Integration of ExtremeControl™ with Fortinet Fortigate Firewalls

Real-time Protection Against Network Threats

In today’s mobile environment user connections are fluid: Users disconnect, move to different locations, or access private or public networks. These access changes are often not accessible by a firewall or from guest portals with local authentication. With these gaps in the data, unauthorized devices and users can gain unauthorized access to the network and introduce security risks.

To close access security gaps, we integrated our network access control product, ExtremeControl, with the Fortinet Fortigate next generation firewall. With this solution, ExtremeControl provides additional end-system data (security posture, username, entry and egress, location, user, and application info) to Fortigate, so it can inspect network traffic based on rules reflecting all access data it received. Based on Fortigate’s data, ExtremeControl then enforces consistent policy throughout the wired and wireless network to avoid network vulnerabilities.

The integration between the Extreme Networks portfolio and the Fortinet Fortigate firewall allows customers to apply different firewall rules based on location without the need to separate locations by VLAN. They can also apply different firewall rules based on function groups (eg. Sales vs Finance) and based on device type (eg. Mac vs Windows vs iPhone).

Fortinet and Extreme Networks tested and validated this solution to offer you unparalleled security protection against cyberattacks. We at Extreme are dedicated to offering you the industry’s first cloud-driven, end-to-end enterprise network. Our 100% in-sourced support and services are working with many customers and are available to share their experience and knowledge.

Benefits

• Deliver real-time user-to-IP mapping to Fortinet Firewalls for more accurate policy enforcement
• Mitigate internal threats via access-layer security controls
• Provide end-system status to Fortinet Firewalls in real-time, including security posture, location, user, and application info

Integrations

• Fortinet Fortigate Firewalls
• ExtremeControl™
The above diagram shows the components required for the Fortigate integration. Clients connect either wired or wirelessly to the Extreme Networks infrastructure. The customer must have the Extreme Management Center for connectivity to the infrastructure and Fortigate firewall along with ExtremeControl to enforce policy on the endpoints.

The user connects to the network either wired or wirelessly. Radius communication goes thru ExtremeControl and based on Radius response assigns the user a policy profile.

The Radius Access Accept is sent to the access switch/access point. Once the address resolution is complete, the Extreme Management Center knows the IP address of the end-system, and the radius accounting message is sent to the firewall. The radius accounting message contains the OP address, username, and Access Control Profile.

The Fortigate firewall applies its firewall rules on traffic from the end systems based on the assigned group/profile. All traffic, for users with an associated profile, traversing the firewall (outbound/internet) now have rules applied.