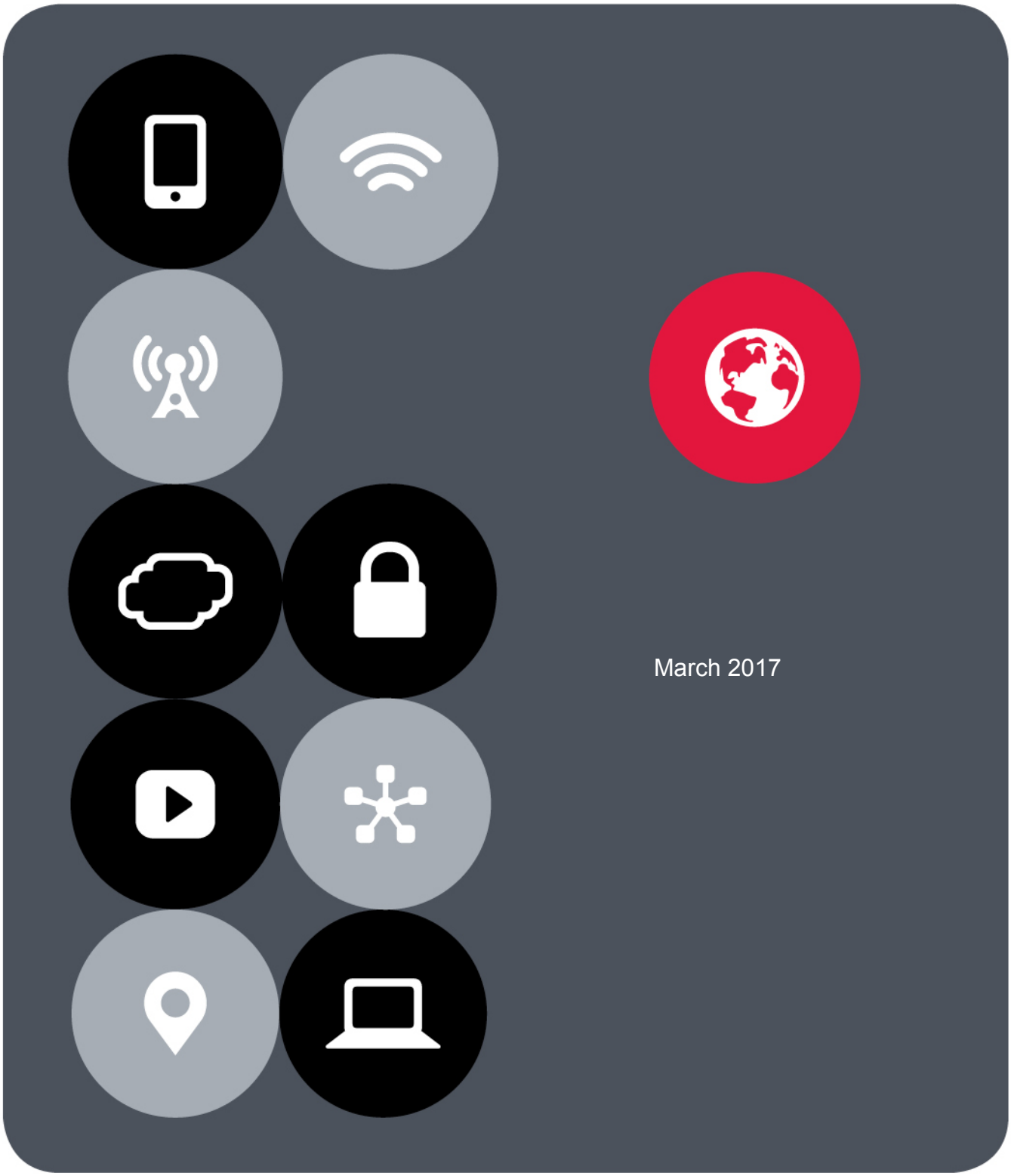
RECOMMENDED PRACTICES GUIDE

The F5 SSL Orchestrator and Symantec DLP Solution:

SSL Visibility and Content Adaption for Data Loss Prevention



March 2017

Contents

Introduction

The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), have been widely adopted by organizations to secure IP communications, and their use is growing rapidly. 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 when inspecting the encrypted traffic. 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 reference to service chain architectures.
- Recommends practices.
- Offers guidance on enforcement of corporate Internet use policies.

Solution Overview

Functional implementation of the solution involves two components: SSL visibility and content adaptation.

- F5 SSL Orchestrator, deployed inline to the wire traffic on either an F5® Herculon™ or F5® BIG-IP® platform, intercepts any outbound secure web request and establishes two separate SSL connections, one with the internal client (the user device) and the other with the requested web server. This creates a decryption zone in between, 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 (REQMOD). 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 (RESPMOD), and re-encryption takes place for the return response from the web server to the client. See Figure 1 for the various elements of the solution automatically created by SSL Orchestrator based on user inputs (which are explained later).

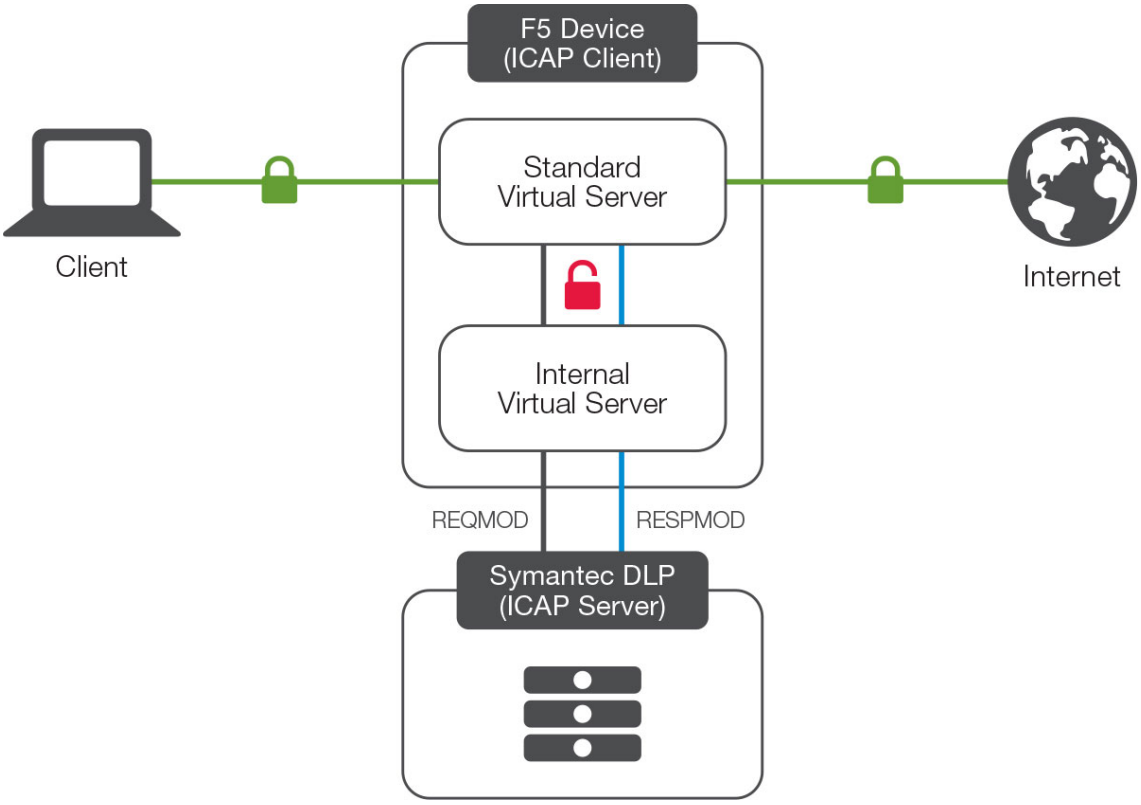


Figure 1: SSL interception and content adaption for modifying HTTP requests and responses

Service chaining

A typical security stack often consists of more than a DLP system. It begins with a firewall, but almost never stops there, with components such as 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, creating a bare-bones security stack consisting of multiple services. In this model, all user sessions are provided the same level of security, as this “daisy chain” of services is hard-wired.

As shown in Figure 2, F5 SSL Orchestrator can load balance, monitor, and dynamically chain together 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 whether to bypass or to decrypt, with decisions about whether to send data to one set of security services or another. This policy-based traffic steering enables better utilization of the existing security services investment and helps to reduce administrative costs.

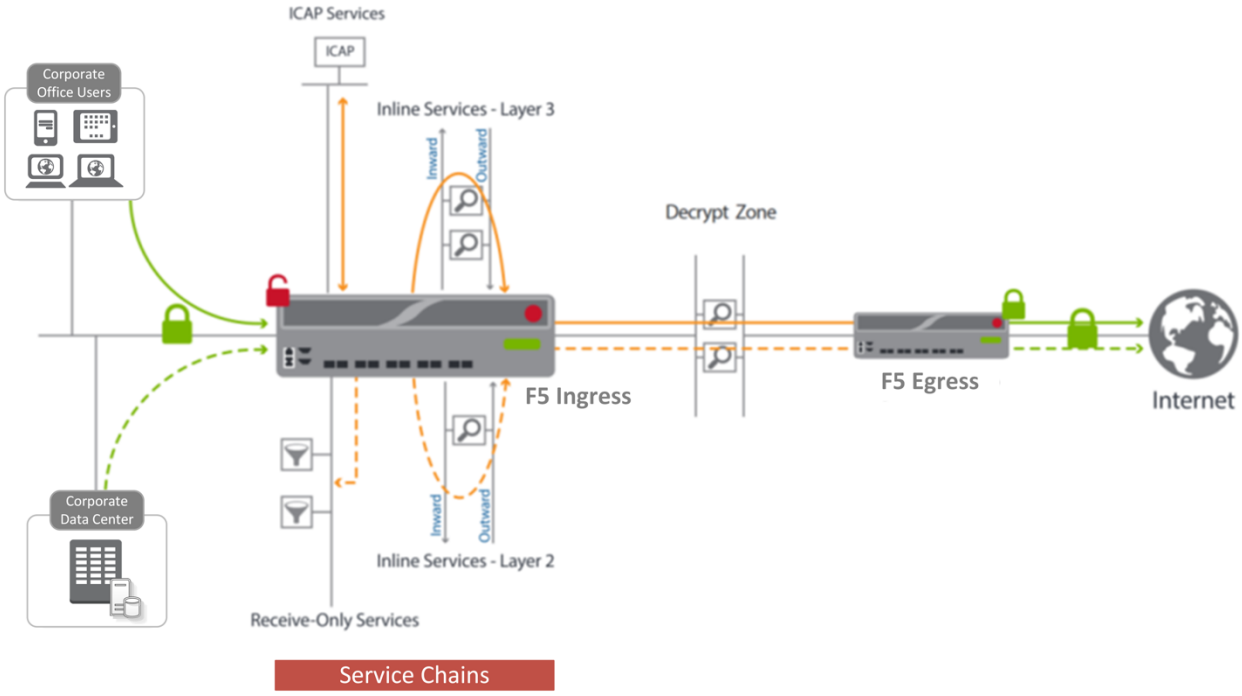


Figure 2: The SSL Orchestrator service chain architecture

SSL Orchestrator enables you to apply different service chains based on context derived from a powerful classification engine. That context can come from:

- Source IP/subnet.
- Destination IP/subnet.
- IP intelligence category.
- IP geolocation.
- Host and domain name.
- URL filtering category.
- Destination port.
- Protocol.

Prerequisites

The recently launched F5® Herculon® SSL Orchestrator™ product line—including the i2800, i5800, i10800—and the existing F5 BIG-IP family of products support this integration. By default, Herculon SSL Orchestrator ships with an installed base module that provides both SSL interception and service chaining capabilities. When deploying the SSL Orchestrator application on a BIG-IP system, however, you must provision BIG-IP® Local Traffic Manager™ (LTM) with a forward proxy add-on license.

For simplicity's sake, unless otherwise noted, references to the BIG-IP system in this document (and some user interfaces) also apply to the Herculon system. The solution architecture and configuration are identical.

Optionally, customers can consider the following modules, which provide additional functionality:

- **A URLF Filtering subscription** to access the URL category database for filtering.
- **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.

To deploy this integration, you first must have installed Symantec DLP Software version 14.5, Maintenance Pack 1 or higher. (Symantec DLP is sometimes also referenced by its acquisition name, Vontu DLP.) 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, the Enforce Server, and a detection server are all installed on the same server. This is a common installation type for testing or risk assessment purposes.
- **Two-tier:** The Oracle Database and the Enforce Server are on the same server, with the detection server on a separate server.
- **Three-tier:** The Oracle Database, the Enforce Server, and a detection server are each on a separate server.

Refer to the installation guide for complete guidance on Symantec DLP installation. (You may need to be a registered user with appropriate privileges to access the resources on the Symantec website.)

An SSL CA certificate—preferably a subordinate certificate authority (CA)—and private key on the F5 system are also needed to generate and issue certificates to the end host for client-requested HTTPS websites that are being intercepted.

Architecture best practices

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

- Deploy inline. Any SSL 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), which are rapidly growing in use. Although the F5 system can be deployed in either inline or passive mode, we highly recommend deploying it inline for this solution.
- Deploy the F5 systems in a device sync/failover device group (S/FDG), which includes the active-standby pair, with a floating IP address for high availability (HA).
- 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 by using 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 the system requires is L3 reachability—however, we recommend deploying the DLP system not more than one hop away. As a generic guideline, 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

A few initial steps should be completed before moving into detailed configuration of SSL Orchestrator. In addition to the tasks below, refer to the Symantec configuration guide for complete guidance on Symantec DLP configuration. (You may need to be a registered user with appropriate privileges to access the resources on the Symantec website.)

Create a policy on the Symantec DLP

Log in to the web UI of the Symantec DLP Enforce Server from a browser. Before creating a policy, you need to 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 of the page.
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, then 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 and not inspect potentially important content.) Then select or enter your request and response filtering configuration values.

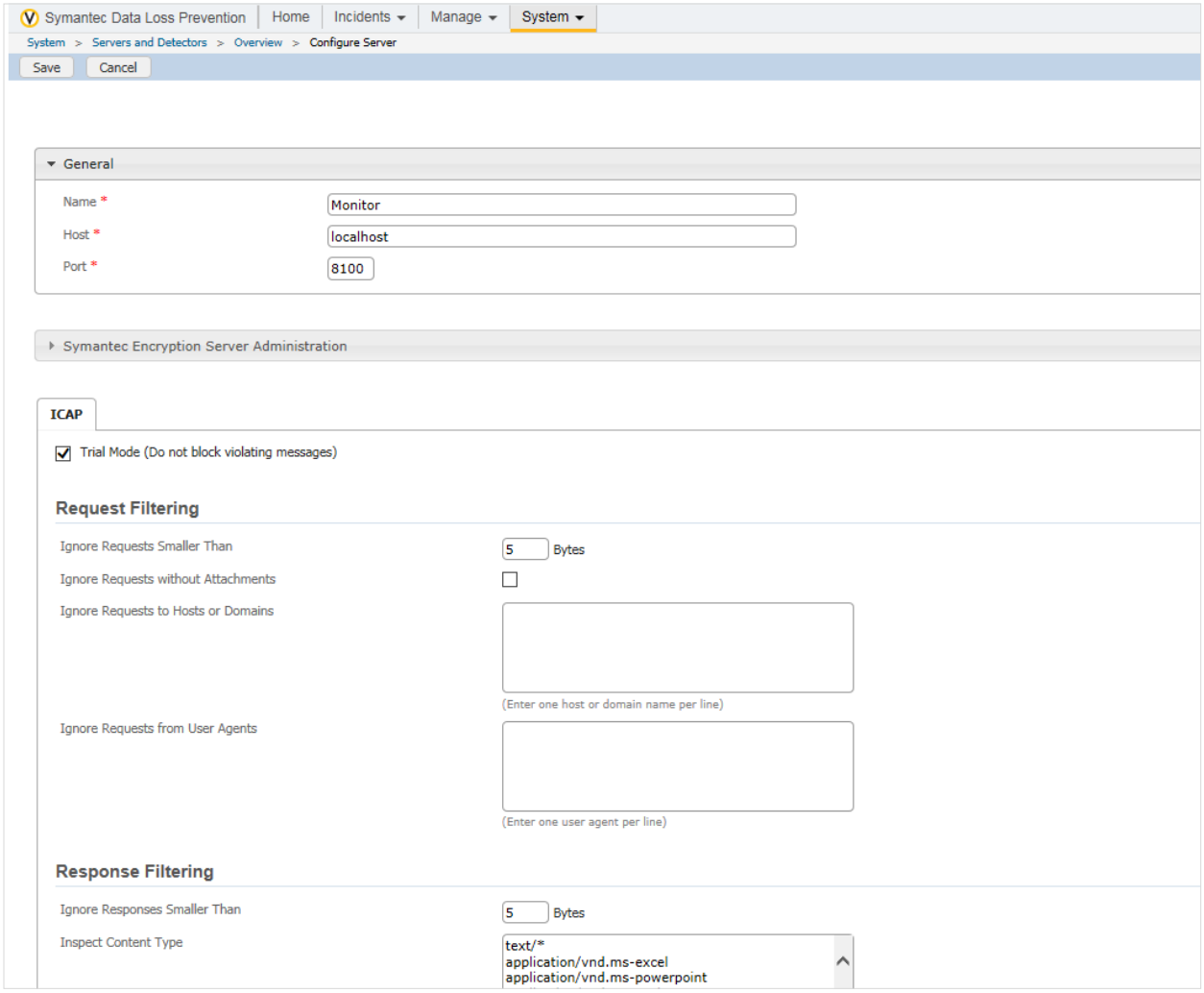


Figure 3: Add the monitor to the Enforce Server

Create a policy

1. From the main menu, navigate to **Manage > Policies > Policy List**.
2. Click **Add Policy** at the top of the page and then click **Next**.
3. On the **Configure Policy** page, enter the policy **Name** and click **Add Rule**.
4. On the **Add Detection Rule** page, choose a **Rule Type** and click **Next**.
5. On the **Edit Rule** page, enter the rule **Name** and matching criteria. Then click **OK**.
6. Once you're returned to the **Configure Policy** page, click **Save**.

See Figure 4 for a sample configuration of a policy named *symconfidential* with a rule type of *Content Matches Keyword* and the keyword *confidential*.

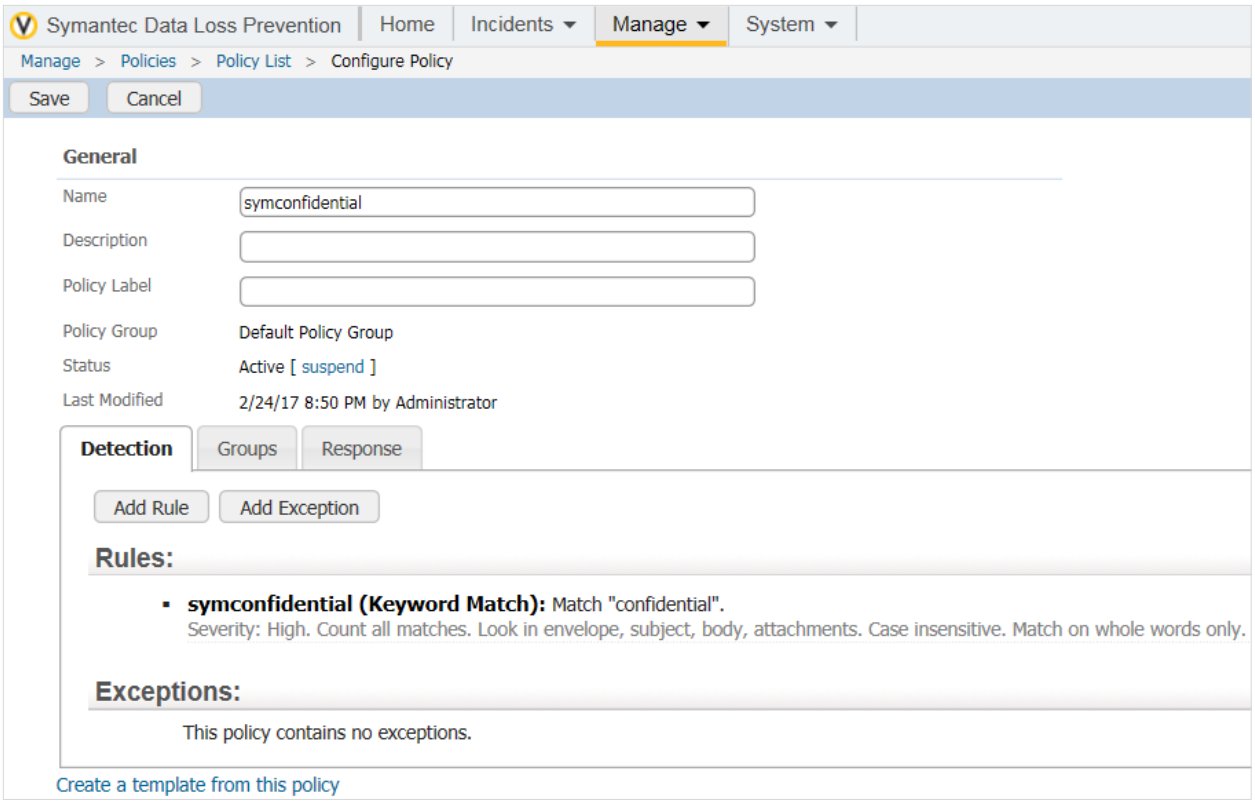


Figure 4: Symantec DLP policy configuration

Create a response rule

1. From the main menu, navigate to **Manage > Policies > Response Rules**.
2. Click **Add Response Rule** at the top of the page and click **Next**.
3. On the **Configure Response Rule** page, enter the rule **Name**, choose the **Action**, and click **Add**.

The sample configuration in Figure 5 shows a response rule named *block* with the action *Prevent: Block.*

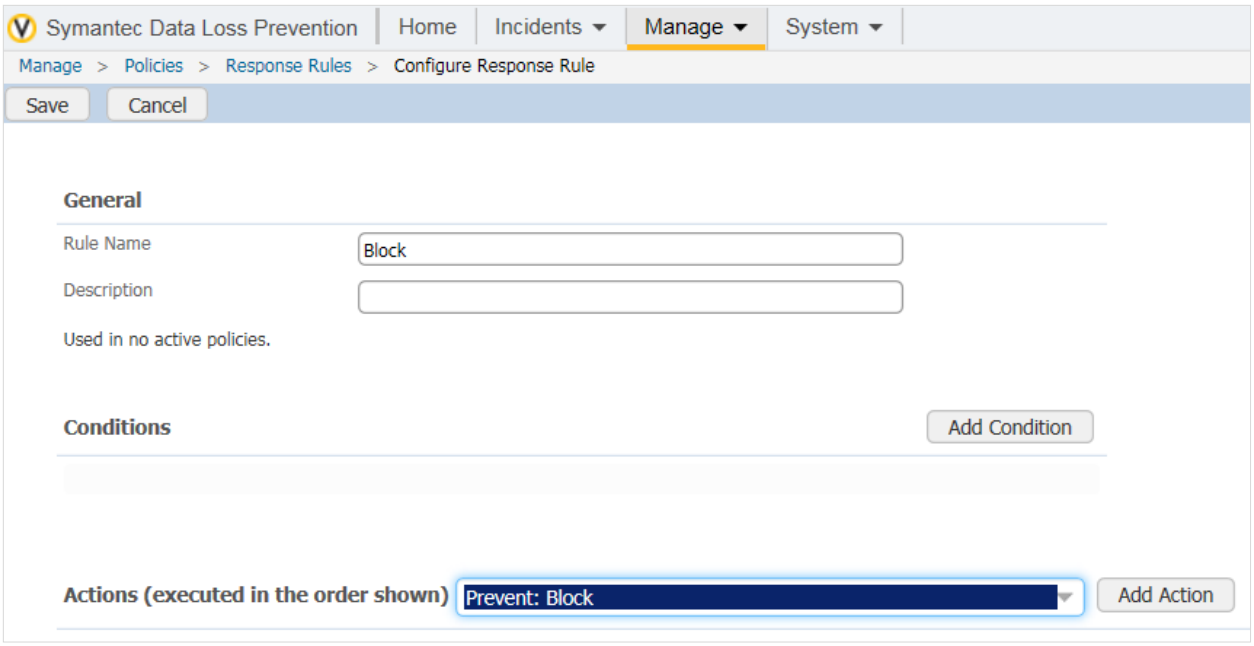


Figure 5: The creation of a response rule

Assign the response rule to the policy

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

Run the SSL Orchestrator Setup Wizard

After you plug in the power supply to the F5 Herculon device, the first things to set up are the management IP address, netmask, and default routing from the command line of your system. (Note: The BIG-IP Setup Wizard is substantially the same, with the exception of a few configuration items, such as SSL certificate configuration, that can readily be performed manually on the BIG-IP system.)

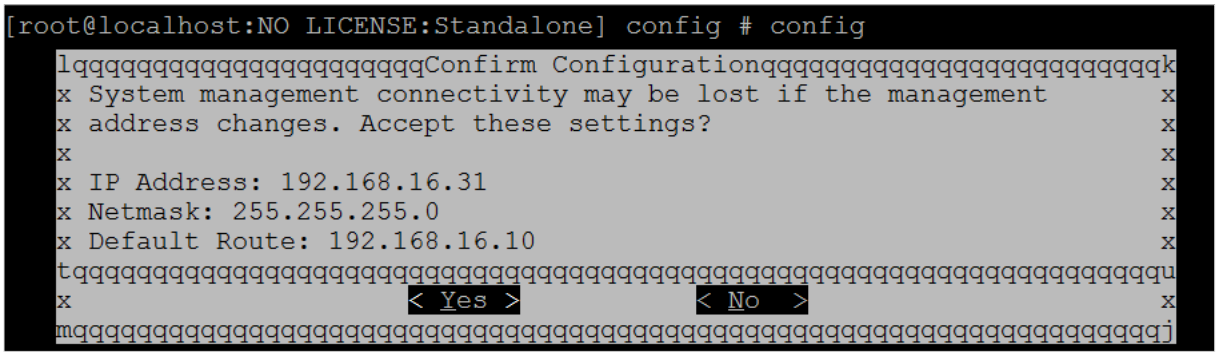


Figure 6: Initial configuration of the management IP from the command line

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, minimal setup configuration for F5 SSL Orchestrator.

Note: If at any time during configuration you need to return to the SSL Orchestrator 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. On the **EULA** screen, click **Accept**. The license activates and the system reboots.
4. Once the system has rebooted, click **Continue**.
5. On the **Device Certificates** screen, click **Next**.
6. Once the **Platform** screen appears, 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** and **Admin Account** passwords, and click **Next**. The Root Account provides access to the command line, while the Admin Account accesses the user interface.

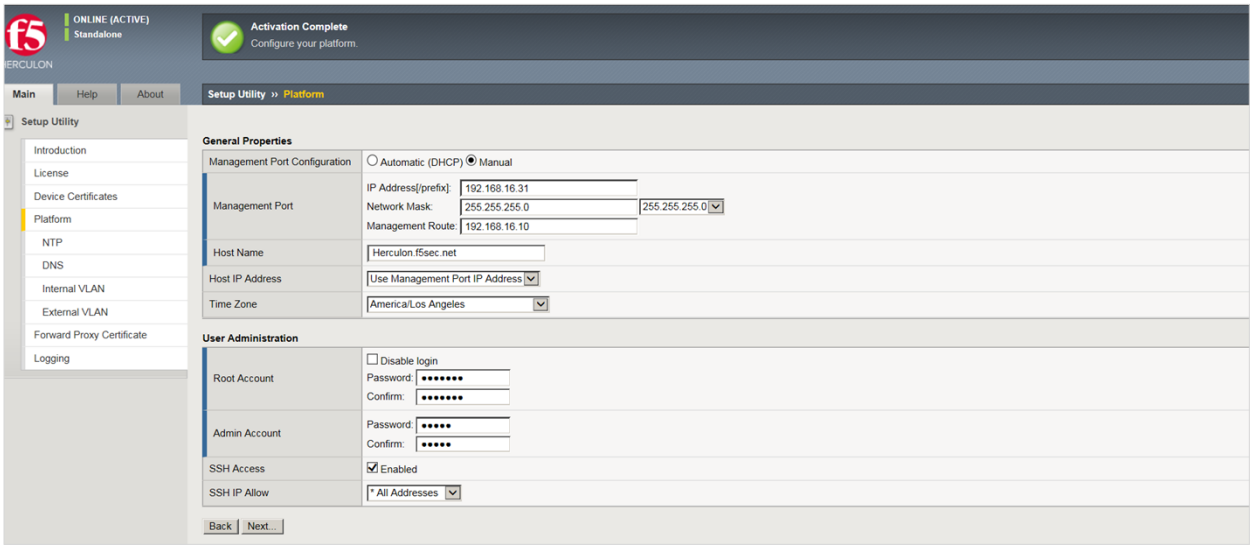


Figure 7: Platform configuration

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. Once the **Network Time Protocol** (NTP) configuration screen opens, enter the IP **Address** of the NTP server to synchronize the system clock with, and click **Add**. Click **Next**.
9. (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 opens. 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.

iv. Click **Next**. The **Internal VLAN** screen opens.

10. On the **Internal VLAN** screen, specify the **Self IP** settings for the internal network:

    i. Enter a self IP **Address**.

    ii. Enter a network mask (**Netmask**) for the self IP address.

    iii. Retain the default values for the **Port Lockdown** and **VLAN Tag ID** settings.

    iv. Under **Interfaces,** select an interface number from the **VLAN Interfaces** list, and then select Tagged or Untagged from the **Tagging** list. (Select **Tagged** when you want traffic for that interface to be tagged with a VLAN ID.) Click **Add.**

    v. Click **Next**. This completes the configuration of the internal VLAN.

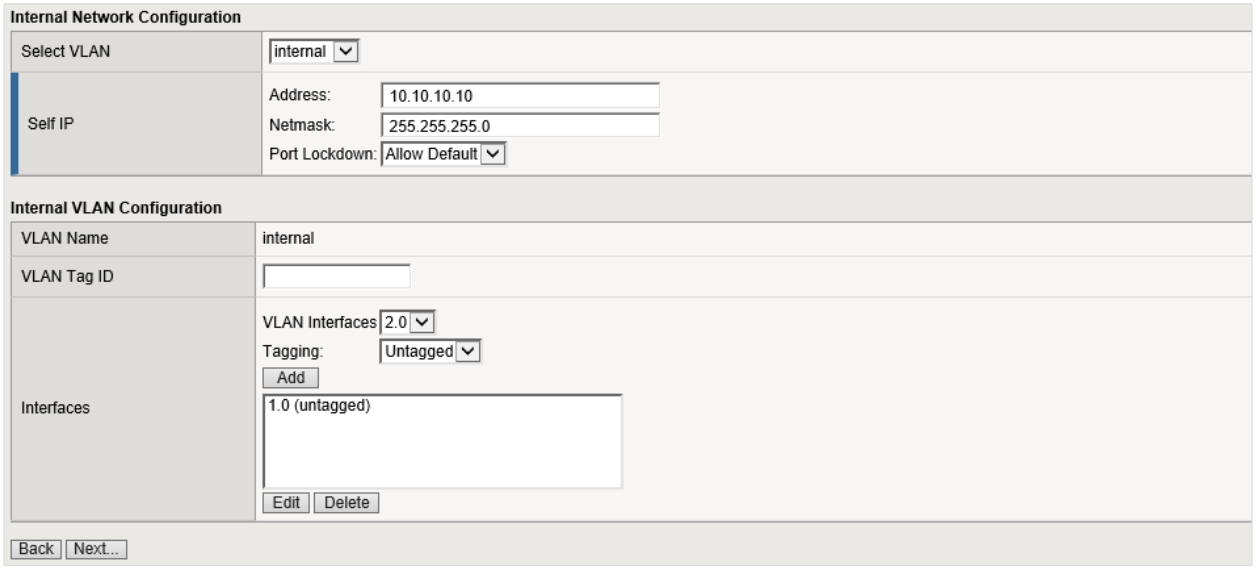


Figure 8: Internal VLAN configuration

11. The **External VLAN** screen opens. Specify the **Self IP** settings for the external network:

    i. Enter a self IP **Address**.

    ii. Enter a network mask (**Netmask**) for the self IP address.

    iii. Retain the default value for the **Port Lockdown** setting.

    iv. Enter the IP address you want to use as the **Default Gateway** to the external VLAN.

    v. Retain the default value (auto) for the **VLAN Tag ID** setting. Click **Next**. This completes the configuration of the external self IP addresses and VLAN.

12. On the **Forward Proxy Certificate** screen, complete the following configuration to import the CA certificate:

    i. For the **Certificate Name**, select **Create New** and enter a name.

ii. For the **Certificate Source**, either select **Upload File** and choose a file, or select **Paste Text** and use copy and paste to enter your certificate source.

iii. For the **Key Source**, either select **Upload File** and choose a file, or select **Paste Text** and use copy and paste to enter your key source.

iv. If your certificate/key source is protected by a passphrase, select **Password** as the **Security Type**, and enter the passphrase. Otherwise leave the default setting. Click **Next**.

13. On the **Logging** screen, select either local or Splunk as the **Publisher Type**.
    - If you select local, specify the **Destination**—either local-db or localsyslog. This determines the destination of your logs, either a local database or a localsyslog server.
    - If you select Splunk, for **Protocol**, select either TCP or UDP. Enter the **IP Address** and **Port** of the Splunk server.
14. Click **Finish**. The SSL Orchestrator configuration page appears with a complete menu displayed on the left side of the page.

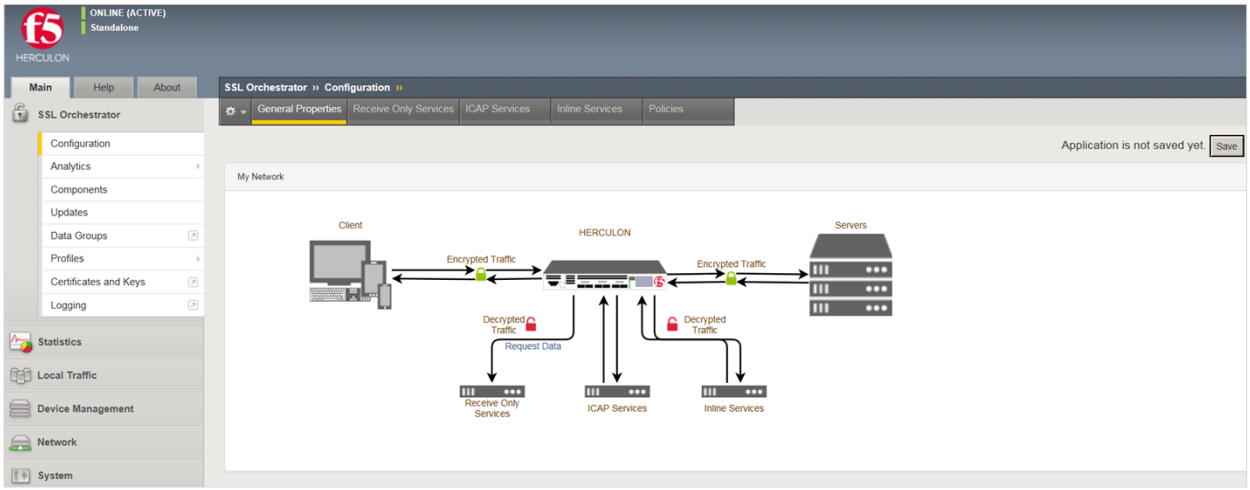


Figure 9: The SSL Orchestrator configuration screen once the initial setup is complete

You are now ready to proceed to the second part of configuration, where you finalize your system for SSL Orchestrator.

Update the SSL Orchestrator version

Periodic updates are available for the SSL Orchestrator configuration utility. To download the latest, follow these steps:

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 and select SSL Orchestrator.

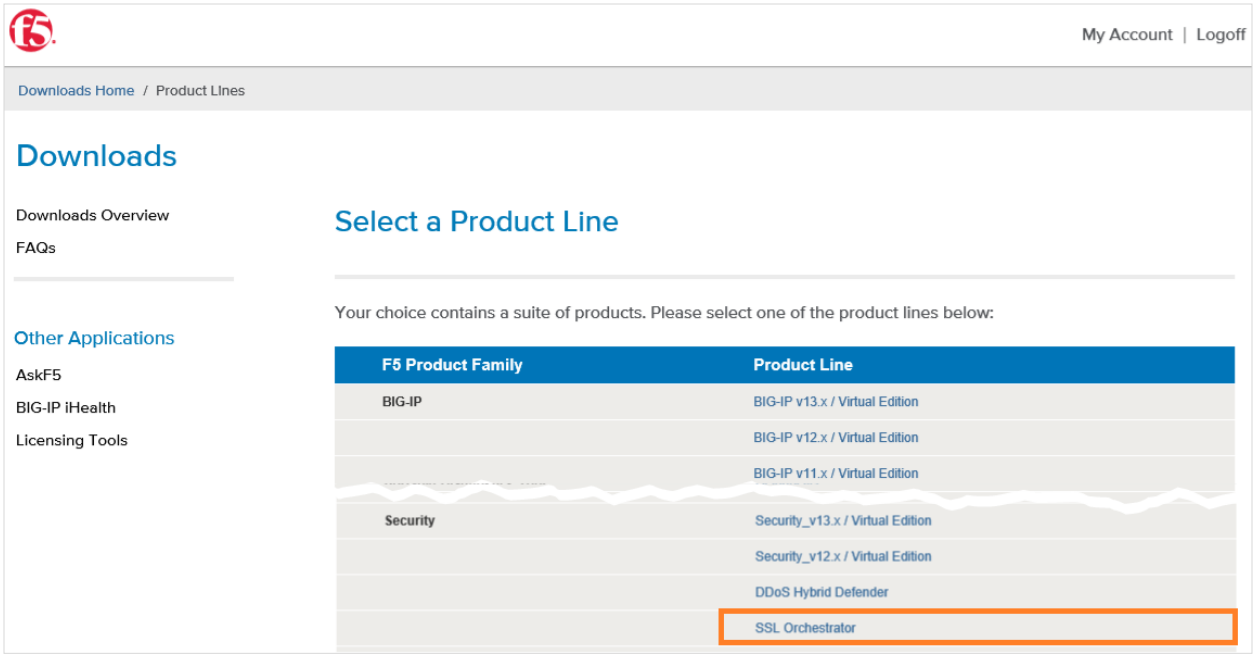


Figure 10: The F5 product download web page

4. Click the SSL Orchestrator container.
5. Select and download the latest version of the SSL Orchestrator .rpm file.
6. Read through the appropriate Release Notes before attempting to use the downloaded file.
7. Once you've read the release notes, log in to the main tab of the F5 device management interface and navigate to **SSL Orchestrator > Updates**.
8. Under **File Name**, click **Browse** and navigate to the .rpm file you saved onto your system. Click **Open** to select it.

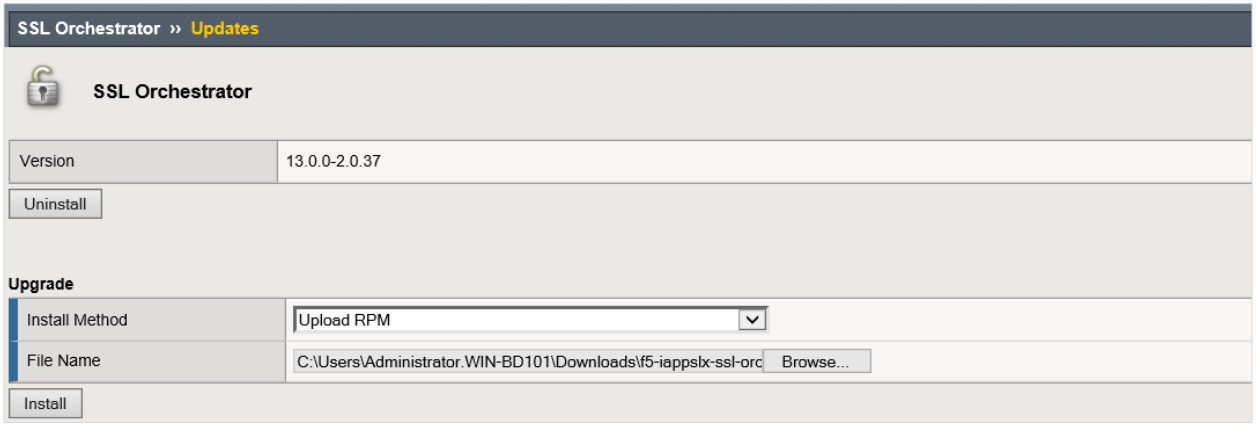


Figure 11: SSL Orchestrator update

9. Click **Install**. The latest version of the SSL Orchestrator configuration utility will be installed. Your system may reboot to make the change take effect.

Back up your F5 system configuration

Before beginning the detailed SSL Orchestrator configuration, we strongly recommend you back up the system configuration using the following steps. This enables you to restore the previous configuration in case of any issues.

1. From the main tab of the F5 management interface, click **System** > **Archives**.
2. To initiate the process of creating a new UCS archive (backup), click **Create**.
3. Enter a *unique* **File Name** for the backup file.
4. Optional:
   - If you want to encrypt the UCS archive file, from the Encryption menu, select Enabled and enter a passphrase. You must supply the passphrase to restore the encrypted UCS archive file.
   - If you want to exclude SSL private keys from the UCS archive, from the Private Keys menu, select **Exclude**.

Figure 12: New system archive creation

5. Click **Finished** to create the UCS archive file.
6. When the backup process is done, examine the status page for any reported errors before proceeding to the next step.
7. Click **OK** to return to the Archive List page.
8. Copy the .ucs file to another system.

To restore the configuration from a UCS archive, navigate to **System > Archives**. Select the name of the UCS file you want to restore and click **Restore**. For details and other considerations for backing up and restoring the system configuration, see Solution K13132 on AskF5: Backing up and restoring BIG-IP configuration files.

SSL Orchestrator Configuration

The example configuration below demonstrates the F5 system steering the outbound web traffic through Symantec DLP, which is part of service chains of security devices. Please refer to the F5 Herculon SSL Orchestrator Setup guide for additional reference during the configuration.

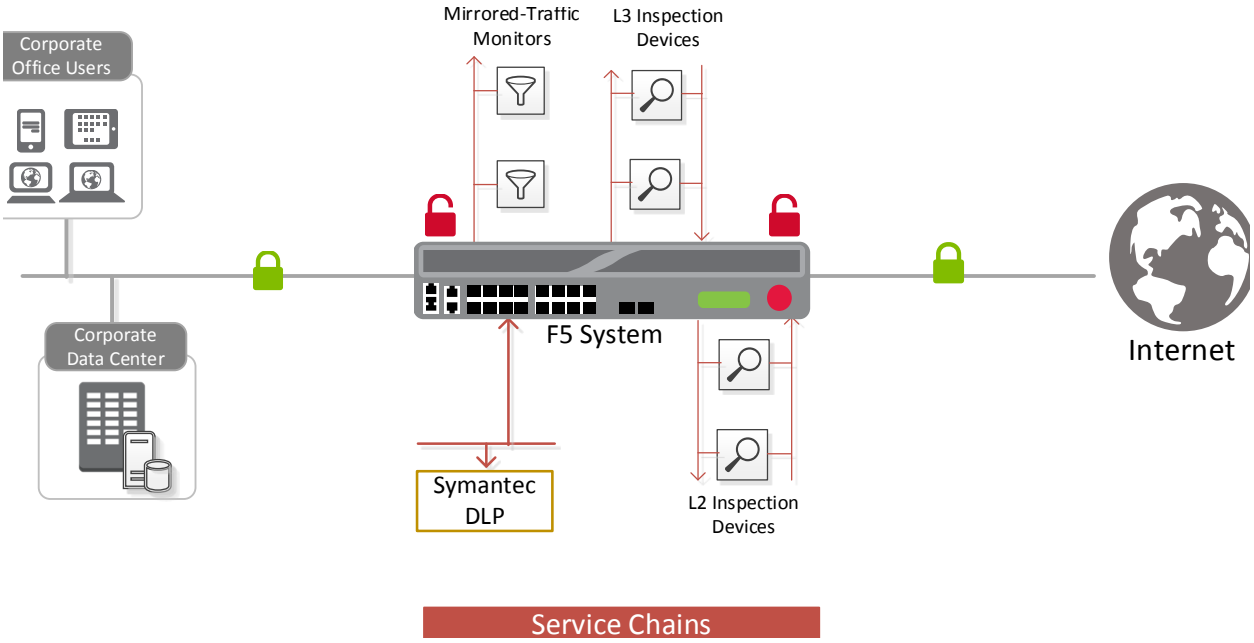


Figure 13: Symantec DLP in an SSL Orchestrator service chain architecture

Set up general properties

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

1. On the main screen of the management console, click **SSL Orchestrator** > **Configuration** > **General Properties**.
2. Answer the configuration questions (see Figure 14) to create the SSL Orchestrator application. (Refer to the User Input column below for examples and tips.)

Question	User Input
Application Service Name	Enter a name without spaces or dashes for the SSL Orchestrator application.
Do you want to set up separate ingress and egress devices with a cleartext zone between them?	You can configure a single Herculon or BIG-IP device to receive both ingress and egress traffic on different networks, or you can configure separate Herculon or BIG-IP devices for ingress and egress traffic. If you choose the latter option, you are asked further questions to enter peer application names, control channel virtual server IPs, and pre-shared keys to establish and protect the communication between the devices. Otherwise, select **No, use one BIG-IP device for ingress and egress**. This sample configuration follows that option.
Which IP address families do you want to support?	Select **Support IPv4 only**. (Currently SSL Orchestrator only supports IPv4 families.)
Which proxy schemes do you want to implement?	SSL Orchestrator can operate in transparent and/or explicit proxy mode. If you choose explicit proxy, a separate explicit proxy configuration section displays for you to choose the VLANs that explicit proxy needs to listen to and so you can enter the IP address and port number of the explicit proxy. Select **Implement Transparent proxy only**.

Do you want to pass UDP traffic through the transparent proxy unexamined?	This option only applies if you selected **Implement transparent proxy only** above. By default, transparent proxy mode manages TCP traffic but allows UDP traffic to pass through unexamined. Choose **No** to prevent the passage of unexamined UDP traffic. Otherwise, select the default, **Yes, pass all UDP traffic unexamined**.
Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?	This option also only applies if you select **Implement transparent proxy only**. By default, transparent proxy mode passes through non-TCP, non-UDP traffic (such as IPSec, SCTP, and OSPF). Choose **No** to block. Otherwise, select the default, **Yes, pass non-TCP, non-UDP traffic**.
Which is the SSL Forward Proxy CA certificate?	Select the certificate authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
Which is the SSL Forward Proxy CA private key?	Select the corresponding private key, which you imported with the CA certificate while configuring the Setup Wizard. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
What is the private-key passphrase (if any)?	Enter the private-key passphrase, if any. If the key does not have a passphrase, leave this field empty.
Which CA bundle is used to validate remote server certificates?	The CA bundle is the collection of root and intermediate certificates for the CA you trust to authenticate servers where your clients might connect. The CA bundle is also known as the local trust store. Select the CA bundle that validates the remote server certificates.
Should connections to servers with expired certificates be allowed?	Remote servers can present expired certificates. Allowing connections to servers with expired certificates can cause a security risk. Legitimate servers do sometimes offer certificates which are overdue for renewal or which were signed by legitimate CAs but that are simply unknown to the F5 system. In the latter case, if you allow connections, consider adding any needed CA certificates to the F5 system CA bundle (trust store). Select **No, forbid connections to servers with expired certificates** to prevent connections to servers that have expired certificates.
Should connections to servers with untrusted certificates be allowed?	Remote servers can present untrusted certificates. Allowing connections to servers with untrusted certificates can cause a security risk. Select **Yes, allow connections to servers with untrusted certificates** if appropriate for your situation and security policies.
Should strict updates be enforced for this application?	If you select this option, you cannot manually modify any settings produced by the application. Once you disable this option, you can manually change your configuration. F5 recommends enabling this setting (select Yes) to avoid misconfigurations that can cause an unusable application.

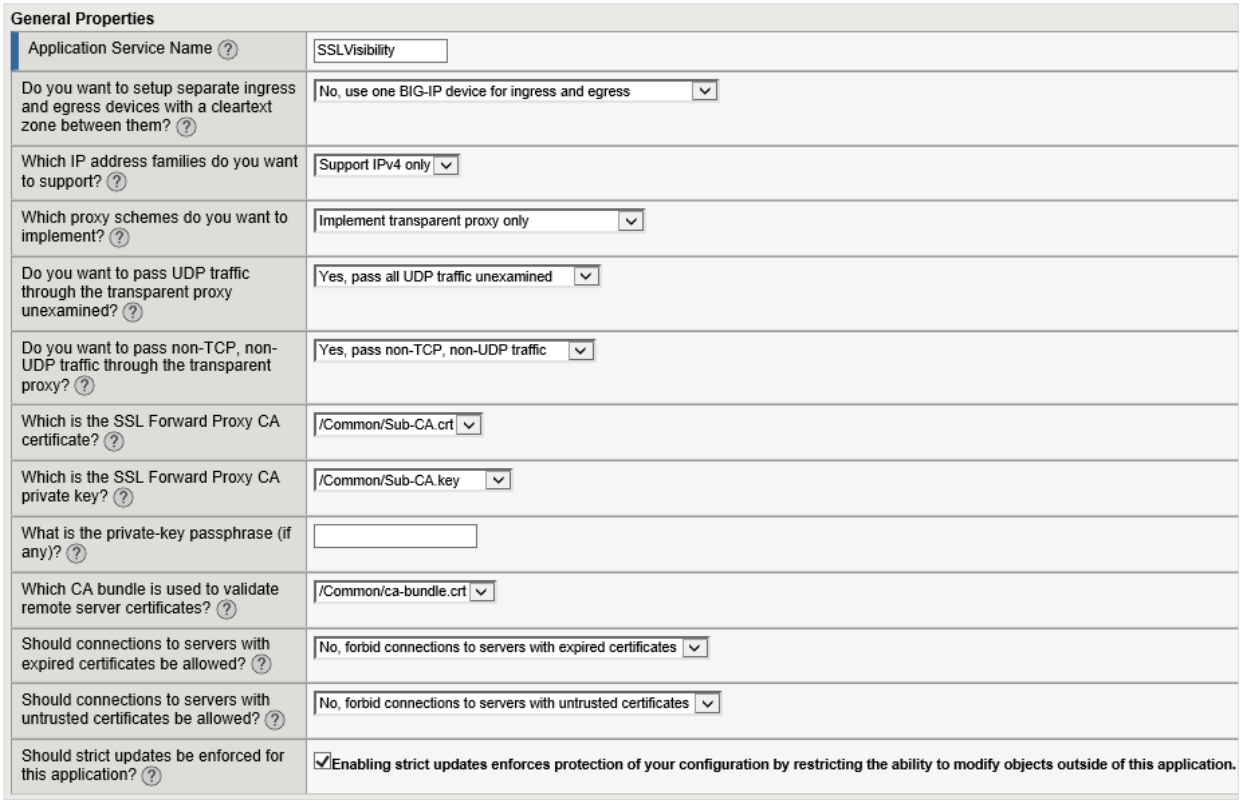


Figure 14: A sample General Properties configuration

3. Continue configuration by scrolling down to **Ingress Device Configuration** (see below.)

Ingress device configuration

The ingress device is one or more ingress VLANs where clients send traffic. The F5 device decrypts the encrypted traffic on ingress and then, based on protocol, source, and destination, classifies the traffic and passes each connection for inspection.

1. Answer each ingress device configuration question. See tips and guidance below.

Question	User Input
Which VLAN(s) will bring client traffic to the transparent proxy?	Select one or more VLANs where transparent-proxy ingress traffic will arrive.
How should a server TLS handshake failure be handled?	Most TLS handshake failures occur during protocol and cipher agreement. You can specify whether to drop or bypass the connection. Typically, select **If server TLS handshake fails the connector fails.**
DNS query resolution	The DNS configuration options are relevant when SSL Orchestrator is implemented in explicit proxy mode or when doing dynamic domain bypass (DDB) in a TCP service chain classifier rule. Specify whether to permit the system to send DNS queries directly to the Internet, or specify one or more local forwarding nameservers to process all DNS queries from SSL Orchestrator. If you choose the former, you can specify to configure local/private DNS zones.

	In this example, select **Send DNS queries to forwarding nameservers on the local network.**
Which local forwarding nameserver(s) will resolve DNS queries from this solution?	Type the IP address of the local nameserver(s) which will resolve the DNS queries.
Do you want to use DNSSEC to validate DNS information?	DNSSEC is a suite of extensions that add security to the DNS protocol by enabling DNS responses to be validated. Select **Yes, use DNSSEC to validate DNS information.**

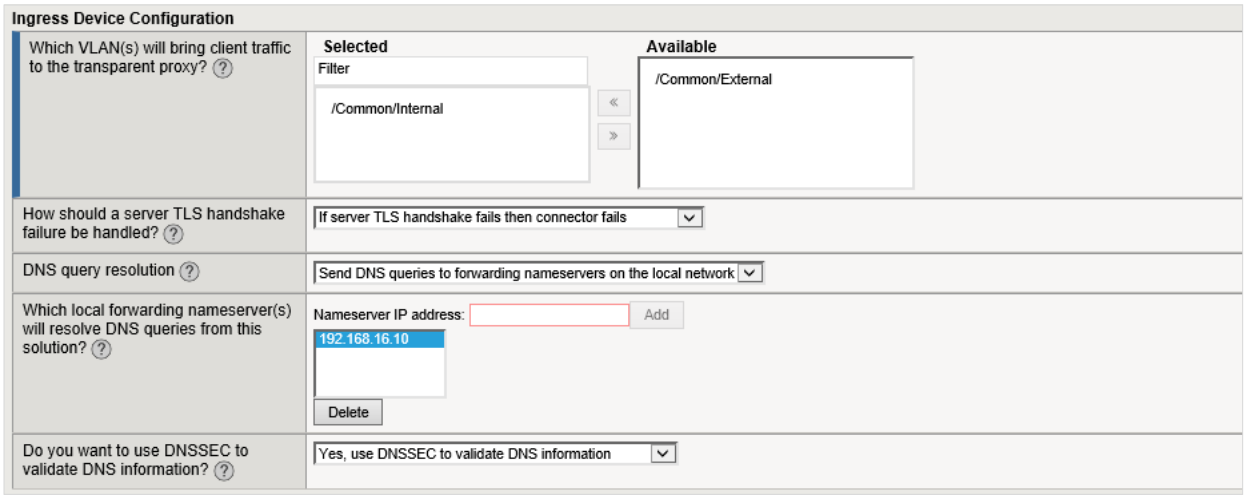


Figure 15: Sample ingress device configuration

2. Continue configuration by scrolling down to **Egress Device Configuration** (see below.)

Egress device configuration

The egress device is one or more egress VLANs where the clients receive traffic. The F5 device decrypts the encrypted response on egress and then, based on protocol, source, and destination, classifies the traffic and passes each connection for inspection before sending it to the requested internal client.

1. Answer each egress device configuration question. Note that in the example below, the same Herculon or BIG-IP device is configured to receive both the ingress and egress traffic.

Question	User Input
Do you want to SNAT client IP addresses?	It is common to translate the client source IP address with the address belonging to the egress for outbound traffic. Choose **No** to preserve the client source IP address. Otherwise, select **Yes, SNAT (replace) client addresses**
Do you want to use a SNAT Pool?	F5 recommends use of a SNAT pool to scale translations instead of overloading the egress interface IP address (AutoMap). Select **Yes, define SNAT Pool addresses for good performance.**

IPv4 SNAT addresses	Enter the IPv4 addresses for the SNAT pool
Should traffic go to the Internet via specific gateways?	Specify whether to route outbound using the default route on the BIG-IP or Herculon system or enter the IP address to be used as the default gateway. In the example above, we selected **No, send outbound / Internet traffic via the default route**.

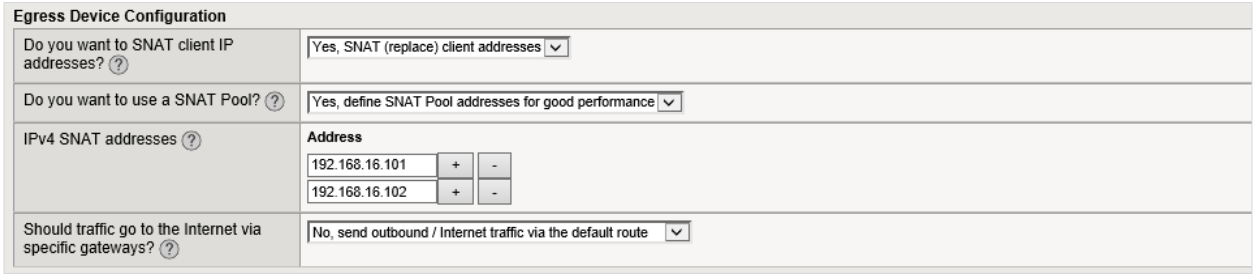


Figure 16: Example egress device configuration

2. Continue configuration by scrolling down to **Logging Configuration** (see below.)

Logging configuration

1. Answer the logging configuration questions using the guidance below.

Question	User Input
What SSL Intercept logging level do you want to enable?	F5 recommends leaving the logging level at the default, **Errors. Log on functional errors**, unless you need to troubleshoot.
Which Log Publisher will process the log messages?	Specify whether to process the logs with an existing log publisher or that logs should be sent to syslog-ng.
What kind of statistics do you want to record?	Specify the kind of statistics you want the system to record. SSL Orchestrator can collect usage data for connections, service chains, services, and more. For optimal performance, keep the settings at the default, **Usage counters only**.

Figure 17: Default logging settings

2. When you're done, click **Save** at the top of the page.

Create the Symantec DLP ICAP service

Before creating ICAP services, you must complete all the configuration sections under **General Properties**. 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 device management interface, navigate to **SSL Orchestrator** > **Configuration** > **ICAP Services**. The ICAP Services screen displays.

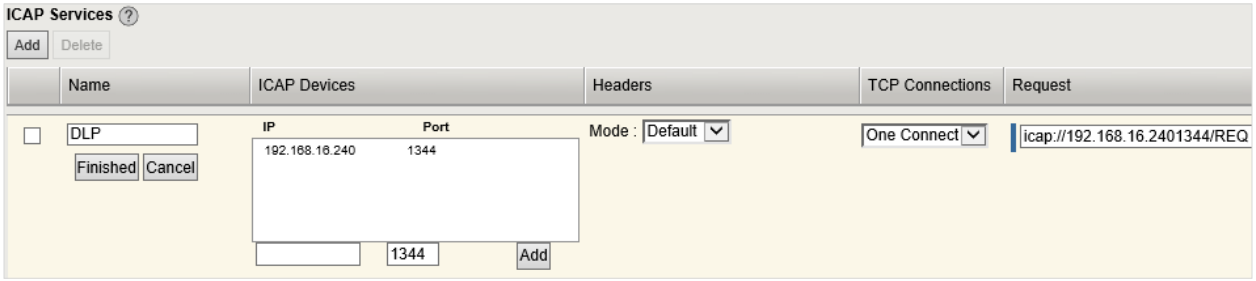


Figure 18A: The left side of the ICAP service configuration screen. (See also Figure 18B.)

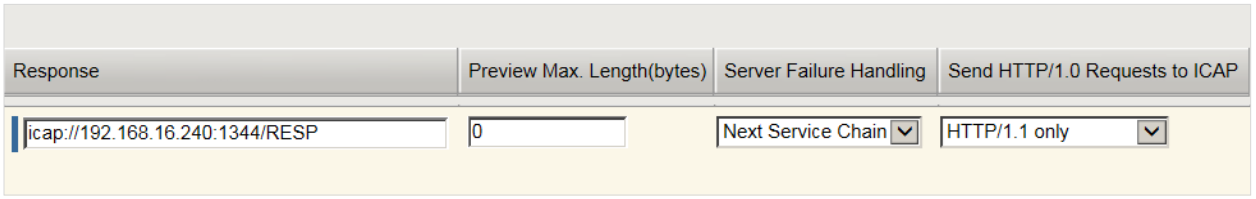


Figure 18B: The right side of the ICAP service configuration screen.

2. Click **Add** to enter information in the configurable fields and create the ICAP service, using the guidance below.

Configuration Field	User Input
Name	Enter a name for the ICAP service.
ICAP Devices	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**.
Headers	Select **Default** to send the default request-specific headers allowed in ICAP requests. Otherwise, select **Custom** to edit the following header values: **Host:** The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource. **Referer:** The Referer request-header allows SSL Orchestrator, which is the ICAP client, to specify (for the ICAP server's benefit) the address (URI) of the resource from which the Request-URI was obtained. **User Agent:** The client that initiates a request. These are often browsers, editors

	or other user tools. **From:** The From request-header field contains the email address of the user who controls the requesting user agent.
TCP Connections	Select **One Connect** to reuse the TCP connections to ICAP servers, which processes multiple transactions.
Request	Enter the ICAP request URI as defined by RFC3507. Usually that means entering ***icap://<SymantecMonitorServerIP>:1344/REQ***
Response	Enter the ICAP response URI as defined by RFC3507. Usually that means entering ***icap://<SymantecMonitorServerIP>:1344/RESP***
Preview Max. Length (bytes)	This is 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.
Server Failure Handling	Select **Next Service Chain** 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.
Send HTTP/1.0 Requests to ICAP	Select **Yes** to send both HTTP/1.1 and HTTP/1.0 requests to the ICAP service. Select **No** to send only HTTP/1.1 requests to the ICAP service. Any HTTP/1.0 requests will not be inspected.

3. Click **Finished**, then click **Save** at the top of the page.

Creating service chains to link services

Before you can set up service chains, you must configure all the services (inline, ICAP, or receive-only). By default, SSL Orchestrator steers traffic through all the security services. You can create a new service chain by defining the service list in the preferred order of services to which traffic should be steered.

Each service chain is linked to service chain classifier rules and processes specific connections based on those classifier 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 any decryption zones between separate ingress and egress devices.

1. To create a service chain, from the main tab, navigate to **SSL Orchestrator** > **Configuration** > **Policies**. The Policies screen displays.

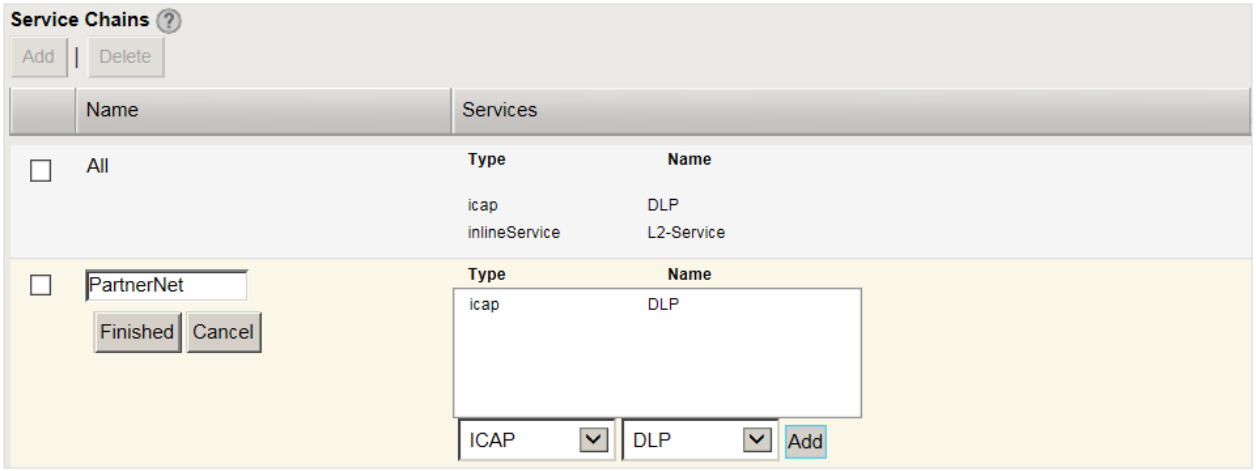


Figure 19: Sample service chain configuration

2. Under **Service Chains**, click **Add**.
3. Enter a **Name** for the service chain.
4. In the order you want SSL Orchestrator to use to steer the traffic, select the service **Type** (ICAP, inline or Receive-only) and service **Name** and click **Add**. Repeat until all services in the chain have been selected in the order you prefer.
5. When you're done with one service chain, click **Finished**.
6. Repeat Steps 2 through 5 to create multiple service chains.

Creating TCP service chain classifier rules

Before you create a TCP service chain classifier rule, you must create one or more service chains. Service chain classifier rules then determine which service chains receive traffic. Each service chain classifier rule selects the specific chain to process ingress connections. Different classifier rules may send connections to the same chain. Each classifier has three filters that match the source IP address, the destination mode, and the application protocol. Filters can also overlap so that the classifier that matches best determines the service chain for a specific connection.

To avoid issues with privacy concerns and adhere to regulatory compliance, some organizations might need to enforce policies to bypass SSL destined to websites that expose personal user information, such as is the case for banking, financial, or government sites. Classifier rules enable such policy implementation based on various context filters derived from a powerful classification engine. Finally, classifier rules can also be used to reject a connection if needed.

1. Once you've created a service chain, continue to scroll down the Policies page to **TCP Service Chain Classifiers**.
2. Click **Add** and create a classifier rule, making selections and completing each field using the guidance below. In the following example, we create a sample TCP service chain classifier rule (as shown in Figure 20) to bypass SSL traffic originating from any internal client on 10.10.10.0 subnet in the corporate network and destined to any health care websites.

Configuration Field	User Input
Name	Enter a name for the TCP service classifier rule.
Phase	Select the SSL/TLS phase you want: **No TLS:** Match only non-TLS/SSL traffic. **Pre-Handshake**: Match TLS connections before any TLS handshake, which means you can allow a connection to bypass SSL inspection completely, without even trying to learn the real name of the remote server. Pre-handshake rules must reject or bypass any connections they match. **TLS Handshake:** Match only at the time of the TLS handshake and never match non-TLS traffic. The traffic is not checked again after the plaintext of a TLS connection becomes available. **Normal**: Match TLS connections at TLS handshake time and possibly again, more specifically, after SSL Orchestrator exposes the plaintext of the TLS connection (so you can manage HTTPS on non-standard ports, for example). Normal rules may also match non-TLS traffic (so, for example, a single rule can handle both HTTPS and HTTP traffic.) For the sample SSL bypass configuration, select **Normal**.
Protocol	Select the protocol to match: **HTTP**, **MAIL**, **ALL,** or **Other.** For the sample, select **ALL** to bypass all encrypted traffic.
Source	Select the source **Type,** either **IP address** or **Data Group,** and then specify the filter **Value**. **IP address** is either a traffic originating IP address or subnet. An explicit 0.0.0.0 will match all the traffic when IP address or subnet is not defined. **Data Group** is simply a user-defined group of related elements, such as a set of IP addresses. Refer to the AskF5.com resource on Data groups to learn more about data groups. For the example, select the source **Type** as **IP address** to match the connection originator and enter 10.10.10.0 in the **value** field, then click **Add**.
Destination	Select the destination **Mode** and specify the filter **Type** and **Value**, which may include: **Address**: Specify the traffic destination based on **IP address** or **Data Group** (as with the source filter). **Geolocation**: Specify two-letter country and three-letter continent codes to match the destination IP against the local geolocation database. **IPI**: Specify the F5 IP Intelligence category or data group against which the destination IP address's reputation is validated. An IP Intelligence subscription is needed for the rule to evaluate against this database of known IP addresses with questionable reputations. **Port**: Specify the port or ports against which the destination port number should be matched. The value can be “any,” one or more TCP port numbers, or ranges like 5557-5559 (use 0 or * to match all). The chief use of this mode is to control non-TLS traffic such as SNMP. **URLF**: Specify URL filtering (URLF) categories or a data group against which the destination URL will be matched. A URLF subscription is needed for the rule to

	evaluate against the URLF database. **Name**: Specify the domain name (with a unique name or using a wildcard) or data group against which the connection's hostname should be matched. **DDB**: Specify the DNS domain name (with a unique name or using a wildcard) against which the destination hostname indicated by the client in TLS Server Name Indication (SNI) is matched. (Refer to RFC 6066 to understand the SNI extension for TLS.) You may use DDB (dynamic domain bypass) to whitelist and bypass traffic to servers that cause TLS handshake problems or that require TLS mutual (client-certificate/smart-card) authentication. A URLF rule in the pre-handshake phase will match URL filtering categories associated with the TLS SNI hostname and otherwise behave like a DDB rule. See the example in Figure 20 below. For the example, select URLF as the destination **Mode**, **Type** for the **category,** and **Health and Medicine** as the **Value** to match if the connection is destined to any websites in the Health and Medicine category of the URLF database. Then click **Add**.
Service Chain	Select the name of a **Service Chain** (defined in the previous procedure) or an action—either **Bypass** or **Reject**. For the example, select **Bypass** in the **Service Chain** selector to enforce the bypass action when both source and destination context filters match for an outbound connection.

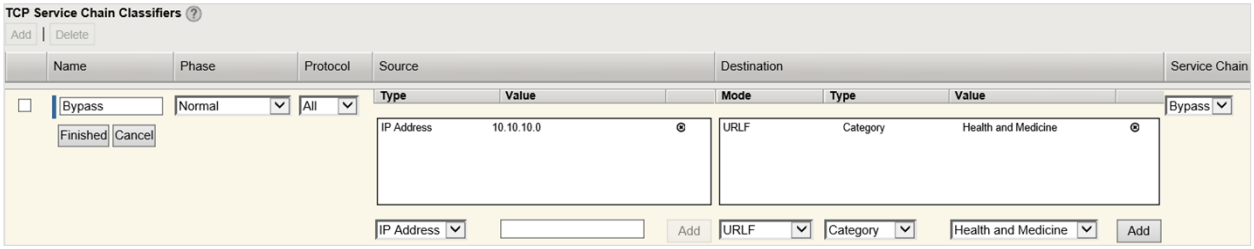


Figure 20: Sample TCP service chain classifier

3. When your classifier rule configuration is complete, click **Finished**.
4. Repeat Steps 2 and 3 to create multiple TCP service chain classifiers.
5. If your answer to "Do you want to pass UDP traffic through the transparent proxy unexamined?" in the General Properties configuration was "**No, manage UDP traffic by classification**," you will be presented with a **UDP Service Chain Classifiers screen** to create UDP rules similar to the TCP rules. Create and configure them following the same basic principles.
6. Finally, click **Deploy** at the top of the page to deploy the configured SSL Orchestrator.

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 BIG-IP or Herculon 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 device's 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
```

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 by pressing **Send**, 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.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan f5j-info@f5.com

Solutions for an application world.