Partnering with Palo Alto Networks to Securely Connect Remote Workforces During the COVID-19 Outbreak

Changing Business Landscape

According to the latest news, while global response intensifies, the COVID-19 outbreak continues to spread around the world. Countries are taking drastic measures to accelerate their responses.

To help contain the spread of the virus, many organizations have mandated or recommended remote work for their staff. Countries like Japan, where spending long hours in the office is still regarded as crucial for success, have been forced to change their workplace culture to help to curb the spread. In addition, governments in many countries have called to shut down schools. Around the globe, millions of parents and workers have been forced into a work-from-home experiment for which many organizations are ill prepared.

Rapid shift in remote work trends

Securely connect remote workforce & branch sites

The Problem

One of the biggest challenges stems from the lack of technology infrastructure, especially lack of access control and strict security protocols to support a larger remote workforce.

Moreover, with cloud-based productivity tools and other employee-facing technologies increasingly prevalent in today's workspace, organizations must consider the need to secure access to these cloud apps and services to ensure business continuity and performance during the outbreak—and hopefully avoid facing the rising costs of a breach.

Enabling Workers Who Need Secure Remote Access

Organizations need to provide immediate, scalable access to large numbers of employees while maintaining a good security posture in the dynamic environment. To do this, organizations need a safe and effective foundation for remote digital access, providing secure access to IT resources in the cloud and on-premises, as well as to the internet from remote locations.

Virtual private network (VPN) technologies are designed to be used by a subgroup of employees; they were not intended to be used by entire companies all at once. Unable to cope with this increased demand, they're likely to crash, bringing all productivity to a halt.

Additionally, being outside the office without access to a secure, local network means devices are stuck with weak security settings. VPNs just don't protect the endpoints. Organizations must enable anyone to work securely, anywhere, on a range of trusted and untrusted devices, and must provide a consistent security policy aligned as closely as possible to what they would enforce at physical corporate locations.

Partnering with Palo Alto Networks for the Best Support During the Outbreak

Palo Alto Networks offers multiple solutions to help organizations secure their remote workforces without compromising performance or the user experience.

GlobalProtect on Physical and Virtualized Next-Generation Firewalls

Every Palo Alto Networks Next-Generation Firewall supports always-on, secure access with GlobalProtect™ network security for endpoints, enabling you to protect your mobile workforce by extending the Palo Alto Networks Security Operating Platform® to all users, wherever they are. GlobalProtect secures traffic by applying the platform's capabilities to understand application use, associate the traffic with users and devices, and enforce security policies with next-generation technologies. To that end, we extend:

- **Our commitment to existing Next-Generation Firewall customers**: We're offering a free 90-day trial of our GlobalProtect subscription to enable instant remote access capacity on your existing infrastructure. We have a reserved hardware pool, along with expedited shipping and procurement, for impacted customers in need of more capacity as their remote workforces grow.

Prisma Access

A globally distributed cloud service, Prisma™ Access scales automatically to provide the capacity your remote workers need, offering the same security functionality as our Next-Generation Firewalls without the need to deploy new infrastructure. As the global situation changes, this means your organization can maintain business continuity as Prisma Access scales wherever capacity changes are required.

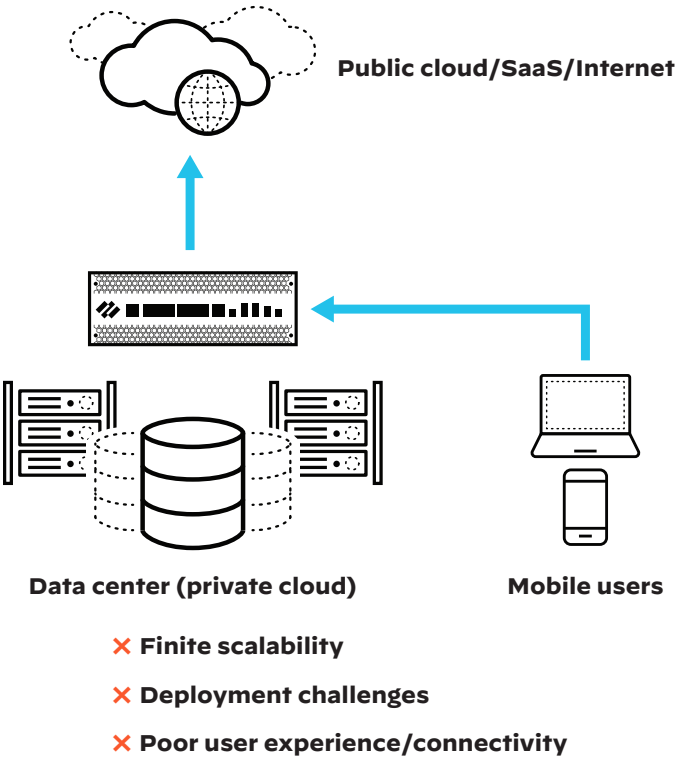

Figure 1: Under-architected remote access

An under-architected remote access solution (see figure 1) doesn't scale well, requiring more hardware to sustain growth and creating deployment challenges due to the underlying complexity of connectivity and location. In most cases, it also offers a poor end user experience, such that many users may choose to disconnect the VPN and connect directly to cloud apps, putting their organizations at risk.

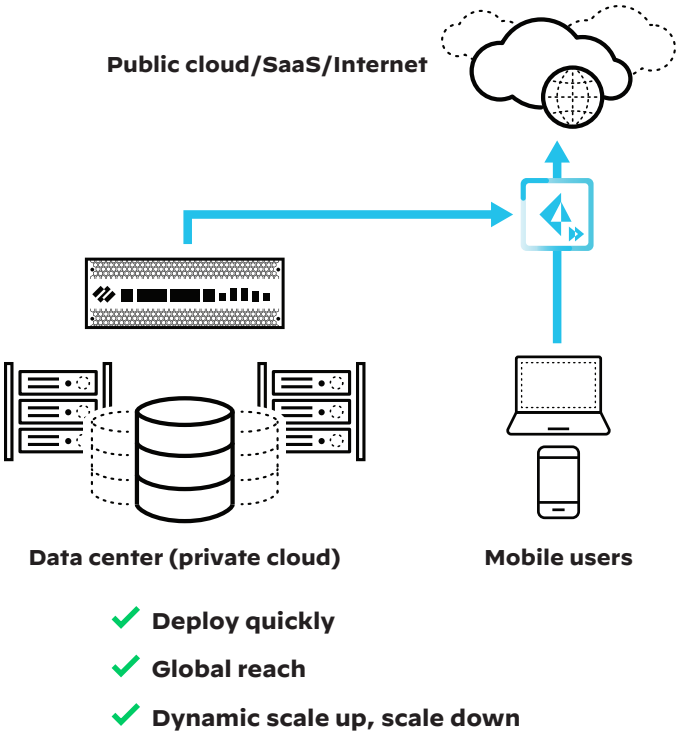

Figure 2: Scalable remote access with Prisma Access

On the other hand, Prisma Access can be deployed quickly, delivered from the cloud. Prisma Access has global reach, with more than 100 points of presence around the globe, and dynamically scales up and down, leveraging the elasticity of the cloud to support any demand. To help that end, we extend:

- **Our commitment to existing Prisma Access customers:** At no additional cost for 90 days, we're offering additional capacity to support unanticipated spikes for mobile users.
- **Our commitment to new customers:** Get Prisma Access with free QuickStart deployment services to accelerate deployment and onboarding of all remote users.

Conclusion

During these difficult times, Palo Alto Networks is dedicated to ensuring organizations can maintain business continuity with scalable access for remote employees, contractors, and partners.

Our solutions enable organizations to solve long-term VPN and disaster recovery requirements with a highly scalable, cloud-based solution that provides mass scale in a matter of hours, with minimal need for on-premises access.

To learn more, please contact your managed security service provider.

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