



F5 Privileged User Access

June 10, 2020

Brian Yates
TSA, World Wide Technology

Username:

Administrator

Password:



Login

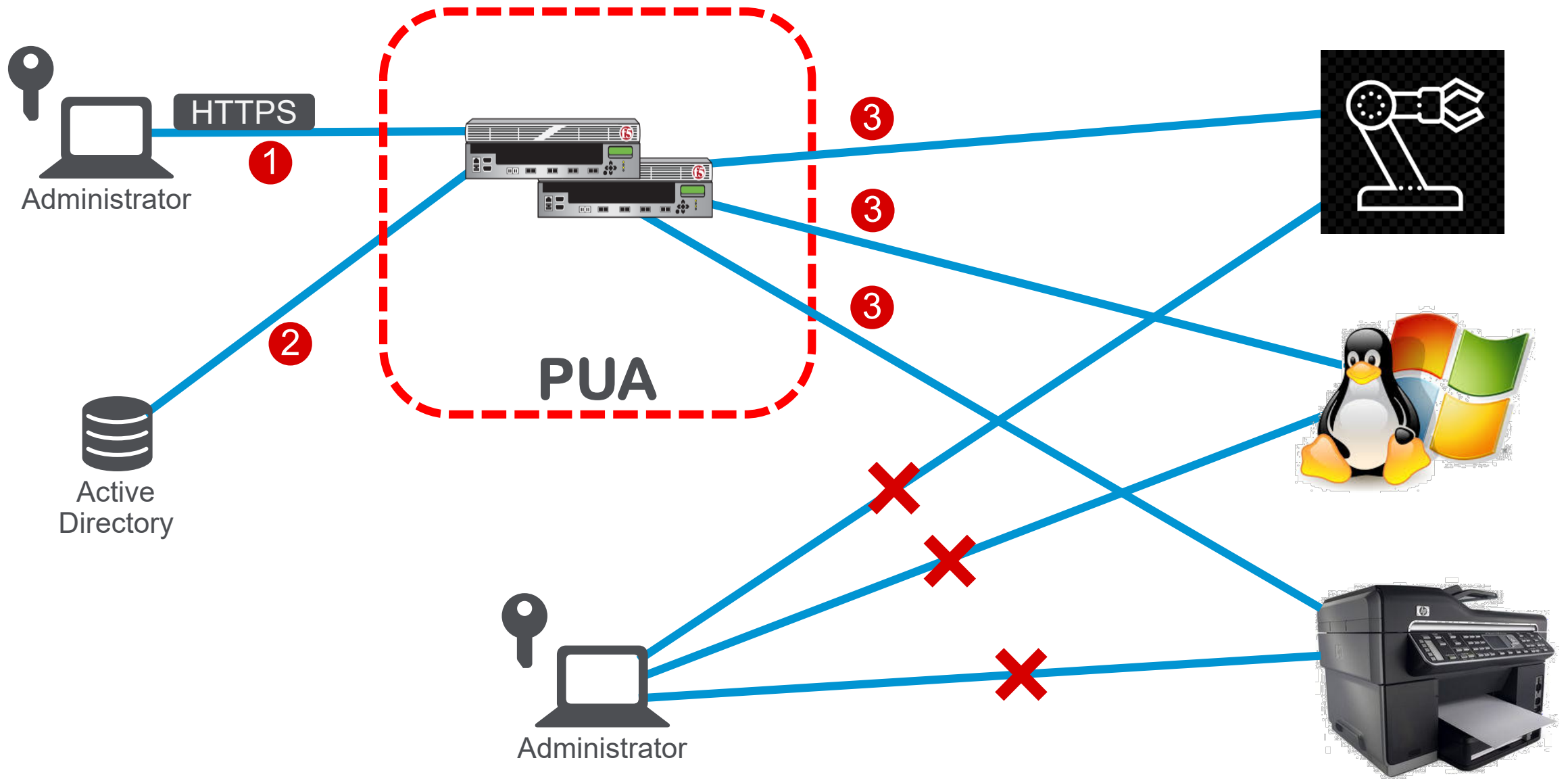
on this com

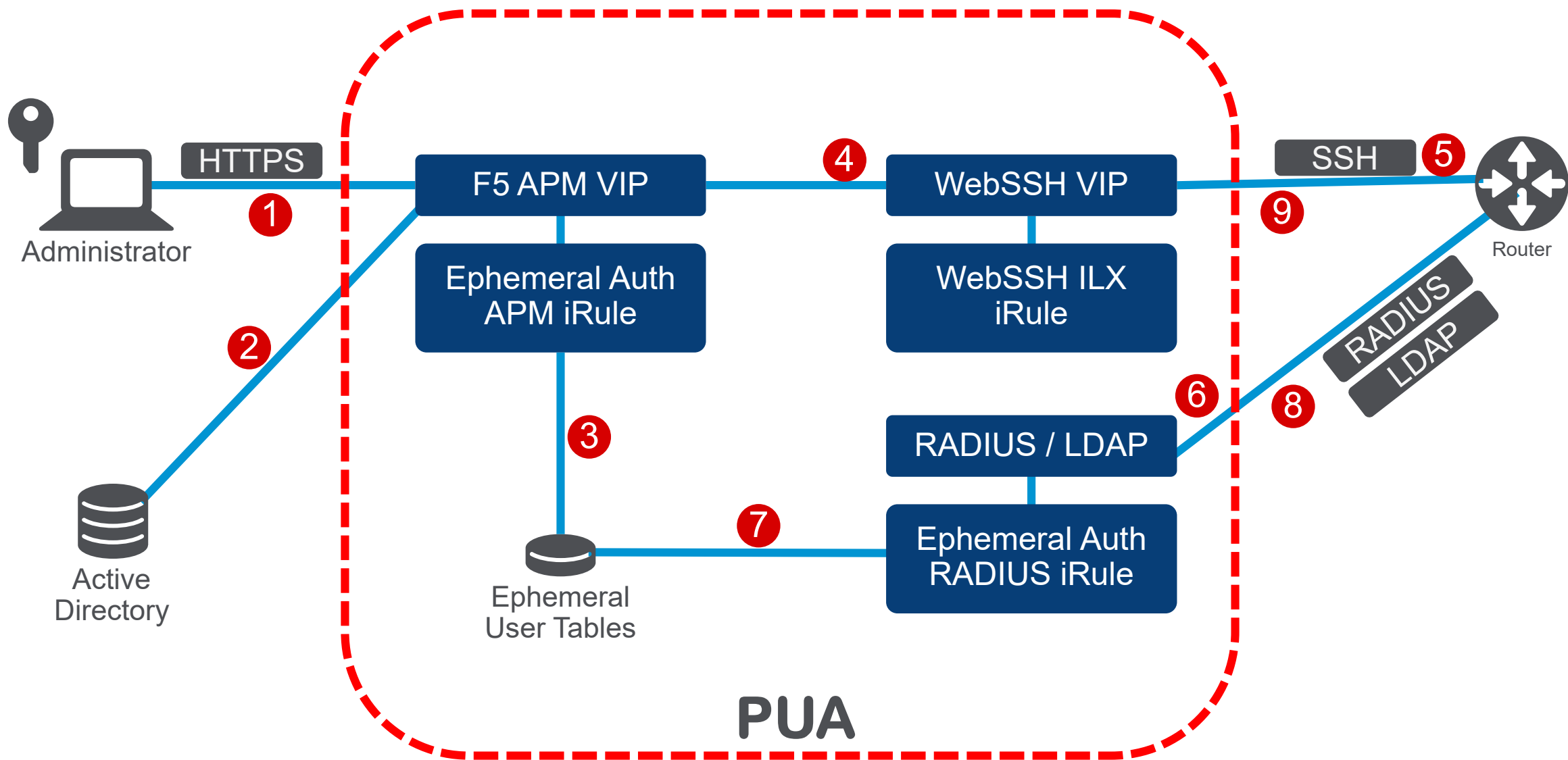
F5 Privileged User Access Solution

- **Configured using F5 Access Policy Manager**
- **Enforces strong CAC authentication for all devices**
- **CLI and GUI configuration via web browser**
- **No Jumphost/Jumpbox required**
- **Provides MFA, SSO and CAC Auth to all:**
 - Servers
 - Routers
 - Switches
 - Printers
 - IoT
 - ICS/SCADA

Why is this important?

- **Provides Cyber Security Scorecard Compliance**
- **DoD Cyber Scorecard MFA CAT 1 finding**
- **Get rid of static passwords, support next gen auth**
- **Fully FIPS Compliant**





Ephemeral Authentication

Ephemeral Authentication

- **Temporary passwords for legacy systems**
- **User has no knowledge or visibility of temporary passcode**
- **BIG-IP becomes authentication server for legacy system**
- **LDAP, RADIUS, Cisco ACS/ISE integration, Custom**
- **BIG-IP may also generate passwords in inject into existing access system (Active Directory, for example)**
- **No agents or software installed on clients, servers, routers**

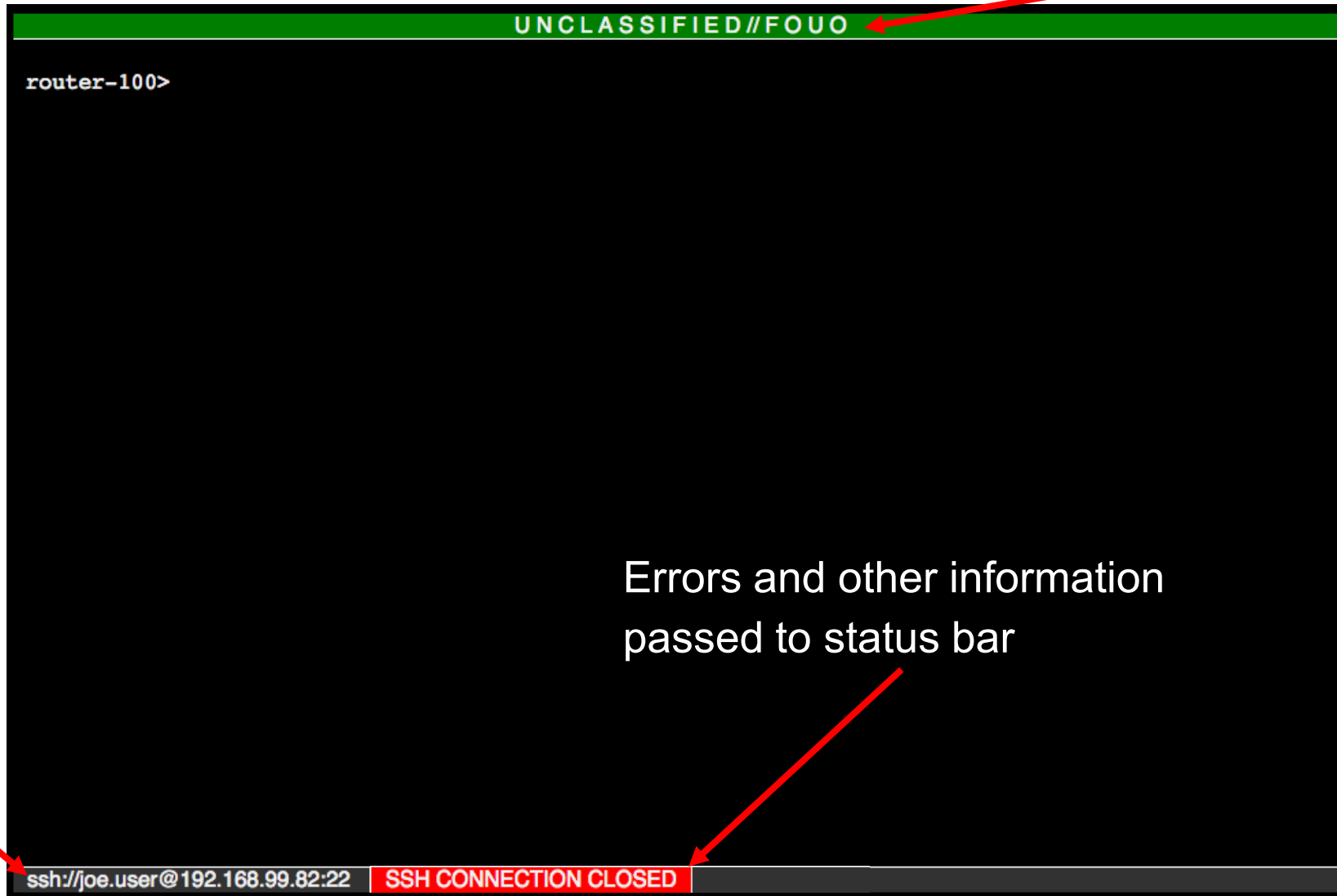
Ephemeral Authentication (continued)

- **Passwords meet criteria for DoDI 8500.2 (strong passwords)**
- **Passwords may rotate on APM session OR per application invocation (true one-time use password)**
- **External database integration is OPTIONAL**
- **Option support for AUTHORIZATION as well through RADIUS attributes**

Web to SSH Gateway

- **Provides CAC/MFA Authentication to SSH resources**
- **Supports both client side logging as well as server side logging to syslog or SIEM servers**
- **SSH Host Key verification and enforcement
(no user option to bypass SSH host key mismatch)**
- **Full terminal emulation (VT-xxx, ANSI, X-Term, etc...)**

Customizable Security Banner (per-host or global)



Status
Bar

Errors and other information
passed to status bar



Enter an internal resource



Routers



Router 100

Web SSH for Router 100



Router 200

Web SSH for Router 200



WebSSH



SSH Server 1

SSH access to server 1



SSH Server 2

SSH access to server 2



BIG-IP SSH



Firewall



Palo Alto SSH



Palo Alto Web



Cloud Services



Amazon AWS Portal



MS Azure Portal



HTTPS Management



BIG-IP Web



Demo



F5 SSL Orchestrator

June 10, 2020

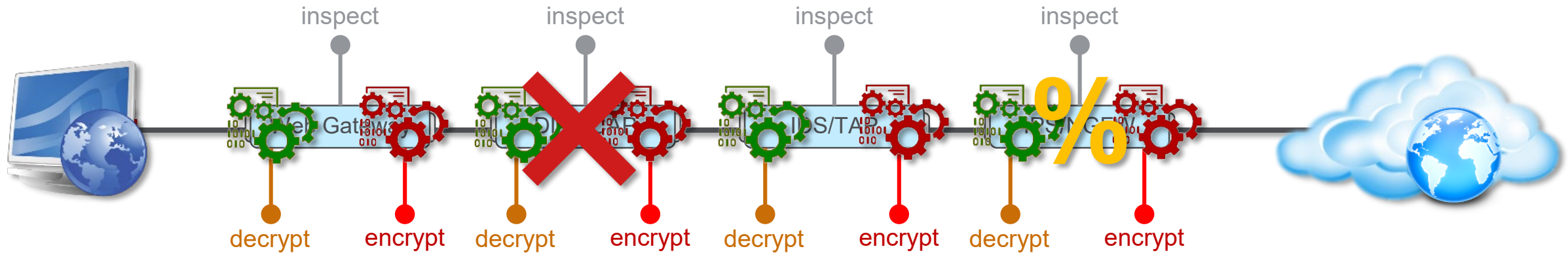
Brian Yates
TSA, World Wide Technology

Defending Against Encrypted Threats

- **Average of 90% of page loads encrypted with SSL/TLS**
- **You can't defend against what you cannot see**
- **SSL Break/Inspect allows security tools to mitigate:**
 - Spyware
 - Phishing attacks
 - Credential theft
 - Session hijacking
 - Malicious files (PDF, Word, etc.)
 - Trojan horse
 - Data Loss

SSL Visibility

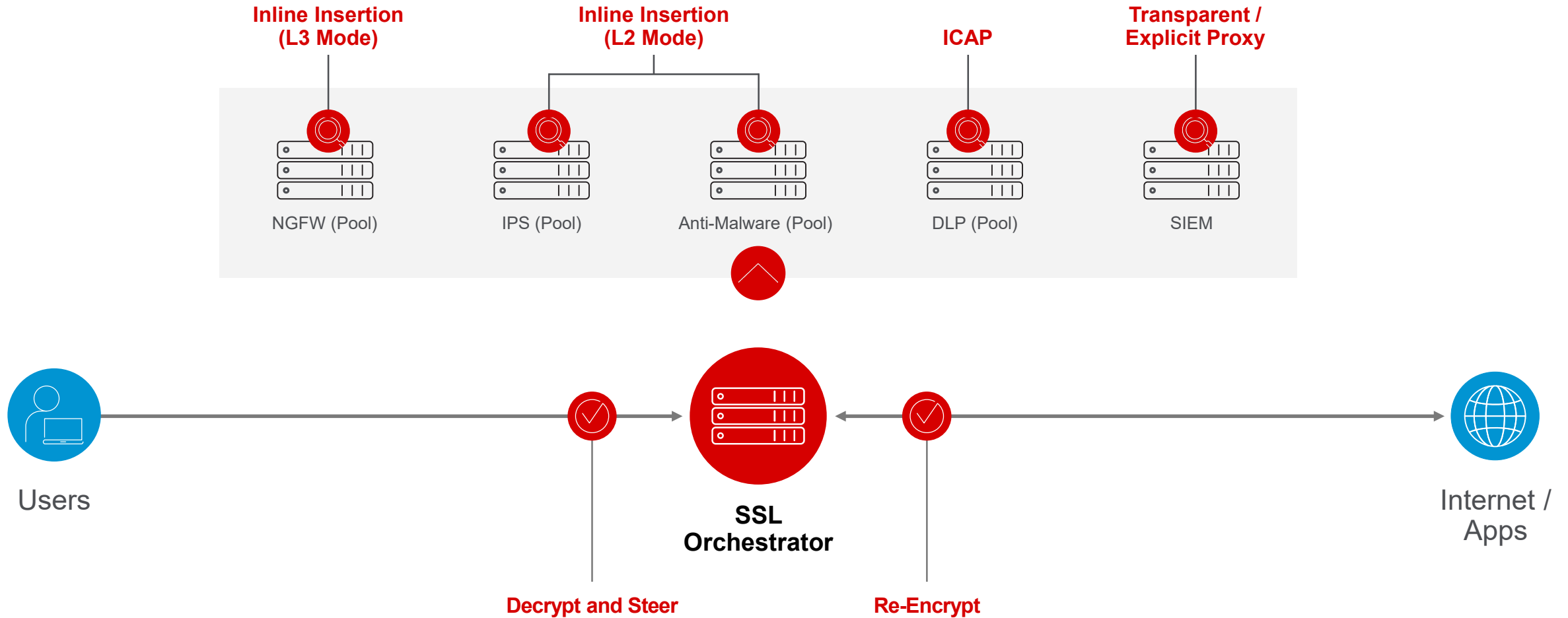
Traditional SSL Daisy-Chain Network Design



Challenges & Realities of Daisy-Chaining

- Multiple Intercept Points
- Multiple Points of Failure
- Increased Latency
- Increased Complexity
- Complicated troubleshooting
- Performance Impacts
- Impacts “Perfect” Forward Secrecy
- Reduced Security ROI
- Must go through every service
- Over-subscribing services
- Complicated Mesh HA Designs
- Bypass on failure (added Hardware)

Broad Topology and Device Support



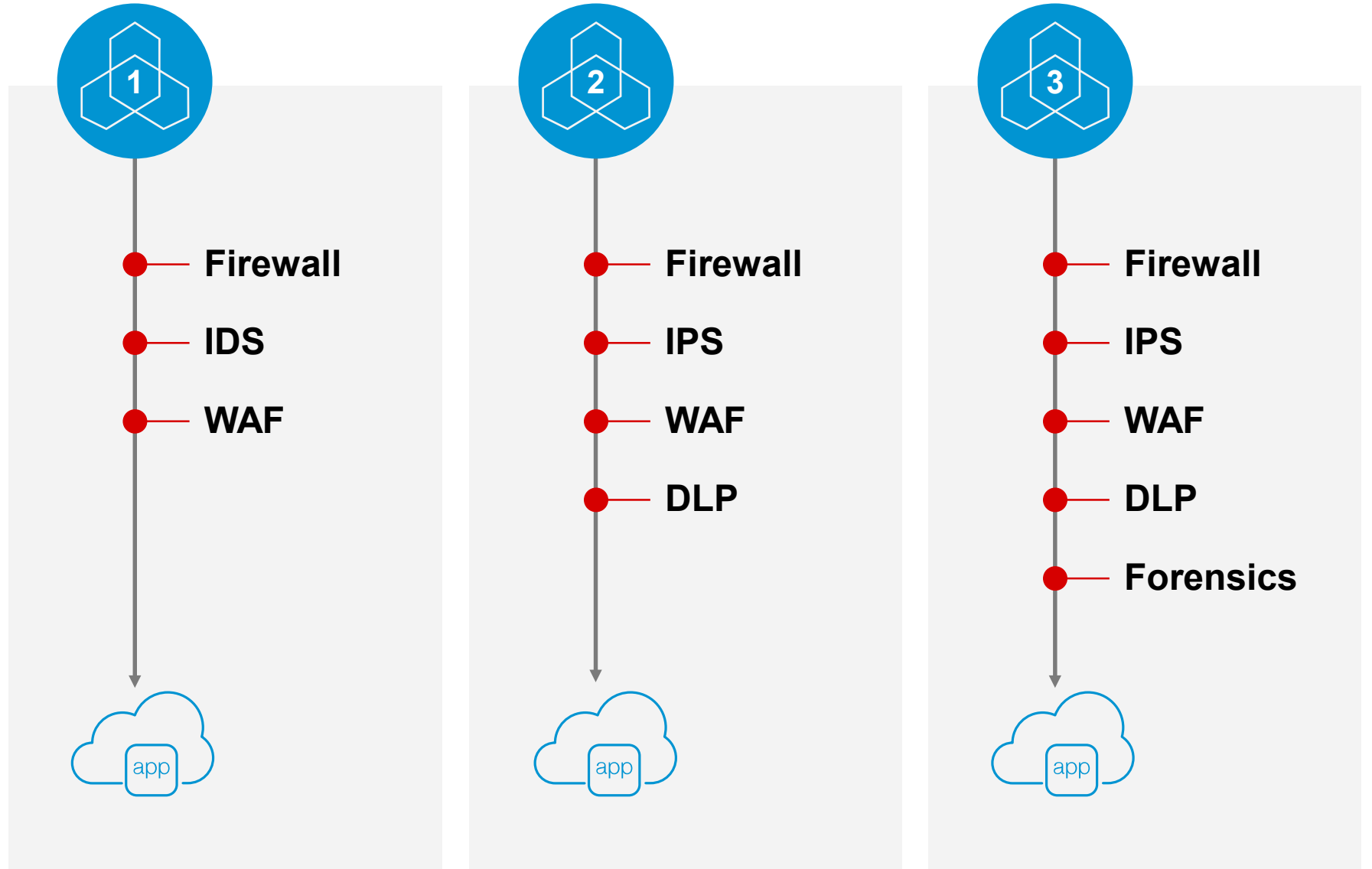
Dynamic Service Chaining

Dynamic grouping
of security devices

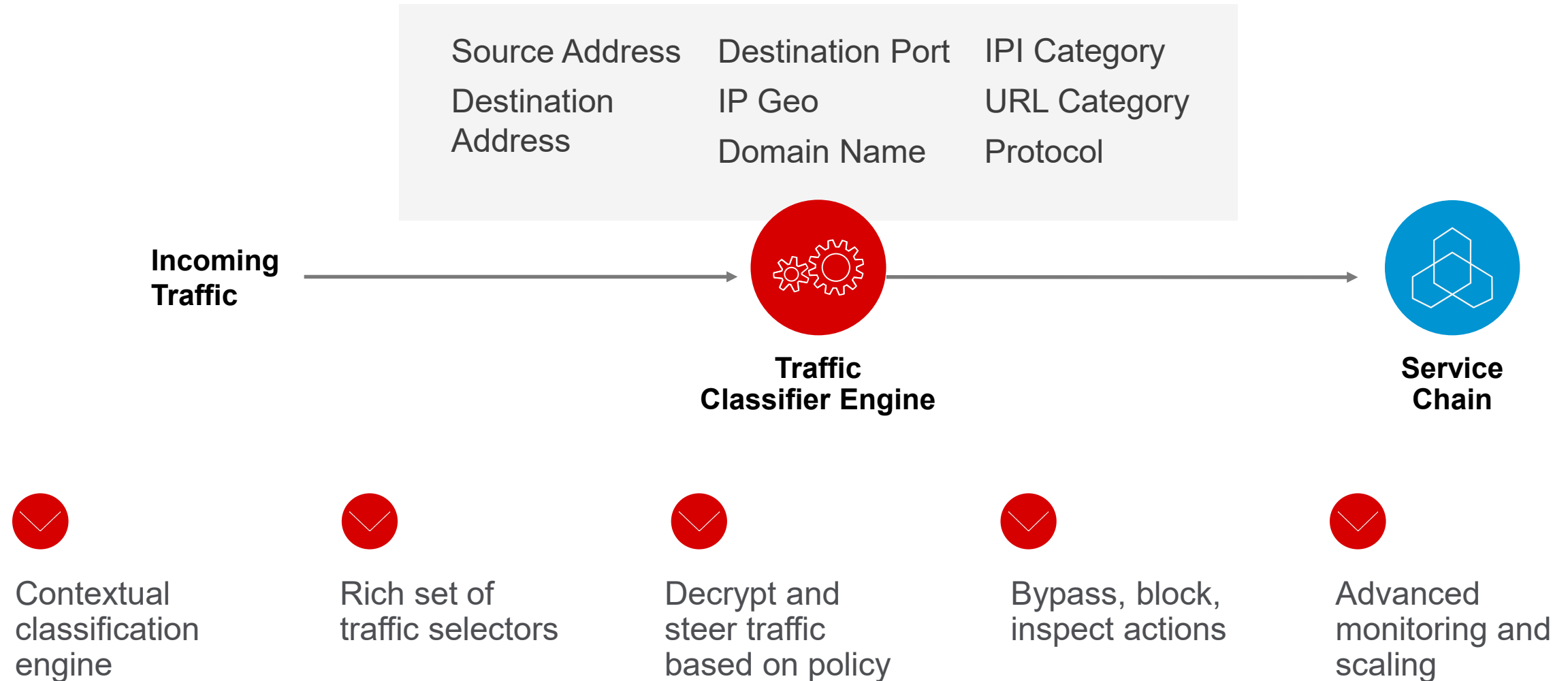
Topology independent

Maximizes security
investments

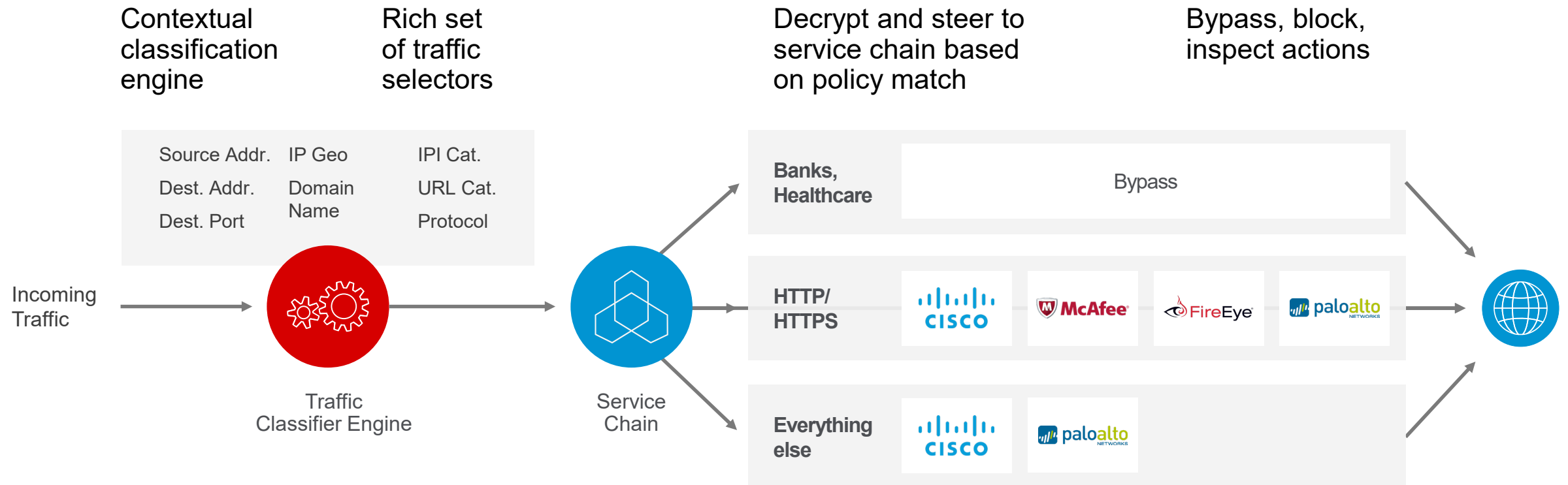
Service insertion,
monitoring, scaling



SSL Orchestrator Policy-Based Traffic Steering



SSL Orchestrator Policy-Based Traffic Steering



We want to pre-filter traffic going to [our Firewall] so we make more effective use of them.

F5 SSL Orchestrator Key Use Cases



SSL/TLS visibility
and orchestration



Maximize security
investments



Risk management
and privacy

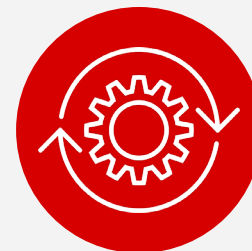
F5 SSL Orchestrator Advantage



Go beyond visibility
with orchestration

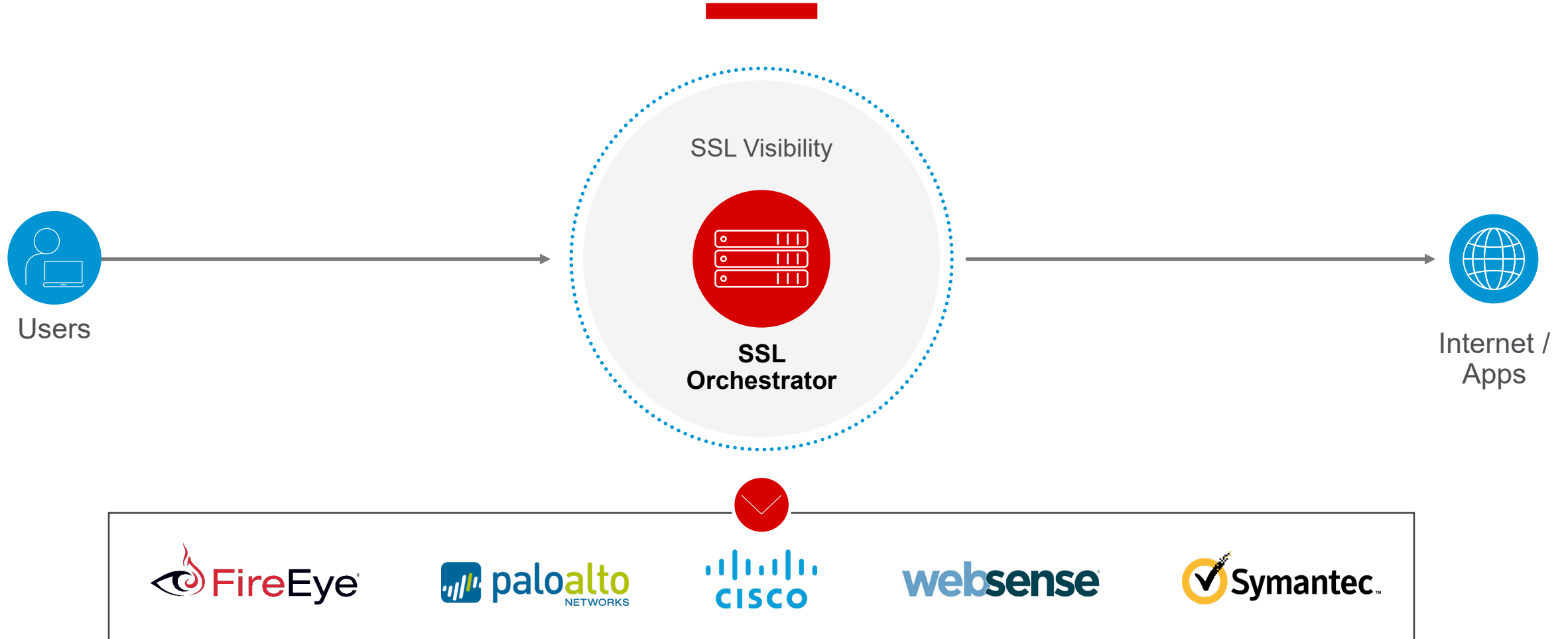


Dynamic service
chaining and policy-
based traffic steering



Seamless
integration

SSL Orchestrator Ecosystem



SSL Orchestrator Ecosystem and Partnerships

F5 BIG-IP and Cisco ASA

Cisco ASA

F5 BIG-IP and Cisco ASA FirePOWER: Using the SSL Intercept with Service Chaining iApps Template v3.0



By
Sanjay Shilole | Solution Engineer,
Business Development
Kashyap Merchant | Access Product
Management

F5 BIG-IP and FireEye NX

FireEye NX

F5 BIG-IP and FireEye NX: Using SSL Intercept with Service Chaining iApps Template v3.0

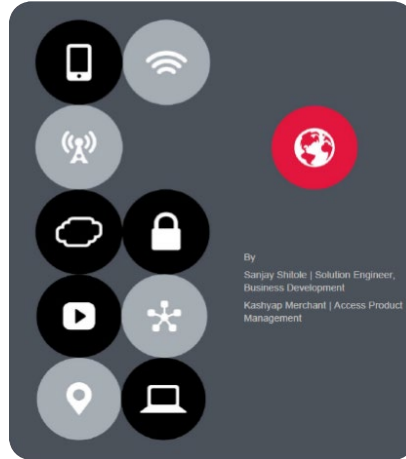


By
Sanjay Shilole | Solution Engineer,
Business Development
Kashyap Merchant | Access Product
Management

F5 BIG-IP and Symantec DLP

Symantec DLP

F5 BIG-IP System with Symantec DLP: Using SSL Intercept with Service Chaining iApps Template v3.0



By
Sanjay Shilole | Solution Engineer,
Business Development
Kashyap Merchant | Access Product
Management

F5 BIG-IP and Palo Alto Networks NGFW

Palo Alto Networks NGFW

The F5 BIG-IP Platform and Palo Alto Networks Next-Gen Firewall Solution: SSL Orchestration with Service Chaining



By
Sanjay Shilole | Solution Engineer,
Business Development
Kashyap Merchant | Access Product
Management



Demo