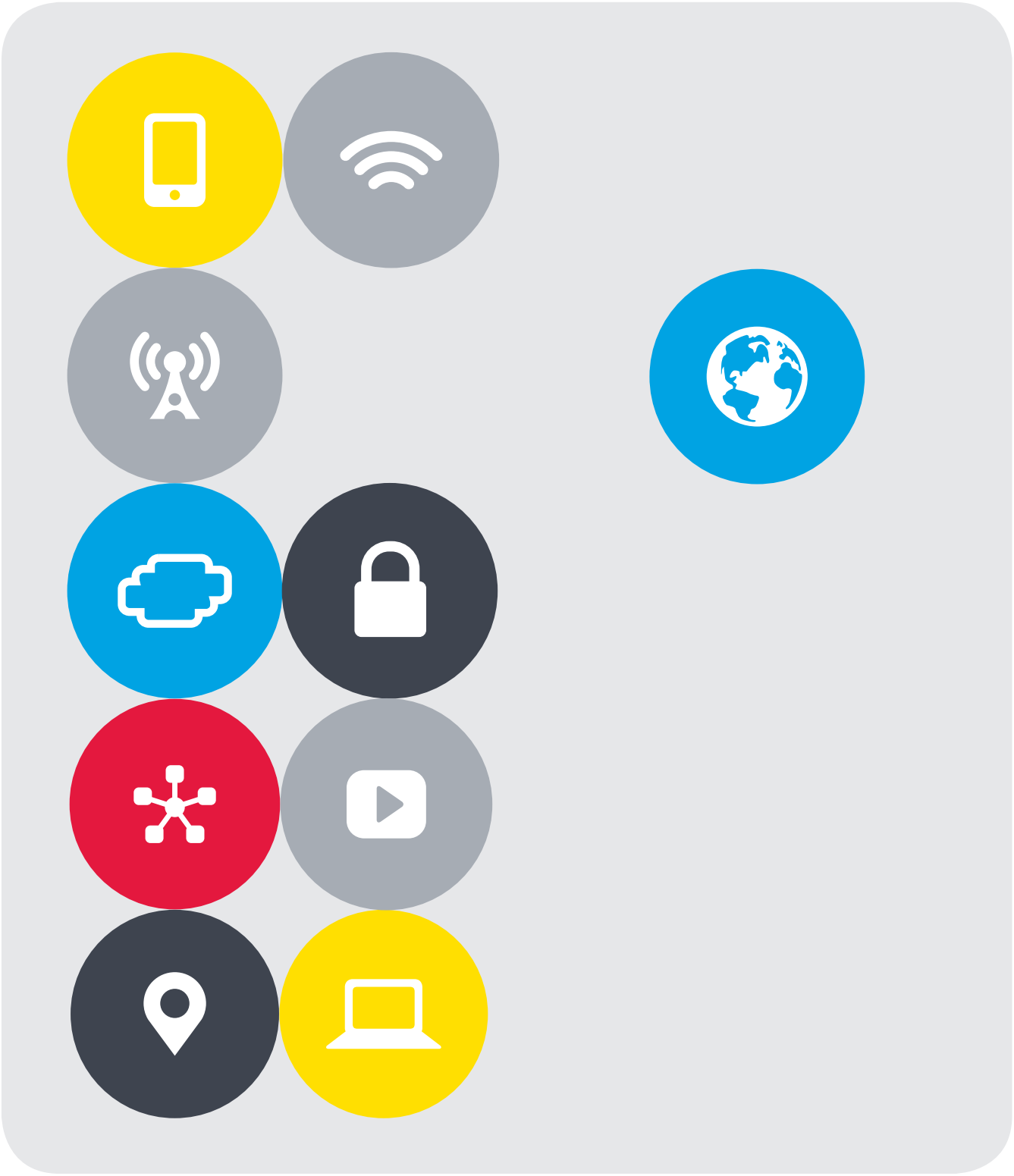
DESIGN GUIDE

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



Contents

Intended Audience

The intended audience for this document includes virtualization and network architects seeking to deploy VMware® NSX™ for vSphere® (NSX-v) in combination with F5® BIG-IP® Local Traffic Manager™ (LTM) devices.

Note: A solid understanding based on hands-on experience with both NSX-v and F5 BIG-IP LTM is a prerequisite to successfully understanding the topics covered in this design guide.

Overview

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 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.

VMware NSX-v is the leading network virtualization solution on the market today and is being deployed across all vertical markets and market segments. NSX reproduces L2-L7 networking and security, including L2 switching, L3 routing, firewalling, load balancing, and IPsec/VPN secure access services completely in software and allows programmatic provisioning and management of these services. More information about these functions is available in the NSX for vSphere Network Virtualization Design Guide here.

F5 BIG-IP is the leading application delivery controller on the market today. The BIG-IP product family provides F5® Software-Defined Application Services™ (SDAS) designed to improve the performance, reliability, and security of mission-critical applications. BIG-IP is available in a variety of form factors, ranging from ASIC-based physical appliances to virtual appliances that run on vSphere. NSX deployments can be coupled with F5 BIG-IP appliances or virtual edition form factors. Learn more about F5 SDAS here.

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

This design guide provides recommended practices and topologies to optimize interoperability between the NSX platform and BIG-IP physical and virtual appliances. It is intended for customers who would like to adopt the SDDC while ensuring compatibility and minimal disruption to their existing BIG-IP environment. The VMware NSX for vSphere Recommended Practices Guide provides step-by-step guidance to implement the topologies outlined in this document.

NSX and BIG-IP Topology Options

As we surveyed our VMware and F5 customers, it was apparent that there are about 20 possible topologies that can be used when connecting BIG-IP to an NSX environment. This design guide focuses on the three that best represent the configurations needed on BIG-IP and on NSX to successfully deploy these form factor, connection method, and logical topology combinations. In addition, this guide highlights the pros and cons of each of the three topologies.

The following figure describes the relationship between:

- BIG-IP form factors
  - BIG-IP virtual edition
  - BIG-IP physical appliance
- With/without NSX overlay
  - VXLAN
  - non-VXLAN (VLAN tagged on untagged)
- BIG-IP placement
  - BIG-IP parallel to NSX Edge
  - BIG-IP parallel to DLR
  - BIG-IP One-arm connected to server network(s)
  - BIG-IP on top of NSX Edge
  - BIG-IP on top of NSX DLR

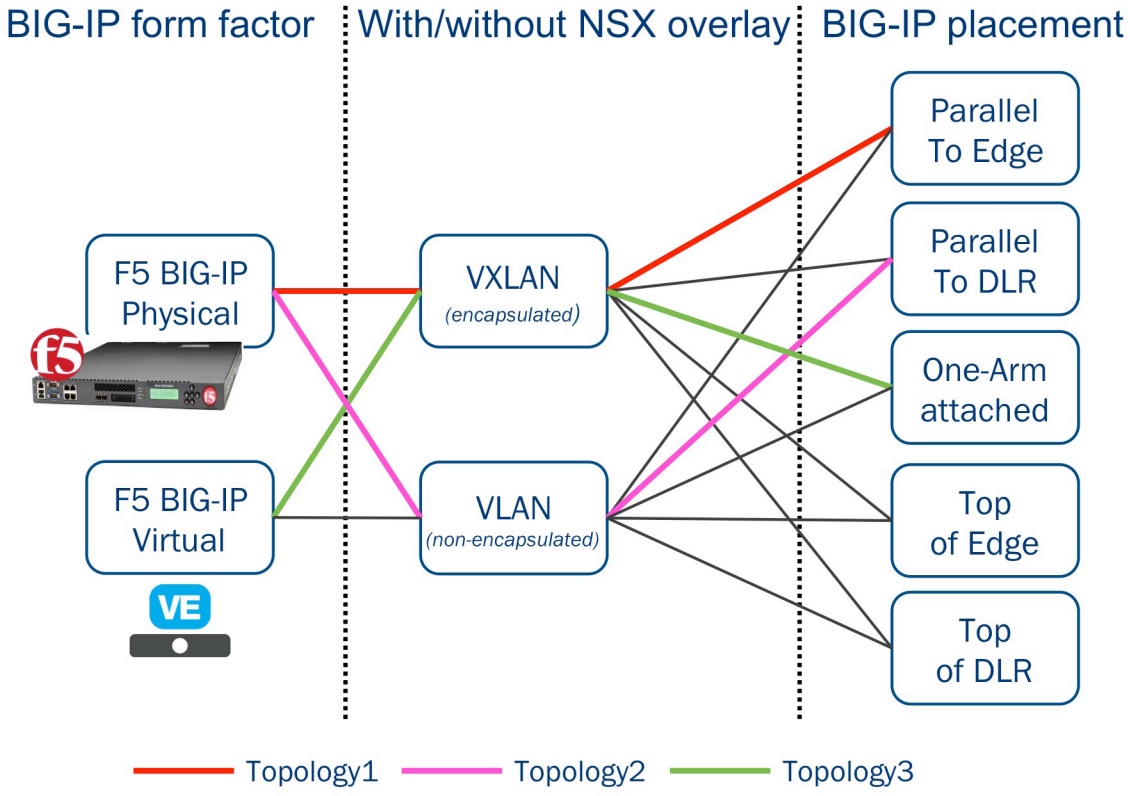


Figure 1. NSX and BIG-IP topology options and relationships

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

In this topology, which is represented by the red lines in Figure 1, the BIG-IP devices are placed parallel to the NSX Edge. Although BIG-IP physical appliances are used in this description, BIG-IP virtual editions can be used the same way. This topology is popular on layer 3 physical fabrics, such as leaf/spine, but also works on layer 2 physical fabrics.

Logical and Physical Views

The BIG-IP appliances are logically installed parallel to the NSX Edges. The NSX Edges can be installed in active/standby mode or active/active mode (active/active requires dynamic routing configuration between the BIG-IP appliances and the Edges).

Below the Edges, a Distributed Logical Router (DLR) provides connectivity to the different applications tiers: Web, App, and DB. Those internal networks can be VLAN or VXLAN. For flexibility, VXLAN is recommended and represented in Figure 2.

The default gateway for the Web, App, and DB servers is the DLR.

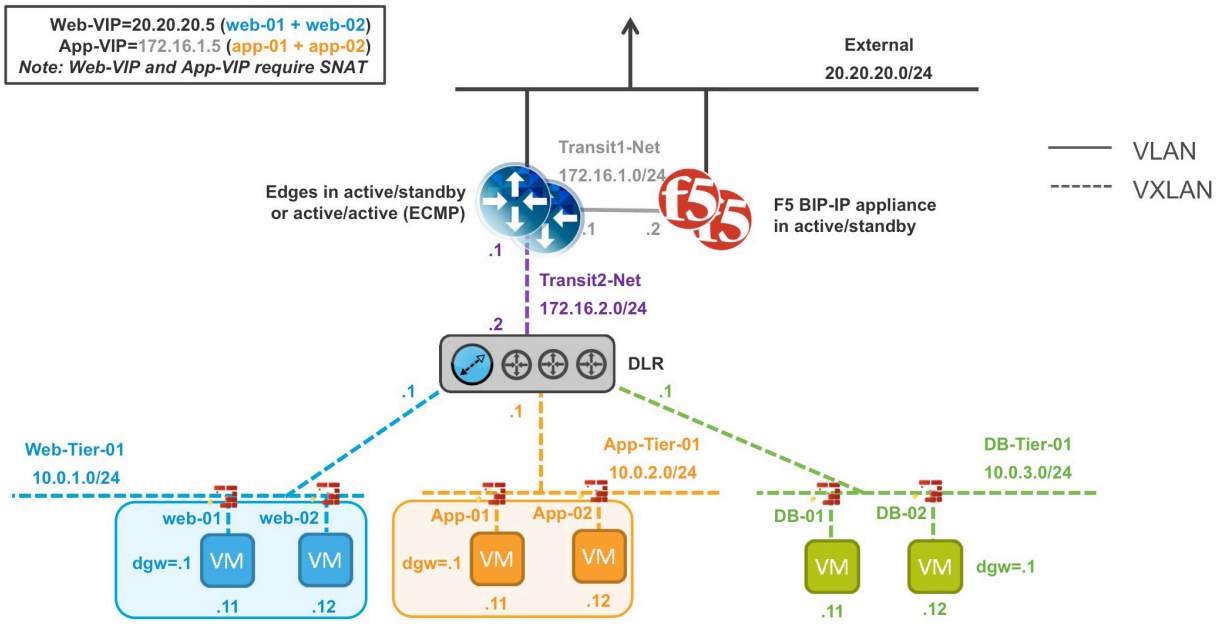


Figure 2. Logical view “Parallel to NSX Edge” with BIG-IP appliances

Following the NSX for vSphere Network Virtualization Design Guide, the recommendation is to physically install the BIG-IP appliances in the edge racks where the external network is available.

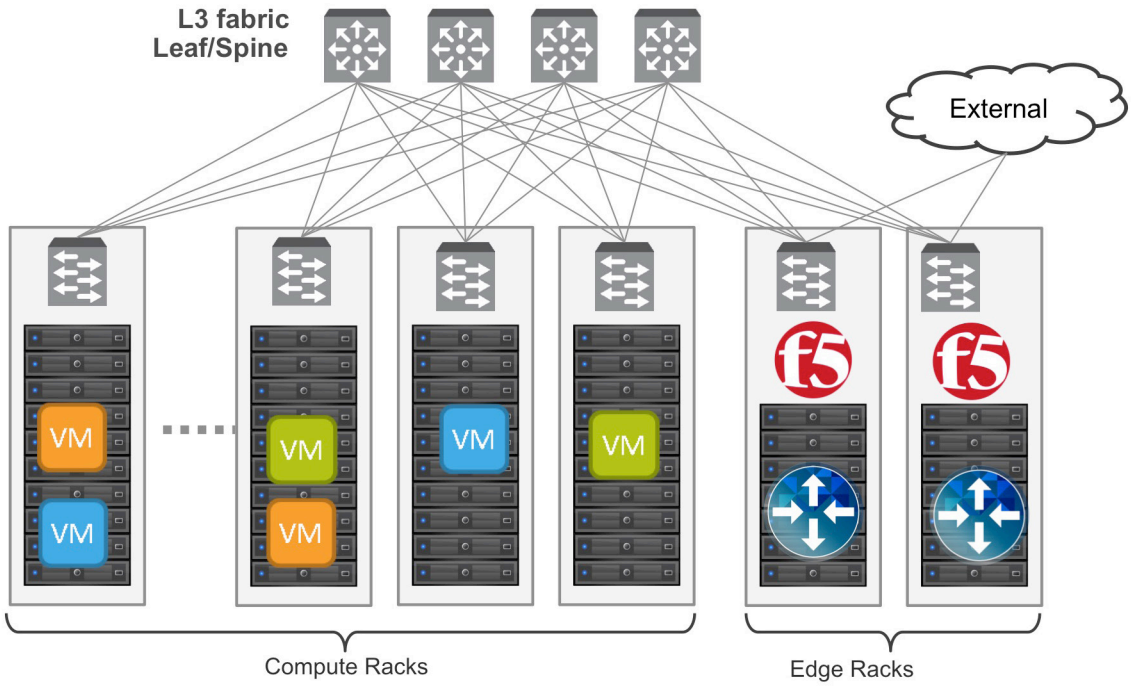


Figure 3. Physical view "Parallel to NSX Edge" with BIG-IP appliances

Traffic Flows

- North-south traffic
  - Logical traffic flows as follows (see Figure 4):
    - From External to BIG-IP appliance
    - From BIG-IP appliance to NSX Edge to DLR to Web
    - From Web to DLR to NSX Edge to BIG-IP appliance
    - From BIG-IP appliance to NSX Edge to DLR to App
    - From App to DLR to DB

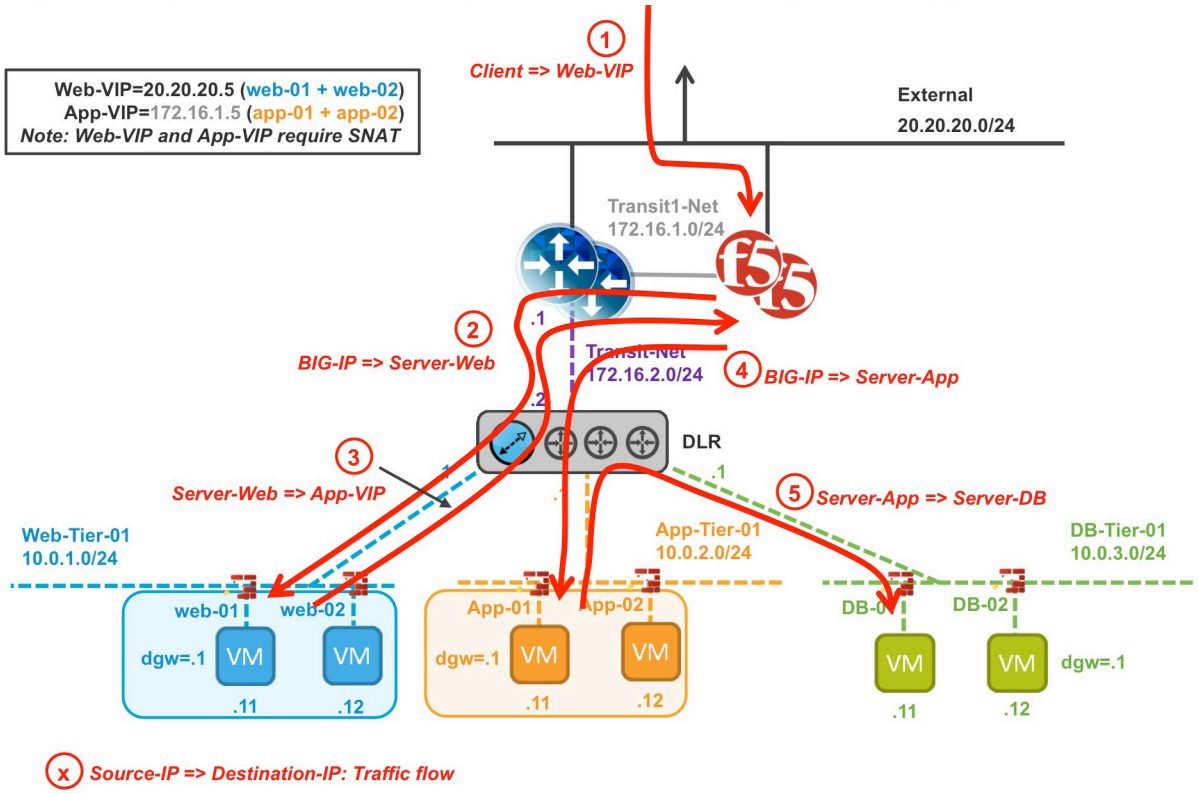


Figure 4. North-south logical traffic flow "Parallel to NSX Edge" with BIG-IP appliances

Physical traffic flows as follows (see Figure 5):

- From External to BIG-IP appliance
- From BIG-IP appliance to ESXi-hosting-Edge to ESXi-hosting-Web
- From ESXi-hosting-Web to ESXi-hosting-Edge to BIG-IP appliance
- From BIG-IP appliance to ESXi-hosting-Edge to ESXi-hosting-App
- From ESXi-hosting-App to ESXi-hosting-DB

Note: BIG-IP and DLR can be configured with dynamic routing (OSPF or BGP) + ECMP. In that case, both Edges process traffic.

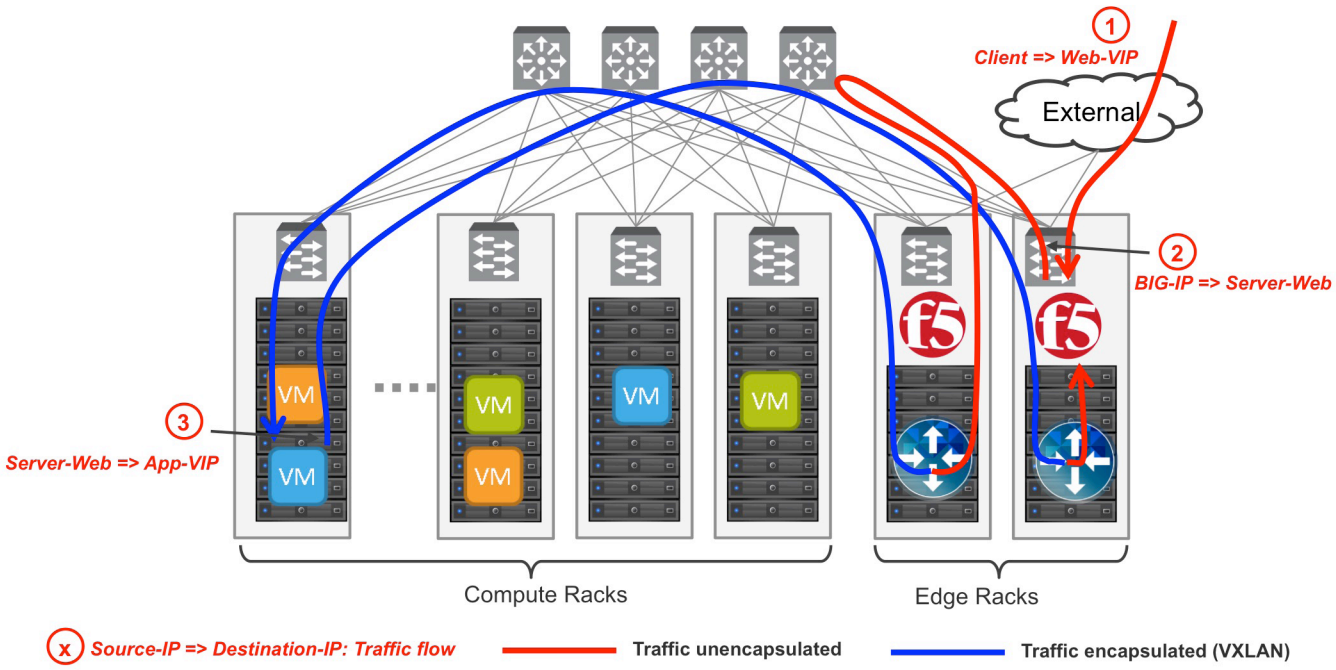


Figure 5. North-south physical traffic flow 1 “Parallel to NSX Edge” with BIG-IP appliances

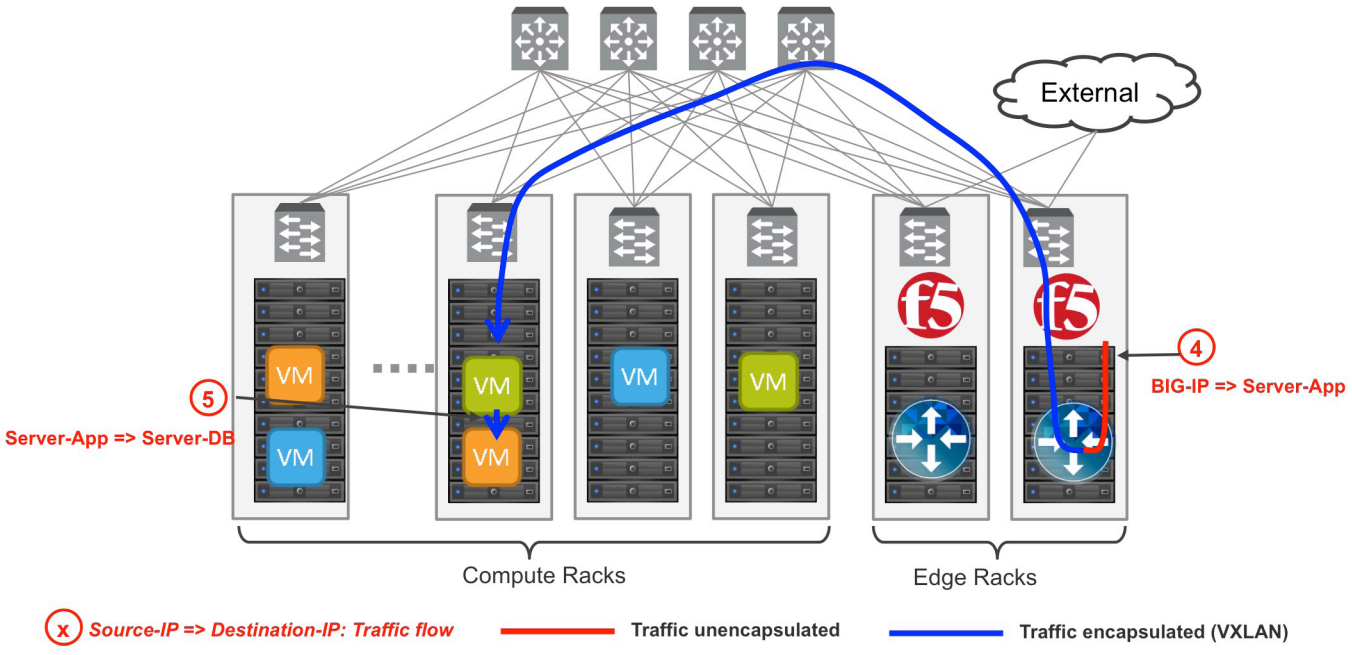


Figure 6. North-south physical traffic flow 2 “Parallel to NSX Edge” with BIG-IP appliances

- South-north traffic

  In this example, a server initiates a security update.

  - Logical traffic flows are as follows (see Figure 7):

    - From Web/App/DB tier to DLR to Edge to External

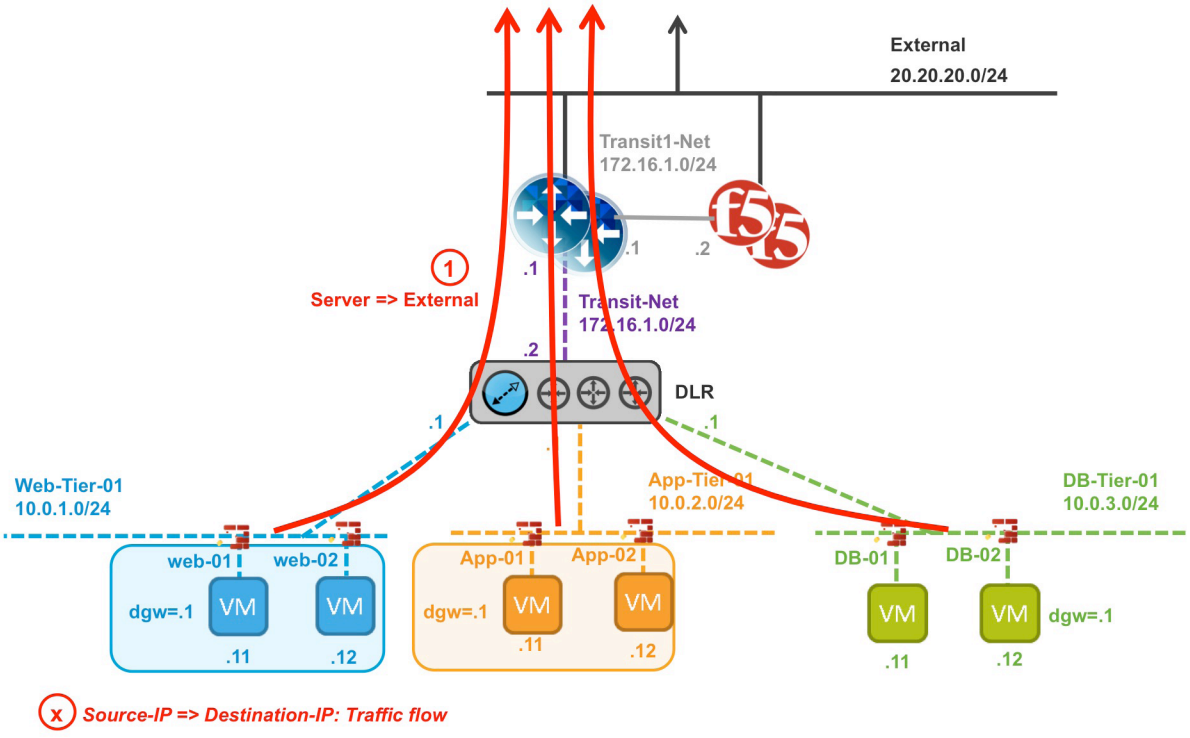


Figure 7. South-north logical traffic flow “Parallel to NSX Edge” with BIG-IP appliances

- Physical traffic flows as follows (see Figure 8):

  - From ESXi-hosting-Web/App/DB to ESXi-hosting-Edge to External.

Note: DLR can be configured with dynamic routing + ECMP. In that case, both Edges process traffic. This is represented in figure 8.

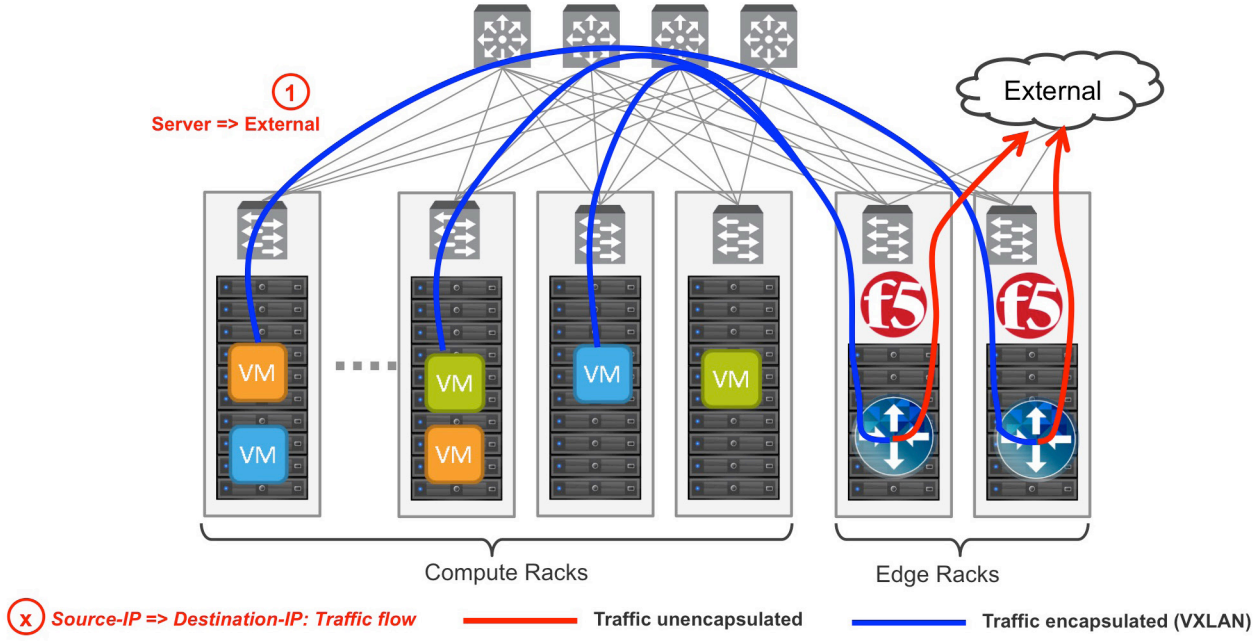


Figure 8. South-north physical traffic flow “Parallel to NSX Edge” with BIG-IP appliances

VIP Requirements

- Web-VIP requires SNAT
- App-VIP requires SNAT

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

In this topology, which is represented by the magenta lines in Figure 1, the BIG-IP appliances are placed parallel to the DLR. In this example, BIG-IP appliances are shown, but BIG-IP virtual edition could also be used the same way.

This topology requires a layer 2 physical fabric (external network is available in all racks).

Logical and Physical Views

BIG-IP appliances are logically installed parallel to the DLR.

The DLR provides connectivity to the Web, App, and DB applications tiers. The internal networks could be VLAN or VXLAN, but in this topology, we are describing a non-VXLAN overlay scenario. Standard 802.1q tagging is used to connect the VLAN-backed virtual networking segments to the physical networking segments to which the BIG-IP devices are connected.

The default gateway for the different servers (Web, App, and DB) is the DLR.

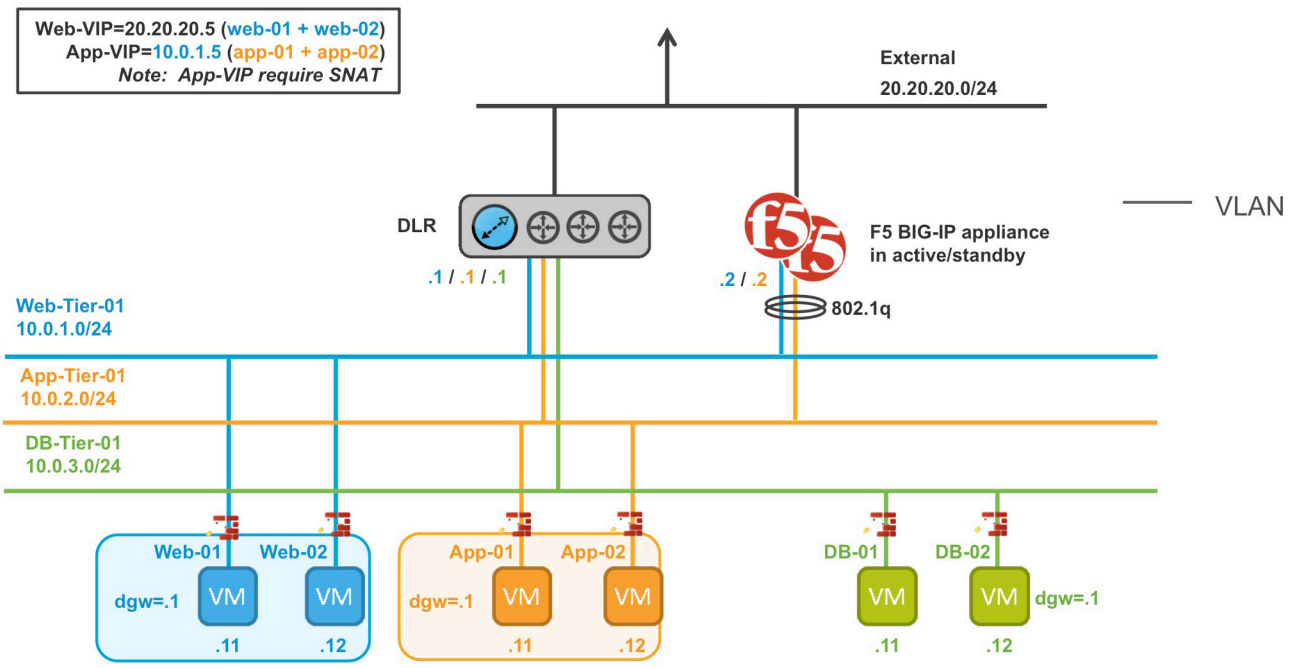


Figure 9. Logical view "Parallel to DLR" with BIG-IP appliances

The recommended topology has the BIG-IP appliances physically connected to the top distribution physical routers.

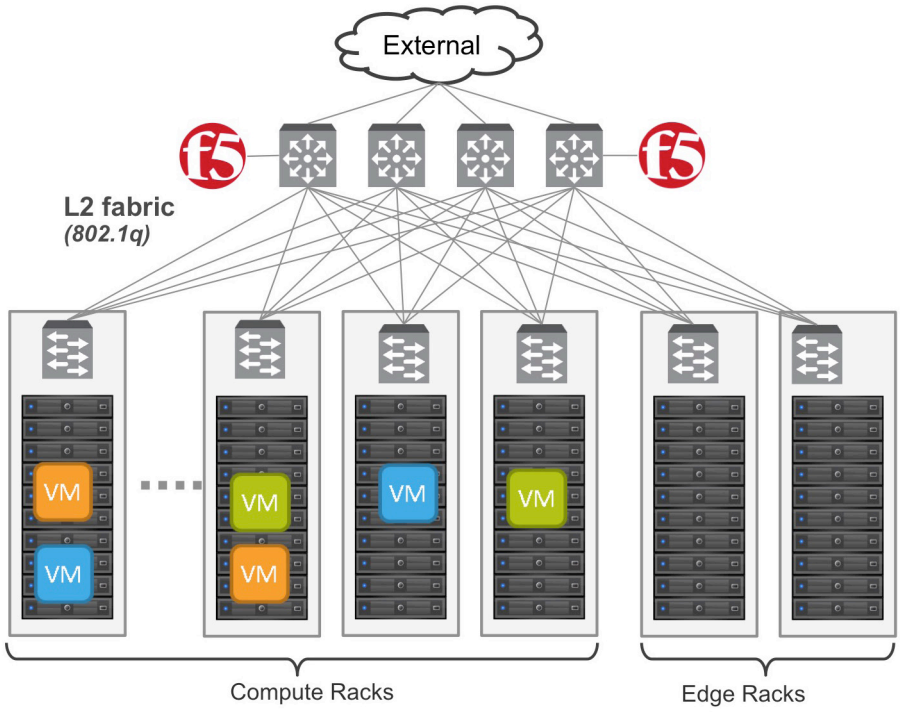


Figure 10. Physical view “Parallel to DLR” with BIG-IP appliances

Traffic Flows

- North-south traffic
  - Logical traffic flows as follows (see Figure 11):
    - From External to BIG-IP appliance
    - From BIG-IP appliance to Web
    - From Web to BIG-IP appliance
    - From BIG-IP appliance to App
    - From App to DLR to DB

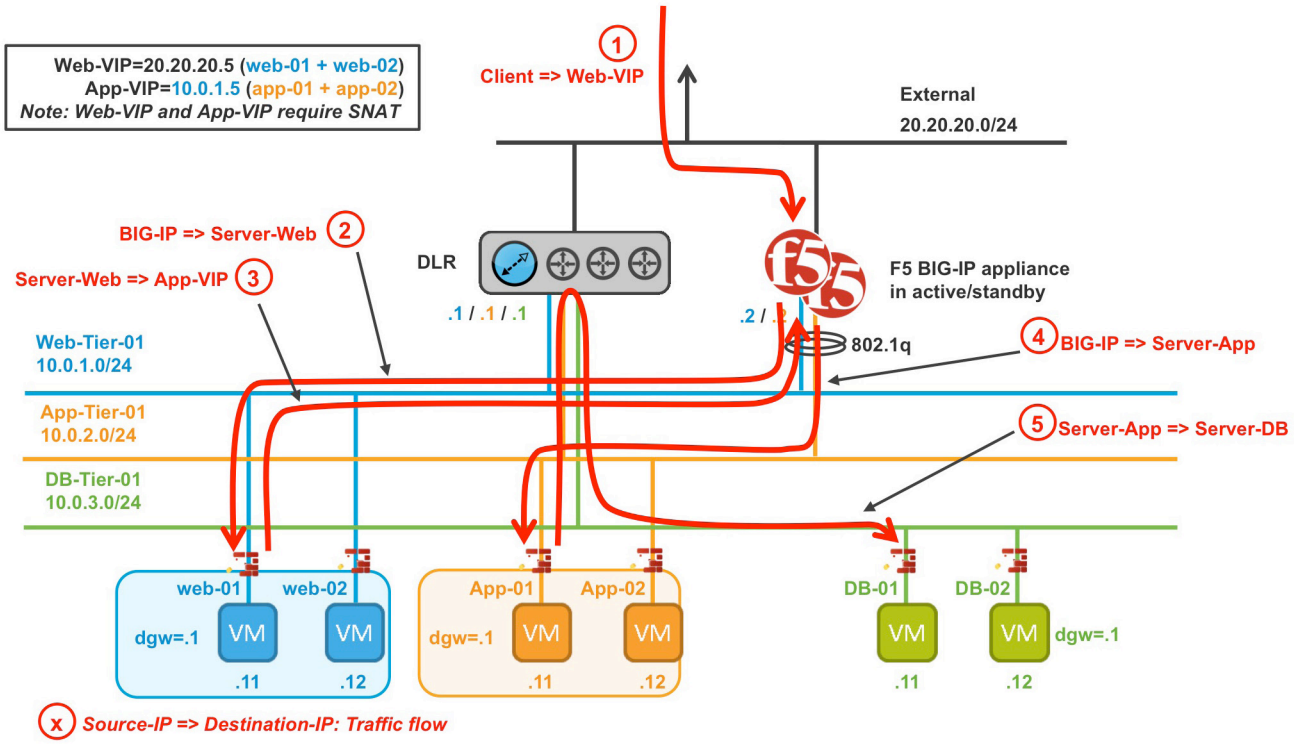


Figure 11. North-south logical traffic flow “Parallel to DLR” with BIG-IP appliances

Physical traffic flows as follows (see Figures 12 and 13):

- From External to BIG-IP appliance
- From BIG-IP appliance to ESXi-hosting-Web
- From ESXi-hosting-Web to BIG-IP appliance
- From BIG-IP appliance to ESXi-hosting-App
- From ESXi-hosting-App to ESXi-hosting-DB

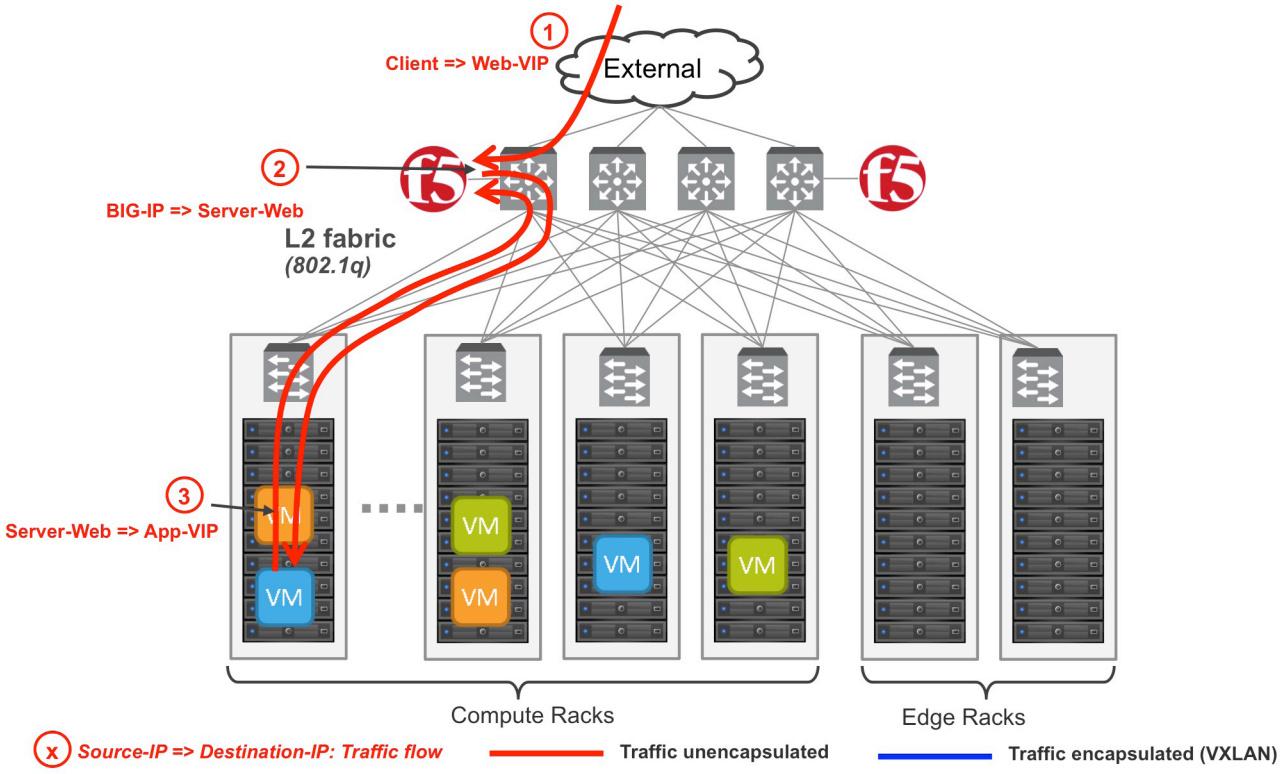


Figure 12. North-south physical traffic flow 1 “Parallel to DLR” with BIG-IP appliances

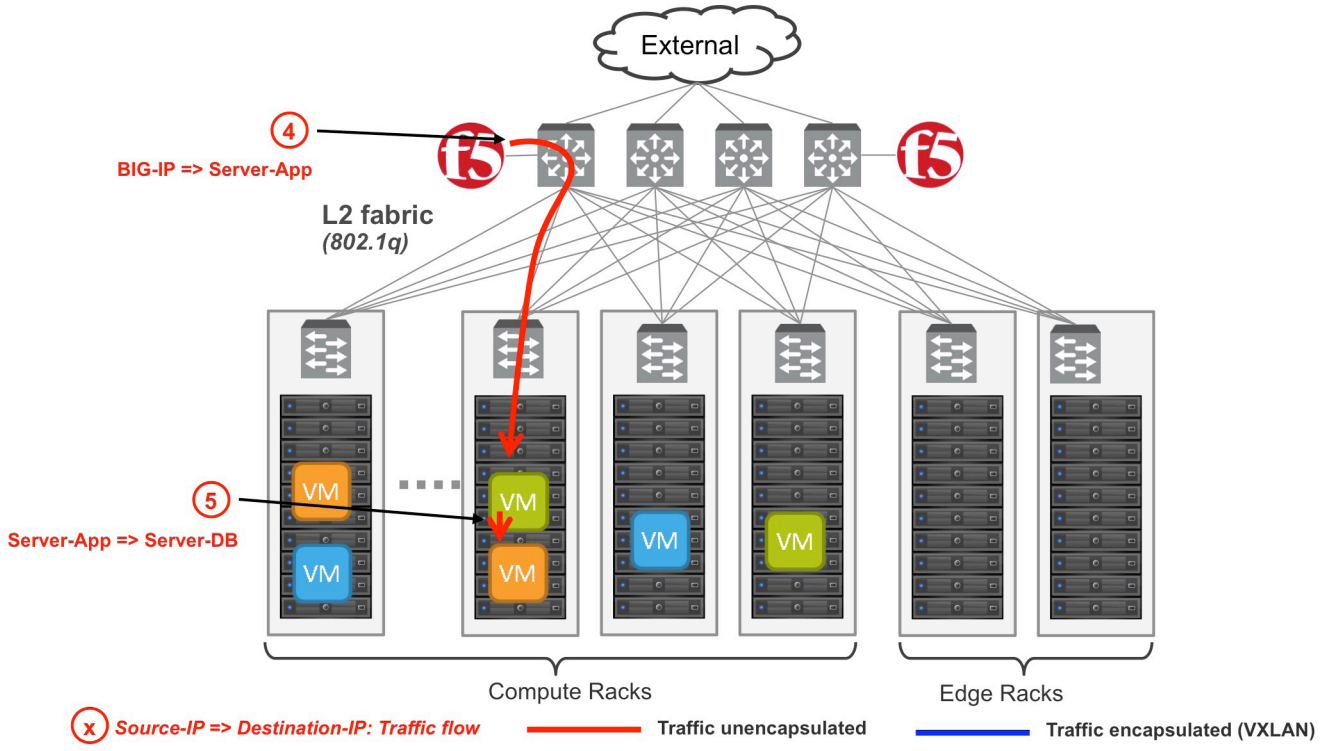


Figure 13. North-south physical traffic flow 2 “Parallel to DLR” with BIG-IP appliances

- South-north traffic

  In this example, the server initiates a security update.

  - Logical traffic flows as follows (see Figure 14):

    - From Web/App/DB to DLR to External

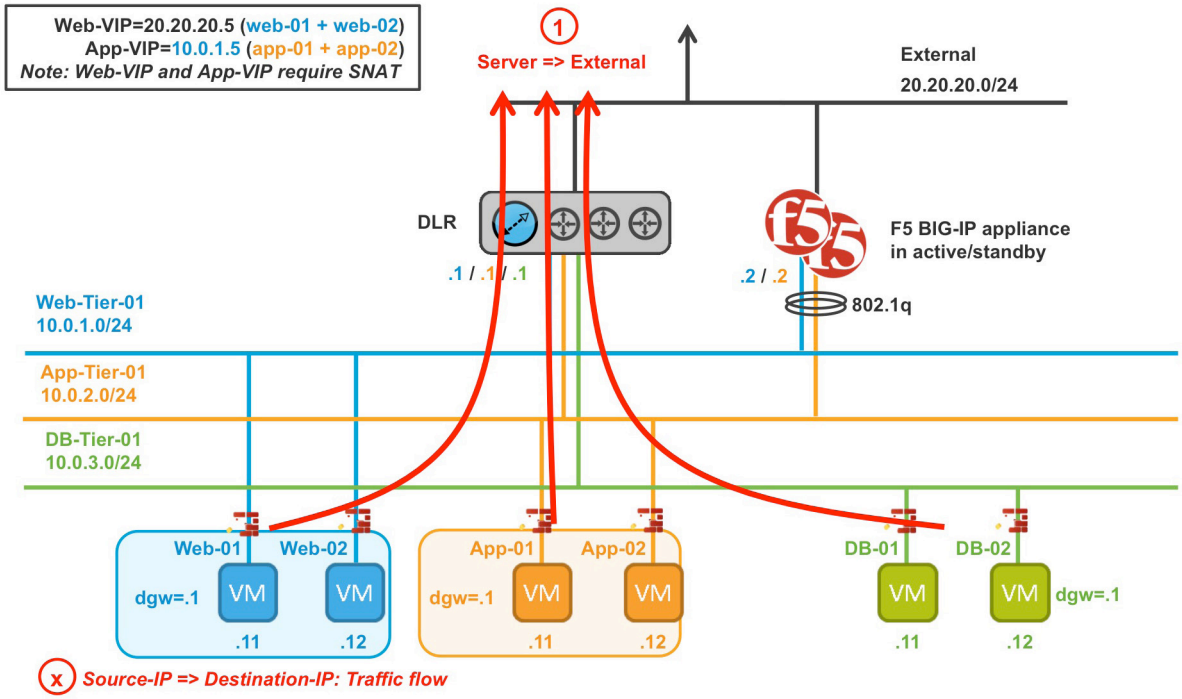


Figure 14. South-north logical traffic flow “Parallel to DLR” with BIG-IP appliances

Physical traffic flows as follows:

- From ESXi-hosting-Web/App/DB to External

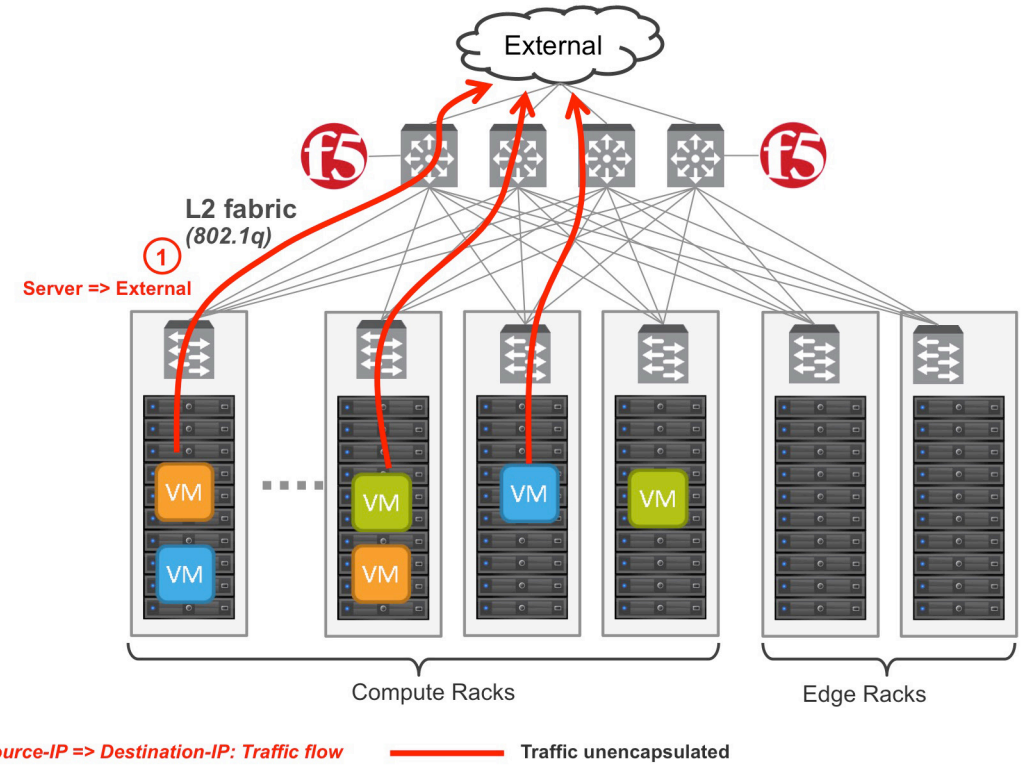


Figure 15. South-north physical traffic flow “Parallel to DLR” with BIG-IP appliances

VIP Requirements

- Web-VIP requires SNAT
- App-VIP requires SNAT

Topology 3: One-Arm Connected using VXLAN Overlays with BIG-IP Virtual Editions

In this topology, which is represented by the green lines in Figure 1, the BIG-IP virtual editions are placed in one-arm mode in the load-balanced server networks. This topology is popular on layer 3 physical fabrics, such as Leaf/Spine but also works on layer 2 physical fabrics.

Logical and Physical Views

At the top, NSX Edges can be installed in active/standby mode or active/active mode (active/active requires dynamic routing configuration between the DLR and Edges).

Below the Edges, a Distributed Logical Router (DLR) provides connectivity to the different applications tiers: Web, App, and DB. Those internal networks can be VLAN or VXLAN (for flexibility VXLAN is recommended and represented in the diagram below).

BIG-IP virtual editions are logically installed in one-arm mode on the load-balanced tiers' logical switches.

The default gateway of the different servers (Web, App, and DB) is the DLR.

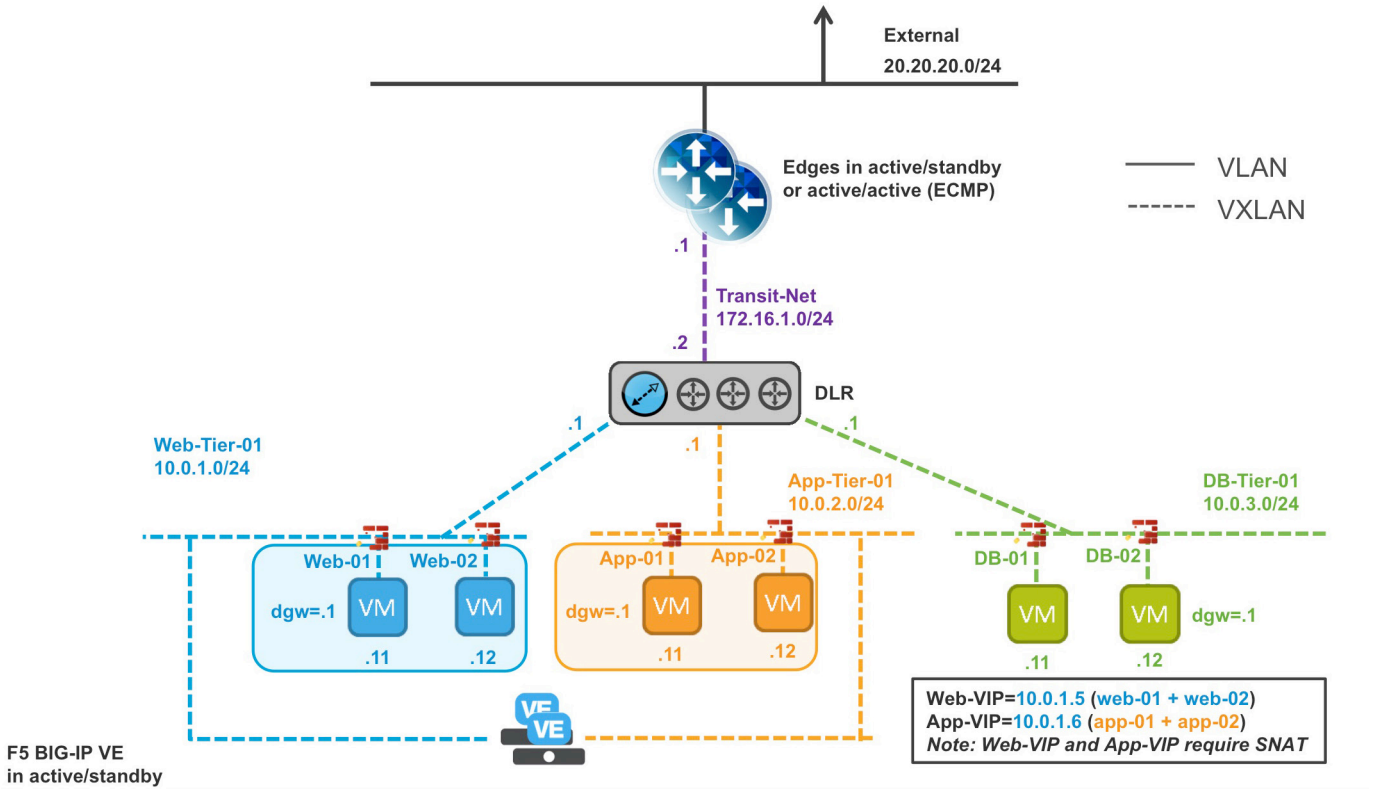


Figure 16. Logical View "One-Arm Connected" with BIG-IP virtual edition

The recommended topology has the BIG-IP virtual edition solutions deployed in the compute rack close to the load-balanced servers.

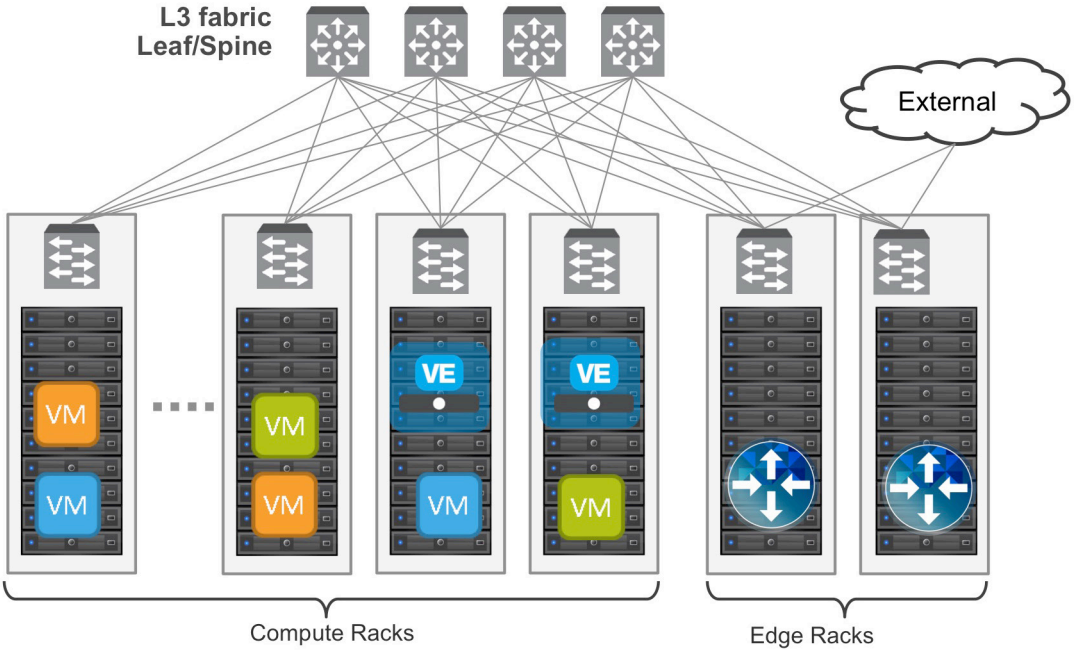


Figure 17. Physical view “One-Arm Connected” with BIG-IP virtual edition

Traffic Flows

- North-south traffic
  - Logical traffic flows as follows (see Figure 18):
    - From External to BIG-IP virtual edition
    - From BIG-IP virtual edition to Web
    - From Web to BIG-IP virtual edition
    - From BIG-IP virtual edition to App
    - From App to DLR to DB

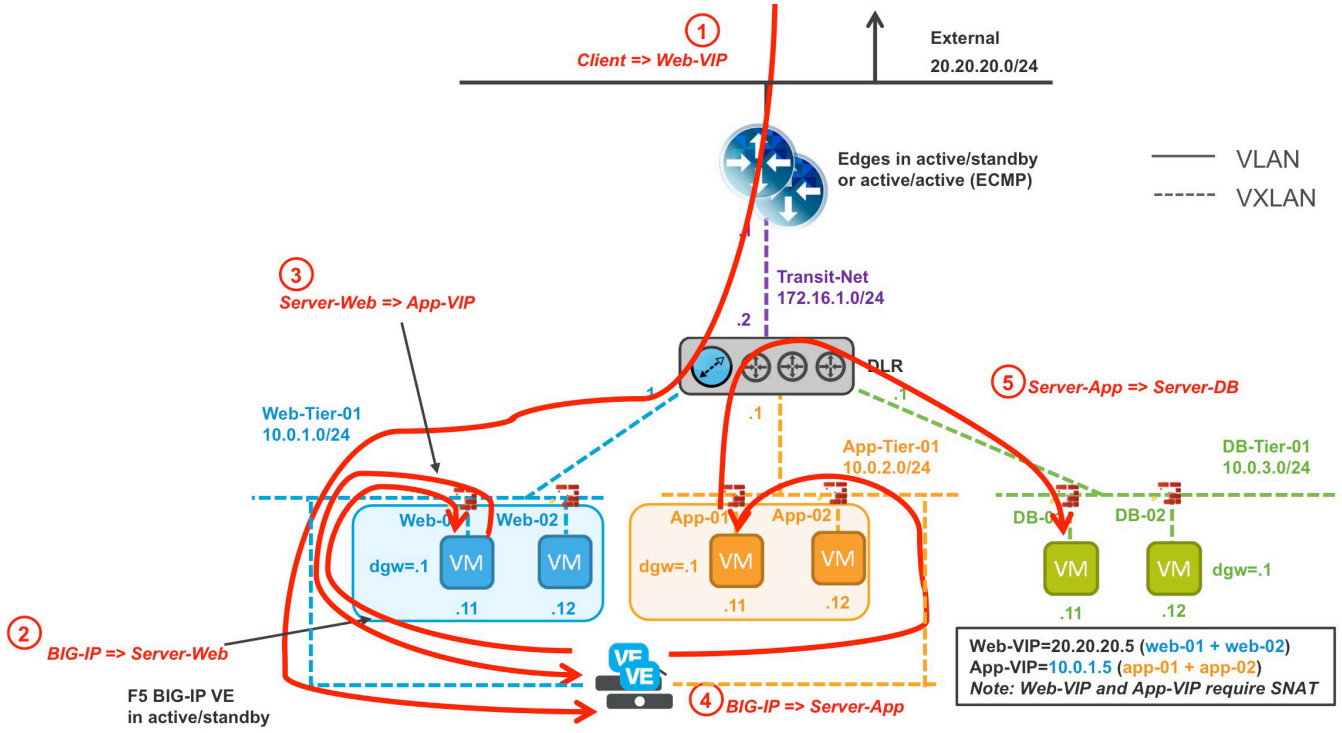


Figure 18. North-south logical traffic flow "One-Arm Connected" with BIG-IP virtual edition

- Physical traffic flows as follows (see Figures 19 and 20):
  - From External to ESXi-hosting-BIG-IP virtual edition
  - From ESXi-hosting-BIG-IP virtual edition to ESXi-hosting-Web
  - From ESXi-hosting-Web to ESXi-hosting-BIG-IP virtual edition
  - From ESXi-hosting-BIG-IP virtual edition to ESXi-hosting-App
  - From ESXi-hosting-App to ESXi-hosting-DB

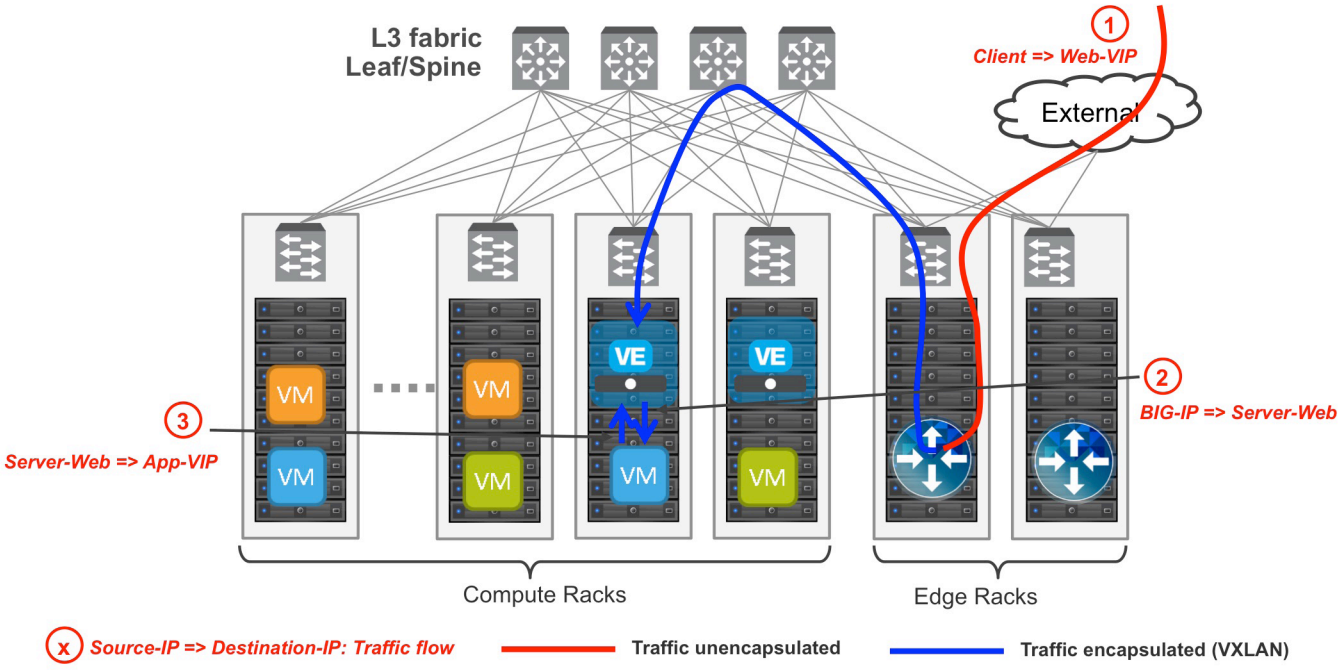


Figure 19. North-south physical traffic flow 1 “One-Arm Connected” with BIG-IP virtual edition

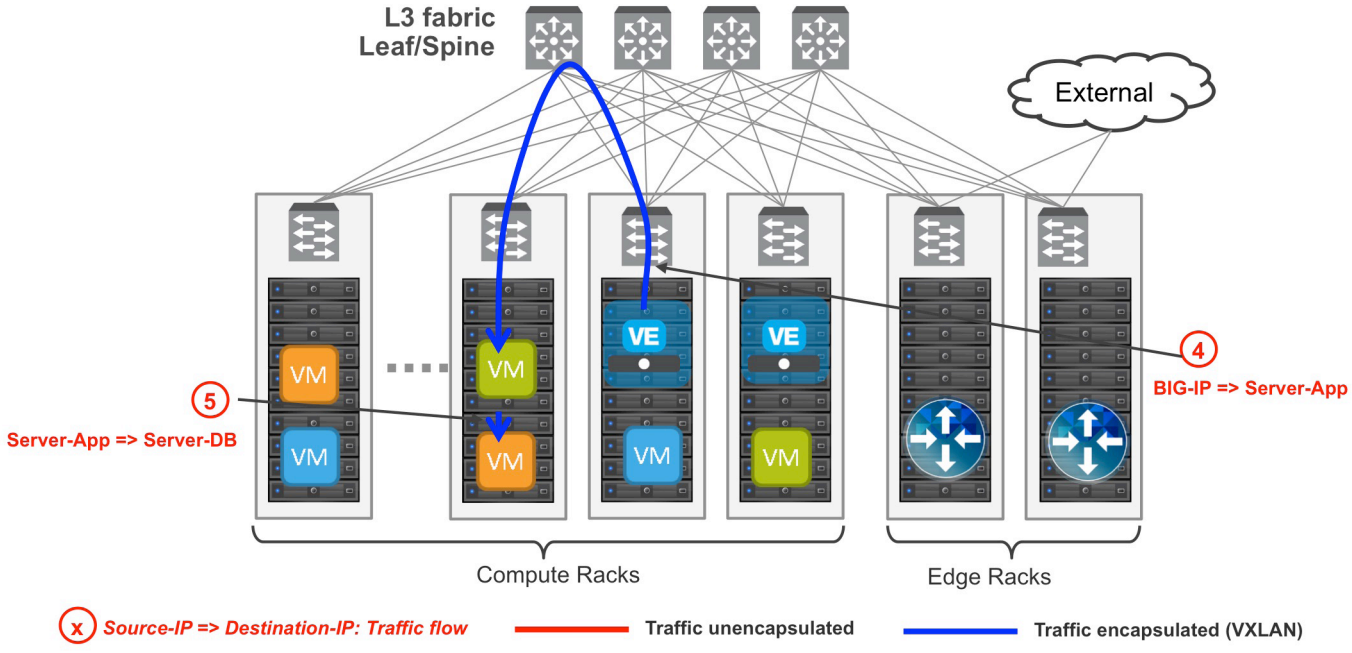


Figure 20. North-south physical traffic flow 2 “One-Arm Connected” with BIG-IP virtual edition

- South-north traffic

  In this example, a server initiates a security update.

  - Logical traffic flows as follows (see Figure 21):
  - From Web/App/DB to DLR to Edge to External

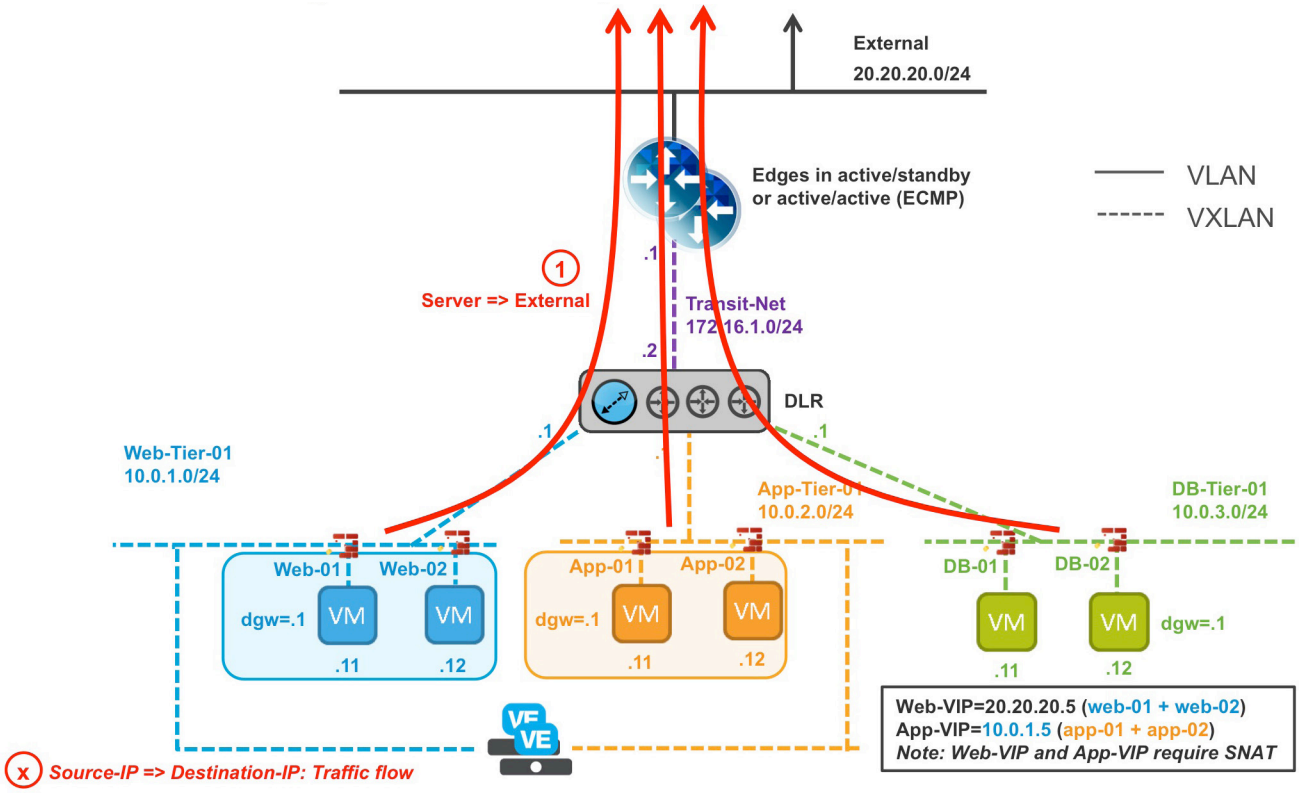


Figure 21. South-north logical traffic flow "One-Arm Connected" with BIG-IP virtual edition

- Physical traffic flows as follows (see Figure 22):
  - From ESXi-hosting-Web/App/DB to ESXi-hosting-Edge to External

Note: DLR can be configured with dynamic routing + ECMP. In that case both Edges process traffic. This is represented in figure 23.

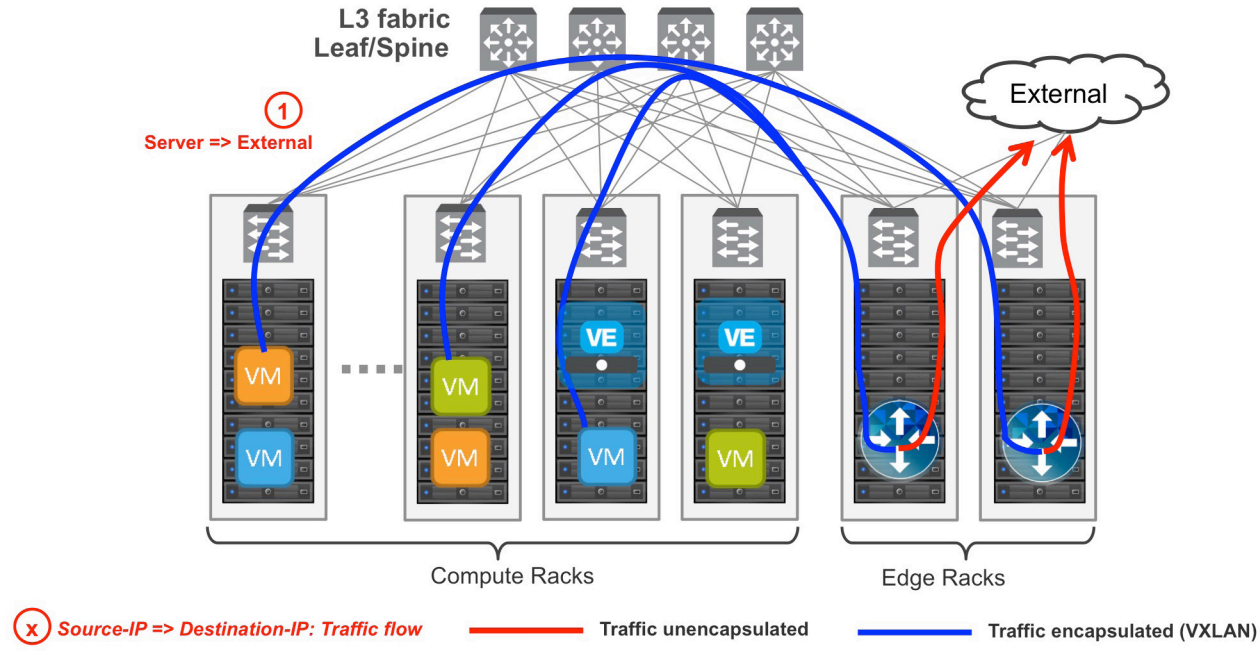


Figure 22. South-north physical traffic flow “One-Arm Connected” with BIG-IP virtual edition

VIP Requirements

- Web-VIP requires SNAT
- App-VIP requires SNAT

Pros and Cons of Using the Illustrated Topologies

Parallel to Edge	Pros	Cons
BIG-IP appliances or virtual editions	Easy to implement Supports very large throughput (multiple 10Gbps) with BIG-IP appliances East-west non load-balanced traffic is DLR-optimized Offers DFW for security even within the same subnet Works on layer 2 or layer 3 fabrics	East-west load-balanced traffic is not DLR-optimized (goes through Edge) Web-VIP and App-VIP require SNAT

Parallel to DLR	Pros	Cons
BIG-IP appliances or virtual editions	Supports very large throughput (multiple 10Gbps) with BIG-IP appliances East-west non load-balanced traffic is DLR-optimized Offers DFW for security even within the same subnet	Web-VIP and App-VIP require SNAT Requires layer 2 fabric (requires all VLANs on all ESXi hosts)

One-Arm Connected	Pros	Cons
BIG-IP virtual edition only	Easy to implement East-west traffic between non load-balanced network is DLR optimized Offers DFW for security even within the same subnet Works on layer 2 or layer 3 fabric	Web-VIP and App-VIP require SNAT

Note: Topologies that do not require SNAT on the VIP are detailed in the Alternative Topologies section.

Alternative Topologies

These two alternative topologies are as valid as the preceding three. We list them to showcase that you can take the configuration guidance from the preceding topologies, mix and match that guidance, and create an architecture that suits your topological needs.

Alternative Topology A: BIG-IP Appliances or Virtual Editions on Top of NSX Edge

This topology is similar to Topology 1, but with the BIG-IP appliances or virtual editions on top of the NSX Edge.

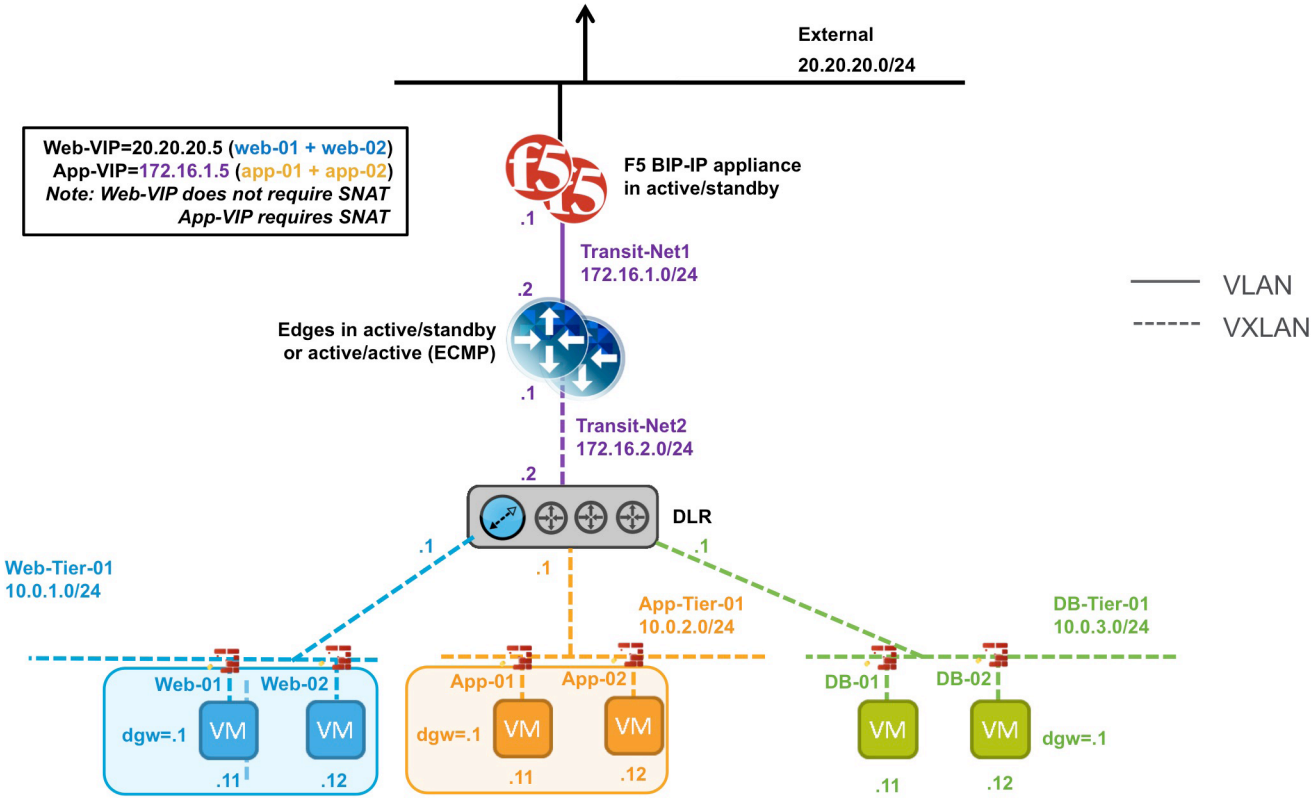


Figure 23. Logical View “On Top of Edge” with BIG-IP appliances

This topology offers the benefit of not requiring SNAT for the Web-VIP.

All north-south traffic (including non-load-balanced traffic) crosses the BIG-IP device.

Alternative Topology B: BIG-IP Appliances or Virtual Editions on Top of DLR

This topology is similar to the Topology 2, but with the BIG-IP appliances or virtual editions on top of the DLR.

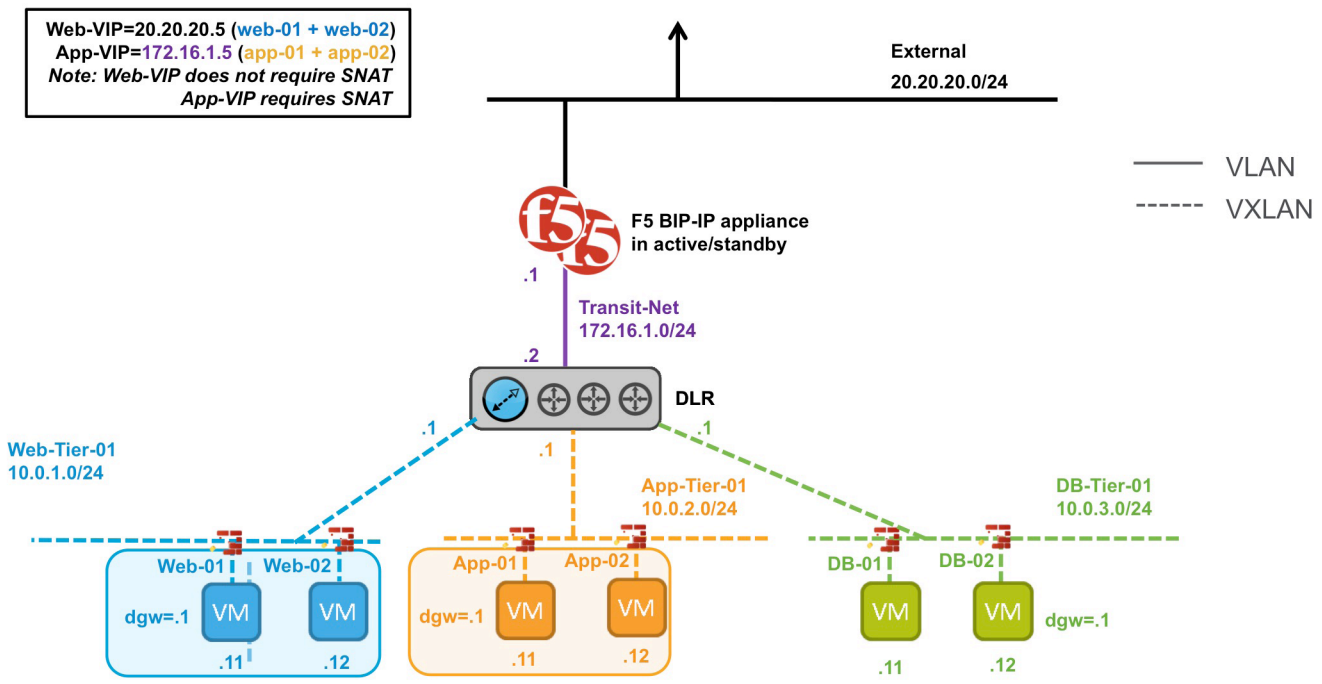


Figure 24 - Logical View "On Top of DLR" with BIG-IP appliances

This topology offers the benefit of not requiring SNAT for the Web-VIP.

All north-south traffic (including non-load-balanced traffic) crosses the BIG-IP device.

Conclusion

This document showcases several possible NSX and BIG-IP interoperability scenarios and illustrates the network topologies needed to accomplish those scenarios.

F5 and VMware are working on a jointly developed API integration between NSX and F5 BIG-IQ®. This will enable IT organizations to fully leverage the combined strengths of NSX virtualization and automation with richer application delivery services enabled by BIG-IP. This planned NSX and 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 depicted in this document will be deployable using this upcoming integration.

For more information 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 info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan K.K. f5j-info@f5.com

Solutions for an application world.