The Essential Guide to Secure Web Gateway

Executive Summary

In this era of extreme mobility, increasing cloud reliance, and an expanding network edge, firewalls can only get you so far in the enforcement of security policies. You need tools that can help your branch offices and remote users connect to the internet in a highly secure manner. And you need cloud-native capabilities to help protect your users and data—wherever they are located.

Secure Web Gateways (SWGs) using cloud-native technologies help organizations fill in the gaps left by technologies designed for an on-premises world. They also set organizations on the right path for future-ready security in cloud and hybrid networks. The promise of applications moving to the cloud is so great that some pundits have predicted the death of firewall—but that outlook may be premature.

SWGs available today can replace some products such as SSL/TLS decryption appliances, sandboxing technologies, and even data loss prevention in some cases. However, SWGs are not necessarily a 1:1 replacement of traditional firewalls, next-generation firewalls, or web application firewalls since they do not provide security for inbound traffic. Most present use cases involve SWGs working in tandem with firewall technologies as an important cybersecurity layer to cost-effectively catch threats that firewalls cannot.

In this paper we explore the nuances of SWGs. We'll cover what they are and what they are not, as well as their appropriate role within an enterprise cybersecurity architecture.

Five network security disruptions a secure web gateway address

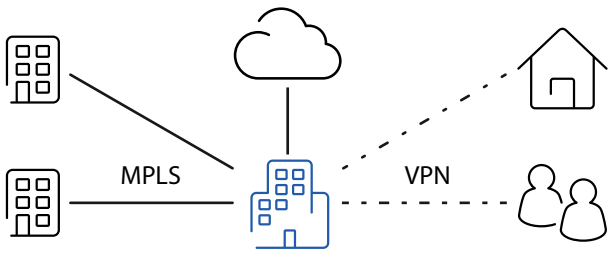
The push for digital transformation in the enterprise has IT departments working diligently to enable employees using company-owned or personal devices, control what sites and data can be accessed, and—perhaps most importantly—empower employees to work from any location.

This macro trend is driving rapid changes in network architecture. Most commonly, organizations are making the decision to connect branch offices and remote users directly to the internet in order to deliver the best performance while using cloud-based applications. These changes are, in turn, causing a number of key disruptions in network security. That means that organizations need to revamp how they inspect traffic to satisfy business and security needs. These disruptions include:

1. Expanding network edge

Software defined wide-area network (SD-WAN) is proliferating throughout the enterprise. According to the latest figures, SD-WAN adoption rates have jumped up from 35% to 54%[1] in the last two years. This change offers a great deal of flexibility. But it also expands the network edge. That makes it harder to monitor network traffic without causing major latency issues at remote offices. Unsurprisingly, 50% of organizations name security as the top challenge in getting the most out of SD-WAN.[2]

Then



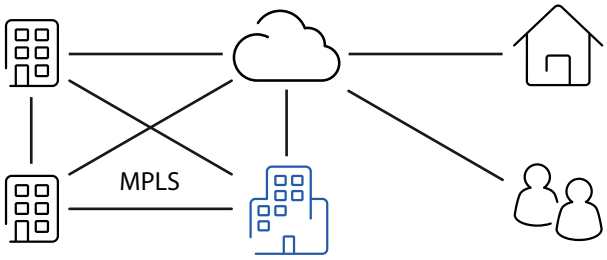
Hub-and-Spoke Architecture

- All traffic backhauled to data center

✓ Centralized security & management

X Latency nightmare for cloud applications

Now



Direct-to-cloud with SD-WAN

- All users connect directly to internet

✓ High performance, cost-effective, reliable

X Breaks centralized security & management

2. Decentralization

Branch and field offices are just the start of the ever-expanding network edge. In addition to these offices, most companies have team members that work from home, from coffee shops, and while traveling. These remote users work beyond the confines of headquarters and require a wide range of options for connectivity and application access. This sprawl puts significant strain on traditional HQ-centric firewalls when network traffic is backhauled with a hub-and-spoke network architecture. It's leaving gaps and causing performance problems across many networks.

3. Hybrid cloud complexity

Network architectures are changing rapidly with the frequent use of SaaS and cloud-based applications. However, there simultaneously remains a lot of enterprise assets housed on-premises at headquarters or in-house data centers. The complexity wrought by this situation makes it challenging for organizations to consistently manage security policies across all users and machines.

4. Encryption's double-edged sword

TLS/SSL encryption has been a boon for modern web security by maintaining data confidentiality in the event it was intercepted, such as a man-in-the-middle attack. That said, it has come with some unintended security headaches. Many organizations struggle to inspect encrypted traffic—even when traditional firewalls claim to offer this feature. It is true they can examine SSL/TLS traffic. However, it reduces firewall performance so greatly that most administrators choose to disable decryption.

5. Security appliance scalability woes

The expansion of IT assets across remote locations, the increased mobility of users, and the rapid growth of cloud-based applications have stretched security resources to the breaking point. Many organizations that rely on appliances and other on-premises tech now face scaling issues. They simply can't meet the demand to support all remote locations and users utilizing on-premises devices. The cost is too high and the management too complex.

Keep in mind that it's not enough to solve for these challenges. You have to do so in a way that keeps user experience for employees high. Those that have positive digital experiences outperform those that don't by more than 200%. They also give you more than 2x the revenue.[3] As such, security has a responsibility to protect connections without introducing latency issues that could harm worker engagement. The trouble? Latency issues abound for web security in mobile era. Especially for those who stick with security status quo.

Research shows that employees engaged in positive digital experiences outperform disengaged ones by more than 200% and generate over twice the revenue.[3]

How cloud-native secure web gateways solve for these disruptions

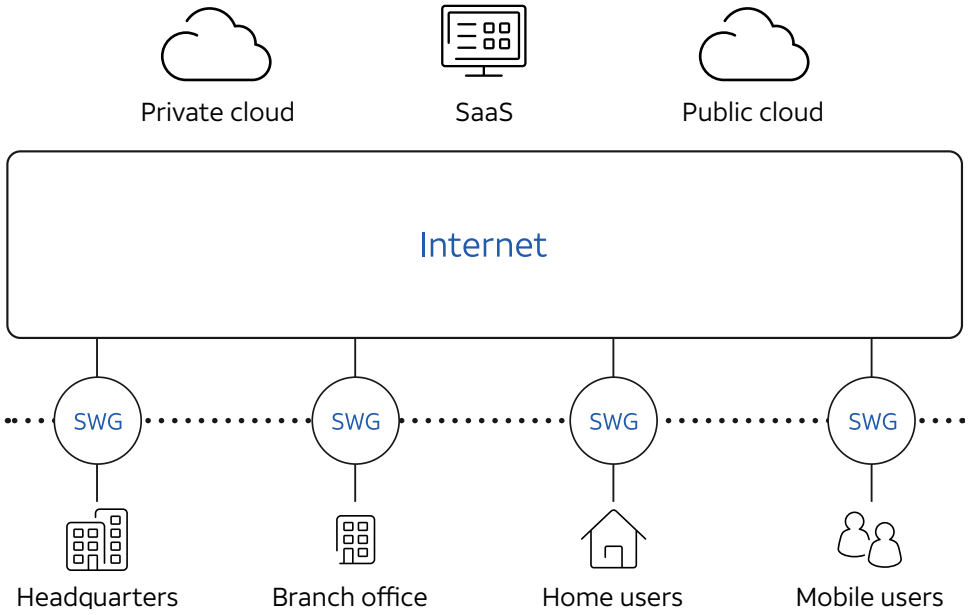
Cloud-native SWG technology addresses the pain points we've discussed. A SWG is fundamentally a web filter that protects outbound user traffic through HTTP or HTTPS inspection. These filters restrict content based on security policies. They also protect user endpoints from web-based threats that can sneak in due to outbound user activity, such as clicking links on websites that are infected with malware.

SWGs can also protect servers when they act as clients. For example, when they go outbound to do things like downloading OS updates. They give enterprises the ability to grant access and control the use of specific cloud-based apps. Best of all, they centralize control, visibility, and reporting across many locations and types of users.

Compare this to next-generation firewalls (NGFWs). Upon their release, NGFWs offered a lot of benefits over layer-4 firewalls. But even NGFWs have their limits. Like traditional firewalls, they were designed to help protect data centers and larger office locations, with the primary purpose of blocking malicious inbound traffic. The primary form factor for NGFWs has been a desktop or rackmount appliance installed at an office location or data center, which is why we call them premises-based firewalls (PBFW). However, PBFWs struggle when the workforce is on the move or remote.

That's a considerable security gap in an era where 70% of employees work out of the office at least some of the time.[4]

Fortunately, this is where a cloud-native secure web gateway excels. SWG technology is best for protection of users on the move. It's web security for the mobile era.



Benefits of cloud-native secure web gateways

Secure web gateways help companies to:

- Take advantage of cost-savings, resiliency, and performance by connecting branch offices and remote users directly to the internet
- Apply security policy consistently across all users, regardless of location
- Centralize visibility across virtually all users and devices into a single dashboard
- Inspect encrypted traffic with minimal effect on network performance
- Quickly scale security as the organization expands
- Reduce the number of physical security appliances they manage

SWG technology offers organizations a more consistent path to policy enforcement when they're centrally managing security policies across multiple locations and a widespread remote user base that's connecting directly to the Internet and cloud resources. It makes it possible to migrate applications to the cloud in fulfillment of business initiatives, while reducing the amount of time dedicated to managing security policies.

Additionally, some SWGs can inspect encrypted web traffic without placing a huge burden on existing firewalls. Selecting a cloud-native SWG offers a way out of the cycle of purchasing ever-more security appliances that add cost and complexity to the cybersecurity architecture.

What secure web gateways can't do

For all of the amazing features offered by a SWG service, it's not a silver bullet. The SWG still needs to work in concert with other security layers in order to maximize defenses.

The most frequent question customers ask about secure web gateway technology is:

Can I replace my firewalls with this?

The answer is that it depends on the use case.

Until businesses move to a fully cloud-based world, SWGs are not an across-the-board firewall killer. Replacing your firewall depends on your environment, as well as where your servers and users are located. Often some, but not all, firewalls can be replaced.

Secure web gateway and premises-based firewalls

SWGs are not meant to replace premises-based firewalls (PBFWs) in data centers. They won't provide the level of inbound filtering or network segmentation needed to protect these centralized in-house assets.

Also, for a large headquarters with many fixed laptops, desktops, or server devices, it would be technically possible to use a SWG but not make sense from a financial standpoint. Here, PBFWs are usually more cost effective. It's much cheaper to buy a PBFW on bandwidth basis than a SWG on a per-user basis.

However, there are use cases where a SWG may be able to affordably replace some firewalls at branch or field offices, assuming they do not support any fixed devices that need to be accessed from outside of the network.

Secure web gateway and web application firewalls

Web application firewalls (WAFs) satisfy a totally different use case than SWGs. WAFs protect websites from inbound attacks that require HTTP/HTTPS content inspection for threat vectors like—

- SQL injections
- OS command injection
- Cross-site scripting attacks

WAFs are also used for content delivery network (CDN) security and distributed denial of service (DDoS) defense.

As we've seen, SWG and various firewall devices often provide different kinds of filtering. They satisfy very different security use cases, which means they can and do co-exist.

In the same vein, there are things SWG can't replace. Things like endpoint security, unified endpoint management, email security tech, SD-WAN appliances, and identity and authentication technology.

What can secure web gateway potentially replace?	What can't secure web gateway replace?
Intrusion prevention systems (IPS)	Firewalls for customers that still have on-prem web / application / file servers
Breach prevention platform (sandbox)	Web application firewalls (WAFs)
Cloud access security brokers (CASB)	Endpoint security
Data loss prevention (DLP)	Unified endpoint management
Load balancers	Secure email gateway (SEG)
SSL / TLS inspection appliances	SD-WAN
Remote location firewall appliances	Identity and authentication

Cloud-native secure web gateway use cases

There are number of important use cases for organizations of all sizes.

- Protection for highly distributed networks: provides uniform security across multiple locations and numerous remote workers
- Solving industry-specific cybersecurity problems: offers flexible security options to financial, retail, healthcare, manufacturing, distribution, federal government organizations
- Application migration to the cloud: provides the means to more safely adopt SaaS applications like Office 365 and to migrate to cloud providers like AWS, Azure, and more
- Security for SD-WAN connections: allows organizations to take advantage of the benefits of SD-WAN by adding a layer of security between each data center or brand location and the internet
- Transform security: helps reduce up-front capital expenditures and move to predictable operational-expenditure model
- Helps support M&As and divestitures: organizations can quickly scale SWG up or down to accommodate changes in the number of physical locations or user count

Learn more

AT&T Global Security Gateway (GSG) is a cloud-native security service that offers unified protection against web-based threats across virtually all office, remote, and mobile users. It's fully managed 24x7 by the AT&T Security Network Operation Center with service options to fit the needs of SMBs to enterprises.

By scaling in the cloud, AT&T GSG improves user experience by removing performance constraints often associated with hardware-based gateway solutions as well as latency caused by backhauling network traffic to central locations where traditional premises-based gateways reside.

AT&T Cybersecurity

AT&T Cybersecurity's edge-to-edge technologies provide phenomenal threat intelligence, collaborative defense, security without the seams, and solutions that fit your business. Our unique, collaborative approach integrates best-of-breed technologies with unrivaled network visibility and actionable threat intelligence from AT&T Alien Labs researchers, Security Operations Center analysts, and machine learning—helping to enable our customers around the globe to anticipate and act on threats to protect their business.

1 https://virtualizationreview.com/articles/2019/07/17/sd-wan-survey.aspx
2 https://virtualizationreview.com/articles/2019/07/17/sd-wan-survey.aspx
3 https://finance.yahoo.com/news/staffconnect-introduces-digital-employee-experience-110010249.html
4 https://www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html