Ping + Palo Alto Networks

Quickly Deploy & Centrally Enforce Secure Access

PALO ALTO NETWORKS
SOLUTION BRIEF

STREAMLINE DEPLOYMENT & MANAGEMENT OF MULTI-FACTOR AUTHENTICATION

Attackers are on the lookout for the weakest link in an enterprise's defenses, and they often find it in stolen or weak credentials. Multi-factor authentication (MFA) thwarts phishing attempts and other credential abuse tactics by requiring users to provide at least two forms of identification to prove they are who they claim to be.

While MFA strengthens security, deploying MFA across today's enterprise can present obstacles. Rigid SCADA systems, mainframe servers and other on-premises applications typically can't support modern authentication but are increasingly being targeted by attacks. And convincing app developers to do the heavy lifting required to update legacy applications to support MFA can be a big ask.

As more and more workers are working remotely whether out of necessity or by choice, you must also provide secure access to both on-premises and cloud applications. But deploying MFA across this type of hybrid environment presents challenges. Even if you overcome them, your app developers must collaborate with IT security teams to QA test, manage and support MFA for each and every application.

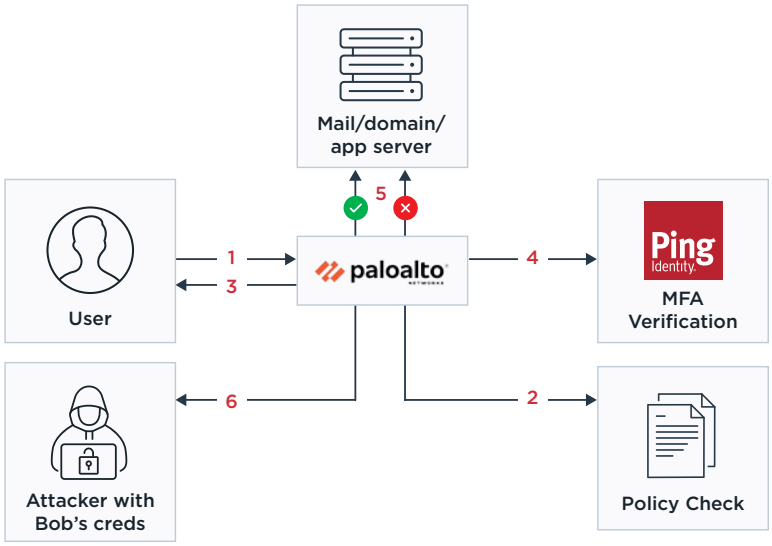
Enter Ping Identity and Palo Alto Networks. The integration between Ping's multi-factor authentication solution and Palo Alto Networks' Next-Generation Firewall simplifies the configuration, management and deployment of MFA, so you can effortlessly roll out strong authentication across your organization.

HOW PING & PALO ALTO NETWORKS WORK TOGETHER

Because it can be challenging to integrate custom and legacy applications, many enterprises enforce MFA on their most critical assets in a handful of locations. As a result, they leave some applications, including sensitive test and development applications, susceptible to credential abuse.

The integration between Ping Identity and Palo Alto Networks eliminates the need to update and manage MFA enforcement at different locations in your enterprise. Your users are able to authenticate using the PingID convenient mobile app. Palo Alto Networks' Next-Generation Firewall serves as the MFA gateway. Whether your users request access to web applications or thick client applications, the firewall serves as the centralized point for authentication and access control.

By enabling authentication policy control at the firewall, the integration makes it possible to enforce MFA without needing to modify your applications or servers. Administrators can configure settings, including defining which applications require strong authentication and how frequently users must reauthenticate, from the same interface where they define firewall security policies. With Ping + Palo Alto Networks, you can effortlessly roll out multi-factor authentication across your network.



1) Bob initiates access to an application in the mail server. 2) Palo Alto Networks' Next-Generation Firewall intercepts, checks if a policy allows access and serves up a captive portal for authentication. 3) Bob is prompted with an MFA challenge and authenticates. 4) Ping verifies Bob for authentication. 5) Bob can now access the application in the mail server. 6) If an attacker attempts to access a resource with Bob's stolen credentials, they fail MFA verification with Ping and can't gain access.

WHAT ARE THE BENEFITS?

- **Deploy Easily:** Enforce MFA across your organization—including on-premises applications and critical systems like SCADA and mainframe servers—without needing to recode or install web proxies.
- **Lower IT Burden:** Reduce IT helpdesk calls by supporting single sign-on (SSO) with a convenient mobile app.
- **Customize Authentication Policies:** Define and enforce policies to meet your specific requirements.
- **Meet Regulatory Requirements:** Comply with PCI DSS and HIPAA requirements for strong authentication and access controls.

Ping Identity

Ping Identity delivers intelligent identity solutions for the enterprise. We enable companies to achieve Zero Trust identity-defined security and more personalized, streamlined user experiences. The PingOne Cloud Platform provides customers, workforce and partners with access to cloud, mobile, SaaS and on-premises applications across the hybrid enterprise.

Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that's transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

For more information about how Ping Identity and Palo Alto Networks joint solutions can help your business, contact us.