# Palo Alto Networks Next-Generation Firewalls and Forescout Technologies, Inc.

## Automate Context-Aware Dynamic Segmentation to Enable Secure Access to Critical Apps and Resources

### Benefits

The integration between Palo Alto Networks NGFWs and Forescout eyeExtend allows you to:

- **Apply segmentation to devices immediately:** Forescout eyeExtend augments Palo Alto Networks NGFW defenses with context-aware dynamic network segmentation of all devices the moment they connect to your network.
- **Streamline IT operations:** Automate security policy compliance and segmentation policy enforcement with Forescout eyeExtend for Palo Alto Networks NGFWs and reduce work for network and security teams.
- **Get insight on device identity and security in real time:** Forescout eyeExtend enables real-time sharing of device identity information by mapping detected IP addresses to user IDs without the use of agents. It also shares device host information profile (HIP) data on security posture and provides device security posture and compliance context of all connected devices to Palo Alto Networks NGFWs.

## The Challenge

In an era of information technology and operational technology convergence, your organization can't rely on guarding the perimeter and trusting that you know everyone and everything accessing your heterogeneous network. Today's sophisticated cyberattackers can bypass 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 have progressed beyond traditional firewalls to incorporate advanced security functions that use deep-packet inspection to allow application-based policy enforcement. With Forescout eyeExtend for Palo Alto Networks Next-Generation Firewall (NGFW), you can 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.

## Forescout eyeExtend

Forescout eyeExtend products automate Enterprise of Things (EoT) security processes between the Forescout platform and other IT and security solutions to improve your organization's operational efficiency and overall security posture.

You can integrate Forescout device intelligence and enforcement capabilities across your current IT and security investments to eliminate device visibility blind spots, automate cross-product workflows, and accelerate your response to risks, incidents, and compliance gaps.

## Palo Alto Networks NGFWs

Palo Alto Networks Machine Learning (ML)-Powered NGFWs inspect all traffic at Layer 7 and offer a prevention-focused architecture that's easy to deploy and operate. Automation reduces manual effort, so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere. 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. The 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 Forescout Technologies, Inc.

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.

The Forescout platform and Palo Alto Networks NGFW work together to enable organizations to implement dynamic network segmentation across device types and network tiers—without requiring prior device knowledge or the need to rebuild networks. Forescout eyeExtend for Palo Alto Networks NGFW automates the context-aware network segmentation process according to security policies.

The process (illustrated below) works like this:

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 Palo Alto Networks NGFW:
   - User ID to IP mapping
   - Device security tags
   - Device posture and compliance context
   - HIP information

3. Palo Alto Networks NGFW uses the information from Forescout to apply identity and context-aware security and access policies.

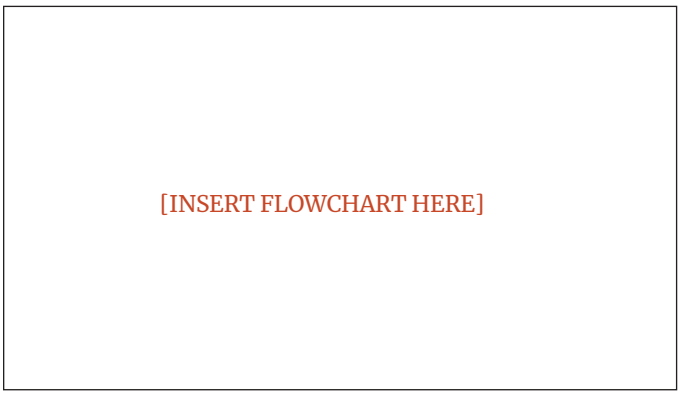


**Figure 1:** eyeExtend and Palo Alto Networks NGFW apply identity and context-aware security and access policies

### Use Case 1: Implementing Dynamic Network Segmentation

#### Challenge

Your organization needs to provide differentiated user access according to users' functional needs. For example, you may need to restrict visitors' access to internet use only, contractors to internet and Microsoft Exchange Server, and partners to internet and internal ordering. You also need to provide this access while making sure to protect critical resources and support user productivity.

#### Solution

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 HIP data. It then dynamically tags and assigns devices to their appropriate Palo Alto Networks NGFW address groups. Based on predefined roles, the Palo Alto Networks NGFW allows differentiated user access according to functional need. This enables business continuity while preventing unauthorized access to sensitive resources.

### Use Case 2: Enhancing Firewall Intelligence to Improve Policy Creation and Enforcement

#### Challenge

Your business wants to improve access policies for various devices by equipping NGFWs with in-depth device context and user information so the firewalls can segment devices based on user ID, tagging, and HIP data.

#### Solution

The Forescout platform pulls essential HIP data on mobile, guest, and BYOD devices and shares it with the Palo Alto Networks NGFW. The Palo Alto Networks GlobalProtect™ agent installed on network devices makes this information exchange possible. HIP data includes information on the latest security patches, antivirus definitions, disk encryption, and jailbroken status, and whether custom corporate applications are running on devices. Forescout eyeExtend also maps device IP addresses discovered by the Forescout platform to firewall user IDs.

### Use Case 3: Continuously Assessing Device Compliance and Enforcing Network Segmentation Policies

#### Challenge

Your business needs to continuously monitor the security posture of all connected devices to ensure compliance.

#### Solution

With Forescout eyeExtend for Palo Alto Networks NGFW, you can continuously track the security posture of all network-connected devices. If a device falls out of compliance—due to out-of-date antivirus software, for example—Forescout eyeExtend automatically notifies the network administrator, removes the device from its assigned Palo Alto Networks NGFW group, and reassigns it to a different group with more limited network access.

## Protecting Critical Resources Together

Forescout eyeExtend for Palo Alto Networks NGFW helps reduce your attack surface, prevent unauthorized access to sensitive resources, and minimize malware proliferation and data breaches. Your security and network teams can easily implement dynamic network segmentation, assign access to resources on the move, and create context-aware security policies. Forescout eyeExtend for Palo Alto Networks NGFW uses comprehensive device visibility and context provided by Forescout eyeSight to assign devices dynamically to predefined Palo Alto Networks NGFW address groups.

## About Forescout Technologies, Inc.

Forescout Technologies, Inc. actively defends the EoT by identifying, segmenting and enforcing compliance of every connected thing. Forescout provides device intelligence that allows its customers across every industry to accurately classify risk, detect anomalies and quickly remediate cyberthreats without disruption of critical business assets. Learn more at www.forescout.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.

paloalto NETWORKS | FORESCOUT

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