Editorial Brief

Eight Things to Know About a Secure Web Gateway

by Tim Chiu
Senior Director, Product Marketing, Symantec

Given the evolving way Web and Cloud applications are used—and the constantly shifting threat landscape organizations must confront—proxy architecture is more important than ever in terms of securing Internet access. It's imperative to have effective compliance and company policy enforcement, and the use of a secure web gateway with advanced functionality is a key piece of an enterprise's security architecture.

While the capabilities of secure web gateways have grown over the years in response to new requirements and threats, the original justification for pairing a proxy with a secure web gateway appliance remains the same: Ease of use and management; a hardened operating system for security; performance-tuned applications; turnkey deployment and easy scalability.

Not only do all of these attributes keep operational costs down, by terminating traffic at the proxy organizations are guaranteed the highest level of security. All content is scanned for risks and threats, including malware and potential data loss.

To better illustrate their capabilities—and to help you identify the solution that best suits your needs—let's review eight things organizations need to know about secure web gateways.

1 Proxy technology – it's unique role in enterprise security

Proxy technology isn't the exciting new kid on the block – it's entrenched and established. Yet that's for good reason: In the networking and security space, nothing is as secure as proxy technology. As the secure web gateway has evolved, proxy has remained a constant feature and the most critical element ensuring the security of the web-browsing experience. Web threats are at an all-time high, so it's hardly surprising so many organizations rely on secure web gateways for protection and performance to complement and strengthen their security architecture.

It's important to recognize, however, that not all secure web gateways are proxies. By specifically mandating a proxy in the secure web gateway, you can be sure that all traffic will be terminated at the proxy. Alternative secure web gateway deployments (such as TAP), have the gateway sitting off to the side and observing traffic as it passes, rather than intercepting and terminating this traffic. While this might be fine for enforcing policy on low usage networks, it's not an effective safety net vs. web-based threats, especially in high usage, high activity networks.

Other options, such as Next Generation Firewalls and Unified Threat Management devices, employ stream-based scanning to protect against threats. Stream-based scanning, however, does not terminate traffic as a proxy does, and has limited time to inspect packets flowing through the system. Evasive techniques (such as delaying or obfuscating packets) can defeat this approach, making proxy the only solution offering full inspection and the highest security possible.

Symantec™

This means a secure web gateway with proxy architecture remains the best available solution for security-conscious organizations.

2 Why powerful cloud-based application controls are key

The move toward cloud-based apps over the last 10 to 15 years has been a boon for productivity for some organizations. Yet this development has also posed security risks. Secure web gateways have subsequently evolved to address this need for cloud application controls. It's no longer enough to block or allow specific applications; a more fine-grained ability to control and block individual operations within these applications (whether by user, group or an entire organization) is a requirement. For example: An organization may wish to make Facebook read-only for everyone except the marketing department or social media manager, who has a need to promote the company on Facebook. Modern secure web gateways incorporate Cloud Access security Broker (CASB) capabilities that give organizations the ability to discover what cloud applications are being used by their end-users, evaluate cloud application compliance and security risks, and enforce cloud application access control policies to meet corporate, compliance and regulatory requirements.

One thing is certain: Cloud applications will continue to evolve. The right secure web gateway features flexible and powerful controls that can be easily updated to keep pace with continuing changes.

3 Dealing with mobile devices and remote users

The mobile explosion over the last few years has led to considerable growth in the number of devices a secure web gateway must handle, thereby increasing bandwidth and scalability requirements, along with an increase in supported browsers and protocols. Mobile versions of popular websites and applications typically use different URLs, commands and operations to achieve the same functionality. This increase created a need for more refined cloud-based application control technology and URL categorization, in order to recognize and secure different versions of the same application.

This isn't the only change mobile has introduced. Users accessing cellular networks and public Wi-Fi has created a need for additional security. Specifically, a solution that protects the device regardless of the network – making hybrid cloud solutions a vital deployment methodology for secure web gateways. Unlike Mobile Device Management solutions which offer only physical device protection, a full-featured cloud-based or hybrid secure web gateway provides a comprehensive answer to the web access problem.

Cloud-based secure web gateways are also an ideal solution for organizations with distributed workforces located in remote offices. A cloud gateway can enforce consistent web and cloud application security policies with traffic going "direct-to-net" versus being back-hauled to headquarter or corporate data centers for policy enforcement.

4 Why encryption in the network is a double-edged sword

Websites using SSL and requiring SSL-encrypted connections are on a serious growth trajectory (the busiest sites saw a 40-percent year-over-year increase in SSL use, according to a recent Netcraft survey). Expect this trend to continue after Google's announcement that SSL use will enhance a company's website rankings.

For organizations, this is a double-edged sword: Ostensibly, it means greater security, but in practice bad actors can hide under this same cloak of invisibility, as encrypted traffic is generally not inspected for malware, data leakage and other threats, due to the limitation of many security products. Secure web gateways with an SSL proxy, however, provide the ability to intercept and decrypt SSL traffic to evaluate it for possible threats, and even feed decrypted content to other security devices, such as data loss prevention (DLP) or advanced threat prevention (ATP) solutions, for inspection or logging.

This process can be resource intensive. The most advanced secure web gateways mitigate this by using hardware-assisted decryption, allowing for a combination of top-level security and performance.

5 How to achieve better user experience through bandwidth usage reduction

Over the years the Web has seen greatly increased use while becoming much more dynamic. Where pages once were static, they now change based on who is viewing the page or the location from which the page is viewed. The adoption of video as the web's preferred content form has also created bandwidth issues (video alone is expected to comprise 90-percent of all bandwidth in the near future).

While technological and infrastructure improvements have mitigated bandwidth pressures somewhat, it remains an important issue in the context of user experience. Secure web gateways with the technological ability to lessen the impact of bandwidth pressure are key in improving user experience. For example, video caching and live stream-splitting allows video content to be streamed or downloaded in a single instance to a secure web gateway, saving bandwidth when multiple users request the same content, a common event with the viral nature of popular web content. The secure web gateway sends cached video (or stream-splits the original video) to all requesters after the initial request is downloaded and delivered.

Additionally, the best secure web gateways have the capability to deal with the common characteristics that make simple web page caching difficult (pages marked non-cacheable even if the data is unlikely to change, for example). Better bandwidth caching rates equals better response times – and minimizes the need for organizations to keep upsizing WAN pipes.

6 The value of authentication and usage reporting

While it's common for today's organizations to use secure web gateways as a control point for access (while depending on proxy architecture for security), they've become important integration points for identity and policy. The need for granular reporting on user activity has enhanced the importance of identity, in terms of both compliance and management.

User authentication and identification enables usage reporting, giving administrators the ability to quickly identify users that may have been infected following an attack. If a specific site is responsible for the intrusion, it can be quickly determined if anyone else visited the same site and could be facing the same exposure.

Additionally, authentication and user identification is a necessary feature of policy development and enforcement. In its absence, organizations would be consigned to developing policy applicable to the entire enterprise, or based strictly on easily spoofable IP addresses. Authentication, on the other hand, allows users to have specific policies related to job function. An example: HR staff may be able to access recruiting websites, while sales staff can utilize sites such as Salesforce.com.

The bottom line: An advanced secure web gateway should offer authorization and identification capabilities deep enough to effectively enforce policies and identify threats.

7 Tapping global intelligence to meet a landscape filled with increased threats

The security threat landscape has shifted over the years from one where email threats were paramount to one where web threats are public enemy number one. Early web defenses focused on identifying bad sites and sorting them into specific categories. Category rating developed into cloud-based real-time rating, as the volume of sites and content that required categorization spiked dramatically (currently, it's estimated 71-percent of the web changes every 24 hours).

Malware scanning, too, has evolved over the years, with the most comprehensive solutions offering two layers of defense: One scanner at the gateway and one at the endpoint solution. Eventually, the option to run files through two separate anti-malware engines and an endpoint solution became available. Features such as file white-listing (which reduced system load by recognizing well-known files such as an iOS update) and static code analysis were also eventually added to the capability of a secure web gateway.

Today, the most advanced secure web gateway serves as an integrated solution, offering full security functionality without compromising on performance. Ideally, this solution is predicated on a real-time rating system that utilizes a global intelligence network, which draws from real-time Internet activity from both networks and endpoint devices, including billions of web requests and emails daily.

8 Why an open-partner ecosystem is so valuable

While it might be nice in theory for a single company to develop all the web security solution components every individual organization requires, in reality that's just not feasible. That's why the best secure web gateway solutions offer an open partner ecosystem, allowing for adjacent technologies to be seamlessly integrated.

Having a flexible and open partner ecosystem makes a secure web gateway a highly flexible solution in its own right – capable of integration with the best technologies available, including authentication vendors, advanced threat vendors, data loss prevention vendors, logging vendors, mobile device management solutions and additional malware scanning.

The Takeaway

Secure web gateways have evolved well beyond their original mandate in order to meet the needs of moder organizations. Today's most advanced solutions offer a full-range of capabilities, including:

- Flexible and powerful cloud application controls
- The ability to handle SSL encryption efficiently and effectively
- The strongest available proxy-based security
- The capability to improve user experience by reducing bandwidth usage
- A flexible open-partner ecosystem
- Real time rating backed by a global intelligence network
- Strong authentication and identification functionality
- Enhanced security for mobile devices, and users in any location
- The ability to orchestrate content to solutions like data loss prevention and advanced threat protection

By employing a secure web gateway with these functions, organizations will reap the rewards of greater security, lower costs and higher efficiency.

Timothy Chiu is a Senior Director of Product Marketing for Symantec (through the acquisition of Blue Coat).

At Blue Coat, Tim has worked in Technical and Product Marketing roles, including managing a team of Product Marketing Managers and Technical Marketing engineers, launching new hardware and software products, and driven the establishment and nurturing of a Technical Advisory Board.

Prior to joining Blue Coat Tim worked at Mirapoint for almost 9 years and was instrumental in driving Mirapoint product direction and sales in his roles as Director of Technical Marketing, Manager of Systems Engineering, Senior Product Manager, and as Director of WW Application Engineering.

Tim holds a master's degree in product management from Santa Clara University, a bachelor's degree in electrical engineering from the University of Pennsylvania, and a bachelor's in economics from the Wharton School of Business. Tim is an alumnus of the Jerome Fisher Program in Management and Technology from the University of Pennsylvania. In his free time, Tim has been an instructor in Unix Administration for UC Berkeley Extension from 1999 to 2005.

About Symantec

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.

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