Q&A from August 20, 2020
Enabling Secure Remote Learning for International Students

We have a large number of students in China and they tend to block VPNs. Has Palo Alto gotten an exception for Prisma so it does not get blocked?

- How can we leverage Prisma Access to assist our students in China to have enhanced access to their educational resources? Prisma Access within China is addressed in this document - **https://www.paloaltonetworks.com/resources/whitepapers/prisma-access-service-in-china**
- We are trying to block areas like China but need to allow only certain students/faculty. can we do this in Prisma? No, we cannot sell Prisma in China, however we may be able to use the hybrid approach with a separate GP gateway in China for this use case. However it is outside of Prisma Access and no SLA's apply.
- I think many here would be interested to hearing more detail about supporting students in China. Can we dig into the practical details of how students would access the Prisma service? We discussed this on the call, however here are some details. We cannot support users in China with Prisma Access. However we can build an environment outside of Prisma Access with a Global Protect gateway inside of China and an unencrypted link outside of China to a device that is connected to Prisma Access. This is not covered under SLA or Prisma Access contract.
- Is there a general architecture diagram for connections in China that you can share with us now? Yes, absolutely. Link is here: https://www.paloaltonetworks.com/resources/whitepapers/prisma-access-service-in-china
- Students connecting to the Prisma cloud from China should not be an issue, right? Yes that is an issue, please see the above answers.

Is there any MFA integration? Yes, for MFA we support two integrations, Radius and SAML.

What sort of IPSec performance from the cloud to the on-prem device can be expected? Under SLA today with Prisma Access, we support 300 Meg with full SLA, we also support 500 Meg with no SSL decrypt and 1Gig with best effort.

Is traffic encrypted between the GlobalProtect/Prisma Access gateway and the gateway that has the IPSec tunnel back to our home campuses? Yes, all connectivity requires IP-SEC tunnels.

So Prisma just moves the vpn off of our palo to a cloud based solution? Basically, yes with autoscaling and agility with the public cloud environments and support for the environment is on Palo Alto Networks, not the user.

For the 300mbps SLA on the IPSec cloud to on-prem tunnel, is that per user, or aggregate?
This number is a guaranteed SLA. We often see throughputs higher than this but we can only guarantee 300mbps

What are the similarities of Prisma to a robust SD-WAN solution? Prisma is designed to be a security solution not a transport system. Prisma has advanced NGFW security features, SD-WAN does not.

How does Prisma Access compare to a service like Cloudflare Access? Prisma is designed to be a security solution not a transport system. Prisma has advanced NGFW security features, SD-WAN does not.

Do those extra services come with the sub or is it extra? They are included in the Prisma Access sub with the exception of DLP.

We already have GP on-prem deployed - does Prisma mean a different portal to select when connecting via GP? You can include those existing gateways in Prisma Access for a hybrid solution.

How does NAT'ing outbound connections from clients to public IPs work with Prisma access? Prisma provides SNAT to public IP's that are assigned to each customer. Those IP's can be configured in SaaS solutions for white listing. They are not shared with any other customer.

Would that connection look like you would with azure? Connectivity to any Public cloud environment would be using an IP-SEC tunnel to any device that can terminate IP-SEC in the VPC or VNET. Typically that can be a native cloud device (virtual gateway) or 3rd party device running in the cloud. Prisma does not currently support any native peering in the public clouds.