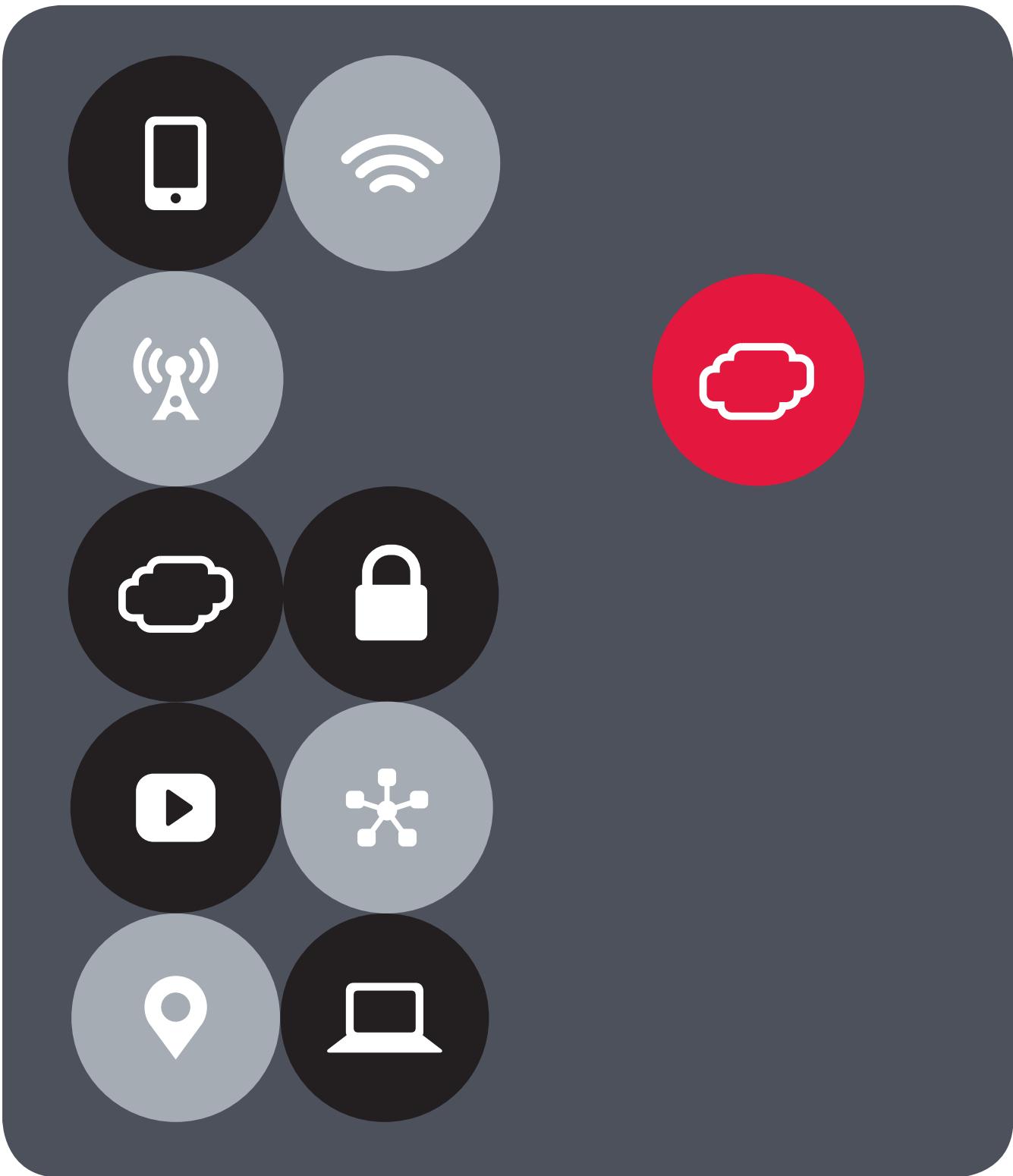




vmware®

BEST PRACTICES

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





BEST PRACTICES

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

Contents

Introduction	3
<hr/>	
Topology 1: Parallel to NSX Edge Using VXLAN Overlays with BIG-IP Physical Appliances	4
Key Components	4
Implementation Infrastructure	5
Traffic Management between Data Centers	5
Create and Deploy DLR	17
NSX Edge Static Routing Configuration	23
BIG-IP Appliance Configuration	25
Validation	36
<hr/>	
Topology 2: Parallel to DLR Using VLANs with BIG-IP Physical Appliances	38
Implementation Infrastructure	39
Create and Deploy DLR	42
BIG-IP Appliance Configuration	48
Validation	60
<hr/>	
Topology 3: One-Arm Connected Using VXLAN Overlays with BIG-IP Virtual Edition	62
Implementation Infrastructure	63
NSX Edge Configuration	66
Create and Deploy DLR	72
NSX Edge Static Routing Configuration	79
BIG-IP Appliance Configuration	81
Provision BIG-IP Network Adapters in vSphere	82
Provision BIG-IP Networking	85
Validation	105
<hr/>	
Conclusion	106



Introduction

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

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

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

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

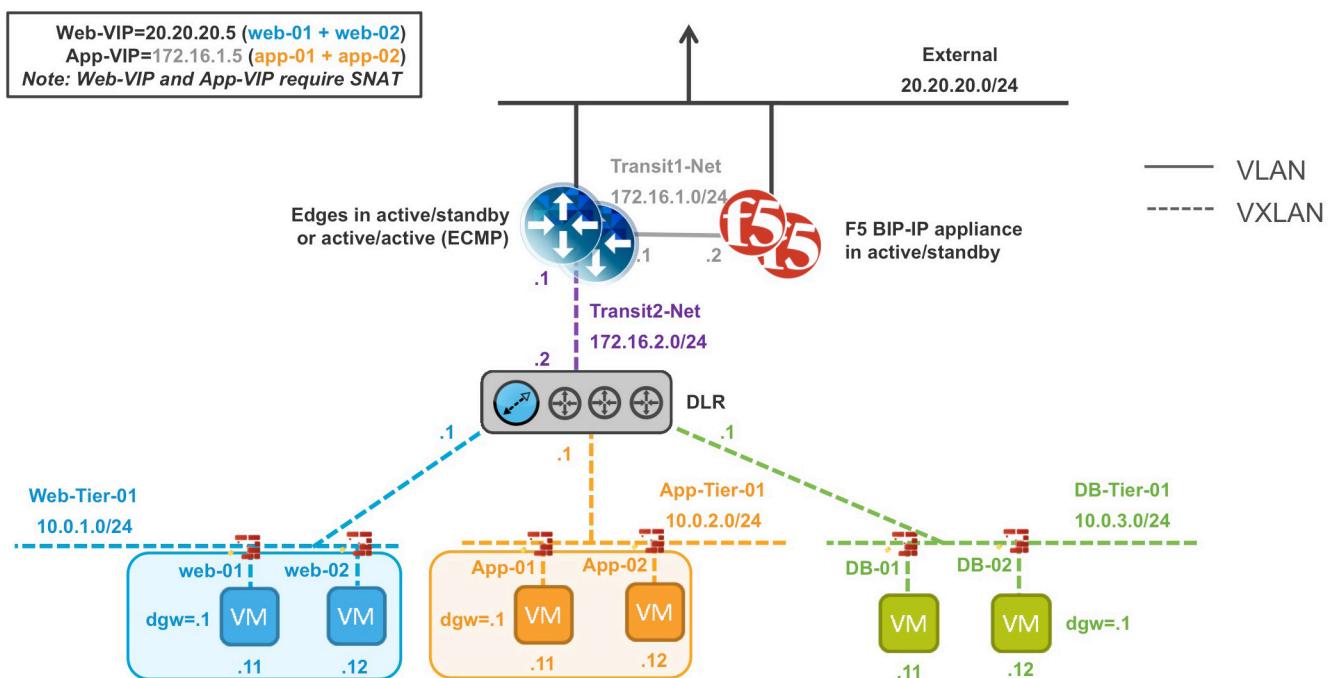


Figure 1. BIG-IP appliance parallel to NSX Edge Services Gateway

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

BEST PRACTICES

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

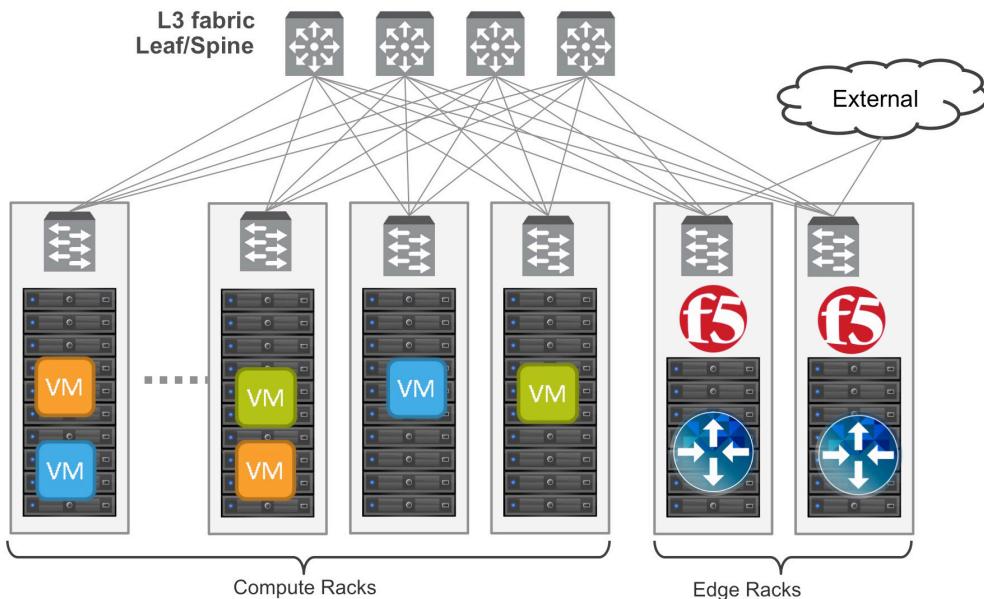


Figure 2. Leaf/spine physical rack infrastructure

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

Implementation Infrastructure

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

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

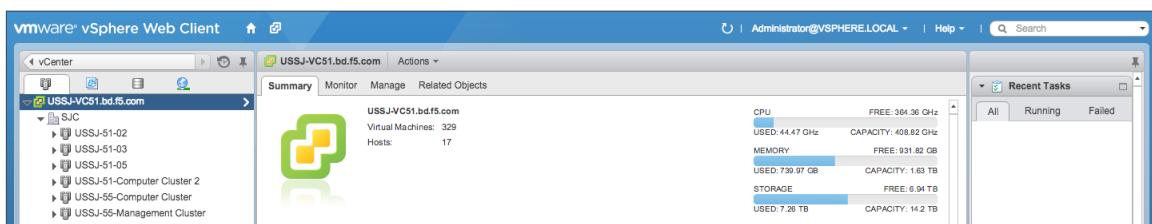


Figure 3. vSphere console



BEST PRACTICES

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

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

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

Prerequisites

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

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

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

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



BEST PRACTICES

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

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

Table 2. Logical switch configuration

Network Segments

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

802.1Q VLAN segments

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

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

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

VXLAN Segments

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

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

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

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

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

BEST PRACTICES

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

NSX Edge Configuration

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

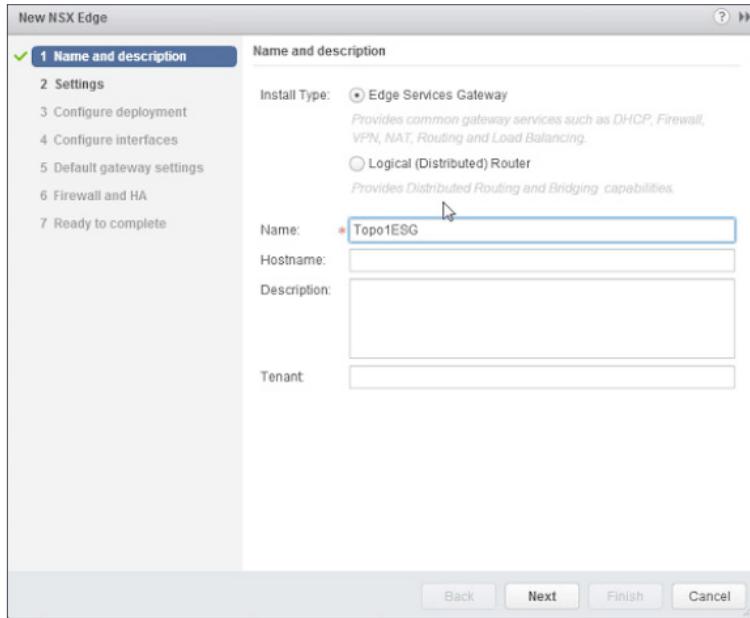


2. Select Edge Services Gateway as the Install Type and provide a name for the device, then click **Next**.

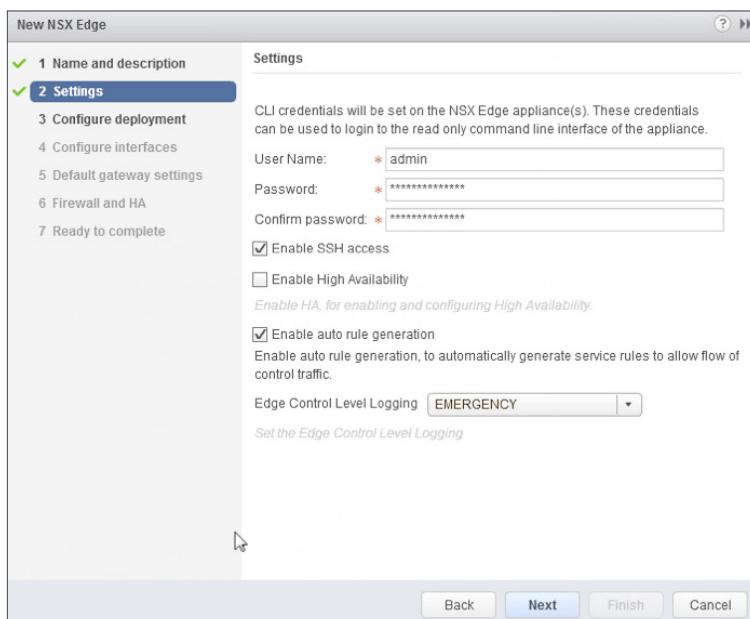


BEST PRACTICES

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



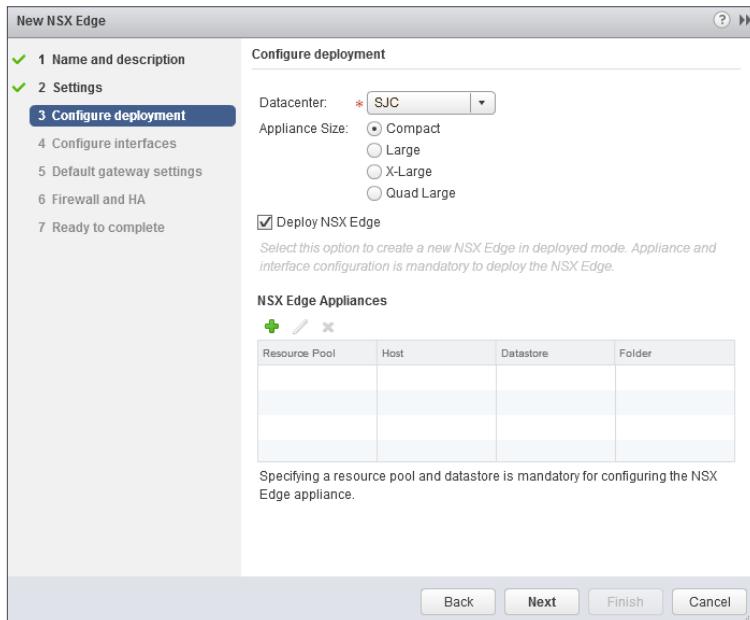
3. Under **Settings**, select **Enable SSH access** and provide a username and password for the Edge Services Gateway. Click **Next**.



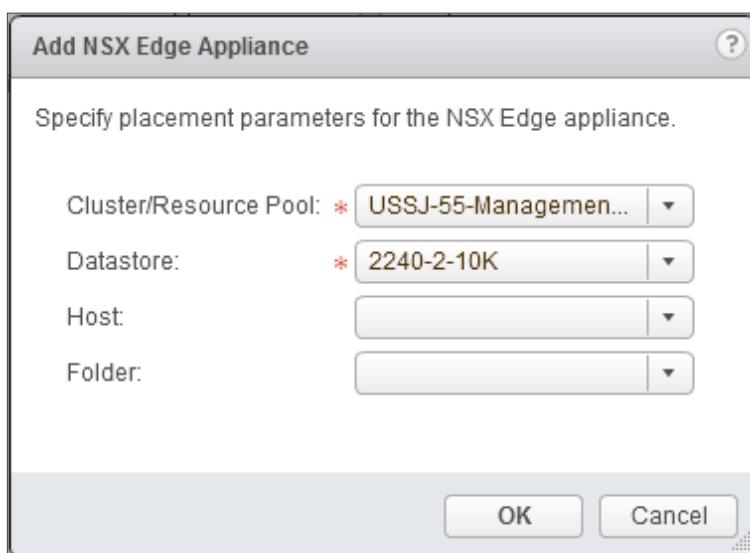
4. Under **Configure deployment**, select the Datacenter and Appliance Size appropriate for your deployment, and check the **Deploy NSX Edge** checkbox. Then click on the green plus symbol (+) under NSX Edge Appliances.

BEST PRACTICES

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



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



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



BEST PRACTICES

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

New NSX Edge

Configure interfaces

Configure interfaces of this NSX Edge

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To

Back Next Finish Cancel

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



BEST PRACTICES

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

Add NSX Edge Interface

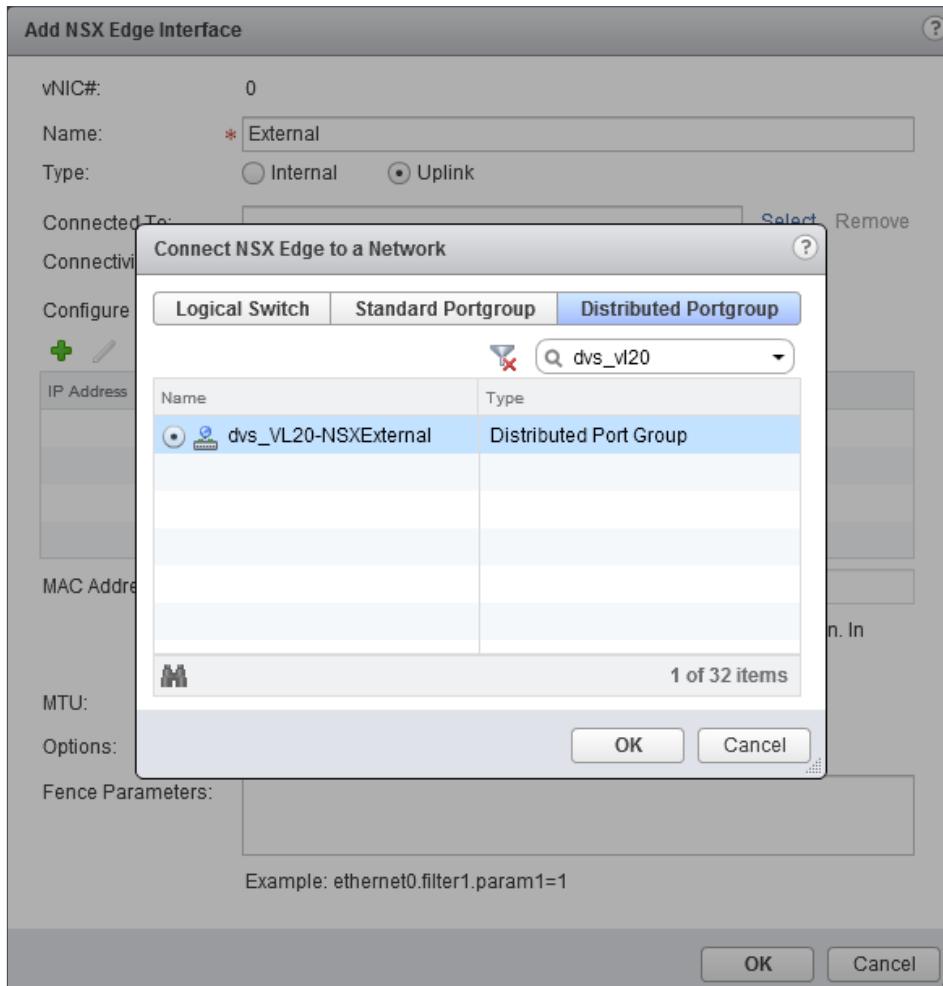
vNIC#:	0
Name:	<input type="text" value="External"/> *
Type:	<input type="radio"/> Internal <input checked="" type="radio"/> Uplink
Connected To:	<input type="text"/> Select Remove
Connectivity Status:	<input type="radio"/> Connected <input checked="" type="radio"/> Disconnected
Configure subnets	
+ Edit X	
IP Address	Subnet Prefix Length
MAC Addresses:	<input type="text"/> <input type="text"/>
You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.	
MTU:	<input type="text" value="1500"/>
Options:	<input type="checkbox"/> Enable Proxy ARP <input type="checkbox"/> Send ICMP Redirect
Fence Parameters:	<input type="text"/> Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

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

BEST PRACTICES

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



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

BEST PRACTICES

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



Add NSX Edge Interface

vNIC#:	0
Name:	<input type="text" value="External"/> *
Type:	<input type="radio"/> Internal <input checked="" type="radio"/> Uplink
Connected To:	dvs_VL20-NSXExternal Change Remove
Connectivity Status:	<input checked="" type="radio"/> Connected <input type="radio"/> Disconnected
Configure subnets	
 	
IP Address	Subnet Prefix Length
MAC Addresses:	<input type="text"/> <input type="text"/>
You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.	
MTU:	<input type="text" value="1500"/>
Options:	<input type="checkbox"/> Enable Proxy ARP <input type="checkbox"/> Send ICMP Redirect
Fence Parameters:	<input type="text"/> Example: ethernet0.filter1.param1=1

[OK](#) [Cancel](#)

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

BEST PRACTICES

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



Add Subnet

Specify the IP addresses in the subnet: *

+ **-pencil** **-x**

Primary IP	IP Address
<input checked="" type="radio"/>	172.16.1.1

Subnet prefix length: * 24

OK **Cancel**

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

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

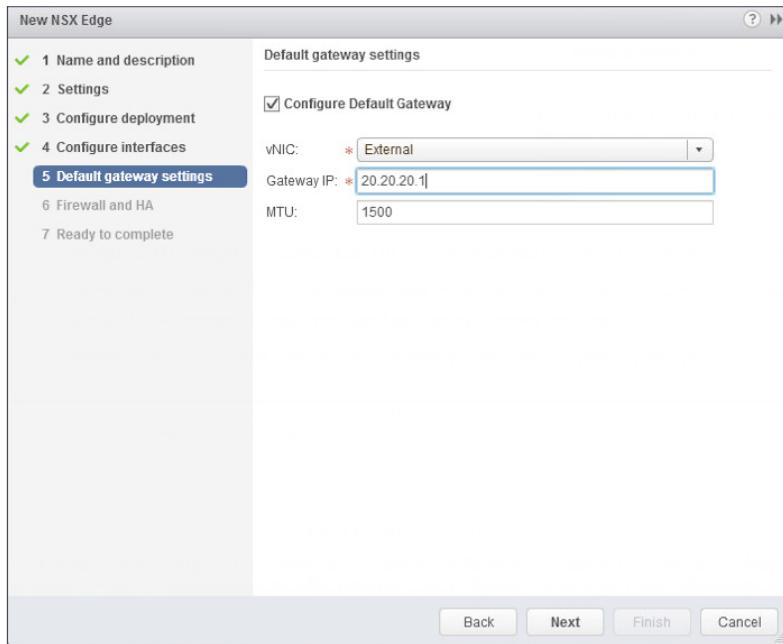
Table 3. NSX Edge network interfaces

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

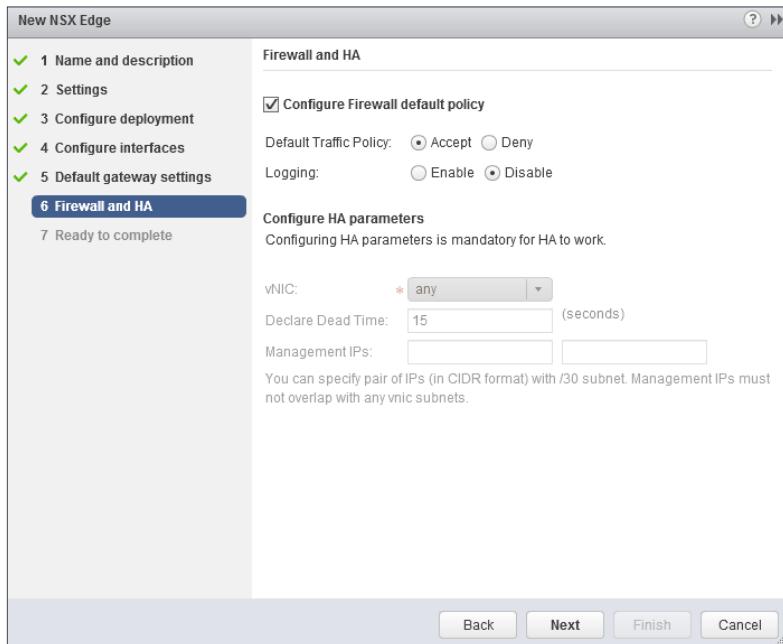
Use the default MTU parameter unless the network is using an MTU of a different size, such as jumbo frames. (Configuring a non-standard MTU that is inconsistent can lead to unnecessary fragmentation of packets or black-holing of some traffic.) Click **Next** to continue.

BEST PRACTICES

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



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



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

BEST PRACTICES

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



Create and Deploy DLR

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

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

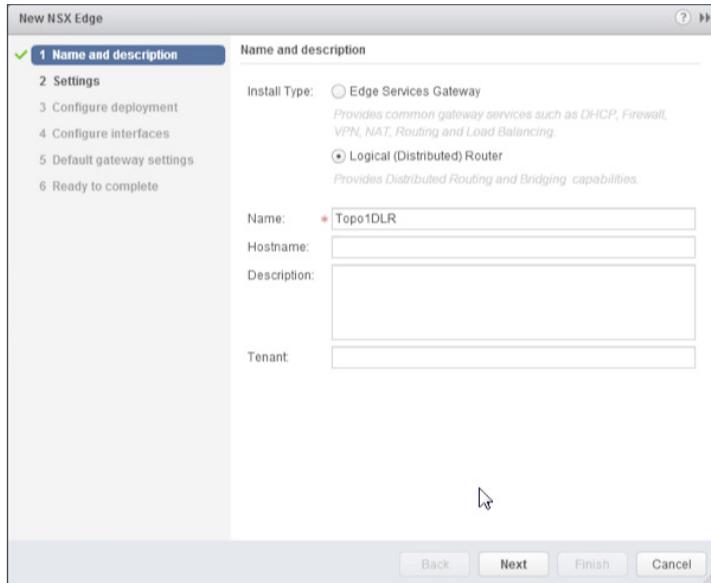
1. Return to the vSphere Web Client console and choose Networking & Security in the left column. Under Networking and Security, choose NSX Edges and then click the green plus symbol (+).

A screenshot of the VMware vSphere Web Client interface. The title bar says "vmware vSphere Web Client". The left sidebar has a "Networking & Security" section with several icons and links: NSX Home, Installation, Logical Switches, NSX Edges (which is selected and highlighted in blue), Firewall, SpoofGuard, Service Definitions, Service Composer, Data Security, Flow Monitoring, Activity Monitoring, Networking & Security Inventory, and NSX Managers. The main panel is titled "NSX Edges" and shows a table with one row. The table has columns for "Id" and "Name". The value for Id is 1 and for Name is blank. There is a green plus sign icon above the table, indicating the ability to add new entries.

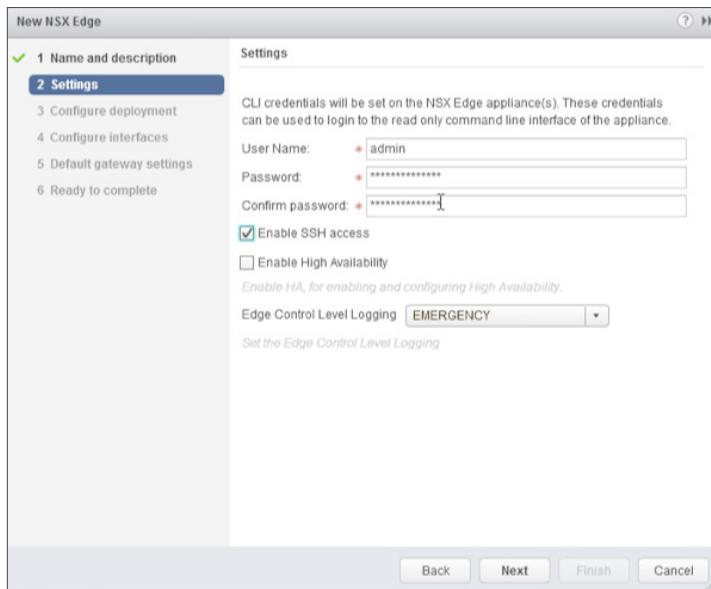
2. Select Logical (Distributed) Router as the Install Type and provide a name for the device, then click Next.

BEST PRACTICES

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



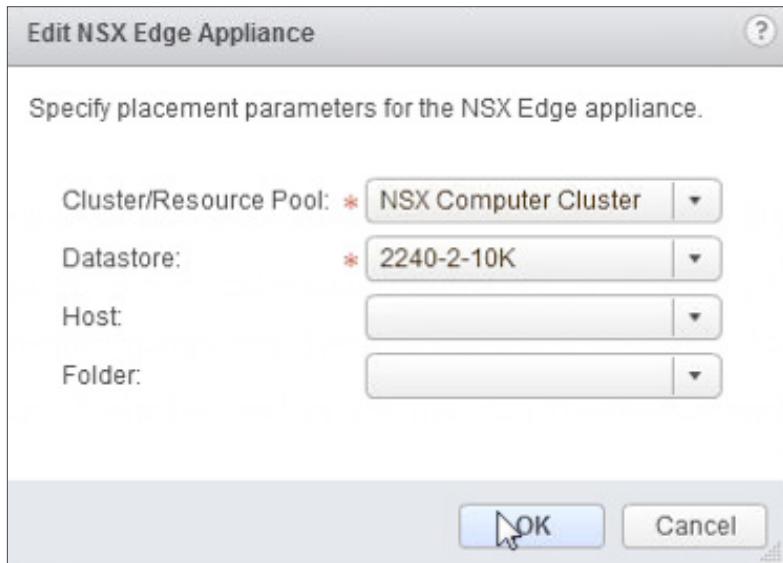
3. Under **Settings**, check **Enable SSH access** and provide a username and password for the Edge Services Gateway. Select **Next**.



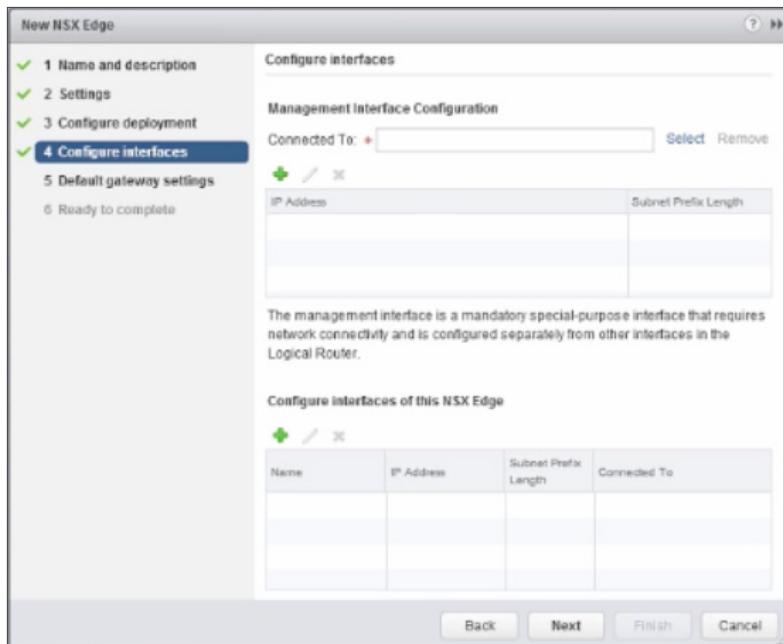
4. Selecting the green plus symbol (+) in the **Configure Deployment** section will display the options in the figure below. Choose the appropriate Cluster/resource pool and Datastore (for this example, the **NSX Computer Cluster** and the **2240-2-10K** datastore). The **Host** is optional. Click **OK**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

BEST PRACTICES

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



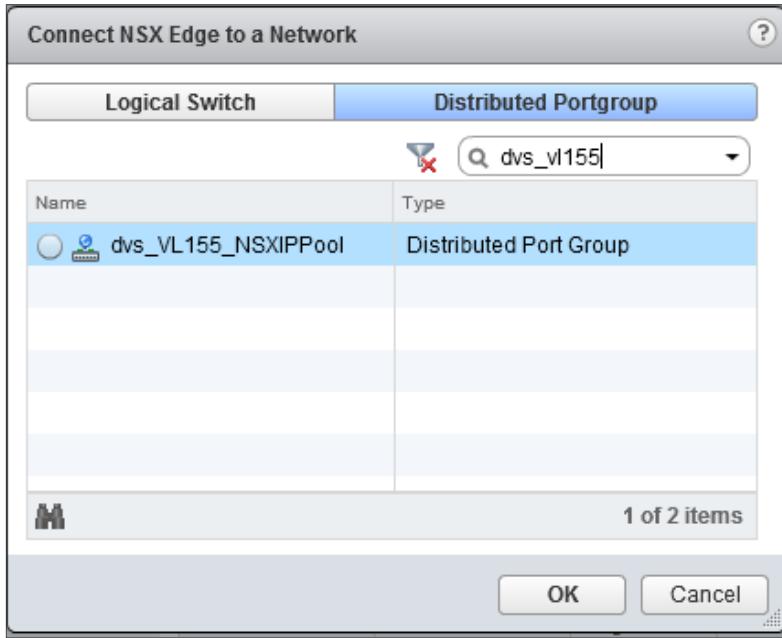
- Select Configure Interfaces, and then click Select to the right of the Connected To text box.



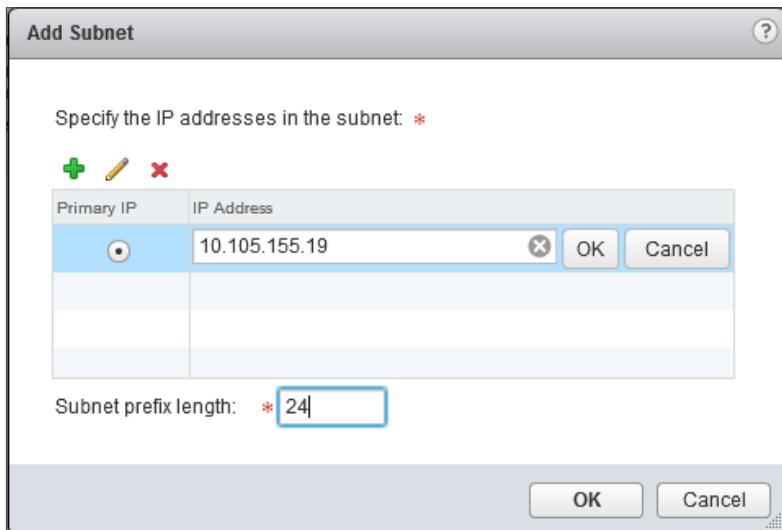
- In this case, the management interface should be connected to a distributed port group that is connected to the shared management VLAN.

BEST PRACTICES

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



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



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

BEST PRACTICES

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

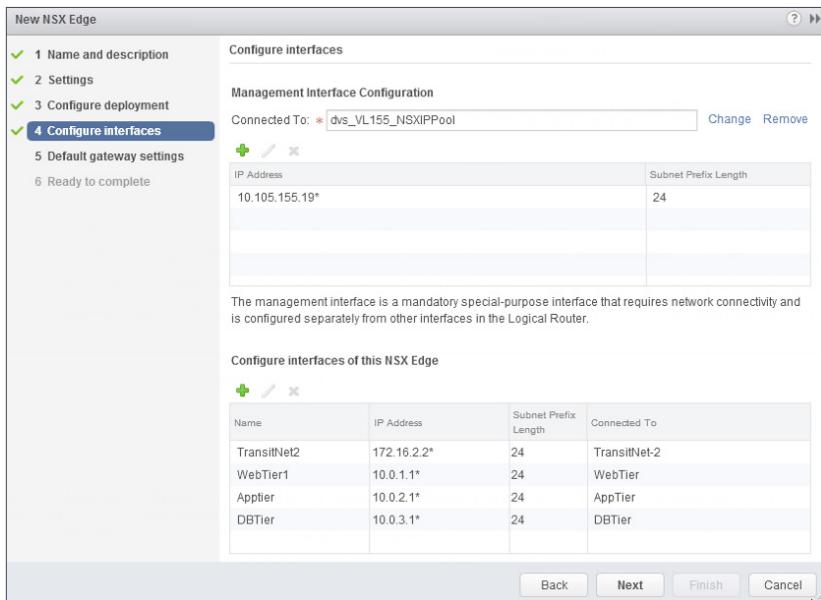


Network Name	Connected To	Type	Network	Interface IP/Subnet Prefix
TransitNet2	TransitNet-2	Uplink	Logical Switch	172.16.2.2/24
WebTier	WebTier	Internal	Logical Switch	10.0.1.1/24
AppTier	AppTier	Internal	Logical Switch	10.0.2.1/24
DBTier	DBTier	Internal	Logical Switch	10.0.3.1/24

Table 4. NSX distributed logical router network interfaces

The DLR interface configuration, once completed, should resemble the dialog box below.

Click **Next** to continue.



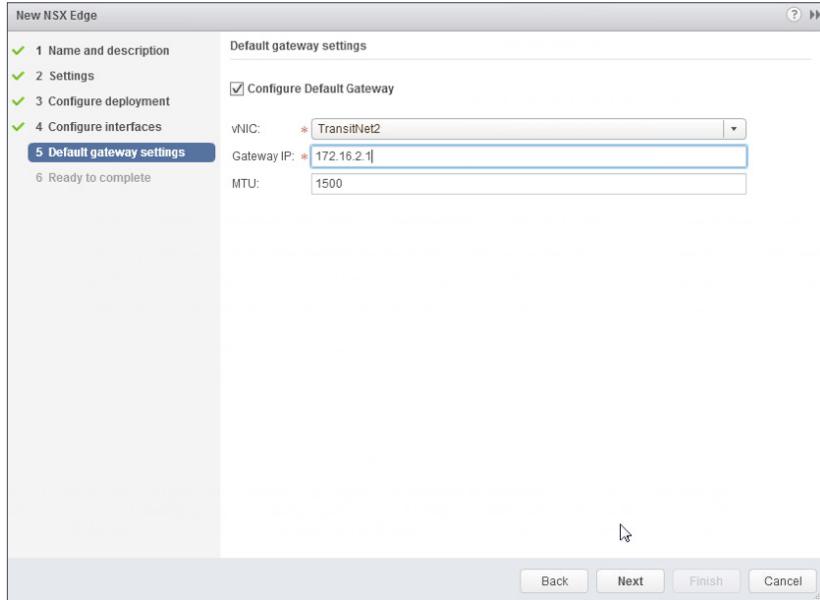
- With the interface settings complete, the next step is to configure the default gateway settings. The default gateway for the DLR is the data center core router that we configured in the previous section across the transit segment TransitNet2.

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

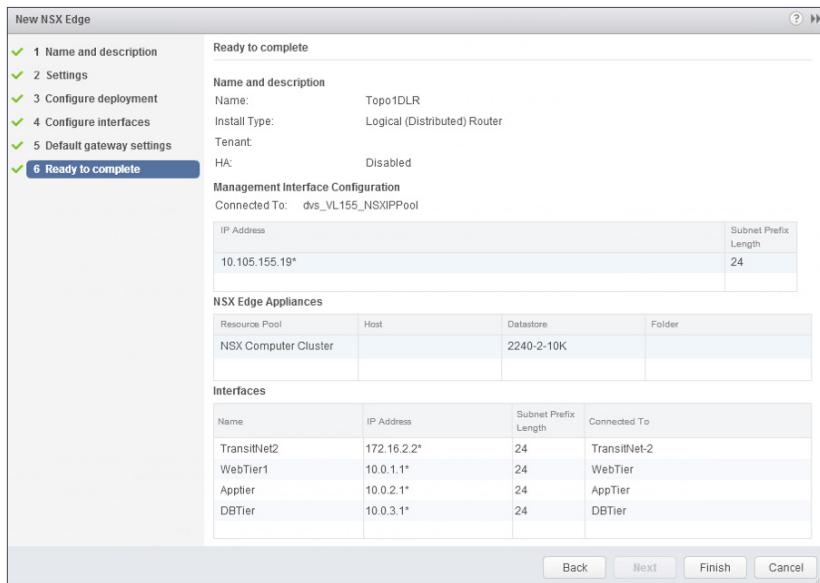


BEST PRACTICES

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



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



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



BEST PRACTICES

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

NSX Edge Static Routing Configuration

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

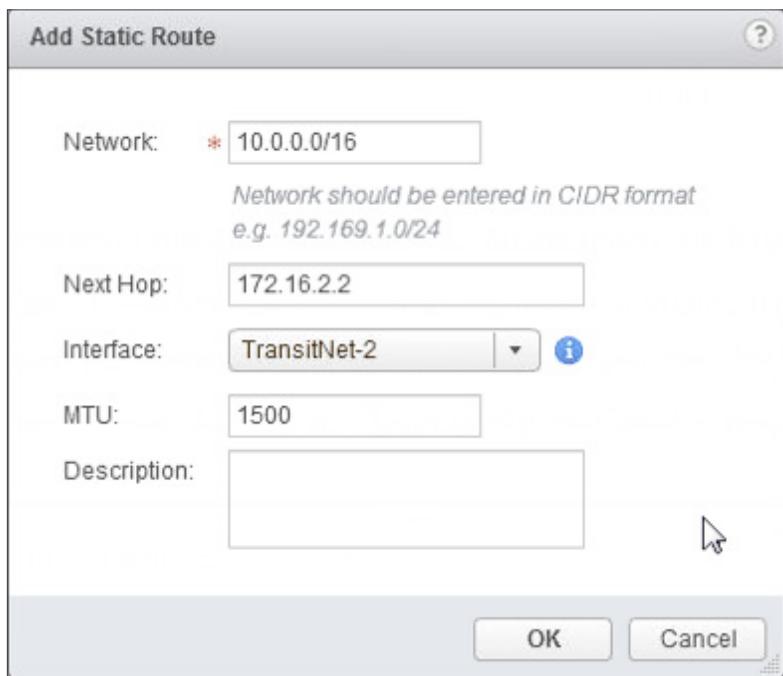
1. Double-click on the NSX Edge you configured in the first section.

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

BEST PRACTICES

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

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



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

Type	Network	Next Hop	Interface
	10.0.0.0/16	172.16.2.2	TransitNet-2



BEST PRACTICES

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

BIG-IP Appliance Configuration

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

Prerequisites

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

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

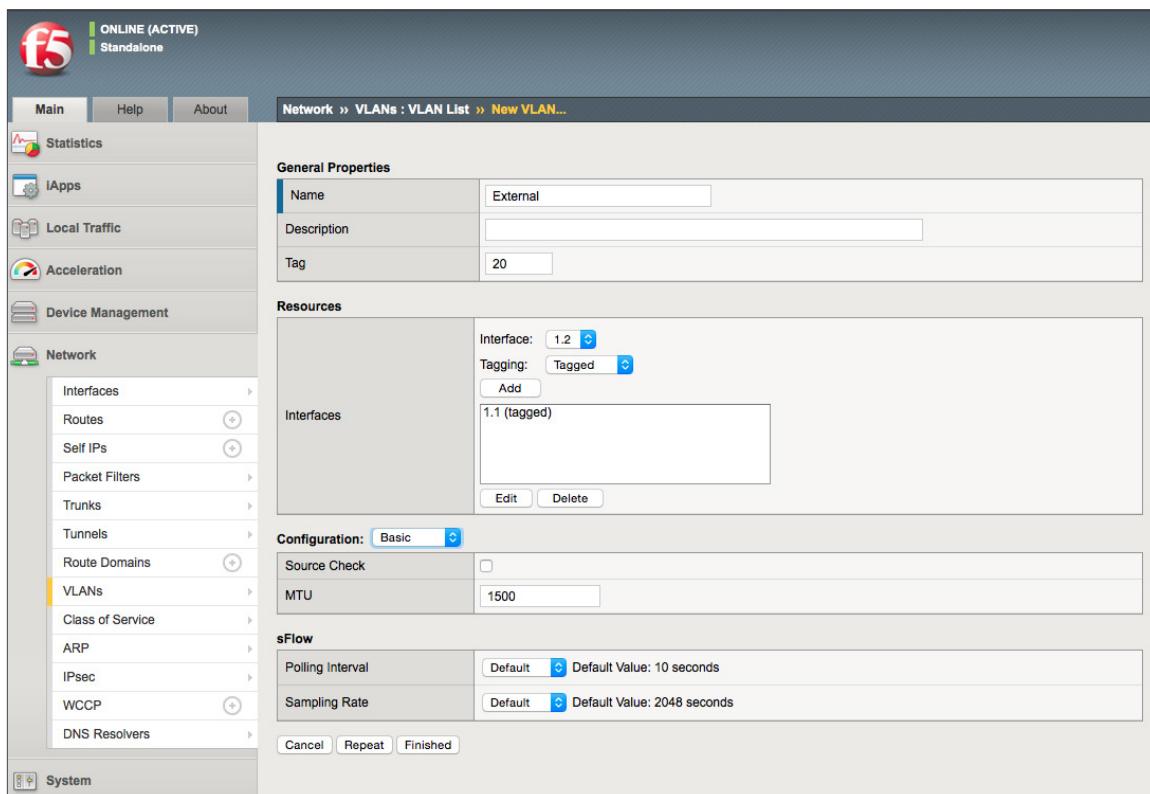
Create VLANs

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

BEST PRACTICES

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

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



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

BEST PRACTICES

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

Configure Self IP Addresses

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

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

The screenshot shows the F5 BIG-IP Management interface. The top bar displays the hostname bd5000.bd.f5.com, date Feb 19, 2015, and user admin. The main navigation bar includes File, Edit, View, Favorites, Tools, and Help. The left sidebar has links for Statistics, iApp, Local Traffic, Acceleration, Device Management, and Network (with sub-links for Interfaces, Routes, Self IPs, and Packet Filters). The current view is under the Network section, specifically in the Self IPs sub-section, with a sub-link for 'New Self IP...'. A progress message 'Receiving configuration data from your device.' is displayed above the configuration form. The configuration form contains the following fields:

Configuration	
Name	ExtSelfIP
IP Address	20.20.20.10
Netmask	255.255.255.0
VLAN / Tunnel	External
Port Lockdown	Allow None
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)

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



BEST PRACTICES

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

9. Complete the configuration for the **TransitNetSelf** self IP using the following settings:
 - a. Name: **TransitNetSelf**
 - b. IP Address: **172.16.1.2**
 - c. Netmask: **255.255.255.0**
 - d. VLAN/Tunnel: **TransitNet1**

The screenshot shows the F5 Management Interface. The top navigation bar includes File, Edit, View, Favorites, Tools, and Help. Below it, the status bar shows Hostname: bd5000.bd.f5.com, Date: Feb 19, 2015, IP Address: 10.105.155.17, Time: 2:16 PM (PST), User: admin, and Role: Administrator. The main header says "ONLINE (ACTIVE)" and "Standalone". The left sidebar has links for Main, Help, About, Statistics, iApp, Local Traffic, Acceleration, Device Management, and Network (with sub-links for Interfaces, Routes, and Self IPs). The current page is "Network > Self IPs > New Self IP...". The configuration form on the right has fields for Name (TransNetSelf), IP Address (172.16.1.2), Netmask (255.255.255.0), VLAN / Tunnel (TransitNet1), Port Lockdown (Allow None), and Traffic Group (traffic-group-local-only (non-floating)). At the bottom of the form are buttons for Cancel, Repeat, and Finished, with "Finished" being highlighted.

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

The screenshot shows the "Network > Self IPs" page. The top navigation bar includes a gear icon, "Self IP List", and a "Create..." button. The main table lists self IP configurations with columns for Name, Application, IP Address, Netmask, VLAN / Tunnel, Traffic Group, and Partition / Path. Two entries are listed: "ExtSelfIP" (IP 20.20.20.10, Netmask 255.255.255.0, VLAN/Path External, Traffic Group traffic-group-local-only, Partition Common) and "TransitNet-01" (IP 172.16.1.2, Netmask 255.255.255.0, VLAN/Path App-Tier, Traffic Group traffic-group-local-only, Partition Common). A "Delete..." button is located at the bottom of the table.

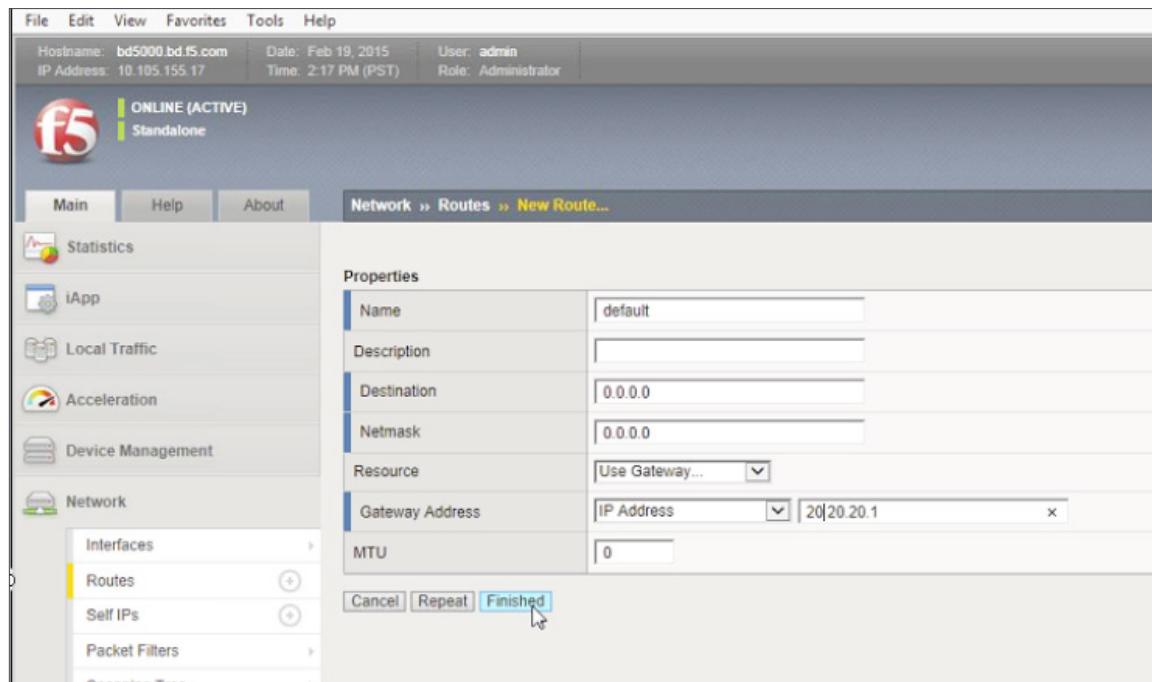
BEST PRACTICES

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

Configure Static Routes

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

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



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



BEST PRACTICES

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

8. The Gateway Address is the address of the NSX Edge Service Gateway on the transit segment TransitNet1: 172.16.1.1.
9. Click Finished to continue.

The screenshot shows the F5 Management Interface. The top bar displays the hostname bd5000.bd.f5.com, IP address 10.105.155.17, date Feb 19, 2015, time 2:17 PM (PST), user admin, and role Administrator. The status bar indicates the device is ONLINE (ACTIVE). The main menu includes File, Edit, View, Favorites, Tools, and Help. Below the menu is a toolbar with icons for Statistics, iApp, Local Traffic, Acceleration, Device Management, and Network. Under Network, the 'Routes' option is selected. The central pane shows a 'Network > Routes > New Route...' dialog. The 'Properties' section contains the following fields:

- Name: ServerRoutes
- Description: (empty)
- Destination: 10.0.0.0
- Netmask: 255.255.0.0
- Resource: Use Gateway... (dropdown)
- Gateway Address: IP Address dropdown set to 172.16.1.1
- MTU: 0

At the bottom of the dialog are three buttons: Cancel, Repeat, and Finished, with Finished being highlighted.

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

Network > Routes							
Route List							
	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource
<input type="checkbox"/>	default	Default IPv4		Partition Default Route Domain	Gateway	20.20.20.1	Common
<input type="checkbox"/>	ServerRoutes		10.0.0.0	255.255.0.0	Partition Default Route Domain	Gateway	172.16.1.1 Common

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,



BEST PRACTICES

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

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

Create application pools

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

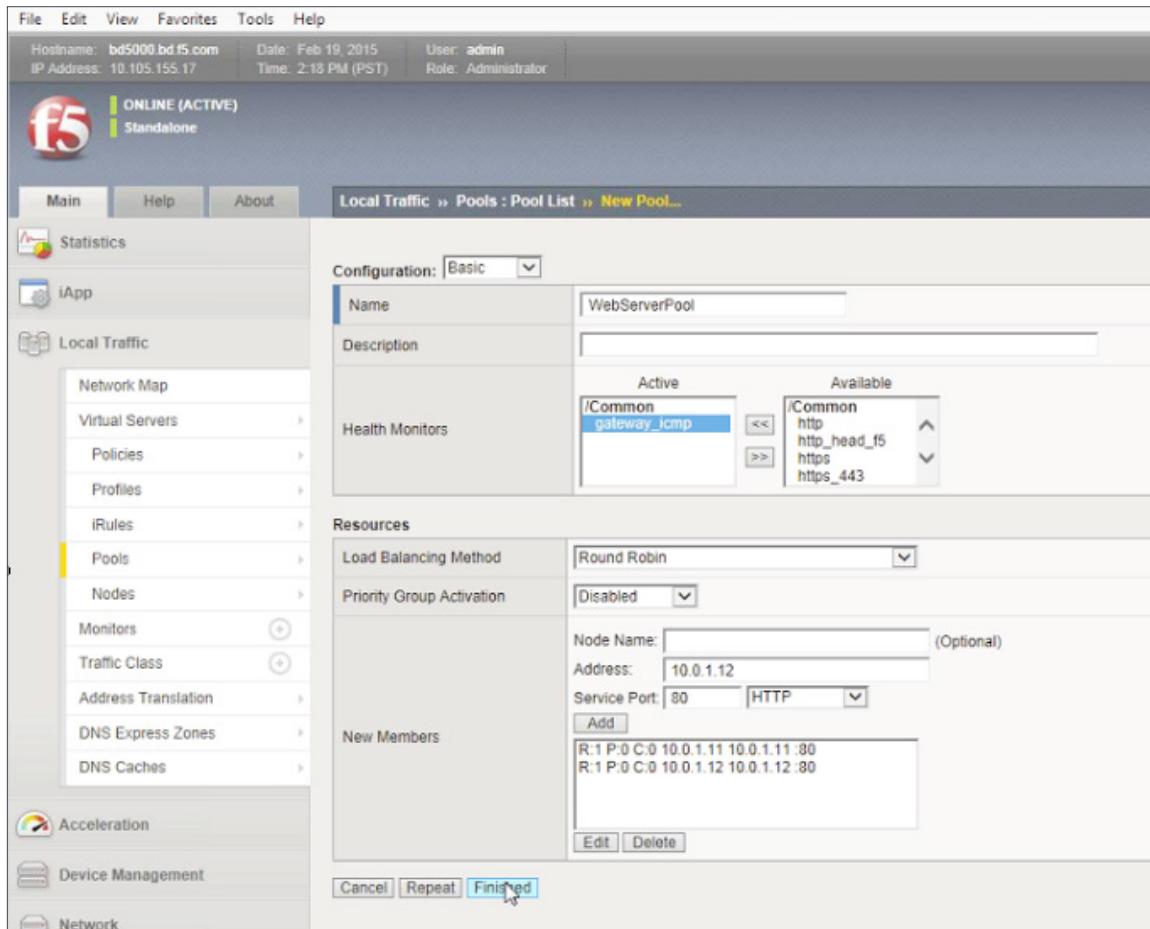
1. On the Main tab, click Local Traffic and then click Pools to display the Pool List screen.
2. In the upper right corner of the screen, click the Create button.
3. In the Name field, type a unique name for the web pool. For this validation, we used WebServerPool.
4. In the Health Monitors section,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

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

Table 5. BIG-IP web tier pool members

BEST PRACTICES

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



8. In the Name field, type a unique name for the web pool. For this validation AppServerPool was used.
9. In the Health Monitors section select an appropriate monitor for your application. In this case, we are choosing a gateway_icmp monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.
10. In the Resources section of the screen select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
11. In the Resources section of the screen, use the New Members setting to add the IP address and port of the web servers (refer to Table 6). Select the Add button for each pool member.
12. Click Finished to complete the pool creation.

BEST PRACTICES

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

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

Table 6. BIG-IP application tier pool members

The completed configuration for the web and application tier pools should look similar to the image above. 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	Create...	
Status	Name	Application	Members	Partition / Path
<input type="checkbox"/>	<input checked="" type="checkbox"/> AppServerPool		2	Common
<input type="checkbox"/>	<input checked="" type="checkbox"/> WebServerPool		2	Common

[Delete...](#)

Create application virtual server

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

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



BEST PRACTICES

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

Screenshot of the F5 BIG-IP Local Traffic Virtual Servers configuration interface.

General Properties:

- Name: Web-Vip
- Description: (empty)
- Type: Standard
- Source: (empty)
- Destination:
 - Type: Host (radio button selected)
 - Address: 20.20.20.5
- Service Port: 80 (HTTP)
- State: Enabled

Content Rewrite:

- Rewrite Profile: None
- HTML Profile: None

Acceleration:

- Rate Class: None
- OneConnect Profile: None
- NTLM Conn Pool: None
- HTTP Compression Profile: None
- Web Acceleration Profile: None
- SPDY Profile: None

Resources:

- iRules:
 - Enabled: (empty)
 - Available: _sys_auth_krbdelegate, _sys_auth_ssl_oc_idap, _sys_auth_ssl_crlip, _sys_auth_ssl_ocsp, _sys_https_redirected
 - Buttons: Up, Down, <<, >>
- Policies:
 - Enabled: (empty)
 - Available: /Common/sys_CEC_video_policy
 - Buttons: <<, >>
- Default Pool: WebServerPool
- Default Persistence Profile: None
- Fallback Persistence Profile: None

Buttons at the bottom: Cancel, Repeat, Finished

BEST PRACTICES

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

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

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

Local Traffic > Virtual Servers : Virtual Server List						
		Virtual Server List		Virtual Address List		Statistics
<input checked="" type="checkbox"/> <input type="checkbox"/>		Status	Name	Application	Destination	Service Port
<input type="checkbox"/>	●	App-Vip		10.0.1.5	80 (HTTP)	Standard
<input type="checkbox"/>	●	Web-Vip		20.20.20.5	80 (HTTP)	Standard

[Create...](#) [Edit...](#) [Common](#)
[Enable](#) [Disable](#) [Delete...](#)

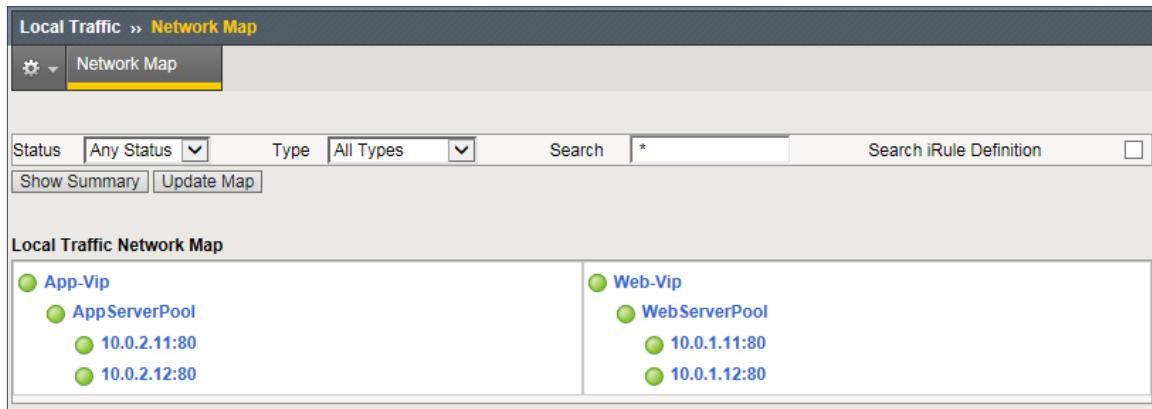
Validation

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

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

BEST PRACTICES

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



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



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

BEST PRACTICES

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



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

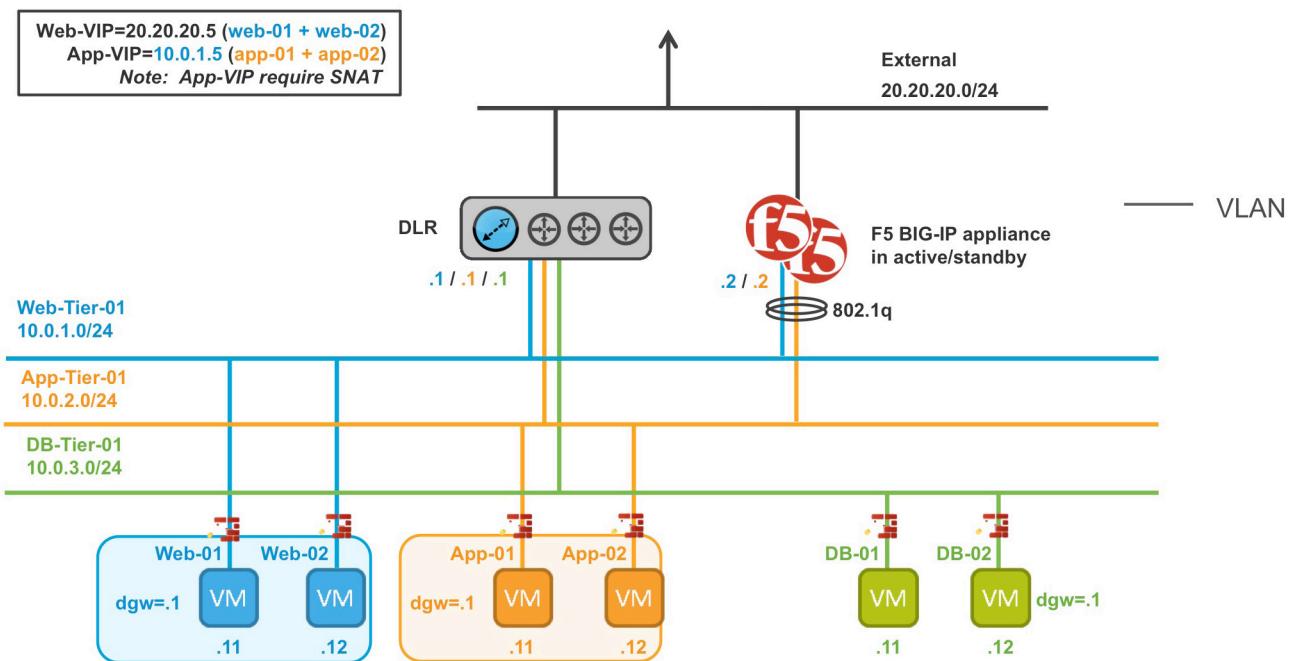


Figure 4. BIG-IP appliances parallel to DLR

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

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

BEST PRACTICES

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

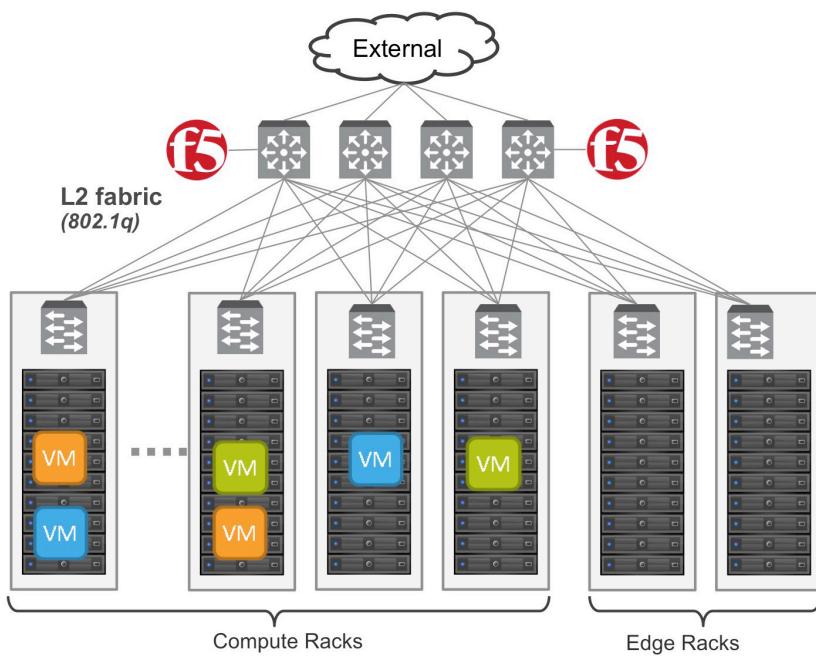


Figure 5. Traditional layer 2 topology with BIG-IP in distribution layer

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

Implementation Infrastructure

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

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



Figure 6. vSphere console



BEST PRACTICES

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

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

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

Prerequisites

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

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

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

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

BEST PRACTICES

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

Network Segments

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

802.1Q VLAN segments

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

VLAN 155 dvs_VL155_NSXIPPool (*not shown*) is for management connectivity.

The 10.105.155.0/24 IP subnet range is configured on this VLAN.

VLAN 160 Web-Tier-01 is the VLAN ID used for the blue web connectivity.

The 10.0.1.0/24 IP subnet range is configured on this VLAN.

VLAN 161 App-Tier-01 is the VLAN ID used for the yellow app connectivity.

The 10.0.2.0/24 IP subnet range is configured on this VLAN.

VXLAN 162 DB-Tier-01 is the VLAN ID used for the green DB connectivity.

The 10.0.3.0/24 IP subnet range is configured on this VLAN.

Figure 7. vSphere DVS VLAN configuration example

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

BEST PRACTICES

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

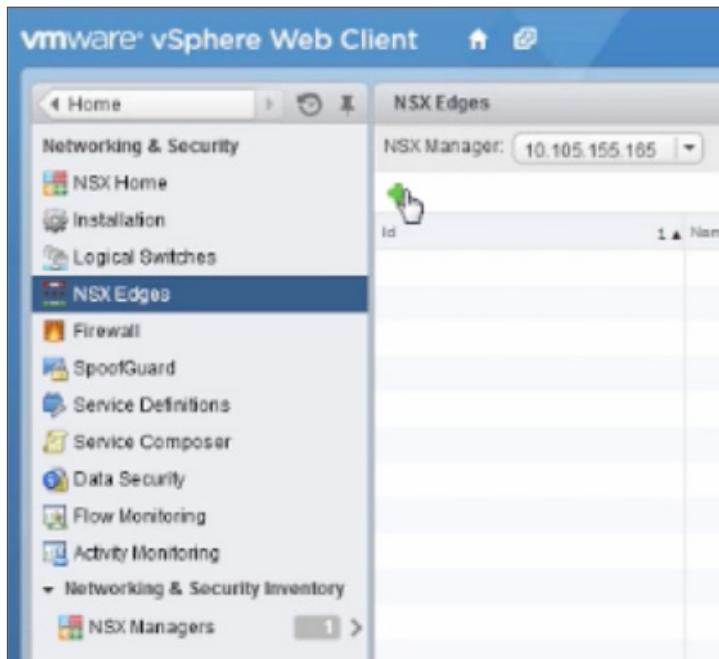


Create and Deploy DLR

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

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

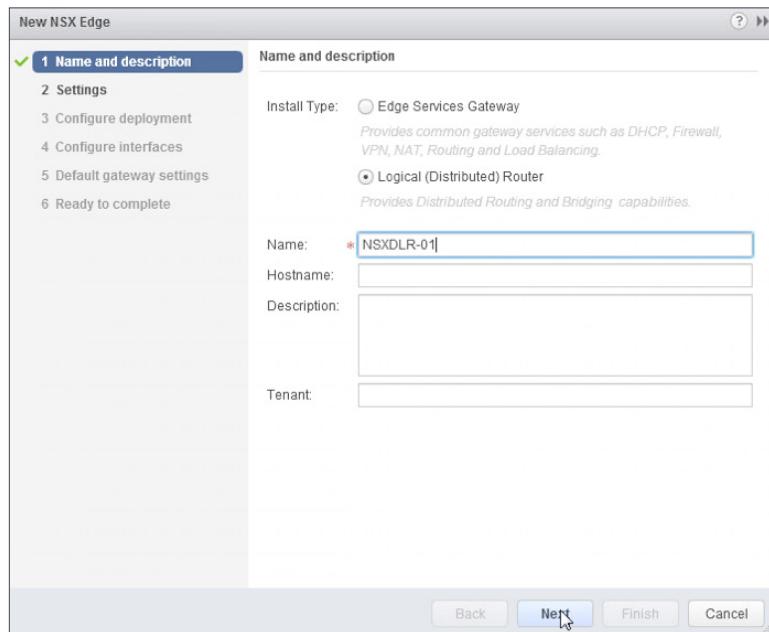
1. Return to the vSphere Web Client console and choose Networking & Security in the left column. Under Networking and Security, choose NSX Edges and then click the green plus symbol (+).



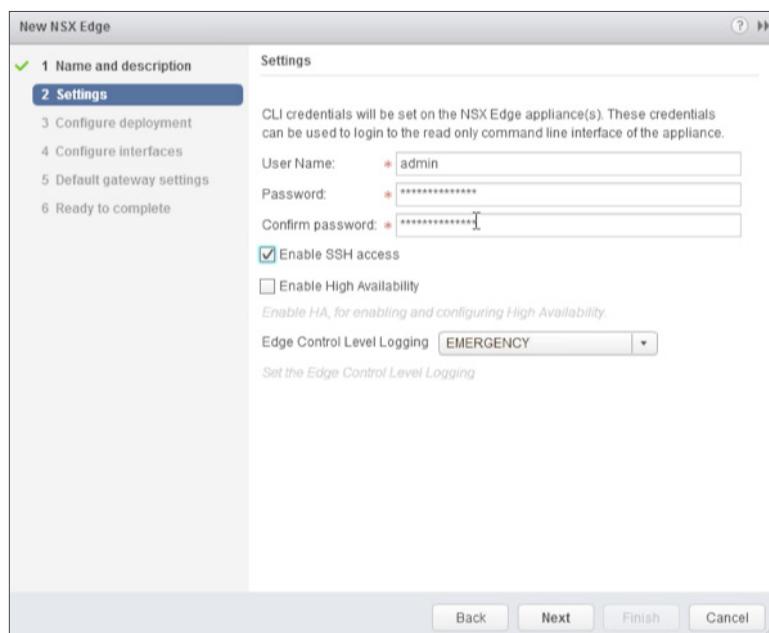
BEST PRACTICES

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

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



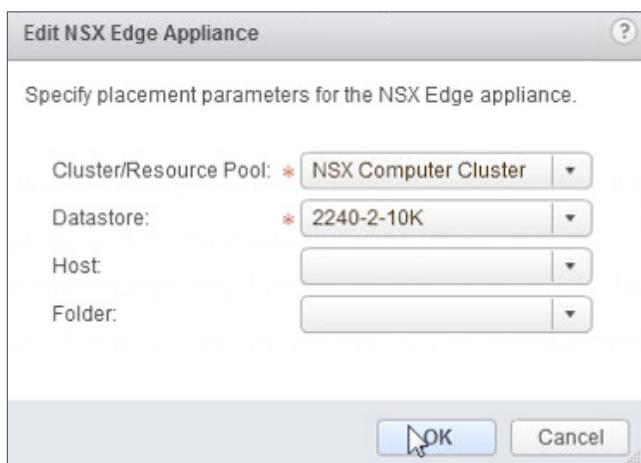
3. Under **Settings**, check the **Enable SSH access** check box and provide a username and password for the Edge Services Gateway. Click **Next** to proceed.



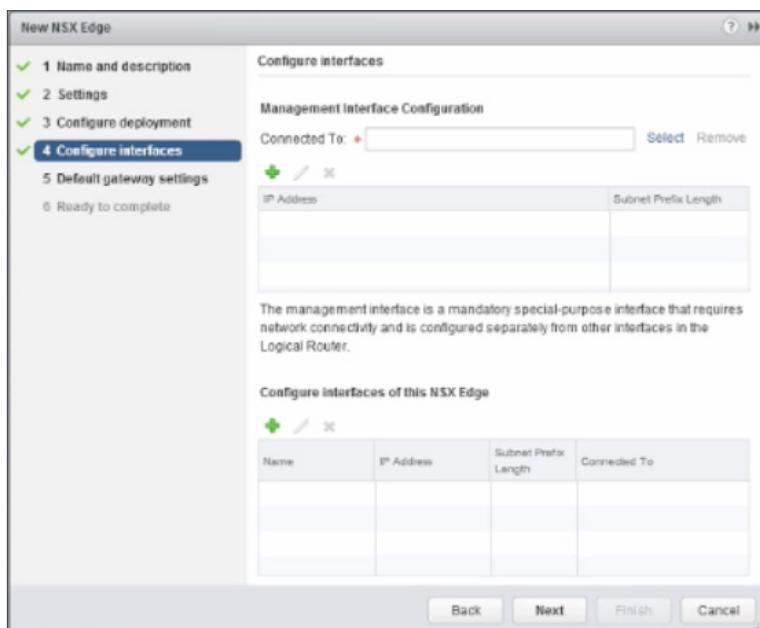
BEST PRACTICES

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

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



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

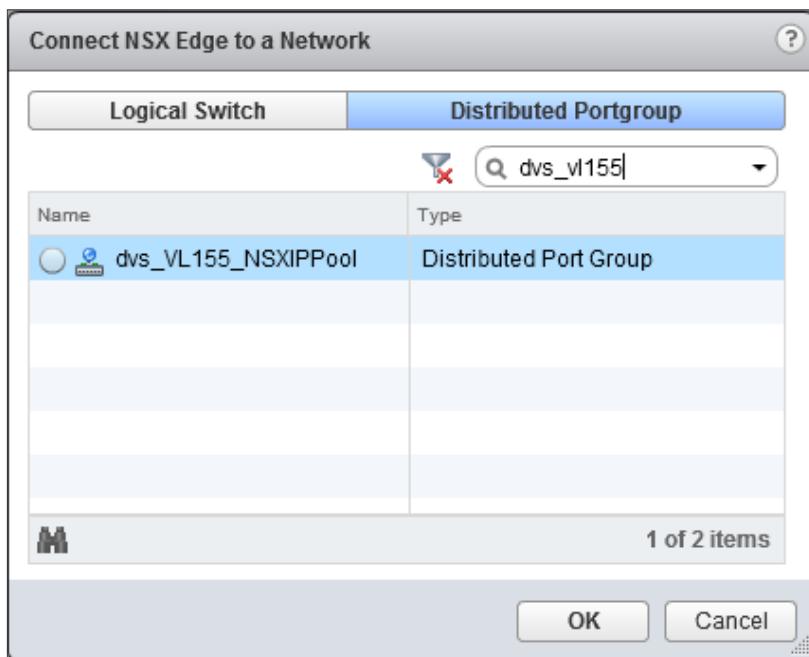


BEST PRACTICES

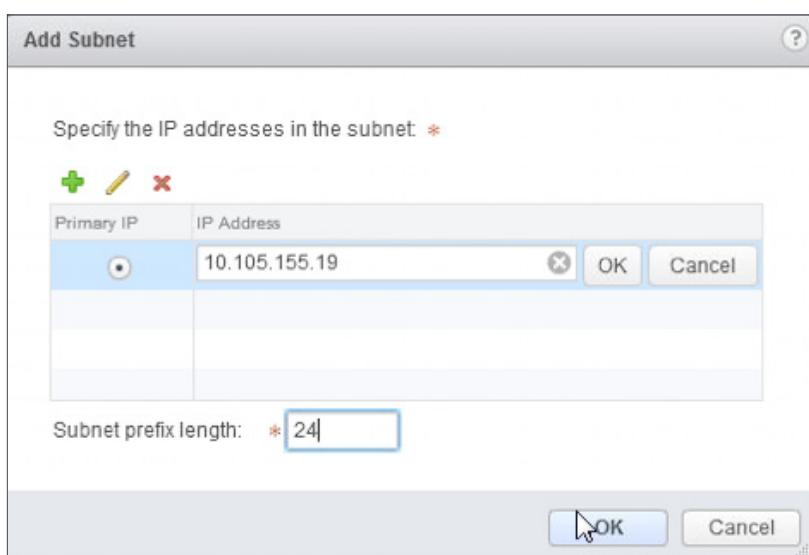
VMware NSX for vSphere (NSX-v) and F5 BIG-IP



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



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



BEST PRACTICES

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



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

Network Name	Connected To	Interface IP/Subnet Prefix
External	dvs_VL20-NSXExternal	20.20.20.2/24
Web-Tier-01	dvs_VL160-Web-Tier-01	10.0.1.1/24
App-Tier-01	dvs_VL161-App-Tier-01	10.0.2.1/24
DBTier	dvs_VL162-DB-Tier-01	10.0.3.1/24

Table 8. NSX distributed logical router network interfaces

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

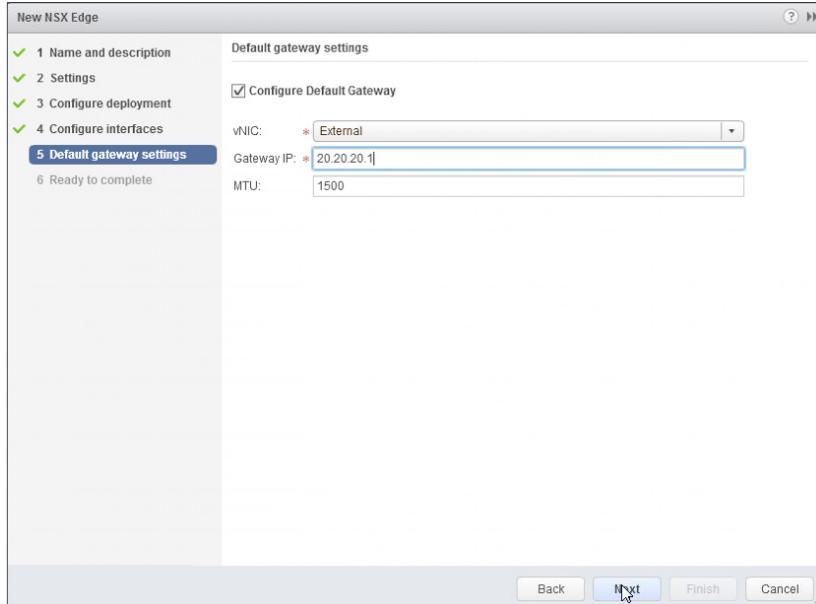
The management interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

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

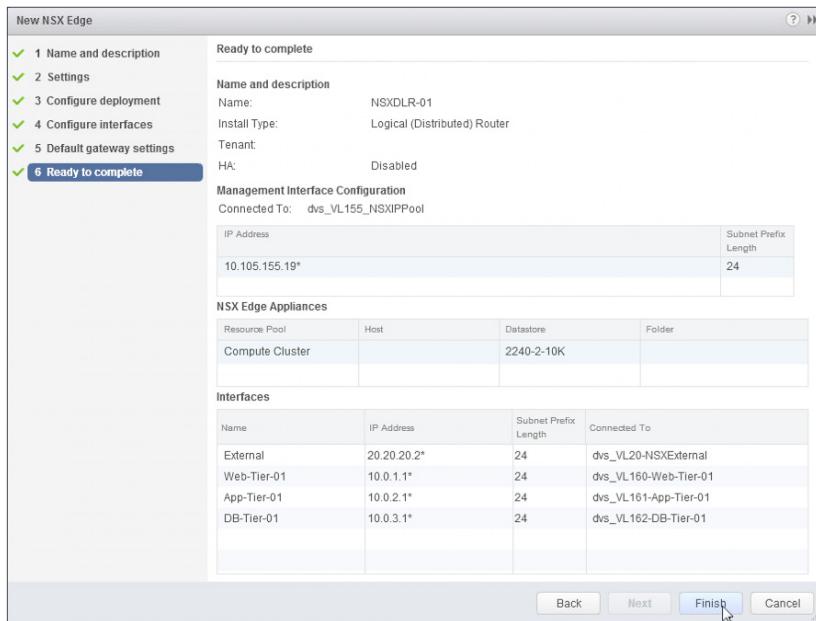


BEST PRACTICES

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



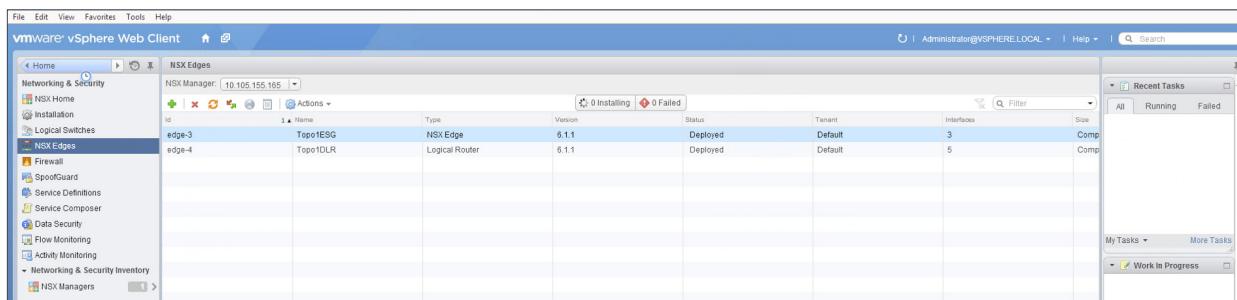
8. Review your configuration under **Ready to complete** and then click **Finish** to deploy the DLR. Depending on the number of ESXi hosts, it may take some time for the DLR deployment to complete.



BEST PRACTICES

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

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



ID	Name	Type	Version	Status	Tenant	Interface	Size
edge-3	Top+1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp
edge-4	Top+1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp

BIG-IP Appliance Configuration

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

Prerequisites

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

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



BEST PRACTICES

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, select Network and then click VLANs.
2. In the upper right corner, click the Create button.

3. Under General Properties, type a unique name for the VLAN. In this case, we used External.
4. For the Tag, enter the External VLAN ID of 20.
5. Under Resources, select Interface 1.1.
6. Select Tagged from the dropdown box and click the Add button below it.



BEST PRACTICES

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

The screenshot shows the F5 BIG-IP configuration interface. The left sidebar navigation menu includes Main, Help, About, Statistics, iApps, Local Traffic, Acceleration, Device Management, Network (with sub-options like Interfaces, Routes, Self IPs, Packet Filters, Trunks, Tunnels, Route Domains, VLANs, Class of Service, ARP, IPsec, WCCP, DNS Resolvers), and System. The 'VLANs' option under 'Network' is selected and highlighted in yellow. The main content area displays the 'New VLAN...' configuration page. The 'General Properties' section contains fields for Name (External), Description (empty), and Tag (20). The 'Resources' section shows an interface mapping for '1.1 (tagged)' with 'Interface' set to '1.2' and 'Tagging' set to 'Tagged'. The 'Configuration' section includes 'Source Check' (unchecked) and 'MTU' (1500). The 'sFlow' section has 'Polling Interval' and 'Sampling Rate' both set to 'Default' with their respective default values. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

7. Click Repeat to continue.
8. Proceed with creating the web tier network. Under General Properties, type a unique name for the VLAN. In this case, we used Web-Tier.
9. For the Tag, enter the TransitNet-1 VLAN ID of 160.
10. Under Resources, select Interface 1.1.
11. Select Tagged from the dropdown box and click the Add button below it.
12. Click Repeat and return to step 8 for VLAN 161 App-Tier to complete the VLAN creation. Click Finished to proceed.
13. Validate the VLAN configuration against the image below.

BEST PRACTICES

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

<input checked="" type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	External		20		1.1	Common
<input type="checkbox"/>	Web-Tier		160		1.1	Common
<input type="checkbox"/>	App-Tier		161		1.1	Common

[Create...](#)

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



BEST PRACTICES

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

The screenshot shows the F5 BIG-IP Configuration interface. The top bar includes File, Edit, View, Favorites, Tools, and Help. The status bar shows Hostname: bd5000.bd.f5.com, Date: Feb 19, 2015, User: admin, IP Address: 10.105.155.17, Time: 2:16 PM (PST), Role: Administrator. The navigation bar on the left lists Main, Help, About, Statistics, iApp, Local Traffic, Acceleration, Device Management, Network (selected), Interfaces, Routes, Self IPs (highlighted), and Port Filters. The main content area shows a 'Loading...' message and 'Receiving configuration data from your device.' Below this, the 'Network > Self IPs > New Self IP...' dialog is open. The 'Configuration' section contains fields for Name (ExtSelfIP), IP Address (20.20.20.10), Netmask (255.255.255.0), VLAN / Tunnel (External), Port Lockdown (Allow None), and Traffic Group (traffic-group-local-only (non-floating)). A checkbox for 'Inherit traffic group from current partition / path' is unchecked. At the bottom of the dialog are Cancel, Repeat, and Finished buttons.

9. Complete the configuration for the WebSelf self IP using the following settings:
 - a. Name: WebSelf
 - b. IP Address: 10.0.1.2
 - c. Netmask: 255.255.255.0
 - d. VLAN/Tunnel: Web-Tier
10. Click the **Repeat** button to continue.



BEST PRACTICES

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

The screenshot shows the F5 Management Interface. The top bar displays the hostname bd5000.bd.f5.com, date Mar 18, 2015, time 3:19 PM (PDT), user admin, and role Administrator. The status is ONLINE (ACTIVE) Standalone. The left sidebar has links for Main, Help, About, Statistics, iApp, Local Traffic, Acceleration, Device Management, Network (selected), Interfaces, and Routes. The main panel title is Network > Self IPs > New Self IP... . The Configuration section contains the following fields:

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

At the bottom are buttons for Cancel, Repeat, and Finished.

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

- a. Name: AppSelf
- b. IP Address: 10.0.2.2
- c. Netmask: 255.255.255.0
- d. VLAN/Tunnel: App-Tier

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

The screenshot shows the F5 Management Interface with the title Network > Self IPs. The left sidebar has links for Self IP List and Create.... The main panel title is Network > Self IPs. The table lists the following self IP configurations:

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	AppSelf		10.0.2.2	255.255.255.0	App-Tier	traffic-group-local-only	Common
<input type="checkbox"/>	ExtSelfIP		20.20.20.10	255.255.255.0	External	traffic-group-local-only	Common
<input type="checkbox"/>	WebSelf		10.0.1.2	255.255.255.0	Web-Tier	traffic-group-local-only	Common

At the bottom are buttons for Delete... and Create....

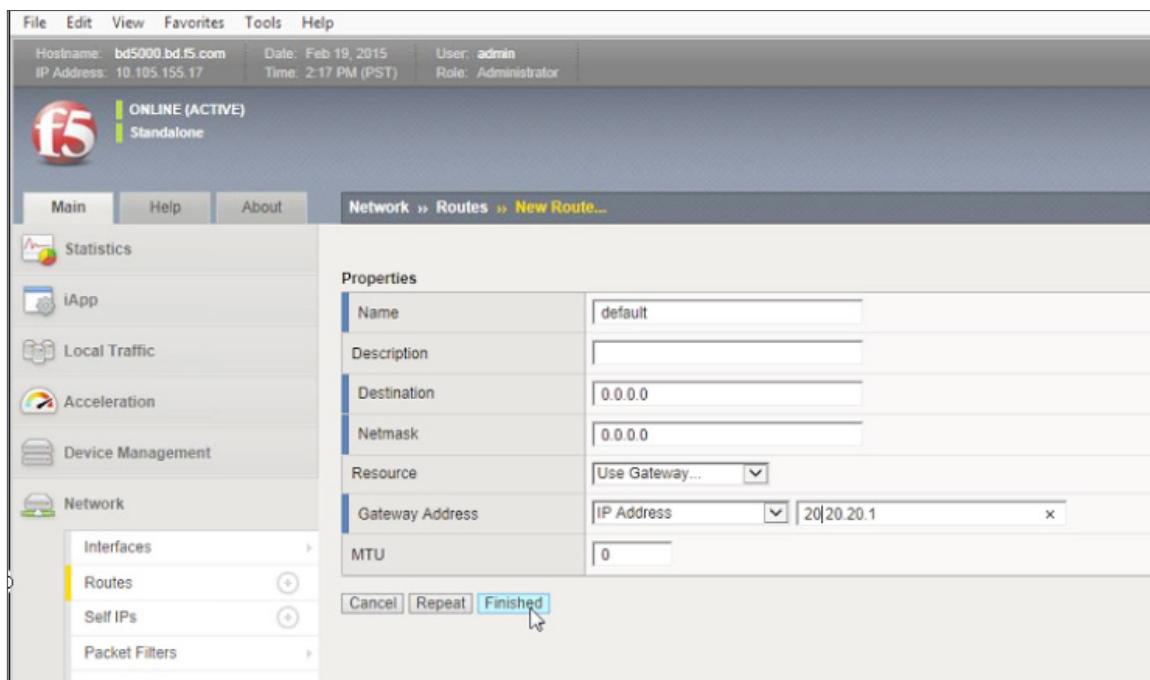
BEST PRACTICES

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

Configure a Default Static Route

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

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



BEST PRACTICES

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



The completed routing configuration should resemble the configuration below.

Network >> Routes							
Route List							
<input checked="" type="checkbox"/>	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource
<input type="checkbox"/>	default	Default IPv4	Partition Default Route Domain	Gateway	20.20.20.1	Common	
Delete...							

Application Configuration

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

Create application pools

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

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

BEST PRACTICES

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

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

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

Table 9. BIG-IP web tier pool members

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



BEST PRACTICES

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

9. Under **Health Monitors**, select an appropriate monitor for your application. In this case we are choosing a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.
10. Under **Resources**, select a **Load Balancing Method**. For basic load balancing in this validation, Round Robin was used.
11. Under **Resources**, use the **New Members** setting to add the IP address and port of the web servers (refer to Table 10). Click the **Add** button for each pool member.
12. Click **Finished** to complete the pool creation.

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

Table 10. BIG-IP application tier pool members

The screenshot shows the F5 BIG-IP Local Traffic interface. The top bar displays the hostname (bd5000.bd.f5.com), date (Feb 19, 2015), and user (admin). The main window is titled "Local Traffic > Pools : Pool List > New Pool...". The "Configuration" dropdown is set to "Basic". The "Name" field contains "AppServerPool". In the "Health Monitors" section, "https_head_15_inband_gateway_icmp" is selected. The "Resources" section shows "Load Balancing Method" set to "Round Robin" and "Priority Group Activation" set to "Disabled". Under "New Members", two members are listed: "10.0.2.11:80" and "10.0.2.12:80". The "Add" button is visible below the member list. At the bottom of the window, there are "Cancel", "Repeat", and "Finished" buttons, with "Finished" being the active button.

BEST PRACTICES

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



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.

A screenshot of the F5 BIG-IP Local Traffic > Pools : Pool List interface. The screen shows a table with two rows: AppServerPool and WebServerPool. Both rows have a green status circle, indicating they are healthy. The AppServerPool row has 2 members and is associated with the Common partition. The WebServerPool row also has 2 members and is associated with the Common partition. There are buttons for 'Create...', 'Delete...', and a search bar at the top.

Create application virtual server

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

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



BEST PRACTICES

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

Screenshot of the F5 BIG-IP Local Traffic interface showing the configuration of a new Virtual Server.

General Properties:

- Name: Web-Vip
- Description: (empty)
- Type: Standard
- Source: (empty)
- Destination:
 - Type: Host (radio button selected)
 - Address: 20.20.20.5
- Service Port: 80 (HTTP)
- State: Enabled

Content Rewrite:

- Rewrite Profile: None
- HTML Profile: None

Acceleration:

- Rate Class: None
- OneConnect Profile: None
- NTLM Conn Pool: None
- HTTP Compression Profile: None
- Web Acceleration Profile: None
- SPDY Profile: None

Resources:

- iRules:
 - Enabled: (empty)
 - Available: _sys_auth_krbdelegate, _sys_auth_ssl_oc_idap, _sys_auth_ssl_crlip, _sys_auth_ssl_ocsp, _sys_https_redirect
- Policies:
 - Enabled: (empty)
 - Available: /Common/sys_CEC_video_policy
- Default Pool: WebServerPool
- Default Persistence Profile: None
- Fallback Persistence Profile: None

Buttons at the bottom: Cancel, Repeat, Finished.

BEST PRACTICES

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

The image has been cropped to highlight the specific configuration.

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

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

Local Traffic > Virtual Servers : Virtual Server List						
		Virtual Server List		Virtual Address List		Statistics
*	Search		Create...			
<input checked="" type="checkbox"/>	Status	▲ Name	Application	Destination	Service Port	Type
<input type="checkbox"/>	●	App-Vip	10.0.1.5	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>	●	Web-Vip	20.20.20.5	80 (HTTP)	Standard	Edit...

[Enable](#) [Disable](#) [Delete...](#)

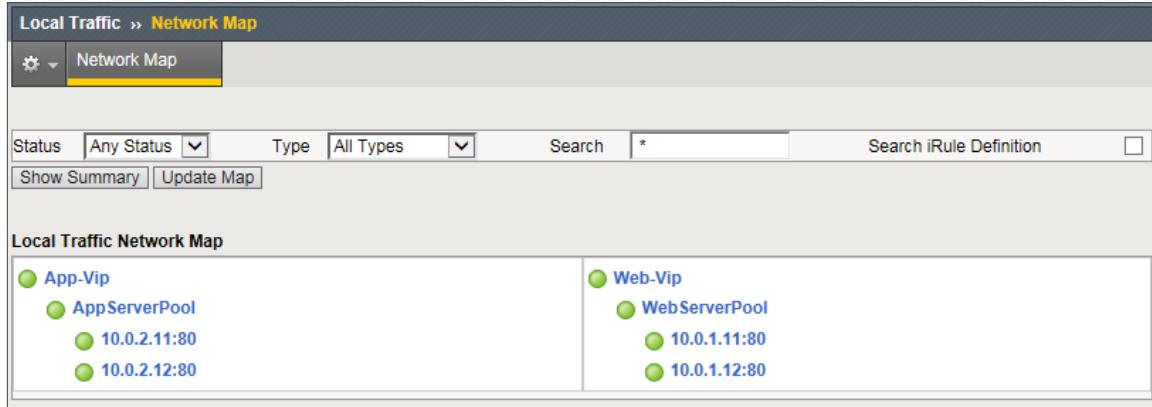
Validation

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

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

BEST PRACTICES

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



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



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

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

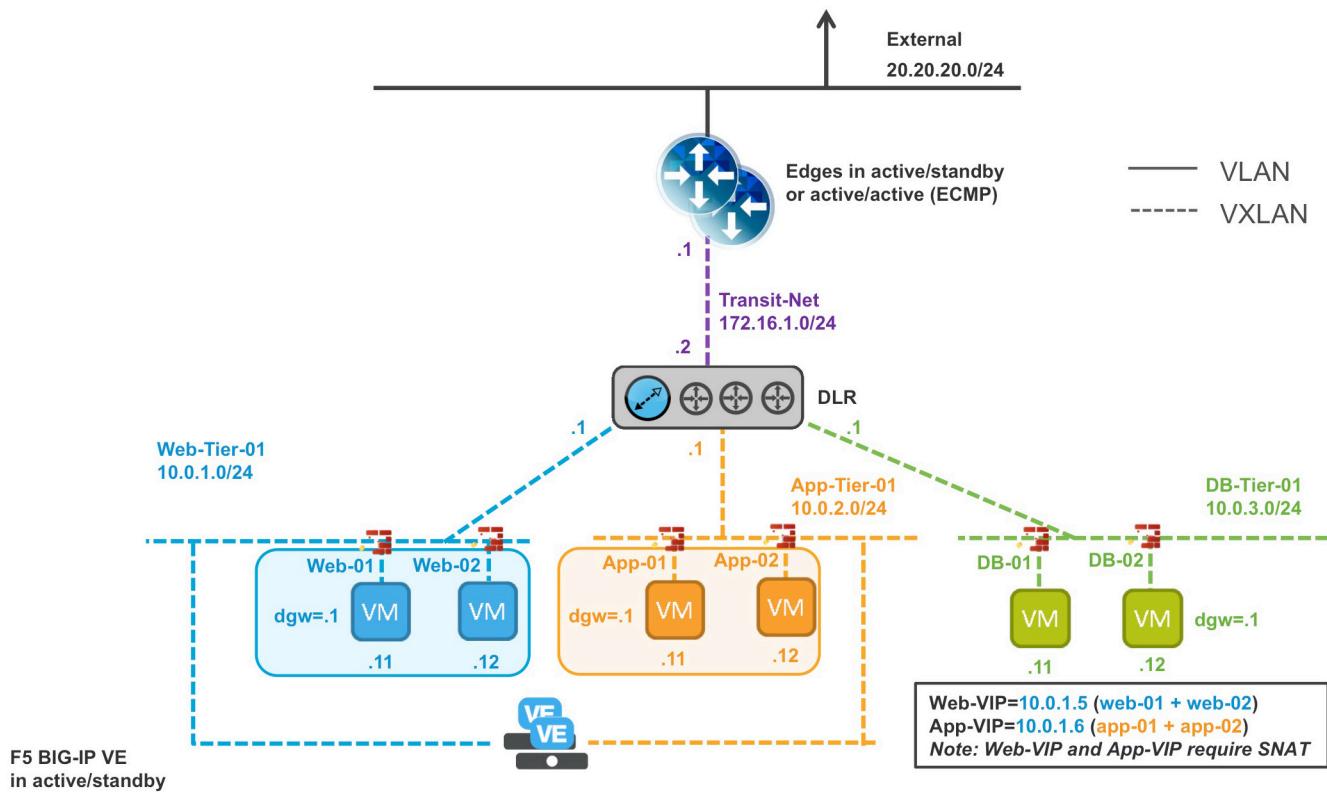


Figure 8. BIG-IP Virtual Edition in one-arm topology within VXLAN environment

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

BEST PRACTICES

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

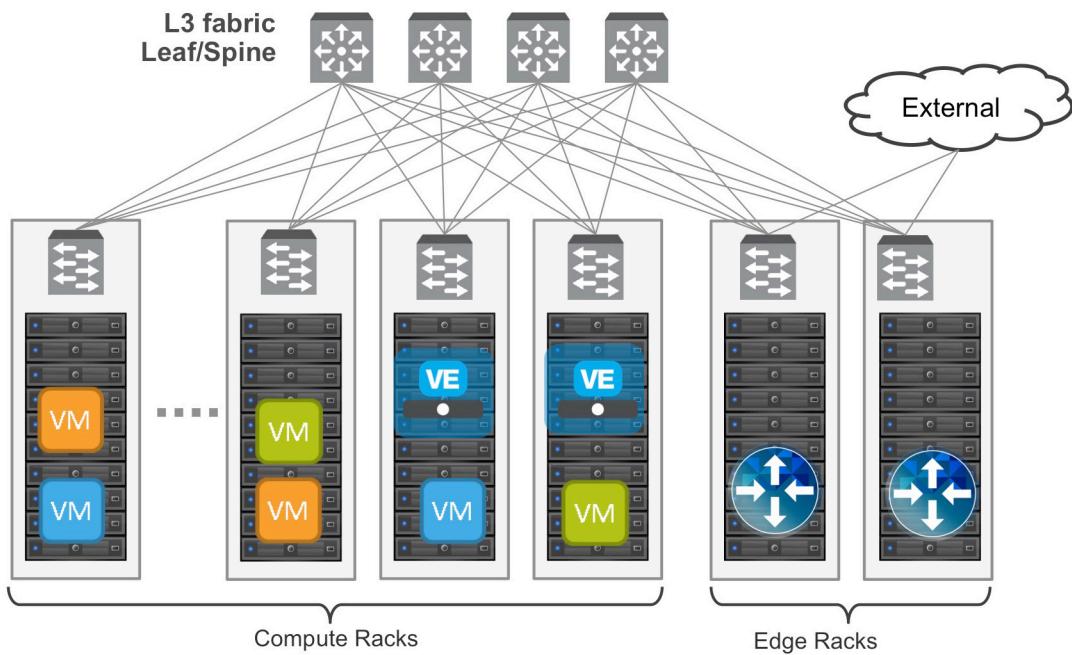


Figure 9. add caption

Implementation Infrastructure

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

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

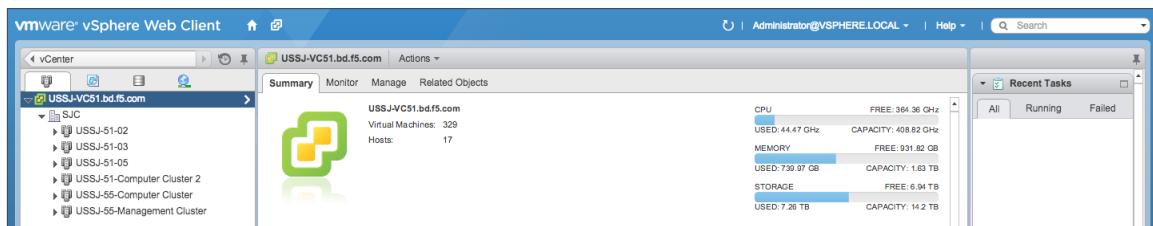


Figure 10. vSphere console



BEST PRACTICES

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

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

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

Prerequisites

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

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

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

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

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



BEST PRACTICES

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

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

Table 12. Logical switch configuration

Network Segments

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

802.1Q VLAN segments

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

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

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

VXLAN segments

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

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

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

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

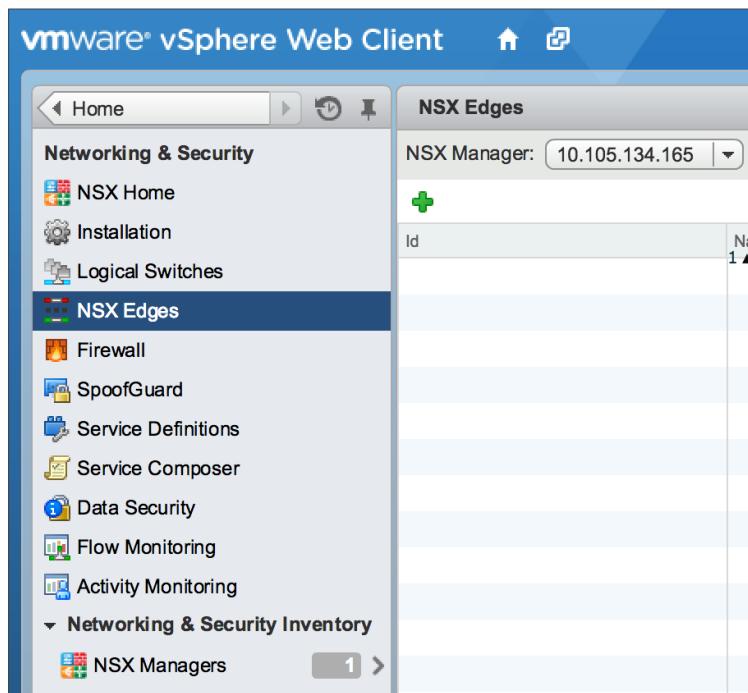
VXLAN 5013 TransitNet-1 is the VXLAN Segment ID used for the transport zone between the DLR and the NSX Edge.

BEST PRACTICES

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

NSX Edge Configuration

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



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



BEST PRACTICES

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

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Name and description

Install Type: Edge Services Gateway
Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.
 Logical (Distributed) Router
Provides Distributed Routing and Bridging capabilities.

Name: * NSXEdge

Hostname:

Description:

Tenant:

Back Next Finish Cancel

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

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Firewall and HA

7 Ready to complete

Settings

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

User Name: * admin

Password: * ****

Confirm password: * ****

Enable SSH access

Enable High Availability
Enable HA, for enabling and configuring High Availability.

Enable auto rule generation
Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.

Edge Control Level Logging: EMERGENCY

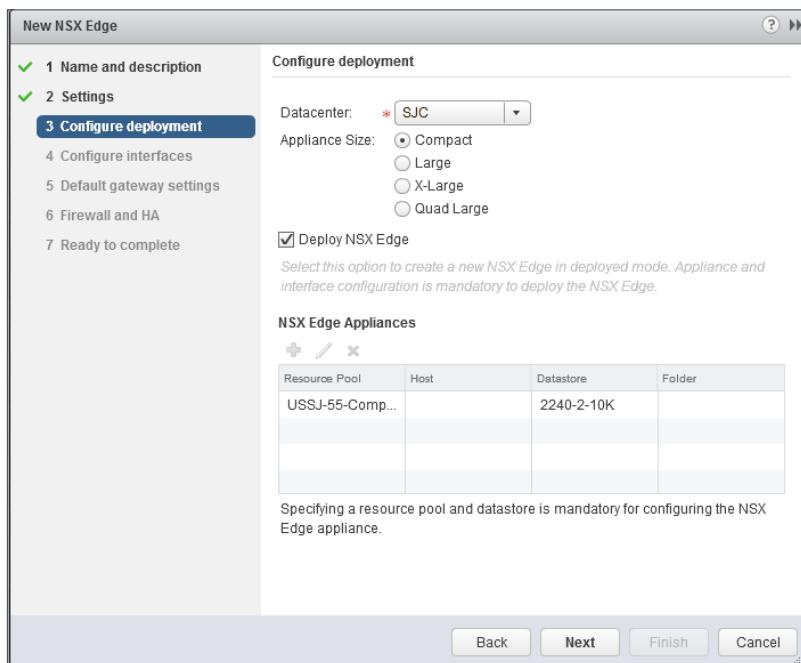
Set the Edge Control Level Logging

Back Next Finish Cancel

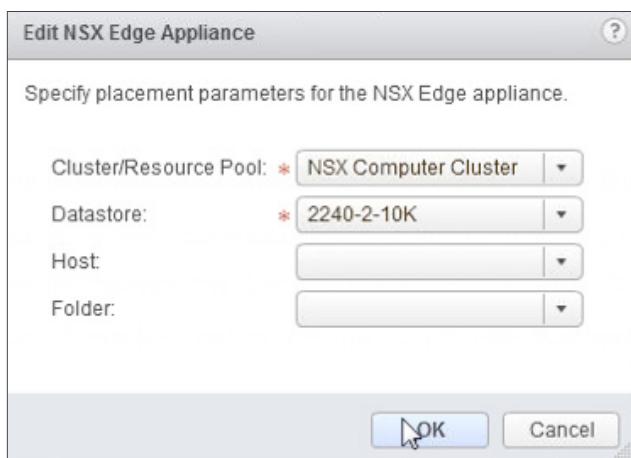
BEST PRACTICES

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

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



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



BEST PRACTICES

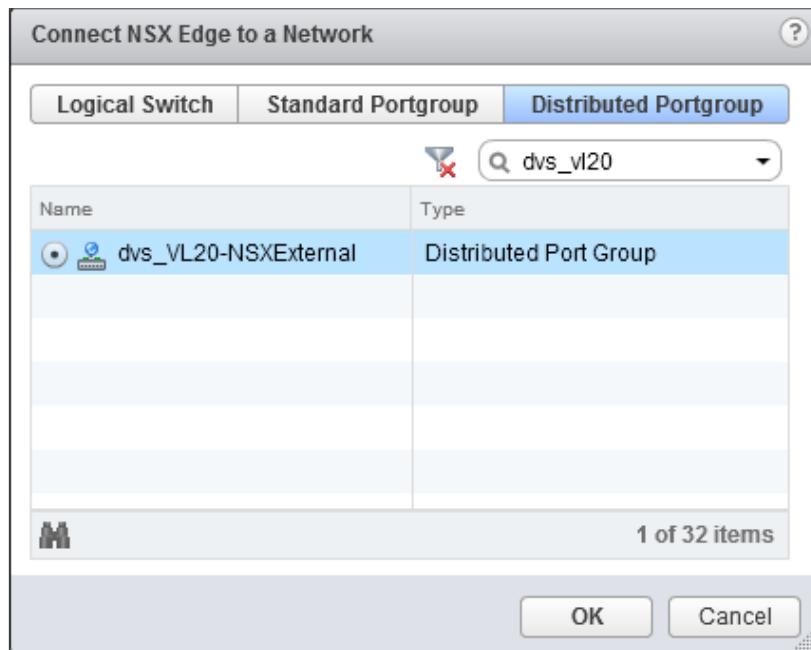
VMware NSX for vSphere (NSX-v) and F5 BIG-IP



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

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

Table 13. NSX Edge network interfaces



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

BEST PRACTICES

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



Add Subnet

Specify the IP addresses in the subnet: *

Primary IP	IP Address
<input checked="" type="radio"/>	17.16.1.1

Subnet prefix length: * 24

OK Cancel

This screenshot shows the 'Add Subnet' dialog box. It displays a table for entering primary IP addresses and a field for the subnet prefix length. The primary IP is set to 17.16.1.1 and the prefix length is 24.

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

New NSX Edge

1 Name and description 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Firewall and HA 7 Ready to complete

Default gateway settings

Configure Default Gateway

vNIC: * External

Gateway IP: * 20.20.20.1

MTU: 1500

Back Next Finish Cancel

This screenshot shows the 'New NSX Edge' configuration wizard at step 5: Default gateway settings. It shows the configuration of the default gateway with the vNIC set to 'External' and the gateway IP set to 20.20.20.1.



BEST PRACTICES

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

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

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Firewall and HA

Configure Firewall default policy

Default Traffic Policy: Accept Deny

Logging: Enable Disable

Configure HA parameters
Configuring HA parameters is mandatory for HA to work.

vNIC: *

Declare Dead Time: (seconds)

Management IPs:

You can specify pair of IPs (in CIDR format) with /30 subnet. Management IPs must not overlap with any vnic subnets.

Back Next Finish Cancel

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

New NSX Edge

1 Name and description
2 Settings
3 Configure deployment
4 Configure interfaces
5 Default gateway settings
6 Firewall and HA
7 Ready to complete

Ready to complete

Name and description
Name: NSXEdge
Install Type: Edge Services Gateway
Tenant:
Size: Compact
HA: Disabled
Automatic Rule Generation: Enabled

NSX Edge Appliances

Resource Pool	Host	Datastore	Folder
USSJ-55-Computer Cluster		2240-2-10K	

Interfaces

vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
0	External	20.20.20.2*	24	dvs_VL20-NSXExternal
1	TransitNet1	172.16.1.1*	24	TransitNet-1

Back Next Finish Cancel

BEST PRACTICES

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



Create and Deploy DLR

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

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

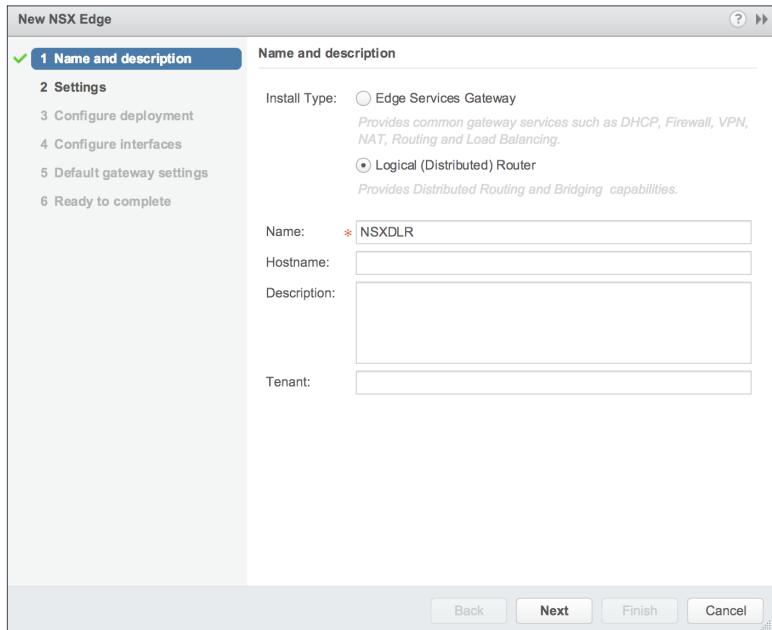
1. Return to the vSphere Web Client console and choose Networking & Security in the left column, then choose NSX Edges and click the green plus symbol (+).

A screenshot of the vSphere Web Client interface. The title bar says "vmware® vSphere Web Client". The left sidebar has a "Networking & Security" section with various icons and links: NSX Home, Installation, Logical Switches, NSX Edges (which is selected and highlighted in blue), Firewall, SpoofGuard, Service Definitions, Service Composer, Data Security, Flow Monitoring, Activity Monitoring, and NSX Managers. Below the sidebar, there's a small table with one row: "Id" and "Name" (with the value "1"). A green plus sign icon is located above the table, indicating the option to add a new entry.

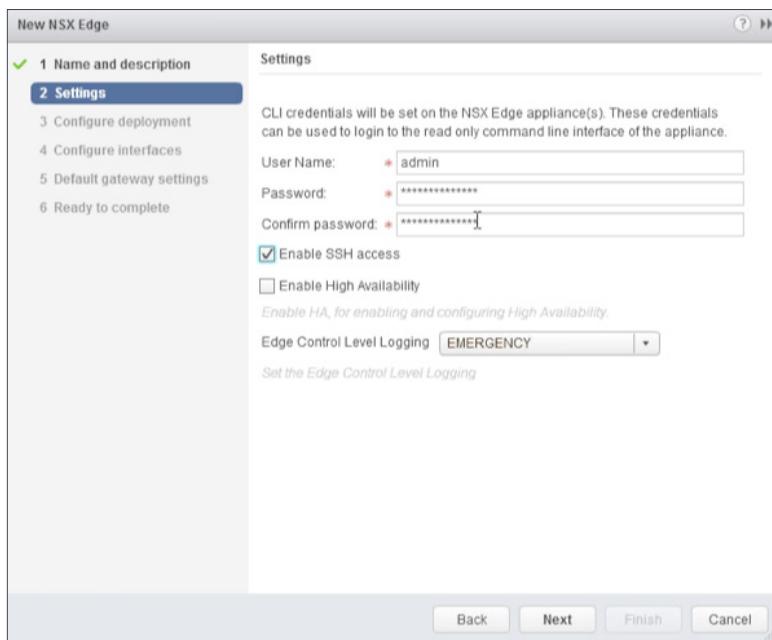
BEST PRACTICES

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

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



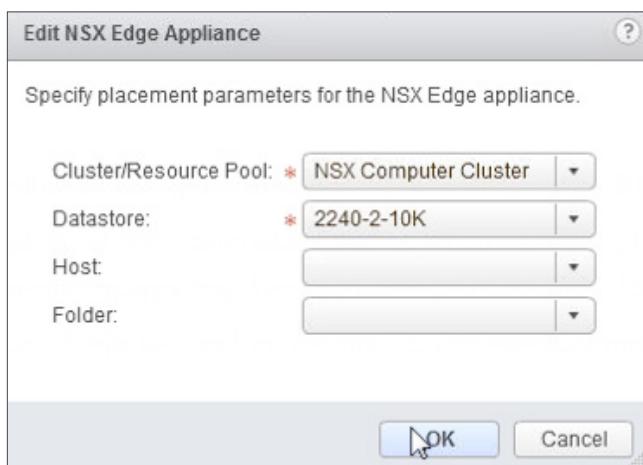
3. Under **Settings**, select **Enable SSH access** and provide a username and password for the Edge Services Gateway. Select **Next**.



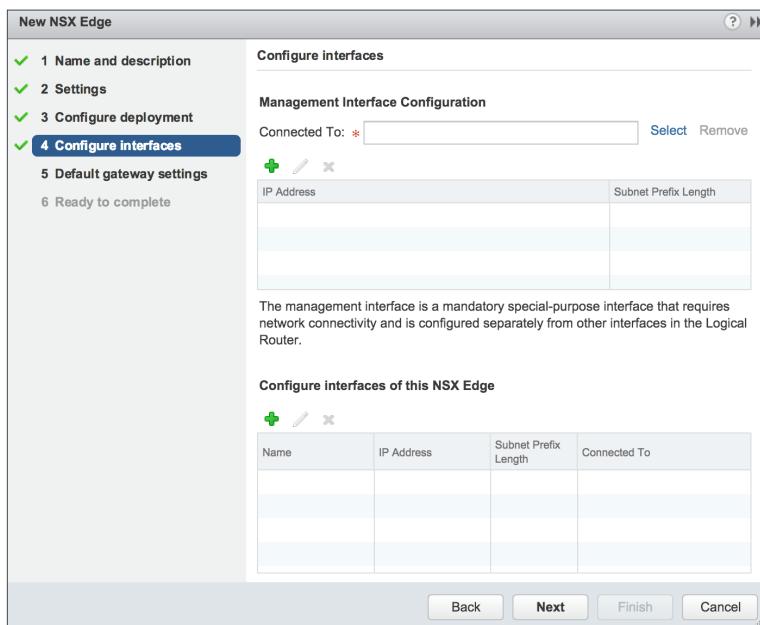
BEST PRACTICES

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

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



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

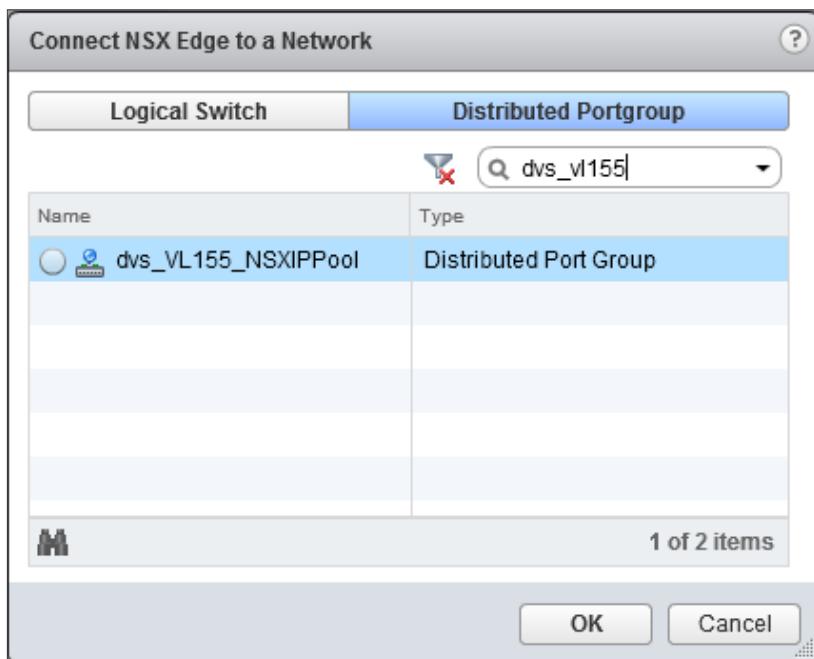


BEST PRACTICES

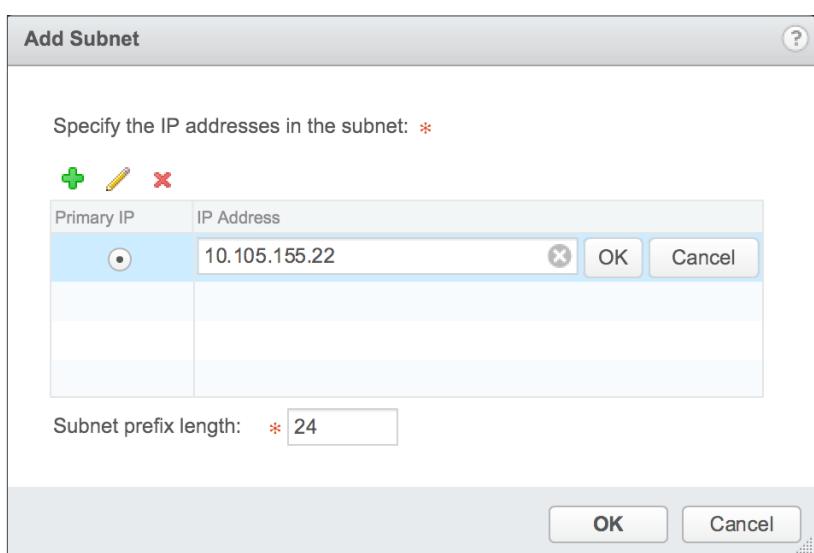
VMware NSX for vSphere (NSX-v) and F5 BIG-IP



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



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



BEST PRACTICES

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

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

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

Table 14. NSX distributed logical router Network interfaces

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

New NSX Edge

Configure interfaces

Management Interface Configuration

Connected To: * dvs_VL155_NSXIPPool Change Remove

IP Address	Subnet Prefix Length
10.105.155.22*	24

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

Configure interfaces of this NSX Edge

Name	IP Address	Subnet Prefix Length	Connected To
TransitNet	172.16.1.2*	24	TransitNet-1
Web-Tier-01	10.0.1.1*	24	Web-Tier-01
App-Tier-01	10.0.2.1*	24	App-Tier-01
DB-Tier-01	10.0.3.1*	24	DB-Tier-01

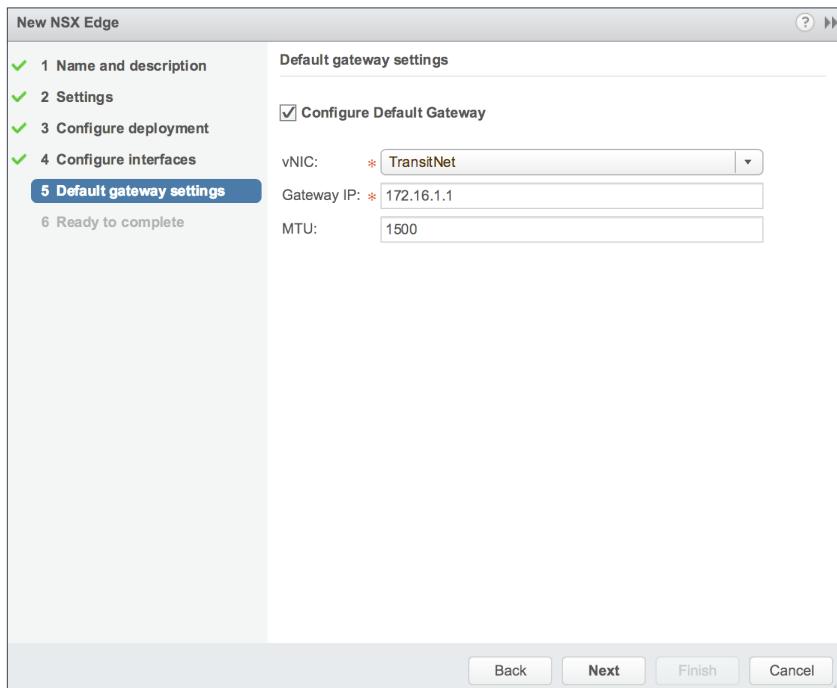
Back Next Finish Cancel

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

BEST PRACTICES

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

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



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

BEST PRACTICES

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

New NSX Edge

<input checked="" type="checkbox"/> 1 Name and description	Ready to complete																																		
<input checked="" type="checkbox"/> 2 Settings																																			
<input checked="" type="checkbox"/> 3 Configure deployment																																			
<input checked="" type="checkbox"/> 4 Configure interfaces																																			
<input checked="" type="checkbox"/> 5 Default gateway settings																																			
<input checked="" type="checkbox"/> 6 Ready to complete																																			
Name and description Name: NSXDLR Install Type: Logical (Distributed) Router Tenant: HA: Disabled Management Interface Configuration Connected To: dvs_VL155_NSXIPPool <table border="1"> <tr> <th>IP Address</th> <th>Subnet Prefix Length</th> </tr> <tr> <td>10.105.155.22*</td> <td>24</td> </tr> </table> NSX Edge Appliances <table border="1"> <thead> <tr> <th>Resource Pool</th> <th>Host</th> <th>Datastore</th> <th>Folder</th> </tr> </thead> <tbody> <tr> <td>USSJ-55-Compu</td> <td></td> <td>2240-2-10K</td> <td></td> </tr> </tbody> </table> Interfaces <table border="1"> <thead> <tr> <th>Name</th> <th>IP Address</th> <th>Subnet Prefix Length</th> <th>Connected To</th> </tr> </thead> <tbody> <tr> <td>TransitNet</td> <td>172.16.1.2*</td> <td>24</td> <td>TransitNet-1</td> </tr> <tr> <td>Web-Tier-01</td> <td>10.0.1.1*</td> <td>24</td> <td>Web-Tier-01</td> </tr> <tr> <td>App-Tier-01</td> <td>10.0.2.1*</td> <td>24</td> <td>App-Tier-01</td> </tr> <tr> <td>DB-Tier-01</td> <td>10.0.3.1*</td> <td>24</td> <td>DB-Tier-01</td> </tr> </tbody> </table>				IP Address	Subnet Prefix Length	10.105.155.22*	24	Resource Pool	Host	Datastore	Folder	USSJ-55-Compu		2240-2-10K		Name	IP Address	Subnet Prefix Length	Connected To	TransitNet	172.16.1.2*	24	TransitNet-1	Web-Tier-01	10.0.1.1*	24	Web-Tier-01	App-Tier-01	10.0.2.1*	24	App-Tier-01	DB-Tier-01	10.0.3.1*	24	DB-Tier-01
IP Address	Subnet Prefix Length																																		
10.105.155.22*	24																																		
Resource Pool	Host	Datastore	Folder																																
USSJ-55-Compu		2240-2-10K																																	
Name	IP Address	Subnet Prefix Length	Connected To																																
TransitNet	172.16.1.2*	24	TransitNet-1																																
Web-Tier-01	10.0.1.1*	24	Web-Tier-01																																
App-Tier-01	10.0.2.1*	24	App-Tier-01																																
DB-Tier-01	10.0.3.1*	24	DB-Tier-01																																
<input type="button" value="Back"/> <input type="button" value="Next"/> <input type="button" value="Finish"/> <input type="button" value="Cancel"/>																																			

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

File Edit View Favorites Tools Help

Administrator@VSPHERE.LOCAL | Help | Search

Networking & Security

NSX Manager: 10.105.155.165

NSX Edges

ID	Name	Type	Version	Status	Tenant	Interfaces	Size
edge-3	Topo1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp
edge-4	Topo1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp

Recent Tasks

All Running Failed

My Tasks More Tasks

Work In Progress

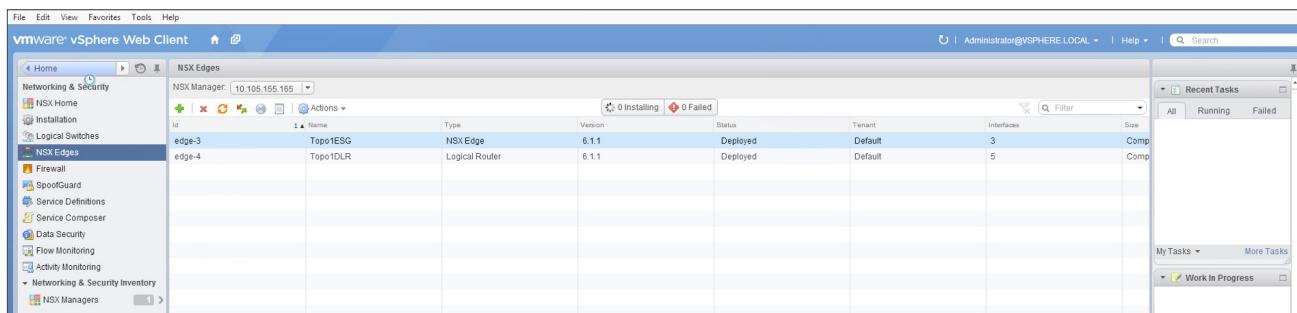
BEST PRACTICES

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

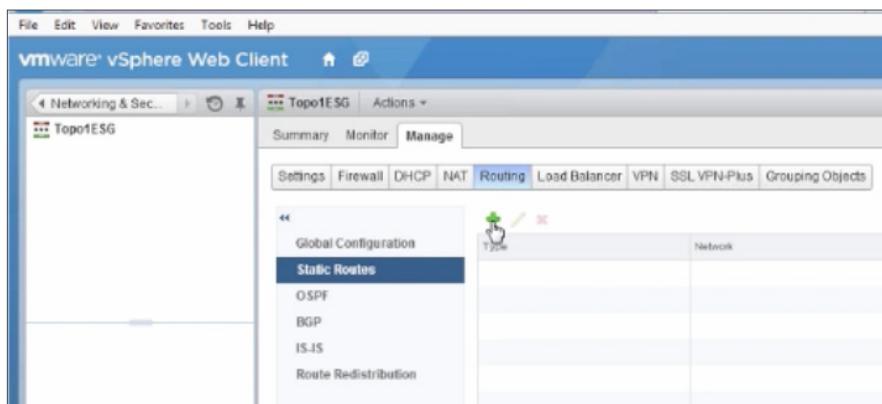
NSX Edge Static Routing Configuration

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

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



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



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



BEST PRACTICES

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

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

MTU: 1500

Description:

OK **Cancel**

- Once complete, select OK to continue.

vmware vSphere Web Client Updated at 12:11 PM | Administrator@VSPHERE.LOCAL | Help ▾

Networking & Sec... NSXEdge Actions ▾

NSXEdge Summary Monitor Manage

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

Global Configuration Static Routes OSPF BGP IS-IS Route Redistribution

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

Publish Changes **Revert**

Type	Network	Next Hop	Interface	MTU	Description
	10.0.0.0/16	172.16.1.2	TransitNet-1	1500	

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



BEST PRACTICES

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

BIG-IP Appliance Configuration

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

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

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

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

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

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

Prerequisites

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

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

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

BEST PRACTICES

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

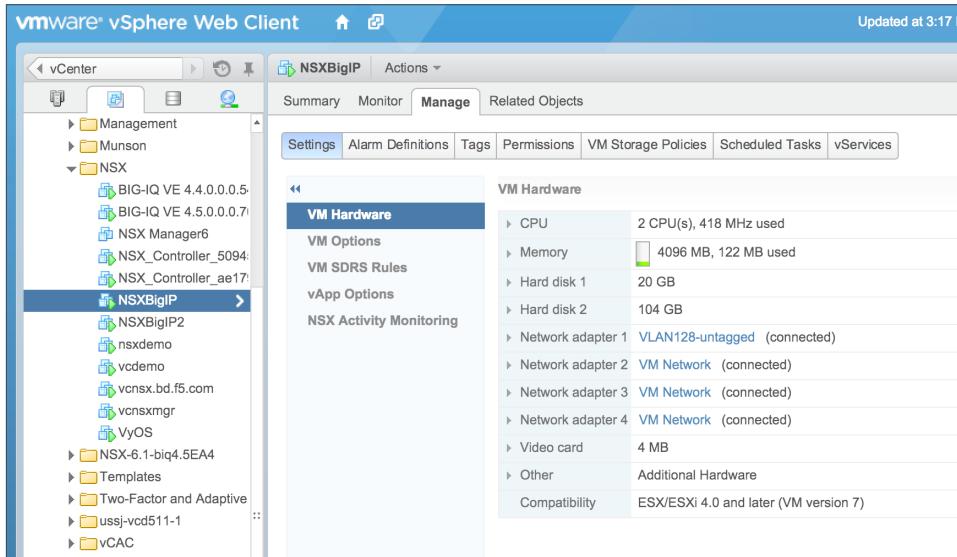
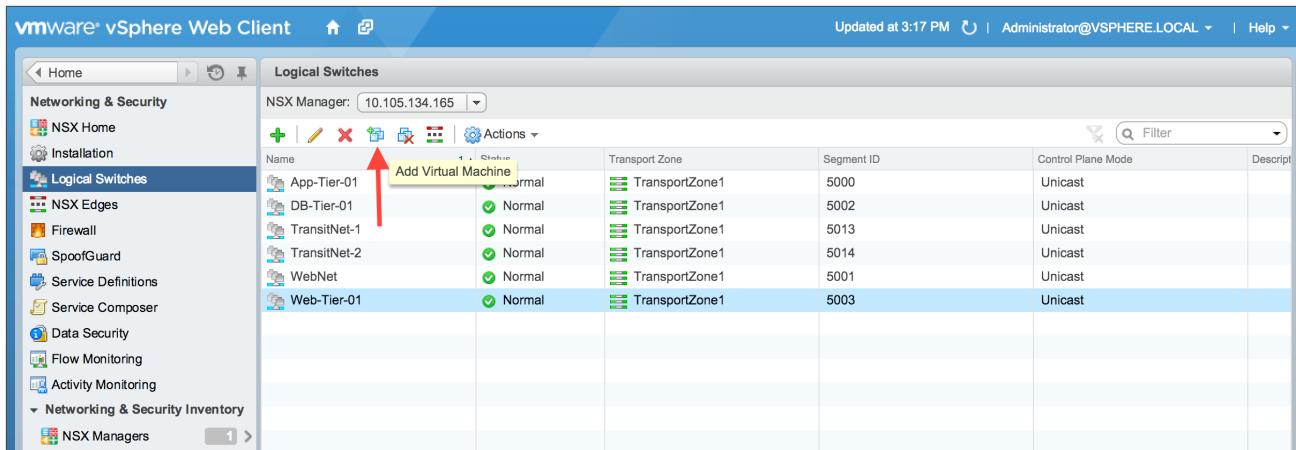


Figure 11. vSphere display of deployed BIG-IP Virtual Edition

Provision BIG-IP Network Adapters in vSphere

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

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





BEST PRACTICES

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

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

The screenshot shows the 'Web-Tier-01 - Add Virtual Machines' wizard. The current step is '1 Select Virtual Machines'. The interface includes a sidebar with steps: 1 Select Virtual Machines (highlighted in blue), 2 Select vNICs, and 3 Ready to complete. The main area is titled 'Select Virtual Machines' with the sub-instruction 'Select VMs to connect to this network'. A 'Filter' button is followed by '(2)Selected Objects'. A search bar contains the text 'nsx'. Below is a list of 'Virtual Machine' objects:

Virtual Machine
<input checked="" type="checkbox"/> NSXBigIP
<input checked="" type="checkbox"/> NSXBigIP2
<input type="checkbox"/> nsx-web-sv-01a
<input type="checkbox"/> nsx-web-sv-01b

At the bottom right of the list area, it says '4 of 96 Objects'. At the very bottom of the window are buttons: Back, Next (highlighted in blue), Finish, and Cancel.

BEST PRACTICES

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

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

Name	Network
NSXBigIP2	<input type="checkbox"/> NSXBigIP2 - Network adapter 4 (VM Network) <input type="checkbox"/> NSXBigIP2 - Network adapter 1 (VM Network) <input checked="" type="checkbox"/> NSXBigIP2 - Network adapter 2 (VM Network) <input type="checkbox"/> NSXBigIP2 - Network adapter 3 (VM Network)
NSXBigIP	<input checked="" type="checkbox"/> NSXBigIP - Network adapter 2 (VM Network) <input type="checkbox"/> NSXBigIP - Network adapter 3 (VM Network) <input type="checkbox"/> NSXBigIP - Network adapter 1 (VLAN128-untagged) <input type="checkbox"/> NSXBigIP - Network adapter 4 (VM Network)

4. For the App-Tier-01 logical switch, repeat the same steps, making sure to choose Network adapter 3.
5. In our environment we are using the VM Network PortGroup as the HANet PortGroup and leaving the Network adapter 4 associated with the VM Network PortGroup.

BEST PRACTICES

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

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

The screenshot shows the NSXBigIP management interface. The top navigation bar includes tabs for Summary, Monitor, Manage (which is selected), and Related Objects. Below this is a sub-navigation bar with tabs for Settings, Alarm Definitions, Tags, Permissions, VM Storage Policies, Scheduled Tasks, and vServices. The main content area is titled "VM Hardware" and displays the following details:

	VM Options	VM SDRS Rules	vApp Options	NSX Activity Monitoring
CPU	2 CPU(s), 0 MHz used			
Memory	4096 MB, 0 MB used			
Hard disk 1	20 GB			
Hard disk 2	104 GB			
Network adapter 1	VLAN128-untagged (connected)			
Network adapter 2	vxw-dvs-507-virtualwire-25-sid-5001-Web-Tier-01 (connected)			
Network adapter 3	vxw-dvs-507-virtualwire-26-sid-5002-App-Tier-01 (connected)			
Network adapter 4	VM Network (connected)			

Provision BIG-IP Networking

Create VLANs

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

The screenshot shows the BIG-IP Configuration Utility interface. The top header includes File, Edit, View, Favorites, Tools, Help, and a user session (User: admin, Role: Administrator). The left navigation pane has sections for Main, Help, About, Statistics, iApp, Local Traffic, Acceleration, Device Management, and Network. Under Network, the VLANs section is selected. The main content area is titled "Network > VLANs > VLAN List" and shows a table with one row: "No records to display." There are buttons for Create, Delete, and a search/filter bar at the bottom.

BEST PRACTICES

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



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

The screenshot shows the F5 BIG-IP configuration interface. At the top, there is a header bar with system information: Hostname: nsxbigip1.bd.f5.com, Date: Feb 27, 2015, IP Address: 172.30.128.16, Time: 3:52 PM (PST), User: admin, and Role: Administrator. Below the header, the status is shown as ONLINE (ACTIVE) and Standalone. The main navigation menu includes Main, Help, and About. The current page is Network > VLANs : VLAN List > New VLAN... The left sidebar has links for Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management, and Network (with sub-links for Interfaces, Routes, Self IPs, Packet Filters, Trunks, Tunnels, Route Domains, VLANs, Class of Service, ARP, and IPsec). The right panel is titled 'General Properties' and shows fields for Name (WebTier01), Description, and Tag. Under 'Resources', there is a table with columns for Interface (set to 1.2) and Tagging (set to Untagged). An 'Add' button is present, and the 'Interfaces' field contains '1.1 (untagged)'. Below this table are 'Edit' and 'Delete' buttons. The 'Configuration' section includes Source Check (unchecked) and MTU (set to 1500). The 'sFlow' section includes Polling Interval (Default, Default Value: 10 seconds) and Sampling Rate (Default, Default Value: 2048 seconds). At the bottom of the right panel are 'Cancel', 'Repeat', and 'Finished' buttons.

BEST PRACTICES

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

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

Network » VLANs : VLAN List						
	VLAN List	VLAN Groups				
	Name		Application	Tag	Untagged Interfaces	Tagged Interfaces
<input type="checkbox"/>	AppTier01		4093	1.2		Common
<input type="checkbox"/>	HANet		4092	1.3		Common
<input type="checkbox"/>	WebTier01		4094	1.1		Common

Repeat steps 1-13 to create the VLANs on the second appliance, NSXBIGIP2.

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

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

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

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

BEST PRACTICES

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

ONLINE (ACTIVE)
Standalone

Main Help About

Statistics Statistics » Welcome

Setup

User Documentation
Technical documentation for this product, including user guides and release notes, is available on the Ask F5 Technical Support web site.

- User Documentation

Preferences
On the System Preferences screen, you can customize the general preferences for the Configuration Utility.

- System Preferences

Additional Setup Options
Use the following additional configuration options to refine the system setup, once you have initially configured the system using the Setup Utility.

- System Device Certificate
- DNS
- NTP
- SNMP
- User Authentication

Setup Utility
Run the Setup Utility again to make changes to basic device settings and standard network configuration.

- Run the Setup Utility
- Run Config Sync/HA Utility

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

Hostname: nsxbigip1.bd.f5.com Date: Feb 27, 2015 User: admin
IP Address: 172.30.128.16 Time: 4:04 PM (PST) Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About

Statistics

Redundant Device Wizard Options

Config Sync	<input checked="" type="checkbox"/> Display configuration synchronization options
High Availability	<input checked="" type="checkbox"/> Display failover and mirroring options Failover Method: Network

Cancel Next...

BEST PRACTICES

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

4. Under Internal Network Configuration, choose the following settings

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

5. Click **Next** to continue.

Hostname: nsxbigip1.bd.f5.com Date: Feb 27, 2015
IP Address: 172.30.128.16 Time: 4:05 PM (PST) User: admin
Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About

Internal Network Configuration

Internal VLAN	<input type="radio"/> Create VLAN internal <input checked="" type="radio"/> Select existing VLAN
Select VLAN	WebTier01
Self IP	Address: 10.0.1.8 Netmask: 255.255.255.0 Port Lockdown: Allow Default
Floating IP	Address: 10.0.1.13 Port Lockdown: Allow Default

Internal VLAN Configuration

VLAN Name	WebTier01
VLAN Tag ID	4094
VLAN Interfaces	1.2
Tagging:	Select...
Add	
Interfaces	1.1 (untagged)

Cancel Next...

BEST PRACTICES

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



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

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

7. Click **Next** to continue.

Hostname: nsxbigip1.bd.f5.com Date: Feb 27, 2015
IP Address: 172.30.128.16 Time: 4:09 PM (PST) User: admin Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About

External Network Configuration

External VLAN	<input type="radio"/> Create VLAN external <input checked="" type="radio"/> Select existing VLAN
Select VLAN	AppTier01
Self IP	Address: 10.0.2.8 Netmask: 255.255.255.0 Port Lockdown: Allow None
Default Gateway	
Floating IP	Address: 10.0.2.13 Port Lockdown: Allow None

External VLAN Configuration

VLAN Name	AppTier01
VLAN Tag ID	4093
Interfaces	VLAN Interfaces: 1.1 Tagging: Select... Add 1.2 (untagged) Edit Delete

Cancel Next...

BEST PRACTICES

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

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

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

9. Click Next to continue.

Hostname: nsxbigip1.bd.f5.com		Date: Feb 27, 2015	User: admin												
		IP Address: 172.30.128.16	Role: Administrator												
ONLINE (ACTIVE) Standalone															
<div style="background-color: #ccc; padding: 5px;"> Main Help About </div>															
<div style="border: 1px solid #ccc; padding: 10px;"> <p>High Availability Network Configuration</p> <table border="0"> <tr> <td style="width: 30%;">High Availability VLAN</td> <td><input type="radio"/> Create VLAN HA <input checked="" type="radio"/> Select existing VLAN</td> </tr> <tr> <td>Select VLAN</td> <td><input type="button" value="HANet"/></td> </tr> <tr> <td>Self IP</td> <td> Address: <input type="text" value="10.254.1.8"/> Netmask: <input type="text" value="255.255.255.0"/> </td> </tr> </table> </div>				High Availability VLAN	<input type="radio"/> Create VLAN HA <input checked="" type="radio"/> Select existing VLAN	Select VLAN	<input type="button" value="HANet"/>	Self IP	Address: <input type="text" value="10.254.1.8"/> Netmask: <input type="text" value="255.255.255.0"/>						
High Availability VLAN	<input type="radio"/> Create VLAN HA <input checked="" type="radio"/> Select existing VLAN														
Select VLAN	<input type="button" value="HANet"/>														
Self IP	Address: <input type="text" value="10.254.1.8"/> Netmask: <input type="text" value="255.255.255.0"/>														
<div style="border: 1px solid #ccc; padding: 10px;"> <p>High Availability VLAN Configuration</p> <table border="0"> <tr> <td>VLAN Name</td> <td>HANet</td> </tr> <tr> <td>VLAN Tag ID</td> <td><input type="text" value="4092"/></td> </tr> <tr> <td>VLAN Interfaces</td> <td><input type="button" value="1.1"/></td> </tr> <tr> <td>Tagging:</td> <td><input type="button" value="Select..."/></td> </tr> <tr> <td>Add</td> <td><input type="button" value="Add"/></td> </tr> <tr> <td>Interfaces</td> <td> 1.3 (untagged) <input type="button" value="Edit"/> <input type="button" value="Delete"/> </td> </tr> </table> </div>				VLAN Name	HANet	VLAN Tag ID	<input type="text" value="4092"/>	VLAN Interfaces	<input type="button" value="1.1"/>	Tagging:	<input type="button" value="Select..."/>	Add	<input type="button" value="Add"/>	Interfaces	1.3 (untagged) <input type="button" value="Edit"/> <input type="button" value="Delete"/>
VLAN Name	HANet														
VLAN Tag ID	<input type="text" value="4092"/>														
VLAN Interfaces	<input type="button" value="1.1"/>														
Tagging:	<input type="button" value="Select..."/>														
Add	<input type="button" value="Add"/>														
Interfaces	1.3 (untagged) <input type="button" value="Edit"/> <input type="button" value="Delete"/>														
<input type="button" value="Cancel"/> <input type="button" value="Next..."/>															

BEST PRACTICES

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

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

Network Time Protocol Configuration

Time Server List	Address: <input type="text" value="10.105.134.20"/> <input type="button" value="Add"/> <div style="background-color: #0070C0; color: white; padding: 2px 5px; margin-top: 5px;">10.105.134.20</div> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> </div>
<input type="button" value="Cancel"/> <input type="button" value="Next"/>	

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

Domain Name Server Configuration

DNS Lookup Server List	Address: <input type="text" value="10.105.134.20"/> <input type="button" value="Add"/> <div style="background-color: #0070C0; color: white; padding: 2px 5px; margin-top: 5px;">10.105.134.20</div> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/> </div>
BIND Forwarder Server List	Address: <input type="text"/> <input type="button" value="Add"/> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/> </div>
DNS Search Domain List	Address: <input type="text"/> <input type="button" value="Add"/> <div style="background-color: #0070C0; color: white; padding: 2px 5px; margin-top: 5px;">localhost</div> <div style="margin-top: 10px;"> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/> </div>
DNS Cache	<input type="checkbox"/>
IP Version	<input type="button" value="IPv4"/>
<input type="button" value="Cancel"/> <input type="button" value="Next"/>	



BEST PRACTICES

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

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

ConfigSync Configuration

Local Address	10.254.1.9 (HANet)
---------------	--------------------

Cancel **Next...**

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

Failover Unicast Configuration

<input checked="" type="checkbox"/> ▲ Local Address	Add...
<input type="checkbox"/> 10.254.1.9	Port
	VLAN
	1026 HANet

Delete

Failover Multicast Configuration

Use Failover Multicast Address	<input type="checkbox"/> Enabled
--------------------------------	----------------------------------

Cancel **Next...**

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

Mirroring Configuration

Primary Local Mirror Address	10.254.1.9 (HANet)
Secondary Local Mirror Address	None

Cancel **Next...**

15. Select Next to continue to Standard Pair Configuration.

Standard Pair Configuration

Establish an Active/Standby pair by discovering another device.

After discovering the other device, the system performs the following actions:

- Establishes trust between authoritative peers
- Creates a device group that contains this device and the peer device
- Creates a traffic group that supports an active/standby configuration

Next...



BEST PRACTICES

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

16. Complete the configuration of NSXBigIP by clicking Finished.

Configure Peer Device
If this is the first device in this active/standby pair that you have configured, then you should click **Finished** and exit this wizard. Then you should proceed to configure the peer device using the Setup Utility. When you reach this page on the peer device, choose the **Discover Configured Peer Device** option.

Finished

Proceed to configuring NSXBigIP2.

1. For Internal Network Configuration, use the following settings:

- Internal VLAN: Select Existing VLAN
- Select VLAN: WebTier01
- self IP
 - Address: 10.0.1.9
 - Netmask: 255.255.255.0
 - Port Lockdown: Allow Default
- Floating IP
 - Address: 10.0.1.13
 - Port Lockdown: Allow Default

2. Select Next to continue.

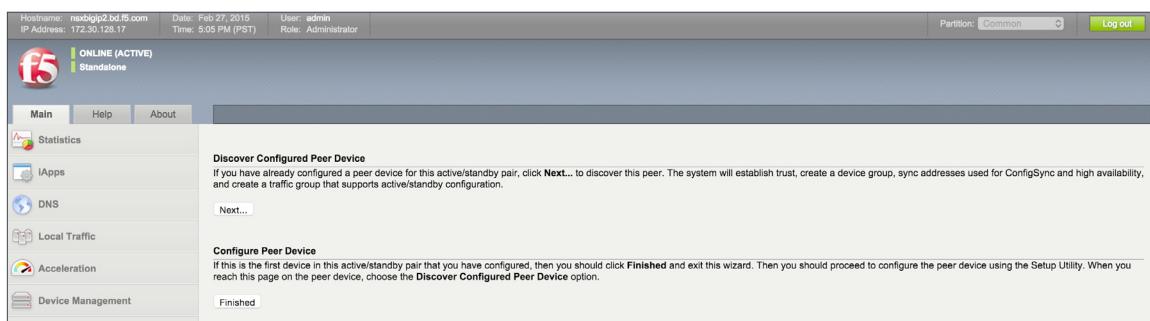
3. For External Network Configuration, use the following settings:

- Internal VLAN: Select Existing VLAN
- Select VLAN: AppTier01
- Self IP
 - Address: 10.0.2.9
 - Netmask: 255.255.255.0
 - Port Lockdown: Allow Default

BEST PRACTICES

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

- Floating IP
 - Address: 10.0.2.13
 - Port Lockdown: Allow Default
4. Select **Next** to continue.
 5. For High Availability Network Configuration, use the following settings:
 - Internal VLAN: Select Existing VLAN
 - Select VLAN: HANet
 - Self IP
 - Address: 10.254.1.9
 - Netmask: 255.255.255.0
 - Port Lockdown: Allow Default
 6. Select **Next** to continue.
 7. To create trust between the two devices and establish a high availability cluster, select **Discover Configured Peer Device**.



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



BEST PRACTICES

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

Hostname: nsxbigip2.bd.f5.com Date: Feb 27, 2015 User: admin
IP Address: 172.30.128.17 Time: 5:06 PM (PST) Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About

Statistics

iApps

DNS

Local Traffic

Acceleration

Device Management

Remote Device Credentials

Device IP Address	172.30.128.16
Administrator Username	admin
Administrator Password	*****

Cancel Retrieve Device Information

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

Hostname: nsxbigip2.bd.f5.com Date: Feb 27, 2015 User: admin
IP Address: 172.30.128.17 Time: 5:08 PM (PST) Role: Administrator

ONLINE (ACTIVE)
Standalone

Main Help About

Statistics

iApps

DNS

Local Traffic

Acceleration

Device Management

Network

System

Remote Device Credentials

Device IP Address	172.30.128.16
Administrator Username	admin
Administrator Password	*****

Device Certificate

Subject	/C=--/ST=WA/L=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Management IP Address	172.30.128.16
Expiration	Sun Feb 21 18:10:23 PST 2025
Serial Number	b1b09f483e9fa775
Signed	Yes
SHA-1	c62c456cc6ebad0c7af2cc390f9bd27ba7bd7b17
MD5	a63efc4ba6baaa250837730f480e463f

Device Properties

Name	nsxbigip1.bd.f5.com
------	---------------------

Sync-Failover Group Properties

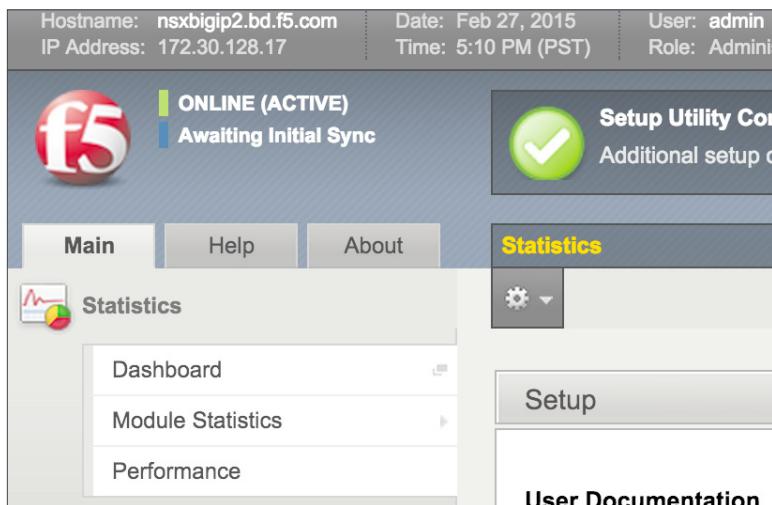
Name	device-group-failover-ad2f4f99ef90
------	------------------------------------

Cancel Finished

BEST PRACTICES

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

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



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

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



BEST PRACTICES

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

The screenshot shows the F5 Device Management interface. At the top, there's a header with the hostname nsxbigip2.bd.f5.com, date Feb 27, 2015, time 5:30 PM (PST), user admin, role Administrator, partition Common, and a Log out button. On the left is a sidebar with tabs for Main, Help, About, Statistics, iApps, DNS, Local Traffic, Acceleration, Device Management (selected), Network, and System. The main content area has a title 'Device Management > Overview'. It shows 'Device Groups' with two entries: 'device-group-failover-ad2f4ff9ef90' (Sync-Failover, Manual, 2 devices) and 'device_trust_group' (Sync-Only, Auto, 2 devices). Below that is a 'Sync Summary' section stating 'All devices in the device group are in sync'. The 'Devices' section lists 'nsxbigip1.bd.f5.com' and 'nsxbigip2.bd.f5.com (Self)' with their sync status and configuration times. Under 'Sync Options', there are radio buttons for 'Sync Device to Group' (selected) and 'Sync Group to Device', and a checkbox for 'Overwrite Configuration'. A 'Sync' button is at the bottom.

Application Configuration

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

Create application pools

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

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

BEST PRACTICES

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

4. Under **Health Monitors**, select an appropriate monitor for your application. In this case we chose a **gateway_icmp** monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.
5. Under **Resources**, select a **Load Balancing Method**. For basic load balancing in this validation, **Round Robin** was used.
6. Under **Resources**, use the **New Members** setting to add the IP address and port of the web servers. Click the **Add** button for each pool member.
7. Select **Repeat** to continue and input the application tier information.

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

Table 15. BIG-IP web tier pool members

The screenshot shows the F5 BIG-IP Local Traffic interface. The main menu bar includes File, Edit, View, Favorites, Tools, and Help. The top status bar shows Hostname: bd5000.bd.f5.com, Date: Feb 19, 2015, Time: 2:18 PM (PST), User: admin, and Role: Administrator. The interface title is Local Traffic > Pools : Pool List > New Pool... . On the left, there's a navigation sidebar with links for Statistics, iApp, Local Traffic (Network Map, Virtual Servers, Policies, Profiles, iRules, Pools, Nodes, Monitors, Traffic Class, Address Translation, DNS Express Zones, DNS Caches), Acceleration, Device Management, and Network. The main content area shows the configuration for a new pool:

- Configuration:** Basic
- Name:** WebServerPool
- Description:** (empty)
- Health Monitors:** /Common/gateway_icmp
- Resources:**
 - Load Balancing Method:** Round Robin
 - Priority Group Activation:** Disabled
 - Node Name:** (Optional)
 - Address:** 10.0.1.12
 - Service Port:** 80 (HTTP)
- New Members:**
 - R:1 P:0 C:0 10.0.1.11 10.0.1.11:80
 - R:1 P:0 C:0 10.0.1.12 10.0.1.12:80

At the bottom right, there are buttons for Cancel, Repeat, and Finished.

BEST PRACTICES

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

13. In the Name field, type a unique name for the web pool. For this validation, AppServerPool was used.
14. Under Health Monitors, select an appropriate monitor for your application. In this case, we are choosing a gateway_icmp monitor to ensure server health, but much more in-depth health monitoring is available to determine application availability.
15. Under Resources, select a Load Balancing Method. For basic load balancing in this validation, Round Robin was used.
16. Under Resources, use the New Members setting to add the IP address and port of the web servers. Click Add for each pool member.
17. Click Finished to complete the pool creation.

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

Table 16. BIG-IP application tier pool members

The screenshot shows the F5 BIG-IP Local Traffic interface. The top navigation bar includes File, Edit, View, Favorites, Tools, and Help. The status bar at the top displays Hostname: bd5000.bd.f5.com, Date: Feb 19, 2015, User: admin, IP Address: 10.105.155.17, Time: 3:51 PM (PST), and Role: Administrator. On the left, a sidebar lists Main, Help, and About, along with various configuration tabs like Statistics, iApp, Local Traffic, iRules, Pools, Nodes, Monitors, Traffic Class, Address Translation, DNS Express Zones, DNS Caches, Acceleration, Device Management, and Network. The main content area shows the 'Local Traffic > Pools : Pool List > New Pool...' screen. It has sections for Configuration (Basic), Name (AppServerPool), Description, Active Health Monitors (/Common/gateway_icmp), Available Health Monitors (https_head_15_inband, tcp, tcp_half_open, udp), Resources (Load Balancing Method: Round Robin, Priority Group Activation: Disabled), and New Members (Node Name: 10.0.2.12, Address: 10.0.2.12, Service Port: 80 (HTTP)). The bottom of the screen shows buttons for Cancel, Repeat, and Finished.

BEST PRACTICES

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



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

A screenshot of the F5 BIG-IP Local Traffic > Pools : Pool List interface. The screen shows a table with two rows. The first row contains 'AppServerPool' with 2 members and the status 'Common'. The second row contains 'WebServerPool' with 2 members and the status 'Common'. Both rows have a green circle icon next to them, indicating successful monitoring. The table has columns for Status, Name, Application, Members, and Partition / Path.

Create application virtual server

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

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



BEST PRACTICES

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

Screenshot of the F5 BIG-IP Configuration interface showing the creation of a new Virtual Server named "Web-Vip".

General Properties:

- Name: Web-Vip
- Description: (empty)
- Type: Standard
- Source: (empty)
- Destination:
 - Type: Host (radio button selected)
 - Address: 20.20.20.5
- Service Port: 80 (HTTP)
- State: Enabled

Content Rewrite:

- Rewrite Profile: None
- HTML Profile: None

Acceleration:

- Rate Class: None
- OneConnect Profile: None
- NTLM Conn Pool: None
- HTTP Compression Profile: None
- Web Acceleration Profile: None
- SPDY Profile: None

Resources:

- iRules:
 - Enabled: (empty)
 - Available: _sys_auth_krbdelegate, _sys_auth_ssl_cc_idap, _sys_auth_ssl_crldp, _sys_auth_ssl_ocsp, _sys_https_redirected
- Policies:
 - Enabled: (empty)
 - Available: /Common sys_CEC_video_policy
- Default Pool: WebServerPool
- Default Persistence Profile: None
- Fallback Persistence Profile: None

BEST PRACTICES

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

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

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

Local Traffic > Virtual Servers : Virtual Server List						
		Virtual Server List		Virtual Address List		Statistics
<input type="checkbox"/> <input checked="" type="checkbox"/> Status <input type="checkbox"/> <input type="checkbox"/> Name		Application	Destination	Service Port	Type	Resources
<input type="checkbox"/>		App-Vip	10.0.1.5	80 (HTTP)	Standard	Edit...
<input type="checkbox"/>		Web-Vip	20.20.20.5	80 (HTTP)	Standard	Edit...

[Enable](#) [Disable](#) [Delete...](#)

Synchronize Changes across the Cluster

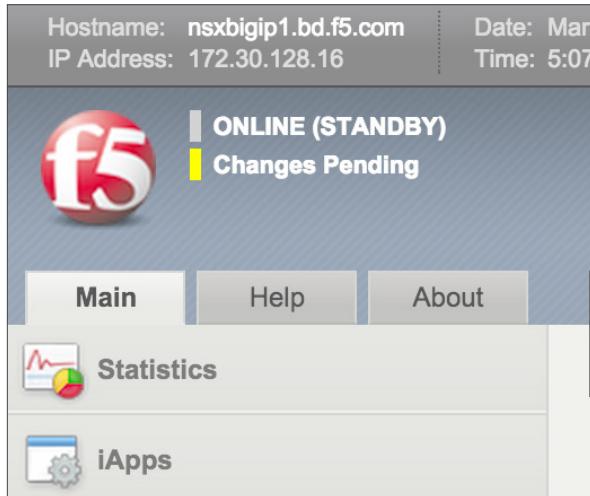
When working with a device cluster, we must initiate the sync process from the device cluster we are making changes to on the peer BIG-IP.

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



BEST PRACTICES

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



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

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

Hostname: nsxbigip1.bd.f5.com Date: Mar 2, 2015 User: admin
IP Address: 172.30.128.16 Time: 5:08 PM (PST) Role: Administrator Partition: Common Log out

ONLINE (STANDBY)
Changes Pending

Main Help About

Statistics iApps

Device Management > Overview

Device Groups

Name	Sync Status	Number of Devices	Device Group Type	Sync Type
device-group-failover-ad2f4f99ef90	Changes Pending	2	Sync-Failover	Manual
device_trust_group	Green	2	Sync-Only	Auto

Sync Summary

Status	Changes Pending
Summary	Changes pending
Details	Recommended action: Synchronize nsxbigip1.bd.f5.com to group device-group-failover-ad2f4f99ef90

Devices

HA Status	Name	Sync Status	Configuration Time
Up	nsxbigip1.bd.f5.com (Self)	Changes Pending	3/2/2015 16:49:32
Up	nsxbigip2.bd.f5.com	Green	2/27/2015 17:30:08

Sync Options

Sync Device to Group
 Sync Group to Device
 Overwrite Configuration

Sync

BEST PRACTICES

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

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

Name	Sync Status	Number of Devices	Device Group Type	Sync Type
device-group-failover-ad24f99ef90	●	2	Sync-Failover	Manual
device_trust_group	●	2	Sync-Only	Auto

Sync Summary Status: In Sync
Summary: All devices in the device group are in sync
Details:

HA Status	Name	Sync Status	Configuration Time
●	nsxbigip1.bd.f5.com (Self)	●	3/2/2015 16:49:32
●	nsxbigip2.bd.f5.com	●	3/2/2015 16:49:32

Sync Options

- Sync Device to Group
- Sync Group to Device

Overwrite Configuration

- This completes the configuration portion for the topology.

Validation

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

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

Local Traffic Network Map	
● App-Vip ● AppServerPool ● 10.0.2.11:80 ● 10.0.2.12:80	● Web-Vip ● WebServerPool ● 10.0.1.11:80 ● 10.0.1.12:80

BEST PRACTICES

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

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



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

Conclusion

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

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

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