

Guia de integração de controlador de LAN sem fio e IPS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Visão geral do Cisco IDS](#)

[Cisco IDS e WLC - Visão geral da integração](#)

[Desconexão IDS](#)

[Projeto de arquitetura de rede](#)

[Configurar o Cisco IDS Sensor](#)

[Configurar o WLC](#)

[Exemplo de configuração do sensor Cisco IDS](#)

[Configurar um ASA para IDS](#)

[Configurar o AIP-SSM para a inspeção de tráfego](#)

[Configurar uma WLC para pesquisar o AIP-SSM para blocos de clientes](#)

[Adicionar uma assinatura de bloqueio ao AIP-SSM](#)

[Monitorar bloqueio e eventos com IDM](#)

[Monitorar a exclusão do cliente em um controlador sem fio](#)

[Monitorar eventos no WCS](#)

[Exemplo de configuração do Cisco ASA](#)

[Exemplo de configuração do sensor do sistema de prevenção de intrusão da Cisco](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

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 Cisco Unified IDS/IPS adota uma abordagem abrangente à segurança — na borda da rede sem fio, borda da rede com fio, borda da WAN e através do data center. Quando um cliente associado envia tráfego mal-intencionado através da Cisco Unified Wireless Network, um dispositivo IDS com fio da Cisco detecta o ataque e envia solicitações shun para os Cisco Wireless LAN Controllers (WLCs), que então desassocia o dispositivo cliente.

O Cisco IPS é uma solução em linha, baseada em rede, projetada para identificar, classificar e interromper com precisão o tráfego mal-intencionado, incluindo worms, spyware/adware, vírus de

rede e abuso de aplicativos, antes que eles afetem a continuidade dos negócios.

Com a utilização do software Cisco IPS Sensor versão 5, a solução Cisco IPS combina serviços de prevenção em linha com tecnologias inovadoras para melhorar a precisão. O resultado é a total confiança na proteção fornecida da sua solução IPS, sem o medo de que o tráfego legítimo seja descartado. A solução Cisco IPS também oferece proteção abrangente da sua rede por meio de sua capacidade exclusiva de colaborar com outros recursos de segurança de rede e oferece uma abordagem proativa para a proteção da sua rede.

A solução Cisco IPS ajuda os usuários a deter mais ameaças com maior confiança através do uso desses recursos:

- **Tecnologias de prevenção em linha precisas:** oferece confiança inigualável para tomar medidas preventivas contra uma variedade maior de ameaças sem o risco de descartar tráfego legítimo. Essas tecnologias exclusivas oferecem análise inteligente, automatizada e contextual dos seus dados e ajudam a garantir que você receba o máximo de sua solução de prevenção de invasão.
- **Identificação de ameaças de vários vetores** — Protege sua rede contra violações de políticas, explorações de vulnerabilidades e atividades anômalas por meio da inspeção detalhada do tráfego nas camadas 2 a 7.
- **Colaboração de rede exclusiva** — Melhora a escalabilidade e a resiliência através da colaboração de rede, incluindo técnicas eficientes de captura de tráfego, recursos de balanceamento de carga e visibilidade do tráfego criptografado.
- **Soluções de implantação abrangentes:** fornece soluções para todos os ambientes, desde pequenas e médias empresas (SMBs) e filiais até grandes empresas e instalações de provedores de serviços.
- **Serviços poderosos de gerenciamento, correlação de eventos e suporte**—Permite uma solução completa, incluindo configuração, gerenciamento, correlação de dados e serviços de suporte avançados. Em particular, o Cisco Security Monitoring, Analysis, and Response System (MARS) identifica, isola e recomenda a remoção precisa de elementos ofensivos para uma solução de prevenção contra invasão em toda a rede. E o Cisco Incident Control System evita novas epidemias de vírus e worms, permitindo que a rede se adapte rapidamente e forneça uma resposta distribuída.

Quando combinados, esses elementos fornecem uma solução abrangente de prevenção em linha e dão a você a confiança para detectar e interromper a mais ampla gama de tráfego mal-intencionado antes que ele afete a continuidade dos negócios. A iniciativa Rede de Autodefesa da Cisco exige segurança integrada e incorporada para soluções de rede. Os sistemas de WLAN baseados no LWAPP (Lightweight Access Point Protocol) atuais suportam somente recursos básicos de IDS devido ao fato de que ele é essencialmente um sistema de Camada 2 e tem poder limitado de processamento de linha. A Cisco lança o novo código em tempo hábil para incluir novos recursos avançados nos novos códigos. A versão 4.0 tem os recursos mais recentes que incluem a integração de um sistema WLAN baseado em LWAPP com a linha de produtos Cisco IDS/IPS. Nesta versão, o objetivo é permitir que o sistema Cisco IDS/IPS instrua as WLCs a bloquear o acesso de determinados clientes às redes sem fio quando um ataque é detectado em qualquer parte da Camada 3 à Camada 7 que envolva o cliente em consideração.

[Prerequisites](#)

[Requirements](#)

Certifique-se de atender a estes requisitos mínimos:

- Firmware WLC versão 4.x e posterior
- O conhecimento sobre como configurar o Cisco IPS e o Cisco WLC é desejável.

Componentes Utilizados

WLC da Cisco

Esses controladores estão incluídos na versão de software 4.0 para modificações de IDS:

- WLC Cisco 2000 Series
- WLC Cisco 2100 Series
- WLC Cisco 4400 Series
- Cisco Wireless Services Module (WiSM)
- Switch de acesso unificado Cisco Catalyst 3750G Series
- Módulo controlador de LAN sem fio (WLCM) da Cisco

Pontos de acesso

- Pontos de acesso leves Cisco Aironet 1100 AG Series
- Pontos de acesso leves Cisco Aironet 1200 AG Series
- Access points leves Cisco Aironet 1300 Series
- Pontos de acesso leves Cisco Aironet 1000 Series

Gerenciamento

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

Plataformas Cisco Unified IDS/IPS

- Sensores Cisco IPS 4200 Series com Cisco IPS Sensor Software 5.x ou posterior.
- SSM10 e SSM20 para os dispositivos de segurança adaptável Cisco ASA 5500 Series com software de sensor Cisco IPS 5.x
- Cisco ASA 5500 Series Adaptive Security Appliances com Cisco IPS Sensor Software 5.x
- Cisco IDS Network Module (NM-CIDS) com Cisco IPS Sensor Software 5.x
- Cisco Catalyst 6500 Series Intrusion Detection System Module 2 (IDSM-2) com Cisco IPS Sensor Software 5.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

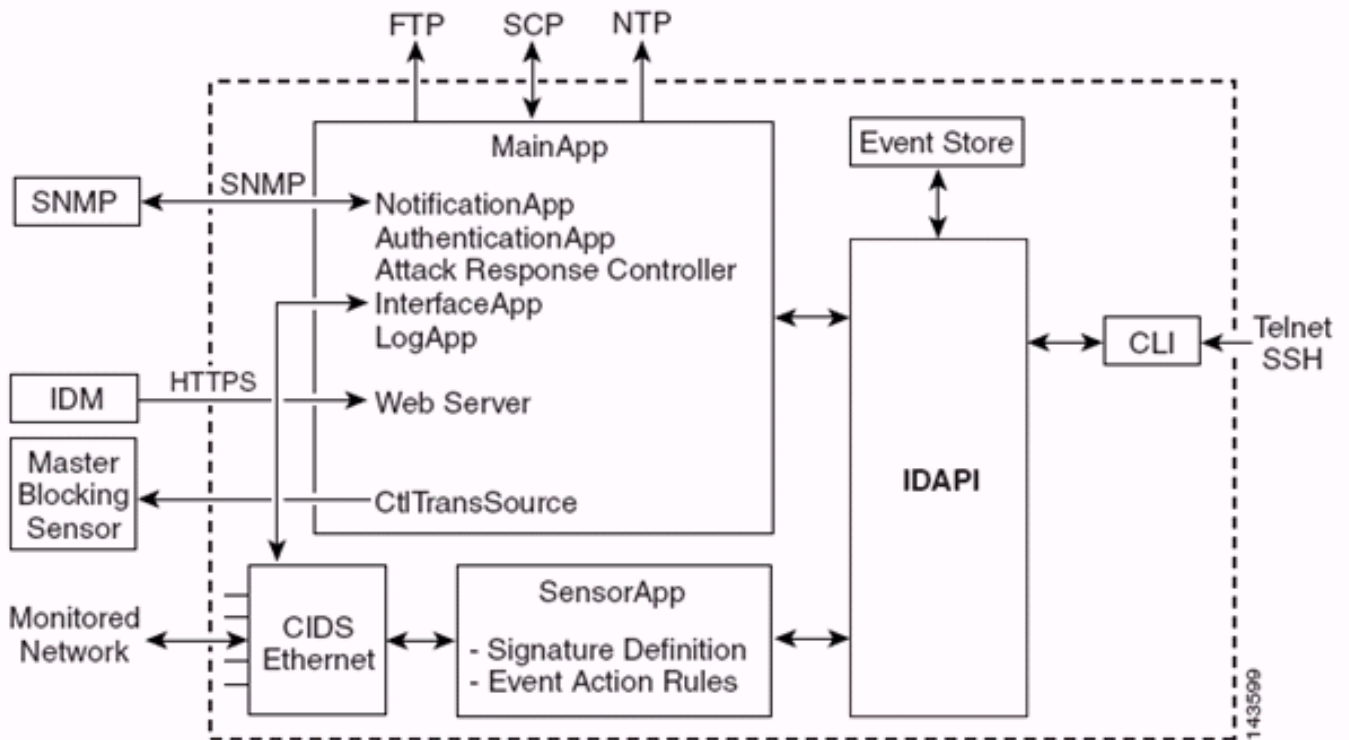
Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Visão geral do Cisco IDS

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

- **Aplicativo Sensor** — Executa captura e análise de pacotes.
- **Event Storage Management and Actions Module** — Fornece armazenamento de violações de política.
- **Módulo de imagem, instalação e inicialização** — Carrega, inicializa e inicia todo o software do sistema.
- **User Interfaces e UI Support Module** — Fornece uma CLI incorporada e o IDM.
- **SO do sensor** — Sistema operacional do host (baseado no Linux).



O aplicativo de sensor (software IPS) consiste em:

- **Aplicativo principal** — Inicializa o sistema, inicia e interrompe outros aplicativos, configura o SO e é responsável por atualizações. Ele contém estes componentes: **Control Transaction Server** — Permite que os sensores enviem transações de controle que são usadas para ativar o recurso de sensor de bloqueio mestre do controlador de resposta a ataque (anteriormente conhecido como controlador de acesso à rede). **Event Store** — Um repositório indexado usado para armazenar eventos de IPS (erros, status e mensagens do sistema de alerta) acessíveis através da CLI, IDM, Adaptive Security Device Manager (ASDM) ou Remote Data Exchange Protocol (RDEP).
- **Interface App** — Trata de desvios e configurações físicas e define interfaces emparelhadas. As configurações físicas consistem em velocidade, duplex e estados administrativos.
- **Log App** — grava as mensagens de log do aplicativo no arquivo de log e as mensagens de erro no Event Store.
- **Attack Response Controller (ARC) (anteriormente conhecido como Network Access Controller)** — Gerencia dispositivos de rede remotos (firewalls, roteadores e switches) para fornecer recursos de bloqueio quando ocorre um evento de alerta. O ARC cria e aplica listas de controle de acesso (ACLs) no dispositivo de rede controlado ou usa o comando **shun** (firewalls).
- **Aplicativo de Notificação** — Envia interceptações SNMP quando disparadas por um alerta,

status e eventos de erro. O aplicativo de notificação usa um agente SNMP de domínio público para isso. Os GETs SNMP fornecem informações sobre a integridade de um sensor. **Servidor Web (servidor HTTP RDEP2)** — Fornece uma interface de usuário da Web. Ele também fornece um meio de se comunicar com outros dispositivos IPS por meio do RDEP2 usando vários servlets para fornecer serviços IPS. **Authentication App** — Verifica se os usuários estão autorizados a executar ações CLI, IDM, ASDM ou RDEP.

- **Aplicativo Sensor (Analysis Engine)** — Executa captura e análise de pacotes.
- **CLI** — A interface que é executada quando os usuários fazem login com êxito no Sensor por meio de Telnet ou SSH. Todas as contas criadas através da CLI usam a CLI como shell (exceto 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 entre si por meio de uma API (Application Program Interface, interface de programa de aplicativos) comum chamada IDAPI. Os aplicativos remotos (outros sensores, aplicativos de gerenciamento e software de terceiros) comunicam-se com os sensores por meio dos protocolos RDEP2 e Security Device Event Exchange (SDEE).

Deve-se observar que o sensor tem estas partições de disco:

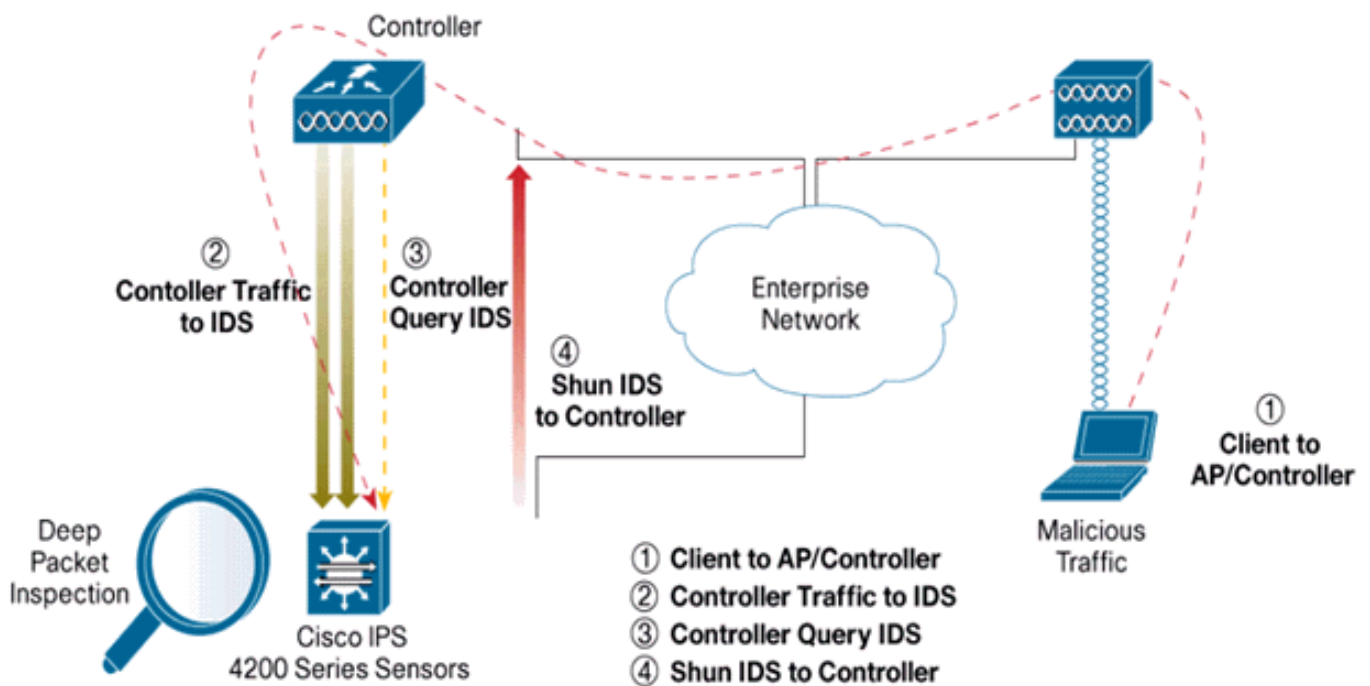
- **Application Partition** — Contém a imagem completa do sistema IPS.
- **Partição de manutenção** — Uma imagem IPS de propósito especial usada para recriar a imagem da partição do aplicativo do IDSM-2. Uma nova imagem da partição de manutenção resulta em configurações perdidas.
- **Partição de Recuperação** — Uma imagem de finalidade especial usada para recuperação do sensor. A inicialização na partição de recuperação permite que os usuários refaçam completamente a imagem da partição do aplicativo. As configurações de rede são preservadas, mas todas as outras configurações são perdidas.

[Cisco IDS e WLC - Visão geral da integração](#)

A versão 5.0 do Cisco IDS apresenta a capacidade de configurar ações de negação quando violações de política (assinaturas) são detectadas. Com base na configuração do usuário no sistema IDS/IPS, uma solicitação shun pode ser enviada a um firewall, roteador ou WLC para bloquear os pacotes de um endereço IP específico.

Com o Cisco Unified Wireless Network Software Release 4.0 para Cisco Wireless Controllers, uma solicitação shun precisa ser enviada a uma WLC para disparar o comportamento de exclusão ou de lista negra do cliente disponível em um controlador. A interface usada pelo controlador para obter a solicitação shun é o comando e a interface de controle no Cisco IDS.

- O controlador permite que até cinco sensores IDS sejam configurados em um determinado controlador.
- Cada sensor IDS configurado é identificado por seu endereço IP ou nome de rede qualificado e credenciais de autorização.
- Cada sensor IDS pode ser configurado em um controlador com uma taxa de consulta exclusiva em segundos.



Desconexão IDS

O controlador consulta o sensor na taxa de consulta configurada para recuperar todos os eventos shun. Uma determinada solicitação shun é distribuída por todo o grupo de mobilidade da controladora que recupera a solicitação do sensor IDS. Cada solicitação shun para um endereço IP de cliente está em vigor para o valor de tempo limite de segundos especificado. Se o valor de tempo limite indicar um tempo infinito, o evento shun terminará somente se a entrada shun for removida no IDS. O status do cliente desligado é mantido em cada controlador no grupo de mobilidade mesmo se qualquer um ou todos os controladores forem redefinidos.

Observação: a decisão de executar um cliente é sempre tomada pelo IDS Sensor. O controlador não detecta ataques de Camada 3. É um processo muito mais complicado determinar que o cliente está iniciando um ataque mal-intencionado na Camada 3. O cliente é autenticado na camada 2, o que é bom o suficiente para que o controlador conceda acesso à camada 2.

Observação: por exemplo, se um cliente recebe um endereço IP ofensivo (desconectado) anterior atribuído, é o limite de tempo do sensor que desbloqueia o acesso da Camada 2 para esse novo cliente. Mesmo que o controlador forneça acesso à Camada 2, o tráfego do cliente pode ser bloqueado nos roteadores na Camada 3 de qualquer forma, porque o Sensor também informa os roteadores sobre o evento shun.

Suponha que um cliente tenha o endereço IP A. Agora, quando a controladora pesquisa o IDS para eventos shun, o IDS envia a solicitação shun para a controladora com o endereço IP A como o endereço IP de destino. Agora, o controlador preto lista este cliente A. No controlador, os clientes são desabilitados com base em um endereço MAC.

Agora, suponha que o cliente altere seu endereço IP de A para B. Durante a próxima pesquisa, o controlador recebe uma lista de clientes desligados com base no endereço IP. Novamente, o endereço IP A ainda está na lista suspensa. Mas como o cliente alterou seu endereço IP de A para B (que não está na lista descartada de endereços IP), esse cliente com um novo endereço IP de B é liberado assim que o tempo limite dos clientes da lista negra é atingido no controlador. Agora, o controlador começa a permitir que esse cliente com o novo endereço IP de B (mas o

endereço MAC do cliente permanece o mesmo).

Portanto, embora um cliente permaneça desabilitado durante o tempo de exclusão do controlador e seja excluído novamente se ele readquirir seu endereço DHCP anterior, esse cliente não será mais desabilitado se o endereço IP do cliente que foi desconectado for alterado. Por exemplo, se o cliente se conectar à mesma rede e o tempo limite de concessão do DHCP não expirar.

Os controladores suportam somente a conexão com o IDS para solicitações de desconexão de clientes que usam a porta de gerenciamento no controlador. O controlador se conecta ao IDS para inspeção de pacotes através das interfaces VLAN aplicáveis que transportam tráfego de cliente sem fio.

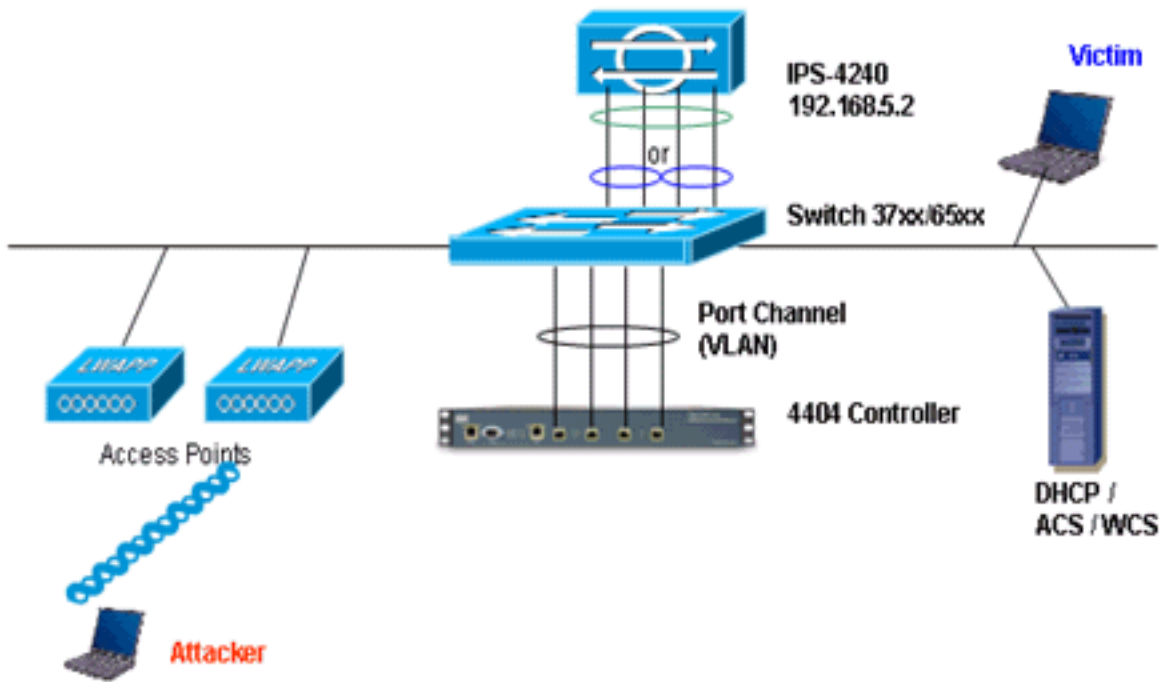
Na controladora, a página Desativar clientes mostra cada cliente que foi desabilitado por meio de uma solicitação de sensor IDS. O comando CLI **show** também exibe uma lista de clientes na lista negra.

No WCS, os clientes excluídos são exibidos na subguia Segurança.

Aqui estão as etapas a seguir para concluir a integração dos Cisco IPS Sensors e Cisco WLCs.

1. Instale e conecte o dispositivo IDS no mesmo switch onde o controlador wireless reside.
2. Espelhe (SPAN) as portas WLC que transportam o tráfego do cliente sem fio para o dispositivo IDS.
3. O dispositivo IDS recebe uma cópia de cada pacote e inspeciona o tráfego nas Camadas 3 a 7.
4. O dispositivo IDS oferece um arquivo de assinatura para download, que também pode ser personalizado.
5. O dispositivo IDS gera o alarme com uma ação de evento de shun quando uma assinatura de ataque é detectada.
6. A WLC pesquisa o IDS para obter alarmes.
7. Quando um alarme com o endereço IP de um cliente sem fio, associado à WLC, é detectado, ele coloca o cliente na lista de exclusões.
8. Uma armadilha é gerada pela WLC e a WCS é notificada.
9. O usuário é removido da lista de exclusões após o período de tempo especificado.

[Projeto de arquitetura de rede](#)



O Cisco WLC está conectado às interfaces gigabit no Catalyst 6500. Crie um canal de porta para as interfaces gigabit e ative a LAG (Link Aggregation, Agregação de links) na 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 está conectado à interface gigabit 5/1 e 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 interfaces de detecção do sensor IPS podem operar individualmente no **modo Promiscutivo** ou você pode combiná-las para criar interfaces em linha para o **modo de detecção em linha**.

No modo promíscuo, os pacotes não fluem pelo sensor. O sensor analisa uma cópia do tráfego monitorado em vez do pacote encaminhado real. A vantagem de operar no modo promíscuo é que o sensor não afeta o fluxo do pacote com o tráfego encaminhado.

Observação: o [diagrama de arquitetura](#) é apenas um exemplo de configuração da arquitetura integrada de WLC e IPS. O exemplo de configuração mostrado aqui explica a interface de detecção de IDS que atua no modo Promiscuto. O [diagrama de arquitetura](#) mostra as interfaces de detecção sendo emparelhadas para atuar no modo Par em linha. Consulte [Modo em Linha](#) para obter mais informações sobre o modo de Interface em Linha.

Nesta configuração, supõe-se que a interface de detecção atue no modo Promiscutivo. A interface de monitoramento do Cisco IDS Sensor está conectada à interface gigabit 5/3 no Catalyst 6500. Crie uma sessão de monitor no Catalyst 6500 onde a interface do canal de porta é a origem dos pacotes e o destino é a interface gigabit onde a interface de monitoração do Cisco IPS Sensor está conectada. Isso replica todo o tráfego de entrada e saída das interfaces com fio do controlador para o IDS para inspeção de Camada 3 a 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 Cisco IDS Sensor](#)

A configuração inicial do Cisco IDS Sensor é feita a partir da porta do console ou conectando um monitor e um teclado ao sensor.

1. Faça login no equipamento: Conecte uma porta de console ao sensor. Conecte um monitor e um teclado ao sensor.
2. Digite seu nome de usuário e senha no prompt de login. **Observação:** o nome de usuário e a senha padrão são cisco. Você será solicitado a alterá-los na primeira vez em que fizer login no aplicativo. Você deve primeiro inserir a senha UNIX, que é cisco. Em seguida, você deve digitar a nova senha 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. Configure o endereço IP, a máscara de sub-rede e a lista de acesso no sensor. **Observação:** essa é a interface de comando e controle no IDS usada para se comunicar com o controlador. Esse endereço deve ser roteável para a interface de gerenciamento do controlador. As interfaces de detecção não exigem endereçamento. A lista de acesso deve incluir o endereço da interface de gerenciamento da(s) controladora(s), bem como endereços permitidos 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 ---
```

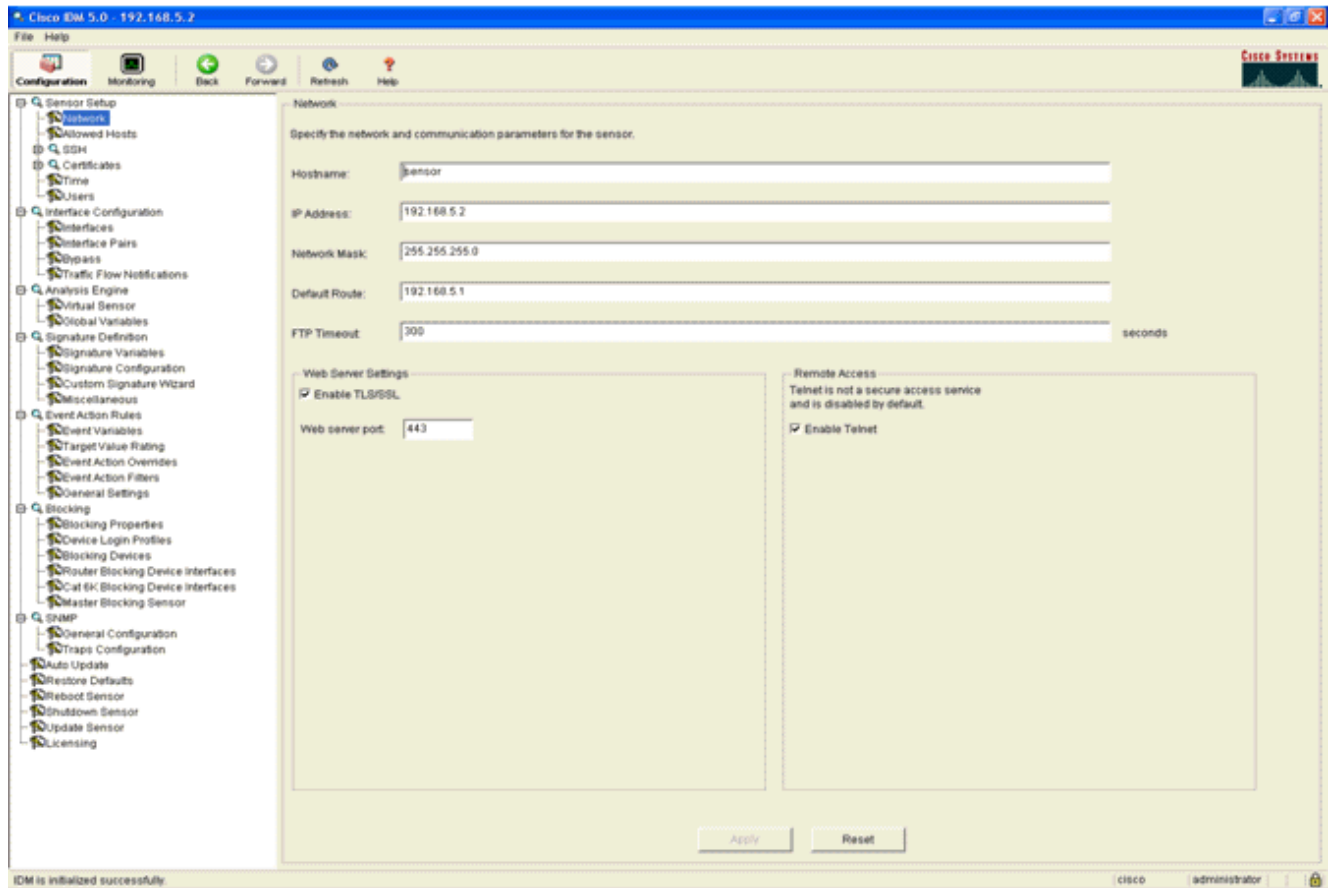
```
4 packets transmitted, 4 packets received, 0% packet loss
```

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

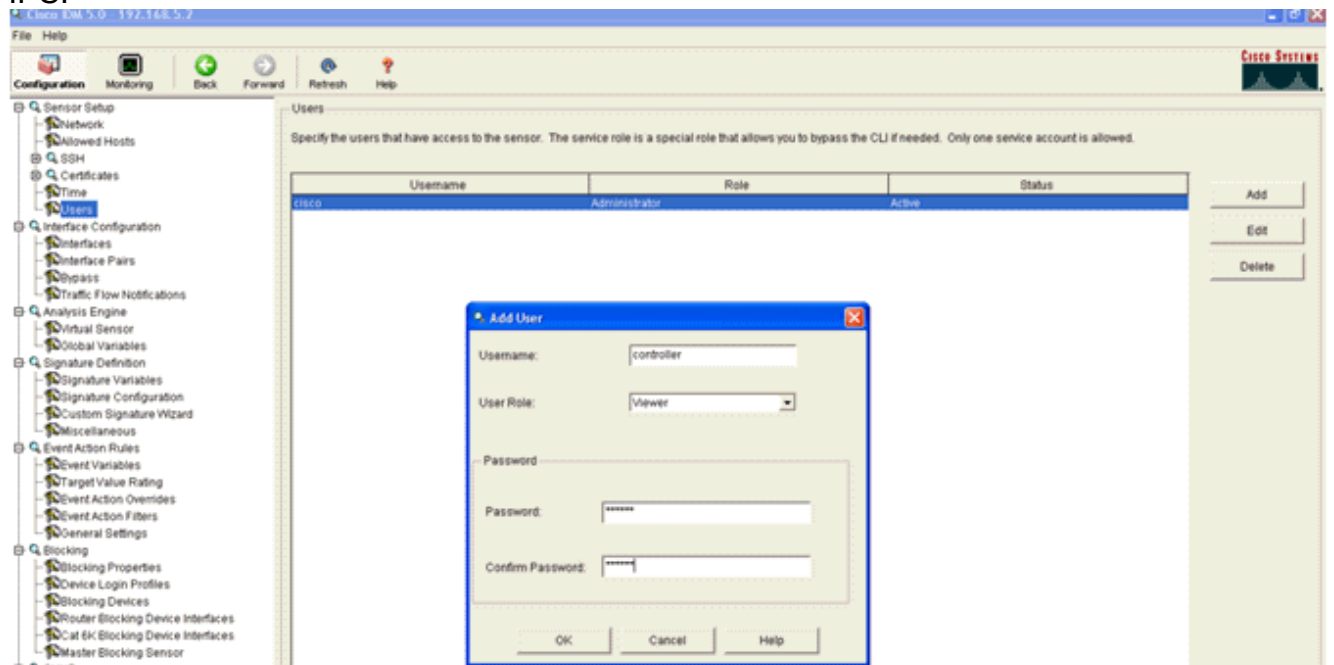
```
sensor#
```

4. Agora você pode configurar o sensor IPS na GUI. Aponte o navegador para o endereço IP

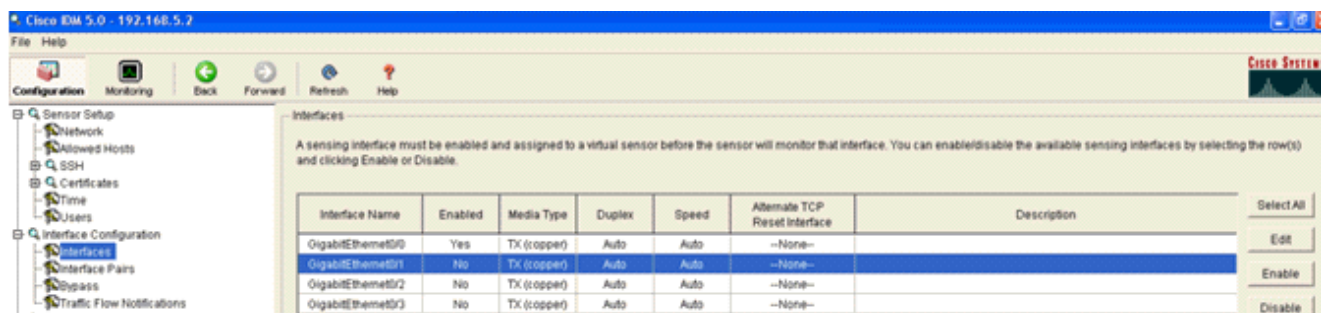
de gerenciamento do sensor. Essa imagem exibe um exemplo em que o sensor está configurado com 192.168.5.2.



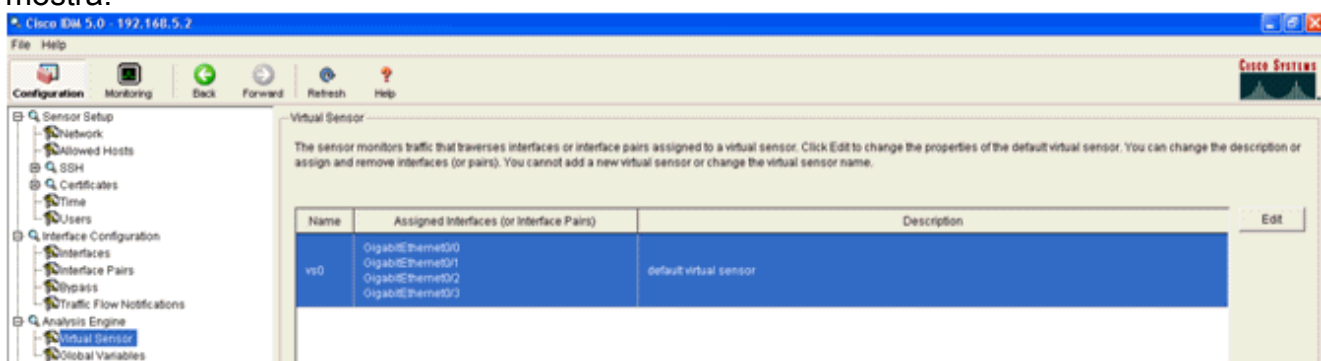
5. Adicione um usuário que a WLC usa para acessar os eventos do sensor IPS.



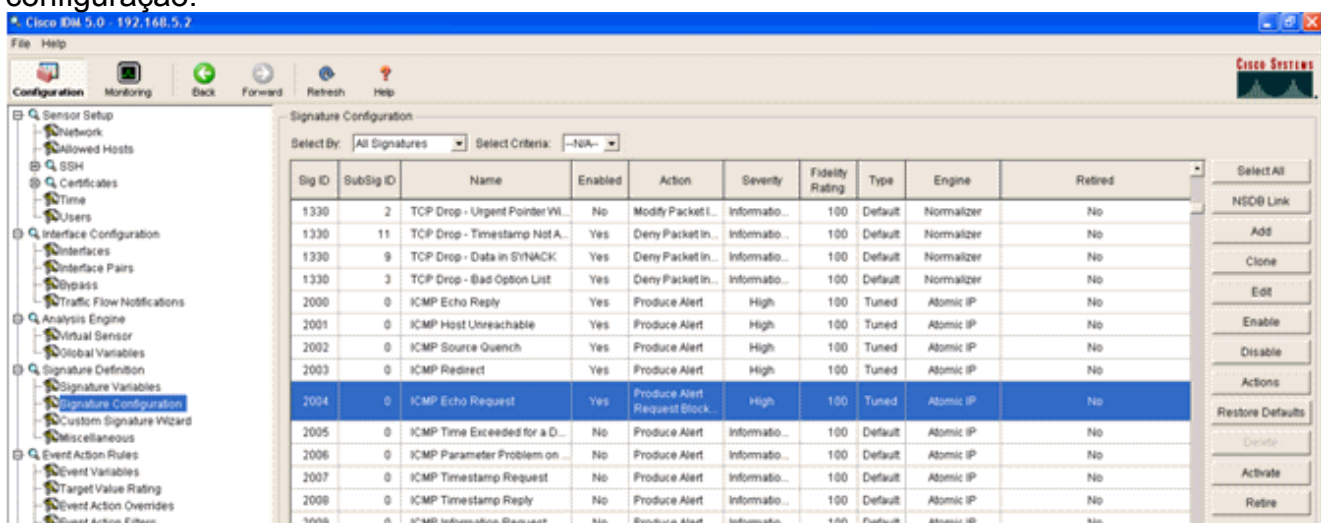
6. Ative as interfaces de monitoramento.



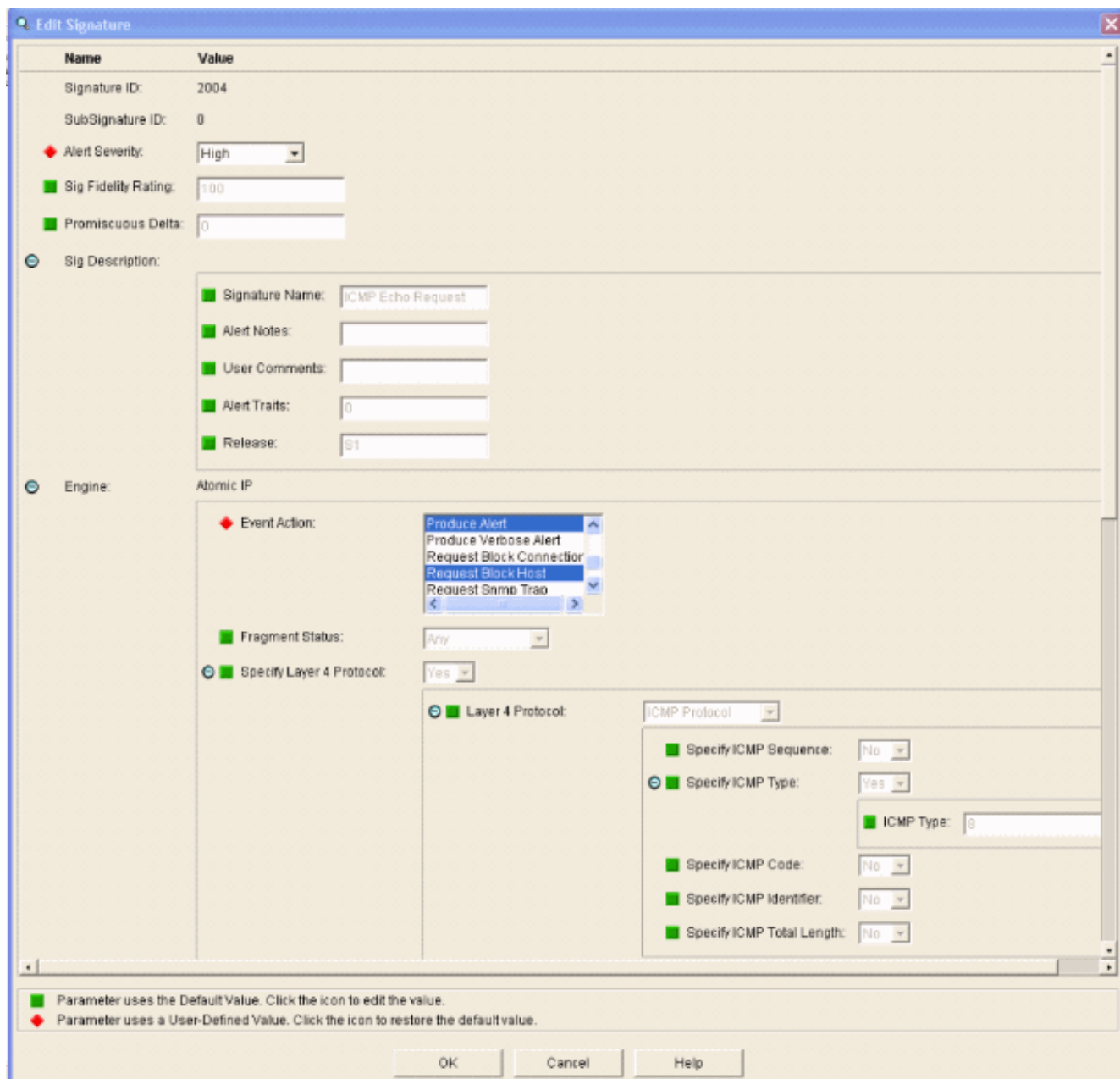
As interfaces de monitoramento devem ser adicionadas ao Mecanismo de Análise, como esta janela mostra:



7. Selecione a assinatura de 2004 (ICMP Echo Request) para executar uma rápida verificação de configuração.



A assinatura deve estar habilitada, Gravidade de alerta definida como **Alta** e Ação de evento definida para **Produzir Alerta** e **Host de Bloco de Solicitação** para que esta etapa de verificação seja concluída.



Configurar o WLC

Conclua estes passos para configurar a WLC:

1. Depois que o aplicativo IPS estiver configurado e pronto para ser adicionado ao controlador, escolha **Security > CIDS > Sensors > New (Segurança > CIDS > Sensores > Novo)**.
2. Adicione o endereço IP, o número da porta TCP, o nome de usuário e a senha que você criou anteriormente. Para obter a impressão digital do sensor IPS, execute esse comando no sensor IPS e adicione a impressão digital SHA1 na WLC (sem dois-pontos). Isso é usado para proteger a comunicação de polling de controlador para 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
```

The screenshot shows the 'CIDS Sensor Add' configuration page in the Cisco WLC GUI. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, Network Access Control, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area is titled 'CIDS Sensor Add' and includes the following fields:

- Index:** 1
- Server Address:** 192.168.5.2
- Port:** 443
- Username:** controller
- Password:** [masked]
- Confirm Password:** [masked]
- Query Interval:** 15 seconds
- State:**
- Fingerprint (SHA1 hash):** 1662E996362A9A1EF08B99A7C1645F5CB56A8842 (40 hex chars)

Buttons for '< Back' and 'Apply' are located at the top right of the configuration area.

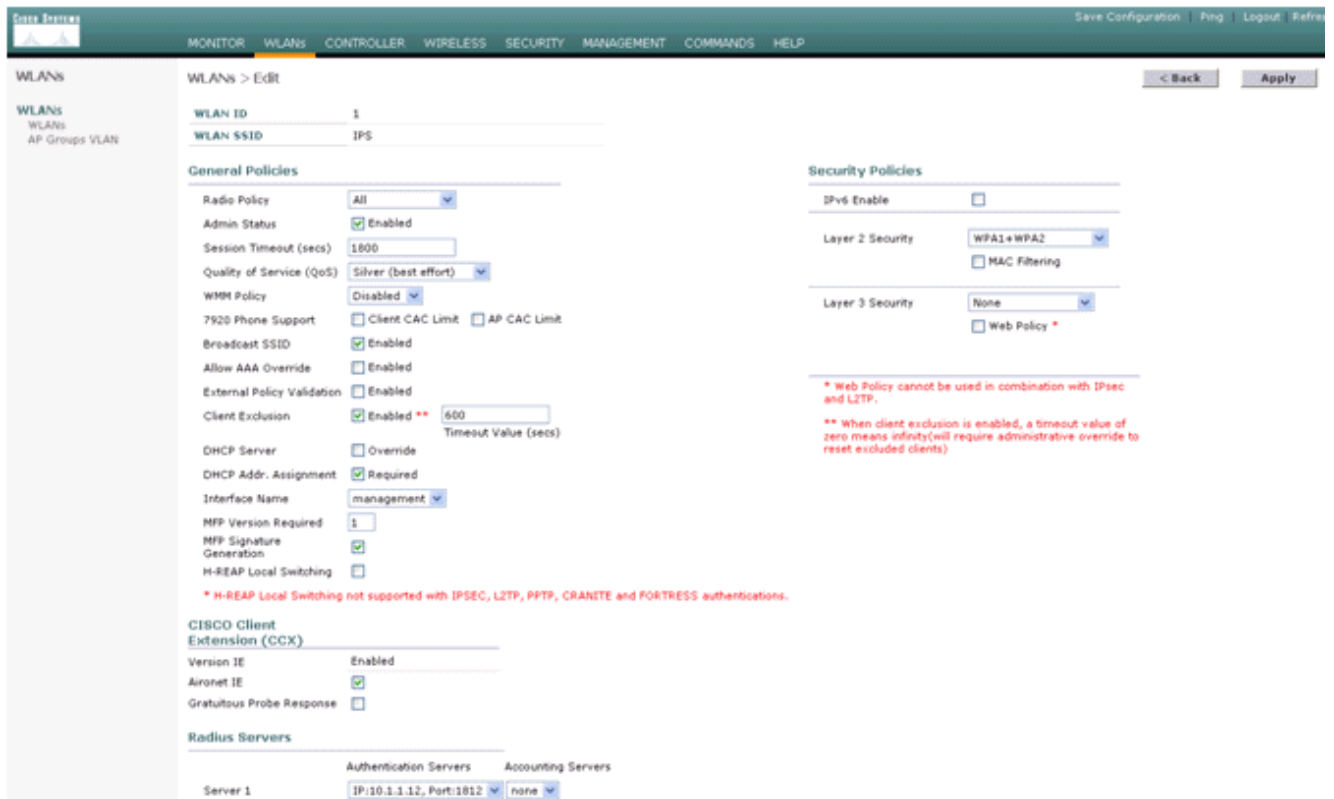
3. Verifique o status da conexão entre o sensor IPS e a WLC.

The screenshot shows the 'CIDS Sensors List' page in the Cisco WLC GUI. The left sidebar is the same as in the previous screenshot. The main content area displays a table with the following data:

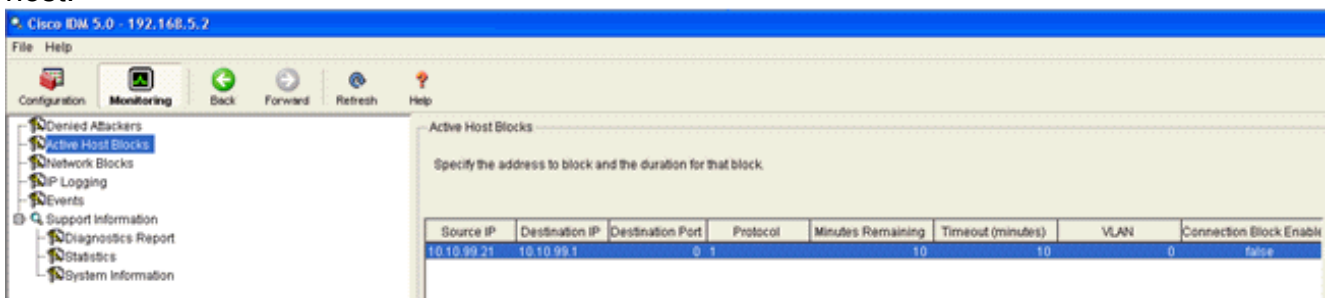
Index	Server Address	Port	State	Query Interval	Last Query (count)	
1	192.168.5.2	443	Enabled	15	Success (6083)	Detail Remove

A 'New...' button is visible at the top right of the table area.

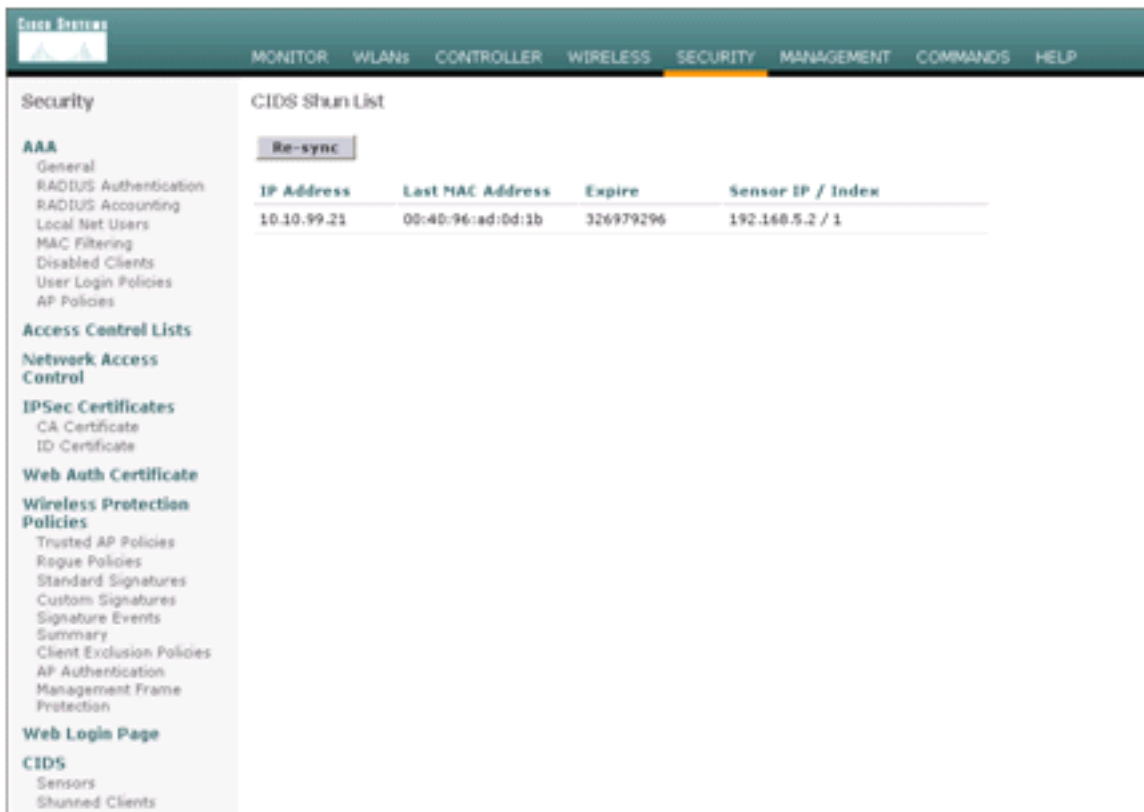
4. Depois de estabelecer a conectividade com o Cisco IPS Sensor, verifique se a configuração da WLAN está correta e se você habilita a **Exclusão do cliente**. O valor de tempo limite de exclusão de cliente padrão é de 60 segundos. Observe também que, independentemente do temporizador de exclusão do cliente, a exclusão do cliente persiste enquanto o bloco do cliente chamado pelo IDS permanecer ativo. O tempo de bloqueio padrão no IDS é de 30 minutos.



5. Você pode disparar um evento no sistema Cisco IPS quando faz uma NMAP Scan para determinados dispositivos na rede ou quando faz um ping para alguns hosts monitorados pelo Cisco IPS Sensor. Quando um alarme for disparado no Cisco IPS, vá para **Monitoramento e blocos de host ativos** para verificar os detalhes sobre o host.

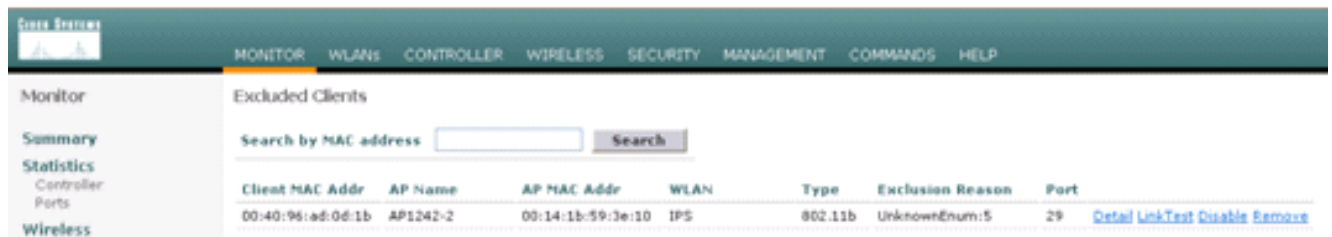


A lista Clientes descontinuados no controlador agora é preenchida com o endereço IP e MAC do

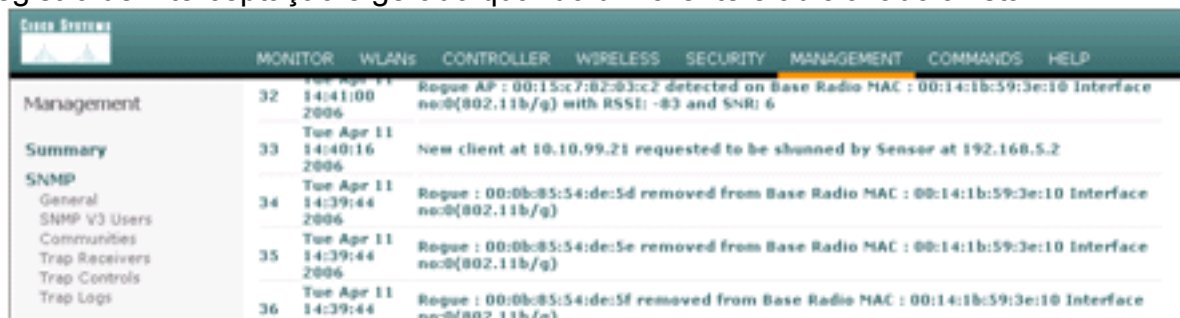


host.
usuário é adicionado à lista de exclusões de clientes.

O

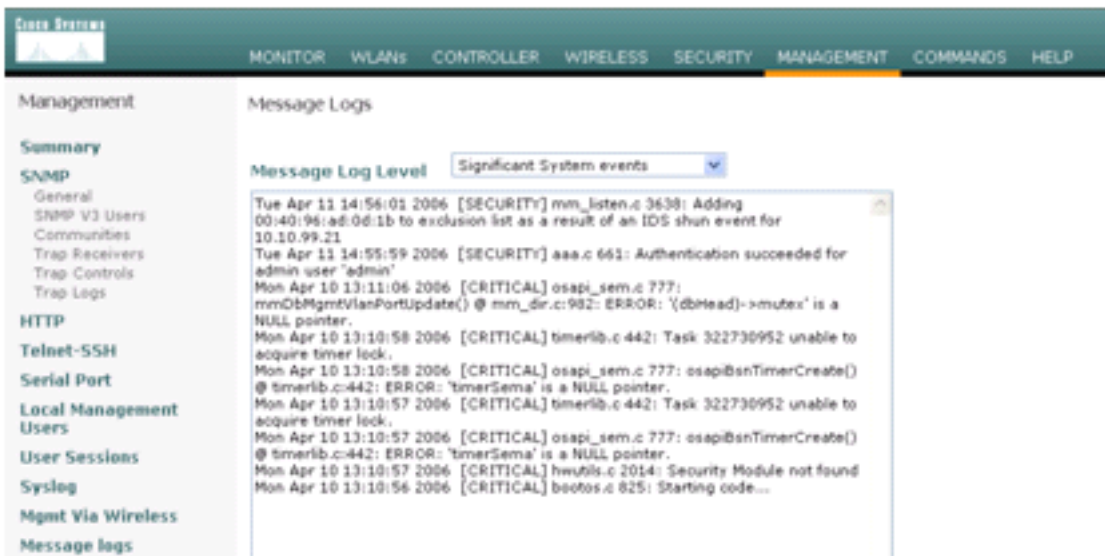


Um registro de interceptação é gerado quando um cliente é adicionado à lista

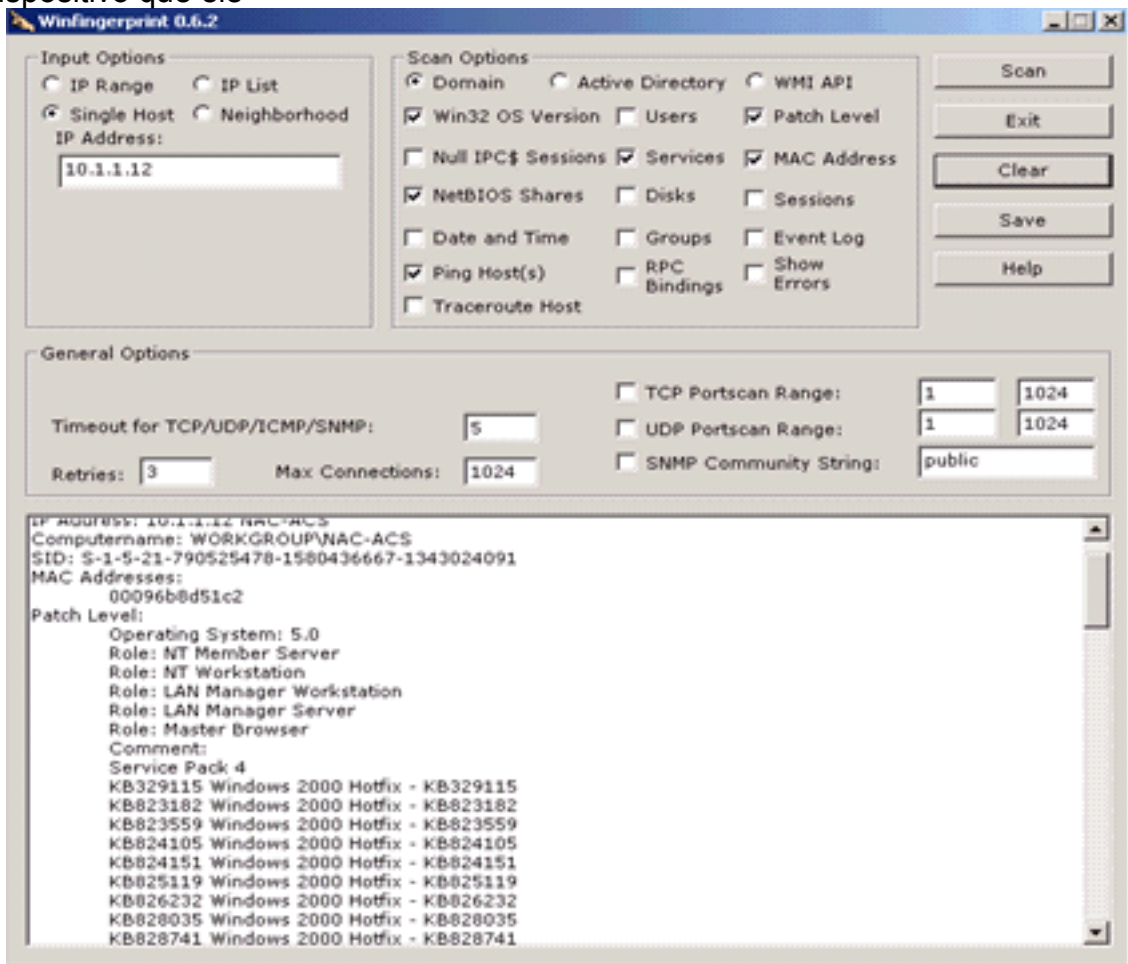


shun.
registro de mensagens também é gerado para o

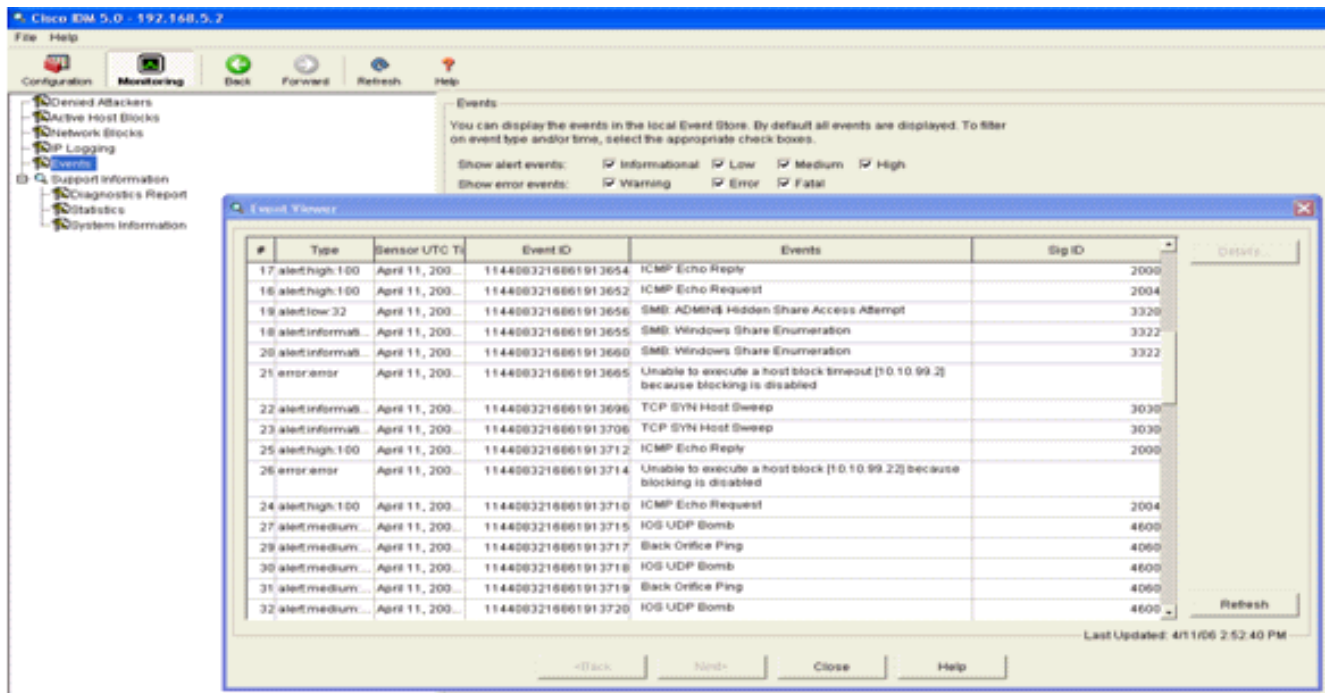
Um



evento. Alguns eventos adicionais são gerados no Cisco IPS Sensor quando uma verificação NMAP é feita em um dispositivo que ele



monitora. Esta janela mostra os eventos gerados no Cisco IPS Sensor.



Exemplo de configuração do sensor Cisco IDS

Esta é a saída do script de configuração 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

```

```

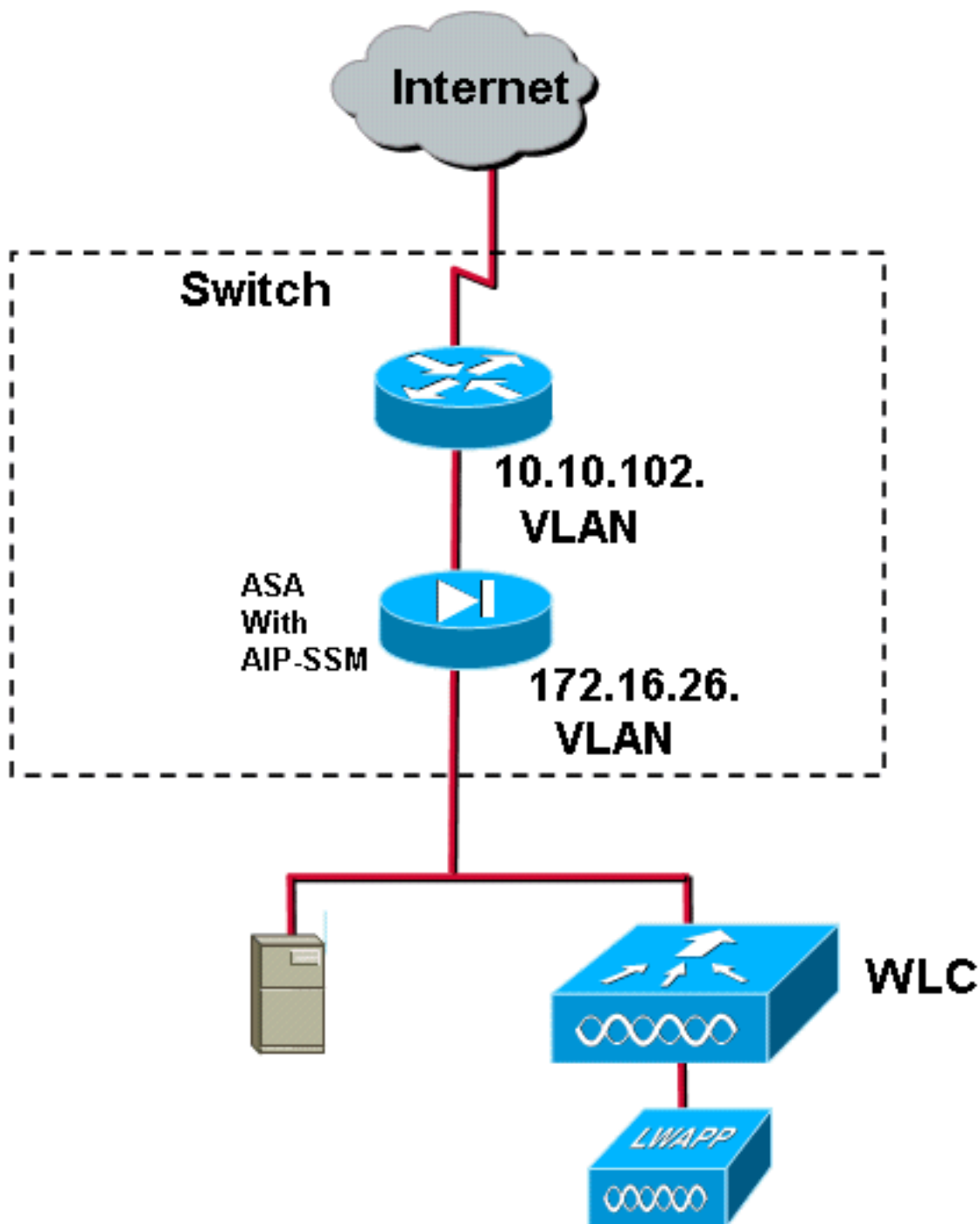
exit
signatures 2002 0
alert-severity high
status
enabled true
exit
exit
signatures 2003 0
alert-severity high
status
enabled true
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|request-block-host
exit
status
enabled true
exit
exit
exit
! -----
service event-action-rules 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 IDS](#)

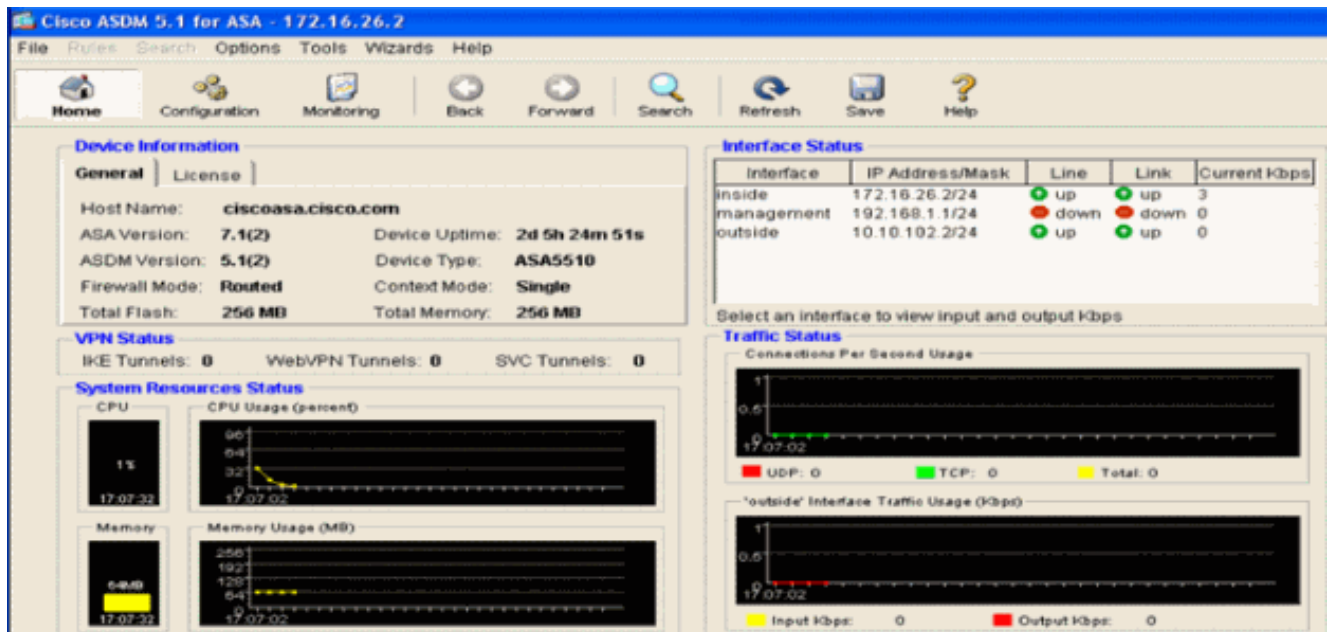
Ao contrário de um sensor de detecção de intrusão tradicional, um ASA deve estar sempre no caminho dos dados. Em outras palavras, em vez de estender o tráfego de uma porta de switch

para uma porta de sniffing passiva no sensor, o ASA deve receber dados em uma interface, processá-los internamente e encaminhá-los para outra porta. Para IDS, use o MPF (modular policy framework, estrutura de política modular) para copiar o tráfego que o ASA recebe para o AIP-SSM (Advanced Inspection and Prevention Security Services Module, módulo interno de serviços de segurança de inspeção e prevenção) para inspeção.

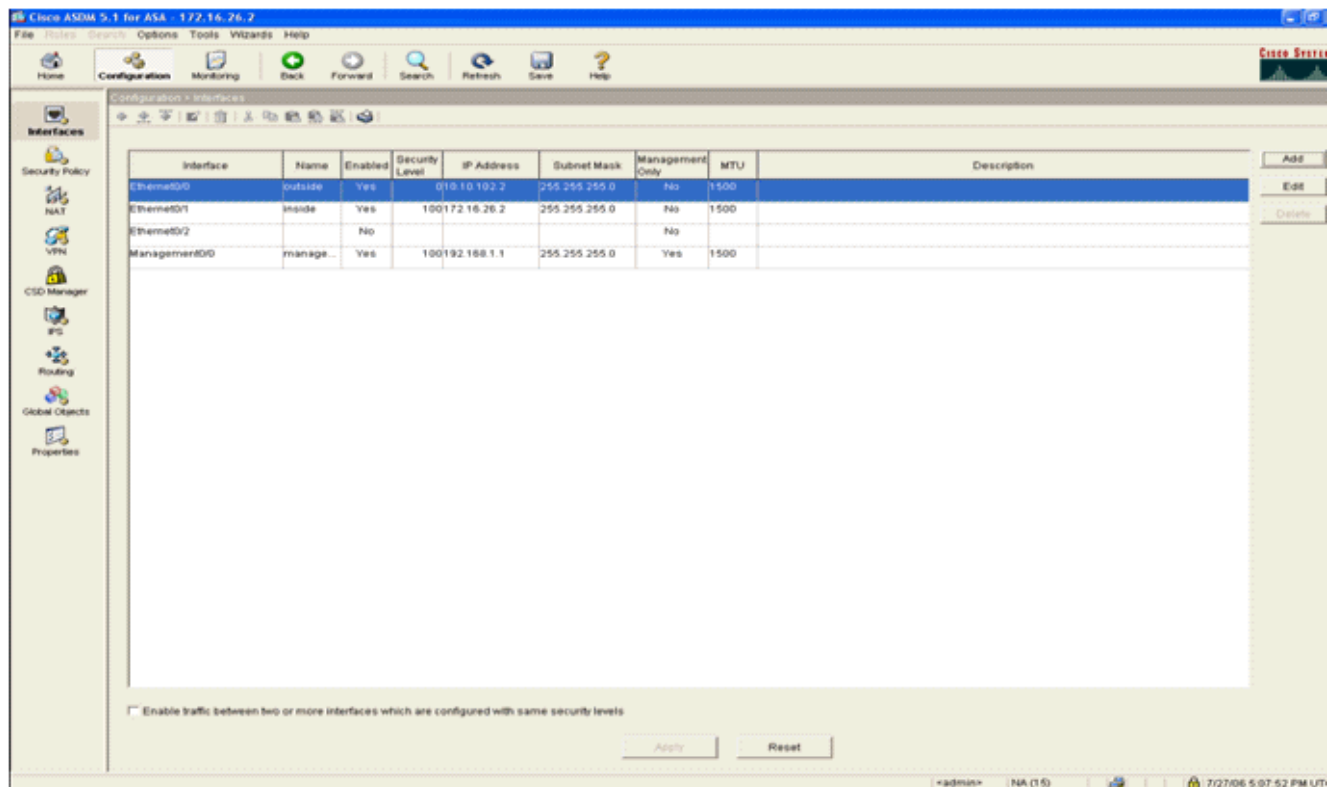


Neste exemplo, o ASA usado já está configurado e transmite tráfego. Estas etapas demonstram como criar uma política que envia dados para o AIP-SSM.

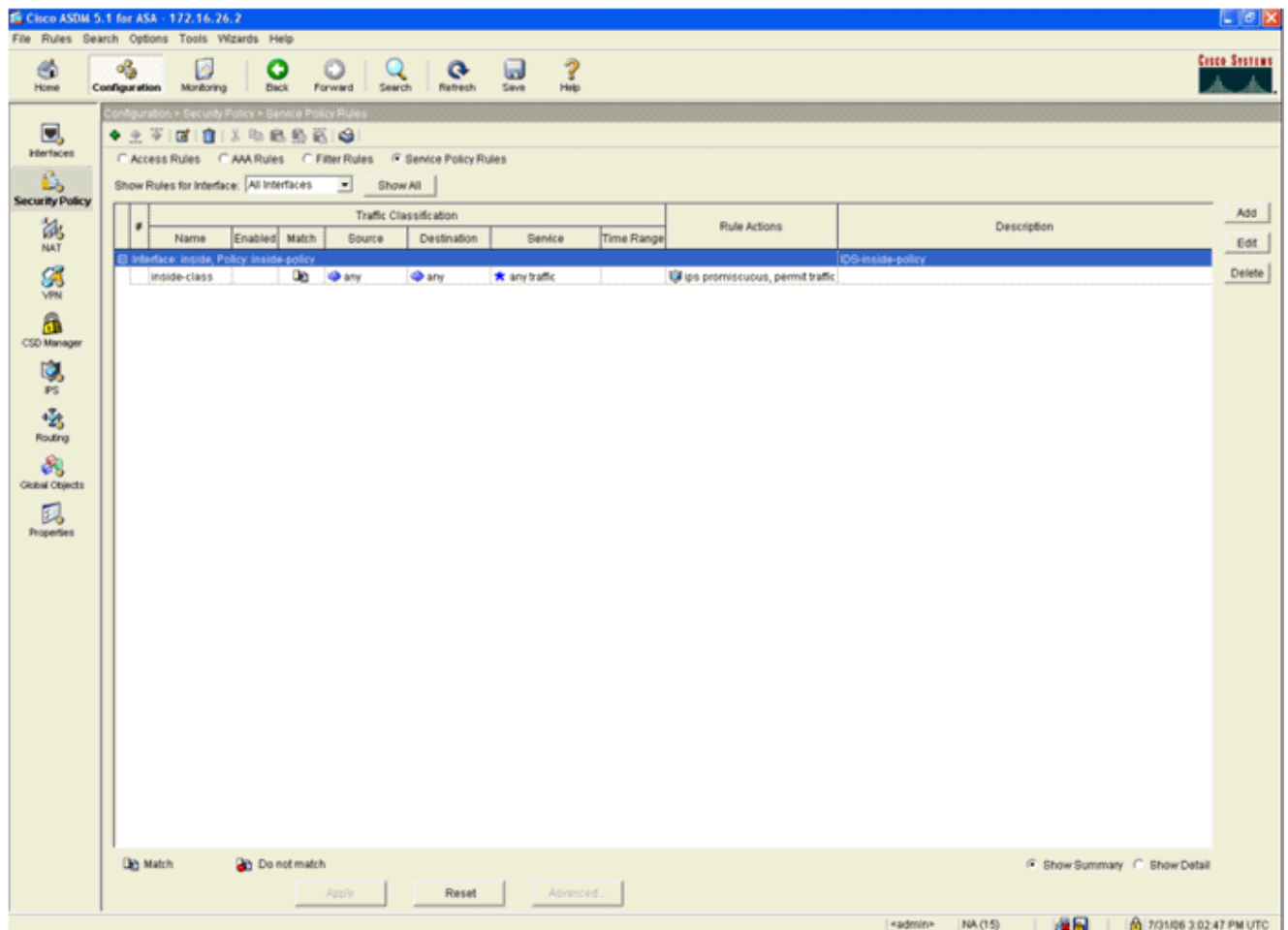
1. Faça login no ASA usando o ASDM. Após o login bem-sucedido, a janela ASA Main System (Sistema principal do ASA) é exibida.



2. Clique em **Configuração** na parte superior da página. A janela muda para uma visualização das interfaces do ASA.



3. Clique em **Security Policy** no lado esquerdo da janela. Na janela resultante, escolha a guia **Service Policy Rules**.



4. Clique em **Adicionar** para criar uma nova política. O Assistente para Adicionar Regra de Política de Serviço é iniciado em uma nova janela. Clique em **Interface** e escolha a interface correta na lista suspensa para criar uma nova política vinculada a uma das interfaces que transmite tráfego. Forneça à política um nome e uma descrição do que ela faz usando as duas caixas de texto. Clique em **Next** para ir para a próxima etapa.

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

Step 1: Configure a service policy.

Step 2: Configure the traffic classification criteria for the service policy rule.

Step 3: Configure actions on the traffic classified by the service policy rule.

Create a service policy and apply to:

Interface:

Policy Name:

Description:

Global - applies to all interfaces

Policy Name:

Description:

< Back Next > Cancel Help

5. Crie uma nova classe de tráfego para aplicar à política.É razoável criar classes específicas para inspecionar tipos de dados específicos, mas neste exemplo, Qualquer tráfego é selecionado para simplificar. Clique em **Avançar** para continuar.

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic match criteria

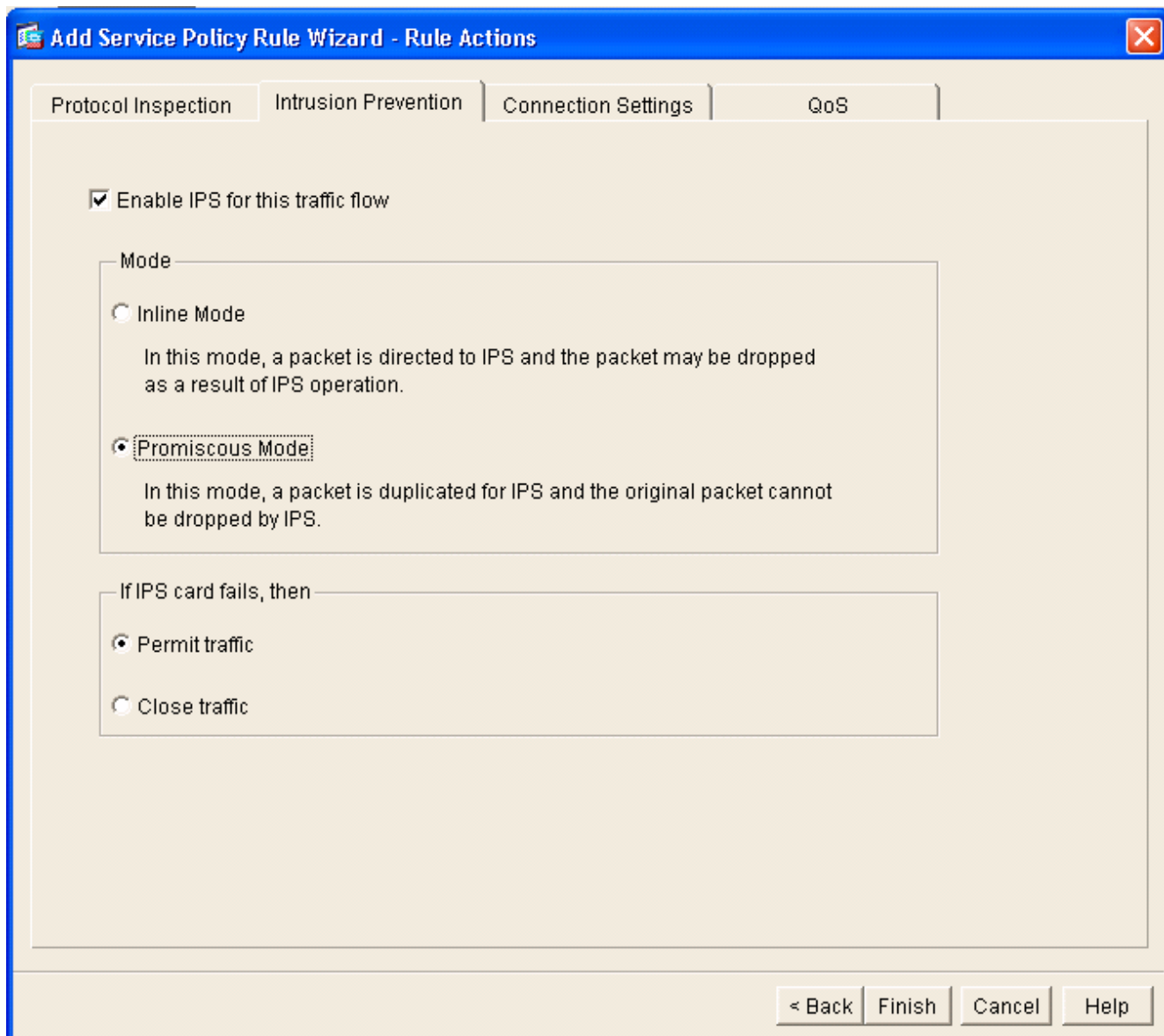
- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

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

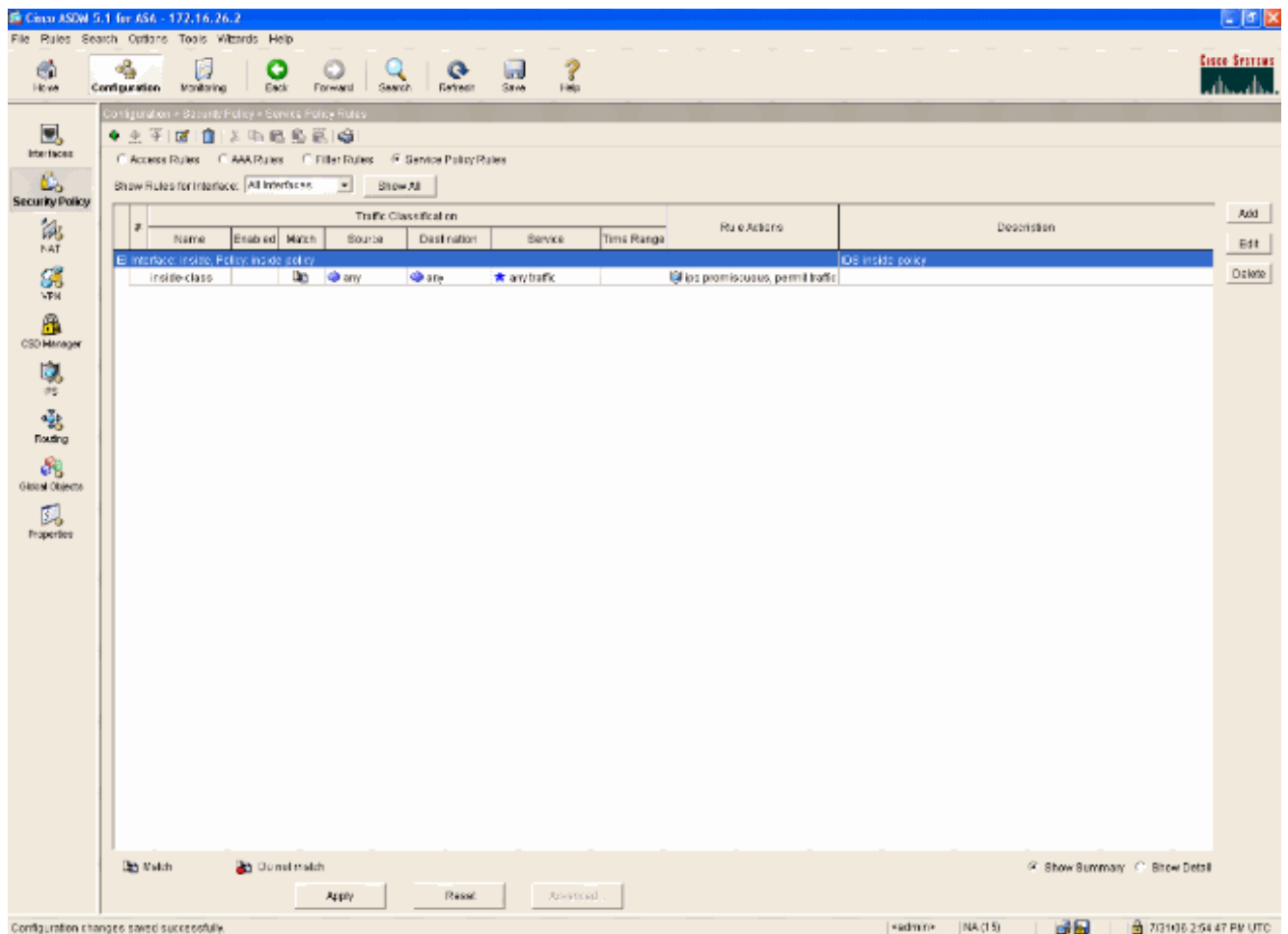
Use class-default as the traffic class.

< Back Next > Cancel Help

6. Conclua estes passos para instrua o ASA a direcionar o tráfego para seu AIP-SSM. Marque **Enable IPS for this traffic flow** para habilitar a detecção de intrusão. Defina o modo como **Promiscuous** para que uma cópia do tráfego seja enviada para o módulo fora de banda, em vez de colocar o módulo em linha com o fluxo de dados. Clique em **Permit traffic** para garantir que o ASA alterne para um estado de fail-open no caso de falha do AIP-SSM. Clique em **Finish** para confirmar a alteração.



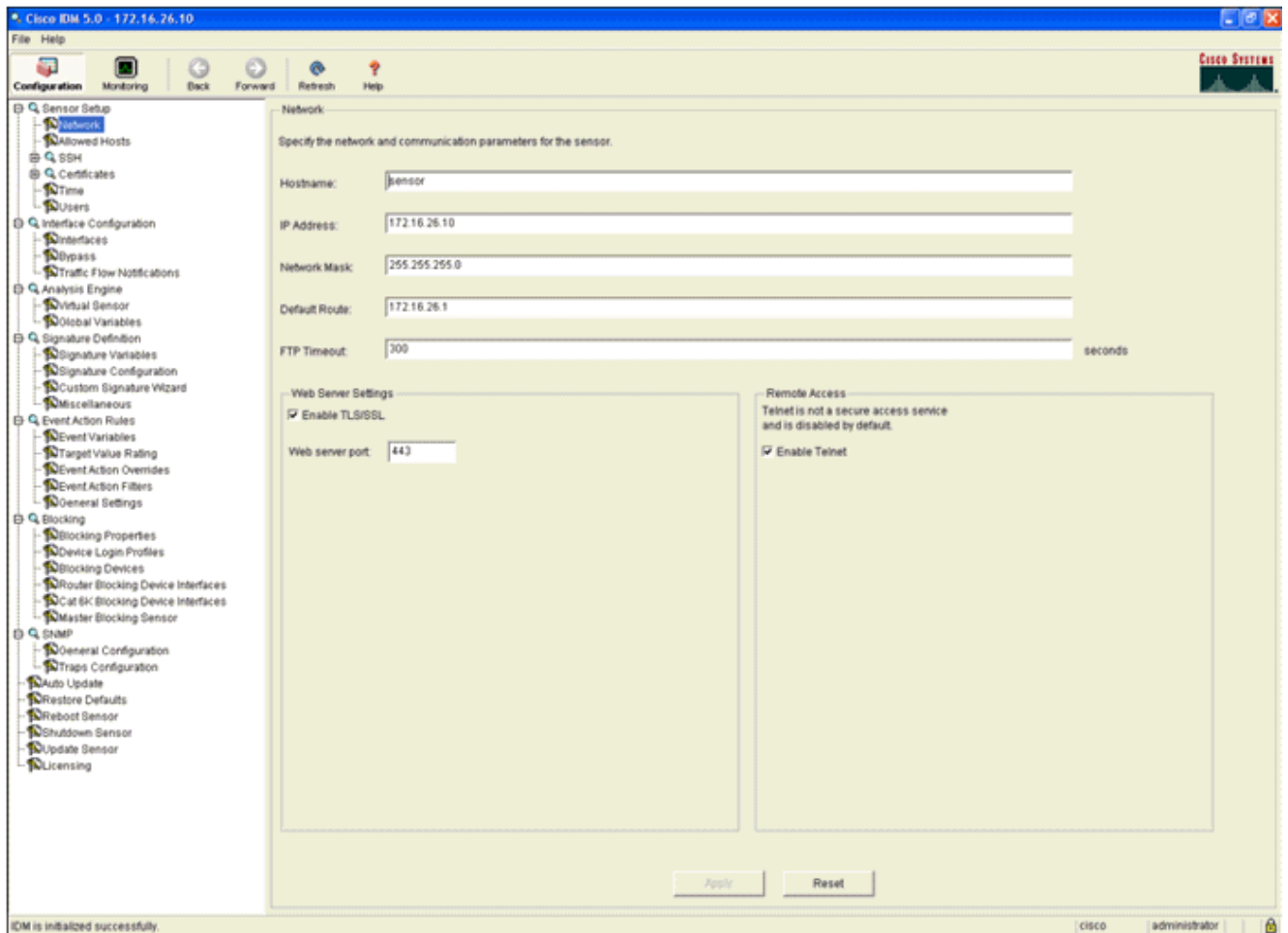
7. O ASA agora está configurado para enviar tráfego para o módulo IPS. Clique em **Salvar** na linha superior para gravar as alterações no ASA.



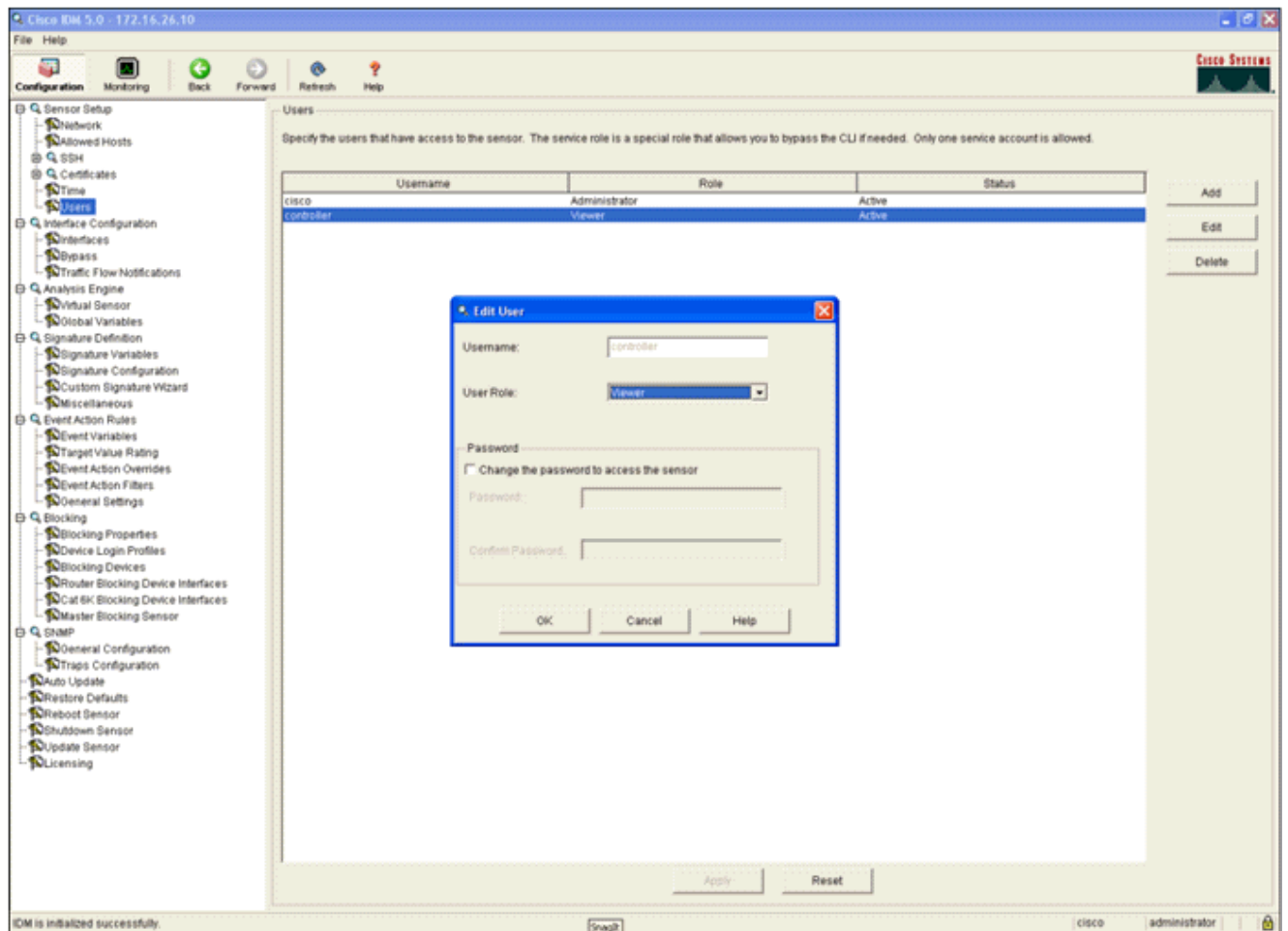
Configurar o AIP-SSM para a inspeção de tráfego

Enquanto o ASA envia dados para o módulo IPS, associe a interface AIP-SSM ao seu mecanismo de sensor virtual.

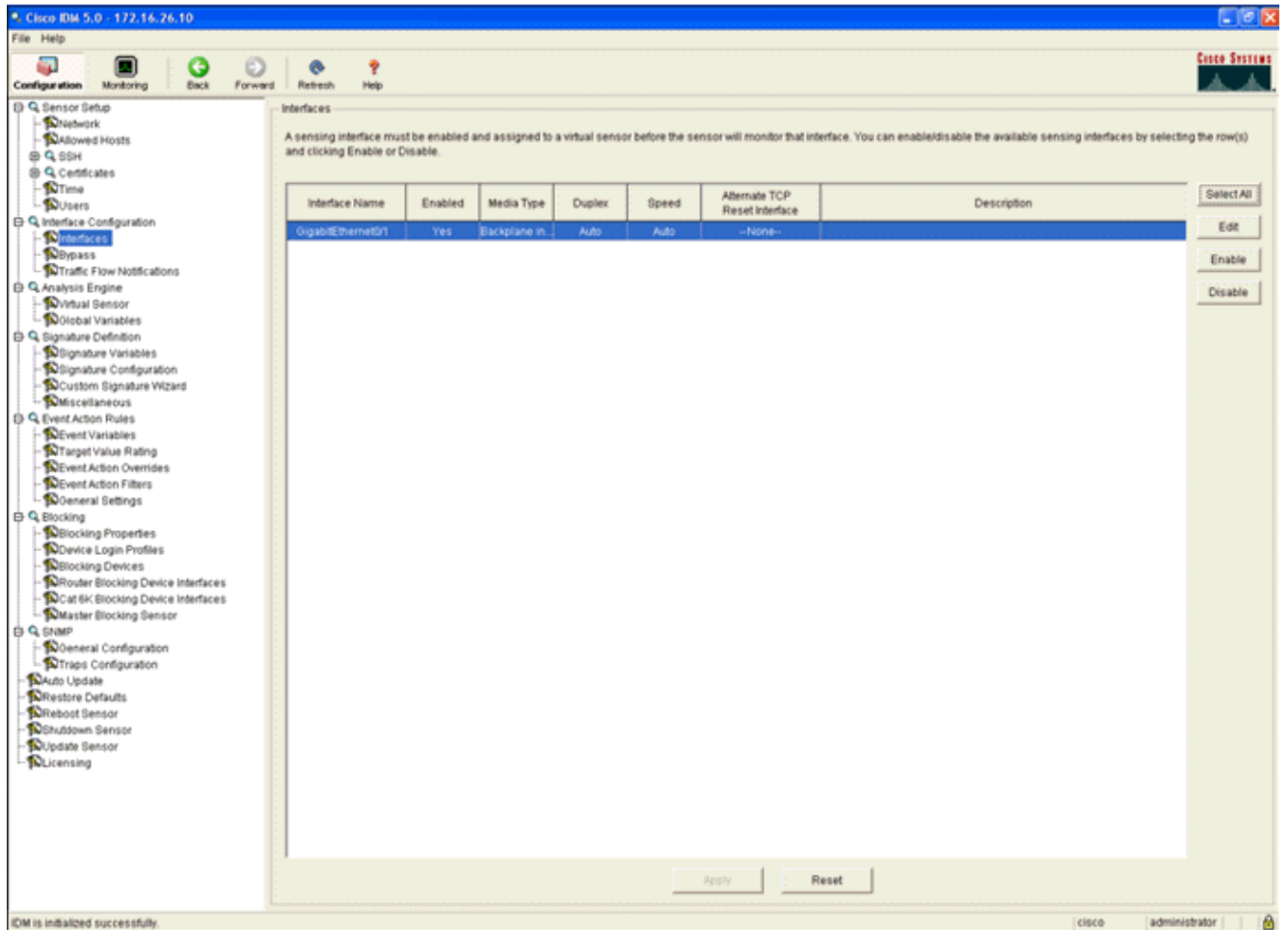
1. Faça login no AIP-SSM usando IDM.



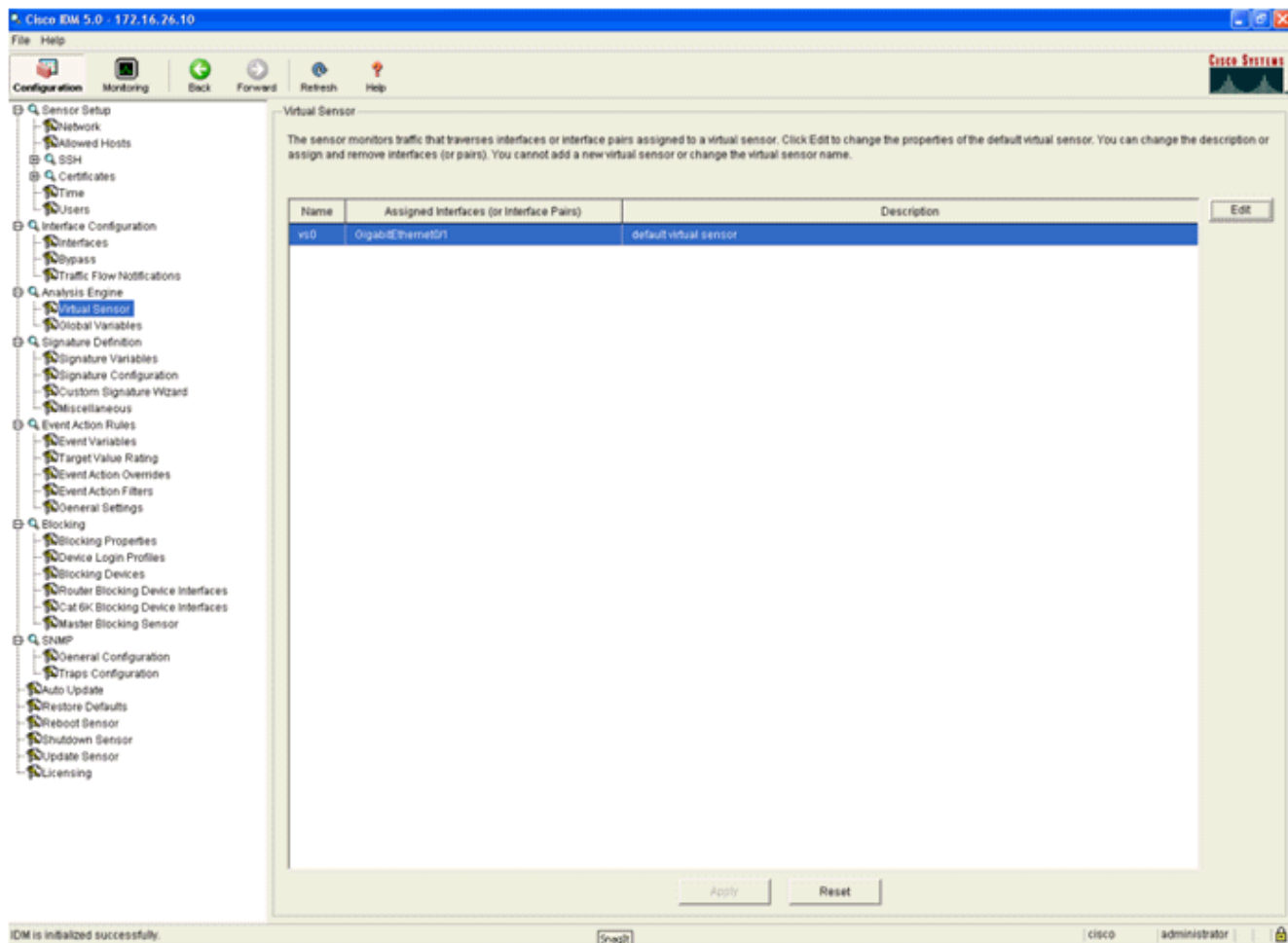
2. Adicione um usuário com pelo menos privilégios de visualizador.



3. Ative a interface.



4. Verifique a configuração do sensor virtual.



[Configurar uma WLC para pesquisar o AIP-SSM para blocos de clientes](#)

Conclua estes passos quando o sensor estiver configurado e pronto para ser adicionado à controladora:

1. Escolha **Security > CIDS > Sensors > New** na WLC.
2. Adicione o endereço IP, o número da porta TCP, o nome de usuário e a senha que você criou na seção anterior.
3. Para obter a impressão digital do sensor, execute esse comando no sensor e adicione a impressão digital SHA1 à WLC (sem dois-pontos). Isso é usado para proteger a comunicação de polling de controlador para 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
```

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

- Index:** 2
- Server Address:** 172.16.26.10
- Port:** 443
- Username:** controller
- Password:** *****
- State:**
- Query Interval:** 10 seconds
- Fingerprint (SHA1 hash):** 90C9969B4EFA74F8528092BBBC483C45B4876C55 (40 hex chars) (hash key is already set)
- Last Query (count):** Success (1400)

4. Verifique o status da conexão entre o AIP-SSM e a WLC.

The screenshot shows the Cisco Systems Security configuration page for CIDS Sensors List. The left sidebar contains a navigation menu with categories: AAA, Access Control Lists, IPSec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area displays a table of CIDS sensors:

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

[Adicionar uma assinatura de bloqueio ao AIP-SSM](#)

Adicione uma assinatura de inspeção para bloquear o tráfego. Embora haja muitas assinaturas que podem fazer o trabalho com base nas ferramentas disponíveis, este exemplo cria uma assinatura que bloqueia pacotes de ping.

1. Selecione a assinatura de 2004 (ICMP Echo Request) para executar uma rápida verificação de

configuração.

The screenshot shows the Cisco IDS 5.0 configuration interface. The main window displays the 'Signature Configuration' table. The table has columns for Sig ID, SubSig ID, Name, Enabled, Action, Severity, Fidelity Rating, Type, Engine, and Retired. The row for Sig ID 2004 is highlighted in blue. The 'Signature Configuration' section is selected in the left-hand navigation tree.

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired
1330	2	TCP Drop - Urgent Pointer WI...	No	Modify Packet I...	Informato...	100	Default	Normalizer	No
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informato...	100	Default	Normalizer	No
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informato...	100	Default	Normalizer	No
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informato...	100	Default	Normalizer	No
2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No
2004	0	ICMP Echo Request	Yes	Produce Alert Request Block...	High	100	Tuned	Atomic IP	No
2005	0	ICMP Time Exceeded for a D...	No	Produce Alert	Informato...	100	Default	Atomic IP	No
2006	0	ICMP Parameter Problem on ...	No	Produce Alert	Informato...	100	Default	Atomic IP	No
2007	0	ICMP Timestamp Request	No	Produce Alert	Informato...	100	Default	Atomic IP	No
2008	0	ICMP Timestamp Reply	No	Produce Alert	Informato...	100	Default	Atomic IP	No
2009	0	ICMP Information Request	No	Produce Alert	Informato...	100	Default	Atomic IP	No

2. Ative a assinatura, defina a Gravidade do alerta como **Alta** e defina a Ação do evento para **Produzir o Host de alerta e bloco de solicitação** para concluir esta etapa de verificação. Observe que a ação Request Block Host (Host de bloco de solicitação) é a chave para sinalizar a WLC para criar exceções de cliente.

Edit Signature

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

Sig Description:

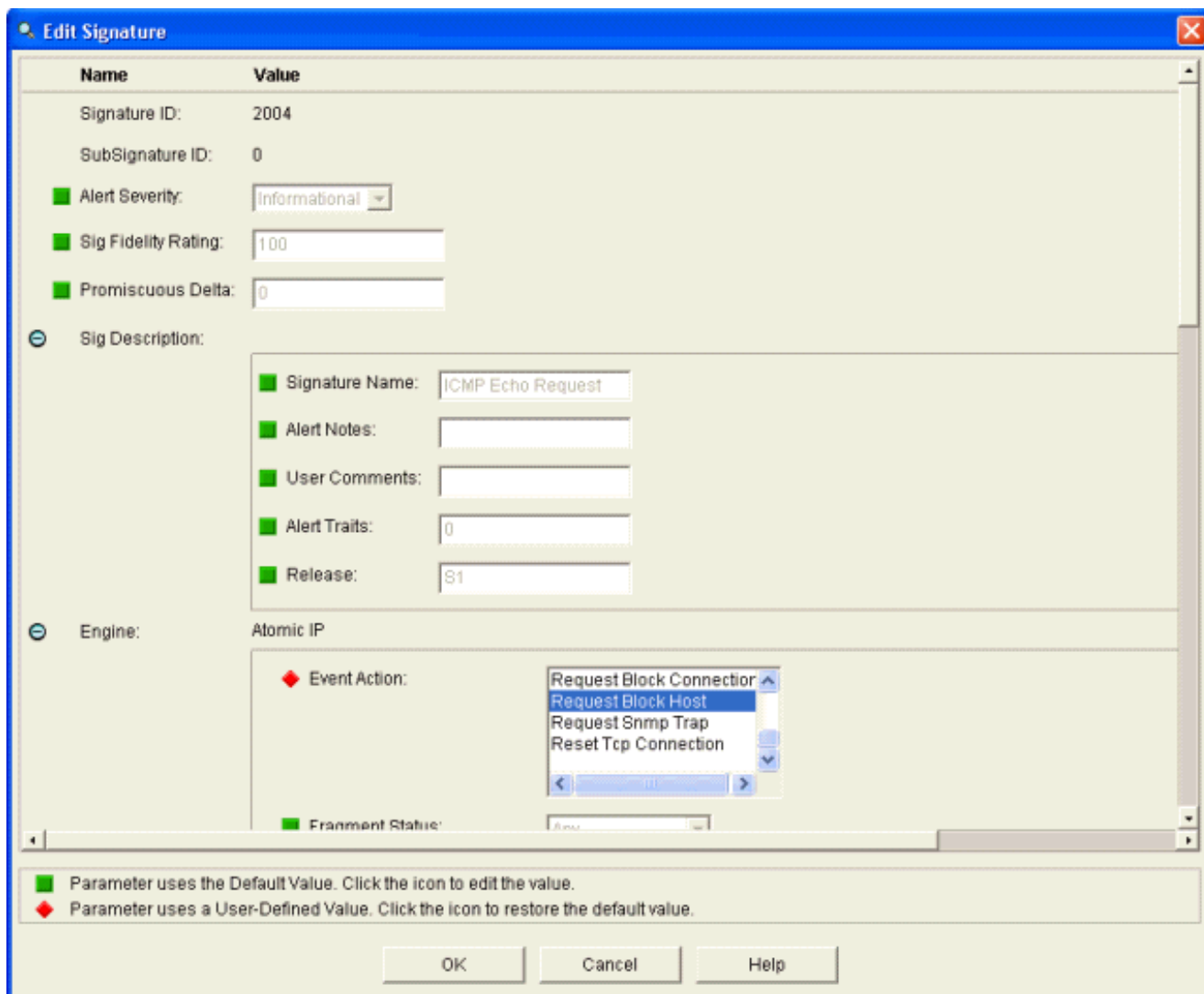
Signature Name:	ICMP Echo Request
Alert Notes:	
User Comments:	
Alert Traits:	0
Release:	B1

Engine: Atomic IP

Event Action:	<ul style="list-style-type: none"> Produce Alert Produce Verbose Alert Request Block Connector Request Block Host Request Snmp Trap 													
Fragment Status:	Any													
Specify Layer 4 Protocol:	Yes													
Layer 4 Protocol:	<table border="1"> <tbody> <tr> <td>ICMP Protocol</td> </tr> <tr> <td> Specify ICMP Sequence:</td> <td>No</td> </tr> <tr> <td> Specify ICMP Type:</td> <td>Yes</td> </tr> <tr> <td> ICMP Type:</td> <td>8</td> </tr> <tr> <td> Specify ICMP Code:</td> <td>No</td> </tr> <tr> <td> Specify ICMP Identifier:</td> <td>No</td> </tr> <tr> <td> Specify ICMP Total Length:</td> <td>No</td> </tr> </tbody> </table>	ICMP Protocol	Specify ICMP Sequence:	No	Specify ICMP Type:	Yes	ICMP Type:	8	Specify ICMP Code:	No	Specify ICMP Identifier:	No	Specify ICMP Total Length:	No
ICMP Protocol														
Specify ICMP Sequence:	No													
Specify ICMP Type:	Yes													
ICMP Type:	8													
Specify ICMP Code:	No													
Specify ICMP Identifier:	No													
Specify ICMP Total Length:	No													

Parameter uses the Default Value. Click the icon to edit the value.
 Parameter uses a User-Defined Value. Click the icon to restore the default value.

OK Cancel Help

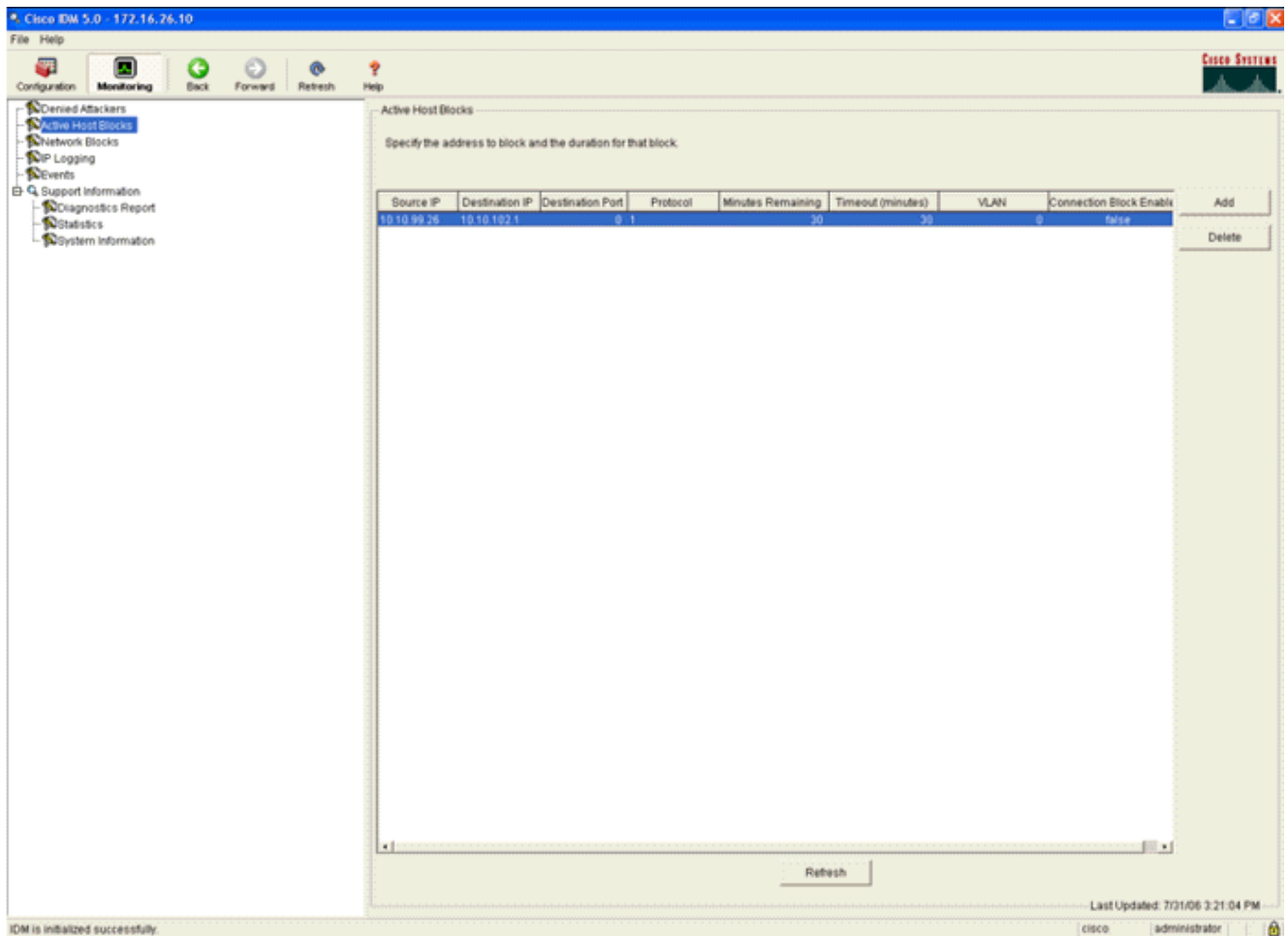


3. Clique em **OK** para salvar a assinatura.
4. Verifique se a assinatura está ativa e se está definida para executar uma ação de bloqueio.
5. Clique em **Apply** para confirmar a assinatura no módulo.

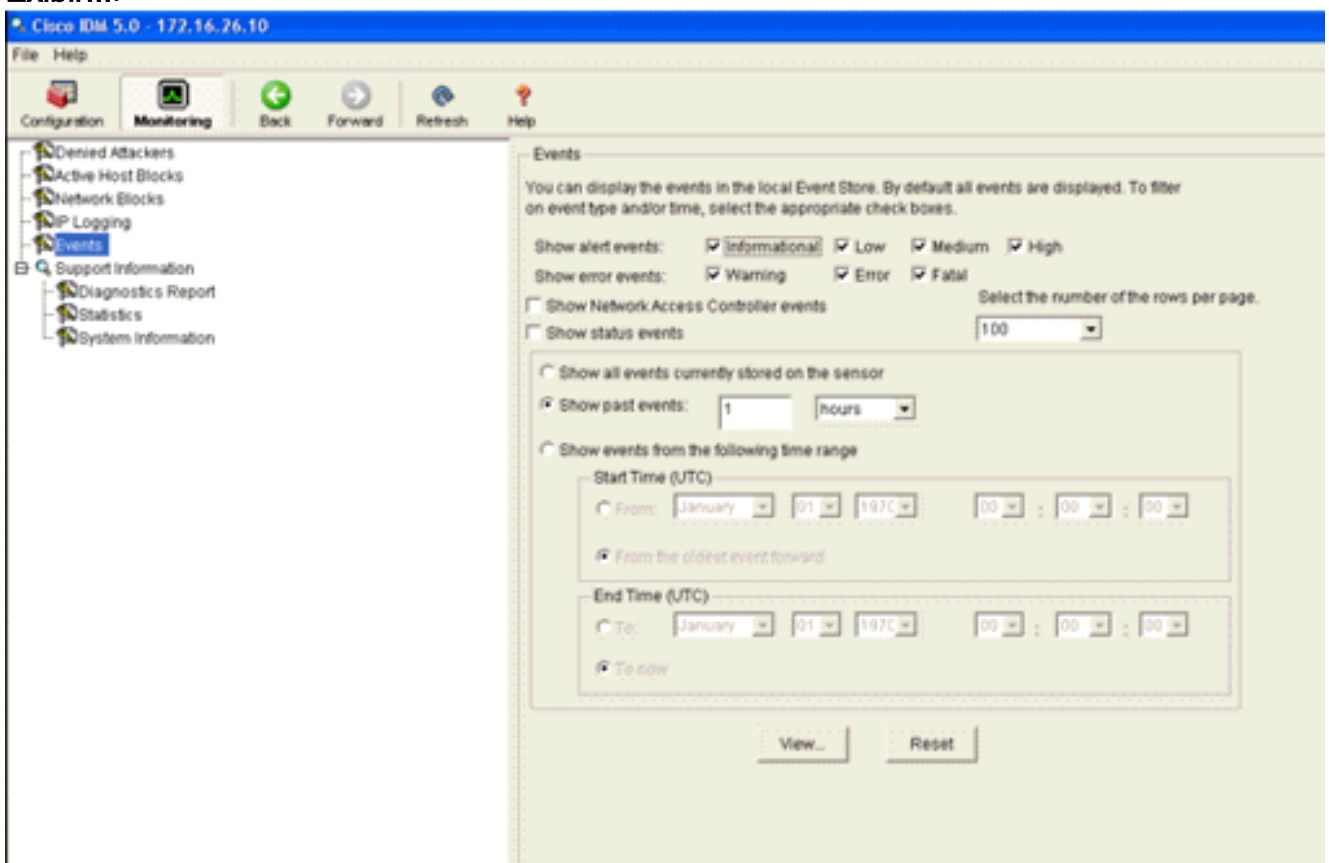
Monitorar bloqueio e eventos com IDM

Conclua estes passos:

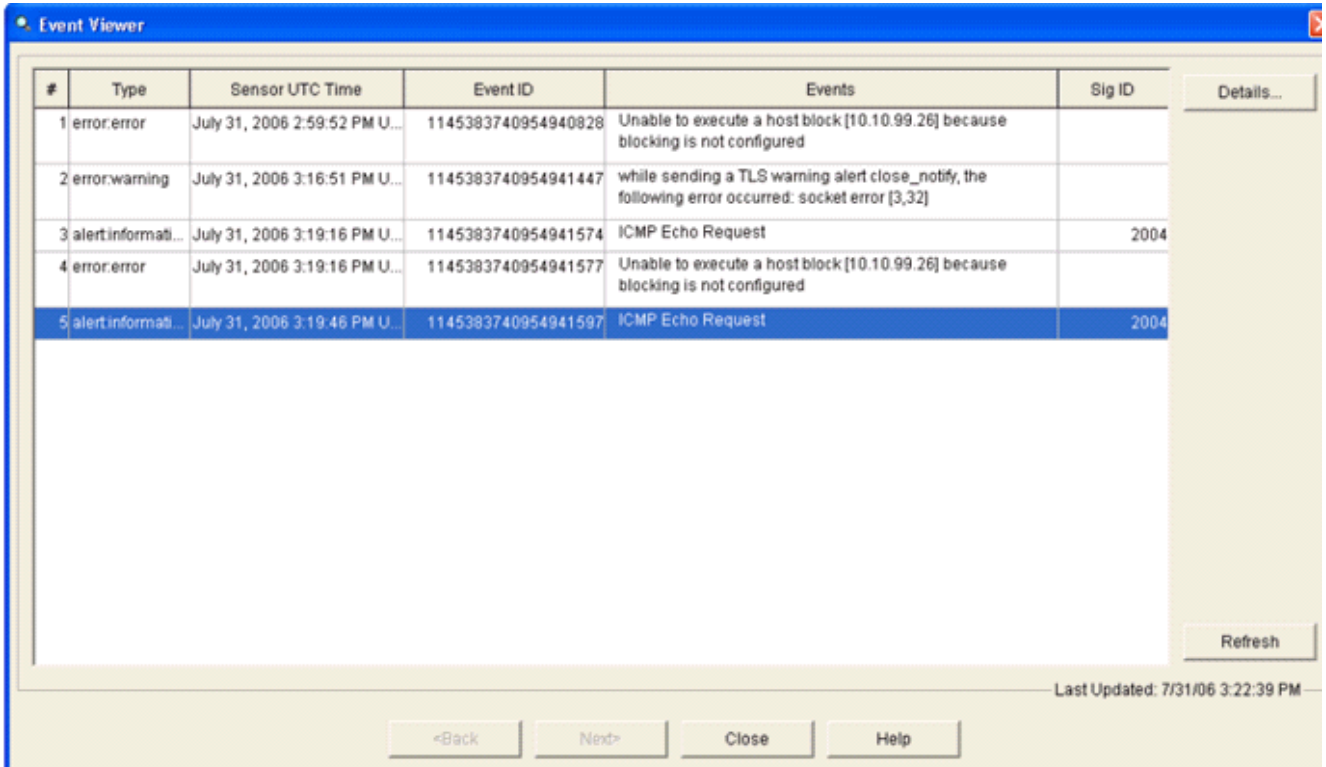
1. Quando a assinatura é disparada com êxito, há dois lugares no IDM para observar isso. O primeiro método mostra os blocos ativos que o AIP-SSM instalou. Clique em **Monitoramento** na linha superior de ações. Na lista de itens exibida no lado esquerdo, selecione **Active Host Blocks**. Sempre que a assinatura do ping for disparada, a janela Blocos de host ativos mostrará o endereço IP do infrator, o endereço do dispositivo sob ataque e o tempo que resta para o qual o bloco está em vigor. O tempo de bloqueio padrão é de 30 minutos e pode ser ajustado. No entanto, a alteração desse valor não é discutida neste documento. Consulte a documentação de configuração do ASA conforme necessário para obter informações sobre como alterar esse parâmetro. Remova o bloco imediatamente, selecione-o na lista e clique em **Excluir**.



O segundo método para exibir assinaturas disparadas usa o buffer de eventos AIP-SSM. Na página Monitoramento do IDM, selecione **Eventos** na lista de itens no lado esquerdo. O utilitário de pesquisa Eventos é exibido. Defina os critérios de pesquisa apropriados e clique em **Exibir...**



2. O Visualizador de Eventos aparece então com uma lista de eventos que correspondem aos critérios fornecidos. Percorra a lista e localize a assinatura ICMP Echo Request modificada nas etapas de configuração anteriores. Procure na coluna Eventos o nome da assinatura ou procure o número de identificação da assinatura na coluna ID de assinatura.



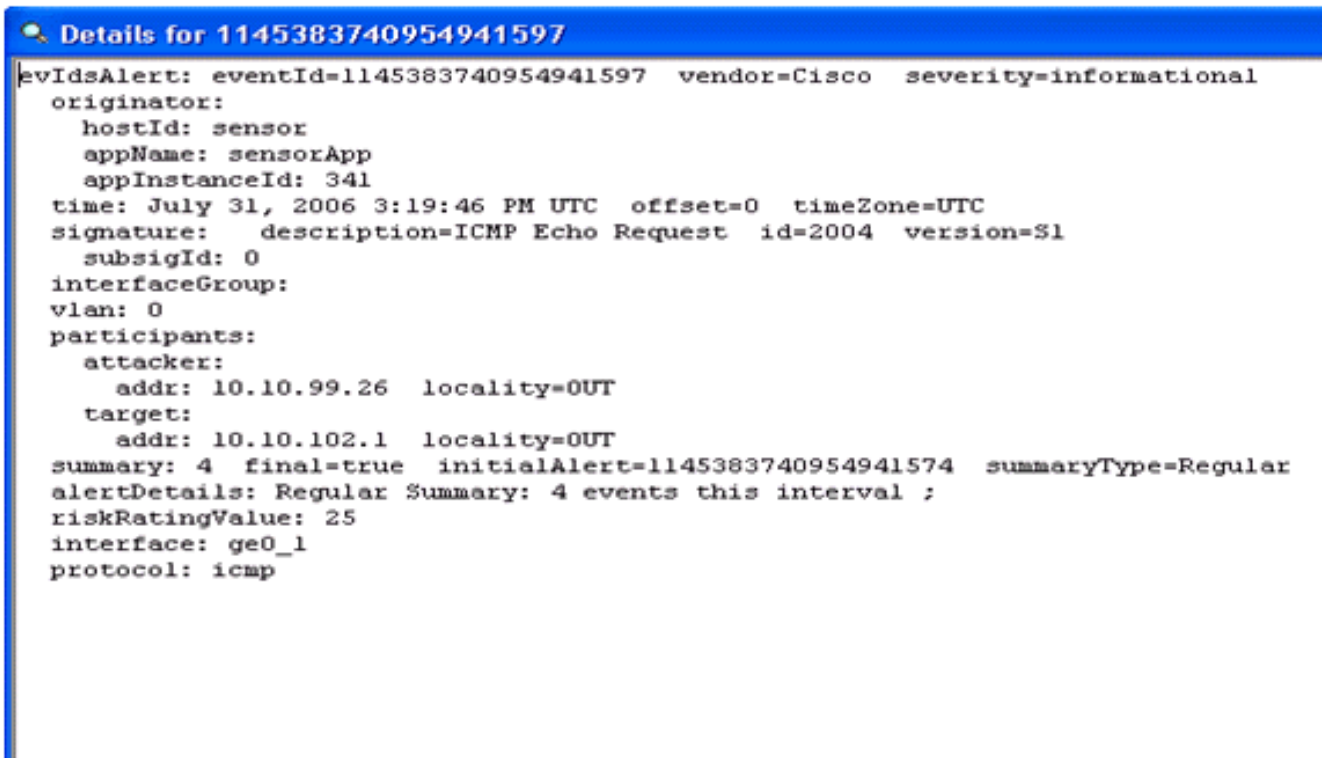
#	Type	Sensor UTC Time	Event ID	Events	Sig ID	Details...
1	error:error	July 31, 2006 2:59:52 PM U...	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
2	error:warning	July 31, 2006 3:16:51 PM U...	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
3	alert:informati...	July 31, 2006 3:19:16 PM U...	1145383740954941574	ICMP Echo Request	2004	
4	error:error	July 31, 2006 3:19:16 PM U...	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
5	alert:informati...	July 31, 2006 3:19:46 PM U...	1145383740954941597	ICMP Echo Request	2004	

Refresh

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

<Back Next> Close Help

3. Depois de localizar a assinatura, clique duas vezes na entrada para abrir uma nova janela. A nova janela contém informações detalhadas sobre o evento que disparou a assinatura.



```
evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
originator:
  hostId: sensor
  appName: sensorApp
  appInstanceId: 341
time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
signature: description=ICMP Echo Request id=2004 version=S1
  subsigId: 0
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: 10.10.99.26 locality=OUT
  target:
    addr: 10.10.102.1 locality=OUT
summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
alertDetails: Regular Summary: 4 events this interval ;
riskRatingValue: 25
interface: ge0_1
protocol: icmp
```

A lista Clientes descontinuados na controladora é preenchida nesse momento com o endereço IP e MAC do host.

The screenshot shows the 'CIDS Shun List' page in the WCS interface. The left sidebar contains a navigation menu with categories like AAA, Access Control Lists, IPsec Certificates, Web Auth Certificate, Wireless Protection Policies, Web Login Page, and CIDS. The main content area has a 'Re-sync' button and a table with the following data:

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

O usuário é adicionado à lista de exclusões de clientes.

The screenshot shows the 'Excluded Clients' page in the WCS interface. The left sidebar contains a navigation menu with categories like Monitor, Summary, Statistics, and Wireless. The main content area has a search bar labeled 'Search by MAC address' and a table with the following data:

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

Monitorar eventos no WCS

Os eventos de segurança que disparam um bloco no AIP-SSM fazem com que o controlador adicione o endereço do infrator à lista de exclusão do cliente. Um evento também é gerado no WCS.

1. Use o utilitário **Monitor > Alarm** no menu principal do WCS para visualizar o evento de exclusão. O WCS exibe inicialmente todos os alarmes não apagados e também apresenta uma função de pesquisa no lado esquerdo da janela.
2. Modifique os critérios de pesquisa para localizar o bloco do cliente. Em Severity (Gravidade), escolha **Minor** e defina também Alarm Category (Categoria de alarme) como **Security (Segurança)**.

3. Clique em Buscar.

The screenshot shows the Cisco Wireless Control System (WCS) interface. The 'Alarms' section is active, displaying a list of critical security events. The left sidebar shows filters for Severity (Critical) and Alarm Category (All Types). A search button is visible. The main table lists alarms with columns for Severity, Failure Object, Owner, Date/Time, and Message. A small status summary table is located at the bottom left of the interface.

Severity	Failure Object	Owner	Date/Time	Message
Critical	Radio_AIR-LAP1242AG-A/G		6/2/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11b/g' is ...
Critical	Radio_AIR-LAP1242AG-A/G		6/2/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11a' is do...
Critical	AP_AIR-LAP1242AG-A/00:14:1b:59:41:80		6/2/06 9:02 AM	AP 'AIR-LAP1242AG-A' disassociated from Control...
Critical	Radio_ap:75:12:e0/2		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11a' is down o...
Critical	Radio_ap:75:12:e0/1		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11b/g' is down...
Critical	AP_ap:75:12:e0/00:0b:85:75:12:e0		7/21/06 1:51 PM	AP 'ap:75:12:e0' disassociated from Controller ...
Critical	Switch_Cisco_Ft_87:4b:90.1.3.15		7/21/06 4:32 PM	Controller '40.1.3.15'. RADIUS server(s) are no...
Critical	AP_AP0013.0493.cdf0/00:13:5f:57:a3:60		7/21/06 4:38 PM	Fake AP or other attack may be in progress. Rog...
Critical	AP_AP0013.0493.ba2r/00:13:5f:57:4d:40		7/21/06 5:31 PM	Fake AP or other attack may be in progress. Rog...
Critical	AP_AP142-8/00:14:1b:5a:16:d0		7/25/06 5:25 PM	Fake AP or other attack may be in progress. Rog...
Critical	Radio_AP-acc-c3750-48-1-FE1-0-3/2		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802....
Critical	Radio_AP-acc-c3750-48-1-FE1-0-3/1		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802....
Critical	AP_AP-acc-c3750-48-1-FE1-0-3/00:0b:85:52:a0:a0		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3' disassociated fr...

Regues	0	282
Coverage	0	0
Security	4	4
Controllers	0	0
Access Points	3	3
Location	0	0

4. A janela Alarme lista somente alarmes de segurança com gravidade menor. Aponte o mouse para o evento que disparou o bloco dentro do AIP-SSM. Em particular, o WCS mostra o endereço MAC da estação cliente que causou o alarme. Ao apontar para o endereço apropriado, o WCS abre uma pequena janela com os detalhes do evento. Clique no link para visualizar esses mesmos detalhes em outra janela.

The screenshot shows the Cisco Wireless Control System (WCS) interface with the 'Alarms' section filtered to show 'Minor' severity events under the 'Security' category. The main table lists four minor security events related to WEP keys and client associations. A tooltip is displayed over the fourth event, providing details about a client MAC address being associated with an AP.

Severity	Failure Object	Owner	Date/Time	Message
Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr...
Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr...
Minor	Client 00:90:7a:04:6d:04		7/31/06 2:36 PM	Client '00:90:7a:04:6d:04' which was associated...
Minor	Client 00:40:96:ad:0d:1b		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated...

Client '00:40:96:ad:0d:1b' which was associated with AP '00:14:1b:5a:16:40', interface '0' is excluded. The reason code is '%(Unknown)'.

Exemplo de configuração do 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#
```

Exemplo de configuração do sensor do sistema de prevenção de intrusão 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.

Troubleshoot

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

Informações Relacionadas

- [Instalando e usando o Cisco Intrusion Prevention System Device Manager 5.1](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances - Guias de configuração](#)
- [Configurando o sensor do Cisco Intrusion Prevention System usando a interface de linha de comando 5.0 - Configurando interfaces](#)
- [Guia de configuração da WLC 4.0](#)
- [Suporte técnico sem fio](#)
- [Perguntas frequentes sobre o Wireless LAN Controller \(WLC\)](#)
- [Exemplo de configuração básica dos controladores LAN sem fio e do access point lightweight](#)
- [Configurando soluções de segurança](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)