Palo Alto Networks and Thales Group

Identity and Access Management to protect the most sensitive area of your network: your users

The Challenge

Weak or stolen passwords lead to the majority of data breaches. Passwords are not enough to protect networks from phishing attacks and insider threats. Today's users work remotely, access up to 27 applications each day, and frequently access hybrid deployments. To keep pace with users, organizations are adopting conditional single sign-on (SSO) solutions at the access entry point. Shifting enforcement to the access entry point enables today's users to access applications efficiently while keeping networks secure against evolving threats that can strike at any time, from outside or inside the network.

Benefits of the Integration

Integration between Palo Alto Networks Next-Generation Firewalls and Thales Group's Authentication and Access Management solutions enables you to:

- **Prevent unauthorized access:** Use the broadest range of authentication methods in the industry, including MFA as well as contextual, adaptive, and pattern-based authentication.
- **Reduce login burden for end users:** Keep users productive with Smart SSO and reduce helpdesk calls.
- **Speed up deployment:** Reduce overhead with automated token lifecycle management and unlimited software tokens.
- **Ensure compliance with security regulations:** Avoid penalties with extensive audit trails.
- **Enable Zero Trust:** Centrally manage user access and security policies across on-premises and multi-cloud environments.
- **Secure traffic and gain greater visibility:** Reduce the attack surface and stop threats with consistent security policies while eliminating remote access blind spots and strengthening security.

Palo Alto Networks

Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) inspect all traffic at Layer 7 and offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

ML-Powered NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The application, content, and user—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

GlobalProtect™ network security for endpoints enables you to protect your mobile workforce by extending NGFW security to all users, regardless of location. It secures traffic by applying the platform's capabilities to understand application use, associate the traffic with users and devices, and enforce security policies with next-generation technologies. By extending NGFW capabilities through the GlobalProtect subscription, you can gain greater visibility into all traffic, users, devices, and applications.

Thales

Thales' industry-leading Authentication and Access Management solutions let enterprises centrally manage and secure access to enterprise IT, web, and cloud-based applications with a Zero Trust approach. Utilizing policy-based conditional access, rigorous SSO, and universal authentication methods, enterprises can effectively prevent breaches, migrate securely to the cloud, and simplify regulatory compliance.

Palo Alto Networks and Thales

Thales' SafeNet Trusted Access (STA) enforces a broad range of authentication methods at the access point while the Palo Alto Networks NGFW inspects traffic, enforces network security policies, and delivers threat prevention, enabling organizations to achieve Zero Trust network security.

With the strong multi-factor authentication (MFA) offered by Thales, weak passwords are replaced by strong, adaptive authentication to add a security layer that validates users and logs their access attempts for audit purposes. By combining Palo Alto Networks NGFW with Thales strong authentication and access management solutions, businesses can meet strict compliance requirements with an elegant solution that ensures the utmost in network protection.

Securing identities and ensuring secure and convenient access to resources is a crucial component of a modern identity and access management (IAM) approach. Stolen

user identities can have serious consequences as they can provide unfettered access to an organization. Implement robust identity management to ensure a secure, compliant, and efficient environment to protect the organization.

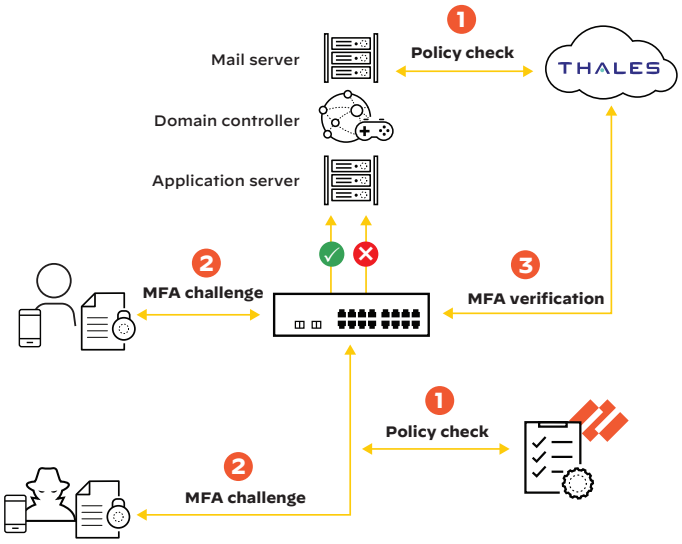

Figure 1: Comprehensive security provided by STA and Palo Alto Networks

Table 1: Thales Supported Authentication Methods	
OTP push	Kerberos
OTP app	PKI credentials
OTP hardware	Google Authenticator
Pattern-based authentication	Passwordless authentication
Out-of-band via email and SMS text messages	Biometric
Password	Voice
	Third party

Use Case 1: Data Privacy and Compliance

Challenge

Insider threats are a leading cause of high-profile data breaches. A data breach is not only a business continuity threat, but also a big threat to an organization's brand reputation. The cost of a data breach has led to many regulations that mandate the use of MFA, especially for privileged users privileged users, such as administrators, who access sensitive network security components like NGFWs.

Solution

STA protects access to GlobalProtect and enables Palo Alto Networks customers to use a wide variety of FIPS- and CC-certified authentication tokens in different form factors. Organizations concerned with regulations like PCI DSS, HIPAA, or NERC CIP can rely on the combined value of STA and GlobalProtect to address both insider and external threats.

Use Case 2: User Experience and Remote Work

Challenge

CISOs are often met with the challenge of balancing security with user experience. This challenge, coupled with shadow IT and hybrid IT, makes the balance even harder to achieve. Organizations need a solution that helps them enforce the right level of security for the right user and use case.

Solution

In conjunction with the network segmentation capabilities of GlobalProtect, STA offers flexibility to the IT team to configure granular policies for different groups of users. A remote administrative worker, for example, can be configured to use an OTP token to gain access to a privileged application, whereas a remote sales executive could use a Thales FIDO2 token or a mobile authenticator like MobilePASS+ to gain access to a customer relationship management (CRM) application. This adaptive SSO capability can help IT create the right user experience for each use case and user group.

Palo Alto Networks and Thales Product Integrations

Product integrations between Palo Alto Networks and Thales include:

- IAM with Palo Alto Networks and Thales Group
- Palo Alto Networks NGFWs with Thales Luna HSM

About Thales

The people you rely on to protect your privacy, rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation. Decisive technology for decisive moments. For more information, visit https://cpl.thalesgroup.com/contact-us.

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. 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