# Cisco Secure Network Analytics

ASA Integration for NSEL Export to Secure Network Analytics 7.4



## Table of Contents

Overview	3
Audience	3
Before You Begin	3
Process Overview	3
Define the NetFlow Export Options	4
Configure NetFlow Creation Criteria	9
Contacting Support 1	4

### 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 <u>Release Notes</u>. 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.



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

File View Tools Wi	zards Window Help	Type topic to search Go	مانتيان
Home 🚱 Configurati	an 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward  Pelp		CISCO

- 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.

File View Tools Wizards Wi	ndow Help			Type topic to search	Go ululu
Home Configuration Mo	nitoring 🔚 Save 🔇 Refresh 🔇 Back	🚫 Forward 🧳 Help			CISCO
t Device Management 🗗 🖗	Configuration > Device Management	<u>&gt; Logging</u> > <u>NetFlow</u>			
H Management Access	Configure NetFlow settings. NetFlow is us	ed to export information about the progres	sion of a flow of packets from s	tart to finish.	
Configuratio Configuratio Configuratio Configuratio Configuratio Configuratio Configuratio	Template Timeout Rate: 2 minute	25			
E-Mail Setup	Flow Update Interval: 1 minute	25			
Logging Filters	Delay transmission of flow creation evolution	ents for short-lived flows			
Rate Limit Syslog Servers	Delay By: 20 seconds				
Syslog Setup	Collectors				
Smart Call-Home	Specify up to five collectors to which N <u>&gt; Firewall &gt; Service Policy Rules</u> .	etFlow packets will be sent. You can then r	natch NetFlow events with the c	ollectors by defining a global serv	ice policy rule in <u>Configuration</u>
Certificate Management	IP Address of Hostname	Interface	Port	Add	
DNS	.1.108	OUTSIDE	5555	Edit	
🕀 🐯 Advanced	.3.97	OUTSIDE	2055		
	.11.22	OUTSIDE	2056	Delete	
	.11.21	0013102	2033		
	Redundant Syslog Messages				
	Enabling NetFlow to export flow inform information is exported through NetFlo	ation makes some syslogs redundant. In th w. You will still be able to enable or disable	ne interest of performance, it is e individual syslogs in <u>Configural</u>	advised to disable the redundant : tion > Device Management > Logo	syslogs as the same <u>jing &gt; Syslog Setup</u> .
< III >	Disable redundant syslog messages	Show Redundant Syslog Messages			
Device Setup					
Firewall					
Remote Access VPN					
Site-to-Site VPN					
Device Management		Ann	Reset		
*		7,455	,		
			admin	15 😡 🛃	12/12/12 4:40:17 PM UTC

- 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.

File View Too	ls Wizards Wir	ndow Help			Type topic to search	© ululu
Home 🖧 Cor	nfiguration 🔯 Mor	itoring 🔚 Save 🔇 Refresh 🔇 Bacl	k 🜔 Forward 🧳 Help			CISCO
Device Manag	gement 🗗 🗜	Configuration > Device Managemen	it > Logging > <u>NetFlow</u>			
🚆 🕀 🌈 Managen	nent Access	Configure NetFlow settings. NetFlow is u	used to export information about th	e progression of a flow of packets from	start to finish.	
System I	mage/Configuratio	Template Timeout Rate: 10 minu	ites			
E-Mai	il Setup	Flow Update Interval: 1 minu	ites			
Event	Lists	Delay transmission of flow creation	events for short-lived flows			
Rate	Limit	Delay By: 60 seconds				
Syslo	g Servers					
SMTP	y Setup	Collectors				
	ow all-Homo	Specify up to five collectors to which > Firewall > Service Policy Rules.	NetFlow packets will be sent. You	can then match NetFlow events with the	collectors by defining a global serv	vice policy rule in <u>Configuration</u>
🕀 🎆 Users/AA	VA III III III III III III III III III I					
E Certificat	e Management	IP Address of Hostname	Interface	Port	Add	
🕀 🚜 DNS		.1.108	OUTSIDE	5555	Edit	
🗄 🐯 Advance	d	.3.97	OUTSIDE	2055		
		.11.22	OUTSIDE	2056	Delete	
		.11.21	OUTSIDE	2055		
					-	

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

🖆 Add NetFlow Collector					
Interface:	management 🔹				
IP Address or Hostname:	· · · · ·				
UDP Port:					
ОК	Cancel Help				

- 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.

NetFlow	Specify up to five collectors to which	NetFlow packets will be sent. You	can then match NetFlow eve	ents with the coll	ectors by defin	ing a global service (	policy rule in <u>Configuratior</u>
Smart Call-Home	> Firewall > Service Policy Rules.						
Certificate Management	IP Address of Hostname	Interface	Port		Add		
DNS	.1.108	OUTSIDE		5555	r die	- -	
Advanced	.3.97	OUTSIDE		2055	Edit		
	.11.22	OUTSIDE		2056	Delete		
	.11.21	OUTSIDE		2055		5	
	L						
	Redundant Suclea Massages						
	Redundant Syslog Messages						
	Redundant Syslog Messages Enabling NetFlow to export flow infor	rmation makes some syslogs redu	dant. In the interest of perfo	ormance, it is ad	vised to disable	e the redundant syste	ogs as the same
	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redur Tow. You will still be able to enable	idant. In the interest of perfo	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant system the redundant system agement > Logging	ogs as the same > Syslog Setup.
	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redur Tow. You will still be able to enable	idant. In the interest of perfo or disable individual syslog:	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant system the redundant system	ogs as the same > <u>Syslog Setup</u> .
	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redur low. You will still be able to enable esShow Redundant Syslog N	idant. In the interest of perfo or disable individual syslog:	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant syslo agement > Logging	ogs as the same <u>&gt; Syslog Setup</u> .
	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redur low. You will still be able to enable Show Redundant Syslog N	idant. In the interest of perfo or disable individual syslog: lessages	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant syste agement > Logging	ogs as the same <u>&gt; Syslog Setup</u> .
Device Setun	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redur low. You will still be able to enable some Show Redundant Syslog N	dant. In the interest of perfo or disable individual syslog: lessages	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant sysle nagement > Logging	ogs as the same > Syslog Setup.
∭ ▶ Device Setup	Redundant Syslog Messages Enabling NetFlow to export flow information is exported through NetF	rmation makes some syslogs redu Flow. You will still be able to enable Show Redundant Syslog M	idant. In the interest of perfe or disable individual syslog: lessages	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant sysk nagement > Logging	ogs as the same ≥ Syslog Setup.
U Device Setup	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redur low. You will still be able to enable Show Redundant Syslog N	idant. In the interest of perfo or disable individual syslog: lessages	ormance, it is ad s in <u>Configuratio</u>	vised to disable <u>n &gt; Device Mar</u>	e the redundant sysl nagement > Logging	ogs as the same <u>&gt; Syslog Setup</u> .
III ► Device Setup G Firewall	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	mation makes some syslogs redu ilow. You will still be able to enable	dant. In the interest of perfo or disable individual syslog: iessages	ormance, it is ad s in <u>Configuratio</u>	vised to disable n > Device Mar	e the redundant sysk aagement > Logging	ogs as the same > Syslog Setup.
Device Setup Firewall	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redu Flow. You will still be able to enable Show Redundant Syslog N	idant. In the interest of perfo or disable individual syslog: lessages	prmance, it is ad	vised to disable	e the redundant sysk aagement > Logging	ogs as the same <u>&gt; Syslog Setup</u> .
Device Setup	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redu iow. You will still be able to enable Show Redundant Syslog N	idant. In the interest of perfo or disable individual syslog: lessages	ormance, it is ad	vised to disable	e the redundant sysk	ogs as the same <u>&gt; Syslog Setup</u> .
Device Setup Firewall Cereice Setup Engrewall Cereice Setup	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redu ilow. You will still be able to enable	idant. In the interest of perfo or disable individual syslog: lessages	ormance, it is ad	vised to disable	e the redundant sysic agement > Logging	ogs as the same > <u>Syslog Setup</u> .
Evice Setup Erewall Eemote Access VPN Site-to-Site VPN Device VPN	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redu iow. You will still be able to enable Show Redundant Syslog N	idant. In the interest of perfe or disable individual syslog: tessages	ormance, it is ad	vised to disable	e the redundant sysk lagement > Logding	ogs as the same ≥ Syslog Setup.
III   Device Setup   Firewall   Emote Access VPN   Site-to-Site VPN   Device Management	Redundant Syslog Messages Enabling NetFlow to export flow infor information is exported through NetF	rmation makes some syslogs redu ilow. You will still be able to enable	dant. In the interest of perfo or disable individual syslog: iessages	ormance, it is ad	vised to disable	e the redundant sysle agement > Logging	ogs as the same <u>&gt; Sysloq Setup</u> .

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.

File View Tools Wizards Win	dow Help							Look For:		G01111	du -
Hom Configuration Moni	itoring 🔚 Save 🌘	Refresh 🕻	🕽 Back 🤇	)Forward 🦓	Help					CISC	0
Firewall 🗗 म	Configuration >	Firewall > Se	rvice Poli	<u>y Rules</u>						Addresses Services Time Ranges	
Access Rules	🗣 Add 📲 🖬 Edit	📋 Delete 🛛 🤊	4 8	🛍 🏥 - 🛛 🔍 Fin	d 🖽 Diagram 🕰 F	Packet Trace				Addresses d	φ×
Service Policy Rules	Traffic Classificat	ion								Add - 🖉 Edit 🔟 Delete   Q, Where U	Jsed
Filter Rules	Name	# Enabled	Match	Source	Destination	Service	Time	Rule Actions	Descr	Filter: Filte	r Clear
Public Servers	Global: Policy:	alobal policy	materi	000.00	0 COUNTOURN	0011100				Name	
Threat Detection	inspection	5	Match	🇆 any	🇆 any	🔍 default-insp		Q Inspect ESMTP		IPv4 Network Objects	
Objects Unified Communications								Inspect FTP (12 more inspect actions)		- In any - In a second	
Advanced	global-class	1 🗸	🕒 Match	🧼 any	any	æ> ip		Send all flow events		VLAN21-1-network/24	
										VLAN22-network/24	
										VLAN23-1-network/24	_
										IPv6 Network Objects	
										Law any	
0											
Device Setup											
Firewall											
Remote Access VPN											
Cite to Cite 1/04											
	•								Þ		
Device Management											
ş				Ap	oply Re	set					
								admin 15		8/20/12 2:58:45	РМ ИТС

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

付 Add Service Poli	cy 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 Poli	cy and Apply To:					
Only one service p you can add a nev	olicy can be configured per interface or at global level. If a service policy already exists, then v 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:						
Olobal - applie	s to all interfaces					
Policy Name:	global_policy *					
Description:						
*Only one service	policy is allowed. Existing service policy names cannot be changed.					
	< Back Next > Cancel Help					

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
O 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.
< Back Next > Cancel Help

- 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 A	ctions	
Protocol Inspection Connec	tion Settings Qos	NetFlow User Statistics	
CTIQBE			
DCERPC	Configure		
DNS	Configure		
ESMTP	Configure		
FTP	Configure		
H.323 H.225	Configure		Ξ
H.323 RAS	Configure		
HTTP	Configure		
ICMP			

8. Click the **NetFlow** tab.

🔂 Ad	d Service Policy Rule Wizard - Rule Actions			X		
Prot	Protocol Inspection Connection Settings Qos NetFlow User Statistics					
	Match NetFlow events with any of configured NetFlow	/ collectors.				
	Flow Event Type	Collectors	Add			
			Edit			
			Delete	e		
			< Back Finish Cance	el Help		

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

<b>1</b>	Add Flow Event		X
Flo	ow Event Type: 🕘 All 🔻		
Co	llectors		
	Collector	Send	Manage
	.1.108	<b>V</b>	
	.3.97		
	.11.22		
	.11.21		
	OK Ca	ncel	Help

- 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.

m~	mannen		_^^^~	Martin and Constant Charles and Charles an
🗄 🐻 Advanced	global-class 1	🕒 Match 🧇 any	🧼 any 💷 ip	VLAN21-1-network/24
	global-class1	🕒 Match 🧇 any	🏟 any 🔹 🛪 an	Representation of the second s
				VLAN23-1-network/24
				.1.23
				IPv6 Network Objects
				any 🌑 🥎 any
A Device Setup				
Firewall				
Remote Access VPN				
Site-to-Site VPN				
Device Management	•		4	
×		Apply Reset		
		ad	min 15	8/21/12 2:33:02 PM UTC

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**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <u>https://www.cisco.com/go/trademarks</u>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)