DHCP Parameter Request List Option 55 Used to Profile Endpoints Configuration Example

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Verify
Troubleshoot
Related Information

Introduction

This document describes the use of the DHCP Parameter Request List option 55 as an alternative method to profile devices that use the Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have:

- Basic knowledge of the DHCP discovery process
- Experience with the use of ISE to configure custom profiling rules

Components Used

The information in this document is based on these software and hardware versions:

- ISE Version 1.2
- Apple iOS
- Windows 8

The information in this document was created from the devices in a specific lab environment. All of
Background Information

In production ISE deployments, some of the more commonly deployed profiling probes include RADIUS, HTTP, and DHCP. With URL redirection in the center of the ISE workflow, the HTTP probe is widely used in order to capture important endpoint data from the User-Agent string. However, in some production use cases, URL redirection is not desired and Dot1x is preferred, which makes it more difficult to accurately profile an endpoint. For example, an employee PC that connects to a corporate Service Set Indentifier (SSID) gets full access while its personal iDevice (iPhone, iPad, iPod) gets Internet access only. In both scenarios, the users are profiled and dynamically mapped to a more specific identity group for authorization profile matching that does not rely on the user to open a web browser. Another commonly used alternative is hostname matching. This solution is imperfect because users might change the endpoint hostname to a non-standard value.

In corner cases such as these, the DHCP probe and DHCP Parameter Request List option 55 can be used as an alternative method to profile these devices. The Parameter Request List field in the DHCP packet can be used in order to fingerprint an endpoint operating system much like an Intrusion Prevention System (IPS) uses a signature in order to match a packet. When the endpoint operating system sends a DHCP discover or request packet on the wire, the manufacturer includes a numeric list of DHCP options that it intends to receive from the DHCP server (default router, Domain Name Server (DNS), TFTP server, etc.). The order by which the DHCP client requests these options from the server is fairly unique and can be used in order to fingerprint a particular source operating system. The use of the Parameter Request List option is not as exact as the HTTP User-Agent string, however, it is far more controlled than the use of hostnames and other statically-defined data.

**Note:** The DHCP Parameter Request List option is not a perfect solution because the data it produces is vendor-dependent and can be duplicated by multiple device types.

Before you configure the ISE profiling rules, use Wireshark captures from an endpoint/Switched Port Analyzer (SPAN) or Transmission Control Protocol (TCP) Dump captures on ISE in order to evaluate the Parameter Request List options in the DHCP packet (if present). This sample capture displays the DHCP Parameter Request List options for a Windows 8 Enterprise PC.

The Parameter Request List string that results is written in the following comma-separated format: 1,15,3,6,44,46,47,31,33,121,249,252,43. Use this format when configuring custom profiling conditions in ISE.

The configuration section demonstrates the use of custom profiling conditions to match iPhones, iPads, and iPods into a single identity group called **Apple-iDevice**. Unlike the Parameter Request List string that is unique to Windows 8, Apple uses a common set of strings across multiple endpoint types. Because of this, it is not possible to differentiate the Apple iDevice type with the use of the Parameter Request List option alone. This is an acceptable configuration in production ISE deployments because the same authorization policy is typically applied to iPhones, iPads, and iPods.
Configure

1. Log on to the ISE admin GUI and navigate to Policy > Policy Elements > Conditions > Profiling. Click Add in order to add a new custom profiling condition. In this example, four unique rules are defined for the most commonly used Apple iDevice Parameter Request List fingerprints. Refer to Fingerbank.org for a complete list of Parameter Request List values. **Note:** The Attribute Value text box might not display all of the numeric options, and you might need to scroll with the mouse or keyboard in order to view the full list.

2. With the custom conditions defined, navigate to Policy > Profiling > Profiling Policies in order to modify a current profiling policy or in order to configure a new one. In this example, the default Apple-iDevice policy is edited in order to include the new Parameter Request List conditions.

3. Add a new compound condition to the Apple-iDevice profiler policy rule and ensure that the OR operand is selected so that any of the configured Parameter Request List strings can result in a match. Modify the Certainty Factor as required in order to achieve the desired profiling result.

   **Note:** Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Verify

Use this section in order to confirm that your configuration works properly.

- Navigate to Administration > Identity Management > Identities > Endpoints and edit the Endpoint Profile for the device/MAC address.
- Confirm that theEndPointPolicy is Apple-iDevice, that the EndPointSource is DHCP Probe, and that the dhcp-parameter-request-list values match the condition values previously configured.

The Output Interpreter Tool (registered customers only) supports certain show commands. Use the Output Interpreter Tool in order to view an analysis of show command output.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

- Verify that the DHCP packets reached the ISE policy nodes that perform the profiling function (with helper-address or SPAN).
- Use the Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump tool in order to natively run TCP Dump captures from the ISE admin GUI.
- Refer to the Fingerbank.org DHCP fingerprint database for a current list of Parameter Request List options.
Ensure that the correct Parameter Request List values are configured in the ISE profiling conditions. Some of the more commonly used strings include:

The Output Interpreter Tool (registered customers only) supports certain `show` commands. Use the Output Interpreter Tool in order to view an analysis of `show` command output.

**Note:** Refer to [Important Information on Debug Commands](#) before you use `debug` commands.

### Related Information

- [Fingerbank.org DHCP Fingerprint Database](#)
- [Technical Support & Documentation - Cisco Systems](#)