IPS-blokkering configureren met IME

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Netwerkdiagram Configuraties De configuratie van de sensor starten Stop de sensor in het IME Blokken configureren voor Cisco IOS-router Verifiëren Start de aanval en de blokkering Problemen oplossen Tips Gerelateerde informatie

Inleiding

Dit document behandelt de configuratie van het IPS-blokkering (Inbraakpreventiesysteem) met het gebruik van de IPS Manager Express (IME). IME en IPS Sensors worden gebruikt om een Ciscorouter te beheren voor blokkering. Denk aan deze punten wanneer u deze configuratie bekijkt:

- Installeer de sensor en controleer of de sensor goed werkt.
- Maak de gebruikersinterface-span aan de router buiten de interface.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3

Cisco IOS-router met Cisco IOS-softwarerelease 12.4

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

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd.



Configuraties

Dit document gebruikt deze configuraties.

- Routerlicht
- Routerhuis



```
!
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
!
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
call rsvp-sync
!
!
1
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
1
!
!
interface FastEthernet0/0
ip address 10.100.100.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface BRI4/0
no ip address
shutdown
interface BRI4/1
no ip address
shutdown
!
interface BRI4/2
no ip address
shutdown
!
interface BRI4/3
no ip address
shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.100.1
ip http server
ip pim bidir-enable
1
1
dial-peer cor custom
!
1
line con 0
line 97 108
line aux 0
line vty 0 4
login
!
end
```

Routerhuis

```
Current configuration : 939 bytes
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
1
logging queue-limit 100
enable password cisco
ip subnet-zero
1
1
no ip cef
no ip domain lookup
1
ip audit notify log
ip audit po max-events 100
!
1
no voice hpi capture buffer
no voice hpi capture destination
!
1
1
interface FastEthernet0/0
 ip address 10.66.79.210 255.255.255.224
 duplex auto
 speed auto
1
interface FastEthernet0/1
ip address 10.100.100.1 255.255.255.0
ip access-group IDS_FastEthernet0/1_in_0 in
!--- After you configure blocking, !--- IDS Sensor
inserts this line. duplex auto speed auto ! interface
ATM1/0 no ip address shutdown no atm ilmi-keepalive ! ip
classless ip route 0.0.0.0 0.0.0.0 10.66.79.193
ip route 1.1.1.0 255.255.255.0 10.100.100.2
no ip http server
no ip http secure-server
1
ip access-list extended IDS_FastEthernet0/1_in_0
permit ip host 10.66.79.195 any
permit ip any any
!--- After you configure blocking, !--- IDS Sensor
inserts this line. ! call rsvp-sync ! ! mgcp profile
default ! ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 exec-timeout 0 0 password cisco
login
line vty 5 15
login
!
!
end
```

De configuratie van de sensor starten

Volg deze stappen om de configuratie van de Sensor te starten.

- 1. Als dit de eerste keer is dat u in de sensor logt, moet u **cisco** invoeren als de gebruikersnaam en **cisco** als het wachtwoord.
- 2. Wanneer het systeem u vraagt, wijzigt u uw wachtwoord. **Opmerking:** Cisco123 is een woordenboek en is niet toegestaan in het systeem.
- 3. Type **installatie** en volg de aanwijzingen in het systeem op om de basisparameters voor de sensoren in te stellen.
- 4. Voer deze informatie in:

```
sensor5#setup
    --- System Configuration Dialog ---
!--- At any point you may enter a question mark '?' for help. !--- Use ctrl-c to abort the
configuration dialog at any prompt. !--- Default settings are in square brackets '[]'.
Current time: Thu Oct 22 21:19:51 2009
Setup Configuration last modified:
Enter host name[sensor]:
Enter IP interface[10.66.79.195/24,10.66.79.193]:
Modify current access list?[no]:
Current access list entries:
!--- permit the ip address of workstation or network with IME Permit: 10.66.79.0/24
Permit:
Modify system clock settings?[no]:
 Modify summer time settings?[no]:
   Use USA SummerTime Defaults?[yes]:
   Recurring, Date or Disable?[Recurring]:
   Start Month[march]:
   Start Week[second]:
   Start Day[sunday]:
   Start Time[02:00:00]:
   End Month[november]:
   End Week[first]:
   End Day[sunday]:
   End Time[02:00:00]:
   DST Zone[]:
   Offset[60]:
 Modify system timezone?[no]:
   Timezone[UTC]:
   UTC Offset[0]:
 Use NTP?[no]: yes
   NTP Server IP Address[]:
   Use NTP Authentication?[no]: yes
     NTP Key ID[]: 1
     NTP Key Value[]: 8675309
```

- 5. Bewaar de configuratie.Het kan een paar minuten duren voor de Sensor de configuratie opslaat.
 - [0] Go to the command prompt without saving this config.
 - [1] Return back to the setup without saving this config.
 - [2] Save this configuration and exit setup.

Enter your selection[2]: 2

Stop de sensor in het IME

Volg deze stappen om de sensor aan de IME toe te voegen.

- 1. Ga naar de Windows PC, die de IPS Manager Express heeft geïnstalleerd en de **IPS Manager Express** opent.
- 2. Kies startpunt > Toevoegen.
- 3. Typ deze informatie en klik op OK om de configuratie te
 - voltooien.

evices	라 무 Home > Devices > De	evice List	
En Elist	Add Z Edit Del	lete 🛛 🕨 Start 👻 📕 Stop	🔹 🅎 Status
	Time Device Name	IP Address Device	Type Event
	C Edit Device		×
	Sensor Name:	Sensor5	
	Sensor IP Address:	10.66.79.195	
	User Name:	cisco]
	Password:	•••••]
	Web Server Port:	443	
	Communication protoc	ol	
	 Use encrypted cor 	nnection (https)	
	Use non-encrypted	d connection (http)	
	Event Start Time (UTC) ———	
	Most Recent Alerts	s	
	Start Date (YYYY:N	MM:DD):	
	Start Time (HH:MM	1:55):	
	Exclude alerts of the f	ollowing severity level(s)	
	Informational	Low Medium High	

4. Kies **Apparaten > sensor5** om de status van de Sensor te controleren en klik dan met de rechtermuisknop om de **Status** te kiezen.Zorg dat u het *abonnement* kunt zien *openen.* bericht.



Blokken configureren voor Cisco IOS-router

Voltooi deze stappen om de blokkering voor de Cisco IOS-route te configureren:

- 1. Open uw webbrowser vanaf de IME-pc en ga naar https://10.66.79.195.
- 2. Klik op **OK** om het HTTPS-certificaat te aanvaarden dat van de Sensor is gedownload.
- 3. Voer in het inlogvenster **cisco** in voor de gebruikersnaam en **123cisco123** voor het wachtwoord.Deze IME-beheerinterface verschijnt:

🚮 Home <u>浸</u> Configuration 🌆 E	ven	t Monitoring) 🚮 Reports 梈 He	lp					
Configuration > Corp-IPS > Policie	5 >	Signatur	e Definitions > sig0 > /	Active Sign	atures				
Corp-IPS									
IPS Policies Signature Definitions	1	C Edit A	ictions 🕥 Enable 💋 Dis	sable 🔇 Re	estore Default	Show	Events 🔹	14	G M
🕀 🙀 sig0		Filter: Sig	JID 💌						
Active Signatures		ID ±1	Name	Enabled	Severity	Fidelity	Base	Si	gnatu
DDo5		1000/0	ID options, Pad Option		Contra Cala	Rating	10	Al	ert ar
DoS		1004/0	IP options-bad Option IP options-Loose Sour		 Infor High 	100	100	54	Alert
🖉 Email	Ш	1006/0	IP options-Strict Sourc		High	100	100	=	Alert
S Instant Messaning		1007/0	IPv6 over IPv4		L Infor	100	25	£7.	Alert
22/L3/L4 Protocol		1101/0	Unknown IP Protocol		💰 Infor	75	18	17	Alert
	Ш	1102/0	Impossible IP Packet		High	100	100	=	Alert
冠 OS	Ш	1104/0	IP Localhost Source S		High	100	100	£7	Alert
Other Services	Ш	1107/0	RFC 1918 Addresses		🚹 Infor	100	25	27	Alert
P2P	Ш	1108/0	IP Packet with Proto 11	 Image: A start of the start of	High	100	100	£7	Alert
Beleases		1109/0	Cisco IOS Interface DoS		🧿 Medium	75	56	57	Alert
		1109/1	Cisco IOS Interface DoS		🤗 Medium	75	56	£7.	Alert
		1109/2	Cisco IOS Interface DoS		😑 Medium	75	56	=	Alert
	4	1109/3	Cisco IOS Interface DoS		😑 Medium	75	56	£7.	Alert
Event Action Rules		1200/0	IP Fragmentation Buff		🔒 Infor	100	25	=	Alert
		1201/0	IP Fragment Overlap		👗 Infor	100	25	=	Alert
🖻 🔀 Anomaly Detections		1202/0	IP Fragment Overrun		High	100	100	-	Alert
	-11	100010	ID F	5.0		100	100	1000	1.1

- 4. Klik in het tabblad Configuration op actieve handtekeningen.
- 5. Klik vervolgens op **Wizard**

Configuration > Corp-IPS > Policie	s > Signature Definitions > sig0 >	Act	<u>8</u>	
Corp-IP5				🔅 Refresh
IPS Policies Signature Definitions Active Signatures Adware/Spyware Attack DDoS	ID +1 Name 1000/0 IP options-Bad Option)isab E	lelo Filter Gear	Q Signature Wizard
i 🛅 DoS	1004/0 IP optione-Loose Sour	200 - F		

Opmerking: het vorige screenshot is door de beperkte ruimte in twee delen gesneden.

6. Kies **ja** en **string TCP** als Signature engine. Klik op **Volgende**.

😨 Custom Signature Wi	zard
N Case Sector	Welcome
	Welcome to the Custom Signature Wizard. This wizard will guide you through the process of defining a custom signature.
	Do you know which Signature Engine you want to use for the custom signature?
	(⊙ Yes
THE SEAL	Select Engine: String TCP
mail parages	○ No

7. U kunt deze informatie als standaard achterlaten of uw eigen handtekening, handtekening en

opmerkingen van de gebruiker invoeren. Klik op **Volgende**.

Custom Signature Wi	zard		Ľ
A Constant March 1946	Signature Identification		
	Signature identification param signature behavior. You must default values, but each requi	eters identify and describe the signature, but do not affect the specify a Signature ID and SubSignature ID. You can override the red value must be unique (not used by another signature).	
	Signature ID: 60000		
En to partie	SubSignature ID: 0		
Lange C	Signature Name: String.	tcp	
tititit	Alert Notes: My Sig	Info	
	User Comments: Sig Co	mment	

8. Kies Event Action en kies Waarschuwen en Aanvraag Blokhost. Klik op Volgende om verder te

gaan Signature Wiza	rð		×
	Engine Specific Parameters Engine-specific parameters dete to fire. You can set the followin	ermine what the signature looks for and what cau g String TCP engine parameters used for this sign	uses the signature nature.
Email FTP VolP Web Pages	Name Vert Action Strip Telnet Options Specify Min Match Length Regex String Service Ports Direction Specify Exact Match Offset Specify Max Match Offset Specify Min Match Offset Specify Min Match Offset Swap Attacker Victim	Value Select item(s) Deny Attacker Inline Deny Attacker Service Pair Inline Deny Attacker Victim Pair Inline Deny Connection Inline Deny Packet Inline Log Attacker Packets Log Pair Packets Log Victim Packets Produce Alert Produce Verbose Alert Request Block Host Request SNMP Trap Reset TCP Connection OK	Select All Select None
	Parameter uses the Def Parameter uses a User-	ault Value. Click the value field to edit the value Defined Value. Click the icon to restore the defa	ult value.

9. Voer een reguliere expressie in, die in dit voorbeeld *testattack* is, voer **23** voor servicepoorten in, kies **To Service** for the Direction en klik op **Next** om verder te gaan.

Engine Specific Parameters Engine-specific parameters determine what the signature looks for and what cause to fire. You can get the following String TCB assigns parameters used for this signal					
Engine-specific parameters determine what the signature looks for and what cause to five. You can get the following String TCR angles parameters used for this signal.					
to fire, you can set the following String TCP engine parameters used for this signal	Engine-specific parameters determine what the signature looks for and what causes the signature to fire. You can set the following String TCP engine parameters used for this signature.				
Name Value					
Event Action Produce Alert Request Block H	iost				
Strip Telnet Options No					
Regex String testattack					
Service Ports 23					
Direction To Service					
Specify Exact Match Offset No					
Specify Min Match Offset No					
Swap Attacker Victim No					

10. U kunt deze informatie als standaard opgeven. Klik op **Volgende**.

😨 Custom Signature V	izar d	X
	Alert Response	
	You can assign the following values to this signature that reflect both your confidence in the fide of the signature and the severity of the attack it represents. The Signature Fidelity Rating is an number from 0 to 100, with 100 reflecting the most confidence in this signature. This number is u to help calculate the Risk Rating, which helps determine what actions result from the firing of this signature.	elity y used is
ET MAN	Signature Fidelity Rating: 75	
pages pages	Severity of the Alert: High	

11. Klik op **Voltooien** om de wizard te voltooien.



12. Kies Configuration > Sg0 > Active Signatures om de nieuwe handtekening te plaatsen onder Sig ID of Sig Name. Klik op Bewerken om de handtekening te

Ivame	Value
⊟-Signature Definition	
Signature ID	60000
SubSignature ID	0
- 🖌 Alert Severity	Medium
- 😿 Sig Fidelity Rating	75
- 🖾 Promiscuous Delta	0
Sig Description	
- 🗹 Signature Name	String.tcp
- 🖌 Alert Notes	My Sig Info
- 🗹 User Comments	Sig Comment
	0
Release	custom
🖹 -Engine	String TCP
- 🗹 Event Action	Produce Alert Request Block Hos
II Strip Telnet Options	No
Specify Min Match Length	No
-Regex String	testattack
Service Ports	23
- Section	To Service
Specify Exact Match Offset	No
- Specify Max Match Offset	No
-Specify Min Match Offset	No
	No
C. Durch Country	

- 13. Klik op **OK** nadat u hebt bevestigd en klik op de knop **Toepassen** om de handtekening op de sensor toe te passen.
- 14. Klik onder Sensor Management op **Block** van het tabblad Configuration. Kies in het linker venster de optie **Eigenschappen blokkeren** en controleer **Blokken inschakelen**.



15. Ga nu vanuit het linker deelvenster naar **Apparaatinlogprofiel**. Klik op **Toevoegen** om een nieuw profiel te maken. Klik na het maken op **OK** en **Toepassen** om te sensor en verder te gaan.

Certificates	S Add Device Login	n Profile 🛛 👔
Blocking Properties	Profile Name: Username (optional):	Router Test
Blocking Devices Router Blocking Device In Cat 6K Blocking Device In Master Blocking Sensor SNMP Someral Configuration	Login Password (op New Password: Confirm New Pass	sword:
Configuration Traps Configuration External Product Interfaces Passwords Licensing Sensor Health The senior Unrichles	Enable Password (o New Password: Confirm New Pass	sword:
Auto/Cisco.com Update	ОК	Cancel Help

16. De volgende stap is router als blokkerend apparaat te configureren. Kies in het linker venster een blokkerend apparaat en klik op Toevoegen om deze informatie toe te voegen. Klik vervolgens op OK en

Server Certificate	O Add Blocking Device	
b Blocking		
- 🚺 Blocking Properties		
Device Login Profiles	IP Address:	10,10,10,10
Blocking Devices	Sensor's NAT Address (optic	onal):
- 🔏 Cat 6K Blocking Device Inl	Device Login Profile:	Router
Master Blocking Sensor		
SNMP	Device Type:	Cisco Router
	Response Capabilities: 💽	Block 🔄 Rate Limit
External Product Interfaces	Communication:	Telnet
🗆 Passwords		i chi
Licensing		
Sensor Health	ОК С	Cancel Help
JP Logging Variables		

17. Stel nu vanuit het linker deelvenster de interfaces van het blokkerende apparaat in. Voeg de informatie toe, klik op **OK** en **Toepassen**.

Certificates	Q Add Router Blocking	Device Interface	X
Trusted Hosts	Pouter Blocking Devices	10 100 100 1	1
Blocking Blocking Properties		5-04	
Device Login Profiles	Blocking Interface:	Feu/I	-
Blocking Devices	Direction:	In	~
Cat 6K Blocking Device Interface	Pre-Block ACL (optional):	blaster	
Master Blocking Sensor	Post-Block ACL (optional):	101	
General Configuration Traps Configuration External Product Interfaces		ncel Help	

Verifiëren

Start de aanval en de blokkering

Voltooi deze stappen om de aanval te starten en het blokkeren:

- 1. Voordat u de aanval start, ga naar de IME, kies **Bewaking van gebeurtenis > Verlaten Attacks Beeld** en kies de sensor aan de rechterkant.
- 2. Telnet aan routerhuis en verifieert de communicatie van de server met deze opdrachten.

Li	ine	User	Host(s)	Idle	Location
* 0	con	0	idle	00:00:00	
226	vty	0	idle	00:00:17	10.66.79.195

```
house#show access-list
Extended IP access list IDS_FastEthernet0/1_in_0
  permit ip host 10.66.79.195 any
  permit ip any any (12 matches)
house#
```

3. Van routerlicht, telnet tot routerhuis en type **testattack**.Sluit of **<space>** of **<enter>** om uw Telnet-sessie te resetten.

```
light#telnet 10.100.100.1
Trying 10.100.100.1 ... Open
```

```
User Access Verification

Password:

house>en

Password:

house#testattack

[Connection to 10.100.100.1 lost]

!--- Host 10.100.100.2 has been blocked due to the !--- signature "testattack"

triggered.
```

4. Telnet om Huis van de router te gebruiken en het bevel **van de** show **toegang-lijst** te gebruiken zoals hier getoond.

```
house#show access-list
Extended IP access list IDS_FastEthernet0/1_in_0
10 permit ip host 10.66.79.195 any
20 deny ip host 10.100.100.2 any (71 matches)
```

30 permit ip any any

5. Vanuit het Dashboard van het IDS Event Viewer verschijnt de Rode Alarm zodra de aanval is gestart.

Date	Time	Sig. Name	Sig. ID			
Device: Corp-IPS (188 items)					
🚊 Severity: high (188 items)						
10/23/2009	09:59:13	String.tcp	60000/0			
	09:59:02	ZOTOB Worm Activity	5570/0			
	09:58:57	Anig Worm File Tran	5599/0			
	09:59:00	Anig Worm File Tran	5599/0			
	09:58:58	Anig Worm File Tran	5599/0			
	09:59:17	Nachi Worm ICMP E	2158/0			

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

<u>Tips</u>

Gebruik deze tips voor probleemoplossing:

• Vanaf de Sensor kijk naar de **show statistics network-access** output en zorg ervoor dat de staat"actief is. Van de console of SSH tot de sensor, wordt deze informatie bekeken: sensor5#show statistics network-access

```
Current Configuration
 AllowSensorShun = false
 ShunMaxEntries = 100
 NetDevice
   Type = Cisco
   IP = 10.66.79.210
   NATAddr = 0.0.0.0
   Communications = telnet
    ShunInterface
     InterfaceName = FastEthernet0/1
     InterfaceDirection = in
State
 ShunEnable = true
 NetDevice
   IP = 10.66.79.210
   AclSupport = uses Named ACLs
   State = Active
 ShunnedAddr
   Host
     IP = 10.100.100.2
     ShunMinutes = 15
     MinutesRemaining = 12
sensor5#
```

 Zorg ervoor dat de communicatieparameter aangeeft dat het juiste protocol wordt gebruikt, zoals telnet of SSH met 3DES. U kunt een handmatige SSH of telnet van een SSH/telnetclient op een pc proberen om de gebruikersnaam en de wachtwoordreferenties te controleren correct zijn. Probeer dan om net of SSH van de Sensor zelf naar de router te tellen en zie of u met succes kunt inloggen op de router.

Gerelateerde informatie

- <u>Cisco-pagina voor beveiligde inbraakpreventie</u>
- Technische ondersteuning en documentatie Cisco Systems