Contents

Introduction

This document provides a simple description for the debugging functionality in Adaptive Security Appliances (ASAs) that run Version 8.4 and later. However, some of the features are available only in Version 9.5(2) and later.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- ASA 5506-X with ASA Software Version 9.5(2)
- Cisco Adaptive Security Device Manager (ASDM) Version 7.5.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Basic Logging Functionality

ASAs handle debug messages differently than Cisco IOS® devices. By default (unless "logging debug-trace", which is described later, is used), they are displayed on the screen either when you are connected through the console port or through telnet/

Independence means that when you enable debugs on the console port and you are connected through SSH, the debugs do not appear on SSH. You have to manually enable them again. Also, if debugs are enabled on one SSH session they will not appear at all on the other session. You can refer to it as **per session debugging.**

There is also no need to enter the **terminal monitor** command on an ASA in order to show debugs, because the debugs enabled on SSH or a telnet session appear regardless of this command. The purpose of this command is much different than in Cisco IOS devices and ASA Syslog Configuration Example describes that feature in depth.

Difference Between Syslog and Debug Messages

The debugs are specified messages for a certain protocol or feature of ASAs. There is no level of debugs, instead they are very detailed and the detail level can be changed. They also might not have a timestamp, message code, or severity level. This is dependent on the particular debug.

This example shows the difference between debugs and syslog messages in regards to the same ping request.

This is an example of debug output after you enter the **debug icmp trace** command:

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

This is an example of a **syslog** message in regards to the same ICMP request:

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

Collect Debugs

The default timeout for SSH or telnet is five minutes and the session is disconnected after this time of inactivity. The default timeout for console connection is 0, which means that user is logged in until the user logs out manually.

Unfortunately the logging feature is limited by the timeout set on a particular management method, so when the SSH session ends the debugs also stop.

In order to continue to collect the debugs for an extended time, you have to use the console connection and then you can redirect them to the syslog server with the **logging debug-trace** command. They will be redirected as syslog message 711001 issued at severity level 7. In order to stop sending this messages to logs, you can use insert "no" before the command.

```
logging debug-trace
no logging debug-trace
```

From Version 9.5.2, the ASA allows you to continue to send debugs as syslog messages after a timeout or log out on a SSH/telnet/console connection. If you enter the **debug-trace persistent** command you will be able to selectively clear debugs enabled in one session from a different session and they will stay active in the background. In order to disable this feature, insert "no" before the command.

```
logging debug-trace persistent
no logging debug-trace persistent
```

By default, all debug messages have a severity of level 7. In order to filter them from unwanted messages you can raise the severity of this message to 3 so you will collect only error messages beside the debugs. Insert "no" in order to disable this redirection.

```
logging message 711001 level 3
```

```
no logging message 711001 level 3
```

Sample Configuration

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

These commands enable you to send error messages and Internet Control Message Protocol (

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

Related Information

- **ASA Syslog Configuration Example**
- **Technical Support & Documentation - Cisco Systems**