Konfigurieren der IPS-Blockierung mit IME

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Netzwerkdiagramm Konfigurationen Starten der Sensorkonfiguration Hinzufügen des Sensors zum IME Konfigurieren der Blockierung für den Cisco IOS-Router Überprüfen Angriff und Blockierung starten Fehlerbehebung Tipps Zugehörige Informationen

Einführung

In diesem Dokument wird die Konfiguration der IPS-Blockierung (Intrusion Prevention System) unter Verwendung von IPS Manager Express (IME) erläutert. IME- und IPS-Sensoren werden zur Blockierung eines Cisco Routers verwendet. Beachten Sie bei dieser Konfiguration folgende Punkte:

- Installieren Sie den Sensor, und stellen Sie sicher, dass der Sensor ordnungsgemäß funktioniert.
- Stellen Sie die Sniffing-Schnittstelle auf den Router außerhalb der Schnittstelle ein.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IPS Manager Express 7.0
- Cisco IPS Sensor 7.0(0.88)E3
- Cisco IOS[®] Router mit Cisco IOS Software, Version 12.4

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden diese Konfigurationen verwendet.

- Routerleuchte
- Router-Haus

Routerleuchte

```
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
line con 0
line 97 108
line aux 0
line vty 0 4
```

```
login
```

! end

Router-Haus

```
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
!
!
```

Starten der Sensorkonfiguration

Führen Sie diese Schritte aus, um die Konfiguration des Sensors zu starten.

- 1. Wenn Sie sich zum ersten Mal beim Sensor anmelden, müssen Sie **cisco** als Benutzernamen und **cisco** als Kennwort eingeben.
- 2. Wenn Sie vom System dazu aufgefordert werden, ändern Sie Ihr Kennwort. **Hinweis:** Cisco123 ist ein Wörterbuch und im System nicht zulässig.
- 3. Geben Sie **setup ein**, und folgen Sie der Systemaufforderung, um die Basisparameter für die Sensoren festzulegen.
- 4. Geben Sie folgende Informationen ein: 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. Speichern Sie die Konfiguration.Es kann einige Minuten dauern, bis der Sensor die Konfiguration gespeichert hat.
 - [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

Hinzufügen des Sensors zum IME

Führen Sie diese Schritte aus, um den Sensor in das IME aufzunehmen.

- 1. Wechseln Sie zum Windows-PC, der IPS Manager Express installiert hat, und öffnen Sie den IPS Manager Express.
- 2. Wählen Sie Home > Add.
- 3. Geben Sie diese Informationen ein und klicken Sie auf **OK**, um die Konfiguration abzuschließen.

Mome Configuratio	n 🔤 Event M	4onitor	Devices > De	s Help		
Device List		Add	Edit Dele	ete 🕨 👂 Start 👻	📕 Stop 👻 🍳	Status
	Т	ime	Device Name	IP Address	Device Type	Event :
		🤊 Edi	t Device	-		X
		Sencor	Name	Sepsor5		
			wante.			
		Sensor	r IP Address:	10.66.79.195		
		User N	lame:	cisco		
		Passw	ord:			
		Web S	erver Port:	443		
		Commi	unication protoco	ol		
		💿 Us	e encrypted con	nection (https)		
		() Us	e non-encrypted	connection (http)		
		Event	Start Time (UTC)	í. <u></u>		
		🕑 Mo	ost Recent Alerts			
		St:	art Date (YYYY:M	M:DD)::	:	
		Sta	art Time (HH:MM)	:55): [:]	:	
		Exclud	e alerts of the fo	llowing severity leve	el(s) ———	
		🛄 Inl	formational 📃	Low Medium	- High	

4. Wählen Sie Geräte > Sensor5, um den Sensorstatus zu überprüfen, und klicken Sie dann mit der rechten Maustaste auf Status. Vergewissern Sie sich, dass das Abonnement erfolgreich geöffnet wurde. Nachricht.



Konfigurieren der Blockierung für den Cisco IOS-Router

Gehen Sie wie folgt vor, um die Blockierung für die Cisco IOS-Route zu konfigurieren:.

- 1. Öffnen Sie auf dem IME-PC Ihren Webbrowser, und gehen Sie zu https://10.66.79.195.
- 2. Klicken Sie auf OK, um das vom Sensor heruntergeladene HTTPS-Zertifikat zu akzeptieren.
- Geben Sie im Anmeldefenster cisco als Benutzernamen und 123cisco123 als Kennwort ein.Diese IME-Verwaltungsschnittstelle wird angezeigt:

🚮 Home 💦 Configuration 🌆 Ev	ent Monitorin	g 🚮 Reports 🧖 He	lp						
Configuration > Corp-IPS > Policies	s > Signatu	re Definitions > sig0 > /	Active Sigr	atures					
Corp-IPS									
IPS Policies	Edit	Actions 🕥 Enable 💋 Dis	sable 🔕 Ri	estore Default	5 Show	Events +	N M		
Signature Definitions	Filter: S	Elbert Sin TO							
😭 Active Signatures				1			6 - C - C - C		
🛜 Adware/Spyware	ID +	Name	Enabled	Severity	Fidelity	Base	Signatu		
Attack					Rating	RR Alert a			
DDoS	1000/0	IP options-Bad Option		1 Infor	75	18	🛃 Alert		
S Email	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		L Infor	100	25	Alert		
L2/L3/L4 Protocol	1101/0	Unknown IP Protocol		👗 Infor	75	18	Alert		
	1102/0	Impossible IP Packet		High	100	100	Alert		
🛜 OS	1104/0	IP Localhost Source S	Image: A start of the start	High	100	100	Alert		
- Souther Services	1107/0	RFC 1918 Addresses		1 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		
The Releases	1109/1	Cisco IOS Interface DoS		Medium	75	56	Alert		
Web Server	1109/2	Cisco IO5 Interface Do5		Medium	75	56	FA Alert		
Sinnatures	1109/3	Cisco IOS Interface DoS		Medium	75	56	Alert		
Event Action Rules	1200/0	IP Fragmentation Buff		i Infor	100	25	F Alert		
R rules0	1201/0	IP Fragment Overlap		i Infor	100	25	fa Alert		
Anomaly Detections	1202/0	IP Fragment Overrup		A High	100	100	fa Alert		
🖄 ها - الت	territe		57			100	A cashe		

- 4. Klicken Sie auf der Registerkarte Konfiguration auf Aktive Signaturen.
- 5. Klicken Sie anschließend auf

Signaturassistent. Configuration > Corp-IPS > Policies	> Signature Definitions > sig0	> Act		
Corp-IPS				C Refresh
Active Signatures Active Signatures Adware/Opyware Attack DDoS DoS	Edit Actions Enable Ø Filter: Sig ID 💉 ID +1 Name 1000/0 IP options-Bad Option	Disab E	alo Filter Clear	Q. Signature Wizard

Hinweis: Der vorherige Screenshot wurde aufgrund der Platzbeschränkung in zwei Teile geschnitten.

6. Wählen Sie Yes und String TCP als Signature-Engine aus. Klicken Sie auf

Weiter.

😨 Custom Signature W	izar d 🔀
	Welcome
	Welcome to the Custom Signature Wizard. This wizard will guide you through the process of defining a custom signature.
	Select Engine: String TCP
inda ares. Inda ares.	○ No

 Sie können diese Informationen als Standard belassen oder Ihre eigene Signature-ID, Signaturname und Benutzerhinweise eingeben. Klicken Sie auf Weiter.

🖸 Custom Signature Wiza	ırd		X
A Destador - BAG	Signature Identific	ation	
	Signature identification signature behavior. Yo default values, but ea	n parameters identify and describe the signature, but do not affect the ou must specify a Signature ID and SubSignature ID. You can override the ch required value must be unique (not used by another signature).	
	Signature ID:	60000	
En Shand	SubSignature ID:	0	
al page 1	Signature Name	String.tcp	
tititit	Alert Notes:	My Sig Info	
FIT	User Comments:	Sig Comment	

8. Wählen Sie Event Action (Ereignisaktion) und Produce Alert and Request Block Host. Klicken Sie auf Weiter, um

fortzufahren.	4		
Custom Signature Wizar	G Engine Specific Parameters		
	Engine-specific parameters deter to fire. You can set the following	rmine what the signature looks for and what caus String TCP engine parameters used for this sign	es the signature ature.
E mai	Name	Value	Select All Select None
Email FTP VoiP Web Pages	Specify Min Match Offse Swap Attacker Victim Parameter uses the Defa Parameter uses a User-D	Produce Verbose Alert Produce Verbose Alert Request Block Host Request SNMP Trap Reset TCP Connection OK Cancel OK Cancel OK Cancel	lt value.

9. Geben Sie einen regulären Ausdruck ein, der in diesem Beispiel *testattack* ist, geben Sie **23** für Service-Ports ein, wählen Sie **To Service** for the Direction aus, und klicken Sie auf **Weiter**, um

fortzufahren.

😨 Custom Signature Wiza	rd				
	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 Request Block Host			
	Strip Telnet Options	No			
All and Z	Specify Min Match Length	No			
m to be be	-Regex String	testattack			
	Service Ports	23			
FILTI	🚽 🗹 Direction	To Service			
HHHH	Specify Exact Match Offset	No			
HHHH	Specify Max Match Offset	No			
	Specify Min Match Offset	No			
	Swap Attacker Victim	No			

10. Sie können diese Informationen als Standard belassen. Klicken Sie auf **Weiter**.

😨 Custom Signature Wi	tard	X
A Des Store Ref.	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 i 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 is any er is used of this
Numda Jack Numda Jack Vieth Pages Vieth Pages Note Decom	Signature Fidelity Rating: 75 Severity of the Alert: High	

11. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.



12. Wählen Sie Configuration > sig0 > Active Signatures (Konfiguration > sig0 > aktive Signaturen), um die neu erstellte Signatur mithilfe der Signature-ID oder des Signaturnamens zu suchen. Klicken Sie auf Bearbeiten, um die Signatur

	Name	Value
6	∃-Signature Definition	1
	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
	😑 -Engine	String TCP
	🗹 Event Action	Produce Alert Request Block Host
	II Strip Telnet Options	No
	Specify Min Match Length	No
	-Regex String	testattack
	Service Ports	23
	- 🗹 Direction	To Service
	S-Specify Exact Match Offset	No
	-Specify Max Match Offset	No
		No
		No
	A Dural Country	1
	□ Parameter uses the Default Value. Click the value ✔ Parameter uses a User-Defined Value. Click the ico	field to edit the value. In to restore the default value.
zuzeiaen	OK	Cancel Help

- 13. Klicken Sie nach der Bestätigung auf **OK** und anschließend auf die Schaltfläche **Übernehmen**, um die Signatur auf den Sensor anzuwenden.
- Klicken Sie auf der Registerkarte Konfiguration unter Sensorverwaltung auf Blockieren. Wählen Sie im linken Bereich Blockierungseigenschaften aus, und aktivieren Sie Blockierung



15. Wechseln Sie im linken Teilfenster zum Geräteanmeldeprofil. Klicken Sie zum Erstellen eines neuen Profils auf Hinzufügen. Klicken Sie nach der Erstellung auf OK und Übernehmen, um den Sensor auszuwählen und

	😨 Add Device Login	Profile
Server Certificate Server Certificate Blocking Blocking Properties Blocking Devices Router Blocking Device In	Profile Name: Username (optional): Login Password (opt	Router Test
Cat 6K Blocking Device Inl Master Blocking Sensor SNMP	New Password: Confirm New Passy	word:
External Product Interfaces	Enable Password (op New Password:	ptional)
Sensor Health IP Logging Variables Auto/Cisco.com Update	Confirm New Pass	word:

16. Im nächsten Schritt wird der Router als Blockierungsgerät konfiguriert. Wählen Sie im linken Teilfenster Blockierungsgerät aus, und klicken Sie auf Hinzufügen, um diese Informationen hinzuzufügen. Klicken Sie dann auf OK und

- Server Certificate	3 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 In	Device Login Profile:	Router	~
SNMP	Device Type:	Cisco Router	~
General Configuration	Response Capabilities: 🗹 Blo	ck 🔄 Rate Limit	
External Product Interfaces	Communication:	Telnet	V
🗆 Passwords		2.	
Licensing			
🖁 Sensor Health	OK Cance	el Help	
JP Logging Variables			

17. Konfigurieren Sie jetzt im linken Bereich die Geräteschnittstellen blockieren. Fügen Sie die Informationen hinzu, klicken Sie auf **OK** und **Übernehmen**.

Certificates	Q Add Router Blocking	Device Interface	X
Trusted Hosts			
Blocking	Router Blocking Device:	10.100.100.1	~
Blocking Properties	Blocking Interface:	Fe0/1	
Blocking Devices	Direction:	In	~
Router Blocking Device Interface	Pre-Block ACL (optional):	blaster	
Master Blocking Sensor	Post-Block ACL (optional):	101	
General Configuration Traps Configuration External Product Interfaces		ancel Help	

<u>Überprüfen</u>

Angriff und Blockierung starten

Gehen Sie wie folgt vor, um den Angriff zu starten und zu blockieren:

- Bevor Sie den Angriff starten, gehen Sie zum IME, wählen Sie Event Monitoring > Dropped Attacks View und wählen Sie den Sensor rechts aus.
- 2. Telnet zu Router House und überprüfen Sie die Kommunikation vom Server mit diesen Befehlen.

```
house#show user
```

Line		U	lser I	Host(s)	Idle	Location	
*	0	con	0		idle	00:00:00	
22	26	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. Von Router Light, Telnet zu Router House und geben **testattack ein**.Drücken Sie entweder **<Leerzeichen>** oder **<Eingabe>**, um Ihre Telnet-Sitzung zurückzusetzen.

```
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"
```

!--- Host 10.100.100.2 has been blocked due to the !--- signature "testat triggered.

4. Telnet zu Router House und verwenden den Befehl show access-list wie hier gezeigt.

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. Im Dashboard der IDS Event Viewer wird der rote Alarm angezeigt, sobald der Angriff gestartet

wurde.

Date		Time	Sig. Name	Sig. ID			
🗟 De	vice: Corp-IPS (188 items)					
🚊 Severity: high (188 items)							
(-10/23/2009	09:59:13	String.tcp	60000/0			
	-10/23/2009	09:59:02	ZOTOB Worm Activity	5570/0			
	-10/23/2009	09:58:57	Anig Worm File Tran	5599/0			
	-10/23/2009	09:59:00	Anig Worm File Tran	5599/0			
1		09:58:58	Anig Worm File Tran	5599/0			
		09:59:17	Nachi Worm ICMP E	2158/0			

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Tipps

Tipps zur Fehlerbehebung:

• Sehen Sie sich den Sensor an, um die Ausgabe statistischer Netzwerkzugriffsdaten anzuzeigen und sicherzustellen, dass der Status aktiv ist. Von der Konsole oder SSH zum Sensor werden diese Informationen angezeigt:

```
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#
```

 Stellen Sie sicher, dass der Kommunikationsparameter anzeigt, dass das richtige Protokoll verwendet wird, z. B. Telnet oder SSH mit 3DES. Sie können ein manuelles SSH oder Telnet von einem SSH/Telnet-Client auf einem PC ausprobieren, um die Richtigkeit von Benutzername und Kennwort zu überprüfen. Versuchen Sie dann, Telnet oder SSH vom Sensor selbst zum Router zu starten, und prüfen Sie, ob Sie sich erfolgreich beim Router anmelden können.

Zugehörige Informationen

- Support-Seite für Cisco Secure Intrusion Prevention
- Technischer Support und Dokumentation Cisco Systems