ASA Integration for NSEL
(for Stealthwatch System v6.10.0)
Copyrights and Trademarks

© 2017 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
# Contents

<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Before You Begin</td>
<td>1</td>
</tr>
<tr>
<td>Process Overview</td>
<td>1</td>
</tr>
<tr>
<td>Define the NetFlow Export Options</td>
<td>2</td>
</tr>
<tr>
<td>Configure NetFlow Creation Criteria</td>
<td>6</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>10</td>
</tr>
</tbody>
</table>
Introduction

This document provides configuration options necessary to configure a Cisco Adaptive Security Appliance (ASA) to export NetFlow Security Event Logging (NSEL) to the Stealthwatch flow collection infrastructure using the Adaptive Security Device Manager (ASDM). Lancope tested the Stealthwatch System with an ASA running ASA OS v9.1(5) and ASDM v7.1(4).

Audience

This document is intended for personnel who need to configure a Cisco ASA to send data to Stealthwatch.

Before You Begin

Before you can complete the procedures in this document, you need the following information:

- IP address of the Stealthwatch Flow Collector that will receive data from the ASA
- Interface on the ASA that will be sending data to the Flow Collector
- UDP port number used to forward NetFlow

Process Overview

The configuration process includes completing the following procedures as detailed in this document:

Define the NetFlow export options.

Configure the NetFlow creation criteria.
Define the NetFlow Export Options

Complete the following steps to set the various options related to the export of NetFlow data from the ASA, including relevant timers and destinations.

1. Log in to the ASDM. The Home page opens.

2. Click Configuration to open the Configuration page.

3. Complete the following steps to access the Netflow page.
   a. At the bottom of the left navigation pane, click Device Management.
   b. In the tree in the left navigation pane, select Logging > NetFlow.

The NetFlow page opens.

© 2017 Cisco Systems, Inc. All Rights Reserved.
4. Do the following:

- In the Template Timeout Rate field, define the frequency that template updates will be sent from the ASA.

  **Note:** We recommend setting this value to 30 minutes or less. In the example below, a template update will occur every 10 minutes.

- In the Flow Update Interval field, define the frequency that status updates for long-lived flows will be sent from ASA.

  **Note:** We recommend setting this value to 1 minute.

- Select the “Delay transmission of flow creation events for short-lived flows” check box.

- In the Delay By field, type 60 to set the amount of time that records are held in cache to 60 seconds. This value matches the recommended Active Timeout value and causes the following to occur:
  - Reduces the number of flow events exported from the ASA.
  - Reduces the licensing implications without significantly changing data reporting.

If the “Delay transmission of flow creation events for short-lived flows” check box is selected, and the flow expires before 60 seconds after the flow creation event, then only one record will be sent (rather than one sent for flow creation and one sent for teardown).
Note: Please contact your Cisco ASA support team if specific concerns about performance implications exist in your environment.

5. Click **Add**. The Add NetFlow Collector dialog opens.

6. Complete the fields as specified below:
   - In the **Interface** field, click the drop-down arrow to define which interface on the ASA will send NetFlow data to the Flow Collector.
   - In the **IP Address or Hostname** field, type the IP address of the Flow Collector that will receive data from the ASA.
   - In the **UDP Port** field, type the port number that will be used to forward NetFlow.

7. Click **OK**. The Netflow page opens with the new Flow Collector information shown in the Collectors section.

8. For performance reasons, we recommend that you clear the “Disable redundant syslog messages” check box. However, you should review any specific performance concerns you have with your Cisco support team.
9. Go to “Configure NetFlow Creation Criteria” next in this guide.
Configure NetFlow Creation Criteria

Complete the following steps to define the criteria for creating NetFlow events that can be exported to the previously defined Flow Collector.

1. At the bottom of the left navigation pane, click Firewall.
2. In the tree in the left navigation pane, click Service Policy Rules to display that page.
4. We recommend that you select the "Global – applies to all interfaces" option to allow the collection of NetFlow statistics for all ASA interfaces and to make the most use of the ASA firewall's NetFlow logging capability.

**Note:** You can select specific interfaces to limit flow output and logging.

6. Do the following:
   - Select the "Create a new traffic class" option.
   - In the "Create a new traffic class" field, type NetFlow Monitor.
   - Select the Any traffic check box to monitor all traffic types traversing the selected interfaces.


8. Click the **NetFlow** tab.
9. Click **Add**. The Add Flow Event dialog opens.

10. Do the following:
   - In the Flow Event Type field, click the drop-down arrow and select **All**. This specifies that all types of NSEL records will be generated by the Cisco ASA.
   - In the Collectors section, select the check box that corresponds to the IP address of the Flow Collector configured earlier.

11. Click **OK**. The Service Policy Rules page opens showing the new service policy.
12. Click **Apply**.

**Contacting Support**

If you need technical support, or wish to make comments about this document, please do one of the following:

- [Open a case online.](#)
- Send an email to [tac@cisco.com](mailto:tac@cisco.com).
- Call:
  - 1-800-553-2447 (U.S.)
  - [Click here for worldwide support numbers](#)