INTEGRATION GUIDE

BIG-IP SSL Orchestrator and Trellix Data Loss Prevention*

SSL/TLS Visibility and Content Adaptation

*Formerly McAfee Data Loss Prevention

Table of Contents

Data transiting between clients (e.g. PCs, tablets, phones, etc.) and servers is predominantly encrypted with Secure Socket Layer (SSL) or the newer Transport Layer Security (TLS) (ref. Google Transparency Report). Pervasive encryption results in threats being hidden and invisible to security inspection unless traffic is decrypted. This creates serious risks, leaving organizations vulnerable to costly data breaches and loss of intellectual property.

An integrated F5® BIG-IP SSL Orchestrator® and Trellix Data Loss Prevention (DLP) (formerly McAfee DLP) solution solves this SSL/TLS challenge across cloud, mobile, and on-premises environments. BIG-IP SSL Orchestrator centralizes SSL/TLS inspection throughout the complex security architectures, providing high-performance decryption of web traffic for security services like Trellix DLP to detect and block data breaches hidden by encryption. This joint solution thus eliminates the blind spots introduced by SSL/TLS and closes any opportunity for attackers.

This guide provides recommended practices for structuring the BIG-IP SSL Orchestrator and Trellix DLP solution.

Solution Overview

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 the client and the server for inspection.

Within the inspection zone, both unencrypted HTTP and decrypted HTTPS requests are encapsulated within Internet Content Adaptation Protocol (ICAP, RFC3507) and steered to the Trellix DLP systems for inspection and possible request modification (REQMOD). In this context, BIG-IP SSL Orchestrator is the ICAP client and Trellix DLP is the ICAP server. After inspection, user HTTPS requests are re-encrypted by BIG-IP SSL Orchestrator, on their way to the web server.

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

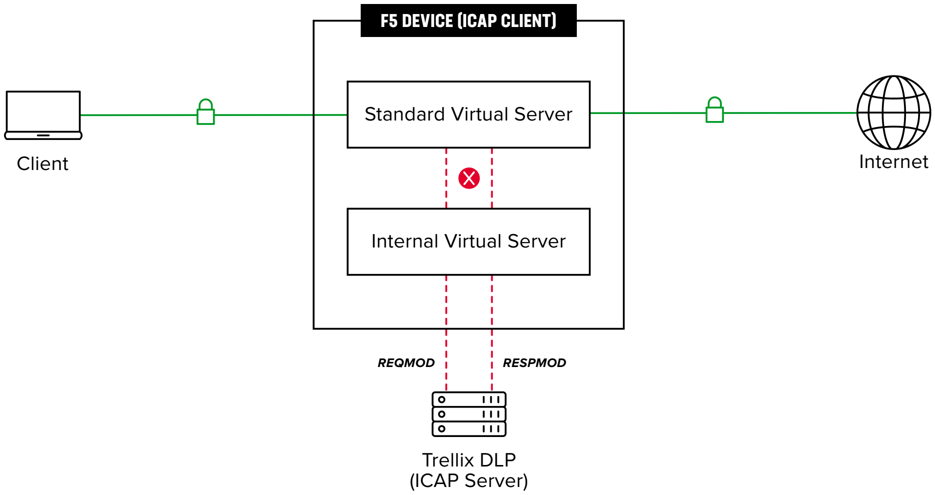


Figure 1: SSL/TLS interception and content adaption for modifying HTTP requests and responses

DYNAMIC SERVICE CHAINING

A typical security stack often consists of multiple systems such as a DLP, next-generation firewall (NGFW), intrusion detection or prevention systems (IDSs/IPSs), and malware analysis tools. All these systems require access to decrypted data for inspection. BIG-IP SSL Orchestrator easily integrates with existing security architectures and centralizes SSL/TLS decryption across these multiple inspection devices in the security stack. This ‘decrypt once and steer to many security devices’ design addresses latency, complexity, and risk issues that can occur if decryption is performed on every single security device. Customers can also create multiple service chains for different traffic flows using the context engine.

Services in BIG-IP SSL Orchestrator

A service in BIG-IP SSL Orchestrator is defined as a pool of identical security devices. For example, a Trellix DLP ICAP service would include one or more Trellix DLP systems. BIG-IP SSL Orchestrator will automatically load balance the traffic to all the systems in a service.

Health monitoring

BIG-IP SSL Orchestrator provides various health monitors to check the health of the security devices in a service and handles failures instantly. For example, in a Trellix DLP ICAP service, should a system fail, BIG-IP SSL Orchestrator will shift the load to the active Trellix DLP systems. Should all the systems in the service fail, BIG-IP SSL Orchestrator will bypass the service to maintain network continuity and maximize uptime.

CONTEXT ENGINE FOR TRAFFIC CLASSIFICATION

BIG-IP SSL Orchestrator's context engine provides the ability to intelligently steer traffic based on policy decisions made using classification criteria, URL category, IP reputation, and flow information. In addition to directing the traffic to service chains, customers can also use the context engine to bypass decryption to applications and websites like financials, government services, health care, and any others, for legal or privacy purposes.

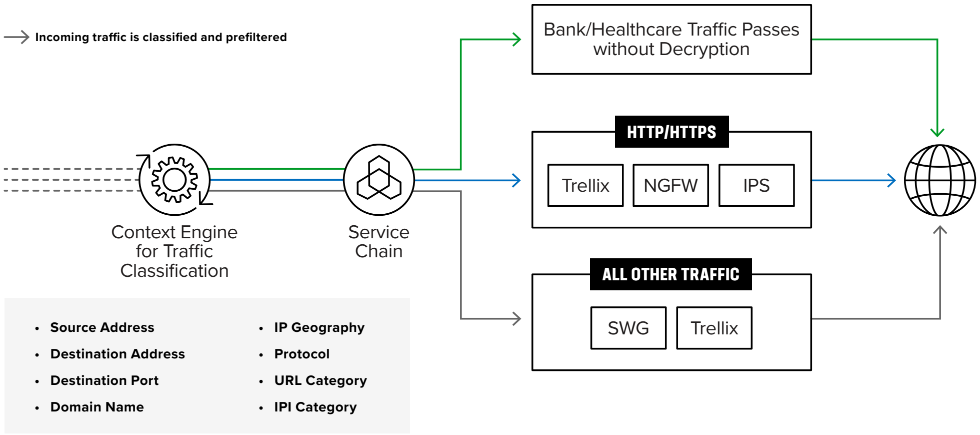


Figure 2: Context engine delivering service chaining and policy-based traffic steering

HIGH AVAILABILITY

BIG-IP SSL Orchestrator supports an active-standby high availability (HA) architecture—one system actively processes traffic while the other remains in standby mode until needed. The goal is to decrease any downtime and eliminates single points of failure. Configuration and user connection information are synchronized automatically between the system

LICENSE COMPONENTS

The BIG-IP SSL Orchestrator solution supports two licensing modes—standalone and LTM add-on.

Standalone model

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.

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

- **F5® 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.
- **F5 Secure Web Gateway Services** to filter and control outbound web traffic using a URL database or an F5 URL filtering (URLF) subscription to access the URL category database.
- An **F5® IP Intelligence Services subscription** for IP reputation service.

LTM add-on module

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

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

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

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

It is recommended to contact Trellix directly for information regarding DLP licensing options and a full understanding of the Trellix DLP product's enforcement and reporting capabilities.

ARCHITECTURE BEST PRACTICES

Several 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 in-line 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 HA pair with a floating IP address.
- Use dual homing. Trellix DLP systems must be dual homed on the inward and outward VLANs with each F5 system in the device S/FDG.
- Achieve further interface redundancy with the Link Aggregation Control Protocol (LACP). LACP manages the connected physical interfaces as a single virtual interface (aggregate group) and detects any interface failures within the group.

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 usernames, 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.

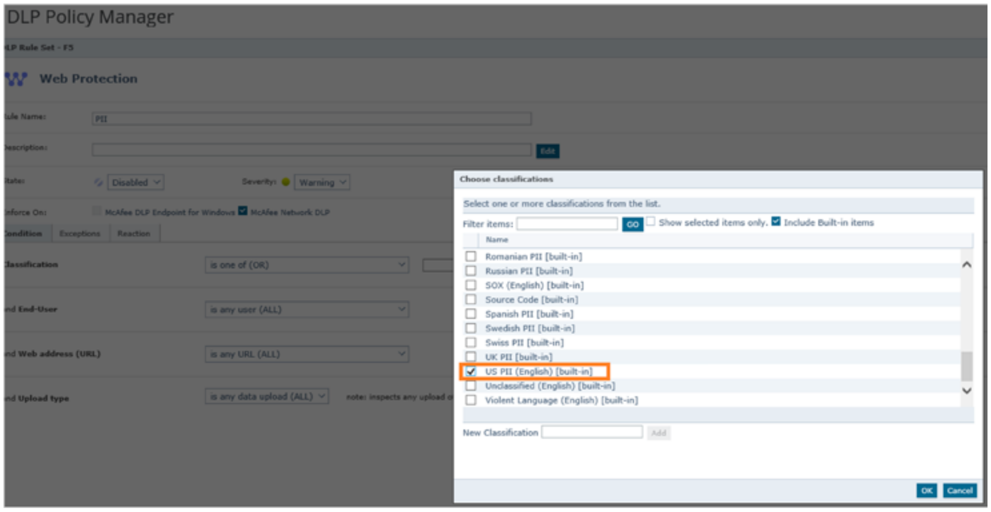
Initial Setup

Complete these initial steps before performing detailed configuration of BIG-IP SSL Orchestrator. In addition, refer to the Trellix DLP product guide and BIG-IP SSL Orchestrator setup knowledge base.

CREATE A DLP POLICY RULE

Log in to the Trellix ePolicy Orchestrator (ePO) system. Verify the DLP system is managed and licensed in the Trellix ePO system.

1. From the main menu, navigate to **Data Protection** > **DLP Policy Manager**.
2. On the DLP Policy Manager page, at the left bottom, click on the Actions drop down list. Choose the **New Rule Set** option.
3. Give a name for the rule set and click **Next**. This will create a new rule set. Next, add a rule to this rule set.
4. Click on the above created rule set. In the **Actions** drop down list, choose **New Rule** > **Web Protection**.
5. Give the rule a name. In the **Classification** section, choose the classification. Example below shows the **US PII** choice selected to flag PII data violations.



DLP Policy Manager

LP Rule Set - F5

Web Protection

ule Name: PII

escription:

tate: Disabled Severity: Warning

nforce On: □ McAfee DLP Endpoint for Windows ☑ McAfee Network DLP

Classification: is one of (OR)

nd End-User: is any user (ALL)

nd Web address (URL): is any URL (ALL)

nd Upload type: is any data upload (ALL) note: inspects any upload o

Choose classifications

Select one or more classifications from the list.

Filter items: □ Show selected items only. ☑ Include Built-in items

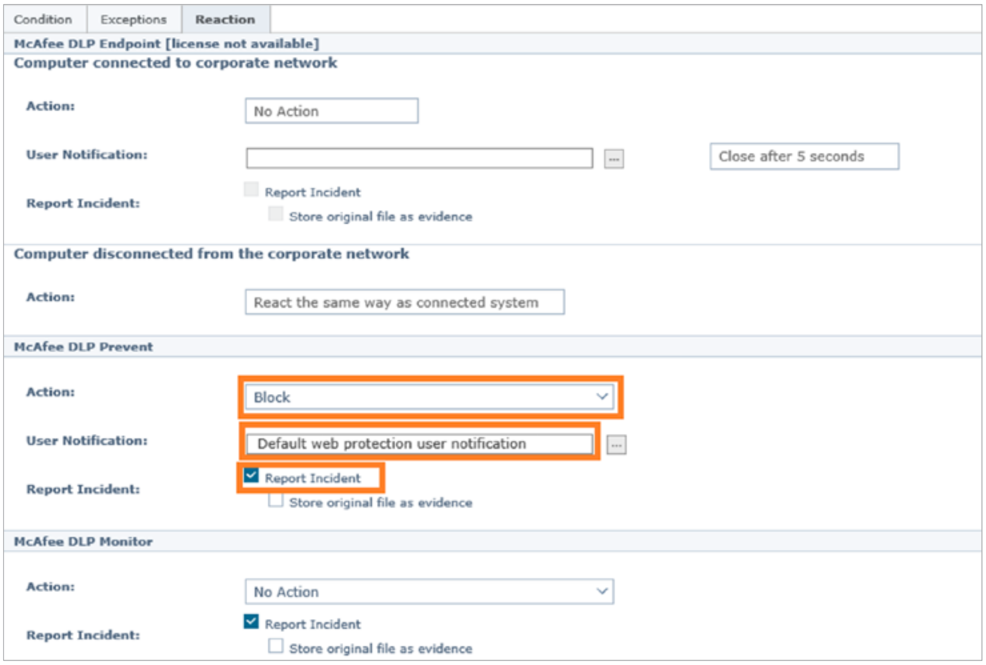
	Name
□	Romanian PII [built-in]
□	Russian PII [built-in]
□	SOX (English) [built-in]
□	Source Code [built-in]
□	Spanish PII [built-in]
□	Swedish PII [built-in]
□	Swiss PII [built-in]
□	UK PII [built-in]
☑	US PII (English) [built-in]
□	Unclassified (English) [built-in]
□	Violent Language (English) [built-in]

New Classification

Figure 3: Example configuration of new rule creation with PII classification in the Trellix ePO system

6. Click on the **Reaction** tab, select the Action, and choose the **User Notification** method. Example below shows the **Block** action and **Default web protection user notification** method selected to report an incident.
7. Click the **Save** button and then press **Close**.

Figure 4: Example configuration for reaction to a policy rule violation in the Trellix ePO system



McAfee DLP Endpoint [license not available]

Computer connected to corporate network

Action: No Action

User Notification: Close after 5 seconds

Report Incident: □ Report Incident
□ Store original file as evidence

Computer disconnected from the corporate network

Action: React the same way as connected system

McAfee DLP Prevent

Action: Block

User Notification: Default web protection user notification

Report Incident: ☑ Report Incident
□ Store original file as evidence

McAfee DLP Monitor

Action: No Action

Report Incident: ☑ Report Incident
□ Store original file as evidence

8. Back in the **DLP Policy Manager** page, click on the **Policy Assignment** tab.
9. In the **Actions** dropdown, choose **Assign Rule Sets to a Policy**. Select the policy and check the rule set that was created above, then click **OK**. The DLP systems that inherit the selected policy will enforce the assigned rule.

CONFIGURE THE VLANS AND SELF-IPS ON THE BIG-IP SYSTEM

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.

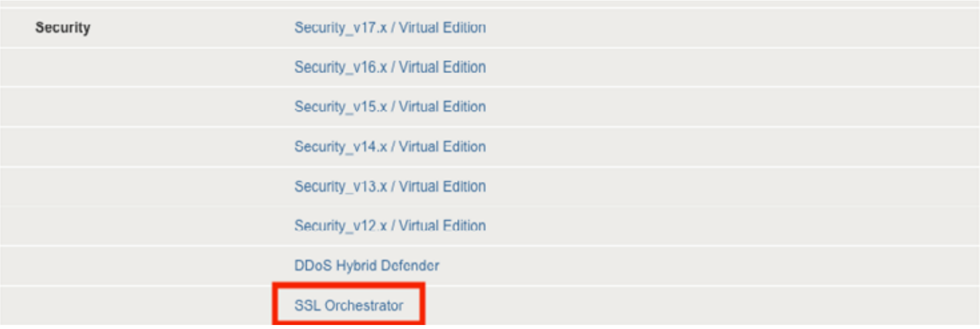
IMPORT A CA CERTIFICATE AND PRIVATE KEY INTO THE BIG-IP SYSTEM

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/TLS certificates for BIG-IP systems to understand the procedure.

UPDATE THE BIG-IP SSL ORCHESTRATOR APPLICATION

Periodic updates are available for BIG-IP SSL Orchestrator. 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 **SSL Orchestrator**, and click the link.



Security	Security_v17.x / Virtual Edition
	Security_v16.x / Virtual Edition
	Security_v15.x / Virtual Edition
	Security_v14.x / Virtual Edition
	Security_v13.x / Virtual Edition
	Security_v12.x / Virtual Edition
	DDoS Hybrid Defender
	SSL Orchestrator

Figure 5: The F5 product download web page

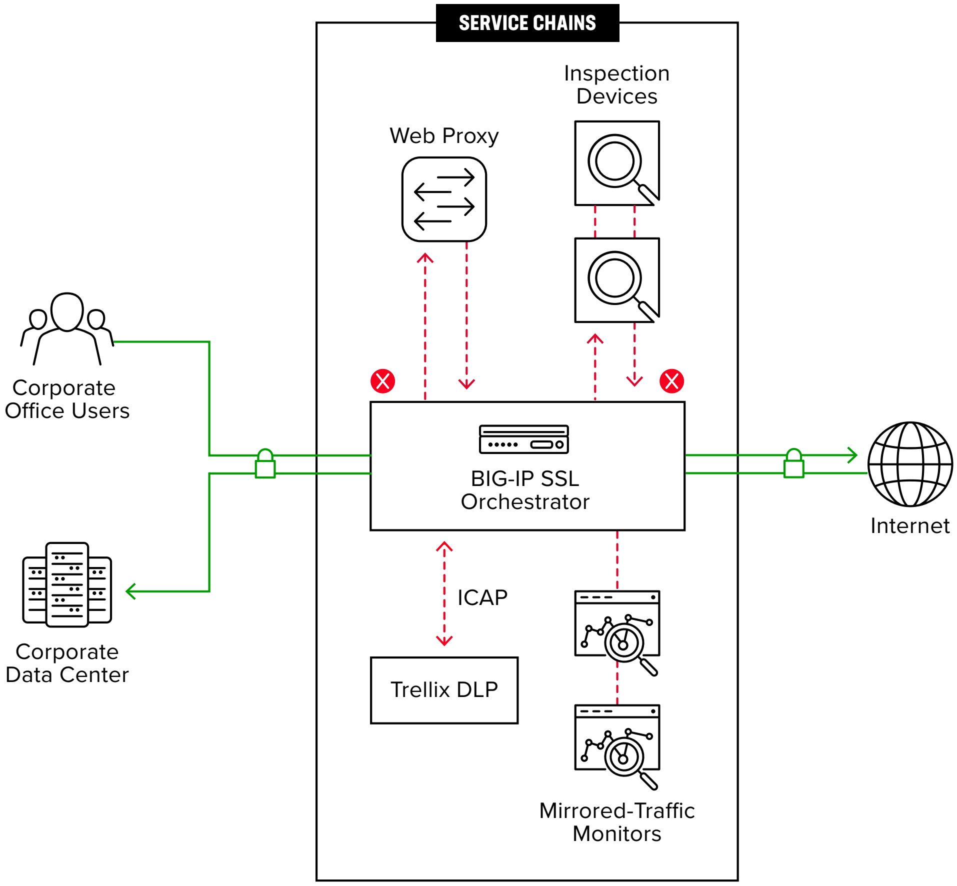
4. Select and download the latest version of the SSL Orchestrator .rpm file.
5. Read the appropriate Release Notes before attempting to use the file.
6. On the **Main** menu, navigate to **SSL Orchestrator** > **Configuration** and click on the **Upgrade SSL Orchestrator** icon in the upper right.
7. 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.

BIG-IP SSL Orchestrator Configuration

In the sample topology demonstrated in Figure 6, the F5 system will be configured as an ICAP client to direct the decrypted web traffic, encapsulated in ICAP to the Trellix DLP service. The Trellix DLP service is defined as a pool of one or many Trellix DLP systems and will be configured as part of a service chain of security devices.

Figure 6: The Trellix DLP system in a BIG-IP SSL Orchestrator service chain architecture



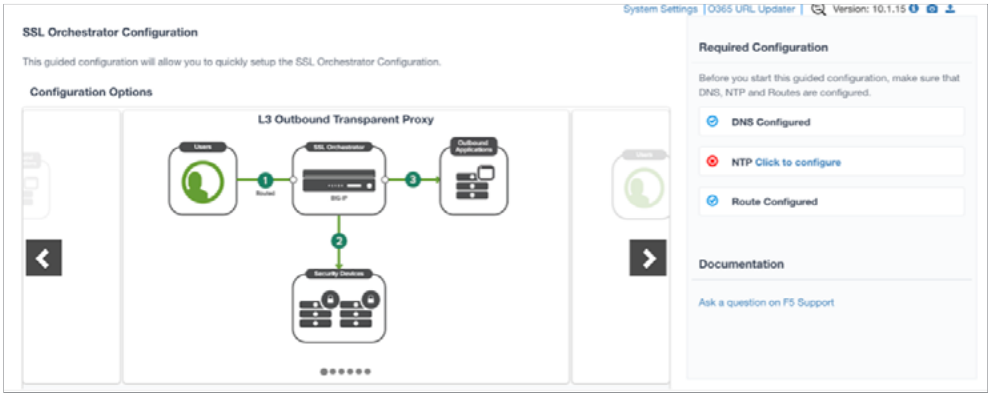
USING GUIDED CONFIGURATION

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.

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

1. Once logged into the F5 system, in the F5 Web UI **Main** menu, click on **SSL Orchestrator** > **Configuration**.

2. Take a moment to review the various configuration options.
3. (Optional.) Satisfy any of the **DNS**, **NTP**, and **Route** prerequisites 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 is not addressed later.



System Settings | O365 URL Updater | Version: 10.1.15

SSL Orchestrator Configuration

This guided configuration will allow you to quickly setup the SSL Orchestrator Configuration.

Configuration Options

L3 Outbound Transparent Proxy

Required Configuration

Before you start this guided configuration, make sure that DNS, NTP and Routes are configured.

- DNS Configured
- NTP Click to configure
- Route Configured

Documentation

Ask a question on F5 Support

Figure 7: The initial guided configuration page

4. No other configurations are required here, so click **Next**.

GUIDED CONFIGURATION WORKFLOW

The first stage of the guided configuration addresses topology.

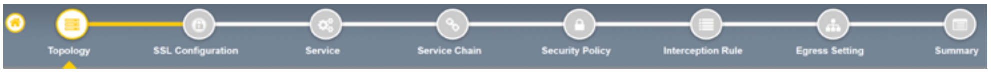


Figure 8: The guided configuration workflow

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 the guidance below.

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.

Topology Properties Cont.	User Input Cont.
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 demonstrates this option.
IP FAMILY	Specify whether you want this configuration to support **IPv4** addresses or **IPv6** addresses.
BIG-IP SSL ORCHESTRATOR TOPOLOGIES	The BIG-IP SSL Orchestrator Topologies option page presents six topologies: 1. **L3 explicit proxy:** The traditional explicit forward proxy. The sample configuration presented here uses this topology. 2. **L3 outbound:** The traditional transparent forward proxy. 3. **L3 inbound:** A reverse proxy configuration. 4. **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. 5. **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. 6. **Existing application:** Designed to work with existing F5® BIG-IP® Local Traffic Manager™ (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 9.

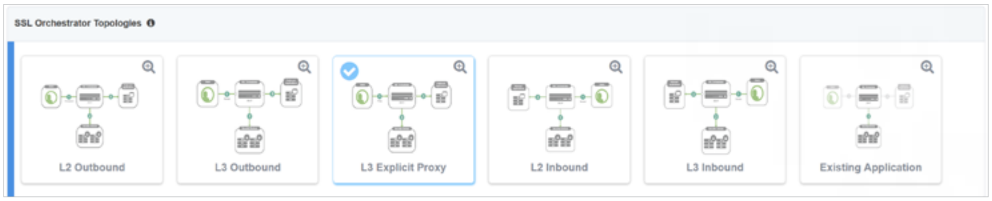


Figure 9: Sample topology configuration

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.

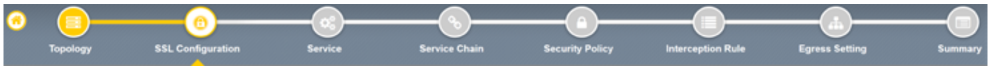


Figure 10: SSL configuration in the workflow

1. Click **Show Advanced Settings** on the right-hand side of the page.
2. Make appropriate **SSL Configuration** selections using the guidance below.

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	Cipher type can be a Cipher Group or Cipher String. • 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.

SSL Configurations Cont.	User Input Cont.
CERTIFICATE KEY CHAIN	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. Leave the Passphrase field empty and click **Add**.
CA CERTIFICATE KEY CHAIN	An SSL/TLS forward proxy must re-sign or forge 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 subordinate CA certificates and keys that were imported earlier, then click **Add**.
SERVER-SIDE SSL/TLS	
CIPHER TYPE	Select **Cipher String** for the default cipher list.
TRUSTED CERTIFICATE AUTHORITY	Use the **ca-bundle.cr**t file, which contains all well-known public CA certificates, for client-side processing.

3. Click **Save & Next**.

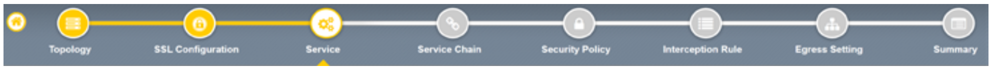
***Note**: SSL/TLS settings minimally require an RSA-based template and CA certificates but can also support elliptic curve (ECDSA) certificates. In this case, BIG-IP SSL Orchestrator would forge an elliptic curve (EC) certificate to the client if the SSL/TLS handshake negotiated an ECDHE_ECDSA cipher. To enable EC forging support, add both an EC template certificate and key, and an EC CA certificate and key.*

Create the Trellix DLP ICAP service

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.

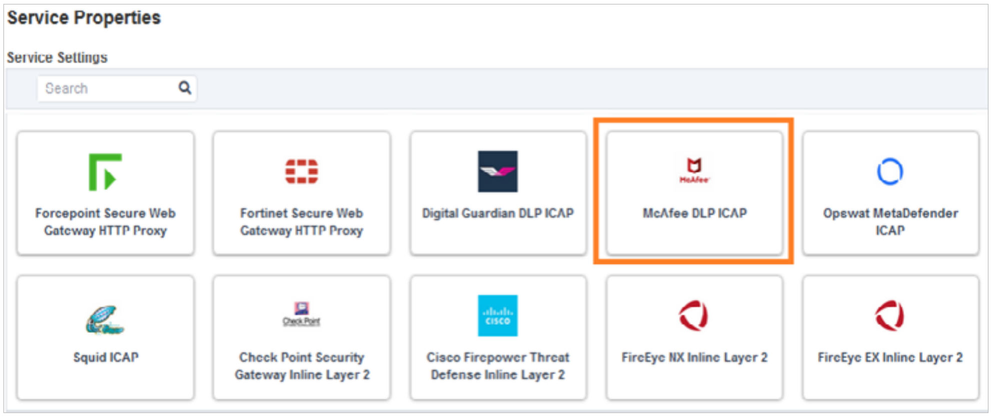
To configure the service:

Figure 11: Service configuration



1. Under **Service List**, click **Add Service**.
2. In the service catalog, double click on the **Trellix DLP ICAP** service tile.

Figure 12: Service catalog


Service Properties
Service Settings
Search
Forcepoint Secure Web Gateway HTTP Proxy
Fortinet Secure Web Gateway HTTP Proxy
Digital Guardian DLP ICAP
McAfee DLP ICAP
Opswat MetaDefender ICAP
Squid ICAP
Check Point Security Gateway Inline Layer 2
Cisco Firepower Threat Defense Inline Layer 2
FireEye NX Inline Layer 2
FireEye EX Inline Layer 2

3. The **Service Properties** page displays. Configure the service using the guidance below.

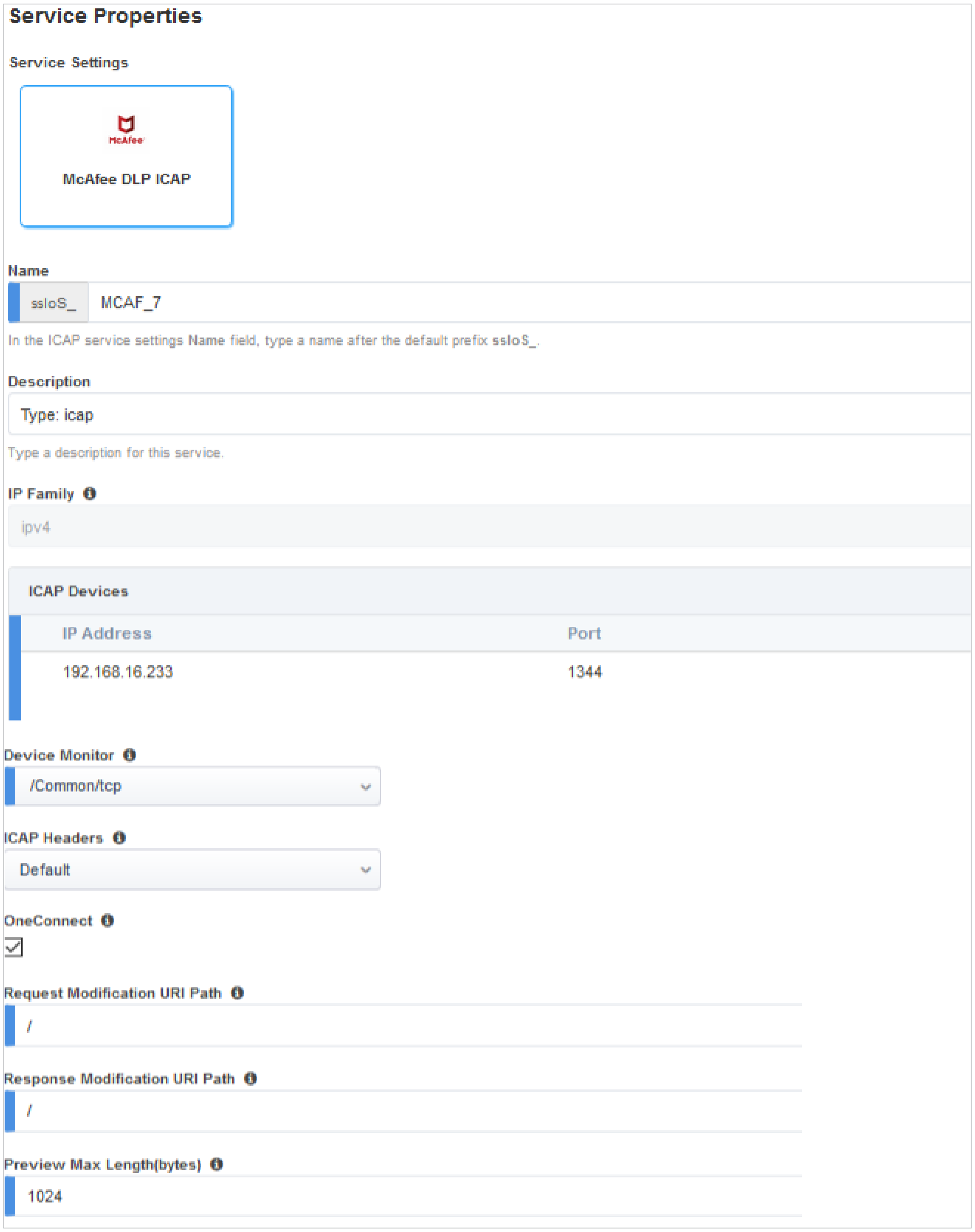
Service Properties	User Input
SERVICE SETTINGS	
NAME	Enter a **Name** for the Trellix DLP ICAP service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters are not case sensitive.
DESCRIPTION	Enter a **Description** for the Trellix DLP ICAP service.
ICAP DEVICES	Click **Add** and enter the IP address and port number of the Trellix DLP system. Make sure that the default ICAP port number is 1344. Click **Add**.

Service Properties Cont.	User Input Cont.
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. • **Referrer:** 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.
ONE CONNECT	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 length for Trellix DLP system is 1024 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**. Click **Add Service** to access the service catalog again for creating additional services.

5. Once all the desired services are created, click **Save & Next** to move on to service chain setup.

Figure 13: Trellix DLP ICAP service properties page



Service Properties

Service Settings

McAfee DLP ICAP

Name

ssloS_ MCAF_7

In the ICAP service settings Name field, type a name after the default prefix ssloS_.

Description

Type: icap

Type a description for this service.

IP Family

ipv4

ICAP Devices

IP Address	Port
192.168.16.233	1344

Device Monitor

/Common/tcp

ICAP Headers

Default

OneConnect

☑

Request Modification URI Path

/

Response Modification URI Path

/

Preview Max Length(bytes)

1024

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.

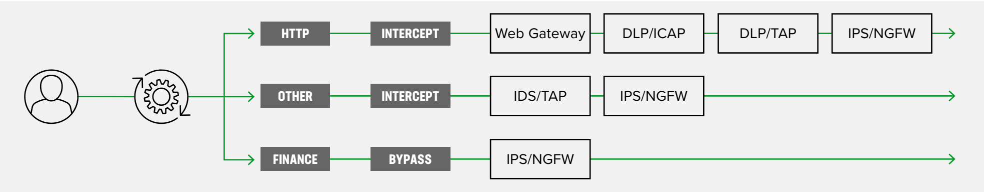


Figure 14: Different traffic flowing through chains of different security services

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.

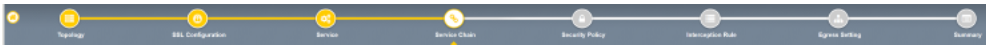
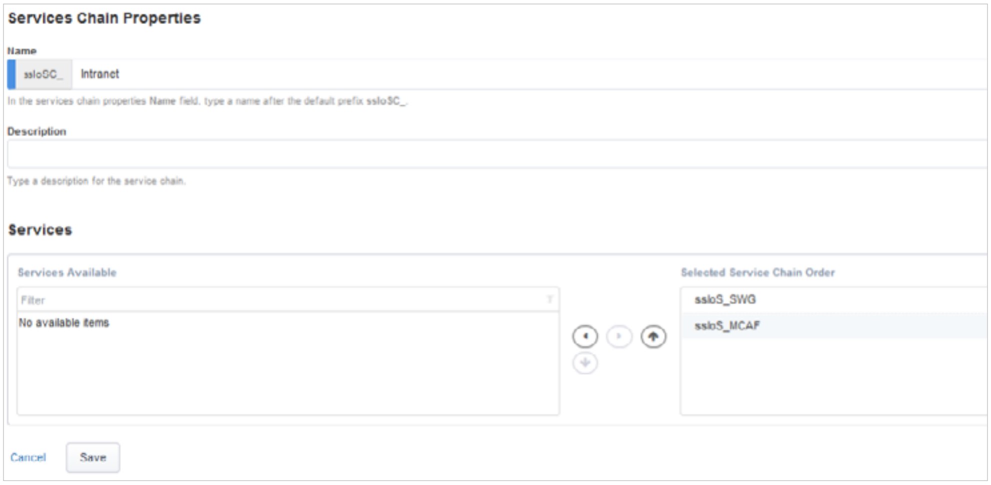


Figure 15: Configuring service chains

To create a service chain:

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

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 the **Trellix DLP ICAP service** and any other desired services from the **Services Available** list and move them into the **Selected Service Chain Order** column. Optionally, order them as desired.



Services Chain Properties

Name

ssloSC_ Intranet

In the services chain properties Name field, type a name after the default prefix ssloSC_.

Description

Type a description for the service chain.

Services

Services Available

Filter

No available items

Selected Service Chain Order

ssloS_SWG

ssloS_MCAF

Cancel Save

Figure 16: Example service chain configuration with Trellix DLP ICAP service and Secure Web Gateway service.

2. Click **Save & Next.**

Security policy

Security policies are the set of rules that govern how traffic is 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.

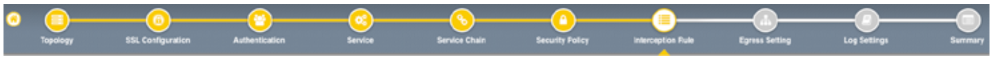
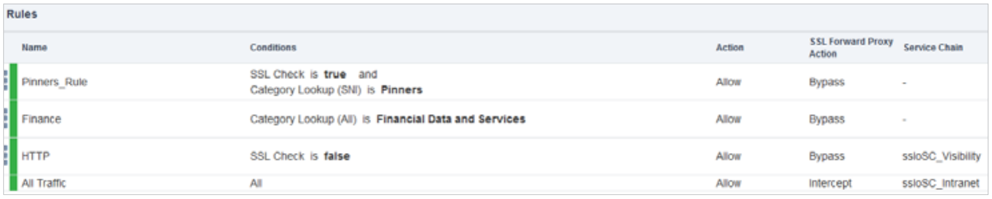


Figure 17: Configuring security policy

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**.



Rules

Name	Conditions	Action	SSL Forward Proxy Action	Service Chain
Pinners_Rule	SSL Check is **true** and Category Lookup (SNI) is **Pinners**	Allow	Bypass	-
Finance	Category Lookup (All) is **Financial Data and Services**	Allow	Bypass	-
HTTP	SSL Check is **false**	Allow	Bypass	ssloSC_Visibility
All Traffic	All	Allow	Intercept	ssloSC_Intranet

Figure 18: Configuring security policy rules

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.

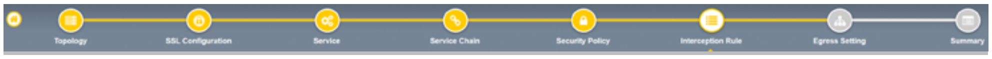


Figure 19: Configuring interception rules

1. To create an interception rule, follow this guidance:
2. Click **Save & Next**.

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.
INGRESS NETWORK	
VLANS	This defines the VLANs through which traffic will enter. For a forward proxy topology (outbound), for instance, this would be the client-side VLAN (Intranet).

Egress setting

The **Egress Setting** page defines the topology-specific egress characteristics.

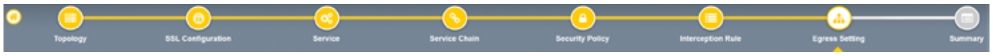


Figure 20: Configuring egress settings

1. To configure these characteristics, follow this guidance:

Egress Settings	User Input
MANAGE SNAT SETTINGS	Defines if and how source NAT (SNAT) is used for egress traffic.
GATEWAYS	Enter the IP address of 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 of 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 successful deployment of the configuration, BIG-IP SSL Orchestrator will display a dashboard. See Figure 21.

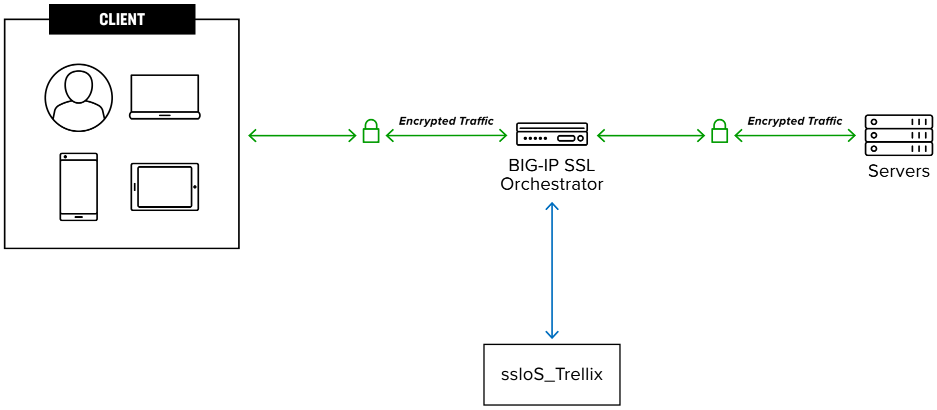


Figure 21: The configuration dashboard after deployment

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 any one of the following three options:

SERVER CERTIFICATE TEST

Open the browser on the client system and navigate to a HTTPS site, for example, https://www.Trellix.com. Once the web 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 has intercepted the web request and reassigned the response from the web server, validating that the functionality enabled by BIG-IP SSL Orchestrator is working as expected.

DECRYPTED TRAFFIC ANALYSIS

Perform a TCP dump from the F5 system command line interface to observe the decrypted clear text HTTP headers and payload. This confirms SSL/TLS interception by BIG-IP SSL Orchestrator.

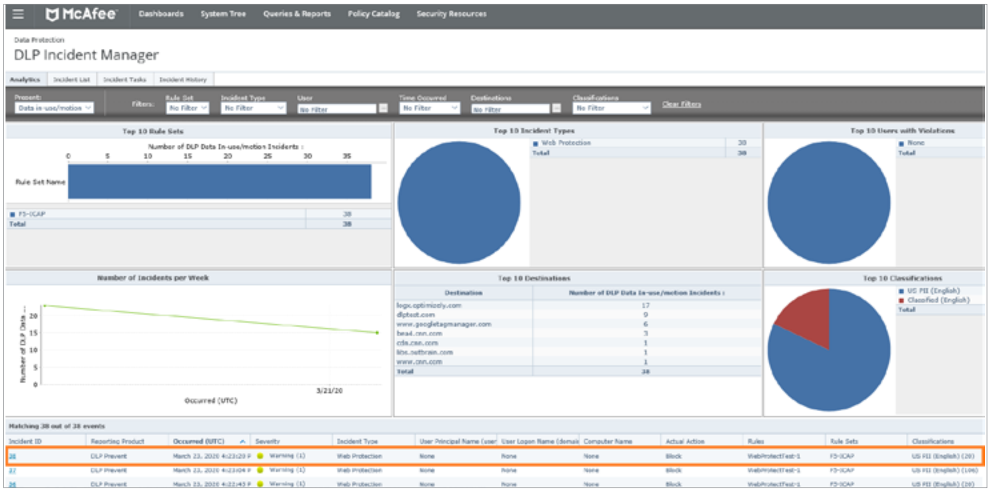
```
tcpdump –lnni eth<n> -Xs0
```

TRELLIX DLP POLICY RULE VIOLATION

On a client device:

1. Open browser and navigate to https://dlptest.com (**DLPTest.com** is a DLP testing resource that focuses on testing to make sure your DLP software is working correctly).
2. Click on the **HTTPS Post** tab. In the text box, input some PII data (an example of PII data is 'ABC Smith, 123-45-6789, 123 Main St, Seattle WA 98008'). Click on the **Submit** button.
3. You will see the '**Access Denied**' message in the response.
4. Open Trellix ePO web UI. From the main menu, navigate to **Data Protection** > DLP Incident Manager. The DLP Incident Manager web page reports the PII violation.

Figure 22: DLP Incident Manager



■ F5-ICAP	38
Total	38

■ Web Protection	38
Total	38

■ None
Total

Destination	Number of DLP Data In-use/motion Incidents :
logx.optimizely.com	17
dlptest.com	9
www.googletagmanager.com	6
bea4.cnn.com	3
cdn.cnn.com	1
libs.outbrain.com	1
www.cnn.com	1
Total	38

■ US PII (English)
■ Classified (English)
Total

Matching 38 out of 38 events

Incident ID	Reporting Product	Occurred (UTC)	Severity	Incident Type	User Principal Name (user	User Logon Name (domain	Computer Name	Actual Action	Rules	Rule Sets	Classifications
38	DLP Prevent	March 23, 2020 4:23:20 P	● Warning (1)	Web Protection	None	None	None	Block	WebProtectTest-1	F5-ICAP	US PII (English) (20)
37	DLP Prevent	March 23, 2020 4:23:04 P	● Warning (1)	Web Protection	None	None	None	Block	WebProtectTest-1	F5-ICAP	US PII (English) (106)
36	DLP Prevent	March 23, 2020 4:22:45 P	● Warning (1)	Web Protection	None	None	None	Block	WebProtectTest-1	F5-ICAP	US PII (English) (20)