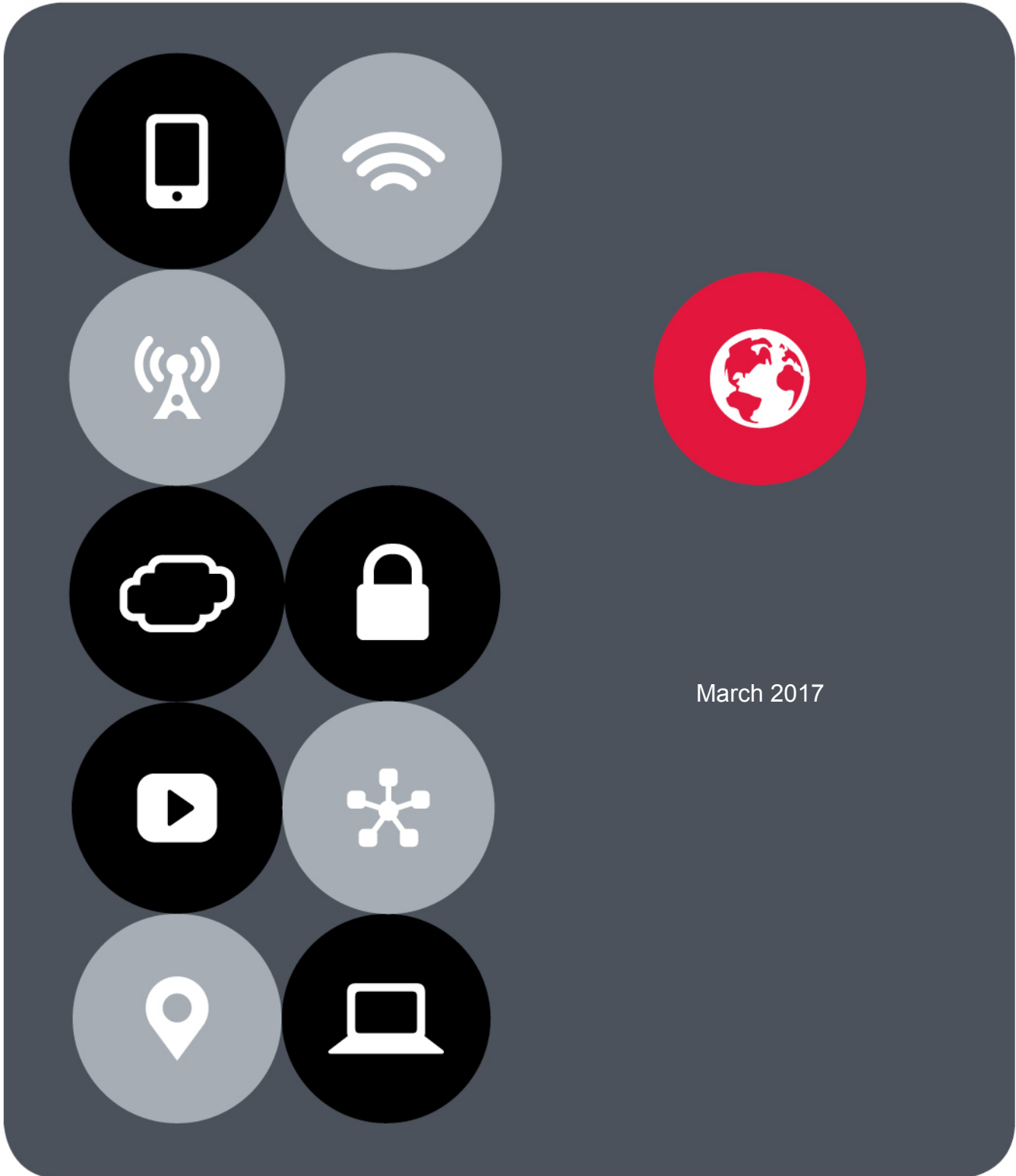# The F5 SSL Orchestrator and Palo Alto Networks Next-Gen Firewall Solution:
SSL Visibility with Service Chaining for Advanced Threat Analysis and Prevention

March 2017

Contents

Introduction

The Secure Sockets Layer (SSL) protocol and its successor, Transport Layer Security (TLS), have been widely adopted by organizations to secure IP communications, and their use is growing rapidly. While SSL provides data privacy and secure communications, it also creates challenges to inspection devices in the security stack when inspecting the encrypted traffic. In short, the encrypted communications cannot be seen as clear text and are passed through without inspection, becoming security blind spots. This creates serious risks for businesses: What if attackers are hiding malware inside the encrypted traffic?

However, performing decryption of SSL/TLS traffic on the security inspection devices, with native decryption support, can tremendously degrade the performance of those devices. This performance concern becomes even more challenging given the demands of stronger, 2048-bit certificates.

An integrated F5 and Palo Alto Networks solution solves these two SSL/TLS challenges. F5® SSL Orchestrator™ centralizes SSL inspection across complex security architectures, enabling flexible deployment options for decrypting and re-encrypting user traffic. It also provides intelligent traffic orchestration using dynamic service chaining and policy-based management. The decrypted traffic is then inspected by one or more Palo Alto Networks next-generation firewalls (NGFWs), which can prevent previously hidden threats and block zero-day exploits. This solution eliminates the blind spots introduced by SSL and closes any opportunity for adversaries.

This guide provides an overview of the joint solution, describes different deployment modes with reference to service chain architectures, recommends practices, and offers guidance on how to handle enforcement of corporate Internet use policies.

The Integrated Solution

The F5 and Palo Alto Networks integrated solution enables organizations to intelligently manage SSL while providing visibility into a key threat vector that attackers often use to exploit vulnerabilities, establish command and control channels, and steal data. Without SSL visibility, it is impossible to identify and prevent such threats at scale.

Key highlights of the joint solution include:

- **Flexible deployment modes** that easily integrate into even the most complex architectures, consolidate the security stack to reduce complexity, and deliver SSL visibility across the security infrastructure.

- **Centralized SSL decryption/re-encryption** with best-in-class SSL hardware acceleration, eliminating the processing burden of multiple decryption/re-encryption workloads on every security inspection hop in the stack, which reduces latency while improving the user experience.

- **Dynamic security service chaining**, which provides policy-based traffic management, thus determining whether traffic should be allowed to pass or be decrypted and sent through a security device or service.

- **An industry-leading application delivery controller** that load balances traffic to multiple devices in the security services, enabling effortless scaling and growth.

- **Built-in health monitors** that detect security service failures and shifts, or bypasses, loads in real time to provide reliability and fault tolerance.

- **Full cipher support**, including support for the PFS-enabled ciphers, to ensure full traffic visibility.

- **Natively integrated security technologies** that leverage a single-pass prevention architecture to exert positive control based on applications, users, and content to reduce the organizational attack surface.

- **Automated creation and delivery of protection mechanisms** to defend against new threats to network, cloud, and endpoint environments.

- **Threat intelligence sharing** that provides protection by taking advantage of the network effects of a community of comprehensive, global threat data to minimize the spread of attacks.
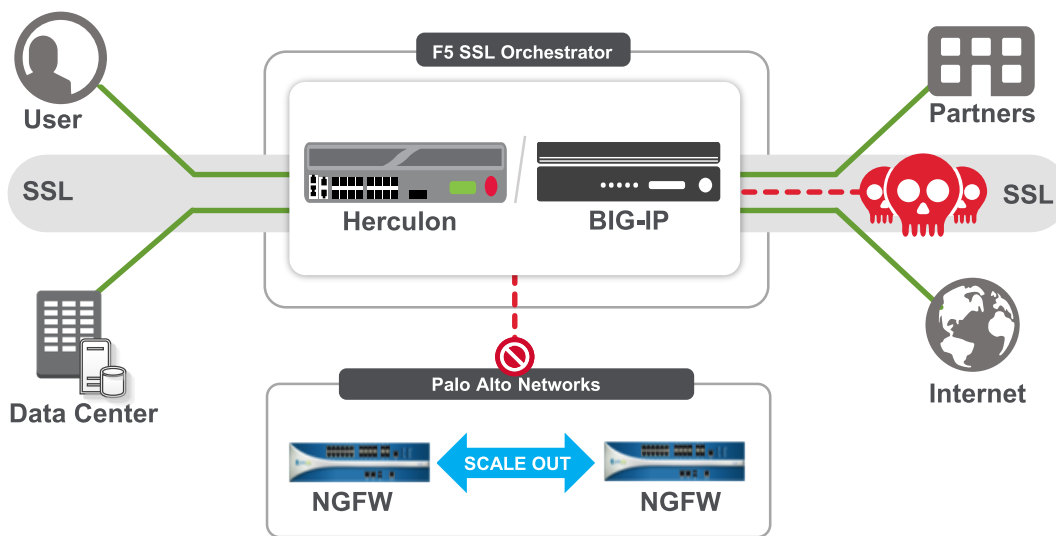

Figure 1: The integrated F5 and Palo Alto Networks NGFW security solution

SSL visibility: How do we do it?

F5's industry-leading full proxy architecture enables an F5 device—either the F5® BIG-IP® system or the F5® Herculon™ platform— to install a decryption/clear text zone between the client and web server, creating an aggregation (and, conversely, disaggregation) visibility point for security services. The F5 system establishes two independent SSL connections—one with the client and the other with the web server. When a client initiates an HTTPS connection to the web server, the F5 system intercepts and decrypts the client-encrypted traffic and steers it to a pool of Palo Alto Networks firewalls for inspection before re-encrypting the same traffic to the web server. The return HTTPS response from the web server to the client is likewise intercepted and decrypted for inspection before being sent on to the client.
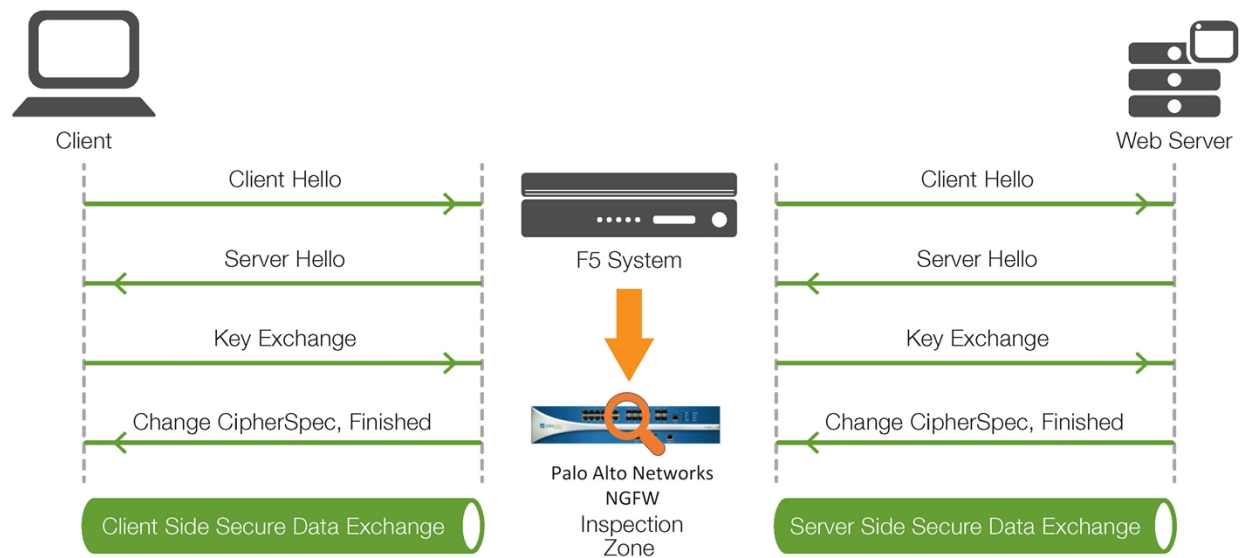
Figure 2: The F5 full proxy architecture

SSL orchestration using security service chains

A typical security stack often begins with a firewall but almost never stops there. To solve specific security challenges, security administrators are accustomed to manually chaining multiple point products such as data loss prevention (DLP) scanners, web application firewalls, intrusion prevention systems (IPS), malware analysis tools, and more, creating a bare-bones security stack consisting of multiple services. In this model, all user sessions are provided the same level of security, as this "daisy chain" of services is hard-wired.

As shown in Figure 3, an F5 device can consolidate the security stack, including NGFW (anti-virus/malware, IPS), ICAP, and DLP, using intelligent traffic orchestration and policy-based steering. The F5 system does this by matching the URL and policies to determine whether to bypass or to decrypt, and whether to send to one set of security services or another.
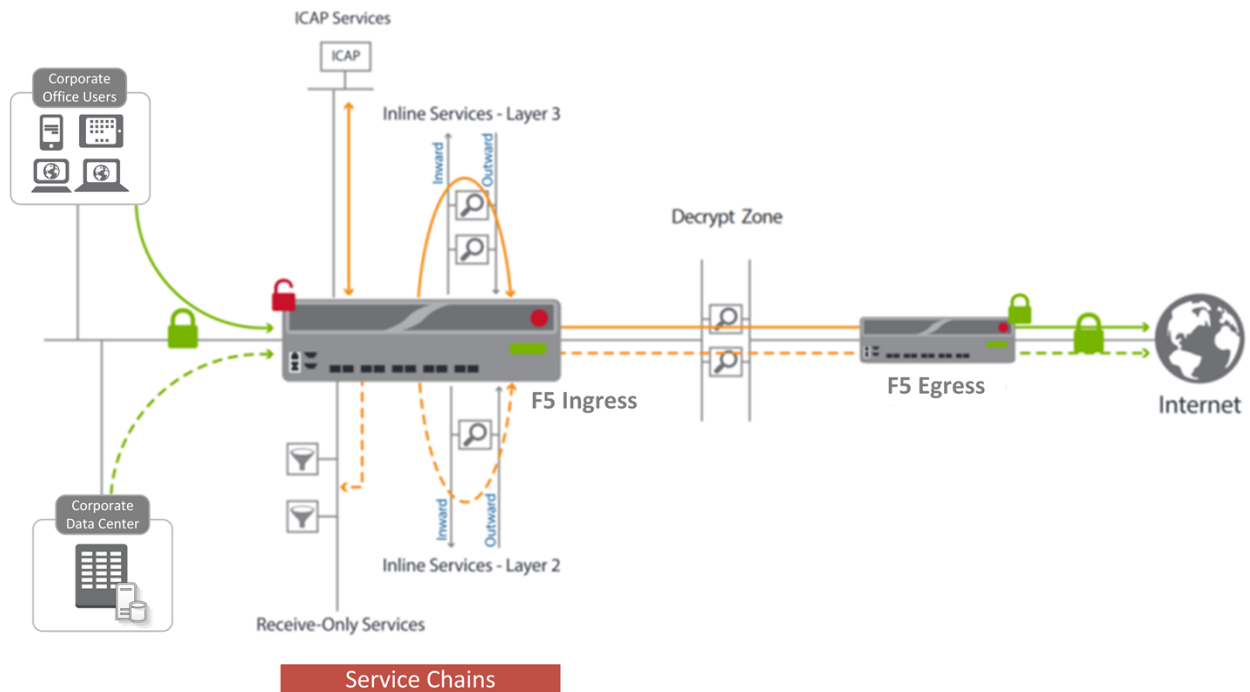
Figure 3: The security service chaining architecture

The F5 SSL visibility solution provides a way to apply different service chains based on context derived from a powerful classification engine. That context can come from:

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

Deployment Planning

Careful advance consideration of deployment options can ensure an efficient and effective implementation of the F5 integrated solution using Palo Alto Network's next-generation security system.

Sizing

The main advantage of deploying an F5 system in the corporate security architecture is that the wire traffic now can be classified as "interesting" traffic, which needs to be decrypted by the F5 system for inspection by Palo Alto

Networks firewalls, and "uninteresting" traffic, which is allowed to pass through or be processed differently according to other corporate policy requirements. This selective steering of only the interesting traffic to the firewall system conserves its valuable resources (as it need not inspect the entire wire traffic), maximizing performance.

As a result, it is important to consider the entire wire traffic volume to calculate the appropriate F5 device size. Depending on the mode of deployment you choose, you will need at least two interfaces on the F5 system for each firewall configured for inline mode and at least one interface for each firewall configured for TAP mode.

Refer to the Herculon SSL Orchestrator Datasheet or BIG-IP Platforms Datasheet and consider the following factors when sizing the F5 system for the integrated solution:

- Port density

- SSL bulk encryption throughput

- System resources

- The number of security services and devices in them

Refer to the Palo Alto Networks Firewall comparison tool for sizing considerations when selecting platforms for the integrated solution.

License components

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

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

Optionally, customers can consider the following:

- **A URL Filtering (URLF) subscription** to use the URL category database for filtering.

- **An F5 IP Intelligence subscription** to detect and block known attackers and malicious traffic.

- **A network hardware security module (HSM)** to safeguard and manage digital keys for strong authentication.

The following Palo Alto Networks products and subscriptions are needed for deploying the solution:

- **A Palo Alto Networks Next-Generation Firewall** for policy-based control of applications, users, and content

- **A Threat Prevention subscription** that includes malware, command-and-control, and vulnerability and exploit protection with IPS capabilities

- **A WildFire subscription** expedites the response to threats by automatically detecting unknown malware and generating and distributing protections to subscribers

Horizontal scaling

The BIG-IP system's ability to steer and load-balance traffic to multiple security devices in a service or service pool enables the Palo Alto security platform to scale horizontally without the need for any functional add-on. This ensures that the service is not only fault-tolerant but also highly available, maximizing throughput.

It is common to configure a single pool of Palo Alto Networks firewalls with the BIG-IP system load-balancing the unencrypted HTTP and decrypted HTTPS traffic to all the pool members. However, if you need to create multiple firewall pools, each taking a different traffic set based on user-defined criteria such as VLAN, tenant, or other criteria; you can do so by leveraging the TCP Service Chain Classifier Rules in SSL Orchestrator. These rules classify the wire traffic based on user-defined network information, IP geolocation, URL category, protocol, or IP intelligence, among other factors, and steer the classified traffic accordingly to a designated service chain the Palo Alto Networks service is part of.
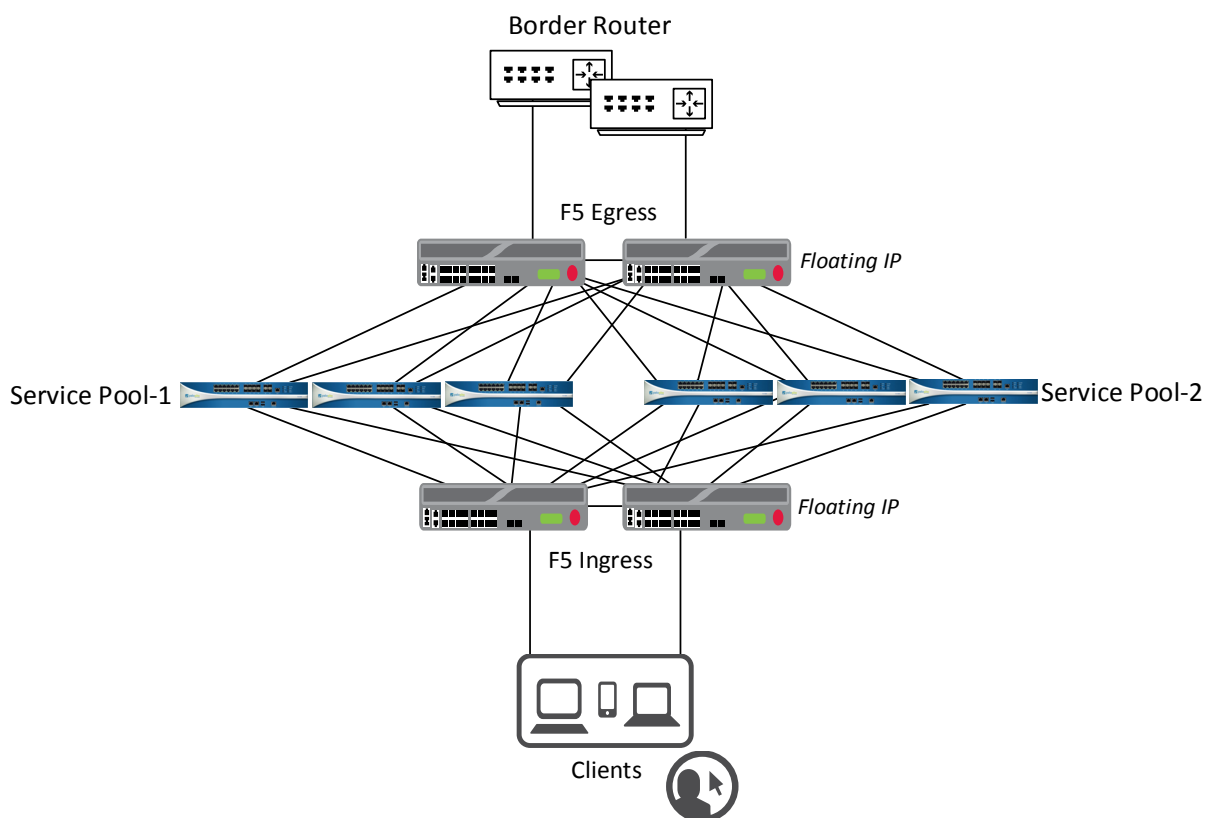
Figure 4: Palo Alto Networks NGFWs in a service/service pool scaling configuration horizontal with the F5 system

Traffic exemptions for SSL inspection

As noted, the BIG-IP system can be configured to distinguish between interesting and uninteresting traffic for the purposes of security processing. Examples of uninteresting traffic (including those types that cannot be decrypted) to be exempted from inspection may include:

- Guest VLANs.

- Applications that use pinned certificates.

- Trusted software update sources like Microsoft Windows updates.

- Trusted backup solutions like a crash plan.

- Any lateral encrypted traffic to internal services to be exempted.

You can also exempt traffic based on domain names and URL categories. The service chain classifier rules of the BIG-IP and Herculon systems enable administrators to enforce corporate Internet use policies, preserve privacy, and meet regulatory compliance.

Traffic exemptions based on URL category might include bypasses (and thus no decryption) for traffic from known sources of these types of traffic:

- Financial

- Health care

- Government services

Certificate requirements

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

To ensure that clients on the corporate network do not encounter certificate errors when accessing SSL-enabled websites from their browsers, the root certificate must be imported into the browser or operating system of the end hosts.

IP addressing

When a Palo Alto Networks firewall is deployed as an L3/routed hop, we recommend configuring its IP addresses for connected inward and outward VLANs from default fixed addressing subnets provided by the SSL Orchestrator application that is derived from a RFC2544 CIDR block of 192.19.0.0 to minimize the likelihood of address collisions.

For example, you can configure a firewall to use the IP address 198.19.0.61/25 on the inward VLAN and 198.19.0.161/25 on the outward VLAN pointing to the Herculon or BIG-IP connected interfaces. You will also need to configure static routes to the internal networks on the firewall inward VLAN and a default route to the Internet on the outward VLAN. The table below explains the IP addresses that you need to configure when deploying multiple firewalls in the service pool.

Palo Alto Networks NGFW	Inward Interface IP	Inward / Internal Gateway	Outward Interface IP	Outward/ Default Gateway
Palo Alto Networks NGFW-1	198.19.0.61/25	198.19.0.10/25	198.19.0.161/25	198.19.0.245/25
Palo Alto Networks NGFW-2	198.19.0.62/25		198.19.0.162/25	
Palo Alto Networks NGFW-n n=<8	198.19.0.6n/25		198.19.0.16n/25 n=<8	

Deployment modes

Due to security concerns around key compromise, Internet sites have started to move away from RSA-based encryption. RSA, as a key exchange encryption protocol, uses the server's key pair to negotiate the symmetric keys used in the encrypted session, therefore potentially compromising the server's private key (such as in the Heartbleed vulnerability), as well as compromising any message, current or past, that uses or used that key pair. Therefore, these websites are transitioning to encryption technologies based on Diffie-Hellman (DH) key agreement protocols that do not expose data if a private key is compromised. Further, making DH keys ephemeral (temporary) defines that cryptography as perfect forward secrecy (PFS). PFS protects past sessions against future compromise of the secret keys, as they are not linked to the server's key pair.

An interesting side effect of this evolution is that passive SSL inspection technologies—systems that exist in the market today and can attach to a span port to passively (and often asynchronously) decrypt SSL/TLS communications—can no longer function. These technologies rely on the client and server performing an RSA key exchange, and they must possess a copy of the server's private key. If the client and server choose a PFS cipher, there is no opportunity for these passive SSL systems to decrypt the data. Many Internet sites and most browsers today prefer PFS ciphers over non-PFS (RSA) ciphers. In addition, the upcoming TLS version 1.3 update will completely remove non-PFS key exchanges, making passive SSL systems nonfunctional. In other words, to perform SSL visibility when employing ciphers based on PFS, an intercept system must be inline to the traffic flow.

Within that provision, various modes of deployment are available for integrating F5 systems with Palo Alto Networks firewalls for advanced threat protection.

Single or double F5 systems

The F5 SSL visibility solution with inline Palo Alto Networks firewalls can be deployed with one or two BIG-IP or Herculon systems.

- **Option 1: A single F5 system with inline Palo Alto Networks NGFW**. This solution entails a single F5 system deployed to perform both decryption and re-encryption of SSL traffic, while Palo Alto Networks firewalls are configured for inline mode and deployed as an L3 service pool on the F5 system.

- **Option 2: Two F5 systems with inline Palo Alto Networks NGFW**. Although a single F5 system delivers all the capabilities and functionality needed to deploy the SSL visibility solution, in some cases,

customers may want to implement a second F5 system on the egress:

- o   When there is a need for increased SSL throughput of the solution, or

- o   When the organization's security policy dictates deploying two SSL intercept appliances for visibility.

When using two F5 systems for the SSL visibility solution, the ingress system on the client side will decrypt the client-encrypted web traffic, while the egress system on the server/Internet side will re-encrypt the same traffic before sending it to the web server, maximizing SSL throughput.

Service pool or sandwich

Deploying the SSL visibility solution using two F5 systems entails two options for configuring the Palo Alto Networks firewalls:

- **As a service pool managed on the ingress F5 system.** The advantage of deploying firewalls in a service pool is that the ingress F5 system can then steer traffic based on user-defined service chain policies.

- **With the pool sandwiched between the ingress and egress F5 systems**. While this type of deployment allows the F5 system to steer unencrypted traffic that has traveled through the service chains to the sandwiched firewalls in the decrypt zone, it has the downside of limiting policy enforcement, as the firewall pool is no longer a part of any services chain. Further, it also complicates the failover design. The firewalls now need to be configured to fail open, as the decrypt zone has no built-in way to go around device failures here.

Both of these mode options are valid for outbound flows (for example, corporate users browsing the web over HTTPS). They are also applicable at any data exchange points in the data center where the encrypted traffic flows outbound from one security zone to another.

Architecture best practices

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

- Deploy the F5 systems in a device sync/failover device group (S/FDG), which includes the active-standby pair, with a floating IP address for high availability (HA).

- Every Palo Alto Networks NGFW in the service pool must be dual-homed on the inward and outward VLANs with each F5 system in the device Sync/Failover Device Group.

- Further interface redundancy can be achieved using the Link Aggregation Control Protocol (LACP). LACP manages the connected physical interfaces as a single virtual interface (aggregate group) and detects any interface failures within the group.

- Unlike with some competing solutions, the F5 systems do not need physical connections to the Palo Alto Networks firewalls. All that the F5 system requires is L3 reachability to steer traffic through the firewalls. In slow networks, however, we recommend deploying the firewalls not more than one hop away. As a generic guideline, when inspection devices are not directly connected to the F5 system, we highly recommend that

you use network and VLAN controls to restrict access to the unencrypted data only for the inspection devices. For the same reason, RFC2544 addresses mandated by the iApp provide that extra level of security control at the network layer.

Initial Setup

A few initial steps should be completed before moving into detailed configuration of SSL Orchestrator.

Configure the Palo Alto Networks NGFW

Palo Alto Networks' next-generation firewalls allow administrators to safely enable applications and prevent known and unknown threats across the network. The native integration of the platform delivers a prevention architecture that provides a range of security features, including application-aware firewall, intrusion prevention, network anti-virus, anti-spyware/malware, URL filtering, and WildFire threat analysis services. Detection of previously unknown malware results in the automated creation of prevention signatures, which are delivered to all subscribers within minutes. With an open, fully documented API, the Palo Alto Networks NGFW is designed to integrate with automation and orchestration systems.

Palo Alto Networks NGFWs can be configured in four modes. A single firewall can be deployed in multiple modes simultaneously:

- Virtual wire (V-Wire): Transparent mode, where two interfaces are bound together and no switching or routing is needed

- Layer 2: Switching mode, where the firewall provides switching between two or more networks

- Layer 3: Routed mode, where the firewall provides routing between two or more networks

- TAP mode: Where the firewall passively monitors traffic copied from a span/monitor port

Management of the firewall is accomplished through the management plane of the device, either through an API, CLI (SSH), or web UI interface. Most commonly, the web UI is used to configure and manage the device. Once logged into the web UI, administrators can configure trusted and untrusted zones, assign interfaces to the zones, and define and enforce policies. It is important that the policies to which the firewalls are configured permit the health monitoring traffic. For further details on how to configure the Palo Alto NGFW, refer to the PAN-OS 7.1 Administrator's Guide.

Run the SSL Orchestrator Setup Wizard

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

```
[root@localhost:NO LICENSE:Standalone] config # config
  lqqqqqqqqqqqqqqqqqqqqqqqConfirm Configurationqqqqqqqqqqqqqqqqqqqqqqqqk
  x System management connectivity may be lost if the management       x
  x address changes. Accept these settings?                           x
  x                                                                   x
  x IP Address: 192.168.16.31                                         x
  x Netmask: 255.255.255.0                                            x
  x Default Route: 192.168.16.10                                      x
  tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqu
  x                   < Yes >                   < No  >               x
  mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
```

Figure 5: Initial configuration of management IP from command line

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

Note: If at any time during configuration you need to return to the SSL Orchestrator Set-Up Wizard, simply click the F5 logo in the upper-left corner of the **Configuration** utility, and on the **Welcome** screen, click **Run the Setup Utility**.

1. On the F5 **Welcome** screen, click **Next**.

2. On the **License** screen, click **Activate**.

3. On the **EULA** screen, click **Accept**. The license activates and the system reboots.

4. Once the system has rebooted, click **Continue**.

5. On the **Device Certificates** screen, click **Next**.

6. Once the **Platform** screen appears, complete the following steps:

    i. Enter the **Host Name** for this system. The **Host Name** must be a fully qualified domain name.

    ii. Under **User Administration**, enter and confirm the **Root Account** and **Admin Account** passwords, and click **Next**. The Root Account provides access to the command line, while the Admin Account accesses the user interface.

Figure 6: Platform configuration

7. The system notifies you to log out and then log back in with your username (*admin*) and new password. Click **OK**. The system reboots.

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

9. (Optional, unless you plan to later use the DNSSEC option in the SSL Orchestrator configuration—in which case this step is required.) The **Domain Name Server** (DNS) screen opens. Complete the following steps:

    i.   To resolve host names on the system, set up the DNS and associated servers: For the **DNS Lookup Server List**, type the **IP Address** of the DNS server and click **Add**.

    ii. If you use BIND servers, add them in the **BIND Forwarder Server** list.

    iii. Add local domain lookups (to resolve local host names) in the **DNS Search Domain** list.

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

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

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

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

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

14

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

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

Figure 7: Internal VLAN configuration

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

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

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

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

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

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

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

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

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

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

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

15

13. On the **Logging** screen, select either local or Splunk as the **Publisher Type**.

- If you select local, specify the **Destination**—either local-db or localsyslog. This determines the destination of your logs, either a local database or a localsyslog server.

- If you select Splunk, for **Protocol**, select either TCP or UDP. Enter the **IP Address** and **Port** of the Splunk server.

14. Click **Finish**. The SSL Orchestrator configuration page appears with a complete menu displayed on the left side of the page.
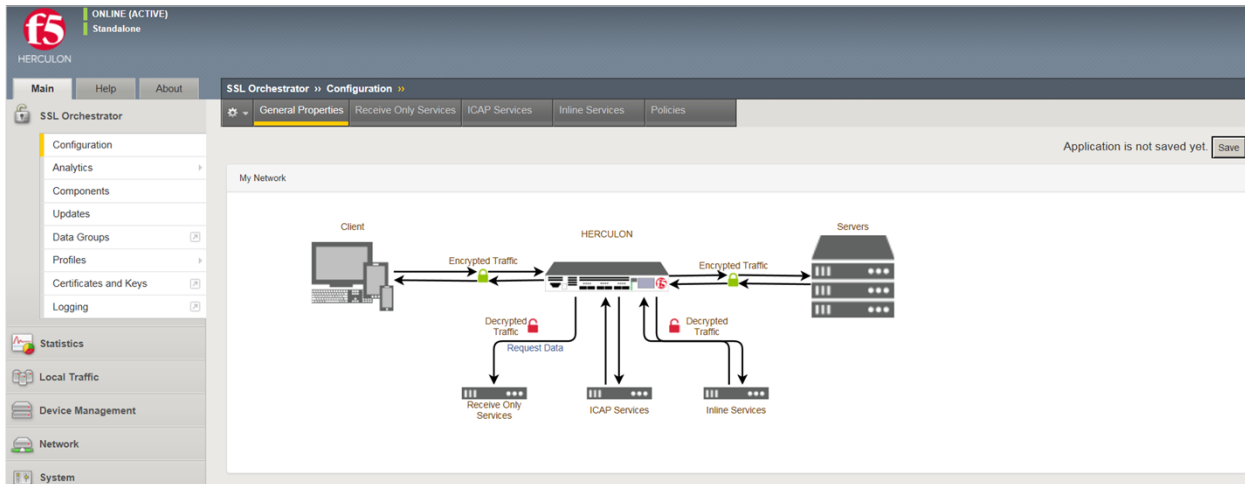
Figure 8: The SSL Orchestrator configuration screen once the initial setup is complete

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

Update the SSL Orchestrator version

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

1. Visit downloads.f5.com. You will need your registered F5 credentials to log in.

2. Click **Find a Download**.

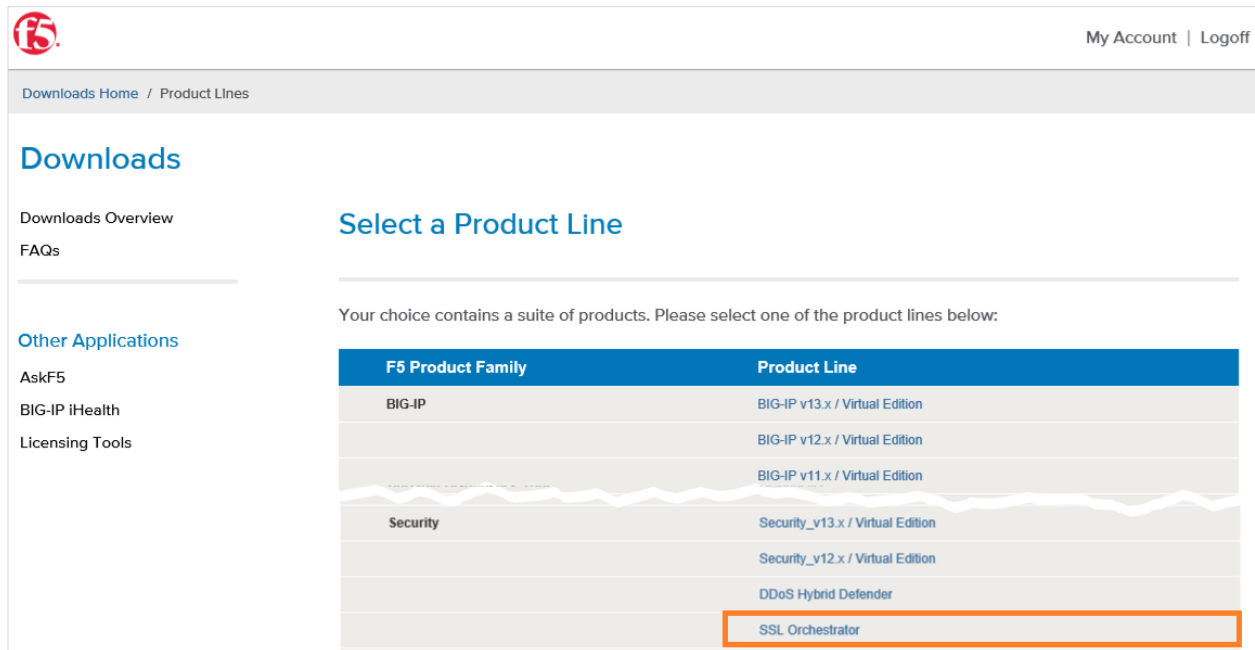3. Scroll to the **Security** product family and select **SSL Orchestrator**.

Figure 9: F5 product download web page

4. Click the SSL Orchestrator container.

5. Select and download the latest version of the SSL Orchestrator .rpm file.

6. Read through the appropriate Release Notes before attempting to use the downloaded file.

7. Once you've read the release notes, log in to the main tab of the F5 BIG-IP management interface and navigate to **SSL Orchestrator > Updates**.

8. Under **File Name**, click **Browse** and navigate to the .rpm file you saved on your system. Click **Open** to select it.
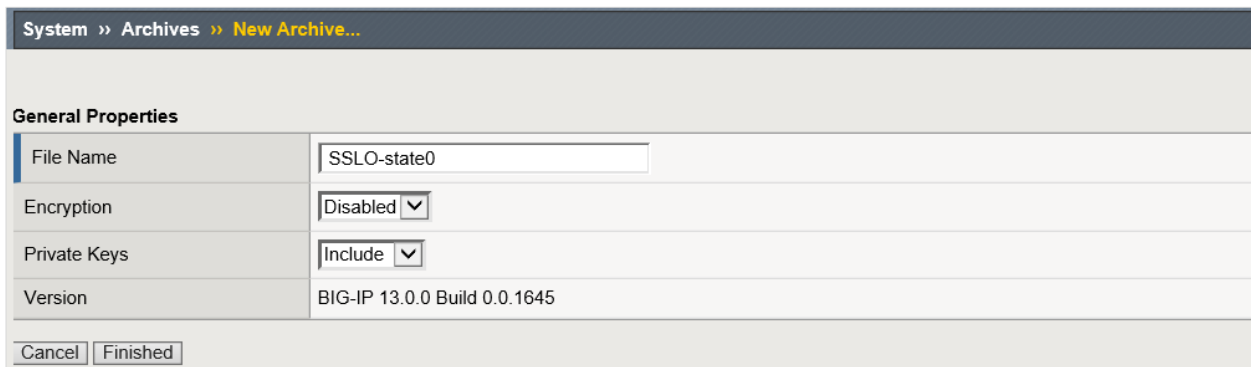
Figure 10: Updating SSL Orchestrator

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

Back up your F5 system configuration

Before beginning the detailed SSL Orchestrator configuration, we strongly recommend you back up the F5 system configuration using the following steps. This enables you to restore the previous configuration in case of any issues.

1. From the main tab of the F5 management interface, click **System > Archives**.

2. To initiate the process of creating a new UCS archive (backup), click **Create**.

3. Enter a *unique* **File Name** for the backup file.

4. Optional:

   - If you want to encrypt the UCS archive file, from the **Encryption** menu, select **Enabled** and enter a passphrase. You must supply the passphrase to restore the encrypted UCS archive file.

   - If you want to exclude SSL private keys from the UCS archive, from the **Private Keys** menu, select **Exclude**.

Figure 11: New system archive creation

5. Click **Finished** to create the UCS archive file.

6. When the backup process is done, examine the status page for any reported errors before proceeding to the next step.

7. Click **OK** to return to the Archive List page.

8. Copy the .ucs file to another system.

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

Configuration for a Single F5 System with Firewalls in L2 or V-Wire Mode (Burrito Design)

This deployment mode entails a single F5 system performing SSL visibility. This single system handles both decryption and re-encryption of HTTPS traffic, with an inspection zone installed between the ingress and the egress.

Figure 12 shows a standalone F5 system configured to intercept, decrypt, and steer the decrypted traffic to a service pool of two Palo Alto Networks firewalls configured in L2 mode or in V-wire mode where the traffic will be inspected for hidden threats. You can also deploy the F5 system as a device sync/failover device group (including an HA pair) with a floating IP address for high availability.
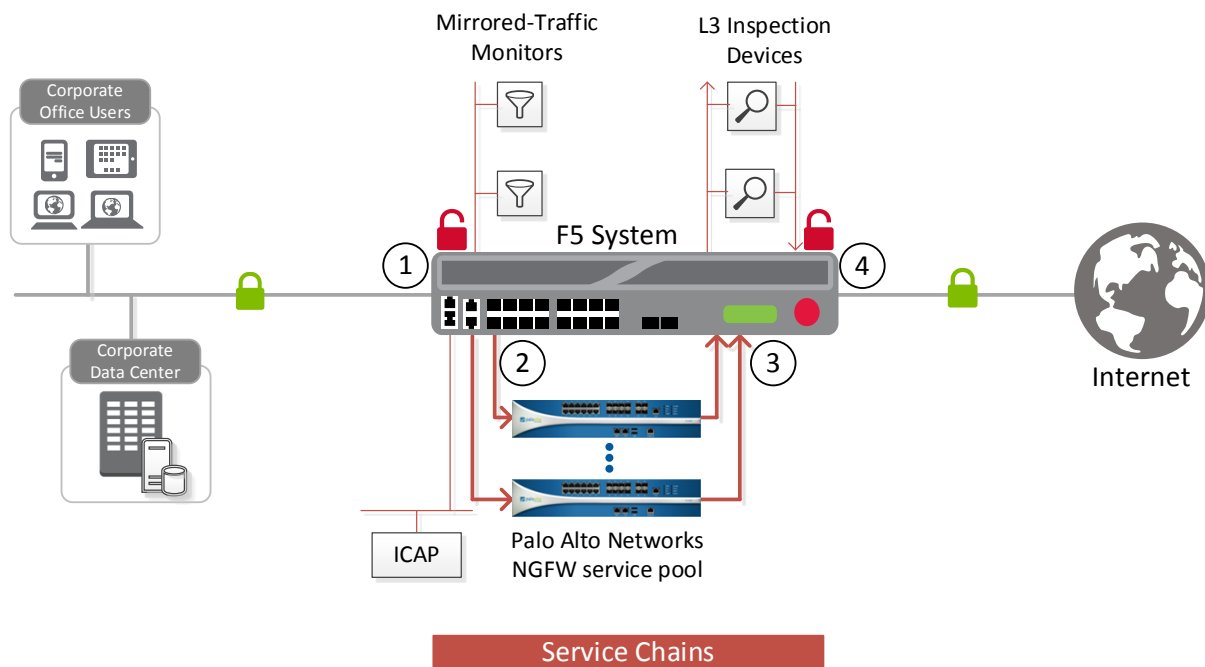
Figure 12: The SSL visibility solution with a security service chain using one F5 system

How traffic flows in this deployment option:

1. Client traffic arriving at the ingress F5 device is classified, and interesting HTTPS traffic is decrypted as part of the SSL forward proxy process.

2. The ingress virtual servers on the F5 system steer the decrypted traffic through a service pool of Palo Alto Networks firewalls as part of a service chain via a service-inward VLAN.

3. The HTTP traffic is inspected by the NGFW for any hidden threats before sending that traffic back to the F5 system on the service-outward VLAN.

4. The F5 system orchestrates the decrypted traffic through other services in the chain before it aggregates and re-encrypts the traffic, which is routed outbound to the web server.

Configure SSL Orchestrator

In the example configuration below, SSL Orchestrator steers the outbound web traffic through the Palo Alto Networks firewall, which is part of a service chain of security devices. Please refer the F5 Herculon SSL Orchestrator Setup guide for additional help during configuration.

General properties

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

1. On the main tab of the management console, click **SSL Orchestrator > Configuration > General Properties**.

2. Answer the configuration questions (see Figure 13) for SSL Orchestrator. (See the table below for examples and tips.)

Question	User Input
Application Service Name	Enter a name without spaces or dashes for the SSL Orchestrator application
Do you want to set up separate ingress and egress devices with a cleartext zone between them?	You can configure a single Herculon or BIG-IP device to receive both ingress and egress traffic on different networks, or you can configure separate Herculon or BIG-IP devices for ingress and egress traffic. If you choose the latter option, you are asked further questions to enter peer application names, control channel virtual server IPs, and pre-shared keys to establish and protect the communication between the devices. Otherwise, select **No, use one BIG-IP device for ingress and egress**. This sample configuration follows that option.
Which IP address families do you want to support?	Select **Support IPv4 only**. (Currently SSL Orchestrator only supports IPv4 families.)
Which proxy schemes do you want to implement?	SSL Orchestrator can operate in transparent and/or explicit proxy mode. If you choose explicit proxy, a separate explicit proxy configuration section displays for you to choose the VLANs that explicit proxy needs to listen to and so you can enter the IP address and port number of the explicit proxy. Select **Implement Transparent proxy only**.
Do you want to pass UDP traffic through the transparent proxy unexamined?	This option only applies if you selected Implement transparent proxy only above. By default, transparent proxy mode manages TCP traffic but allows UDP traffic to pass through unexamined. Choose **No** to prevent the passage of unexamined UDP traffic. Otherwise, select the default, **Yes, pass all UDP traffic unexamined**.
Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?	This option also only applies if you select **Implement transparent proxy only**. By default, transparent proxy mode passes through non-TCP, non-UDP traffic (such as IPSec, SCTP, and OSPF). Choose **No** to block. Otherwise, select the default, **Yes, pass non-TCP, non-UDP traffic**.
Which is the SSL Forward Proxy CA certificate?	Select the Certificate Authority (CA) certificate that your clients will trust to authenticate intercepted TLS connections. If you did not use the Setup Wizard,

	you must import a CA certificate before you can use this functionality.
Which is the SSL Forward Proxy CA private key?	Select the corresponding private key, which you imported with the CA certificate while configuring the Setup Wizard. If you did not use the Setup Wizard, you must import a CA certificate before you can use this functionality.
What is the private-key passphrase (if any)?	Enter the private-key passphrase, if any. If the key does not have a passphrase, leave this field empty.
Which CA bundle is used to validate remote server certificates?	The CA bundle is the collection of root and intermediate certificates for the CA you trust to authenticate servers where your clients might connect. The CA bundle is also known as the local trust store. Select the CA bundle that validates the remote server certificates.
Should connections to servers with expired certificates be allowed?	Remote servers can present expired certificates. Allowing connections to servers with expired certificates can cause a security risk. Legitimate servers do sometimes offer certificates which are overdue for renewal or which were signed by legitimate CAs but that are simply unknown to the F5 system. In the latter case, if you allow connections, consider adding any needed CA certificates to the F5 system CA bundle (trust store). Select **No, forbid connections to servers with expired certificates** to prevent connections to servers that have expired certificates.
Should connections to servers with untrusted certificates be allowed?	Remote servers can present untrusted certificates. Allowing connections to servers with untrusted certificates can cause a security risk. Select **Yes, allow connections to servers with untrusted certificates** if appropriate for your situation and security policies.
Should strict updates be enforced for this application?	If you select this option, you cannot manually modify any settings produced by the application. Once you disable this option, you can manually change your configuration. F5 recommends enabling this setting (select **Yes**) to avoid misconfigurations that can cause an unusable application.

Figure 13: Sample general properties configuration

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

Ingress device configuration

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

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

Question	User Input
Which VLAN(s) will bring client traffic to the transparent proxy?	Select one or more VLANs where transparent-proxy ingress traffic will arrive.
How should a server TLS handshake failure be handled?	Most TLS handshake failures occur during protocol and cipher agreement. You can specify whether to drop or bypass the connection. Typically, select **If server TLS handshake fails the connector fails**.
DNS query resolution	Specify whether to permit the system to send DNS queries directly to the Internet, or specify one or more local forwarding nameservers to process all DNS queries from SSL Orchestrator. If you choose the former, you can specify to configure local/private DNS zones. In this example, select **Send DNS queries to forwarding nameservers on the local network**.

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

Figure 14: Sample ingress device configuration

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

Egress device configuration

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

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

Question	User Input
Do you want to SNAT client IP addresses?	It is common to translate the client source IP address with the address belonging to the egress for outbound traffic. Choose **No** to preserve the client source IP address. Otherwise, select **Yes, SNAT (replace) client addresses**.
Do you want to use a SNAT Pool?	F5 recommends use of a SNAT pool to scale translations instead of overloading the egress interface IP address (AutoMap). Select **Yes, define SNAT Pool addresses for good performance**.
IPv4 SNAT addresses	Enter the IPv4 addresses for the SNAT pool.

Should traffic go to the Internet via specific gateways?	Specify whether to route outbound using the default route on the F5 system or enter the IP address to be used as the default gateway.
	In the example above, we selected **No, send outbound / Internet traffic via the default route**.

Figure 15: Sample egress device configuration

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

Logging configuration

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

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

Figure 16: Default logging settings

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

Create layer 2 inline service

Note: Before creating inline services, you must complete configuration of all the sections in the General Properties tab.

Inline services pass traffic through one or more firewalls at layer 2 or layer 3. The firewalls are configured to communicate with the F5 system via two VLANs. In this section, we will configure an L2 inline service for a pair of Palo Alto firewalls.

1. On the main tab, click **SSL Orchestrator > Configuration > Inline Services**. The **Inline Services** screen displays.

2. Click **Add**.

3. Enter information for the configurable fields, following the guidance below.

Configuration Field	User Input
Name	Type a **Name** for the inline service.
Service Type	Select **Layer 2** from the **Service Type** list.
Interfaces	Select the **From BIG-IP** and **To BIG-IP** system interfaces connected to the firewall and their respective VLANs **Tags**. Click **Add**. If you have multiple firewalls in the service pool, choose the F5 system interfaces connected to each firewall and their VLANs tags and click **Add** before moving to the next one. If you choose to use the **Ratio** field, the F5 system distributes connections among pool members in a static rotation according to ratio weights that you define. For example, if you have two devices, and one handles twice as much traffic as the other, you can set the ratio to 1 on the smaller device and 2 on the larger one.
Translate port for HTTP traffic	Select **No** if the connections should use their original destination ports. Choose **Yes** to translate the port for HTTP traffic to either 80, 8080, or 8443.
Connection Handling On Outage	Select **Skip Service** to allow connections to skip the service you are configuring if all the devices in the service pool are unavailable. Or select **Reject Connection** to reject every connection reaching the service when the service is down.

4. Leave other Inline Services configuration at their default settings.

5. When done, click **Finished**, then click **Save** at the top of the page.

Configuration for an F5 System with Firewalls in L3 Mode

This deployment is similar to the solution explained above in the section called, "Configuration for a F5 BIG-IP system with a firewall in L2 or V-Wire mode." The only difference is that the inline service type is configured as an L3 service.
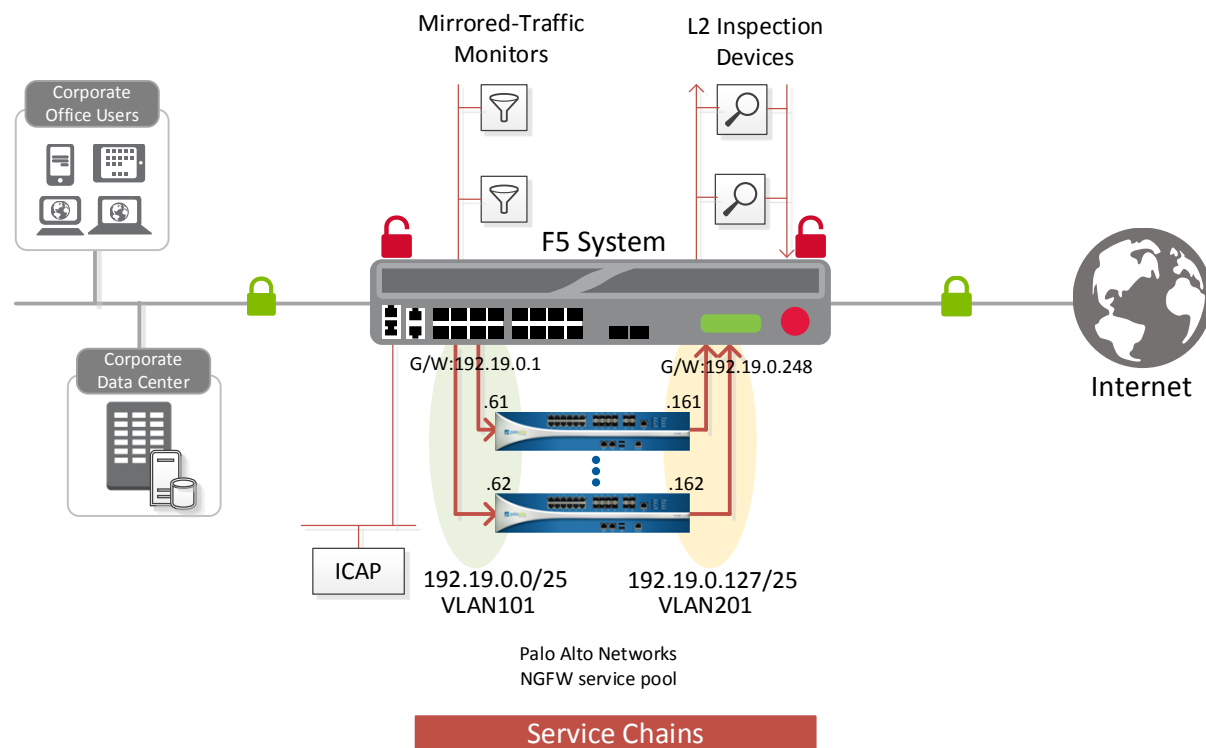

Figure 17: The SSL visibility solution with a Palo Alto Networks NGFW configured in L3 mode

Create the layer 3 inline service

The layer 3 inline service, as a prerequisite, requires you to configure the IP addresses on the firewall(s) from a specific fixed addressing scheme as explained in the section on IP addressing. This configuration enables the F5 system to send to, and receive from, the firewall using a pre-defined set of addresses.

1. On the main tab, click **SSL Orchestrator > Configuration > Inline Services**.

2. Enter information for the configurable fields, following the guidance below.

Configuration Field	User Input
What is the IPv4 (CIDR /19) subnet-block base address?	For IPv4, F5 recommends the default block 198.19.0.0/19. Click Add.
	Even though you can change the base address of each address block (IPv4) from which subnets and addresses are assigned, changing an address block has several implications, must be done with caution, and is not recommended or

	supported by F5.
Name	Enter a **Name** for the inline service.
Service Type	Select **Layer 3** from the **Service Type** list.
Interfaces	Select **From BIG-IP** and **To BIG-IP** system interfaces connected to the firewall(s) and their respective VLANs **Tags**.
Available Devices	Select the **IP Address(es)** of the firewall(s).
	In the sample configuration in Figure 18, the two configured IP addresses on each of the firewalls in the service pool are selected. These firewalls are preconfigured from the CIDR block of 192.19.0.0.
Translate port for HTTP traffic	Select **No** if the connections should use their original destination ports.
	Choose **Yes** to translate the port for HTTP traffic to either 80, 8080, or 8443.
Connection Handling On Outage	Select **Skip Service** to allow connections to skip the service you are configuring if all the devices in the service pool are unavailable.
	Or select **Reject Connection** for the system to reject every connection reaching the service when the service is down.

Figure 18: Inline layer 3 service configuration

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

Configuring the F5 System with Firewalls in TAP Mode

In this solution option, the F5 system is configured to provide a packet-by-packet copy of both the unencrypted HTTP and decrypted HTTPS traffic to Palo Alto Networks NGFW devices wherein the IPS/WildFire is configured for TAP mode.
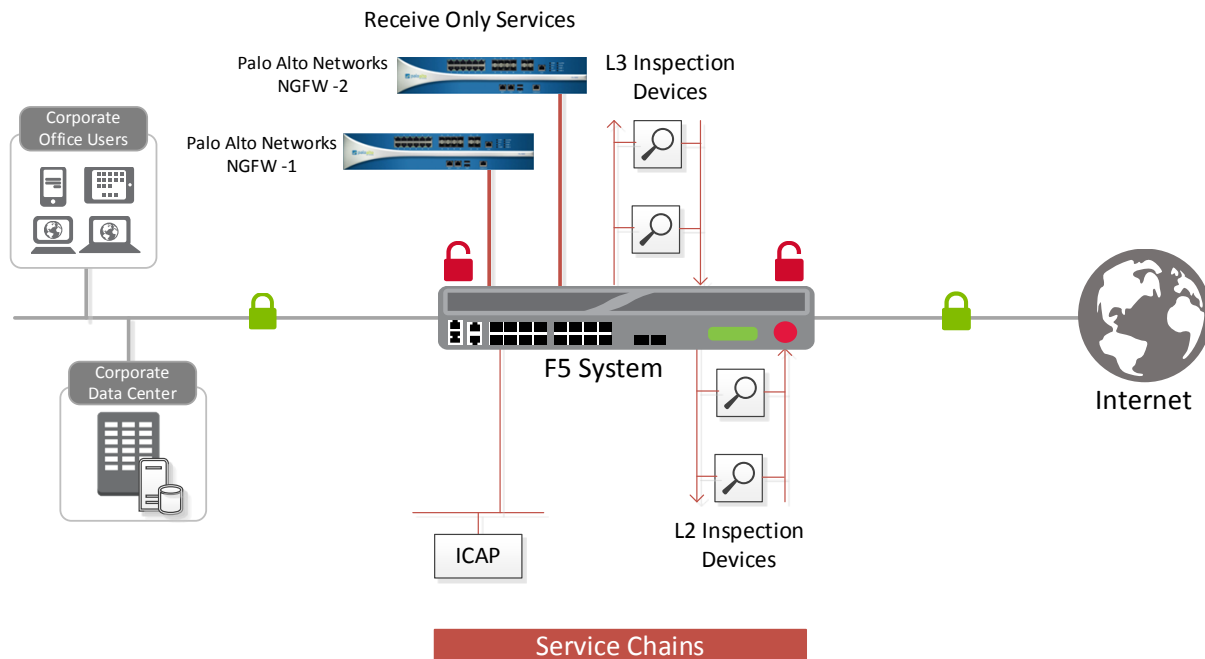
Figure 19: The SSL visibility solution for firewalls in TAP mode

Create a receive-only service

When firewalls are configured for receive-only service, they only receive traffic for inspection and do not send the traffic back to the F5 system. You can configure up to 10 receive-only services using the SSL Orchestrator configuration utility.

1. On the main tab, click **SSL Orchestrator > Configuration > Receive Only Services**.

2. Enter information for the configurable fields, following the guidance below.

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

Figure 20: Sample receive-only service configuration

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

Alternative Architectures

As previously explained in the Deployment Modes section, you may want to deploy a second F5 device for various reasons. This section briefly addresses these alternative architecture and the additional configuration steps needed for deployment.

Two F5 systems with firewalls deployed as a service pool

This solution is similar to the one explained in the section called, Configuring the F5 System with Palo Alto Networks Firewalls in L2 or V-Wire Mode. The only difference is that a second F5 device (the egress device) is introduced to offload re-encryption from the ingress device.

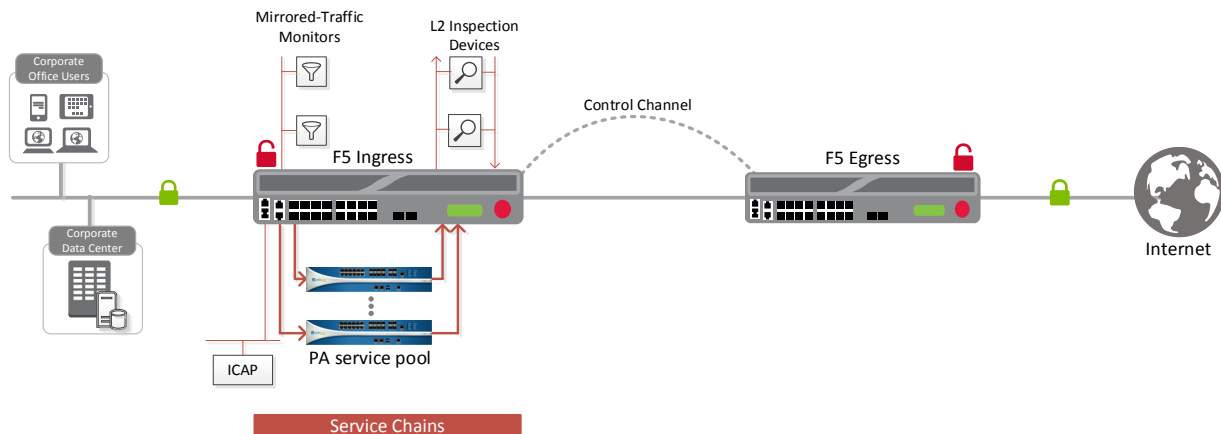Figure 21: The SSL visibility solution with security service chaining using two F5 systems

Additional configuration steps

For this deployment scenario, you must configure the SSL Orchestration application separately on the ingress and egress F5 devices to enable them to cooperate via a control channel. At least a /30 CIDR block is needed for IP connectivity of the control channel virtual servers on the F5 systems.

Configure the ingress F5 device: General properties

The ingress device is either an F5 device or a sync-failover device group where each client sends traffic. The ingress device is one or more ingress VLANs where the clients send traffic. The ingress device decrypts the traffic and then, based on protocol, source, and destination, classifies the traffic and passes each connection for inspection.

1. On the main tab, click **SSL Orchestrator > Configuration > General Properties**.

2. Enter information for the additional configurable fields that are specific to configuring separate ingress and egress devices. Follow the guidance below.

Question	User Input
Application Service Name	Enter a name without spaces or dashes for the SSL Orchestrator application service.
Do you want to setup separate ingress and egress devices with a cleartext zone between them?	Select **Yes, configure separate ingress and egress BIG-IP devices**.
Is this device the ingress or egress device?	Select **This is the INGRESS device to which clients connect**.
What is the EGRESS device Application Service name?	Enter the name of the SSL Orchestrator application service you intend to configure on the egress device. For the sake of ease, you can use the same SSL Orchestrator application service name on both the ingress and egress devices.
What is the IP address of the EGRESS device control-channel virtual server?	Enter the IP address of the control channel virtual server over on the egress device.
What IP address should THIS (ingress) device's control-channel virtual server use?	Enter the IP address of the virtual server for the control channel.
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 F5 devices.

General Properties

Application Service Name ⓘ	SSLVisibility
Do you want to setup separate ingress and egress devices with a cleartext zone between them? ⓘ	Yes, configure seperate ingress and egress BIG-IP devices ⌄
Is this device the ingress or egress device? ⓘ	This is the INGRESS device to which clients connect ⌄
What is the EGRESS device Application Service name? ⓘ	SSLVisibilty
What is the IP address of the EGRESS device control-channel virtual server? ⓘ	192.168.10.2
What IP address should THIS (ingress) device's control-channel virtual server use? ⓘ	192.168.10.1

Figure 22: Sample general configuration when ingress and egress devices will be separate

3. Continue configuration with the decryption zone configuration below.

Configure the ingress F5 device: Decryption zone to egress device configuration

1. Once you've completed the additional General Properties configuration, continue to scroll down the page and answer the following configuration question, using the guidance below.

Question	User Input
Are there parallel service devices in the decrypt zone?	Select **No, send outbound traffic via the BIG-IP default route(s)**. Or select **Yes** when firewalls will be sandwiched in the decrypt zone between the ingress and egress devices.

2. When done, click **Finished**, then click **Save** at the top of the page.

Configure the egress F5 device: General properties

The egress device is either an F5 device or a sync-failover device group that receives traffic that has traveled through the specified service chain and directs that traffic to the final destination. The ingress and egress devices also send each other control messages that 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 through TCP connections to port 245, at an IP address users specify, on each F5 system.

1. On the main tab, click **SSL Orchestrator > Configuration > General Properties**.

2. Enter information for the additional configurable fields that are specific to separate ingress and egress devices. Follow the guidance below.

Question	User Input
Application Service Name	Enter a name without spaces or dashes for the SSL Orchestrator application service.
Do you want to setup separate ingress and egress devices with a cleartext zone between them?	Select **Yes, configure separate ingress and egress BIG-IP devices**.
Is this device the ingress or egress device?	Select **This is the EGRESS device which connects to a server**.
What is the INGRESS device Application Service name?	Enter the name for the SSL Orchestrator application service configured on the ingress device.
What is the IP address of the INGRESS device control-channel virtual server?	Enter the IP address of the control channel virtual server on the ingress device.
What IP address should THIS (egress) device's control-channel virtual server use?	Enter the IP address of the virtual server for the control channel.

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.

3. Continue configuration with the decryption zone configuration below.

Configure the egress F5 device: Egress device configuration

1. Once you've completed the additional General Properties configuration, continue to scroll down the page and answer this additional configuration question using the guidance below.

Question	User Input
Which VLAN(s) are part of the decrypt zone? (These bring traffic from the ingress device)	Select one or more VLANs where transparent-proxy ingress traffic will arrive.

Note: If you chose **Explicit proxy** in the General Properties section to answer the question "**Which proxy schemes do you want to implement?**" a separate explicit proxy configuration section displays here instead. In that case, choose the VLANs that explicit proxy will listen to, and enter the IP address and port number of the explicit proxy.

Configure the egress F5 device: Decrypt zone to ingress device configuration

1. Continue to scroll down the page and answer the question, **Are there parallel service devices in the decrypt zone?**

- Select **No, send outbound traffic via the BIG-IP default route(s).**

- Or select **Yes** when firewalls will be sandwiched in the decrypt zone between the ingress and egress devices.

2. When done, click **Finished**, then click **Save** at the top of the page.

Two F5 systems with firewalls sandwiched in the decryption zone

In this case, the Palo Alto Networks firewalls are deployed as a load balancing pool between the ingress and egress F5 systems in the decrypt zone and are *not* part of the service chains.
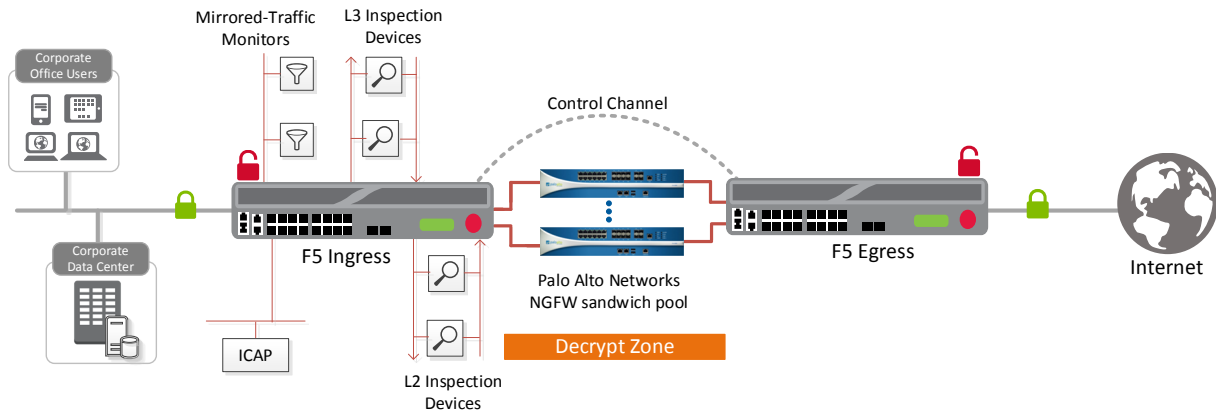
Figure 23: The SSL visibility solution with a Palo Alto Networks NGFW service pool sandwiched between two F5 systems

Additional configuration steps

This scenario requires, as a prerequisite, that you have created a pair of VLANs—one on the ingress F5 device and another on the egress device for each Palo Alto Networks firewall in the sandwiched pool. The IP addresses of each pair of VLANs will be from the same subnet if the firewalls are configured for L2/V-Wire mode and from different subnets if the firewalls are configured in L3 mode.

Configure the ingress device: Decrypt zone to egress device configuration

1. On the main tab, click **SSL Orchestrator > Configuration > General Properties**. Scroll down to the additional configuration section specific to use of a decryption zone.

Figure 24: Sample decrypt zone to egress device configuration

2. Answer the additional questions using the guidance below.

Question	User Input
Are there parallel service devices in the decrypt zone?	Select **Yes, send outbound traffic via one or more service device(s)**.
What are the IPv4 decrypt zone gateway addresses?	Enter the IP address of the outward interface of the last layer 3 device in the decrypt zone. • If the firewall is configured for L2/ v-wire mode, the gateway IP address is the address on a VLAN on the next hop egress device. • If the firewall is configured as L3 hop, this IP address will be the address on a VLAN on the next hop firewall.

3. Once you've entered an IP address, click **+** to add additional addresses. You can enter multiple gateways if you have multiple firewalls and want to load balance across them.

4.   Use the ratio value to control the load balancing.

5.   When done, click **Finished**, then click **Save** at the top of the page.

Configure the egress device: Decrypt zone to ingress device configuration

1.   On the main tab, click **SSL Orchestrator > Configuration > General Properties**. Scroll down to the additional configuration section specific to use of a decryption zone.

Decrypt Zone to Ingress Device Configuration			
Are there parallel service devices in the decrypt zone? ⑦	Yes, send outbound traffic via one or more service device(s) ⌄		
What are the IPv4 decrypt zone gateway addresses? ⑦	**Ratio**	**IPv4 gateway address**	
	1	192.168.20.2	+ −
	1	192.168.30.2	+ −
What are the intranet networks (subnets)? ⑦	**IPV4/IPV6 Subnet**	**IPV4/IPV6 Mask(CIDR)**	
	10.10.10.0	255.255.255.0	+ −

Figure 25: Sample decrypt zone to ingress device configuration

2.   Answer the additional configuration questions using the guidance below.

Question	User Input
Are there parallel service devices in the decrypt zone?	Select **Yes, send outbound traffic via one or more service device(s)**.
What are the IPv4 decrypt zone gateway addresses?	Enter the IP address of the outward interface of the last layer 3 device in the decrypt zone.
What are the intranet networks (subnets)?	Enter the IP address and mask-length, in CIDR format, for intranet subnet masks. Typical IPv4 entries include 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. Click **+** as needed to add additional addresses.

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

Creating service chains to link services

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

Each service chain is linked to service chain classifier rules and processes specific connections based on those classifier rules, which look at protocol, source, and destination addresses. Additionally, service chains can include inline, ICAP, or receive-only services, as well as any decryption zones between separate ingress and egress devices.

1.   On the main tab, click **SSL Orchestrator > Configuration > Policies**. The policies screen displays.

2.   Under **Service Chains**, click **Add**.

3.   Enter a **Name** for the service chain.

4. In the order you want SSL Orchestrator to use to steer the traffic, select the service **Type** (ICAP, inline or receive-only) and service **Name** and click **Add**. (See Figure 26.)

5. Repeat Step 4 until all services in the chain have been selected in the order you prefer.

6. When you're done with the service chain, click **Finished**.

7. Repeat Steps 2 through 6 to create multiple service chains.

Figure 26: Sample service chain configuration

Creating TCP service chain classifier rules

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

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

1. Once you've created a service chain, continue to scroll down the **Policies** page to **TCP Service Chain Classifiers**.

2. Click **Add** and create a classifier rule, making selections and completing each field using the guidance below.

3. The example below creates a sample TCP service chain classifier rule (as shown in figure 27) to bypass SSL traffic originating from any internal client on 10.10.10.0 subnet in the corporate network and destined to any health care websites.

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

	URLF: Specify URL filtering (URLF) categories or a data group against which the destination URL will be matched. A URLF subscription is needed for the rule to evaluate against the URLF database.
	Name: Specify the domain name (with a unique name or using a wildcard) or data group against which the connection's hostname should be matched.
	DDB: Specify the DNS domain name (with a unique name or using a wildcard) against which the destination hostname indicated by the client in TLS Server Name Indication (SNI) is matched. Refer to RFC 6066 to understand the SNI extension for TLS. You may use DDB (dynamic domain bypass) to whitelist and bypass traffic to servers that cause TLS handshake problems or that require TLS mutual (client-certificate/smart-card) authentication. A URLF rule in the pre-handshake phase will match URL filtering categories associated with the TLS SNI hostname and otherwise behave like a DDB rule. See the example in Figure 27 below.
	Select **URLF** as the **Destination Mode**, **Category** as the **Type**, and **Health and Medicine** as the **Value** to match, if the connection is destined to any websites in the Health and Medicine category of the URLF database. Then click **Add**.
Service Chain	Select the name of a **Service Chain** (defined in the previous procedure) or an action—either **Bypass** or **Reject**.
	Select **Bypass** in the **Service Chain** selector to enforce a bypass action when both source and destination context filters match for an outbound connection.

Figure 27: Sample TCP service chain classifier

4. When your classifier rule configuration is complete, click **Finished**.

5. Repeat Steps 2 and 3 to create multiple TCP service chain classifiers.

6. If your answer to "**Do you want to pass UDP traffic through the transparent proxy unexamined?**" in the General Properties configuration was "**No, manage UDP traffic by classification**," you will be presented with a **UDP Service Chain Classifiers** screen to create UDP rules similar to the TCP rules. Create and configure them following the same basic principles.

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

Handling NAT

When a firewall is deployed as a service in the SSL Orchestrator service chain, it is no longer the Internet edge device. So performing the network address translation (NAT) on this firewall is no longer advisable. It is also important to perform NAT of the client's outbound traffic after the firewall default routes to the F5 device for re-encryption. There are two ways to handle this:

- **Option A**: Implement NAT on the F5 system using the SNAT pool feature. (See Figure 28.). In this case the NAT will be performed for the client's outbound traffic on the egress of the F5 system. In the case of firewalls deployed as sandwich pool using two F5 systems, NAT should be implemented on the egress F5 system.
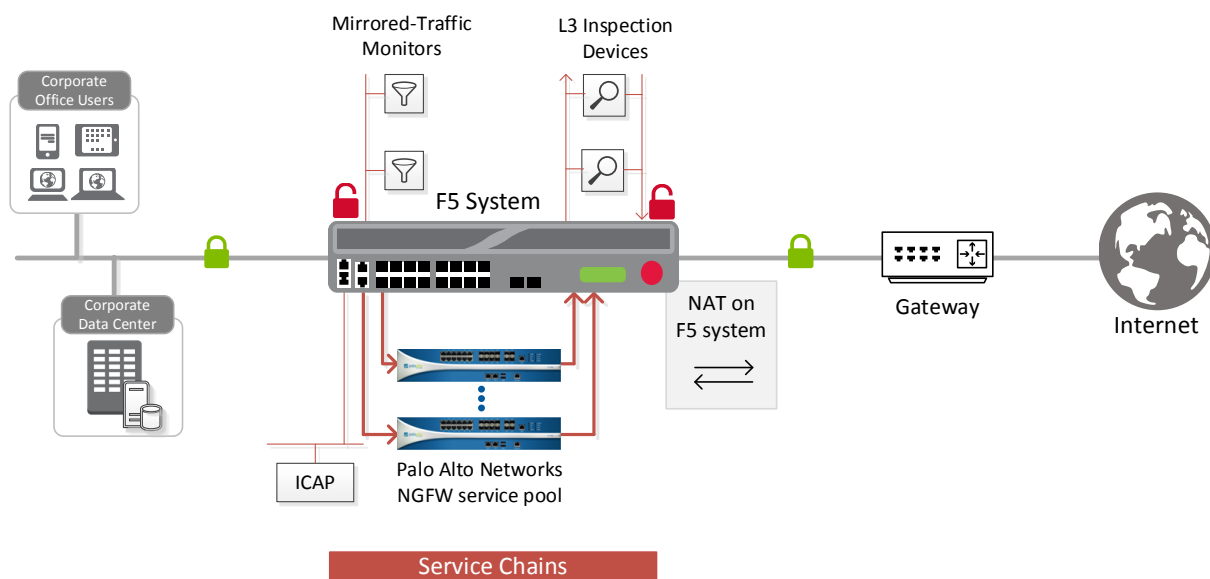

Figure 28: NAT on the BIG-IP system (option A)

Traditionally, an edge firewall is often implemented on the perimeter to inspect/control access to multiple protocols, and not all of these protocols are supported by SSL Orchestrator. When this firewall is moved from the edge and configured in the service chain to inspect decrypted traffic, any unsupported protocol traffic that goes around SSL Orchestrator is not inspected and therefore potentially vulnerable. The second option, Option B explained below, recommends the needed design change to overcome this challenge, as well as NAT recommendations.

- **Option B**: A Palo Alto Networks NGFW platform can perform more than firewall functions; it can also inspect and protect from threats. Segregate the firewall and inspection functionalities of the NGFW onto two different physical or virtual systems (vsys), and implement NAT post re-encryption on the edge firewall while the inspection modules (IPS and WildFire) remain part of the system in the service chain. (See Figure 29.) In this case, the F5 system can either hand off the re-encrypted packets to the edge firewall, or forward and re-route the traffic from the edge firewall to the gateway.
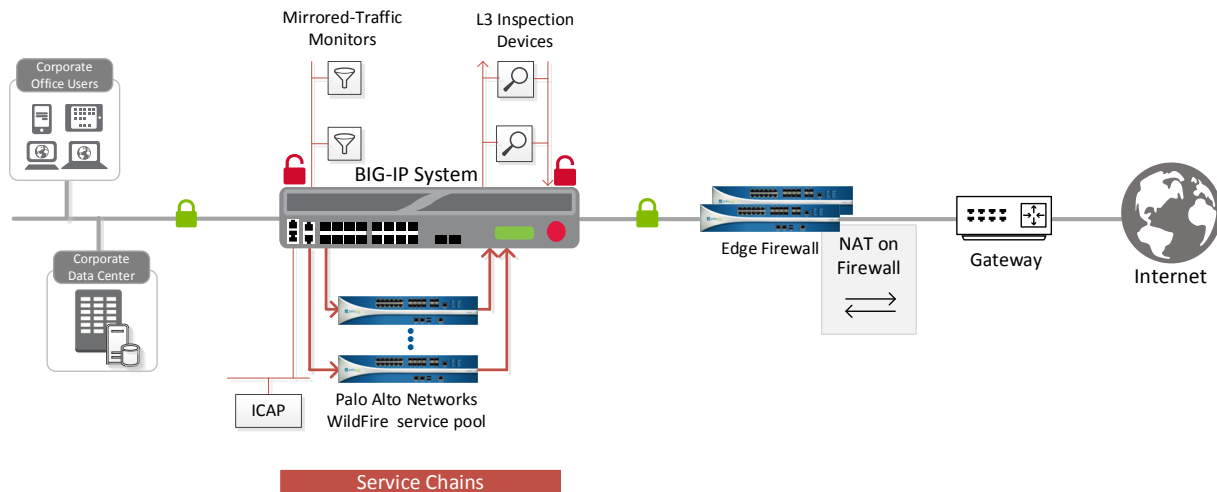
Figure 29: NAT on the Palo Alto Networks firewall (option B)

Testing the Solution

You can test the deployed solution using the following options:

- **Server certificate test**

  Open a browser on the client system and navigate to an HTTPS site, for example, https://www.google.com. Once the site opens in the browser, check the server certificate of the site and verify that it has been issued by the local CA set up on the F5 system. This confirms that the SSL forward proxy functionality enabled by SSL Orchestrator is working correctly.

- **Decrypted traffic analysis on the F5 system**

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

  ```
  tcpdump –lnni eth<n> -Xs0
  ```

- **Decrypted traffic analysis on the Palo Alto Networks NGFW**

  From the web UI, go to **Monitoring > Packet Capture > Create**, and enable a **Packet Filter**. Create stages to capture packets, specify file names, and then click **OK**.

Download the captured file(s) and analyze the HTTP packets. The packet header and payload should be in clear text, indicating SSL decryption. It is very important to turn off packet capture once the job completes.