Leitfaden zur Integration von Wireless LAN-Controllern und IPS

Inhalt

Einführung

Das Cisco Unified Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) ist Teil des Cisco Self-Defending Network und die erste integrierte kabelgebundene und Wireless-Sicherheitslösung der Branche. Cisco Unified IDS/IPS verfolgt einen umfassenden Sicherheitsansatz - am Wireless-Edge, am kabelgebundenen Edge, am WAN-Edge und im Rechenzentrum. Wenn ein verbundener Client schädlichen Datenverkehr über das Cisco Unified Wireless Network sendet, erkennt ein kabelgebundenes Cisco IDS-Gerät den Angriff und sendet keine Anfragen an Cisco Wireless LAN Controller (WLCs), die dann das Client-Gerät trennen.

Das Cisco IPS ist eine netzwerkbasierte Inline-Lösung, die schädlichen Datenverkehr, einschließlich Würmern, Spyware/Adware, Netzwerkviren und Anwendungsmissbrauch, genau

identifizieren, klassifizieren und stoppen kann, bevor sie die Geschäftskontinuität beeinträchtigen.

Mit der Cisco IPS Sensor Software Version 5 kombiniert die Cisco IPS-Lösung Inline-Prevention-Services mit innovativen Technologien, um die Genauigkeit zu erhöhen. Das Ergebnis ist uneingeschränktes Vertrauen in den Schutz Ihrer IPS-Lösung, ohne dass der legitime Datenverkehr verloren geht. Die Cisco IPS-Lösung bietet darüber hinaus einen umfassenden Schutz Ihres Netzwerks durch die einzigartige Möglichkeit, mit anderen Netzwerksicherheitsressourcen zusammenzuarbeiten, und bietet einen proaktiven Ansatz für den Schutz Ihres Netzwerks.

Mit der Cisco IPS-Lösung können Benutzer mehr Bedrohungen mit größerer Sicherheit stoppen, indem sie die folgenden Funktionen nutzen:

- **Präzise Inline-Präventionstechnologien** - Bietet beispielloses Vertrauen, um vorbeugende Maßnahmen gegen eine Vielzahl von Bedrohungen zu ergreifen, ohne dass das Risiko besteht, legitimen Datenverkehr zu verwerfen. Diese einzigartigen Technologien ermöglichen eine intelligente, automatisierte, kontextbezogene Analyse Ihrer Daten und stellen sicher, dass Sie Ihre Intrusion Prevention-Lösung optimal nutzen können.
- **Multi-Vector Threat Identification** - Schützt Ihr Netzwerk durch detaillierte Überprüfung des Datenverkehrs in Layer 2 bis 7 vor Richtlinienverletzungen, Schwachstellen-Exploitationen und ungewöhnlichen Aktivitäten.
- **Einzigartige Zusammenarbeit im Netzwerk**: Verbessert Skalierbarkeit und Ausfallsicherheit durch Netzwerkzusammenarbeit, einschließlich effizienter Techniken zur Erfassung des Datenverkehrs, Funktionen zum Lastenausgleich und Transparenz für verschlüsselten Datenverkehr.
- **Umfassende Bereitstellungslösungen** - Bietet Lösungen für alle Umgebungen, von kleinen und mittleren Unternehmen (KMUs) und Zweigstellen bis hin zu Installationen großer Unternehmen und Service Provider.
- **Leistungsstarke Management-, Ereigniskorrelations- und Support-Services** - Ermöglicht eine Komplettlösung mit Konfigurations-, Management-, Datenkorrelations- und erweiterten Support-Services. Das Cisco Security Monitoring, Analysis, and Response System (MARS) identifiziert, isoliert und empfiehlt die präzise Entfernung von Angriffselementen für eine netzwerkweite Intrusion Prevention-Lösung. Das Cisco Incident Control System verhindert neue Würmer- und Virenangriffe, indem es das Netzwerk in die Lage versetzt, sich schnell anzupassen und eine verteilte Reaktion darauf zu ermöglichen.

In Kombination bieten diese Elemente eine umfassende Inline-Präventionslösung, mit der Sie die größte Bandbreite an schädlichem Datenverkehr erkennen und stoppen können, bevor er die Geschäftskontinuität beeinträchtigt. Die Cisco Self-Defending Network-Initiative erfordert integrierte und integrierte Sicherheitsfunktionen für Netzwerklösungen. Aktuelle LWAPP-basierte WLAN-Systeme (Lightweight Access Point Protocol) unterstützen nur grundlegende IDS-Funktionen, da es sich im Wesentlichen um ein Layer-2-System handelt und die Verarbeitungsleistung für Leitungen begrenzt ist. Cisco veröffentlicht neuen Code zeitnah, um neue erweiterte Funktionen in die neuen Codes aufzunehmen. Version 4.0 bietet die neuesten Funktionen, darunter die Integration eines LWAPP-basierten WLAN-Systems in die Cisco IDS/IPS-Produktlinie. In dieser Version soll das Cisco IDS/IPS-System die WLCs anweisen, den Zugriff auf Wireless-Netzwerke für bestimmte Clients zu sperren, wenn ein Angriff auf Layer 3 bis Layer 7 erkannt wird, an dem der Client beteiligt ist.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Mindestanforderungen erfüllen:

- WLC-Firmware Version 4.x und höher
- Kenntnisse zur Konfiguration von Cisco IPS und Cisco WLC sind wünschenswert.

Verwendete Komponenten

Cisco WLC

Diese Controller sind in der Softwareversion 4.0 für IDS-Änderungen enthalten:

- Cisco WLC der Serie 2000
- Cisco WLC der Serie 2100
- Cisco WLC der Serie 4400
- Cisco Wireless Services Module (WiSM)
- Cisco Catalyst Unified Access Switch der Serie 3750G
- Cisco Wireless LAN Controller-Modul (WLCM)

Access Points

- Cisco Aironet Lightweight Access Points der Serie 1100 AG
- Cisco Aironet Lightweight Access Points der Serie 1200 AG
- Cisco Aironet Lightweight Access Points der Serie 1300
- Cisco Aironet Lightweight Access Points der Serie 1000

Management

- Cisco Wireless Control System (WCS)
- Cisco Sensor der Serie 4200
- Cisco IDS Management - Cisco IDS Device Manager (IDM)

Cisco Unified IDS/IPS-Plattformen

- Cisco IPS Sensoren der Serie 4200 mit Cisco IPS Sensor Software 5.x oder höher
- SSM10 und SSM20 für die Cisco Adaptive Security Appliances der Serie ASA 5500 mit Cisco IPS Sensor Software 5.x
- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Cisco IPS Sensor Software 5.x
- Cisco IDS Network Module (NM-CIDS) mit Cisco IPS Sensor Software 5.x
- Cisco Catalyst Intrusion Detection System Module 2 (IDSM-2) der Serie 6500 mit Cisco IPS Sensor Software 5.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

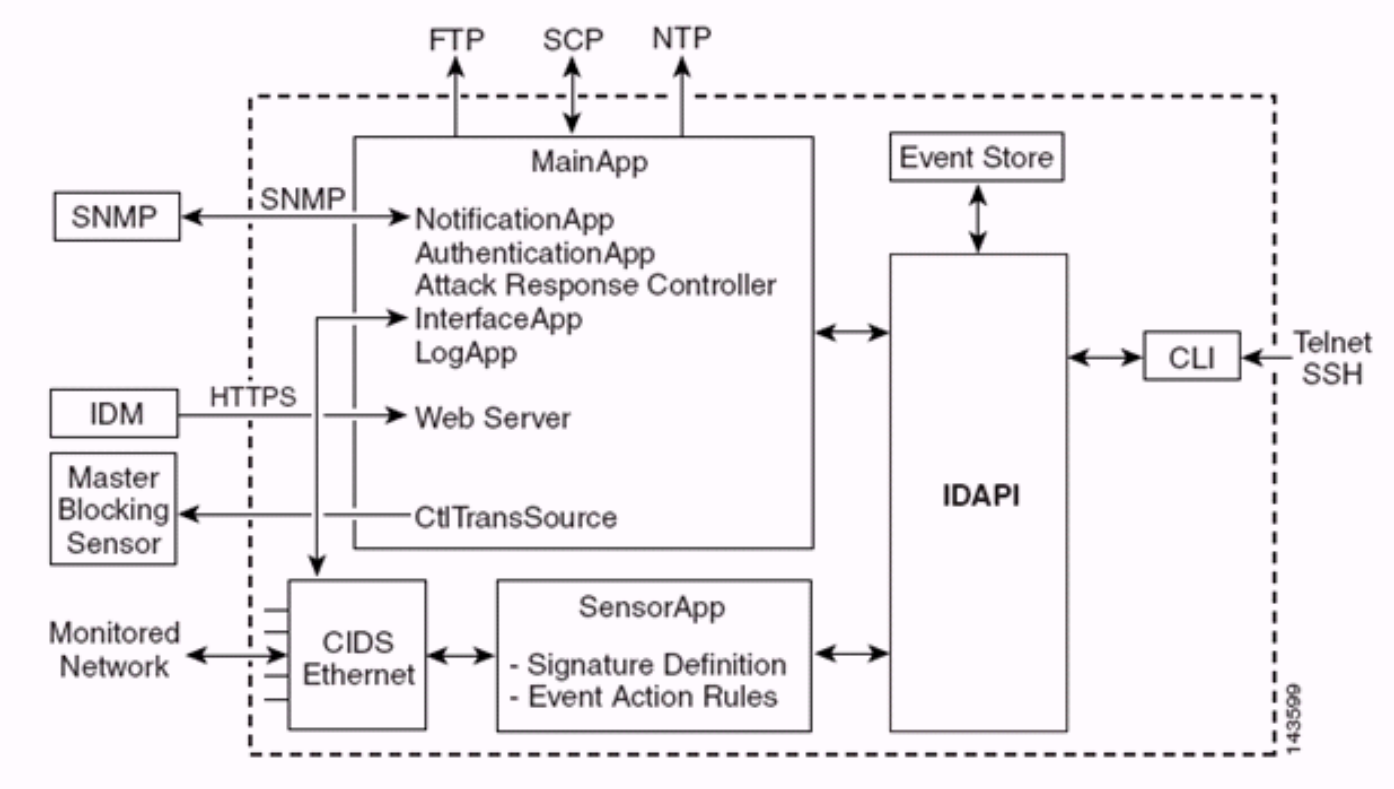
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Cisco IDS im Überblick

Die wichtigsten Komponenten des Cisco IDS (Version 5.0) sind:

- **Sensor-App** - Führt die Paketerfassung und -analyse durch.
- **Event Storage Management and Actions Module** - Ermöglicht das Speichern von Richtlinienverletzungen.
- **Imaging, Install and Startup Module** (**Imaging**, Installation und Startmodul) - Laden, Initialisieren und Starten der gesamten Systemsoftware.
- **Benutzeroberflächen und UI-Support-Modul** - Stellt eine integrierte CLI und das IDM bereit.
- **Sensor OS** - Host-Betriebssystem (basierend auf Linux).



Die Sensor Application (IPS Software) besteht aus:

- **Main App**: Initialisiert das System, startet und stoppt andere Anwendungen, konfiguriert das Betriebssystem und ist für Upgrades verantwortlich. Es enthält folgende Komponenten:**Control Transaction Server** - Ermöglicht es den Sensoren, Steuerungstransaktionen zu senden, die zum Aktivieren der Master-Sperrsensorfunktion des Attack Response Controllers (ehemals Network Access Controller) verwendet werden.**Event Store** - Ein indizierter Speicher zum Speichern von IPS-Ereignissen (Fehler, Status- und Warnsystemmeldungen), auf die über CLI, IDM, Adaptive Security Device Manager (ASDM) oder Remote Data Exchange Protocol (RDEP) zugegriffen werden kann.
- **Interface App**: Behandelt Umgehungs- und physische Einstellungen und definiert paarweise Schnittstellen. Die physischen Einstellungen bestehen aus Geschwindigkeits-, Duplex- und Verwaltungsstatus.
- **Log App** (Protokollanwendung): Schreibt die Protokollmeldungen der Anwendung in die Protokolldatei und die Fehlermeldungen in den Event Store.
- **Attack Response Controller (ARC) (ehemals Network Access Controller)** - Verwaltet Remote-Netzwerkgeräte (Firewalls, Router und Switches), um Blockierungsfunktionen bereitzustellen,

wenn ein Warnereignis aufgetreten ist. ARC erstellt und wendet Zugriffskontrolllisten (ACLs) auf dem kontrollierten Netzwerkgerät an oder verwendet den Befehl **shun** (Firewalls).
- **Notification App**: Sendet SNMP-Traps, wenn sie durch Warn-, Status- und Fehlerereignisse ausgelöst werden. Die Benachrichtigungs-App verwendet dazu einen SNMP-Agent für eine öffentliche Domäne. Die SNMP GETs liefern Informationen zum Zustand eines Sensors.**Webserver (HTTP RDEP2-Server)** - Stellt eine Webbenutzeroberfläche bereit. Es bietet auch die Möglichkeit, über RDEP2 mit anderen IPS-Geräten zu kommunizieren, indem mehrere Servlets verwendet werden, um IPS-Dienste bereitzustellen.**Authentifizierungsanwendung**: Überprüft, ob Benutzer zur Ausführung von CLI-, IDM-, ASDM- oder RDEP-Aktionen autorisiert sind.
- **Sensor App (Analysis Engine)** - Führt die Paketerfassung und Analyse durch.
- **CLI** - Die Schnittstelle, die ausgeführt wird, wenn sich Benutzer über Telnet oder SSH erfolgreich beim Sensor anmelden. Alle über die CLI erstellten Konten verwenden die CLI als Shell (mit Ausnahme des Dienstkontos - nur ein Dienstkonto ist zulässig). Zulässige CLI-Befehle hängen von der Berechtigung des Benutzers ab.

Alle IPS-Anwendungen kommunizieren miteinander über eine gemeinsame API (Application Program Interface), die IDAPI genannt wird. Remote-Anwendungen (andere Sensoren, Verwaltungsanwendungen und Software von Drittanbietern) kommunizieren über RDEP2- und SDEE-Protokolle (Security Device Event Exchange) mit Sensoren.

Beachten Sie, dass der Sensor über folgende Datenträgerpartitionen verfügt:

- **Anwendungspartition**: Enthält das vollständige IPS-Systemabbild.
- **Maintenance Partition** (Wartungspartition) - Ein spezielles IPS-Image, das verwendet wird, um die Anwendungspartition von IDSM-2 neu zu formatieren. Ein Re-Image der Wartungspartition führt zu Verlust der Konfigurationseinstellungen.
- **Wiederherstellungspartition** - Ein spezielles Abbild, das zur Wiederherstellung des Sensors verwendet wird. Durch das Starten in die Wiederherstellungspartition können Benutzer die Anwendungspartition vollständig neu abbilden. Die Netzwerkeinstellungen bleiben erhalten, aber alle anderen Konfigurationen gehen verloren.

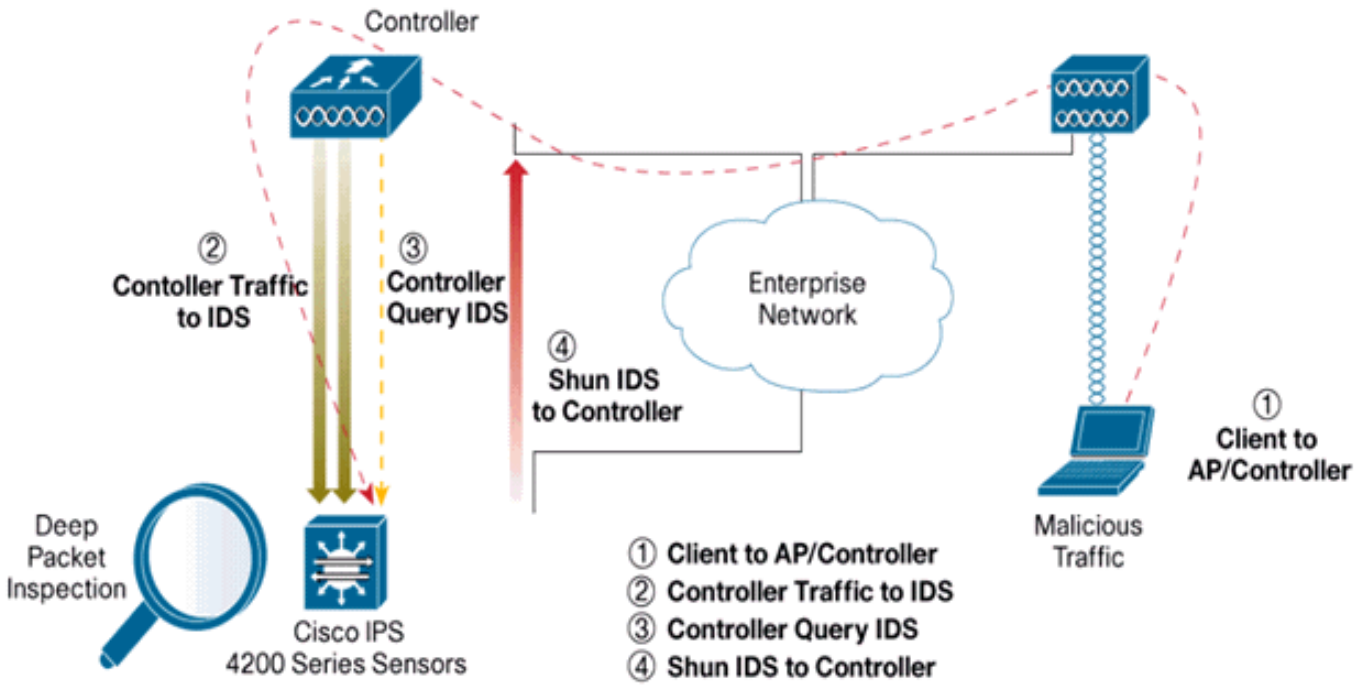
Cisco IDS und WLC - Integrationsübersicht

Version 5.0 des Cisco IDS ermöglicht die Konfiguration von Ablehnungsaktionen, wenn Richtlinienverletzungen (Signaturen) erkannt werden. Je nach Benutzerkonfiguration im IDS/IPS-System kann eine Shun-Anfrage an eine Firewall, einen Router oder einen WLC gesendet werden, um die Pakete von einer bestimmten IP-Adresse zu blockieren.

Mit der Cisco Unified Wireless Network Software Version 4.0 für Cisco Wireless Controller muss eine Shun-Anfrage an einen WLC gesendet werden, um das auf einem Controller verfügbare Blacklisting oder Ausschlussverhalten der Clients auszulösen. Die Schnittstelle, die der Controller zum Abrufen der Shun-Anforderung verwendet, ist die Command-and-Control-Schnittstelle des Cisco IDS.

- Der Controller ermöglicht die Konfiguration von bis zu fünf IDS-Sensoren auf einem bestimmten Controller.
- Jeder konfigurierte IDS-Sensor wird durch seine IP-Adresse oder einen qualifizierten Netzwerknamen und Autorisierungsanmeldeinformationen identifiziert.
- Jeder IDS-Sensor kann auf einem Controller mit einer eindeutigen Abfragerate in Sekunden

konfiguriert werden.



IDS-Shunding

Der Controller fragt den Sensor mit der konfigurierten Abfragerate ab, um alle Shun-Ereignisse abzurufen. Eine gegebene Shun-Anforderung wird über die gesamte Mobilitätsgruppe des Controllers verteilt, der die Anfrage vom IDS-Sensor abruft. Jede Shun-Anforderung für eine Client-IP-Adresse gilt für den angegebenen Wert für die Timeout-Sekunden. Wenn der Timeout-Wert eine unbegrenzte Zeit anzeigt, endet das Shun-Ereignis nur, wenn der Shun-Eintrag auf dem IDS entfernt wird. Der gemiedete Client-Status wird auf jedem Controller in der Mobilitätsgruppe auch dann beibehalten, wenn einer oder alle Controller zurückgesetzt werden.

Hinweis: Die Entscheidung, einen Client zu sperren, wird immer vom IDS-Sensor getroffen. Der Controller erkennt keine Layer-3-Angriffe. Es ist weitaus komplizierter festzustellen, ob der Client einen bösartigen Angriff auf Layer 3 auslöst. Der Client wird auf Layer 2 authentifiziert, sodass der Controller den Layer-2-Zugriff gewähren kann.

Hinweis: Wenn einem Client z. B. eine IP-Adresse zugewiesen wird, die bereits einen Angriff auslöst (gelöscht), ist es an der Sensor-Zeitüberschreitung, den Layer-2-Zugriff für diesen neuen Client zu deaktivieren. Selbst wenn der Controller den Zugriff auf Layer 2 gewährt, kann der Client-Datenverkehr ohnehin an Routern in Layer 3 blockiert werden, da der Sensor auch Router über das Shun-Ereignis informiert.

Angenommen, ein Client hat die IP-Adresse A. Wenn der Controller das IDS auf Shun-Ereignisse abfragt, sendet das IDS jetzt die Shun-Anforderung an den Controller, wobei die IP-Adresse A die Ziel-IP-Adresse ist. Der Controller schwarz listet diesen Client A auf. Auf dem Controller werden Clients basierend auf einer MAC-Adresse deaktiviert.

Nehmen Sie nun an, dass der Client seine IP-Adresse von A in B ändert. Bei der nächsten Abfrage erhält der Controller eine Liste mit Clients, die auf der IP-Adresse basieren. Auch dieses Mal befindet sich die IP-Adresse A noch immer in der Liste "Shunned" (Shunned). Da der Client jedoch seine IP-Adresse von A nach B geändert hat (die nicht in der gefälschten Liste der IP-Adressen enthalten ist), wird dieser Client mit einer neuen IP-Adresse von B freigegeben, sobald

die Zeitüberschreitung der in Blacklists aufgeführten Clients auf dem Controller erreicht ist. Der Controller lässt diesem Client nun die neue IP-Adresse von B zu (die MAC-Adresse des Clients bleibt jedoch gleich).

Obwohl ein Client während der Ausschlusszeit des Controllers deaktiviert bleibt und beim erneuten Abruf seiner vorherigen DHCP-Adresse wieder ausgeschlossen wird, wird dieser Client nicht mehr deaktiviert, wenn sich die IP-Adresse des Clients ändert, der nicht aufgerufen wird. Wenn der Client beispielsweise eine Verbindung mit demselben Netzwerk herstellt und das DHCP-Lease-Timeout nicht abgelaufen ist.

Controller unterstützen nur die Verbindung mit dem IDS für Client-Shunning-Anfragen, die den Management-Port des Controllers verwenden. Der Controller stellt über die entsprechenden VLAN-Schnittstellen, die Wireless-Client-Datenverkehr übertragen, eine Verbindung zum IDS für die Paketprüfung her.

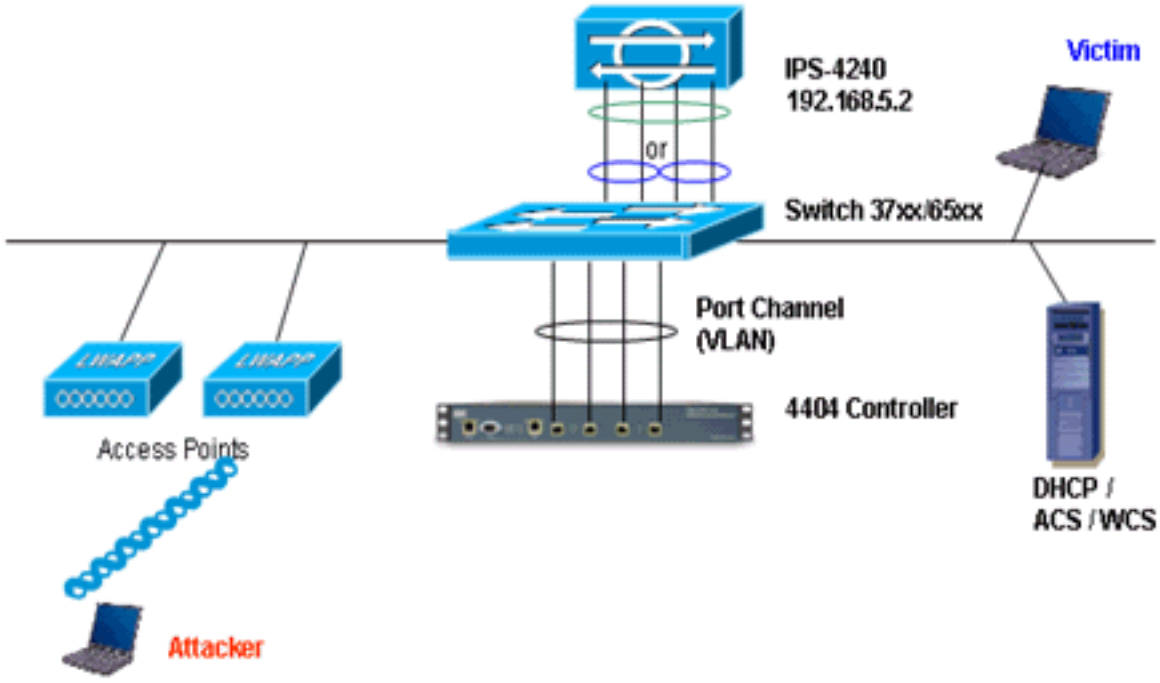
Auf der Seite "Disable Clients" (Clients deaktivieren) wird auf dem Controller jeder Client angezeigt, der über eine IDS-Sensor-Anfrage deaktiviert wurde. Der Befehl CLI **show** zeigt auch eine Liste von Clients an, die auf Blacklists gesetzt sind.

Im WCS werden die ausgeschlossenen Clients unter der Unterregisterkarte "Sicherheit" angezeigt.

Im Folgenden finden Sie die erforderlichen Schritte, um die Integration von Cisco IPS-Sensoren und Cisco WLCs abzuschließen.

1. Installieren Sie die IDS-Appliance auf demselben Switch, auf dem sich der Wireless Controller befindet, und schließen Sie sie an.
2. Spiegelung (SPAN) der WLC-Ports, die den Wireless-Client-Datenverkehr zur IDS-Appliance übertragen.
3. Die IDS-Appliance empfängt eine Kopie aller Pakete und prüft den Datenverkehr auf Layer 3 bis 7.
4. Die IDS-Appliance bietet eine herunterladbare Signaturdatei, die auch angepasst werden kann.
5. Die IDS-Appliance generiert den Alarm mit einer Ereignisaktion "Shun", wenn eine Signatur eines Angriffs erkannt wird.
6. Der WLC fragt das IDS nach Alarmen ab.
7. Wenn ein Alarm mit der IP-Adresse eines Wireless-Clients, der dem WLC zugeordnet ist, erkannt wird, wird der Client in die Ausschlussliste aufgenommen.
8. Ein Trap wird vom WLC generiert, und WCS wird benachrichtigt.
9. Der Benutzer wird nach dem angegebenen Zeitraum aus der Ausschlussliste entfernt.

Netzwerkarchitekturdesign



Der Cisco WLC ist mit den Gigabit-Schnittstellen des Catalyst 6500 verbunden. Erstellen Sie einen Port-Channel für die Gigabit-Schnittstellen, und aktivieren Sie Link Aggregation (LAG) auf dem WLC.

```
(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
```

Der Controller ist an die Schnittstelle Gigabit 5/1 und Gigabit 5/2 auf dem Catalyst 6500 angeschlossen.

```
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
```

Die Sensorschnittstellen des IPS-Sensors können einzeln im **Promiscuous-Modus** betrieben werden oder Sie können sie zu Inline-Schnittstellen für den **Inline-Sensing-Modus** kombinieren.

Im Promiscuous-Modus fließen Pakete nicht durch den Sensor. Der Sensor analysiert eine Kopie des überwachten Datenverkehrs und nicht das tatsächlich weitergeleitete Paket. Der Vorteil des Promiscuous-Modus besteht darin, dass der Sensor den Paketfluss mit dem weitergeleiteten Datenverkehr nicht beeinträchtigt.

Hinweis: Das Architekturdiagramm ist nur eine Beispieleinrichtung der integrierten WLC- und IPS-Architektur. Die hier gezeigte Beispielkonfiguration erklärt die IDS-Sensorschnittstelle, die im Promiscuous-Modus arbeitet. Das Architekturdiagramm zeigt die Sensorschnittstellen, die zusammengefasst werden, um im Inline-Paarmodus zu agieren. Weitere Informationen zum Inline-Schnittstellenmodus finden Sie unter Inline-Modus.

Bei dieser Konfiguration wird davon ausgegangen, dass die Sensorschnittstelle im Promiscuous-Modus arbeitet. Die Überwachungsschnittstelle des Cisco IDS-Sensors ist an die Gigabit-Schnittstelle 5/3 des Catalyst 6500 angeschlossen. Erstellen Sie eine Überwachungssitzung auf dem Catalyst 6500, wobei die Port-Channel-Schnittstelle die Quelle der Pakete ist und das Ziel die Gigabit-Schnittstelle ist, an die die Überwachungsschnittstelle des Cisco IPS-Sensors angeschlossen ist. Dadurch wird der gesamte ein- und ausgehende Datenverkehr von den kabelgebundenen Schnittstellen des Controllers zum IDS für die Layer-3- bis Layer-7-Überprüfung repliziert.

```
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#
```

Konfigurieren des Cisco IDS-Sensors

Die Erstkonfiguration des Cisco IDS-Sensors erfolgt über den Konsolenport oder durch den Anschluss eines Monitors und einer Tastatur an den Sensor.

1. Melden Sie sich bei der Appliance an:Verbinden Sie einen Konsolenport mit dem Sensor.Schließen Sie einen Monitor und eine Tastatur an den Sensor an.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort an der Eingabeaufforderung ein.**Hinweis:** Der Standardbenutzername und das Standardkennwort sind beide Cisco. Bei der ersten Anmeldung bei der Appliance werden Sie aufgefordert, diese zu ändern. Sie müssen zuerst das UNIX-Kennwort (cisco) eingeben. Dann müssen Sie das neue Passwort zweimal eingeben.

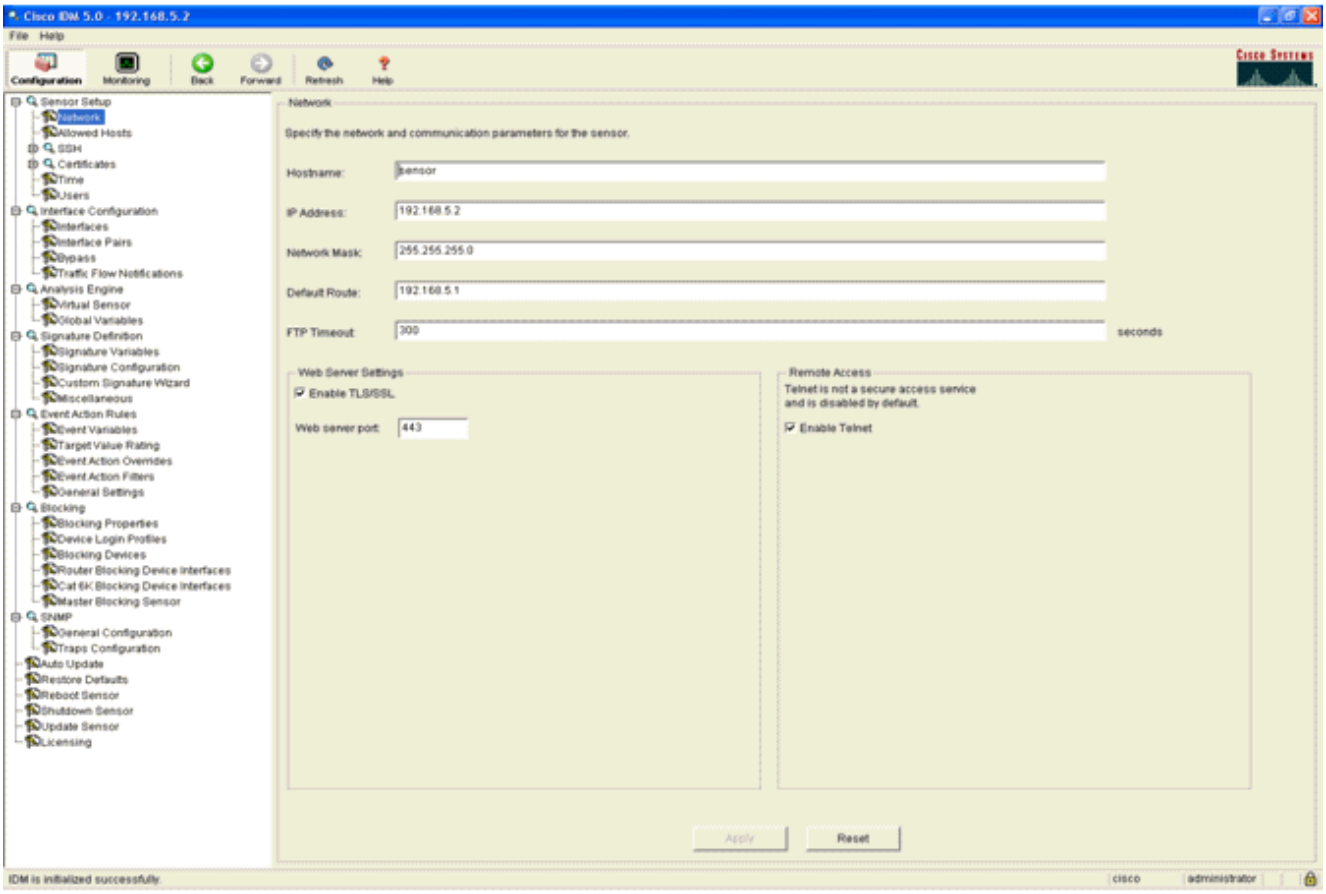
```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. 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. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und die Zugriffsliste auf dem Sensor.**Hinweis:** Dies ist die Command-and-Control-Schnittstelle auf dem IDS, die für die Kommunikation mit dem Controller verwendet wird. Diese Adresse sollte an die Controller-Verwaltungsschnittstelle weitergeleitet werden können. Die Sensorschnittstellen erfordern keine Adressierung. Die Zugriffsliste sollte die Management-Schnittstellenadresse des/der Controller sowie zulässige Adressen für die Verwaltung des IDS enthalten.

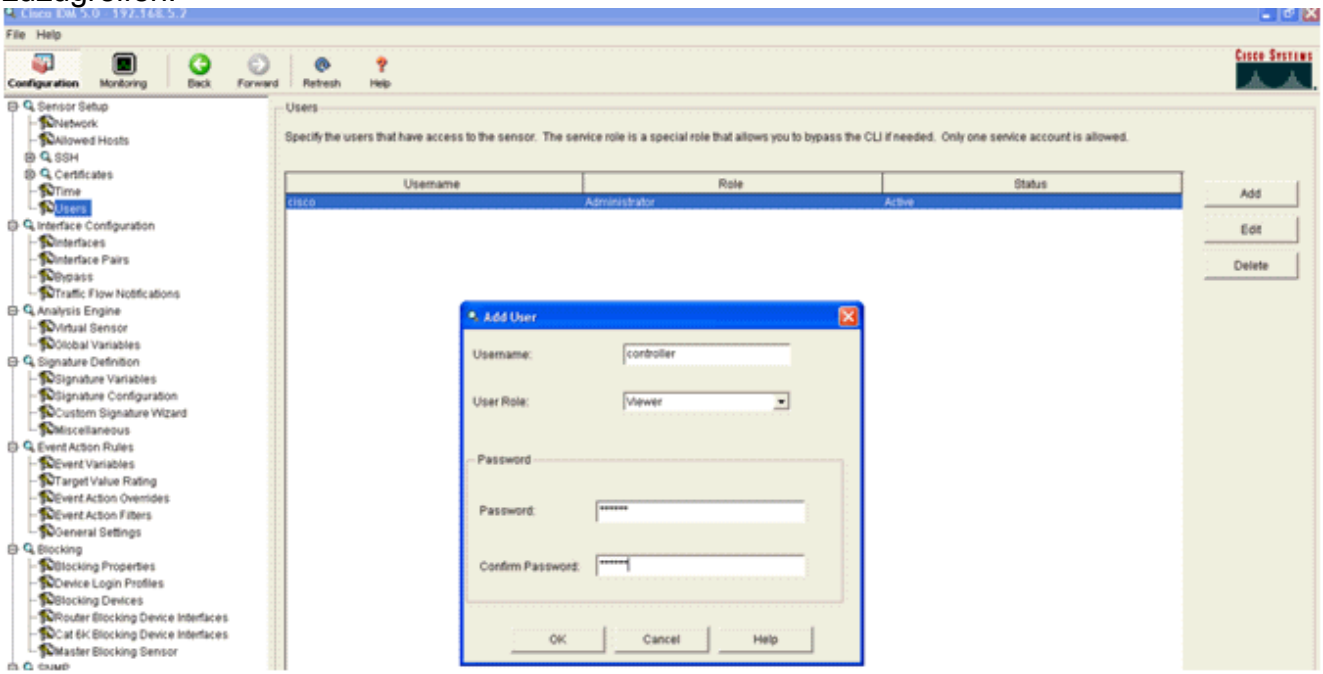
```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
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#
```

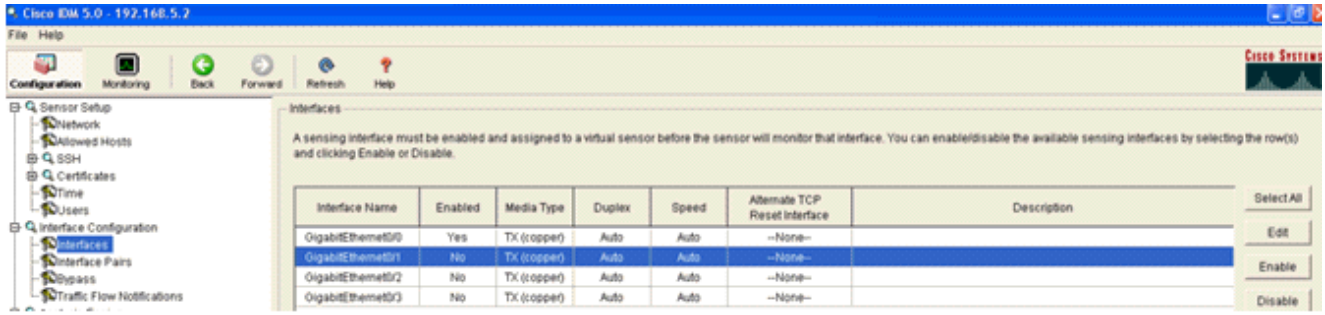
4. Sie können den IPS-Sensor jetzt über die Benutzeroberfläche konfigurieren. Zeigen Sie den Browser auf die Management-IP-Adresse des Sensors. Dieses Bild zeigt ein Beispiel, in dem der Sensor mit 192.168.5.2 konfiguriert ist.



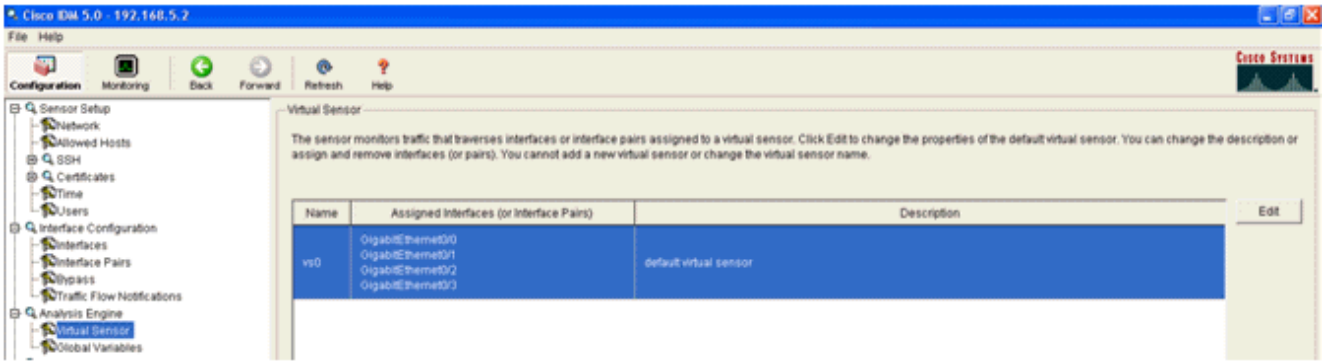
5. Fügen Sie einen Benutzer hinzu, den der WLC verwendet, um auf die IPS-Sensorereignisse zuzugreifen.



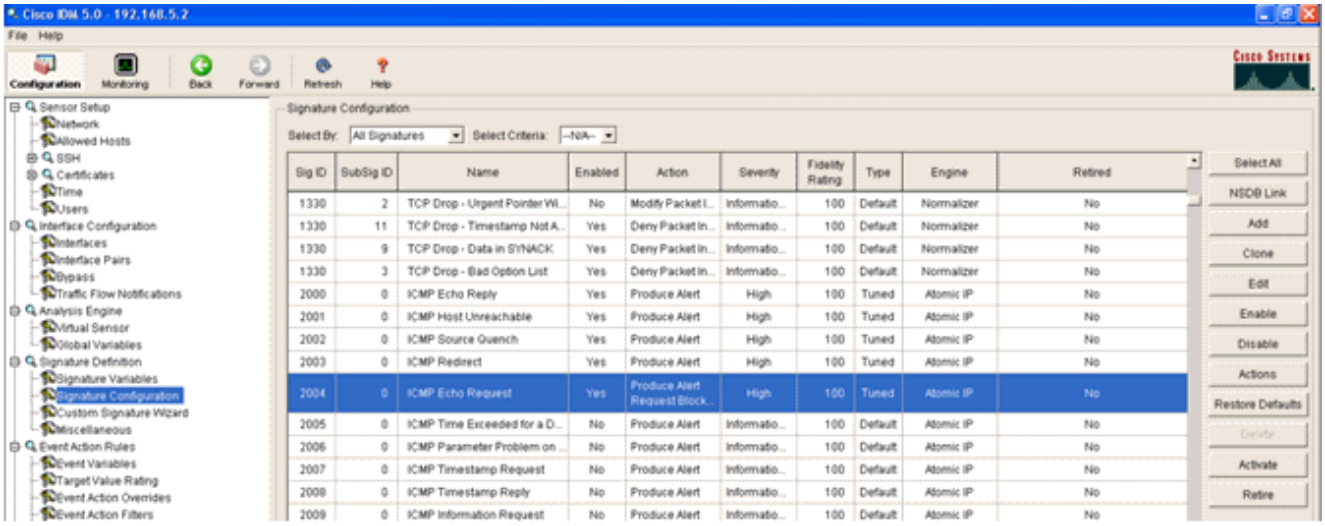
6. Aktivieren Sie die Überwachungsschnittstellen.



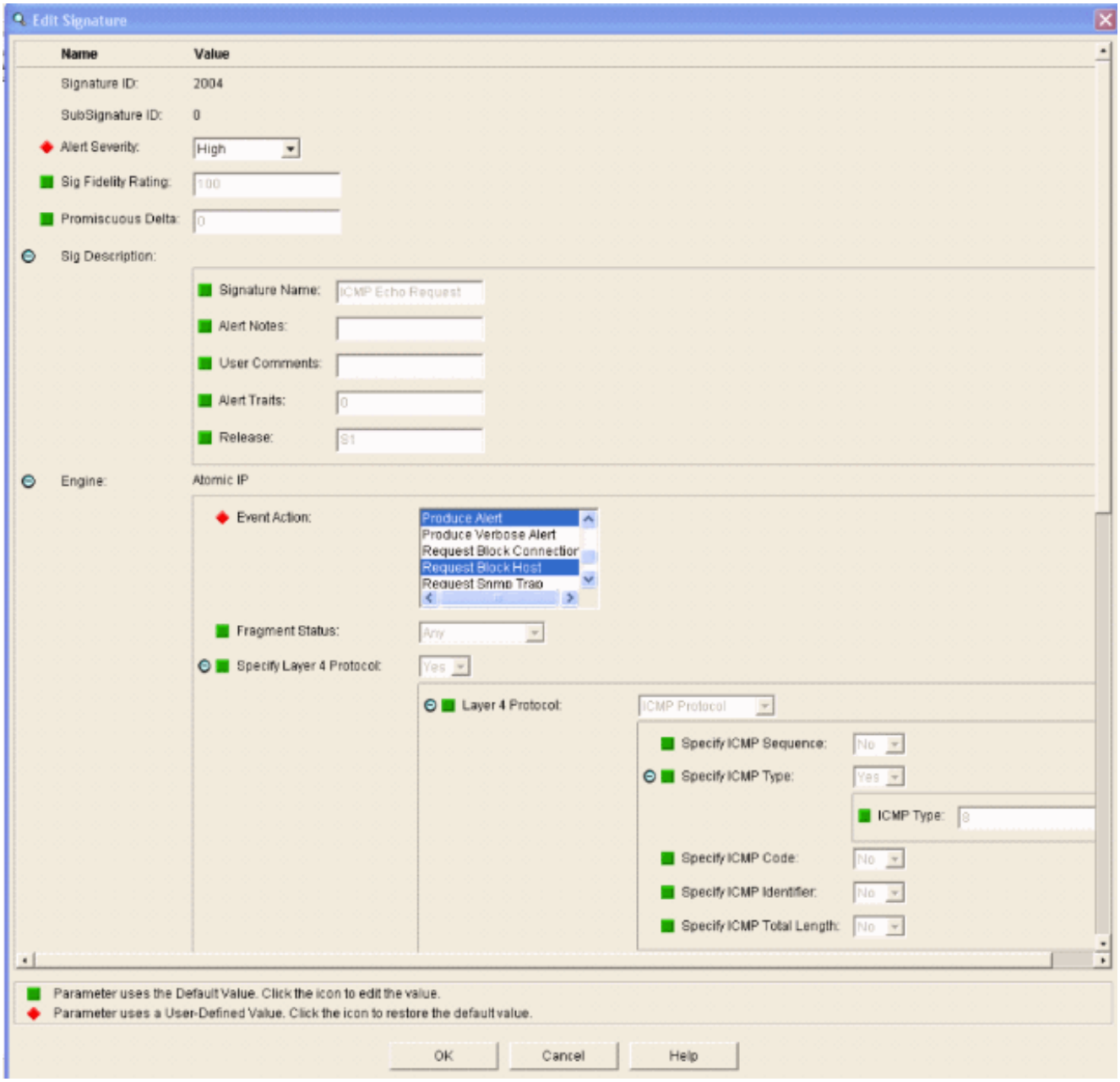
Die Überwachungsschnittstellen müssen der Analysis Engine hinzugefügt werden, wie in diesem Fenster Folgendes angezeigt
wird:



7. Wählen Sie die 2004-Signatur (ICMP Echo Request) aus, um eine schnelle Einrichtungsüberprüfung
durchzuführen.



Die Signatur sollte aktiviert sein, der Alert-Schweregrad auf **Hoch** und die Event Action (Ereignisaktion) auf **Produce Alert** and **Request Block Host** gesetzt sein, damit dieser Verifizierungsschritt abgeschlossen werden
kann.

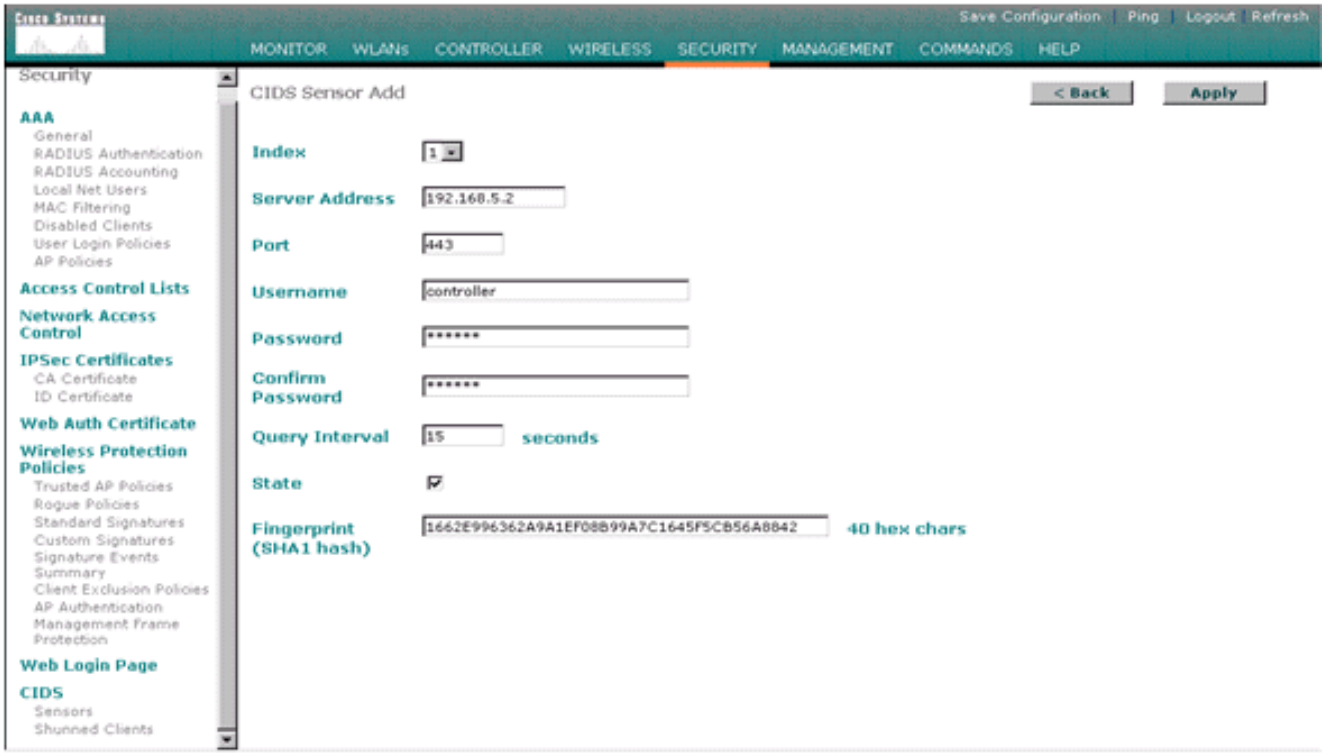


Konfigurieren des WLC

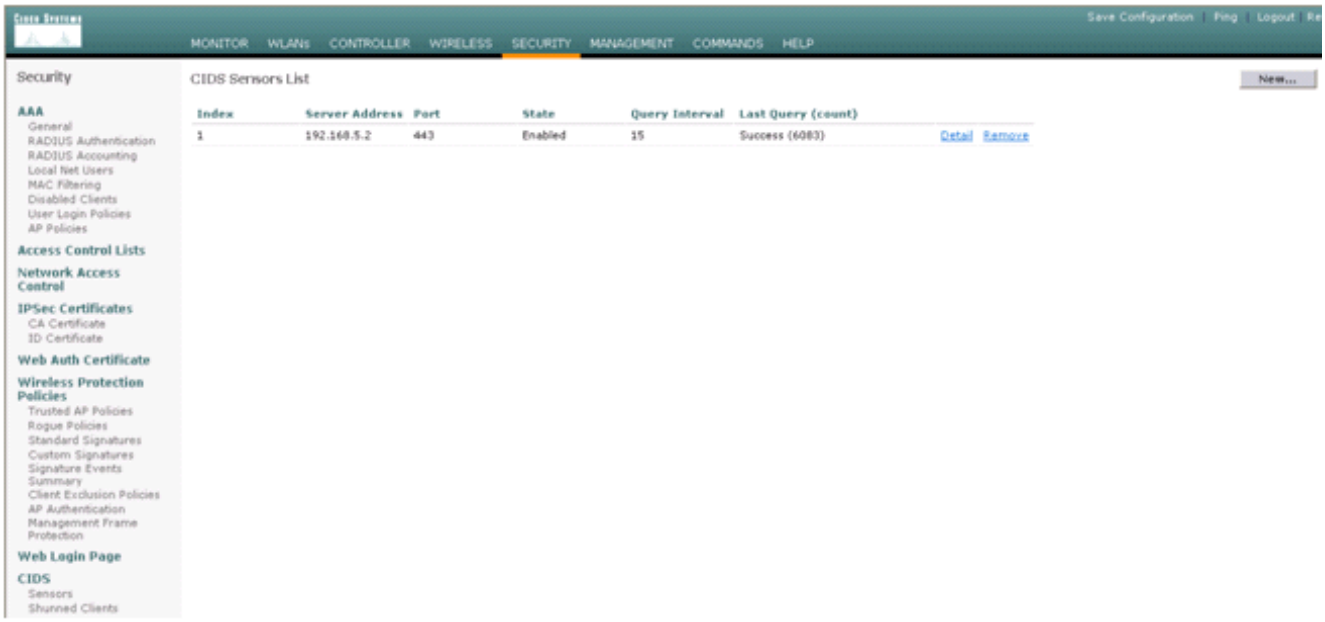
Gehen Sie wie folgt vor, um den WLC zu konfigurieren:

1. Wenn die IPS-Appliance konfiguriert ist und im Controller hinzugefügt werden kann, wählen Sie **Security > CIDS > Sensors > New aus**.
2. Fügen Sie die IP-Adresse, die TCP-Portnummer, den Benutzernamen und das Kennwort hinzu, die Sie zuvor erstellt haben.Um den Fingerabdruck vom IPS-Sensor abzurufen, führen Sie diesen Befehl im IPS-Sensor aus, und fügen Sie den SHA1-Fingerabdruck auf dem WLC hinzu (ohne Doppelpunkt). Diese Funktion dient zum Sichern der Abfragekommunikation zwischen Controller und IDS.

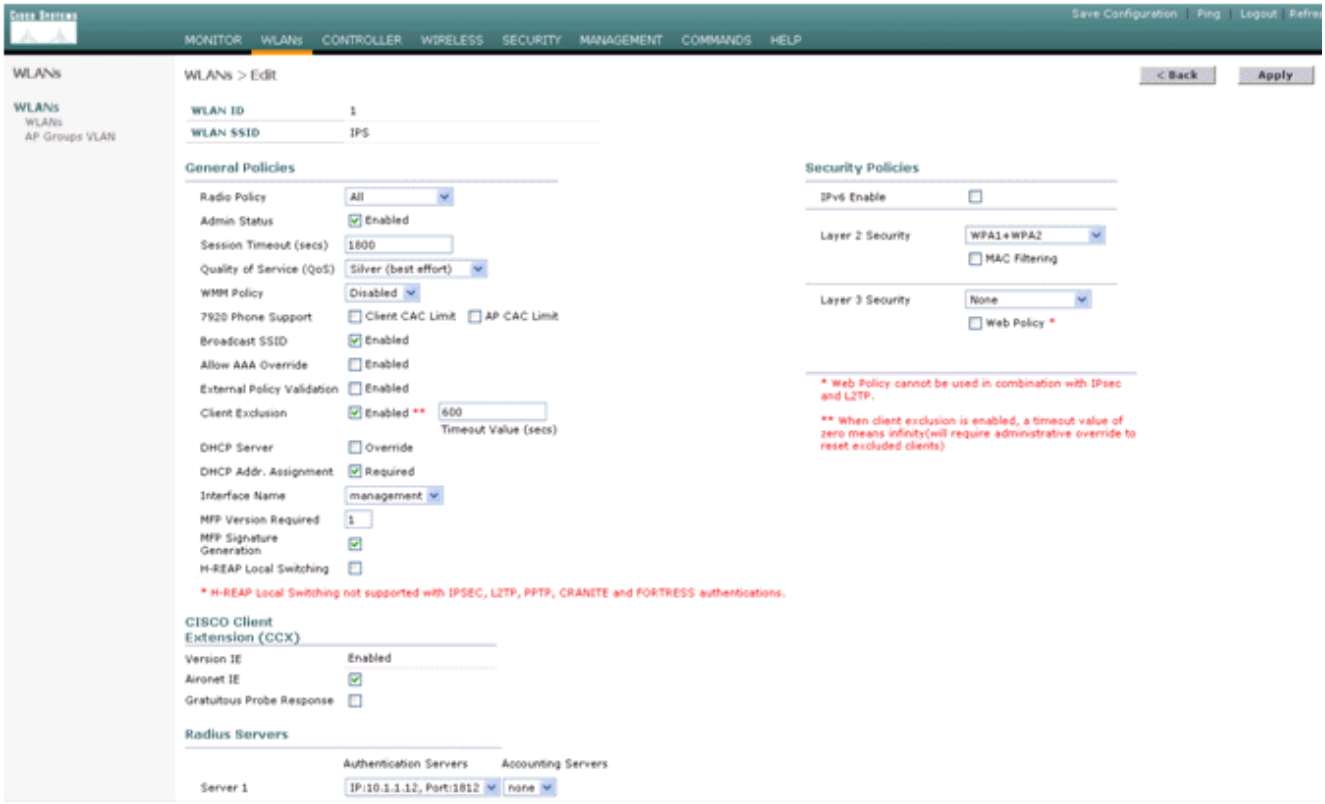
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



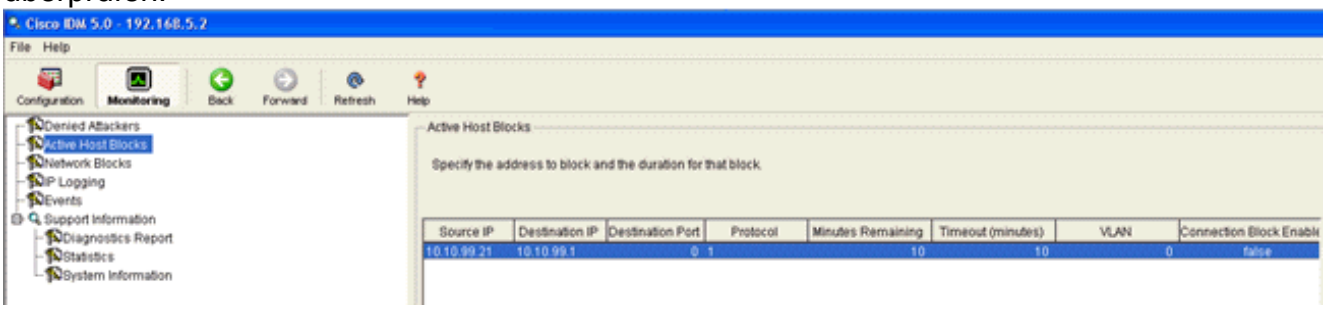
3. Überprüfen Sie den Status der Verbindung zwischen dem IPS-Sensor und dem WLC.



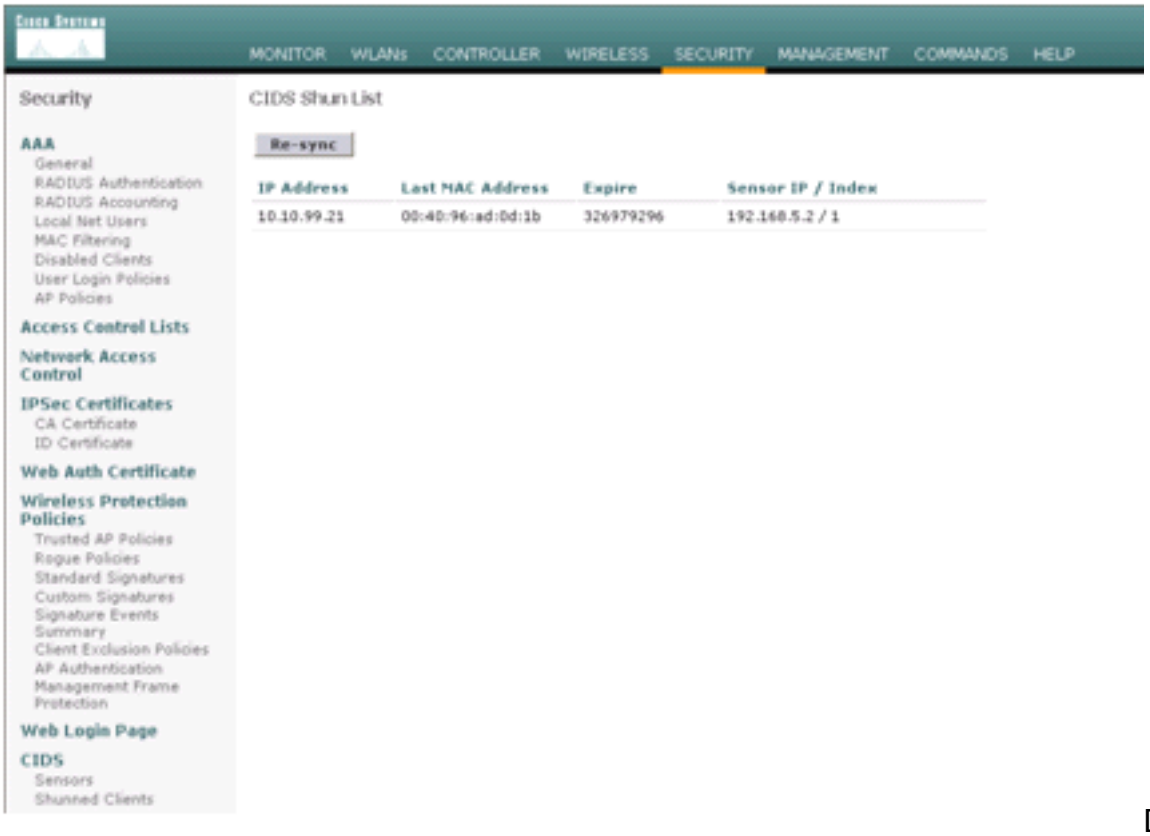
4. Wenn Sie die Verbindung mit dem Cisco IPS-Sensor hergestellt haben, stellen Sie sicher, dass die WLAN-Konfiguration korrekt ist und dass Sie die **Client-Ausschluss** aktivieren.Der Timeout-Standardwert für Clientausschlüsse ist 60 Sekunden. Beachten Sie außerdem, dass der Client-Ausschluss unabhängig vom Client-Ausschlusszeitgeber so lange andauert, wie der vom IDS aufgerufene Clientblock aktiv bleibt. Die standardmäßige Blockierungszeit im IDS beträgt 30
Minuten.



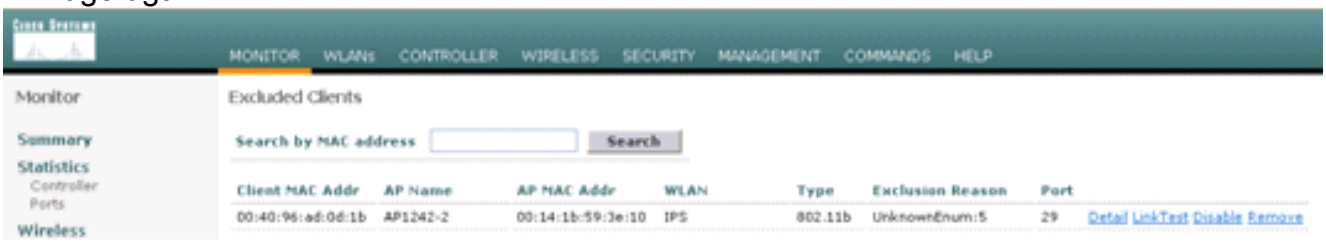
5. Sie können ein Ereignis im Cisco IPS-System auslösen, wenn Sie eine NMAP-Prüfung auf bestimmte Geräte im Netzwerk durchführen oder wenn Sie einen Ping an einige Hosts senden, die vom Cisco IPS-Sensor überwacht werden. Sobald ein Alarm im Cisco IPS ausgelöst wird, gehen Sie zu **Monitoring und Active Host Blocks**, um die Details zum Host zu überprüfen.



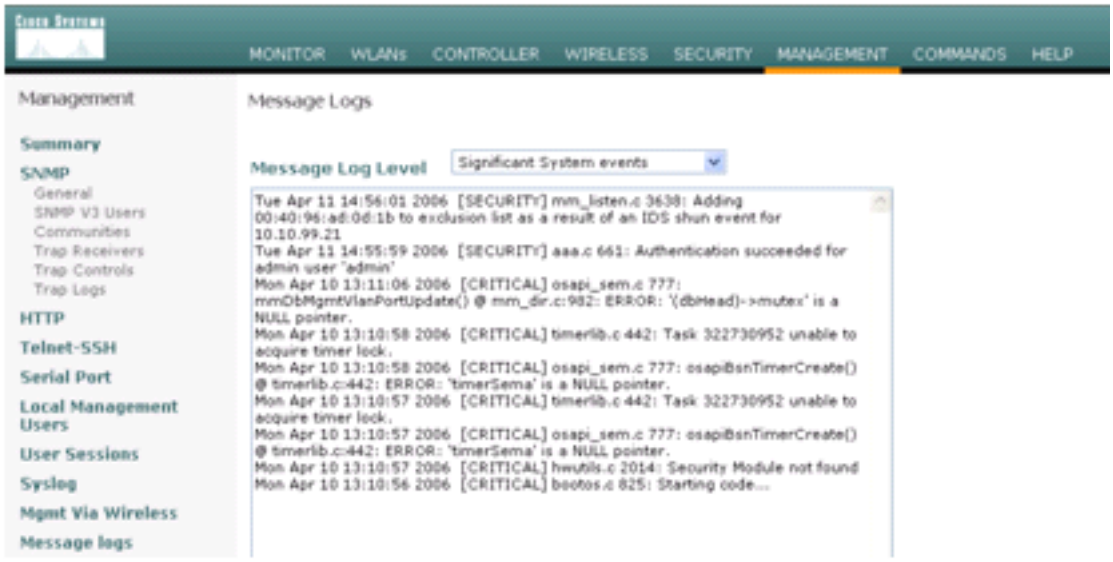
Die Liste "Shunned Clients" im Controller ist jetzt mit der IP- und MAC-Adresse des Hosts



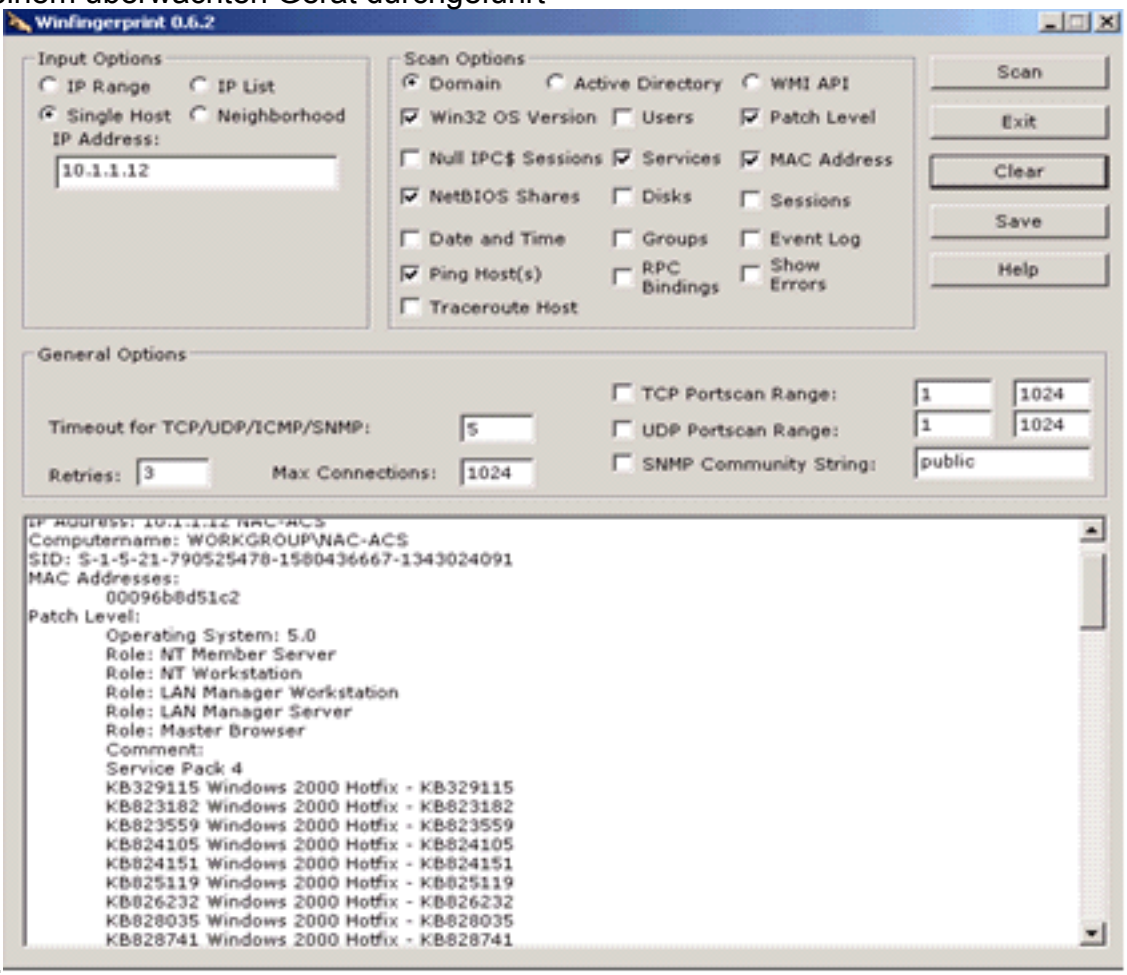
gefüllt. Der Benutzer wird der Clientausschlussliste hinzugefügt.



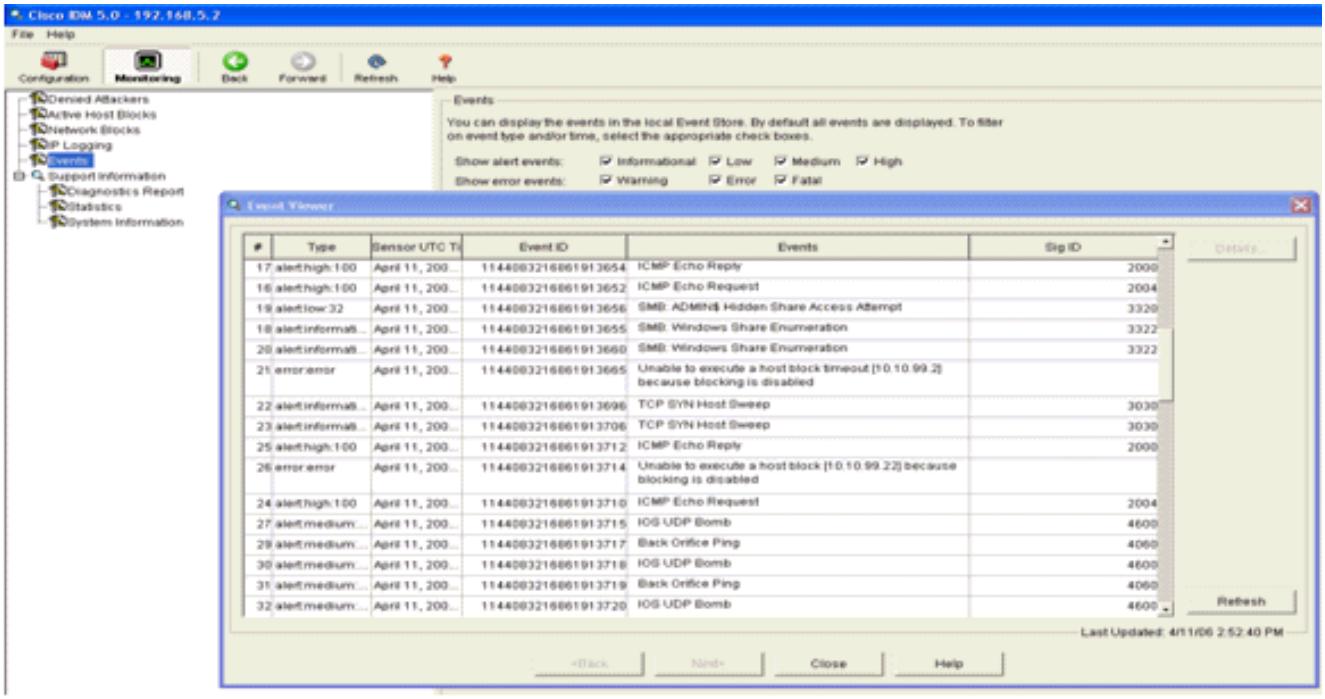
Ein Trap-Protokoll wird generiert, während ein Client der Shun-Liste hinzugefügt wird. Für das Ereignis wird auch ein Meldungsprotokoll



generiert. Im Cisco IPS-Sensor werden einige zusätzliche Ereignisse generiert, wenn eine NMAP-Prüfung auf einem überwachten Gerät durchgeführt



wird. In diesem Fenster werden die im Cisco IPS-Sensor generierten Ereignisse angezeigt.



Beispielkonfiguration für Cisco IDS-Sensoren

Dies ist die Ausgabe des Setup-Skripts für die Installation:

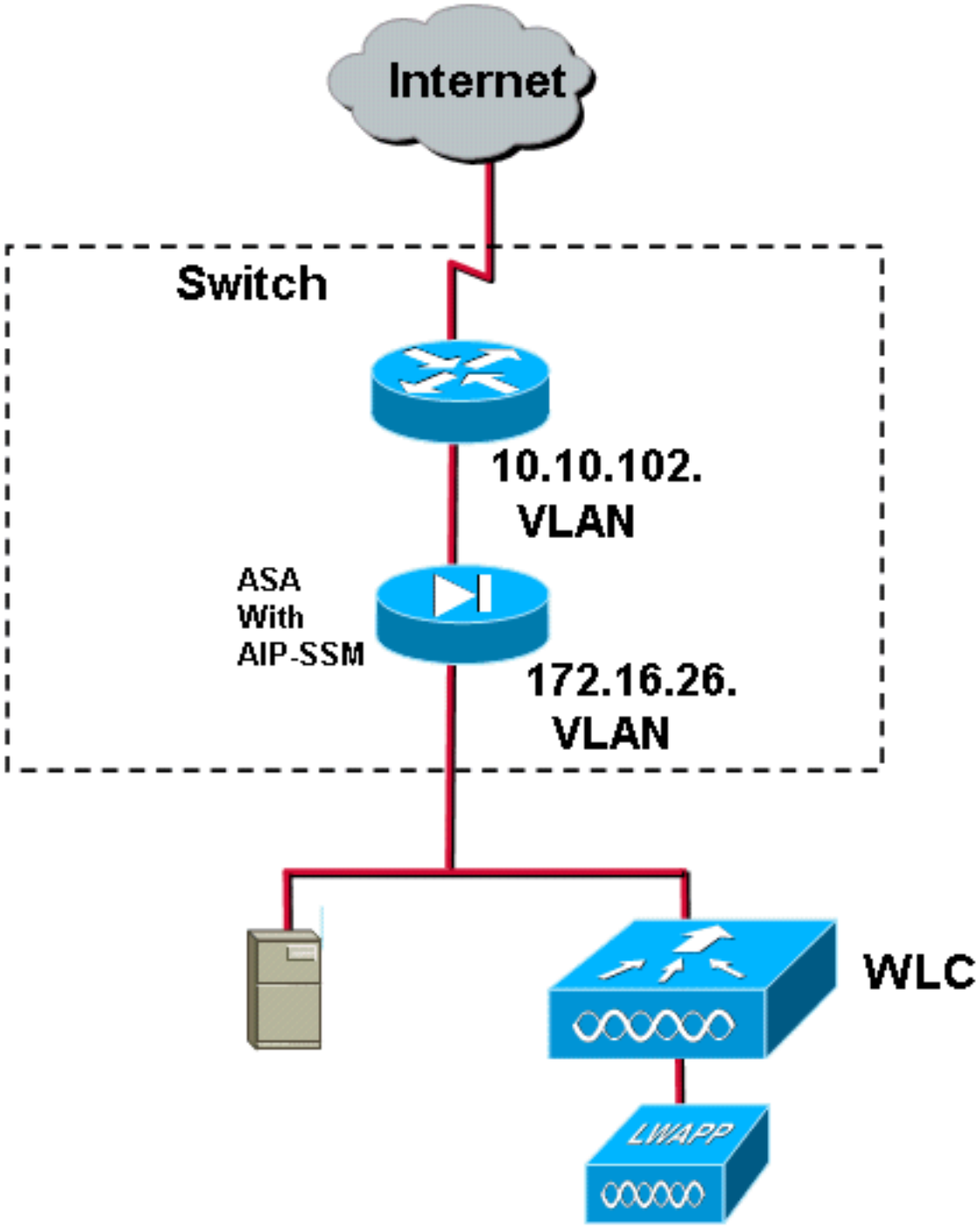
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 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#
```

Konfigurieren einer ASA für IDS

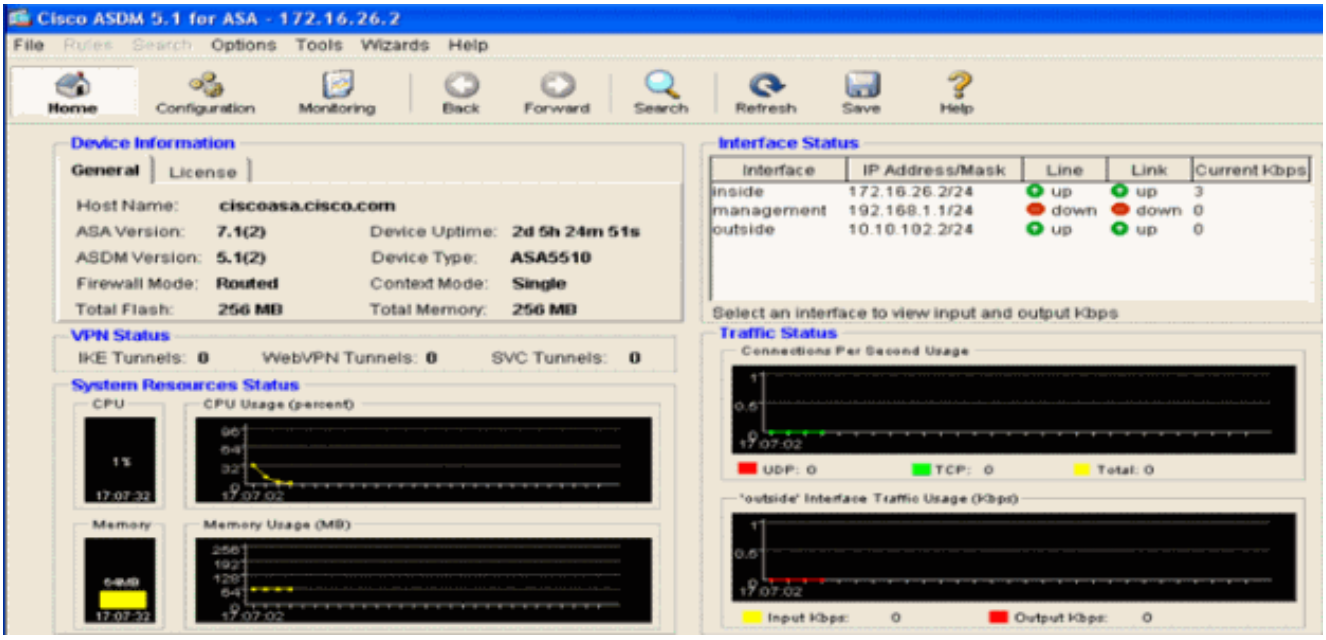
Anders als bei einem herkömmlichen Angriffserkennungssensor muss sich eine ASA immer im Datenpfad befinden. Anders ausgedrückt: Anstatt den Datenverkehr von einem Switch-Port über

einen passiven Sniffing-Port am Sensor zu verteilen, muss die ASA Daten über eine Schnittstelle empfangen, intern verarbeiten und dann an einen anderen Port weiterleiten. Für IDS verwenden Sie das Modular Policy Framework (MPF), um Datenverkehr, den die ASA empfängt, zur Überprüfung an das interne Advanced Inspection and Prevention Security Services Module (AIP-SSM) zu kopieren.

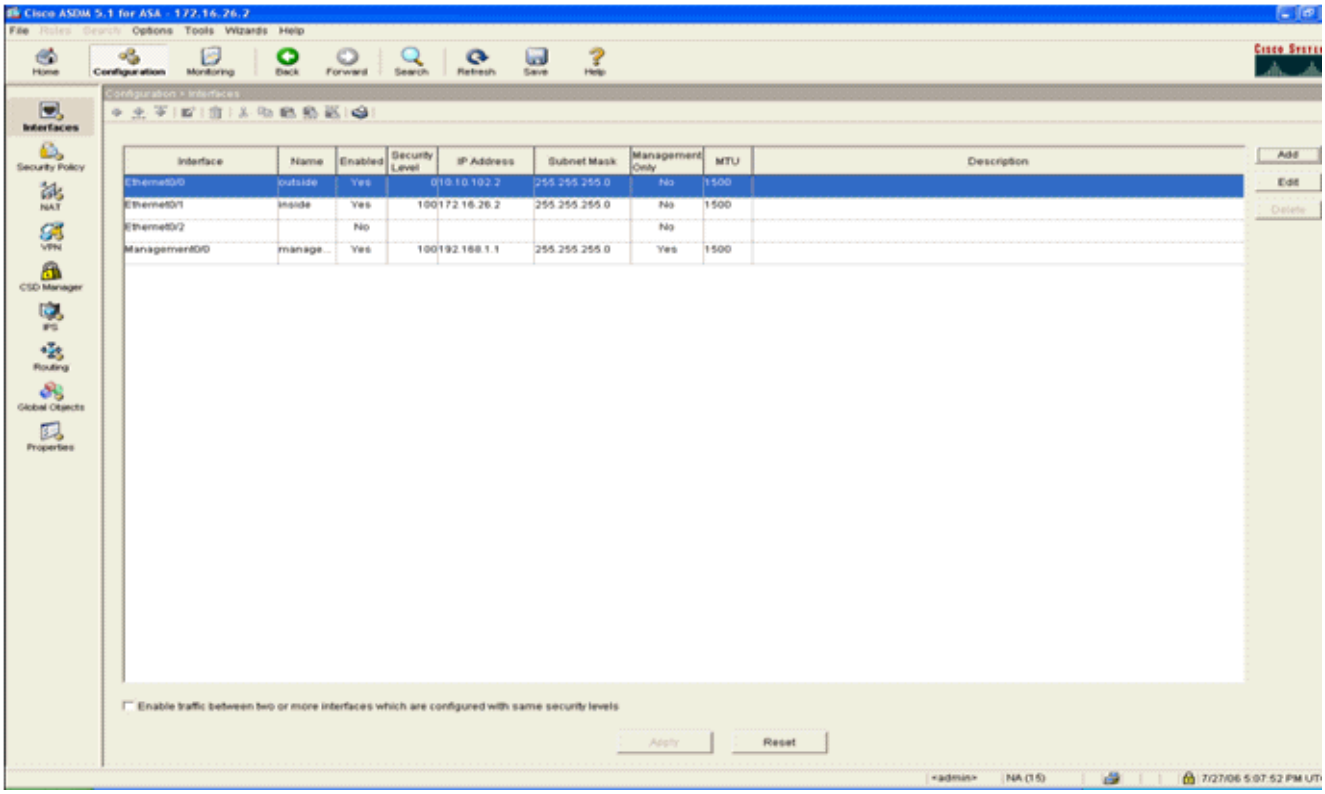


In diesem Beispiel ist die verwendete ASA bereits eingerichtet und leitet den Datenverkehr weiter. Diese Schritte veranschaulichen die Erstellung einer Richtlinie, die Daten an das AIP-SSM sendet.

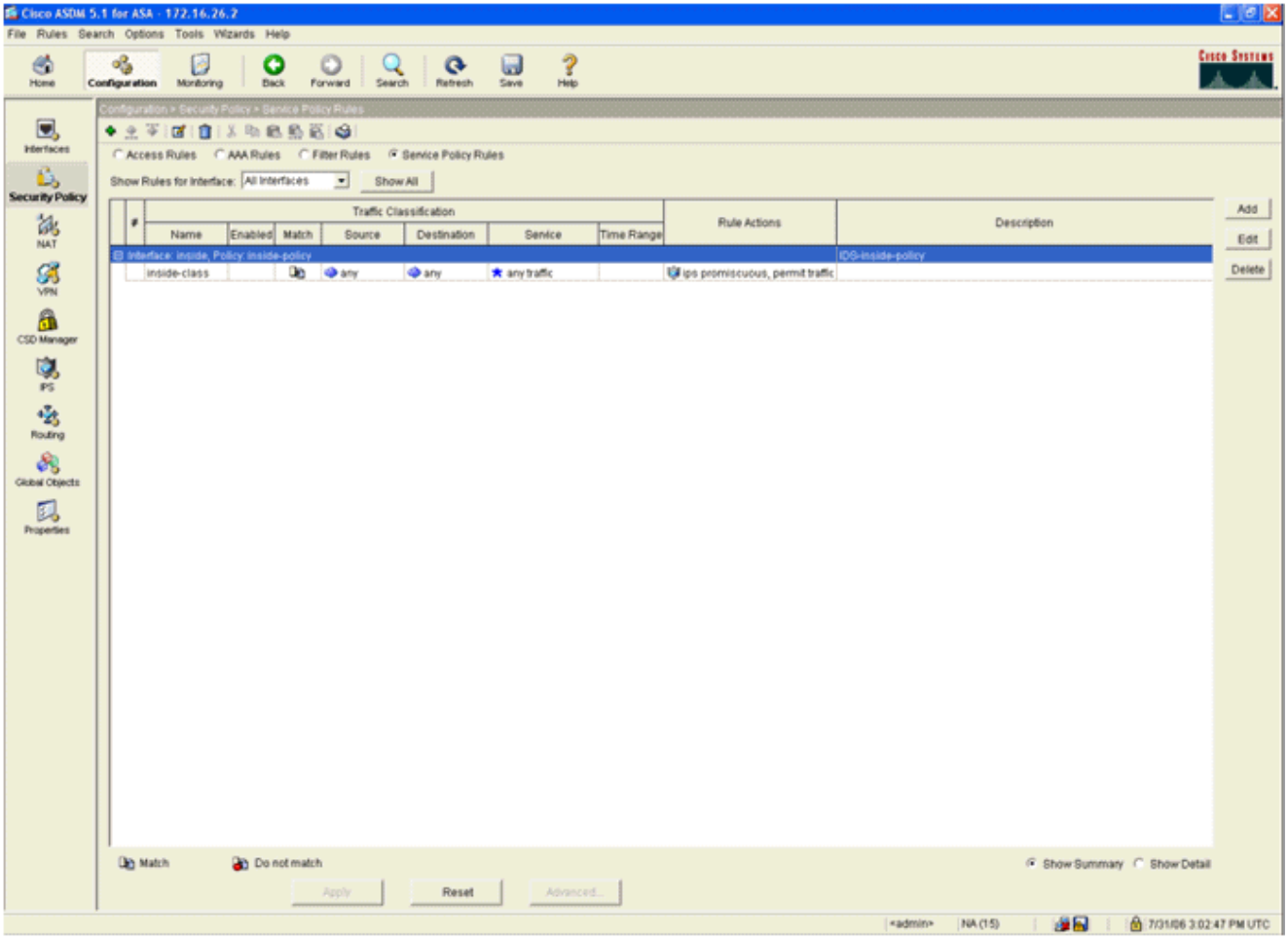
1. Melden Sie sich mit ASDM bei der ASA an. Nach erfolgreicher Anmeldung wird das Fenster "ASA Main System"
   angezeigt.



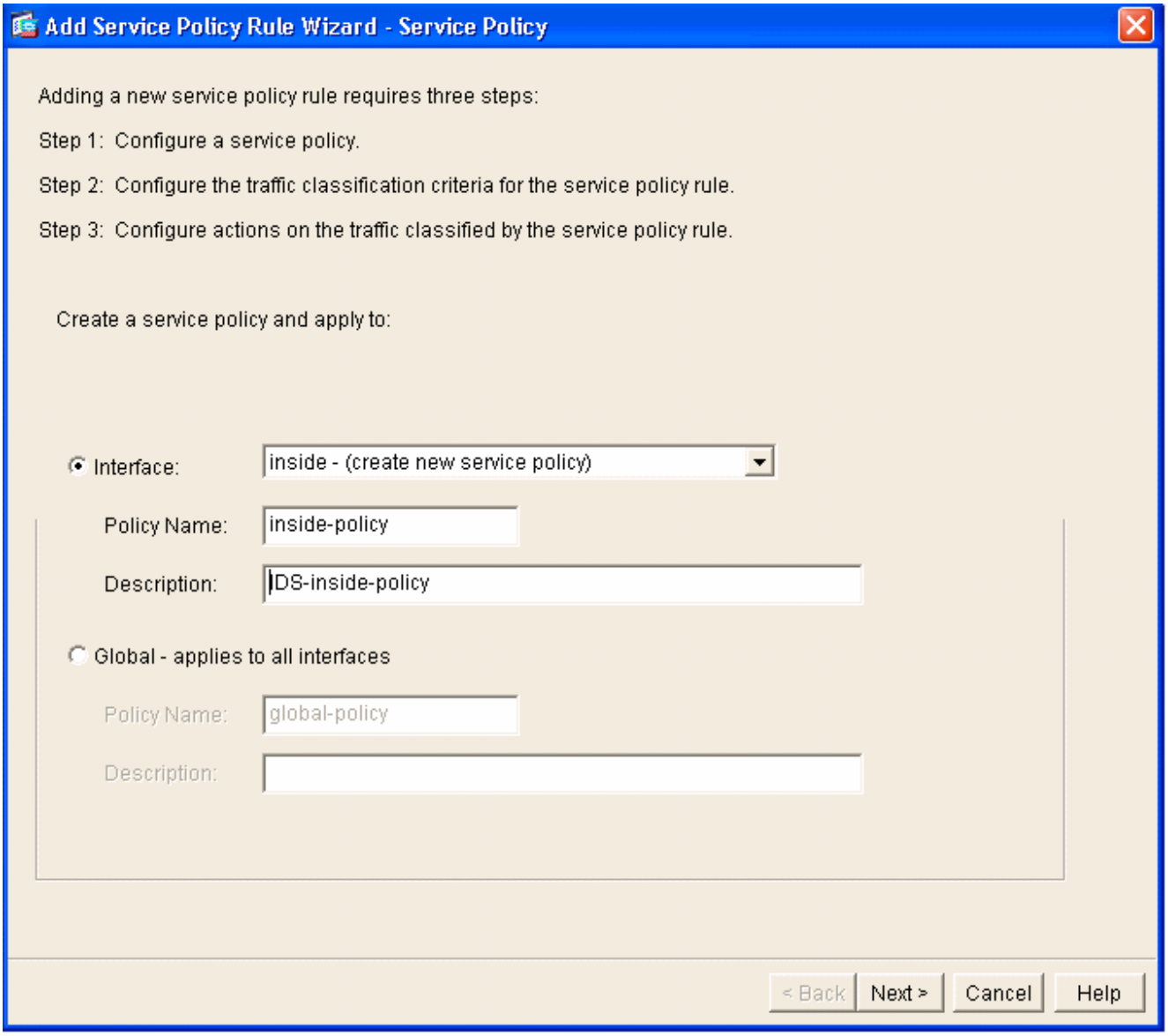
2. Klicken Sie oben auf der Seite auf **Konfiguration**. Das Fenster zeigt die ASA-Schnittstellen an.



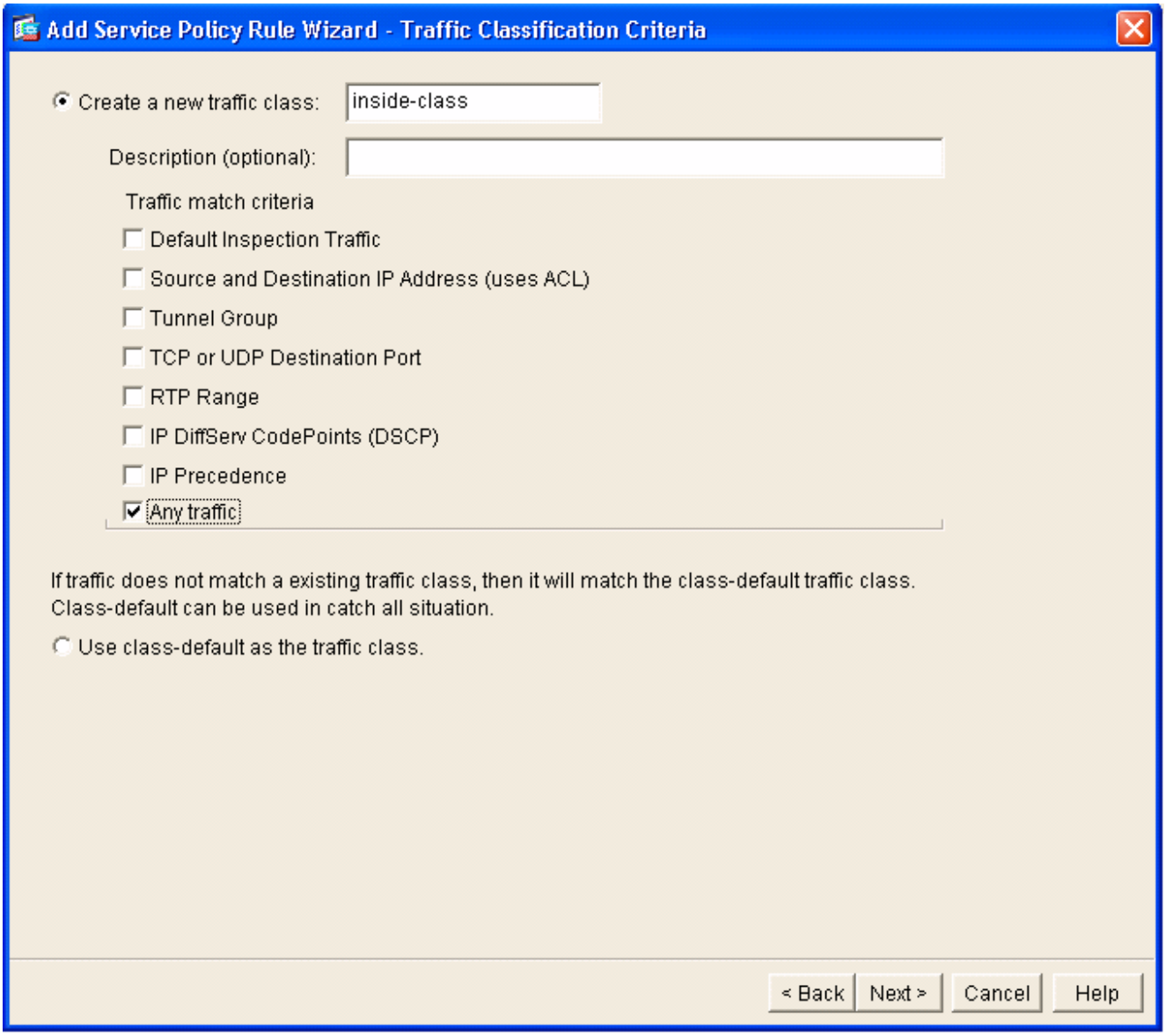
3. Klicken Sie links im Fenster auf **Sicherheitsrichtlinie**. Wählen Sie im sich daraus ergebenden Fenster die Registerkarte **Service Policy Rules (Servicebestimmungen)** aus.



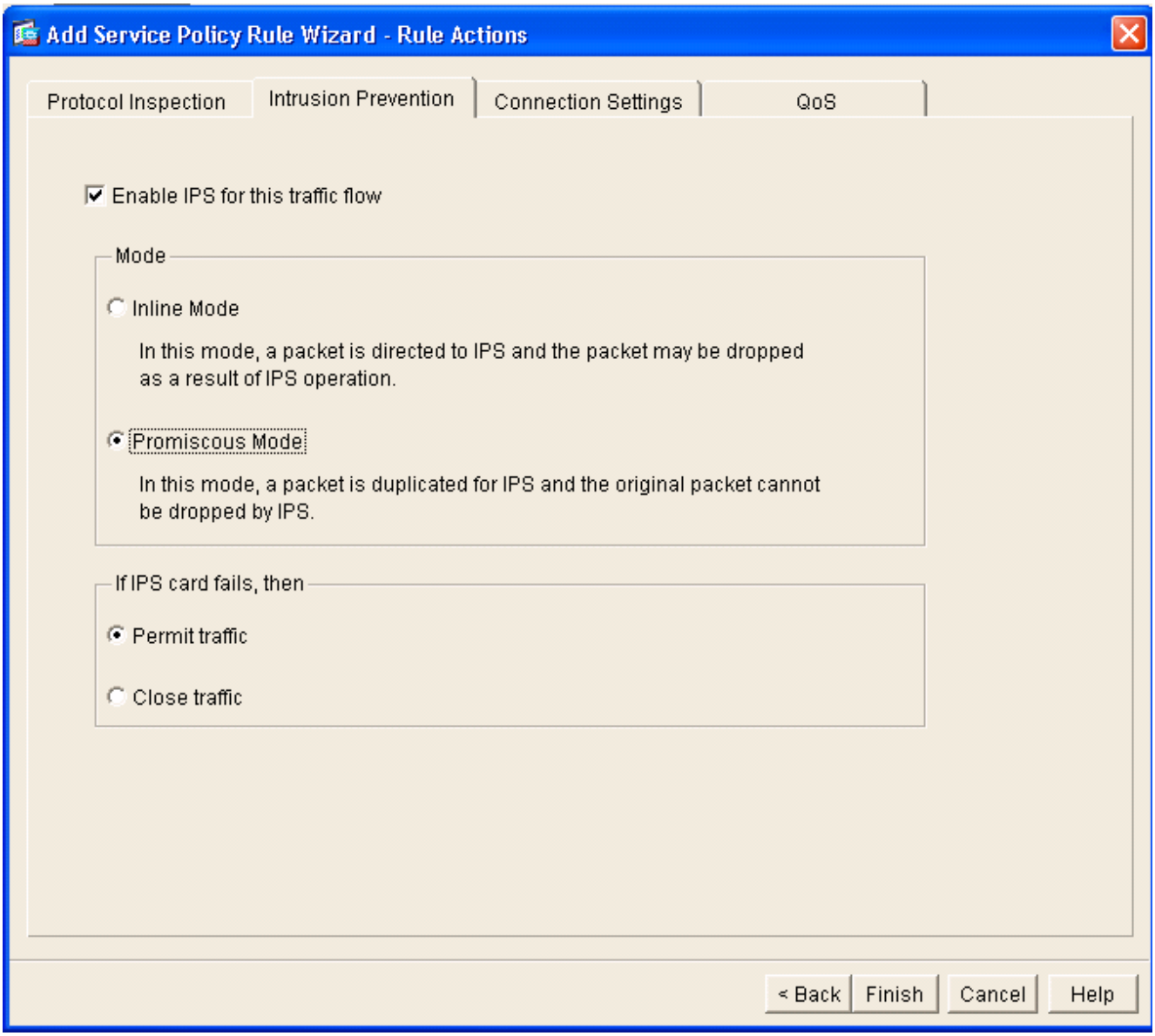
4. Klicken Sie auf **Hinzufügen**, um eine neue Richtlinie zu erstellen. Der Assistent zum Hinzufügen von Service Policy-Regeln wird in einem neuen Fenster gestartet.Klicken Sie auf **Interface** (Schnittstelle), und wählen Sie dann in der Dropdown-Liste die richtige Schnittstelle aus, um eine neue Richtlinie zu erstellen, die an eine der Schnittstellen gebunden ist, die den Datenverkehr weiterleiten.Geben Sie der Richtlinie einen Namen und eine Beschreibung der Vorgehensweise in den beiden Textfeldern.Klicken Sie auf **Weiter**, um mit dem nächsten Schritt
fortzufahren.



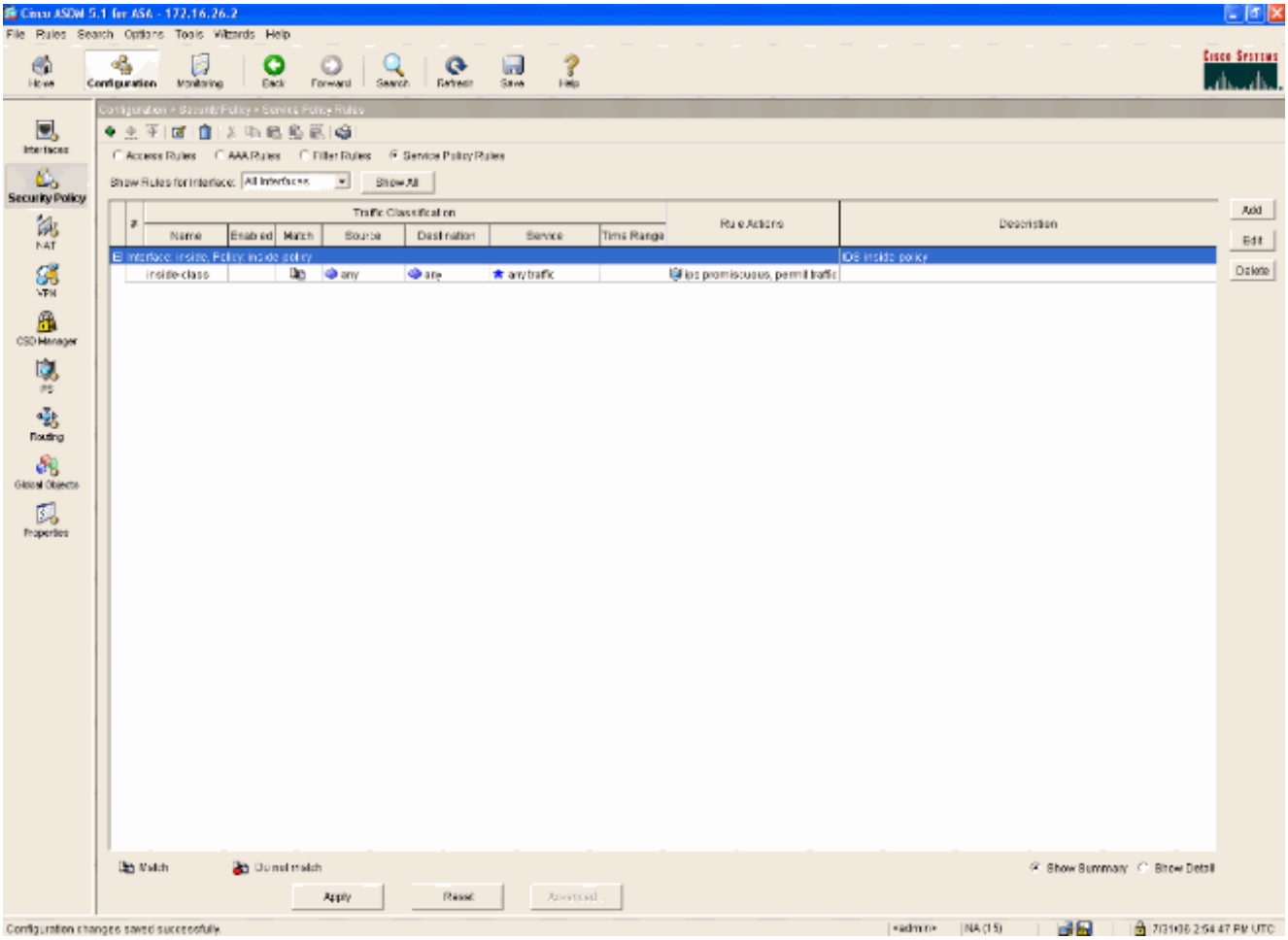
5. Erstellen Sie eine neue Datenverkehrsklasse, die auf die Richtlinie angewendet werden soll.Es ist sinnvoll, spezifische Klassen zu erstellen, um bestimmte Datentypen zu überprüfen. In diesem Beispiel wird jedoch Any Traffic (Beliebiger Datenverkehr) aus Gründen der Einfachheit ausgewählt. Klicken Sie auf **Weiter**, um fortzufahren.



6. Führen Sie diese Schritte aus, umWeisen Sie die ASA an, den Datenverkehr an ihr AIP-SSM weiterzuleiten.Aktivieren Sie **IPS für diesen Datenverkehrsfluss aktivieren**, um die Angriffserkennung zu aktivieren.Legen Sie den Modus auf **Promiscuous fest**, sodass eine Kopie des Datenverkehrs an das Out-of-Band-Modul gesendet wird, anstatt das Modul in Übereinstimmung mit dem Datenfluss zu platzieren.Klicken Sie auf **Datenverkehr zulassen**, um sicherzustellen, dass die ASA bei Ausfall des AIP-SSM in den Fail-Open-Zustand wechselt.Klicken Sie auf **Fertig stellen**, um die Änderung zu bestätigen.



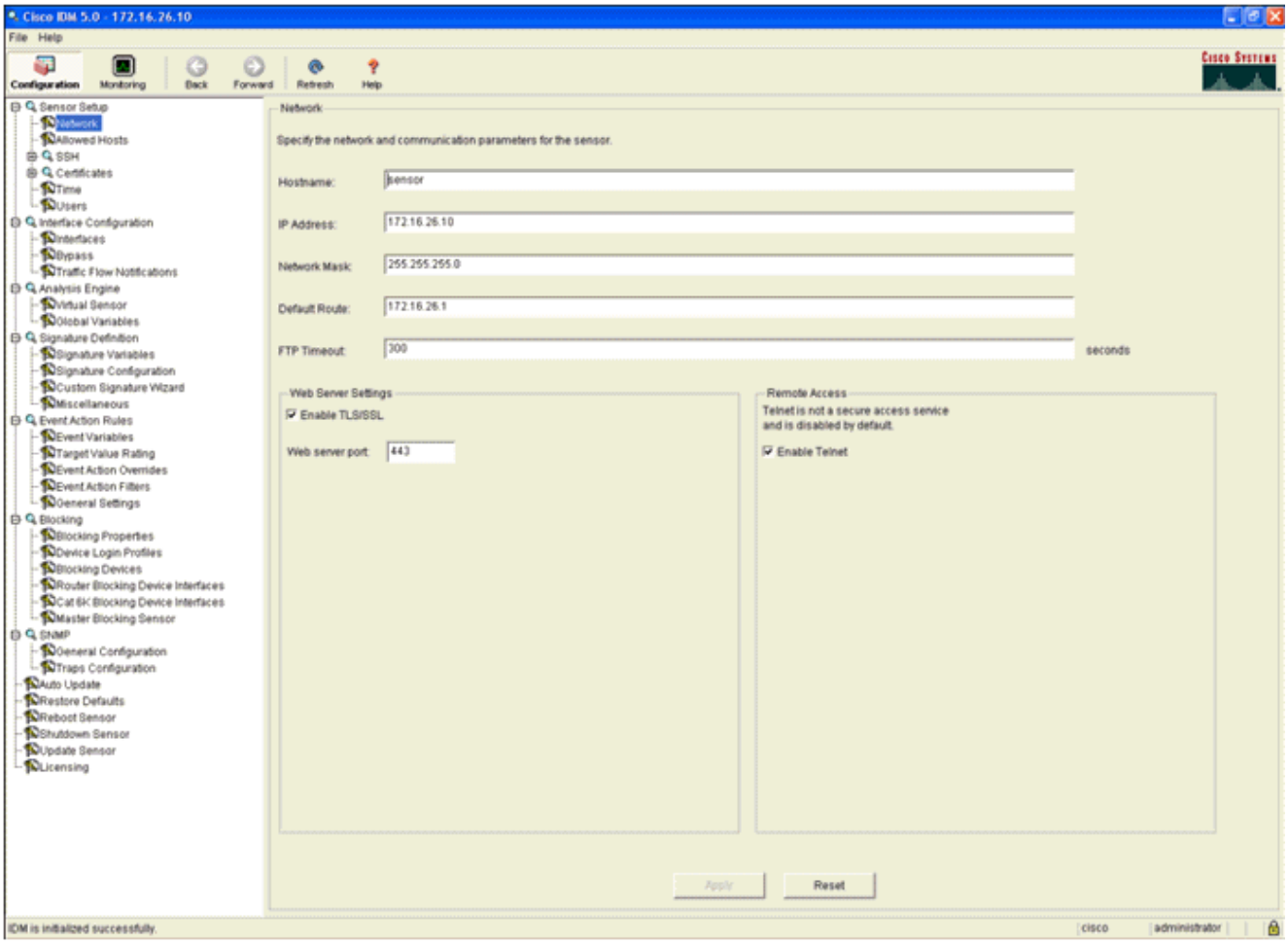
7. Die ASA ist jetzt so konfiguriert, dass Datenverkehr an das IPS-Modul gesendet wird. Klicken Sie in der obersten Zeile auf **Speichern**, um die Änderungen in die ASA zu schreiben.



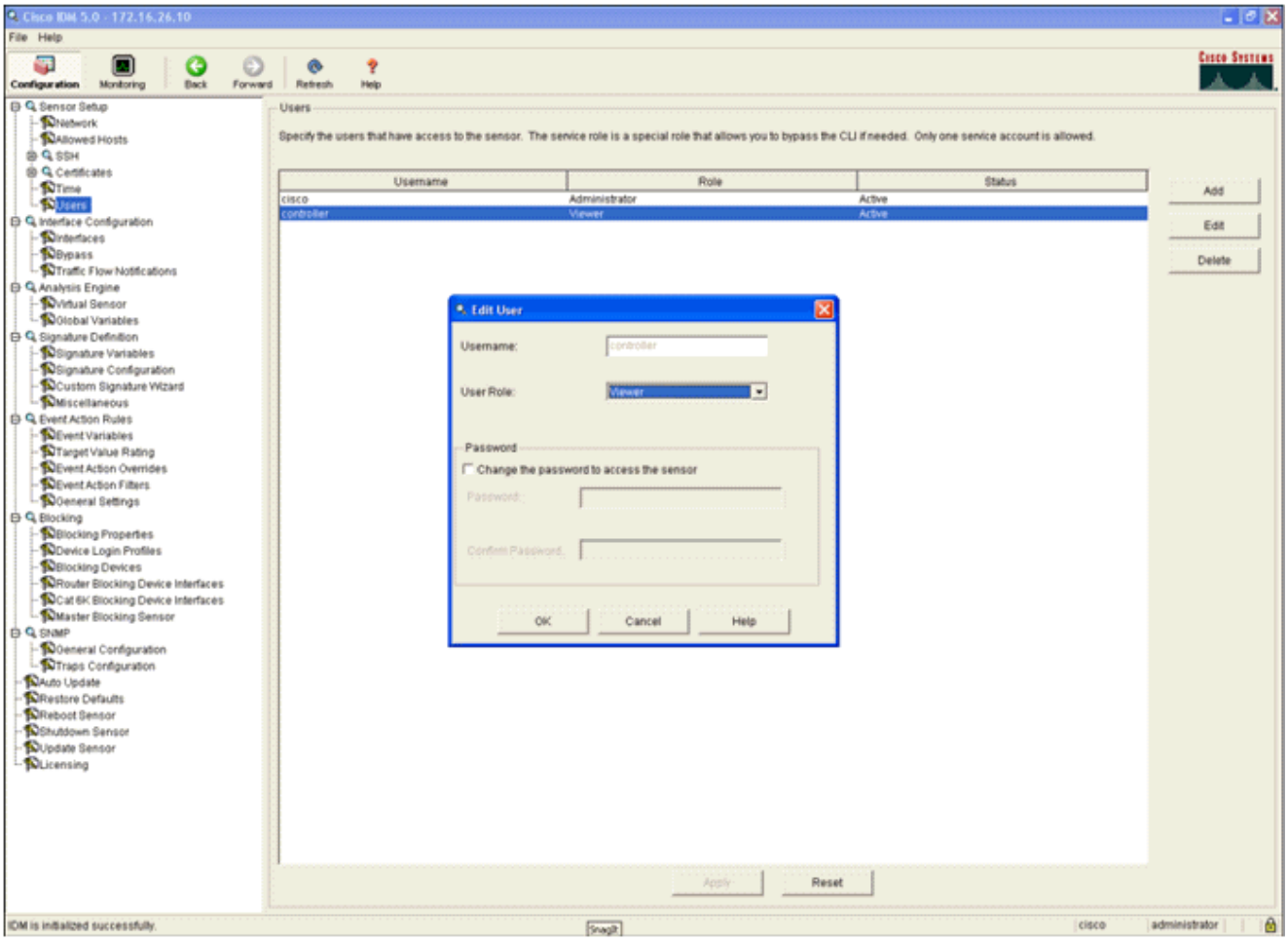
Konfigurieren des AIP-SSM für die Datenverkehrsüberprüfung

Während die ASA Daten an das IPS-Modul sendet, ordnen Sie die AIP-SSM-Schnittstelle der virtuellen Sensor-Engine zu.

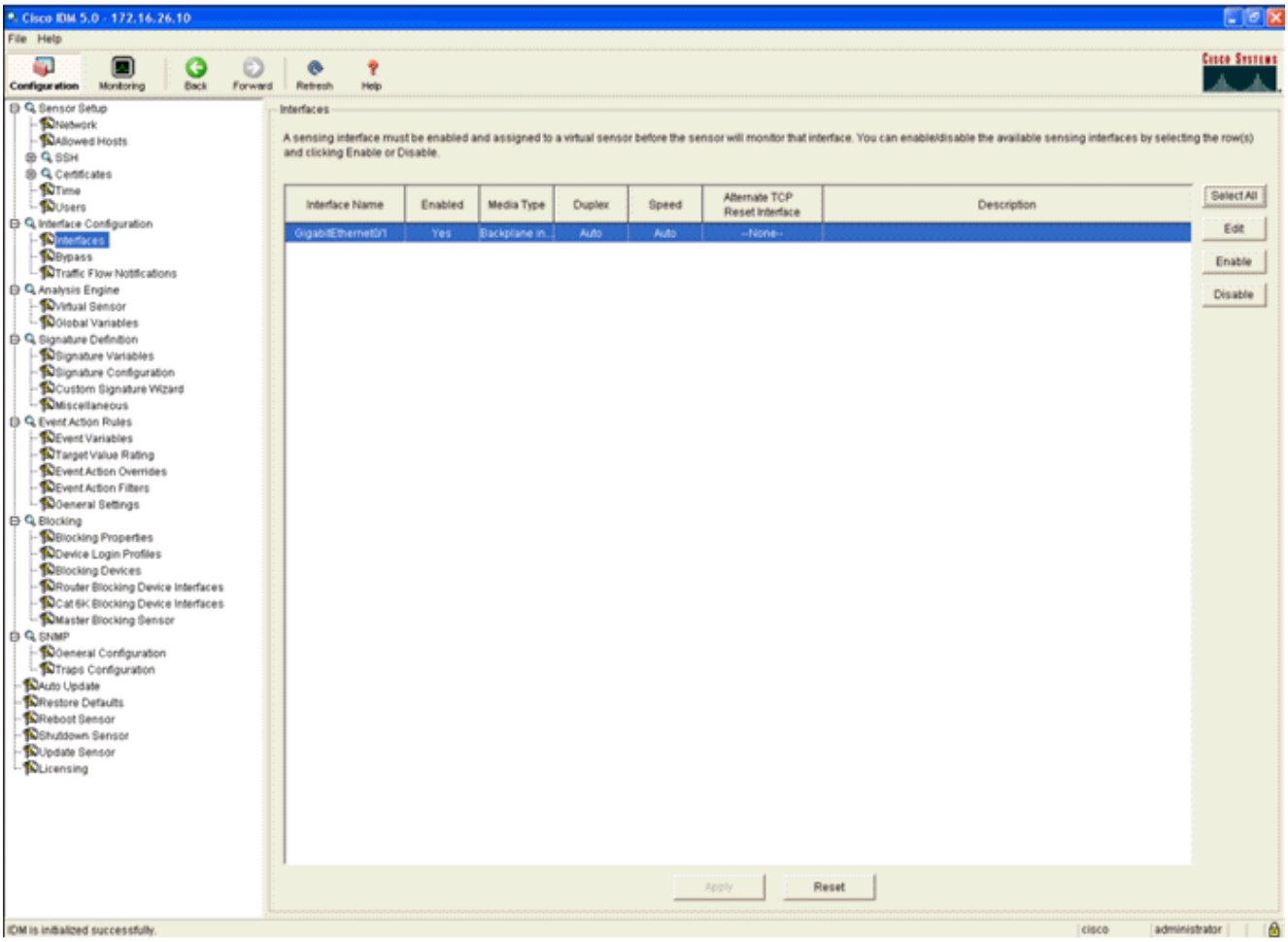
1. Melden Sie sich mit IDM beim AIP-SSM an.



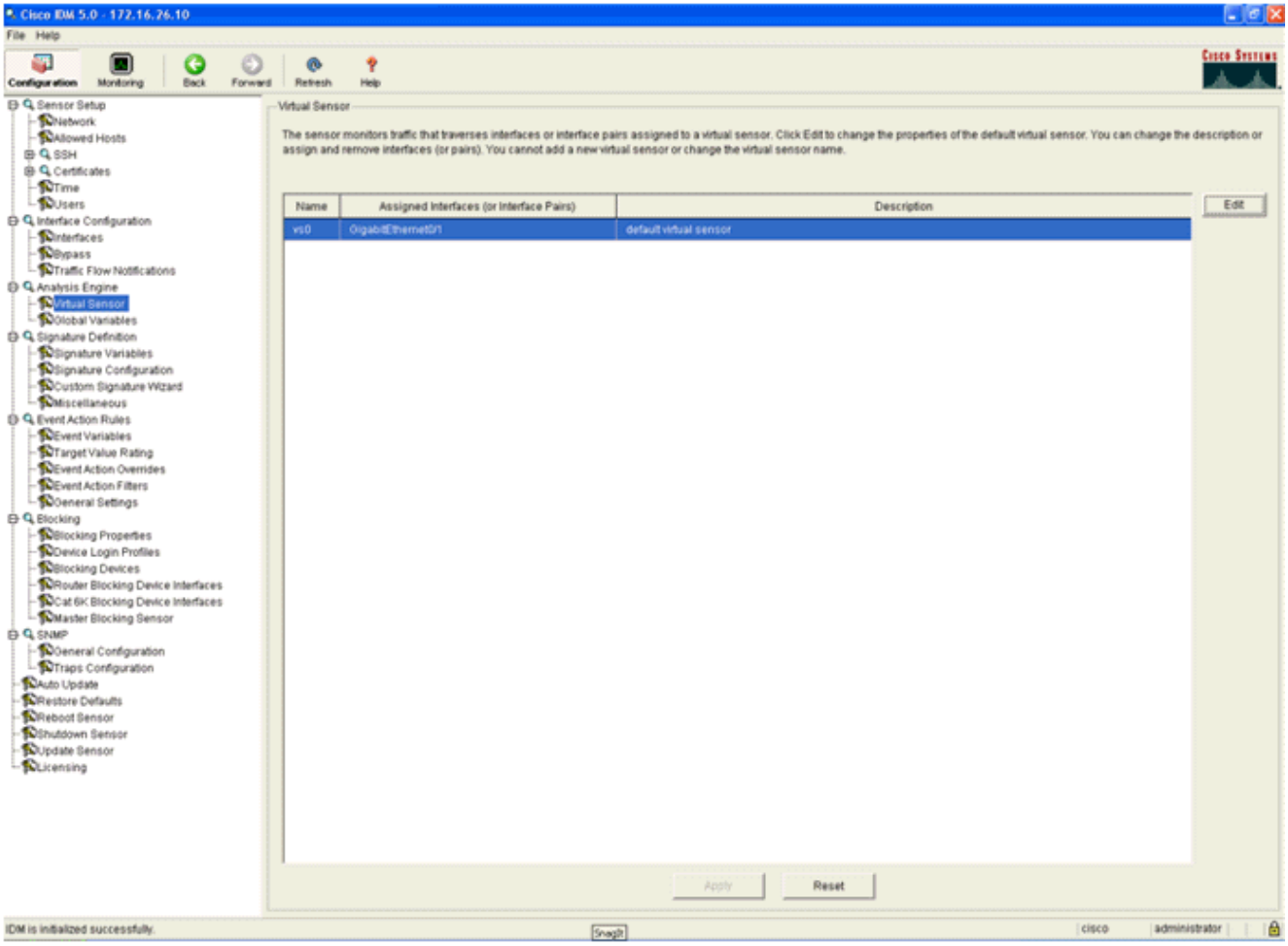
2. Fügen Sie einen Benutzer mit mindestens Anzeigeberechtigungen hinzu.



3. Aktivieren Sie die Schnittstelle.



4. Überprüfen Sie die Konfiguration des virtuellen Sensors.

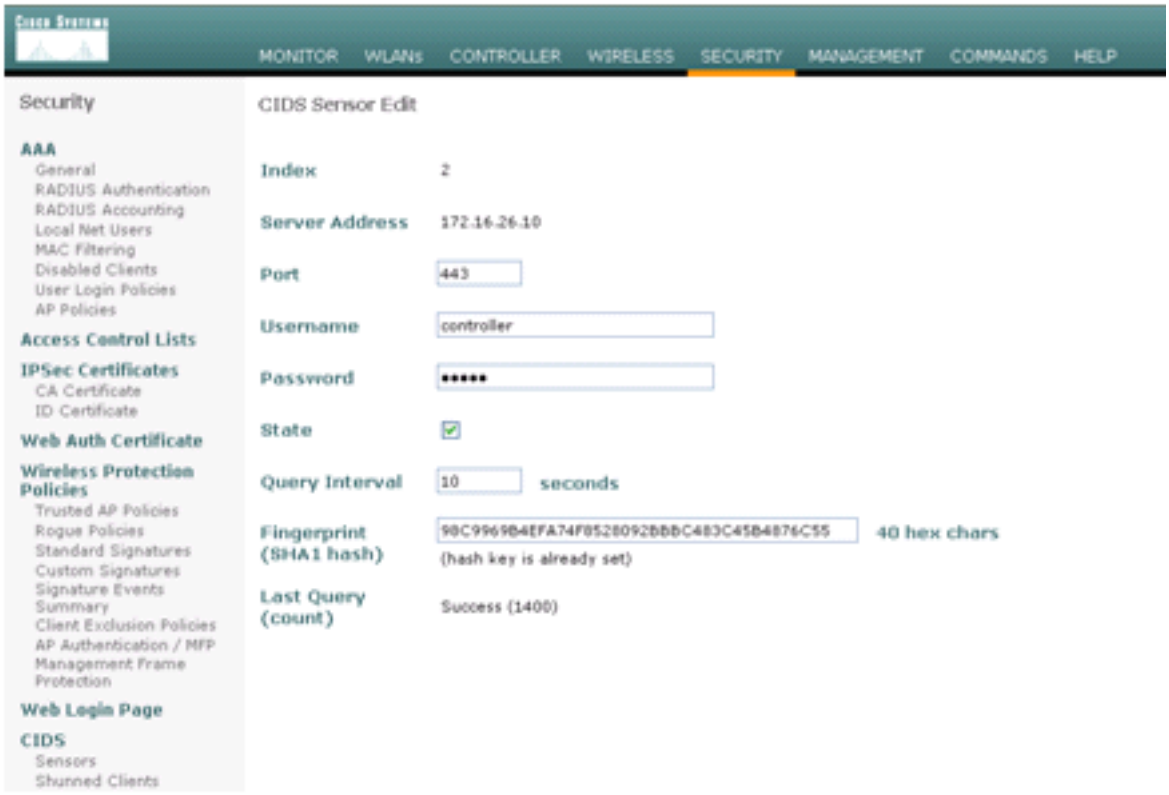


Konfigurieren eines WLC zum Abrufen des AIP-SSM für Client-Blöcke

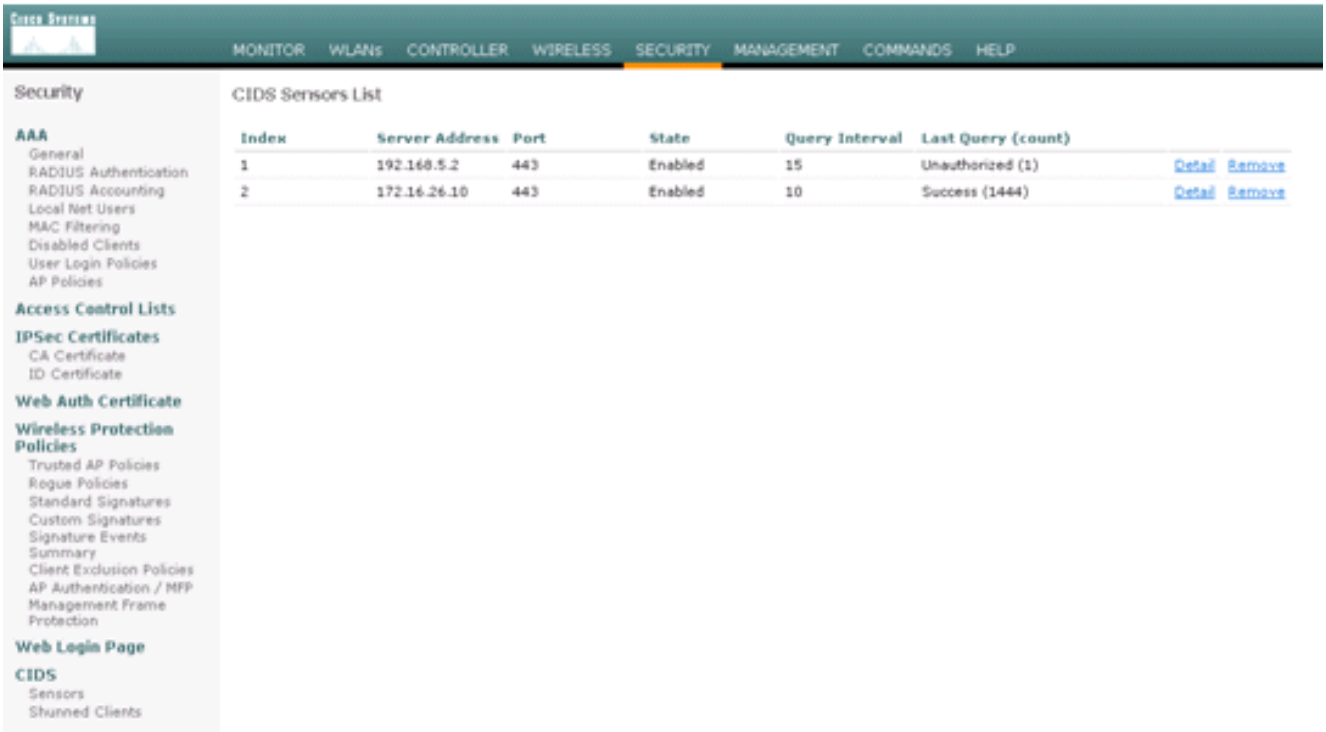
Führen Sie die folgenden Schritte aus, sobald der Sensor konfiguriert und zum Hinzufügen im Controller bereit ist:

1. Wählen Sie **Security > CIDS > Sensors > New** in the WLC aus.
2. Fügen Sie die IP-Adresse, die TCP-Portnummer, den Benutzernamen und das Kennwort hinzu, die Sie im vorherigen Abschnitt erstellt haben.
3. Um den Fingerabdruck vom Sensor abzurufen, führen Sie diesen Befehl im Sensor aus, und fügen Sie den SHA1-Fingerabdruck auf dem WLC hinzu (ohne Doppelpunkt). Diese Funktion dient zum Sichern der Abfragekommunikation zwischen Controller und IDS.

```
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
```



4. Überprüfen Sie den Status der Verbindung zwischen dem AIP-SSM und dem WLC.

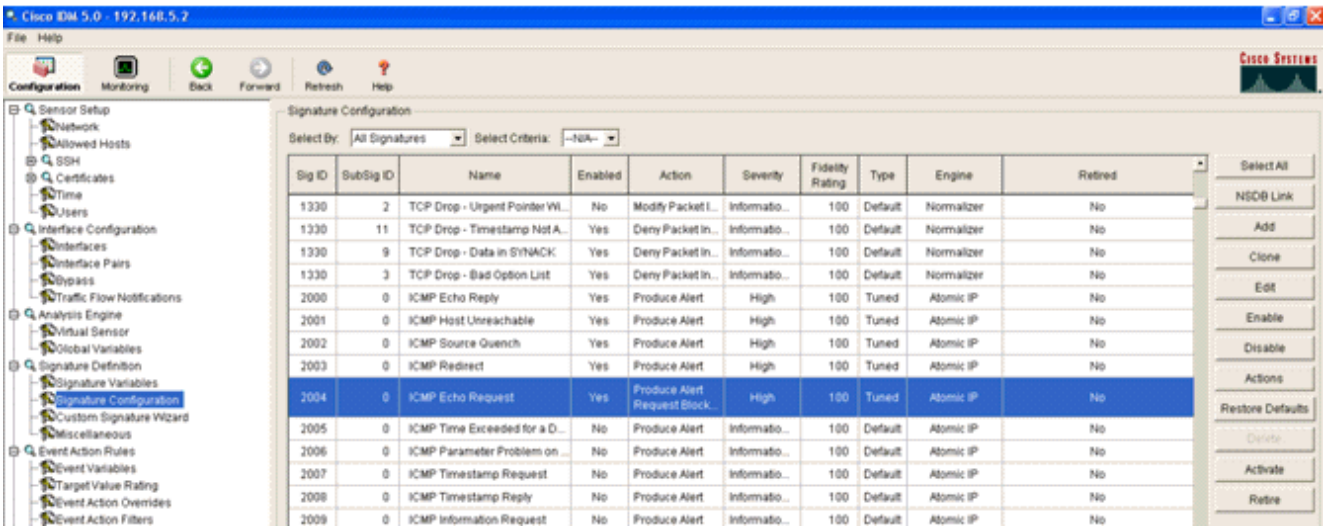


Hinzufügen einer Blockierungssignatur zum AIP-SSM

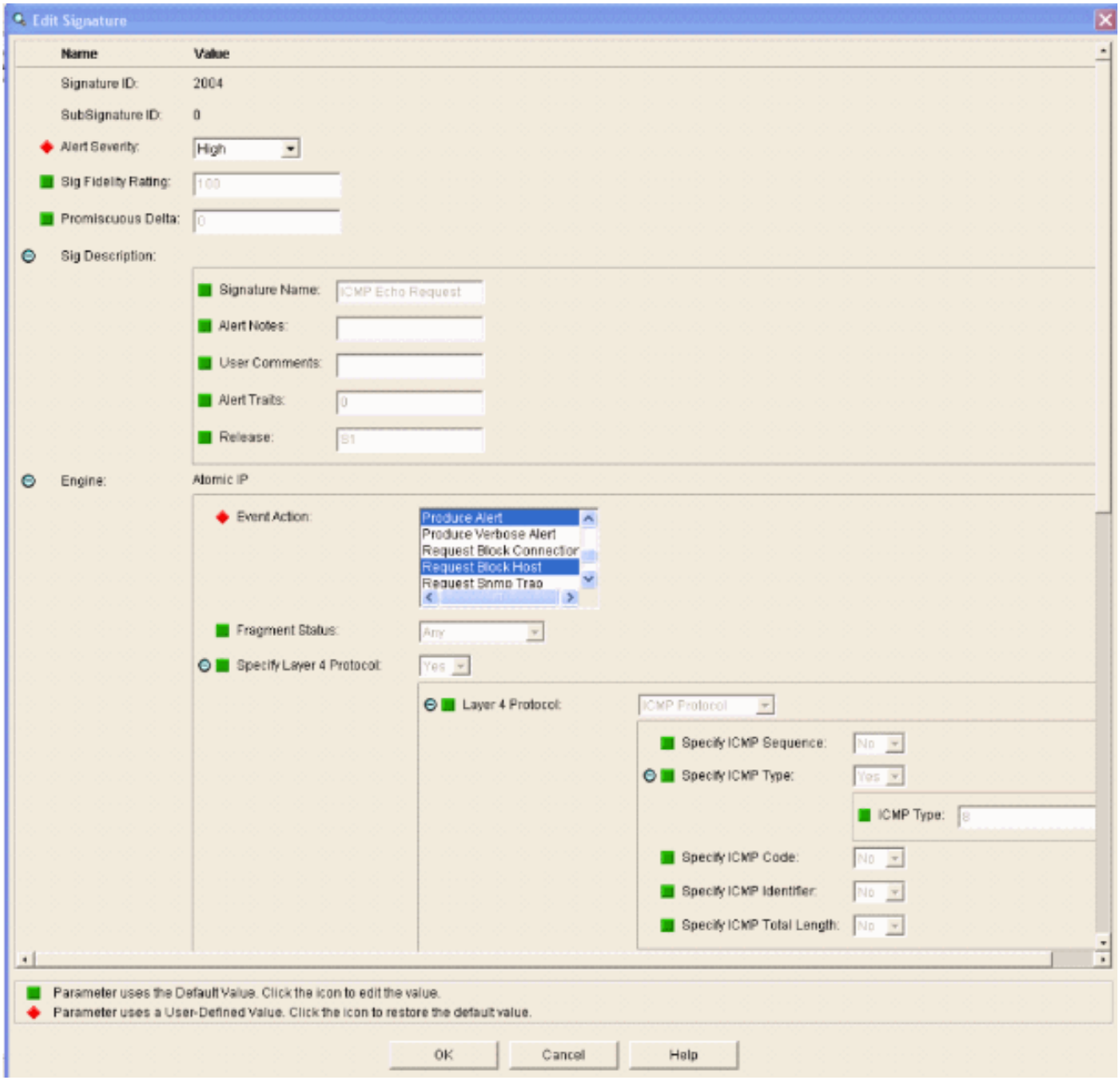
Fügen Sie eine Überprüfungssignatur hinzu, um Datenverkehr zu blockieren. Obwohl es viele Signaturen gibt, die diese Aufgabe auf der Grundlage der verfügbaren Tools ausführen können, wird in diesem Beispiel eine Signatur erstellt, die Ping-Pakete blockiert.

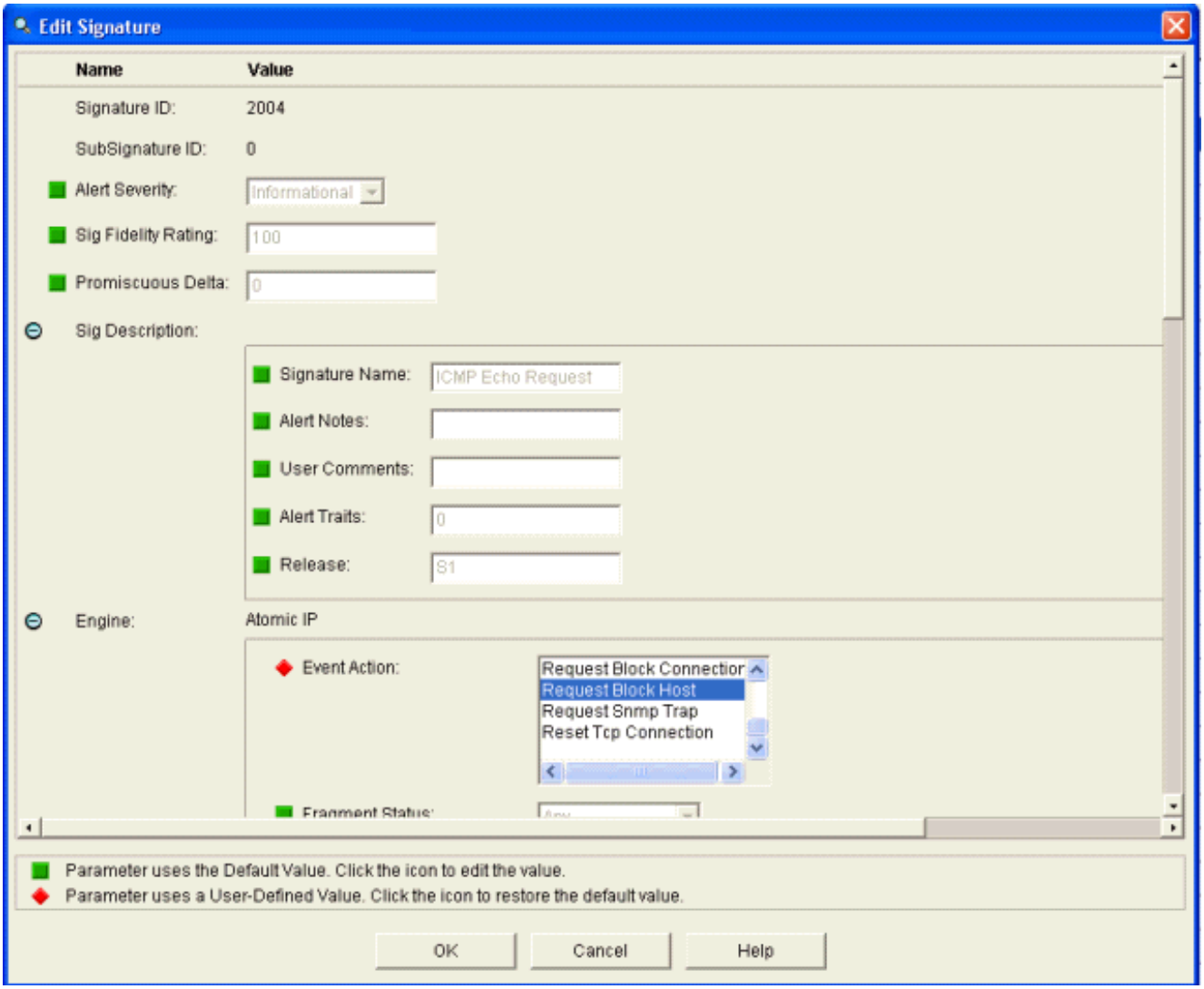
1. Wählen Sie die **2004-Signatur (ICMP-Echo-Anforderung)**, um eine schnelle Einrichtungsüberprüfung

durchzuführen.



2. Aktivieren Sie die Signatur, legen Sie den Alert Severity (Schweregrad der Warnung) auf **High (Hoch)** fest, und legen Sie die Event Action (Ereignisaktion) auf **Produce Alert** and **Request Block Host fest**, um diesen Verifizierungsschritt abzuschließen. Beachten Sie, dass die Aktion "Request Block Host" der Schlüssel für die Signalisierung des WLC zum Erstellen von Clientausnahmen
ist.


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:
S1
Engine:
Atomic IP
Event Action:
Produce Alert
Produce Verbose Alert
Request Block Connection
Request Block Host
Request Snmp Trap
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

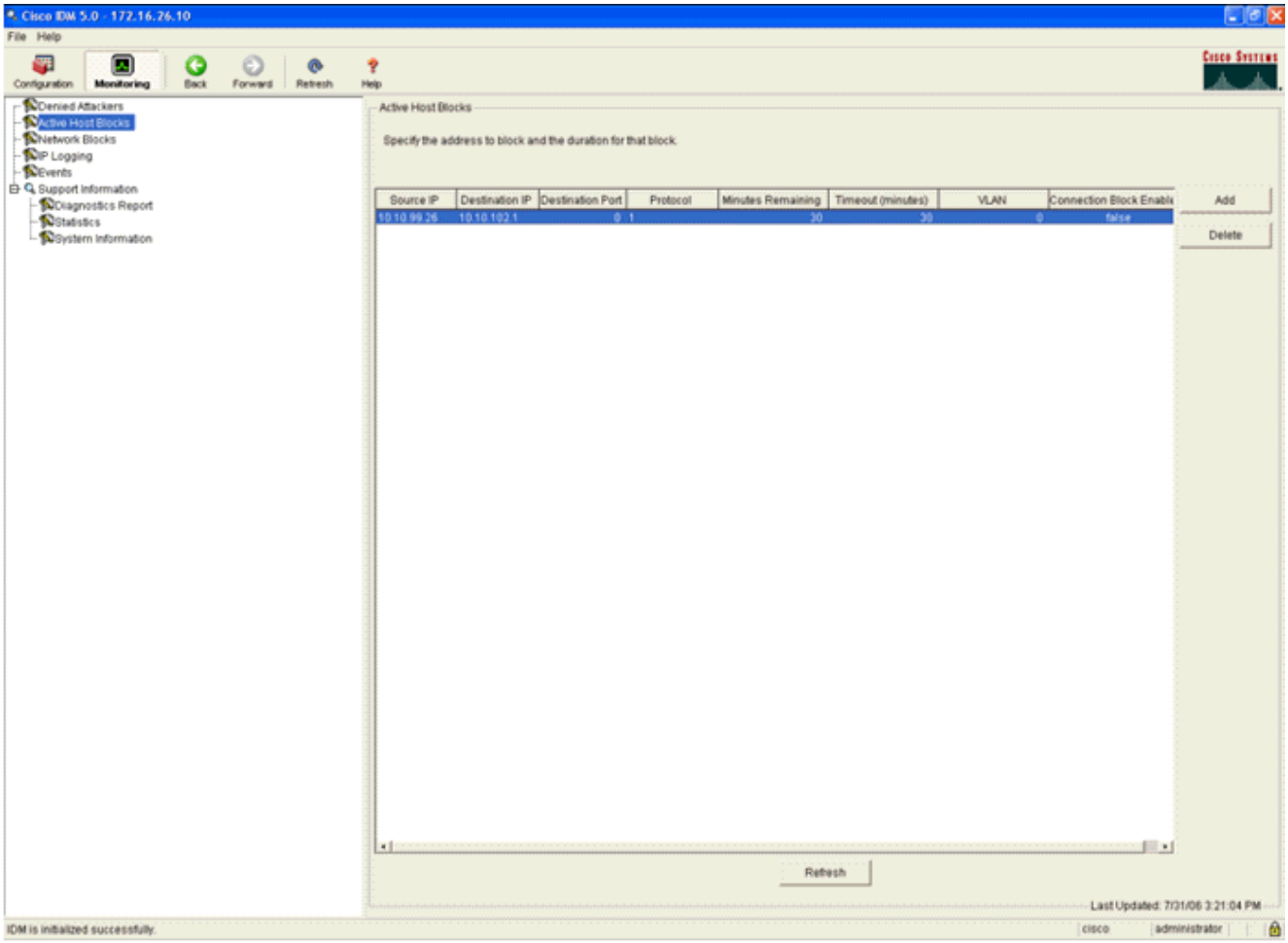


3. Klicken Sie auf **OK**, um die Signatur zu speichern.
4. Überprüfen Sie, ob die Signatur aktiv ist und für eine Blockierungsaktion festgelegt ist.
5. Klicken Sie auf **Apply**, um die Signatur auf das Modul zu übertragen.

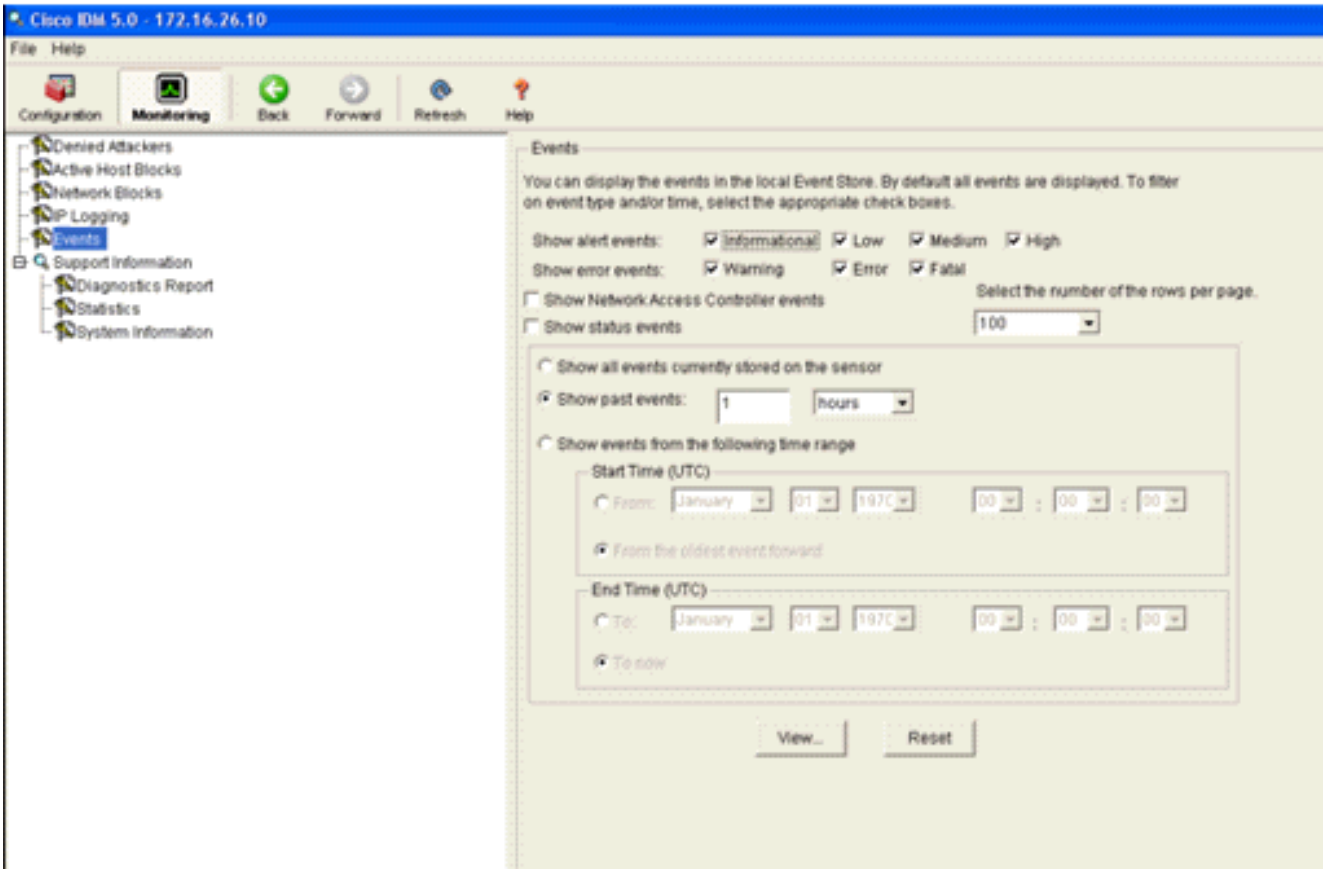
Überwachung von Blockierung und Ereignissen mit IDM

Führen Sie diese Schritte aus:

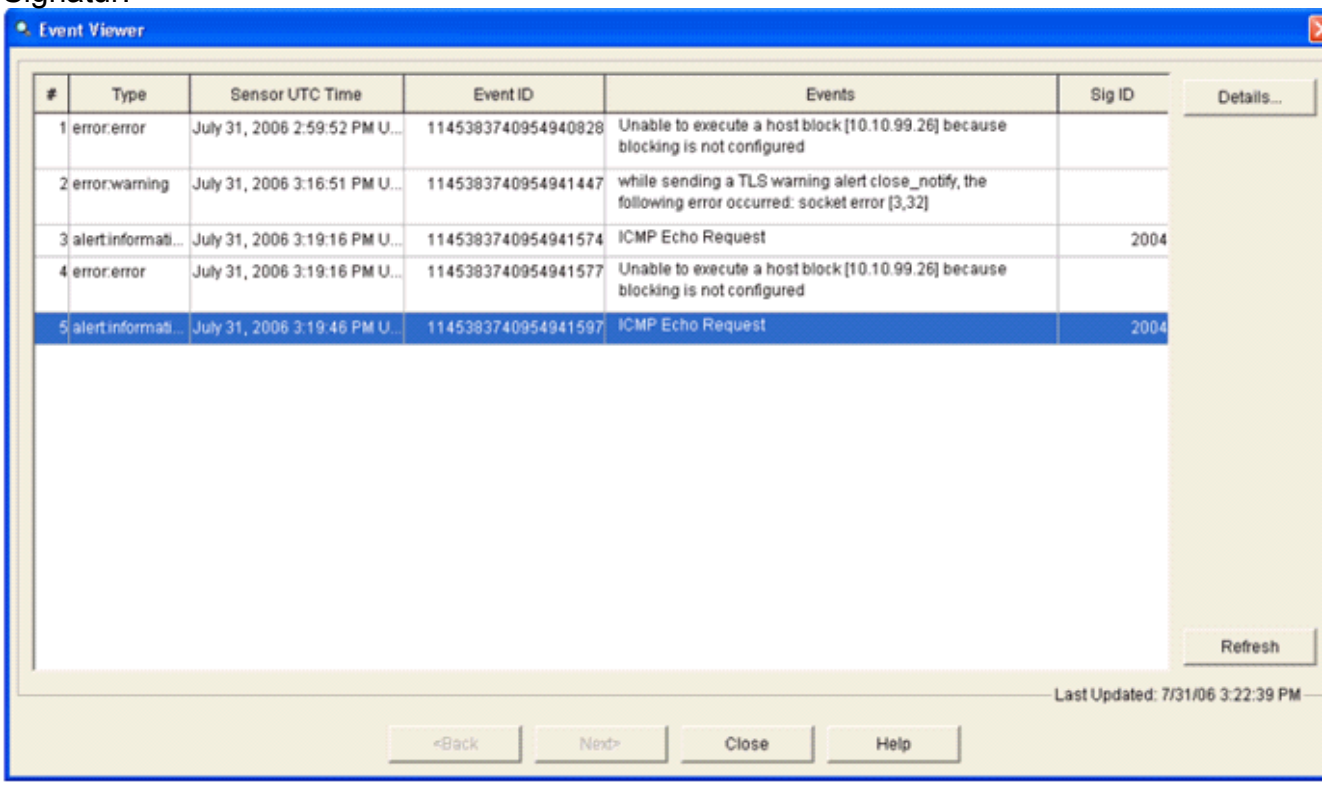
1. Wenn die Signatur erfolgreich feuert, gibt es innerhalb von IDM zwei Stellen, um dies zu beachten.Die erste Methode zeigt die aktiven Blöcke, die vom AIP-SSM installiert wurden. Klicken Sie in der oberen Aktionszeile auf **Monitoring**. Wählen Sie in der Liste der Elemente, die links angezeigt wird, **Active Host Blocks** aus. Wenn die Ping-Signatur auslöst, zeigt das Fenster Active Host Blocks (Aktive Host-Blöcke) die IP-Adresse des Angreifers, die Adresse des Geräts, gegen das ein Angriff stattfindet, und die Zeit, für die der Block noch gültig ist. Die Standardblockierungszeit beträgt 30 Minuten und kann eingestellt werden. Die Änderung dieses Werts wird in diesem Dokument jedoch nicht behandelt. Weitere Informationen zum Ändern dieses Parameters finden Sie in der ASA-Konfigurationsdokumentation (falls erforderlich). Entfernen Sie den Block sofort, wählen Sie ihn aus der Liste aus, und klicken Sie dann auf
Löschen.



Die zweite Methode zum Anzeigen ausgelöster Signaturen verwendet den AIP-SSM-Ereignispuffer. Wählen Sie auf der Seite IDM Monitoring (IDM-Überwachung) **Events (Ereignisse)** in der Liste Items (Elemente) auf der linken Seite aus. Das Dienstprogramm für die Veranstaltungssuche wird angezeigt. Legen Sie die gewünschten Suchkriterien fest, und klicken Sie auf
Anzeigen....



2. Die Ereignisanzeige wird dann mit einer Liste von Ereignissen angezeigt, die den angegebenen Kriterien entsprechen. Blättern Sie durch die Liste, und suchen Sie nach der Signatur für die ICMP-Echo-Anforderung, die in den vorherigen Konfigurationsschritten geändert wurde.Suchen Sie in der Spalte Events (Ereignisse) nach dem Namen der Signatur, oder suchen Sie in der Spalte Sig ID (Signatur-ID) nach der Identifikationsnummer der
Signatur.



3. Nachdem Sie die Signatur gefunden haben, doppelklicken Sie auf den Eintrag, um ein neues Fenster zu öffnen. Das neue Fenster enthält detaillierte Informationen zum Ereignis, das die

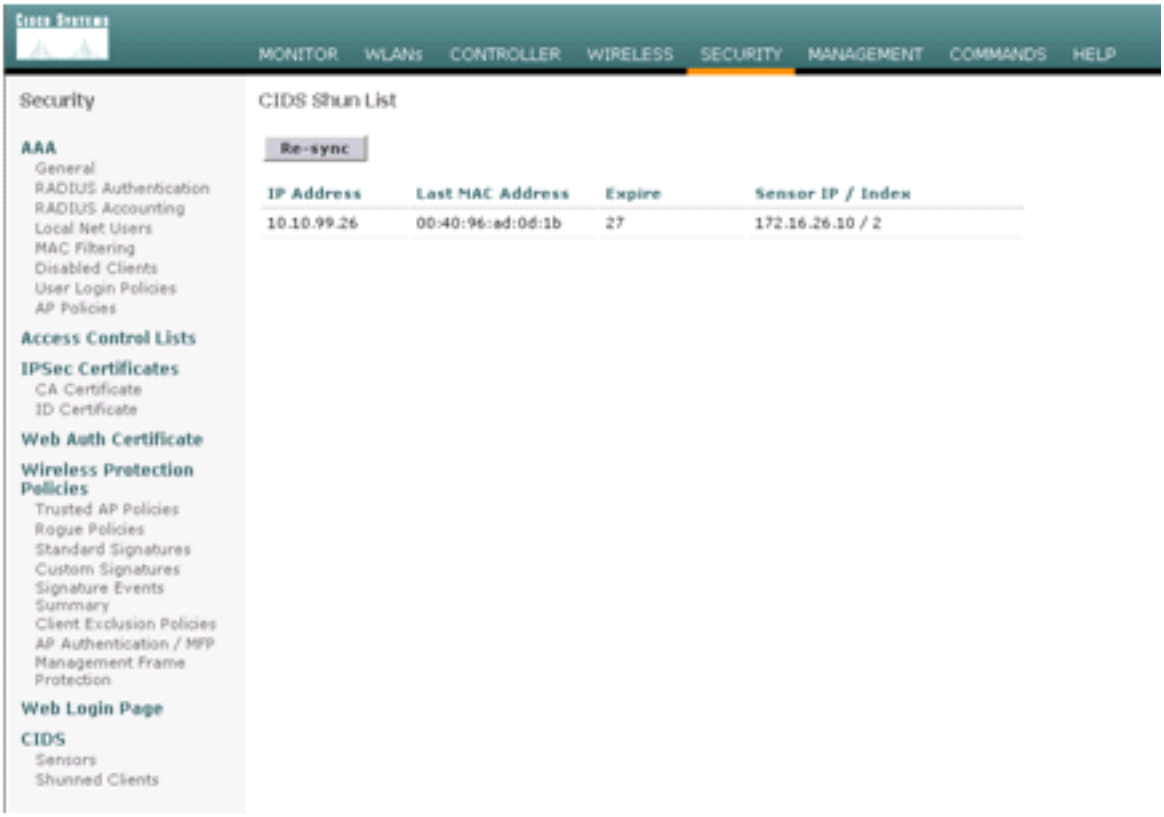
Signatur ausgelöst hat.

Details for 1145383740954941597

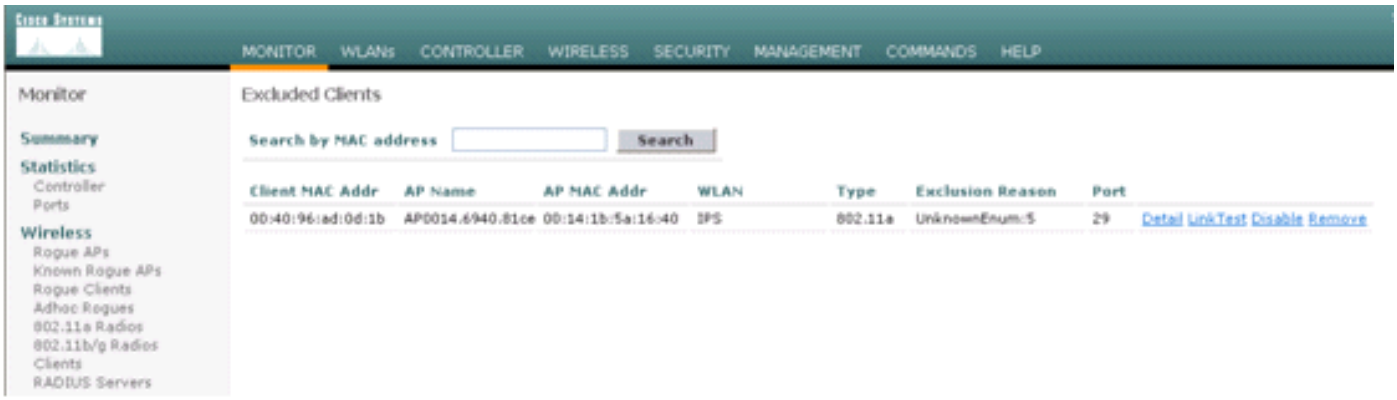
```
evIdsAlert: eventId=1145383740954941597  vendor=Cisco  severity=informational
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 341
  time: July 31, 2006 3:19:46 PM UTC  offset=0  timeZone=UTC
  signature:   description=ICMP Echo Request  id=2004  version=S1
    subsigId: 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
```

Überwachung des Client-Ausschlusses in einem Wireless-Controller

Die Liste "Shunned Clients" im Controller wird zu diesem Zeitpunkt mit der IP- und MAC-Adresse des Hosts ausgefüllt.



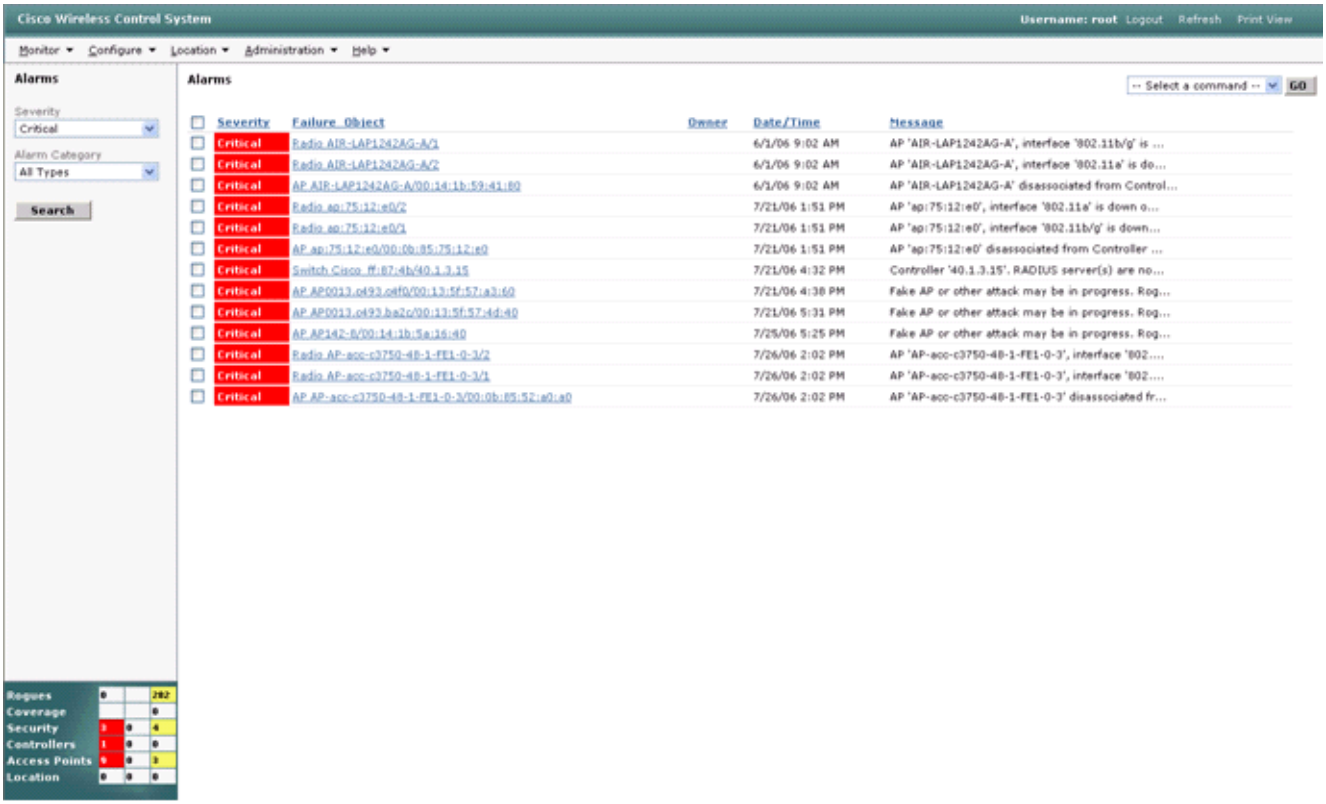
Der Benutzer wird der Clientausschlussliste hinzugefügt.



Überwachung von Ereignissen in WCS

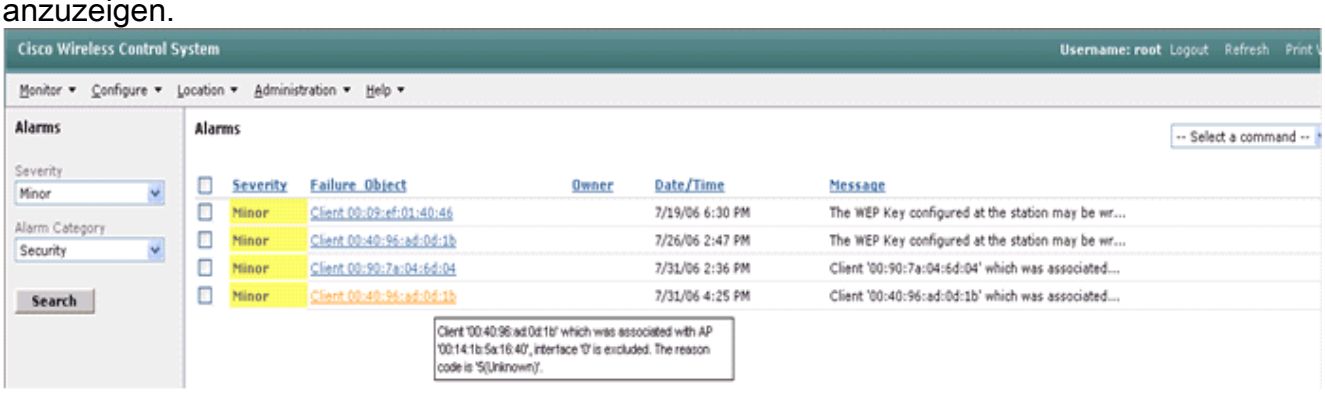
Sicherheitsereignisse, die einen Block im AIP-SSM auslösen, veranlassen den Controller, die Adresse des Straftäters der Ausschlussliste des Clients hinzuzufügen. Ein Ereignis wird auch in WCS generiert.

1. Verwenden Sie das Dienstprogramm **Monitor > Alarms** im WCS-Hauptmenü, um das Ausschlussereignis anzuzeigen. WCS zeigt zunächst alle nicht gelesenen Alarme an und zeigt auch eine Suchfunktion auf der linken Seite des Fensters an.
2. Ändern Sie die Suchkriterien, um den Clientblock zu suchen. Wählen Sie unter Severity (Schweregrad) die Option **Minor (Gering) aus**, und legen Sie die Alarmkategorie auch auf **Security (Sicherheit)** fest.
3. Klicken Sie auf **Suchen**.



4. Im Fenster Alarm werden dann nur Sicherheitswarnungen mit geringem Schweregrad angezeigt. Zeigen Sie mit der Maus auf das Ereignis, das den Block innerhalb des AIP-SSM

ausgelöst hat.Insbesondere zeigt WCS die MAC-Adresse der Client-Station an, die den Alarm ausgelöst hat. Durch den Verweis auf die entsprechende Adresse öffnet WCS ein kleines Fenster mit Ereignisdetails. Klicken Sie auf den Link, um die gleichen Details in einem anderen Fenster
anzuzeigen.



Cisco ASA - Beispielkonfiguration

```
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 Intrusion Prevention System - Beispielkonfiguration

```
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#
```

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Installation und Verwendung von Cisco Intrusion Prevention System Device Manager 5.1
- Cisco Adaptive Security Appliances der Serie ASA 5500 - Konfigurationsleitfäden
- Konfigurieren des Cisco Intrusion Prevention System-Sensors mithilfe der Befehlszeilenschnittstelle 5.0 - Konfigurieren von Schnittstellen

- WLC-Konfigurationsleitfaden 4.0
- Technischer Support für Wireless
- Häufig gestellte Fragen zum Wireless LAN Controller (WLC)
- Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point
- Konfigurieren von Sicherheitslösungen
- Technischer Support und Dokumentation für Cisco Systeme