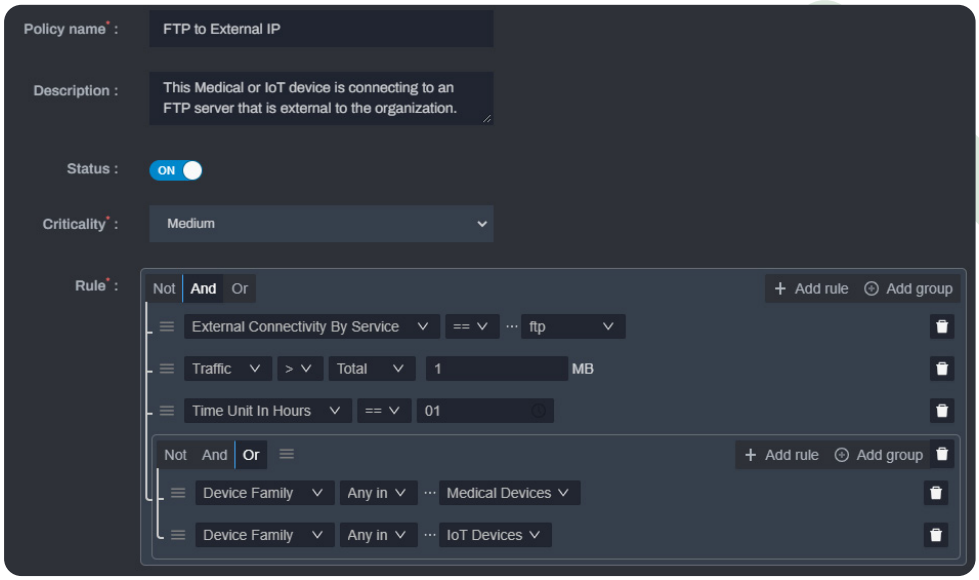
Policy Management

While suspicious traffic can be detected using different kinds of security and anomaly detection techniques, every organization has its own set of corporate security policies they want to monitor on the network to ensure they are being followed. That's why Asimily Insight offers the most powerful policy management functionality available in the medical device security space. Using Insight, you can create policies that define a network anomaly event, using more than 30 parameters, including attributes of the device such as its model or function and properties of the network connection such as the traffic volume, destination, port and protocol. Policies can be further customized on a per-network, per-facility, or per-device type basis, since not all policies will be appropriate for the entire organization.

Asimily also leverages this policy engine to deliver updated policies to customers on a frequent basis. These policies cover emerging threats, such as active malware campaigns and recently-released vulnerabilities under active exploitation. Asimily's security research team, along with the Customer Success team, actively collaborates with customers to develop new policies that meet their needs.

Anomalies created by custom policies are treated just like any other anomaly in Insight. You can triage and assign them to others in your organization, or manage them in your SIEM using Asimily's integrations.

What you don't know about your network can hurt you. Try Asimily Insight and discover what you've been missing.



Technology

- Advanced boolean logic allows virtually any policy to be expressable
- 30+ parameters available for rule creation
- Built-in security and anomaly policies updated regularly for emergent threats

Example Use Cases

- Detect "low and slow" data exfiltration attacks that others might miss
- Discover network issues that add risk, such as overly permissive firewall rules or misconfigured DNS
- Track vendors and their access to devices in the field
- Discover if exploit vectors for critical vulnerabilities are present in the network