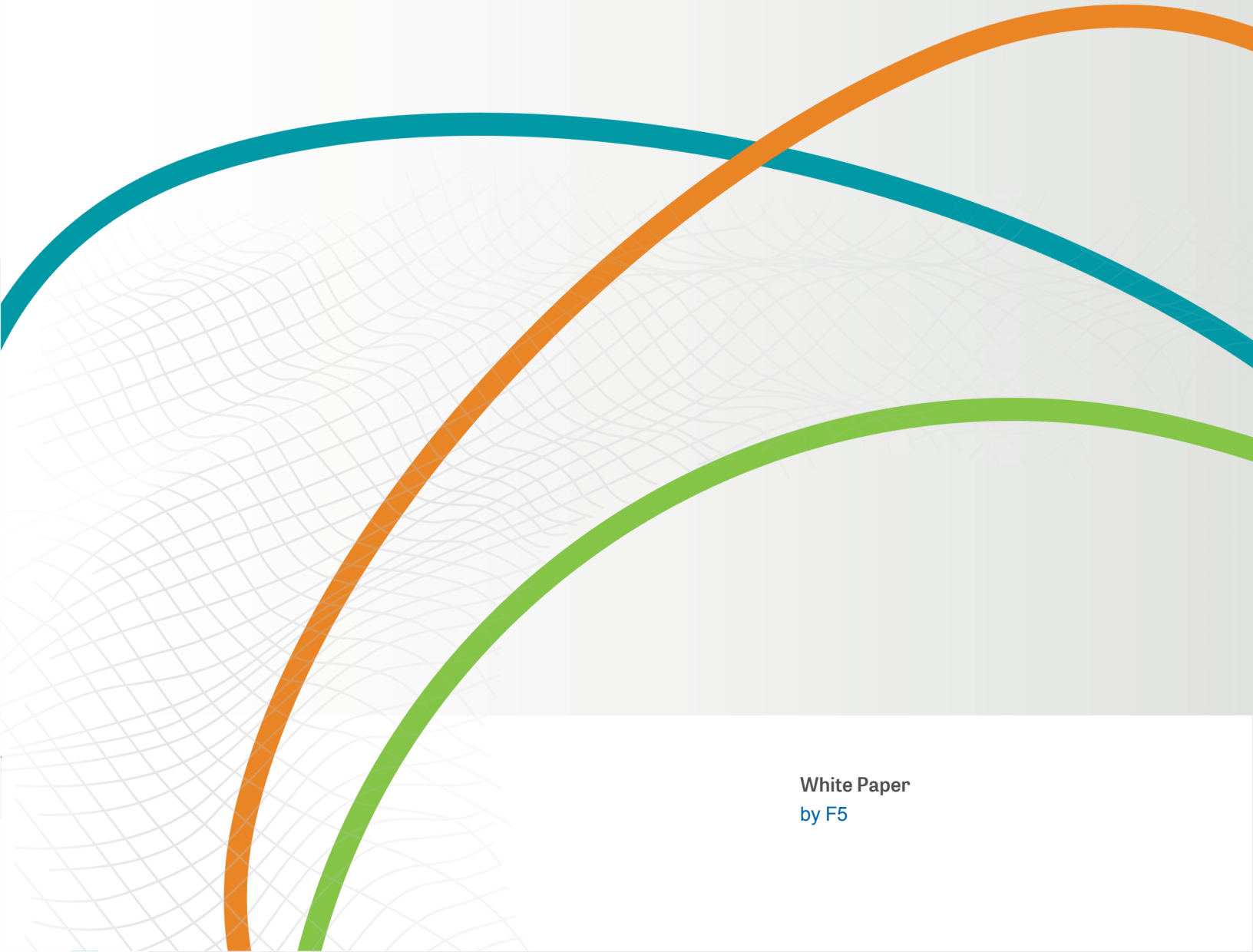
Filling the Threat Management Gateway Void with F5

With the discontinuation of Microsoft Forefront Threat Management Gateway, enterprises need to find a replacement. F5 Secure Web Gateway Services offer a superior solution to secure and manage corporate web access.



White Paper

by F5

Introduction

The recent discontinuation of Microsoft Forefront Threat Management Gateway (TMG) requires enterprises to find a new solution to secure corporate access to the web. In choosing a new solution, it's important for decision-makers to ensure that the solution they select includes the features and functionality necessary to ensure safe and appropriate web access.

Combining comprehensive features and functionality with superior scalability and performance, F5® Secure Web Gateway Services are uniquely positioned to provide the best alternative for TMG replacement.

Moving Forward

Moving beyond TMG, how will the enterprise provide its users with secure and controlled access to the Internet? Failure in outbound security—whether it's a direct financial impact from data loss or the liability or loss of employee productivity due to inappropriate use of the Internet—can be very costly to the enterprise.

In addition to using traditional and next-generation firewalls, many organizations have identified a need to use a web proxy, such as TMG, to deliver user access to Internet resources while protecting corporate assets. Figure 1 shows an example of this type of architecture.

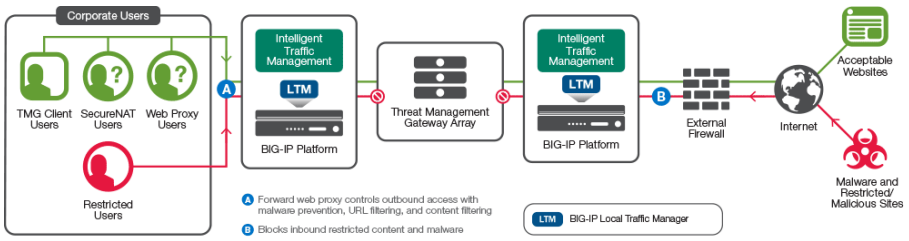


Figure 1: TMG web proxy array architecture

While there are various vendors and solutions available to the enterprise, IT decision-makers should ensure the solution they select contains the necessary feature set to ensure secure and managed access to Internet resources, including the four functions outlined below.

Forward web proxy

Providing a level of anonymity between corporate systems and resources on the Internet is a key requirement to providing secure web access. A solution should include a full forward proxy where outbound connections are terminated at the proxy and reestablished on behalf of the client. The client system (whether located on premises or remotely) should be obscured from the Internet resource.

URL/content filtering

To prevent malicious or inappropriate traffic from entering the corporate environment, a web proxy needs to have visibility into a given site/content and respond accordingly. This includes both encrypted (SSL) traffic as well as unencrypted.

User access control

Enterprises often need to control different users' access to Internet resources according to a number of factors such as position, work hours, and general business need. For a web proxy to provide real value to the enterprise, it must incorporate a variety of features and functionality that control access based upon users' attributes and behavior.

Auditing and compliance

Ensuring acceptable use policies are appropriately configured and adhered to is a critical function of both HR and IT departments. A web proxy solution must include the ability to monitor and report on end-user activity.

The F5 Solution: Secure Web Gateway Services

F5 Secure Web Gateway Services provide enterprises with a comprehensive, forward-proxy solution. As shown in Figure 2, the combination of F5 BIG-IP® Access Policy Manager™ (APM), BIG-IP® Local Traffic Manager™ (LTM), and BIG-IP® Advanced Firewall Manager™ (AFM) creates a solution that significantly streamlines web proxy deployments while providing enhanced functionality and security.

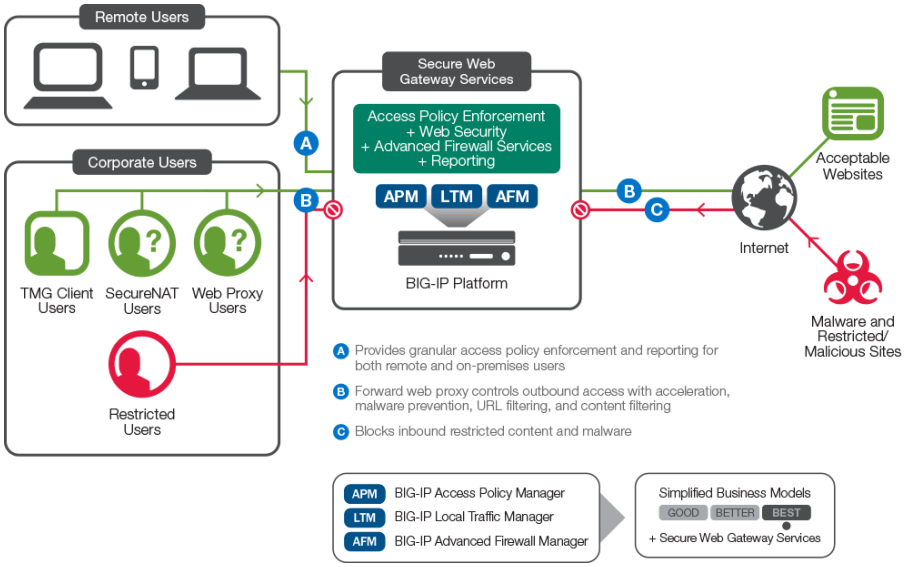


Figure 2: F5 Secure Web Gateway Services architecture.

Forward Web Proxy

Secure Web Gateway Services provide full, forward web proxy functionality, including the ability to evaluate and proxy encrypted, SSL-based traffic. The solution can be configured to secure web access for a variety of clients, both internal and remote.

With Secure Web Gateway Services, rather than a client connecting directly to a web resource outside of the enterprise, the client connects to and requests content (such as a web page or file) from the proxy server. The Secure Web Gateway Services proxy server then makes the request on behalf of the client. This obscures the internal clients and allows the proxy server to evaluate the request and/or response and apply various controls.

Many administrators face the challenge of how to proxy and secure SSL-based traffic while still ensuring the confidentiality of the end user's information. Secure Web Gateway Services address this by providing category-based proxy services. For example, an organization may want to intercept, analyze, and filter employees' SSL-encrypted, HTTPS traffic while excluding banking-related activities.

URL and Content Filtering

A critical function of a web proxy is to provide a central control point for web access, ensuring only acceptable and secure activity is allowed. User access controls along with URL filtering and content inspection deliver this control.

Secure Web Gateway Services block access to more malicious sites than any other solution. The threat intelligence behind Secure Web Gateway Services analyzes more than 5 billion web requests every day to produce a comprehensive categorization database of 40 million website URLs.

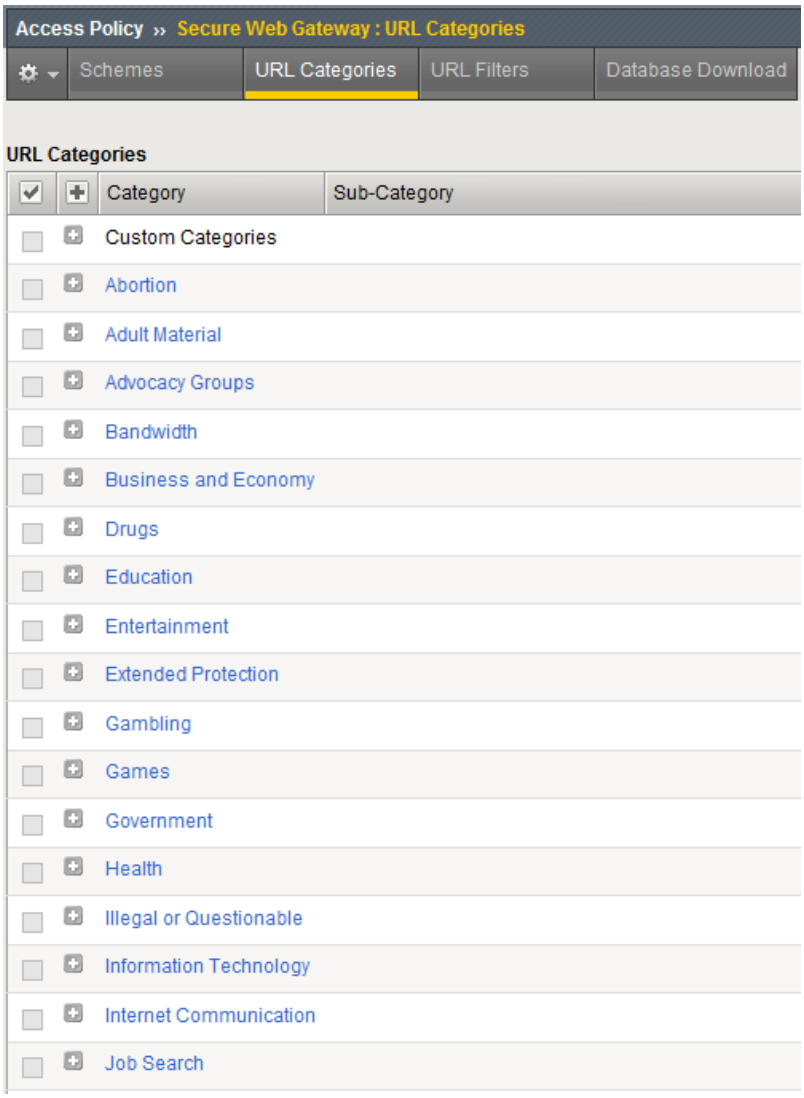


Figure 3: The solution includes predefined and customizable URL category filters.

User Access Control

Not all users are created equal. To effectively establish and enforce acceptable use policies, enterprises need to have the ability to evaluate a given user and apply controls appropriately based upon multiple factors such as group membership, authentication method, time of day, and so on.

Secure Web Gateway Services use the power of BIG-IP Access Policy Manager to give administrators the flexibility to evaluate and assign policy at an extremely granular level.

For example, an administrator might apply a specific set of URL filters to a particular user within a certain Active Directory group for a specific period of time.

With the increasing popularity of bring-your-own-device (BYOD) and mobile workforces, controlling web activity for both remote and on-site users is an administrative challenge that an effective proxy solution should address. Acting as a single point of control in the organization's perimeter network, the F5 solution can provide remote users with access to corporate assets as well as secure Internet web access.

Compliance

Ensuring acceptable and secure web access is more than just good business; more often than not, it's corporate policy—with the potential for very real consequences if not appropriately managed.

Secure Web Gateway Services provide IT administrators and HR professionals with the tools they need to ensure acceptable use policies are both effective and appropriate. The solution includes several dynamically generated and exportable reports that provide a clear picture of the enterprise's web activity. Additionally, the F5 solution can be integrated with many remote central logging systems.

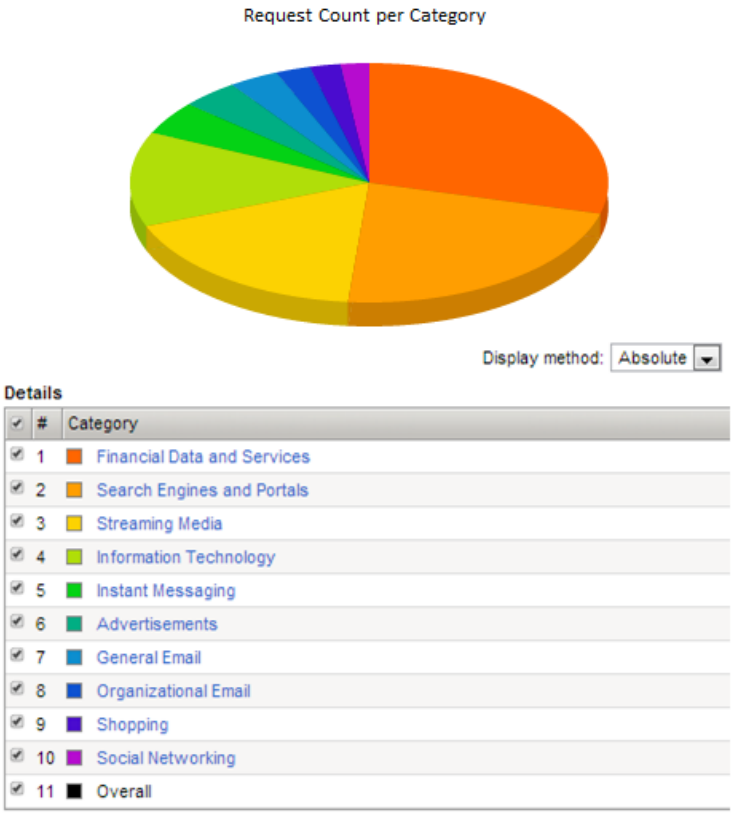


Figure 4: Granular activity reporting helps ensure compliance with corporate policies.

Conclusion

With the discontinuation of Microsoft Forefront Threat Management Gateway, organizations that have relied upon or have been considering using TMG to secure corporate access to the web are now faced with a challenge.

While there are many vendors and solutions to choose from, F5 Secure Web Gateway Services offer a superior alternative. The F5 solution combines granular access control, robust compliance reporting, and the most comprehensive categorization database to provide the single point of control enterprises need to ensure safe and appropriate web access.

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com