

Thales and Palo Alto Networks

Adding protection to the most sensitive area of your network – your users



The IT perimeter is changing and organizations need to be able to implement secure and seamless access to applications from any location for their users. By combining the solutions offered by Thales and Palo Alto Networks, organizations can implement access controls and deploy multi-factor authentication while balancing security and user experience.

The Challenge

Corporate infrastructures are changing and the traditional IT perimeter is becoming blurred as more organizations diversify and are faced with maintaining security in hybrid deployments which consist of a mix of legacy, custom, and cloud applications.

Some legacy or custom applications may not always support the use of anything other than a password. This becomes problematic as studies have highlighted that 81% of data breaches are due to stolen or weak passwords¹.

Securing users within an environment is becoming a crucial component to ensuring the security measures put in place offer complete protection. Deploying multi-factor authentication and access controls aide organizations in thwarting a wide range of breach attempts by mitigating the potential of credential abuse – including pass-the-hash attacks, brute force attacks and more.



By deploying Palo Alto Networks Next Generation Firewall with Thales's Authentication and Access Management solutions you can streamline deployment of strong authentication and increase the protection of your infrastructure efficiently without needing to replace any existing components.

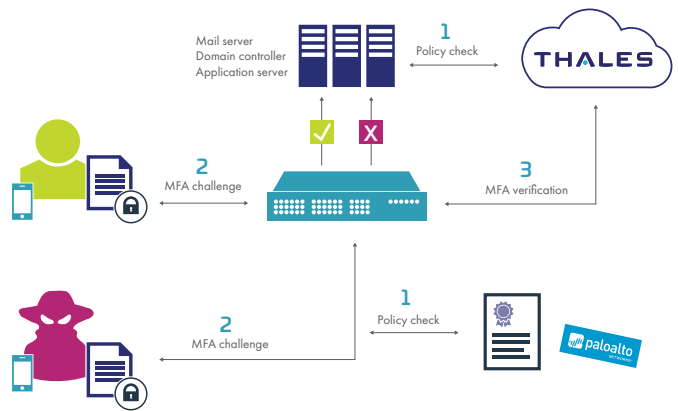
Key Benefits

- Versatile integration methods to support hybrid deployments
- Automated multi-factor token lifecycle management
- Enforce strong authentication based on risk evaluation of network, device OS and location
- Centrally manage access policies for applications
- Reduced IT helpdesk and infrastructure costs
- Prevents unauthorized access
- Enables compliance with security regulations
- Supports OOB/Push authentication
- Balances Security with Usability
- Unlimited Software Tokens
- Multiple Authentication methods per user supported

Thales's Authentication and Access Management Solutions

Thales's SafeNet Trusted Access combines easy to deploy access management and strong authentication allowing organizations to balance security with the end user experience. SafeNet Trusted Access enables administrators to create access policies that evaluate risk conditions and validates users by enforcing strong authentication where needed, ensuring the right people have access under the right conditions.

Thales solutions are offered as a cloud service simplifying adoption and enabling organizations to automatically and rapidly deploy a strong layer of security without any additional infrastructure investment.



Thales and Palo Alto Networks

While Palo Alto Networks Next-Generation Firewall inspects traffic, enforces network security policies, and delivers threat prevention, Thales's SafeNet Trusted Access solution adds additional risk evaluations and enforces the need for strong authentication where needed. With the strong, multi-factor authentication offered by Thales, weak passwords are replaced by an additional security layer that validates users, and logs their access attempts for audit purposes. By combining Palo Alto Networks Next-Generation Firewall with Thales's strong authentication and access management solutions businesses can meet strict compliance requirements with an elegant solution that ensures the utmost in network protection.

Strong Authentication

SafeNet Trusted Access platform supports a wide range of two-factor authentication options, including traditional AD password, hardware tokens, software tokens, web-based tokens and certificate based authenticators. This allows users to authenticate from anywhere at any time. With access policies, organizations can define what type of authentication is needed, and offers the capability to combine authentication methods. SafeNet's MobilePass+ supports out-of-band push authentication on mobile devices which provides a streamlined user experience while enforcing a strong authentication method. By leveraging the existing user repository organizations can set up automation policies that will provide users with an authentication method without IT involvement. The simple and user friendly self-service options empower users to adopt the use of multi-factor authentication in a frictionless way which increases user deployment without overburdening the IT helpdesk.

Powerful Access Controls and Centralized Management

Access policies can be set up in SafeNet Trusted Access based on application or group membership, centralizing the management of security policies against the entire environment. Integration options enable organizations to protect their GlobalProtect and extend the

enforcement of multi-factor authentication to all the applications in their environment. The flexible policy engine permits administrators to set policies which evaluate risk conditions and implements stronger controls for users who are accessing resources from older operating systems and mobile devices, or augment the firewall policies set in the Palo Alto Networks devices to deny access from certain geographic locations. Add further protection with SafeNet Trusted Access to other sensitive applications by setting policies which require multiple authentication methods. All of this is managed through a centralized console which provides real-time analytics and empowers administrators to quickly and easily adjust policies based on business and compliance requirements.

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.

About Palo Alto Networks

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and endpoints. Find out more at <https://www.paloaltonetworks.com>.

> thalescpl.com <



Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax: +1 954 888 6211 • E-mail: sales@thalessec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com