LEARNING MADE EASY

Cloud Secure Web Gateway For Dummies

Palo Alto Edition

The world has changed. Work is no longer somewhere we go, but rather something we do. Although remote and mobile working isn't new, the global pandemic necessarily hastened the broad adoption of work-from-home and work-from-anywhere models in modern enterprises. In the wake of the pandemic, many organizations have embraced this "new normal," and it seems that this hybrid work model is here to stay. According to the Palo Alto Networks study *The State of Hybrid Workforce Security 2021*, more than three-quarters of employees want to continue working from home at least part of the time.

Workers aren't the only ones who have "left the building." Many core business applications, traditionally hosted in on-premises corporate data centers, have been replaced by software as a service (SaaS) applications. *The Flexera 2022 State of the Cloud Report* found that 49 percent of all enterprise workloads run in the public cloud today, and Zippia.com's *30 SaaS Industry Statistics [2023]: Trends + Analysis* reports that organizations are already using an average of 110 SaaS apps and 99 percent of companies will be using one or more SaaS solutions by the end of 2023.

As a result of these important trends, the majority of workers and the applications they access are now used outside the corporate perimeter. Today, the World Wide Web is the new network perimeter. In this guide, you'll discover how a cloud secure web gateway (SWG)

delivers complete security in a single, cloud-delivered platform to protect all your users and applications — wherever they are.

Protecting Internet Traffic with a Cloud Secure Web Gateway

A SWG is an on-premises or cloud-delivered network security solution that filters unwanted software/malware from internet traffic and enforces corporate and regulatory policy compliance. Instead of connecting directly to a website or application, a user accesses the SWG, which is then responsible for connecting the user to the desired website/application and performing functions such as web filtering, web visibility, malicious content inspection, web access controls, and other security measures.

When SWGs were first defined as a category in the security market, most (if not all) of them consisted of proxy vendor solutions. However, SWGs and proxies are not the same thing: A proxy is a networking function, whereas SWG is a security solution. A proxy is a dedicated computer or software that sits between an end client (such as a desktop computer or mobile device) and a desired destination (such as a website, server, or web- or cloud-based application). By acting as an intermediary between the client and destination, proxies can shield the client's Internet Protocol (IP) address from the destination, providing a layer of privacy. As shown in Figure 1, a proxy:

- Receives a web request from a client
- Terminates the connection
- Establishes a new connection with the desired destination
- Sends the data on the client's behalf

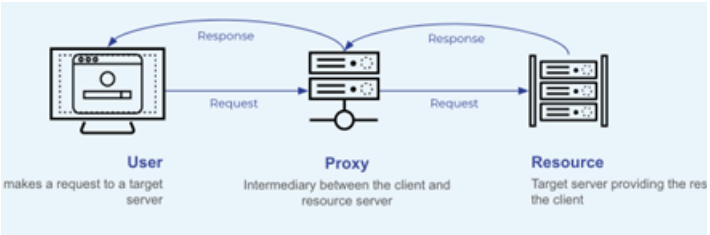

Figure 1: A proxy functions as an intermediary between an end client and a destination resource.

Some of the key limitations associated with traditional on-premises web proxy appliances include:

- **Incomplete security:** On-premises web proxy appliances and other multivendor legacy products were never designed for the cloud and fail to provide complete, consistent security across all users, locations,

and devices. The inability of on-premises web proxy appliances to secure all apps (web and non-web), lack of inline traffic inspection, and poor integration with cloud ecosystems increases organizational risk.

- **Limited app coverage:** More than half of all remote workforce threats are for non-web apps, which are invisible to web proxies. Security teams can't block what they can't see, so the risk of a data breach increases without security for both web and non-web apps.
- **Poor end-user experience:** Performance bottlenecks result when organizations backhaul remote worker internet traffic to data center–based web proxy appliances for access and security. In addition, remote workers often use a virtual private network (VPN), not a SWG, to obtain access to private applications, which can cause confusion and connectivity issues, resulting in more calls to the IT help desk.
- **Multivendor appliance limitations:** Using appliances from multiple vendors results in a lack of centralized management, inconsistent security policies, slow performance, and poor visibility into network threats across the organization. Multivendor siloed appliances lead to inconsistent policies, increase maintenance costs, and limit visibility and collaboration among networking and security teams.

REMEMBER

Applications at headquarters are accessed through a remote-access VPN. When users access cloud applications, they're disconnected from the VPN and exposed to risk. This is one reason why organizations use SWGs: to provide secure Internet access when users are disconnected from the VPN.

Many organizations rely on a cloud SWG to secure Internet access for remote and branch office users; servers, virtual desktop infrastructure (VDI), and Internet of Things (IoT) devices in branch locations, and even headquarters/campus locations with high bandwidth requirements where they need to offload from on-premises to the cloud. Additionally, a cloud SWG provides visibility into user access, internet-based threats, and web traffic, as well as internet controls and enforcement with

access controls, function control, SaaS and data protection controls, and safe internet-browsing capabilities. Finally, a cloud SWG can be used to improve the end-user experience. Instead of back-hauling all web traffic to a corporate data center, which introduces latency, network performance can be dramatically improved by connecting directly to the cloud.

SWGs are also not a substitute for firewalls. First-generation firewalls only inspected IP addresses, ports, or other router-based (layer 2 and 3) protocols. On-premises web proxies operate at layer 7, and next-generation firewalls operate at both the network and application layers (layers 3 and 7, respectively). A cloud SWG moves these capabilities to the cloud and supports proxy-based architectures.

Starting Your SASE Journey with Cloud Secure Web Gateway

One of the challenges of deploying SWG functionality is that it is typically set up as a stand-alone environment without coordinating workflows, reporting, or logging with other security infrastructure in the organization. This can lead to increased complexity over time as organizations often have multiple security-point products that make their security operations less efficient and effective.

More recently, a new approach for security infrastructure emerged. As defined by Gartner, a secure access service edge (SASE; pronounced "sassy") combines networking and security services into one unified, cloud-delivered solution that includes the following, as summarized in Figure 2:

- **Networking**
  - Software-defined wide area network (SD-WAN)
  - VPNs
  - Quality of service (QoS)
  - Routing
  - SaaS acceleration
- **Security**
  - Cloud SWG
  - Cloud access security broker (CASB)
  - Firewall as a service (FWaaS)
  - Data loss prevention (DLP)
  - Domain Name System (DNS) security
  - Threat prevention

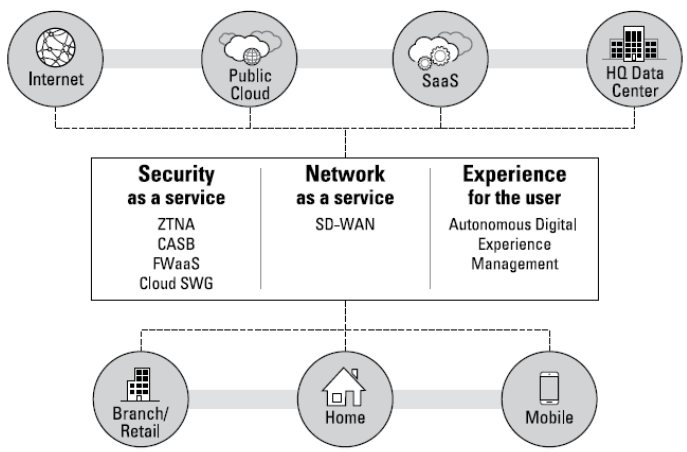

Figure 2: SASE delivers advanced network and security capabilities in a converged cloud-delivered solution.

This allows companies to deliver multiple types of security services from the cloud, such as SWG, advanced threat prevention, FWaaS, DNS security, CASBs, DLP, and others.

SWG is just one of the many security services that a SASE solution must provide. As organizations grow and add more and more remote users, coverage and protection become more difficult. These challenges are compounded by the rapid growth and widespread adoption of SaaS applications, the proliferation of managed and unmanaged personal devices accessing enterprise applications, and the decentralized nature of different enterprise applications running in the corporate data center and in the public cloud. A SASE solution moves SWG into the cloud, providing protection in the cloud through a unified platform for complete visibility and control over the entire network.

REMEMBER

A SASE solution should include SWG, enabling organizations to control web access and enforce security policies that protect users from malicious websites, malware, phishing attacks, SaaS platform attacks, man-in-the-middle attacks, and more.

SASE provides many benefits for organizations including:

- **Securing your remote workforce:** Protect your users, applications, and data with artificial intelligence (AI)/machine-learning (ML)–powered in-line security inspection for all web traffic, both web and non-web.
- **Streamlining network management and operations:** Centralize management and enforcement of security policies, and unify multiple point products and vendors with a single platform.
- **Improving user experiences:** Provide consistent user access and improve user experience with complete visibility and precise control over the end-to-end connection.

TIP

Check out the following resources from Palo Alto Networks to help you protect your internet traffic with a cloud SWG:

- **E-book:** *SASE For Dummies, 2nd Special Edition*
- **Web page:** Cloud Secure Web Gateway
- **White paper:** Modernize Your Secure Web Gateway with SASE

paloalto NETWORKS

9781394186235