



F5 for Service Providers

Jak čelit skutečným výzvám této doby v
Telco/ISP prostředí?

Martin Oravec, F5

m.oravec@f5.com



Impact of COVID-19

HEALTH AND SCIENCE

Italy to close all schools and universities through March 15 as coronavirus death toll rises

PUBLISHED WED, MAR 4 2020 5:09 AM EST | UPDATED 2 HOURS AGO

Holly Ellyatt
@HOLLYELLYATT

SHARE    

KEY POINTS

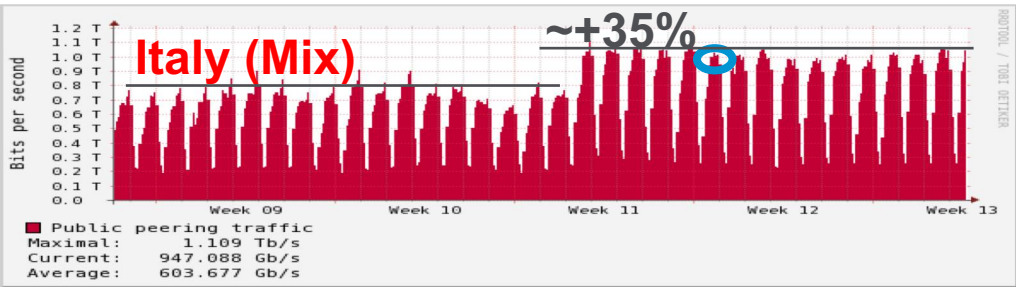
- Italy was the worst-affected country from the coronavirus outside Asia earlier Wednesday, temporarily overtaking Iran in terms of the number of deaths and infections from the virus.
- The death toll in Italy, Europe's worst-affected country, jumped to 79 on Tuesday from 52. As of Wednesday morning, there are 2,502 cases of the virus in Italy.

TRENDING



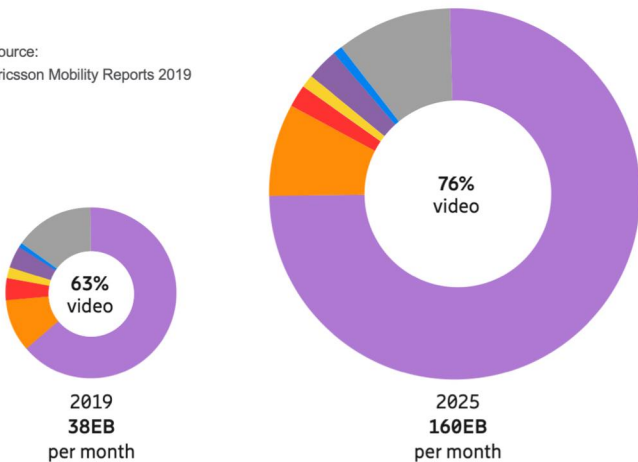
Vodafone reports 50% rise in internet use as more people work from home

Coronavirus places greater demand on network in Europe as families stay indoors



Video Social networking Web browsing Audio Software download and update P2P

Source:
Ericsson Mobility Reports 2019



¹ Traffic from embedded video in web browsing and social media is included in the application category "Video"

What Has Been Done by EU to Save Bandwidth



Thierry Breton  @ThierryBreton · Mar 18

Important phone conversation with @ReedHastings, CEO of @Netflix

To beat #COVID19, we #StayAtHome

Teleworking & streaming help a lot but infrastructures might be in strain.

To secure Internet access for all, let's #SwitchToStandard definition when HD is not necessary.

 368

 389

 621



[Show this thread](#)

Technology

Netflix to cut streaming quality in Europe for 30 days

🕒 19 March 2020 | 📄 76



 Share

US & WORLD / TECH / CORONAVIRUS

YouTube joins Netflix in reducing video quality in Europe

Streams now set to standard definition by default

By Jon Porter | @JonPorty | Mar 20, 2020, 6:17am EDT

TECH / AMAZON / NETFLIX

Amazon and Apple are reducing streaming quality to lessen broadband strain in Europe

Following in Netflix and YouTube's footsteps



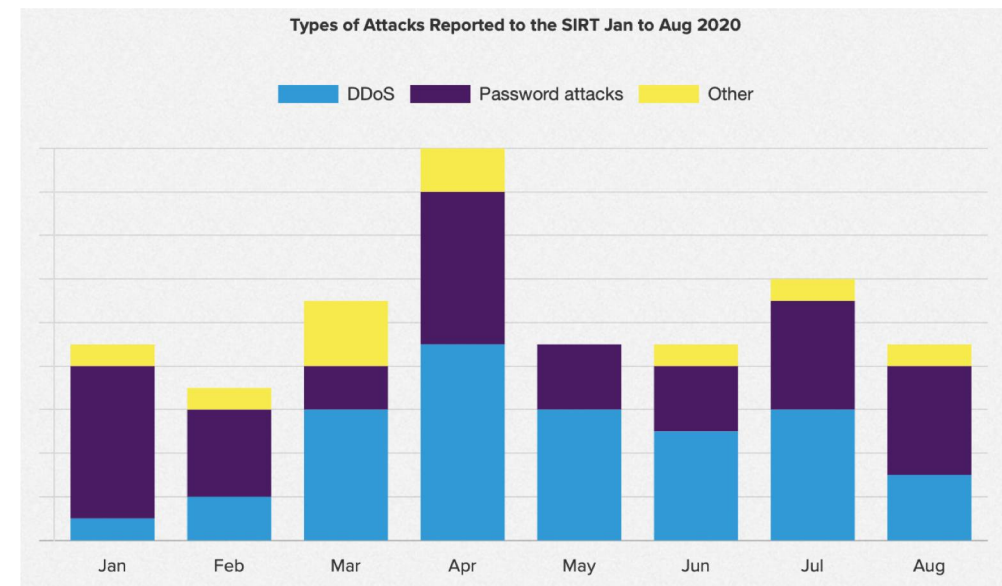
DDoS attacks increase

542 %

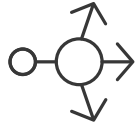
quarter-over-quarter amid
COVID-19 pandemic (*)

(*) Nexusguard Q1 2020 Threat Report

e.g. article to read - <https://www.f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic>

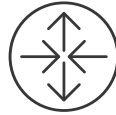


Service Provider Targeted F5's Solution Portfolio



Data Traffic Management

- SGi / Edge Network Simplification
- Intelligent Traffic Mgmt
- Dynamic Service Function Chaining
- Policy Enforcement
- TCP Optimization
- Video/ABR Optimization
- Deep Packet Inspection
- Content Filtering
- Traffic Detection Function



Signaling Traffic Management

- Domain Name System (DNS)
- SIP Traffic Management
- Diameter Solutions
- Radius, GTP and other Telco specific LB/Proxy
- Log's load-balancing, replication, ...



Security

- End-2-End Multi-Layered Dynamic Security
- Device Security
- Network Firewall
- Application Firewall
- Application Security
- DDoS Protection
- GTP Firewall
- VoLTE Firewall

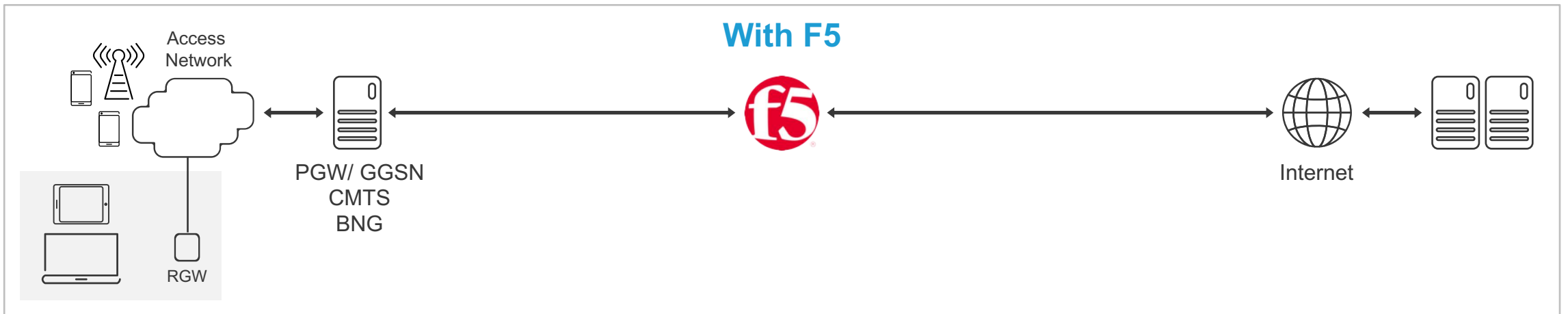
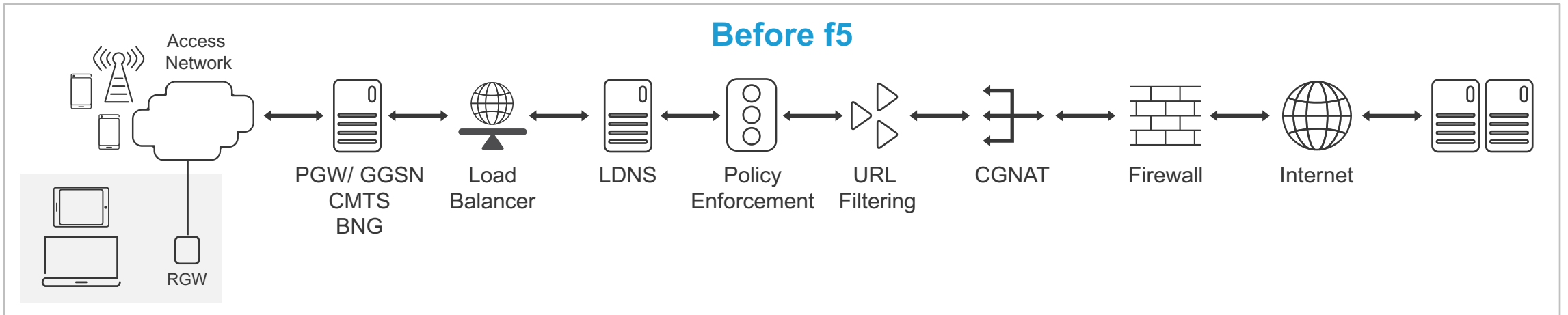


Virtualization / NFV / Edge / MultiCloud

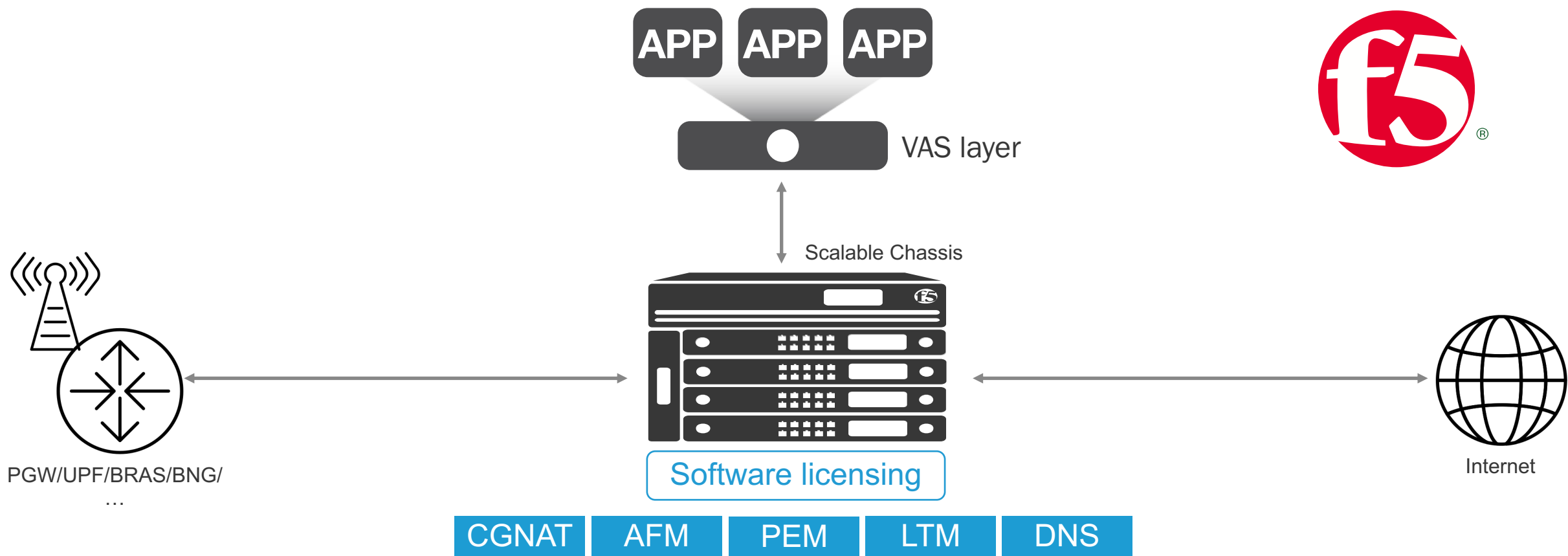
- Based on Virtual Edition
- Packaged NFV solutions
- Standalone VNF management and orchestration for custom solution
- Orchestrated Containerized Telco Edge
- TOSCA and ONAP aligned

A Different Approach with F5

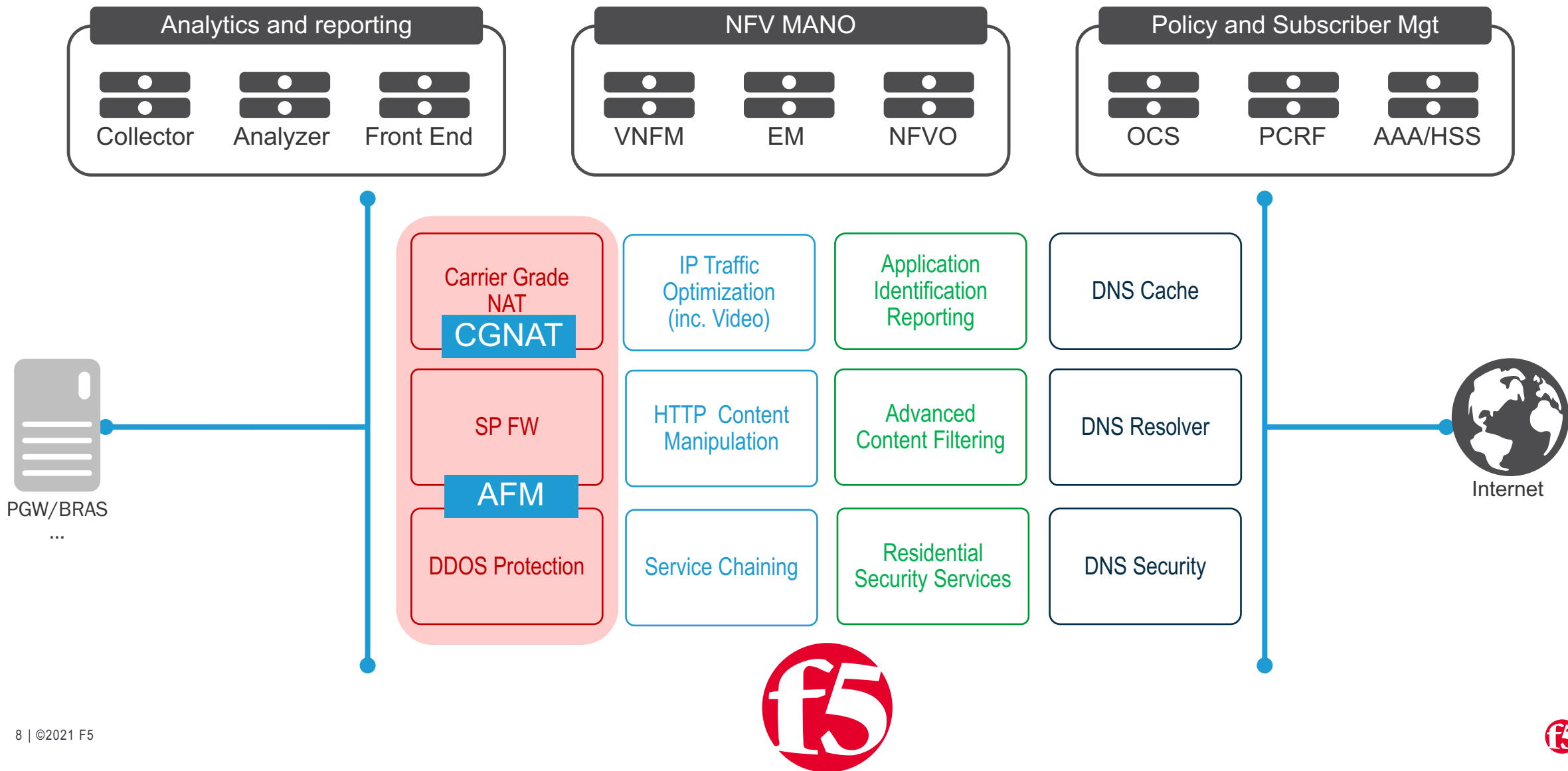
A UNIFIED PLATFORM SIMPLIFIES DELIVERY OF NETWORK SERVICES



How the scalability and consolidation works



F5 Solution SP Data Traffic Mgmt Solution summary



Carrier Grade NAT Overview



Translation Methods

- Network Address & Port Translation (NAPT)
- Port Block Allocation (PBA)
- Deterministic NAT (DNAT)
- NAT44
- NAT64 & DNS64
- Endpoint Independent Mapping
- Endpoint Independent Filtering
- Port Control Protocol (PCP)



Tunneling Methods

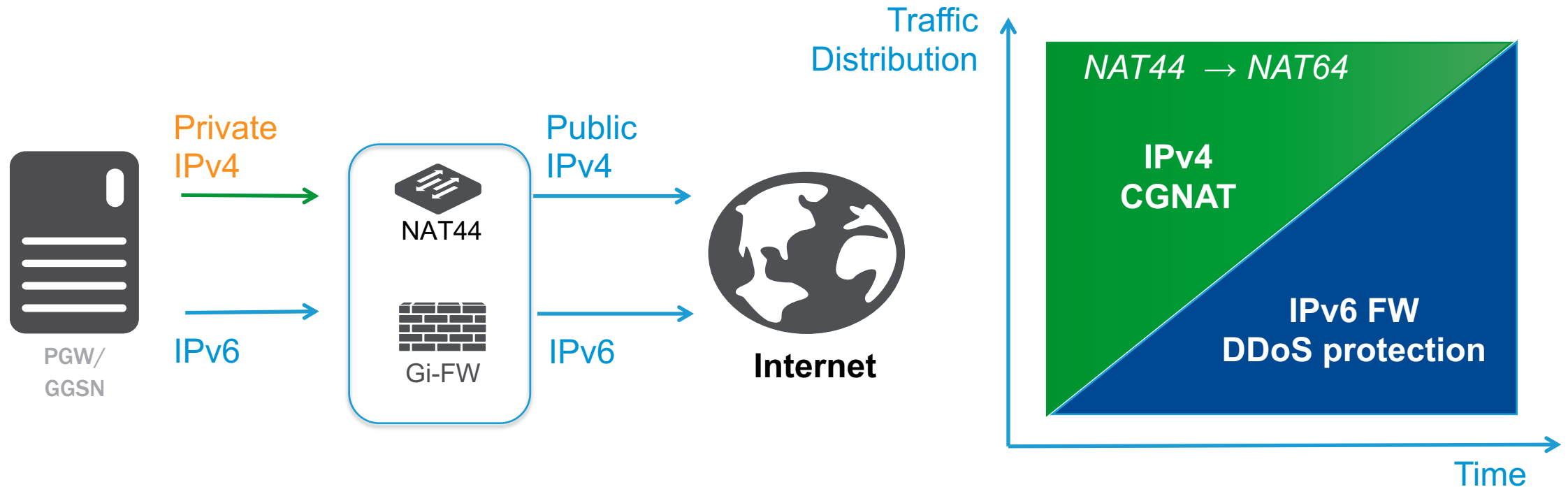
- DS-Lite support with AFTR
- 464XLAT
- 6RD
- MAP-E/MAP-T
- lw4o6



Logging Options

- High-speed logging – syslog based
- Customizable logging options
- IPFIX / Netflow Reporting
- Subscriber identity log enrichment
- Data Retention Compliances

AFM as Edge FW – CGNAT, IPv4/6 FW and anti DoS



UNPRECEDENTED SCALE
&
PERFORMANCE

GRADUAL TRANSITION
FROM IPV4 CGNAT TO
IPV6 FW AND DDOS

INVESTMENT
PROTECTION

AFM - FW Policy Editor

ID	Name	State	Protocol	Source	Destination	Actions	Logging
1	rule-icmp <input type="checkbox"/> Auto Generate UUID Description	<div>Scheduled ▼ Schedule: work-time ▼</div>	<div>ICMP ▼ Type : Code (Any) : </div>	<div>VLANs vlan_20 add new source Add</div>	<div>(Any) add new destination Add</div>	<div>Action: Accept ▼ iRule: None ▼ Send to Virtual: None ▼ Service Policy: None ▼ Protocol Inspection Profile: None ▼ Classification Policy: None ▼</div>	<input checked="" type="checkbox"/> Logging
<div> <div> <div>Name</div> <div>work-time</div> </div> <div> <div>Partition / Path</div> <div>Common</div> </div> <div> <div>Description</div> <div></div> </div> <div> <div>Date Range</div> <div>Indefinite ▼</div> </div> <div> <div>Time Range</div> <div>Between... ▼ 08:00 to 18:00</div> </div> <div> <div>Days Valid</div> <div> <input type="checkbox"/> Sunday <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input type="checkbox"/> Saturday </div> </div> </div>							
			Any		www.f5.com	Accept Send to virtual: vs-f5.com	Yes
			Any	10.1.20.0/24	10.1.10.7	Accept	Yes
			UDP	Any	Addresses 10.1.10.10 10.1.10.20-10.1.10.23 10.1.40.0/24	Accept Service Policy: test-timer-policy	No
<input type="checkbox"/> 5	rule-test-port-misuse	Enabled	UDP	Any	Addresses 10.1.10.10 Ports 53	Accept Service Policy: test-port-misuse-policy	No
<input type="checkbox"/> 6	rule-default-internet	Enabled	Any	VLANs vlan_20	Any	Accept Classification Policy: policy-p2p-drop	No

Enabled
Disabled
Scheduled

an IPv4 or IPv6 address
an IPv4 or IPv6 address range
address list
a fully qualified domain name
geographic location
IP-Intelligence category
VLAN, Zone
port, port range, port list

AFM - (D)DoS Attack Vectors

- Manual Configuration
- Detection / Reporting only
- Auto-Threshold (Learning)
- Dynamic Attack Signatures
- Bad Actor and Attacked Destination Detection
- Ability to initiate BGP Blackhole, Redirect, Flowspec

Partition	Common
Description	
Threshold Sensitivity	Medium
Default Whitelist	None Manage Address Lists
Families	<input checked="" type="checkbox"/> Network <input type="checkbox"/> DNS <input type="checkbox"/> SIP

Filter Attack Vectors

State: --- Vector Type: --- Add Filter: ---

Network | 1 Vector Enabled, Dynamic Signatures Disabled

Network Family settings [Configure settings](#) (Includes Dynamic Signatures)

	Vector Name	Type	State	Threshold Mode	Detection EPS	Detection %	Mitigation EPS	Bad A
<input type="checkbox"/>	TTL <= <tunable>	Bad Header IPv4	Disabled					
<input type="checkbox"/>	IPv6 Hop Count <= <tunable>	Bad Header IPv6	Disabled					
<input type="checkbox"/>	IPv6 Extension Header Too Large	Bad Header IPv6	Disabled					
<input type="checkbox"/>	IPv6 Extended Header Frames	Bad Header IPv6	Disabled					
<input type="checkbox"/>	IP Option Frames	Bad Header IPv4	Disabled					
<input type="checkbox"/>	Too Many Extension Headers	Bad Header IPv6	Disabled					
<input type="checkbox"/>	Unknown TCP Option Type	Bad Header TCP	Disabled					
<input type="checkbox"/>	Option Present With Illegal Length	Bad Header TCP	Disabled					
<input type="checkbox"/>	TCP Option Overruns TCP Header	Bad Header TCP	Disabled					
<input type="checkbox"/>	TCP Flags-Bad URG	Bad Header TCP	Disabled					
<input type="checkbox"/>	IP Fragment Flood	Flood	Disabled					
<input type="checkbox"/>	IPv6 Fragment Flood	Flood	Disabled					
<input checked="" type="checkbox"/>	TCP SYN Flood	Flood	Mitigate	Fully Automatic	Infinite	500	Infinite	Enable
<input type="checkbox"/>	TCP SYN ACK Flood	Flood	Disabled					
<input type="checkbox"/>	TCP RST Flood	Flood	Disabled					
<input type="checkbox"/>	TCP Window Size	Flood	Disabled					
<input type="checkbox"/>	ICMPv4 Flood	Flood	Disabled					
<input type="checkbox"/>	ICMPv6 Flood	Flood	Disabled					
<input type="checkbox"/>	UDP Flood	Flood	Disabled					

Properties

TCP SYN Flood

State
Mitigate

Threshold Mode
☒ Fully Automatic
☐ Auto Detection / Multiplier Based Mitigation
☐ Manual Detection / Auto Mitigation
☐ Fully Manual

Attack Floor EPS
100

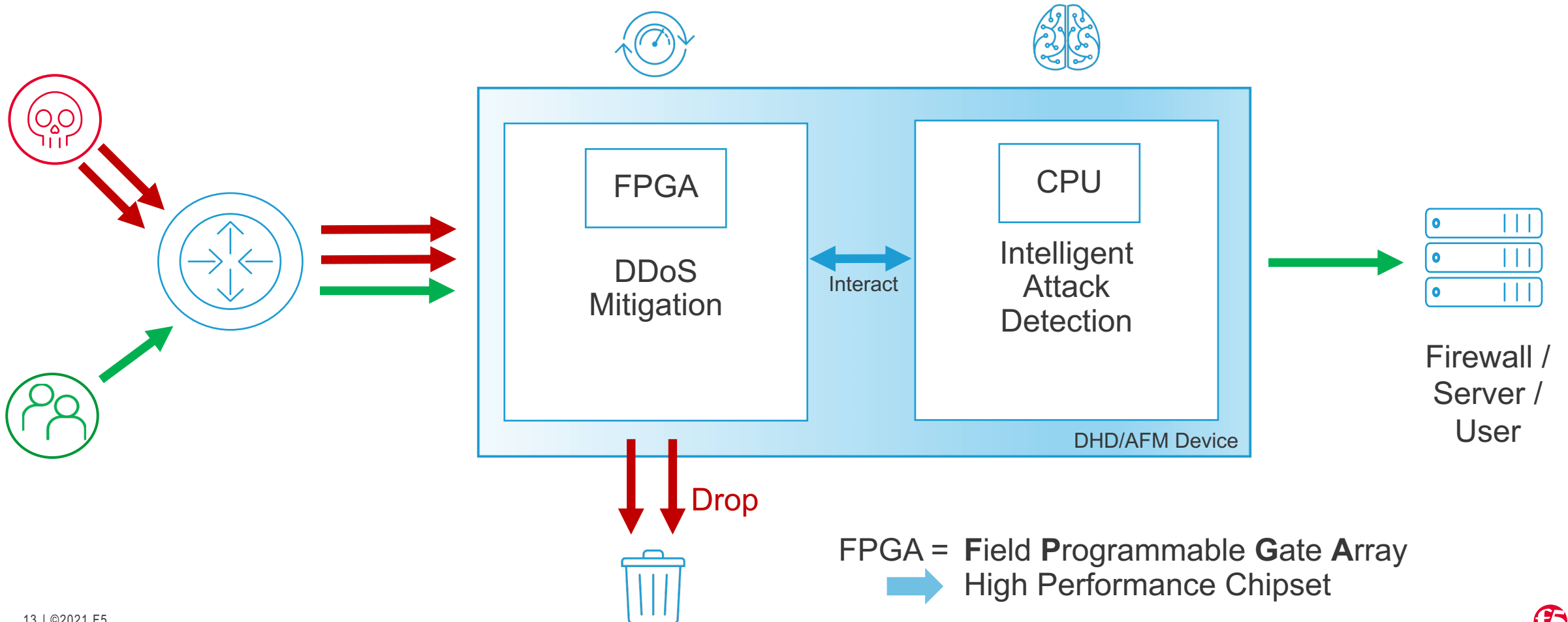
Attack Ceiling EPS
Infinite

☒ Bad Actor Detection
☒ Add Source Address to Category
Category Name
denial_of_service
Sustained Attack Detection Time
60 seconds
Category Duration Time
14400 seconds
☒ Allow External Advertisement

☒ Attacked Destination Detection
☒ Add Destination Address to Category
Category Name
attacked_ips
Sustained Attack Detection Time
10 seconds
Category Duration Time
900 seconds
☒ Allow External Advertisement

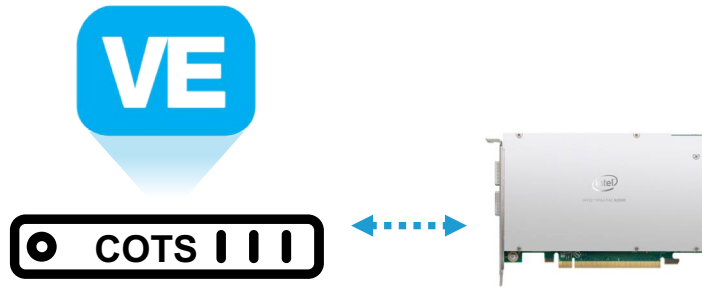
Logical separation of Mitigation and Compute Unit

CPU FOR SMART DETECTION AND FPGA FOR EFFECTIVE MITIGATION



Augmented DDoS Protection for NFV Environments

MITIGATE LARGER ATTACKS WHILE LOWERING CPU UTILIZATION AND TCO



BIG-IP VE for SmartNICs – DDoS Mitigation

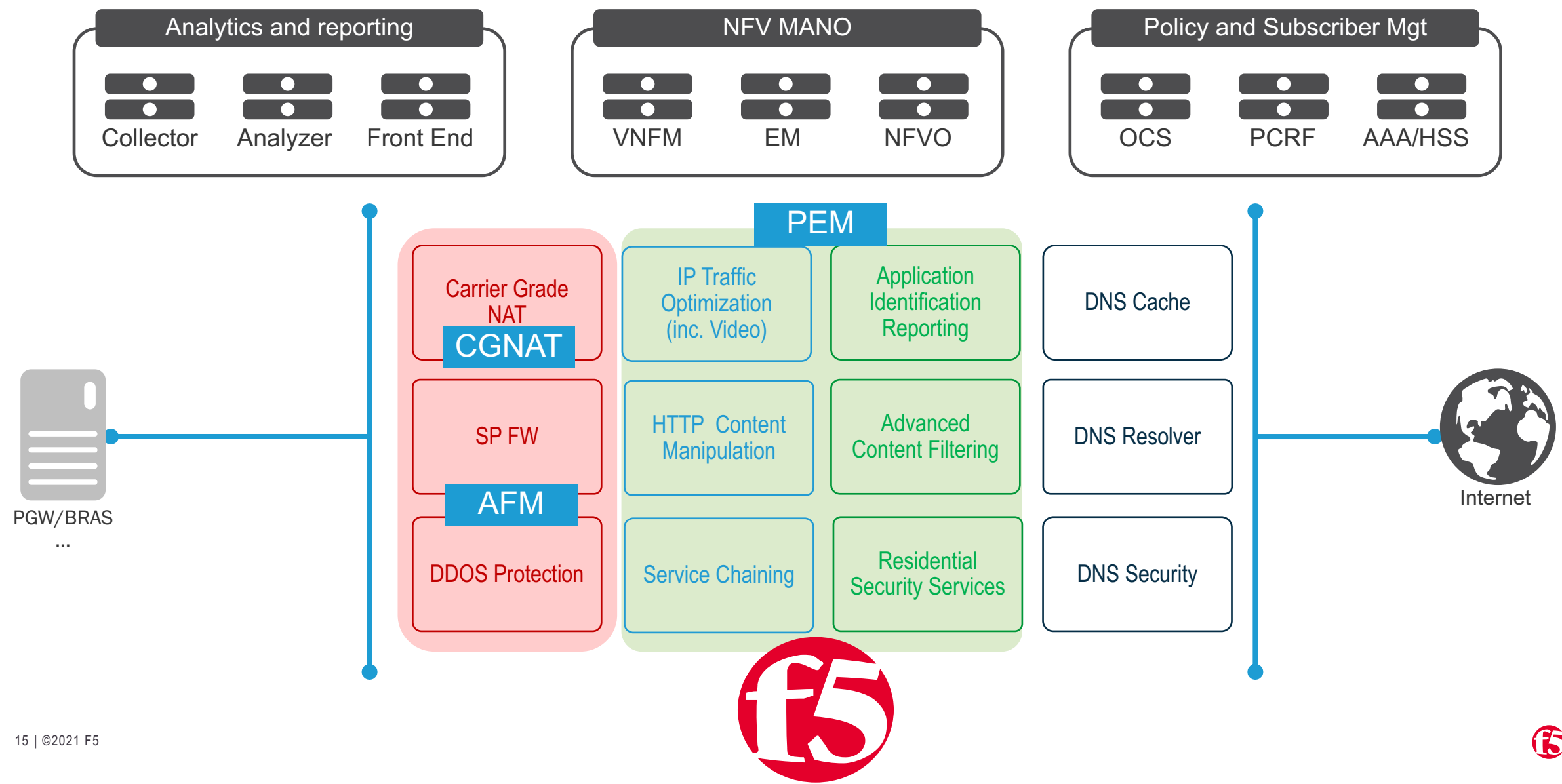
- Offload DDoS detection/mitigation to SmartNIC
- 100+ DoS vectors supported, as well as SYN cookies, allow-listing, BDoS
- 93% of all vectors handled in FPGA
- Packet inspection & drop both occur at line rate

20X greater DDoS mitigation capacity

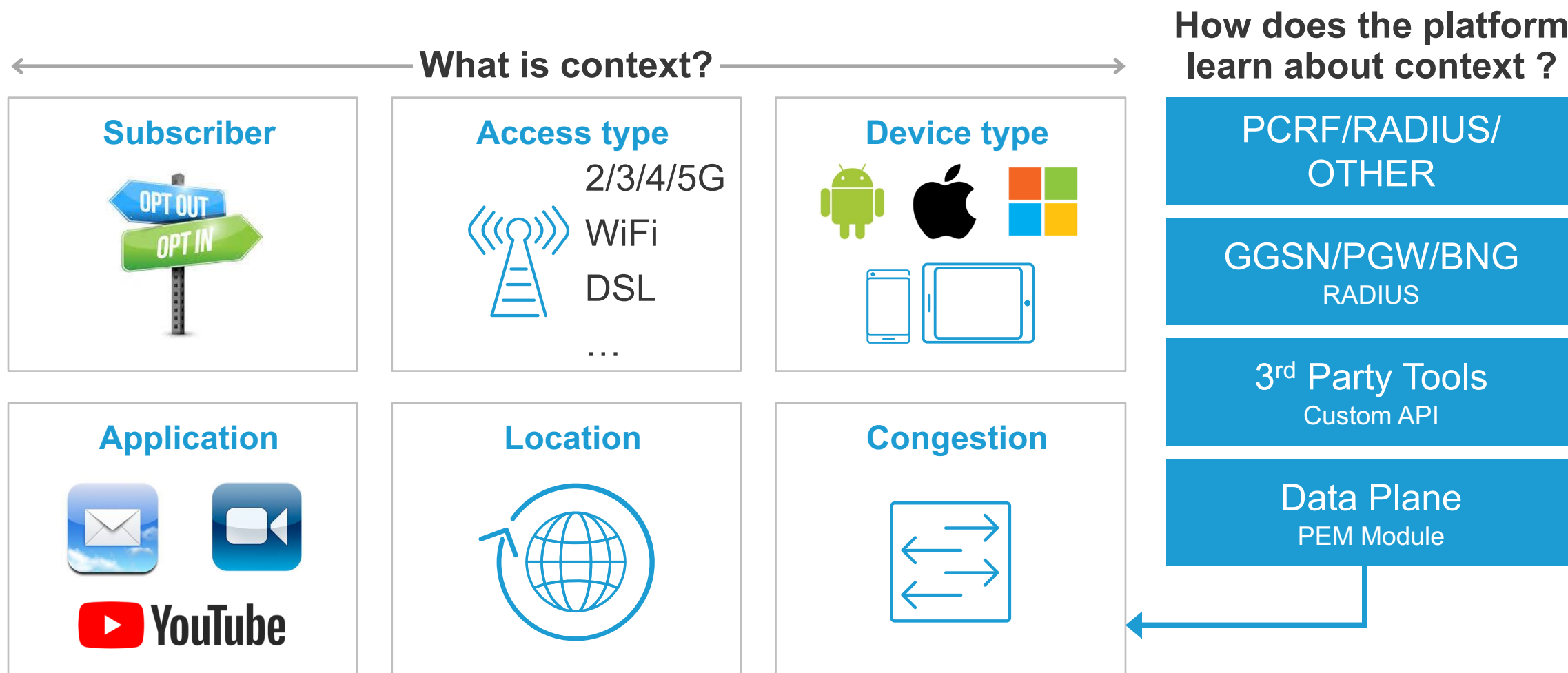
67% reduction in required compute

70% lower VE CPU utilization

F5 Solution SP Data Traffic Mgmt Solution summary

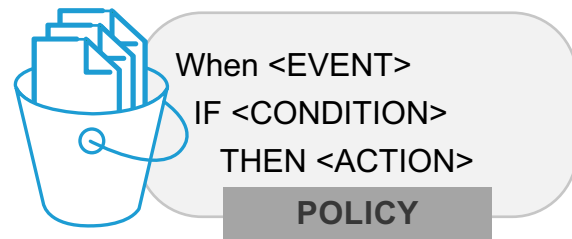


Context-Aware and Policy-Driven Traffic management



Policy is a set of rules.

A **rule** defines conditions that the traffic must meet (or not meet) for the rule to apply



A RULE

Condition

- Classification criteria – App / Category
- Flow information
- URL information
- Custom criteria

Action

- Allow / Drop traffic
- Traffic Optimization
- Forwarding traffic to a specific endpoint or series of endpoints for value-added services
- HTTP traffic redirection
- Headers Manipulation, Content Insertion
- Advanced Reporting
- Usage monitoring and reporting
- Traffic marking DSCP, L2 802.1p
- Enforcing rate control using a bandwidth control policy
- ...

F5 Approach for Video traffic control



ABR Video Detection and Classification with F5 Policy Enforcement Manager (PEM)

Ability to detect and classify traffic by using heuristic and deep packet inspection signature



F5 provides the capability to control video from the network layer for TCP based video traffic

Ability to apply Bandwidth control policies (per subscriber/per app) to rate limit TCP video



F5 provides the capability to control video from the network layer for UDP based video traffic

Ability to apply Bandwidth control policies pacing Video traffic over QUIC over UDP

Video Control Use Case 1 - Just in Time Emulation

Bandwidth saved for videos not played completely

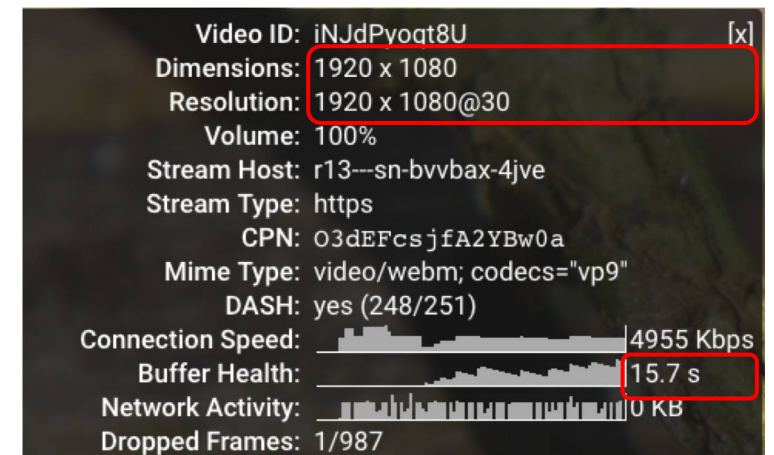
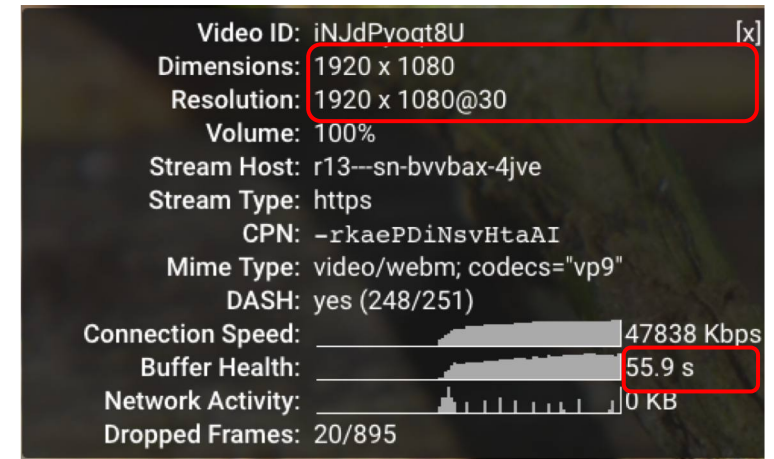
Saving Bandwidth while leaving the same Quality of Experience

No impact on resolution

Possible implementations

- Device type dependent
- Subscriber dependent
- RAT-Type dependent
- Dynamic (bandwidth saving)

YouTube Stats for Nerds



Video Control Use Case 2 - Resolution Control

Force ABR video to go to a lower resolution

Bandwidth saving

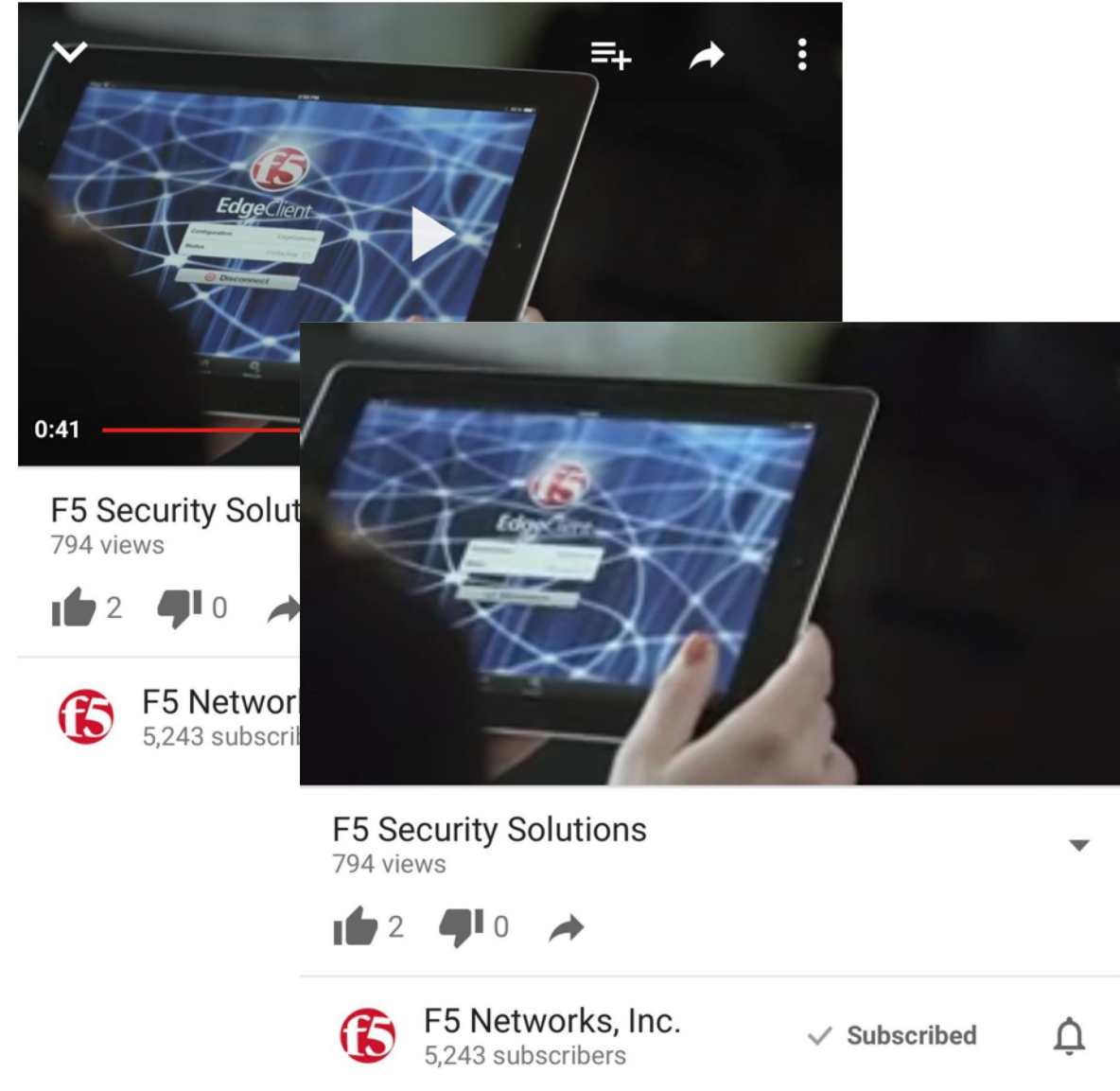
- Radio Network

Data Saving

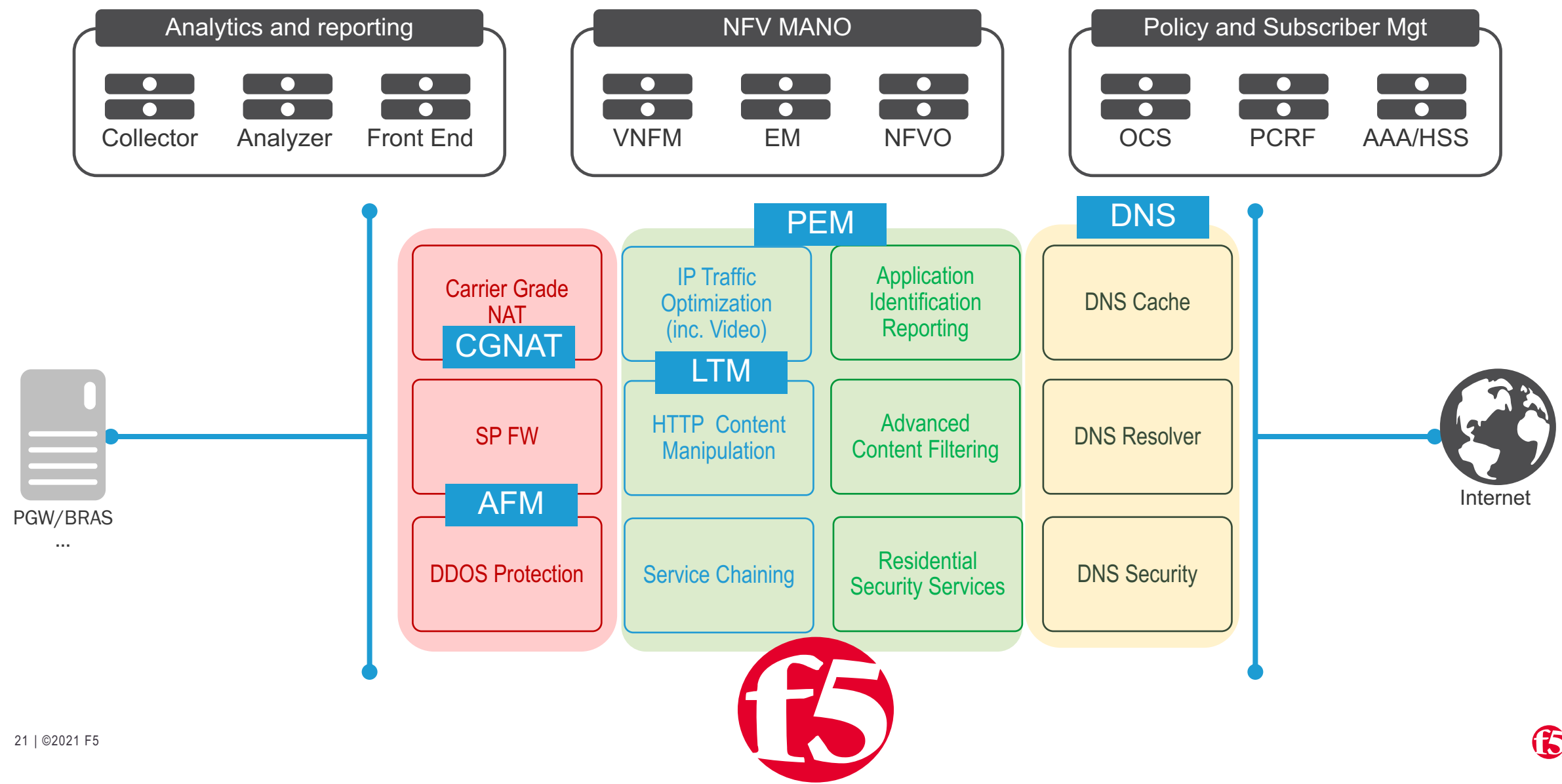
- Subscriber Quality of Experience for some traffic plans

Can be applied on a subscriber basis

- Dynamic provisioning
- E.g. Small Screen vs Large Screen



F5 Solution SP Data Traffic Mgmt Solution summary



Encrypted DNS

Flavors of Encrypted DNS

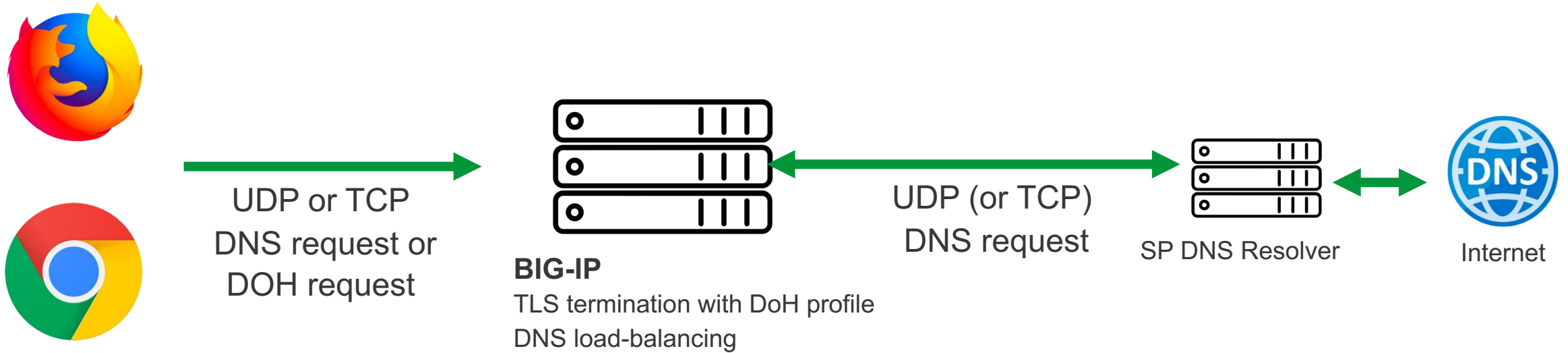
DNS-over-TLS (DOT)

- Adds privacy to DNS
- Impacts **Visibility** and **Control** of DNS

DNS-over-HTTPS (DOH)

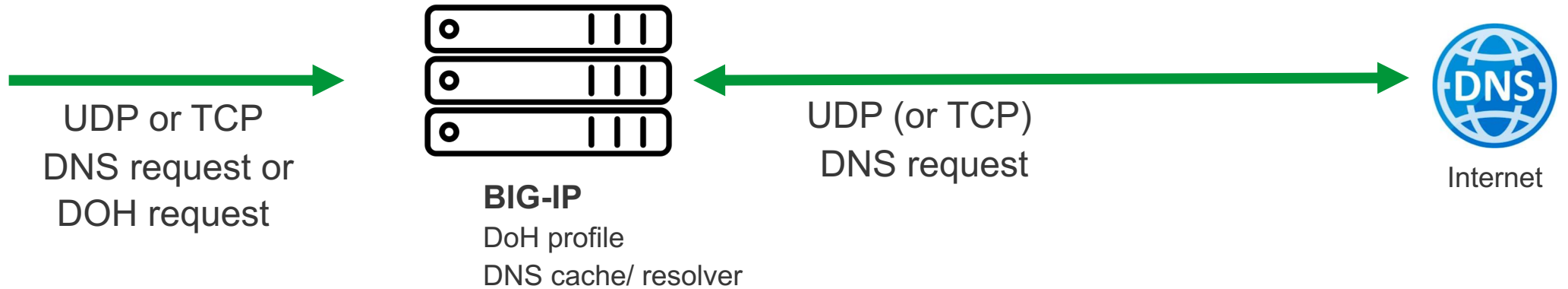
- Newer approach
- Impacts **Visibility** and **Control** of DNS
- Looks like web traffic – impossible to block
- Promoted by Browser vendors (Firefox, Chrome) and Over-the-Top DNS providers (Google, Cloudflare)

DoH/T TLS offload



- Customer wants to keep everything on the server-side the same way it was in the non-DoH previous slide
- Client IP preservation
- UDP or TCP server-side
- Protocol translation for Doh TCP to UDP or TCP options based on request size or can be forced to TCP if required

DoH/T (caching) Resolver



- Customer takes advantage of the DNS profile for security functionality
- UDP or TCP
- Protocol translation for Doh TCP to UDP or TCP options based on request size or can be forced to TCP if required

Going virtual? Serialized vs Consolidated

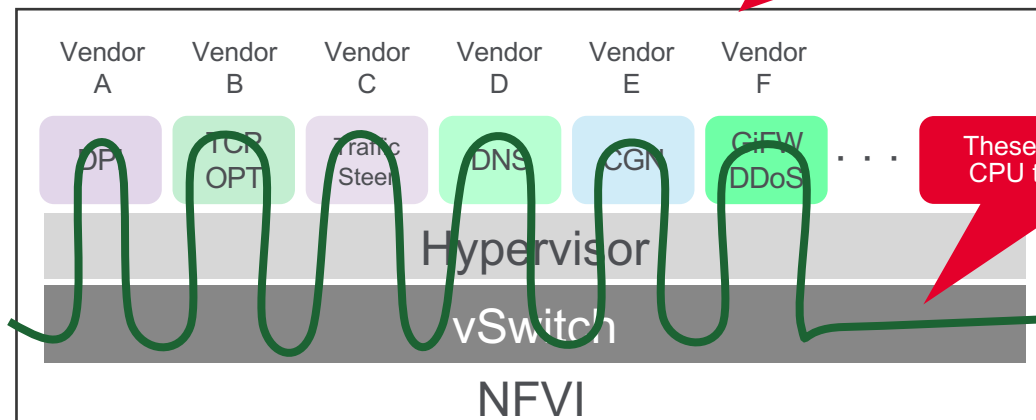
Serialized

- Increase the number of VMs
- Higher CPU usage -> re-calculate L2/L3 header
- Decrease performance due to virtual switch latency
- Complex network structure
- Increase OPEX/CAPEX due to operate huge number of VMs
- Orchestration Complexity

6x8vCPU=48vCPU

These function also use CPU to transfer packet

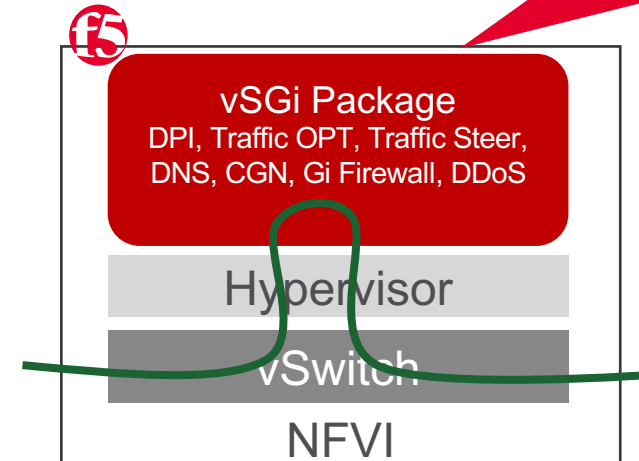
VS



Consolidated (Single Pass Architecture)

- Decrease the number of VMs
- Lower CPU usage
- Increase performance
- Simple network structure
- Decrease OPEX/CAPEX
- Simple orchestration policy

1x20vCPU=20vCPU
60+% reduction



F5 VNF deployment public reference Rakuten

Single VNF Image for Full SGi-LAN Services

- ✓ Common OS for CGNAT, DPI, DDoS, FW, IPS, Service Chaining, Load Balancing, DNS, Parental Control, illegal site blocking, etc
- F5 minimizes Latency – Less CPU hops
- Optimized resource consumption
- Service Chaining (FMSS) Support for Consumer & Enterprise Managed Security Service Creation – “Secure Internet” Services

<https://www.f5.com/company/news/press-releases/f5-partners-with-rakuten-mobile-to-support-new-cloud-native-mobi>

