PRISMA ACCESS
BY PALO ALTO NETWORKS

Secure the Cloud: Cloud-Enabled Mobile Workforce

Overview

As organizations adopt the cloud, new requirements for protecting and enabling mobile users are emerging. For years, the standard tool for mobile users was remote access VPN. In fact, for many people, "remote access" and "VPN" are synonymous.

However, with the number of applications and workloads moving to the cloud, the need for remote access is diminishing. In addition, it's apparent that organizations need more than remote access—they need secure access to cloud applications and the internet as well.

In light of the fundamental changes introduced by cloud adoption, is remote access VPN still relevant today, or is it time to reevaluate the role of remote access and use a better architecture?

The Limitations of Remote Access

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

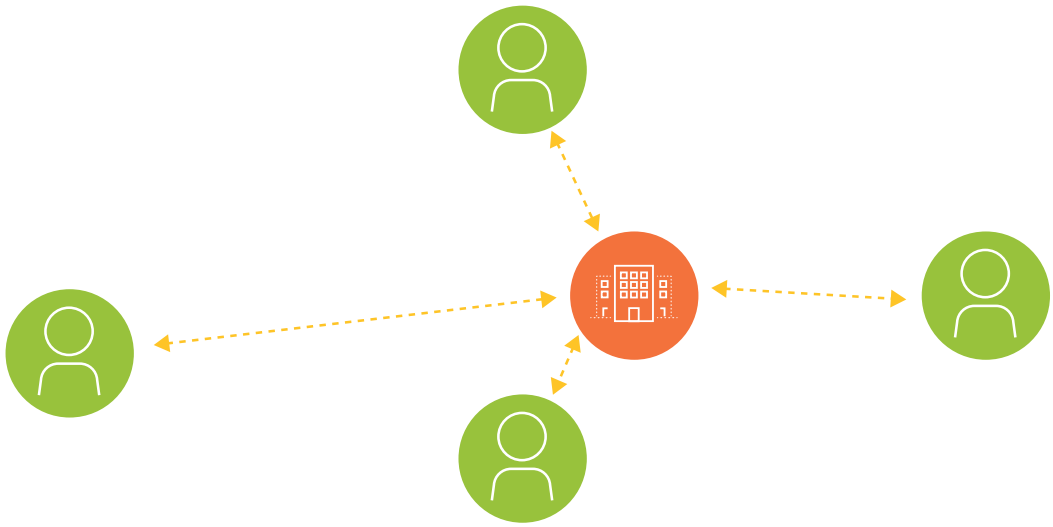

Figure 1: Traditional remote access VPN architecture

Remote access VPN uses a hub-and-spoke architecture, with users connected by tunnels of various lengths depending on their distance from the data center. Nearby users may enjoy high performance, but distance degrades performance, introducing issues with speed, bandwidth, and latency. Nevertheless, this is the optimal architecture for data center applications because the goal is to reach the "hub" where your internal data center is located.

The model breaks down when a mixture of cloud applications is involved. With remote access VPN, traffic 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. With cloud applications, this traffic essentially follows a "trombone" path, making a lengthy trip to headquarters to reach an internet-accessible location. This is sensible from a security perspective if your headquarters has traffic inspection at the internet perimeter, but it doesn't make sense for network optimization.

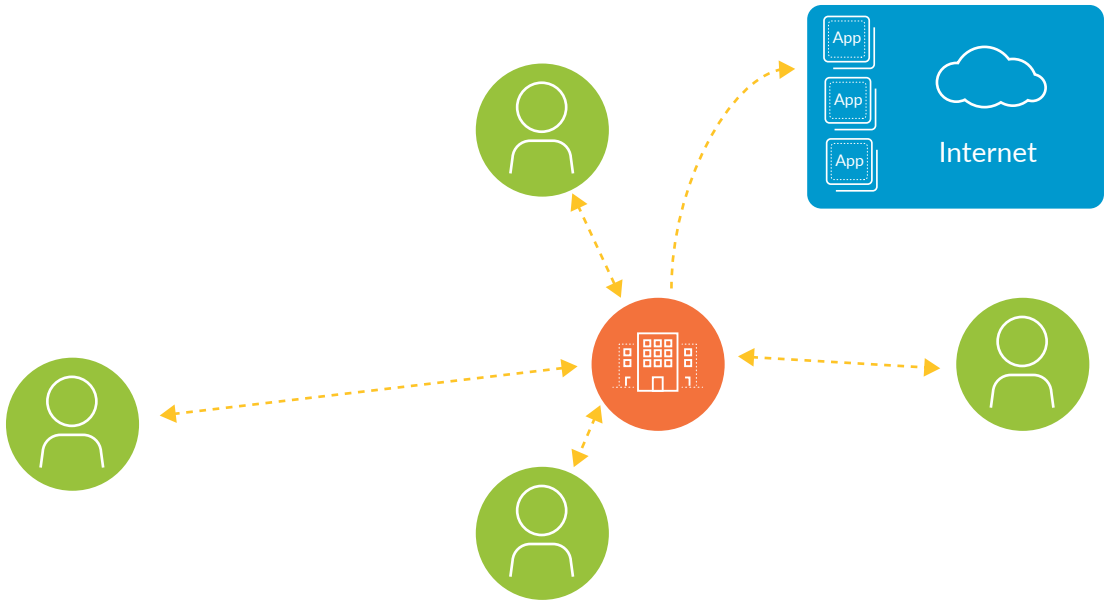

Figure 2: Traditional remote access VPN backhauling traffic to reach the cloud

Using cloud applications over remote access VPN can hurt the user experience, and as a result, end users tend to avoid using remote access VPN whenever possible. They tend to connect when they need access to the internal data center and disconnect when they do not, which leads to multiple issues. When users are disconnected, their organizations lose visibility into application usage, control over access to unsanctioned applications, and the ability to enforce security.

This situation cannot be solved by adding more VPN gateways. A remote access VPN gateway is simply a termination point for a tunnel, and it does not provide any traffic inspection. For that, you need additional security measures.

Unsatisfactory Compromises

To compensate for the networking problems with remote access VPN, IT teams typically introduce a number of compromises with certain security implications:

- **User-initiated tunnel:** A common remote access VPN deployment model is to let users initiate the tunnel as needed. Typically, they will connect for a short time, complete their work with a given application, and disconnect. When disconnected, they have direct access to the internet with no traffic inspection.
- **Split-tunnel VPN:** A common yet insecure method of deploying remote access VPN is to set up a policy that permits split tunnel. In this model, traffic bound for the corporate domain goes over the VPN tunnel, and everything else goes directly to the internet. The improvements in network performance come at a cost, though: there is no traffic inspection at all for internet and cloud traffic.
- **Web proxy/secure web gateway:** To compensate for scenarios when users are 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. However, by definition, a web proxy does not fully inspect network traffic. Even worse, the traffic inspection the proxy does perform will be fundamentally different from the inspection that's happening at headquarters, with inconsistent results depending on users' locations.

With the rapid growth of mobile workforces and cloud-based applications, organizations are finding that their 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

The mobile workforce needs access to the data center and the internet as well as applications in the public, private, and hybrid cloud. A proper architecture should optimize access to all applications, wherever they or your users are located. Prisma™ Access (formerly GlobalProtect™ cloud service) provides cloud-delivered security infrastructure that makes it possible for your organization to connect users to a nearby cloud gateway, enable secure access to all applications, and maintain full visibility and inspection of traffic across all ports and protocols.

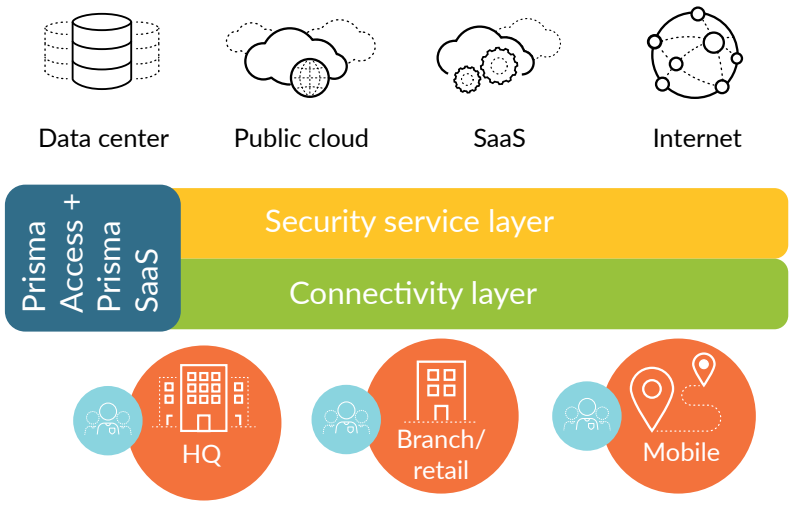

Figure 3: Easy access to the connectivity layer, wherever your users are

For managed mobile devices:

- Users with managed devices have the GlobalProtect app installed on their laptop, mobile phone, or tablet. The GlobalProtect app connects to Prisma Access automatically whenever internet access is available, without requiring any user interaction.
- Users can access all of their applications, whether in the cloud or the data center. The connectivity layer connects applications in different locations, making it possible to establish secure access (based on App-ID™ and User-ID™ technology policies) to public cloud, software as a service (SaaS), and data center applications.
- Prisma Access delivers protection through the security service layer, such as protections against known and unknown malware, exploits, command-and-control (C2) traffic, and credential-based attacks.

For unmanaged/BYOD devices:

- Your organization can deploy Prisma Access in conjunction with Mobile Device Management (MDM) integration to support bring-your-own-device (BYOD) policies. The integration enables capabilities such as per-app VPN.
- Users with unmanaged devices, such as contractors and employees with BYOD devices, can access applications without an app installed by using Prisma Access with Clientless VPN.
- Clientless VPN also enables secure access to SaaS applications from unmanaged devices with inline protections by using SAML proxy integration. This functionality works in conjunction with Prisma SaaS.

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 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.

Built for the Future

No matter where you are on your journey to the cloud, Prisma can help:

- Cloud-enabled mobile workforce
- Cloud-connected branch
- Zero Trust cloud security
- Cloud governance and compliance
- Cloud data protection
- Cloud threat protection
- Secure DevOps

To learn more about how Prisma can secure your key cloud initiatives, visit www.paloaltonetworks.com/prisma.

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

secure-the-cloud-cloud-enabled-mobile-workforce-b-052319