# Contents

Introduction.................................................................................................................................................. 4

The Integrated F5 and FireEye Solution........................................................................................................ 4

SSL Visibility: How Do We Do It?................................................................................................................ 5

Service chaining ........................................................................................................................................ 6

Deployment Planning ................................................................................................................................... 7

Sizing.......................................................................................................................................................... 8

License components ................................................................................................................................... 8

Horizontal scaling...................................................................................................................................... 9

Traffic exemptions for SSL inspection....................................................................................................... 9

Certificate requirements............................................................................................................................ 10

Deployment modes ................................................................................................................................... 10

Architecture best practices....................................................................................................................... 11

Configuration: Initial Setup........................................................................................................................ 12

Configure FireEye NX .............................................................................................................................. 12

Run the SSL Orchestrator Setup Wizard .................................................................................................. 12

Update the SSL Orchestrator version .................................................................................................... 16

Back up your F5 system configuration.................................................................................................... 18

Configuring a Single F5 System with FireEye NX in Inline Mode (Burrito Design) .............................. 19

Configure SSL Orchestrator.................................................................................................................... 20

Configuring the BIG-IP System with FireEye NX in TAP Mode ............................................................ 26

Create the receive-only service .............................................................................................................. 27

Alternative Architectures.......................................................................................................................... 28

Two F5 systems with FireEye NX deployed as a service pool ................................................................. 28

Two F5 systems with FireEye NX devices sandwiched in the decryption zone....................................... 31

Creating service chains to link services ................................................................................................. 33

Creating TCP service chain classifier rules ............................................................................................ 34

Testing the Solution................................................................................................................................ 36
Introduction

SSL/TLS has been widely adopted by organizations to secure IP communications, and its use is increasing. While SSL provides data privacy and secure communications, it also creates challenges to security infrastructure components that are in place to inspect the encrypted traffic. In short, the encrypted communications cannot be seen like clear text and thus are passed through without inspection, rendering any defense-in-depth security architecture ineffective. This creates significant risks to businesses: What if attackers are hiding malware inside the encrypted traffic?

Security devices today, such as intrusion prevention systems (IPSs) and next-generation firewalls (NGFWs), lack the processing power to easily decrypt SSL/TLS traffic. This performance concern becomes even more challenging with the demands of 2048-bit certificates. The processing capacity of these security devices is further reduced when they are deployed in inline mode, taking not only the interesting traffic—that is, any wire traffic that needs to be inspected—but all the wire traffic. Alternatively, deploying these devices in monitoring mode conserves system resources but comes at a cost: they alert administrators to the threats but do not block them.

An integrated F5 and FireEye solution solves these two SSL/TSL challenges. F5® SSL Orchestrator™ centralizes SSL inspection across complex security architectures, providing flexible deployment options to decrypt and re-encrypt 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 FireEye NX devices, which can prevent previously hidden threats and block zero-day web 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 F5 and FireEye Solution

The integrated F5 and FireEye advanced threat protection 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

---

1 The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle.
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, determines 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.
- **Right-sized security infrastructure** by sending only appropriate traffic through security controls via service chains and URL filtering.
- **Coordinated support** from FireEye and F5.

![Figure 1: The integrated F5/FireEye solution](image)

**SSL Visibility: How Do We Do It?**

F5's industry-leading full proxy architecture enables the F5® BIG-IP® or F5® Herculon™ system 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 FireEye NX devices 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](image)

**Service chaining**

A typical security stack often consists of more than advanced anti-malware protection systems. It begins with a firewall but almost never stops there, with components such as intrusion detection/prevention systems (IDS/IPS), web application firewalls, data loss prevention (DLP), and more. To solve specific security challenges, security administrators are accustomed to manually chaining these multiple point security products by 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, SSL Orchestrator can load balance, monitor, and dynamically chain security services, including next-gen firewalls, DLP, IDS/IPS, web application firewalls, and anti-virus/malware, by matching the user-defined policies to determine whether to bypass or decrypt and whether to send to one set of security services or another. This policy-based traffic steering capability allows for better utilization of the existing security services investment and helps to reduce administrative costs.
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. With either platform, F5 SSL Orchestrator enables you 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 FireEye NX advanced threat protection 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 FireEye NX devices, 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 FireEye NX platform 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 system size. Depending on the mode of deployment you choose, you will need at least two interfaces on the F5 system for each FireEye NX device configured for inline mode and at least one interface for each FireEye NX 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 FireEye NX Platform datasheet for sizing considerations when selecting platforms for the integrated solution.

License components

The recently launched F5® Herculon SSL Orchestrator product line—the i2800, i5800, i10800—and 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. Deploying SSL Orchestrator on an F5 system requires TMOS 13.0 or higher, and you must provision BIG-IP® Local Traffic Manager™ (LTM) with a SSL forward proxy add-on license.

Optionally, customers can consider the following modules:

- A URLF Filtering subscription to use the URL category database for filtering.
- An F5 IP Intelligence subscription to detect and block known bad actors and malicious traffic.
- A network hardware security module (HSM) to safeguard and manage digital keys for strong authentication.

The following FireEye products and subscriptions are needed for deploying the solution:

- A FireEye Network Security (NX) appliance or MVX Smart Grid Distributed Deployment for advance threat protection
Horizontal scaling

The F5 system’s ability to steer and load-balance traffic to multiple security devices in a service or service pool enables the FireEye NX 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 FireEye NX devices with the F5 system load-balancing the unencrypted HTTP and decrypted HTTPS traffic to all the pool members. However, if you need multiple FireEye NX device pools, each taking a different traffic set based on user-defined criteria such as VLAN, tenant, or other criteria, you can accomplish that 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 FireEye NX service is part of.

Traffic exemptions for SSL inspection

As noted, the F5 system can be configured to distinguish between interesting and uninteresting traffic for the purposes of security processing. Examples of uninteresting traffic to be exempted from inspection (including those types that cannot be decrypted) may include:

- Guest VLANs.
RECOMMENDED DEPLOYMENT PRACTICES
F5 and FireEye NX: SSL Visibility with Service Chaining

- 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. 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

The service chain classifier rules of the F5 system enable administrators to enforce corporate Internet use policies, preserve privacy, and meet regulatory compliance.

Certificate requirements

An SSL certificate—preferably a subordinate certificate authority (CA)—and private key on the F5 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.

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 FireEye NX for advanced threat protection.

**Single or double F5 systems**

The F5 SSL visibility solution with inline FireEye NX device(s) can be deployed with one or two F5 systems.

- **Option 1: A single F5 system with inline FireEye NX platform.** This solution entails a single F5 system deployed to perform both decryption and re-encryption of SSL traffic, while FireEye NX device(s) are configured for inline mode and deployed as an L3 service pool on the F5 system.

- **Option 2: Two F5 systems with inline FireEye NX platform.** 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:
  - When there is a need for increased SSL throughput of the solution
  - 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 FireEye platform:

- **As a service pool managed on the ingress F5 system.** The advantage of deploying FireEye NX devices 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 exited the service chains to the sandwiched FireEye NX devices, it has the downside of limiting any service chain policy enforcement, as the FireEye NX devices is no longer a part of any services chain on the ingress F5 system. Moreover, it complicates the failover design. The firewalls now needed 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/FGD), which includes the active-standby pair, with a floating IP address for high availability (HA).
RECOMMENDED DEPLOYMENT PRACTICES
F5 and FireEye NX: SSL Visibility with Service Chaining

- Every FireEye NX in the service pool should 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 system does not need physical connections to the FireEye NX devices. All that the F5 system requires is L2 reachability to steer traffic through the devices. In slow networks, however, we recommend deploying the FireEye NX devices 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.

Configuration: Initial Setup

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

Configure FireEye NX

F5 SSL Orchestrator integrates with either a standard (integrated) NX appliance or the distributed Smart Grid deployment (either locally managed or via Cloud MVX). Either architecture can be deployed out of band or inline. While the out of band approach (on a TAP/SPAN port) is obviously easier to deploy and less intrusive, FireEye strongly recommends inline deployment to enable blocking of attacks and callbacks (C2 traffic).

Please refer to the System Administration Guide for FireEye NX at https://docs.fireeye.com to configure the FireEye NX device to inspect traffic for advanced threats. You need a license-bound user login to access this site.

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 BIG-IP Setup Wizard is substantially the same, 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
x System management connectivity may be lost if the management
x address changes. Accept these settings? [Y/n] y
x IP Address: 192.168.16.31
x Netmask: 255.255.255.0
x Default Route: 192.168.16.10
< Yes > < No >
```

Figure 5: Initial configuration of the management IP from the 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.

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.

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.

![Internal VLAN configuration](image)

**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.

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.

![Image](image-url)

**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](http://downloads.f5.com). You will need your registered F5 credentials to log in.
2. Click **Find a Download**.

![Figure 9: The F5 product download web page](https://example.com/download_page.png)

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

### 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.**
5. Click **Finished** to create the UCS archive file.
RECOMMENDED DEPLOYMENT PRACTICES
F5 and FireEye NX: SSL Visibility with Service Chaining

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: Backing up and restoring BIG-IP configuration files.

Configuring a Single F5 System with FireEye NX in Inline Mode (Burrito Design)

This deployment mode entails a single F5 system performing SSL visibility which 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 FireEye NX devices configured in inline 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.

![Diagram of F5 System with FireEye NX in Inline Mode](image)

Figure 12: The SSL Orchestrator solution with service chain using one F5 system
How traffic flows in this deployment option:

1. Client web traffic arriving at the F5 ingress 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 FireEye NX devices as part of a service chain via a service inward VLAN.

3. The HTTP traffic is inspected by the FireEye NX 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

The sample configuration below demonstrates SSL Orchestrator steering the outbound web traffic through the FireEye NX service, which is part of service chains of security devices. Please refer to the F5 Herculon SSL Orchestrator Setup guide for additional help during configuration.

General properties

This is the first step in creating the SSL Orchestrator application, and it 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) to create the SSL Orchestrator application. (Refer to the User Input column below for examples and tips.)

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Service Name</td>
<td>Enter a name without spaces or dashes for the SSL Orchestrator application service.</td>
</tr>
<tr>
<td>Do you want to set up separate ingress and egress devices with a cleartext zone between them?</td>
<td>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 <strong>No, use one BIG-IP device for ingress and egress</strong>. This sample configuration follows that option.</td>
</tr>
<tr>
<td>Which IP address families do you want to support?</td>
<td>Select <strong>Support IPv4 only</strong>. (Currently SSL Orchestrator only supports IPv4 families.)</td>
</tr>
<tr>
<td>Which proxy schemes do you want to implement?</td>
<td>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</td>
</tr>
<tr>
<td>Question</td>
<td>Answer</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>enter the IP address and port number of the explicit proxy.</td>
<td>Select <strong>Implement Transparent proxy only</strong>.</td>
</tr>
<tr>
<td>Do you want to pass UDP traffic through the transparent proxy unexamined?</td>
<td>This option only applies if you selected <strong>Implement transparent proxy only</strong> above. By default, transparent proxy mode manages TCP traffic but allows UDP traffic to pass through unexamined. Choose <strong>No</strong> to prevent the passage of unexamined UDP traffic. Otherwise, select the default, <strong>Yes, pass all UDP traffic unexamined</strong>.</td>
</tr>
<tr>
<td>Do you want to pass non-TCP, non-UDP traffic through the transparent proxy?</td>
<td>This option also only applies if you select <strong>Implement transparent proxy only</strong>. By default, transparent proxy mode passes through non-TCP, non-UDP traffic (such as IPSec, SCTP, and OSPF). Choose <strong>No</strong> to block. Otherwise, select the default, <strong>Yes, pass non-TCP, non-UDP traffic</strong>.</td>
</tr>
<tr>
<td>Which is the SSL Forward Proxy CA certificate?</td>
<td>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.</td>
</tr>
<tr>
<td>Which is the SSL Forward Proxy CA private key?</td>
<td>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.</td>
</tr>
<tr>
<td>What is the private-key passphrase (if any)?</td>
<td>Enter the private-key passphrase, if any. If the key does not have a passphrase, leave this field empty.</td>
</tr>
<tr>
<td>Which CA bundle is used to validate remote server certificates?</td>
<td>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.</td>
</tr>
<tr>
<td>Should connections to servers with expired certificates be allowed?</td>
<td>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 BIG-IP system. In the latter case, if you allow connections, consider adding any needed CA certificates to the BIG-IP system CA bundle (trust store). Select <strong>No, forbid connections to servers with expired certificates</strong> to prevent connections to servers that have expired certificates.</td>
</tr>
<tr>
<td>Should connections to servers with untrusted certificates be allowed?</td>
<td>Remote servers can present untrusted certificates. Allowing connections to servers with untrusted certificates can cause a security risk. Select <strong>Yes, allow connections to servers with untrusted certificates</strong> if appropriate for your situation and security policies.</td>
</tr>
<tr>
<td>Should strict updates be enforced for this application?</td>
<td>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 <strong>Yes</strong>) to avoid misconfigurations that can cause an unusable application.</td>
</tr>
</tbody>
</table>
Ingress device configuration

The ingress is one or more ingress VLANs where the 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. Once you’ve completed the **General Properties** configuration, continue to scroll down the page to **Ingress Device** configuration.

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

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which VLAN(s) will bring client traffic to the transparent proxy?</td>
<td>Select one or more VLANs where transparent-proxy ingress traffic will arrive.</td>
</tr>
<tr>
<td>How should a server TLS handshake failure be handled?</td>
<td>Most TLS handshake failures occur during protocol and cipher agreement. You can specify whether to drop or bypass the connection. Typically, select <strong>If server TLS handshake fails the connector fails.</strong></td>
</tr>
<tr>
<td>DNS query resolution</td>
<td>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</td>
</tr>
</tbody>
</table>
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.

---

<table>
<thead>
<tr>
<th>Ingress Device Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Which VLAN(s) will bring client traffic to the transparent proxy?</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Selected</strong></td>
<td><strong>Available</strong></td>
</tr>
<tr>
<td>Filter</td>
<td>/Common/Internal</td>
</tr>
</tbody>
</table>

| How should a server TLS handshake failure be handled? |  |
| **Selected** | **Available** |
| If server TLS handshake fails then connector fails |  |

| DNS query resolution |  |
| **Selected** | **Available** |
| Send DNS queries to forwarding nameservers on the local network |  |

| Which local forwarding nameserver(s) will resolve DNS queries from this solution? |  |
| **Selected** | **Available** |
| Nameserver IP address | 192.168.16.10 |

| Do you want to use DNSSEC to validate DNS information? |  |
| **Selected** | **Available** |
| Yes, use DNSSEC to validate DNS information |  |

---

Figure 14: Sample ingress device configuration

3. 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 device 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 egress device configuration question. Note that in the example below, the same F5 device is configured to receive both the ingress and egress traffic, but the egress is one or more egress VLANs where the clients receive traffic.

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you want to SNAT client IP addresses?</td>
<td>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</td>
</tr>
</tbody>
</table>
RECOMMENDED DEPLOYMENT PRACTICES
F5 and FireEye NX: SSL Visibility with Service Chaining

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 BIG-IP or Herculon 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.

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

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>What SSL Intercept logging level do you want to enable?</td>
<td>F5 recommends leaving the logging level at the default, Errors. Log on functional errors, unless you need to troubleshoot.</td>
</tr>
<tr>
<td>Which Log Publisher will process the log messages?</td>
<td>Specify whether to process the logs with an existing log publisher or that logs should be sent to syslog-ng.</td>
</tr>
<tr>
<td>What kind of statistics do you want to record?</td>
<td>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.</td>
</tr>
</tbody>
</table>
Create the 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 FireEye NX devices.

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.

<table>
<thead>
<tr>
<th>Configuration Field</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a Name for the inline service.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Select Layer 2 from the Service Type list.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Select the From BIG-IP and To BIG-IP system interfaces connected to the FireEye NX and their respective VLANs Tags. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>If you have multiple FireEye NX devices in the service pool, choose the F5 system interfaces connected to each FireEye NX and their VLANs' tags and click <strong>Add</strong> before moving to the next one.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> FireEye NX is a layer 7 device and can read and handle traffic with VLAN tags; however, it doesn't process these VLAN tags. 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.</td>
</tr>
<tr>
<td>Translate Port for HTTP Traffic</td>
<td>Select Yes to 8443 (or 80 or 8080). For the FireEye NX device to recognize that the steered traffic has been decrypted, it needs to be sent on a non 443 TCP port.</td>
</tr>
</tbody>
</table>
Connection Handling On Outage

<table>
<thead>
<tr>
<th>Connection Handling On Outage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select <strong>Skip Service</strong> to allow connections to skip the service you are configuring if all the devices in the service pool are unavailable.</td>
</tr>
<tr>
<td>Or select <strong>Reject Connection</strong> to reject every connection reaching the service when the service is down.</td>
</tr>
</tbody>
</table>

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

![Figure 17: Sample inline service configuration](image)

**Configuring the BIG-IP System with FireEye NX 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 the FireEye NX device(s) configured for TAP mode.
Create the receive-only service

When FireEye NX devices 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**.

<table>
<thead>
<tr>
<th>Configuration Field</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the inline service.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the receiving interface’s MAC Address. The MAC address can be obtained from the FireEye NX web UI, navigating to <strong>About &gt; Interfaces</strong>.</td>
</tr>
<tr>
<td>IP Address</td>
<td>In the IP Address field, 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 F5 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.</td>
</tr>
<tr>
<td>VLAN</td>
<td>From the VLAN list, select the VLAN where the receive-only device resides.</td>
</tr>
<tr>
<td>interface</td>
<td>Select the associated F5 system Interface.</td>
</tr>
</tbody>
</table>

2. When you’re done, click **Finished**, then click **Save** at the top of the page.
Alternative Architectures

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

Two F5 systems with FireEye NX deployed as a service pool

This solution is similar to the one explained in the section called, “Configuration for a Single F5 System with FireEye NX in Inline Mode.” The only difference is that a second F5 device (the egress device) is introduced to offload re-encryption from the ingress device.

Additional configuration steps

In this deployment scenario, you must configure SSL Orchestrator separately on the ingress and egress F5 devices 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 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.

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Service Name</td>
<td>Enter a name without spaces or dashes for the SSL Orchestrator application service.</td>
</tr>
<tr>
<td>Do you want to setup separate ingress and egress devices with a cleartext zone between them?</td>
<td>Select Yes, configure separate ingress and egress BIG-IP devices.</td>
</tr>
<tr>
<td>Is this device the ingress or egress device?</td>
<td>Select This is the INGRESS device to which clients connect.</td>
</tr>
<tr>
<td>What is the EGRESS device Application Service name?</td>
<td>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.</td>
</tr>
<tr>
<td>What is the IP address of the EGRESS device control-channel virtual server?</td>
<td>Enter the IP address of the control channel virtual server over on the egress device.</td>
</tr>
<tr>
<td>What IP address should THIS (ingress) device’s control-channel virtual server use?</td>
<td>Enter the IP address of the virtual server for the control channel.</td>
</tr>
<tr>
<td>What is the control-channel pre-shared key?</td>
<td>Enter a pre-shared key (PSK) value to enable cryptographic protection of the service chain control channel between the ingress and egress F5 devices.</td>
</tr>
</tbody>
</table>

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.
RECOMMENDED DEPLOYMENT PRACTICES
F5 and FireEye NX: SSL Visibility with Service Chaining

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there parallel service devices in the decrypt zone?</td>
<td>Select No, send outbound traffic via the BIG-IP default route(s). Or select Yes when FireEye NX devices will be sandwiched in the cleartext zone between the ingress and egress devices.</td>
</tr>
</tbody>
</table>

Figure 22: Sample configuration for the decrypt zone to egress device

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 after a connection travels through the specified service chain and then directs that traffic to its final destination. When separate ingress and egress devices are set up, they send each other control messages. These 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 that the user specifies, on each F5 system.

1. On the main tab, click **SSL Orchestrator > Configuration > General Properties**.
2. Enter information for the additional configurable fields, following the guidance below.

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Service Name</td>
<td>Enter a name without spaces or dashes for the SSL Orchestrator application service.</td>
</tr>
<tr>
<td>Do you want to setup separate ingress and egress devices with a cleartext zone between them?</td>
<td>Select Yes, configure separate ingress and egress BIG-IP devices</td>
</tr>
<tr>
<td>Is this device the ingress or egress device?</td>
<td>Select This is the EGRESS device which connects to a server.</td>
</tr>
<tr>
<td>What is the INGRESS device Application Service name?</td>
<td>Enter the name for the SSL Orchestrator application service configured on the ingress device.</td>
</tr>
<tr>
<td>What is the IP address of the INGRESS device control-channel virtual server?</td>
<td>Enter the IP address of the control channel virtual server on the ingress device.</td>
</tr>
<tr>
<td>What IP address should THIS (egress) device’s control-channel virtual server use?</td>
<td>Enter the IP address of the virtual server for the control channel.</td>
</tr>
<tr>
<td>What is the control-channel pre-shared key?</td>
<td>Enter a pre-shared key (PSK) value to enable cryptographic protection of the service chain control channel between the ingress and egress devices.</td>
</tr>
</tbody>
</table>

3. Continue configuration with the additional configuration 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.

4. Continue to scroll down the page and answer the remaining configuration question, following the guidance below.

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there parallel service devices in the decrypt zone?</td>
<td>Select No, send outbound traffic via the BIG-IP default route(s).</td>
</tr>
</tbody>
</table>

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

### Two F5 systems with FireEye NX devices sandwiched in the decryption zone

In this case, the FireEye NX devices 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.

![Diagram of two F5 systems with FireEye NX devices](image)

*Figure 23: The SSL visibility solution with two F5 systems with a FireEye NX pool in decrypt zone*

**Additional configuration steps**

This scenario requires, as a prerequisite, that you have already created a pair of VLANs—one on the ingress F5
device and another on the egress for each FireEye NX device(s) in the sandwiched pool.

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

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.

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there parallel service devices in the decrypt zone?</td>
<td>Select Yes, send outbound traffic via one or more service device(s).</td>
</tr>
<tr>
<td>What are the IPv4 decrypt zone gateway addresses?</td>
<td>Enter the IP address of the outward interface of the last layer 3 device in the decrypt zone. The gateway IP address is the address on a VLAN on the next hop egress F5 device.</td>
</tr>
</tbody>
</table>

| Decrypt Zone to Egress Device Configuration | | | |
|--------------------------------------------|---|---|
| Are there parallel service devices in the decrypt zone? | Yes, send outbound traffic via one or more service device(s): | ✓ |
| What are the IPv4 decrypt zone gateway addresses? | Ratio | IPv4 gateway address |
| | 1 | 192.168.30.1 |
| | 1 | 192.168.30.1 |

Figure 24: Sample configuration for the decrypt zone to egress device

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

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

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.

<table>
<thead>
<tr>
<th>Question</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there parallel service devices in the decrypt zone?</td>
<td>Select Yes, send outbound traffic via one or more service device(s).</td>
</tr>
<tr>
<td>What are the IPv4 decrypt zone gateway addresses?</td>
<td>Enter the IP address of the outward interface of the last layer 3 device in the decrypt zone. The gateway IP address is the address on a VLAN on the next hop ingress F5 device.</td>
</tr>
<tr>
<td>What are the intranet networks (subnets)?</td>
<td>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.</td>
</tr>
</tbody>
</table>
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. Service chains can include each of the three types of services (inline, ICAP, or receive-only), as well as any decryption zones between separate ingress and egress devices.

1. To create a service chain, from the main tab, navigate to 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**. Repeat until all services in the chain have been selected in the order you prefer.

5. When you’re done with one service chain, click **Finished**.

6. Repeat Steps 2 through 5 to create multiple service chains.

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. In the following example, we create 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.

<table>
<thead>
<tr>
<th>Configuration Field</th>
<th>User Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the TCP service classifier rule.</td>
</tr>
<tr>
<td>Phase</td>
<td>Select the SSL/TLS phase you want:</td>
</tr>
<tr>
<td>No TLS</td>
<td>Match only non-TLS/SSL traffic.</td>
</tr>
<tr>
<td>Pre-Handshake</td>
<td>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.</td>
</tr>
<tr>
<td>TLS Handshake</td>
<td>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.</td>
</tr>
<tr>
<td>Normal</td>
<td>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</td>
</tr>
</tbody>
</table>
### Protocol

Select the protocol to match: **HTTP, MAIL, ALL, or Other.**

For the sample, 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.

For the example, select the source **Type** as **IP address** 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.

For the example, select URLF as the destination **Mode**, **Type** for the **category**, 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
RECOMMENDED DEPLOYMENT PRACTICES
F5 and FireEye NX: SSL Visibility with Service Chaining

<table>
<thead>
<tr>
<th>Service Chain</th>
<th>click Add.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the name of a Service Chain (defined in the previous procedure) or an action—either Bypass or Reject. For the example, select Bypass in the Service Chain selector to enforce the bypass action when both source and destination context filters match for an outbound connection.</td>
<td></td>
</tr>
</tbody>
</table>

3. When your classifier rule configuration is complete, click Finished.

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

5. 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.

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

Testing the Solution

You can test the deployed solution using any one of the following three 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 system.
  ```
tcpdump -lnni eth<n> -Xs0
  ```
**FireEye deployment test**

Using the FireEye web interface, log in to the FireEye NX GUI and click **About**, and then click **Deployment check** and perform the checks there. Note that this test will redirect the client to FireEye hosted sites to download benign traffic that will generate an alert, but it does require that traffic to pass through the appliance. (The appliance must be in the path of traffic from the Internet to the client). Additionally, some of these checks may cause a security alert, so it is important to coordinate these tests with your security team for this testing in the production network.