Guida all'integrazione di Controller LAN wireless e IPS

Sommario

Introduzione

Il Cisco Unified Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) fa parte di Cisco Self-Defending Network ed è la prima soluzione di sicurezza wireless e cablata integrata del settore. Cisco Unified IDS/IPS adotta un approccio completo alla sicurezza: ai limiti wireless, cablati, WAN e attraverso il centro dati. Quando un client associato invia traffico dannoso attraverso la Cisco Unified Wireless Network, un dispositivo IDS cablato Cisco rileva l'attacco e invia richieste shun ai Cisco Wireless LAN Controller (WLC), che quindi dissociano il dispositivo client.

Cisco IPS è una soluzione inline basata su rete progettata per identificare, classificare e arrestare in modo accurato il traffico dannoso, inclusi worm, spyware/adware, virus di rete e abusi delle

applicazioni, prima che influiscano sulla business continuity.

Utilizzando il software sensore Cisco IPS versione 5, la soluzione Cisco IPS combina servizi di prevenzione in linea con tecnologie innovative per migliorare l'accuratezza. Il risultato è una totale fiducia nella protezione fornita della soluzione IPS, senza il timore di perdere il traffico legittimo. La soluzione Cisco IPS offre anche una protezione completa della rete grazie alla possibilità unica di collaborare con altre risorse di sicurezza della rete e fornisce un approccio proattivo alla protezione della rete.

La soluzione Cisco IPS consente agli utenti di bloccare un numero maggiore di minacce con maggiore sicurezza grazie all'utilizzo di queste funzionalità:

- **Tecnologie di prevenzione in linea accurate**: offrono la massima sicurezza per intraprendere azioni preventive contro una più ampia gamma di minacce senza il rischio di far cadere il traffico legittimo. Queste tecnologie uniche offrono un'analisi contestuale intelligente, automatizzata dei dati e consentono di ottenere il massimo dalla soluzione di prevenzione delle intrusioni.
- **Identificazione delle minacce multi-vettoriali**: protegge la rete da violazioni delle policy, sfruttamento delle vulnerabilità e attività anomale attraverso un'ispezione dettagliata del traffico nei livelli da 2 a 7.
- **Collaborazione unica in rete**: migliora la scalabilità e la resilienza attraverso la collaborazione in rete, incluse tecniche efficienti di acquisizione del traffico, funzionalità di bilanciamento del carico e visibilità nel traffico crittografato.
- **Soluzioni di installazione complete**: fornisce soluzioni per tutti gli ambienti, dalle piccole e medie imprese (PMI) alle filiali, dalle grandi aziende alle installazioni di provider di servizi.
- **Potenti servizi di gestione, correlazione degli eventi e supporto**: offrono una soluzione completa che include configurazione, gestione, correlazione dei dati e servizi di supporto avanzati. In particolare, il sistema MARS (Security Monitoring, Analysis, and Response System) di Cisco identifica, isola e consiglia la rimozione precisa degli elementi dannosi per una soluzione di prevenzione delle intrusioni a livello di rete. Inoltre, il Cisco Incident Control System previene la diffusione di nuovi worm e virus consentendo alla rete di adattarsi rapidamente e fornire una risposta distribuita.

Se combinati, questi elementi offrono una soluzione di prevenzione in linea completa e consentono di rilevare e arrestare la più ampia gamma di traffico dannoso prima che influisca sulla business continuity. L'iniziativa Cisco Self-Defending Network richiede una sicurezza integrata e integrata per le soluzioni di rete. Gli attuali sistemi WLAN basati su LWAPP (Lightweight Access Point Protocol) supportano solo le funzionalità IDS di base, in quanto si tratta essenzialmente di un sistema di layer 2 e ha una potenza di elaborazione di linea limitata. Cisco rilascia tempestivamente il nuovo codice per includere nuove funzionalità avanzate nei nuovi codici. La versione 4.0 offre le funzionalità più recenti che includono l'integrazione di un sistema WLAN basato su LWAPP con la linea di prodotti Cisco IDS/IPS. In questa versione, l'obiettivo è quello di consentire al sistema Cisco IDS/IPS di istruire i WLC di bloccare alcuni client dall'accesso alle reti wireless quando viene rilevato un attacco dal layer 3 al layer 7 che interessa il client in questione.

Prerequisiti

Requisiti

Assicurarsi di soddisfare i seguenti requisiti minimi:

- Firmware WLC versione 4.x e successive
- Èconsigliabile avere a disposizione informazioni su come configurare Cisco IPS e Cisco WLC.

Componenti usati

Cisco WLC

Questi controller sono inclusi nella versione software 4.0 per le modifiche IDS:

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

Access point

- Cisco Aironet serie 1100 AG Lightweight Access Point
- Cisco Aironet serie 1200 AG Lightweight Access Point
- Cisco Aironet serie 1300 Lightweight Access Point
- Cisco Aironet serie 1000 Lightweight Access Point

Gestione

- Cisco Wireless Control System (WCS)
- Cisco serie 4200 Sensor
- Gestione Cisco IDS - Cisco IDS Device Manager (IDM)

Piattaforme Cisco Unified IDS/IPS

- Cisco IPS serie 4200 Sensori con software sensore Cisco IPS 5.x o versioni successive.
- SSM10 e SSM20 per Cisco ASA serie 5500 Adaptive Security Appliance con software sensore Cisco IPS 5.x
- Cisco ASA serie 5500 Adaptive Security Appliance con software sensore Cisco IPS 5.x
- Cisco IDS Network Module (NM-CIDS) con software sensore Cisco IPS 5.x
- Cisco Catalyst serie 6500 Intrusion Detection System Module 2 (IDSM-2) con software sensore Cisco IPS 5.x

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

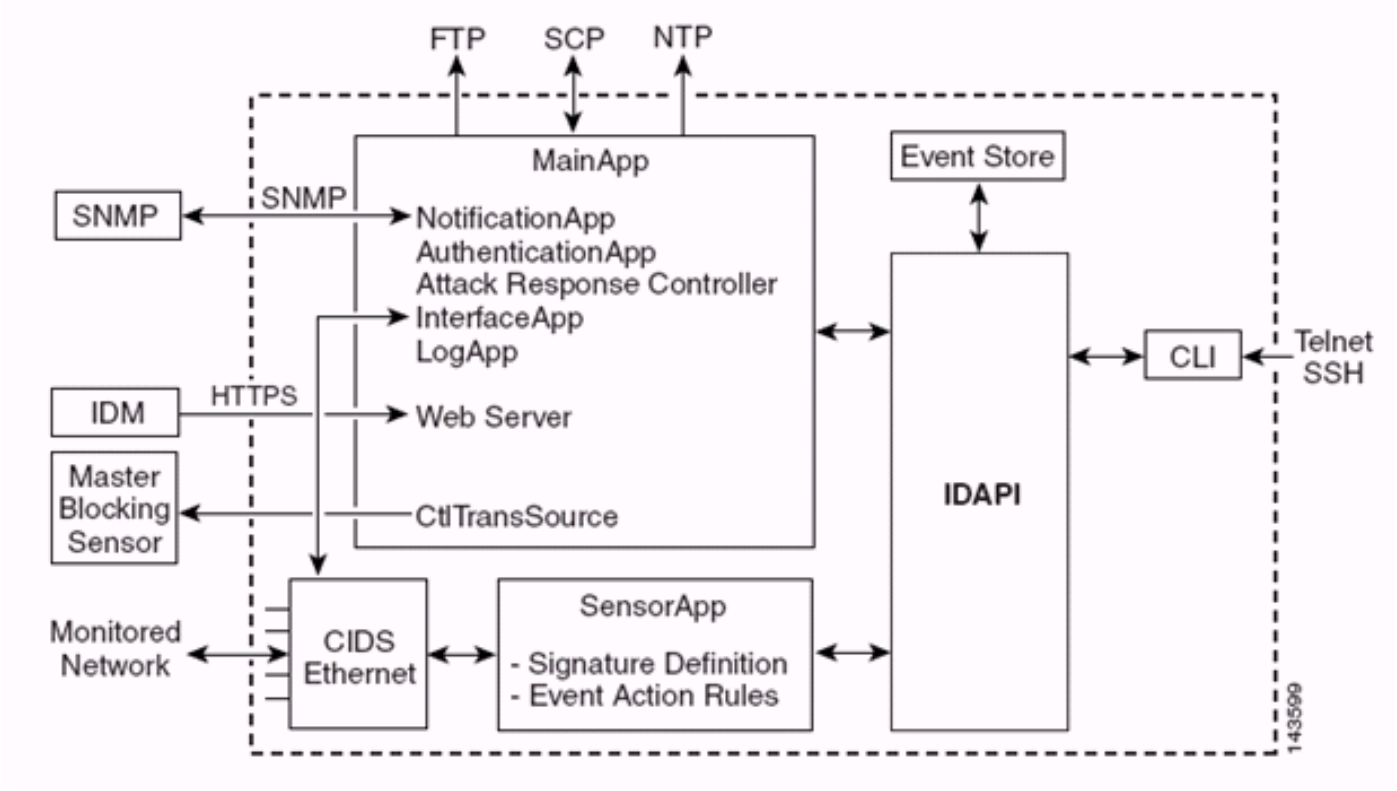
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Panoramica di Cisco IDS

I componenti principali di Cisco IDS (versione 5.0) sono:

- **Applicazione sensore**: consente di acquisire e analizzare i pacchetti.
- **Modulo Event Storage Management and Actions**: fornisce lo storage delle violazioni delle regole.
- **Imaging, Install and Startup Module**: carica, inizializza e avvia tutto il software di sistema.
- **User Interfaces and UI Support Module**: fornisce una CLI incorporata e IDM.
- **Sistema operativo sensore**: sistema operativo host (basato su Linux).



L'applicazione sensore (software IPS) è costituita da:

- **Applicazione principale**: inizializza il sistema, avvia e arresta altre applicazioni, configura il sistema operativo ed è responsabile degli aggiornamenti. Contiene i seguenti componenti:**Control Transaction Server**: consente ai sensori di inviare transazioni di controllo utilizzate per abilitare la funzionalità Master Blocking Sensor di Attack Response Controller (precedentemente nota come Controller di accesso alla rete).**Event Store**: archivio indicizzato utilizzato per memorizzare gli eventi IPS (errori, messaggi di stato e di sistema di allarme) accessibile tramite CLI, IDM, Adaptive Security Device Manager (ASDM) o Remote Data Exchange Protocol (RDEP).
- **Applicazione interfaccia (Interface App**) - Gestisce le impostazioni di bypass e fisiche e definisce le interfacce accoppiate. Le impostazioni fisiche sono costituite dallo stato di velocità, duplex e amministrativo.
- **Log App**: scrive i messaggi di log dell'applicazione nel file di log e i messaggi di errore nell'archivio eventi.
- **Attack Response Controller (ARC) (noto in precedenza come Network Access Controller)**: gestisce dispositivi di rete remoti (firewall, router e switch) per fornire funzionalità di blocco quando si verifica un evento di avviso. ARC crea e applica elenchi di controllo di accesso (ACL) sul dispositivo di rete controllato o utilizza il comando **shun** (firewall).
- **Notification App**: invia trap SNMP quando vengono attivate da un evento di avviso, stato ed errore. A tale scopo, l'app di notifica utilizza un agente SNMP di dominio pubblico. I comandi GET di SNMP forniscono informazioni sullo stato di un sensore.**Server Web (server HTTP**

RDEP2): fornisce un'interfaccia utente Web. Consente inoltre di comunicare con altri dispositivi IPS tramite RDEP2 utilizzando diversi servlet per fornire servizi IPS.**Authentication App**: verifica che gli utenti siano autorizzati a eseguire azioni CLI, IDM, ASDM o RDEP.
- **Applicazione sensore (motore di analisi)**: acquisisce e analizza i pacchetti.
- **CLI**: l'interfaccia eseguita quando gli utenti riescono ad accedere al sensore tramite Telnet o SSH. Tutti gli account creati tramite la CLI utilizzano la CLI come shell (ad eccezione dell'account del servizio - è consentito un solo account del servizio). I comandi CLI consentiti dipendono dai privilegi dell'utente.

Tutte le applicazioni IPS comunicano tra loro tramite una API (Application Program Interface) comune denominata IDAPI. Le applicazioni remote (altri sensori, applicazioni di gestione e software di terze parti) comunicano con i sensori tramite i protocolli RDEP2 e Security Device Event Exchange (SDEE).

Si noti che il sensore dispone delle seguenti partizioni del disco:

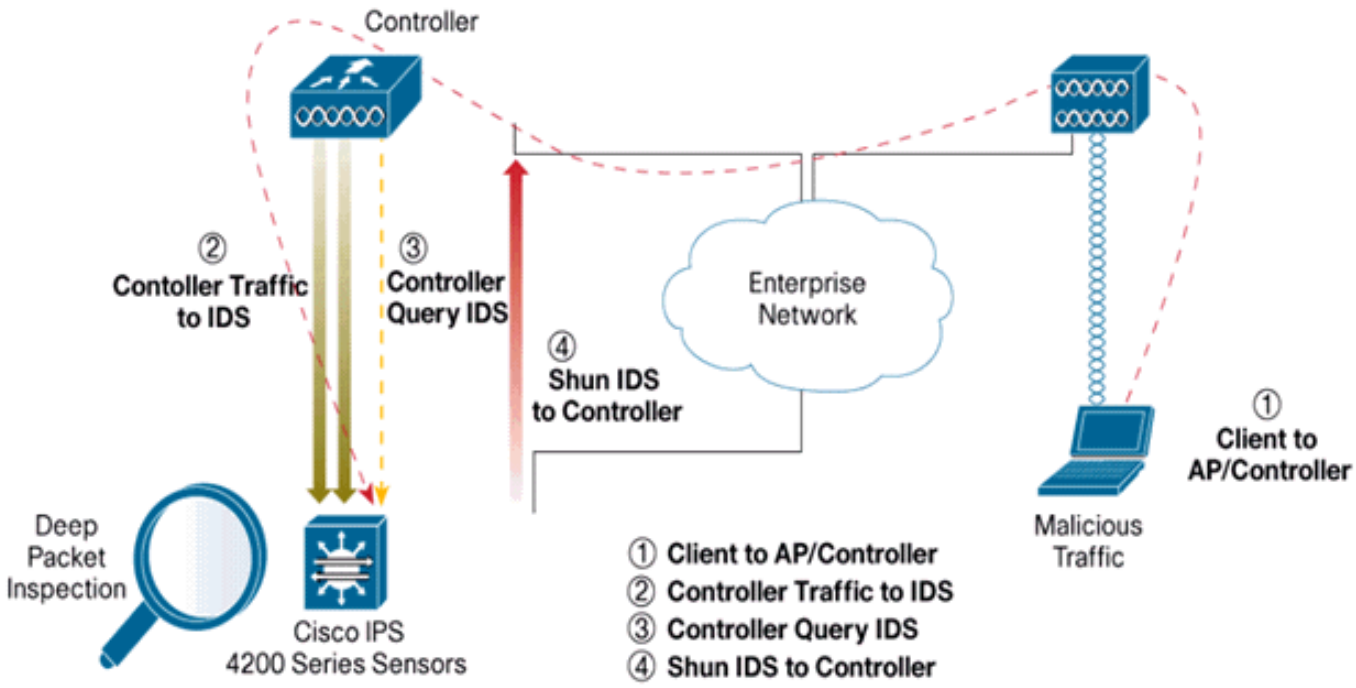
- **Partizione applicazioni**: contiene l'immagine completa del sistema IPS.
- **Partizione di manutenzione**: un'immagine IPS per scopi speciali utilizzata per ricreare l'immagine della partizione applicativa di IDSM-2. Una nuova immagine della partizione di manutenzione comporta la perdita delle impostazioni di configurazione.
- **Partizione di ripristino**: immagine speciale utilizzata per il ripristino del sensore. L'avvio nella partizione di ripristino consente agli utenti di ricreare completamente l'immagine della partizione applicativa. Le impostazioni di rete vengono mantenute, ma tutte le altre configurazioni vengono perse.

Cisco IDS e WLC - panoramica sull'integrazione

La versione 5.0 di Cisco IDS introduce la capacità di configurare le azioni di negazione quando vengono rilevate violazioni dei criteri (firme). In base alla configurazione utente sul sistema IDS/IPS, è possibile inviare una richiesta shun a un firewall, un router o un WLC per bloccare i pacchetti da un particolare indirizzo IP.

Con il software Cisco Unified Wireless Network versione 4.0 per i controller wireless Cisco, è necessario inviare una richiesta shun a un WLC per attivare il comportamento di esclusione o blacklist del client disponibile su un controller. L'interfaccia usata dal controller per ottenere la richiesta shun è l'interfaccia di comando e controllo su Cisco IDS.

- Il controller consente di configurare fino a cinque sensori IDS su un determinato controller.
- Ogni sensore IDS configurato viene identificato dal relativo indirizzo IP o nome di rete qualificato e dalle credenziali di autorizzazione.
- Ogni sensore IDS può essere configurato su un controller con una frequenza di query univoca in secondi.



Shun IDS

Il controller esegue una query sul sensore alla frequenza di query configurata per recuperare tutti gli eventi shun. Una determinata richiesta shun viene distribuita in tutto il gruppo di mobilità del controller che recupera la richiesta dal sensore IDS. Ogni richiesta di shun per un indirizzo IP client è attiva per il valore di timeout dei secondi specificato. Se il valore di timeout indica un tempo infinito, l'evento shun termina solo se la voce shun viene rimossa dall'IDS. Lo stato del client ignorato viene mantenuto su ogni controller nel gruppo di mobilità anche se uno o tutti i controller vengono reimpostati.

Nota: la decisione di evitare un client viene sempre presa dal sensore IDS. Il controller non rileva attacchi di livello 3. È un processo molto più complesso determinare che il client sta lanciando un attacco dannoso al layer 3. Il client viene autenticato al layer 2, che è sufficiente al controller per concedere l'accesso al layer 2.

Nota: ad esempio, se a un client viene assegnato un indirizzo IP che causa un errore precedente (non utilizzato), è possibile sbloccare l'accesso di layer 2 per questo nuovo client solo dopo il timeout del sensore. Anche se il controller consente l'accesso al layer 2, il traffico del client potrebbe comunque essere bloccato sui router del layer 3, perché il sensore informa anche i router dell'evento shun.

Si supponga che un client abbia l'indirizzo IP A. Ora, quando il controller esegue il polling dell'IDS per individuare gli eventi shun, l'IDS invia la richiesta shun al controller con l'indirizzo IP A come indirizzo IP di destinazione. Ora, il controller nero elenca questo client A. Sul controller, i client sono disabilitati in base a un indirizzo MAC.

Si supponga ora che il client cambi il proprio indirizzo IP da A a B. Durante il polling successivo, il controller ottiene un elenco di client esclusi in base all'indirizzo IP. Anche in questo caso, l'indirizzo IP A è ancora nell'elenco degli indirizzi non utilizzati. Tuttavia, poiché il client ha modificato il proprio indirizzo IP da A a B (che non è incluso nell'elenco degli indirizzi IP esclusi), questo client con un nuovo indirizzo IP di B viene rilasciato una volta raggiunto il timeout dei client in lista nera sul controller. A questo punto, il controller inizia a consentire al client di utilizzare il

nuovo indirizzo IP di B (ma l'indirizzo MAC del client rimane lo stesso).

Pertanto, anche se un client rimane disabilitato per la durata del tempo di esclusione del controller e viene riescluso se acquisisce nuovamente l'indirizzo DHCP precedente, tale client non viene più disabilitato se l'indirizzo IP del client ignorato viene modificato. Ad esempio, se il client si connette alla stessa rete e il timeout del lease DHCP non è scaduto.

I controller supportano solo la connessione all'IDS per le richieste di shun client che utilizzano la porta di gestione del controller. Il controller si connette all'IDS per l'ispezione dei pacchetti tramite le interfacce VLAN applicabili che trasportano il traffico client wireless.

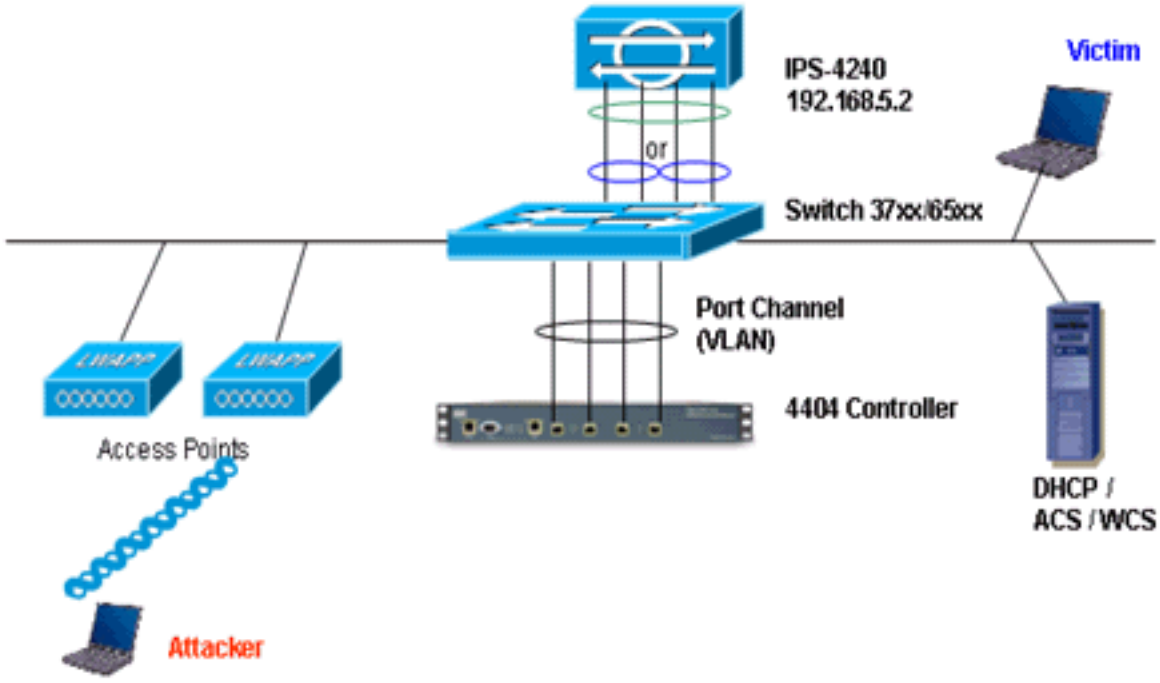
Sul controller, la pagina Disabilita client mostra ciascun client che è stato disabilitato tramite una richiesta del sensore IDS. Il comando **show** della CLI visualizza anche una lista nera dei client.

In Sistema colori Windows i client esclusi vengono visualizzati nella scheda secondaria Protezione.

Di seguito viene riportata la procedura per completare l'integrazione dei sensori Cisco IPS e dei WLC di Cisco.

1. Installare e collegare l'accessorio IDS sullo stesso switch su cui risiede il controller wireless.
2. Eseguire il mirroring (SPAN) delle porte WLC che trasportano il traffico client wireless all'accessorio IDS.
3. L'appliance IDS riceve una copia di ogni pacchetto e controlla il traffico dal layer 3 al layer 7.
4. L'accessorio IDS offre un file di firma scaricabile che può anche essere personalizzato.
5. L'accessorio IDS genera un allarme con un'azione evento shun quando viene rilevata una firma di attacco.
6. Il WLC analizza l'IDS per rilevare eventuali allarmi.
7. Quando viene rilevato un allarme con l'indirizzo IP di un client wireless associato al WLC, il client viene inserito nell'elenco di esclusione.
8. Il WLC genera una trap e il WCS ne riceve notifica.
9. L'utente viene rimosso dall'elenco di esclusione dopo il periodo di tempo specificato.

Progettazione dell'architettura di rete



Il Cisco WLC è collegato alle interfacce gigabit del Catalyst 6500. Creare un canale di porta per le interfacce Gigabit e abilitare il protocollo LAG (Link Aggregation) sul 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
```

Il controller è collegato all'interfaccia gigabit 5/1 e gigabit 5/2 sullo switch 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
```

Le interfacce di rilevamento del sensore IPS possono funzionare singolarmente in **modalità promiscua** oppure è possibile accoppiarle per creare interfacce in linea per la **modalità di rilevamento in linea**.

In modalità promiscua, i pacchetti non passano attraverso il sensore. Il sensore analizza una copia del traffico monitorato anziché il pacchetto inoltrato. Il vantaggio di operare in modalità promiscua è che il sensore non influisce sul flusso del pacchetto con il traffico inoltrato.

Nota: il diagramma dell'architettura è solo un esempio di configurazione dell'architettura integrata WLC e IPS. L'esempio di configurazione qui mostrato spiega l'interfaccia di rilevamento IDS che agisce in modalità promiscua. Il diagramma dell'architettura mostra le interfacce di rilevamento accoppiate per funzionare in modalità Inline Pair. Per ulteriori informazioni sulla modalità interfaccia in linea, fare riferimento a Modalità in linea.

In questa configurazione, si presume che l'interfaccia di rilevamento agisca in modalità promiscua. L'interfaccia di monitoraggio del sensore Cisco IDS è collegata all'interfaccia 5/3 Gigabit del Catalyst 6500. Creare una sessione di monitoraggio sullo switch Catalyst 6500 quando l'interfaccia del canale della porta è l'origine dei pacchetti e la destinazione è l'interfaccia Gigabit a cui è connessa l'interfaccia di monitoraggio del sensore Cisco IPS. In questo modo tutto il traffico in entrata e in uscita dalle interfacce cablate del controller viene replicato negli IDS per l'ispezione di layer 3-7.

```
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#
```

Configurazione del sensore Cisco IDS

La configurazione iniziale del sensore Cisco IDS viene effettuata dalla porta della console o

collegando un monitor e una tastiera al sensore.

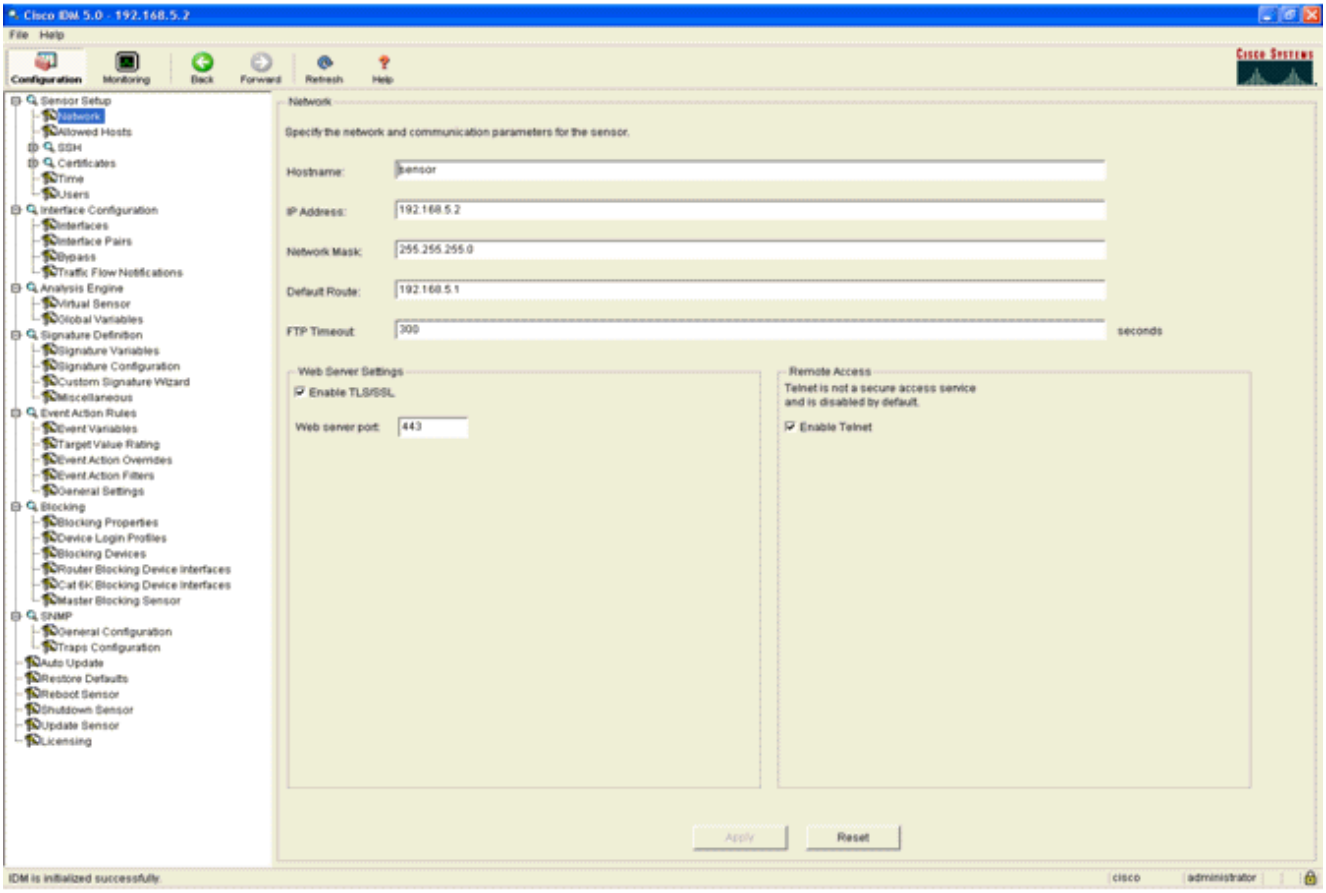
1. Accedere all'accessorio:Collegare una porta console al sensore.Collegare un monitor e una tastiera al sensore.
2. Digitare il nome utente e la password al prompt di accesso.**Nota:** il nome utente e la password predefiniti sono entrambi cisco. Al primo accesso all'accessorio verrà richiesto di modificarli. È necessario prima immettere la password UNIX, ovvero cisco. Immettere quindi la nuova password due volte.

```
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.
```

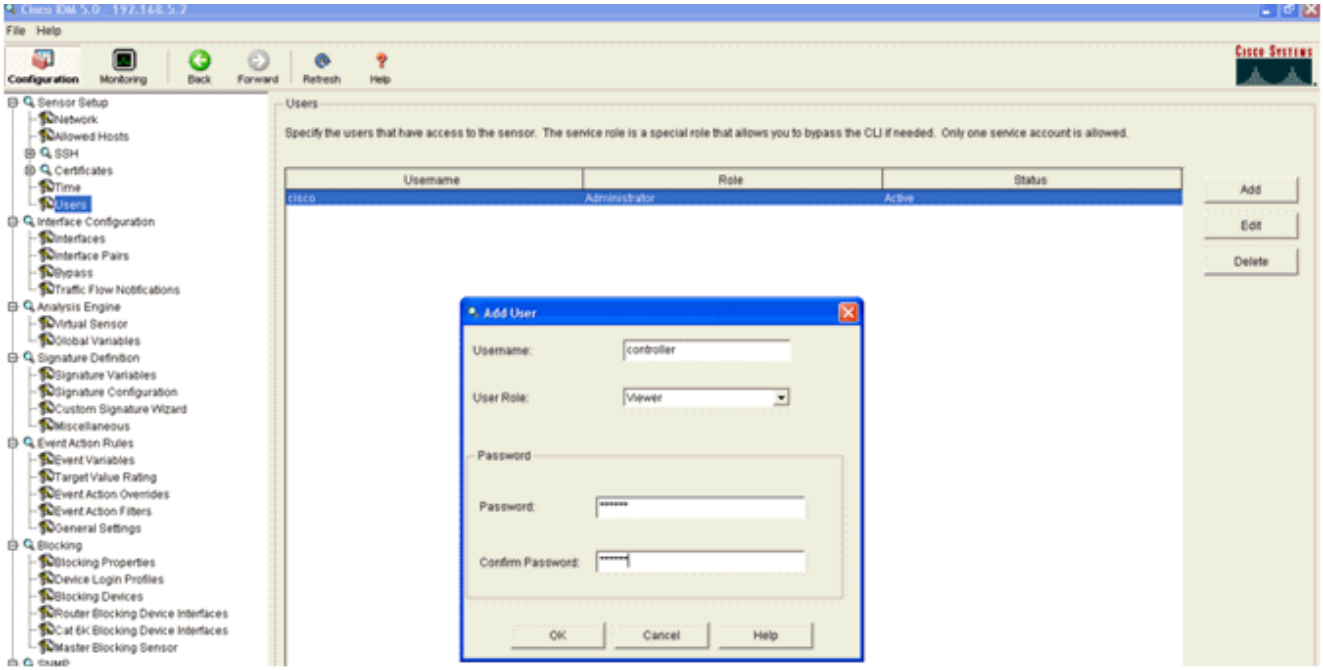
3. Configurare l'indirizzo IP, la subnet mask e l'elenco degli accessi sul sensore.**Nota:** questa è l'interfaccia di comando e controllo sull'IDS utilizzata per comunicare con il controller. Questo indirizzo deve poter essere indirizzato all'interfaccia di gestione del controller. Le interfacce di rilevamento non richiedono indirizzamento. L'elenco degli accessi deve includere l'indirizzo dell'interfaccia di gestione del controller e gli indirizzi consentiti per la gestione dell'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#
```

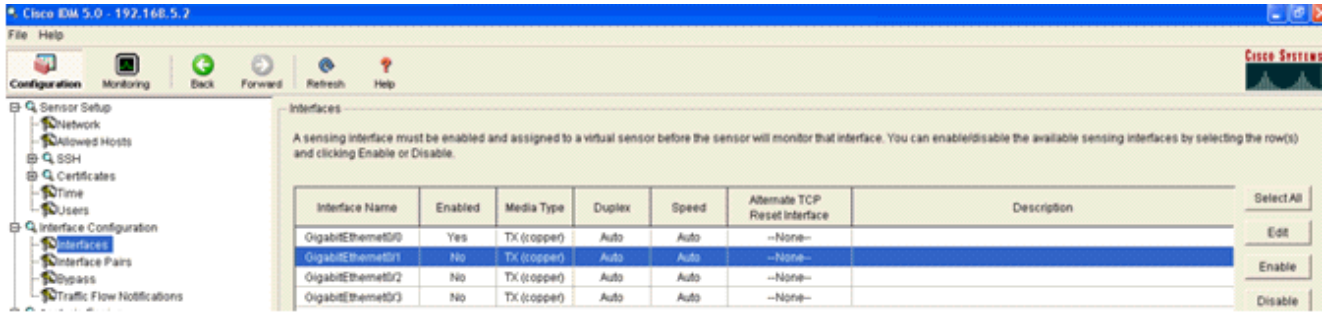
4. Èquindi possibile configurare il sensore IPS dalla GUI. Puntare il browser all'indirizzo IP di gestione del sensore. L'immagine mostra un esempio di sensore configurato con 192.168.5.2.



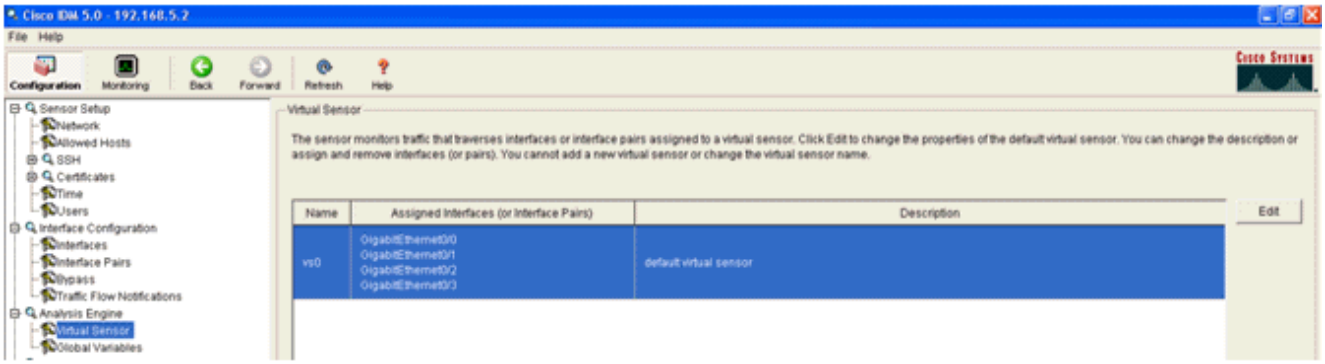
5. Aggiungere un utente usato dal WLC per accedere agli eventi del sensore IPS.



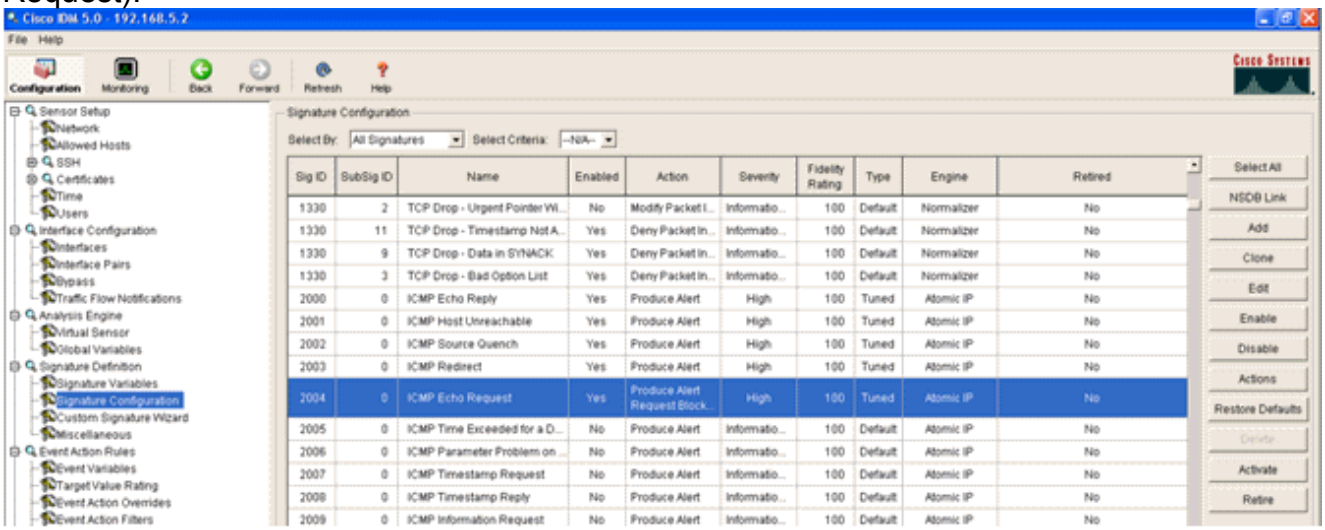
6. Abilitare le interfacce di monitoraggio.



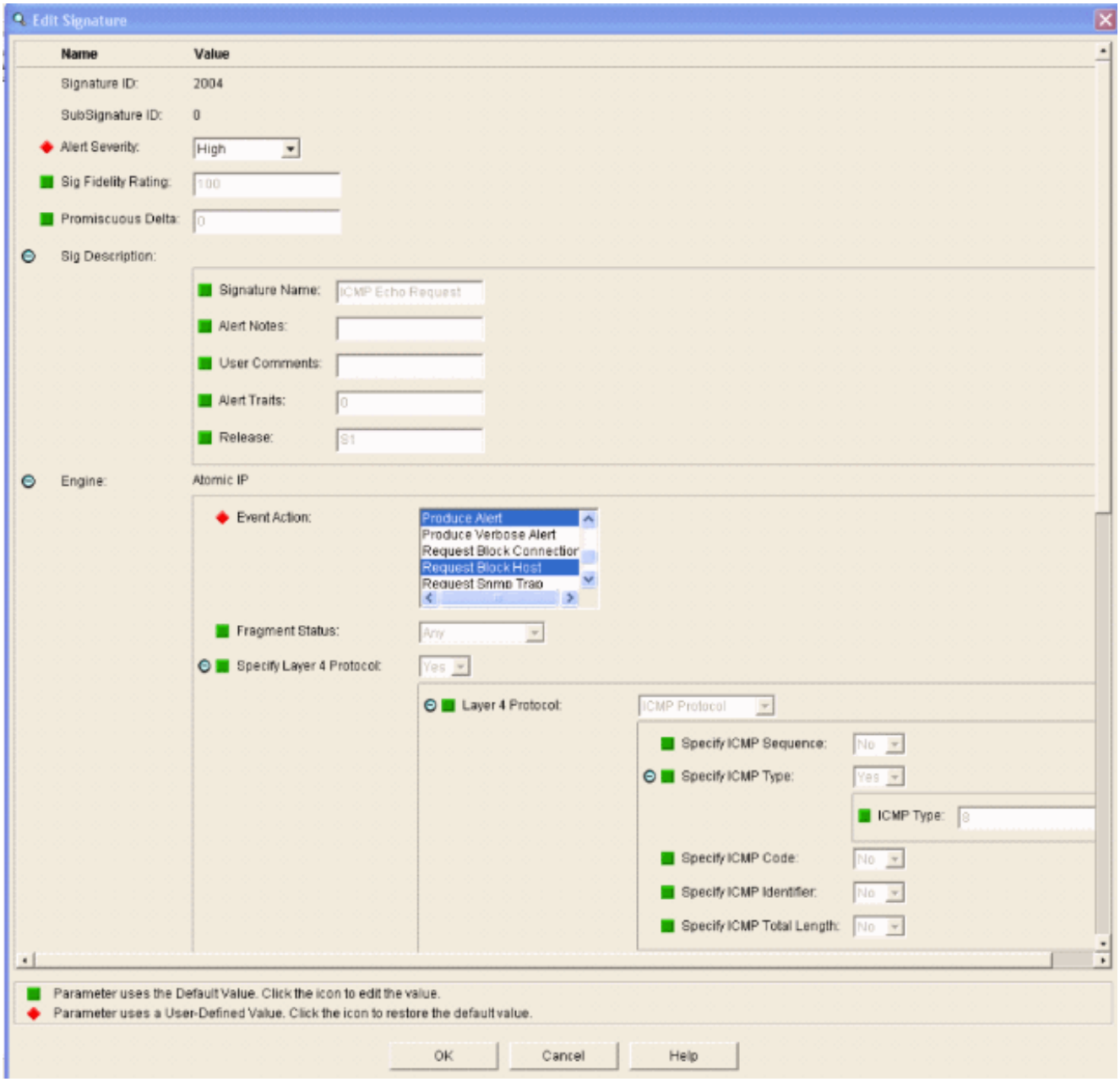
Le interfacce di monitoraggio devono essere aggiunte al motore di analisi, come mostrato in questa
finestra:



7. Per eseguire una rapida verifica della configurazione, selezionare la firma 2004 (ICMP Echo Request).



Affinché la fase di verifica venga completata, è necessario abilitare la firma, impostare la gravità dell'avviso su **Alta** e impostare l'azione evento su **Produzione host avvisi** e **host richieste di
blocco**.

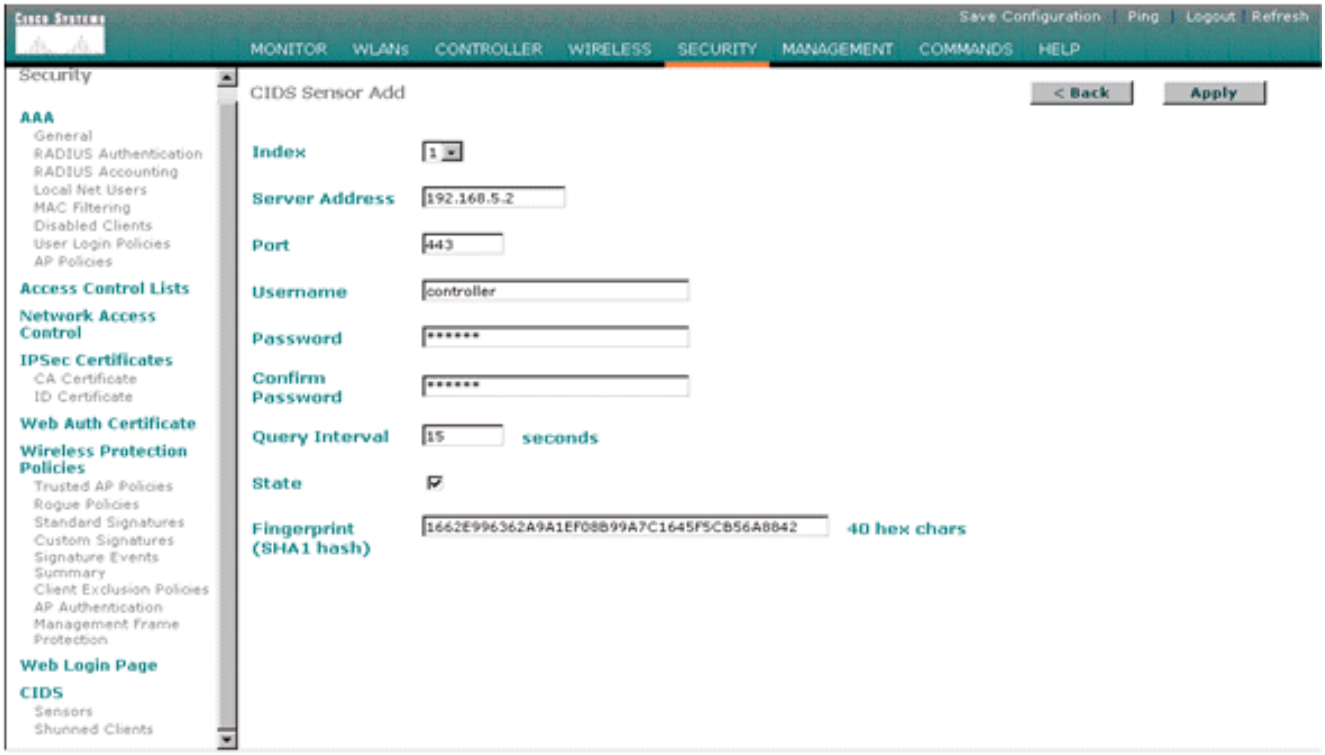


Configurare il WLC

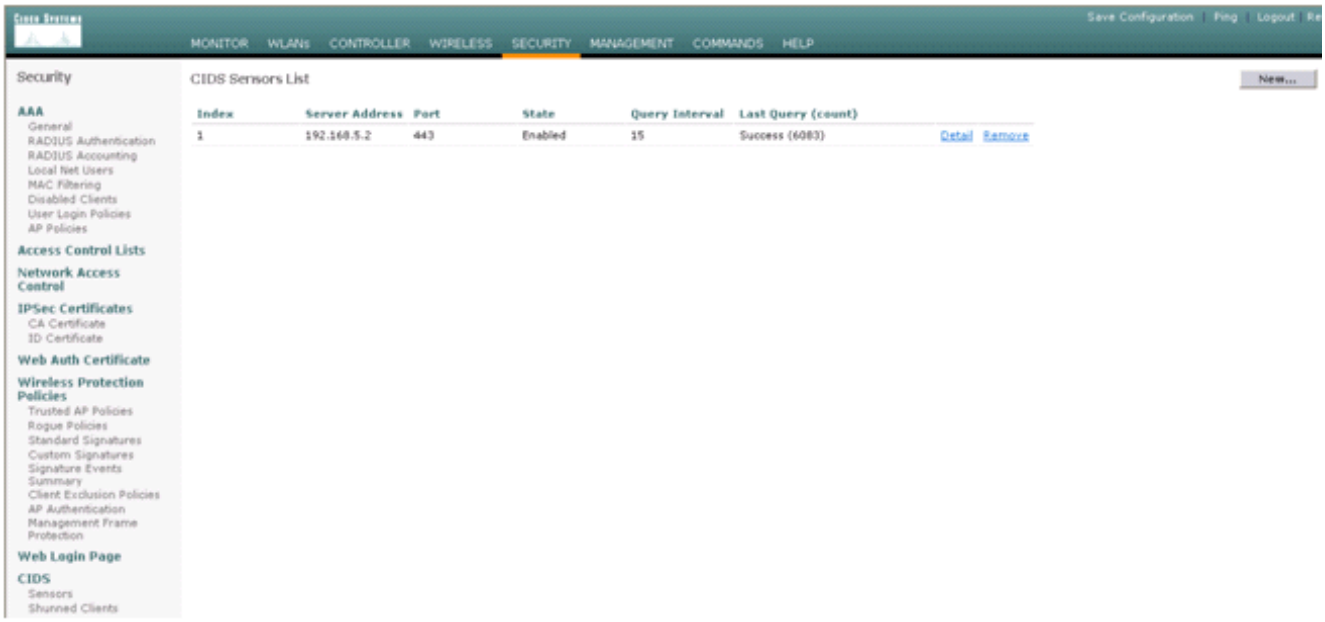
Per configurare il WLC, completare i seguenti passaggi:

1. Una volta configurato l'accessorio IPS e pronto per essere aggiunto al controller, scegliere **Sicurezza > CIDS > Sensori > Nuovo**.
2. Aggiungere l'indirizzo IP, il numero di porta TCP, il nome utente e la password creati in precedenza.Per ottenere l'impronta digitale dal sensore IPS, eseguire questo comando nel sensore IPS e aggiungere l'impronta digitale SHA1 sul WLC (senza i due punti). Utilizzato per proteggere la comunicazione di polling da controller a IDS.

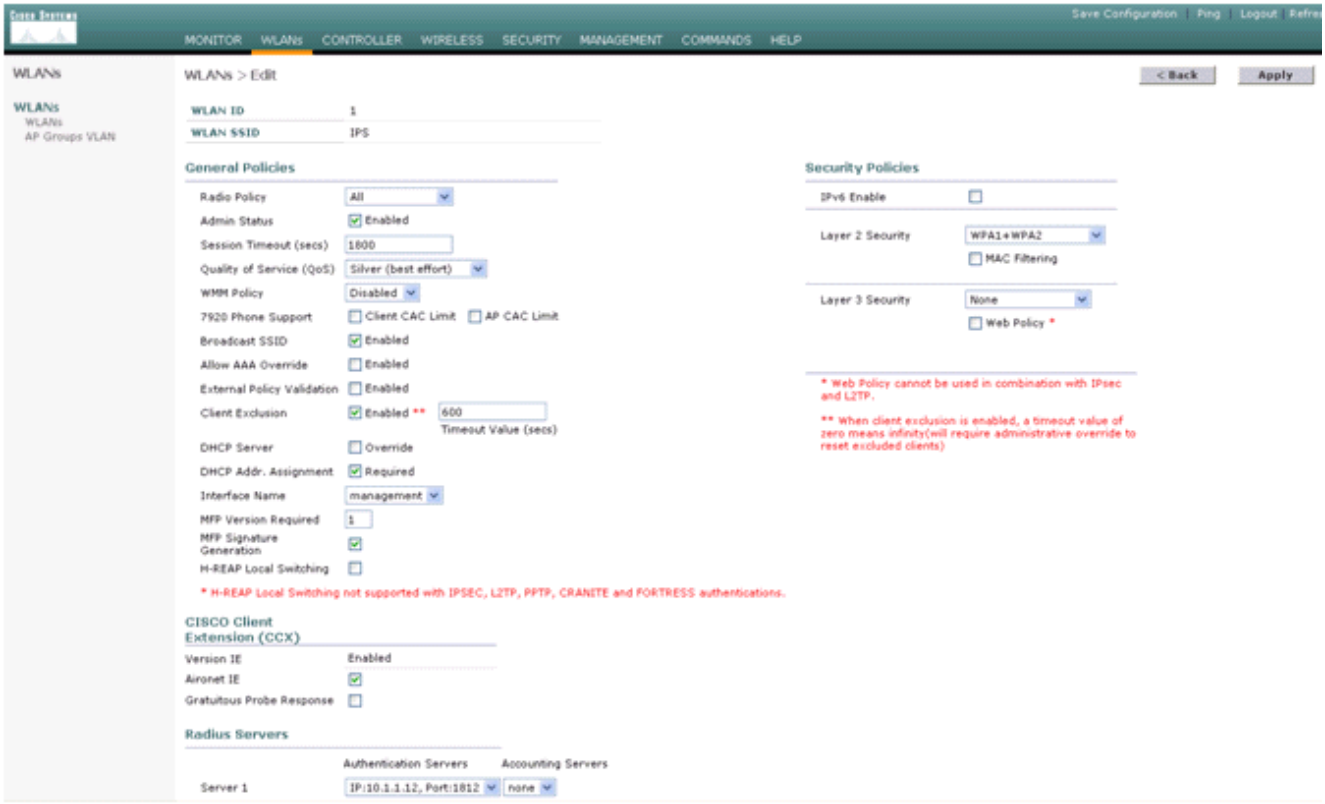
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



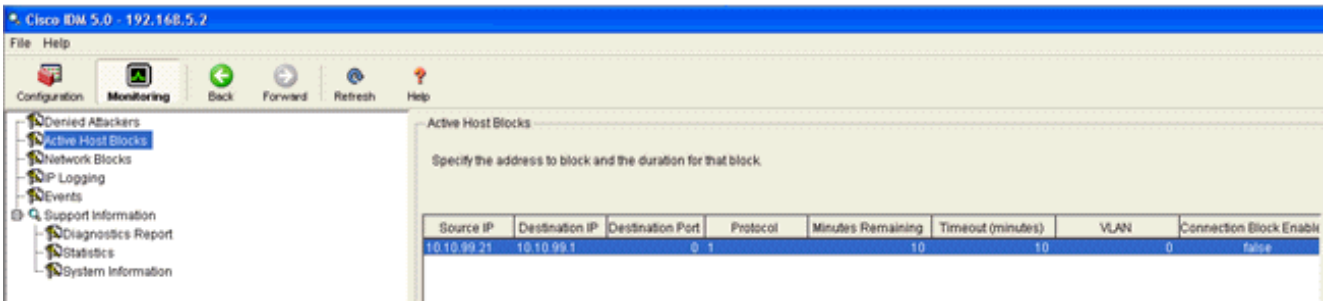
3. Controllare lo stato della connessione tra il sensore IPS e il WLC.



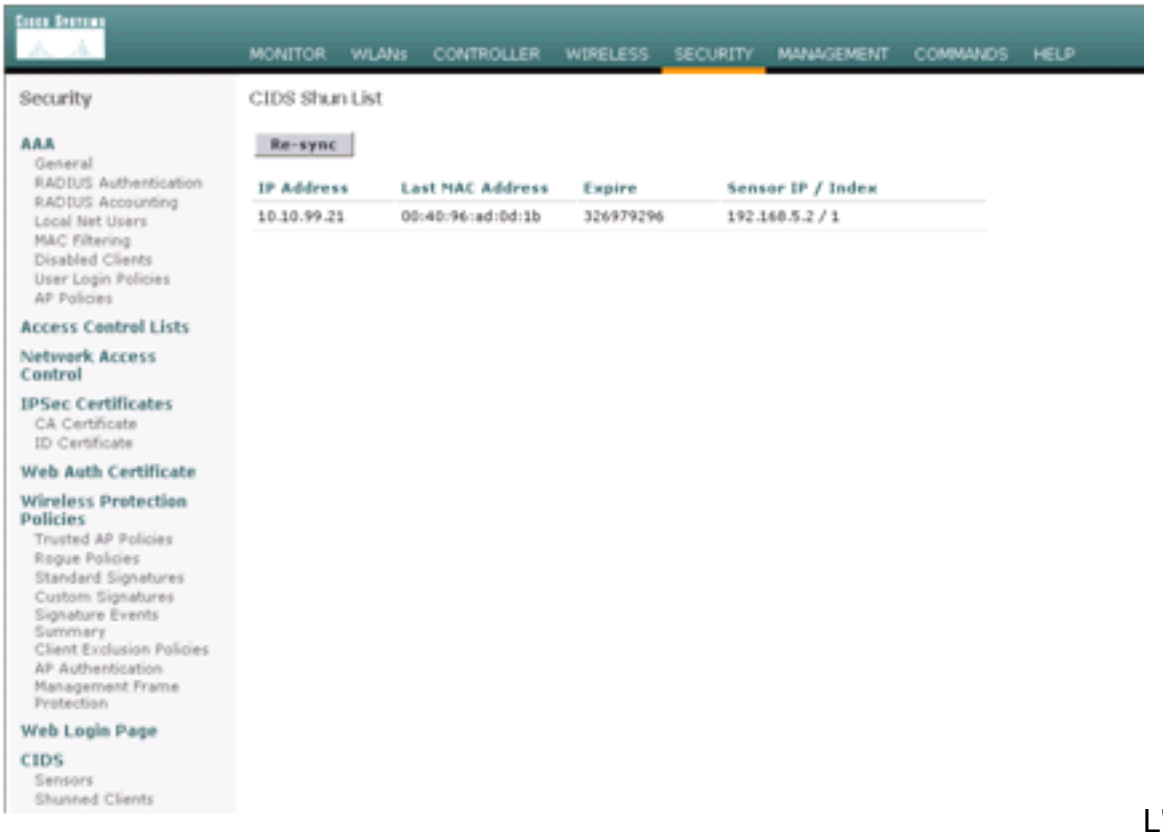
4. Una volta stabilita la connettività con il sensore Cisco IPS, verificare che la configurazione WLAN sia corretta e che sia abilitata l'**esclusione del client**.Il valore predefinito del timeout di esclusione dei client è 60 secondi. Si noti inoltre che, indipendentemente dal timer di esclusione dei client, l'esclusione dei client persiste finché il blocco client richiamato da IDS rimane attivo. Il tempo di blocco predefinito nell'IDS è 30 minuti.



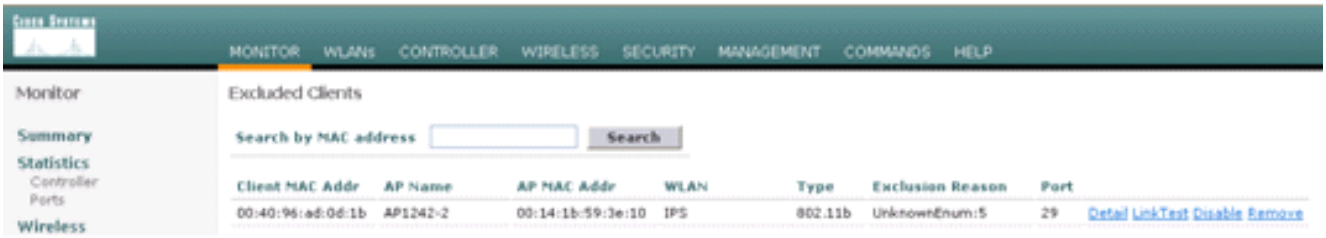
5. Èpossibile attivare un evento nel sistema Cisco IPS quando si esegue una scansione NMAP su determinati dispositivi della rete o quando si esegue un ping su alcuni host monitorati dal sensore Cisco IPS. Dopo aver attivato un allarme nell'IPS Cisco, passare a **Monitoraggio e blocchi host attivi** per verificare i dettagli sull'host.



Nell'elenco Shun Client del controller vengono ora inseriti gli indirizzi IP e MAC

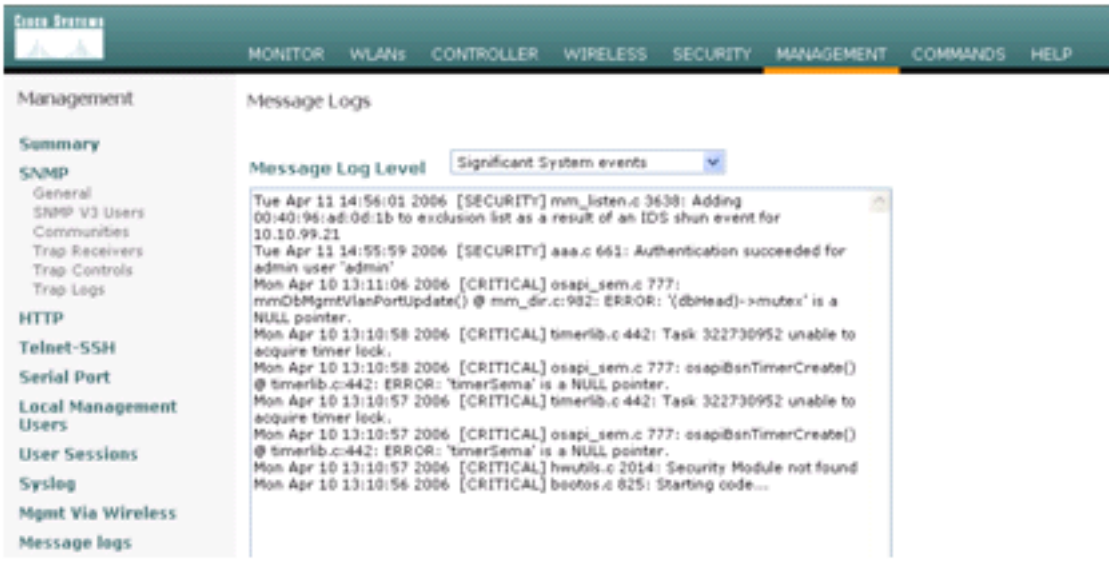


dell'host. L'ut
ente viene aggiunto all'elenco di esclusione
client.

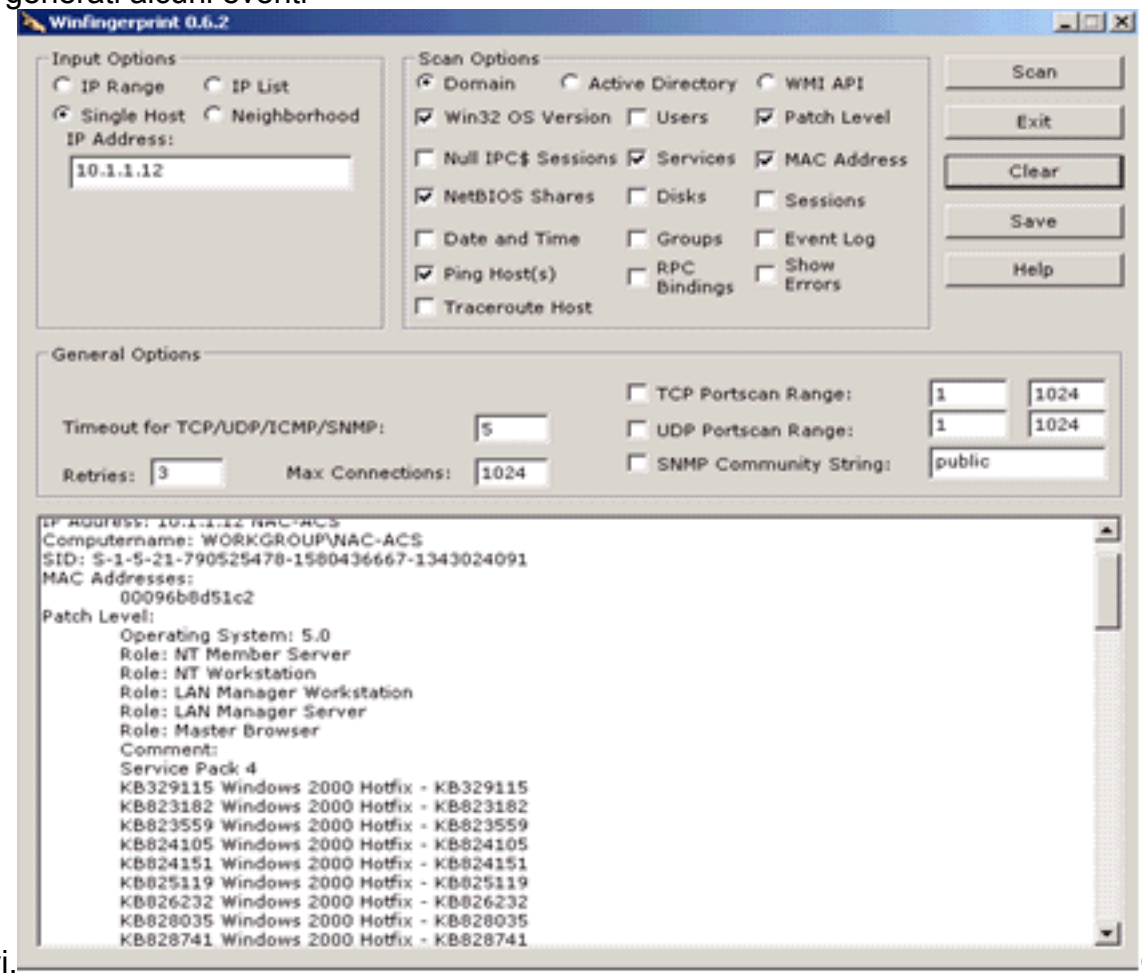


Quando un client viene aggiunto all'elenco dei file condivisi, viene generato un registro delle

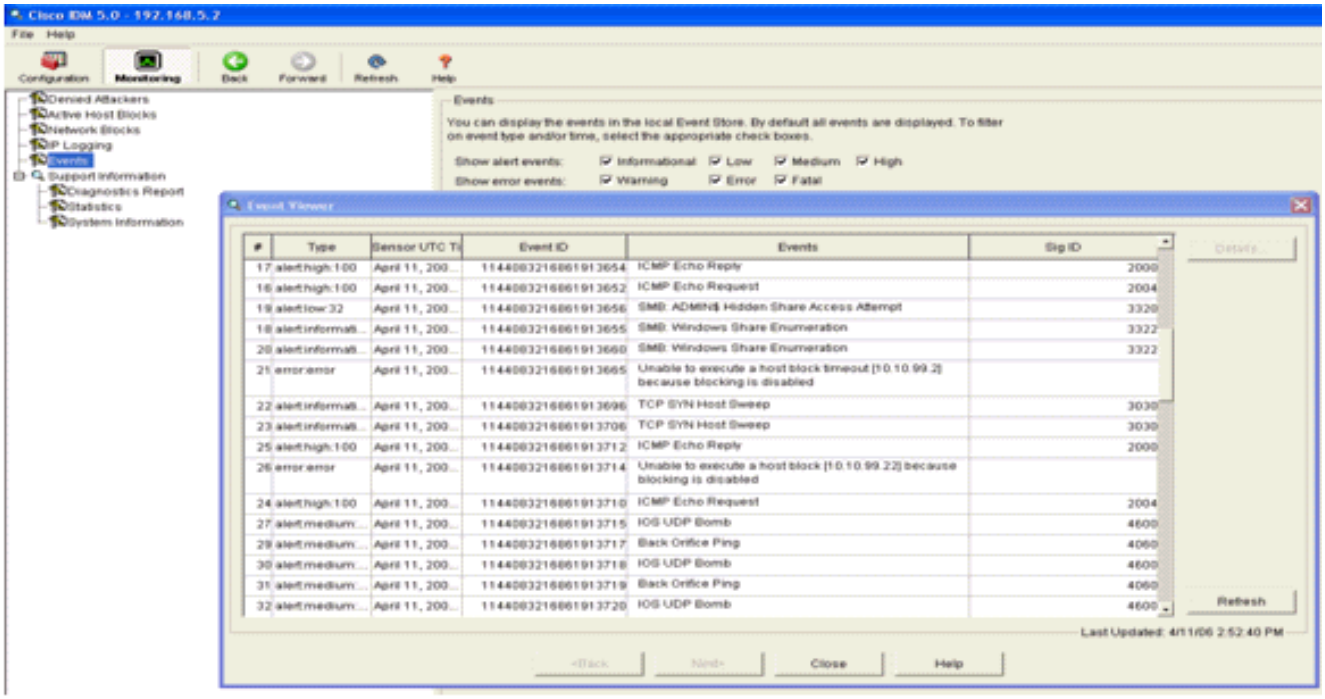
trap. Per
l'evento viene inoltre generato un registro



messaggi. Quando si esegue una scansione NMAP su un dispositivo monitorato, nel sensore Cisco IPS vengono generati alcuni eventi



aggiuntivi. Questa finestra mostra gli eventi generati nel sensore Cisco IPS.



Esempio di configurazione del sensore Cisco IDS

Questo è l'output dello script di installazione:

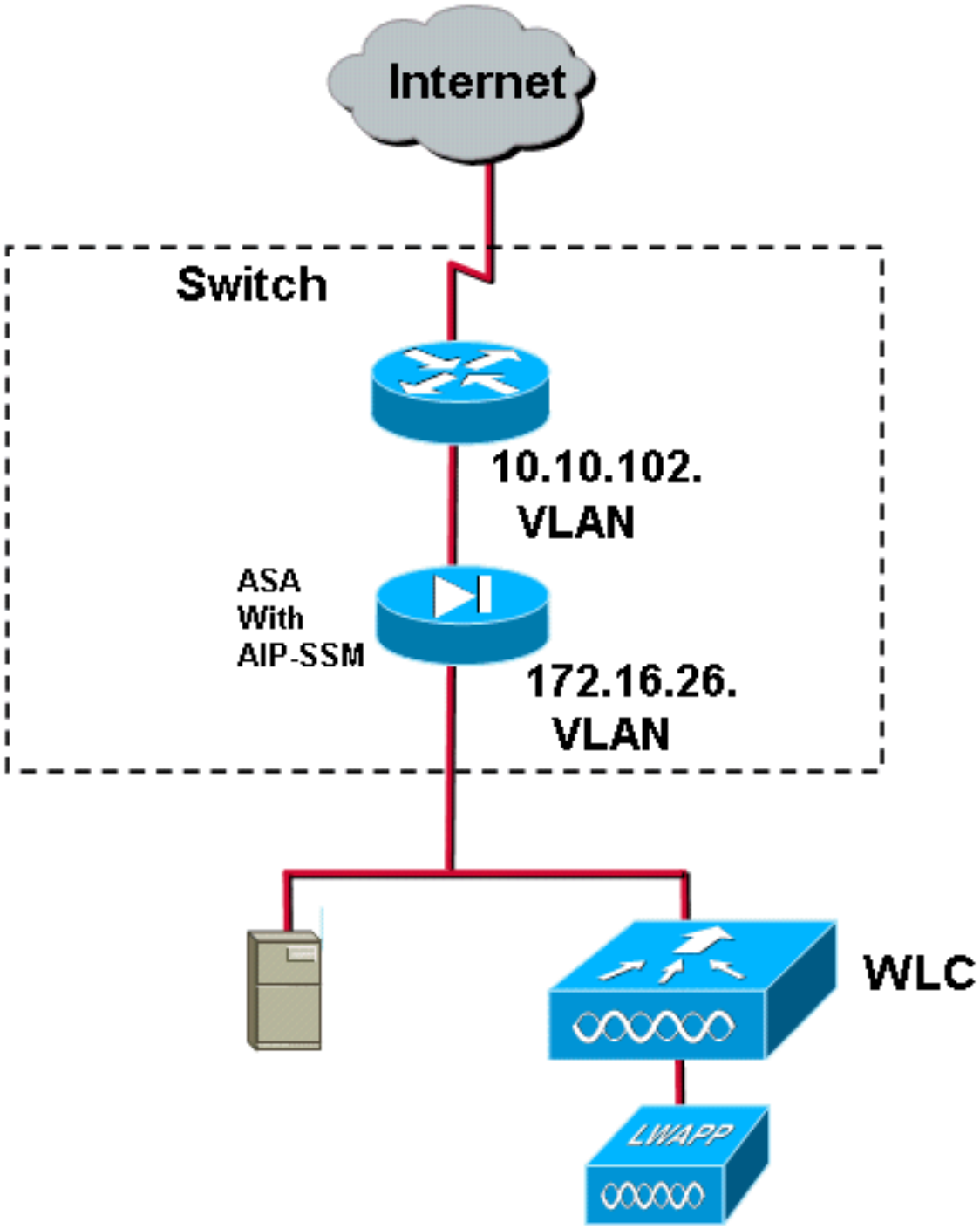
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list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

Configurazione di un'ASA per IDS

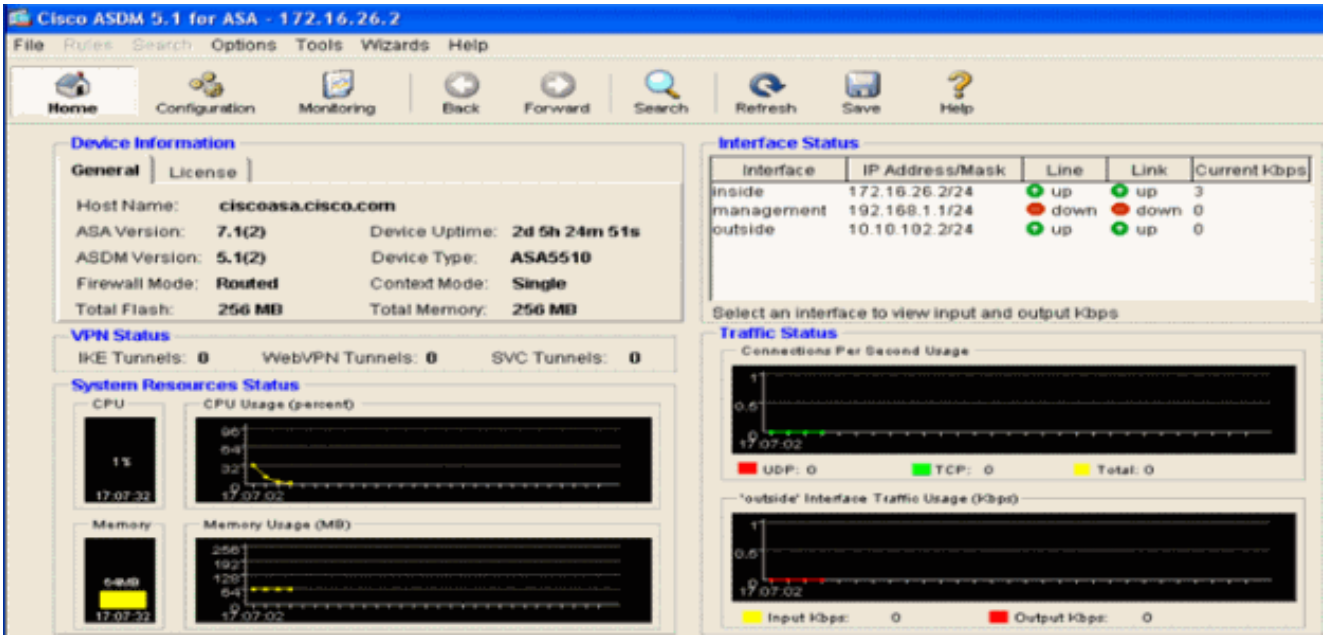
A differenza di un sensore di rilevamento delle intrusioni tradizionale, un'ASA deve sempre trovarsi nel percorso dati. In altre parole, invece di estendere il traffico da una porta dello switch a

una porta di sniffing passivo sul sensore, l'ASA deve ricevere i dati su un'interfaccia, elaborarli internamente e quindi inoltrarli su un'altra porta. Per gli IDS, usare la struttura policy modulare (MPF) per copiare il traffico che l'ASA riceve sul modulo interno dei servizi di sicurezza per l'ispezione avanzata e la prevenzione (AIP-SSM) per l'ispezione.

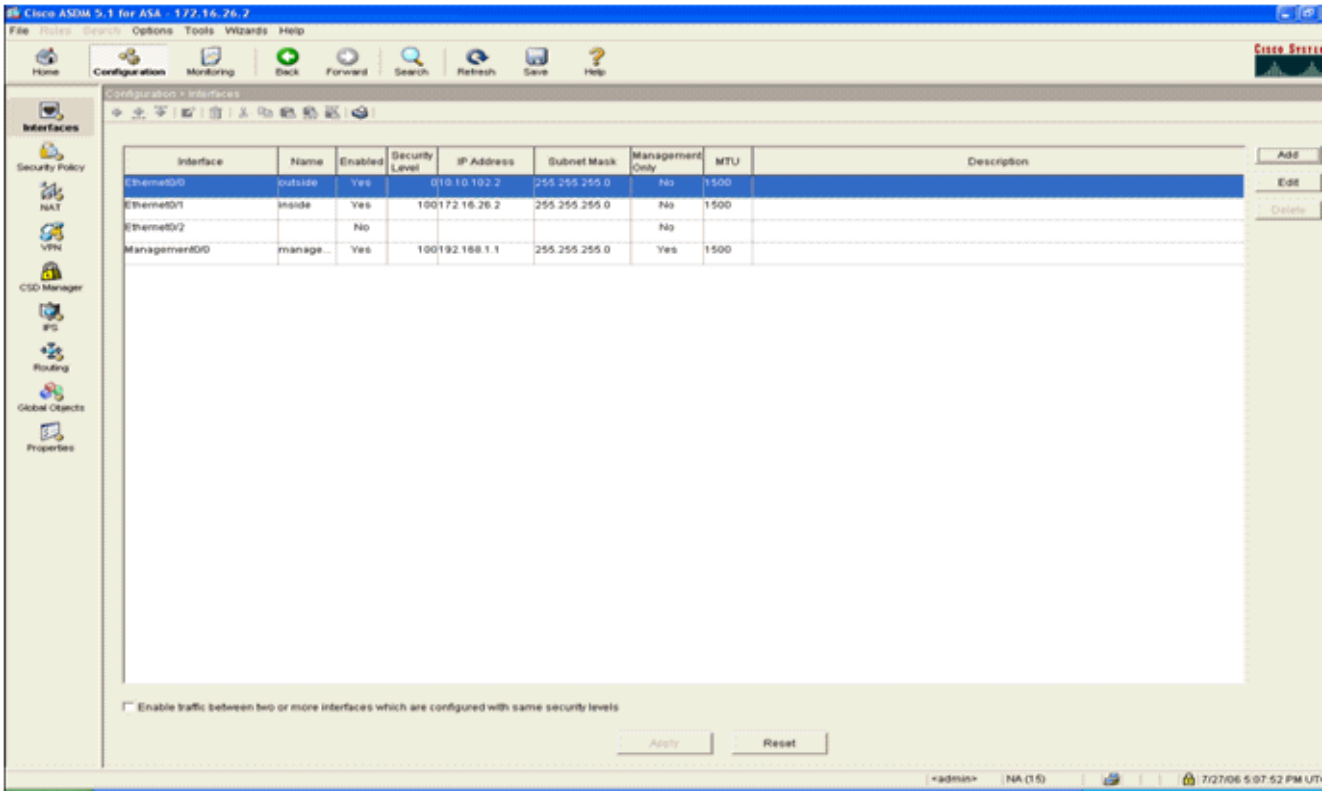


Nell'esempio, l'appliance ASA è già configurata e trasmette il traffico. In questa procedura viene illustrato come creare una regola per l'invio di dati a AIP-SSM.

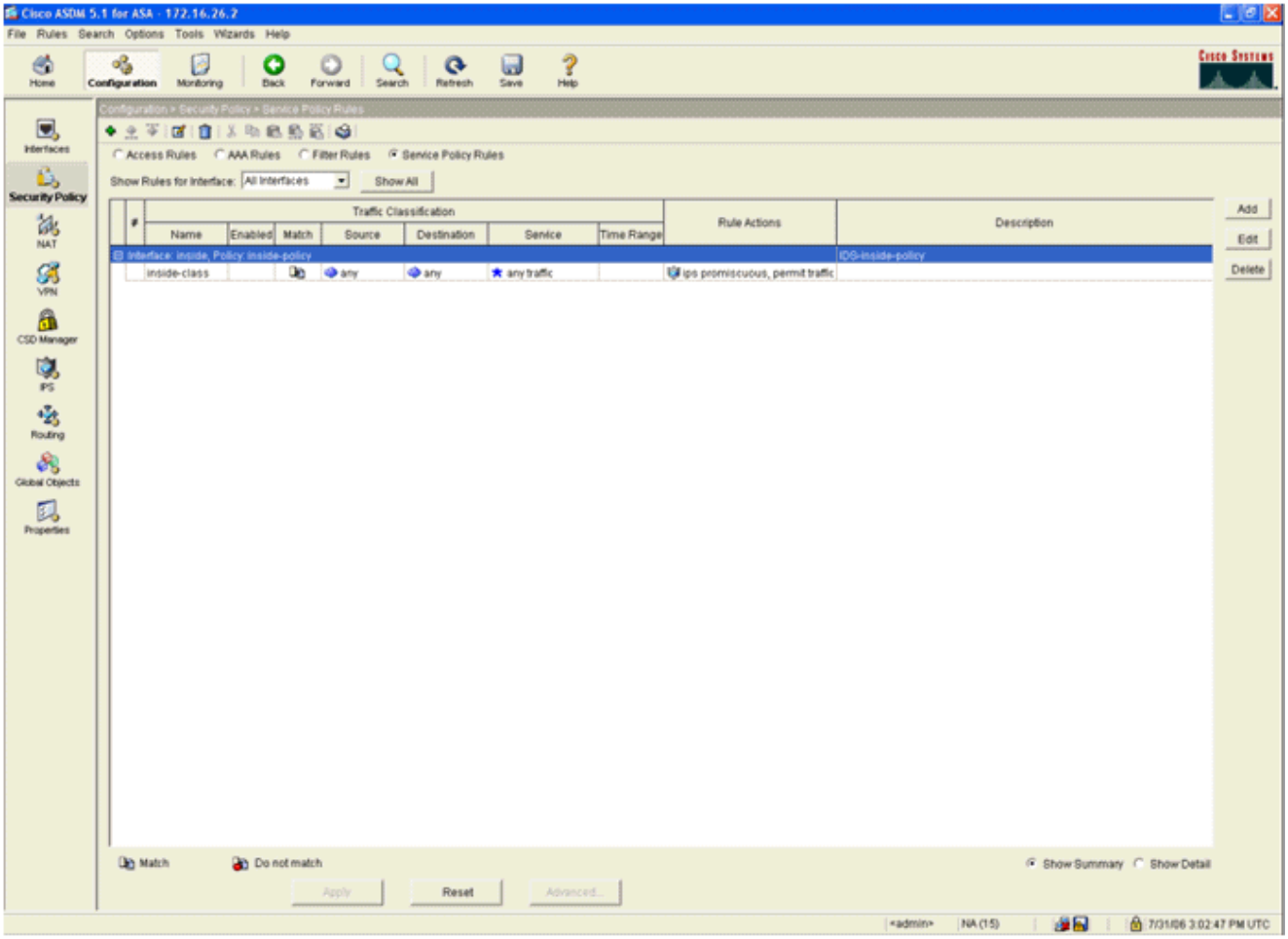
1. Accedere all'ASA utilizzando ASDM. Dopo aver eseguito correttamente l'accesso, viene visualizzata la finestra ASA Main System (Sistema principale ASA).



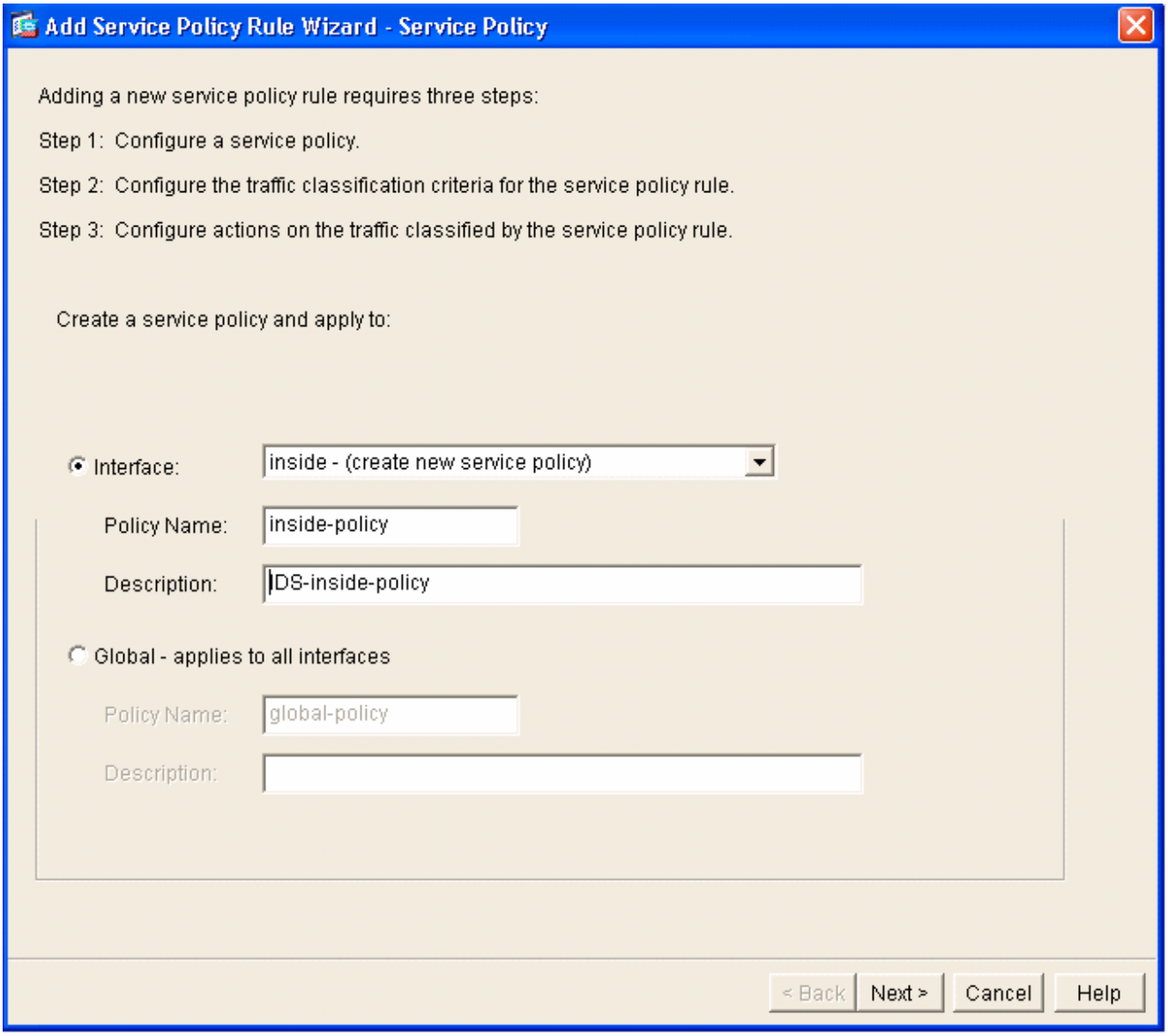
2. Fare clic su **Configuration** (Configurazione) nella parte superiore della pagina. La finestra mostra le interfacce
ASA.



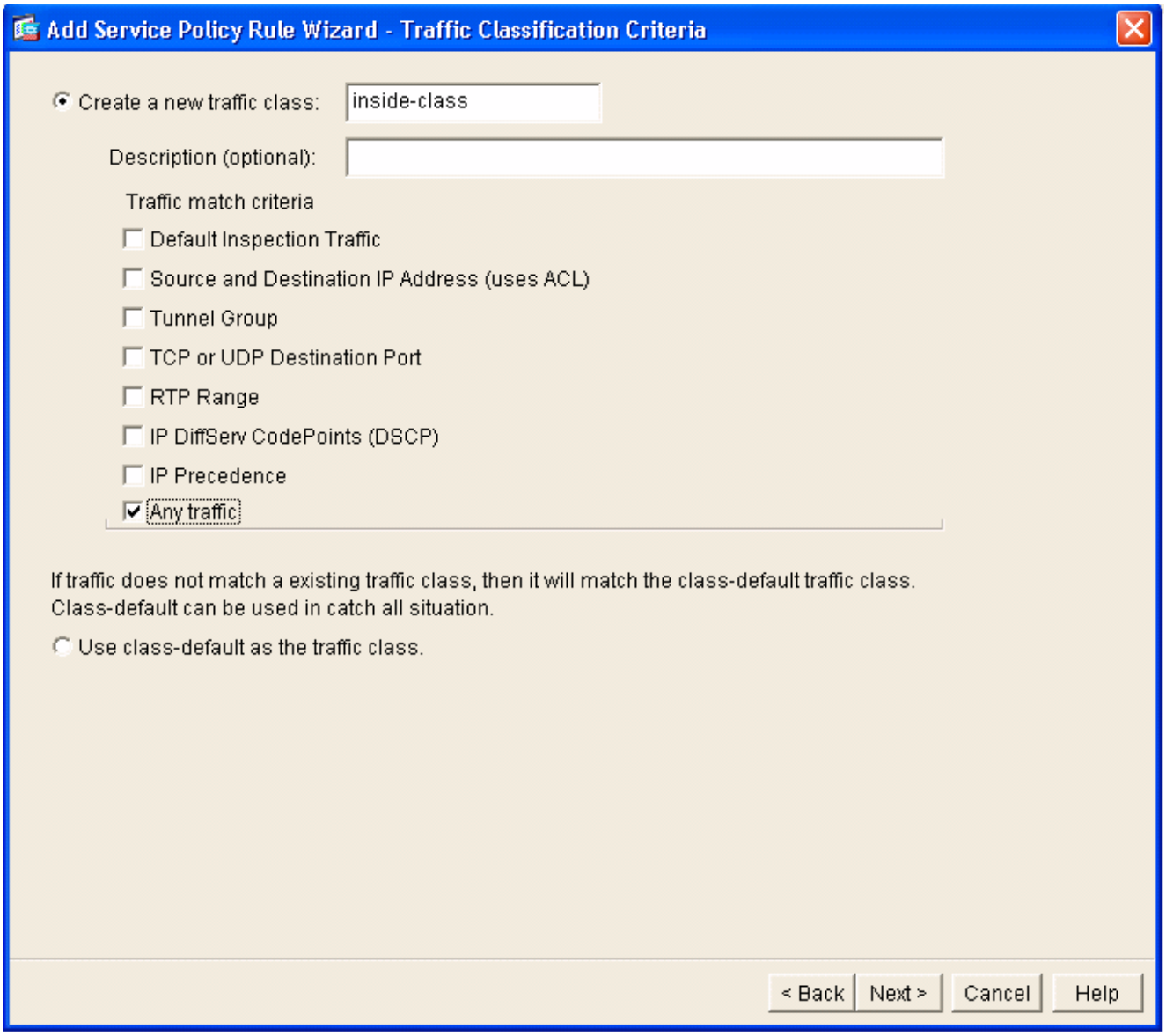
3. Fare clic su **Criteri di protezione** sul lato sinistro della finestra. Nella finestra risultante, scegliere la scheda **Regole dei criteri di servizio**.



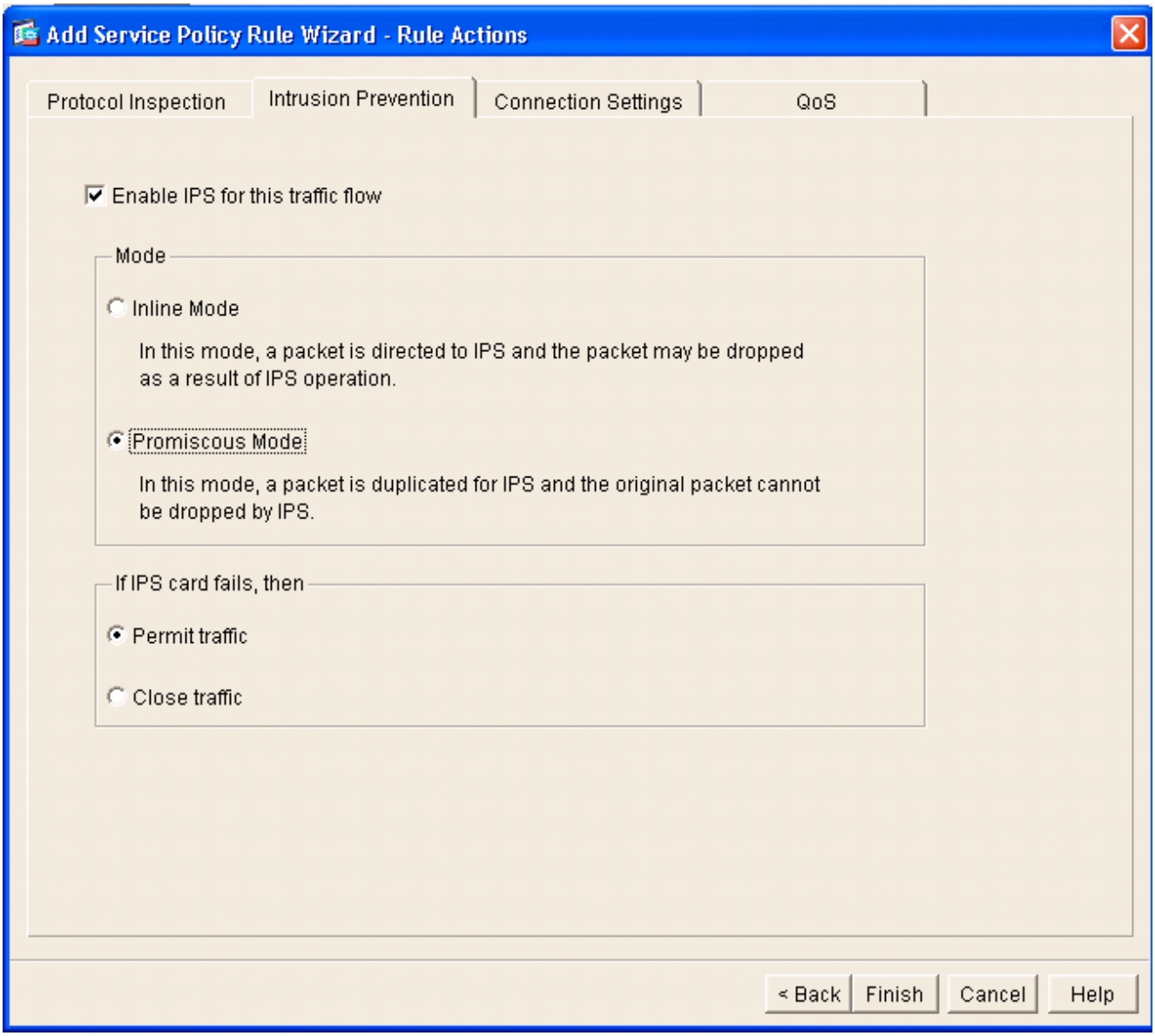
4. Per creare un nuovo criterio, fare clic su **Add** (Aggiungi). L'Aggiunta guidata regole dei criteri del servizio verrà avviata in una nuova finestra.Fare clic su **Interface** (Interfaccia), quindi selezionare l'interfaccia corretta dall'elenco a discesa per creare un nuovo criterio associato a una delle interfacce che attraversano il traffico.Assegnare al criterio un nome e una descrizione dell'operazione eseguita utilizzando le due caselle di testo.Per passare alla fase successiva, fare clic su **Next**
(Avanti).



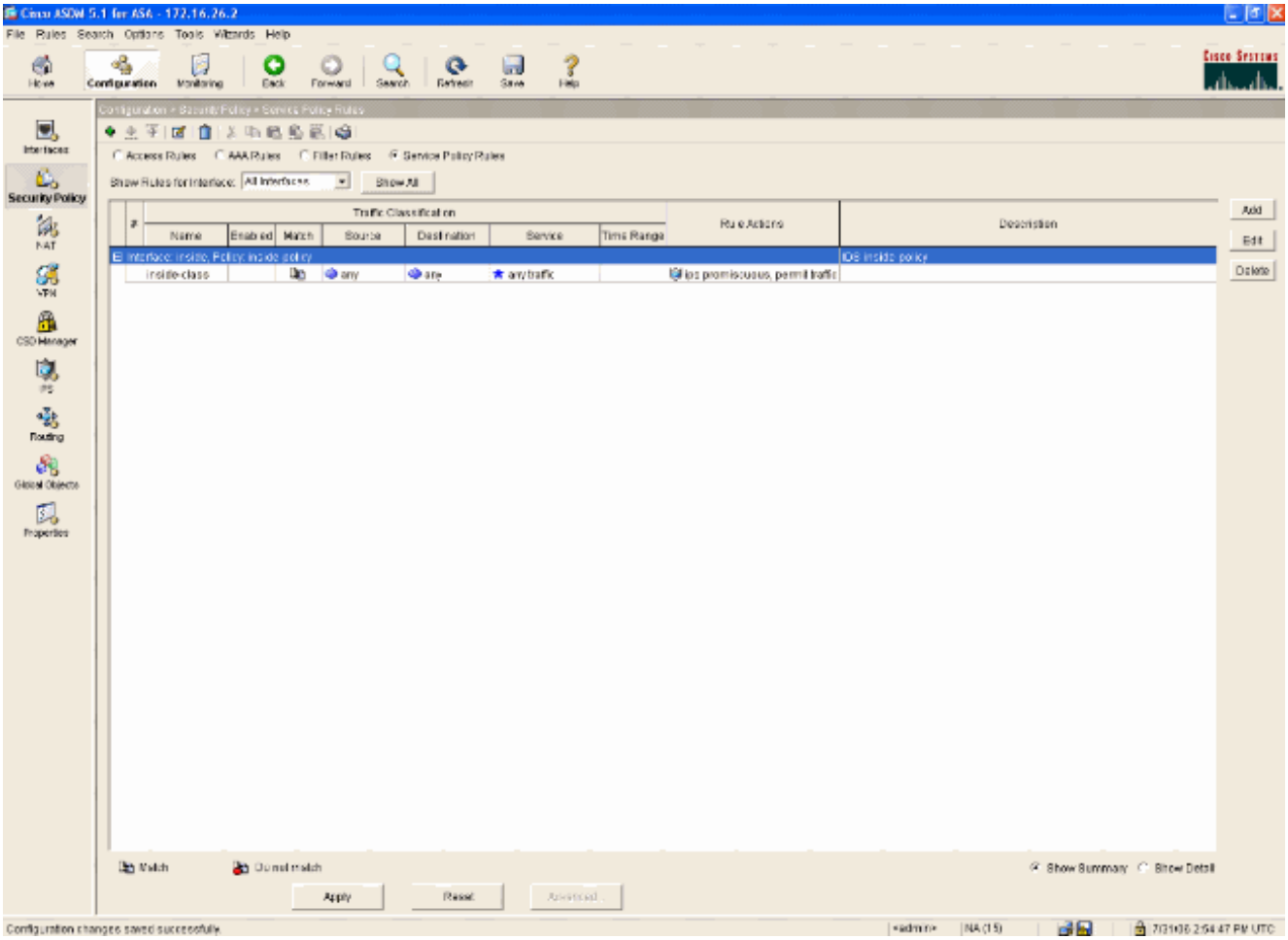
5. Creare una nuova classe di traffico da applicare al criterio.Sebbene sia consigliabile creare classi specifiche per l'analisi di tipi di dati specifici, nell'esempio riportato viene selezionata l'opzione Any Traffic per semplicità. Per continuare, fare clic su **Next** (Avanti).



6. Completare questi passaggi perindicare all'ASA di indirizzare il traffico sul suo server AIP-SSM.Per abilitare il rilevamento delle intrusioni, selezionare **Abilita IPS per questo flusso** di **traffico**.Impostare la modalità su **Promiscua** in modo che una copia del traffico venga inviata al modulo fuori banda anziché posizionare il modulo in linea con il flusso di dati.Fare clic su **Permit traffic** (Autorizza traffico) per verificare che l'ASA passi allo stato fail-open in caso di errore dell'AIP-SSM.Per eseguire il commit della modifica, fare clic su **Fine**.



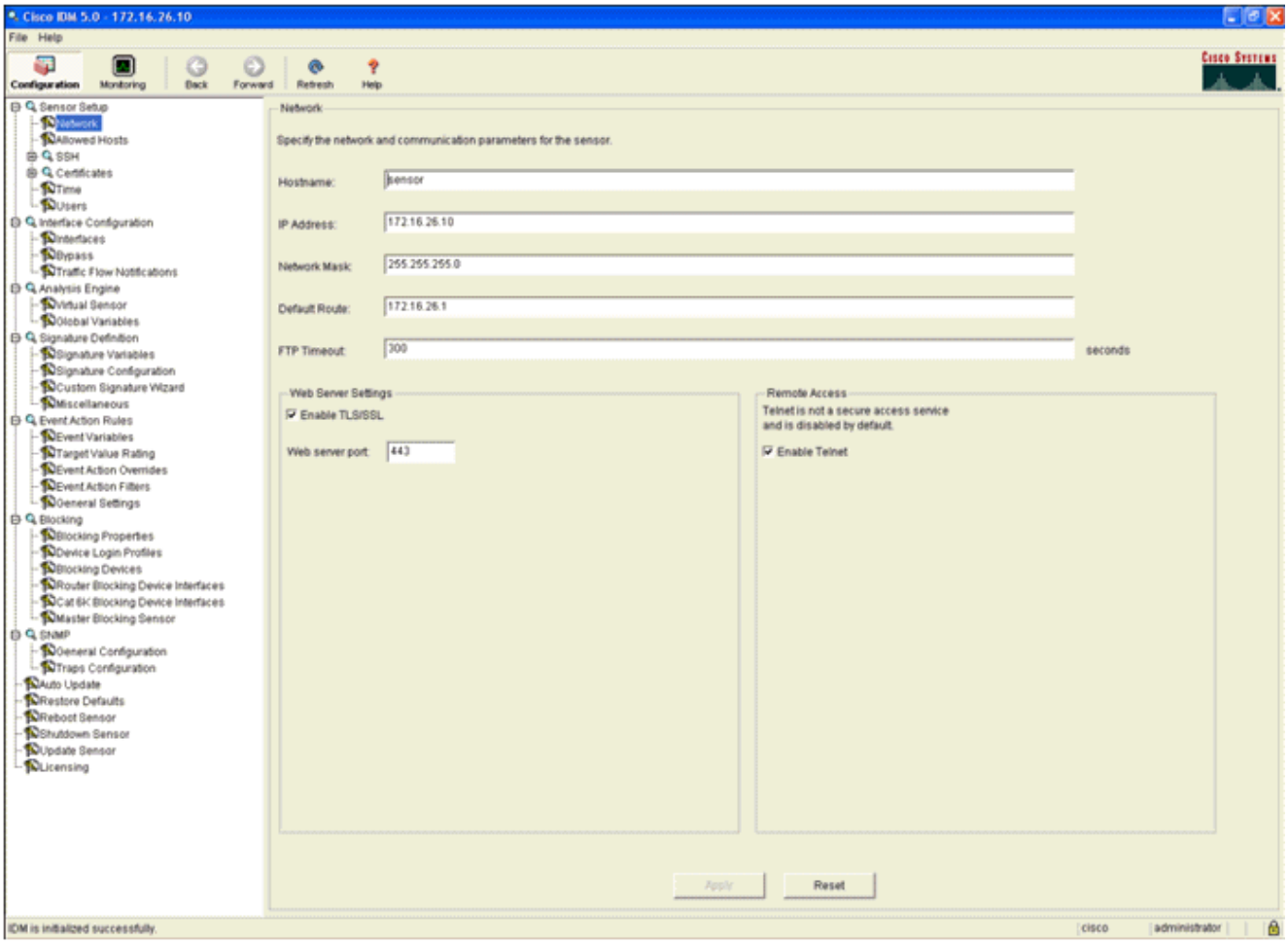
7. L'ASA è ora configurata per inviare il traffico al modulo IPS. Per salvare le modifiche sull'appliance ASA, fare clic su **Save** nella riga superiore.



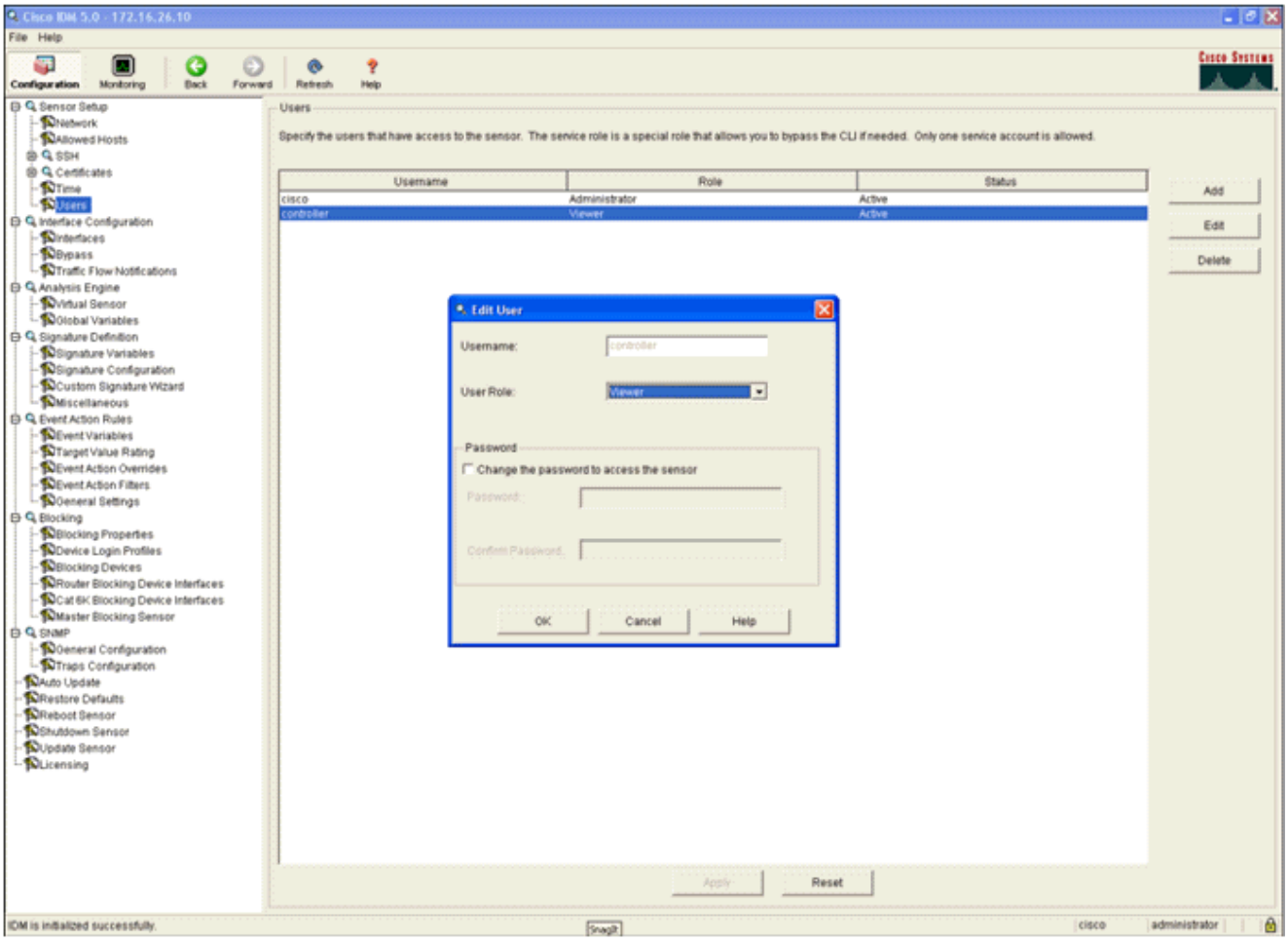
Configurazione di AIP-SSM per l'ispezione del traffico

Mentre l'ASA invia i dati al modulo IPS, associare l'interfaccia AIP-SSM al motore dei sensori virtuali.

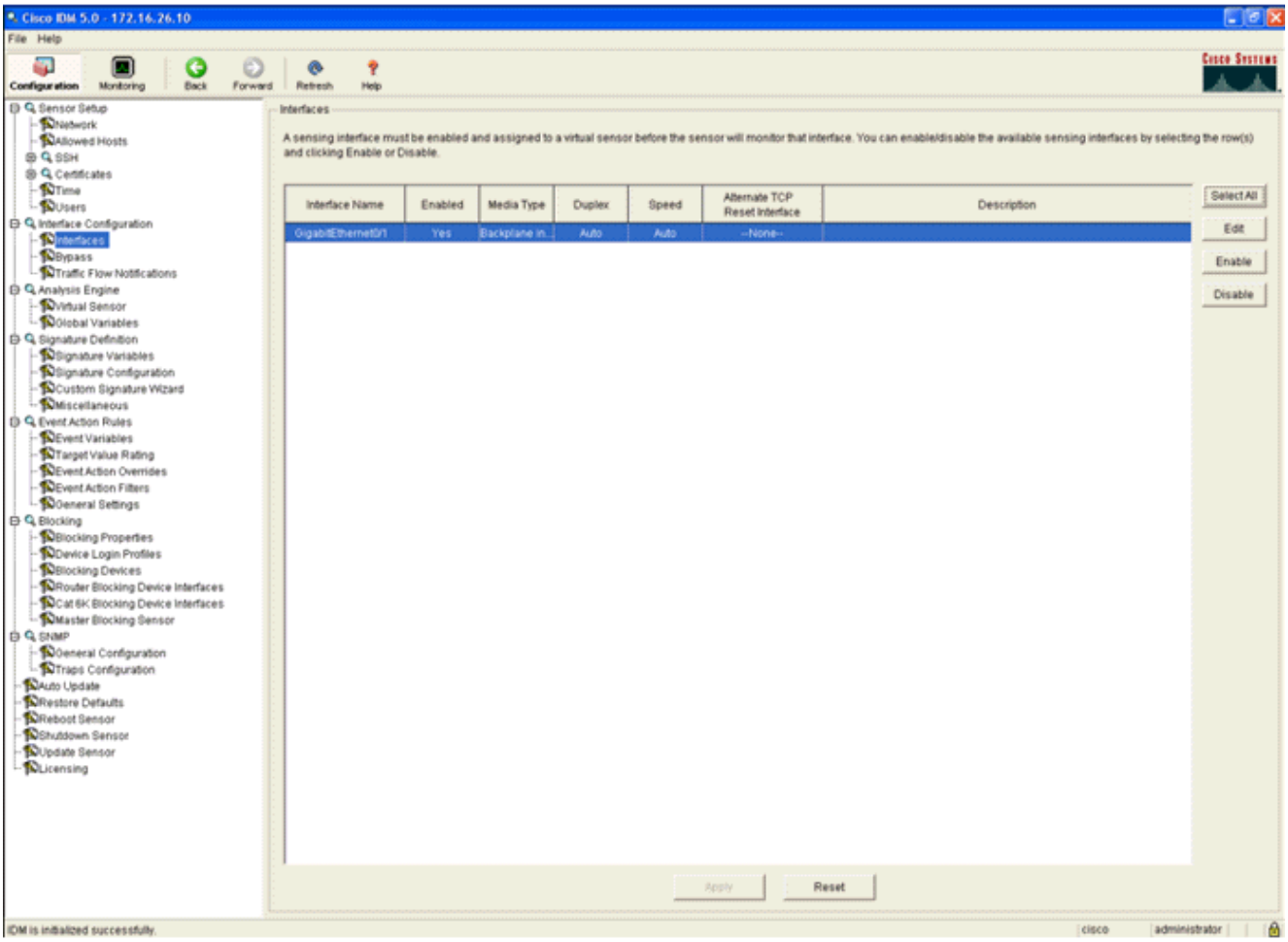
1. Accedere a AIP-SSM utilizzando IDM.



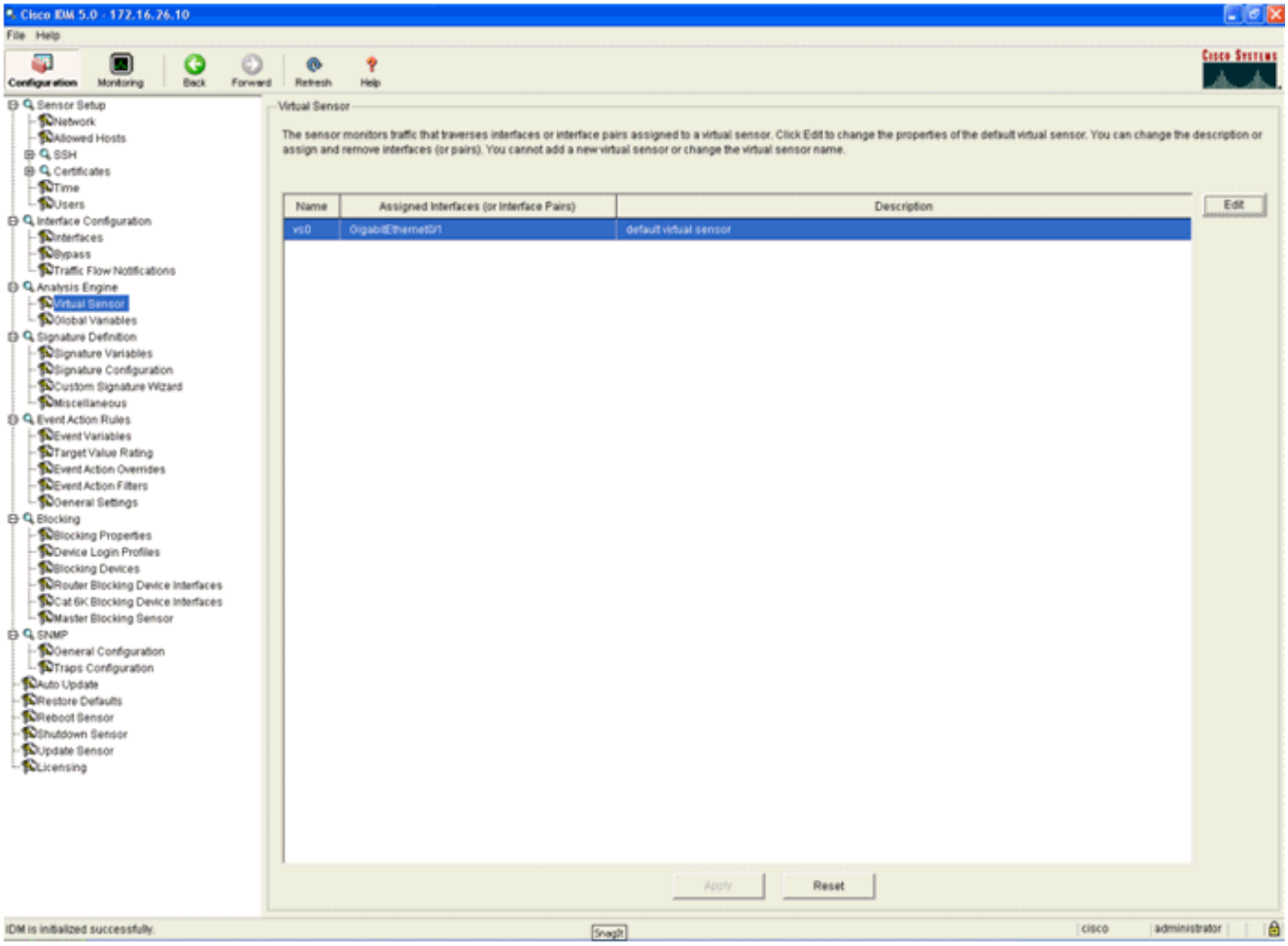
2. Aggiungere un utente con almeno privilegi di visualizzatore.



3. Abilitare l'interfaccia.



4. Controllare la configurazione del sensore virtuale.

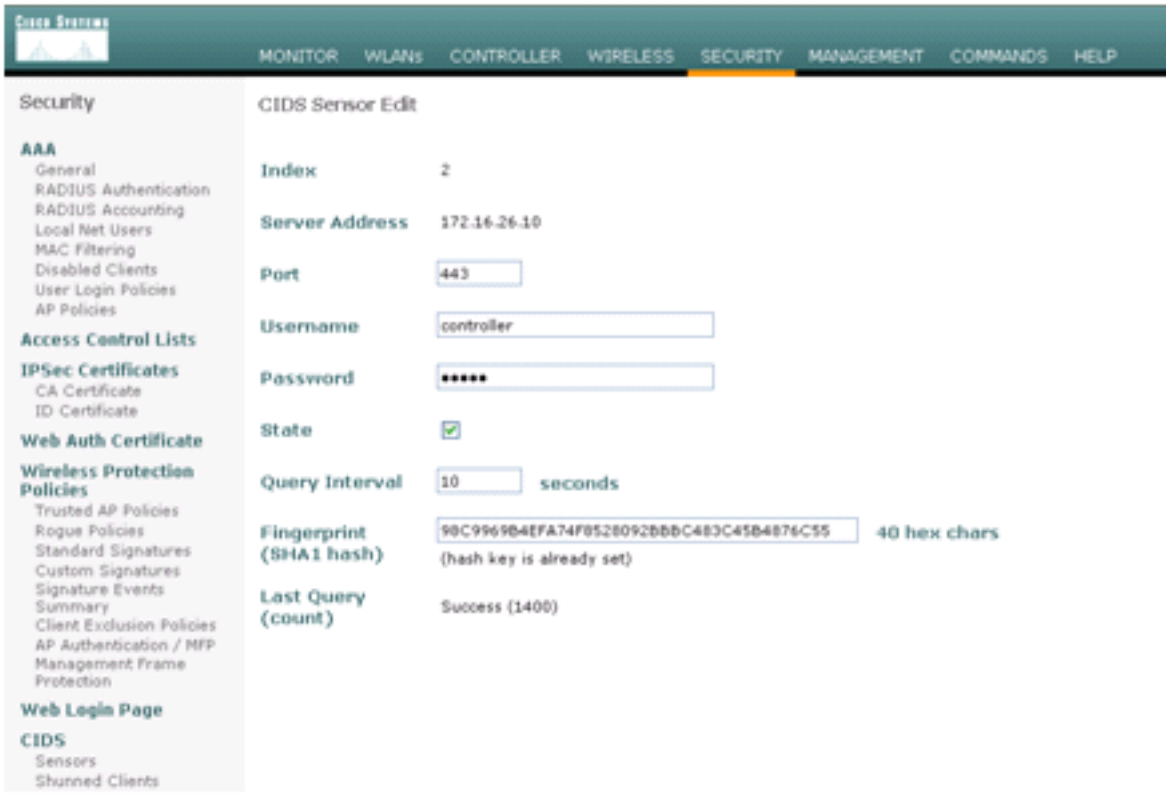


Configurare un WLC per eseguire il polling di AIP-SSM per i blocchi client

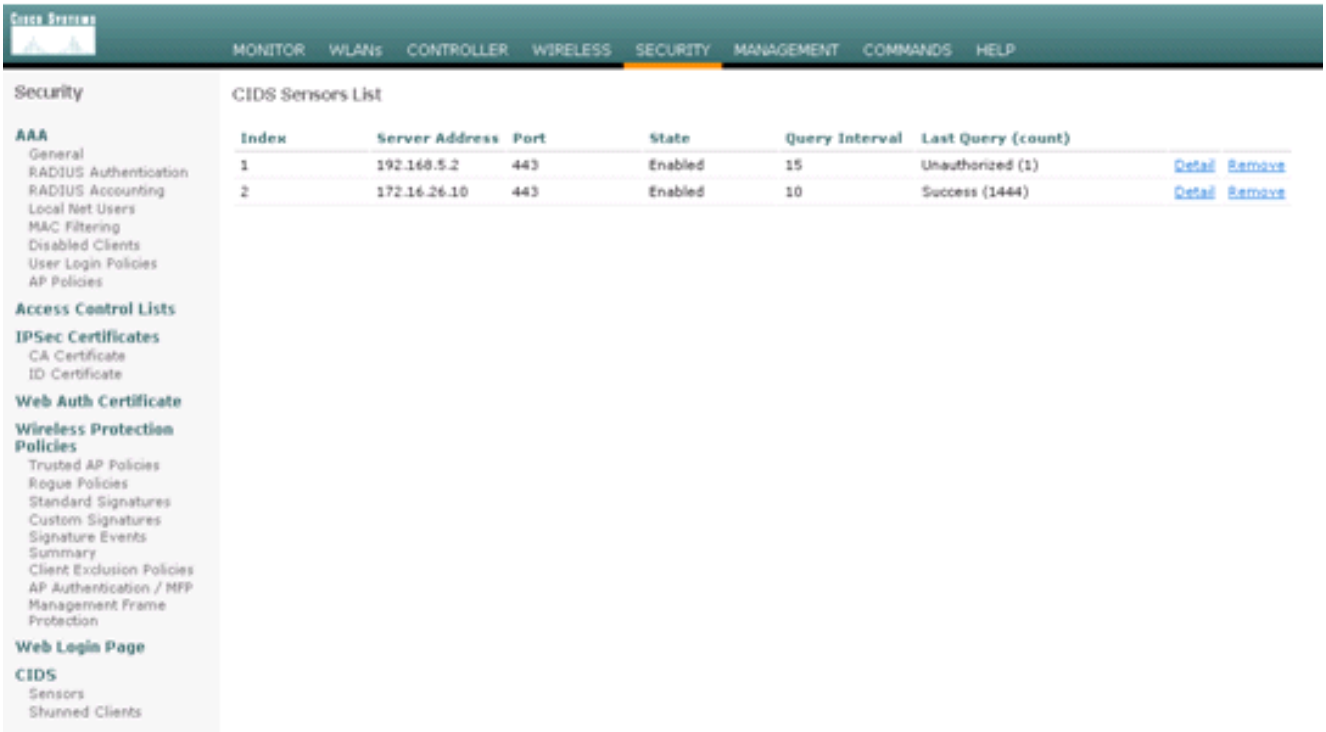
Completare questi passaggi quando il sensore è configurato e pronto per essere aggiunto nel controller:

1. Scegliere **Sicurezza > CIDS > Sensori > Nuovo** nel WLC.
2. Aggiungere l'indirizzo IP, il numero di porta TCP, il nome utente e la password creati nella sezione precedente.
3. Per ottenere l'impronta digitale dal sensore, eseguire questo comando nel sensore e aggiungere l'impronta digitale SHA1 sul WLC (senza i due punti). Utilizzato per proteggere la comunicazione di polling da controller a 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
```



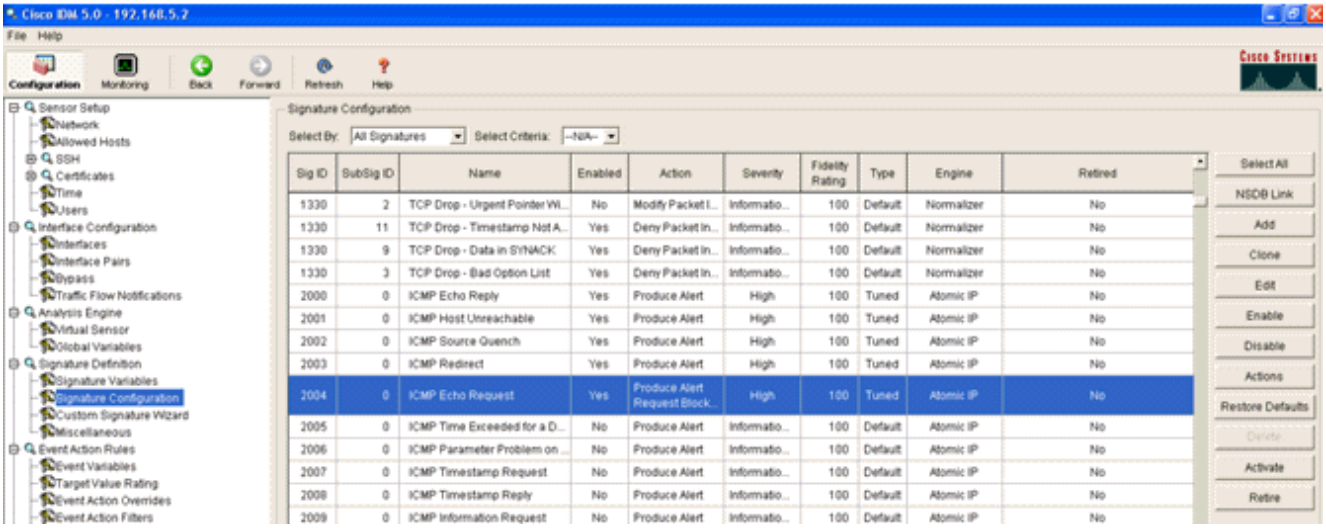
4. Controllare lo stato della connessione tra l'AIP-SSM e il WLC.



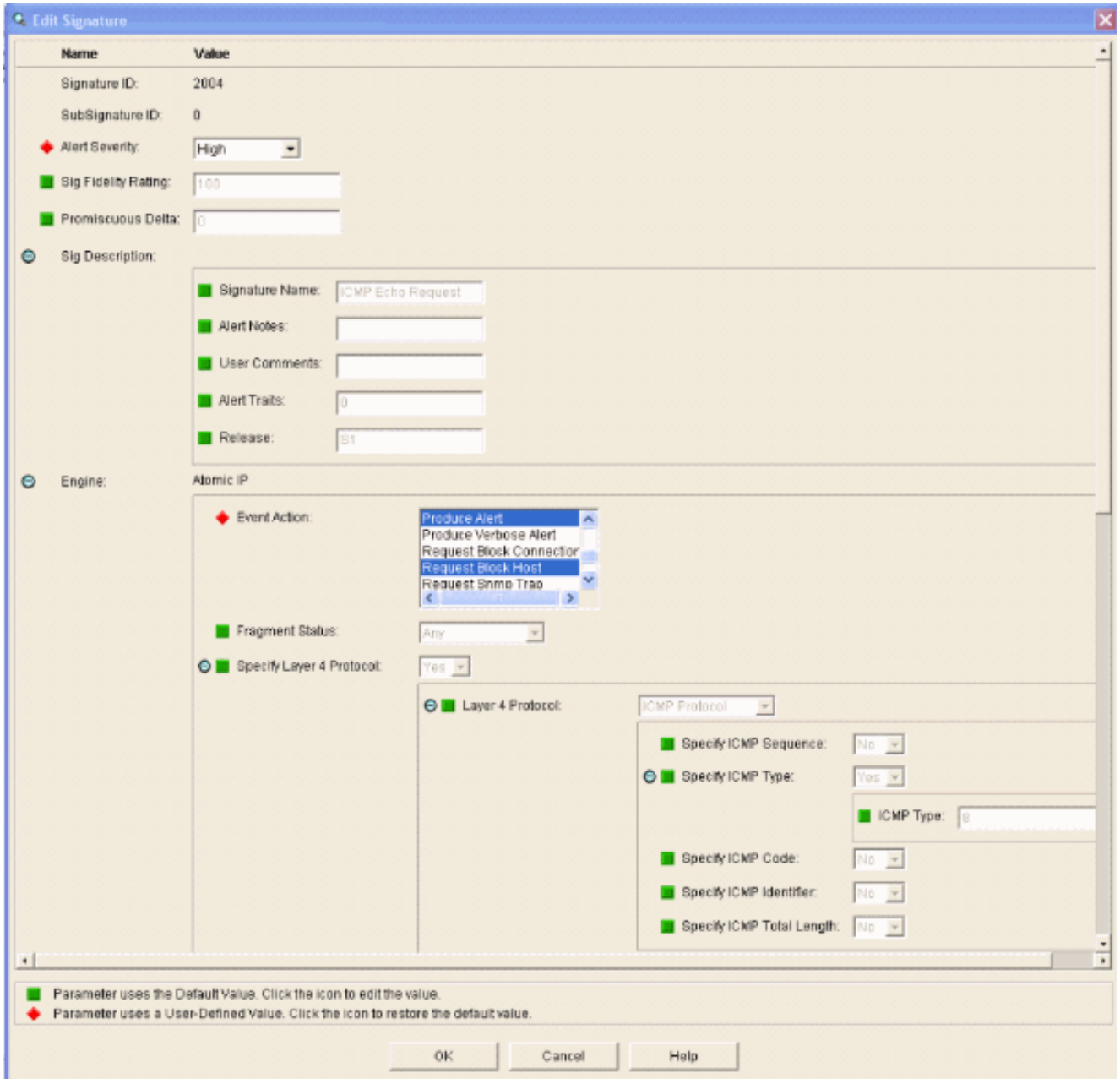
Aggiungere una firma di blocco a AIP-SSM

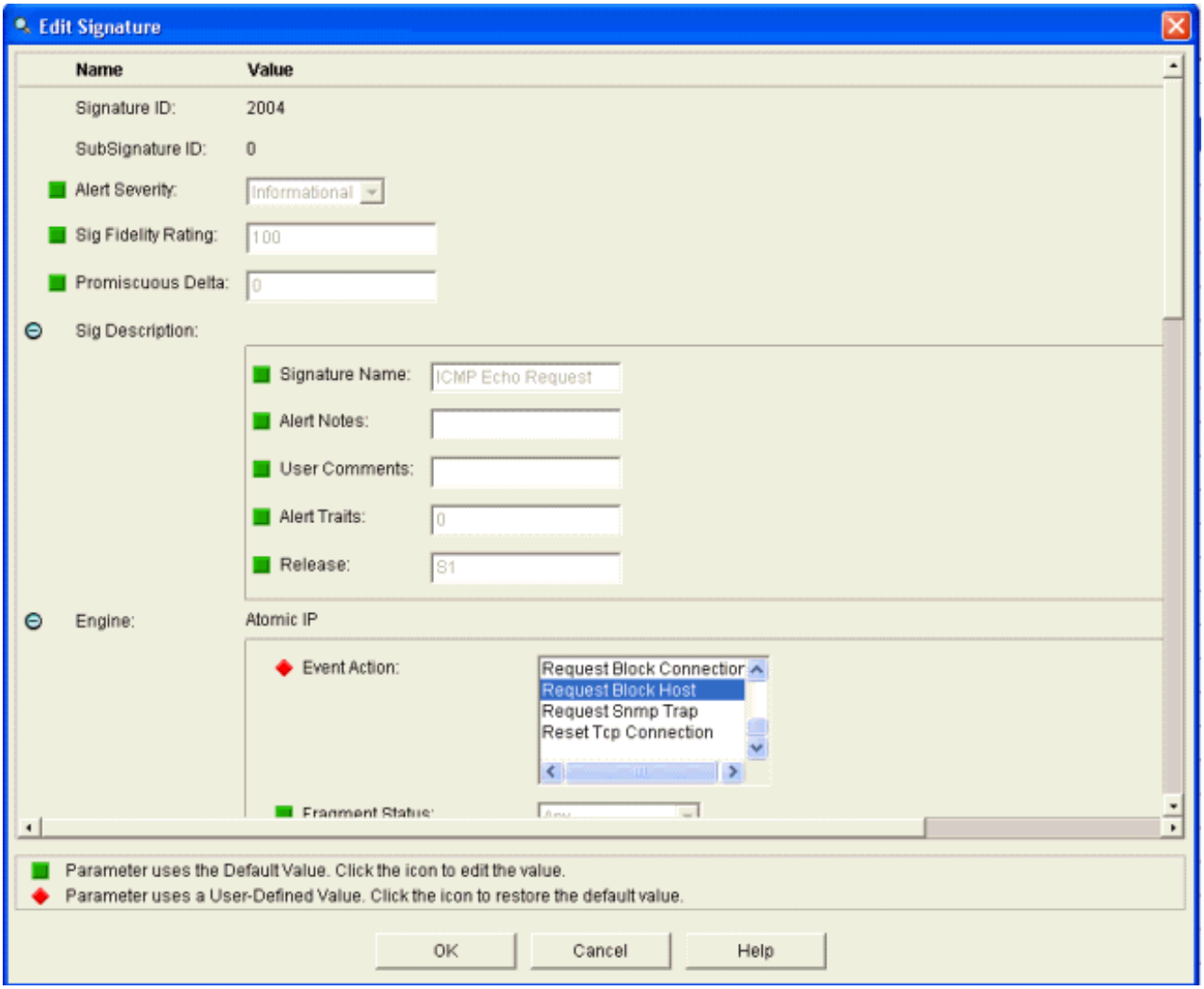
Aggiungere una firma di ispezione per bloccare il traffico. Sebbene siano presenti molte firme che possono eseguire il processo in base agli strumenti disponibili, in questo esempio viene creata una firma che blocca i pacchetti ping.

1. Selezionare la **firma 2004 (ICMP Echo Request)** per eseguire una rapida verifica della configurazione.



2. Per completare la procedura di verifica, abilitare la firma, impostare la gravità dell'avviso su **Alta** e impostare Azione evento su **Produzione host avvisi** e **host blocchi richieste**. L'azione Host blocco richiesta è la chiave per segnalare il WLC e creare eccezioni client.



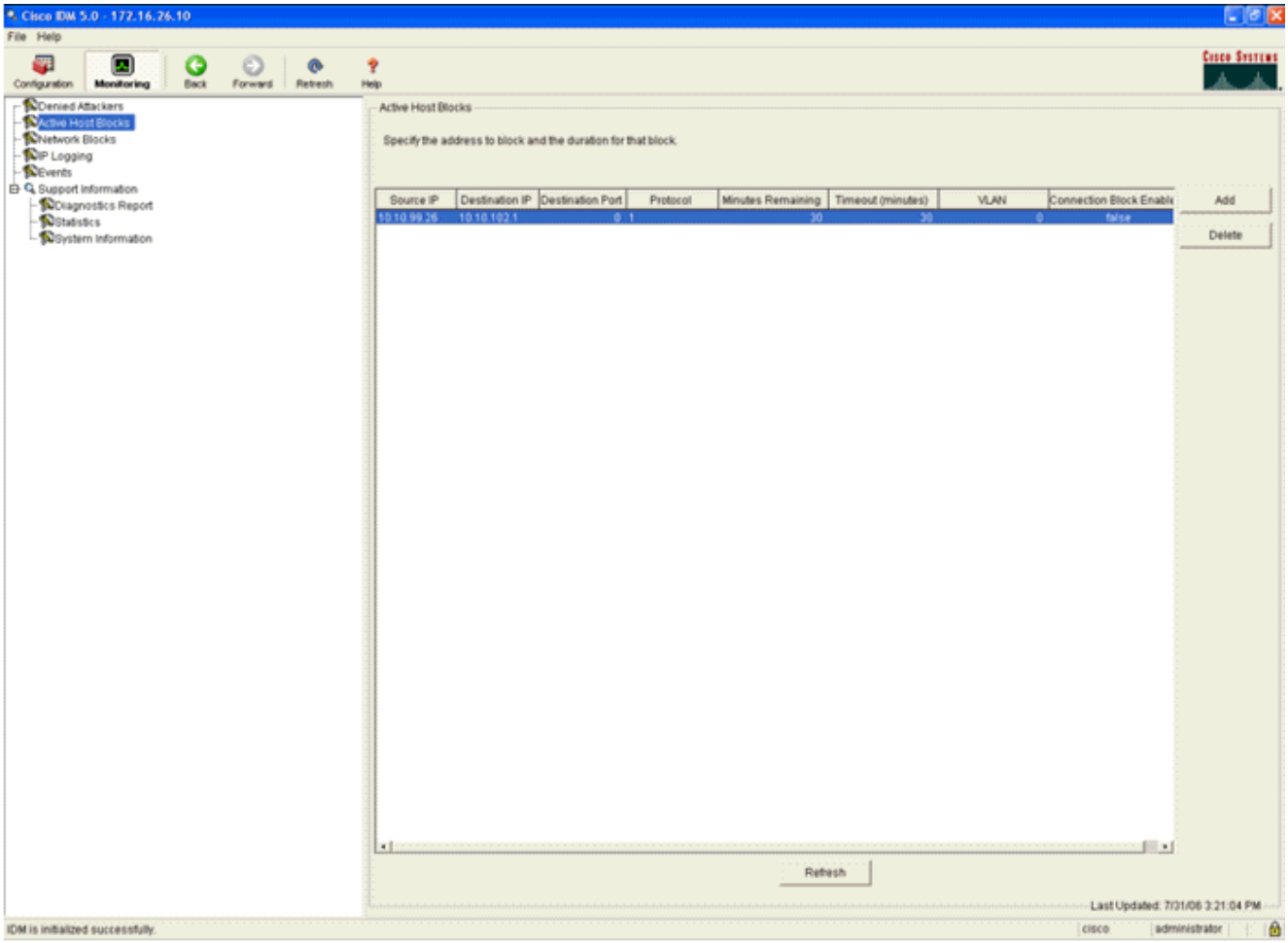


3. Per salvare la firma, fare clic su **OK**.
4. Verificare che la firma sia attiva e impostata per eseguire un'azione di blocco.
5. Per eseguire il commit della firma nel modulo, fare clic su **Applica**.

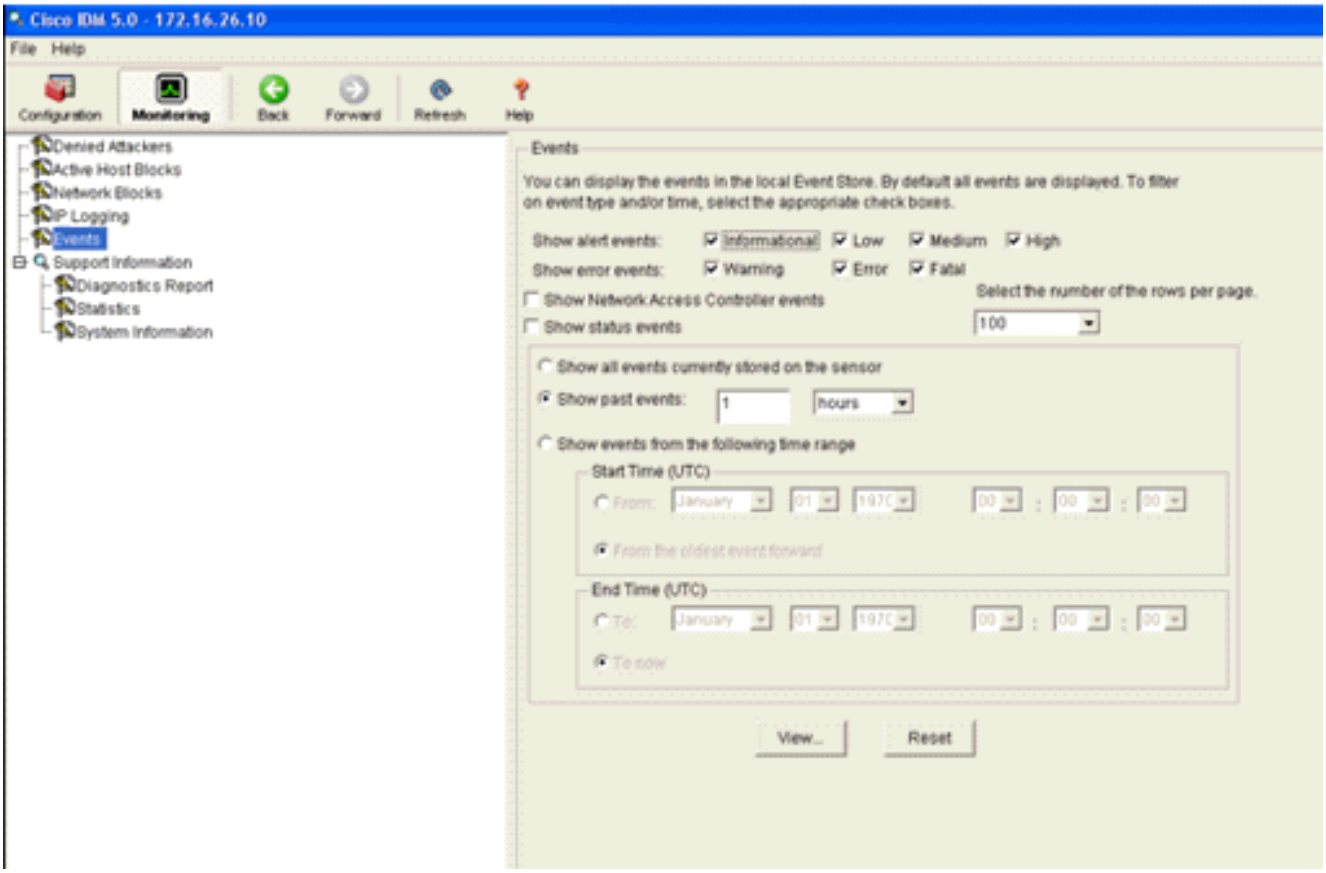
Monitoraggio del blocco e degli eventi con IDM

Attenersi alla seguente procedura:

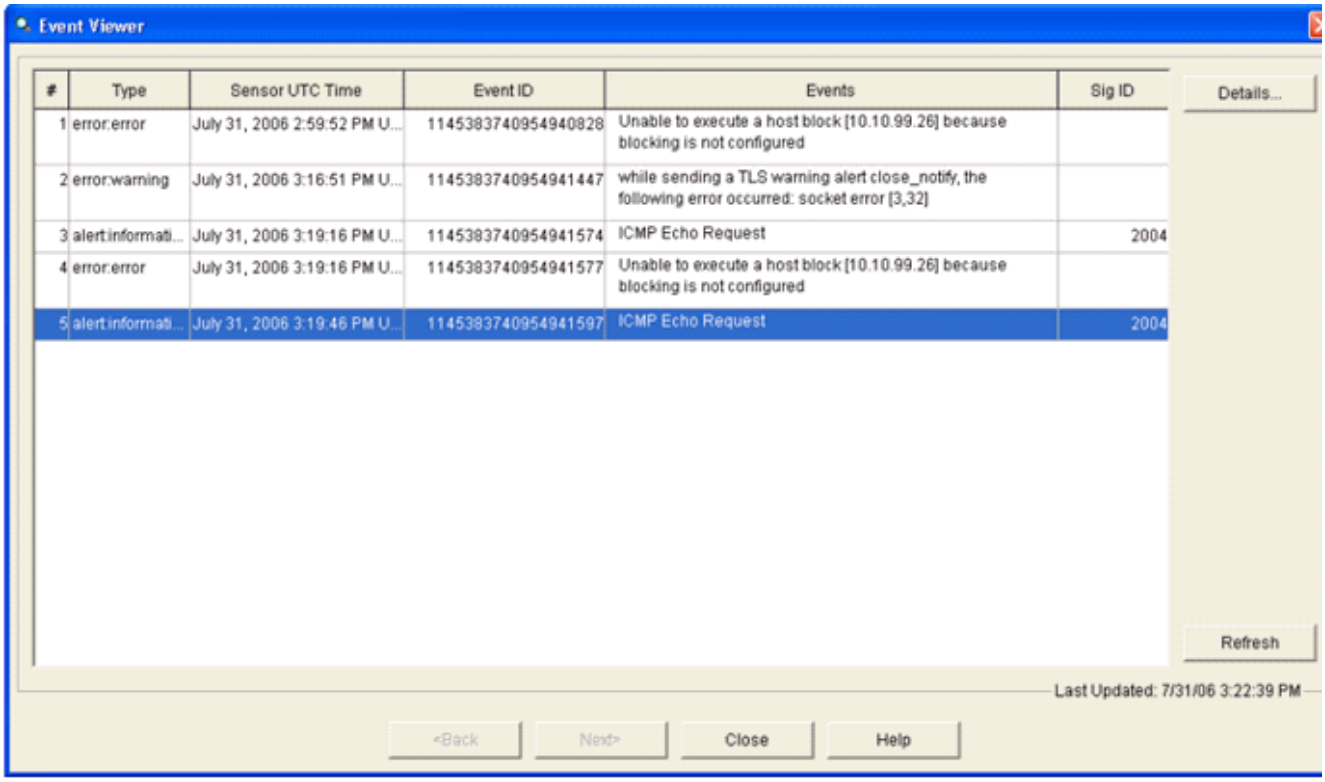
1. Quando la firma viene attivata correttamente, in IDM sono disponibili due posizioni in cui annotare questa condizione.Il primo metodo mostra i blocchi attivi installati da AIP-SSM. Fare clic su **Monitoraggio** nella riga superiore delle azioni. Nell'elenco di elementi visualizzato sul lato sinistro, selezionare **Blocchi host attivi**. Ogni volta che viene attivata la firma ping, nella finestra Blocchi host attivi vengono visualizzati l'indirizzo IP del trasgressore, l'indirizzo del dispositivo da attaccare e il tempo rimanente per il quale il blocco è attivo. Il tempo di blocco predefinito è di 30 minuti ed è regolabile. La modifica di questo valore non viene tuttavia illustrata in questo documento. Per informazioni su come modificare questo parametro, consultare la documentazione della configurazione dell'ASA. Rimuovere il blocco immediatamente, selezionarlo dall'elenco e fare clic su **Elimina**.



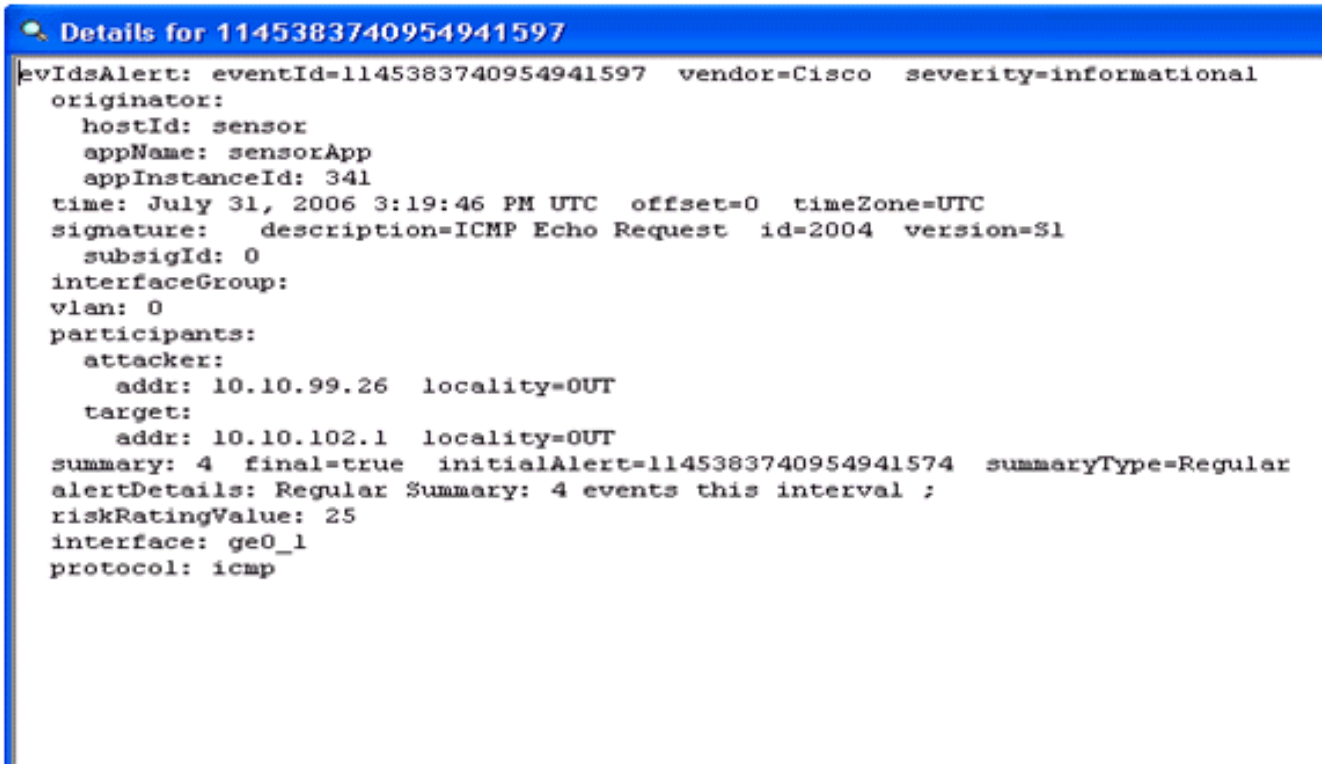
Il secondo metodo per visualizzare le firme attivate utilizza il buffer degli eventi AIP-SSM. Dalla pagina Monitoraggio IDM, selezionare **Eventi** nell'elenco degli elementi a sinistra. Viene visualizzata l'utilità di ricerca Eventi. Impostare i criteri di ricerca appropriati e fare clic su
Visualizza....



2. Viene quindi visualizzato il Visualizzatore eventi con un elenco di eventi che corrispondono ai criteri specificati. Scorrere l'elenco e cercare la firma della richiesta echo ICMP modificata nei passaggi di configurazione precedenti.Cercare nella colonna Eventi il nome della firma oppure il numero di identificazione della firma nella colonna Signature ID.

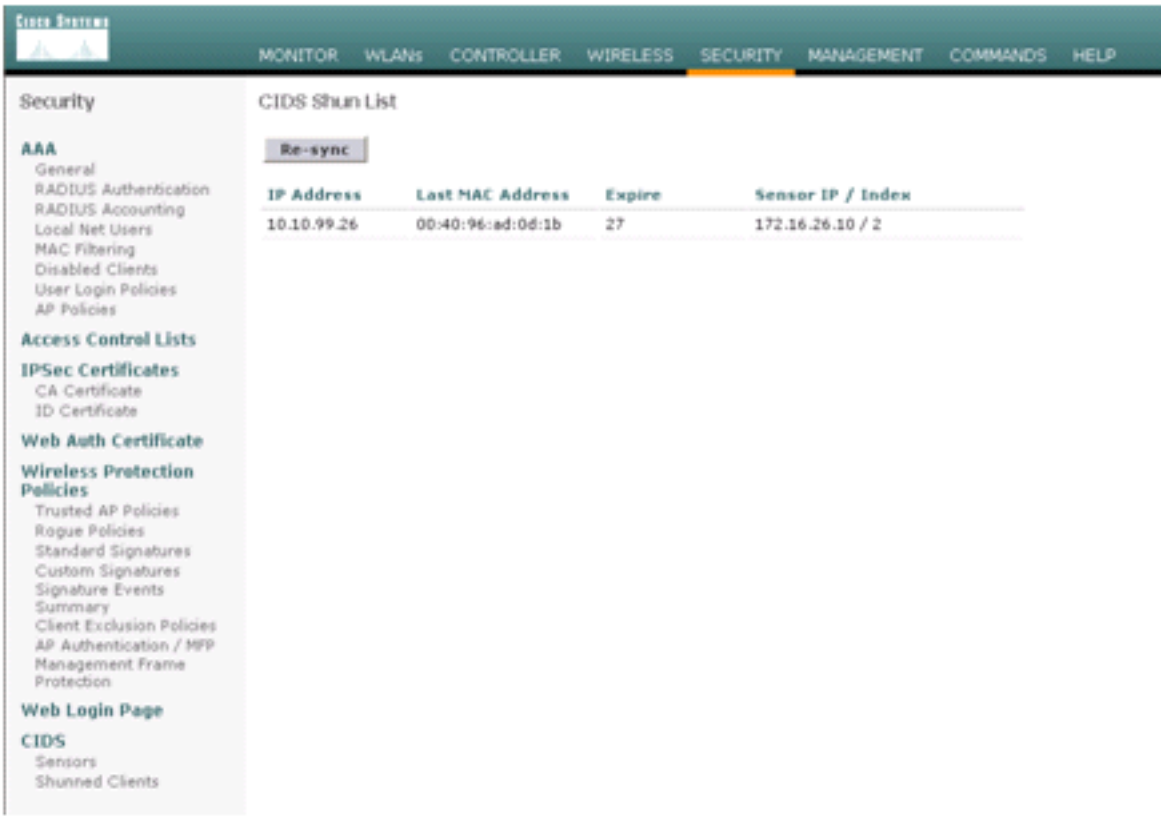


3. Dopo aver individuato la firma, fare doppio clic sulla voce per aprire una nuova finestra. La nuova finestra contiene informazioni dettagliate sull'evento che ha attivato la firma.

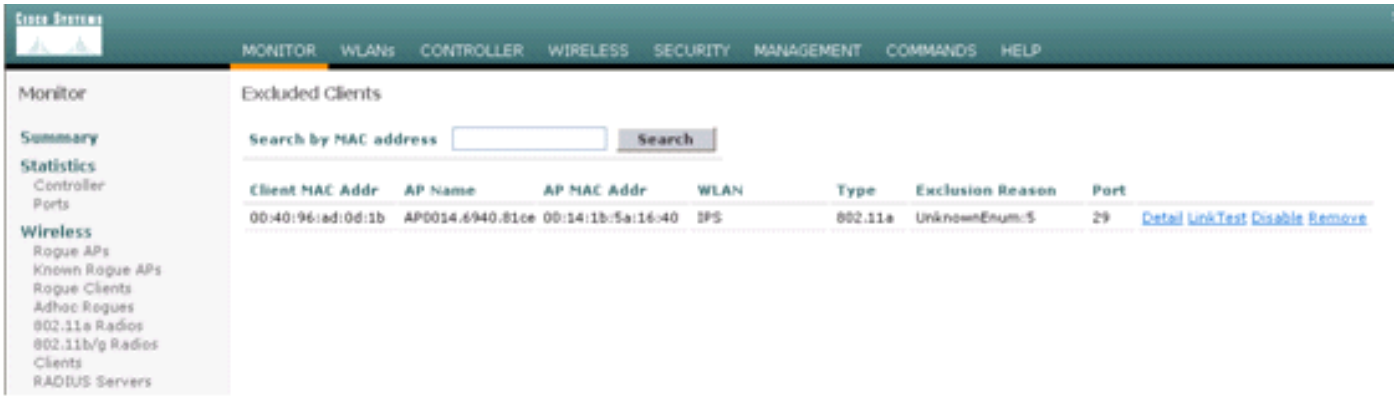


Monitorare l'esclusione dei client in un controller wireless

A questo punto, nell'elenco dei client esclusi del controller vengono inseriti gli indirizzi IP e MAC dell'host.



L'utente viene aggiunto all'elenco di esclusione client.

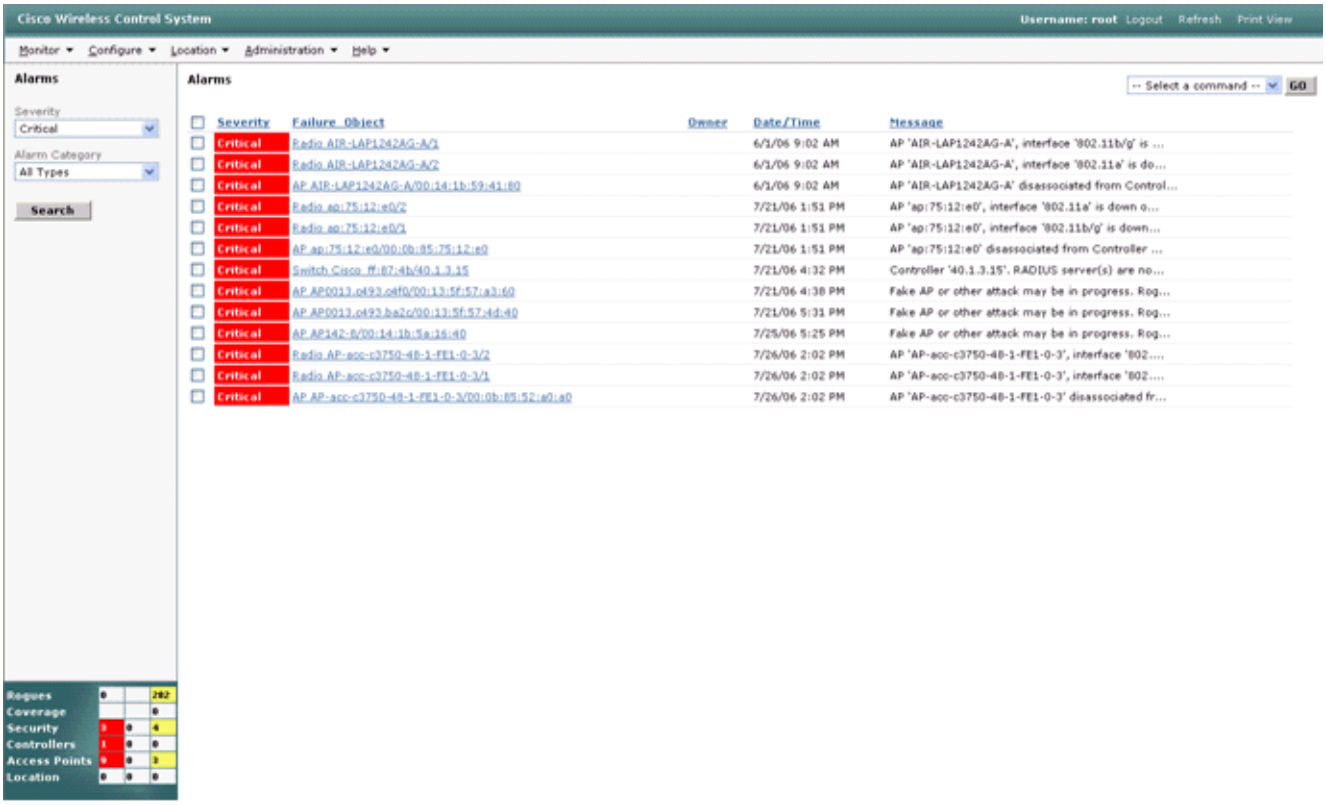


Monitoraggio eventi in WCS

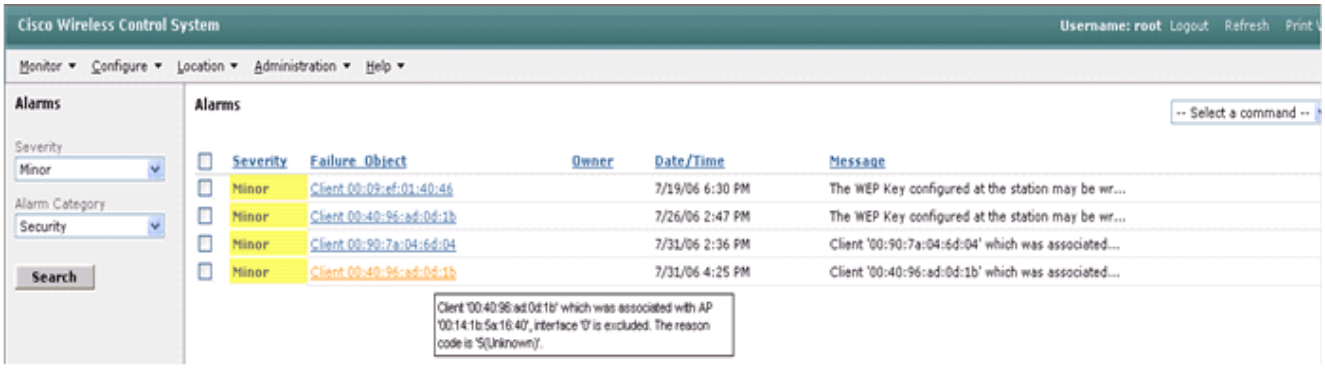
Gli eventi di sicurezza che attivano un blocco all'interno di AIP-SSM fanno in modo che il controller aggiunga l'indirizzo del trasgressore all'elenco di esclusione dei client. In WCS viene inoltre generato un evento.

1. Per visualizzare l'evento di esclusione, utilizzare l'utilità **Monitor > Alarms** del menu principale di Sistema colori Windows. WCS visualizza inizialmente tutti gli allarmi non cancellati e presenta inoltre una funzione di ricerca sul lato sinistro della finestra.
2. Modificare i criteri di ricerca per trovare il blocco client. In Gravità scegliere **Minore** e impostare anche la categoria di allarme su **Sicurezza**.
3. Fare clic su

Cerca.



4. La finestra Allarme elenca quindi solo gli allarmi di sicurezza con un livello di gravità minore. Puntare il mouse sull'evento che ha attivato il blocco all'interno di AIP-SSM.In particolare, WCS mostra l'indirizzo MAC della stazione client che ha causato l'allarme. Posizionando il puntatore del mouse sull'indirizzo appropriato, viene visualizzata una piccola finestra con i dettagli dell'evento. Fare clic sul collegamento per visualizzare gli stessi dettagli in un'altra finestra.



Esempio di configurazione di Cisco ASA

```
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#
```

Esempio di configurazione del sensore Cisco Intrusion Prevention System

```
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#
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Installazione e utilizzo di Cisco Intrusion Prevention System Device Manager 5.1
- Appliance Cisco ASA serie 5500 Adaptive Security - Guide alla configurazione
- Configurazione del sensore Cisco Intrusion Prevention System con l'interfaccia della riga di comando 5.0 - Configurazione delle interfacce
- Guida alla configurazione WLC 4.0
- Supporto tecnico wireless
- Domande frequenti sui Wireless LAN Controller (WLC)
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Configurazione delle soluzioni di sicurezza
- Documentazione e supporto tecnico – Cisco Systems