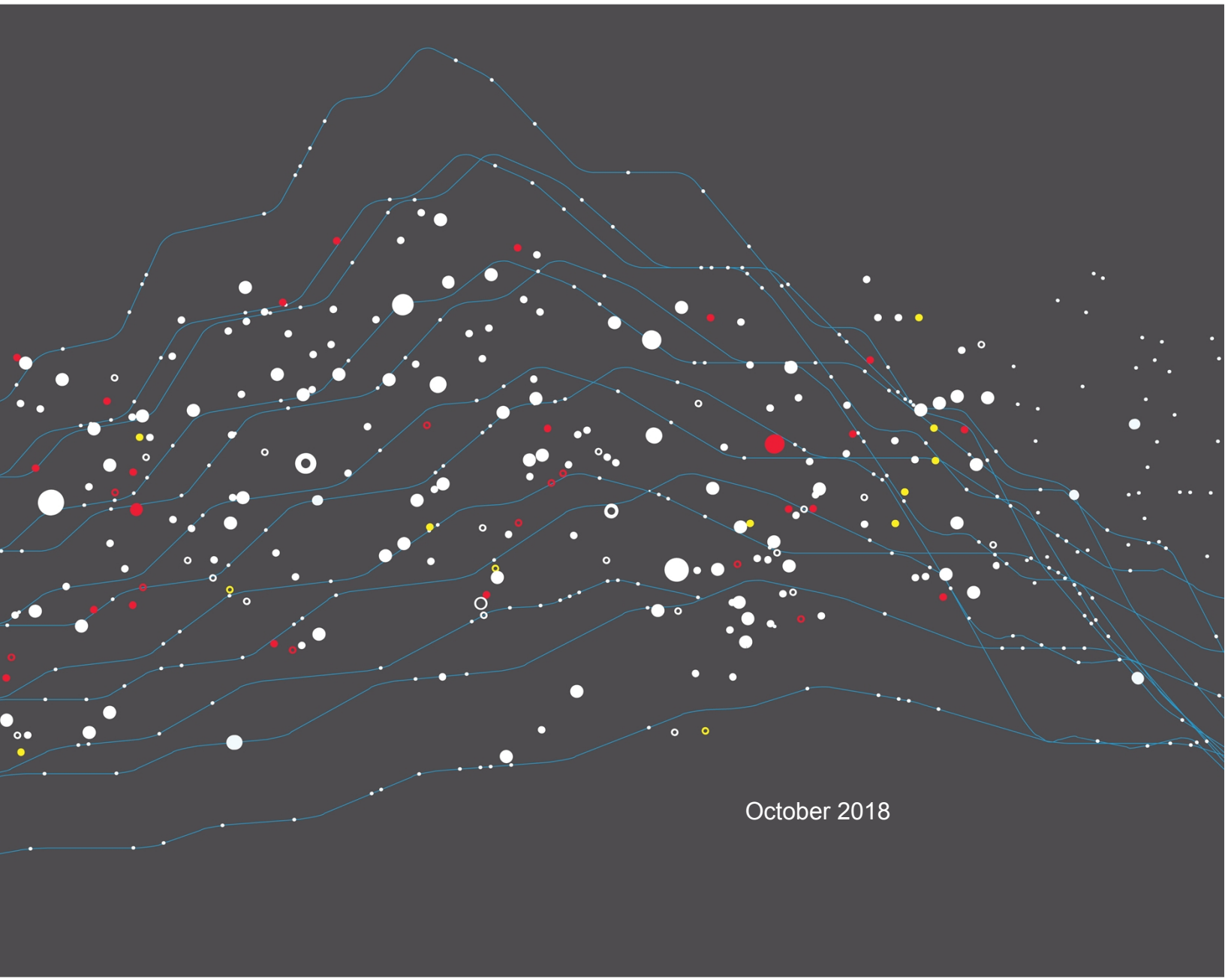
RECOMMENDED PRACTICES GUIDE

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



October 2018

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?

Security devices today, 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[1] solution solves these two SSL/TSL challenges. 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, includes 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, and 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, which reduces latency while improving the user experience.
- **Dynamic security service chaining**, which provides policy-based traffic management, determines whether traffic should be allowed to pass or be decrypted and sent through a security device or service.

[1] 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.

- **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 the 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.

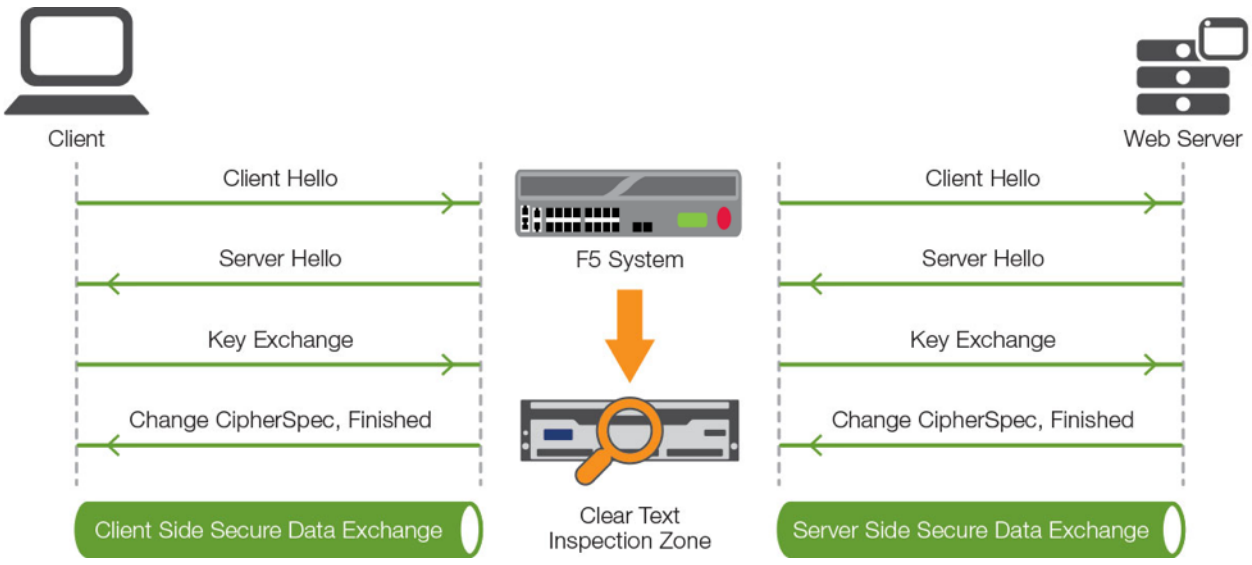


Figure 1: The F5 full proxy architecture

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.

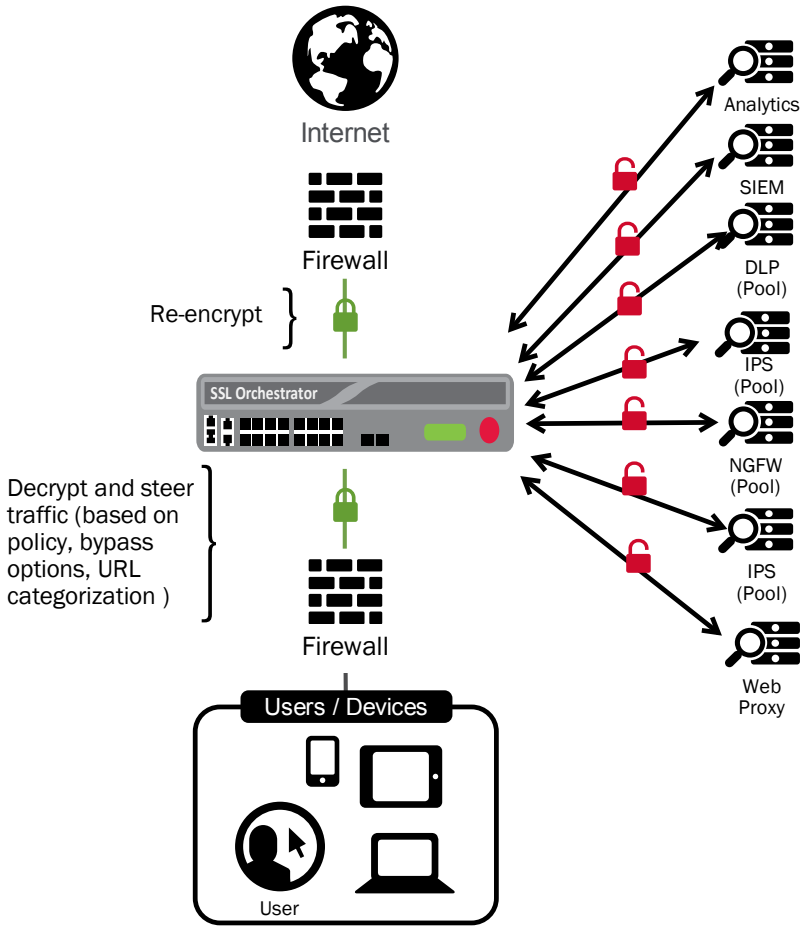


Figure 2: A service chain

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.

License components

The F5 SSL Orchestrator product line—the i2800, i5800, i10800, i11800, i15800—supports this joint solution. SSL Orchestrator devices ship with an installed base module that provides both SSL interception and service chaining capabilities. SSL Orchestrator can also be deployed as an application on an existing F5® BIG-IP® system. It supports both layer 2 (L2) wire and layer 3 (L3) network modes of operation to decrypt inbound and outbound traffic. Please contact your local F5 representative to further understand the licensing and deployment options.

Unless otherwise noted, references to SSL Orchestrator and the 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** to detect and block known bad actors and bad traffic.
- **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® Access Manager™** to authenticate and manage user access.

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

Architecture best practices

A number of best practices can help ensure a streamlined architecture that optimizes performance and reliability as well as security. 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.

Initial Setup

Complete these initial steps before performing detailed configuration of SSL Orchestrator.

Run the SSL Orchestrator Setup Wizard

After you plug in the F5 device, the first things to set up are the management IP address, netmask, and default routing from the command line of your system. Log in to the web UI using the configured management IP address (default web interface credentials are *admin/admin*). The SSL Orchestrator Setup Wizard guides you through the basic configuration. (Note: The Setup Wizard is substantially the same regardless of whether you are deploying SSL Orchestrator on an existing F5 system or new hardware. The few exceptions, such as SSL certificate configuration, can readily be performed manually on current F5 systems.)

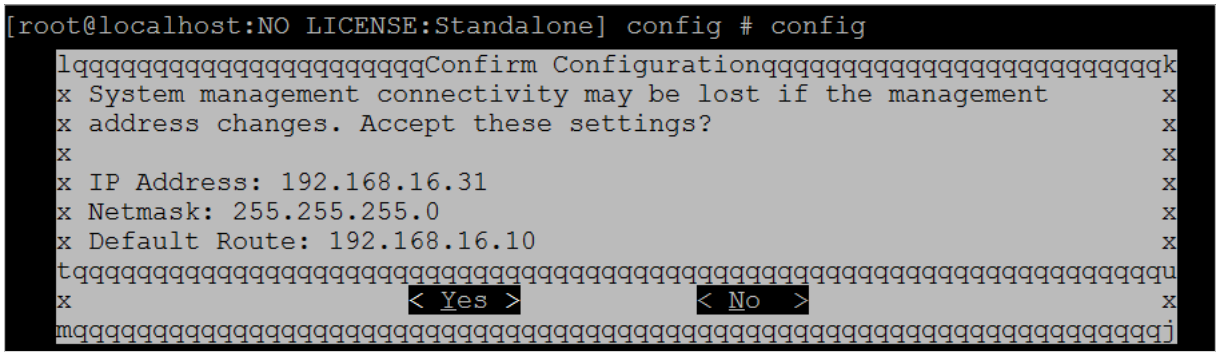


Figure 3: Initial configuration of the management IP from the command line

Note: If at any time during configuration you need to return to the Set-Up Wizard, simply click the F5 logo in the upper-left corner of the Configuration utility, and on the Welcome screen, click **Run the Setup Utility**.

1. On the F5 Welcome screen, click **Next**.
2. On the **License** screen, click **Activate**.
3. Enter the Registration Key. Follow the F5 Licensing steps to activate the SSLO license.
4. On the **EULA** screen, click **Accept**. The license activates and the system reboots.
5. Once the system has rebooted, the **Device Certificates** screen displays. Import a certificate authority (CA) signed device certificate, or you can continue using the default self-signed certificate. Click **Next**.
6. The **Platform** screen displays. Complete the following steps:
    i. Enter the **Host Name** for this system. The **Host Name** must be a fully qualified domain name.

ii. Under **User Administration**, enter and confirm the **Root Account** passwords, and click **Next**. The Root Account provides access to the command line, while the Admin Account accesses the user interface.

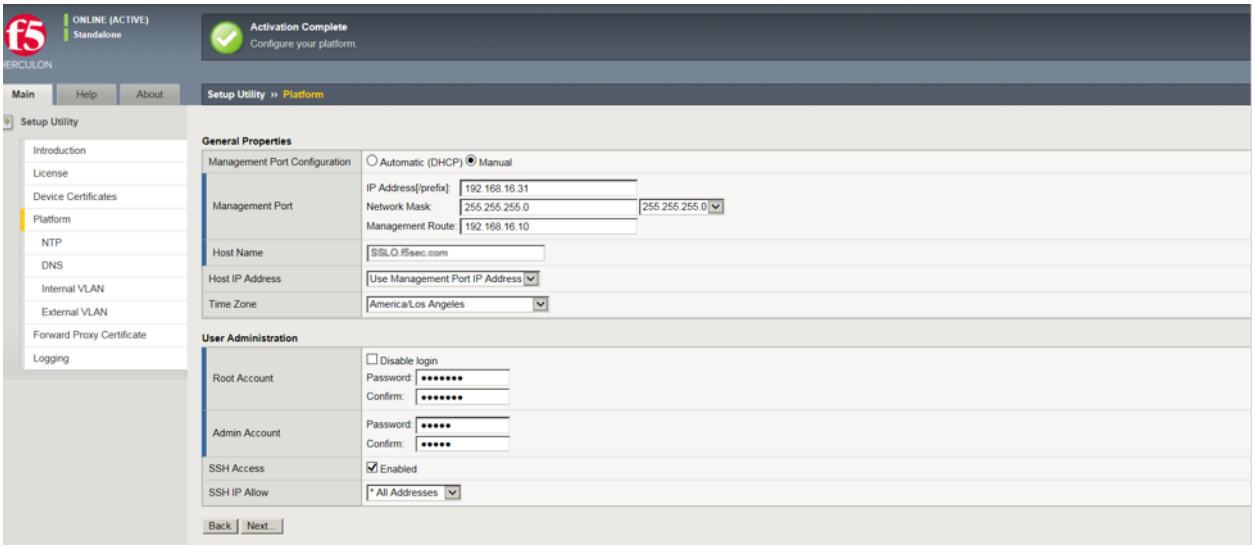


Figure 4: Platform configuration

7. The system notifies you to log out and then log back in with your username (*admin*) and new password. Click **OK**. The system reboots.
8. Log in. The **Forward Proxy** certificate page displays. An SSL CA certificate—preferably a subordinate CA—and private key on the F5 system are needed to generate and issue certificates to the end host for client-requested HTTPS websites that are being intercepted. Enter the name for the certificate and import the sub CA certificate and **Key**, then click **Next**.
9. On the **Network** web page, click **Next** to configure network settings.
10. The **Redundancy** page displays. Deselect **Config sync** and click **Next**. (You will set up high availability [HA] after finishing the initial steps.)
11. When the **Network Time Protocol** (NTP) configuration screen displays, enter the IP **Address** of the NTP server to synchronize the system clock with, and click **Add**. Click **Next**.
12. (Optional, unless you plan to later use the DNSSEC option in the SSL Orchestrator configuration—in which case this step is required.) The **Domain Name Server** (DNS) screen opens. Complete the following steps:
    i. To resolve host names on the system, set up the DNS and associated servers: For the **DNS Lookup Server List**, type the **IP Address** of the DNS server and click **Add**.
    ii. If you use BIND servers, add them in the **BIND Forwarder Server** list.
    iii. Add local domain lookups (to resolve local host names) in the **DNS Search Domain** list.
13. Click **Next**. The configuration screen appears with a complete menu on the left. (See Figure 5.) You are ready to set up high availability and finalize your system for SSL Orchestrator.

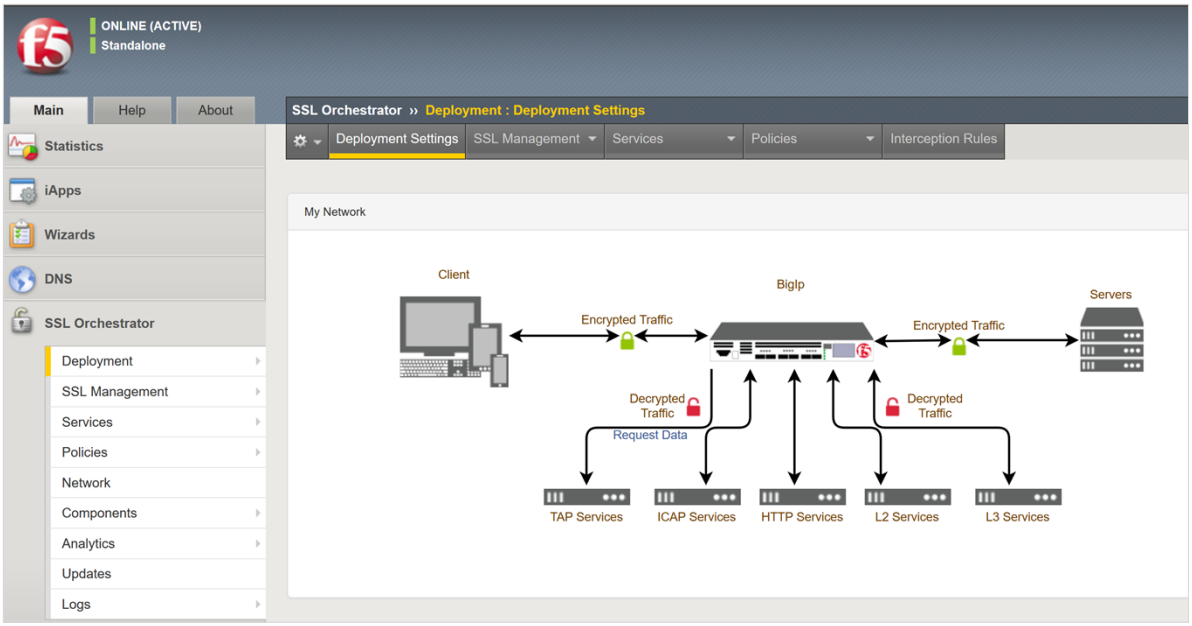


Figure 5: The SSL Orchestrator configuration screen once the initial setup is complete

Set up high availability

F5 highly recommends deploying SSL Orchestrator in an HA pair to ensure a high level of operational performance. Before setting up HA, you should already have installed the secondary SSL Orchestrator unit and completed its initial setup.

1. Click the F5 logo in the upper-left corner of the Configuration utility, and on the Welcome screen, click **Run Config Sync/HA Utility.**
2. In the **Standard Network Configuration** section, click **Next**.
3. Leave the default settings for **Redundant Device Wizard Options** and click **Next**.
4. Enter the **IP address** and add the **VLAN interface** for **High Availability Network and VLAN configuration**.
5. For **Network Time Protocol Configuration**, enter the NTP server **IP address** and click **Add**, if you didn't already configure one during initial setup. Click **Next.**
6. For **Domain Name Server Configuration**, enter the DNS server **IP address** and click **Add**, if you didn't already configure one in during initial setup. Click **Next.**
7. For **Configuration Sync Configuration**, choose the Network IP address you configured in step 4. Click **Next.**
8. For **Failover Unicast Configuration,** select the HA interface and management interface, then click **Next**.
9. For **Mirroring Configuration**, select the HA interface as the **Primary Local Mirror Address**.
10. Under **Standard Pair Configuration**, click **Next**.
11. Pause here, go to the secondary device, and complete steps 1-10 of this HA procedure for that device, too.
12. Returning to this primary device, under **Discover Configure Peer or Subordinate Device**, click **Next**.

13. Under **Retrieve Device Credentials**, enter the secondary SSL Orchestrator unit/peer **IP address**, **Administration Username** and credentials, and click **Retrieve Device Information**.
14. Once the peer **Device Certificate** is verified, click **Device Certificate Matches**.
15. Verify the Peer **Device Name** and click **Add Device**. This completes the active-standby HA setup.

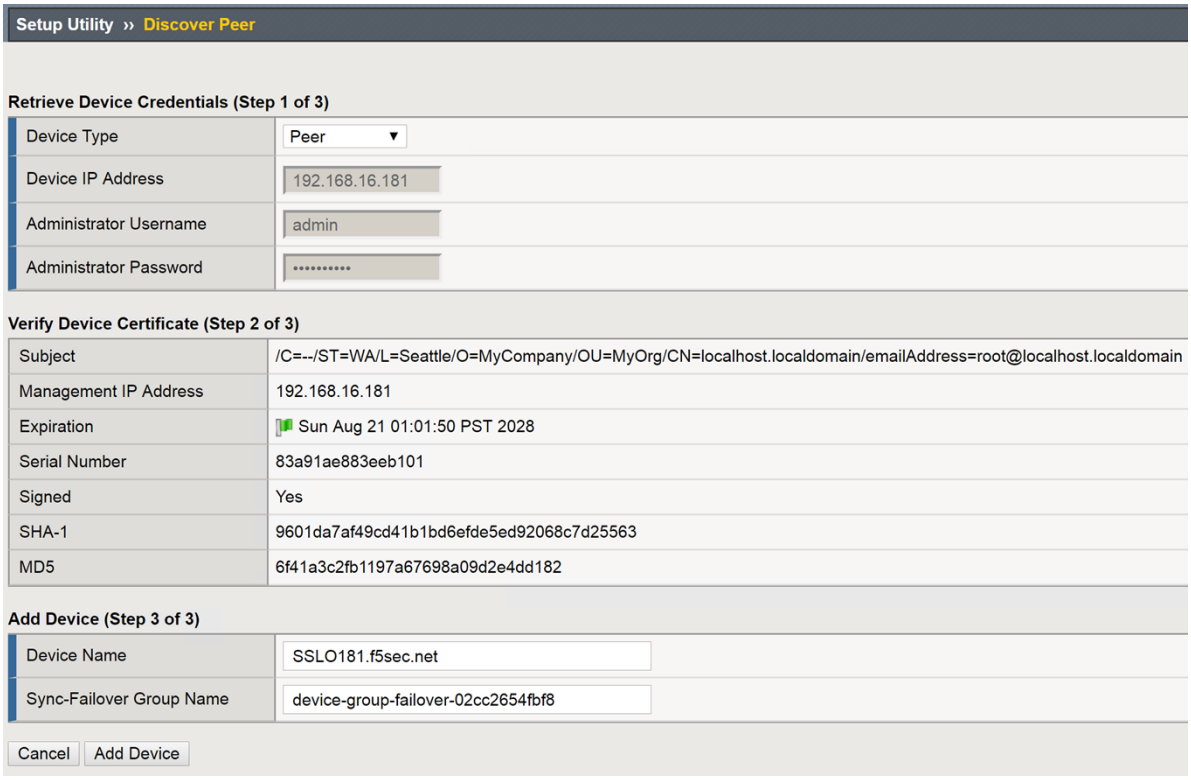


Figure 6: Sample configuration for peer discovery to setup HA

Update the SSL Orchestrator version

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

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

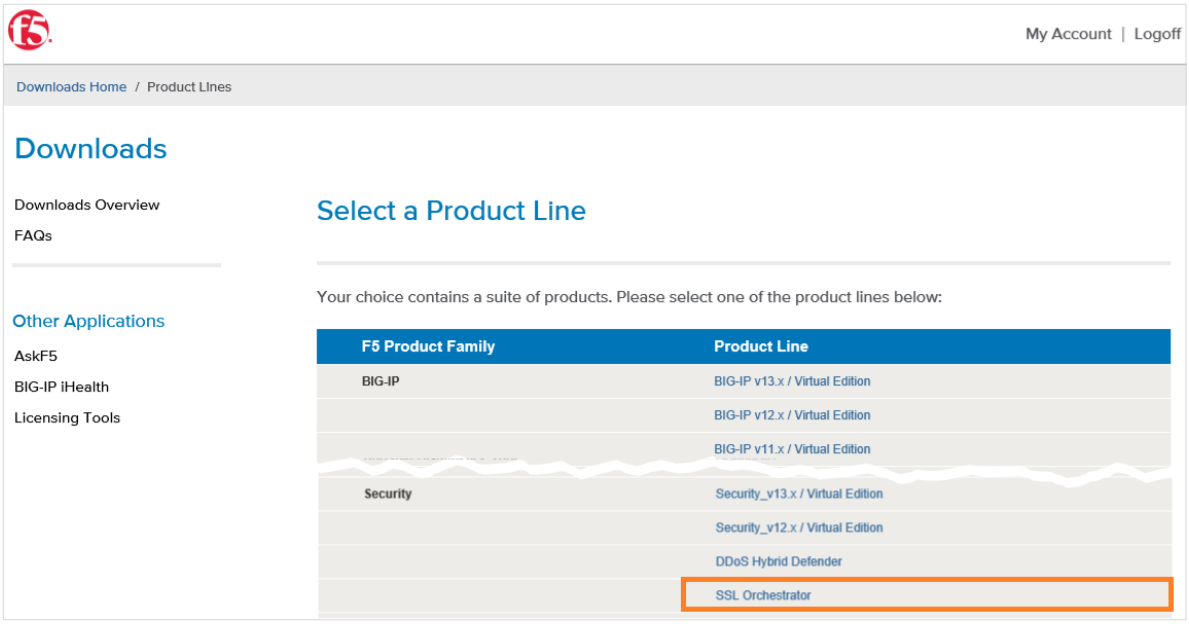


Figure 7: The F5 product download web page

4. Select and download the latest version of the SSL Orchestrator.rpm file.
5. Read the appropriate Release Notes before attempting to use the file. Then log in to the F5 management interface and navigate to **SSL Orchestrator > Updates**.
6. Under **Upgrade**, for **File Name**, click **Browse** and navigate to the .rpm file you downloaded. Select it and click **Open**.

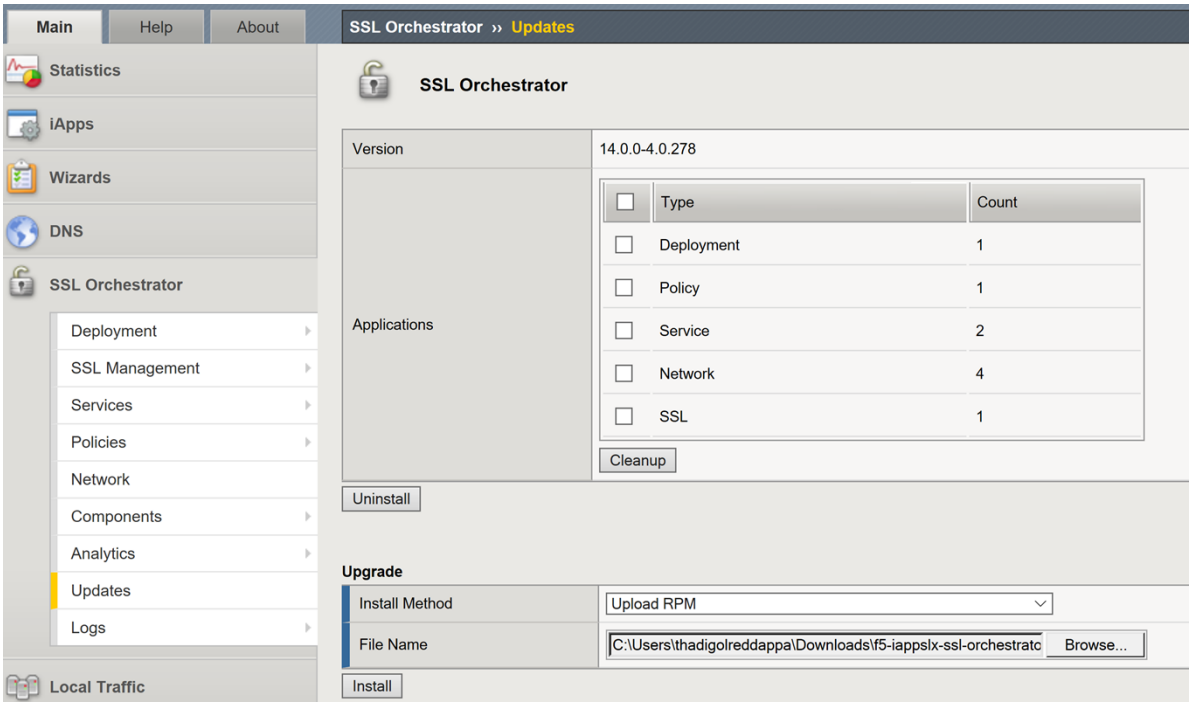


Figure 8: Updating SSL Orchestrator

7. Click **Install**. Your system may reboot to effect the change.

SSL Orchestrator Configuration

Before you proceed to deploy the SSL Orchestrator application, you must have configured the internal and external networks including VLANS, IP addresses and, default gateway. Refer to the Basic Network Setting link for the detailed steps.

Set up the deployment

This step must be completed before you can set up services and service chains.

1. On the F5 management console, click **SSL Orchestrator** > **Deployment > Deployment Settings.**
2. Answer the configuration questions (see Figure 9) to create the SSL Orchestrator application. (Refer to the User Input column below for examples and tips.) Then click **Finished**.

Configuration Field	User Input
General Properties	
Application Service Name	Type a **name** for the SSL Orchestrator deployment.
Strict Update	Select the check box if you want strict updates enforced to protect your configuration. If this is enabled, you cannot manually modify any of the settings produced by the application. Once this is disabled, you can manually change your configuration. However, we strongly recommend that you enable this setting to avoid misconfigurations that can render your application completely unusable.
Deployed Network	Specify the SSL Orchestrator deployed network as either **layer 2 (L2) Wire** or **layer 3 (L3) Network**.
IP Family	Specify whether you want this configuration to support **IPv4** addresses, **IPv6** addresses, or **both**.
Egress Configuration	
Manage SNAT Settings	Choose **Auto Map** to replace the client source IP address with the self IP address belonging to the egress for outbound traffic. This is recommended for small traffic volumes due to limitation of port numbers that can be allocated for translations. For larger volumes of traffic, F5 recommends use of a SNAT (Secure Network Address Translation) pool to scale translations instead of overloading the egress interface IP address. When **SNAT** is chosen, you will need to enter **IPv4 SNAT addresses** for the SNAT pool for translations.
Gateway	Specify whether to route outbound using the **default route** on the F5 system or enter the **IP address** to be used as the default gateway.

DNS	
DNS Query Resolution	This solution uses DNS extensively. You can either permit the system to send DNS queries directly out to **Internet Authoritative Name Server** or specify one or more **Local Forwarding Name Servers** to process all DNS queries. Direct resolution can be more reliable than using forwarders but requires outbound UDP/TCP port 53 access to the Internet.
Local Forwarding Nameserver(s)	If you selected **Local Forwarding Name Servers**, type the **IP address** of the name server(s) that will resolve all DNS queries from this solution, and click **Add**.
Local/Private Forward Zones	If you selected **Internet Authoritative Name Server,** type the **IP address** of one or more name servers and click **Add**.
DNSSec Validation	Specify whether you want to use DNSSEC to validate the DNS information.
Logging	
Logging Level	F5 recommends leaving the logging level at the default, **Errors.** Log on functional errors, unless you need to troubleshoot.

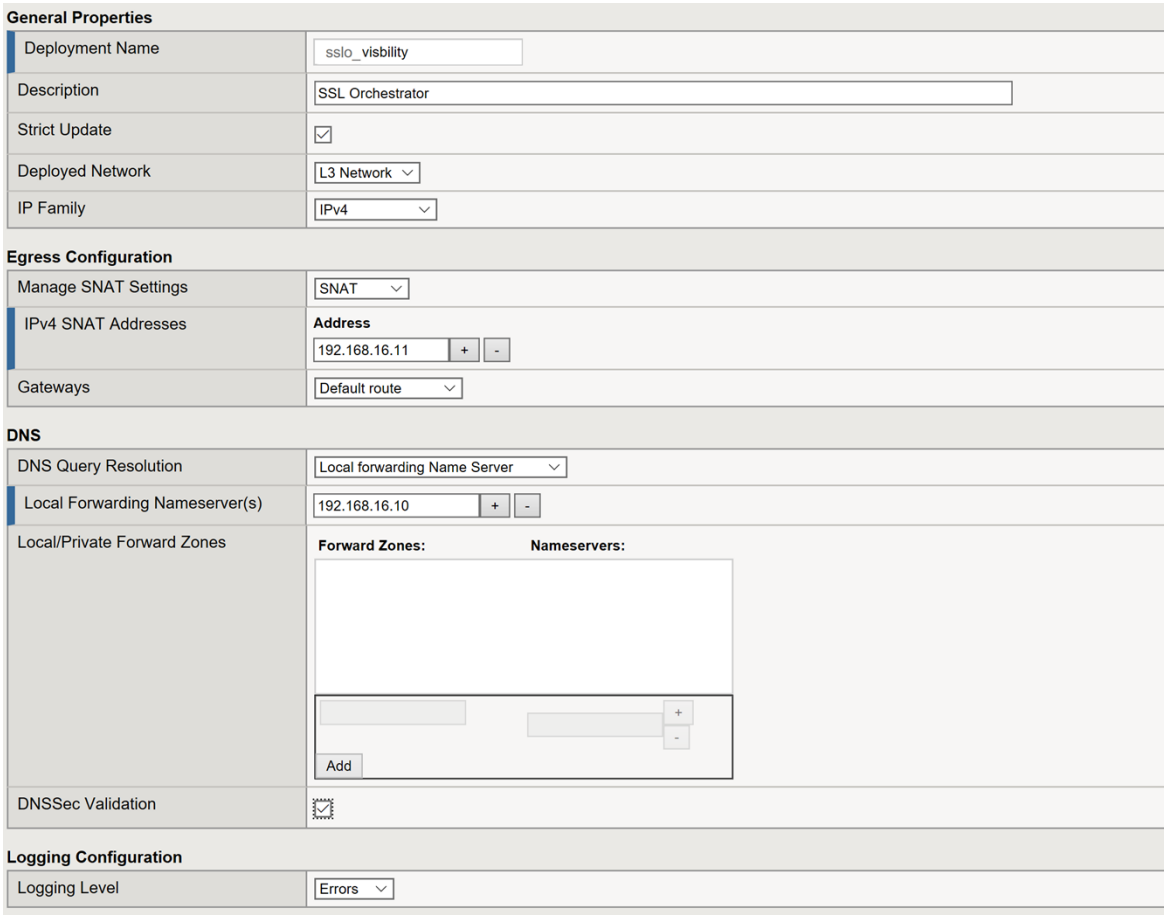


Figure 9: Sample SSL Orchestrator deployment configuration

Create the FireEye service

You can configure FireEye NX either in inline mode as an L2 service or in TAP mode.

Configuring as an L2 service

When FireEye NX is configured as a L2 service as shown in Figure 10, SSL Orchestrator steers the unencrypted and decrypted web traffic through the FireEye NX pool, which is part of the service chain(s) of security devices.

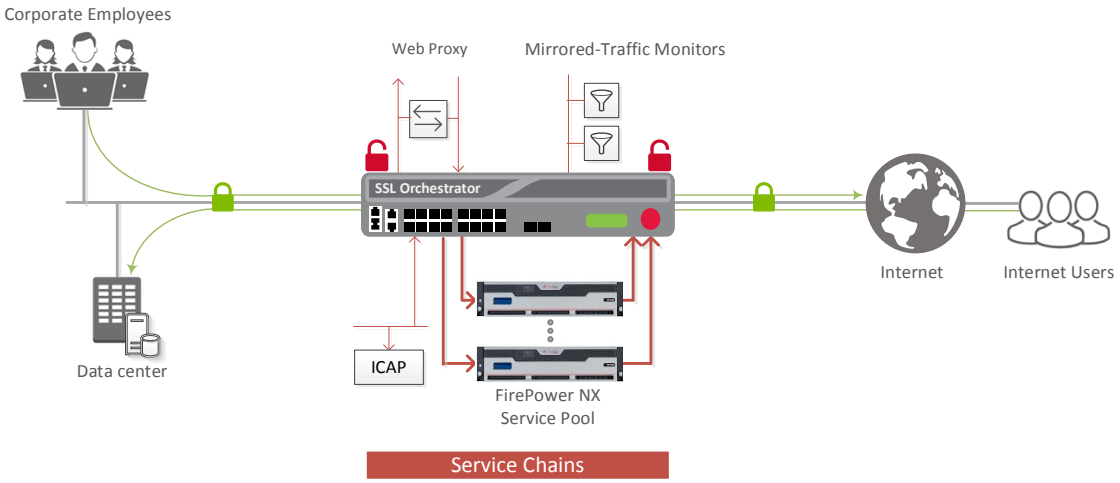


Figure 10: Sample inline deployment architecture

Before you follow the configuration steps to create the L2 service for FireEye NX, you must have created the inward and outward VLANs and assigned the interfaces on SSL Orchestrator that are connected to FireEye NX device(s).

1. On the main tab of the F5 management interface, navigate to **SSL Orchestrator** > **Services** > **L2 Services**. The L2 Services screen displays.
2. Click **Create** to create the L2 service and configure using the guidance below.
3. Click **Finished,** leaving other options at their defaults.

Configuration Field	User Input
Name	Enter a **Name** for the L2 service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters are not case sensitive.
L2 Service	
Paths	Specify the VLAN pairs (inward and outward VLAN) on the F5 device that are connected to FireEye NX. If you have configured SSL Orchestrator systems 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 you have multiple FireEye devices, choose the respective VLAN pair and click **Add**. You can enter the ratio for every FireEye NX device in the pool to control the load it receives.

Service Down Action	Specify how you want the system to 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 is 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.
Port Remap	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.

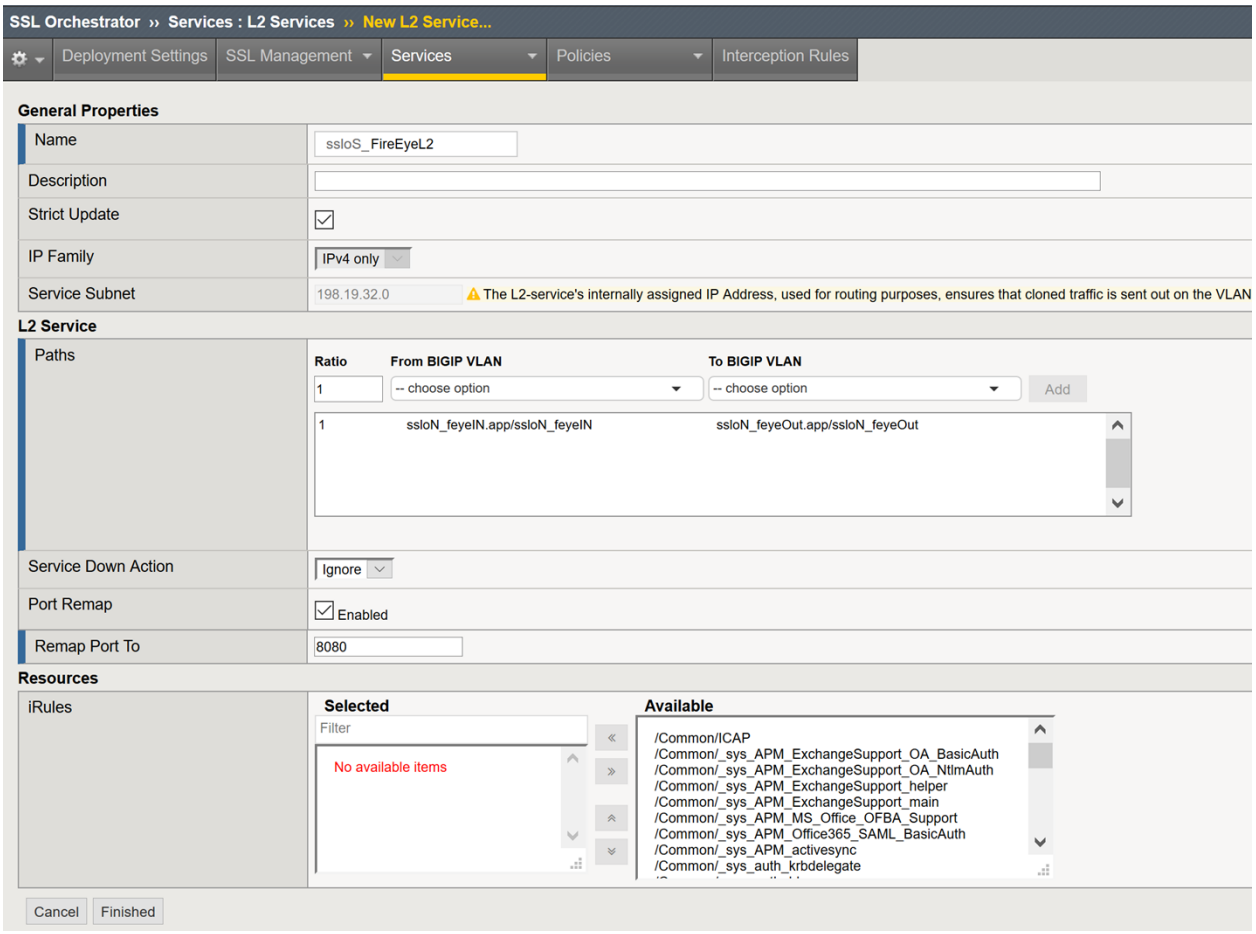


Figure 11: Sample L2 service configuration

Configuring as a TAP service

In the deployment mode shown in Figure 12, the F5 system copies the unencrypted and decrypted web traffic to the FireEye NX TAP pool, which is part of the service chain(s) of security devices.

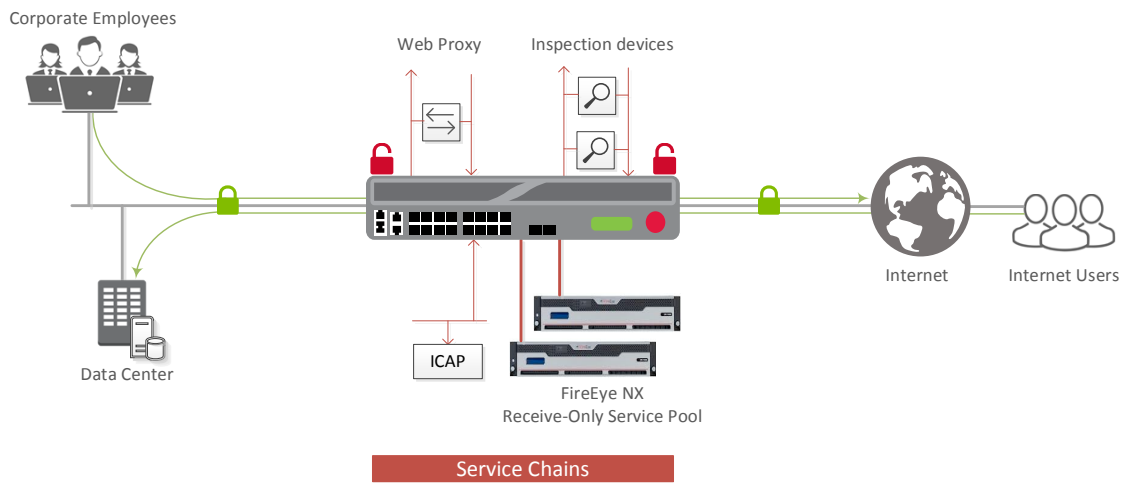


Figure 12: TAP service architecture

Before you follow these configuration steps to create the TAP service for FireEye NX, you must have created the VLAN(s) and assigned the interface(s) on SSL Orchestrator that will be used to reach the FireEye device(s).

1. On the main tab of the F5 management interface, navigate to **SSL Orchestrator** > **Services** > **TAP Services**. The TAP Services screen displays.
2. Click **Create** to create the TAP service and configure using the guidance below.
3. Click **Finished,** leaving other options at their defaults.

Configuration Field	User Input
Name	Enter a **Name** for the TAP service.
TAP Services	
MAC Address	Type the **MAC Address** of the receiving interface of the FireEye NX. This address must be reachable by an F5 VLAN.
VLAN	Specify the VLAN where the FireEye NX device resides.
Interface	Select the associated F5 system interface.
Service Down Action	Specify how you want the system to handle failure of an 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.

Port Remap	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.

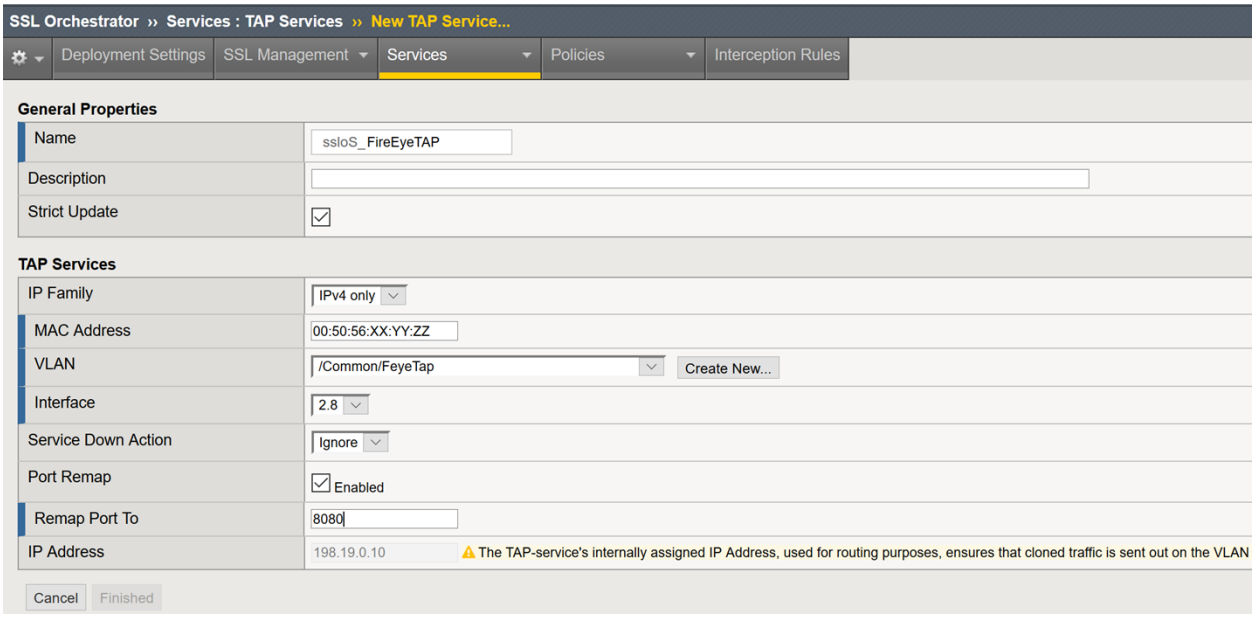


Figure 13: Sample TAP service configuration

Set up the SSL profile

An SSL CA certificate—preferably a subordinate certificate authority (CA)—and private key on the F5 system are needed to generate and issue certificates to the end host for client-requested HTTPS websites that are being intercepted. For the complete procedure, see solution K13302 on AskF5: Configuring the BIG-IP system to use an SSL chain certificate.

1. On the main tab of the F5 management interface, navigate to **SSL Orchestrator > SSL Management > SSL Settings**. The **SSL Settings Services** screen displays.
2. Click **Create** to create and configure the SSL profile using the guidance below, then click **Finished**.

Configuration Field	User Input
General Properties	
Application Service Name	Type a **Name** for the SSL profile.
Proxy Section	
Forward Proxy	Leave the enable box selected.

Bypass on Handshake Alert	Leave the default **disabled** option selected to disable SSL forward proxy bypass on receiving a handshake failure, protocol version, or unsupported extension alert message during the server-side SSL handshake.
Bypass on Client Cert Failure	Leave the default **disabled** option selected to disable SSL forward proxy bypass on failure to receive the requested client certificate.
Client-Side SSL	
Cipher Type	Select **Cipher String** for the default cipher list.
Certificate Key Chains	Select the **default.crt** certificate, **default.key** key, **default.crt** chain and leave the **Passphrase** field empty. Click **Add**.
CA Certificate Key Chains	Specify one or more configured Subordinate Certificate Authority (CA) certificates and keys to associate with the SSL profile. Select **Certificate**, **Key Chain**, and **Passphrase** settings for the certificate key chain. (If the key does not have a passphrase, leave that field blank.) 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 certificate authority (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 **drop** or **ignore** the connection even if the specified Certificate Response Control (CRL) file is not trusted.
OCSP	Specify the supported OCSP .
CRL	Specify the supported CRL.

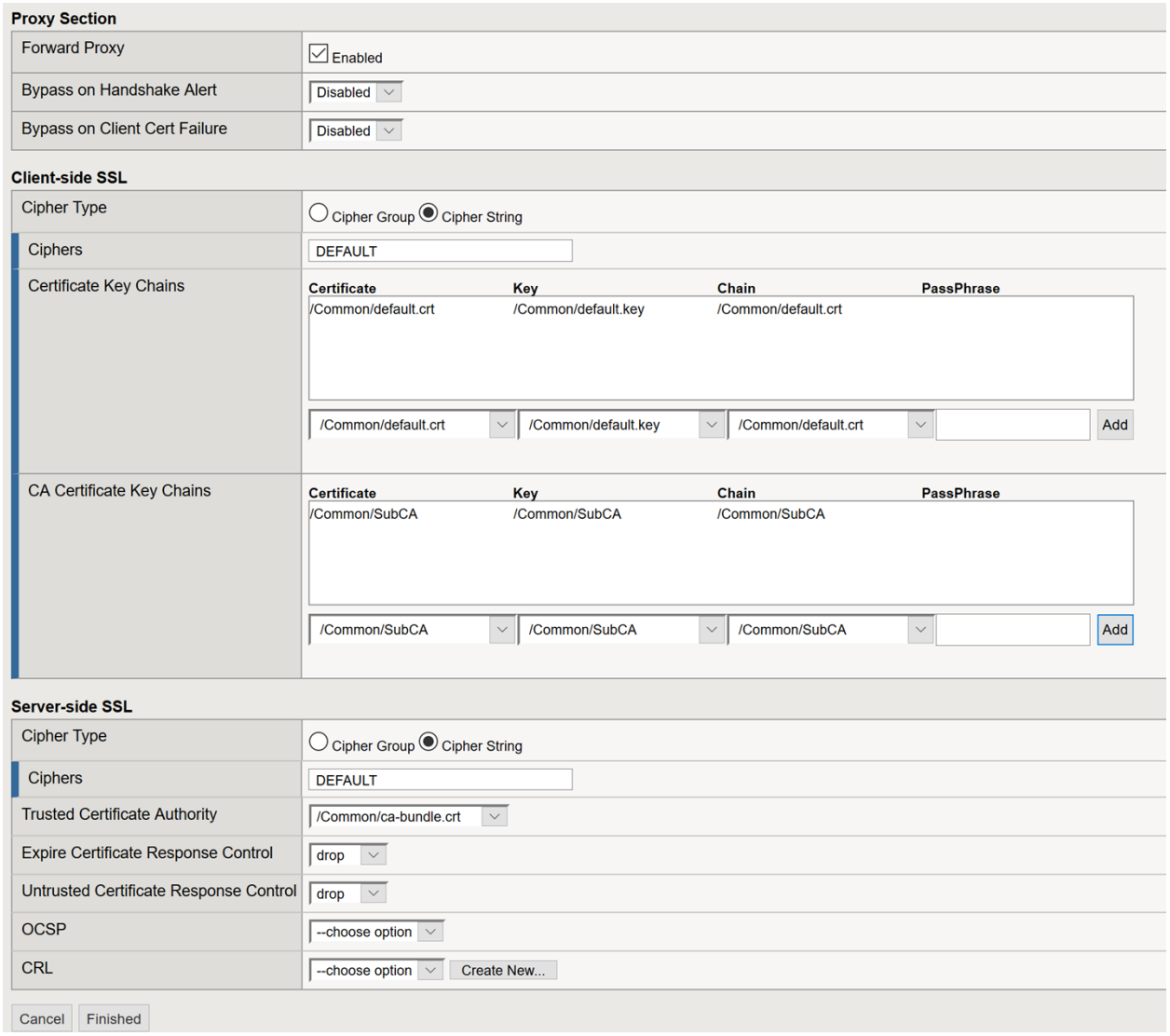


Figure 14: Sample SSL profile configuration

Create service chains to link services

Before you set up service chains, ensure you have configured any other necessary security services (HTTP, ICAP, L2, L3, and TAP) required by security devices from other vendors (e.g., ICAP for Symantec or HTTP for Cisco WSA). By default, SSL Orchestrator steers traffic through all the services. You can create a new service chain by defining the preferred order in which traffic should be steered.

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.

1. From the F5 device management interface, navigate to **SSL Orchestrator** > **Policies> Access Per-Request Policies**. The **Per-Request Policies** screen displays.

2. Click **Create** to create and configure the per-request service chain using the guidance below.

Configuration Field	User Input
General Properties	
Name	Type a **Name** for the per-request service chain.
TCP Service Chain	
Intercept Chain	In the order you want SSL Orchestrator to steer traffic, select an **Available Service** and click **<** to move it to the **Selected Services** box. Repeat or rearrange until all services in the chain are listed in the order you prefer.
Non Intercept Chain	Specify, and order as necessary, available services for the non-decrypted chain.
UDP Service Chain	
Service Chain Sequence	In the order you want SSL Orchestrator to steer traffic, select an **Available Service** and click **<** to move it to the **Selected Services** box. Repeat or rearrange until all services in the chain are listed in the order you prefer.

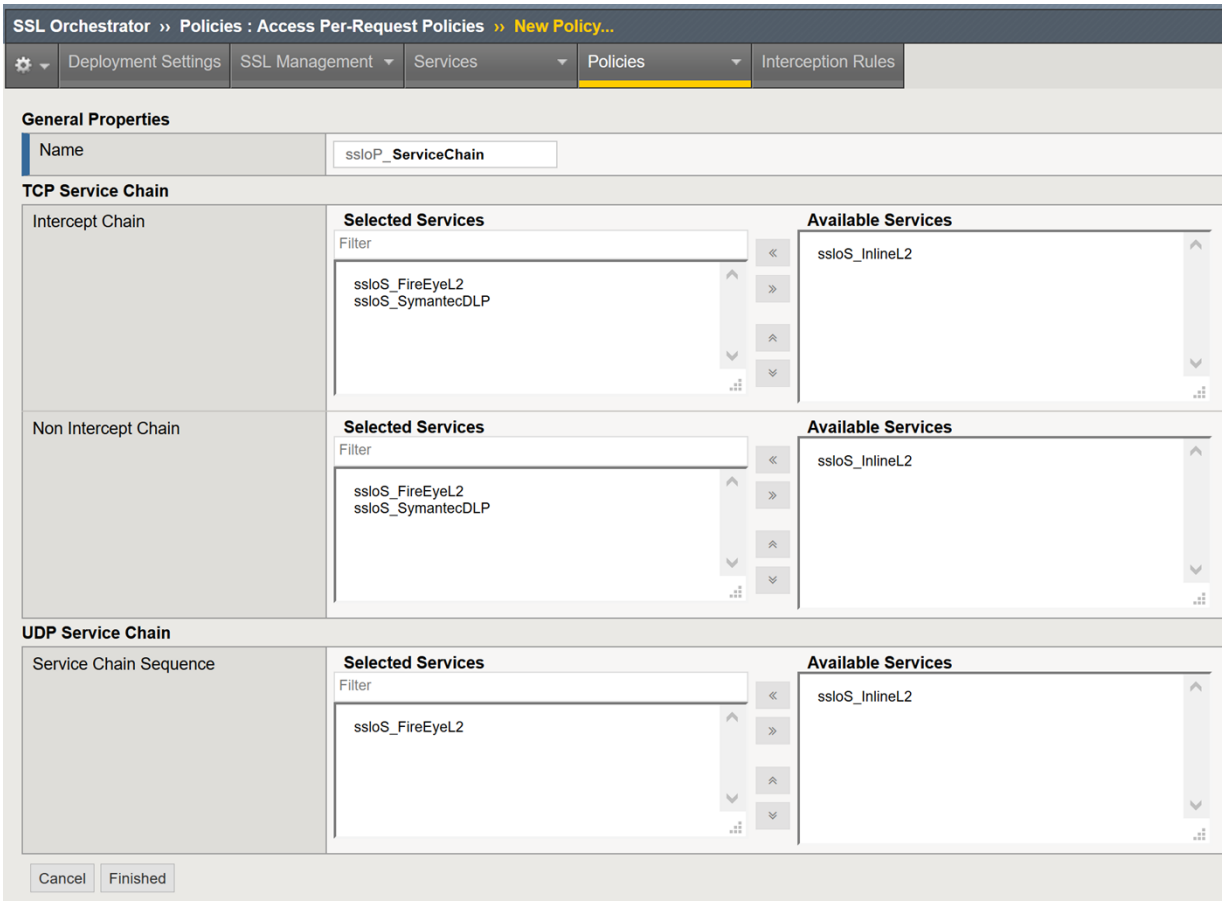


Figure 15: Sample per-request policy configuration

3. Click **Finished**.
4. On the **Per-Request Policies** screen that appears, click **+ Show All** below the per-request policy and click the TCP policy name to review it. The policy editor page will display so you can further finetune the policy using advanced configurations as desired. In the sample in Figure 16, for example, you could click **SSL Intercept Policy** to bypass SSL traffic destined to websites that expose personal user information, such as banking, financial, or government sites.

Figure 16: Sample per-request TCP policy

Create the interception rule

Before you create an interception rule, you must create one or more service chains.

1. On the F5 device management interface, navigate to **SSL Orchestrator > Deployment > Interception Rules**. The **SSL Settings Services** screen displays.
2. Click **Edit Default Outbound Rules** to create and configure the rule using the guidance below.
3. Click **Finished**.

Configuration Field	User Input
General Properties	*Leave all General Properties settings at their defaults.*
Proxy Setting	
Proxy Scheme	SSL Orchestrator can operate in transparent and/or explicit proxy mode. If you choose explicit proxy, enter the IP address and port number of the explicit proxy.
Classify UDP	If you selected **transparent proxy** above, by default TCP traffic will be managed but UDP traffic will pass through unexamined. Ensure Classify UDP is selected to manage UDP as well as TCP traffic.
Allow non-UDP/non-TCP	If you selected **transparent proxy** above, non-TCP, non-UDP traffic (such as IPSec, SCTP, and OSPF) will be blocked. Ensure this option is selected to pass non-UDP and non-TCP traffic.
Security	
SSL	Select the SSL profile.

Per Request Policy	Select the per-request policy you want.
Ingress Network	
VLANs	Select one or more ingress VLANs where the client traffic will arrive.
L7 Interception Rules	
Protocols	Specifies the protocol of the connection (based on port or protocol recognition) for interception.

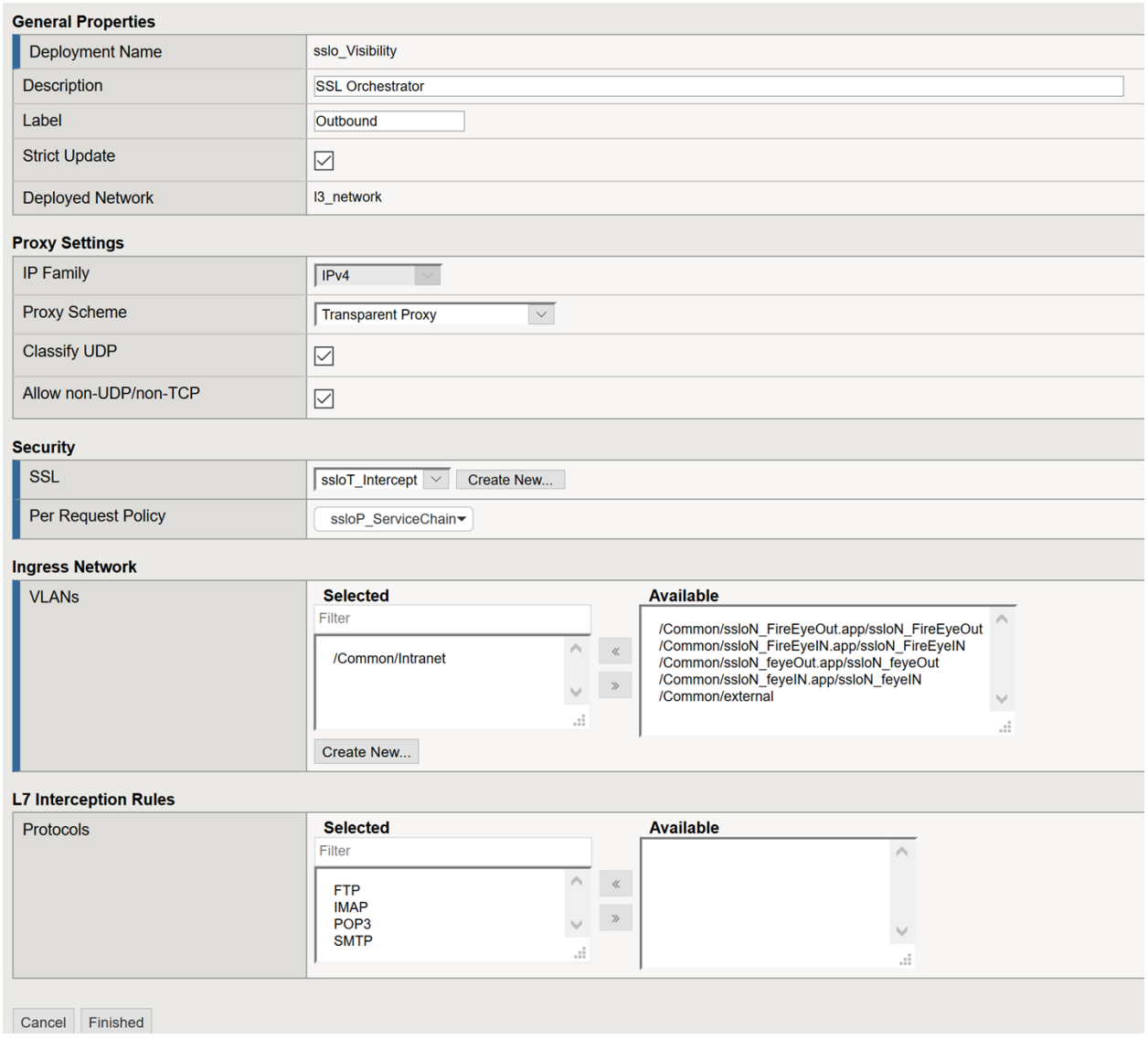


Figure 17: Sample interception rule configuration

Testing the Solution

You can 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 these tests with your 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