Secure Remote Access with Palo Alto Networks and Okta

Benefits of the Integration

Palo Alto Networks and Okta offer a joint solution that:

- Enables business agility with integrated, cloud-delivered services that deploy quickly, scale to meet demand, and are centrally managed.
- Lowers risk to the business from cyberattacks and reputation-damaging security breaches.
- Reduces cost and complexity by eliminating security point products and decreasing on-premises hardware.
- Improves user productivity with a consistent, responsive, and secure experience from any location, for all applications, regardless of the device.

The Challenge

For many organizations, more and more users, data, and services are located outside the protection of the traditional network perimeter. At the same time, employees are using dozens of applications—including on-premises and software-as-a-service (SaaS) apps—to accomplish their work. Typically, organizations have deployed an array of point products to handle different security requirements for remote workers, such as secure web gateways, application firewalls, secure virtual private network (VPN) access, cloud access security brokers (CASBs), and more. This not only increases administrative costs and complexity, but also makes for inconsistent user experiences. If an organization has not implemented single sign-on (SSO), user experiences become even more complex, and the situation starts to impact remote worker productivity.

Okta

The Okta Identity Cloud makes it easy for organizations to securely connect their users with the resources they need to do their job. Okta centralizes access to SaaS apps, web access management (WAM) and custom web apps, APIs, and infrastructure. Users sign in with one set of credentials to access all of the resources they need to be productive, wherever and on whatever devices they choose. Administrators can assign resources relevant to a user's role and set access policies based on role, the resource the user is trying to access, and more. You can prompt for a second factor based on risk signals from the device, network, geography, etc.—or, if risk is low, you can allow for a passwordless experience. Finally, Okta can centralize user stores from on-premises systems such as Active Directory® or LDAP, as well as HR systems such as Workday®, and automate on/offboarding of applications, saving administrators time and reducing the risk of misconfigurations.

Palo Alto Networks

Prisma™ Access by Palo Alto Networks is a secure access service edge (SASE) solution that provides network connectivity and consistent security to mobile users and branch offices anywhere in the world. It simplifies networking and security, replacing conventional point products such as firewalls, proxies, secure web gateways, remote access VPNs, CASBs, DNS security solutions, and more. Prisma Access supports the Zero Trust network access (ZTNA) model, driving identity-based access controls to applications while maintaining full visibility and inspection of network traffic to stop threats and control data movement. If you are an existing Palo Alto Networks Next-Generation Firewall customer, you can provision these same services on your on-premises or cloud-deployed firewalls. Both options enable you to extend consistent security policies to remote workers.

Prisma SaaS works with Prisma Access to address your CASB needs and provide deep visibility into SaaS risks, data protection, leakage prevention, data governance, compliance assurance, advanced threat prevention, and more.

Palo Alto Networks and Okta

Quickly and confidently embrace remote workforce initiatives with Okta and Palo Alto Networks. Integrated security capabilities reduce the risk of successful cyberattacks and reputation-damaging security breaches while reducing cost and complexity. A consistent experience securely connects users to the tools they need to work, whether on-premises or in the cloud, improving productivity and satisfaction from any location and for all applications. Prisma Access and Prisma SaaS by Palo Alto Networks as well as Okta remote access services are based in the cloud, which means they deploy quickly, scale with demand, and reduce both on-premises hardware and the operational load on network and security teams.

For customers with Palo Alto Networks Next-Generation Firewalls, GlobalProtect™ network security for endpoints—a firewall subscription—offers the same secure remote access service as Prisma Access.

Use Case No. 1: Enable Seamless, Secure Remote Access

Challenge

Traditional VPNs are designed for users to access the data center, so traffic to the internet or SaaS apps often "hairpins" through a data center, impacting performance and scalability. If a user's experience is cumbersome, they may turn off their VPN for internet access or use personal credentials to log in to SaaS applications, putting data security at risk and exposing their device—and your network—to threats the next time they connect.

Solution

With Palo Alto Networks and Okta, your remote workers enjoy the same simple, convenient identity management and secure connection experience whether they are accessing the internet; SaaS; or public, hybrid, or private clouds. Prisma Access and its client app, GlobalProtect, offer an always-on connection for a range of operating systems and devices, eliminating the need to start a VPN or log in to a secure web gateway. Prisma Access is cloud-delivered, scales with demand, and inspects all traffic for threats 24/7.

Okta's SSO, part of the Okta Identity Cloud, integrates with Prisma Access to ensure users only need to enter a single set of credentials, rather than remember different passwords and authentication schemes for different applications. With centralized, identity-driven security policies, IT can provision access only to the resources a particular user needs, and workers can seamlessly get access to the tools they need to be productive from anywhere. Once users are authenticated, you may configure Prisma Access to apply additional security policies, such as preventing users from visiting websites associated with phishing or hacking.

Use Case No. 2: Strengthen Security with MFA

Challenge

Many environments require multi-factor authentication (MFA) to enhance security for critical systems or meet compliance requirements. However, it is often difficult or time-consuming to rearchitect application login processes to add MFA.

Solution

Okta Adaptive MFA, part of the Okta Identity Cloud, also integrates with Prisma Access, allowing Okta customers to quickly set MFA policies without needing to take critical resources offline. You can configure Prisma Access to enforce MFA for some or all users and/or applications, so you don't have to change existing applications to meet security requirements. With Okta's Adaptive MFA solution, you can also leverage robust risk signals (e.g., from an IP address, device, or geography) to inform potential risk around a particular authentication attempt. You can set policies to step up MFA if high risk is detected, or even provide a password-less experience if risk is low.

Use Case No. 3: Support BYOD

Challenge

Students, contractors, and partners need access to applications and data while using their own devices. Corporate employees often access applications from their personal mobile devices. They don't want to install client software—but you want to validate access, secure data in transit, protect your environment from unmanaged devices, and prevent data leakage (e.g., sensitive files downloaded to unmanaged devices).

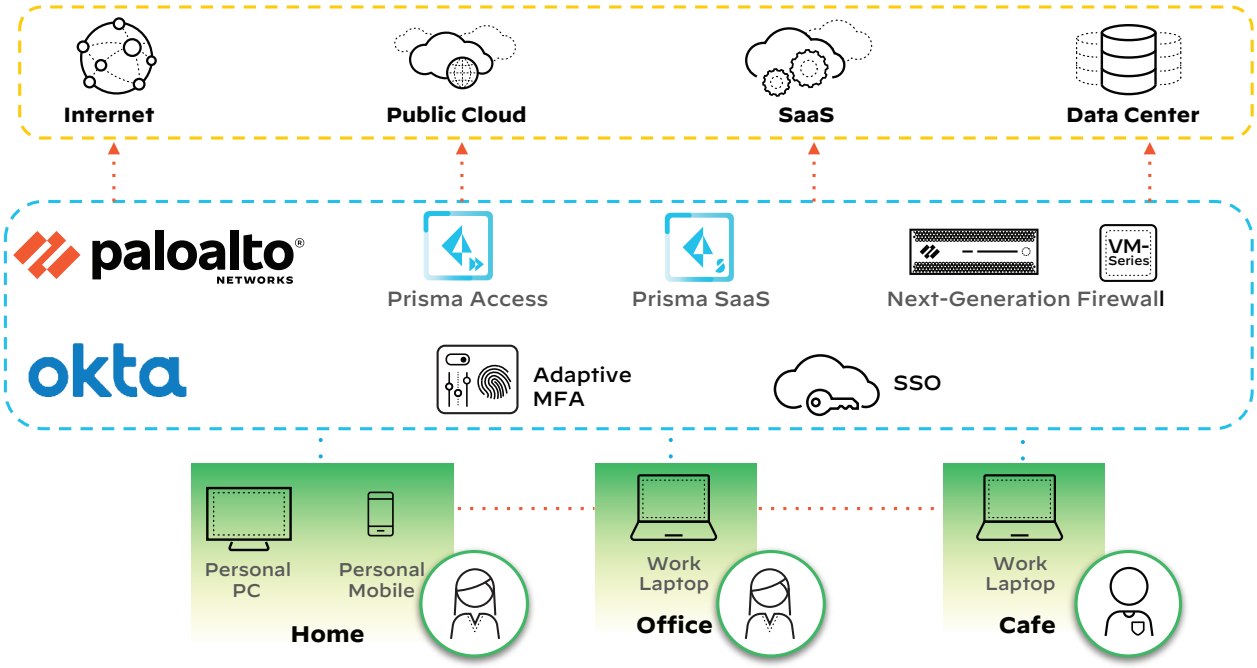

Figure 1: Palo Alto Networks and Okta integration—consistent security for remote workers, no matter where they are

Solution

Palo Alto Networks and Okta can secure remote access to enterprise and SaaS applications without the need to install client software on unmanaged devices. With Okta, Prisma Access, and Prisma SaaS, remote users with valid credentials can log in to a portal using a secure web browser and launch on-premises and sanctioned SaaS applications you make available to them. Using Okta's flexible policy engine, you can set additional identity-driven security policies, such as limiting the applications users can access or the actions they can perform on unmanaged devices. Once again, you can apply security policies to authenticated users through Prisma Access; for example, you may want to disable file downloads for certain applications to maintain data privacy.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Nearly 8,000 organizations, including Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile and Twilio, trust Okta to help protect the identities of their workforces and customers.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

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