F5 Secure Web Gateway Services Reference Architecture

Caught between high-profile security breaches, APTs, and “millennial” employees who expect 24/7 Internet access, forward-looking IT organizations can consolidate web access and security into a high-performance, strategic point of control: F5 Secure Web Gateway Services.

Technical White Paper

by David Holmes

Contents

Introduction

The most high-profile security breaches of recent memory started with spear-phishing attacks. These campaigns targeted the *employees* of specific organizations and enticed them with downloads filled with malicious software into their corporations' networks. That malware then enabled the exfiltration of customers' sensitive and personally identifiable information (PII), trade secrets, or financial assets. New, even more sophisticated and dangerous threats are exploding on the web daily. The menu of malware now available includes drive-by downloads and the threat du jour, watering-hole attacks. The significance and coverage of these events are prompting today's IT security organizations to specifically increase their security postures around employees' use of and access to the Internet.

Traditionally, organizations have attempted to enforce a measure of web security on their users by requiring the use of a forward proxy to intercept and inspect the users' outbound Internet connections. Anyone who has worked in a reasonably large enterprise network has likely encountered these proxies (and perhaps attempted to evade them). Vendors have specialized in these forward proxies for a decade, but over that time the technology itself has not improved significantly.

The Challenges of Securing Outbound Access

While the forward proxy technology has stood still, the problem space has not. The challenges have been evolving, specifically around three areas:

- The increased use of "SSL everywhere" is blinding traditional forward proxies.
- The unexpected severity of phishing attacks is increasing the stakes.
- Device sprawl and administration requirements are forcing organizations to consider equipment consolidation.

Traditional forward proxies have been blind to SSL traffic and malware payloads, often requiring separate, complementary devices to complete the solution.

These changes have been occurring around the world, yet the forward proxy solutions have not kept up. Administrators are looking for a solution that meets these new challenges.

F5 Secure Web Gateway Services

Because F5 products occupy the strategic point of control in the network, F5 Networks is uniquely positioned to help organizations secure their users with high-capacity, high-performance web security on the same platforms those organizations use for application delivery control.

The F5 Difference

What makes F5® Secure Web Gateway Services different from traditional forward proxies? There are five major differences, and these differences are critical to understanding the ability of the F5 solution to complete a web-security reference architecture.

- **Integrated malware detection.** Traditional forward-proxy solutions perform similar URL filtering but require an additional appliance or set of devices to perform malware detection. The Secure Web Gateway Services solution integrates this functionality into the same platform.
- **Scale and performance.** The reference architecture for Secure Web Gateway Services delivers a much higher scalability factor than traditional forward proxies. This enables fewer devices to handle web security and lowers CapEx for the enterprise.
- **SSL interception.** The increased use of SSL in all organizations requires a means to intercept and inspect outbound SSL connections. Traditional solutions often involve an F5 Application Delivery Controller (ADC) to perform this functionality. Incorporating Secure Web Gateway Services into the main ADC platform achieves consolidation gains.
- **Federated single sign-on.** The F5 solution is the only one on the market today that integrates federated single sign-on (SSO). This mature F5 technology enables an organization to create a captive portal page for authenticating users each morning and then to provide SSO for the remainder of the day, enhancing the user experience and saving precious time.
- **Consolidation of security services.** All of these outbound security services are available on every F5 platform. The inbound security features are as well. This means that consolidation for both inbound and outbound access and security are available at the strategic point of control in the network.

These differences enable F5 Secure Web Gateway Services to provide a compelling architecture for both web security and application security.

Three Fundamental Features of a Secure Web Gateway

All use cases of Secure Web Gateway Services are built on a foundation of three security functions: URL filtering, malware scanning, and reporting.

URL categorization and filtering

The most basic of these functions is the URL categorization and filtering provided in Secure Web Gateway Services. A database of billions of URLs that are scored and evaluated is delivered to the Secure Web Gateway Services platform daily, with updates occurring every few minutes. This URL categorization database includes sites that host malware, phishing proxies, or click-jacking sites, and it may be customized for enterprise-specific content.

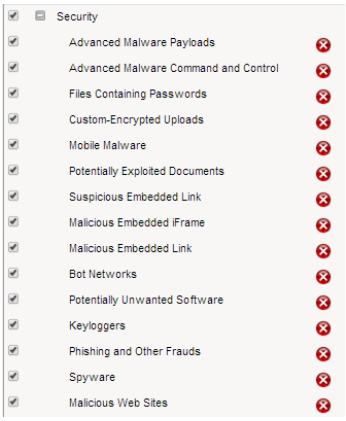

Figure 1: The security category of the URL database

Malware scanning

The URL categorization database can alert Secure Web Gateway Services that certain content should be subject to additional scans for malware. The F5 solution can then intercept and inspect malware payloads and links in the most popular file formats, such as Adobe Flash and Adobe PDF.

Reporting

To make good policy, as well as to adhere to industry and government regulations, administrators require visibility. Because Secure Web Gateway Services is the strategic point of control for outbound web access, it is the natural place to monitor and report on web usage trends. Some organizational policies require logging every request, and some organizations log only those requests that trigger a risk alert. The F5 solution accommodates both. Popular reports available, for example, include a report identifying the users who consume the most bandwidth in the network.

The security engine at the heart of F5 Secure Web Gateway Services is the Websense URL categorization database. Websense monitors billions of URLs every day to compile this real-time threat intelligence source.

Understanding Explicit and Transparent Proxies

F5 Secure Web Gateway Services can automatically function as a transparent forward proxy for all user requests flowing through it to the Internet. When the solution is used this way, administrators do not have to make changes to each device's settings or to group policy to be able to intercept user sessions.

Secure Web Gateway Services also can function as an explicit proxy. Unlike transparent proxy mode, the explicit forward proxy mode requires administrators to explicitly define the outgoing forward proxy for each of the target devices (and users) on the network. While this sounds like more administration work, organizations have found that there are significant, tangible security benefits associated with explicit proxy mode.

Secure Web Gateway Services automatically creates auto configuration files in either WPAD or PAC format. Otherwise, the settings for the explicit proxy can be pushed out via group policy or another enterprise management solution.

How F5 Customers Use Secure Web Gateway Services

The Secure Web Gateway Services reference architecture anticipates four typical customer scenarios. These scenarios are not mutually exclusive and, in fact, are usually collocated.

- **Context-aware security.** The Secure Web Gateway Services secures users in the familiar corporate environment.
- **Bandwidth control**. The F5 solution can limit bandwidth consumption by media content type and thus influence user behavior.
- **Acceptable use policy presentation.** Secure Web Gateway Services helps organizations provide network access for visiting users while deferring much of the associated liability by requiring acceptance of an acceptable use policy.
- **Compliance.** Payment Card Industry (PCI) guidelines associated with security for credit card numbers require that servers within a cardholder data environment (CDE) use a forward proxy to access update servers across the Internet.

Deployment Scenarios

To achieve the goals of the customer scenarios, the actual deployment of Secure Web Gateway Services will typically fall into three distinct models: corporate, guest access, and PCI CDE DMZ. These deployment scenarios, which support multiple customer scenarios, are differentiated by the features enabled in each. In addition, regardless of the deployment scenario, the solution provides:

- URL categorization and filtering.
- Malware scanning.
- Reporting.

Corporate Deployment Scenario

A corporate deployment of the Secure Web Gateway Services solution has many possible configuration profiles to fit different network and security requirements. While no two organizations are the same, for most, Secure Web Gateway Services secures outbound web traffic generated by the organization's employees by categorizing and filtering URLs, scanning for embedded malware, and optionally curbing unproductive web behavior.

In general, a typical corporate architecture will include the Secure Web Gateway Services base functionality of URL filtering, malware scanning, and reporting, plus a common set of additional features:

- Integration with the corporate directory for user identification
- SSL interception
- Federated SSO

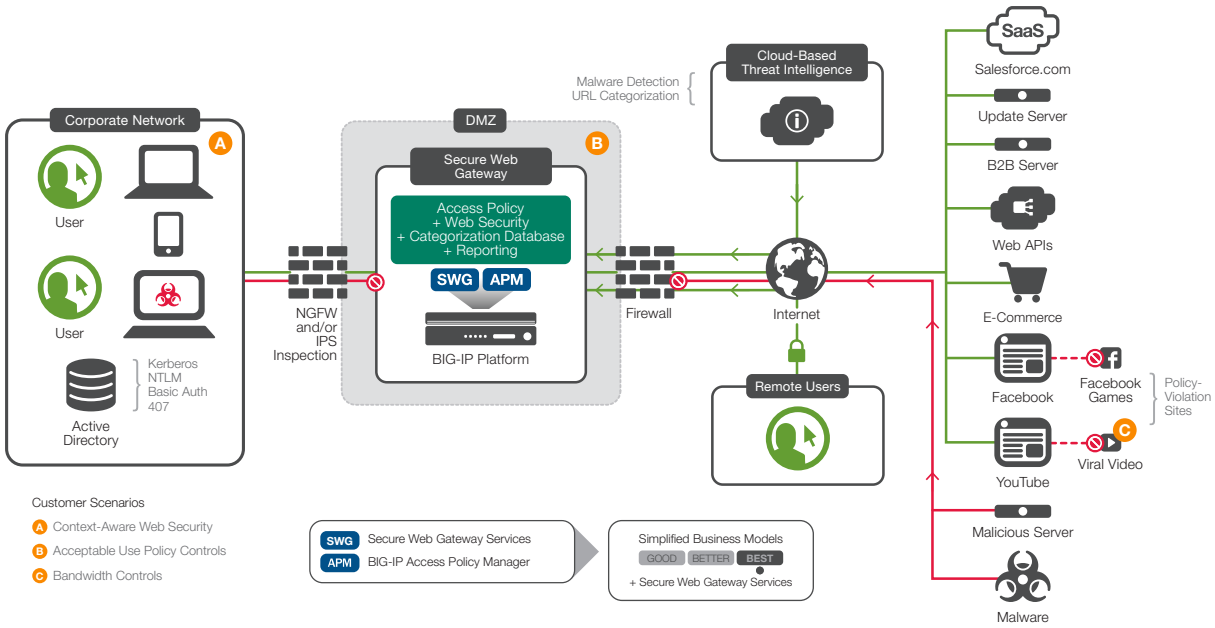

Figure 2: A corporate deployment scenario, which may support all four customer scenarios.

Using corporate directories for user identification

The Secure Web Gateway Services solution secures traffic at Layer 7 with the understanding of application protocols inherent in its ADC platform. However, it intercepts traffic at Layers 3 and 4, IP and TCP. Because these layers do not provide mapping to the

user, the Secure Web Gateway Services protocol can collaborate with Microsoft Active Directory service to map an IP address to an authenticated username.

By coordinating Secure Web Gateway Services with Active Directory, administrators can see who is doing what, when, and which users may be infected by malware. When Active Directory communication is enabled, the audit log for a request will include the name of the user associated with the request.

If mapping cannot be determined (perhaps because of a rogue device on the network), Secure Web Gateway Services offers three possible approaches for the unauthenticated connection:

1. The connection can be denied for maximum security.
2. The connection can be associated with a much more restrictive security policy.
3. The connection can be forwarded to a captive portal, where the user will be required to authenticate (thereby allowing Secure Web Gateway Services to track the user associated with that device).

Inspecting encrypted traffic

Inspecting encrypted outbound traffic is no longer optional. The increasing use of HTTPS as the default transport protocol means that administrators must be able to able crack open these connections for inspection. The SSL intercept feature of Secure Web Gateway Services works by automatically generating certificates that appear as the target website to internal users. The browser, which is configured to trust the solution's digital certificate, thinks that it is communicating directly with the target website.

While SSL intercept is a powerful feature, there are times when administrators will not want to intercept the connection, including for:

- Websites that provide online banking. Typically an administrator will not want to intercept the user data for financial institutions.
- Websites that require client certificate authentication. Due to how the SSL protocol is structured, Secure Web Gateway Services cannot intercept sites that require client certificate authentication.
- Websites that fingerprint the server certificate. Automated update servers sometimes have the target certificate embedded in their client software and will throw an error if SSL intercept is used.

- High-trust SaaS sites. Many administrators have a high trust relationship with their most frequently used SaaS platforms. They may choose, in the interest of performance, to avoid intercepting and inspecting each user connection to those services.

Note that client certificate authentication is not compatible with transparent SSL proxies. Nor are certificate pinning services or any services that validate the fingerprint of the server certificate (such as Microsoft Windows Update). For sites that require client certificate authentication or other features not compatible with transparent SSL proxies, administrators can create a custom category of whitelisted sites for which the inspection can be bypassed. Ultimately, the choice of which websites should be bypassed for SSL intercept is a policy decision to be made and managed by the administrator.

The F5® iApps® Template for Secure Web Gateway Services can be used to manage the categories of sites that should be bypassed for SSL intercept.

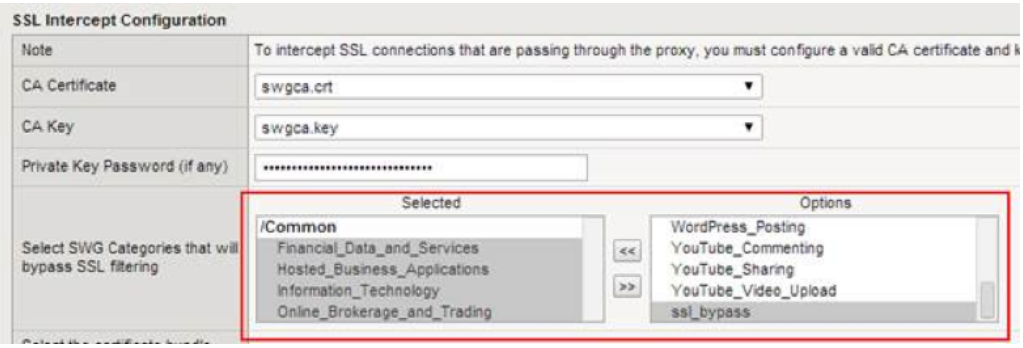

Figure 3: SSL bypass categories as managed with an iApps Template

Making safety a corporate policy

Modern browsers and search engines include filtering modes to prevent search results from displaying sites that are known malware hosts. Google refers to theirs as SafeSearch, and Microsoft calls theirs SmartScreen Filter.

When users fail to use these safe mode browsers, they can be exposed to malware and malicious URLs in their unfiltered search results. In addition, most search engines have gone to SSL only, making it difficult for web security to accommodate safe searches. Secure Web Gateway Services can detect and block links embedded inside these search results, effectively making safe searches a company-wide policy.

Delivering federated SSO

One of the most powerful features of Secure Web Gateway Services is federated SSO. The solution can be configured to interoperate with enterprise SSO tools (via SAML and other technologies) to

convert Internet access login into authenticated access to enterprise portals and Software as a Service (SaaS) applications. This delivers policy-based control and monitoring of which users may access what websites, when, and with what risks involved.

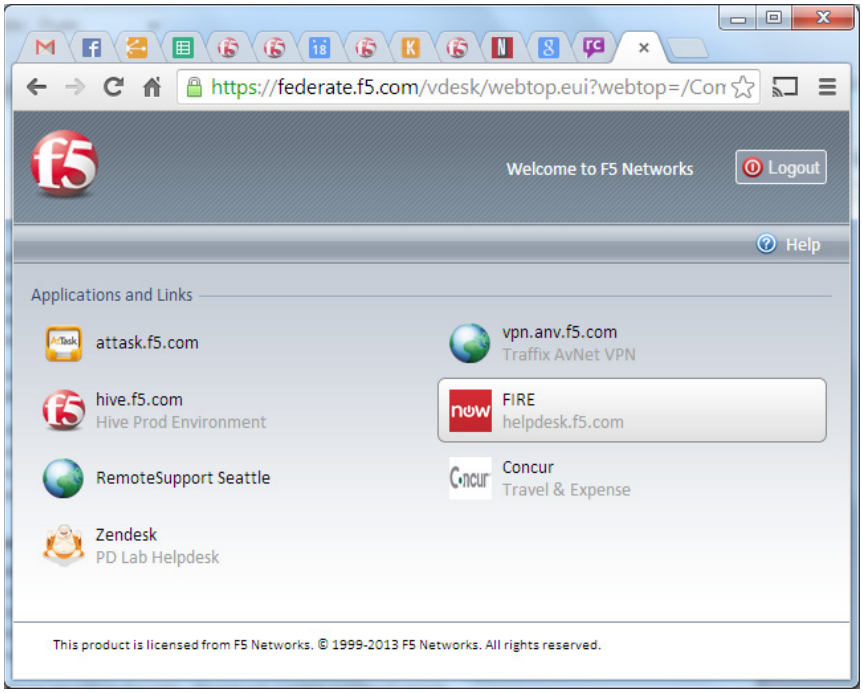

Figure 4: A sample daily login page with federated SSO

Imagine an organization with 20 integrated SaaS applications in the cloud. The federated SSO feature of Secure Web Gateway Services can automatically authenticate every user to each of the 20 services without requiring the users to re-enter their credentials. Of course this saves time, but much more importantly, it consolidates authentication to a single service to minimize password management.

Turn a captive portal into a daily federation page via the SAML IdP.

Some SAML identity providers (IdP) can use NTLM to log in transparently so users never have to enter their usernames and passwords. They simply see a quick browser redirection on their first access to the captive portal and would not have to enter usernames and passwords beyond logging into their desktops.

Endpoint inspection

The access policies of Secure Web Gateway Services allow client-side checks to collect and verify user system information. These client-side checks can be critical to ensuring that remote workers have equipped their PCs and laptops with anti-virus and anti-malware

services. This policy can be enforced to a specific security level before access to network resources is granted.

Bandwidth controls

Secure Web Gateway Services provides organizations the ability to change user behavior through bandwidth controls based on content type (such as streaming media), URL categories, applications, or protocols (such as FTP). Bandwidth limitation options are good for low-capacity links and for particular content types—bandwidth hogs—the organization wants to suppress to help change user behavior.

Bandwidth quotas (the cumulative bandwidth used in a given time) offer less real-time control but can achieve the same goal of dissuading use of bandwidth-hogging applications.

- **Limit viral videos without denying all entertainment.** Secure Web Gateway Services recognizes and categorizes thousands of websites as entertainment sites. Administrators can use this category to control not only access to those sites but how much access is allowed. For example, suppose that periodic access to a video website is necessary for an employee to do his job, but the organization does not want its employees watching the array of viral videos that normally propagate around an office every day.

  Secure Web Gateway Services can enforce this policy through the use of the Websense viral videos URL category. This often-updated category contains the list of currently popular videos, making it easy for an administrator to set the policy allowing only a certain amount of viewing per day. Operations that identify with this problem love the Secure Web Gateway Services solution for the level of control it provides.

- **Provide controls around Netflix.** Media streaming sites like Netflix are another type of entertainment site to which Secure Web Gateway Services can control access. Some organizations will want those types of sites blocked all the time for all users. Other groups may want those sites available only after hours, possibly for employees who have to be present, but not necessarily engaged. Such different policies can be enforced on a group-by-group level.

Guest Access Deployment Scenario

A more specific deployment scenario for Secure Web Gateway Services is acceptable use to provide guest access. When deployed in this way, the F5 solution secures access to the Internet specifically for guests, who may include visitors accessing a guest wireless network or a set of independent contractors on their own contractor network.

Secure Web Gateway Services may authenticate guest users, but most organizations merely require a guest user to accept terms and then rely on Secure Web Gateway Services to protect that user from malicious web sites or embedded malware.

Much of the work to secure and report guest access connections is the same as in the corporate deployment scenario. For wireless guests, however, restrictions may be looser (for example, without productivity locks), while the restrictions remain tighter for contractors.

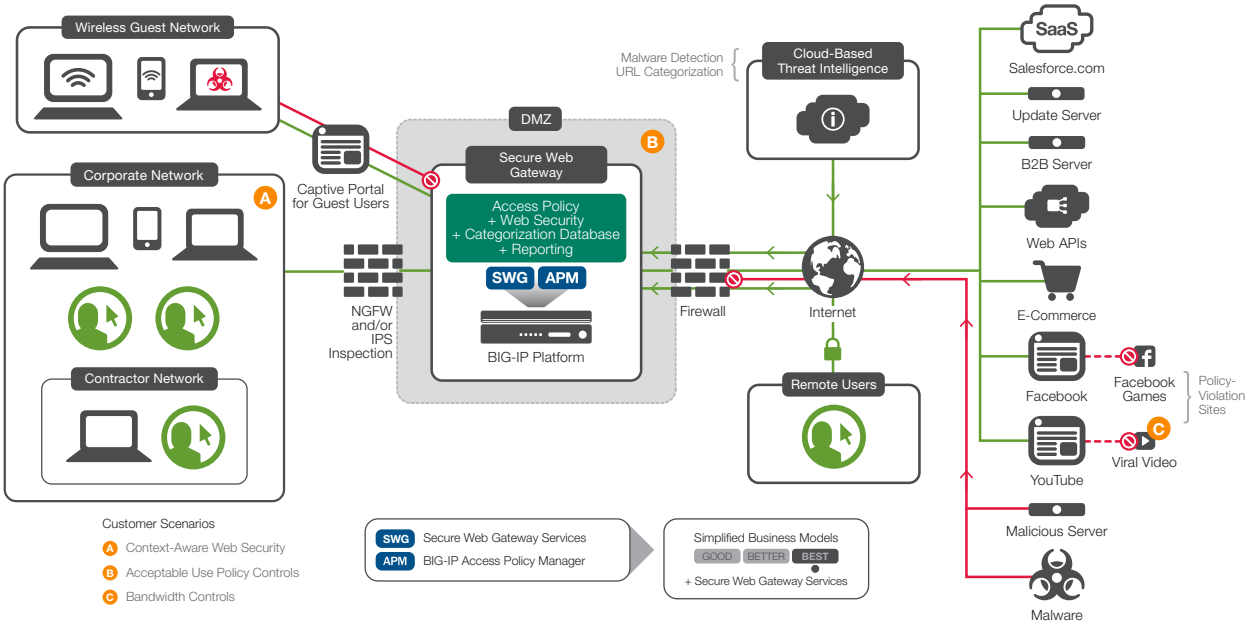

Figure 5: A guest access deployment with a captive portal

A typical Secure Web Gateway Services deployment for guest access involves enabling a common number of features, such as:

- Transparent proxy mode.
- A captive portal.
- URL filtering.
- Malware scanning.
- Reporting.

While all are important, the key distinctive feature in this model is the captive portal.

The captive portal

Any user who has logged into a guest wireless access point in a coffee shop or hotel is familiar with the concept of a captive portal. The captive portal is a page through which the user must traverse in order to log in to the network. Sometimes the captive portal will require credentials, such as a hotel room number for billing. In most cases, the captive portal will, at a minimum, require the user to accept terms of service.

By requiring the user to acknowledge the acceptable use policy, an organization can transfer some liability to that user. Typical use policies instruct the user not to spoof packets, attack other computers or networks, or sniff other user traffic. If the user does and litigation occurs as a result, the organization can say the user broke her promise not to do so.

PCI CDE DMZ Deployment Scenario

This scenario is a deployment of Secure Web Gateway Services for the purpose of maintaining compliance with PCI security guidelines. For example, Secure Web Gateway Services is commonly used to create a PCI DSS-compliant cardholder data environment (CDE). Section 1.3.7 of the PCI DSS standard requires that if any servers in the CDE make connections to the Internet, there must be a controlling forward proxy protecting those servers. Deploying Secure Web Gateway Services around a CDE provides this compliance while securing outbound connections and communications.

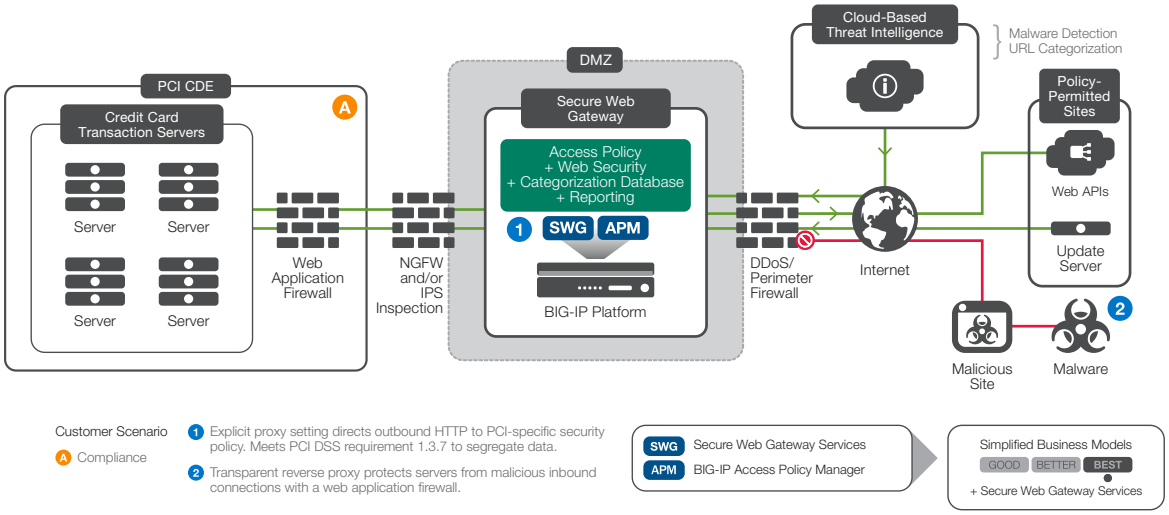

Figure 6: A PCI CDE deployment of the F5 solution

In these cases, the goal of the security administrator should be to proxy as much as possible, thereby reducing the threat surface. If the server inside the environment is eventually compromised, a malware-aware proxy can make it harder for the attacker to load attack tools onto that server.

A typical protected DMZ deployment of Secure Web Gateway Services involves enabling the base functionality plus the explicit or transparent proxy mode feature.

For maximum security in a PCI CDE DMZ, an administrator can create whitelists of sites by setting up a custom category.

Using the explicit proxy to protect DNS services

One of the security benefits of explicit proxies is that the proxy becomes the default name server for all external requests. This allows the administrator to detach the internal DNS server from having to serve external addresses, reducing the threat surface for name services. For example, imagine an attacker who has mapped the network from the outside and discovered the internal DNS name server intra.example.com. If this internal name server is detached from serving external addresses, the attacker cannot poison its cache.

When used in the explicit mode, Secure Web Gateway Services can be attached to an external DNS server. This can free the internal corporate DNS server from having to function as an external resolution source. In this case, the internal DNS server can be configured to not forward requests for external resources (because Secure Web Gateway Services is handling those). This reduces the threat surface, proofing the internal DNS against cache-poisoning, etc.

Query case randomization

Query case randomization is a technique that adds an additional layer of security to name queries by randomly changing the case of a name and then ensuring that the reply has the exact same case as the modified request. For example, if the user requests an address for www.example.com, a service such as Secure Web Gateway Services that performs query case randomization may change the query to wWw.EXamPle.com. When the response is processed, a check can be made to ensure that the case in the response matches. This prevents attackers from sneaking in address changes by blasting out fake responses for requests to popular sites such as Google Mail or financial institutions.

Customer Scenarios by Deployment Scenario

The three basic deployment scenarios support the four typical customer scenarios, providing configuration options that will best meet organizational goals.

Deployment Mode	Context-Aware Security	Bandwidth Control	Acceptable Use Policy Presentation	Compliance
Corporate	●	●	●	–
Guest Access	●	●	●	–
PCI CDE DMZ	–	–	–	●

Figure 7: How the deployment scenarios support various customer scenarios

Migration from Microsoft Forefront TMG

Many organizations are using the discontinuation of Microsoft Forefront Threat Management Gateway (TMG) as an opportunity to switch to F5 Secure Web Gateway Services.

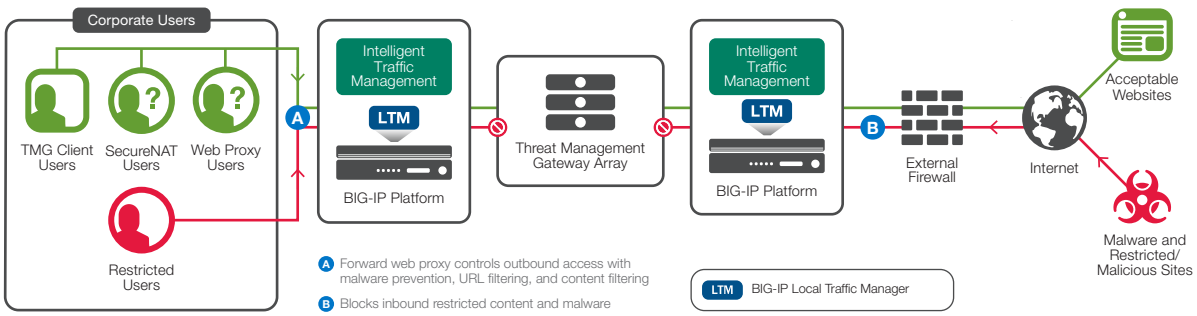

Figure 8: The position of the Microsoft TMG array within a typical corporate network

The F5 solution can be better than a drop-in replacement for TMG, since the forward proxy functionality can be enabled on the F5 BIG-IP® Local Traffic Manager™ (LTM) devices that were abutting the TMG. The forward-proxy security is consolidated into the BIG-IP platform, saving CapEx and OpEx and improving performance.

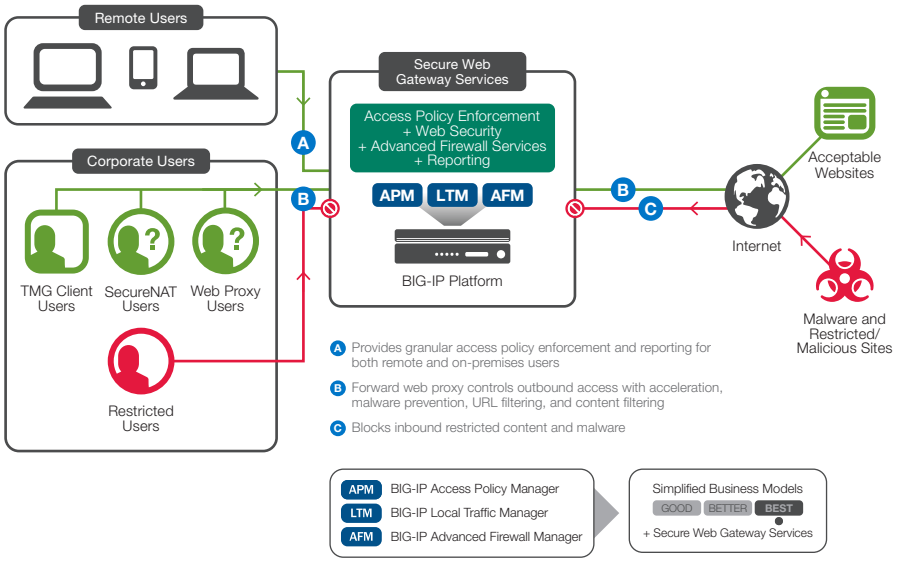

Figure 9: The network after a migration from TMG to Secure Web Gateway Services

Sizing the Solution Platform

Like all F5 solutions, Secure Web Gateway Services can be deployed on any platform in the F5 portfolio. A service engineer can help F5 customers determine if their current platforms are already sufficient for Secure Web Gateway Services.

Method	BIG-IP 2200	BIG-IP 5200	BIG-IP 10200
Explicit Filter, Scanning transactions/second	1,800	5,700	8,300
Explicit Filter Only transactions/second	9,800	37,000	45,000
Transparent Filter, Scanning transactions/second	1,700	5,600	8,300
Transparent Filter Only transactions/second	11,200	40,000	41,000

Figure 10: F5 platform scales

Licensing and Concurrent Users

Every F5 platform is assigned a concurrent session limit to ensure the best user experience. Web pages of different sizes affect the performance of Secure Web Gateway Services

differently. The optimal number of concurrent licensed users for popular F5 platforms ranges from 100 to 30,000.

F5 Platform	Secure Web Gateway Concurrent Connections
VIPRION 2400	30,000
10000 series	20,000
7000 series	15,000
5000 series	10,000
4000 series	5,000
2200	1,000
VE	100

Figure 11: Concurrent user licensing for popular F5 platforms, based on average page sizes of 16 KB

Conclusion

This reference architecture illustrates how F5 Secure Web Gateway Services can help the IT administrator in large enterprises, small to medium-sized businesses, and payment processing data centers.

- Organizations are using the F5 solution to secure the web for their internal users. The solution's URL categorization and filtering keeps users away from sites hosting malware and curbs unproductive Internet use. The granular deployment of security policies provides a tighter security envelope around in-house contractors.
- Small businesses are leveraging Secure Web Gateway Services to provide Internet access to visiting guests without taking on additional liability.
- Payment processing data centers use Secure Web Gateway Services to secure the scope of the payment servers by creating a PCI CDE DMZ.

The F5 Secure Web Gateway Services solution adds value by consolidating these services into a platform the organization already has deployed at the strategic point of control in the network.

But of course, in today's hostile environment, with targeted spear-phishing campaigns, drive-by downloads, watering hole attacks, and APTs, value cannot be the only story. A more robust security posture must be part of the solution. That's where SSL interception and malware scanning come in to complete the security picture, reduce the threat surface, and simplify the tasks of IT administrators.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.

WP-SEC-23060 0614