INTEGRATION GUIDE

BIG-IP SSL Orchestrator and Symantec Data Loss Prevention

SSL/TLS Visibility and Content Adaptation

Table of Contents

The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), have been widely adopted by organizations to secure IP communications. But while SSL/TLS provides data privacy and secure communications, it also creates challenges to inspection devices such as data loss prevention (DLP) software in the security stack. In short, the encrypted communications cannot be seen as clear text and are passed through without inspection, becoming security blind spots. This creates serious risks, leaving organizations vulnerable to costly data breaches and loss of intellectual property. But today's security devices, such as intrusion prevention systems (IPSs) and next-generation firewalls (NGFWs), lack the processing power to easily decrypt SSL/TLS traffic. This performance concern becomes even more challenging with the demands of 2048-bit certificates.

An integrated F5® BIG-IP SSL Orchestrator® and Symantec Data Loss Prevention (DLP) solution solves these two SSL/TLS challenges across cloud, mobile, and on-premises environments. BIG-IP SSL Orchestrator centralizes SSL/TLS inspection across complex security architectures, providing flexible deployment options for decrypting and re-encrypting user traffic. It also provides intelligent traffic orchestration using dynamic service chaining and policy-based management. Once decrypted, the traffic is inspected by Symantec DLP, which can detect and block data breaches and exfiltration of sensitive data previously hidden by encryption. This joint solution thus eliminates the blind spots introduced by SSL/TLS and closes any opportunity for attackers.

This guide provides an overview of the joint solution, describes deployment with service chain architectures, and recommends reliable practices.

Solution Overview

Functional implementation of the solution involves both SSL/TLS visibility and content adaptation.

BIG-IP SSL Orchestrator, deployed inline to the wire traffic, intercepts any outbound secure web request and establishes two separate SSL/TLS connections, one each with the client (the user device) and the requested web server. This creates a decryption zone between them, providing SSL/TLS visibility for inspection.

Within the decryption zone, the content adaptation feature of BIG-IP SSL Orchestrator conditionally forwards both unencrypted HTTP and decrypted HTTPS requests by encapsulating them within Internet Content Adaptation Protocol (ICAP, RFC3507). These encapsulated requests go to a pool of Symantec DLP servers for inspection and possible

request modification (REQMOD). In this context, BIG-IP SSL Orchestrator is the ICAP client and Symantec DLP is the ICAP server. After inspection, user HTTPS requests are re-encrypted on their way to the web server.

The same process of decryption, inspection, possible response modification (RESPMOD), and re-encryption takes place for the return response from the web server to the client. See Figure 1.

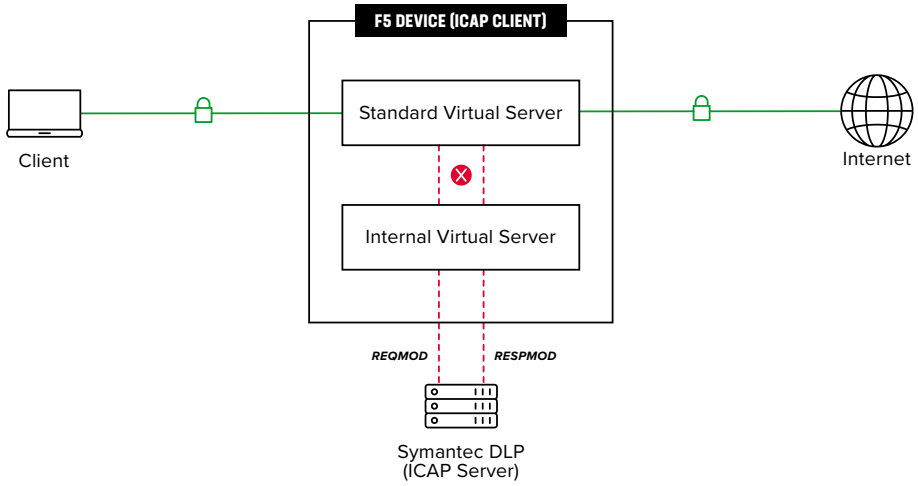


Figure 1: SSL/TLS interception and content adaption for modifying HTTP requests and responses

DYNAMIC SERVICE CHAINING

A typical security stack often consists of more than advanced anti-malware protection systems, with additional components such as a firewall, IDSs or intrusion prevention systems (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 NGFWs, DLPs, 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.

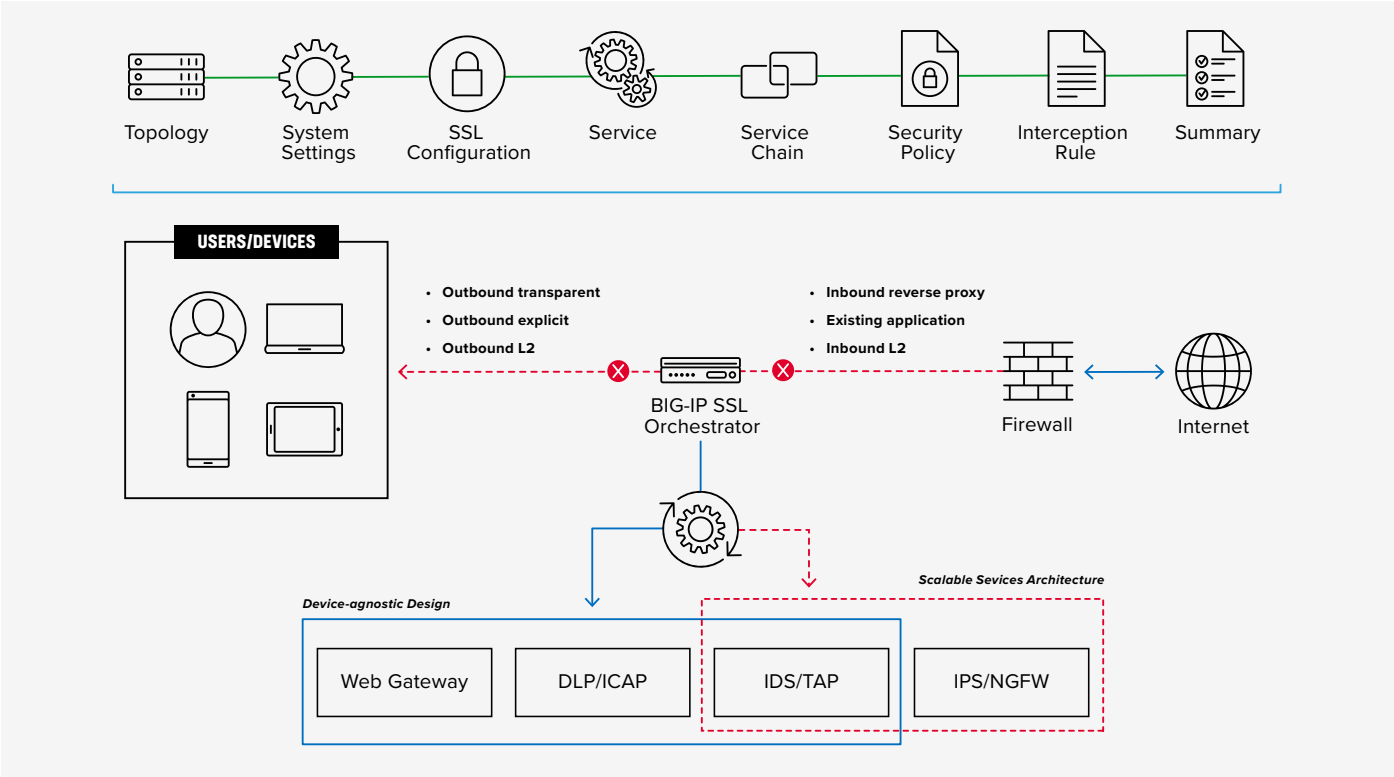


Figure 2: A service chain

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

- Source IP/subnet
- Destination IP/subnet
- An F5® IP Intelligence 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.

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 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.

To deploy this joint solution, administrators first must have installed Symantec DLP software version 14.5, Maintenance Pack 1 or higher. Symantec DLP software is composed of three components: Oracle Database, Enforce Server, and a detection server. It supports three different installation types:

- **Single-tier:** In single-tier installation, the Oracle Database, Enforce Server, and detection server are all installed on the same server. This is a common installation for testing or risk assessment.
- **Two-tier:** The Oracle Database and Enforce Server are on the same server, with a separate detection server.
- **Three-tier:** The Oracle Database, Enforce Server, and detection server are each on a separate server.

Refer to the Symantec DLP technical documentation for complete guidance. (You may need to be registered with appropriate privileges to access resources on the Symantec website.)

ARCHITECTURE BEST PRACTICES

A number of best practices can help ensure a streamlined architecture that optimizes performance and reliability, as well as security. F5 recommendations include:

- Deploy inline. Any SSL/TLS visibility solution must be inline to the traffic flow to decrypt perfect forward secrecy (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.
- Use dual-homing. The Symantec DLP server must be dual-homed on the inward and outward VLANs with each BIG-IP system in the device S/FDG.
- Achieve further interface redundancy with the Link Aggregation Control Protocol (LACP). LACP manages the connected physical interfaces as a single virtual interface (aggregate group) and detects any interface failures within the group.

SECURITY BEST PRACTICES

SSL/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. With an integrated BIG-IP SSL Orchestrator solution, all traffic to a security device is decrypted—including user names, passwords, and social security and credit card numbers. It is therefore highly recommended that security services be isolated within a private, protected enclave defined by BIG-IP SSL Orchestrator. It is technically possible to configure BIG-IP SSL Orchestrator to send the decrypted traffic anywhere that it can route to, but this is a dangerous practice that should be avoided.

Initial Setup

Complete these initial steps before performing detailed configuration of BIG-IP SSL Orchestrator. In addition, refer to the Symantec DLP documentation.

CREATE A POLICY ON THE SYMANTEC DLP

Log in to the web UI of the Symantec DLP Enforce Server. Before creating a policy, add the DLP monitor to the Enforce Server:

Add the monitor

1. Navigate to **System > Server and Detectors** and click **Add Server** at the top.
2. Select **Network & Mobile Prevent for Web** for ICAP integration with the F5 system, and then click **Next**.
3. Enter a **Name** and **Host**. If you're creating a single-tier Symantec DLP installation, the host is *localhost*.
4. The default **Request Filtering** and **Response Filtering** options direct the solution to ignore and not inspect content smaller than 4096 bytes. We recommend carefully considering these values. (If you set them too high, the DLP may ignore potentially important content.) Then select or enter your request and response filtering configuration values.

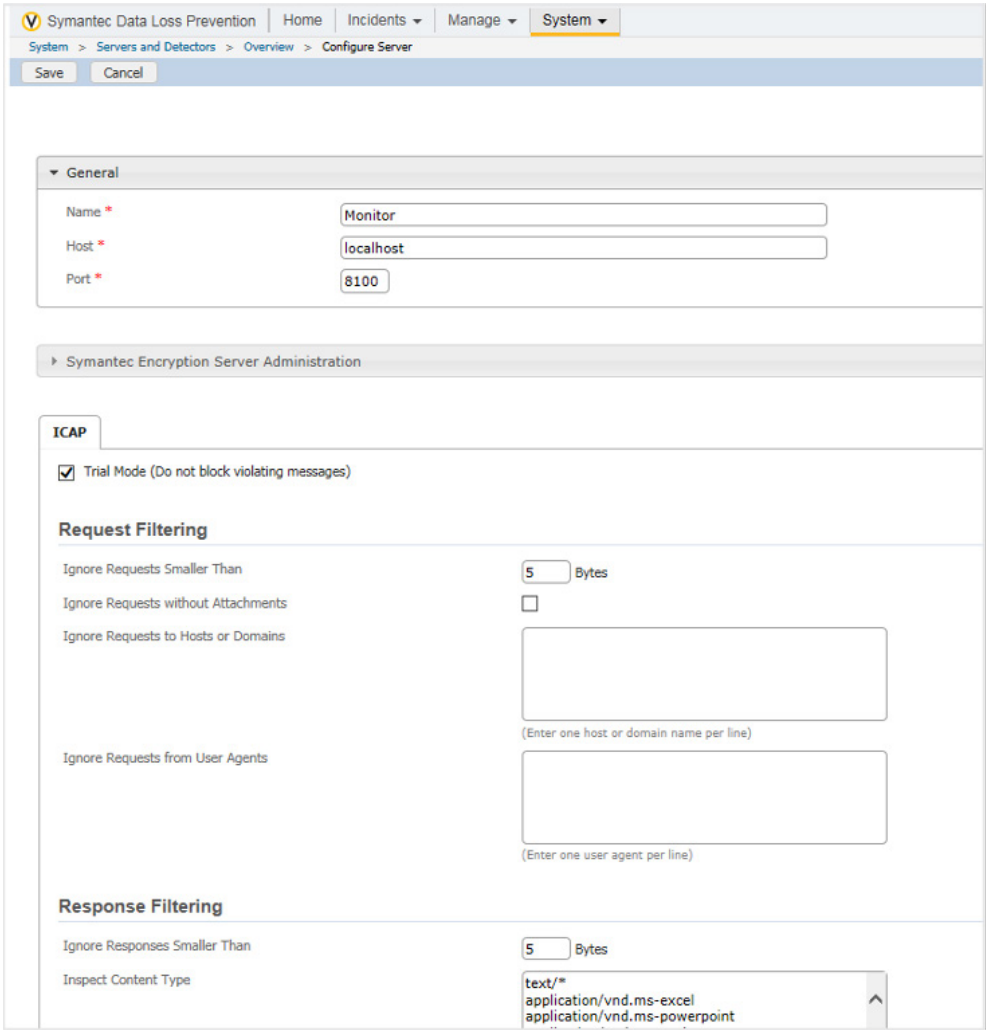


Figure 3: Adding the monitor to the Enforce Server

Create a policy

1. From the main menu, navigate to **Manage** > **Policies** > **Policy List**.
2. Click **Add Policy** and then click **Next**.
3. Under **Configure Policy**, enter the policy Name and click **Add Rule**.
4. Under **Add Detection Rule**, choose a **Rule Type** and click **Nex**t.
5. Under **Edit Rule**, enter the rule **Name** and matching criteria. Then click **OK**.
6. Once you're returned to the **Configure Policy** screen, click **Save**. See Figure 4 for sample configuration of a policy named *symconfidential* with a rule type of *Content Matches Keyword* and the keyword *confidential*.

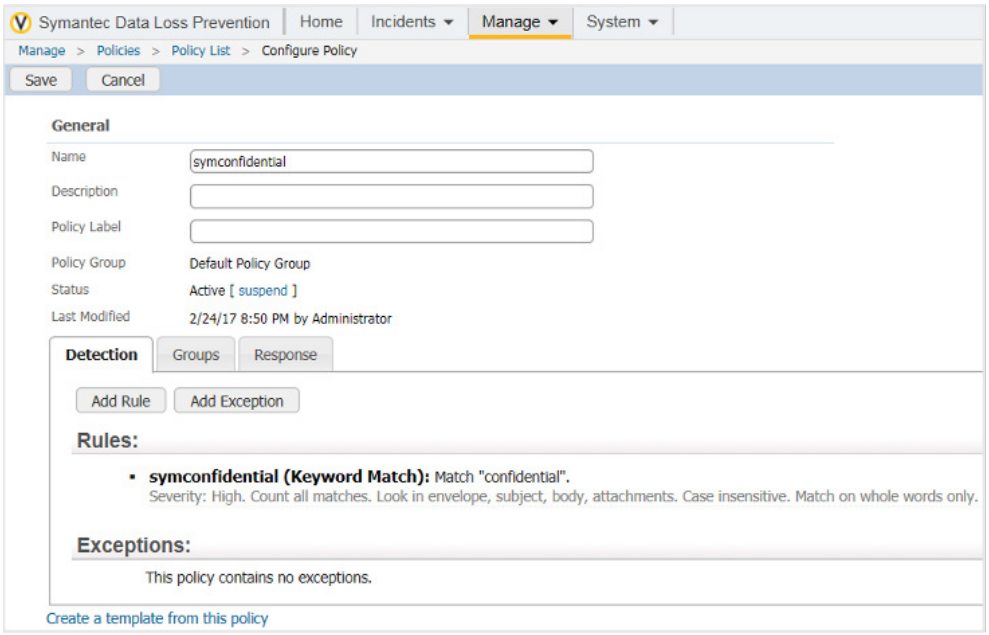
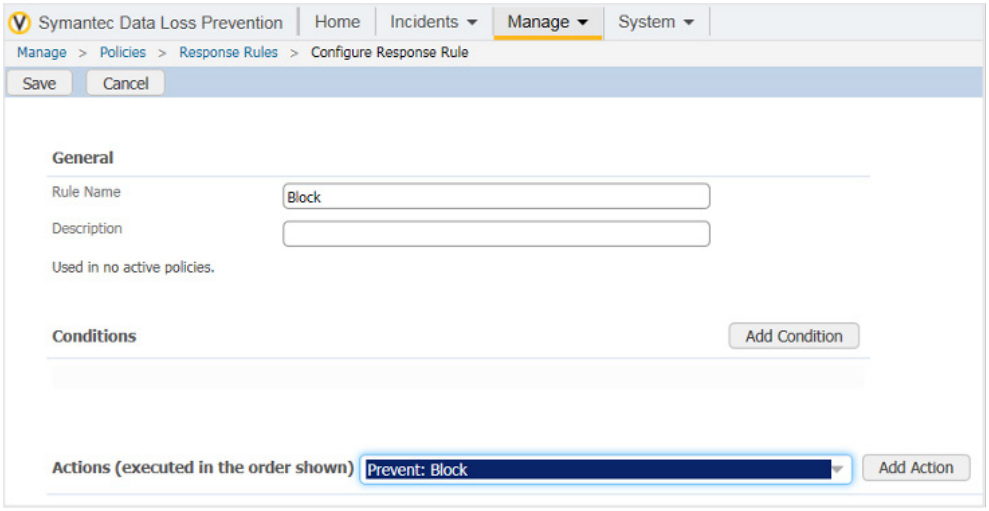


Figure 4: Symantec DLP policy configuration

Create a response rule

1. From the main menu, navigate to **Manage** > **Policies** > **Response Rules**.
2. Click **Add Response Rule** and click **Next**.
3. On the **Configure Response Rule** page, enter the rule **Name**, choose the **Action**, and click **Add**. See a sample configuration in Figure 5.

Figure 5: The creation of a response rule



Assign the response rule to the policy

1. From the main menu, navigate to **Manage** > **Policies** > **Policy List**.
2. Click the name of the policy you want to map to the response rule.
3. Click the **Response** tab, choose the **Response Rule** you want, and click **Save**.

CONFIGURE THE VLANS AND SELF-IPS ON BIG-IP

For BIG-IP SSL Orchestrator 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 ON BIG-IP

For BIG-IP 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 BIG-IP SSL Orchestrator in 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. (If you are upgrading from a previous major version, refer to the BIG-IP SSL Orchestrator setup guide for the recovery procedure.)

To download the latest update:

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

Figure 6: 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. On the F5 system's **Main** menu, navigate to **iApps > Package Management LX** and click on the **Import** button in the upper right.
7. Click **Choose File** and navigate to the .rpm file you downloaded. Select it and click **Open**.
8. Click **Upload**.

You are now ready to proceed to detailed configuration.

BIG-IP SSL Orchestrator Configuration

In the sample configuration in Figure 7, the F5 system steers outbound web traffic through Symantec DLP, which is part of one or more service chains of security devices.

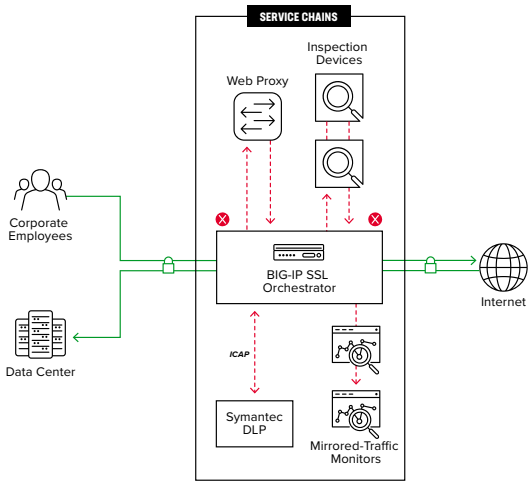


Figure 7: Symantec DLP in a BIG-IP SSL Orchestrator service chain architecture

USING GUIDE 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.

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

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

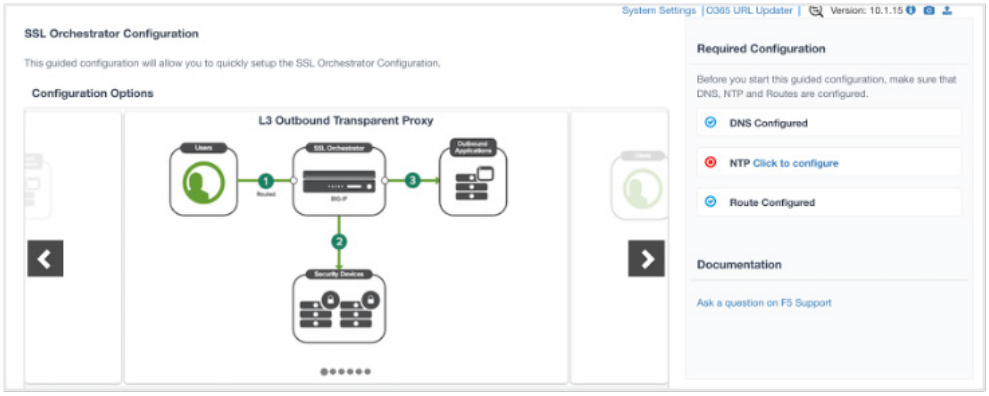


Figure 8: The initial guided configuration page

GUIDED CONFIGURATION WORKFLOW

The first stage of the guided configuration addresses topology.

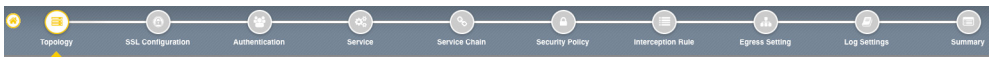


Figure 9: The guided configuration workflow

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 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 8.

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 10: 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	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 ICAP service

Configure up to 10 ICAP services using the BIG-IP SSL Orchestrator configuration utility.

Figure 11: Service configuration

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 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).

To configure the service:

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

Service Properties	User Input
SERVICE SETTINGS	
NAME	Enter a **Name** for the Symantec ICAP service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters are not case sensitive.
DESCRIPTION	Enter a **Description** for the Symantec service.
ICAP DEVICES	Click **Add** and enter the IP address and port number of the Symantec DLP. If you have a multi-tier installation, this must be the IP address of the Symantec Monitor Server. The default ICAP port number is 1344. Click **Add**.
ICAP HEADERS	Select Default to send the **default request-specific headers allowed in ICAP requests**. Otherwise, select Custom to edit the following header values: • **Host:** Specifies the Internet host and port number of the requested resource, as obtained from the original URI given by the user or referring resource. • **Referer:** Allows BIG-IP SSL Orchestrator, as the ICAP client, to specify (for the ICAP server) the address (URI) of the resource from which the Request-URI was obtained. • **User Agent:** The client that initiates a request, often browsers, editors or other user tools. • **From:** Contains the email address of the user who controls the requesting user agent.

SSL Configuration Cont.	User Input Cont.
ONECONNECT	Select **One Connect** to reuse the TCP connections to ICAP servers, which process multiple transactions.
REQUEST	Leave the default ICAP request URI as defined by RFC3507. **icap://${SERVER_IP}:${SERVER_PORT}/req**
RESPONSE	Leave the default ICAP response URI as defined by RFC3507. **icap://${SERVER_IP}:${SERVER_PORT}/res**
PREVIEW MAX. LENGTH (BYTES)	The number of bytes sent to the ICAP server as a preview of each HTTP request or response. The recommended preview size for Symantec DLP is 0 bytes.
SERVICE DOWN ACTION	Select **Ignore** for the system to allow the request or response to continue to the next service in the service chain. Or select **Reset Connection** if you want the system to reset the connection to the client, discarding the request and response.
HTTP VERSION	Select to send both HTTP/1.0 & HTTP/1.1 requests to the ICAP service.
ICAP POLICY	If you want to associate a BIG-IP LTM policy (for example: Disable ADAPT request/response based on HTTP req/rep properties) to the ICAP service, select the policy here.

4. Click **Save** to return to the **Service List**. 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.

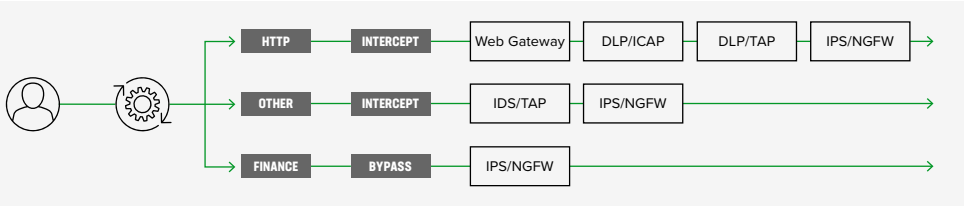


Figure 12: Different traffic flowing through chains of different security services

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 13: 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	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:

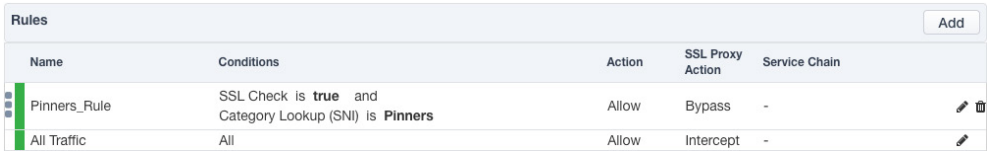
- Whether or not to allow the traffic indicated in the rule.
- Whether or not to decrypt that traffic.
- Which service chain (if any) to pass the traffic through.

Figure 14: Configuring security policy

BIG-IP SSL Orchestrator's guided configuration 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 15: 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 16: 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
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 17: 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.

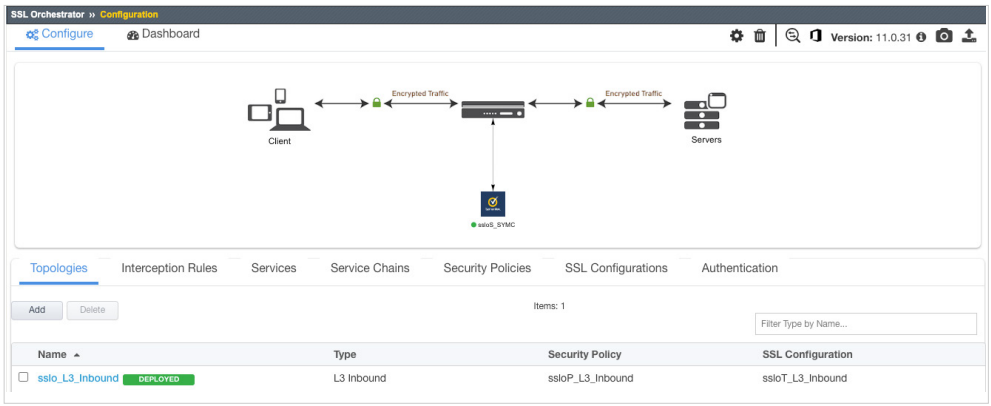
2. Click **Save & Next**.

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 are satisfied with the defined settings, click **Deploy**. Upon successfully deployment of the configuration, BIG-IP SSL Orchestrator will display a dashboard. See Figure 18.

Figure 18: The configuration dashboard after deployment



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.

Testing the Solution

Test the deployed solution using the following three options:

SERVER CERTIFICATE TEST

Open the browser on the client system and navigate to an HTTPS site, for example, https://www.google.com. Once the page loads, check the server certificate by clicking the padlock on the address bar. Verify that the certificate has 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 as expected.

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
```

SYMANTEC DLP POLICY VIOLATION

On a client device, open any secure email service such as gmail.com and compose a mail or upload an attachment with a body containing the word “confidential.” (This word was used as *content match keyword* in the earlier defined policy in Symantec DLP.) When you attempt to **Send** the mail to a recipient on the Internet, it will trigger a policy violation event and the mail will be blocked as per the action defined in the assigned response rule to the policy in the DLP. This confirms that the content adaption functionality enabled by BIG-IP SSL Orchestrator is working as expected.