Cisco Secure Network Analytics

ASA Integration for NSEL Export to Secure Network Analytics 7.4

Table of Contents

Overview

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

> In v7.4.0 we rebranded our Cisco Stealthwatch Enterprise products to Cisco Secure Network Analytics. For a complete list, refer to the Release Notes. In this guide, you will see our former product name, Stealthwatch, used whenever necessary to maintain clarity, as well as terminology such as Stealthwatch Management Console and SMC.

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:

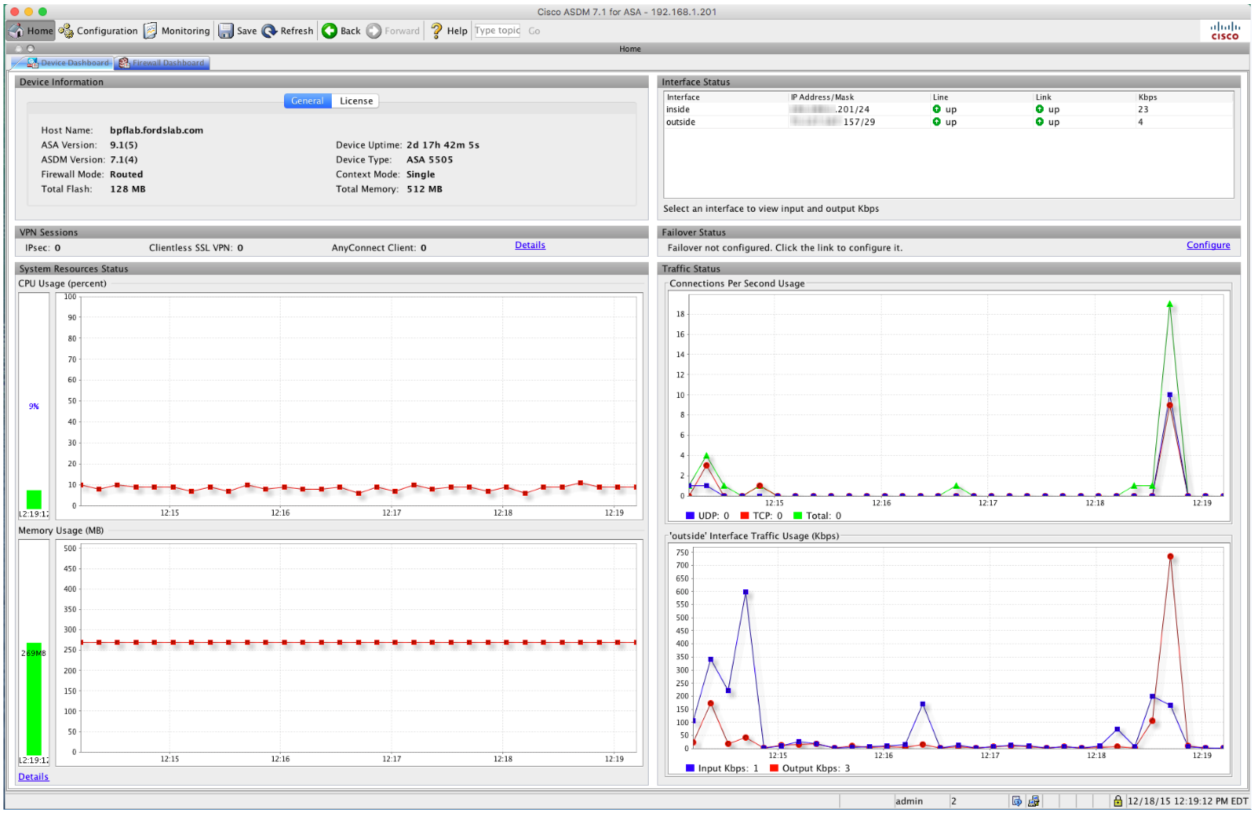
Define the NetFlow export options.

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.



Host Name: bpflab.fordslab.com
ASA Version: 9.1(5)
ASDM Version: 7.1(4)
Firewall Mode: Routed
Total Flash: 128 MB

Device Uptime: 2d 17h 42m 5s
Device Type: ASA 5505
Context Mode: Single
Total Memory: 512 MB

Interface	IP Address/Mask	Line	Link	Kbps
inside	[redacted].201/24	up	up	23
outside	[redacted]157/29	up	up	4

Select an interface to view input and output Kbps

IPsec: 0 Clientless SSL VPN: 0 AnyConnect Client: 0 Details

Failover not configured. Click the link to configure it. Configure

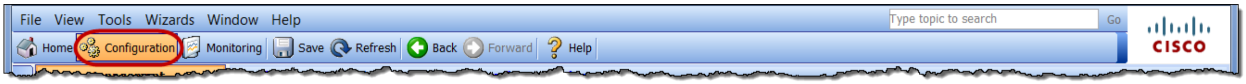
🟦 UDP: 0 🟥 TCP: 0 🟩 Total: 0

🟦 Input Kbps: 1 🟥 Output Kbps: 3

Details

admin 2 12/18/15 12:19:12 PM EDT

2. Click **Configuration** to open the Configuration page.

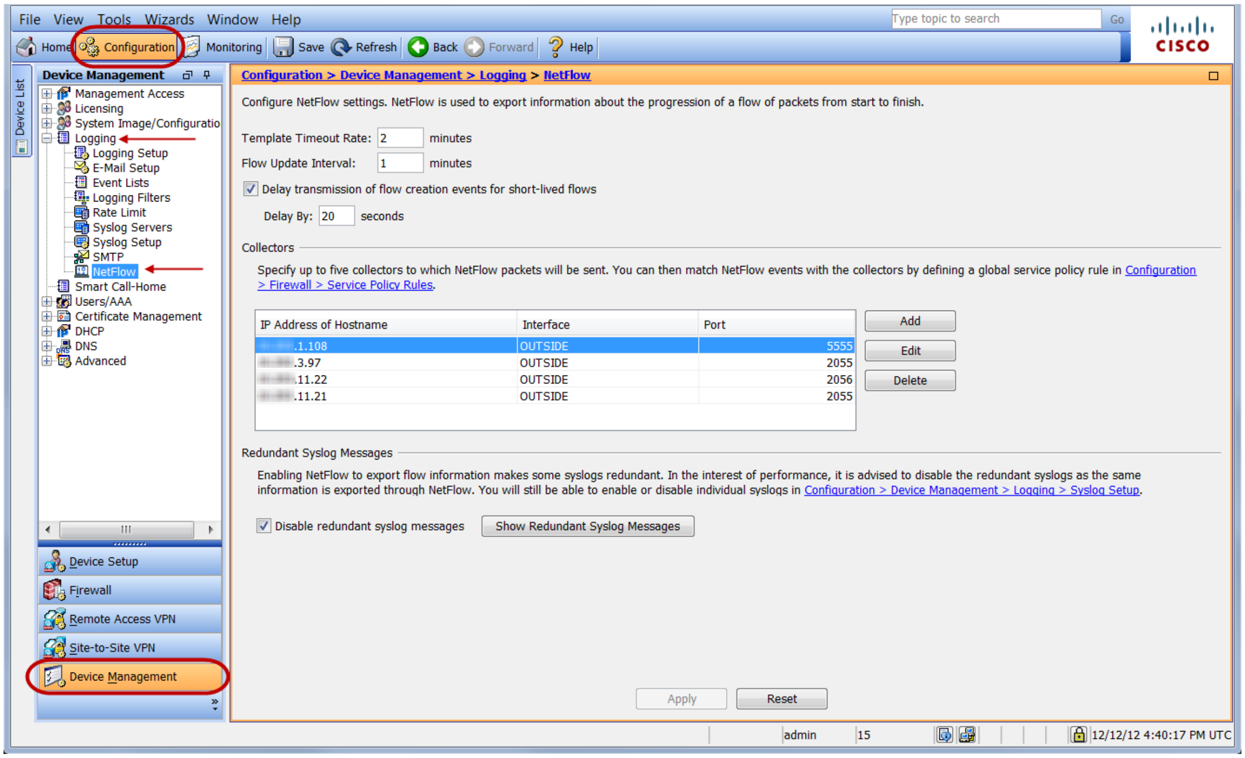


3. Complete the following steps to access the Netflow page.

    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.



Configuration > Device Management > Logging > NetFlow

Configure NetFlow settings. NetFlow is used to export information about the progression of a flow of packets from start to finish.

Template Timeout Rate: 2 minutes

Flow Update Interval: 1 minutes

☑ Delay transmission of flow creation events for short-lived flows

Delay By: 20 seconds

Collectors

Specify up to five collectors to which NetFlow packets will be sent. You can then match NetFlow events with the collectors by defining a global service policy rule in Configuration > Firewall > Service Policy Rules.

IP Address of Hostname	Interface	Port
[redacted].1.108	OUTSIDE	5555
[redacted].3.97	OUTSIDE	2055
[redacted].11.22	OUTSIDE	2056
[redacted].11.21	OUTSIDE	2055

Redundant Syslog Messages

Enabling NetFlow to export flow information makes some syslogs redundant. In the interest of performance, it is advised to disable the redundant syslogs as the same information is exported through NetFlow. You will still be able to enable or disable individual syslogs in Configuration > Device Management > Logging > Syslog Setup.

☑ Disable redundant syslog messages

4. Do the following:

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

      - We recommend setting this value to 5 minutes or less. In the example below, a template update will occur every 10 minutes.

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

      - We recommend setting this value to 1 minute.

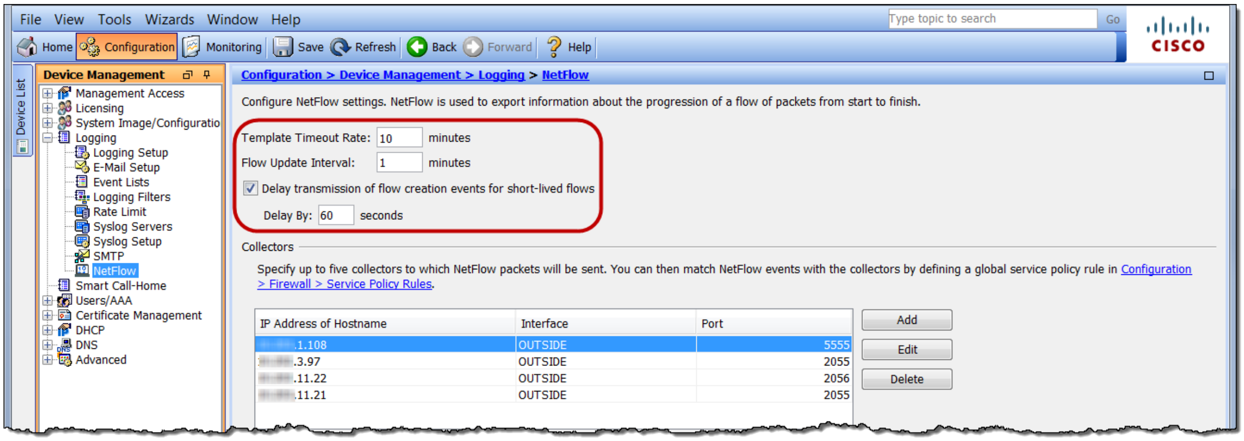
   c. Select the “Delay transmission of flow creation events for short-lived flows” check box.

   d. 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).

> Please contact your Cisco ASA support team if specific concerns about performance implications exist in your environment.



Configuration > Device Management > Logging > NetFlow

Configure NetFlow settings. NetFlow is used to export information about the progression of a flow of packets from start to finish.

Template Timeout Rate: 10 minutes

Flow Update Interval: 1 minutes

☑ Delay transmission of flow creation events for short-lived flows

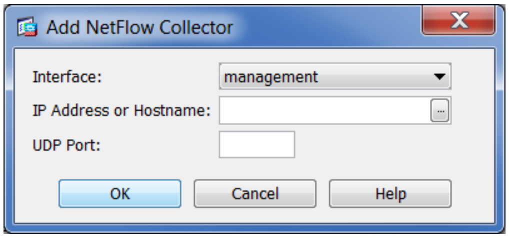
Delay By: 60 seconds

Collectors

Specify up to five collectors to which NetFlow packets will be sent. You can then match NetFlow events with the collectors by defining a global service policy rule in Configuration > Firewall > Service Policy Rules.

IP Address of Hostname	Interface	Port
[redacted].1.108	OUTSIDE	5555
[redacted].3.97	OUTSIDE	2055
[redacted].11.22	OUTSIDE	2056
[redacted].11.21	OUTSIDE	2055

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

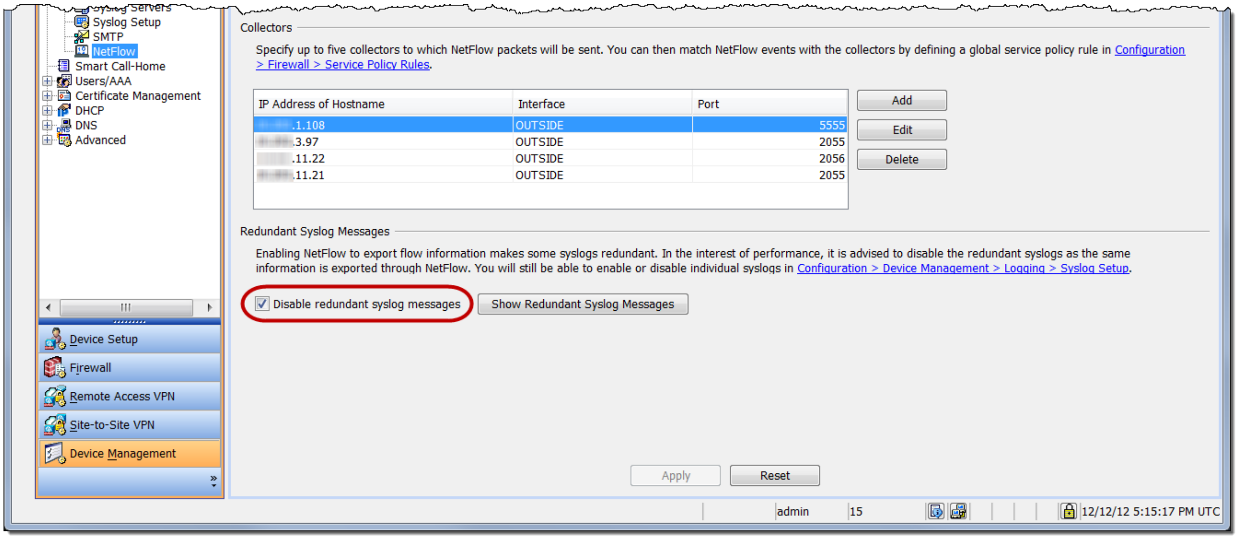


Interface: management

IP Address or Hostname:

UDP Port:

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.



Collectors

Specify up to five collectors to which NetFlow packets will be sent. You can then match NetFlow events with the collectors by defining a global service policy rule in Configuration > Firewall > Service Policy Rules.

IP Address of Hostname	Interface	Port
[redacted].1.108	OUTSIDE	5555
[redacted].3.97	OUTSIDE	2055
[redacted].11.22	OUTSIDE	2056
[redacted].11.21	OUTSIDE	2055

Redundant Syslog Messages

Enabling NetFlow to export flow information makes some syslogs redundant. In the interest of performance, it is advised to disable the redundant syslogs as the same information is exported through NetFlow. You will still be able to enable or disable individual syslogs in Configuration > Device Management > Logging > Syslog Setup.

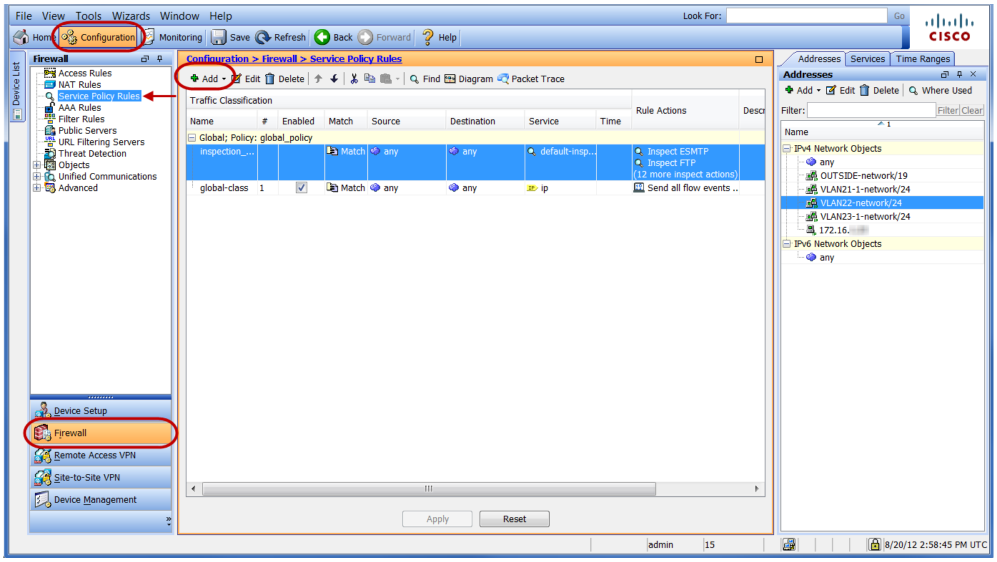
☑ Disable redundant syslog messages

9. Go to “Configure NetFlow Creation Criteria” next in this guide.

Configure NetFlow Creation Criteria

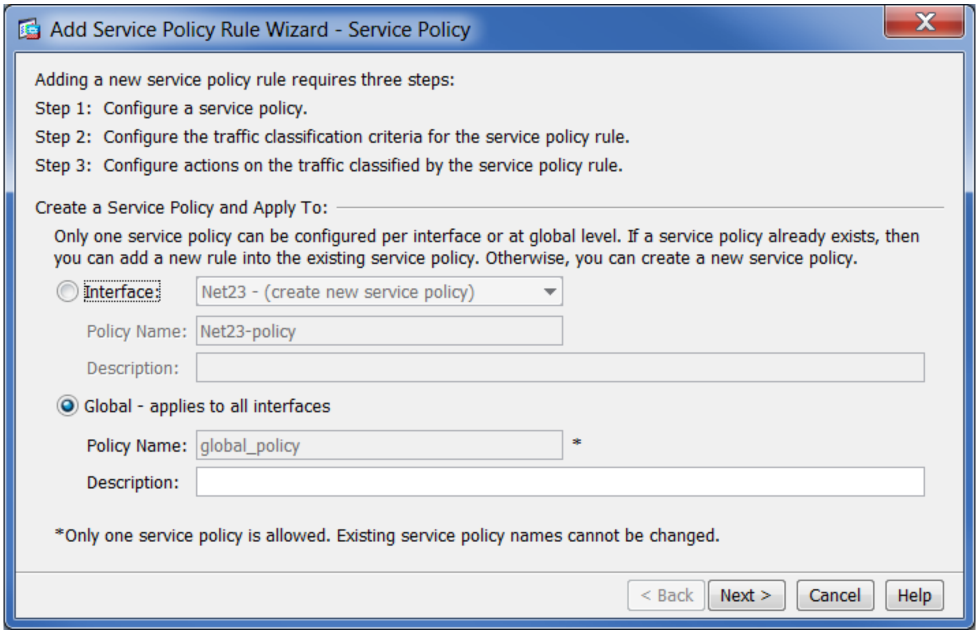
Complete the following steps to define the criteria for creating NetFlow events that can be exported to the previously defined Flow Collector.

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.



Traffic Classification								Rule Actions	Descr
Name	#	Enabled	Match	Source	Destination	Service	Time		
Global; Policy: global_policy									
inspection_...			Match	any	any	default-insp...		Inspect ESMTP Inspect FTP (12 more inspect actions)	
global-class	1	☑	Match	any	any	ip		Send all flow events ..	

3. In the tool bar, click **Add**. The Add Service Policy Rule Wizard: Service Policy page opens.



Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

○ Interface: Net23 - (create new service policy)

Policy Name: Net23-policy

Description:

● Global - applies to all interfaces

Policy Name: global_policy *

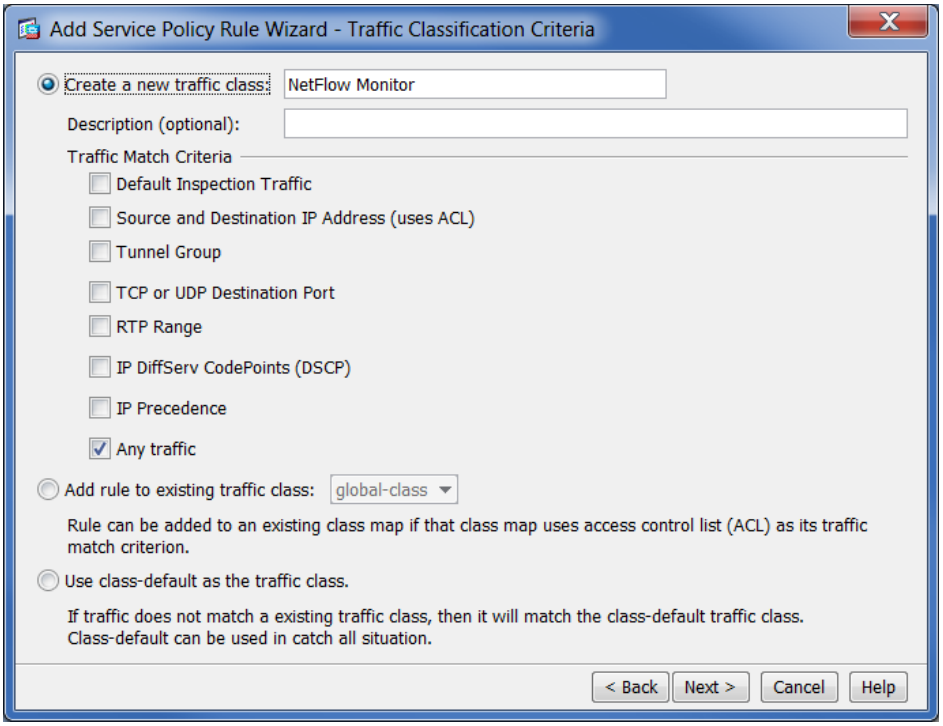
Description:

*Only one service policy is allowed. Existing service policy names cannot be changed.

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.

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

5. Click **Next.** The Add Service Policy Rule Wizard: Traffic Classification Criteria page opens.



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: NetFlow Monitor

Description (optional):

Traffic Match Criteria

- □ Default Inspection Traffic
- □ Source and Destination IP Address (uses ACL)
- □ Tunnel Group
- □ TCP or UDP Destination Port
- □ RTP Range
- □ IP DiffServ CodePoints (DSCP)
- □ IP Precedence
- ☑ Any traffic

○ Add rule to existing traffic class: global-class

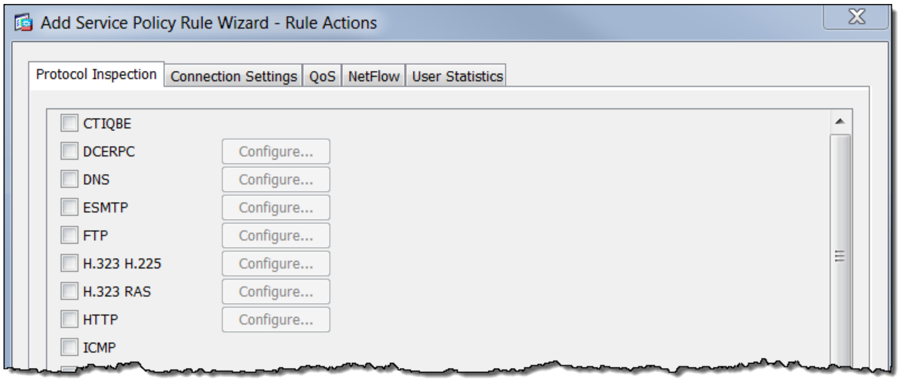
Rule can be added to an existing class map if that class map uses access control list (ACL) as its traffic match criterion.

○ Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

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.

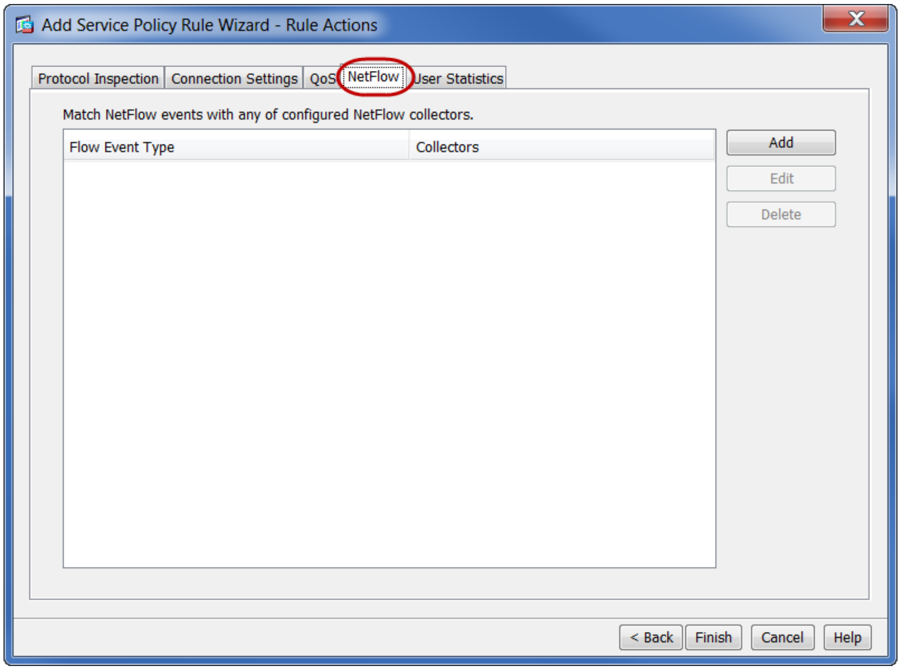
7. Click **Next.** The Add Service Policy Rule Wizard: Rule Actions page opens.



Add Service Policy Rule Wizard - Rule Actions

- □ CTIQBE
- □ DCERPC
- □ DNS
- □ ESMTP
- □ FTP
- □ H.323 H.225
- □ H.323 RAS
- □ HTTP
- □ ICMP

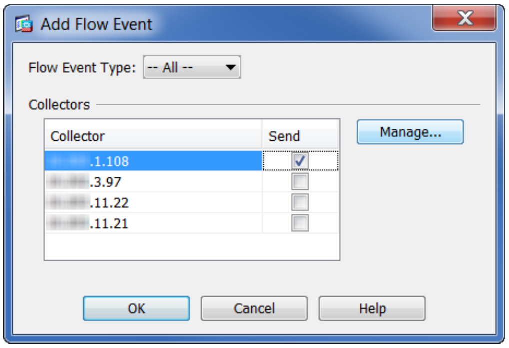
8. Click the **NetFlow** tab.



Match NetFlow events with any of configured NetFlow collectors.

Flow Event Type	Collectors

9. Click **Add**. The Add Flow Event dialog opens.

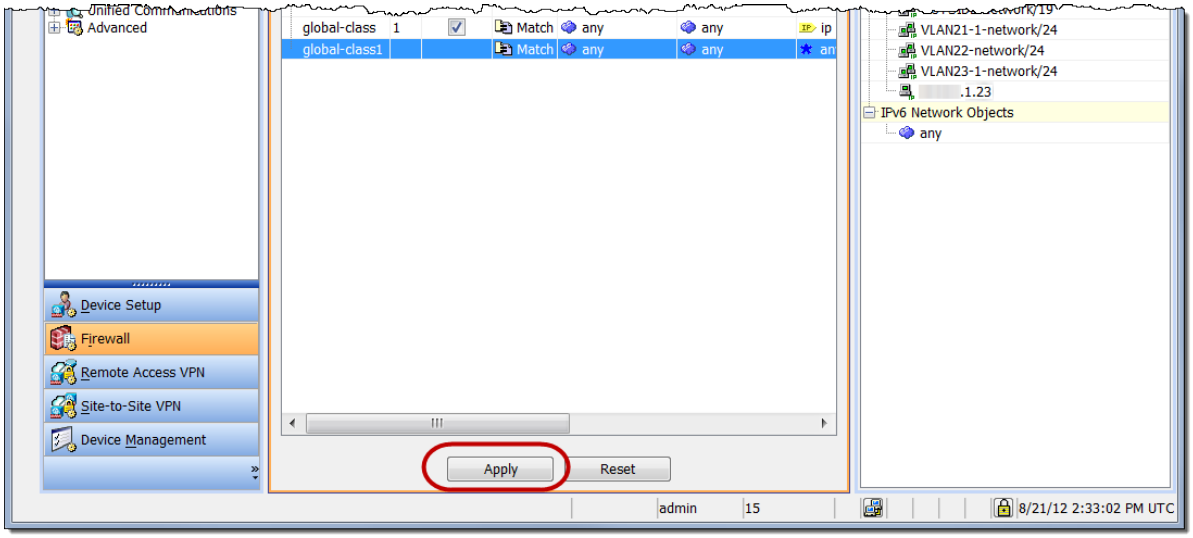


Flow Event Type: -- All --

Collector	Send
[redacted].1.108	☑
[redacted].3.97	□
[redacted].11.22	□
[redacted].11.21	□

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.



global-class	1	☑	Match	any	any	ip
global-class1			Match	any	any	an

12. Click **Apply**.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information