Forescout eyeExtend
for Check Point® 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 (NGFW's) have progressed beyond traditional firewall to incorporate advanced security functions. But organizations can no longer rely on guarding their perimeter and trusting that they know everyone and everything that is accessing their heterogenous network in an information technology (IT) and operational technology (OT) convergence era.

Forescout eyeExtend for Check Point NGFW lets you harness real-time device visibility across all network attached endpoints to help detect today's attacks and automate response workflows for applying identity- and context-aware security policies and network segmentation to stop them.

Challenges

- Enforcing NGFW policies based on not only users but also devices across the heterogeneous enterprise network as devices change and move
- Implementing network segmentation dynamically across all devices and users in real time to prevent unauthorized access to sensitive enterprise resources

The Solution

The Forescout platform and Check Point Next-Generation Firewall (NGFW) work together to provide complete device visibility and policy-based dynamic network segmentation for secure access to critical applications and resources. Forescout eyeExtend for Check Point 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, assess posture and assign the correct context to new connecting devices and then allow access based on the correct context. This staff-intensive process could lead to errors, including missing critical devices—resulting in downtime or excessive administrative work. Forescout eyeExtend for Check Point NGFW automates the context-aware network segmentation process as per security policies. eyeExtend for Check Point NGFW leverages the comprehensive device visibility and context provided by Forescout eyeSight. Forescout eyeSight furnishes contextual device insight on everything from device type, location on network, and user information to security posture for systems connected to your heterogeneous network. The rich, granular device and user insight enables eyeExtend for Check Point NGFW to assign devices dynamically to predefined

eyeExtend

Benefits

- Gain complete device visibility and in-depth context across all network-connected systems including corporate, personal, guest, virtual, cloud instances, IoT and OT devices
- Augment Check Point NGFW defenses with dynamic, context-aware network segmentation of all devices the moment they connect to the network

Highlights

- Discover, auto-classify and assess all IP connected devices
- Get device security posture and compliance context of all devices
- Receive real-time device identity information by mapping detected IP addresses to NGFW user IDs
- Dynamically assign devices to predefined NGFW groups based on granular device and user context
- Enforce user- and role-based network access control in real time, reducing dependency on network devices

Check Point NGFW 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 Check Point NGFW helps to reduce your attack surface, prevent unauthorized access to sensitive resources and minimize malware proliferation and data breaches.

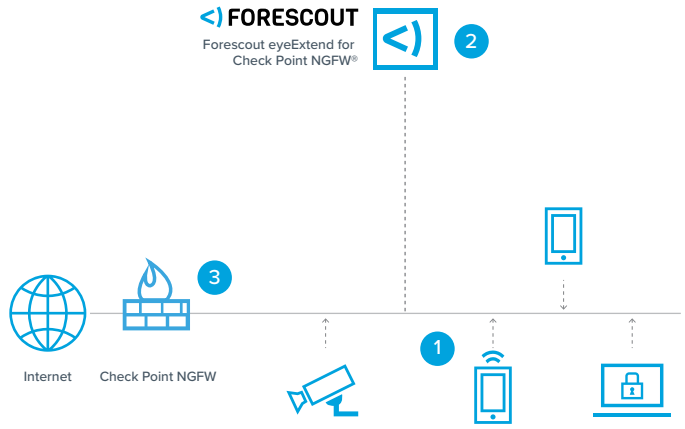
Use Cases

Enable dynamic network segmentation

Forescout eyeExtend for Check Point NGFW matches connecting devices' IP addresses with NGFW user IDs and captures user information, device properties, classification and security posture. It then dynamically assigns these devices to their appropriate Check Point NGFW groups. Based on pre-defined roles, Check Point NGFW allows differentiated access to these users such as visitors access to internet, contractors to Exchange server and partners to only internal ordering, thereby restricting them to their individual functional needs. This enables business continuity while preventing unauthorized access to sensitive resources.

Continuously assess device compliance and enforce network segmentation policies

The Forescout platform continuously monitors device posture and compliance context 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 eyeSight discovers, classifies and assesses devices as they connect to the network
2. Forescout eyeExtend sends one or more of the following properties to NGFW
   - User ID to IP mapping
   - Device security tags
   - Device posture & compliance context
3. The NGFW leverages the information from Forescout eyeExtend to apply identity and context-aware security policies and enforce access controls

FORESCOUT

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