Security & DDOS solutions for core SP infrastructure:
(In)Security in the Internet-of-things age

Bernd Kunze

SP Solutions Architect EMEA

50000000000 connected devices by 2020

2014 John Chambers CES Keynote puts IoE at $19 Trillion dollar opportunity:

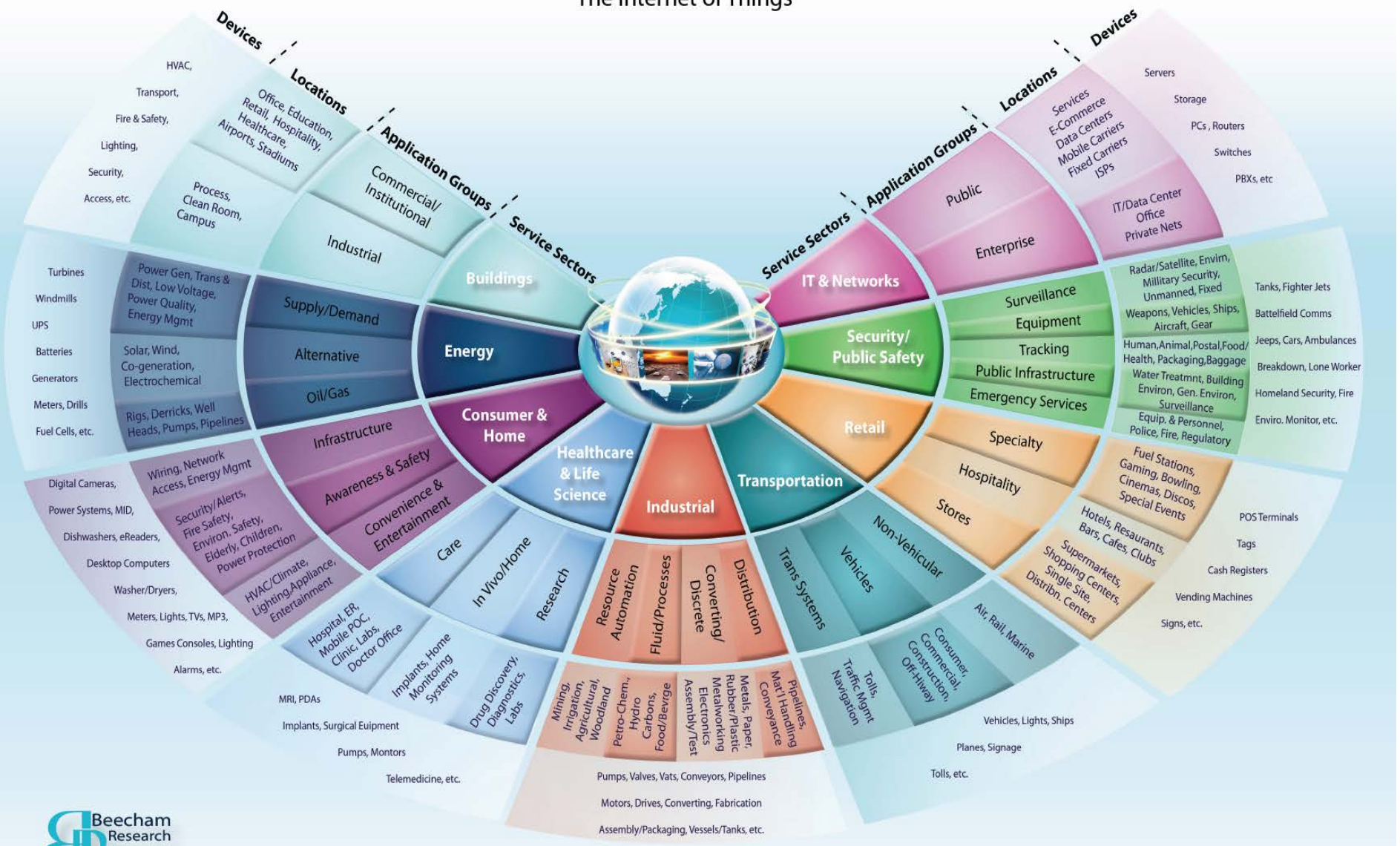
"Cisco predicts that the IoE Value at Stake will be **$14.4 trillion** for companies and industries worldwide in the next decade. More specifically, over the next 10 years, the Value at Stake represents an opportunity to increase global corporate profits by about 21 percent."

144000000000000000000 $ =
127208448000000000000 €*

*As of 4/13/16

M2M World of Connected Services

The Internet of Things



Beecham Research

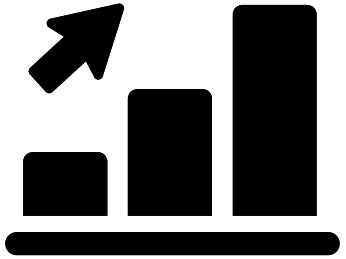
Boston | London

info@beechamresearch.com +44 (0)845 533 1758 www.beechamresearch.com

IoE: Paradigm Shift In Networking

Network Connectivity

- *Scale and performance*
- *Explosion of IP addresses (Relax: IPV6 offers 665,570,793,348,866,943,898,599 per square meter)*
- *Longer lived connection*
- *Low data volume*
- *High session setup rates*



Application Requirements

- *Scale and performance*
- *Big Data grows even bigger*
- *Control plane and data plane*
- *Signaling overload protection*
- *Always-on requires data availability at all times*
- *Network flexibility to address spikes in usage*

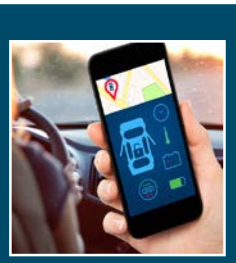
Maintaining Security

- *Millions of unpatched devices*
- *Network side defense*
- *Prevent IoE morphing into IoB*
- *DDoS protection to and from IoE's*
- *Compliance and privacy*
- *StrongerCryptography*

Profitability

The IoE Network Effect

- **SCALING** networks
- End-to-End **SECURITY**
- **PROFITABLE** new services



Connected Cars

Connected Homes

Connected Cities

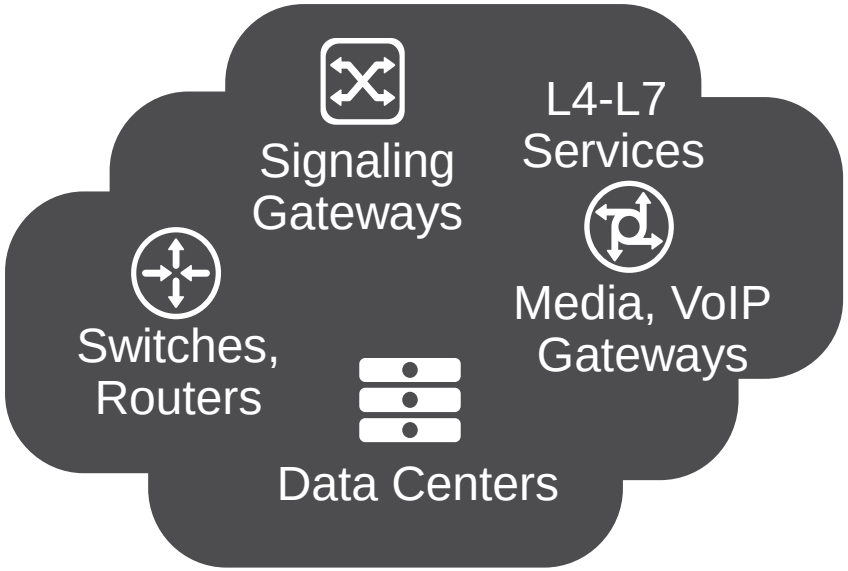
Wearables and Utilities

Surge in SP Network Access

Spikes in Application Usage

Increasing Connection Rates

50B Connected Devices Worldwide by 2020



Service Provider Core Networks

Service Provider Challenges

- Network Signaling Spikes
- Diameter Signaling Storms
- Surge in DNS Queries
- IPv6 Addressing Requirements
- New DDoS Attack Vectors
- DNS Security Vulnerabilities
- Squeeze in Profit Margins
- New Service Delivery Models

Solutions Can Help

IoE Service Chain Solution

Connected Cars

Connected Homes

Connected Cities

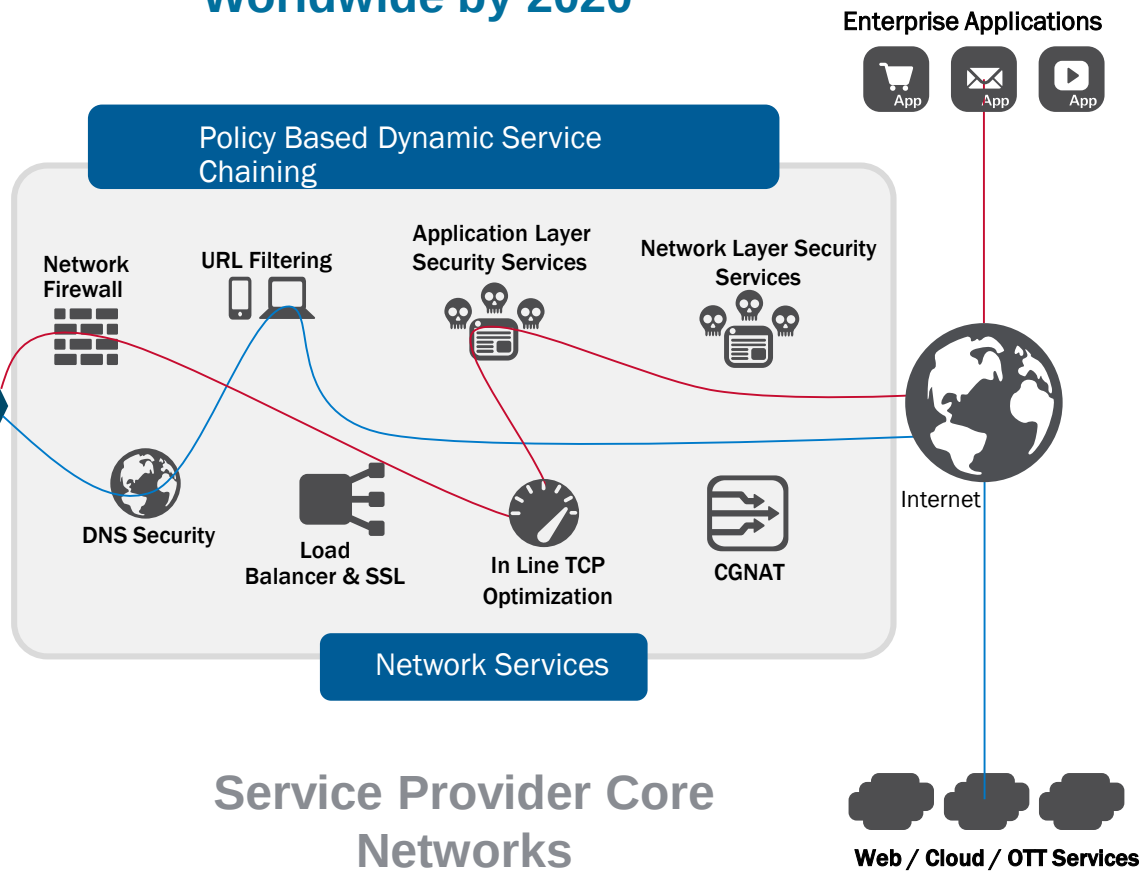
Wearables and Utilities

Surge in SP Network Access

Spikes in Application Usage

Increasing Connection Rates

50B Connected Devices Worldwide by 2020



- Differentiated Service offerings
- Efficient Service Delivery & Improved Network Performance
- Help address security vulnerabilities
- 5G Latency budget conformity
- Bi-directional communication
- Large scale DDoS protection

The Role Of NFV/SDN

KEY: Solution Integration leveraging a strong NFV/SDN Ecosystem


Connected Cars


Connected Homes


Connected Cities


Wearables and Utilities

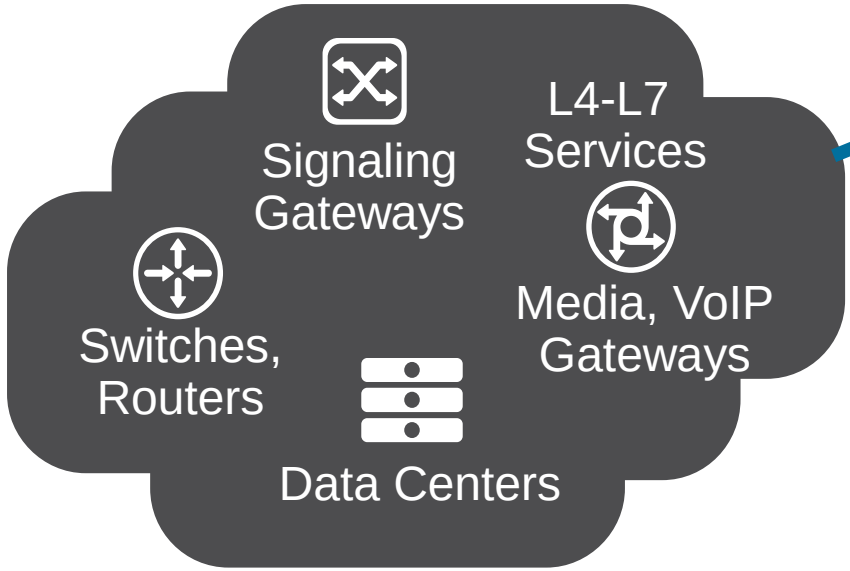
Surge in SP Network Access

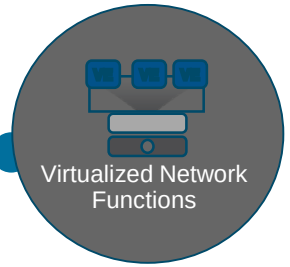
Spikes in Application Usage

Increasing Connection Rates

50B Connected Devices Worldwide by 2020

Effective Network Virtualization is Key





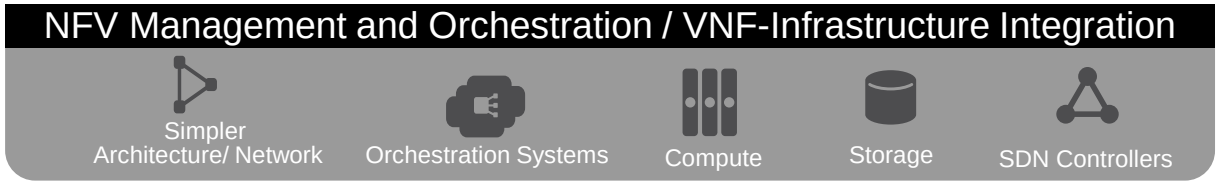
Service Provider Core Networks

- Scalable DNS
- Load Balancing
- Network Firewall

- Application Layer Firewall
- IPv6 Routing
- Carrier Grade NAT

- Diameter Routing
- Protocol Gateway
- Policy Enforcement

- Traffic Classification
- Subscriber Classification
- Application Awareness



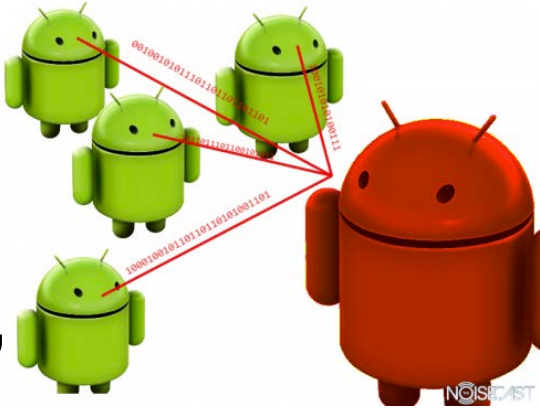
Victim or abuser: The questionable role of IoE devices

The Hidden Threat

Consumer grade IoE devices such as wearables present an attractive target for attackers:

- Massive capacities for bot herding
- Activist bashing of brands
- Military attacks on public infrastructures
- Ransom attacks
- Exploits to compromise control plane (SIP, DNS, etc.) from “inside”

The Unsolved Question



Newly discovered exploits may address thousands, if not hundred of thousand devices.

Higher quality devices may have a higher chance of updates.

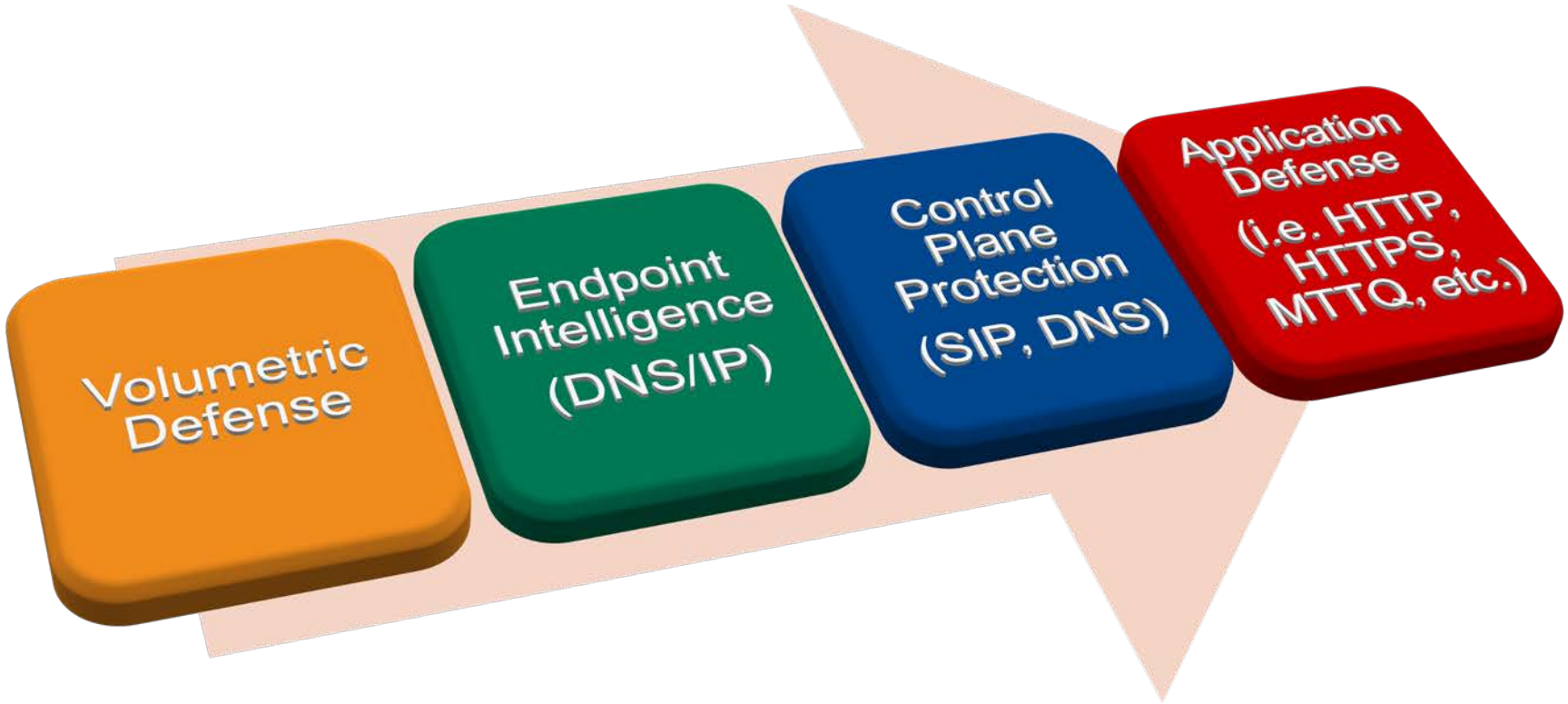
The mass market with embedded, 1€ COG's for networking hardware will never see updates.

Operators have no choice other than implementing defense services to protect their infrastructure not only from attacks from the outside but also from the inside, additionally avoiding devices form a bot net.

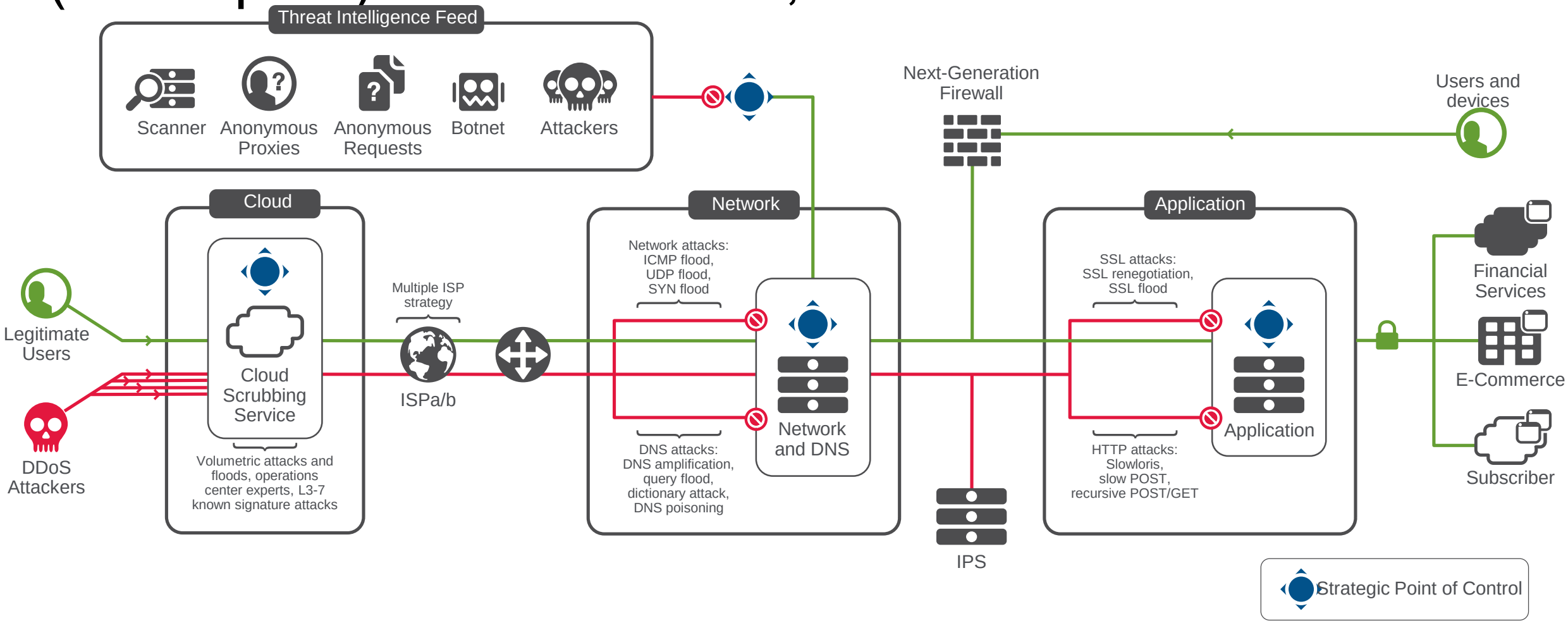
Once a victim of a compromise, the IoE device(s) become offenders.

Once again the perimeter shifts. For operators, DDoS attacks now can originate from both sides of security demarcation line. Nothing is trusted anymore.

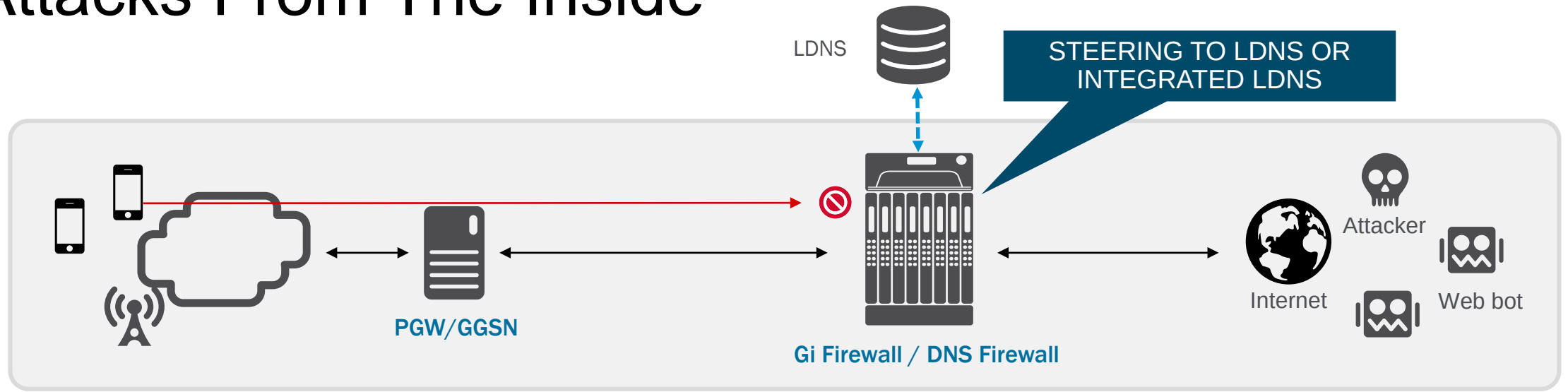
Multi Layered Defense



Use Case: Cloud-based scrubbing with on-premises (on/off path) DDoS defense, firewall and L7 defense

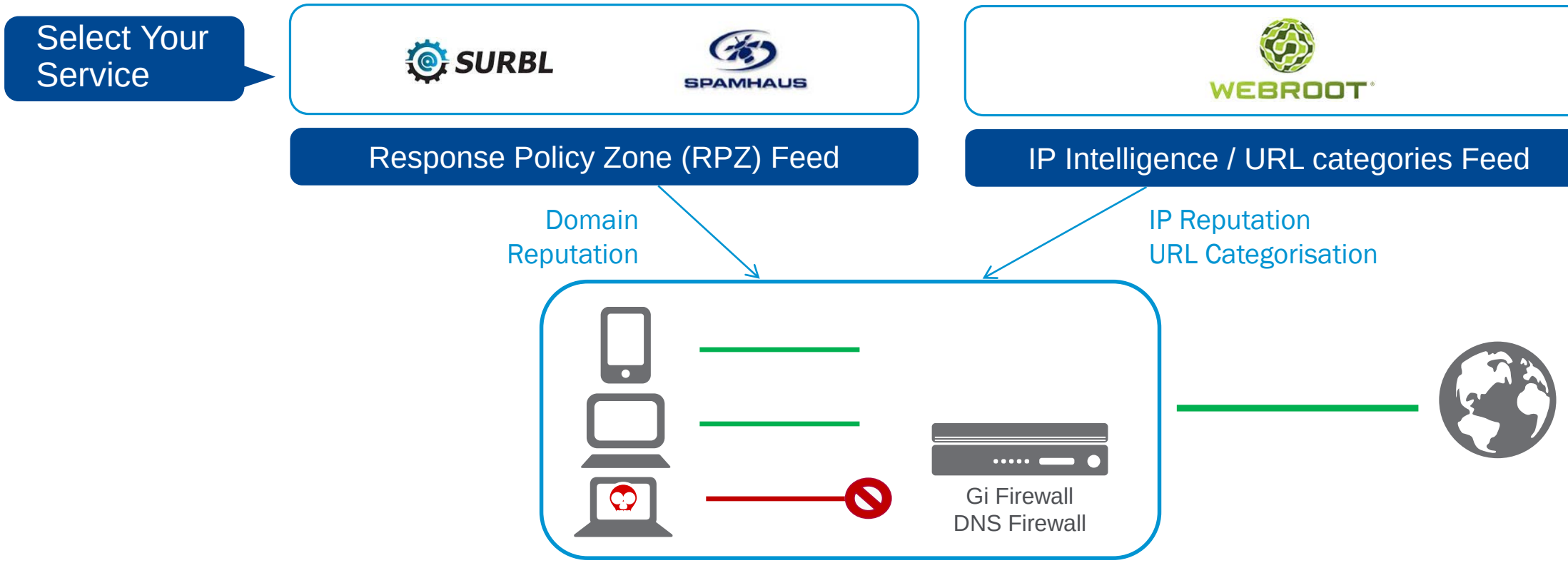


Use Case: Protecting DNS Infrastructure Against Attacks From The Inside



- DNS per-user rate limiting
  - Risk: Malware on mobile
  - Mitigation: Restrict DNS rate of requests per user to "normal" levels
- DNS tunneling
  - Risk: Free-of-charge mobile data and DNS server overload
  - Mitigate: Detect tunneling of HTTP over DNS and block it

DNS Reputational Intelligence

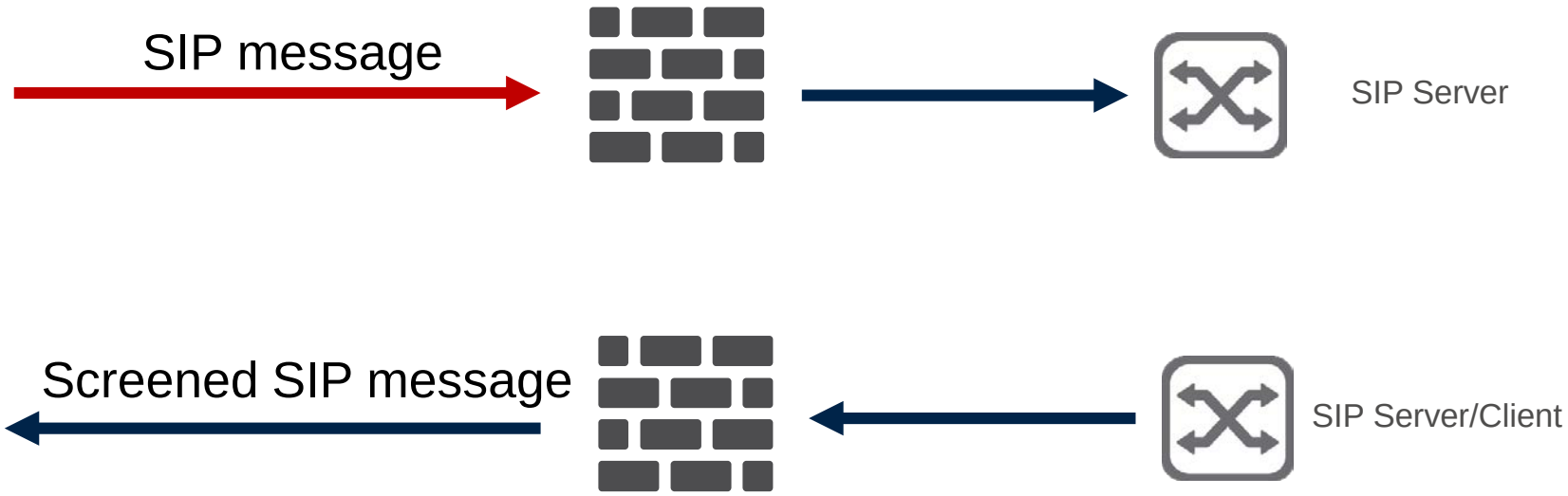


- Mitigate DNS threats by blocking access to malicious IPs
- Reduce malware and virus infections

- Prevent malware and sites hosting malicious content from ever communicating with a client

- Inhibit the threat at the earliest opportunity – Internet activity starts with a DNS request

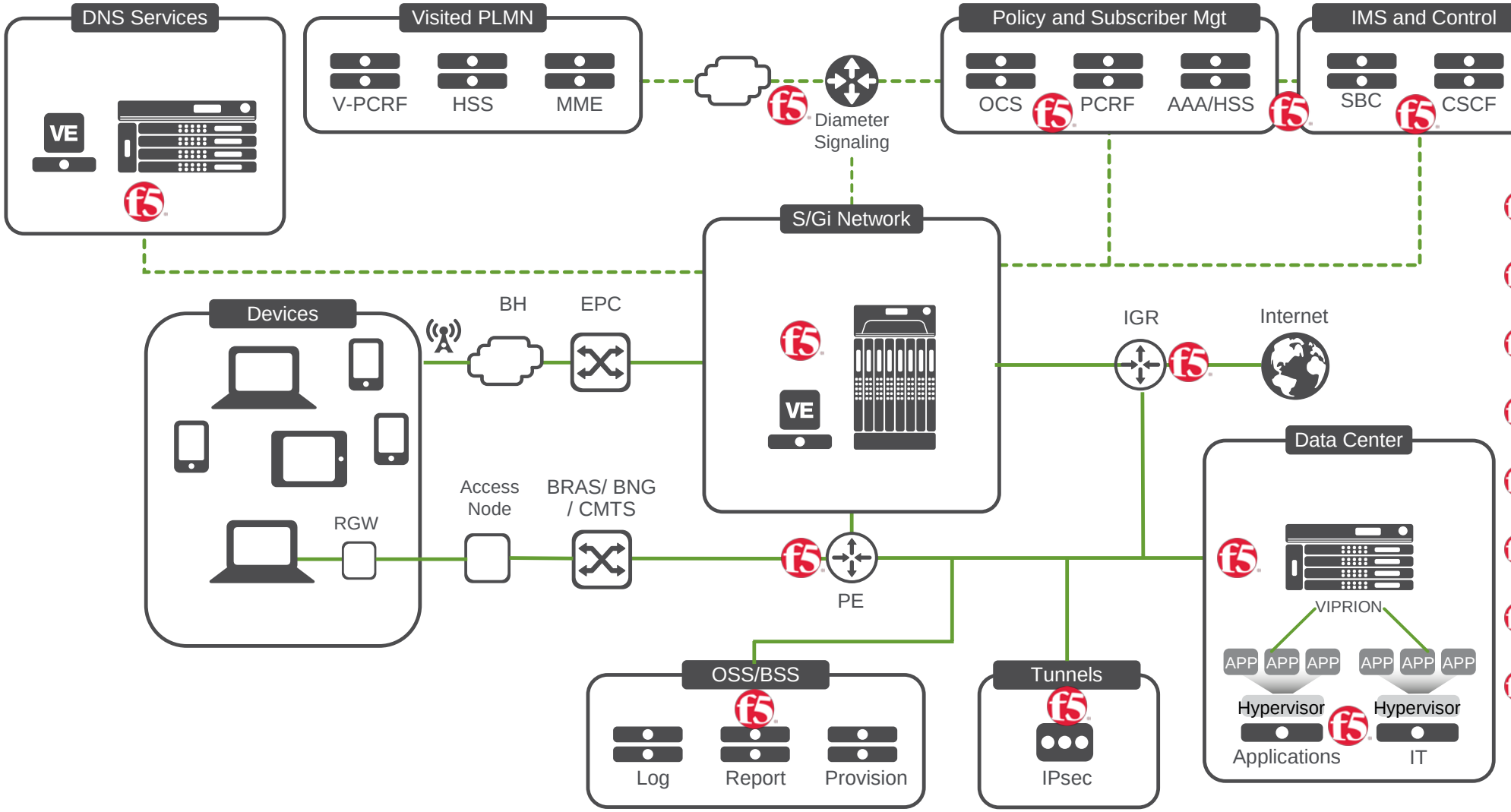
SIP: Security



SIP Security controls:

- Screening, Policing, Protocol Conformance
- Per-Source throttling
- Access Control, White/Black Listing based on any content
- DDoS Prevention
- Topology hiding
- Field manipulation

F5 Deployment Footprints



- Internet Peering
- Internet Data Center
- Subscriber Aggregation
- Signaling Choke Points
- Secure DNS Delivery
- IMS & VoLTE Systems
- Management Systems
- Tunnel Termination

Example Solution: Connected Car

IoE adds new L7 protocols to the TCP/IP stack

WEB

Application : HTTP, DNS

- LB, FW, DOS, APM

Session : SSL/TLS/DTLS

- Encrypt/decrypt/intercept

Transport :TCP/UDP

- LB,FW, Optimization

Network : IPv4, IPv6

- DPI

F5 core: L4-L7

Data Plane

Control Plane

Management Plane

Programmability

Analytics

IOT

Application : MQTT, CoAP

- APM, LB, FW, DOS, PUB/SUB

Session : SSL/TLS/DTLS

- Encrypt/decrypt/intercept

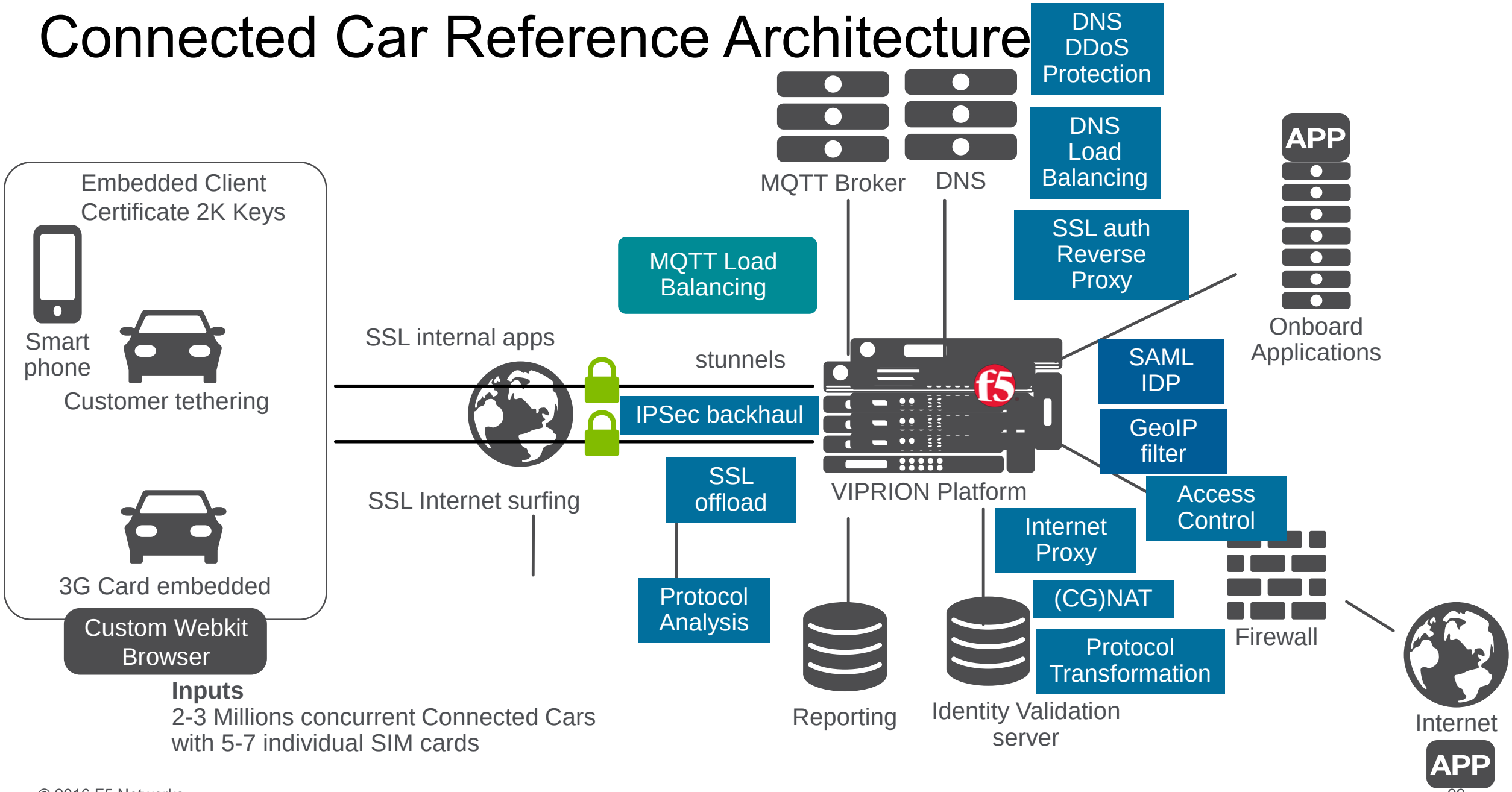
Transport :TCP/UDP

- LB,FW, Optimization

Network : IPv4, IPv6

- DPI

Connected Car Reference Architecture



Inputs
2-3 Millions concurrent Connected Cars
with 5-7 individual SIM cards

Managing IoE Security At Scale

Addressing The Most Pressing Security Needs

Functionality	Usage
IP Intelligence	Prevents access from endpoints with known bad reputation
IP Geo-location	Prevent prohibited usage Supports geographically limited services
High Density Session Scale	Preserve state for long lived, high capacity, low data volume sessions
High Speed, Full Proxy Architecture	Latency reduction Service chaining Protocol translations (CG)NAT Protocol optimizations Crypto Offload Content filtering
DDoS Detection and mitigation	L3/4 volumetric attack defense (IPv4/IPv6) L4-7 defense for SIP, HTTP, DNS
Device Service Clustering	Scale beyond traditional 2 node cluster solutions (up to 32 devices) Stateful, sub second failover support

Closing Thoughts and Q&A

Not That I Want To Speak About Products, but...

Highest performance

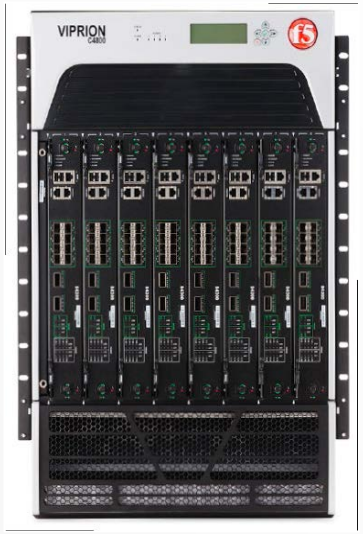
Scale Up On Demand

Lower Operating Costs

VIPRION B4450 Blade

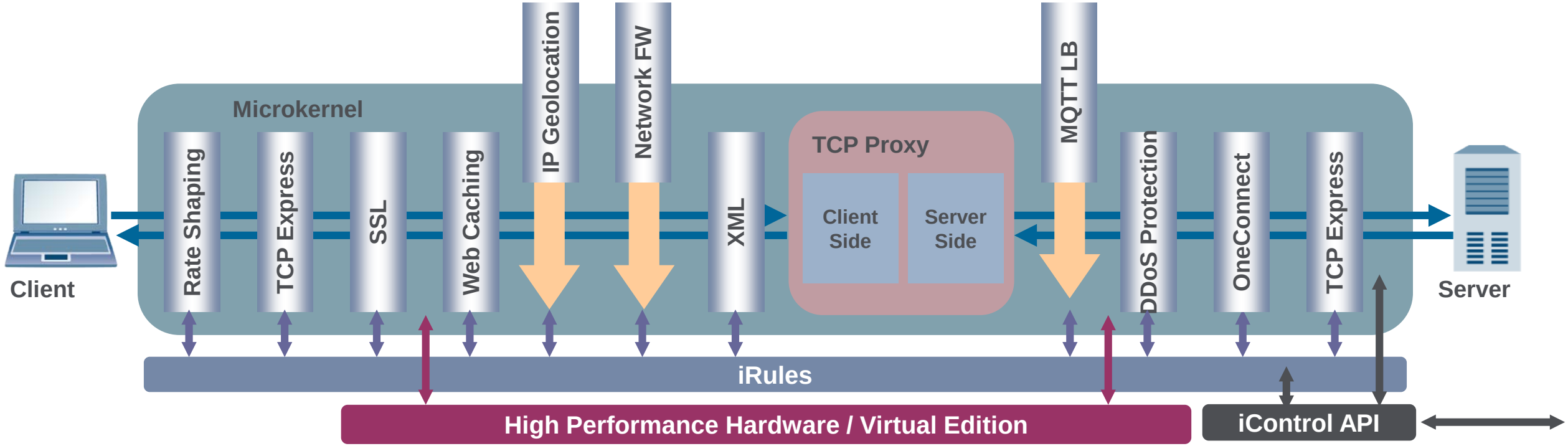
- 24 CPU Cores (Dual 12 Core)
- 256GB Memory
- 2x 100GBASE-SR4 - QSFP28 Ports
- 6x 40GBASE-SR4 QSFP+ Ports
- 160G L4/L7
- 6M L7 RPS
- 2.5M L4 CPS
- 190M Concurrent Connections
- 150K SSL TPS (2K)
- 80G H/W Compression
- 1.6TB SSD
- 48 vCMP Instances
- NEBS

VIPRION C4800



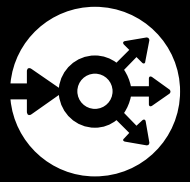
- 1.2 TB Throughput
- 20M L4 CPS
- 1.5B Concurrent Connections
- 1.2M SSL TPS
- 48x 40G Ports
- 16x 100G Ports
- 384 Virtual Instances

Functional Representation Of IoE in TMOS



- Traffic Management Microkernel (TMM)
- End-to-end TCP optimization (IPv4 and IPv6)
- Migration offload IPv4 to IPv6
- Pluggable software modules (SSL, caching, compression, WAF, etc.)
- Extendable functionality (iRules, iControl API)

F5 Service Provider Solution Portfolio



Data Traffic Management

- Gi Network Simplification
- Intelligent Traffic Mgmt
- Dynamic Service Chaining
- Policy Enforcement
- TCP Optimization
- Content Filtering
- CG-NAT/DS-Lite

Signaling Traffic Management

- Domain Name System (DNS)
- SIP signaling
- Diameter Solutions
  - DRA
  - DEA
  - LB
  - SLF
  - LTE Roaming
  - 3G/4G IWF

Security

End-2-End Multi-Layered Dynamic Security

- Device Security
- Network & Infrastructure Security
- Application Security
- L4-L7 DDoS Protection
- Control plan security: DNS, Diameter, SIP

Virtualization / NFV

- Virtual Editions
- Management and Orchestration of NFV Services

Solutions for an application world.