STRATA™
BY PALO ALTO NETWORKS

Guide to Safely Enabling Medical Applications and Devices

Security with Healthcare Context

Rapid advancements in electronic health technology have equipped healthcare organizations with a new suite of tools aimed at improving clinical outcomes. These same advancements, however, have broadened the attack surface for cyberthreats and complicated efforts to protect the already challenging healthcare environment. Security products are evolving to help healthcare organizations better deal with widening attack vectors, but protecting a hospital network with security tools that lack context around the medical systems and data they are meant to protect may not be adequate to keep up with today's demands. Whether to secure electronic medical record (EMR) systems, clinical applications, connected medical devices, or protected health information (PHI), your security products must be able to apply just the right protection for each use case.

Palo Alto Networks offers a suite of integrated security products to identify and classify medical systems and devices as well as apply comprehensive protection and security policies to help you safely enable innovative medical technology. This guide will discuss how different Palo Alto Networks products go about achieving this objective.

Introduction

Modern healthcare IT teams maintain a complex IT infrastructure to support their business services and care operations. Most systems, such as network equipment, servers, workstations, and printers, are not unique to the healthcare industry. There are three essential groups of systems unique to healthcare organizations, however, which today's security products must be aware of to ensure proper security policies are enforced:

- **EMR platforms:** Digital transformation in healthcare has digitized EMR, and today, just about every care provider organization uses EMR systems from platform vendors such as Epic and Cerner.
- **Clinical applications:** Efforts to standardize communication between clinical applications led to the creation of communication standards such as HL7 and DICOM.
- **Connected medical devices:** Commonly used medical devices, such as drug infusion pumps or patient monitoring systems, are now connected to hospital networks to exchange data crucial to patients' treatment and safety.

Beyond these technologies, factors such as mobility and cloud technology have transformed how data is accessed, processed, and stored. As healthcare organizations cater to the needs of providers and patients to access data from anywhere with any device type, protecting mobile assets and mobile access to data is becoming a challenge. With cloud technology, healthcare organizations have traditionally been reluctant to fully adopt cloud as part of their infrastructure, but many are already consuming cloud services through software-as-a-service (SaaS) delivery and adopting cloud strategies, usually starting with extending certain services to the public cloud. The cloud is transforming healthcare services to be highly agile and scalable, but it is a challenge to secure data and services that no longer reside on your premises. Attempts to replicate on-premises security tools in the cloud will not suffice.

With mobility and cloud technology changing how and where the data is accessed, processed, and stored, today's healthcare organizations must leverage security tools that can apply consistent protection to fixed and mobile endpoints, networks, and clouds while accounting for the context of the crucial medical systems they are protecting.

Palo Alto Networks Security Operating Platform

The Palo Alto Networks philosophy is to prevent successful cyberattacks. Due to an ever-escalating volume of threats, manual response across myriad best-of-breed security products has proven a daunting challenge. Consequently, Palo Alto Networks built the Security Operating Platform® to provide prevention through automation applied consistently across networks, endpoints, and clouds.

Our Next-Generation Firewall natively classifies all traffic, regardless of port, protocol, or encryption. This complete visibility into network activity allows healthcare organizations to substantially reduce their attack surface, block all known threats, and quickly discover and defend against previously unknown threats using WildFire® malware prevention service. Cortex XDR™ detects sophisticated threats with integrated response capabilities and unmatched accuracy while the Cortex XDR agent uses multiple methods of prevention to stop malware and exploits directly on endpoints.

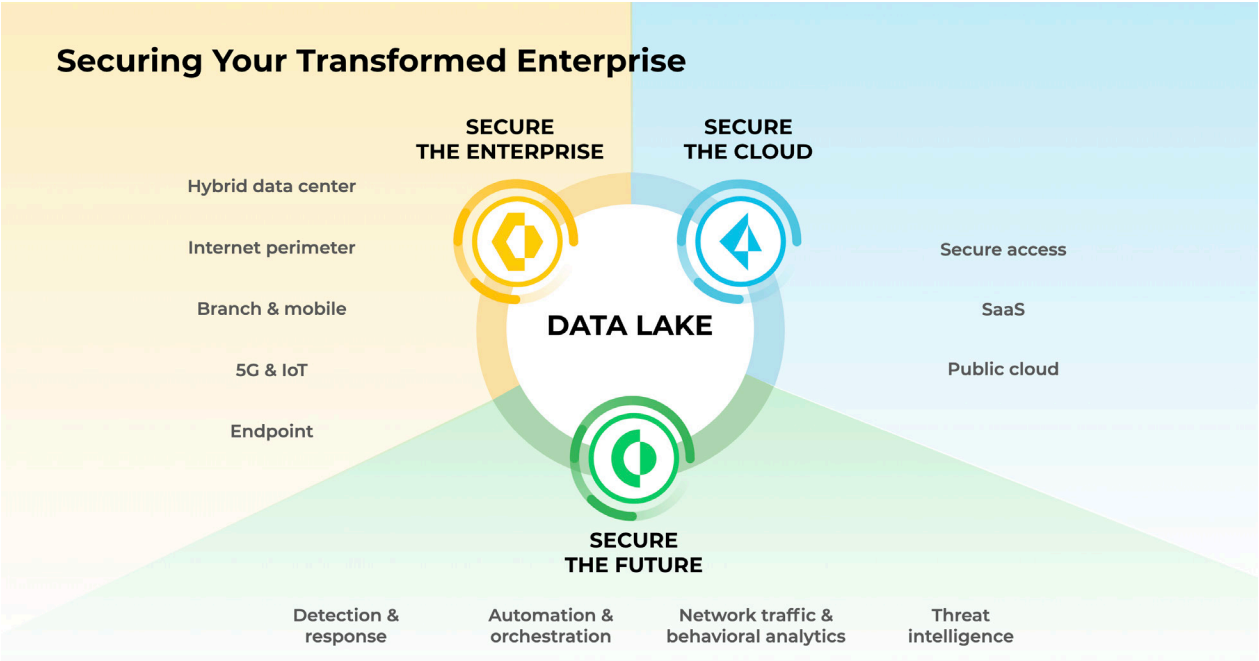

Figure 1: Security for your enterprise, cloud, and future

The Prisma™ cloud security suite provides comprehensive visibility and risk mitigation capabilities optimized for any cloud or multi-cloud environment. Automated coordination among these and the other natively integrated components of the Security Operating Platform—along with the delivery of cloud-based security services to complement network- and endpoint-based sensors and enforcement points—produces better security outcomes. The result is an innovative offering that delivers maximum protection for an organization's entire computing environment while greatly reducing the need for costly human intervention and remediation.

Here is an overview of some capabilities of our Next-Generation Firewalls:

- **Threat Prevention** stops exploits from reaching vulnerable endpoints and workloads, disrupts command-and-control (C2) traffic, and enforces intrusion prevention system (IPS) protection across all ports and protocols.
- **Malware prevention** blocks the delivery of malicious payloads carrying known and unknown malware, including ransomware, based on the latest Unit 42 threat intelligence, third-party threat feeds, and automated updates from WildFire.
- **URL Filtering** blocks access to inappropriate or malicious websites and prevents credential theft by blocking attempts to submit corporate credentials to unknown websites.
- **DNS Security** identifies infected hosts attempting to establish contact with an attacker by sinkholing DNS queries to hostile domains.
- **User and entity behavior analytics (UEBA)** uses Cortex XDR to track down attackers operating from within your organization.
- **Application visibility** lets you maintain oversight of all applications, across all ports and protocols; enforce policies to allow access to sanctioned applications based on User-ID™ technology and host information profile (HIP); allow tolerated applications with threat inspection; and block unsanctioned applications.

Identify and Protect Medical Systems with App-ID

As mentioned, our Next-Generation Firewall classifies all traffic regardless of port and protocol, and identifies many applications without any special configuration. App-ID™ technology on the Next-Generation Firewall identifies thousands of applications, including popular EMR platforms, such as Epic and Cerner; medical communication standards, such as DICOM and HL7; and point-of-care device traffic from devices such as infusion pumps, ECGs, and patient monitoring systems. Setting up App-ID on our Next-Generation Firewalls takes no effort at all. With the Expedition migration tool and the built-in Policy Optimizer feature on our Next-Generation Firewall, migrating conventional security rules to sophisticated App-ID rules is simple. Taking advantage of App-ID offers multiple benefits, ensuring you can improve your organization's security posture.

Get Visibility

As a foundational element of our platform, App-ID is always on. It uses multiple identification techniques to determine the exact identity of applications traversing your network, including those that try to evade detection by masquerading as legitimate traffic, hopping ports, or using encryption. Combined with information from User-ID, App-ID ensures you always know who is using what on your network.

> App-ID™ is a patented traffic classification technology only available on Palo Alto Networks Next-Generation Firewalls. It determines an application's identity irrespective of port, protocol, SSH/SSL encryption, or any other evasive tactic applications may use. It applies multiple classification mechanisms—including application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.

Safely Enable Applications

App-ID enables you to see deep into the applications on your network and learn how they work, their behavioral characteristics, and their relative risk. Armed with this information, your security team can use positive enforcement to allow the applications or specific application functions that enable your business.

Reduce the Attack Surface Area

Enforcing App-ID-based security rules reduces the attack surface more than traditional port-based rules because you can apply security policy to the desired traffic regardless of the port number the application uses. Many applications in a hospital network use custom TCP ports, and the Next-Generation Firewall's ability to identify and apply appropriate security rules removes the headache of manually identifying and configuring them.

Employ a Positive Enforcement Model

Our Next-Generation Firewalls support a positive enforcement model. You can allow sanctioned applications and application functions while you block or tightly control the remaining applications and unknown traffic. In addition, you can specify users and groups allowed to use sanctioned applications. All allowed traffic is scanned for threats and sensitive data, greatly reducing the attack surface across your organization.

Source User	From Port	To Zone	Destination	To Port	Application	Action
asel/tstu	53688	untrust	52.37.243.173	443	slack-base	allow
asel/tstu	53687	untrust	52.37.243.173	443	slack-base	allow
asel/tstu	53691	untrust	52.37.243.173	443	slack-base	allow
asel/tstu	53675	untrust	34.206.12.193	443	ssl	allow
asel/tstu	42047	untrust	54.174.219.117	443	ssl	allow
	55598	VW_trust	192.168.11.136	3613	alaris-dcmp	allow
	55599	VW_trust	192.168.11.136	3613	alaris-dcmp	allow

Figure 2: Alaris infusion pump device communication identified by a Next-Generation Firewall

Figure 2 shows an example of our Next-Generation Firewall identifying traffic from an Alaris™ infusion pump, denoting that the source of this traffic is likely an infusion pump device. Visibility into this type of information can aid in creating specific security policies for the same types of medical devices—regardless of which virtual local area network (VLAN) or network zone the source devices are in—and can support network segmentation efforts. The Next-Generation Firewall can also monitor unencrypted clinical application traffic and prevent it from traversing unsecure network segments or egressing to internet without a proper virtual private network (VPN) tunnel or encryption.

Many clinical applications use the HL7 communication standard to exchange PHI and feed different interfaces with relevant information. HL7 does not have native data security or encryption built into its protocol, however, so it should only be used through a VPN tunnel or SSH tunneling to encrypt the payload when used with external entities. To prevent clinical applications from transmitting unencrypted PHI via HL7, you can set a simple, all-inclusive security rule (as shown in figure 3) to prevent unencrypted HL7 traffic from leaving the network. You can also set the rule to generate an email alert to enable rapid response and resolution in case of a violation.

	Source			Destination			
Name	Zone	Address	User	Zone	Address	Application	Action
Web	any	any	any	any	any	ssl web-browsing	Allow
Outbound DICOM	any	any	any	Outside	any	hl7	Deny
Consumer Box	any	any	asel/base	any	any	boxnet-consumer-a...	Deny
Enterprise Box	any	any	asel/base	any	any	boxnet-enterprise-a...	Allow

Figure 3: Example rule preventing unencrypted HL7 traffic from leaving the secure network

Leveraging App-ID simplifies security rule creation and maintenance. When creating permissions for groups of clinical staff to access an EMR system, a firewall administrator may have to create multiple rules to provision access for different zones and user groups, and then manage these whenever new zones or groups are created. App-ID allows security rules to be applied directly to applications, such as the Epic EMR, letting administrators apply much more flexible rules and reduce revisions.

With our Next-Generation Firewall's ability to trigger an authentication sequence when specific traffic is observed, you can implement additional access protection. For example, if any user from a specific group tries to access the VLAN or zone housing your EMR platforms from an unusual location, the firewall can invoke multi-factor authentication (MFA) to verify the user's identity. The GlobalProtect™ agent must be installed on the user's device to enable the firewall to redirect the user to a browser-based authentication sequence.

Source User	From Port	To Zone	Destination	To Port	Application	Action
asel/tstu	42047	untrust	54.174.219.117	443	ssl	allow
asel/tstu	53675	untrust	34.206.12.193	443	ssl	allow
asel/tstu	55997	VW_trust	192.168.61.13	443	epic	allow

Figure 4: Next-Generation Firewall identifying a specific user accessing an Epic EMR system

Prisma Access for Protecting Remote Clinics and Mobile Users

Extending the same App-ID and medical system security to remote clinics and remote users is simple with Prisma Access by Palo Alto Networks. A cloud-delivered Next-Generation Firewall inspects all traffic from remote clinics and mobile users, allowing you to enforce consistent policies on traffic between your remote clinics, data center, and the public internet. Prisma Access delivers Next-Generation Firewall security from the cloud so that only data center-bound traffic is routed back to your data center, eliminating the need for traffic hairpinning and lowering your overall bandwidth requirements. Just like our Next-Generation Firewall, the comprehensive prevention capabilities of Prisma Access are built in. Figure 5 shows an overview of Prisma Access for networks and users.

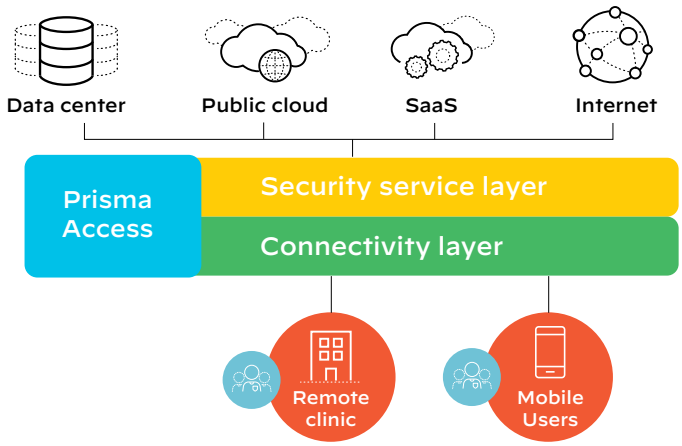

Figure 5: Security for remote clinics and mobile users

Prisma Access for Networks

Many branch offices are geographically spread out and lack full-time IT staff, which makes deploying, managing, and upgrading security hardware logistically challenging. You can use Prisma Access to connect your remote networks over a standard IPsec connection (using any existing router, SD-WAN edge device, or firewall that supports IPsec) to secure traffic, protect confidential information, and address data privacy compliance requirements. Prisma Access implements a full-mesh VPN within the security overlay, eliminating the complexity and headaches normally associated with branch-to-branch networking.

Prisma Access for Users

Mobile users need consistent security to access data center and cloud applications. Remote access VPN falls short because users typically connect to a gateway to access data center applications, and then disconnect from the VPN to get better performance (but less security) when accessing cloud and internet applications. Prisma Access brings protection closer to your users: when installed on a user's smartphone, tablet, or laptop, the GlobalProtect app automatically establishes an IPsec/SSL VPN tunnel to Prisma Access to provide the full protection of the Security Operating Platform without the backhaul to headquarters. With Prisma Access, all users have secure, fast access to all applications in the cloud, on the internet, or in your data center. The GlobalProtect app also lets you establish access policies based on HIP, enabling even more granular security policies tied to device characteristics (e.g., operating system, patch level, presence of required endpoint software) when accessing sensitive applications. Large populations of users may need to change locations from time to time, as conferences, weather, and natural disasters can strain local infrastructure. Prisma Access monitors conditions and automatically scales to add capacity in regions that need it.

Protect PHI in SaaS Environments with Prisma SaaS

With most healthcare organizations today using SaaS offerings for communication and collaboration tools, such as email, messaging, productivity suites, file sharing and storage, telehealth, videoconferencing, and more, it is crucial to protect sensitive data (e.g., PHI) on these SaaS applications. Some organizations have invested in cloud access security broker (CASB) products to gain some visibility and secure data uploaded and shared. Prisma SaaS plays a similar role, protecting data in SaaS environments and continuously monitoring to detect and prevent access settings that violate data disclosure policies. Equipped with data loss prevention (DLP) features, it ensures that data stored in SaaS environments is classified and flagged if an undesired condition is identified. Prisma SaaS also has built-in HIPAA data categorization to provide visibility into PHI stored and accessed in sanctioned SaaS environments. With out-of-the-box integration with the Security Operating Platform, Prisma SaaS extends WildFire coverage to your sanctioned SaaS environments. WildFire determines if files stored in a SaaS environment are malicious or not and can detect unknown threats by detonating unknown files in both virtual and physical sandbox systems.

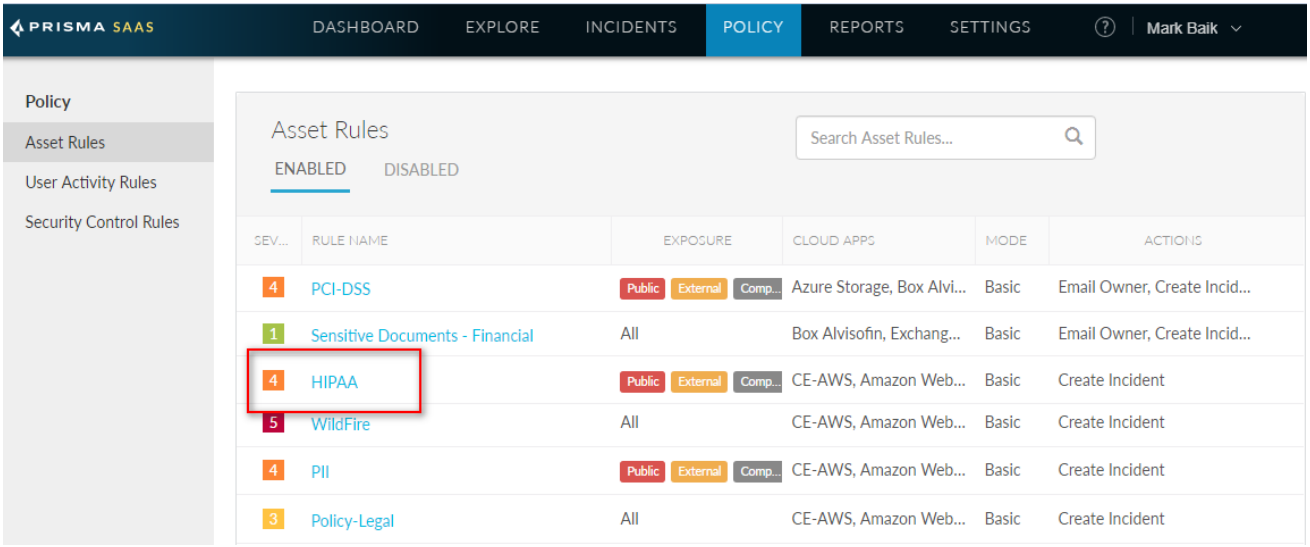

Figure 6: Example of a HIPAA asset rule enabled from Prisma SaaS on multiple cloud apps

Prisma SaaS lets organizations:

- Lower risk of exposure to malware and threats that propagate through SaaS environments.
- Lower risk of inappropriate sharing configurations within SaaS applications that may result in a reportable breach and HIPAA fines.
- Build on other hospital initiatives focused on promoting collaboration between medical staff while maintaining the safety of patient data.

Protect PHI in Public Cloud Environments

Your security policies should be consistent wherever your data is accessed or stored—whether in your data center, SaaS environments, or public clouds. Modern healthcare organizations are starting to embrace the public cloud, creating cloud-based services for patients and care providers. However, replicating existing security capabilities in the cloud is difficult and often ineffective. As the industry sees more cloud applications, from EMR and other clinical applications to PACS archives and informatics tools used for clinical research, the problem becomes more apparent.

Palo Alto Networks VM-Series Virtualized Next-Generation Firewalls offer the same security as our hardware firewalls, making it simple to replicate firewall capabilities to public cloud. Deployed as a secure gateway for a single virtual private cloud (VPC) or VNet, the VM-Series can inspect and protect data traffic within the VPC as well as its ingress and egress traffic. Deployed within the transit VPC where you deploy shared services such as security, the VM-Series can secure traffic between all VPCs, including backend traffic between the hospital network and the public cloud. The same App-ID and other features of the Next-Generation Firewall can be applied to all traffic.

Prisma Cloud enables continuous security monitoring, HIPAA compliance validation, and cloud storage security capabilities across your multi-cloud environments. An API-based tool, Prisma Cloud provides continuous monitoring—all asset information is constantly updated, and every change made to any cloud resource can be logged and set to alert, or even revert. Prisma Cloud also features dashboards and reports for a multitude of compliance frameworks, including HIPAA, so healthcare organizations can continuously assess their environments and quickly fix issues as needed.

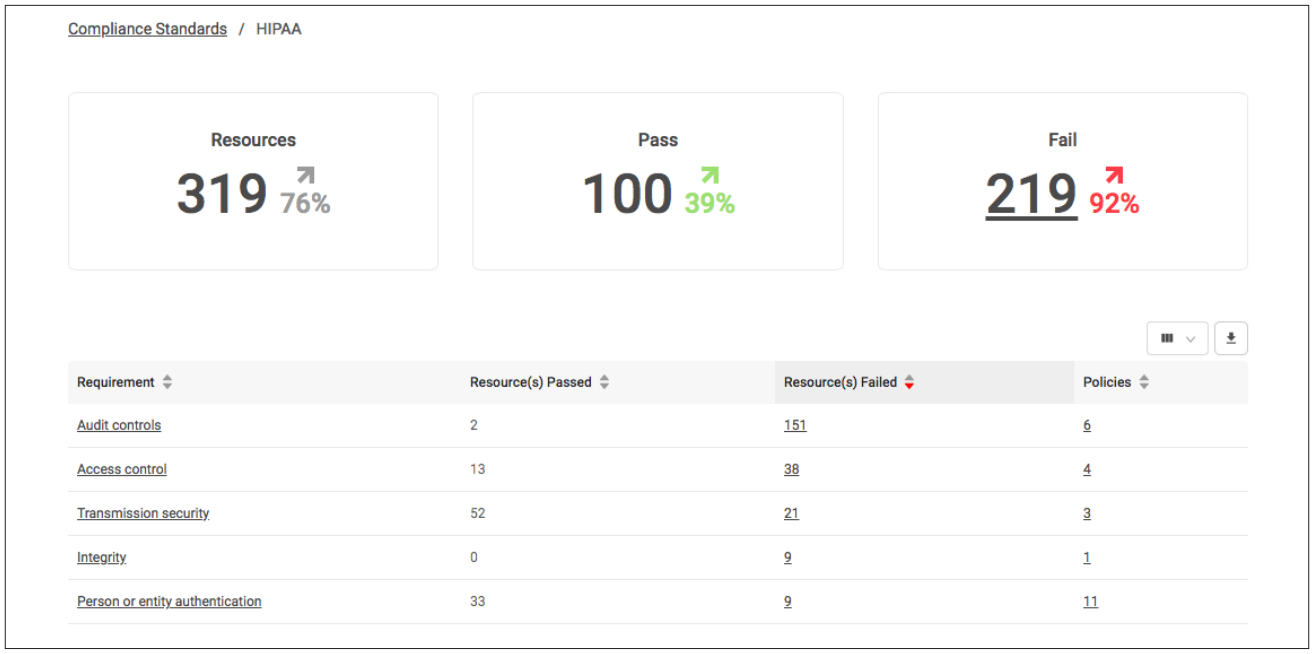

Figure 7: HIPAA dashboard in Prisma Cloud

Conclusion

Integrated next-generation security products provide comprehensive protection with healthcare context for all your critical systems, including EMR systems, clinical applications, and connected medical devices, and extend this capability to your remote clinics and mobile users as well as your SaaS and public cloud environments. Additionally, being able to protect PHI in SaaS environments while continuously assessing HIPAA compliance for your public cloud assets strengthens efforts to safely enable your innovative health technologies.

To learn more about the Palo Alto Networks Security Operating Platform or other services and offerings, take a complimentary Ultimate Test Drive or request a demo.

For additional healthcare-focused resources, please visit our healthcare industry page.

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