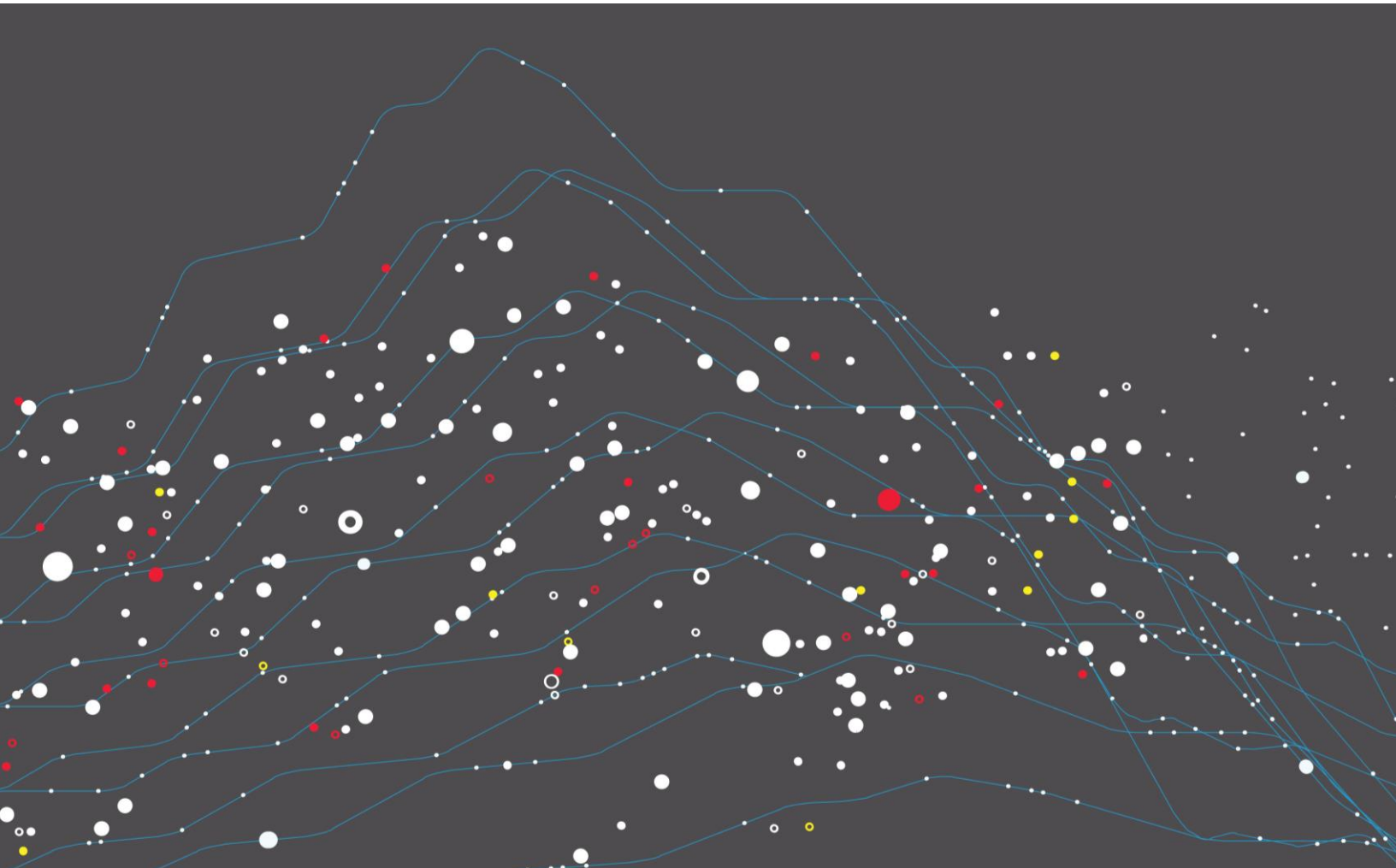




RECOMMENDED PRACTICES GUIDE

# The F5 SSL Orchestrator and Menlo Security Solution: SSL Visibility solution in a Proxy Chain with Multiple Egress Paths



May 2020

# Contents

Introduction and Prerequisites .....	3
Licensing .....	3
Configuring network connectivity (VLANs, self-IPs and routes) .....	3
Importing a CA certificate and private key .....	6
Upgrading the guided configuration file .....	7
SSL Orchestrator Guided Configuration .....	8
Guided configuration workflow .....	8
Topology properties .....	8
SSL configuration .....	10
Configuring services .....	12
Configuring service chains .....	13
Security policy .....	14
Interception rules .....	16
Egress setting .....	17
Configuration summary and deployment .....	17
Dynamically handling egress flows .....	18
iRules configuration .....	18
Modifying interception rules and disabling strictness .....	20
Configuring the per-request policy .....	21
Appendix .....	25
iRule-Explicit .....	25
iRule-GW .....	25

# Introduction and Prerequisites

This document outlines the step by step procedure for configuring the F5® SSL Orchestrator® and Menlo Security Web Isolation platform solution in a proxy chain when multiple egress paths are needed for different traffic category types.

## Licensing

The F5 SSL Orchestrator solution supports two licensing modes: standalone and LTM add-on:

### Standalone Model

The dedicated high performance [F5 SSL Orchestrator iSeries](#) product line— i2800, i5800, i10800, i11800, i15800 and High Performance Virtual Editions (HP VE)— HP 8vCPU, HP 16 vCPU supports the standalone license model.

This option is suited for environments that need standalone security solutions and have no need to integrate with other F5 software functions. Standalone mode restricts the F5 platform to the following additional software modules:

- **F5® Access Manager™** (formerly known as **F5® BIG-IP® APM**) to authenticate and manage user access.
- **F5® Secure Web Gateway (SWG)** Services to filter and control outbound web traffic using a URL database (OR) **F5 URL filtering (URLF)** subscription to access the URL category database.
- An **F5® IP Intelligence (IPI)** subscription for IP reputation service.

### LTM Add-on Module

The high-end [F5® VIPRION platform™](#) (chassis) which can run multiple BIG-IP guest instances enabled by the F5 Virtual Clustered Multiprocessing (vCMP) technology, and the [F5 BIG-IP platform](#) support the LTM add-on module.

This option is suited for environments that need to deploy SSL Orchestrator on an existing F5 device or have other functions that must run on the same device. There are no specific restrictions on additional F5 software modules. Optionally, customers can add the functionality of:

- A **URL Filtering (URLF)** subscription.
- An **F5 IP Intelligence**.
- A network **Hardware Security Module (HSM)** to safeguard and manage digital keys for strong authentication.

**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.**

## Configuring network connectivity (VLANs, self-IPs and routes)

For SSL Orchestrator deployment in a layer 3 (routed or explicit proxy) topology, the F5 system must be configured with appropriate internal (client-facing) and external (outbound-facing) VLANs, self-IPs, and routes. The VLANs

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

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 setup the VLANs and self-IPs.

1. On the F5 BIG-IP web UI, navigate to **Network > VLANs**.
2. Create the VLANs and associate them with the corresponding interface. See Figure 1.

Network >> VLANs : VLAN List >> New VLAN...

**General Properties**

Name: Internal  
Description: Internal VLAN  
Tag:

**Resources**

Interface: 1.2  
Tagging: Untagged  
Add  
Interfaces: 1.1 (untagged)  
Edit Delete

**Configuration:** Basic

Source Check:   
MTU: 1500

**sFlow**

Polling Interval: Default  
Sampling Rate: Default

Cancel Repeat Finished

Figure 1: Sample VLAN configuration

3. Once done with a VLAN configuration, click **Finished**. Repeat Steps 2 and 3 to configure both internal and external VLANs.

Network >> VLANs : VLAN List

VLAN List VLAN Groups

\* Search Create...

<input checked="" type="checkbox"/>	Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
<input type="checkbox"/>	external	4093	1.1			Common
<input type="checkbox"/>	internal	4094	1.2			Common

Figure 2: VLAN list

4. Next, navigate to **Network > Self IPs**. Create the IP addresses and associate them with the corresponding VLANs.

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

Network >> Self IPs >> New Self IP...

**Configuration**

Name	10.10.10.157
IP Address	10.10.10.157
Netmask	255.255.255.0
VLAN / Tunnel	internal
Port Lockdown	Allow Default
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)
Service Policy	None

Cancel Repeat Finished

Figure 3: Sample Self IP configuration

- Once done, click **Finished**. Repeat as needed to configure and associate IP addresses for both the internal and external VLANs.

Network >> Self IPs

Self IP List

Search Create...

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	10.10.10.157		10.10.10.157	255.255.255.0	internal	traffic-group-local-only	Common
<input type="checkbox"/>	192.168.16.157		192.168.16.157	255.255.255.0	external	traffic-group-local-only	Common

Figure 4: Self IP list

- Last, navigate to **Network > Routes**. Configure the default route to the Internet via the external interface.

Network >> Routes >> New Route...

**Properties**

Name	external_default_gateway
Description	Default route to Internet
Destination	0.0.0.0
Netmask	0.0.0.0
Resource	Use Gateway...
Gateway Address	IP Address 192.168.16.10
MTU	

Cancel Repeat Finished

Figure 5: Sample default route configuration

- Click **Finished**.

## Importing a CA certificate and private key

For SSL Orchestrator 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 SSL Orchestrator in 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.

1. Navigate to **System > Certificate Management**.
2. Browse to select the key and click **Import**.

The screenshot shows the 'Import SSL Certificates and Keys' dialog box. The 'Import Type' is set to 'Key'. Under 'Key Name', the 'New' radio button is selected, and the name 'Sub-CA' is entered. Under 'Key Source', the 'Upload File' radio button is selected, and a 'Browse...' button is visible next to the file path 'subrsa.f5labs.com.key'. The 'Security Type' is set to 'Normal'. The 'Free Space on Disk' is 10038 MB. At the bottom, there are 'Cancel' and 'Import' buttons.

Figure 6: Importing the CA key

3. After the key has been successfully imported, select it.

The screenshot shows the 'SSL Certificate List' table. The table has columns for Status, Name, Contents, Key Security, Common Name, Organization, Expiration, and Partition / Path. A row is selected with Name 'Sub-CA' and Key Security 'Normal'. The table also includes a search bar and 'Import...' and 'Create..' buttons.

Status	Name	Contents	Key Security	Common Name	Organization	Expiration	Partition / Path
<input checked="" type="checkbox"/>	Sub-CA	RSA Key	Normal				Common

Figure 7: Selecting the imported CA key

4. Browse to select the certificate and click **Import**.

The screenshot shows the 'Import SSL Certificate' dialog box. The 'Import Type' is set to 'Certificate'. Under 'Certificate Name', the path '/Common/Sub-CA' is entered. Under 'Certificate Source', the 'Upload File' radio button is selected, and a 'Browse...' button is visible next to the file path 'subrsa.f5labs.com.cer'. The 'Free Space on Disk' is 10038 MB. At the bottom, there are 'Cancel' and 'Import' buttons.

Figure 8: Importing the CA certificate

## Upgrading the guided configuration file

Periodic updates are available for SSL Orchestrator guided configuration. Download the latest SSL Orchestrator pack from [downloads.f5.com](https://downloads.f5.com). (More information about the guided configuration follows in the next section.)

1. On the product line page, select the SSL Orchestrator product line and download the latest **.rpm** file.

### Select a Download

**Product:** SSL Orchestrator  
**Version:** 15.0.0  
**Container:** SSL\_Orchestrator

Please select the file you wish to download, make sure you have read the appropriate [Release Notes](#) before attempting to use the file.

Filename	Description	Size
<a href="#">f5-iappslx-ssl-orchestrator-15.0.0-6.0.307.noarch.rpm</a>	f5-iappslx-ssl-orchestrator-15.0.0-6.0.307.noarch.rpm	5 MB
<a href="#">f5-iappslx-ssl-orchestrator-15.0.0-6.0.307.noarch.rpm.md5</a>	MD5 file for f5-iappslx-ssl-orchestrator-15.0.0-6.0.307.noarch.rpm	87 Bytes
<a href="#">f5-iappslx-ssl-orchestrator-15.0.0-6.1.12.noarch.rpm</a>	f5-iappslx-ssl-orchestrator-15.0.0-6.1.12.noarch.rpm	5 MB
<a href="#">f5-iappslx-ssl-orchestrator-15.0.0-6.1.12.noarch.rpm.md5</a>	MD5 file for f5-iappslx-ssl-orchestrator-15.0.0-6.1.12.noarch.rpm	86 Bytes

Figure 9: Guided configuration .rpm files on the SSL Orchestrator download page

2. On the F5 BIG-IP web UI, navigate to **SSL Orchestrator > Configuration**.
3. On the **Configuration** page, click **Upgrade SSL Orchestrator** in the upper left.
4. Select the downloaded .rpm file and click **Upgrade and Install**. See Figure 10.

### Upgrade SSL Orchestrator RPM

To begin installation you have to download a SSL Orchestrator RPM(.rpm) file from [downloads.f5.com](https://downloads.f5.com) (Security). Once downloaded you can upload the RPM below.

Import SSL Orchestrator RPM

f5-iappslx-ssl-orchestrator-15.0.0-6.0.307.noarch.rpm

Figure 10: Selecting with the downloaded .rpm file to upgrade

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

5. When the upgrade is completed, click **Continue**.

## SSL Orchestrator Guided Configuration

The procedures below will walk you through the guided configuration to build the explicit proxy and policies to proxy chain with Menlo Security. In the sample configuration, traffic destined to educational institutes is filtered by a URL filter policy on SSL Orchestrator and forwarded to Menlo Security for inspection.

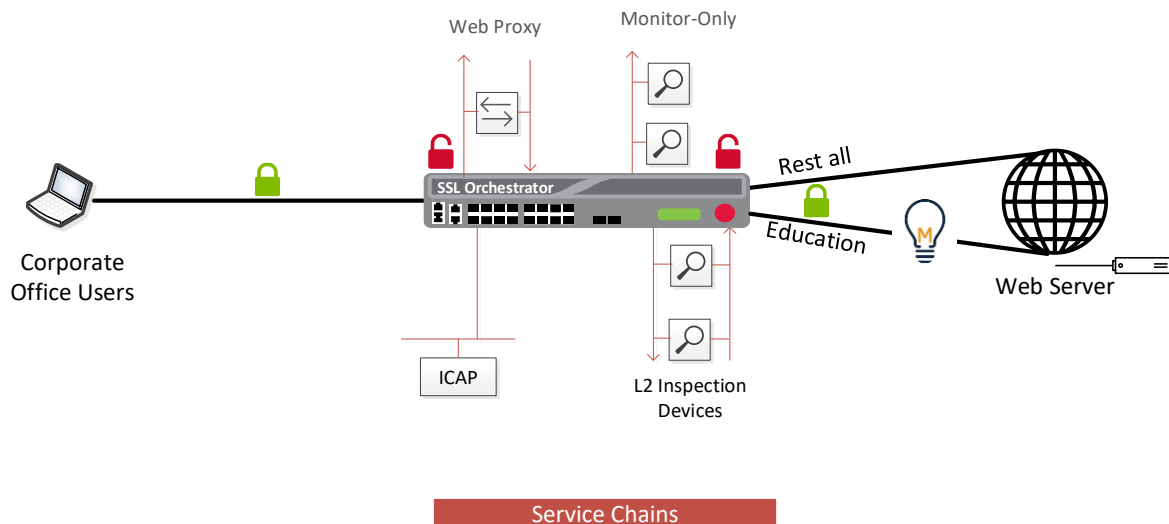


Figure 11: The F5 and Menlo Security solution

1. Once logged into the F5 system, in the F5 Web UI **Main** menu, click on **SSL Orchestrator > Configuration**.
2. Take a moment to review the various configuration options.
3. (Optional) Satisfy any of the DNS, NTP, and Route prerequisites on the 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.

## Guided configuration workflow

The SSL Orchestrator guided configuration presents a completely new and streamlined user experience. This workflow-based architecture provides intuitive, re-entrant configuration steps tailored to a selected topology.

The steps below will walk through the guided configuration to build a simple transparent forward proxy.

The first stage of the guided configuration addresses topology.



Figure 12: Topology configuration in the workflow

### Topology properties

SSL Orchestrator creates discreet configurations based on the selected topology. An explicit forward proxy topology



## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

will ultimately create an explicit proxy listener.

**Note 1:** The **Proxy Connect** option in the SSL Orchestrator UI is only available for explicit proxy topologies.

**Note 2:** SSL Orchestrator currently only supports upstream proxy chaining with the explicit proxy outbound topology (explicit-to-explicit). SSL Orchestrator supports the following topology egress modes:

- Explicit-to-transparent
- Explicit-to-explicit (proxy chain)
- Transparent-to-transparent
- Explicit passthrough (SSL Orchestrator in transparent mode)

1. Make appropriate selections in the Topology Properties section of the configuration using the guidance below.

Topology Properties	User Input
<b>Name</b>	Enter a <b>Name</b> for the SSL Orchestrator deployment.
<b>Description</b>	Enter a <b>Description</b> for this deployment.
<b>Protocol</b>	<p>The <b>Protocol</b> option presents four protocol types:</p> <ul style="list-style-type: none"><li>• <b>TCP:</b> Creates a single TCP wildcard interception rule for the L3 inbound, L3 outbound, and L3 explicit proxy topologies.</li><li>• <b>UDP:</b> Creates a single UDP wildcard interception rule for L3 inbound and L3 outbound topologies.</li><li>• <b>Other:</b> Creates a single “any protocol” wildcard interception rule for L3 inbound and L3 outbound topologies. Typically used for non-TCP/UDP traffic flows.</li><li>• <b>Any:</b> Creates the TCP, UDP, and non-TCP/UDP interception rules for outbound traffic flows. The sample configuration demonstrates this option.</li></ul>
<b>IP Family</b>	Specify whether this configuration should support <b>IPv4</b> addresses or <b>IPv6</b> addresses.
<b>SSL Orchestrator Topologies</b>	<p>The SSL Orchestrator Topologies options present six topologies:</p> <ol style="list-style-type: none"><li>1. <b>L3 Explicit Proxy:</b> The traditional explicit forward proxy. The sample configuration uses this topology.</li><li>2. <b>L3 Outbound:</b> The traditional transparent forward proxy.</li><li>3. <b>L3 Inbound:</b> A reverse proxy configuration.</li><li>4. <b>L2 Inbound:</b> 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.</li><li>5. <b>L2 Outbound:</b> 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.</li></ol>

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

	<p>6. <b>Existing Application:</b> 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.</p> <p>The sample configuration deploys SSL Orchestrator as an L3 explicit proxy for decrypting outbound TLS/SSL traffic. See Figure 13.</p>
--	--

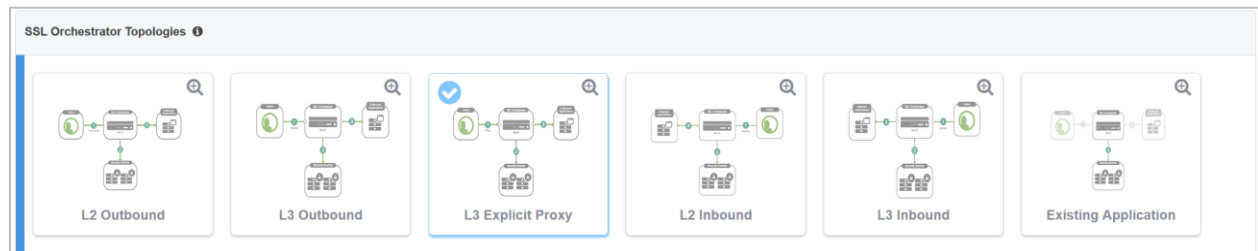


Figure 13: Sample topology configuration

2. Click **Save & Next**.

## SSL configuration

This section defines the specific SSL settings for the selected topology (a forward proxy in the sample) 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 14: 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
<b>SSL Profile</b>	
<b>Name</b>	Enter a <b>Name</b> for the SSL profile.
<b>Description</b>	Enter a <b>Description</b> for this SSL profile.
<b>Client-Side SSL</b>	
<b>Cipher Type</b>	<p>The cipher type can be a <b>Cipher Group</b> or <b>Cipher String</b>. The latter is recommended.</p> <ul style="list-style-type: none"> <li>• For <b>Cipher Group</b>, select a previously defined cipher group (which can be defined if necessary, by navigating to <b>Local Traffic &gt; Ciphers &gt; Groups</b>).</li> <li>• When <b>Cipher String</b> is selected, a field will be populated with the</li> </ul>

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

	default option, which is optimal for most environments. (Otherwise, users could also enter a cipher string that appropriately represents the client-side TLS requirement.)
<b>Certificate Key Chains</b>	<p>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 customers the opportunity to apply their own template private key, and optionally to 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 BIG-IP system is installed.</p> <p>Select the default.crt certificate, default.Key key, default.crt chain and leave the <b>Passphrase</b> field empty, then click <b>Add</b>.</p>
<b>CA Certificate Key Chains</b>	<p>An SSL forward proxy must re-sign or forge a remote server certificate to local clients using a local certificate authority (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.</p> <p>Specify one or more configured CA certificates and keys that were imported, then click <b>Add</b>.</p>
<b>Server-Side SSL</b>	
<b>Cipher Type</b>	Select <b>Cipher String</b> for the default cipher list.
<b>Ciphers</b>	Uses the <b>ca-bundle.crt</b> file, which contains all well-known public CA certificates, for client-side processing.
<b>Expired Certificate Response Control</b>	Select whether to <b>Drop</b> or <b>Ignore</b> the connection even if the specified certificate response control (CRL) file has expired.
<b>Untrusted Certificate Response Control</b>	Select whether to drop or ignore the connection even if the specified CRL file is not trusted.
<b>OCSP</b>	Specify the supported <b>OCSP</b> .
<b>CRL</b>	Specify the supported <b>CRL</b> .

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

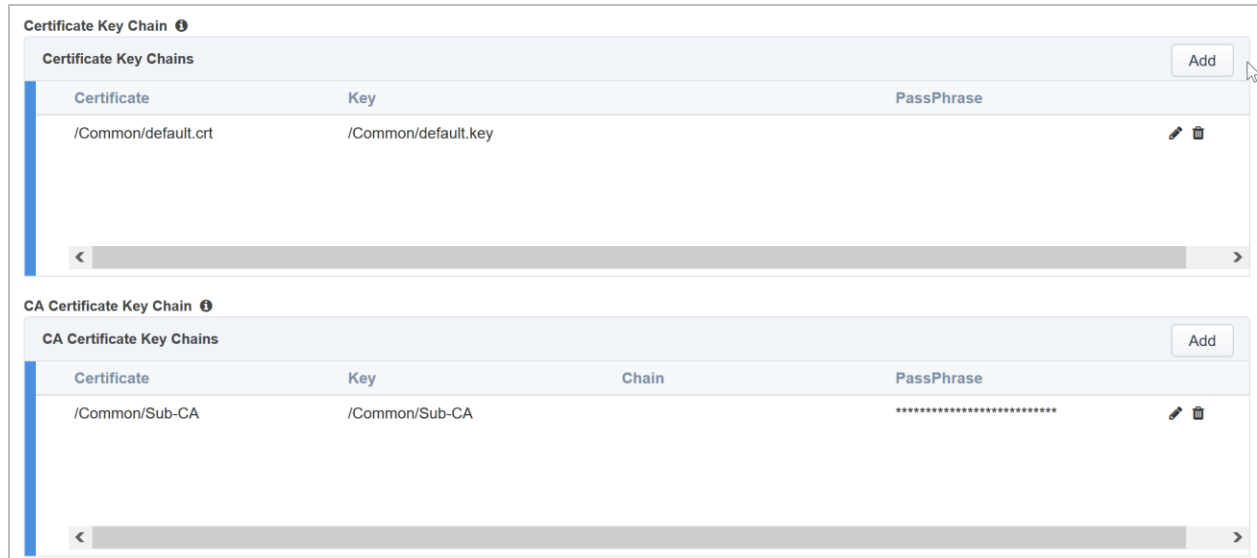


Figure 15: Sample SSL configuration

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.

### Configuring services

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 16: Service configuration

This step is optional. Use the service catalog if you want to configure services for various security vendor products and technologies as part of an SSL Orchestrator service chain.

1. Under **Service List**, click **Add Service**.
2. In the service catalog, double click the service you want to configure (or select the service and click **Add**. (If the version of SSL Orchestrator being used doesn't have this option, select the generic L2 service.)

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

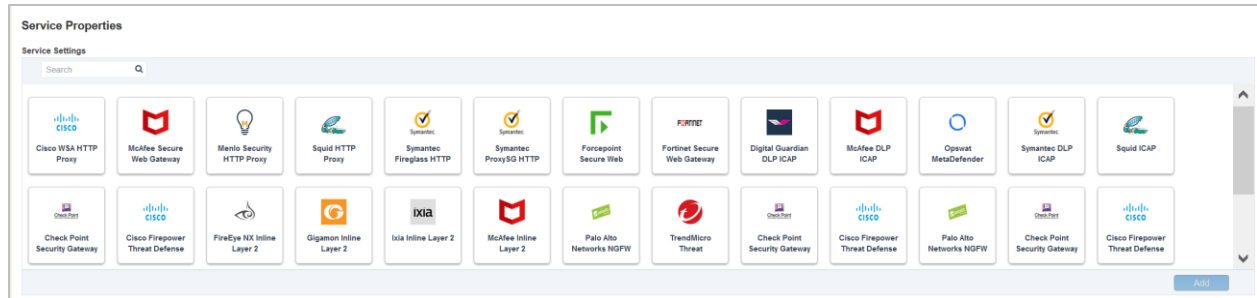


Figure 17: A service catalog

3. The **Service Properties** page displays. Configure the service as needed using onscreen options.

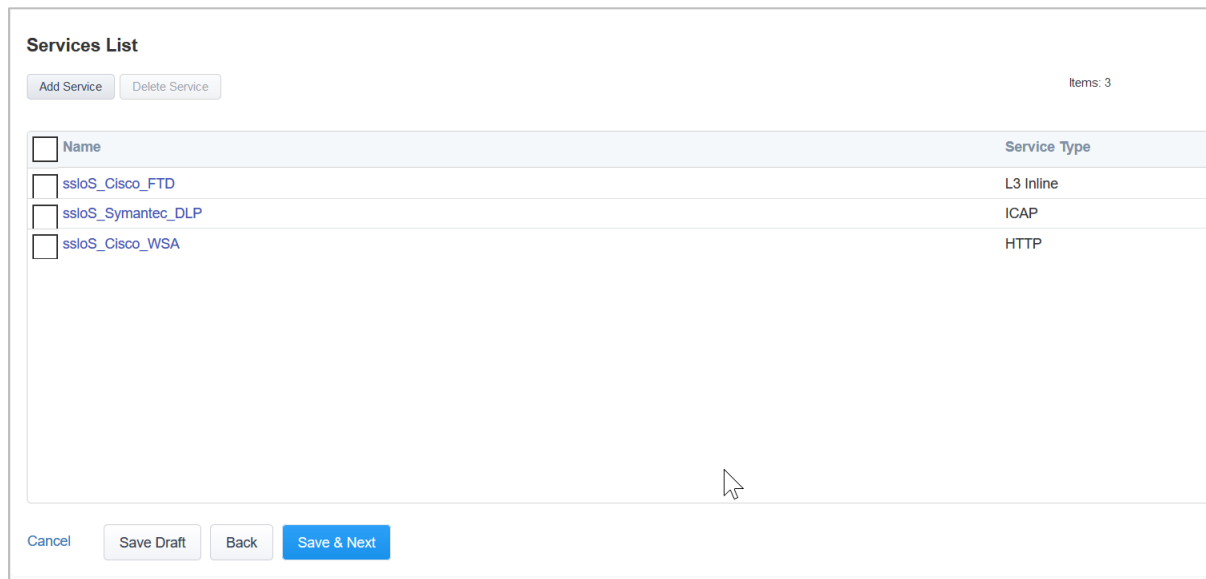


Figure 18: Sample services added for Cisco FTD, Symantec DLP, and Cisco WSA

4. Click **Save & Next**.

### Configuring 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, while traffic destined to a financial service URL can bypass decryption and flow through a still smaller set of security services.

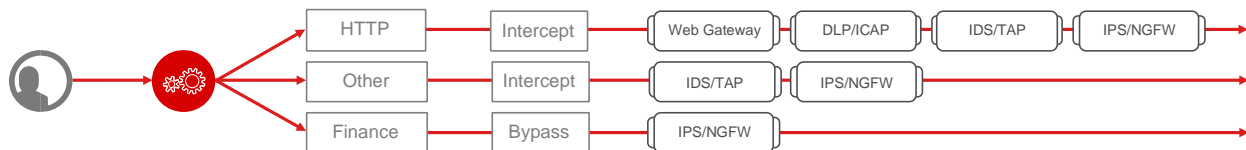


Figure 19: Different traffic flowing through chains of different security services

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

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

services (inline, ICAP, or receive-only), as well as decryption zones between separate ingress and egress devices.



Figure 20: Configuring service chains

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

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

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

2. Click **Save & Next**.

**Services Chain Properties**

**Name**  
In the services chain properties Name field, type a name after the default prefix ssloSC\_

ssloSC\_srv

**Description**  
Type a description for the service chain.

**Services**

**Services Available**  
Filter: ssloS\_FEYE

**Selected Service Chain Order**  
ssloS\_Cisco\_FTD  
ssloS\_Cisco\_WSA  
ssloS\_Symantec\_DLP

Figure 21: Sample service chain with Cisco FTD, Symantec DLP, and Cisco WSA

## 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 22: 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.

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

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**.

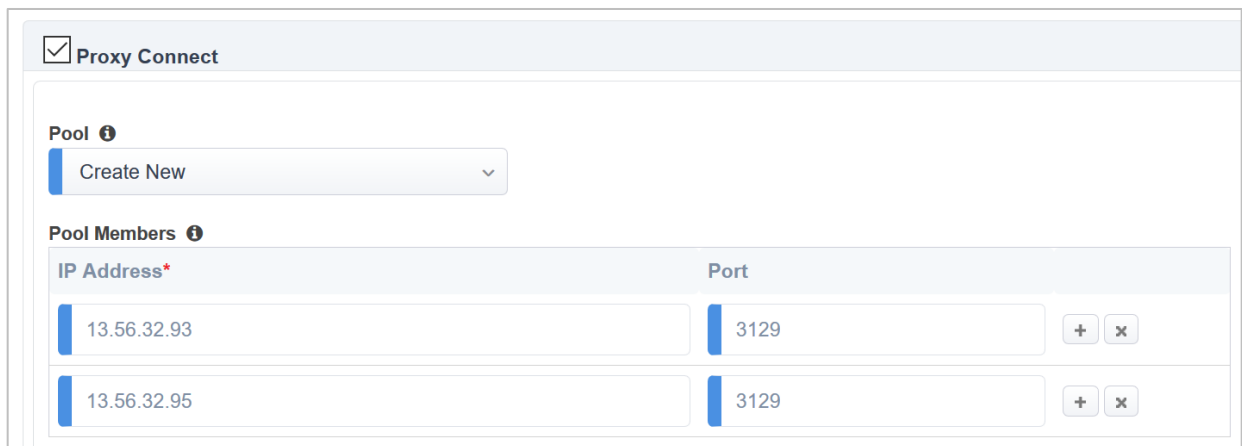


Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check and SNI Category is <b>Pinners</b>	Allow	Bypass	-
All Traffic	All	Allow	Intercept	-

Figure 23: Adding security rules

By default, SSL Orchestrator defines a single egress pool for transparent proxy traffic. For an upstream explicit proxy (that is, a "proxy chain"), however, SSL Orchestrator inserts two proxy select agents in the visual policy. Proxy chaining is configurable in the SSL Orchestrator security policy UI by enabling the **Proxy Connect** option and then defining the IP and port of the upstream proxy.

4. Scroll down and click **Proxy Select**.
5. Click **Pool** and select **Create New**.
6. Add the IP address and port number for Menlo Security. Click **+** to add multiple IP addresses.
7. Click **Save & Next**. Proxy connect creates two proxy select agents in the visual policy. This will enable F5 proxy chaining with Menlo Security.



Proxy Connect

Pool ⓘ  
Create New

Pool Members ⓘ

IP Address*	Port
13.56.32.93	3129
13.56.32.95	3129

Figure 24: Enabling proxy connect for proxy chaining

8. Navigate to **Access > Policies/ Profiles > Per-Request Policies** and click **Edit** on the policy row to launch the visual policy editor. This policy will be customized in the next procedure.

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

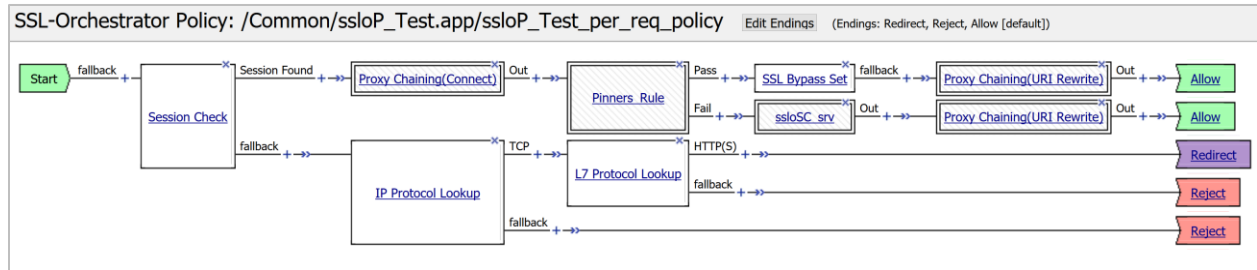


Figure 25: The per-request policy in the visual editor

9. The first Proxy Select sets up an initial connection without URI rewrite.

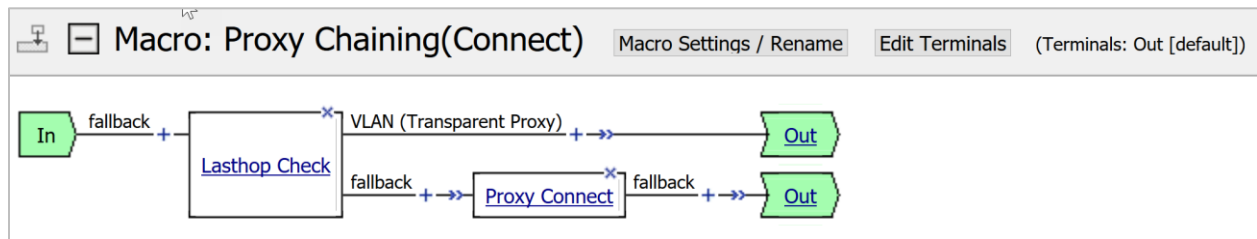


Figure 26: Proxy chaining (connect) macro

10. The second sets up a connection, but with a URI rewrite.

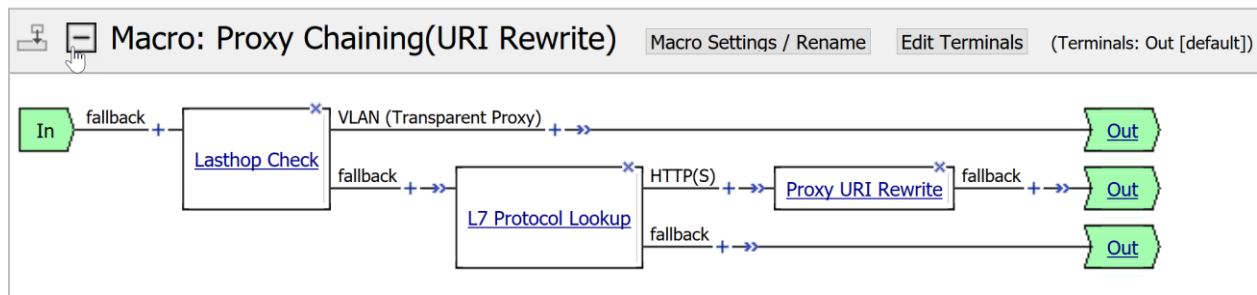


Figure 27: Proxy chaining (URI rewrite) macro

The two proxy select agents are required to address traffic flow through SSL Orchestrator. In the proxy chaining process, if a certificate is not cached, SSL Orchestrator must *first* egress to the remote server to validate and then consume the remote server certificate. The first proxy select agent in the visual policy handles the initial outbound flow, while the second handles the re-encrypted flow.

The first proxy select follows a last-hop check, which flows to the VLAN branch if this is a transparent proxy request, and to fallback if this is an explicit proxy request. This simply sets up a connect to retrieve the remote server certificate over an explicit proxy request.

The second proxy select follows the last-hop check and an L7 protocol lookup. If the L7 protocol lookup returns HTTP or HTTPS, the proxy select sets up a connect or a proxied HTTP request for the re-encrypted traffic

## 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 others. The resulting BIG-IP LTM virtual servers will bind the SSL settings, VLANs, IPs, and security policies created in the topology workflow.



## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution



Figure 28: Configuring interception rules

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

Interception Rule	User Input
<b>Label</b>	Enter a <b>Name</b> for the label.
<b>Description</b>	Enter a <b>Description</b> for this rule.
<b>Proxy Server Settings</b> 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.	
<b>IPv4 Address</b>	Specify the explicit proxy listening IP address.
<b>Port</b>	Specify the port number.
<b>Access profile</b>	Specify the access policy (optional).
<b>Ingress Network</b>	
<b>VLANs</b>	This defines the VLANs through which traffic will enter. For a forward proxy topology (outbound), this would be the client-side VLAN (intranet).

2. Click **Save & Next**.

### Egress setting

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

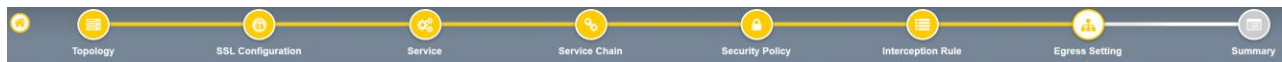


Figure 29: Configuring egress settings

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

Egress Settings	User Input
<b>Manage SNAT Settings</b>	Define if and how source NAT (SNAT) is used for egress traffic.
<b>Gateways</b>	Enter the IP address of 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 the workflow-configured objects.

1. To review the details for any given setting, click the corresponding arrow on the far right.

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

2. To edit any setting, click the corresponding pencil icon, which will display the settings page in the workflow.
3. When the settings are as desired, click **Deploy**. SSL Orchestrator will display a dashboard as shown in Figure 30.

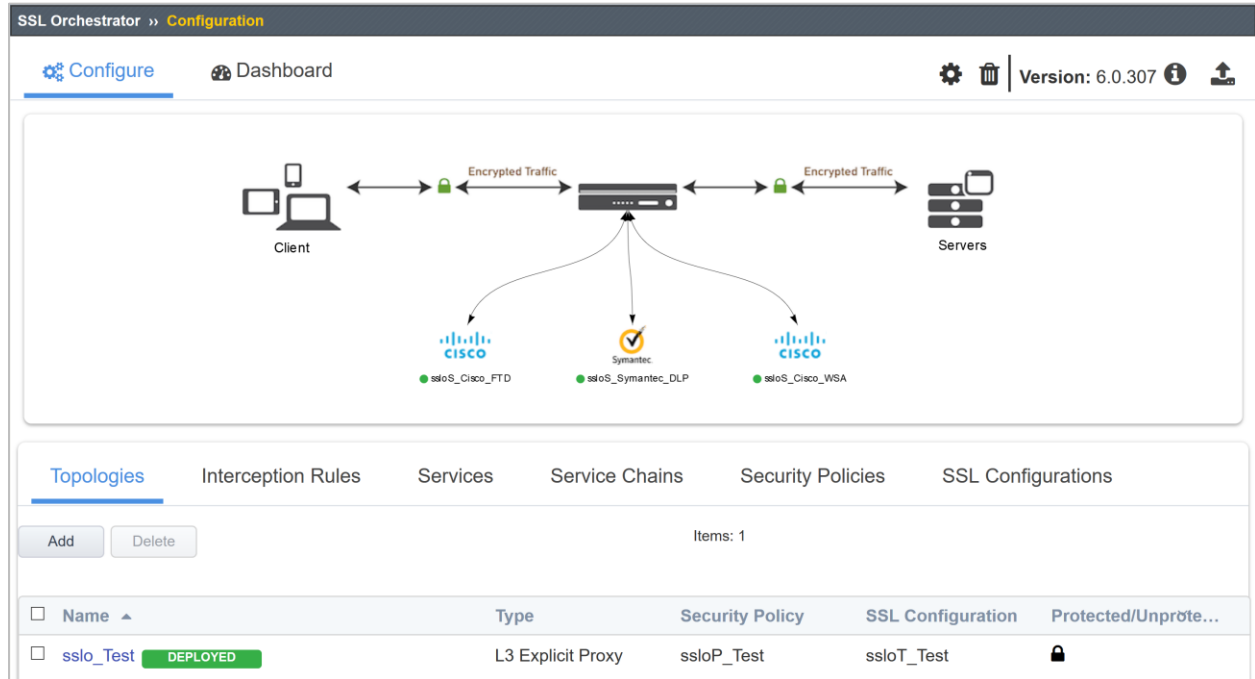


Figure 30: A successfully deployed SSL Orchestrator configuration

## Dynamically handling egress flows

Administrators can customize and build a policy to dynamically choose the egress path based on based on URL category lookup. In this sample scenario, the default egress path is an upstream Menlo explicit proxy (that is, a proxy chain), except for **.edu** URLs, which must follow a different routed path.

**Note:** This is just one sample use case in which manual URL categorization passes traffic through or around proxy select agents in the visual policy. Simply evaluating against a client/server IP or port can be done directly in the visual policy without using F5® iRules®. Any other case that requires categorization will need some version of the iRule configuration below.

### iRules configuration

1. Create an iRule called **iRule-GW** that will collect the shared variable and perform a manual category lookup. If the category matches, a per-flow variable will be assigned. The object of the sample iRule below is to manually query a single or set of URL categories, and if matched, set a per-flow variable. The per-flow variable is read within the visual policy to direct traffic through or around proxy select agents.

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

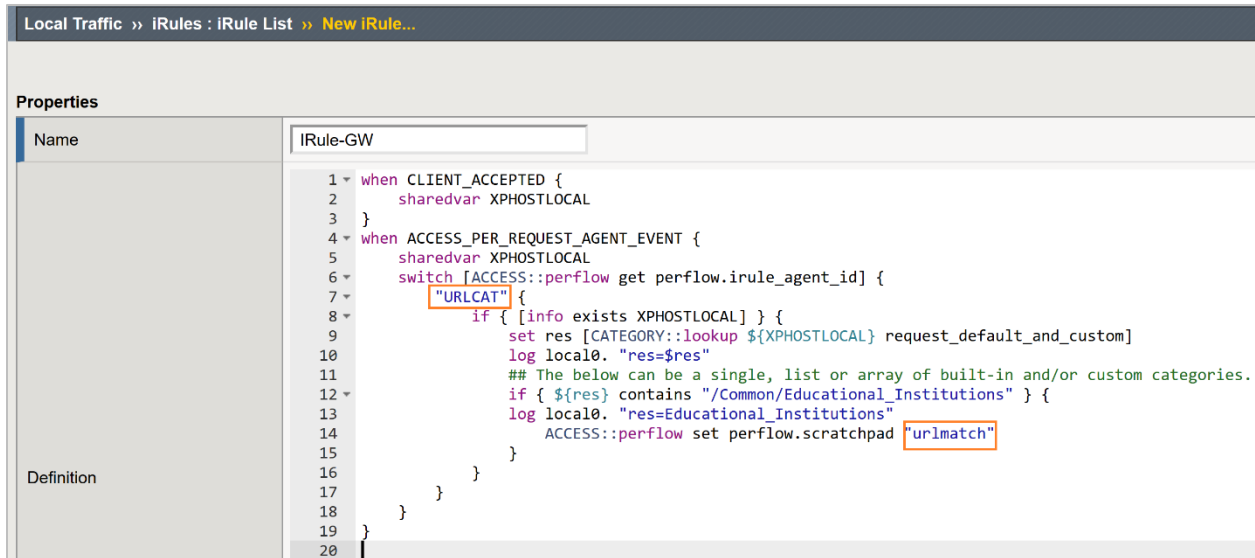


Figure 31: Sample IRule-GW iRule

2. Create an iRule called **iRule-Explicit** that will grab the explicit proxy request URL from the client and save it to a shared variable.

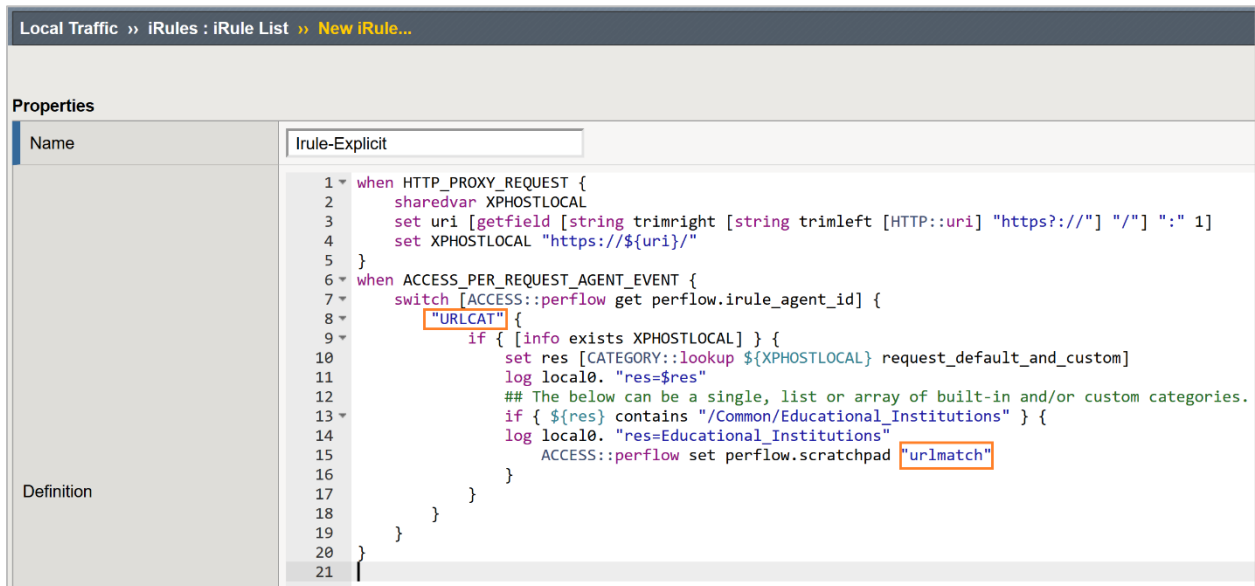


Figure 32: Sample iRule-Explicit iRule

3. Review the two iRules. (These samples can be found in the Appendix.)

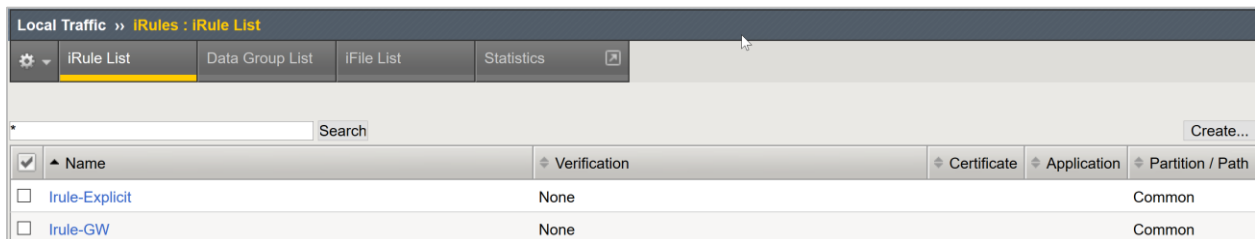


Figure 33: The created iRules

## Modifying interception rules and disabling strictness

1. Navigate to **SSL Orchestrator > Configuration** and click **Interception Rules**.

<a href="#">Topologies</a> <a href="#">Interception Rules</a> <a href="#">Services</a> <a href="#">Service Chains</a> <a href="#">Security Policies</a> <a href="#">SSL Configurations</a>									
Items: 2									
Name ▲	Label	Source Ad...	Destination Addr...	Service ...	Pro...	VLAN	Topology	SS...	
sslo_Test-in-t-4	Outbound	0.0.0.0/0	0.0.0.0/0	0	tcp	/Common/sslo_Test.app/sslo_Test-xp-tunnel	sslo_Test	ssloT_	
sslo_Test-xp-4	Outbound	0.0.0.0/0	10.10.10.191/32	3128	tcp	/Common/external,/Common/internal	sslo_Test		

Figure 34: The SSL Orchestrator Interception Rules configuration tab

- L7 Profile Type: HTTP
- L7 Profile: sslo\_[appname]-xp-http
- iRules: add **iRule-Explicit**

**L7 Profile Type**

HTTP ▼

Select an L7 profile type.

**L7 Profile**

/Common/sslo\_Test.app/sslo\_Test-xp-http ▼

Select an L7 profile that associates with the L7 profile type or click **Create New** to create a new profile.

**Resources**

**iRules ⓘ**

**Available**

Filter ▼

- /Common/Irule-GW
- /Common/sslo\_Test.app/sslo\_Test-in\_t
- /Common/sslo\_Test.app/sslo\_Test-lib

**Selected**

- /Common/Irule-Explicit
- sslo\_Test-xp

Figure 35: Updating the iRule for the -xp-4 interception rule

2. Modify the **-in-t** interception rule to the following setting:
  - iRules: add **iRule-GW**

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

**L7 Profile Type**  
HTTP

Select an L7 profile type.

**L7 Profile**  
/Common/sslo\_Test.app/sslo\_Test-xp-http

Select an L7 profile that associates with the L7 profile type or click **Create New** to create a new profile.

**Resources**

**iRules**

**Available**

Filter

- /Common/lrule-GW
- /Common/sslo\_Test.app/sslo\_Test-in\_t
- /Common/sslo\_Test.app/sslo\_Test-lib

**Selected**

- /Common/lrule-Explicit
- sslo\_Test-xp

Figure 36: Updating the iRule for the **-in-t** interception rule

3. Click **Security Policies** and disable strictness by clicking the lock to unlock it. Keep in mind that with strictness disabled, the topology configuration is read-only from the SSL Orchestrator UI.

Topologies	Interception Rules	Services	Service Chains	Security Policies	SSL Configurations
Add Delete Items: 1					
<input type="checkbox"/>	Name ▲	Topologies ▼	Per Request Policy	Protected/Unprotected Configuration	
<input type="checkbox"/>	ssloP_Test	sslo_Test	ssloP_Test		<a href="#">Click to Protect Configuration</a>

Figure 37: SSL Orchestrator configuration showing how to disable security policy strictness

4. Click **Interception Rules**.

## Configuring the per-request policy

Proxy chaining support in the SSL Orchestrator security policy requires two agents:

- A proxy-select agent, **Proxy Chaining (Connect)**, at the beginning of the policy that creates the initial outbound path
- A separate proxy-select agent, **Proxy Chaining (URI Rewrite)**, at the end of the policy that appropriately rewrites the request to an upstream explicit proxy.

As the decision for the initial proxy selection must happen before any VPE categorization, manual categorization

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

must be handled in an iRule based on the HTTP Connect URL entering the SSL Orchestrator explicit proxy listener.

To configure this setup:

1. Navigate to **Access > Policies/Profiles > Per-Request Policies** and click **Edit** for the appropriate policy row to launch the visual policy editor.

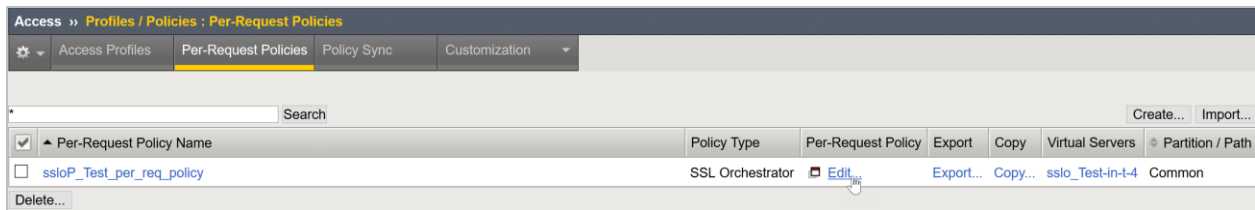


Figure 38: Per-request policy editing

2. Click **Add New Macro** and create a new macro called **Proxy Chain (Stage 1)**.
3. Insert an **iRule event** agent with the following settings. (This agent is found on the **General Purpose** tab.)
  - **ID:** URLCAT
  - **Expect Data:** Client Accepted
  - **Branch Rule Name:** urlmatch
  - **Branch Rule Expression:** Click **Advanced** and, per Figure 39, enter `expr { [mcget {perflow.scratchpad}] == "urlmatch" }`

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

Properties\* **Branch Rules\***

Name:

---

**Custom iRule Event Agent**

ID	<input type="text" value="URLCAT"/>
Expect Data	<input type="text" value="Client Accepted"/>

Note: Use this option when using this per-request policy for SSL Orchestrator use cases only. Do not use this option for APM and SWG use cases.

Properties\* **Branch Rules\***

Add Branch Rule Insert Before:

---

Name:

Expression: *Empty* [change](#)

Name: *fallback*

**Simple** **Advanced\***

```
expr { [mcget {perflow.scratchpad}] == "urlmatch" }
```

Figure 39: Configuring the iRule agent and branch rule

4. In the visual policy editor, include the **Proxy Chaining (Connect)** macro on the iRule agent's fallback branch.

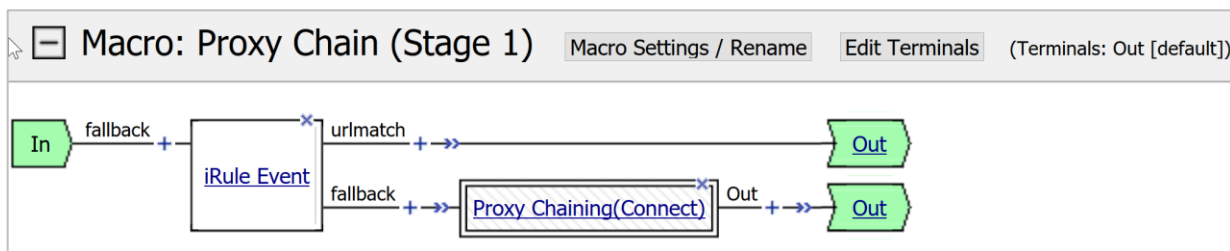


Figure 40: The proxy chain (Stage 1) macro in the visual policy editor

5. Create another macro called **Proxy Chain (Stage 2)**.
6. Insert an **Empty** agent (found on the **General Purpose** tab) with the following settings:
  - **Branch Rule Name:** urlmatch
  - **Branch Rule Expression:** `expr { [mcget {perflow.scratchpad}] == "urlmatch" }`

## RECOMMENDED DEPLOYMENT PRACTICES

### The F5 SSL Orchestrator and Menlo Security Solution

7. Include the **Proxy Chaining (URI Rewrite)** macro on the empty agent's fallback branch.

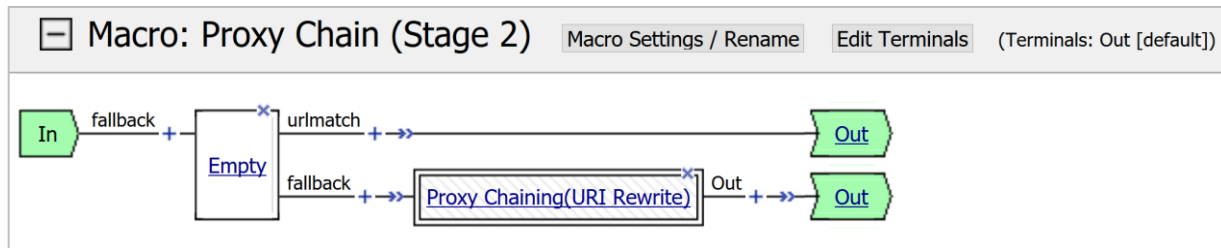


Figure 41: The proxy chain (Stage 2) macro

8. Replace the **Proxy Chaining (Connect)** macro in the main policy with the new **Proxy Chain (Stage 1)** agent.
9. Replace all the **Proxy Chaining (URI Rewrite)** macros in the main policy with the new **Proxy Chain (Stage 2)** agent.

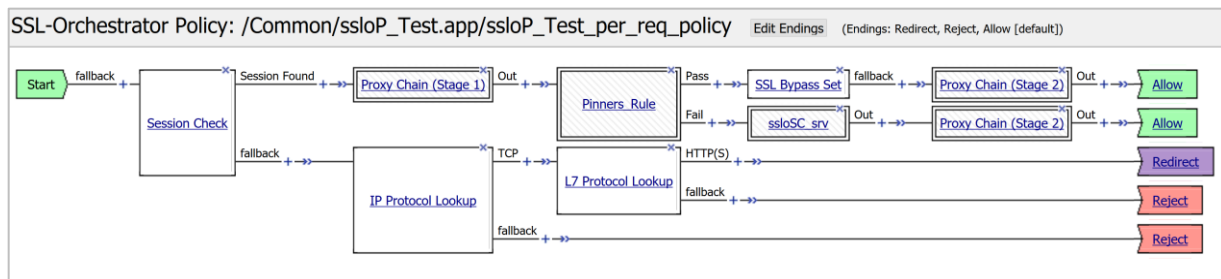


Figure 42: The updated per-request policy

When this process is complete, traffic will flow like this:

- The client's explicit proxy request enters the -xp-4 virtual server, and the associated iRule re-formats the URL and stores it in a shared variable.
- After the TCP tunnel is created, the client's TLS handshake enters the -in-t virtual server and activates the SSL Orchestrator security policy.
- The **Proxy Chain (Stage 1)** agent calls an iRule event on the iRule attached to the -in-t virtual server. It grabs the shared URL variable from the initial connection and performs a manual CATEGORY::lookup. If the result contains a match to the \_Urls custom category, a per-flow variable is created (**urlmatch**) and the traffic follows a path that does not include the proxy select. If the URL does not match, the traffic follows the branch that includes the proxy select.
- Normal security policy processing proceeds.
- At the end of each "allow" branch, the **Proxy Chain (Stage 2)** agent issues a simple branch condition to test for the per-flow variable (**urlmatch**). If the variable exists, it follows the branch without the proxy select. If it doesn't match, it follows the branch with the proxy select.
- Therefore, if the URL captured in the explicit proxy connect request matches the edu custom category match, it sets a variable. In the security policy, if the variable exists, proxy select agents are skipped and traffic egresses via a standard routed path. If the variable does not exist, the proxy select agents are engaged and SSL Orchestrator directs egress via proxy chaining to the upstream gateway.



## Appendix

### iRule-Explicit

```
when HTTP_PROXY_REQUEST {
    sharedvar XPHOSTLOCAL
    set uri [getfield [string trimright [string trimleft [HTTP::uri] "https?://" ] "/" ] ":" 1]
    set XPHOSTLOCAL "https://${uri}/"
}
when ACCESS_PER_REQUEST_AGENT_EVENT {
    switch [ACCESS::perflow get perflow.irule_agent_id] {
        "URLCAT" {
            if { [info exists XPHOSTLOCAL] } {
                set res [CATEGORY::lookup ${XPHOSTLOCAL} request_default_and_custom]
                log local0. "res=$res"
                ## The below can be a single, list or array of built-in and/or custom
categories.
                if { ${res} contains "/Common/Educational_Institutions" } {
                    log local0. "res=Educational_Institutions"
                    ACCESS::perflow set perflow.scratchpad "urlmatch"
                }
            }
        }
    }
}
```

### iRule-GW

```
when CLIENT_ACCEPTED {
    sharedvar XPHOSTLOCAL
}
when ACCESS_PER_REQUEST_AGENT_EVENT {
    sharedvar XPHOSTLOCAL
    switch [ACCESS::perflow get perflow.irule_agent_id] {
        "URLCAT" {
            if { [info exists XPHOSTLOCAL] } {
                set res [CATEGORY::lookup ${XPHOSTLOCAL} request_default_and_custom]
                log local0. "res=$res"
                ## The below can be a single, list or array of built-in and/or custom
categories.
                if { ${res} contains "/Common/Educational_Institutions" } {
                    log local0. "res=Educational_Institutions"
                    ACCESS::perflow set perflow.scratchpad "urlmatch"
                }
            }
        }
    }
}
```

---

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

©2020 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of the respective owners with no endorsement or affiliation, expressed or implied, claimed by F5. TMPL-CORE-215662710 | 03.18

