SOLUTION OVERVIEW

F5 Secure Web Gateway Services as an SSL Orchestrator Service

Balancing fast application access with organizational security can be a daunting task. Powerful URL categorization and content filtering can empower you to allow, block, or confirm and continue access to sites and applications on a user-by-user basis, providing security without compromising employee productivity.

KEY BENEFITS

Save deployment time and administration costs
Insert a secure web gateway per-request profile directly into your SSL Orchestrator dynamic service chain.

Enforce organizational policies
Maintain employee productivity or restrict access to prohibited content categories.

Decrease footprint and lower TCO
Deploy F5 Secure Web Gateway Services on the same platform as SSL Orchestrator to lower your footprint and total cost of ownership (TCO).

Prevent malware compromises
Draw from the F5 Secure Web Gateway Services database of deny-listed URLs to prevent access to known malicious, malware-laden sites.

The Problem of Uncontrolled Web Access

Giving employees completely unrestricted, uncontrolled web and application access is risky. You need to prevent your users from accessing websites and applications that may be infected with malware, and from accidentally compromising your network. You may also need to restrict access to prohibited web content categories, or block traffic to bandwidth chokers such as streaming services or online gaming. Whatever the needs of your network, you should be able to enforce restrictions and control the websites and applications your users access without issues and with minimal downtime. And since you know your network best, enforcing organizational policies and ensuring organizational security by performing these essential functions should not compromise flexibility.

Web access gateways allow you to categorize and classify web traffic—protecting your organization and your users from malicious websites and cloud traffic that may infect or attack your network and applications, while allowing you to enforce policies that meet your organization's unique needs. Flexibility and programmability are at the heart of F5 Secure Web Gateway Services.

Secure Web Gateway Services can now be deployed as a service within F5 SSL Orchestrator to suit your categorization, classification, and content inspection needs for encrypted traffic. SSL Orchestrator enables the subscription-based Secure Web Gateway Services to be exposed as a recognized service in the SSL Orchestrator Services Catalog, providing visibility into, and orchestration, categorization, and classification for, all encrypted traffic traversing your network, both inbound and outbound. To learn more about the capabilities of SSL Orchestrator, read the product data sheet.

With the addition of Secure Web Gateway Services as a service supported by SSL Orchestrator, you can manage web access across your organization with URL categorization. This allows you to enforce organizational policies against access to specific content, prevent access to potentially malware-laden websites and apps, or stop bandwidth chokers, among other uses. With access to a constantly-expanding database of URLs—currently consisting of hundreds of URL categories and tens of millions of pre-defined URLs—you can leverage Secure Web Gateway Services' intelligent classification engine to block or accept traffic. Secure Web Gateway Services is also the only web access gateway to secure against both inbound and outbound malware, so you can defend your organization against a variety of attack vectors.

So, what does Secure Web Gateway Services provide on top of the SSL Orchestrator solution?

SSL Orchestrator offers:

- TLS decryption
- Dynamic service chaining
- Intelligent, context-aware traffic routing
- Real-time traffic classification
- Support for multiple technologies
- Multiple service insertion
- Programmable logic
- SSL Orchestrator per-request policy
- Layer 3-6 functionality

Additional functionality for SSL Orchestrator with Secure Web Gateway Services as an SSL Orchestrator service includes:

- URL filtering
- URL classification
- Content inspection
- Secure web gateway per-request policy
- Layer 7 functionality

Enable Traffic Classification and Action in Your SSL Orchestrator Dynamic Service Chain

ENFORCING ORGANIZATIONAL POLICY AND ENSURING ORGANIZATIONAL SECURITY SHOULD NOT COME AT THE EXPENSE OF FLEXIBILITY.

Implementing a secure web gateway within your SSL Orchestrator topology allows you to deploy Secure Web Gateway Services on the same box as SSL Orchestrator. This combination delivers all the benefits of an SSL Orchestrator subscription while providing the additional benefits of a robust URL classification engine. Secure Web Gateway Services features regular URL database updates as new threats and URLs are identified. With F5 Secure Web Gateway Services in an SSL Orchestrator topology, you can insert the Secure Web Gateway Services directly inline in your SSL Orchestrator topology, leading to a smaller appliance footprint, decreased total cost of ownership (TCO), and lower latency through SSL Orchestrator's efficient dynamic service chaining.

Secure Web Gateway Services as an SSL Orchestrator service allows you to enforce corporate policy, protect against inappropriate content in web searches, and prevent access to malicious sites or denylisted URLs. With this combined solution, you can identify malicious content and block it from traversing your network. You can also prevent unnecessary strain on your network by blocking access to sites and applications that can dominate crucial bandwidth, such as online gaming and streaming sites. F5 Secure Web Gateway Services in an SSL Orchestrator topology also provides support for Safe Search—a search engine feature that prevents offensive content and images from showing up in search results.

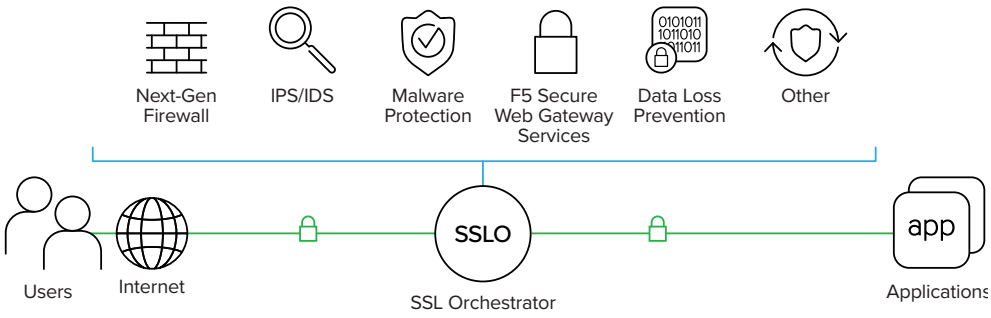

Figure 1: Implement F5 Secure Web Gateway Services in your SSL Orchestrator deployment to enable URL classification and action in your dynamic service chain.

WITH SECURE WEB GATEWAY SERVICES, YOU CAN IDENTIFY MALICIOUS CONTENT AND BLOCK IT FROM TRAVERSING YOUR NETWORK.

Secure Web Gateway Services also allows you to create per-request policies to accept or block content to specific URL categories on a user-by-user basis, if needed. With secure web gateway per-request policies, you can provide logic to determine how to best process URL requests. Depending on the actions you include in the per-request policy, you can control whether or not to bypass SSL traffic and determine whether to allow or reject a URL request based on URL categories and a database of pre-defined URLs maintained by Secure Web Gateway Services.

Adding F5 Secure Web Gateway Services in your SSL Orchestrator topology also gives you access to analytics tools for URL access that run through SSL Orchestrator. With accessible dashboards, you can view statistical information about traffic logged by the BIG-IP system for Secure Web Gateway. Graphs, such as Top URLs by Request Count and Top Categories by Blocked Request Count, summarize activities over time. Using the robust analytics for this tool, you can detect patterns in complex attack vectors or gain insight into commonly-accessed URL categories.

KEY FEATURES

Analyze traffic with a robust classification engine
F5 Secure Web Gateway Services features URL filtering and traffic classification powered by a robust database with hundreds of pre-defined URL categories and 60 million URLs and counting.

Intelligently classify traffic to allow or block
With powerful URL categorization and filters, you can allow, block, or confirm and continue access to sites and applications on a user-by-user basis. Enforce security without compromising employee productivity.

Enable Safe Search
F5 Secure Web Gateway Services allows you to enable Safe Search—a search engine feature that can prevent offensive content and images from showing up in search results.

Protect your application layer
F5 Secure Web Gateway Services sits inline in an SSL Orchestrator topology and functions at the application layer, in comparison to other supported SSL Orchestrator services which function at Layer 3 to Layer 6.

Flexible customization options for your secure web gateway
With F5 Secure Web Gateway Services programmable logic, you can create per-request policies for all URL requests for inbound and outbound traffic.

Conclusion

Using a web access gateway does not have to compromise the flexibility of your controls or deployment. With Secure Web Gateway Services as an SSL Orchestrator service, you can add Secure Web Gateway Services to your security stack with no service downtime when traffic may be accidentally bypassed. Additionally, with the secure web gateway add-on subscription, you can reduce your security footprint and prevent security oversubscription. With the robust customization options of the Secure Web Gateway Services per-request policy, you can protect your network from malware and enforce corporate policy according to your individualized needs. The Secure Web Gateway Services URL database updates continuously, ensuring that your system leverages the latest URL categorizations as new threats emerge. No matter what your traffic classification and action needs, Secure Web Gateway Services as an SSL Orchestrator service gives you a flexible, secure, and up-to-date solution for your web access needs.

TAKE THE NEXT STEP

Deploy F5 Secure Web Gateway Services as a part of the services catalog in the latest version of SSL Orchestrator. Download the latest version of BIG-IP at downloads.f5.com.

To learn more, contact your F5 representatives or visit the F5 SSL Orchestrator product page.