Secure Transformation: Replacing Remote Access VPN with Prisma Access

Remote access VPN has been an enterprise network staple for years, and for many people, the phrases "remote access" and "VPN" are synonymous. However, enterprises are rapidly adopting cloud applications that are changing the requirements for security and networking. Network and security teams are asking about how to secure access to all applications—not just those in the data center.

In light of these new requirements, is remote access VPN still relevant today, or is it time to reevaluate the role of remote access and use a better architecture?

Limitations of Remote Access

Remote access is primarily architected to do one thing: act as a gateway that allows users located beyond the perimeter firewall to access resources in the data center.

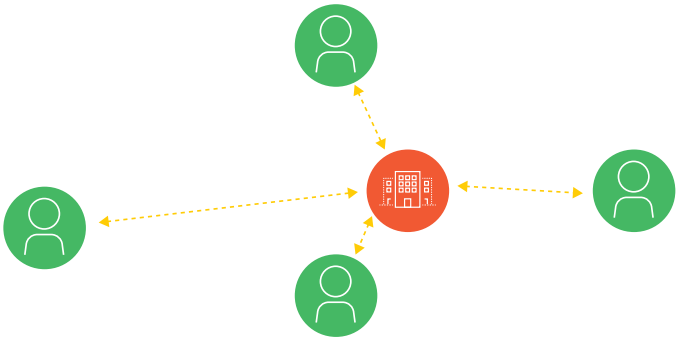

Figure 1: Traditional remote access VPN architecture

Architecturally, remote access VPN is a hub-and-spoke architecture, with users sitting in spokes of various lengths depending on their distance from the hub—the internal data center. Distance degrades performance and introduces issues with latency, but this is nevertheless the optimal architecture for data center applications because the goal is to reach the hub.

The model breaks down when there is a mix of cloud applications in the environment. Traffic in a remote access VPN always goes to the VPN gateway first, even if the application is hosted in the cloud. As a result, the traffic goes to the VPN gateway at headquarters, then egresses from the corporate perimeter firewall to the internet, with the application response going back to headquarters before it returns to the user. Traffic essentially follows a "trombone" path, making a lengthy trip to headquarters to reach a location that is accessible via the internet. Although this is sensible from a security perspective (given that headquarters has traffic inspection at the internet perimeter), it doesn't make sense for network optimization.

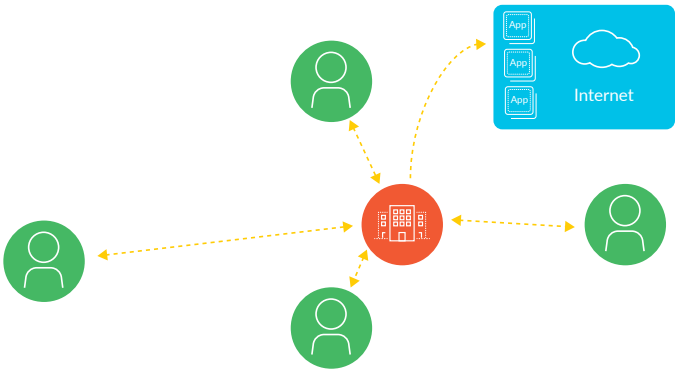

Figure 2: Traditional remote access VPN backhauling traffic to reach the cloud

Using cloud applications over remote access VPN can harm the user experience, so end users tend to avoid using remote access VPN whenever possible. Instead, they connect when they need access to the internal data center and disconnect when they do not, which leads to problems with security policy enforcement. When users are not connected, the organization loses visibility into application usage, control over access to unsanctioned applications, and the ability to enforce security.

This situation cannot be resolved by adding more VPN gateways. A remote access VPN gateway is simply a termination point for the tunnel, and it does not provide traffic inspection. Even if more VPN gateways were deployed, they would not be able to inspect traffic without additional security measures.

Unsatisfactory Compromises

To compensate for the networking problems with remote access VPN, organizations typically make compromises that have negative security implications.

- **User-initiated tunnel:** Another common remote access VPN model lets users initiate the tunnel as needed for access to the internal data center. Typically, users will connect for a short time, complete their work with a given application, and disconnect. When not connected, users again have direct access to the internet with no inspection of traffic.
- **Split-tunnel VPN:** A common but unsecure method of deploying remote access VPN is to set up a split tunnel. With a split tunnel, traffic bound for the corporate domain goes over the VPN tunnel, and everything else goes directly to the internet. This may reduce latency for internet traffic, but it means there is no traffic inspection at all for internet or cloud traffic.
- **Web proxy:** To compensate for times when the user is not connected to the VPN, many organizations have tried alternative network security measures, such as using a proxy for the web browser when users are off-network. By definition, though, a web proxy does not perform full inspection of network traffic. Even worse, the traffic the proxy does inspect will fundamentally differ from that inspected at headquarters, with inconsistent results depending on the user's location.

With the rapid growth of mobile workforces and cloud-based applications, organizations are finding remote access VPN is neither optimized for the cloud nor secure. A new approach is necessary to account for today's application mix. A Modern Architecture for the Mobile Workforce

A mobile workforce needs access to the data center, the internet, and applications in public, private, and hybrid clouds. In other words, the proper architecture should optimize access to all applications, wherever they or the users are located. Prisma™ Access provides cloud-delivered security infrastructure that makes it possible to connect users to a nearby cloud gateway, provide secure access to all applications, and maintain full visibility and inspection of traffic across all ports and protocols.

For Managed Mobile Devices

Users' managed devices—laptops, mobile phones, or tablets—have the GlobalProtect™ app installed. The app automatically connects to Prisma Access whenever internet access is available, without requiring user interaction.

Prisma Access connects applications in different locations through its connectivity layer, so users can access all their applications, whether in the cloud or the data center. The connectivity layer makes it possible to establish secure access—based on App-ID™ and User-ID™ technology policies—to public cloud, software as a service, and data center applications.

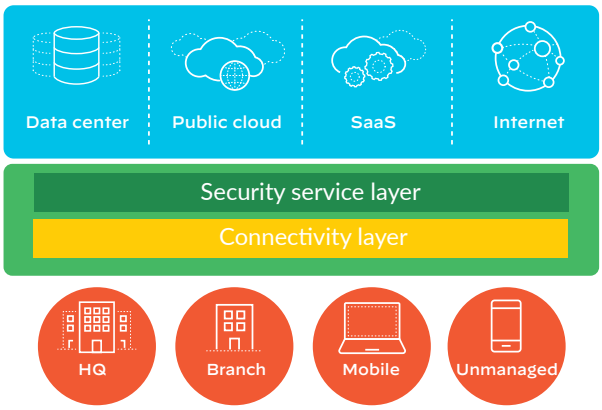

Figure 3: Cloud-delivered protection for all users, no matter where they are

Prisma Access delivers protection through the security service layer. This includes the security you count on from the Palo Alto Networks Security Operating Platform®, such as protection against known and unknown malware, exploits, command-and-control traffic, and credential-based attacks.

For Unmanaged/BYOD Devices

You can deploy Prisma Access in conjunction with mobile device management (MDM) integration to support the use of bring-your-own-device (BYOD) policies. Integration enables capabilities like per-app VPN. Users with unmanaged devices, such as contractors and employees with BYOD devices, can get remote access to the data center with clientless VPN. This approach enables secure access to SaaS applications from unmanaged devices with in-line protections by using SAML proxy integration.

Built for the Future

If you're reevaluating your remote access VPN deployment, consider making the move to an architecture designed to secure access to all applications with the protection to stop successful cyberattacks. With Prisma Access, your organization can move past the limitations of remote access VPN and support the full spectrum of applications your users need.

To learn more, visit 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

secure-transformation-replacing-vpn-with-prisma-access-sb-100820