# Configuración de la sincronización de dispositivos al Administrador de seguridad

## Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Metodología de demostración
Detección de un solo dispositivo
Pasos para realizar la detección de un solo dispositivo:
Pasos para realizar la detección de un solo dispositivo:
Paso 1:
Paso 2:
Descubrimiento masivo de dispositivos
Pasos para realizar la detección masiva de dispositivos:
Paso 1:
Paso 2:
Paso 3:

## Introducción

Este documento describe diferentes maneras de sincronización de la configuración de ASA a CSM.

## Prerequisites

#### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Security Manager
- Dispositivo de seguridad adaptable

#### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Security Manager 4.25
- Dispositivo de seguridad adaptable

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

#### Antecedentes

El administrador de seguridad de Cisco ofrece servicios de supervisión y gestión centralizados para los dispositivos Cisco ASA.

## Metodología de demostración

Este documento describe dos métodos u opciones diferentes para sincronizar la configuración de ASA a CSM.

- Detección de un solo dispositivo
- · Redescubrimiento masivo de dispositivos

## Detección de un solo dispositivo

La detección única solo se puede realizar si el dispositivo se agrega al inventario. Solo se puede realizar cuando el dispositivo tiene

- Configuraciones de contexto de seguridad para dispositivos ASA, PIX y FWSM que se ejecutan en modo de contexto múltiple.
- Configuraciones de sensores virtuales para dispositivos IPS.
- Información del módulo de servicio para dispositivos Catalyst.

## Pasos para realizar la detección de un solo dispositivo:

Puede realizar la detección de dispositivos cuando haya realizado cualquier cambio en la CLI del dispositivo o si el dispositivo se quitó y se volvió a agregar.

Para comprobar si los cambios pendientes aún no se han sincronizado , observe el ejemplo mencionado.

Haga clic con el botón derecho del ratón en el dispositivo correspondiente del panel del

dispositivo y seleccione la opción Detectar cambios fuera de banda.



Si no hay cambios, la página se muestra como no se han encontrado cambios salientes para este dispositivo.

🆏 008 Ownges		-	D	×
[08 Detail 008 Summary				
Devices Groups	CORDenals [Instantionerry]			
Alter - V	No Out of Band-changes found for this device			
- Copartnet				
- Cheal				
Lucite				
E Shice (				

Si se han realizado cambios, las líneas se resaltan según la leyenda.

State Coll Changes			-		30
ODE Desire ODE Summary					
Dentura Groups	Contests Transfer Langer				
File I - Hare - V	Latest Config Tensor In CDH	Ranning Carify Tensor Nan Device			T
C C C C C C C C C C C C C C C C C C C	P econer-list lot extended permit -1 may may * 20 30 to inpping hide unername 37 36	econes-list int entended people - main reging static to bogging hide unertaine linguing consider informational	Added	d ne hani	w ds
C C C C C C C C C C C C C C C C C C C	Jogging Nuffword informational     Jogging nome informational     res inside 1500     do not opticate 1500     do not opticate 1500     sta mann 1500	logging boffword informational logging mem informational men inside 1990 ein outside 1990 ein musi 1900 ein musi 1900 ein musi 1900			

## Pasos para realizar la detección de un solo dispositivo:

Paso 1:

Haga clic con el botón derecho del ratón en el nombre del dispositivo correspondiente del panel del dispositivo y elija la opción Detectar directivas en los dispositivos.



Paso 2:

Para el método de recuperación de un solo dispositivo, sólo puede ver el cuadro de diálogo Crear tarea de detección. En caso de que esté recibiendo un cuadro de diálogo de detección masiva , cierre y vuelva a abrirlo.

Dispone de 3 opciones para realizar la detección.

- Dispositivo en vivo: Obtiene la configuración del dispositivo en vivo , que está en la red.
- Archivo de configuración: Puede elegir el archivo de configuración y continuar con la detección.
- Configuración predeterminada de fábrica: restablece el dispositivo a las configuraciones predeterminadas. Este método se puede utilizar para dispositivos que sólo ejecutan el modo de contexto único o para dispositivos con contextos de seguridad individuales.

C	reate Discovery Task		×
	Discovery Task Name:	discovery:2024-Jul-19 09:09:36	
		Live Device	
	Discover From:	○ Config File	
		Factory Default Configuration	
		Config File: Browse	
		Discover Policies for Security Contexts	
	Policies To Discover Select the policies to d	crower	
	Detect ASA-CX/Fire	POWER Module	
	Inventory		
	Platform Settings		
	Firewall Services		
	NAT Policies		
	Routing Policies		
	SSL Policy		
	RA VPN Policies		
	IPS		
		OK Cancel Help	

Asegúrese de conocer la topología de red y los cambios que pueden producirse en ella antes de continuar con la detección.

Warning	, ×
	Discovery will replace existing policies with those discovered. Loss of sharing, inheritance will happen with all policies associated with the device Do you wish to continue?
	Do not show this again
	Yes No

Una vez completada la detección, puede ver la pantalla emergente con el estado de Detección completada.

	100%		
Status: Devices to be discovered: Devices discovered auccessfully: Devices discovered with errors:	Discovery compi 1 1 0	ieled with warni	ngs
iscovery Details			
Type Name	Sevenity	State	Discovered From
🐉 ASA 1	•	Discovery Co	inpleted with Warnings Live Device
		Severity	Description
Messages 12 not discovered		Severity	Cescription Policy discovery does not support the following CLI in your configuration:
Messages 11 not discovered blotes discovered		Severity	Description Policy description Pulicy description the following CLI in your configuration:
Messages 11 not docuvered slides discovered sisting policy objects reused		Severity	Cescription Pulcy decovery does not support the following CLI in your configuration: Une 6/mo ascin history enable Une 60/mo
Messages If not discovered blotes discovered xisting policy objects reused blotes discovered		Severity	Description Policy discovery does not support the following CLI in your configuration: Line fono mac address auto Line 60:no accimitization enable Line 62:no arp penelt-renconnected Line 63:arp rate-limit 8192 Line 68:timeout pat-klate 0:00:30
Messages LL not decovered slides discovered xisting policy objects reused plicies discovered		Severity	Description Palicy descovery does not support the following CLI in your configuration: Line 6:ono acchiness auto Line 60:no acchinest enternate Line 60:arp rate-linit 8:192 Line 60:timeout pat-viate 0:00:30 Line 70:timeout top-prony-reasentialy 0:01:00 Line 70:timeout footing-com 0:00:00
Messages 11 not docuvered olicies discovered visiting policy objects reused olicies discovered		Severity	Cescription Pulcy discovery does not support the following CLI in your configuration: Une 60:no acids intervenable Une 60:arp permit nonconnected Une 60:arp rate-limit 8:92 Une 68:timeout pet-state 0:00:30 Une 73:timeout top-proxy-reaseenably 0:01:00 Une 74:timeout floating core 0:00:00 Action
Messages I not docovered olicies discovered xisting policy objects reused olicies discovered		Severity	Description           Palicy discovery does not support the following CLI in your configuration:           Line 6ine mac-address auto           Line 6ine mac-address auto           Line 62:no arp pensit-reconnected           Line 63:arp rate-limit 8192           Line 68:timeout pat-klate 0:00:30           Line 73:timeout top-proxy-reassenbly 0:01:00           Line 74:timeout floating-conn 0:00:00           Action           If you wish to manage these commands in CS Manager, please use the "Nex Config" function

Y de los cambios fuera de banda tampoco puede tener ningún cambio.



#### Descubrimiento masivo de dispositivos

Para detectar políticas para varios dispositivos, puede llevar a cabo un redescubrimiento masivo. Es importante tener en cuenta que el redescubrimiento masivo se limita a los dispositivos activos , aquellos que están actualmente operativos y accesibles dentro de su red.

No puede realizar la detección masiva en el contexto de seguridad, sensores virtuales. Los módulos de servicio se pueden detectar si se seleccionan por separado.

#### Pasos para realizar la detección masiva de dispositivos:

Paso 1:

Vaya a Política > Detectar políticas en el dispositivo



#### Paso 2:

Si va a realizar una redetección masiva, sólo puede aparecer el cuadro de diálogo de redetección masiva.

Desde los dispositivos disponibles en el panel izquierdo , elija la lista de dispositivos para los que desea detectar políticas y muévalos al lado derecho.



#### Paso 3:

Compruebe si todos los dispositivos seleccionados aparecen en la lista y haga clic en Finish (Finalizar) para continuar con el redescubrimiento masivo.

Asegúrese de conocer la topología de red y los cambios que pueden producirse en ella antes de continuar con la detección.





#### Ambos dispositivos se han detectado correctamente.

	107%						
Status: Devices to be discovered: Devices discovered successfully: Devices discovered with errors:	Discovery comp 2 2 0	sleted with a		nga			
Iscovery Details	Severity	State	_		Discovered From		
ASA 1	0	Discover	ry Car	opicted with Warrings	Live Device		
S 454.2	0	Discours	ry Car	noleted with Warnings	Live Device		
_							
		Seventy		Description			
Messages AP self-configuration was not doo	overed.	Seventy	~	Description No CAP sml configurat	ion file found on device.		
Messages Resages S2 xml configuration was not doo S2 xml configuration was not doo	overed.	Severity	^	Description No DAP xml configurat	ion file found on device.		
<ul> <li>Messages</li> <li>Minimi configuration was not deposite on the second second</li></ul>	overed. overed. on device or not	Seventy	^	Description No DAP sml configurat	ion file found on device.		
Messages AP tool configuration was not dep SD tool configuration was not dep ostocan package file is not found i complete Remote Access VPN Cor	overed. overed. on device or not rhfguration	Seventy 0 0 0	^	Description No CAP sel configurat	ion file found on device.		
Messages Messages SD xml configuration was not deo ostacan package file is not found i complete Remote Access VPN Cor L1 not discovered	overed. overed. on device or not rifiguration	Seventy 0 0 A A	^	Description No DAP sel configurat	ion file found on device.		
Messages AP totil configuration was not doo so totil configuration was not doo ostscan package file is not found o complete Remote Access VPV Cor L1 not docovered skices docovered	overed. overed. on device or not nfiguration	Seventy 0 0 0 0	A	Description No DAP sel configurat Action No action is required.	ion file found on device.		
Messages 30 smil configuration was not doo 30 smil configuration was not doo tostocan package file is not found o ncomplete Remote Access VPN Con 1.1 not docovered tolicies docovered tolicies docovered tolicies docovered	overed. overed. on device or not ofiguration	Seventy 0 0 A 0 0 0 0 0	•	Description No DAP sel configurat Action No action is required.	ion file found on device.		

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).