Palo Alto Networks ML-Powered Next-Generation Firewall and Extreme Networks

Ensuring User and Application Access Control Across All Points of the Network Infrastructure

Benefits of the Integration

With the Palo Alto Networks Next-Generation Firewall (NGFW) and Extreme Networks integration, your organization can:

- Improve security and compliance by extending user and app awareness to the access edge of the network.
- Mitigate internal threats by allowing the firewall to trigger user quarantine and block listing for application-based violations.
- Improve firewall accuracy by eliminating stale IP address-to-username mappings.
- Simplify firewall management by eliminating complex LDAP/AD integration.

The Challenge

Before deciding to grant a user access to an internal or internet-based resource, it's important to know who the user is, their role in the organization, what application they need to access, where the user is accessing the network, and what the risks are. And to be effective for today's networks, firewalls must be able to associate the IP address with the active user, and Network Access Control (NAC) solutions and edge switches need to know which applications the end system is using. Firewalls that rely on LDAP/Active Directory® (AD) integration for IP address-to-user mapping often end up with stale or misleading information since LDAP/AD doesn't know when a user disconnects from the network. These firewalls also don't help determine where users connect to the network—from wired, wireless, secure, or public locations. Guest access portals that use local authentication also present a problem to LDAP/AD-dependent firewalls because they're invisible to LDAP/AD. Additionally, LDAP/AD integrations tend to be complex for IT teams to configure and manage.

ExtremeControl ExtremeCloud IQ Site Engine

The ExtremeControl™ access control solution from Extreme Networks gives you centralized in-depth visibility and control over all endpoints across your network through one flexible, easy-to-consume dashboard. ExtremeControl securely enables BYOD and Internet of Things (IoT) connections to protect your network from external threats. You can centrally manage and define granular policies to meet compliance obligations and locate, authenticate, and apply targeted policies to users and devices. The ExtremeControl app is available as part of ExtremeCloud™ IQ Site Engine, which extends Extreme Networks' flagship cloud management solution to third-party devices and non-cloud native devices—providing the flexibility to manage your network in the cloud or on-premises.

Palo Alto Networks NGFWs

Palo Alto Networks NGFWs offer a prevention-focused architecture that's easy to deploy and operate. The machine learning (ML)-powered NGFWs inspect all traffic, including all applications, threats and content, and tie that traffic to the user, regardless of location or device type. Automation reduces manual effort, so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters most, and enforce consistent protection everywhere. The user, application and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies and write rules that are easy to understand and maintain.

Palo Alto Networks and Extreme Networks

The integration between Palo Alto Networks NGFW and Extreme Networks ensures fine-grained user and application access control at all points of network access. With Palo Alto Networks NGFW and ExtremeCloud IQ Site Engine, enterprises can realize the benefits of cost savings and increased productivity from new network trends without raising their risk of compliance failure or a security breach.

Integrating Palo Alto Networks NGFW with Extreme Networks' ExtremeCloud IQ Site Engine addresses all four considerations for granting user access and provides seamless application-based policy enforcement at the network edge (wireless and wired), data center edge, and internet edge. Palo Alto Networks NGFW also detects threats originating from internal users and reports the source IP address to ExtremeCloud IQ Site Engine. The user is then located and quarantined, removing the threat and preventing additional damage.

Use Case 1: Providing Client Insights to Security Administrators

Challenge

One of the challenges for security administrators is the rapid identification of client identities and supporting network device information from standard firewall logs. When a malicious event is detected, network administrators need to quickly have a full picture, including a client's username, location, and assigned network security policies, so that informed decisions can be made.

Solution

ExtremeCloud IQ Site Engine solves this challenge and provides Palo Alto Networks NGFWs with accurate and dynamic IP address-to-username mapping. ExtremeCloud IQ Site Engine detects when a user connects to the wired or wireless network, authenticates the user, and sends the IP address, username, location, and policy-applied information to Palo Alto Networks NGFWs. For locally authenticated guest access, the ExtremeCloud IQ Site Engine guest access portal sends the correct guest access username-to-IP address mapping to Palo Alto Networks NGFWs.

The Palo Alto Networks NGFW and Extreme Networks integration offers granular, accurate mapping of user entry and egress from the network and creates higher accuracy for dynamic policy enforcement and reporting. It also provides seamless access control across wired, wireless, and remote access using ExtremeCloud IQ Site Engine as the central point for authentication, authorization, and access (AAA) services.

Use Case 2: Coordinated Security Policy Enforcement at the Edge

Challenge

Due to the increase in ransomware attacks and self-propagating malicious programs such as WannaCry, organizations today need the ability to quickly execute security policies across all points of their network. Security administrators need the ability to deliver unified security policy enforcement at all points on a network.

Solution

Integrating Palo Alto Networks NGFWs with ExtremeCloud IQ Site Engine and policy-based switches and access points allows security policy enforcement at all the connection points to the network, including wireless edge, wired edge, data center edge, and internet edge. When a Palo Alto Networks NGFW detects threats or malicious packets originating from an internal user, it notifies ExtremeCloud IQ Site Engine and supplies the user's source IP address. ExtremeCloud IQ Site Engine then locates the access layer port associated with the IP address, blocks the traffic with a quarantine policy, and block lists the username. If the user connects to another port, they will still be quarantined. And, if the user connects from a wireless access point, they will be quarantined from the access point and block listed.

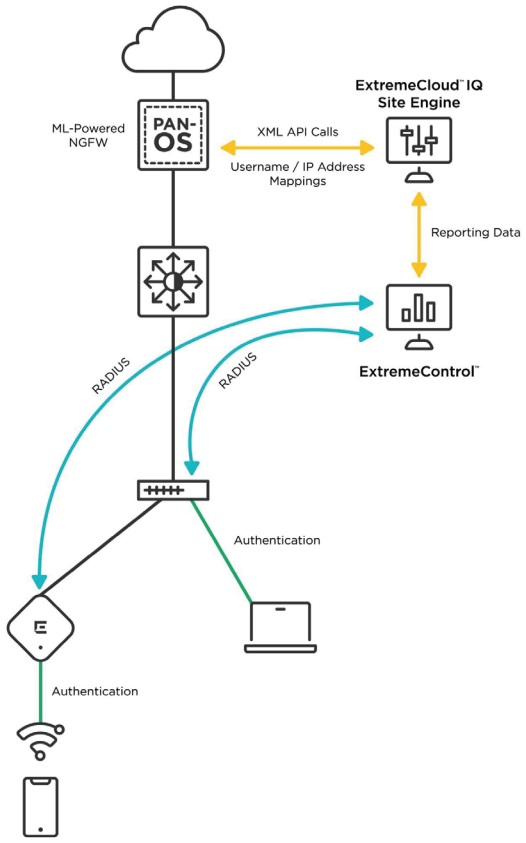

Figure 1: Palo Alto Networks NGFW and Extreme Networks' integration points

About Extreme Networks

Extreme Networks creates effortless networking experiences that enable us all to advance. We push the boundaries of technology, using ML, artificial intelligence (AI), analytics and automation. Over 50,000 customers globally trust our end-to-end, cloud-driven networking solutions and rely on our top-rated services and support to accelerate digital transformation. Learn more at www.extremenetworks.com.

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. For more information, visit www.paloaltonetworks.com.

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