Datasheet

Forescout eyeExtend

Palo Alto Networks® NGFW

Automate context-aware dynamic network segmentation

Today's sophisticated cyberattacks are adept at bypassing traditional network security defenses to break into the enterprise network and gain access to sensitive information. The first line of defense against such attacks, next-generation firewalls (NGFWs) have progressed beyond traditional firewalls to incorporate advanced security functions leveraging deep-packet inspection to allow application-based policy enforcement. But organizations can no longer rely on guarding their perimeter and trusting that they know everyone and everything that is accessing their heterogeneous network in an information technology and operational technology convergence era.

Forescout eyeExtend for Palo Alto Networks Next-Generation Firewall (NGFW) lets you harness real-time visibility across all network-attached devices to help detect today's attacks and implement device identity and context-aware security policies and dynamic network segmentation to stop them.

Challenges

- Implementing network segmentation dynamically across the heterogeneous enterprise network as devices move and networks change
- Enforcing NGFW policies across all devices and users to prevent unauthorized access to sensitive enterprise resources

The Solution

The Forescout platform and Palo Alto Networks Next-Generation Firewall work together to provide policy-based network segmentation on all network connected devices for secure access to critical applications and resources. Forescout eyeExtend for Palo Alto Networks NGFW enables organizations to implement dynamic network segmentation across device types and network tiers—without requiring prior device knowledge or having to rebuild networks.

Today, NGFW administrators must manually identify and assign the correct context to new connecting devices and then allow access based on that context. This staff-intensive process can lead to errors and miss critical devices, resulting in downtime or excessive administrative work. Forescout eyeExtend for Palo Alto Networks NGFW automates the context-aware network segmentation process according to security policies.

eyeExtend for Palo Alto Networks NGFW leverages the comprehensive device visibility and context provided by Forescout eyeSight. eyeSight furnishes contextual device insight on everything from device type, location on the network, hygiene and user information to security posture. The rich, granular device and user insight enables eyeExtend for Palo Alto Networks NGFW assign devices dynamically to

eyeExtend

Benefits

- Augment Palo Alto Networks NGFW defenses with context-aware dynamic network segmentation of all devices the moment they connect to the network
- Streamline network and security operations by automating security policy compliance and segmentation policy enforcement

Highlights

- Provide device security posture and compliance context of all connected devices to the NGFW
- Share real-time device identity information by mapping detected IP addresses to user IDs without the use of agents
- Share device Host Information Profile (HIP) data on security posture
- Dynamically assign devices to predefined NGFW address groups based on granular device and user context
- Enforce user- and role-based network access in real time

predefined Palo Alto Networks NGFW address groups. This helps organizations implement dynamic network segmentation, assign access to resources on the move and create context-aware security policies.

In summary. Forescout eyeExtend for Palo Alto Networks NGFW helps to reduce your attack surface, prevent unauthorized access to sensitive resources and minimize malware proliferation and data breaches.

Use Cases

Implement dynamic network segmentation

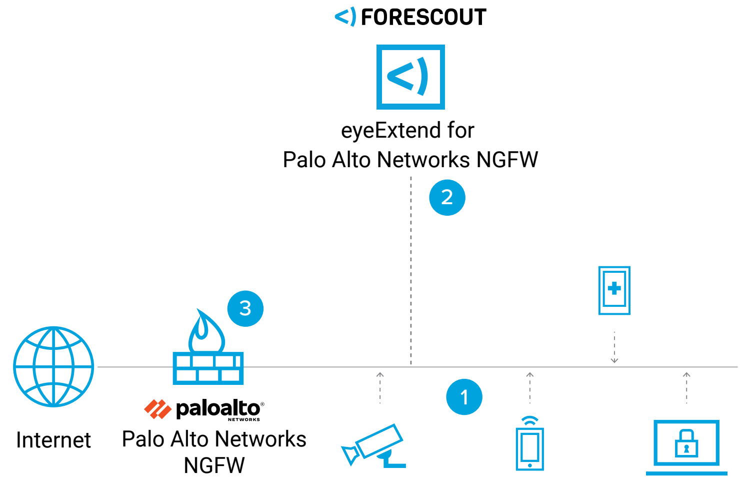
Forescout eyeExtend for Palo Alto Networks NGFW matches connecting devices' IP addresses with NGFW user IDs and captures user information, device properties, classification and security posture, including Host Information Profile (HIP) data. It then dynamically tags and assigns devices to their appropriate Palo Alto Networks NGFW address groups. Based on predefined roles, the NGFW allows differentiated user access according to functional need. For example, visitors can be restricted to internet use only, contractors to internet and Exchange Server and partners to internet and internal ordering. This enables business continuity while preventing unauthorized access to sensitive resources.

Enhance firewall intelligence for better policy creation and enforcement

Forescout platform pulls essential Host Information Profiles (HIP) on mobile, guest and BYOD devices and shares with the NGFW, which is otherwise unavailable without the Palo Alto Networks Global Protect Agent installed on network devices. HIP data includes information on the latest security patches, antivirus definitions, disk encryption, jailbroken status and whether custom corporate applications are running on devices. eyeExtend also maps device IP addresses discovered by the Forescout platform to firewall User-IDs. The in-depth device context and user information helps the firewall to segment devices based on user ID, Tagging and HIP data and improve access policies for devices.

Continuously assess device compliance and enforce network segmentation policies

The Forescout platform continuously monitors the security posture of all connected devices. If a device falls out of compliance—due to out-of-date antivirus software, for example—eyeExtend sends an automatic notification to the network administrator, removes the device from its assigned NGFW group and reassigns it to a different group with more limited network access.



1. Forescout discovers, classifies and assesses devices as they connect to the network
2. Forescout eyeExtend sends one or more of the following properties to the Palo Alto Networks NGFW
   a. User ID to IP mapping
   b. Device security tags
   c. Device posture and compliance context
   d. HIP information
3. Palo Alto Networks NGFW leverages this information from Forescout to apply identity and context-aware security and access policies

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com