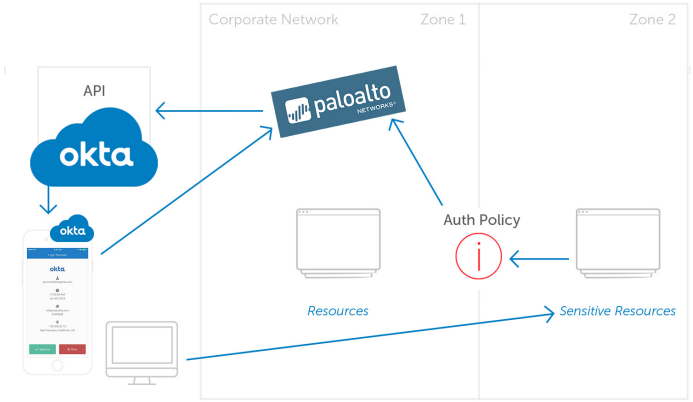
Okta and Palo Alto Networks Integration for Authentication and Access Control

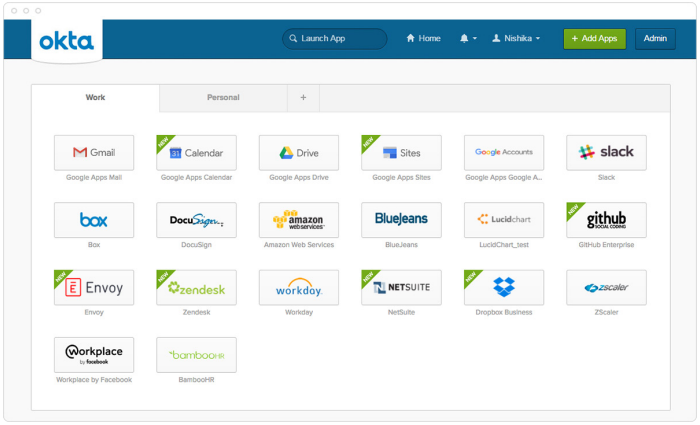
With the ever increasing use of stolen credentials in lateral movement, the ability to enforce secure authentication policies to sensitive corporate applications and data is a top concern. This is compounded by the growing mix of applications in the cloud that complement or replace applications in the data center, bringing its own set of authentication and access requirements. It is growing more important to find ways to bring identity and security together, to integrate and unify everything for easier administration and boost end-user production, while further enhancing the protection of data.

Palo Alto Networks and Okta have partnered to help organizations bring identity and security together for the enforcement of access policy, regardless of where customer applications reside. The Palo Alto Networks next-generation firewall delivers the identity-based enforcement of network traffic policies using Okta authentication and identity management. With this integration, Okta Multi-Factor Authentication (MFA) can be used to secure any internal application, irrespective of its support for RADIUS or other enterprise authentication protocols. This enables organizations to pervasively deploy MFA across all their applications - cloud and data center, legacy and modern.



Multi-Factor Authentication integration with Okta

One of the core functions of the next-generation firewall is a set of identity-based enforcement technologies. When used with Multi-Factor Authentication policy, the firewall can control network access based on authentication through Okta MFA. Palo Alto Networks uses the Okta MFA API for this integration. This has several benefits. First, the organization can use their Okta rollout directly with Palo Alto Networks without having to stand up a separate RADIUS server just for MFA if they choose, immediately reducing IT costs and resources. Second, the tight integration takes advantage of the advanced Okta MFA policies for better fine-grained access. Finally, Palo Alto Network customers can take advantage of the Okta MFA options including a mobile device soft token (on iOS, Android or Windows Phone), hard tokens such as Yubikey, SMS, or voice as well.



Okta and Palo Alto Networks Integration for Authentication and Access Control

okta

Single Sign-On integration with Okta

Palo Alto Networks supports SAML 2.0 as an authentication profile in PAN-OS 8.0. Now Palo Alto Networks customers can get seamless single sign-on to all SAML-enabled applications including those enabled through the 5000+ applications in the Okta Application Network. Okta also has full support for federation protocols for additional applications that support federation standards. Applications in the cloud with any kind of login form can, additionally, be easily added to Okta.

Palo Alto Networks supports SAML authentication profile with the GlobalProtect client, Captive Portal, SSL VPN, and administrative UI modules.