F5 SSL Orchestrator and McAfee DLP Solution:
SSL Visibility and Content Adaptation

April 2020

Contents

Introduction

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

This guide provides recommended practices for structuring the F5 SSL Orchestrator and McAfee DLP solution.

Solution Overview

F5 SSL Orchestrator, deployed inline to the wire traffic, intercepts any outbound secure web request and establishes two separate SSL 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 McAfee DLP systems for inspection and possible request modification (REQMOD). In this context, SSL Orchestrator is the ICAP client and McAfee DLP is the ICAP server. After inspection, user HTTPS requests are re-encrypted by 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.
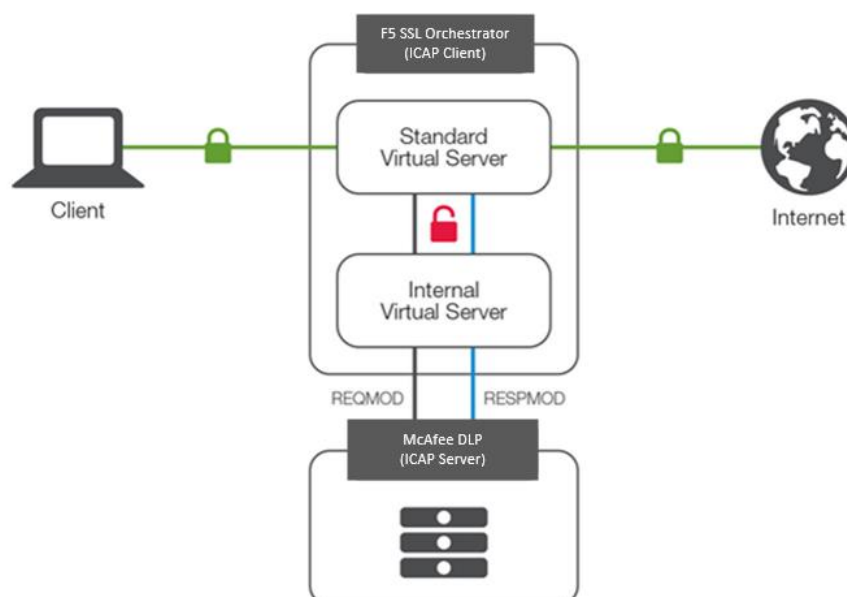

Figure 1: SSL interception and content adaption for modifying HTTP requests and responses

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 (IDS/IPS), and malware analysis tools. All these systems require access to decrypted data for inspection. 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 F5 SSL Orchestrator

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

Health Monitoring

F5 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 McAfee DLP ICAP service, should a system fail, the F5 SSL Orchestrator will shift the load to the active McAfee DLP systems. Should all the systems in the service fail, SSL Orchestrator will bypass the service to maintain network continuity and maximize uptime.

Context Engine for Traffic Classification

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.
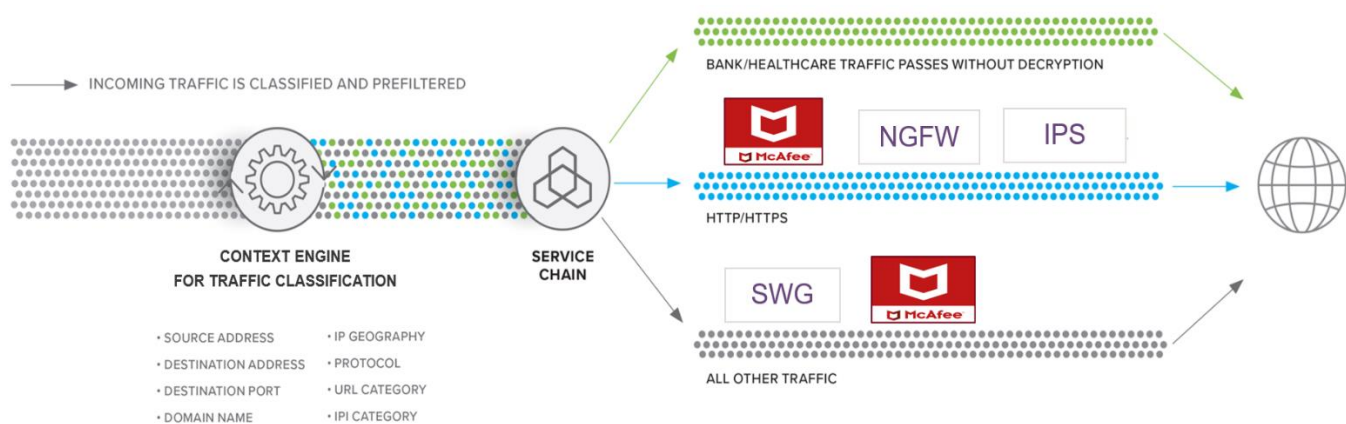

Figure 2: Context engine delivering service chaining and policy-based traffic steering

High Availability

SSL Orchestrator supports an active-standby 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 systems.

License Components

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

Standalone Model

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

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

- **F5® Access Manager™** (formerly known as **F5® BIG-IP® APM**) to authenticate and manage user access.

- **F5® Secure Web Gateway** (**SWG**) Services to filter and control outbound web traffic using a URL database (OR) **F5 URL filtering** (**URLF**) subscription to access the URL category database.

- An **F5® IP Intelligence** (**IPI**) subscription for IP reputation service.

LTM Add-on Module

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

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

- A **URL Filtering (URLF)** subscription.

- An **F5 IP Intelligence**.

- A network **Hardware Security Module** (HSM) to safeguard and manage digital keys for strong authentication.

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

It is recommended to contact McAfee directly for information regarding DLP Licensing options and a full understanding of the McAfee 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 visibility solution must be in-line to the traffic flow to decrypt perfect forward secrecy (PFS) cipher suites such as ECDHE (elliptic curve Diffie-Hellman encryption).

- Deploy 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. McAfee 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 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 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 SSL Orchestrator. It is technically possible to configure 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 SSL Orchestrator. In addition, refer to the McAfee DPL product guide and F5 SSL Orchestrator setup knowledge base on f5.com.

Create a DLP Policy Rule

Log in to the McAfee ePolicy Orchestrator [ePO] system. Verify, the DLP system is managed and licensed in ePO.

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 **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 **US PII** choice selected to flag PII data violations.
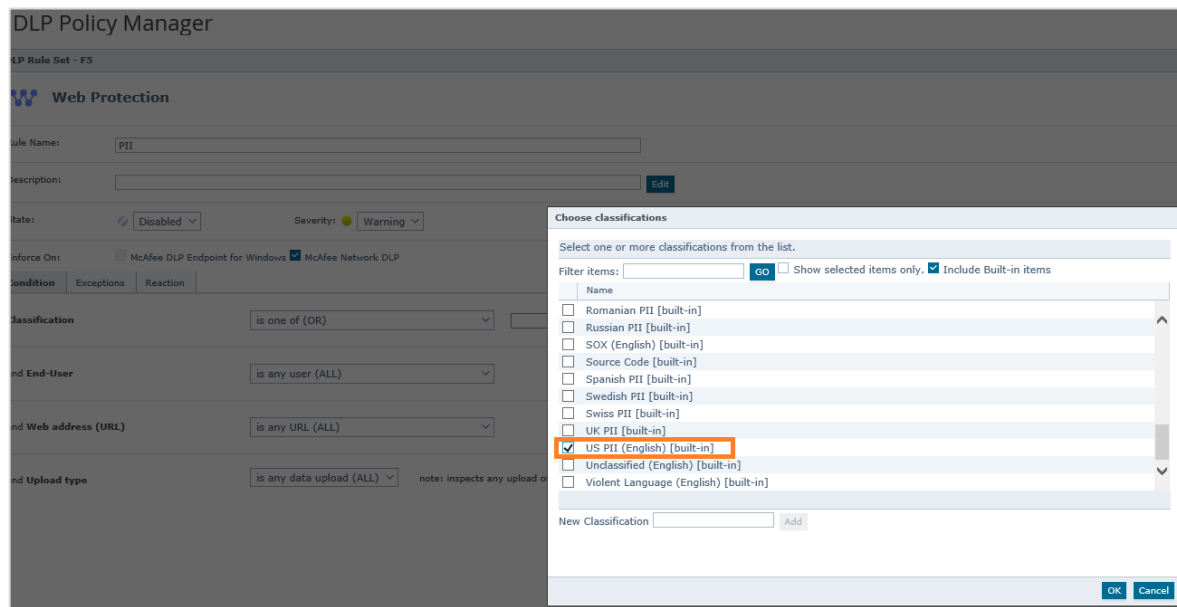
Figure 3: example configuration of new rule creation with PII classification, in McAfee ePO system

6. Click on the **Reaction** tab and 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 McAfee ePO system

7

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**. DLP systems which inherit the selected policy will enforce the assigned rule.

Configure the VLANs and self-IPs on F5 System

For 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 F5 System

For SSL Orchestrator in an outbound traffic topology, a local CA certificate and private key are required to re-sign the remote server certificates for local (internal) clients. For SSL Orchestrator in an inbound traffic topology, remote clients terminate their TLS sessions at the F5 system, so it must possess the appropriate server certificates and private keys. Refer to the F5 support article on managing SSL certificates for F5 systems to understand the procedure.

Update the SSL Orchestrator Application

Periodic updates are available for SSL Orchestrator. (If you are upgrading from a previous major version, refer to the 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**.

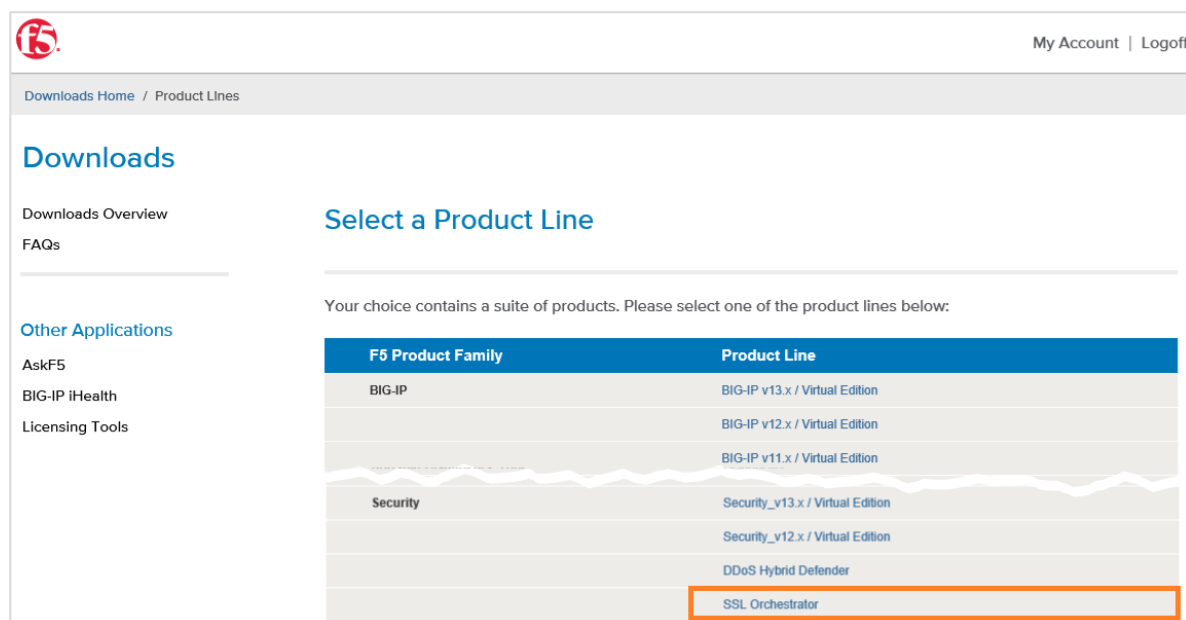3. Scroll to the **Security** product family, select **SSL Orchestrator**, and click the link.

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 '**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.

SSL Orchestrator Configuration

In the sample topology demonstrated in Figure 8, the F5 system will be configured as an ICAP client to direct the decrypted web traffic, encapsulated in ICAP to McAfee DLP service. The McAfee DLP service is defined as a pool of one or many McAfee DLP systems, and will be configured as part of a service chain of security devices.
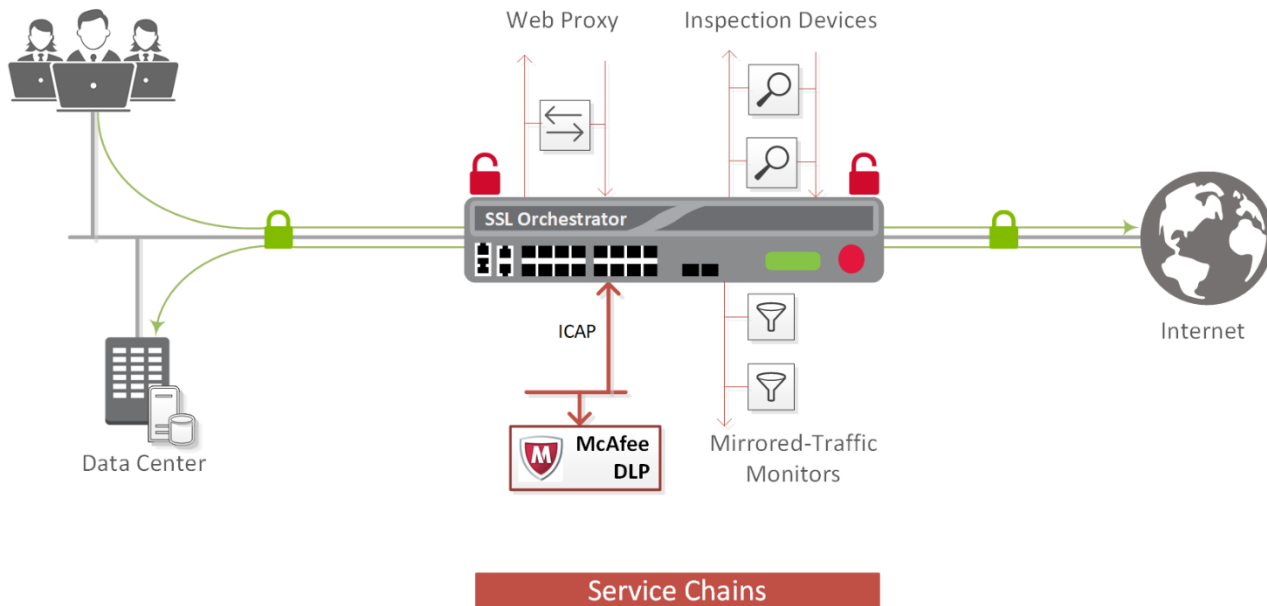
Figure 6: McAfee DLP system in an SSL Orchestrator service chain architecture

Using Guided Configuration

The 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.**

1. Take a moment to review the various configuration options.

2. (Optional.) Satisfy any of the **DNS**, **NTP** and **Route** prerequisites from this initial configuration page. Keep in mind, however, that the SSL Orchestrator guided configuration will provide an opportunity to define DNS and route settings later in the workflow. Only NTP is not addressed later.
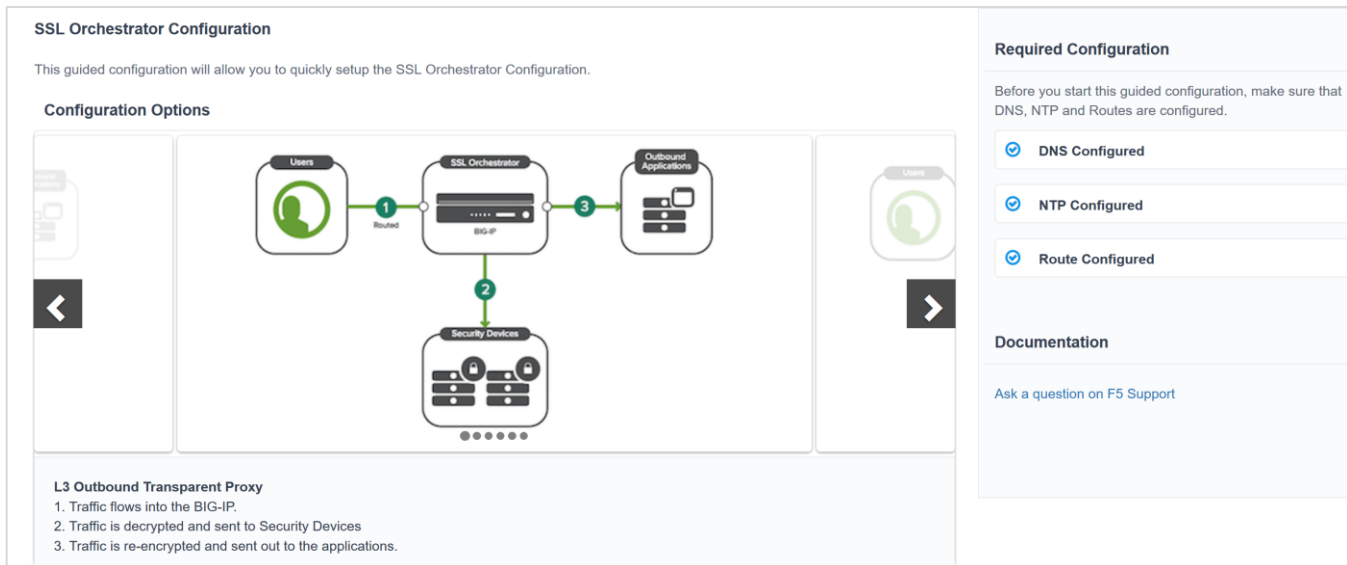

Figure 7: The initial guided configuration page

3. 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

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 SSL Orchestrator deployment.
Description	Enter a **Description** for this 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. 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.
SSL Orchestrator Topologies	The **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 SSL Orchestrator as a bump-in-the-wire in an existing routed path, where SSL Orchestrator presents no IP addresses on its outer edges. 5. **L2 Outbound**: Provides a transparent path for outbound traffic flows, inserting SSL Orchestrator as a bump-in-the-wire in an existing routed path, where SSL Orchestrator presents no IP addresses on its outer edges. 6. **Existing Application**: Designed to work with existing BIG-IP LTM applications that already perform their own SSL handling and client-server traffic management. The Existing Application workflow proceeds directly to service creation and security policy definition, then exits with an SSL Orchestrator-type access policy and per-request policy that can easily be consumed by a BIG-IP LTM virtual server. The sample configuration presented here deploys SSL Orchestrator as an L3 explicit proxy for decrypting outbound TLS/SSL traffic. See Figure 9.
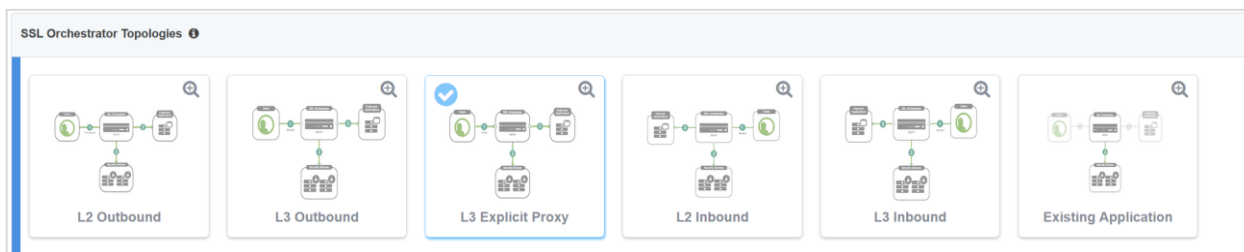
Figure 9: Sample topology configuration

2. Click **Save & Next**.

SSL Configuration

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

Figure 10: SSL configuration in the workflow

1. Click **Show Advanced Settings** on the right-hand side of the page.

    3. Make appropriate **SSL Configuration** selections using the guidance below.

SSL Configuration	User Input
SSL Profile	
Name	Enter a **Name** for the SSL profile.
Description	Enter a **Description** for this SSL profile.
Client-Side SSL	
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 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 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 Chains	An SSL 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	
Cipher Type	Select **Cipher String** for the default cipher list.
Trusted Certificate Authority	Uses the ca-bundle.crt file, which contains all well-known public CA certificates, for client-side processing.

4. Click **Save & Next**.

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

Create the McAfee 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.

Figure 11: Service configuration

To configure the service:

1. Under **Service List**, click **Add Service**.

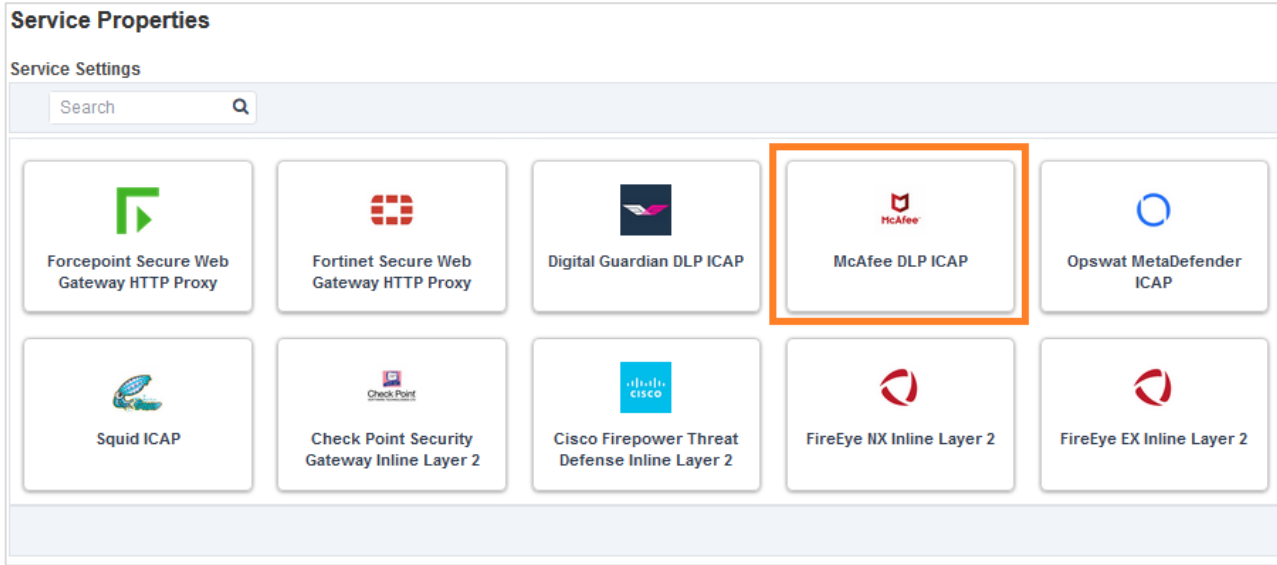2. In the service catalog, double click on the **McAfee DLP ICAP** service tile.

Figure 12: Service catalog

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 McAfee 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 McAfee DLP ICAP service.

13

ICAP Devices	Click **Add** and enter the IP address and port number of the McAfee DLP system. Make sure that 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. • **Referrer:** Allows 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.
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 length for McAfee 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.

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

Figure 13: McAfee DLP ICAP service properties page

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.

Configure 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.
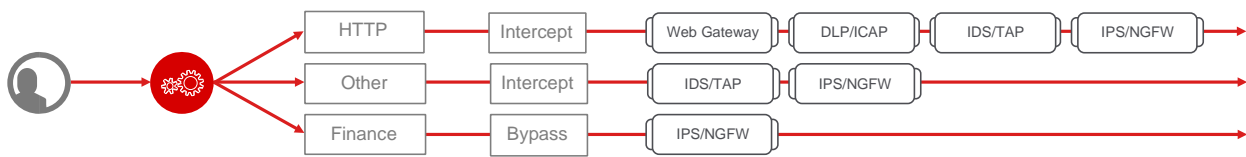

Figure 14: 'Traffic flows' through chains of different security services

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

Figure 16: Example service chain configuration with McAfee DLP ICAP service and Secure Web Gateway [SWG] service

2. Click **Save & Next**.

Security Policy

Security policies are the set of rules that govern how traffic is processed in SSL Orchestrator. The actions a rule can require include:

- Whether or not to allow the traffic indicated in the rule.

- Whether or not to decrypt that traffic.

- Which service chain (if any) to pass the traffic through.

Figure 17: Configuring security policy

SSL Orchestrator's guided configuration presents an intuitive rule-based, drag-and-drop user interface for the definition of security policies. In the background, SSL Orchestrator maintains these security policies as visual per-request policies. If traffic processing is required that exceeds the capabilities of the rule-based user interface, the underlying per-request policy can be managed directly.

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

Figure 19: Configuring interception rules

1. To create an interception rule, follow the guidance below.

Intercept Rule	User Input
Label	Enter a **Name** for the label
Description	Enter a **Description** for this Intercept Rule
Proxy Server Settings This setting, which displays when configuring an explicit proxy, defines the SSL Orchestrator explicit proxy listening IP address and proxy port. For explicit proxy authentication, this section also allows for the selection of an F5® Access Manager® (BIG-IP APM) SWG-explicit access policy.	
IPv4 Address	Specify the explicit proxy listening IP address.
Port	Specify the port number.
Access Profile	Specify the access policy (optional).
Ingress Network	
VLANs	This defines the VLANs through which traffic will enter. For a forward proxy topology (outbound), for instance, this would be the client-side VLAN (Intranet).

2. Click **Save & Next**.

Egress Setting

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

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

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 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**.

4. Upon successfully deployment of the configuration, SSL Orchestrator will display a dashboard. See Figure 21.
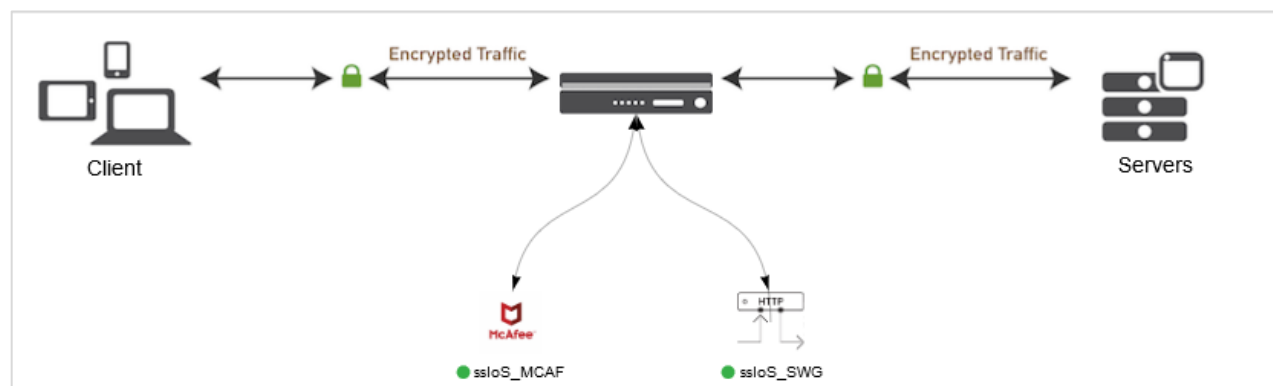
This completes configuration of SSL Orchestrator as a forward proxy. At this point an internal client should be able to browse to external (Internet) resources, and decrypted traffic will flow across the security services.

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.mcafee.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 forward proxy has intercepted the web request and reassigned the response from the web server, validating that the functionality enabled by SSL Orchestrator is working as expected.
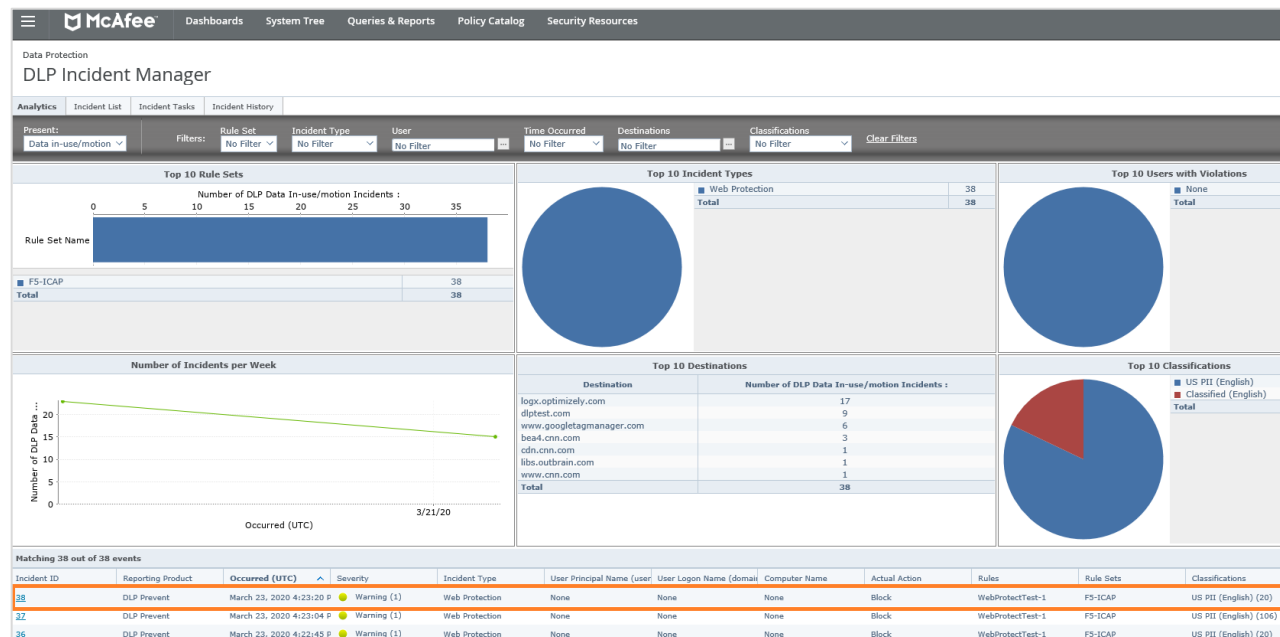
Decrypted Traffic Analysis

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

```
tcpdump –lnni eth<n> -Xs0
```

McAfee 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 McAfee ePO web UI. From the main menu, navigate to **Data Protection > DLP Incident Manager**. The DLP Incident Manager web page reports the PII violation.