INTEGRATION GUIDE

BIG-IP SSL Orchestrator and Menlo Security Remote Browser Isolation

SSL/TLS Visibility Solution in a Proxy Chain with Multiple Egress Paths

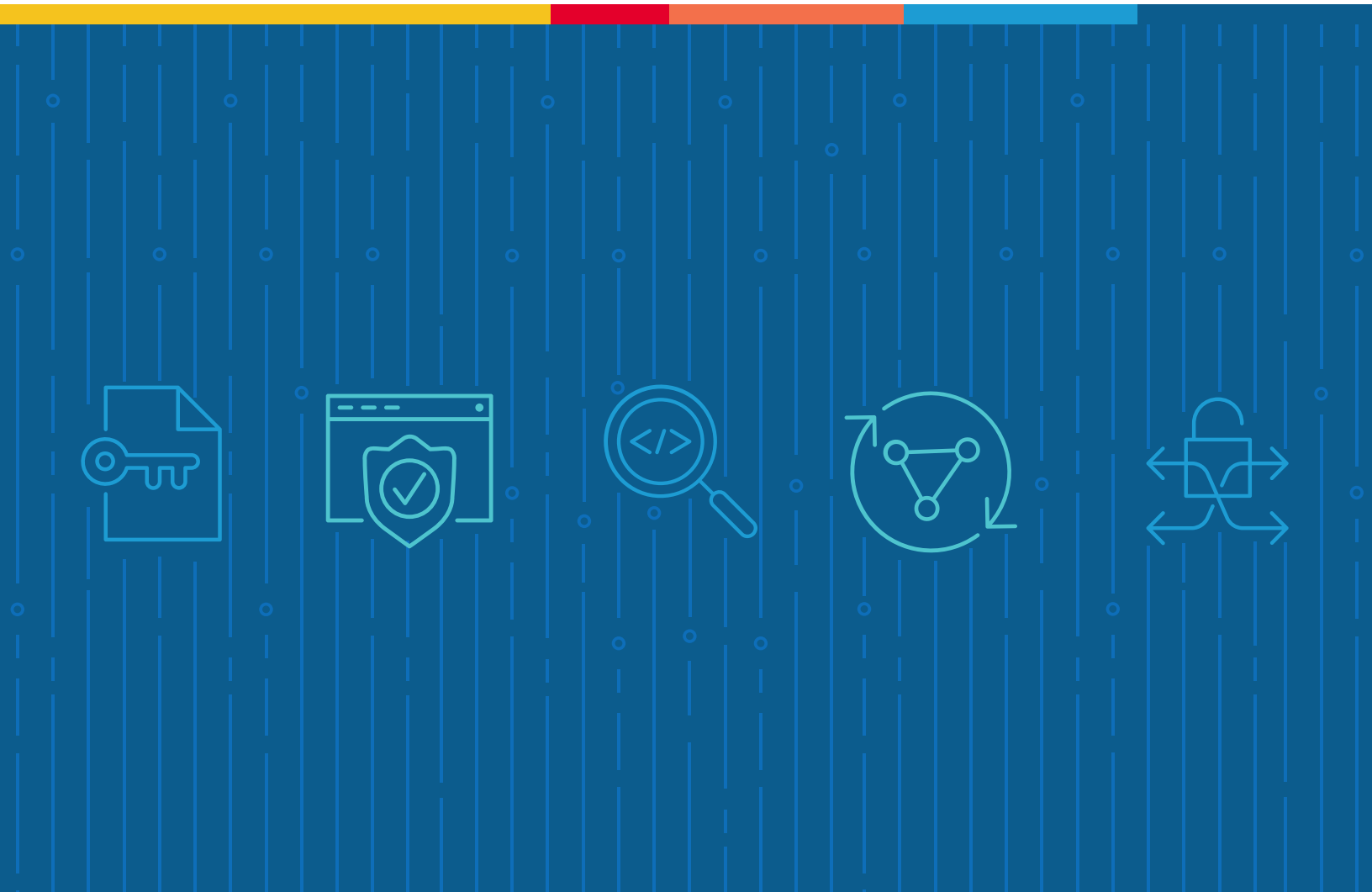


Table of Contents

3 Introduction

3 The F5 and Menlo Security Integrated Solution

4 SSL/TLS Visibility: How Do We Do it?

5 Dynamic Service Chaining

6 Topologies

6 License Components

7 Sizing

8 Traffic Exemptions for SSL/TLS Inspection

8 Best Practices for the Joint Solution

8 Architecture Best Practices

9 Security Best Practices

9 Certificate Requirements

9 IP Addressing

10 Initial Setup

10 Configure the VLANs and Self-IPs

10 Import a CA Certificate and Private Key

10 Update the BIG-IP SSL Orchestrator Version

11 Back Up Your F5 System Configuration

12 BIG-IP SSL Orchestrator Configuration

12 Guided Configuration

13 Guided Configuration Workflow

22 Dynamically Handling Egress Flows

24 Configuring the Per-Request Policy

27 Testing the Solution

28 Appendix

The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), are being widely adopted by organizations to secure IP communications. While SSL/TLS provides data privacy and secure communications, it also presents challenges for inspection devices within the security stack. In short, encrypted communications can't be seen as clear text and are passed through without inspection, resulting in security blind spots. This creates serious risks for businesses: What if attackers are hiding malware inside the encrypted traffic?

However, the process of performing decryption of SSL/TLS traffic on security inspection devices, even with native decryption support, can significantly degrade the performance of those devices. This is particularly true given the demands of stronger 2048-bit certificates.

An integrated F5 and Menlo Security solution solves these two SSL/TLS challenges. F5® BIG-IP® SSL Orchestrator® centralizes SSL/TLS inspection across complex security architectures, enabling flexible deployment options for decrypting and re-encrypting 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 Menlo Security Remote Browser Isolation, which can prevent previously hidden threats and block zero-day exploits. This solution eliminates the blind spots introduced by SSL/TLS and closes any opportunity for adversaries.

This overview of the joint F5 and Menlo Security solution describes different deployment modes with reference to service chain architectures, recommends practices, and offers guidance on how to handle enforcement of corporate Internet use policies.

The F5 and Menlo Security Integrated Solution

The F5 and Menlo Security integrated solution enables organizations to intelligently manage SSL/TLS 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/TLS visibility, it's impossible to identify and prevent such threats at scale.

Key highlights of the joint solution include:

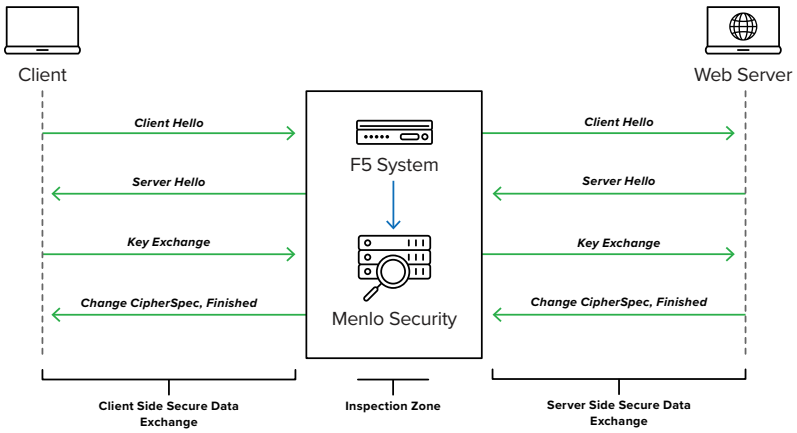
- **Flexible deployment modes** that easily integrate into even the most complex architectures, consolidate the security stack to reduce complexity, and deliver SSL/TLS visibility across the security infrastructure.

- **Centralized SSL/TLS decryption/re-encryption** with best-in-class SSL/TLS 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, thus determining 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 the perfect forward secrecy (PFS)-enabled ciphers, to ensure full traffic visibility.
- **Natively integrated security technologies** that leverage a single-pass prevention architecture to exert positive control based on applications, users, and content to reduce the organization's attack surface.
- **Automated creation and delivery of protection mechanisms** to defend against new threats to network, cloud, and endpoint environments.
- **Threat intelligence sharing** that provides protection by taking advantage of the network effects of a community of comprehensive, global threat data to minimize the spread of attacks.

SSL/TLS VISIBILITY: HOW DO WE DO IT?

F5's industry-leading full proxy architecture enables BIG-IP SSL Orchestrator to install a decryption/clear text zone between the client and web server, creating an aggregation (and disaggregation) visibility point for security services. The F5 system establishes two independent SSL/TLS connections—one with the client and the other with the web server. When a client initiates an HTTPS connection to the web server, BIG-IP SSL Orchestrator intercepts and decrypts the client-encrypted traffic and steers it to a pool of Menlo Security Remote Browser Isolation 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

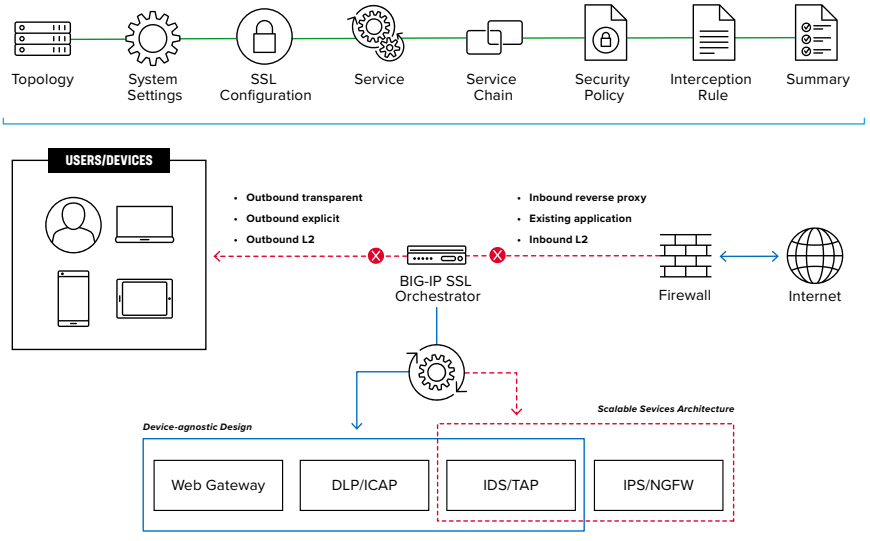


DYNAMIC SERVICE CHAINING

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 (IDSs/IPSs), web application firewalls (WAFs), 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.

BIG-IP SSL Orchestrator not only decrypts the encrypted traffic, but it also load balances, monitors, and dynamically chains security services, including next-generation firewalls (NGFWs), data loss prevention (DLP), IDSs/IPSs, WAFs, 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



The powerful classification engine of BIG-IP SSL Orchestrator applies different service chains based on context derived from:

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

TOPOLOGIES

Different environments call for different network implementations. While some can easily support SSL/TLS visibility at layer 3 (routed), others may require these devices to be inserted at layer 2. BIG-IP 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 BIG-IP SSL Orchestrator product line—the i2800, r2800, i4800, r4800, i5800, r5800, i10800, r10800, r10900, i11800, i15800, and Virtual Edition High Performance (HP)—supports this joint solution. The F5® VIPRION® platform and the F5® VELOS® platform are also supported. BIG-IP SSL Orchestrator devices ship with an installed base module that provides both SSL/TLS interception and service chaining capabilities. Please contact your local F5 representative to further understand the licensing and deployment options.

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

Optionally, customers can add the functionality of:

- An **F5 URLF subscription** to access the URL category database.
- An **F5® IP Intelligence Services subscription** for IP reputation service.
- A network **hardware security module (HSM)** to safeguard and manage digital keys for strong authentication.

- **F5® Secure Web Gateway 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.
- **F5® BIG-IP® Advanced Firewall Manager™ (AFM)** to protect against denial-of-service.
- **F5® BIG-IP® Advanced WAF®** to protect against common vulnerabilities (CVEs) and web exploits, targeted attacks, and advanced threats.
- **An F5® BIG-IP® Local Traffic Manager™ (LTM)** add-on software license mode. This solution's supported on all F5® BIG-IP® iSeries® and older F5 hardware platforms and has no specific restrictions on additional F5 software modules (including the above software services). This option's suited for environments that need to deploy BIG-IP SSL Orchestrator on an existing BIG-IP device or have other functions that must run on the same device.

SIZING

The main advantage of deploying BIG-IP SSL Orchestrator in the corporate security architecture is that the wire traffic now can be classified as "interesting" traffic, which needs to be decrypted by BIG-IP SSL Orchestrator for inspection by Menlo Security Remote Browser Isolation, and "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 Menlo Security Remote Browser Isolation conserves its valuable resources (as it need not inspect the entire wire traffic), maximizing performance.

As a result, it's important to consider the entire wire traffic volume to calculate the appropriate F5 system size. Menlo Security Remote Browser Isolation will require one interface on the F5 system to allow traffic flow through logical inbound and outbound service interfaces.

Refer to the BIG-IP SSL Orchestrator data sheet and consider the following factors when sizing the F5 system for the integrated solution:

- Port density.
- SSL/TLS bulk encryption throughput.
- System resources.
- The number of security services and devices in them.

TRAFFIC EXEMPTIONS FOR SSL/TLS 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 can't be decrypted) to be exempted from inspection may include:

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

You can also exempt traffic based on domain names and URL categories. The policy rules of BIG-IP SSL Orchestrator 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
- Healthcare
- Government services

Best Practices for the Joint Solution

Several 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 that optimizes performance, reliability, and security, F5 recommendations include:

- Deploy inline. Any SSL/TLS visibility solution must be inline to the traffic flow to decrypt PFS cipher suites such as elliptic curve Diffie-Hellman encryption (ECDHE).
- Deploy BIG-IP SSL Orchestrator in a device sync/failover device group (S/FDG) that includes the high-availability (HA) pair with a floating IP address.

- 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/TLS 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 BIG-IP SSL Orchestrator is integrated into the security architecture, all traffic to a security device is decrypted—including usernames, passwords, and social security and credit card numbers. It's therefore highly recommended that security services be isolated within a private, protected enclave defined by BIG-IP SSL Orchestrator. It's technically possible to configure BIG-IP SSL Orchestrator to send decrypted traffic anywhere reachable by the routing setup, but this high-risk practice should be avoided.

CERTIFICATE REQUIREMENTS

Different certificate requirements apply depending on the traffic flow direction.

Outbound traffic flow (internal client to Internet)
An SSL/TLS 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 don't encounter certificate errors when accessing SSL/TLS-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/TLS orchestration is similar to traditional reverse web proxy SSL/TLS handling. At a minimum, it requires a server certificate and an associated private key that matches the host name external users are trying to access. This could be a single instance certificate or a wildcard or subject alternative name (SAN) certificate if inbound SSL/TLS orchestration is defined as a gateway service.

IP ADDRESSING

When Menlo Security Remote Browser Isolation is deployed as an explicit proxy, F5 recommends configuring its IP address from default fixed addressing subnets. These subnets are provided by BIG-IP SSL Orchestrator and derived from an RFC2544 CIDR block of 198.19.0.0 to minimize the likelihood of address collisions.

For example, a Menlo Security Remote Browser Isolation platform can be configured to use the IP address 198.19.0.61/25 pointing to the BIG-IP SSL Orchestrator-connected interfaces. Static routes may also need to be configured for proper routing.

Initial Setup

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

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 and 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/TLS 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 SSL/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/TLS certificates for F5 systems to understand the procedure.

UPDATE THE BIG-IP SSL ORCHESTRATOR VERSION

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

1. Visit downloads.f5.com. You'll 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 3: The F5 product download web page

4. Select and download the latest version of the BIG-IP SSL Orchestrator .rpm file.
5. Read the appropriate Release Notes before attempting to use the file.
6. Log into the F5 system. On the F5 web UI in 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 .rpm file you downloaded. Select it and click **Open**.
8. Click **Upload and Install**.

You are now ready to proceed to detailed configuration.

BACK UP YOUR F5 SYSTEM CONFIGURATION

Before beginning detailed BIG-IP SSL Orchestrator configuration, we strongly recommend you back up the F5 system configuration using the following steps. This enables you to restore the previous configuration in case any issues arise.

1. From the main tab of the F5 management interface, click **System** > **Archives**.
2. To initiate the process of creating a new UCS archive (backup), click **Create**.
3. Enter a unique **File Name** for the backup file.
4. Optional:

- If you want to encrypt the UCS archive file, from the **Encryption** menu, select **Enabled** and enter a passphrase. You must supply the passphrase to restore the encrypted UCS archive file.
- If you want to exclude SSL/TLS private keys from the UCS archive, from the **Private Keys** menu, select **Exclude**.

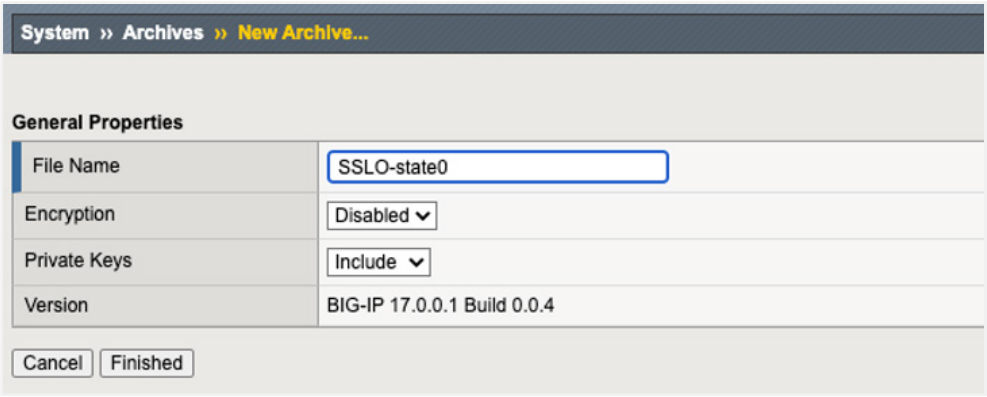


Figure 4: New system archive creation

5. Click **Finished** to create the UCS archive file.

6. When the backup process is done, examine the status page for any reported errors before proceeding to the next step.
7. Click **OK** to return to the **Archive List** page.
8. Copy the .ucs file to another system.

To restore the configuration from a UCS archive, navigate to **System** > **Archives**. Select the name of the UCS file you want to restore and click **Restore**. For details and other considerations for backing up and restoring the F5 system configuration, see this article on MyF5: K13132: Backing up and restoring BIG-IP configuration files with a UCS archive.

BIG-IP SSL Orchestrator Configuration

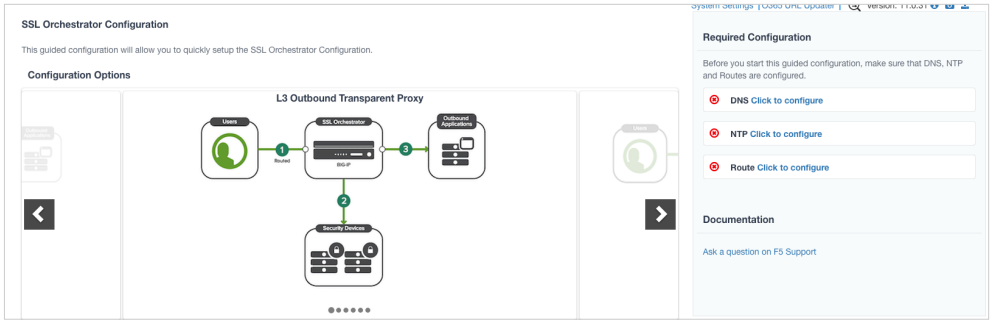
Menlo Security Remote Browser Isolation is configured as an explicit proxy service in BIG-IP SSL Orchestrator. The sample configuration below will focus on a traditional outbound (forward proxy) use case with Menlo Security configured as an explicit proxy service. BIG-IP SSL Orchestrator steers the unencrypted and decrypted web traffic through the pool, which is part of one or more service chains of security devices.

GUIDED CONFIGURATION

The BIG-IP SSL Orchestrator guided configuration presents a completely new and streamlined user experience. This workflow-based architecture provides intuitive, reentrant configuration steps tailored to a selected topology. These steps 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 BIG-IP SSL Orchestrator guided configuration will provide an opportunity to define DNS and route settings later in the workflow. Only NTP isn't addressed later.
4. No other configurations are required in this section, so click **Next**.

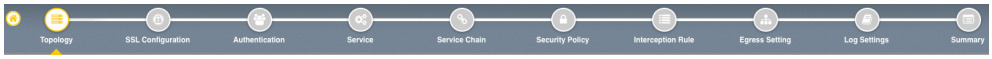
Figure 5: The initial guided configuration page



GUIDED CONFIGURATION WORKFLOW

The first stage of the guided configuration addresses topology.

Figure 6: The guided configuration workflow



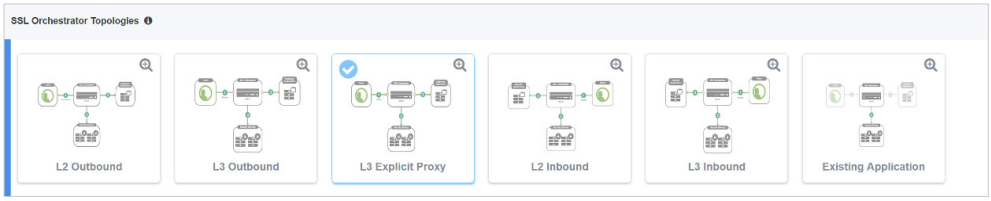
Topology properties

1. BIG-IP 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 this guidance:

Topology Properties	User Input
NAME	Enter a **Name** for the BIG-IP SSL Orchestrator deployment.
DESCRIPTION	Enter a **Description** for the service.
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. Figure 7 and the sample configuration here demonstrate this option.
IP FAMILY	Specify whether you want this configuration to support **IPv4** addresses or **IPv6** addresses.

Topology Properties Cont.	User Input Cont.
BIG-IP SSL ORCHESTRATOR TOPOLOGIES	The BIG-IP SSL Orchestrator Topologies option page presents six topologies: • **L3 explicit proxy:** The traditional explicit forward proxy. The sample configuration presented here uses this topology. • **L3 outbound:** The traditional transparent forward proxy. • **L3 inbound:** A reverse proxy configuration. • **L2 inbound:** Provides a transparent path for inbound traffic flows, inserting BIG-IP SSL Orchestrator as a bump-in-the-wire in an existing routed path, where BIG-IP SSL Orchestrator presents no IP addresses on its outer edges. • **L2 outbound:** Provides a transparent path for outbound traffic flows, inserting BIG-IP SSL Orchestrator as a bump-in-the-wire in an existing routed path, where BIG-IP SSL Orchestrator presents no IP addresses on its outer edges. • **Existing application:** Designed to work with existing BIG-IP LTM applications that already perform their own SSL/TLS handling and client-server traffic management. The existing application workflow proceeds directly to service creation and security policy definition, then exits with a BIG-IP 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 BIG-IP SSL Orchestrator as an L3 explicit proxy for decrypting outbound SSL/TLS traffic. See Figure 7.

Figure 7: Sample topology configuration



2. Click **Save & Next**.

SSL configuration

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

Figure 8: SSL configuration in the workflow

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

SSL Configuration	User Input
SSL/TLS PROFILE	
NAME	Enter a **Name** for the SSL/TLS profile.
DESCRIPTION	Enter a **Description** for this SSL/TLS profile.
CLIENT-SIDE SSL/TLS	
CIPHER TYPE	The cipher type can be a **Cipher Group** or **Cipher String**. The latter's 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 SSL/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/TLS 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 and leave the Passphrase field empty, then click **Add**.
CA CERTIFICATE KEY CHAINS	An SSL/TLS 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 CA certificates and keys that were imported, then click **Add**.
SERVER-SIDE SSL/TLS	
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's expired.
UNTRUSTED CERTIFICATE RESPONSE CONTROL	Select drop or ignore the connection even if the specified CRL file isn't trusted.
OCSP	Specify the supported **OCSP**.
CRL	Specify the supported **CRL**.

3. Click **Save & Next**.

Note: SSL/TLS settings minimally require an RSA-based template and CA certificates but can also support elliptic curve (ECDSA) certificates. In this case, BIG-IP SSL Orchestrator would forge an EC certificate to the client if the SSL/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 Menlo Security service

The Menlo Security service is configured as an L3 explicit proxy.

Configuring as an L3 explicit proxy service

The Services List section defines the security services that interact with BIG-IP SSL Orchestrator. The guided configuration includes a services catalog that contains common product integrations. Beneath each of these catalog options is one of these 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 service:

1. Under **Service List**, click **Add Service**.
2. In the service catalog, double click **Menlo Security** service. (If the version of BIG-IP SSL Orchestrator you're using doesn't have this option, then use the generic HTTP service.) The **Service Properties** page displays.
3. Configure the service using the guidance below. To configure either as an L3 or TAP service, refer to the next two sections of this document.

Service Properties	User Input
SERVICE SETTINGS	
NAME	Enter a **Name** for the Menlo Security service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters aren't case sensitive.
DESCRIPTION	Enter a **Description** for the service.
NETWORK CONFIGURATION	Click **Add**. Then, create the **From VLAN** and **To VLAN** pairs (these are often the same for explicit proxy) by entering a name and selecting the interface. These VLAN pairs and the associated interfaces define the network connectivity between BIG-IP SSL Orchestrator and the Menlo Security device. If you have configured BIG-IP 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 multiple Menlo Security devices are involved, choose the respective VLAN pair and click **Add**. Enter the desired ratio for every Menlo Security in the pool to control the load it receives.

Service Properties Cont.	User Input Cont.
SERVICE DOWN ACTION	Specify how the system should handle a failure of the explicit proxy service or times when it's 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 an RST on the client connection for TCP traffic. For UDP traffic, this action is the same.
IRULES	BIG-IP SSL Orchestrator allows for the insertion of additional F5® iRules® logic at different points, but additional iRules aren't required. An iRule defined at the service only affects traffic flowing across this service. It's important to understand, however, that these iRules mustn't 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 the service chain setup.

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

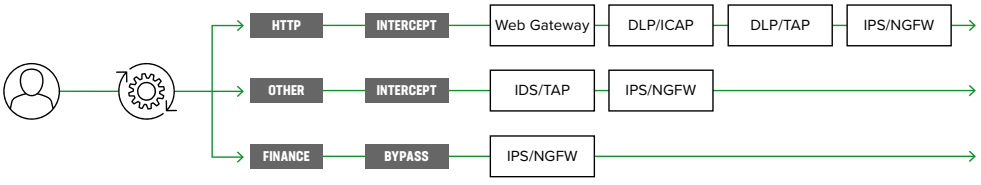
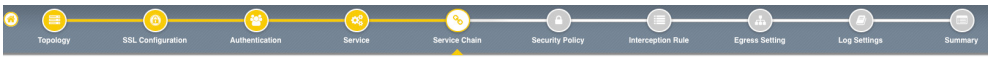


Figure 10: Different traffic flowing through chains of different security services

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 the configured security services:

1. Under **Services List**, click **Add Service**. Make selections using this guidance:

Service Chain Properties	User Input
NAME	Enter a **Name** for the per-request service chain.
DESCRIPTION	Enter a **Description** for this service chain.
SERVICES	Select any number of desired services 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's processed in BIG-IP SSL Orchestrator. The actions a rule can require include:

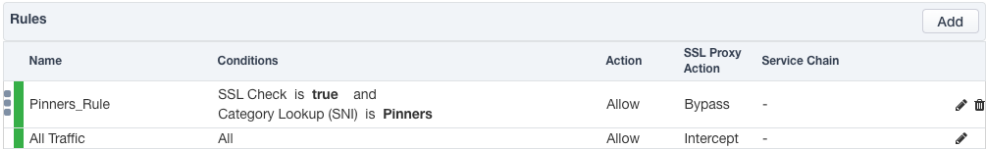
- Whether or not to allow the traffic indicated in the rule.
- Whether or not to decrypt that traffic.
- Which service chain (if any) to pass the traffic through.

Figure 12: Configuring security policy

The guided configuration of BIG-IP SSL Orchestrator presents an intuitive, rule-based, drag-and-drop user interface for the definition of security policies. In the background, BIG-IP 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

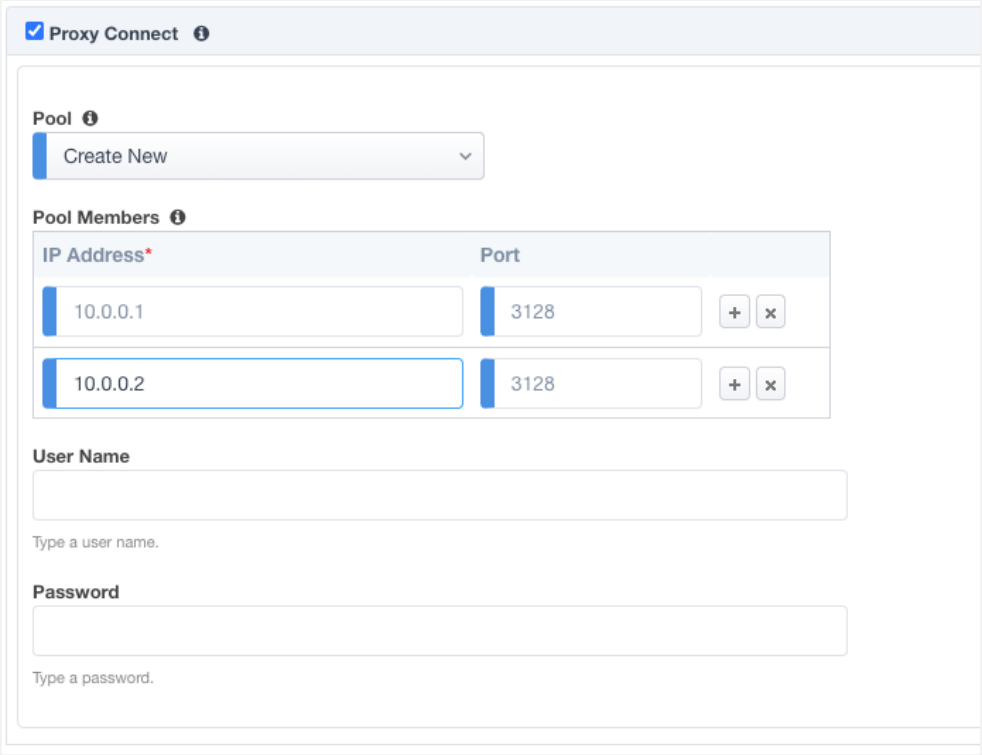


By default, BIG-IP SSL Orchestrator defines a single egress pool for transparent proxy traffic. For an upstream explicit proxy (that is, a "proxy chain"), however, BIG-IP SSL Orchestrator inserts two proxy select agents in the visual policy. Proxy chaining is configurable in the BIG-IP SSL Orchestrator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

1. Scroll down and click **Proxy Select**.
2. Click **Pool** and select **Create New**.
3. Add the IP address and port number for Menlo Security. Click + to add multiple IP addresses.
4. Click **Save & Next**.

Proxy Connect creates two proxy select agents in the visual policy. This will enable F5 proxy chaining with Menlo Security.

Figure 14: Enabling Proxy Connect



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/TLS settings, VLANs, IPs, and security policies created in the topology workflow.

Figure 15: Configuring interception rules

1. To configure the interception rule, follow this guidance:

Intercept Rule	User Input
LABEL	Enter a **Name** for the label.
DESCRIPTION	Enter a **Description** for this rule.
PROXY SERVER SETTINGS	This setting, which displays when configuring an explicit proxy, defines the BIG-IP 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 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 16: Configuring egress settings

1. To configure these characteristics, follow this guidance:

Egress Settings	User Input
MANAGE SNAT SETTINGS	Define if and how source NAT (SNAT) is 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.

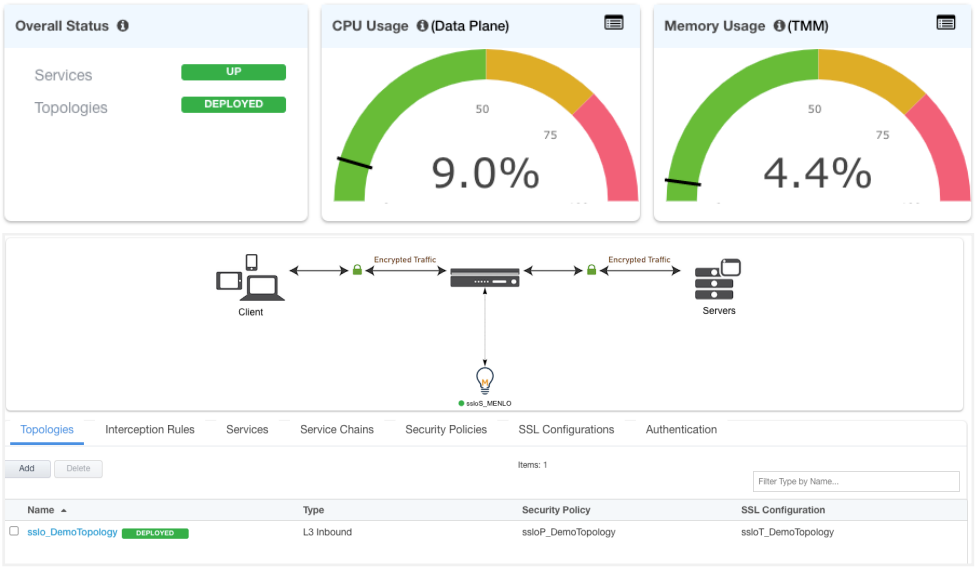
2. Once done, click **Save & Next**.

Configuration summary and deployment

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

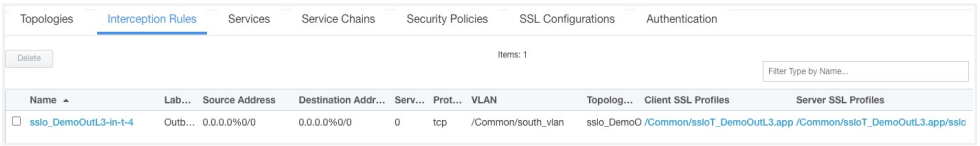
1. To review the details for any given setting, click the corresponding arrow icon on the far right.
2. To edit any given setting, click the corresponding pencil icon. Clicking the pencil icon will display the selected settings page in the workflow.
3. When you're satisfied with the defined settings, click **Deploy**. Upon successfully deployment of the configuration, BIG-IP SSL Orchestrator will display a dashboard. See Figure 17.

Figure 17: The configuration dashboard after deployment



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

Figure 18: The dashboard's Interception Rules tab



This completes configuration of BIG-IP 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.

Dynamically Handling Egress Flows

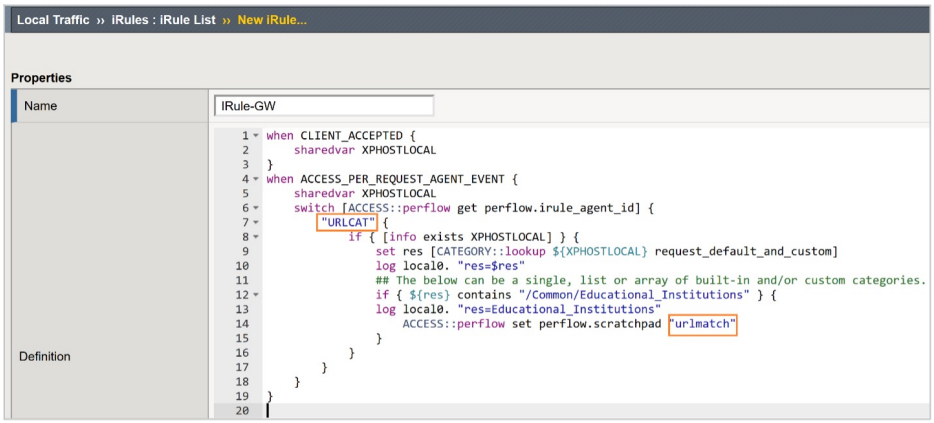
Administrators can customize and build policies to dynamically select the egress path based on URL category lookup. In this sample scenario, the default egress path is an upstream Menlo Security explicit proxy (that is, a proxy chain), except for **.edu** URLs, which must follow a different routed path.

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. Directly evaluating against a client/server IP or port can be achieved within the visual policy without using iRules. For any other case requiring categorization, some version of the iRule configuration below will be necessary.

iRules configuration

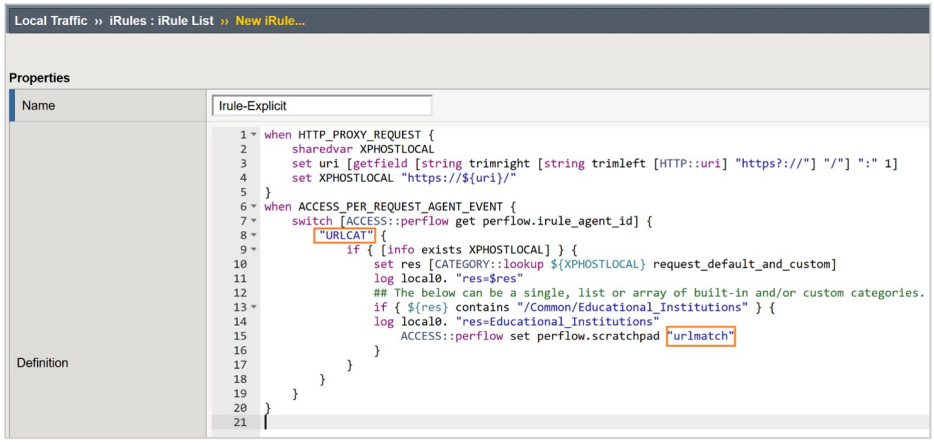
1. Create an iRule called **iRule-GW** that will collect the shared variable and perform a manual category lookup. If the category matches, a per-flow variable will be assigned. The object of the sample iRule below is to manually query a single or set of URL categories, and if matched, set a per-flow variable. The per-flow variable is read within the visual policy to direct traffic through or around proxy select agents. See Figure 19.

Figure 19: The iRule-GW iRule



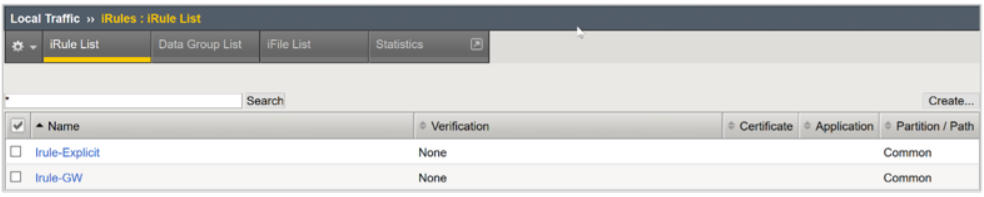
2. Create an iRule called **iRule-Explicit** that will grab the explicit proxy request URL from the client and save it to a shared variable. See Figure 20.

Figure 20: The iRule-Explicit iRule



3. Review the two iRules. (These samples can be found in the Appendix.) See Figure 21.

Figure 21: The two iRules

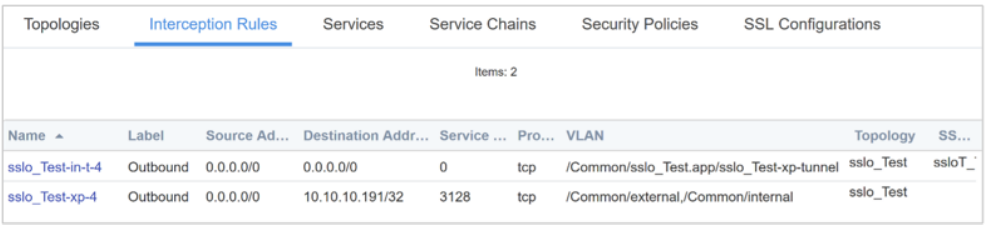


Modifying interception rules and disabling strictness

To modify interception rules and disable strictness, follow this guidance:

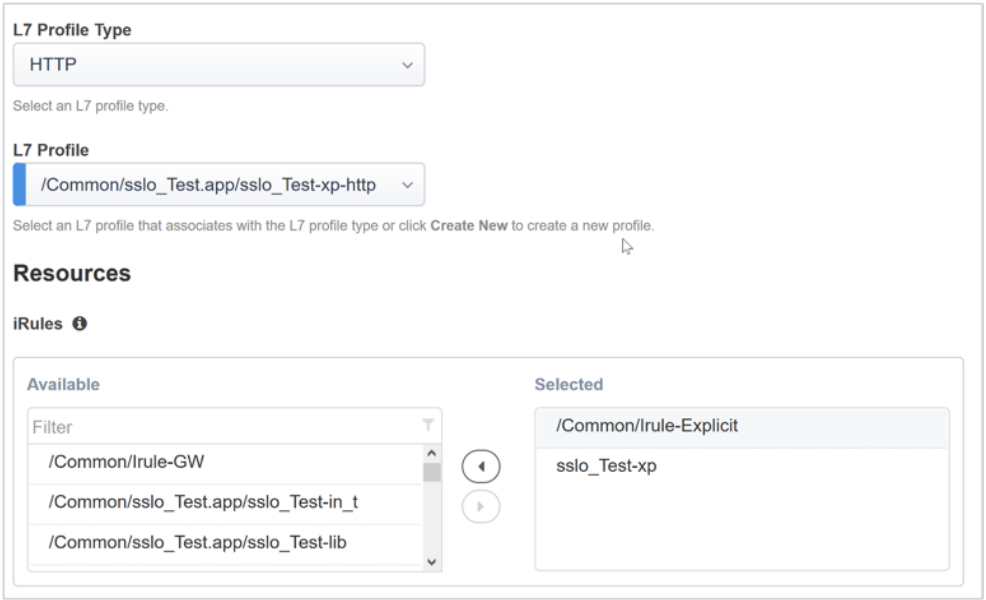
1. Navigate to **SSL Orchestrator > Configuration** and click **Interception Rules** (see Figure 22).

Figure 22: The Interception Rules



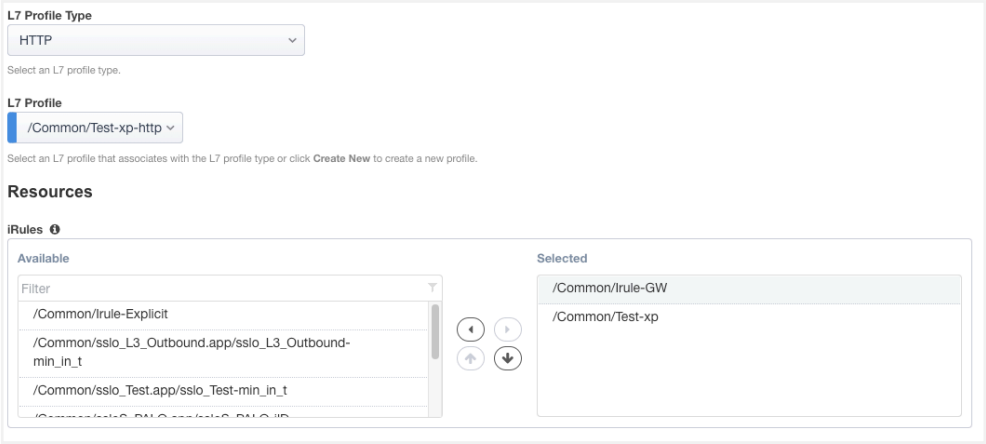
2. Set the L7 Profile Type to **HTTP**. Set the L7 Profile to **sslo_[appname]-xp-http**. Set the iRule to **iRule-Explicit** (see Figure 23).

Figure 23: The Profile and iRule settings



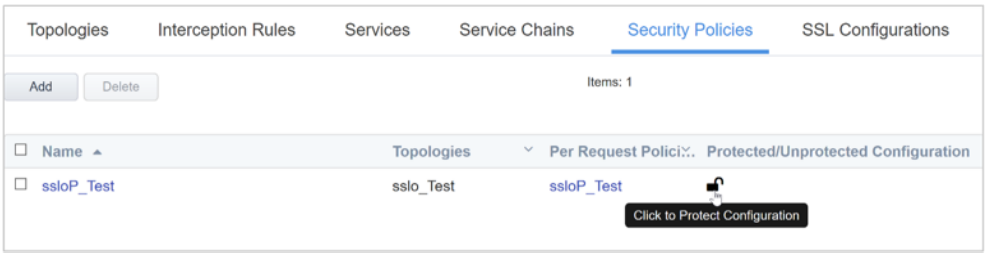
3. Modify the **-in-t** interception rule to the following setting: iRules: add **iRule-GW** (see Figure 24).

Figure 24: The -in-t interception rule



4. 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 BIG-IP SSL Orchestrator UI (see Figure 25).

Figure 25: The Security Policies



5. Select **Click to Protect Configuration**.

Configuring the Per-Request Policy

Proxy chaining support in the BIG-IP SSL Orchestrator security policy requires two agents.

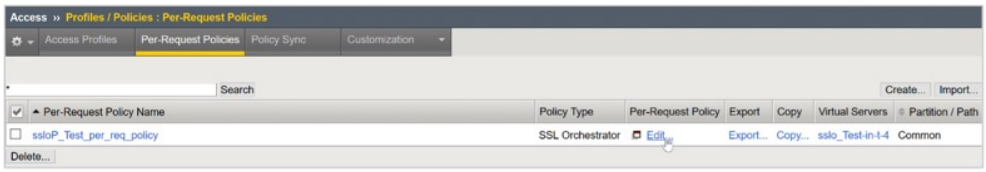
- A proxy-select agent, **Proxy Chaining (Connect)**, at the beginning of the policy that creates the initial outbound path.
- A separate proxy-select agent, **Proxy Chaining (URI Rewrite)**, at the end of the policy that appropriately rewrites the request to an upstream explicit proxy.

As the decision for the initial proxy selection must happen before any VPE categorization, manual categorization must be handled in an iRule based on the HTTP Connect URL entering the BIG-IP 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 (see Figure 26).

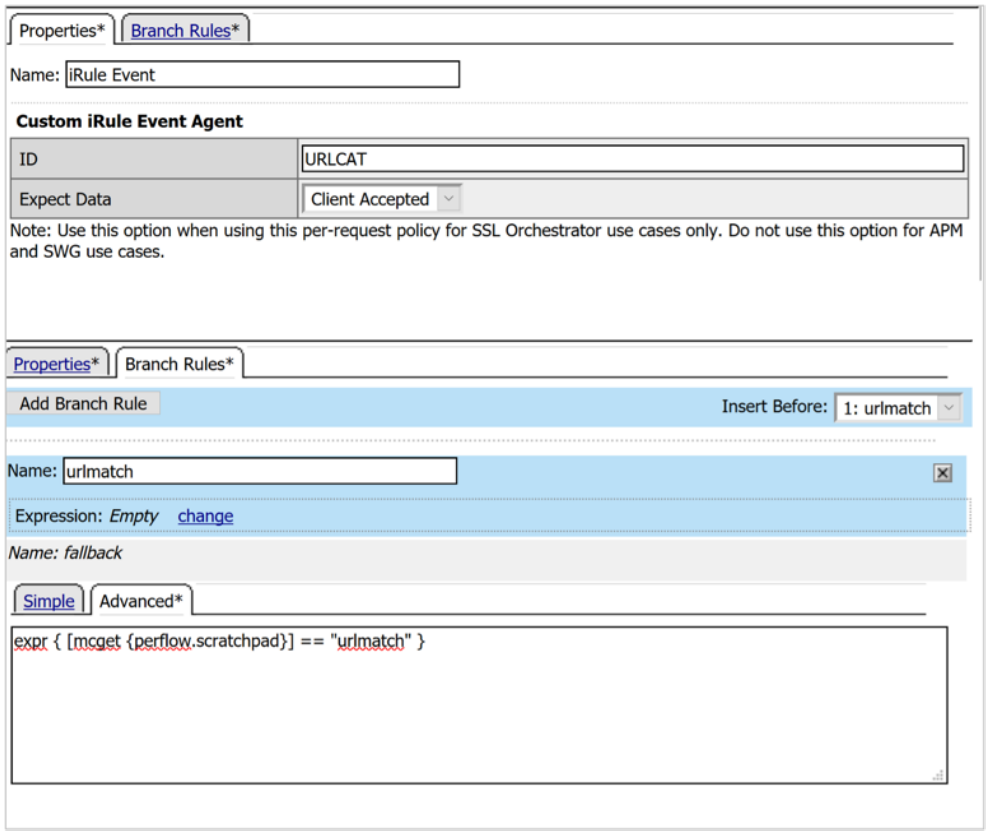
Figure 26: The Per-Request Policies



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 (see Figure 27):

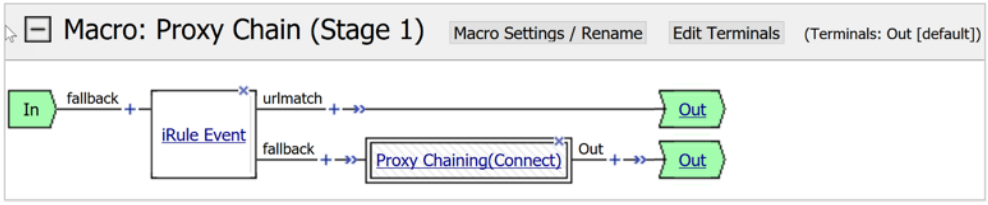
- Set the ID to **URLCAT**. Set Expect Data to **Client Accepted**. Set the Branch Rule Name to **urlmatch**. Click **Advanced** and, per Figure 27, enter **expr { [mcget {perflow.scratchpad}] == "urlmatch" }**.

Figure 27: The iRule Event



4. In the visual policy editor, include the **Proxy Chaining (Connect)** macro on the iRule agent's fallback branch (see Figure 28).

Figure 28: The visual policy editor

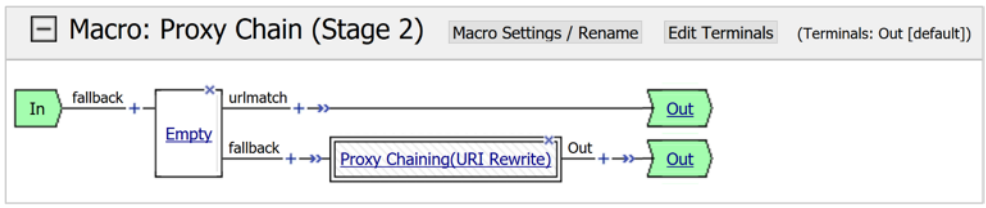


5. Create another macro called Proxy Chain (Stage 2).
6. Insert an Empty agent (found on the General Purpose tab) with the following settings:

- Branch Rule Name: **urlmatch**.
- Branch Rule Expression: **expr { [mcget {perflow.scratchpad}] == "urlmatch" }**.

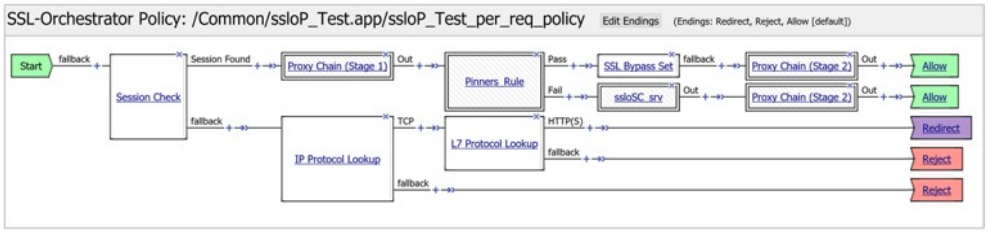
7. Include the Proxy Chaining (URI Rewrite) macro on the empty agent's fallback branch (see Figure 29).

Figure 29: The Proxy Chaining URL rewrite 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 (see Figure 30).

Figure 30: The main 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 SSL/TLS handshake enters the -in-t virtual server and activates the BIG-IP 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 URL's 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 BIG-IP SSL Orchestrator directs egress via proxy chaining to the upstream gateway.

Testing the Solution

Test the deployed solution using these 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's been issued by the local CA set up on the F5 system. This confirms that the SSL/TLS forward proxy functionality enabled by BIG-IP 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/TLS interception by the F5 device.

  ```
  tcpdump –lnni eth<n> -Xs0
  ```

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"
                }
            }
        }
    }
}
```