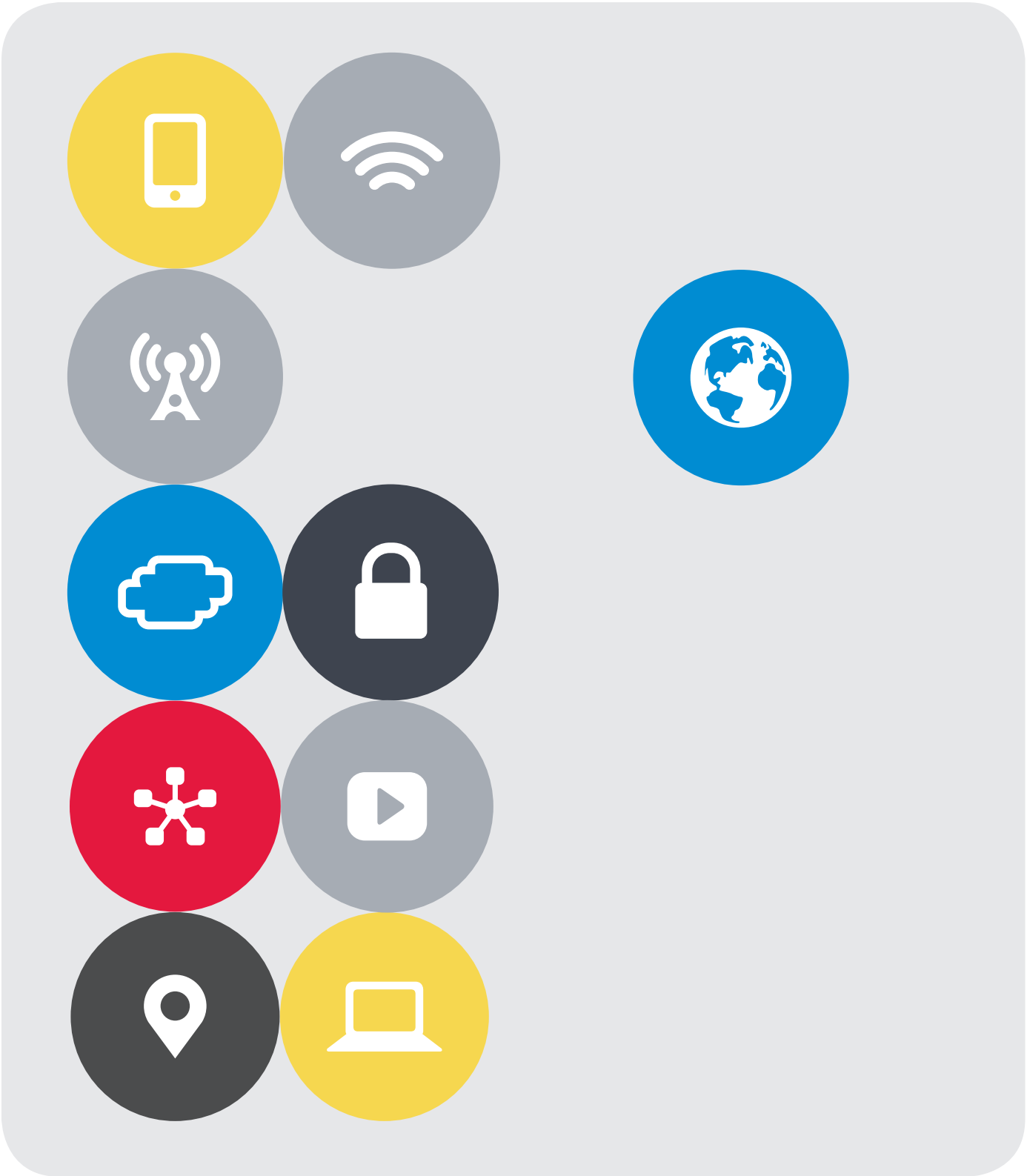
Virtual Solutions for Your NFV Environment



Contents

Introduction

Key benefits:

NFV benefits for service providers include:

- Increased revenue-to-cost ratios—Roll out new services with a streamlined, cost-efficient network.
- CapEx and OpEx predictability—Control deployment and operational costs.
- Service velocity and portability—Rapidly provision network and deploy new services faster to market.
- Network agility and elastic scaling—Quickly and easily spin up and spin down network services.

With rapid increases in application usage, data services, and connected devices, service providers must look at new ways to evolve their networks in order to dynamically address massive growth. In addition, they need to cost-effectively deliver more differentiated services to their customers.

Network functions virtualization (NFV) and software-defined networking (SDN) enable service providers to transform how they build and scale their networks with more flexible and agile architectures. These architectures can help service providers rapidly deliver new services and pursue profitable business models.

F5 offers a rich portfolio of products and solutions for immediate deployment in NFV environments. F5's carrier-class solutions are deployed in core strategic points of control in the network spanning across the data, signaling, and application planes. These highly scalable solutions help you optimize and secure the most critical applications and services in your network including the SGI, Evolved Packet Core (EPC), Diameter signaling, and IMS networks.

F5 modules and services leverage the F5® TMOS® operating system, giving you complete visibility, flexibility, high performance, and control across all your services. The F5 purpose-built hardware and software platforms—as well as F5's general purpose, server-based virtual network functions (VNFs)—all run on TMOS. This allows you to seamlessly provision intelligent network services across both existing and virtualized networks.

In addition, F5 VNFs can integrate with your preferred vendors for NFV orchestration and/or SDN controllers.

Build a Virtualized Network with F5 VNFs

F5 offers a broad portfolio of products and solutions that allow maximum flexibility as you deploy and virtualize your network. Whether you need to virtualize elements in your S/Gi network (such as policy management, Gi Firewall, CGNAT, or intelligent traffic steering), or virtualize your control plane (using DNS and Diameter signaling), F5 VNFs can help you achieve your goals.

F5 BIG-IP® virtual editions (VEs) are VNFs such as virtual firewall (vFW), virtual Application Delivery Controller (vADC), virtual policy charging enforcement function (vPCEF), and virtual DNS (vDNS).

Virtual Firewall (vFW)

BIG-IP® Advanced Firewall Manager® (AFM) VE is a virtual firewall that provides the widest range of security functionality and a multi-layered defense across every domain in your network. This VNF protects against sophisticated emerging threats that can cause network congestion, service degradation, and service outages. The vFW can be deployed across the data, signaling, and application planes. It can also be deployed as a Gi firewall, data center firewall, GTP, and SIP firewall.

Virtual CGNAT (vCGN)

Virtual carrier-grade NAT (CGNAT) is supported on BIG-IP AFM VE or it can serve as a standalone. It offers a broad set of tools that enable you to successfully migrate to IPv6 while continuing to support and interoperate with existing IPv4 devices and content. This VNF provides tunneling solutions with Dual-Stack Lite capabilities as well as native network address translation solutions, such as NAT44 and NAT64.

Virtual Policy Charging Enforcement Function (vPCEF)

BIG-IP® Policy Enforcement Manager™ (PEM) VE is a virtual policy charging enforcement function. It gives you the insight to understand subscriber behavior and manage traffic with a wide range of policy enforcement capabilities. This VNF also offers intelligent Layer 4–7 traffic steering, HTTP redirect, network intelligence, header enrichment, and dynamic control of network resources through subscriber-and context-aware solutions.

Virtual Content Insertion (vCI)

Virtual content insertion is supported on BIG-IP PEM VE. It enables you to insert content, such as targeted ads to subscribers based on their profile and location. Leveraging subscriber awareness functionality, you can add various content into the HTML header to provide more personalized, revenue-generating services.

Virtual URL Filtering (vURL Filtering)

Virtual URL filtering is supported on BIG-IP PEM VE. It enables you to classify traffic based on specific URL categories, which can be customizable according to different regions. In addition, with vURL filtering, you can implement parental control services, which block traffic to specific websites based on certain URL categories or based on specific URLs you define.

Virtual TCP Optimization (vTCPO)

Virtual TCP optimization is supported on all BIG-IP virtual editions. It provides an optimized TCP stack that can significantly improve subscriber Quality of Experience (QoE) by minimizing the effects of congestion and packet loss for 3G/4G networks. This VNF focuses on optimizing the TCP protocol, which accounts for the vast majority of Internet traffic including optimizing encrypted connections. It also improves QoE by optimizing the TCP stack to provide high goodput, minimizing bufferbloat, and allowing fairness between flows. vTCPO can deliver up to twice the performance for subscribers and four times the bandwidth efficiency.

Virtual Application Delivery Controller (vADC)

BIG-IP® Local Traffic Manager™ (LTM) VE is a virtual Application Delivery Controller. It enables you to deliver network services in a reliable, secure, and optimized way. This VNF provides Layer 4–7 load-balancing and Layer 7 traffic management—allowing you to optimize and offload other network resources, including value-added services (VAS) platforms and other VNFs in your network.

Virtual SIP Routing and Load Balancing (vSRLB)

Virtual SIP routing and load balancing is supported on all BIG-IP virtual editions. It offers a full L4-L7 SIP-aware load-balancing solution providing the scalability and flexibility to deploy SIP solutions within IMS environments for LTE services. This gives you the ability to integrate new voice and multimedia services with greater ease and confidence. It also provides high availability for your SIP infrastructure and application servers by continuously monitoring and managing SIP sessions between the different servers.

Virtual DNS (vDNS)

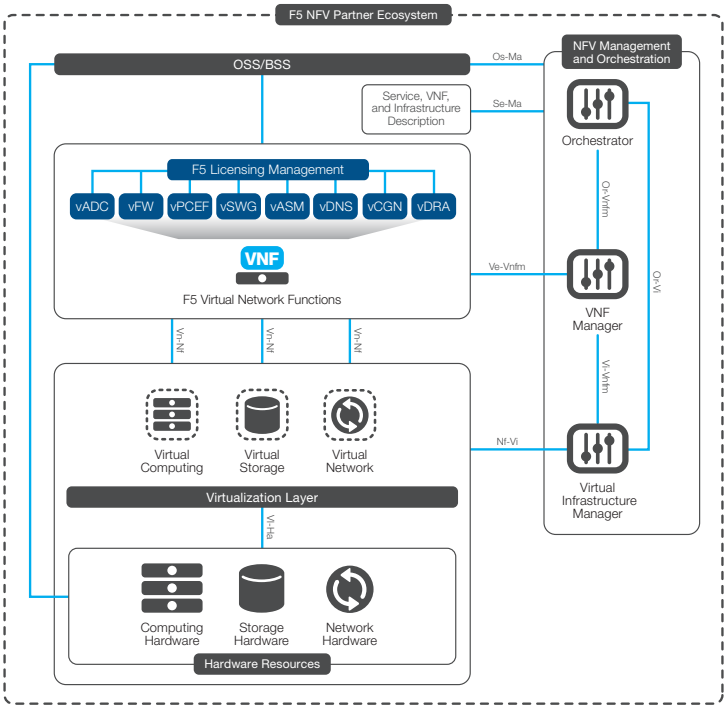
BIG-IP® DNS VE is a virtual DNS. It secures your DNS infrastructure through high-performance DNS services, scales DNS responses to survive volume increases and distributed denial-of-service (DDoS) attacks, and ensures high availability of your global applications and services. This VNF also provides DNS scalability and delivery offload to your LDNS infrastructure. By delivering faster response times for content being accessed by fixed and mobile devices, vDNS offers higher subscriber QoE.

Virtual Web Application Firewall (vWAF)

BIG-IP® Application Security Manager™ (ASM) VE is a virtual web application firewall that secures web applications in traditional, virtual, and private cloud environments. It provides unmatched protection that helps secure applications against layer 7 threats including DDoS, SQL injection, OWASP Top Ten, brute force, and zero-day web application attacks. The vWAF also mitigates DOS-heavy URL attacks, prevents execution of fraudulent transactions, and stops in-browser session hijacking. With this VNF, you can achieve industry security standards compliance with key regulatory mandates.

Virtual Secure Web Gateway (vSWG)

BIG-IP® Access Policy Manager® (APM) VE is a virtual secure web gateway. This flexible, high-performance access and security solution provides unified global access to applications and your network. It uses powerful analytics combined with a collection of sophisticated signature and heuristic detection engines. These can identify and eradicate general and specialized threats and block malware or malicious scripts within web pages by scanning return HTTP/HTTPS traffic. The vSWG also uses content-based and contextual data gathered from web pages. This data detects patterns that indicate the presence of advanced persistent threats (APTs) and other complex attacks that may evade other systems.



F5 provides a wide breadth of VNFs within the NFV architecture.

Flexible Deployment Options

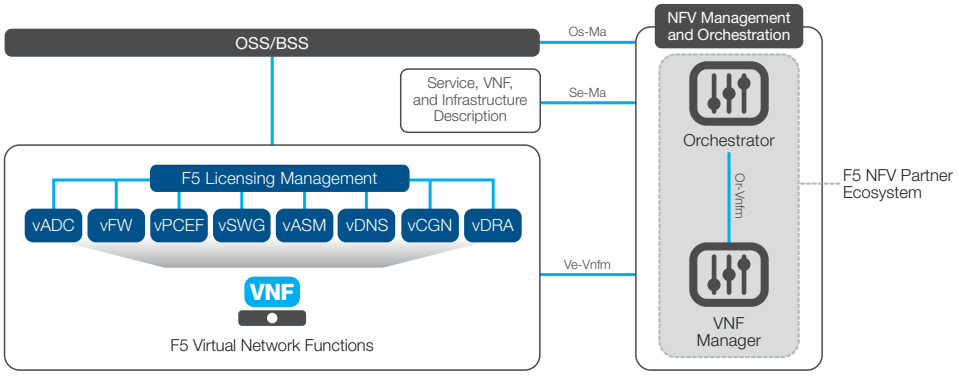
Whether you are deploying a completely virtualized network or migrating only certain network elements as VNFs, the F5 portfolio of BIG-IP and SDC products supports both virtual editions as well as purpose-built hardware platforms. All F5 solutions are built on top of the TMOS operating system, allowing you to seamlessly transition your networks from the F5 VIPRION® chassis and BIG-IP appliances to virtual editions. You can maintain a hybrid network architecture that can be tailored and customized based on your network requirements and NFV migration roadmap—while providing a high quality of service for your subscribers.

Management and Orchestration

Achieving the benefits of NFV requires a robust, flexible management and network orchestration system. Service providers must be able to introduce new services to market with greater agility and velocity. They also need to develop elastic networks that can dynamically spin up and spin down multiple network function instances based on network capacity or specific service requirements.

NFV aims to reduce vendor lock-in, especially as it relates to managing and orchestrating VNFs. As a service provider, you would ideally have a primary management and orchestration system that manages multiple vendor VNFs and the existing legacy hardware in the network. On the management and orchestration (MANO) front, you can deploy F5 VNFs and integrate with the NFV orchestrators and SDN controllers of a preferred choice of vendors.

F5 is an active participant in the broader NFV ecosystem and can plug into multiple systems based on your requirements and preferences. F5 VNFs have standard APIs and REST APIs that can seamlessly be integrated into leading orchestration solutions including Alcatel-Lucent Cloudband, HP NFV Director, Cloudstack, Cisco, OpenStack, Open Daylight, Openflow, Puppet, and Chef—allowing ease of provisioning, instantiating, and managing VNFs in the network.



F5 VNF integration with management and orchestration systems.

Supported Hypervisors

F5 offers the most flexible deployment options with support across all major virtualization platforms. F5 VEs support the broadest range of major hypervisor and virtualization platforms for VMware, KVM , Xen, Hyper-V, and Linux.

	LAB	25M	200M	1G	3G	5G	10G
VMware vSphere	●	●	●	●	●	●	●
KVM and community Xen	●	●	●	●	●	●	●
Citrix XenServer	●	●	●	●	●	●	●
Microsoft Hyper-V	●	●	●	●	●		

Standards-Based Architecture

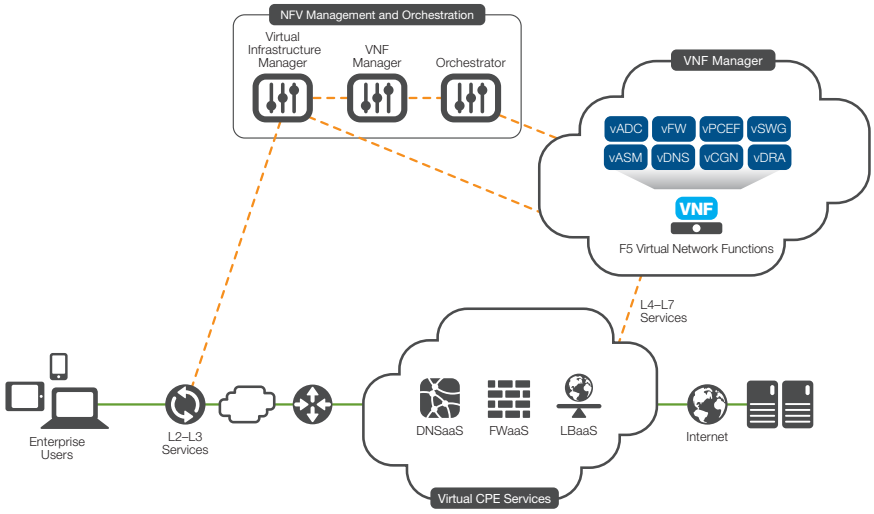
NFV has gained momentum in large part due to service provider initiatives for deploying a cost-effective, scalable, and elastic network—as well as the push by industry standards bodies to standardize NFV deployment. F5 is a member and actively participates in ETSI NFV, IETF, Openstack Forum, Open Networking Foundation, and other NFV/SDN standards bodies and consortia, ensuring that F5 solutions can be integrated within your NFV network architecture.

Use Cases

Virtual CPE

Virtual CPE helps service providers leverage common NFV infrastructure for services deployed in the cloud and in the network. With NFV, where multiple core network functionality is offered, virtual CPE enables you to adopt a cloud model. The cloud model lets you share a common pool of resources and dynamically allocate physical compute and network resources to these VNFs. You can also deploy individual instances of virtualized network functions and offer them as services.

All F5 VNFs can be deployed as a service, including Load-Balancing (LBaaS), Firewall (FWaaS), and DNS (DNSaaS). By leveraging virtual CPE, you'll achieve faster deployments in the network, faster recognition, higher revenues from service monetization, and a higher ROI.

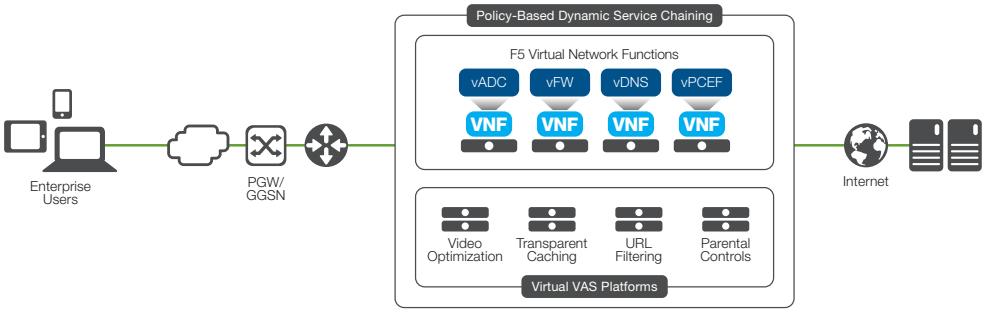


Use case: Virtual CPE using F5 VNFs.

Virtual Gi-LAN

Service providers can offer new services and optimize network traffic resources by using the network elements within their Gi-LAN. The Gi-LAN includes network elements such as firewalls, policy enforcement, and CGNAT—as well as video optimization, URL filtering, and content caching devices. Virtualizing the Gi-LAN enables you to build a cost-effective model, allowing for faster time to market to introduce new services while reducing network complexity.

F5 VNFs are a core component within your virtual Gi-LAN, providing solutions such as virtual policy enforcement, virtual firewall, and virtual Application Delivery Controller. These virtual solutions will enable you to provide intelligent traffic steering to VAS components. You'll be able to dynamically chain together services based on real-time subscriber and application awareness, as well as secure your Gi-LAN. This will allow you to innovate, improve subscriber QoE, and lower costs.



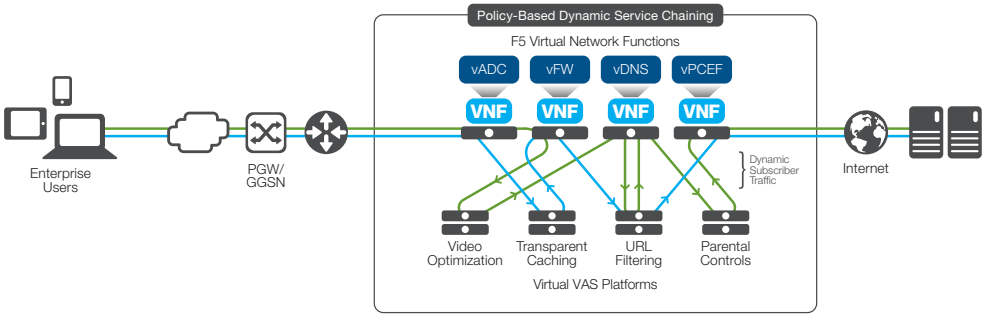
Use case: Virtual Gi-LAN using F5 VNFs.

Service Chaining

By leveraging SDN to abstract the control functionality from the underlying network and NFV, service providers can realize greater automation and virtualization—increasing agility while reducing OpEx and CapEx.

Service chaining allows you to develop new services by intelligently chaining multiple functions within the network. You'll have the agility and flexibility to dynamically chain functions together based on network or business requirements—without having to manually reconfigure network components. You can also reduce time to market and lower operational costs as you trial and deploy new network and revenue-generating services.

With BIG-IP intelligent traffic steering functionality, service chaining can be based on either having "meta header" information or applying service steering policies for each of the VNFs during the traffic flow.

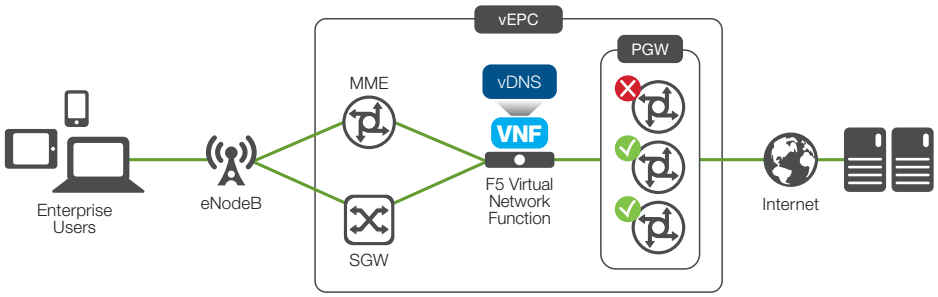


Use case: Service chaining using F5 VNFs.

Virtual EPC

A strategic component of the network that can be virtualized is the Evolved Packet Core (EPC). Virtualizing the EPC allows service providers to quickly realize significant TCO savings and increase speed to market in rolling out new services. In addition, service providers can reduce OpEx by dynamically spinning up and spinning down various network resources based on network demand and capacity.

BIG-IP VE solutions include virtualized GTP load balancers, policy management, and Diameter signaling solutions. F5's virtual ADC—based on BIG-IP LTM VE—helps you perform GTP load balancing among a group of PGWs/SGWs. And with the BIG-IP DNS solution leveraging its global server load balancing (GSLB) and dynamic gateway selection functionality, you can monitor virtual packet gateways and only provide answers to the DNS queries for gateways that are active and available. If a packet gateway goes down, BIG-IP DNS will distribute the traffic load intelligently across only the available packet gateways, ensuring the best subscriber experience.



Use case: Virtual EPC using F5 VNFs.

Carrier-Class Performance

When migrating your network from purpose-built hardware to a virtualized network built on commercial off-the-shelf (COTS) hardware, you should not have to compromise on network performance, scalability, and reliability. F5 VNFs can be scaled out to 40 Gbps and support x86 architectures that provide equal or better performance than purpose-built hardware.

Service providers will continue to build hybrid networks, with many compute-intensive services left on purpose-built hardware. These services include SSL, IPsec, video compression, and application delivery control. With a hybrid network approach, you can maintain key functionality on hardware while evolving VNFs in the same network. This also enables you to place ADCs in front of VNFs—effectively scaling them out and providing the high availability that you demand in your network.

F5 VNFs

All F5 VNFs are F5 virtual editions that run on the TMOS operating system. All BIG-IP modules are available as VNFs and can be purchased by throughput tier from the 10M non-production lab license to the 25M, 200M, 1G, 3G, 5G, and 10G production licenses.

Virtual Network Function	F5 Virtual Edition	License
Virtual Firewall (vFW)	BIG-IP AFM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual CGNAT (vCGN)	BIG-IP AFM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual Policy Charging Enforcement Function (vPCEF)	BIG-IP PEM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual Content Insertion (vCI)	BIG-IP PEM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual URL Filtering (vURL Filtering)	BIG-IP PEM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual TCP Optimization (vTCPO)	BIG-IP VEs	Lab/25M/200M/1G/3G/5G/10G
Virtual Application Delivery Controller (vADC)	BIG-IP LTM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual SIP Routing and Load Balancing (vSRLB)	BIG-IP VEs	Lab/25M/200M/1G/3G/5G/10G
Virtual DNS (vDNS)	BIG-IP DNS VE	Lab/25M/200M/1G/3G/5G/10G
Virtual Web Application Firewall (vWAF)	BIG-IP ASM VE	Lab/25M/200M/1G/3G/5G/10G
Virtual Secure Web Gateway (vSWG)	BIG-IP APM VE	Lab/25M/200M/1G/3G/5G/10G

Conclusion

F5 VNFs are interoperable with leading management and orchestration systems—providing a complete NFV ecosystem. You'll have a flexible, agile, and scalable network that helps you deliver services faster to market, improve network efficiency, and reduce CapEx and OpEx.

Learn more about the F5 NFV Architecture at f5.com/serviceprovider.

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 f5j-info@f5.com

©2018 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. DC0518 | OV-SP-234981316 0518