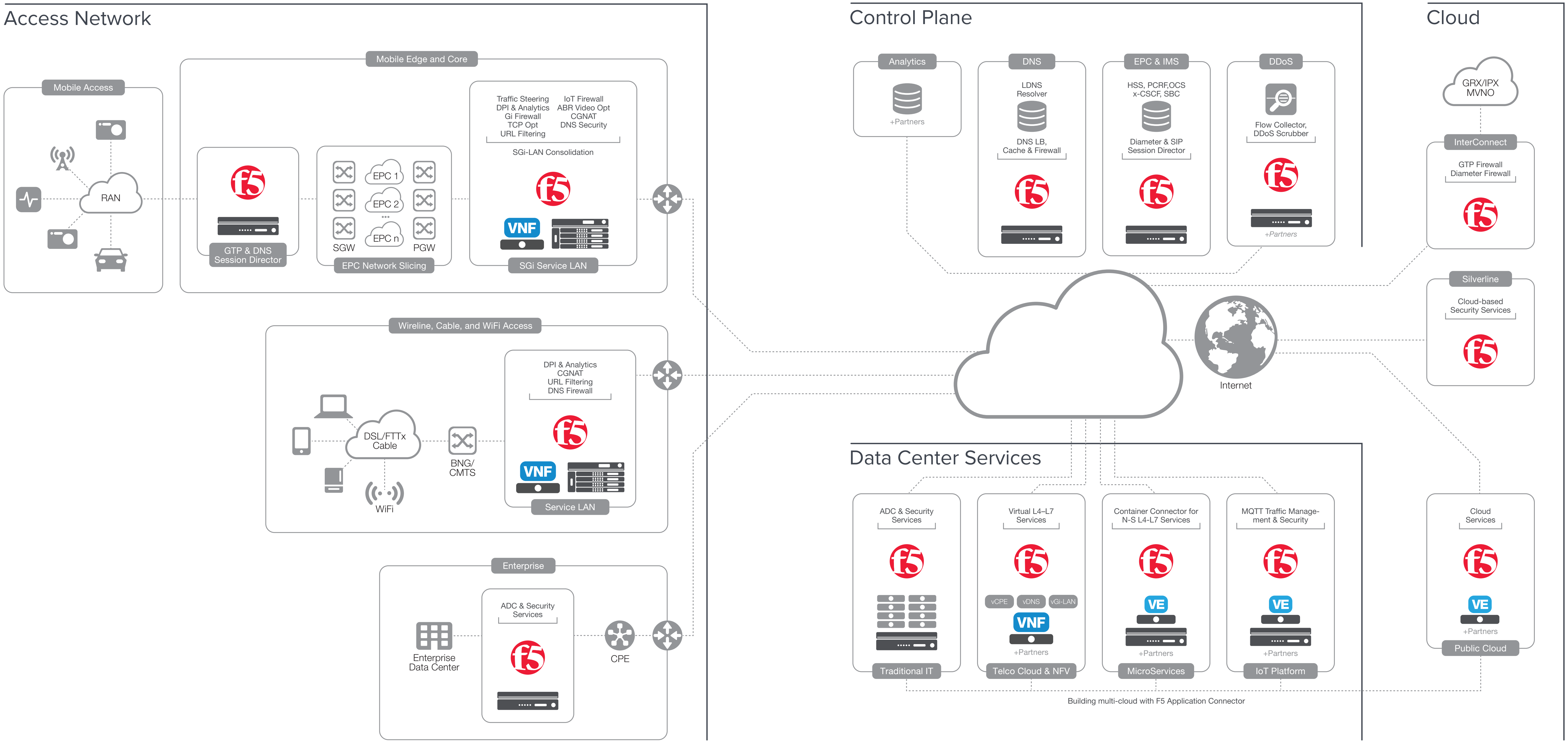
Solutions Guide

F5 solutions for the emerging 5G landscape

F5 Solutions

for the emerging 5G landscape.



Networks continue to evolve in the face of ever-growing traffic volume and complexity—as well as the increasing pressure to reduce costs, grow the business faster, and drive profitability. 5G accelerates this transformation of the network. It enables new services and applications, from the RAN to the cloud: connected cars, smart homes, IoT smart meters, and more.

F5 provides end to end solutions for 5G enablement today. We offer service velocity, scale, a unified and easy way to control and manage application services across the network, and the ability to protect your network and your customers in this era of rapid digital transformation.

Your network. 5G ready.

USE CASE 1

GI LAN CONSOLIDATION IN THE ACCESS NETWORK

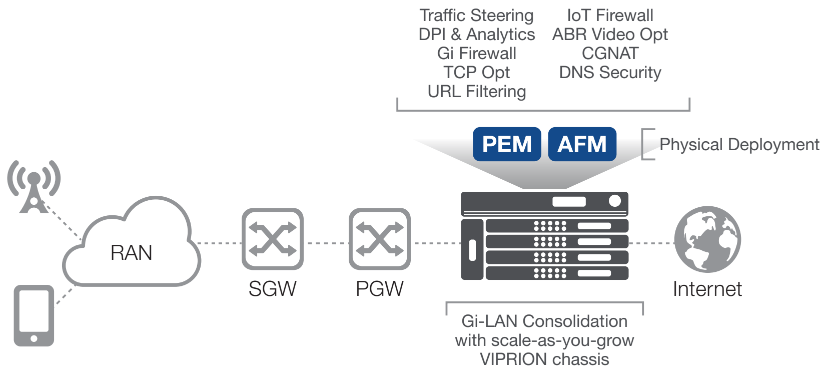
F5 consolidates multiple L4-L7 functions into a single, cost-effective, simple solution—and enables service providers to rationalize the number of different vendors and operating systems in the network. Of all these functions, the most important are TCP / IP optimization, Gi Firewall, CGNAT, traffic steering, deep packet inspection, URL filtering, and DNS security.

The F5 Gi LAN solution also includes newer functionalities which are important in the context of evolving the network to 5G—including ABR video optimization, and a device-aware IoT firewall.

F5 offers the Gi LAN solution in both physical and network function virtualization (NFV) environments. In an NFV environment, F5 can deliver a highly scalable solution that leverages our in-house load balancing technology to provide the scale-out, failover, and redundancy mechanisms you need.

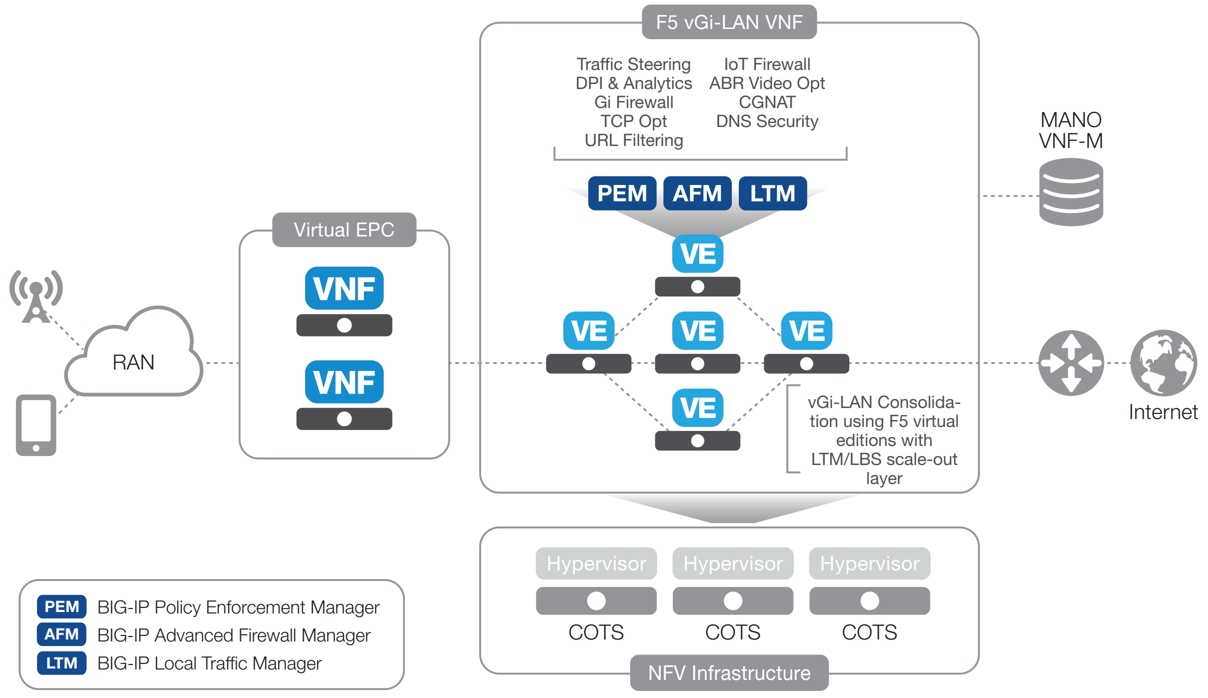
MOBILE ACCESS PHYSICAL SGI-LAN DEPLOYMENTS

Consolidation of multiple functions increases efficiency.



MOBILE ACCESS VIRTUAL SGI-LAN DEPLOYMENTS

Highly scalable network function virtualization.



PEM	BIG-IP Policy Enforcement Manager
AFM	BIG-IP Advanced Firewall Manager
LTM	BIG-IP Local Traffic Manager

USE CASE 2

MOBILE ACCESS AND NETWORK SLICING IN THE ACCESS NETWORK

Network Slicing

An important characteristic of the new 5G architecture is the ability to “slice” the network in different segments, all the way from the radio network into the core. This allows providers to dedicate resources to different use cases, and allocate those resources in the best possible way. For example, a self-driving car requires ultra-low latency and high throughput from the radio and core network; but smart metering can function with much higher latency and lower throughputs.

The 5G radio and core standards have been designed with network slicing in mind. In the 5G non-standalone architecture, the 5G radio will be connected to an existing 4G core network—which doesn’t support network slicing by nature. For service providers that wish to introduce network slicing in a 4G core network, F5 can enable this with its GTP session directors and DNS session directors.

GTP Session Director

The F5 GTP session director allows providers to create different SGW-PGW slices based on characteristics that are much more granular than what standard DNS techniques can provide. The GTP session director can intercept GTP-C messages and, based on a locally configured policy (using GTP-C attribute filtering), can steer GTP-C messages to the right SGW and/or PGW.

DNS Session Director

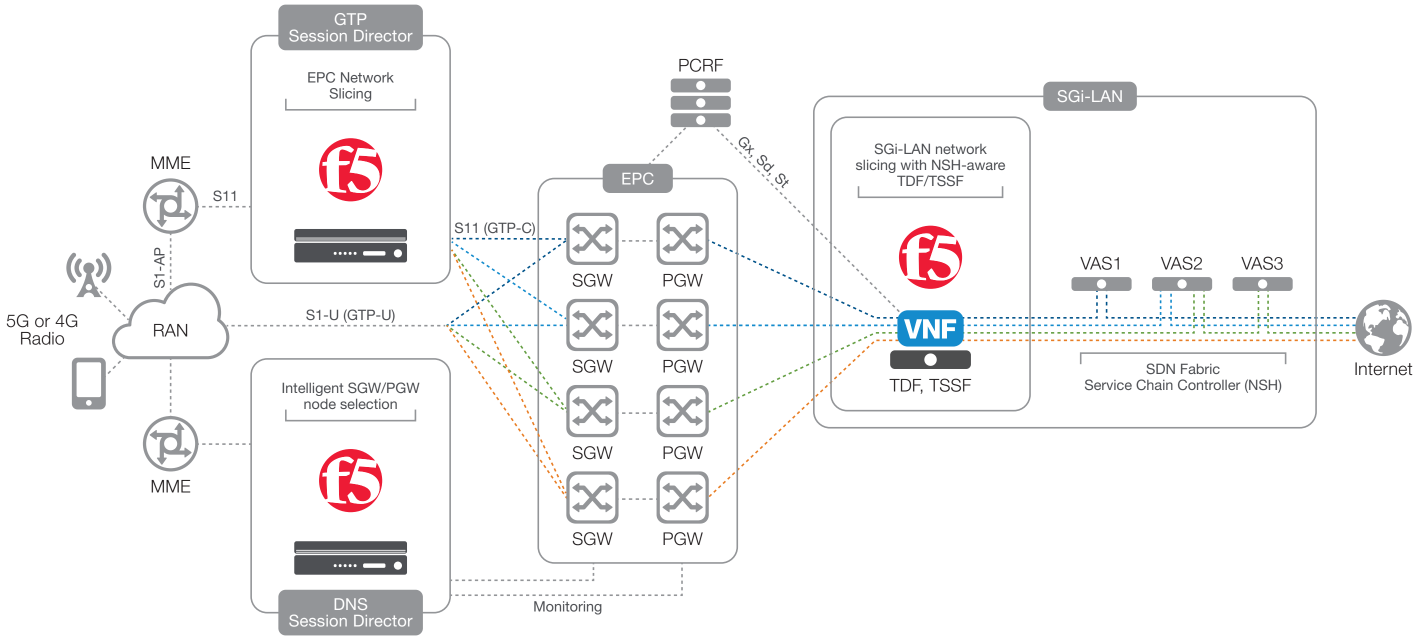
The DNS session director can be leveraged to influence standard DNS responses so they spread GTP sessions over the available SGWs and PGWs. It actively monitors the SGWs and PGWs and ensures that when the MME sends a DNS request to find the IP address of a SGW or PGW, no IP address will be returned for a SGW or PGW that is operationally down.

TDF (traffic detection function) **or** **TSSF** (traffic steering support function) **for Gi LAN network slicing**

Network slicing on the Gi LAN can be obtained via a policy-controlled traffic steering and service chaining function—both a TDF and TSSF function offer this capability. The PCRF provides a user- or device-specific steering policy to the TDF/TSSF to get the necessary “slicing” function applied in the rest of the Gi LAN. In addition to traditional per-subscriber proxy-based steering and service chaining, F5 now also supports the IETF NSH model, whereby an NSH header is added to the packets. This allows the SDN network and the participating service function nodes (VAS) to figure out what service to apply, and where to forward the packet next.

MOBILE ACCESS—EPC NODE SELECTION & NETWORK SLICING SOLUTIONS

Radio access to core network slicing solutions for resource allocation.



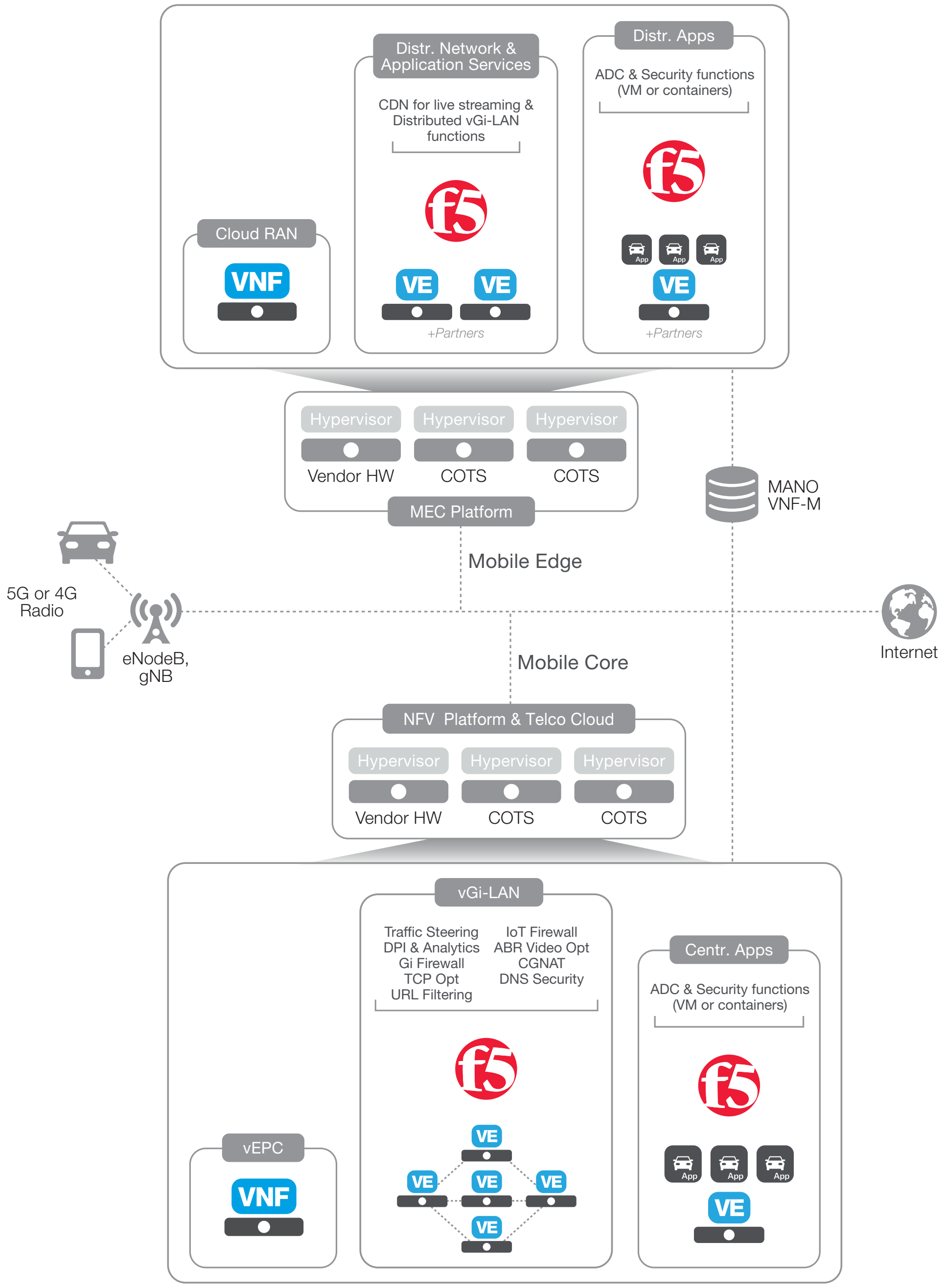
USE CASE 3

MULTI-ACCESS EDGE COMPUTING IN THE ACCESS NETWORK

Multi-access edge computing allows providers to deploy applications and network functions much closer to their end users. F5 provides Virtual Edition software for all of its L4-L7 networking functions, so these solutions can be deployed either centrally, or in a distributed way.

F5 can provide distributed virtual Gi LAN functions at the MEC level; but it can also provide Application Delivery Control (ADC) and security services for applications that are deployed as micro-services within containerized infrastructures.

GETTING 5G READY AT THE EDGE



USE CASE 4

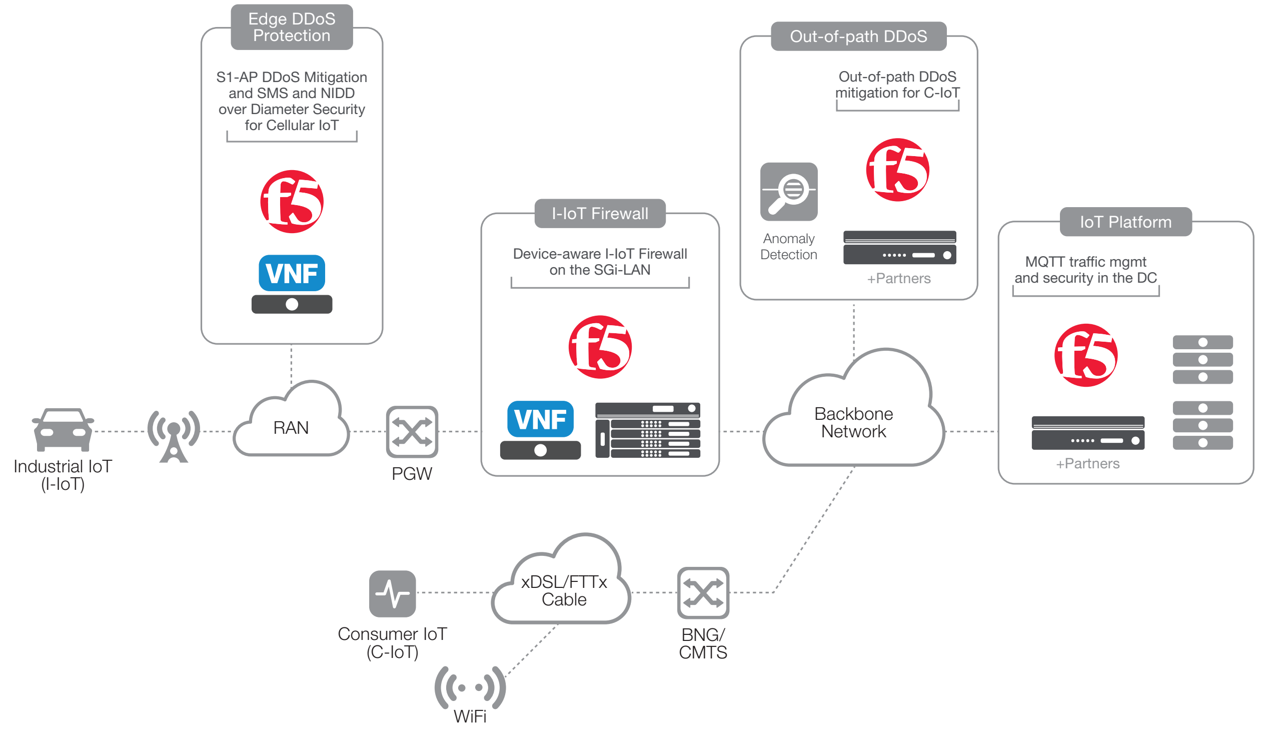
SERVICE PROVIDER IoT SOLUTIONS IN THE ACCESS NETWORK AND THE DATA CENTER

F5 provides solutions for IoT traffic management and security in both the service provider network and the data center. The IoT firewall is a Gi firewall dedicated to IoT devices. It can manage and control which sites, based on IP addresses or URLs, are accessible to and from the IoT device—on a per-device basis, optionally guided by a PCRF. An IoT device should typically connect to the IoT application itself and nothing else. F5 offers a subscriber-aware firewall that can install a security policy for each IoT device which eliminates the need to segment the Gi LAN for every single IoT use case.

In addition to solutions that control the "managed" industrial IoT devices connected to the network, F5 provides a solution to protect a service provider's network and infrastructure from attacks launched by "unmanaged" consumer IoT devices. Many of these C-IoT devices are connected to the network without the end users changing their default passwords, making them very vulnerable to becoming part of botnets that are remotely controlled by hackers. Together with Flowmon and other partners, F5 is working on a solution that allows the service provider to detect anomalies in the traffic so that bad actors can be isolated from the network and attacks mitigated.

When the service provider not only delivers the network connectivity for the IoT use cases but also the IoT platform itself, that IoT platform might need advanced MQTT (Message Queuing Telemetry Transport) traffic management capabilities as well as IoT security functions. MQTT is one of the more popular IoT protocols; F5 now has a protocol parser that enables our solutions to check the validity of MQTT messages by looking deep into the payload, provide intelligent load balancing, and offer smart authentication capabilities by copying SSL certificate information into the MQTT payload.

ACCESS, DATA CENTER, AND OUT-OF-PATH SOLUTIONS



Edge DDoS Protection
S1-AP DDoS Mitigation and SMS and NIDD over Diameter Security for Cellular IoT
VNF
I-IoT Firewall
Device-aware I-IoT Firewall on the SGi-LAN
VNF
Out-of-path DDoS
Out-of-path DDoS mitigation for C-IoT
Anomaly Detection
+Partners
IoT Platform
MQTT traffic mgmt and security in the DC
+Partners
Industrial IoT (I-IoT)
RAN
PGW
Backbone Network
Consumer IoT (C-IoT)
xDSL/FTTx Cable
BNG/ CMTS
WiFi

USE CASE 5

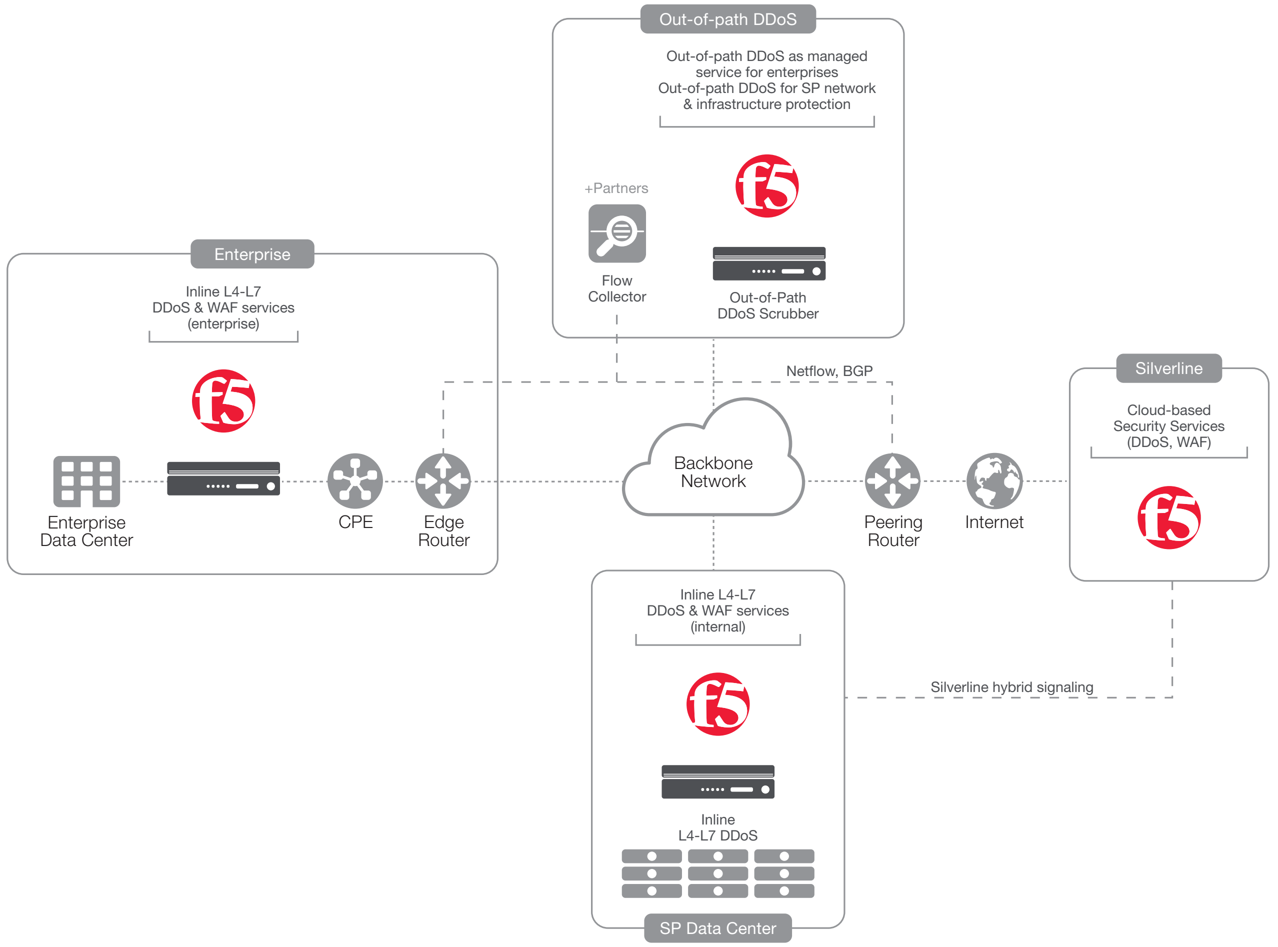
SERVICE PROVIDER DDoS SOLUTIONS IN THE ACCESS NETWORK, DATA CENTER AND THE CLOUD

F5 can provide a multi-tiered solution to help service providers mitigate against DDoS attacks. The first tier is delivered from the cloud by means of our Silverline cloud-based DDoS mitigation service. Service providers can use this service to mitigate against attacks aimed at saturating peering and/or transit links. No 'on-network' solution can isolate an attack that saturates incoming peering links.

The second tier of defense is aimed at mitigating volumetric attacks that occur inside the service provider network. At this tier F5 partners with Flowmon Networks, Genie Networks, and other partners, who collect NetFlow records from the edge and peering routers. When their solutions detect a volumetric attack, they instruct routers to drop the traffic or redirect it to an F5 scrubbing center that will clean the traffic and reinject it into the data path.

The third tier of defense is a pure inline solution that is either deployed as a clean pipe service on the customer's premises (for an enterprise), or at the service provider data center in front of application servers and control plane elements. The F5 inline solution provides highly effective and scalable mitigation against both volumetric L4 DDoS attacks as well as sophisticated L7 DDoS attacks (including OWASP top 10 attacks and WAF policies). F5 also provides intelligent DNS DDoS mitigation techniques.

SERVICE PROVIDER DDoS SOLUTIONS FOR MULTI-LAYER SECURITY



Out-of-path DDoS
Out-of-path DDoS as managed service for enterprises
Out-of-path DDoS for SP network & infrastructure protection
+Partners
Flow Collector
Out-of-Path DDoS Scrubber
Enterprise
Inline L4-L7 DDoS & WAF services (enterprise)
Enterprise Data Center
CPE
Edge Router
Netflow, BGP
Backbone Network
Peering Router
Internet
Silverline
Cloud-based Security Services (DDoS, WAF)
Inline L4-L7 DDoS & WAF services (internal)
Inline L4-L7 DDoS
SP Data Center
Silverline hybrid signaling

WE MAKE APPS

GO

FASTER. SMARTER. SAFER.

Learn more about F5’s service provider solutions at f5.com/solutions/service-provider

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com