Contents

Introduction ................................................................................................................................................... 3
Solution Overview ........................................................................................................................................ 3
   Service chaining ....................................................................................................................................... 4
   Prerequisites ........................................................................................................................................... 5
   Architecture best practices ................................................................................................................... 6
Initial Setup ................................................................................................................................................... 7
   Create a policy on the Symantec DLP ...................................................................................................... 7
      Add the monitor ................................................................................................................................... 7
      Create a policy.................................................................................................................................... 8
   Create a response rule ............................................................................................................................ 8
      Assign the response rule to the policy .................................................................................................. 9
Run the SSL Orchestrator Setup Wizard .................................................................................................... 9
Set up high availability ............................................................................................................................. 11
Update the SSL Orchestrator version ......................................................................................................... 13
SSL Orchestrator Configuration .................................................................................................................. 14
   Set up the deployment ............................................................................................................................ 15
   Create the ICAP service ........................................................................................................................ 17
   Set up the SSL profile ........................................................................................................................... 19
   Create service chains to link services ................................................................................................. 21
   Create the interception rule ................................................................................................................. 23
Testing the Solution .................................................................................................................................... 24
   Server certificate test ............................................................................................................................ 24
   Decrypted traffic analysis ...................................................................................................................... 25
   Symantec DLP policy violation ............................................................................................................... 25
Introduction

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 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® SSL Orchestrator™ and Symantec Data Loss Prevention (DLP) solution solves these two SSL/TLS challenges across cloud, mobile, and on-premises environments. SSL Orchestrator centralizes SSL 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 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 visibility and content adaptation.

- 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 them, providing SSL visibility for inspection.

- Within the decryption zone, the content adaptation feature of 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 (REPMOD). In this context, 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 (REPMOD), and re-encryption takes place for the return response from the web server to the client. See Figure 1.
Service chaining

A typical security stack often consists of more than a DLP system, with additional components such as a firewall, intrusion detection or prevention systems (IDS/IPS), web application firewalls, malware analysis tools, and more. To solve specific security challenges, security 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.

F5 SSL Orchestrator not only decrypts the encrypted traffic, it also load balances, monitors, and dynamically chains security services, including next-generation firewalls, DLPs, IDS/IPSs, web application firewalls, 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.

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 category subscription.
- IP geolocation.
- Host and domain name.
- An F5 URL filtering category subscription.
• Destination port.
• Protocol.

Figure 2: A service chain

Prerequisites

The F5® SSL Orchestrator™ product line—the i2800, i5800, i10800, i11800, i15800—supports this joint solution. SSL Orchestrator devices ship with an installed base module that provides both SSL interception and service chaining capabilities. SSL Orchestrator can also be deployed as an application on an existing F5® BIG-IP® system. Please contact your local F5 representative to understand the licensing and deployment options.

Unless otherwise noted, references to 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.

Optionally, customers can consider adding the functionality of:

• A URL filtering (URLF) subscription to access the URL category database.
• An F5 IP Intelligence subscription to detect and block known bad actors and bad traffic.
- A network hardware security module (HSM) to safeguard and manage digital keys for strong authentication.
- F5® Secure Web Gateway (SWG) Services to filter and control outbound web traffic using a URL database.
- F5® Access Manager™ to authenticate and manage user access.

To deploy this joint solution, you 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**

These recommended practices can help streamline the architecture to optimize performance, reliability, and security:

- **Deploy inline.** Any SSL visibility solution must be inline 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.** The Symantec DLP server 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.
- **Unlike some competing solutions, the F5 system does not need physical connections to the Symantec DLP. All that is required is L3 reachability—however, we recommend deploying the DLP system not more than one hop away.** Generally, when inspection devices are not directly connected to the F5 system, we highly recommend the use of network and VLAN controls to restrict access to the unencrypted data only to the inspection devices.
Initial Setup

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

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 Next.
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.

![Symantec DLP policy configuration](image)

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.
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.

Run the SSL Orchestrator Setup Wizard

After you plug in the F5 device, the first things to set up are the management IP address, netmask, and default routing from the command line of your system. Log in to the web UI using the configured management IP address (default web interface credentials are admin/admin). The SSL Orchestrator Setup Wizard guides you through the basic configuration. (Note: The Setup Wizard is substantially the same regardless of whether you are deploying SSL Orchestrator on an existing F5 system or new hardware. The few exceptions, such as SSL certificate configuration, can readily be performed manually on current F5 systems.)
Note: If at any time during configuration you need to return to the Set-Up Wizard, simply click the F5 logo in the upper-left corner of the Configuration utility, and on the Welcome screen, click Run the Setup Utility.

1. On the F5 Welcome screen, click Next.
2. On the License screen, click Activate.
3. Enter the Registration Key. Follow the F5 Licensing steps to activate the SSL Orchestrator license.
4. On the EULA screen, click Accept. The license activates and the system reboots.
5. Once the system has rebooted, the Device Certificates screen displays. Import a certificate authority (CA) signed device certificate or continue using the default, self-signed certificate. Click Next.
6. When the Platform screen displays, complete the following steps:
   i. Enter the Host Name for this system. The Host Name must be a fully qualified domain name.
   ii. Under User Administration, enter and confirm the Root Account passwords, and click Next. The root account provides access to the command line, while the admin account accesses the user interface.

![Platform configuration](image)

7. The system notifies you to log out and then log back in with your username (admin) and new password. Click OK. The system reboots.
8. Log in. The Forward Proxy Certificate page displays. An SSL CA certificate—preferably a subordinate certificate authority (CA)—and private key on the F5 system are needed to generate and issue certificates to the end host for client-requested HTTPS websites that are being intercepted. Enter the name for the certificate and import the sub CA certificate and key, then click Next.
9. On the Network web page, click Next to configure network settings.
10. The Redundancy web page displays. Deselect Config sync and click Next. (You will set up high availability [HA] after finishing the initial steps.)
11. When the Network Time Protocol (NTP) configuration screen displays, enter the IP Address of the NTP server to synchronize the system clock with, and click Add. Click Next.

12. (Optional, unless you plan to later use the DNSSEC option in the SSL Orchestrator configuration—in which case this step is required.) The Domain Name Server (DNS) screen displays. Complete the following steps:
   i. To resolve host names on the system, set up the DNS and associated servers: For the DNS Lookup Server List, type the IP Address of the DNS server and click Add.
   ii. If you use BIND servers, add them in the BIND Forwarder Server list.
   iii. Add local domain lookups (to resolve local host names) in the DNS Search Domain list.

13. Click Next. The configuration screen appears with a complete menu on the left. (See Figure 8.) You are ready to set up high availability and finalize your system for SSL Orchestrator.

![Figure 8: The SSL Orchestrator configuration screen once the initial setup is complete](image)

Set up high availability

F5 highly recommends deploying SSL Orchestrator in an HA pair to ensure a high level of operational performance. Before setting up HA, you should already have installed the secondary SSL Orchestrator unit and completed its initial setup.

1. Click the F5 logo in the upper-left corner of the Configuration utility, and on the Welcome screen, click Run Config Sync/HA Utility.
2. In the Standard Network Configuration section, click Next.
3. Leave the default settings for Redundant Device Wizard Options and click Next.
4. Enter the IP address and add the VLAN Interface for High Availability Network and VLAN configuration.
5. For **Network Time Protocol Configuration**, enter the NTP server’s **IP address** and click **Add**, if you didn’t already configure one during initial setup. Click **Next**.

6. For **Domain Name Server Configuration**, enter the DNS server **IP address** and click **Add**, if you didn’t already configure one in the Initial setup. Click **Next**.

7. For **Configuration Sync Configuration**, choose the Network IP address you configured in step 4 of this procedure, and click **Next**.

8. For **Failover Unicast configuration**, select the HA interface and management interface and click **Next**.

9. For **Mirroring Configuration**, select the HA interface as the **Primary Local Mirror Address**.

10. In the **Standard Pair Configuration** section, click **Next**.

11. Pause here, go to the secondary device, and complete steps 1-10 of this HA procedure for that device, too.

12. Returning to this primary device, under **Discover Configure Peer or Subordinate Device**, click **Next**.

13. Under **Retrieve Device Credentials**, enter the secondary SSL Orchestrator unit/peer **IP address**, enter the **Administration Username** and credentials, and click **Retrieve Device Information**.

14. Once the peer **Device Certificate** is verified, click **Device Certificate Matches**.

15. Verify the peer **Device Name** and click **Add Device**. This completes the active-standby HA setup.

---

Figure 9: Sample configuration for peer discovery to set up HA
Update the SSL Orchestrator version

Periodic updates are available for the SSL Orchestrator configuration utility. To download the latest:

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 10: The F5 product download web page](image)

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. Then log in to the F5 management interface and navigate to SSL Orchestrator > Updates.
6. Under Upgrade, for File Name, click Browse and navigate to the .rpm file you downloaded. Select it and click Open.
7. Click **Install**. Your system may reboot to effect the change.

**SSL Orchestrator Configuration**

Before you proceed to deploy the SSL Orchestrator application, you must have configured the internal and external networks including VLANs, IP addresses, and the default gateway. Refer to the [Basic Network Setting support on AskF5](#) for detailed steps.

In the sample configuration in Figure 12, the F5 system steers outbound web traffic through Symantec DLP, which is part of service chains of security devices.
Set up the deployment

This step must be completed before you can set up services, service chains, and classifier rules.

1. On the F5 management console, click SSL Orchestrator > Deployment > Deployment Settings.
2. Answer the configuration questions (see Figure 13) to create the SSL Orchestrator application. (Refer to the User Input column below for examples and tips.)
3. Click Finished.

<table>
<thead>
<tr>
<th>Configuration Field</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Application Service Name</td>
<td>Type a name for the SSL Orchestrator deployment.</td>
</tr>
<tr>
<td>(Deployment Name)</td>
<td></td>
</tr>
<tr>
<td>Strict Update</td>
<td>Select the check box if you want strict updates enforced to protect your configuration. If this is enabled, you cannot manually modify any of the settings produced by the application. Once this is disabled, you can manually change your configuration. However, we strongly recommend that you enable this setting to avoid misconfigurations that can render your application completely unusable.</td>
</tr>
<tr>
<td>Deployed Network</td>
<td>Specify the SSL Orchestrator deployed network as either Layer 2 (L2) Wire or Layer 3 (L3) Network.</td>
</tr>
<tr>
<td>IP Family</td>
<td>Specify whether you want this configuration to support IPv4 addresses, IPv6 addresses, or both.</td>
</tr>
</tbody>
</table>
### Manage SNAT Settings

Choose **Auto Map** to replace the client source IP address with the self IP address belonging to the egress for outbound traffic. This is recommended for small traffic volumes due to limitation of port numbers that can be allocated for translations.

For larger volumes of traffic, F5 recommends use of a **SNAT** (Secure Network Address Translation) pool to scale translations instead of overloading the egress interface IP address. When **SNAT** is chosen, you will need to enter **IPv4 SNAT addresses** for the SNAT pool for translations.

### Gateways

Specify whether to route outbound using the **Default route** on the F5 system or enter the **IP address** to be used as the default gateway.

### DNS

#### DNS Query Resolution

This solution uses DNS extensively. You can either permit the system to send DNS queries directly out to **Internet Authoritative Name Server** or specify one or more **Local Forwarding Name Servers** to process all DNS queries.

Direct resolution can be more reliable than using forwarders but requires outbound UDP/TCP port 53 access to the Internet.

#### Local Forwarding Nameserver(s)

If you selected **Local Forwarding Name Servers**, type the **IP address** of one or more name server(s) which will resolve all DNS queries from this solution and click **Add**.

#### Local/Private Forward Zones

If you selected **Internet Authoritative Name Server** type the **IP address** of one or more nameservers and click **Add**.

#### DNSSEC Validation

Specify whether you want to use DNSSEC to validate the DNS information.

### Logging

#### Logging Level

F5 recommends leaving the logging level at the default, **Errors**. Log on functional errors, unless you need to troubleshoot.
Create the ICAP service

You can configure up to 10 ICAP services using the SSL Orchestrator configuration utility. After you create the ICAP service and add it to a TCP service chain, SSL Orchestrator sends only HTTP traffic to that chain.

1. On the main tab of the F5 management interface, navigate to **SSL Orchestrator > Services > ICAP Services**. The ICAP Services screen displays.
2. Click **Create** to create the ICAP service and configure using the guidance below.
3. Click **Finished**.
<table>
<thead>
<tr>
<th>Configuration Field</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a Name for the ICAP service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters are not case sensitive.</td>
</tr>
<tr>
<td>ICAP Devices</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 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 processes 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. |
Set up the SSL profile

An SSL CA certificate—preferably a subordinate certificate authority (CA)—and private key on the F5 system are needed to generate and issue certificates to the end host for client-requested HTTPS websites that are being intercepted. For the complete procedure, see solution K13302 on AskF5: Configuring the BIG-IP system to use an SSL chain certificate.

1. On the main tab of the F5 management interface, navigate to SSL Orchestrator > SSL Management > SSL Settings. The SSL Settings Services screen displays.
2. Click Create to create and configure the SSL profile using the guidance below.
3. Click Finished.
## Configuration Field | User Input
--- | ---
**General Properties** |  
**Application Service Name** | Type a name for the SSL profile.

**Proxy Section** |  
**Forward Proxy** | Leave the enable box checked.

**Bypass on Handshake Alert** | Leave the default disabled option selected to disable SSL forward proxy bypass on receiving a handshake failure, protocol version, or unsupported extension alert message during the server-side SSL handshake.

**Bypass on Client Cert Failure** | Leave the default disabled option selected to disable SSL forward proxy bypass on failure to receive the requested client certificate.

**Client-Side SSL** |  
**Cipher Type** | Select Cipher String for the default cipher list.

**Certificate Key Chains** | Select the default.crt certificate, default.key key, default.crt chain and leave the passphrase field empty. Click Add.

**CA Certificate Key Chains** | Specify one or more configured Subordinate Certificate Authority (CA) certificates and keys to associate with the SSL profile. Select Certificate, Key Chain, and Passphrase settings for the certificate key chain. (If the key does not have a passphrase, leave that field blank.) Then click Add.

**Server-Side SSL** |  
**Cipher Type** | Select Cipher String for the default cipher list.

**Ciphers** | Uses the ca-bundle.crt file, which contains all well-known public certificate authority (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 has expired.

**Untrusted Certificate Response Control** | Select drop or ignore the connection even if the specified Certificate Response Control (CRL) file is not trusted.

**OCSP** | Specify the supported OCSP.

**CRL** | Specify the supported CRL.
Create service chains to link services

Before you can set up service chains, you must have configured all the services (HTTP, ICAP, L2, L3 & TAP). By default, SSL Orchestrator steers traffic through all the services. You can create a new service chain by defining the preferred order in which traffic should be steered.

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.

1. From the F5 device management interface, navigate to SSL Orchestrator > Policies > Access Per-Request Policies. The Per-Request Policies screen displays.

2. Click Create to create and configure the per-request service chain using the guidance below.
3. Click Finished.

4. On the Per-Request Policies screen that appears, click + Show All below the per-request policy and click the TCP policy name to review it. The policy editor page will display so you can further finetune the policy using advanced configurations as desired. In the sample in Figure 17, for example, you could click **SSL Intercept Policy** to bypass SSL traffic destined to websites that expose personal user information, such as banking, financial, or government sites.
Create the interception rule

Before you create an interception rule, you must create one or more service chains.

1. On the F5 device management interface, navigate to SSL Orchestrator > Deployment > Interception Rules. The SSL Settings Services screen displays.

2. Click Edit Default Outbound Rules to create and configure the rule using the guidance below.

3. Click Finished.

<table>
<thead>
<tr>
<th>Configuration Field</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Properties</strong></td>
<td>Leave all General Properties settings at their defaults.</td>
</tr>
<tr>
<td><strong>Proxy Setting</strong></td>
<td></td>
</tr>
<tr>
<td>Proxy Scheme</td>
<td>SSL Orchestrator can operate in transparent and/or explicit proxy mode. If you choose explicit proxy, enter the IP address and port number of the explicit proxy.</td>
</tr>
<tr>
<td>Classify UDP</td>
<td>If you selected transparent proxy above, by default TCP traffic will be managed but UDP traffic will pass through unexamined. Ensure Classify UDP is selected to manage UDP as well as TCP traffic.</td>
</tr>
<tr>
<td>Allow non-UDP/non-TCP</td>
<td>If you selected transparent proxy above, non-TCP, non-UDP traffic (such as IPSec, SCTP, and OSPF) will be blocked. Ensure this option is selected to pass non-UDP and non-TCP traffic.</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
</tr>
<tr>
<td>SSL</td>
<td>Select the SSL profile.</td>
</tr>
<tr>
<td>Per Request Policy</td>
<td>Select the per-request policy you want.</td>
</tr>
<tr>
<td>Ingress Network</td>
<td></td>
</tr>
<tr>
<td>VLANs</td>
<td>Select one or more Ingress VLANs where the client traffic will arrive.</td>
</tr>
<tr>
<td>L7 Interception Rules</td>
<td></td>
</tr>
<tr>
<td>Protocols</td>
<td>Specifies the protocol of the connection (based on port or protocol recognition) for interception.</td>
</tr>
</tbody>
</table>
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 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 forward proxy 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 -l -n -i 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 SSL Orchestrator is working as expected.