

SSL Intercept

Design for Core EPS Solution

Table of Contents

1. Document References and Controls 4

1.1. References 4

1.2. Version Control 4

1.3. Distribution 4

1.4. Document Sign-off 4

2. Document Overview 5

2.1. Overview 5

2.2. Audience 5

2.3. Exclusions & Caveats 5

3. Solution Overview 5

3.1. Single PoP Diagram 5

3.2. Logical Flow Diagram 6

4. Hardware & Virtual Platforms 6

4.1. Physical Platform Specifications 7

4.2. Optical Transceiver Specifications 10

4.3. Licensing Information 11

4.4. TMOS & BIG-IQ Version 11

4.5. Provisioning 11

5. Solution Components 12

5.1. Device Management 12

6. Physical Architecture 14

6.1. PoP Cabling 14

7. Logical Architecture 14

7.1. IP Addressing & Port Lockdown 14

7.2. Routing (TMM) 14

7.3. iApps 14

7.4. High Availability 14

7.5. Logging & Alerting 15

7.6. Configuration Backups 15

7.7. SSL Ciphers 16

7.8. SWG Database Updates 17

8. BIG-IP Configuration 17

8.1. Inside BIG-IPs 17

8.2. Outside BIG-IPs 18

8.3. VIPRIONs 18

9. Appendix 26

9.1. References 26

9.2. List of F5 Acronyms 26

Table of Tables

[Table 1: Disabled System Services 13](#_Toc505263861)

Table of Figures

[Figure 1: Single PoP Diagram 5](#_Toc505263862)

[Figure 2: Logical Flow Diagram 6](#_Toc505263863)

[Figure 3: VIPRION 4480 Chassis Specifications 7](#_Toc505263864)

[Figure 4: VIPRION 4450 Blade Specifications 8](#_Toc505263865)

[Figure 5: BIG-IP i10800 Platform Specifications 9](#_Toc505263866)

[Figure 6: QSFP+ 40BASE-SR Transceiver Specifications 10](#_Toc505263867)

[Figure 7: SFP+ 10GBASE-SR Transceiver Specifications 10](#_Toc505263868)

[Figure 8: PoP Physical Cabling Diagram 14](#_Toc505263869)

[Figure 9: "DEFAULT:ECDHE\_ECDSA" SSL Cipher List 16](#_Toc505263870)

[Figure 7: Bypass IPS iRule Code Sample 23](#_Toc505263871)

[Figure 7: Bypass IPS Logic iRule Code Sample 23](#_Toc505263872)

[Figure 7: Disable SSL Interception iRule Code Sample 24](#_Toc505263873)

[Figure 7: Disable SSL Interception Logic iRule Code Sample 24](#_Toc505263874)

[Figure 7: Control Debug and Alert Logging iRule Code Sample 24](#_Toc505263875)

[Figure 7: Example Debug Logic iRule Code Sample 24](#_Toc505263876)

[Figure 7: Bypass SWG iRule Code Sample 24](#_Toc505263877)

[Figure 7: Bypass SWG Logic iRule Code Sample 24](#_Toc505263878)

[Figure 7: Scan for SSL iRule Code Sample 25](#_Toc505263879)

[Figure 7: Scan for HTTP iRule Code Sample 25](#_Toc505263880)

# Document References and Controls

## References

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref. No.** | **Document Title** | **Author** | **Version** | **Date** |
|  |  |  |  |  |
|  |  |  |  |  |

## Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date Distributed** | **Author** | **Change(s)** |
| 1.0 | 2016-10-27 | Regan Anderson | Initial draft |

## Distribution

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Department** | **Contact Details** |
|  |  |  |  |

## Document Sign-off

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Department** | **Sign-off** |
|  |  |  |  |

# Document Overview

## Overview

This document details the design of the Core Enterprise Perimeter Security (EPS) Solution for Shared Services Canada (SSC) as required by 3.2.4.2.3 of the Enterprise Perimeter Security RFP.

## Audience

This document’s audience includes the following Shared Services Canada teams:

* Infrastructure Planning & Engineering
* Information Security
* Cryptography

## Exclusions & Caveats

# Solution Overview

[SALES OR RFP VERBIAGE HERE]

## Single PoP Diagram

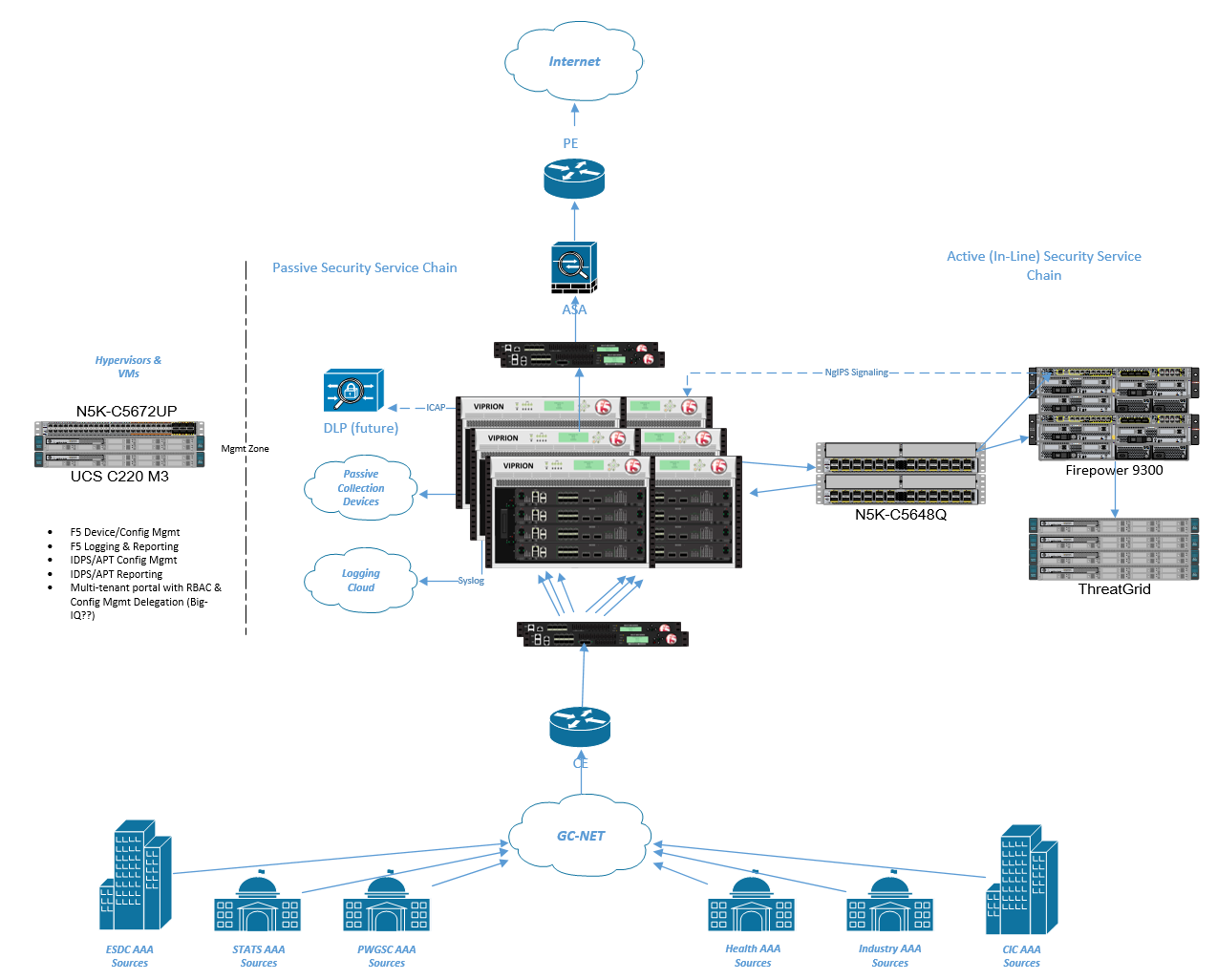
This diagram illustrates the physical and virtual components that make up a single point of presence (PoP). 

Figure 1: Single PoP Diagram

## Logical Flow Diagram

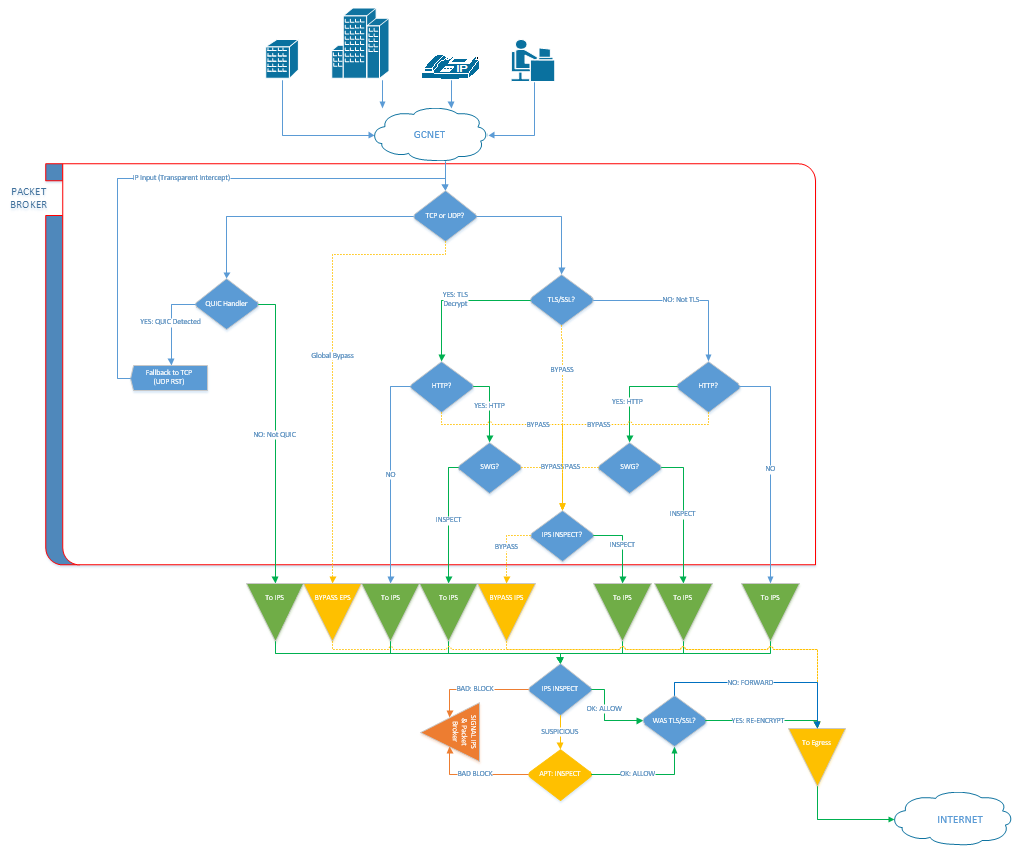
This diagram provides an in-depth view of the logic a packet will be evaluated against as it traverses this solution.

Figure 2: Logical Flow Diagram

# Hardware & Virtual Platforms

The F5 hardware platforms chosen for this solution include:

* Lab
  + Six (6) VIPRION 4480 w/ four (4) 4450 blades each
  + Four (4) BIG-IP i10800
* Datacenter-1
  + Six (6) VIPRION 4480 w/ four (4) 4450 blades each
  + Four (4) BIG-IP i10800
* Datacenter-2
  + Six (6) VIPRION 4480 w/ four (4) 4450 blades each
  + Four (4) BIG-IP i10800
* Datacenter-3
  + Six (6) VIPRION 4480 w/ four (4) 4450 blades each
  + Four (4) BIG-IP i10800

This solution will also utilize the following optical transceivers:

* VIPRION & BIG-IP QSFP+ 40BASE-SR4 Transceiver (Short Range, 100 m)
* BIG-IP & VIPRION SFP+ 10GBASE-SR Transceiver (Short Range)

The virtual platforms chosen for this solution include:

* Lab
  + Two (2) BIG-IQ Centralized Management (VE)
  + Three (3) BIG-IQ Data Collection Device (VE)
* Production Management Zone
  + Two (2) BIG-IQ Centralized Management (VE)
  + Three (3) BIG-IQ Data Collection Device (VE)

## Physical Platform Specifications

### VIPRION 4480 Chassis



Figure 3: VIPRION 4480 Chassis Specifications

### VIPRION 4450 Blade

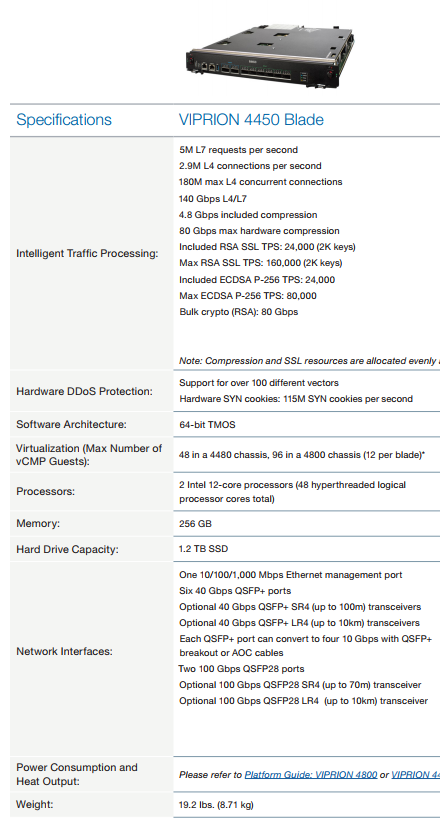


Figure 4: VIPRION 4450 Blade Specifications

### BIG-IP i10800

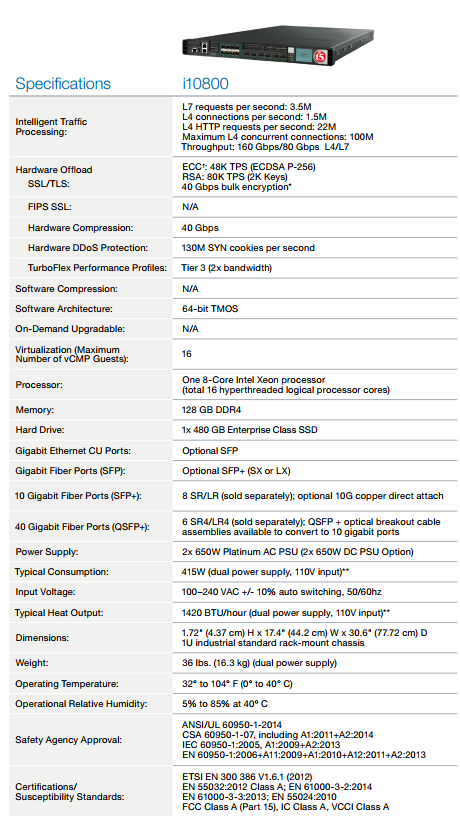


Figure 5: BIG-IP i10800 Platform Specifications

## Optical Transceiver Specifications

### QSFP+ 40BASE-SR4 Transceiver



Figure 6: QSFP+ 40BASE-SR Transceiver Specifications

### SFP+ 10GBASE-SR Transceiver



Figure 7: SFP+ 10GBASE-SR Transceiver Specifications

## Licensing Information

Platform licensing for the deployed hardware includes:

* VIPRION 4480
  + BIG-IP Local Traffic Manager (LTM)
  + BIG-IP DNS
  + BIG-IP Advanced Firewall Manager (AFM)
  + BIG-IP Application Security Manager (ASM)
  + BIG-IP Access Policy Manager (APM)
  + BIG-IP Secure Web Gateway (SWG)
  + BIG-IP Application Visibility and Reporting (AVR)
  + Advanced Routing Module
  + SSL Forward Proxy
  + IP Intelligence Services
* BIG-IP i10800
  + BIG-IP Local Traffic Manager (LTM)
  + BIG-IP Application Visibility and Reporting (AVR)

In addition to the hardware above, the following Virtual Edition licenses will be used:

* BIG-IQ Centralized Management (VE)
* BIG-IQ Data Collection Device (VE)

## TMOS & BIG-IQ Version

The primary decision factors when determining which version of TMOS and BIG-IQ to utilize in this environment were functionality, stability, and support. For this reason, TMOS 13.1.0.2 with the latest hotfix has been selected as the target version for all BIG-IPs and VIPRIONs, as it provides all the functionality required by SSC in addition to long term support. This release is currently scheduled to reach End of Software Development in December 2022 and End of Technical Support in December 2023.

The targeted BIG-IQ Centralized Management version is 5.4.0 with the latest hotfix. This version of BIG-IQ is the most feature-rich and provides the most advanced reporting capabilities. This release is currently scheduled to reach End of Software Development in December 2019 and End of Technical Support in December 2020.

## Provisioning

Module provisioning for the deployed hardware includes:

* VIPRION 4480
  + BIG-IP Local Traffic Manager (LTM)
  + BIG-IP Advanced Firewall Manager (AFM)
  + BIG-IP Application Security Manager (ASM)
  + BIG-IP Access Policy Manager (APM)
  + BIG-IP Secure Web Gateway (SWG)
  + BIG-IP Application Visibility and Reporting (AVR)
  + IP Intelligence Services
* BIG-IP i10800
  + BIG-IP Local Traffic Manager (LTM)
  + BIG-IP Application Visibility and Reporting (AVR)

# Solution Components

## Device Management

### Management IP Addressing

Each BIG-IP will be configured with two management IP addresses. One address will be used for access to the BIG-IP GUI (HTTPS) & CLI (SSH), while the other will provide access to AOM (Always-On Management / console via SSH).

Each VIPRION will be configured with five management IP addresses. One address will be used to manage the chassis / primary blade (Management IP Address) and will provide access to the BIG-IP GUI (HTTPS) & CLI (SSH), while the other four addresses will provide direct access to each blade installed in the system (Cluster Member IP Addresses) in addition to facilitating critical intra-cluster communication.

Failure to configure the cluster member IP address on all slots may result in failover daemon (sod) communication issues.

### Management Routing

By default, all BIG-IPs will be configured with a default gateway on their management interface. This will automatically create a 0.0.0.0/0 management route. To ensure the Websense database download mechanism utilizes the management interface on the VIPRIONs, two additional /1 routes will be created. These more specific management routes (default metric of 9) will take precedent over TMM routes (default metric of 0) for all management traffic destined for the Internet.

Additional management routes may be created to ensure other management related services egress through the management interface (e.g. NTP, SNMP).

### Device Certificates

SSC will provide device certificates signed by their internal or external Certificate Authority (CA). These certificates will include the Client Authentication and Server Authentication Extended Key Attributes, a requirement to ensure potential future interoperability with other F5 products is supported. Certificate Signing Requests (CSRs) will be generated from each BIG-IP.

### Sensitive Data Storage

The BIG-IP system uses Secure Vault, a super-secure SSL-encrypted storage system, to securely store sensitive data such as SSL key passphrases, built-in monitor passwords, users, and administrator and services passwords.

Each BIG-IP device comes with a unit key and a master key. Upon first boot, the BIG-IP system automatically creates a master key for encryption purposes. The master key encrypts sensitive data, such as AAA servers, admin passwords/secrets, and SSL private key passphrases. Additionally, the system uses the master key to synchronize certificates between BIG-IP devices. Further increasing security, the master key is also encrypted by the unit key, which is an AES 256 symmetric key. The unit key represents the device and is stored in EEPROM hardware.

### Private Key Storage (FIPS 140-2 HSM)

Private keys used for inbound and outbound SSL decryption operations will be stored in the on-board FIPS Level 2 certified F5 Device Cryptographic Module on each VIPRION. Private keys relating to inbound/outbound SSL decryption are not required on the BIG-IP i10800 ADCs. Add more about the module once it is certified.

### Management Services

#### NTP

F5 recommends configuring at least three unique NTP servers. It is important to maintain accurate time on all systems for accurate log timestamps. NTP traffic will be routed via the management interface.

#### DNS

F5 recommends configuring at least two unique DNS servers. These DNS servers are used to resolve the Websense database download server as well as integrated AAA services. DNS traffic will be routed via the management interface.

#### Syslog

Important system events are sent to one or more remote syslog servers. Syslog traffic will be routed via the management interface.

#### SNMP

The F5 BIG-IP system supports SNMP versions: v1, v2c, and v3. The BIG-IP system implementation of SNMP is based on the well-known SNMP package, Net-SNMP.

The BIG-IP system complies with the standard SNMP implementation, by including both an SNMP agent, a set of standard SNMP MIB files, and a set of enterprise MIB files (those that are specific to the BIG-IP system). The enterprise and vendor specific MIB files reside on both the BIG-IP system and system running the SNMP manager. SNMP traffic will be routed via the management interface.

### System Services

The following BIG-IP system daemons are not required in this environment and will be disabled:

|  |  |  |
| --- | --- | --- |
| Daemon | Description | Notes |
| big3d | The big3d process is used by BIG-IP GTM and Enterprise Manager to collect statistics from remotely managed BIG-IP LTM devices. This process is also used by BIG-IP GTM for auto-discovery of objects. | If GTM or Enterprise Manager is added to the environment this daemon should be re-enabled. |
| named | The named daemon is a DNS server included in BIND. | This daemon is not required for LTM or APM functionality. |

Table 1: Disabled System Services

### Management Routing

#### Inbound administrative connections

Inbound connections sent to the BIG-IP management IP address which arrive on the management interface are processed by the Linux operating system. Inbound connections sent to a Self IP which arrive on a TMM interface are processed by TMM. If the Self IP is configured to allow a connection to the destination service port of a local management service (e.g. SSH), TMM hands the connection off to the Linux operating system, which then processes the connection request.

No BIG-IP management/administrative services will be exposed via TMM interfaces/Self IPs.

#### Outbound administrative connections

Outbound connections sent from the BIG-IP system by administrative applications (SNMP, SSH, NTP, etc.) are processed by the Linux operating system. These connections may either use the management address or a Self IP address as the source address. The BIG-IP system compares the destination address to the management routing table (default metric of 9) and the TMM routing table (default metric of 0) to determine the interface through which the BIG-IP system routes the traffic.

***Note****: This behaviour applies only to unsolicited outbound traffic: traffic that is not in response to a request originated by a remote host. A response to a request originated by a remote host is returned to the last MAC address traversed by the inbound request.*

Management routes will be configured to ensure management related services (NTP, DNS, SNMP, Syslog) are routed via the BIG-IP management interface.

More information about this behaviour can be found here:  
<http://support.f5.com/kb/en-us/solutions/public/13000/200/sol13284.html>

# Physical Architecture

The following sections describe the physical integration points for the solution and highlight cabling requirements.

## PoP Cabling

Four (4) BIG-IP i10800 ADCs and six (6) VIPRION 4480 chassis, each populated with four (4) 4450 blades, will be installed in the lab environment as well as each of the three (3) PoPs.

[ADD PHYSICAL CABLING DIAGRAM]

Figure 8: PoP Physical Cabling Diagram

# Logical Architecture

The following section describes logical architecture components of the solution.

## IP Addressing & Port Lockdown

Each BIG-IP will require a single non-floating Self IP for each VLAN it resides on. Floating Self IP’s are required on the inside and outside BIG-IP i10800 pairs to facilitate client traffic failover from one BIG-IP to the other – this floating IP will be shared by both BIG-IPs in a Sync-Failover group and will be a member of traffic-group-1. The following VLANs on the BIG-IP i10800s do not require a floating Self IP:

* HA VLAN

All Self IPs will be configured with a port lockdown setting of “Allow None.” This will prevent access to the BIG-IP management plane through a TMM interface. The only exception to this configuration are the HA Self IPs, which will be configured with a port lockdown setting of “Allow Default.” This setting will permit HA communication between devices in an HA pair/cluster over their respective dedicated L2 (non-routed) HA VLANs.

## Routing (TMM)

This solution utilizes statically configured routes to forward traffic through the security service chain as well as between the internal/GC-NET and external/Internet zones.

## iApps

iApps is a user-customizable framework for deploying applications that enables a BIG-IP administrator to templatize sets of functionality. iApps provide the foundation of the SSL Intercept solution that is deployed on each VIPRION chassis.

## High Availability

This section only applies to the BIG-IP i10800 ADCs that are deployed as high availability (HA) pairs. The VIPRIONs that form part of this solution are standalone units and do not participate in an HA configuration.

### Device Service Clusters (DSC) / Device Groups

The inside and outside BIG-IP i10800 ADCs will be deployed in HA pairs, also known as Device Service Clusters or Device Groups. Each of these pairs will be configured in a single Sync-Failover device group (one device group per pair). To align with F5 recommended practices, this device group will not be configured with automatic configuration synchronization (Automatic Sync) but will be configured to synchronize the full configuration during a configuration sync operation (Full Sync).

The “High Availability” section does not apply to the VIPRION chassis’ as they will be deployed as standalone units.

### Traffic Groups

All BIG-IP HA pairs will be configured with a single traffic group, traffic-group-1. This configuration will facilitate an Active/Standby failover group for BIG-IPs that are in an HA pair. These traffic groups will be configured to utilize the “HA Group” failover method. To minimize network disruption during failover, a MAC Masquerade Address will be configured for the traffic groups associated with HA pairs. The recommended practice for selecting an appropriate and unique MAC masquerade address outlined in SOL3523 will be followed.

SOL3523: Choosing a unique MAC address for MAC masquerade  
<https://support.f5.com/kb/en-us/solutions/public/3000/500/sol3523.html>

### ConfigSync

ConfigSync will be configured to utilize the HA VLAN and HA Self IPs.

### Network Failover

Unicast Network Failover will be implemented and will utilize the Management Addresses as well as the HA Self IPs as local addresses. This provides a diverse path for network heartbeats (Management interface & TMM interfaces), and should reduce the risk of a split-brained scenario (e.g. Active/Standby pair going Active/Active).

A failover event may be trigged due to one of the following reasons:

* Manually by an administrator
* Failure of a system critical daemon
* Failure of a system (e.g. loss of power)
* Trigged by real-time HA Group scoring

In a two device, active/standby cluster, when failover has been initiated for a traffic group, the traffic group will become active on the standby BIG-IP. The newly active BIG-IP will send gratuitous ARPs (GARPs) for all of the virtual IPs (e.g. virtual server IPs, SNAT IPs, floating IPs) it is now active for. This device will remain active until the next failover event occurs.

### Mirroring

The Primary Local Mirror Address will be configured to use the HA Self IP. Connection mirroring will be configured on the BIG-IP i10800 ADCs to minimize the disruption to clients during a failover event between ADCs.

## Logging & Alerting

Default BIG-IP logging & alerting will be performed via the local logging facilities, syslog, and via SNMP traps. MCP audit logging will be set to “Verbose” in order to log configuration changes made on the system (MCP audit log events are stored locally and sent via syslog).

The BIG-IP rotates its local log files after 7 days to prevent disk space exhaustion.

## Configuration Backups

BIG-IQ Centralized Management platform will be configured to collect configuration backups on all BIG-IPs

## SSL Ciphers

Cryptography in this environment must conform to the SSC’s cryptography standards. The following SSL cipher string will be utilized on all Client & Server SSL profiles to adhere to these requirements:

DEFAULT:ECDHE\_ECDSA

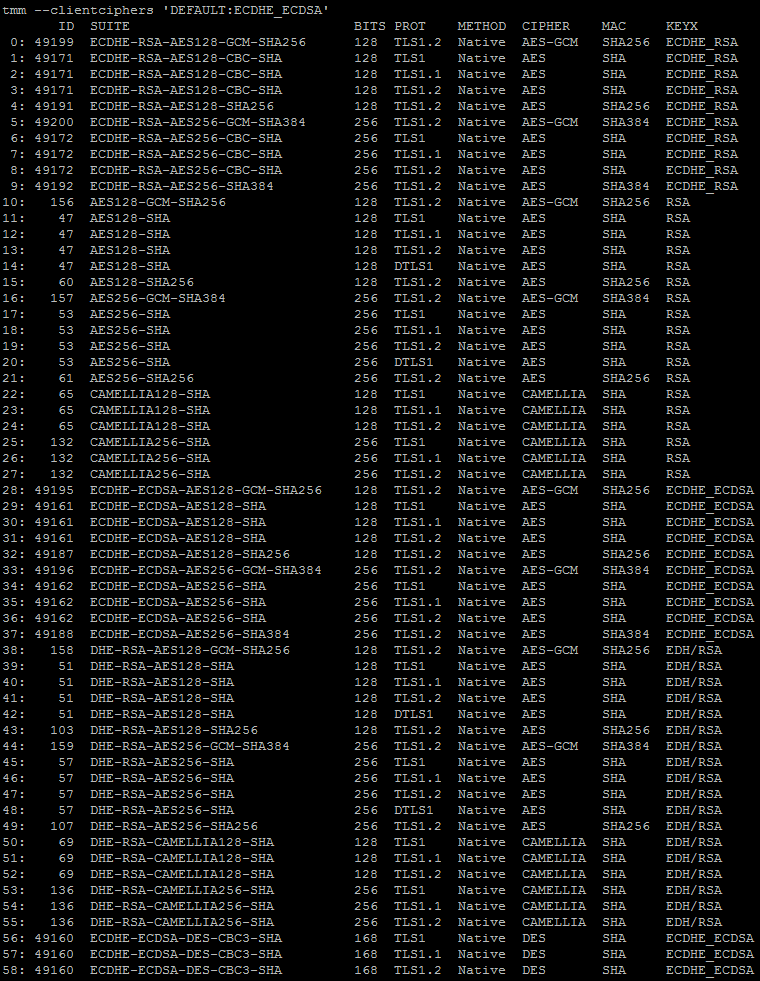
This produces the following list of ciphers (ordered by preference):  


Figure 9: "DEFAULT:ECDHE\_ECDSA" SSL Cipher List

## SWG Database Updates

To obtain the most recent updates to the Websense database the VIPRION systems must have direct access to downloads.websense.com via TCP port 80 or alternatively access via a proxy. The BIG-IP will utilize the management interface to connect to the download server.

Database updates occur in the following intervals:

Master – Daily, during the configured download schedule window. It is recommended that this download is scheduled for a period of lower network utilization (e.g. after business hours).

RTU – Every ten minutes.

ACE – Every fifteen minutes.

The VIPRIONs will require outbound access to download.websense.com on TCP/80 via their management interface/IP or indirectly through a proxy.

# BIG-IP Configuration

There are two active/standby pairs of BIG-IP i10800’s in each PoP and six standalone VIPRIONs. One pair BIG-IP i10800 pair resides of the “inside” of the solution and is closest to GC-NET, while another pair resides on the “outside” of the solution and is closest to the Internet. These two pairs of BIG-IPs forward IP traffic between GC-NET and the Internet by load balancing that traffic to the standalone VIPRION chassis, which are sandwiched between the inside and outside BIG-IP pairs (refer to “Figure 1 – Single PoP Diagram” for a visual representation). This design allows the solution to easily scale-out by simply adding additional VIPRION chassis to the inbound/outbound load balancing pools.

## Inside BIG-IPs

### BIG-IQ Analytics iApp

The BIG-IQ Analytics iApp is deployed on this pair of BIG-IPs and facilitates the collection of statistical and state data by BIG-IQ Centralized Management.

### BIG-IP LTM Configuration

The BIG-IP LTM configuration on the inside HA pair of BIG-IP i10800 ADCs consists of a series of virtual servers which are designed to pass traffic between the inside CE router and the load balanced VIPRIONs.

There are a total of eight (8) virtual servers which perform the following functions:

Bidirectional Forwarding Detection (BFD) forwarding virtual server- This virtual server facilitates the forwarding of BFD packets through the Core EPS Solution.

Border Gateway Protocol (BGP) forwarding virtual server- This virtual server facilitates the forwarding of BGP packets through the Core EPS Solution.

In2Out-(any/tcp/udp)-vs virtual servers – These virtual servers facilitate the load balancing of IP traffic from GC-NET to the VIPRIONs. The BIG-IP uses the Least Connections load balancing method to ensure connections are equally distributed amongst the standalone VIPRIONs. TCP/IP based analytics are captured on the client-side (GC-NET) of the In2Out-tcp-vs virtual server and collects statistics on the following entities: Virtual Server, Client IP, Client Subnet, Next Hop Ethernet Address, Continent, Country, Region, City, and Postal Code.

Out2In-(any/tcp/udp)-vs virtual servers – These virtual servers facilitate the forwarding of IP traffic from the VIPRIONs to GC-NET. TCP/IP based analytics are captured on the client-side (Internet) of the Out2In-tcp-vs virtual server and collects statistics on the following entities: Virtual Server, Client IP, Client Subnet, Next Hop Ethernet Address, Continent, Country, Region, City, and Postal Code.

## Outside BIG-IPs

### BIG-IQ Analytics iApp

The BIG-IQ Analytics iApp is deployed on this pair of BIG-IPs and facilitates the collection of statistical and state data by BIG-IQ Centralized Management.

### BIG-IP LTM Configuration

The BIG-IP LTM configuration on the outside HA pair of BIG-IP i10800 ADCs consists of a series of virtual servers which are designed to pass traffic between the outside PE router/L2 firewall and the load balanced VIPRIONs.

There are a total of eight (8) virtual servers which perform the following functions:

Bidirectional Forwarding Detection (BFD) forwarding virtual server- This virtual server facilitates the forwarding of BFD packets through the Core EPS Solution.

Border Gateway Protocol (BGP) forwarding virtual server- This virtual server facilitates the forwarding of BGP packets through the Core EPS Solution.

In2Out-(any/tcp/udp)-vs virtual servers – These virtual servers facilitate the load balancing of IP traffic from the VIPRIONs to the Internet. TCP/IP based analytics are captured on the client-side (GC-NET) of the In2Out-tcp-vs virtual server and collects statistics on the following entities: Virtual Server, Client IP, Client Subnet, Next Hop Ethernet Address, Continent, Country, Region, City, and Postal Code.

Out2In-(any/tcp/udp)-vs virtual servers – These virtual servers facilitate the forwarding of IP traffic from the Internet to the VIPRIONs. The BIG-IP uses the Least Connections load balancing method to ensure connections are equally distributed amongst the standalone VIPRIONs. TCP/IP based analytics are captured on the client-side (Internet) of the Out2In-tcp-vs virtual server and collects statistics on the following entities: Virtual Server, Client IP, Client Subnet, Next Hop Ethernet Address, Continent, Country, Region, City, and Postal Code.

## VIPRIONs

The VIPRION configuration is encapsulated in four iApps. The purpose and function of each iApp is described in the following sections.

### Platform Initialization iApp

This iApp manages module provisioning, the configuration of global system settings, and the configuration network trunks (link aggregation) to the Cisco infrastructure.

This iApp is deployed after license activation and initial base configuration. The iApp performs the following configuration tasks:

* Module Provisioning – Nominally provisions BIG-IP AFM, ASM, APM, AVR, LTM, and SWG.
* Network Trunk – Establishes LACP-enabled trunk to Cisco Nexus 3K switches.
* System Logging – Sets MCPD logging level to verbose. This enables logging of all user-initiated changes to the system configuration. Allows administrator to define logging level (Informational, Error, or Debug) for the following Local Traffic services:
  + HTTP
  + HTTP Compression
  + IP
  + Layer 4
  + Network
  + SSL
  + Traffic Management OS

### Base Configuration iApp

This iApp deploys configuration that is specific to the SSL Intercept functionality at a system/global level (supports all tenants). This iApp is deployed after the Platform Initialization iApp and performs the following configuration tasks:

* Hostname – Allows administrator to define device’s hostname.
* Management Access – Configures secure ciphers (i.e. no SSLv2/v3) and sets idle timeouts to 600 seconds.
* Networking
  + VLANs – Allows administrator to define ingress (inside) and egress (outside) VLAN tags.
  + Self IPs – Allows administrator to define ingress (inside) and egress (outside) Self IPs.
  + Static Routes – Allows administrator to define default routes (gateways) to the Internet as well as the internal network.
    - IPv4-Internet-DefaultRoute – Default route pointing toward Internet. The next hop is the active outside BIG-IP i10800.
    - IPv4-Internal\_DefaultRoute – Default route pointing toward GC-NET. The next hop is the active inside BIG-IP i1800.
* DNS Servers – Allows the administrator to define DNS lookup servers and search domains that are used by the system for name resolution.
* NTP Servers – Allows the administrator to define NTP servers that are used for clock synchronization.
* SMTP Servers – Allows the administrator to define an SMTP server that can be used to e-mail custom & scheduled reports.
* Syslog – Allows the administrator to define remote syslog servers that will be used to collect system log data.
* Blacklist Download – Configures periodic download of Customer hosted URL blacklist.
  + The blacklist download functionality utilizes iCall to periodically execute an on-box Python script. This script fetches a URL blacklist from a Customer defined/hosted webserver and then parses the contents of the list. Once the list has been parsed it is loaded into the VIPRION’s global URL blacklist category and is immediately evaluated against subsequent HTTP requests.
* Global Category Bypass Data Group – Creates data group that maintains a list of globally bypassed URL categories (e.g. Health, Financial and Data Services). SSL/TLS connections that match categories defined in this data group bypass SSL interception.
* iRules – Deploys iRule logic that handles connection processing and SSL Intercept functionality.
  + sslintercept-ingress-tcp-rule - The primary function of this iRule is to detect TLS handshakes and determine whether to intercept or bypass the TLS connection based on the following criteria:
    - Global bypass - ability to bypass all TLS
    - Tenant bypass - ability to bypass all TLS from one or more tenants
    - Global category bypass - ability to bypass TLS based on global category list
    - Tenant category bypass - ability to bypass TLS based on tenant custom category

HTTP and intercepted HTTPS are passed to a second SWG virtual server which performs additional processing (e.g. blacklist checks) whereas bypassed HTTPS is routed through the inspection zone to the egress virtual server. Connections that match a defined list of server speaks first (SSF) ports are passed to a second SSF virtual server, which is configured to support SSF protocols.

* + sslintercept-service-swg-tcp-rule - The purpose of this iRule is to update the signalling table (FPSSLTRACK) with the updated ephemeral source port of a client connection as the port typically changes as the connection traverses the SWG service.
  + sslintercept-ingress-ssf-tcp-rule - The primary function of this iRule is to support server speaks first (SSF) protocols. This iRule also attempts to detect TLS handshakes and determine whether to intercept or bypass the TLS connection based on the following criteria:
    - Global bypass - ability to bypass all TLS
    - Tenant bypass - ability to bypass all TLS from one or more tenants
    - Global category bypass - ability to bypass TLS based on global category list
    - Tenant category bypass - ability to bypass TLS based on tenant SSF custom category
  + tls-detect-rule - The purpose of this iRule is to detect an SSL/TLS ClientHello in a flow and bypass the inspection device (e.g. SourceFire) if SSL/TLS is detected. Instead of passing through the inspection layer, the SSL/TLS flow is sent directly to the egress virtual server.
  + QUIC\_detect\_rule - The purpose of this iRule is to detect an QUIC protocol connection attempt and reject it. This will force Chome browsers to fall back to standard TCP based TLS connections.
  + service-pool-healthcheck - The purpose of this iRule is to drop a connection (e.g. BGP/BFD) if the L2 service pool is offline. This facilitates the failure of a PoP if the L2 inspection device fails to pass traffic.
  + sslintercept-egress-tcp-rule - The purpose of this iRule is to determine whether to enable client SSL (intercepted SSF TLS) and server SSL (intercepted TLS) profiles before sending traffic to the outbound gateway.
  + sslintercept-library-rule – This iRule contains a list of commonly used procedures, such as the HTTP protocol detection procedure.
* Profiles – Deploys profiles that support the SSL Intercept solution.
  + Client & Server SSL – A combination of client and server SSL profiles are utilized in the SSL Intercept solution. These profiles facilitate the SSL forward proxy behaviour of the VIPRIONs including the interception and bypass of SSL/TLS. To intercept SSL/TLS connections, a subordinate CA certificate and private key are installed on each VIPRION. Each tenant has the option of using the default provided by Shared Services Canada or their own. In either case, the provided certificate and key must have key signing authority and must be trusted by the clients residing within that tenant’s environment.
  + FastL4 – Tunes virtual servers to optimize the processing of specific types of traffic when full proxy functionality is not required.
  + FTP – Facilitates the support of FTP connectivity through the SSL Intercept solution.
  + DoS – The Global-DoS profile is assigned to GC-NET and Internet facing virtual servers and protects the system as well as upstream and downstream devices against a variety of IP-based DoS attack vectors.
  + Logging – The logging profiles facilitate the logging of system and connection information to local and remote logging destinations.
* Pools
  + Inside-NextHop – Contains IP of next-hop gateway (active inside BIG-IP i10800) for traffic originating from the Internet.
  + Outside-NextHop – Contains IP of next-hop gateway (active outside BIG-IP i10800) for traffic originating from GC-NET.
  + ICAP – Contains IP(s) of Data Loss Prevention (DLP) servers.
  + PCAP – Contains IP of passive packet capture device.
  + High Speed Logging (HSL) – Contains IP(s) HSL server(s) that security related log events are sent to.
* URL Categories
  + Global-Blacklist – This category contains a list of globally (across all tenants) blacklisted URLs and is used by the SWG module to evaluate and block matching client requests. This category is automatically updated by the Blacklist Download function described above.
* Firewall Policies & Rules
  + Global-Blacklist – This firewall policy matches and blocks IP addresses (source and/or destination) that have been defined in the Blacklist-IPs address list.
* Virtual Servers
  + Bidirectional Forwarding Detection (BFD) forwarding virtual server- This virtual server facilitates the forwarding of BFD packets through the Core EPS Solution.
  + Border Gateway Protocol (BGP) forwarding virtual server- This virtual server facilitates the forwarding of BGP packets through the Core EPS Solution.

### Tenant Configuration iApp

This iApp deploys configuration that is specific to the SSL Intercept functionality at a tenant level. An instance of this iApp is deployed for every tenant of this solution and these deployments take place after the Base Configuration iApp has been deployed. The Tenant Configuration iApp performs the following configuration tasks:

* Networking
  + Route Domains – Two tenant specific route domains are used to forward traffic through the two Layer 2 IPS devices.
  + VLANs – Four tenant specific VLANs are used to facilitate traffic forwarding through the two Layer 2 IPS devices.
  + Self IPs – Four tenant specific Self IPs are used to facilitate traffic forwarding through the two Layer 2 IPS devices.
* Access – An access profile/policy as well as per-request policy are used for authentication and URL filtering (detailed below).
* URL Categories
  + Bypass - This category contains a list of tenant defined bypass URLs and is used by the SSL Intercept solution to determine whether a connection should be bypassed (skip SSL interception).
  + SSF-Bypass – This category contains a list of tenant defined bypass URLs and is used by the SSL Intercept solution to determine whether a server speaks first (SSF) connection should be bypassed (skip SSL interception).
  + Block – This category contains a list of tenant defined blacklisted URLs and is used by the SWG module to evaluate and block matching client requests.
* Profiles
  + Analytics – These profiles allow you to visually analyze the performance of web applications, TCP traffic, and overall system statistics.
    - HTTP – HTTP-based analytics are captured on the Captive Portal, Hosted WebApp, and SWG virtual servers. This profile collects Max TPS, Throughput, and Page Load Time metrics as well as the following entities: URLs, Countries, Client IP, Response Codes, User Agents, Methods, and OS and Browers.
    - TCP – TCP/IP-based analytics are captured on the client-side and server-side of the FTP, Inside Ingress TCP/SSF-TCP, and Outside Ingress TCP virtual servers and collects statistics on the following entities: Virtual Server, Client IP, Continent, Country, and Region.
  + Client & Server SSL – A combination of client and server SSL profiles are utilized in the SSL Intercept solution. These profiles facilitate the SSL forward proxy behaviour of the VIPRIONs including the interception and bypass of SSL/TLS. To intercept SSL/TLS connections, a subordinate CA certificate and private key are installed on each VIPRION. Each tenant has the option of using the default provided by Shared Services Canada or their own. In either case, the provided certificate and key must have key signing authority and must be trusted by the clients residing within that tenant’s environment. Inherits defaults defined by related global SSL profiles.
  + FastL4 – Tunes virtual servers to optimize the processing of specific types of traffic when full proxy functionality is not required. Inherits defaults defined by related global FastL4 profiles.
  + FTP – Facilitates the support of FTP connectivity through the SSL Intercept solution. Inherits defaults defined by global FTP profile.
  + ICAP – The ICAP profile facilitates communication to the ICAP service.
  + HTTP – Defines specific HTTP/HTTPS handling settings required for supporting HTTP/HTTPS web applications that are WAF protected.
  + Logging – The logging profiles facilitate the logging of system, connection, and request information to local and remote logging destinations.
  + SSH Proxy – This profile provides granular control of SSH sessions that pass through the SSL Intercept solution, including the ability to log different SSH actions.
* Pools – Two tenant-specific pools facilitate the forwarding of traffic through the Layer 2 IPS devices.
* Virtual Servers
  + Inside-ingress-tcp-vs – This virtual server receives TCP traffic forwarded from the active inside BIG-IP i10800. The sslintercept-ingress-tcp-rule iRule is assigned to this virtual server.
  + Inside-ingress-udp-vs – This virtual server receives UDP traffic forwarded from the active inside BIG-IP i10800. This traffic is forwarded to the Layer 2 IPS pool for inspection.
  + Inside-ingress-any-vs – This virtual server receives non-TCP/UDP traffic forwarded from the active inside BIG-IP i10800. This traffic is forwarded to the Layer 2 IPS pool for inspection.
  + Service-swg-tcp-vs – This virtual receives HTTP and decrypted HTTPS traffic from Inside-ingress-tcp-vs and applies SWG policies to the traffic such the global and tenant-specific blacklists. A webcache/ramcache profile, which enables caching of web content, is assigned to this virtual server.
  + Inside-ingress-ssf-tcp-vs – This virtual server receives TCP-based server speaks first (SSF) traffic from the Inside-ingress-tcp-vs. The sslintercept-ingress-ssf-tcp-rule iRule is assigned to this virtual server.
  + Inside-ingress-ftp-vs – This virtual server receives FTP traffic forwarded from the active inside BIG-IP i10800. This traffic is forwarded to the Layer 2 IPS pool for inspection.
  + Inside-egress-bypass-vs – This virtual sever receives TCP traffic that was bypassed around the inspection devices such as initial SSL handshakes and traffic that matches IP bypass criteria.
  + IPS0(1/2)-Inside-egress-tcp-vs – These virtual servers receive TCP traffic that was forwarded through the Layer 2 IPS devices and subsequently forward this traffic on to the Outside-NextHop pool / outside gateway. The sslintercept-egress-tcp-rule iRule is assigned to these virtual servers.
  + IPS0(1/2)-Inside-egress-udp-vs – These virtual servers receive UDP traffic that was forwarded through the Layer 2 IPS devices and subsequently forward this traffic on to the Outside-NextHop pool / outside gateway.
  + IPS0(1/2)-Inside-egress-any-vs – These virtual servers receive non-TCP/UDP traffic that was forwarded through the Layer 2 IPS devices and subsequently forward this traffic on to the Outside-NextHop pool / outside gateway.
  + Outside-ingress-tcp-vs – This virtual server receives TCP traffic that was forwarded by the active outside BIG-IP i10800. This traffic is forwarded to the Layer 2 IPS pool for inspection. This virtual server utilizes the global DoS profile and has the tls-detect-rule iRule assigned.
  + Outside-ingress-udp-vs – This virtual server receives UDP traffic that was forwarded by the active outside BIG-IP i10800. This traffic is forwarded to the Layer 2 IPS pool for inspection. This virtual server utilizes the global DoS profile.
  + Outside-ingress-any-vs – This virtual server receives non-TCP/UDP traffic that was forwarded by the active outside BIG-IP i10800. This traffic is forwarded to the Layer 2 IPS pool for inspection. This virtual server utilizes the global DoS profile.
  + Outside-egress-bypass-vs – This virtual sever receives TCP traffic that was bypassed around the inspection devices such as SSL/TLS-based traffic.
  + IPS0(1/2)-Outside-egress-tcp-vs – These virtual servers receive TCP traffic that was forwarded through the Layer 2 IPS devices and subsequently forward this traffic on to the Inside-NextHop pool / inside gateway.
  + IPS0(1/2)-Outside-egress-udp-vs – These virtual servers receive UDP traffic that was forwarded through the Layer 2 IPS devices and subsequently forward this traffic on to the Inside-NextHop pool / inside gateway.
  + IPS0(1/2)-Outside-egress-any-vs – These virtual servers receive non-TCP/UDP traffic that was forwarded through the Layer 2 IPS devices and subsequently forward this traffic on to the Inside-NextHop pool / inside gateway.
  + Hosted-WebApp-HTTP – This virtual server receives HTTP traffic destined for a specific web application and facilitates WAF protection. This traffic is forwarded to the Layer 2 IPS pool for inspection. This virtual server utilizes the global DoS profile and the HTTP analytics profile.
  + Hosted-WebApp-HTTPS – This virtual server receives HTTPS traffic destined for a specific web application and facilitates WAF protection of the app as well as decryption and inspection of SSL/TLS traffic. This traffic is forwarded to the Layer 2 IPS pool for inspection. This virtual server utilizes the global DoS profile and the HTTP analytics profile.
  + Captive-Portal-HTTP-vs – This virtual server hosts a portal for tenants that must display an EULA or authenticate clients before allowing Internet connectivity.
  + Captive-Portal-HTTPS-vs – This virtual server hosts a portal for tenants that must display an EULA or authenticate clients before allowing Internet connectivity.
  + Service-icap-tcp-vs – This virtual server facilitates communication between the VIPRION an an ICAP service, such as a DLP device.
  + Service-pcap-tcp-vs – This virtual server can be used to send a copy of TCP traffic traversing it to a passive inspection device.
  + Service-ssh-vs – This virtual server can proxy and log SSH traffic traversing the SSL Intercept solution.

### F5 iRules

The SSL Intercept solution utilizes a set of iRules to deliver key functionality. iRules provide incredible flexibility to meet current and future requirements relating to the Core EPS Solution.

#### Bypass IPS

Bypassed SSL/TLS as well as global tenant bypassed traffic can bypass the IPS directly to the outside next-hop. This is controlled by the static::BYPASS\_THROUGH variable in the sslintercept-ingress-tcp-rule iRule:

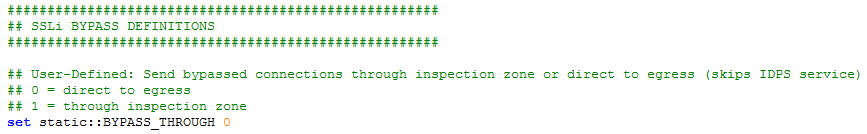


Figure 10: Bypass IPS iRule Code Sample

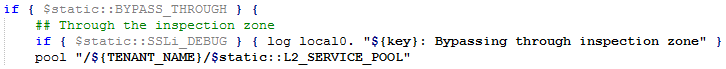


Figure 11: Bypass IPS Logic iRule Code Sample

#### Disable SSL Interception

SSL Interception can be enabled/disabled on the tenant level (see Bypass IPS) or globally by setting the static::BYPASS\_SSL\_FORWARD\_PROXY\_BYPASS variable in the sslintercept-ingress-tcp-rule iRule:



Figure 12: Disable SSL Interception iRule Code Sample

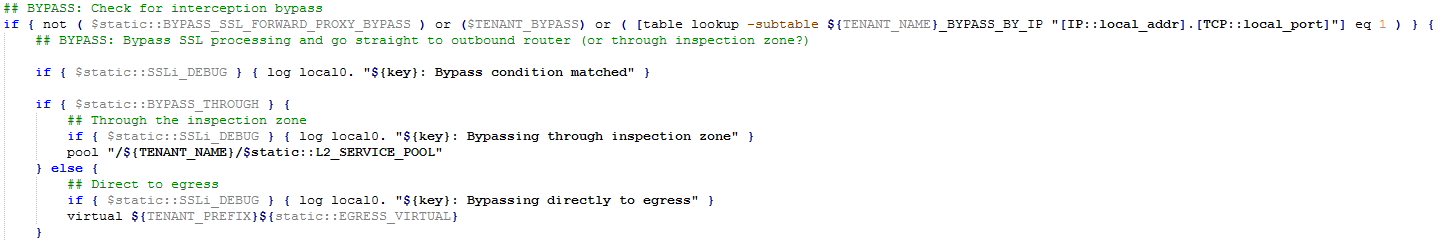


Figure 13: Disable SSL Interception Logic iRule Code Sample

#### Control Debug & Alert Logging

Debug and alert logging can be enabled to troubleshoot issues relating to SSL Intercept functionality such as unexpected URL categorization, failing connections, and failed inspection services. Debug and alert logging is controlled by two variables in the sslintercept-ingress-tcp-rule iRule:

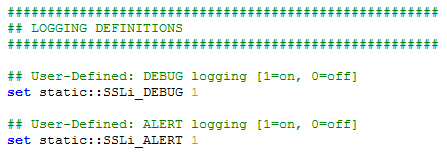


Figure 14: Control Debug and Alert Logging iRule Code Sample



Figure 15: Example Debug Logic iRule Code Sample

#### Bypass SWG

Secure Web Gateway (SWG) functionality can be enabled/disabled on the global level by setting the static::BYPASS\_SWG variable in the sslintercept-ingress-tcp-rule iRule:



Figure 16: Bypass SWG iRule Code Sample

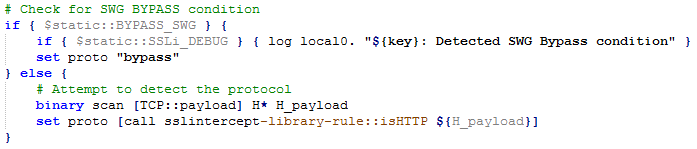


Figure 17: Bypass SWG Logic iRule Code Sample

#### Scan for SSL on any TCP port

This solution is capable of detecting and decrypting SSL/TLS on any TCP port. The excerpt of iRule code in the figure below attempts to detect an SSL handshake / ClientHello in the client TCP payload. If a handshake is detected the iRule immediately enables the SSL profiles which in turn enable the SSL Forward Proxy functionality on the VIPRION.

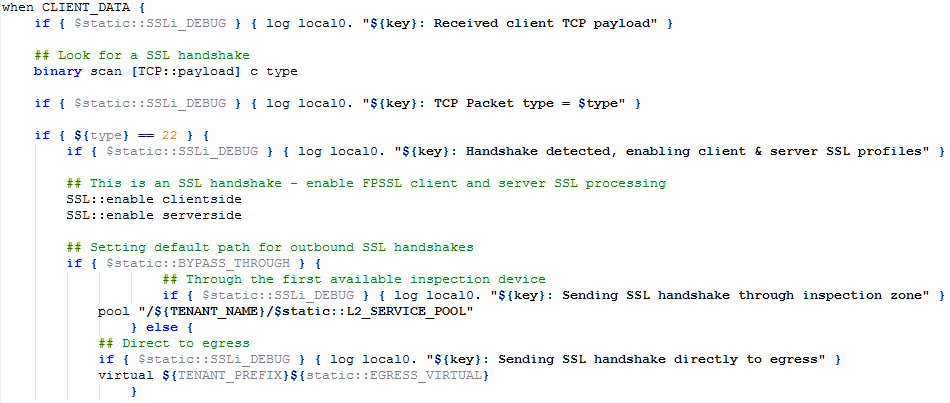


Figure 18: Scan for SSL iRule Code Sample

#### Scan for HTTP in any TCP payload

This solution can detect HTTP payload in unencrypted and decrypted (intercepted) connections. If HTTP payload is detected the system forwards that connection to the SWG service for additional Layer 7 evaluation.

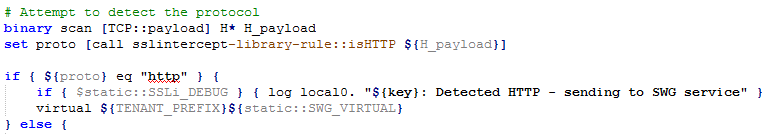


Figure 19: Scan for HTTP iRule Code Sample

### BIG-IQ Analytics iApp

The BIG-IQ Analytics iApp is deployed on each VIPRION system and facilitates the collection of statistical and state data by BIG-IQ Centralized Management.

### BIG-IP Access Policy Manager and Secure Web Gateway Design

BIG-IP Access Policy Manager (APM) and Secure Web Gateway (SWG) provide authentication and URL classification & blocking functionality.

#### Authentication & AAA Servers

BIG-IP APM provides several AAA methods, including but not limited to: Active Directory, LDAP, NTLM, Kerberos, Client Certificate Authentication, and RADIUS. It is also capable of combining more than one AAA method to satisfy multi-factor authentication (MFA) requirements.

#### Access Policy

Each tenant is assigned an access policy. This access policy allows the tenant to require authentication, through a captive portal, prior to allowing their end users / clients online. The authentication policy is built using F5’s intuitive Visual Policy Editor (VPE).

#### Per-Request Policies

Each tenant is assigned a per-request policy (PRP). The per-request policy enforces the global and tenant-specific blacklist/block custom categories. It also provides the ability for the tenant to enforce step-up authentication to prompt users for credentials when accessing specific sites or after a configured period of time.

# Appendix

## References

**BIG-IP Hardware Datasheet**<http://www.f5.com/pdf/products/big-ip-platforms-datasheet.pdf>

**VIPRION Hardware Datasheet**  
<https://www.f5.com/pdf/products/viprion-overview-ds.pdf>

**F5 Software Support Policy**  
<https://support.f5.com/kb/en-us/solutions/public/5000/900/sol5903.html>

**BIG-IP LTM and TMOS 13.1.0 Release Notes**  
<https://support.f5.com/kb/en-us/products/big-ip_ltm/releasenotes/product/relnote-bigip-ve-13-1-0.html>

**BIG-IP LTM 13.1.0 Documentation**<https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20LTM&version=13.1.0>

**BIG-IP ASM 13.1.0 Documentation**<https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20ASM&version=13.1.0>

**BIG-IP AFM 13.1.0 Documentation**  
<https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20AFM&version=13.1.0>

**BIG-IP APM 13.1.0 Documentation**  
<https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20APM&version=13.1.0>

**BIG-IP Analytics 13.1.0 Documentation**<https://support.f5.com/csp/knowledge-center/software/BIG-IP?module=BIG-IP%20Analytics&version=13.1.0>

## List of F5 Acronyms

|  |  |
| --- | --- |
| APM | Access Policy Manager |
| ARP | Address Resolution Protocol |
| ASM | Application Security Manager |
| BIND | Berkley Internet Naming Daemon |
| CNAME | Canonical NAME |
| CPU | Central Processing Unit |
| DC | Data Center |
| DDoS | Distributed Denial of Service |
| DMZ | De-Militarized Zone |
| DNS | Domain Name System (Service) |
| DoS | Denial of Service |
| DR | Disaster Recovery |
| EIF | Endpoint Independent Filtering |
| EIM | Endpoint Independent Mapping |
| FQDN | Fully Qualified Domain Name |
| GTM | Global Traffic Manager |
| GUI | Graphical User Interface |
| HA | High Availability |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HyperText Transfer Protocol (Secure) |
| ICMP | Internet Control Message Protocol |
| IP | Internet Protocol |
| ISP | Internet Service Provider |
| LAN | Local Area Network |
| LACP | Link Aggregation Control Protocol |
| LTM | Local Traffic Manager |
| MAC | Media Access Control |
| Mb | Megabits |
| MB | Megabytes |
| NAT | Network Address Translation |
| NTP | Network Time Protocol |
| OS | Operating System |
| OSI | Open Systems Integration |
| OSS | Operation & Support Systems (Services) |
| OWA | Outlook Web Access |
| PAM | Pluggable Authentication Module |
| RD | Route Domain |
| RFC | Request for Comment |
| SCTP | Stream Control Transmission Protocol |
| SNAT | Secure NAT |
| SNMP | Simple Network Management Protocol |
| SoW | Statement of Work |
| SQL | Structured Query Language |
| SSL | Secure Socket Layer |
| TCL | Tool Command Language |
| TCP | Transmission Control Protocol |
| UCS | User Configuration Set |
| UDP | User Datagram Protocol |
| URI | Uniform Resource Indicator |
| URL | Uniform Resource Locator |
| VE | Virtual Edition |
| VLAN | Virtual Local Area Network |
| WAN | Wide Area Network |
| XML | eXtensible Markup Language |