# Controlador do Wireless LAN e guia de integração IPS

## Índice



## Introdução

O Sistema de Detecção de Intrusão (IDS) e o Sistema de Prevenção de Intrusão (IPS) da Cisco são parte da Cisco Self-Defending Network e é a primeira solução integrada de segurança de rede com e sem fio na indústria. O IDS/IPS unificado Cisco toma um abordagem abrangente à Segurança — na borda wireless, borda prendida, borda MACILENTO, e com o centro de dados. Quando um cliente associado envia o tráfego malicioso através da rede de Cisco Unified Wireless, um dispositivo prendido Cisco IDS detecta o ataque e envia-o evita pedidos aos controladores de LAN do Cisco Wireless (WLC), que dissociam então o dispositivo do cliente.

O ips Cisco é uma solução inline, Com base na rede, projetada identificar, classificar, e parar exatamente o tráfego malicioso, incluindo worms, spyware/adware, vírus da rede, e abuso do

aplicativo, antes que afetem a continuidade do negócio.

Com a utilização da versão 5 do software de sensor do ips Cisco, a solução do ips Cisco combina serviços inline da prevenção com as Tecnologias inovativas para melhorar a precisão. O resultado é confiança total na proteção fornecida de sua solução IPS, sem o medo do tráfego legitimado que está sendo deixado cair. A solução do ips Cisco igualmente oferece a proteção detalhada de sua rede com sua capacidade original para colaborar com outros recursos da segurança de rede e fornece um abordagem proativa à proteção de sua rede.

Os usuários das ajudas da solução do ips Cisco param mais ameaças com maior confiança com o uso destas características:

- **Tecnologias inline exatas da prevenção** — Fornece a confiança incomparável para tomar a ação preventiva contra uma escala mais larga das ameaças sem o risco de deixar cair o tráfego legitimado. Estas Tecnologias originais oferecem a análise inteligente, automatizada, do contexto de seus dados e ajudam-na a assegurar-se de que você receba o a maioria fora de sua solução da prevenção de intrusão.
- **identificação da ameaça do Multi-vetor** — Protege sua rede das violações da política, das explorações da vulnerabilidade, e da atividade anômala com inspeção detalhada do tráfego nas camadas 2 com o 7.
- **Colaboração da rede exclusiva** — Aumenta a escalabilidade e a elasticidade com a Colaboração da rede, incluindo técnicas da captação do tráfego, capacidades da função de balanceamento de carga, e a visibilidade eficientes no tráfego criptografado.
- **Soluções detalhadas do desenvolvimento** — Fornece soluções para todos os ambientes, das pequenas e médias empresas (SMB) e dos lugar do escritório filial às grandes instalações da empresa e do provedor de serviços.
- **Gerenciamento, correlação de evento, e serviços de assistência poderosos** — permite uma solução completa, incluindo a configuração, o Gerenciamento, a correlação dos dados, e serviços de assistência avançados. Em particular a monitoração, a análise, e o sistema de resposta do Cisco Security (MARTE) identificam, isolados, e recomendam a remoção da precisão de elementos de ofensa, para uma solução larga da prevenção de intrusão da rede. E o Sistema de controle de incidente da Cisco impede manifestações novas do worm e do vírus permitindo a rede adaptar e fornecer rapidamente uma resposta distribuída.

Quando combinados, estes elementos fornecem uma solução inline detalhada da prevenção e dão-lhe a confiança para detectar e parar a escala a mais larga do tráfego malicioso antes que afete a continuidade do negócio. A iniciativa da rede de auto-definição de Cisco chama para a Segurança integrada e incorporado para soluções de rede. O protocolo de pouco peso atual do Access point (LWAPP) - sistemas de WLAN baseados apoia somente as características básicas IDS devido ao fato de que é essencialmente um sistema da camada 2 e limitou o linha-processamento da potência. Código novo das versões Cisco em tempo oportuno para incluir recursos aprimorado novos nos códigos novos. A liberação 4.0 tem as características as mais atrasadas que incluem a integração de um sistema de WLAN LWAPP-baseado com a linha de produto de Cisco IDS/IPS. Nesta liberação, o objetivo é permitir que o sistema de Cisco IDS/IPS instrua os WLC para obstruir determinados clientes do acesso às redes Wireless quando um ataque é detectado em qualquer lugar da camada 3 com a camada 7 que envolve o cliente na consideração.

## Pré-requisitos

## Requisitos

Assegure-se de que você cumpra estes requisitos mínimos:

- Versão de firmware 4.x WLC e mais tarde
- O conhecimento em como configurar o ips Cisco e Cisco WLC é desejável.

## Componentes Utilizados

### Cisco WLC

Estes controladores são incluídos com Software Release 4.0 para alterações IDS:

- Cisco 2000 Series WLC
- Cisco 2100 Series WLC
- WLC Cisco 4400 Series
- Módulo de serviços do Cisco Wireless (WiSM)
- O Cisco Catalyst 3750G Series unificou o switch de acesso
- Módulo de controlador de LAN do Cisco Wireless (WLCM)

### Pontos de acesso

- Lightweight Access Points da série Cisco Aironet 1100 AG
- Lightweight Access Points da série Cisco Aironet 1200 AG
- Lightweight Access Points do Cisco Aironet série 1300
- Lightweight Access Points do Cisco Aironet série 1000

### Gerenciamento

- Sistema de controle sem fio da Cisco (WCS)
- Sensor do Cisco 4200 Series
- Gerenciamento do Cisco IDS - Gerenciador de dispositivo do Cisco IDS (IDM)

### Cisco unificou Plataformas IDS/IPS

- Sensores Cisco IPS série 4200 com software de sensor 5.x do ips Cisco ou mais tarde.
- SSM10 e SSM20 para o Dispositivos de segurança adaptáveis Cisco ASA série 5500 com software de sensor 5.x do ips Cisco
- Dispositivos de segurança adaptáveis Cisco ASA série 5500 com software de sensor 5.x do ips Cisco
- Módulo de rede do Cisco IDS (NM-CIDS) com software de sensor 5.x do ips Cisco
- Módulo intrusion detection system 2 do Cisco Catalyst 6500 Series (IDSM-2) com software de sensor 5.x do ips Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

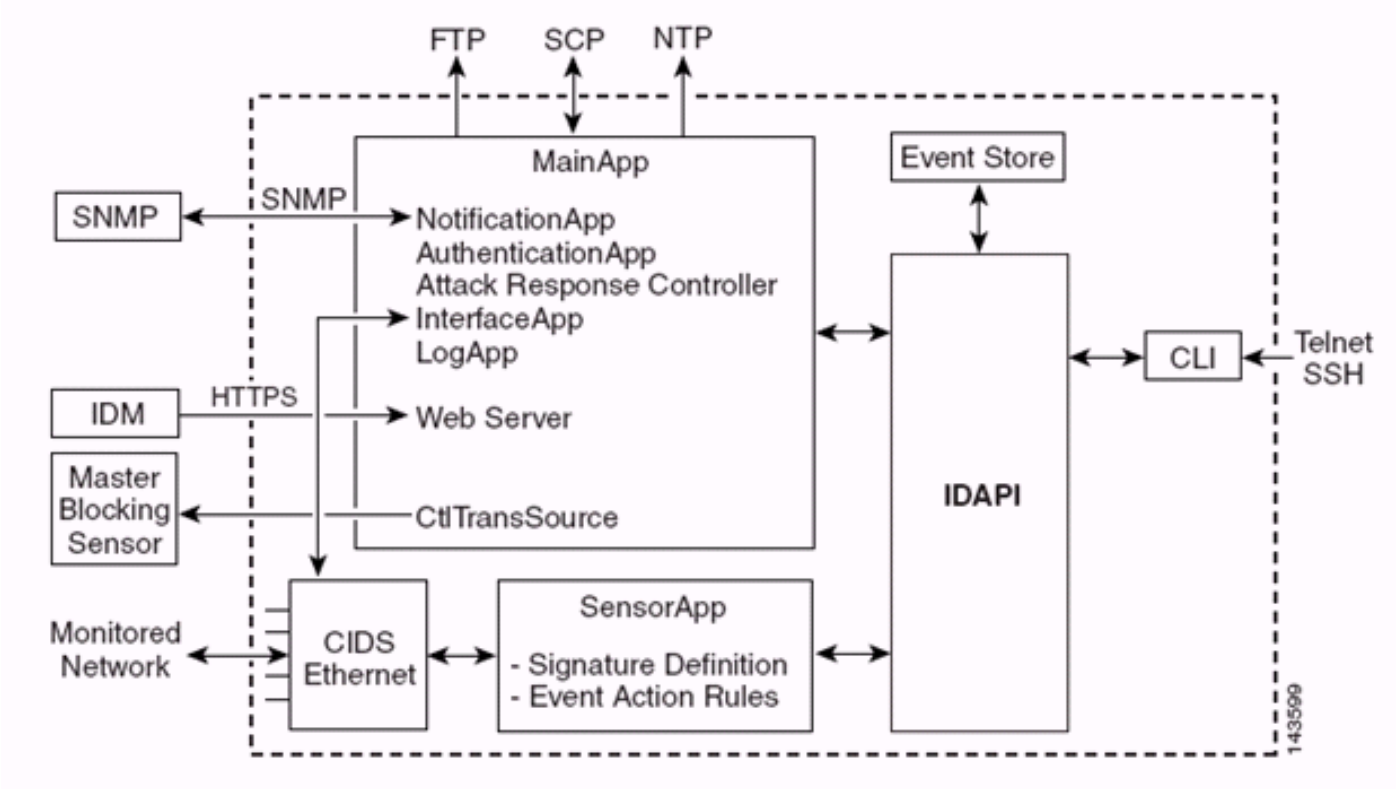
Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre

convenções de documentos.

## Vista geral do Cisco IDS

Os componentes principais do Cisco IDS (versão 5.0) são:

- **App do sensor** — Executa a captura de pacote de informação e a análise.
- **Gestão de armazenamento do evento e módulo das ações** — Fornece o armazenamento de violações da política.
- **A imagem latente, instala e módulo Startup** — As cargas, inicializam, e começam todo o software do sistema.
- **As interfaces do utilizador e o UI apoiam o módulo** — Fornece um CLI encaixado e o IDM.
- **OS do sensor** — Sistema operacional do host (baseado em Linux).




O aplicativo do sensor (software IPS) consiste:

- **App principal** — Inicializa o sistema, começa e para outros aplicativos, configura o OS e é responsável para elevações. Contém estes componentes:**Servidor de transação do controle** — Permite que os sensores enviem as transações do controle que são usadas para permitir o mestre do controlador da resposta do ataque (conhecido anteriormente como o controlador do acesso de rede) que obstrui a capacidade do sensor.**Loja do evento** — Uma loja posicionada usada para armazenar eventos IPS (erros, estado e mensagens de sistema alertas) que seja acessível com o CLI, o IDM, o Security Device Manager adaptável (ASDM), ou o protocolo de intercâmbio de dados remoto (RDEP).
- **App da relação** — Os punhos contorneiam e ajustes físicos e definem relações emparelhadas. Os ajustes físicos consistem na velocidade, no duplex, e nos estados administrativos.
- **App do log** — Redige os mensagens de registro do aplicativo ao arquivo de registro e aos Mensagens de Erro à loja do evento.

- **Controlador da resposta do ataque (ARCO) (conhecido anteriormente como o controlador do acesso de rede)** — controla dispositivos de rede remotos (Firewall, Roteadores, e Switches) fornecer a obstrução de capacidades quando um evento alerta ocorreu. O ARCO cria e aplica o Access Control Lists (ACLs) no dispositivo de rede controlado ou usa o **comando shun** (Firewall).
- **App da notificação** — Envia o SNMP traps quando provocado por um alerta, por um estado, e por uns eventos do erro. O App da notificação usa um agente SNMP do public domain isto. O SNMP GET fornece a informação sobre a saúde de um sensor.**Servidor de Web (server HTTP RDEP2)** — Fornece uma relação de usuário de web. Igualmente fornece meios comunicar-se com outros dispositivos IPS com RDEP2 usando diversos servlet para proporcionar serviços IPS.**App da autenticação** — Verifica que os usuários estão autorizados executar ações CLI, IDM, ASDM, ou RDEP.
- **App do sensor (motor da análise)** — Executa a captura de pacote de informação e a análise.
- **CLI** — A relação que é executada quando os usuários entrarem com sucesso ao sensor com o telnet ou o SSH. Todas as contas criadas com o CLI usam o CLI como seu shell (a não ser que a conta de serviço - somente uma conta de serviço é permitida). Os comandos CLI permitidos dependem do privilégio do usuário.

Todos os aplicativos IPS se comunicam um com o otro com um Application Program Interface comum (API) IDAPI chamado. Os aplicativos remotos (os outros sensores, aplicativos de gerenciamento, e software de terceira parte) comunicam-se com os sensores com RDEP2 e protocolos da troca do evento do dispositivo de segurança (SDEE).

Deve-se notar que o sensor tem estes partições de disco:

- **Partição de aplicativo** — Contém a imagem do sistema completa IPS.
- **Separação da manutenção** — Uma imagem IPS do propósito especial usada para criar nova imagem o partição de aplicativo do IDSM-2. Criar nova imagem da separação da manutenção conduz aos ajustes de configuração perdidos.
- **Separação da recuperação** — Uma imagem do propósito especial usada para a recuperação do sensor. O booting na separação da recuperação permite usuários de criar nova imagem completamente o partição de aplicativo. As configurações de rede são preservadas, mas todas configurações restantes são perdidas.

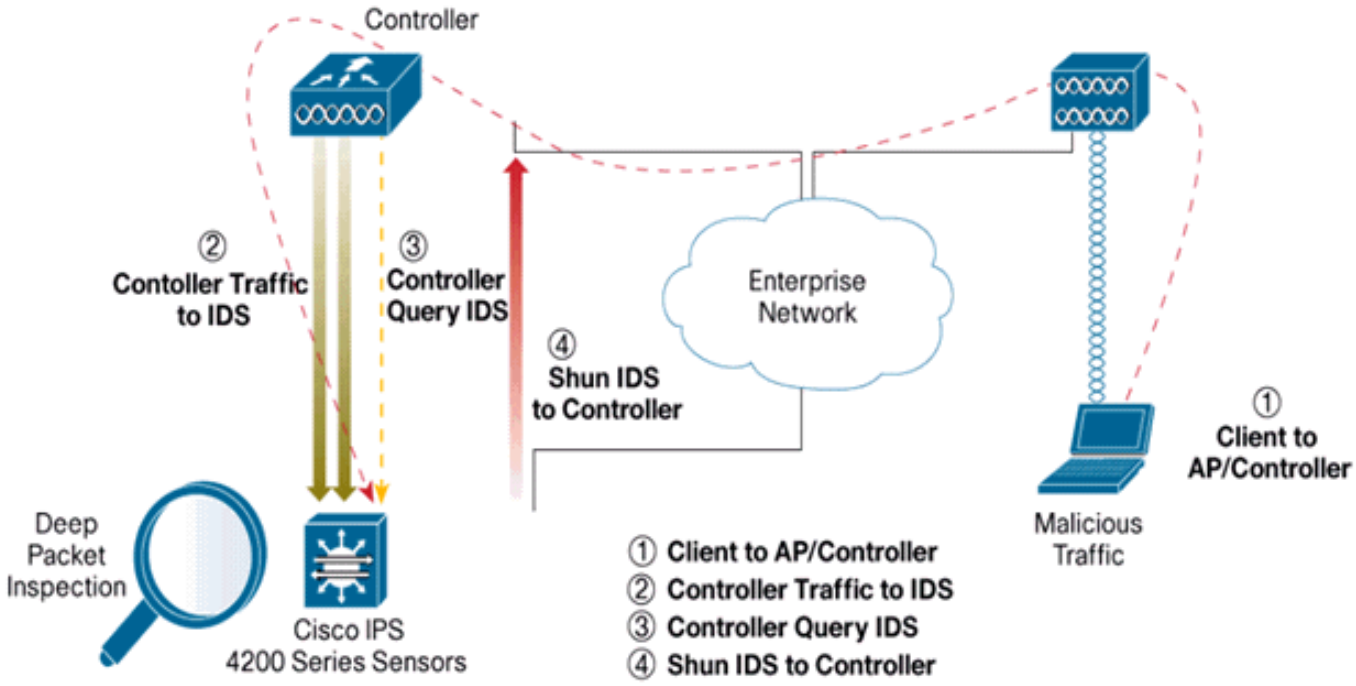
## Cisco IDS e WLC – Vista geral da integração

A versão 5.0 do Cisco IDS introduz a capacidade para configurar nega ações quando as violações da política (assinaturas) são detectadas. Baseado na configuração do usuário no sistema IDS/IPS, um pedido evitar pode ser enviado a um Firewall, a um roteador, ou a um WLC a fim obstruir os pacotes de um endereço IP particular.

Com a liberação de software de rede 4.0 do Cisco Unified Wireless para controladores do Cisco Wireless, um pedido evitar precisa de ser enviado a um WLC a fim provocar o cliente que põr ou o comportamento da exclusão disponível em um controlador. A relação que o controlador se usa para obter o pedido evitar é o comando e a interface de controle no Cisco IDS.

- O controlador permite que até cinco sensors de IDS sejam configurados em um controlador dado.
- Cada sensor de IDS configurado é identificado por seus endereço IP de Um ou Mais Servidores Cisco ICM NT ou credenciais qualificadas do nome de rede e da autorização.

- Cada sensor de IDS pode ser configurado em um controlador com uma taxa original da pergunta nos segundos.




## Evitar IDS

O controlador pergunta o sensor na taxa configurada da pergunta a fim recuperar todos os eventos evitar. Dado evita o pedido é distribuído durante todo o grupo inteiro da mobilidade do controlador que recupera o pedido do sensor de IDS. Cada um evita o pedido para um endereço IP cliente é de fato para o valor especificado dos segundos do intervalo. Se o valor de timeout indica uma estadia infinita, a seguir o evento evitar termina somente se a entrada evitar é removida no IDS. O estado evitado do cliente está mantido em cada controlador no grupo da mobilidade mesmo se alguns ou todos os controladores são restaurados.

**Note**: A decisão para evitar um cliente é feita sempre pelo sensor de IDS. O controlador não detecta ataques da camada 3. É um processo distante mais complicado para determinar que o cliente está lançando um ataque malicioso na camada 3. O cliente é autenticado na camada 2 que é boa bastante para que o controlador conceda o acesso da camada 2.

**Note**: Por exemplo, se um cliente obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT (evitado) de ofensa precedente atribuído, é até o intervalo do sensor para desbloquear o acesso da camada 2 para este cliente novo. Mesmo se o controlador dá o acesso na camada 2, o tráfego do cliente pôde ser obstruído no Roteadores na camada 3 de qualquer maneira, porque o sensor igualmente informa o Roteadores do evento evitar.

Supõe que um cliente tem o endereço IP de Um ou Mais Servidores Cisco ICM NT A. Agora, quando o controlador vota o IDS para evitar eventos, o IDS envia o pedido evitar ao controlador com endereço IP de Um ou Mais Servidores Cisco ICM NT A como o endereço IP de destino. Agora, o preto do controlador alista este cliente A. No controlador, os clientes são enfermos baseados em um MAC address.

Agora, supõe que o cliente muda seu endereço IP de Um ou Mais Servidores Cisco ICM NT de A ao B. Durante a votação seguinte, o controlador obtém uma lista de clientes evitados baseados no endereço IP de Um ou Mais Servidores Cisco ICM NT. Esta vez outra vez, o endereço IP de

Um ou Mais Servidores Cisco ICM NT A está ainda na lista evitada. Mas desde que o cliente mudou seu endereço IP de Um ou Mais Servidores Cisco ICM NT de à B (que não está na lista evitada de endereços IP de Um ou Mais Servidores Cisco ICM NT), este cliente com um endereço IP de Um ou Mais Servidores Cisco ICM NT novo de B é liberado uma vez que o intervalo de clientes listados pretos é alcançado no controlador. Agora, o controlador começa permitir a este cliente com novo o endereço IP de Um ou Mais Servidores Cisco ICM NT de B (mas do endereço MAC de cliente permanece o mesmo).

Consequentemente, embora um cliente permaneça deficiente para a duração do tempo da exclusão do controlador e re-seja excluído se obter novamente seu endereço de DHCP precedente, esse cliente é desabilitado já não se o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente que é mudanças evitadas. Por exemplo, se o cliente conecta ao a mesma rede e o intervalo do aluguel de DHCP não são expirados.

Conexão do apoio dos controladores somente ao IDS para o cliente que evita os pedidos que usam a porta de gerenciamento no controlador. O controlador conecta ao IDS para a inspeção de pacote de informação através das interfaces de VLAN aplicáveis que levam o tráfego do cliente Wireless.

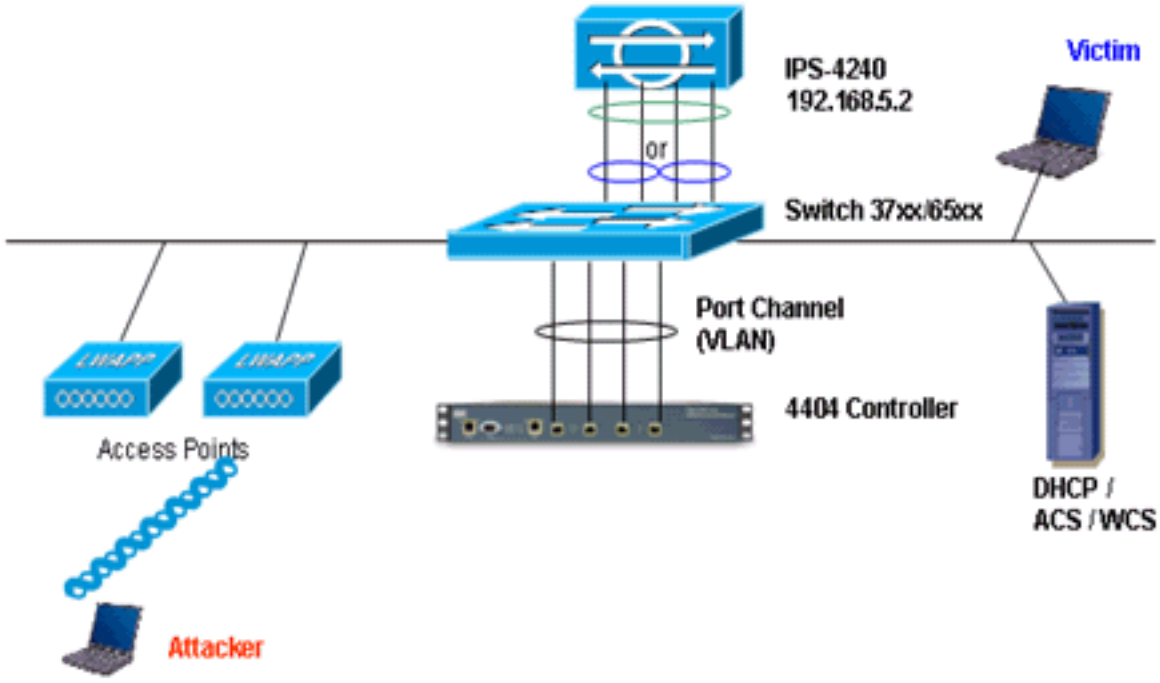
No controlador, a página dos clientes do desabilitação mostra cada cliente que foi desabilitado através de um pedido do sensor de IDS. O comando cli show igualmente indica uma lista de clientes põr.

No WCS, os clientes excluídos são indicados sob a aba do sub da Segurança.

Estão aqui as etapas a seguir a fim terminar a integração dos sensores do ips Cisco e do Cisco WLC.

1. Instale e conecte a ferramenta de IDS no mesmo interruptor onde o controlador wireless reside.
2. Espelhe (PERÍODO) as portas WLC que levam o tráfego do cliente Wireless à ferramenta de IDS.
3. A ferramenta de IDS recebe uma cópia de cada pacote e inspeciona o tráfego na camada 3 com o 7.
4. A ferramenta de IDS oferece um arquivo de assinatura carregável, que possa igualmente ser personalizado.
5. A ferramenta de IDS gerencie o alarme com uma ação do evento de evita quando uma assinatura do ataque é detectada.
6. O WLC vota o IDS para alarmes.
7. Quando um alarme com o endereço IP de Um ou Mais Servidores Cisco ICM NT de um cliente Wireless, que esteja associado ao WLC, é detectado, põe o cliente na lista da exclusão.
8. Uma armadilha é gerada pelo WLC e pelo WCS é notificada.
9. O usuário é removido da lista da exclusão após o período especificado.

## Projeto da arquitetura de rede




Cisco WLC é conectado às interfaces de gigabit no Catalyst 6500. Crie um canal de porta para as interfaces de gigabit e permita a agregação do link (RETARDAÇÃO) no 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
```

O controlador é conectado para conectar o gigabit 5/1 e o gigabit 5/2 no 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
```

As relações de detecção do sensor IPS podem operar-se individualmente no **modo misturado** ou você pode emparelhá-las para criar relações inline para o **modo de detecção Inline**.

No modo misturado, os pacotes não correm através do sensor. O sensor analisa uma cópia do tráfego monitorado um pouco do que o pacote enviado real. A vantagem do funcionamento no modo misturado é que o sensor não afeta o fluxo de pacote de informação com o tráfego enviado.

**Note**: O diagrama da arquitetura é apenas uma instalação do exemplo do WLC e do IPS da arquitetura integrada. O exemplo de configuração mostrado aqui explica o IDS que detecta a relação que atua no modo misturado. O diagrama da arquitetura mostra as relações de detecção que estão sendo emparelhadas junto para atuar no modo Inline dos pares. Refira o modo Inline para obter mais informações sobre do modo Inline da relação.

Nesta configuração, supõe-se que a relação de detecção atua no modo misturado. A relação da monitoração do sensor do Cisco IDS é conectada à interface de gigabit 5/3 no Catalyst 6500. Crie uma sessão de monitor no Catalyst 6500 onde a interface de canal de porta é a fonte dos pacotes e o destino é a interface de gigabit onde a relação da monitoração do sensor do ips Cisco é conectada. Isto replicates todo o ingresso e tráfego de saída das relações prendidas controlador ao IDS para a camada 3 com a inspeção da camada 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#
```

## Configurar o sensor do Cisco IDS

A configuração inicial do sensor do Cisco IDS é feita da porta de Console ou conectando um monitor e um teclado ao sensor.

1. Início de uma sessão ao dispositivo:Conecte uma porta de Console ao sensor.Conecte um monitor e um teclado ao sensor.
2. Datilografe seu nome de usuário e senha na alerta de login.**Note**: O nome de usuário padrão e a senha são ambos Cisco. Você é alertado mudá-los a primeira vez você início de uma sessão ao dispositivo. Você deve primeiramente incorporar a senha Unix, que é Cisco. Então você deve incorporar a senha nova duas vezes.

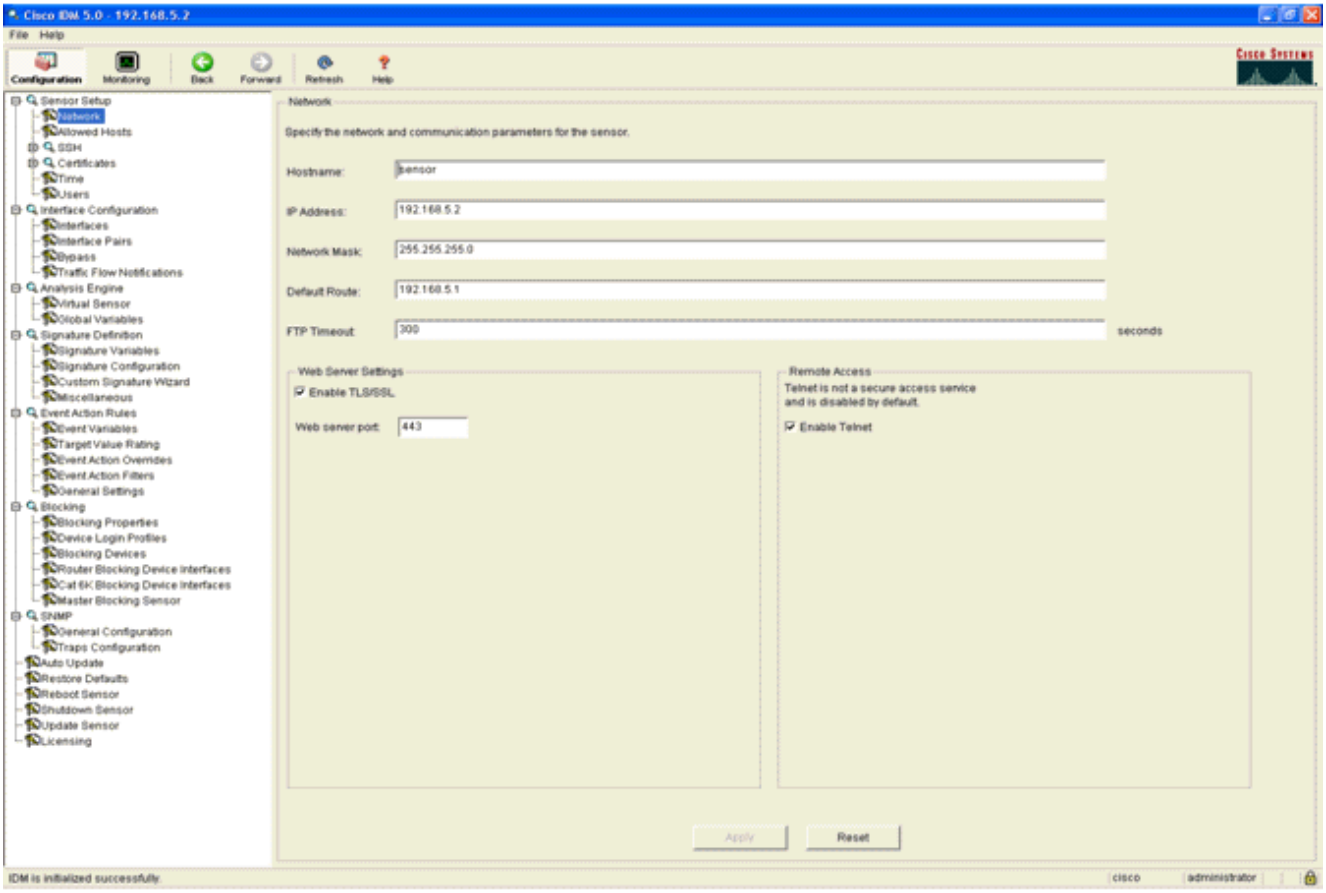
```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. 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. Configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT, a máscara de sub-rede e a lista de acessos no sensor.**Note**: Esta é o comando e a interface de controle no IDS usado para comunicar-se com o controlador. Este endereço deve ser roteável à interface de gerenciamento do controlador. As relações de detecção não exigem o endereçamento. A lista de acessos deve incluir o endereço da interface de gerenciamento dos controladores, assim como endereços permissíveis para o Gerenciamento do IDS.

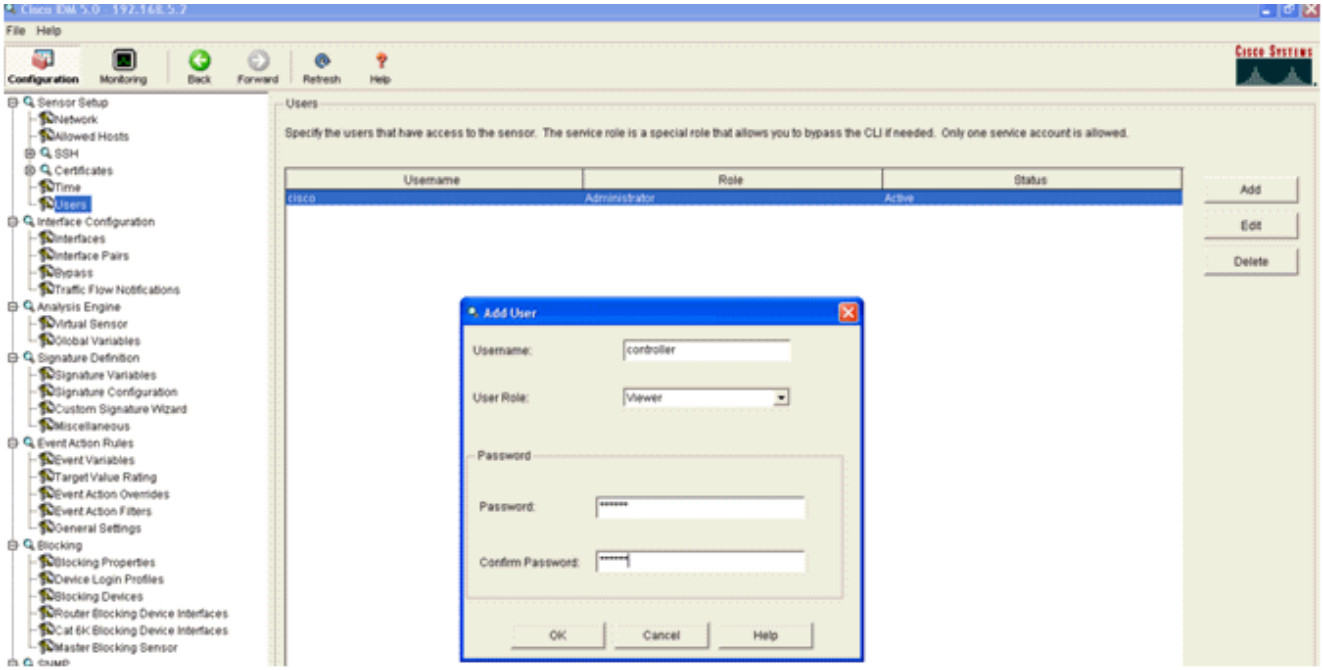
```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
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. Você pode agora configurar o sensor IPS do GUI. Aponte o navegador ao endereço IP de

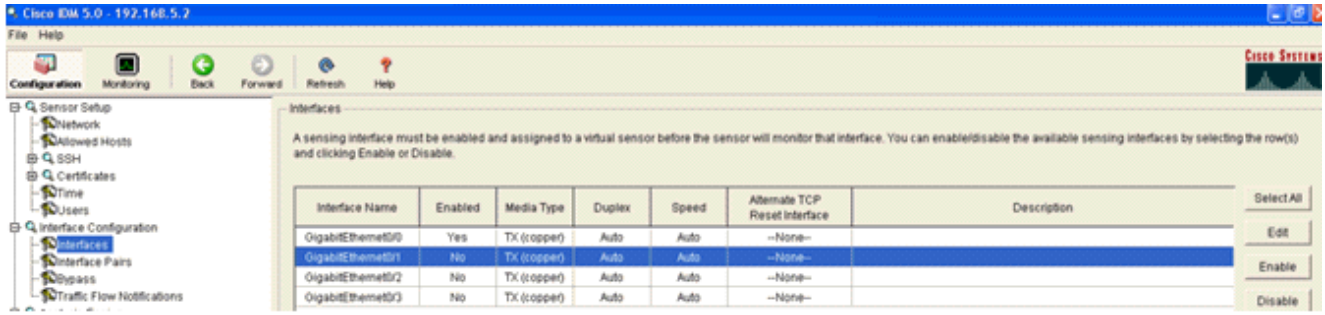
gerenciamento do sensor. Este exibições de imagem uma amostra onde o sensor seja configurado com
192.168.5.2.



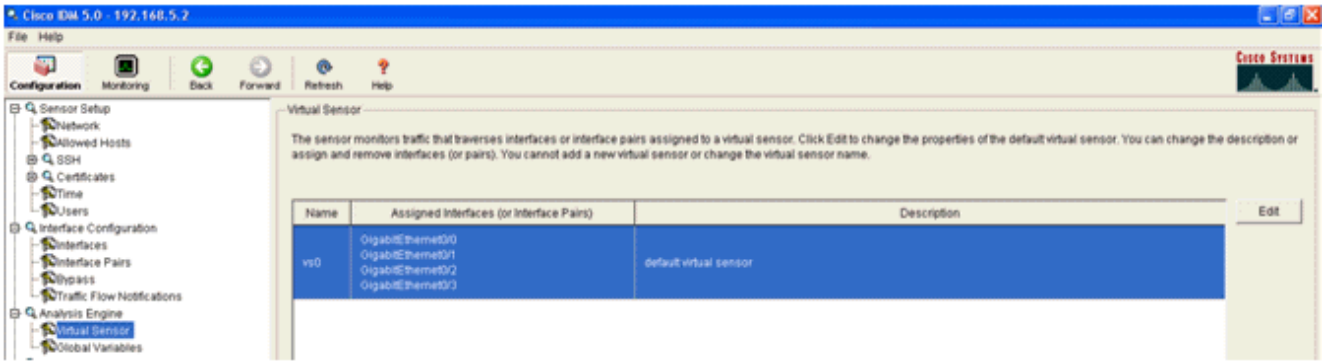

5. Adicionar um usuário que o WLC se use para alcançar os eventos do sensor IPS.



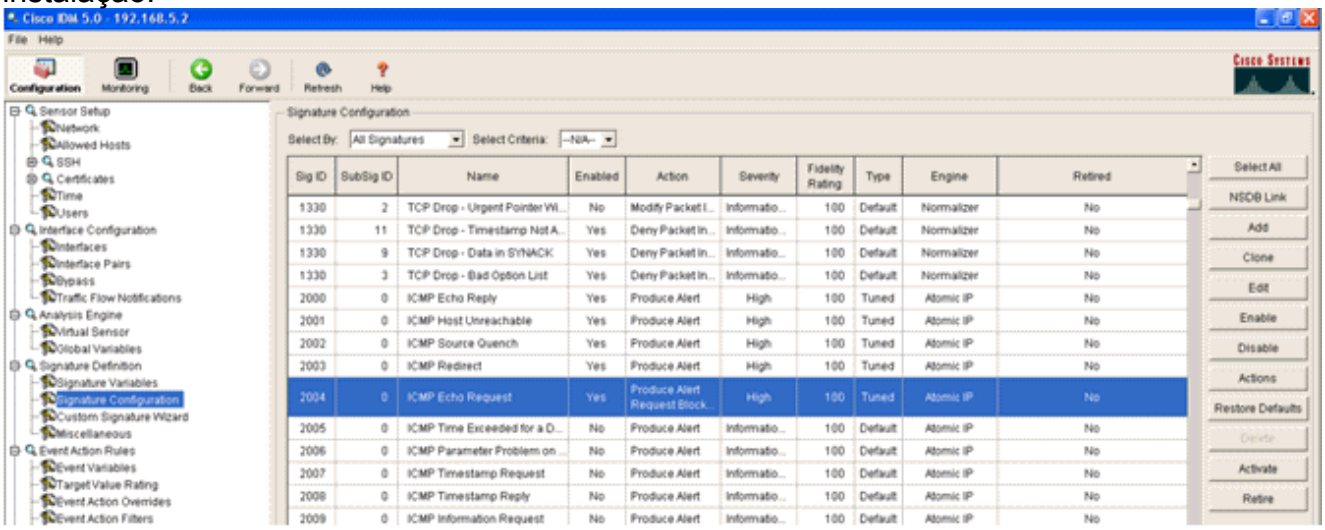

6. Permita as relações da monitoração.



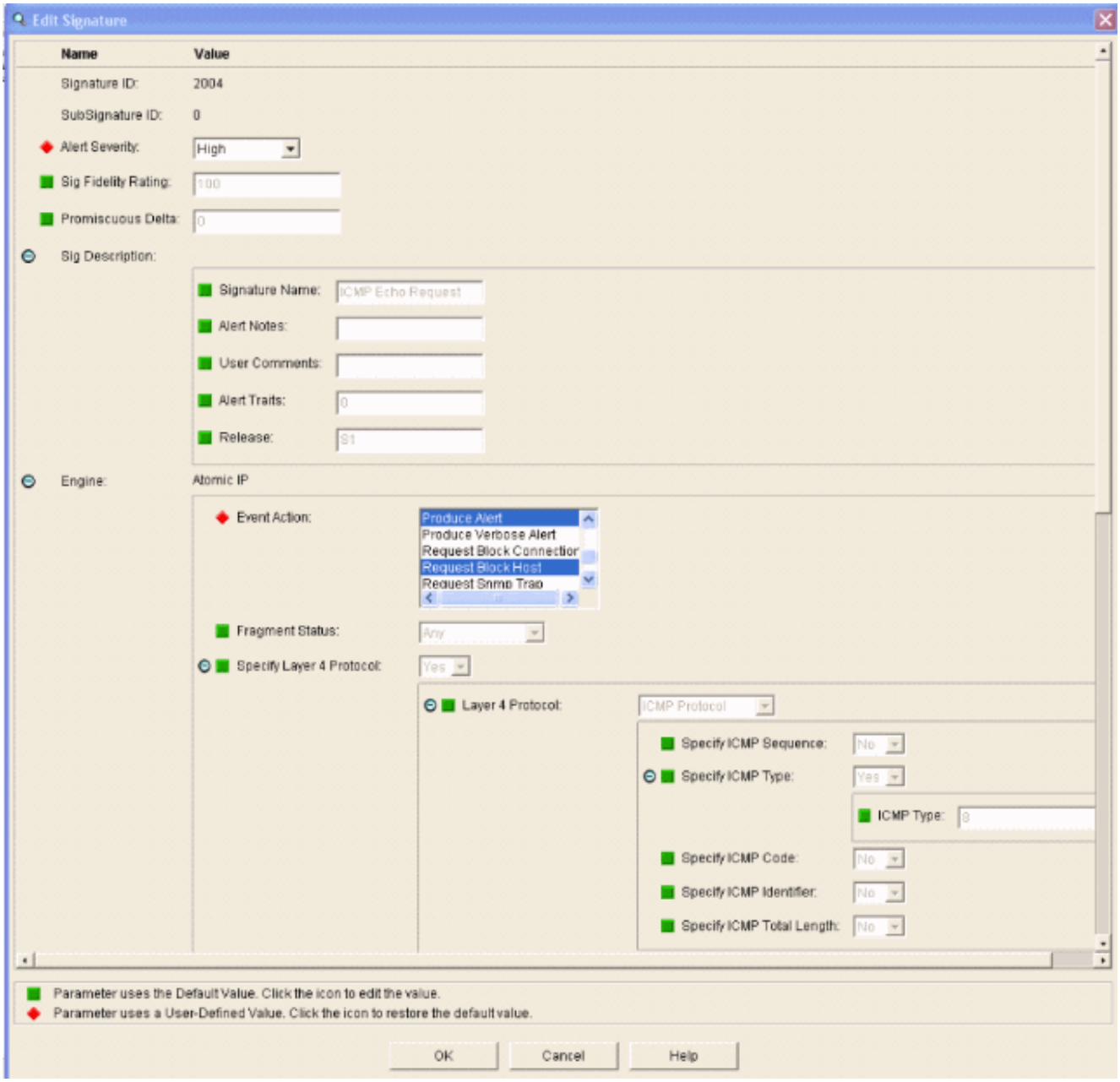

As relações da monitoração devem ser adicionadas ao motor da análise, porque este indicador
mostra:




7. Selecione a assinatura 2004 (requisição de eco ICMP) a fim executar uma verificação rápida da
instalação.




A assinatura deve ser permitida, grupo alerta da severidade à **elevação** e grupo da ação do evento **de produzir o host do bloco do alerta** e de **pedido** para que este passo de verificação seja
terminado.

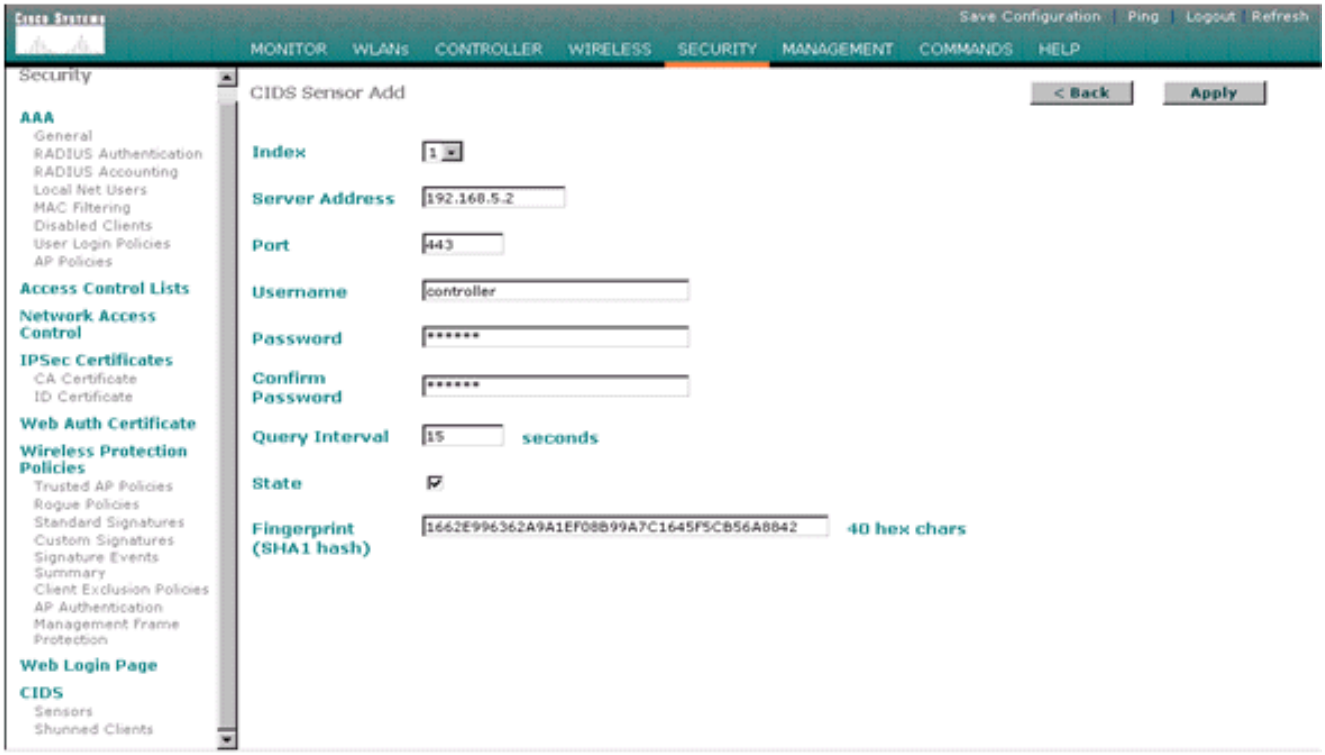



## Configurar o WLC

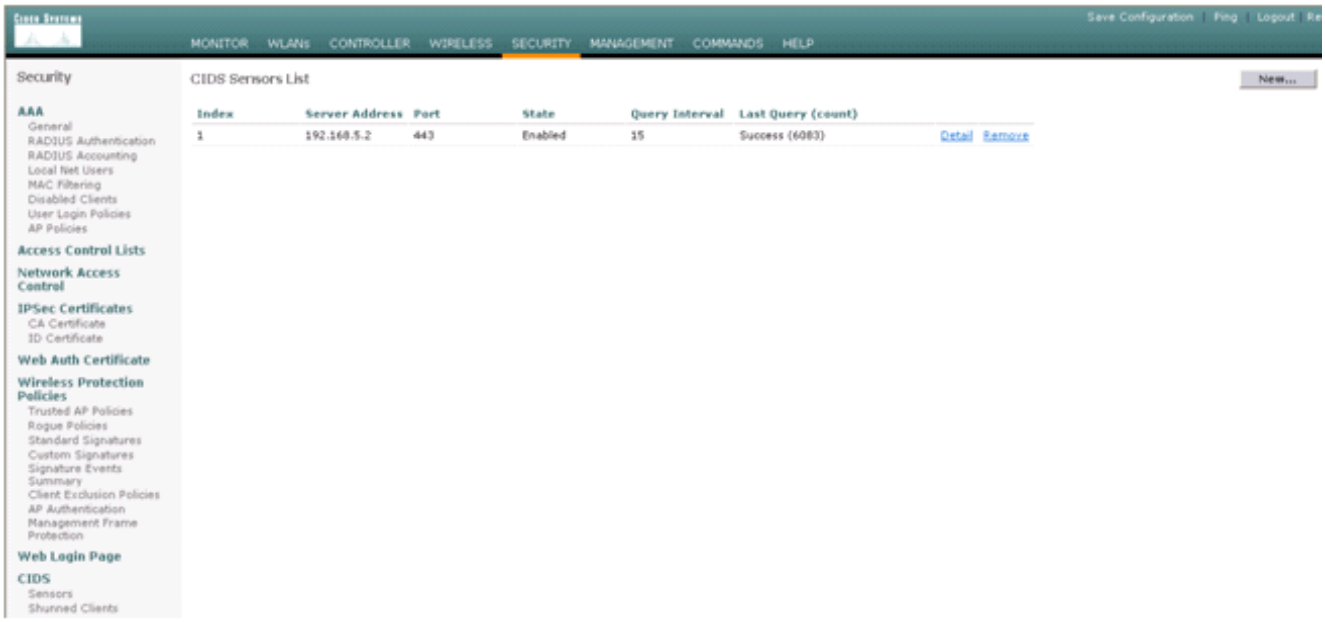
Termine estas etapas a fim configurar o WLC:

1. Uma vez que o dispositivo IPS é configurado e se apronta para ser adicionado no controlador, escolha a **Segurança > os CID > os sensores > novo**.
2. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT, número de porta de TCP, nome de usuário e senha que você criou previamente.A fim obter a impressão digital do sensor IPS, execute este comando no sensor IPS e adicionar a impressão digital SHA1 no WLC (sem os dois pontos). Isto é usado para fixar a comunicação da votação controlador-à-IDS.

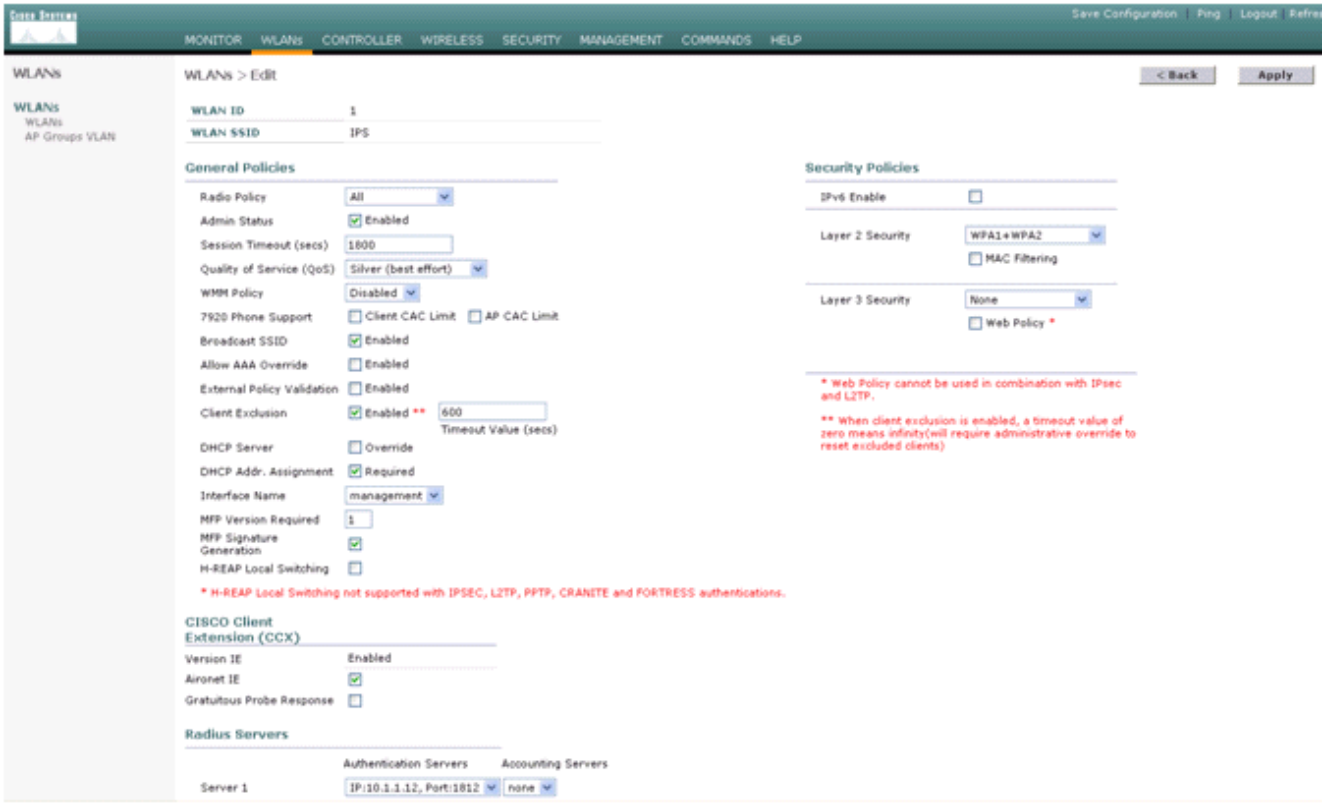
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



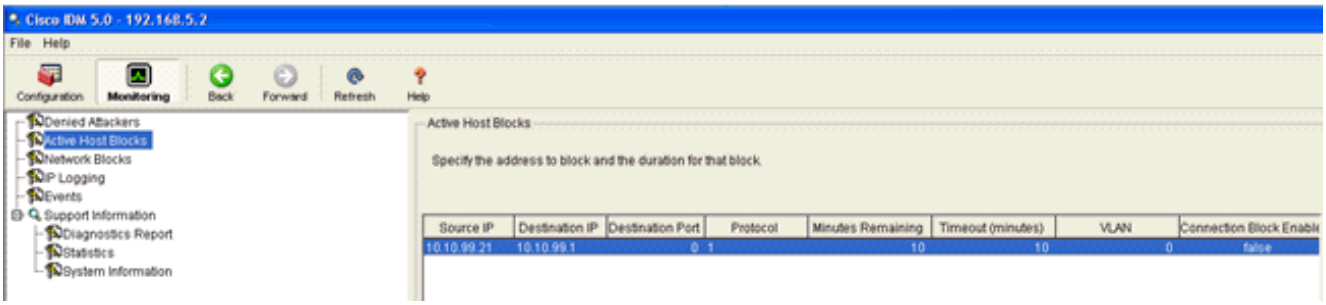

3. Verifique o estado da conexão entre o sensor IPS e o WLC.



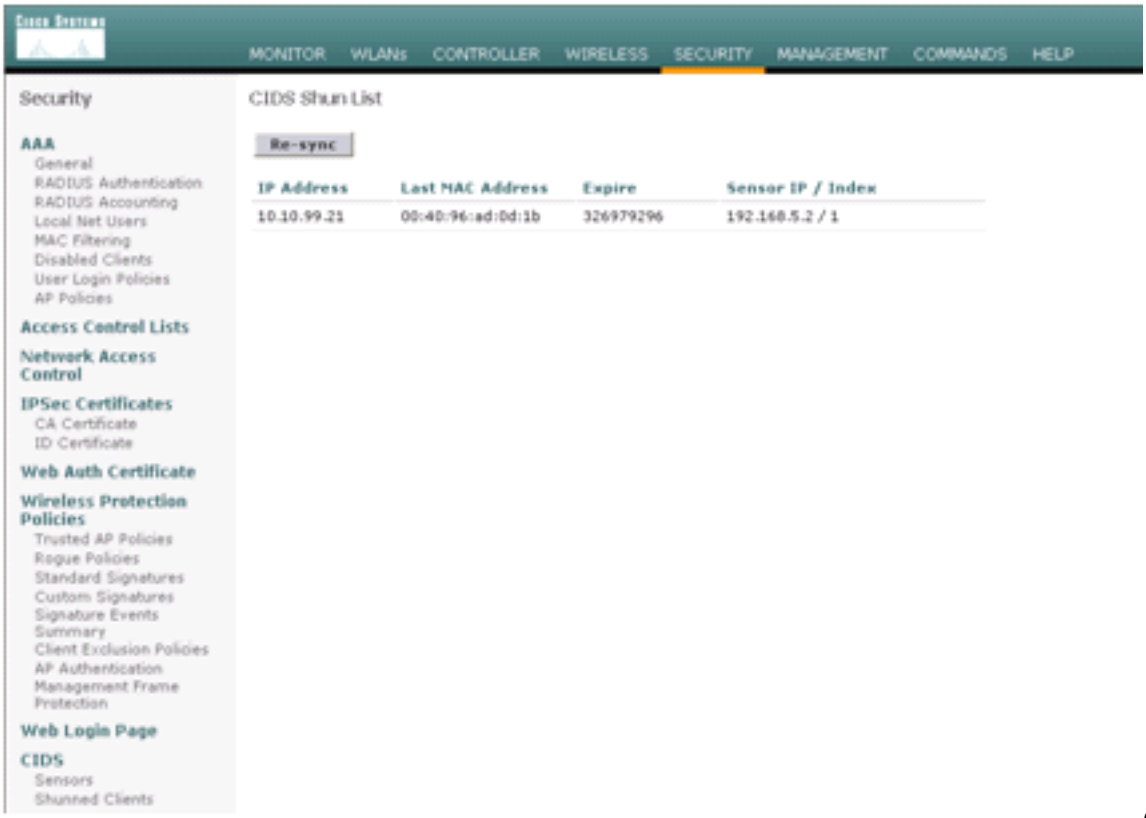

4. Uma vez que você estabelece a Conectividade com o sensor do ips Cisco, certifique-se que a configuração WLAN está correta e isso você permite a **exclusão do cliente**.O valor de timeout da exclusão do cliente do padrão é 60 segundos. Igualmente note que apesar do temporizador da exclusão do cliente, a exclusão do cliente persiste enquanto o bloco do cliente invocado pelo IDS permanece ativo. O tempo do bloco do padrão no IDS é 30 minutos.



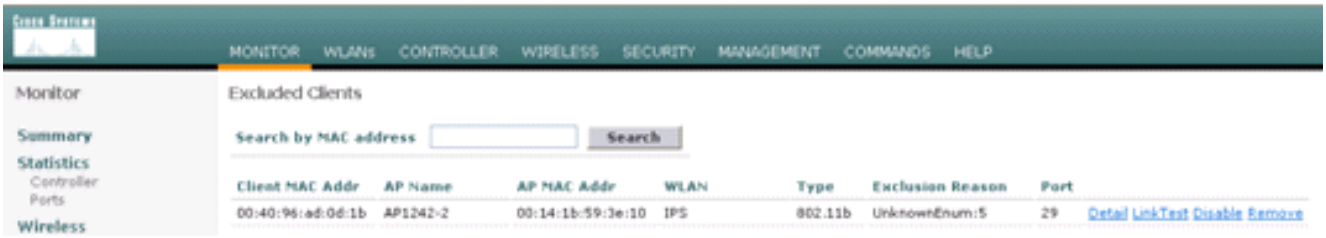

5. Você pode provocar um evento no sistema do ips Cisco qualquer um quando você faz uma varredura NMAP a determinados dispositivos na rede ou quando você faz um sibilo a alguns anfitriões monitorados pelo sensor do ips Cisco. Uma vez que um alarme é provocado no ips Cisco, vá aos **blocos da monitoração e do host ativo** a fim verificar os detalhes sobre o host.




Os clientes evitados alistam no controlador são povoados agora com o IP e o MAC address

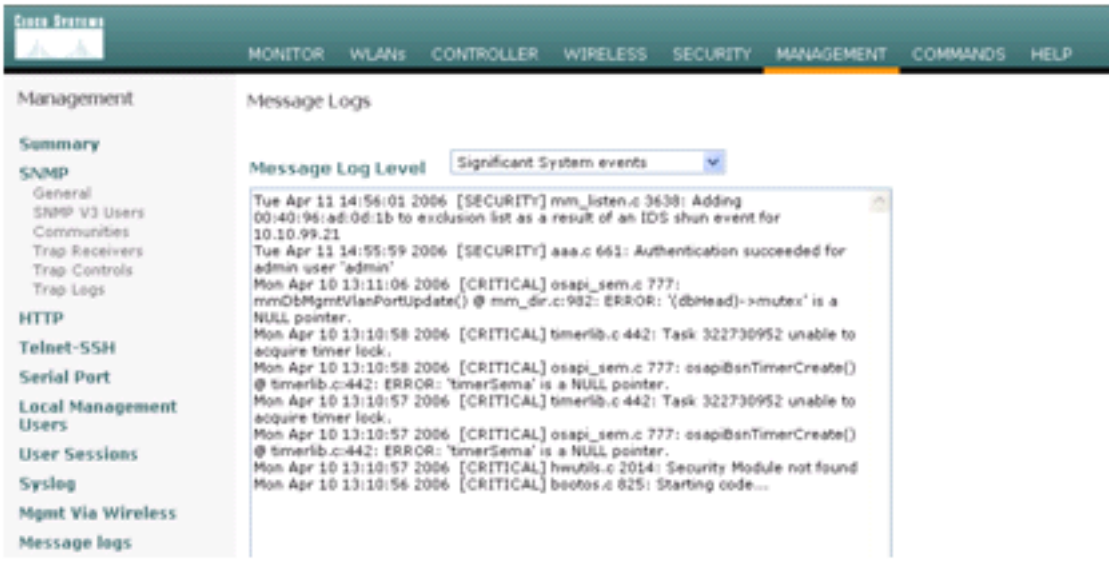



do host. O usuário é adicionado à lista da exclusão do cliente.

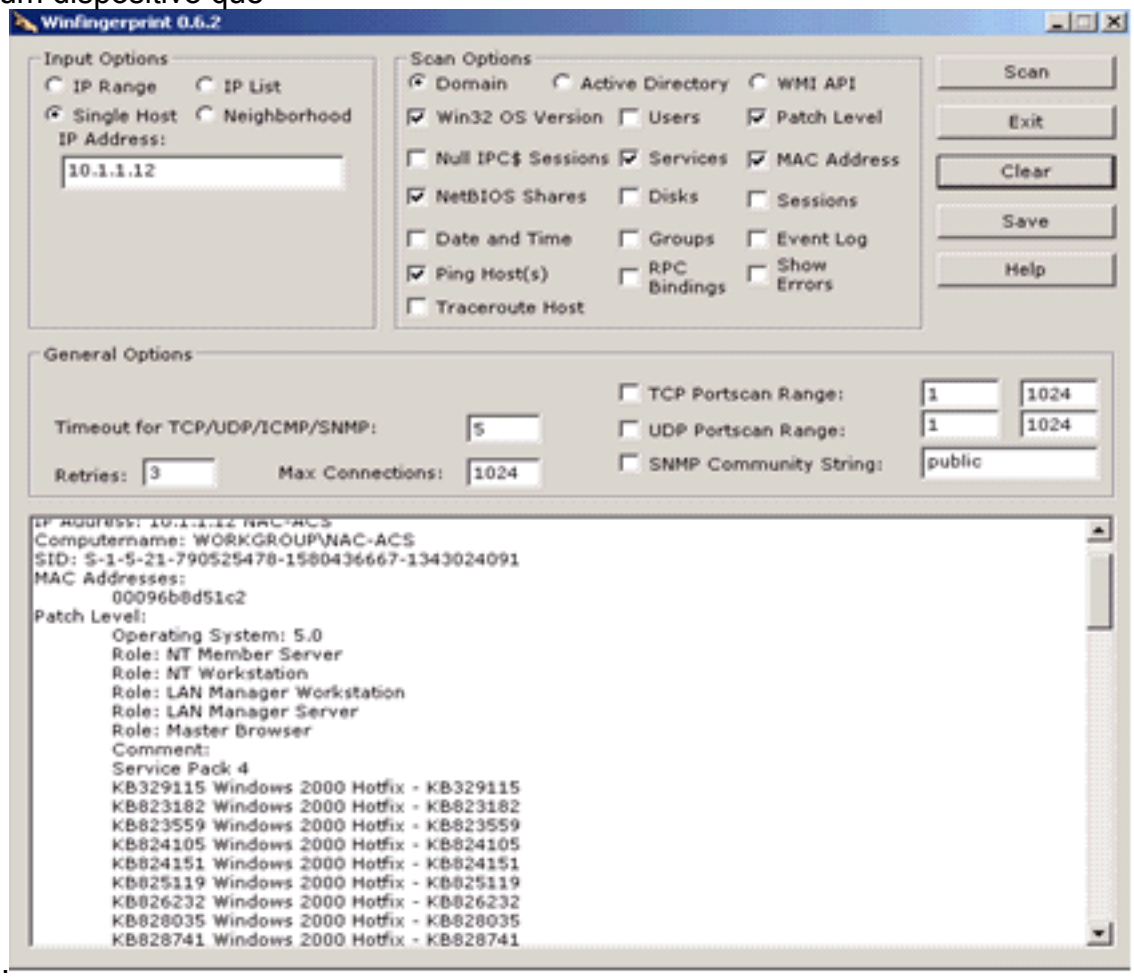



Um log da armadilha é gerado enquanto um cliente é adicionado à lista

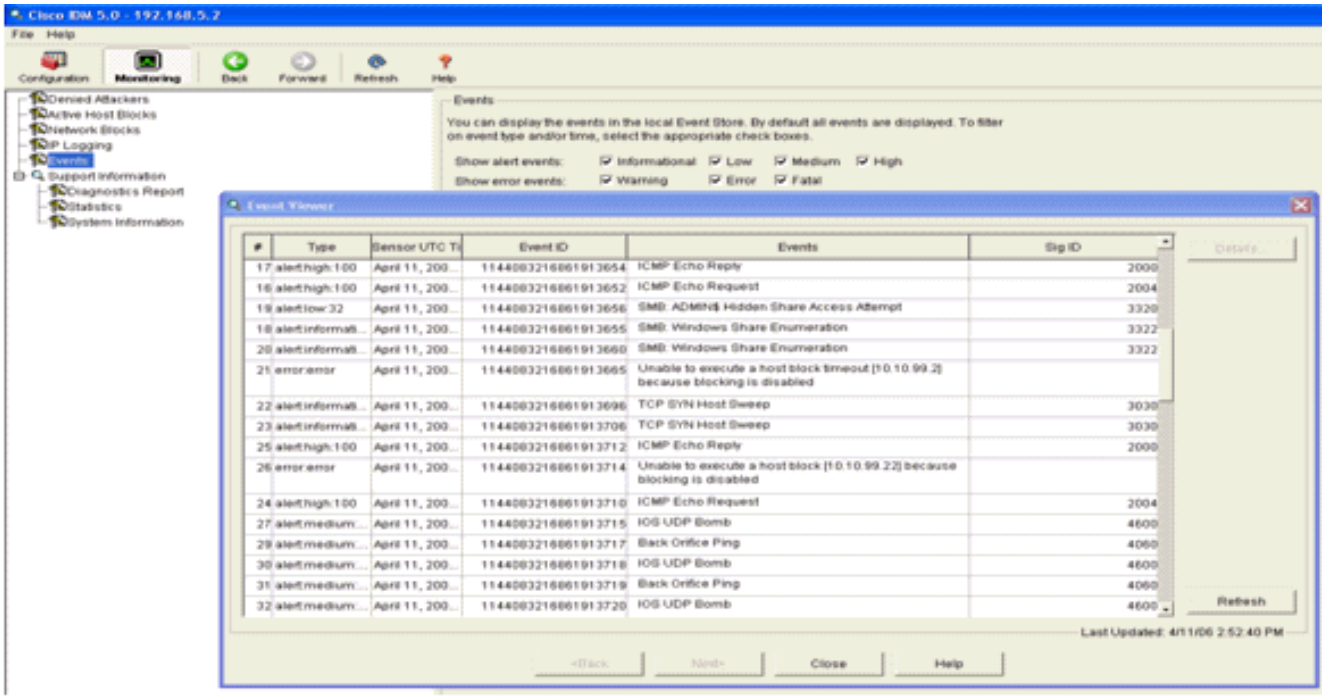

evitar. Um log de mensagens é gerado igualmente para o




evento. Alguns eventos adicionais estão gerados no sensor do ips Cisco quando uma varredura NMAP é feita em um dispositivo que




monitore. Este indicador mostra os eventos gerados no sensor do ips Cisco.




## Configuração de exemplo do sensor do Cisco IDS

Esta é a saída do script de instalação da instalação:

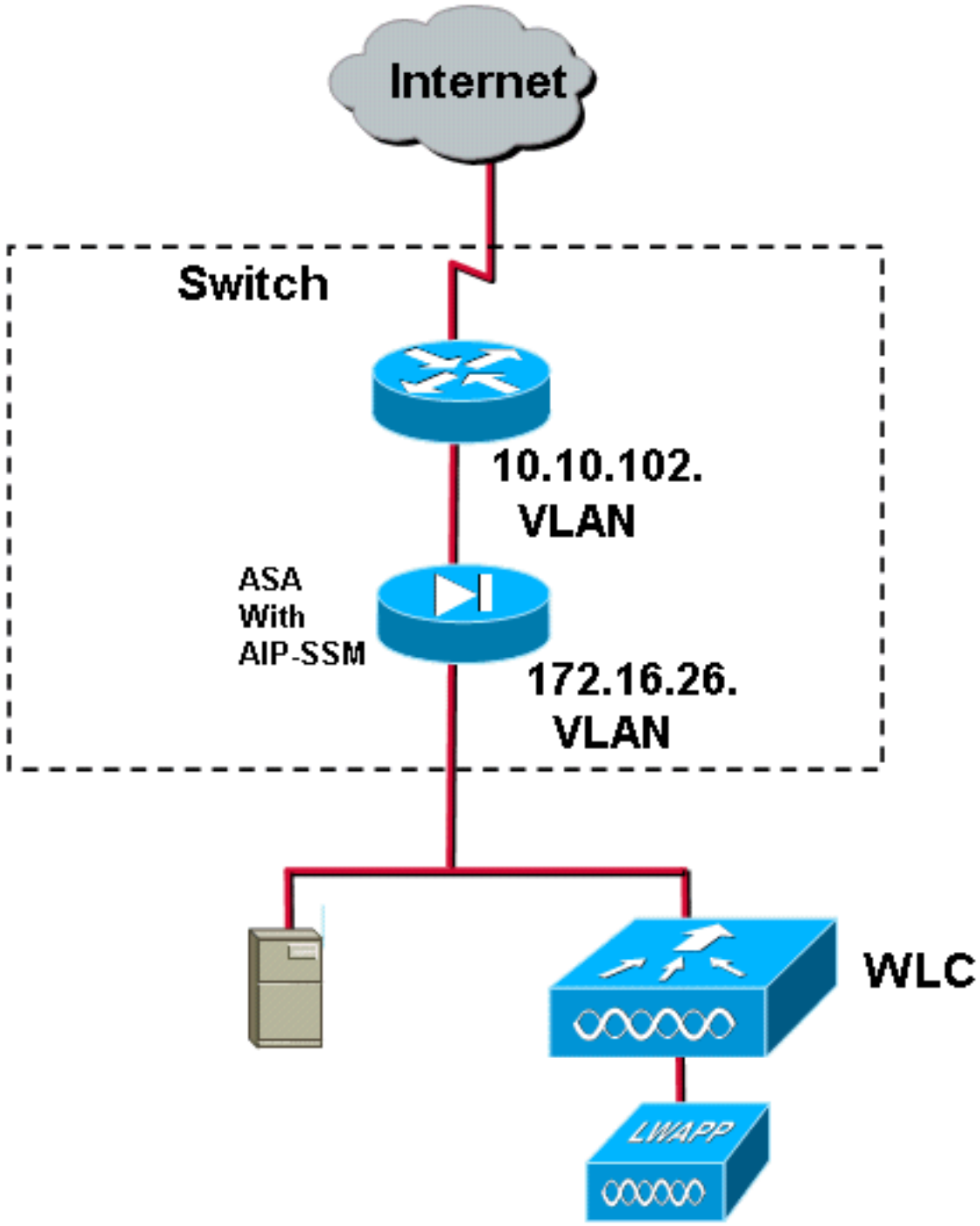
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list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

## Configurar um ASA para o IDS

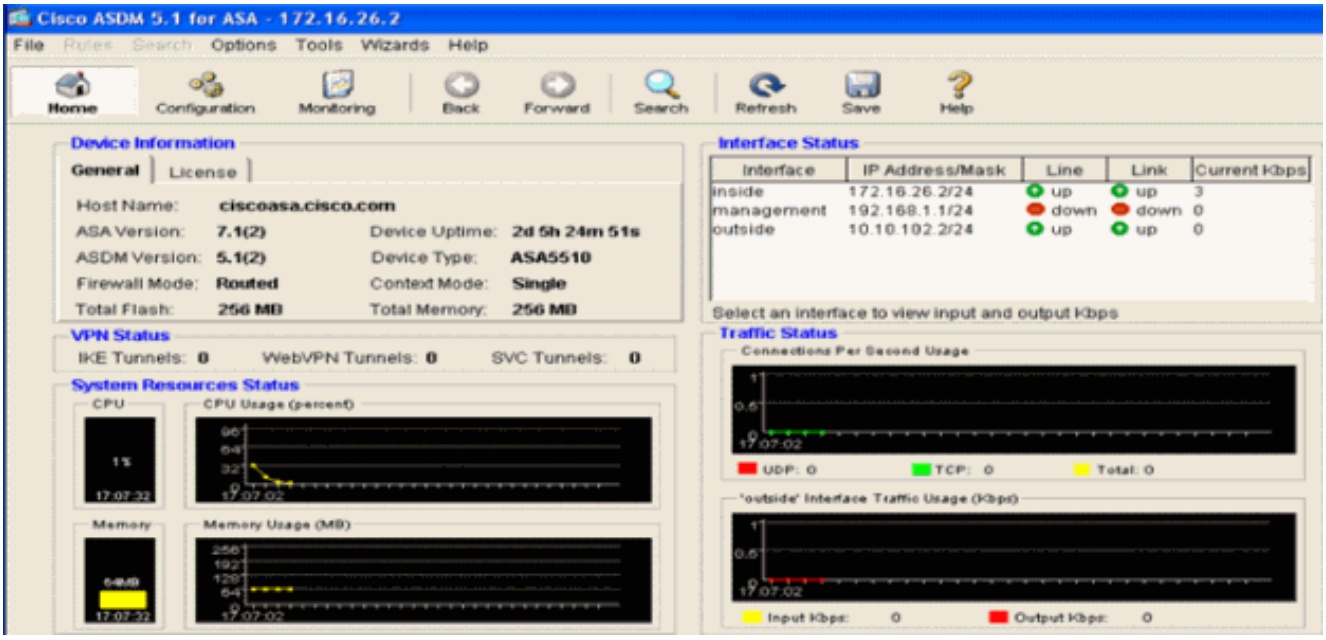
Ao contrário de um sensor tradicional da intrusion detection, um ASA deve sempre estar no trajeto de dados. Ou seja em vez de medir o tráfego de uma porta de switch sobre a uma porta passiva

do sniffing no sensor, o ASA deve receber dados em uma relação, processa-a internamente, e envia-lhe então para fora uma outra porta. Para o IDS, use a estrutura de política modular (MPF) a fim copiar o tráfego que o ASA recebe sobre ao módulo de Serviços de segurança avançado interno da inspeção e da prevenção (AIP-SSM) para a inspeção.

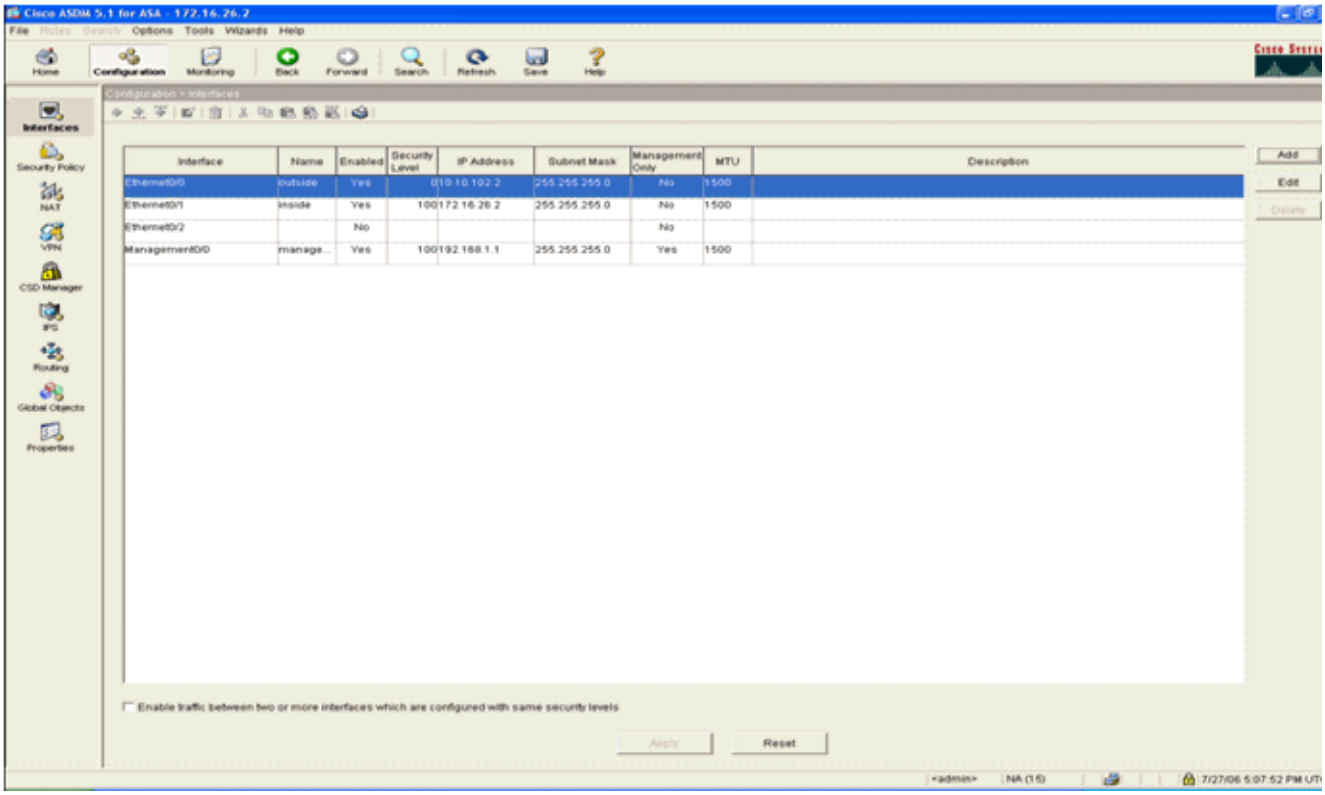



Neste exemplo, o ASA usado já setup e passa o tráfego. Estas etapas demonstram como criar uma política que envie dados ao AIP-SSM.

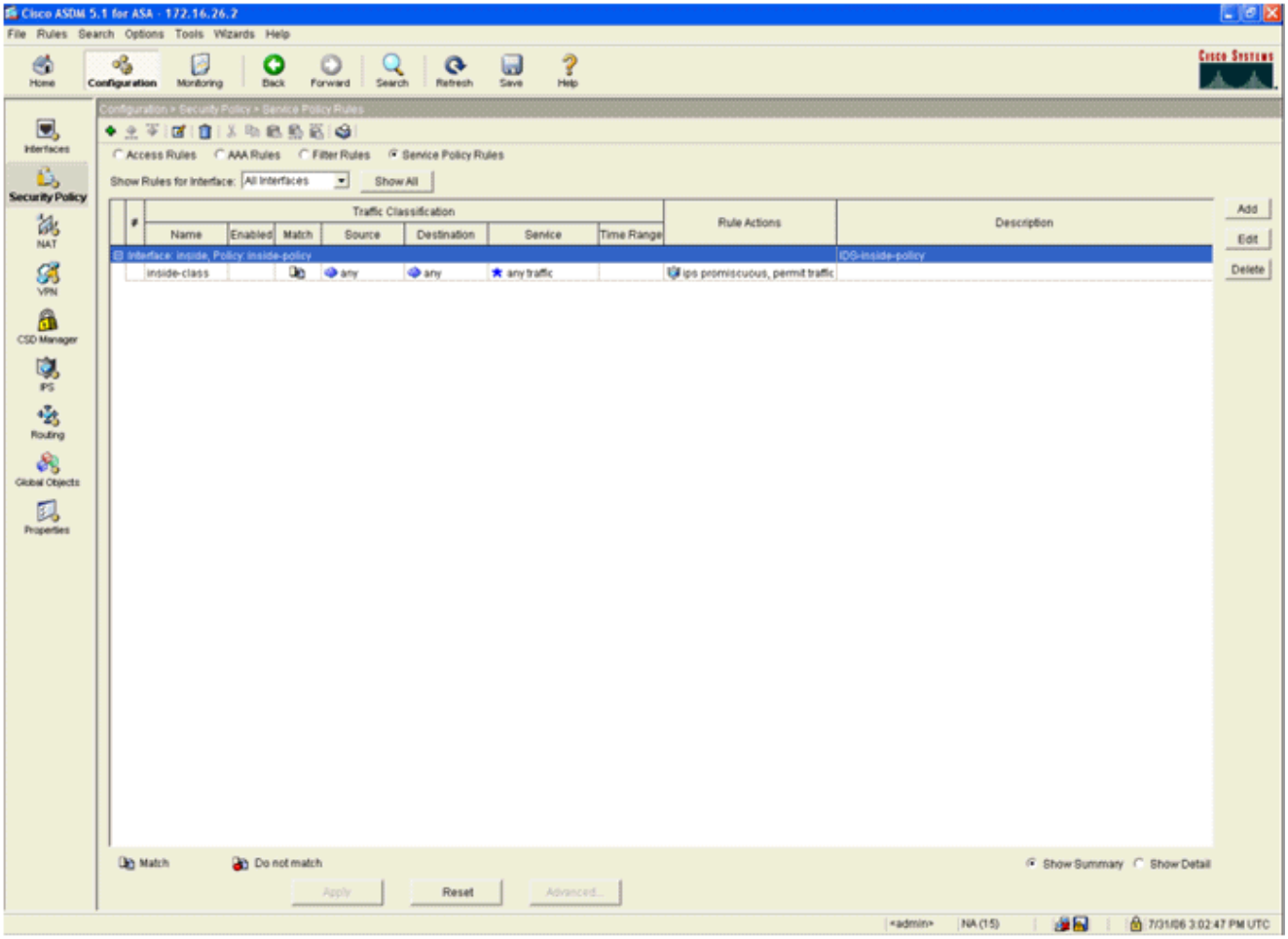
1. Log no ASA usando o ASDM. Em cima do login bem-sucedido, o indicador do sistema principal ASA
   aparece.



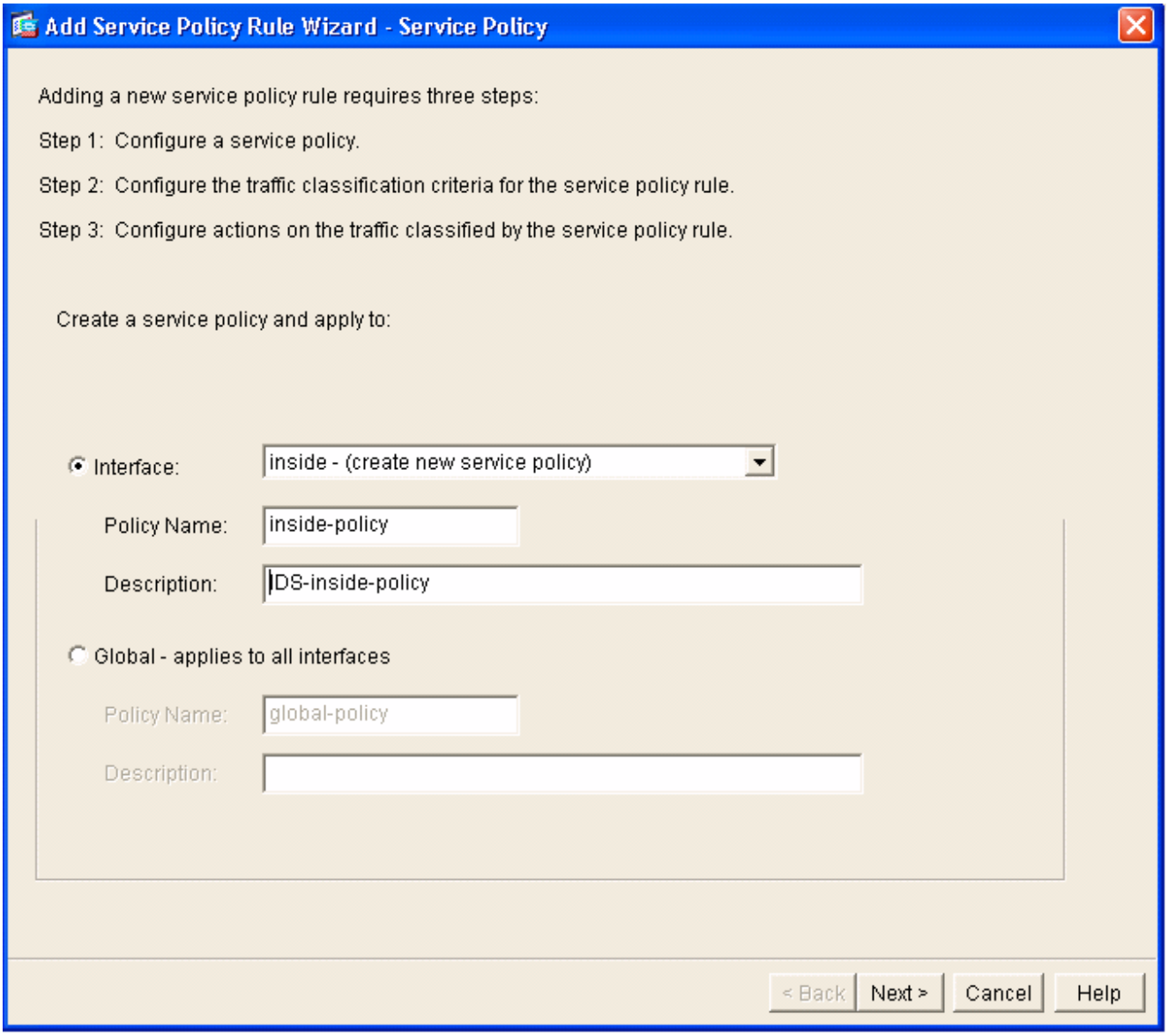

2. Clique a **configuração na** parte superior da página. O indicador comuta a uma ideia das relações
ASA.



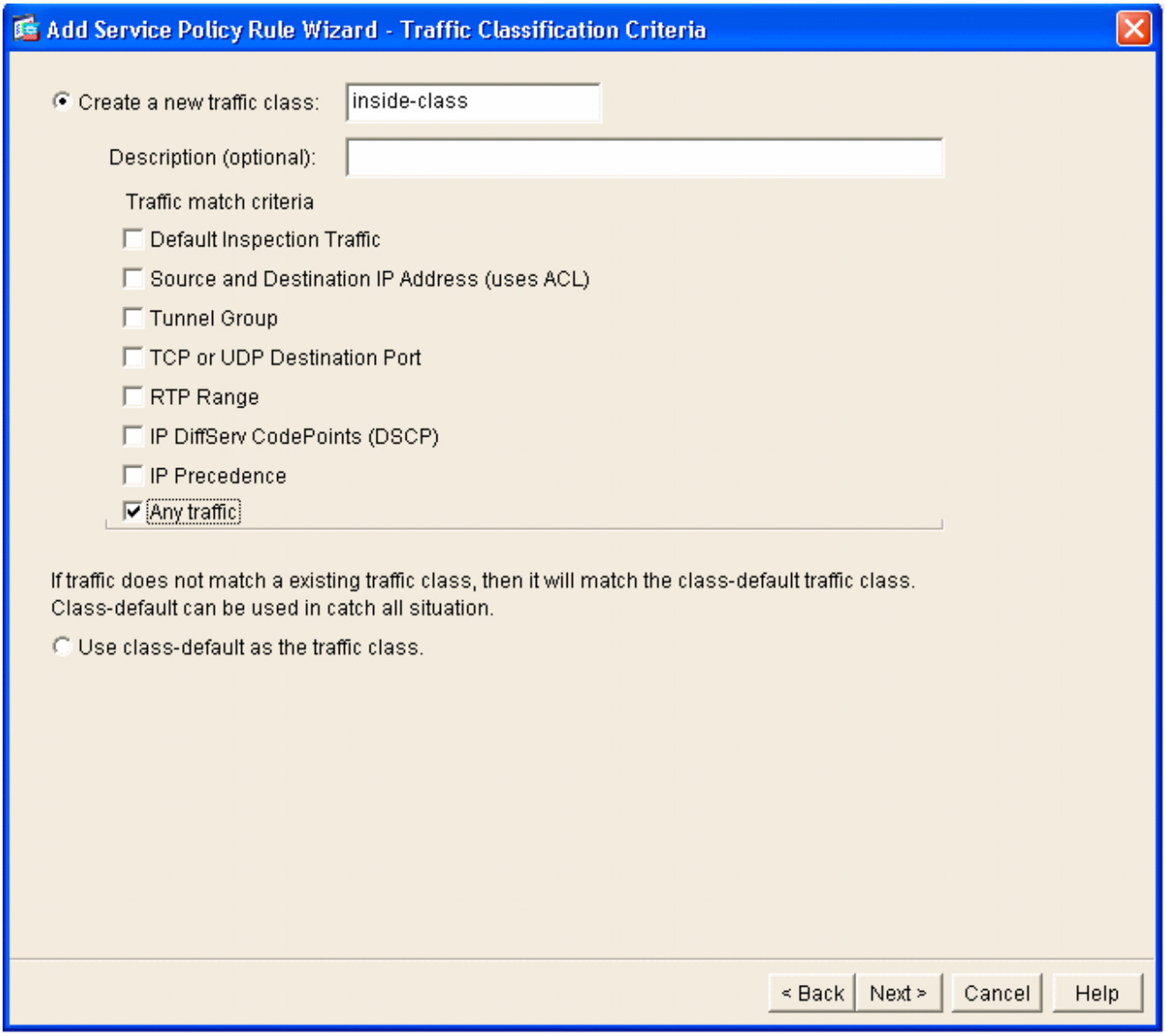

3. Clique a **política de segurança no** lado esquerdo do indicador. No indicador resultante, escolha a aba das **regras da política de serviços**.



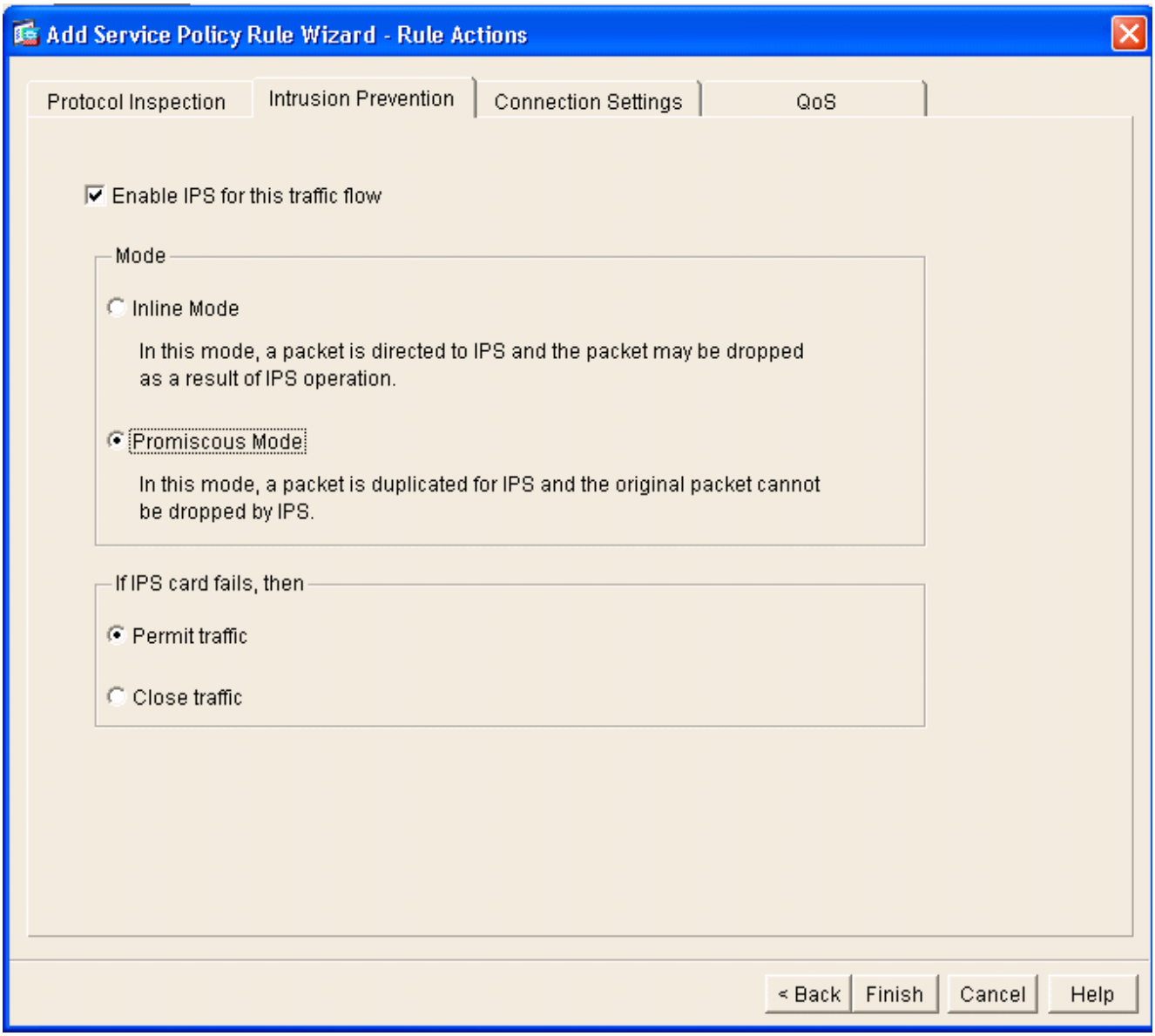

4. O clique **adiciona** a fim criar uma política nova. O assistente da regra da política de serviços adicionar lança-se em uma nova janela.Clique a **relação** e escolha então a relação correta da lista de drop-down a fim criar uma política nova que seja limitada a uma das relações que passa o tráfego.Dê à política um nome e uma descrição do que a política faz usando as duas caixas de texto.Clique **em seguida** a fim mover-se para a próxima etapa.



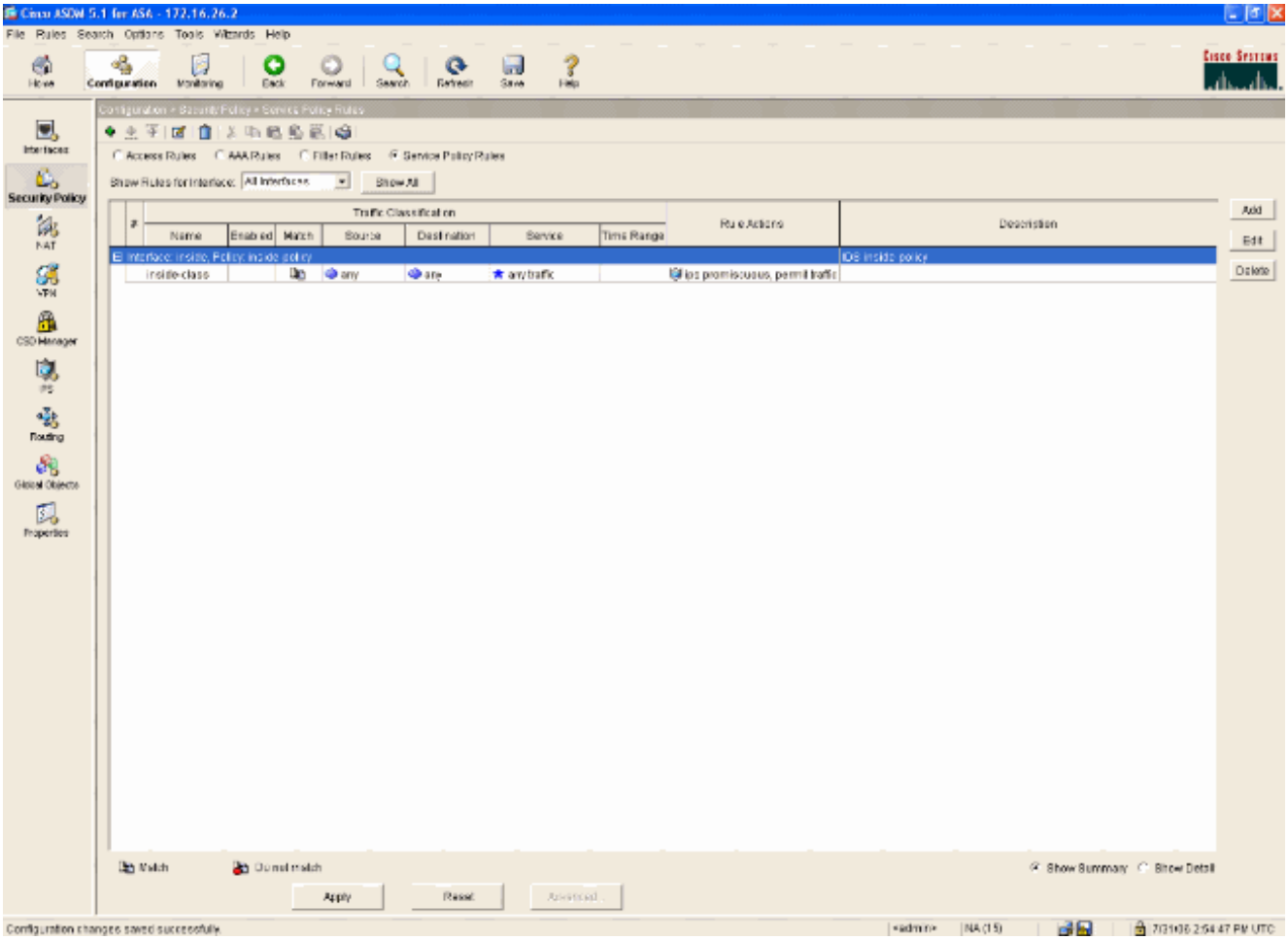

5. Construa uma classe de tráfego nova para aplicar-se à política.Érazoável construir classes específicas a fim inspecionar tipos de dados específicos, mas neste exemplo, todo o tráfego é selecionado para a simplicidade. Clique **em seguida** a fim continuar.




6. Termine estas etapasinstrua o ASA para dirigir sobre o tráfego a seu AIP-SSM.A verificação **permite o IPS para este fluxo de tráfego** a fim permitir a intrusion detection.Ajuste o modo a **promíscuo** de modo que uma cópia do tráfego seja enviada ao módulo fora da banda em vez de colocar o módulo inline com o fluxo de dados.Clique o **tráfego da licença** a fim assegurar-se de que o ASA comute a um estado falha-aberto caso o AIP-SSM falhar.Clique o **revestimento** a fim comprometer a
mudança.



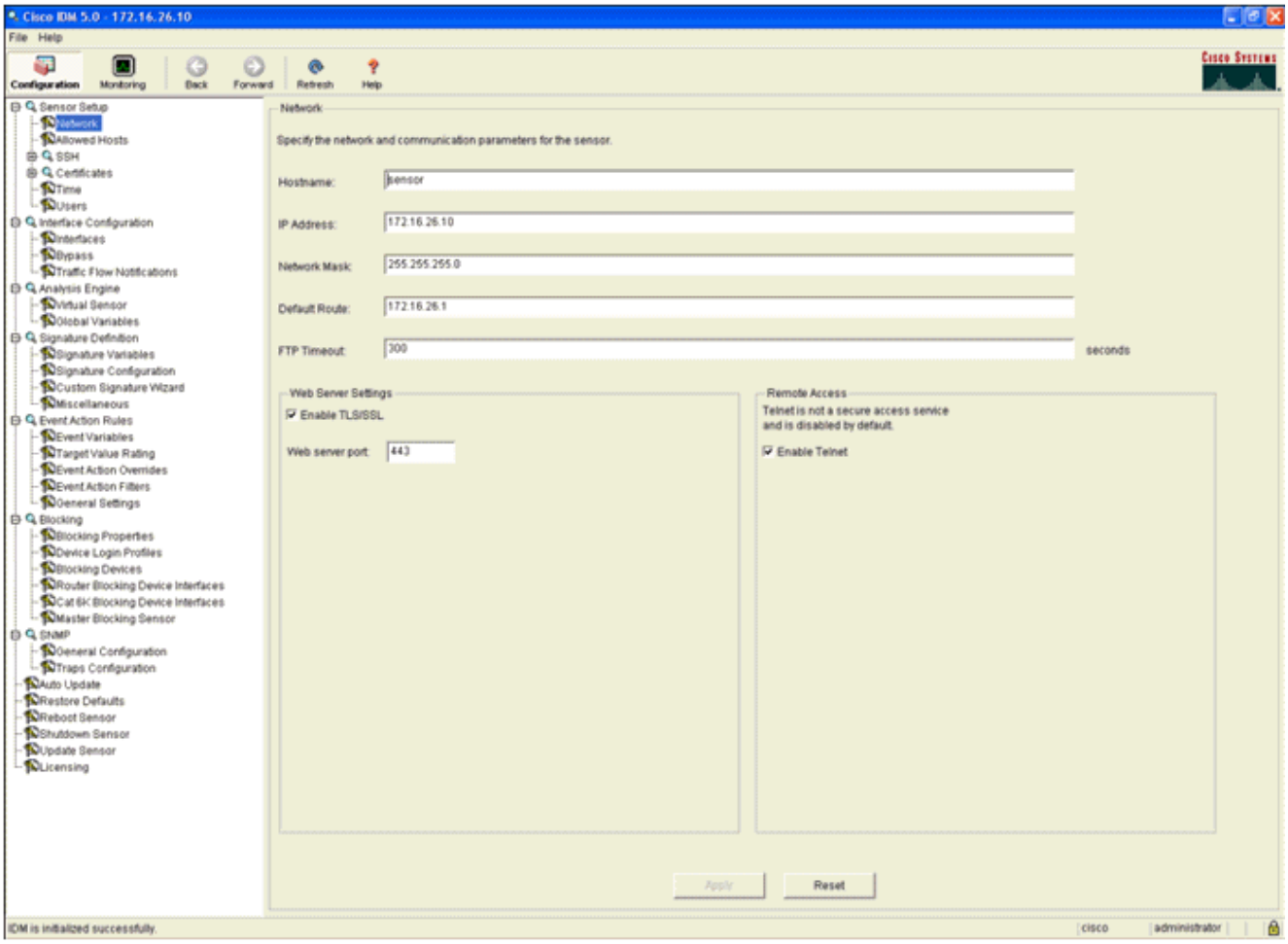

7. O ASA é configurado agora para enviar o tráfego ao módulo ips. **Salvaguarda do** clique na fileira superior a fim escrever as mudanças ao
ASA.



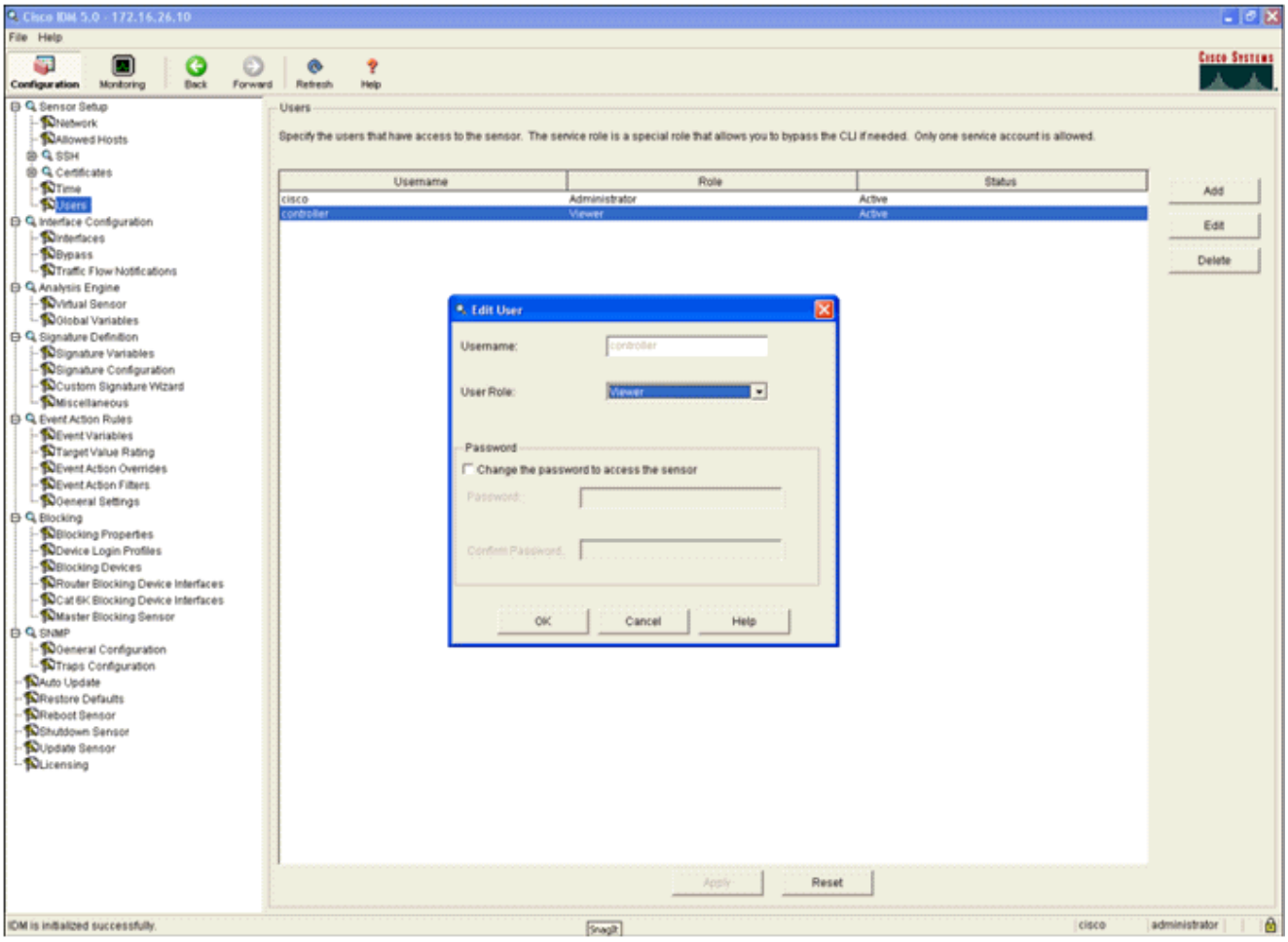

## Configurar o AIP-SSM para a inspeção do tráfego

Quando o ASA enviar dados ao módulo ips, associe a relação AIP-SSM a seu motor virtual do sensor.

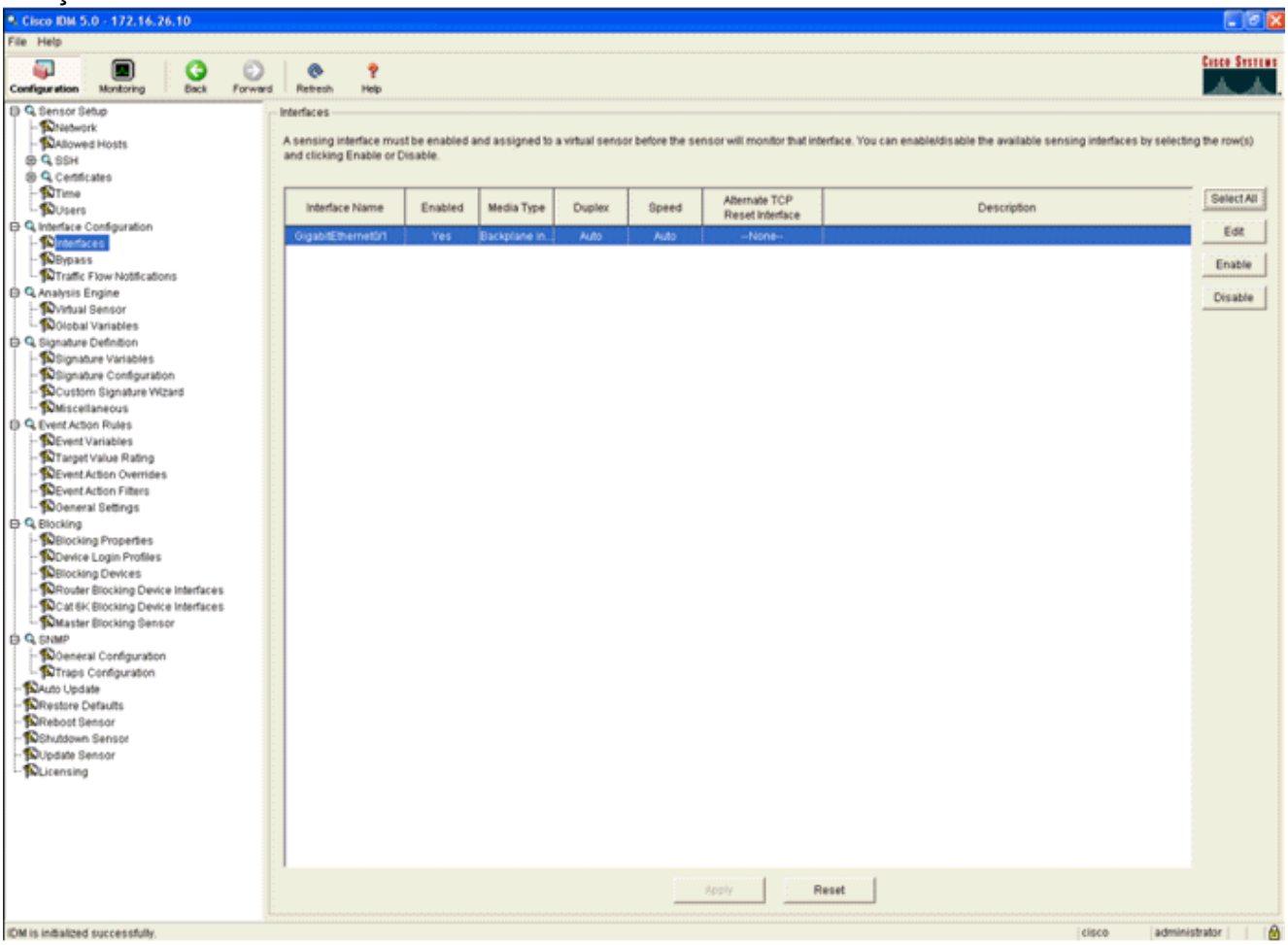
1. Entre ao AIP-SSM usando o
   IDM.



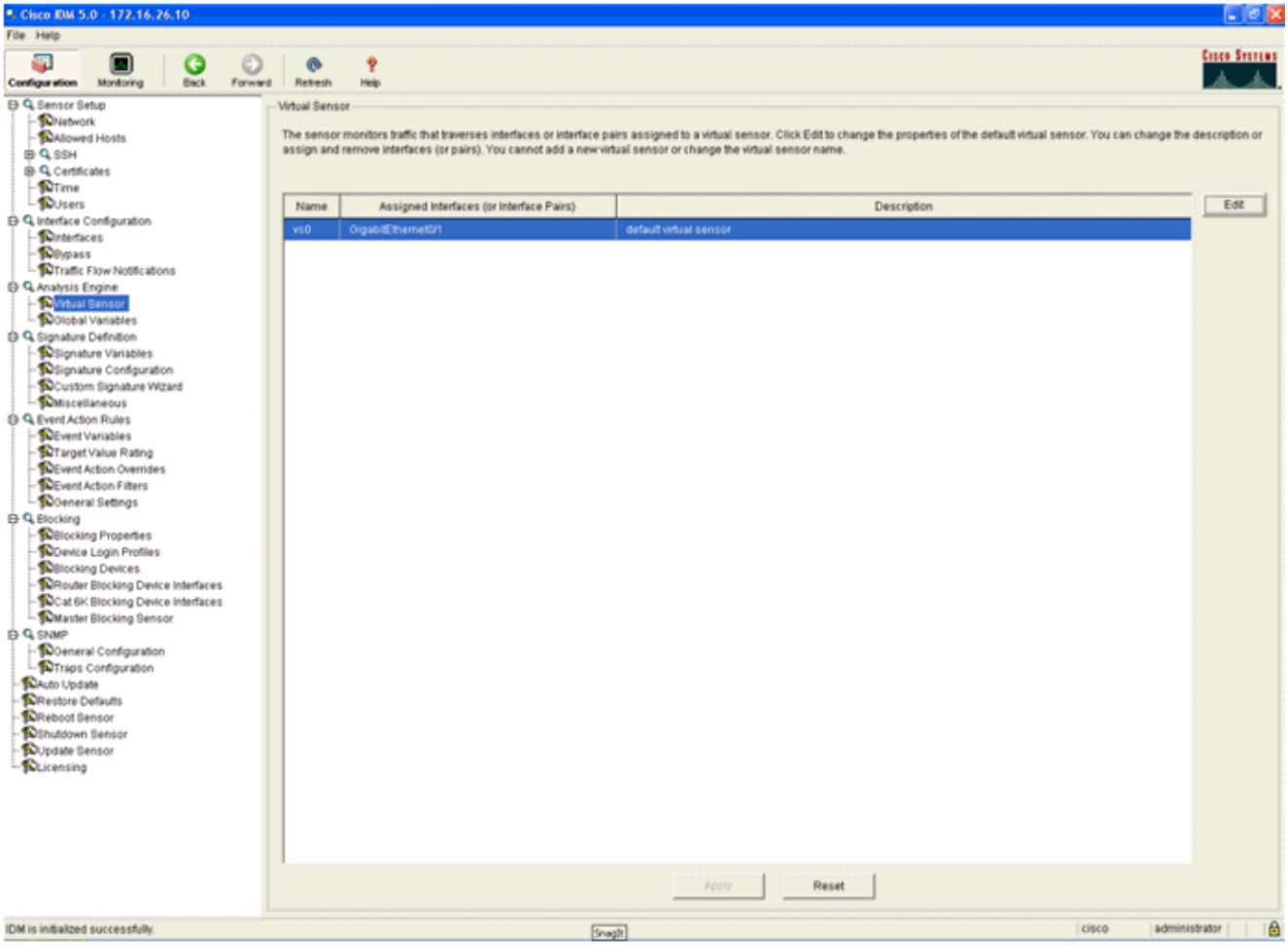

2. Adicionar um usuário com pelo menos privilégios do visor.



3. Permita a relação.




4. Verifique a configuração de Sensor Virtual.

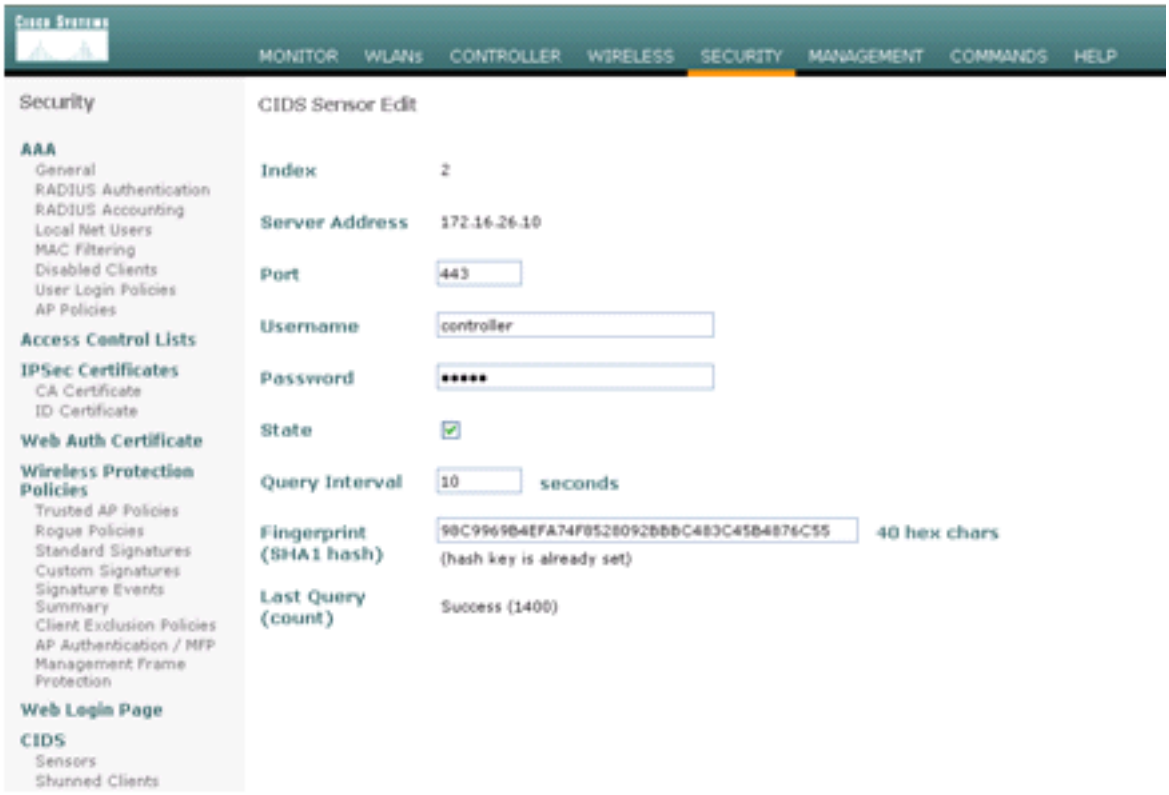



## Configurar um WLC para votar o AIP-SSM para blocos do cliente

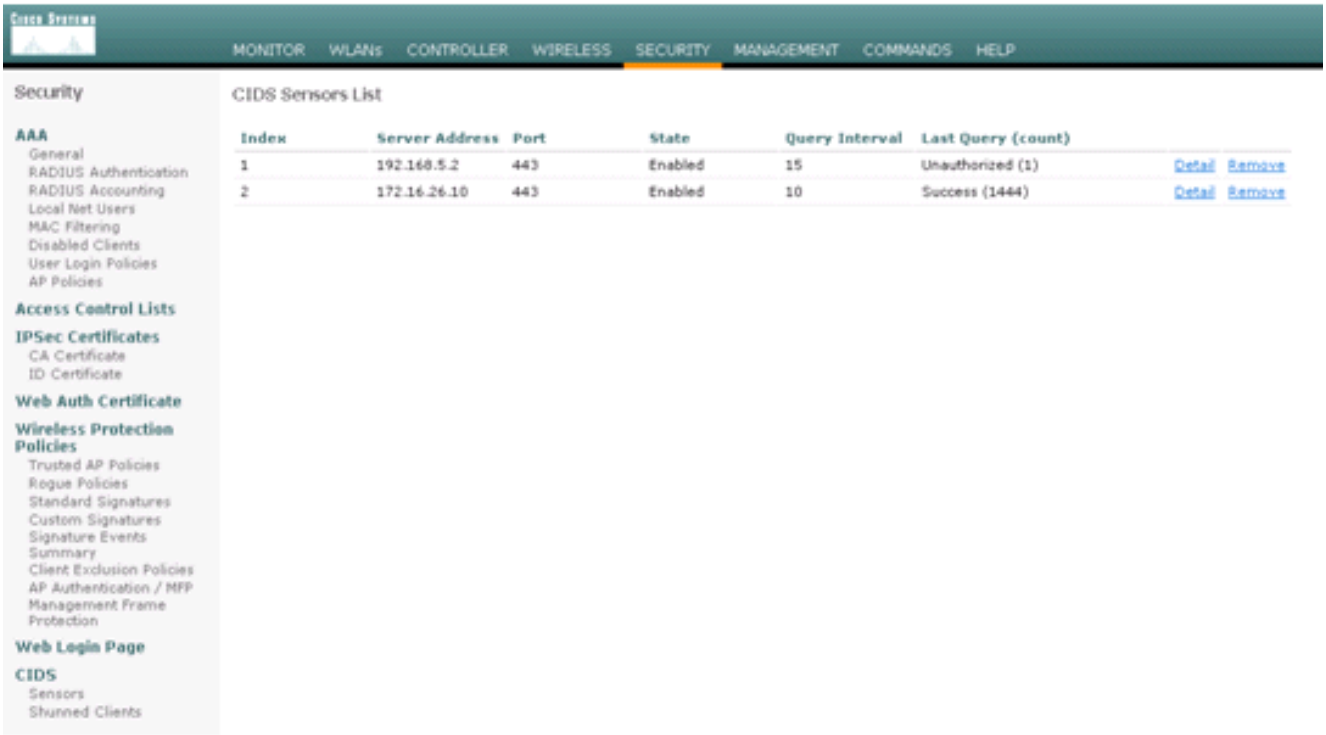
Termine estas etapas uma vez que o sensor é configurado e apronte-as para ser adicionadas no controlador:

1. Escolha a **Segurança > os CID > os sensores > novo no** WLC.
2. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT, número de porta de TCP, nome de usuário e senha que você criou na seção anterior.
3. A fim obter a impressão digital do sensor, execute este comando no sensor e adicionar a impressão digital SHA1 no WLC (sem os dois pontos). Isto é usado para fixar a comunicação da votação controlador-à-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. Verifique o estado da conexão entre o AIP-SSM e o WLC.

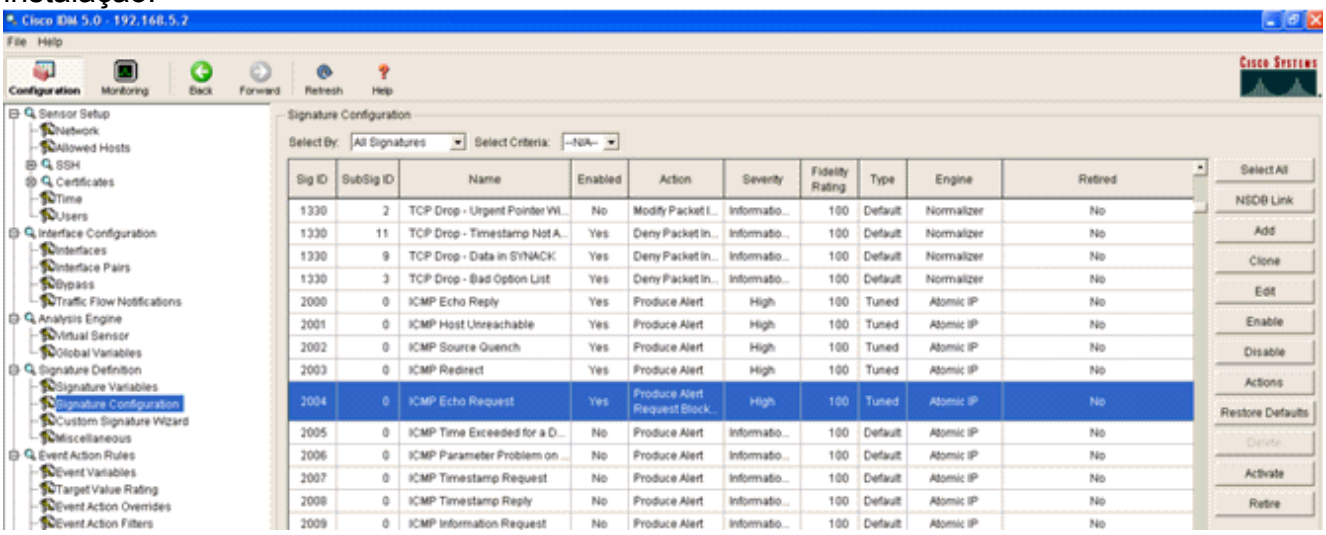



## Adicionar uma assinatura de obstrução ao AIP-SSM

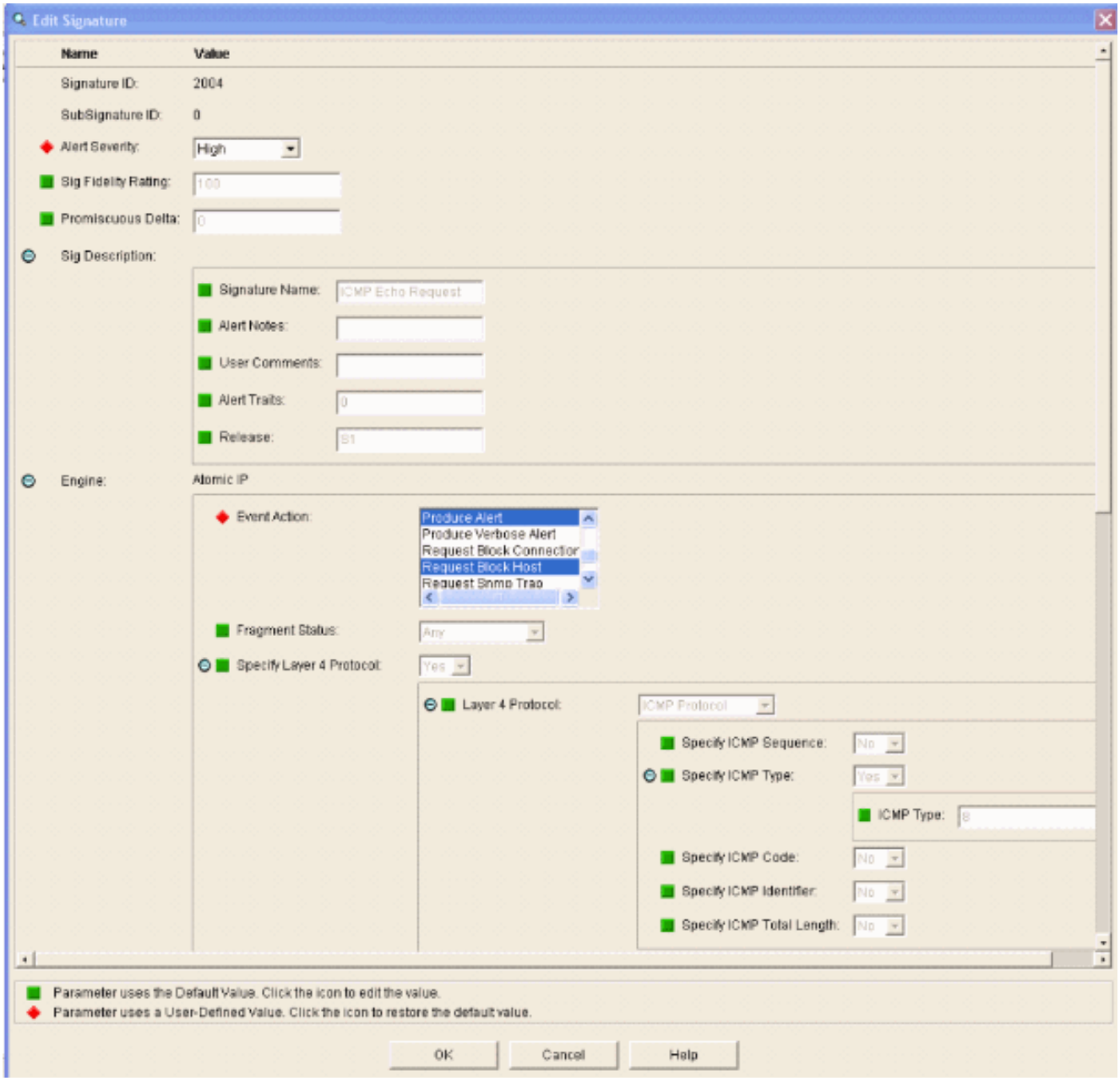
Adicionar uma assinatura da inspeção para obstruir o tráfego. Embora haja muitas assinaturas que podem fazer o trabalho baseado nas ferramentas disponíveis, este exemplo cria uma assinatura que obstrua pacotes de ping.

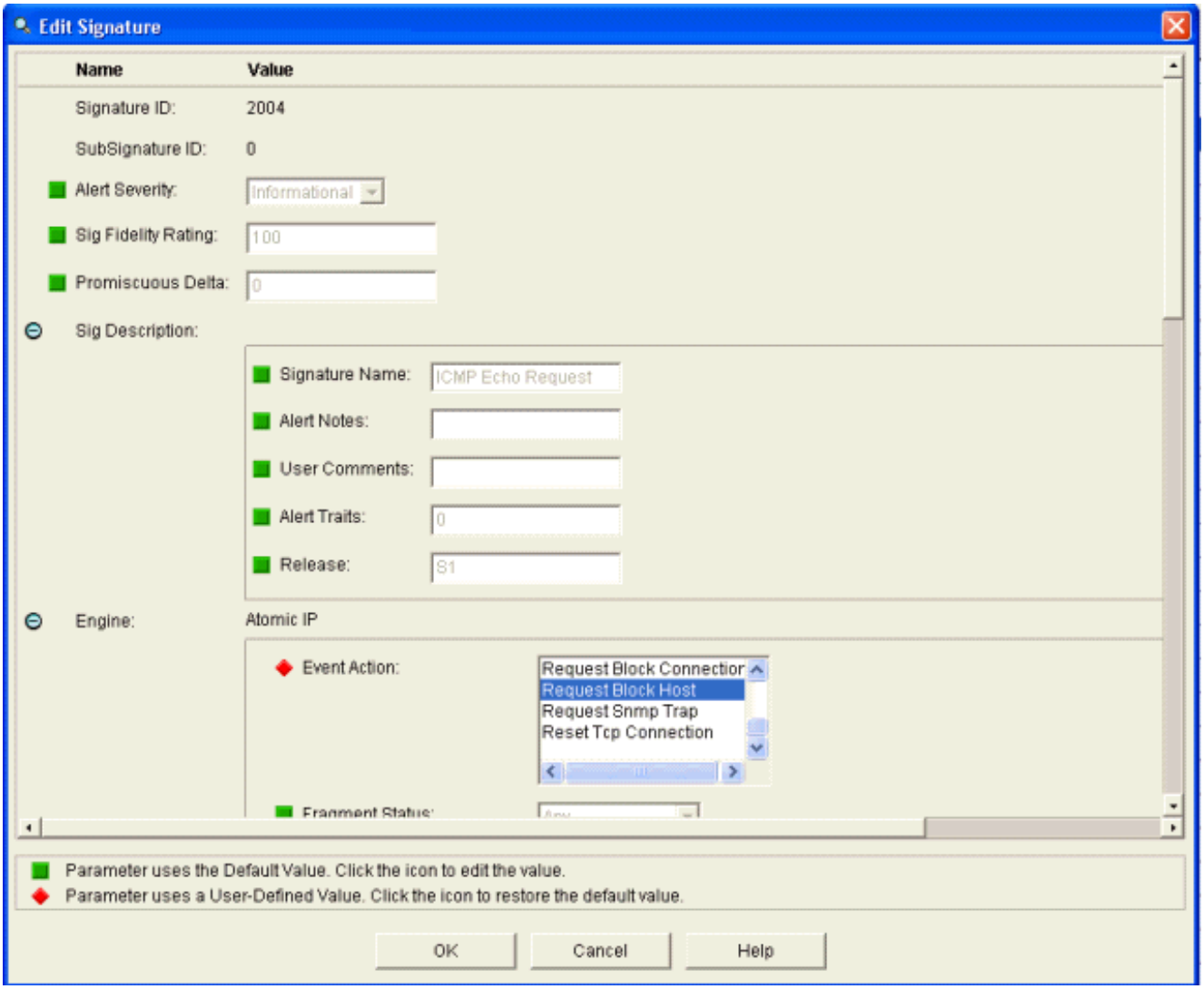
1. Selecione a **assinatura 2004 (requisição de eco ICMP)** a fim executar uma verificação rápida da

instalação.




2. Permita a assinatura, ajuste a severidade alerta à **elevação** e ajuste a ação do evento **para produzir o host do bloco do alerta** e de **pedido** a fim terminar este passo de verificação. Note que a ação do host do bloco de pedido é a chave a sinalizar o WLC para criar exceções do cliente.



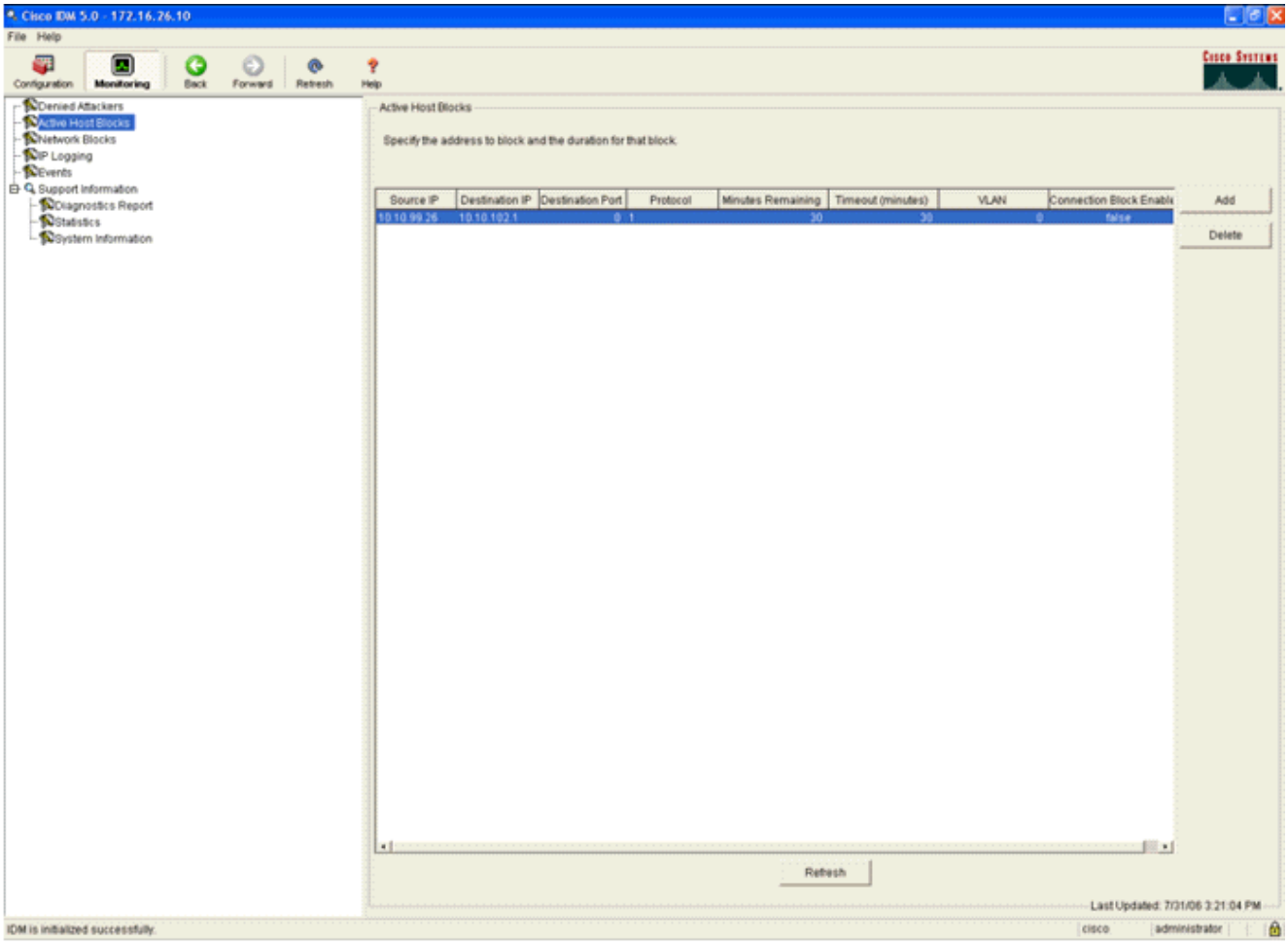



3. Clique a **APROVAÇÃO** a fim salvar a assinatura.
4. Verifique que a assinatura é ativa e que está ajustada para executar uma ação de obstrução.
5. O clique **aplica-se** a fim comprometer a assinatura ao módulo.

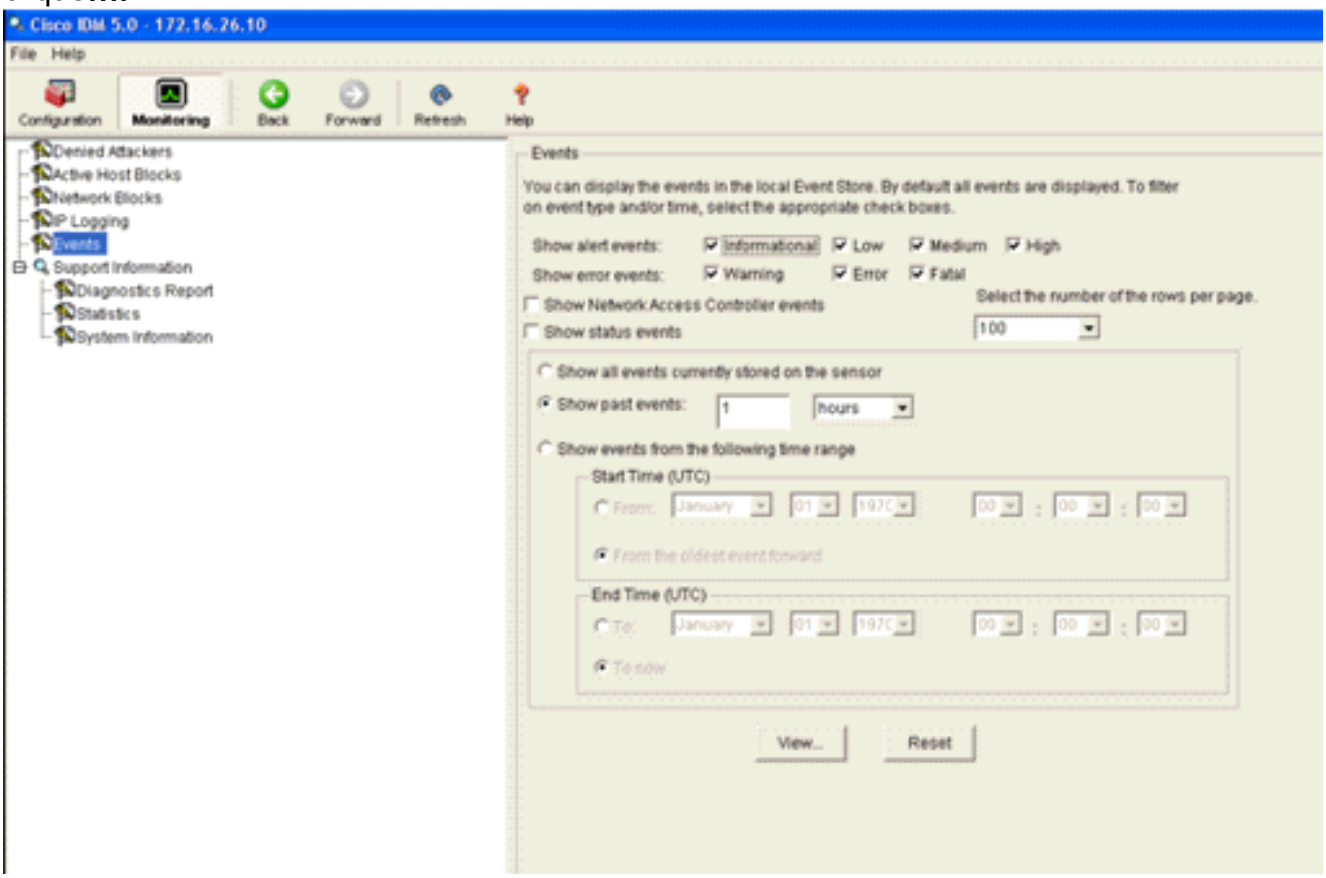
## Monitore a obstrução e os eventos com IDM

Conclua estes passos:

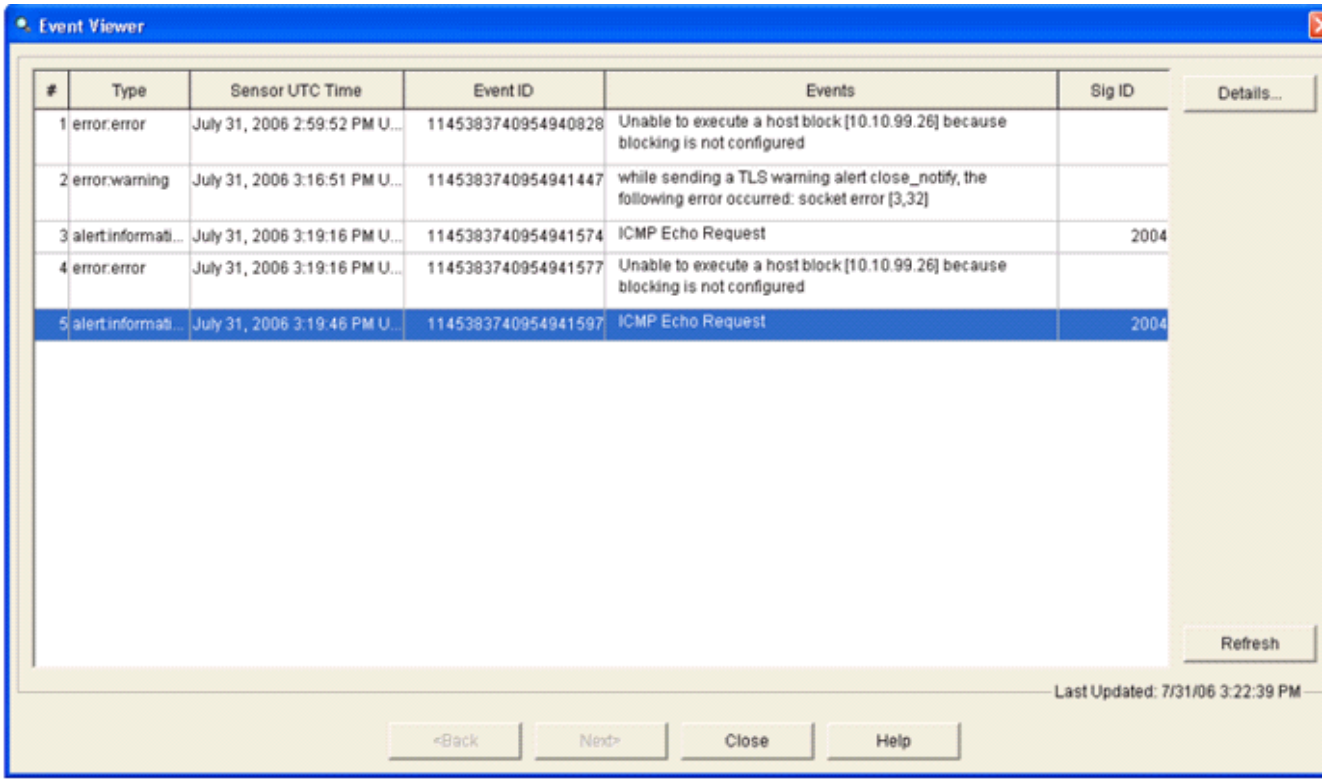
1. Quando os fogos da assinatura com sucesso, lá forem dois lugares dentro do IDM para notar isto.O primeiro método mostra aos blocos ativos que o AIP-SSM instalou. Clique a **monitoração** ao longo da fileira superior das ações. Dentro da lista de artigos que aparece no lado esquerdo, o **host ativo** seleto **obstrui**. Sempre que os disparadores da assinatura do sibilo, o host ativo obstruem o indicador mostra o endereço IP de Um ou Mais Servidores Cisco ICM NT do delinquente, o endereço do dispositivo sob o ataque, e o tempo que permanece para quais o bloco é de fato. O padrão que obstrui o tempo é 30 minutos e é ajustável. Contudo, mudando este valor não é discutido neste documento. Consulte a documentação de configuração ASA como necessário para obter informações sobre de como mudar este parâmetro. Remova o bloco imediatamente, selecione-o da lista e clique-o então a
**supressão**.



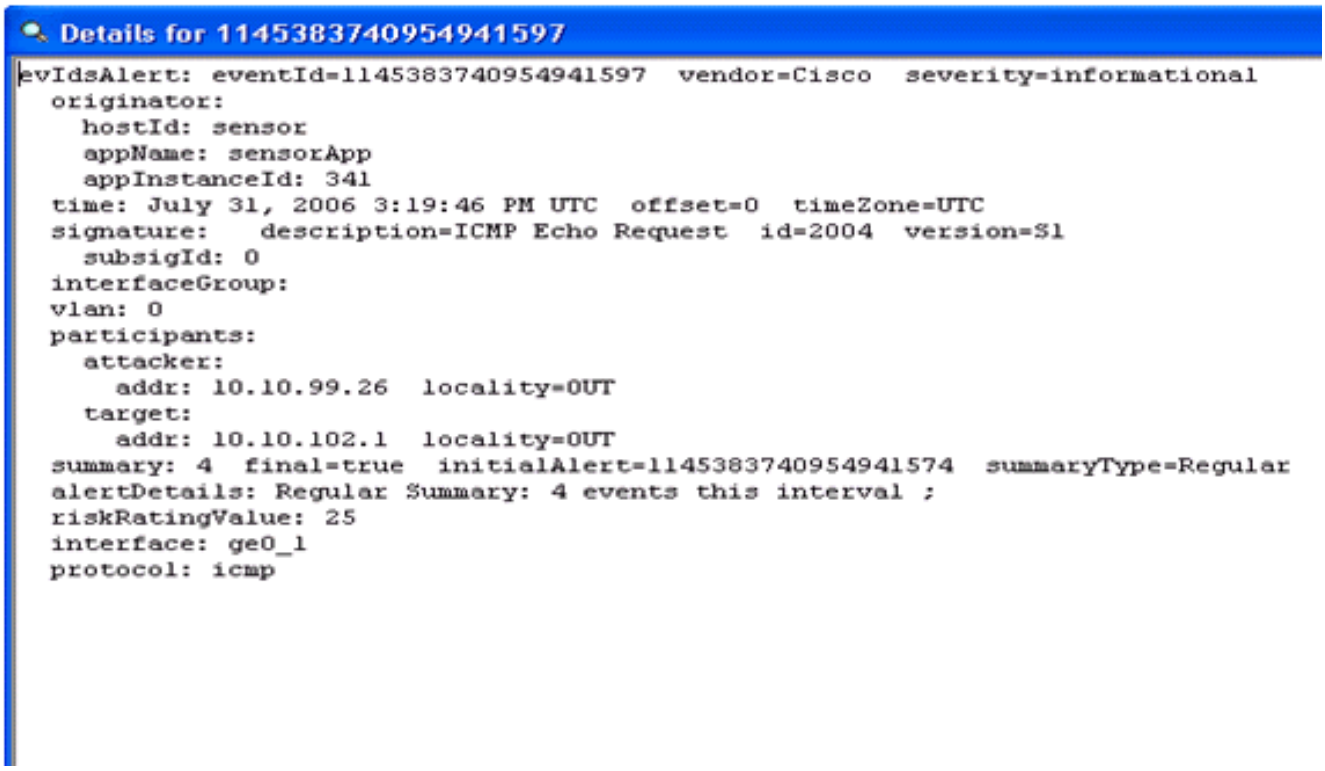

O segundo método para ver assinaturas provocadas usa o buffer do evento AIP-SSM. Da página da monitoração IDM, selecione **eventos na** lista dos artigos no lado esquerdo. A utilidade da busca dos eventos aparece. Ajuste critérios de pesquisa e a **opinião** apropriados do
clique....



2. O visualizador de eventos aparece então com uma lista de eventos que combinam os critérios dados. O rolo através da lista e encontra a assinatura da requisição de eco ICMP alterada nas etapas da configuração precedente.Olhe na coluna dos eventos para o nome da assinatura, ou então procure pelo número de identificação da assinatura sob a coluna dos Sig
ID.

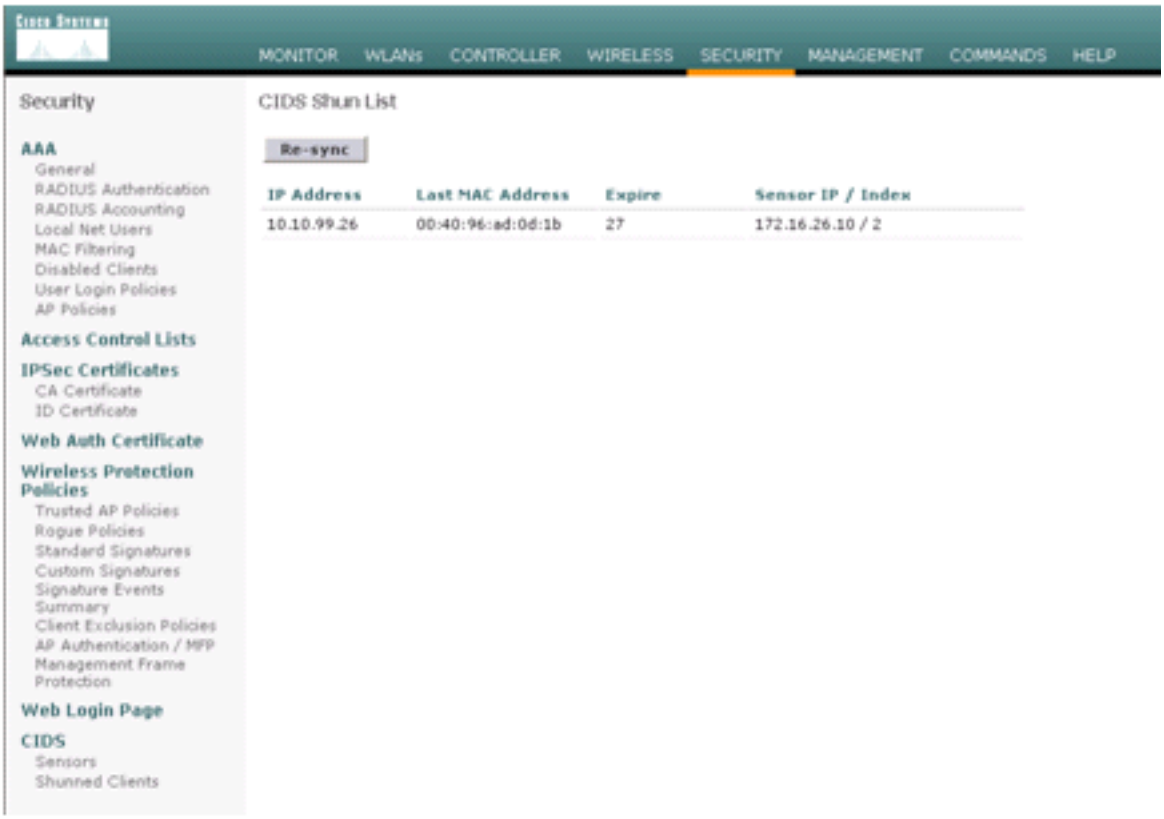



3. Depois que você encontra a assinatura, fazer duplo clique a entrada a fim abrir uma nova janela. A nova janela contém a informação detalhada no evento que provocou a assinatura.

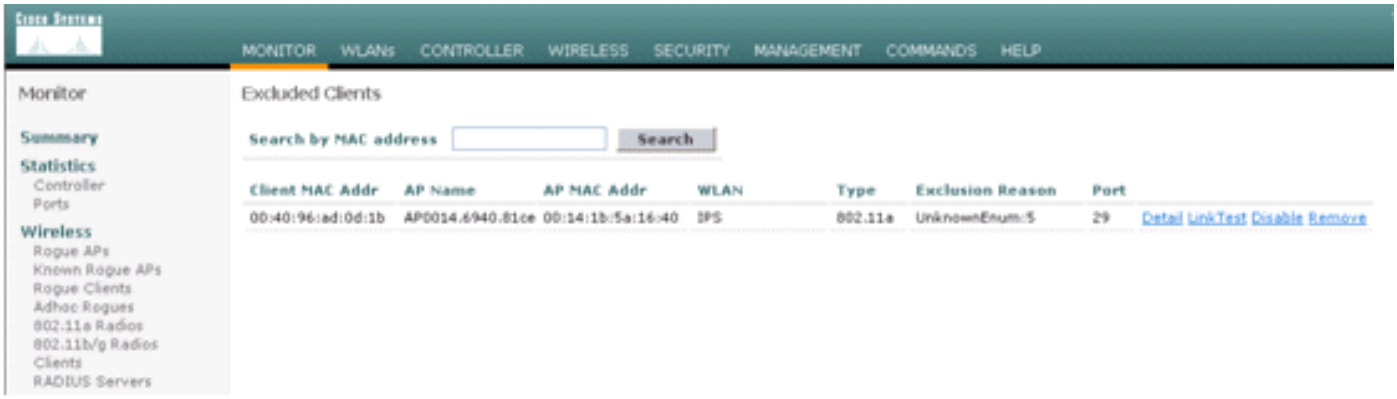



## Monitore a exclusão do cliente em um controlador wireless

Os clientes evitados alistam no controlador são povoados neste momento do tempo com o IP e o MAC address do host.




O usuário é adicionado à lista da exclusão do cliente.

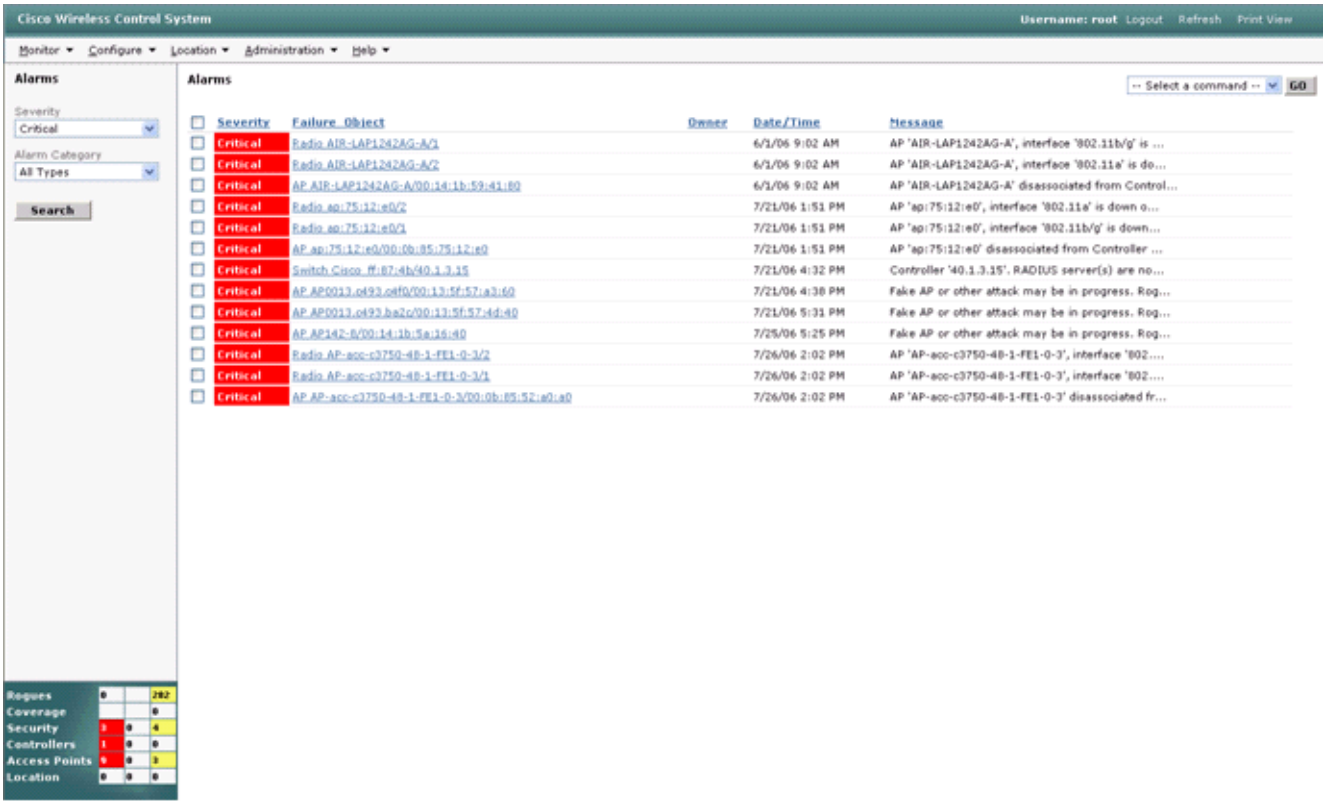



## Monitore eventos no WCS

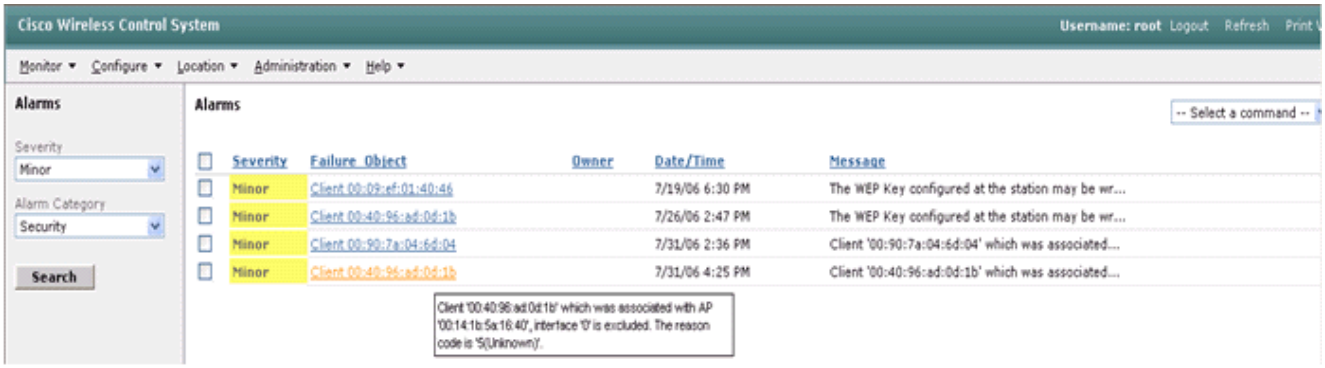
Eventos de segurança que provocam um bloco dentro da causa AIP-SSM o controlador para adicionar o endereço do delinquente à lista da exclusão do cliente. Um evento é gerado igualmente dentro do WCS.

1. Use o **monitor > os alarmes** de serviço público do menu principal WCS a fim ver o evento da exclusão. O WCS indica inicialmente todos os alarmes uncleared e igualmente apresenta uma função de pesquisa no lado esquerdo do indicador.
2. Altere os critérios de pesquisa para encontrar o bloco do cliente. Sob a severidade, escolha o **menor**, e igualmente ajuste a categoria do alarme à **Segurança**.
3. Clique em

Buscar.




4. O indicador do alarme alista então somente alarmes da Segurança com severidade menor. Aponte o rato no evento que provocou o bloco dentro do AIP-SSM.Em particular, o WCS mostra o MAC address da estação do cliente que causou o alarme. Apontando no endereço apropriado, PNFque WCS um indicador pequeno com o evento detalha. Clique o link a fim ver estes mesmos detalhes em um outro indicador.




## Configuração de exemplo de 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#
```

## Configuração de exemplo do sensor de Sistema de prevenção de intrusões da Cisco

```
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#
```

## Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

## Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## Informações Relacionadas

- Instalando e usando o gerenciador de dispositivo 5.1 do Sistema de prevenção de intrusões da Cisco
- Dispositivos de segurança adaptáveis Cisco ASA série 5500 - Manuais de configuração
- Configurando o sensor de Sistema de prevenção de intrusões da Cisco usando a interface da linha de comando 5.0 - configurando relações
- Manual de configuração 4.0 WLC
- Suporte técnico wireless
- Controlador do Wireless LAN (WLC) FAQ
- Exemplo de Configuração Básica de Controladoras de Wireless LAN e Pontos de Acesso Lightweight
- Configurando soluções da Segurança
- Suporte Técnico e Documentação - Cisco Systems