Consistent Security Policy Enforcement Across Remote Clinics for Healthcare Networks

Industry

Healthcare

Use Case

Zero Trust network access for remote clinics; SD-WAN hub for remote site connectivity

Business Benefits

Improved business continuity, user experience, and productivity with greater consistency and cyber resilience

Operational Benefits

Simplified management and better visibility with secure direct internet access for remote locations and clinic-to-clinic connectivity

Security Benefits

Consistent security policy enforcement across the organization

Business Drivers

Many factors are driving digital transformation in healthcare today—the shift to a value-based care model, expansion of the connected medical ecosystem, cloud adoption, the explosion of telehealth, and the "new normal" brought upon by the COVID-19 pandemic, among others. What's more, the onset of the pandemic has dramatically accelerated the pace of the transformation.

These developments are changing how healthcare professionals access enterprise resources as well as challenging traditional security approaches. Healthcare organizations must be capable of enabling secure access, protecting end users and applications, and controlling data from anywhere if they are to provide optimal patient care and maintain sustainable business operations.

Business Challenge

Some healthcare organizations have been reluctant to adopt the cloud and cloud technologies in the past because of concerns over data security and compliance. However, the industry is beginning to understand how these concerns can be addressed so organizations can harness the benefits of the public cloud to stay competitive.

Most healthcare organizations already heavily utilize plenty of software-as-a-service (SaaS) applications, from enterprise business applications to electronic health record systems and clinical applications. As more healthcare and enterprise services move to the public cloud, an institution's applications and data are less and less confined to the data center. Securely accessing enterprise resources that are no longer isolated on-premises becomes a challenge, especially for organizations that have focused heavily on building security capabilities at their network perimeter.

Many hospital systems are used by multiple remote clinics, community centers, and medical offices. These remote facilities primarily connect to the main hospital or data center over a wide area network (WAN) link leveraging virtual private network (VPN) tunnels. All traffic from remote facilities, including cloud- and internet-bound traffic, is therefore tunneled first to the main location. This "hairpinning" of traffic introduces latency and impacts end user response times. However, direct access to cloud and internet resources from these remote facilities and users is not provisioned for two main reasons:

- Security controls necessary to protect the organization and meet regulatory compliance are only available at the main perimeter location.
- Replicating security controls at each remote facility is not cost-effective or operationally efficient, and it is a challenge to ensure consistency.

Traditional Security Approach

With the rise of modern WAN technologies, such as software-defined WAN (SD-WAN), healthcare organizations can optimize connectivity to remote facilities and route traffic intelligently over multiple network transport services, improving application response times and network availability. However, traditional perimeter-based security approaches were not designed to keep up with the dynamic demands of SD-WAN architecture.

With traditional network security, it's difficult to address several key challenges:

- Accessing SaaS and other cloud services from remote clinics and users requires hairpinning through the data center, degrading user experience and performance.
- Expensive WAN links become saturated with internet traffic, creating a bottleneck for other important back-office traffic flow.
- Consistent security policy enforcement is difficult and costly to achieve at each remote location.

These issues drive up administrative costs and create operational challenges, signifying the need for a change in the industry. Effective, modern architecture should optimize access to all applications, wherever they or their users are located.

Palo Alto Networks Approach

In 2019, Gartner defined a new cloud-delivered architecture for networking and security called the secure access service edge (SASE, pronounced like "sassy"), which converges first-generation, standalone products with a common service delivery model. Palo Alto Networks provides a complete SASE solution that addresses the aforementioned problems. Our purpose-built cloud native Prisma® Access service, combined with Prisma SD-WAN, delivers the industry's most comprehensive SASE platform. This enables organizations to transform their networking and security infrastructure while realizing a market-leading return on investment (ROI). Our SASE solution combines a global high-performance network with next-generation SD-WAN to simplify the delivery of consistent security at scale while ensuring an optimal work-from-anywhere experience.

Prisma Access provides cloud-delivered security infrastructure that makes it possible to connect remote facilities to a nearby cloud gateway, enabling secure access to all applications together with full visibility and inspection of traffic across all ports and protocols.

Networking and network security services delivered from the cloud help organizations embrace mobility. Prisma Access provides consistent security and access to cloud applications (public cloud, private cloud, and SaaS) through a common framework for a seamless user experience. Bidirectional networking, delivered from more than 100 locations in 76 countries, enables branch-to-branch and branch-to-HQ traffic. All users, whether at the main hospital or remote clinics, or while working from home or on the road, connect to Prisma Access to safely use cloud and data center applications as well as the internet.

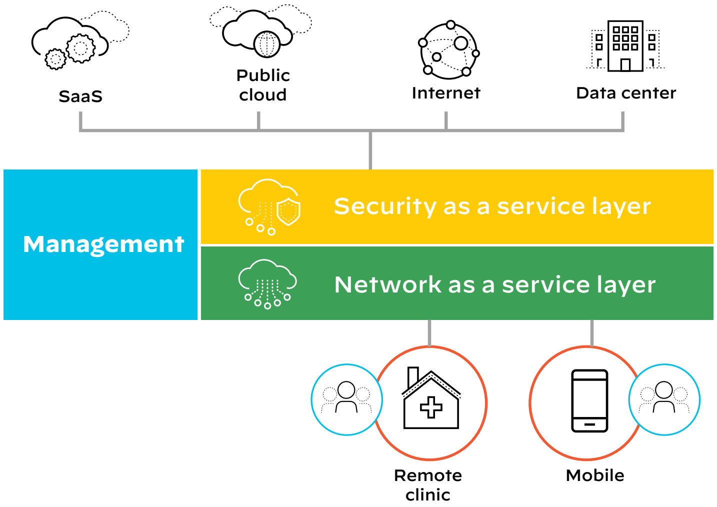

Figure 1: Prisma Access, a secure access service edge

The following security capabilities can be delivered using Prisma Access:

- **Firewall as a service (FWaaS)**—Next-Generation Firewall (NGFW) security for branch offices and retail locations.
- **DNS Security**—advanced analytics and machine learning to stop threats in DNS traffic.
- **Threat Prevention**—blocking of exploits, malware, and command-and-control (C2) traffic using threat intelligence.
- **Cloud secure web gateway (SWG)**—blocking of malicious sites using static analysis and machine learning.
- **Data loss prevention (DLP)**—prevention of data breaches, along with enhancements to data privacy and compliance.
- **Cloud access security broker (CASB)**—governance and data classification to stop threats with inline and API-based security.
- **Sandboxing**—zero-day threat prevention with the industry-leading WildFire® service.

Prisma Access consolidates more than 10 networking and security capabilities into a single cloud-delivered platform, including NGFW, VPN, SD-WAN, Zero Trust Network Access (ZTNA), and more. It simplifies network and security management, reduces security risk with best-in-class network security, and provides infinite remote access scalability and application performance for remote users.

With this architecture, healthcare organizations do not need on-premises security appliances in remote locations. An existing branch router or third-party firewall at the site, an SD-WAN edge device, or any other IPsec-compatible device can be repurposed to connect to Prisma Access. Policies are applied to the traffic in the cloud service, complemented by the full networking to handle routing to the internet, back to the main hospital or data center, or even over full-mesh VPN for clinic-to-clinic applications.

This immediately eliminates operational expenses, such as the shipping, installation, and ongoing maintenance of extra IT equipment at remote sites. Staffing can focus on operations and protecting the organization from regional cloud gateways rather than handling the enforcement at each remote facility's network edge.

Security for SD-WAN

In addition to native integration with our own Prisma SD-WAN, Prisma Access has integration with other SD-WAN vendors' products so that you can deploy SD-WAN securely. For SD-WAN devices that support split tunneling at the edge device, you can route the traffic from the edge to Prisma Access for enforcement of internet security policies. The remainder of the SD-WAN traffic passes over the SD-WAN cloud fabric. For SD-WAN environments that support a service chain from the fabric gateway, use Prisma Access for security enforcement rather than routing the traffic back.

Customer Implementation Example

A large healthcare provider in the US had implemented SD-WAN to optimize connectivity across more than 800 clinics and offices. The provider leveraged Prisma Access to gain cloud-delivered security capabilities and address security gaps across its clinics and SD-WAN connectivity. The primary goal was to achieve consistent security policy enforcement for all of the provider's clinics, WAN traffic, and traffic to both the internet and their public cloud infrastructure. With Prisma Access acting as the SD-WAN hub and security provider, the customer was able to enable direct internet connectivity from remote locations and achieve consistent security policy enforcement across their infrastructure.

Implementation Overview

Products Deployed

- Prisma Access with Threat Prevention, URL Filtering, WildFire, and GlobalProtect™
- VM-500 with Threat Prevention, DNS Security, URL Filtering, WildFire, and GlobalProtect
- Cortex® Data Lake

Deployment Details

- Existing third-party vendor SD-WAN implementation across all remote clinics.
- Prisma Access deployed as the SD-WAN hub interconnecting remote clinics, HQ, public cloud infrastructure, and the data center.
- Aggregated 50–400 remote clinics in each IPsec tunnel from third-party SD-WAN vendor gateways into Prisma Access.
- 800+ remote clinics into 16 tunnels across eight regions in the US.
- Prisma Access enabled at each region where the third-party SD-WAN gateways reside to minimize latency.
- Threat Prevention, URL Filtering, and WildFire services enabled across the environment.
- VM-500 deployed on AWS® with security services enabled as a transit gateway for security policy enforcement in the cloud.
- Cortex Data Lake aggregating logs from Prisma Access, VM-Series on AWS, and from the customer's existing Panorama™ managing multiple NGFWs.

Benefits of Using Prisma Access

Business Benefits

- Improved business continuity with greater cyber resiliency and security posture.
- Improved end user experience with both data center and internet applications for better staff productivity and patient care.

Operational Benefits

- Simplified security management of remote facilities and WAN connectivity.
- Improved visibility with security inspection for remote facilities and WAN connectivity.
- Direct internet access with security for remote clinics and users.
- Secure clinic-to-clinic connectivity.
- Quick ramp-up of connectivity and security for new or acquired remote sites.

Security Benefits

- Consistent security and data protection policies enforced at all locations.
- Centralized security logs for on-premises, cloud, and WAN activities for enhanced security analytics and response capabilities.

Additional Resources

- Resource Page: Learn more about Prisma Access
- Resource Page: Learn more about Prisma SD-WAN
- Demo Center: Request a demo of Prisma Access
- White Paper: Secure Access Service Edge (SASE)
- White Paper: Security Reference Blueprint for Healthcare IT

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