RECOMMENDED PRACTICES GUIDE

F5 SSL Orchestrator and McAfee Web Gateway:

SSL Visibility for Advanced Threat Analysis and Prevention

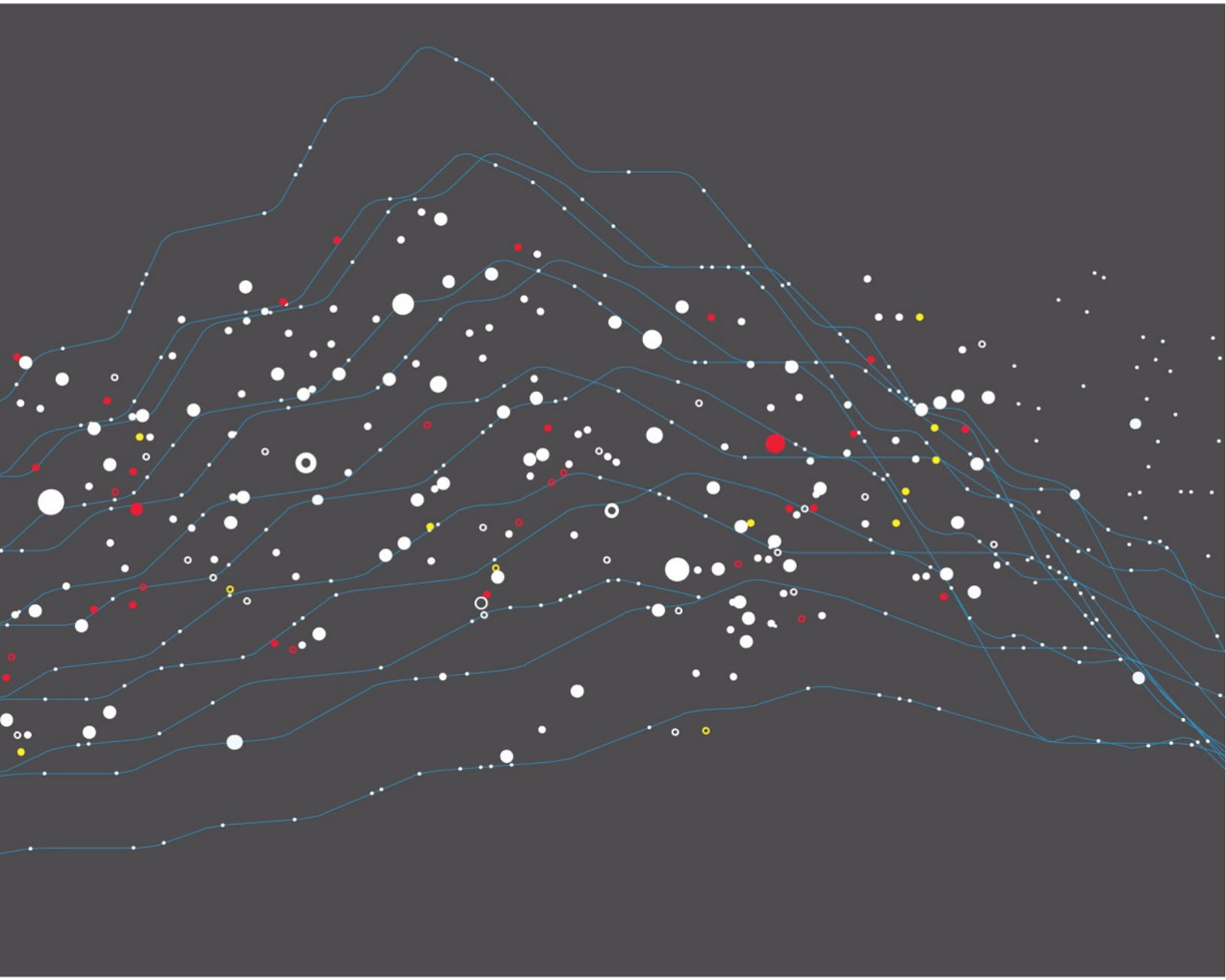


Table of Contents

Introduction

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

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

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

F5 SSL Orchestrator with its ability to address HTTP proxy devices inside its decrypted inspection zone allows the MWG to provide optimal security functionality while offloading SSL and complex orchestration to the F5 system.

This guide provides an overview of the F5-McAfee joint solution and describes different deployment modes with reference to service chain architectures and recommended practices.

The Integrated F5-McAfee Solution

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

F5 SSL Orchestrator provides:

- **Multi-layered security**

  To solve specific security challenges, security administrators are accustomed to manually chaining together multiple point products, creating a bare bone "security stack" consisting of multiple services. A typical stack may include components like Data Leak Prevention (DLP) scanners, Web Application Firewalls (WAF), Intrusion Prevention and Detection Systems (IPS and IDS), Malware Analysis tools, and more. In this model, all user sessions are provided the same level of security, as this "daisy chain" of services is hard-wired.

- **Dynamic service chaining**

  Dynamic service chaining effectively breaks the daisy chain paradigm by processing specific connections based on context provided by the Security Policy, which then allows specific types of traffic to flow through arbitrary chains of services. These service chains can include five types of services: layer 2 inline services, layer 3 inline services, receive-only services, ICAP services, and HTTP web proxy services.

  A Service in SSL Orchestrator

  A service in SSL Orchestrator system is defined as a pool of one or more same security devices. For example, a McAfee DLP ICAP service would include one or more McAfee DLP systems. SSL Orchestrator will automatically load balance the traffic to all the systems in a service.

  Health Monitoring

  F5 SSL Orchestrator provides various health monitors to check the health of the security devices in a service and handles failures instantly. For example, in a McAfee DLP ICAP service, should a system fail, the F5 SSL Orchestrator will shift the load to the active McAfee DLP systems. Should all the systems in the service fail, SSL Orchestrator will bypass the McAfee DLP ICAP service to maintain network continuity and maximize uptime.

- **Topologies**

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

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

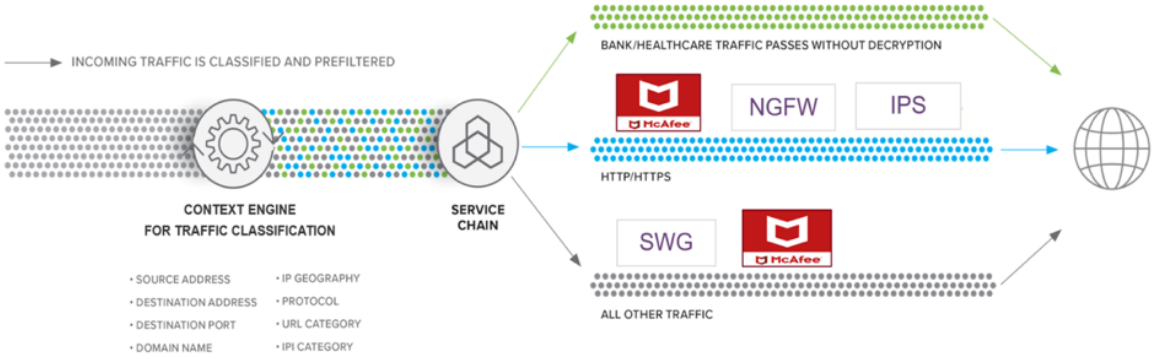
- **Security Policy**

  The SSL Orchestrator Security Policy provides a rich set of context-aware methods to dynamically determine how best to optimize traffic flow through the security stack. Context can minimally come from the following:

  - Source and destination address/subnet
  - URL filtering and IP intelligence - Subscriptions
  - Host and domain name
  - Destination port
  - IP geolocation
  - Protocol

- **Context Engine for Traffic Classification**

  SSL Orchestrator's context engine provides the ability to intelligently steer traffic based on policy decisions made using classification criteria, URL category, IP reputation, and flow information. In addition to directing the traffic to service chains, customers can also use the context engine to bypass decryption to applications and websites like financials, government services, health care, and any others, for legal or privacy purposes.



McAfee Web gateway Appliance provides:

- **Advanced Anti-Malware Protection**

  McAfee's anti-malware protection can identify known malicious files as well as analyze unknown files for hidden threats. Proactive intent analysis filters out previously unknown, or zero-day malicious content from web traffic in real time.

- **Intelligent Sharing**

  McAfee Web Gateway creates and shares new file reputations for zero-day malware discovered by the Gateway.

- **Application Visibility and Granular Application Control**

  Application visibility grants full control over web applications such as those included in the Office365 suite, GSuite, Facebook, Webmail, Dropbox, etc.

- **Granular Policy Options**

  McAfee's policy options can block individual web objects and file types based on any arbitrary Boolean combination of well over 200 transaction properties including Geolocation, Category, Reputation, User, User Groups, and true file type.

- **Automated Traffic Analysis**

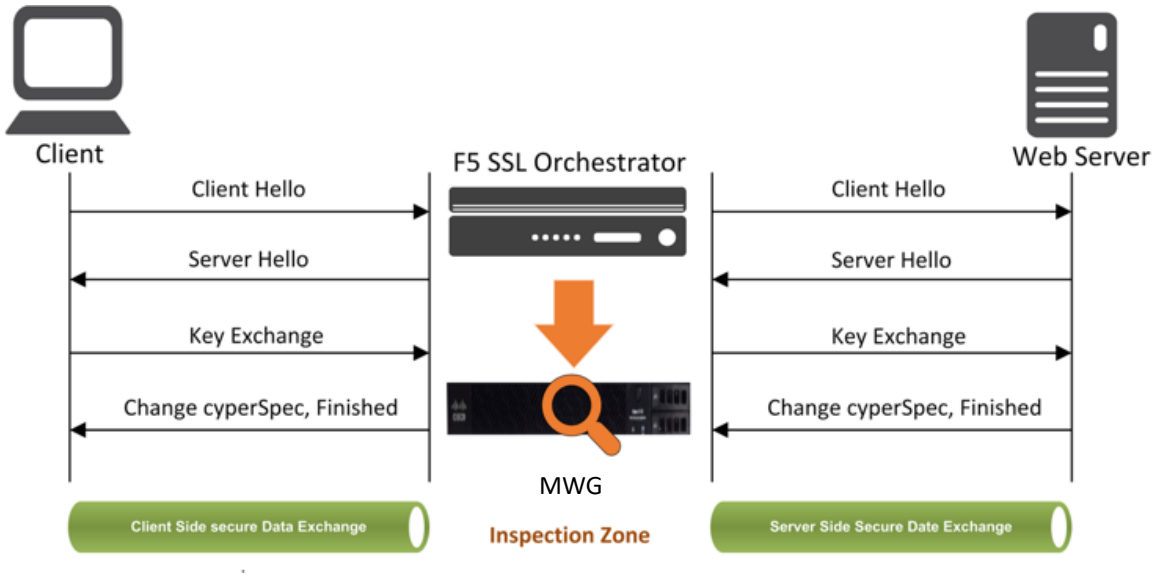
  Automated analysis scans all web traffic in real time for both known and new malware, using dynamic reputation and behavior-based analysis on all web content. MWG also has the capability to quickly be adapted to new application features and associated security challenges like domain fronting, and tenant restrictions.

- **Advanced Threat Analysis Integration**

  McAfee Web Gateway integrates with McAfee Advanced Threat Defense, an advanced malware detection technology that combines customizable sandboxing with in-depth static code analysis.

SSL visibility: How do we do it?

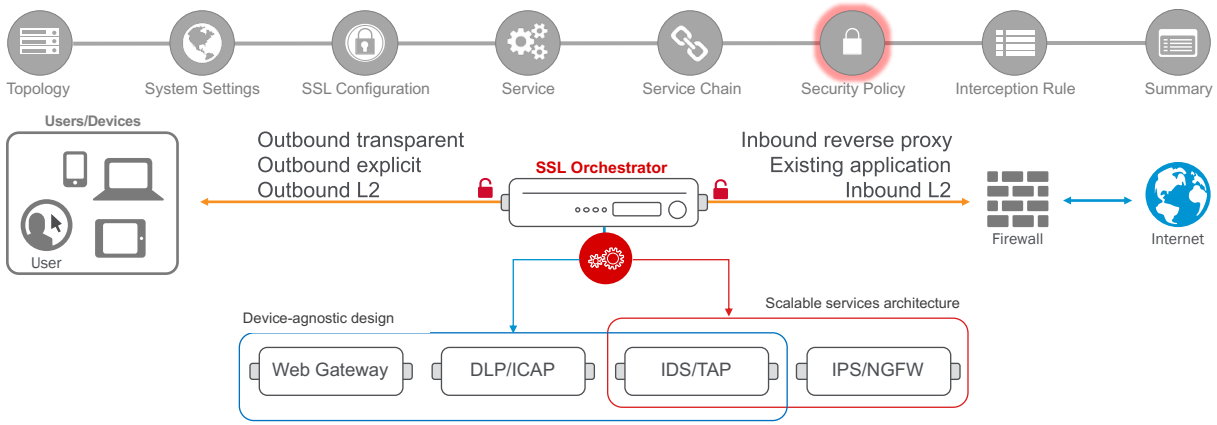
F5's industry-leading full-proxy architecture enables F5 SSL Orchestrator to install a decryption/clear-text zone between the client and web server, creating an aggregation (and, conversely, disaggregation) visibility point for security services. The F5 BIG-IP system establishes two independent SSL connections - one with the client and the other with the server. When a client initiates a TLS connection to the server, the F5 BIG-IP system intercepts and decrypts the client encrypted traffic and steers it to a pool of security devices for inspection before re-encrypting the same traffic to the server. The returned response from the server to the client is likewise intercepted and decrypted for inspection before being sent on to the client.



SSL orchestration using security service chains

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 the figure above, SSL Orchestrator can load balance, monitor, and dynamically chain security services, including next-gen firewalls, DLP, IDS/IPS, web application firewalls, and antivirus/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.



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 the MWG security system.

Sizing

The main advantage of deploying 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 SSL Orchestrator for inspection by MWG, and “uninteresting” traffic, which is allowed to pass through or be processed differently according to other corporate policy requirements. This selective steering of only the interesting traffic to the firewall system conserves its valuable resources (as it need not inspect the entire wire traffic), maximizing performance.

As a result, it is important to consider the entire wire traffic volume to calculate the appropriate F5 BIG-IP device size. The MWG system will require two interfaces on the F5 BIG-IP systems (or one 802.1Q VLAN tagged interface) to allow traffic flow through logical inbound and outbound service interfaces.

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

- Port density
- SSL bulk encryption throughput
- System resources
- The number of security services and devices in service chain

Note: The F5 SSL Orchestrator has no specific port density requirement. Layer 3 must be layer 3 adjacent (routable), and layer 2 devices must be layer 2 adjacent (switched), and the F5 BIG-IP supports 802.1Q VLAN tagging so a single interface can be logically divided into multiple VLANs. Security devices can connect to the F5 BIG-IP across a switched or routed architecture, so port density in this case is expandable. The only significant requirement is that inline security devices (layer 2, layer 3, and HTTP devices) must have separate physical or logical inbound and outbound interfaces.

License components

The F5 SSL Orchestrator solution supports two licensing modes: standalone and LTM add-on:

Standalone software license mode

This option supports the following platforms:

- i2800
- i5800
- i10800
- i11800
- i15800
- VE High Performance (HP – 8vCPU)
- VE High Performance (HP – 16vCPU)

This option is suited for environments that need standalone security solutions and have no need to integrate with other F5 software functions. Standalone mode restricts the F5 BIG-IP platform to the following additional software modules:

- **F5® Access Manager™** (formerly known as **F5® BIG-IP® APM**) to authenticate and manage user access
- **F5® Secure Web Gateway** (**SWG**) Services to filter and control outbound web traffic using a URL database (OR) **F5 URL filtering** (**URLF**) subscription to access the URL category database
- An **F5® IP Intelligence** (**IPI**) subscription for IP reputation service

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

LTM add-on software license mode

This option supports all F5 BIG-IP platforms and has no specific restrictions on additional F5 software modules (including the above software services). This option is suited for environments that need to deploy SSL Orchestrator on an existing F5 BIG-IP device or have other functions that must run on the same device.

Optional licensing options

In addition to the above licensing modes, the following may also be licensed:

- **A URL Filtering (URLF) subscription** to use the URL category database for filtering.
- **An F5 IP Intelligence (IPI) subscription** to detect and block known attackers and malicious traffic.
- A network **Hardware Security Module (HSM)** to safeguard and manage digital keys for strong authentication.

Traffic exemptions for SSL inspection

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

- Guest VLANs
- Applications that use pinned certificates
- Trusted software update sources
- Trusted backup solutions
- Any lateral encrypted traffic to internal services to be exempted

You can also exempt traffic based on domain names and URL categories. The policy rules of the F5 BIG-IP SSL Orchestrator system 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, including (but not limited to):

- Financial
- Health care
- Government services

Certificate requirements

Depending on the direction of flow, there are different certificate requirements.

Outbound traffic flow (internal client to Internet)

An SSL certificate and associated private key - preferably a subordinate certificate authority (CA) - on the F5 BIG-IP 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 do not encounter certificate errors when accessing SSL-enabled websites from their browsers, this issuing certificate must be locally trusted in the client environment.

Inbound traffic flow (Internet client to internal applications)

Inbound SSL orchestration is similar to traditional reverse web proxy SSL 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 wildcard or subject alternative name (SAN) certificate if inbound SSL Orchestrator is defined as a gateway service.

Architecture recommended practices

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

- Deploy inline. Any SSL visibility solution must be in-line to the traffic flow to decrypt perfect forward secrecy (PFS) cipher suites such as ECDHE (elliptic curve Diffie-Hellman encryption).

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

- Every McAfee Web Gateway in the service pool must be dual homed on the “to-service” (F5 BIG-IP to MWG) and “from-service” (MWG back to F5 BIG-IP) VLANs with each F5 BIG-IP system in the device sync/failover device group. This can be physically separate interfaces or a single 802.1Q tagged VLAN for logical separation.

- 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 BIG-IP systems do not need physical connections to the MWG. The F5 BIG-IP system requires only layer 3 reachability to the MWG. In slow networks, however, we recommend deploying the services not more than one hop away.

Security recommended practices

SSL orchestration generally presents a new paradigm in the typical network architecture. Before, client-server traffic passed encrypted to inline security services, which then had to perform their own decryption if they needed to inspect that traffic. Integrated with SSL Orchestrator, now ALL traffic to a security device is decrypted – including usernames, passwords, social security and credit card numbers, etc. It is therefore highly recommended that security services be isolated within a private, protected enclave defined by the SSL Orchestrator. It is technically possible, however, to configure the SSL Orchestrator to send the decrypted traffic anywhere that it can route to, but this is a dangerous practice that should be avoided.

IP addressing

The recommended approach to integrating security devices is to physically move them to an isolated enclave of the SSL Orchestrator. This generally requires re-addressing inline layer 3 security services. The following assumes this approach is being taken, and the example IP addresses represent a local/internal addressing scheme. As previously stated, it is entirely possible to configure the SSL Orchestrator to send decrypted traffic anywhere that it can route to, but this is a dangerous practice.

F5 and McAfee Web Gateway Appliance (MWG)

When the McAfee Web Gateway is deployed as either a transparent proxy or explicit proxy, F5 recommends configuring its IP addresses for connected to-service and from-service interfaces from private addressing subnets provided by SSL Orchestrator. The default subnets are derived from an RFC2544 CIDR block of 198.19.0.0, which improves security and minimizes the likelihood of address collisions.

For example, you can configure an MWG to use the IP address 198.19.96.10/25 on its to-service interface and 198.19.96.130/25 on its from-service interface. The table below explains the IP addresses that you need to configure when deploying multiple MWGs in a service pool.

Device	To-Service IP	From-Service IP	Gateway
MWG 1	198.19.96.10/25	198.19.96.130/25	198.19.96.245
MWG 2	198.19.96.11/25	198.19.96.131/25	
MWG n	198.19.96.x/25	198.19.96.x/25	

The MWG would then default route back to SSL Orchestrator on a defined address in the from-service subnet. In the example above, that IP address is 198.19.96.245.

Note: A /25 network (255.255.255.128) subdivides a regular /24 network into two subnets and is a simple way to maximize local protected IP addressing for security services. These are the IP subnets and schemes that the SSL Orchestrator uses by default, but any addressing scheme can be used.

198.19.96.1 - 198.19.96.126
198.19.96.129 - 198.19.96.254

Additionally, while it can, SSL Orchestrator does not by default source NAT (SNAT) the client source address across inline layer 3 services. Plus, it is usually favorable for inline security devices to see the true client IP address. Inline layer 3 services may therefore also need a static route back to the to-service side of the SSL Orchestrator for IPs/subnets that match the client-side network. For example,

Client-side network: *10.20.0.0/24*
SSL Orchestrator service to-service self: *198.19.96.7/25*
SSL Orchestrator service from-service self: *198.19.96.245/25*

In this example, the client would be coming from the 10.20.0.0/24 subnet, an IP subnet foreign to the MWG. It may be necessary to create a static route that directs MWG to forward any return traffic destined to this subnet back to the SSL Orchestrator to-service self IP address (ex. 198.19.96.7).

Initial setup

Initial setup includes configuration of McAfee Web Gateway and setup of SSL Orchestrator. Once these steps are complete, you can proceed to configuration for the specific deployment scenario you choose.

Configure McAfee Web Gateway prerequisites

Before the MWG can receive traffic from the SSL Orchestrator, there are a few basic configurations that must be completed. Any and all licenses should be applied, and basic system setup should be completed. Along with many other settings, the system setup will include configuration of the hostname and Domain Name Servers (DNS). The system hostname will be configured as well as the IP address, subnet mask, and hostname for the management interface. Additional interfaces will be configured further on in this guide.

Configure SSL Orchestrator prerequisites

Before you begin configuring the SSL Orchestrator, there are a few prerequisite operations that need to be addressed.

Define client side and outbound (e.g. Internet) side VLANs and self-IPs

For SSL Orchestrator in a layer 3 (routed or explicit proxy) topology, the F5 BIG-IP system must be configured with appropriate client-facing and outbound-facing VLANs and self-IPs. The VLANs define the connected interfaces, and the self-IPs define the respective IPv4 and/or IPv6 subnets. In the F5 BIG-IP system UI, under the Network menu, configure the client side and outbound side VLANs and self-IPs appropriately.

Import CA certificate and private key

For SSL Orchestrator in an outbound traffic topology, a local CA certificate and private key are required to resign the remote server certificates for local (internal) clients. In the F5 BIG-IP system UI, under System –> Certificate Management, import the required Certificate Authority certificate and private key. Ensure that internal clients trust this local certificate authority.

Update the SSL Orchestrator Application

Periodic updates are available for SSL Orchestrator. (If you are upgrading from a previous major version, refer to the SSL Orchestrator setup guide for the recovery procedure.)

To download the latest update:

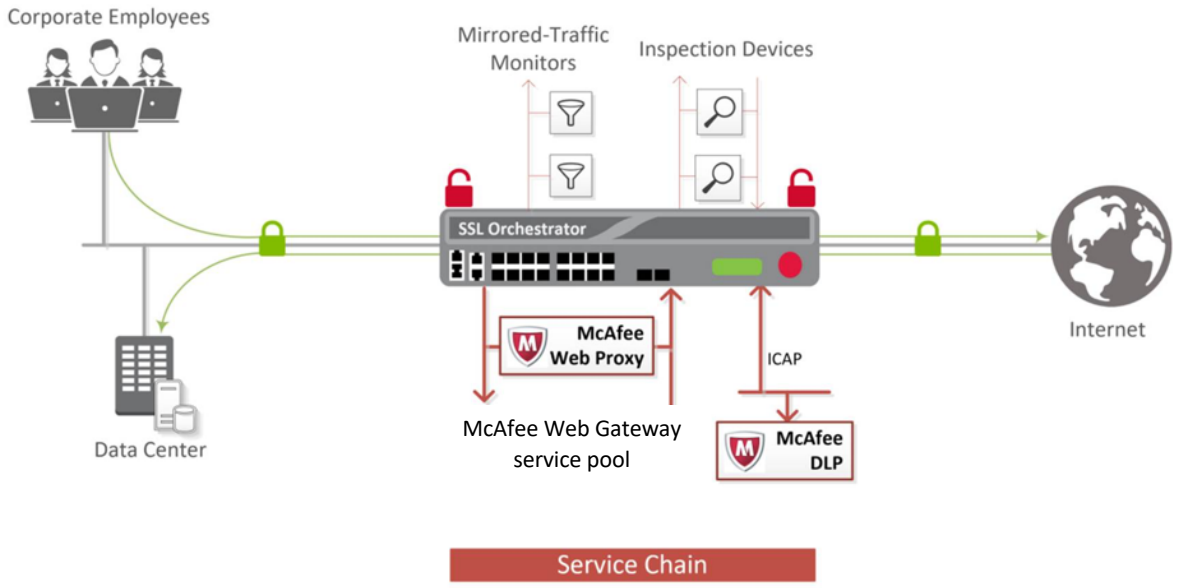
1. Visit downloads.f5.com. You will need your registered F5 credentials to log in.
2. Click **Find a Download**.
3. Scroll to the **Security** product family, select **SSL Orchestrator**, and click the link.

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

Configuring SSL Orchestrator integration with the McAfee Web Gateway appliance

The SSL Orchestrator is configured to send decrypted traffic to an inline MWG. SSL Orchestrator handles both decryption and re-encryption of HTTPS traffic, with an inspection zone installed between the ingress and egress. Decrypted traffic is steered to a service pool of MWG devices. You can also deploy the F5 BIG-IP system as a device sync/failover device group (including an HA pair) with a floating IP address for high availability.

The MWG can be configured as either a transparent proxy or explicit proxy inside the inspection zone.



How traffic flows in this deployment:

- Client traffic arriving at the ingress side of the F5 BIG-IP system is classified, and interesting HTTPS traffic is decrypted as part of the SSL handling process.

- SSL Orchestrator steers the decrypted traffic through the load balanced MWG service pool as part of a service chain of potentially multiple types of security services.

- The HTTP traffic is inspected by the MWG services for any hidden threats before sending that traffic back to the F5 BIG-IP system.

- The F5 BIG-P system orchestrates the decrypted traffic through other services in the chain before it aggregates and re-encrypts the traffic, which is then routed to the next destination.

Note: Inside the SSL Orchestrator inspection zone, all traffic passing to the McAfee Web Gateway is unencrypted HTTP. It is a security recommended practice to protect this device and the network between it and the SSL Orchestrator device. It is therefore recommended that the MWG devices be moved to the secure enclave created by SSL Orchestrator. This brings with it a few architectural changes.

If the MWG was previously installed in the network to service client traffic, as either a transparent or explicit proxy, the SSL Orchestrator must now fulfill that role. If the MWG was configured as an explicit proxy, SSL Orchestrator must then be configured as an explicit proxy and clients must communicate with SSL Orchestrator as their explicit proxy gateway. If the MWG was configured as a transparent proxy, the SSL Orchestrator must then be configured as a transparent proxy and routed client traffic must now pass through it. The MWG devices inside the inspection zone can be explicit or transparent, irrespective of the SSL Orchestrator proxy mode.

If the MWG device was previously handling explicit proxy user authentication, the SSL Orchestrator must now fulfill this role. The F5 Access Policy Manager (APM) module can be provisioned to provide the required explicit forward proxy authentication functionality.

Configure McAfee Web Gateway

The following are the minimum requirements to configure a MWG device for integration with SSL Orchestrator. Please refer to McAfee documentation for additional product-specific information.

Configure interfaces

The MWG devices must be physically or logically two-armed. In other words, it must have separate physical or logical to-service and from-service interfaces. This can either be two separate physical interfaces, or a single 802.1Q VLAN tagged interface (a single interface with two tagged VLANs).

To complete the interface configuration in the MWG GUI, navigate to **Appliances -> (this appliance) -> Network Interfaces**. Relevant settings are described below:

- Hostname – enter a unique hostname for this MWG appliance.

- Default Gateway (IPv4) – traffic will route from the MWG appliance back to SSL Orchestrator. The IP address used here will be the “from-service” F5 BIG-IP self-IP (ex. 198.19.96.245).

Under the “Enable these network interfaces” section:

- Enable the MWG “to-service” interface. This is the interface that receive decrypted HTTP traffic from the SSL Orchestrator. Configure its IPv4 settings manually and supply an IP address in the pre-defined subnet (ex. 198.19.96.10). Enter the appropriate subnet mask (ex. 255.255.255.128).

- Enable the MWG "from-service" interface. This is the interface that sends decrypted HTTP traffic from MWG back to the SSL Orchestrator. Configure its IPv4 settings manually and supply an IP address in the pre-defined subnet (ex. 198.19.96.131). Enter the appropriate subnet mask (ex. 255.255.255.128).

Note that SSL Orchestrator supports handling of both IPv4 and IPv6 traffic flows. To allow IPv6 traffic to flow through the MWG, add IPv6 addresses in the MWG configuration, then create an IPv6 version of the MWG service in SSL Orchestrator.

Optionally configure 802.1Q VLANs

If two separate data plane interfaces are not available, it is also possible to configure a single interface with two 802.1Q tagged VLANs.

From the MWG UI, under **Appliances -> (this appliance) -> Network Interfaces**, select and enable the raw interface to use.

- Configure the IPv4 and IPv6 settings for this interface as Disabled.
- Click the "Add VLAN…" button and supply a unique VLAN ID in the dialog box.
- Click the "Add VLAN…" button again and supply a unique VLAN ID in the dialog box.
- Click to enable the first VLAN and configure its IPv4 settings manually. Supply an IP address in the pre-defined subnet (ex. 198.19.96.10). Enter the appropriate subnet mask (ex. 255.255.255.128).
- Click to enable the second VLAN and configure its IPv4 settings manually. Supply an IP address in the pre-defined subnet (ex. 198.19.96.131). Enter the appropriate subnet mask (ex. 255.255.255.128).

Configure routes

The MWG devices will require two routes:

1. A gateway route to send user traffic outbound – Traffic will route from the MWG appliance back to SSL Orchestrator. The IP address used here will be the "from-service" F5 BIG-IP self-IP (ex. 198.19.96.245). This is defined in the MWG UI under **Appliances -> (this appliance) -> Network Interfaces**, in the "Default gateway (IPv4)" setting.

2. A static return route – SSL Orchestrator does not source NAT (SNAT) traffic across inline security devices by default, so the source address passing through the MWG will be foreign and will need a static return route to define the path back to the F5 BIG-IP system on the inbound side of the MWG. Looking at the following example,

Client-side network:	*10.20.0.0/24*
SSL Orchestrator service to-service self:	*198.19.96.7/25*
SSL Orchestrator service from-service self:	*198.19.96.245/25*

In this example, the client would be coming from the 10.20.0.0/24 subnet, an IP subnet foreign to the MWG. It is, therefore, necessary to create a static route that directs MWG to forward any return traffic destined to the subnet back to the SSL Orchestrator service inbound self IP address (ex. 198.19.96.7). This is defined in the MWG UI under **Appliances -> (this appliance) -> Static Routes**.

Configure DNS

DNS settings are minimally required to allow the MWG devices to talk to remote services, including DNS, license and engine updates. There are generally two options for DNS. It can either pass through the management interface or the data plane outbound interface. DNS is configured in the MWG UI under **Appliances -> (this appliance) -> Domain Name Services**.

Configure the web proxy service

The services attached to SSL Orchestrator are opaque to the external environment. They are protected, isolated, and do not interact outside of the internal connectivity with the F5 BIG-IP. Most important, services (devices connected to the F5 BIG-IP) and topologies (how SSL Orchestrator consumes network traffic) are independent of one another. For example, McAfee Web Gateway can be deployed as an explicit or transparent proxy inside the SSL Orchestrator inspection zone, while the deployed topology can be explicit forward proxy, transparent forward proxy, or even in a layer 2 bump-in-the-wire mode. With this in mind, the simplest, most efficient, and most flexible configuration option for the MWG in the SSL Orchestrator inspection zone is as an explicit proxy, irrespective of the SSL Orchestrator topologies defined.

The following settings will detail how to configure MWG as an explicit proxy. Please refer to the appropriate MWG documentation for more detailed information on configuring MWG. In the MWG UI under **Appliances -> (this appliance) -> Proxies (HTTP(S), FTP, SOCKS, ICAP…)**:

Web Proxy Service	User Input
Network Setup	Select Proxy (Optional WCCP).
Advanced Outgoing Connection Settings	Check the IP spoofing options. This will enable MWG to egress with the client's IP address.
Outbound Source IP List	Enter an IP address here in the same subnet as MWG's outbound interface (ex. 198.19.96.132). The source NAT policy will change data plane (client) traffic to this source address as it leaves the MWG.
HTTP Proxy	Click the plus sign to create a new HTTP proxy. Assign an appropriate listener IP address and port. This is the IP address and port that SSL Orchestrator will target. It is appropriate here to use a wildcard IP address (0.0.0.0), and the standard MWG explicit proxy port (9090). Click the OK button to save.

Click Save Changes in top right of the MWG UI to commit the changes.

To source NAT or not to source NAT

SSL Orchestrator is able to dynamically service chain traffic flows by a unique process of active "signaling". As a packet leaves the F5 BIG-IP for a security device, a marker is created so that when the traffic returns, the marker restores context and continues moving the packets through the security stack. If a security device attempts its own external connection, that device-initiated traffic would not be signaled, thus SSL Orchestrator's device isolation posture would prevent it from traversing the inspection zone. Should a security device require its own external connectivity then, it would be necessary to create a separate "control" channel on the F5 BIG-IP. This control channel is described more completely in the SSL Orchestrator configuration section below but is essentially a virtual server attached to the security device's from-service VLAN, listening on the device's outbound source IP address. Thus, to differentiate between decrypted client-server traffic that must continue through the service chain, and device-initiated traffic that must egress directly, minimally the source IP addresses must be different. McAfee Web Gateway supports a feature called "IP spoofing", that when enabled retains the client's IP address on egress. It is therefore highly recommended to enable IP spoofing so that only device-initiated traffic will source from the MWG's outbound IP address and be captured by the separate control channel virtual server, while normal client-server traffic sources from the client's IP address and flows through the service chain. It also benefits upstream security devices (devices later in the service chain) if they're able to see the client's real IP address.

If IP spoofing is disabled, all traffic egresses MWG on the device's outbound interface IP address, which would then require a separate source NAT policy to translate client-server traffic to an alternate source IP to create the separate traffic patterns. As this is not recommended, instructions for creating this source NAT policy are not included here.

- In McAfee Web Gateway **prior to 8.2**, IP spoofing functions natively by simply enabling the IP spoofing options in the "Proxies (HTTP(S), FTP, SOCKS, ICAP…)" section, under "Advanced Outgoing Connection Settings". You can then skip the following steps and move directly to SSL Orchestrator configuration.

- In McAfee Web Gateway versions **8.2 and later**, IP spoofing must be enabled, but also requires a source NAT policy. The following steps detail that process.

Configure a source NAT policy

If running a version of McAfee Web Gateway **prior to 8.2**, IP spoofing (egressing with the client's real IP address) requires both the IP Spoofing settings enabled, and a separate source NAT policy.

To create the source NAT policy, under the **Policy** section in the MWG UI, navigate to Common Rules and click the **Add Rule…** button.

Source NAT Policy	User Input
Name	Provide a unique name for this policy.
Rule Criteria	Select to apply this rule Always.

Action	Select Continue.
Events	Click the **Add** button, and then **Event…** and create the following rule: `Enable Outbound Source IP Override (Client.IP)` • **Add** -> **Event…** • Select **Enable Outbound Source IP Override (IP)** • Click the **Parameters…** button • Click the **Parameter Property** button • Select **Client.IP** and click the **OK** button. • Click the **OK** button, then again to complete the rule. Click **Finished** to complete the source NAT rule.

The McAfee Web Gateway appliance should now be ready to receive decrypted HTTP traffic on its explicit proxy listener IP address and port. Data plane (client) traffic will egress MWG with the client's true self IP address, and any MWG-initiated traffic will egress on the appliance's from-service interface IP address. It is now time to configure the SSL Orchestrator to integrate this MWG service.

Configure SSL Orchestrator

A McAfee Web Gateway is configured as an HTTP service in SSL Orchestrator. This configuration will focus on the traditional outbound (forward proxy) use case. Once logged into the F5 BIG-IP system, navigate to the SSL Orchestrator menu and review the environment.

Create the SSL Orchestrator deployment through Guided Configuration

The SSL Orchestrator Guided Configuration presents an entirely new and streamlined user experience. This workflow-based architecture provides intuitive, re-entrant configuration steps tailored to the selected topology.

The following steps will walk through the Guided Configuration (GC) to build a simple transparent forward proxy.

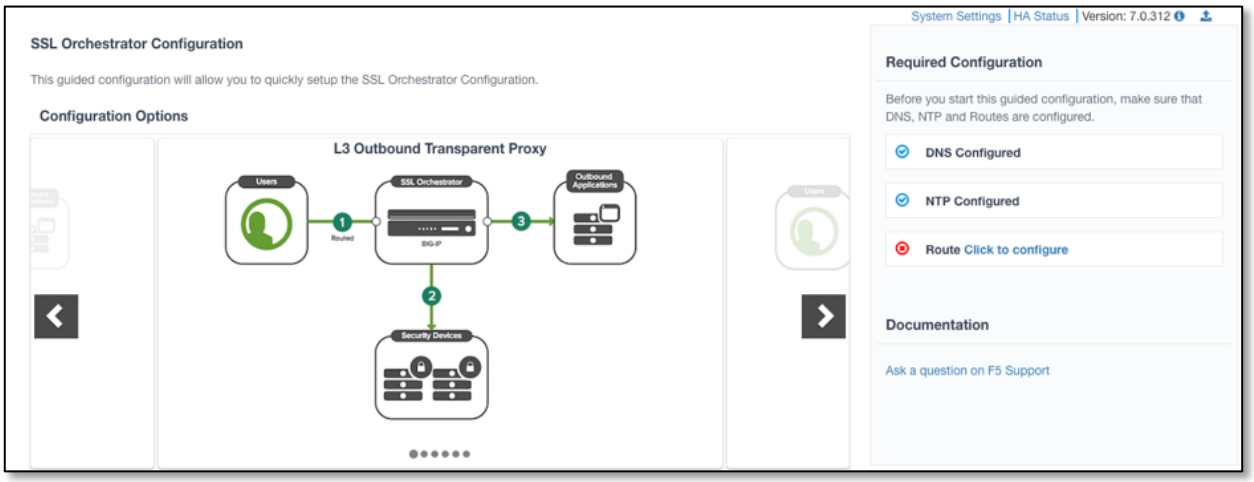
Initialization

If this is the first-time accessing SSL Orchestrator in a new F5 BIG-IP build, upon first access, the Guided Configuration (GC) will automatically load and deploy the built-in SSL Orchestrator package.

Configuration review and prerequisites

Take a moment to review the topology options and workflow configuration steps involved. Optionally satisfy any of the DNS, NTP and Route prerequisites from this page. Keep in mind, however, that aside from NTP, the SSL Orchestrator

GC will provide an opportunity to define DNS and route settings later in the workflow. No other configurations are required on this page, so click Next.



Topology Properties

SSL Orchestrator creates discrete configurations based on the selected topology. An explicit forward proxy topology will ultimately create an explicit proxy listener and its relying transparent proxy tunnel. If a subsequent transparent forward proxy topology is configured, it will not overlap the existing explicit proxy objects. The Topology Properties page provides the following options,

Topology Properties	User Input
Name	Enter a **Name** for the SSL Orchestrator deployment.
Description	Enter a **Description** for this SSL Orchestrator deployment.
Protocol	The Protocol option presents four protocol types: • **TCP** – this option creates a single TCP wildcard interception rule for the L3 Inbound, L3 Outbound L3, and L3 Explicit Proxy topologies. SSL and TLS are primarily used with TCP protocols. A TCP topology will create the necessary architecture to decrypt and re-encrypt traffic flows. • **UDP** – this option creates a single UDP wildcard interception rule for L3 Inbound and L3 Outbound topologies. A UDP topology does not perform decryption but can service chain UDP traffic. • **Other** – this option creates a single any-protocol wildcard (all non-TCP/non-UDP traffic) interception rule for L3 Inbound and L3 Outbound topologies. A non-TCP/non-UDP topology does not perform decryption or

	service chaining. It creates a routed path for non-TCP/non-UDP traffic flows. • **Any** – this option creates the TCP, UDP and non-TCP/UDP interception rules for outbound traffic flows. Select TCP to support decrypted traffic flows though the inline McAfee Web Gateway.
IP Family	Specify whether you want this configuration to support **IPv4** addresses or **IPv6** addresses.
SSL Orchestrator Topologies	The SSL Orchestrator Topologies option page presents six topologies: • **L3 Explicit Proxy** – this is the traditional explicit forward proxy. • **L3 Outbound** – this is the traditional transparent forward proxy. • **L3 Inbound** – this is a reverse proxy configuration. • **L2 Inbound** – the layer 2 topology options insert SSL Orchestrator as a bump-in-the-wire in an existing routed path, where SSL Orchestrator presents no IP addresses on its outer edges. The L2 Inbound topology provides a transparent path for inbound traffic flows. • **L2 Outbound** – the layer 2 topology options insert SSL Orchestrator as a bump-in-the-wire in an existing routed path, where SSL Orchestrator presents no IP addresses on its outer edges. The L2 Outbound topology provides a transparent path for outbound traffic flows. • **Existing Application** – this topology is designed to work with existing LTM applications. Whereas the L3 Inbound topology provides an inbound gateway function for SSL Orchestrator, Existing Application works with LTM virtual servers that already perform their own SSL handling and client-server traffic management. The Existing Application workflow proceeds directly to service creation and security policy definition, then exits with an SSL Orchestrator-type access policy and per-request policy that can easily be consumed by an LTM virtual server. Select L3 Outbound (transparent proxy) or L3 Explicit Proxy to support decrypted forward proxy traffic flows through the McAfee Web Gateway.

Click Save & Next.

SSL Configurations

This page defines the specific SSL settings for the selected topology, in this case a forward proxy, and controls both client-side and server-side SSL options. If existing SSL settings are available (from a previous workflow), it can be selected and re-used. Otherwise the SSL Configurations page creates new SSL settings for this workflow.

SSL Configurations	User Input
SSL Profile	
Name	Enter a **Name** for the SSL profile.
Description	Enter a **Description** for this SSL profile.
Client-side SSL	
Cipher Type	Cipher type can be a Cipher Group or Cipher String. If the former, select a previously-defined cipher group (from Local Traffic – Ciphers – Groups). If the latter, enter a cipher string that appropriately represents the client-side TLS requirement. For most environments, DEFAULT is optimal.
Certificate Key Chain	The certificate key chain represents the certificate and private key used as the "template" for forged server certificates. While re-issuing server certificates on-the-fly is generally easy, private key creation tends to be a CPU-intensive operation. For that reason, the underlying SSL Forward Proxy engine forges server certificates from a single defined private key. This setting allows customers to apply their own template private key, and 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 BIG-IP system is installed. Click Add, select default.crt and default.key, and click Done.
CA Certificate Key Chain	An SSL forward proxy must re-issue ("forge") remote server certificate to local clients using a local certificate authority (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. Assuming a local CA certificate and key were imported at the beginning of these steps, select them here. SSL Settings minimally require RSA-based template and CA certificates but can also support Elliptic Curve (EC) certificates. In this case, SSL Orchestrator would re-issue (forge) an EC certificate to the client if the TLS handshake negotiated an ECDHE_ECDSA cipher. To enable EC forging support, add both an EC template certificate and key, and EC CA certificate and key.

[Advanced] Bypass on Handshake Alert	This setting allows the underlying SSL Forward Proxy process to bypass SSL decryption if an SSL handshake error is detected on the server-side. It is recommended to leave this disabled.
[Advanced] Bypass on Client Certificate Failure	This setting allows the underlying SSL Forward Proxy process to bypass SSL decryption if it detects a Certificate request message from the server, as in when a server requires mutual certificate authentication. It is recommended to leave this disabled.
The above two Bypass options can create a security vulnerability. If a colluding client and server can force an SSL handshake error, or force client certificate authentication, they can effectively bypass SSL inspection. It is recommended that these settings be left disabled.	
Server-side SSL	
Cipher Type	Cipher type can be a Cipher Group or Cipher String. If the former, select a previously-defined cipher group (from Local Traffic – Ciphers – Groups). If the latter, enter a cipher string that appropriately represents the server-side TLS requirement. For most environments, DEFAULT is optimal.
Trusted Certificate Authority	Browser vendors routinely update the CA certificate stores in their products to keep up with industry security trends, and to account for new and revoked CAs. In the SSL forward proxy use case, however, the SSL visibility product now performs all server-side certificate validation, in lieu of the client browser, and should therefore do its best to maintain the same industry security trends. F5 BIG-IP ships with a CA certificate bundle that maintains a list of CA certificates common to the browser vendors. However, a more comprehensive bundle can be obtained from the F5 Downloads site. It is otherwise safe to select the built-in ca-bundle.crt.
[Advanced] Expire Certificate Response	SSL Orchestrator performs validation on remote server certificates and can control what happens if it receives an expired server certificate. The options are **drop**, which simply drops the traffic, and **ignore**, which mirrors an expired forged certificate to the client. The default and recommended behavior for forward proxy is to drop traffic on an expired certificate.
[Advanced] Untrusted Certificate Authority	SSL Orchestrator performs validation on remote server certificates and can control what happens if it receives an untrusted server certificate, based on the Trusted Certificate Authority bundle. The options are **drop**, which simply drops the traffic, and **ignore**, which allows the traffic and forges a good certificate to the client. The default and recommended behavior for forward proxy is to drop traffic on an untrusted certificate.
[Advanced] OCSP	This setting selects an existing or can create a new OCSP profile for server-side Online Certificate Status Protocol (OCSP) and OCSP stapling. With this enabled, if a client issues a Status_Request message in its ClientHello message (an indication that it supports OCSP stapling), SSL Orchestrator will

	issue a corresponding Status_Request message in its server-side TLS handshake. SSL Orchestrator will then forge the returned OCSP stapling response back to the client. If the server does not respond with a staple but contains an Authority Info Access (AIA) field that points to an OCSP responder URL, SSL Orchestrator will perform a separate OCSP request. The returned status is then mirrored in the stapled client-side TLS handshake.
[Advanced] CRL	This setting selects an existing or can create a new CRL profile for server-side Certificate Revocation List (CRL) validation. With this enabled, SSL Orchestrator attempts to match server certificates to locally cached CRLs.

Click Save & Next.

Services

The Services List page is used to define security services that attach to SSL Orchestrator. The Guided Configuration includes a services catalog that contains common product integrations. Each icon represents a security product integration deployed as one of the five basic service types. The service catalog also provides "generic" security services if your security service is not included in the catalog. Depending on screen resolution, it may be necessary to scroll down to see additional services.

To define the MWG service, select it in the service catalog and click Add, or simply double-click the icon.

Services	User Input
Name	Provide a unique name to this service (example "MWG").
Auto Manage Addresses	When enabled the Auto Manage Addresses setting provides a set of unique, non-overlapping, non-routable IP addresses to be used by the security service. If disabled, the To and From IP addresses must be configured manually. It is recommended to leave this option enabled (checked).

In environments where SSL Orchestrator is introduced to existing security devices, it is a natural tendency to not want to have to move these devices. And while SSL Orchestrator certainly allows it, by not moving the security devices into SSL Orchestrator-protected enclaves, customers run the risk of exposing sensitive decrypted traffic, unintentionally, to other devices that may be connected to these existing networks. It is therefore highly recommended, and a security recommended practice, to remove SSL Orchestrator-integrated security devices from existing networks and place them entirely within the isolated enclave created and maintained by SSL Orchestrator.

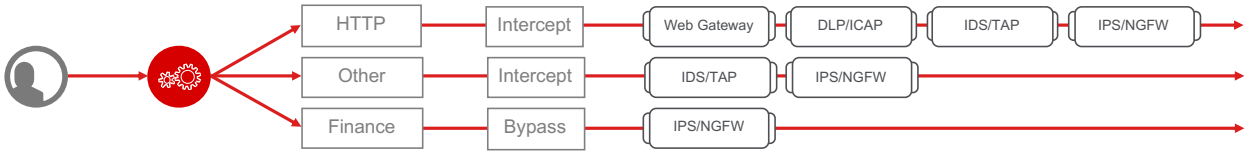
Proxy Type	This defines the proxy mode that the inline HTTP service is in. If in explicit proxy mode, the configuration will request the service's listening IP address and proxy port. If in transparent proxy mode, the configuration will simply request the service's inbound interface IP address. To support MWG explicit proxy mode authentication, configure this service as Explicit.
To Service Configuration	With the Auto Manage Addresses option enabled, this IP address will be pre-defined, therefore the to-service interface of the service must match this IP subnet. SSL Orchestrator uses an RFC2544 internal, non-routable address space (198.19.x.y/19). With the Auto Manage Addresses option disabled, the IP addresses must be defined manually. This assigned address specifies the F5 BIG-IP VLAN self-IP from which traffic will be flowing to the service. • **To Service** – with the Auto Manage Addresses option enabled, this IP address will be pre-defined, therefore the inbound side of the service must match this IP subnet. With the Auto Manage Addresses option disabled, the IP address must be defined manually. • **VLAN** – select the Create New option, provide a unique name (ex. MWG_in), select the F5 BIG-IP interface connecting to the inbound side of the service, and add a VLAN tag value if required.
Service Down Action	SSL Orchestrator also natively monitors the load balanced pool of security devices, and if all pool members fail, can actively bypass this service (**Ignore**), or stop all traffic (**Reset**, **Drop**).
Security Devices	An inline HTTP service may be defined as the load balances set of multiple devices on the same IP subnets. Minimally one device IP address must be defined. ▪ When the **Proxy Type** option is set to Explicit, this setting must specify the listening IP address and port of the HTTP proxy device. ▪ When the **Proxy Type** option is set to Transparent, this setting must specify the to-service IP address of the HTTP proxy device. Click Add, enter the service's inbound-side IP Address, the port value if explicit, then click Done.
From Service Configuration	With the Auto Manage Addresses option enabled, this IP address will be pre-defined, therefore the from-service interface of the service must match this IP subnet. SSL Orchestrator uses an RFC2544 internal, non-routable address space (198.19.x.y/19). With the Auto Manage Addresses option disabled, the IP addresses must be defined manually. This assigned address specifies the F5 BIG-IP VLAN self-IP to which traffic will be flowing from the service back to

	the F5 BIG-IP. This IP address should also be the gateway routing address on the layer 3 service to ensure all traffic is sent back to the F5 BIG-IP. • **From Service** – with the Auto Manage Addresses option enabled, this IP address will be pre-defined, therefore the outbound side of the service must match this IP subnet. With the Auto Manage Addresses option disabled, the IP address must be defined manually. • **VLAN** – select the Create New option, provide a unique name (ex. MWG_out), select the F5 BIG-IP interface connecting to the outbound side of the service, and add a VLAN tag value if required.
Manage SNAT Settings	This setting allows SSL Orchestrator to SNAT (source NAT) traffic to an inline service. This is especially useful in a load-balanced SSL Orchestrator scaling configuration but is not required here. Leave it set to None.
Authentication Offload	When an Access authentication profile is attached to an explicit forward proxy topology, this option will present the authenticated username value to the service as an X-Authenticated-User HTTP header. To enable delegate authentication to the MWG appliance, enable this option. MWG authentication is addressed later in this guide.
iRules	SSL Orchestrator allows for the insertion of additional iRule logic at different points. An iRule defined at the service only affects traffic flowing across this service. It is important to understand, however, that these iRules must not be used to control traffic flow (ex. pools, nodes, virtuals, etc.), 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. Additional iRules are not required, however, so leave this empty.

Click Save. When required services have been created, click Save & Next.

Service Chains

Service chains are arbitrarily ordered lists of security devices. Based on environmental requirements, different service chains may contain different re-used 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 of the security services, while non-HTTP traffic goes through a subset, and traffic destined to a financial service URL can bypass decryption and still flow through a smaller set of security services.



Click Add to create a new service chain containing all of the security services.

Service Chains	User Input
Name	Provide a unique name to this service (ex. "my_service_chain").
Services	Select any number of desired service and move them into the **Selected Service Chain Order** column, optionally also ordering them as required. In this lab, select all of the services. Click Save.

Click Save & Next.

Security Policy

Security policies are the set of rules that govern how traffic is processed in SSL Orchestrator. The "actions" a rule can take include,

- Whether or not to allow the traffic (Allow or Reject)
- Whether or not to decrypt the traffic (Intercept or Bypass)
- Which service chain (if any) to pass the traffic through

The SSL Orchestrator Guided Configuration presents an intuitive rule-based, drag-and-drop user interface for the definition of security policies. The security policy defines the set of traffic matching rules and corresponding actions to take on matches. The built-in security policy contains two rules:

- **Pinners_Rule** – used to match URLs on a Pinners custom URL category, for TLS bypass. The Pinners custom URL category is a built-in category and contains a non-exhaustive list of sites known to use certificate pinning. You may need to add sites to this list based on specific business requirements.

- **All Traffic** – the default catch-all rule for any traffic that does not match other rules. By default, this rule allows and intercepts (decrypts) traffic but does not preselect any service chain. Optionally edit this rule to add a "default" service chain.

In the background, 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. By default, this rule allows and intercepts (decrypts) traffic but does not preselect any service chain. Create any security rules as required, then click Save & Next.

Note that once the per-request policy is manipulated, the rules-based user interface can no longer be used.

Interception Rule

Interception rules are based on the selected topology and define the "listeners", analogous to LTM virtual servers, that accept and process different types of traffic (ex. TCP, UDP, other). The resulting LTM virtual servers will bind the SSL settings, VLANs, IP addresses, and security policies created in the topology workflow. Again, note that security services are opaque within the protected inspection zone, thus the proxy mode deployed for the inline McAfee Web Gateway is irrespective to the SSL Orchestrator topology mode. The following will demonstrate SSL Orchestrator as either a transparent or explicit forward proxy.

Interception Rule	User Input
Common Settings	
Source Address	The source address field provides a filter for incoming traffic based on source address and/or source subnet. It is usually appropriate to leave the default 0.0.0.0%0/0 setting applied to allow traffic from all addresses to be processed.
Destination Address/Mask	The destination address/mask field provides a filter for incoming traffic based on destination address and/or destination subnet. As this is a transparent forward proxy configuration, it is appropriate to leave the default 0.0.0.0%0/0 setting applied to allow all outbound traffic to be processed.
Ingress Network – VLANs	This defines the VLANs through which traffic will enter. For a transparent forward proxy topology, this would be a client-side VLAN.
Transparent Proxy Settings	
Port	This defines a matching destination port for ingress traffic flows. It may be desirable to only process HTTP port 80 or HTTPS port 443 for example. The default 0 port pattern processes outbound traffic on any port.
Security Policy Settings	This defines the security policy that will process traffic based on traffic matching rules. This will default to the previously created security policy.
Explicit Proxy Settings	

Proxy Server Settings – IPV4 (or IPV6) Address	This address is the IP address that clients will target to access external resources. This is typically done by setting the browser's proxy server settings to this address, or by using Proxy Auto-Configuration (PAC) or WPAD scripts to point client user-agents at this IP address.
Proxy Server Settings – Port	The proxy service instance also requires a listening port. This is traditionally port 8080 or 3128.
Proxy Server Settings – Access Profile	In order to perform authentication on explicit forward proxy traffic, F5 Access Policy Manager (APM) must be licensed and provisioned. Explicit forward proxy authentication is then defined within an "SWG-Explicit" access profile. Once an SWG-Explicit access profile is created, it can be selected here to enable authentication on this explicit forward proxy instance. Proxy authentication is covered in a later chapter.
Note while visible for an explicit proxy topology, the Port setting is greyed out and non-editable. The port for an explicit proxy is defined in the Proxy Server Settings section of this page.	

Click Save & Next.

Egress Settings

The Egress Setting page defines the topology-specific egress characteristics.

Egress Settings	User Input
Manage SNAT Settings	Defines if and how source NAT (SNAT) is used for egress traffic.
Gateways	Defines the next hop route for traffic. For an outbound configuration, this is usually a next hop upstream router.

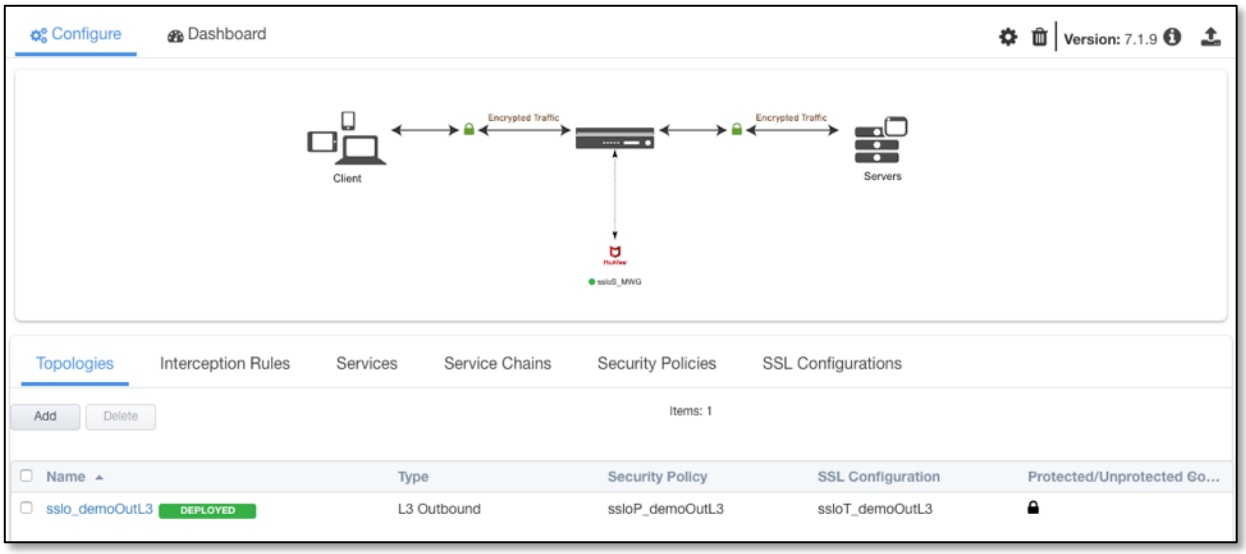
Click Save & Next.

Summary

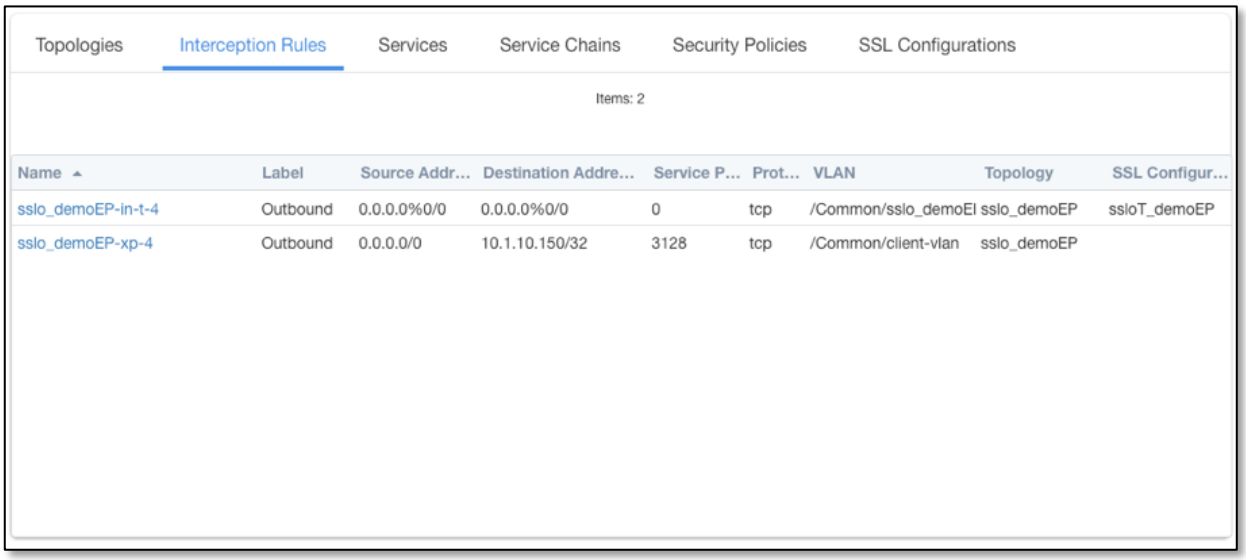
The summary page presents an expandable list of all of the workflow-configured objects. To expand the details for any given setting, click the corresponding arrow icon on the far right. To edit any given setting, click the corresponding pencil icon. Clicking the pencil icon will send the workflow back to the selected settings page.

When satisfied with the defined settings, click Deploy.

Upon successfully deploying the configuration, SSL Orchestrator will now display a **Configure** view.



The **Interception Rules** tab may show one or two interception rules (listeners), depending on transparent or explicit proxy topology creation.



In the above,

- If an SSL Orchestrator L3 outbound (transparent proxy) topology was created:
    - The **-in-t-4** listener receives traffic from the client and performs all of the SSL Orchestrator functions (i.e. decryption, service chaining).

- If an SSL Orchestrator explicit proxy topology was created:
    - The **-xp-4** listener is the explicit proxy service endpoint that receives traffic from the client. All HTTP and HTTPS traffic is tunneled through this listener.
    - The **-in-t-4** listener receives traffic from the -xp-4 tunnel and performs all of the SSL Orchestrator functions (i.e. decryption, service chaining).

DNS Query Resolution (explicit proxy topology)

An explicit forward proxy performs DNS resolution on the client's behalf. For an SSL Orchestrator explicit proxy topology to work, you must also define DNS settings. Under the main SSL Orchestrator Configuration page, click on the gear icon in the top right to access System settings. This configuration step creates a DNS resolver object.

- Select Internet Authoritative Nameserver and enter Local/Private Forward Zones, or
- Select Local Forwarding Nameserver and enter Local DNS Nameservers

Control channel virtual server

Previously, the McAfee Web Gateway appliance was configured with IP spoofing, and optionally a source NAT policy to cause MWG to egress traffic on the client's IP address. This creates different traffic patterns for normal client-server traffic and device-initiated traffic so that a separate "control channel" virtual server can be created to catch device-initiated traffic and egress directly. In the F5 BIG-IP UI, navigate to Local Traffic -> Virtual Servers and client the **Create** button.

Source NAT Virtual Server	User Input
Type	Select Performance (Layer 4).
Source Address	Enter the MWG's from-service interface IP address here. This is the source address that the virtual server will filter on, to capture device-initiated traffic.
Destination Address/Mask	Enter 0.0.0.0/0 to allow this virtual server to capture all MWG-initiated outbound traffic. You may optionally tighten this filter to specific IP addresses.
Service Port	Enter 0 to allow this virtual server to capture MWG-initiated traffic destined to any port. You may optionally tighten this filter to specific ports.
Protocol	Select * All Protocols.
Protocol Profile (Client)	Select fastL4.
VLAN and Tunnel Traffic	Enable only on the MWG **from-service** VLAN.
Source Address Translation	Enable SNAT only if the SSL Orchestrator topology also defines egress SNAT.
Address Translation	This setting must be disabled (unchecked).
Port Translation	This setting must be disabled (unchecked).

Default Pool	Create a new pool here and enter the same egress route IP address used in the SSL Orchestrator topology. If System Route was selected in the topology, do not assign a pool here.

Click Finished to complete this virtual server configuration. At this point, the McAfee Web Gateway appliance will have access to Internet resources through this virtual server.

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

Testing the solution

You can test the deployed solution using the following options:

Server certificate test

To test an explicit forward proxy topology, configure a client's browser proxy settings to point this this listening IP address and port. Ensure that the client trusts the local issuing CA certificate. Open a browser from the client and attempt to access an external HTTPS resource. Once the page is loaded, observe the server certificate of that site and take note of the certificate issuer, which should be the local issuing CA. If you have access to the client's command line shell and the **cURL** or **wget** utilities, you can simulate browser access using one of the following commands:

```
curl -vk --proxy [proxy IP:port] https://www.example.com
```

```
wget --no-check-certificate -e use_proxy=yes -e https_proxy=[proxy IP:port] -dO –
https://www.example.com
```

Both of these commands will display both the HTML server response, and the issuer of the server's certificate.

Decrypted traffic analysis on the F5 BIG-IP system

Perform a tcpdump on the F5 BIG-IP system to observe the decrypted clear text traffic. This confirms SSL interception by SSLO.

```
tcpdump –lnni [interface or VLAN name] -Xs0
```

As a function of adding a new service, the UI requires a name for each (source and destination) network. SSL Orchestrator will then create separate source and destination VLANs for inline security devices, and those VLANs will be encapsulated within separate application service paths. For example, given an inline HTTP service named "MWG" with its "From BIGIP VLAN" named "**MWG_in**", and its "To BIGIP VLAN" named "**MWG_out**", its corresponding F5 BIG-IP VLANs would be accessible via the following syntax:

ssloN_ + *[network name]* + ***.app/ssloN_*** + *[network name]*

Example:
ssloN_MWG_in.app/ssloN_MWG_in
ssloN_MWG_out.app/ssloN_MWG_out

A tcpdump on the source side VLAN of this FireEye service would therefore look like this:

```
tcpdump -lnni ssloN_MWG_in.app/ssloN_MWG_in -Xs0
```

The security service VLANs and their corresponding application services are all visible from the F5 BIG-IP UI under Network -> VLANs.

Decrypted traffic analysis on the McAfee Web Gateway

From the MWG UI:

- Navigate to the Troubleshooting section and Packet Tracing.
- In the Command line parameters field, enter:

  ```
  -s 0 -i any
  ```

  This will capture traffic on all interfaces. To optionally capture on a specific interface, replace the word 'any' above with the name of the interface.

- Click the **tcpdump start** button to start a capture, **tcpdump stop** the stop the capture, and then download the resulting capture to review (typically in Wireshark).
- It is also possible, if SSH access is enabled, to access the MWG console directly and issue **tcpdump** commands natively.

Proxy policy analysis on the McAfee Web Gateway

From the MWG UI:

- Navigate to the Troubleshooting section and Rule Tracing Central.
- Enter client IP address to be monitored and click Go button.
- Stop trace by clicking on the X button that "replaced" the Go button.
- More details can be found in the appropriate McAfee Web Gateway Product Guide for your version.

Additional considerations

There are a few other configuration concepts that you may need to explore when integrating a McAfee Web Gateway with SSL Orchestrator.

Authentication

The services attached to SSL Orchestrator are opaque to the external environment, thus they are protected, isolated, and do not interact outside of the internal connectivity with the F5 BIG-IP. If a McAfee Web Gateway appliance requires authenticated user identity, SSL Orchestrator must be configured to perform the user authentication and pass identity information to MWG as a "delegate token". To do authentication, the F5 BIG-IP additionally requires Access Policy Manager (APM) module activation. The following details this very simple configuration to enable delegate authentication to the MWG appliance.

Configure an APM access policy to authenticate explicit forward proxy users

Configuration of forward proxy client authentication is beyond the scope of this guide, except that explicit forward proxy authentication must use the **SWG-Explicit** profile type, and transparent forward proxy authentication uses the **SWG-Transparent** profile type for captive portal authentication.

- For explicit forward proxy authentication, create or edit an explicit proxy SSL Orchestrator topology and attach the SWG-Explicit access profile on the Interception Rules page of the topology workflow, under the **Access Profile** option.

- For transparent forward proxy (captive portal) authentication, refer to the SSL Orchestrator deployment guide for additional instructions.

Configure the MWG service definition to pass the delegate token

In the SSL Orchestrator UI, under Services, select to the edit the MWG service. Click to enable the **Authentication Offload** setting (checked). This option when enabled will send the authenticated user identity to the inline HTTP service as an X-Authenticated-User HTTP header.

Configure the MWG to consume the delegate token

Delegate token consumption is configured in a policy. In the MWG UI, in the Policy section, navigate to Common Rules and click the **Add Rules…** button.

Delegate Token Policy	User Input
Name	Provide a unique name for this policy.

Rule Criteria	Select **If the following criteria is matched** and click the **Add** button, and then **User/Group criteria**. Select the Athentication.IsAuthenticated option, equals, and false. Click the **OK** button.
Action	Select Continue.

Events	Click the **Add** button, and then **Set Property Value…** and create the following rule:
	
	`Set Authentication.UserName = Header.Get("X-Authenticated-User")`
	`Set Authentication.IsAuthenticated = true`
	
	• **Add** -> **Set Property Value…**
	• Select **Authentication.UserName**
	• Click the **Add…** button
	• Click the **Parameter Property** button
	• Select **Header.Get(String)** and click the **Parameters…** button
	• In the Parameter Value field, enter X-Authenticated-User and click the **OK** button.
	• Click the **OK** button, then again to complete the rule.
	
	• **Add** -> **Set Property Value…**
	• Select **Authentication.IsAuthenticated**
	• In the Parameter value field, select true.
	• Click the **OK** button.

Click **Finished** to complete the delegate authentication rule.

Additional rules can optionally be created within the Web Gateway to collect user group information from a username query to an external directory. Alternatively rules similar to the above can be used to process authenticated user groups in an X-Authenticated-Groups header populated by F5 BIG-IP.

The McAfee Web Gateway appliance should now be ready to receive the user identity via the delegate X-Authenticated-User HTTP header. MWG may now use this user identity as if it had collected the value itself from direct challenge-response authentication.

If creating service networks manually

Security recommended practice is to move security devices to SSL Orchestrator's protected network enclave. When doing so, SSL Orchestrator provides a set of internal network addresses that the security service can use. This is the **Auto Manage** setting in the service definition. In the event that you choose not to heed this security recommendation, or otherwise need to create alternate addressing for the inline security service, in the service definition, uncheck the Auto Manage option and perform the following steps.

Disable the Auto-Manage option and alter the **To Service Configuration** and **From Service Configuration** sections.

Egress Settings	User Input
To Service Configuration (select Create New)	
Name	Provide a unique local name (ex. MWG_in)
VLAN	Select Create New (or select an existing VLAN if one exists) • Select the correct inbound-side interface (F5 BIG-IP to service) • Enter a VLAN tag value, as required
Network Settings	• Enter the SSL Orchestrator inbound-side self-IP (ex. 198.19.96.7) • Enter the corresponding Netmask (ex. 255.255.255.128)
From Service Configuration (select Create New)	
Name	Provide a unique local name (ex. MWG_out)
VLAN	Select Create New (or select an existing VLAN if one exists) • Select the correct inbound-side interface (service to F5 BIG-IP) • Enter a VLAN tag value, as required
Network Settings	• Enter the SSL Orchestrator outbound-side self-IP (ex. 198.19.96.245) • Enter the corresponding Netmask (ex. 255.255.255.128)

All other settings are the same.

DNS caching

In the above configurations, the McAfee Web Gateway requires some amount of external connectivity, minimally to reach licensing and subscription update services, but also if an explicit proxy, to reach DNS. The control channel virtual server and MWG IP spoofing enables this direct connectivity. However, when SSL Orchestrator is also an explicit proxy, both devices require DNS, thus requiring two queries for each site accessed.

If SSL Orchestrator is licensed as an add-on to base Local Traffic Manager (LTM), the above DNS requirement can be further optimized using the F5 BIG-IP "DNS Services" license. With this license, F5 BIG-IP can act as a DNS cache for both SSL Orchestrator and for MWG. As traffic passes through the SSL Orchestrator explicit proxy, a DNS query is performed through the cache. If no record exists, external DNS is consulted, and a value returned and cached. When MWG performs its request, the record is immediately served from the same cache. To enable DNS caching, first ensure that the **DNS Services license** is activated.

To create the DNS Services cache configuration:

Create a DNS Cache configuration, in the F5 BIG-IP UI, under **DNS -> Caches -> Cache List**, click Create…

DNS Cache	User Input
Name	Provide a unique name.
Resolver Type	Select Transparent (None).

All other settings here can be changed as needed.

Create a DNS profile, in the F5 BIG-IP UI, under **Local Traffic -> Profiles -> Services -> DNS**, click Create…

DNS Profile	User Input
Name	Provide a unique name.
DNS Cache	Select Enabled.
DNS Cache Name	Select the previously created DNS Cache.

Create a DNS Proxy virtual server. To allow access to the McAfee Web Gateway, this virtual server should be on an address local to either the to-service or from-service VLANs defined for the MWG. In the F5 BIG-IP UI, under **Local Traffic -> Virtual Servers**, click Create…

DNS Cache Virtual Server	User Input
Name	Provide a unique name.
Type	Select Standard.

Source Address	Select 0.0.0.0/0.
Destination Address/Mask	Use an IP address here that is in the same subnet as the MWG's to-service or from-service VLAN.
Service Port	Enter port 53 here.
Protocol	Select UDP.
Protocol Profile (Client)	Select udp.
DNS Profile	Select the previously create DNS profile.
VLANs and Tunnel Traffic	Select the corresponding MWG to-service or from-service VLAN.
Source Address Translation	Enable Source NAT (SNAT) as required to allow access to external DNS.
Address Translation	Check to enable.
Port Translation	Check to enable.
Default Pool	Click the plus side (+) to create a new pool that points to an external DNS resource (ex. 8.8.8.8) or select an existing DNS services pool if one exists.

Finally, configure the McAfee Web Gateway to point to this virtual server IP address for DNS queries. If SSL Orchestrator is configured as an explicit proxy, configure its DNS Local Forwarding Nameserver settings to point to this same virtual server IP address.