IPS TCP opnieuw instellen met IME

Inhoud

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

Inleiding

Dit document behandelt de configuratie van het IPS (Inbraakpreventiesysteem) TCP-reset met behulp van IPS Manager Express (IME). IME en IPS Sensors worden gebruikt om een Ciscorouter voor TCP-reset te beheren. Denk bij het bekijken van deze configuratie aan deze punten:

- 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 <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Configureren

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Configuraties

Dit document gebruikt de configuraties die hier worden weergegeven.

- Routerlicht
- <u>Routerhuis</u>

Routerlicht

```
Current configuration : 906 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
hostname light
1
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
!
!
1
ip ssh time-out 120
ip ssh authentication-retries 3
1
call rsvp-sync
!
1
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
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
1
interface BRI4/3
no ip address
shutdown
1
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
1
hostname house
1
logging queue-limit 100
enable password cisco
!
ip subnet-zero
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
!
interface FastEthernet0/1
ip address 10.100.100.1 255.255.255.0
 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
1
1
call rsvp-sync
!
mgcp profile default
1
1
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 inlogt, moet u **cisco** invoeren als de gebruikersnaam en **cisco** als wachtwoord.
- 2. Wanneer het systeem u vraagt, wijzigt u uw wachtwoord. **Opmerking:** Cisco123 is een woordenboek en is niet toegestaan in het systeem.
- 3. Stel het type in en vul de systeemmelding in 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 Configuration:

```
networkParams
ipAddress 10.66.79.195
netmask 255.255.255.224
defaultGateway 10.66.79.193
hostname Corp-IPS
telnetOption enabled
!--- Permit the IP address of workstation or network with IME accessList ipAddress
10.66.79.0 netmask 255.255.255.0
exit
timeParams
summerTimeParams
active-selection none
exit.
exit
service webServer
general
ports 443
exit
exit
```

- Bewaar de configuratie. Het kan een paar minuten duren voordat 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.

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 open de IPS Manager Express.
- 2. Kies startpunt > Toevoegen

evices c	구 면 Home > Devices	> Devic	ce List	11-22 AP	-
🚰 Device List	🗣 Add 🗹 Edit 🗊	Delete	🕨 🕨 Start 👻	📕 Stop 👻 🔍	👌 Status
	Time Device N	ame	IP Address	Device Type	Event
	C Edit Device				X
	Sensor Name:	ļ	Corp-IPS		
	Sensor IP Addres		10.66.79.195		
	User Name:	6	cisco		
	Password:	6			
	Web Server Port:		443		
	Communication pr	otocol –			
	O Use encrypte	l connec	tion (https)		
	Use non-encr	pted co	nnection (http)		
	Event Start Time	UTC) —			
	Most Recent /	lerts			
	Start Date (Y)	YY:MMG	DD)::		
	Start Time (H	I:MM:SS): :	:	
	Exclude alerts of	he follow	wing severity lev	el(s)	
	Informational	Lov		High	

- 3. Typ deze informatie en klik op **OK** om de configuratie te voltooien.
- 4. Kies Apparaten > Corp-IPS om de status van de sensor te controleren en klik met de rechtermuisknop om de status van het apparaat te kiezen.Zorg ervoor dat u abonnement kunt zien

geopend.



Configureer de TCP-reset voor Cisco IOS-router

Voltooi deze stappen om de TCP-reset voor de Cisco IOS-router 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 🐉 Configuration 🌆 Ex	ent Monitor	ing 🚮 Reports 🧖 He	lp				
Configuration > Corp-IPS > Policie	s > Signat	ure Definitions > sig0 > a	Active Sigr	atures			
Corp-IPS							
IPS Policies Signature Definitions	C Edi	t Actions 🕥 Enable 💋 Di	sable 🔇 R	estore Default	Show	Events 🔹	1 🗞 M
Active Signatures	Filter:	Sig ID 💉					
Adware/Spyware	ID A	Mama	Enabled	Sought	Fidelity	Base	Signatu
🛛 🖀 Attack	10	- Maine	Linguieu	Devency	Rating	RR	Alert an
DDo5	1000/0	IP options-Bad Option		👔 Infor	75	18	Alert
DoS G Fanal	1004/0	IP options-Loose Sour		High	100	100	Alert
	1006/0	IP options-Strict Sourc	~	High	100	100	Alert
S Instant Messaging	1007/0	IPv6 over IPv4		🔥 Infor	100	25	Alert
L2/L3/L4 Protocol	1101/0	Unknown IP Protocol	V	🔥 Infor	75	18	Alert
	1102/0	Impossible IP Packet		High	100	100	Alert
🧏 OS	1104/0	IP Localhost Source S	V	High	100	100	Alert
- Services	1107/0	RFC 1918 Addresses		🔥 Infor	100	25	Alert
P2P	1108/0	IP Packet with Proto 11		High	100	100	Alert
Reconnaissance	1109/0	Cisco IOS Interface DoS		Medium	75	56	Alert
Releases	1109/1	Cisco IOS Interface DoS		Medium	75	56	Alert
Web Server	1109/2	Cisco IOS Interface DoS		😑 Medium	75	56	Alert
All Signatures	1109/3	Cisco IOS Interface DoS		😑 Medium	75	56	Alert
Event Action Rules	1200/0	IP Fragmentation Buff	V	i Infor	100	25	Alert
🖓 rules0	1201/0	IP Fragment Overlap		i Infor	100	25	Alert
😑 🔂 Anomaly Detections	1202/0	IP Fragment Overrun		High	100	100	Alert
	1 100010	ID 5	57		100	100	07 11 1

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

Configuration > Corn-IPS > Policies	> Signature Definitions > sign >	Act	4	
Corp-IP5	> signature permittans > sign	Het		🔅 Refresh
Active Signatures Active Signatures Adware/Spyware Attack DDoS DoS	Edit Actions Enable Filter: Sig ID ID *1 Name 1000/0 IP options-Bad Option	Disab E	lelo Filter Cear	Q Signature Wizard

6. In de wizard kiest u **Ja** en kiest u **TCP** als de Signature-motor. Klik op **Volgende**.

😨 Custom Signature Wiza	rd
N Constanting	Welcome
	Welcome to the Custom Signature Wizard. This wizard will guide you through the pro- a custom signature. Do you know which Signature Engine you want to use for the custom signature?
Numda ages Net Pages King pages	Select Engine: String TCP

7. U kunt deze informatie als voorbeeld geven of uw eigen handtekening, de naam van de handtekening en de opmerkingen van de gebruiker invoeren. Klik op

Volgende.	
-----------	--

🖸 Custom Signature Wiza	rd	X
VIII III	Signature Identification	
	Signature identification parameters identify and describe the signature behavior. You must specify a Signature ID and Su default values, but each required value must be unique (not	e signature, but do not affect the bSignature ID. You can override the t used by another signature).
	Signature ID: 60000	
E TAKO PARA	SubSignature ID: 0	
ST TROUGHT	Signature Name: String.tcp	
1111111	Alert Notes: My Sig Info	
THE	User Comments: Sig Comment	

8. Kies Event Action, en kies Waarschuwen en Reset TCP verbinding produceren. Klik op OK en vervolgens op Volgende om verder te

	Engine Specific Paran	meters	
	Engine-specific parameter to fire. You can set the f	ers determine what the signature looks for and what ca following String TCP engine parameters used for this sig	auses the signature gnature.
	Name	Value	
	₩ Event Action	Select item(s)	×
Email FTP VolP Web	Specify Min Match Le Regex String Service Ports Direction Specify Exact Match Specify Max Mat Specify Min Match Specify	Joins Deny Attacker Inline ength Deny Attacker Service Pair Inline Deny Attacker Victim Pair Inline Deny Connection Inline Deny Packet Inline Deny Packet Inline Deny Packet Inline Log Pair Packets Log Pair Packets Log Victim Packets ch Offset Produce Alert Produce Verbose Alert Produce Verbose Alert Request Block Host Request SNMP Tran Ø Reset TCP Connection OK	Select All Select None
R 9-	Parameter uses	the Default Value. Click the value field to edit the value	e. ault value.

9. Voer een reguliere expressie in en in dit voorbeeld wordt testattack gebruikt. Voer 23 in voor servicepoorten, kies voor de service voor de draairichting en klik op Volgende om verder te gaan.

Con Marca State	Engine Specific Parameters		
	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 Reset TCP Connection	
	Strip Telnet Options	No	
	Specify Min Match Length	No	
	Regex String	testattack	
	-Service Ports	23	
1711171	- In Direction	To Service	
+++++++	Specify Exact Match Offset	No	
111111		No	
	Specify Min Match Offset	No	
	Swap Attacker Victim	No	

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

😨 Custom Signature Wiz	ar d	\mathbf{x}
A DESCRIPTION	Alert Response	
	You can assign the following values to this signature that reflect both your confidence in the of the signature and the severity of the attack it represents. The Signature Fidelity Rating is number from 0 to 100, with 100 reflecting the most confidence in this signature. This number to help calculate the Risk Rating, which helps determine what actions result from the firing or signature.	e fidelity s any er is used of this
THE SEAL	Signature Fidelity Rating: 75	
Hand Contract of the second	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-naam**. Klik op **Bewerken** om de handtekeningen te bekijken.

Name	Value
 Signature Definition 	
Signature ID	60000
SubSignature ID	0
😿 Alert Severity	Medium
😿 Sig Fidelity Rating	75
🖬 Promiscuous Delta	0
😿 Signature Name	string.tcp
Alert Notes	My Sig Info
Ser Comments	Sig Comment
🖸 Alert Traits	0
🖸 Release	custom
÷ Engine	String TCP
Event Action	Produce Alert Reset TCP Connection
Strip Telnet Options	No
Specify Min Match Length	No
Regex String	testattack
Service Ports	23
😿 Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	No
Specify Min Match Offset	No
Swap Attacker Victim	No
A Burt Caustre	
 Parameter uses the Default Value. Click the value Parameter uses a User-Defined Value. Click the ic 	e field to edit the value. I on to restore the default value.
ОК	Cancel Help

13. Klik op **OK** nadat u hebt bevestigd en klik op de knop **Toepassen** om de handtekening op de sensor toe te passen.

Verifiëren

Start de aanval en de TCP-reset

Voltooi deze stappen om de aanval te starten en de TCP-reset uit te voeren:

- 1. Voordat u de aanval start, gaat u naar de IME, kiest u Event Monitoring > Dropped Attacks View en kiest u de sensor aan de rechterkant.
- 2. Van het Licht van de router, van het telnet tot het Huis van de router en ga **testattack** in.Sluit of **<space>** of **<enter>** om uw Telnet-sessie te resetten.

```
User Access Verification

Password:

house>en

Password:

house#testattack

[Connection to 10.100.100.1 closed by foreign host]
```

- !--- Telnet session has been reset due to the !--- signature "String.tcp" triggered.
- Vanuit het Dashboard van het IPS 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)		
	09:59:13	String.tcp	60000/0
	09:59:02	ZOTOB Worm Activity	5570/0
-10/23/2009	09:58:57	Anig Worm File Tran	5599/0
	09:59:00	Anig Worm File Tran	5599/0
-10/23/2009	09:58:58	Anig Worm File Tran	5599/0
-10/23/2009	09:59:17	Nachi Worm ICMP E	2158/0

Problemen oplossen

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

Tips

Gebruik deze tips voor probleemoplossing:

 Shunning werkt uit de bevels- en controlepoort om de controlelijsten van de routertoegang (ACL's) opnieuw te programmeren. De TCP resets worden verzonden vanuit de snuifinterface van de sensor. Wanneer u span in de switch instelt, gebruikt u de opdracht set span <src_mod/src_port><dest_mod/dest_port>, waarbij beide inkomende pakketten zijn ingeschakeld zoals hier wordt getoond.

```
banana (enable) set span 2/12 3/6 both inpkts enable
Overwrote Port 3/6 to monitor transmit/receive traffic of Port 2/12
Incoming Packets enabled. Learning enabled. Multicast enabled.
banana (enable)
banana (enable)
banana (enable) show span
Destination : Port 3/6
!--- connect to sniffing interface of the sensor
Admin Source : Port 2/12
!--- connect to FastEthernet0/0 of Router House
Oper Source : Port 2/12
Direction : transmit/receive
Incoming Packets: enabled
Multicast : enabled
```

 Als de TCP-reset werkt, controleer of het alarm is geactiveerd voor het handelstype TCP Reset. Als het alarm verschijnt, controleer dan of het signatuur type is ingesteld op TCP resetten.Meld u aan met behulp van de serviceklasse om deze opdracht te worstelen en uit te geven. Deze opdracht neemt aan dat de sensatieinterface op eth0 is ingesteld. [root@sensor1 root]#tcpdump -i eth0 -n **Opmerking:** Honderd tcp resets worden naar het slachtoffer/doelwit gestuurd en 100 worden naar de aanvaller/cliënt gestuurd.Dit is een voorbeeld-uitvoer:

```
03:06:00.598777 64.104.209.205.1409 >
10.66.79.38.telnet: R 107:107(0) ack 72 win 0
03:06:00.598794 64.104.209.205.1409 >
10.66.79.38.telnet: R 108:108(0) ack 72 win 0
```

03:06:00.599360 10.66.79.38.telnet >
64.104.209.205.1409: R 72:72(0) ack 46 win 0
03:06:00.599377 10.66.79.38.telnet >
64.104.209.205.1409: R 73:73(0) ack 46 win 0

Gerelateerde informatie

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