WatchGuard Network Discovery

Technical Brief
WatchGuard Technologies, Inc.
Published: May 2016

Introduction

This short technical brief outlines the need for WatchGuard's **Network Discovery** service, available on current WatchGuard Firebox® models running version 11.11 of the Fireware® operating system or higher. It explains how the services works and the important security benefits an organization gains.

You cannot secure a network that you do not understand

Best practices in Information Security (Info Sec) require that the IT engineers responsible for network security maintain a current map or diagram of their network topology. Info Sec professionals have long taught that the first step in any vulnerability management program is to discover and identify all of the assets in a network and to understand their role.

For example, PCI DSS Requirement 1.1.2 mandates that the following exists: *"Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks."*[1]

Often the IT infrastructure has been inherited from previous IT employees. It is rare when IT admins start out with a network that they have designed from day one. If they are lucky there may be a Visio diagram that shows the network topology, but often it is not well understood, especially in smaller companies. When Managed Service Providers (MSPs) first engage with a client, one of the first steps is to discover everything that has been put in place by the existing part-time IT staff. It is essential for the MSP responsible for maintaining and securing the network to discover all devices that are connected.

But the most important part of the asset discovery process requires monitoring for new endpoint asset connections, especially those a company doesn't know about. These suspicious connections represent several possible threats:

[1] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.1, April 2015. Full standard is available from PCI Security Standards Council, LLC at www.pcistandards.org.

1) **Unauthorized IT components installed by employees**

If an employee brings a personal laptop from home, it is highly likely that it does not have the same strong endpoint antivirus protection that is required at the corporate level. When that employee plugs it into an Ethernet port or connects wirelessly, it is a risk to the entire company.

Well-intentioned employees may have installed their own server applications or software, such as a web server, without approval from IT. While they may be able to get an initial install completed, they probably do not follow best practices in patching regularly to maintain protection against vulnerability exploits.

Another common example of employee carelessness: workers may install unauthorized wireless access points to provide more convenient network access in their area, but that represents a risk since outsiders may find it easier to attack the network from that weak point.

2) Attackers trying to hack their way onto the corporate network

A more sinister risk is unauthorized or "rogue" access points that hackers may attach to a network port or another network device like a switch or router.

Malicious software may be installed on internal devices. Botnets may have installed bot software that is calling home to the Command and Control center using unusual communication mechanisms.

Current Solutions

Today network admins use open source tools like nmap[2] to scan for all devices on their network. Small and midsize businesses have an especially tough time keeping track of every computing device in their environment. They cannot afford complex asset discovery and vulnerability management systems so they rely on the popular, open source utility nmap because it's flexible and efficient. Nmap uses raw IP packets to determine the hosts that are available on the network, the services (application name and version) those hosts are offering, and the operating systems (and OS versions) they are running. With Network Discovery service, WatchGuard goes beyond just basic nmap scanning to provide an interactive view of asset details that integrate with real-time log and threat information from the firewall.

Network Discovery with WatchGuard Firebox

With a WatchGuard Unified Threat Management (UTM) Firebox appliance, admins do not need to run separate tools to see everything that is connected to the network. The network admin defines a scan, which can either be launched instantly or scheduled for a quieter time. This scan uses nmap technology along with other techniques (detailed below). The results are shown in an interactive visual map in the Web user interface.

[2] For more details about nmap, refer to the open source project at https://nmap.org/

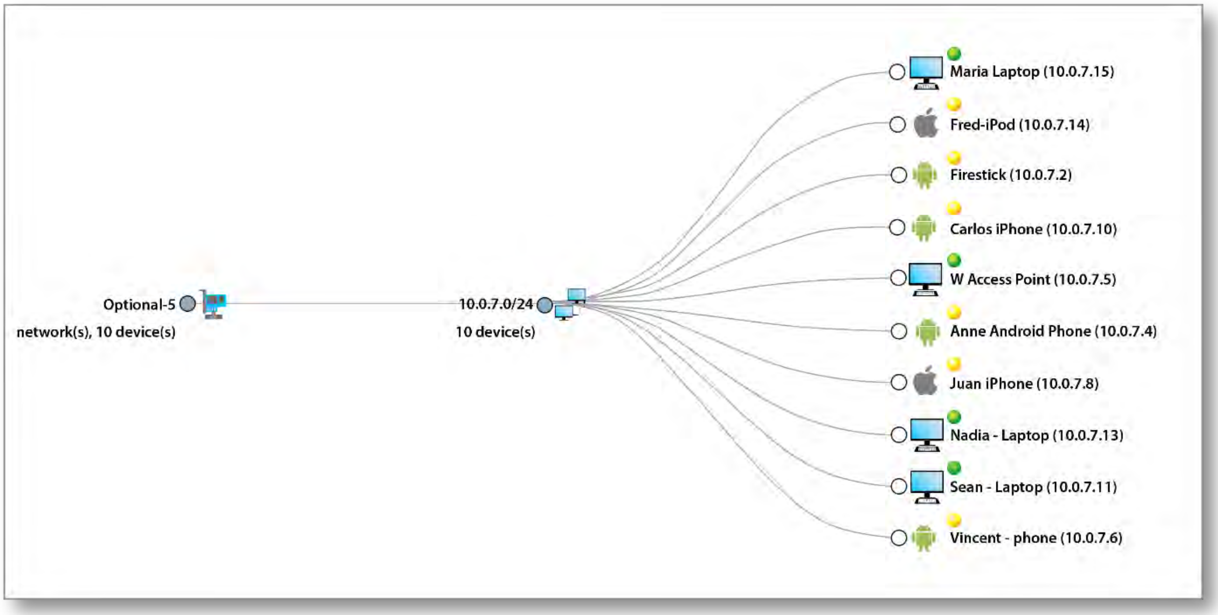
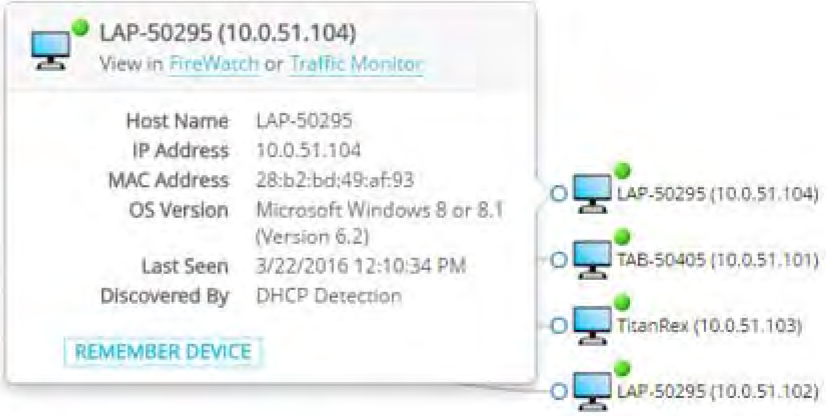

Optional-5
network(s), 10 device(s)
10.0.7.0/24
10 device(s)
Maria Laptop (10.0.7.15)
Fred-iPod (10.0.7.14)
Firestick (10.0.7.2)
Carlos iPhone (10.0.7.10)
W Access Point (10.0.7.5)
Anne Android Phone (10.0.7.4)
Juan iPhone (10.0.7.8)
Nadia - Laptop (10.0.7.13)
Sean - Laptop (10.0.7.11)
Vincent - phone (10.0.7.6)

Figure 1. *Network Discovery creates a map of every node on your network*

Network Discovery allows IT staff to map out the network behind their firewall. Assets in the network are identified and represented with an icon when appropriate, including:

- **IP Address**
- **MAC Address**
- **Type of device** – iOS, Android, MAC, Windows, etc.
- **Any ports that are open** – IT admins can see if web server ports are open on network clients, for example, which could indicate a potential network compromise

Admins can search and filter all device data to zero in on key areas of interest. They can mark devices as "known" and assign descriptive names. New, unfamiliar devices will immediately stand out when they show up without names.



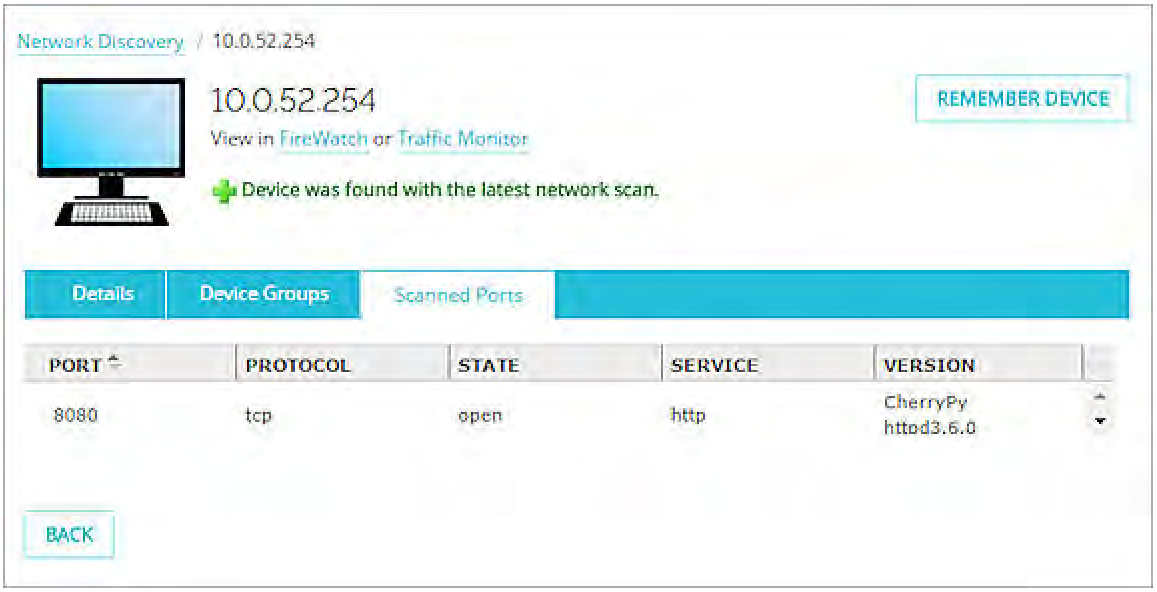
LAP-50295 (10.0.51.104)
View in FireWatch or Traffic Monitor

Host Name LAP-50295
IP Address 10.0.51.104
MAC Address 28:b2:bd:49:af:93
OS Version Microsoft Windows 8 or 8.1 (Version 6.2)
Last Seen 3/22/2016 12:10:34 PM
Discovered By DHCP Detection

Figure 2. *One-click integration with WatchGuard's FireWatch and Traffic Monitor tools*

The firewall admin can immediately and quickly investigate suspicious devices using direct integration with the visibility tools available on the firewall, including FireWatch and Traffic Monitor. One click through to FireWatch will provide a clear visual indication of the type of traffic that is passing through the IP address.

To see details about which ports the device used to connect to the network, select the **Scanned Port** tab. *The Scanned Port tab only appears when a device is discovered by an nmap network scan.*


Network Discovery / 10.0.52.254
10.0.52.254
View in FireWatch or Traffic Monitor
REMEMBER DEVICE
Details
Device Groups
Scanned Ports
BACK

Device was found with the latest network scan.

PORT	PROTOCOL	STATE	SERVICE	VERSION
8080	tcp	open	http	CherryPy httpd3.6.0

Figure 3. *Details revealed by Network Discovery scan*

The details that appears for each port include:

- **Port** – port number
- **Protocol** – protocol in use on the port – for example, TCP or UDP
- **State** – current state of the port
- **Service** – name of the service in use on the port
- **Version** – version of the service appears when available

Asset identification with Network Discovery

A number of techniques can be used to identify devices in a network. They are listed below in the order of precision. Network Discovery always defaults to the most precise option available when determining information about a device on the network.

- FireClient, the mobile security agent from WatchGuard that is installed on iOS and Android devices
- HTTP header information from the Firebox Web Portals for hotspot or user authentication
- The MS Exchange Event Monitor, which is used for Single Sign-on

- DHCP Fingerprinting[3] uses information that is passed in the exchange of packets when the client gets an IP address, even if the Firebox is used as a DHCP server or relay. DHCP option 55 for the parameter request list includes information that identifies the device OS.
- An active scan with nmap

Conclusion

Network admins today are challenged with the asset discovery and security audit of complex networks. They need to troubleshoot problems as they occur, and identify any new or suspicious activity. WatchGuard's Network Discovery service provides an efficient, flexible, and integrated service that saves time for IT staff and helps them to keep their networks and data safe and secure.

Network Discovery is available in the current generation of Firebox models, from the Firebox T Series to the M5600. Available as a stand-alone subscription service, the service is also automatically included – along with a host of other powerful security capabilities – in WatchGuard's UTM Security Suite.

For more information about Network Discovery and other best-in-class security capabilities from WatchGuard, visit www.watchguard.com.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard is headquartered in Seattle, Wash. with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. Part.No. WGCE66914_060216

[3] http://lets-start-to-learn.blogspot.com/2015/02/dhcp-fingerprinting.html