REDUCE COSTS AND COMPLEXITY WITH NETWORK SECURITY CONSOLIDATION

Industry
Government

Use Case
Reduce network security costs and complexity by consolidating multiple security point products into one platform.

Business Benefits
Reduce the overhead associated with purchasing, deploying, operating and managing a plethora of security products, each designed to do a small range of things.

Operational Benefits
Minimize network disruption and risk with an extensible, flexible platform that protects your business as it expands, adopts new technologies or moves to the cloud. Improve visibility and simplify compliance by leveraging a consolidated set of screens, dashboards, logs and reports on a variety of security threats, including attempts at data exfiltration.

Security Benefits
Automatically correlate threat insights across the organization, and swiftly update threat prevention to every platform deployment regardless of location – endpoint, network or cloud.

Business Problem

To improve efficiency and increase client satisfaction, governments continue to adopt digital technologies that modernize their processes and better serve citizens. Every expansion into new digital technologies (remote employee access, client self-service, Wi-Fi, SaaS, cloud, IoT and more) also introduces vulnerabilities and points where the network can be infiltrated. In addition, as governments collect and store more valuable data digitally, they become attractive targets for cyberattackers seeking to spy or profit. The result is a cybersecurity arms race in which new attack vectors are countered with new security products.

This comes at a significant cost to governments. Every new solution that helps secure endpoints, SaaS, remote access, or other network areas and functions also adds complexity and cost. More security products can bestow a false sense of security, since the complexity of many point products can reduce visibility, instead of improving security, for the network and its endpoints. Solutions often add new hardware, which increases Capex costs. Individual solutions are also individually managed, increasing operational overhead and straining under-resourced security teams. Finally, these solutions function in isolation, making it impossible to leverage insights from the others, speed threat prevention or achieve an integrated view of an organization's security posture.

Business Drivers

Consolidation of network security into fewer devices is being driven by several factors, but underlying all of them is the desire to use security resources efficiently – particularly since the demand for cybersecurity professionals outstrips supply.[1]

High-profile data breaches have elevated the importance of cybersecurity in senior government positions. Government data breaches often involve the loss of valuable personal information, or highly confidential data that has national security value. Administrators now want regular reports on cybersecurity statistics and effectiveness. These are proving difficult and time-consuming to pull together as security solutions proliferate.

1. http://blog.indeed.com/2017/01/17/cybersecurity-skills-gap-report/

As cyberattacks increase in volume and sophistication, governments are finding it more difficult to keep pace with thwarting them. Since 98 percent of network compromises take only minutes to execute,[2] the focus must be on prevention rather than detection. Preventing the spread of new or multi-method threats requires correlation and coordination, which are two areas where discrete security functions (such as within a UTM) and products fall short. Correlation and coordination become even more difficult to execute as the numbers of vendors and products increase.

Similarly, governments must regularly demonstrate compliance with applicable data protection, privacy, accounting and other regulations. Data aggregation and correlation between multiple security products to support these initiatives are time-consuming for security teams.

Traditional Approaches

As new threats emerge, the traditional approach has been to add new, discrete security appliances and solutions to the network and its elements. For example, security vendors countered application-level attacks with intrusion prevention systems. As viruses became popular, governments added antivirus to endpoints. Phishing emails increased the popularity of content filtering.

This approach has resulted in an explosion of separate appliances and solutions for network security, including:

- Firewalls
- Web proxy servers
- Network intrusion detection/prevention
- Gateway antivirus/anti-spam solutions
- Virtual private network (VPN) appliances
- Content filtering
- Web filtering
- Zero-day exploit prevention
- Cloud and SaaS security
- SSL decryption devices

There are distinct challenges with multiple security vendors and appliances:

- **Lack of visibility:** With multiple unintegrated security products, it's difficult to get a comprehensive view of network traffic and potential threats.
- **Operational complexity:** Each point product is separately managed by its own management interface, requires time and training to manage, and results in greater overhead for security teams, which must manually update security appliances, correlate insights, amalgamate logs and events, and trawl through logs.
- **Reduced performance:** As the numbers of boxes and solutions increase, so does network latency, impacting time-sensitive applications.
- **Higher costs:** More devices cost more to purchase, including support and subscriptions.

It's becoming more common to link many separate security solutions together using a security information and event management product. While SIEMs are useful, they are most useful for forensic analysis, incident response and remediation.

Some security vendors attempt to consolidate multiple security functions into a single physical appliance, sharing power, cooling and rack space. However, their software technologies remain unintegrated, and they cannot share context and correlate between security functions. Many vendors have separate management interfaces for different security functions.

Palo Alto Networks Approach

In stark contrast to other approaches, Palo Alto Networks® consolidates multiple complementary security functions into a single, natively integrated platform, safely enabling users, applications and traffic across endpoints, networks, cloud and SaaS environments. The many benefits of this platform approach include:

- **Faster time to threat prevention:** Automatically correlated insights between security functions, as well as automatic distribution of signatures and other preventions, quickly repel the newest threats in all locations.
- **Greater security** insights due to contextual threat intelligence applied across security functions.
- **Simpler management:** The entire suite of security functions and policies is managed from a single interface, reducing management complexity for IT and security teams.

2. Verizon 2017 Data Breach Investigations Report

- **Comprehensive safe enablement:** A single pane of glass provides complete visibility into users, applications and traffic in all locations across mobile, network, cloud and SaaS environments.
- **Flexibility:** Organizations can choose which security functions to integrate and add security functions over time as business needs change.
- **Lower operating costs:** New security functions do not require more hardware installations, additional training for security teams or more management overhead.
- **Less disruption:** Adding new security functions does not disrupt availability or require architecture changes. In many cases you can add security functions remotely, eliminating a truck roll or the requirement for on-site IT or security staff.
- **Reduced latency:** Fewer boxes and traffic inspection points improve latency for time-sensitive applications.

Palo Alto Networks Next-Generation Security Platform automatically correlates insights on emerging threats across endpoints, data centers, SaaS and cloud resources, ensuring fast responses to any threat without manual intervention. As you add security capabilities, coordination increases, as does return on investment. Platform security capabilities include the following:

- **Next-Generation Firewall** classifies all traffic – including encrypted traffic – and enforces policies based on applications, users and content without sacrificing performance. It can selectively decrypt encrypted traffic for analysis and segment networks based on users or groups.
- **WildFire™** cloud-based threat analysis service dynamically analyzes suspicious content in a virtual environment to discover zero-day threats.
- **Threat Prevention** includes IPS, malware protection, DNS sinkhole, and command-and-control protection.
- **URL Filtering** continually updates with new phishing and malware sites, as well as sites associated with attacks, even blocking malicious links in emails.
- **GlobalProtect™** network security for endpoints extends a VPN and the protection of the Palo Alto Networks platform to mobile staff, employees with mobile devices and third-party contractors.
- **Traps™** advanced endpoint protection blocks exploits and malware on critical assets, such as POS devices, unpatched servers and corporate endpoints.
- **AutoFocus™** service provides contextual threat intelligence analysis on all Palo Alto Networks threat data.
- **Aperture™** service provides security for SaaS applications.
- **Panorama™** network security management enables you to control your distributed network of next-generation firewalls from one central location via a virtual or physical appliance.

Users of the Next-Generation Security Platform benefit from the most comprehensive library of collective threat data in the world. Palo Alto Networks customers share threat data to minimize the spread of attacks and raise the costs to attackers. The detection of a new threat in one customer environment that is sharing threat information triggers the automatic creation and dissemination of prevention mechanisms across thousands of customers. Governments wishing to operate their own threat intelligence cloud on-premise can do so as well.

Best Practices and Deployment Considerations

Palo Alto Networks platform deployments are available in a range of physical appliances as well as virtualized for all popular virtual environments, serving the smallest offices to the largest headquarters and data centers. With Palo Alto Networks virtualized platform deployments, governments can extend the security of the on-premise network to AWS® and Microsoft® Azure® environments as well as hybrid and private clouds.

Some government agencies may not wish to send files to a cloud-based malware analysis environment for inspection or have their appliances communicate with a vendor's network outside their organization. These agencies can implement their own private malware analysis environments, which can be optionally configured to receive signature updates and other preventions from the Palo Alto Networks threat intelligence cloud, either automatically or via manual updates.

To better understand how Palo Alto Networks government customers have leveraged the Next-Generation Security Platform and achieved network consolidation, read the following real-world example.

Actual Customer Implementation

One Palo Alto Networks customer, a large U.S. government agency, operates as a federal entity and has autonomous branches in all 50 states. The agency owns a private network that connects all branches to several data centers and connects to the internet through four gateways spread across the country. For maximum reliability and security, the agency's network has perimeter protection at each branch, and each branch connects to the network through two separate gateways. Hundreds of thousands of internal users employ the network to securely access the internet, "corporate" applications, and databases and applications from other related agencies.

Customer Business Challenge

Like many federal agencies, the customer refreshes its network routing and security architecture every five to seven years. During the last major refresh, echoing similar past decisions by businesses and governments, the agency chose stand-alone appliances for perimeter security functions. Each perimeter gateway used Cisco® firewalls, Blue Coat® WebFilter appliances and McAfee® IPS appliances. Since the federal and each state entity have individual security policy requirements, each needed to apply and control its own policy set at each gateway. As a result, most state branches had four of each appliance – firewalls, web filtering appliances and IPSs – for a total of 12 perimeter appliances, with half under state control and half under federal control. Different management systems for different vendor systems made it very difficult gain a holistic view of traffic traversing the network. The agency relies on an integrator to operate, administer and maintain the network, and research into potential threats was time-consuming, as was compilation of security reports for management.

The agency wanted to simplify operational management and improve visibility into advanced threats, believing that consolidating perimeter security functions would help speed up identification and prevention of modern and application-level cyberattacks on the network as well as coordinate responses. Other customers have come to this realization only after serious breaches or after periods of growth, when operational overhead and growing pains become impossible to ignore. Agency decision-makers also knew they needed to find a way to eliminate the duplication of every appliance at every gateway while still maintaining separate policy control for federal and state entities. Ultimately, they chose Palo Alto Networks Next-Generation Security Platform to address these challenges.

Implementation Overview

The following details this agency's Palo Alto Networks deployment:

Products deployed:

- Palo Alto Networks Next-Generation Firewall appliances (PA-5020) with Threat Prevention, URL Filtering and WildFire subscriptions
- WildFire private cloud WF-500 appliances
- PAN-DB private cloud on an M-500 appliance
- Panorama network security management on physical appliances

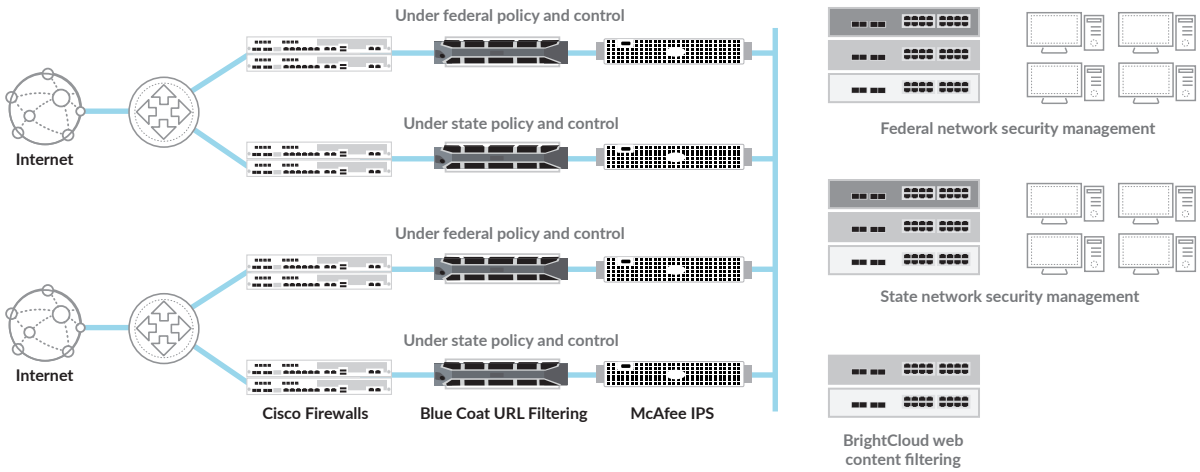

Figure 1: Before consolidation – typical state perimeter and management

How customer implemented network security consolidation (high level):

At the perimeter of each state network:

- The perimeter is secured with one PA-5020 appliance for each gateway, offering redundancy. Each appliance includes redundant power supplies and fan trays.
- Every appliance performs multiple security functions: application-aware firewall, IPS, network anti-malware, DNS sinkhole, web filtering and zero-day threat prevention.
- All appliances are centrally managed with Panorama, ensuring consistent security policies.
- An M-500 appliance contains the agency's on-premise PAN-DB private cloud, which automatically updates appliances every five minutes with malicious URLs.
- WF-500 appliances make up the agency's on-premise WildFire private cloud, which automatically updates appliances every five minutes with signatures for newly discovered threats.

How customer's network security consolidation works (high level):

- The customer divided each PA-5020 physical appliance into two virtual systems: one for the federal entity and one for the state. Each virtual system is a separately managed, logical appliance with differing policies and traffic.
- The customer transitioned existing port- and protocol-level firewall policies to take advantage of the platform's App-ID™ technology. Application whitelisting safely enables corporate applications and excludes all else.
- WF-500 appliances enable the customer to analyze suspicious files in a sandbox environment in the agency's own network without having to send files to the cloud. Appliances automatically forward potential risky files for analysis to the WF-500, which analyzes the file and automatically sends confirmed malware to WildFire for signature generation. Generated signatures are automatically distributed to all WildFire customers.
- URL Filtering policies ensure employees do not access prohibited web content at work, no matter where they are working.
- PAN-DB constantly and automatically updates URL signatures in its database, based on what URL Filtering sees for malicious URLs as well as URLs where WildFire finds zero-day malware or spyware.
- Panorama a single plane of glass that integrates real-time views, logs and reports across security functions. From a single management console, a state can see which URLs have been recently blocked, which known threats have been detected and blocked (e.g., spyware attempting to steal data, ransomware attempting entry), and which suspicious files have been sandboxed by WildFire. The integrator can generate quality reports on traffic and threats in minutes, instead of the many hours it took with the previous solution.
- The agency is successfully integrating the Next-Generation Security Platform into their SIEM.
- While the agency could have also used the PA-5020 for SSL decryption, it continues to use its existing decryption appliance.

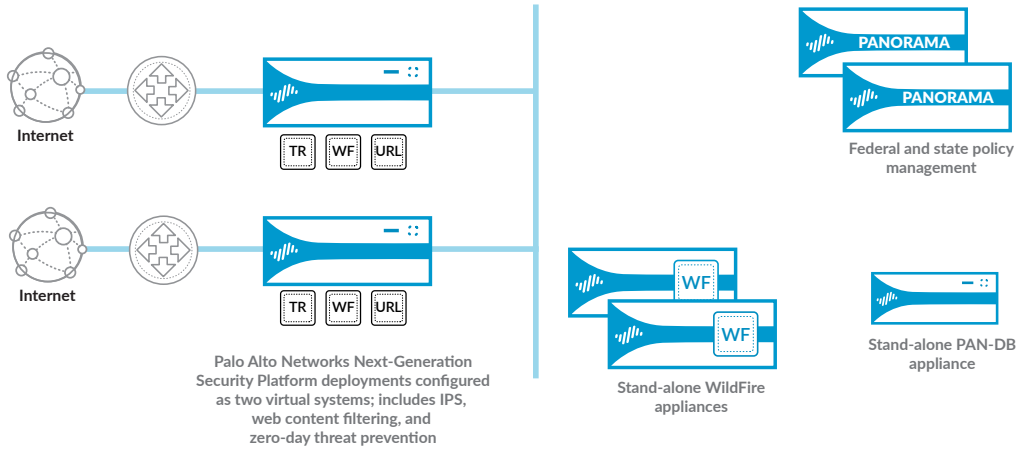

Figure 2: After consolidation – typical state perimeter and management

Results

With a consolidated view of traffic and potential threats, the agency can respond to threats much more quickly. They no longer need to weave together reports from different devices or management systems. With fewer devices and policies to manage, as well as fewer manual updates, the agency will spend less money operating the network while vastly improving the visibility of traffic. The agency has all the security functions it had before and can enjoy the new capability of zero-day threat prevention. With more than 75 percent of the states deployed, installation has been smooth and on schedule.

Benefits of Network Security Consolidation

By leveraging the Palo Alto Networks platform to consolidate several security functions, all organizations can reap the following benefits:

Business Benefits:

- Decrease capital and operations costs with fewer devices to deploy and manage
- Simplify compliance with a consolidated set of logs and reports on a variety of security threats

Operational Benefits:

- Minimize network disruption with the ability to add new security functions as needed on the same platform
- Reduce manual work of correlating threats across multiple devices and platforms
- Simplify and speed report creation process for management
- Free up security teams to perform high-value work

Security Benefits:

- Get better visibility into threats through a single pane of glass, with context and analysis
- Use a positive enforcement model for tighter control of application traffic
- Reduce the attack surface by eliminating unknown or unexpected applications
- Enable faster time to threat prevention with automated updates pushed regularly to devices

Additional Resources

Further resources on the advantages of network security consolidation can be found at the links below.

- Next-Generation Security Platform Overview
- The Value of the Next-Generation Security Platform
- State of Colorado saves staff time and millons in product costs with device consolidation

Services to Help You

Support

Palo Alto Networks Customer Support automates the discovery of related cases to increase productivity and get you to a resolution more quickly. We offer multiple support packages: Standard, Premium and Premium Plus. You can also opt for your own technical account manager as a subscription-based extension of Premium Support. Premium Plus provides both a designated technical support engineer and technical account manager, who will learn and understand your deployment at both technical and business levels, accelerating incident resolution.

Consulting

Palo Alto Networks Consulting Services provide access to specialized talent knowledgeable in ensuring the safe enablement of applications. By matching talent to task, we deliver the right expertise at the right time, dedicated to your success.

Resident engineers, for example, provide on-site product expertise and are uniquely qualified to advise you on getting the most out of your Next-Generation Security Platform deployment.

Education

Training from a Palo Alto Networks Authorized Training Center delivers the knowledge and expertise to prepare you to protect our way of life in the digital age. Our trusted security certifications provide the necessary Next-Generation Security Platform knowledge to prevent successful cyberattacks and safely enable applications.

Conclusion

As an organization's digital footprint expands, so do the potential threat vectors. Network and security teams have enough to manage without constant manual security updates, log aggregation, event correlation and security actions from multiple management interfaces. A recent survey of almost 150 of our customers showed that consolidating multiple security functions on a single platform resulted in Opex savings and, moreover, improved attack analysis.[3] These customers deployed an average of 3.2 subscriptions on their next-generation appliances, and reported average reductions of:

- 26 percent in the amount of time required to add new rules to manage their firewalls.
- 25 percent in the number of security alerts requiring human intervention.
- 30 percent in the time it takes an analyst to investigate an event in order to drive a technical action to prevent or block an incident.

These savings could be yours. For more information on how security network consolidation with Palo Alto Networks could reduce your total cost of ownership, reach out to your Palo Alto Networks account team and sign up for a free TCO calculator session.

3. Verizon 2017 Data Breach Investigations Report

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