Configurer le routeur et SDM et l'interface de ligne de commande Cisco IOS dans Cisco IOS IPS

Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Configuration Activer Cisco IOS IPS avec un SDF par défaut Ajouter des signatures supplémentaires après l'activation du SDF par défaut Sélectionner des signatures et travailler avec des catégories de signatures Mettre à jour les signatures des fichiers SDF par défaut Informations connexes

Introduction

Dans Cisco Router and Security Device Manager (SDM) 2.2, la configuration IPS de Cisco IOS[®] est intégrée à l'application SDM. Vous n'avez plus besoin de lancer une fenêtre séparée pour configurer Cisco IOS IPS.

Dans Cisco SDM 2.2, un nouvel assistant de configuration IPS vous guide tout au long des étapes nécessaires pour activer Cisco IOS IPS sur le routeur. En outre, vous pouvez toujours utiliser les options de configuration avancée pour activer, désactiver et régler Cisco IOS IPS avec Cisco SDM 2.2.

Cisco vous recommande d'exécuter Cisco IOS IPS avec les fichiers de définition de signature prédéfinis (SDF) : attentat-drop.sdf, 128 Mo.sdf et 256 Mo.sdf. Ces fichiers sont créés pour les routeurs avec différentes quantités de mémoire. Les fichiers sont fournis avec Cisco SDM, qui recommande les SDF lorsque vous activez Cisco IOS IPS pour la première fois sur un routeur. Ces fichiers peuvent également être téléchargés à partir de <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u> (clients <u>enregistrés</u> uniquement).

Le processus d'activation des SDF par défaut est détaillé dans la section <u>Enable Cisco IOS IPS</u> with a Factory Default SDF. Lorsque les SDF par défaut ne sont pas suffisants ou que vous voulez ajouter de nouvelles signatures, vous pouvez utiliser la procédure décrite dans <u>Ajouter des</u> <u>signatures supplémentaires après avoir activé le SDF par défaut</u>.

Conditions préalables

Conditions requises

Java Runtime Environment (JRE) version 1.4.2 ou ultérieure est requis pour utiliser Cisco SDM 2.2. Un fichier de signature configuré et recommandé par Cisco (basé sur la DRAM) est fourni avec Cisco SDM (chargé sur la mémoire flash du routeur avec Cisco SDM).

Components Used

Les informations de ce document sont basées sur Cisco Router and Security Device Manager (SDM) 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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Configuration

Activer Cisco IOS IPS avec un SDF par défaut

Procédure CLI

Suivez cette procédure afin d'utiliser l'interface de ligne de commande pour configurer un routeur de la gamme Cisco 1800 avec Cisco IOS IPS pour charger 128MB.sdf sur la mémoire flash du routeur.

- Configurez le routeur pour activer la notification d'événement SDEE (Security Device Event Exchange).
 yourname#conf t
- 2. Entrez les commandes de configuration (une par ligne), puis appuyez sur Ctrl+Z pour terminer.

yourname(config)#ip ips notify sdee

- 3. Créez un nom de règle IPS utilisé pour l'association aux interfaces. yourname(config)#ip ips name myips
- 4. Configurez une commande d'emplacement IPS pour spécifier à partir de quel fichier le système IPS Cisco IOS lit les signatures.Cet exemple utilise le fichier sur flash : 128 Mo.sdf. La partie URL d'emplacement de cette commande peut être toute URL valide qui utilise la mémoire Flash, le disque ou les protocoles via FTP, HTTP, HTTPS, RTP, SCP et TFTP afin de pointer vers les fichiers.

yourname(config)#ip ips sdf location flash:128MB.sdf

Remarque : Vous devez activer la commande terminal monitor si vous configurez le routeur

via une session Telnet ou si les messages SDEE ne s'affichent pas lors de la création du moteur de signature.

- 5. Activez IPS sur l'interface sur laquelle vous voulez activer l'IPS Cisco IOS pour analyser le trafic. Dans ce cas, nous avons activé sur les deux directions sur l'interface 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
```

Lors de la première application d'une règle IPS à une interface, Cisco IOS IPS démarre les signatures créées à partir du fichier spécifié par la commande SDF locations. Les messages SDEE sont consignés sur la console et envoyés au serveur Syslog si configurés. Les messages SDEE avec *<number>* de *<number>* moteurs indiquent le processus de création du moteur de signature. Enfin, lorsque les deux nombres sont identiques, tous les moteurs sont construits. **Remarque :** le réassemblage virtuel IP est une fonction d'interface qui (lorsqu'elle est activée) réassemble automatiquement les paquets fragmentés qui entrent dans le routeur via cette interface. Cisco recommande d'activer l'assemblage virtuel ip sur toutes les interfaces où le trafic entre dans le routeur. Dans l'exemple ci-dessus, outre l'activation de « ip virtual-assembly » sur l'interface fastEthernet 0, nous le configurons également sur l'interface interne VLAN 1.

yourname(config-if)**#ip virtual-reassembly**

Procédure SDM 2.2

Suivez cette procédure afin d'utiliser Cisco SDM 2.2 pour configurer un routeur de la gamme Cisco 1800 avec Cisco IOS IPS.

1. Dans l'application SDM, cliquez sur **Configurer**, puis sur **Prévention des**

	🗳 Home	Configure	Monitor	@ Retesh	Save	Q. Search	P Help	Cisco Systems
	Tesks	🕼 Intrusion	Prevention Sys	tem (IPS)				
	Preventioned and PCL	Create IPS E The IPS rul specifies 9	dit IPS le configuration with le location of the SC	ind configures IP OF (signature de	PS rules on Inition file)	an interface :	and also	
	1 1 40 1 2 2 2 2 2 2 2 2 2		Use Case	e Scenario nituaion Preventio di a interface Verani Verani Verani Verani	-			
	NET Intrusion Prevention County of Service Refer Net:				Lau	ich IPS Rule	Wizard	
intrusions	Intrusion Prevention	n System (IPS)						02:45:58 UTC Mon Mar 13 2008 @

2. Cliquez sur l'onglet Create IPS, puis sur Launch IPS Rule Wizard.Cisco SDM nécessite une notification d'événement IPS via SDEE afin de configurer la fonctionnalité IPS de Cisco IOS. Par défaut, la notification SDEE n'est pas activée. Cisco SDM vous invite à activer la notification d'événement IPS via SDEE, comme illustré sur cette image



3. Click OK.La fenêtre Assistant Stratégies IPS de la boîte de dialogue Assistant Stratégies IPS



s'affiche.

4. Cliquez sur Next (Suivant).La fenêtre Sélectionner les interfaces

S POLICION HILLOID			
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		
diilleak.com 17	FastEthernet0	9	▼

s'affiche.

- 5. Choisissez les interfaces pour lesquelles vous voulez activer IPS, puis cliquez sur la case **Entrant** ou **Sortant** afin d'indiquer la direction de cette interface. **Remarque :** Cisco recommande d'activer les directions entrantes et sortantes lorsque vous activez IPS sur une interface.
- 6. Cliquez sur Next (Suivant).La fenêtre SDF Locations s'affiche.
- 7. Cliquez sur **Add** afin de configurer un emplacement SDF.La boîte de dialogue Ajouter un emplacement de signature

IPS Wizard	Specify the locations from white Cisco IOS IPS. If Cisco IOS IPS	th the SDF (signature definit) fails to load the SDF from the SDF from the SDF from the SDF file.	on file) should be loaded by the he first location, it tries the
~	SDF Locations	ssiuny loads the SDF me.	
			Add
10			Move Up
17-20	Add a Signature Location		Move Down
	Specify SDF onflash: File Name onflash:	256MB.sdf	
7	C Specify SDF using URL	:	
	Profesoi	http://www.www.	cation, it can
	i intest		
	Econole Fautosave		sedf
	ок	Cancel Help	
171-24			
A Long			

- s'affiche.
 8. Cliquez sur la case d'option Spécifier SDF sur flash, puis sélectionnez 256MB.sdf dans la liste déroulante Nom du fichier sur flash.
- 9. Cliquez sur la case **auto save**, puis sur **OK**.**Remarque :** l'option d'enregistrement automatique enregistre automatiquement le fichier de signature en cas de modification de signature.La fenêtre SDF Locations affiche le nouvel emplacement



marque : Vous pouvez ajouter des emplacements de signature supplémentaires afin de désigner une sauvegarde.

- 10. Cochez la case **Utiliser les signatures intégrées (comme sauvegarde)**.**Remarque :** Cisco vous recommande de ne pas utiliser l'option de signature intégrée, sauf si vous avez spécifié un ou plusieurs emplacements.
- 11. Cliquez sur **Suivant** pour continuer.La fenêtre Résumé s'affiche.



12. Cliquez sur Finish.La boîte de dialogue État de remise des commandes affiche l'état au fur et à mesure que le moteur IPS compile toutes les

Commands Delivery Status	\mathbf{X}
Command Delivery Status:	
Preparing commands for delivery Submitting 10 commands, please wait Configuration delivered to router.	8
<u>s</u>	×
ок	

signatures.

13. Une fois le processus terminé, cliquez sur **OK**.La boîte de dialogue État de compilation des signatures affiche les informations de compilation des

igna	ture Compilation St	atus		l
PS s	ignature engines are l	built and are n	eady to scan packets.	
				Τ
				1
NO.	Engine	Status	No of Signatures	ł
2	MULTI-STRING	Skipped	No New Signatures	E
3	STRING.ICMP	Loaded	1	
4	STRING.UDP	Loaded	17	L
5	STRING.TCP	Loaded	58	L
6	SERVICE.FTP	✓ Loaded	3	L
7	SERVICE.SMTP	Loaded	2	
8	SERVICE.RPC	✓ Loaded	29	
9	SERVICE.DNS	✓ Loaded	31	I
10	SERVICE.HTTP	✓ Loaded	132	
11	ATOMIC.TCP	✓ Loaded	11	L
12	ATOMIC.UDP	✓ Loaded	9	
13	ATOMIC.ICMP	Skipped	No New Signatures	
14	ATOMIC.IPOPTIONS	✓ Loaded	1	
15	ATOMIC.L3.IP	Loaded	5	ŀ
4				
		Close		

signatures.

Ces informations indiquent

quels moteurs ont été compilés et le nombre de signatures dans ce moteur. Pour les moteurs qui affichent *Ignoré* dans la colonne d'état, aucune signature n'est chargée pour ce moteur.

- 14. Cliquez sur **Fermer** afin de fermer la boîte de dialogue État de compilation des signatures.
- 15. Afin de vérifier quelles signatures sont actuellement chargées sur le routeur, cliquez sur **Configurer**, puis sur **Prévention des intrusions**.
- Cliquez sur l'onglet Modifier IPS, puis sur Signatures.La liste des signatures IPS apparaît dans la fenêtre Signatures.

Tasks Intrusion Prevention System (IPS) Create IPS Edit IPS Create IPS Edit IPS Olichal Settings Olichal Settings <t< th=""><th>🚯 Home</th><th>Configure 🔯 Monitor</th><th>@ Retresh</th><th></th><th>Save</th><th>Q. Search</th><th>P Help</th><th></th><th>Cist</th><th>CO SYSTE</th></t<>	🚯 Home	Configure 🔯 Monitor	@ Retresh		Save	Q. Search	P Help		Cist	CO SYSTE
Create IPS Edit IPS IPS Policies IPS Policies	Tesks	😺 Intrusion Prevention Sys	tem (IPS)							
Image: Society Rude	-	Create IPS Edit IPS								
Schedularies Source Prevention Source Prevention Source Prevention	and and	IPS Policies	Dig Impo	e =	Select to	N. ALSO	natures · Oriteria: -NIA	•	Te	al[303]
SDEE Messages Bignatures Emakled I Sig D Subsig D Name Action Sevently Emakled Sig VIN Image: State Categories Image: State	Connections	🔂 Global Settings	Seler	t Al	A Ad	· Fat Edit	1 Delete C Enable O De	able	G	1 Detail
Number of RCL Number of RCL<	34	G SDEE Messages	Ecotion	-	000	la san D	himme	Action	County	For
With Categories Bin Attack	wall and RCL	Signatures	2		3157	SubSig C	FTP PASY Port Spoof	Action	high	SERVE
V/FN B Attack B Service	-	E OS	0		11002	0	Grutella Server Reply	alarm	low	STRIN
B- Sentce B- Sentce B- Sentce B- L2L_3L_4 Protocol B- Releases 3129 Menail Virus C Variant File Attac drop reset alarm medium 500 Noting Sinta 3129 Menail Virus C Variant File Attac drop reset medium 500 Noting Sinta Sinta 1 rWWV Albaba attack 2 alarm low 500 National Sinta Sinta Sinta Sinta Image: Sinta low Sinta National Sinta Sinta Sinta Sinta Image: Sinta Image: Sinta Sinta Sinta National Sinta	UPN	B- Attack	0	-	5088	0	vWWW Akopia Mini/vend access	alarm	low	SERVE
Courty Rudt B- Releases 3129 0 Minual Virus C Variant File Attac drop reset medium SER Noticing 0 5094 1 rWWV Alibaba attack 2 alarm low SER NHT 0 5094 1 rWWV Alibaba attack 2 alarm low SER NHT 0 5094 0 rWWV Alibaba attack 2 alarm low SER NHT 0 5094 0 rWWV Alibaba attack 2 alarm low SER NHT 0 5094 0 rWWV Alibaba attack 2 alarm low SER NHT 0 11212 0 Yahoo Messenger Through HT alarm informational SER NHT 0 5080 0 rWWV SGI wrap bug alarm medium SER N 50952 0 rWWV VTI Open attempt alarm medium SER N 50952 0 Back Door TandScout alarm high STR N 60962 1 DNS Authors Request alarm	500	B- L2/L3/L4 Protocol	0		3153	0	FTP Improper Address	alarm	medium	SERVI
Notices 5084 1 rWWV Alibaba attack 2 alarm low SER Not 5084 0 rWWV Alibaba attack 2 alarm low SER Not 11212 0 rWWV Alibaba attack 2 alarm low SER Init 11212 0 rWWV Alibaba attack 2 alarm low SER Init 11212 0 rWWV EM WebSphere access alarm low SER Init 5080 0 rWWV SGI wrap bug alarm medium SER Init 5082 0 rWWV VTI Open attempt alarm medium SER Init 5082 0 Back Door TransScout alarm high STR Init 1005 Authors Request alarm kow SER	ourly Rudit	B- Releases	0	T	3129	0	Mmail Virus C Variant File Attac	alarm drop reset	medium	SERVE
NHT S004 0 VMWV Albaba attack 2 elarm low S08 NHT 11212 0 Yahoo Messenger Through HT elarm informational S58 State 5080 0 VMWV IEM WebSphere access elarm low S58 State 3218 0 VMWV SCI wrap bug elarm medium S58 State 5052 0 VMWV VTI Open attempt elarm medium S58 State 9535 0 Back Door TensScout elarm high S18 State 6062 1 DNS Authors Request elarm low S28	Routing		0		5084	1	vWWV Alibaba attack 2	alarm	low	SERVI
INIT Image: Constraint of the second of	51.		0		5084	0	vWWV Albaba effack 2	alarm	low	SERVE
Image: Construction Image: Construct	1		0		11212	0	Yahoo Messenger Through HT	olarm	informational	SERVE
Image: Service Image: Service 3218 0 vWWVSCI wrap bug alarm medium SER Image: Service 5052 0 vWWVVTI Open attempt alarm medium SER Image: Service 9535 0 Back Door TendScout alarm High STR Image: Service 6062 1 DNS Authors Request alarm kow SER	TOHI		0		5080	0	vWWV IBM WebSphere access	alarm	low	SERV
Image: constraint of the second se	0		0		3218	0	vWWV SGI wrap bug	alarm	medium	SERVE
Image: Construction	n Prevention		0	1	5052	0	vWWV VTI Open attempt	olarm	medium	SERVE
y of Service 6062 1 DNS Authors Request alarm low SER			0		9535	0	Back Door TansScout	olarm	high	STRIN
	y of Service		0		6062	1	DNS Authors Request	alarm	low	SERVE
	-		4			10000			and the second	

Ajouter des signatures supplémentaires après l'activation du SDF par défaut

Procédure CLI

Aucune commande CLI n'est disponible pour créer des signatures ou lire les informations de signature à partir du fichier IOS-Sxxx.zip distribué. Cisco vous recommande d'utiliser SDM ou Management Center for IPS Sensors pour gérer les signatures sur les systèmes IPS Cisco IOS.

Pour les clients qui ont déjà un fichier de signature prêt et qui souhaitent fusionner ce fichier avec le fichier SDF qui s'exécute sur un système IPS Cisco IOS, vous pouvez utiliser cette commande :

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

Le fichier de signature défini par la commande signature location est l'emplacement où le routeur charge les fichiers de signatures lors du rechargement ou lorsque l'IPS IOS du routeur est reconfiguré. Pour que le processus de fusion réussisse, le fichier défini par la commande signature file location doit également être mis à jour.

 Utilisez la commande show afin de vérifier les emplacements de signature actuellement configurés.Le résultat indique les emplacements de signature configurés. Cette commande indique l'emplacement de chargement des signatures en cours. yourname#show ip ips signatures Builtin signatures are configured

Les dernières signatures ont été chargées à partir de flash:128MB.sdfVersion S128.0 de

Cisco SDFTrend SDF version V0.0

 Utilisez la commande copy <url>ips-sdf, avec les informations de l'étape précédente, afin de fusionner les fichiers de signature.

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#

Après avoir exécuté la commande **copy**, le routeur charge le fichier de signature dans la mémoire, puis crée les moteurs de signature. Dans la sortie du message SDEE de la console, l'état de construction de chaque moteur de signature s'affiche.%IPS-6-ENGINE_BUILD_SKIPPED indique qu'il n'existe aucune nouvelle signature pour ce moteur.%IPS-6-ENGINE_READY indique qu'il existe de nouvelles signatures et que le moteur est prêt. Comme précédemment, le message « 15 des 15 moteurs » indique que tous les moteurs ont été construits.IPS-7-UNSUPPORTED_PARAM indique qu'un certain paramètre n'est pas pris en charge par Cisco IOS IPS. Par exemple, CapturePacket et ResetAfterIdle.**Remarque** : ces messages sont fournis à titre d'information uniquement et n'auront aucune incidence sur la capacité ou les performances de signature IPS de Cisco IOS. Ces messages de journalisation peuvent être désactivés en définissant le niveau de journalisation supérieur au débogage (niveau 7).

3. Mettez à jour le SDF défini par la commande signature location, de sorte que lorsque le routeur se recharge, il dispose de la signature fusionnée et des signatures mises à jour. Cet exemple montre la différence de taille de fichier après l'enregistrement de la signature fusionnée dans le fichier 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

Avertissement : Le nouveau fichier 128MB.sdf contient désormais des signatures fusionnées par le client. Le contenu est différent du fichier Cisco 128MB.sdf par défaut. Cisco vous recommande de changer le nom de ce fichier pour éviter toute confusion. Si le nom est modifié, la commande signature location doit également être modifiée.

Procédure SDM 2.2

Une fois Cisco IOS IPS activé, de nouvelles signatures peuvent être ajoutées au routeur qui exécute un jeu de signatures avec la fonction d'importation de Cisco SDM. Complétez ces étapes afin d'importer de nouvelles signatures :

- 1. Choisissez les SDF par défaut ou le fichier de mise à jour IOS-Sxxx.zip pour importer des signatures supplémentaires.
- 2. Cliquez sur Configurer, puis sur Prévention des intrusions.
- 3. Cliquez sur l'onglet **Modifier IPS**, puis cliquez sur **Importer**.

IPS Policies	De Impo	t = Select I	by: All Sig	natures - Criteria:N(A,	*	Te	ital[303]
🚯 Global Settings	From P	с	d • 💣 Edit	1 Delete 🔘 Enable 🔾 Dis	able	6	🗟 Details
SDEE Messages	From re	outer flash	SASa D	Name	Action	Severity	Erv
Signatures	B CITABUTCO	3157	0	FTP PASV Port Spoot	alarm	high	SERVI
All Categories		11002	0	Grutella Server Reply	alarm	kow	STRIN
E Attack		6000	0	Alfild/ Alconia Mini/and access	alarm	low	CEPA
E Gervice	0	5000	0	www.Auopia Herveria access	alarm	IOW	SERVI
E L2/L3/L4 Protocol	0	3153	0	FTP Improper Address	alarm	medium	SERVI
⊞- <u> </u> Releases	•	3129	0	Mimail Virus C Variant File Attac	alarm drop reset	medium	SERVI
	0	5084	1	vWWV Alibaba attack 2	aiarm	low	SERVI
	0	5084	0	vWWV Alibaba attack 2	alarm	low	SERVI
	0	11212	0	Yahoo Messenger Through HT	alarm	informational	SERVI
	0	5080	0	vWWV IBM WebSphere access	alarm	low	SERVI
	0	3218	0	vWWV SGI wrap bug	alarm	medium	SERVI
	0	5052	0	vWWV VTI Open attempt	alarm	medium	SERVI
	0	9535	0	Back Door TansScout	alarm	high	STRIN
	0	6062	1	DNS Authors Request	alarm	low	SERVI
	1					· · ·	•

- 4. Choisissez From PC dans la liste déroulante Importer.
- 5. Sélectionnez le fichier à partir duquel vous voulez importer des

Import	2 🛛
Look jn: 😂 CCOSigs	• 🔁 🖆 📰 •
105-5208.zip 105-5214.zip 105-5209.zip 105-5215.zip 105-5210.zip 105-5216.zip 105-5211.zip 105-5217.zip 105-5212.zip 105-5213.zip	
<	>
File name: 105-5217.zip	<u>Q</u> pen
Files of type: All Files (".")	Cancel

signatures.

Cet exemple utilise la dernière

- mise à jour téléchargée à partir de Cisco.com et enregistrée sur le disque dur du PC local.
 6. Cliquez sur **Open.Avertissement :** en raison de contraintes de mémoire, seul un nombre limité de nouvelles signatures peuvent être ajoutées en plus des signatures déjà déployées. Si trop de signatures sont sélectionnées, le routeur risque de ne pas pouvoir charger toutes
 - les nouvelles signatures en raison d'un manque de mémoire.Une fois le chargement du fichier de signature terminé, la boîte de dialogue Importation IPS

Name KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe Grutella Client Request Grutella Server Reply	Deployed Ves Yes Yes Yes	Se Import
Name KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe Grutella Client Request Grutella Server Reply	Ves Ves Ves Ves Ves	
KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe Grutella Client Request Grutella Server Reply	Ves Ves Ves Ves	1 4 4
KaZaA v2 UDP Client Probe KaZaA v2 UDP Client Probe Grutella Client Request Grutella Server Reply	Yes Ves Yes	4
KaZaA v2 UDP Client Probe Grutella Client Request Grutella Server Reply	Yes Yes	4
Grutella Client Request Grutella Server Reply	Yes	
Grutella Server Reply		U
Challe Sie Research	VAO	
C Providence in these introduction age of the	No	
George Pile Request	No	-
Bearshare File Request	NO	-
KaZaA Client Activity	Yes	P
Gnucleus File Request	Yes	9
Limewire File Request	No	
Morpheus File Request	No	Г
Phex File Request	No	Г
Swapper File Request	No	Г
XoloX File Request	No	Г
GTK-Grutela File Request	Yes	F
Mutelin File Request	No	Г
Hotine Clerit Login	No	-
Hotine Ele Transfer	No	-
riourie rije fransner	NO	-
	KaZaA Client Activity Gnucleus File Request Limewire File Request Morpheus File Request Phex File Request Swapper File Request XoloX File Request GTK-Gnutella File Request Mutella File Request Hotine Client Login Hotine File Transfer	KaZaA Client Activity Yes Grucleus File Request Yes Limewire File Request No Morpheus File Request No Phex File Request No Swapper File Request No XoloX File Request No GTK-Grutela File Request No Mutelia File Request No Hotline Client Login No

apparaît.

- 7. Naviguez dans l'arborescence de gauche, puis cliquez sur la case à cocher **Importer** en regard des signatures à importer.
- 8. Cliquez sur la case d'option **Fusionner**, puis cliquez sur **OK**. **Remarque**: l'option Remplacer remplace la signature actuelle définie sur le routeur par les signatures que vous sélectionnez pour importer. Lorsque vous cliquez sur OK, l'application Cisco SDM transmet les signatures

Signature Delivery Status	
Delivering SDF to router	

au routeur.

Remarque : Une

utilisation élevée du CPU se produit lors de la compilation et du chargement des signatures. Une fois Cisco IOS IPS activé sur l'interface, le fichier de signature commence à se charger. Le routeur met environ cinq minutes à charger le répartiteur principal SDF. Vous pouvez essayer d'utiliser la commande **show process cpu** afin d'afficher l'utilisation du CPU à partir de l'interface de ligne de commande du logiciel Cisco IOS. Cependant, n'essayez pas d'utiliser des commandes supplémentaires ou de charger d'autres SDF pendant que le routeur charge le SDF. Cela peut faire que le processus de compilation des signatures soit plus long (puisque l'utilisation du CPU est proche de 100 % au moment du chargement du SDF). Vous devrez peut-être parcourir la liste des signatures et les activer si elles ne sont pas dans l'état *activé*.Le nombre total de signatures est passé à 519. Ce numéro inclut toutes les signatures disponibles dans le fichier IOS-S193.zip qui appartiennent à la sous-catégorie Partage de

fichiers.



Pour obtenir des informations plus détaillées sur l'utilisation de Cisco SDM pour gérer la fonctionnalité IPS de Cisco IOS, reportez-vous à la documentation de Cisco SDM à l'adresse suivante :

Sélectionner des signatures et travailler avec des catégories de signatures

Afin de déterminer comment sélectionner efficacement les signatures correctes pour un réseau, vous devez connaître certaines choses sur le réseau que vous protégez. Les informations mises à jour sur la catégorie de signatures dans Cisco SDM 2.2 et versions ultérieures aident les clients à sélectionner le jeu de signatures approprié pour protéger le réseau.

La catégorie est un moyen de regrouper les signatures. Il permet de limiter la sélection des signatures à un sous-ensemble de signatures qui sont pertinentes les unes pour les autres. Une signature peut appartenir à une seule catégorie ou à plusieurs catégories.

Voici les cinq catégories de niveau supérieur :

- OS : catégorisation des signatures basée sur le système d'exploitation
- Attaque : catégorisation des signatures en fonction des attaques
- Service : catégorisation des signatures basée sur les services

- Protocole de couche 2-4 : catégorisation des signatures au niveau du protocole
- Versions : catégorisation des signatures basée sur les versions

Chacune de ces catégories est divisée en sous-catégories.

Prenons l'exemple d'un réseau domestique avec une connexion haut débit à Internet et un tunnel VPN vers le réseau d'entreprise. Le pare-feu Cisco IOS est activé sur la connexion ouverte (non-VPN) à Internet du routeur haut débit pour empêcher toute connexion provenant d'Internet et connectée au réseau domestique. Tout le trafic provenant du réseau domestique vers Internet est autorisé. Supposons que l'utilisateur utilise un PC Windows et des applications telles que HTTP (navigation Web) et e-mail.

Le pare-feu peut être configuré de sorte que seules les applications dont l'utilisateur a besoin soient autorisées à traverser le routeur. Cela contrôlera le flux du trafic indésirable et potentiellement indésirable qui peut se propager sur l'ensemble du réseau. Considérez que l'utilisateur domestique n'a pas besoin d'un service spécifique ou n'en utilise pas. Si ce service est autorisé à circuler à travers le pare-feu, une attaque peut utiliser un trou potentiel pour circuler sur le réseau. Les meilleures pratiques ne permettent que les services nécessaires. Maintenant, il est plus facile de sélectionner les signatures à activer. Vous devez activer les signatures uniquement pour les services que vous autorisez à traverser le pare-feu. Dans cet exemple, les services incluent la messagerie électronique et HTTP. Cisco SDM simplifie cette configuration.

Afin d'utiliser la catégorie pour sélectionner les signatures requises, choisissez **Service > HTTP**, et activez toutes les signatures. Ce processus de sélection fonctionne également dans la boîte de dialogue d'importation de signatures, dans laquelle vous pouvez sélectionner toutes les signatures HTTP et les importer dans votre routeur.

Les catégories supplémentaires à sélectionner sont DNS, NETBIOS/SMB, HTTPS et SMTP.

Mettre à jour les signatures des fichiers SDF par défaut

Les trois SDF (attaque-drop.dsf, 128 Mo.sdf et 256 Mo.sdf) sont actuellement affichés sur Cisco.com à l'adresse <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u> (clients <u>enregistrés</u> uniquement). Les nouvelles versions de ces fichiers seront publiées dès qu'elles seront disponibles. Afin de mettre à jour les routeurs qui exécutent Cisco IOS IPS avec ces SDF par défaut, accédez au site Web et téléchargez les dernières versions de ces fichiers.

Procédure CLI

1. Copiez les fichiers téléchargés à l'emplacement à partir duquel le routeur est configuré pour charger ces fichiers. Pour savoir où le routeur est actuellement configuré, utilisez la commande **show running-config | dans la** commande **ip ips sdf**.

Router#show running-config | in ip ips sdf ip ips sdf location flash://256MB.sdf autosave Dans cet exemple, le routeur utilise 256MB.sdf sur la mémoire flash. Le fichier est mis à jour lorsque vous copiez le nouveau fichier 256MB.sdf téléchargé dans la mémoire Flash du routeur.

2. Rechargez le sous-système IPS Cisco IOS pour exécuter les nouveaux fichiers.Il existe deux façons de recharger Cisco IOS IPS : rechargez le routeur ou reconfigurez Cisco IOS IPS pour déclencher le sous-système IOS IPS pour recharger les signatures. Afin de reconfigurer Cisco IOS IPS, supprimez toutes les règles IPS des interfaces configurées, puis réappliquez les règles IPS aux interfaces. Cela déclenchera le rechargement du système IPS Cisco IOS.

Procédure SDM 2.2

Complétez ces étapes afin de mettre à jour les SDF par défaut sur le routeur :

- 1. Cliquez sur Configurer, puis sur Prévention des intrusions.
- 2. Cliquez sur l'onglet Edit IPS, puis sur Global

💪 IPS Policies			ල් Ed
🔂 Global Settings		Item Name	Item Value
G SDEE Messages		Syslog	Enabled
A Signaturas		SDEE	Enabled
GB orginatores	•	SDEE Alerts	200
		SDEE Messages	200
		SDEE Subscription	1
		Engine Options	Disabled
		Lice Built in Signatures (as backup)	Enabled
		Derv Action on IPS interface	Disabled
		Shun Event	Disabled
		Timeout	30
		Configured SDF Locations: 4 Add a	Edit 🏦 Delete 🎓 Move Up 🐥 Move Down 🔊 Reload §
		Analy-Wadesian add	
		Rechtlich 20MD edf (autocaua)	
		flash:0128MB.sdf (autosave)	
		flash:0128MB.sdf (autosave)	
		flash://128MB.sdf (autosave)	

La partie supérieure de l'interface utilisateur affiche les paramètres globaux. La moitié inférieure de l'interface utilisateur affiche les emplacements SDF actuellement configurés. Dans ce cas, le fichier 256MB.sdf de la mémoire flash est configuré.

3. Choisissez **Gestion des fichiers** dans le menu Fichier.La boîte de dialogue Gestion des fichiers

- 🖘 flash:	Name	Size(bytes)	Time Modified
	128MB.sdf	504630	08/25/05 01:37:0
	256MB.sdf	725688	01/28/06 10:40:0
	backup.cfg	5,564	10/07/05 10:10:3
	c180x-advipservicesk9-mz.124-6.T	17,795,940	03/11/06 14:08:2
	common.tar	1,007,616	10/24/05 00:32:1
	home.shtml	1,038	10/24/05 00:32:1
	home.tar	113152	10/24/05 00:32:1
	sdm.tar	4,049,920	10/24/05 00:32:1
	sdmconfig-18xx.cfg	1,820	03/04/06 22:15:5
	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 10:49:4
	ssiclient-win-1.0.2.127.pkg	319662	03/04/06 22:17:1

4. Cliquez sur Charger le fichier à partir du PC.La boîte de dialogue Enregistrer le fichier

Look in: 🛍) SDF	- 🗢 🗈 💣 🏥-
128M8.sd 256M8.sd attack-dr	f Dop.edf	
al arran - ar	op.sor	
ile <u>pame</u> :	256MB.edf	

s'affiche.

5. Choisissez le fichier SDF à mettre à jour, puis cliquez sur **Ouvrir**.Le message d'avertissement SDM

SDM Warni	ng,	
	This directory already contains overwrite?	s a file named 256MB.sdf. Do you want to
	Yes	No

s'affiche.

6. Cliquez sur **Oui** afin de remplacer le fichier existant.Une boîte de dialogue affiche la progression du processus de



téléchargement.

 Une fois le processus de téléchargement terminé, cliquez sur Recharger les signatures dans la barre d'outils de l'emplacement SDF. Cette action recharge l'IPS Cisco IOS.

IPS Policies		ى
olobal Settings	Item Name	Item Value
SDEE Messages	Syslog	Enabled
. Signaturas	» SDEE	Enabled
8 orginatures	SDEE Alerts SDEE Messages	200
	SDEE Messages	200
	Engine Ontions	
	Fail Closed	Disabled
	Use Built-in Signatures (as backup)	Enabled
	Deny Action on IPS interface	Disabled
	Shun Event	
	Timeout	30
	Configured SDF Locations: Add C Ed	it 🏦 Delete 🚖 Move Up 🐥 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed	st 📋 Delete 🎓 Move Up 🖶 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed	it 👔 Delete 👚 Move Up 🖶 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash://sdmips.sdf flash://128MB.sdf (autosave)	it 👚 Delete 👚 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash:0sdmips.sdf flash:0128MB.sdf (autosave)	it 👚 Delete 🚖 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash://sdmips.sdf flash://128MB.sdf (autosave)	it 🗊 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash:0128MB.sdf (autosave)	it 🗊 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash://sdmips.sof flash://128MB.sdf (autosave)	it 🗊 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash:0128MB.sdf flash:0128MB.sdf (autosave)	st 🗊 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash:0128MB.sdf flash:0128MB.sdf (autosave)	st 🗊 Delete 🏦 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash:0900000000000000000000000000000000000	st 🗊 Delete 🏦 Move Up 🤑 Move Down 🔊 Reload Signa
	Configured SDF Locations: Add C Ed flash:0128MB.sdf (autosave)	st 👚 Delete 🏦 Move Up 🤑 Move Down 🔊 Reload Signa

Remarque : le package IOS-Sxxx.zip contient toutes les signatures prises en charge par Cisco IOS IPS. Les mises à niveau de ce package de signatures sont publiées sur Cisco.com dès qu'elles sont disponibles. Afin de mettre à jour les signatures contenues dans ce paquet, voir <u>Étape 2</u>.

Informations connexes

- <u>Système de prévention des intrusions Cisco</u>
- Avis de champs relatifs aux produits de sécurité (y compris CiscoSecure Intrusion Detection)
- <u>Support technique Cisco Systems</u>