



BIG-IP SSL Orchestrator and Cisco Firepower Threat Defense

SSL/TLS Visibility with Service Chaining for Advanced Malware Protection



Table of Contents

| | |
|-----------|--|
| 3 | Introduction |
| 3 | The F5 and Cisco Integrated Solution |
| 4 | SSL/TLS Visibility: How Do We Do it? |
| 5 | Dynamic Service Chaining |
| 6 | Topologies |
| 6 | License Components |
| 7 | Sizing |
| 8 | Traffic Exemptions for SSL/TLS Inspection |
| 8 | Best Practices for the Joint Solution |
| 8 | Architecture Best Practices |
| 9 | Security Best Practices |
| 9 | Certificate Requirements |
| 9 | IP Addressing |
| 10 | Initial Setup |
| 10 | Configure the VLANs and Self-IPs |
| 10 | Import a CA Certificate and Private Key |
| 11 | Update the BIG-IP SSL Orchestrator Version |
| 11 | Back up Your F5 System Configuration |
| 12 | BIG-IP SSL Orchestrator Configuration |
| 13 | Guided Configuration |
| 13 | Guided Configuration Workflow |
| 24 | Handling NAT |
| 25 | Testing the Solution |

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/TLS 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 can't 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 Cisco Advanced Malware Protection (AMP) solution solves these two SSL/TLS challenges. F5® BIG-IP® SSL Orchestrator® centralizes SSL/TLS 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 Cisco Firepower Threat Defense (FTD) firewalls—also called next-generation firewalls (NGFWs)—which can prevent previously hidden threats and block zero-day exploits. The Cisco FTD solution may be delivered using several combinations of Cisco Firepower and ASA platforms and software images. This solution eliminates the blind spots introduced by SSL/TLS 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 F5 and Cisco Integrated Solution

The F5 and Cisco integrated solution enables organizations to intelligently manage SSL/TLS 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/TLS visibility, it is impossible to identify and prevent such threats at scale.

Key highlights of the joint solution include:

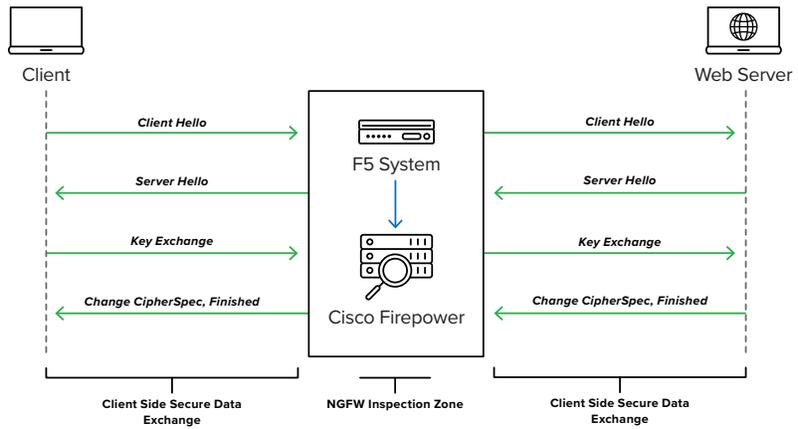
- **Flexible deployment modes** that easily integrate into even the most complex architectures, consolidate the security stack to reduce complexity, and deliver SSL/TLS visibility across the security infrastructure.

- **Centralized SSL/TLS decryption/re-encryption** with best-in-class SSL/TLS 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 perfect forward secrecy (PFS) enabled ciphers, to ensure full traffic visibility.
- **Advanced sandboxing capabilities** to perform automated static and dynamic analysis, then uncover stealthy threats and help the security team to understand, prioritize, and block sophisticated attacks.
- **Point-in-time malware detection and blocking** using anti-virus (AV) detection engines, one-to-one signature matching, machine learning, and fuzzy fingerprinting.
- **Global threat intelligence sharing** by Cisco experts who analyze millions of malware samples and push that intelligence to Cisco AMP to correlate against this context-rich knowledge base, which enables it to proactively defend against known and emerging threats.

SSL/TLS VISIBILITY: HOW DO WE DO IT?

The F5 system establishes two independent SSL/TLS 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 Cisco Firepower devices (or devices running Firepower Services) 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 1: SSL/TLS interception and content adaption for modifying HTTP requests and responses

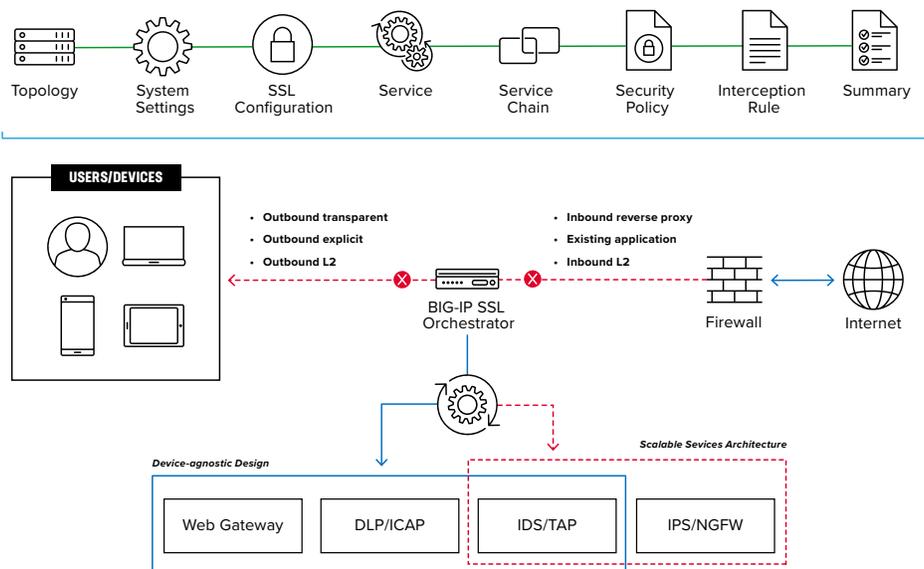


DYNAMIC SERVICE CHAINING

A typical security stack often consists of more than advanced anti-malware protection systems, with additional components such as a firewall, intrusion detection or prevention systems (IDSs/IPs), web application firewalls (WAFs), malware analysis tools, and more. To solve specific security challenges, administrators are accustomed to manually chaining these point security products. In this model, all user sessions are provided the same level of security, as this “daisy chain” of services is hard-wired.

BIG-IP SSL Orchestrator not only decrypts the encrypted traffic—it also load balances, monitors, and dynamically chains security services, including NGFWs, data loss prevention (DLP), IDSs/IPs, WAFs, and AV/anti-malware systems. It does this by matching user-defined policies, which determine what to intercept and whether to send data to one set of security services or another based on context. This policy-based traffic steering enables better utilization of existing security investments and helps reduce administrative costs.

Figure 2: A service chain



The powerful classification engine of BIG-IP SSL Orchestrator applies different service chains based on context derived from:

- Source IP/subnet
- Destination IP/subnet
- An F5® IP Intelligence Services subscription
- IP geolocation
- Host and domain name
- An F5 URL filtering (URLF) category subscription
- Destination port
- Protocol

TOPOLOGIES

Different environments call for different network implementations. While some can easily support SSL/TLS visibility at layer 3 (routed), others may require these devices to be inserted at layer 2. BIG-IP SSL Orchestrator can support all these networking requirements with the following topology options:

- Outbound transparent proxy
- Outbound explicit proxy
- Outbound layer 2
- Inbound reverse proxy
- Inbound layer 2
- Existing application

LICENSE COMPONENTS

The [BIG-IP SSL Orchestrator](#) product line—the i2800, r2800, i4800, r4800,i5800, r5800, i10800, r10800, r10900, i11800, i15800, and Virtual Edition High Performance (HP)—supports this joint solution. F5® VIPRION® platform and F5® VELOS® platform are also supported. BIG-IP SSL Orchestrator devices ship with an installed base module that provides both SSL/TLS interception and service chaining capabilities. Please contact your local F5 representative to further understand the licensing and deployment options.

Unless otherwise noted, references to BIG-IP SSL Orchestrator and the F5® BIG-IP® system in this document (and some user interfaces) apply equally regardless of the F5 hardware or virtual edition (VE) used. The solution architecture and configuration are identical.

Optionally, customers can add the functionality of:

- An **F5 URLF subscription** to access the URL category database.
- An **F5® IP Intelligence Services subscription** for IP reputation service.
- A network **hardware security module (HSM)** to safeguard and manage digital keys for strong authentication.

- **F5® Secure Web Gateway Services** to filter and control outbound web traffic using a URL database.
- **F5® BIG-IP® Access Policy Manager® (APM)** to authenticate and manage user access.
- **F5® BIG-IP® Advanced Firewall Manager™ (AFM)** to protect against denial-of-service.
- **F5® BIG-IP® Advanced WAF®** to protect against common vulnerabilities (CVEs) and web exploits, targeted attacks, and advanced threats.
- **An F5® BIG-IP® Local Traffic Manager™ (LTM)** add-on software license mode. This solution's supported on all F5® BIG-IP® iSeries® and older F5 hardware platforms and has no specific restrictions on additional F5 software modules (including the above software services). This option's suited for environments that need to deploy BIG-IP SSL Orchestrator on an existing BIG-IP device or have other functions that must run on the same device.

Cisco Firepower can be deployed:

- Via **FTD**, a unified software image, on the ASA 5000x and Firepower 2100/4100/9300 platforms.
- Via FirePOWER Services on a separate FirePOWER module on an ASA 5500x platform.

SIZING

The main advantage of deploying BIG-IP SSL Orchestrator in the corporate security architecture is that the wire traffic now can be classified as “interesting” traffic, which needs to be decrypted by BIG-IP SSL Orchestrator for inspection by Cisco Firepower, 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's important to consider the entire wire traffic volume to calculate the appropriate F5 device size. Depending on the chosen mode of deployment, administrators 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 [BIG-IP SSL Orchestrator data sheet](#) and consider the following factors when sizing the F5 system for the integrated solution:

- Port density.
- SSL/TLS bulk encryption throughput.
- System resources.
- The number of security services and devices in them.

TRAFFIC EXEMPTIONS FOR SSL/TLS INSPECTION

As noted, BIG-IP SSL Orchestrator 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 such as those for Microsoft Windows updates.
- Trusted backup solutions, such as 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 BIG-IP SSL Orchestrator 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

Best Practices for the Joint Solution

Several best practices can help optimize the performance, reliability, and security of the joint solution.

ARCHITECTURE BEST PRACTICES

To ensure a streamlined architecture that optimizes performance, reliability, and security, F5 recommendations include:

- Deploy inline. Any SSL/TLS visibility solution must be inline to the traffic flow to decrypt perfect forward secrecy (PFS) cipher suites such as elliptic curve Diffie-Hellman encryption (ECDHE).
- Deploy BIG-IP SSL Orchestrator in a device sync/failover device group (S/FDG) that includes the high-availability (HA) pair with a floating IP address.
- Use dual-homing. The Cisco FTDs must be dual-homed on the inward and outward VLANs with each F5 system in the device S/FDG.

- Achieve further interface redundancy with 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.

SECURITY BEST PRACTICES

BIG-IP SSL Orchestrator generally presents a new paradigm in the typical network architecture. Previously, client/server traffic passed encrypted to inline security services, which then had to perform their own decryption if they needed to inspect that traffic. When BIG-IP SSL Orchestrator is integrated into the security architecture, all traffic to a security device is decrypted—including user names, passwords, and social security and credit card numbers. It's therefore highly recommended that security services be isolated within a private, protected enclave defined by BIG-IP SSL Orchestrator. It's technically possible to configure BIG-IP SSL Orchestrator to send the decrypted traffic anywhere that it can route to, but this high-risk practice should be avoided.

CERTIFICATE REQUIREMENTS

Different certificate requirements apply depending on the traffic flow direction.

Outbound traffic flow (internal client to Internet)

An SSL/TLS certificate and associated private key—preferably a subordinate certificate authority (CA)—on the F5 system are needed to issue certificates to the end host for client-requested external resources that are being intercepted. To ensure that clients on the corporate network don't encounter certificate errors when accessing SSL/TLS-enabled websites from their browsers, this issuing certificate must be locally trusted in the client environment.

Inbound traffic flow (Internet users to internal applications)

Inbound SSL/TLS orchestration is similar to traditional reverse web proxy SSL/TLS handling. It minimally requires a server certificate and associated private key that matches the host name external users are trying to access. This may be a single instance certificate, or a wildcard or subject alternative name (SAN) certificate if inbound SSL/TLS orchestration is defined as a gateway service.

IP ADDRESSING

When a Cisco FTD 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 BIG-IP SSL Orchestrator, that are derived from a RFC2544 CIDR block of 192.19.0.0. This minimizes 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 F5 connected interfaces. You'll 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.

| Cisco FTD | Inward Interface IP | Inward/Internal Gateway | Outward Interface IP | Outward/Default Gateway |
|----------------------|---------------------|-------------------------|--------------------------|-------------------------|
| CISCO FTD-1 | 198.19.0.61/25 | 198.19.0.10/25 | 198.19.0.161/25 | 198.19.0.245/25 |
| CISCO FTD-2 | 198.19.0.62/25 | 198.19.0.10/25 | 198.19.0.162/25 | 198.19.0.245/25 |
| CISCO FTD-N N < 8 | 198.19.0.6n/25 | 198.19.0.10/25 | 198.19.0.16n/25 n ≤ 8 | 198.19.0.245/25 |

Initial Setup

Initial setup includes configuration of Cisco Firepower on ASA and setup of BIG-IP SSL Orchestrator. Once these steps are complete, you can proceed to configuration for your chosen specific deployment scenario.

CONFIGURE THE VLANS AND SELF-IPS

For BIG-IP SSL Orchestrator deployment in a layer 3 (routed or explicit proxy) topology, the F5 system must be configured with appropriate client-facing, outbound-facing VLANs and self-IPs and routes. The VLANs define the connected interfaces, and the self-IPs define the respective IPv4 and/or IPv6 subnets. Refer to the F5 [Routing Administration Guide](#) for configuration steps to set up the VLANs and self-IPs.

IMPORT A CA CERTIFICATE AND PRIVATE KEY

For BIG-IP SSL Orchestrator in an outbound traffic topology, a local CA certificate and private key are required to re-sign the remote server certificates for local (internal) clients. For BIG-IP SSL Orchestrator in an inbound traffic topology, remote clients terminate their SSL/TLS sessions at the F5 system, so it must possess the appropriate server certificates and private keys. Refer to the F5 support article on [managing SSL/TLS certificates for F5 systems](#) to understand the procedure.

UPDATE THE BIG-IP SSL ORCHESTRATOR VERSION

Periodic updates are available for BIG-IP SSL Orchestrator. To download the latest:

1. Visit downloads.f5.com. You'll need your registered F5 credentials to log in.
2. Click **Find a Download**.
3. Scroll to the **Security** product family, select **SSL Orchestrator**, and click the link.

Figure 3: The F5 product download web page

| | |
|-----------------|--|
| Security | Security_v17.x / Virtual Edition |
| | Security_v16.x / Virtual Edition |
| | Security_v15.x / Virtual Edition |
| | Security_v14.x / Virtual Edition |
| | Security_v13.x / Virtual Edition |
| | Security_v12.x / Virtual Edition |
| | DDoS Hybrid Defender |
| | SSL Orchestrator |

4. Select and download the latest version of the BIG-IP SSL Orchestrator .rpm file.
5. Read the appropriate Release Notes before attempting to use the file.
6. Log into the F5 system. On the F5 web UI in the **Main** menu, navigate to **SSL Orchestrator > Configuration** and click **Upgrade SSL Orchestrator** in the upper right.
7. Click **Choose File** and navigate to the .rpm file you downloaded. Select it and click **Open**.
8. Click **Upload and Install**.

You are now ready to proceed to detailed configuration.

BACK UP YOUR F5 SYSTEM CONFIGURATION

Before beginning detailed BIG-IP 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 any issues arise.

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/TLS private keys from the UCS archive, from the **Private Keys** menu, select **Exclude**.

Figure 4: New system archive creation

| General Properties | |
|--------------------|-----------------------------|
| File Name | SSLO-state0 |
| Encryption | Disabled |
| Private Keys | Include |
| Version | BIG-IP 17.0.0.1 Build 0.0.4 |

Cancel Finished

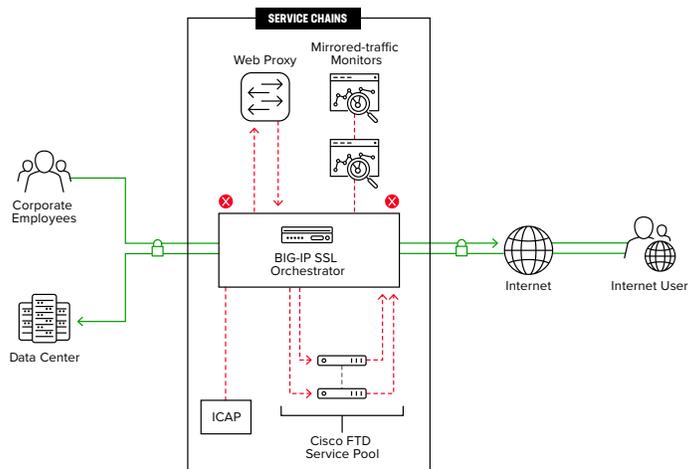
5. Click **Finished** to create the UCS archive file.
6. When the backup process is done, examine the status page for any reported errors before proceeding to the next step.
7. Click **OK** to return to the **Archive List** page.
8. Copy the .ucs file to another system.

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 F5 system configuration, see Solution K13132 on AskF5: [AskF5 Solution K13132: Backing up and restoring configuration files](#).

BIG-IP SSL Orchestrator Configuration

Cisco FTD can be configured as a layer 3 (L3) or layer 2 (L2) or TAP service in BIG-IP SSL Orchestrator. The sample configuration below will focus on a traditional outbound (forward proxy) use case with Cisco FTD configured as an L2 service as shown in Figure 5. BIG-IP SSL Orchestrator steers the unencrypted and decrypted web traffic through the Cisco FTD pool, which is part of a service chain(s) of security devices.

Figure 5: A sample L2 service deployment architecture

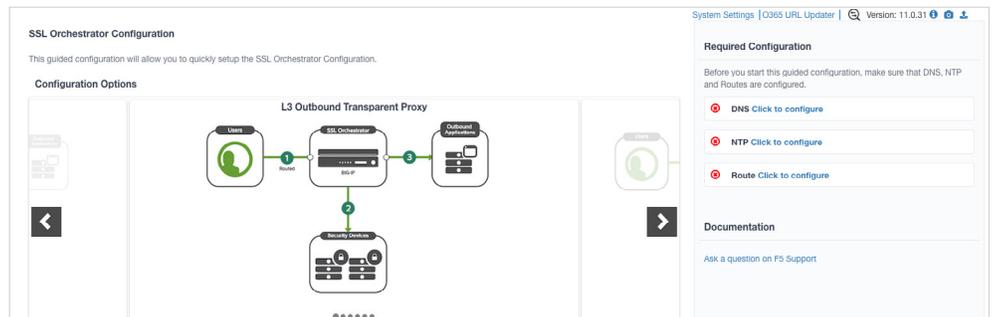


GUIDE CONFIGURATION

The BIG-IP SSL Orchestrator guided configuration presents a completely new and streamlined user experience. This workflow-based architecture provides intuitive, reentrant configuration steps tailored to a selected topology. These steps walk through the guided configuration to build a simple transparent forward proxy:

1. Once logged into the F5 system, on the F5 web UI **Main** menu, click **SSL Orchestrator > Configuration**.
2. Take a moment to review the various configuration options.
3. (Optional.) Satisfy any of the DNS, NTP, and Route prerequisites from this initial configuration page. Keep in mind, however, that the BIG-IP SSL Orchestrator guided configuration will provide an opportunity to define DNS and route settings later in the workflow. Only NTP isn't addressed later.

Figure 6: The initial guided configuration page



4. No other configurations are required in this section, so click **Next**.

GUIDED CONFIGURATION WORKFLOW

The first stage of the guided configuration addresses topology.

Figure 7: The guided configuration workflow

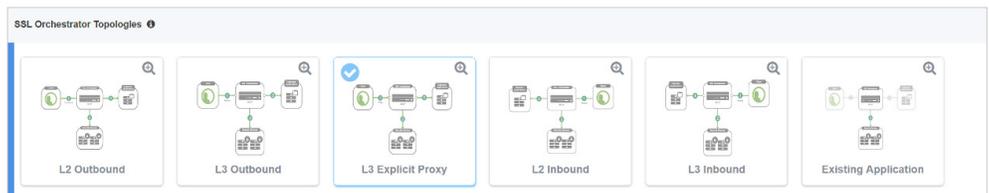


Topology properties

1. BIG-IP SSL Orchestrator creates discreet configurations based on the selected topology. An explicit forward proxy topology will ultimately create an explicit proxy listener. Make appropriate selections in the **Topology Properties** section of the configuration, using this guidance:

| Topology Properties | User Input |
|------------------------------------|--|
| NAME | Enter a Name for the BIG-IP SSL Orchestrator deployment. |
| DESCRIPTION | Enter a Description for this deployment |
| PROTOCOL | <p>The Protocol option presents four protocol types:</p> <ul style="list-style-type: none"> • TCP: Creates a single TCP wildcard interception rule for the L3 inbound, L3 outbound, and L3 explicit proxy topologies. • UDP: Creates a single UDP wildcard interception rule for L3 inbound and L3 outbound topologies. • Other: Creates a single “any protocol” wildcard interception rule for L3 inbound and L3 outbound topologies. Typically used for non-TCP/UDP traffic flows. • Any: Creates the TCP, UDP, and non-TCP/UDP interception rules for outbound traffic flows. Figure 7 and the sample configuration here demonstrate this option. |
| IP FAMILY | Specify whether you want this configuration to support IPv4 addresses or IPv6 addresses. |
| BIG-IP SSL ORCHESTRATOR TOPOLOGIES | <p>The BIG-IP SSL Orchestrator Topologies option page presents six topologies:</p> <ul style="list-style-type: none"> • L3 explicit proxy: The traditional explicit forward proxy. The sample configuration presented here uses this topology. • L3 outbound: The traditional transparent forward proxy. • L3 inbound: A reverse proxy configuration. • L2 inbound: Provides a transparent path for inbound traffic flows, inserting BIG-IP SSL Orchestrator as a bump-in-the-wire in an existing routed path, where BIG-IP SSL Orchestrator presents no IP addresses on its outer edges. • L2 outbound: Provides a transparent path for outbound traffic flows, inserting BIG-IP SSL Orchestrator as a bump-in-the-wire in an existing routed path, where BIG-IP SSL Orchestrator presents no IP addresses on its outer edges. • Existing application: Designed to work with existing BIG-IP LTM applications that already perform their own SSL/TLS handling and client-server traffic management. The existing application workflow proceeds directly to service creation and security policy definition, then exits with a BIG-IP SSL Orchestrator-type access policy and per-request policy that can easily be consumed by a BIG-IP LTM virtual server. <p>The sample configuration presented here deploys BIG-IP SSL Orchestrator as an L3 explicit proxy for decrypting outbound SSL/TLS traffic. See Figure 8.</p> |

Figure 8: Sample topology configuration



2. Click **Save & Next**

SSL configuration

This section defines the specific SSL/TLS settings for the selected topology (a forward proxy in this example) and controls both client-side and server-side SSL/TLS options. If existing SSL/TLS settings are available from a previous workflow, they can be selected and reused. Otherwise, the **SSL Configuration** section creates new SSL/TLS settings.

Figure 9: SSL configuration in the workflow



1. Click **Show Advanced Settings** on the right.
2. Make appropriate **SSL Configuration** selections using this guidance.

| SSL Configuration | User Input |
|----------------------------|--|
| SSL/TLS PROFILE | |
| NAME | Enter a Name for the SSL/TLS profile. |
| DESCRIPTION | Enter a Description for this SSL/TLS profile.. |
| CLIENT-SIDE SSL/TLS | |
| CIPHER TYPE | <p>The cipher type can be a Cipher Group or Cipher String. The latter's recommended.</p> <ul style="list-style-type: none"> • For Cipher Group, select a previously defined cipher group (which can be defined if necessary by navigating to Local Traffic > Ciphers > Groups.) • When Cipher String is selected, a field will be populated with the DEFAULT option, which is optimal for most environments. (Otherwise, users could also enter a cipher string that appropriately represents the client-side SSL/TLS requirement.) |
| CERTIFICATE KEY CHAINS | <p>The certificate key chain represents the certificate and private key used as the template for forged server certificates. While reissuing server certificates on the fly is generally easy, private key creation tends to be a CPU-intensive operation. For that reason, the underlying SSL/TLS forward proxy engine forges server certificates from a single defined private key. This setting gives administrators the opportunity to apply their own template private key and to optionally store that key in a FIPS-certified HSM for additional protection. The built-in default certificate and private key uses 2K RSA and is generated from scratch when the F5 system is installed.</p> <p>Select the default.crt certificate, default.key key, and default.crt chain and leave the Passphrase field empty, then click Add.</p> |
| CA CERTIFICATE KEY CHAINS | <p>An SSL/TLS forward proxy must re-sign or forge a remote server certificate to local clients using a local CA certificate, and local clients must trust this local CA. This setting defines the local CA certificate and private key used to perform the forging operation.</p> <p>Specify one or more configured CA certificates and keys that were imported, then click Add.</p> |
| SERVER-SIDE SSL/TLS | |
| CIPHER TYPE | Select Cipher String for the default cipher list. |
| CIPHERS | Uses the ca-bundle.crt file, which contains all well-known public CA certificates for client-side processing. |

| | |
|--|--|
| EXPIRED CERTIFICATE RESPONSE CONTROL | Select whether to Drop or Ignore the connection even if the specified Certificate Response Control (CRL) file's expired. |
| UNTRUSTED CERTIFICATE RESPONSE CONTROL | Select drop or ignore the connection even if the specified CRL file isn't trusted. |
| OCSP | Specify the supported OCSP . |
| CRL | Specify the supported CRL . |

3. Click **Save & Next**.

Note: SSL/TLS settings minimally require an RSA-based template and CA certificates but can also support elliptic curve (ECDSA) certificates. In this case, BIG-IP SSL Orchestrator would forge an EC certificate to the client if the SSL/TLS handshake negotiated an ECDHE_ECDSA cipher. To enable EC forging support, add both an EC template certificate and key, and an EC CA certificate and key.

Create the Cisco FTD service

You can configure Cisco FTD either in inline mode as an L2 or L3 hop, or in TAP mode.

Configuring as an L2 service

The Service List section defines the security services that interact with BIG-IP SSL Orchestrator. The guided configuration includes a services catalog that contains common product integrations. Beneath each of these catalog options is one of the five basic service types: L3, L2, ICAP, TAP, and HTTP service.

The service catalog also provides “generic” security services. (It may be necessary to scroll down to see additional services.)

Figure 10: Service configuration



To configure the service:

1. Under **Service List**, click **Add Service**.
2. In the service catalog, double click **Cisco FTD** service. (If the version of BIG-IP SSL Orchestrator you're using doesn't have this option, then use the generic L2 service.)
3. The **Service Properties** page displays.
4. Configure the service using the guidance below. To configure either as an L3 or TAP service, refer to the next two sections of this document.

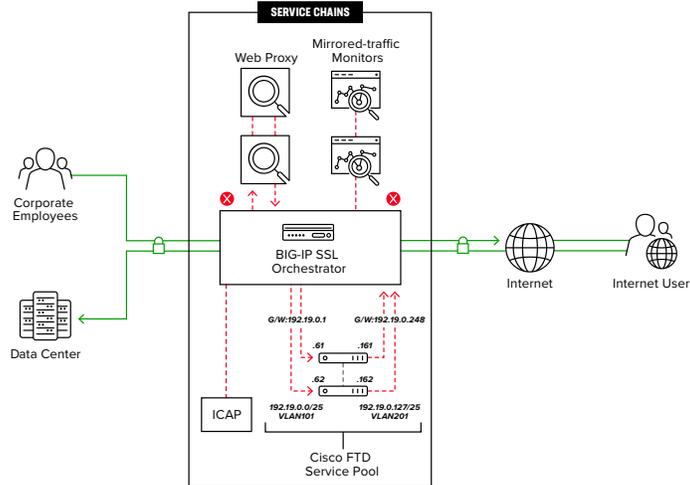
| Service Properties | User Input |
|-------------------------|---|
| SERVICE SETTINGS | |
| NAME | Enter a Name for the Cisco FTD service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters aren't case sensitive. |
| DESCRIPTION | Type a Description for the service. |
| NETWORK CONFIGURATION | <p>Click Add, then create the From VLAN and To VLAN pairs (inward and outward VLANs) by entering a name and selecting the interface. These VLAN pairs and the associated interfaces define the network connectivity between BIG-IP SSL Orchestrator and the inline security device.</p> <p>If you have configured BIG-IP SSL Orchestrator systems in a sync/failover device group for HA, then the VLAN pairs must be connected to the same L2 virtual network from every device.</p> <p>If you have multiple Cisco FTD appliances, choose the respective VLAN pair and click Add. You can enter the ratio for every FTD in the pool to control the load it receives.</p> |
| SERVICE DOWN ACTION | <p>The certificate key chain represents the certificate and private key used as the template for forged server certificates. While reissuing server certificates on the fly is generally easy, private key creation tends to be a CPU-intensive operation. For that reason, the underlying SSL/TLS forward proxy engine forges server certificates from a single defined private key. This setting gives customers the opportunity to apply their own template private key and optionally to store that key in a FIPS-certified HSM for additional protection. The built-in default certificate and private key uses 2K RSA and is generated from scratch when the BIG-IP system is installed.</p> <p>Select the default.crt certificate, default.key key, and default.crt chain and leave the Passphrase field empty, then click Add.</p> |
| ENABLE PORT REMAP | Select Enable Port Remap . |
| REMAP PORT | For the Cisco FTD to recognize that the steered traffic has been decrypted, it needs to be sent on a non-443 TCP port. Select a non-443 port. |
| IRULES | BIG-IP SSL Orchestrator allows for the insertion of additional F5® iRules® logic at different points, but additional iRules aren't required. An iRule defined at the service only affects traffic flowing across this service. It's important to understand, however, that these iRules mustn't be used to control traffic flow (for example, pools, nodes, or virtual servers), but rather should be used to view/modify application layer protocol traffic. For example, an iRule assigned here could be used to view and modify HTTP traffic flowing to/from the service. Leave this field empty to configure without iRules. |

- Click **Save** to return to the Service List section. To configure additional services, click **Add Service** to access the service catalog again.
- Once all the desired services are created, click **Save & Next** to move on to the service chain setup.

Configuring as an L3 service

When Cisco FTD is configured as an L3 service as shown in Figure 11, BIG-IP SSL Orchestrator routes the unencrypted and decrypted web traffic through the Cisco FTD pool, which is part of the service chain(s) of security devices.

Figure 11: L3 service deployment architecture



1. On the **Service Properties** page (refer to the previous procedure if necessary), configure the service using this guidance:

| Service Properties | User Input |
|-------------------------|--|
| SERVICE SETTINGS | |
| NAME | Enter a Name for the Cisco FTD service. This name can contain 1-15 alphanumeric or underscore characters but must start with a letter. Letters aren't case sensitive. |
| DESCRIPTION | Enter a Description for the Cisco FTD Service. |
| SERVICE DEFINITION | Click Create New , then create the To Service VLAN (outward VLAN) by entering a name and selecting the interface. The VLAN and the associated interface define the network connectivity from BIG-IP SSL Orchestrator to the inline security device. |
| SERVICE DOWN ACTION | Specify how you want the system to handle a failure of the L3 service or times when it is otherwise unavailable: <ul style="list-style-type: none"> • Ignore: Specifies that the traffic to the service is ignored and is sent to the next service in the chain. • Drop: Specifies that the system initiates a close on the client connection. • Reset: Specifies that the system immediately sends a Reset on the client connection for TCP traffic. For UDP traffic, this action's the same. |
| SECURITY DEVICES | Click Add and enter the IP address of the inward VLAN configured on Cisco FTD and connected to BIG-IP SSL Orchestrator. If you have multiple FTDs, add the IP address of the inward VLAN on each FTD. BIG-IP SSL Orchestrator will create a load balancing pool of FTDs. |

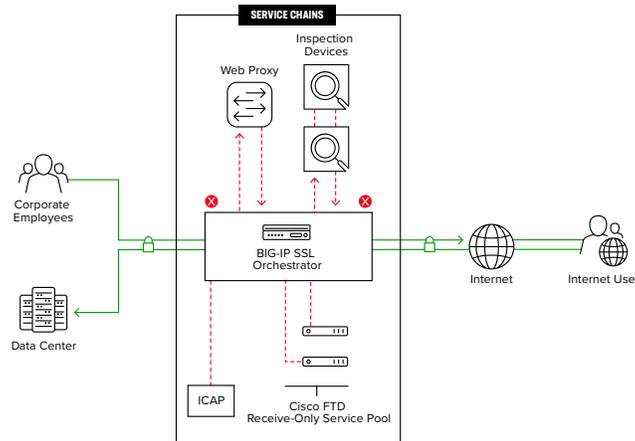
| FROM SERVICE CONFIGURATION | Click Create New , then create the From Service VLAN (inward VLAN) by entering a name and selecting the interfaces. The VLAN and the associated interface define the network connectivity to BIG-IP SSL Orchestrator from the inline security device. |
|----------------------------|--|
| REMAP PORT | For Cisco FTD to recognize that the steered traffic has been decrypted, it needs to be sent on a non-443 TCP port. Select and enter a non-443 port. |
| MANAGE SNAT SETTINGS | Choose whether you want to use network addresses translation. |
| RESOURCES | |
| IRULES | Additional iRules are not required, but BIG-IP SSL Orchestrator allows for the insertion of additional iRules logic at different points. An iRule defined at the service only affects traffic flowing across this service. It's important to understand, however, that these iRules mustn't be used to control traffic flow (for example, pools, nodes, or virtual servers), but rather should be used to view/modify application layer protocol traffic. For example, an iRule assigned here could be used to view and modify HTTP traffic flowing to/from the service. Leave this field empty to configure without iRules. |

2. Click **Save**.

Configuring as a TAP service

In a TAP service mode (see Figure 12), the F5 system copies the unencrypted and decrypted web traffic to the Cisco FTD pool, which is part of the service chain(s) of security devices.

Figure 12: A TAP service deployment architecture



1. On the TAP **Service Properties** page, configure the service using this guidance:

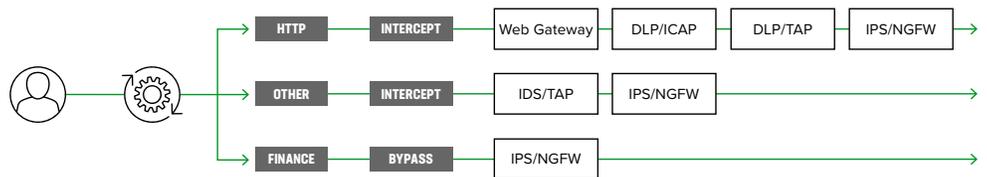
| Configuration Field | User Input |
|---------------------|---|
| NAME | Enter a Name for the TAP service. |
| TAP SERVICE | |
| MAC ADDRESS | Type the MAC Address of the receiving interface of the Cisco FTD. This address must be reachable by an F5 system VLAN. |

| | |
|---------------------|--|
| VLAN | Click Create New and specify the VLAN where the Cisco FTD device resides. |
| INTERFACE | Select the associated F5 system interface. |
| SERVICE DOWN ACTION | Specify how you want the system to handle a failure of the TAP service or when it is otherwise unavailable. <ul style="list-style-type: none"> Ignore: Specifies that the traffic to the service is ignored and is sent to the next in chain. Drop: Specifies that the system initiates a close on the client connection. Reset: Specifies that the system immediately sends an RST on the client connection for TCP and UDP traffic. |
| PORT REMAP | For the Cisco FTD to recognize that the steered traffic has been decrypted, it needs to be sent on a non-443 TCP port. Select a non-443 port. |

Configuring service chains

Service chains are arbitrarily ordered lists of security devices. Based on the ecosystem’s requirements, different service chains may contain different, reused sets of services, and different types of traffic can be assigned to different service chains. For example, HTTP traffic may need to go through all the security services while non-HTTP traffic goes through a subset of those services, and traffic destined to a financial service URL can bypass decryption and still flow through a smaller set of security services.

Figure 13: Different traffic flowing through chains of different security services



Each service chain’s linked to service chain classifier rules and processes specific connections based on those rules, which look at protocol, source, and destination addresses. Service chains can include each of the three types of services (inline, ICAP, or receive-only), as well as decryption zones between separate ingress and egress devices.

Figure 14: Configuring service chains



To create a new service chain containing all the configured security services:

1. Under Services List, click **Add Service**. Make selections using this guidance:

| Service Chain Properties | User Input |
|--------------------------|--|
| NAME | Enter a Name for the per-request service chain. |
| DESCRIPTION | Provide a Description for this service chain. |
| SERVICES | Select any number of desired services from the Services Available list and move them into the Selected Service Chain Order column. Optionally, order them as required. |

2. Click **Save & Next**.

Security policy

Security policies are the set of rules that govern how traffic's processed in BIG-IP SSL Orchestrator. The actions a rule can require include:

- Whether or not to allow the traffic indicated in the rule.
- Whether or not to decrypt that traffic.
- Which service chain (if any) to pass the traffic through.

Figure 15: Configuring security policy



The guided configuration of BIG-IP SSL Orchestrator presents an intuitive rule-based, drag-and-drop user interface for the definition of security policies. In the background, BIG-IP SSL Orchestrator maintains these security policies as visual per-request policies. If traffic processing is required that exceeds the capabilities of the rule-based user interface, the underlying per-request policy can be managed directly.

1. To create a rule, click **Add**.
2. Create a security rule as required.
3. Click **Add** again to create more rules or click **Save & Next**.

Figure 16: Configuring security policy

| Rules | | | | | Add |
|--------------|--|--------|--------------------------|---------------|-----|
| Name | Conditions | Action | SSL Forward Proxy Action | Service Chain | |
| Pinnars_Rule | SSL Check and SNI Category is Pinnars | Allow | Bypass | - | |
| All Traffic | All | Allow | Intercept | - | |

Figure 17: Configuring interception rules

Interception rules

Interception rules are based on the selected topology and define the listeners (analogous to BIG-IP LTM virtual servers) that accept and process different types of traffic, such as TCP, UDP, or other. The resulting BIG-IP LTM virtual servers will bind the SSL/TLS settings, VLANs, IPs, and security policies created in the topology workflow.



1. To configure the interception rule, follow this guidance:

| Intercept Rule | User Input |
|------------------------------|--|
| LABEL | Enter a Name for the label. |
| DESCRIPTION | Enter a Description for this rule. |
| PROXY SERVER SETTINGS | This setting, which displays when configuring an explicit proxy, defines the BIG-IP SSL Orchestrator explicit proxy listening IP address and proxy port. For explicit proxy authentication, this section also allows for the selection of a BIG-IP APM SWG-explicit access policy. |
| IPV4 ADDRESS | Specify the explicit proxy listening IP address. |
| PORT | Specify the port number. |
| ACCESS PROFILE | Specify the access policy (optional). |
| INGRESS NETWORK | |
| VLANS | This defines the VLANs through which traffic will enter. For a forward proxy topology (outbound), this would be the client-side VLAN (intranet). |

2. Click **Save & Next**.

Egress setting

The **Egress Setting** section defines topology-specific egress characteristics.

Figure 18: Configuring egress settings



1. To configure these characteristics, follow this guidance:

| Egress Settings | User Input |
|----------------------|--|
| MANAGE SNAT SETTINGS | Define if and how source NAT (SNAT) is used for egress traffic. |
| GATEWAYS | Enter the IP address of the next hop route for traffic. For an outbound configuration, this is usually a next hop upstream router. |

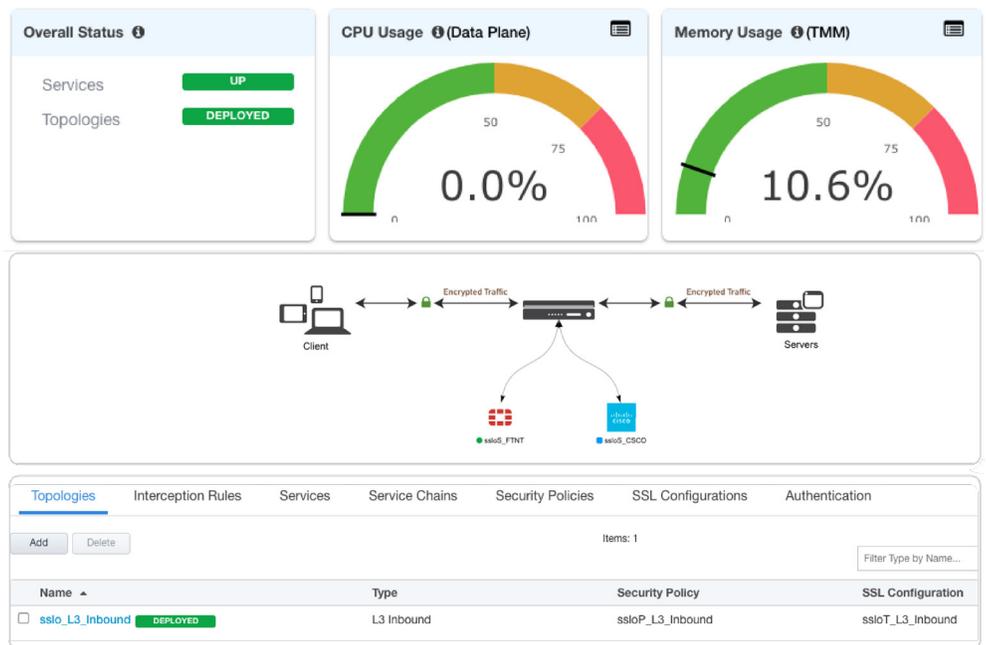
2. Once done, click **Save & Next**.

Configuration summary and deployment

The configuration summary presents an expandable list of all the workflow-configured objects

1. To review the details for any given setting, click the corresponding arrow icon on the far right.
2. To edit any given setting, click the corresponding pencil icon. Clicking the pencil icon will display the selected settings page in the workflow.
3. When you're satisfied with the defined settings, click **Deploy**. Upon successful deployment of the configuration, BIG-IP SSL Orchestrator will display a dashboard. See Figure 19.

Figure 19: The configuration dashboard after deployment



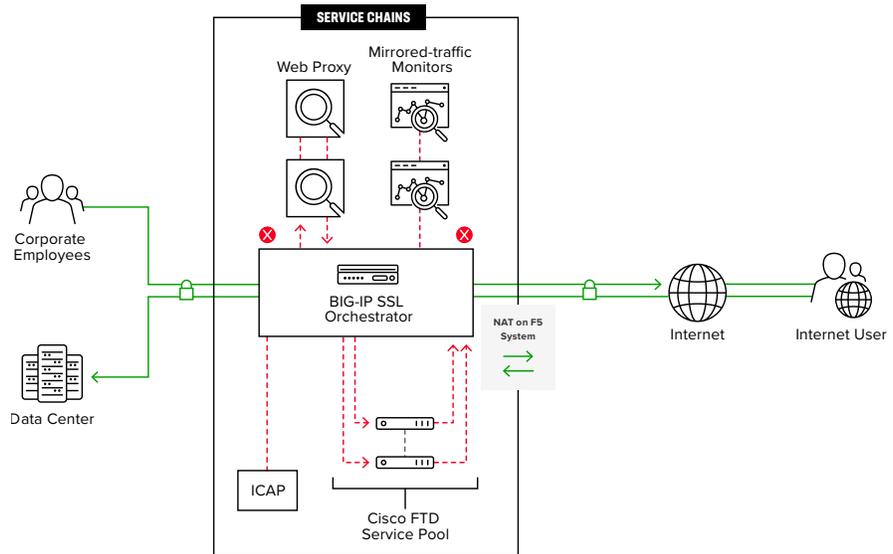
4. This completes configuration of BIG-IP SSL Orchestrator as a forward proxy. At this point an internal client should be able to browse to external (Internet) resources, and decrypted traffic will flow across the security services.

Handling NAT

When a Cisco ASA with Firepower Services module is deployed as a service in the BIG-IP SSL Orchestrator service chain, it's no longer the Internet edge device. Therefore, performing the network address translation (NAT) on ASA is no longer advisable. It's also important to perform NAT of the client's outbound traffic after it exits the ASA to the F5 egress 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 20.) In this case, the NAT will be performed for the client's outbound traffic on the egress of the F5 system. When firewalls are deployed as a sandwich pool using two F5 systems, NAT should be implemented on the egress F5 system.

Figure 20: NAT on the F5 system (option A)

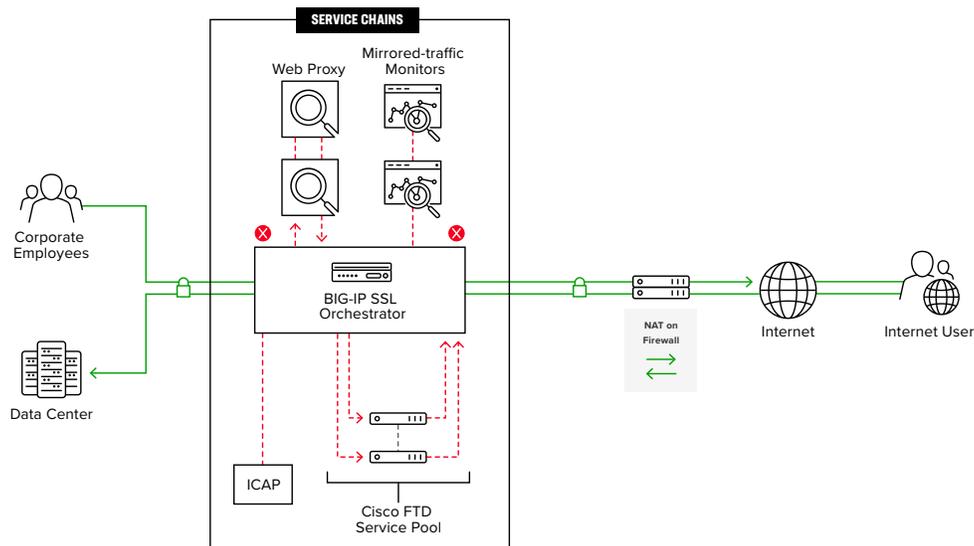


Traditionally, an ASA is often implemented on the perimeter to inspect/control access to multiple protocols, and not all these protocols are supported by BIG-IP SSL Orchestrator. When this ASA is moved from the edge and configured in the service chain to inspect decrypted traffic, any unsupported protocol traffic that goes around BIG-IP SSL Orchestrator isn't inspected and potentially vulnerable.

The second option, Option B, represents the needed design change to overcome this challenge, as well as NAT recommendations.

- **Option B:** segregate the ASA firewall capabilities and Firepower Services onto two different physical or virtual contexts and implement NAT post re-encryption on the edge firewall while the inspection SFR module remains part of the F5 system in the service chain. (See Figure 21.) 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 21: NAT on the Cisco ASA (option B)



Testing the Solution

Test the deployed solution using these 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's been issued by the local CA set up on the F5 system. This confirms that the SSL/TLS forward proxy functionality enabled by BIG-IP 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/TLS interception by the BIG-IP device.

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

- **Decrypted traffic analysis on the Cisco ASA:** 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/TLS decryption. It's very important to turn off packet capture once the job completes.

