Configurazione del blocco IPS con l'IME

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Esempio di rete Configurazioni Avvia la configurazione del sensore Aggiungere il sensore all'IME Configurazione del blocco per il router Cisco IOS Verifica Lanciare l'attacco e il blocco Risoluzione dei problemi Suggerimenti Informazioni correlate

Introduzione

In questo documento viene descritta la configurazione del blocco IPS (Intrusion Prevention System) tramite l'utilizzo dell'IME (Intrusion Prevention System). I sensori IME e IPS vengono utilizzati per gestire un router Cisco per il blocco. Tenere presente quanto segue quando si considera questa configurazione:

- Installare il sensore e accertarsi che funzioni correttamente.
- Estendere l'interfaccia di sniffing al router esterno all'interfaccia.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IPS Manager Express 7.0
- Sensore Cisco IPS 7.0(0.88)E3
- Router Cisco IOS[®] con software Cisco IOS versione 12.4

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

Configurazione

Esempio di rete

Nel documento viene usata questa impostazione di rete.



Configurazioni

Nel documento vengono usate queste configurazioni.

- Luce router
- Router House

Luce router

```
Current configuration : 906 bytes
!
version 12.4
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
1
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
!
!
!
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
1
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
!
dial-peer cor custom
1
1
line con 0
line 97 108
line aux 0
line vty 0 4
```

```
login
```

! end

Router House

```
Current configuration : 939 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname house
logging queue-limit 100
enable password cisco
!
ip subnet-zero
!
1
no ip cef
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
!
1
no voice hpi capture buffer
no voice hpi capture destination
1
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
!
!
```

Avvia la configurazione del sensore

Completare questa procedura per avviare la configurazione del sensore.

- Al primo accesso al sensore, è necessario immettere cisco come nome utente e cisco come password.
- Quando il sistema chiede di cambiare la password. Nota: Cisco123 è una parola del dizionario e non è consentita nel sistema.
- 3. Digitare setup e seguire il prompt di sistema per impostare i parametri di base per i sensori.
- 4. Immettere le informazioni seguenti:

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. Salvare la configurazione.Il salvataggio della configurazione da parte del sensore può richiedere alcuni minuti.

[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.

Aggiungere il sensore all'IME

Completare questa procedura per aggiungere il sensore all'IME.

- 1. Passare al PC Windows, in cui è stato installato IPS Manager Express e aprire **IPS Manager Express**.
- 2. Scegliete Home > Aggiungi.
- 3. Digitare queste informazioni e fare clic su **OK** per completare la

<i>c</i> .	
contial	Iraziona
connigu	

Devices	리 무 Home > Devices > D)evice List	440.0
🚰 Device List	Add Z Edit 🗊 De	elete 🛛 🕨 Start 👻 📕 Stop 👻	🔹 🗞 Status
	Time Device Name	IP Address Device Ty	/pe Event
	😨 Edit Device		
	Sensor Name:	Sensor5	
	Sensor IP Address:	10.66.79.195	
	User Name:	cisco	
	Password:	•••••	
	Web Server Port:	443	
	Communication protoc	col	
	O Use encrypted co	nnection (https)	
	O Use non-encrypte	ed connection (http)	
	Event Start Time (UT)	o	
	Most Recent Alert	c, ts	
	Start Date (YYYY:	MM(DD): : : :	
	Start Time (HH:MI	M(SS):	
	Exclude alerts of the l	following severity level(s)	

 Scegliere Dispositivi > sensore5 per verificare lo stato del sensore, quindi fare clic con il pulsante destro del mouse per scegliere Stato. Verificare che la sottoscrizione sia stata aperta correttamente. messaggio.



Configurazione del blocco per il router Cisco IOS

Completare questa procedura per configurare il blocco per il router Cisco IOS:.

- 1. Dal PC IME, aprire il browser Web e visitare il sito https://10.66.79.195.
- 2. Fare clic su **OK** per accettare il certificato HTTPS scaricato dal sensore.
- Nella finestra Login, immettere cisco come nome utente e 123cisco123 come password.Viene visualizzata la seguente interfaccia di gestione IME:

Home 💦 Configuration 🌆 Ev	ent Monitorin	g 🚮 Reports 🦻 He	lp				
Configuration > Corp-IPS > Policies	s > Signatu	re Definitions > sig0 > /	Active Sigr	natures			
Corp-IPS							
IPS Policies Signature Definitions	C Edit	Actions 🥥 Enable 💋 Dis	sable 🔇 R	estore Default	Show	Events +	1 🗞 M
😑 🥁 sig0	Filter: Si	Filter: Sig ID					
Mattive Signatures	ID +1	Name	Enabled	Severity	Fidelity	Base	Signatu
DDoS	1000/0	IP options-Bad Option		. Infor	75	18	Alert a
- 📓 DoS	1004/0	IP options-Loose Sour	Ē	High	100	100	Alert
Email	1006/0	IP options-Strict Sourc	~	High	100	100	E Aler
S Instant Messaging	1007/0	IPv6 over IPv4		L Infor	100	25	Aler
S L2/L3/L4 Protocol	1101/0	Unknown IP Protocol	V	💰 Infor	75	18	Aler
- 😤 Network Services	1102/0	Impossible IP Packet		High	100	100	Aler
S OS	1104/0	IP Localhost Source S	Image: A start of the start	High	100	100	Aler
- Services	1107/0	RFC 1918 Addresses		🔥 Infor	100	25	Aler
P2P	1108/0	IP Packet with Proto 11	 Image: A start of the start of	High	100	100	Aler
Seconnaissance Releases	1109/0	Cisco IOS Interface DoS		🧿 Medium	75	56	Aleri
	1109/1	Cisco IOS Interface DoS	· · ·	🥝 Medium	75	56	Aleri
Web Server	1109/2	Cisco IO5 Interface Do5		😑 Medium	75	56	Aler
All Signatures	1109/3	Cisco IOS Interface DoS		😑 Medium	75	56	Aleri
Event Action Rules	1200/0	IP Fragmentation Buff		1 Infor	100	25	Aleri
- R rules0	1201/0	IP Fragment Overlap		👗 Infor	100	25	Aler
🖻 🔀 Anomaly Detections 🛛 🗸	1202/0	IP Fragment Overrun	Image: A start and a start	High	100	100	Aleri
	1 connin	10.5	E.21	and the f	100	100	1000 11 1

- 4. Nella scheda Configurazione fare clic su Firme attive.
- 5. Fare quindi clic su **Firma**

Configuration > Corp-IPS > Policie	s > Signature Definitions > sig0 > A	ict	🔾 🔾
Corp-IPS	Filter: Sig ID	ab <u>lelo</u> Filter Clear	Q Signature Wizard
Attack	ID +1 Name	e l	
🔀 Do5	1004/0 IP options-Loose Sour		

Nota: lo screenshot precedente è stato suddiviso in due parti a causa dei limiti di spazio.

6. Scegliere **Yes** e **String TCP** come motore della firma. Fare clic su **Next** (Avanti).

😨 Custom Signature W	/izard 🔀
N The States	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 REAL	Select Engine: String TCP
Anda Anda Anda Anda Anda Anda Anda Anda	O No

7. Èpossibile lasciare queste informazioni come predefinite oppure immettere il proprio

Signature ID, il nome della firma e le note utente. Fare clic su **Next** (Avanti).

🔮 Custom Signature Wi	izar d	X
A Destruction of the	Signature Identification	
	Signature identification parameters identify and describe the signature signature behavior. You must specify a Signature ID and SubSignature default values, but each required value must be unique (not used by	ure, but do not affect the ure ID. You can override the y another signature).
	Signature ID: 60000	
E Mand	SubSignature ID: 0	
al long to a	Signature Name: String.tcp	
1111111	Alert Notes: My Sig Info	
	User Comments: Sig Comment	

8. Scegliere Azione evento, quindi Genera avviso e Host richieste bloccate. Per continuare, fare clic su

Avanti.

🧿 Custom Signature Wizar	d		X
NOSSEGUE I	Engine Specific Parameters		
	Engine-specific parameters deter to fire. You can set the following	mine what the signature looks for and what cau String TCP engine parameters used for this sign	uses the signature nature.
	Name	Value	
	Event Action	© Select item(s)	_ 🛛
Email FTP VolP Web Pages	 Strip Telnet Options Specify Min Match Length Regex String Service Ports Direction Specify Exact Match Offset Specify Max Match Offset Specify Min Match Offset Swap Attacker Victim 	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 Cancel	Select All Select None
	Parameter uses the Defa Parameter uses a User-D	ault Value. Click the value field to edit the value Defined Value. Click the icon to restore the defa	ult value.

9. Immettere un'espressione regolare , che in questo esempio è *testattack*, immettere **23** per le porte di servizio, scegliere **Al servizio** per la direzione e fare clic su **Avanti** per continuare.

🦁 Custom Signature Wiza	rd	
10-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-	Engine Specific Parameters	
	Engine-specific parameters determine what to fire. You can set the following String TC	at the signature looks for and what causes the signature IP engine parameters used for this signature.
	Name	Value
	Event Action	Produce Alert Request Block Host
(H) (H)	- G Strip Telnet Options	No
	Specify Min Match Length	No
m to be be	-Regex String	testattack
No and a second	Service Ports	23
FILTI	Tirection	To Service
HHHHH	Specify Exact Match Offset	No
HHHH	Specify Max Match Offset	No
	Specify Min Match Offset	No
	Swap Attacker Victim	No

10. Èpossibile lasciare queste informazioni come predefinite. Fare clic su **Next** <u>(Avanti)</u>.

😨 Custom Signature Wiza	rd	$\overline{\mathbf{X}}$
	Alert Response	
	You can assign the following v of the signature and the sever number from 0 to 100, with 10 to help calculate the Risk Ratin signature.	alues to this signature that reflect both your confidence in the fidelity rity of the attack it represents. The Signature Fidelity Rating is any 10 reflecting the most confidence in this signature. This number is used ng, which helps determine what actions result from the firing of this
E TAYON AND	Signature Fidelity Rating:	75
1ail	Severity of the Alert:	High

11. Per completare la procedura guidata, fare clic su **Fine**.



12. Scegliere **Configurazione > sig0 > Firme attive** per individuare la nuova firma creata in base all'**ID** o al **nome del** segno. Per visualizzare la firma, fare clic su

Tagine	Value
G-Signature Definition	
Signature ID	60000
SubSignature ID	0
🖌 Alert Severity	Medium
- 😿 Sig Fidelity Rating	75
🖾 Promiscuous Delta	0
Sig Description	12 ⁻
🐼 Signature Name	String.tcp
🐼 Alert Notes	My Sig Info
- 🐨 User Comments	Sig Comment
	0
🖾 Release	custom
	String TCP
- 🗹 Event Action	Produce Alert Request Block Ho
	No
Specify Min Match Length	No
-Regex String	testattack
-Service Ports	23
- Z Direction	To Service
Specify Exact Match Offset	No
- Specify Max Match Offset	No
-Specify Min Match Offset	No
	No
C. Dural Causton	-

13. Per applicare la firma al sensore, fare clic su **OK** dopo aver confermato e fare clic sul pulsante **Apply** (Applica).

14. Nella scheda Configurazione, in Gestione sensori fare clic su **Blocco**. Nel riquadro di sinistra, scegliere **Proprietà blocco** e selezionare **Attiva**



15. Dal riquadro di sinistra, passare al **profilo di accesso al dispositivo**. Per creare un nuovo profilo, fare clic su **Aggiungi**. Una volta creato, fare clic su **OK** e su **Apply** (Applica) per effettuare il rilevamento e continuare.

Certificates	S Add Device Login	1 Profile	Z
Blocking Properties	Profile Name: Username (optional):	Router Test	
Blocking Devices Router Blocking Device In Cat 6K Blocking Device In Master Blocking Sensor SNMP Conseral Configuration	New Password (op Confirm New Pass	word:	
External Product Interfaces External Product Interfaces Consistent of the second sec	Enable Password (o New Password: Confirm New Pass	sword:	
Auto/Cisco.com Update	ОК	Cancel Help	

16. Il passaggio successivo è configurare il router come dispositivo di blocco. Per aggiungere queste informazioni, dal riquadro di sinistra scegliere Periferica di blocco, fare clic su Aggiungi. Quindi fare clic su OK e su

Applica.	F		
- 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 (optional):		
- 🔏 Cat 6K Blocking Device Inl	Device Login Profile:	Router	~
- 🚺 Master Blocking Sensor			
SNMP	Device Type:	Cisco Router	X
General Configuration	Response Capabilities: 📝 Blo	ck 🔄 Rate Limit	
Traps Configuration		- 1 . A	
External Product Interraces	Communication:	Teinet	
Senser Health		U Hele	
TD Legging Veriables			
Provide the second s			

 A questo punto, dal riquadro di sinistra configurare le interfacce dei dispositivi di blocco. Aggiungere le informazioni desiderate, quindi fare clic su OK e su Applica.

Certificates	Q Add Router Blocking	Device Interface	X
Trusted Hosts	Pouter Blocking Devices	10 100 100 1	1
Blocking Resking Properties	Kouter blocking bevice.	10,100,100,1	
	Blocking Interface:	Fe0/1	
Blocking Devices	Direction:	In	~
Router Blocking Device Interface	Pre-Block ACL (optional):	blaster	1
Master Blocking Sensor	Post-Block ACL (optional):	101	
General Configuration Traps Configuration External Product Interfaces		ncel Help	

Verifica

Lanciare l'attacco e il blocco

Completare questi passaggi per lanciare l'attacco e bloccare:

- 1. Prima di lanciare l'attacco, andare all'IME, scegliere **Monitoraggio eventi > Vista attacchi** scartati e scegliere il sensore sulla destra.
- 2. Telnet su Router House e verificare la comunicazione dal server con questi comandi.

L	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#
```

 Da Router Light, Telnet a Router House e digitare testattack.Premere <space> o <enter> per ripristinare la sessione Telnet.

ripristinare la sessione l'elnet.
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 su Router House e utilizzare il comando **show access-list**, come mostrato di seguito.

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. Dal Dashboard del Visualizzatore eventi IDS, viene visualizzato l'allarme rosso una volta avviato

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Suggerimenti

l'atta a a a

Suggerimenti per la risoluzione dei problemi:

• Dal sensore, controllare l'output **show statistics network-access** e verificare che lo stato sia attivo. Dalla console o dal protocollo SSH al sensore, vengono visualizzate le seguenti informazioni:

```
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#
```

 Verificare che il parametro di comunicazione indichi che viene utilizzato il protocollo corretto, ad esempio Telnet o SSH con 3DES. È possibile provare un'autenticazione SSH o Telnet manuale da un client SSH/Telnet su un PC per verificare che le credenziali di nome utente e password siano corrette. Quindi, provare a raggiungere il router in modalità Telnet o SSH dal sensore stesso e verificare se è possibile accedere al router correttamente.

Informazioni correlate

- Pagina di supporto per Cisco Secure Intrusion Prevention
- Documentazione e supporto tecnico Cisco Systems