Cloud Secure Web Gateway

Brand equity, remote connectivity, and IT operations are arguably more fragile than ever. The speed of workforce and cloud transformation have made securing access to the internet and enterprise SaaS apps challenging for most businesses. With the risk of consumer confidence easily lost with a single data breach, it's paramount that organizations strengthen a key tenet of enterprise security: secure web gateways (SWGs).

Today, adversaries continue to enhance their social engineering techniques, acquire advanced toolkits, and utilize as-a-service offerings to easily exploit known weaknesses in legacy SWGs. For this reason, it's important that security teams shore up defenses with best-in-class internet and SaaS security to protect what matters most: your digital way of work and life.

Business and Operational Benefits

- **Protect against advanced attacks and data loss** with a suite of best-in-class security services that inspect all traffic in real time with AI/ML-powered inline detection models.
- **Enable hybrid workforce and boost productivity** with a cloud-native Zero Trust platform that seamlessly scales to match traffic demands as they vary over time.
- **Simplify management and enforcement** with uniform policies across all locations, including data centers, HQ, branches, and remote users.
- **Reduce the cost and burden** to maintain multiple on-premises hardware or hybrid deployments with a single cloud-based SWG.

Shortcomings of Traditional SWGs

For many years, SWGs were deployed as on-premises web proxy appliances, backhauling branch and remote user traffic through dedicated lines or virtual private networks (VPNs). However, these precloud legacy SWGs—built on a hub-and-spoke architecture—were never designed to support today's distributed networks. As a result, they cause latency, operational friction, and, most critically, poor security outcomes. To make matters worse, simply moving on-premises security stacks to the cloud has shown to be equally ineffective, as many cloud-based proxies also fail to meet modern demands for dynamic scalability, consistent location-agnostic connectivity, and Zero Trust security.

So, what's needed? Organizations today demand and expect the highest security outcomes with AI and ML-powered protections, seamless user experiences, and the ability to mitigate risk amid digital and workforce transformation. The goal is to securely connect every user, application, and device from any location with uninterrupted access and uniform enforcement.

Solution Overview

Prisma Access, by Palo Alto Networks, is a security service edge (SSE) solution that delivers best-in-class cloud SWG functionality, including advanced URL filtering, SSL decryption, SaaS application control, and advanced threat prevention. Prisma Access operationalizes next-generation security deployment with a pervasive and always-on cloud-native infrastructure entirely managed by Palo Alto Networks. Mobile users and remote sites can securely access the internet and enterprise applications according to corporate policies, whether those apps are hosted in corporate data centers, public cloud(s), or SaaS-based.

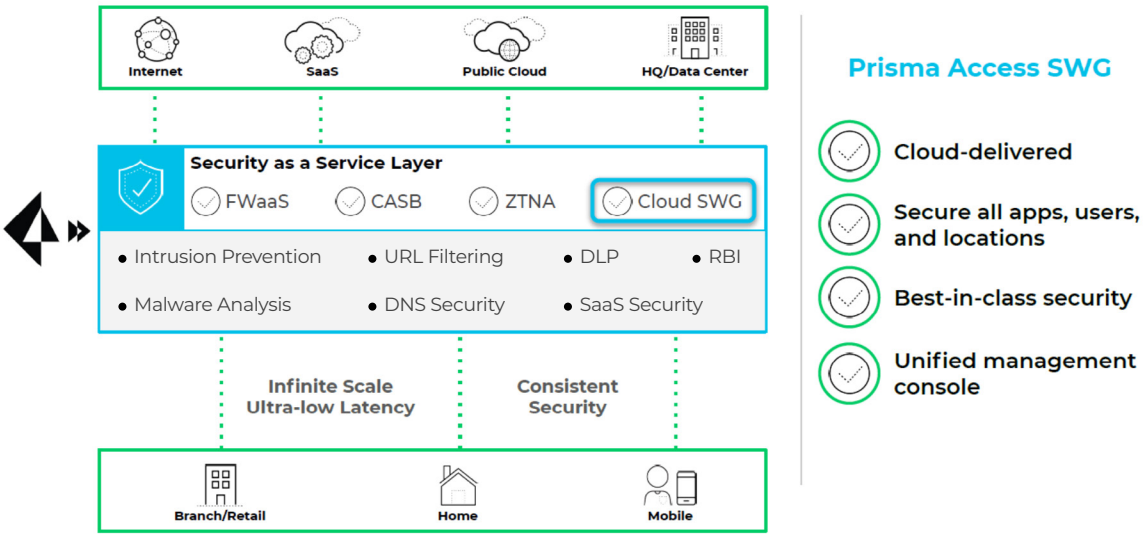

Figure 1: Prisma Access cloud secure web gateway as part of SSE architecture

Full-Stack Security as a Service

Prisma Access coordinates intelligence across all attack vectors to stop exploits and unknown threats, including malware, fileless attacks, phishing, and malicious URLs, as well as DNS-based attacks. Advanced Threat Prevention, Advanced URL Filtering, DNS Security, and Advanced WildFire® services work together to provide comprehensive internet and SaaS security. Natively integrated Enterprise Data Loss Prevention (DLP), next-generation cloud access security broker (NG-CASB), and remote isolation browser (RBI) are also available.

Table 1: Available Security Services	
Security Services	**Details**
Advanced Threat Prevention	Stop zero-day threats, known exploits, malware, spyware, and malicious command and control (C2) with industry-leading threat prevention. Prevent 60% more unknown injection attacks and 48% more highly evasive C2 traffic than traditional intrusion prevention systems.
Advanced URL Filtering	Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, and stop 88% of malicious URLs at least 48 hours before other vendors.
Advanced WildFire®	Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
DNS Security	Gain 40% more threat coverage and stop 85% of malware that abuses DNS for C2 and data theft, all without requiring infrastructure changes.
Enterprise DLP (add-on)	Protect sensitive data across all networks, clouds, and users. Enable data protection and compliance in minutes while eliminating deployment and ongoing management cycles.
NG-CASB (add-on)	Gain proactive SaaS visibility, protection against misconfigurations, and real-time data protection for best-in-class SaaS security.
RBI (add-on)	Create a secure isolation channel between users and remote browsers to keep malicious files and zero-day web threats from executing on user machines. RBI combines the latest vector and pixel-based technologies to deliver superior isolation with a near-native user experience.

For a detailed description of product features and capabilities, please refer to the Prisma Access datasheet.

High Availability and Performance

Prisma Access operates across multiple clouds with dedicated fibers, providing the highest level of availability, even in the event of a zone failure or that of an entire cloud provider. Unlike other solutions that rely on physical servers in rented colocation facilities, Prisma Access leverages the elastic scale and availability of the world's largest hyperscale public clouds—Google Cloud Platform and Amazon Web Services. Prisma Access is the only solution that guarantees 99.999% uptime with less than 10 ms security processing and boasts the industry's only SaaS performance SLA for unmatched performance and user experience. Moreover, unlike legacy SWGs that backhaul all user and web traffic, Prisma Access' cloud-native single-pass architecture removes latency by performing multiple operations only once on a packet. This enables traffic processing at line-rate speeds without performance degradation, even when multiple features and services are enabled.

Flexible Connection Methods

While many companies want to move quickly to an SSE solution, network architectural changes, no-default routes, and industry-specific requirements can add complexity. We get it. Moving away from legacy SWGs can seem overwhelming, especially when countless hours have already been invested in deploying on-premises appliances and maintaining security policies. Fortunately, there are flexible connectivity options to ensure any legacy or alternative cloud proxy architectures can move to Prisma Access with minimal networking changes.

Table 2: Connectivity Options

PAC Files	Easily migrate from on-premises or alternative web proxy to Prisma Access via the cloud explicit-proxy connection. A simple change to existing Proxy Auto-Configuration files means minimal networking changes.
Agent	The GlobalProtect app provides secure connectivity from all managed devices to the internet, SaaS, and private applications across all ports and protocols. The single unified agent supports explicit proxy connections and can even coexist with third-party VPN agents.
Agentless	For unmanaged devices for which you can't install an agent, clientless options provide secure access to on-premises and SaaS web applications.
Site-to-Site IPsec	Prisma Access provides security services for remote networks and safely enables commonly used applications and web access. Remote networks can connect to Prisma Access via Prisma SD-WAN or IPsec-capable devices.

Select Palo Alto Networks hardware appliances can be deployed as a proxy, NGFW, or both to help meet on-premise proxy requirements or to simplify your cloud transformation journey in low-risk phases. Additional guidance for organizations with proxy-based architectures can be found in the solution brief A Proxy-Based Migration Approach.

Web Security Cloud Management

The Prisma Access Cloud Management console provides SWG administrators and IT security teams visibility into all applications, users, and threats, along with actionable insights to immediately improve security effectiveness and simplify management. The single pane of glass offers a unified management experience that includes out-of-the-box predefined configurations and web security best practices to mitigate risk quickly and accelerate speed to market.

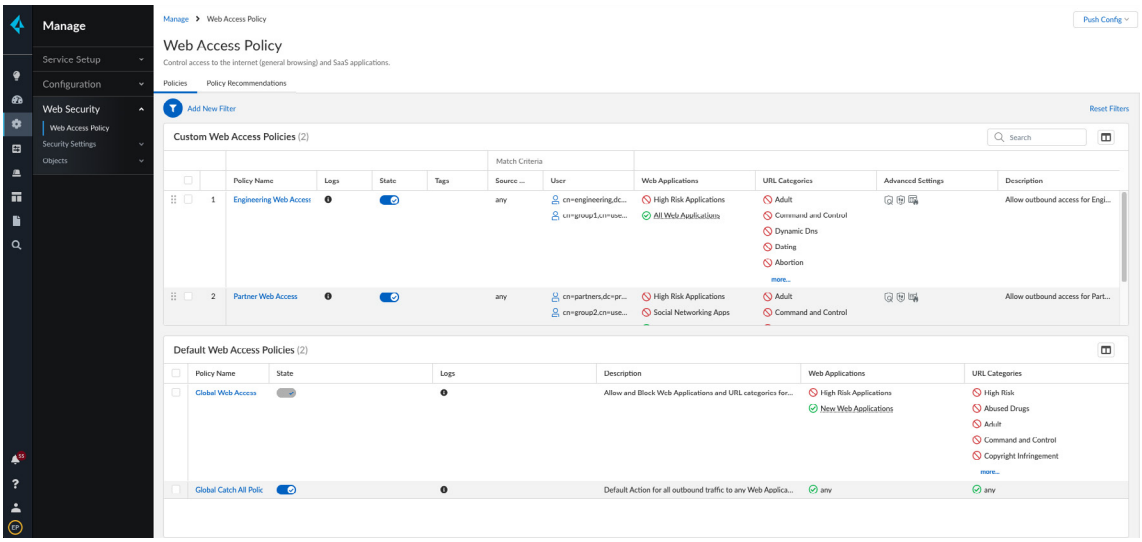

Figure 2: Prisma Access Cloud Management Dashboard

Digital Experience Management

Autonomous Digital Experience Management (ADEM) is an add-on service to Prisma Access that provides native, end-to-end visibility of the entire service delivery path. ADEM provides two ways to monitor the user experience:

Remote users	ADEM is integrated into GlobalProtect so no additional appliances or software is needed. Once GlobalProtect authenticates, ADEM is enabled according to the policies configured in Prisma Access.
Remote networks	ADEM can be integrated into the Prisma SD-WAN Instant-On Network (ION) appliance. ADEM is available for remote networks when Prisma SD-WAN is connected to Prisma Access.

ADEM continuously monitors each segment—from endpoint to application—to identify baseline application metrics and provide visibility into any deviations or events that might degrade the user experience so organizations can quickly isolate problems for remediation.

Global Customer Services

Global Customer Services delivers the guidance, expertise, and resources necessary for maximizing the value of your Prisma Access security investment. Professional Services, Customer Success, support, ongoing education, and adoption tools ensure protection from intruders at every stage of your cybersecurity journey. Contact your Palo Alto Networks account manager to obtain the services that fit your needs.

Deploying a consistent and integrated cloud SWG—as part of an SSE architecture—for all users, data, and devices will not only stop sophisticated cyberattacks but streamline operations and improve user experiences. Branches, home offices, and remote users can now securely connect to the internet and all business-critical apps, irrespective of location, with the same level of access and uniform security as corporate headquarters.

To learn more about Prisma Access Cloud SWG, visit our webpage or contact your Palo Alto Networks representative.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com