Extreme Networks Integration with Fortinet FortiGate Platform Firewalls

Benefits

- Delivers real-time User-to-IP mapping to Fortinet Firewalls for more accurate policy enforcement
- Mitigates internal threats via access-layer security controls
- Provides end-system status to Fortinet Firewalls in real-time, including security posture, location tracking, user, and applications being used

Requirements

- Extreme Networks NetSight Advanced, Version 4.1 or later
- Extreme Networks NAC 4.1 or later with 802.1X or Web Authentication/ Registration where usernames are populated into NAC
- Edge Switches that support RADIUS Accounting must be integrated within NAC)
- Fortinet FortiGate Platform Firmware Version 5.0, Build 208 or later

Real-time Protection Against Network Threats

The effectiveness of any firewall is contingent on accurate policy enforcement, but occurrences like users disconnecting from the network or connecting public versus private networks are often not reflected in firewall data sources. Adding to security challenges are guest access portals that use local authentication but which remain invisible to the firewall directory, resulting in access to the network without proper verification.

The subsequent inaccuracies can result wrong security policy being applied to wrong user and application at the wrong time.

Extreme Networks integration with Fortinet FortiGate Firewalls enables security managers to resolve these challenges by delivering more accurate policy enforcement throughout the network. The solution uses Extreme Networks NetSight Advanced management application to provide FortiGate with granular, accurate mapping of user entry and egress from the network, and provide seamless policy control across wired, wireless and remote access points.

COMPREHENSIVE NETWORK-DRIVEN SECURITY

Using NetSight as the central point for authentication, authorization and access (AAA) services, the integrated solution streamlines policy enforcement and automates manual tasks while enabling IT administrators to troubleshoot security issues faster and more effectively.

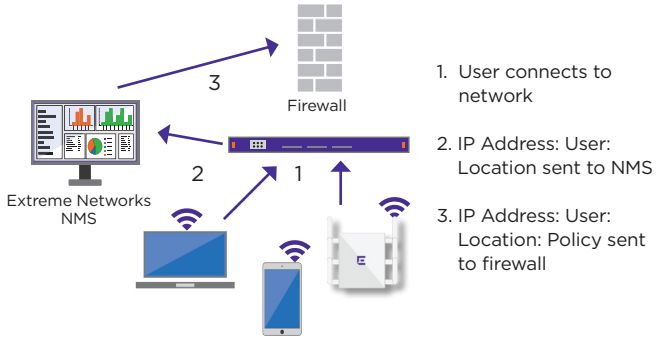
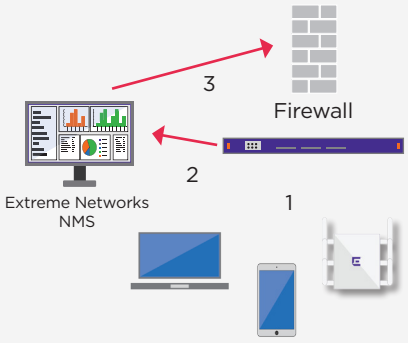


Figure 1. User to IP Address Mapping



1. User disconnects from network
2. IP Address: User: Disconnect Message sent to NMS
3. IP Address: User: Disconnect Message sent to firewall

Figure 2. Detecting User Disconnects

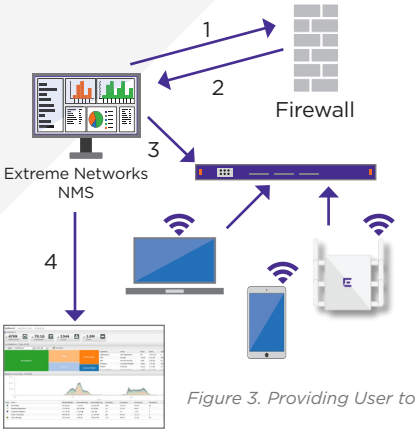
As a user connects or disconnects to the network, a state change indication is sent from NetSight to the FortiGate mapping tables to overwrite stale entries and ensure accurate policy application. When a credentialed user is successfully authenticated by NetSight, the FortiGate handler sends a Radius accounting start to the FortiGate UTM Box, enabling the firewall to create a username and a group IP mapping, and applying a policy to that mapping.

NetSight increases the accuracy of user-to-IP mapping by sharing the IP address, username, location, and policy information to the FortiGate Firewall. To enable locally-authenticated guest access, NetSight also sends Guest Access User-to-IP address mapping to the FortiGate firewall. The real-time integrity of the Username-to-IP address mapping is maintained by NetSight's support for RADIUS Accounting. When a user connects or disconnects from the network, NetSight will notify the Fortinet firewall of the state change, guaranteeing that the mapping is correctly cleared in the firewall.

APPLICATION VISIBILITY AT THE EDGE

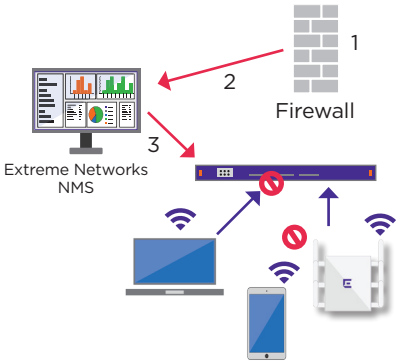
To deliver granular security at the wireless and wired edge, NetSight shares information with edge switches about which applications specific users are using. This provides extended visibility and control to block unnecessary or malicious applications before they negatively impact the network. Application visibility at the edge also allows NetSight to report, which users are affected by specific outages or service upgrades, or identify users that are leveraging or abusing specific applications.

When the FortiGate firewall detects threats or malicious packets originating from an internal user, it notifies NetSight and supplies the source IP address of the user. NetSight then locates the access layer port associated with that IP address, blocks the traffic with a quarantine policy, and blacklists the user name. If the user connects to another port they will still be quarantined. If the user is connecting from a wireless access point they will be quarantined from the AP and blacklisted.



1. NMS requests application information for user.
2. Firewall returns IP: User: Application
3. Modified policy pushed to switch
4. NMS generates application use reports

Figure 3. Providing User to Application Mapping



1. Firewall detects threat
2. Firewall sends notification to NMS
3. NMS Quarantines user and blocks traffic at switch port or AP

Figure 4. Enforcement at Switch Port or AP

The increasing and complex demands of organizations today require the highest level of security to protect business-critical network communications. Extreme Networks and Fortinet FortiGate integration ensures fine-grained user and application control at all points of the network and Internet edge, wired and wireless access points, and the data center. The solution allows organizations to gain the benefits of more accurate real-time policy enforcement and increased IT productivity without increased security risk.

Extreme networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800