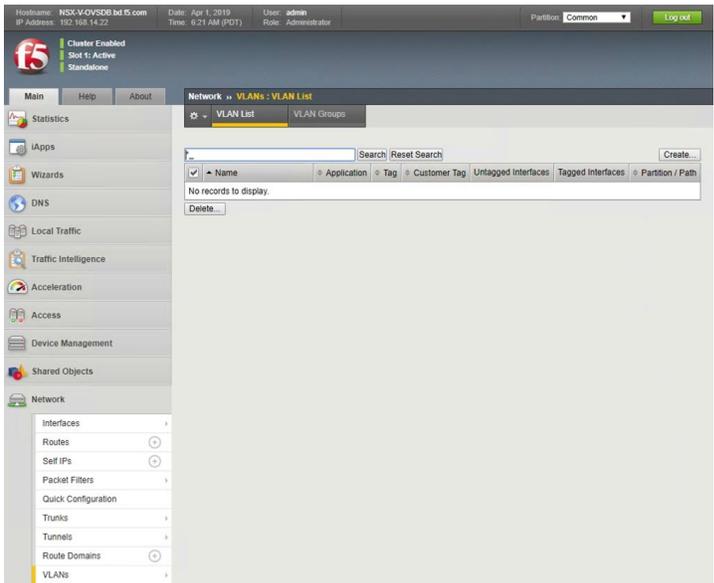
### Prerequisites

- BIG-IP Version 13.1 and above.
- The BIG-IP is configured with a management IP address in the proper subnet.
- Licenses have been applied and activated.
- Appropriate provisioning of resources is complete.
- Base configuration of services DNS, NTP, SYSLOG are configured.
- BIG-IP Interface 1.1 or an available interface that is connected is wired to a physical or virtual switch (trunk) configured to support 802.1Q tagging of traffic. In our specific use case this is VLANs 50, 102 and 176.

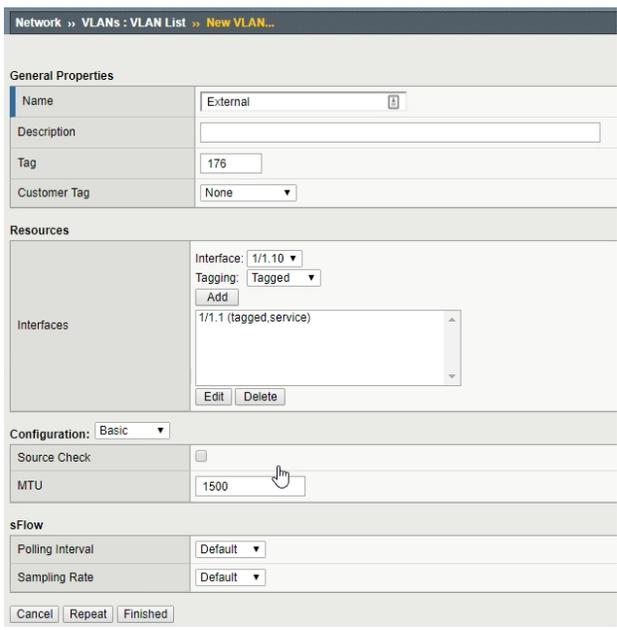
For info on how to perform these installation and basic setup steps, refer to <http://support.f5.com> and consult the appropriate implementation guide for your version and device.

## Create VLANs

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



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



## INTEGRATION GUIDE

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

4. In the New VLAN Menu
  - 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

Cancel Repeat Finished

## INTEGRATION GUIDE

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

3. In the New VLAN Menu
  - 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**

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

Configuration: Basic

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

**sFlow**

Polling Interval	Default
Sampling Rate	Default

Cancel Repeat Finished

Network » VLANs : VLAN List

VLAN List VLAN Groups

\* Search Create...

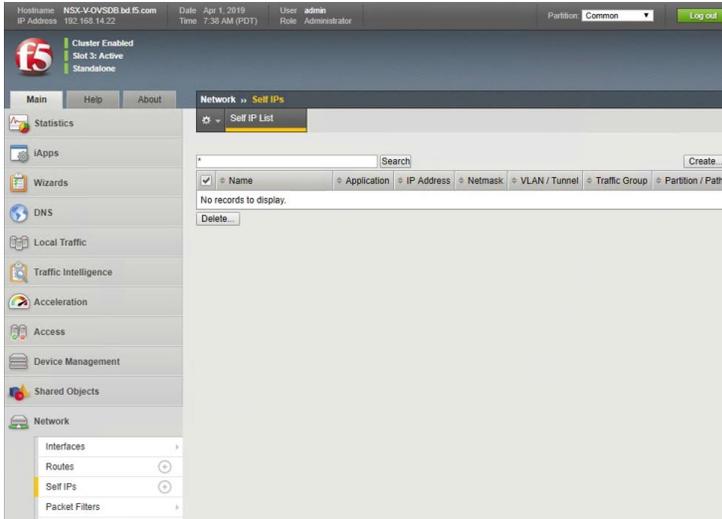
<input checked="" type="checkbox"/>	Name	Application	Tag	Customer Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	External		176			1/1.1	Common
<input type="checkbox"/>	NSX-CTRL		102			1/1.1	Common
<input type="checkbox"/>	VTEP		50			1/1.1	Common

Delete...

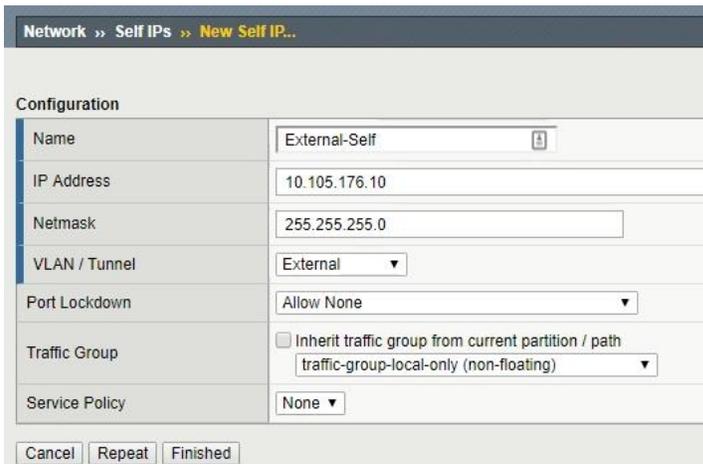
## Configure Self IP Addresses

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 Menu
  - 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



## INTEGRATION GUIDE

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

### 4. In New Self IP Menus

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

The screenshot shows the 'New Self IP' configuration window. The breadcrumb path is 'Network >> Self IPs >> New Self IP...'. The configuration table is as follows:

Configuration	
Name	NSX-CTRL-Self
IP Address	192.168.2.250
Netmask	255.255.0.0
VLAN / Tunnel	NSX-CTRL
Port Lockdown	Allow Default
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Buttons: Cancel, Repeat, Finished

### 5. In New Self IP Menus

- Type a unique name in the Name box. In this example, we used "VTEP-Self" (without double quotes).
- In the IP address box, provide the IP address for the External network, in our example, we used 192.172.50.81
- 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 Finished Button to complete the configuration

The screenshot shows the 'New Self IP' configuration window. The breadcrumb path is 'Network >> Self IPs >> New Self IP...'. The configuration table is as follows:

Configuration	
Name	VTEP-Self
IP Address	192.172.50.81
Netmask	255.255.255.0
VLAN / Tunnel	VTEP
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

Buttons: Cancel, Repeat, Finished

## 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

Search

Create...

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<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

Delete...

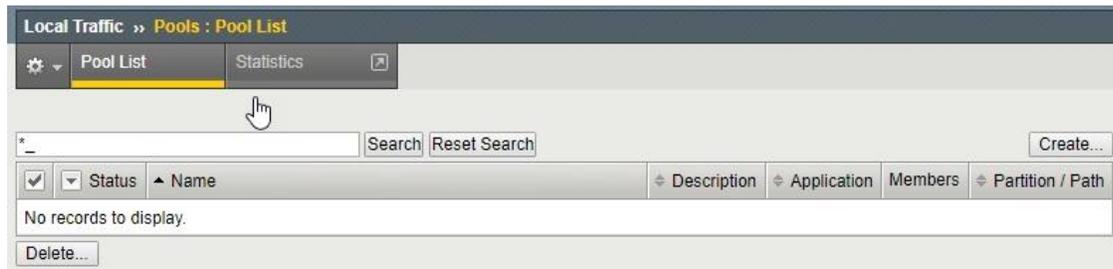
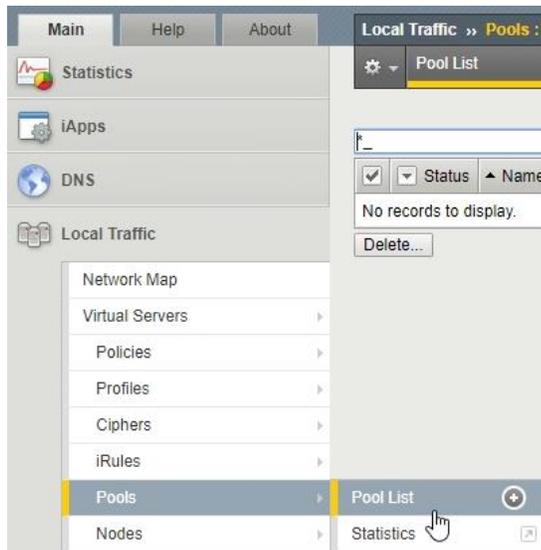
## INTEGRATION GUIDE

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

### Create Pools

Prior to creating the OVSDDB 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.

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

Configuration: Basic

Name: WebTier-Pool

Description:

Health Monitors

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

New Node  New FQDN Node  Node List

Node Name: (Optional)

Address: 10.0.1.12

Service Port: 443

Add

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

Edit Delete

Cancel Repeat Finished

## 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.

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

Configuration: Basic

Name: AppTier-Pool

Description:

Health Monitors

Active	Available
gateway_icmp	http
	http_head_f5
	https
	https_443

Resources

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members

New Node  New FQDN Node  Node List

Node Name: (Optional)

Address: 10.0.2.12

Service Port: 8443

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
10.0.2.11	10.0.2.11	8443		0
10.0.2.12	10.0.2.12	8443		0

Buttons: Cancel, Repeat, Finished

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.

Local Traffic » Pools : Pool List

Status	Name	Description	Application	Members	Partition / Path
Offline (Enabled)	AppTier-Pool			2	Common
Offline (Enabled)	WebTier-Pool			2	Common

Buttons: Delete...

## 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.



## INTEGRATION GUIDE

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

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

Network >> Route Domains >> New Route Domain...

**General Properties**

Name: RD-200  
ID: 200  
Description:

**Configuration**

Strict Isolation:  Enabled  
Parent Name: None  
VLANs: Members: Available: /Common, http-tunnel, socks-tunnel  
Dynamic Routing Protocols: Enabled: BFD Available: BGP, IS-IS, OSPFv2, OSPFv3, PIM  
Bandwidth Controller: None  
Connection Limit: 0  
Eviction Policy: None  
Buttons: Cancel, Repeat, Finished

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

Network >> Route Domains

Route Domain List

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

Delete...

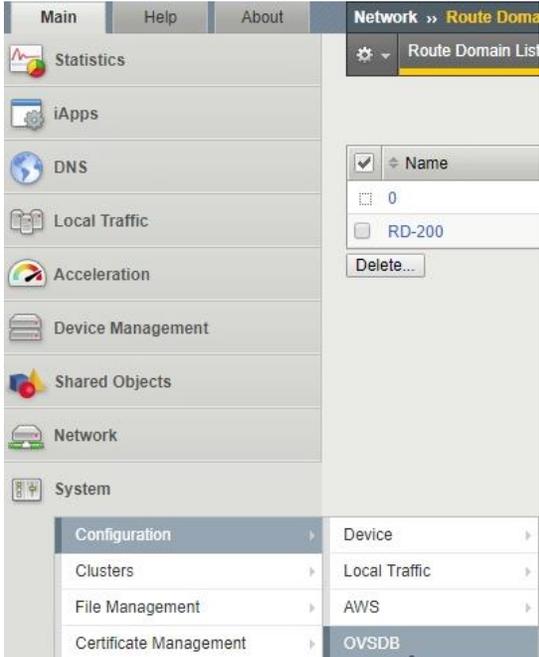
## INTEGRATION GUIDE

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

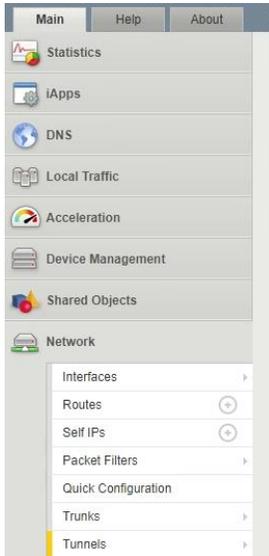
2. In the OVSDB Configuration menus
  - a. In the General Properties section
    - i. OVSDB – Select Enable
    - ii. Controller Addresses – Enter the Addresses of the NSX Controllers clicking add after entering each one. In this example we used 192.168.2.45, 192.168.2.46, 192.168.2.47
    - iii. Tunnel 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 displays the 'System >> Configuration : OVSDB' interface. The breadcrumb trail includes 'Device', 'Local Traffic', 'AWS', and 'OVSDB'. The 'General Properties' section includes: OVSDB (Enable), Controller Addresses (192.168.2.45, 192.168.2.46, 192.168.2.47), Flooding Type (Replicator), Logical Routing Type (None), Port (6640), Tunnel Local Address (192.172.50.81), Tunnel Floating Addresses (Selected and Available lists), Tunnel Maintenance Mode (Active), and Log Level (Info). The 'Credentials' section includes: Certificate File (default.crt), Certificate Key File (default.key), and CA Certificate File (None). The 'BFD Settings' section includes: BFD (Enable) and Route Domain (RD-200). An 'Update' button is located at the bottom.

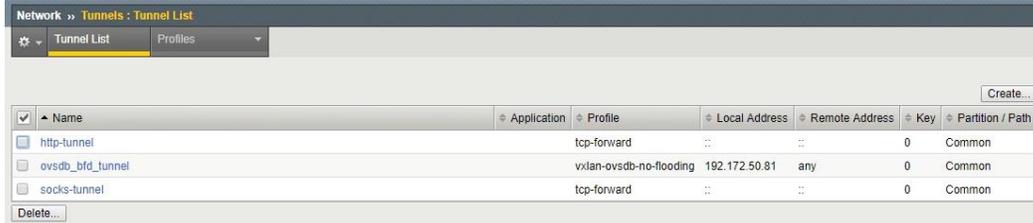
## INTEGRATION GUIDE

### 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.



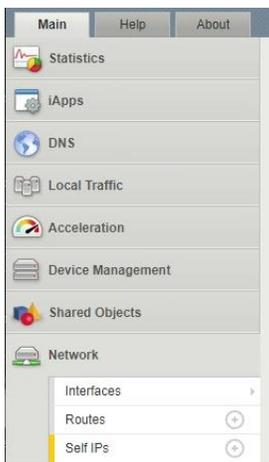
The screenshot shows the main navigation menu of the NSX management console. The 'Network' menu item is expanded, showing a list of sub-items: Interfaces, Routes, Self IPs, Packet Filters, Quick Configuration, Trunks, and Tunnels. The 'Tunnels' item is highlighted.



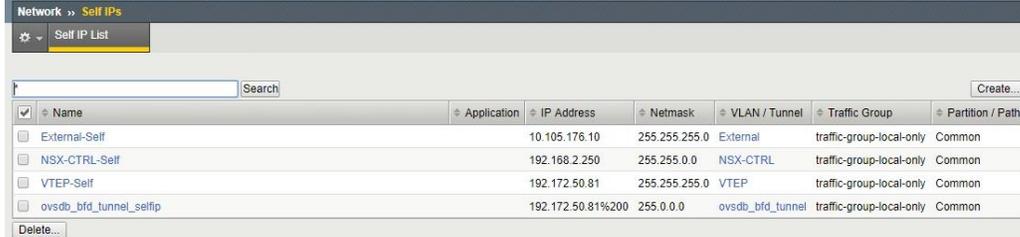
The screenshot shows the 'Network >> Tunnels : Tunnel List' page. The 'Tunnel List' tab is selected. A table displays the following data:

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

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



The screenshot shows the main navigation menu of the NSX management console. The 'Network' menu item is expanded, showing a list of sub-items: Interfaces, Routes, and Self IPs. The 'Self IPs' item is highlighted.



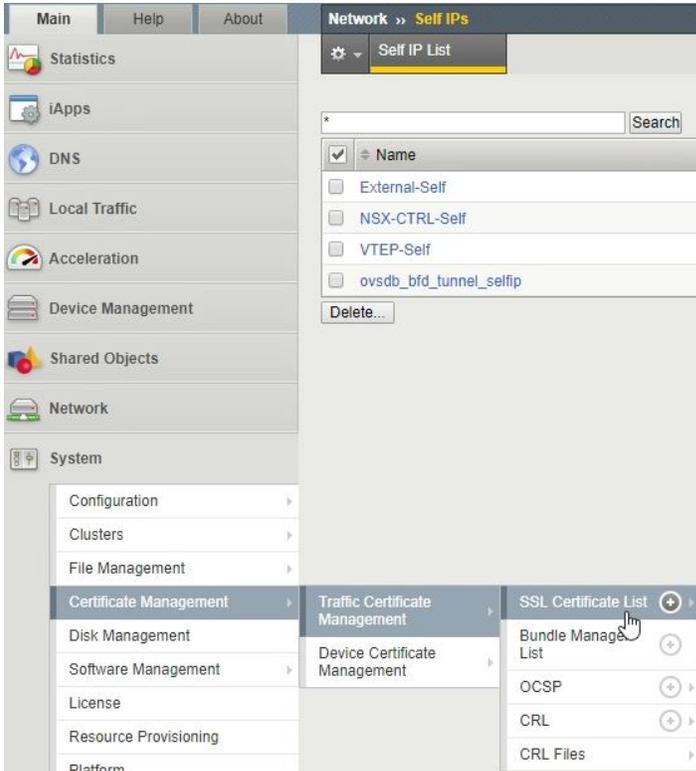
The screenshot shows the 'Network >> Self IPs' page. The 'Self IP List' tab is selected. A table displays the following data:

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

## 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.



## 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)**

The screenshot shows the VMware NSX Certificate Management console. The breadcrumb navigation is: System >> Certificate Management : Traffic Certificate Management : SSL Certificate List >> default.crt. The 'Certificate' sub-menu is selected. The console displays the following information:

General Properties	
Name	default.crt
Partition / Path	Common
Certificate Subject(s)	localhost.localdomain, MyCompany

Certificate Properties	
Public Key Type	RSA
Public Key Size	2048 bits
Expires	Jul 14 2029 05:21:54 GMT
Version	3
Serial Number	301008114
Fingerprint	SHA256/4C: [redacted]
Subject	Common Name: localhost.localdomain Organization: MyCompany Division: IT Locality: Seattle State Or Province: WA Country: US
Issuer	Self
Email	root@localhost.localdomain
Subject Alternative Name	

Buttons: Export..., Renew...

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)**

The screenshot shows the VMware NSX Certificate Management console with the 'Certificate Export' dialog box open. The 'Certificate Text' field contains the following text:

```
-----BEGIN CERTIFICATE-----
MIIDrjCCApagAwIBAgIEEfeE8jANBgkqh
VWxzCzAJBgNVBAGTAldBMRAwDgYDVQOH
-----
```

The 'Certificate File' field contains the text: Download default.crt. A 'Cancel' button is visible at the bottom left of the dialog.

The screenshot shows a Notepad application window titled 'Untitled - Notepad'. The text in the window is:

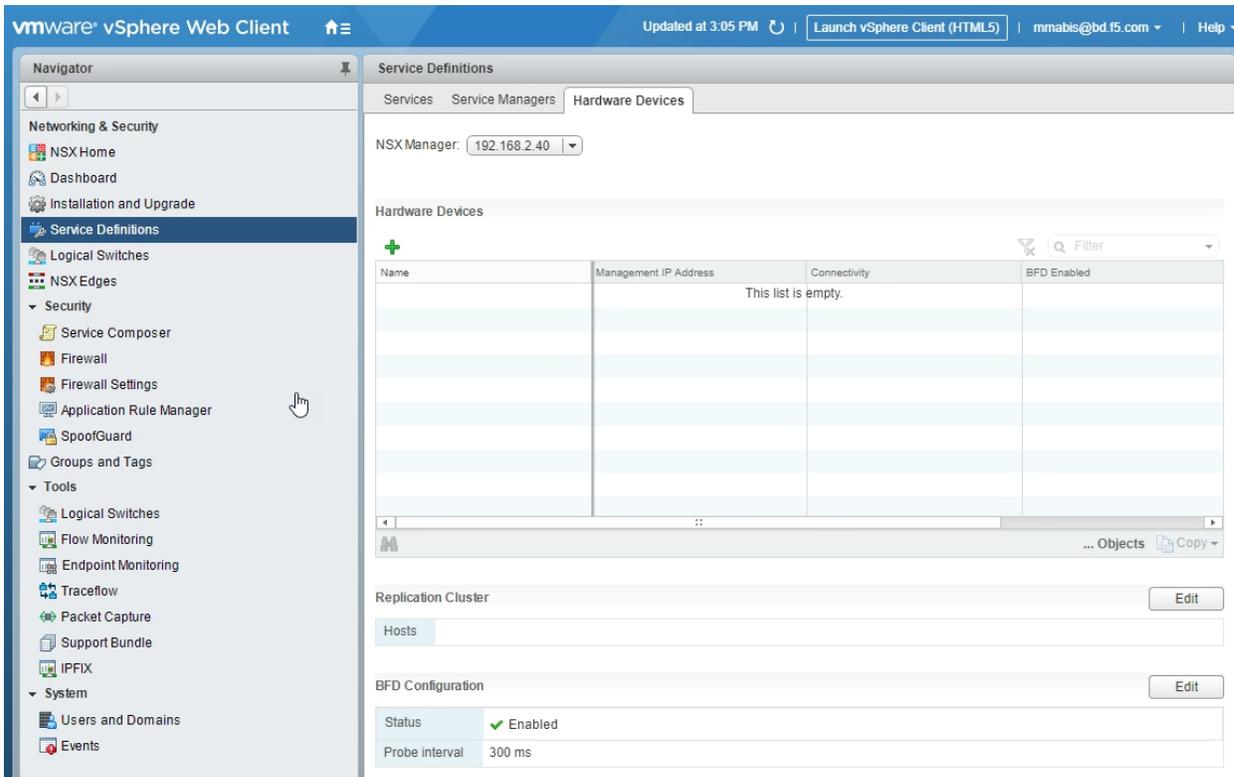
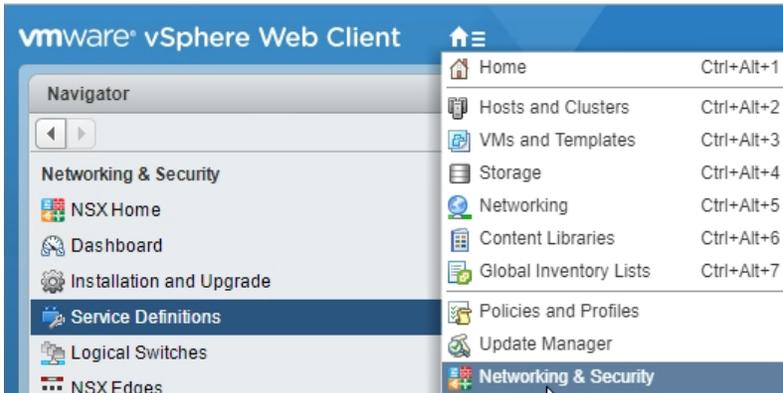
```
-----BEGIN CERTIFICATE-----
MIIDrjCCApagAwIBAgIEEfeE8jANBgkqh
VWxzCzAJBgNVBAGTAldBMRAwDgYDVQOH
-----
```

The status bar at the bottom indicates 'Windows (CRLF) Ln 23, Col 1 100%'.

## 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.



## 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.

Add Hardware Device

Name: \* nsx-bip.bd.f5.com

Description:

Certificate: \*  
z69zQLro4H9O6wAtbs FBleX6+6+fpXu8eYTsqLu  
OMPczXg==  
-----END CERTIFICATE-----

Enable BFD

OK Cancel

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.**

Service Definitions

Services Service Managers Hardware Devices

NSX Manager: 192.168.2.40

Hardware Devices

+ | ✎ ✖ | ⌂ Actions Filter

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

1 Objects Copy

## INTEGRATION GUIDE

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

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

The screenshot shows the 'Service Definitions' interface with the 'Hardware Devices' tab selected. The 'NSX Manager' dropdown is set to '192.168.2.40'. Below, the 'Hardware Devices' table lists one device: 'nsx-bip.bd.f5.com' with a Management IP Address of '192.168.2.250', Connectivity 'Up', and BFD Enabled 'checked'. An 'Edit' button is visible in the 'Replication Cluster' section below.

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

- 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 'Edit Replication Cluster Configuration' dialog box shows two lists of objects. The 'Available Objects' list contains 8 items, and the 'Selected Objects' list also contains 8 items. All items in both lists are checked. The 'OK' button is highlighted.

Available Objects	Selected Objects
✓ sjc-bd-esx-017.bd.f5.com	✓ sjc-bd-esx-108.bd.f5.com
✓ sjc-bd-esx-018.bd.f5.com	✓ sjc-bd-esx-107.bd.f5.com
✓ sjc-bd-esx-102.bd.f5.com	✓ sjc-bd-esx-106.bd.f5.com
✓ sjc-bd-esx-103.bd.f5.com	✓ sjc-bd-esx-105.bd.f5.com
✓ sjc-bd-esx-105.bd.f5.com	✓ sjc-bd-esx-103.bd.f5.com
✓ sjc-bd-esx-106.bd.f5.com	✓ sjc-bd-esx-102.bd.f5.com
✓ sjc-bd-esx-107.bd.f5.com	✓ sjc-bd-esx-018.bd.f5.com
✓ sjc-bd-esx-108.bd.f5.com	✓ sjc-bd-esx-017.bd.f5.com

- Once completed the Replication Cluster hosts will be populated.

The 'Replication Cluster' section shows the 'Hosts' tab populated with five hosts: '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', and 'sjc-bd-esx-017.bd.f5.com'. An 'Edit' button is visible in the top right corner.

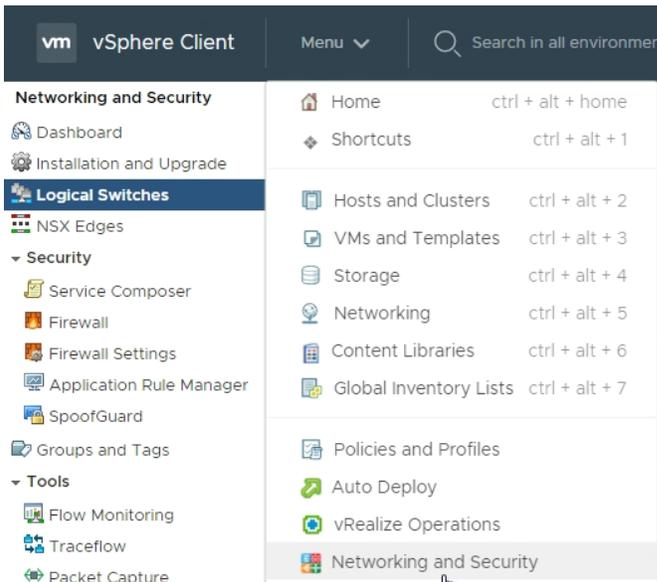
## INTEGRATION GUIDE

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 menu select Logical Switches.



#### 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	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	Status	Transport Zone	Connected VMs	Hardware Ports Binding
virtualwire-19	5001	WebTier	Normal	Transit2-Net	6	0
virtualwire-20	5002	AppTier	Normal	Transit2-Net	7	0
virtualwire-21	5003	DBTier	Normal	Transit2-Net	3	0

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 <a href="#">Select</a>	

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

Specify Hardware Port ×

Select Hardware Port for attaching it to the Logical Switch.

Selected: local0

Q Search

Name
<input checked="" type="radio"/> local0
<input type="radio"/> local1
<input type="radio"/> local2
<input type="radio"/> local3

1 - 4 of 4 objects

- 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.

Manage Hardware Bindings | WebTier ×

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

+ ADD  DELETE

Switch	Port	VLAN
nsx-bip.bd.f5.com	local0	Select 0

- 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	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 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	Connect Edge	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

Manage Hardware Bindings | AppTier

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

+ ADD DELETE

Switch	Port	VLAN
No items to display		

CANCEL OK

11. Click the Select link in the Port section

Manage Hardware Bindings | AppTier

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

Specify Hardware Port ✕

Select Hardware Port for attaching it to the Logical Switch.

Selected: local0

Q Search

Name
<input checked="" type="radio"/> local0
<input type="radio"/> local1
<input type="radio"/> local2
<input type="radio"/> local3

1 - 4 of 4 objects

- 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.

Manage Hardware Bindings | AppTier ✕

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

+ ADD DELETE

Switch	Port	VLAN
<input type="text" value="nsx-bip.bd.f5.com"/>	<input type="text" value="local0"/> Select	<input type="text" value="1"/>

- 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 ▼

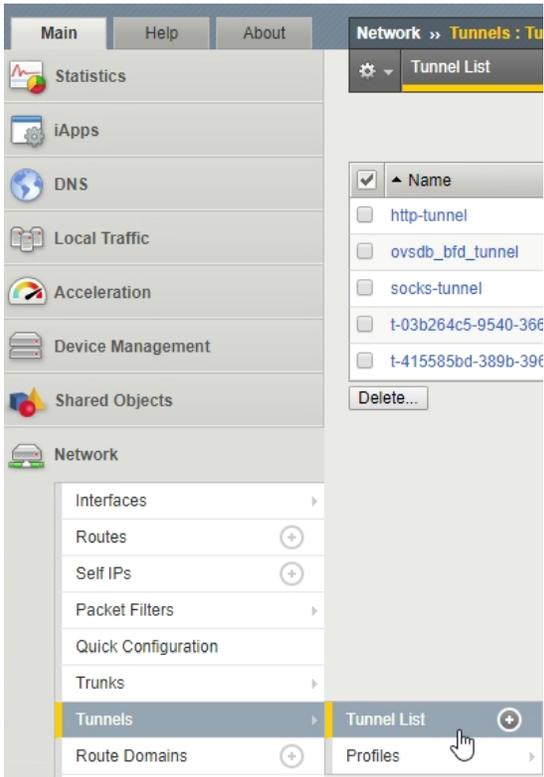
+ ADD EDIT DELETE ADD VM REMOVE VM ACTIONS ▼

Logical Switch ID	Segment ID	Name	Status	Transport Zone	Connected VMs	Hardware Ports Binding
<input checked="" type="radio"/> virtualwire-19	5001	WebTier	Normal	Transit2-Net	6	1
<input type="radio"/> virtualwire-20	5002	AppTier	Normal	Transit2-Net	7	1
<input type="radio"/> 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

<input checked="" type="checkbox"/>	Name	Application	Profile	Local Address	Remote Address	Key	Partition / Path
<input type="checkbox"/>	http-tunnel		tcp-forward	::	::	0	Common
<input type="checkbox"/>	ovsdb_bfd_tunnel		vxlan-ovsdb-no-flooding	192.172.50.81	any	0	Common
<input type="checkbox"/>	socks-tunnel		tcp-forward	::	::	0	Common
<input type="checkbox"/>	t-03b264c5-9540-3666-a34a-c75d828439bc		vxlan-ovsdb	192.172.50.81	any	5001	Common
<input type="checkbox"/>	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 'Self IPs' page in the BIG-IP Configuration Utility. The page title is 'Network >> Self IPs'. There is a search bar and a 'Create...' button in the top right corner. Below the search bar is a table with the following data:

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<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"/>	ovsdb_bfd_tunnel_selfip		192.172.50.81%200	255.0.0.0	ovsdb_bfd_tunnel	traffic-group-local-only	Common

There is a 'Delete...' button at the bottom left of the table.

## 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

- Type a unique name in the Name box. In this example, we used "AppTier-Self" (without double quotes).
- In the IP address box, provide the IP address for the External network, in our example, we used 10.0.2.10
- Provide the appropriate subnet mask in the Netmask box. In this example, we used 255.255.255.0.
- For the VLAN/Tunnel, select Tunnel (t-41558...) from the dropdown box.
- Use the default settings (Allow None) for Port Lockdown and Traffic Group.
- 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

Cancel Repeat Finished

Network » Self IPs

Self IP List

Search Create...

<input 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

Delete...

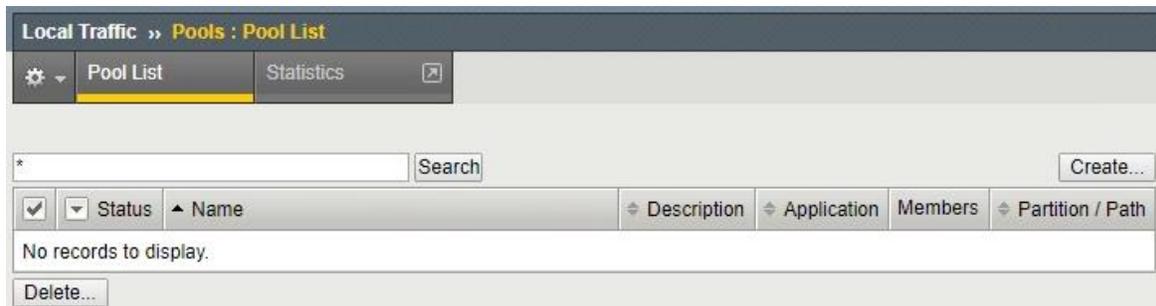
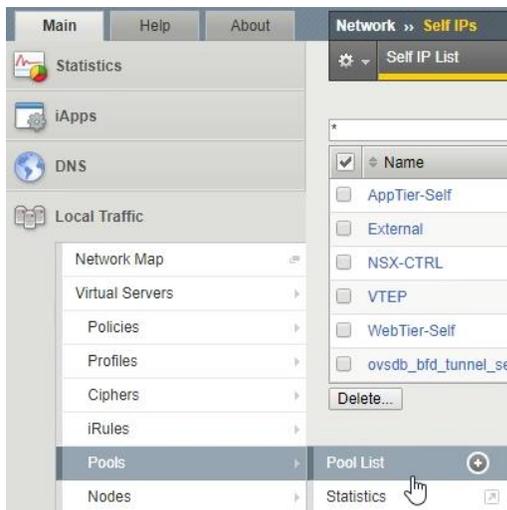
# Application Configuration

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.



## 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

The screenshot shows the 'New Pool...' configuration page in the BIG-IP interface. The breadcrumb navigation is 'Local Traffic >> Pools : Pool List >> New Pool...'. The configuration is set to 'Basic'.

**Configuration:** Basic

**Name:** WebServerPool

**Description:** (Empty field)

**Health Monitors:** Active: /Common gateway\_icmp; Available: /Common http, http\_head\_f5, https, https\_443

**Resources:** Load Balancing Method: Round Robin; Priority Group Activation: Disabled

**New Members:** New Node (selected), New FQDN Node (unselected). Node Name: (Optional); Address: 10.0.1.12; Service Port: 443; HTTPS (selected). An 'Add' button is present.

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

Buttons: Cancel, Repeat, Finished

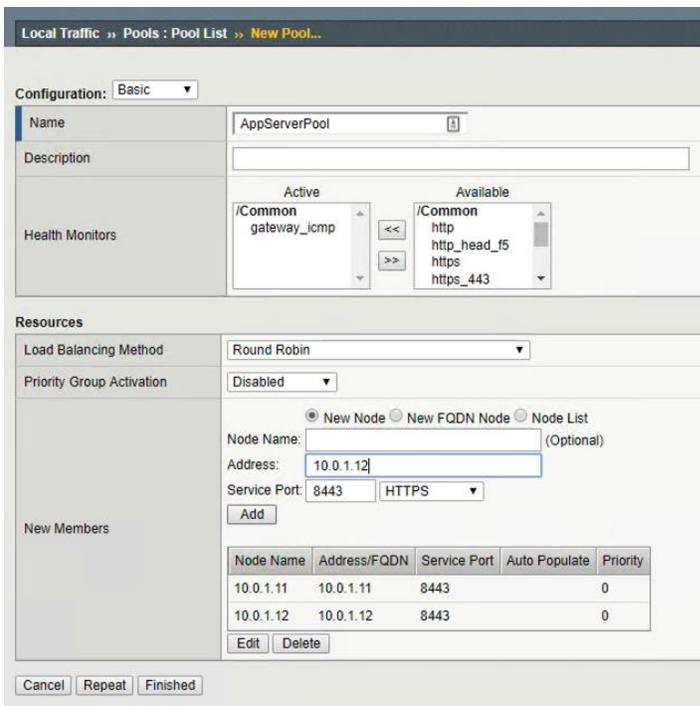
**INTEGRATION GUIDE**

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

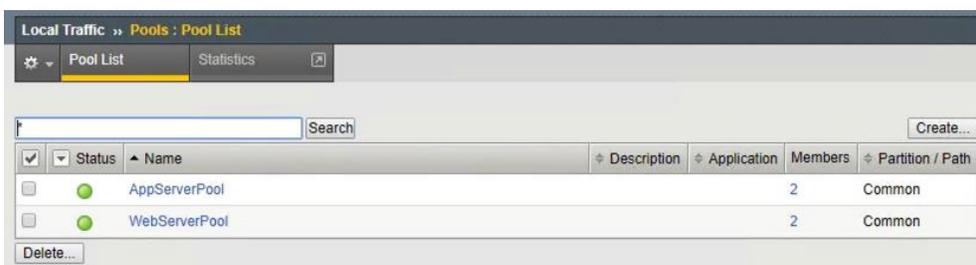
4. In the New Pool menus. **(Make sure to remove any members if the repeat button leaves previous data)**
  - a. In the Name field, type a unique name for the App pool. For this validation AppServerPool was used.
  - b. In the Health Monitors section select an appropriate monitor for your application. 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 ovssdb-tunnel VXLAN network.

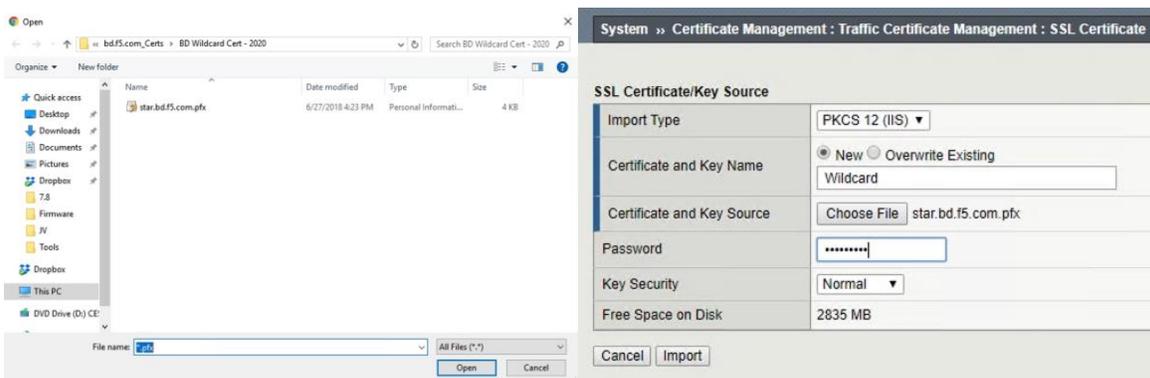


## Import SSL Certificate

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

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

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

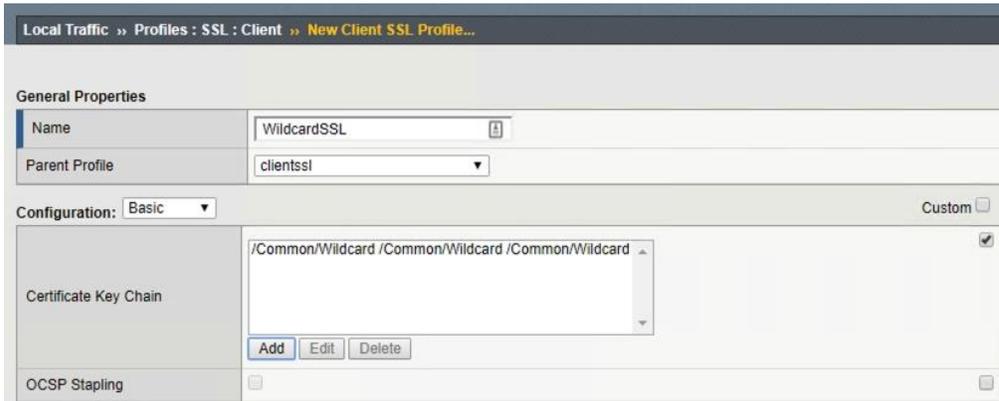
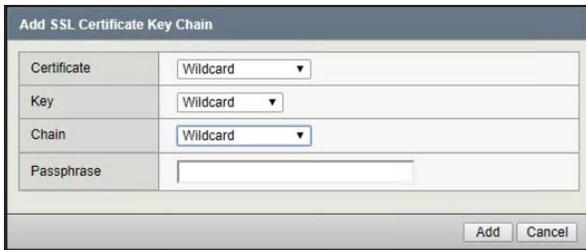
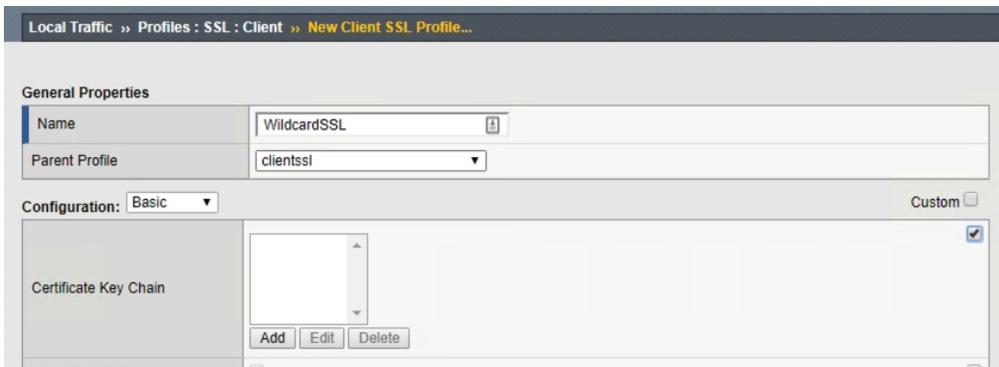


Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition
<input checked="" type="checkbox"/>	Wildcard	RSA Certificate & Key	Normal	*.bd.f5.com	F5 Networks Inc	Jun 27, 2020	Common
<input type="checkbox"/>	ca-bundle	Certificate Bundle				Jan 18, 2020 - Oct 6, 2046	Common
<input type="checkbox"/>	default	RSA Certificate & Key	Normal	localhost.localdomain	MyCompany	Mar 29, 2029	Common
<input type="checkbox"/>	f5-ca-bundle	RSA Certificate		Entrust Root Certificati...	Entrust	Dec 7, 2030	Common
<input type="checkbox"/>	f5-irule	RSA Certificate		support.f5.com	F5 Networks	Jul 18, 2027	Common

## Create ClientSSL Profile

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

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



## Create Application Virtual Servers

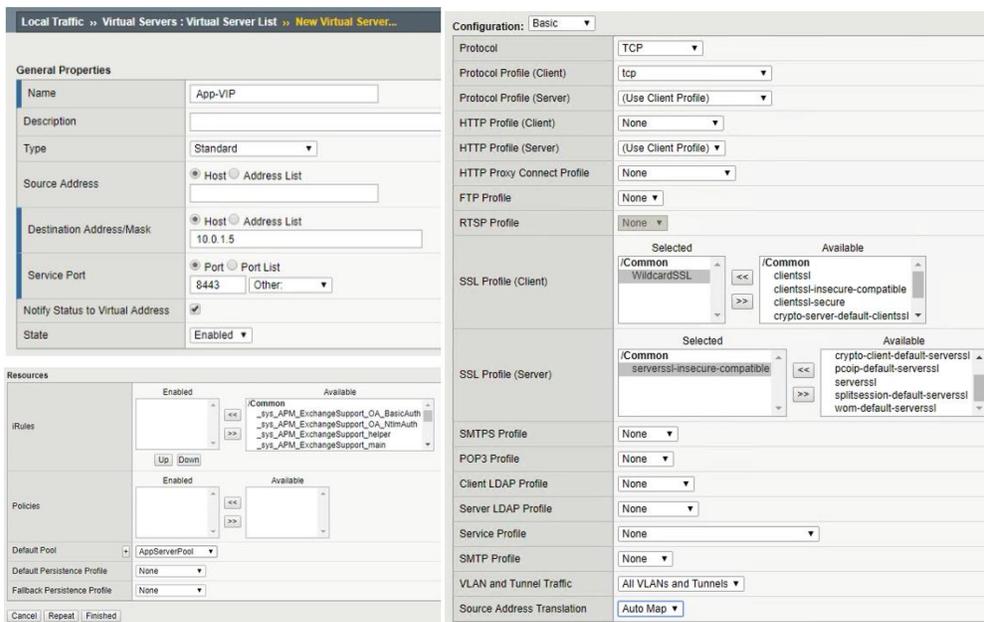
In creating a virtual server, you specify a destination IP address and service port on which the BIG-IP appliance is listening for application traffic to be load balanced to the appropriate application pool members. In this validation, we have two virtual servers (VIPs) to create: one for the WebTier, which will be available to the external network on the 10.105.176.0/24 segment, and the other for the AppTier, available on the WebTier logical network.

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

The screenshot displays the 'New Virtual Server' configuration window in the F5 BIG-IP management console. The window is divided into several sections:

- General Properties:**
  - Name: Web-VIP
  - Destination Address/Mask: 10.105.176.5
  - Service Port: 443
  - State: Enabled
- Resources:**
  - Default Pool: WebServerPool
- Configuration (Basic):**
  - Protocol: TCP
  - SSL Profile (Client): WildcardSSL (Selected)
  - SSL Profile (Server): serverssl-insecure-compatible (Selected)
  - Source Address Translation: Auto Map

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



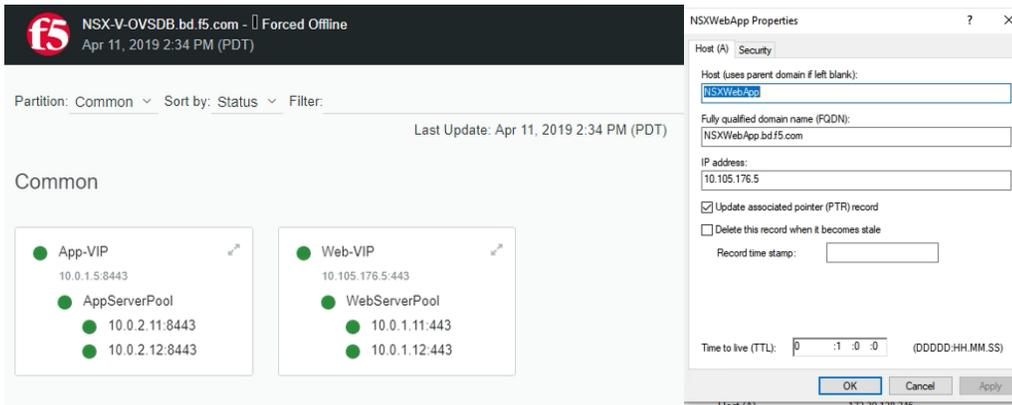
The virtual server list ought to look similar to the one shown below. The green status icons indicate that all systems are going with the validation application. The virtual servers and the associated pools are reachable and healthy.

Local Traffic >> Virtual Servers : Virtual Server List							
Virtual Server List		Virtual Address List		Statistics			
Status	Name	Description	Application	Destination	Service Port	Type	Resources
	App-VIP			10.0.1.5	8443	Standard	Common
	Web-VIP			10.105.176.5	443 (HTTPS)	Standard	Common

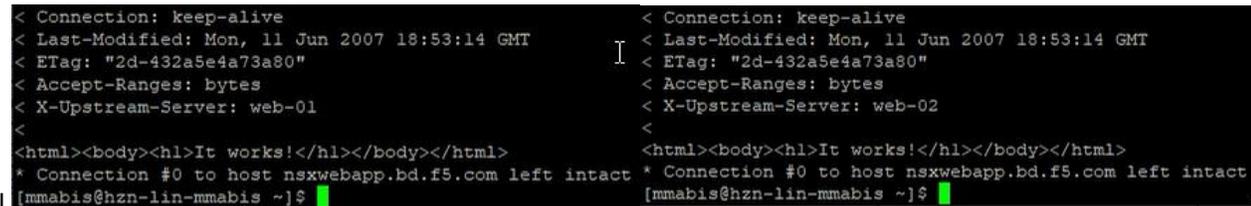
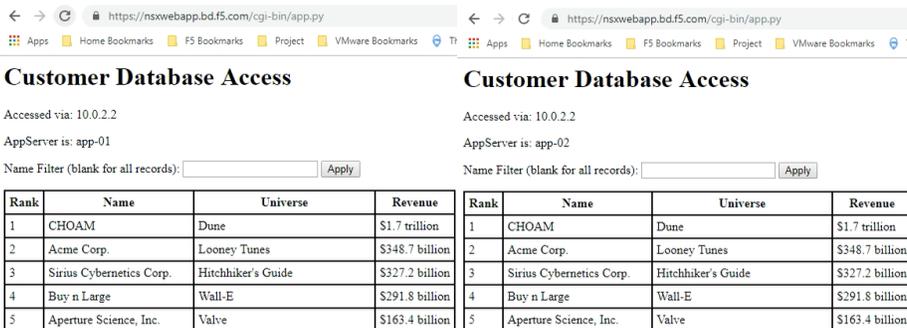
# Validation

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

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



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



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

# Troubleshooting

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

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

## BIG-IP OVSDB Troubleshooting

- TMSH:**

```
tmsch list net tunnels tunnel <tunnel-name>
tmsch list net fdb tunnel <tunnel-name>
tmsch list net self
tmsch list net arp
tmsch list net route
tmsch show net tunnels endpoint tunnel-name <tunnel-name>
tmsch show net tunnels tunnel <tunnel-name>
tmsch 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 ovldb_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
-----
uid          inactivity_probe is_connected max_backoff other_config status target
-----
9c579b5d-f0c0-4159-b2f1-d4b496a3ba01 [] true [] () (sec_since_connect="118", sec_since_disconnect="140", state=ACTIVE) "s1:192.168.2.45:6640"
f5a7e0a6-181d-4e0c-94d1-bd66e97d2cf [] true [] () (sec_since_connect="200", sec_since_disconnect="222", state=ACTIVE) "s1:192.168.2.46:6640"
412940b6-2612-4dde-b593-5908618f21c8 [] true [] () (sec_since_connect="273", sec_since_disconnect="295", state=ACTIVE) "s1:192.168.2.47:6640"

Tunnel table
-----
uid          bfd_config_local          bfd_config_remote          remote          bfd_params
-----
2892ef1a-c942-4b98-9413-ed7f2f6fdda (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.30", bfd dst mac="00:50:56:ef:3d:f0") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 f62d06e4-9c45-4525-8701-278c9e5ac816
bf209194-740e-4652-85bd-b904a330139b (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.31", bfd dst mac="00:50:56:61:b7:e0") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 556dc505-a969-49e6-8763-b43706843d60
46add929-d166-406c-aaeb-e28f77ea3349 (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.32", bfd dst mac="00:50:56:60:67:9e") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 0c5d2d41-a58b-4f5b-906d-0a9ef16135b6
4ecf69de-37be-4469-909a-1d03924daaa5 (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.33", bfd dst mac="00:50:56:68:40:1c") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 6c415526-2dab-46a5-8473-4a9e2fea0e2f
919aeeed-9ca1-40ef-a650-9ffd5350f3d9 (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.34", bfd dst mac="00:50:56:60:12:b5") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 b68a61bb-21f7-4087-a26c-a7a22e29e84d
14e66503-b683-4896-a413-e7ecd93ef2e9 (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.39", bfd dst mac="00:50:56:64:ae:a6") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 f7700709-fa0a-4141-9254-183060563b9e
0074575-201e-42d4-a7d9-a5199cd902 (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.40", bfd dst mac="00:50:56:66:77:ea") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 46c93b54-a3ea-4d8e-9221-4a3ea792c776
5d013507-5b76-4a16-b71f-488cb71a61b8 (bfd dst ip="192.172.50.81", bfd dst mac="00:23:e9:fc:f9:c3") (bfd dst ip="192.172.50.41", bfd dst mac="00:50:56:66:58:d4") (enabled="true", forwarding="true", min_rx="300") (enabled="true", forwarding="true", remote_state=up, state=up) ef35d1ad-33cb-407f-bee1-1145745e24a4 aa42e10e-0e54-429f-988d-7afcf51eb27
```

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

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