EQUINIX

DISTRIBUTED SECURITY SOLUTION BRIEF

SECURE WEB ACCESS IN A DISTRIBUTED ENVIRONMENT

Enhance edge network security in a hybrid/multicloud architecture with Secure Web Gateways (SWGs)

Traditional solutions are based on a static network perimeter protected by security appliances, with the assumption that enterprises can identify unfamiliar elements in their own environments.

Executive Overview

Enterprises on a digital transformation journey are shifting infrastructure from a fixed and siloed state to one that is distributed and dynamic, creating new entry and exit points and thus a greater number of attack surfaces for malicious actors to exploit. As these attack points proliferate, edge network security becomes increasingly challenging—and essential. To protect against these threats, enterprises need complete visibility and control over all web traffic.

One way they can enhance web security is by using Secure Web Gateways (SWGs) to inspect traffic for protection against progressively sophisticated web threats. Below, we'll explore multiple SWG architectures and how to optimize SWG functionality at the digital edge.

Background

Enterprises are struggling to keep up with the number and variety of web threats arising in an increasingly dynamic web environment. Static network perimeters and centralized security appliances are no match for this rapidly changing environment. Today's chief information security officers must envision a network security model built upon a hybrid architecture composed of distributed network services that can monitor all web transactions on-premises and/or in a cloud environment. Such a model allows them to find and shut down all web attack vectors, capabilities that Secure Web Gateways provide.

Web Traffic Grows Exponentially

Cisco estimates that global internet traffic will reach 4.8 zettabytes per year by 2022.[1] As enterprises increasingly invest in web content, infrastructure and services, hackers are pivoting to exploit this greater web usage. In fact, data suggests the web is more dangerous than ever, with web applications the most reported type of data breach according to the Verizon 2018 Data Breach Investigations Report.[2]

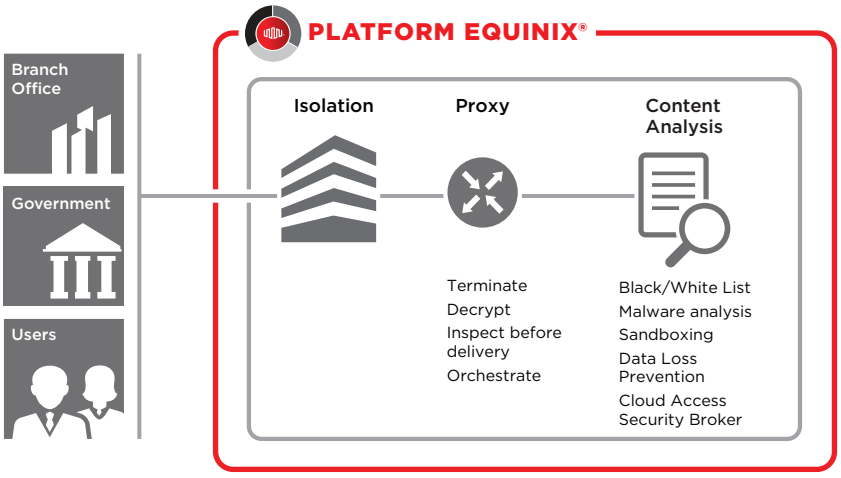
1 http://www.enterprisenetworkingplanet.com/netsp/global-internet-traffic-on-track-to-hit-4.8-zettabytes-by-2022.html

2 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

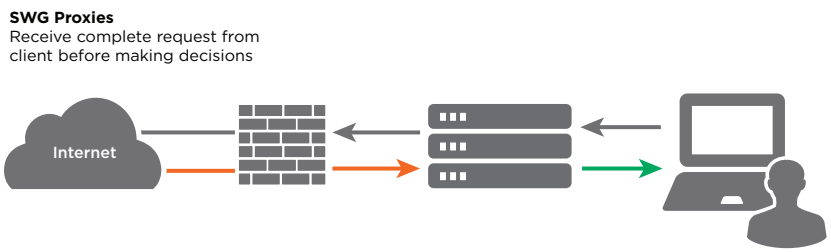
Secure Web Gateway Overview

Secure Web Gateways defend users from web threats via URL filtering, advanced threat protection and malware protection. By acting as traffic gateways at chosen control points, SWGs allow enterprises to control and protect web traffic. Key capabilities of typical SWG solutions include visibility and classification of web traffic, policy enforcement, data loss prevention (DLP), threat protection, and decryption and re-encryption of traffic. In some cases, Cloud Access Security Broker (CASB) functionality is included as a feature.

SWGs are primarily used for monitoring and visibility (for example, observing user behavior on the internet), advanced threat defense and protecting remote offices and mobile workers.



Typically built on a proxy-based architecture, SWGs act as gateways, terminating and re-establishing connections to and from a server (web, ftp, etc.) on behalf of a client. As an intermediary, the SWG terminates inbound connections and emulates a client in order to originate a separate outbound connection to a server. As a result, the SWG can analyze web content and recognize security risks within websites or web content.



SWG 101

How SWGs Stop Attacks

Most SWGs can identify threats concealed in web traffic that would otherwise evade detection by traditional next-generation firewalls (NGFWs) and other perimeter-based security solutions. An SWG eliminates ambiguities by monitoring the entire web session and blocking or filtering based on customer-defined policy, making it one of the best ways to discover and stop attacks before they can do harm.

The 3 Types of SWGs

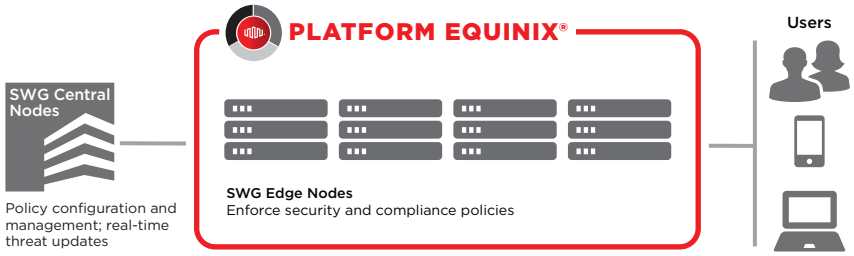
SWGs are implemented as on-premises appliances, cloud-based services or hybrid models that combine the two. An on-premises offering comes in the form of software or a hardware appliance and has been the traditional method for enterprises to manage web security. Cloud-based services for branch offices, remote workers and mobile threats typically use a proxy-based service by placing the gateway in line or by sending all web traffic to the SWG using generic routing encapsulation (GRE) or policy-based routing.

Future Trends

Increasingly sophisticated hybrid models are emerging, with enterprises seeking to bolster the effectiveness of traditional on-premises proxies with Software as a Service (SaaS) components. These can protect users in remote branch offices where an on-premises device would be impractical or prohibitively expensive.

Secure Web Gateways Are Ideally Situated at the Digital Edge

While Secure Web Gateways are well established in the industry, new deployment models require consideration. In a cloud-based, distributed environment, an enterprise's network security perimeter moves from a centralized data center to a decentralized architecture straddling the data center, branch offices and clouds. This new secure edge distributes SWG functionality, enabling visibility into all web traffic, usage control and regulatory control policy management.



In addition, hybrid and/or cloud-based SWG implementations are able to protect remote offices and users connected directly to the internet without degrading performance or delaying delivery. Distributed edge nodes inspect web traffic and enforce web policy near end users, greatly reducing overall web traffic latency.

Conclusion

As enterprises shift applications and workloads to the cloud, they must move some or all their web security to a new, secure edge. A distributed, cloud-based or hybrid SWG solution enables them to protect all users and applications, regardless of where they connect from.

Where to Get Help

Platform Equinix® offers several cloud-based and hybrid SWG solutions. For more information on how web security applies in your environment, please contact securityteam@equinix.com.

Network Traffic Then vs. Now

The Old Model

The data center used to be where most—if not all—enterprise applications were deployed. Enterprise architectures backhauled traffic from branch offices to the data center using a hub-and-spoke connectivity model. As traffic patterns shifted to the internet, security gateways were built to allow secure internet access, including secure web access in the form of on-premises, appliance-based SWGs. SWGs were centralized to minimize the cost and complexity of securing multiple locations.

On the Move

As enterprise applications began moving to the cloud, traffic moved with them. Rather than backhauling traffic, enterprises began implementing local internet breakouts from remote offices, sending traffic directly to the internet. Unfortunately, this work-around allowed traffic to bypass the network security perimeter, including on-premises, centralized, appliance-based SWGs, resulting in an inability to track all web traffic.

Equinix Americas
+1.650-598.6000
info@equinix.com

Equinix EMEA
+31.20.754.0305
info@eu.equinix.com

Equinix Asia-Pacific
+852.2970.7788
info@ap.equinix.com

SB_Secure-Web-Access_US-EN | 8995 | v112619 | 1119 | Q219SL