PRISMA ACCESS
BY PALO ALTO NETWORKS

Deploying Prisma Access at Palo Alto Networks

Summary

This white paper covers the Palo Alto Networks IT department's migration from GlobalProtect™ cloud service to Prisma™ Access. We will review our requirements and deployment strategies to help customers in similar situations benefit from our journey and insights. Among the highlights of our deployment:

- We migrated Palo Alto Networks users globally from GlobalProtect to Prisma Access in four months. This included Prisma Access design, limited pilots with select users, and ramp-up to full deployment.
- We have more than 5,000 unique mobile users utilizing Prisma Access to connect to cloud-based and on-premises applications.
- We were able to reuse and extend our existing GlobalProtect configuration settings.
- Our GlobalProtect Gateways operating on firewalls saw a 50% drop in bandwidth use one month after deploying Prisma Access, due to rapid adoption.

This is a technical paper and assumes the reader is familiar with the Prisma Access configuration steps. Please refer to the Prisma Access Administrator's Guide and other product-related documentation as needed.

Problem Statement

IT departments face challenges securing mobile users who need access to the internet, on-premises applications located in different corporate sites (e.g., headquarters, data centers, and branch offices), and applications running in the cloud. Users and applications can be anywhere. Network and security teams need to deliver a solution that:

- Protects all users
- Provides secure connectivity to access applications
- Secures cloud-based and on-premises applications
- Maintains full visibility of users' activity
- Extends existing security policies for consistent enforcement

Palo Alto Networks is a fast-growing company, with more than 7,000 users, more than 25 global office locations, and on-premises applications in three regions—North America; Europe, Middle East, and Africa (EMEA); and Asia Pacific, Japan, and China (APJC). More than 75% of our applications are cloud-based, with the remainder hosted on-premises across data centers in all three regions. We use all major public clouds and need to provide secure connectivity for all our employees, wherever they are.

We have Palo Alto Networks next-generation firewalls at all of our locations, which we leverage to route traffic using Border Gateway Protocol (BGP).

We have been using GlobalProtect across our global locations, providing a set of GlobalProtect Gateways to global users globally, as shown in figure 1. We use Panorama™ network security management to centrally administer all our firewalls, and we operate GlobalProtect with a lean team:

- Three network security engineers who focus on security and network connectivity
- Two customer experience support engineers who manage trouble tickets and provide the first level of support to employees
- One identity management engineer who focuses on centralized user management, authentication, and certificates

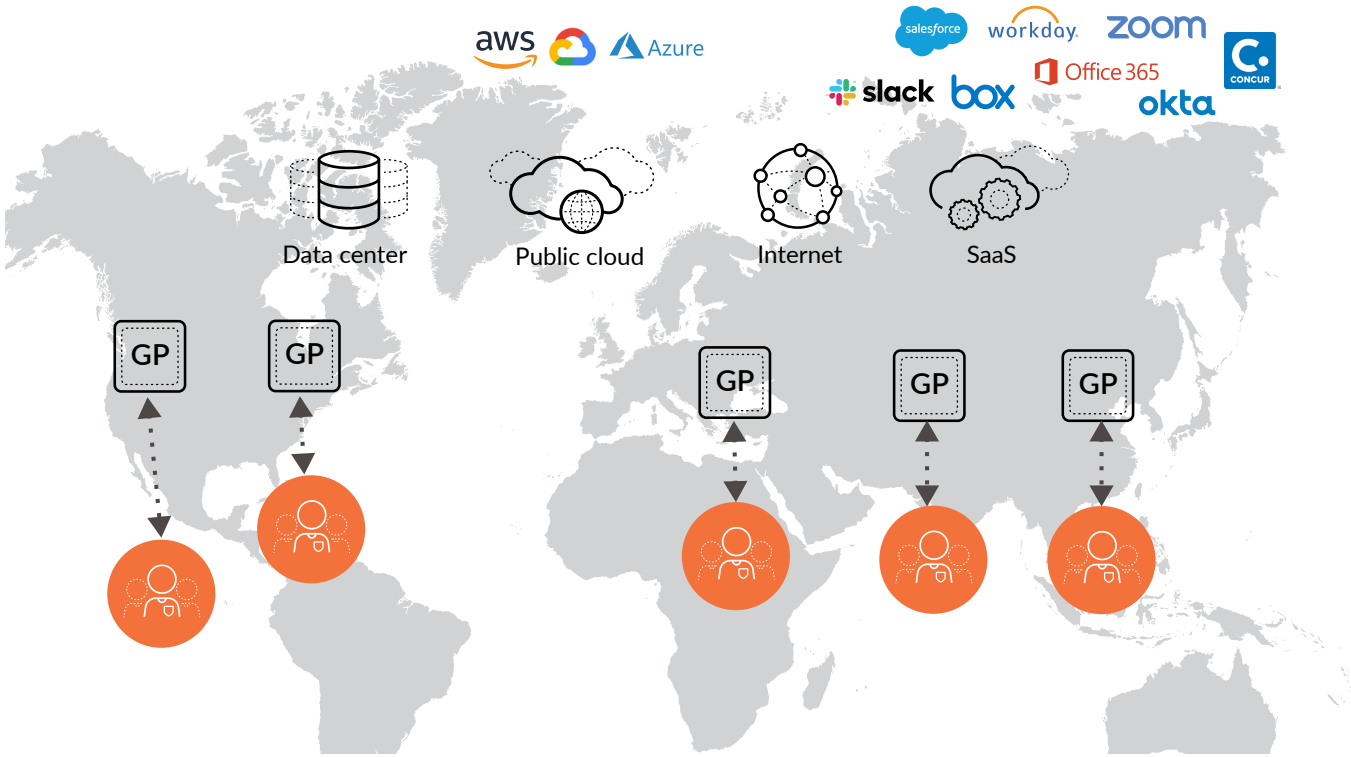

Figure 1: Secure connectivity with GlobalProtect

GlobalProtect Architectural Details

Our GlobalProtect design supports the following capabilities:

1. **Always-on tunnel:** Users on laptops are connected to GlobalProtect Gateways whenever their machines have network connectivity. On mobile devices, we don't enforce GlobalProtect agent usage yet.
2. **Two-factor authentication:** Certificates and Active Directory® credentials are used as the second factor when connecting to GlobalProtect Portal and Gateways.
3. **Multi-factor authentication (MFA):** We use identity management software such as Okta®, Ping Identity®, or Yubikey® for step-up authentication to our cloud-based and on-premises applications.
4. **Internal host detection:** Enabled when users are at a campus location, this ensures that IPsec tunnels are not needed while connected to the internal network, as shown in figure 2.
5. **Current security policies based on User-ID and App-ID:** We decrypt almost all of our egress SSL traffic.
6. **Host information profile (HIP) policies:** The GlobalProtect agent provides User-ID and HIP data.

Why Prisma Access

Our GlobalProtect environment works well, but we need to constantly track the user experience across different gateway locations. For example, if the user experience is slow in a given region, we have to monitor performance, track bandwidth, work with the internet service provider to increase capacity, or build out more GlobalProtect gateways. Although we are a global organization, we do not have data centers in all possible geographies where our users are located, which can also create logistical issues about whether to host a gateway in our own data center, at a cloud provider, or find a local colocation facility.

Looking at Prisma Access, we immediately saw the benefits, including that it:

- Simplifies our architecture and reduces our IT overhead as a fully managed service. It provides automatic code version upgrades, selection of gateways, and gateway performance as part of the service.
- Provides better coverage of gateway locations and delivers a more consistent user experience with constantly expanding global coverage.
- Provides a seamless user experience and automatically scales, providing consistent bandwidth for gateways at all sites.
- Eliminates the need for us to deal with ISPs for gateway connectivity.

- Extends our existing security and connectivity policy based on User-ID, certificates, and routing, resulting in simplified deployment.
- Lets us integrate with Prisma SaaS reverse proxy and SAML proxy, in conjunction with Clientless VPN, allowing us to secure sanctioned software-as-a-service (SaaS) and internal applications when users access these applications using mobile or unmanaged devices.

We went from initial design to a limited global pilot—and finally to a full global deployment—in approximately four months, using the Panorama Plugin to design, configure, and manage our deployment. We were able to build a Prisma Access architecture that extends our security features set: User-ID™ and App-ID™ technology, Threat Prevention, URL Filtering, WildFire® malware prevention service, Prisma SaaS and Cortex XDR™. Prisma Access logs stored in Cortex™ Data Lake, which subsequently makes them available to Cortex XDR for our security operations center (SOC), extend our visibility into mobile user traffic (see figure 2).

The rest of this paper describes various aspects of our Prisma Access journey, including our requirements, design, pilot, and full global deployment.

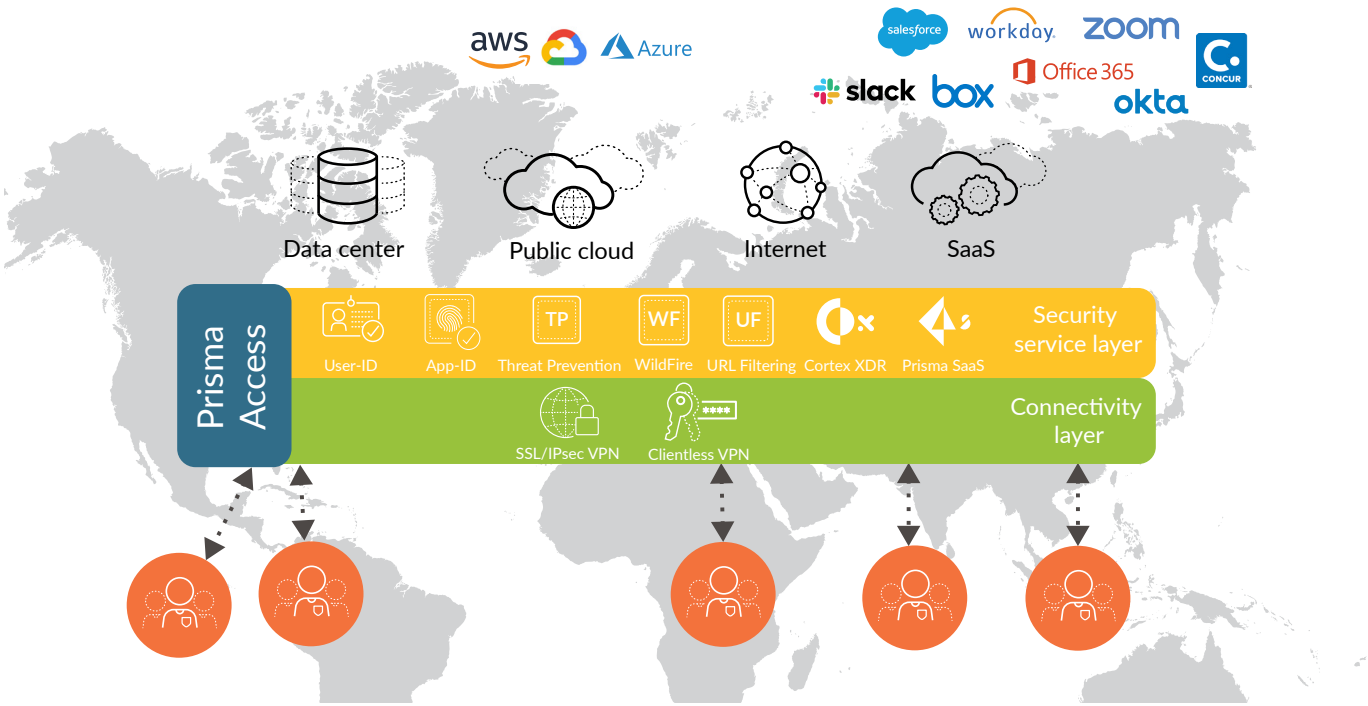

Figure 2: Prisma Access architecture

Design Considerations: Planning

Before working on Prisma Access, we checked the requirements:

- **Panorama version:** Prisma Access requires Panorama 8.1 or later. Our Panorama version was 9.0 at the time.
- **Licenses:** We had the following licenses activated:
  - Cortex Data Lake for all available theaters—Americas and EMEA—with enough storage (400 TB at the time).
  - Prisma Access mobile user license for 12,000 users.
- **IP Subnets:** We carved out our IP subnets from our existing IP address space (RFC 1918) for Mobile Users, Prisma Access Infrastructure subnet. These need to be configured on the Panorama Cloud plugin tab in the configuration section.
- **Portal name and BGP autonomous system (AS):** We used the default domain "myportal.gpcloudservice.com" to name our portal and let Prisma Access automatically create the necessary certificates as well as publish the hostname to the public DNS servers. We went with the default BGP private AS numbers assigned by the Prisma Access configurator.
- **Domains and DNS:** We got our list of internal domains and DNS resolvers.

Note: For our Prisma Access implementation, we used a single IP address pool for all mobile users worldwide.

Tip: For the mobile user subnet, we made sure the address space doesn't overlap with typical home/business wireless routers. For example, we avoided 192.168.x.x and other well-known private address spaces.

Design Considerations: Service Connections

Palo Alto Networks is a global organization with applications and services residing in three main locations: North America, EMEA, and APJC. North America has data centers and local applications. EMEA and APJC have local facilities (e.g., labs, applications). Other network services, such as DNS and Active Directory, are distributed globally.

We configured four service connections in Prisma Access—one in North America, two in EMEA, and one in APJC—to allow mobile users globally to access local resources closest to them. We built the service connections between our corporate firewalls and Prisma Access regions one by one, starting with North America, followed by EMEA, and then APJC.

IPsec Tunnels for Service Connections

We built our IPsec tunnels with public addressing, between our internet-facing corporate firewalls and the public address of the closest region in Prisma Access. For example, we chose the "US-West" region to build a service connection with our firewalls at our headquarters in Santa Clara, California. We used predefined network profiles: IKE Crypto & IKE gateways based on earlier deployments.

Our service connections are shown in figure 3 as red lines.

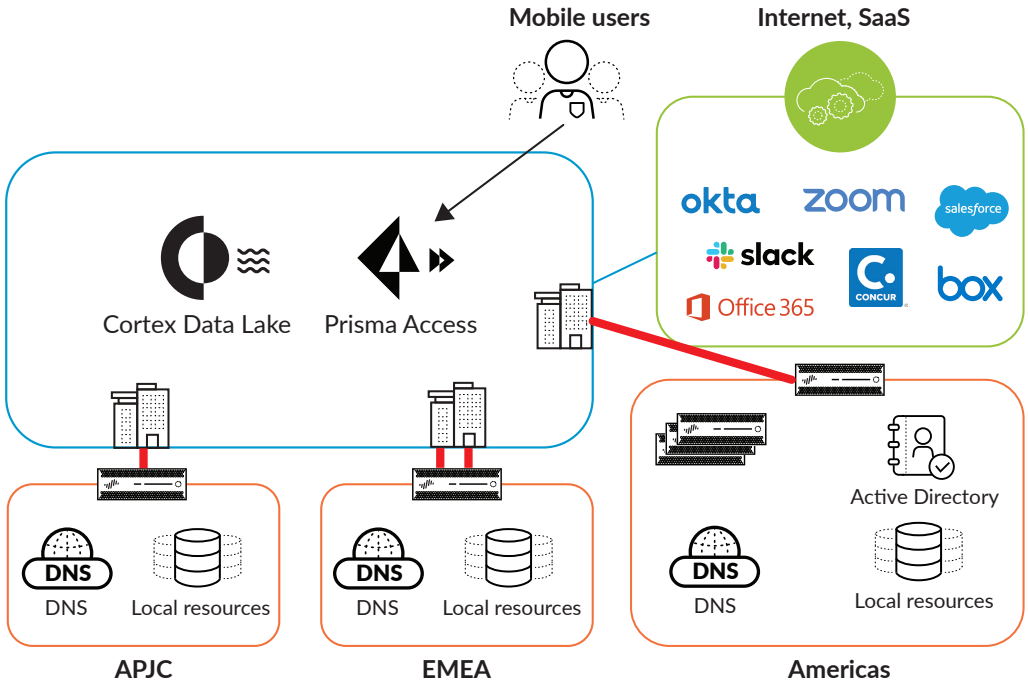

Figure 3: Prisma Access service connections

Design Considerations: Routing

BGP Peering

We built BGP peering with Prisma Access and our corporate firewalls through the service connections. We used non-public IP addresses on our firewalls and the BGP peer addresses exposed through Prisma Access from our infrastructure subnet (see figure 4). Note the infrastructure subnet space (in red) and the BGP IDs on the Prisma Access regions.

BGP Route Advertisement to Prisma Access

We used our existing IP addressing and GlobalProtect routing space to determine our networks and local resources in North America, EMEA, and APJC. As shown in figure 4, we advertise these routes to Prisma Access using BGP Export rules:

- The North American service connection is advertising the entire existing GlobalProtect address space to Prisma Access using BGP. We're advertising summary routes (i.e., non-exact matches) to Prisma Access.
- The EMEA and APJC service connections are advertising specific local prefixes to Prisma Access using BGP.
- One EMEA site is advertising the entire GlobalProtect address space with a longer AS-Path, and we use AS-Path prepending to elongate the AS-Path list for routes advertised from EMEA. This gives us redundancy in case our North American connection goes down.

Design redundancy: Advertising specific local routes from EMEA and APJC to Prisma Access while advertising all routes from North America allows us to reach local resources in EMEA and APJC even if the service connections to those regions go down.

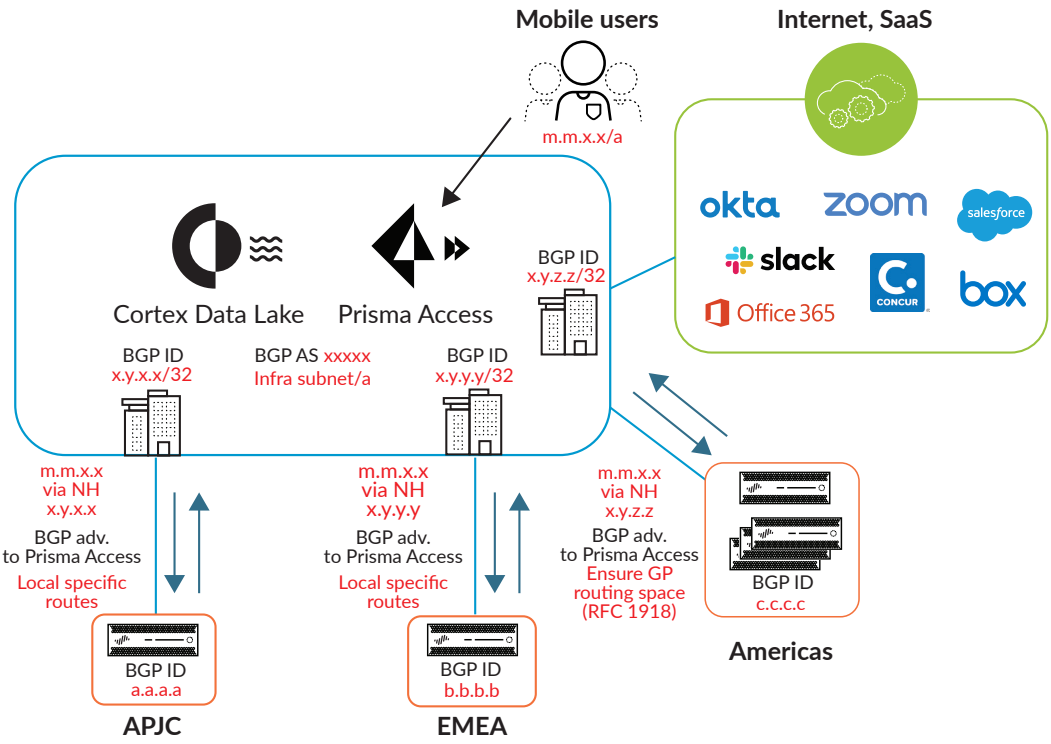

Figure 4: Prisma Access BGP routing

Routing Mobile User Space from Palo Alto Networks Enterprise to Prisma Access

As figure 4 shows, we're learning the Prisma Access mobile user space in North America, EMEA, and APJC. In each case, the BGP next-hop attribute is different, allowing the return traffic from on-premises offices to Prisma Access to take the local service connection as the next hop.

SD-WAN Integration

Our SD-WAN endpoint provider is one of the leading vendors of SD-WAN technology. We use a mesh of current SD-WAN devices to connect multiple sites. However, our current SD-WAN software doesn't support BGP with Prisma Access, so we're using our SD-WAN devices to pass through IPsec tunnels used for our service connections. For now, SD-WAN is invisible to Prisma Access. SD-WAN integration is on our roadmap for when we upgrade our SD-WAN endpoints to software that supports BGP with Prisma Access.

Design Considerations: Mobile Users

We were able to mostly reuse our existing templates from GlobalProtect and add them to the Prisma Access mobile user templates.

Mobile User Authentication

When a mobile user connects to a Prisma Access Portal, we use our existing GlobalProtect Authentication Profile to authenticate the user. This consists of two-factor authentication:

1. Active Directory-based credentials at the Prisma Access Portal validate the user based on Active Directory credentials through the service connection in North America. The mobile user is then assigned an address from the mobile user address space. The mobile user shares HIP data and, after successful authentication, builds an IPsec tunnel with the GlobalProtect Gateway.
2. Certificates on laptop and mobile devices are distributed through either our endpoint management software or mobile device management software. We were able to reuse the GlobalProtect certificates that were already deployed.

GlobalProtect Always-On

Just as with GlobalProtect, we kept our always-on policy for user logon.

Internal Host Detection

We reused our internal gateway for internal host detection. We do not require endpoints to have tunnel connections when on the internal network. We use the GlobalProtect agent to get User-ID and HIP data from endpoints.

GlobalProtect Agent Disable

We allow users to disable the GlobalProtect agent for up to two hours. With Prisma Access, the GlobalProtect agent automatically re-enables itself after this period.

Access Policy for Mobile Users

We use the following policy, depending on whether a user comes from a laptop or mobile device (e.g., iPhone or Android phone):

1. **Laptops:** Prisma Access always-on with GlobalProtect agent. Users have access to cloud-based and on-premises applications once authenticated. Users additionally have to use identity management software, such as Okta, Ping Identity, or Yubikey, for MFA.
2. **Mobile devices:** These don't generally use Prisma Access. The GlobalProtect agent isn't mandatory for our mobile devices.
   a. **On-premises:** Users can access cloud-based and on-premises applications with Active Directory credentials, certificates, and identity management software for MFA.
   b. **Off-premises:** Today, mobile users can only access SaaS applications and use Active Directory credentials, certificates, and identity management software. We plan to use Prisma SaaS with Prisma Access Clientless VPN to improve SaaS security by always redirecting off-premises users through the nearest Prisma Access gateway so consistent security policies can be applied.

Security Policies for Prisma Access

We were able to use our existing device groups from Panorama, and this allowed us to reuse our security policies and egress SSL decryption policies. Two key points to keep in mind:

1. **Terminate mobile users at trust zones.** We built our IPsec tunnels for service connections in such a way that the IPsec tunnels terminate on existing GlobalProtect trust zones. This allows us to reuse our existing security policies (see figure 5—light-green boxes indicate trusted zones). A mobile user ends on a trust zone after being successfully authenticated and existing security policies can be applied.
2. **Reuse existing security policies and simplify zones.** Prisma Access has two different zone types: "trust" and "untrust." We reused our security policies by selecting them as the Parent Device Group and mapped zones as "trust" or "untrust." This allowed us to reuse existing security policies and security profiles as well as other policy objects (e.g., application groups and objects, address groups), HIP objects, profiles, and authentication policies.

Tip: Since Prisma Access locations are distributed globally, egress internet traffic (Netflix®, YouTube®, etc.) doesn't need to be backhauled to the corporate data center. Egress internet traffic leaves the Prisma Access gateway serving the mobile user.

For us, this provides the best of both worlds: we don't need to use a split tunnel, yet we still have full application visibility for mobile users.

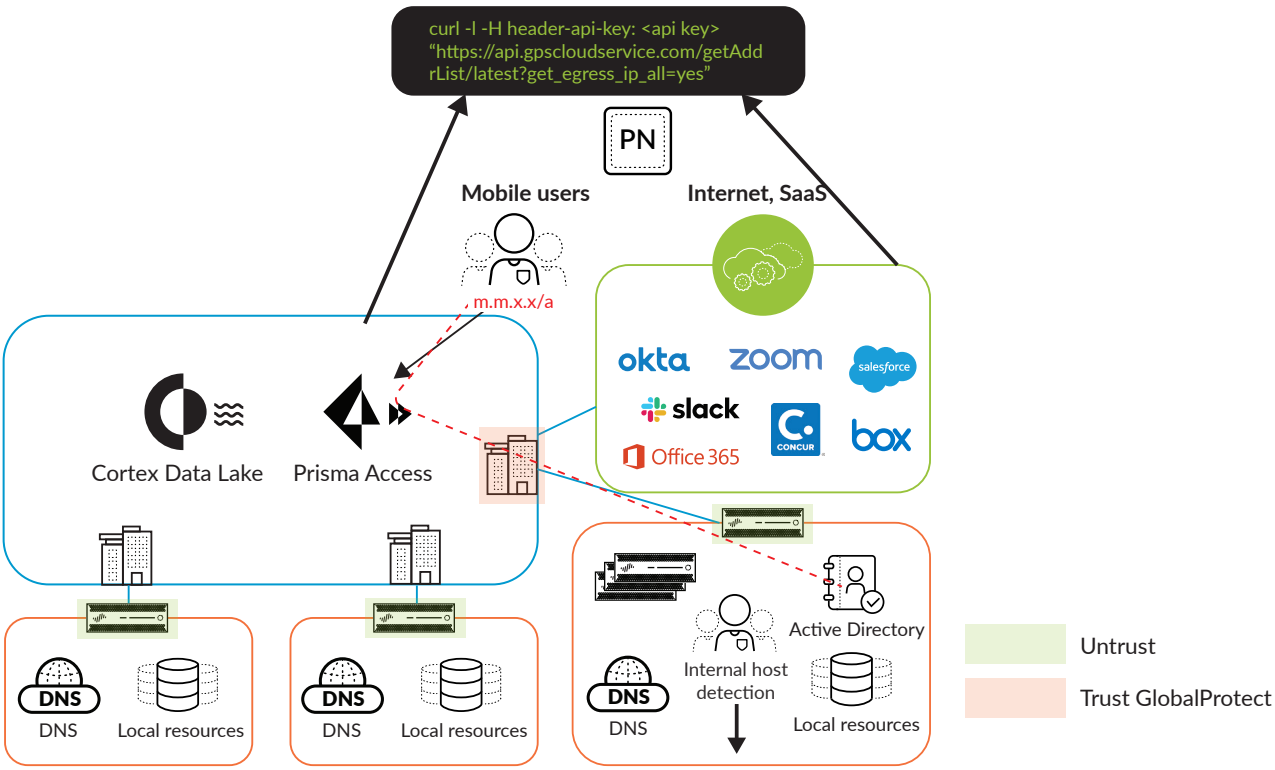

Figure 5: Security policies, zones, and whitelisting of Prisma Access IP address space

Since we use egress SSL decryption, we can reuse those policies as traffic leaves our enterprise network bound for the internet or cloud applications through Prisma Access locations.

Whitelist Prisma Access IP Address Space with MFA Identity Provider

We need to whitelist Prisma Access IP address space so mobile users can access cloud-based and internal applications without being continuously prompted for MFA. We also:

- Initially needed whitelisting at Prisma Access setup
- Need whitelisting to be updated periodically when new Prisma Access locations are added or Prisma Access infrastructure is upgraded

We integrated a curl command available with Prisma Access into our MFA automation workflows. See figure 5 for the manual version of the command (in the black dialog box).

Prisma Access Limited Global Pilot

Once the Prisma Access design and configuration were complete, we wanted to drive a limited global pilot for 30 days (see figure 6). Our approach was as follows:

1. **We identified 300 Prisma Access champions globally.** For the user mix, we identified users in IT, Engineering, Product Management, Sales, Customer Support, Marketing, Legal, and HR to ensure representation across the company. We handpicked these champions so we could get direct feedback on user experience and issues. Users could revert to GlobalProtect if they ran into critical issues.
2. **We pushed the Prisma Access Portal as the default portal to the GlobalProtect agent for the champions.** We used our endpoint management software to push the new Prisma Access Portal configuration to clients.
3. **We set up a Slack channel to report/track Prisma Access issues** quickly and ramp up our Support organization. Most issues we saw were related to fine-tuning security policies.

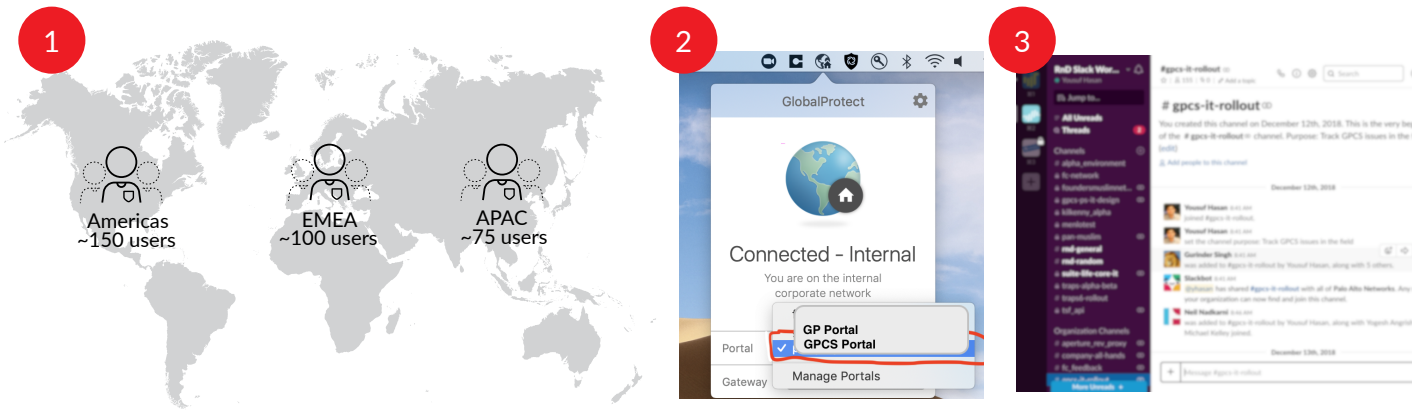

Figure 6: Limited global pilot

Tracking Champion Usage of Prisma Access

We wanted to track our champion's usage of Prisma Access. The current Panorama view is instantaneous and doesn't report a historical view of user adoption over time. As such, we built our own reporting dashboard using the Cortex Data Lake data, where we could see 30-day usage of Prisma Access users based on the metrics below. This view shows us the adoption trend over a period of time, providing an adoption baseline over 30, 60, or 90 days.

Key performance indicators in our report:

1. **Prisma Access successful login**—people who used Prisma Access successfully at least once.
2. **People not using GlobalProtect cloud service (or Prisma Access)**
   a. **GP successful login**—people still using GlobalProtect who have no Prisma Access usage. Some people just had the GlobalProtect agent disabled perpetually, with no expiry timer.
   b. **No Prisma Access or GP login**—mostly inactive contractors.

3. **GP agent disabled for more than 10 hours in the last 60 days**—people who continuously disable the GlobalProtect agent. We had several Engineering and Sales people who needed to disable the agent.
4. **IHD connection**—people who use Prisma Access or GlobalProtect but use "Internal Gateway" because they're based out of a Palo Alto Networks campus. These users are not using Prisma Access while connected to the internal gateway.

Figure 7 shows a view of the dashboard. This view is recent, after our Prisma Access production deployment, but gives a good idea of the aforementioned metrics. Metric 1 and 2 are mutually exclusive, and 4 is a subset of 1 and 2.

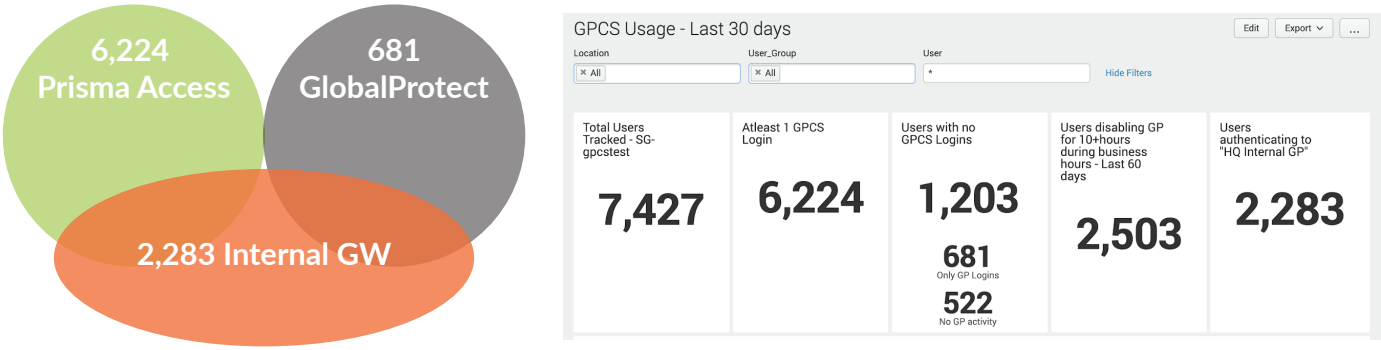

Figure 7: Prisma Access and GlobalProtect usage metrics

Prisma Access Production Deployment

After the 30-day pilot, we wanted to roll out Prisma Access in production. We gave ourselves three weeks to deploy globally. We took a few days for planning and set aside two weeks to push the new Prisma Access Portal as the default portal to the GlobalProtect agent for users in different global theaters.

We also wanted to ramp up users slowly so as to not overwhelm our support team with issues. This slow ramp-up is reflected in steps 4a and 4b in the following. Here are the steps we took:

1. **IT communicated with targeted users for the first few days.** We initially targeted select users and informed them that they would be able to use Prisma Access in addition to GlobalProtect in a certain one- to two-day window. This prevented the Prisma Access rollout support teams from being overwhelmed by onboarding new users.
2. **We provided a user FAQ through our IT communication channels.** This helped us clarify some important points ahead of time, such as the fact that, when users are on campus using the internal gateway, they're not Prisma Access mobile users. We also guided users on how to report issues and capture logs.

   We even listed some common known issues that users could fix on their own. For example, if the user's home Wi-Fi network has the same IP address space as the mobile user address space, they should change their home Wi-Fi network IP address space to work around this issue.
3. **We tracked user issues in the first few weeks.** Our pilot paid off here as our Support team was ready to deal with a few issues, mostly whitelisting of Prisma Access address space and security policy tuning.
4. **We ramped up gradually**, pushing the new Prisma Access Portal as the default portal to the GlobalProtect agent for users.
   a. Week 1—Americas: 50 users on day 1; 100 on day 2; 200 on day 3; 400 on day 4; 800 on day 5; 1,000 on day 6; 2,000 on day 7; everyone else on day 8
   b. Week 2—EMEA, APJC: 300 on day 1; 600 on day 2; 1,000 on day 3; everyone else on day 4

Table1: Observations from Our Prisma Access Deployment	
What We Liked	**Challenges**
GlobalProtect Bandwidth Freed Up • Our GlobalProtect Gateways saw a 50% overall drop in bandwidth use one month after deploying Prisma Access.	
Prisma Access Setup • Compared to deploying GlobalProtect, Prisma Access has less control in terms of configuring gateways. However, we got used to the ease of provisioning. Network engineers gradually stopped worrying about it. • We could utilize routing design to run BGP across multiple service connections. • We used SD-WAN devices to pass through IPsec tunnels between service connections. SD-WAN integration looks promising, but needs planning.	**Documentation** • Documentation available at the time of our initial deployment lacked some details. Documentation has been improving over time and should no longer be a challenge for customers.
Device Groups and Templates • We were able to simply extend current GlobalProtect policies and templates to Prisma Access without having to recreate them.	**Troubleshooting** • Troubleshooting requires mostly looking at the Panorama Plugin to extract information, without direct access to Prisma Access locations. The network engineers were not used to thinking this way.
Identifying Champions • A mixture of people from various departments provided a diverse mix of Prisma Access users.	**Tracking Usage over Time** • We were unable to get the usage metrics needed for deployment out of the box, but we were able to build our own reports using data from Cortex Data Lake as a workaround.

What's Next

We plan to incorporate the following capabilities in the coming months:

1. **SD-WAN integration:** Our current SD-WAN vendor doesn't support BGP with Prisma Access. When we upgrade, we'll look into enabling it.
2. **Prisma Access for Remote Networks:** This is a better fit for our smaller locations.
3. **Prisma Access and GlobalProtect in hybrid mode:** We'll keep a few GlobalProtect Gateways for legacy functionality.
4. **Protection for sanctioned SaaS applications when using unmanaged devices:** We'll take advantage of Prisma Access Clientless VPN with Prisma SaaS SAML Proxy.
5. **Enhanced Reporting:** We'll be able to maintain historical views—daily, monthly, and last 90/180 days—for each of the user categories:
   - Users by region, per gateway
   - Users by org

Conclusion

With good planning, deploying Prisma Access is simple and fun. It has changed the way we think about many things, especially how we handle operations. We're impressed with the capabilities we have gained, especially in freeing up resources and delivering the protection our staff needs.

PRISMA ACCESS
BY PALO ALTO 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

deploying-prisma-access-at-palo-alto-networks-cs-110419