Configureer router en sloten en Cisco IOS CLI in Cisco IOS IPS

Inhoud

Inleiding
<u>Voorwaarden</u>
<u>Vereisten</u>
Gebruikte componenten
<u>Conventies</u>
<u>Configureren</u>
Cisco IOS IPS met fabrieksstandaard SDF inschakelen
Extra handtekeningen toevoegen nadat standaard SDF is ingeschakeld
<u>Selecteer Handtekeningen en werk met handtekeningen</u>
<u>Handtekeningen voor standaard SDF-bestanden bijwerken</u>
Gerelateerde informatie

Inleiding

In Cisco de router en de Manager van het Veiligheidsapparaat (middel dm) 2.2, de configuratie van Cisco IOS[®] IPS binnen de toepassing sm wordt geïntegreerd. U hoeft niet langer een afzonderlijk venster te starten om Cisco IOS IPS te configureren.

In Cisco slecht 2.2, zal een nieuwe IPS configuratie wizard u door de stappen leiden die nodig zijn om Cisco IOS IPS op de router in te schakelen. Daarnaast kunt u nog de geavanceerde configuratieopties gebruiken om Cisco IOS IPS met Cisco DSM 2.2 in te schakelen, uit te schakelen en af te stemmen.

Cisco raadt aan dat u Cisco IOS IPS met de geprezen kenmerkende bestanden (SDF's) draait: aanval-drop.sdf, 128 MB.sdf en 256 MB.sdf. Deze bestanden worden gemaakt voor routers met verschillende hoeveelheden geheugen. De bestanden worden gebundeld met Cisco DSM, dat SDF's aanbeveelt wanneer u eerst Cisco IOS IPS op een router toestaat. Deze bestanden kunnen ook worden gedownload van <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u> (alleen <u>geregistreerde</u> klanten).

Het proces om de standaard SDF's in te schakelen is gedetailleerd in <u>Cisco IOS IPS met een</u> <u>fabrieksstandaard SDF</u>. Wanneer de standaard SDF's niet volstaan of u nieuwe handtekeningen wilt toevoegen, kunt u de procedure gebruiken die is beschreven in <u>Extra handtekeningen</u> <u>toevoegen nadat U Default SDF hebt ingeschakeld</u>.

Voorwaarden

Vereisten

Java Runtime Environment (JRE) versie 1.4.2 of hoger is vereist om Cisco DM 2.2 te gebruiken. Een door Cisco aanbevolen en aangepast bestand voor handtekeningen (gebaseerd op DRAM) is gebundeld met Cisco DSM (geladen op routergeheugen met Cisco DSM).

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco Router en Security Devices Manager (DSM) 2.2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Cisco IOS IPS met fabrieksstandaard SDF inschakelen

CLI-procedure

Voltooi deze procedure om de CLI te gebruiken om een Cisco 1800 Series router met Cisco IOS IPS te configureren om 128MB.sdf op de routerflitser te laden.

- Configureer de router om de melding van de Security Devices Exchange (SDEE)gebeurtenis in te schakelen.
 yourname#conf t
- 2. Voer configuratieopdrachten in (één per regel) en druk vervolgens op Cntl+Z om te eindigen. yourname(config) **#ip ips notify sdee**
- 3. Maak een IPS regel naam die wordt gebruikt om aan interfaces te associëren. yourname(config)#ip ips name myips
- 4. Configuratie een IPS plaatsopdracht om te specificeren van welk bestand het Cisco IOS IPSsysteem handtekeningen zal lezen.Dit voorbeeld gebruikt het bestand op flitser: 128 MB.sdf. Het URL-gedeelte van deze opdracht kan een geldige URL zijn die flitser, schijf of protocollen via FTP, HTTP, HTTPS, RTP, SCP en TFTP gebruikt om naar de bestanden te wijzen.

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

Opmerking: U moet de opdracht van de **terminalmonitor** inschakelen als u de router via een Telnet-sessie configureren of u de SDEE-berichten niet ziet wanneer de ondertekenaar-machine bezig is met bouwen.

5. Schakel IPS op de interface in waar u Cisco IOS IPS wilt in om verkeer te scannen. In dit geval, hebben we op beide richtingen op interface FastEthernet 0 geactiveerd.

```
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
```

De eerste keer dat een IPS-regel op een interface wordt toegepast, begint Cisco IOS IPS bouwde handtekeningen van het bestand dat door de opdracht SDF-locaties wordt gespecificeerd. SDEE-berichten worden ingelogd op de console en naar de syslig-server verzonden indien geconfigureerd. De SDEE-berichten met *<nummer>* van *<aantal>* motoren geven het proces voor het bouwen van de motor voor handtekeningen aan. Tenslotte, als de twee getallen gelijk zijn, worden alle motoren gebouwd.**Opmerking:** IP virtuele reassemblering is een interfaceoptie die (wanneer ingeschakeld) automatisch gefragmenteerde pakketten reassembleert die in de router door die interface komen. Cisco raadt u aan om IP virtueel-assembleren op alle interfaces toe te staan waar het verkeer in de router komt. In het bovenstaande voorbeeld, naast het inschakelen van "ip Virtual-assembleren" op interface FastEthernet 0, vormen we het ook op de binnenkant interface VLAN 1.

yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly

PROCEDURE 2.2

Voltooi deze procedure om Cisco DSM 2.2 te gebruiken om een Cisco 1800 Series router met Cisco IOS IPS te configureren.

- 1. In de toepassing sm, klik Configureren, en klik dan
 - Inbraakpreventie.

😚 Hone	Configure [Monito	Retech Save	Q. Search	P Help	Cisco Systems
Tenks	Intrusion Prevention Sy	stem (IPS)			
Previol and RCL	Create IPS Edit IPS The IPS rule configuration will specifies the location of the t	zand configures IPS rule SDF (signature definition	s on an interfac file).	e and also	
2	Use Ca	se Scenario			
Security Audit		I Intrusion Prevention ster to interface			
Nat Nat Princeson Prevention					
Cualty of Service			Launch IPS Ru	e Wizard	
Intrusion Preventio	system (IPS)				02:45:58 UTC Mon Mar 13 2008

2. Klik op het tabblad **IPS maken** en klik vervolgens op **Wizard IPS-regel starten**.Cisco PDM vereist IPS-eventkennisgeving via SDEE om de Cisco IOS IPS-functie te configureren. Standaard is het SDEE-bericht niet ingeschakeld. Cisco dm vraagt u om IPS gebeurtenis

kennisgeving via SDEE zoals in dit beeld te



3. Klik op **OK**.Het venster Welcome to the IPS Policy Wizard van het dialoogvenster IPSbeleidswizard



4. Klik op **Volgende**.Het venster Interfaces selecteren verschijnt.

IPS Policies Wizard			
IPS Wizard	Select Interfaces Select the interfaces to which the IPS rule s should be applied to inbound or outbound.	hould be applied. Also cho	ose whether the rule
	Interface Name	Inbound	Outbound
A 11	BRID		
diliticali. com 17 19	FastEthernet0	9	· 되
		< Back Next > Finis	Cancel Help

- 5. Kies de interfaces waarvoor u IPS wilt inschakelen en klik op het selectieteken **Inbound** of **Outbound** om de richting van die interface aan te geven.**Opmerking:** Cisco raadt u aan om zowel inkomende als uitgaande richtingen in te schakelen wanneer u IPS op een interface activeert.
- 6. Klik op Volgende. Het venster voor SDF-locaties verschijnt.
- 7. Klik op **Add** om een SDF-locatie te configureren.Het dialoogvenster Locatie toevoegen verschijnt.

PS Wizard	SDF Locations		
	Specify the locations from w Cisco IOS IPS. If Cisco IOS locations in order until it su	hich the SDF (signature definition file) IPS fails to load the SDF from the first ccessfully loads the SDF file.	should be loaded by the location, it tries the
~	SDF Locations		
			Add
			Delete
130	Add a Signature Locat	ion	Move Up
1225	G Specify SDE onfactor	MH	Move Down
	File Name onflash	256MB s/ff	
48	C Specify SDE using LL		
	Protocoli	http:///	cation, it can
	ulie:7		
	and the second se		
AL	P autosave		
	ок	Cancel Help	
R PAR			J
A Lotte			

- 8. Klik op de knop **SDF opgeven op** de **flitser-**radioknop en kies 256MB.sdf in de vervolgkeuzelijst **Bestandsnaam op** de **flitser**.
- 9. Klik op het selectieteken **automatisch opslaan** en klik op **OK.OPMERKING:** De optie IntraSave zal automatisch het bestand opslaan wanneer er een wijziging in de handtekening is aangebracht.Het venster SDF-instellingen toont de nieuwe SDF-



pmerking: U kunt extra locaties voor handtekening toevoegen om een back-up aan te wijzen.

- 10. Klik op het aanvinkvakje **Ingebouwde handtekeningen gebruiken (als back-up)**. **Opmerking:** Cisco raadt u aan de ingebouwde signatuur niet te gebruiken tenzij u een of meer locaties hebt opgegeven.
- 11. Klik op **Volgende** om verder te gaanHet venster Samenvatting verschijnt.



12. Klik op Voltooien. Het dialoogvenster Opdrachtstatus geeft de status weer zoals de IPS-

Commands Delivery Status	×
Command Delivery Status:	
Preparing commands for delivery Submitting 10 commands, please wait Configuration delivered to router.	2
<u> </u>	× 2
ок	

motor alle handtekeningen samenstelt.

13. Klik op **OK** nadat het proces is voltooid.Het dialoogvenster Compilatiestatus van handtekeningen geeft de informatie over de compilatie van handtekeningen

No.	Engine	Status	No of Signatures
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 Signature:
14	ATOMIC.IPOPTIONS	Loaded	1
15	ATOMIC L3.IP	Loaded	5

Deze informatie laat zien welke

motoren zijn samengesteld en hoeveel handtekeningen in die motor zijn aangebracht. Voor motoren die in de statuskolom zijn *gemonteerd*, is er geen handtekening geladen voor die motor.

- 14. Klik op **Sluiten** om het dialoogvenster Compilatiestatus van de handtekening te sluiten.
- 15. Om te verifiëren welke handtekeningen op het ogenblik op de router worden geladen, klik op **Configureren** en klik vervolgens op **Inbraakpreventie**.
- 16. Klik op het tabblad IPS bewerken en vervolgens op Handtekeningen. De lijst met IPShandtekeningen verschijnt in het venster Handtekeningen.

Teaks Intrusion Prevention System (IPS) Create IPS Edd IPS Create IPS Edd IPS Create IPS Edd IPS Solect NI Solect NI All Synatures Clearing Total 303 Solect NI Solect NI <th col<="" th=""><th>Home</th><th>Configure [Monitor</th><th>O Retresh</th><th>Sav</th><th></th><th>C. Search</th><th>P Help</th><th></th><th>EIII</th><th>10 57111</th></th>	<th>Home</th> <th>Configure [Monitor</th> <th>O Retresh</th> <th>Sav</th> <th></th> <th>C. Search</th> <th>P Help</th> <th></th> <th>EIII</th> <th>10 57111</th>	Home	Configure [Monitor	O Retresh	Sav		C. Search	P Help		EIII	10 57111
Create IPS Edd IPS Import * Select All Adds-tr Otheria: -NA- * Totalig SD Import * Select All Adds-tr Edd IPS Delate Import * Select All Adds-tr Totalig SD Import * Select All Adds-tr Edd IPS Delate Import * Select All Adds-tr Edd IPS Delate Import * Select All Adds-tr <	Tasks	😺 Intrusion Prevention Sys	tem (IPS)								
Image: PS Policies Image: PS	-	Create IPS Edit IPS									
Schedularies Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Delete C Enable Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Dela Solect All A Add * E Edit Disable Disable Solect All A Add * E Edit Disable Disable Sole	defines and	IPS Policies		t = 51	Nect b	ALSO	natures · Oriteria: -NIA	•	Te	fal[303]	
SDEE Messages Bigs abures Binabled I Sig D Subscription Bigs abures Binabled I Sig D Name Action Seventy Bigs VIN OS OS OS 0 P1D PASV Pott Spood oken Pigh SSRV ON OS OS 0 P1D PASV Pott Spood oken Pigh SSRV ON OS Attack 0 9008 0 VMWV Akopia MinVend access oken bow SERV O Attack 0 9008 0 VMWV Akopia MinVend access oken bow SERV O 11002 0 Grutelia Server Ringhy oken bow SERV O 3008 0 VMWV Akopia MinVend access oken bow SERV O 3129 0 Menal Virus C Variant File Attac drug oken bow SERV O 5004 1 rtww Akbaba attack 2 oken oken bow SERV O 5004 0 rtww Akbaba attack 2 oken oken bow SERV<	Connectors	🔂 Global Settings	E Selec	TAL 4	Add	· TAT Edit	1 Delete C Enable C De	able	G	Detail	
ended and RCL Image: Signatures image:	34	G SDEE Messages	Frating	1 0	-0	0.400.0	La	Action	- County	I for	
Wind Categories B	ewall and RCL	Signatures	2 Enabled	1 3	10	Subsigle	FTP PASV Port Spoof	Action	high	D.L	
VIN B Attack B Service B Attack B Service B L2/L3/L4 Protocol B Releases B Releases B State B L2/L3/L4 Protocol B Releases B Releases B State B State B Releases B Releases B State B State B Releases B State B Releases B State B <td>1</td> <td>D All Categories</td> <td></td> <td>11</td> <td>002</td> <td>0</td> <td>Grutella Server Reply</td> <td>alarm</td> <td>kow</td> <td>STRIN</td>	1	D All Categories		11	002	0	Grutella Server Reply	alarm	kow	STRIN	
Be- Service Be- 128_31_4 Protocol Be- Releases Image: Service Be- Releases Image: Service Image: Service Image: Ser	UPN	B- Attack			000	0	WWW Akopia MinWend access	alarm	low	SERVI	
Rouling Image: Control of the section of the secti	50	B- Service B- L2L3L4 Protocol	0	3	153	0	FTP Improper Address	olarm	medium	SERVE	
Noting 5084 1 r/WWV Albaba attack 2 alarm low SERV NAT 5084 0 r/WWV Albaba attack 2 alarm low SERV NAT 11212 0 Yahoo Messenger Through HT alarm informational SERV NAT 5080 0 r/WWV EM WebSphere access alarm low SERV Soon Phevention 5080 0 r/WWV SGI wrap bug alarm medium SERV Soon Phevention 5052 0 r/WWV SGI wrap bug alarm medium SERV Social Phevention 9535 0 Back Door TansScout alarm high STRM Social Phevenition 6062 1 DNS Authors Request alarm low SERV	rourity Rudit	B 🛄 Releases	0	3	129	0	Mimail Virus C Variant File Attac	alarm drop reset	medium	SERVE	
Image: State of the state	Routing		0	6	084	1	vWWV Alibaba attack 2	alarm	low	SERV	
NHT Image: Stress of the s	51.		0	5	004	0	vWWW Albaba attack 2	alarm	low	SERVE	
Initiation Image: Second S	10		0	11	212	0	Yahoo Messenger Through HT	olarm	informational	SERVE	
Image: Service Image: Service 3218 0 vMWV SGI wrap bug alarm medium SERVice Image: Service SSS2 0 vMWV VTI Open attempt alarm medium SERVice Image: Service 9535 0 Back Door TansScout alarm high STRM Image: Service 6062 1 DNS Authors Request alarm low SERVice	TOHI		0	5	080	0	vWWV IBM WebSphere access	olarm	low	SERV	
Son Prevention Image: Solid Soli	0		0	3	218	0	vWWV SGI wrap bug	alarm	medium	SERVE	
Image: Service Image:	sion Prevention		0	5	052	0	vWWW VTI Open attempt	olarm	medium	SERVE	
dby of Service 6062 1 DNS Authors Request alarm low SERV			0	9	535	0	Back Door TansScout	olarm	high	STRIN	
	sity of Service		0		062	1	CNS Authors Request	alarm	low	SERVE	
	0.							- Contractor	and the second		

Extra handtekeningen toevoegen nadat standaard SDF is ingeschakeld

CLI-procedure

Er is geen CLI-opdracht beschikbaar om handtekeningen te maken of informatie te lezen over de handtekening in het gedistribueerde IOS-Sxxx.zip-bestand. Cisco raadt u aan om of het Centrum van het Beheer voor IPS Sensoren te gebruiken om de handtekeningen op Cisco IOS IPS systemen te beheren.

Voor klanten die al een ondertekend bestand klaar hebben en dit bestand met SDF willen samenvoegen dat op een Cisco IOS IPS-systeem draait, kunt u deze opdracht gebruiken:

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

Het bestand van de handtekening dat door het commando van de locatie van de handtekening wordt gedefinieerd, is waar de router bestanden van de handtekeningen laadt wanneer het wordt herladen of wanneer de router IOS IPS wordt hergeconfigureerd. Om het fuserende proces succesvol te zijn, moet het bestand dat door de opdracht voor het lokaliseren van het bestand wordt gedefinieerd ook worden bijgewerkt.

 Gebruik de opdracht tonen om de momenteel geconfigureerde ondertekenlocaties te controleren.De uitvoer toont de geconfigureerde locaties van handtekeningen. Deze opdracht toont aan waar de huidige actieve handtekeningen zijn geladen. yourname#show ip ips signatures Builtin signatures are configured

De handtekeningen zijn voor het laatst geladen vanaf flitser:128MB.sdfCisco SDF-release versie S.128.0Trend SDF-release versie V0.0

	10101		
2.	Gebr	ruik	t de opdracht kopie <<i>url</i>> IPS-sdf samen met de informatie uit de vorige stap om
	besta	anc	len met handtekeningen samen te voegen.
	yourr	name	e#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
	Loadi	ing	mysignatures.xml from 10.10.10.5 (via Vlan1): !
	[OK -	- 16	512 bytes]
	*Oct	26	02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
	No er	ntry	$_{\prime}$ 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
		0.0	no new signature definitions for this engine
	*UCt	26	02:43:34.920: %1PS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures -
	*0+	20	3 OI 15 engines
	^OCL	20	02:43:34.920: %1PS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - Chere are
	*Oat	26	10 new signature definitions for this engine
	-00L	20	1 of 15 orginos
	*Oct	26	4 OI IJ ENGINES 02.43.34 920. & IDG_6_ENGINE BUILD SKIDDED. STRING UDD - there are
	000	20	no new signature definitions for this engine
	*Oct	26	02:43:34,924: %TPS-6-ENGINE BUILDING: STRING.TCP - 59 signatures -
	000	20	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 -
		0.0	7 of 15 engines
	*Oct	26	02:43:37.288: %1PS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are
	*0~+	20	no new signature definitions for this engine
	~00L	20	02:45:57.200: %1PS-0-ENGINE_BUILDING: SERVICE.RPC - 29 SIGNALULES -
	*Oct	26	0 01 15 engines 02.43.37 288. %IDC_6_ENGINE BUILD SKIDDED. SEDVICE RDC - there are
	000	20	no new signature definitions for this engine
	*Oct	26	02.43.37 292. %IPS-6-ENGINE BUILDING. SERVICE DNS - 31 signatures -
	000	20	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#

Nadat u de opdracht **kopie** geeft, laadt de router het signatebestand in het geheugen en bouwt dan de signatuur motoren. In de SDEE-berichtuitvoer van de console wordt de bouwstatus voor elke kenmerkende motor weergegeven.%IPS-6-ENGINE_BUILD_SKIPPED geeft aan dat er geen nieuwe handtekeningen voor deze motor zijn.%IPS-6-ENGINE_READY geeft aan dat er nieuwe handtekeningen zijn en dat de motor klaar is. Zoals voorheen geeft het bericht "15 van 15 motoren" aan dat alle motoren zijn gebouwd.IPS-7-UNSUPPORTED_PARAM geeft aan dat een bepaalde parameter niet door Cisco IOS IPS wordt ondersteund. Bijvoorbeeld CapturePacket en ResetAfterIdle.**OPMERKING:** Deze berichten zijn alleen ter informatie en hebben geen effect op de functies of prestaties van Cisco IOS IPS-handtekeningen. Deze houtlogberichten kunnen worden uitgeschakeld door het logniveau hoger in te stellen dan het fouilleren (niveau 7).

3. Update de SDF die door de opdracht voor de locatie van de handtekeningen wordt gedefinieerd, zodat wanneer de router wordt herladen, de gefuseerde handtekeningen worden ontvangen met een aangepaste handtekening. Dit voorbeeld toont het verschil in bestandsgrootte nadat de samengevoegde handtekening is opgeslagen in het 128MB.sdf flitsbestand.

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

Waarschuwing: de nieuwe 128MB.sdf bevat nu door de klant samengevoegde handtekeningen. De inhoud is anders dan het Cisco standaard 128MB.sdf-bestand. Cisco raadt u aan dit bestand met een andere naam te wijzigen om verwarring te voorkomen. Als de naam wordt gewijzigd, moet de opdracht voor de locatie van de handtekening ook worden gewijzigd.

PROCEDURE 2.2

Nadat Cisco IOS IPS is toegelaten, kunnen de nieuwe handtekeningen in de router worden toegevoegd die een signatuur die met de de invoerfunctie van Cisco PDM loopt. Voltooi deze stappen om nieuwe handtekeningen te importeren:

- 1. Kies de standaard SDFs of het update bestand van IOS-Sxxx.zip om extra handtekeningen te importeren.
- 2. Klik op Configureren en vervolgens op Inbraakpreventie.
- 3. Klik op het tabblad IPS bewerken en vervolgens op Importeren.

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	SAS0 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
B- 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. Kies van PC in de vervolgkeuzelijst Importeren.
- 5. Selecteer het bestand waaruit u handtekeningen wilt

Import				2 🔀
Look ja: 📔	CCOSig	1	• • 🗈 🔿	* 🖬 •
105-5208 105-5209 105-5210 105-5211 105-5212 105-5213	.zip .zip .zip .zip .zip .zip .zip	105-5214.zip 105-5215.zip 105-5216.zip		>
File pame:	105-52	17.zip		<u>O</u> pen
Files of type:	All Files	(".")	•	Cancel

importeren.

Dit voorbeeld gebruikt de

nieuwste update die van Cisco.com is gedownload en op de lokale vaste schijf van de PC is opgeslagen.

6. Klik op **Openen**. **Waarschuwing:** vanwege geheugenbeperkingen kunnen slechts een beperkt aantal nieuwe handtekeningen worden toegevoegd bovenop handtekeningen die al zijn ingezet. Als te veel handtekeningen zijn geselecteerd, kan de router mogelijk niet alle nieuwe handtekeningen vanwege gebrek aan geheugen laden.Nadat de bestandslading voor handtekening is voltooid, verschijnt het dialoogvenster IPS-

All Categories	[Select		
E Attack	Name	Deployed	Import		
E-Service	KaZaA v2 UDP Client Probe	Yes	R		
General Service	KaZaA v2 UDP Client Probe	Yes	R		
-DNS	KaZaA v2 UDP Client Probe	Yes	V		
Finger	Gnutella Client Request	Yes	R.		
FTP	Grutella Server Reply	Yes	V		
Ident	Otella File Request	No	Г		
IMAP	Bearshare File Request	No	Г		
NNTP	KaZaA Client Activity	Yes	V		
LPR	Gnucleus File Request	Yes	V		
NTP	Limewire File Request	No	Г		
POP	Morpheus File Request	No			
	Phex File Request	No			
SMTP	Swapper File Request	No			
SNMP	XoloX File Request	No	Г		
	GTK-Gnutella File Request	Yes	R		
File Sharing	Mutella File Request	No	Г		
SOCKS	Hotline Client Login	No	Г		
TETP	Hotine File Transfer	No	Г		
ep2: Merge The specified signatures will Replace All the old signatures deploye	be merged with the signatures already de	eployed on the rou	ter.		

invoer.

- 7. Navigeer door de linkerboomweergave en klik op het aanvinkvakje **Importeren** naast de handtekeningen die u wilt importeren.
- 8. Klik op de knop **Merge** en vervolgens op **OK**.**Opmerking:** De optie Vervangen vervangt de huidige handtekening die op de router is ingesteld, door de handtekeningen die u hebt geselecteerd om te importeren.Zodra u OK klikt, levert de toepassing Cisco PDM de handtekeningen aan de

	Signature Delivery Status	
	Delivering SDF to router	
uter		

Opmerking: Bij het

compileren en laden van handtekeningen wordt gebruik gemaakt van hoge CPU's. Nadat Cisco IOS IPS op de interface is ingeschakeld, start het bestand voor handtekeningen. De router duurt ongeveer vijf minuten om SDF te laden. U kunt proberen de opdracht **Show proces cpu** te gebruiken om het CPU-gebruik van de Cisco IOS-software CLI te bekijken. Probeer echter geen extra opdrachten te gebruiken of andere SDF's te laden terwijl de router SDF's laadt. Dit kan ertoe leiden dat het proces voor het samenstellen van handtekeningen langer duurt (aangezien het CPU-gebruik bij het laden van de SDF dicht bij 100 procent ligt). Het kan nodig zijn om door de lijst met handtekeningen te bladeren en de handtekeningen in te schakelen als deze niet in enabled-status zijn.Het totale aantal handtekeningen is toegenomen tot 519. Dit aantal bevat alle handtekeningen die in het IOS-S193.zip-bestand beschikbaar zijn en behoren tot de subcategorie Bestand delen.



Voor geavanceerde onderwerpen over hoe te om Cisco PDM te gebruiken om de functie van Cisco IOS IPS te beheren, verwijs naar de documentatie van Cisco PDM bij deze URL:

Selecteer Handtekeningen en werk met handtekeningen

Om effectief de juiste handtekeningen voor een netwerk te selecteren moet u een paar dingen over het netwerk weten die u beschermt. Bijgewerkte informatie van de categorie van handtekeningen in Cisco slecht 2.2 en hulp later klanten verder om de juiste reeks handtekeningen te selecteren om het netwerk te beschermen.

Deze categorie is een manier om handtekeningen te groeperen. Het helpt de selectie van handtekeningen te beperken tot een subset van handtekeningen die voor elkaar relevant zijn. Eén handtekening zou tot één categorie kunnen behoren of tot meerdere categorieën kunnen behoren.

Dit zijn de vijf topcategorieën:

- Besturing op basis van het besturingssysteem
- Attack-gebaseerde kenmerkende categorisatie voor aanvallen
- Service-/op service gebaseerde kenmerkende categorisatie

- Layer 2-4 protocol/protocol-gebaseerde gecategorisatie op protocolniveau
- Release-op release gebaseerde kenmerkende categorisatie

Elk van deze categorieën wordt verder onderverdeeld in subcategorieën.

Neem bijvoorbeeld een thuisnetwerk met een breedbandverbinding naar het internet en een VPNtunnel naar het bedrijfsnetwerk. De breedbandrouter heeft Cisco IOS Firewall die op de open (niet-VPN) verbinding met het internet is ingeschakeld om te voorkomen dat een verbinding van het internet afkomstig is en op het thuisnetwerk wordt aangesloten. Al het verkeer dat van het thuisnetwerk naar internet afkomstig is, is toegestaan. Stel dat de gebruiker een op Windows gebaseerde PC gebruikt en toepassingen zoals HTTP (web browsing) en e-mail gebruikt.

De firewall kan zo worden geconfigureerd dat alleen de toepassingen die de gebruiker nodig heeft, door de router kunnen stromen. Dit zal de stroom van ongewenst en potentieel slecht verkeer controleren die door het netwerk kan zich verspreiden. Denk eraan dat de thuisgebruiker geen specifieke service nodig heeft of gebruikt. Als die service door de firewall is toegestaan, is er een mogelijk gat dat een aanval kan gebruiken om door het netwerk te stromen. De beste praktijken maken alleen diensten mogelijk die nodig zijn. Nu is het gemakkelijker om te selecteren welke handtekeningen u kunt toelaten. U hoeft alleen handtekeningen in te schakelen voor de services die u in de firewall kunt gebruiken. In dit voorbeeld omvatten de diensten e-mail en HTTP. Cisco PDM vereenvoudigt deze configuratie.

Om de categorie te gebruiken om de vereiste handtekeningen te selecteren, kies **Service > HTTP** en selecteer alle handtekeningen. Dit selectieproces werkt ook in het dialoogvenster voor de invoer van handtekeningen, waarin u alle HTTP-handtekeningen kunt selecteren en in uw router kunt importeren.

Extra categorieën die moeten worden geselecteerd zijn DNS, NEToverheid/MKB, HTTPS en MTP.

Handtekeningen voor standaard SDF-bestanden bijwerken

De drie per-gebouwde SDF's (aanval-drop.dsf, 128MB.sdf en 256MB.sdf) worden momenteel op Cisco.com gepost op <u>http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup</u> (alleen_geregistreerde klanten). Nieuwe versies van deze bestanden worden gepubliceerd zodra ze beschikbaar zijn. Om routers bij te werken die Cisco IOS IPS met deze standaard SDF's uitvoeren, gaat u naar de website en download de nieuwste versies van deze bestanden.

CLI-procedure

 Kopieer de gedownload bestanden naar de locatie waar de router is ingesteld om deze bestanden te laden. Om te weten te komen waar de router momenteel wordt gevormd, gebruik de show in werking stellen- | in ip ips sdf opdracht.

Router#**show running-config | in ip ips sdf** ip ips sdf location flash://256MB.sdf autosave In dit voorbeeld gebruikt de router 256MB.sdf op de flitser. Het bestand wordt bijgewerkt wanneer u de nieuwe gedownload 256MB.sdf naar de routerflitser kopieert.

2. Herladen van het Cisco IOS IPS-subsysteem om de nieuwe bestanden te starten. Er zijn twee manieren om Cisco IOS IPS te herladen: herladen van de router of opnieuw configureren Cisco IOS IPS om het IOS IPS-subsysteem te activeren om handtekeningen opnieuw te laden. Om Cisco IOS IPS aan te passen verwijder alle IPS-regels van de geconfigureerde interfaces, en pas vervolgens de IPS-regels opnieuw toe op de interfaces. Dit zal het Cisco IOS IPS-systeem activeren om te herladen.

PROCEDURE 2.2

Voltooi deze stappen om de standaard SDFs op de router bij te werken:

- 1. Klik op Configureren en vervolgens op Inbraakpreventie.
- 2. Klik op het tabblad IPS bewerken en vervolgens op Global Settings

IPS Policies			ේ
3 Global Settings		Item Name	Item Value
SDEE Messages		Syslog	Enabled
Cianoturas		SDEE	Enabled
g signatures	-	SDEE Alerts	200
		SDEE Messages	200
		SDEE Subscription	1
		Engine Options	Disabled
		Fail Closed	Disabled
		Derv Action on IPS interface	Disabled
		Chup Event	Disabled
		Timeout	30
		Configured SDF Locations: 4 Add	' Edit 🏦 Delete 🎓 Move Up 🐥 Move Down 🔊 Reload
		flash://sdmips.sdf	
		nasitorizombisur (autosare)	

De bovenkant van de UI toont de mondiale instellingen. De onderste helft van de UI toont momenteel gevormde SDF plaatsen. In dit geval wordt het 256MB.sdf-bestand uit flash-geheugen ingesteld.

3. Kies Bestandsbeheer uit het menu Bestand.Het dialoogvenster File Management

ish:	Name	Size(bytes)	Time Modified
	128MB.sdf	504630	08/25/05 01:37:02
	256MB.sdf	725688	01/28/06 10:40:00
	backup.cfg	5,564	10/07/05 10:10:32
	c180x-advipservicesk9-mz.124-6.T	17,795,940	03/11/06 14:08:26
	common.tar	1,007,616	10/24/05 00:32:16
	home.shtml	1,038	10/24/05 00:32:16
	home.tar	113152	10/24/05 00:32:16
	sdm.tar	4,049,920	10/24/05 00:32:18
	sdmconfig-18x.cfg	1,820	03/04/06 22:15:56
	sdmips.sdf	527028	03/13/06 03:14:42
	securedesktop-ios-3.1.1.27-k9.pkg	1,684,577	03/04/06 22:17:02
	sigcategories.xml	321559	11/11/05 10:49:46
	ssiclient-win-1.0.2.127.pkg	319662	03/04/06 22:17:18

verschijnt.

4. Klik op Bestand laden vanaf een pc.Het dialoogvenster Bestand opslaan als

Save File		2 🛚
Look jn:) SDF	- 🕈 🖆 📰 -
128M8.sc 256M8.sc 256M8.sc attack-dr	af 9 op.sdf	

verschijnt.

5. Kies SDF dat moet worden bijgewerkt en klik op Openen. Het bericht van de Waarschuwing



6. Klik op Ja om het bestaande bestand te vervangen. Een dialoogvenster geeft de voortgang



van het uploadproces weer.

7. Nadat het uploadproces is voltooid, klikt u op **Handtekeningen opnieuw laden** op de SDFlocatie, werkbalk. Deze actie herlaadt de Cisco IOS IPS

👃 IPS Policies		ල් 8
🐻 Global Settings	Item Name	Item Value
G SDEE Messages	Syslog	Enabled
Signatures	 SDEE Alerts SDEE Messages SDEE Subscription Engine Options Fail Closed Use Built-in Signatures (as backup) Deny Action on IPS interface Shun Event Timeout 	200 200 1 Disabled Enabled Disabled 30
		50
	Configured SDF Locations: Add C Ed	sit 🗊 Delete 🏦 Move Up 🦊 Move Down 🔊 Reload Signatu
	Configured SDF Locations: Add C En flash://sdmips.sdf flash://128MB.sdf (autosave)	st 🟦 Delete 🎓 Move Up 🤑 Move Down 🔊 Reload Signatu
	Configured SDF Locations: Add C Ed flash:0sdmips.sdf flash:0128MB.sdf (autosave)	st 👔 Delete 🎓 Move Up 🦊 Move Down 🔊 Reload Signatu

Opmerking: het IOS-Sxxx.zip-pakket bevat alle handtekeningen die Cisco IOS IPS ondersteunt. Uploads naar dit pakket handtekeningen worden op Cisco.com geplaatst zodra ze beschikbaar worden. Zie <u>Stap 2</u> voor het bijwerken van de handtekeningen in dit pakket.

Gerelateerde informatie

- <u>Cisco-inbraakpreventiesysteem</u>
- Security meldingen uit het veld (inclusief Cisco Secure Inbraakdetectie)
- <u>Technische ondersteuning Cisco-systemen</u>