PA-400 Series for SMBs

Delivering Enterprise-Grade Security to Small and Medium Businesses

Businesses of every size and industry are vulnerable to cybersecurity threats. This is especially true today as more organizations embrace cloud services, remote work, and mobile devices than ever before. Small and medium-sized businesses (SMBs) face many of the same risks as larger enterprises. In fact, smaller companies may be even more at risk because many lack the resources to proactively prevent attacks. It's critical that small businesses are secured with the same level of enterprise security as corporate headquarters and data centers.

Business Benefits

- Complete Zero Trust Network Security at small offices and deliver safe context-based access for all users and devices
- Real-time prevention of known threats and zero-day attacks with embedded machine learning (ML) and natively integrated, cloud-delivered security services
- Low TCO
- Simple purchasing options
- Minimal maintenance with a resilient design

PA-400 Series Overview

The Palo Alto Networks PA-400 Series, comprising the PA-460, PA-450, PA-440, and PA-410, brings ML-Powered Next-Generation Firewall (NGFW) capabilities to small and medium businesses. The world's first ML-Powered NGFW enables organizations to prevent unknown threats, see and secure everything—including the Internet of Things (IoT)—and reduce errors with automatic policy recommendations, even at every small office location.

The controlling element of the PA-400 Series is PAN-OS, the same software that runs all Palo Alto Networks NGFWs, from the most powerful PA-7080 to the flexible VM-Series NGFW, as well as the cloud-delivered Prisma SASE solution. PAN-OS® natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The application, content, and user—in other words, the elements that run businesses—then serve as the basis of your security policies, resulting in improved security posture and reduced incident response times.

Key Capabilities

Enterprise-Grade Security with Best-in-Class PAN-OS

PAN-OS is the software that fuels our ML-Powered Next-Generation Firewalls. By leveraging the key technologies natively built into PAN-OS—App-ID™, Content-ID™, Device-ID™, and User-ID™—you can have complete visibility and control of the applications in use across all users and devices in all locations all the time. And, because of inline machine learning, and because the application and threat signatures automatically update our firewalls with the latest intelligence, security teams can be confident allowed traffic is free of known and unknown threats.

Visibility into Applications, Users, and Content

App-ID enables network security administrators to see the applications on the network and learn how they work, their behavioral characteristics, and their relative risk. It identifies the applications traversing the network irrespective of port, protocol, evasive techniques, or encryption(TLS/SSL). App-ID uses the application, not the port, as the basis for all safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic shaping. In addition, it also identifies all payload data within an application (e.g., files and data patterns) to block malicious files and thwart exfiltration attempts.

For new users, App-ID enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, delivering a rule set that is more secure and easier to manage. PAN-OS also offers the ability to create custom App-ID tags for proprietary applications, or customers can request App-ID development for new applications from Palo Alto Networks.

For more detailed information on App-ID, refer to the App-ID Tech Brief.

Security Policies Based on User Activity

PAN-OS enforces security for users at any location, on any device, while adapting policy based on user activity. It enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses—and provides dynamic security actions based on user behavior to restrict suspicious or malicious users.

PAN-OS easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more. As a user is identified, PAN-OS then applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android® mobile devices, macOS®, Windows®, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).

Secure Encrypted Traffic

With over 90% of internet traffic being encrypted, network security administrators have to be able to secure (decrypt-secure-encrypt) traffic right within the NGFW. PAN-OS is ideal for this as it inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2. It provides tools that offer rich visibility into TLS traffic, such as the amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, even before decrypting the traffic.

PAN-OS enables control over the use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks and facilitates easy deployment of decryption with built-in troubleshooting logs. To help organizations meet compliance and privacy requirements, PAN-OS allows network security administrators to enable or disable decryption flexibly based on URL category, source and destination zone, address, user, user group, device, and port.

For more information on securing encrypted traffic, refer to Decryption: Why, Where and How.

ML-Powered Next-Generation Firewall

The PA-400 Series with PAN-OS is a ML-Powered NGFW that embeds machine learning in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts. It leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW and uses behavioral analysis to detect IoT devices and make policy recommendations as part of a cloud-delivered and natively integrated service on the NGFW. Our firewalls also automate policy recommendations that save time and reduce the chance of human error.

For a more complete description of PAN-OS features, you can refer to Firewall Feature Overview Datasheet.

Detect and Prevent Advanced Threats with Cloud-Delivered Security Services

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our cloud-delivered security services use the network effect of 80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats with:

- **Threat Prevention**—goes beyond a traditional intrusion prevention system (IPS) to prevent all known threats across all traffic in a single pass without sacrificing performance.
- **Advanced URL Filtering**—provides best-in-class web protection while maximizing operational efficiency with the industry's first real-time web protection engine and industry-leading phishing protection.
- **WildFire®**—ensures files are safe with automatic detection and prevention of unknown malware powered by industry-leading cloud-based analysis and crowdsourced intelligence from more than 42,000 customers.
- **DNS Security**—harnesses the power of ML to detect as well as prevent threats over DNS in real time and empowers security personnel with the intelligence and context to craft policies and respond to threats quickly and effectively.
- **IoT Security**—provides the industry's most comprehensive IoT security solution, delivering ML-powered visibility, prevention, and enforcement in a single platform.
- **Enterprise DLP**—offers the industry's first cloud-delivered enterprise DLP that consistently protects sensitive data across networks, clouds, and users.
- **SaaS Security**—delivers integrated SaaS security that lets you see and secure new SaaS applications, protect data, and prevent zero-day threats at the lowest total cost of ownership.

PA-400 Series for Small and Medium Businesses

The PA-400 Series ML-Powered NGFWs are purpose-built for securing independent small office locations. Their uncompromising performance, packed into a small desktop form factor, makes them ideal for securing SMBs.

Prevent Data Breaches with Enterprise-Grade Security

Challenge

Small and medium businesses need enterprise-grade network security with support for cloud-delivered security services to block advanced threats. These businesses need locally deployed, modern, powerful NGFWs that prevent known and unknown threats by embedding ML inline, deploy security services to protect all applications, and decrypt traffic to prevent threats.

Solution

The PA-400 Series ML-Powered NGFWs are powered by the same full-featured PAN-OS and support all the cloud-delivered security services to protect against advanced threats. As all security services are deployed directly on the PA-400 Series, this architecture consolidates all network security functions onto a single device (no need for separate UTM, IPS or Web/URL filtering appliance, for example). With up to 10x performance compared to the previous generation PA-220, the PA-400 Series packs the performance required to deliver complete enterprise-grade security, bringing the ML-Powered NGFW (with decryption) to SMBs. Since it is built with our Single-Pass Architecture, the PA-400 Series maintains performance even as all security services are deployed on it.

Affordable Prices and Low TCO

Challenge

To protect against threats like ransomware and credential phishing, SMBs need access to the same tools and security available to large enterprises, but at an affordable price and with simple purchasing processes.

Solution

Our cloud-delivered security services natively integrate into our PA-400 Series appliances to detect and prevent advanced threats and enable SMBs to consolidate security tools. To enable easier, faster adoption of our industry-leading cloud-delivered security services and simplify procurement, we're introducing the PA-400 Series Subscription Bundles. There are two PA-400 Series Subscription Bundles available, Professional and Enterprise. Learn more about the PA-400 Subscription Bundles.

Table 1: Cloud-Delivered Security Services Bundles for the PA-400 Series

Cloud-Delivered Security Service	Professional Bundle	Enterprise Bundle
Threat Prevention (TP)	✓	✓
WildFire (WF)	✓	✓
Advanced URL Filtering (AURL-F)	✓	✓
DNS Security	✓	✓
SD-WAN		✓
IoT Security (DRDL)		✓
SaaS Security Inline		✓

Segmentation to Protect Critical Data, Applications, and Resources

Challenge

To secure networks from modern-day attacks, SMBs need to segment local traffic to isolate parts of the network from each other. Segmentation ensures that if one part of the network is exposed to a threat, that threat cannot migrate over to other sensitive parts of the network.

Solution

The PA-400 Series has up to eight 10/100/1000 RJ-45 ports that can segment local traffic at the location, isolating key portions of the network from each other. For more technical documentation on securing the perimeter and segmentation, you can refer to Perimeter Security for the Campus and Branch.

Minimize Maintenance with a Resilient Design

Challenge

SMBs have unique requirements for IT equipment, including firewalls. Firewalls need to be extremely resilient, as servicing appliances can quickly add to the total cost of managing security. Additionally, firewalls need to be quiet, as the NGFW might be deployed in a small customer-facing location. These locations might not have a dedicated rack or cabinet, so the firewalls should offer multiple mounting options.

Solution

All of the NGFWs in the PA-400 Series are designed with fanless cooling, which means that they will offer very quiet operation in small (and customer-facing) office and retail environments. The fanless design also means that these NGFWs have no moving parts, which increases their resiliency. The PA-460, PA-450 and PA-440 offer a dual (optional) redundant power supply to avoid network downtime from a power supply failure. The PA-400 Series has a compact, quiet design with multiple mounting options (desktop, rackmount, wall mount) for a range of scenarios.

Conclusion

Providing uncompromising security to small independent office locations requires access to the same tools that are available within data centers and large campus locations. The threats are the same, and the tools need to be fully featured as well. With the new PA-400 Series ML-Powered NGFWs from Palo Alto Networks, network security administrators now have access to an affordable array of options to achieve this uncompromising security.

Powered by the same PAN-OS and with options to the same cloud-delivered security services available to high-end NGFWs, network security administrators can deploy the PA-400 Series ML-Powered NGFWs and rest assured with best-in-class security at every office location. Cloud-delivered security services on the PA-400 Series ML-Powered NGFWs are now available in easy-to-purchase-and-deploy security service bundles.

Ready to get your hands on our ML-Powered Next-Generation Firewalls? Take an Ultimate Test Drive.

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. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. 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