# Introduction to SSL Orchestrator

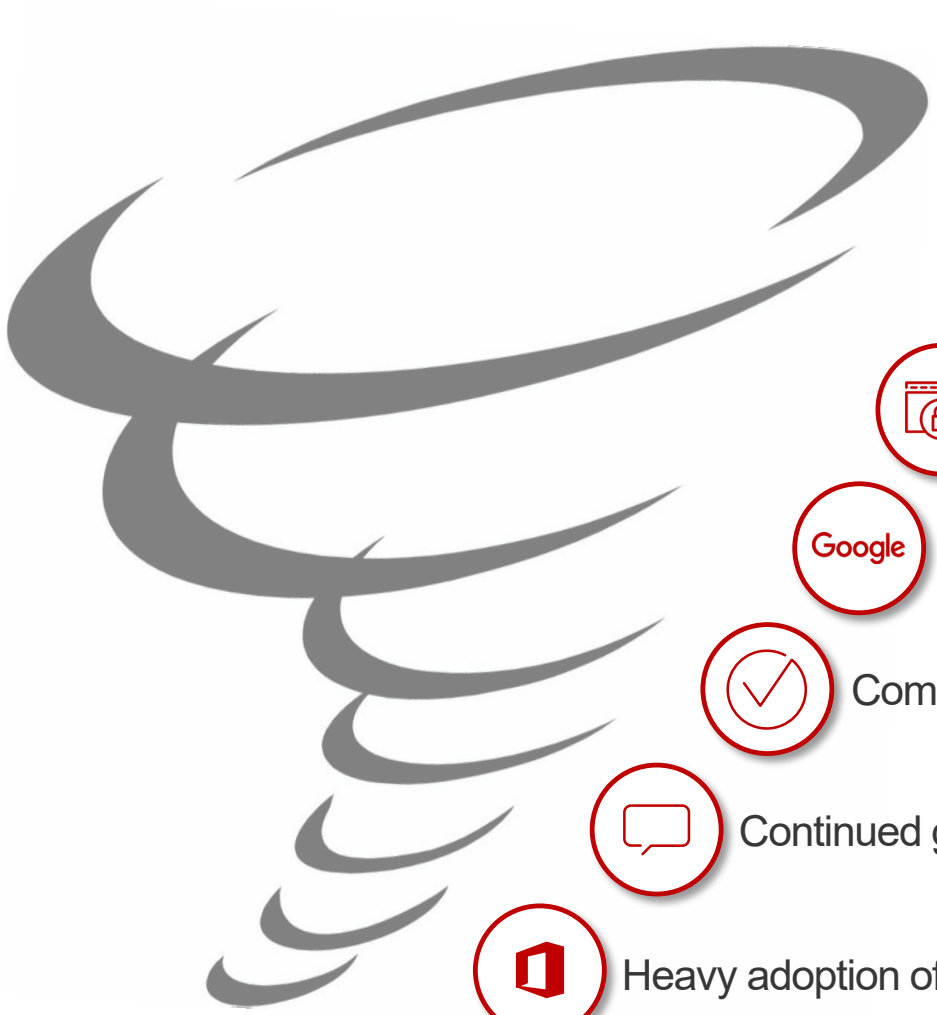
# Encryption is now the norm

**89%**

of page loads are now encrypted with SSL / TLS

SOURCE: F5.COM/LABS

# What's Driving Encrypted Traffic

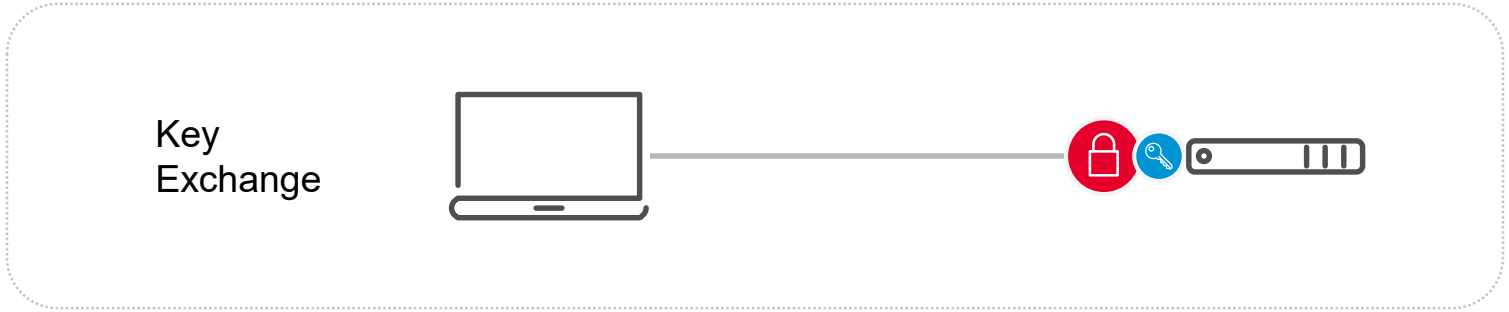


- Increased focus on user and data privacy
- Chrome browser warnings
- Certificate Authorities offering free SSL / TLS certs (Let's Encrypt)
- Google Search result rankings
- Compliance with government privacy regulations (ex. GDPR)
- Continued growth of social networks
- Heavy adoption of Office 365 and other online productivity suites

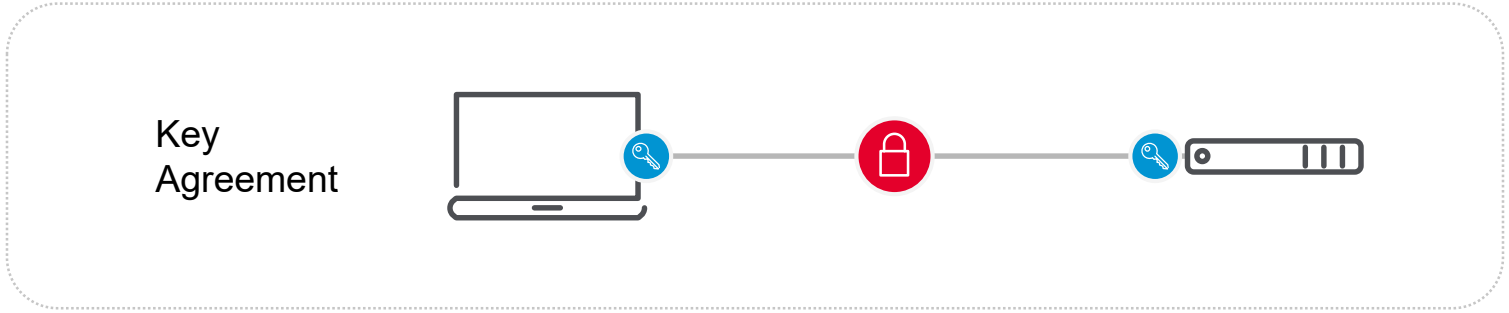
# Perfect Forward Secrecy

**Ephemeral keys** used to encrypt and decrypt information for each session, exposing only a small portion of sensitive user data if the latest key is compromised.

## RSA, most common




## Diffie-Hellman (Ephemeral)




**88%** of hosts prefer forward secrecy

Source: 2017 F5 TLS Telemetry Report

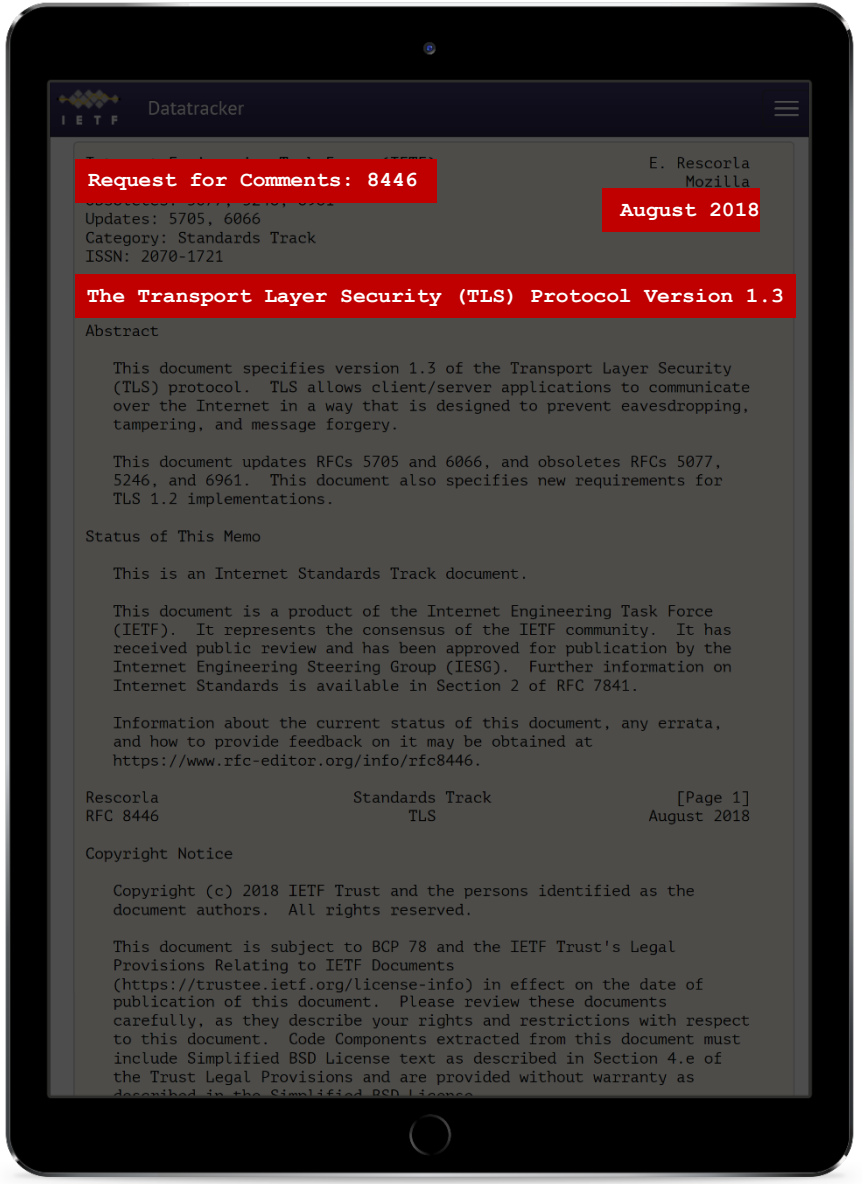
# TLS 1.3 ratified

Designed to be **easy to deploy**

Mandatory use of **PFS Ciphers**

**Shorter handshake** to reduce latency and lower CPU usage

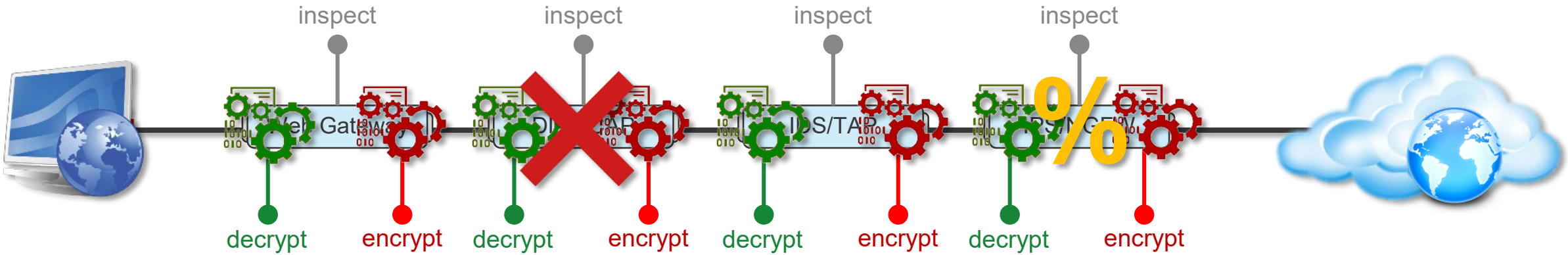
**Improved performance** with 0-RTT



# F5 SSL Orchestrator

# 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)

If done correctly, SSL visibility is the best line of defense against encrypted malware.

# SSL Orchestrator

## Evolution

### 4.0

- Dynamic service chaining
- Traffic classification
- L3 Outbound
- L2/L3, ICAP, TAP services

- Access v2 refactor
- L3 inbound
- HTTP services
- Explicit proxy auth
- ICAP filtering
- vCMP support
- Email and FTP support
- Certificate revocation
- iRule injection

### 5.0

- Guided configuration
- L2 inbound/outbound
- Existing application
- Topologies
- Service catalog

### 6.0

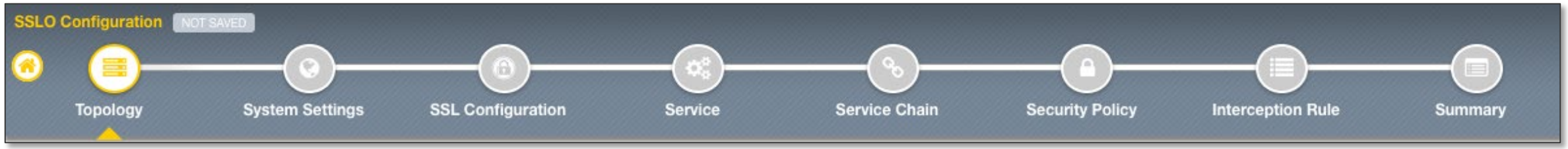
- Captive portal auth
- Chassis support
- TLS 1.3 support
- On-box analytics

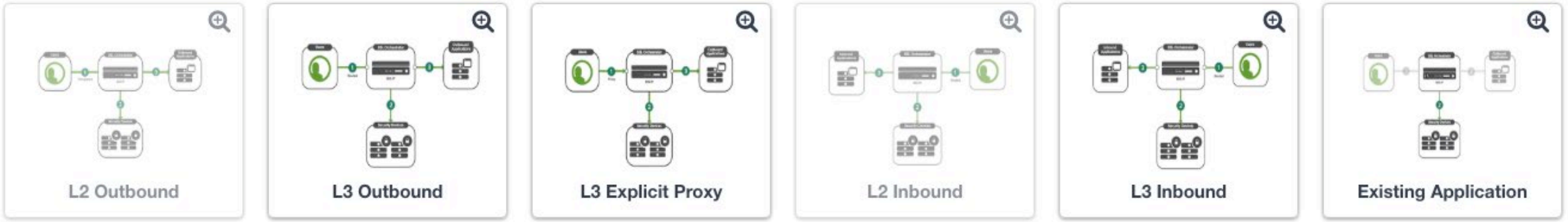
### 7.0

- Stability enhancements
- HA enhancements
- L2 enhancements

# SSL Orchestrator Architecture

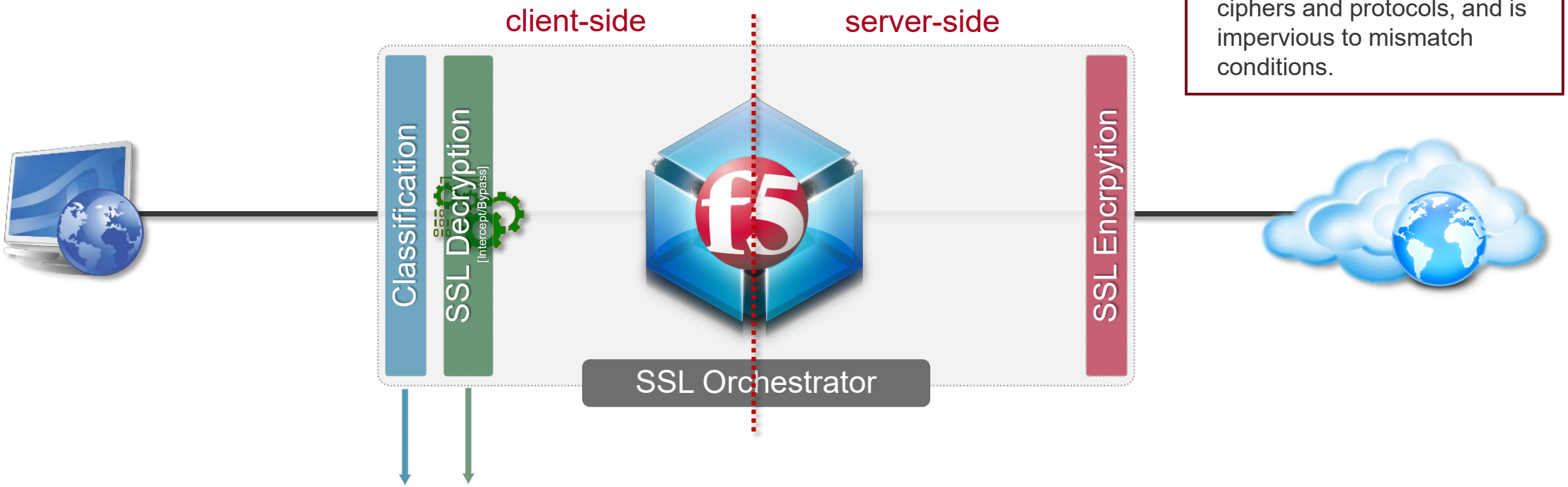
## Guided Configuration: Topologies



# SSL Orchestrator

## A Functional Overview




- IP Reputation
- Source IP
- Destination IP
- IP Geolocation
- Destination Port
- Domain Name/SNI
- URL Filtering Category
- Protocol

SSL Decryption occurs based on classification Service Chain assigned. Action is either to Intercept (decrypt) or Bypass.

### Cipher Diversity

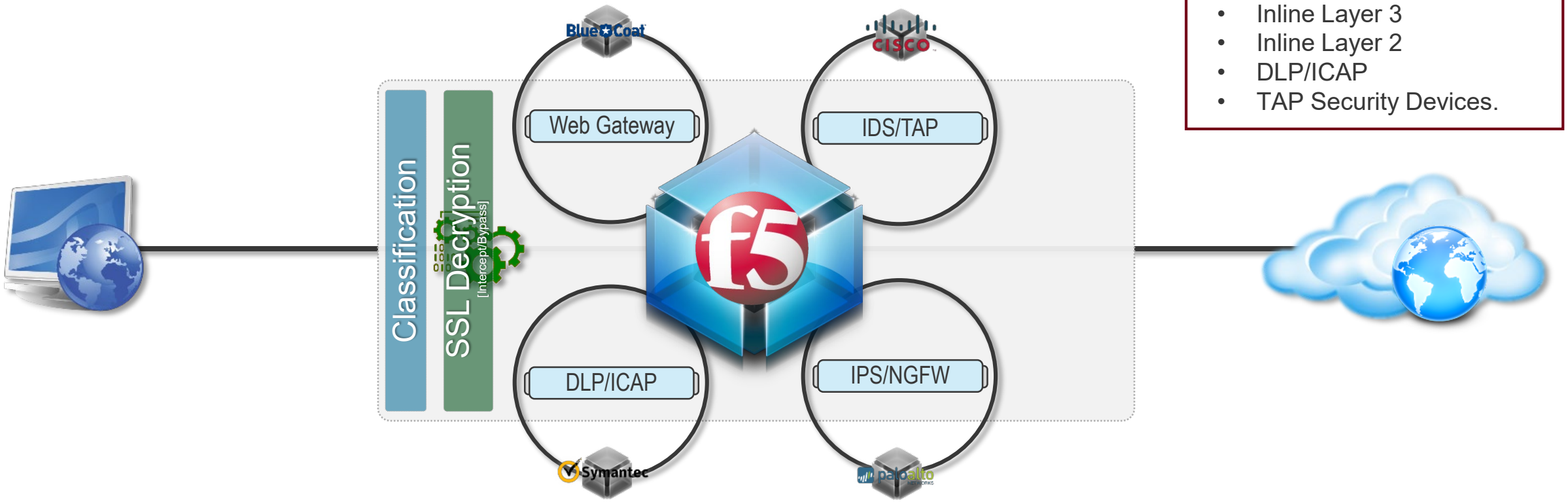
The proxy architecture allows for independent control of client-side and server-side ciphers and protocols, and is impervious to mismatch conditions.

### SSLO Flow Support

Ingress (inbound) & Egress (outbound) flow support.

# SSL Orchestrator

## A Functional Overview




**Dynamic Device Support**

SSL Orchestrator supports:

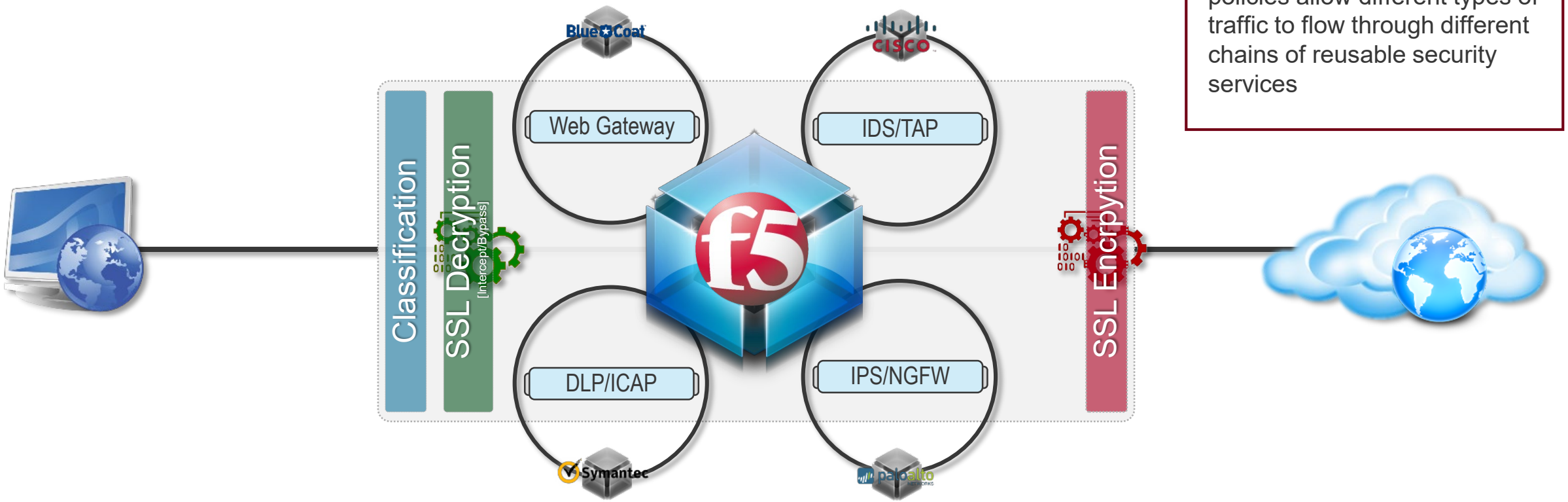
- Inline HTTP (Web Proxy)
- Inline Layer 3
- Inline Layer 2
- DLP/ICAP
- TAP Security Devices.

# SSL Orchestrator

## A Functional Overview

**Dynamic Service Chaining**

Context-based classification policies allow different types of traffic to flow through different chains of reusable security services

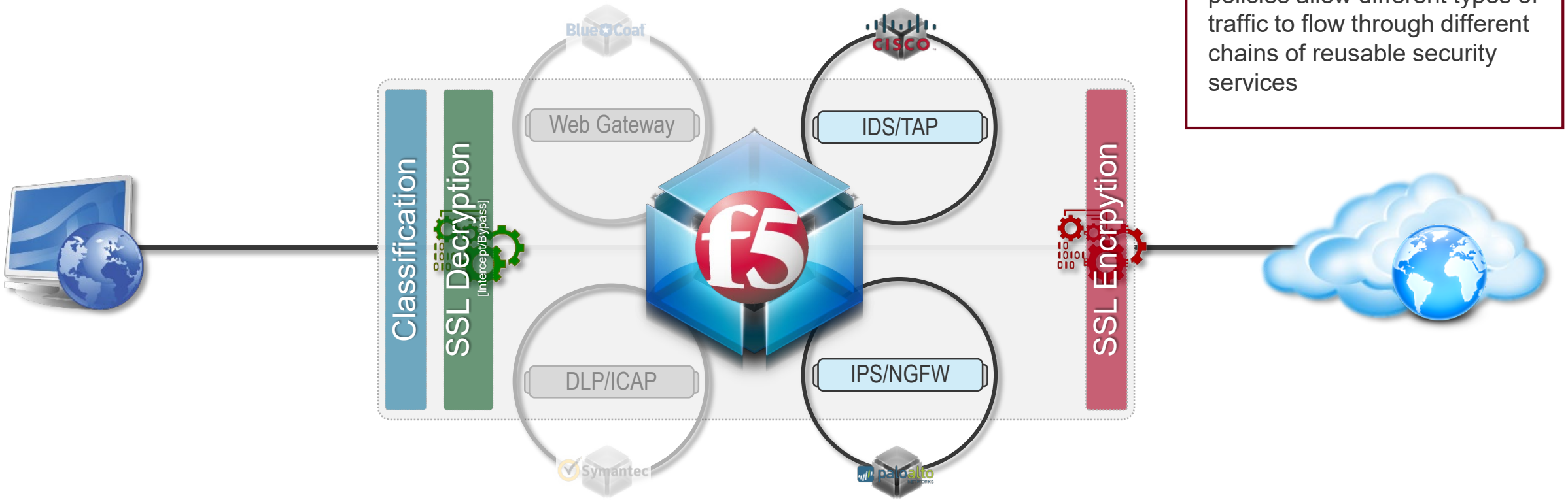


# SSL Orchestrator

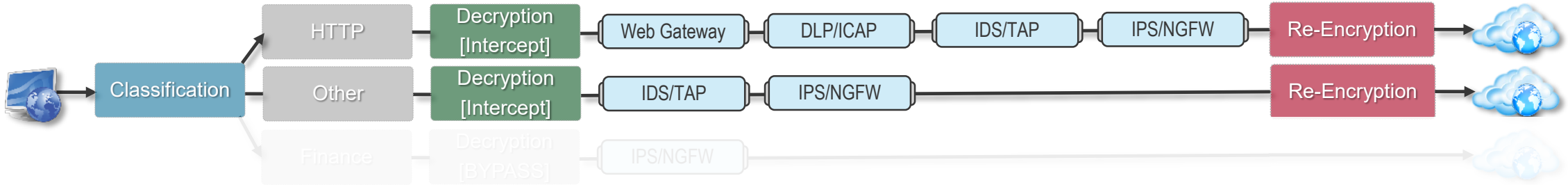
## A Functional Overview

**Dynamic Service Chaining**

Context-based classification policies allow different types of traffic to flow through different chains of reusable security services




Dynamic Service Chain

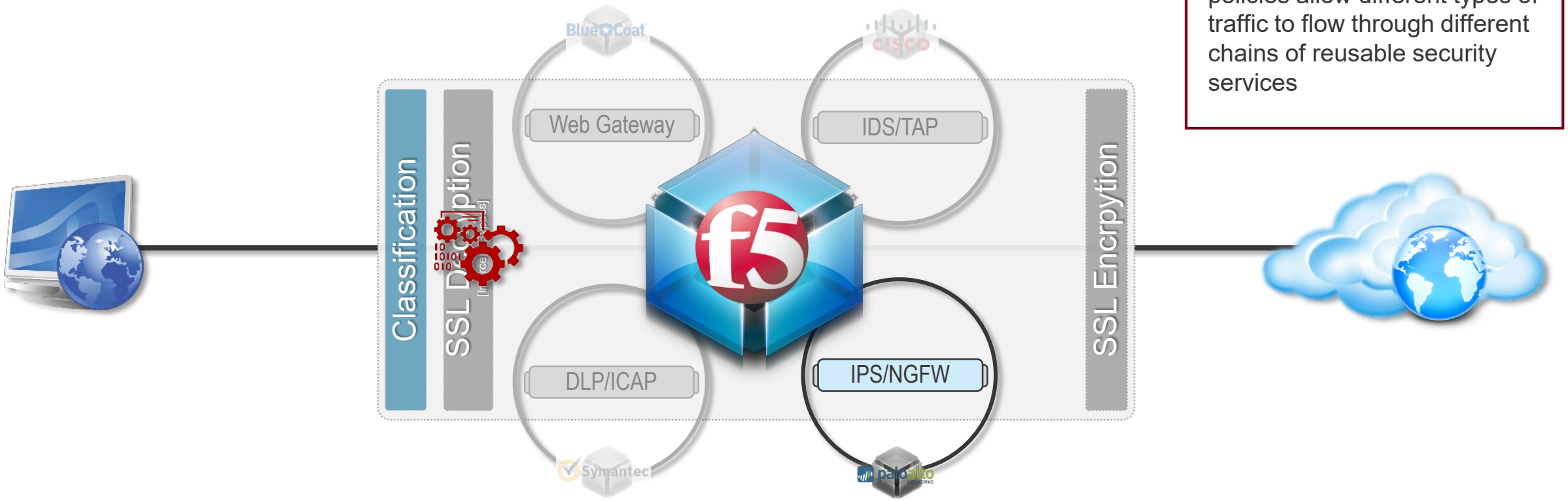


# SSL Orchestrator

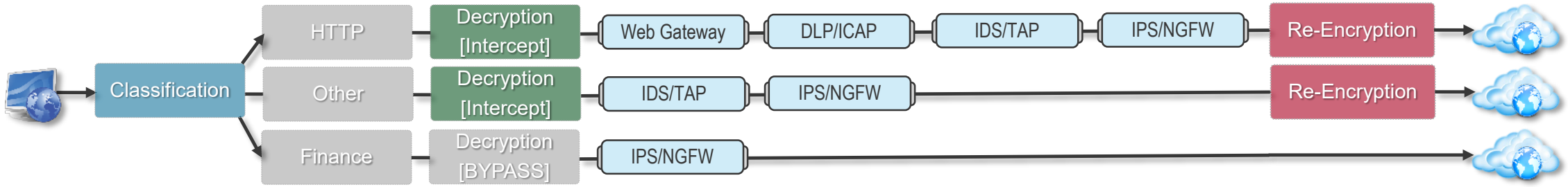
## A Functional Overview

**Dynamic Service Chaining**

Context-based classification policies allow different types of traffic to flow through different chains of reusable security services




Dynamic Service Chain



# SSL Orchestrator

## A Functional Overview

### Dynamic Scaling

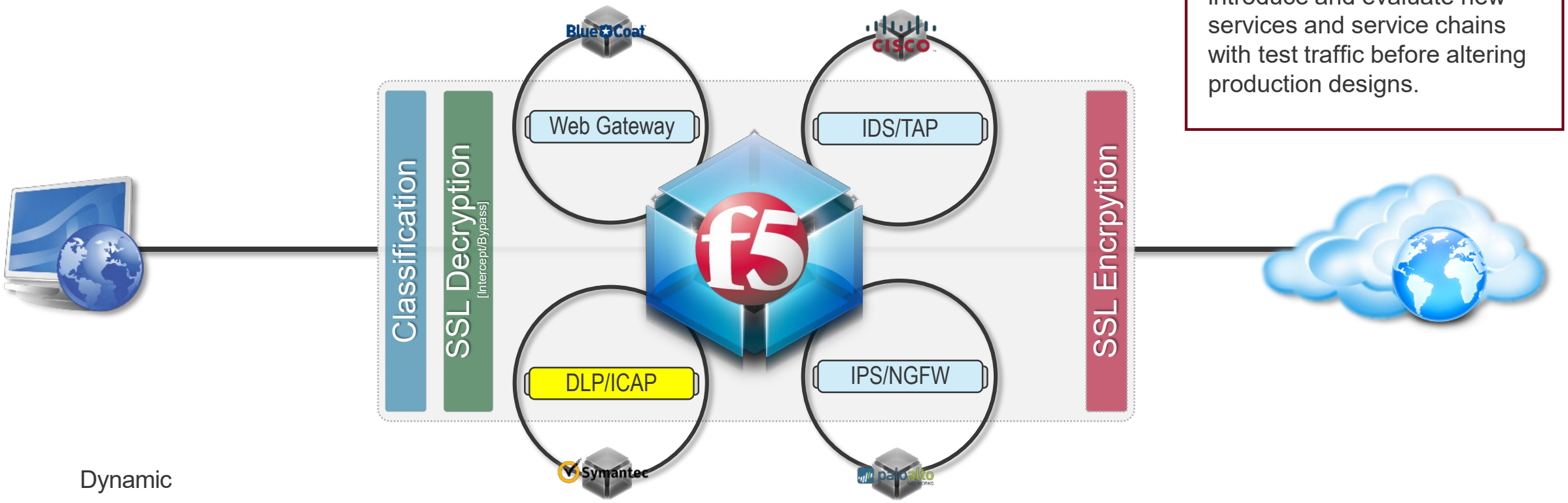
A full proxy architecture provides for robust load balancing, monitoring and independent scaling of any number of security devices.

# SSL Orchestrator

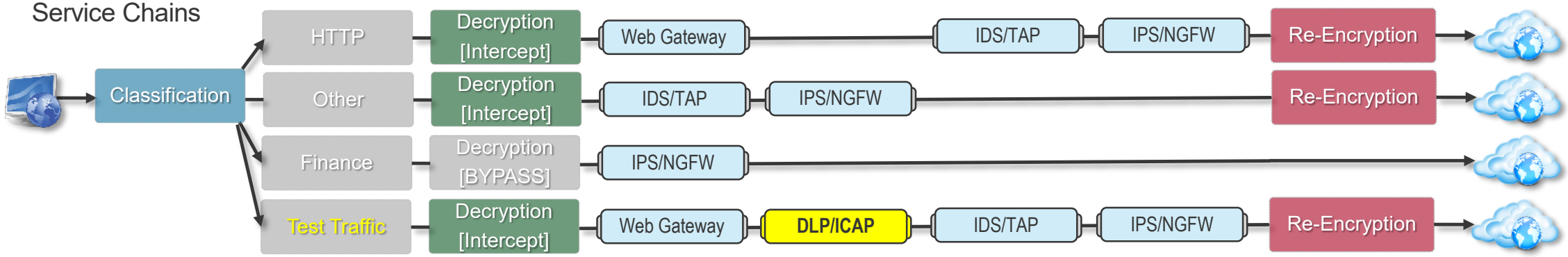
## A Functional Overview

### Dynamic Evaluation

The ability to dynamically introduce and evaluate new services and service chains with test traffic before altering production designs.

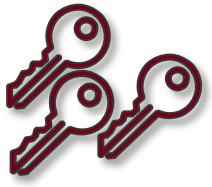



Dynamic
Service Chains



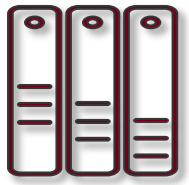
# SSL Orchestrator

## Technology Advantages



### Cipher Diversity

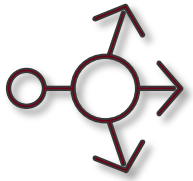
The proxy architecture allows for independent control of client side and server side ciphers and protocols, and is impervious to mismatch conditions.



### Dynamic Device Support

SSL Orchestrator supports:

- Inline HTTP
- Inline Layer 3
- Inline Layer 2
- DLP/ICAP
- TAP security devices.



### Dynamic Service Chaining

Context-based policies allow different types of traffic to flow through different chains of reusable security services.

### Dynamic Scaling

A full proxy architecture provides for robust load balancing, monitoring and independent scaling of any number of security devices.

### Dynamic Evaluation

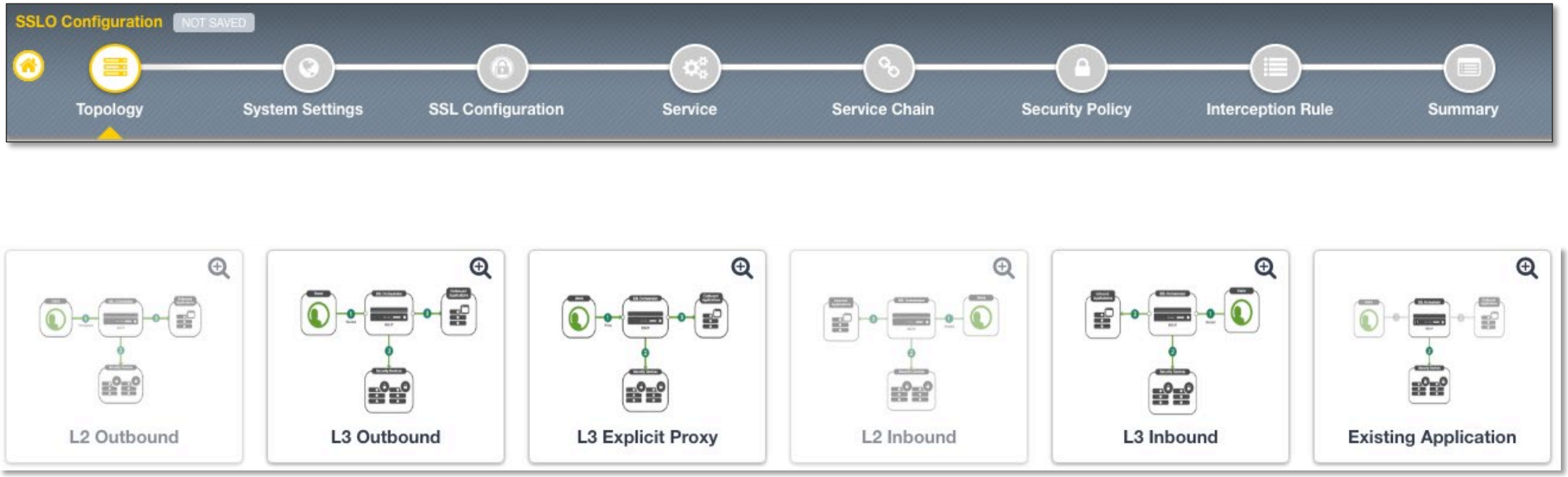
The ability to dynamically introduce and evaluate new services and service chains with test traffic before altering production designs.

# SSL Orchestrator

## Guided Configuration: Dashboard

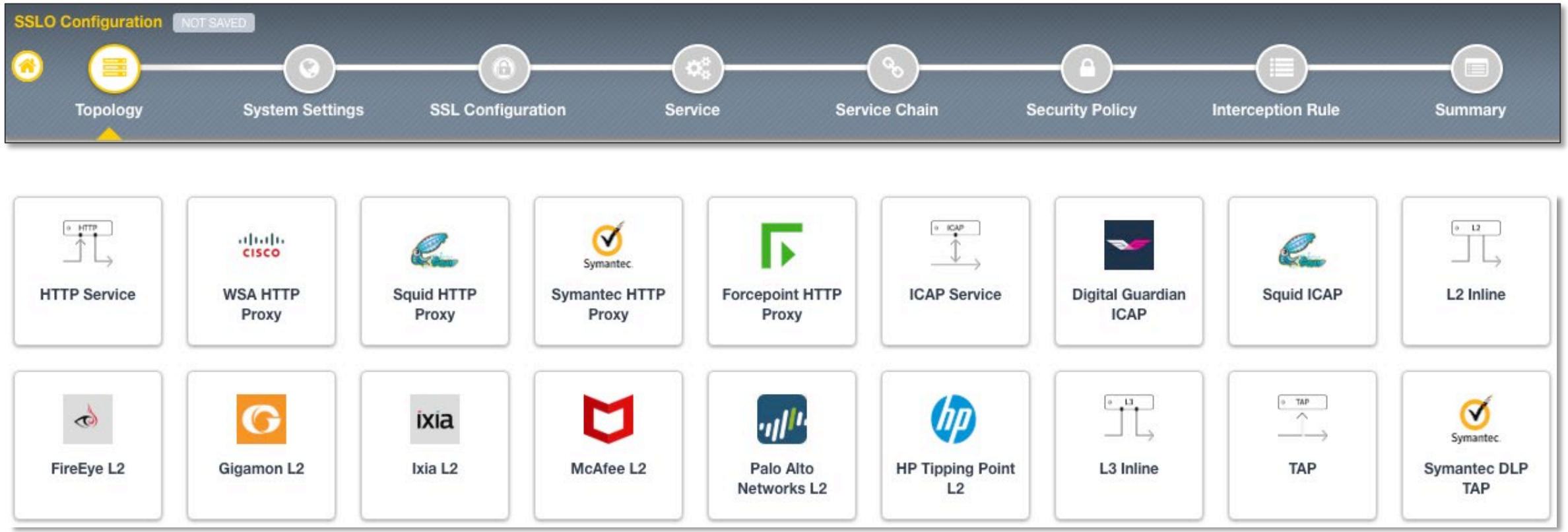
# SSL Orchestrator

## Guided Configuration: Topologies



# SSL Orchestrator

## Guided Configuration: Service Catalog (Expanding)



# Let’s walk through an SSLO Demo

# F5 DoD Account Team

| | | | | | |
|---|---|---|---|---|---|
| Air Force | | AE / East | Eddie Augustine | e.augustine@f5.com | 301-717-4131 |
| | | AE / West | Dustin Purkey | D.Purkey@F5.com | 714-501-4815 |
| | | SE / East | Arnulfo Hernandez | A.Hernandez@f5.com | 202-360-1984 |
| | | SE / West | Paul Deakin | p.deakin@f5.com | 949-395-0051 |
| DISA | | AE | David Thomas | d.thomas@f5.com | 703-930-9623 |
| | | AE | Thomas Ries | T.Ries@f5.om | 703-850-4654 |
| | | SE | Anthony Graber | anthony.graber@f5.com | 443-987-6487 |
| Navy<br>Marine Corps | | AE / East | John Manning | j.manning@f5.com | 703-898-4135 |
| | | AE / West | Archie Newell | a.newell@f5.com | 858-922-2654 |
| | | SE /East | Paul Simmons | p.simmons@f5.com | 843-300-7392 |
| | | SE / West | Jimmy Jennings | j.jennings@f5.com | 951-334-8558 |
| Pentagon<br>Defense<br>Agencies | | AE | Mark Oldknow | m.oldknow@f5.com | 512-410-9462 |
| | | SE | August Weinerstein | a.winterstein@f5.com | 301-660-9644 |
| Army | | MAM / West | Brig Lambert | B.Lambert@f5.com | 801-319-1221 |
| | | MAM / East | Todd Favakeh | t.favakeh@f5.com | 847-334-5610 |
| | | SE /East | Shaun Simmons | s.simmons@f5.com | 412-329-8366 |
| | | SE / West | Michael Slavinsky | M.Slavinsky@f5.com | 206-637-2056 |

# F5 DoD Virtual User Group (DoDVUG) Schedule

| Date | Title | F5 DoDVUG Topic |
|---|---|---|
| **Apr 9th** Thursday@ 1500 | F5 DoD Virtual User Group #1 | F5 Access Policy Manager with remote access, network tunneling, and CAC/PIV Authentication. |
| **April 23rd** Thursday@ 1500 | F5 DoD Virtual User Group #2 | Get Your SaaS in Gear Enterprise Application Strategy |
| **May 7th** Thursday@ 1500 | F5 DoD Virtual User Group #3 | Advanced Security - F5 ASM |
| **May 21st** Thursday@ 1500 | F5 DoD Virtual User Group #4 | Automation/Orchestration - F5 A/O Toolchain |
| **June 4th** Thursday@ 1500 | F5 DoD Virtual User Group #5 | SCCA / SACA |
| **June 18th** Thursday@ 1500 | F5 DoD Virtual User Group #6 | SSLO Orchestrator |
| **July 9th** Thursday@ 1500 | F5 DoD Virtual User Group #7 | Advanced Web Application Firewall (AWAF) and App Protect |
| **July 30th** Thursday@ 1500 | F5 DoD Virtual User Group #8 | How To Series – Preso & Hands on Lab – Cooking with iRules |
| **August 20th** Thursday@ 1500 | F5 DoD Virtual User Group #9 | How To Series – Preso & Hands on Lab – Cloud |
| **September 17th** Thursday@ 1500 | F5 DoD Virtual User Group #10 | How To Series – Preso & Hands on Lab – SSL Essentials |
| **October 15th** Thursday@ 1500 | F5 DoD Virtual User Group #10 | How To Series – Preso & Hands on Lab – TBD |