



Deploying the BIG-IP System for SSL Intercept v1.5

Welcome to the F5® deployment guide for configuring the BIG-IP® system for SSL Intercept. This document contains guidance on configuring the BIG-IP system to act as a forward proxy, decrypting outbound encrypted traffic so it can be inspected by service chains you configure, and then re-encrypting it for delivery to the destination. Non-encrypted traffic may also be classified and sent through service chains.

This guide provides instructions on configuring the BIG-IP system version 12.0 and later using an iApp™ template to simplify deployment and maintenance. As a part of the iApp, you can configure the BIG-IP system to send traffic to multiple in-line services (both at Layer 2 and Layer 3), receive-only services, ICAP services, and Metric Collector services for inspection. If you are using separate BIG-IP systems for ingress and egress traffic, the iApp adds the ability to place additional inspection devices in the decrypt zone between the two devices. See [Understanding Service Chain Classification on page 52](#) for a detailed description of how the SSL Intercept chooses service chains.

Why F5?

SSL Visibility

The proliferation of websites now leveraging SSL (including TLS in this document) encryption to protect users poses a challenge to security sensor pools in their mission to eliminate malware and attacks for outbound application requests. With the BIG-IP system, SSL Intercept can be leveraged to provide full visibility into user traffic.

SSL termination is resource-intensive. F5 BIG-IP devices include dedicated hardware processors specializing in SSL/TLS processing. In both inbound and outbound deployment scenarios, using F5 SSL Intercept solution provides uncompromising visibility into SSL traffic.

For those with policy and privacy concerns, you can configure the iApp so it does not decrypt requests to sites with sensitive data.

For more information on SSL visibility, see the **F5 Lightboard Lesson: SSL Outbound Visibility** on DevCentral: <https://devcentral.f5.com/articles/lightboard-lessons-ssl-outbound-visibility-20888>

Products and applicable versions

Product	Version
BIG-IP LTM	12.0, 12.1, 12.1.1
iApp Template Version	f5.ssl_intercept_svc_chain.v1.5.8 (all users should be on this or a later version)
Deployment guide version	1.2 (see Document Revision History on page 58)
Last updated	04-05-2017

Important: Make sure you are using the most recent version of this deployment guide, available at <http://f5.com/pdf/deployment-guides/f5-ssl-intercept-v1.5-dg.pdf>.

All documentation and additional information for this solution can be found at <https://support.f5.com/kb/en-us/products/ssl-orchestrator.html>.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com

Contents

Prerequisites and configuration notes	3
Terminology used in this solution	5
Configuration example and flow	7
Traffic flow	7
Order for completing the iApp configuration	8
How to configure in-line services using the SSL Intercept iApp template	9
Configuring the iApp for receive-only services	11
Preparation worksheet	12
Using this guide	15
Configuring the BIG-IP system using the iApp template	16
Downloading and importing the SSL Intercept iApp template	16
Getting Started with the SSL Intercept iApp	16
Template Selection	16
Welcome	17
Basic Configuration	18
In-line Services	21
Receive-Only Services	27
ICAP Services	28
Metrics Collector Services	30
Service Chains	31
TCP Service Chain Classifier Rules	32
UDP Service Chain Classifier Rules	35
Explicit Proxy Configuration	37
Ingress Device Configuration	38
Service Chain Classification Previewer	40
Egress Device Configuration (for a one device scenario)	42
Egress Device Configuration (for the separate ingress and egress device scenario)	44
Logging Configuration	47
Next Steps	48
Removing or modifying the iApp configuration	49
Understanding Service Chain Classification	50
Appendix: Additional configuration settings	54
Configuring the initial DNS settings on the BIG-IP system	54
Optional URL filtering	54
Known Issues	55
Document Revision History	56

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this guide. Read all of the prerequisites before configuring the iApp.

Important prerequisites and notes

- iApp version `f5.ssl_intercept_svc_chain.v1.5.8` contains important security improvements over previous versions. **All users should upgrade to this version as soon as possible.** See *Upgrading an Application Service from previous version of the iApp template on page 16* for instructions. See <https://support.f5.com/csp/article/K53244431> and <https://support.f5.com/csp/article/K23001529> for details.
- You must have an SSL Intercept license in order to use this functionality. Contact your F5 sales representative for details.
- We strongly recommend you back up the BIG-IP configuration before running the iApp template, as well as before making any major changes to an existing iApp configuration. See *Backing up the BIG-IP configuration before starting the configuration (or before major changes to the iApp) on page 51* for instructions.
- Because of the new features and advanced functionality in this version of the iApp template, you **cannot upgrade** an existing Application Service based on any `f5.ssl_intercept.v1.0.0` or `f5.ssl_airgap_egress` template to this version. You must start a new deployment using this template.
- For this implementation, your Sync-Failover Device Group can only contain two BIG-IP devices for high availability.
- When configuring high availability for multiple BIG-IP systems in a Sync-Failover Device Group, **DO NOT** use the Automatic Sync option. You must manually synchronize the configuration for this implementation. See *Synchronizing the BIG-IP configuration on page 50*.
- You can only have one instance of this iApp running on a BIG-IP system. You cannot have multiple instances of this iApp on any BIG-IP device.
- To intercept TLS (SSL) traffic, you must provide a Certificate Authority (CA) PKI certificate and matching private key for SSL Forward Proxy. Your TLS clients must trust this CA certificate to sign server certificates. You should have installed this certificate on the system when you ran the Setup Wizard.

If you did not import the CA certificate in the Setup Wizard, you must install your CA certificate **before** configuring this iApp. This CA certificate must have the **Digital Signature** and **Certificate Signing** key-usage properties. To import certificates and keys onto the BIG-IP system, see **System > File Management > SSL Certificate List**. For specific instructions on importing certificates and keys, see the Help tab or the BIG-IP system documentation on support.f5.com.

- This solution does not currently support vCMP implementations.
- You must download and import the SSL Intercept iApp template before you can begin the configuration. *Downloading and importing the SSL Intercept iApp template on page 16*.

General prerequisites and notes

- For this guide, the BIG-IP system **must** be running version 12.0 or later. This guide does not apply to previous versions.
- Be sure to see *Understanding Service Chain Classification on page 52* for a flow diagram and detailed explanation of how the system chooses service chains, including how the match score is calculated, and Dynamic Domain Bypass information.
- The name you give the iApp template, as well as the names you give to services and service chains are limited to 15 alphanumeric characters, including underscores, and **must** start with a letter. This message is repeated in the applicable sections of the iApp walkthrough.
- We strongly recommend using the Preparation Worksheet form (<http://f5.com/pdf/deployment-guides/ssl-intercept-preparation-worksheet.pdf>) or the *Preparation worksheet on page 12* before starting the iApp to gather a list of IP addresses, interfaces, tags and so on, you need to complete the iApp.
- See *Terminology used in this solution on page 5* for important definitions of terms used in this guide and the iApp.
- If you choose the option in this iApp template to use DNSSEC to validate DNS information, the iApp configures the initial DNSSEC keys (root Trust Anchor and div.isc.org DLV Anchor keys). When the issuer updates (replaces) those keys, you must use the Reconfigure option on the iApp template, and then click Finished. The iApp automatically retrieves the new keys. See *6. Do you want to use DNSSEC to validate DNS information? on page 41* for more information.

If you are deploying this iApp template for DNSSEC, you must have performed the initial DNS configuration on the BIG-IP system. To configure DNS on the BIG-IP system, go to **System > Configuration > Device > DNS**. In the **DNS Lookup Server List** row, add your DNS servers. For complete instructions, see the BIG-IP documentation or the Help tab.

- ▶ Be sure to see [Known Issues on page 57](#) to review any known issues that exist for this solution.
- ▶ Deleting the entire iApp configuration is a multi-step process. See [Removing or modifying the iApp configuration on page 51](#) for specific instructions.
- ▶ If you are using the iApp template for logging, before configuring the iApp we strongly recommend you configure the system to send log messages to one or more external log servers. You can choose to store logs on the BIG-IP device, but this is less desirable because BIG-IP devices have limited log storage capacity. To control where log messages are sent or stored, you must configure BIG-IP High Speed Logging features outside of the iApp template. You can then select the Log Publisher object you create in the iApp template. Configuring external logging is outside the scope of this document; for instructions see: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-0-0/4.html.

System and networking prerequisites and notes

- ▶ When separate ingress and egress devices are set up they will send each other control messages. Those can go through the decrypt zone, or around it if you configure a different path through the network. In either case, the messages are sent via TCP connections to port 245 (at an IP address you specify) on each BIG-IP from random TCP ports on the other BIG-IP.
- ▶ If you are using the BIG-IP system in a highly available configuration using a Sync-Failover device group (recommended), you must have configured the cluster before configuring the iApp template. See the BIG-IP documentation for details: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-device-service-clustering-admin-12-0-0.html. For this configuration, the Sync-Failover group can only include two BIG-IP devices.
- ▶ If you want to use IP Intelligence and/or URL filtering in this implementation, you just have the appropriate license(s) on the BIG-IP system. Contact your F5 Sales representative for specific information. Both of these options are selectable in the TCP Service Chain Classifier rule section [TCP Service Chain Classifier Rules on page 34](#) and IP Intelligence is also available in the optional [UDP Service Chain Classifier Rules on page 37](#) section. If you are deploying optional URL filtering, we strongly recommend updating the URL database before running the iApp template, see [Optional URL filtering on page 56](#).
- ▶ The Service Chain Classification Previewer is an Early Access feature and may change or not be present in future versions.
- ▶ If you are using more than a single, standalone BIG-IP system, anytime you click Finish on the iApp template, you should manually synchronize the configuration. See [Synchronizing the BIG-IP configuration on page 50](#).

Service-specific prerequisites and notes

- ▶ When installing this iApp on a BIG-IP Virtual Edition (VE), Layer 2 in-line services can NOT use the same physical interface for both Inward and Outward VLANs (not even with different VLAN tag numbers).
- ▶ Layer 3 in-line services require the user to give service (inspection) devices IP addresses from the choices in the iApp. If you are using Layer 3 in-line services, this iApp is designed to send and receive information from them using a pre-defined set of addresses. If your configuration requires different addressing, see [2. Do you want to replace in-line service subnet block\(s\)? on page 23](#). Note that changing the subnet blocks is not recommended or supported by F5 Networks, and should only be done if you understand the consequences.
- ▶ If you plan to use in-line services in this deployment and are using two devices in a Sync-Failover Group, it is critical that you configure and then SAVE the VLAN information in the In-Line Services section on both BIG-IP systems that are a part of this configuration. You must then synchronize the configuration to the other device before configuring the rest of the template. See the sections [How to configure in-line services using the SSL Intercept iApp template on page 9](#) and [Synchronizing the BIG-IP configuration on page 50](#) for more information.
- ▶ After deploying the iApp template, if you want to modify or remove an active in-line service, see the instructions in [Modifying or deleting an in-line service you already created on page 10](#).
- ▶ If you choose to configure Receive-Only services and are using more than a single, standalone BIG-IP system (multiple devices in a Sync-Failover group): After you click Finished on the device you are currently configuring, on each device in the Sync-Failover group you must use the Reconfigure option (click **iApps > Application Services > name you gave the iApp > Reconfigure** (on the menu bar)), and then click Finished (even if you do not make any other changes) in order for the iApp to install the non-floating configuration for Receive-Only services on each device. See [Receive-Only Services on page 29](#) for more information.
- ▶ The Metrics Collector service is an Early Access feature and may change or not be present in future versions of this solution.

Terminology used in this solution

This section defines some of the terms used in this guide and the iApp template.

- **Sync-Failover device group**

A Sync-Failover device group (part of the Device Service Clustering (DSC®) functionality) contains BIG-IP devices that synchronize their configuration data and fail over to one another when a device becomes unavailable. In this configuration, a Sync-Failover device group supports a maximum of two devices. For more information on Sync-Failover device groups, see the BIG-IP documentation: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-device-service-clustering-admin-12-0-0/5.html#conceptid. For information on synchronizing the configuration, see [Synchronizing the BIG-IP configuration on page 50](#).
- **Ingress device**

The ingress BIG-IP system is the device (or Sync-Failover device group) to which each client sends traffic. In the scenario where both ingress and egress traffic are handled by the same BIG-IP system, ingress refers to the ingress VLAN(s) where the clients send traffic. The ingress BIG-IP system (or ingress VLAN(s)) decrypts the traffic and then based on protocol, source, destination, and so on, classifies it and passes each connection for inspection based on service chains you will configure (or allows certain connections to bypass service-chain processing based on your selections).
- **Egress device**

The egress BIG-IP system is the device (or Sync-Failover device group) that receives the traffic after a connection traverses the chosen service chain and then directs it to its final destination. In the scenario where both ingress and egress traffic are handled by the same BIG-IP system, egress refers to the egress VLAN(s) where the BIG-IP system receives traffic.
- **In-line services**

In-line services pass traffic through one or more service (inspection) devices at Layer 2 (MAC/bump in the wire) or Layer 3 (IP). Each service device communicates with the ingress BIG-IP device over two VLANs called *Inward* and *Outward* which carry traffic toward the intranet and the Internet respectively. You can configure up to ten in-line services using the iApp template. For detailed information on configuring in-line services, see [How to configure in-line services using the SSL Intercept iApp template on page 9](#).
- **Receive-only services**

Receive-only services refer to services that only receive traffic for inspection, and do not send it back to the BIG-IP system. Each receive-only service provides a packet-by-packet copy of the traffic (e.g. plaintext) passing through it to an inspection device. You can configure up to ten receive-only services using the iApp template. For more information on receive-only services, see [Receive-Only Services on page 29](#).
- **ICAP services**

Each ICAP service uses the ICAP protocol (<https://tools.ietf.org/html/rfc3507>) to refer HTTP traffic to one or more Content Adaptation device(s) for inspection and possible modification. You can add an ICAP service to any TCP service chain, but only HTTP traffic is sent to it, as ICAP does not support other protocols. You can configure up to ten ICAP services using the iApp template. For more information on ICAP services, see [ICAP Services on page 30](#).
- **Metric Collector services**

The purpose of the metric collector services is to gather statistical information (like bytes transferred) whenever they are placed in a service chain. These services are internal to the SSL intercept iApp and do not examine or modify data in connections. You can see the statistics in the BIG-IP Configuration utility. For more information on metric collector services, see [Metrics Collector Services on page 32](#). Note this is an Early Access feature and may change or not be present in future versions of this solution.
- **Service chains**

SSL Intercept service chains process specific connections based on classifier rules which look at protocol, source and destination addresses, and so on. These service chains can include four types of services (Layer 2 in-line services, Layer 3 in-line services, receive-only services, and ICAP services) you define, as well as any decrypt zone between separate ingress and egress devices). For more information on service chains, see [Service Chains on page 33](#).
- **Service chain classifier rules**

Each service chain classifier rule chooses ingress connections to be processed by a service chain you configure (different classifier rules may send connections to the same chain). Each classifier rule has three filters. The filters match source (client) IP address, destination (which can be IP address, IP Intelligence category, IP geolocation, domain name, domain URL Filtering category, or server port), and application protocol (based on port or protocol detection). Filters can overlap so the solution chooses the classifier rule which best matches each connection.

For more information, see the detailed section [Understanding Service Chain Classification on page 52](#).
For more information on service chain classifier rules, see [TCP Service Chain Classifier Rules on page 34](#) and/or [UDP Service Chain Classifier Rules on page 37](#).

- **Service Chain Classification Previewer**

The service chain classification previewer is a useful tool that allows you to use a web browser or HTTP client to ascertain which service chain would be chosen for a connection with certain parameters of protocol, source, destination, and so on. It is a small web page/service hosted on the ingress BIG-IP device (or device group). For more information on the previewer, see [Service Chain Classification Previewer on page 42](#). Note this is an Early Access feature and may change or not be present in future versions of this solution.

- **Decrypt zone**

A decrypt zone refers to the network region between separate ingress and egress BIG-IP devices where cleartext data is available for inspection. Basically an extra in-line service can be placed at the end of every service chain for additional inspection. You cannot configure a decrypt zone in the scenario where a single BIG-IP system handles both ingress and egress traffic.

- **Transparent/Explicit Proxy**

This solution can operate in transparent and/or explicit proxy mode. A transparent proxy intercepts normal communication without requiring any special client configuration; clients are unaware of the proxy in the network. An explicit proxy requires manual configuration on the client. In this solution, the transparent proxy scheme can intercept all types of TLS and TCP traffic. It can also process UDP and forward other types of IP traffic. The explicit proxy scheme supports only HTTP(S) per RFC2616.

- **Certificate Authority (CA) certificate**

This solution requires a Certificate Authority PKI (public key infrastructure) certificate and matching private key for SSL Forward Proxy. Your TLS clients must trust this CA certificate to sign server certificates. You must import the certificate and key before you start the iApp template, as importing certificates and keys is not a part of the template. See **System > File Management > SSL Certificate list > Import** to install your CA certificate. This CA certificate must have the **Digital Signature** and **Certificate Signing** key-usage properties.

- **SNAT**

A SNAT (Secure Network Address Translation) is a feature that defines routable alias IP addresses that the BIG-IP substitutes for client IP source addresses when making connections to hosts on the external network. A **SNAT pool** is a pool of translation addresses that you can map to one or more original IP addresses. Translation addresses in a SNAT pool are not self IP addresses.

- **Static and Floating configuration objects**

In the iApp and this guide, we refer to static and floating BIG-IP configuration objects. *Static* configuration objects mean those objects which must be configured separately on each device, such as VLAN and self IP objects. These objects are not synchronized across the BIG-IP devices in a Sync-Failover group, as those object must remain unique.

Floating configuration objects are those that are shared across the Sync-Failover group, such as virtual servers and pools. These objects are synchronized to all devices in the cluster.

- **Data groups (including @pinners)**

A BIG-IP data group is a group of related elements, such as a set of IP addresses for specific clients. These data groups are used in the iRules that are a part of the iApp template and eliminate the need to list multiple values as arguments in an iRule expression. Data groups are not created by the iApp (with the exception of @pinners described in the next paragraph), but you can use them in your service chain classifier rules. This allows you to create and maintain these groups without having to modify the iApp. For more information on data groups, see [Using BIG-IP Data Groups to match IP address, domain names, geolocations, or IPI/URL filtering categories \(optional\) on page 34](#).

The iApp does include one preconfigured domain-name matching data group called **@pinners** which contains a list of domain names. These are domain names of some TLS- (SSL-) based services from well-known businesses like Microsoft that support software (such as Microsoft Update) which may not work well when their connections are intercepted and decrypted by the SSL Intercept solution. For complete details, see [Using the @pinners data group on page 34](#).

- **iApp and Application Service**

The iApp is the template you use to configure the BIG-IP system for SSL Intercept. An Application Service is the resulting configuration produced and owned by the iApp template.

Configuration example and flow

This guide describes how to configure the BIG-IP system as an SSL Forward Proxy with a decrypt zone. The ingress/egress BIG-IP system scenario looks like the following diagram (in a one-device scenario, a single BIG-IP handles both ingress and egress duties. In that case, there will be no decrypt zone between BIG-IP devices). Note that while the diagram shows a single BIG-IP system for the ingress and egress, this will often be two devices in a high availability configuration, referred to as a Sync-Failover device group.

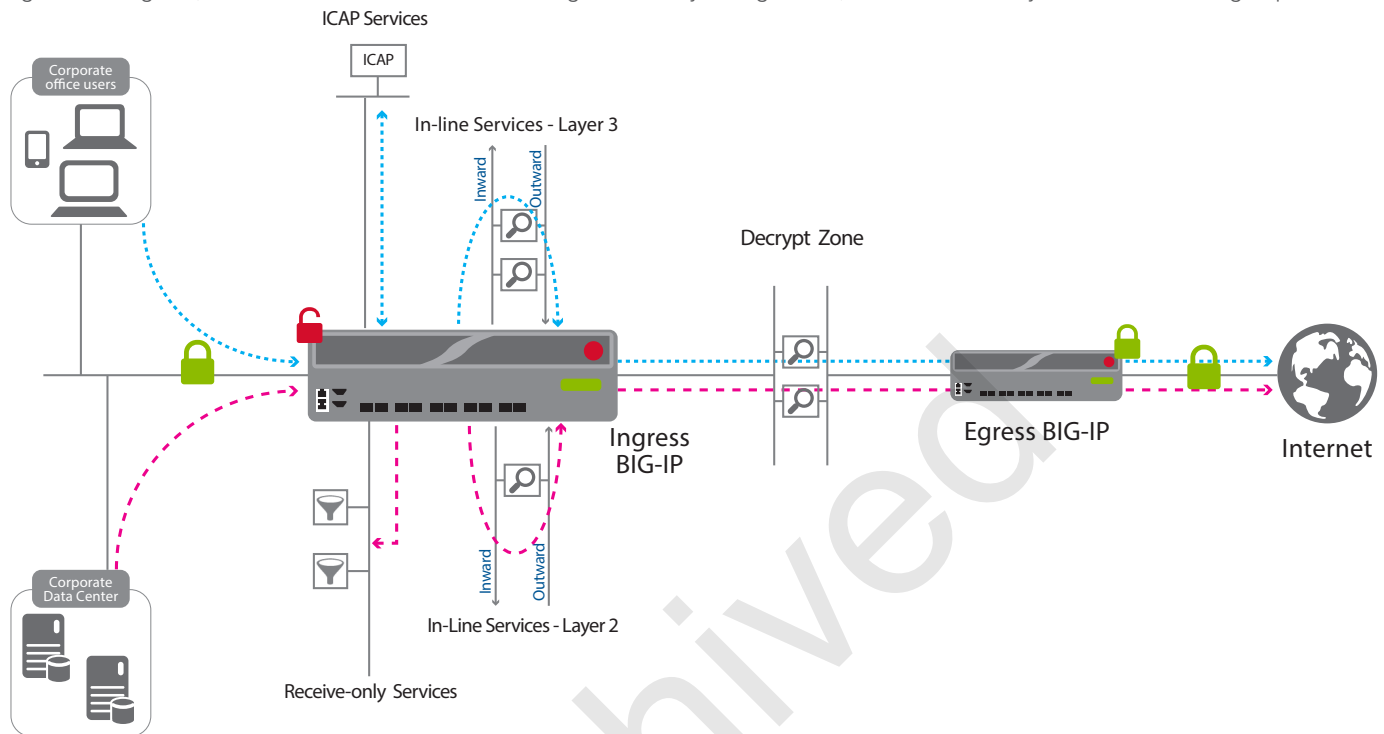


Figure 1: Logical configuration diagram of the SSL intercept configuration using an ingress and egress BIG-IP system

Traffic flow

Traffic originates on the VLANs you specify. In our configuration example, we have two locations from which encrypted traffic originates: corporate users, and the corporate data center.

Each client sends traffic to the ingress BIG-IP device (or the ingress side of a single BIG-IP system). The ingress BIG-IP system decrypts the traffic, and then based on protocol, source, destination, and so on, classifies the traffic and then passes each connection for inspection based on service chains you will configure (or allows certain connections to bypass service-chain processing based on your selections).

This iApp template supports in-line services on Layer 2 and Layer 3, receive-only services, ICAP services, and metrics collector services. If you are using separate BIG-IP systems for ingress and egress traffic as shown in the diagram, you can also have a *decrypt zone* network between them that carries plaintext and you may place service devices in that network for further inspection. Note that even when ingress and egress devices are separate, the ingress device must have a route to remote servers so the decryption function can fetch servers' PKI certificates. See [Terminology used in this solution on page 5](#) for definitions of the services.

In our example, the traffic from the corporate office users is sent to ICAP services (which deliver HTTP requests/replies to ICAP servers) and then in-line services at Layer 3 (which send traffic through an L3 gateway or proxy device) for inspection. Traffic from the corporate data center is sent to receive-only services (the BIG-IP provides a copy of the decrypted data stream to the receive-only devices) and then in-line services at Layer 2 (which send traffic through an L2 'bump-in-the-wire' device) for inspection. You may configure multiple services in the chain depending on the level of inspection you want. See [Understanding Service Chain Classification on page 52](#) for a detailed description of how the SSL Intercept chooses service chains.

After a connection traverses the chosen service chain, the egress BIG-IP device (or the egress side of a single BIG-IP system) directs it to its final destination. Each service chain is an ordered list of services of various types. For TLS connections the decryption function always precedes the service chain and the re-encryption function comes after. In between those, the connection's plaintext is available to services (inspectors) in the chain.

Order for completing the iApp configuration

The following list shows the order of tasks for completing the SSL Intercept iApp configuration. This list is meant to provide a general overview of the steps necessary; detailed information is found in the iApp walkthrough and in the first pages of this guide.

To review the definitions of the terms used in this list, see [Terminology used in this solution on page 5](#). We recommend reading this entire guide before visiting the links referenced in this list.

1. **Complete the Preparation Worksheet.**

You can use the Preparation Worksheet form (<http://f5.com/pdf/deployment-guides/ssl-intercept-preparation-worksheet.pdf>) or the [Preparation worksheet on page 12](#).

2. **Download and import the iApp template**

If the SSL Intercept iApp template is not present on your BIG-IP system, follow the instructions in [Downloading and importing the SSL Intercept iApp template on page 16](#).

3. **Open the template and complete the Template Selection, Welcome, and General Configuration sections.**

Template Selection contains the Name field and template selection. *Welcome* contains inline help options and an option to delete the iApp configuration. *General Configuration* contains questions about your BIG-IP setup, as well as CA certificate, proxy mode, and IP addressing family questions. These sections of the walkthrough start with [Template Selection on page 17](#).

4. **Configure In-Line services (if applicable)**

If you have any Layer 2 or Layer 3 in-line services to add to this configuration, configure the in-line services section of the iApp as applicable. See [How to configure in-line services using the SSL Intercept iApp template on page 9](#) for information on how to configure in-line services. The in-line services section of the iApp walkthrough starts on [page 23](#).

- a. If you are using a pair of BIG-IP systems as a Sync-Failover group for HA, it is important to save and then synchronize the configuration after configuring Stage 1 of the in-line service(s).
- b. After synchronizing the configuration, re-enter the template to complete Stage 2 of the in-line services configuration.

5. **Configure Receive-Only (if applicable)**

If you have any receive-only services you want to be a part of this configuration, configure the receive-only section. The receive-only section of the iApp walkthrough starts on [page 29](#).

- a. If you are using two BIG-IPs as a Sync-Failover group, you must save and synchronize the configuration after configuring the receive-only service(s). You must open and save the configuration on the other system (no changes necessary).
- b. After synchronizing the configuration, re-enter the template on one system to complete the rest of the template.

6. **Configure ICAP services (if applicable)**

If you have any ICAP services you want to be a part of this configuration, configure the ICAP section of the template. The ICAP section of the iApp walkthrough starts on [page 30](#).

7. **Configure Metrics Collector (optional)**

If you plan to use metrics collector services to gather statistical information, configure the metrics collector section of the template. The metrics collector section of the iApp walkthrough starts on [page 32](#).

8. **Configure Service Chains**

After creating the applicable services, you configure the service chains. Service chains consist of a list of one or more of the services you configured. The service chain section of the iApp walkthrough starts on [page 33](#).

9. **Configure Service Chain Classifier rules**

After creating service chains, you configure the service chain classifier rules which process specific connections using the service chains you configured. The service chain classifier rules section of the iApp walkthrough starts on [page 34](#).

10. **Configure Explicit Proxy options (optional)**

If you are using explicit proxy, you configure these options. The ingress section of the iApp walkthrough starts on [page 39](#).

11. **Ingress Device configuration**

Next, you configure ingress device settings, such as VLAN, certificate, and DNS information. The ingress section of the iApp walkthrough starts on [page 40](#).

12. **Service Chain Classification previewer (optional)**

The previewer allows you to preview the path of a connection through the service chains. The previewer section of the iApp walkthrough starts on [page 42](#).

13. **Egress Device configuration**

Next, you configure egress device settings. The egress section of the iApp walkthrough starts on [page 44](#).

14. **Configuring Logging (optional)**

The last section gives you the different logging options. The logging section of the iApp walkthrough starts on [page 49](#).

How to configure in-line services using the SSL Intercept iApp template

Because of the extreme flexibility of the SSL Intercept iApp template, the configuration for in-line services is a multi-step process. To help eliminate any potential confusion, this section provides an overview of how to configure the iApp template for in-line services.

For step-by-step guidance, see *In-line Services on page 23* in the iApp walkthrough section. The following flow diagram visually represents the process.

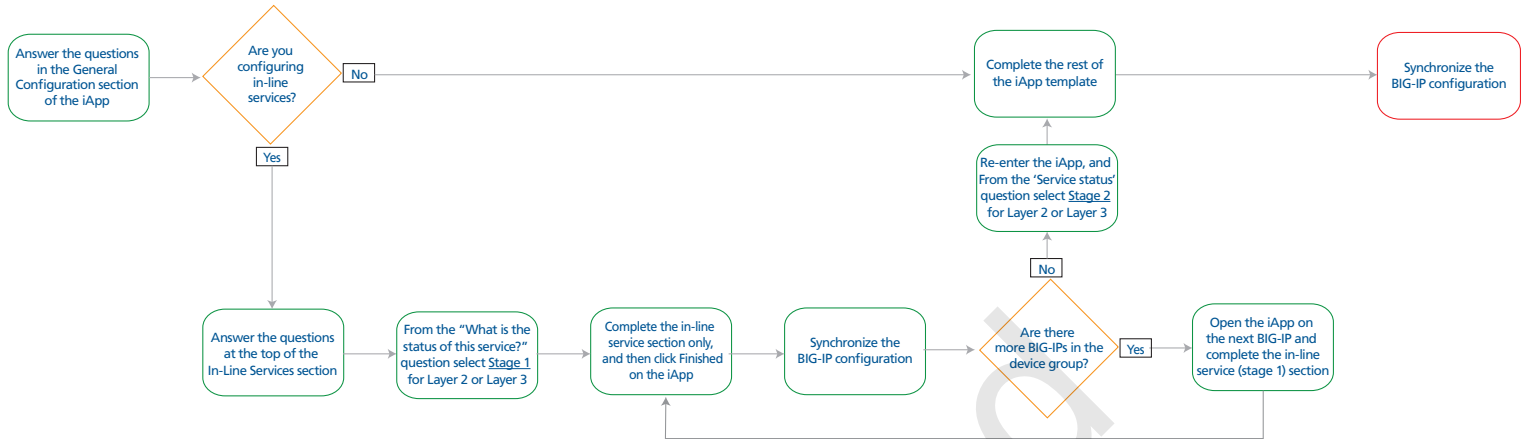


Figure 2: In-line service flow chart

i Important If you are only using a standalone BIG-IP system and not a Sync-Failover Group for high availability, you do not need to perform the ConfigSync operation. You do still need to save the configuration after configuring the stage 1 options and then re-enter the template to configure stage 2.

Importance of synchronizing the BIG-IP configuration for in-line services

If you are using more than a single (standalone) BIG-IP system, you must configure the VLAN information (using one of the Stage 1 options described in the following bullets) on both devices in the Sync-Failover group, synchronizing the configuration after each. This is because the process of configuring VLANs creates all of the static configuration objects— objects which the synchronization process does not replicate across BIG-IP devices in the cluster. Additionally, synchronizing the configuration after the entering the VLAN information makes the other devices aware you intend to setup one or more in-line services (but this does not actually configure VLANs on any of these devices). If you are using a standalone BIG-IP system, this is not applicable.

In-line service types

The following is a brief overview of the service types and how to use them.

➤ **Configuring in-line services for the first time (and modifying existing services or temporarily removing a service)**

When you are initially configuring in-line services, you choose one of the *Stage 1* options to first configure the VLAN information (and load balancing information for Layer 2 services). You would also select this option if you have already submitted the template and want to modify an existing in-line service, or temporarily remove a service from the configuration without permanently deleting it.

- **Stage 1: Configure VLANs for Layer 2 (bump in the wire)**

When you are initially configuring the iApp for Layer 2 in-line services, you select this option. When you select stage 1, the questions about the service name, number of devices, and VLAN details appear. You **MUST** configure these options, submit the iApp, and then synchronize the configuration (see *page 50*) before completing the remainder of the template.

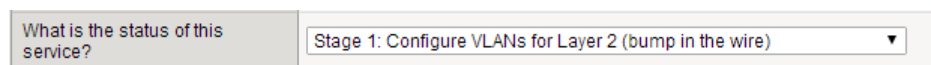


Figure 3: Configuring stage 1 of a layer 2 in-line service

- **Stage 1: Configure VLANs for Layer 3 (IP gateway)**

When you are initially configuring the iApp for Layer 3 in-line services, you select this option. When you select stage 1, the questions about the service name and VLAN information appear. You MUST configure these options, submit the iApp, and then synchronize the configuration (see [page 50](#)) before completing the remainder of the template.

What is the status of this service?	Stage 1: Configure VLANs for Layer 3 (IP gateway) ▼
-------------------------------------	---

Figure 4: Configuring stage 1 of a layer 3 in-line service

➤ **Preparing in-line services for use in a service chain**

After you have completed the initial VLAN configuration, the next step is to activate the in-line services you created.

- **Stage 2: Finalize Layer 2 (bump in the wire) configuration**

Once you have completed Stage 1 of the Layer 2 services and synchronized the configuration, you use the Reconfigure option on the application service to re-enter the template and then select this option enable the service to be used in a service chain. When you select this option, the questions about the service name, service failure options, and port for HTTP traffic appear. Configure these options as applicable, and then configure the rest of the template.

What is the status of this service?	Stage 2: Finalize Layer 2 (bump in the wire) configuration ▼
-------------------------------------	--

Figure 5: Configuring stage 2 of a layer 2 in-line service

- **Stage 2: Finalize Layer 3 (IP gateway) configuration**

Once you have completed Stage 1 of the Layer 3 services and synchronized the configuration, you use the Reconfigure option on the application service to re-enter the template and then select this option to enable the service to be used in a service chain. When you select this option, the questions about the service name and VLAN information appear. You MUST configure these options, submit the iApp, and then synchronize the configuration before completing the remainder of the template.

What is the status of this service?	Stage 2: Finalize Layer 3 (IP Gateway) configuration ▼
-------------------------------------	--

Figure 6: Configuring stage 2 of a layer 3 in-line service

➤ **Unconfigured (or delete existing service when I click Finished)**

Use this option if you want to completely and permanently remove an existing in-line service from the configuration. Once you select this option and then click Finished on the iApp, the in-line service is permanently gone.

What is the status of this service?	Unconfigured (or delete existing service when I click Finished) ▼
-------------------------------------	---

Figure 7: An unconfigured in-line service

Modifying or deleting an in-line service you already created

In order to delete or modify an in-line service that has been already configured and set to Stage 2, use the following guidance.

1. Use the Reconfigure option on the template (**iApps > Application Services > name you gave the iApp > Reconfigure** (on the menu bar) to re-enter the iApp.
2. In the In-Line Services section, find the service you want to modify or delete.
3. From the *What is the status of this service?* question, select the applicable Stage 1 option (either Layer 2 or Layer 3).
4. Click **Finished** on the iApp and then synchronize the configuration.
5. The next steps depend on if you want to modify or delete the service.

Modifying an inline service

- a. After you set the service to Stage 1 and have synchronized the configuration, reconfigure the iApp again. You can then modify the VLAN (and load balancing information for Layer 2 in-line services) as necessary.
- b. After you have modified the service, click **Finished**, and then synchronize the configuration.

Deleting an inline service

- a. After you set the service to Stage 1 and have synchronized the configuration, use the reconfigure option again to enter the template.
- b. From the *What is the status of this service?* question for the in-line service you want to delete, select **Unconfigured (or delete existing service when i click Finished)**.
- c. Click **Finished**, and then synchronize the configuration. The in-line service is now deleted.

If you want to delete the entire iApp configuration, see [Removing or modifying the iApp configuration on page 51](#).

Configuring the iApp for receive-only services

If you are using more than a single, standalone BIG-IP device, configuring the iApp for receive-only services does not require the two-stage process that in-line services does, but it does require an additional task.

1. After configuring receive-only services in the iApp and clicking Finished, synchronize the configuration.
2. Open the iApp template on the other BIG-IP system in the Sync-Failover group.
3. Simply click Finished without making any other changes. This installs the non-floating objects for the receive-only configuration.

See [Receive-Only Services on page 29](#) for step-by-step guidance.

Preparation worksheet

This table includes the information that is helpful to have before configuring the iApp template. **We strongly recommend you print these tables and then enter the information so you have it available when you configure the iApp template.** For a separate, form-enabled version of the worksheet, see <http://f5.com/pdf/deployment-guides/ssl-intercept-preparation-worksheet.pdf>.

More specific information on individual items can be found in the template walkthrough or in the Configuration example.

BIG-IP Preparation worksheet																																																											
<p>BIG-IP IP Addresses and iApp template name</p> <p>You should have the following BIG-IP addresses available or reserved.</p> <p>You may have more than two Gateway addresses. Only two spaces are shown for space. Use the back of these sheet or the margins.</p>	<p style="text-align: center;">Ingress</p> <p>Management port IP for each Ingress device in the cluster</p> <p>1) _____</p> <p>2) _____</p> <p>IP Address for Ingress device control-channel virtual server</p> <p>1) _____</p> <p>If you are configuring separate Ingress and Egress devices, the template needs to know the name you will give the iApp application service (the Name field at the top of the template) on the other device. You can use the same name for the iApp application on both devices.</p> <p>This name must be 1-15 alphanumeric or underscore characters and must start with a letter (not case sensitive).</p> <p>Ingress device iApp name: _____</p>		<p style="text-align: center;">Egress</p> <p>Decrypt zone: IPv4 gateway (Self IP) addresses (if using IPv4)</p> <p>1) _____</p> <p>2) _____ (etc)</p> <p>Decrypt zone: IPv6 gateway (Self IP) addresses (if using IPv6)</p> <p>1) _____</p> <p>2) _____ (etc)</p> <p>IP Address for Egress device control-channel virtual server</p> <p>1) _____</p> <p>Address of each IPv4 exit gateway (if using IPv4)</p> <p>1) _____</p> <p>2) _____ (etc)</p> <p>Address of each IPv6 exit gateway (if using IPv6)</p> <p>1) _____</p> <p>2) _____ (etc)</p> <p>If configuring separate ingress and egress devices: Egress device iApp name: _____</p>																																																								
	In-line Services Initial VLAN configuration																																																										
<p>In-Line Services</p> <p>For each in-line service you plan to use (if any), you first need to assign an Interface to the Inward and Outward VLANs and possibly a tag. You can include a maximum of 10 services.</p> <p>Each service can have up to 8 devices. We only provide space for 4 services with 4 devices for each service here, see the printable version for more.</p> <p>It is helpful to also record the name you will give the service, as you have to type this name when configuring service chains.</p>	<table border="1"> <thead> <tr> <th>Service name</th> <th>Inward VLAN Interface</th> <th>Tag</th> <th>Outward VLAN interface</th> <th>Tag</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td><td> </td><td> </td></tr> </tbody> </table>				Service name	Inward VLAN Interface	Tag	Outward VLAN interface	Tag																																																		
	Service name	Inward VLAN Interface	Tag	Outward VLAN interface	Tag																																																						
<p>Each Service can be either Layer 2 (bump in the wire), or Layer 3 (IP Gateway).</p> <p>For each in-line service, no matter which type, you must choose whether you want to inspect all apparent HTTP traffic on port 80, 8080, or 8443, or if connections should use their original ports (such as 443, though unencrypted).</p> <p>If you are deploying a Layer 3 in-line service, see In-line Services on page 23 for specific information about the device IP addresses.</p>																																																											

BIG-IP Preparation worksheet

Receive Only Services

For each receive-only service you plan to use (if any), you must provide the MAC address and a unique IP address to go with it. The MAC must be reachable via a BIG-IP VLAN, and the IP must be homed on a subnet configured on the same VLAN. You can include a maximum of 10 services.

Service Name	Device Addresses		Device Network	
	MAC Address	Nominal IP Address	BIG-IP VLAN	Interface

ICAP Services

If you are deploying the template for ICAP services, you can define up to 10 ICAP services. Each service can include multiple ICAP servers. We only include space for 4 services, and 4 servers per service in the table; you may have more. See the printable worksheet for the full table.

Only specify a port if it is different than the ICAP default port: 1344.

Editing ICAP headers is optional.

Service Name	ICAP Device Addresses			
	IP Address	Port	IP Address	Port

Service Name	ICAP Request and Response Processing URIs	
	Request	Response

Service Name	Optional: Editing ICAP headers			
	ICAP Host header	ICAP Referer header	ICAP User-Agent header	ICAP From header

Optional: Explicit Proxy

If you are implementing an explicit proxy, you must choose the BIG-IP VLAN on which the proxy should listen, and the IPv4 and/or IPv6 address and port.

VLAN(s)	IPv4 Address (if applicable)	Port	IPv6 Address (if applicable)	Port

BIG-IP Preparation worksheet

Optional: SNAT Pool addresses

If will configure secure address translation (SNAT) to replace clients' source IP addresses on outbound connections with addresses belonging to the BIG-IP (recommended) you must assign IP addresses (which are routed to the egress BIG-IP device).

SNAT Pool IP addresses	

DNS

You must decide whether you want to send DNS queries to forwarding nameservers on the local network or directly to nameservers across the Internet

Send to forwarding nameservers on local network	Send to nameservers across the Internet										
<p>You should have at least two nameservers on the local network. Specify the IP addresses (you may have more/less than 4)</p> <p>1) _____</p> <p>2) _____</p> <p>3) _____</p> <p>4) _____</p>	<p>The ingress device will locate Internet nameservers automatically, but you must choose if you want to configure local/private DNS zones. If you do, you must specify the local/private forwarding zones. You may have more/less than 4.</p> <p>This also requires DLV keys (long hexadecimal strings). You should prepare to copy them from your local source and then paste them into the iApp.</p> <table border="1"> <thead> <tr> <th>Forward Zone</th> <th>Nameserver</th> </tr> </thead> <tbody> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> <tr><td> </td><td> </td></tr> </tbody> </table>	Forward Zone	Nameserver								
Forward Zone	Nameserver										

Optional: Service Chain Classification Previewer

If you want to use the previewer to use a web browser or HTTP client to see which service chain would be chosen for a connection, you need to gather this information. Only enter the IPv4/IPv6 information for the version you are using.

VLANs with access	
IPv4 address for previewer (if using v4)	
IPv6 address for previewer (if using v6)	
TCP port for previewer (port 80 is usually fine)	
Existing SSL profile (optional)	
IPv4 subnets clients must connect from	
IPv6 subnets clients must connect from	

Once you have gathered the information using the worksheet, continue with the iApp walkthrough starting on the next page.

Using this guide

This deployment guide is intended to help users deploy the SSL Intercept v1.5 iApp template using the BIG-IP system. The iApp template configuration portion of this guide walks you through the entire iApp, giving information and guidance for each question. The questions in the UI for the iApp template itself are all displayed in a table and at the same level.

In this guide, we have grouped related questions and answers in a series of lists. Questions are part of an ordered list and are underlined and in italics or bold italics. Options or answers are part of a bulleted list, and in bold. Questions with dependencies on other questions are shown nested under the top level question, as shown in the following example:

1. *Top-level question found in the iApp template*

The text under the question provides information specific to the question.

- ***Select an object you already created from the list***
Some questions have options for selecting previously created objects, such as an SSL certificate; shown in bold italic. The text under the bullet provides information about the choice.

- **Choice #1** (in a drop-down list)

- **Choice #2** (in the list)

a. *Second level question dependent on selecting choice #2*

Explanatory text

- **Sub choice #1**
Explanatory text

- **Sub choice #2**

a. *Third level question dependent on sub choice #2*

Explanatory text

- **Sub-sub choice**
Explanatory text

- **Sub-sub #2**

a. *Fourth level question (and so on)*

Explanatory text

Configuring the BIG-IP system using the iApp template

Use this section for guidance on downloading, importing, and configuring the iApp template for SSL Intercept. We recommend you complete the *Preparation worksheet on page 12* before starting the iApp configuration. We strongly recommend backing up the configuration before starting the iApp, see *Removing or modifying the iApp configuration on page 51* for instructions.

Downloading and importing the SSL Intercept iApp template

The first task is to download the SSL Intercept iApp template, and then import it onto the BIG-IP system.

To download and import the iApp

1. Open a web browser and go to downloads.f5.com.
2. Click **Find a Download**, and then in the **Security F5 Product Family** section, click **SSL Orchestrator**.
3. Select BIG-IP version **12.1** from the list, and then click **SSL Orchestrator**.
4. Accept the End User License agreement, and then download the iapps zip file to a location accessible from your BIG-IP system.
5. Extract (unzip) the **f5.ssl_intercept_svc_chain.v1.5.8.tmpl** file. *All users should be on this or a later version.*
6. Log on to the BIG-IP system web-based Configuration utility.
7. On the Main tab, expand **iApp**, and then click **Templates**.
8. Click the **Import** button on the right side of the screen.
9. Click a check in the **Overwrite Existing Templates** box.
10. Click the **Browse** button, and then browse to the location you saved the iApp file.
11. Click the **Upload** button. The iApp is now available for use.

Upgrading an Application Service from previous version of the iApp template

If you configured your BIG-IP system the f5.ssl_intercept iApp template, and a new version comes out, use the following procedure to upgrade the iApp template to the most recent version.

When you upgrade to the current template version, the iApp retains all of your settings for use in the new template. In some new versions, you may notice additional questions or existing questions asked in different ways, but your initial settings are always saved.

To upgrade an Application Service to the current version of the template

1. From the Main tab of the BIG-IP Configuration utility, expand **iApp** and then click **Application Services**.
2. Click the name of your existing f5.ssl_intercept_svc_chain application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. At the top of the page, in the **Template** row, click the **Change** button to the right of the list.
5. From the **Template** list, select **f5.ssl_intercept_svc_chain.<latest version>**.
6. Click **Finished**.
7. Synchronize the configuration across the devices in the Sync-Failover device group.

After you synchronize the configuration, you can re-enter the template and modify any of the settings as usual.

Getting Started with the SSL Intercept iApp

To begin the iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.

Template Selection

This section contains general template information, including the name you give the iApp Application Service

1. **Name**

In the **Name** box, type a name for this application service. In our example, we use **intercept**.

 **Warning** Names must contain 1-15 alphanumeric or underscore characters and must start with a letter (not case sensitive).

2. From the **Template** list, select **f5.ssl_intercept_svc_chain.v1.5.8** (or newer if applicable).
3. Leave **Device Group** and **Traffic Group** at their default settings (these options only appear if you selected **Advanced** from the **Configuration** list at the top of the template).

Welcome

At the bottom of the Welcome section of the iApp template, you will find the following questions.

1. **Do you want to see inline help?**

Select whether you want to see informational and help messages inline throughout the template. Important and critical notes are always shown, no matter which selection you make. Because of the number of different advanced options in the template, we recommend you select **Yes, show inline help** at least the first time you use the iApp template.

- **Yes, show inline help**

Select this option to show inline help for most questions in the template.

- **No, do not show inline help**

Select this option if you do not want to see inline help. If you are familiar with this iApp template, or with the BIG-IP system in general, you can select this option to hide the inline help text.

2. **Do you want to remove this application service?**

Select whether you want to configure the system for SSL Intercept or completely remove an existing SSL Intercept configuration.

This feature exists because the iApp template creates or modifies some system configuration objects which are not removed when you delete the iApp application service. If you select to remove the application service using this option, all objects not normally removed by the template are cleanly removed. You can then delete the Application Service normally.

- **NO. I want to CONFIGURE the SSL Intercept application**

Select this option to configure the BIG-IP system using the SSL Intercept iApp template. Continue with the next section.

- **Yes. I want to REMOVE this SSL Intercept application service**

Select this option if you previously deployed the SSL Intercept iApp and want to completely remove the entire configuration. If you select this option, the Application Service Removal section appears, and the rest of the template goes away.

- a. **Which step do you want to perform now?**

Select the appropriate step. You must perform both of the following options to remove the configuration entirely.

- **First step-- remove floating objects**

Select this option as the first step in the removal process, and then click **Finished**. The floating objects, such as virtual servers are deleted. You must synchronize the configuration (see [Synchronizing the BIG-IP configuration on page 50](#)).

- **Final step-- remove static objects (like VLANs)**

Select this option if you have already performed the first step. Click **Finished**, and static objects are removed.

IMPORTANT: You must perform this step on every BIG-IP system in the Sync-Failover device group.

When you have finished the final step on all BIG-IP devices, click **iApps > Application Services**. Click the box next to your SSL Intercept service, and then click **Delete**. The configuration is now completely deleted.

If you experience an error, be sure to see [*You may experience a "cannot delete" error in certain situations after configuring the Egress device to send traffic to the Internet via specific gateways on page 57.*](#)

Archived

General Configuration

This section contains general information the system needs before you begin configuring services and service chains.

1. ***Do you want to configure separate ingress and egress BIG-IP devices with a decrypt zone network between them?***

Choose whether or not you are using separate devices for ingress and egress traffic (with a decrypt network zone between the two devices). If you are deploying separate devices (or separate Sync-Failover Groups), you must run this iApp on both devices, selecting the appropriate answers in the following questions.

- **No. This BIG-IP device will handle ingress and egress**

Select this option if you have the same BIG-IP (or Sync-Failover group) will receive both ingress and egress traffic on different networks. Continue with #2.

- **Yes. Configure separate ingress and egress BIG-IP devices**

Select this option if you are configuring separate devices (or Sync-Failover Groups) for ingress and egress traffic. You must run this template on both devices, and select which device you are currently configuring from the following question.

- a. ***Is THIS device the ingress or egress BIG-IP device?***

Choose whether the device you are currently configuring is the ingress or egress device. Your answer determines some of the questions that appear in the remainder of the template.

- **THIS DEVICE is the INGRESS device to which clients connect**

Select this option if you are currently configuring the Ingress BIG-IP device. You must answer the following questions.

- a. ***What is the name you have the iApp on the EGRESS device?***

Type the name you gave (or will give) the iApp template application service on the Egress BIG-IP device. Again, this name must contain 1-15 alphanumeric or underscore characters and must start with a letter (not case sensitive). The iApp uses this as part of the service channel communication between devices.

- b. ***What is the IP address of the EGRESS device control-channel virtual server?***

Type the IP address of the service chain control channel virtual server over on the EGRESS device. This device (ingress) must have an IP route to that IP address.

- c. ***What IP address should THIS (ingress) device's control-channel virtual server use?***

You must assign an IP address to the virtual server for the service chain control channel on a VLAN (and subnet) which will carry control data to and from the egress device (often VLAN *external*). The control channel uses TCP port 245.

- d. ***What is the control-channel pre-shared key?***

Type a pre-shared key (PSK) value to enable cryptographic protection of the service chain control channel between the ingress and egress devices. You must enter exactly the same PSK value on **both** the ingress and egress devices. The PSK value must be a string of printable ASCII characters-- you may enter a passphrase or a text representation (such as hexadecimal or base64) of a binary key.

- **THIS DEVICE is the EGRESS device which connects to servers**

Select this option if you are currently configuring the Egress device.

- a. ***What is the name you have the iApp on the INGRESS device?***

Type the name you gave, or will give, the iApp template application service on the Ingress BIG-IP device. Again, this name must contain 1-15 alphanumeric or underscore characters and must start with a letter (not case sensitive). The iApp uses this as part of the service channel communication between devices.

- b. ***What is the IP address of the INGRESS device control-channel virtual server?***

Type the IP address of the service chain control channel virtual server over on the INGRESS device. This device (egress) must have an IP route to that IP address.

- c. ***What IP address should THIS (egress) device's control-channel virtual server use?***

You must assign an IP address to the virtual server for the service-chain control channel on a VLAN (and subnet) which will carry control data to and from the egress device (often VLAN *external*). The control channel uses TCP port 245.

- d. ***What is the control-channel pre-shared key?***

Enter a pre-shared key (PSK) value to enable cryptographic protection of the service-chain control channel between the ingress and egress devices. You must enter exactly the same PSK value on both the ingress and egress devices. The PSK value must be a string of printable ASCII characters-- you may enter a passphrase or a text representation (such as hexadecimal or base64) of a binary key. Continue with Step 8.

2. **Which CA certificate shall SSL Intercept use?**

This question does not appear if you chose separate devices and are currently configuring the Egress device

Select the Certificate Authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections. You imported the CA certificate and private key 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.

Whenever you CHANGE the CA certificate, you must enter the passphrase (if any) that protects the private key.

3. **Which private key goes with the CA certificate?**

This question does not appear if you chose separate devices and are currently configuring the Egress device

Select the corresponding private key. Again, you either imported this using the Setup Wizard, or must manually import it.

4. **What is the private-key passphrase (if any)?**

This question does not appear if you chose separate devices and are currently configuring the Egress device

If applicable, type the private-key passphrase. If the key does not have a passphrase leave the field empty.

5. **How do you want to handle SSLv3 connections?**

This question does not appear if you chose separate devices and are currently configuring the Egress device

Choose how you want the system to handle connections made using SSLv3.

- **Reject all SSLv3 connections**

Select this option to have the system reject all SSLv3 connection attempts. This option is the most secure.

- **Treat SSLv3 just like TLS (enable interception)**

Select this option to have the system handle SSLv3 connection attempts the same way as TLS. This allows you to intercept these connections and send the decrypted contents through a service chain. It is important to note this does not make SSLv3 secure.

- **Treat SSLv3 as non-TLS for service-chain classification**

Select this option to have the system handle SSLv3 connection attempts like other non-TLS connections and send them to service chains chosen by TCP classifier rules. Note these connections are still encrypted and not intercepted.

6. **How do you want to handle SSLv2 connections?**

This question does not appear if you chose separate devices and are currently configuring the Egress device

Choose how you want the system to handle connections made using SSLv3. Note that SSLv2 is long obsolete and insecure, and these connections cannot be intercepted (decrypted) by this iApp.

- **Reject all SSLv2 connections**

Select this option to reject all SSLv2 connection attempts. This option is the most secure.

- **Treat SSLv2 as non-TLS for service-chain classification**

Select this option to have the system handle SSLv2 connection attempts like other non-TLS connections and send them to service chains chosen by TCP classifier rules. Note these connections are still encrypted and not intercepted.

7. **Do you want to enforce TLS secure renegotiation?**

This question does not appear if you chose separate devices and are currently configuring the Egress device

Choose whether you want to enforce TLS secure renegotiation. To avoid a serious TLS vulnerability, both client and server must use secure renegotiation per RFC5746. By default, when this solution detects an attempt to use insecure renegotiation it terminates the affected TLS session to avert loss of session security.

However, you may select to allow use of insecure TLS renegotiation to disable secure-renegotiation enforcement (thereby exposing affected TLS sessions to man-in-the-middle attacks). This may permit TLS sessions with obsolete servers and/or clients.

- **Require use of TLS secure renegotiation (RFC5746)**

Select this option to require the use of TLS secure renegotiation. This option is the most secure.

- **Allow use of insecure TLS renegotiation (not advised)**

Select this option if you want to allow insecure TLS renegotiation. This option is not recommended. This may permit TLS sessions with obsolete servers and/or clients.

8. ***Which IP address families do you want to support?***

Choose whether you want this configuration to support IPv4 addresses, IPv6 addresses, or both. If you do not choose to support both address families, you must configure IP addresses in the family you select for all IP address fields in this iApp. If you choose both IPv4 and IPv6, you can send intercepted IPv6 traffic through an IPv4 Layer 3 service device.

- **Support only IPv4**

Select this option if you want the BIG-IP system to only support IPv4 for this implementation and do not require IPv6 support.

- **Support only IPv6**

Select this option if you want the BIG-IP system to only support IPv6 for this implementation and do not require IPv4 support.

- **Support both IPv4 and IPv6**

Select this option if you want the iApp to support both IPv4 and IPv6.

9. ***Which proxy schemes do you want to implement?***

Choose whether you want the system to operate in transparent proxy mode, explicit proxy mode, or both.

- **Implement transparent proxy only**

Select this option if you want the system to operate in transparent proxy mode only. The transparent proxy scheme can intercept all types of TLS and TCP traffic. It can also process UDP traffic (see the following question), and forward all other types of traffic. The transparent proxy requires no client configuration modifications.

- a. ***Do you want to pass UDP traffic through the transparent proxy unexamined?***

By default, transparent-proxy mode manages TCP traffic but allows UDP traffic to pass through unexamined. You may choose to manage UDP as well as TCP traffic-- for example, to redirect QUIC web connections to HTTPS (so you can intercept them) or to send UDP traffic to a receive-only service.

- **No, manage UDP traffic via service-chain classification**

Select this option if you want to configure specific service chain classifier rules for UDP traffic. Selecting this option causes the section [UDP Service Chain Classifier Rules on page 37](#) to appear where you configure these service chain classifier rules.

- **Yes, pass all UDP traffic through unexamined**

Select this option if you want the system to pass UDP traffic through without inspecting it. In this case, the UDP service chain classifier rule section does not appear.

- b. ***Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?***

If you select to implement a transparent proxy, you can choose to pass non-TCP, non-UDP traffic through this solution unexamined or to block traffic that is not TCP or UDP. By default, transparent-proxy mode blocks all non-TCP/UDP traffic (for example, IPSec or SCTP).

- **No, block all non-TCP, non-UDP traffic (IPSec, SCTP, OSPF, etc.)**

Select this option if you want the system to block all non-TCP, non-UDP traffic.

- **Yes, pass non-TCP, non-UDP traffic (IPSec, SCTP, OSPF, etc.)**

Select this option if you want the system to pass all traffic that is not TCP or UDP. If you choose this option, this traffic will not be classified or processed by any service chain. Continue with question #6.

- **Implement both transparent and explicit proxies**

Select this option if you want the system to operate in explicit and transparent proxy modes simultaneously. If you select this option, you will see the following transparent proxy questions, and the section [Explicit Proxy Configuration on page 39](#) appears later in the template.

- a. ***Do you want to pass UDP traffic through the transparent proxy unexamined?***

By default, transparent-proxy mode manages TCP traffic but allows UDP traffic to pass through unexamined. You may choose to manage UDP as well as TCP traffic-- for example, to redirect QUIC web connections to HTTPS (so you can intercept them) or to send UDP traffic to a receive-only service.

- **No, manage UDP traffic via service-chain classification**

Select this option if you want to configure specific service chain classifier rules for UDP traffic. Selecting this option causes the section [UDP Service Chain Classifier Rules on page 37](#) to appear where you configure these service chain classifier rules.

- **Yes, pass all UDP traffic through unexamined**

Select this option if you want the system to pass UDP traffic through without inspecting it. In this case, the UDP service chain classifier rule section does not appear.

b. **Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?**

If you select to implement a transparent proxy, you can choose to pass non-TCP, non-UDP traffic through this solution unexamined or to block traffic that is not TCP or UDP. By default, transparent-proxy mode blocks all non-TCP/UDP traffic (for example, IPSec or SCTP).

- **No, block all non-TCP, non-UDP traffic (IPSec, SCTP, OSPF, etc.)**

Select this option if you want the system to block all non-TCP, non-UDP traffic.

- **Yes, pass non-TCP, non-UDP traffic (IPSec, SCTP, OSPF, etc.)**

Select this option if you want the system to pass all traffic that is not TCP or UDP. If you choose this option, this traffic will not be classified or processed by any service chain.

Continue with question #6.

- **Implement only explicit proxy**

Select this option if you want the system to operate in explicit proxy mode only. The explicit proxy scheme supports only HTTP(S) per RFC2616. If you choose to configure an explicit proxy you will assign a specific IP address and TCP port on which HTTP explicit-proxy clients will connect to it. If you choose this option, the section [Explicit Proxy Configuration on page 39](#) appears later in the template.

If you chose a single BIG-IP device to handle ingress and egress, or chose separate devices and that you are currently configuring the ingress device, continue with [In-line Services on page 23](#).

If you chose separate devices and you are currently configuring the egress device, continue with [Egress Device Configuration \(for the separate ingress and egress device scenario\) on page 46](#).

In-line Services

In this section you can configure the iApp for Layer 2 or Layer 3 in-line services. These services are used in diverse service chains you configure later in the template. In-line services pass traffic through one or more service (inspection) devices at Layer 2 (LAN) or Layer 3 (IP). Each service device communicates with the BIG-IP device (on the ingress side) over two VLANs called *Inward* and *Outward* which carry traffic toward the intranet and the Internet respectively. For more information, review [How to configure in-line services using the SSL Intercept iApp template on page 9](#).

i Important *If deploying the template for in-line services for the first time, you must complete the following two separate tasks:*

- *First, you must complete the following in the In-Line services area of the template:*
 - a. *Answer the questions as applicable until you get to the [What is the status of this service?](#) question. From that question, select one of the **Stage 1** options and then complete the rest of the questions that appear in the in-line services section.*
 - b. *After you configure the VLANs in the In-Line Services section, click the **Finished** button at the bottom of the template without completing the rest of the template.*
 - c. *If you are using more than one standalone BIG-IP device, after you click **Finished**, you must synchronize the BIG-IP configuration to the other device in the ingress device group (see [Synchronizing the BIG-IP configuration on page 50](#) for guidance).*
 - d. *Repeat each step in this task for all ingress devices in the Sync-Failover group.*
- *Second, after configuring all VLAN information on **both** devices and synchronizing the configuration, use the Reconfigure option to open run this iApp again on just one device in the ingress-device Sync-Failover group.*

In the In-line services section, select one of the Stage 2 options for each in-line service you configured, and then complete the rest of the in-line services section. After completing the in-line services, complete the rest of the template as applicable.

After deploying the template, if you want to add more in-line services at a later time and reconfigure the template, you must again update the in-line service configuration on all devices, and then synchronize the configuration again.

Return to [How to configure in-line services using the SSL Intercept iApp template on page 9](#) for more information and a flow diagram.

If you do not have any in-line services you want to be a part of this configuration, continue with [Receive-Only Services on page 29](#).

1. **How many in-line services do you want to configure?**

Select the total number of in-line services (Layer 2 and Layer 3) you want to set up (not counting any services in the decrypt zone if deploying separate ingress and egress devices). In-line services do not include receive-only and/or ICAP services, those services are configured later.

You can select up to 10 in-line services in this configuration.

2. **Do you want to replace in-line service subnet block(s)?**

*This question only appears if the number of in-line services in the first question is set to **None***

Choose whether or not you want to replace the service-network subnet block(s). The IP subnets and addresses for in-line services are assigned by this iApp and must be used by all configured in-line service devices. You can change the base address of each address block (IPv4 or IPv6) from which subnets and addresses are assigned if necessary, but only **before** configuring in-line services. However, changing an address block has several implications and must be done carefully, and is not recommended or supported.

⚠ Warning *Replacing the service-network subnet blocks is NOT recommended and NOT SUPPORTED by F5. Only use this option if you have a specific need and understand the consequences.*

The IP subnets assigned to Inward and Outward VLAN pairs for in-line services must not collide with any intranet (local/private) or Internet (remote/public) IP addresses. Those subnets are allocated from an IPv4 CIDR /19 block (which allows for thirty-two /24 subnets) and/or an IPv6 /48 prefix block.

For IPv4, F5 recommends the block 198.19.0.0/19 to minimize the likelihood of address collisions. For IPv6, F5 recommends the prefix fd06:4d61:1::/48. If you insist upon replacing this block, we suggest you choose a distinct ULA (RFC 4193) prefix.

- **No, use standard subnet block(s) recommended by F5**
Select this option if you want to use the standard subnet blocks recommended by F5. No further information is required.
- **Yes, replace standard subnet block(s) (NO F5 SUPPORT)**
Select this option if you want to replace the standard subnet block(s). As noted, this option is not supported by F5 Networks, use at your own risk.

If you replace a standard subnet block you assume responsibility for translating addresses shown in this iApp template for configuring Layer 3 in-line services. That is straightforward for IPv6 addresses-- just replace the first three hextets. For IPv4 addresses you must replace the first two octets, then for the third octet, substitute the sum of the third octets of your base value and the value shown in the iApp template. Besides address translation, you also assume full responsibility for any address collisions or routing problems.

a. What is the IPv4 (CIDR /19) subnet-block base address?

Enter the IPv4 base address of a CIDR /19 block (it will look like X.Y.Z.0 where X is 1-223, Y is 0-255, and Z is 0-224). The default value is 198.19.0.0 (recommended by F5).

b. What is the IPv6 /48 subnet-block prefix?

Enter an IPv6 /48 prefix (it will look like X:Y:Z:: where X, Y, and Z are each 1-4 hexadecimal digits, and X should probably start with 'fd'). The default value is fd06:4d61:1:: (recommended by F5).

3. Should Layer 3 service devices see real client IP:port?

Choose whether layer 3 service devices should see the real client IP and port. As an SSL Intercept connection is sent through a Layer 3 in-line service, an IP alias (from a block of SNAT addresses on the Inward subnet) may optionally be substituted for the real client IP address (naturally, the real address is restored after the connection passes through the service). Aliasing client addresses lets service devices recognize traffic coming from SSL Intercept in order to apply specific security or routing policies to it.

When you do not want to alias client IP you must choose whether to (a) keep client IP but allow occasional port aliasing, or (b) keep client IP and port always--but at the price of failing some connections when the desired IP:port is not available (due to TCP protocol TIME_WAIT state, or to the way BIG-IP CMP works).

- **No. Alias client IP to distinctive IP range**
Select this option if you want the system to alias the client IP address to a distinct range of IP addresses.
- **Mostly. Keep client IP but sometimes alias client port**
Select this option if you want the system to keep the client IP address and the port when possible. The BIG-IP uses a different source port when a client re-uses a TCP source port before the TIME_WAIT state has elapsed. The BIG-IP may also need to change the source TCP port to enable F5 Clustered Multiprocessing for performance reasons.
- **Always. Keep client IP:port-- but fail some connections**
Select this option if you want the layer 3 service devices to see the real client IP and port at all times. This means that some connections may fail if the port is unavailable (due to TIME_WAIT, etc). This is not a permanent failure, the client can attempt the connection again and the connection may succeed.

4. May in-line service devices initiate their own network traffic via Outward VLANs?

Choose whether in-line service devices can initiate their own network traffic using the outward VLANs. Normally all network traffic reaching an SSL Intercept ingress device via an outward VLAN/subnet is part of a service-chain connection. For security, SSL Intercept usually rejects unrecognized traffic trying to leave an outward VLAN using the ingress device as a gateway. However, you may choose to allow in-line service devices to connect to remote network resources through the ingress device.

- **No. Reject non-service-chain traffic leaving Outward VLANs**
Select this default option if you want the system to reject all traffic leaving the outward VLANs that is not part of a service chain.
- **Yes. Let service devices initiate outbound network traffic**
Select this option if you want to let in-line service devices initiate outbound network traffic. Note that the source IP address for such traffic must be that of a service device on the Outward subnet. You may have to add IP routes for Outward subnets-- pointing to the ingress device-- to the SSL Intercept egress device (if any) and/or to your network infrastructure.


5. **How many units are in the INGRESS sync/failover device group?**

Select the number of BIG-IP devices that are in your ingress Sync-Failover device group. For this configuration, you can have a maximum of two BIG-IP devices in a device group.

- **1 unit: standalone BIG-IP device**
Select this option if you only have a single BIG-IP device for Ingress traffic.
- **2 units: BIG-IPs in a Sync-Failover device group (HA pair)**
Select this option if you have two BIG-IP devices in the sync/failover device group. This is a traditional high availability (HA) pair.

6. **What is the unit number you want to use for this device?**

Choose the unit number you want to assign to this BIG-IP device.

 **Note:** This unit number is only used for identification purposes in this iApp and is not an existing unit identifier or used outside the iApp.

For example, if you have two devices in your device service cluster for high availability, assign unit ID **1** to the first device. When you are configuring this iApp on the other device in the cluster, assign that device unit ID **2**.

7. **What is THIS unit's management-port IP address?**

Type the IP address for management port for the device you are configuring.

The next task is to configure perform the in-line service(s) configuration for each service you specified in question #1.


• **In-line Service 1**

Complete the following for each in-line service.

As noted in the template, each in-line service has an Inward and Outward VLAN. Each Inward and Outward VLAN must be connected to the same Layer 2 virtual network from both devices in the Sync-Failover group. Inward and Outward VLANs on different BIG-IP devices may use different interfaces to connect to the same Layer 2 virtual networks.

a. **What type of service is this?**

Select the type of service you want to configure. Note that both Layer 2 and Layer 3 services have two options, Stage 1 or Stage 2. Select Stage 1 when you are configuring a service for the first time to add VLAN information, or if you want to take the service out of the configuration without deleting it. Only select Stage 2 when you have completed Stage 1, saved the template, and then synchronized the configuration. The unconfigured option will delete the service once you submit the template by clicking Finished.

 **Important** If you are using this iApp for the first time or configuring a new in-line service, in order to configure the system for in-line services, you must first select the Stage 1 option for the appropriate service type in order to complete the VLAN information.

• **Unconfigured (or delete existing service when I click Finished)**

Select this option if you want to remove the service from the iApp configuration. When you select this option, the service is permanently deleted when you click the **Finished** button on the iApp template. This option differs from the Stage 1 options because while unconfigured services are deleted when submitting the template, Stage 1 services cannot be added to a service chain, but are not deleted when you submit the template.

• **Stage 1: Configure VLANs for Layer 2 (bump in the wire)**

Select this option if you are initially configuring a Layer 2 bump in the wire service. Once you select this option, the following questions appear about the name of the service, and load balancing and VLAN information for the service. When you select this option, the service cannot (yet) be added to any service chain you configure later, but it exists in the iApp configuration and will not be deleted.

a. **What is the name of this service?**

Type a short, unique name for this service. You use this name when you change the service type to Stage 2, and also when you create service chains later in this iApp. This name can contain 1-15 alphanumeric or underscore characters, but must start with a letter. Letters are not case-sensitive.

b. **How many Layer 2 service devices are there?**

Select the number of Layer 2 service you want to be a part of this configuration. This information is used for load balancing traffic to the Layer 2 devices. The system can load balance traffic to up to eight Layer 2 service (inspection) devices for each one of the in-line services you are configuring.

If the Layer 2 devices do not have the same specifications, you can adjust the load balancing traffic ratios when you enter the VLAN information in the next question. This allows you to send a higher percentage of traffic to higher-powered device(s).

c. ***What are the L2 service device VLANs and load balancing ratios?***

Type the Layer 2 service device VLANs and load balancing ratio for each of the devices you specified in the previous question. Click the **Add** button to include more rows. The number of rows **must match** the number you selected in question b.

Ratio


If you choose to use the **Ratio** field, the BIG-IP system distributes connections among pool members in a static rotation according to ratio weights that you define. In this case, the number of connections that each system receives over time is proportionate to the ratio weight you defined for each pool member or node. This number must be between 1-100.

For example, if you have five devices and you assign a ratio of **1** to the first three devices, and a ratio of **2** to the fourth device, and a ratio of **3** to the fifth device; the first three devices with a ratio of 1 each receive 1/8 of the traffic. The fourth device receives 1/4 of the traffic, and the fifth device receives 3/8 of the traffic.

VLANs

For each VLAN pair you must specify the BIG-IP interface and VLAN tag (if any; 0 means untagged) each VLAN will use. On BIG-IP VE (Virtual Edition) the Inward and Outward VLANs for any particular Layer 2 service device **MUST** use different interfaces (to avert MAC address collisions).

Keep track of the order in which you add VLAN pairs for specific service devices. When you add Inward/Outward VLAN pairs for those service devices to the other BIG-IP devices in the Sync-Failover group, add them in the same order. You should also assign the same load balancing ratio to each service device on all of the BIG-IP devices in the Sync-Failover group.

 **Critical** *Once you have completed all of the in-line services for a new in-line service (including any Layer 3 services), you must click Finished on the iApp. If you are using more than a single, standalone BIG-IP system, you must synchronize the configuration across all the devices in the Sync-Failover group before continuing.*

• **Stage 1: Configure VLANs for Layer 3 (IP gateway)**

Select this option if you are initially configuring a Layer 3 IP gateway service. Once you select this option, the following questions appear about the name of the service and VLAN information. When you select this option, the service cannot (yet) be added to any service chain you configure later, but it exists in the iApp configuration and will not be deleted.


a. ***What is the name of this service?***

Type a short, unique name for this service. You use this name when you create service chains later in this iApp. This name can contain 1-15 alphanumeric or underscore characters, but must start with a letter. Letters are not case-sensitive.

VLANs

For each VLAN pair you must specify the BIG-IP interface and VLAN tag (if any; 0 means untagged) each VLAN will use. On BIG-IP VE (Virtual Edition) the Inward and Outward VLANs for any particular Layer 2 service device **MUST** use different interfaces (to avert MAC address collisions).

Each Inward VLAN must be connected to the same Layer 2 virtual network from every device in the Sync-Failover Device Group— and each Outward VLAN likewise, but to a distinct Layer 2 virtual network. Inward and Outward VLANs on different BIG-IP devices may use different interfaces and even tags (with external bridging) to connect to the same Layer 2 virtual networks.

 **Critical** *Once you have completed all of the in-line services for a new in-line service (including any Layer 2 services), you must click Finished on the iApp. If you are using more than a single, standalone BIG-IP system, you must synchronize the configuration across both the devices in the Sync-Failover group before continuing.*

• **Stage 2: Finalize Layer 2 (bump in the wire) configuration**

Select this option when you are ready to include your Layer 2 in-line services in a service chain(s). Only select this option when you have finished the Layer 2 [Stage 1](#) questions and synchronized the configuration.

Note that each Layer 2 service (inspection) device must transfer packets between its Inward and Outward VLANs. Packets will be sourced from various MAC's on each VLAN and destined for MAC's on the other (a Layer 2 device logically resembles a bridge).

a. What is the name of this service?

Type the same name you used for the Layer 2 in-line service in the Stage 1 section step a.

This name must be exactly the same you gave the service in the Stage 1 section.

b. Should service failure block connections?

Choose whether the BIG-IP system, in the event of a failure of all the devices in this service, should block connections or just let them skip this service and send it to the next service in the chain.

You must answer this question because when none of the service (inspection) devices for a service is working, connections reaching it (as one link in a service chain) cannot be processed normally.

Note: *Either action is taken only once for each connection, so if a long-lived connection is allowed to skip a service which is offline (because all of its service devices are down at the moment it begins) none of the packets for that connection will ever go through the service, even if it comes back online later.*

- **No. When service is down let connections skip it**

Select this option to allow connections to skip the service you are configuring if all the devices in the service are unavailable. If you select this option, the system excludes this service from the connection's service chain, and the connection goes to the next service in the chain.

- **Yes. Reject connections when service is down**

Select this option if the system should reject every connection reaching this service when the service is down.

c. Do you want to run all apparent HTTP traffic through one TCP port?

Select whether you want the system to use the original destination port, or to send all traffic that appears to be HTTP through one TCP port (the original destination port is restored after). This question is necessary because some service (inspection) devices do not recognize and analyze HTTP protocol streams on non-standard ports.

- **No. Connections use original ports (like 443, though decrypted)**

Select this option if the connections should use their original destination ports.

- **Yes. Send all apparent HTTP traffic via port 80**

Select this option if all HTTP traffic should be sent via port 80. The original destination port is restored by the BIG-IP system afterwards.

- **Yes. Send all apparent HTTP traffic via port 8080**

Select this option if all HTTP traffic should be sent via port 8080. The original destination port is restored by the BIG-IP system afterwards.

- **Yes. Send all apparent HTTP traffic via port 8443**

Select this option if all HTTP traffic should be sent via port 8443. The original destination port is restored by the BIG-IP system afterwards.

- **Stage 2: Finalize Layer 3 (IP Gateway) configuration**

Select this option when you are ready to complete your Layer 3 in-line services for use in service chain(s). Only select this option when you have finished the Layer 3 *Stage 1* questions and synchronized the configuration.

Select this option if you are configuring a Layer 3 service. Layer 3 service (inspection) devices for this service must be dual- or quad-homed on the Inward (**198.19.x.0/25** and/or **fd06:4d61:1:x::/121**) and Outward (**198.19.x.128/25** and/or **fd06:4d61:1:x::128/121**) subnets. Each must forward outbound-to-the-Internet traffic to the Outward-subnet gateway(s) **198.19.x.245** and/or **fd06:4d61:1:x::f5**. Traffic inbound-to-the-intranet must be delivered to source addresses (SNAT's-- **198.19.x.{32-47}** and/or **fd06:4d61:1:x::{20-2f}**) on the Inward subnet or else routed to the Inward-subnet gateway(s) **198.19.x.10** and/or **fd06:4d61:1:x::a**.

a. Select available devices

Select the IP-address pairs of the Layer 3 devices which support this service. For example, if you choose **198.19.1.64 (164)** you must configure a Layer 3 service device to use the IP address **198.19.1.64/25** on the Inward VLAN/subnet and **198.19.1.164/25** on the Outward VLAN/subnet. Layer 3 service devices must behave as routers or transparent proxies. If you configure multiple devices traffic will be load balanced through them.

b. Should service failure block connections?

Choose whether the BIG-IP system, in the event of a failure of all the devices in this service, should block connections or just let them skip this service and send it to the next service in the chain.

You must answer this question because when none of the service (inspection) devices for a service is working, connections reaching it (as one link in a service chain) cannot be processed normally.

➡ **Note:** *Either action is taken only once for each connection, so if a long-lived connection is allowed to skip a service which is offline (because all of its service devices are down at the moment it begins) none of the packets for that connection will ever go through the service, even if it comes back online later.*

- **No. When this service is down let connections skip it**
Select this option to allow connections to skip the service you are configuring if all the devices in the service are unavailable. If you select this option, the system excludes this service from the connection's service chain, and the connection goes to the next service in the chain.
- **Yes. Reject connections when this service is down**
Select this option if you want the system to reject every connection reaching this service when the service is down.

c. ***Do you want to run all apparent HTTP traffic through one TCP port?***

Select whether you want the system to use the original destination port, or to send all traffic that appears to be HTTP through one TCP port (the original destination port is restored after). This question appears because some service (inspection) devices do not recognize and analyze HTTP protocol streams on non-standard ports.

- **No. Connections use original ports (like 443, though decrypted)**
Select this option if the connections should use their original destination ports.
- **Yes. Send all apparent HTTP traffic via port 80**
Select this option if all HTTP traffic should be sent via port 80. The original destination port is restored by the BIG-IP system afterwards.
- **Yes. Send all apparent HTTP traffic via port 8080**
Select this option if all HTTP traffic should be sent via port 8080. The original destination port is restored by the BIG-IP system afterwards.
- **Yes. Send all apparent HTTP traffic via port 8443**
Select this option if all HTTP traffic should be sent via port 8443. The original destination port is restored by the BIG-IP system afterwards.

Return to [In-line Service 1 on page 25](#) to repeat this procedure for each of the in-line services you specified.

i Important *Remember, if you just finished configuring Stage 1 for in-line services, you must click Finished.*

If you are using more than a single, standalone BIG-IP device, you must repeat this section on each in the Sync-Failover device group (the Ingress Sync-Failover group if using separate ingress/egress devices). After completing the Stage 1 configuration on all ingress devices, synchronize the configuration (see [Synchronizing the BIG-IP configuration on page 50](#)), before returning to select an Stage 2 service type and then completing the in-line service configuration.

If you are using a standalone BIG-IP device, after clicking Finished, simply re-enter the template using the Reconfigure option (click iApps > Application Services > name you gave the iApp > Reconfigure (on the Menu bar)), and then configure Stage 2.

Receive-Only Services

In this section, you configure any receive-only device(s) that are a part of this configuration. Receive-only services only receive traffic for inspection, and do not send it back to the BIG-IP system. Each receive-only service provides a packet-by-packet copy of the traffic (e.g., plaintext) passing through it to an inspection device. This is done by replacing the MAC address in every copied packet with the MAC address of the service/inspection device.

i Important *If you choose to use Receive-Only services and are using more than a single, standalone BIG-IP system (two devices in a Sync-Failover group) only:*

After you click Finished on the device you are currently configuring, synchronize the configuration. On the other device in the Sync-Failover group you must use the Reconfigure option (click iApps > Application Services > name you gave the iApp > Reconfigure (on the menu bar)), and then click Finished (even if you do not make any other changes) in order for the iApp to install the non-floating configuration for Receive-Only services on each device.

If you do not have any receive-only devices you want to be a part of this configuration, continue with [ICAP Services on page 30](#).

1. **How many receive-only services do you want to configure?**

Select the total number of receive-only services you want to be a part of this configuration. You can select up to 10 services.

• **Receive-Only Service 1**

For each receive-only service you specified in question #1, you must complete the following.

a. **What is the name of this service?**

Type a short, unique name for this service. You use this name when you create service chains later in this iApp. This name can contain 1-15 alphanumeric or underscore characters, but must start with a letter. Letters are not case-sensitive.

b. **What is the inspection device's MAC address?**

Type the MAC address of the receive-only device. This address must be reachable (bridged) via a BIG-IP VLAN (such as **internal**).

c. **On which network is the device located?**

Specify the network (VLAN and Interface) for each receive-only device you are configuring.

• **VLAN**

Select the VLAN on which the receive-only device resides.

• **Interface**

Select the associated BIG-IP interface.

d. **What is the nominal IP address for this device?**

Type the nominal IP address for this device. You must assign a nominal IP (host) address to each receive-only device to identify it inside the BIG-IP system. That address must be homed on the same subnet as one (any one) of the BIG-IP's Self IP addresses.

i Important *The receive-only device does NOT have to recognize or use the nominal IP address. The nominal IP address 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.*

• **Repeat for each receive-only service you want to use in this deployment**

Configure each of the receive-only services using the appropriate information for that service.

This completes the Receive-only service configuration. Continue with [ICAP Services on page 30](#).

ICAP Services

In this section, you configure the ICAP (Internet Content Adaptation Protocol) services that are a part of this configuration. Each ICAP service uses the ICAP (RFC3507) protocol to refer HTTP traffic to one or more Content Adaptation device(s) for inspection and possible modification.

If you do not have any ICAP services you want to be a part of this configuration, continue with [Service Chains on page 33](#).

1. How many ICAP services do you want to configure?

Choose the number of ICAP services you want to configure as a part of this implementation. You can define up to 10 ICAP services. Note that you can add an ICAP service to any TCP service chain, but only HTTP traffic is sent to it, because ICAP does not support UDP.

• **ICAP Service 1**

For each ICAP service you specified in question #1, you must complete the following.

a. What is the name of this service?

Type a short, unique name for this service. You use this name when you create service chains later in this iApp. This name can contain 1-15 alphanumeric or underscore characters, but must start with a letter. Letters are not case-sensitive.

b. Which ICAP device(s) will inspect HTTP requests for this service?

Specify a unique IP address and the port for each receive-only service you are configuring. If you add more than one ICAP device, they become part of a BIG-IP load balancing pool with a TCP health monitor attached to each device.

• **IP address**

Type the IP address of one of your ICAP devices.

• **ICAP Port**

Type the port your ICAP service is using (if different from 1344, the default).

Click **Add** to include more services.

c. Do you want to use OneConnect to these ICAP servers?

Choose whether or not you want to use the OneConnect feature for the ICAP servers. The F5 OneConnect profile improves performance by reusing TCP connections to ICAP servers to process multiple transactions.

If your ICAP servers do not support multiple ICAP transactions per TCP connection, select **No** to disable OneConnect. See <https://support.f5.com/kb/en-us/solutions/public/7000/200/sol7208.html> for more information on OneConnect.

d. What is the ICAP Request processing URI?

Type the ICAP request and response URIs (as defined by RFC3507) that are applicable for your ICAP server for example, **icap://icap.example.net/antivirus**). Consult your ICAP server documentation for specific information about the Request and Response processing URIs.

You can place the macros `${SERVER_IP}` and `${SERVER_PORT}` into a URI (for example,

icap://\${SERVER_IP}:\${SERVER_PORT}/REQMOD) and they will be replaced with the IP address and port of the specific ICAP server chosen to handle a particular transaction.

e. What is the ICAP Response processing URI?

Type the ICAP Response processing URI for this service. Consult your ICAP server documentation for specific information about the Request and Response processing URIs.

f. Do you want to edit headers?

Choose whether or not you want the BIG-IP system to edit the headers with information you specify (you can find general information on ICAP headers in RFC 3507 section 4.3). Consult your ICAP server documentation for specific information.

• **No, I do not want to edit the headers**

Select this option if you do not want to edit the headers.

• **Yes, I want to edit the headers**

Select this option if you want edit the headers, and then answer all of the following questions.

a. What is the ICAP Host header value?

Type an IP address (or FQDN) for the **Host: ICAP** header.

b. What is the ICAP Referer header value?

Type a value for the **Referer: ICAP** header.

c. What is the ICAP User-Agent header value?

Type a value for the **User-Agent: ICAP** header.

d. What is the ICAP From header value?

Type a value for the **From: ICAP** header.

g. What is the maximum length in bytes of the ICAP preview?

Type the number of bytes you want to use as the maximum length for the ICAP preview. Bytes of content up to the specified number are sent to the ICAP server as a preview of each HTTP request or response. If you set the maximum preview length to zero (0), then requests and responses are streamed through the ICAP server. The largest value currently supported is 51200 (50KB).

h. How should ICAP server unavailability/failure be handled?

Choose how you want the system to handle times when an ICAP server has failed or is otherwise unavailable.

- **Let request/response go to next service in chain**

Select this option if you want the system to let the request/response continue to the next service in the service chain.

- **Reset connection to client (discard request/response)**

Select this option if you want the system to reset the connection to the client, discarding the request/response.

i. Do you want to send HTTP 1.0 requests to ICAP?

Choose whether you want the BIG-IP system to send only HTTP/1.1 requests to the ICAP servers, or if the system should send both HTTP/1.1 and HTTP/1.0 request to the ICAP servers. If you select only HTTP/1.1 requests are sent, then HTTP/1.0 requests are not inspected, and are forwarded along to the next device in the chain.

- **No, send only HTTP/1.1 requests to ICAP**

Select this option if you only want to send HTTP/1.1 requests to the ICAP service. Any HTTP/1.0 requests are not inspected.

- **Yes, send HTTP/1.0 as well as HTTP/1.1 requests to ICAP**

Select this option if you want to send both HTTP/1.1 and HTTP/1.0 requests to the ICAP service.

- **Repeat for each ICAP service you want to use in this deployment**

Configure each of the ICAP services using the appropriate information for that service.

This completes the ICAP services configuration. Continue with [Metrics Collector Services on page 32](#).

Metrics Collector Services


Metrics Collector services accumulate statistical information (such as bytes transferred) whenever they are placed in service chains. These services are internal to the SSL intercept configuration; they do not modify or scan data in connections. For these collectors, you only need to specify a name for the metric collector service(s) you want to include.

You can review the statistics accumulated by a metrics-collector service in the BIG-IP Configuration utility. Click **Local Traffic > Virtual Servers > Name of the virtual server associated with a metrics collector service > Statistics** (on the menu bar). The name of each metrics collector service appears in the **Description** field of its virtual server. You may also investigate statistical data using TMSH or SNMP.

1. *What is the name of your Metric Collector service(s)?*

Type a name for the Metric Collector service. Like the other names in this deployment, you are limited to 15 characters.

If you want to include more metric collectors, click the **Add** button and a new row appears. You can add any given metrics collector service to more than one service chain if you want.

 **Note:** *Metrics Collector services are an Early Access feature and may change or not be present in future versions of this solution.*

Continue with [Service Chains on page 33](#).

Archived

Service Chains


In this section, you configure service chains using the services you defined in the previous sections. The service chains comprise a list of the services you configured, and then the Service Chain Classifier Rules (which you configure in the next section) determine which of these service chains receive traffic.

1. **Service Chains**

Use this section to configure the SSL Intercept service chains.

- **Chain name**

Type a short name for this service chain. A service chain name may contain 1-15 alphanumeric or underscore characters and must start with a letter (not case-sensitive). Use spaces or commas to separate service names.

 **Important** *You cannot use any of the keywords 'all', 'bypass', 'reject', or 'drop', nor the name of any (inspection) service you previously configured in this iApp as a service chain name.*

- **Service List**

Type the names of the services (in-line, receive-only, and/or ICAP) you defined in the iApp.

For example, if you used the iApp to configure two services that process HTTP traffic, one you named **DLP** and the other you named **AUP**, you might define a service chain with the Chain Name **web** and with the Service List **AUP, DLP** which would first check URL's against your Acceptable Use Policy, and then monitor web requests for sensitive data exfiltration. You do not have to specify the decryption and re-encryption functions in this list – they bookend every chain.

Click the **Add** button to create additional service chains.

Some things to keep in mind while configuring Service chains:

- Services cannot be used twice in the same service chain,
- Services can be used in multiple chains,
- Not all services must be used,
- The order of the services in the chain is the order in which the traffic will pass through the services,
- If present, devices in the decrypt zone will see traffic after all services,
- Returning traffic will pass through the services in the reverse order.

This completes the service chain configuration. Next, you configure the Service Chain classifier rules that determine which of the service chains you just configured receive traffic. Continue with [TCP Service Chain Classifier Rules on page 34](#).

TCP Service Chain Classifier Rules

In this section, you configure the TCP service chain classifiers. Each service chain classifier rule chooses the specified chain to process ingress connections. Different classifier rules may send connections to the same chain.

Each classifier has three filters. The filters match source (client) IP address, destination (which can be IP address, IP Intelligence category, IP geolocation, domain name, domain URL Filtering category, or server TCP port), and application protocol (based on TCP port or protocol detection). Filters can overlap (for example, you might wish connections from a special subnet 10.20.111.0/24 to traverse service chain 'C_Suite' while sending connections from the enclosing subnet range 10.20.0.0/16 via service chain 'HQ') so the solution chooses the classifier rule which best matches each connection.

For detailed information of the settings in this section, see [Understanding Service Chain Classification on page 52](#).

Using BIG-IP Data Groups to match IP address, domain names, geolocations, or IPI/URL filtering categories (optional)

To match IP addresses, domain names, geolocations, or IPI/URL Filtering categories against the contents of data groups (which you configure and maintain outside this iApp), insert the special match target **@DG** where **DG** is the name of a data group, such as **/Common/IPIlist**. The name (or IP address) of each record in the data group is the match target. For **@DG** domain-name matching only, you can append an exclamation point (!) to a record name to indicate suffix-match instead of exact match. For example, the record name **F5.COM** would NOT match destination **www.f5.com** but **.F5.COM!** would. Use leading dots (.) to avert errors like **F5.COM!** matching **www.not-f5.com**.)

Each record's value is empty, or for Dst matches (only) is optionally a keyword or service-chain name as explained below. When you use **@DG** syntax to match destinations against a data group, the chain name in the classifier rule becomes a default which you can override by setting the data-group value for any particular match in the data group to a chain name or keyword.

For specific information on configuring data groups on the BIG-IP system (**Local Traffic > iRules > Data Group list**), see the BIG-IP documentation or the Help tab on the Data Group List page.

Using the @pinners data group

The special domain-name matching data group **@pinners** (for use in classifier rules) contains a list of domain names. They are the domain names of some TLS- (SSL-) based services from well-known businesses like Microsoft that support software (such as Microsoft Update) which may not work well when their connections are intercepted and decrypted by the SSL Intercept solution. They are called *pinners* because they all "pin" the PKI certificates they will trust to those signed by specific CA's (that is, not the locally-trusted CA used by the F5 SSL Intercept solution).

F5 provides an initial list of pinners, which you may view in the BIG-IP Configuration utility by clicking **Local Traffic > iRules > Data Group List**, and then **<iapp name>-pinners**.

You may edit the list, for example, to add more domain names. Note the syntax for suffix matching: to match all domain names ending in **.xyz.com**, you enter **".xyz.com!"**— the exclamation point at the end of the domain name requests suffix matching instead of simple matching.

If you edit the list, then the SSL Intercept iApp will NOT update it any more, even if you reconfigure the iApp template and clicked Finished, UNLESS you delete the whole data group or delete all the names in it. If the data group is missing or empty, when you reconfigure the iApp, the iApp will recreate it with the initial list of pinner domain names provide by F5.

1. Service Chain Classifier Rules

Specify service chain classifier rules using the following guidance. If more than one classifier matches a connection, the best-matching classifier determines the service chain for that connection (so the order of classifier rules in the list is not important). Classifiers can also reject a connection or let it bypass the service chain (bypass TLS interception). The default action applies to connections which do not match any classifier. See [Understanding Service Chain Classification on page 52](#) for a detailed description of the following settings.

- **Phase**

Choose which Phase you want for this classifier. The options are Normal, No TLS, Pre-handshake, and TLS handshake.

- » **Normal**

When Match Phase is **Normal** the rule may match TLS connections at TLS handshake time and possibly again-- more specifically-- after SSL Intercept 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).

- » **No TLS**
If you select this Phase, the rules match only non-TLS traffic.
- » **Pre-handshake**
Pre-handshake rules match BEFORE any TLS handshake, which means they can allow a connection to bypass SSL Inspection completely-- not even trying to learn the real name of the remote server. All DDB rules (see below) must have Phase set to **Pre-handshake**.
- » **TLS handshake**
TLS handshake rules match only at TLS handshake time-- they never match non-TLS traffic and they are not checked again after the plaintext of a TLS connection becomes available.

- **Src**

The **Src** (source) filter is one or more IP subnet or host addresses. If the source IP of an ingress connection matches an address in the **Src** filter, the other filters will be checked. Using ***** means all-addresses; **@DG** includes addresses from a Data Group (see description earlier in this section). Specify source addresses as prefix/mask-length (CIDR format) like 203.0.113.0/24 or fd5:f:5:cc0f::/64 (to specify a single host omit the mask-length, like 203.0.113.55). Use spaces or commas to separate multiple filter items.

- **Mode**

Choose the mode you want to use for this classifier rule. The mode you choose determines the value you will use for the **Dst** (destination). You can choose one of the following modes for each classifier rule:

- » **Addr**

If you select **Addr** (address(es)), the **Dst** filter you will configure consists of one or more IP subnet or host addresses just like the **Src** filter.

- » **Geo**

If you select **Geo** (geolocation), the **Dst** you will configure contains 2-letter country and 3-letter continent codes against which the IP Geolocation of the destination server is compared. The continent codes are: **CAF**=Africa, **CAN**=Antarctica, **CAS**=Asia, **CEU**=Europe, **CNA**=North America, **COC**=Oceania, **CSA**=South. The country codes are those of ISO 3166 alpha-2.

- » **IPI**

If you select **IPI** (IP inspection), the **Dst** you will configure contains one or more IP Intelligence categories against which the destination IP address's reputation is matched. You must replace SPACE characters in names of IP Intelligence categories with underscores (**_**) before adding them to **Dst**. While you must have an IP Intelligence license to use this functionality, the iApp will not display an error if you do not, this classifier rule will just not match any connections.

- » **DDB**

If you select **DDB** (Dynamic Domain Bypass), the **Dst** you will configure contains one or more DNS domain names (unique or wildcard) against which the destination hostname indicated by the client in TLS SNI is matched. This mode is special because it classifies traffic before the SSL Intercept solution attempts any TLS handshake with the remote server (that is, in Match Phase 'Pre-handshake'). You may use DDB to whitelist and bypass traffic to servers which cause TLS handshake problems or that require TLS mutual (client-certificate/smart-card) authentication. For DDB, the **Chain** value you will select MUST be **bypass** or **reject**. For DDB only, the tilde symbol (~) matches an empty/missing hostname.

For security, the DDB facility ensures the destination IP address for each bypassed connection corresponds to the allowed domain. DDB may replace the destination IP address supplied by the client with one freshly obtained from DNS. See [Dynamic Domain Bypass on page 55](#) for more information.

- » **Name**

If you select **Name** (domain name), the **Dst** you will configure contains one or more DNS domain names (unique or wildcard) against which the connection's destination hostname is matched.

- » **URLF**

If you select **URLF** (URL Filtering), the **Dst** you will configure is one or more URL Filtering categories against which the URL categorization of the destination server is compared. You must replace SPACE characters in names of URL Filtering categories with underscores (**_**) before adding them to **Dst**. While you must have an URL Filtering license to use this functionality, the iApp will not display an error if you do not. Instead this classifier rule will just not match any connections. See [Optional URL filtering on page 56](#) for instructions on updating the database and other useful information.

» **Port**

If you select **Port** for the mode, the **Proto** value must be **Any**. For Port, Dst contains one or more TCP port numbers or ranges like 5557-5559 (use 0 or * to match all) against which the destination port number is matched. The main use of this mode is to control non-TLS traffic such as SSH. Again, if you select Port, the **Proto** value MUST be **Any**.

• **Dst**

Dst is destination of the connection. The value of this field is based on the selection you made for the **Mode** (descriptions are found in each mode listed above). If applicable, specify definition addresses as prefix/mask-length (CIDR format) like 203.0.113.0/24 or fd5:f:5:cc0f::/64 (to specify a single host omit the mask-length, like 203.0.113.55). Use spaces or commas to separate multiple filter items. You must replace SPACE characters in names of IP Intelligence and URL Filtering categories with underscores (_) when adding them to Dst.

• **Proto**

The **Proto** (protocol) value specifies the protocol of the connection (based on port or protocol recognition). You can specify one of the following protocols:

» **Any**

Select this option if you want to allow all protocols for this classifier rule.

» **HTTP**

Select this option if you want to limit the protocol for this classifier rule to HTTP.

» **Mail**

Select this option if you want to limit the classifier rule to the standard ports for SMTP, IMAP, and POP, plus SMTP protocol recognition.

» **SSLv2/3**

Select this option if you want the rule to match only when SSLv2 and/or SSLv3 connections are treated as non-TLS.

» **Other**

Select this option if you want to limit the classifier rule to all other protocols except HTTP and Mail (SMTP, IMAP, and POP).

• **Chain**

Type the name of the Service Chain you configured that you want to use for this classifier rule. This must be the name you gave a service chain **or** a special keyword: **all**, **bypass**, or **reject**. **All** means a chain including all services-- first receive-only services, then ICAP services, then in-line services. **Bypass** lets the connection go to its destination without traversing any service chain. **Reject** terminates the connection. When you use @DG syntax (as described at the beginning of this section) to match destinations against a data group, the chain label in the classifier rule becomes a default which you can override by setting the data-group value for any particular match in the data group to a chain label or keyword.

2. **How should unmatched connections be handled?**

Choose how the system should handle unmatched connections.

• **Send them through a chain of ALL services (except metrics collectors)**

Select this option if unmatched connections should go through a chain of all services you have configured. This is the same as choosing All for the Chain value as described above.

• **Let them BYPASS all service chain**

Select this option if you want unmatched connections to bypass the service chains entirely.

• **REJECT them**

Select this option if unmatched connections should be rejected by the system.

3. **Do you want to view detailed classifier documentation?**

Choose whether you want see detailed information about TCP Service Chain Classifiers. Much of the information in this section is included in the detailed classifier documentation.

• **Hide classifier documentation**

Select this option to hide the classifier documentation.

• **Show classifier documentation**

Select this option to view detailed information on how to configure TCP service chain classifiers.

Continue with the next section.

UDP Service Chain Classifier Rules

This section only appears if you selected to implement either transparent proxy or both transparent and explicit proxies, AND to manage UDP traffic via service-chain classification in [General Configuration on page 19](#).

In this section, you configure the UDP service chain classifier rules. Each service chain classifier rule chooses UDP ingress connections to be processed by a specified service chain (different classifier rules may send connections to the same chain). Each classifier rule has three filters. The filters test source (client) IP address, destination (which can be IP address, IP Intelligence category, or server UDP port), and application protocol (based on UDP port or protocol detection). Filters can overlap so the solution chooses the classifier rules which best matches each connection. For more details, see [Understanding Service Chain Classification on page 52](#).

Using BIG-IP data groups to match IP address, domain names, geolocations, or IPI/URL filtering categories (optional)

To match IP addresses, domain names, geolocations, or IPI/URL Filtering categories against the contents of data groups (which you configure and maintain outside this iApp), insert the special match target **@DG** where **DG** is the name of a data group, such as **/Common/Iplist**. The name (or IP address) of each record in the data group is the match target. For @DG domain-name matching only, you can append an exclamation point (!) to a record name to indicate suffix-match instead of exact match. For example, the record name **F5.COM** would NOT match destination **www.f5.com** but **.F5.COM!** would. Use leading dots (.) to avert errors like **F5.COM!** matching **www.not-f5.com**.

Each record's value is empty, or for Dst matches (only) is optionally a keyword or service-chain name as explained below. When you use @DG syntax to match destinations against a data group, the chain name in the classifier rule becomes a default which you can override by setting the data-group value for any particular match in the data group to a chain name or keyword.

For specific information on configuring Data Groups on the BIG-IP system (**Local Traffic > iRules > Data Group list**), see the BIG-IP documentation or the Help tab on the Data Group List page. Also see [Using the @pinner data group on page 34](#).

1. Service Chain Classifier Rules

Specify service chain classifier rules using the following guidance. If more than one classifier rule matches a connection, the best-matching classifier rule determines the service chain for that connection (so the order of classifier rules in the list is not important). Classifier rules can also reject a connection or let it bypass the service chain. The default action applies to connections which do not match any classifier rule.

- **Src**

The **Src** (source) filter is one or more IP subnet or host addresses. If the source IP of an ingress connection matches an address in the **Src** filter, the other filters will be checked. Using ***** means all-addresses; **@DG** includes addresses from a Data Group (see description earlier in this section). Specify source addresses as prefix/mask-length (CIDR format) like **203.0.113.0/24** or **fd5:f5:cc0f::/64** (to specify a single host omit the mask-length, like **203.0.113.55**). Use spaces or commas to separate multiple filter items.

- **Mode**

Choose the mode you want to use for this classifier rule. The mode you choose determines the value you will use for the **Dst** (destination). You can choose one of the following modes for each classifier rule:

- » **Addr**

If you select **Addr** (address(es)), the **Dst** filter you will configure consists of one or more IP subnet or host addresses just like the **Src** filter.

- » **Geo**

If you select **Geo** (geolocation), the **Dst** you will configure contains 2-letter country and 3-letter continent codes (see [Prerequisites and configuration notes on page 3](#) for continent codes) against which the IP Geolocation of the destination server is compared.

- » **IPI**

If you select **IPI** (IP inspection), the **Dst** you will configure contains one or more IP Intelligence categories against which the destination IP address's reputation is matched. You must replace SPACE characters in names of IP Intelligence categories with underscores (_) before adding them to Dst. While you must have an IP Intelligence license to use this functionality, the iApp will not display an error if you do not, this classifier rule will just not match any connections.

- » **Port**

If you select When mode is 'Port' . For Port, Dst contains one or more TCP port numbers or ranges like **5557-5559** (use 0 or * to match all) against which the destination port number is matched. The chief use of this mode is to control non-TLS traffic such as SSH. If you select Port, the **Proto** value MUST be **All**.

- **Dst**
Dst is destination of the connection. The value of this field is based on the selection you made for the **Mode** (descriptions are found in each mode listed above). If applicable, specify definition addresses as prefix/mask-length (CIDR format) like 203.0.113.0/24 or fd5:f:5:cc0f::/64 (to specify a single host omit the mask-length, like 203.0.113.55). Use spaces or commas to separate multiple filter items. You must replace SPACE characters in names of IP Intelligence categories with underscores (_) when adding them to Dst.
- **Proto**
The **Proto** (protocol) value specifies the protocol of the connection (based on port or protocol recognition). You can specify one of the following protocols:
 - » **All**
Select this option if you want to specify all protocols for this classifier rule.
 - » **QUIC**
Select this option if you want to limit the protocol for this classifier rule to QUIC (UDP ports 80 and 443). the Proto value 'QQQQ'
 - » **QQQQ**
Select this option if you want to limit the classifier rule to recognize QUIC connection attempts (but not session-resumption!) dynamically on any port.
 - » **Other**
Select this option if you want the limit the classifier rule to all other protocols except QUIC and QQQQ.
- **Chain**
Type the name of the Service Chain you configured that you want to use for this classifier rule. This must be the name you gave a service chain **or** a special keyword: **all**, **bypass**, or **reject**. **All** means a chain including all services-- first receive-only services, then ICAP services, then in-line services. **Bypass** lets the connection go to its destination without traversing any service chain. **Reject** causes the connection to be refused (With UDP classifier rules there is no + to re-classify.) When you use @DG syntax (as described at the beginning of this section) to match destinations against a data group, the chain label in the classifier rule becomes a default which you can override by setting the data-group value for any particular match in the data group to a chain label or keyword.

2. How should unmatched connections be handled?

Choose how the system should handle unmatched connections.

- **Send them through a chain of ALL services (except metrics collectors)**
Select this option if unmatched connections should go through a chain of all services you have configured. This is the same as choosing All for the Chain value as described above.
- **Let them BYPASS all service chain**
Select this option if you want unmatched connections to bypass the service chains entirely.
- **REJECT them**
Select this option if unmatched connections should be rejected by the system.

3. Do you want to view detailed classifier documentation?

Choose whether you want see detailed information about UDP Service Chain Classifiers. Much of the information in this section is included in the detailed classifier documentation.

- **Hide classifier documentation**
Select this option to hide the classifier documentation.
- **Show classifier documentation**
Select this option to view detailed information on how to configure UDP service chain classifiers.

Continue with either [Explicit Proxy Configuration on page 39](#) if applicable, or [Ingress Device Configuration on page 40](#).

Explicit Proxy Configuration

This section only appears if you selected an *Explicit proxy* (or both *transparent and explicit*) in the *General Configuration* section. If you specified you are implementing an explicit proxy, use this section to configure the explicit proxy options.

1. **Which VLAN(s) should the explicit proxy listen on?**

From the Options list, select the BIG-IP VLAN(s) on which the explicit proxy should listen.

2. **What IPv4 address and port should the explicit proxy use?**

This question only appears if you selected you are using IPv4 addresses.

Specify the IPv4 address and port the system should use for the explicit proxy virtual server.

- **IPv4 address**
Type the IPv4 address you want to use for the explicit proxy virtual server.
- **Port**
Type the port for the explicit proxy, if different from the default, **3128**.

3. **What IPv6 address and port should the explicit proxy use?**

This question only appears if you selected you are using IPv6 addresses.

Specify the IPv6 address and port the system should use for the explicit proxy virtual server.

- **IPv4 address**
Type the IPv6 address you want to use for the explicit proxy virtual server.
- **Port**
Type the port for the explicit proxy, if different from the default, **3128**.

Continue with *Ingress Device Configuration* on page 40.

Archived

Ingress Device Configuration

In this section, you configure the options on the ingress BIG-IP device, such as SSL certificates and keys, and DNS query information.

1. ***Which VLAN(s) will bring client traffic to the transparent proxy?***

This question appears if you selected Transparent Proxy or both Transparent and Explicit proxies in the General Configuration section

Select the VLAN(s) on which transparent-proxy ingress traffic will arrive (you must configure ingress VLAN(s) and Self IP address(es) outside this iApp, typically in the Setup Wizard).

2. ***Which CA bundle is used to validate remote server certificates?***

Select the CA bundle that is used to validate the remote server certificates. The CA bundle is the collection of root and intermediate certificates for the Certificate Authorities (CA's) you trust to authenticate servers to which your clients might connect. The CA bundle is also known as the local trust store.

3. ***Should connections to servers with expired certificates be allowed?***

Choose what happens with connections to servers with expired certificates. Sometimes remote servers present certificates which have expired. Allowing connections to servers with expired certificates can cause a security risk because clients (which see only substitute server certificates from the BIG-IP SSL Forward Proxy CA) may inadvertently connect to untrustworthy servers. Legitimate servers do sometimes offer certificates which are overdue for renewal or which were signed by legitimate CA's which are simply unknown to the BIG-IP system. If you allow connections in the latter case you should consider adding any needed CA certificates to the BIG-IP CA bundle (trust store).

- **Yes, allow connections to servers with expired certificates.**
Select this option to allow connections to the servers that have expired certificates.
- **No, forbid connections to servers with expired certificates**
Select this option if the system should prevent connections to servers that have expired certificates.

4. ***Should connections to servers with untrusted certificates be allowed?***

Choose what happens with connections to servers with expired certificates. Sometimes remote servers present certificates which were issued by an unknown Certificate Authority (CA). Allowing connections to servers with untrusted certificates can cause a security risk because clients (which see only substitute server certificates from the BIG-IP SSL Forward Proxy CA) may inadvertently connect to untrustworthy servers. Legitimate servers do sometimes offer certificates which are overdue for renewal or which were signed by legitimate CA's which are simply unknown to the BIG-IP. If you allow connections in the latter case you should consider adding any needed CA certificates to the BIG-IP CA bundle (trust store).

- **Yes, allow connections to servers with untrusted certificates.**
Select this option to allow connections to the servers that have untrusted certificates.
- **No, forbid connections to servers with untrusted certificates**
Select this option if the system should prevent connections to servers that have untrusted certificates.

5. ***How should DNS queries be resolved?***

Choose how DNS queries should be resolved. If you choose to send DNS queries directly to nameservers across the Internet you may have to update your firewall configuration to allow the BIG-IP system's DNS queries on UDP and TCP port 53. If you choose to send DNS queries to local forwarding nameservers you should specify at least two.

Note: *This solution uses DNS extensively. You can either permit the system to send DNS queries directly out to the Internet or specify one or more local forwarding nameservers to process all DNS queries from SSL Intercept. Direct resolution can be more reliable than using forwarders but requires outbound UDP and TCP port 53 access to the Internet.*

- **Send DNS queries directly to nameservers across the Internet**
Select this option if you want the system to send DNS queries directly to nameservers across the Internet. This option dynamically contacts the root nameservers and resolves names according to the current Internet DNS tree. Remember, in this case, you may have to update your firewall configuration to allow the BIG-IP system's DNS queries on UDP and TCP port 53.
- **Send DNS queries to forwarding nameservers on the local network**
Select this option if you want the BIG-IP system to send DNS queries to forwarding nameservers on the local network. You must specify the local forwarding nameservers in the next question.

a. Which local forwarding nameserver(s) will resolve DNS queries from this solution?

Type the IP address of the local forwarding nameserver you want to use to resolve DNS queries from this solution. Click **Add** to include more servers. We recommend you enter at least two nameservers. Note these nameservers are (or can be) different than those used for the general BIG-IP DNS settings found at **System > Configuration > Device > DNS**.

6. Do you want to use DNSSEC to validate DNS information?

Choose whether or not you want to use DNSSEC to validate the DNS information. Using DNSSEC to validate DNS information improves security. Dynamic Domain Bypass can use DNSSEC on all BIG-IP devices.

i Important *This iApp will configure initial DNSSEC keys (root Trust Anchor and dlv.isc.org DLV Anchor keys). When those keys are updated (replaced) by their issuers, you may experience lookup failures as a result.*

In this case, you must return to the iApp template using the Reconfigure option (iApps > Application Services > name you gave this iApp > Reconfigure (on the menu bar)) and simply click Finished without making any modifications. The iApp template automatically retrieves the new keys.

- **No, do NOT use DNSSEC to validate DNS information**

Select this option if you do not want to use DNSSEC to validate DNS information. Continue with the next question.

- **Yes, use DNSSEC to validate DNS information**

Select this option if you want to use DNSSEC to validate DNS information for increased security.

As stated in the prerequisites, if you are deploying the iApp template for DNSSEC, you must have DNS configured on the BIG-IP system. To configure DNS on the BIG-IP system, go to **System > Configuration > Device > DNS**. In the DNS Lookup Server List row, add your DNS servers. For complete instructions, see the BIG-IP documentation or the Help tab.

7. Do you want to configure local/private DNS zones?

This question only appears if you selected Send DNS queries directly to nameservers across the Internet

Choose whether or not you want to configure local/private DNS zones. Many organizations have some domain names in DNS zones which are not visible to the Internet. We call those zones *forward zones* because we have to forward queries for records in those zones to local nameservers inside the organization. If you want to use any local DNS forward zones select **Yes**.

- **No, do not configure any local/private DNS zones**

Select this option if you do not want to configure local/private DNS zones at this time. You can always re-enter the iApp at another time to configure these DNS zones.

- **Yes, configure local/private DNS zones**

Select this option if you want to configure local/private DNS zones. You must add the local/private forward zones in the following question.

a. List local/private Forward Zones

Use this area to list the local/private forward zones you want to add to this configuration.

- **Forward Zone**

Type the forward zone you want to add to this configuration. Each local forward zone is identified by the trailing part of a domain name, such as CORP.EXAMPLE.COM.

- **Nameservers**

Type the IP address(es) of a nameserver which answers queries for domains in that zone (separate IP addresses with spaces or commas).

- **DLV keys**

Enter your DLV (DNSSEC Lookaside Validation) key. When a forward zone is signed with a DLV key NOT registered with dlv.isc.org, paste the current DLV key resource-records (RRs), that is, the DNSKEY and DS RR's for the zone— separated by commas (NOT spaces)— into the DLV field (only a small part of the value will be visible).

Some zones will not have DLV RR's— just enter any which your DNS administrator supplies. To enter DLV RR's you will probably wish to copy the DNSKEY and DS RR's into a text editor (just a single (long) line per RR— place a comma at the end of each) then copy-and-paste the whole text at once into the DLV field in the iApp.

Service Chain Classification Previewer

The service chain classification previewer is a tiny web page/service hosted on the ingress BIG-IP device (or Sync-Failover group) that lets you use a web browser or HTTP client to ascertain which service chain would be chosen for a connection with certain parameters of protocol, source, destination, and so on.

➡ **Note:** *The Service Chain Classification Previewer is an Early Access feature and may change or not be present in future versions of this solution.*

1. Do you want to enable the service chain classification previewer?

Choose whether or not you want to enable the previewer.

- **No, do not enable the service chain classification previewer**

Select this option if you do not want to enable the service chain classification previewer at this time. You can always re-enter the iApp at a later time and enable the previewer.

- **Yes, enable the service chain classification previewer**

Select this option to enable the service chain classification previewer. You must answer the following questions.

- a. On which VLAN(s) should the previewer be accessible?

Select the VLAN or VLANs that should have access to the previewer. You have the option of restricting access to clients on specific subnets later in this section.

- b. What IPv4 address should the previewer use?

This question only appears if you specified you wanted to support IPv4 addresses

Type the IPv4 address you want to use for access to the previewer.

- c. What IPv6 address should the previewer use?

This question only appears if you specified you wanted to support IPv6 addresses

Type the IPv6 address you want to use for access to the previewer.

- d. Which TCP port should the previewer use?

Type the TCP port you want the TCP previewer to use. This must be a port number and not the name of the service port.

- e. Which Client SSL Profile should the previewer use?

If you want to protect the previewer (and any credentials used to access it), select the Client SSL profile you created outside the template that includes the appropriate certificate and key. This TLS protection is optional. Creating this Client SSL profile is outside the scope of this document, see the BIG-IP documentation for specific details. If you want to use this functionality, but have not yet created a Client SSL profile, you can leave this set to None, and then complete the template. Then you can create the Client SSL profile and then re-enter the template to select the profile you created.

- f. Do you want to limit previewer access to clients on special subnets?

Choose whether or not you want to limit access to the previewer to clients homed on a specific (IPv4 and/or IPv6) subnet (or block of subnets under a CIDR mask). Clients with IP addresses on other subnets cannot access the previewer.

- **No, allow any client IP to access the previewer**

Select this option if you want any client IP to access the previewer.

- **Yes, allow only clients on special subnets to access the previewer**

Select this option if you want to restrict access to the previewer to clients on the subnets you specify.

- a. What IPv4 subnet must previewer clients connect from?

This question only appears if you specified you wanted to support IPv4 addresses

Type the IPv4 subnet you want clients to have to connect from. Use client subnet number(s) in CIDR format (like 203.0.113.0/24). The default value (*) allows all subnets.

- b. What IPv6 subnet must previewer clients connect from?

This question only appears if you specified you wanted to support IPv6 addresses

Type the IPv6 subnet you want clients to have to connect from. Use client subnet number(s) in CIDR format (like 203.0.113.0/24). The default value (*) allows all subnets.

g. Optional: What username and password do you want to use for the previewer?

If you create a user name and password here then clients will have to supply them (via HTTP Basic Auth) in order to preview service chain classification. Leave these fields empty to permit access without credentials. This is a modest security measure. Do NOT enter any normal user or service-account login name and password here. Just create a special user name and password for the previewer if you want to require them.

The following shows an example of the previewer.

F5 SSL Intercept
Service-Chain Classification Previewer

TCP UDP

Client address: 10.127.10.1
 Server address: 104.219.104.148
 Server port: 443 (guess = HTTP) Protocol: Guess by port

TLS (SSL)
 Match phase: Pre-handshake Handshake Intercepted
 Server domain: www.novelties.example.com

SHOW RULES Classify

```

  graph LR
    scan[scan] --> decrypt[decrypt]
    decrypt --> ids[ids]
    ids --> dlp[dlp]
    dlp --> antivirus[antivirus]
    antivirus --> reencrypt[reencrypt]
  
```

Chain scan chosen by rule 2, match score 54 (mode URLF). Client matched 10.0.0.0/8 in rule, server matched Shopping.

Matching classifier rules, best match first

RULE	PHASE	SRC	MODE	DST	PROTO	CHAIN
Score 54, client matches 10.0.0.0/8 in rule, server matches Shopping.						
2	Normal	10.0.0.0/8	URLF	Shopping	HTTP	scan
Score 33, client matches ANY in rule, server matches *.com.						
1	Normal	0.0.0.0/0	Name	*.com	Any	web
Score 2, client matches ANY in rule, server matches ANY in rule.						
3	Normal	0.0.0.0/0	Addr	0.0.0.0/0	Any	all
RULE	PHASE	SRC	MODE	DST	PROTO	CHAIN

Figure 8: Example of the previewer

This completes the previewer section. Continue with the Egress device configuration on the next page.

Egress Device Configuration (for a one device scenario)

Use this section to configure the egress settings on a single BIG-IP system. If you are using a separate ingress and egress device, see the next section ([Egress Device Configuration \(for the separate ingress and egress device scenario\)](#)).

1. Do you want to SNAT client addresses?

Choose whether or not you want to hide client addresses using SNAT. For security it is common to replace proxy clients' source-IP addresses on outbound connections with addresses belonging to the egress device using a BIG-IP SNAT pool.

- **No. Pass client addresses unaltered**

Select this option if you do not want to SNAT (hide) client IP addresses and pass client address unaltered.

- **Yes. SNAT (replace) client addresses**

Select this option to define suitable SNAT addresses to hide client IP addresses.

- a. Do you want to use a SNAT Pool?

Choose whether you want the system to use a SNAT Pool or SNAT Auto Map. A SNAT Pool allows you to define a list of addresses the BIG-IP system can use for address translation.

SNAT Auto Map uses a BIG-IP Self IP address to replace each client source IP address. With SNAT Auto Map you do not have to define a pool of distinct host addresses for SNAT to use. However, each TMM (Traffic Management Microkernel) instance can only use a fraction of the port numbers associated with any Self IP address. As traffic volume increases, TMM instances will exhaust their SNAT port allocations and start to drop connections. Counter-intuitively, more powerful BIG-IP devices are more likely to drop connections when using SNAT Auto Map. Unless your traffic volume is small, we recommend you define SNAT addresses instead of using SNAT Auto Map.

- **No, use SNAT Auto Map (not recommended)**

Select this option if want to use SNAT Auto Map. You should only use SNAT Auto Map if you have a small volume of traffic. We strongly recommend creating a SNAT Pool.

- **Yes, define SNAT addresses for good performance**

Select this option to define a list of addresses the BIG-IP system can use for address translation. These IP addresses must be otherwise unused. We recommend including one IP address for every CPU on your BIG-IP system. To view the number of CPUs on the system, click **System > Device > General**, and then look at the **CPU Count** row.

- a. What are the IPv4 SNAT addresses?

This question only appears if you specified you wanted to support IPv4 addresses

Type at least as many IPv4 host addresses as the number of CPUs on the ingress device. Each address must be uniquely assigned and routed to the ingress device. It is best to assign addresses which are adjacent and grouped under a CIDR mask, for example, 203.0.113.8 up through 203.0.113.15 which fill 203.0.113.8/29.

- b. What are the IPv6 SNAT addresses

This question only appears if you specified you wanted to support IPv6 addresses

Type at least as many IPv6 host addresses as the number of CPUs on the ingress device. Each address must be uniquely assigned and routed to the ingress device. It is best to assign addresses which are adjacent and grouped under a CIDR mask.

2. Should traffic go to the Internet via specific gateways?

Choose whether or not you want the system to let all SSL intercept traffic use the default route, or if you want to specify Internet gateways (routers). If you chose to use specific gateways, you can also define the ratio of traffic sent to each device.

- **No. Send outbound/Internet traffic via the default route**

Select this option if you want outbound/Internet traffic out using the default route on the BIG-IP system. Continue with [Logging Configuration on page 49](#).

- **Yes. Send outbound/Internet traffic via specific gateways**

Select this option if you want to define a list of gateways (routers) to handle outbound SSL Intercept traffic (and control the share of traffic each is given).

a. What is the address of each IPv4 exit gateway?

This question only appears if you specified you wanted to support IPv4 addresses

Type the IPv4 address(es) of one or more exit gateways (routers). Make sure those gateways route return traffic (e.g., packets addressed to intranet networks) to the exit-VLAN floating Self IP address. Click **Add** include additional addresses. Gateways should respond to a gateway_icmp monitor.

b. What is the address of each IPv6 exit gateway?

This question only appears if you specified you wanted to support IPv6 addresses

Type the IPv6 address(es) of one or more exit gateways (routers). Make sure those gateways route return traffic (e.g., packets addressed to intranet networks) to the exit-VLAN floating Self IP address. Click **Add** include additional addresses. Gateways should respond to a gateway_icmp monitor.

c. Non-public IPv6 networks via IPv6 gateways

If you want to route connections to any non-public IPv6 networks using the IPv6 gateways you specified, enter the prefix/mask-length (CIDR) of each here. Non-public IPv6 networks are those outside the 2000::/3 block, such as ULA networks in the fc00::/7 block. Your organization and your VPN-linked business partners likely have some non-public IPv6 networks.

This completes the egress device configuration for the single BIG-IP scenario. Continue with [Logging Configuration on page 49](#).

Archived

Egress Device Configuration (for the separate ingress and egress device scenario)

Use this section to configure the egress settings if using a separate egress BIG-IP device.

1. **Which VLAN(s) are part of the decrypt zone? (These bring traffic from the ingress device)**

Select the BIG-IP VLAN(s) connected to the decrypt zone (on which traffic from the ingress BIG-IP device arrives). The VLAN(s) must already exist on the system before you can select them here.

2. **Does the decrypt zone hold parallel service devices?**

Choose whether the decrypt zone contains parallel service devices. Choose 'Yes' if there is only one path through the decrypt zone AND the egress device routes all intranet traffic along it, you may choose 'No.'

- **No. Send inbound traffic via BIG-IP intranet route(s)**

Select this option if there is only one path through the decrypt zone AND the egress device routes all intranet traffic along it. Continue with #3.

- **Yes. Send inbound traffic via one or more service device(s)**

Select this option to send inbound traffic through the decrypt zone via one or more Layer 2 or Layer 3 service devices (i.e., anytime you have parallel service devices in the decrypt zone). You must answer the following questions:

- a. **What are the IPv4 ingress gateway addresses?**

This question only appears if you specified you wanted to support IPv4 addresses

Type the IPv4 address(es) of one or more ingress gateways (ingress-device Self IPs for Layer 2 service devices, or IPs of Layer 3 service devices).

You can control the share of traffic sent to each ingress gateway IP by adjusting its ratio value (for example, if one gateway can handle 45 Mbit/sec and another 150 Mbit/sec, give them ratio values 1 and 3 respectively).

Click **Add** include additional addresses. Note these gateways should respond to a gateway_icmp monitor.

- b. **What is the address of each IPv6 exit gateway?**

This question only appears if you specified you wanted to support IPv6 addresses

Type the IPv4 address(es) of one or more ingress gateways (ingress-device Self IPs for Layer 2 service devices, or IPs of Layer 3 service devices).

You can control the share of traffic sent to each ingress gateway IP by adjusting its ratio value (for example, if one gateway can handle 45 Mbit/sec and another 150 Mbit/sec, give them ratio values 1 and 3 respectively).

Click **Add** include additional addresses. Note these gateways should respond to a gateway_icmp monitor.

- c. **What are the intranet networks (subnets)?**

Type the IP address and mask-length (CIDR format) of (blocks of) intranet subnets accessed via the ingress device. Typical IPv4 entries include 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.

3. **Which CA bundle is used to validate remote server certificates?**

The CA bundle is the collection of root and intermediate certificates for the Certificate Authorities (CA's) you trust to authenticate servers that you clients might connect to. (Sometimes the CA bundle is known as the local trust store.)

This solution makes outbound TLS connections on behalf of clients. You can control which remote server certificates will be trusted and how problems with remote TLS servers should be handled. If you want to trust a custom bundle of Certificate Authority (CA) certificates (root and intermediate) to authenticate remote servers, you must load that bundle into the BIG-IP (System > File Management > SSL Certificate List) then select it here. Only CA bundles that already exist on the system appear in the list, so if you add a bundle while configuring the iApp, you will not be able to select it until you exit and then re-enter the template.

4. **Should connections to servers with expired certificates be allowed?**

Choose what happens with connections to servers with expired certificates. Sometimes remote servers present certificates which have expired. Allowing connections to servers with expired certificates can cause a security risk because clients (which see only substitute server certificates from the BIG-IP SSL Forward Proxy CA) may inadvertently connect to untrustworthy servers. Legitimate servers do sometimes offer certificates which are overdue for renewal or which were signed by legitimate CA's which are simply unknown to the BIG-IP. If you allow connections in the latter case you should consider adding any needed CA certificates to the BIG-IP CA bundle (trust store).

- **Yes, allow connections to servers with expired certificates.**
Select this option to allow connections to the servers that have expired certificates.

- **No, forbid connections to servers with expired certificates**
Select this option if the system should prevent connections to servers that have expired certificates.

5. **Should connections to servers with untrusted certificates be allowed?**

Choose whether or not you want to allow connections to servers with untrusted certificates for the same reasons described in #4.

- **Yes, allow connections to servers with untrusted certificates.**
Select this option to allow connections to the servers that have untrusted certificates.
- **No, forbid connections to servers with untrusted certificates**
Select this option if the system should prevent connections to servers that have untrusted certificates.

6. **Do you want to SNAT client IP addresses?**

Choose whether or not you want to hide client addresses using SNAT. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device.

For security it is common to replace proxy clients' source IP addresses on outbound connections with addresses belonging to the egress device using a BIG-IP SNAT pool.

- **No. Pass client addresses unaltered**
Select this option if you do not want to hide client IP addresses using SNAT and pass client address unaltered.
- **Yes. Replace (SNAT) client addresses**
Select this option to define suitable SNAT addresses to hide client IP addresses.

a. **Do you want to use a SNAT Pool?**

Choose whether you want the system to use a SNAT Pool or SNAT Auto Map. A SNAT Pool allows you to define a list of addresses the BIG-IP system can use for address translation. In this case, we recommend specifying one SNAT Pool IP address for each CPU on your BIG-IP system. To view the number of CPUs on the system, click **System > Device > General**, and then look at the **CPU Count** row.

SNAT Auto Map uses a BIG-IP Self IP address to replace each client source IP address. With SNAT Auto Map you do not have to define a pool of distinct host addresses for SNAT to use. However, each TMM (Traffic Management Microkernel) instance can only use a fraction of the port numbers associated with any Self IP address. As traffic volume increases, TMM instances will exhaust their SNAT port allocations and start to drop connections. Counter-intuitively, more powerful BIG-IP devices are more likely to drop connections when using SNAT Auto Map. Unless your traffic volume is small, we recommend you define SNAT addresses instead of using SNAT Auto Map.

- **No, use SNAT Auto Map (not recommended)**
Select this option if want to use SNAT Auto Map. You should only use SNAT Auto Map if you have a small volume of traffic. We strongly recommend creating a SNAT Pool.
- **Yes, define SNAT addresses for good performance**
Select this option to define a list of addresses the BIG-IP system can use for address translation. These IP addresses must be otherwise unused. We recommend including one IP address for every CPU on your BIG-IP system. To view the number of CPUs on the system, click **System > Device > General**, and then look at the **CPU Count** row.

a. **What are the IPv4 SNAT addresses?**

This question only appears if you specified you wanted to support IPv4 addresses

Type at least as many IPv4 host addresses as the number of CPUs on the BIG-IP device. Each address must be uniquely assigned and routed to the device. It is best to assign addresses which are adjacent and grouped under a CIDR mask, for example, 203.0.113.8 up through 203.0.113.15 which fill 203.0.113.8/29.

b. **What are the IPv6 SNAT addresses**

This question only appears if you specified you wanted to support IPv6 addresses

Type at least as many IPv6 host addresses as the number of CPUs on the BIG-IP device. Each address must be uniquely assigned and routed to the device. It is best to assign addresses which are adjacent and grouped under a CIDR mask.

7. Should traffic go to the Internet via specific gateways?

Choose whether or not you want the system to let all SSL intercept traffic use the default route, or if you want to specify Internet gateways (routers). If you chose to use specific gateways, you can also define the ratio of traffic sent to each device.

- **No. Send outbound/Internet traffic via the default route**

Select this option if you want outbound/Internet traffic out using the default route on the BIG-IP system. Continue with [Logging Configuration on page 49](#).

- **Yes. Send outbound/Internet traffic via specific gateways**

Select this option if you want to define a list of gateways (routers) to handle outbound SSL Intercept traffic (and control the share of traffic each is given).

- a. What are the IPv4 outbound gateway addresses?

This question only appears if you specified you wanted to support IPv4 addresses

Type the IPv4 address(es) of one or more exit gateways (routers). Make sure those gateways route return traffic (e.g., packets addressed to intranet networks) to the exit-VLAN floating Self IP address. Click **Add** include additional addresses. Gateways should respond to a gateway_icmp monitor.

- b. What are the IPv6 outbound gateway addresses?

This question only appears if you specified you wanted to support IPv6 addresses

Type the IPv6 address(es) of one or more exit gateways (routers). Make sure those gateways route return traffic (e.g., packets addressed to intranet networks) to the exit-VLAN floating Self IP address. Click **Add** include additional addresses. Gateways should respond to a gateway_icmp monitor.

- c. Non-public IPv6 networks via IPv6 gateways

If you want to route connections to any non-public IPv6 networks using the IPv6 gateways you specified, enter the prefix/mask-length (CIDR) of each here. Non-public IPv6 networks are those outside the 2000::/3 block, such as ULA networks in the fc00::/7 block. Your organization and your VPN-linked business partners likely have some non-public IPv6 networks.

This completes the egress device configuration for the separate device scenario. Continue with [Logging Configuration on page 49](#).

Logging Configuration

This section contains information about how to configure logging of SSL Intercept activity.

1. **What SSL Intercept logging level do you want to enable?**

Choose the level of logging you want the system to perform for this implementation. The SSL Intercept solution can generate log messages to help you monitor (and optionally debug) system activity. Log messages may be sent to one or more external log servers (preferred) and/or stored on the BIG-IP device (less desirable because BIG-IP devices have limited log storage capacity).

To control where log messages are sent or stored, you must configure BIG-IP High Speed Logging features outside of the iApp template. This configuration is outside the scope of this document, see the BIG-IP documentation for instructions: https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-external-monitoring-implementations-12-0-0/4.html.

The key BIG-IP configuration object for High Speed Logging is called a Log Publisher. If you enable SSL Intercept logging at the Normal or Debug levels you should configure then select a BIG-IP Log Publisher to send the log messages to your log server(s) and/or store them on the BIG-IP device.

- **Errors. Log only functional errors**

Select this option if you only want to log errors related to the functioning of the SSL Intercept solution..

- **Normal. Log connection data as well as errors**

Select this option for a normal level of logging. In this case, the system logs per-connection data in addition to functional errors.

- **Debug. Log debug data as well as Normal-level data**

Select this option if you want the system to log debug data as well as connection data and functional errors. We recommend using this mode only during setup or troubleshooting, as it consumes more resources on the BIG-IP system.

2. **Which BIG-IP Log Publisher will process the log messages?**

Choose whether an existing Log Publisher object will process the log messages or if messages should not be processed by a Log Publisher and just sent to syslog-ng. Use of a Log Publisher is strongly recommended for good system performance. The syslog-ng service is useful for Errors-only logging but is too slow for Normal or Debug logging when the system is used in production. A Log Publisher delivers log messages to one or more Log Destinations. Log Destinations may include Syslog, ArcSight, Splunk, and other log servers as well as the BIG-IP's local log database. To use a Log Publisher, it must already be present on the system; the iApp template does not create one.

- **None (send log messages to syslog-ng)**

This option is not recommended for use in production systems. Select this option if you want the system to send log messages to the BIG-IP management-plane syslog-ng subsystem.

- **Select the Log Publisher you created from the list**

If you have configured BIG-IP High Speed Logging (outside of this iApp), select the appropriate Log Publisher object. A Log Publisher delivers log messages to one or more Log Destinations. Log Destinations may include Syslog, ArcSight, Splunk, and other log servers.

3. **What kind of statistics do you want to record?**

Choose the kind of statistics you want the system to record. The SSL Intercept solution can collect usage data for connections, service chains, services, and so on. The solution can also record remote domain names and TLS cipher suites for TLS connections if you wish, but gathering such data consumes more system resources.

Domain names are taken from remote server PKI certificates (or client SNI in the case of Dynamic Domain Bypass) and may include a wildcard. TLS cipher suites may not be recorded when a connection bypasses interception.

If you choose to collect any statistics, the BIG-IP system starts saving extra data in memory for the use of integration with performance reporting systems like Splunk or BIG-IP iStats integration.

- **None**

Select this option if you do not want the system to record statistics.

- **Usage counters only-- no remote-domain+cipher records**

Select this option for the system to record usage counters only, and not statistics on remote-domain and cipher records.

- **Usage counters and remote-domain+cipher records (may slow system)**

Select this option if you want the system to record both usage counters and remote-domain and cipher records. Use this option with caution, as it may cause slower performance on the BIG-IP system.

This completes the iApp configuration. Review your answers to the questions, and then click the **Finished** button.

Next Steps

After completing the iApp Template, the BIG-IP Application Services page opens for the application service you just created. To see the list of all the configuration objects created to support the implementation, on the Menu bar, click **Components**. The complete list of all related objects opens. You can click individual objects to see the settings. Once the objects have been created (on all BIG-IP systems in the Sync-Failover group if applicable), you are ready to use the new deployment.

Client configuration

If you chose the explicit proxy option (or both explicit and transparent), ensure that your network infrastructure routes packets addressed to the explicit proxy address to the BIG-IP system.

If you selected the transparent proxy option (or both explicit and transparent), you must ensure the default route for all SSL (TLS) clients whose traffic you want to inspect leads to a Self IP address configured on one of the ingress VLANs you selected for client-side traffic on the ingress BIG-IP system (or the ingress BIG-IP device in a two-device configuration).

Synchronizing the BIG-IP configuration

Use the following information to manually synchronize the BIG-IP configuration across devices in the Sync-Failover device Group.

For complete information, see

https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip-device-service-clustering-admin-12-0-0/6.html.

i Important *As stated in the prerequisites, DO NOT configure your Sync-Failover device group for Automatic Sync. You must manually synchronize the configuration using the following guidance.*

1. On the Main tab, click **Device Management > Overview**.
2. In the Device Groups area of the screen, from the **Name** column, select the name of the relevant device group. The screen expands to show a summary and details of the sync status of the selected device group, as well as a list of the individual devices within the device group.
3. In the **Devices** area of the screen, in the Sync Status column, select a device.
4. From the **Sync options** list, select to either **Sync Device to Group** or **Sync to Device**.
5. Click **Sync**.

Removing or modifying the iApp configuration

Use this section for guidance on removing or modifying the iApp template configuration.

Modifying the iApp configuration

The iApp Application Service you just created can be modified if you find it necessary to make changes to the configuration.

1. On the Main tab, click **iApp > Application Services > name of your Application Service > Reconfigure**.
2. Make any modifications to the template. If you modify in-line services, see [Modifying or deleting an in-line service you already created on page 10](#).
3. Click the **Finished** button.

Modifying an in-line service


To modify or remove an existing in-line service, see [Modifying or deleting an in-line service you already created on page 10](#).

Removing the iApp configuration

Completely removing the iApp configuration is a two-step process available in the iApp template. There are two steps because the system must first delete the floating objects, such as virtual servers and pools before it can delete the static objects (such as VLANs). You must also synchronize the configuration after each step.

If you do not use the two-step process in the template to remove the configuration and just delete the Application Service directly, you may have orphaned objects on your system. Typically these objects are harmless, but in this case, we recommend you restore the BIG-IP configuration you saved before deleting the iApp Application Service and then use the two-step process in the iApp.

1. Use the Reconfigure option on the Application service to re-enter the template.
2. In the Welcome section at the top, from the *Do you want to remove this application service?* question, select the Yes option.
3. From the *Which step do you want to perform now?* question, select **First step-- remove floating objects**.
4. Click **Finished**, and then synchronize the configuration.
5. Use the Reconfigure option to re-enter the template again.
6. From the *Which step do you want to perform now?* question, select **Final step-- remove static objects (like VLANs)**.
7. Click **Finished**, and then synchronize the configuration.
8. Click **iApps > Application Services**, click the box next to the name of your iApp service and then click **Delete**.

 **Critical** *Once you specify you want to delete the configuration, when you select either of the steps (first or final) and then click Finished, the configuration objects are completely deleted. You cannot get them back unless you restore the entire BIG-IP configuration from a previous archive.*

Backing up the BIG-IP configuration before starting the configuration (or before major changes to the iApp)

Before beginning the iApp configuration, or before you make substantial changes, we strongly recommend you back up the BIG-IP configuration using the following guidance. This allows you to restore the previous configuration in case of any issues.

For more details, complete instructions, and other considerations for backing up and restoring the BIG-IP configuration, see SOL 13132 on Ask F5: <https://support.f5.com/kb/en-us/solutions/public/13000/100/sol13132.html>.

1. On the BIG-IP system, click **System > Archives**.
2. To initiate the process of creating a new UCS archive (back up), click **Create**.
3. In the **File Name** box, type a name for the file. This file name must be unique.
4. Optional: If you want to encrypt the UCS archive file, from the **Encryption** menu, select **Enabled** and enter a passphrase.
5. Optional: If you want to exclude SSL private keys from the UCS archive, from the **Private Keys** menu, select **Exclude**.
6. Click **Finished**.
7. To restore the configuration from a UCS archive, go to **System > Archives**. Click the name of the UCS file you want to restore. Click **Restore**. Again, see <https://support.f5.com/kb/en-us/solutions/public/13000/100/sol13132.html> for details.

Understanding Service Chain Classification

The *service chain classifier*, or just “classifier,” is the element of the SSL Intercept solution which selects the proper service chain to handle each connection. (A “connection” is a particular packet flow between client (source, abbreviated Src) and server (destination, abbreviated Dst), identified by the “five-tuple” of IP protocol (TCP or UDP) plus client (Src) and server (Dst) IP addresses and port numbers.)

The following flowchart is a guide to the way the service chain classifier works.

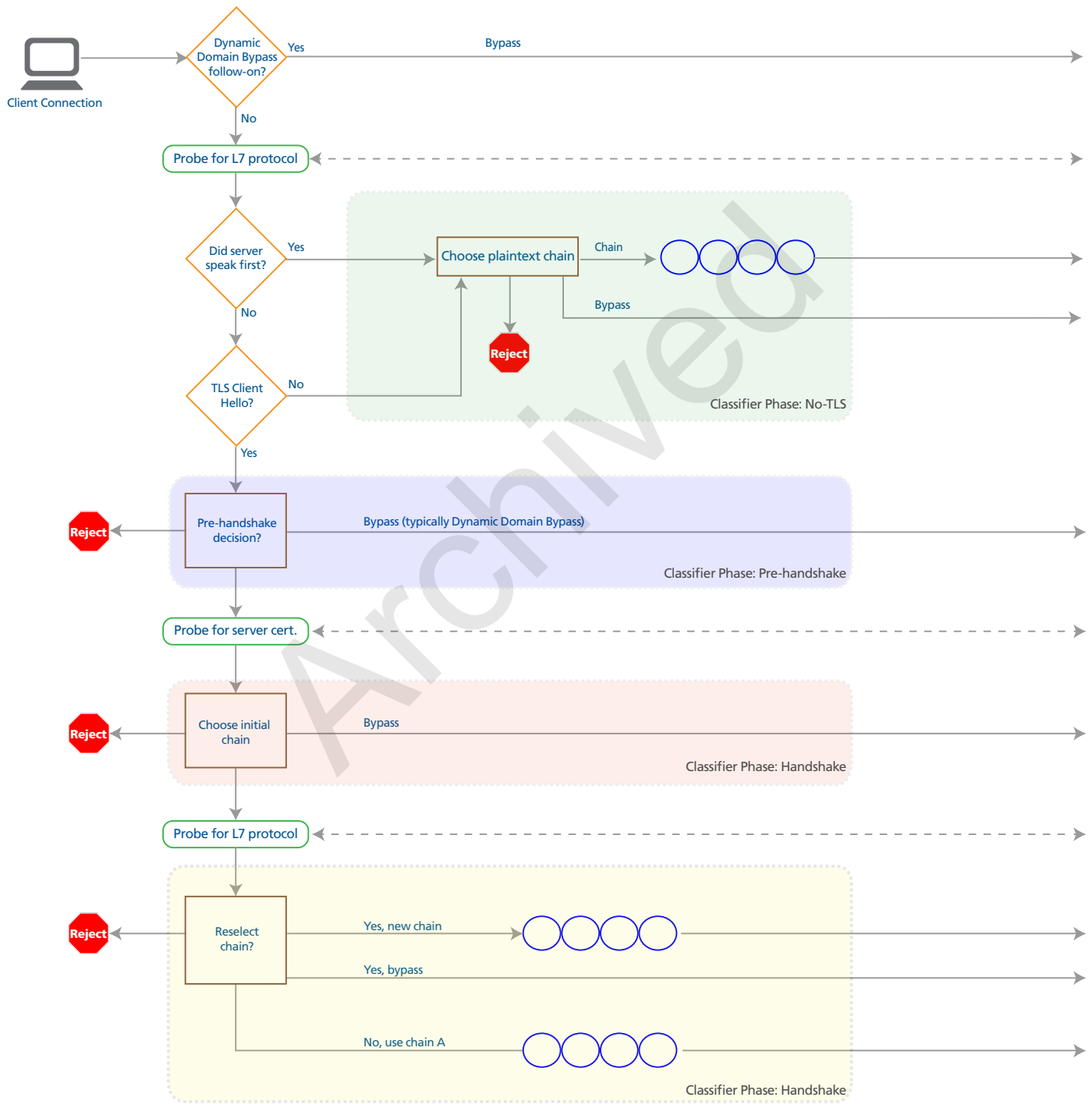


Figure 9: Service Chain Classifier Rule flow

The classifier has a set of rules for TCP connections, and another set of rules for UDP when UDP service chains are enabled.

The classifier matches information describing each connection, such as its client and server IP addresses, against criteria specified in the classifier rules. For example, a classifier rule might match all connections from clients homed on a certain IP subnet. Another classifier rule might match all connections going to servers in a certain country (using IP Geolocation).

Four phases of matching TCP rules to connections

The classifier matches TCP rules to connections in four phases. One of the phases is for connections which do not use TLS (SSL). The other three phases are for TLS connections, which are more complicated to manage.

No TLS phase

When a connection does not use TLS the classifier can recognize the application protocol (such as HTTP) for that connection as it starts. A classifier rule which applies in this **No TLS** phase can select a service chain which will not change during the life of the connection. Since UDP connections never use TLS, UDP classifier rules have only one matching phase, which is equivalent to the TCP **No TLS** phase.

Things are different when a connection does use TLS. The three classifier phases in that case are "Pre-handshake," "Handshake," and "Intercepted."

Pre-handshake phase

The classifier matches Pre-handshake rules in the interval after recognizing that a connection will use TLS (because the client has sent a TLS Client Hello message) but before SSL Intercept attempts TLS handshakes with the server or client. Only in the Pre-handshake phase is it possible to totally bypass TLS interception; that is, to allow the client to establish a TLS channel to the server without any disturbance from the SSL Intercept solution. Pre-handshake rules may only select the special **reject** or **bypass** chains because in order to get data to run through a regular service chain the SSL Intercept solution must participate in TLS handshakes— and then the classifier can match rules in the Handshake or Intercepted phases.

In the Pre-handshake phase the classifier does not yet know the verified name(s) of the server because a TLS handshake with the server is needed to get that information. Therefore Pre-handshake rules match server names in a special manner called *Dynamic Domain Bypass (DDB) matching* which is detailed in [Dynamic Domain Bypass on page 55](#). DDB matching is just like Name matching except the server name which DDB (and URLF) classifier rules match in the Pre-handshake phase is taken from the Server Name Indication (SNI) value supplied in the TLS Client Hello message and validated in a special way using DNS. As explained on [page 55](#), DDB makes it possible to match server-names and URL Filtering categories securely in the Pre-handshake phase.

Handshake phase

The classifier matches Handshake-phase rules after performing a TLS handshake with the remote server but before completing a TLS handshake with the client. Sometimes SSL Intercept will use cached information about the server in lieu of completing an extra handshake with it. In this phase, the server's verified names are available from its PKI certificate to support normal Name and URLF matching. Most commonly, decisions to bypass based on server identity or URL Filtering category are made in the Handshake phase using the reliable name information available in this phase. A regular service chain (or **reject**) may also be chosen in this phase. If the connection is not rejected or bypassed, it is intercepted, which means that the TLS armor is stripped from the flow so the application protocol data inside it can be serviced/inspected by the service chain.

When the classifier finds no matching rule for a TLS connection in the Pre-handshake or Handshake phase it selects the default service chain, which is commonly **all**. That means the connection is intercepted (decrypted), giving the classifier one last chance to find a matching rule in the Intercepted phase.

Intercepted phase

In the Intercepted phase the classifier matches rules after it gets a chance to recognize the application protocol which was concealed beneath TLS encryption in earlier phases. A rule which matches in this phase may override the service chain selected in an earlier phase. If a client makes a TLS connection to server port 200, a Handshake-phase rule might select a service chain with only an IDS service in it for that connection, because port 200 is not associated with any popular protocol. Stripping TLS from that connection, however, might reveal that the real application protocol is HTTP (so the connection is really "HTTPS to a non-standard port"). An Intercept-phase rule could then replace the service chain with one that includes an ICAP anti-malware service as well.

A classifier rule might change the service chain to bypass in the Intercepted phase. At that point it is too late to avoid decrypting the TLS connection, so the SSL Intercept solution simply forwards the application data through a TLS connection to the remote server without steering it through any local services, so no cleartext data ever leaves the BIG-IP system.

Configuring classifier rules

When configuring classifier rules, you can choose whether a rule should match in the No-TLS, Pre-Handshake, TLS Handshake, or **Normal** phases. You cannot create a rule to match only in the Intercepted phase, rather, the option **Normal** means the rule may match in any of the No-TLS, Handshake, or Intercepted phases. **Normal** rules are very useful because they let you correctly select service chains for traffic on well-known or non-standard ports, with or without TLS, based on your security policy, with just a few rules. To do the same work with rules that match only in a particular phase would require a lot of duplication and make the classifier policy harder to understand and maintain.

Classifier rule matching

For every phase, classifier rules are matched first on client IP address. Only if the client IP address matches the IP address(es) and/or subnets in a rule are the other criteria tested. Next, rules are matched on application protocol (such as HTTP or SSH). When feasible the application protocol is recognized by looking at the actual application data, but in the Pre-handshake and Handshake phases, and for hard-to-parse protocols, a guess based on port number is used. For example, in the Handshake phase a connection to TCP port 587 is considered Mail. However, it could be recognized as HTTP in the Intercepted phase. Sometimes a client will try to use a firewall port open for connections of one type to smuggle traffic of another type.

No-TLS rules cannot match on server Name or URL Filtering category (as the URL Filtering category database is indexed by server name).

Pre-handshake rules match TLS connections early, using SNI values tempered by DNS lookups to match server names (called **DDB** instead of **Name** as a sort of reminder) and URL Filtering categories (as explained later).

Otherwise, classifier rules may match according to: server IP address; server port; server geolocation; server IP reputation; server name; and server URL Filtering category; as well as application protocol.

Note that protocol **Any** means *any protocol*, but **Other** means *any protocol other than HTTP, Mail, SSH, or DNS*.

In every phase, when the matching expression in a rule uses a data-group lookup (@data-group), the service-chain selection may also be taken from that data group, overriding the (default) service chain specified at the end of the rule.

Multiple-Name Matching

Often a TLS server will have multiple names, perhaps with wildcards, to identify the services it hosts. When a client uses SNI to name the service it wants to contact and that name is one the server owns (per the server's certificate, according to RFC 6125), then the classifier will use precisely that name for rule matching. For example, when a client asks (using SNI) for www.f5.com and the server certificate names both f5.com and *.f5.com, the classifier will use www.f5.com to match Name and URLF rules (URL Filtering categories are keyed by server name). When a client does not supply an SNI value (or the SNI is invalid) the classifier cannot know which of the server's names is the right one for the connection, so the classifier uses all of the server's names to match Name rules. For URLF matching when there is no SNI, the classifier looks up the URL Filtering category of the server's first non-wildcard name, or when all the server's names have wildcards, the URLF category of the parent domain of the first wildcard name (the *example.com* part of ***.example.com**). Classifier CPU cycles are minimized when clients use SNI.

Understanding Match scores

It is common for more than one classifier rule to match a given connection. Classifier rules are more or less specific, to accommodate administrative policies like "generally connections to Internet websites will be inspected by the DLP and antivirus scanners, but connections to Financial Services websites will only be inspected by antivirus (to avoid false DLP alerts), while connections to specially-listed local bank websites will not be inspected at all." Such a policy would need three classifier rules: one that matched all HTTP and HTTPS connections, one that matched connections to Financial Services websites, and one that matched a list of bank website domain names. A connection to a shopping website would match only the first rule, a connection to a brokerage-firm website would match the first and second, and a connection to a local credit-union could match all three.

Because each of the rules which match a connection may select a different service chain, the classifier needs to decide just which rule to apply. The classifier chooses the rule that matches best, meaning most specifically. The classifier computes a *match score* for each rule and the rule with the highest match score (in each phase) selects the service chain. The match score for a rule is the sum of the match scores for client/Src IP and server/Dst match criterion.

The match score for an IP address match (client/Src or server/Dst) is the length of the IPv6 CIDR mask for the address in the rule plus 1. For example, every exact (host) IP match has a match score of 129. The match scores for IPv4 subnets are scaled up to IPv6 proportions so that an IPv4 /24 (Class C) roughly equals an IPv6 /64. A rule with an exact (host) match for both Src and Dst IP would have a final match score of 258 (which is the highest possible match score). A rule for which neither Src nor Dst matches at all has a

final score of 0 (zero). Note that an **any value** (* or IP ::/0) match has a score of 1, so the classifier can distinguish between matching a very broad rule (Src=any, Dst=any) and failing to match any rule at all.

The match scores for other criteria are based on the precision and accuracy of each criterion. For example, the score for an exact server-name (domain-name) match is 129 like the score for an exact (host) address match. However, the score for a partial name match depends on the number and type of components and wildcards in the name-matching expression. A match to *.com, for example, has a score of 32. The match score for example.com is 48. For svr[0-9].example.com, 64.

For IP geolocation, matching a continent yields a score of 16 and matching a country is worth 24. An IP Intelligence (reputation) category match scores 40. A URL Filtering category match has a score of 32. The score for an exact TCP or UDP port match is 17, and port-range match scores are equal to $(17 - \log_2(\text{size-of-range}))$, so narrow ranges have higher scores (for example, port range 20-21 is worth 16 while port range 52000-57000 would score only 5).

You can test and review the ways your classifier rules match using the Service Chain Classification Previewer (see [Service Chain Classification Previewer on page 42](#)).

Service chain selection

When the classifier selects a service chain for a TLS connection in the Handshake phase which results in that connection being intercepted (decrypted), then the classifier will consider that connection again in the Intercepted phase, and possibly choose a different service chain to process the decrypted flow. However, between the Handshake and Intercepted phases, packets for the connection will be steered through the service chain selected in the Handshake phase. A service device in that initial service chain could interrupt that flow before the classifier runs in the Intercepted phase (for example, an IDP service might reset a TCP flow to a shunned server address). It is common for the same service chain to be selected in both the Handshake and Intercepted phases (for example, when a connection uses a well-known port so the classifier's initial application-protocol guess is not invalidated by examining the decrypted flow after interception). When the same service chain is selected in both phases, the flow through the initial service chain is not disturbed. However, when a new service chain is selected in the Intercept phase then the flow through the initial chain will be dropped and a new flow will be established through the new chain.

Other factors that affect services in a chain

Even after the classifier selects a service chain for a connection, some other considerations may affect the links in that chain: services incompatible with the actual application protocol for the connection may be skipped (for example, an ICAP service may be skipped when a connection's application protocol is not HTTP), and services which are unavailable because all their service devices are offline may be skipped (depending on policy).

The classifier does not try to match connections to *problem servers* when the administrator has enabled auto-bypass after server-side TLS handshake problems. Such connections bypass service-chain classification as well as TLS interception, based strictly on destination IP:port.

Dynamic Domain Bypass

A TLS client may insert any domain name into the SNI (Server Name Indication) option of a Client Hello message that it sends to any server IP address. Nothing in the TLS protocol enforces any correspondence between SNI and the real name(s) of a remote server (that is, the name(s) asserted in the server's certificate and validated by its CA). Therefore, one must not simply substitute SNI values for server names when making service-chaining or traffic-handling decisions with security implications.

On the other hand, one often wishes to make a policy decision about handling a connection before performing the server-side TLS handshake necessary to learn the remote server's real name(s) from its certificate. F5 has invented a secure way to use SNI values for name-based policy decisions (such as name matching or URL Filtering category matching). In SSL Intercept the process is called Dynamic Domain Bypass, or DDB

Dynamic Domain Bypass works as follows: when the classifier selects a service chain on the basis of an SNI value supplied by the client (for example, when matching rules in the Pre-handshake phase), SSL Intercept independently resolves that SNI domain name to one or more IP addresses, using DNSSEC for verification when possible. If the server (destination) address specified by the client is one of the addresses obtained by SSL Intercept, the connection is made to that address. Otherwise, SSL Intercept replaces the server address specified by the client with one that it trusts (because it has independently obtained and verified it). This frustrates any malicious client which tries to fool gateways like SSL Intercept into allowing connections to malicious server IP's by placing domain names of trusted servers into SNI. With DDB, when a client uses SNI to ask for a connection to a trusted domain, that client gets a connection to that trusted domain—only. Legitimate clients are satisfied, and malicious clients are frustrated.

The DDB process inside SSL Intercept supports server persistence for good application performance.

Appendix: Additional configuration settings

Use this section for additional settings you may need to configure on the BIG-IP system.

Configuring the initial DNS settings on the BIG-IP system

In order to use the iApp template, you must have DNS configured on the BIG-IP system. If you ran the Setup Wizard, you likely configured the DNS servers at that time. If you did not use the Setup Wizard, follow the guidance in this section.

Note that these DNS settings are for the iApp template itself. When configuring the iApp, you choose additional DNS configuration options concerning how DNS queries should be resolved, and whether or not you want to use DNSSEC to validate DNS information.

i Important *The BIG-IP system must have a self IP address in the same local subnet and VLAN as the DNS server or a route to the DNS server if located on a different subnet. The route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
 - a. In the **Address** box, type the IP address of a DNS server.
 - b. Click the **Add** button.
4. Click **Update**.

Optional URL filtering

If you have licensed URL filtering on your BIG-IP system, to enable filtering by URL category in classifier rules, you must provision SWG (no SWG license is needed. Provisioning SWG just enables the URL Filtering module). URL filtering is configured in the iApp template in the TCP Service Chain Classifier Rule section by selecting **URLF** from the **Mode** list.

Before configuring URL filtering, we recommend you update the URL database, and strongly recommend you use the download-schedule command shown below to schedule recurring updates. Updates must be performed from the BIG-IP command line.

First, ensure you can reach download.websense.com on port 80 from the BIG-IP command line (using **curl** for example).

Next, from the BIG-IP command line, use the following commands to view and update the URL category database.

```
tmssh list sys url-db download-result
```

This command lists the current version number for the master and real-time security update URL category databases.

```
tmssh list sys url-db
```

This command lists the configuration settings for the URL categorization database.

```
tmssh list sys url-db url-category
```

This command lists the current URL categories.

```
tmssh modify sys url-db download-schedule urldb start-time HH:MM end-time HH:MM
```

This command schedules a daily download of the URL categorization database between what you configure as the “start-time” and “end-time”.

```
tmssh modify sys url-db download-schedule urldb download-now true
```

This command initiates a one-time download of the URL categorization database.

i Important *We strongly recommend using the download-schedule command to set up regular, recurring downloads of the URL category database.*

For more information on these and other TMSH commands, see the Traffic Management Shell (tmssh) Reference Guide for the BIG-IP version you are using. For example, if you are using BIG-IP version 12.0, the guide can be found at:

https://support.f5.com/kb/en-us/products/big-ip_itm/manuals/product/bigip-tmssh-reference-12-0-0.html.

Known Issues

Use this section to learn about known issues in this solution and any available workaround. These issues are all slated to be fixed before the iApp is official released.

You may experience fluctuating results from ICAP traffic in a service chain with high preview sizes

For the question *What is the maximum length in bytes of the ICAP preview?*, if you used a value significantly higher than the default (1024), you may experience varied results for traffic with ICAP in the service chain. The traffic latency you experience depends on how large you set the preview, as well as traffic load, ICAP response times, and other potential factors. This is not an issue with the BIG-IP system, but more because some ICAP servers are slow with large preview sizes.

ICAP servers are responding with 400-level errors when they should be giving 200 or 204 messages

If you experience a scenario where traffic is sent to an ICAP server in the service chain, and the ICAP server response is a 400 level error when it should respond with a 200 or 204 message, use the following guidance.

In answer to the *What is the ICAP Request processing URI?* and *What is the ICAP Response processing URI?*, use the whole request string, including the request/response URI, for example, `icap://{SERVER_IP}:{SERVER_PORT}/reqmod`.

You may experience a "cannot delete" error in certain situations after configuring the Egress device to send traffic to the Internet via specific gateways

You may receive an error stating an object cannot be deleted because it is in use by a static route if, in the Egress device configuration (or the Egress side of a single device), you specified that traffic should go to the Internet via specific gateways, and then configured gateway addresses. The error will look similar to the following:

The Pool (/Common/intercept.app/intercept-70) cannot be deleted because it is in use by a static route (/Common/intercept.app/intercept-70-tgt-4

The error occurs when you attempt one of the following:

- You attempt to delete the iApp template configuration (remove the application service) using the two step process at the top of the iApp template, or
- You initially configured the Egress device to send traffic to the Internet via specific gateways, but then re-enter the template and change the setting to send outbound / Internet traffic via the default route.

To workaround this issue, you must manually delete the static route objects created by the iApp. You can find these routes by clicking **Network > Routes**. The routes that should be removed start with the name you gave the iApp template, followed by **-exit-4-A**. If you specified multiple routes, the name will be the same, but the letter at the end will increment (-exit-4-B, -exit-4-C, etc).

Once you have deleted the routes, you can re-enter the iApp template and either finished deleting the iApp template, or modify the Egress outbound traffic configuration.

Occasional connection failure followed by success with multihomed TLS servers

The first attempt to connect to a particular alternate IP address for a multihomed TLS-enabled service may fail when the client sends an SNI value which was previously sent with a connection to some other IP address for the same service. Subsequent connection attempts to the given IP address using the same SNI will succeed. This issue may only be noticed when a non-web-browser TLS client cycles through the IP addresses of a multihomed service without retrying failed connection attempts, while trying different IP addresses obtained from round-robin DNS.

Port ranges in classifier rules don't work and errors are logged

In the initial release of this solution, port ranges like "20-21" in classifier rules don't work. Port number lists like "20, 21" may be used in lieu of port ranges.

Service-chain previewer rule list may not show some lower-scoring rules

In the initial release of this solution, the list of rules (other than the best-matching rule) which match a connection may not include some rules with lower match scores.

Document Revision History

Version	Description	Date
1.0	New guide for the latest version of the iApp template, f5.ssl_intercept_svc_chain.v1.5.0.	08-23-2016
1.1	Updated the diagram and clarified some of the information in <i>Understanding Service Chain Classification on page 52</i> .	08-26-2016
1.2	<p>Updated this guide for iApp version f5.ssl_intercept_svc_chain.v1.5.8. This version contains the following changes:</p> <ul style="list-style-type: none"> - Important security improvements (see https://support.f5.com/csp/article/K53244431 and https://support.f5.com/csp/article/K23001529 for details). F5 recommends all users upgrade to this version as soon as possible. - In the General Information section of the iApp, there are new questions asking about how you want to handle SSLv3 and SSLv2 connections, as well as how to enforce TLS secure renegotiation. See questions 5-7 in <i>General Configuration on page 19</i>. - In the In-Line Services section of the iApp, there are new questions asking if Layer 3 services devices should see real client IP and port, and if in-line services devices may initiate their own network traffic via outward VLANs. See questions 3 and 4 in <i>In-line Services on page 23</i>. 	04-05-2017

Archived

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

