Draadloze LAN-controller en IPS-integratiegids

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies **Cisco IDS-Overzicht** Cisco IDS- en WLC-integratieoverzicht **IDS-switching** Ontwerp van netwerkarchitectuur Cisco IDS-sensor configureren **De WLC configureren** Configuratie van Cisco IDS-sensor en voorbeelden ASA configureren voor IDS Het AIP-SSM configureren voor verkeersinspectie Een WLC configureren om AIP-SSM voor clientblokken te selecteren Voeg een blokkerende handtekeningen aan het AIP-SSM toe Monitorblokkering en gebeurtenissen met IDM Uitsluiting van monitor-client in een draadloze controller Monitorgebeurtenissen in WCS Cisco ASA voorbeeldconfiguratie Cisco-configuratie van sensor voor inbraakpreventiesysteem Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Het Cisco Unified Inbraakdetectiesysteem (IDS)/Inbraakpreventiesysteem (IPS) maakt deel uit van het Cisco zelfverdedigend netwerk en is de eerste geïntegreerde bekabelde en draadloze security oplossing in de sector. Cisco Unified IDS/IPS neemt een uitgebreide benadering van beveiliging: bij de draadloze rand, bekabelde rand, WAN-rand en via het datacenter. Wanneer een verbonden client kwaadaardig verkeer door het Cisco Unified Wireless Network verstuurt, detecteert een Cisco aangesloten IDS-apparaat de aanval en stuurt u shun verzoeken naar Cisco draadloze LAN-controllers (WLC's), die dan het clientapparaat scheiden.

Cisco IPS is een inline, op netwerk gebaseerde oplossing, ontworpen om kwaadaardig verkeer, inclusief wormen, spyware / adware, netwerkvirussen en toepassingsmisbruik nauwkeurig te identificeren, te classificeren en te stoppen voordat ze de bedrijfscontinuïteit beïnvloeden.

Met het gebruik van Cisco IPS Sensor softwareversie 5 combineert de Cisco IPS-oplossing inline preventie met innovatieve technologieën om de nauwkeurigheid te verbeteren. Het resultaat is totaal vertrouwen in de geboden bescherming van uw IPS-oplossing, zonder de angst voor het laten vallen van legaal verkeer. De Cisco IPS-oplossing biedt ook uitgebreide bescherming van uw netwerk door zijn unieke vermogen om met andere bronnen voor netwerkbeveiliging samen te werken en biedt een proactieve benadering van de bescherming van uw netwerk.

De oplossing van Cisco IPS helpt gebruikers meer bedreigingen met groter vertrouwen door het gebruik van deze functies te stoppen:

- Nauwkeurige inline preventietechnologie biedt een ongekend vertrouwen om preventieve actie te ondernemen tegen een bredere reeks bedreigingen zonder het risico van het laten vallen van legaal verkeer. Deze unieke technologieën bieden een intelligente, geautomatiseerde, contextuele analyse van uw gegevens en helpen ervoor te zorgen dat u het meeste uit uw oplossing voor inbraakpreventie ontvangt.
- Identificatie van meerdere vectorbedreigingen Bescherm uw netwerk tegen beleidsschendingen, kwetsbaarheidsuitbuitingen en anomalische activiteit door gedetailleerde inspectie van verkeer in Lagen 2 tot en met 7.
- Unieke netwerksamenwerking verbetert schaalbaarheid en veerkracht door netwerksamenwerking, inclusief efficiënte technieken voor verkeersopnamen, mogelijkheden voor taakverdeling en zichtbaarheid in versleuteld verkeer.
- **Uitgebreide implementatieoplossingen**—biedt oplossingen voor alle omgevingen, van kleine en middelgrote bedrijven (MKB's) en vestigingslocaties tot grote ondernemingen en serviceproviders.
- Krachtig beheer, correlatie van gebeurtenissen en ondersteuningsdiensten Maakt een volledige oplossing mogelijk, inclusief configuratie, beheer, gegevenscorrelatie en geavanceerde ondersteuningsdiensten. In het bijzonder identificeert, isoleert en raadt het Cisco Security Monitoring, Analysis, and Response System (MARS) precisie-verwijdering van offending-elementen aan voor een netwerkbrede inbraakpreventieoplossing. En het Cisco Incidentcontrolesysteem voorkomt nieuwe worm- en virusuitbraken door het netwerk in staat te stellen om zich snel aan te passen en een gedistribueerde respons te bieden.

In combinatie met elkaar bieden deze elementen een uitgebreide on line preventie oplossing en geven u het vertrouwen om de breedste reeks kwaadaardig verkeer te detecteren en te stoppen voordat dit de bedrijfscontinuïteit beïnvloedt. Het Cisco Zelfverdedigend Netwerk initiatief vereist geïntegreerde en ingebouwde veiligheid voor netwerkoplossingen. Huidige Lichtgewicht Access Point Protocol (LWAPP)-gebaseerde WLAN-systemen ondersteunen alleen fundamentele IDS-functies vanwege het feit dat het in wezen een Layer 2-systeem is en de beperkte lijnverwerkingskracht heeft. Cisco geeft nieuwe code tijdig vrij om nieuwe verbeterde functies in de nieuwe codes op te nemen. release 4.0 heeft de nieuwste functies, waaronder de integratie van een op LWAPP gebaseerd WLAN-systeem met de Cisco IDS/IPS-productlijn. In deze release is het doel om het Cisco IDS/IPS-systeem in te schakelen om de WLCs op te dragen om bepaalde clients te blokkeren voor toegang tot draadloze netwerken wanneer een aanval ergens van Layer 3 wordt gedetecteerd via Layer 7 dat de client in overweging neemt.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze minimumeisen voldoet:

- WLC firmware versie 4.x en hoger
- Kennis over het configureren van Cisco IPS en de Cisco WLC is wenselijk.

Gebruikte componenten

Cisco WLC

Deze controllers zijn opgenomen met softwarerelease 4.0 voor IDS-aanpassingen:

- Cisco WLC 2000 Series-switches
- Cisco 1200 Series WLC-lijnkaart
- Cisco 4400 Series WLC-module
- Cisco draadloze servicesmodule (WiSM)
- Cisco Catalyst 3750G Series Unified Access-Switch
- Cisco draadloze LAN-controllermodule (WLCM)

Access points

- Cisco Aironet 1100AG Series lichtgewicht access points
- Cisco Aironet 1200AG Series lichtgewicht access points
- Cisco Aironet 1300 Series lichtgewicht access points
- Cisco Aironet 1000 Series lichtgewicht access points

Beheer

- Cisco draadloos Control System (WCS)
- Cisco 4200 Series sensor
- Cisco IDS-beheer Cisco IDS-apparaatbeheer (IDM)

Cisco Unified IDS/IPS-platforms

- Cisco IPS 4200 Series sensoren met Cisco IPS Sensor software 5.x of hoger.
- SSM10 en SM20 voor Cisco ASA 5500 Series adaptieve security applicaties met Cisco IPS Sensor software 5.x
- Cisco ASA 5500 Series adaptieve security applicaties met Cisco IPS Sensor software 5.x
- Cisco IDS-netwerkmodule (NM-CIDS) met Cisco IPS Sensor softwareversie 5.x
- Cisco Catalyst 6500 Series module voor inbraakdetectiesysteem, release 2 (IDSM-2) met Cisco IPS Sensor softwareversie 5.x

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

Cisco IDS-Overzicht

De belangrijkste onderdelen van Cisco IDS (versie 5.0) zijn:

- Sensor App-voert pakketvastlegging en analyse uit.
- Event Storage Management en actiemodule biedt opslag van beleidsovertredingen.
- Beeld, Installeer en Opstartmodule: laadt, initialiseert, en start alle systeemsoftware.
- Gebruikers interfaces en UI-ondersteuningsmodule biedt een ingesloten CLI en de IDM.
- Sensor OS-host besturingssysteem (gebaseerd op Linux).



De Sensor-toepassing (IPS-software) bestaat uit:

- App—initialiseert het systeem, start en stop andere toepassingen, vormt het besturingssysteem en is verantwoordelijk voor upgrades. Het bevat deze onderdelen:Transactieserver besturen - Hiermee kunnen de sensoren controletransacties verzenden die worden gebruikt om de controller voor de aanvallen-respons (voorheen bekend als Network Access Controller) hoofdblokkeersensor in te schakelen.Event Store-An geïndexeerd Store die wordt gebruikt om IPS-gebeurtenissen op te slaan (fouten, status en waarschuwingssysteemmeldingen) die toegankelijk zijn via CLI, IDM, Adaptieve Security Devices Manager (ASDM) of Remote Data Exchange Protocol (RDEP).
- **App-app** verwerkt bypass en fysieke instellingen en definieert gekoppelde interfaces. De fysieke instellingen bestaan uit snelheid, duplex en administratieve staten.
- **Meld App**—schrijft de logberichten van de toepassing in het logbestand en de foutmeldingen in de Event Store.
- Attack Response Controller (ARC) (voorheen bekend als Network Access Controller) Hiermee beheert u externe netwerkapparaten (firewalls, routers en switches) om blokkeringsfuncties te bieden wanneer er een waarschuwingsgebeurtenis is opgetreden. ARC maakt toegangscontrolelijsten (ACL's) op het gecontroleerde netwerkapparaat en past deze toe of gebruikt de **shun**-opdracht (firewalls).
- App-melding stuurt SNMP-trap af als deze is geactiveerd door een melding, status en fout gebeurtenissen. De app gebruikt hiervoor een SNMP-agent van het publieke domein. De SNMP GET's geven informatie over de gezondheid van een sensor. Web Server (HTTP RDEP2 server) - Biedt een web user interface. Het voorziet ook in een middel om met andere

IPS-apparaten door RDEP2 te communiceren met behulp van verschillende servicesystemen om IPS-services te leveren. **App-verificatie** gaat na of de gebruikers zijn geautoriseerd om CLI-, IDM-, ASDM- of RDEP-acties uit te voeren.

- Sensor App (Analysis Engine) voert pakketvastlegging en analyse uit.
- CLI-De interface die wordt uitgevoerd wanneer gebruikers met succes inloggen op de sensor via telnet of SSH. Alle rekeningen die via de CLI zijn gemaakt, gebruiken de CLI als hun shell (behalve de servicekaccount - er is slechts één servicerekening toegestaan). Toegestaan CLIopdrachten zijn afhankelijk van de rechten van de gebruiker.

Alle IPS-toepassingen communiceren met elkaar via een gemeenschappelijk APItoepassingsprogramma (Application Program Interface) met de naam IDAPI. Remotetoepassingen (andere sensoren, beheertoepassingen en software van derden) communiceren met Sensoren via RDEP2 en Security Devices Exchange (SDEE)-protocollen.

Let op, de Sensor heeft deze diskpartities:

- Toepassingsverdeling bevat het volledige IPS-systeembeeld.
- Onderhoudspartitie Een IPS-afbeelding voor speciale doeleinden, gebruikt om de toepassingsverdeling van IDSM-2 opnieuw in beeld te brengen. Een nieuw beeld van de onderhoudspartitie resulteert in verloren configuratie-instellingen.
- Hersteloptie Een afbeelding met een speciaal doel, gebruikt voor het herstel van de sensor. Met het starten in de herkenningsopdeling kunnen gebruikers de toepassingsopdeling volledig opnieuw image geven. De netwerkinstellingen worden bewaard, maar alle andere configuraties gaan verloren.

Cisco IDS- en WLC-integratieoverzicht

Versie 5.0 van het Cisco IDS introduceert de mogelijkheid om ontkennende acties te configureren wanneer beleidsschendingen (handtekeningen) worden gedetecteerd. Op basis van gebruikersconfiguratie bij het IDS/IPS-systeem kan een tijdelijke aanvraag worden verzonden naar een firewall, router of WLC om de pakketten te blokkeren vanaf een bepaald IP-adres.

Met de Cisco Unified Wireless Network Software release 4.0 voor Cisco draadloze controllers moet een tijdelijke aanvraag naar een WLC worden verzonden om het gedrag van client voor blokkering of uitsluiting van een controller te activeren. De interface die de controller gebruikt om het shun-verzoek te ontvangen, is de opdracht- en bedieningsinterface op Cisco IDS.

- De controller stelt maximaal vijf IDS-sensoren in staat om op een bepaalde controller te worden geconfigureerd.
- Elke geconfigureerde IDS-sensor wordt geïdentificeerd aan de hand van het IP-adres of aan de hand van de gekwalificeerde netwerknaam en de autorisatie-referenties.
- Elke IDS-sensor kan worden ingesteld op een controller met een unieke query-snelheid in seconden.



IDS-switching

De controller vraagt de sensor met de ingesteld query rate om alle onduidelijke gebeurtenissen op te halen. Een bepaald shun-verzoek wordt verspreid over de gehele mobiliteitsgroep van de controller die het verzoek van de IDS-sensor ontvangt. Elke gescande aanvraag voor een client-IP-adres is van kracht voor de gespecificeerde timeout seconden waarde. Als de waarde voor de tijdelijke versie een oneindige tijd aangeeft, wordt de tijdelijke gebeurtenis alleen beëindigd als de tijdelijke versie van het programma is verwijderd. De status van de gescande client wordt gehandhaafd op elke controller in de groep van mobiliteit, zelfs als alle controllers opnieuw worden ingesteld.

Opmerking: De beslissing om een client te blokkeren wordt altijd genomen door de IDS-sensor. De controller detecteert Layer 3-aanvallen niet. Het is een veel gecompliceerder proces om te bepalen dat de klant een kwaadaardige aanval op Layer 3 lanceert. De client is geauthentificeerd op Layer 2 wat goed genoeg is voor de controller om Layer 2 toegang te verlenen.

Opmerking: Als een client bijvoorbeeld een eerder toegewezen offend (geordend) IP-adres krijgt, is het tot de tijd van de Sensor om Layer 2-toegang voor deze nieuwe client te deblokkeren. Zelfs als de controller toegang geeft op Layer 2, is het mogelijk dat het clientverkeer geblokkeerd wordt bij routers in Layer 3, omdat de sensor ook routers van de shun-gebeurtenis informeert.

Stel dat een client IP-adres A heeft. Wanneer de controller op de IDS-toets voor startgebeurtenissen instelt, stuurt IDS het shun-verzoek naar de controller met IP-adres A als doeladres van het IP-adres. Nu, de controller zwarte lijst deze client A. Op de controller worden de klanten uitgeschakeld op basis van een MAC-adres.

Ga er nu van uit dat de client zijn IP-adres van A naar B wijzigt. Tijdens de volgende enquête krijgt de controller een lijst met verzonden klanten op basis van IP-adres. Dit keer is IP-adres A nog in de gescande lijst. Maar omdat de klant zijn IP-adres heeft gewijzigd van A naar B (dat niet in de genooide lijst van IP-adressen staat), wordt deze client met een nieuw IP-adres van B vrijgegeven zodra de tijdelijke versie van de zwarte beursgenoteerde klanten op de controller is bereikt. Nu, begint de controller deze client toe te staan met het nieuwe IP-adres van B (maar het client-MAC-

adres blijft hetzelfde).

Hoewel een client voor de duur van de uitsluitingstijd van de controller uitgeschakeld blijft en opnieuw wordt uitgesloten als hij zijn vorige DHCP-adres opnieuw verwerft, wordt die client niet langer uitgeschakeld als het IP-adres van de client dat wordt verzonden, verandert. Als de client bijvoorbeeld verbinding maakt met hetzelfde netwerk en de DHCP-leasetijd niet is verlopen.

Controllers ondersteunen alleen verbinding met IDS voor client-shunning van verzoeken die gebruik maken van de beheerpoort op de controller. De controller sluit aan op IDS voor pakketinspectie via de toepasbare VLAN-interfaces die draadloos clientverkeer mogelijk maken.

Op de controller wordt elke client uitgeschakeld met een IDS-sensor-aanvraag. De CLI **show** commandoopdracht toont ook een lijst met klanten die op de zwarte lijst staan.

Op het WCS worden de uitgesloten klanten weergegeven onder het subtabblad Security.

Hier zijn de stappen die moeten worden ondernomen om de integratie van Cisco IPS Sensoren en Cisco WLCs te voltooien.

- 1. Installeer en sluit het IDS-apparaat aan op dezelfde switch waar de draadloze controller zich bevindt.
- 2. Spiegelen (SPAN): de WLC-poorten die het draadloze clientverkeer naar het IDS-apparaat uitvoeren.
- 3. Het IDS-apparaat ontvangt een kopie van elk pakket en inspecteert het verkeer op Layer 3 tot en met 7.
- 4. Het IDS-apparaat biedt een downloadbaar signatuurbestand, dat ook kan worden aangepast.
- 5. Het IDS-apparaat genereert het alarm bij een noodactie van shun wanneer een aanvalsaanwijzing wordt gedetecteerd.
- 6. De WLC polls de IDS voor alarmen.
- 7. Wanneer een alarm met het IP adres van een draadloze client, dat aan WLC is gekoppeld, wordt gedetecteerd, zet deze de client in de uitsluitingslijst.
- 8. De WLC en WCS worden in kennis gesteld van een val.
- 9. De gebruiker wordt na de opgegeven periode van de uitsluitingslijst verwijderd.

Ontwerp van netwerkarchitectuur



Cisco WLC is aangesloten op de Gigabit-interfaces op Catalyst 6500. Maak een poortkanaal voor de Gigabit interfaces en laat Link Aggregation (LAG) op de WLC toe.

(Cisco Controller) >show interface summary

Interface Name	Port	Vlan Id	IP Address	Туре	Ap Mgr
ap-manager	LAG	untagged	10.10.99.3	Static	Yes
management	LAG	untagged	10.10.99.2	Static	No
service-port	N/A	N/A	192.168.1.1	Static	No
virtual	N/A	N/A	1.1.1.1	Static	No
vlan101	LAG	101	10.10.101.5	Dynamic	No

De controller is aangesloten op interface gigabit 5/1 en gigabit 5/2 op Catalyst 6500.

```
cat6506#show run interface gigabit 5/1
Building configuration...
Current configuration : 183 bytes
1
interface GigabitEthernet5/1
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
cat6506#show run interface gigabit 5/2
Building configuration...
Current configuration : 183 bytes
1
interface GigabitEthernet5/2
switchport
```

```
switchport trunk encapsulation dotlg
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
cat6506#show run interface port-channel 99
Building configuration...
Current configuration : 153 bytes
1
interface Port-channel99
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

De sensatieinterfaces van de IPS Sensor kunnen afzonderlijk functioneren in **Promiscuous Mode** of u kunt deze koppelen om inline interfaces te maken voor de **Inline Sensing-modus**.

In de modus Promiscuous, stromen pakketten niet door de sensor. De Sensor analyseert een kopie van het gecontroleerde verkeer in plaats van het werkelijk doorgestuurde pakket. Het voordeel om in Promiscuous Mode te werken is dat de Sensor de pakketstroom met het doorgestuurde verkeer niet beïnvloedt.

Opmerking: Het <u>architectuurdiagram</u> is slechts een voorbeeldinstelling van de geïntegreerde WLC- en IPS-architectuur. De voorbeeldconfiguratie die hier wordt getoond, verklaart de IDSsensatieinterface die in Promiscuous Mode werkt. In het <u>architectuurschema</u> is te zien hoe de sensatieinterfaces aan elkaar worden gekoppeld om in de modus Inline paar te kunnen optreden. Raadpleeg de <u>inline modus</u> voor meer informatie over de inline interfacemodus.

In deze configuratie wordt aangenomen dat de sensatieinterface in Promiscuous Mode werkt. De controleinterface van de Cisco IDS-sensor wordt aangesloten op de Gigabit interface 5/3 op Catalyst 6500. Maak een monitorsessie op Catalyst 6500 waar de poort-kanaalinterface de bron van de pakketten is en de bestemming de Gigabit interface is waar de controleinterface van de Cisco IPS Sensor wordt aangesloten. Dit repliceert al het invoer- en toegangsverkeer van de controller-bekabelde interfaces naar de IDS voor Layer 3 door Layer 7-inspectie.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3
cat6506#show monitor session 5
Session 5
```

Туре	: Local Session
Source Ports	:
Both	: Po99
Destination Ports	: Gi5/3
cat6506#	

Cisco IDS-sensor configureren

De eerste configuratie van de Cisco IDS-sensor wordt uitgevoerd vanaf de console-poort of door een monitor en een toetsenbord aan te sluiten op de sensor.

- 1. Meld u aan bij het apparaat:Sluit een console poort op de sensor aan.Sluit een monitor en een toetsenbord aan op de sensor.
- 2. Typ uw gebruikersnaam en wachtwoord in de aanmelding.Opmerking: de standaard gebruikersnaam en wachtwoord zijn beide cisco. Als u zich voor het eerst in het apparaat inlogt, wordt u gevraagd deze boeken te wijzigen. U moet eerst het UNIX-wachtwoord invoeren, dat cisco is. Dan moet u het nieuwe wachtwoord tweemaal invoeren.
 login: cisco

```
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws.
By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.
```

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

```
If you require further assistance please contact us by sending
email to export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to <u>https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet</u> (registered
customers only) to obtain a new license or install a license.
```

3. Configureer het IP-adres, het subnetmasker en de toegangslijst in de sensor. Opmerking: Dit is de opdracht- en bedieningsinterface op de IDS die wordt gebruikt om met de controller te communiceren. Dit adres moet routeerbaar zijn naar de verwerkingsbeheerinterface. De sensatieinterfaces hoeven niet te worden gericht. De toegangslijst dient het (de) interfaceadres(s) van de controller(s) te bevatten, evenals de toegestane adressen voor het beheer van de IDS.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes: ?[yes]: yes
sensor(config)#exit
sensor#
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.6/1.0 ms
sensor#
```

4. U kunt nu de IPS Sensor vanaf de GUI configureren. Wijs de browser aan het IP adres van

het beheer van de sensor. Dit beeld geeft een voorbeeld weer waarin de sensor is ingesteld in

192.168.5.2.

Cisco IDM 5.0 - 192.168.5.2				S 🛛 🕄
File Help				
Configuration Monitoring Dack Forward	d Refresh Hel			Cisco Systems
Configuration Configu	Retresh Hei R	nd communication parameters for the sensor.	Pernote Access Tainet is not a secure access service and is disable by default. IP Enable Teinet	Seconds
IDM is initialized successfully.				cisco administrator A

- 5. Voeg een gebruiker toe die de WLC gebruikt om tot de IPS Sensor gebeurtenissen toegang te
 - hebben.

Cinco DW 5.0 - 192.168.5.2				- C 🐹
File Help				
Configuration Monitoring Back Forward	🕐 📍 Retresh Help			Cisco Sections
G SSH G SSH G SSH	isers ipecify the users that have access to the sensor. The s	ervice role is a special role that allows you to bypass the	CLI If needed. Only one service account is allowed.	
-STime	Usemame	Role	Status	
- Duters	isco	Administrator	Active	
Q Interface Configuration				Edt
- Dinterfaces				
- Ninterface Pairs				Delete
- Nejpass				
Butratic Flow Notications				
- Ninual Sensor	Add User			
Solobal Variables				
🛱 🔍 Signature Definition	Osemame:	Cormoner		
- Signature Variables				
-Signature Configuration	User Role:	Viewer ·		
-Sucustom Signature Wigard				
D C. Event Artico Bules				
- Sevent Variables	- Password			
- Target Value Rating				
- Devent Action Overrides		Transmission and the second seco		
- Sevent Action Filters	Password:			
- Deneral Settings				
E Q Blocking	Castro Barrow			
Device Logic Properties	Consim Passwor	*		
- Slocking Devices		;		
- Router Blocking Device Interfaces				
- Cat 6K Blocking Device Interfaces	06	Cancel Help		
Staster Blocking Sensor	<u> </u>			
rh G cuap				

- 6. Schakel de bewakingsinterfaces
 - in.



De bewakingsinterfaces moeten worden toegevoegd aan de Analyse-engine, zoals blijkt uit dit

venster:				
• Cisco IDM 5.0 - 192.168.5.2				
File Help				
Configuration Monitoring Back Form	ward Refresh	? Help		Cisco Systems
 B Q Sensor Setup ■ Nietwork ■ Nietwork ■ Q SSH ■ Q Centificates ■ QCintificates ■ DTime 	Vitual Senso The sensor assign and	or monitors traffic that traverses interfaces or interface pa remove interfaces (or pairs). You cannot add a new vit	irs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the wal sensor or change the virtual sensor name.	description or
LNUsers	Name	Assigned Interfaces (or Interface Pains)	Description	Edit
Antertace computation Sintertaces Notertaces Notertace Pairs Notpass Notertace Pairs Notertace Notertace Pairs Notertace Pairs Notertace Pairs Notertace Pairs Notertace Noterace Notertace Noterace Noterace Notertace Not	vs0	OlgabitEthernet00 OlgabitEthernet0/1 OlgabitEthernet0/2 OlgabitEthernet0/2	default vitual sensor	
C. Analysis Engine				

7. Selecteer de handtekening van 2004 (ICMP Echo-aanvraag) om een snelle verificatie van de installatie uit te

voeren.											
Cisco IDM 5.0 - 192.168.5.2											💶 🗗 🔀
File Help											
Configuration Monitoring Dack Forward	nd Retres	en 1989									Cisco Sestius
Q. Sensor Setup Network Setup Setup	Select Dy	Configuration	on tures 💌 Belect Criteria: 🖡	-NA- 💌							
D Q SSH D Q Centricates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	Select All
1 DUsers	1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	informatio	100	Default	Normalizer	No	NSDB Dink
D Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Dinterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Clone
- Shrats	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
O Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
- DVirtual Sensor	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
D Q Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
- Signature Variables		-			Developed Alast						Actions
- Signature Configuration	2004		ICMP Echo Request		Request Block	High		Tuned	Atomic IP	No	Restore Defaults
Custom Signature W2ard	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	
D Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio_	100	Default	Atomic IP	No	Deorbe.
- Sevent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Activate
- Target Value Rating	2008	0	ICMP Timestamo Restv	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Dutin
Event Action Overrides Event Action Eithers	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	- CORDA
1.1.1. Barris construction of sectors	1000		and a second sec	1.10	- research reserve	a subsect particular	1.00		California de la		

De handtekening moet worden ingeschakeld, de ernst moet worden ingesteld op **High** and Event Action (**High** and Event Action) om **alarmhost** en **Block Host** te **aanvragen** voor deze verificatiestap te

voltooien.



De WLC configureren

Volg deze stappen om de WLC te configureren:

- 1. Kies **Security > CIDS > Sensors > New** wanneer het IPS-apparaat is geconfigureerd en klaar is om aan de controller toe te voegen.
- Voeg het IP adres, TCP poortnummer, gebruikersnaam en wachtwoord toe dat u eerder hebt gemaakt.Om de vingerafdruk van de IPS Sensor te verkrijgen, voert u deze opdracht uit in de IPS Sensor en voegt u de SHA1-vingerafdruk op de WLC (zonder de kolom) toe. Dit wordt gebruikt om de stemming tussen de controller en de IDS te beveiligen. sensor#show tls fingerprint MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19 SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42

Cases Stateme	A	and an a state of the	A Substation	un a la initiation of	And the second second	Save Co	nfiguration P	ing Logout Refresh
A. A.	MONITOR WLAN	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	CIDS Sensor Add						< Back	Apply
General RADIUS Authentication	Index	1.						
Local Net Users MAC Filtering	Server Address	192.168.5.2						
Disabled Clients User Login Policies AP Policies	Port	443						
Access Control Lists	Username	controller						
Network Access Control	Password	•••••						
IPSec Certificates CA Certificate ID Certificate	Confirm Password							
Web Auth Certificate Wireless Protection	Query Interval	15 500	onds					
Policies Trusted AP Policies	State	R						
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hash)	1662E996362A9	A1EF08899A7C	1645F5C856A	8842 40 he	ex chars		
Web Login Page								
CIDS Sensors Shunned Clients								

3. Controleer de status van de verbinding tussen de IPS Sensor en de

VVLO.									
Conta Brattan									Logout Re
A.A.	MONITOR 1	WLANS CONTROLLE	R WIRELESS	SECURITY	MANAGEMENT CO	MMANDS HELP			
Security	CIDS Senso	rs List						1	New
AAA	Index	Server Address	Port	State	Query Inter	ral Last Query (count)			
General RADIUS Authentication RADIUS Accounting Local Net Users MAC Fibering Disabled Clients User Login Policies AP Policies	1	192.168.5.2	443	Enabled	15	Success (6083)	Detail Ramove		
Access Control Lists									
Network Access Control									
IPSec Certificates CA Certificate ID Certificate									
Web Auth Certificate									
Wireless Protection Policies Trusbed AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summery Client Exclusion Policies AP Authentication Nanagement Prame Protection									
Web Login Page									
CIDS Sensors Shunned Clients									

4. Nadat u de connectiviteit met de Cisco IPS Sensor hebt vastgesteld, zorg er dan voor dat de WLAN-configuratie correct is en dat u clientuitsluiting activeert.De standaard waarde van de client uitsluiting timeout is 60 seconden. Merk ook op dat, ongeacht de uitsluitingstijden van de cliënt, de uitsluiting van de cliënt blijft bestaan zolang het door de IDS ingeroepen clientblok actief blijft. De standaardbloktijd bij de IDS is 30 minuten.

Conce Destrone									Save Config	uration Ping	Logout Refre		
AA	MONITOR WLANS CO	INTROLLER WIRELES	S SECURITY	MANAGEMENT	COMMANDS	HELP							
WLANS	WLANs > Edit									< Back	Apply		
WLANS	WLAN ID	1											
AP Groups VLAN	WLAN SSID	1PS											
	General Policies						Security Policies						
	Radio Policy	All 👻					1Pv6 Enable						
	Admin Status	Enabled											
	Session Timeout (secs)	1800					Layer 2 Security	WPA1+WPA2	×				
	Quality of Service (QoS)	Silver (best effort)	v .					MAC Hitering					
	WMM Policy	Disabled 🐱					Layer 3 Security	None	*				
	7920 Phone Support	Client CAC Limit	AP CAC Limit					Web Policy *					
	Broadcast SSID	Enabled 🖌											
	Allow AAA Override	Enabled											
	External Policy Validation	Enabled					 Web Policy cannot be and L2TP. 	used in combination	with IPsec				
	Client Exclusion	Enabled ** 600	et Value (cerci)				** When client exclusion	n is enabled, a time:	out value of				
	DHCP Server	C Override	or same (sets)				reset excluded clients)	require administrati	live overnide to				
	DHCP Addr. Assignment	Required											
	Interface Name	management 🛩											
	MFP Version Required	1											
	MFP Signature Generation												
	H-REAP Local Switching												
	* H-REAP Local Switching	p not supported with IPSE	C, LZTP, PPTP, C	RANITE and FORT	RESS authentical	ions.							
	CISCO Client Extension (CCX)												
	Version IE	Enabled											
	Aironet IE	2											
	Gratuitous Probe Response												
	Radius Servers												
		Authentication Servers	Accounting	Servers									
	Server 1	1P:10.1.1.12, Port:181	t 👻 none 👻										

5. U kunt een gebeurtenis in het Cisco IPS-systeem activeren of wanneer u een NMAP-scan maakt naar bepaalde apparaten in het netwerk of wanneer u een ping doet naar bepaalde hosts die wordt gecontroleerd door de Cisco IPS-sensor. Zodra een alarm in Cisco IPS wordt geactiveerd, ga naar **Controle en Actieve Host Block** om de details over de host te controleren.

Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	* Hap
- NDenied Attackers - NAttive Host Blocks - Nietwork Blocks - Nietwork Blocks - Nietworks - Nietworks	Active Host Blocks
Support information Statistics System information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable 10.10.99.21 10.10.99.1 0 1 10 10 0 failse

De lijst Gekoppelde clients in de controller is nu ingevuld met het IP- en MAC-adres van de

Cores Stremes		CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shun List	Continuouser	THE LET				
AAA General RADDUS Authentication RADDUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Re-sync 1P Address 10.10.99.21	last MAC Address 10:40:96:ad:0d:1b	Expire 326979296	Sen: 192.3	or IP / Index 660.5.2 / 1		
Access Control Lists							
Network Access Control							
IPSec Certificates CA Certificate ID Certificate							
Web Auth Certificate							
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection							
Web Login Page							
CIDS Sensors Shunned Clients							
t.							
ruiker wordt toege	voedd aan d	de liist					

Clientuitsluiting.

Ann fannen	MONITOR	WLANS	CONTROLLER	WIRELESS SEC	CURITY M	ANAGEMENT C	OMMANDS HEL		
Monitor	Excluded C	lients							
Summary	Search by ?	MAC addr	ess	Seam	ch				
Statistics Controller	Client MAC	Addr J	AP Name	AP MAC Adde	WLAN	Туре	Exclusion Reas	on Port	
Wireless	00:40:95:85	06:1b A	UP1242-2	00:14:1b:59:3e:10	IPS	802.11b	UnknownEnum:5	29	Detail LinkTest Disable Remove

Een logbestand wordt gegenereerd als een client wordt toegevoegd aan de lijst met

Contra Station	MONITOR WLAN	IS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP						
Management	32 14:41:00 2006	Rogue AP : 00:15:c7:82:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface ne:0(802.11b/g) with RSSI: -83 and SNR: 6						
Summary	Tue Apr 11 33 14:40:16 2006	New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2						
SNMP General SNMP V3 Users	Tue Apr 11 34 14:39:44 2006	Regue: 00:0b:05:554:de:5d removed from Base Radio MAC: 00:14:1b:59:3e:10 Interface no:0(802.11b/g)						
Communities Trap Receivers	Tue Apr 11 35 14:39:44 2006	Regue: 00:0b:05:554:de:Se removed from Base Radio MAC: 00:14:1b:S9:3e:10 Interface no:0(802.11b/g)						
Trap Logs	Tue Apr 11 36 14:39:44	Rogue: 00:0b:05:54:34:25f removed from Base Radio NAC: 00:14:1b:59:3e:10 Interface m-m/882 11b/a5						

wordt ook een berichtlogbestand gegenereerd voor de



gebeurtenis.

ommige extra gebeurtenissen worden gegenereerd in de Cisco IPS Sensor wanneer een NMAP-scan wordt uitgevoerd op een apparaat dat door de sensor wordt

gecontroleerd.

Toput Options			
input spoons	C Scan Options		I
C IP Range C IP List	Ormain C Active Direct C	ory C WMI API	Scan
Single Host C Neighborhood IP Address:	₩in32 OS Version Users	Patch Level	Exit
10.1.1.12	🗖 Null IPC\$ Sessions 🖓 Servi	es 🔽 MAC Address	Clear
	🔽 NetBIOS Shares 🔲 Disks	C Sessions	
	Date and Time Group	s Event Log -	Save
	Ping Host(s) PRPC	- Show	Help
	Traceroute Host	igs Errors -	
General Options			
	T TCP F	ortscan Range: 1	1024
Timeout for TCP/UDP/ICMP/SNMP:		ortscan Range: 1	1024
		Community String:	blic
Retries: 3 Max Conne	ections: 1024	comment country 1	······
ID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2	67-1343024091		
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho KB823559 Windows 2000 Ho	tix - KB329115 tfix - KB323182 tfix - KB823589 tfix - KB82359		
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho KB824105 Windows 2000 Ho KB824151 Windows 2000 Ho	tfix - KB329115 tfix - KB323182 tfix - KB823182 tfix - KB82359 tfix - KB824105 tfix - KB824151		
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho KB823159 Windows 2000 Ho KB824151 Windows 2000 Ho KB825119 Windows 2000 Ho KB825119 Windows 2000 Ho KB825129 Windows 2000 Ho	tfix - KB329115 tfix - KB323182 tfix - KB823182 tfix - KB823559 tfix - KB824105 tfix - KB824151 tfix - KB825119 tfix - KB825119		
atch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho KB823182 Windows 2000 Ho KB824105 Windows 2000 Ho KB824105 Windows 2000 Ho KB824151 Windows 2000 Ho KB826232 Windows 2000 Mo KB826035 Windows 2000 Mo KB828741 Windows 2000 Mo KB828741 Windows 2000 Mo	tfix - KB329115 tfix - KB329115 tfix - KB823182 tfix - KB823559 tfix - KB824151 tfix - KB824151 tfix - KB825119 tfix - KB828035 tfix - KB828035		-

toont gebeurtenissen die in de Cisco IPS Sensor zijn gegenereerd.

S

I THE H

Monitoring Monitoring Denied Attackers Durtwe host Blocks Divervork Blocks Divervork Blocks Divervork Blocks Divervork Blocks Divervork Blocks	Option Option Performance Provided Refresh Performance Provided Performance Performance Show error events: Performance Performance Provided Performance Performance	or .
- Distatutics	Q. Lincol Warmer	
Solystem Information		•
	If the part of the second	1000 DEMOL.
	16 ale4blab 100 Anril 11 200 1144003216061613642 ICMP Echo Request	2004
	19 abertiow 32 April 1 200 1144003216851013656 SMB ADMINE Hidden Share Access Atempt	1329
	18 alertinformati, April 11, 200, 1144003216861013655 SMR Windows Share Enumeration	3322
	20 alertinformati. April 11, 200 1144003216861913660 SMB: Windows Share Enumeration	3322
	21 empremor April 11, 200 1144003216861913665 Unable to execute a host block timeout (10.10.99.2) because blocking is disabled	
	22 alertinformati. April 11, 200 1144063216661913696 TCP SYN Host Sweep	30.30
	23 alertinformati. April 11, 200 1144003216661913706 TCP SYN Host Sweep	3030
	25 alerthigh:100 April 11, 200 1144003216661913712 ICMP Echo Reply	2000
	26 error error April 11, 200 1144503216861913714 Unable to execute a host block [10.10.99.22] because blocking is disabled	
	24 alerthigh:100 April 11, 200 1144003216861913710 ICMP Echo Request	2004
	27 alertmedium April 11, 200 1144003216861913715 IOS UDP Bomb	4600
	29 aleftmedium April 11, 200	4060
	30 aletmedium April 11, 200 1144003216861913718 IOS UDP Bomb	4600
	31 alertmedium April 11, 200 1144003216661913719 Back Orifice Ping	4060
	32 aletmedium April 11, 200 1144003216661913720 IOG UDP Bomb	4600 - Rebesh

Configuratie van Cisco IDS-sensor en voorbeelden

Dit is de uitvoer uit het setup-script van de installatie:

sensor#**show config** ! ------! Version 5.0(2) ! Current configuration last modified Mon Apr 03 15:32:07 2006 ! -----service host network-settings host-ip 192.168.5.2/25,192.168.5.1 host-name sensor telnet-option enabled access-list 10.0.0/8 access-list 40.0.0/8 exit time-zone-settings offset 0 standard-time-zone-name UTC exit exit ! -----service notification exit ! -----service signature-definition sig0 signatures 2000 0 alert-severity high status enabled true exit exit signatures 2001 0 alert-severity high status enabled true exit

```
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert | request-block-host
exit
status
enabled true
exit
exit
exit
! _____
service event-action-rules rules0
exit
! ------
service logger
exit
! ------
service network-access
exit
! ------
service authentication
exit
! ------
service web-server
exit
| _____
service ssh-known-hosts
exit
! ------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/0
exit
exit
! ------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
exit
! ------
service trusted-certificates
exit
sensor#
```

ASA configureren voor IDS

In tegenstelling tot een traditionele inbraakdetectiesensor moet een ASA altijd in het datapad zijn. Met andere woorden, in plaats van het oversteken van verkeer van een switch poort naar een passieve snuffelpoort op de Sensor, moet de ASA gegevens op één interface ontvangen, het intern verwerken, en het dan naar een andere haven doorsturen. Voor IDS gebruikt u het modulaire beleidskader (MPF) om verkeer te kopiëren dat de ASA ontvangt naar de interne security servicesmodule voor geavanceerde inspectie en preventie (AIP-SSM) voor inspectie.



In dit voorbeeld is de ASA die gebruikt wordt al ingesteld en passeert verkeer. Deze stappen tonen aan hoe een beleid te creëren dat gegevens naar het AIP-SSM stuurt.

1. Meld u aan in de ASA met ASDM. Na succesvolle inloggen verschijnt het ASA Main System venster.

📫 Cisco ASDM 5.1 for ASA - 172.16.26.2		deleteletelete
File Rules Search Options Tools Wizards Help		
Home Configuration Monitoring Back Forward Search	Refresh Save Help	
Device Information	- Interface Status	
General License	Interface IP Address/Mask Line	Link Current Kbps
Host Name: ciscoasa.cisco.com	inside 172.16.26.2/24 O up O management 192.168.1.1/24 O down	up 3 down 0
ASA Version: 7.1(2) Device Uptime: 2d 5h 24m 51s ASDM Version: 5.1(2) Device Type: ASA5510 Firewall Mode: Routed Context Mode: Single	outside 10.10.102.224 Up	up u
Total Flash: 256 MB Total Memory: 256 MB	Reject an interface to view input and output kines.	
VPN Status IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0	Traffic Status Connections Per Decond Usage	
CPU CPU Usage (percent)	0.5	
00	+9 07:02	
17:07:32 19:07:02	- 'outside' Interface Traffic Usage (Kbps)	ii: 0
Memory Uzage (MB)	1	
64 192 64 17 07 32 19 07 02	0.0 17 07.02 Input Kbps: 0 Output Kbps:	0

2. Klik op **Configuration** boven in de pagina. Het venster switch naar een weergave van de ASA interfaces.

Cisco ASDM 5	1 for ASA - 172,16,26	2													
te Roles Des	ordigue ation Montoring	Dards Help	O	Search	Retresh	Gave .	?								Cinco Srat
	◆ 魚平(町)前)。	1.00.00.00.0	6 4												
Security Policy	Interface	Name	Enabled	Security	IP Address	Sub	netMask	Managemen	MTU		Desc	iption			Add
24	Ethernet0/0	outside	Yes	0	10.10.102.2	255.25	15.255.0	No	1500						Edit
NAT	Ethernet0/1	knolde	Yes	100	172.16.26.2	255.25	6.255.0	740	1500			********	********		
<i>5</i> 3	Ethernet0/2		No					No							
VPN	Management0/0	manage	Yes	100	192.168.1.1	255.25	15 255 0	Yes	1500						
the state															
95 F5															
474															
Routing															
8															
Global Objects															
53															
Properties															
	1														
	Enable traffic betwe	en two or more in	derfaces w	hich are c	onfigured with s	ame secu	and levels								
									1.0						
								AP\$11		Reset					
											+admin>	NA (15)		A 7/27/06 5	07 52 PM U

3. Klik aan de linkerkant van het venster op **Beveiligingsbeleid**. Kies in het resulterende venster het tabblad **Service Policy** Standards.

📫 Cisco ASDM 1	5.1 for ASA - 172,16.2	26.2	
File Rules Se	arch Options Tools	Wizards Help	fores foresas
Home C	configuration Monitorin	ng Back Forward Search Refresh Seve Hep	
-	Configuration + Security	y Palicy + Senice Policy Rules	
bierfaces	• • • • • •	3 時 8 影 8 (9)	
8	C Access Rules	AAA Rules Pilter Rules Pilter Rules	
Security Policy	Show Rules for Interf	tace: All Interfaces Show All	
24		Traffic Classification Rule Actions Description	Add
NAT	E interface: inside, i	Enaded Match Source Lestination Service Inne Hange Policy Inside policy DO-Inside-policy	Edt
SK VEN	inside-class	Db @ any @ any ★ any traffic U\$ los promiscuous, permit traffic	Delete
<u>a</u>			
CSD Manager			
PS			
Routing			
8			
Properties			
	De Match	🚯 Do not match 🕫 Show Summary 🔿 S	Show Detail
		Apply Reset Advanced	
	,		131/06 3:02:47 PM UTC

4. Klik op **Toevoegen** om een nieuw beleid te maken. De wizard Servicebeleid toevoegen start in een nieuw venster.Klik op **Interface** en kies vervolgens de juiste interface in de vervolgkeuzelijst om een nieuw beleid te maken dat aan een van de interfaces is gebonden die verkeer doorgeven.Geef het beleid een naam en een beschrijving van wat het beleid doet met behulp van de twee tekstvakjes.Klik op **Volgende** om naar de volgende stap te gaan.

🚰 Add Service Policy	Rule Wizard - Service Policy	
Adding a new service p	policy rule requires three steps:	
Step 1: Configure a se	ervice policy.	
Step 2: Configure the t	traffic classification criteria for the service policy rule.	
Step 3: Configure action	ons on the traffic classified by the service policy rule.	
Create a service poli	icy and apply to:	
Interface:	inside - (create new service policy)	
Policy Name:	inside-policy	
Description:	DS-inside-policy	
C Global - applies	to all interfaces	
Policy Name:	global-policy	
Description:		
	< Back Next > Cancel	Help

5. Bouw een nieuwe verkeersklasse om op het beleid van toepassing te zijn.Het is redelijk om specifieke klassen op te zetten om specifieke gegevenstypen te inspecteren, maar in dit voorbeeld wordt Elk verkeer voor eenvoud geselecteerd. Klik op **Volgende** om verder te gaan

🖆 Add Service Policy Rule Wizard - Traffic Classifi	ation Criteria 🛛 🔀
Create a new traffic class: inside-class	
Description (optional):	
Traffic match criteria	
🗖 Default Inspection Traffic	
🗖 Source and Destination IP Address (uses A	CL)
🗖 Tunnel Group	
TCP or UDP Destination Port	
🗖 RTP Range	
🔲 IP DiffServ CodePoints (DSCP)	
IP Precedence	
Any traffic	
If traffic does not match a existing traffic class, then it w Class-default can be used in catch all situation. C Use class-default as the traffic class.	ill match the class-default traffic class.
	< Back Next > Cancel Help

6. Voltooi deze stappen omde ASA op te dragen het verkeer naar zijn AIP-SSM te sturen.Controleer IPS voor deze verkeersstroom inschakelen om inbraakdetectie mogelijk te maken.Stel de modus in op Promiscuous zodat er een kopie van het verkeer naar de module wordt verzonden in plaats van de module in lijn met de gegevensstroom te plaatsen.Klik op Verkeersverkeer toestaan om te verzekeren dat de ASA switches aan een open staat in het geval dat AIP-SSM mislukt.Klik op Voltooien om de wijziging aan te geven.

鱰 Add Service Policy	Rule Wizard - Rule Ad	tions		
Protocol Inspection	Intrusion Prevention	Connection Settings	QoS]
🔽 Enable IPS for	this traffic flow			
Mode ———				
C Inline Mode	o o postratio divested to	IDC and the neekst may	he drepped	
as a result (e, a packet is directed to of IPS operation.	ir 5 anu ine packel may	be aroppea	
Promiscous	Mode			
In this mode be dropped	e, a packet is duplicated by IPS.	for IPS and the original p	oacket cannot	
If IPS card fails	s, then			
 Permit traffic 	:			
C Close traffic				
			< Back Finish	Cancel Help

7. ASA is nu ingesteld om verkeer naar de IPS-module te sturen. Klik op **Save** in de bovenste rij om de wijzigingen in de ASA te schrijven.

🖺 Cinco ASDM	5.1 for ASA - 172,16.	26.2								
File Rules S	earch Options Tools	Wittands Help								
Ca Howe	Configuration Monitori	ing Dack Forwar	u Search Re	Ce 🔜	? Hep					other the
	Contiguration + B2con	e/ Folicy + Service Policy Ri	ulus							
Ξ,	🔹 🕾 🐨 🖬 🛍	日本市民会民国	à l							
interfaces	C Access Rules	C AAA Rules C Filler P	Gules 👎 Service P	olicy Pales						
Concurring Continue	Show Rules for Inter	riace: All Interfaces	Bhow All							
Security Pully			Truffic Classificatio	n			Due bebase		Description	Add
PAT NAT	Name	Enabled Match	Source Desir	ation 8	tervice T	ims Ranga	Pou e Aceuro		Description	Edit
08	E Interface: Inside,	Policy: inside policy	ww.	* and	afic		lios promissuous, permittadia	IDS inside policy		Delete
VPN							a to be a received by a second			
8										
CSD Hanager										
i,	1									
- Bouting										
Giolad Objects										
1										
Properties										
	1									
	Den Walch	Const risich							@ ShowSummary C. B	inc-v Detail
		And	v l p	tesset.	Assessed .	1				
Contauration of						_		Leaderice	N4/15	0105 3-51 47 BM 1/20
Conditional Condition	milles successes point									2117020441P# 010

Het AIP-SSM configureren voor verkeersinspectie

Terwijl de ASA gegevens naar de IPS module stuurt, associeert u de AIP-SSM-interface met de virtuele sensor.

1. Aanmelden bij de AIP-SSM met IDM.

Cisco IDM 5.0 - 172.16.26.10				
File Help				
Configuration Mentaring Each Forw	And Refresh Her			Cisco System
E Q Sensor Setup	- Network			
- Diteburgek				
-10Allowed Hosts	Specify the network	and communication parameters for the sensor.		
B G Centicates		1		
- Time	Hostname:	Jeensor		
L- Dusers		[
Q Interface Configuration	IP Address:	172.16.26.10		
- Dopass				
Traffic Flow Notifications	Network Mask:	255 255 255 0		
D Q Analysis Engine				
- Wintual Sensor Olabal Variables	Default Route:	172.16.26.1		
E Q. Signature Definition				
- Signature Variables	FTP Timeout:	300		seconds
- Signature Configuration				
Subscellaneous	Web Server Settin	gs	Remote Access	
D Q Event Action Rules	F Enable TLS/SS	L	Telnet is not a secure access service	
- DEvent Variables			and is disaded by delate.	
- Target Value Rating	Web server port	443	P Enable Teinet	
- Devent Action Filters				
Someral Settings				
E Q Blocking				
Device Losis Properties				
- BBlocking Devices				
- NRouter Blocking Device Interfaces				
- Cat 6K Blocking Device Interfaces				
ED C. CNMP				
- Someral Configuration				
L Traps Configuration				
- NAuto Update				
- Rebot Sensor				
- Shutdown Sensor				
- DUpdate Sensor				
- NLicensing				
		Japly	Reset	
IDM is initialized successfully.				cisco administrator

2. Voeg een gebruiker toe met minstens

kijkerrechten.



3. Schakel de interface

in.

Cisco IDM 5.0 - 172.16.26.10									
File Help									
Configuration Montoring Back	Forward	Retresh Help							Citte State
D Q Sensor Setup		Interfaces							
- Niedwork		A capaing interface mus	of he enabled a	of accined to	a virtual cance	u hatve the ca	nan will monitor that in	lertara. Vou can anabiaidisable lha available sansing interface	s by selecting the marks)
R C CCH		and clicking Enable or I	Disable.	in an official of	a mana areas	n serve ure or		enace, row can ensure an analous sensing menace	a strategy and readily
S Q Centificates									
- Time							Alternate TCP		Select All
- Dubers		Interface Name	Enabled	Media Type	Ouplex	Speed	Reset Interface	Description	Emminie L
- Sinterfaces		GigabitEthernet0/1	Yes	Backplane in	Ado	Auto	None		Edt
- DPpass Drafic Flow Notifications									Enable
Q Analysis Engine									Disable
- Virtual Sensor									
Signature Definition									
Signature Variables									
- Signature Configuration									
Custom Signature Wizard									
D Q Event Action Rules									
- DEvent Variables									
- Target Value Rating									
- NEvent Action Overrides									
- Oeneral Settings									
E Q Blocking									
- DBlocking Properties									
- Blocking Devices									
- Router Blocking Device Interface	es								
- Cat 6K Blocking Device Interface	es :								
- Master Blocking Sensor									
- Doneral Configuration									
Traps Configuration									
- Auto Update									
- Restore Defaults									
Shutdown Sensor									
- Dupdate Sensor									
Licensing									
							Repty E	leset	
IDM is initialized successfully.								cisco	administrator

4. Controleer de configuratie van de virtuele sensor.



Een WLC configureren om AIP-SSM voor clientblokken te selecteren

Voltooi deze stappen nadat de sensor is ingesteld en klaar is om aan de controller toe te voegen:

- 1. Kies **Beveiliging > CIDS > Sensoren > Nieuw** in de WLC.
- 2. Voeg het IP-adres, TCP-poortnummer, gebruikersnaam en wachtwoord toe dat u in de vorige sectie hebt gemaakt.
- 3. Om de vingerafdruk van de sensor te verkrijgen, voert u deze opdracht uit in de Sensor en voegt u de SHA1-vingerafdruk op de WLC (zonder de kolom) toe. Dit wordt gebruikt om de stemming tussen de controller en de IDS te beveiligen.

```
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```

Conce Stateme								
A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Serve	ior Edit						
General RADIUS Authentication	Index		2					
RADIUS Accounting Local Net Users MAC Filtering	Server Ad	ldress	172-16-26-10					
Disabled Clients User Login Policies	Port		443					
AP Policies Access Control Lists	Usernam	0	controller					
IPSec Certificates CA Certificate ID Certificate	Password		•••••					
Web Auth Certificate	State		X					
Wireless Protection Policies	Query Int	erval	10 sec	onds				
Rogue Policies	Fingerprin	3n	90C996984EFA74	F0528092888	483C458487	40 her	k chars	
Standard Signatures Custom Signatures	(SHA1 ha	sh)	(hash key is alre	ady set)				
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Last Quer (count)	Y	Success (1400)					
Web Login Page								
CIDS Sensors Shunned Clients								

4. Controleer de status van de verbinding tussen het AIP-SSM en de

WLC.								
Circo Station	MONITOR W	LANS CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMM	ANDS HELP		
Security	CIDS Sensors	List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Index 1	Server Address 192.168.5.2	Port 443	State Enabled	Query Interval	Last Query (count) Unauthorized (1)	Detail	Remaye
	2	172.16.26.10	443	Enabled	10	Success (1444)	Datai	Bamaya
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / NFP Management Prame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

Voeg een blokkerende handtekeningen aan het AIP-SSM toe

Voeg een inspectie handtekening toe om verkeer te blokkeren. Hoewel er veel handtekeningen zijn die de taak kunnen uitvoeren op basis van de beschikbare gereedschappen, creëert dit voorbeeld een handtekening die pakketjes blokkeert.

1. Selecteer de handtekening van 2004 (ICMP Echo-aanvraag) om een snelle verificatie van de installatie uit te

voeren.											
Cisco IDM 5.0 - 192,168.5.2											- 8 X
File Help											
Configuration Monitoring Eack Forward	Retro	n Help									Cisco Sestens
⊕ Q, Sensor Setup	Signature	Configuration	08								
- SNetwork	Related De	All Piece	Anna al Relationaria	100							
- SAllowed Hosts	Denect by	r. bereigin	notes Til neserronnen i	1011							
ID G. Certificates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity	Type	Engine	Retired	Select All
- STime	_						Haong				NSDB Link
- Dusers	1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	informatio	100	Default	Normalizer	No	
D Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Dinterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Cione
- Semans	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In.,	informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
© Q. Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Enable
- Nitual Sensor	2002	0	ICMP Source Quench	Ves	Produce Alert	Hab	100	Tuned	Atomic IP	Nin	
- Toolobal Variables	1002		MAR Reduct	Mag	Produce Plant	Link	100	Tunna	Pagennie 10	No.	Disable
- Signature Variables	2003	0	ICMP REDIREC	162	Produce Alen	High	100	Tuned	Addition (P	140	Actions
Signature Configuration Scustom Signature Witard	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Atomic IP	No	Restore Defaults
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Concern 1
D Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Adormic IP	No	
- Sevent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Activate
- STarget Value Rating	2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio	100	Default	Adormic IP	No	Rates
-Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	

2. Schakel de handtekening in, stel de noodtoestand in op Hoog en stel de actie voor gebeurtenis in om de host voor waarschuwing en aanvraag te produceren om deze verificatiestap te voltooien. Merk op dat de actie Block Host van het Aanvraag de sleutel is tot het signaleren van de WLC om client uitzonderingen te maken.

Name Value	🗣 Edit Signature				iteriteriteriteriteriteriteriteriteri
Signature ID: 2064 ButSignature ID: 0 Aut Signature ID: 0 Big Fidels Rather: 100 Promissious Data: 100 Promissious Data: 100 Big Fidels Rather: 100 Avent Notes: 100 Promissious Data: 100 Big Description: Bigmature Name: ColP Ector Registed Avent Notes: 100 Provide Commenta: 100 Signature Documenta: 100 Bigeody ICMP Sequence: 100 Bigeody ICMP Code: 100 Bigeody ICMP Code: 100 Bigeody ICMP Total Length: 100 Bigeody ICMP Code: 100	Name	Value			
SubSignature ID: 0 Attert Seventy: Hugn :: Big Fidels / Halms: 100 Promissous Datts: 0 Sig Description: Signature Name: Signature Name: Signature Name: User Comments: User Comments: User Comments: 0 Response 0 Programmet Distation: Produce Vehicles Auf .: Pragment Distation: Request Bool Commentor: Big Extify Liver 4 Protocol: Signetify ICMP Type:: Big Beckly ICMP Type: Dispeckly ICMP Type: Big Beckly ICMP Type: Big Beckly ICMP T	Signature ID:	2004			
Avant Seventy: High:	SubSignature ID:	0			
Big Fideling Rading: Promissouss Delta Sig Description: Biggnature Name: MOP Ector Request User Comments: User Comments: User Comments: User Comments: Engine: Momission: Produce Vehices Aler: Produce Vehices Aler: Produce Vehices Aler: Produce Vehices Aler: Produce Vehices Aler: Produce Veh	🔶 Alert Severity:	High			
Promiscuous Detta: Sig Description: Sig Description: Sig Description: Sig Adurt Name: Sig Comments: Adurt Trads: Release: Sig Comments: Adurt Trads: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments	Sig Fidelity Rating:	100			
 Sig Description: Signature Name: CMP Echo Properts Arent Nobe: User Comments: Arent Traits: Berniese: Testameter uses the Default Value. Click the icon to reditte the default value. 	Promiscuous Delta:	0			
Signalare Name: WP Esho Pequest User Comments: User Comments: Extra later Notes: Extra later Notes: Extra later Notes: Extra later Notes: Extra later Issue: Extra later Issue: Extra later Issue: Extra later Verbese Aler Request Book Connector Request Book Protocol: Expensive: Issue: Issue: Arr Issue: Request Book Connector Request Book Protocol: Issue: Issue: Request Book Protocol: Request Book Protoc	Sig Description:				
Alert Note::::::::::::::::::::::::::::::::::::		Signature Name: IOMP Echo	Request		
 User Comments: Alert Trade: Reisase: Reisase: Respire: Atomic IP Event Action: Produce Area Respire: Atomic IP Event Action: Produce Area Respire: Atomic IP Event Action: Produce Mode Acting Produce Book Connector Respire: Fragment Status: Respire: Specify Layer 4 Protocol: Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: Specify ICMP Type: Specify ICMP Type: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: Respire: 		Alert Notes:			
Alert Trait: Release: Image: Alert Trait: Release: Image: Ima		User Comments:	<u></u>		
Produce Vert Halls. Preisase: Engine: Abmic IP Evend Action: Produce Verboes Avert Specify ICMP Sequence: If I avert 4 Produce Specify ICMP Type: If I avert Parameter uses the Default Value. Click the icon to restore the default value. OK Cancel Halp		Alari Traiter	<u></u>		
Preveste: 1 Atomic IP Event Action: Produce Aleft Produce Aleft Produce State Prequest Stock Connector Request Stock Connector					
Nomic P Engine: Nomic P Event Action: Produce Verbage Aleri Request Block Denotion Fragment Btabus: Any		Release:			
Preduce Vertes event Action: Produce Vertes event Action: Produce Vertes event Action: Produce Vertes event Action: Produce Vertes event Action: Preduce Block Avent Arry Fragment Bladus: Arry Pragment Bladus: Preducet Bonn Tab Producet Bo	Engine:	Alomic IP			
Fragment Status: Any Specify Layer 4 Protocol: Specify ICMP Sequence: No Specify ICMP Type: Specify ICMP Typ		Event Action:	Produce Alert Produce Verbose Alert Request Block Connector Request Block Host Perquest Book Host		
Fragment Blabus: Fragment Blabus: Specify Layer 4 Protocol: Specify ICMP Protocol: Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: Specify ICMP Code: No w Specify ICMP Code: No w Specify ICMP Total Length: No w Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Halp			< >		
Parameter uses the Default Value. Click the icon to edit the value. OK Cancel OK Cancel		Fragment Status:	Any		
CMP Protocol Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: Specify ICMP Code: No Specify ICMP Code: No Specify ICMP Code: No Specify ICMP Identifier: No Specify ICMP Total Length: Specify ICMP		Specify Layer 4 Protocol:	Yes 💌		
Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: ICMP Type: ICMP Type: Specify ICMP Code: Specify ICMP Code: Specify ICMP Identifier: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: OK Cancel Halp			E Layer 4 Protocol:	ICMP Protocol	
Specify ICMP Type: ICMP Typ				Specify ICMP Sequence:	No
ICMP Type: ICMP Type: Specify ICMP Code: No Specify ICMP Identifier: No Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. Parameter uses a User-Defined Value. Click the icon to restore the default value. OK Cancel Help				Specify ICMP Type:	Yes
Specity ICMP Code: No Specity ICMP Identifier: No Specity ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Help				8.8.8.8.8.8.8.8	ICMP Type:
Specify ICMP Identifier: No Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Help				Coacily ICMD Code:	
Aprices rower administer. 1980 Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Halp				Opecity ICMP Identifier	
Parameter uses the Default Value. Click the icon to edit the value. Parameter uses a User-Defined Value. Click the icon to restore the default value. OK Cancel Help				Concilia I CMP Total Landth:	
Parameter uses the Default Value. Click the icon to edit the value. Parameter uses a User-Defined Value. Click the icon to restore the default value. OK Cancel Help				apecity town rotal Lengin.	
Parameter uses are certain yaue. Once the icon to earl the value. Parameter uses a User-Defined Value. Click the icon to restore the default value. OK Cancel Help	Paramalar uses the D	afaultitalas. Citabilas teas la editiona	unium.		
OK Cancel Help	 Parameter uses the U Parameter uses a Us 	er-Defined Value. Click the icon to rest	tore the default value.		
			OK Cancel	Help	

S. Ed	lit Signature			×
	Name	Value		-
	Signature ID:	2004		
	SubSignature ID:	0		
	Alert Severity:	Informational 💌		
•	Sig Fidelity Rating:	100	_	
	Promiscuous Delta:	0		
Θ	Sig Description:			
		Signature Name:	ICMP Echo Request	
		Alert Notes:		
		User Comments:		
		Alert Traits:	0	
		Release:	81	
Θ	Engine:	Atomic IP		
		Event Action:	Request Block Connection	
•		Eranment Status	e' Dima la l	•
•	Parameter uses the D Parameter uses a Use	efault Value. Click the icc er-Defined Value. Click th	on to edit the value. he icon to restore the default value.	
			OK Cancel Help	

- 3. Klik op **OK** om de handtekening op te slaan.
- 4. Controleer dat de handtekening actief is en dat deze is ingesteld om een blokkerende actie uit te voeren.
- 5. Klik op **Toepassen** om de handtekening aan de module te binden.

Monitorblokkering en gebeurtenissen met IDM

Voer de volgende stappen uit:

 Als het branden van handtekeningen succesvol is, zijn er twee plaatsen binnen IDM om hiervan nota te nemen. De eerste methode toont de actieve blokken die AIP-SSM heeft geïnstalleerd. Klik op Monitoring in de bovenste rij van acties. Selecteer in de lijst met items aan de linkerkant de optie Actieve hostblokken. Wanneer de ping signatuur in werking stelt, toont het Actieve venster van de Blokken van de Host Block het IP adres van de overtreder, het adres van het aan te vallen apparaat en de resterende tijd waarvoor het blok in werking is. De standaard blokkeertijd is 30 minuten en kan worden aangepast. Het wijzigen van deze waarde wordt echter niet in dit document besproken. Raadpleeg de ASA configuratie documentatie indien nodig voor informatie over het wijzigen van deze parameter. Verwijder het blok direct en selecteer het in de lijst en klik vervolgens op Verwijderen.



De tweede methode om geactiveerd handtekeningen te bekijken gebruikt de AIP-SSM-event buffer. Selecteer **Evenementen** in de lijst met items aan de linkerkant van de pagina IDM Monitoring. Het zoekprogramma van Evenementen verschijnt. Stel de juiste zoekcriteria in en klik op

Weergeven....

Cisco IDM 5.0 - 172.16.26.10	
File Help	
Configuration Moniforming Eack Forward Retresh	📍 Help
Conversion C	Events To can display the events in the local Event Store. By default all events are displayed. To filte event type and/or time, eelect the appropriate check boses. Show are events I for events I for events I for intervents I for events I for intervents I for events I for intervents I for events I for events <pi events<="" for="" p=""> I for events I for</pi>

2. Het Event Viewer verschijnt dan met een lijst van gebeurtenissen die voldoen aan de gegeven criteria. Scrolt door de lijst en vind de handtekening van het ICMP Echo-verzoek die in de vorige configuratiestappen is gewijzigd.Kijk in de kolom Events voor de naam van de handtekening of zoek anders naar het identificatienummer van de handtekening onder de kolom Sig

ŧ	Туре	Sensor UTC Time	Event ID	Events	Sig ID	Details.
1	error:error	July 31, 2006 2:59:52 PM U	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
2	error:warning	July 31, 2006 3:16:51 PM U	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
3	alert informati	July 31, 2006 3:19:16 PM U	1145383740954941574	ICMP Echo Request	2004	
4	error.error	July 31, 2006 3:19:16 PM U	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
5	alastisfame all	1-2-24 2006 2-40 46 DM 11	1116202740054041507	IOMD Eaks Dogwoot	0000	
	alert mormas	July 31, 2006 3.19.46 PM 0	1140303140834341381	icime Echo Request	2004	
	anget shrorthad	July 31, 2006 3.19.46 PM 0	1140303740934941597	CMP ECHO Request	2004	

 Nadat u de handtekening hebt geplaatst, dubbelklikt u op de ingang om een nieuw venster te openen. Het nieuwe venster bevat gedetailleerde informatie over de gebeurtenis die tot de handtekening heeft geleid.

```
Details for 1145383740954941597
evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
  originator:
   hostId: sensor
   appName: sensorApp
    appInstanceId: 341
  time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
  signature: description=ICMP Echo Request id=2004 version=S1
    subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: 10.10.99.26 locality=OUT
    target:
     addr: 10.10.102.1 locality=OUT
  summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
  alertDetails: Regular Summary: 4 events this interval ;
  riskRatingValue: 25
  interface: ge0 1
  protocol: icmp
```

Uitsluiting van monitor-client in een draadloze controller

De lijst Gekoppelde clients in de controller is op dit moment ingevuld met het IP- en MAC-adres van de host.

toro Innen	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Locin Religion	Re-sync IP Addres 10.10.99.24	• La 6 00	st MAC Address 0:40:96:ad:0d:1b	Expire 27	Sen 172.	sor IP / Index 16.26.10 / 2		
AP Policies Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MPP Nanagement Frame Protection								
CIDS Sensors Shunned Clients								

De gebruiker wordt toegevoegd aan de lijst Clientuitsluiting.

MONE	ITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		_
Monitor Exclu Summary Sear Statistics Centroller Ports Dords Wireless Roque APs Known Roque APs Roque Clients Adhoc Reques 802.11b/g Radios Clients	uded Clients rch by MAC add nt NAC Addr 01961ad10d11b	AP Name AP0014.6940.81ce	AP NAC Add	Search r WLAN 16:40 IPS	Type 802.11	Exclusion La UnknownE	Reason num:5	Port 29	Detail Unit Test Disable Remove

Monitorgebeurtenissen in WCS

Beveiligingsgebeurtenissen die een blok binnen het AIP-SSM veroorzaken, veroorzaken dat de controller het adres van de overtreder aan de lijst van klantuitsluitingen toevoegt. Ook binnen WCS wordt een gebeurtenis gegenereerd.

 Gebruik de monitor > Alarmprogramma's in het hoofdmenu van het WCS om de uitsluitingsgebeurtenis te bekijken. WCS geeft eerst alle ongewisse alarmen weer en heeft ook een zoekfunctie aan de linkerkant van het venster.

- 2. Wijzig de zoekcriteria om de clientblokkering te vinden. Selecteer onder Ernst de optie **Klein** en stel de categorie Alarm ook in voor **beveiliging**.
- 3. Klik op

Zoeken.

Monitor × Configure × Location × Administration × Belo × Alarms Alarms - Select a command													
Alarms Alarms - Select a command	have a second seco												
	- ¥ 60												
Example 1													
Critical Critical Severity Eallure Object Owner Date/Time Message													
Alerro Category 6/2/06 9/02 AM AP 'AIR-LAP1242AG-A', interface '802.11b/g' is													
All Types V Critical Radio AlR-LAP1242AG-A/2 6/1/06 9102 AM AP 'AIR-LAP1242AG-A', interface '802.11a' is do													
Critical AP_AIR_LAP1242AG-AY001411b159141160 6/1/06 9102 AM AP_AIR_LAP1242AG-AY disessociated from Control													
Search Critical Radio ap:75:12:e0/2 7/21/06 1:51 PM AP 'ap:75:52:e0', interface '002:11a' is down o													
Critical Radio a0:75:12:e0/1 7/21/06 1:51 PM AP 'ap:75:12:e0', interface '002:11b/g' is down													
Critical AP.api75122:e0/00:00:05:75:12:e0													
Critical Smitch Cisco #187:4h/40.1.3.15 7/22/06 4132 PM Controller '40.1.3.15', RADIUS server(s) are no													
Critical AP.A20033.0(92.0df0/001335f:57:a3160 7/2L/06.4:38 PM Fake AP or other attack may be in progress. Rog													
Critical AP AP0013.0(93.ba2/2001315f57.rtd:40 7/2L/06.5131 PM Fake AP or other attack may be in progress. Rog													
Critical <u>AF.AP142-B/0011413b.5613140</u> 7/25/06 5125 PM Fake AP or other attack may be in progress. Rog													
Critical Radia AP-acc-c3750-48-1-FE1-0-1/2 7/28/06 2:02 PM AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802													
Critical Radio AP-acc-c3750-40-1-FE1-0-3/1 7/26/06 2:02 PM AP 'AP-acc-c3750-40-1-FE1-0-3/1 02													
Critical AP.AP-acc-c3750-48-1-FE1-0-3/00:0b:55.52:a0:a0 7/26/06.2:02 PM AP 'AP-acc-c3750-48-1-FE1-0-3' disassociated fr													

4. Het Alarmvenster toont vervolgens alleen veiligheidsalarmen met een geringe ernst. Wijs de muis aan op de gebeurtenis die het blok in het AIP-SSM heeft geactiveerd. In het bijzonder toont WCS het MAC-adres van het clientstation dat het alarm heeft veroorzaakt. Door aan het juiste adres te wijzen, verschijnt WCS een klein venster met de gebeurtenis details. Klik op de link om deze gegevens in een ander venster te bekijken

рекіјкен.							
Cisco Wireless Control Sy	ystem					Username: rool	t Logout Refresh Print
Monitor • Configure • L	ocation	n 🔹 <u>A</u> dminis	stration • Help •				
Alarms	Alar	ms					Select a command
Severity Minor		Severity	Failure Object	Owner	Date/Time	Message	
(renter (renter)		Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr	
Alarm Category		Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr	
Jocany		Minor	Client 00:90:7a:04:6d:04		7/31/06 2:36 PM	Client '00:90:7a:04:6d:04' which was associated	
Search		Minor	Client 00:40:95:ad:0d:15		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated,	
			Client '00:40:96 ad 0d:16 '00:14:16:56:16:40', inter code is '5(Uninown)'.	f which was ass face 안 is exclud	ociated with AP ed. The reason		

Cisco ASA voorbeeldconfiguratie

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
```

```
names
1
interface Ethernet0/0
nameif outside
 security-level 0
 ip address 10.10.102.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
ip address 172.16.26.2 255.255.255.0
1
interface Ethernet0/2
 shutdown
 no nameif
no security-level
no ip address
1
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
1
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
mtu outside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
nat (inside) 102 0.0.0.0 0.0.0.0
route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.12 255.255.255.255 inside
http 0.0.0.0 0.0.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd enable management
!
class-map inside-class
 match any
```

```
!
!
policy-map inside-policy
description IDS-inside-policy
class inside-class
ips promiscuous fail-open
!
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Cisco-configuratie van sensor voor inbraakpreventiesysteem

```
sensor#show config
| _____
! Version 5.0(2)
! Current configuration last modified Tue Jul 25 12:15:19 2006
! ------
service host
network-settings
host-ip 172.16.26.10/24,172.16.26.1
telnet-option enabled
access-list 10.0.0/8
access-list 40.0.0/8
exit
exit
| _____
service notification
exit
! ------
service signature-definition sig0
signatures 2004 0
engine atomic-ip
event-action produce-alert | request-block-host
exit
status
enabled true
exit
exit
exit
! ------
service event-action-rules rules0
exit
! ------
service logger
exit
! ------
service network-access
exit
! ------
service authentication
exit
| _____
service web-server
exit
| _____
service ssh-known-hosts
exit
! ------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
```

```
physical-interface GigabitEthernet0/1
exit
exit
! ------
service interface
exit
! ------
service trusted-certificates
exit
sensor#
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Installeren en gebruiken van Cisco Inbraakpreventiesysteem Manager 5.1
- <u>Cisco ASA 5500 Series adaptieve security applicaties Configuratiehandleidingen</u>
- De Cisco-sensor voor inbraakpreventiesysteem configureren met behulp van de opdrachtregel interface 5.0 - interfaces configureren
- <u>WLC-configuratiegids 4.0</u>
- Draadloze technische ondersteuning
- WLC FAQ (draadloze LAN-controller)
- Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point
- Beveiligingsoplossingen configureren
- <u>Technische ondersteuning en documentatie Cisco Systems</u>