MEDIGATE & PALO ALTO NETWORKS INTEGRATION

A Superior Cybersecurity Solution for Connected IoT and IoMT Devices

Medigate by Claroty and Palo Alto Networks have teamed up to deliver a best-in-class solution that addresses the security risks of connected devices in healthcare networks.

KEY CAPABILITIES

- **Fingerprint all connected devices with granular detail**
- **Create External Dynamic Lists (EDL) to group devices for security controls**
- **Utilize EDL groups to build granular policies in your Palo Alto Networks NGFW**

KEY BENEFITS

- **Efficiently and effectively identify and secure connected devices**
- **Mitigate security flaws and reduce the risk of a successful cyberattack**
- **Enhance and simplify controls to prevent infected devices from compromising other systems**

THE CHALLENGE

Protecting the Invisible

Securing the connected devices that underpin healthcare networks and enable care delivery requires a purpose-built solution powered by full visibility into each device's manufacturer, its proprietary protocols, and the clinical workflows and context in which it operates.

However, the diversity of device types, range of manufacturers and software versions, and prevalence of proprietary protocols in healthcare networks make full visibility exceedingly difficult to attain. Without it, simply identifying a device and its communication profile — much less defining and enforcing safe and effective firewall policies to help protect it — is impossible.

Managing the Undetected

Clinical context is critical for detecting abnormal device behavior in healthcare networks. Only a deep understanding of clinically valid workflows and connected device protocols can enable the efficient detection of suspicious or otherwise anomalous device behavior.

THE SOLUTION

Overview

The integration between Medigate by Claroty and Palo Alto Networks combines Medigate's clinical expertise and innovative platform with Palo Alto Networks's proven Next-Generation Firewall (NGFW) capabilities to enable healthcare organizations to leverage their existing Palo Alto Networks NGFW investment to extend comprehensive cybersecurity to their clinical networks.

How it Works

Medigate's platform utilizes the External Dynamic List (EDL) function within the Palo Alto Networks NGFW to share highly granular device information. This information can then be queried by the NGFW via an EDL on a regular basis to reflect any device changes, allowing for the creation of granular-yet-dynamic security policies, tagging of devices, and many other key functions to be performed on the firewall.

More specifically:

Step 1: Medigate's physical appliance is quickly and easily installed in the clinical network and then integrated with existing Palo Alto Networks NGFWs.

Step 2: The Medigate appliance analyzes network traffic to automatically identify and populate all highly granular device information within a central, comprehensive inventory in the Medigate platform.

Step 3: The NGFW queries this inventory for the following pieces of device information via an EDL to enrich its data and enable efficient, clinically-informed security policies:

- **Device Category** (i.e. Medical)
- **Device Type** (i.e. MRI)
- **Device Manufacturer** (i.e. Philips)

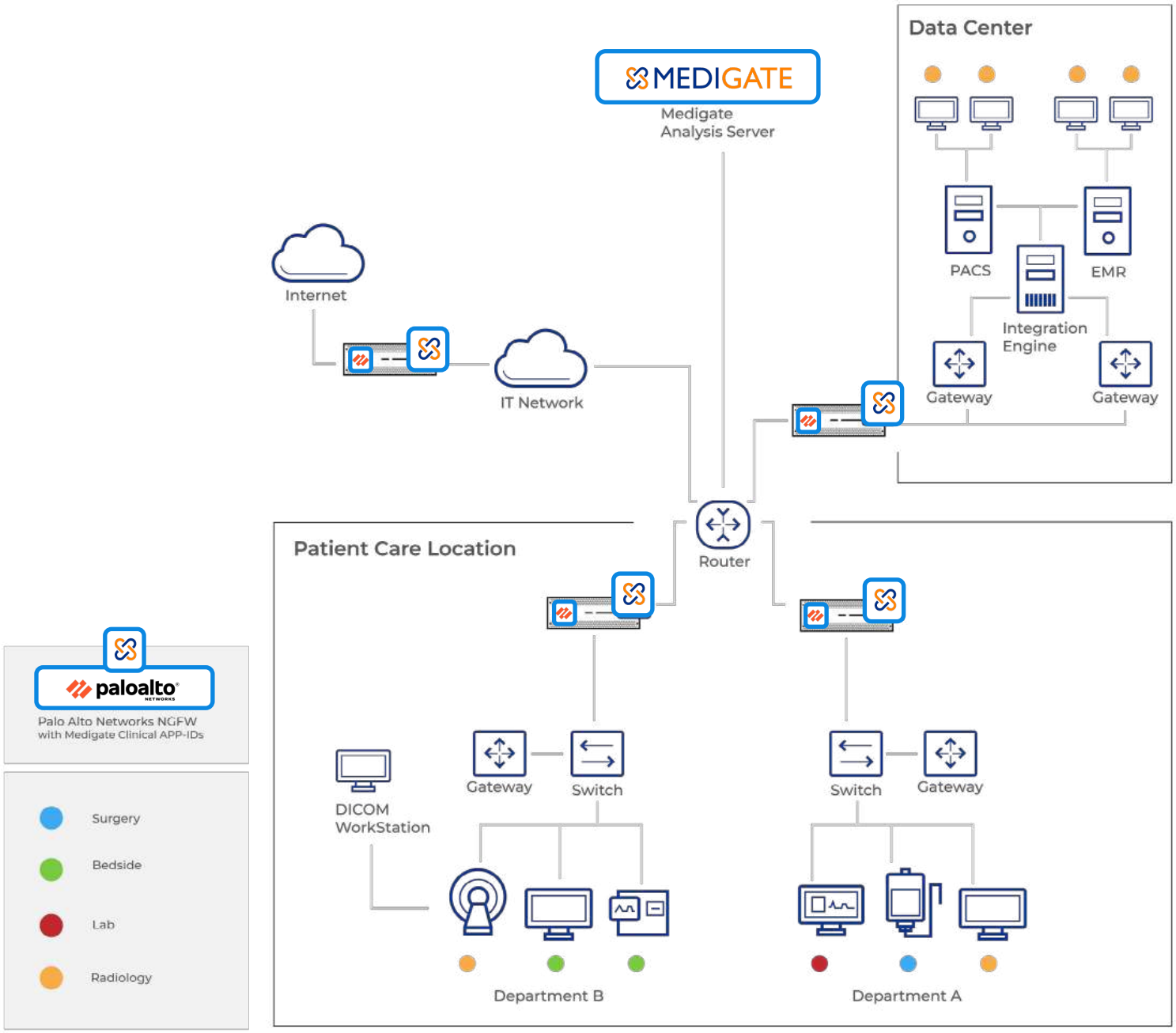
Step 4: The NGFW can then re-query this information via an EDL on a regular basis to ensure firewall policies are updated as relevant changes occur, such as a device leasing a new IP through DHCP, for example.

This functionality allows for the creation of dynamic firewall policies based on asset characteristics (i.e. all MRIs made by Philips, for instance) and enables all devices that meet such a policy's criteria to be automatically identified with each query.

THE SOLUTION

Reference Architecture

Previously, firewall rules had to rely on network zones, IP addresses, and ranges. Instead, this integration uses EDLs based on device functionality and vendor to add new levels of granularity and, ultimately, empower healthcare organizations with far more specific (and effective) security policies. A sample reference architecture for the integration is as follows:



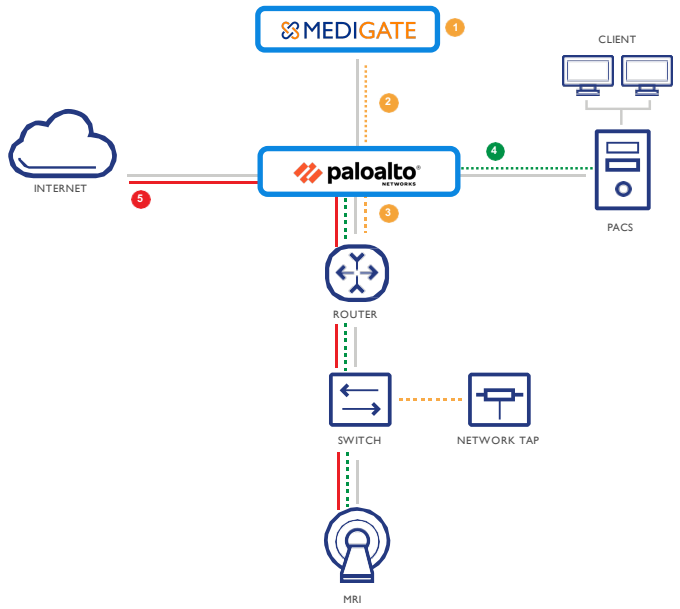
THE SOLUTION

Policy Enforcement Example

Healthcare organizations can enforce policies to block a device tagged as an MRI, for example, from accessing the internet or other zones within the clinical network. Such policies can also be enforced to allow the device to communicate only with its dedicated imaging server.

Moreover, the Port and Protocol Restriction features allow control over not only with which devices the MRI could communicate, but they can also ensure it communicates only with predefined ports and via proprietary protocols set by the manufacturer.

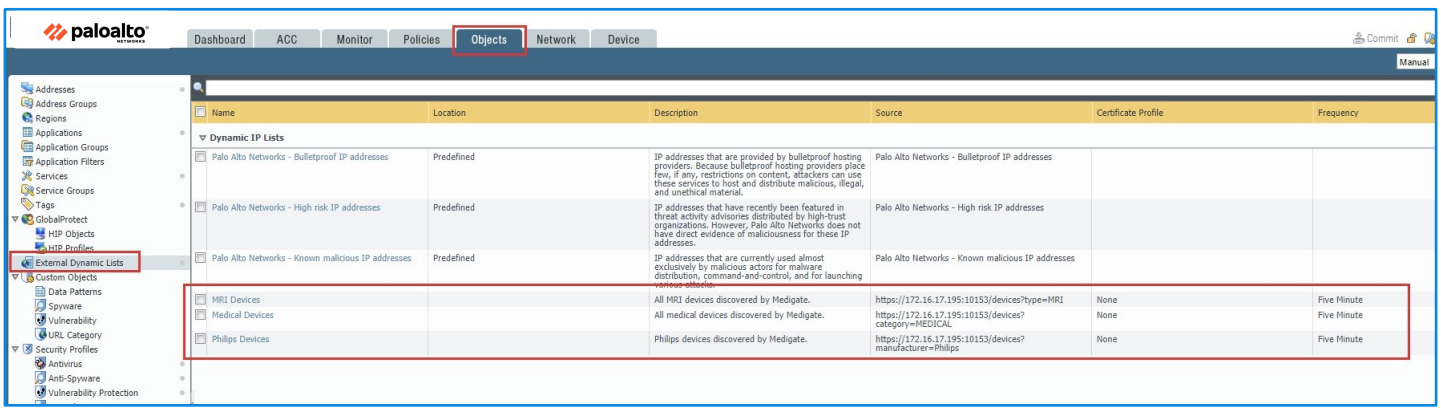
As such, the MRI in this example would only be able to communicate with its imaging server via DICOM protocol. SMB packets would be intercepted.



1. Medigate identifies connected medical devices, and granular information such as type and vendor.
2. Medigate creates an External Dynamic List with this type and vendor, and the Palo Alto NGFW queries this list to identify all specific MRIs.
3. A security policy is set in the firewall by the administrator, which allows the MRI to communicate only with the PACS. Additionally, rules are added to deny communication to the internet.
4. The MRI successfully manages to connect to the PACS.
5. A forbidden connection attempt from the MRI to the internet is blocked.

---

2 Medigate creates an External Dynamic List with this type and vendor, and the Palo Alto NGFW queries this list to identify all specific MRIs.



ABOUT

About Medigate by Claroty

Securing the clinical environment requires a new security strategy and coordinated approach as IT, OT, IoT and physical systems converge and the threat of bad actors exploiting vulnerabilities across new and old infrastructure is increasing. It also requires detailed knowledge of every connected device, their proprietary protocols, and the clinical workflows to which they are integral.

Medigate by Claroty gives you the confidence to see, secure, and manage all devices connected to your network and turn the associated data into a powerful resource. It means the end of any compromise between security and usability – put simply, it allows you to connect with confidence.

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. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.