RSA® NETWITNESS®
Packets
Implementation Guide

F5 SSL Orchestrator

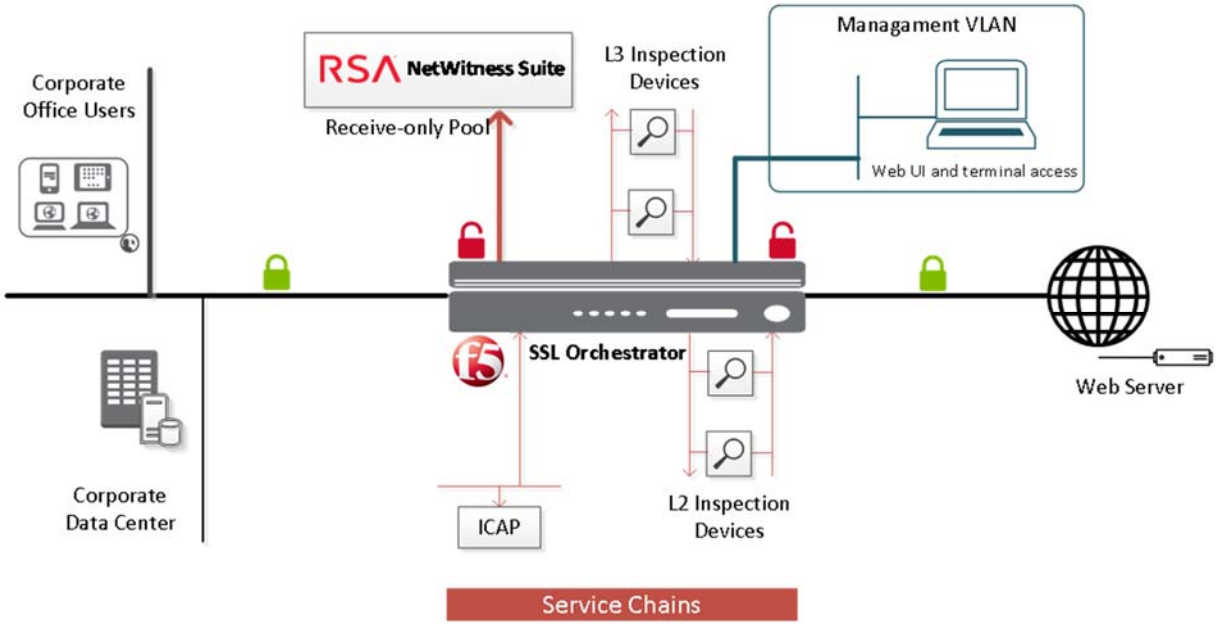
Daniel R. Pintal, RSA Partner Engineering
Last Modified: June 7, 2017

RSA READY

Solution Summary

F5® SSL Orchestrator™ security solution centralizes SSL inspection across complex security architectures for decrypting and re-encrypting outbound SSL traffic. The decrypted SSL traffic along with unencrypted traffic is passively copied to RSA Netwitness Suite for inspected to uncover hidden threats and block zero-day exploits. This solution eliminates the blind spots introduced by SSL and closes any opportunity for adversaries.

The integration between the F5 and RSA Netwitness Suite provides Network Security Engineers and Analysts with the ability to collect, investigate and research unencrypted and encrypted network traffic at the packet level. When used in combination with RSA ESA a variety of notifications can be enabled to alert network security engineers of threats to the infrastructure.



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the F5 SSL Orchestrator with RSA Netwitness. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All F5 BIG-IP components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure F5 BIG-IP is properly configured and secured before deploying to a production environment. For more information, please refer to the F5 BIG-IP documentation or website.

F5 BIG-IP Configuration

Pre-Requisites

Careful advance consideration of deployment can ensure an efficient and effective implementation of the F5 integrated solution with RSA Netwitness Suite. This section helps you with information on License components, best practices and initial steps. Once these steps are complete, you can proceed to the configuration of the SSL Orchestrator.

License components

The recently launched F5 Herculon purpose-built security product line—i2800, i5800, i10800—and the existing F5 BIG-IP family of products support the integration. By default, Herculon SSL Orchestrator ships with an installed base module that provides both SSL interception and service chaining capabilities. To deploy the SSL Orchestrator application on a BIG-IP system, the system must be running TMOS 13.0 or higher, and BIG-IP® Local Traffic Manager™ (LTM) must be provisioned 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:

- A URL Filtering (URLF) subscription to use the URL category database for filtering.
- An F5 IP Intelligence subscription to detect and block known attackers and malicious traffic.
- A network hardware security module (HSM) to safeguard and manage digital keys for strong authentication.

Architecture best practices

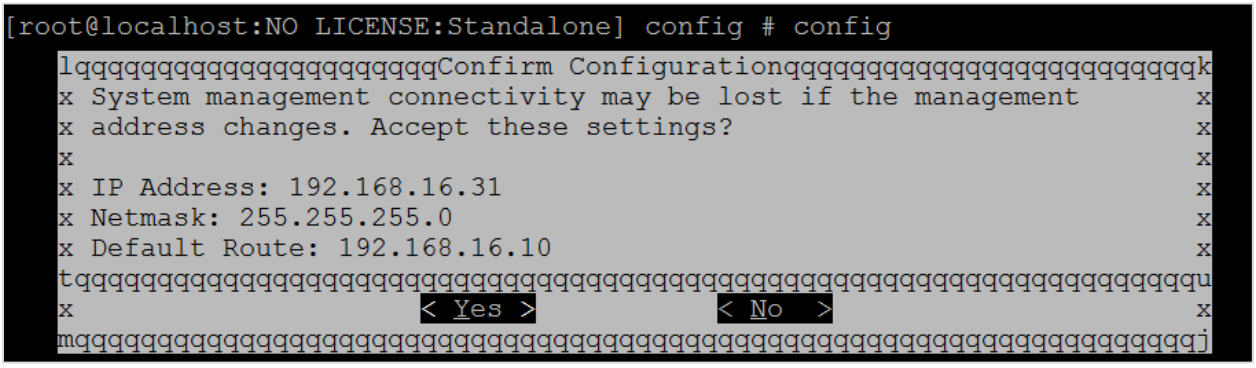
A number of best practices can help ensure a streamlined architecture that optimizes performance and reliability as well as security. F5 recommendations include:

- Deploy 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).
- Further interface redundancy can be achieved 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 with some competing solutions, the F5 systems do not need physical connections to the RSA Netwitness Suite. All the F5 system requires is L3 reachability to send the copied decrypted and unencrypted traffic. In slow networks, however, we recommend deploying the RSA Netwitness Suite not more than one hop away. As a generic guideline, when inspection devices are not directly connected to the F5 system, we highly recommend use of network and VLAN controls to restrict access to the unencrypted data only to the inspection devices.

Run the SSL Orchestrator Setup Wizard

After you plug in the power supply to 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.

Important: The Setup Wizard for Herculon is substantially the same as for the BIG-IP system, with the exception of a few configuration items, such as SSL certificate configuration, that can readily be performed manually on the BIG-IP system.

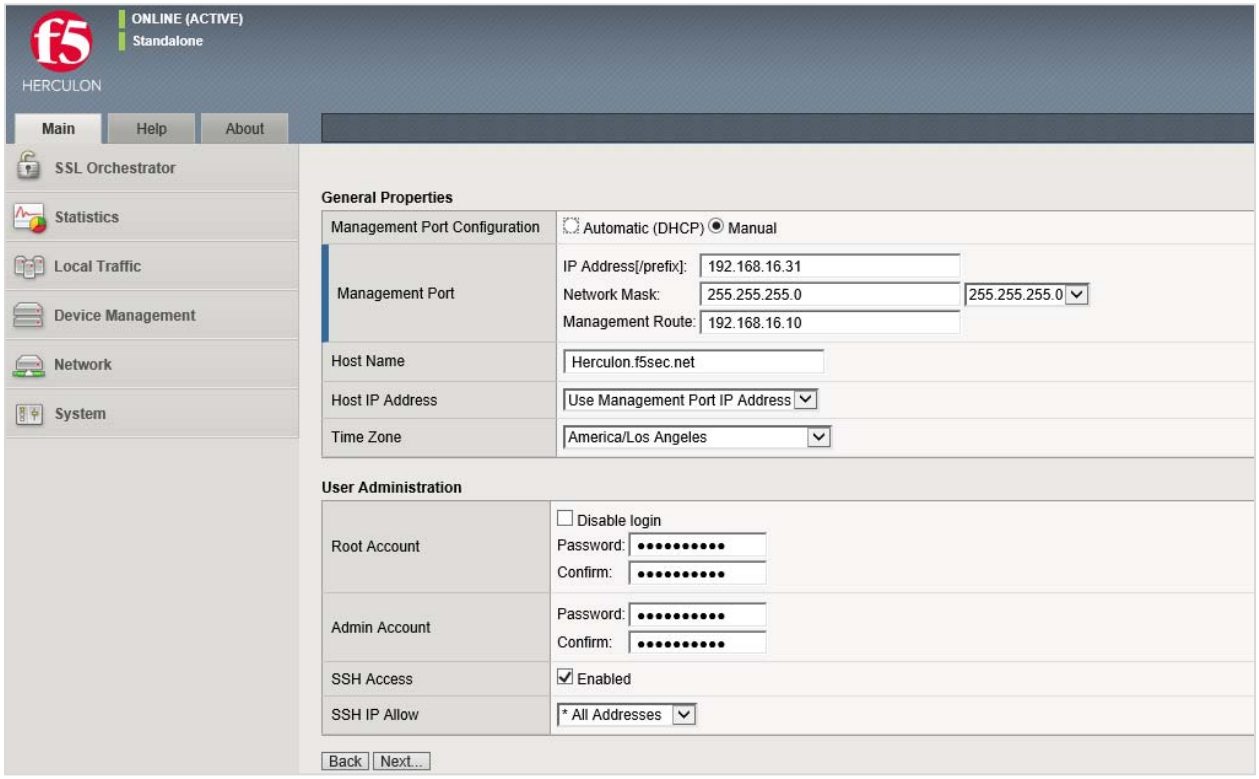


Log in to the web UI using the configured management IP address (default web interface credentials are **admin/admin**). The SSL Orchestrator Setup Wizard guides you through the basic, minimal setup configuration for F5 SSL Orchestrator.

Important: 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.

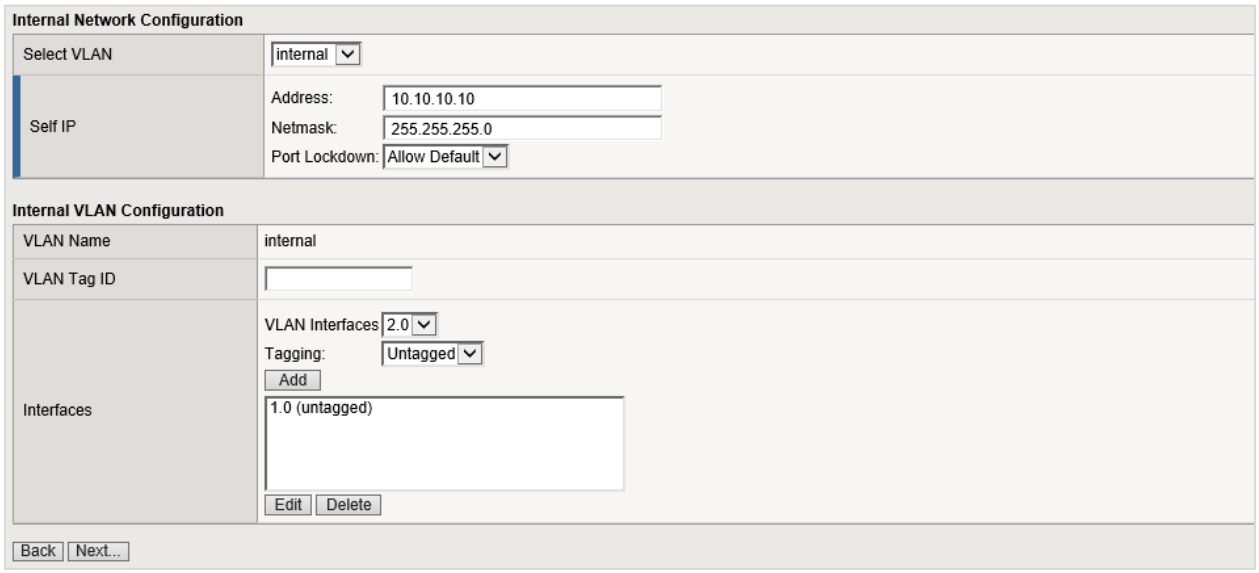
1. On the F5 **Welcome** screen, click **Next**.
2. On the **License** screen, click **Activate**.
3. On the **EULA** screen, click **Accept**. The license activates and the system reboots.
4. Once the system has rebooted, click **Continue**.
5. On the **Device Certificates** screen, click **Next**.

6. Once the **Platform** screen appears, complete the following steps:
   - Enter the **Host Name** for this system. The **Host Name** must be a fully qualified domain name.
   - 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.



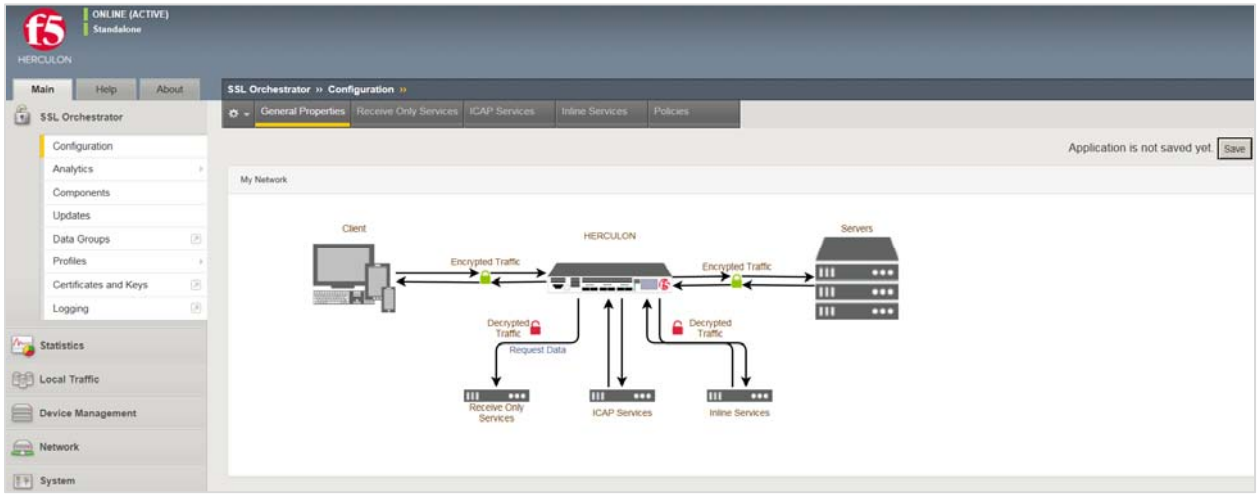
7. The system notifies you to log out and then log back in with your username (*admin*) and new password.
8. Click **OK**. The system reboots.
9. Once the **Network Time Protocol** (NTP) configuration screen opens, enter the IP **Address** of the NTP server to synchronize the system clock with, and click **Add**. Click **Next**.
10. (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:
    - 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**.
    - If you use BIND servers, add them in the **BIND Forwarder Server** list.
    - Add local domain lookups (to resolve local host names) in the **DNS Search Domain** list.
    - Click **Next**. The **Internal VLAN** screen opens.

11. On the **Internal VLAN** screen, specify the **Self IP** settings for the internal network:
    - Enter a self IP **Address**.
    - Enter a network mask (**Netmask**) for the self IP address.
    - Retain the default values for the **Port Lockdown** and **VLAN Tag ID** settings.
    - 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**.
    - Click **Next**. This completes the configuration of the internal VLAN.



12. The **External VLAN** screen opens. Specify the **Self IP** settings for the external network:
    - Enter a self IP **Address**.
    - Enter a network mask (**Netmask**) for the self IP address.
    - Retain the default value for the **Port Lockdown** setting.
    - Enter the IP address you want to use as the **Default Gateway** to the external VLAN.
    - 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.
13. On the **Forward Proxy Certificate** screen, complete the following configuration to import the CA certificate:
    - For the **Certificate Name**, select **Create New** and enter a name.
    - 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.
    - 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.
    - 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**.
14. 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.

15. Click **Finish**. The SSL Orchestrator configuration page appears with a complete menu displayed on the left side of the page.

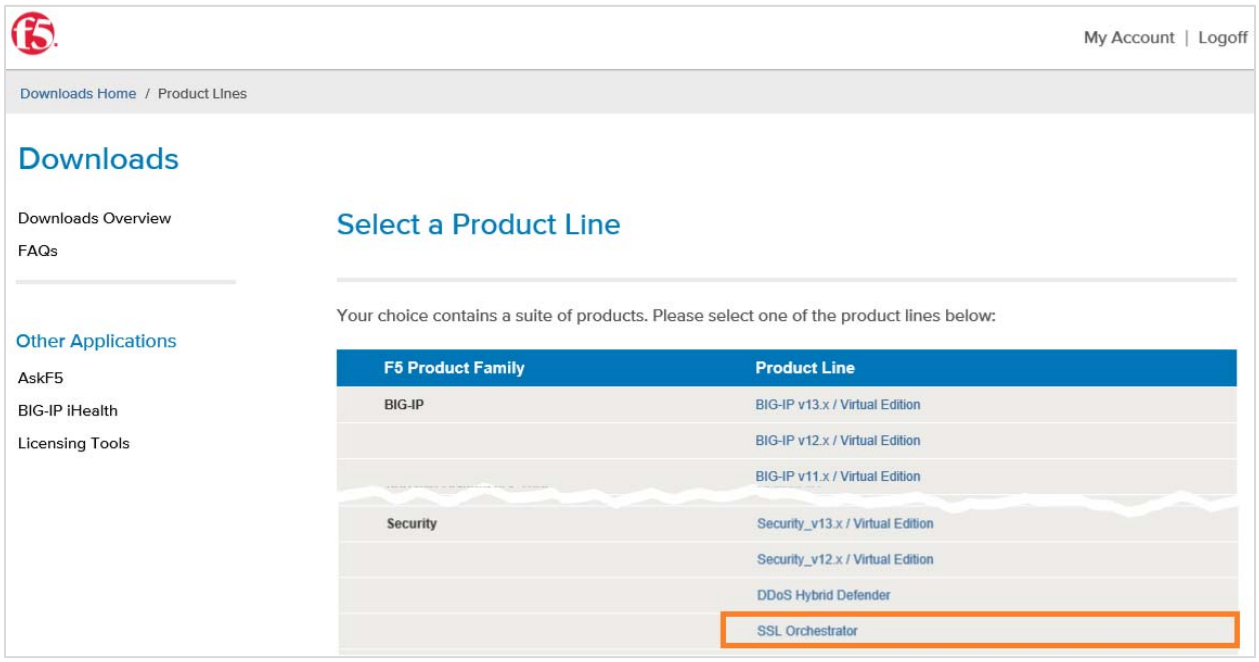


You are now ready to proceed to the second part of configuration, where you finalize your system for SSL Orchestrator.

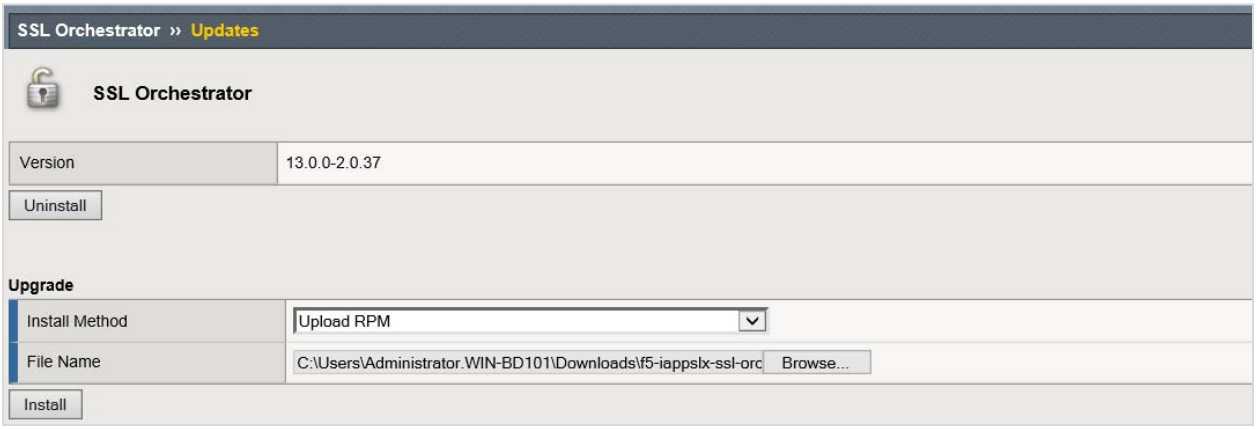
Update the SSL Orchestrator version

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**.



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 BIG-IP management interface and navigate to **SSL Orchestrator > Updates**.
8. Under **File Name**, click **Browse** and navigate to the .rpm file you saved on your system. Click **Open** to select it.



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

Back up your F5 system configuration

Before beginning the detailed SSL Orchestrator configuration, we strongly recommend you back up the F5 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**.

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 BIG-IP system configuration, see *Solution K13132* on AskF5: Backing up and restoring BIG-IP configuration files.

SSL Orchestrator Configuration

This section covers step by step configuration of the F5 SSL Orchestrator to provide a packet-by-packet copy of both the unencrypted HTTP and decrypted HTTPS traffic to RSA Netwitness suite configured for TAP mode. At any point during the configuration if you need additional help, refer the F5 Herculon SSL Orchestrator Setup guide.

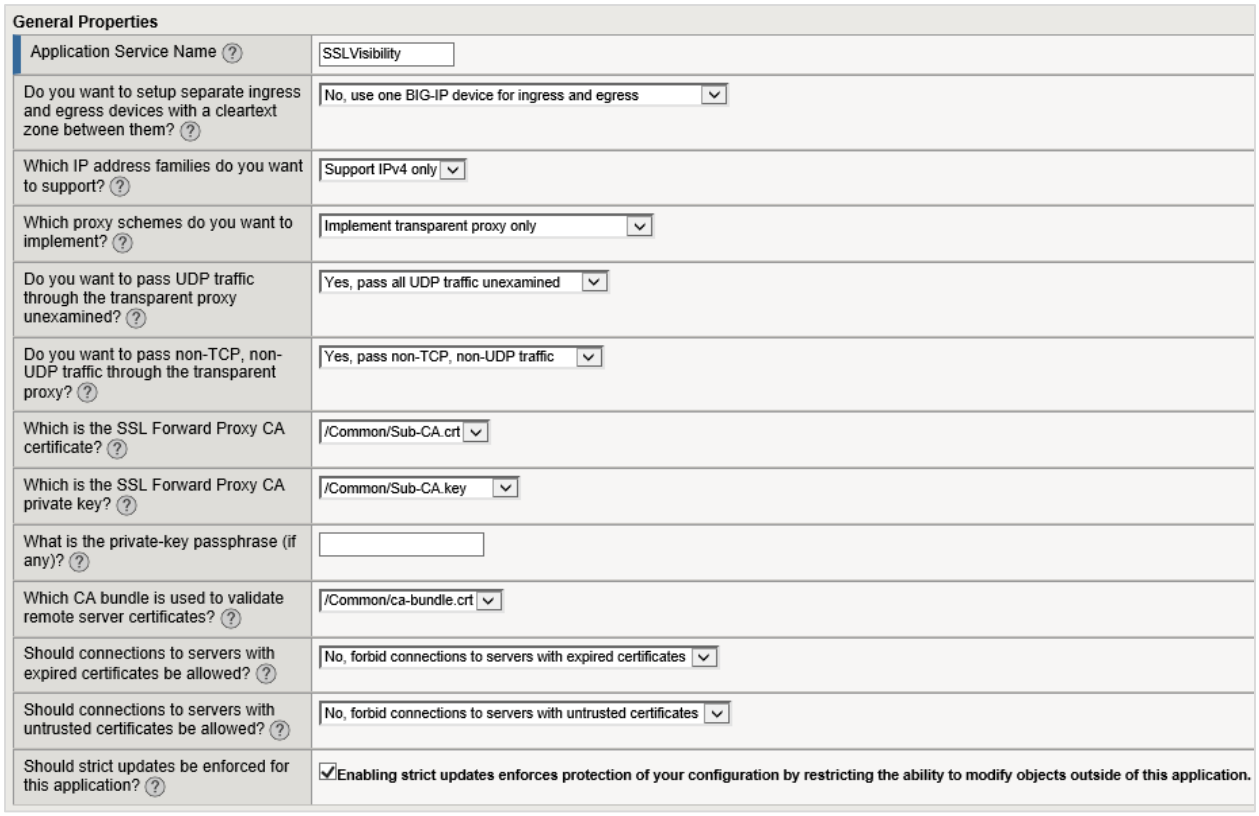
General properties

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 for SSL Orchestrator. (Also see the table 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 clear text 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.



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

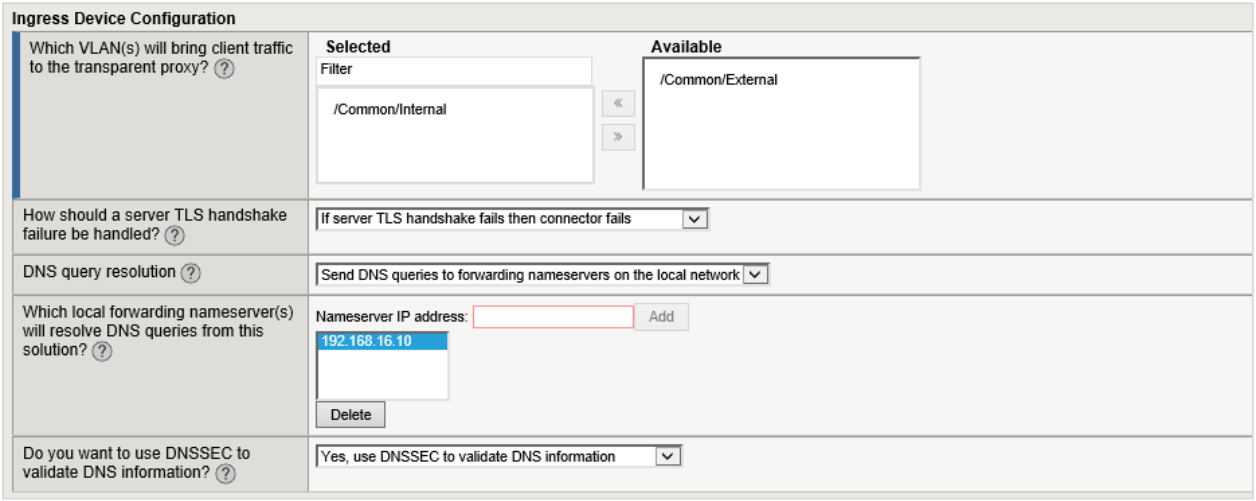
Ingress device configuration

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.

4. Answer each 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	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.**



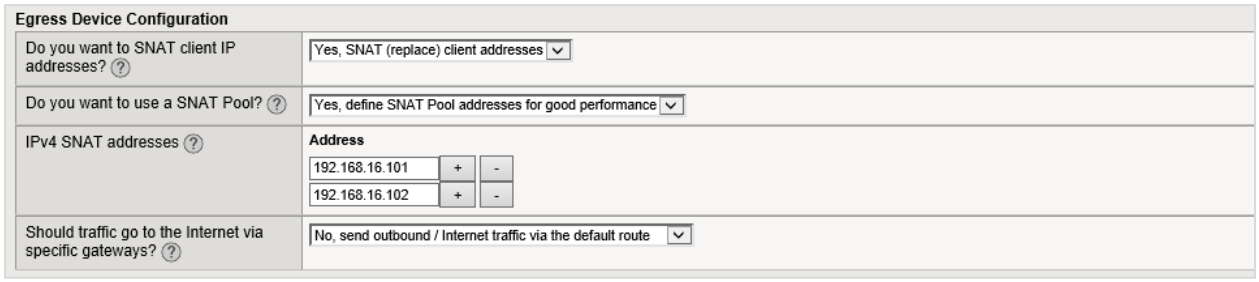
5. Continue configuration by scrolling down to **Egress Device Configuration** (see below.)

Egress device configuration

The egress device is one or more egress VLANs where the clients receive traffic. The F5 system 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.

6. Answer each configuration question. Note that in this example, 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 F5 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**.



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

Logging configuration

8. Answer the configuration questions using the guidance below.

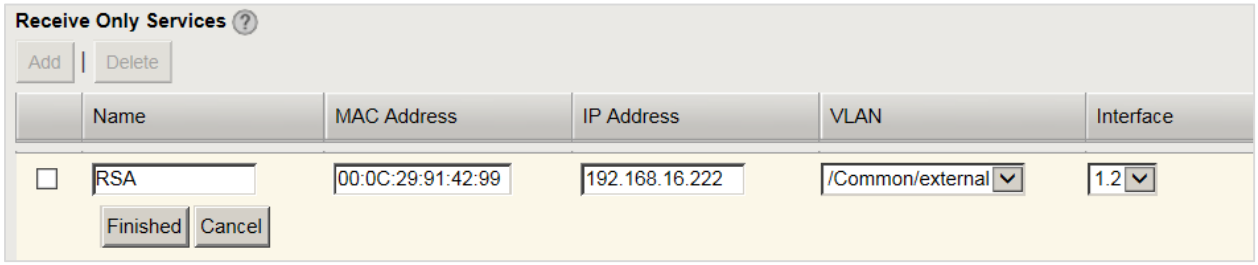
Question	User Input
What SSL Intercept logging level do you want to enable?	F5 recommends leaving the logging level at the default, Errors. Log on functional errors, unless you need to troubleshoot.
Which Log Publisher will process the log messages?	Specify whether to process the logs with an existing 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.

Create a receive-only service

You can configure up to 10 receive-only services using the SSL Orchestrator configuration utility.

1. On the main tab, click **SSL Orchestrator > Configuration > Receive Only Services**.
2. Enter information for the configurable fields, following the guidance below.

Configuration Field	User Input
Name	Enter a **Name** for the receive-only service.
MAC Address	Enter the receiving interface's **MAC Address**. The MAC address can be obtained from the web UI.
IP Address	Enter the nominal **IP Address** for this device. Each receive-only device requires a nominal IP host address to identify the device in the F5 system. This nominal IP address must be homed on the same subnet as one (any one) of the BIG-IP self-IP addresses. It does not have to be on the same VLAN as the receive-only device. No IP packets will ever be sent to the nominal IP address (but it must be unique on the network while it is assigned in this solution).
VLAN	From the VLAN list, select the **VLAN** where the receive-only device resides.
interface	Select the associated BIG-IP system **Interface**.



3. When done, click **Save** at the top of the page.
4. Finally, click **Deploy** at the top of the page to deploy the configured SSL Orchestrator.

SSL Orchestration has the capabilities to service chain and steer decrypted and unencrypted traffic to multiple inspection devices (DLP, NGFW, IPS etc.) in the security stalk. Refer the Appendix section to understand on how to create service chain and enforce policies.

Testing the Solution

You can test the deployed solution using the following options:

- Server certificate test

  Open a browser on the client system and navigate to an HTTPS site, for example, **https://www.facebook.com**. Once the site opens in the browser, check the server certificate of the site and verify that it 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 correctly.

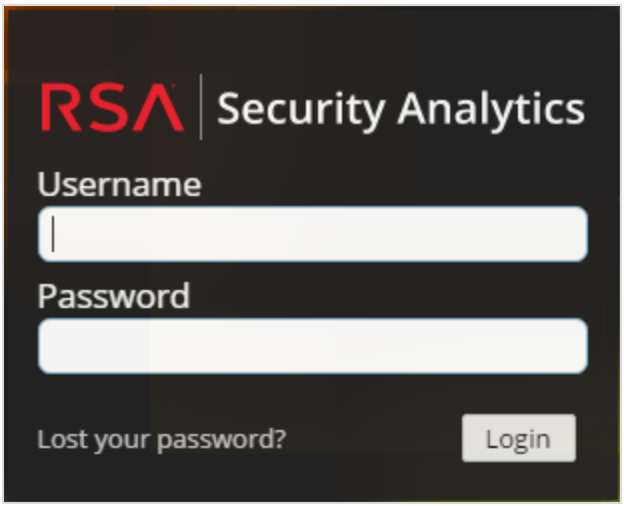
- Decrypted traffic analysis on the F5 system

  Perform a TCP dump on the F5 system to observe the decrypted clear text traffic. This confirms SSL interception by the F5 device.

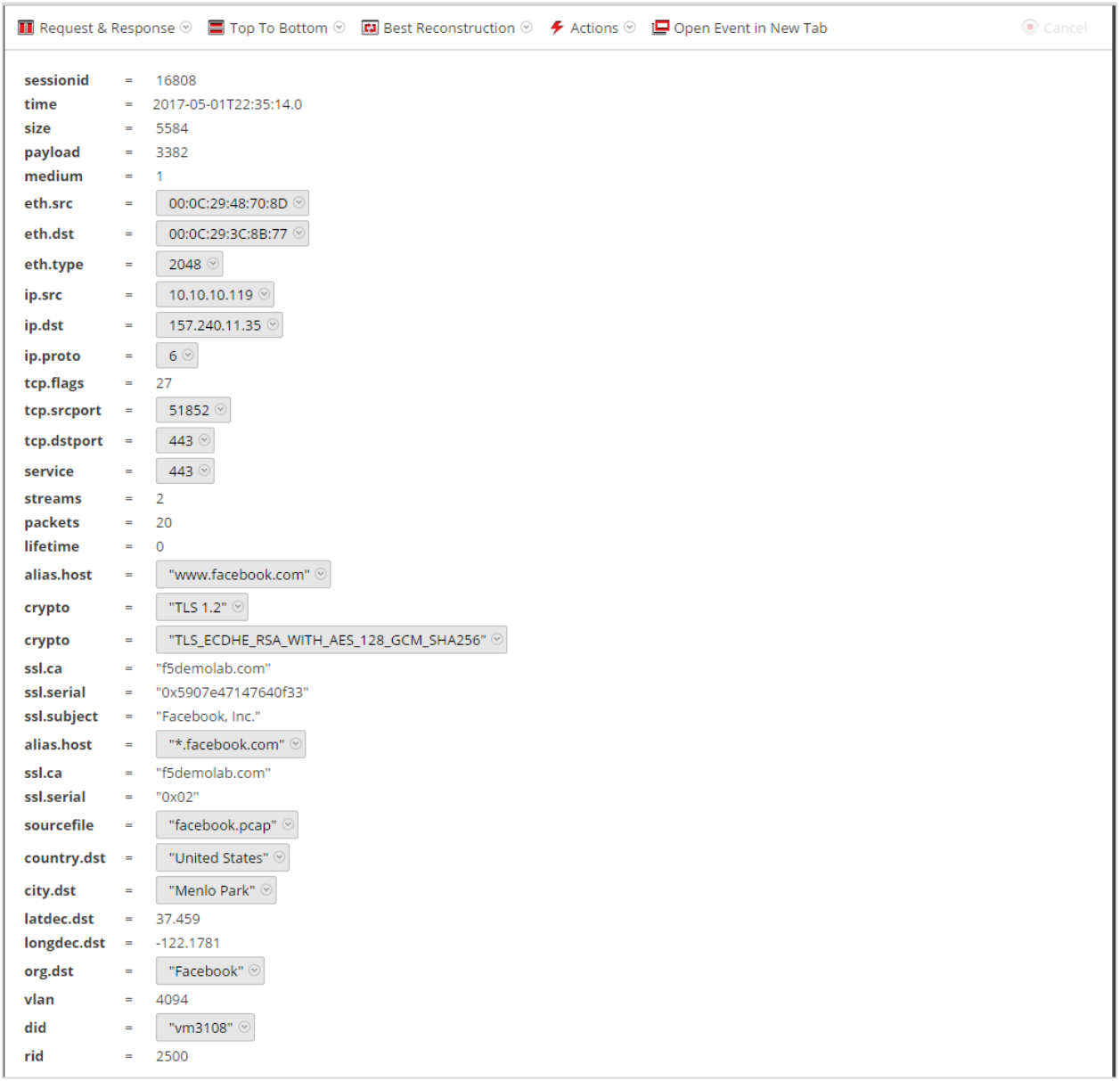
  ```
  tcpdump –l nni  et h<n> -Xs0
  ```

RSA Netwitness Packet Receipt Verification

1. To verify receipt of the F5 BIG-IP Orchestrator decrypted SSL packets, log on as the Administrator to RSA Netwitness.



2. Using Netwitness Investigator drill down into the content collected from the F5 Orchestrator to locate the packets captured by RSA Netwitness.



Certification Checklist for RSA NetWitness

Date Tested: May 30, 2017

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	10.6.3	Virtual Appliance
F5 SSL Orchestrator	2.2	Virtual Appliance

Security Analytics Test Case	Result
Outbound SSL Decryption	
HTTPS	
Google Search	✓
Bing Search	✓
Facebook	✓
YouTube	✓
Twitter	✓
LinkedIn	✓
Reddit	✓
WEBMAIL	
GMail	✓
Yahoo	✓
Live	✓
AOL	✓
Inbound SSL Decryption	
HTTPS	
Web Server	N/A

✓ = Pass ✗ = Fail N/A = Non-Available Function

RSA READY

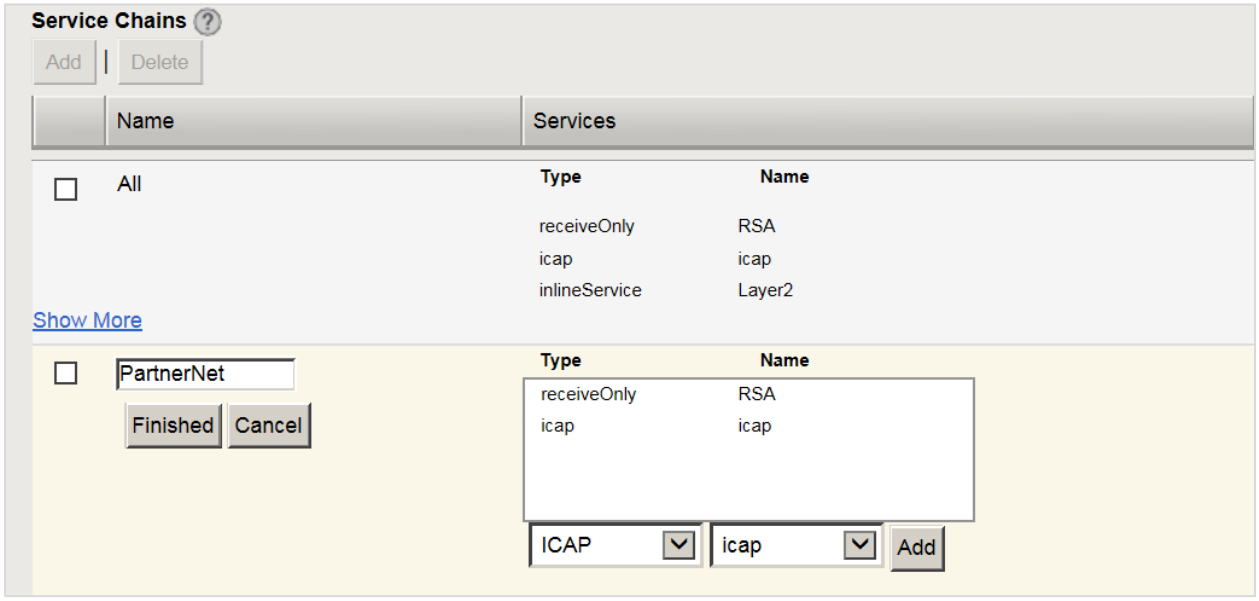
Appendix

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. Additionally, service chains can include inline, ICAP, or receive-only services, as well as any decryption zones between separate ingress and egress devices.

3. On the main tab, click **SSL Orchestrator > Configuration > Policies**. The policies screen displays.
4. Under **Service Chains**, click **Add**.
5. Enter a **Name** for the service chain.
6. 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**.
7. Repeat Step 4 until all services in the chain have been selected in the order you prefer.
8. When you're done with the service chain, click **Finished**.
9. Repeat Steps 2 through 6 to create multiple service chains.



Creating TCP service chain classifier rules

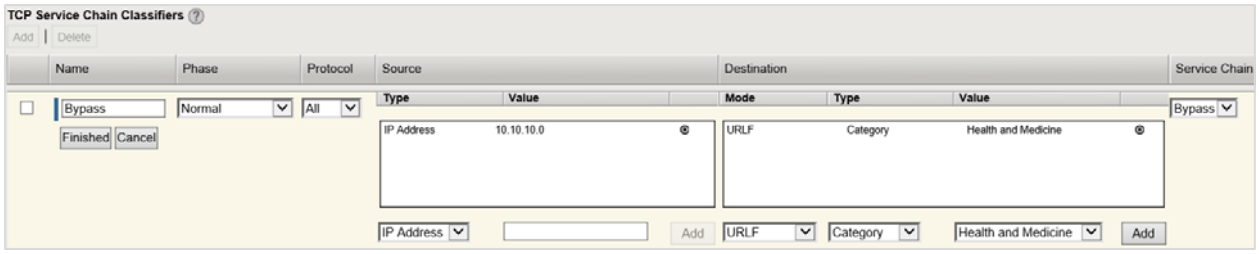
Before you create a TCP service chain classifier rule, you must **create one or more service chains**. Service chain classifier rules then determine which service chains receive traffic. Each service chain classifier rule selects the specific chain to process ingress connections. Different classifier 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.

10. Once you've created a service chain, continue to scroll down the **Policies** page to **TCP Service Chain Classifiers**.
11. Click **Add** and create a classifier rule, making selections and completing each field using the guidance below.
12. The example below creates a sample TCP service chain classifier rule 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.) Select **Normal** in this sample SSL bypass configuration.
Protocol	Select the protocol to match: **HTTP**, **MAIL**, **ALL**, or **Other**. 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. Select **IP Address** as the source **Type** 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. Select **URLF** as the **Destination Mode**, **Category** as the **Type**, 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**. Select **Bypass** in the **Service Chain** selector to enforce a bypass action when both source and destination context filters match for an outbound connection.



13. When your classifier rule configuration is complete, click **Finished**.
14. Repeat Steps 2 and 3 to create multiple TCP service chain classifiers.
15. 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.

Finally, click **Deploy** at the top of the page to deploy the configured SSL Orchestrator.