Security Service Edge and Application Security

Zero Trust

As the global cybersecurity leader, Palo Alto Networks protects more than 85,000 government and enterprise customers worldwide. We are uniquely positioned to support federal agencies in addressing Zero Trust strategy requirements prescribed in the January 2022 U.S. Office of Management and Budget (OMB) memorandum M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. This federal Zero Trust architecture strategy aims to advance agencies' security capabilities to comply with the May 2021 White House Executive Order on Improving the Nation's Cybersecurity. Palo Alto Networks can supplement agencies' perimeter defense capabilities while allowing direct internet access for critical applications needed to support agency missions. We provide integrated capabilities that are flexible enough to secure all traffic, applications and users, no matter where they reside or where the applications and data live.

Unprecedented Security Mandates

Federal agencies and departments are modernizing their network security to defend against endless cyberthreats while enabling an increasingly mobile workforce. In doing so, agency practices must align with new directives like the Executive Order, OMB Zero Trust memorandum and National Defense Authorization Act. These directives require agencies to make significant changes to address cybersecurity in a timely way.

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. The Palo Alto Networks Prisma® technology suite allows agencies to streamline endpoint security solutions, enhancing the security posture needed for increased adoption of cloud technologies and mobile users. By extending current firewall policies to the edge, agencies can migrate to a new Zero Trust architecture seamlessly.

Secure Access Service Edge Offers a Holistic Approach

In 2019, research and advisory firm Gartner identified a new networking and security model called secure access service edge (SASE). This model combines wide area networking (WAN) and network security services, such as Zero Trust Network Access (ZTNA), cloud access security broker (CASB) and firewall as a service (FWaaS) into a single, comprehensive and integrated solution supporting all traffic, applications and users. This new model allows agencies to rapidly authenticate users, identify and mitigate potential security threats and fully inspect content.

By converging SD-WAN with a comprehensive and cloud-delivered security stack, SASE removes the need for agencies to maintain separate infrastructure for internet and private applications, as was once the case with conventional proxy- and software-defined perimeter products. Combining SASE and Zero Trust principles empowers agencies to achieve ZTNA with a single solution that can consistently apply and enforce security policies across the entire network.

How Palo Alto Networks Meets Zero Trust Tenets

A pioneer in Zero Trust, Palo Alto Networks provides the most comprehensive set of capabilities aligned with the National Institute of Standards and Technology (NIST) SP 800-207 Zero Trust Architecture publication and the Department of Defense (DOD) Zero Trust Reference Architecture Version 1.0. Prisma Access enables true end-to-end ZTNA with common policy enforcement, along with full Layer 7 visibility over all ports and protocols. Rather than focusing on the enterprise data center, Palo Alto Networks Prisma SASE delivers cloud-based converged capabilities where and when agencies need them. Aligning physical, virtual and SASE infrastructure policy enforcement facilitates the improved incident response objectives of the Executive Order.

Our industry-defining Next-Generation Firewall (NGFW) operating platform called Palo Alto Networks PAN-OS® is the foundation for our solution with Prisma Access. Palo Alto Networks is both a ten-time Gartner Magic Quadrant NGFW leader and Forrester Research leader in Zero Trust extended ecosystem providers. The platform enables extension of common policy and ZTNA policy enforcement points across physical, virtual and FWaaS form factors, meeting the tenets of an effective end-to-end Zero Trust architecture implementation, which include:

- Ensure all resources can be securely accessed, regardless of their location.
- Leverage a least-privileged access strategy and strictly enforce access control.
- Inspect and log all traffic.

Complying with these tenets is essential to fulfilling the OMB memo requirement to define users, applications and content that will be included in the Zero Trust environment. Palo Alto Networks User-ID™, Application-ID™ and Content-ID™ agents come standard in every PAN-OS device. Our fully integrated capabilities enable visibility and control over users, applications and content, rather than relying on incomplete and/or continually changing information like a user's IP address or current location relative to the security perimeter.

What's more, our Palo Alto Networks Panorama™ centralized management system provides a single-pane view of security configuration across all NGFWs in an enterprise, allowing agencies to achieve predictable levels of performance even for complex, hybrid computing environments.

Prisma Access Blends Security and Networking Capabilities

Palo Alto Networks Prisma Access, a dynamic, cloud-delivered security service, empowers agencies to protect distributed infrastructure, users and applications by extending ZTNA enforcement policies for mobile users and remote locations. When coupled with existing NGFWs, the solution enables a consistent security approach that supports agencies' compliance with recent government mandates, including: a secure, enhanced user experience; cloud scale and agility; reduced risk exposure; and more efficient and direct mobile access to internal data center, cloud and legacy resources.

Prisma Access works together with the Palo Alto Networks GlobalProtect™ application, which is available on most smartphones, tablets and laptops. GlobalProtect automatically establishes a secure connection to Prisma Access to enforce security policy without requiring a backhaul to headquarters. Together, Prisma Access and GlobalProtect establish access policies based on host information profile (HIP), enabling granular security policies tied to device characteristics. Prisma Access can also simplify remote branch (B/C/P/S) connectivity, leveraging low-cost commodity internet and providing direct, secure cloud access.

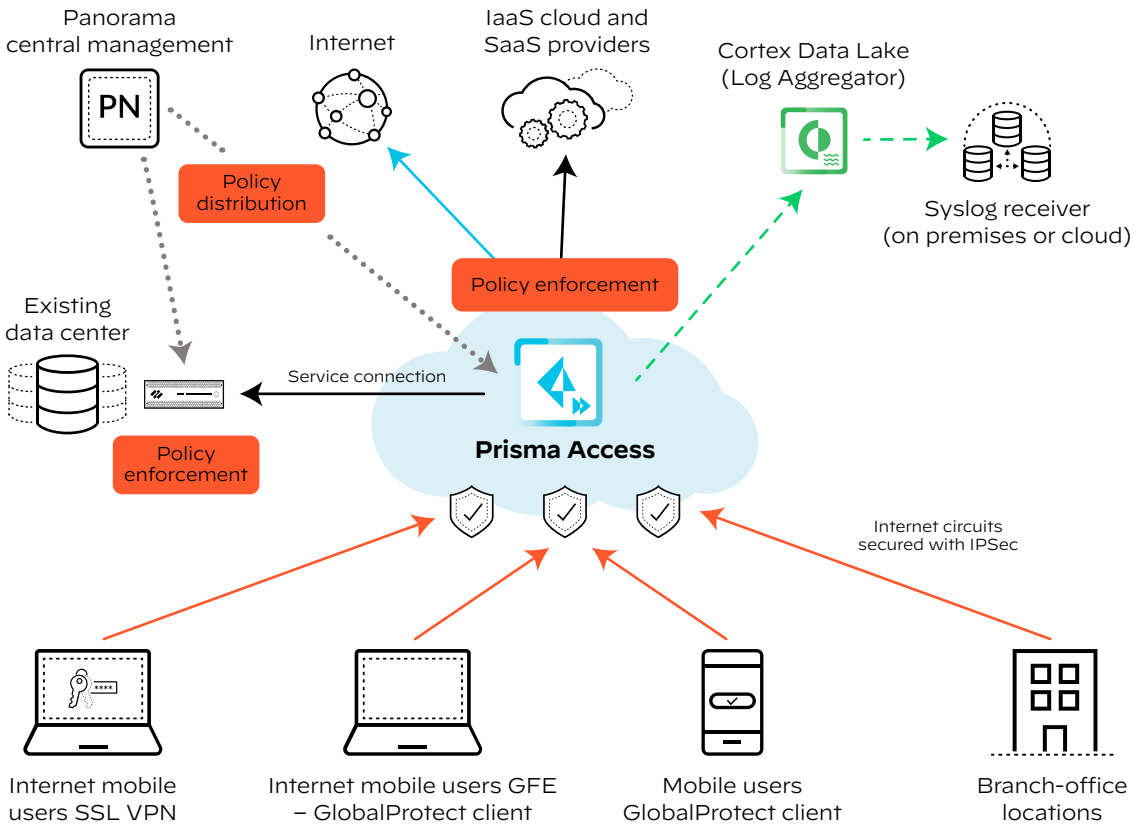

Figure 1: Prisma Access for mobile users

Figure 1 depicts the Prisma Access architecture, showing users connecting to Prisma Access and securely accessing the data center, cloud service and internet. Prisma Access reduces architecture and management complexity while maintaining a consistent set of security policies for users regardless of location, and ensures compliance with policy enforcement initiatives.

The Executive Order on Improving the Nation's Cybersecurity also sets investigative and remediation capability goals of enhanced event logging and log visibility, centralized access, log management and relevant data retention. Cloud native Cortex Data Lake (CDL), part of Prisma Access, is preconfigured to enable continuous centralized logging integration with security information and event management (SIEM) tools. Enabling real-time security alert analysis based on network traffic, the FedRAMP-Authorized CDL and Prisma Access solution empowers agencies to meet the Executive Order's logging visibility and access goals.

SASE for Application Security

OMB Memorandum M-22-09, the Federal Zero Trust architecture strategy, directs agencies to secure applications and workloads with modern software development lifecycle practices, including continuous integration/continuous delivery (CI/CD) and infrastructure as code (IaC).

Combining Palo Alto Networks NGFW platforms to create scalable security stacks brings the policy enforcement point as close to the applications or data as possible. This allows inspection points where they are needed, artificially directing traffic, while maintaining control and visibility of all data and users. The Palo Alto Networks CN-Series firewall is the first NGFW integrated with containerized applications. It allows full inspection of east-to-west traffic within an application stack and the ability to scale as user demand grows. The Palo Alto Networks VM-Series firewall provides a scalable ingress/egress point as well as traditional NGFW capabilities that can scale with compute resources.

High-Level Architecture

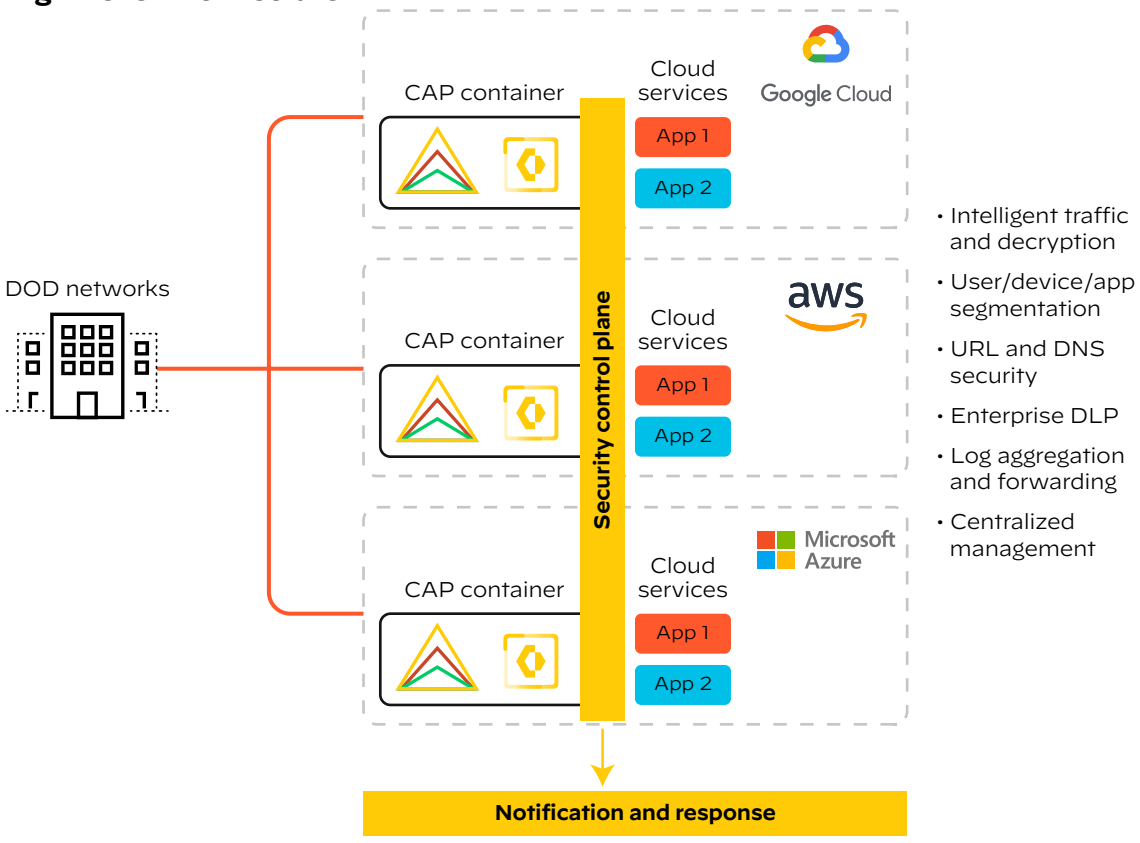

Figure 2: Containerized security stacks deployable in any environment

Prisma Cloud secures infrastructure, applications, data and entitlements across the world's largest clouds, all from a single unified solution. With a combination of cloud service provider APIs and a unified agent framework, users gain unmatched visibility and protection. Prisma Cloud integrates with any CI/CD workflow to secure cloud infrastructure and applications early in development. Scan IaC templates, container images, serverless functions and more while gaining powerful, full-stack runtime protection. This is unified security for DevOps and security teams.

Providing secure remote access and securing the network transport layer, the SASE application security stack establishes a security boundary around sensitive resources and provides Zero Trust policy enforcement points where they are needed. Tying all these components together with a unified policy and single management layer provides the framework for an overall Zero Trust architecture.

Palo Alto Networks Long-Term Commitment

Palo Alto Networks is uniquely positioned to deliver components of a Zero Trust architecture through a rich set of best-of-breed user, application and infrastructure security capabilities. The Prisma Access SASE solution integrates with existing enterprise tools, such as SIEM and Enterprise Identity and Access Management (IAM), allowing agencies to leverage existing infrastructure and maximize return on investment.

Palo Alto Networks is committed to the SASE framework. We will continue adding functionality and third-party integrations to our Prisma platform to reliably and sustainably make Zero Trust actionable for our valued federal customers.

Additional Resources

Find out more about how you can strengthen security with Zero Trust. Learn about Palo Alto Networks Services and Support offerings that can help you maximize the value of your investment and protect your department or agency. Contact the Palo Alto Networks federal team for additional information or visit the Palo Alto Networks federal website.

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