
# Securing Remote Workforces with Prisma Access

Prisma Access by Palo Alto Networks is a secure access service edge (SASE) solution for securely connecting users—wherever they are—to applications and services anywhere, whether in public or private clouds, software as a service (SaaS), your data center, or the internet. Delivered as a cloud service, Prisma Access can inspect traffic on all ports and protocols. It can also provide an array of security services, including SSL Decryption, advanced threat prevention, sandboxing, Data Loss Prevention (DLP), Zero Trust Network Access (ZTNA), and more.

Prisma™ Access is a cloud native, entirely software-based solution that takes advantage of public cloud services to dynamically scale with demand. Cloud-agnostic and hardware-neutral, Prisma Access offers more than 100 points of presence in more than 76 countries for optimal performance and localization.

**Figure 1:** Prisma Access points of presence

## Prisma Access at Scale

Mobile user access has already been a challenge for many organizations. Now, the COVID-19 pandemic has accelerated the need for organizations to ensure secure mobile user access while maintaining business continuity. Scaling traditional remote access VPN and mobile user access is difficult, often requiring physical infrastructure changes and expansion. This ponderous manual effort—procuring hardware, building, testing, and finally deploying it into production, not to mention making changes to supporting infrastructure, such as switches and load balancers—all takes considerable time.

Prisma Access dynamically scales to meet user throughput demands, helping ensure business continuity.

As a cloud native offering leveraging public cloud services, Prisma Access can take advantage of practically limitless compute scale with no manual intervention. When a high-throughput event such as the COVID-19 outbreak occurs, Prisma Access detects and monitors increased traffic volume and scales automatically, with no performance impact on users.

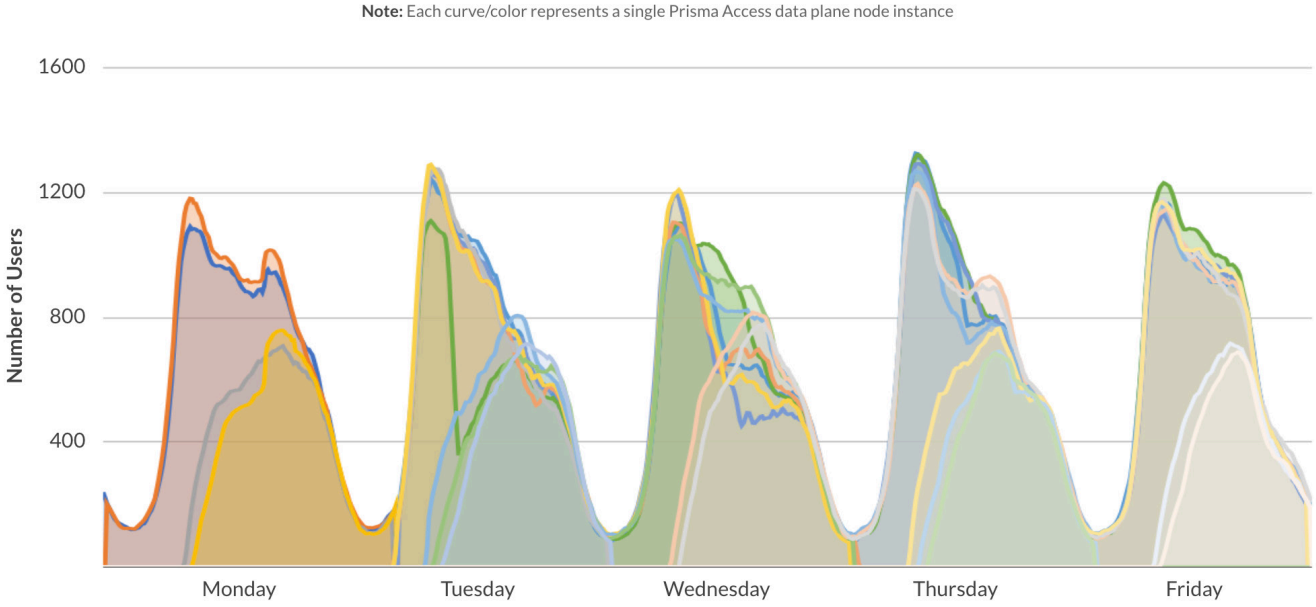


**Figure 2:** Real-world Prisma Access auto-scaling

## Architecture

Prisma Access achieves scale and high performance with a purpose-built cloud native architecture and private customer instances.

Because Prisma Access uses a private global fiber backbone network for transport, customers can on-ramp to an edge location as close to them as possible, and then egress as close to their destination as possible. This reduces middle-mile variability, providing an unsurpassed user experience wherever your data resides—the cloud, SaaS, or the data center.

All customer instances of Prisma Access are private. A private data plane for each customer avoids the security issues and congestion that tend to result from competition for limited cloud resources, as often found in multitenant architectures.

Traditionally, organizations have backhauled all mobile user traffic through their data centers to enforce security and enable remote access. Because of real world limitations, this can be difficult to manage and provides a subpar user experience. Because Prisma Access enforces security from more than 100 points of presence in the cloud, only traffic destined for your private on-premises applications is routed to your data centers. This preserves the user experience while enabling rapid scaling and preventing saturation of data center VPN gateways.

## Security

Unlike proxy-based architectures, SASE solutions with next-generation firewall capabilities—such as Prisma Access—are not limited to inspecting a small number of network protocols. This also means such solutions are suitable to handle all types of network traffic, not just web-based traffic.

The way proxy-based solutions handle user sessions can be problematic for many applications, including SaaS applications like Microsoft Office 365®. For this reason, every proxy has a "bypass list"—a list of applications and URLs the proxy must ignore during inspection so as not to break them. For organizations looking to inspect all internet-based traffic, bypass lists create a dilemma: either leave bypassed traffic completely uninspected or increase complexity by adding more application firewalls to the internet gateways.

Prisma Access keeps your environment simple by including the capabilities of a secure web gateway within a Next-Generation Firewall that natively inspects all ports and protocols in a single cloud-delivered solution.

## Management

Prisma Access can be centrally managed alongside existing PA-Series and VM-Series physical and virtualized Next-Generation Firewall deployments, respectively, using the familiar Panorama™ network security management GUI, enabling Palo Alto Networks customers to easily apply network security policies to Prisma Access. For new customers not already using Panorama, the new cloud management portal provides a simple way to rapidly deploy and configure Prisma Access.

Visit us online to learn more.

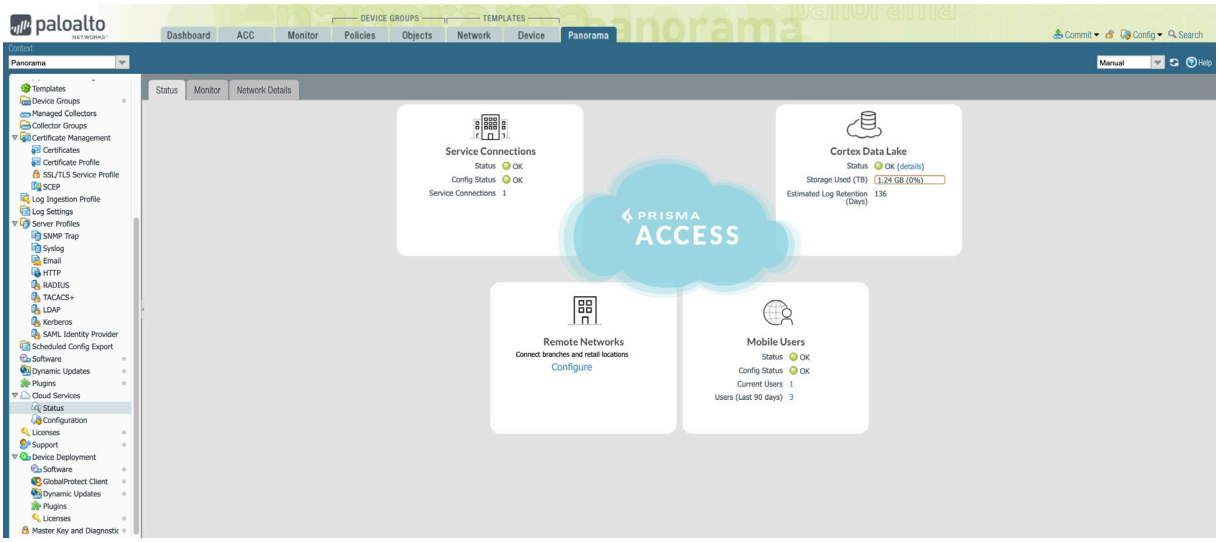


**Figure 3:** Panorama console

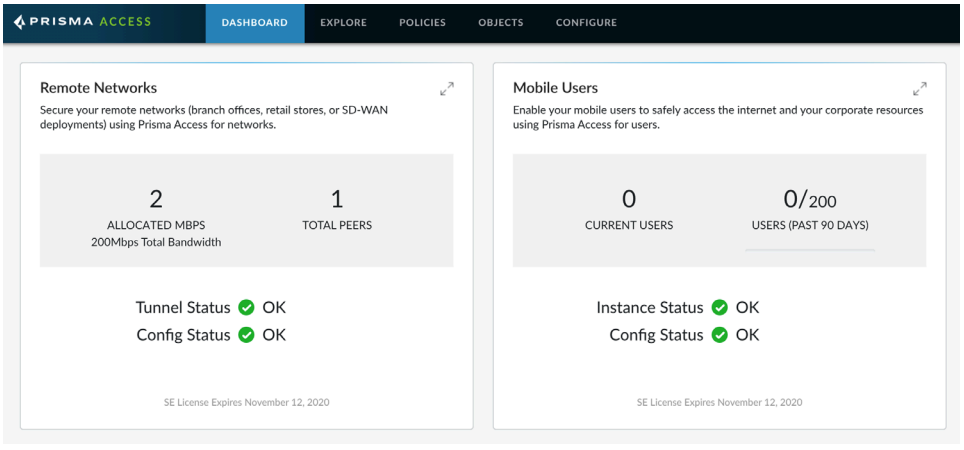


**Figure 4:** Prisma Access cloud console

paloalto NETWORKS

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