

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





Contents

Introduction		
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	
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	
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	
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.

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.

vmware [®] vSphere Web Client	Ø	🕗 Administrator@VSPHERE.LOCAL + Help +	I Q Search -
	USSJ-VC51.bd.f5.com Actions ~ Summary Monitor Manage Related Objects USSJ-VC51.bd.f5.com Virtual Machines: 329 Hosts: 17	CPU FREE: 364.30 CH2 USED: 44.47 CH2 CAPACITY: 408.82 CH2 MEUORY FREE: 031.82 CB USED: 750.97 CB CAPACITY: 1.53 TB STORAGE FREE: 6.04 TB	¥ ▼
 Im USSJ-55-Computer Cluster Im USSJ-55-Management Cluster 		USED: 7.26 TB CAPACITY: 14.2 TB	



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

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.

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 (+).

vmware [®] vSphere Web Cli	ent 🔒 🗗
Home 🕨 🔊 I	NSX Edges
Networking & Security	NSX Manager: 10.105.134.165
🚟 NSX Home	+
🙀 Installation	Id Na
💁 Logical Switches	1
NSX Edges	
👸 Firewall	
in SpoofGuard	
뿾 Service Definitions	
Service Composer	
🗿 Data Security	
🙀 Flow Monitoring	
III Activity Monitoring	
✓ Networking & Security Inventory	
NSX Managers	

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

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



New NSX Edge		(? H
1 Name and description	Name and description	
 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Firewall and HA 7 Ready to complete 	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: Topo1ESG Hostname: Description: Tenant	
	Back Next Finish Ca	incel

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

Ne	ew NSX Edge	?	**
~	1 Name and description	Settings	Ī
~	2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Firewall and HA 7 Ready to complete	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: Confirm password: Confirm password: Confirm password: Configuring High Availability Enable High Availability Enable High Availability Enable auto rule generation Enable auto rule generation Enable auto rule generation Enable auto rule generation Enable auto rule generation, to automatically generate service rules to allow flow of control traffic.	f
		Edge Control Level Logging EMERGENCY Set the Edge Control Level Logging	
		Back Next Finish Cancel	

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.

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



Ne	ew	NSX Edge				(?) ₩
~	1	Name and description	Configure deployn	nent		
~	2	2 Settings	Determine)	
	E	Configure deployment	Appliance Size:	SJC +	J	
	4	Configure interfaces	Appliance size.	Compact		
	Ę	Default gateway settings		O X-Large		
	6	Firewall and HA		Quad Large		
	7	Ready to complete	🖌 Deploy NSX E	dge		
			NSX Edge Applian	Host	Datastore	Folder
			Specifying a reso Edge appliance.	urce pool and datastor	e is mandatory for c	onfiguring the NSX
				Back	Next	Finish Cancel

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.

Add NSX Edge Appliance		?
Specify placement parameter:	s for the NSX Edge appliance.	
Cluster/Resource Pool: *	USSJ-55-Managemen 💌	
Datastore: *	2240-2-10K 🔹	
Host:	•	
Folder:	•	
	OK Cance	

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

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



New NSX Edge					?₩
 1 Name and description 	Configure in	nterfaces			
2 Settings3 Configure deployment	Configure i	nterfaces of this	NSX Edge		
4 Configure interfaces 5 Default gateway settings	vNIC#	Name	IP Address	Subnet Prefix Length	Connected To
6 Firewall and HA 7 Ready to complete					
			Back	Next Fir	nish Cancel

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

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



dd NSX Edge Interfa	ce
vNIC#:	0
Name:	* External
Туре:	O Internal O Uplink
Connected To:	Select Remove
Connectivity Status:	Connected Disconnected
Configure subnets	
🕈 🧷 🗙	
IP Address	Subnet Prefix Length
MAC Addresses:	
	You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.
MTU:	1500
Options:	Enable Proxy ARP Send ICMP Redirect
Fence Parameters:	
	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**.

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



Add NSX Edge	e Interface
VNIC#:	0
Name:	* External
Type:	O Internal O Uplink
Connected	To: Select Remove
Connectivi	Connect NSX Edge to a Network (?)
Configure	Logical Switch Standard Portgroup Distributed Portgroup
+ /	📡 🔍 dvs_vl20 🗸
IP Address	Name Type
	Avs_VL20-NSXExternal Distributed Port Group
MAC Addre	
	n. In
	M 1 of 32 items
MTU:	
Options:	OK Cancel
Fence Para	meters:
	Example: ethernet0.filter1.param1=1
	OK Cancel

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

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



Add NSX Edge Interfac	;e (?
vNIC#:	0
Name:	External
Туре:	Internal O Uplink
Connected To:	dvs_VL20-NSXExternal Change Remove
Connectivity Status:	Connected Disconnected
Configure subnets	
🕈 / 🗙	
IP Address	Subnet Prefix Length
MAC Addresses:	
	You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.
MTU:	1500
Options:	Enable Proxy ARP Send ICMP Redirect
Eence Parameters	
	Example: athernat0 filter1 param1=1
	OK Cancel

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

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



Add Subnet		?)
Specify the IP	addresses in the subnet: ∗		
+ ∕ ×			
Primary IP	IP Address		
$\overline{\bullet}$	172.16.1.1	OK Cancel	
Subnet prefix I	ength: * 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	Туре	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.

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



New NSX Edge		(?) H
 1 Name and description 2 Settings 3 Configure deployment 	Default gateway settings	
 4 Configure interfaces 	vNIC: * External *	
5 Default gateway settings	Gateway IP: * 20.20.20.1	
6 Firewall and HA	MTU: 1500	
7 Ready to complete		
		0
	Back Next Finish	Cancer

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

New NSX Edge			(?) ₩
 1 Name and description 	Firewall and HA		
 2 Settings 3 Configure deployment 	Configure Firewall	default policy	
✓ 4 Configure interfaces	Default Traffic Policy:	 Accept Oeny 	
 5 Default gateway settings 	Logging:	🔵 Enable 💿 Disable	
6 Firewall and HA 7 Ready to complete	Configure HA paramet Configuring HA param	t ers eters is mandatory for HA	to work.
	vNIC: * Declare Dead Time: Management IPs: You can specify pair of	any T5 TPs (in CIDR format) with	(seconds) //30 subnet. Management IPs must
	not overlap with any vn	ic subnets.	
		Back	Next Finish Cancel

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



Create and Deploy DLR

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

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

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



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

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



New NSX Edge		(? H
1 Name and description	Name and description	
 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Ready to complete 	Install Type: C Edge Services Gateway Provides common gateway services su VPN, NAT, Routing and Load Balancin C Logical (Distributed) Router Provides Distributed Routing and Bridg	rch as DHCP, Firewall, g. ging capabilities.
	Name: Topo1DLR Hostname: Description: Tenant	
	3	
	Back Next	Finish Cancel

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

New	NSX Edge		? H
New 1 2 3 4 5 6	NSX Edge Name and description Settings Configure deployment Configure interfaces Default gateway settings 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 (s). These credentials can be used to login to the read only command line interface of the appliance (s). These credentials can be used to login to the read only command line interface of the appliance (s). These credentials can be used to login to the read only command line interface of the appliance (s). These credentials can be used to login to the read only command line interface of the appliance (s). These credentials can be used to login to the read only command line interface of the appliance (s). The set of	? >>
		Back Next Finish C	ancel

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.

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



dit NSX Edge Appliance			
pecify placement paramet	ers	s for the NSX Edge appliar	nce.
Cluster/Resource Pool:	*	NSX Computer Cluster	•
Datastore:	*	2240-2-10K	•
Host:			•
Folder:	1		-

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

 ✓ 1 Name and description ✓ 2 Settings ✓ 3 Configure deployment ✓ 4 Configure interfaces ✓ 5 Default gateway settings ⑤ Roady to complete ✓ Addees ✓ Addees ✓ Unit of the management interface is a mandatory special-purpose interface in a mandatory special-purpose interfaces in Logical Router. Configure interfaces of this NSX Edge ✓ 1 Name P Addees Subnet Prefix Longin Connected To 						w NSX Edge		
 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Roady to complete Management interface Configuration Connected To: + Select 2 X Address Subnet Prefax L Configure interfaces of this NSX Edge Management interfaces of this NSX Edge Management interfaces of this NSX Edge Management interfaces of this NSX Edge 				faces	Configure inte	 1 Name and description 		
5 Default gateway settings © Ready to complete IP Address Submit gateway settings IP Address Submit gateway settings IP Address IP Address Submit gateway settings IP Address IP Address Submit gateway settings IP Address IP Addr	Remove	Select	2 Settings 3 Configure deployment 4 Configure interfaces					
6 Ready to complete Subret Prefix L The management interface is a mandatory special-purpose interface that network connectivity and is configured separately from other interface in the Logical Router. Configure interfaces of this NSX Edge					• / ×	5 Default gateway settings 6 Ready to complete		
The management interface is a mandatory special-purpose interface that network connectivity and is configured separately from other interfaces in Logical Router. Configure interfaces of this NSX Edge Configure interfaces of this NSX Edge Mame P Address Subnet Prefix Langth Connected To	Length	Subnet Prefix L			IP Address			
The management interface is a mandatory special-purpose interface that network connectivity and is configured separately from other interfaces in Logical Router. Configure interfaces of this NSX Edge Configure interfaces of this NSX Edge Image: Configure interfaces of this NSX Edge								
Name IP Address Subnet Prefix Length Connected To	trequires the	rpose interface that a other interfaces in	datory special-pu d separately from ge	ent interface is a ma ctivity and is configur rfaces of this NSX E	The manager network conn Logical Route Configure int			
		Connected To	Subnet Prefix Length	I th Address	Name			

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

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



Connect NSX Edge to a Network			
Logical Switch	Distributed Portgroup		
	🌠 🔍 dvs_vl155		
Name	Туре		
🔘 🚨 dvs_VL155_NSXIPPod	Distributed Port Group		
**	4 - 5 0 14		
199	1 of 2 items		
	OK Cancel		

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

Add Subnet		(2
Specify the IP	addresses in the subnet: *		
🔶 🧶 🗶			
Primary IP	IP Address		
\odot	10.105.155.19	OK Cancel	
Subnet prefix	length: <mark>*</mark> 24		
		OK Cancel)

 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.

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



Network Name	Connected To	Туре	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.

New NSX Edge					? •			
1 Name and description2 Settings	Configure interfaces							
3 Configure deployment 4 Configure interfaces	Connected To: * dvs_VL155_NSXIPPool Cha							
5 Default gateway settings	IP Address			Subnet P	refix Length			
6 Ready to complete	10.105.155.19*	24	narina kaongon					
	The management i is configured separ Configure interface	nterface is a mandatory s ately from other interface: es of this NSX Edge	pecial-purpose interfa s in the Logical Route	ace that requires netw r.	vork connectivity and			
	Name	e IP Address Subnet		Connected To				
	TransitNet2	172.16.2.2*	24	TransitNet-2				
	WebTier1	10.0.1.1*	24	WebTier				
	Apptier	10.0.2.1*	24	AppTier				
	DBTier	10.0.3.1*	24	DBTier				
			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 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.

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



 A name and description S settings Configure deployment Configure Default Gateway Configure Default Gateway MIC: • TransitNet2 • • Gateway IP: • 1721621 MTU: • 1500 	New NSX Edge			(4 (S
 ✓ 4 Configure interfaces ✓ VIIC: * TransitNet2 ✓ TransitNet2 ✓ Gaeway IP: 172.16.2.1 MTU: 1500 	 1 Name and description 2 Settings 3 Configure deployment 	Default gatewa	ay settings Default Gateway	
S Default gateway settings Gateway IP: ◆ 172:18:2.1 MTU: 1500	 4 Configure interfaces 	vNIC: *	TransitNet2	
6 Ready to complete	5 Default gateway settings	Gateway IP: *	172.16.2.1	
	6 Ready to complete	MTU:	1500	
			la l	
Back Navt Shiph Connel			Book Next Shich	Concol

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.

1 Name and description	Ready to complete							
2 Cottions								
2 Settings	Name and description							
3 Configure deployment	Name:	Topo1DLR						
4 Configure interfaces	Install Type:	Logical (Distributed)	Router					
5 Default gateway settings	Tenant							
6 Ready to complete	HA:	Disabled						
	Management Interface Col	nfiguration						
	Connected To: dvs_VL1	55_NSXIPPool						
	IP Address	IP Address						
	10.105.155.19*							
	NSX Edge Appliances							
	Resource Pool	Host	Datastore		Folder			
	NSX Computer Cluster		2240-2-10K					
	Interfaces							
	Name	IP Address	Subnet Prefix Length	Connected T	Connected To			
	TransitNet2	172.16.2.2*	24	TransitNet	-2			
	WebTier1	10.0.1.1*	24	WebTier				
	Apptier	10.0.2.1*	24	AppTier				
	DBTier	10.0.3.1*	24	DBTier				

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

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



File Edit View Favorites Tools H	lelp									
vmware [,] vSphere Web Cli	ient 🕈 🖉					Ŭ I Adm	inistrator@VSPHERE.LOCAL + I	Help +	I Q Search	•
(Home) 🔊 I	NSX Edges									*
Networking & Security	NSX Manager: 10.105.155.165	•							* 👔 Recent Tasks	-
NSX Home	🔶 🗙 😅 🎭 🛞 🔟 🕴	🚳 Actions 👻		🛟 0 Installing 🚸 0 Failed			📡 🔍 Filter	•	All Running	Failed
gg installation	ld 1.	Name	Туре	Version	Status	Tenant	Interfaces	Size		
Sector 2 Contract Switches	edge-3	Topo1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp		
🗮 NSX Edges	edge-4	Topo1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp		
Firewall										
Regional SpoolGuard										
🌼 Service Definitions										
// Service Composer										
🚳 Data Security										
💽 Flow Monitoring									My Tasks 🔻	More Tasks

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.

File Edit View Favorites Tools Help											
Vmware vSphere Web Client 🛉 @											
(Home) 🔊 I	NSX Edges									Ŧ	
Networking & Security	NSX Manager: 10.105.155.165	 ▼							* 🛐 Recent Tasks	-	
NSX Home	🔶 🗙 😅 🖏 🛞 🗎 🗎	i Actions →		🛟 0 Installing 🚸 0 Failed			📡 🔍 Filter	•	All Running	Failed	
(g) Installation	ld 1	A Name	Туре	Version	Status	Tenant	Interfaces	Size			
Sector 2015 Switches	edge-3	Topo1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp			
NSX Edges	edge-4	Topo1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp			
Firewall											
M SpoofGuard											
Service Definitions											
Service Composer											
Data Security											
💽 Flow Monitoring									My Tasks 🔻	More Tasks	

 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.

File Edit View Favorites Tools H	kelp ient 🕈 🖉							
4 Networking & Sec 🕨 🧐 🕱	Topo1ESG Actions +							
Topo1ESG	Summary Monitor Manage							
	Settings Firewall DHCP NAT Routing Load Balancer VPN SSLVPN-Plus Grouping Obj							
	++ Global Configuration	5	×		Network			
	Static Routes							
	O SPF BGP IS-IS Route Redistribution							



 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.

Network:	* 10.0.0/16	
	Network should be entere e.g. 192.169.1.0/24	ed in CIDR format
Next Hop:	172.16.2.2	
Interface:	TransitNet-2	• 🚯
MTU:	1500	
Description:		
		5

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





BIG-IP Appliance Configuration

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

Prerequisites

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

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

Create VLANs

- 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.

File Edit View Favorites Tools	; Help								
Hostname: bd5000.bd.f5.com Dat IP Address: 10.105.155.17 Tim	Nantana & Malanda Ma								
CONLINE (ACTIVE) Standaione									
Main Help About	Network » VLANs : VLAN List								
Statistics	o v VLAN List VLAN Groups								
iApp		Cysto							
Local Traffic	🖌 Anme	Application Tag Untagged Interfaces Tagged Interfaces Partition / Path							
A	No records to display.								
Acceleration	Delete								
Device Management									
Retwork									
Interfaces									
Routes									
Self IPs (
Packet Filters									
Spanning Tree									
Trunks									

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.

	ONLINE (ACTIVE)		
I	Standalone		
Main	Help About	Network » VLANs : VLAN List	» New VLAN
Statis	tics		
		General Properties	
(10) - 44F-		Name	External
Local	Traffic	Description	
	eration	Тад	20
E Device	e Management	Resources	
-			Interface: 1.2 🗘
Netwo	ork		Tagging: Tagged
Inte	erfaces >		Add
Rou	utes 💮	Interfaces	1.1 (tagged)
Sel	f IPs 💮		
Pac	cket Filters		
Tru	nks		Edit Delete
Tur	nels	Configuration: Basic	
Rou	ute Domains 💮	Source Check	
VL/	ANs	MTU	1500
Cla	ss of Service		
AR	P >	sFlow	
IPs	ec >	Polling Interval	Default 😂 Default Value: 10 seconds
WC	CCP (+)	Sampling Rate	Default 📀 Default Value: 2048 seconds
DN	S Resolvers	Cancel Repeat Finished	
Se System	m		

- 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.

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.

File Edit View Favorites Tools Hel	p	
Hostname: bd5000.bd.f5.com Date: Fet IP Address: 10.105.155.17 Time: 2.1	9 19, 2015 User: admin 6 PM (PST) Role: Administrator	
ONLINE (ACTIVE) Standalone	Loading Receiving configuration	1 data from your device.
Main Help About	Network » Self IPs » New Se	If IP
Statistics	Configuration	
Los IApp	Name	ExtSelfIP
Local Traffic	IP Address	20 20.20.10
Acceleration	Netmask	255.255.255.0
Device Management	VLAN / Tunnel	External
	Port Lockdown	Allow None
Network	Traffic Group	Inherit traffic group from current partition / path
Interfaces >		tranic-group-tocal-only (non-troating)
Routes 💮	Cancel Repeat Finished	
Self IPs 📀		
Packat Filters		

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

File Edit View Favorites Tools Hel	p	
Hostname: bd5000.bd.f5.com Date: Fei IP Address: 10.105.155.17 Time: 2:1	b 19, 2015 User: admin 6 PM (PST) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	Network » Self IPs » New Sel	f IP
Statistics	Configuration	
Ligi IApp	Name	TransNetSelf
Local Traffic	IP Address	172.16.1.2
Acceleration	Netmask	255.255.255.0
Device Management	VLAN / Tunnel	TransitNet1
	Port Lockdown	Allow None
Network	Traffic Group	Inherit traffic group from current partition / path
Interfaces >		samc-group-local-only (non-lioating)
Routes (+)	Cancel Repeat Finished	
Self IPs 📀	υg	

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

Net	work » Self IPs						
₽	✓ Self IP List						
		-	-				Create
	Anne	Application	+ IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
	ExtSelfIP		20.20.20.10	255.255.255.0	External	traffic-group-local-only	Common
	TransitNet-01		172.16.1.2	255.255.255.0	App-Tier	traffic-group-local-only	Common
Del	ete						

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.

- 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.

File Edit View Favorites Tools	Help	
Hostname: bd5000.bd.f5.com Date: IP Address: 10.105.155.17 Time:	Feb 19, 2015 User: admin 2:17 PM (PST) Role: Administr	
ONLINE (ACTIVE) Standalone		
Main Help About	Network » Routes » Ne	w Route
Statistics	Properties	
iApp	Name	default
Local Traffic	Description	
Acceleration	Destination	0.0.0.0
Device Management	Netmask	0.0.0.0
	Resource	Use Gateway
Network	Gateway Address	IP Address 20/20.20.1 ×
Interfaces	MTU	0
Routes 🕘		2
Self IPs 📀	Cancer Repeat Finishe	*
Packet Filters	2 C	
Output and Taxa		

- 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.

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.

File Edit View Favorites Tools Hel	p	
Hosiname: bd5000.bd.f5.com Date: Fel IP Address: 10.105.155.17 Time: 2.1	9 19, 2015 User: admin 7 PM (PST) Role: Administra	ator
ONLINE (ACTIVE) Standalone		
Main Help About	Network » Routes » New	w Route
Statistics		
-	Properties	
Log IApp	Name	ServerRoutes
Local Traffic	Description	
Acceleration	Destination	10.0.0.0
	Netmask	255.255.0.0
Device Management	Resource	Use Gateway
Network	Gateway Address	IP Address V 172.16.1.1 ×
Interfaces >	MTU	0
Routes 💮		
Self IPs 📀	Cancel Repeat Finished	3

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

Net	Network » Routes									
₽	- Route List									
								Add		
	▼ Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path		
	default		Default IPv4		Partition Default Route Domain	Gateway	20.20.20.1	Common		
	ServerRoutes		10.0.0.0	255.255.0.0	Partition Default Route Domain	Gateway	172.16.1.1	Common		
Del	ete									

Application Configuration

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



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

Create application pools

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

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

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

Table 5. BIG-IP web tier pool members

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



File Edit View Favorites Tools He Hostname: bd5000 bd f5.com Date: Fi IP Address: 10.105.155.17 Time. 2 ONLINE (ACTIVE) Standalone	dp eb 19, 2015 User: admin 18 PM (PST) Role: Administrato	ar 11 int - 1. New Dool
Statistics		
-	Configuration: Basic 🗸	1
iApp	Name	WebServerPool
Local Traffic	Description	
Network Map		Active Available
Virtual Servers	Health Monitors	/Common gateway icmp
Policies	rieaun monitors	http_head_f6
Profiles		https_443
iRules >	Resources	
Pools	Load Balancing Method	Round Robin
Nodes >	Priority Group Activation	Disabled
Monitors 💿		Node Name: (Ontional)
Traffic Class 💿		Address: 10.0.1.12
Address Translation		Service Port: 80 HTTP V
DNS Express Zones	New Members	Add
DNS Caches		R:1 P:0 C:0 10.0.1.12 10.0.1.12 :80
Acceleration		Edit Delote
Device Management	Cancel Repeat Finished	
Network	Constant Contrast County See	

- 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.

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

File Edit View Favorites Tools He	elp						
Hosiname: bd5000.bd.f5.com Date: Fe IP Address: 10.105.155.17 Time: 3	eb 19, 2015 User: admin 51 PM (PST) Role: Administrato						
Standalone	Receiving configurat	tion data from your device.					
Main Help About	Local Traffic » Pools : Pool	List » New Pool					
Statistics	Configuration: Basic 🗸	1					
iApp	Name	AppServerPool					
Local Traffic	Description						
Network Map		Active Available					
Virtual Servers	Health Monitors	gateway_icmp st inband h					
Policies		≥> tcp_haif_open ∨ udp					
Profiles							
iRules >	Resources	David Dabia					
Pools	Load Balancing Method	Round Robin					
Nodes	Priority Group Activation	Disabled					
Monitors (+)		New Node Node List					
Traffic Class 🕒		Node Name: (Optional)					
Address Translation		Address: 10.0.2.12					
DNS Express Zones	New Members	Add					
DNS Caches	New Members	R 1 P 0 C 0 10 0 2 11 10 0 2 11 80					
Acceleration		R ⁻¹ P-0 C-0 10.0.2.12 10.0.2.12-80					
Device Management		Edit Delete					
Network	Cancel Repeat Finched						

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.

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



Loca	Local Traffic » Pools : Pool List												
⇔ -	Pool List	Statisti	cs 🗷										
*			Sea	rch									Crea
	 Status 	 Name 									Application	Members	Partition / F
	0	AppServerPool										2	Common
	0	WebServerPool										2	Common
Delet	e												

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.

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



File	Edit View Favorites Tools Help		
Hoste IP Ad	name: bd5000.bd.f5.com Dale: Feb Idress: 10.105.155.17 Time: 2:23	19, 2015 User: admin PM (PST) Role: Administrator	
-	ONLINE (ACTIVE)		
	Standalone		
M	ain Help About	Local Traffic » Virtual Servers	: Virtual Server List » New Virtual Server
1 too	Statistics		
	Арр	Name	Web-Vip
	ocal Traffic	Description	
	Network Map	Туре	Standard
	Virtual Servers	Source	
	Policies >	Destination	Type: Host O Network
	Profiles	Desthation	Address: 20.20.20.5
	iRules >	Service Port	80 HTTP V
i,	Pools	State	Enabled
	Nodes >	Configuration: Basic	ht
	Monitors (+)	Source Address Translation	Auto Map 🔽
		Content Rewrite	
		Rewrite Profile	None
		HTML Profile	None 🔽
		Acceleration	Newslay
		Rate Class	None V
		OneConnect Profile	None V
		NTLM Conn Pool	None V
		HTTP Compression Profile	None
		Web Acceleration Profile	None
		SPDY Profile	None 🗸
		Resources	
			Enabled Available
		Rules	sys_auth_ssl_cc_idap
			Up Down
			Enabled Available
		Policies	sys_CEC_video_policy
			>>
		Default Pool	WebServerPool
		Default Persistence Profile	None
		Fallback Persistence Profile	None
		Cancel Repeat Finished	
		Contraction of Contra	



- 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	Local Traffic » Virtual Servers : Virtual Server List									
⇔ ⇒	Virtual S	Server List	Virtual Address List	Statistics	-					
*			Sea	irch						Create
	 Status 	▲ Name			Application	Destination	Service Port	Type	Resources	Partition / Path
	0	App-Vip				10.0.1.5	80 (HTTP)	Standard	Edit	Common
	0	Web-Vip				20.20.20.5	80 (HTTP)	Standard	Edit	Common
Enable	e Disab	le 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.
VMware NSX for vSphere (NSX-v) and F5 BIG-IP



Local Traffic » Network Map	
🔅 🚽 Network Map	
Status Any Status 🗸 Type All Types 🗸 St	arch * Search iRule Definition
Show Summary Update Map	
Local Traffic Network Map	
O App-Vip	🔘 Web-Vip
O AppServerPool	O WebServerPool
10.0.2.11:80	10.0.1.11:80
10.0.2.12:80	10.0.1.12:80
1	- L

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



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



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



Figure 4. BIG-IP appliances parallel to DLR

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

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





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

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

Implementation Infrastructure

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

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



Figure 6. vSphere console



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

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

Prerequisites

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

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

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

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

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.

File Edit View Favorites Tools H	Help						
vmware vSphere Web C	lient 🕈 🖉					Updated at 10:19 AM	U Administrator@VSPHERE.LOCAL - Help -
🖣 Home 🕨 🗐 🖡	Portgroups						
0000	Actions +						🃡 🍱 🔍 Filter 🔹
👻 🚱 vcdemo	Name	1 A VLAN ID	Status	Port Binding	Network Protocol Profile	Number of VMs	Number of Ports
→ MSXDemo	▲ 131_LR_Internal	VLAN access: 131	Normal	Static binding (elastic)		0	128
se none	AvPortGroup2	VLAN access: 0	📀 Normal	Static binding (elastic)		0	128
with the two is a second secon	& dvs_Trunk_All	VLAN trunk: 1-1000	📀 Normal	Static binding (elastic)		0	256
✓ ministructureDVS	& dvs_VL11	VLAN access: 11	O Normal	Static binding (elastic)		0	128
🗢 🚊 (28) Portgroups	& dvs_VL115	VLAN access: 115	O Normal	Static binding (elastic)		0	128
▶	& dvs_VL115_INF	VLAN access: 115	O Normal	Static binding (elastic)		0	47
	& dvs_VL116_WEB	VLAN access: 116	O Normal	Static binding (elastic)		0	8
	& dvs_VL117_APP	VLAN access: 10	O Normal	Static binding (elastic)		0	8
	& dvs_VL118_CLIENT1	VLAN access: 118	Normal	Static binding (elastic)		0	128
	& dvs_VL119_Client2	VLAN access: 119	O Normal	Static binding (elastic)		0	8
	& dvs_VL120_DB	VLAN access: 120	O Normal	Static binding (elastic)		0	8
	Avs_VL121	VLAN access: 121	O Normal	Static binding (elastic)		0	128
	& dvs_VL121_Storage	VLAN access: 121	Ø Normal	Static binding (elastic)		0	8
	& dvs_VL128untag	VLAN access: 128	O Normal	Static binding (elastic)		0	256
	& dvs_VL130_daas_IIm	VLAN access: 130	O Normal	Static binding (elastic)		0	8
	& dvs_VL155_NSXIPPool	VLAN access: 155	O Normal	Static binding (elastic)		2	128
	& dvs_VL156-NSXExtra	VLAN access: 156	O Normal	Static binding (elastic)		0	128
	Avs_VL157-NSXF5Mgmt	VLAN access: 157	O Normal	Static binding (elastic)		0	128
	avs_VL158-NSXMgmt	VLAN access: 158	O Normal	Static binding (elastic)		0	128
	A dvs_VL160-Web-Tier-01	VLAN access: 160	O Normal	Static binding (elastic)		0	8
	Avs_VL161-App-Tier-01	VLAN access: 161	O Normal	Static binding (elastic)		0	8
	Avs_VL162-DB-Tier-01	VLAN access: 162	Normal	Static binding (elastic)		0	8
	& dvs_VL20-NSXExternal	VLAN access: 20	O Normal	Static binding (elastic)		1	128
	& dvs_VL31_iSession	VLAN access: 31	Normal	Static binding (elastic)		0	8
	& dvs_VLAN32_iSession	VLAN access: 32	Normal	Static binding (elastic)		0	8
	InfrastructureDV-DVUplinks-42	VLAN trunk: 0-4094	Normal	Static binding		0	4

Figure 7. vSphere DVS VLAN configuration example

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



Create and Deploy DLR

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

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

 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 (+).



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.

New NSX Edge		(?) H
1 Name and description	Name and description	
2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Ready to complete	Install Type: Edge Services Gateway Provides common gateway services such as DHCP, Firewal VPN, NAT, Routing and Load Balancing. (Logical (Distributed) Router Provides Distributed Routing and Bridging capabilities.	
	Name: * NSXDLR-01	
	Back Nert Finish C	ancel

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.

New	NSX Edge		?	+1
/ 1	Name and description	Settings		
2 3 4 5 6	Settings Configure deployment Configure interfaces Default gateway settings Ready to complete	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:		
		Back Next Finish Ca	ncel	



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.

Edit NSX Edge Appliance		?
Specify placement parameters	s for the NSX Edge applian	ice.
Cluster/Resource Pool: *	NSX Computer Cluster	•
Datastore: *	2240-2-10K	•
Host:		•
Folder:		•
	Сок С	ancel

- 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**.

1 Name and description	Configure interfaces				
2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings	Management Connected To	Interface Configurat	tion		Select Remove
6 Ready to complete	IP Address	ment interface is a ma edivity and is configu	andafory special-pr	Subr urpose inte n other inte	net Prefix Length dace that requires daces in the
	Configure int	erfaces of this NSX E	Edge		
	Name	I ⁿ Address	Subnet Prefix Length	Connected	To



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

Connect NSX Edge to a Network	?
Logical Switch	Distributed Portgroup
	🌠 🔍 dvs_v1155
Name	Туре
Avs_VL155_NSXIPPool	Distributed Port Group
M	1 of 2 items
	OK Cancel

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

+ / ×	1			
Primary IP	IP Address			
۲	10.105.155.19	8	OK	Cancel
Subnet prefi	x length: * 24			



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.

					\odot		
1 Name and description	Configure interface	Configure interfaces					
2 Settings 3 Configure deployment	Management Interface Configuration						
A Configure interfaces	Connected To: * d		Change Remove				
5 Default gateway settings	+ / x						
6. Deadu to complete	IP Address	IP Address					
6 Ready to complete	10.105.155.19*			24			
	The management in	nterface is a mandatory s	special-purpose interf	face that requires net	work connectivity an		
	The management ir is configured separ	nterface is a mandatory s ately from other interface	special-purpose interf s in the Logical Route	face that requires net er.	work connectivity an		
	The management in is configured separ	nterface is a mandatory s rately from other interface	pecial-purpose interf s in the Logical Route	face that requires net er.	work connectivity and		
	The management in is configured separ	nterface is a mandatory s ately from other interface as of this NSX Edge	special-purpose interf s in the Logical Route	face that requires net er.	work connectivity and		
	The management in is configured separ Configure interface Name	nterface is a mandatory s iately from other interface es of this NSX Edge	special-purpose interf s in the Logical Route Subnet Prefix Length	face that requires new er. Connected To	work connectivity and		
	The management in is configured separ Configure interface	nterface is a mandatory s ataly from other interface es of this NSX Edge IP Address 20.20.20.2*	Special-purpose interf s in the Logical Route Subnet Prefix Length 24	face that requires net	work connectivity and		
	The management in is configured separ Configure interface	ately from other interface ately from other interface as of this NSX Edge IP Address 20.20.20.2* 10.0.1.1*	Special-purpose interf s in the Logical Route Subnet Prefix Length 24 24	Connected To dvs_VL20-NSXExte dvs_VL160-Web-Ti	work connectivity an ernal ier-01		
	The management in the separation of the management in the separation of the separati	IP Address 20.20.20.2* 10.0.1.1* 10.0.2.1*	Subnet Prefix Length 24 24 24	Connected To dvs_VL20-NSXExte dvs_VL160-Web-Ti dvs_VL161-App-Tit	work connectivity and ernal ier-01		
	The management in is configured separ Configure interface	Iterface is a mandatory stately from other interface ately from other interface as of this NSX Edge 20.20.20.22* 10.0.1.1* 10.0.2.1* 10.0.3.1*	Subnet Prefix Length 24 24 24 24 24	Connected To dvs_VL20-NSXExta dvs_VL160-Web-Ti dvs_VL161-App-Tin dvs_VL162-DB-Tie	work connectivity an smal ler-01 r-01		
	The management in is configured separation Configure interface	Interface is a mandatory stately from other interface as of this NSX Edge 20.20.20.2* 10.0.1.1* 10.0.2.1* 10.0.3.1*	Subnet Prefix Length 24 24 24 24 24	Connected To dvs_VL20-NSXExte dvs_VL160-Web-Ti dvs_VL161-App-Tit dvs_VL162-DB-Tite	work connectivity and smal er-01 er-01		

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.

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



lew NSX Edge		?
 1 Name and description 2 Settings 3 Configure deployment 	Default gateway settings ☑ Configure Default Gateway	
4 Configure interfaces	vNIC: * External	•
5 Default gateway settings	Gateway IP: * 20.20.20.1	
6 Ready to complete	MTU: 1500	
	Back	Finish Cancel

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.

1 Name and description	Ready to complete							
2 Settings								
3 Configure deployment	Name and description	NEVEL D 01						
5 configure deproyment	Name.	NOADER-01	d Deuter					
4 Conligure Internaces	Install type. Logical (Distributed) Router							
5 Default gateway settings	Terrani.	Dischlad						
6 Ready to complete		Disableu						
	Management Interface	Configuration						
	Connected To: dvs_v	L155_NSXIPP00I						
	IP Address				Subnet Prefix			
	10.105.155.19*	24						
	NSX Edge Appliances							
	Resource Pool Host Datastore Folder				er			
	Compute Cluster		2240-2-10K					
	Interfaces							
	Name	IP Address	Subnet Prefix Length	Connected To				
	External	20.20.20.2*	24	dvs_VL20-NSX	External			
	Web-Tier-01	10.0.1.1*	24	dvs_VL160-We	b-Tier-01			
	App-Tier-01	10.0.2.1*	24	dvs_VL161-Ap	p-Tier-01			
	DB-Tier-01	10.0.3.1*	24	dvs_VL162-DB-Tier-01				



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

File Edit View Favorites Tools Help										
vmware vSphere Web Cl	ient 🕈 🖉					ال Adr	ninistrator@VSPHERELOCAL + I	Help +	I Q Search	•
(Home) 🔊 I	NSX Edges									
Networking & Security	NSX Manager: 10.105.155.16	5 -							* 🛐 Recent Tasks	-
🔡 NSX Home	+ × 0 % 0 0	🚳 Actions 👻		🛟 0 Installing 🚸 0 Failer			📡 🔍 Filter	•	All Running	Failed
@ Installation	ld	1 A Name	Туре	Version	Status	Tenant	Interfaces	Size		
Sector Switches	edge-3	Topo1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp		
NSX Edges	edge-4	Topo1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp		
Firewall										
Real SpoolGuard										
🌼 Service Definitions										
Service Composer										
🔞 Data Security										
Flow Monitoring									My Tasks 🔻	Nore Tasks
Activity Monitoring										
 Networking & Security Inventory 									 Work in Progres 	/S 🗆
NSX Managers 🛛 🚺 >										

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 <u>http://support.f5.com</u> and consult the appropriate Implementation guide for your version and device.

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.

File Edit View Favorites Tools H	Help		
Hosiname: bd5000.bd.f5.com Date: F IP Address. 10.105.155.17 Time. 2	fer Feb 19,2015 Ultour admin ne 214 PM (PST) Rule Administration Partition	Common 🗸	Logost
Standalone			
Main Help About	Network in VLANE: VLAN List		
Statistics	e . VAN List VLAN Greeps		
iApp			Chate
E Local Traffic	✓ ▲ Name © Application © Tag Untagged Interfaces	Tagged Interfaces	Partition / Path
	No records to display.		
Acceleration	Delete		
Device Management			
Network			
Interfaces >			
Routes 💿	⊙ — •		
Self IPs			
Packet Filters			
Spanning Tree			
Trunks			
Tunnels			
Route Domains (+)			
VLANS .			
ARP			

- 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.

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



CONLINE (ACTIVE) Standalone		
Main Help About	Network » VLANs : VLAN L	Jst » New VLAN
Ma Statistics		
	General Properties	
iApps	Name	External
Local Traffic	Description	
	Tag	20
Acceleration	lay	20
Device Management	Resources	
	-	Interface: 1.2 🗘
Network		Tagging: Tagged 🗘
Interfaces		Add
Routes 📀	Interfaces	1.1 (tagged)
Self IPs 📀		
Packet Filters		
Trunks		Edit Delete
Tunnels	Configuration: Basic	9
Route Domains 📀	Source Check	
VLANs	мти	1500
Class of Service		
ARP	sFlow	
IPsec >	Polling Interval	Default Value: 10 seconds
WCCP 📀	Sampling Rate	Default 😋 Default Value: 2048 seconds
DNS Resolvers	Cancel Repeat Finished	
। ड्राङ्		

- 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.

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



Netw	Network » VLANs : VLAN List								
.⇔	VLAN List	VLAN Groups							
								Create	
	Name			Application	▲ Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path	
	External				20		1.1	Common	
	Neb-Tier				160		1.1	Common	
	App-Tier				161		1.1	Common	
Delet	e								

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.

- 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.

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



File Edit View Favorites Tools H	lelp	
Hostname: bd5000.bd.f5.com Date: F IP Address: 10.105.155.17 Time: 2	eb 19, 2015 User: admin 16 PM (PST) Role: Adminis	itrator
ONLINE (ACTIVE) Standalone	Loading Receiving config	juration data from your device.
Main Help About	Network » Self IPs »	lew Self IP
Statistics	Configuration	
iApp	Name	ExtSetfIP
Local Traffic	IP Address	20 20.20.10
Acceleration	Netmask	255.255.255.0
Device Management	VLAN / Tunnel	External
Device management	Port Lockdown	Allow None
Network	Traffic Group	Inherit traffic group from current partition / path
Interfaces		traffic-group-local-only (non-floating)
Routes 🕑	Cancel Repeat Finish	ed
Self IPs 📀		
Packat Filters		

- 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.

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



Hostname: bd5000.bd.f5.com Date: IP Address: 10.105.155.17 Time:	Mar 18, 2015 User: admin 3:19 PM (PDT) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About	Network » Self IPs » New Se	əlf IP
Mage Statistics		
	Configuration	
Ligi IApp	Name	WebSelf
Local Traffic	IP Address	10.0.1.2
Acceleration	Netmask	255.255.255.0
	VLAN / Tunnel	Web-Tier
	Port Lockdown	Allow None
Network	Traffic Group	Inherit traffic group from current partition / path
Interfaces	•	
Routes 📀	Cancel Repeat 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.

Netwo	ork » Self IPs						
‡-	Self IP List						
							Create
•	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
	AppSelf		10.0.2.2	255.255.255.0	App-Tier	traffic-group-local-only	Common
	ExtSelfIP		20.20.20.10	255.255.255.0	External	traffic-group-local-only	Common
🗆 V	VebSelf		10.0.1.2	255.255.255.0	Web-Tier	traffic-group-local-only	Common
Delete	e						

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.

- 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.

File Edit View Favorites Tools He	lp			
Hostname: bd5000.bd.f5.com Date: Fe IP Address: 10.105.155.17 Time. 2:	b 19, 2015 User: admin 17 PM (PST) Role: Administrato			
CONLINE (ACTIVE) Standalone				
Main Help About	Network » Routes » New I			
Statistics	Properties			
iApp	Name	default		
Local Traffic	Description			
Acceleration	Destination	0.0.0.0		
Device Management	Netmask	0.0.0.0		
better management	Resource	Use Gateway		
Network	Gateway Address	IP Address 20/20.20.1 ×		
Interfaces >	мти	0		
Routes 📀				
Self IPs 📀	Cancel Kepeat Finished			
Packet Filters				
Conserving Trees				



The completed routing configuration should resemble the configuration below.

Network	Network » Routes							
‡:- ₹	oute List							
		_						
								Add
💌 🗢 N:	ame	+ Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
🗌 defa	ult		Default IPv4		Partition Default Route Domain	Gateway	20.20.20.1	Common
Delete	1							

Application Configuration

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

Create application pools

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

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



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

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

Table 9. BIG-IP web tier pool members

File Edit View Favorites Tools He	lp	
Hostname: bd5000.bd.f5.com Date: Fe IP Address: 10.105.155.17 Time: 21	b 19, 2015 User: admin 18 PM (PST) Role: Administrato	
Standatone	Local Traffic Books : Dool	List New Dool
Main neip About	Local Hallic » Pools Pool	LISE 3. NEW POOLss.
Statistics	Configuration: Basic V	
iApp	Name	WebServerPool
Local Traffic	Description	
Network Map		Active Available
Virtual Servers	Health Monitors	gateway_icmp <
Policies		►>> https https_443
Profiles		
iRules	Resources	
Pools	Load Balancing Method	Round Robin
Nodes	Priority Group Activation	Disabled
Monitors 📀		Node Name: (Optional)
Traffic Class 📀		Address: 10.0.1.12
Address Translation		Service Port 80 HTTP
DNS Express Zones	New Members	Add
DNS Caches		R:1 P:0 C:0 10.0.1.12 10.0.1.12 :80
Acceleration		Edt Delete
Device Management	Cancel Repeat Finis ed	
Retwork	24	

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



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

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

Table 10. BIG-IP application tier pool members

File Edit View Favorites Tools Hel	p	
Hosiname: bd5000.bd.f5.com Date: Fel IP Address: 10.105.155.17 Time: 3.5	b 19, 2015 User: admin 1 PM (PST) Role: Administrator	
ONLINE (ACTIVE) Standaione	Receiving configurati	on data from your device.
Main Help About	Local Traffic » Pools : Pool	List » New Pool
Statistics	Configuration: Basic 🔽	
iApp	Name	AppServerPool
Coral Traffic	Description	
Network Map		Active Available
Virtual Servers >	Health Monitors	gateway_icmp ss inband A
Policies >		tcp_half_open v
Profiles	Beeguraan	
Pools	Load Balancing Method	Round Robin
Nodes	Priority Group Activation	Disabled
Monitors (+)		
Traffic Class 🕘		Node Name: (Optional)
Address Translation		Address: 10.0.2.12
DNS Express Zones	New Members	Service Port: 80 HTTP V
DNS Caches	New Manuers	R1 P0 C0 10 02 11 10 0 2 11 80
Acceleration		
Device Management		Edt Delete
Network	Cancel Repeat Finished	



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

Local	Local Traffic » Pools : Pool List							
₩ -	Pool List		Statistics	Ø				
*				Sear	ch			Create
	Status	 Name 				Application	Members	Partition / Path
	0	AppServe	rPool				2	Common
	0	WebServe	erPool				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.

- 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.

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



File	Edit View Favorites Tools Hel	þ	
Host	name: bd5000.bd.f5.com Date: Fel	b 19, 2015 User: admin 3 PM (PST) Role: Administrator	
	Standalone		
M	ain Help About	Local Traffic » Virtual Server	s : Virtual Server List » New Virtual Server
2	Statistics		
	App	General Properties	Web-Vin
60	Local Traffic	Description	
	Network Map	Туре	Standard
	Virtual Servers	Source	
	Policies >		Type: I Host O Network
	Profiles	Destination	Address: 20.20.20.5
	iRules >	Service Port	80 HTTP V
	Pools >	State	Enabled V
	Nodes >	Continuentions Basic	là.
-	Monitors (+)	Source Address Translation	Auto Man X
			L and sold
		Content Rewrite	None
		HTM Profile	Nana V
		FTIME FTONS	
		Acceleration	
		Rate Class	None
		OneConnect Profile	None
		NTLM Conn Pool	None 🗸
I.		HTTP Compression Profile	None
		Web Acceleration Profile	None
		SPDY Profile	None 🗸
		Resources	
			Enabled Available
		Defer	
		incluines	Sys_auth_ssl_ocsp Sys_auth_ssl_ocsp
			Up Down
			Enabled Available
		Policies	sys CEC video_policy
			22
		Default Pool	WebServerPool
		Default Persistence Profile	None
		Fallback Persistence Profile	None
		Conset Depend Finisherd	
		Cancer [Repear] [Finished]	



The image has been cropped to highlight the specific configuration.

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

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

Local	Local Traffic » Virtual Servers : Virtual Server List									
	Virtual S	erver List	Virtual Address List	Statistics	-					
*			Sea	rch		-				Create
	 Status 	 Name 			Application	Destination	Service Port	Type	Resources	Partition / Path
	0	App-Vip				10.0.1.5	80 (HTTP)	Standard	Edit	Common
	0	Web-Vip				20.20.20.5	80 (HTTP)	Standard	Edit	Common
Enabl	le Disab	le 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.

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



Local Traffic » Network Map	
🔅 👻 Network Map	
Status Any Status 🗸 Type All Types 🗸	Search * Search iRule Definition
Show Summary Update Map	
Local Traffic Network Map	
App-Vip	O Web-Vip
App ServerPool	O WebServerPool
10.0.2.11:80	10.0.1.11:80
10.0.2.12:80	0 10.0.1.12:80
1	

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



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



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



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

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





Figure 9. add caption

Implementation Infrastructure

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

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



Figure 10. vSphere console



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

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

Prerequisites

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

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

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

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

Note: In our environment, we put the F5 BIG-IP management interface on the VLAN128untaggd 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.

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.



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 (+).

vmware [®] vSphere Web Cl	ient 🔒 🗗
Home 🕨 🔊 🖡	NSX Edges
Networking & Security	NSX Manager: 10.105.134.165 🛛 🔻
🕂 NSX Home	+
🎯 Installation	ld N
💁 Logical Switches	1.
NSX Edges	
👸 Firewall	
ng SpoofGuard	
뿾 Service Definitions	
/ Service Composer	
🗿 Data Security	
🙀 Flow Monitoring	
Activity Monitoring	
✓ Networking & Security Inventory	
😽 NSX Managers 🛛 🚺 🔪	

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

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



New NSX Edge		? •
1 Name and description	Name and description	
 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Firewall and HA 	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. 	
7 Ready to complete	Name: * NSXEdge Hostname: Description: Tenant:	
	Back Next Finish Ca	ncel

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

Nev	v NSX Edge	3 »
~	1 Name and description	Settings
	 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Firewall and HA 7 Ready to complete 	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: admin P
		Back Next Finish Cancel

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



 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.

New NSX Edge				(*)
 1 Name and description 	Configure deployme	nt		
✓ 2 Settings	Datacenter	910	1	
3 Configure deployment	Appliance Size:	O Compact)	
4 Configure interfaces	0	Large		
5 Default gateway settings		X-Large		
6 Firewall and HA	_) Quad Large		
7 Ready to complete	Deploy NSX Edg	e		
	Select this option to interface configurati	create a new NSX E on is mandatorv to d	dge in deployed mo eplov the NSX Edae	de. Appliance and
	NCV Edge Appliance	-		
	NSX Edge Appliance	es		
	Resource Pool	Host	Datastore	Folder
	USSJ-55-Comp		2240-2-10K	
	Specifying a recourt	a nool and datastor	o is mandatory for co	onfiguring the NSY
	Edge appliance.	e poor and datastor	e is mandatory for co	uinguning the NSA
		Back	Next	-inish Cancel

 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.

pecify placement parameter	s for the NSX Edge appliar	nce.
Cluster/Resource Pool: *	NSX Computer Cluster	•
Datastore: *	2240-2-10K	•
Host:		
Folder:		



 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	Туре	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

Connect NSX Edge to a Network ?				
Logical Switch	Standard Portgroup		Distributed Portgroup	
		📡 🖸	l dvs_vl20 ▼	
Name		Туре		
💿 🟯 dvs_VL20-N	ISXExternal	Distribu	uted Port Group	
м			1 of 32 items	
			OK Cancel	

 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.

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



Primary IP	IP Address			
۲	17.16.1.1	0	ок	Cancel

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.

INC	ew NSX Edge				?	
~	1 Name and description	Default gatew	ay settings	in a carain bain in		
/	2 Settings 3 Configure deployment	Configure Default Gateway				
~	4 Configure interfaces	vNIC: *	External	•		
	5 Default gateway settings	Gateway IP: 🕴	20.20.20.1			
	6 Firewall and HA	MTU:	1500			
	7 Ready to complete					

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



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



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





Create and Deploy DLR

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

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

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


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.

New NSX Edge		€ €
1 Name and description	Name and descriptio	n
2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Ready to complete	Install Type: Provi NAT, • Lo Provi	ige Services Gateway des common gateway services such as DHCP, Firewall, VPN, Routing and Load Balancing. gical (Distributed) Router des Distributed Routing and Bridging capabilities.
	Name: * NSX Hostname: Description: Tenant:	DLR
		Back Next Finish Cancel

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

Ne	w	NSX Edge		?	**
~ (1 3 4 5 6	Name and description Settings Configure deployment Configure interfaces Default gateway settings 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:		
			Back Next Finish Ca	ncel	



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

Specify placement parameters	for the NSX Edge appliar	ice.
Cluster/Resource Pool: *	NSX Computer Cluster	•
Datastore: *	2240-2-10K	•
Host:		•
Folder:		•

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

					\bigcirc
1 Name and description	Configure in	terfaces			
2 Settings	Managemen	t Interface Configura	tion		
4 Configure interfaces	Connected T	0: *			Select Remove
5 Default gateway settings	🛉 / ×				
6 Ready to complete	IP Address			Subr	net Prefix Length
	network conn Router. Configure in	ectivity and is configu terfaces of this NSX	red separately from	n other inter	faces in the Logica
	network conn Router. Configure in	ectivity and is configu terfaces of this NSX	red separately from	n other inter	faces in the Logica
	network conn Router. Configure in Mame	terfaces of this NSX	Edge Subnet Prefix Length	Connected	faces in the Logica
	network conm Router. Configure in P	terfaces of this NSX	Edge Subnet Prefix Length	Connected	faces in the Logica
	network conm Router. Configure in P // X Name	terfaces of this NSX	Edge Subnet Prefix Length	Connected	faces in the Logica
	network conn Router.	terfaces of this NSX	Edge Subnet Prefix Length	Connected	faces in the Logica
	network conn Router. Configure in Ame	terfaces of this NSX IP Address	Edge Subnet Prefix Length	Connected	faces in the Logic



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

Connect NSX Edge to a Network						
Logical Switch	Distributed Portgroup					
	🌠 🔍 dvs_vl155					
Name	Туре					
Avs_VL155_NSXIPPool	Distributed Port Group					
84	1 of 2 items					
	OK Cancel					

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

Add Subnet		?				
Specify the IP	addresses in the subnet: *					
🕈 🥖 🗙 Primary IP	IP Address					
•	10.105.155.22	OK Cancel				
Subnet prefix length: * 24						
		OK Cancel				



 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	Туре	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				(?)			
 1 Name and description 	Configure interfaces						
 2 Settings 3 Configure deployment 4 Configure interfaces 	Management Inter	Change Remove					
5 Default gateway settings	IP Address			Subnet Prefix Length			
o Ready to complete	10.105.155.22*			24			
	The management interface is a mandatory special-purpose interface that requered network connectivity and is configured separately from other interfaces in the Logical Router.						
	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**.



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.

N	ew	NSX Edge			?	⊧⊧
> > > >	1 2 3 4	Name and description Settings Configure deployment Configure interfaces	Default gatewa	y settings lefault Gateway TransitNet		-
	5	Default gateway settings Ready to complete	Gateway IP: * MTU:	172.16.1.1 1500		
				Back Next Finish Can	cel	D,

 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.

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



1 Name and description								
· · · · · · · · · · · · · · · · · · ·	Ready to complete	Ready to complete						
 2 Settings 3 Configure deployment 4 Configure interfaces 5 Default gateway settings 6 Ready to complete 	Name and description Name: NSXDLR Install Type: Logical (Distributed) Router Tenant: HA:							
	Management Inter Connected To: d	f <mark>ace Configuratio</mark> Ivs VL155 NSXIP	n 'Pool					
	IP Address				Subnet Prefix Lenoth			
	10.105.155.22*				24			
	NSX Edge Applianc	es						
	Resource Pool	Host	Datastore	Folder				
	USSJ-55-Compi		2240-2-10K					
	Interfaces							
	Name	IP Address	Subnet Prefix Length	Connected	i To			
	TransitNet	172.16.1.2*	24	TransitN	et-1			
	Web-Tier-01	10.0.1.1*	24	Web-Tie	r-01			
	App-Tier-01	App-Tier-01 10.0.2.1* 24 App-Tier-0						
	DB-Tier-01	10.0.3.1*	24	DB-Tier-	01			

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

File Edit View Favorites Tools I	Help									
vmware [,] vSphere Web C	lient 🕈 🖉					t ا م	ministrator@VSPHERE.LOCAL + I	Help +	I Q Search	
(Home) 🔊 🖡	NSX Edges									Ŧ
Networking & Security	NSX Manager: 10.105.155.16	5 🔻							• 🛐 Recent Tasks	-
NSX Home	+ × C % 0 🗉	i Actions ◄		🛟 0 Installing 👍 0 Failed	d		📡 🔍 Filter	•	All Running	Failed
Se Installation	Id	1 A Name	Туре	Version	Status	Tenant	Interfaces	Size		
Sector Switches	edge-3	Topo1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp		
NSX Edges	edge-4	Topo1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp		
SpoolGuard								_		
Service Definitions										
Service Composer										
🚳 Data Security										
📻 Flow Monitoring									My Tasks 🔻	More Tasks
Activity Monitoring									* Work In Dronto	
 Networking & Security Inventory 									- WORK IN Progre	00 []
NSX Managers										



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.

File Edit View Favorites Tools Help										
VmtWare' vSphere Web Client 🕈 🖉 🛛 🕹 🕹 🖉										•
(Home) 🔊 I	NSX Edges									*
Networking & Security	NSX Manager: 10.105.155.165	•							• 🛐 Recent Tasks	-
H NSX Home	🔶 🗙 😅 💺 🛞 🗎 🗎	🎯 Actions 👻		🛟 0 Installing 🚸 0 Failed			📡 🔍 Filter	•	All Running	Failed
@ Installation	ld 1	A Name	Туре	Version	Status	Tenant	Interfaces	Size		
State Logical Switches	edge-3	Topo1ESG	NSX Edge	6.1.1	Deployed	Default	3	Comp		
🗮 NSX Edges	edge-4	Topo1DLR	Logical Router	6.1.1	Deployed	Default	5	Comp		
Firewall										
R SpoolGuard										
🌼 Service Definitions										
Service Composer										
🚳 Data Security										
Flow Monitoring									My Tasks 👻 🛛 🕅	fore Tasks
Activity Monitoring										
 Networking & Security Inventory 									 Work In Progress 	s 🗆
NSX Managers 📰 🗦										

 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.

File Edit View Favorites Tools H	elp			
vmware [,] vSphere Web Cl	ent 🕈 🖉	A		
4 Networking & Sec 🕨 🕤 🕱	Topo1ESG Actions +			
Topo1ESG	Summary Monitor Manage			
	Settings Firewall DHCP NAT	Routing Load Balancer	VPN SSL VPN-Plus	Grouping Objects
	Global Configuration	<u>5</u> ∕×	Network	
	Static Routes			
	OSPF BGP IS-IS Route Redistribution			

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**.

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



Add Static Route)	?
Network: *	10.0.0/16 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 Cance	el

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

vmware [®] vSphere Web Cl	ient 🔒 🖗			Upda	ated at 12:11 PM 💍	Administrator@	/SPHERE.LOCAL - Help -
Networking & Sec Sec	NSXEdge Actions -						
NSAEdge	Summary Monitor Manage Settings Firewall DHCP NAT Routing Load Balancer VPN SSL VPN-Plus Gn 44 Changes to the Static Routing configuration Changes to the Static Routing configuration will tak to publish. Static Routes Publish Changes Revert				after being published. F	Please click on "Pu	blish Changes"
	OSPF	ቀ / ×					Q Filter
	IS-IS	Туре	Network	Next Hop	Interface	MTU	Description
	Route Redistribution		10.0.0/16	172.16.1.2	TransitNet-1	1500	

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



BIG-IP Appliance Configuration

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

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-ve-setupvmware-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-deviceservice-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 <u>http://support.f5.com</u> 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.

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



vmware [®] vSphere Web Cli	ient 🔒 🗗				Updated at 3:17 P
VCenter	NSXBigIP Actions -				
	Summary Monitor Manage R Settings Alarm Definitions Tags	Related Objects Permissions VM Sto VM Hardware VM Sto > CPU > Memory > Hard disk 1 > Hard disk 2 > Network adapter 1 > Network adapter 2 > Network adapter 3 > Network adapter 4 > Video card	2 CPU(s), 418 2 CPU(s), 418 4096 MB, 4 20 GB 104 GB VLAN128-untr VM Network VM Network 4 MB Additional Har	Scheduled Tasks Scheduled Tasks MHz used 122 MB used 122 MB used (connected) (connected) (connected) (connected)	vServices
▶ □ ussj-vcd511-1 □ vCAC		Compatibility	207220714.0		NOT 7)

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.

 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).

vmware [®] vSphere Web Cl	ient 🔒 🗗			Updated at 3:17 PM 💍 Adm	ninistrator@VSPHERE.LOCAL -	Help 🗸		
Home 🕨 🐑 🖡	Logical Switches							
Networking & Security	NSX Manager: 10.105.134.165	K Manager: (10.105.134.165 🛛 💌						
tome NSX Home	+ 🕢 🗙 🖬 🗞 🖽 🗄	Actions 👻			📡 🔍 Filter	•		
installation	Name	. Statue	Transport Zone	Segment ID	Control Plane Mode	Descript		
🌺 Logical Switches	Add Virtual M		TransportZone1	5000	Unicast			
NSX Edges	NB-Tier-01	O Normal	TransportZone1	5002	Unicast			
📑 Firewall	n TransitNet-1	O Normal	TransportZone1	5013	Unicast			
न SpoofGuard	http://www.com/com/temperature/com/tem	Normal	TransportZone1	5014	Unicast			
🗒 Service Definitions	🐏 WebNet	O Normal	TransportZone1	5001	Unicast			
Service Composer	💁 Web-Tier-01	📀 Normal	TransportZone1	5003	Unicast			
Data Security						_		
🔣 Flow Monitoring								
ktivity Monitoring								
✓ Networking & Security Inventory								
🔠 NSX Managers 🛛 🚺 🗦								

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.

🧏 Web-Tier-01 - Add Virtual Machine	25	(?) ₩
1 Select Virtual Machines 2 Select vNICs	Select Virtual Machines Select VMs to connect to this network	
3 Ready to complete	Filter (2)Selected Objects	
	📡 (Q nsx	•
	Virtual Machine	
	NSXBigIP2	
	nsx-web-sv-01a	
	Mi 4	of 96 Objects
	Back Next Finish	Cancel

- 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.

💯 Web-Tier-01 - Add Virtual Machines							
 1 Select Virtual Machines 2 Select vNICs 	Select vNICs Select at least one vnic for each virtual machine you want to connect to this network.						
3 Ready to complete							
	Name	Network					
		NSXBigIP2 - Network adapter 4 (VM Network)					
		NSXBigIP2 - Network adapter 1 (VM Network)					
	MSXBIGIP2	SXBigIP2 - Network adapter 2 (VM Network)					
		NSXBigIP2 - Network adapter 3 (VM Network)					
		VSXBigIP - Network adapter 2 (VM Network)					
		NSXBigIP - Network adapter 3 (VM Network)					
		NSXBigIP - Network adapter 1 (VLAN128-untagged)					
		SXBigIP - Network adapter 4 (VM Network)					
4		::					
		Back Next					

- 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.



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

NSXBigIP Actions -						
Summary Monitor Manage Related Objects						
Settings Alarm Definitions Tags	Permissions VM Sto	rage Policies Scheduled Tasks vServices				
44	VM Hardware					
VM Hardware	▶ CPU	2 CPU(s), 0 MHz used				
VM Options	Memory	4096 MB, 0 MB used 20 GB 104 GB				
vApp Options	▶ Hard disk 1					
NSX Activity Monitoring	▶ Hard disk 2					
	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

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

File Edit View Favorites Tools Hi	Is Help								
Hosiname: bd5000.bd.f5.com Date: F IP Address: 10.105.155.17 Time. 2	Nacionas M0000M Kom Die fra 19.2015 Unor abbie Pactione II de State 11.015 The 21.414 (25.71) Biel Andreamistate Pactione II de State 11.015 The 21.414 (25.71) Biel Andreamistate								
Standalone									
Main Help About	Metwork w VIANS : VLAN List								
Statistics	O - VLAN List VLAN Groups								
IApp		(C) sate.							
E Local Traffic	V • Name	Application Tag Untagged Interfaces Tagged Interfaces Partition / Path							
Acceleration	No records to display.								
Acceleration	Delete								
Device Management									
Retwork									
Interfaces >									
Routes	⊙ ⊗ — ∘								
Self IPs									
Packet Filters									
Spanning Tree									
Tunnels									
Route Domains (+)									
VLANS ,									



- 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.
- 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.

Hostna IP Add	ame: nsxbigip1.bd.f5.com Iress: 172.30.128.16	Date: Feb 27, 2015 Time: 3:52 PM (PST)	: Feb 27, 2015 User: admin : 3:52 PM (PST) Role: Administrator				
ſ	ONLINE (ACTIVE) Standalone						
Ma	in Help Ab	Network	» VLANs : VLAN List	» New VLAN.	•		
Maga S	tatistics	Conorol	Proportion				
🔜 i/	Apps	Nome	roperties	Mah TiarOd			
		Name		webilerui			
5 D	NS	Descript	ion				
D: L	ocal Traffic	Tag					
🦳 A	cceleration	Resource	Resources				
Device Management					Interface: 1.2 ¢ Tagging: Untagged ¢		
<u> </u>	etwork	Interface	Interfaces		1.1 (untagged)		
	Interfaces	E.					
	Routes	(+)					
	Self IPs	 Image: Image: Ima			Edit Delete		
	Packet Filters	Configura	ation: Basic 🜲				
	Trunks	Source (Check	0			
	Tunnels	мти		1500			
	Route Domains	÷					
	VLANs	sFlow			2		
	Class of Service	Polling I	nterval	Default 🗘	Default Value: 10 seconds		
	ARP	Samplin	g Rate	Default \$	Default Value: 2048 seconds		
	IPsec	Cancel	Repeat Finished				

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



- 7. Click Repeat to continue.
- 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.

Netv	Network » VLANs : VLAN List								
*	, VLAN List	VLAN Groups							
•			Search						Create
	▲ Name			Application	≑ Tag	Untagged Interfaces	Tagged Interfaces	≑ Parti	tion / Path
	AppTier01				4093	1.2		Commo	on
	HANet				4092	1.3		Commo	on
	WebTier01				4094	1.1		Commo	on
Dele	te								

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.

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





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

Hostname: r IP Address: 1	nsxbigip1.bd.f5.0 172.30.128.16	com Date Time	: Feb 27, 2015 :: 4:04 PM (PST)	User: admin Role: Administrator	
	ONLINE (ACT Standalone	rive)			
Main	Help	About			
Magazina Statistic	cs				
_			Redundant D	Device Wizard Optio	ns
iApps			Config Sync	;	Display configuration synchronization options
S DNS			High Availab	bility	 Display failover and mirroring options Failover Method: Network
Local T	raffic		Cancel N	lext	



- 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: Fe IP Address: 172.30.128.16 Time: 4:0	b 27, 2015 User: admin 05 PM (PST) Role: Administr	ator
ONLINE (ACTIVE) Standalone		
Main Help About		
Statistics	Internal Network Configurat	ion
iApps	Internal VLAN	Create VLAN internal O Select existing VLAN
	Select VLAN	WebTier01 \$
Local Traffic	Self IP	Address: 10.0.1.8 Netmask: 255.255.255.0 Port Lockdown: Allow Default \$
Device Management	Floating IP	Address: 10.0.1.13 Port Lockdown: Allow Default \$
Network	Internal VLAN Configuration	
Svetem	VLAN Name	WebTier01
BT Oysten	VLAN Tag ID	4094
	Interfaces	VLAN Interfaces 1.2 Tagging: Select Add 1.1 (untagged) Edit Delete
	Cancel Next	



- 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: Fe IP Address: 172.30.128.16 Time: 4:0	eb 27, 2015 User: admin 09 PM (PST) Role: Administrator	
ONLINE (ACTIVE) Standalone		
Main Help About		
Mag Statistics	External Network Configuration	
iApps	External VLAN	Create VLAN external Select existing VLAN
C DNS	Select VLAN	AppTier01 \$
Local Traffic	Self IP	Address: 10.0.2.8 Netmask: 255.255.255.0 Port Lockdown: Allow None
	Default Gateway	
Device Management	Floating IP	Address: 10.0.2.13 Port Lockdown: Allow None \$
System	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	



- 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.comDate:FeIP Address:172.30.128.16Time:4:	b 27, 2015 User: admin 10 PM (PST) Role: Administrator			
ONLINE (ACTIVE) Standalone				
Main Help About				
Statistics				
	High Availability Network Config	uration		
iApps	High Availability VLAN	Create VLAN HA Select existing VLAN		
S DNS	Select VLAN	(HANet 🗘		
<u></u>	CalfulD	Address: 10.254.1.8		
Local Traffic	Sell IP	Netmask: 255.255.255.0		
Acceleration	High Availability VLAN Configura	ation		
Device Management	VLAN Name	HANet		
Alabuark	VLAN Tag ID	4092		
Network		VLAN Interfaces 1.1 \$		
System		Tagging: Select \$		
		Add		
	Interfaces	1.5 (untagged)		
		Edit Delete		
	Cancel Next			



10. 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: 10.105.134.20 Add 10.105.134.20 Edit Delete				
Cancel 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 Configurat	ion
DNS Lookup Server List	Address: 10.105.134.20 Add 10.105.134.20 Edit Delete Up Down
BIND Forwarder Server List	Address: Add Edit Delete Up Down
DNS Search Domain List	Address: Add localhost Edit Delete Up Down
DNS Cache	
IP Version	IPv4 V
Cancel Next	



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

Config Sync 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					
Local Address		\Rightarrow VLAN			
10.254.1.9	1026	HANet			
Delete					
Failover Multicast Configuration					
Use Failover Multicast Address					
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.





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

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.

Hostname: nsxblgip2.bd.f5.com Date: IP Address: 172.30.128.17 Time:	Feb 27, 2015 User: admin 5.05 PM (PST) Role: Administrator Partition: Common C Log out
I ONLINE (ACTIVE) Standalone	
Main Help About	
Ma Statistics	
	Discover Configured Peer Device
IApps	If you have already configured a peer device for this active/standby pair, click Next to discover this peer. The system will establish trust, create a device group, sync addresses used for ConfigSync and high availability, and create a traffic group that supports active/standby configuration.
S DNS	Next
Local Traffic	Confirme Data Davia
Acceleration	Compare rear 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.
Device Management	Finished

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.

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



Hostname: nsxbigip2.bd.f5.com IP Address: 172.30.128.17	Date: Feb 27, 2015 Time: 5:06 PM (PST)	User: admin Role: Administrator			
ONLINE (ACTIVE) Standalone					
Main Help Abo	out				
Mage Statistics					
	Remote Dev	Remote Device Credentials			
iApps	Device IP /	Address	172.30.128.16		
S DNS	Administra	tor Username	admin		
Local Traffic	Administra	tor Password	•••••		
Acceleration	Cancel	letrieve Device Informat	ion		
Device Management					

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

Hostname: nsxbigip2.bd.f5.com Date: File IP Address: 172.30.128.17 Time: 5:	eb 27, 2015 User: admin 08 PM (PST) Role: Administrato	
ONLINE (ACTIVE) Standalone		
Main Help About		
Mage Statistics		
-	Remote Device Credentials	
IApps	Device IP Address	172.30.128.16
S DNS	Administrator Username	admin
Local Traffic	Administrator Password	****
Acceleration	Device Certificate	
	Subject	/C=/ST=WA/L=Seattle/O=MyCompany/OU=MyOrg/CN=localhost.localdomain/emailAddress=root@localhost.localdomain
Device Management	Management IP Address	172.30.128.16
Network	Expiration	IF Sun Feb 21 18:10:23 PST 2025
I HELWOIK	Serial Number	b1b09f483e9fa775
System	Signed	Yes
	SHA-1	c62c456cc6ebad0c7af2cc390f9bd27ba7bd7b17
	MD5	a63efc4ba6baaa250837730f480e463f
	Device Properties	
	Name	nsxbigip1.bd.f5.com
	Sync-Failover Group Properties	S
	Name	device-group-failover-ad2f4f99ef90
	Cancel Finished	



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



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

Hostname: IP Address:	nsxbigip2.bd.f5.co 172.30.128.17		ate: Feb 27, 2 ime: 5:28 PM (015 U: (PST) Ri	ser: admin ble: Administrator				Partition: Common	Cog out
6	ONLINE (ACTI Awaiting Initial	VE) I Sync								
Main	Help	About	Dev	ice Manage	ment » Overview					
Magazina Statisti	cs		*	 Overview 	,					
iApps			Dev	ice Groups						
S DNS			÷ 1	Name			Number of Devices	Device Group Type	Sync Type	
Local T	raffic		dev	/ice-group-fa	ilover-ad2f4f99ef90	Awaiting Initial Sync	2	Sync-Failover	Manual	
0			dev	vice_trust_gr	oup	•	2	Sync-Only	Auto	
Accele	ration			Sync Summ	ary Status Awa	iting Initial Sync				
Device	Management				Summary The	device group is awaiting the initial co	nfig sync			
Over	rview				Details Reco	ommended action: Synchronize one	of the devices to the group			
Devi	ces		De	evices						Show Advanced View
Devi	ice Groups		Ð	HA Status	▲ Name		Sync Status		Configuration Time	
Devi	ice Trust		, 9	<u>o</u> .	nsxbigip1.bd.f5.c	com	Awaiting Initial Sync		no value set	
Traff	fic Groups		0	~	nsxbigip2.bd.f5.c	com (Self)	Awaiting Initial Sync		no value set	
Networ	14		S) 0 1 1	ync Options Sync Devic Sync Group Overwrite C Sync	e to Group o to Device ionfiguration					

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

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



	i:30 PM (PST) Role: Administrator				Partition: Common	Log out
ONLINE (ACTIVE)						
Main Help About	Device Management » Overview					
Mage Statistics	🔅 🚽 Overview					
iApps	Device Groups					
S DNS	Name		Number of Devices	Device Group Type	Sync Type	
Terr Local Traffic	device-group-failover-ad2f4f99ef90	•	2	Sync-Failover	Manual	
	device_trust_group	0	2	Sync-Only	Auto	
Acceleration Device Management	Sync Summary Status In S Summary All o Details	ync levices in the device group are in	sync			
Uverview						
Devices	Devices				Show Advan	ced View
Devices Device Groups	HA Status Anne		Sync Status	Configuratio	Show Advan	ced View
Devices Device Groups	HA Status A Name nsxbigip1.bd.f5.	com	 Sync Status 	© Configuratio 2/27/2015 17:3	Show Advan n Time 10:08	ced View
Devices Device Groups Device Trust Traffic Groups	Devices HA Status Name Image: state of the state	com com (Self)	 Sync Status 	Configuratio 2/27/2015 17:3 2/27/2015 17:3	Show Advan n Time 30:08 30:08	ced View

Application Configuration

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

Create application pools

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

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



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

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

Table 15. BIG-IP web tier pool members

File Edit View Favorites Tools	Help			
Hosiname: bd5000.bd.f5.com Dale: IP Address: 10.105.155.17 Time:	Feb 19, 2015 User: admin 2:18 PM (PST) Role: Administratic			
ONLINE (ACTIVE) Standaione	Local Traffic Boole - Doo			
Ctatistics	Local Hume // Pools Poo			
Jausues	Configuration: Basic V	J		
iApp	Name	WebServerPool		
Local Traffic	Description			
Network Map		Active Available		
Virtual Servers	Health Monitors			
Policies	>	Intp_nead_t5 Intps		
Profiles		nups_443		
iRules	Resources			
Pools	Load Balancing Method	Round Robin		
Nodes	Priority Group Activation	Disabled		
Monitors (+)		Node Name: (Optional)		
Traffic Class 📀		Address: 10.0.1.12		
Address Translation		Service Port: 80 HTTP V		
DNS Express Zones	New Members	Add		
DNS Caches	>	R:1 P:0 C:0 10.0.1.11 10.0.1.12 80		
Acceleration		Edit Delete		
Device Management	Cancel Repeat Finisted			
Network				



- 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

File Edit View Favorites Tool Hosiname: bd5000.bd.f5.com D	s Help ale: Feb	19, 2015 User: admin	
IP Address: 10.105.155.17 Ti ONLINE (ACTIVE) Standalone		PM (PST) Role: Administrato	r Ion data from your device.
Main Help Abou	t	Local Traffic » Pools : Pool	I List » New Pool
Statistics		Configuration: Basic 🔽	
iApp		Name	AppServerPool
Local Traffic		Description	
Network Map Virtual Servers Policies	>	Health Monitors	Active Available
Profiles		Pasourcas	
Pools	-	Load Balancing Method	Round Robin
Nodes		Priority Group Activation	Disabled
Monitors Traffic Class Address Translation	 → → 		New Node O Node List Node Name: (Optional) Address: 10.0.2.12
DNS Express Zones			Service Port: 80 HTTP
DNS Caches		New Members	R:1 P 0 C 0 10.0.2.11 10 0.2.11 :80
Acceleration			R-1 P-0 C-0 10 0 2-12 10 0 2-12 30
Device Management			Edit Delete
Network		Cancel Repeat Finched	



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.

Local T	raffic »	Pools : P	Pool List	
⇔ - □	Pool List		Statistics	
t				Search
•	Status	 Name 		
	0	AppServe	rPool	
	0	WebServe	erPool	
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, expand Local Traffic and then select Pools. The Pool List screen opens.
- 2. In the upper right corner of the screen, click Create.
- 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.
- Under Resources at the bottom of the New Virtual Server configuration page, select the WebServerPool from the dropdown box.
- 8. Again, select **Repeat** to continue to configure the application tier virtual server.



File Edit View Favorites Tools Hel	p			
Hosiname: bd5000.bd.f5.com Date: Feb	19, 2015 User: admin			
IP Address: 10.105.155.17 Time. 2.2	3 PM (PST) Role: Administrator			
Standalone				
Main Help About	Local Traffic » Virtual Servers	: Virtual Server List » New Virtual Server		
Statistics				
	General Properties			
iApp	Name	Web-Vip		
Local Traffic	Description			
Network Map	Туре	Standard		
Virtual Servers	Source			
Policies >		Type: Host O Network		
Profiles >	Destination	Address: 20.20.20.5		
iRules >	Service Port	80 HTTP V		
Pools >	State	Enabled V		
Nodes >	Continuention: Basic	- Là		
Monitors	Source Address Translation	Auto Man w		
		Point map •		
	Content Rewrite			
	Rewrite Profile			
	HTML Profile	None		
	Acceleration			
	Rate Class	None		
	OneConnect Profile	None		
	NTLM Conn Pool	None V		
1	HTTP Compression Profile	None		
	Web Acceleration Profile	None		
	SPDY Profile	None		
	Resources			
		Enabled Available sys_auth_krbdelegate		
	Rules	sys_auth_ssl_cc_idap		
		sys_auth_ssl_ocsp sys_https_redirect		
		Up Down		
		Enabled Available		
	Policies	<pre></pre>		
		32		
	Default Pool	WebServerPool V		
	Default Persistence Profile	None		
	Eallback Dereictence Drafile	Nona		
	r alluaux reisistence Prome	Indexe A		
	Cancel Repeat Finished			

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	Local Traffic » Virtual Servers : Virtual Server List									
☆ -	Virtual	Server List	Virtual Address List	Statistics	-					
			I							
*			Sea	arch						Create
	 Status 	▲ Name			Application	+ Destination	Service Port	Type	Resources	Partition / Path
	0	App-Vip				10.0.1.5	80 (HTTP)	Standard	Edit	Common
	0	Web-Vip				20.20.20.5	80 (HTTP)	Standard	Edit	Common
Enable	e Disal	ole 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.



Hostname: IP Address:	nsxbigip1.bd.f5.com Date: 172.30.128.16 Time:				
Changes Pending					
Main	Help	About			
Mage Statistics					
iApps					

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: M IP Address: 172.30.128.16 Time: 5	Var 2, 2015 User: admin 5:08 PM (PST) Role: Administrator				Partition: Common 🗘 Log out
Changes Pending					
Main Help About	Device Management » Overview				
Mage Statistics	🔅 🗸 Overview				
iApps	Device Groups				
S DNS	Name		Number of Devices	Device Group Type	Sync Type
Local Traffic	device-group-failover-ad2f4f99ef90	O Changes Pending	2	Sync-Failover	Manual
	device_trust_group	9	2	Sync-Only	Auto
Overview	Details Rec	nges pending ommended action: Synchronize nsxt	bigip1.bd.f5.com to group device-group-failo	ver-ad2f4f99ef90	Show Advanced View
Device Groups	HA Status Anne		Sync Status	Config	guration Time
Device Trust	nsxbigip1.bd.f5.	com (Self)	O Changes Pending	3/2/201	5 16:49:32
Traffic Groups	nsxbigip2.bd.f5.	com	٩	2/27/20	15 17:30:08
Network	Sync Options Sync Device to Group Sync Group to Device Overwrite Configuration Sync				



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

I ONLINE (STANDBY)					
Main Help About	Device Management » Overview				
Statistics	🌣 🗸 Overview				
iApps	Device Groups				
S DNS	Name		Number of Devices	Device Group Type	Sync Type
1 and Traffia	device-group-failover-ad2f4f99ef90	•	2	Sync-Failover	Manual
Local Hand	device_trust_group	9	2	Sync-Only	Auto
Device Management Overview	Summary All de Details	vices in the device group are in	sync		Show Advanced View
Devices	the Status		÷ Suno Status	+ Configuration	Show Advanced View
Device Groups	nervision hd f5 o	nm (Self)	• Sync Status	3/2/2015 16:49:	12
Device Trust				0/2/2015 10:40:4	
Traffic Groups 📀	Tiskolgipz.bu.is.o	011		3/2/2013 10:43.	24
Network	Sync Options Sync Device to Group Sync Group to Device				
	Overwrite Configuration				
	Sync				

4. This completes the configuration portion for the topology.

Validation

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

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

Local Traffic » Network Map			
🔅 👻 Network Map			
Status Any Status V Type All Types V	Search	*	Search iRule Definition
Show Summary Update Map			
Local Traffic Network Map			
O App-Vip	🔘 We	b-Vip	
AppServerPool	0	WebServerPool	
10.0.2.11:80		🥥 10.0.1.11:80	
10.0.2.12:80		10.0.1.12:80	

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

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



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

Conclusion

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

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

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

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

Americas Asia-Pacific info@f5.com apacinfo@f5.

Asia-Pacific Europe/Middle-East/Africa apacinfo@f5.com emeainfo@f5.com

a Japan K.K. f5j-info@f5.com



©2015 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. 0615 BESTP-VIRT-43953