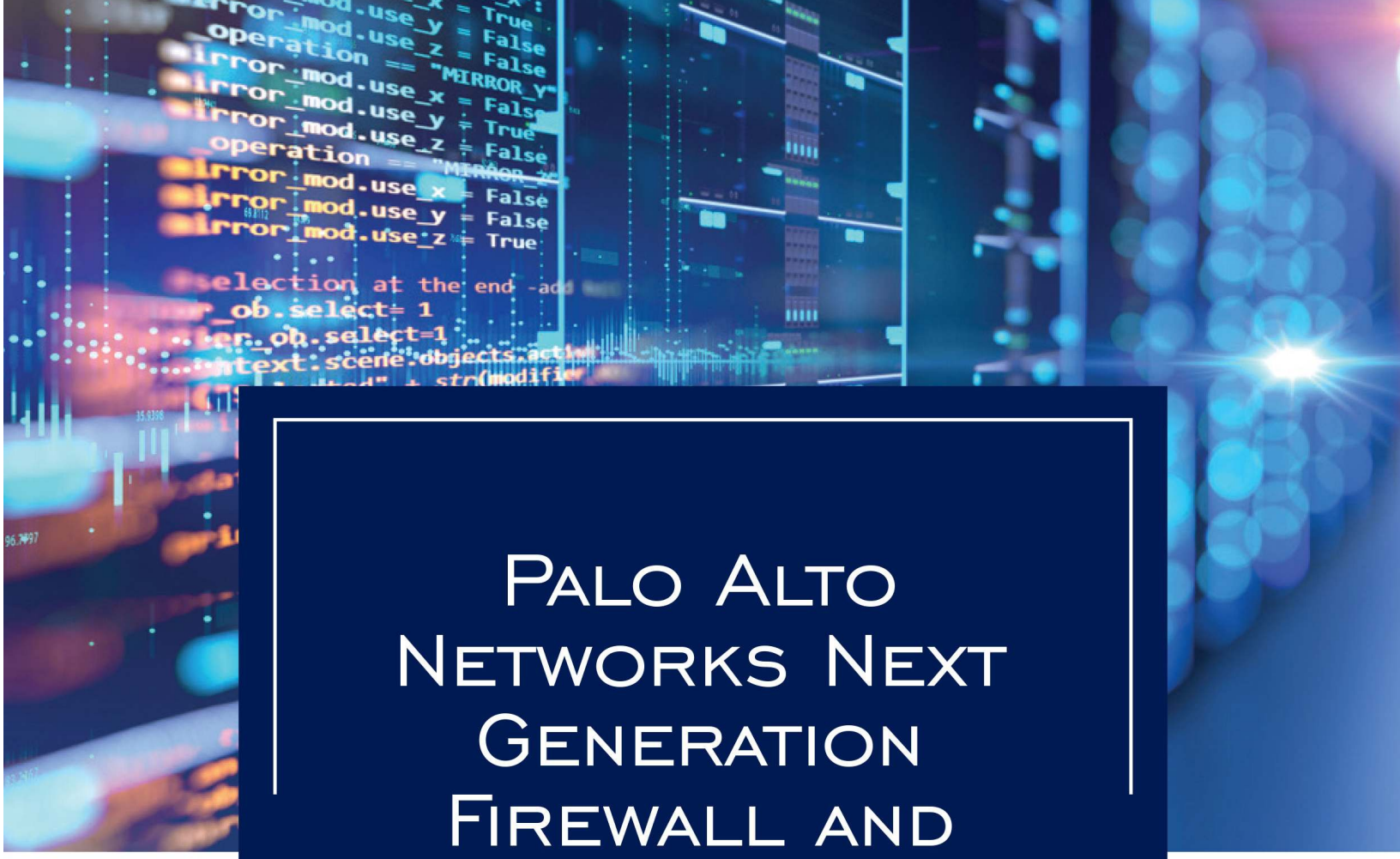


Palo Alto Networks Next Generation Firewall and Ericom Shield

Comprehensive Protection from Web-based Threats

ERICOM
Be Connected, Be Secure

The Challenge

Organizations will see a much higher rate of attack for unknown malware due to the vulnerability associated with endpoint attack vectors via a web browser. Attacks may originate from URL links embedded in emails or messages, or from malicious scripts in legitimate websites which cannot be detected by traditional security approaches.

Browsing is a common and essential business practice in almost all organizations making businesses susceptible to browser-borne threats. In fact, some of the highest profile cybersecurity breaches started with a user's click on a seemingly benign website that introduced a piece of malware into the corporate network. The costs and damages associated with recovering from one of these attacks can threaten profitability and business continuity. on up.

Key benefits of the integration

Stops web based malicious attacks, known and unknown, before threats reach the endpoint
Clientless – nothing to install on the end-user device
Empowers users with confidence to browse the web without fear of data exploits, ransomware, phishing, malvertising or other threats
Stops hackers from evading detection and infiltrating your network

Ericom Shield integrates with Palo Alto Next Generation Firewall using standard URL Redirection or proxy chain techniques

Ericom Shield

Ericom Shield is an award-winning Remote Browser Isolation (RBI) platform that offers a secure approach to protect corporate end-user devices against web-borne and zero-day threats. With Shield, a secure execution environment is created between users and the Internet. While users access websites, virtual browsers located in air-gapped and remote, isolated, and disposable Linux containers are executing each web session. A secure visual stream is transmitted from the container back to the browser on the user's device providing a natural experience. Users can access business-critical Internet services, while protecting endpoints and the corporate networks from malware, phishing, crypto mining and other such threats.

Palo Alto Networks

The Palo Alto Networks® next-generation Firewall prevents successful cyberattacks through intelligent automation. The platform combines network and endpoint security with threat intelligence and accurate analytics to help streamline routine tasks, automate protection and prevent cyber breaches. Tight integrations across the platform and with ecosystem partners delivers consistent security across clouds, networks and mobile devices, natively providing the right capabilities at the right place across all stages of the attack lifecycle.

Palo Alto Networks Next Generation Firewall and Ericom Shield

The integration of Palo Alto Networks next-generation firewall and Ericom Shield provides a multi-layer defense that effectively protects organizational networks and data from the full range of known, unknown, emerging and zero-day threats, while facilitating essential, productive web-based business activity.

Palo Alto Networks next-generation firewalls detect known and unknown threats, even in encrypted traffic. Based on URL Filtering, requested sites that are whitelisted are opened natively on the user's endpoint browser while blacklisted sites are blocked. Uncategorized or unidentifiable sites are redirected to Ericom Shield for browsing under remote isolation, safely away from the corporate network and end user devices.

The integrated Palo Alto Networks and Ericom solution secures business-critical web-based activity and protects against undetectable threats and human factor vulnerabilities by:

- Inspecting and blocking detectable and known malicious content at the firewall
- Filtering blacklisted URLs
- Isolating all active untrusted web content away from the endpoint and internal networks
- Abstracting web content on endpoint as a fully interactive media stream
- Protecting file downloads from the internet and disarming potentially malicious content
- Providing optional read-only mode to protect against phishing attack credential theft

Use case #1

Challenge: Some professions, such as cybersecurity researchers, require access to browse the dark web to research new threats. The investigators need to browse safely without themselves being victimized.

Solution: With the Palo Alto Networks next-generation firewall and Ericom Shield integrated solution, URL filtering is tailored for investigators to gather data on the relevant dark web sites, which would otherwise be blacklisted for most users. The Palo Alto Networks next-generation firewall detects and denies the bulk of the known attacks stemming from those sites. Using Ericom Shield, the uncategorized, unknown, and suspicious websites are rendered by an isolated browser remote from the endpoint in the DMZ, so that any potential malware cannot infect endpoint devices and from there, enter internal corporate networks.

Benefit: Specific users or teams that require open access to the internet to perform their jobs can do so freely without attracting malicious content.

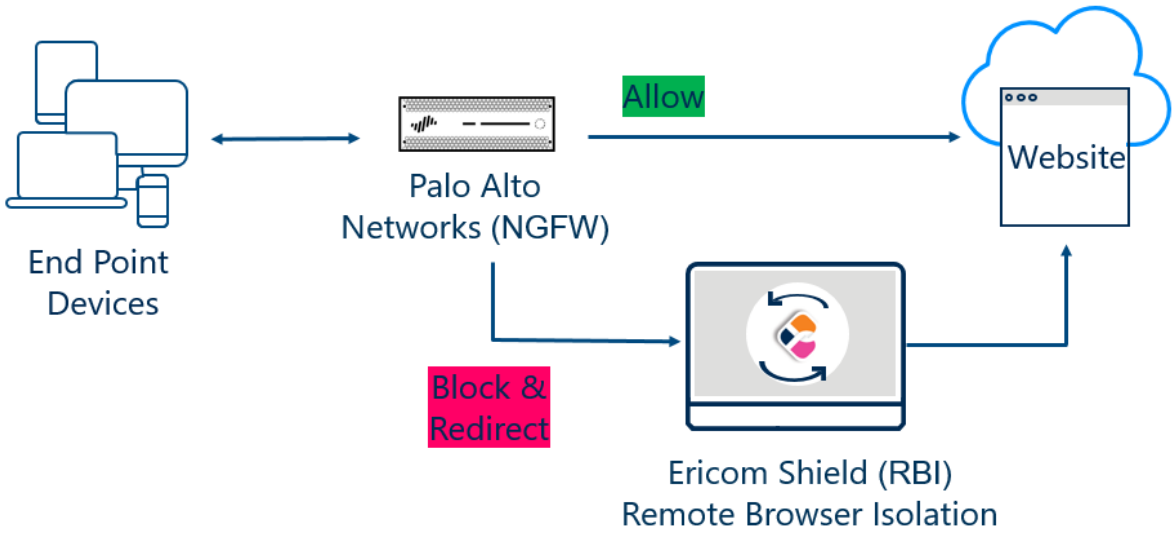
Use case #2

Challenge: End-users are constantly bombarded with phishing links aimed at stealing sensitive data, such as access credentials. Eventually, an email will appear authentic enough to fool a user into entering their corporate credentials that can be used maliciously to gain access to mission critical systems and harm business operations.

Solution: With the Palo Alto Networks next-generation firewall and Ericom Shield integrated solution, the bulk of known phishing sites are blocked by Palo Alto Networks, while harder to categorize sites are opened by Ericom Shield's built-in anti-phishing feature. Ericom Shield allows the site to be opened, but in read only mode, to prevent users from entering sensitive data. If the site is deemed safe after the user interacts with it in read-only mode, it can then be white listed in Palo Alto Networks so that the user can fully interact with this site it.

Benefit: Malicious websites cannot steal end-user's sensitive access credentials and data. The user is able to interact with potentially malicious sites in read-only mode to determine if it is safe.

Diagram



ERICOM
BE CONNECTED, BE SECURE

About Ericom Software

As a global leader in securing and connecting the digital workspace, Ericom offers solutions that secure browsing, and optimize safe desktop and application delivery to any device, anywhere. Ericom enterprise-grade remote browser isolation, secure remote access, and cloud enablement solutions provide a superior work experience and optimize enterprise productivity at tens of thousands of organizations of all sizes, with over ten million users. Founded in 1993, Ericom has offices in the US, UK, and EMEA, and distributors and partners throughout North America, Europe, APAC and Africa. Find out more at https://www.EricomShield.com.

About Palo Alto

We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices. Find out more at www.paloaltonetworks.com.

ERICOM
BE CONNECTED, BE SECURE