

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 software release 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.

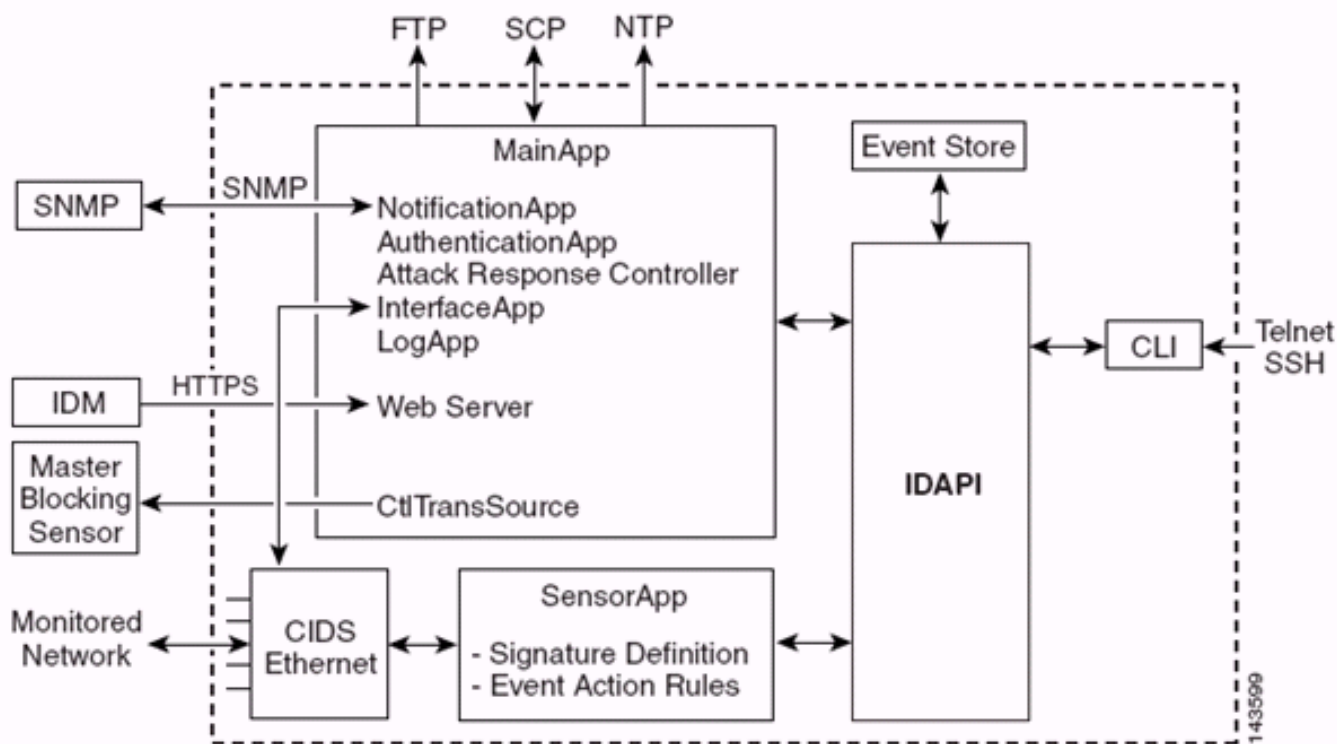
Conventies

Raadpleeg [Cisco Technical Tips Conventions \(Conventies voor technische tips van Cisco\) voor 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 serviceaccount - er is slechts één servicerekening toegestaan). Toegestaan CLI-opdrachten zijn afhankelijk van de rechten van de gebruiker.

Alle IPS-toepassingen communiceren met elkaar via een gemeenschappelijk API-toepassingsprogramma (Application Program Interface) met de naam IDAPI. Remote-toepassingen (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:

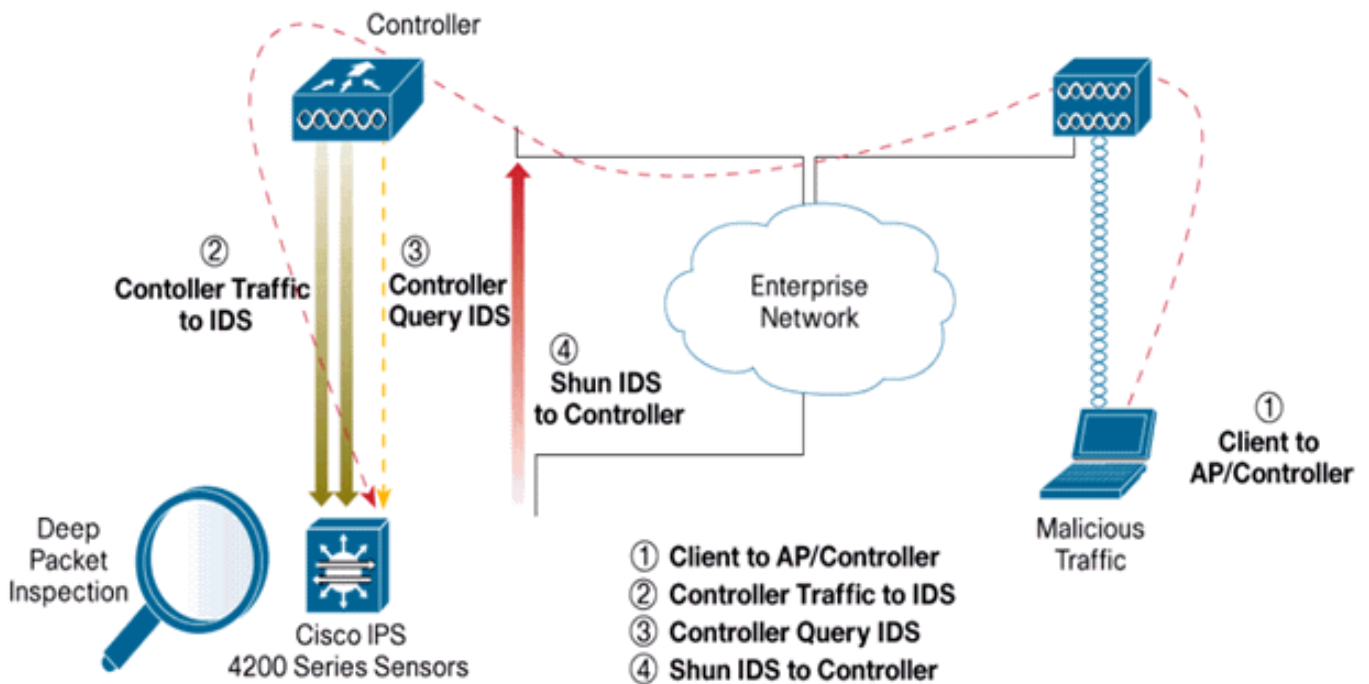
- **Toepassingsverdeling** - bevat het volledige IPS-systeembeeld.
- **Onderhoudspartitie** — Een IPS-afbeelding voor speciale doeleinden, gebruikt om de toepassingsverdeling van IDSM-2 opnieuw in beeld te brengen. Een nieuw beeld van de onderhoudspartitie resulteert in verloren configuratie-instellingen.
- **Hersteloptie** — Een afbeelding met een speciaal doel, gebruikt voor het herstel van de sensor. Met het starten in de herkenningsoptie 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 netwerknamen 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 geauthenticeerd 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 deblokken. 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 genoemde 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.

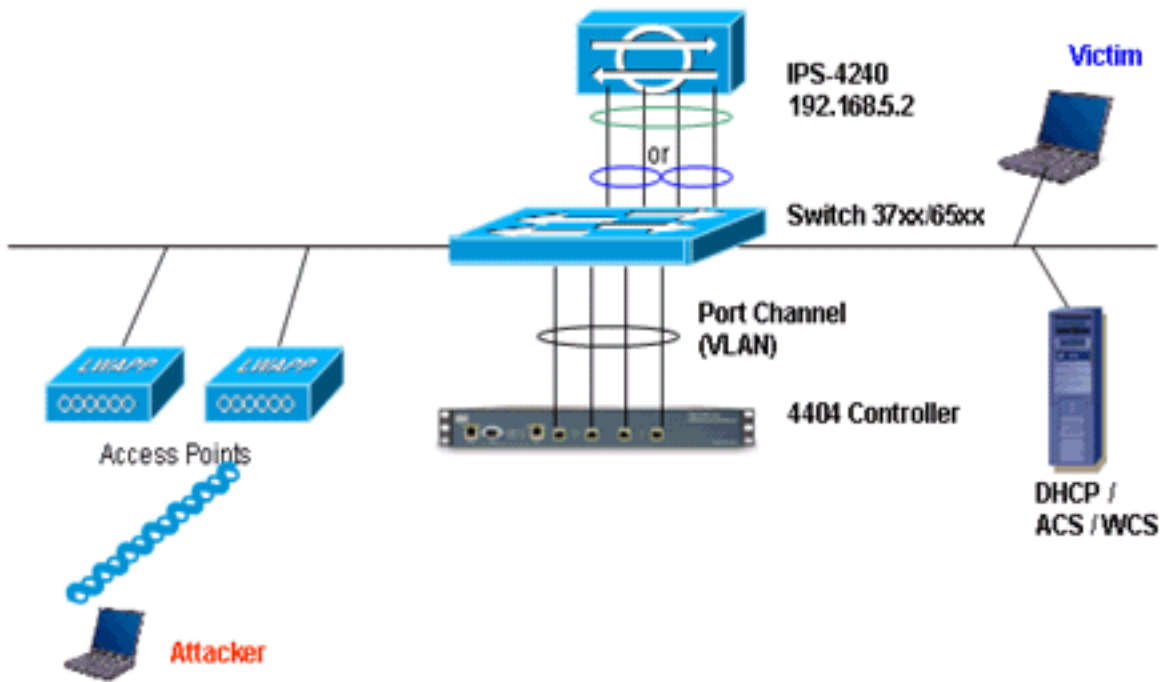
Op de controller wordt elke client uitgeschakeld met een IDS-sensor-aanvraag. De CLI **show** commando opdracht toont ook een lijst met klanten die op de zwarte lijst staan.

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 | Type | 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
```

```
!
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
```

```
!
interface GigabitEthernet5/2
 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 port-channel 99
Building configuration...
```

```
Current configuration : 153 bytes
!
interface Port-channel99
 switchport
 switchport trunk encapsulation dot1q
 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 [architectuurdiagram](#) is slechts een voorbeeldinstelling van de geïntegreerde WLC- en IPS-architectuur. De voorbeeldconfiguratie die hier wordt getoond, verklaart de IDS-sensatieinterface die in Promiscuous Mode werkt. In het [architectuurschema](#) is te zien hoe de sensatieinterfaces aan elkaar worden gekoppeld om in de modus Inline paar te kunnen optreden. Raadpleeg de [inline modus](#) 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
-----
Type                : 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 https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet (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) interface-adres(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 40.0.0.0/8
```

```
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 ---
```

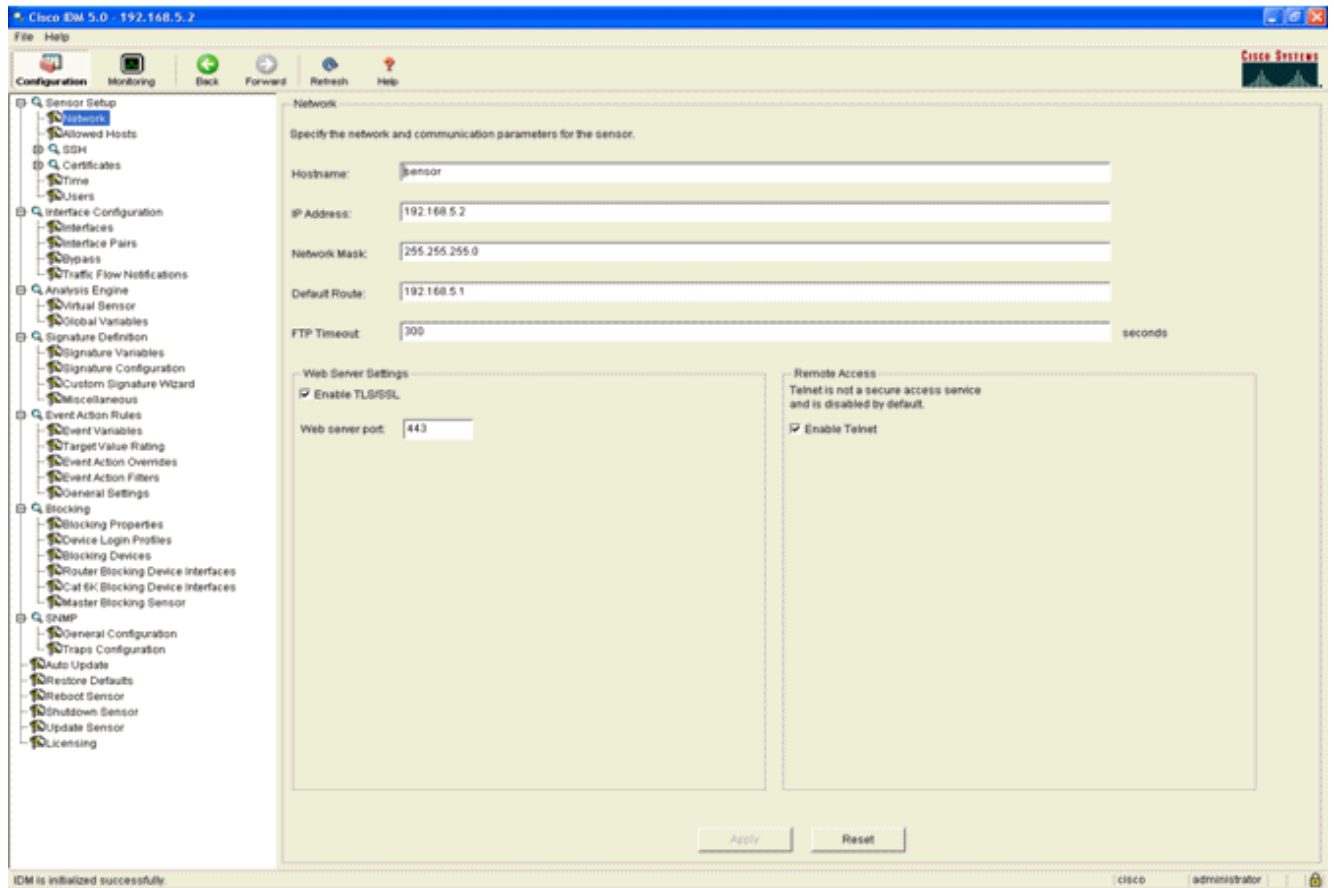
```
4 packets transmitted, 4 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.3/0.6/1.0 ms
```

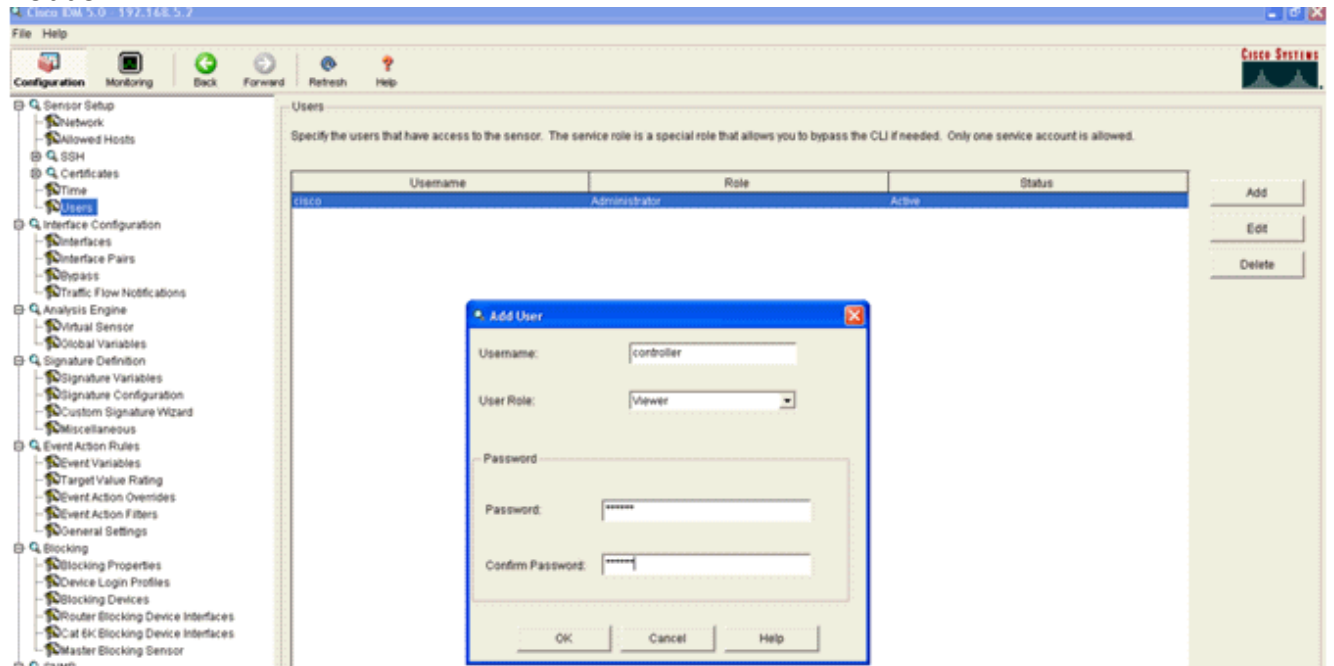
```
sensor#
```

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

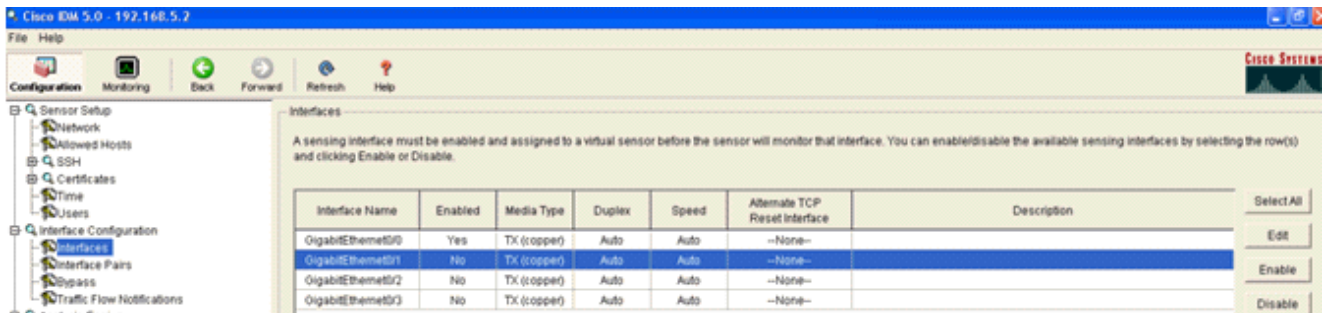
het beheer van de sensor. Dit beeld geeft een voorbeeld weer waarin de sensor is ingesteld in 192.168.5.2.



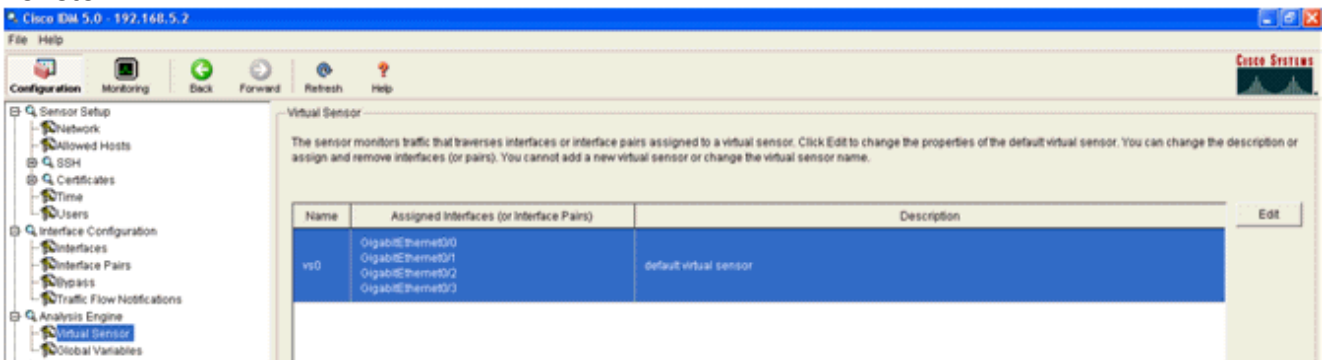
5. Voeg een gebruiker toe die de WLC gebruikt om tot de IPS Sensor gebeurtenissen toegang te hebben.



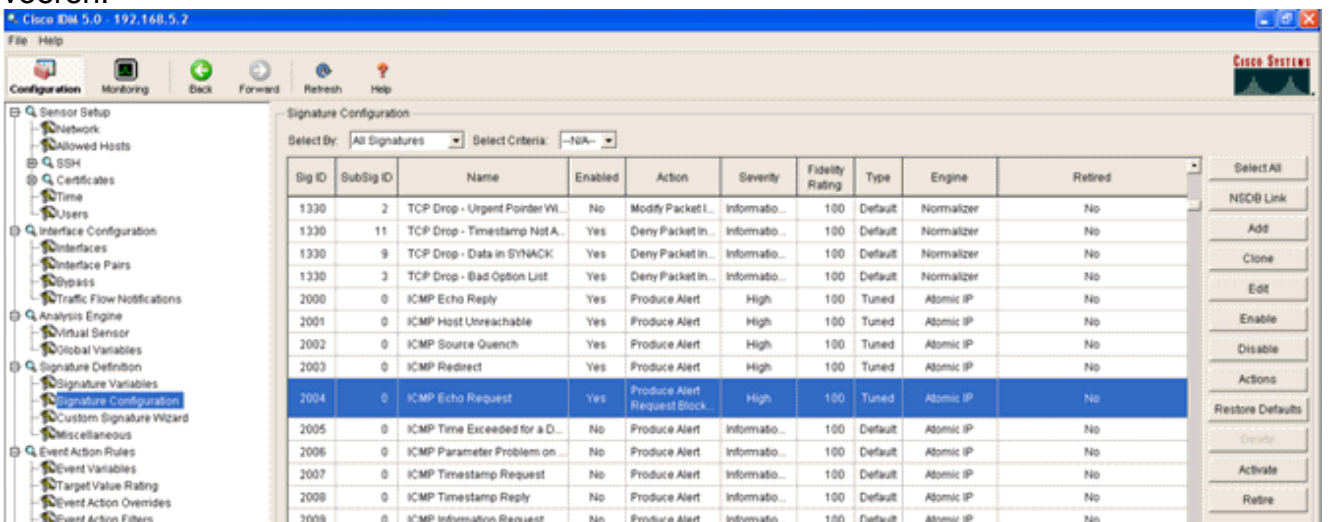
6. Schakel de bewakingsinterfaces in.



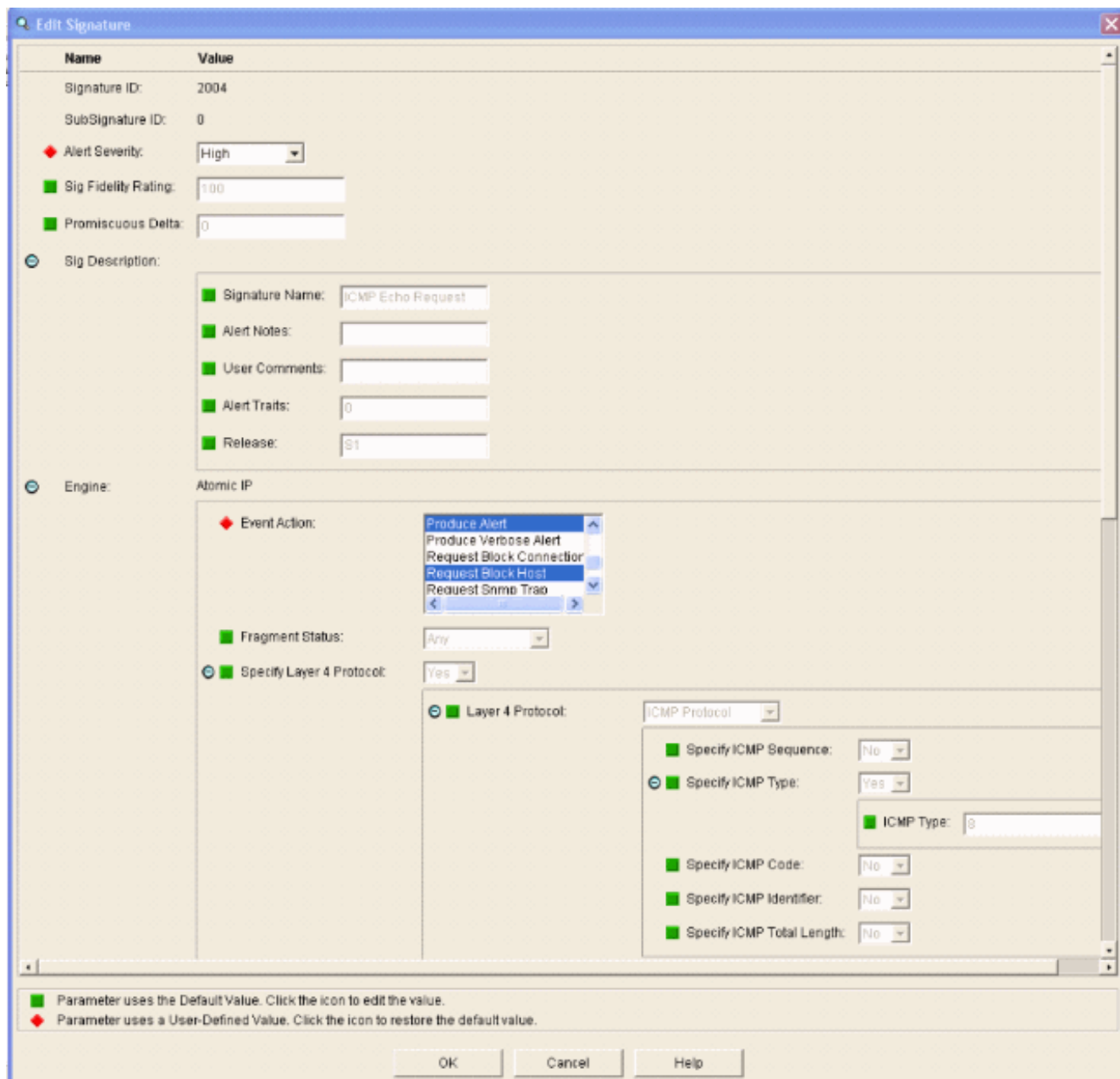
De bewakingsinterfaces moeten worden toegevoegd aan de Analyse-engine, zoals blijkt uit dit venster:



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



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.
2. 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
```

Cisco Systems Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

CIDS Sensor Add < Back Apply

Index 1

Server Address 192.168.5.2

Port 443

Username controller

Password *****

Confirm Password *****

Query Interval 15 seconds

State

Fingerprint (SHA1 hash) 1662E996362A9A1EF08B99A7C1645F5CB56A8842 40 hex chars

AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies

Access Control Lists

Network Access Control

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
Management Frame Protection

Web Login Page

CIDS
Sensors
Shunned Clients

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

Cisco Systems Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Security

CIDS Sensors List New...

| Index | Server Address | Port | State | Query Interval | Last Query (count) | |
|-------|----------------|------|---------|----------------|--------------------|---|
| 1 | 192.168.5.2 | 443 | Enabled | 15 | Success (6083) | Detail Remove |

AAA
General
RADIUS Authentication
RADIUS Accounting
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies

Access Control Lists

Network Access Control

IPSec Certificates
CA Certificate
ID Certificate

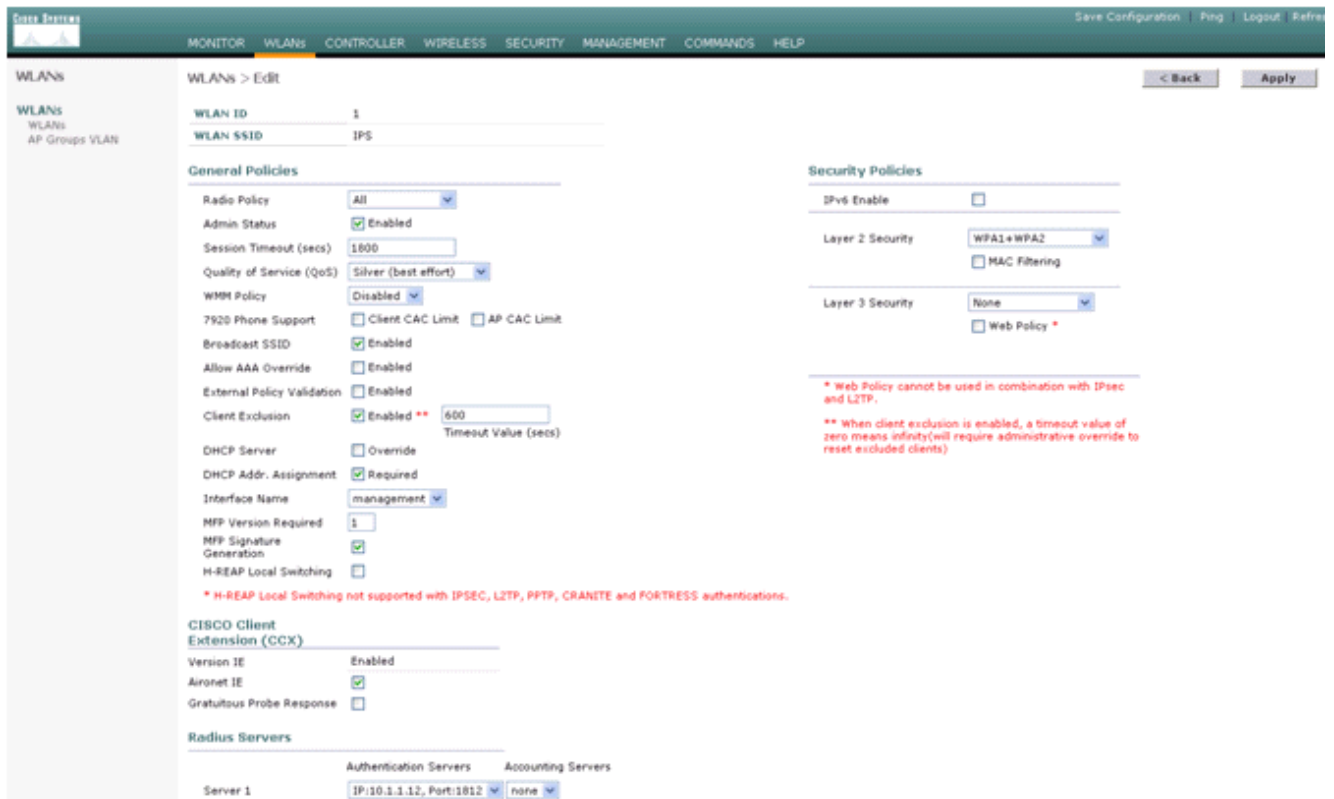
Web Auth Certificate

Wireless Protection Policies
Trusted AP Policies
Rogue Policies
Standard Signatures
Custom Signatures
Signature Events
Summary
Client Exclusion Policies
AP Authentication
Management Frame Protection

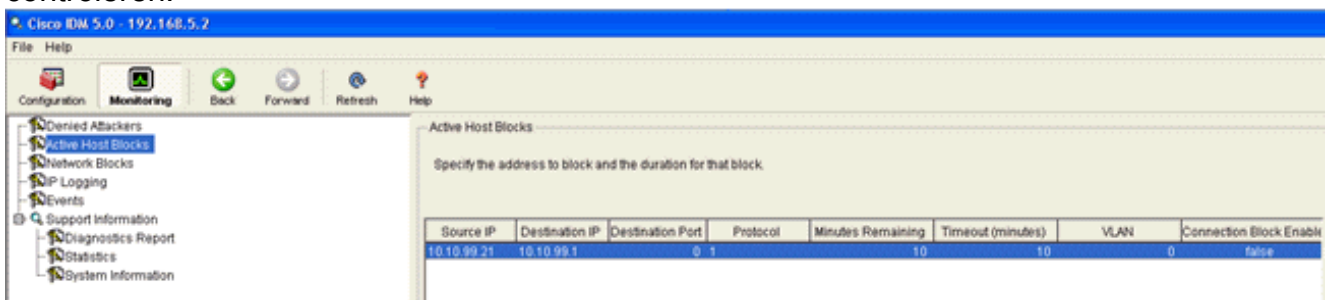
Web Login Page

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.



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.



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

The screenshot shows the Cisco Systems Security page. The left sidebar contains a navigation menu with categories: AAA, Access Control Lists, Network Access Control, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, and Web Login Page. The main content area is titled "CIDS Shun List" and features a "Re-sync" button. Below the button is a table with the following data:

| IP Address | Last MAC Address | Expire | Sensor IP / Index |
|-------------|-------------------|-----------|-------------------|
| 10.10.99.21 | 00:40:96:ad:0d:1b | 326979296 | 192.168.5.2 / 1 |

host.
gebruiker wordt toegevoegd aan de lijst
Clientuitsluiting.

De

The screenshot shows the Cisco Systems Monitor page. The left sidebar contains a navigation menu with categories: Monitor, Summary, Statistics, Controller, Ports, and Wireless. The main content area is titled "Excluded Clients" and features a search bar labeled "Search by MAC address" with a "Search" button. Below the search bar is a table with the following data:

| Client MAC Addr | AP Name | AP MAC Addr | WLAN | Type | Exclusion Reason | Port | |
|-------------------|----------|-------------------|------|---------|------------------|------|---|
| 00:40:96:ad:0d:1b | AP1242-2 | 00:14:1b:59:3e:10 | IPS | 802.11b | UnknownEnum:5 | 29 | Detail Link Test Disable Remove |

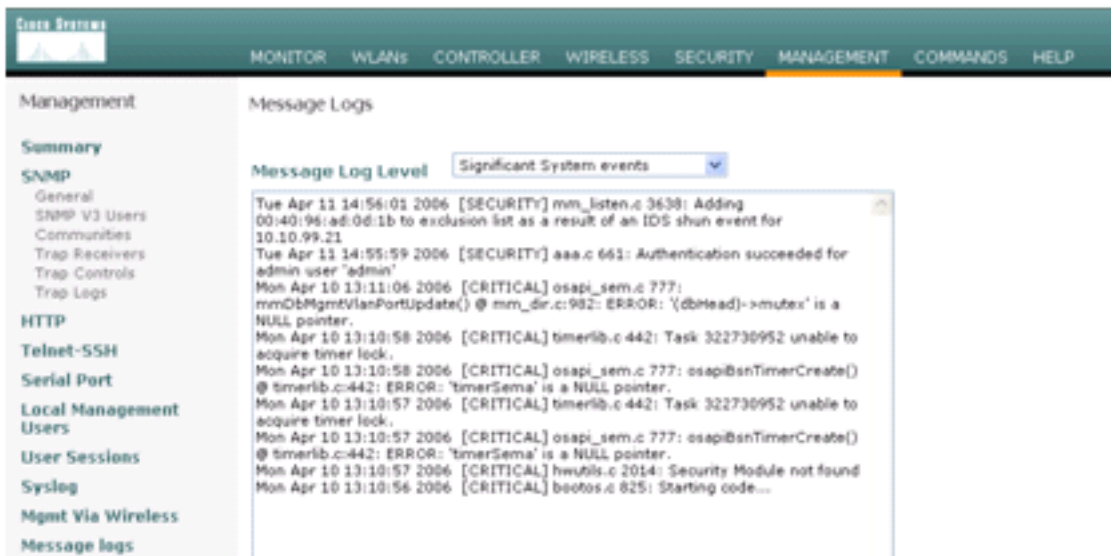
Een logbestand wordt gegenereerd als een client wordt toegevoegd aan de lijst met

The screenshot shows the Cisco Systems Management page. The left sidebar contains a navigation menu with categories: Management, Summary, and SNMP. The main content area displays a log of events with the following data:

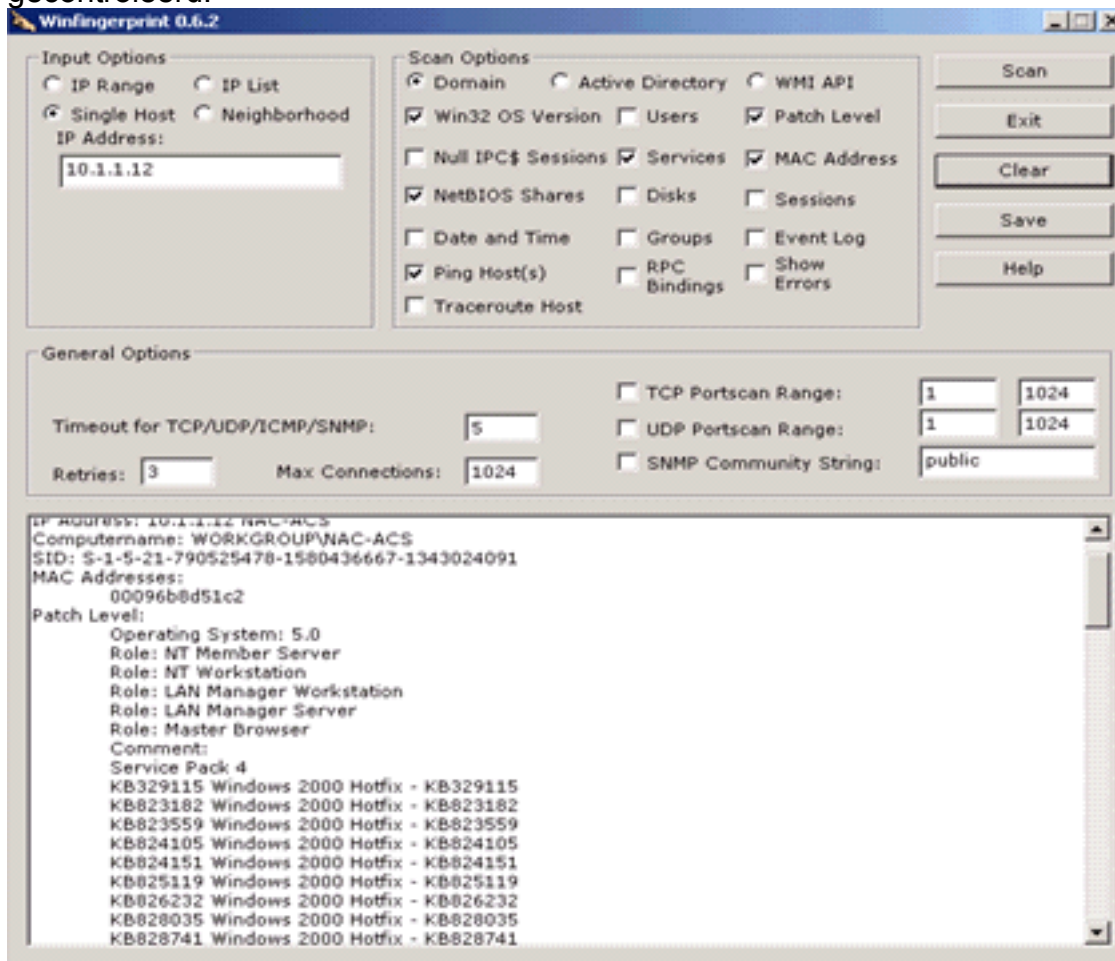
| Event ID | Time | Message |
|----------|--------------------------|---|
| 32 | Tue Apr 11 14:41:00 2006 | Rogue AP : 00:15:c7:02:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) with RSSI: -83 and SNR: 6 |
| 33 | Tue Apr 11 14:40:16 2006 | New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2 |
| 34 | Tue Apr 11 14:39:44 2006 | Rogue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) |
| 35 | Tue Apr 11 14:39:44 2006 | Rogue : 00:0b:85:54:de:5e removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) |
| 36 | Tue Apr 11 14:39:44 | Rogue : 00:0b:85:54:de:5f removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) |

tonnen.
wordt ook een berichtlogbestand gegenereerd voor de

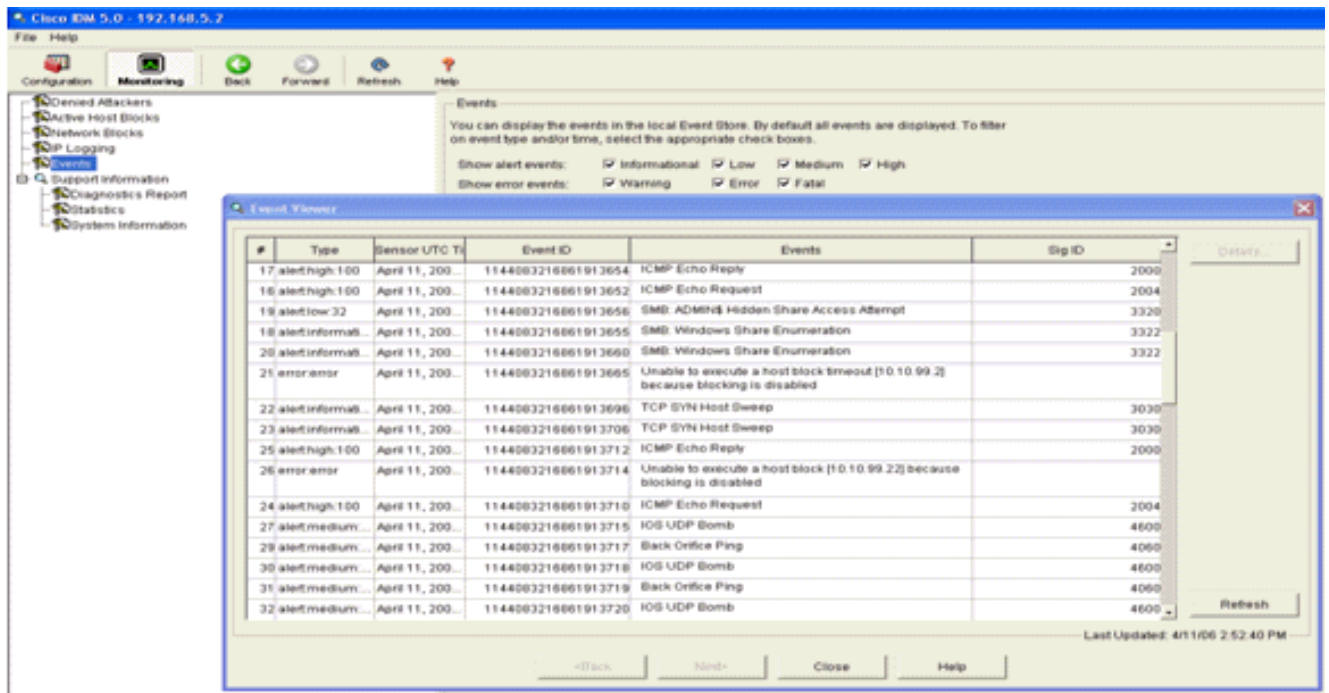
Er



gebeurtenis. S
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.



Dit venster toont gebeurtenissen die in de Cisco IPS Sensor zijn gegenereerd.



[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 10.0.0.0/8
access-list 40.0.0.0/8
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

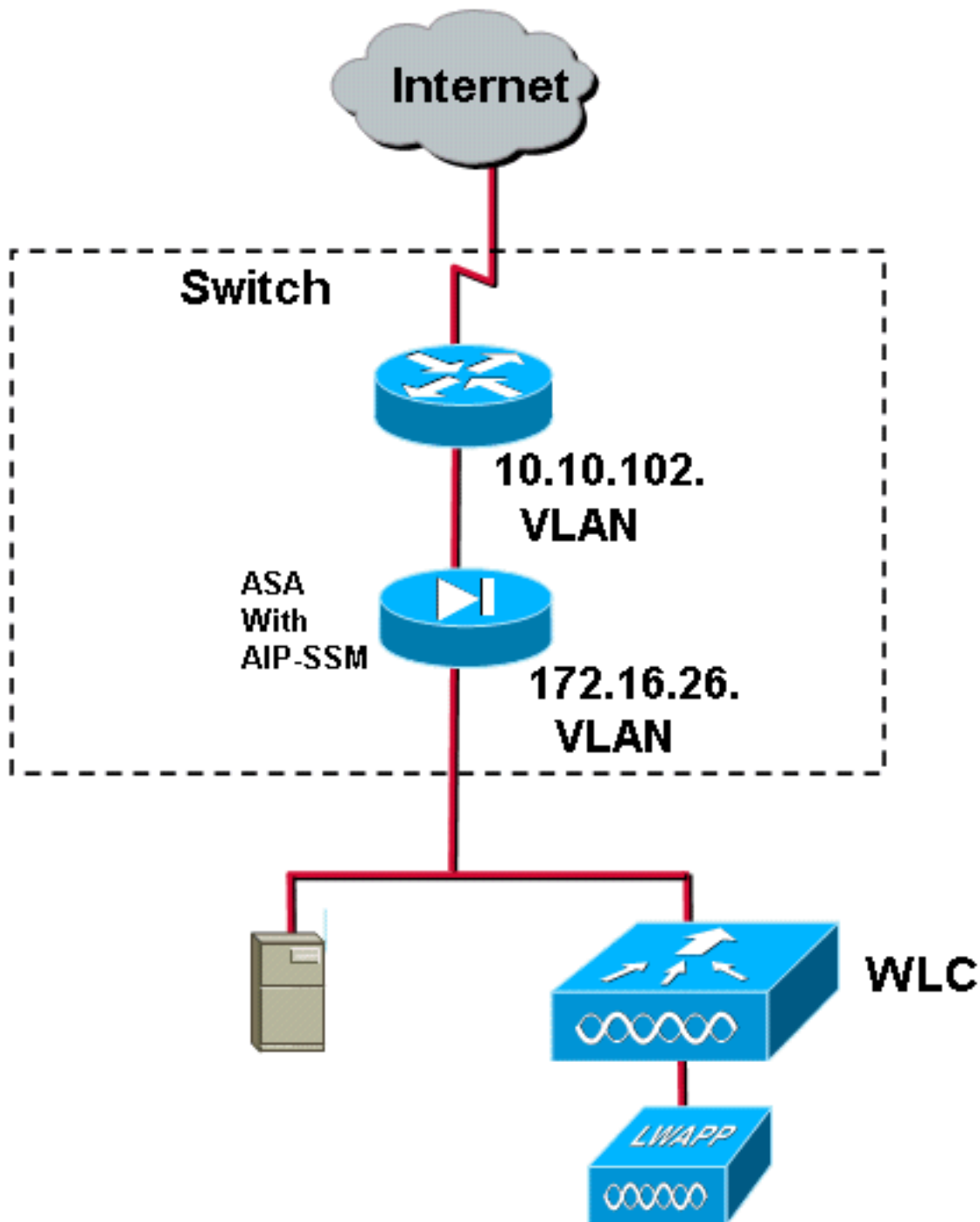
```

```
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](#)

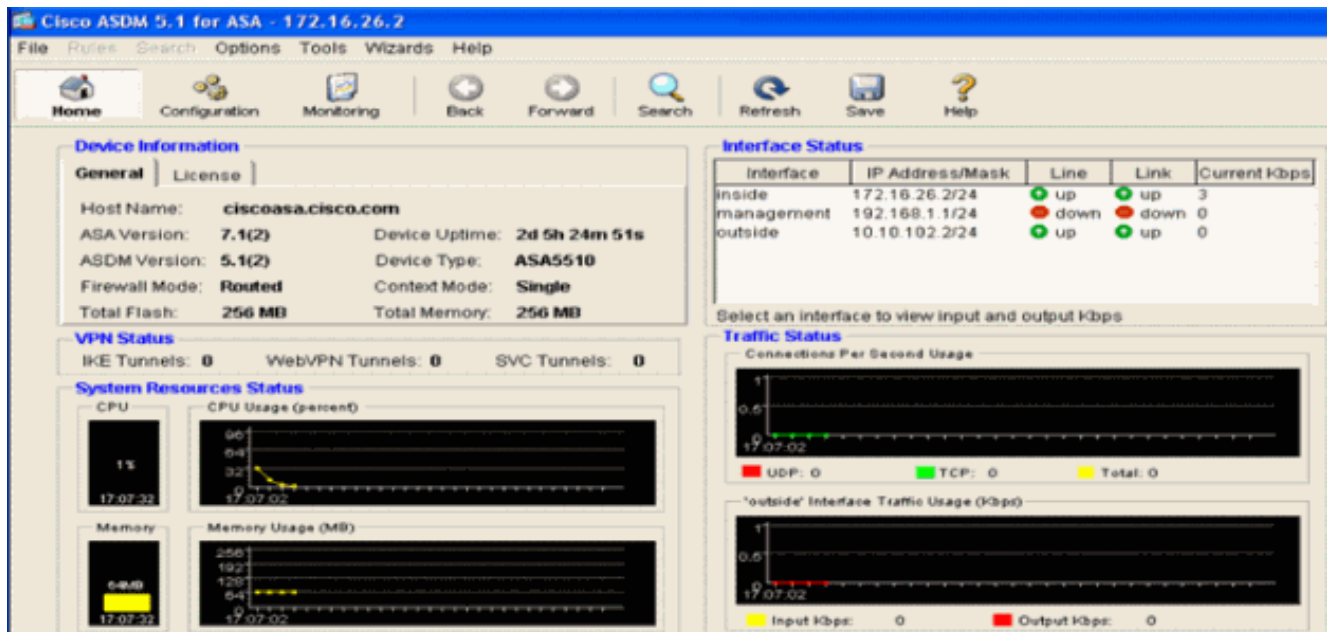
In tegenstelling tot een traditionele inbraakdetectiesensor moet een ASA altijd in het datapad zijn. Met andere woorden, in plaats van het oversteken van verkeer van een switch poort naar een

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.

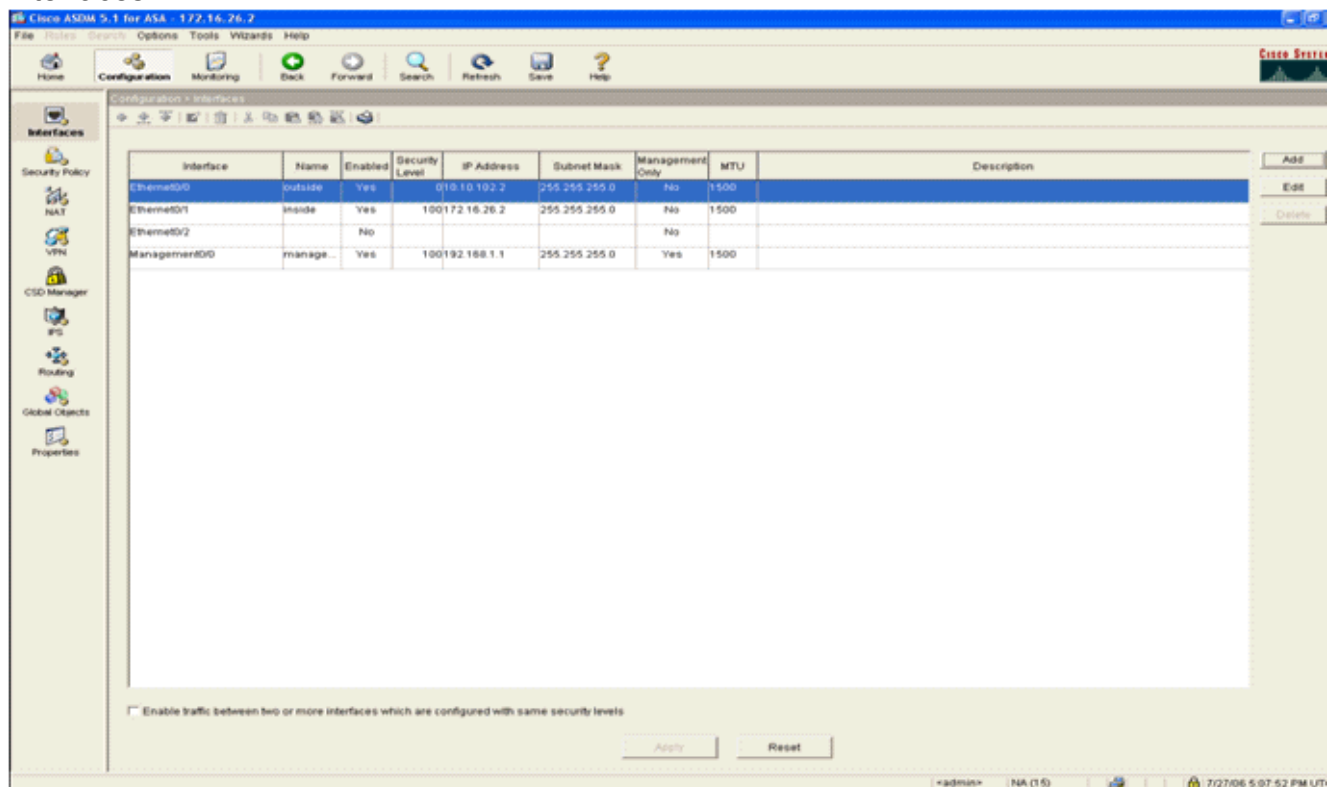


In dit voorbeeld is de ASA die gebruikt wordt al ingesteld en passeert verkeer. Deze stappen tonen aan hoe een beleid te creëren dat gegevens naar het AIP-SSM stuurt.

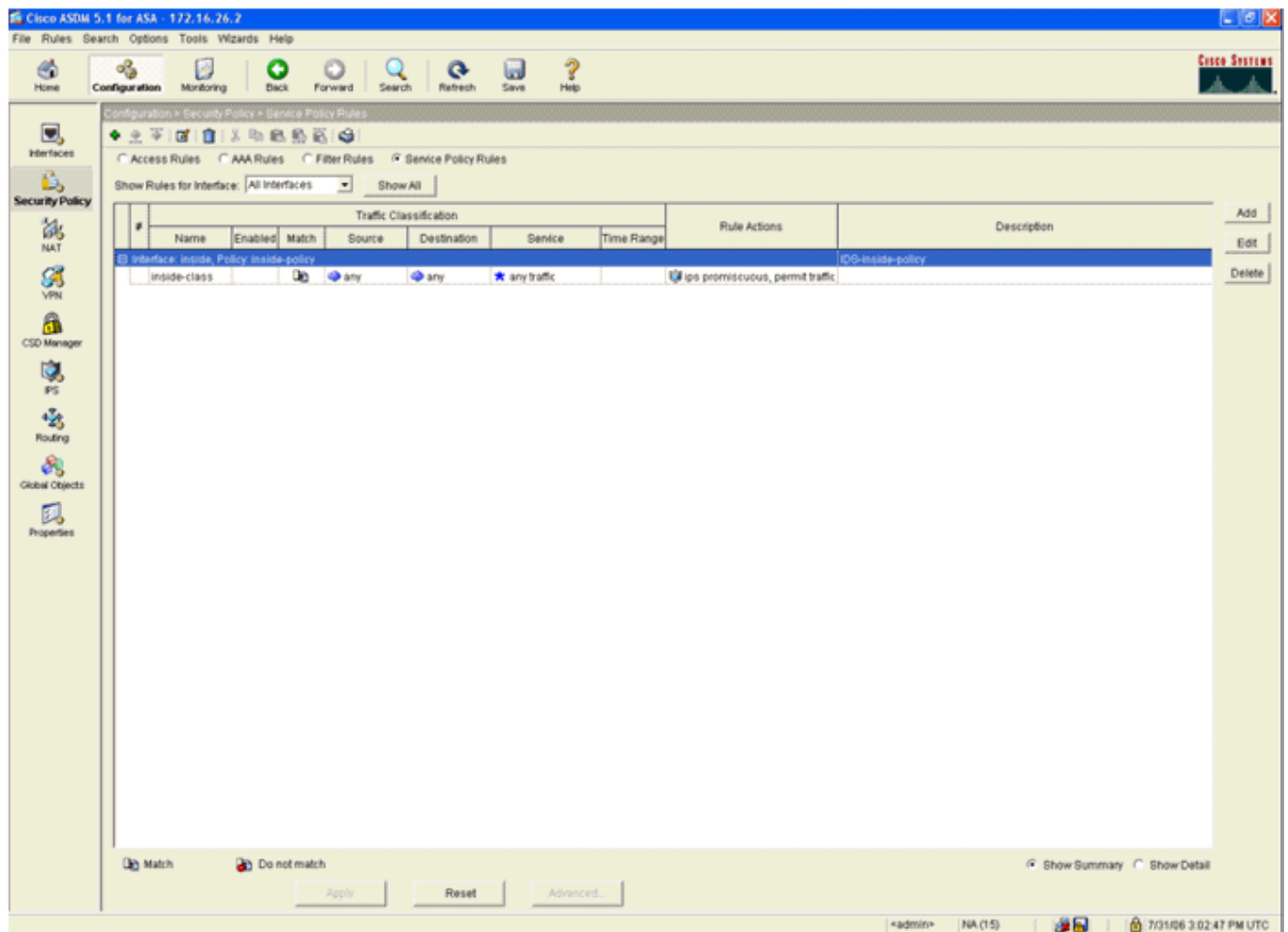
1. Meld u aan in de ASA met ASDM. Na succesvolle inloggen verschijnt het ASA Main System venster.



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



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



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 policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Interface:

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

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 eenvoudig geselecteerd. Klik op **Volgende** om verder te gaan

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic match criteria

Default Inspection Traffic

Source and Destination IP Address (uses ACL)

Tunnel Group

TCP or UDP Destination Port

RTP Range

IP DiffServ CodePoints (DSCP)

IP Precedence

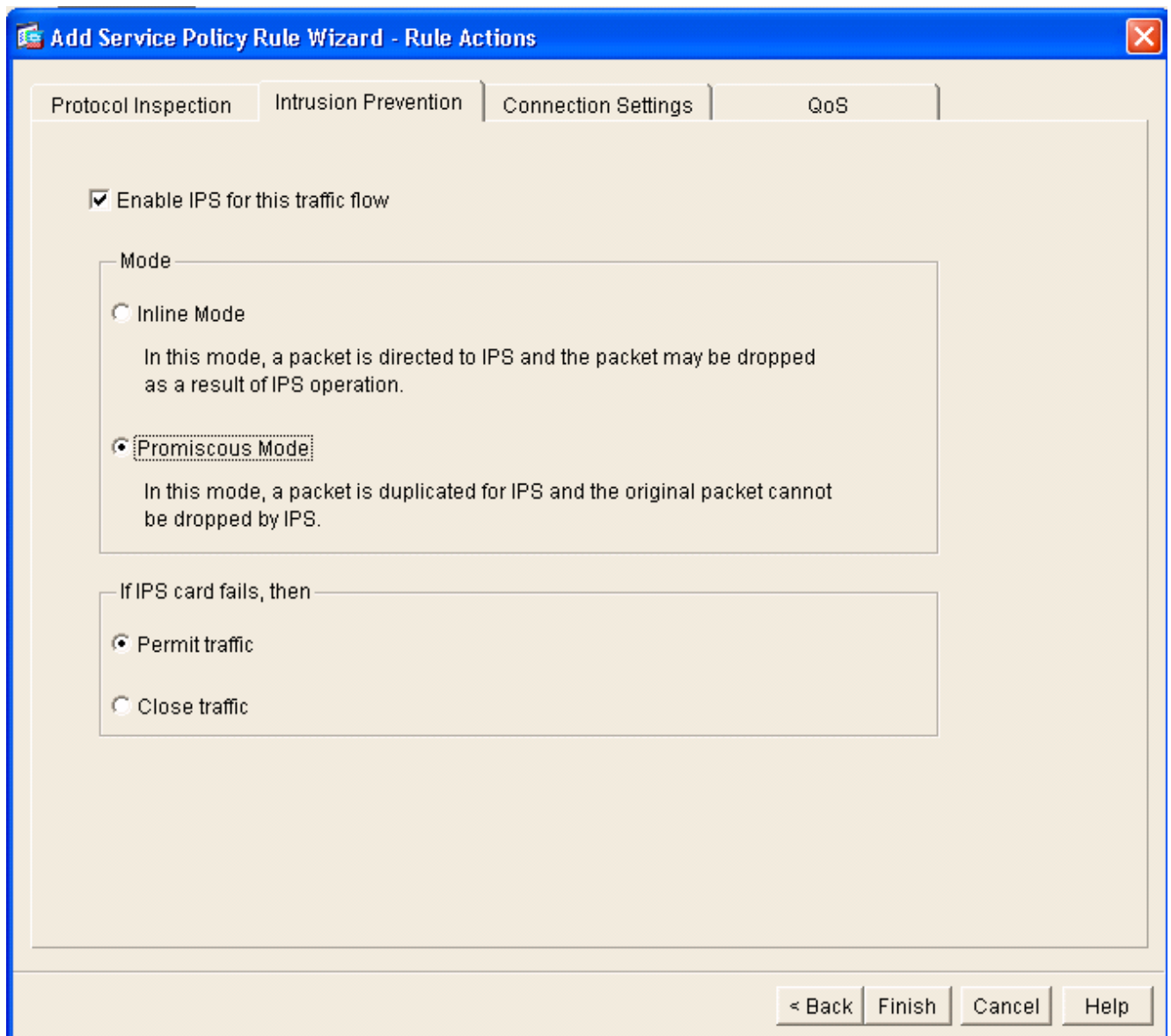
Any traffic

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

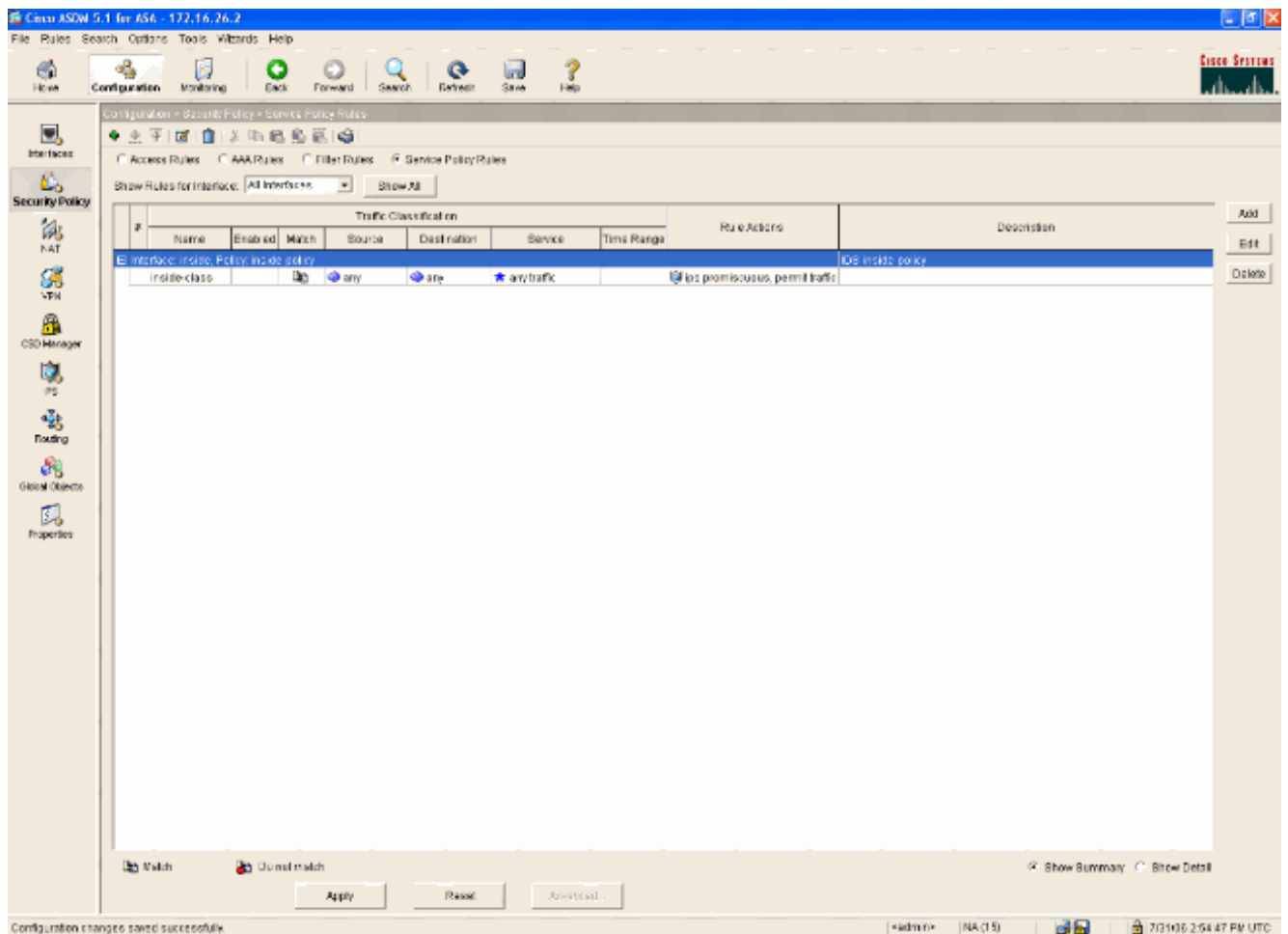
Use class-default as the traffic class.

< 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 **Voltoeien** om de wijziging aan te geven.



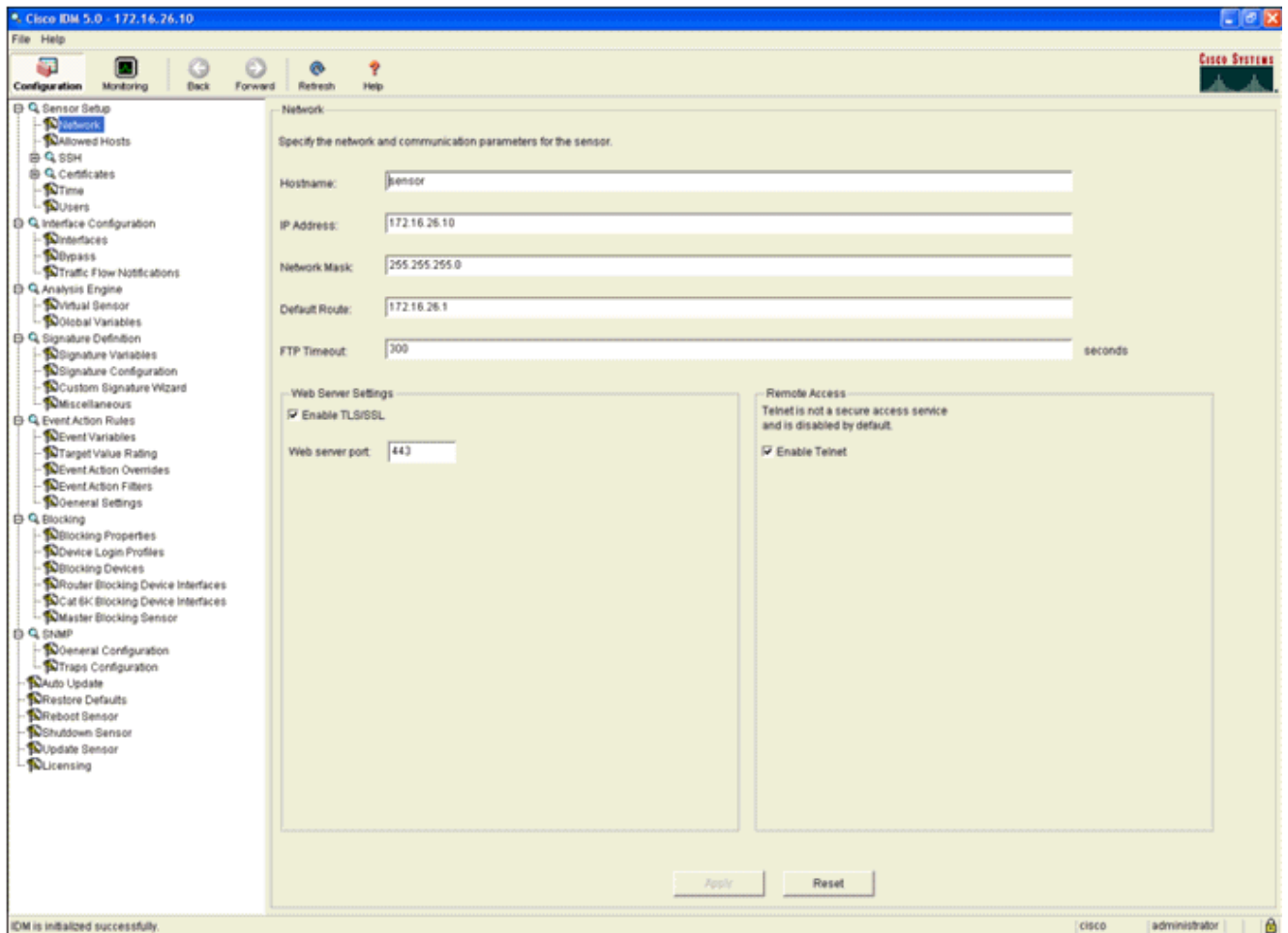
7. ASA is nu ingesteld om verkeer naar de IPS-module te sturen. Klik op **Save** in de bovenste rij om de wijzigingen in de ASA te schrijven.



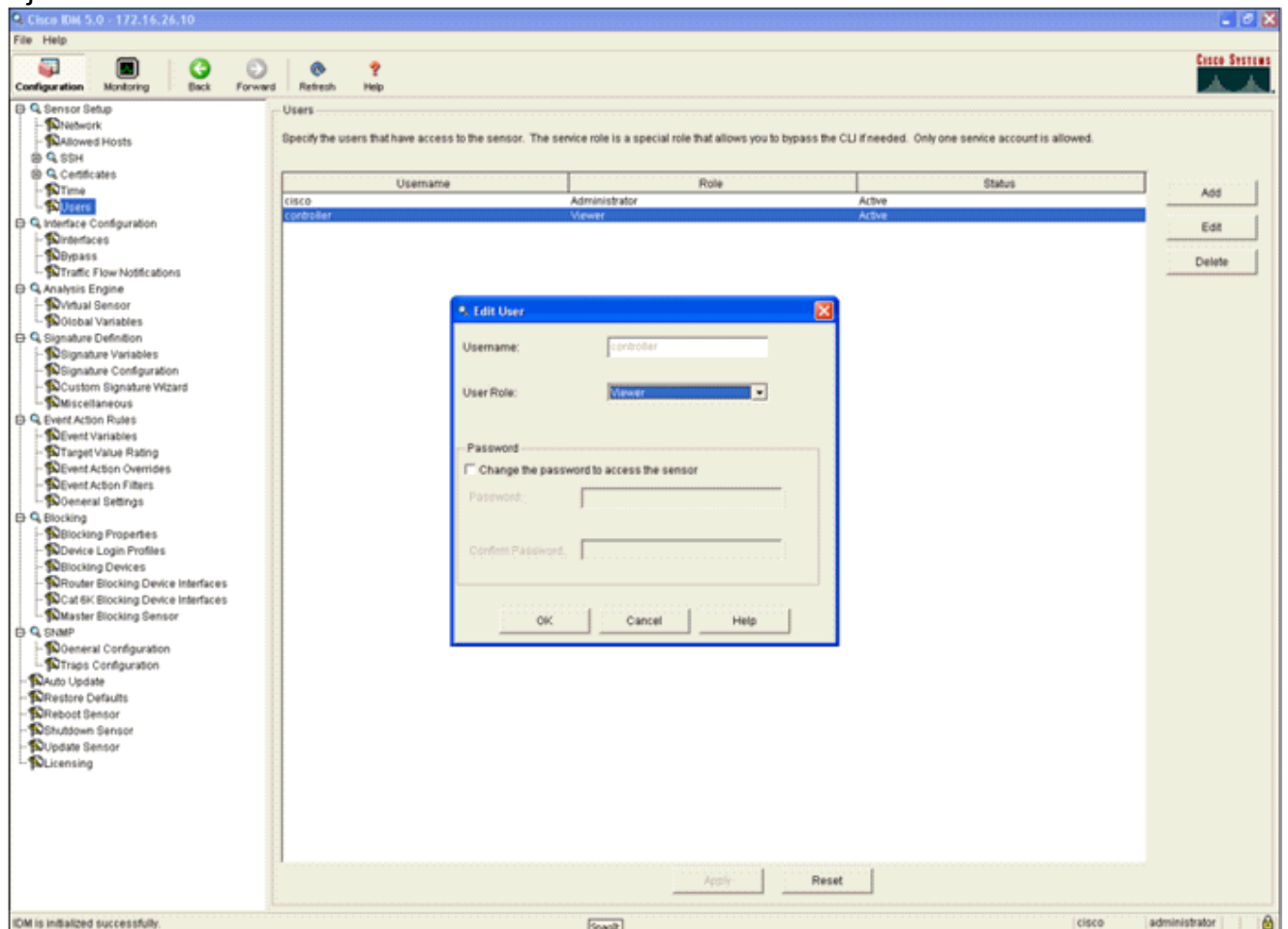
Het AIP-SSM configureren voor verkeersinspectie

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

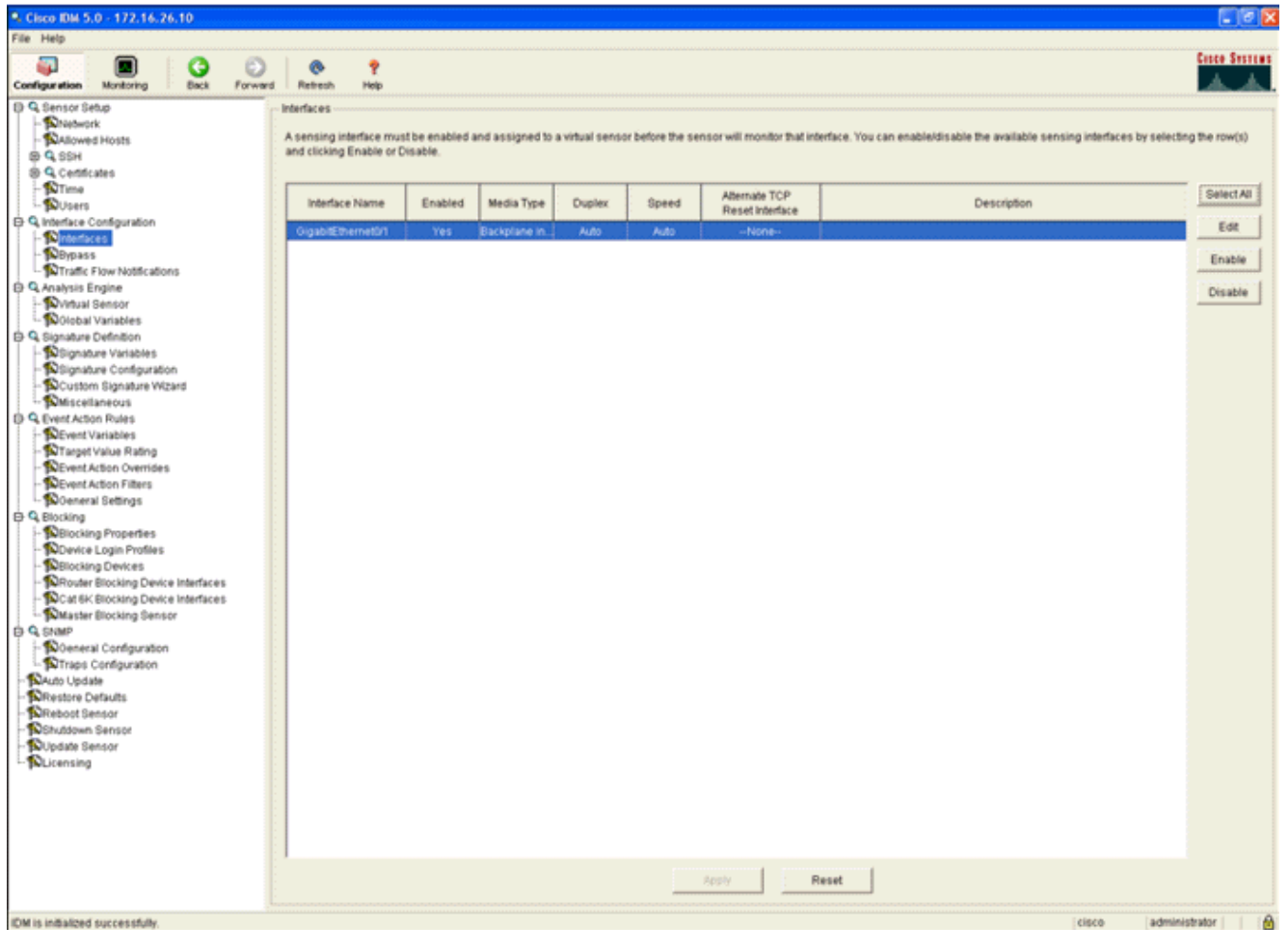
1. Aanmelden bij de AIP-SSM met IDM.



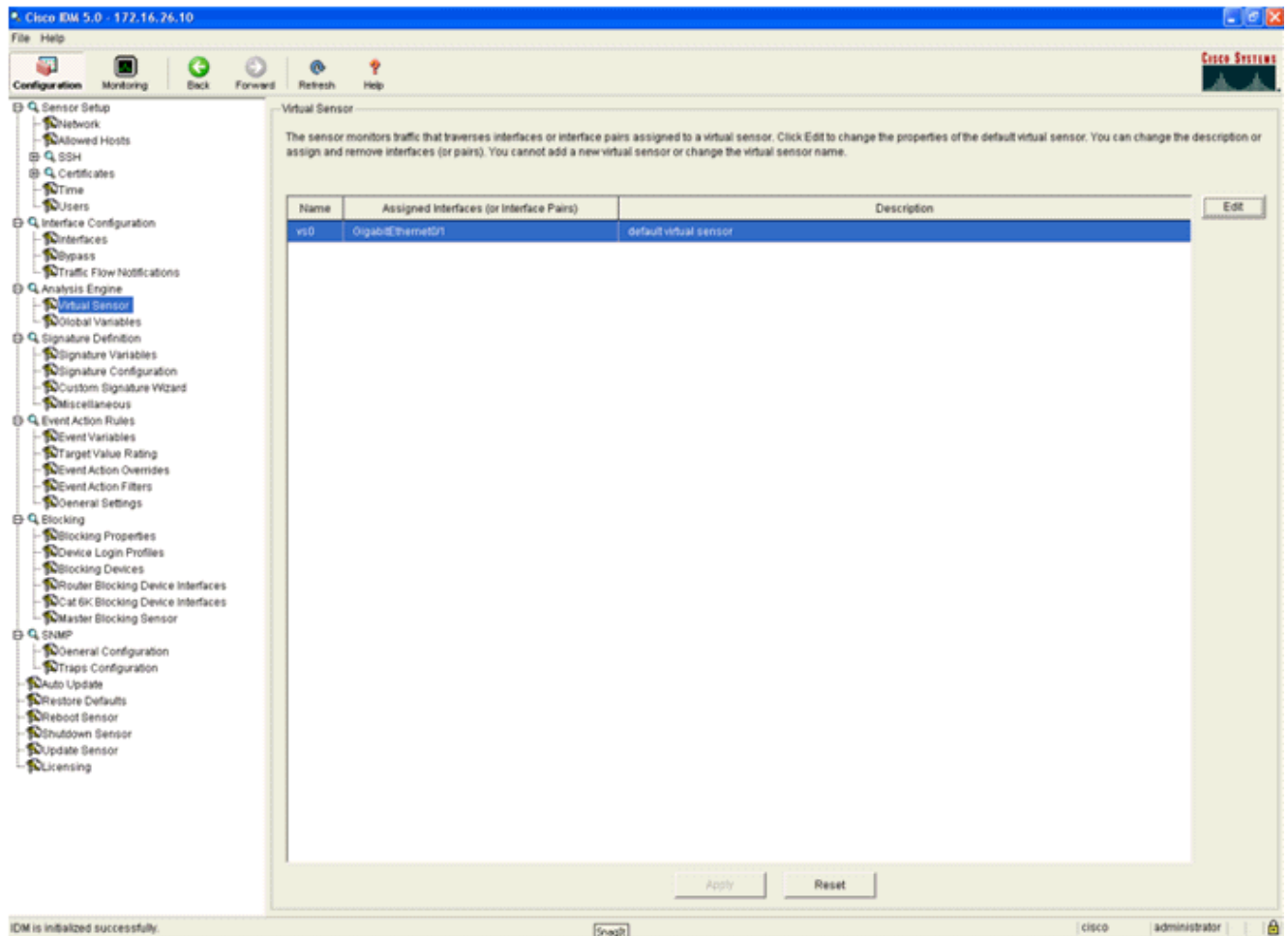
2. Voeg een gebruiker toe met minstens kijkerrechten.



3. Schakel de interface in.



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.

```
sensor#show tls fingerprint
```

```
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
```

The screenshot shows the Cisco Systems Security page with the 'CIDS Sensor Edit' configuration. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area displays the following configuration details:

- Index:** 2
- Server Address:** 172.16.26.10
- Port:** 443
- Username:** controller
- Password:** *****
- State:**
- Query Interval:** 10 seconds
- Fingerprint (SHA1 hash):** 90C9969B4EFA74F8528092BDBC483C45B4876C55 (40 hex chars) (hash key is already set)
- Last Query (count):** Success (1400)

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

The screenshot shows the Cisco Systems Security page with the 'CIDS Sensors List' configuration. The left sidebar is identical to the previous screenshot. The main content area displays a table with the following data:

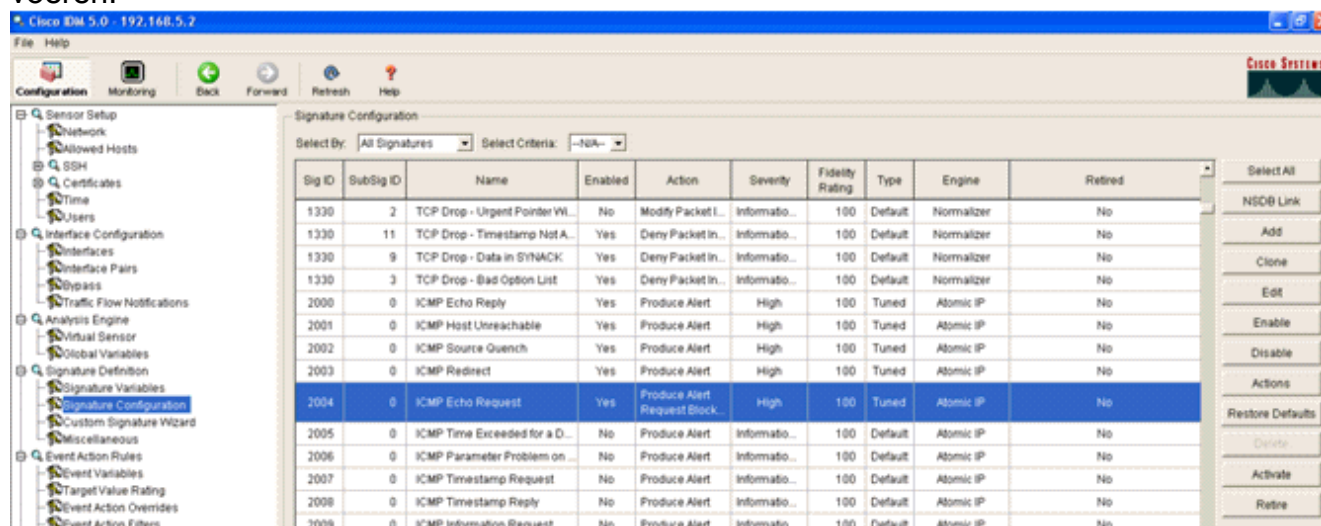
| Index | Server Address | Port | State | Query Interval | Last Query (count) | |
|-------|----------------|------|---------|----------------|--------------------|---|
| 1 | 192.168.5.2 | 443 | Enabled | 15 | Unauthorized (1) | Detail Remove |
| 2 | 172.16.26.10 | 443 | Enabled | 10 | Success (1444) | Detail Remove |

[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

voeren.



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.

Edit Signature

| Name | Value |
|----------------------|-------|
| Signature ID: | 2004 |
| SubSignature ID: | 0 |
| Alert Severity: | High |
| Sig Fidelity Rating: | 100 |
| Promiscuous Delta: | 0 |

Sig Description:

Signature Name: ICMP Echo Request

Alert Notes:

User Comments:

Alert Traits: 0

Release: B1

Engine: Atomic IP

Event Action: Produce Alert

Fragment Status: Any

Specify Layer 4 Protocol: Yes

Layer 4 Protocol: ICMP Protocol

Specify ICMP Sequence: No

Specify ICMP Type: Yes

ICMP Type: 8

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

| Name | Value |
|----------------------|---------------|
| Signature ID: | 2004 |
| SubSignature ID: | 0 |
| Alert Severity: | Informational |
| Sig Fidelity Rating: | 100 |
| Promiscuous Delta: | 0 |

Sig Description:

| | |
|-----------------|-------------------|
| Signature Name: | ICMP Echo Request |
| Alert Notes: | |
| User Comments: | |
| Alert Traits: | 0 |
| Release: | 81 |

Engine: Atomic IP

Event Action: Request Block Host

Fragment Status: Any

Legend:
 ■ 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.

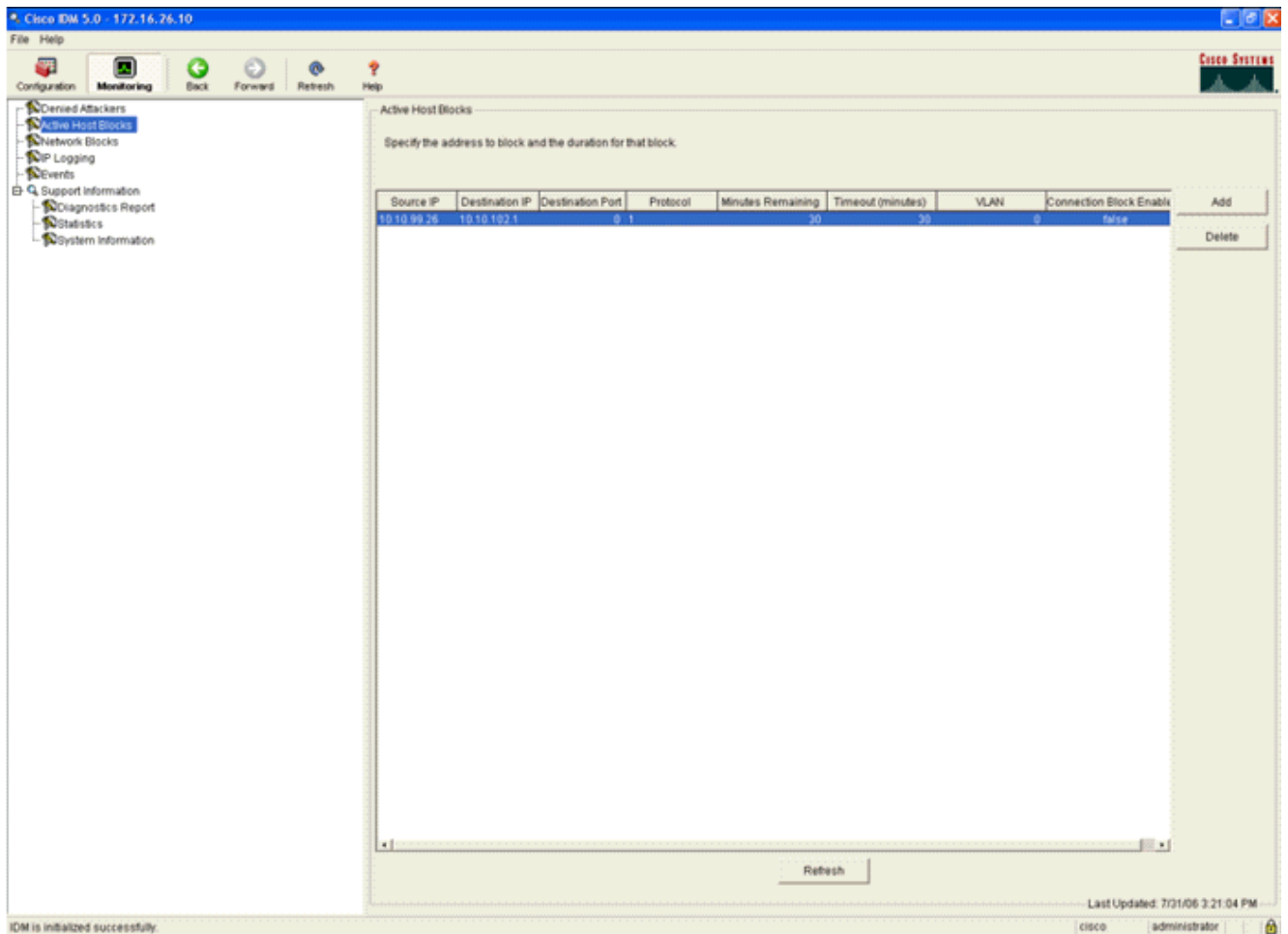
Buttons: OK, Cancel, Help

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.

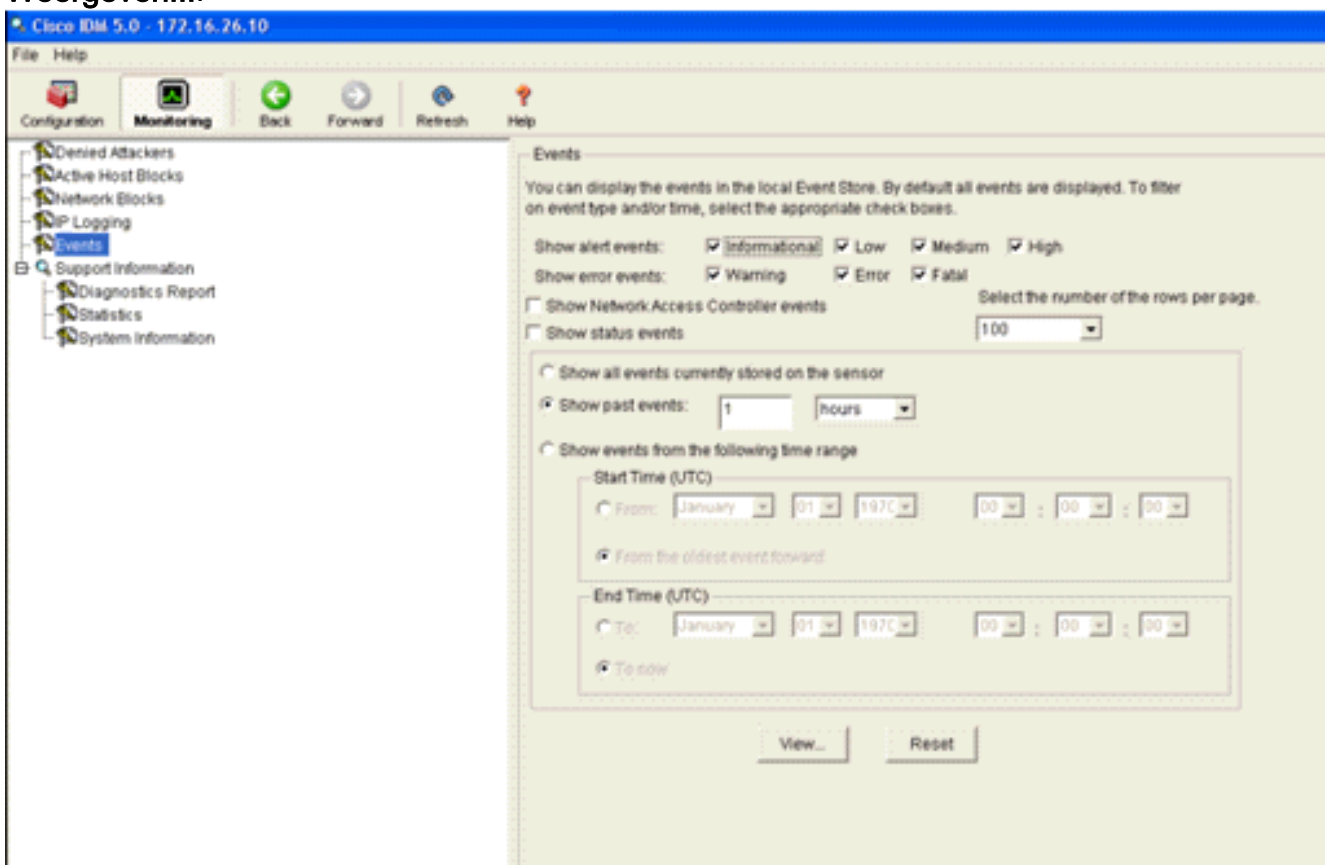
Monitorblokkering en gebeurtenissen met IDM

Voer de volgende stappen uit:

1. 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....**



2. Het Event Viewer verschijnt dan met een lijst van gebeurtenissen die voldoen aan de gegeven criteria. Scrollt 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 ID.

| # | Type | Sensor UTC Time | EventID | 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 | alert:informati... | July 31, 2006 3:19:46 PM U... | 1145383740954941597 | ICMP Echo Request | 2004 | |

Last Updated: 7/31/06 3:22:39 PM

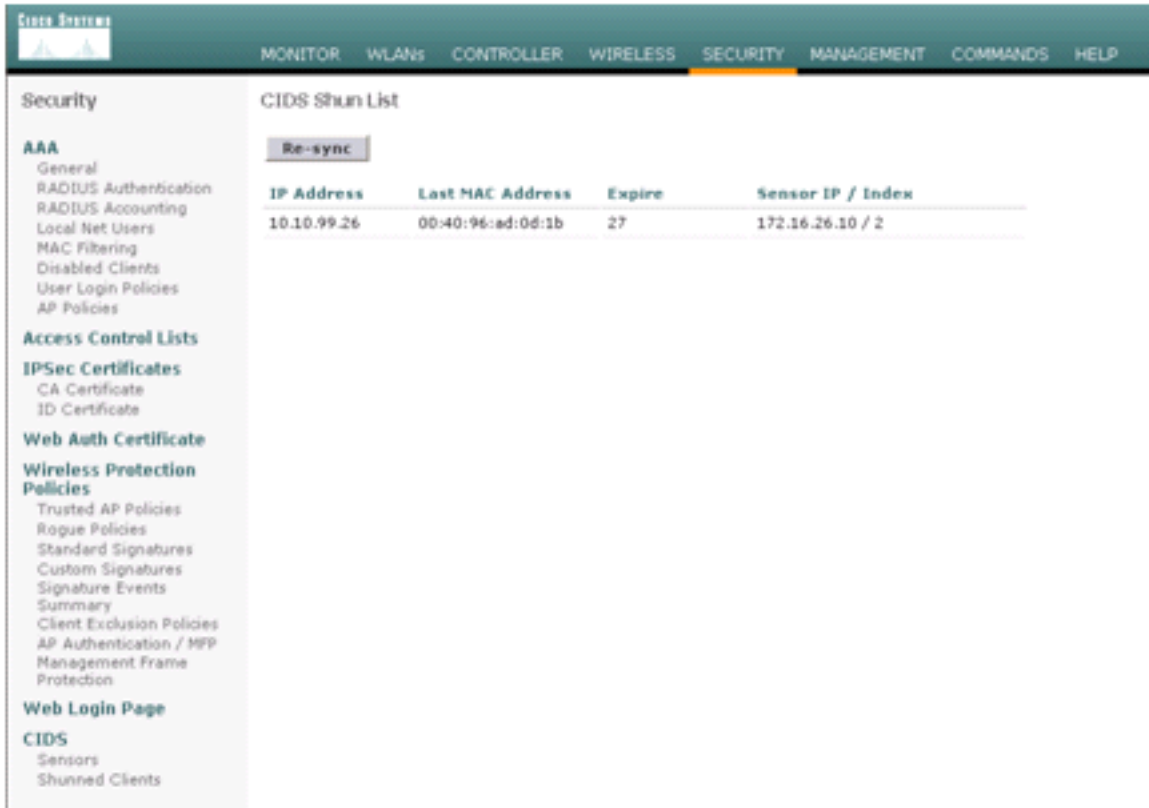
3. Nadat u de handtekening hebt geplaatst, dubbelklikt u op de ingang om een nieuw venster te openen. Het nieuwe venster bevat gedetailleerde informatie over de gebeurtenis die tot de handtekening heeft geleid.

```

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

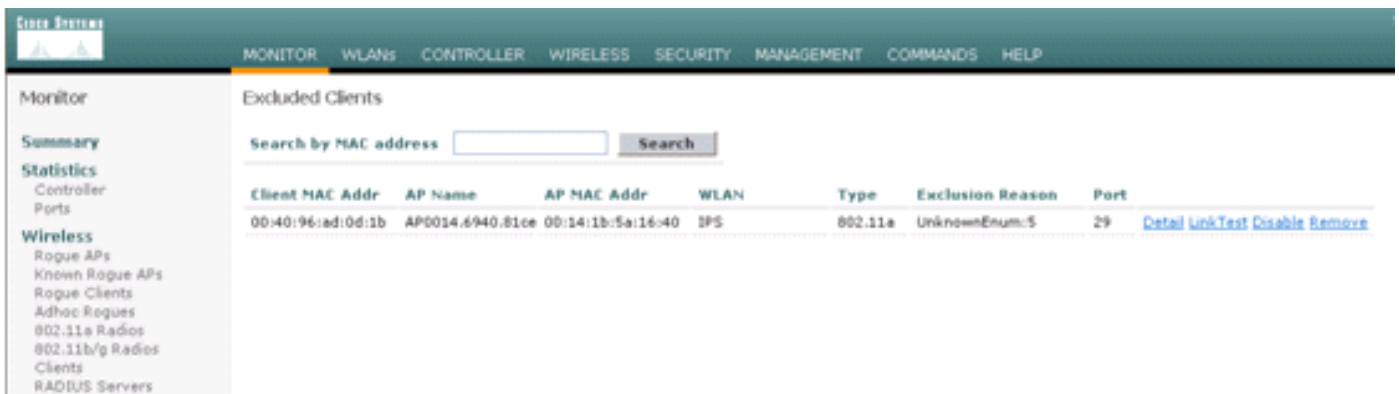
De lijst Gekoppelde clients in de controller is op dit moment ingevuld met het IP- en MAC-adres van de host.



The screenshot shows the Cisco WCS interface with the 'SECURITY' tab selected. On the left, the 'Security' menu is expanded to show 'AAA' > 'CIDS'. The main area displays the 'CIDS Shun List' with a 'Re-sync' button and a table of shunned clients.

| IP Address | Last MAC Address | Expire | Sensor IP / Index |
|-------------|-------------------|--------|-------------------|
| 10.10.99.26 | 00:40:96:ad:0d:1b | 27 | 172.16.26.10 / 2 |

De gebruiker wordt toegevoegd aan de lijst Clientuitsluiting.



The screenshot shows the Cisco WCS interface with the 'MONITOR' tab selected. On the left, the 'Monitor' menu is expanded to show 'Wireless' > 'Excluded Clients'. The main area displays the 'Excluded Clients' page with a search bar and a table of excluded clients.

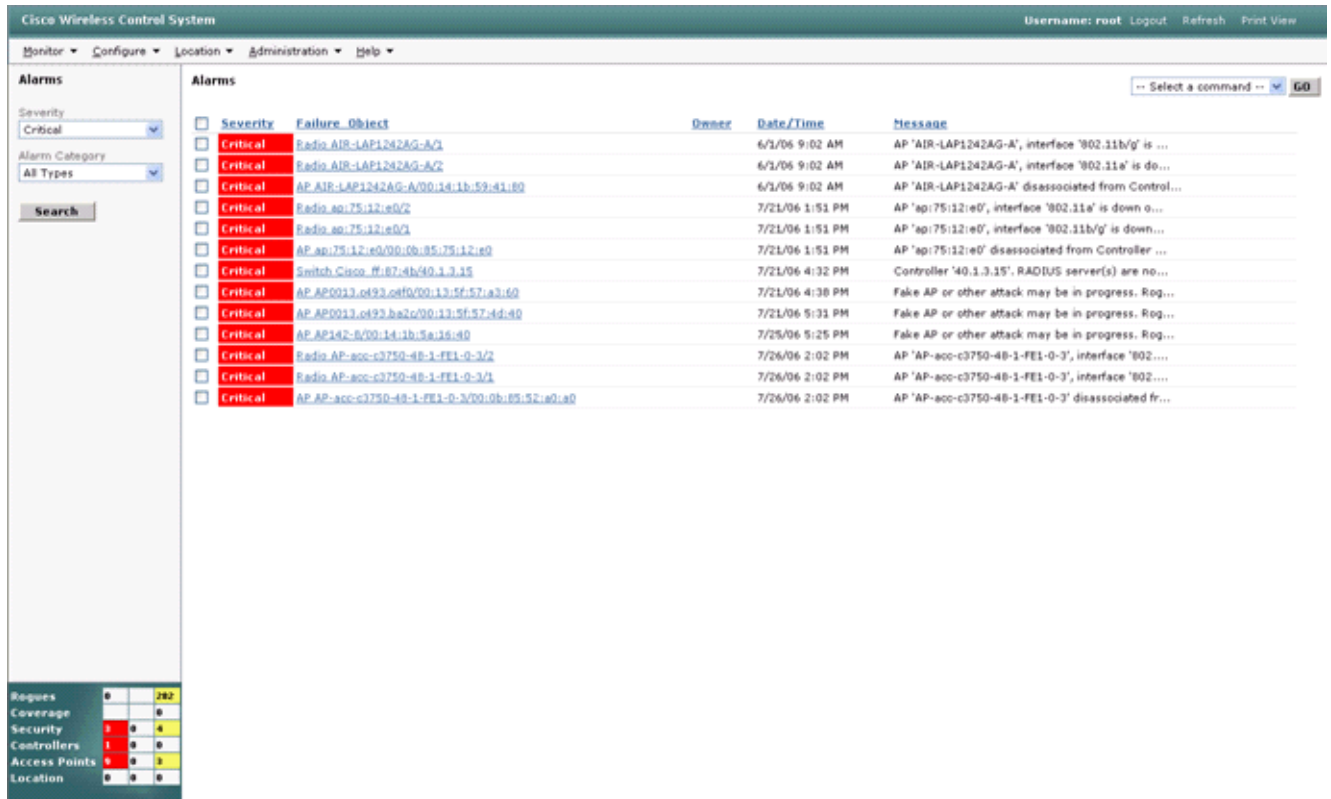
| Client MAC Addr | AP Name | AP MAC Addr | WLAN | Type | Exclusion Reason | Port | |
|-------------------|------------------|-------------------|------|---------|------------------|------|---|
| 00:40:96:ad:0d:1b | AP0014.6940.81ce | 00:14:1b:5a:16:40 | IPS | 802.11a | UnknownEnum:5 | 29 | Detail Link Text Disable Remove |

Monitoregebeurtenissen 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.

1. 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.

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



- 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.



Cisco ASA voorbeeldconfiguratie

```

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

```

```
names
!
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
!
interface Ethernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  management-only
!
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 10.0.0.0/8  
access-list 40.0.0.0/8  
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](#)
- [Cisco ASA 5500 Series adaptieve security applicaties - Configuratiehandleidingen](#)
- [De Cisco-sensor voor inbraakpreventiesysteem configureren met behulp van de opdrachtregel interface 5.0 - interfaces configureren](#)
- [WLC-configuratiegids 4.0](#)
- [Draadloze technische ondersteuning](#)
- [WLC FAQ \(draadloze LAN-controller\)](#)
- [Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point](#)
- [Beveiligingsoplossingen configureren](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)