Recommended Practices Guide

F5 Networks Air Gap Egress Inspection with SSL Intercept:
Deploying F5 BIG-IP Local Traffic Manager with
Websense® TRITON® AP-DATA Protector
for Data Loss Prevention

F5 BIG-IP Local Traffic Manager and Websense TRITON AP-DATA Protector

Version 1.1

Contents

Introduction 1
Assumptions, constraints, dependencies, and risks 2
Purpose 2
F5 BIG-IP LTM Air Gap Egress Inspection with SSL Intercept and Websense TRITON AP-DATA protector solution overview 3
Configuration prerequisites 5
Infrastructure 6
F5 BIG-IP 6
Configuration instructions 6
Configure Websense TRITON AP-DATA protector 6
Run and configure the F5/Websense TRITON AP-DATA protector iApp 8
Integrate the F5/Websense TRITON AP-DATA protector iApp with an existing F5 Air Gap Egress Inspection with SSL Intercept Multi-BIG-IP deployment 11
Conclusion 13

1 Recommended Practices Guide

Introduction

This document is intended as a guide of recommended practices for deploying F5 traffic management operating system (TMOS) 11.6.0 Local Traffic Manager (LTM) with Websense® TRITON® AP-DATA protector versions 7.8.3, 7.8.4, and 8.0.0. You may use this guide with the latest version of F5 TMOS and TRITON AP-DATA, but it was developed and tested with the above versions.

F5 BIG-IP LTM enhances Websense TRITON AP-DATA in the following ways:

- **Scalability** – Easily deploy multiple TRITON AP-DATA protectors for scalability and redundancy.
- **Load Balancing** – Load balance the protector using a number of load balancing methods.
- **Session Persistence** – Ensure connections will persist to and from the protector to avoid session interruption.
- **Health Monitoring** – Easily deploy a specific protector with the ICAP BIG-IP health monitor.
- **Extensibility** – Deploy the protector with the optional F5 BIG-IP Secure Web Gateway (SWG) to enhance SWG content scanning with comprehensive data loss prevention (DLP) protection for the Enterprise.
- **SSL Visibility** – In conjunction with F5 Air Gap Egress Inspection with SSL Intercept, BIG-IP decrypts SSL traffic to allow the Websense protector to scan HTTP POSTs for policy violations. BIG-IP will re-encrypt the SSL traffic to complete the session to the origin server as TRITON AP-DATA policy allows.
- **SWG SSL Bypass** - Create an SSL inspection bypass list for HTTPS sites that should not be inspected by BIG-IP with F5 BIG-IP SWG.

The recommended practices in this guide use F5 iApp technology that provides the following benefits:

- **Ease of deployment** – The F5/Websense TRITON AP-DATA protector iApp enables quick deployment of the protector with F5 Air Gap Egress Inspection with SSL Intercept. The iApp, which accompanies this guide, will configure the

Websense protector load balancing, session persistence, health monitoring, ICAP profiles, server pools, and virtual servers.

- **Configuration compliance** – The F5/Websense protector iApp ensures that all configuration changes are made within the iApp. Configuration parameters must meet the criteria set within the iApp thereby reducing configuration errors.
- **Configuration Security** - If a change is made directly to a configuration object that was created with the F5/Websense protector iApp, by default, the change is rejected (when the iApp's strict updates are enabled). Alternatively, advanced users may modify iApp-created objects as required when strict iApp updates are disabled.

Assumptions, constraints, dependencies, and risks

Recommended Practices Guide | F5 BIG-IP Local Traffic Manager and Websense TRITON AP-DATA Protector

1. **Assumption:** This recommended practices guide assumes the reader has previously deployed the F5 Air Gap Egress Inspection with SSL Intercept iApp with multi-BIG-IP architecture. An internal BIG-IP and an external BIG-IP is used to create an "Inspection Zone" or "Air Gap" providing true physical separation of internal and external traffic flows. The internal BIG-IP decrypts outbound SSL traffic so that third-party devices may reside in the inspection zone and perform shallow or deep packet inspection and optional enforcement. The external BIG-IP re-encrypts the outbound traffic and allows encrypted communications to continue to the origin server.
2. **Constraint:** Although this guide specifically references a multi-BIG-IP Air Gap Egress Inspection with SSL Intercept architecture, other deployment scenarios are possible (the F5/Websense TRITON AP-DATA protector iApp may be used in a single BIG-IP Air Gap Egress with SSL Inspection deployment and SSL bridging scenarios).

   Additional scenarios will be added to this guide in the future.
3. **Dependency:** This guide requires the specified version of the F5/Websense protector iApp as referred to herein. The latest version of this recommended practices guide shall represent the latest iApp.
4. **Risk:** Failure to execute the configuration example in this guide may result in a configuration error and/or undefined behavior. Please follow the configuration example in this guide carefully for best results.

Purpose

Recommended Practices Guide | F5 BIG-IP Local Traffic Manager and Websense TRITON AP-DATA Protector

With F5 BIG-IP local traffic manager (LTM) and Air Gap Egress Inspection with SSL Intercept, performing deep inspection of SSL traffic flows with heterogeneous

inspection technologies is possible. The Websense TRITON AP-DATA protector offers best-of-breed data loss prevention (DLP) content analysis and can be combined with other F5 product offerings to craft unique “inspection zone” use cases. This guide outlines the configuration details required to integrate F5 BIG-IP LTM with the Websense protector. The steps are a series of recommended practices to follow in order to build an integrated solution. As with any system deployment, the steps are examples and the deployed environment may not exactly match this example.

After completing this guide, you will be able to:

Deploy the Websense protector with an existing multi-BIG-IP Air Gap Egress Inspection with SSL Intercept architecture.

- Use F5 BIG-IP LTM to provide SSL visibility to the protector.
- Use F5 BIG-IP LTM to scale the protector to desired capacity.
- Use F5 BIG-IP LTM to load balance multiple Websense protectors.
- Use BIG-IP LTM to monitor the health of the Websense protector.

Please refer to the latest Air Gap Egress Inspection with SSL Intercept Deployment Guide and iApp for additional information (https://f5.com/solutions/deployment-guides/air-gap-egress-inspection-with-ssl-intercept-big-ip-v114-ltm).

In addition, this recommended practices guide will enable you to complete the following tasks:

1. Configure the F5/Websense TRITON AP-DATA protector iApp.
2. Modify Air Gap Egress Inspection with SSL Intercept iApp configuration objects to successfully integrate the Websense protector.

F5 BIG-IP LTM Air Gap Egress Inspection with SSL Intercept and Websense TRITON AP-DATA protector solution overview

The following diagram illustrates F5 Air Gap Egress Inspection with SSL Intercept when combined with the F5/Websense TRITON AP-DATA protector iApp in a multi-BIG-IP intercept Air Gap architecture:

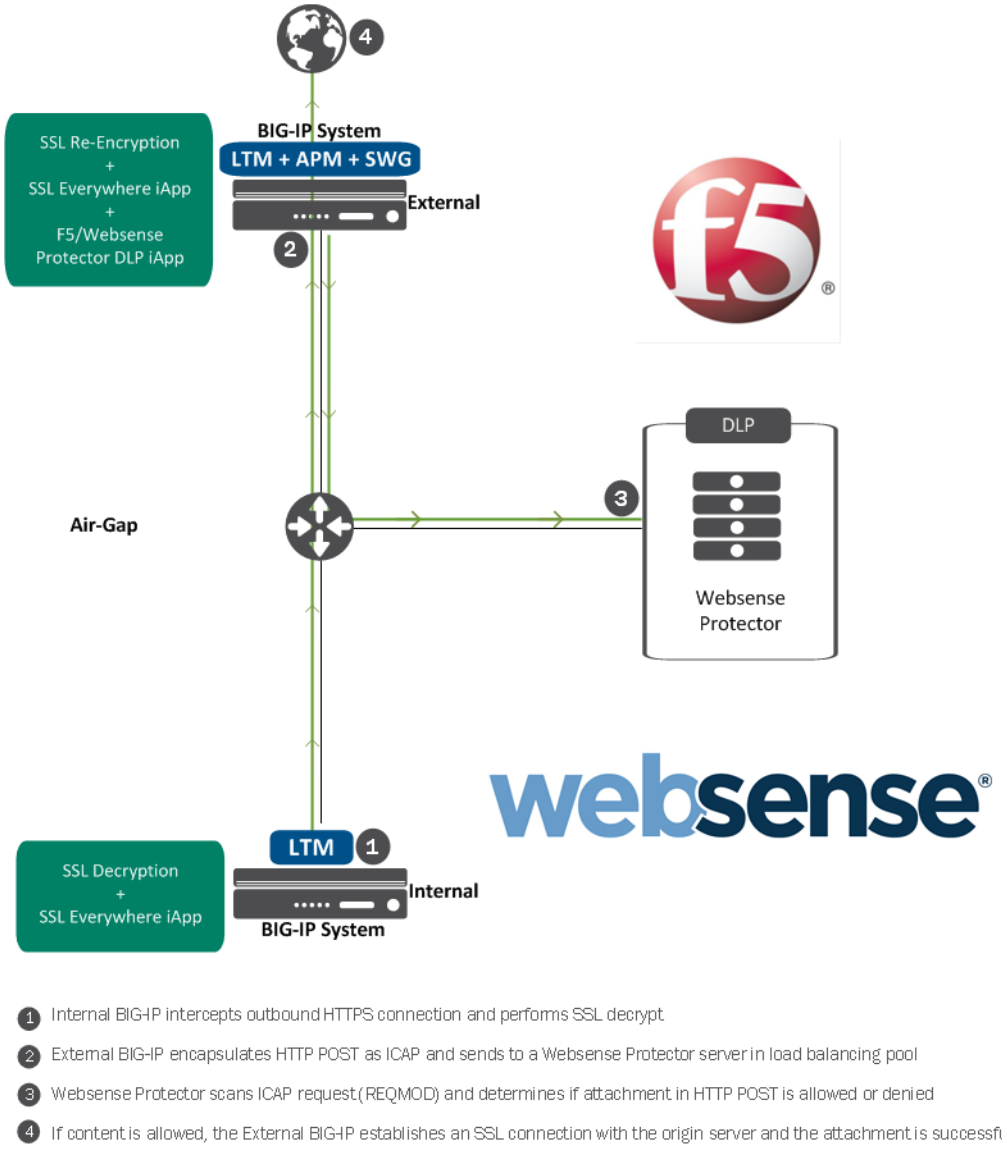


Figure 1. High-level F5/Websense TRITON AP-DATA protector DLP traffic flow

This section will provide greater detail regarding the environment overview diagram above (figure 1). There are multiple F5-supported use cases for Air Gap Egress Inspection with SSL Intercept. This recommended practices guide focuses on a single use case using a “routed mode” multi-BIG-IP Air Gap Egress Inspection with SSL Intercept scenario.

The below graphic (figure 2) and accompanying steps are for reference only. The F5/ Websense protector recommended practices in this guide are intended to “layer” on top of the F5 Air Gap Egress Inspection with SSL Intercept architecture.

The following is excerpted from the Air Gap Egress Inspection with SSL Intercept Deployment Guide (https://f5.com/solutions/deployment-guides/air-gap-egress-inspection-with-ssl-intercept-big-ip-v114-ltm).

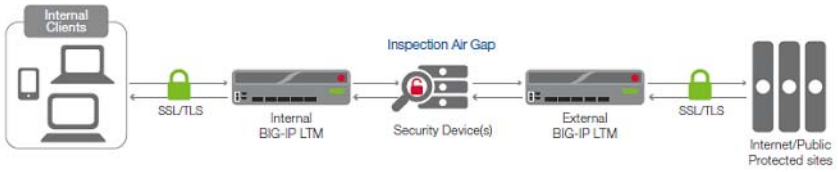


Figure 2: Air Gap Egress Inspection with SSL Intercept with multiple BIG-IPs

The traffic flow for this scenario is:

1. An internal client requests an encrypted site, and due to network routing, the browser's request is sent to the internal BIG-IP LTM.
2. The client initiates an SSL session with the internal BIG-IP LTM.
3. The BIG-IP LTM initiates a separate SSL session with the remote encrypted site (origin server), through the external BIG-IP LTM. The origin server sends its server certificate to the internal BIG-IP LTM as part of the negotiation.
4. The internal LTM generates a server certificate on the fly to match the properties of the remote host's server certificate and presents that to the client to complete the client-side SSL negotiation.
5. After completing the SSL handshake, the client sends its HTTP request. The internal BIG-IP LTM processes this request, disables server-side SSL, injects a special HTTP header, and sends the traffic to the next destination, ultimately to the external BIG-IP LTM.
6. The external BIG-IP LTM receives the request on its port 80 wildcard virtual server. This virtual server is configured with an ICAP Request Adapt Profile, and sends a sideband request to Websense TRITON AP-DATA protector
7. The Websense protector receives the request, along with any POST data sent by the client, and performs analysis. If the request violates policy, the protector returns a notification page to the external BIG-IP LTM to be delivered to the end user. Otherwise, it will notify the external BIG-IP LTM to continue processing.
8. If the request violated policy, the external BIG-IP LTM returns the notification page back to the internal BIG-IP LTM. If the request is allowed to proceed, the external BIG-IP LTM detects the special HTTP header, applies a server SSL profile, and then sends the request on to the origin server, encrypted normally on port 443.

Configuration prerequisites

This section covers various requirements needed for the recommended practices in this guide, including prerequisites, product licensing, software, and/or hardware requirements.

Infrastructure

The following prerequisites need to be addressed prior to implementing the practices in this guide. The solution utilizes the following infrastructure:

- Websense TRITON AP-DATA installation
- Websense TRITON AP-DATA protector
- Latest F5 Air Gap Egress Inspection with SSL Intercept Deployment Guide and iApp
- Administrator login credentials to both F5 BIG-IP and Websense protector devices

F5 BIG-IP

- Multiple BIG-IP hardware or virtual appliances configured for Air Gap Egress Inspection with SSL Intercept as described in the deployment guide and iApp.
- This guide is based on BIG-IP software release 11.6.0.
- This solution relies on F5 Local Traffic Manager (LTM) and requires an LTM software license with an SSL Forward Proxy feature license.
- "Best" Licensing for Access Policy Manager (APM) Secure Web Gateway (SWG) and SWG subscription.

Configuration instructions

Recommended Practices Guide | F5 BIG-IP Local Traffic Manager and Websense TRITON AP-DATA Protector

Configure Websense TRITON AP-DATA protector

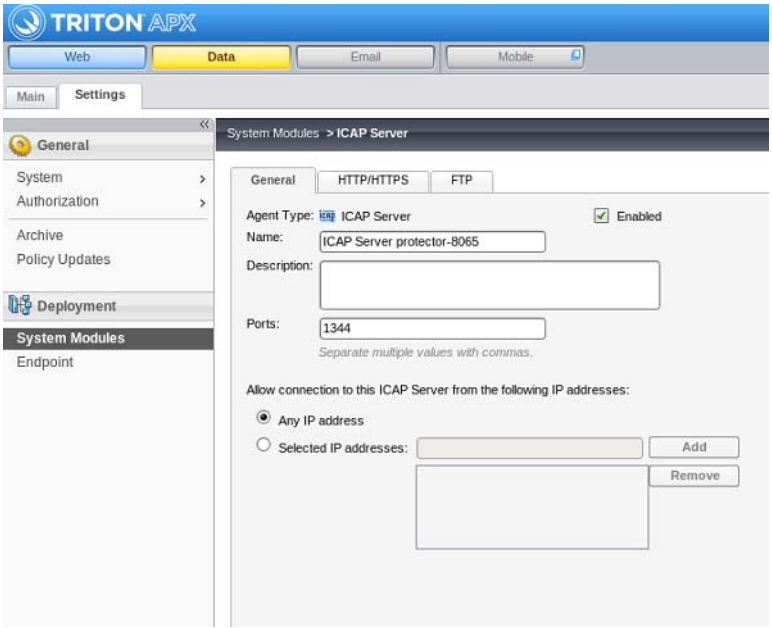
Install the Websense TRITON AP-DATA protector. This configuration only requires the ICAP integration to be configured on the protector — SPAN/Mirror and Inline/Bridge mode are not required. For additional information, see the Installation Guide for Websense TRITON AP-DATA Gateway and Discover (http://www.websense.com/content/support/library/data/v80/install/install_dss.pdf#page=44).

1. **If this is a new installation, follow the "Installing the protector software" section of the manual referenced above.**
2. **Enable ICAP**.
   a. Log on to the **TRITON AP-DATA user interface**.

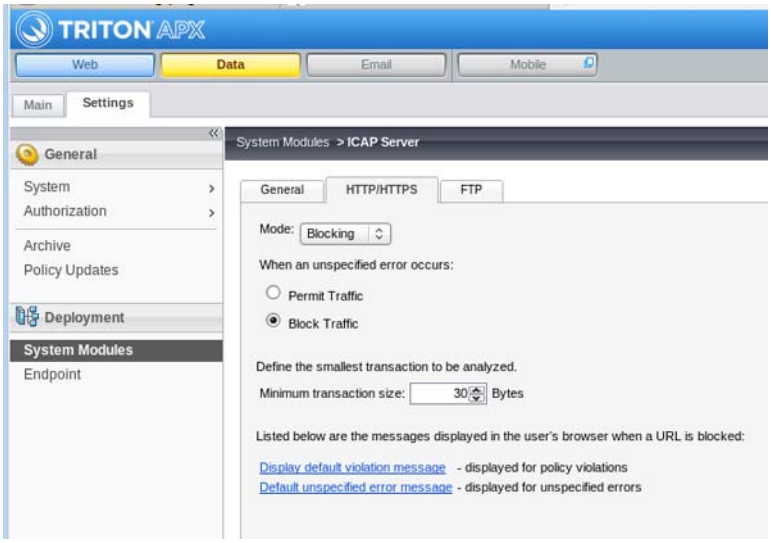
b. Navigate to **Data > Settings > Deployment > System Modules**.

c. Expand the **Protector**, and double-click the **ICAP Server**.

d. Check the **Enabled** box, and **Allow connections** from the external BIG-IP LTM.



e. In the **HTTP/HTTPS** tab, confirm the **Mode** selection is set as desired.

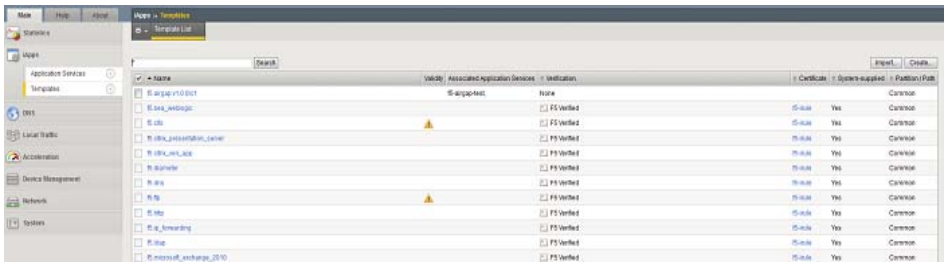


f. Click **Ok**.

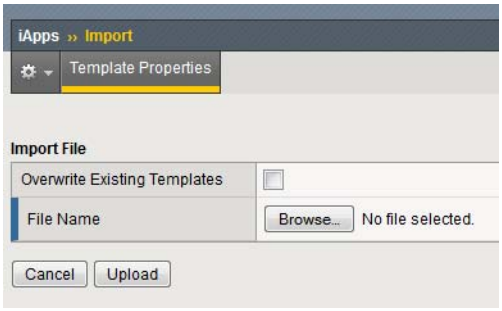
g. Click **Deploy.**

Run and configure the F5/Websense TRITON AP-DATA protector iApp

1. Obtain the F5/Websense TRITON AP-DATA protector iApp file, websense.data_protector_v1_20150206.tmpl, and save it to your desktop. The file will need to be unzipped before it can be imported to BIG-IP. You may obtain the file from here:
2. **Import the iApp**:
   a. In the **iApps tab**, go to **Templates.**
   b. Click the **Import…** button



c. Under **Import File**, in the File Name field, click the **Browse** button.



d. Select the **websense.data_protector_v1_20150206.tmpl** file saved to the desktop in step 1 above.

e. Click the **Upload** button.

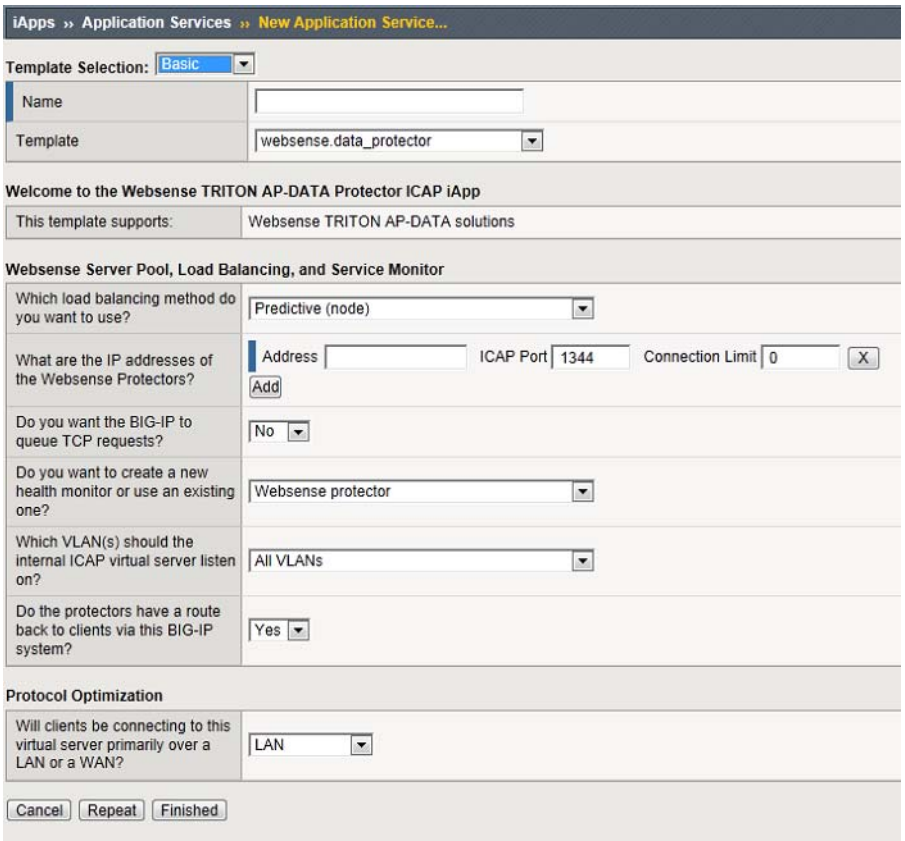
3. **Run the iApp**:

a. In the **iApps tab**, go to **Application Services** >"+."

b. Under Template Selection, in the **Name** field, enter a descriptive name for the iApp.

c. Select the template that was imported in Step 2.

d. The following screen displays:



e. From the "**Which load balancing method do you want to use?**" drop-down field, select the appropriate load balancing method. Leaving the default value is fine.

f. In response to "**What are the IP addresses of the Websense protectors?**," enter the IP address or addresses, ICAP port, and connection limit (optional) of the Websense protectors that will be used.

g. From the "**Do you want the BIG-IP to queue TCP requests?**" drop-down menu, select **No**.

h. From the "**Do you want to create a new health monitor or use an existing one?**" drop-down menu, select **Websense protector.**

Note: Selecting "Websense Protector" will create a custom ICAP health monitor developed specifically for this solution.

i. From the "**How often (in seconds) do you want the BIG-IP system to check on the health of each ICAP server?**" field, leave the default value (recommended), or enter a number in seconds.

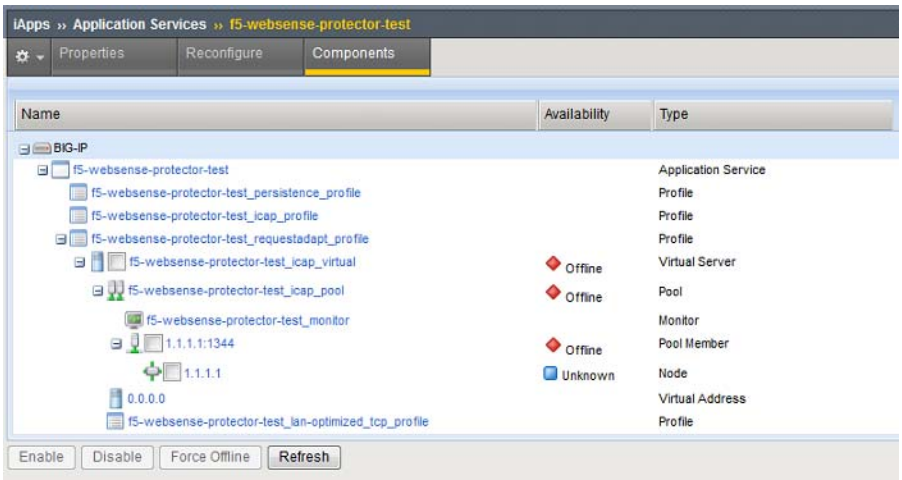
j. From the "**Which VLAN(s) should the internal ICAP virtual server listen on?**" drop-down menu, leave the default value (recommended until the solution is tested), or select the appropriate VLANs.

k. From the "**Do the ICAP servers have a route back to clients via this BIG-IP system?**" drop-down menu, select **Yes.**

l. Under **Protocol Optimization**, from the "**Will clients be connecting to this virtual server primarily over a LAN or WAN?**" drop-down menu, select the appropriate access method.

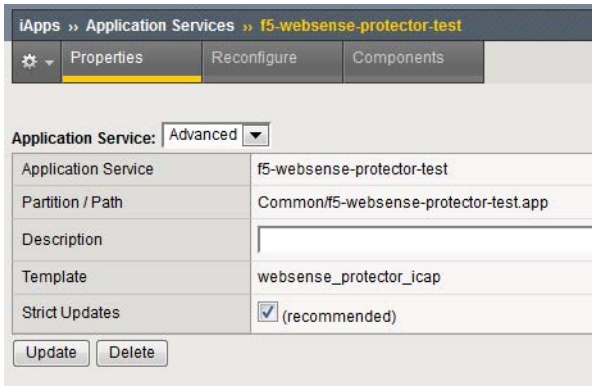
m. Click the **Finished** button.

Once you have finished, several BIG-IP configuration objects are created, as shown in the screenshot below:



n. Go to the **Properties** tab.

o. Next to **Application Service**, click the drop-down menu, and select **Advanced**.



p. De-select the **Strict Updates** check box, and click the **Update** button.

Note: This will allow BIG-IP configuration objects created with the iApp to be manually modified. It is important to select this check box again once necessary modifications have been made. Leaving this check box selected prevents accidental configuration changes. It is highly recommended that this check box stay selected.

Important

The F5 Air Gap Egress Inspection with SSL Intercept iApp must also have Strict Updates turned off in order to modify the configuration objects to reference configuration objects created using the F5/Websense TRITON AP-DATA protector iApp. Once the configuration is complete, Strict Updates can be enabled.

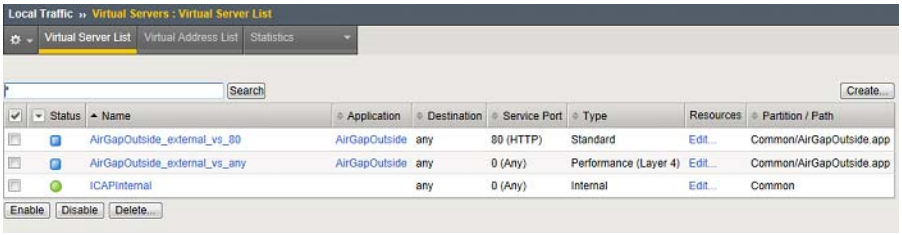
Integrate the F5/Websense TRITON AP-DATA protector iApp with an existing F5 Air Gap Egress Inspection with SSL Intercept Multi-BIG-IP deployment

Recommended Practices Guide | F5 BIG-IP Local Traffic Manager and Websense TRITON AP-DATA Protector

1. **Modify the F5/Websense ICAP Virtual Server:**

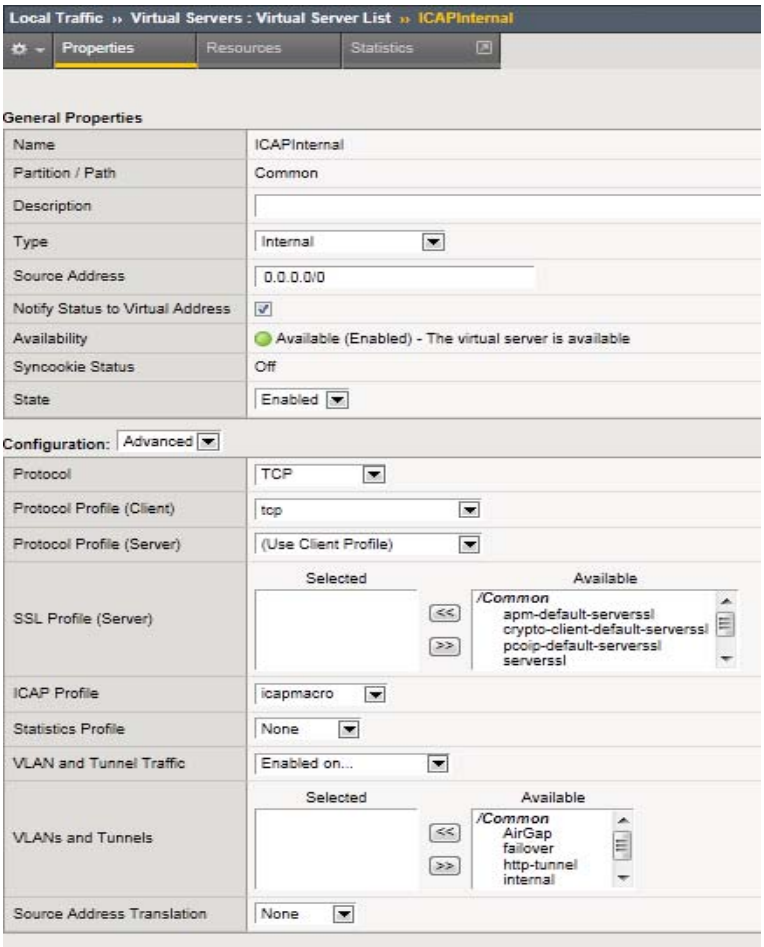
   Once the configuration objects have been created by the F5/Websense protector iApp, it is now time to integrate the solution. From the external BIG-IP, go to the

Local Traffic tab and then Virtual Servers. You should see similar F5 iApp-created objects (the names in the screenshot are examples only):



a. From the Virtual Server List, select the **ICAP Internal** virtual server.

b. Next to **Configuration**, click the drop-down menu, and select **Advanced**. From the **ICAP Profile** drop-down menu, select the ICAP profile created by the F5/Websense protector iApp.



In this example, the ICAP profile example name is “icapmacro.”

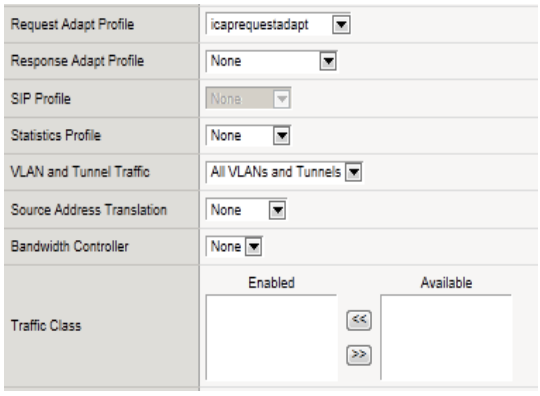
c. Click the Update button.

2. **Modify the F5 Air Gap Egress Inspection with SSL Intercept Port 80 Virtual Server.**

a. Select the **Port 80** virtual server.

b. Next to **Configuration**, click the drop-down menu, and select **Advanced**.

c. Scroll down to **Request Adapt Profile**, from the drop-down menu, select the profile created by the F5/Websense protector iApp.



In this example, the Request Adapt Profile example name is "icaprequestadapt."

d. Click the **Update** button.

Conclusion

This concludes the recommended practices guide for the deployment of F5 BIG-IP LTM with Websense TRITON AP-DATA protector. The configuration details may vary from the deployed network topology.