[eBook]

The Whats, Whys and Hows of a Secure Web Gateway:

Ensuring advanced network protection in the digital era

CLOUD365

getting IT done for you

[index]

[introduction]

The Internet has never been a good place to navigate unchecked and that's what the original Secure Web Gateway architectures were created to do: decrypt and inspect online traffic to mitigate risks in an organization. But long gone are the days when IT departments were able to deploy hardware SWG appliances on-premises and monitor traffic within those bounds or use VPN connections for the occasional remote worker.

Cloud computing exploded over the past few years and points of access multiplied. The numbers are staggering: driven by digital transformation and cloud-first enterprise strategies, the global cloud computing market reached the unprecedented size of $480 billion last year. It is expected to grow exponentially over the next three years to reach $947 billion in 2026, according to Zippia.

We are now living in digital times, which means the foundation of any company has transitioned or is in the process of transitioning to the cloud. In The U.S. alone, 94% of enterprises use some kind of cloud services, while 67% of all enterprise infrastructure is now cloud-based. Zippia estimates that, by 2026, 45% of all enterprise IT budgets will be spent on the cloud. Hybrid workers access enterprise applications from anywhere and navigate the web on their work devices on and off premises. A whole new set of needs, demands, and threats has emerged, and companies need to adopt the next generation of Secure Web Gateway solutions.

In this eBook, we delve into the critical aspects of a Secure Web Gateway, equipping you with comprehensive insights for navigating the digital security landscape.

[What is a Secure Web Gateway and why it is important]

Gartner defines it as a solution to "protect Web-surfing devices from infection and enforce company policies." To be effective, it must include URL filtering, malicious code detection, and application controls. We should look at the SWG as a decisive component of the SASE — Secure Access Service Edge — framework, a piece that fits the security puzzle companies must complete in today's digital environment.

Here's why the next-generation SWG is so important: companies continue to transition to cloud services and digital architectures at lightning speeds and must monitor a growing number of remote workers and devices. We clearly see that some of the effects of the pandemic are permanent, especially around hybrid work. Employees need secure access to Internet-based applications and have a mix of personal and company devices, logging in and out of what used to be a confined network controlled and inspected on-premises by the IT department.

Those security hardware appliances? Costly, hard to scale, and absolutely not created for speed and efficiency. A cloud-first strategy demands a better security approach because data is now in transit at all times and users are accessing sensitive company data from multiple devices and locations. There are privacy concerns, content filtering considerations, and leakage prevention on top of security risks. Simply put, the Secure Web Gateway solution allows companies to control who has access to what from where while ensuring a smooth, bug and delay-free work environment.

[How it guarantees Access Control & Threat Prevention]

These are the two main pain points that IT must solve when looking at the new enterprise infrastructure: how to control access and how to prevent threats in a distributed network with virtually endless access points and profiles. A Secure Web Gateway solution it's a service in the cloud to do this, starting with URL filtering and inline inspection of encrypted traffic. It allows IT to lay out a consistent security policy and enforce it with all of the workers, regardless of their location or hybrid work status.

It also facilitates the control and visibility of applications, identifying sanctioned and unsanctioned ones, gives IT visibility into real-time logs, and analyzes traffic based on identity and context to better identify threats. In a nutshell, only traffic that is deemed safe and in accordance with organizational policies is allowed through.

All management is done via a web-based portal with support from the SWG provider. The goal is to maximize security without compromising operational efficiency.

So, as a middle protection for Site-to-Internet and User-to-Internet traffic, a Secure Web Gateway provides full protection for web and internet-based attacks.

[Threat Intelligence Gathering — the secrets behind a successful Secure Web Gateway]

Consultancy firm PwC defines Threat Intelligence as the process by which specialists collect, analyze, and disseminate information about cyber threats and vulnerabilities. This is a proactive approach that requires constant monitoring and action.

In a blog post, Aryaka's Chief Technology Officer, Srini Addepalli, describes how the Secure Web Gateway plays a "crucial role" in threat intelligence gathering. It relies on data feeds from reputable providers to acquire valuable information about different aspects, including:

- **Reputation of IP addresses, domains, URLs, files, and SaaS services: The SWG leverages threat/data intelligence feeds to assess the reputation of these entities. This information helps in identifying potentially malicious or suspicious sources, allowing the system to make informed decisions.**

- Categorization of domains, URLs, and SaaS services: By utilizing the intelligence feeds, the SWG can determine the categories to which domains, URLs, and SaaS services belong. This categorization aids in policy enforcement and enables organizations to define granular security controls based on specific categories.
- Malware classification of content: The SWG employs the gathered threat intelligence to classify potential malware based on content analysis. By examining the characteristics of the content, the system can identify and block or quarantine malicious files or websites, preventing them from causing harm.
- Data classification of content: The SWG also utilizes data classification intelligence feeds to classify the content of web traffic. This classification helps identify sensitive or confidential information that may be transmitted or accessed, enabling organizations to enforce data protection policies effectively.

As all internet-bound and SaaS traffic passes through the SWG, it has the ability to collect various attributes of the traffic. By leveraging threat/data intelligence feeds, the SWG can enrich these attributes with valuable threat information. This information not only facilitates policy enforcement across different security engines but also provides visibility into the threats present in the traffic flowing through the SWG.

The enhanced visibility enables organizations to detect and mitigate potential security risks in real-time, ensuring a robust security posture.

[The critical role of Security and Access Control Engines]

As Srini Addepalli explains in the same blog article, security engines process traffic sessions before they are TLS/SSL decrypted. They act on all the Internet bound HTTP traffic and stop the traffic session if they identify any potential risk.

· **IP Reputation-based Threat Protection Security Engine:** The administrators of the SWG are empowered with the capability to create policies based on specific IP categories, IP reputation scores, and other generic attributes, enabling them to establish tailored security measures. This engine offers robust protection to users who access websites known for hosting malware and phishing content. Leveraging comprehensive threat intelligence collected on destination IP addresses, the engine efficiently identifies and mitigates potential risks, safeguarding users from malicious activities. By assessing the reputation of each IP address, the security engine makes well-informed decisions on the appropriate actions to be taken in alignment with the matching policy, ensuring a proactive and dynamic security posture.

- **Domain Reputation-based Threat Protection Security Engine:** The administrators of SWG possess the capability to create policies based on domain categories, domain reputation scores, and other generic attributes, allowing them to define desired security measures effectively. This engine provides comprehensive protection to users accessing websites flagged for hosting malware and phishing content. Leveraging domain threat intelligence gathered from various sources, including HTTP CONNECT host header, TLS SNI for TLS-based HTTP traffic, and host header of clear HTTP traffic, the engine evaluates policies to accurately identify and mitigate potential risks. By incorporating domain reputation data, the security engine ensures proactive defense measures, strengthening overall security posture and safeguarding users from potential threats.

In addition to reputation-based threat protection, SWGs offer robust access control capabilities, allowing administrators to provide differentiated access to users when accessing various Internet sites. This powerful security engine enables administrators to create policies based on domain categories, which are provided by reputable threat intelligence providers.

By leveraging domain categories, SWG administrators can simplify their management experience by classifying a vast number of Internet sites into a few overarching categories. This classification system enhances efficiency and ease of policy creation, ensuring that administrators can effectively define access control measures without the need for granular configuration for each individual site.

Moreover, the access control engine also provides the flexibility to specify individual domain names within the policies. This allows administrators to have fine-grained control over access to specific sites, accommodating situations where specific sites require unique access permissions or restrictions.

The flexibility of the access control engine proves particularly useful in scenarios where false positives occur in the domain categorization process. In such cases, administrators can create exceptions within the policies to override the categorization and ensure accurate access control for affected sites.

The ability to handle exceptions empowers administrators to maintain a balance between stringent security measures and providing necessary access for legitimate sites that might be misclassified.

[Moving from legacy to a cloud-based WAN architecture and seeing the whole picture with Unified SASE]

We've been talking about the massive enterprise transition to cloud computing that occurred over the past few years and that means leaving legacy systems behind. The idea of WAN — Wide Area Network — Transformation accelerated with the pandemic after years of maturation. As Gartner put it in its research, "the data center is no longer the center of gravity" and applications are distributed across data centers, cloud, and edge.

The problem with legacy WAN architectures is that they were not designed for this digital era, cannot be easily scaled and redefined, and proved to be too inflexible and complex in the age of cloud-native applications. They add costs and require more and more hardware to secure the edge, with complex maintenance. Additionally, many companies acquired solutions from different vendors over the years and ended up with fragmented policies that spell trouble when it comes to security and vulnerabilities.

Moving from an obsolete WAN architecture to a cloud-based one is inevitable. Companies that put it off will end up with increased security risks and rising costs. A cloud-based WAN architecture provides the flexibility and simplicity that is needed for effective management of the IT environment. The best-case scenario is a one-stop solution that can be centrally orchestrated and allows for the convergence of security and networking. Providing visibility into both will give administrators the ability to observe, identify and act in real-time, with homogenous policies, software-defined workflows, and a single vendor to deal with.

As mentioned before, there are several pieces to this SASE puzzle and it's important to see the whole picture and the benefits of a Unified SASE strategy. This is the way to a consolidated and simplified deployment using the same vendor, a single policy repository, and a single software stack.

The convergence of network and security, combined with integrated observability and lifecycle services, reduces complexity and costs. The company doesn't have to deal with multiple vendors and divergent policies anymore. It doesn't need IT teams to acquire specializations with different vendors and stitch together a security approach.

Unified SASE drives application acceleration and allows for faster deployment, reduces the hardware footprint, increases observability, and centralizes security management. It might even be the key to bridging hybrid work demands as the world adjusts to this permanent shift in the workforce.

[Conclusion and next steps]

Cloud computing has exploded and hybrid work trends are only driving more growth. An interesting set of statistics analyzed by Zippia show that the average employee in the U.S. uses 36 cloud-based services per day and that 87% of U.S. businesses already have a hybrid cloud strategy in place.

With the transformation of network architectures and off-premises access, companies are faced with security, privacy, and compliance challenges. They need to provide secure access to employees, regardless of where they are, while ensuring a smooth experience and monitoring traffic for malicious actors. This is why Secure Web Gateways play such a big role in today's modern enterprise strategies.

SWGs are, in fact, becoming increasingly important solutions due to the nature of work and enterprise infrastructures. In sum, a cloud-first strategy means that enterprise-wide applications and data are accessed virtually from everywhere at any time, as they are no longer tethered to on-premises data centers. Organizations adopted a hybrid workforce model and that is driving up cloud usage, as well as enlarging the potential surface of attacks, security breaches, and more.
We must think of the SWG as part of a SASE framework that is the most advantageous when approached as a Unified solution. The Secure Web Gateway from our partner Aryaka is just that. It helps modern CIOs revamp their infrastructure and simplify operations with a converged networking and security solution that secures internet access for all workers — remote or in-office — as we settle into a hybrid workforce.

Aryaka's SWG is a cloud-based gateway that protects against web-based attacks while reducing infrastructure costs, unifies security solutions, and ushers in a new era of efficiency that leaves behind the complexity and legacy WAN architectures. Get in touch with us and start your journey towards a more secure future.