Configuración de Cisco IOS IPS con un router y SDM

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Información Relacionada

Introducción

Este documento describe cómo utilizar Cisco Router and Security Device Manager (SDM) versión 2.5 para configurar Cisco IOS[®] Intrusion Prevention System (IPS) en 12.4(15)T3 y versiones posteriores.

Las mejoras en SDM 2.5 relacionadas con IOS IPS son:

- Número total de firma compilada que se muestra en la GUI de la lista de firmas
- Archivos de firma SDM (formato de archivo zip; por ejemplo, sigv5-SDM-S307.zip) y paquetes de firma CLI (formato de archivo pkg; por ejemplo, IOS-S313-CLI.pkg) se puede descargar juntos en una operación
- Los paquetes de firma descargados se pueden enviar automáticamente al router como opción

Las tareas involucradas en el proceso de aprovisionamiento inicial son:

- 1. Descargue e instale SDM 2.5.
- 2. Utilice SDM Auto Update para descargar el paquete de firma IPS de IOS en un equipo local.
- 3. Inicie el asistente de políticas IPS para configurar IOS IPS.
- 4. Verifique que la configuración y las firmas de IOS IPS estén correctamente cargadas

Cisco SDM es una herramienta de configuración basada en Web que simplifica la configuración de router y seguridad mediante asistentes inteligentes que ayudan a los clientes a implementar, configurar y supervisar de forma rápida y sencilla un router de Cisco sin necesidad de conocer la interfaz de línea de comandos (CLI).

SDM versión 2.5 se puede descargar de Cisco.com en <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm</u> (sólo clientes registrados). La nota de la versión se puede encontrar en <u>http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/soft</u> ware/release/notes/SDMr.25.html

Nota: Cisco SDM requiere una resolución de pantalla de al menos 1024 x 768.

Nota: Cisco SDM requiere que el tamaño del montón de memoria Java no sea inferior a 256 MB para configurar IOS IPS. Para cambiar el tamaño del montón de memoria Java, abra el panel de control Java, haga clic en la pestaña **Java**, haga clic en **View** ubicado en Java Applet Runtime Settings y, a continuación, introduzca **-Xmx256m** en la columna Java Runtime Parameter.

Java Runtime Set Java Runtime Versions	tings		I	
Product Name	Version	Location	Java Runtime Parame	
IRE	1.6.0_03	C:\Program Files\Java\	-Xmx256m	
RE	1.6.0_03	C:\Program Files\Java\	-Xmx256m	

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 IOS IPS en las versiones 12.4(15)T3 y posteriores
- Router de Cisco y Security Device Manager (SDM) versión 2.5

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

Nota: Abra una sesión de consola o telnet al router (con "monitor de término" activado) para monitorear los mensajes cuando utilice SDM para aprovisionar IPS de IOS.

- 1. Descargue SDM 2.5 de Cisco.com en <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm</u> (<u>sólo</u> clientes registrados) e instálelo en un equipo local.
- 2. Ejecute SDM 2.5 desde el PC local.
- 3. Cuando aparezca el cuadro de diálogo Inicio de sesión de IOS IPS, introduzca el mismo

nombre de usuario y contraseña que utiliza para la autenticación de SDM en el

IOS IPS Login		X
Enter User n	ame and password for IOS IPS	
Username:	admin	
Password:	[*****	
]	OK Cancel	

router.

- 4. En la interfaz de usuario de SDM, haga clic en **Configurar** y, a continuación, haga clic en **Prevención de intrusiones**.
- 5. Haga clic en la pestaña Edit IPS.
- 6. Si la notificación SDEE no está habilitada en el router, haga clic en **Aceptar** para habilitar la notificación

SDEE.

Information		×
į	SDEE notification is not enabled. IPS will enable SDEE notification so it can receive SDEE messages.	
	OK	

- 7. En el área Descargar archivo de firma de Cisco.com de la ficha Editar IPS, haga clic en el botón de opción Obtener el archivo SDM más reciente y el botón de opción CLI pkg y, a continuación, haga clic en Examinar para seleccionar un directorio en su equipo local en el que guardar los archivos descargados.Puede elegir el directorio raíz del servidor TFTP o FTP, que se utilizará más adelante cuando implemente el paquete de firma en el router.
- 8. Haga clic en **Descarga**.



9. Cuando aparezca el cuadro de diálogo Inicio de sesión de CCO, utilice su nombre de usuario y contraseña registrados de

CCO Log	jin		×	
Enter	CO Userna	ame and Password		
Usem	ame:	user	_	
Passv	vord:	****		
	ок	Cancel Help		
ссо				SDM se conecta

Cisco.com y comienza a descargar el archivo SDM (por ejemplo, sigv5-SDM-S307.zip) y el archivo pkg de CLI (por ejemplo, IOS-S313-CLI.pkg) en el directorio seleccionado en el paso 7.Una vez descargados ambos archivos, SDM le solicita que envíe el paquete de firma descargado al router.



- 10. Haga clic en No porque el IPS del IOS todavía no se ha configurado en el router.
- 11. Después de que SDM descargue el paquete de firma IOS CLI más reciente, haga clic en la pestaña **Create IPS** para crear la configuración IPS de IOS inicial.
- 12. Si se le solicita que aplique cambios al router, haga clic en Aplicar cambios.
- Haga clic en Iniciar Asistente para reglas IPS. Aparece un cuadro de diálogo para informarle de que SDM necesita establecer una suscripción SDEE al router para recuperar alertas.



14. Click OK.Aparecerá el cuadro de diálogo Authentication Required (Autenticación

uthenticatio	n Required
Enter login de	tails to access level_1 or view_access on
/172.25.90.3	ð:
<u>U</u> ser name:	admin
Password:	****
_	,
Save this p	password in your password list
	OK Cancel
Authentication	n scheme: Integrated Windows

requerida).

15. Ingrese el nombre de usuario y la contraseña que utilizó para SDM para autenticarse en el router y haga clic en **Aceptar**. Aparecerá el cuadro de diálogo Asistente para políticas IPS.

IPS Policies Wizard		×
IPS Wizard	Welcome to the IPS Policies Wizard This wizard helps you to configure the IPS rules for an interface and to specify the	
	location of the configuration and the signature file. This wizard will assist you in configuring the following tasks:	
R	* Select the interface to apply the IPS rule.	
1000	* Select the traffic flow direction that should be inspected by the IPS rules.	
	* Specify the config location and select the category of signatures to be applied to the selected interfaces.	
	To continue, click Next.	
	< Back Next > Finish Cancel	Help

16. Haga clic en Next

(Siguiente).

IPS Policies Wizard			2
IPS Wizard	Select Interfaces Select the interfaces to which the IPS rule should be applied to inbound or outbound	should be applied. Also cho d.	ose whether the rule
	Interface Name	Inbound	Outbound
	GigabitEthernet0/0		
17 A. 10	GigabitEthernet0/1	ج	
	Vlan1		
	Vlan192		
		< Back Next > Finis	Cancel Help

17. En la ventana Interfaces seleccionadas, elija la interfaz y la dirección a la que se aplicará el IPS de IOS y, a continuación, haga clic en **Siguiente** para continuar.

Signature File and Publ	To Mana
Cignoturo Filo	ic key
Specify the signal	ture file you want to use with IOS IPS.
Signature File:	tttp://10.1.1.253/IOS-8313-CLI.pkg
C Get the latest sig	nature file from Cisco.com and save to PC.
Location:	Browse
	Download
Configure Public K	iev
Name:	realm-cisco.pub
Key:	FE3F0C87 89BCB7BB 994AE74C FA9E481D F65 50437722 FFBE85B9 5E4189FF CC189CB9 69C 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5535 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF F3020301 0001
J	
	Signature File

18. En el área Archivo de firma de la ventana Archivo de firma y Clave pública, haga clic en el botón de opción Especificar el archivo de firma que desea utilizar con IOS IPS y, a continuación, haga clic en el botón Archivo de firma (...) para especificar la ubicación del archivo de paquete de firma, que será el directorio especificado en el paso

Specify Signature File	×
C Specify signature file	on flash
File Name on flash:	
Specify signature file	using URL
Protocol:	tttp 💌
tftp://	10.1.1.253/IOS-8313-CLI.pkg
Example:	http://10.10.10.1/IOS-S259-CLI.pkg
C Specify signature file	on the PC
Location:	Browse
ОК	Cancel Help

19. Haga clic en el botón de opción Especificar archivo de firma mediante URL y elija un

protocolo de la lista desplegable Protocolo.**Nota:** Este ejemplo utiliza TFTP para descargar el paquete de firma al router.

- 20. Ingrese la URL para el archivo de firma y haga clic en Aceptar.
- 21. En el área Configure Public Key (Configurar clave pública) de la ventana Signature File (Archivo de firma) y Public Key (Clave pública), introduzca **realm-cisco.pub** en el campo Name (Nombre) y, a continuación, copie esta clave pública y péguela en el campo Key (Clave).

 30820122
 30000609
 2A864886
 F70D0101
 01050003
 82010F00
 3082010A
 02820101

 00C19E93
 A8AF124A
 D6CC7A24
 5097A975
 206BE3A2
 06FBA13F
 6F12CB5B
 4E441F16

 17E630D5
 C02AC252
 912BE27F
 37FDD9C8
 11FC7AF7
 DCD081D9
 43CDABC3
 6007D128

 B199ABCB
 D34ED0F9
 085FADC1
 359C189E
 F30AF10A
 C0EFB624
 7E0764BF
 3E53053E

 5B2146A9
 D7A5EDE3
 0298AF03
 DED7A5B8
 9479039D
 20F30663
 9AC64B93
 C0112A35

 FE3F0C87
 89BCB7BB
 994AE74C
 FA9E481D
 F65875D6
 85EAF974
 6D9CC8E3
 F0B08B85

 50437722
 FFBE85B9
 5E4189FF
 CC189CB9
 69C46F9C
 A84DFBA5
 7A0AF99E
 AD768C36

 006CF498
 079F88F8
 A3B3FB1F
 9FB7B3CB
 5539E1D1
 9693CCBB
 551F78D2
 892356AE

 2F56D826
 8918EF3C
 80CA4F4D
 87BFCA3B
 BFF668E9
 689782A5
 CF31CB6E
 B4B094D3

 F3020301
 0001
 Image and the set the set the set and the set and the set and the set an

Nota: Esta clave publica se puede descargar de Cisco.com en: <u>http://www.cisco.com/pcgi</u> <u>bin/tablebuild.pl/ios-v5sigup</u> (sólo clientes<u>registrados</u>) .

22. Para continuar, haga clic en Next (Siguiente).

O THEAT	Coning Location and Category
A A A A A A A A A A A A A A A A A A A	Config Location Specify the directory path of the IPS configuration files where IOS IPS sub-system stores the signature information and the user-defined modifications. If Cisco IOS IPS fails to contact the specified location, it will retry for a specific timeout period until it successfully contacts the specified location.
	Choose Category Signature categories are subsets of signatures created for routers with different amounts of available memory. The basic category is recommended for routers with less than 128 MB of memory. The advanced category is recommended for routers with 128 MB of memory, or more. Choose Category.

23. En la ventana Config Location and Category , haga clic en el botón **Config Location** (...) para especificar una ubicación en la que se almacenarán la definición de firmas y los archivos de configuración.Aparece el cuadro de diálogo **Agregar ubicación de**

Directory Name:		
C Specify the config locatio	on using URL.	
Protocol:	http 💌	
http://		1
Example:	http://10.10.10.1/ips5	
Number of Retries (1-5):		
Timeout (1-10):	(sec)	

configuración.

24. En el cuadro de diálogo Add Config Location, haga clic en el botón de opción Specify the

config location on this router y luego haga clic en el **botón Directory Name** (...) para localizar el archivo de configuración. Aparece el cuadro de diálogo Elegir carpeta para permitirle seleccionar un directorio existente o crear un nuevo directorio en la memoria flash del router para almacenar la definición de firma y los archivos de

Choose Folder	×
🔄 New Folder	
E 1ash: L ips]
OK Cancel	Help

configuración.

- 25. Haga clic en **Nueva carpeta** situada en la parte superior del cuadro de diálogo si desea crear un nuevo directorio.
- 26. Una vez que seleccione el directorio, haga clic en **Aceptar** para aplicar los cambios y luego haga clic en **Aceptar** para cerrar el cuadro de diálogo Agregar ubicación de configuración.
- 27. En el cuadro de diálogo Asistente para políticas IPS, seleccione la categoría de firma según la cantidad de memoria instalada en el router. Existen dos categorías de firma que puede elegir en SDM: Basic y Advanced.Si el router tiene instalada una DRAM de 128 MB, Cisco recomienda que elija la categoría Basic para evitar fallas de asignación de memoria. Si el router tiene instalada una DRAM de 256 MB o más, puede elegir cualquiera de las categorías.
- 28. Una vez que seleccione una categoría a utilizar, haga clic en Siguiente para continuar con la página de resumen.La página de resumen proporciona una breve descripción de las tareas de configuración inicial de IOS IPS.



29. Haga clic en **Finalizar** en la página de resumen para entregar las configuraciones y el paquete de firma al router.Si la opción de comandos de vista previa está activada en la configuración Preferencias de SDM, SDM muestra el cuadro de diálogo Enviar configuración al router que muestra un resumen de los comandos CLI que SDM envía al router.

ip ips notify SDEE ip ips name sdm_ips_rule interface GigabitEthernet0/1 ip ips sdm_ips_rule in exit ip ips config location flash:/ips/ ip ips signature-category category all retired true exit ◀ The differences between the running configuration and the startup configuration are loc router is turned off.	tas that will be delivered to the router's running configuration.	
ip ips name sdm_ips_rule interface GigabitEthernet0/1 ip ips sdm_ips_rule in exit ip ips config location flash:/ips/ ip ips signature-category category all retired true exit ◀ ■ The differences between the running configuration and the startup configuration are loc router is turned off.		-
interface GigabitEthernet0/1 ip ips sdm_ips_rule in exit ip ips config location flash:/ips/ ip ips signature-category category all retired true exit The differences between the running configuration and the startup configuration are loc router is turned off.	_ips_rule	
Ip ips sdm_ips_rule in exit ip ips config location flash:/ips/ ip ips signature-category category all retired true exit The differences between the running configuration and the startup configuration are loc router is turned off.	Ethernet0/1	
exit ip ips config location flash:/ips/ ip ips signature-category category all retired true exit The differences between the running configuration and the startup configuration are loc router is turned off.	rule in	
ip ips config location frashbips/ ip ips signature-category category all exit exit Ine differences between the running configuration and the startup configuration are loc router is turned off.	Kan Analysinal	
category all retired true exit The differences between the running configuration and the startup configuration are los router is turned off.	alon fiash Jips/	_
retired true exit The differences between the running configuration and the startup configuration are log router is turned off.	alegory	
exit The differences between the running configuration and the startup configuration are log router is turned off.		
The differences between the running configuration and the startup configuration are log router is turned off.		-
The differences between the running configuration and the startup configuration are lo router is turned off.		×
	etween the running configuration and the startup configuration are lost whenever th ff.	e
Save running config. to router's startup config.	config. to router's startup config.	
This operation can take several minutes.	n can take several minutes.	

30. Haga clic en **Entregar** para continuar.Aparece el cuadro de diálogo Estado de entrega de comandos para mostrar el estado de entrega de los

ommands Delivery Status	
Command Delivery Status:	
Preparing commands for delivery Submitting 14 commands, please wait Configuration delivered to router.	1
<u>.</u>	Þ
ок	

comandos._____

31. Cuando los comandos se envían al router, haga clic en **Aceptar** para continuar.El cuadro de diálogo Estado de la configuración de IOS IPS muestra que las firmas se están cargando



32. Cuando se cargan las firmas, SDM muestra la ficha **Editar IPS** con la configuración actual. Verifique qué interfaz y en qué dirección está habilitado el IPS del IOS para verificar la configuración

Cisco Router and	d Security Device M Tools Help	anager (SDM): 172	1.25.90.39					
💰 Home	Corfgue	Monitor	O G	e Search	? Heip			cisco
Tesks	😺 Intrusion Pr	revention Syste	em (IPS)					
	Create IPS Edit	IPS Security Da	shboard IPS Migra	don				
1	E IPS Policie	05	haberbarene au	-	B Enstie	Z Felt (B Disable	e El Disable Al	
Interfaces and Connections	E Clotal Se	es.	anienaces. IAI	internacies 💌	Charles (g con g clean	e Că Disebie ha	
5 2	B) Orderande	strings	Interface Name	IP	Inbound	Outbound	VFR status	Description
975 1	Auto Upd	ate	GigabitEthernet0	172.25.90.39	Disabled	Disabled	on	
Freval and ACL	SEAP CO	nfiguration	OigsbitEthernet0	10.1.1.8	Enabled	Disabled	on	
~	Starget	Value Rating	Vlan1	no IP address	Disabled	Disabled	off	ing international
<u> 100</u>	Th Event	Action Overrides	Vlan192	192.168.1.6	Disabled	Disabled	on	
VPN	E Deput	Action Filters	1					
F an	Ma Circles	Accourting						
	Con Sagnature	18 1	1					
Security Rudit								
3 ² 0								
Rouang								
Sec.								
1								
NHT								
1								
			-					
Inclusion Prevencion								
100 E			IPS Filter Details	C Inbound F	itter C Outb	ound Filter		
Cambo of Service								
Region HAC			A IPS rule is er traffic.	vabled, but there	e is no filter co	infigured for this	rule. IPS will sca	n all Inbound
Rddkionel Tasks								

La consola del router muestra que las firmas se han cargado.

🖉 172.25.90.30 - TuTTY ied *Jan 13 16:41:08 PST: %IPS-6-ENGINE BUILDS_STARTED: 16:41:08 PST Jan 13 2008 *Jan 13 16:41:08 PST: %IPS-6-ENGINE_BUILDING: multi-string - 0 signatures - 1 of 13 engines *Jan 13 16:41:08 PST: %IPS-6-ENGINE_READY: multi-string - build time 8 ms - packets for thi this engine will be scanned *Jan 13 16:41:00 PST: 4IPS-6-ENGINE BUILDING: service-http - 622 signatures - 2 of 13 engines *Jan 13 16:41:33 PST: 4IPS-6-ENGINE_READY: service-http - build time 24892 ms - packets for t this eng ine will be scanned *Jan 13 16:41:33 PST: %IPS-6-ENGINE_BUILDING: string-top - 961 signatures - 3 of 13 engines *Jan 13 16:42:32 PST: %IPS-6-ENGINE_READY: string-top - build time 59424 ms - packets for this engin *Jan 13 16142132 PST: %IPS-6-ENGINE_BUILDING: string-udp - 75 signatures - 4 of 13 engines *Jan 13 16:42:33 PST: %IPS-6-ENGINE_READY: string-udp - build time 948 ms - packets for this engine will be scanned *Jan 13 16:42:33 PST: %IPS-6-ENGINE_BUILDING: state - 28 signatures - 5 of 13 engines *Jan 13 16:42:33 PST: %IPS-6-ENGINE_READY: state - build time 104 ms - packets for this engine will be scanned "Jan 13 16:42:33 PST: %IPS-6-ENGINE BUILDING: atomic-ip = 275 signatures = 6 of 13 engines "Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: atomic-ip - build time 532 ms - packets for this engine w iii be scanned *Jan 13 16:42:34 PST: \IPS-6-ENGINE_DUILDING: string-icmp - 3 signatures - 7 of 13 engines *Jan 13 16:42:34 PST: \IPS-6-ENGINE_READY: string-icmp - build time 32 ms - packets for this engine vili be scanned *Jan 13 16:42:34 PST: \IPS-6-ENGINE_BUILDING: service-ftp - 3 signatures - 8 of 13 engines *Jan 13 16:42:34 PST: \IPS-6-ENGINE_READY: service-rpc - build time 200 ms - packets for this engine will be scanned *Jan 13 16:42:34 PST: \IPS-6-ENGINE_BUILDING: service-rpc - build time 200 ms - packets for this engine will be scanned *Jan 13 16:42:34 PST: \IPS-6-ENGINE_BUILDING: service-dns - 30 signatures - 10 of 13 engines *Jan 13 16:42:34 PST: \IPS-6-ENGINE_READY: service-dns - build time 36 ms - packets for this engine vill be scanned will be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: normalizer - 9 signatures - 11 of 13 engines *Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: normalizer - build time 0 ms - packets for this engine wi ll be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures - 12 of 13 engine *Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms - packets for thi s engine will be scanned *Jan 13 16:42:34 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 26 signatures - 13 of 13 engines *Jan 13 16:42:34 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 36 ms - packets for this engin w111 be scanned Jan 13 16:42:34 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 86304 ms

33. Utilice el comando show ip ips Signature count para verificar que las firmas se carguen

```
COrrectamente.
router#show ip ips signatures count
Cisco SDF release version S313.0
Trend SDF release version V0.0
|
snip
|
Total Signatures: 2158
Total Enabled Signatures: 829
Total Retired Signatures: 1572
Total Compiled Signatures: 580
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
```

El aprovisionamiento inicial de IOS IPS con SDM 2.5 ha finalizado.

 Verifique los números de firma con SDM como se muestra en esta imagen.

🕵 Cisco Router ar	d Security Device Manager (SDM): 1	72.25.90.39							_0
File Edit View	Tools Help								
💰 Home	Configure 🔯 Monitor	Refresh	s	ave	Q. Search	? Help		•	cisco
Tasks	💌 Intrusion Prevention Sys	item (IPS)							
	Create IPS Edit IPS Security D	ashboard	IPS Mi	gration)				_
	PS Policies	Dig Imp	ort = v	/ierw bry:	AJ Signa	eures V Criteria _NIA *	Total[2158]	Compiled[584	1
Connections	Global Settings Relect Al Q. Add - 12 Edt C Engle Q Degle Q Forder								1
3	etebqU ctuA 🖏	England		Ship	Secon	Nerra	Action	Country	Frank I A
Freval and ACL	8 SEAP Configuration	00000		9423	Source 1	Back Door Psychward	produce-site	high	65
<u></u>	Se Target Value Rating			9423	0	Back Door Psychward	produce-aler	high	100
UPN	Event Action Overrides			5343	0	Apache Host Header Cross Ste	produce-aler	high	100
200	Fit Event Action Filters			3122	0	SMTP EXPN root Recon	produce-aler	low	85
	Signatures	1 o		5099	0	MSN Messenger Webcam Duffe	produce-aler	high	00
Security Hoot	B	•		5537	0	ICO Client DNS Request	produce-aler	informational	100
000	Attack	•		3316	0	Project1 DOS	produce-aler	high	75
Routing	DoS	0		11003	0	Gtella File Request	produce-aler	low	100
10	Reconnaissance Reconnaissance Reconnaissance	•		\$195	1	Red Hat Stronghold Recon attai	produce-aler	low/	100
NRT	3- Instant Messaging	•		\$196	0	Red Hat Stronghold Recon attac	produce-aler	low/	100
121	Adware/Spyware Original Adware/Spyware Original Adware/Spyware	•		5773	1	Simple FHP Blog Unauthorized F	produce-aler	low	70
et a se la constanti de la const	B- DDoS	•		5773	0	Simple FHP Blog Unauthorized F	produce-aler	low	65
	B- Network Services Web Server	•		5411	0	Linksys Http DoS	produce-aler	high	85
104	B-Q P2P	•		12019	0	SideFind Activity	produce-aler	low	65
Quality of Service	el-enall el-enall	•		5070	0	vWWV moscies.dll Access	produce-aler	nedun	100
200	🗄 🦾 Releases	0		3169	0	FTP SITE EXEC for	produce-aler	high	85
NRC		0		5605	0	Windows Account Locked	produce-aler	informational	85
154		4							1
Roditional Tasks						Apply Changes Discard Ch	81025		
PS Signatures							16:53:0	2 PST Sun Jan 1	3 2008

Información Relacionada

- <u>Cisco IOS IPS en Cisco.com</u>
- Paquete de firma IPS de Cisco IOS
- <u>Archivos de firma IPS de Cisco IOS para SDM</u>
- Introducción a Cisco IOS IPS con formato de firma 5.x
- Guía de Configuración de Cisco IOS IPS
- <u>Visor de eventos de Cisco IDS</u>
- Soporte Técnico y Documentación Cisco Systems