# Configuración del Administrador de Seguridad en Cisco IOS IPS

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Información Relacionada

## **Introducción**

Cisco Security Manager forma parte de Cisco Security Management Suite, que ofrece una administración y aplicación de políticas completas para la red de autodefensa de Cisco. Cisco Security Manager es una aplicación de clase empresarial líder del sector para la gestión de la seguridad. Cisco Security Manager aborda la gestión de la configuración de los servicios de seguridad de firewall, VPN y del sistema de prevención de intrusiones (IPS) en los routers, dispositivos de seguridad y módulos de servicios de seguridad de Cisco.

Para obtener un resumen de las características y ventajas de Cisco Security Manager, así como de las nuevas funciones de la versión 3.1, consulte la hoja de datos de Cisco Security Manager 3.1 en

<u>http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product\_data\_sheet0900aecd</u> <u>8062bf6e.html</u>. Puede descargar Cisco Security Manager 3.1 de Cisco.com en <u>http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app</u> (<u>sólo</u> clientes\_registrados).

Este documento describe cómo utilizar Cisco Security Manager 3.1 para realizar la configuración inicial de IOS IPS. Para los routers ya configurados con IOS IPS, los clientes pueden utilizar directamente Cisco Security Manager 3.1 para las tareas de aprovisionamiento.

**Nota:** Cisco Security Manager 3.1 soporta solamente las imágenes IOS 12.4(11)T2 y posteriores para configurar IOS IPS.

## **Prerequisites**

### **Requirements**

No hay requisitos específicos para este documento.

#### **Componentes Utilizados**

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

- Cisco Security Manager 3.1
- Cisco IOS 12.4(11)T2

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.

#### **Convenciones**

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

## **Configurar**

Complete estos pasos para configurar IOS IPS:

- 1. Ejecute el cliente Cisco Security Manager 3.1 desde su PC local.
- 2. Elija **Nuevo dispositivo** en el menú Archivo para agregar un dispositivo a Cisco Security Manager

Edit View P	olicy Map Tools H	nnected to 172.25.90.8 No		
Sew Device	CHAN D	2		
gone Device				
Delete Device		Device: 1/2.25.90.91 Pc	icy: HexConfigs	
Seve	Col+5	Prepended FlexConfigs		
Vew Changes.		Nio.	Name	Description
Yaldate				
Sybrit				
Sugenit and Dep	kay			
Depky				
Discard				
Edit Device Gro	ups			
Neg Device Gro	1.p			
Add Devices to	Gene			
Bint	Ctd4P			
t.e	Col+Q			
D HELESS FLOR		Appended FlexConfigs		
[] Inspection	Rules	No.	Name	Description
E Settings				
C was like 1	K Hules			
D web ricer	POJED			
INAT				
Site to Site VPR				
Remote Access	I VPN			
B SSL VPN				
] Interfaces				
8 Platform				
FlexCorbgs				
				Values Proview 🔄 🗟 🖉 🖄

 En la ventana Nuevo dispositivo, elija cómo desea agregar el dispositivo. Este ejemplo agrega el dispositivo desde la red.

🏦 New Device - Choose Method (Step 1 of)		×
Please choose how you would like to add the device:		
Add Device From Network		
When you add a device that is live on the network, Cisco Security Manager makes a secure connection with the device and discovers its identifying information and properties.		
Add from Configuration File	-	
When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.	T.	
Add New Device	100	
You can add a device that is not yet on the network by specifying the device's identifying information and credentials.	1	
Add Device From DCR	ŕ	
If you are using other CiscoWorks applications and your devices have already been added to the device credentials repository, you can import them into Cisco Security Manager.		
Back Next Pinsh	Cancel	Help

- 4. Haga clic en Next (Siguiente).
- 5. Introduzca los detalles de identidad del dispositivo que desea agregar. Por ejemplo, nombre de host y dirección

IP.

Identity		
IP Type:	Static 🖌	
Host Name:		
Domain Name:		
IP Address:	172.25.90.91	
Display Name:*	172.25.90.91	
OS Type:*	×	
	105 - 12.3+	
	105 - Catalyst 6500/7600	
Discover Device Se	ettin PIX	
Discover:	IP5	
	ASA	
	Pirewal Policies	
	DPS Policies	
	RA VPN Policies	
	Discover Policies for Security Contexts	

- 6. Haga clic en Next (Siguiente).
- 7. Introduzca las credenciales principales, como el nombre de usuario, la contraseña o la contraseña Enable para el router IOS que desea agregar.
- 8. Haga clic en **Finalizar** para agregar el dispositivo a Cisco Security Manager.**Nota:** En este ejemplo se asume que el usuario ya tiene un router preconfigurado y puede iniciar sesión en el router con las credenciales adecuadas.

Password:* Password: Enable Password: Confirm:  HTTP Credentials Username: Password: Confirm: HTTP Port: Password: Confirm:  HTTP Sport: HTTPS Port: HTTPS StDEP Mode: HTTPS StDEP Mode: HTTPS StDEP Mode: StMP	Primary Credentials	risco 1224				
Password:       Confirm:         Enable Password:       Confirm:         HTTP Credentials       Use Primary Credentials         Username:       Password:         Password:       Confirm:         Confirm:       Confirm:         HTTP Port:       90         HTTPS Port:       91         PS RDEP Mode:       HTTPS         Certificate Common Name:       Confirm:         RX-Boot Mode       SMMP	Username:	CBC01234		<b>F</b>		
Enable Password: Confirm: Confirm: HTTP Credentials Username: Password: Confirm: Con	Password:*		Confirm:*			
HTTP Credentials         Use Primary Credentials         Username:         Password:         Confirm:         HTTP Port:         90         HTTPS Port:         91         HTTPS Port:         92         Confirm:         Confirm:         Confirm:         MTTP Sport:         90         HTTPS Port:         91         MTTPS Port:         92         Certificate Common Name:         Confirm:	Enable Password:		Confirm:			
Use Primary Credentials   Username:   Password:   Confirm:   HTTP Port:   80   HTTPS Port:   90   HTTPS Port:   91   PS RDEP Mode:   HTTPS   Certificate Common Name:   Confirm:     RX-Boot Mode	HTTP Credentials					
Username: Password: Confirm: HTTP Port:  80 HTTPS Port:  443 IPS RDEP Mode:  HTTPS Certificate Common Name: Confirm: Confirm:		Use Primary Credentials				
Password:       Confirm:       HTTP Port:       80       HTTPS Port:       943       IPS RDEP Mode:       HTTPS       Certificate Common Name:       Confirm:		Username:				
Confirm:         HTTP Port:         #0         HTTPS Port:         #43         IPS RDEP Mode:         HTTPS         Certificate Common Name:         Confirm:		Password:				
HTTP Port: 80 HTTPS Port: 443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm: Confirm:		Confirm:				
HTTPS Port: [443 IPS RDEP Mode: HTTPS Certificate Common Name: Confirm:	HTTP Port:	80				
IPS RDEP Mode:     HTTPS       Certificate Common Name:     Confirm:       RX-Boot Mode     SNMP	HTTPS Port:	443				
Certificate Common Name: Confirm: Confirm: RX-Boot Mode SNMP	IPS RDEP Mode:	HTTPS				
RX-Boot Mode SNMP	Certificate Common Name:		Confirm:			
RA-5000 PROB	DV-Boot Mode	0.840				
	RX-000( P000					

Cuando aparece "Detección finalizada" en la ventana Estado de detección, ha agregado correctamente un dispositivo a Cisco Security Manager. Una vez que haya agregado correctamente un dispositivo en Cisco Security Manager, debe asignar una clave pública para habilitar IPS.

	The second second						
-	100%		_				
Status:	Discovery comple	ted with warn	inos				
Devices to be discovered:	1						
Devices discovered successfully:	1						
Devices discovered with errors:	0						
Discovery Details							
Type Name	Severity	a mananananana	Rate	Innantanananana	Discovered	From	
172.25.90.91	0	Discovery C	ompleted with Warnings	Live Device			
Messages		Severity	Description				
Messages Interfaces wide open for traffic		Severity	Description The following interface ng a new Access-rule	s are wide open for	traffic as there is r	no ACL applied on t	hem. Addi
Messages Interfaces wide open for braffic Policies discovered		Severity	Description The following interface ng a new Access-rule i emission of traffic any ExetEtheoreth	is are wide open for on these interfaces i more:	traffic as there is r reans that there w	no ACL applied on t ill no longer be suc	them. Addi h implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused		Severity @ @	Description The following interface ng a new Access-rule i emission of traffic any FastEthernet0 FastEthernet1	is are wide open for on these interfaces i more:	traffic as there is r nears that there w	no ACL applied on t ell no longer be suc	hem. Addi /
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered		Severity (1) (2) (2) (2) (3) (3) (4) (4) (4) (4) (4) (4) (4) (4	Description The following interface ing a new Access-rule i emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3	is are wide open for on these interfaces i more:	traffic as there is n nears that there w	no ACL applied on t ill no longer be suc	them. Addi /
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Seventy	Description The following interface ing a new Access-rule in emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 Dualt 10 adu0	is are wide open for on these interfaces i more:	traffic as there is r nears that there w	no ACL applied on t ill no longer be suc	them. Addi /
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Severity (C) (C) (C) (C) (C) (C) (C) (C)	Description The following interface ng a new Access-rule emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet5	is are wide open for on these interfaces i more:	traffic as there is n nears that there w	no ACL applied on t ell no longer be suc	them. Addi / h implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity (1) (2) (2) (2) (2) (3) (3) (4) (4) (5) (4) (5) (4) (5) (5) (5) (5) (5) (5) (5) (5	Description The following interface ing a new Access-rule i emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet5 FastEthernet5 FastEthernet6 FastEthernet6 FastEthernet6 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet8 Fa	is are wide open for in these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ed to be wide open	no ACL applied on t ill no longer be suc	them. Addi h implicit p fric. If not, c
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful		Severity (i) (i) (i) (i) (i) (i) (i) (i)	Description The following interface ng a new Access-rule of ermission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 Point in aduo Action Please verify whether nfigure an access rule	is are wide open for on these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ad to be wide open	no ACL applied on t ill no longer be suc for all types of tra	them. Addi h implicit p fric. If not, o
Messages Interfaces wide open for braffic Policies discovered Existing policy objects reused IPS signature policy not discovered Add Device Successful		Seventy (i) (ii) (iii)) (iii) (iii) (iii) (iii)(	Description The following interface ing a new Access-rule in emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet4 FastEthernet5 FastEthernet5 FastEthernet5 FastEthernet5 FastEthernet6 FastEthernet6 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet7 FastEthernet8 F	is are wide open for on these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ed to be wide open	no ACL applied on t all no longer be suc for all types of tra	them, Add / h implicit p
Messages Interfaces wide open for traffic Policies discovered Existing policy objects reused IP5 signature policy not discovered Add Device Successful	•	Sevenity © © @	Description The following interface ing a new Access-rule in emission of traffic any FastEthernet0 FastEthernet1 FastEthernet2 FastEthernet3 FastEthernet4 F	is are wide open for in these interfaces i more: these interfaces ne or ACL accordingly.	traffic as there is n nears that there w ed to be wide open	no ACL applied on t all no longer be suc for all types of tra	them. Add A h implicit p

- 9. En el menú de la izquierda, vaya a la pantalla de configuración de FlexConfigs.
- 10. Haga clic en la interfaz de usuario de FlexConfigs en el lado derecho de la pantalla y, a continuación, haga clic en el icono

Agregar.

Cinco Security Manager - admir	Connected to '172.25.90	<b>*</b>	ز المالد
Dae Eldt Jawa Boych Rab Toos	Reb		
	3 ?		
Denkes 🔂 🖗	Device: 172.25.90.33	Palicy: FlexConfigs	
Filter : none 💉	Prepended PlexCon	la	
<ul> <li>Department.</li> <li>Location</li> <li>Al</li> <li>172.25.90.33</li> <li>172.25.90.34</li> </ul>	- No	Nome	Description
AAA Rules Access Rules Inspection Rules (i) Settings	Appended FlexConf	igs	Parcellan
Transparent Rules	And Personal Property lies	and the second se	Description
Web Filter Rules			
C Employ			
E Synthetics			
I total an Date			
CI MAT			
C State State VEN			
ED. Bamota Arcane VEN			
CO CO VEN			
E Marfaras			
E Platform			Values Preview + +
1 Continue			
Trançores			(#00)

11. En la lista FlexConfigs seleccionados, elija IOS\_IPS\_PUBLIC\_KEY y haga clic en Aceptar.

Filter : none		Name	
D care sta anti-		IOS_IPS_PUBLIC_KEY	
E CATEK_ECLB_portchannel			
Oviok_inewal_hukpe_var_inkerraces			
D 105 CA server			
E 105 compress config			
105 config root wireless station			
105 console AAA bypass			
105 Copy Image			
105_enable_SSL	>>	]	
IOS_FPM	<<		
105_IPS_SIGNATURE_CATEGORY	 	,	
IOS_PKI_with_AAA			
105_set_clock			
105_VOIP_advance			
105_V0IP_simple			
105_VPN_config_gre_tunnel			
105_VPN_set_interface_desc			
105_VPN_shutdown_inside_interface			

- 12. Haga clic en **Guardar** para guardar los cambios.**Nota:** La FlexConfig de IOS\_IPS\_PUBLIC\_KEY contiene la configuración para la clave pública.
- 13. En el menú de la izquierda, elija General Settings, situado debajo del encabezado IPS.
- 14. Introduzca la ubicación de configuración IPS en la memoria flash. Ésta es la ubicación en la que se ubican las configuraciones IPS.
- 15. Haga clic en **Guardar** para guardar los cambios.

Cisco Security Manager - admin Co	nected to '172.25.90.8'		
De for her ford Be fore 5	2		_
Devkes 🔁 🗇	Device: 172.25.90.33 Policy: General Settings		
Filter :	Block Traffic when IPS engine unan Apply Deny Action on: Ingress Interface SDEE Properties Maximum Subscriptions:* 1 Maximum Alerts:* 200 Maximum Messages:* 200	valable	
AAAA Rules  Access Rules  Dropectun Rules  Settings Transparent Rules  PFS Signatures EVent Actions Centeral Settings NAT Site to Site VPN ERenote Access VFN EStu VeN ED Interfaces Platform Platform Platform VenterActions VenterAccess VenterAcces VenterAcces VenterAccess VenterAcces V	IPS Config Location:       Fisch:/ps         Max retries:       I         Traeout seconds between retries:       D		
			ave

**Nota:** Asegúrese de que el directorio de ubicación ya se ha creado en la memoria flash del router. Si no es así, utilice el comando **mkdir <directory\_name>** para crear el directorio de ubicación.

- 16. Para habilitar IPS, navegue hasta Reglas de interfaz, marque la casilla de verificación Enable IPS y luego haga clic en Add Row.
- 17. En el cuadro de diálogo Agregar regla IPS, introduzca un nombre para la regla IPS en el campo Nombre de regla y, a continuación, haga clic en **Agregar fila** para incluir las interfaces en las que se debe aplicar IPS.

🙀 Cisco Security Manager - admin I	annexted to '172.25.99.8'
Elle Edit Yew Balicy Map Ioolis	9ab
🖢 🖉 💽 💽 🛸 🗟 🗇	
	Device 172 25 90.33 Policy Interface Rules
Denkes	
Fiter : - none - w	V (nuble 25
Department	No. Rule Name ACL Name Interface (Direction)
Jacation	
- (1) Al	
172.25.90.33	ADD IPS RUAE
172.25.90.34	Add/tdt IPS Rule
	Pair Name* Instal
	W.L.Name:
	Interface (Derection) Derection
AAA Rules	
Access Rules	
Dispection Rules	
E Settings	
Transparent Rules	
Web Filter Rules	
E 195	Add Row
🗇 Signatures	
Event Actions	OK Cancel Help
General Settings	
Disterface Rules	
INAT	
Size to Size VPN	
Remote Access VPN	
B SSL VPN	
E Interfaces	
E Platform	
I Hercomps V	
	Save

18. Haga clic en el botón de opción que indica en qué dirección debe aplicarse la regla IPS y, a continuación, haga clic en **Seleccionar** para elegir las interfaces

Direction:*				
In	Out		Both	
Interfaces:*	[		Select	
	_	~	Carcal	Hab

adecuadas.

19. Elija una interfaz de la lista Selector de interfaces y haga clic en

Available In	terfaces:	
Firendole b		
Filter :	none	~
Do	t11Radio0	
🖤 Fa	stEthernet0	
🖝 Fa	stEthernet1	
🖝 Fa	stEthernet2	
🖝 Fa	stEthernet3	
E Fa	stEthernet4	
w vie	an1	
Al 💭	-Interfaces	
Ex	ternal	
In 🔂	ternal	
Selected		
Vlan1		
2/		
L		

20. Haga clic en Guardar para guardar los cambios.



21. Elija **Tools > Apply IPS Update** para instalar las firmas IPS más



22. Elija el archivo de firma más reciente y haga clic en

#### Siguiente.

Turner Signatu	ra I Indator I at			labert fundables	105 CT MCD
Libbe: Diduaro	re opoaces			Latest Available:	IPS-CS-MGR-sig-S282-reg-E1.zp IPS-CS-MGR-sig-S282-reg-E1.zip
	File	Sig.	Engine	Latest Applied:	IPS-CS-MGR-sig-5282-reg-E1.zip
IPS-CS-MGR-sig-S	278-req-E1.zip	278	1	Latest Deployed:	IPS-CS-MGR-sig-5282-req-E1.zip
IPS-CS-MGR-sig-S	280-req-E1.zip	280	1	Last Checked On:	Apr 10 2007 10:46:37
IDC /C M/D do C	102 years E1 ain	202		Last Downloaded On: Apr 19 2007 10:45:48	
aro-co-mak-sig-o	202-red-c1-ap	202		Last Deployed On:	Apr 23 2007 17:56:38
					Check For Updates
					Download Latest Updates
Update Details	i			1	
File: Description:	IPS-CS-MGR-sig-S IPS-CS-MGR-sig-S	282-req-E1.zip 282-req-E1.zip			
Date:	Apr 19 2007	Size:	3.8MB		
Release:	5282	Required Engine Le	vel: E1	]	

23. Elija los dispositivos en los que se debe aplicar la actualización IPS y haga clic en **Siguiente**.

Type: Local Signatures Policies	172.25.90.33
<ul> <li>Department</li> <li>Location</li> <li>All</li> <li>172.25.90.33</li> <li>172.25.90.33</li> </ul>	
Select All Deselect All	Back Next Finish Cancel Hel

24. Haga clic en **Finalizar** para aplicar las firmas.

	Therein	1	<u> </u>	Y	(		mppiny	
ID	Sub	Name	Actions	Severity	Fidelity	Source	Enabled	Risk F
1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default	true	18
1001	0	IP options-Record Packet Route	Produce Alert	Infomiational	100	Detaut	1060	122
1002	0	IP options-Timestamp	Produce Alert	Infomiational	100	Default	(also	13
1003	0	IP options Provide s, c, h, tcc	Produce Alert	Informational	100	Oefault	(false)	3
1094	0	IP options-Loose Source Route	Produce Alert	Hep	100	Oefault	(alsa	100
1095	0	IP options-SATNET ID	Produce Alert	Informational	100//	Oefault	(also	(\$)
1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default	true	100
<			.0					
								1

25. Navegue hasta IPS y elija **Firmas** para ver la lista de todas las firmas

	0.0	2					-	TAXABLE INCOME.
Devices	20	Device: 1	72.25.9	0.33 Policy: Signatures				
Rer: -none w		· file	r: ( no	ne)				
A Decartment	_			× (			Apply	Oear
Location		D	Sub	distantianan Nore settenenten	tis initialistication and an initialistic	Severity	Fidelity	Source
AI .		1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default
172.25.90.35		1965	0	JP uptons-Record Packet Route	Produce Aiert	Aristeinite	100	Datest
		1062	0	JP optons-Telestawp	Produce Wert	kroteeroint	100	Defeix .
		1002	0	IP options = rovide s, c, h, tcc	Produce Alert	Arroteening //	100	Datast
		1003	0	JP optertex-Loose Source Route	Produce Ajert	1400	100	Defect.
	_	1005	0	IP options SATNET ID	Produce Alert	hometon#	100	Datast
		1006	0	IP options-Strict Source Route	Produce Alert	High	100	Default
Frend	^	1002	116	Pop over Port () () () () () ()	( Produce Alert ) ( ) ( ) ( ) ( ) ( ) ( )	kroteinin ///	1/ 60%	history)
Access Dules	- 1	1101	0	Uninown IP Protocol	Produce Alert	Informational	75	Default
Inspection Rules		1102	0	Impossible IP Packet	Produce Alert	High	100	Default
8 Settings		1104	0	IP Localhost Source Spool	Produce Alert	High	100	Default
Transparent Rules		1102	110	APC 1918 Addresses Seen (111111	Produce Wert ////////////////////////////////////	Kristeinin ///	1/ /01	history)
Web Filter Rules		1108	0	IP Packet with Proto 11	Produce Alert	High	100	Default
IP5	- 11	1104	116	Gaco 305 Interface DoS ///////////////////////////////////	())))))///////////////////////////////	111 mbHUII	1118	hinted )
Supports     Support	- 1	1109	112	Gaco 105 Interface Do5	Produce Alert	Nedum	5	Defeit
General Settings		1108	211	Geo 105 Interface DoS	Produce Aiert	Nedan	3	Owland
Dinterface Rules		1109	992	Gion 105 Interface DoS	Produce diert	Hedun	3	Ortest
NAT		1200	0	If framer Combe	Denv Partiel Inine Protine Aert	and an and a second	001	Ortest
Site to Site VPN		1202	an	IP Frammeri Covernin - Datastram Too Long	Denv Parket Inine Produce Alert	11111111111	100	Contration of the
Remote Access VPN		4		Program creature balagian roo sang	neid cener neistriggen weit		100	2000
SOL WHY Inderforms	1	1				Marc 18 data in and		DA COLO
Station .						Vew update Level		

26. Elija **File > Submit and Deploy** para implementar IPS en el router IOS.

Sew Device Col+N	3	?						
Delete Device	1	Nevice: 1	72.25.9	3.33 Policy: Signatures				
Saun Oulus	П	- Filte	r (	(* -)				
Ven Changes		-			~		Acoly	Oner
Validate		ID.	Sub.	Nane	Adtons	Severky	Fidelity	Source
Submit		1000	0	IP options-Bad Option List	Produce Alert	Informational	75	Default /
Submit and Depkoy	H.	1000	1116	IP options Record Packet Route	() Produce Alert () () () () ()	kniskiering ///	1// 605	Auto)
Depky	11	1002	112	IP options-Timestamp	Produce filert	herothererot	100	Outaut
Discard	н	1003	0	P options-Fravide s.c.h.tct	Produce diert	Informational	100	Cufault
Edit Device Groups		1004	18	IP options Loose Source Route	Produce Alert	Hot	100	Ordent
leg Device Group		1005	211	IP options GATNET ID	Produce filert	Informational	100	Outsut
Add Devices to Ggoup		1006	000	P options-Shirt Sauce Raite	Produce Alert	Hoh	100	Default
39% ObleP		1007	1116	Bedder Bed (11111111111111111	unnin hall all all all all all all all all al	Sectements (111)	11/606	1 seco
tyt Col+Q		1101	000	Unincen IP Protocol	Produce Alert	Informational	14000	Defailt
Temestes Rules	1	1102	0	Incossile & Parket	Produce Alert	Hab	100	Defail
E Settinos	1	1104	0	Disrabat Sagra Sagra	Drockute Alert	Herb.	100	Colard
Transparent Rules		( state	in	11111111111111111111111111111111111111	11111111111111111111111111111111111111	1111 Jackardala	11166	1ALLAN
Web Filter Rules		1100	1600	in the state of the second sec	Inder Mat	mand	100	(mm)
195		1198	in	Prese were berling	Produce rear	1111 MALLING	Sum	(ALLA)
Signatures	11	TTAG	EU.	CBO ICS INSERTION DOS	HODICE MALE	all and the	COU	Carson
Event Actions		7105	20	Caso Jus aneerace pes	Produce Here	1 bear	am	Caland
T Interface Rules		1105	199	cisco pro asseriace pos	Produce siert	() (seared ))	BUI	Carrie .
NAT		7705	12	Carco Jus Interface Dos	Produce April	() Noaru ()	200	Caland
Site to Site VPN	1	1500	1611	The Extension Contactor ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	Deny Packet Inine, Produce Alert	11 papaletora	100	Calant
Remote Access VPN		1202	0	IP Fragment Overrun - Datagrain Too Long	Deny Packet Inline, Produce Alert	High	100	Default 1
SSL VPN		<		-				>
Interfaces						View Update Level		

27. Elija el dispositivo en el que desea implementar los cambios y haga clic en

~	3 172.25.90.33		

28. Vea el estado de implementación para verificar si hay algún error.

the second s					
nof men or and o crains					
			_		
	125				
Status:	Deployed (1 out of 1 d	sevices com	pleted.)		
Deployment Job Name:	admin_job_2007-04-24	10:53:10.	468		
Devices To Be Deployed:	1				
Devices Deployed Successfully:	1				
Devices Deployed with Errors:	0				
Deployment Details (1/1 loaded	£)				
Device S	tatus Su	mmary	Method	Config	Transcript
135 OF 00 55 00 00 00 00 00 00 00 00 00 00 00	a site		(Barrison)	EA.	10
172.25.90.33 SUCCEED	co 🖓 warn	ing: 2	Device	*	*
172.25.90.33 SUCCEED	an an warn	ing: 2	Device	*	*
172.25.90.33 SUCCEED	co <u>"</u> wern	ng: 2	Device	*	*
Messages	co <u>"D</u> warn Seve	erity	scription >>> Difference of file "C:\PROGRA	~1\CSCOpx\MDCite	90 mp\2007.04.24_10.53.
Messages Nut of Band Change: CLI	co Wern	erity De-	scription scription >>> Difference of file "C:\/PROGRA _job_admin_job_2007-04-24 10_5: Oldiff archived" and file "C:\PROGRA	~1\CSCOpx\MDC\te 3_10_468\lphase1\1 A&~1CSCOpx\MDC\te	mpl/2007.04.24_10.53. 72_25_90_33_4294980 templ/2007.04.24_10.5
Messages Dut of Band Change: CLI Operation Successful	CU Jawarn Seve C	erity De: 2 2 3 15 74 3.1	scription >>> Difference of file "C:\PROGRA _job_admin_job_2007-04-24 10_5 0)diff_archived" and file "C:\PROG 15_job_admin_job_2007-04-24 10_	~1\CSCOpx\MDC\te 3_10_468\lphase1\1 RA~1\CSCOpx\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53 72_25_90_33_4294960 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Jut of Band Change: CLI Operation Successful ig update compilation warning	co da warn Seve d d d	erity Dec 2 2 2 2 2 2 2 2 2 2 2 2 2	scription >>> Difference of file "C:\PROGRA _job_admin_job_2007-04-24 10_5 0)diff_archived" and file "C:\PROG 15_job_admin_job_2007-04-24 10_ 740)diff_uploaded".	~1\CSCOpx\MDC\te 3_10_468\lphase1\1 RA~1\CSCOpx\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Out of Band Change: CLI Operation Successful ig update compilation warning ig update engine compilation status	co di warn Seve di di di di di	erity Dec 2 2 2 2 2 2 2 2 2 2 2 2 2	scription scription >>> Difference of file "C:\PROGRA _iob_admin_job_2007-04-24 10_Si 0\diff_archived" and file "C:\PROG 15_job_admin_job_2007-04-24 10_ 740\diff_uploaded". Ra	~1\CSCOpx:\MDC\te 3_10_468\lphase1\1 X&~1\CSCOpx.\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Messages Dut of Band Change: CLI Operation Successful lig update engine compilation status Operation Successful	CU Seve      	erity De: 2 15 3 15 74 0 3.1 80 0 -9 0 -9 0 -9	scription >>> Difference of file "C:\PROGRA .job_admin_job_2007-04-24 10_5 Ojdiff_archived" and file "C:\PROGI 15_job_admin_job_2007-04-24 10_ 740\diff_uploaded".	~1\CSCOpx\MDC\te 3_10_468\lphase1\1 X&~1\CSCOpx\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful ig update compilation warning ig update engine compilation status Operation Successful Operation Successful	CU Jawarn	Prity Der 15 15 15 15 15 15 15 15 15 15	scription >>> Difference of file "C:\PROGRA _job_admin_job_2007-04-24 10_5 0)diff_archived" and file "C:\PROGI 15_job_admin_job_2007-04-24 10_ 740\diff_uploaded". Ra tion	~1\CSCOpx\MDC\te 8_10_468\lphase1\1 RA~1\CSCOpx\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful lig update compilation warning lig update engine compilation status Operation Successful Operation Successful Deployment Log	Seve A A A A A A A A A A A A A A A A A A	Price 2	scription scription >>> Difference of file "C:\PROGRA _job_admin_job_2007-04-24 10_5 0\diff_archived" and file "C:\PROG 15_job_admin_job_2007-04-24 10_ 740\diff_uploaded". Na tion	~1\CSCOpx\MDC\te 3_10_468\lphase1\1 RA~1\CSCOpx\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53, 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949
Messages Dut of Band Change: CLI Operation Successful Rig update compilation warning Rig update engine compilation status Operation Successful Deployment Log	co warn	rity Der 2 2 2 2 3 5 5 5 5 5 5 5 5 5 5 5 5 5	sciption sciption >>> Difference of file "C:\PROGRA _job_admin_job_2007-04-24 10_51 0)diff_archived" and file "C:\PROGRA _job_admin_job_2007-04-24 10_ 740)diff_uploaded". Na tion	~1\CSCOpx\MDC\te 8_10_468\lphase1\1 X&~1\CSCOpx\MDC\ 53_10_468\lphase1	mpl/2007.04.24_10.53. 72_25_90_33_4294980 templ/2007.04.24_10.5 \172_25_90_33_42949
Messages Nut of Band Change: CLI Operation Successful lig update engine compilation status Operation Successful Operation Successful Operation Successful	CU JS Warn	erity De: 2 15 3 15 74 0 3.1 80 0 -9 0 4.d	scription scription >>> Difference of file "C:\PROGRA 	~1\CSCOpx:\MDC\te 3_10_468\lphase1\1 X&~1\CSCOpx:\MDC\ 53_10_468\lphase1	mp\2007.04.24_10.53. 72_25_90_33_4294980 temp\2007.04.24_10.5 \172_25_90_33_42949

## Información Relacionada

- Página de productos y servicios de Cisco IOS Intrusion Prevention System (IPS)
- Introducción a Cisco IOS IPS con formato de firma 5.x
- <u>Compatibilidad con formato de firma IPS 5.x y mejoras de uso</u>
- <u>Cisco Intrusion Prevention System</u>
- Avisos de campo de productos de seguridad (incluida CiscoSecure Intrusion Detection)
- <u>Soporte Técnico Cisco Systems</u>