INTEGRATION BRIEF

THE FORTINET & CLAROTY JOINT SOLUTION

The integration between Fortinet and Claroty combines Claroty xDome with the FortiGate and FortiNAC solutions, augmenting the Fortinet Security Fabric with industry-leading asset inventory, threat detection, and segmentation capabilities. Integrating xDome, the most powerful Extended Internet of Things (XIoT) — IT, OT, IoMT, IoT, and other connected devices — cybersecurity solution, into the Fortinet Security Fabric extends and deepens coverage across the entire digital attack surface.

The resulting joint-solution provides holistic visibility and monitoring coverage across the XIoT, as well as seamless creation and real-time enforcement of firewall and NAC policies. These capabilities greatly streamline and optimize otherwise-tedious and error-prone aspects of network segmentation initiatives for XIoT environments, ultimately allowing for automated protection against potentially threatening activity and other violations.

Claroty xDome integrates with Fortinet's next generation firewall, FortiGate, and Fortinet's network access control solution, FortiNAC, to provide organizations with accurate identification and analysis of all XIoT devices in their environments. This information helps streamline the ongoing management and maintenance of assets and automates the enforcement of dynamic access and micro-segmentation policies that keep the network safe. xDome's Network Policy Management capability leverages Claroty's domain expertise to recommend segmentation policies that can be easily and automatically enforced via existing infrastructure.

How It Works

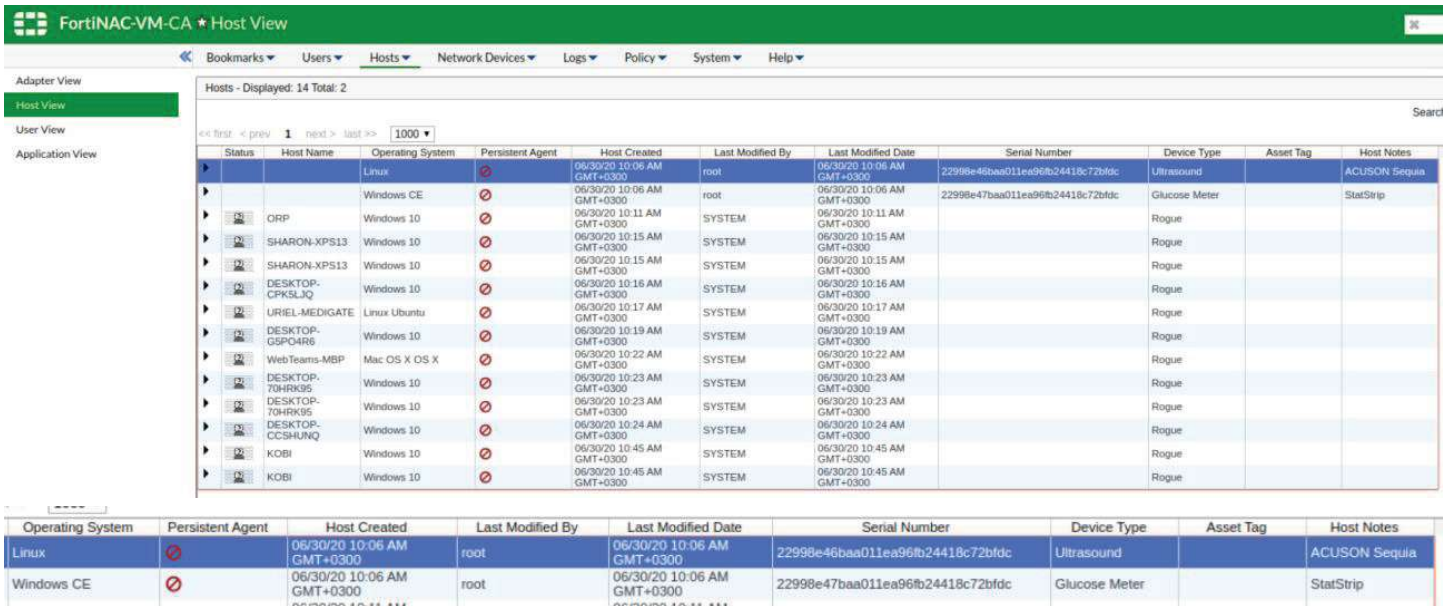
Claroty xDome continuously monitors the network to provide a real-time inventory of all XIoT devices connecting to the network and alerting to risky or anomalous activity. Claroty xDome leverages the broadest and deepest portfolio of XIoT protocol coverage, along with Claroty Team82's domain-specific research into these protocols, to provide a highly detailed, centralized inventory of XIoT assets. xDome feeds this information, via Fortinet's Fabric-Ready APIs to FortiNAC and transfers IP-based tags to FortiGate, which matches the IP of a device with a tag based on its type, vendor, and model. This flow of information enables the automated creation and precise enforcement of NAC and firewall policies to prevent risky communications and attack propagation.

Key Capabilities

Visibility and Insights

Claroty xDome collects and interprets network traffic to establish comprehensive asset visibility. This unmatched asset inventory enables FortiNAC and FortiGate to better manage and enforce network security policies.

- After collecting network traffic, Claroty xDome discovers all XIoT assets to create a comprehensive asset inventory.
- Through integrations with other IT management systems and feeds from external and proprietary sources, xDome identifies device locations and available patches and updates.
- xDome feeds the detailed XIoT device information, which includes manufacturer, make, model, OS, soft ware versions, embedded software, etc., to FortiNAC and FortiGate to ensure they have complete and accurate device inventories and profiles to inform and optimize their respective policies.
- xDome assesses the risks of each asset, providing a risk score and empowering confident action with the ability to simulate how a change will impact that risk score.



Detection and Prevention

Claroty xDome is built to detect threats and other vulnerabilities within networks, empowering FortiNAC and FortiGate to act on potential threats and issues before they impact network operations.

- xDome continuously monitors network traffic and device behaviors, examining network and device protocols and comparing activity with expected behavior to pinpoint the earliest indicators of potential threats.
- When xDome identifies a potential threat, the solution alerts administrators in real-time with precise contextual information to optimize response efforts.
- Administrators can then take immediate action against rogue or otherwise suspicious devices, anomalous activity, and other indicators of potential threats through a variety of mechanisms within FortiGate and FortiNAC, such as quarantining the device, restricting internet access, placing the device in a separate VLAN, and/or refining respective policies to minimize exposure.

Network Policy Enforcement

Claroty xDome provides visibility and network policy recommendations, empowering FortiGate and FortiNAC to support effective network segmentation and zero trust architecture.

- xDome generates expert-defined recommendations for network policies based on the roles, behaviors, operational context, and other details of all devices and activity throughout the entire XIoT environment.
- FortiGate and FortiNAC use xDome's device and threat information to further streamline the creation and enforcement of network policies and firewall rules to support effective segmentation.
- FortiGate can also extend the applicability and ease of xDome's recommended firewall policies by dynamically refining them based a device's IP, network zone, tag-to-tag traffic, port, and protocol, among others, and then automatically enforcing them to optimize protection.
- FortiNAC can establish micro-segmentation by enforcing network access policies in real-time to contain attacks and prevent unauthorized access.
- FortiNAC, such as quarantining the device, restricting internet access, placing the device in a separate VLAN, and/or refining respective policies to minimize exposure.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally.

For more information, visit claroty.com or email contact@claroty.com.