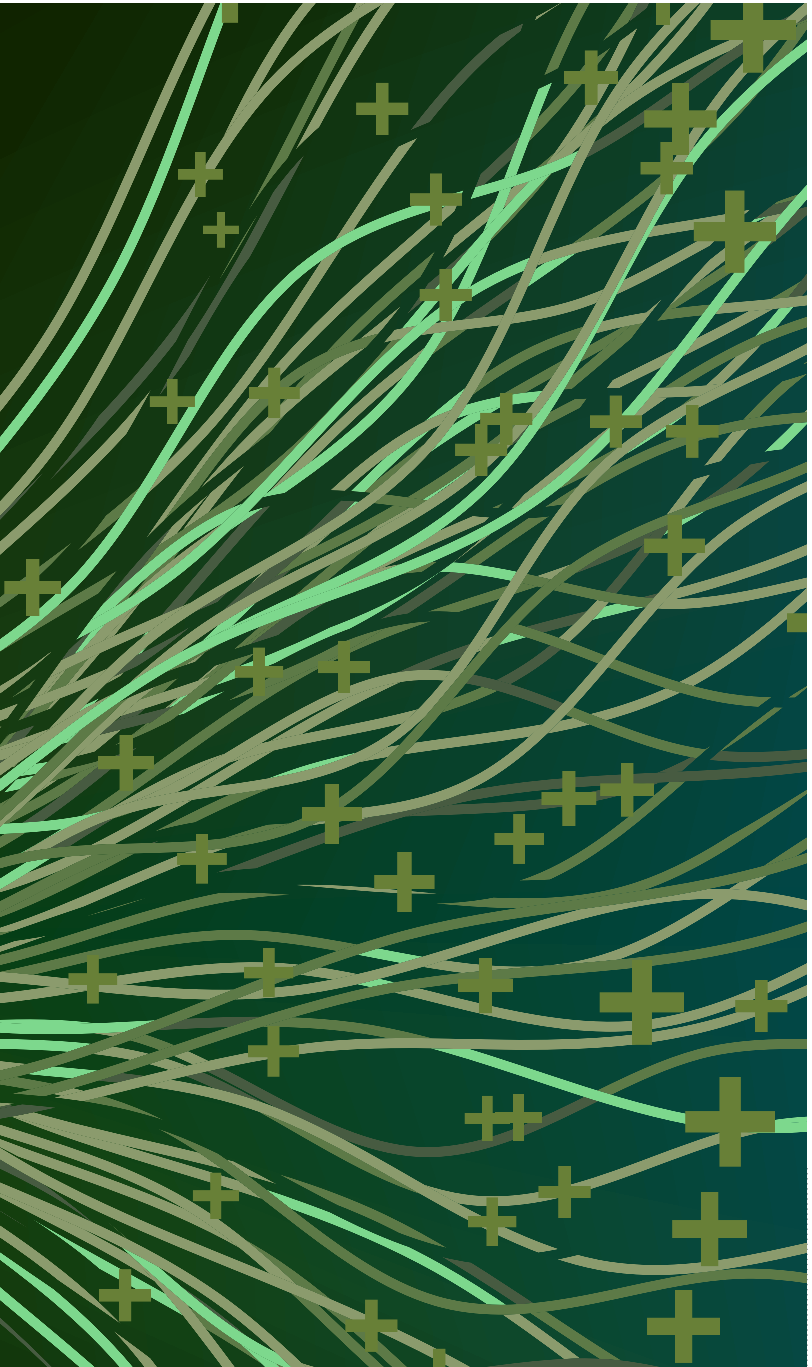

E-Guide

NETWORK-BASED CONTROLS: SECURING THE INTERNET OF THINGS

TechTarget | SearchSecurity

Home

Network-based controls: Securing the Internet of things

DEVICES MAY NOT connect to enterprise access systems or inventory and patching mechanisms. This expert eGuide explains how you can take back control with these widely used network protocols.

Home

Network-based controls: Securing the Internet of things

NETWORK-BASED CONTROLS: SECURING THE INTERNET OF THINGS

Johannes B. Ullrich

Enterprise networks are becoming inundated with "smart" things and industrial sensors. But with no antimalware available, and little centralized configuration management, endpoint security is difficult -- if not impossible. Many devices, such as smart meters or the digital video recorders used in surveillance systems, don't connect to enterprise access controls or inventory and patching mechanisms. As a result, it's important to find methods for securing the Internet of things (IoT) and bring your own devices, using network-based controls that can scale and be centrally managed with existing tools.

Policies and technologies to enforce inventory controls are critical for data security and risk management. Most Internet-connected devices can only be managed efficiently via Dynamic Host Configuration Protocol, a network protocol used for automating IP parameters. DHCP can do a lot more than just hand out IP addresses and DNS settings. Its support for additional features is spotty, however. In some cases, firmware updates and configurations can be

Home

Network-based controls: Securing the Internet of things

sent to devices -- DHCP is critical to advertise the location of these files.

DHCP logs and lease files can also provide reasonably good inventories. Restricting DHCP to known devices, or using it to segregate new devices into subnets, is a commonly used technique to enforce inventory control policies. DHCP server configurations should always tie back to an IP address management and inventory control system. Figure 1 shows a small sample of DHCP logs that include the name of the device asking for an address.

DHCP LOGS

```
DHCPREQUEST for 192.0.2.1 from 00:24:e4:dd:ee:ff (WSD-5CA8) via re1
DHCPREQUEST for 192.0.2.2 from 24:a4:3c:aa:bb:cc (unifac) via re1_vlan2
DHCPREQUEST for 192.0.2.3 from 70:3e:ac:11:22:33 (iPhone) via re1
```

FIGURE 1: DEVICES IDENTIFYING THEMSELVES AS PART OF A DHCP REQUEST.

Home

Network-based controls: Securing the Internet of things

In addition to DHCP logging, devices need DNS for IP address management just like any other computer system using IP. While DNS was developed, in part, to save humans from having to remember IP addresses; for devices, DNS allows manufacturers to retain static host names for APIs that resolve to varying or multiple IP addresses. DNS requests can be used to assist in inventorying devices — the queries can indicate the type of device and how it is used, as shown in Figure 2.

DNS REQUESTS

```
query: netcom.netatmo.net IN A + (10.5.0.86)
query: api.parse.com IN A + (fd14:5d44:4428:1::35)
query: scalews.withings.net IN A + (10.5.0.86)
```

FIGURE 2: DNS QUERIES SENT BY A WEATHER STATION, AN IPHONE AND A SCALE.

FIREWALL CHALLENGES

Luckily, most devices do not have to accept unsolicited connections from outside the perimeter. But many systems still need to establish outbound

Home

Network-based controls: Securing the Internet of things

connections.

Restricting these connections is tricky, especially if a device wants to connect to cloud services or content delivery networks. It's hard, if not impossible, to establish sensible firewall rules in these cases. With HTTP connections, it may be possible to proxy the connections and inspect the data that's sent and received, in an attempt to eliminate data leaks and detect malicious code retrieved by the device.

Often overlooked as a sensor, the Network Time Protocol (NTP) is still used by many devices to synchronize computer clock times on packet-based networks. In some cases, devices use a pre-set NTP server, which may indicate which device is sending the NTP request. Some systems may attempt to connect to a NTP server assigned via DHCP.

Most security teams have access to these types of network-based controls. To develop better security processes for the Internet of things, all it takes is use of these existing tools to start looking for potential events associated with devices, and enforcement of inventory control policies.

Home

Network-based controls: Securing the Internet of things

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.