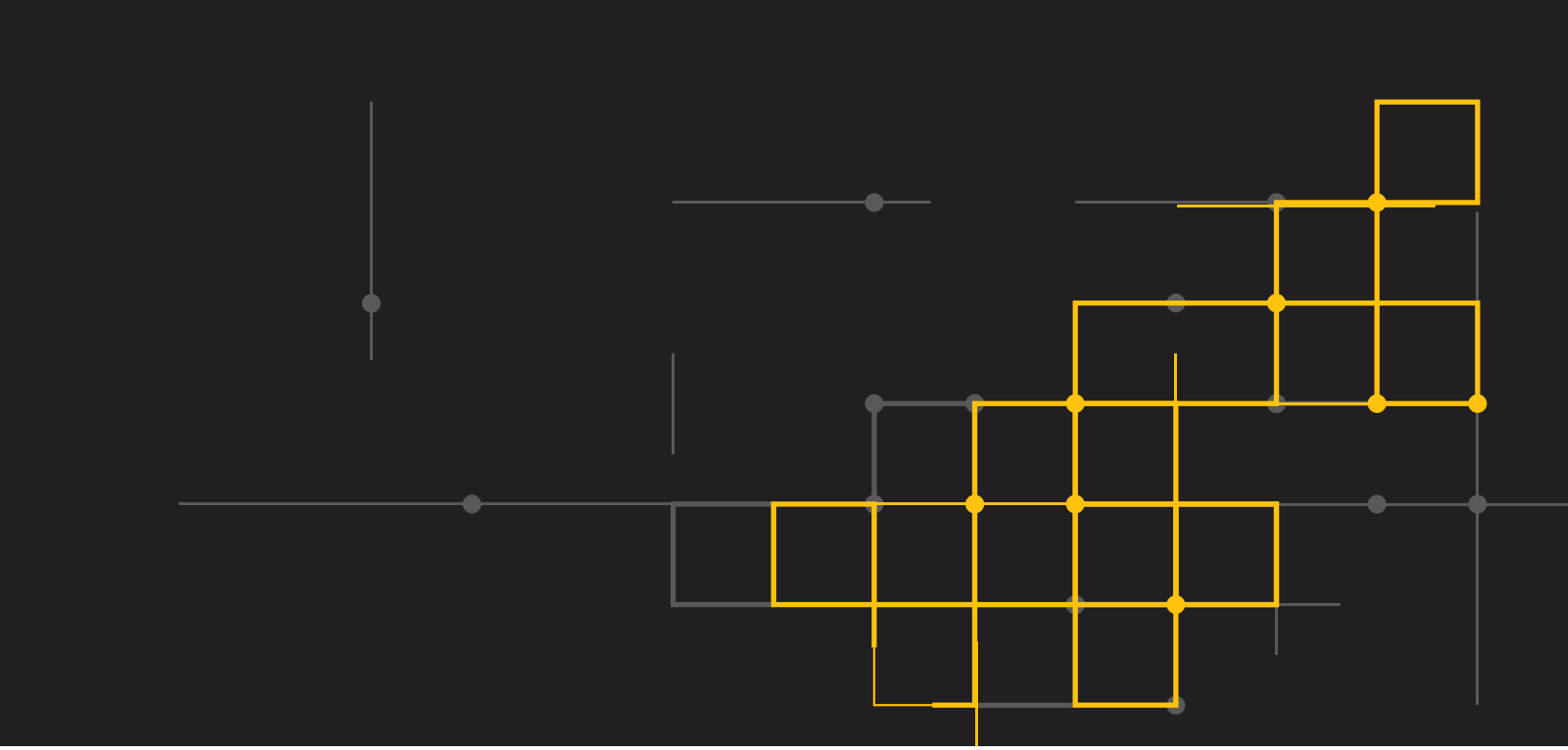

Next Generation Secure Web Gateway: The Cornerstone of Your Security Architecture

A closer look reveals why proxy-based secure web gateway architecture is uniquely effective in defending against web-based threats.

Symantec

The web is central to the way we work, live, and play – and therefore it is also a focal point for cybercrime. Organizations are targeted more than ever today, and the volume, diversity, and sophistication of web-based threats are at all-time highs.

Many enterprises have responded by re-examining their approach to web security, which is a positive development. Unfortunately, it has also led to some incorrect and counterproductive assumptions about current web security technology, particularly secure web gateways, also known as web proxy solutions.

A closer examination of web proxy architecture reveals that its role is more critical today than ever, and that it is in fact the only architecture that can provide full protection against today's web-based threats.

This paper provides a brief recap of the functionality provided by web proxies, why proxy architecture is still a vital building block for a comprehensive web defense, and how web proxies can work with other solutions such as next-gen firewall (NGFW) to deepen the organization's defenses against advanced web-based threats.

What Exactly Is a Web Proxy?

A web proxy is simply a server that handles traffic to and from websites. Typically, a user types in the address of a website he/she wishes to view, and the browser sends that request to the web proxy. The web proxy then examines the request and performs security-related tasks such as authentication and authorization, and if there are no issues it sends the request to the server hosting the page. It also examines the requested content for malware and other threats before sending it to the user's browser.

> Proxy architecture is the only architecture that delivers absolute protection against today's advanced web-based threats.

In essence, the web proxy provides a "quarantine" service for web traffic. It examines 100% of the traffic between users and HTTP/HTTPS sites, and categorizes all URLs so that malicious sites or pages can be identified and blocked while good URLs remain accessible according to policies.

For many in IT, the term "secure web gateway" (SWG) is interchangeable with web proxy. However, it's important to note that not all SWGs are proxies. When they were first introduced, SWGs were implemented to enforce corporate or organizational policy, such as preventing shopping on the web during office hours. In today's threat-laden world, the SWG needs to incorporate a web proxy to provide full defense against web-based cybercrime, malware, and phishing.

Why? Because by specifically mandating a proxy in the SWG, you have a guarantee that all traffic is terminated at the proxy. And when all web traffic terminates at the web proxy, the proxy has the ability to scan 100 percent of the content going through the proxy and wait for an analysis result before releasing that data to the user. The proxy can also perform authentication and ensure that no traffic flows through or tunnels through to the Internet without inspection or control.

What Does a Proxy-Based SWG Do that NGFW Doesn't?

Non-proxy SWG deployments and other technologies such as NGFWs (including TAP or SPAN port deployments), do not terminate traffic. With TAP or SPAN port devices, the gateway sits off to the side of the network, observing traffic as it passes by, instead of intercepting and terminating it.

NGFWs use stream-based detection methodologies, examining the traffic as it's streaming by on the wire. These deployments have a specific flaw. Malware or other threats can get through to the internal network if the gateway or NGFW doesn't detect the threat in time, or doesn't send out a TCP reset packet in time to disrupt the flow of traffic. In addition, because of the nature of stream based scanning, it is possible for malware to be delivered using fragmented packets over a period of time and remain undetected. A proxy by its nature would wait for an entire object to be assembled and scanned before allowing it to be delivered.

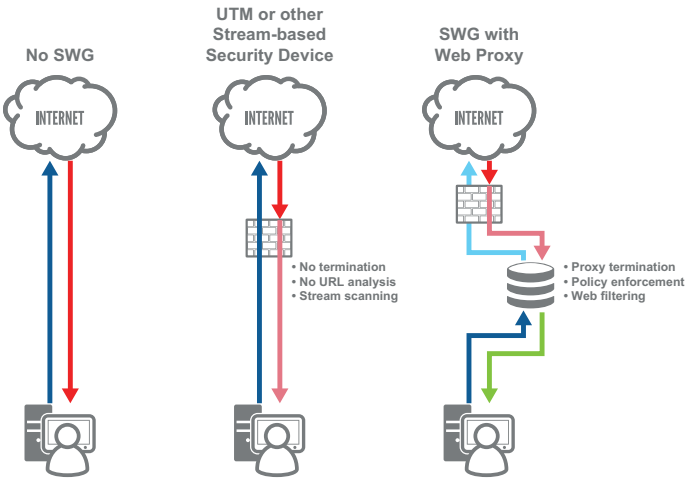

Figure 1 – Why a Proxy-based Secure Web Gateway is Different

Moreover, NGFWs are designed to allow traffic through the device in order to properly categorize the application, an approach that Network World said "could easily result in unintended consequences and insecure configurations – a valid concern" during its Clear Choice test.

Equally important, NGFW deployments do not effectively collect and analyze information about the URLs requested by users. NGFW solutions typical categorize only domains. Web proxy architectures, on the other hand, can categorize URLs, which allows for more granular policies that enable IT security teams and administrators to block only malicious content while providing access to the larger site.

To fully appreciate the advantage of this capability, imagine what happens if malicious content is found on a major site such as Microsoft or CNN. With typical NGFWs, the entire site needs to be blocked, whereas a web proxy solution such as the Blue Coat ProxySG can block the single URL while granting access to the rest of the site.

Complementing the capabilities of ProxySG is Global Intelligence Network, a part of the Symantec Global Intelligence Network that gathers intelligence on emerging threats from over 75 million users and more than 1 billion requests per day. This provides a level of visibility that is unmatched by any NGFW vendor. For example, Symantec's testing identified the top 125 malicious URLs and passed them through both the Symantec SWG and the leading NGFW. While Symantec flagged all the URLs, the NGFW had significant issues, including:

- **76 URLs were classified by the NGFW as "Unknown."** This means 61% of the bad sites would not even be classified by the NGFW technology.
- **Only 5 URLs were identified as malware**, meaning the other 95% could potentially get through.
- **There were several serious mis-classifications on the part of the NGFW**. Some sites were classified as Search Engine, or Personal Site, which are potentially malicious sites. These URLs would not be blocked by even the most diligent firewall admin.

The Global Intelligence Network also provides a real-time feedback loop in all of Symantec's products, offering the ability to update systems in real time as new threats are detected. For example, if a new threat is discovered by the Symantec Malware Analysis Appliance sandboxing solution, information about that malware is sent in real time to the Global Intelligence Network, and that information is shared with all other Symantec products, so they can immediately block the URL on which the threat is hosted.

A web proxy also offers some unique capabilities with regard to policy and manipulation of web pages. For example the ability to suppress, add, or rewrite headers are unique web proxy features available in web policy. Web proxies can also rewrite and redirect URLs as well as analyze and manipulate scripts on web pages.

The unique nature of the proxy can also be used to enforce protocol compliance. A proxy operates on the application layer with two separate connections (one on each side of the conversation), providing the ability to verify compliance to protocol standards, and preventing traffic that is not compliant (or correcting and fixing non-compliant traffic). For example, the streaming proxy can completely stop a buffer overflow attack, using protocol compliance enforcement.

This same feature also provides the ability to translate protocols from one side of the conversation to the other. For example, if a client is only capable of IPv4, the proxy can be used to proxy a conversation to an IPv6 web server, enabling access even without IPv6 support on the client side. Likewise an IPv6 only client or environment can access an IPv4 web server through a web proxy.

In short, the NGFW is not a guaranteed security mechanism. It may work well for enforcing organizational policy, but it's definitely not a safeguard against web-borne threats that may overwhelm the capability of the device by overloading it, causing it to react slowly and rendering it unable to block threats.

What Does NGFW Do that SWG Doesn't?

Does all of the discussion from the previous section mean you should use web proxies in place of an NGFW? Not at all.

The NGFW is good at certain things the web proxy is not built for, such as providing protection for applications and protocols beyond the standard web-based protocols, and examining packet-based threats. IT leaders in your organization need to decide whether you need those particular protections; and if so, the NGFW may be an excellent addition to your layered defenses.

However, there's no doubt that most threats enter the organization through the web today, and protecting the organization with the best-of-breed web security should be the priority. Web proxies in the SWG solution should be the fundamental building block of a sound security solution.

Misconceptions about Web Proxy

The most common apprehension about secure web gateways is that they're inherently slow – that they were not designed to handle the enormous volume of web traffic on today's enterprise networks.

The truth is that a SWG with proxy architectures can accommodate massive volumes of web traffic without delays or latency. Symantec's ProxySG provides an excellent example. Utilizing patented web caching techniques along with protocol optimizations and the fastest rating technologies, ProxySG appliances often provide better web performance than the client had experienced without a proxy architecture.

Ironically, the performance numbers posted for NGFW solutions can actually be quite misleading. NGFW performance numbers tend to be function-specific. While it is common for NGFW vendors to specify the throughput for firewall, threat protection, and VPN functionalities separately, these are individual, best-case numbers. Consequently, these numbers would certainly decrease once the user activates firewall and threat protection in parallel, for example. It is important to distinguish this from the actual performance of the appliance in a real-world environment, as overall performance is generally a key selling point of NGFW solutions.

In addition, if you're concerned about being able to incorporate next-generation security features and the latest security technologies, there's no worry with Symantec since Symantec integrates with most best-of-breed security technologies in the industry. By using industry-standard interfaces such as ICAP, Symantec offers a truly secure control point for integrating important new security technologies such as whitelisting, sandboxing, static code analysis, and the latest developments in anti-malware, DLP, and other technologies.

Conclusion

Today, the only way to ensure full protection against web threats is to intercept all web bound traffic using a proxy-based secure web gateway architecture. Protecting your mission-critical network from inbound threats should be a top priority, and your SWG should use proxy architecture to process all web-bound traffic.

Utilizing a secure web gateway solution such as ProxySG gives you the ability to inspect all traffic, and set policies to block threats that are both well known and detected in real-time. The proxy architecture provided by Symantec also offers the high performance needed for complete inspection and malware scanning of all web traffic.

Perhaps even more important, using proxy architecture to defend against web-borne threats gives you the ability to start seeing security in a whole new light – not simply as a line of defense against the unthinkable, but also as a source of empowerment for your business. Because when you can stop worrying about potential threats, you can start focusing on new possibilities.

About Symantec

Symantec Corporation World Headquarters

350 Ellis Street Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

SYMC_wp_Next-Gen_Secure_Web_Gateway_EN_v1a