WHITE PAPER

The Cloud-Enabled Secure Web Gateway

How Advanced Secure Web Gateways Play a Critical Security Role in a Cloud-Centric World

TABLE OF CONTENTS

What Role Can Secure Web Gateways Play in a Cloud-Centric World?

IT security professionals have long recognized that a secure web gateway (SWG) plays a critical role protecting an enterprise, its employees, and its customers from web-borne threats. However, some individuals have the mistaken idea that SWGs are old technology that has not progressed beyond basic proxy functionality such as routing user requests to URLs and web filtering. Others are under the impression that once an organization starts moving applications to cloud platforms it can rely solely on security products running in the cloud. In reality, today's leading-edge SWGs provide the following capabilites:

- Incorporate in one package a wide range of advanced technologies for threat detection, data loss prevention, network optimization, and compliance policy enforcement
- Fully leverage cloud resources such as curated security policies, threat intelligence, and cloud-based sandboxes for malware detection and analysis

For enterprises with applications on both on-premises data centers and public cloud platforms, SWGs also enable much stronger security and better application performance than cloud-based security products alone can provide. This white paper will examine how secure web gateways have evolved and why they have a critical role to play in today's cloud-enabled world.

The Remarkable Evolution of SWGs

The Early Days

Early SWGs were hardware appliances deployed in corporate data centers to protect employees and other computer users from web-based threats. They served as web proxies, receiving requests from users' browsers to connect to a web page, authenticating the users, and connecting the user to the servers hosting the web pages. They also enhanced the performance of web applications through caching (storing and reusing repeatedly-viewed web content such as HTML pages, images, and video streams), compression, and protocol optimization.

A SURVEY OF ORGANIZATIONS WITH AT LEAST 500 EMPLOYEES FOUND THAT 62% HAD INSTALLED AN SWG

SWGs also filtered requests by blocking user access to websites that were known to be malicious, that violated corporate acceptable use policies (sites with pornography or hate speech), and that violated policies about using corporate resources during working hours for non-work activities, such as shopping, streaming movies, and playing online games.

Finally, the early SWGs logged and reported on how users connected to websites. Administrators could monitor and analyze employee interaction with websites to identify trends, troubleshoot network problems, and react faster to attacks.

Vastly Expanded Security

As the name implies, SWGs act as gateways between web users and the Internet: a single point where all web traffic can be monitored and corporate policies for web use can be enforced. This strategic position makes SWGs a natural place to build in additional network security technologies that defend against a very wide range of cyber crimes, malware, and phishing. Additional capabilities in today's SWGs may include the following:

- **Strong user authentication** using a wide variety of identity sources, including NTLM, LDAP, RADIUS, one-time passwords, and certificates
- **High-speed decryption and re-encryption** of SSL/TLS traffic, so attackers can not use encryption to conceal malware or command and control traffic into and out of the corporate network
- **Malware detection** using multiple anti-malware engines and detection methods
- **Multi-layered deep content inspection and analysis** to detect spam and application-level threats in the payloads of network traffic
- **Data Loss Prevention (DLP)** to identify confidential information and block it from leaving the corporate network
- **Cloud Access Security Broker (CASB)** features to monitor and control what applications users can access and how documents and files are sent to the cloud
- **Web (browser) isolation** to create a safe browsing experience, prevent malware from moving from browsers onto employees' systems, and block sharing of credentials on suspicious websites
- **Policy enforcement** with many types of policies and more granularity, including policies related to security, acceptable web use, encryption, and compliance

The current generation of SWGs offers security features that can not be found in next-generation firewalls (NGFWs) and other security solutions that do not include a proxy. These features include assembling and scanning entire objects before delivering any part of them to users, collecting and analyzing information about individual URLs (rather than websites that might contain many URLs with completely different risk levels), and the ability to rewrite and redirect URLs and analyze and manipulate scripts on web pages.

SWGS HAVE EVOLVED TO PROVIDE MORE VALUE IN A CLOUD-CENTRIC WORLD

Highly Scalable Hardware

SWG appliances have grown enormously in efficiency, reliability, and power. Key features added over the years include custom operating systems designed for processing security data, specialized chips for decrypting SSL/TLS traffic, redundant components, and automatic power supply failover. The newest generation of SWG appliances scales to accommodate the largest organizations and includes feature innovations such as remote browser isolation, cloud application visibility and control, deep file inspection for malware, DLP, and much more. For information on the latest Symantec® SWG features, see the SWG Appliance Product Brief.

SWGs in a Cloud-Centric World

Besides adding security features and scalable hardware options, SWGs have evolved to provide more value in a cloud-centric world. Major enhancements have included:

- SWGs as a cloud service
- Fully leveraging cloud resources
- Integration into cloud-based security suites

SWGs as a Cloud Service

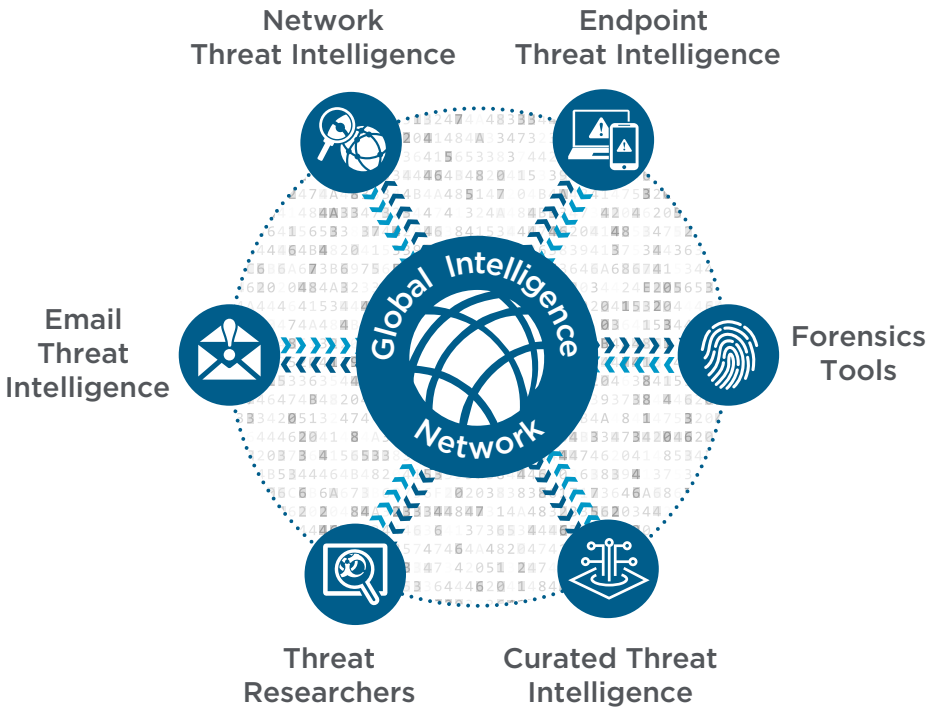
Advanced secure web gateways can now be deployed in data centers, in private clouds (running in virtual machines managed by the enterprise), and in public clouds hosted by third party providers. They run on physical servers and on virtualization platforms such as VMWare, Microsoft Hyper-V, and Amazon Web Services (AWS). SWG virtual appliances enable enterprises to offer SWG as a Service to remote offices and employees working at home and on the road, with the full range of security and network optimization features.

IT teams can deploy the form factor that best fits the location, scale, and economics of each work environment, while enforcing security and compliance policies consistently across all sites and benefiting from centralized visibility, reporting, and management.

Now SWGs of all types can leverage cloud resources to acquire up-to-the-minute threat intelligence and to handle specialized forms of analysis. For instance, the Symantec Global Intelligence Network monitors more than 175 million endpoints and SWGs and proxies protecting 80 million users. It uses artificial intelligence to analyze over 3.7 billion lines of telemetry to identify and categorize emerging threats and suspicious and malicious URLs and websites. Key data is continually forwarded to hardware and virtual SWGs in data centers and in cloud deployments and to hosted SaaS platforms.

COMPREHENSIVE, UP-TO-DATE THREAT INTELLIGENCE DRAMATICALLY INCREASES THE EFFECTIVENESS OF TODAY'S ADVANCED SWGS

Figure 1: Symantec Global Intelligence Network



SWGs can take advantage of threat data feeds and crowdsourced threat information available on the web. Comprehensive, up-to-date threat intelligence dramatically increases the effectiveness of today's advanced SWGs. Some SWG vendors provide curated policy services. Rather than having to create all policies from scratch, organizations can choose from a selection of recommended, strong, and maximum policies crafted by security experts. This not only saves time, it puts policy management in the hands of security experts and reduces the risk of errors and unintended consequences from imperfectly designed policies.

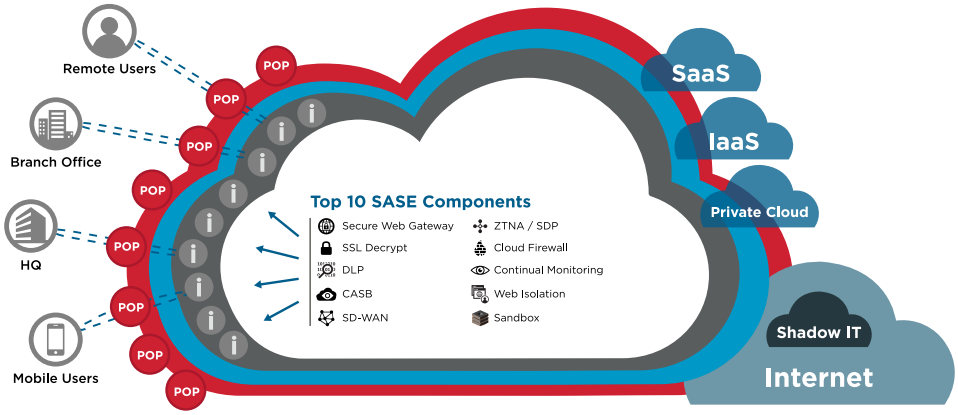
SWGs can also leverage cloud services for tasks like malware detection and analysis. For example, when an SWG encounters an unknown file as an email attachment or a web download, it can send the file to a cloud-based service that uses multiple antimalware engines to test it. If those tests are inconclusive, the file can be executed and monitored in an isolated sandbox on the cloud to see if it performs malicious actions. These cloud services offload specialized, processing-intensive tasks from the SWG and return a verdict that allows the SWG to take actions like terminating the session, quarantining the file, or sending it through to the user. The time needed for this additional testing and analysis usually is imperceptible to the employee being protected.

SWG technology can provide the core of a comprehensive cloud-delivered network security service. An example of this is Symantec Web Protection, which offers protection against advanced threats, controls access between employees and websites, and helps IT teams implement zero-trust security and a Secure Access Service Edge (SASE) architecture.

The technologies integrated into Symantec Cloud SWG include:

- **A proxy-based SWG,** including advanced authentication and proper handling of SSL/TLS decryption, built upon Symantec industry-leading technology in those areas.
- **A cloud firewall service,** based on advanced NGFW technology that performs deep inspection on network traffic over all ports and protocols and applies access policies based on applications, user groups, and other factors.
- **A CASB** that monitors and controls access to and use of cloud applications and helps administrators detect and block access to shadow IT and other unauthorized applications.
- **Web and email isolation** that executes and renders web pages and emails in a cloud-based isolation chamber so ransomware and malware can not be installed or executed on employee endpoints, and so users can not submit corporate credentials and other sensitive information on suspicious websites.
- **DLP** that analyzes outbound web, application, and email traffic to prevent sensitive content from leaving your network.
- **Content and malware analysis with sandboxing,** to identify known and unknown malware and block zero-day attacks.

Figure 2: SASE Framework



SWGs During the Long Era of Hybrid Architectures

Most enterprises today are transitioning computing workloads to the cloud to take advantage of the flexibility of SaaS applications, the scalability of cloud platforms, and the opportunity to let a service provider install and manage computing resources.

THE VOLUME OF ENCRYPTED TRAFFIC HAS BEEN GROWING RAPIDLY, FROM HALF OF WEB TRAFFIC AT THE BEGINNING OF 2014 TO ABOUT 95% IN 2024

But for many organizations, these transitions are going to take years to complete fully. Only a certain percentage of applications and services can be moved or replaced each year. In many cases it is simply not worth the expense and effort to move software that is performing well in the data center. Finally, many organizations must store and process data on their own premises to meet security and privacy regulations and to retain the confidence of their customers.

Consequently, we have entered the long era of hybrid architectures where some applications run in corporate data centers and others on public cloud platforms. The two sets of applications need to coexist, to interact, and to be managed (and protected) by the same IT and security teams.

SWGs give enterprises the flexibility to deploy critical security solutions in the form factor that is best for each location and use case in a blended environment (on-premises, virtual, cloud, and SaaS).

SWG Appliances for Data Centers and Large Offices

The most recent generation of SWG hardware appliances are incredibly reliable and scale up to support large data centers and offices with tens of thousands of employees. They also offer the best performance and price-performance for large offices, because most of the routing and enforcement actions are performed in the same location as the users, applications, and data. SWG virtual appliances can also be deployed in data centers when that is appropriate.

Decryption at Scale

Another essential reason to deploy a properly-sized hardware appliance in large offices is the need to ensure that all web traffic in both directions is decrypted and scanned. This is very important, because the volume of encrypted traffic has been growing rapidly, from half of web traffic at the beginning of 2014 to about 95% at the end of 2020 (Google Transparency Report). Decryption can consume a tremendous amount of processing power. Some cloud-only web security solutions can not handle decryption on a large scale. This forces administrators to choose between letting encrypted traffic go through (creating unacceptable security risks) or blocking the traffic that cannot be decrypted (creating serious user satisfaction issues).

TODAY'S SWGS ENABLE IT ORGANIZATIONS TO CONTROL THE PACE OF THEIR TRANSITION TO THE CLOUD WITHOUT MULTIPLYING TOOLS OR SACRIFICING SECURITY

Virtual Appliances to Protect Remote Offices

SWG virtual appliances are an ideal solution to support employees in remote offices. Whether they are running on a virtual platform like VMware or Microsoft Hyper-V in a regional office, or on a public cloud platform like Amazon AWS, they can provide comprehensive web security services to small and medium-sized offices without requiring on-site hardware or local technical support.

SWG Cloud Services for Remote Offices and Employees in the Field

A comprehensive web security service built around an SWG can support both remote offices and employees working at home and in the field. Running on a cloud platform, it can protect hundreds or thousands of employees, scaling up and down as web access varies. Cloud-enabled SWGs can form a core component of a SASE architecture, providing network and security services to remote offices and mobile workers who connect directly to the cloud rather than backhauling traffic to corporate data centers.

Simplified Management and Consistent Policy Enforcement

When enterprises use different security solutions for data centers and cloud platforms, they face all the challenges involved in learning, configuring, and managing multiple tools. Typically, they also have trouble combining and correlating information between the tools, which creates extra work and slows down analysis and incident response.

When the same SWG technology can be deployed across data centers, remote locations, cloud platforms, and hosted services, IT teams only need to learn and manage one solution. They also benefit from unified visibility and reporting for security events and data. In addition, the use of a single underlying solution ensures that security and compliance policies will be enforced consistently across the entire enterprise.

Flexible Licensing

Some SWG providers also offer flexible licensing. For instance, Broadcom has made Symantec SWG licenses portable between hardware and virtual appliances and cloud services. If organizations consolidate data centers or move applications to the cloud, they can protect their investment by moving licenses to different form factors.

Summary: Cloud-Enabled SWGs in a Cloud-Centric World

SWGs have come a long way from their original incarnation as hardware appliances that focused simply on proxying user requests for URLs and providing web filtering.

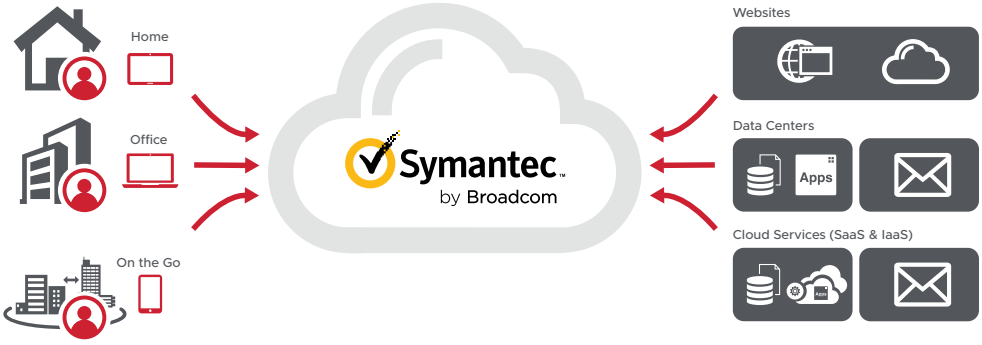
Today they incorporate a wide range of critical security capabilities, including advanced authentication, decryption at scale, malware detection, web traffic optimization, data loss prevention, CASB features, web isolation, and granular enforcement of a wide range of security and privacy policies.

Further, SWGs have evolved to fit into a cloud-centric world, offering new options for SWG virtual appliances that run in virtual environments and on cloud platforms and leverage cloud services such as threat intelligence and cloud-based malware analysis and sandboxing. These same advanced SWG solutions are also at the core of comprehensive, cloud-based SaaS web security service offerings.

In fact, for enterprises working with environments that blend on-premises, irtual, cloud, and SaaS resources, SWGs offer flexibility and simplicity which can not be matched by data center-only or cloud-only security products. The new generation of highly-scalable SWG hardware appliances offers outstanding performance and security for data centers and large offices. SWG virtual appliances and cloud services support remote offices and employees in the field without the challenges of local hardware and support. Common features and a single console simplify management and ensure that security and compliance policies are enforced consistently everywhere.

In short, today's SWGs enable IT organizations to control the pace of their transition to the cloud without multiplying tools or sacrificing security.

Figure 3: Securing the Digital Transformation



To see if your SWG solution is delivering the security you need, review the Appendix: Is Your SWG Keeping Pace?

Appendix: Is Your SWG Keeping Pace?

Does your SWG maximize your security and network performance? Here are some capabilities to look for.

A Wide Range of Security Technologies

To protect enterprises and employees from the ever-expanding number of web-based threats, an SWG should make use of a wide range of security capabilities. They should include a web proxy, web filtering, strong user authentication, malware detection, deep content inspection, DLP and CASB features, web (browser) isolation, granular policy enforcement, and threat intelligence supported by a large community of customer data.

Network Optimization for Web Applications

To improve employee productivity and reduce network costs, an SWG should provide caching of HTML pages and images, streaming media splitting and caching, compression, bandwidth management, and protocol optimization.

Decryption at Scale

When security tools can not handle the surging level of SSL/TLS encryption (now estimated to be 95% of all web traffic), they are forced to let some traffic go through without decryption or inspection, creating unacceptable security risks. An SWG should have the processing power and specialized software and hardware to decrypt 100% of SSL/TLS traffic for inspection (excluding traffic that must remain encrypted to meet security and privacy regulations).

Broad Support for Encryption Cipher Suites

When SWGs do not support all the cipher suites used by websites, they either downgrade some traffic to a weaker cipher, which increases the risk of attackers successfully decrypting data in motion, or allow traffic to bypass inspection, which can allow attackers to hide malware and command and control communications. SWGs should support the broadest range of the latest cipher suites. For more information on the need to support the latest cipher suites, see The Importance of Broad Cipher Suite Support When Inspecting Encrypted Traffic.

On-Premises and Cloud Deployment Options

To give enterprises the flexibility to deploy an SWG in the form that best meets the needs and budgets of each location and work environment, the SWG should be available as a range of hardware and virtual appliances for data centers and for large and medium-sized offices, as well as options for cloud deployment and for cloud-hosted SaaS services to protect small offices and employees working at home and in the field.

Ability to Leverage Cloud Resources

To take advantage of up-to-the-minute threat data and cloud-based security tools, SWGs should be supported by a threat intelligence service that incorporates information from security experts and thousands of customers. They should also be integrated with cloud services for tasks such as policy adoption, malware analysis, and sandboxing. If possible, the vendor should offer a library of curated policies, so organizations do not have to develop all of their policies from scratch.

A Track Record of Industry Leadership

An SWG should have a proven history of achievement and innovation. For example, Symantec solutions have been a top player in The Radicati Group Corporate Web Security Market Quadrant for 15 years. Read the Radicati Group Corporate Web Security - Market Quadrant 2022 report or review the summary. Note that in reports prior to 2016 the Symantec SWG is listed under BLUE COAT® Systems.

SWG-Cloud-WP102 March 3, 2025