



When we think about next generation firewalls there is one company which has been at the forefront for firewall innovation: Palo Alto Networks. Palo Alto Networks have developed a series of firewalls which are both secure and simplistic thanks to a string of developments and innovative technologies. What's great about these firewalls is that they enable organisations to repair the firewall themselves, without external influence or intervention from the company.

The firewall architecture is high performance and incorporates relevant business elements such as content, users and applications and packs them under a high policy control system. The platform is purpose-built and is based on Palo Alto Networks Single-Pass Parallel Processing (SP3) Architecture.

[View less](#)

SP3 possesses the following revolutionary features:

- Traffic is only examined once
- Hardware combines with dedicated processing resources for added security
- Safe and secure networking
- Efficient content scanning and management provides a line-rate
- Low-latency performance under load

As a business owner you are aware of the importance of your network security. Robust network security and a reliable firewall are imperative if you want to maintain a secure network and keep your business records and applications safe from harm.

Palo Alto Networks develop enterprise level firewalls to defend your organisation against intruders and foul play. Ensure that you align your company with the firewall developers who are dedicated to innovation and the constant development of a revolutionary security platform.

Palo Alto Networks security systems combine firewall, advanced threat protection, URL filtering and IDS/IPS. These functions are all inherently built into the security platform to ensure better security than traditional firewalls.

Safeguard your business against possible online and network related threats by incorporating a Palo Alto Networks firewall into your organisation. For more information on next generation firewalls and network security, [contact us](#) at Bitrate.

Visibility into Application, Users and Content



Palo Alto Networks provide high quality next generation firewalls which allow for granular control of applications being used on the network as well as identifying the user and not the IP via integration into LDAP directory structures such as Microsoft Active directory. These insights into the network traffic and users allow administrators to learn about and control applications effectively and efficiently, as well as inspect all applications traversing the firewall for known threats, and unknown zero hour threats via an integrated cloud based threat detection engine .

Palo Alto Networks Firewall Solutions

-

Management Platforms



-

PA- 3000 Series Firewall



-

PA-200 Firewall



-

PA-2000 Series Firewall



- PA-500 Firewall



- PA-5000 Series Firewall



- PA-7050 Firewall Series



- VM Series Firewalls



With the Panorama centralised management platforms from Palo Alto Networks you are able to manage all of your firewalls from one location. This increases management capabilities, reduces the time it takes to identify firewall issues and ultimately increases productivity and security.

[Show more...](#)

[Mobile Device Management \(GP-100\)](#)

Features

Ensuring mobile security is a necessity for organisations which conduct business transactions through mobile applications. Mobile Device Management (GP-100) provides a mobile management platform which can safely enable

mobile devices for business use. This is achieved through the use of mobile security platform GlobalProtect, an original, integrated solution to mobile security. GlobalProtect is comprised of 3 components. These are: GlobalProtect Gateway, GlobalProtect Mobile Security Manager and GlobalProtect App. All of these features are available on the Palo Alto Networks Mobile Device Management (GP-100) while the GlobalProtect App is available on iOS and Android devices.

[read more](#)

Panorama Virtual Appliance (ESXi)

If your business deploys multiple firewalls then it is necessary to have a centralised management system which will provide you with clear visibility over your entire network. Palo Alto Networks Panorama Series provide a centralised management platform making it easy to manage an entire network of next-generation firewalls from a single location.

[read more](#)

Panorama M-100 Appliance

If your business has a number of firewalls running consistently then it can turn into a managerial nightmare. In this situation it is best to have a centralised management platform from which all of your organisations firewalls can be effectively managed. A management platform such as Panorama from [Palo Alto Networks](#) enables network administrators to gain complete visibility over the network making it easy to manage multiple firewalls on the network.

[read more](#)

Palo Alto Applications visibility and control



The problem with IP addresses and port numbers is that they carry very little information about what is actually on the network. This omission is a critical oversight because information regarding applications, users and content on the network affords employers the opportunity to identify risks and respond quickly in order to negate these risks.

[Read More](#)

Palo Alto Networks Features

Palo Alto Networks and their “next generation” firewalls contain a number of features which go above and beyond traditional firewall features to provide added security in a constantly developing

digital landscape. Contributing factors such as developing network infrastructure, application usage, and a change in user behaviour have resulted in an increased number of developing threats which are posed to your businesses network.

[Application ID](#)

[Application Visibility](#)

[Centralized Management](#)

[Content-ID](#)

[Redundancy & Resiliency](#)

[Virtual Systems](#)

[Data Filtering](#)

[Decryption](#)

[Device Management Flexibility](#)

[GlobalProtect](#)

[URL Filtering](#)

[VPN](#)

[IPS](#)

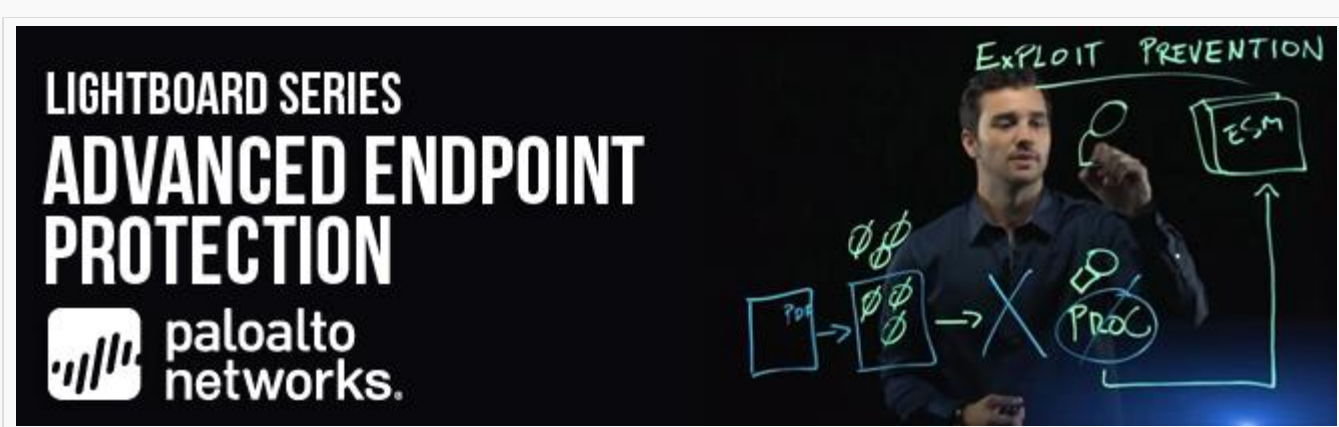
[Modern Malware Protection](#)

[Networking](#)

[Policy Control](#)

[User-ID](#)

Traps/Wildfire



With a unique approach to the problem, Palo Alto Networks Traps prevents sophisticated attacks on the endpoint before malicious activity can run. In this Lightboard session learn more about how Traps does the impossible.

Checkout this next-generation white-board video where Palo Alto Networks' Systems Engineer Specialist, Garrett Hamilton, walks through today's threat landscape and Palo Alto Networks Advanced Endpoint Protection.

Watch this exciting product overview to learn how:

- You can save on unnecessary remediation by preventing APT attacks on the endpoint
- Traps policy restrictions and unique integration with WildFire™ form a powerful executable prevention

Increasing visibility between the network and the endpoint complete enterprise security