INTEGRATION GUIDE

BIG-IP SSL Orchestrator and OPSWAT MetaDefender ICAP Server

SSL/TLS Visibility with Service Chaining

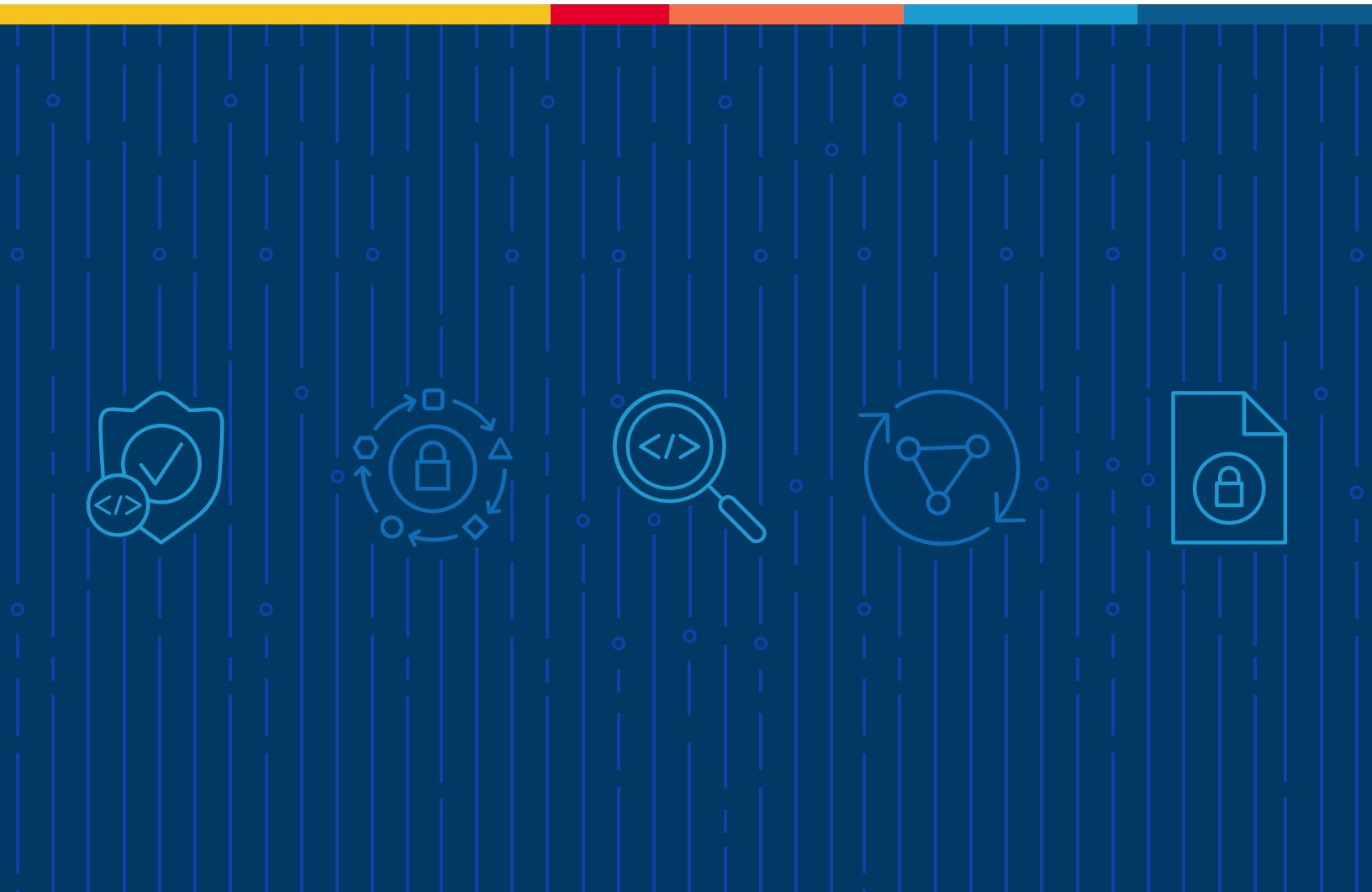


Table of Contents

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 creates challenges to inspection devices in the security stack. In short, the encrypted communications can't be seen as clear text and are passed through without inspection, becoming security blind spots. This creates serious risks for businesses: What if attackers are hiding malware inside the encrypted traffic?

However, performing decryption of SSL/TLS traffic on the security inspection devices, with native decryption support, can tremendously degrade the performance of those devices, especially given the demands of stronger, 2048-bit certificates.

An integrated F5 and OPSWAT MetaDefender 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 OPSWAT MetaDefender ICAP Servers, 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 OPSWAT 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 OPSWAT MetaDefender Integrated Solution

The F5 and OPSWAT MetaDefender 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 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 OPSWAT MetaDefender ICAP Servers 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.

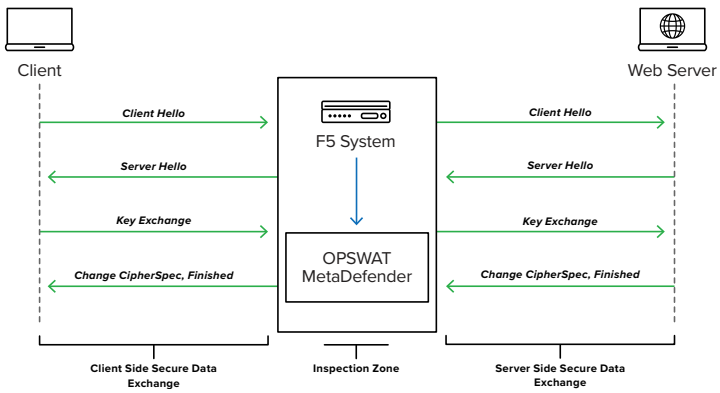


Figure 1: The F5 full proxy architecture

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.

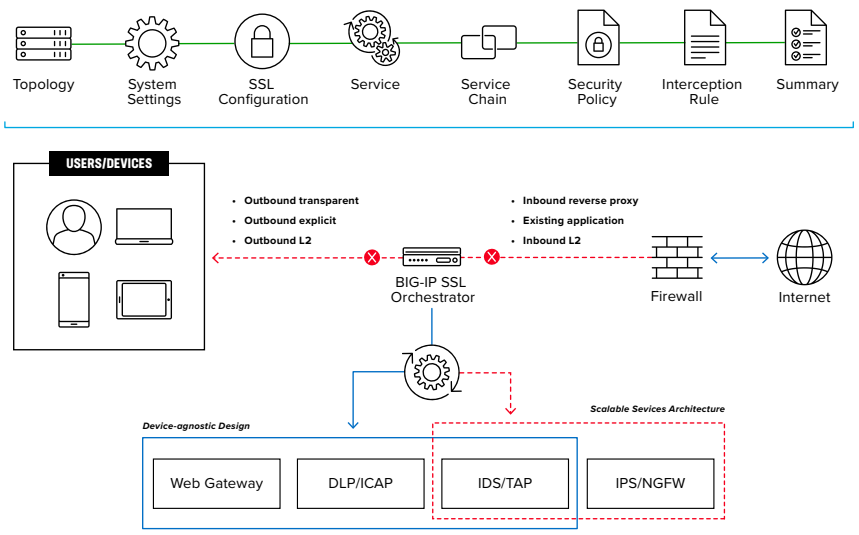


Figure 2: A service chain

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 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.

The following OPSWAT products and subscriptions are needed for deploying the solution:

- An **OPSWAT MetaDefender Core** for Advanced Threat Protection.
- An **OPSWAT MetaDefender ICAP** Server that includes ICAP capabilities.
- An **OPSWAT License**.

Refer to the OPSWAT technical documentation for complete guidance. (Administrators may need to be registered with appropriate privileges to access this resource.)

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 an OPSWAT MetaDefender ICAP Server, 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 the OPSWAT MetaDefender ICAP Server 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. The OPSWAT MetaDefender ICAP Server will require one interface on the F5 system to allow ICAP traffic to flow between them.

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 service chain.

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 like those for Microsoft Windows updates.

- Trusted backup solutions, such as a crash plan.
- Any lateral encrypted traffic to internal services that should be exempted.

Administrators 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
- Health care
- Government services

Best Practices for the Joint Solution

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

ARCHITECTURE BEST PRACTICES

Several best practices can help optimize the 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 that can be reached by the routing setup, but this is a high-risk practice that should be avoided.

CERTIFICATE REQUIREMENTS

Different certificate requirements apply depending on the 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 minimum, it requires a server certificate and associated private key that matches the host name that external users are trying to access. This may be a single instance certificate or a wildcard or subject alternative name (SAN) certificate if inbound SSL/TLS orchestration is defined as a gateway service.

IP ADDRESSING

When an OPSWAT MetaDefender ICAP Server is deployed, F5 recommends configuring its IP address from default fixed addressing subnets. These subnets are provided by BIG-IP SSL Orchestrator and derived from a RFC2544 CIDR block of 19819.0.0 to minimize the likelihood of address collisions.

For example, an ICAP Server can be configured to use the IP address 198.19.0.61/25 VLAN on the Service VLAN pointing to the BIG-IP SSL Orchestrator-connected interface. The table below explains the necessary IP addresses to configure when deploying multiple ICAP Servers in the service pool.

OPSWAT Metadata ICAP Server	ICAP Interface IP	ICAP Default Gateway
OPSWAT METADATA ICAP SERVER-1	198.19.0.61/25	Not needed
OPSWAT METADATA ICAP SERVER-2	198.19.0.62/25	Not needed
OPSWAT METADATA ICAP SERVER-N *N=<8*	198.19.0.6n/25	Not needed

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 plus self-IPs and routes. The VLANs define the connected interfaces, and the self-IPs define the respective IPv4 and/or IPv6 subnets. Refer to the F5 Routing Administration Guide for configuration steps to set up the VLANs and self-IPs.

IMPORT A CA CERTIFICATE AND PRIVATE KEY

For SSL/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 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 and log in with registered F5 credentials.
2. Click **Find a Download**.
3. Scroll to the **Security** product family, select **SSL Orchestrator**, and click the link.

Figure 3: The F5 product download web page

4. Select and download the 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.

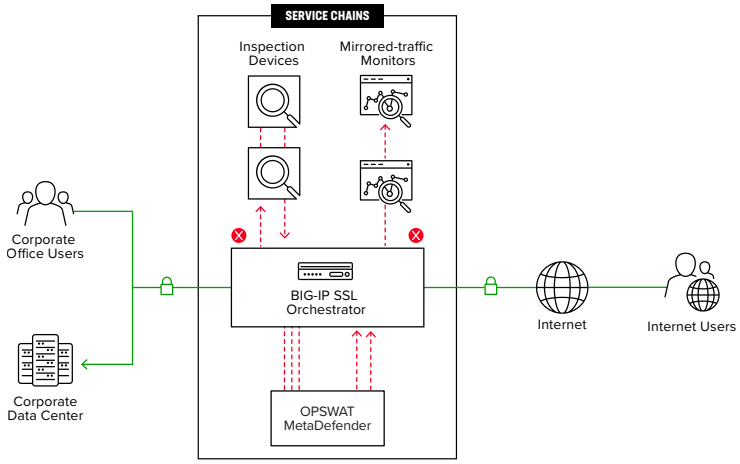
7. Click **Choose File** and navigate to the downloaded .rpm file. Select it and click Open.
8. Click **Upload and Install**.

Detailed configuration can now proceed.

BIG-IP SSL Orchestrator Configuration

An OPSWAT MetaDefender ICAP Server is configured as an ICAP Server service in BIG-IP SSL Orchestrator. The sample configuration below focuses on a traditional outbound (forward proxy) use case with OPSWAT MetaDefender ICAP Server configured as an ICAP service. (See Figure 4.) BIG-IP SSL Orchestrator steers the unencrypted and decrypted web traffic through the OPSWAT pool, which is part of one or more service chains of security devices.

Figure 4: A sample inline deployment architecture



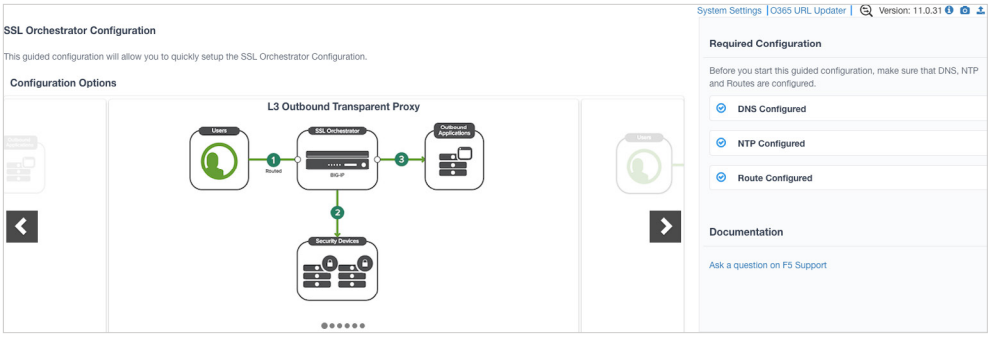
GUIDED CONFIGURATION

The BIG-IP SSL Orchestrator 10.1 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**.

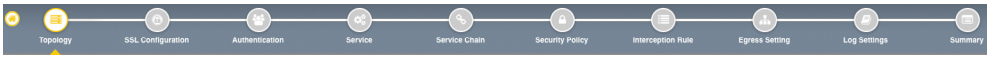
Figure 5: The initial guided configuration page



GUIDED CONFIGURATION WORKFLOW

The first stage of the guided configuration addresses topology.

Figure 6: The guided configuration workflow



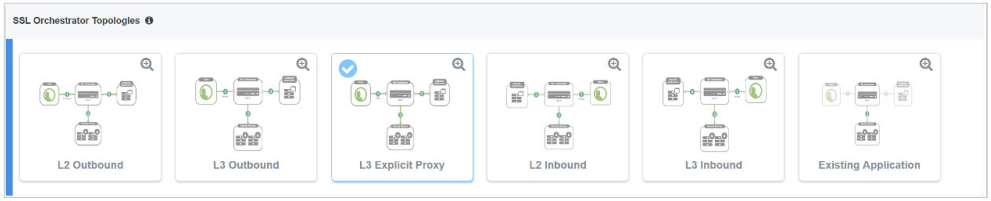
Topology properties

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	Type a **Name** for the BIG-IP SSL Orchestrator deployment.
DESCRIPTION	Type a **Description** for this BIG-IP SSL Orchestrator deployment.
PROTOCOL	The Protocol option presents four protocol types: • **TCP:** Creates a single TCP wildcard interception rule for the L3 inbound, L3 outbound, and L3 explicit proxy topologies. • **UDP:** Creates a single UDP wildcard interception rule for L3 inbound and L3 outbound topologies. • **Other:** Creates a single "any protocol" wildcard interception rule for L3 inbound and L3 outbound topologies. Typically used for non-TCP/UDP traffic flows. • **Any:** Creates the TCP, UDP, and non-TCP/UDP interception rules for outbound traffic flows. The sample configuration here demonstrates this option.
IP FAMILY	Specify whether the configuration should support **IPv4** addresses or **IPv6** addresses.

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: A 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 Configurations	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 OPSWAT MetaDefender service

The OPSWAT MetaDefender service needs to be configured as an ICAP Server.

Configuring as an ICAP 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: The service configuration

To configure the service:

1. Under **Service List**, click **Add Service**.
2. In the service catalog, double click **OPSWAT MetaDefender ICAP** service. (If the version of BIG-IP SSL Orchestrator you're using doesn't have this option, then use the generic ICAP service.) This option is available from the ICAP tab in newer versions. The **Service Properties** page displays.
3. Configure the service using the guidance below, which shows ICAP service configuration.

Service Properties	User Input
SSL/TLS PROFILE	
NAME	Enter a **Name** for the OPSWAT MetaDefender 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 OPSWAT MetaDefender service.
ICAP DEVICES	Under **ICAP Devices** click Add. Enter the IP address of the ICAP server and click Done. Repeat this step if multiple OPSWAT MetaDefenders are involved.
REQUEST MODIFICATION URI	Enter the **ICAP Request URI**: /OMSScanReq-AV.
RESPONSE MODIFICATION URI	Enter the **ICAP Response URI**: /OMSScanResp-AV.
SERVICE DOWN ACTION	Specify how the system should handle a failure of the ICAP 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.

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

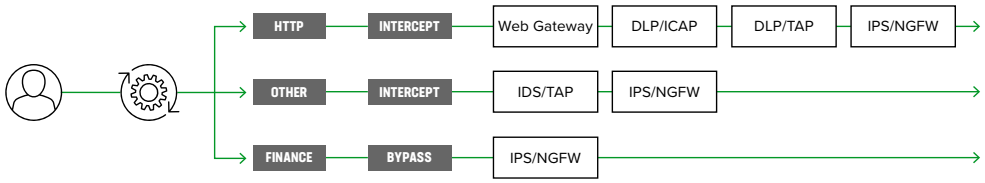


Figure 10: Different traffic flowing through chains of different security services

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	Type a **Name** for the per-request service chain.
DESCRIPTION	Provide 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**.

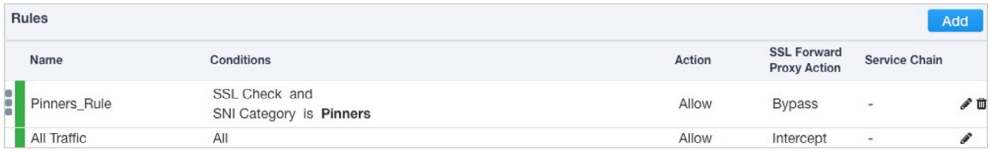


Figure 13: Configuring security policy

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 14: Configuring interception rules

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

Intercept Rule	User Input
LABEL	Enter a **Name** for the label.
DESCRIPTION	Enter a **Description** for this rule.
SOURCE ADDRESS	Specify the source address of the connection.
DESTINATION ADDRESS/MASK	Specify the destination address/mask of the connection.
PORT	Specify the port of the connection.
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. Once done, Click **Save & Next**.

Egress setting

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

Figure 15: Configuring egress settings

1. To configure these characteristics, follow this guidance:

Engress 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 to display the settings page in the workflow.
3. When the desired settings have been defined, click **Deploy**. Upon successful deployment of the configuration, BIG-IP SSL Orchestrator will display a dashboard. See Figure 16.

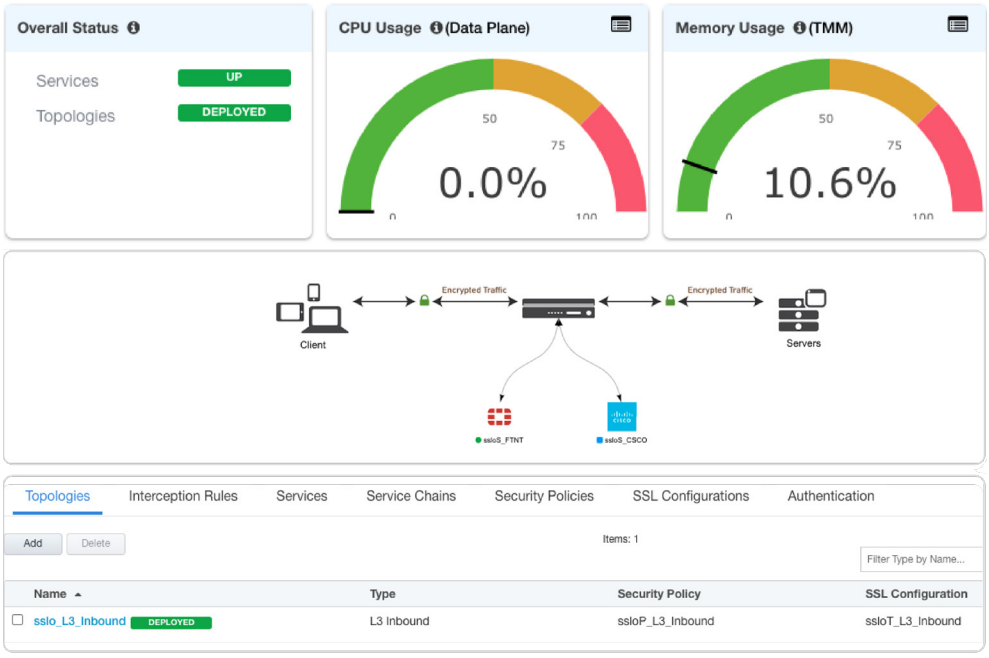


Figure 16: The configuration dashboard after deployment

This completes configuration of BIG-IP SSL Orchestrator as a Layer 3, Inbound proxy. At this point an external (internet) client should be able to browse to internal resources, and decrypted traffic will flow across the security services.

Testing the Solution

Test the deployed solution using the following 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
  ```

- **Decrypted traffic analysis on the OPSWAT MetaDefender ICAP Server:** From the web UI, go to Monitoring > Packet Capture > Create, and enable a Packet Filter. Create stages to capture packets, specify file names, and then click OK. Download the captured file(s) and analyze the HTTP packets. The packet header and payload should be in clear text, indicating SSL/TLS decryption. It's very important to turn off packet capture once the job completes.

DC 04.2023 | GUIDE-SEC-1083857230