NETWORK SECURITY FOR DISTRIBUTED NETWORKS

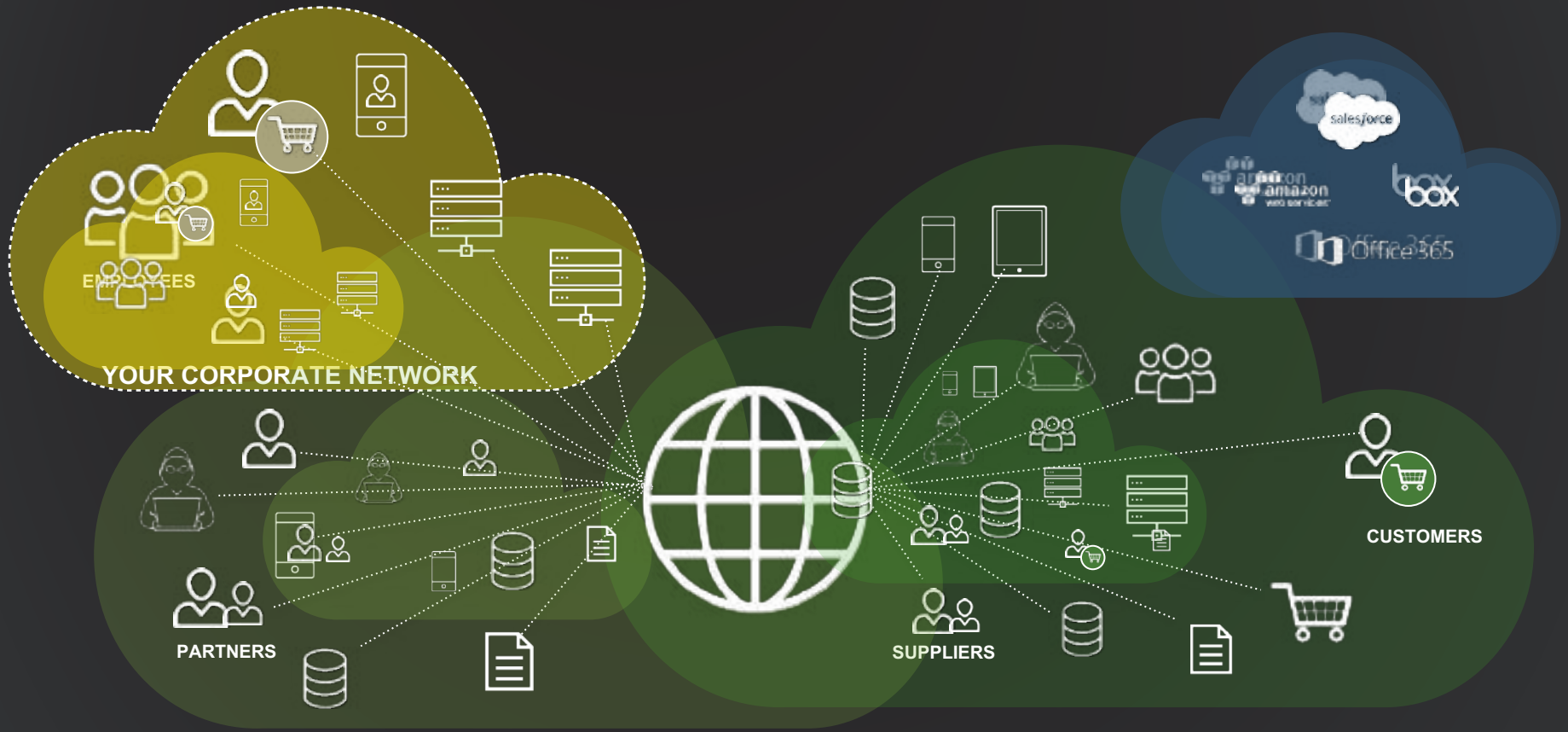
Somruetai Khreuasuk
Network Engineer

FORCEPOINT

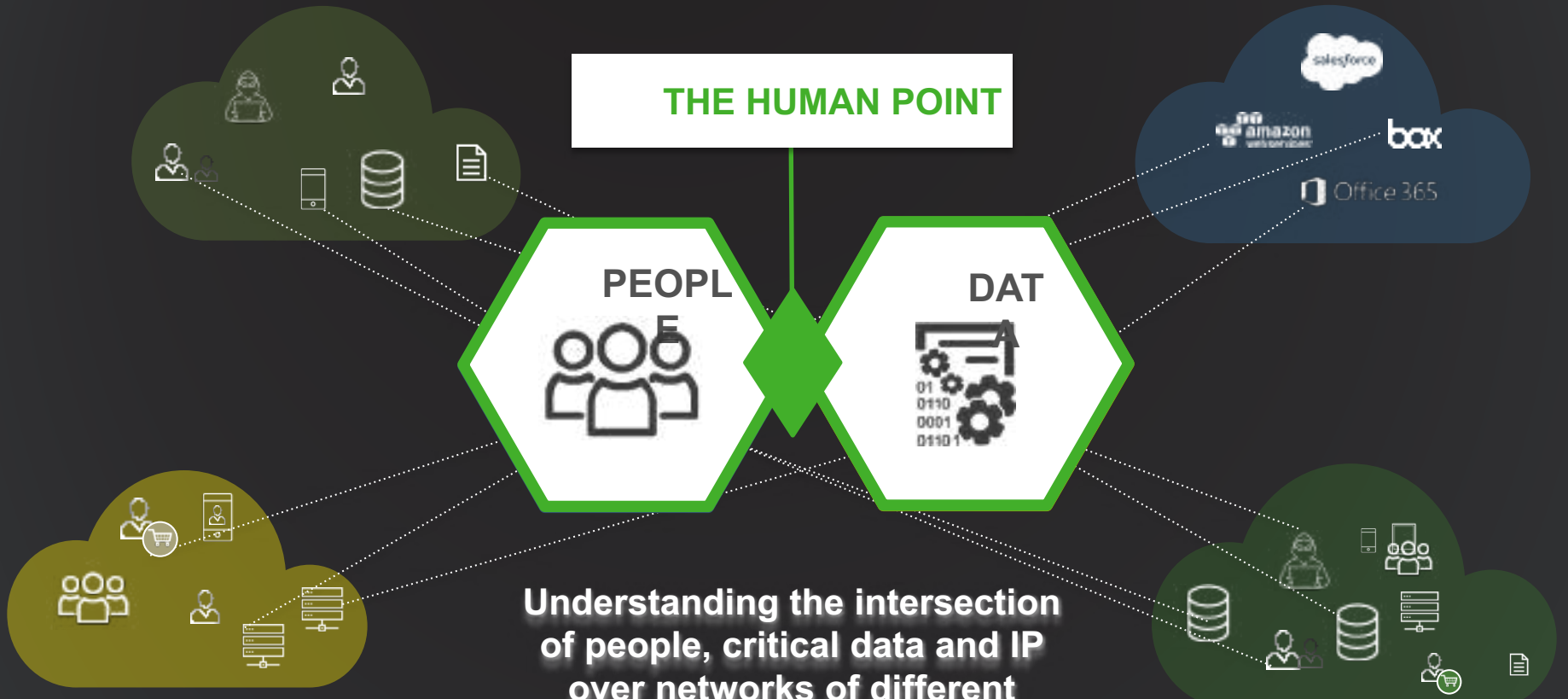
PURPOSE-BUILT TO PROVIDE A NEXT GENERATION CYBERSECURITY SOLUTION

- One of the largest private cybersecurity companies in the world, with thousands of enterprise and government customers in more than 150 countries.
- Created by Raytheon in 2016 to commercialize defense-grade technologies for the enterprise security market.
- Leading supplier to global Intelligence community and high assurance cyber missions.
- One of the most comprehensive security product portfolios in the industry.

FOCUS ON THE TRUE CONSTANTS



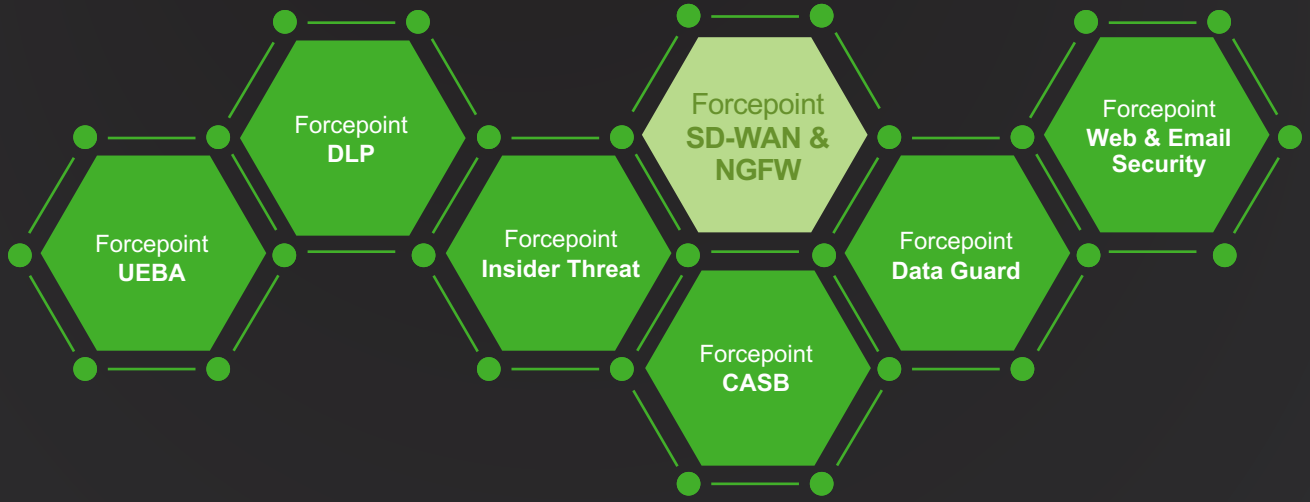
FOCUS ON THE TRUE CONSTANTS



Understanding the intersection of people, critical data and IP over networks of different trust levels.

THE HUMAN POINT SYSTEM

THE RHYTHM OF PEOPLE



THE FLOW OF DATA

360° VISIBILITY

UNIFIED POLICY

RAPID ENFORCEMENT

EFFICIENT COMPLIANCE

TOP VISIONARY IN 2018 GARTNER MAGIC QUADRANT

Source: Gartner (October 2018)

Gartner

*"Forcepoint has demonstrated **consistently good feature quality** and an **expanded capacity** to execute on its roadmap. The vendor is a **valid shortlist candidate** on enterprise firewall shortlists for **distributed organizations**."*

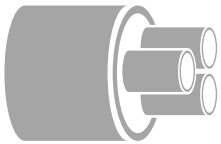
Strengths

- Product Vision
- Customer Experience
- Capabilities
- Ease of Use

WHY ORGANIZATIONS SHORTLIST FORCEPOINT

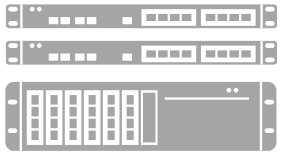
#1 NGFW & IPS SECURITY

Top-ranked security on NSS Labs' NGFW and NGIPS tests



SD-WAN MULTI-LINK™ OPTIMIZATION

Unique and praised by end users VPN Mesh technology

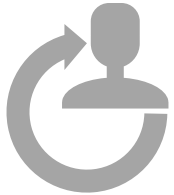


CLUSTERING & HIGH AVAILABILITY

The best clustering capabilities available on the market place

SINGLE-PANE MANAGEMENT

Simply the smartest management system in the industry



OPERATIONAL EFFICIENCY

Zero-touch deployments and one-click updates/upgrades

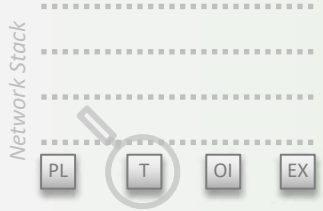
TRUE ENTERPRISE SOLUTION

Greater Agility with Lower TCO

The Forcepoint Difference: Innovation + Integration

SECURITY

Other Vendors

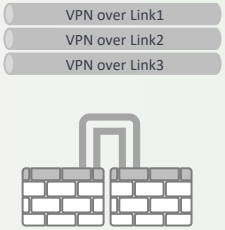


Packet Inspection

vs.

AVAILABILITY

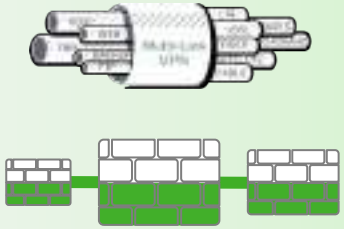
Other Vendors



Basic Redundancy Bolted-on

vs.

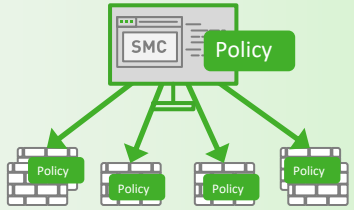
Forcepoint



Mixed Clustering Built-in

vs.

Forcepoint



Centralized Policy Management

Security

- #1 in NSS Labs Security Tests
- Pioneer in anti-evasion IPS
- High-speed SSL inspection
- Endpoint context-aware
- Pioneer in application proxying
- Service chaining SWG & CASB

Connectivity

- Direct-to-cloud SD-WAN
- Site-to-site Multi-Link™ VPN
- Multi-ISP transport independence
- Pioneer in firewall clustering

Manageability

- Global scalability
- Low-touch deployment
- Policy-based automation
- Updates without downtime
- Interactive visualization, including 3rd party devices

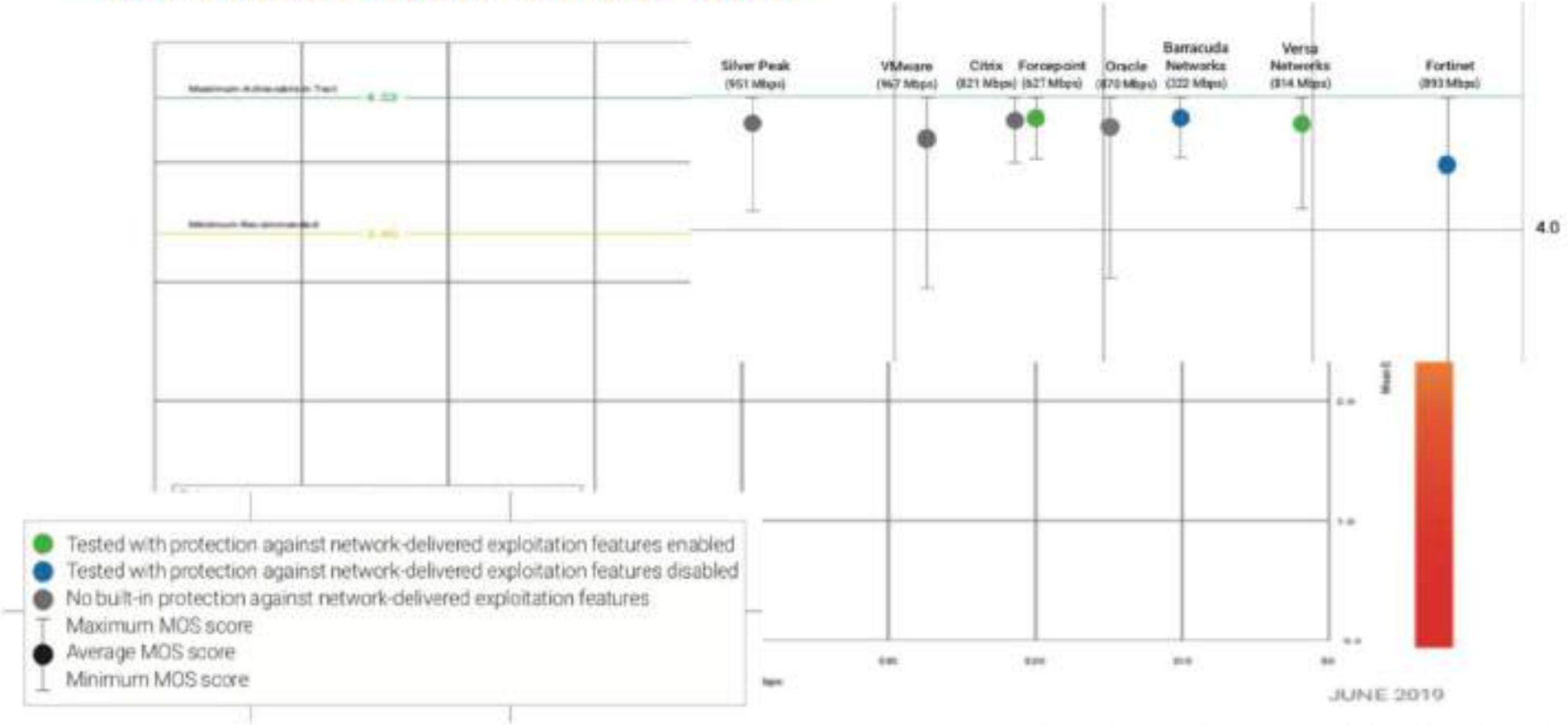
#1 Network Security

86%
Fewer Cyberattacks

69%
Fewer Breaches

Source: IDC Research

NSS LAB SD-WAN VALUE MAP



ENTERPRISE **SECURITY** AND **TCO**

NGFW
5th Consecutive Time

NGIPS
2nd Consecutive Time

"The security effectiveness of the Forcepoint NGFW 3301 was unsurpassed in the NSS Labs 2017 NGFW test. ***The Forcepoint NGFW should be on every company's short list.***"

Thomas Skybakmoen,
Distinguished Research Director
NSS Labs

NSS Labs 2017 NGFW Test

Forcepoint NGFW Certifications & Gartner

Gartner

Sole Visionary 2018, Enterprise Firewall

Recommended for Short Lists

NSS LABS

#1 in Security

Highest Security Effectiveness

Top NGFW
2018, 2017

Top NGIPS
2018, 2017

NETWORK SECURITY MUST DEFEND AGAINST **LAYERS WITHIN LAYERS**

Evasions

"camouflage"

App
(HTTP, SQL, etc.)

TCP
(Overlapping, Extra)

IP
(Fragments, Ordering)

Exploits

"delivery vehicles"

Unpatched Vulnerabilities
(SMB, Web, DB, etc.)

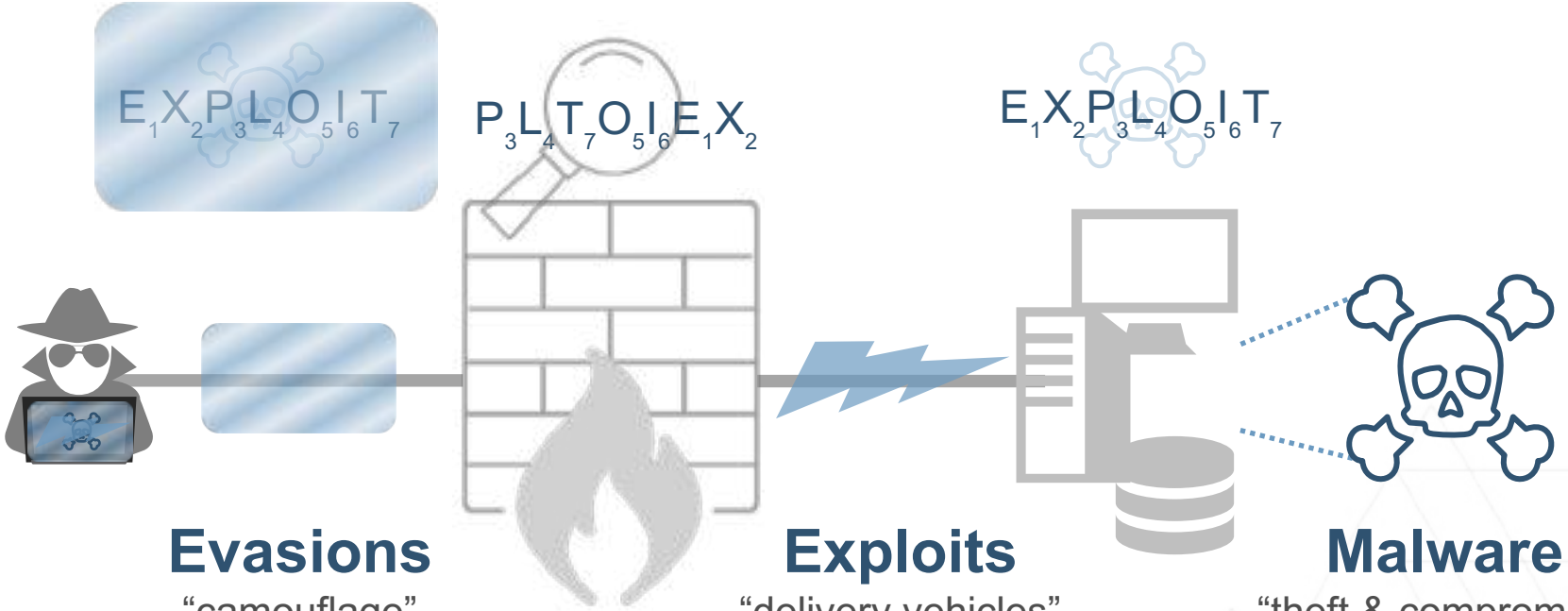
Zero-Days

Malware

"theft & compromise"

Ransomware
Data Theft
User Compromise
System Corruption

WHY TAKING **A NEW APPROACH** TO SECURITY IS SO IMPORTANT



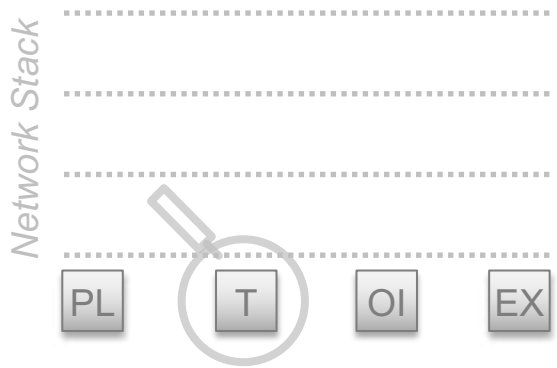
Evasions
"camouflage"

Exploits
"delivery vehicles"

Malware
"theft & compromise"

FORCEPOINT DIFFERENCE: STRONGEST INTRUSION PREVENTION

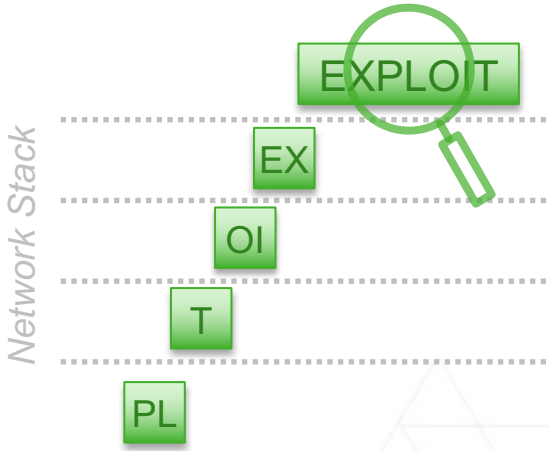
Packet Inspection



Misses protocol/encoding evasions

Pattern-matching misses new variants

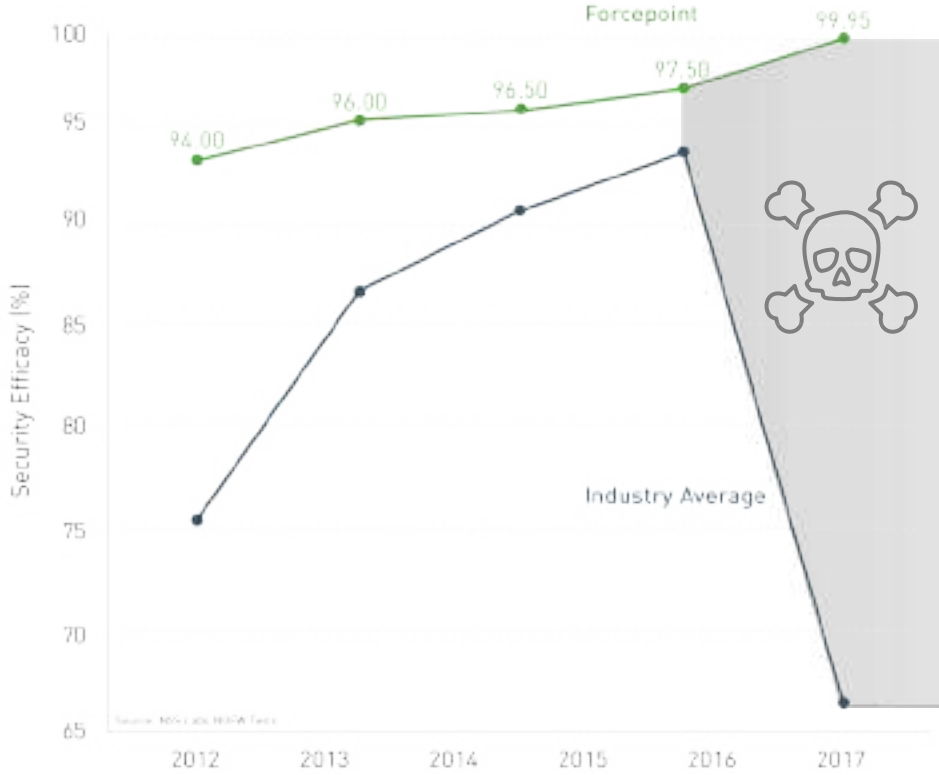
Forcepoint STREAM Inspection



Sees actual payloads – immune to packet evasions

Vulnerability-centric scanning
for preemptive protection

THE **EVASION GAP** – MOST VENDORS LEAVE NETWORKS EXPOSED



Many NGFW & IPS fail to stop evasions

Exploit Kits now make evasions easy

- Metasploit
- Shadow Brokers leaked toolkit

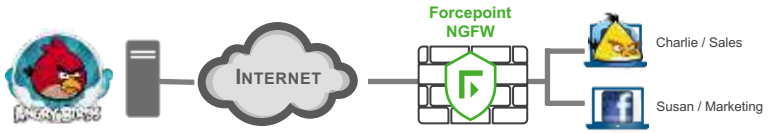
Attacks combining techniques to spread

- Learning from WannaCry → Petya

USAGE CONTROLS

Next generation way to define policies

- User
  - Agent-based user control
- Application
  - Over 7,400+ application fingerprints
- URL Categorization
  - More than 120 security and filtering categories



Source	Destination	Service	Action
Sales	Internet	Skype	✓
Marketing	Internet	Facebook Chat	⛔
Charlie	Internet	Facebook Chat	✓
Susan	Internet	Angry Birds	⛔

Forcepoint NGFW provides control of over **7,400+ apps**

FORCEPOINT NGFW – NGFW VS SSM PROXY

Example: How NGFW vs SSM Proxy handles SSH (SFTP) differently

"Is this really SSH (SFTP) traffic passing through port 22?"

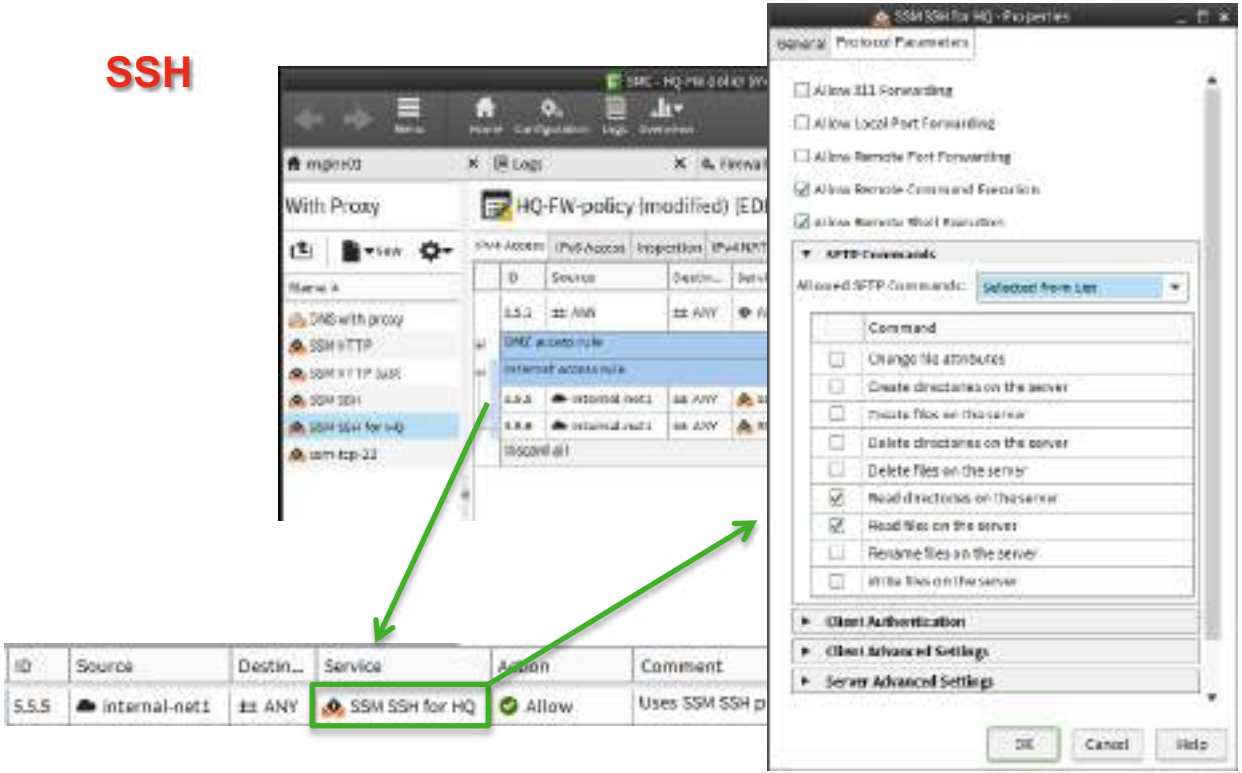
Yes: ALLOW **No: DENY**

No further control possible without breaking connection

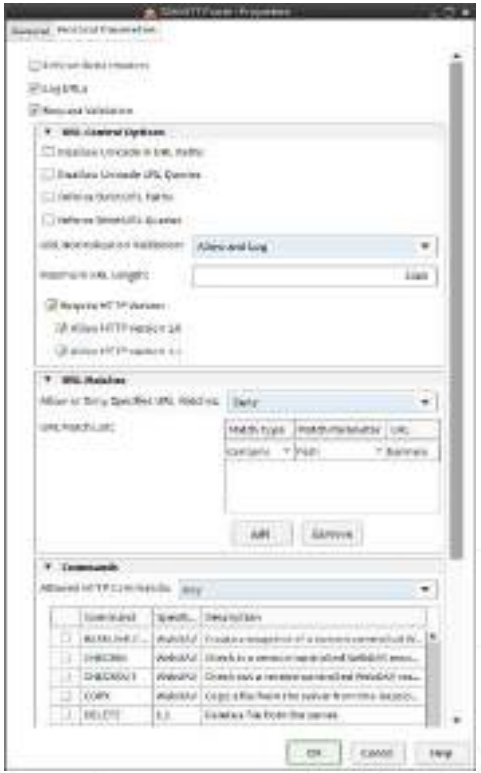
The session is not broken after upload is DENY

SSH & HTTP PROXY CONTROLS

SSH

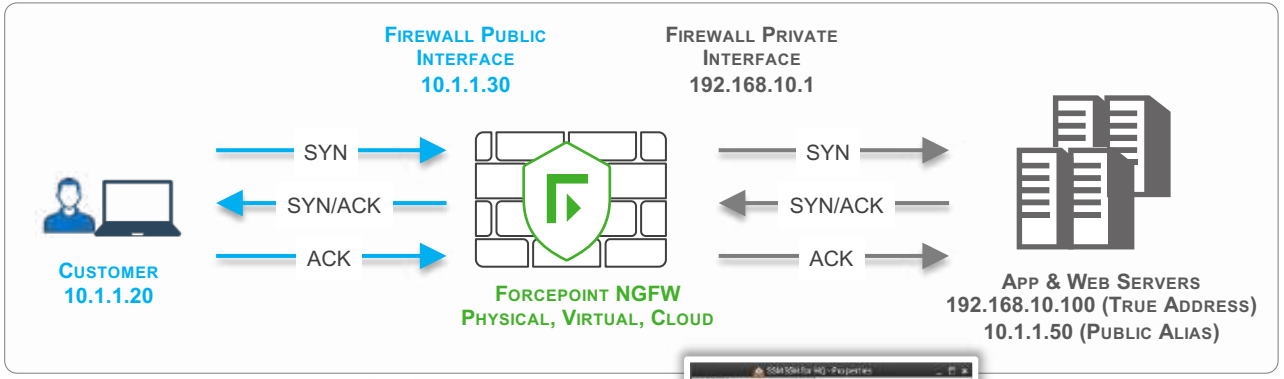


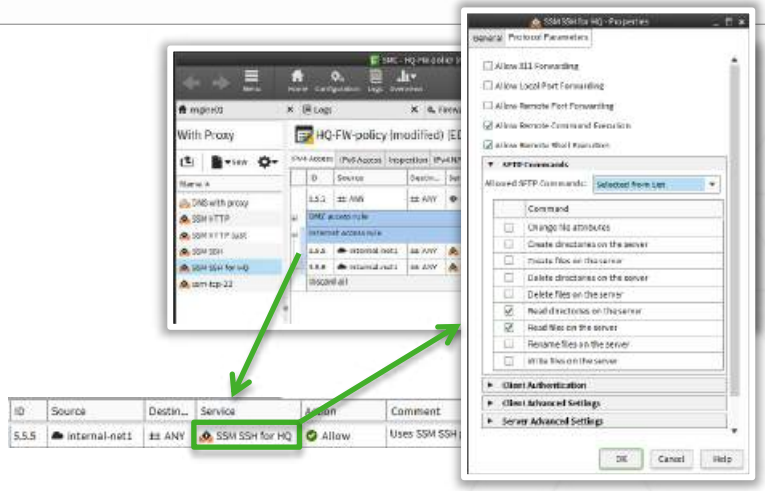
HTTP



COMMAND CONTROLS (PROXY FIREWAL)

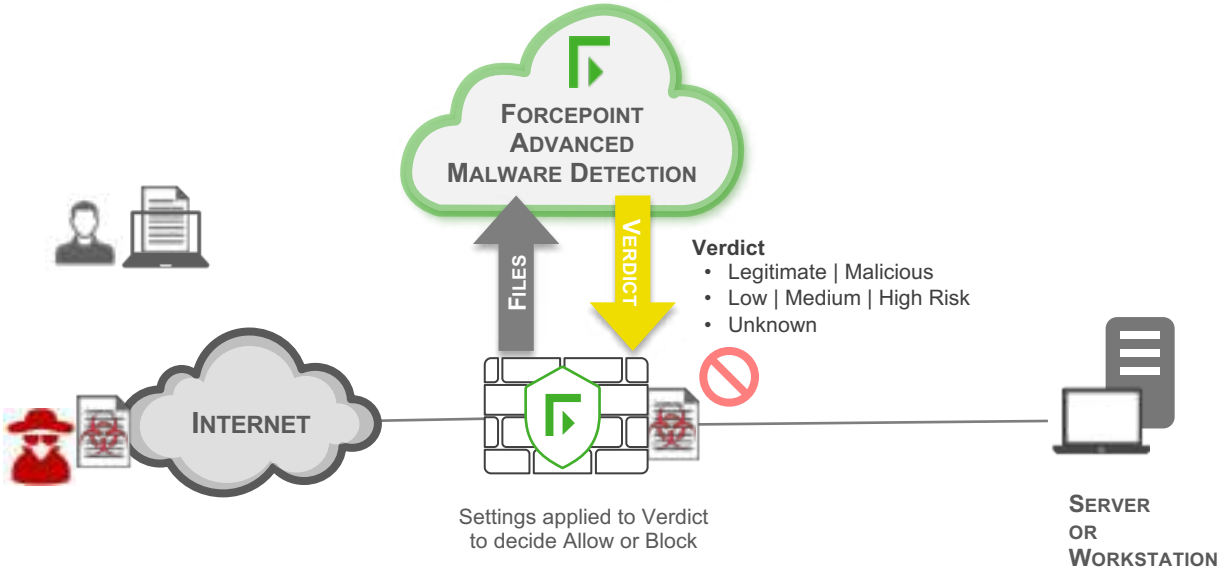
- Specific proxies for
  - UDP
  - TCP
  - HTTP
  - SSH / SFTP
  - HTTPS
  - FTP
  - TFTP
  - DNS
- Rewrites protocol headers
  - Masks identity of origin
  - Prevents data exfiltration
- Allows very fine grained control E.g.
  - Protocol version
  - Authentication method
  - Allowed commands



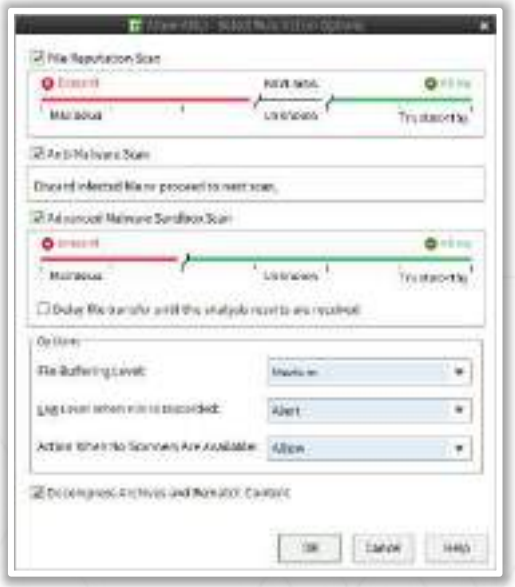


FORCEPOINT NGFW ADVANCED MALWARE DETECTION

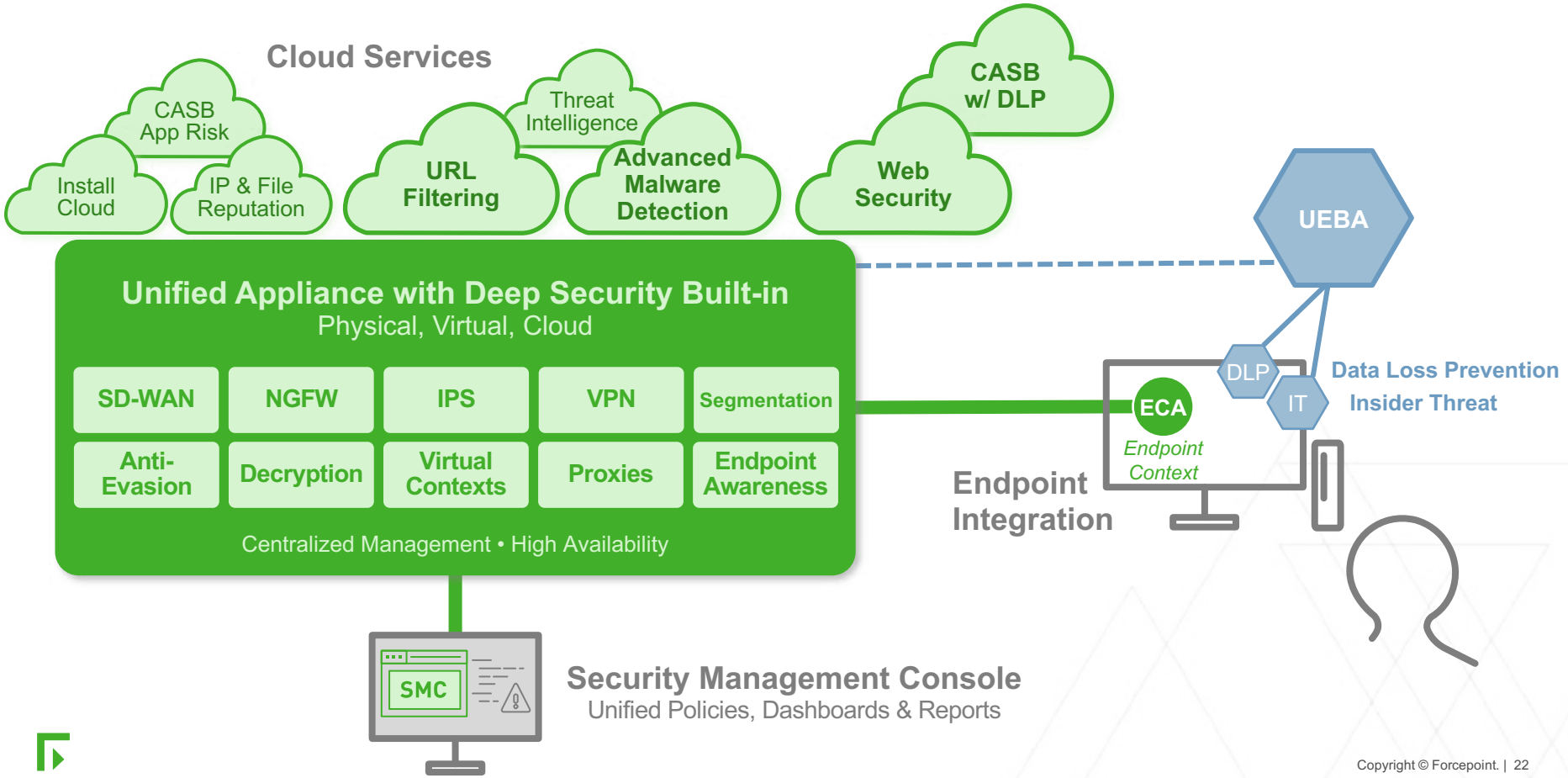
- Advanced Persistent Threats, Zero-Day Threats, and Advanced Malware
- Provide deep content inspection analyzes for unknown objects
- Available in Cloud and On-Premise



100% Effective
No False Positives
2016 NSS BDS



NETWORK SECURITY POWERED BY THE HUMAN POINT SYSTEM



FORCEPOINT LINES OF NGFW & IPS **UNIFIED APPLIANCES**

6200 Series
Max 66 interfaces
FW 240 Gbps, IPS & NGFW 22 Gbps

Data Center

3300 Series
Max 35 interfaces
FW 80-160 Gbps, IPS & NGFW 9-15 Gbps

Campus

2100 Series
Max 28 interfaces
FW 60-80 Gbps, IPS & NGFW 5-7.5 Gbps

Edge

1100 Series
12 interfaces + opt. 2 modules
FW 50-60 Gbps, IPS & NGFW 1.5-3 Gbps

Office

300 Series (desktop)
5 interfaces + opt. 2 modules and WLAN on 325
FW 4 Gbps, IPS & NGFW 200 Mbps

320X (ruggedized)
4 interfaces + WLAN
FW 2 Gbps, IPS & NGFW 200 Mbps

Branch

100 Series (desktop)
10 interfaces (8 switch ports) + WLAN on 325
FW 1.5 Gbps, IPS & NGFW 150 Mbps

SOHO

CLOUD
AWS
Azure

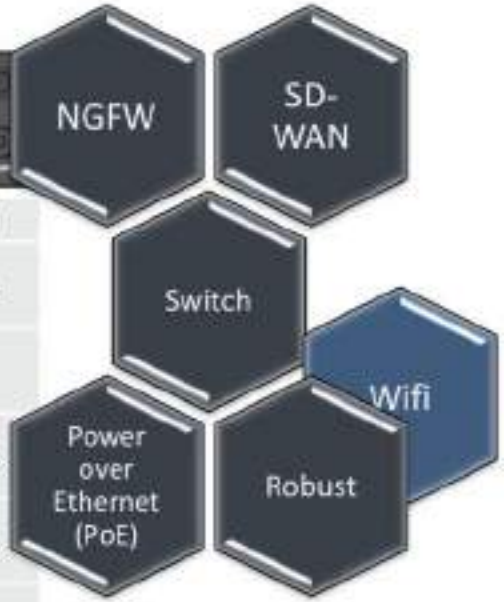
VIRTUAL
Hyper-V,
KVM
VMware
ESXi & ESX

Forcepoint 120W Wireless appliance

Design	Desktop, fanless robust solution
Fixed Interfaces	8 x GE RJ45 2 ports support POE (Switch support at engine 6.8)
Other fixed interfaces	2 x USB, 1 x serial,
Wireless	IEEE 802.11 ac/a/b/g/n
Powering	AC wall socket 12VDC / 2A AC wall socket 54VDC/ 1.3A
Redundancy	Clustering, Multi-Link
Reliability (MTBF)	100 000+ hours
Operating temperature	5–+40°C (+41+104°F)
Dimensions (W x H x D)	225 x 150 x 44 mm

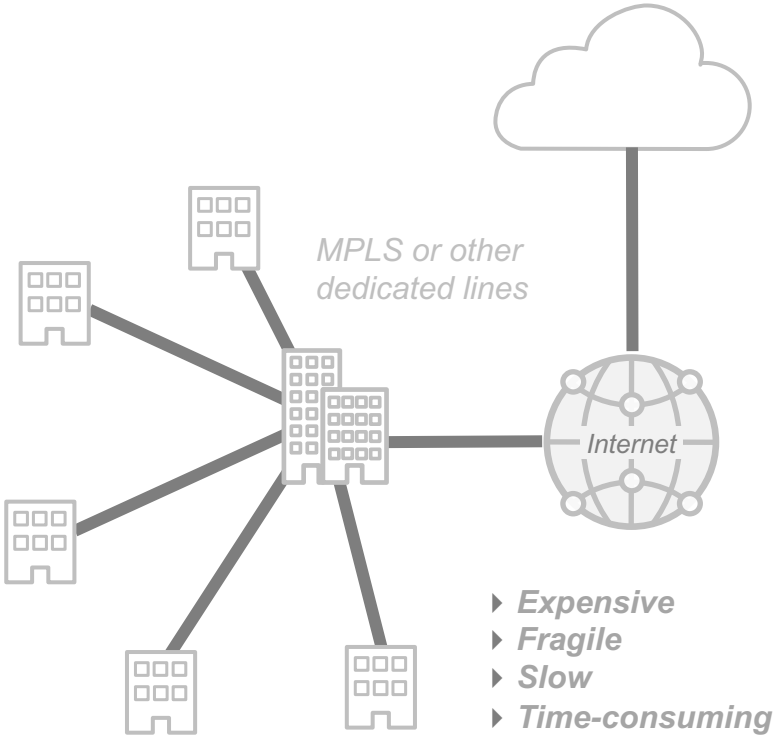
PERFORMANCE[1]	FP 120W
NGFW/NGIPS throughput [HTTP 21kB payload]	300 Mbps
Max firewall throughput [UDP 1518 byte]	4 Gbps
Max inspection throughput [UDP 1518 byte]	900 Mbps
TLS 1.2 inspection throughput [HTTP 44kB payload]	180 Mbps
IPsec VPN throughput AES-GCM-256	1.2 Gbps
Concurrent IPsec VPN tunnels	10 000
Concurrent inspected TCP connections	100 000
Max concurrent inspected HTTP connections	50 000
VLAN tagging	unlimited

1) Performance numbers may change for final product.



SD-WAN OFFERS A BETTER WAY TO CONNECT SITES TO THE INTERNET

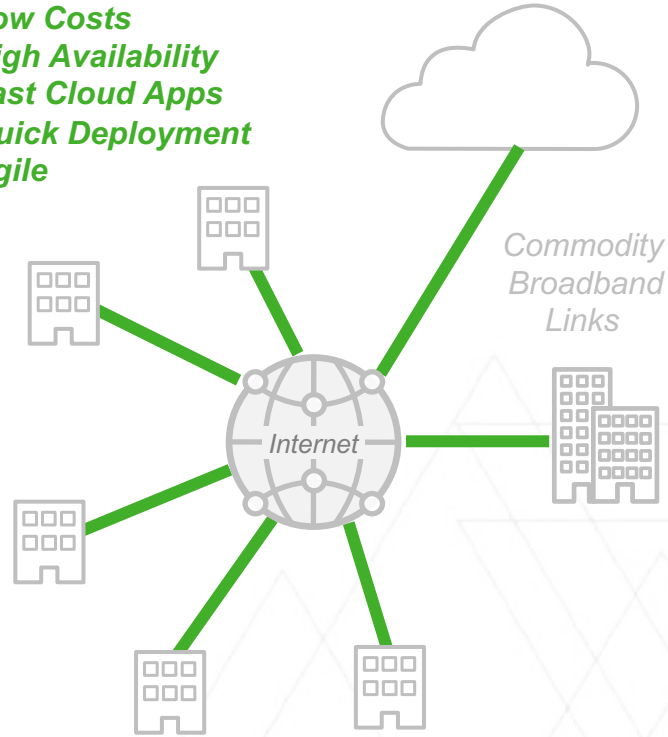
Traditional "Hub-and-Spoke"



- *Expensive*
- *Fragile*
- *Slow*
- *Time-consuming*
- *Inflexible*

SD-WAN Direct-to-Cloud

- *Low Costs*
- *High Availability*
- *Fast Cloud Apps*
- *Quick Deployment*
- *Agile*



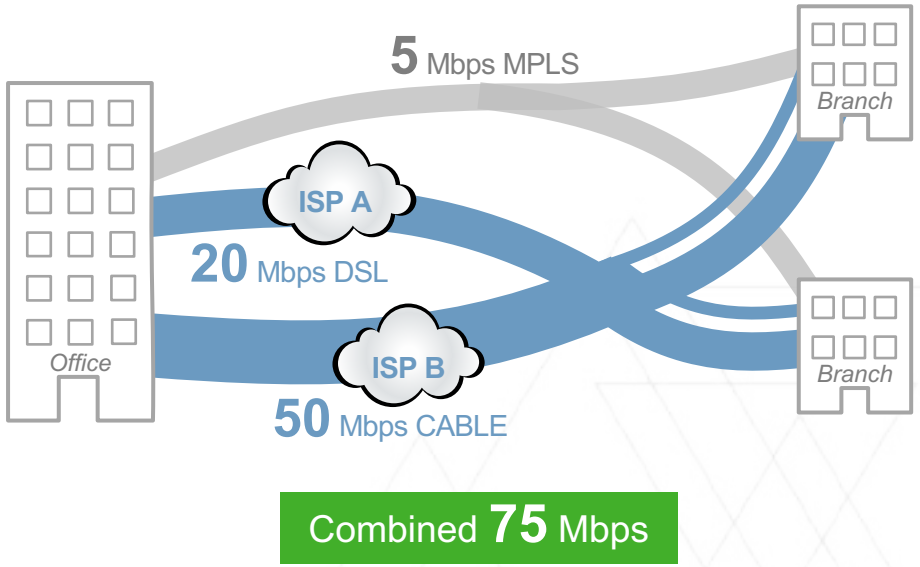
SECURE ENTERPRISE SD-WAN

SD-WAN with multiple, disparate links per location

- Load balancing
- Application bandwidth and Quality of Service (QoS)
- Site-to-site VPNs

Enterprise scale and manageability

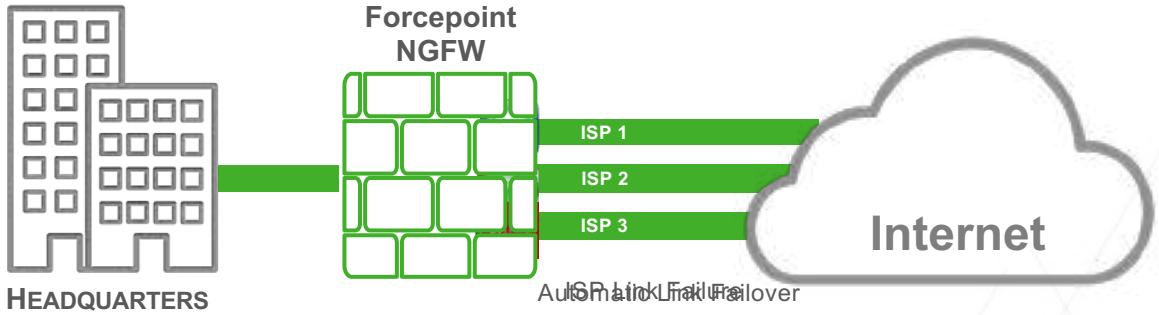
- Networking & security together
- Centralized – not remote – admin



MULTI-ISP WAN CLUSTERING

Ability to cluster different network ISP links together and dynamically balance connections between ISPs, transparently transferring connections from one ISP to another in case of a failure

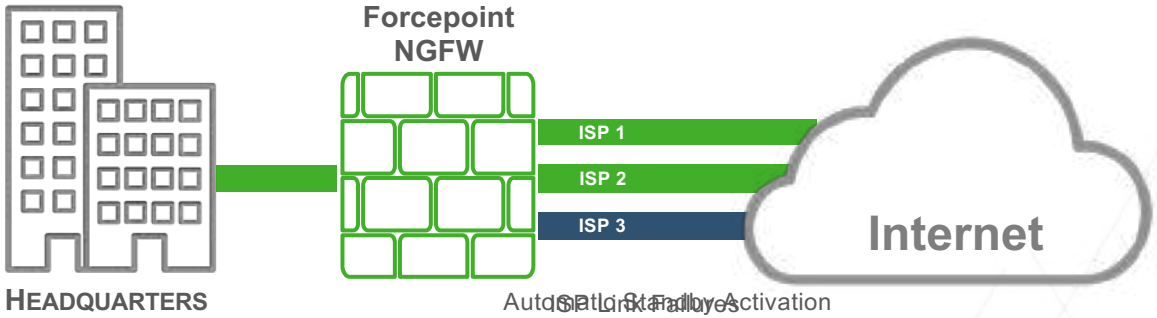
- Easy and simple ISP multi-homing
- Better service for users by selecting always the fastest link
- Business Continuity
- For inbound, outbound and VPN traffic



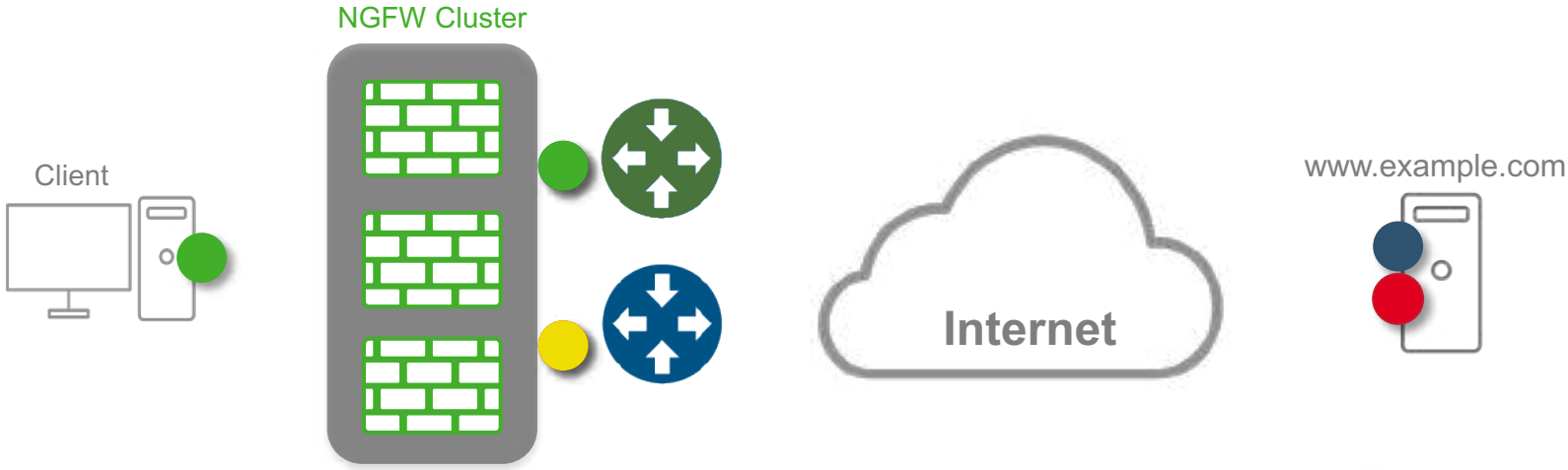
STANDBY LINKS FOR HIGH AVAILABILITY

Standby links allow the definition of a link as a backup that is only activated when all primary links are unavailable.

- Minimize the use of more expensive links
- Multiple standby links possible
- Automatic activation and de-activation

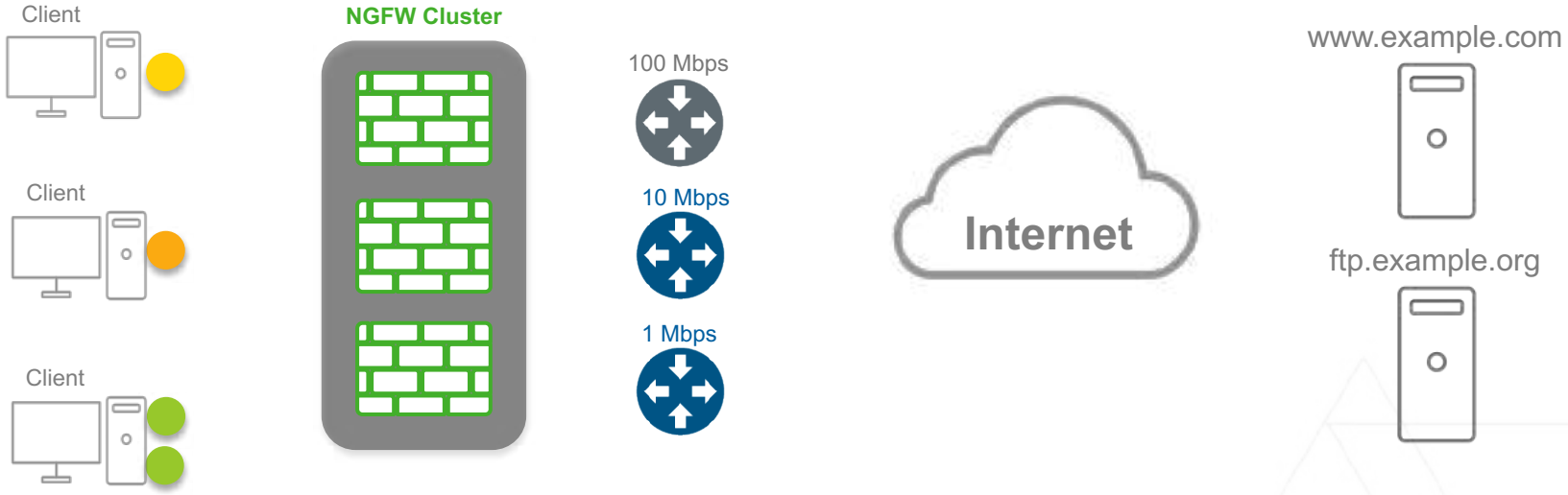


LOAD BALANCING RTT METHOD



- Client sends SYN packet to destination
- Firewall duplicates the SYN with different source IP address, one for each provider address space
- Fastest SYN-ACK in response is selected
- TCP RST sent for remaining links to close gracefully

LOAD BALANCING RATIO METHOD

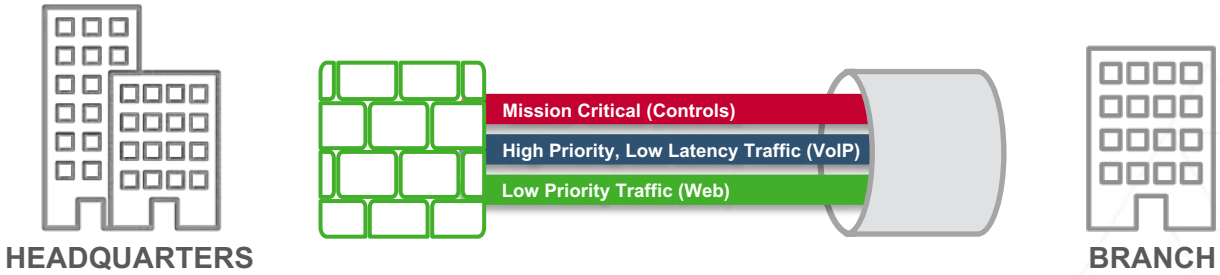


Example: Connections are distributed approximately at 100:10:1 ratio.

QOS AND TRAFFIC PRIORITIZATION

Provide better service to certain traffic by managing existing bandwidth more efficiently

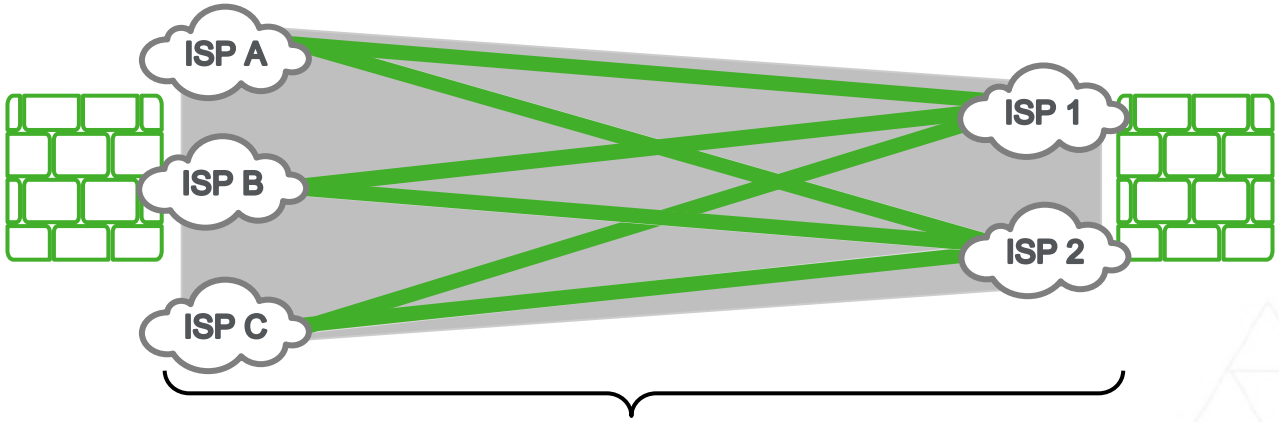
- Prioritize network communication in QoS policy per (VLAN) interface
- Manage existing bandwidth more efficiently instead of buying additional bandwidth
- Traffic classification can be used to select preferred tunnels in Multi-Link VPN



VPN **HIGH AVAILABILITY**

VPN Gateway
3 End-Points

VPN Gateway
2 End-Points



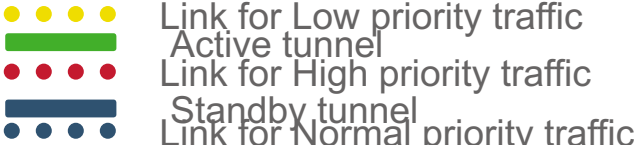
6 End-Point to End-Point (Multi-link) Tunnels

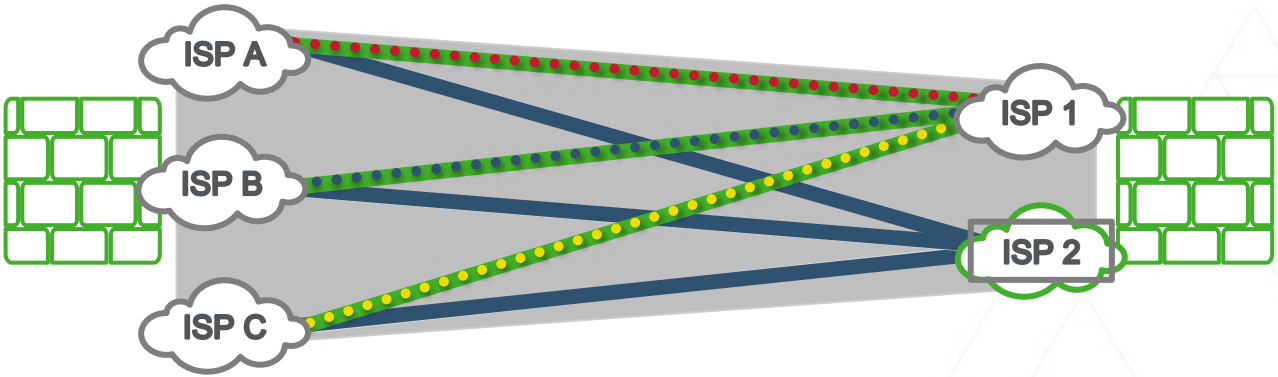
1 Site-to-Site Tunnel

MULTI-LINK VPN **LINK MODE**

The Link Mode of a VPN link determines how the link is used for VPN traffic:

- Active
- Standby
- Aggregate
- QoS-Based link selection





DRAG-AND-DROP **SETUP OF VPNs** – IN MINUTES, NOT HOURS

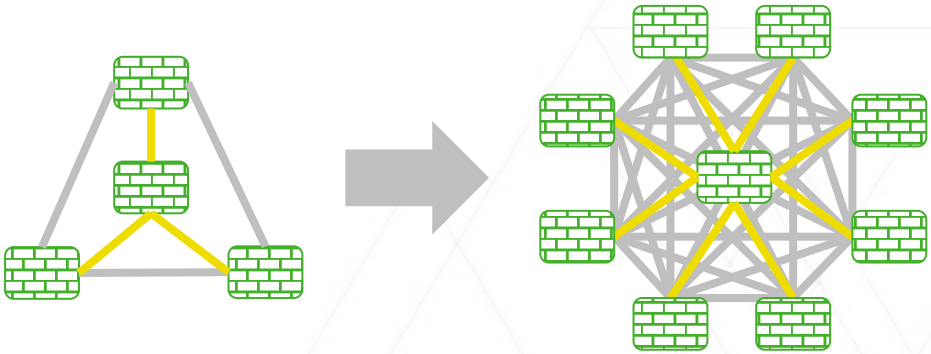
Enable site-to-site communications

Tailor policies for groups of sites

Create many different topologies

- Full-mesh, star, hub-and-spoke
- Handle thousands of sites efficiently

Scale up VPNs with just a few clicks



ENTERPRISE SD-WAN PROVIDES **MPLS SAVINGS** AND MUCH MORE

up to **90%** Savings

or **10x** Speedup

vs. MPLS

Agility

- ISP load-balancing
- Faster provisioning
- Automated VPNs

Continuity

- Transparent failover
- Zero-downtime updates

Faster Apps

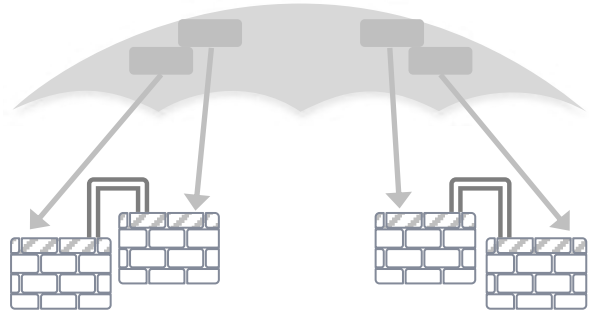
- Active-active
- Direct-to-Cloud connectivity
- QoS and bandwidth optimization

Security

- Deep Inspection
- Segmentation
- Granular decryption

FORCEPOINT DIFFERENCE: MOST SCALABLE, HIGHEST AVAILABILITY

Basic Failover



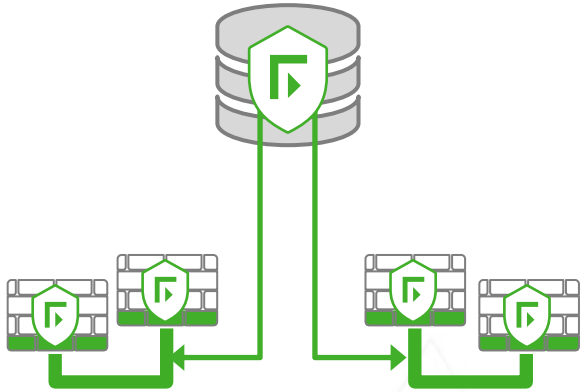
Bolted on top

- Often just 2 or 4 nodes of same model

Updates are painful – clusters go offline

- Each firewall updated separately
- After all done, cluster reassembled and brought online

Forcepoint Advanced Clustering



Built in from ground up

- Up to 16 nodes of mixed models, software versions

Updates are seamless – clusters stay running

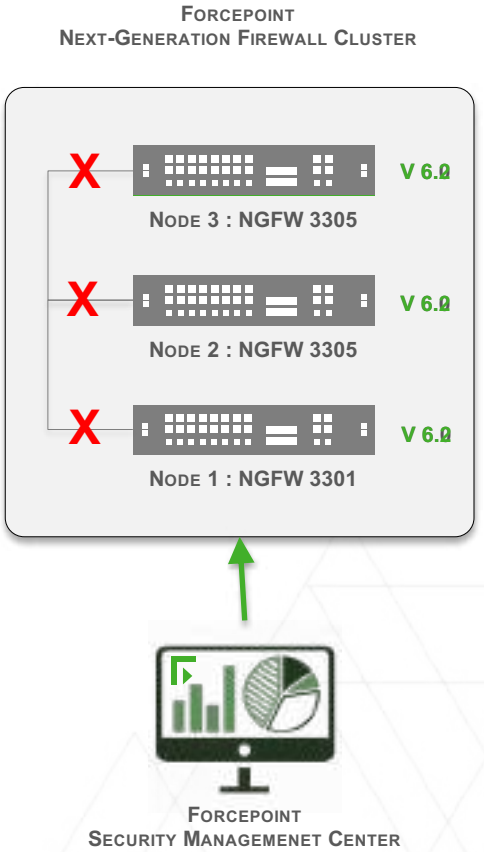
- Updates applied progressively
- Cluster never drops traffic

FORCEPOINT NGFW ADVANCED CLUSTERING

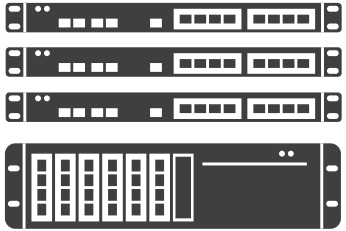
Clustering ensures high availability of the security engines, thus allowing uninterrupted operations during system maintenance and updates.

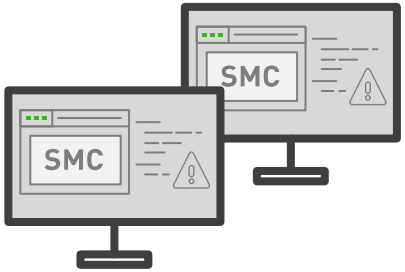
No Need to Take Firewalls Offline whether updating security policy, software version or even hardware

- Eliminates the risk of downtime
- Resilient to software and hardware failures
- Software and hardware upgrades without service windows
- Extends lifetime of investments



ENTERPRISE **RESILIENCE**





Clustered Networks

Active-Active, multi-ISP

Direct-to-Cloud high performance

No external routers needed

Clustered Devices

Active-Active, mixed devices/versions

Scales to 16 nodes

No external load balancers needed

Replicated Management

Policy-driven connectivity & security

Failover for rapid recovery

Distributed logs for ongoing visibility

Management at Scale

53%
Less
IT Staff Time

73%
Faster Incident
Response

Source: IDC Research

Flexible Deployment to Automate Operations

Zero-Touch
For unclustered appliances

Depot-to-site shipment of hardware

Appliance boots and asks Forcepoint Install Cloud for address of SMC console

Downloads configuration

USB
Used for clusters

Depot-to-site shipment of hardware

SMC admin loads config onto USB key

Technician inserts USB key into appliances

API-based
Used for clusters

Depot-to-site shipment of hardware

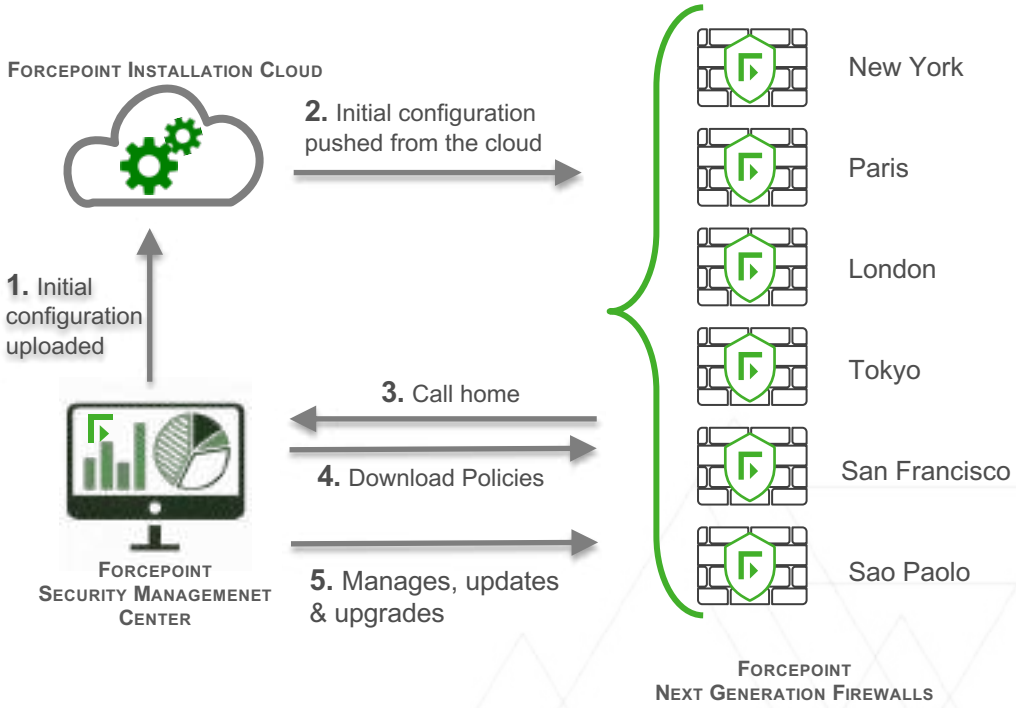
Technician uses tool to register site

Tool contacts SMC via APIs to get initial config for appliance

FORCEPOINT NGFW ZERO-TOUCH DEPLOYMENT

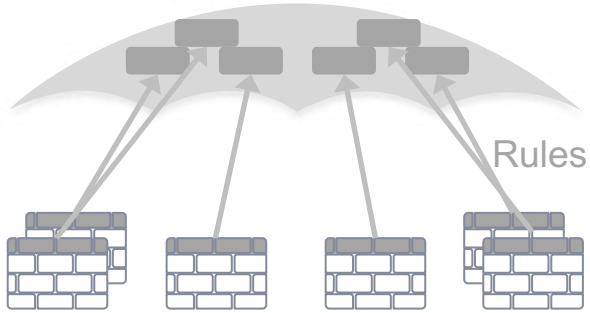
Cloud based plug & play installation

- Fast and easy remote site rollouts
- Cut deployment time from days to minutes
- Eliminate manual setup
- Scales to large networks
- Automatic policy push



FORCEPOINT DIFFERENCE: POLICY-CENTRIC MANAGEABILITY

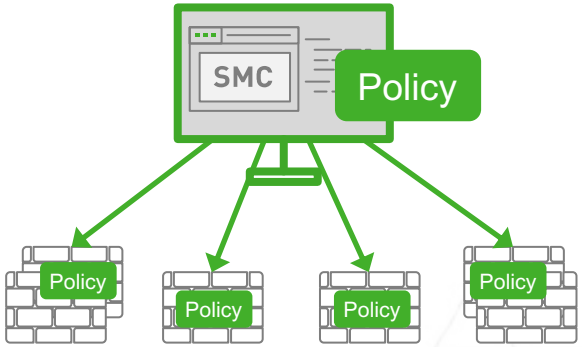
Remote Configuration



Manual, Low-level Rules

Repetitive

Forcepoint Centralized Management



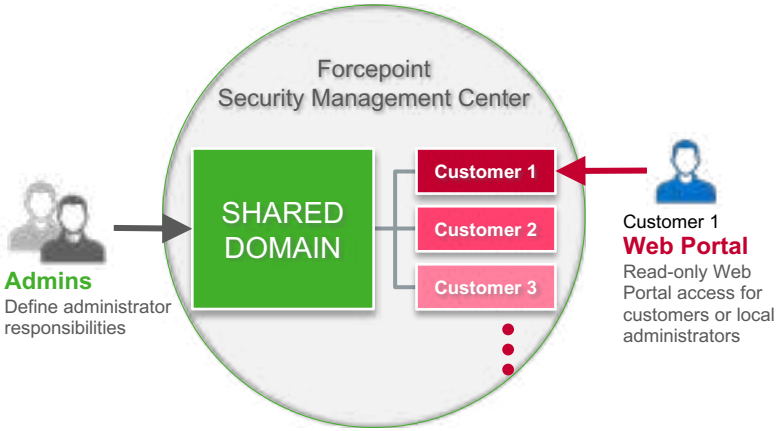
Automated, High-level Policies

Update hundreds of sites
in minutes, not hours

MULTI-TENANT MSSP OPERATIONS

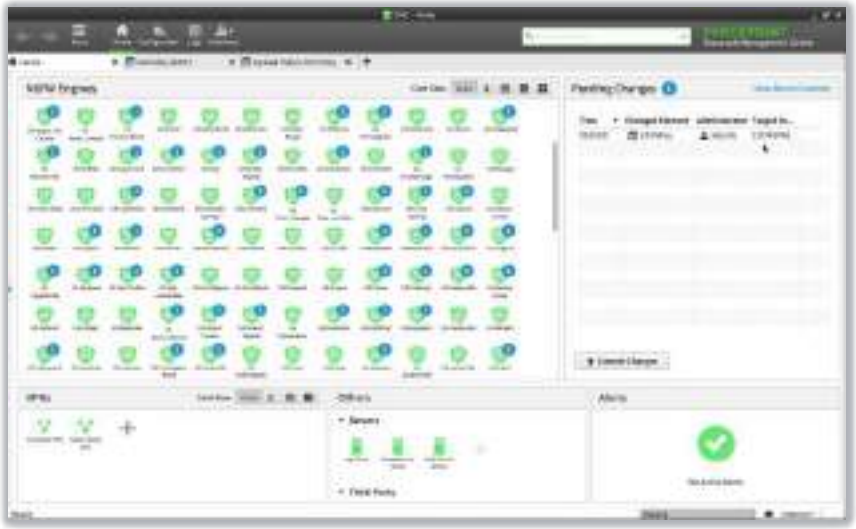
Compartmentalize Distributed Security

- All elements are stored in the same Management Server Database
- Domains are totally isolated from each other
- All Domains inherit elements from the Shared Domain



Region, Business Unit or Security Domains

ENTERPRISE **MANAGEABILITY** – UNPARALLELED VISIBILITY & CONTROL



Manage Branches • Edge • Data Centers • Cloud from one console

See what's happening everywhere & interactively drill down

Turn sophisticated business processes into automated policies

Update hundreds of locations in minutes, not hours

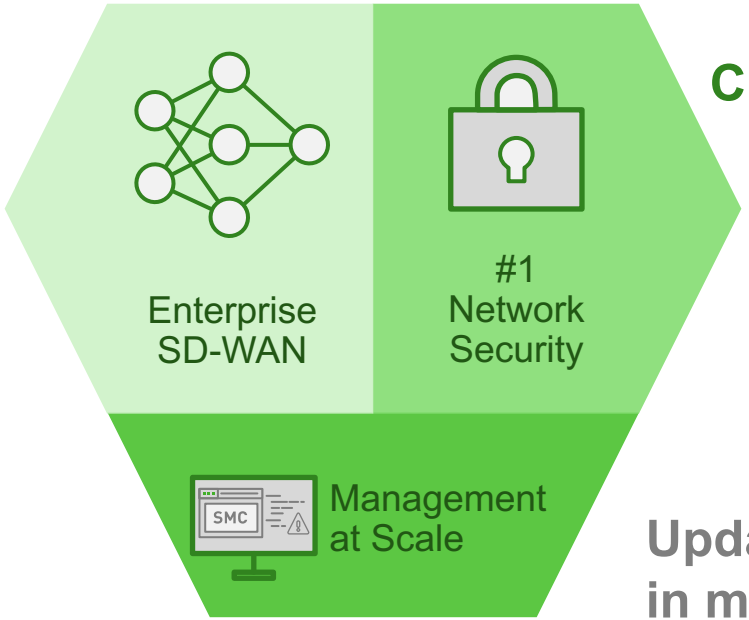
REAL-TIME MONITORING OVERVIEWS

- Customizable overview dashboards
- Hundreds of statistics available

WHY CUSTOMERS CHOOSE **FORCEPOINT SD-WAN, NGFW & IPS**

Always-on, even at cloud scale

Don't accept downtime, keep your people and business productive



Closes the Evasion Gap

Connect & protect your entire network with the #1 defense against Evasions, Exploits, and Malware

Updates hundreds of sites in minutes, not hours

Understand & control your users and data, everywhere, while reducing IT & compliance burdens

NEXT STEP: See it for yourself

THANK YOU

