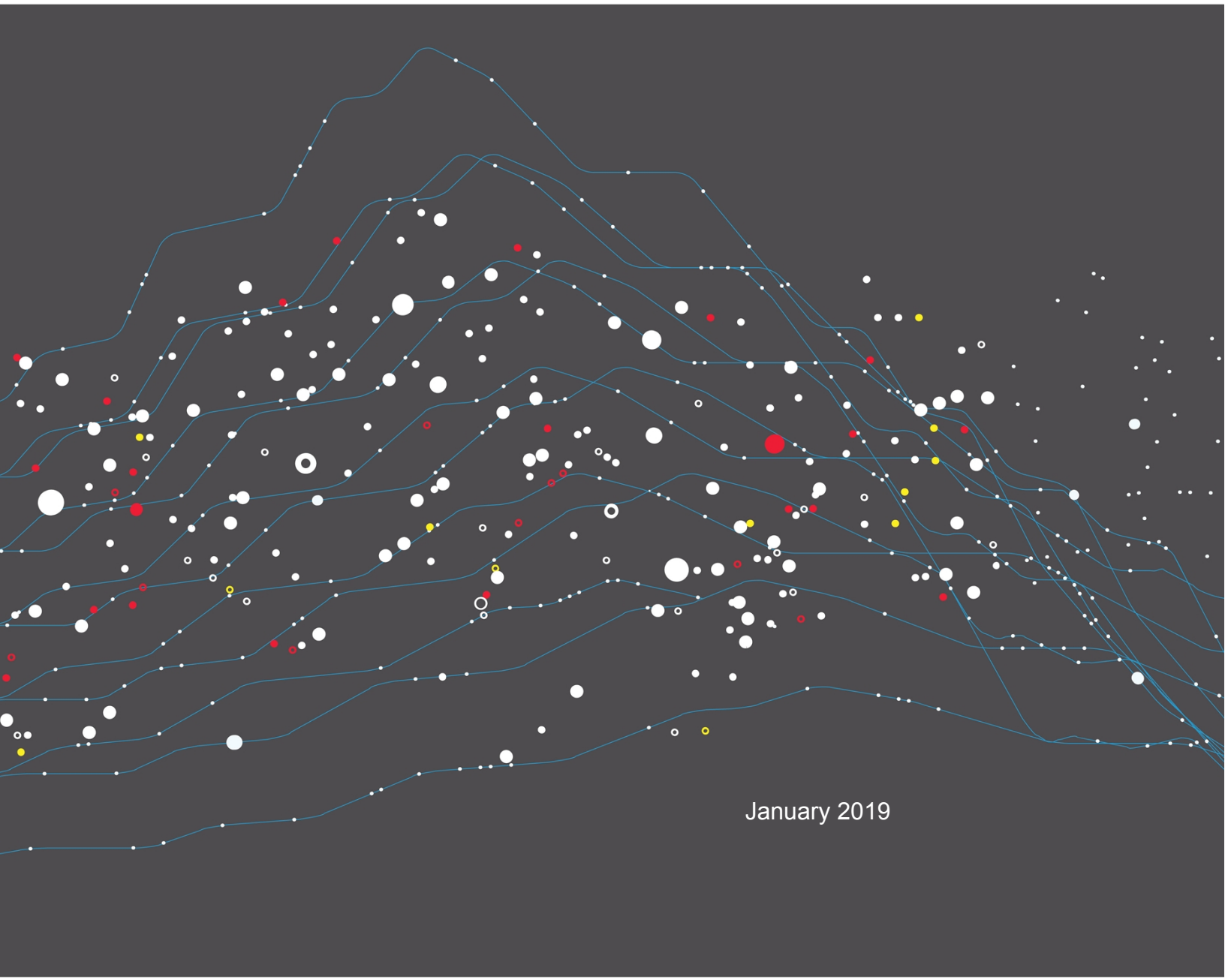
RECOMMENDED PRACTICES GUIDE

F5 SSL Orchestrator and FireEye NX: SSL Visibility with Service Chaining



January 2019

Contents

Introduction

SSL/TLS has been widely adopted by organizations to secure IP communications. While SSL provides data privacy and secure communications, it also creates challenges to security infrastructure components. In short, the encrypted communications cannot be seen like clear text and thus are passed through without inspection, rendering any defense-in-depth security architecture ineffective. This creates significant risks to businesses: What if attackers are hiding malware inside the encrypted traffic?

Today's security devices, such as intrusion prevention systems (IPSs) and next-generation firewalls (NGFWs), lack the processing power to easily decrypt SSL/TLS traffic, especially given the demands of 2048-bit certificates. The processing capacity of these security devices is further reduced when they are deployed inline, taking not only the interesting traffic that needs to be inspected, but all the wire traffic. Deploying these devices in monitoring mode conserves system resources, but at a cost: They alert administrators to threats but do not block them.

An integrated F5 and FireEye solution solves these two SSL/TSL challenges. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and the stages of an attack life cycle. Meanwhile, F5® SSL Orchestrator™ centralizes SSL inspection across complex security architectures, providing flexible deployment options to decrypt and re-encrypt user traffic. It also provides intelligent traffic orchestration using dynamic service chaining and policy-based management. The decrypted traffic is then inspected by one or more FireEye NX devices, which can prevent previously hidden threats and block zero-day web exploits. This solution eliminates the blind spots introduced by SSL and closes any opportunity for adversaries.

This overview of the joint solution discusses different deployment modes with reference to service chain architectures, recommended practices, and guidance on how to handle enforcement of corporate Internet use policies.

The integrated F5 and FireEye solution

The integrated F5 and FireEye advanced threat protection solution enables organizations to intelligently manage SSL while providing visibility into a key threat vector that attackers often use to exploit vulnerabilities, establish command and control channels, and steal data. Without SSL visibility, it is impossible to identify and prevent such threats at scale.

Key highlights of the joint solution include:

- **Flexible deployment modes** that easily:
  - Integrate into even the most complex architectures.
  - Consolidate the security stack to reduce complexity.
  - Deliver SSL visibility across the security infrastructure.
- **Centralized SSL decryption/re-encryption** with best-in-class SSL hardware acceleration, eliminating the processing burden of multiple decryption/re-encryption workloads on every security inspection hop in the stack. This reduces latency while improving the user experience.

- **Dynamic security service chaining**, which provides policy-based traffic management and determines whether traffic should be allowed to pass or be decrypted and sent through a security device or service.
- **An industry-leading application delivery controller** that load balances traffic to multiple devices in the security services, enabling effortless scaling and growth.
- **Built-in health monitors** that detect security service failures and shifts or bypasses loads in real time to provide reliability and fault tolerance.
- **Full cipher support,** including support for perfect forward secrecy (PFS)-enabled ciphers, to ensure full traffic visibility.
- **Right-sizing of the security infrastructure,** sending only appropriate traffic through security controls via service chains and URL filtering.
- **Coordinated support** from FireEye and F5.

Solution Overview

F5's industry-leading full proxy architecture enables SSL Orchestrator to install a decryption/clear text zone between the client and web server, creating an aggregation (and, conversely, disaggregation) visibility point for security services. The F5 system establishes two independent SSL connections—one with the client and the other with the web server. When a client initiates an HTTPS connection to the web server, the F5 system intercepts and decrypts the client-encrypted traffic and steers it to a pool of FireEye NX devices for inspection before re-encrypting the same traffic to the web server. The return HTTPS response from the web server to the client is likewise intercepted and decrypted for inspection before being sent on to the client.

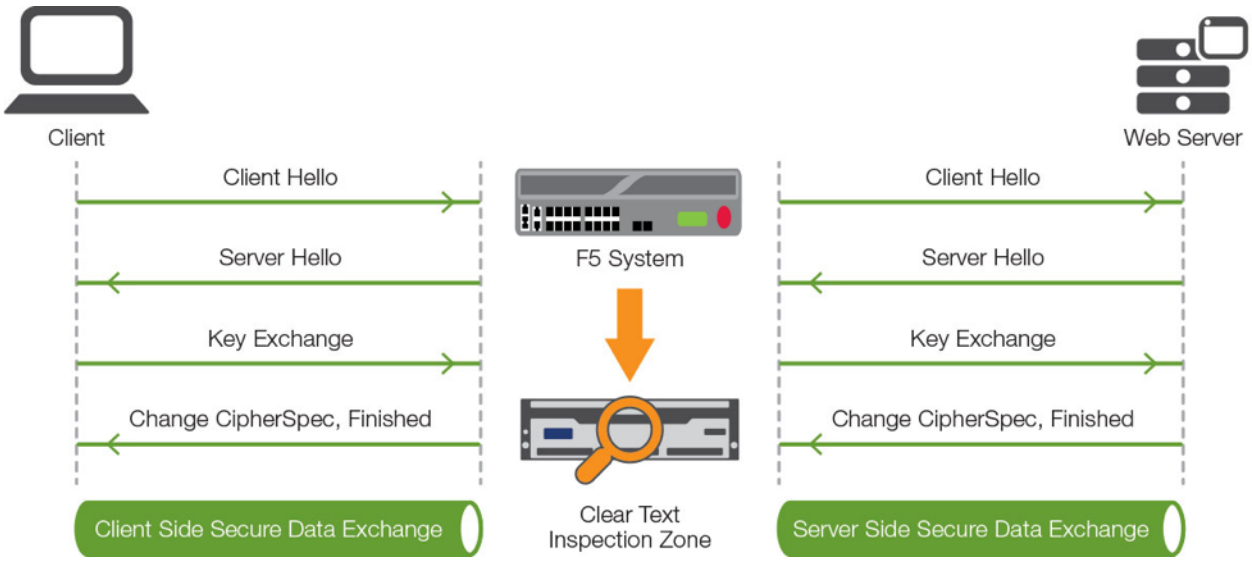


Figure 1: The F5 full proxy architecture

Dynamic service chaining

A typical security stack often consists of more than advanced anti-malware protection systems, with additional components such as a firewall, intrusion detection or prevention systems (IDS/IPS), web application firewalls, malware analysis tools, and more. To solve specific security challenges, administrators are accustomed to manually chaining these point security products. In this model, all user sessions are provided the same level of security, as this “daisy chain” of services is hard-wired.

F5 SSL Orchestrator not only decrypts the encrypted traffic, it also load balances, monitors, and dynamically chains security services, including next-generation firewalls, DLPs, IDS/IPSs, web application firewalls, and anti-virus/anti-malware systems. It does this by matching user-defined policies, which determine what to intercept and whether to send data to one set of security services or another based on context. This policy-based traffic steering enables better utilization of existing security investments and helps reduce administrative costs.

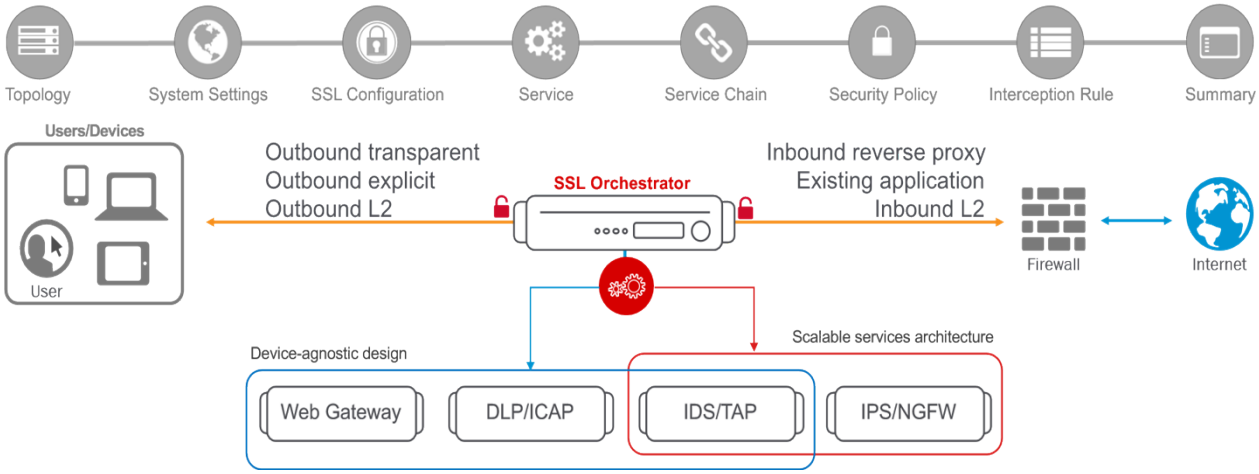


Figure 2: A service chain

SSL Orchestrator’s powerful classification engine applies different service chains based on context derived from:

- Source IP/subnet.
- Destination IP/subnet.
- An F5® IP Intelligence category subscription.
- IP geolocation.
- Host and domain name.
- An F5 URL filtering category subscription.
- Destination port.
- Protocol.

Topologies

Different environments call for different network implementations. While some can easily support SSL visibility at layer 3 (routed), others may require these devices to be inserted at layer 2. SSL Orchestrator can support all these networking requirements with the following topology options:

- Outbound transparent proxy
- Outbound explicit proxy
- Outbound layer 2
- Inbound reverse proxy
- Inbound layer 2
- Existing application

License components

The F5 SSL Orchestrator product line—the i2800, i5800, i10800, i11800, i15800, and Virtual Edition High Performance (HP)—supports this joint solution. SSL Orchestrator devices ship with an installed base module that provides both SSL interception and service chaining capabilities. Please contact your local F5 representative to further understand the licensing and deployment options.

Unless otherwise noted, references to SSL Orchestrator and the F5® BIG-IP® system in this document (and some user interfaces) apply equally regardless of the F5 hardware used. The solution architecture and configuration are identical.

Optionally, customers can add the functionality of:

- **An F5 URL filtering (URLF) subscription** to access the URL category database.
- **An F5 IP Intelligence subscription** for IP reputation service.
    - **A network hardware security module (HSM)** to safeguard and manage digital keys for strong authentication.
- **F5® Secure Web Gateway (SWG) Services** to filter and control outbound web traffic using a URL database.
- **F5® BIG-IP® Access Policy Manager® (APM)** to authenticate and manage user access.
- **A BIG-IP® Local Traffic Manager™ (LTM) add-on software license mode.** This solution is supported on all F5 BIG-IP iSeries and older F5 hardware platforms with no specific restrictions on additional F5 software modules (including the software services listed above). This option is suited for environments that need to deploy SSL Orchestrator on an existing BIG-IP device or have other functions that must run on the same device.

To deploy the joint solution, the FireEye component must first be installed. FireEye NX supports inline (L2) mode as well as TAP mode operations. Refer to the FireEye technical documentation for complete guidance.

Sizing

The main advantage of deploying SSL Orchestrator in the corporate security architecture is that wire traffic now can be classified either as “interesting” traffic, which needs to be decrypted by SSL Orchestrator for inspection by FireEye NX, or “uninteresting” traffic, which is allowed to pass through or be processed differently according to other corporate policy requirements. This selective steering of only the interesting traffic to FireEye NX conserves its valuable resources (as it need not inspect all wire traffic), maximizing performance.

As a result, it is important to consider the entire wire traffic volume to calculate the appropriate F5 device size. The FireEye NX system will require two interfaces on the F5 systems (or one 802.1q VLAN tagged interface) to allow traffic flow through logical inbound and outbound service interfaces.

Refer to the SSL Orchestrator Datasheet and consider the following factors when sizing the F5 system for the integrated solution:

- Port density
- SSL bulk encryption throughput
- System resources
- The number of security services and devices in the service chain(s)

Traffic exemptions for SSL inspection

As noted, the F5 system can be configured to distinguish between interesting and uninteresting traffic for the purposes of security processing. Examples of uninteresting traffic (including those types that cannot be decrypted) that may be exempted from inspection include:

- Guest VLANs.
- Applications that use pinned certificates.
- Trusted software update sources like those for Microsoft Windows.
- Trusted backup solutions, such as a crash plan.
- Any lateral encrypted traffic to internal services.

Administrators can also exempt traffic based on domain names and URL categories. The policy rules of the F5 SSL Orchestrator system enable administrators to enforce corporate Internet use policies, preserve privacy, and meet regulatory compliance.

Traffic exemptions based on URL category might include bypasses (and thus no decryption) for traffic from known sources of these types of traffic:

- Financial
- Health care
- Government services

Best Practices for the Joint Solution

A number of best practices can help optimize the performance and reliability, as well as the security, of the joint solution.

Architecture best practices

To ensure a streamlined architecture, F5 recommendations include:

- Deploy inline. Any SSL visibility solution must be inline to the traffic flow to decrypt PFS cipher suites such as ECDHE (elliptic curve Diffie-Hellman encryption).
- Deploy SSL Orchestrator in a device sync/failover device group (S/FDG) that includes the high-availability (HA) pair with a floating IP address.
- Use dual-homing. The FireEye NX devices must be dual-homed on the inward and outward VLANs with each F5 system in the device S/FDG.
- Achieve further interface redundancy with the Link Aggregation Control Protocol (LACP). LACP manages the connected physical interfaces as a single virtual interface (aggregate group) and detects any interface failures within the group.

Security best practices

SSL orchestration generally presents a new paradigm in the typical network architecture. Previously, client/server traffic passed encrypted to inline security services, which then had to perform their own decryption if they needed to inspect that traffic. When SSL Orchestrator is integrated into the security architecture, *all* traffic bound for a security device is decrypted—including user names, passwords, social security and credit card numbers, etc. It is therefore highly recommended that organizations isolate security services within a private, protected enclave defined by SSL Orchestrator.

It is technically possible to configure SSL Orchestrator to send the decrypted traffic anywhere that can be reached by the routing setup, but this is a high-risk practice that should be avoided.

Certificate requirements

Different certificate requirements apply depending on the direction of traffic flow.

Outbound traffic flow (internal client to Internet)

An SSL certificate and associated private key—preferably a subordinate certificate authority (CA)—on the F5 system are needed to issue certificates to the end host for client-requested external resources that are being intercepted. To ensure that clients on the corporate network do not encounter certificate errors when accessing SSL-enabled websites from their browsers, this issuing certificate must be locally trusted in the client environment.

Inbound traffic flow (Internet users to internal applications)

Inbound SSL orchestration is similar to traditional reverse web proxy SSL handling. At minimum, it requires a server

certificate and associated private key that matches the host name that external users are trying to access. This may be a single instance certificate or a wildcard or subject alternative name (SAN) certificate if inbound SSL orchestration is defined as a gateway service.

Initial Setup

Complete these initial steps before performing detailed configuration of SSL Orchestrator. When upgrading from a previous version of SSL Orchestrator, refer to the SSLO setup guide for the recovery procedure.

Configure the VLANs and self-IPs

For deployment in a layer 3 (routed or explicit proxy) topology, the F5 system must be configured with appropriate client-facing, outbound-facing VLANs plus self-IPs and routes. The VLANs define the connected interfaces, and the self-IPs define the respective IPv4 and/or IPv6 subnets. Refer to the F5 Routing Administration Guide for configuration steps to set up the VLANs and self-IPs.

Import a CA certificate and private key

For SSL orchestration in an outbound traffic topology, a local CA certificate and private key are required to re-sign the remote server certificates for local (internal) clients. For an inbound traffic topology, remote clients terminate their TLS sessions at the F5 system, so it must possess the appropriate server certificates and private keys. Refer to the F5 support article on managing SSL certificates for F5 systems to understand the procedure.

Update the SSL Orchestrator version

Periodic updates are available for SSL Orchestrator. To download the latest:

1. Visit downloads.f5.com and log in with registered F5 credentials.
2. Click **Find a Download**.
3. Scroll to the **Security** product family, select **SSL Orchestrator**, and click the link.

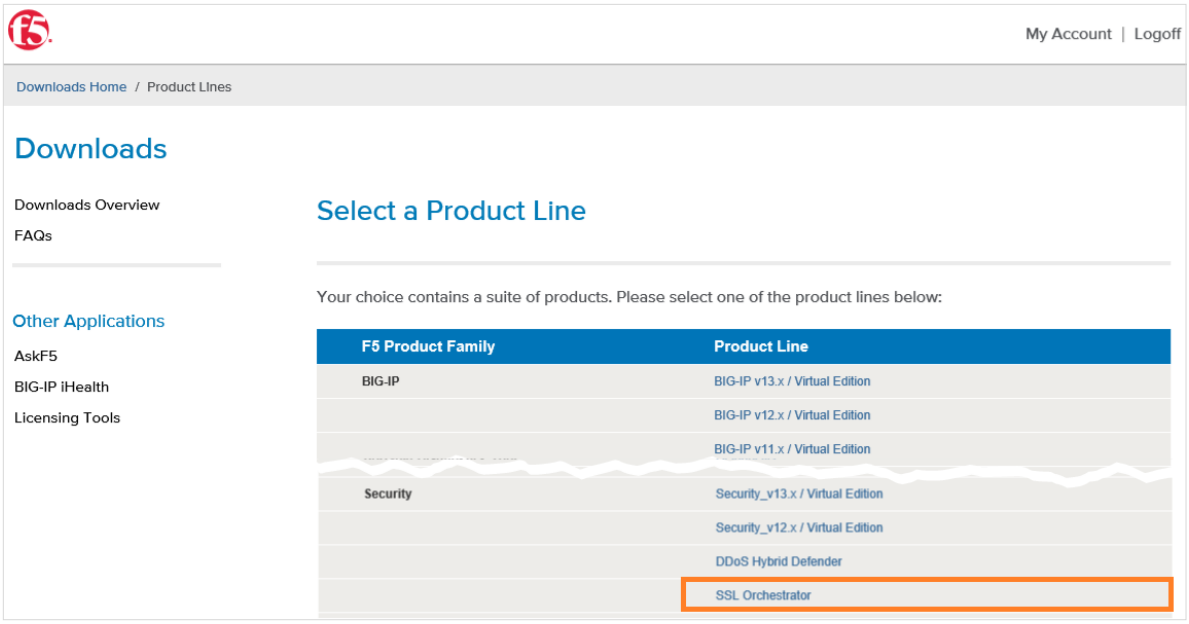


Figure 3: The F5 product download web page

4. Select and download the .rpm file for the latest version of the SSL Orchestrator.
5. Read the appropriate Release Notes before attempting to use the file.
6. Log into the F5 web UI system. On the **Main** menu, navigate to **SSL Orchestrator > Configuration** and click **Upgrade SSL Orchestrator** in the upper right.
7. Click **Choose File** and navigate to the downloaded .rpm file. Select it and click **Open**.
8. Click **Upload and Install**, then proceed to the second part of configuration, finalizing the F5 system for SSL Orchestrator.

SSL Orchestrator Configuration

A FireEye NX device can be configured as a layer 2 service or as a TAP service in SSL Orchestrator. The sample configuration below focuses on a traditional outbound (forward proxy) use case with FireEye NX configured as a L2 service. (See Figure 4.) In this use case, SSL Orchestrator steers the unencrypted and decrypted web traffic through the FireEye NX pool, which is part of one or more service chains of security devices.

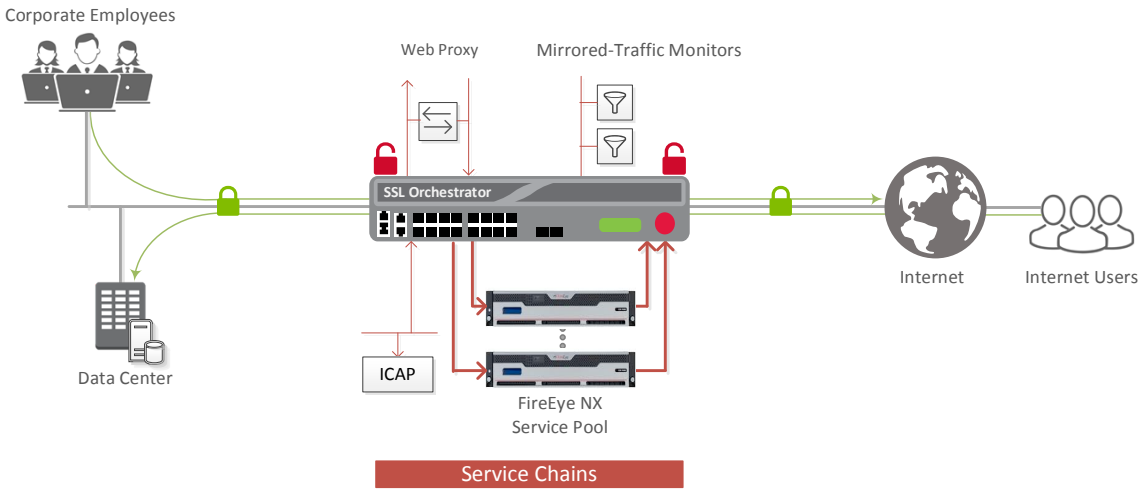


Figure 4: A sample inline deployment architecture

Guided configuration

The SSL Orchestrator 5.0 guided configuration feature presents a completely new and streamlined user experience. This workflow-based architecture provides intuitive, reentrant configuration steps tailored to a selected topology. The steps below will walk through the guided configuration to build a simple transparent forward proxy.

1. Once logged into the F5 system, on the F5 Web UI **Main** menu, click **SSL Orchestrator** > **Configuration.**
2. Take a moment to review the various configuration options.
3. (Optional.) Satisfy any of the **DNS**, **NTP** and **Route** prerequisites from this initial configuration page. Keep in mind, however, that the SSL Orchestrator guided configuration will provide an opportunity to define DNS and route settings later in the workflow. Only NTP is not addressed later.

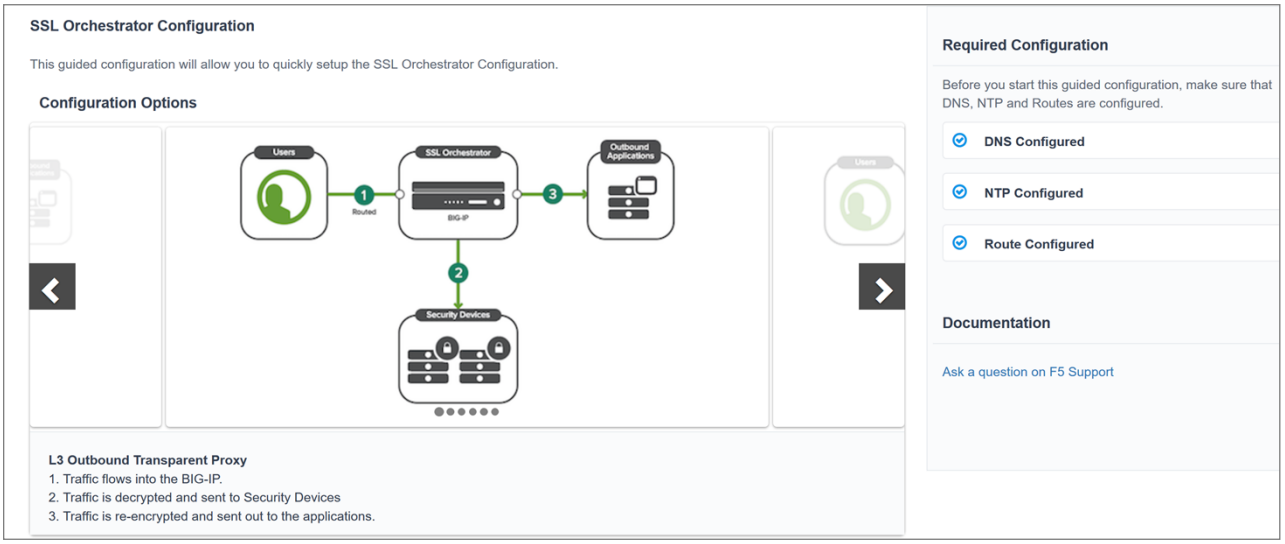


Figure 5: The initial guided configuration page

4. No other configurations are required in this section, so click **Next**.

Guided configuration workflow

The first stage of the guided configuration addresses topology.

Figure 6: The guided configuration workflow

Topology properties

1. SSL Orchestrator creates discreet configurations based on the selected topology. An explicit forward proxy topology will ultimately create an explicit proxy listener. Make appropriate selections in the **Topology Properties** section of the configuration, using the guidance below.

Topology Properties	User Input
Name	Type a **Name** for the SSL Orchestrator deployment.
Description	Type a **Description** for this SSLO deployment
Protocol	The **Protocol** option presents four protocol types: • **TCP**: Creates a single TCP wildcard interception rule for the L3 inbound, L3 outbound, and L3 explicit proxy topologies. • **UDP**: Creates a single UDP wildcard interception rule for L3 inbound and L3 outbound topologies. • **Other**: Creates a single “any protocol” wildcard interception rule for L3 inbound and L3 outbound topologies. Typically used for non-TCP/UDP traffic flows. • **Any**: Creates the TCP, UDP and non-TCP/UDP interception rules for outbound traffic flows. The sample configuration here demonstrates this option.
IP Family	Specify whether the configuration should support **IPv4** addresses or **IPv6** addresses.
SSL Orchestrator Topologies	The SSL Orchestrator Topologies option page presents six topologies: 1. **L3 Explicit Proxy**: The traditional explicit forward proxy. The sample configuration presented here uses this topology. 2. **L3 Outbound**: The traditional transparent forward proxy. 3. **L3 Inbound**: A reverse proxy configuration. 4. **L2 Inbound**: Provides a transparent path for inbound traffic flows, inserting SSL Orchestrator as a bump-in-the-wire in an existing routed path, where SSL Orchestrator presents no IP addresses on its outer edges. 5. **L2 Outbound**: Provides a transparent path for outbound traffic flows, inserting SSL Orchestrator as a bump-in-the-wire in an existing routed path, where SSL Orchestrator presents no IP addresses on its outer edges. 6. **Existing Application**: Designed to work with existing BIG-IP LTM applications that already perform their own SSL handling and client-server

	traffic management. The Existing Application workflow proceeds directly to service creation and security policy definition, then exits with an SSL Orchestrator-type access policy and per-request policy that can easily be consumed by a BIG-IP LTM virtual server. The sample configuration presented here deploys SSL Orchestrator as an L3 explicit proxy for decrypting outbound TLS/SSL traffic. See Figure 7.

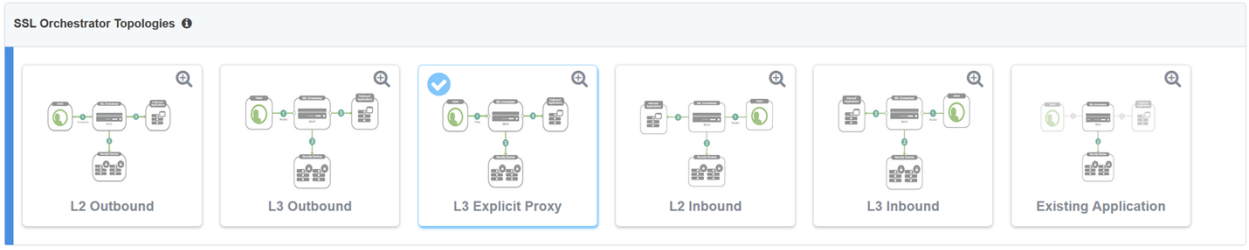


Figure 7: Sample topology configuration

2. Click **Save & Next**.

SSL configuration

This section defines the specific SSL settings for the selected topology (a forward proxy in this example) and controls both client-side and server-side SSL options. If existing SSL settings are available from a previous workflow, they can be selected and reused. Otherwise, the **SSL Configuration** section creates new SSL settings.

Figure 8: SSL configuration in the workflow

1. Click **Show Advanced Settings** on the right.
2. Make appropriate **SSL Configuration** selections using the guidance below.

SSL Configuration	User Input
SSL Profile	
Name	Enter a **Name** for the SSL profile.
Description	Enter a **Description** for this SSL profile
Client-Side SSL	
Cipher Type	The cipher type can be a **Cipher Group** or **Cipher String**. The latter is recommended. • For **Cipher Group**, select a previously-defined cipher group (which can be defined if necessary by navigating to **Local Traffic > Ciphers > Groups**). • When **Cipher String** is selected, a field will be populated with the DEFAULT option, which is optimal for most environments. (Otherwise, users could also enter a cipher string that appropriately represents the

	client-side TLS requirement.
Certificate Key Chains	The certificate key chain represents the certificate and private key used as the template for forged server certificates. While reissuing server certificates on the fly is generally easy, private key creation tends to be a CPU-intensive operation. For that reason, the underlying SSL forward proxy engine forges server certificates from a single defined private key. This setting gives administrators the opportunity to apply their own template private key and to optionally store that key in a FIPS-certified HSM for additional protection. The built-in default certificate and private key uses 2K RSA and is generated from scratch when the F5 system is installed. Select the default.crt certificate, default.key key, and default.crt chain. Leave the **Passphrase** field empty and click **Add**.
CA Certificate Key Chains	An SSL forward proxy must re-sign or forge a remote server certificate to local clients using a local CA certificate, and local clients must trust this local CA. This setting defines the local CA certificate and private key used to perform the forging operation. Specify one or more configured subordinate CA certificates and keys that were imported, then click **Add**.
Server-Side SSL	
Cipher Type	Select **Cipher String** for the default cipher list.
Ciphers	Uses the ca-bundle.crt file, which contains all well-known public CA certificates, for client-side processing.
Expired Certificate Response Control	Select whether to drop or ignore the connection even if the specified certificate response control (CRL) file has expired.
Untrusted Certificate Response Control	Select whether to drop or ignore the connection even if the specified CRL file is not trusted.
OCSP	Specify the supported **OCSP**.
CRL	Specify the supported **CRL**.

3. Click **Save & Next**.

Note: SSL settings minimally require an RSA-based template and CA certificates but can also support elliptic curve (ECDSA) certificates. In this case, SSL Orchestrator would forge an elliptic curve (EC) certificate to the client if the TLS handshake negotiated an ECDHE_ECDSA cipher. To enable EC forging support, add both an EC template certificate and key, and an EC CA certificate and key.

Create the FireEye service

The Services List section defines the security services that interact with SSL Orchestrator. The guided configuration includes a services catalog that contains common product integrations. Beneath each of these catalog options is one of the five basic service types: layer 3, layer 2, ICAP, TAP, and HTTP service.

The service catalog also provides “generic” security services. (It may be necessary to scroll down to see additional services.)

Figure 9: Service configuration

To configure the FireEye service:

1. Under **Service List**, click **Add Service**.
2. In the service catalog, double click **FireEye** service. The **Service Properties** page displays.
3. Configure the service using the guidance below.

Service Properties	User Input
Service Settings	
Name	Enter a **Name** for the FireEye service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters are not case sensitive.
Description	Enter a **Description** for the FireEye service.
Network Configuration	Click **Add**. Then create the **From VLAN** and **To VLAN** pairs (inward and outward VLANs) by selecting the interfaces. These VLAN pairs and the associated interfaces define the network connectivity from SSL Orchestrator to the inline security device. If the SSL Orchestrator systems have been configured in a sync/failover device group for HA, then the VLAN pairs must be connected to the same layer 2 virtual network from every device. If multiple FireEye devices are involved, choose the respective VLAN pair and click **Add**. Enter the desired ratio for every FireEye NX device in the pool to control the load it receives.
Service Down Action	Specify how the system should handle a failure of the L2 service or times when it is otherwise unavailable: • **Ignore:** Specifies that the traffic to the service is ignored and sent to the next service in the chain. • **Drop:** Specifies that the system initiates a close on the client connection. • **Reset:** Specifies that the system immediately sends a RST on the client connection for TCP traffic. For UDP traffic, this action is the same.

Enable Port Remap	Select **Enable Port Remap**.
Remap Port	For the FireEye NX device to recognize that the steered traffic has been decrypted, it needs to be sent on a non-443 TCP port. Select a non-443 port.
iRules	Additional iRules are not required, but SSL Orchestrator allows for the insertion of additional F5 iRules® logic at different points. An iRule defined at the service only affects traffic flowing across this service. It is important to understand, however, that these iRules must not be used to control traffic flow (for example, pools, nodes, or virtual servers), but rather should be used to view/modify application layer protocol traffic. For example, an iRule assigned here could be used to view and modify HTTP traffic flowing to/from the service. Leave this field empty to configure without iRules.

4. Click **Save** to return to the **Service List** section. To configure additional services, click **Add Service** to access the service catalog again.
5. Once all the desired services are created, click **Save & Next** to move on to service chain setup.

Configure service chains

Service chains are arbitrarily ordered lists of security devices. Based on the ecosystem's requirements, different service chains may contain different, reused sets of services, and different types of traffic can be assigned to different service chains. For example, HTTP traffic may need to go through all of the security services while non-HTTP traffic goes through a subset of those services and traffic destined to a financial service URL can bypass decryption and still flow through a smaller set of security services.

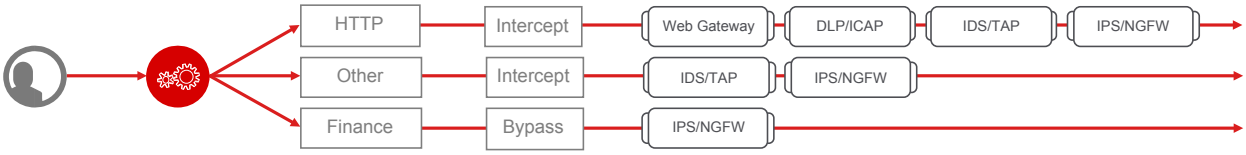


Figure 10: Different traffic flowing through chains of different security services

Each service chain is linked to service chain classifier rules and processes specific connections based on those rules, which look at protocol, source, and destination addresses. Service chains can include each of the three types of services (inline, ICAP, or receive-only), as well as decryption zones between separate ingress and egress devices.

Figure 11: Configuring service chains

To create a new service chain containing all of the configured security services needed:

1. Under **Services List**, click **Add Service**. Make selections using the guidance below.

Service Chain Properties	User Input
Name	Enter a **Name** for the per-request service chain.
Description	Provide a **Description** for this service chain
Services	Select any number of desired service from the **Services Available** list and move them into the **Selected Service Chain Order** column. Optionally, order them as required.

2. Click **Save & Next**.

Security policy

Security policies are the set of rules that govern how traffic is processed in SSL Orchestrator. The actions a rule can require include:

- Whether or not to allow the traffic indicated in the rule.
- Whether or not to decrypt that traffic.
- Which service chain (if any) to pass the traffic through.

Figure 12: Configuring security policy

SSL Orchestrator's guided configuration presents an intuitive rule-based, drag-and-drop user interface for the definition of security policies. In the background, SSL Orchestrator maintains these security policies as visual per-request policies. If traffic processing is required that exceeds the capabilities of the rule-based user interface, the underlying per-request policy can be managed directly.

1. To create a rule, click **Add**.
2. Create a security rule as required.
3. Click **Add** again to create more rules, or click **Save & Next**.

Figure 13: Configuring security policy

Interception rules

Interception rules are based on the selected topology and define the listeners (analogous to BIG-IP LTM virtual servers) that accept and process different types of traffic, such as TCP, UDP, or other. The resulting BIG-IP LTM virtual servers will bind the SSL settings, VLANs, IPs, and security policies created in the topology workflow.

Figure 14: Configuring interception rules

1. To configure the interception rule, follow the guidance below.

Intercept Rule	User Input
Label	Enter a name or **Label** for the rule.
Description	Enter a **Description** for this intercept rule.
Proxy Server Settings This setting, which displays when configuring an explicit proxy, defines the SSL Orchestrator explicit proxy listening IP address and proxy port. For explicit proxy authentication, this section also allows for the selection of a BIG-IP APM SWG-explicit access policy.	
IPv4 Address	Specify the explicit proxy listening IP address.
Port	Specify the port number.
Access profile	Specify the access policy (optional).
Ingress Network	
VLANs	This entry defines the VLANs through which traffic will enter. For a forward proxy topology (outbound), for instance, this would be the client-side VLAN (intranet).

2. Click **Save & Next**.

Egress setting

The **Egress Setting** section defines topology-specific egress characteristics.

Figure 15: Configuring egress settings

1. To configure these characteristics, follow the guidance below.

Egress Settings	User Input
Manage SNAT Settings	Define if and how source NAT (SNAT) will be used for egress traffic.
Gateways	Enter the IP address of the next hop route for traffic. For an outbound

	configuration, this is usually a next hop upstream router.

2. Once done, click **Save & Next**.

Configuration summary and deployment

The configuration summary presents an expandable list of all of the workflow-configured objects.

1. To review the details for any given setting, click the corresponding arrow icon on the far right.
2. To edit any given setting, click the corresponding pencil icon. Clicking the pencil icon will display the selected settings page in the workflow.
3. When the desired settings are defined, click **Deploy**. Upon successfully deployment of the configuration, SSL Orchestrator will display a dashboard. See Figure 16.

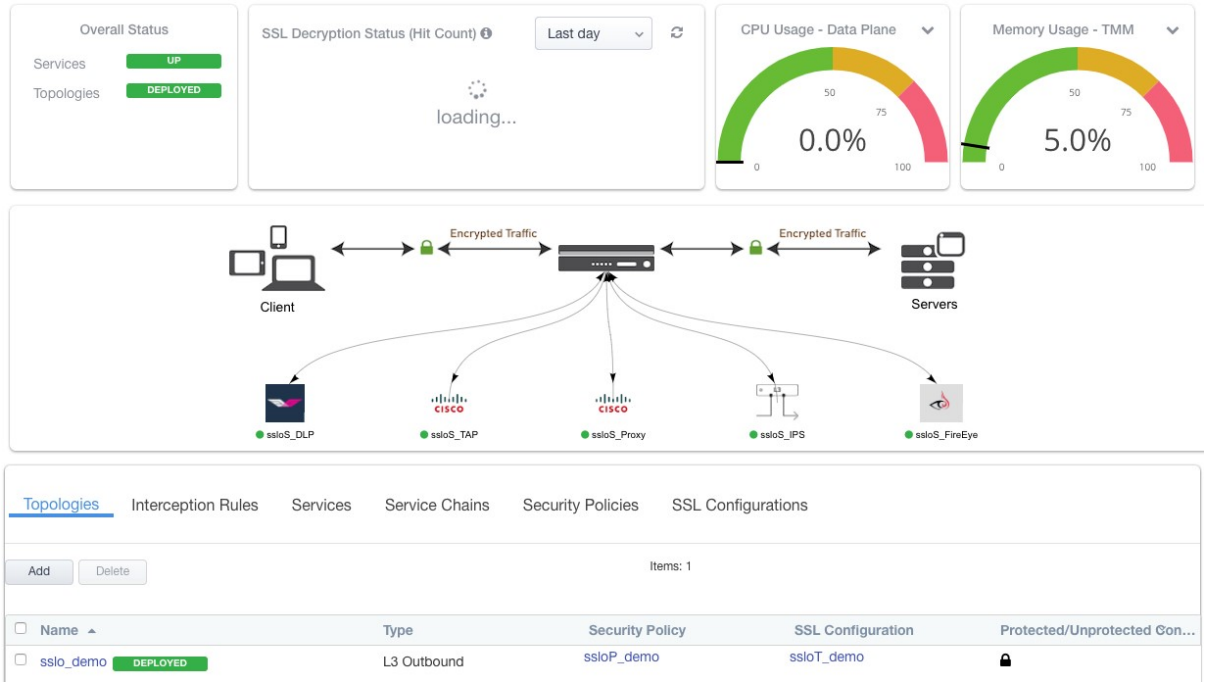
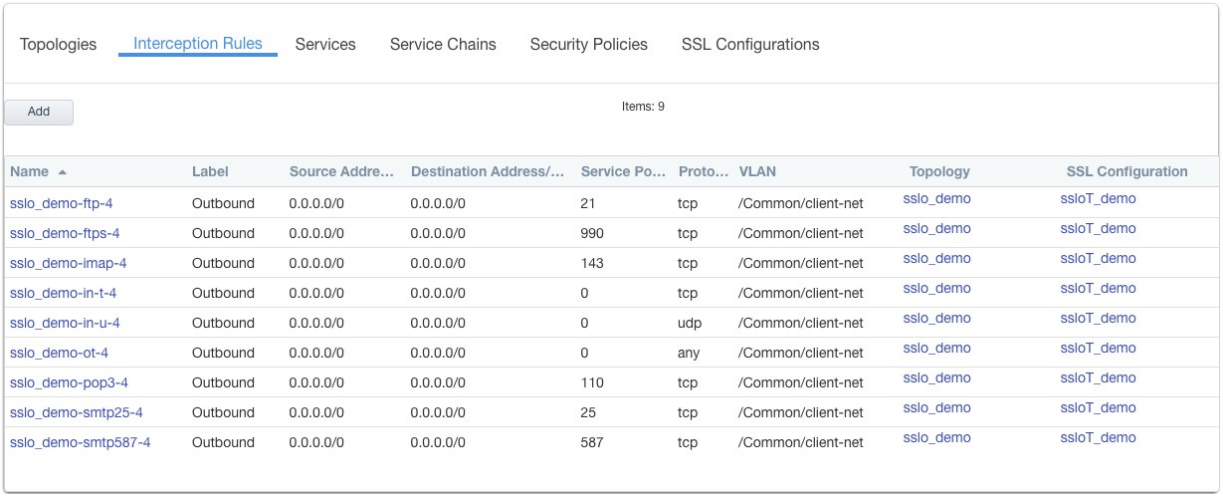


Figure 16: The configuration dashboard after deployment

4. Click the **Interception Rules** tab to display the listeners created per the selected topology.



Name	Label	Source Addre...	Destination Address/...	Service Po...	Proto...	VLAN	Topology	SSL Configuration
sslo_demo-ftp-4	Outbound	0.0.0.0/0	0.0.0.0/0	21	tcp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-ftps-4	Outbound	0.0.0.0/0	0.0.0.0/0	990	tcp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-imap-4	Outbound	0.0.0.0/0	0.0.0.0/0	143	tcp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-in-t-4	Outbound	0.0.0.0/0	0.0.0.0/0	0	tcp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-in-u-4	Outbound	0.0.0.0/0	0.0.0.0/0	0	udp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-ot-4	Outbound	0.0.0.0/0	0.0.0.0/0	0	any	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-pop3-4	Outbound	0.0.0.0/0	0.0.0.0/0	110	tcp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-smtp25-4	Outbound	0.0.0.0/0	0.0.0.0/0	25	tcp	/Common/client-net	sslo_demo	ssloT_demo
sslo_demo-smtp587-4	Outbound	0.0.0.0/0	0.0.0.0/0	587	tcp	/Common/client-net	sslo_demo	ssloT_demo

Figure 17: The dashboard's Interception Rules tab

This completes configuration of SSL Orchestrator as a forward proxy. At this point an internal client should be able to browse to external (Internet) resources, and decrypted traffic will flow across the security services.

Testing the Solution

Test the deployed solution using any one of the following three options:

- **Server certificate test:** Open a browser on the client system and navigate to an HTTPS site, for example, https://www.google.com. Once the site opens in the browser, check the server certificate of the site and verify that it has been issued by the local CA set up on the F5 system. This confirms that the SSL forward proxy functionality enabled by SSL Orchestrator is working correctly.
- **Decrypted traffic analysis on the F5 system:** Perform a TCP dump on the F5 system to observe the decrypted clear text traffic. This confirms SSL interception by the system.

```
tcpdump –lnni eth<n> -Xs0
```

- **FireEye deployment test:** Using the FireEye web interface, log in to the FireEye NX GUI and click About, and then click Deployment check and perform the checks there. Note that this test will redirect the client to FireEye hosted sites to download benign traffic that will generate an alert, but it does require that traffic to pass through the appliance. (The appliance must be in the path of traffic from the Internet to the client). Additionally, some of these checks may cause a security alert, so it is important to coordinate with the organization's security team for this testing in the production network.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447
// Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com