# Configuración del router y SDM y de la CLI de Cisco IOS en Cisco IOS IPS

### Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configurar Habilitar Cisco IOS IPS con un SDF predeterminado de fábrica Agregar firmas adicionales después de habilitar el SDF predeterminado Seleccionar firmas y trabajar con categorías de firmas Actualizar firmas para archivos SDF predeterminados Información Relacionada

### **Introducción**

En Cisco Router and Security Device Manager (SDM) 2.2, la configuración de Cisco IOS<sup>®</sup> IPS se integra en la aplicación SDM. Ya no es necesario que inicie una ventana independiente para configurar Cisco IOS IPS.

En Cisco SDM 2.2, un nuevo asistente de configuración IPS le guiará a través de los pasos necesarios para habilitar Cisco IOS IPS en el router. Además, todavía puede utilizar las opciones de configuración avanzadas para habilitar, inhabilitar y ajustar Cisco IOS IPS con Cisco SDM 2.2.

Cisco recomienda ejecutar Cisco IOS IPS con los archivos de definición de firma (SDF) preconfigurados: attack-drop.sdf, 128MB.sdf y 256MB.sdf. Estos archivos se crean para routers con diferentes cantidades de memoria. Los archivos se agrupan con Cisco SDM, que recomienda SDF cuando active por primera vez Cisco IOS IPS en un router. Estos archivos también se pueden descargar desde <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u> (sólo clientes registrados).

El proceso para habilitar los SDF predeterminados se detalla en <u>Habilitar Cisco IOS IPS con un</u> <u>SDF Predeterminado de Fábrica</u>. Cuando los SDF predeterminados no son suficientes o desea agregar nuevas firmas, puede utilizar el procedimiento descrito en <u>Agregar firmas adicionales</u> <u>después de Habilitar el SDF predeterminado</u>.

## **Prerequisites**

### **Requirements**

Se necesita Java Runtime Environment (JRE) versión 1.4.2 o posterior para utilizar Cisco SDM 2.2. Un archivo de firma recomendado y optimizado por Cisco (basado en DRAM) se incluye con Cisco SDM (cargado en la memoria flash del router con Cisco SDM).

#### **Componentes Utilizados**

La información de este documento se basa en el router y el administrador de dispositivos de seguridad (SDM) de Cisco 2.2.

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.

### <u>Configurar</u>

#### Habilitar Cisco IOS IPS con un SDF predeterminado de fábrica

#### Procedimiento CLI

Complete este procedimiento para utilizar la CLI para configurar un Cisco 1800 Series Router con Cisco IOS IPS para cargar 128MB.sdf en la memoria flash del router.

- Configure el router para habilitar la notificación de eventos de intercambio de dispositivos de seguridad (SDEE).
   vourname#conf t
- 2. Ingrese los comandos de configuración (uno por línea) y luego presione Cntl+Z para finalizar. yourname(config)#ip ips notify sdee
- 3. Cree un nombre de regla IPS que se utilice para asociar a interfaces. yourname(config)#ip ips name myips
- 4. Configure un comando de ubicación IPS para especificar de qué archivo leerá las firmas el sistema IPS de Cisco IOS.Este ejemplo utiliza el archivo en flash: 128 MB.sdf. La parte de la URL de ubicación de este comando puede ser cualquier URL válida que utilice flash, disco o protocolos a través de FTP, HTTP, HTTPS, RTP, SCP y TFTP para señalar los archivos. yourname(config)#ip ips sdf location flash:128MB.sdf

**Nota:** Debe habilitar el comando **terminal monitor** si configura el router a través de una sesión Telnet o no verá los mensajes SDEE cuando se construya el motor de firma.

 Active IPS en la interfaz donde desea habilitar Cisco IOS IPS para analizar el tráfico. En este caso, habilitamos en ambas direcciones en la interfaz fastEthernet 0.
 yourname(config)#interface fastEthernet 0

yourname(config-if)#ip ips myips in

```
*Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS:
      SDF loaded successfully from opacl
*Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS:
       SDF loaded successfully from flash:128MB.sdf
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
       OTHER - 4 signatures - 1 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_READY:
       OTHER - 0 ms - packets for this engines will be scanned
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
       MULTI-STRING - 0 signatures - 2 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED:
       MULTI-STRING - there are no new signature definitions for this engine
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
       STRING.ICMP - 1 signatures - 3 of 15 engines
*Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
       STRING.ICMP - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING:
       STRING.UDP - 17 signatures - 4 of15 engines
*Oct 26 00:32:31.393: %IPS-6-ENGINE_READY:
       STRING.UDP - 448 ms - packets for this engine will be scanned
*Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING:
       STRING.TCP - 58 signatures - 5 of 15 engines
*Oct 26 00:32:33.641: %IPS-6-ENGINE_READY:
       STRING.TCP - 2248 ms - packets for this engine will be scanned
*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING:
       SERVICE.FTP - 3 signatures - 6 of 15 engines
*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY:
       SERVICE.FTP - 16 ms - packets for this engine will be scanned
*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING:
       SERVICE.SMTP - 2 signatures - 7 of 15 engines
*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY:
       SERVICE.SMTP - 28 ms - packets for this engine will be scanned
*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
       SERVICE.RPC - 29 signatures - 8 f 15 engines
*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
       SERVICE.RPC - 92 ms - packets for this engine will be scanned
*Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING:
       SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 00:32:33.801: %IPS-6-ENGINE_READY:
       SERVICE.DNS - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING:
       SERVICE.HTTP - 132 signatures - 10 of 15 engines
*Oct 26 00:32:44.505: %IPS-6-ENGINE_READY:
       SERVICE.HTTP - 10704 ms - packets for this engine will be scanned
*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING:
       ATOMIC.TCP - 11 signatures - 11 of 15 engines
*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY:
       ATOMIC.TCP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING:
       ATOMIC.UDP - 9 signatures - 12 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
       ATOMIC.UDP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
       ATOMIC.ICMP - 0 signatures - 13 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED:
       ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
       ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
       ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
       ATOMIC.L3.IP - 5 signatures - 15 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
       ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned
```

yourname(config-if)#ip ips myips out yourname(config-if)#ip virtual-reassembly

La primera vez que se aplica una regla IPS a una interfaz, Cisco IOS IPS inicia las firmas generadas desde el archivo especificado por el comando de ubicaciones SDF. Los mensajes SDEE se registran en la consola y se envían al servidor syslog si están configurados. Los mensajes SDEE con *<number>* de *<number>* motores indican el proceso de construcción del motor de firma. Por último, cuando los dos números son iguales, todos los motores están construidos.**Nota:** El reensamblado virtual IP es una función de interfaz que (cuando está activada) reensambla automáticamente los paquetes fragmentados que entran en el router a través de esa interfaz. Cisco recomienda que habilite ip virtual-assembly en todas las interfaces donde el tráfico entra en el router. En el ejemplo anterior, además de activar "ip virtual-assembly" en la interfaz fastEthernet 0, lo configuramos también en la interfaz interna VLAN 1.

#### **Procedimiento SDM 2.2**

Complete este procedimiento para utilizar Cisco SDM 2.2 para configurar un Cisco 1800 Series Router con Cisco IOS IPS.

1. En la aplicación SDM, haga clic en **Configurar** y, a continuación, haga clic en **Prevención de** 

🚯 Home 😝	🖧 Configure 😥 Monitor 🗣 🚽 🧣 Monitor	Cisco System
Tesks [	Intrusion Prevention System (IPS)	
Prestaces and Convectors	Create IPS Edit IPS The IPS rule configuration witzed configures IPS rules on an interface and also specifies the location of the SDF (signature definition file).	
Presult and RCL	Use Case Scenario Network based Intrusion Prevention	
Security Hudi age Noting		
ाळान Cuality of Service दिक्रून NHC	Launch IPS Rule Wizard.	
intrusion Prevention By	ystem (IP 6)	02:45:58 UTC Mon Mar 13 2008

intrusiones.

2. Haga clic en la ficha Create IPS y, a continuación, haga clic en Launch IPS Rule Wizard.Cisco SDM requiere la notificación de eventos IPS a través de SDEE para configurar la función Cisco IOS IPS. De forma predeterminada, la notificación SDEE no está habilitada. Cisco SDM le solicita que active la notificación de eventos IPS a través de SDEE, como se



muestra en esta imagen:

3. Click OK.Aparecerá la ventana Welcome to the IPS Policies Wizard (Bienvenido al Asistente de políticas IPS) del cuadro de diálogo IPS Policies Wizard (Asistente de políticas

IPS Policies Wizard		×
IPS Wizard	Welcome to the IPS Policies Wizard	
	The IPS rule configuration wizard configures IPS rules on an interface and also specifies the location of the SDF (signature definition file). You must specify the direction of the traffic that should be scanned. If you do not want all traffic to be scanned, you should specify the interesting traffic to be scanned. The router loads the SDF and starts scanning the interesting traffic.	
	This wizard will assist you in configuring the following tasks	
130	* Select the interface to apply the IPS rule.	
10125	* Select the traffic flow direction that should be inspected by the IPS rules.	
	* Specify the location of the SDF to be used by the router.	
	To continue, click Next.	
	Back Next> Finish Cancel	Help

4. Haga clic en Next (Siguiente). Aparecerá la ventana Seleccionar interfaces.

PS Policies Wizard			Į
IPS Wizard	Select Interfaces Select the interfaces to which the IPS rule s should be applied to inbound or outbound.	should be applied. Also cho	ose whether the rule
	Interface Name	Inbound	Outbound
	BRIO		
distrational Transfer	FastEthernet0	<b>v</b>	v 🖓
		< Back Next > Finis	Cancel Help

- 5. Elija las interfaces para las que desea habilitar IPS, y haga clic en la casilla de verificación **Entrante** o **Saliente** para indicar la dirección de esa interfaz.**Nota:** Cisco recomienda que habilite tanto las direcciones entrantes como las salientes cuando habilite IPS en una interfaz.
- 6. Haga clic en Next (Siguiente). Aparecerá la ventana Ubicaciones de SDF.
- 7. Haga clic en **Agregar** para configurar una ubicación SDF.Aparecerá el cuadro de diálogo Agregar una ubicación de

IPS Wizard	SDF Locations Specify the locations from w Cisco IOS IPS. If Cisco IOS locations in order until it su	thich the SDF (signature definition file) IPS fails to load the SDF from the first ccessfully loads the SDF file.	) should be loaded by th location, it tries the
D.	SDF Locations		Add
11			Delete
10	Concernation of the second		Move U
1225	Add a Signature Locat     Specify SDE onfacts	ion 🔛	Move Do
	File Name onflash:	256MB.sdf	
1 1 1 <b>1</b> 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	C Specify SDF using U	RL:	
	Protocol	http://www.www.www.	cation, it can
	http://		
	Econole: Fautosave		
FREEMAN	ок	Cancel Help	
			-
		< Back Next >	inish Cancel

- 8. Haga clic en el botón de opción **Especificar SDF en flash** y elija 256MB.sdf en la lista desplegable **Nombre de archivo en flash**.
- 9. Haga clic en la casilla de verificación **Autosave** y haga clic en **OK**.**Nota:** La opción Autosave guarda automáticamente el archivo de firma cuando hay un cambio de firma.La ventana Ubicaciones de SDF muestra la nueva ubicación de



a: Puede agregar ubicaciones de firma adicionales para designar una copia de seguridad.

- Haga clic en la casilla de verificación Usar firmas integradas (como copia de seguridad).Nota: Cisco recomienda que no utilice la opción de firma integrada a menos que haya especificado una o más ubicaciones.
- 11. Haga clic en **Next** para continuar.Aparecerá la ventana Resumen.



12. Haga clic en Finish (Finalizar).El cuadro de diálogo Estado de entrega de comandos muestra el estado a medida que el motor IPS compila todas las

Commands Delivery Status	
Command Delivery Status:	
Preparing commands for delivery Submitting 10 commands, please wait Configuration delivered to router.	<u>^</u>
<u>&lt;</u>	× ×
ОК	

firmas.

13. Una vez que el proceso haya finalizado, haga clic en **Aceptar**.El cuadro de diálogo Estado de compilación de firmas muestra la información de compilación de

igna	ture Compilation St	atus		1			
IPS signature engines are built and are ready to scan packets.							
No.	Engine	Status	No of Signatures	1			
2	MULTI-STRING	Skipped	No New Signatures				
3	STRING.ICMP	Loaded	1				
4	STRING.UDP	✓ Loaded	17				
5	STRING.TCP	✓ Loaded	58				
6	SERVICE.FTP	✓ Loaded	3				
7	SERVICE.SMTP	✓ Loaded	2				
8	SERVICE.RPC	✓ Loaded	29				
9	SERVICE.DNS	Loaded	31				
10	SERVICE.HTTP	✓ Loaded	132				
11	ATOMIC.TCP	Loaded	11				
12	ATOMIC.UDP	✓ Loaded	9				
13	ATOMIC.ICMP	Skipped	No New Signatures				
14	ATOMIC.IPOPTIONS	✓ Loaded	1				
15	ATOMIC.L3.IP	🖌 Loaded	5				
4				•			
		Close	1				

firmas.

Esta información muestra qué

motores se han compilado y el número de firmas en ese motor. Para los motores que muestran *Omitido* en la columna de estado, no hay ninguna firma cargada para ese motor.

- 14. Haga clic en **Cerrar** para cerrar el cuadro de diálogo Estado de compilación de firmas.
- 15. Para verificar qué firmas están cargadas actualmente en el router, haga clic en **Configurar** y luego haga clic en **Prevención de intrusiones**.
- 16. Haga clic en la ficha **Edit IPS** y, a continuación, haga clic en **Firmas**.La lista de firmas IPS aparece en la ventana

Firmas.								
😫 Cisco Router a	nd Security Device Manager (SDM	): 192.168.1	8.1					202
File Edit View	Tools Help						C.c.	en Evennuer
🔥 Home	🚳 Configure [ Monitor	Retresh	Save	Q Search	9 Help		CI8	
Tasks	😝 Intrusion Prevention Syst	tem (IPS)						
	Create IPS Edit IPS							
Interfaces and	IPS Policies	Dig Import	• Select I	W. Al Sig	natures • Oriteria: -NIA	•	Te	tal[303]
comectors	Global Settings	Select /	Al & Ad	t = 📑 Edit	1 Delete 🔘 Enable 🔾 Dis	sable	6	Details
Second and Mr.	SDEE Messages	Enabled	SgD	SubSig ID	Name	Action	Sevently	Eng.*
	D Al Categories		3157	0	FTP PASY Port Spoof	alarm	high	SERVI
<u> 3</u>	B- OS	0	11002	0	Gnutella Server Reply	alarm	low	STRIN
	B- Service	0	5088	0	vWWV Akopia MinVend access	alarm	low	SERVI
60	B L2/L3/L4 Protocol	0	3153	0	FTP Improper Address	alarm	medium	SERVI
Security Audit	B- Releases	•	3129	0	Mmail Virus C Variant File Attac	alarm drop reset	medium	SERVI
Routing		0	5084	1	vWWW Alibaba attack 2	alarm	low	SERVI
51.		0	5084	0	vWWV Albaba attack 2	alarm	low	SERVI
100		0	11212	0	Yahoo Messenger Through HT	olarm	informational	SERVI
		0	5080	0	vWWV IEM WebSphere access	alarm	low	SERVI
<b>I</b>		0	3218	0	vWWV SGI wrap bug	alarm	medium	SERVI
Intrusion Prevention		0	5052	0	vWWV VTI Open attempt	alarm	medium	SERVI
· @		0	9535	0	Back Door TensScout	olarm	high	STRIN
Quality of Service		0	6062	1	<b>CNS Authors Request</b>	alarm	low	SERVE
•						- Companya - Companya		
NRC					Apply Changes Discard Cha	1915		
IPS Signatures						03:10:2	5 UTC Mon Mar 1	3 2006

#### **Procedimiento CLI**

No hay ningún comando CLI disponible para crear firmas o leer información de firma del archivo IOS-Sxxx.zip distribuido. Cisco recomienda que utilice SDM o Management Center for IPS Sensors para administrar las firmas en los sistemas IPS de Cisco IOS.

Para los clientes que ya tienen un archivo de firma preparado y desean fusionar este archivo con el SDF que se ejecuta en un sistema IPS de Cisco IOS, puede utilizar este comando:

```
yourname#show running-config | include ip ips sdf
ip ips sdf location flash:128MB.sdf
yourname#
```

El archivo de firma definido por el comando de ubicación de firma es donde el router carga los archivos de firmas cuando se recarga o cuando se reconfigura el IPS del IOS del router. Para que el proceso de fusión sea exitoso, también se debe actualizar el archivo definido por el comando de ubicación del archivo de firma.

1. Utilice el comando show para verificar las ubicaciones de firma configuradas actualmente.El resultado muestra las ubicaciones de firma configuradas. Este comando muestra desde dónde se cargan las firmas actuales en ejecución.

yourname#show ip ips signatures

Builtin signatures are configured

Las firmas se cargaron por última vez desde flash:128MB.sdfVersión S128.0 de Cisco SDFVersión V0.0 de Trend SDF

2. Utilice el comando copy <url> ips-sdf, junto con la información del paso anterior, para fusionar archivos de firma.

```
yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
Loading mysignatures.xml from 10.10.10.5 (via Vlan1): !
[OK - 1612 bytes]
*Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport
4715
*Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from
       tftp://10.10.10.5/mysignatures.xml
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature
       definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures -
       2 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are
       no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures -
       3 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are
       no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures -
       4 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are
       no new signature definitions for this engine
*Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures -
       5 of 15 engines
*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False -
       This parameter is not supported
```

```
*Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this
```

```
engine will be scanned
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures -
       6 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are
      no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE BUILDING: SERVICE.SMTP - 2 signatures -
       7 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures -
       8 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures -
       9 of 15 engines
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures -
       10 of 15 engines
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
       11 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures -
       12 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures -
       13 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are
      no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures -
       14 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are
       no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures -
       15 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are
       no new signature definitions for this engine
```

yourname#

Después de ejecutar el comando **copy**, el router carga el archivo de firma en la memoria y luego genera los motores de firma. En la salida del mensaje SDEE de la consola, se muestra el estado de construcción de cada motor de firma.%IPS-6-ENGINE\_BUILD\_SKIPPED indica que no hay nuevas firmas para este motor.%IPS-6-ENGINE\_READY indica que hay nuevas firmas y que el motor está listo. Como antes, el mensaje "15 de 15 motores" indica que todos los motores han sido construidos.IPS-7-UNSUPPORTED\_PARAM indica que un parámetro determinado no es soportado por Cisco IOS IPS. Por ejemplo, CapturePacket y ResetAfterIdle.**Nota:** Estos mensajes son sólo para información y no afectarán a la capacidad o el rendimiento de la firma IPS de Cisco IOS. Estos mensajes de registro se pueden desactivar estableciendo el nivel de registro más alto que la depuración (nivel 7).

 Actualice el SDF definido por el comando de ubicación de firma, de modo que cuando el router se recargue, tenga la firma combinada configurada con firmas actualizadas. Este ejemplo muestra la diferencia de tamaño de archivo después de guardar la firma combinada en el archivo flash 128MB.sdf.

yourname#**show flash:** 

-#- --length-- ----date/time----- path

4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf

yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
 -#- --length-- ----date/time----- path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf

Advertencia: El nuevo archivo 128MB.sdf ahora contiene firmas combinadas con el cliente. El contenido es diferente del archivo 128MB.sdf predeterminado de Cisco. Cisco recomienda que cambie este archivo a un nombre diferente para evitar confusiones. Si se cambia el nombre, también se debe cambiar el comando de ubicación de firma.

#### Procedimiento SDM 2.2

Después de que Cisco IOS IPS se haya habilitado, se pueden agregar nuevas firmas al router que ejecuta un conjunto de firmas con la función de importación de Cisco SDM. Complete estos pasos para importar nuevas firmas:

- 1. Elija los SDF predeterminados o el archivo de actualización IOS-Sxxx.zip para importar firmas adicionales.
- 2. Haga clic en Configurar y, a continuación, haga clic en Prevención de intrusiones.
- 3. Haga clic en la ficha Edit IPS y, a continuación, haga clic en

#### Import. Intrusion Prevention System (IPS) Create IPS Edit IPS IPS Policies Minport \* Select by: All Signatures \* Criteria: --N/A-- \* Total[303] Global Settings d • 🕼 Edit 🗊 Delete 📀 Enable 🕥 Disable From PC C Details SDEE Messages From router flash SubSig ID Name Action Severity Erx \* UNIT Signatures \* e. FTP PASV Port Spoot All Categories 11002 0 **Grutella Server Reply** STRIN 🖻 🥘 OS alarm low 0 E- Attack 5088 0 vWWV Akopia Min/Vend access alarm SERVI low 0 E Gervice E L2/L3/L4 Protocol 3153 0 FTP Improper Address SERVI 0 alarm medium E C Releases alarm medium 3129 0 Mimail Virus C Variant File Attac drop SERVI 0 reset 5084 vWWW Alibaba attack 2 SERVI 1 alarm low 0 5084 0 rWWW Alibaba attack 2 SERVI alarm low 0 11212 0 Yahoo Messenger Through HT' alarm informational SERVI 0 5080 0 vWWV IBM WebSphere access alarm SERVI 0 low 3218 0 vWWV SGI wrap bug alarm medium SERVI 0 5052 0 vWWW VTI Open attempt medium SERVI 0 alarm 9535 0 Back Door TansScout alarm high STRIN 0 6062 **DNS Authors Request** SERVI 1 alarm low 0 • . Apply Changes Discard Changes 03:11:25 UTC Mon Mar 13 2006

- 4. Elija Desde PC en la lista desplegable Importar.
- 5. Seleccione el archivo desde el que desea importar las

Look jn: 🗀 CCO:	Sigs	
105-5208.zip 105-5209.zip 105-5210.zip 105-5211.zip 105-5212.zip 105-5213.zip	105-5214.zip 105-5215.zip 105-5216.zip	
<		

### firmas.

En este ejemplo se utiliza la última

actualización descargada de Cisco.com y guardada en el disco duro del equipo local.

6. Haga clic en **Abrir**. **Advertencia**: Debido a la restricción de memoria, sólo se puede agregar un número limitado de firmas nuevas a la parte superior de las firmas que ya se han implementado. Si se seleccionan demasiadas firmas, es posible que el router no pueda cargar todas las firmas nuevas debido a la falta de memoria. Cuando se complete la carga del archivo de firma, aparecerá el cuadro de diálogo Importación de

pr.			
All Categories	-		Sele
E- Attack	Name	Deployed	Import
E Service	KaZaA v2 UDP Client Probe	Yes	V
General Service	KaZaA v2 UDP Client Probe	Yes	V
-DNS	KaZaA v2 UDP Client Probe	Yes	V
Finger	Gnutella Client Request	Yes	V
FTP	Gnutella Server Reply	Yes	¥
Ident	Gtella File Request	No	Г
IMAP	Bearshare File Request	No	Г
NNTP	KaZaA Client Activity	Yes	F
LPR	Gnucleus File Request	Yes	F
NTP	Limewire File Request	No	Г
POP	Morpheus File Request	No	Г
R-Services	Phex File Request	No	
SMTP	Swapper File Request	No	Г
SNMP	XoloX File Request	No	
	GTK-Grutella File Request	Yes	2
File Sharing	Mutelia File Request	No	Г
	Hotine Client Login	No	5
TETP	Hotine File Transfer	No	
p2: ferge The specified signatures will Replace	be merged with the signatures already de	ployed on the rou	ter.

#### IPS.

- 7. Desplácese por la vista de árbol izquierda y haga clic en la casilla de verificación **Importar** junto a las firmas que desea importar.
- 8. Haga clic en el botón de opción Combinar y, a continuación, haga clic en Aceptar. Nota: La

opción Reemplazar reemplaza el conjunto de firmas actual en el router con las firmas que seleccione para importar.Cuando haga clic en Aceptar, la aplicación Cisco SDM enviará las



firmas al router.

Durante la compilación y la carga de firmas se produce un uso elevado de la CPU. Después de que Cisco IOS IPS esté habilitado en la interfaz, el archivo de firma comienza a cargarse. El router tarda unos cinco minutos en cargar el SDF. Puede intentar utilizar el comando **show process cpu** para ver la utilización de la CPU desde la CLI del software Cisco IOS. Sin embargo, no intente utilizar comandos adicionales ni cargar otros SDF mientras el router carga el SDF. Esto puede hacer que el proceso de compilación de la firma tarde más en completarse (ya que la utilización de la CPU se acerca al 100% en el momento de cargar el SDF). Es posible que deba examinar la lista de firmas y habilitarlas si no están en estado *habilitado*.El número total de firma ha aumentado a 519. Este número incluye todas las firmas disponibles en el archivo IOS-S193.zip que pertenecen a la subcategoría Compartir archivos.

💪 IPS Policies	Q	B Impo	nt =	Select b	y: Al Sig	natures 💌 Criteria:N/A	•	To	tal[305]
🐼 Global Settings	E	R Selec	t All	4 Add	i • 🗃 Edit	1 Delete 🔘 Enable 🥥 Dis	able	0	Details
SDEE Messages	Er	abled		Sin D	SubSin D	Name	Action	Severity	En/
Signatures	».	(A)		3157	0	FTP PASV Port Spoof	alarm	high	SERVI
All Categories				11002	0	Grudella Server Recky	alarm	low.	STRN
B- Attack		0	_	6000	0	MANN Akonia Mini/and access	alarm	low	CEPLA
🕀 🦲 Service		0		0000	0	www.Augaa.Minivend.access	asarm	low	SERVI
L2/L3/L4 Protocol		0		3153	0	FTP Improper Address	alarm	medium	SERVI
E - Releases		•		3129	0	Mimail Virus C Variant File Attac	alarm drop reset	medium	SERVI
		0		5084	1	VWW Albaba attack 2	alarm	low	SERVI
		0		5084	0	vWWV Alibaba attack 2	alarm	low	SERV1
		0		11212	0	Yahoo Messenger Through HT	alarm	informational	SERV1
		0		5080	0	WWW IBM WebSphere access	alarm	low	SERVI
		0		3218	0	VWW/SGI wrap bug	alarm	medium	SERV1
		0		5052	0	WWW VTI Open attempt	alarm	medium	SERVI
		0		9535	0	Back Door TansScout	alarm	high	STRIN
		0		6062	1	DNS Authors Request	alarm	low	SERV1
		1						· · ·	

Para obtener información sobre temas más avanzados sobre cómo utilizar Cisco SDM para administrar la función Cisco IOS IPS, consulte la documentación de Cisco SDM en esta URL:

#### Seleccionar firmas y trabajar con categorías de firmas

Para determinar cómo seleccionar de forma efectiva las firmas correctas para una red, debe saber algunas cosas sobre la red que está protegiendo. La información actualizada de la categoría de firma en Cisco SDM 2.2 y posteriores ayuda a los clientes a seleccionar el conjunto correcto de firmas para proteger la red.

La categoría es una forma de agrupar firmas. Ayuda a restringir la selección de firmas a un subconjunto de firmas que son relevantes entre sí. Una firma sólo puede pertenecer a una categoría o puede pertenecer a varias categorías.

Estas son las cinco categorías principales:

- SO: categorización de firmas basada en el sistema de operaciones
- Ataque: categorización de firma basada en ataques
- Servicio: categorización de firma basada en servicios
- Protocolo de capa 2-4: categorización de firma basada en protocolo
- Versiones: categorización de firmas basada en versiones

Cada una de estas categorías se divide en subcategorías.

Por ejemplo, considere una red doméstica con una conexión de banda ancha a Internet y un túnel VPN a la red corporativa. El router de banda ancha tiene Cisco IOS Firewall activado en la conexión abierta (no VPN) a Internet para evitar que cualquier conexión se origine desde Internet y se conecte a la red doméstica. Se permite todo el tráfico que se origina desde la red doméstica a Internet. Suponga que el usuario utiliza un PC basado en Windows y aplicaciones como HTTP (exploración web) y correo electrónico.

El firewall se puede configurar de modo que sólo las aplicaciones que necesita el usuario puedan fluir a través del router. Esto controlará el flujo de tráfico no deseado y potencialmente malo que puede propagarse por la red. Tenga en cuenta que el usuario de inicio no necesita ni utiliza un servicio específico. Si se permite que ese servicio fluya a través del firewall, existe un agujero potencial que un ataque puede utilizar para fluir por la red. Las prácticas recomendadas solo permiten los servicios necesarios. Ahora, es más fácil seleccionar qué firmas se van a habilitar. Debe activar las firmas sólo para los servicios que permita que fluyan a través del firewall. En este ejemplo, los servicios incluyen correo electrónico y HTTP. Cisco SDM simplifica esta configuración.

Para utilizar la categoría para seleccionar las firmas requeridas, elija **Service > HTTP**, y habilite todas las firmas. Este proceso de selección también funciona en el diálogo de importación de firmas, donde puede seleccionar todas las firmas HTTP e importarlas al router.

Las categorías adicionales que deben seleccionarse incluyen DNS, NETBIOS/SMB, HTTPS y SMTP.

#### Actualizar firmas para archivos SDF predeterminados

Los tres SDFs por construcción (attack-drop.dsf, 128MB.sdf y 256MB.sdf) se encuentran actualmente disponibles en Cisco.com en <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u> (<u>sólo</u> clientes <u>registrados</u>). Las versiones más recientes de estos archivos se publicarán tan pronto como estén disponibles. Para actualizar los routers que ejecutan Cisco IOS IPS con estos SDF predeterminados, vaya al sitio web y descargue las últimas versiones de estos archivos.

#### Procedimiento CLI

1. Copie los archivos descargados en la ubicación desde la que se ha configurado el router para cargar estos archivos. Para averiguar dónde está configurado actualmente el router, utilice el comando **show running-config | en el** comando **ip ips sdf**.

Router#show running-config | in ip ips sdf ip ips sdf location flash://256MB.sdf autosave En este ejemplo, el router utiliza 256MB.sdf en la memoria flash. El archivo se actualiza cuando copia el nuevo archivo descargado 256MB.sdf en la memoria flash del router.

2. Recargue el subsistema IPS de Cisco IOS para ejecutar los nuevos archivos. Hay dos maneras de recargar Cisco IOS IPS: recargue el router o vuelva a configurar Cisco IOS IPS para activar el subsistema IOS IPS para recargar las firmas. Para reconfigurar Cisco IOS IPS, quite todas las reglas IPS de las interfaces configuradas y luego vuelva a aplicar las reglas IPS a las interfaces. Esto activará la recarga del sistema IPS de Cisco IOS.

#### Procedimiento SDM 2.2

Complete estos pasos para actualizar los SDF predeterminados en el router:

- 1. Haga clic en **Configurar** y, a continuación, haga clic en **Prevención de intrusiones**.
- 2. Haga clic en la ficha Edit IPS y, a continuación, haga clic en Global Settings

IPS Policies			ਭ
3 Global Settings		Item Name	litern Value
SDEE Messages		Syslog	Enabled
A Cinnaturae		SDEE	Enabled
8 orginatores	•	SDEE Alerts	200
		SDEE Subscription	1
		Engine Options	
		Fail Closed	Disabled
		Use Built-in Signatures (as backup)	Enabled
		Deny Action on IPS interface	Disabled
		Shun Event	20
		Configured SDF Locations: 4 Add 2	Edit 🏦 Delete 🚖 Move Up 🖶 Move Down 🔊 Reload
		flashuïsdmips.sdf	
		flash://128MB.sdf (autosave)	

La parte superior de la interfaz de usuario muestra la configuración global. La mitad inferior de la interfaz de usuario muestra las ubicaciones SDF configuradas actualmente. En este caso, se configura el archivo 256MB.sdf de la memoria flash.

3. Elija Administración de archivos en el menú Archivo. Aparecerá el cuadro de diálogo

#### Administración de

-manash:	Name	Size(bytes)	Time Modified
	128MB.sdf	504630	08/25/05 01:37:0
	256MB.sdf	725688	01/28/06 10:40:00
	backup.cfg	5,564	10/07/05 10:10:3
	c180x-advipservicesk9-mz.124-6.T	17,795,940	03/11/06 14:08:20
	common.tar	1,007,616	10/24/05 00:32:10
	in home.shtml	1,038	10/24/05 00:32:10
	in home.tar	113152	10/24/05 00:32:10
	👩 sdm.tar	4,049,920	10/24/05 00:32:18
	sdmconfig-18xx.cfg	1,820	03/04/06 22:15:50
	sdmips.sdf	527028	03/13/06 03:14:4:
	securedesktop-ios-3.1.1.27-k9.pkg	1,684,577	03/04/06 22:17:0
	sigcategories.xml	321559	11/11/05 10:49:40
	ssiclient-win-1.0.2.127.pkg	319662	03/04/06 22:17:10

4. Haga clic en Cargar archivo desde el PC. Aparecerá el cuadro de diálogo Guardar

Look jn: 🔁 SDF	• C 🕆 🗊•
126MB.sdf     256MB.sdf     attack-drop.sdf	

archivo.

5. Elija el SDF que debe actualizarse y haga clic en Abrir. Aparece el mensaje de advertencia



de SDM.

6. Haga clic en Yes para reemplazar el archivo existente.Un cuadro de diálogo muestra el



progreso del proceso de carga.

 Una vez que el proceso de carga haya finalizado, haga clic en Recargar firmas en la barra de herramientas de ubicación de SDF. Esta acción recarga el IPS de Cisco IOS

👃 IPS Policies		۲. Contraction and the second s
🚮 Global Settings	Item Name	Item Value
G SDEE Messages	Syslog	Enabled
🦉 Signatures	* SDEE Alerts SDEE Alerts SDEE Subscription Engine Options Fail Closed Use Built-In Signatures (as backup) Deny Action on IPS interface	200 200 1 Disabled Enabled Disabled
	Shun Event	20
	Timeout	30
	Configured SDF Locations: Add @ Ed	su dit 🏦 Delete 🛊 Move Up 🖶 Move Down 🔊 Reload Signat
	Configured SDF Locations: Add C Ed	30 dit 🏦 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload Signat
	Configured SDF Locations: Add C Ed flash://sdmips.sdf flash://128MB.sdf (autosave)	su

**Nota:** El paquete IOS-Sxxx.zip contiene todas las firmas que admite Cisco IOS IPS. Las actualizaciones de este paquete de firma se publican en Cisco.com en cuanto estén disponibles. Para actualizar las firmas contenidas en este paquete, vea el <u>Paso 2</u>.

### Información Relacionada

- <u>Cisco Intrusion Prevention System</u>
- Avisos de campo de productos de seguridad (incluida CiscoSecure Intrusion Detection)
- <u>Soporte Técnico Cisco Systems</u>