paloalto NETWORKS

PRISMA BY PALO ALTO NETWORKS

Four Good Reasons to Modernize Your Remote Access Security Now

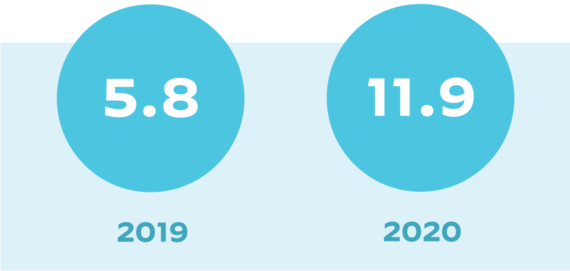
Prisma Access delivers on-demand scalability, full firewall functionality in the cloud, and more

Remote Is the New Normal

Remote work—also known as telecommuting—is nothing new. In 1979, IBM allowed five employees to work remotely as an experiment, which led to more than 2,000 IBM remote workers in just a few years.[1] Since then, the percentage of home-based employees has steadily increased. According to a recent Gallup survey, the percentage of U.S. workers who telecommute at least one day a month has increased from 42% in 2019 to 49% in 2020.[2]

The COVID-19 pandemic accelerated this trend. As of August 2020, more than a quarter (26%) of U.S. employees were working exclusively from home, and nearly 4 in 10 (38%) were at home more than half of the time.[3] Among workers who normally work at home part time, the average number of home-based workdays doubled from 5.8 in 2019 to 11.9 days in 2020.[4] As companies have been forced to move the bulk of their workforce offsite, many are finding that the advantages outweigh the downsides. In addition, workers are overwhelmingly in favor of the change, with 76% of global office workers expressing a desire to continue working from home.[5] Working offsite used to be the exception; now it is the rule.

Average number of days/month worked at home (U.S.)



Legacy Infrastructures Struggle to Keep Up

Moving to a predominantly remote workforce puts strains on existing infrastructures, and as a result, many organizations are grappling with the limitations of their current architectures in three key areas: scalability, security, and performance.

Inability to Scale

When COVID-19 lockdowns went into effect, organizations saw their remote workforce grow by orders of magnitude—in some cases, literally overnight. Legacy architectures—which rely on hardware-based networking and security appliances deployed at each branch location—require physically shipping and manually configuring hardware to each corporate site. Accommodating additional remote users strains bandwidth limitations on northbound internet links and requires adding additional hardware to scale remote users. Unfortunately, legacy architectures are just too inflexible, requiring costly hardware and software upgrades when they can least afford it.

Security Complexity

As organizations migrate applications and information to the cloud, they come up against limitations in their security architecture. Security architects respond with technologies such as secure web gateway (SWG), web application firewall (WAF), and cloud access security broker (CASB). These additions solve specific problems but also increase complexity, making it difficult to maintain consistent policies and introducing gaps in the organization's overall security posture.

Another aspect of this problem is the increased usage of cloud-based, public, and private software as a service (SaaS) to replace on-premises applications such as enterprise resource planning (ERP), customer relationship management (CRM), and human resources management (HRM). A burgeoning use of unsanctioned, personal cloud applications—the so-called "shadow IT"—makes it challenging for organizations to protect managed corporate devices at home and enforce acceptable use policies.

[1] "The History of Remote Work, 1560-Present," TopTal, last accessed December 15, 2020.

[2] Jeffrey M. Jones, "U.S. Remote Workdays Have Doubled During Pandemic," Gallup, August 31, 2020.

[3] Ibid.

[4] Ibid.

[5] Mark Murphy, "The Surprising Truth About How Many Employees Want to Keep Working From Home," Forbes, November 8, 2020.

Degraded Performance

Architectures designed for a geographically concentrated employee population are too inefficient to support today's distributed workforces. One example is hairpinning, which refers to the practice of routing all remote traffic through the headquarters' data center (see figure 1). While this approach can help standardize security and simplify network monitoring, it also has drawbacks. For one thing, all traffic must flow through a centralized location, regardless of destination—a recipe for bottlenecks that degrade network performance and create a single point of failure. In addition, this architecture increases latency, which can impair video conferencing and other media applications.

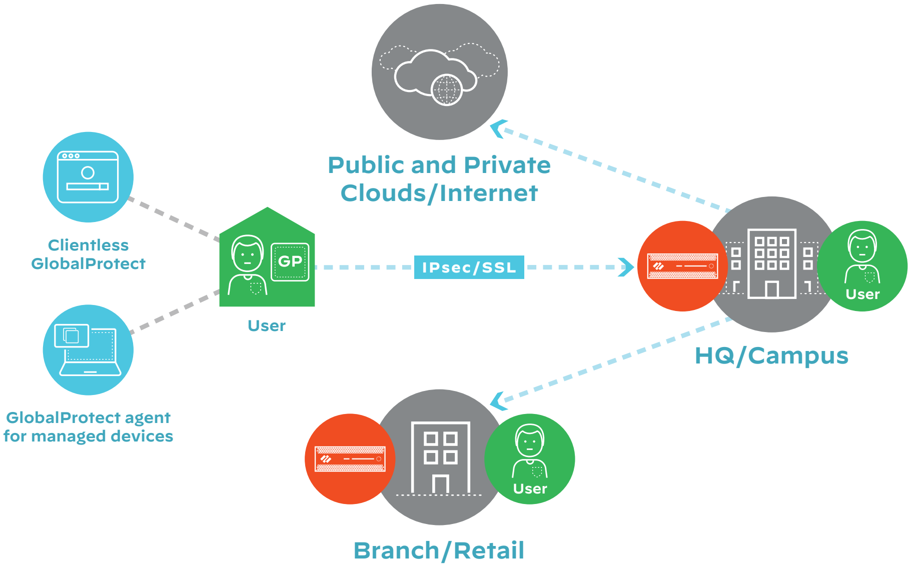


Figure 1: Hairpinning in traditional architectures

SASE Solves These Problems and More

To address these challenges, organizations are turning to a secure access service edge (SASE) model. SASE is the convergence of wide area networking (WAN) and network security services such as CASB, firewall as a service (FWaaS), SWG, and and zero trust network access (ZTNA) into a single, cloud-delivered service model. Top-tier SASE solutions support all types of cloud applications—public cloud, private cloud, and SaaS—through a common framework (see figure 2).

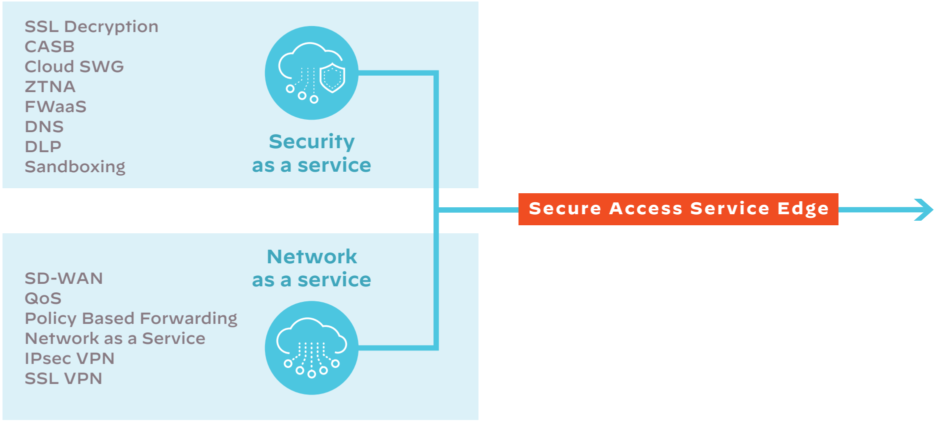
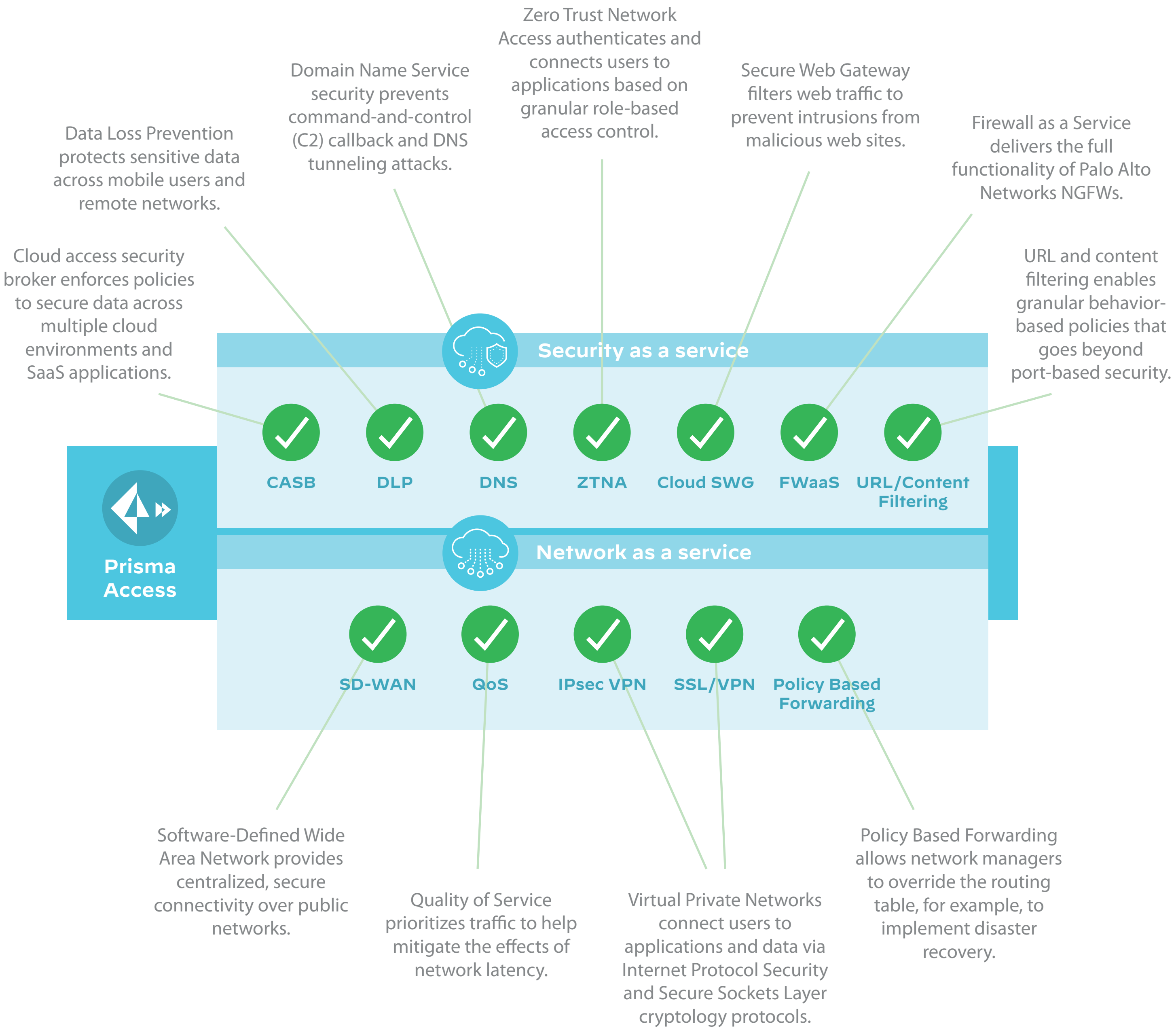


Figure 2: Typical SASE architecture

Prisma Access: The Key to Unlocking SASE

Prisma® Access is a comprehensive SASE solution that enables organizations to deliver protection from the cloud while reducing capital costs and cutting the overhead normally associated with deploying security at scale. Prisma Access uses a common cloud-based infrastructure to deliver both network connectivity and security services (see figure 3).



Cloud access security broker enforces policies to secure data across multiple cloud environments and SaaS applications.

Data Loss Prevention protects sensitive data across mobile users and remote networks.

Domain Name Service security prevents command-and-control (C2) callback and DNS tunneling attacks.

Zero Trust Network Access authenticates and connects users to applications based on granular role-based access control.

Secure Web Gateway filters web traffic to prevent intrusions from malicious web sites.

Firewall as a Service delivers the full functionality of Palo Alto Networks NGFWs.

URL and content filtering enables granular behavior-based policies that goes beyond port-based security.

Software-Defined Wide Area Network provides centralized, secure connectivity over public networks.

Quality of Service prioritizes traffic to help mitigate the effects of network latency.

Virtual Private Networks connect users to applications and data via Internet Protocol Security and Secure Sockets Layer cryptology protocols.

Policy Based Forwarding allows network managers to override the routing table, for example, to implement disaster recovery.

Figure 3: Prisma Access functionality

Prisma Access Complements GlobalProtect

Many organizations now connect their remote workforces using GlobalProtect™, the VPN solution offered with Palo Alto Networks Next-Generation Firewalls. By extending next-generation firewall capabilities through GlobalProtect, they can extend their corporate security (see figure 4) policies to remote users, just as if they were at the office.

Prisma Access complements GlobalProtect for Palo Alto Networks NGFW by providing on-demand, elastic scale for remote users. Rather than hairpinning traffic back to headquarters, remote workers connect directly to the global Prisma Access service edge, which provides integrated networking and security services for accessing public and private cloud services, data center applications, and public internet, all with a seamless user experience.

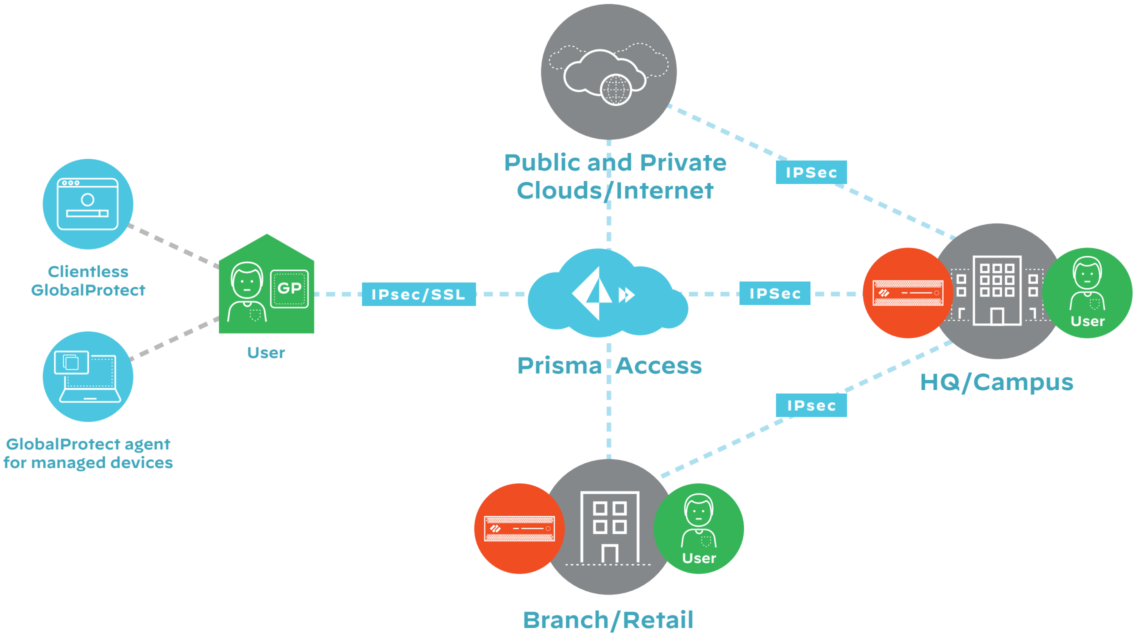


Figure 4: Prisma Access deployed in conjunction with GlobalProtect

[6] Joe Delio, "Leveraging GlobalProtect and Prisma Access during the COVID-19 Pandemic," Palo Alto Networks, March 13, 2020.

Why You Should Consider Prisma Access

The case for Prisma Access is strong and compelling. Here are four good reasons to include Prisma Access in your strategic planning.

Reason 1: On-Demand Scalability

Prisma Access is built on a global high-performance network that ensures infinite scalability for secure remote access. With more than 100 points of presence, Prisma Access can deliver five times the uptime availability with low latency (less than 10 milliseconds guaranteed by SLAs) for an optimal user experience.

Schlumberger Triples Number of Remote Users in Just Days

The COVID-19 crisis posed an enormous challenge for global energy giant Schlumberger. Nearly overnight, the number of remote employees needing to work securely from remote locations increased dramatically. Schlumberger turned to Palo Alto Networks for help.

The next-generation cybersecurity provided by Prisma Access allowed the company to scale from 25K to 80K users in a matter of days with no disruption to productivity. Schlumberger also uses GlobalProtect to extend the Schlumberger user experience into the home and Cortex® XSOAR as the hub of the company's Next Generation Security Operations Center in Houston.

Reason 2: Infrastructure Modernization

Deploying Prisma Access helps modernize your infrastructure to accommodate a large population of remote workers. By eliminating hairpinning, Prisma Access moves security closer to the end user (see figure 5).

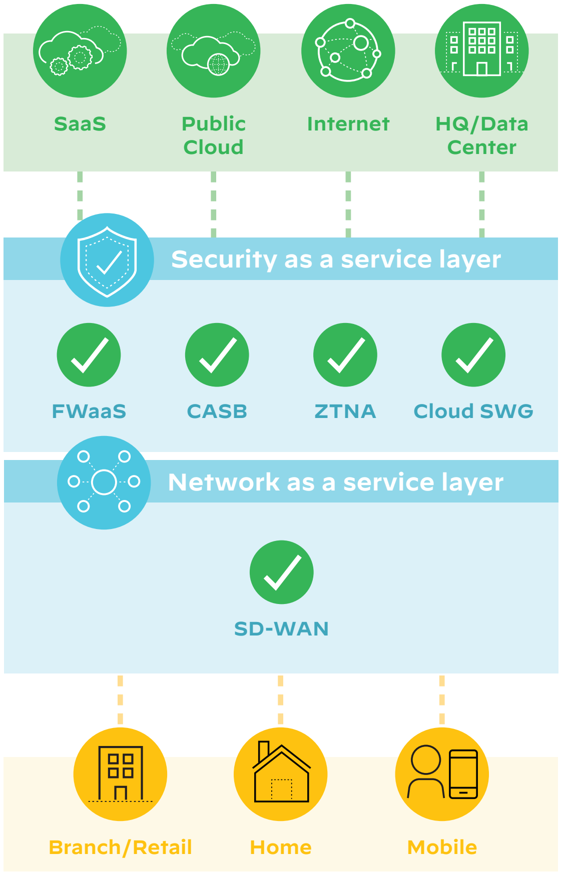


Figure 5: Modernizing your infrastructure with Prisma Access

Reason 3: Simplified SaaS Migration

Migrating to the cloud can seem like a daunting task. Any time you migrate on-premises applications to cloud SaaS, all of your application, user, and security policies need to follow. Prisma Access provides you with a simplified, seamless path to the cloud. Leveraging Panorama as its management and policy interface, Prisma Access allows you to seamlessly migrate your accumulated user, security, and application-specific policies from your firewall deployments. Best of all, you can leverage all of your existing investments in training security analysts and engineers, all while keeping your existing GlobalProtect deployments (see figure 6).

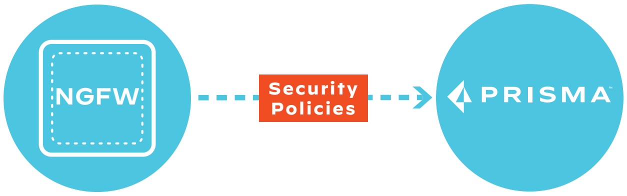


Figure 6: Migrating security policies

Reason 4: Familiar, Trusted Security Capabilities

Prisma Access has all the capabilities of Palo Alto Networks NGFW solutions, delivered from the cloud to secure your remote workforce. Now, there is no need to bolt on additional security components that require training and can leave gaps in your protection. Prisma Access allows you to move gracefully into the cloud at your own pace with confidence that you are protected by a known and trusted security solution that can grow and adapt to your dynamic needs.

Your Next Steps

Moving applications and data from on-premises infrastructure to the cloud and supporting an increasingly remote workforce can be challenging. However, deploying remote access security does not have to be. Prisma Access provides mobile user scalability for the short- and medium-term surge in remote working along with the ability to modernize your infrastructure over the long term.

As the pressure mounts to transition to the cloud, you cannot afford to wait. Take a hard look at Prisma Access today to see how you can benefit from our comprehensive SASE approach. Contact your Palo Alto Networks representative today or visit https://www.paloaltonetworks.com/prisma/access.

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