ワイヤレス LAN コントローラおよび IPS 統合ガイド

内容

概要

Cisco Unified 侵入検知システム（IDS）/侵入防御システム（IPS）は、Cisco Self-Defending Network の一部で、業界初の統合型有線および無線セキュリティ ソリューションです。Cisco Unified IDS/IPS は、無線、有線、WAN およびデータセンターを介した包括的なセキュリティを提供します。アソシエートされるクライアントが、Cisco Unified Wireless Network を介して悪意のあるトラフィックを送信すると、Cisco 有線 IDS デバイスは攻撃を検出し、回避要求を Cisco Wireless LAN Controller（WLC）に送信し、クライアント デバイスのアソシエーションを解除します。

Cisco IPS は、インラインのネットワークベースのソリューションで、ワーム、スパイウェア/アドウェア、ネットワーク ウイルスおよびアプリケーションの悪用など、悪意のあるトラフィック

がビジネスの継続性に影響を与える前に、これらを正確に特定、分類、停止します。

Cisco IPS Sensor ソフトウェア バージョン 5 を使用することで、Cisco IPS ソリューションは、インライン防止サービスと革新的なテクノロジーを組み合わせることで精度を改善します。その結果、IPS ソリューションによって提供される保護に絶対の信頼を寄せることができるため、正規のトラフィックがドロップされることを心配する必要はありません。Cisco IPS ソリューションは、他のネットワーク セキュリティ リソースと協力する独自機能により、ネットワークを包括的かつ予防的に保護します。

Cisco IPS ソリューションでは、ユーザは、次の機能を使用することで、さらに正確に多くの脅威を停止できます。

- **精度の高いインライン防御テクノロジー**：正規のトラフィックをドロップすることなく、多様な脅威に対する防御策を確実に講じることができます。これらの独自のテクノロジーにより、データのインテリジェントな自動コンテキスト分析が提供されるので、侵入防御ソリューションを最大限利用できます。
- **マルチベクトル脅威特定**：レイヤ 2 ~ 7 のトラフィックを綿密に検査することで、ポリシー違反、脆弱性不正利用および異常なアクティビティからネットワークを保護します。
- **一意なネットワーク コラボレーション**：効率的なトラフィック キャプチャ テクノロジー、ロードバランシング機能および暗号化トラフィックの把握など、ネットワーク コラボレーションを介して優れた拡張性と復元力を提供します。
- **包括的な導入ソリューション**：小中規模ビジネス（SMB）やブランチ オフィス ロケーションから大規模な企業やサービス プロバイダー インストールまで、すべての環境に適したソリューションを提供します。
- **強力な管理、イベント相関関係およびサポート サービス**：構成、管理、データ相関関係および高度なサポート サービスなど、完全なソリューションを可能にします。特に、Cisco Security Monitoring, Analysis, and Response System（MARS）は、ネットワーク規模の侵入防御ソリューションのために、攻撃要素を特定および隔離し、精密な除去を推奨します。また、Cisco Incident Control System は、ネットワークの迅速な順応性を実現にすることで、新しいワームおよびウイルスの発生を防ぎ、分散応答を提供します。

これらの要素を組み合わせることで、包括的なインライン防御ソリューションが提供され、悪意のあるさまざまなトラフィックがビジネスの継続性に影響を与える前に、これらを確実に検知および停止できます。Cisco Self-Defending Network は、ネットワーク ソリューションの統合型ビルトイン セキュリティを提供します。現在の Lightweight Access Point Protocol（LWAPP）ベース WLAN システムは、実質的にレイヤ 2 システムであり、回線処理能力が制限されるため、基本的な IDS 機能しかサポートできません。Cisco は、新しい拡張機能を含めた新しいコードをタイムリーに提供します。リリース 4.0 は、LWAPP ベース WLAN システムと Cisco IDS/IPS 製品ラインを統合する最新機能を提供します。このリリースでは、レイヤ 3 ~ 7 で攻撃が検出された場合にクライアントに配慮して、Cisco IDS/IPS システムが特定のクライアントによるワイヤレス ネットワークへのアクセスをブロックするよう WLC に指示できます。

前提条件

要件

次の最小要件を満たすことを確認してください。

- WLC ファームウェア バージョン 4.x 以降
- Cisco IPS の設定方法に関する知識（Cisco WLC 推奨）

使用するコンポーネント

Cisco WLC

IDS 変更のためにソフトウェア リリース 4.0 には、次のコントローラが含まれます。

- Cisco 2000 シリーズ WLC
- Cisco 2100 シリーズ WLC
- Cisco 4400 シリーズ WLC
- Cisco Wireless Services Module（WiSM）
- Cisco Catalyst 3750G Series Unified Access Switch
- Cisco Wireless LAN Controller モジュール（WLCM）

アクセス ポイント

- Cisco Aironet 1100 AG シリーズ Lightweight アクセス ポイント
- Cisco Aironet 1200 AG シリーズ Lightweight アクセス ポイント
- Cisco Aironet 1300 シリーズ Lightweight アクセス ポイント
- Cisco Aironet 1000 シリーズ Lightweight アクセス ポイント

管理

- Cisco Wireless Control System（WCS）
- Cisco 4200 シリーズ センサー
- Cisco IDS Management：Cisco IDS Device Manager（IDM）

Cisco Unified IDS/IPS プラットフォーム

- Cisco IPS 4200 シリーズ センサー（Cisco IPS Sensor ソフトウェア 5.x 以降）
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの SSM10 および SSM20（Cisco IPS Sensor ソフトウェア 5.x）
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（Cisco IPS Sensor ソフトウェア 5.x）
- Cisco IDS Network Module（NM-CIDS）（Cisco IPS Sensor ソフトウェア 5.x）
- Cisco Catalyst 6500 シリーズ侵入防御システム モジュール 2（IDSM-2）（Cisco IPS Sensor ソフトウェア 5.x）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

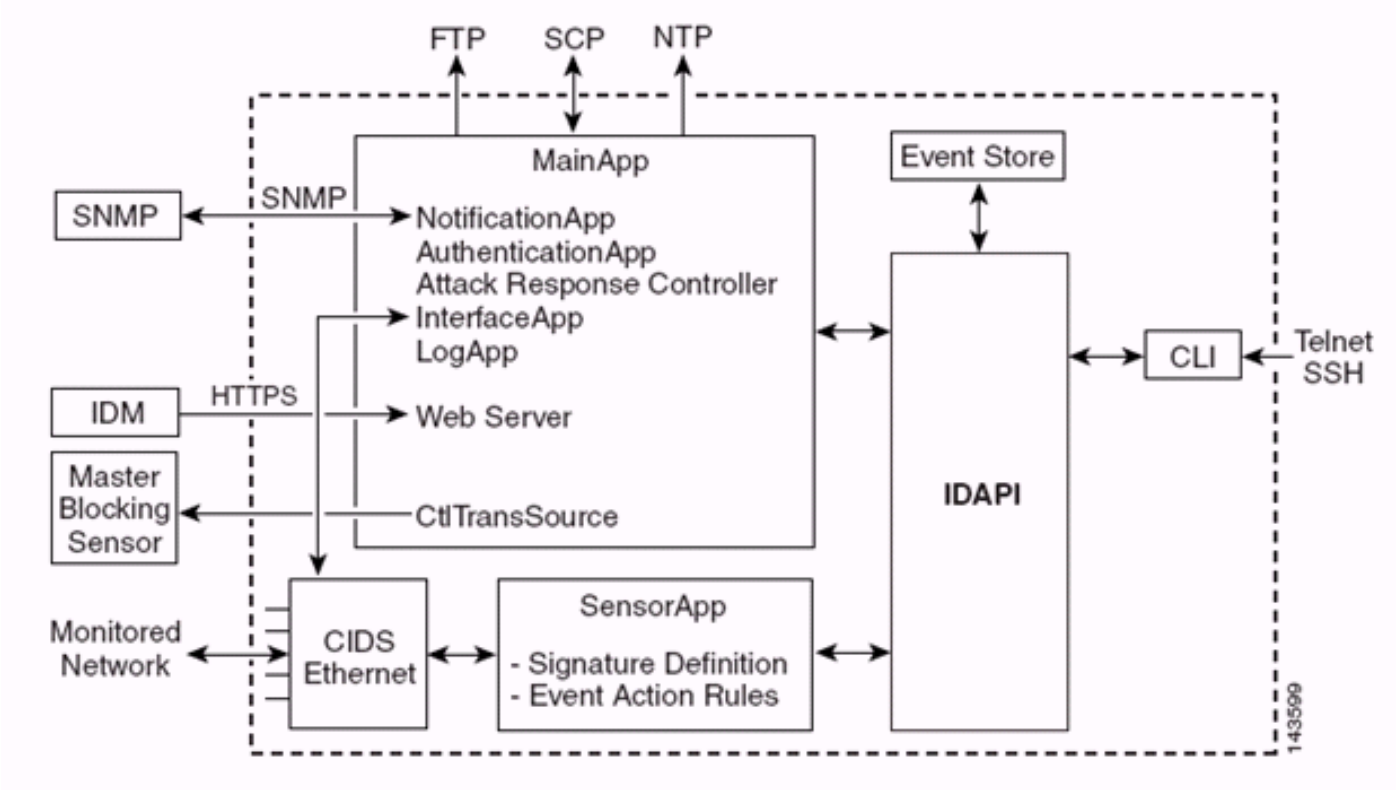
Cisco IDS の概要

次に、Cisco IDS（バージョン 5.0）の主なコンポーネントを示します。

- **Sensor App**：パケットの取り込みと分析を実行します。
- **イベント ストレージ管理およびアクション モジュール**：ポリシー違反のストレージを提供し

ます。

- **イメージング、インストールおよびスタートアップ モジュール**：システム ソフトウェアをロード、初期化および開始します。
- **ユーザ インターフェイスおよび UI サポート モジュール**：組み込み CLI および IDM を提供します。
- **Sensor OS**：ホスト オペレーティング システム（Linux ベース）。



次に、センサー アプリケーション（IPS ソフトウェア）の構成要素を示します。

- **Main App**：システムを初期化、他のアプリケーションを起動および停止、OS を設定し、アップグレードを行います。次に、この構成要素を示します。**Control Transaction Server**：Attack Response Controller（以前の Network Access Controller）Master Blocking Sensor 機能を可能にするために使用される制御トランザクションをセンサーから送信できるようにします。**Event Store**：IPS イベント（エラー、ステータスおよびアラート システム メッセージ）の保存に使用されるインデックス付きストアです。CLI、IDM、Adaptive Security Device Manager（ASDM）または Remote Data Exchange Protocol（RDEP）からアクセスできます。
- **Interface App**：バイパスおよび物理設定を処理し、ペアにするインターフェイスを定義します。物理設定は、速度、デュプレックスおよび管理状態で構成されます。
- **Log App**：アプリケーションのログ メッセージをログ ファイルに書き込み、エラー メッセージを Event Store に書き込みます。
- **Attack Response Controller（ARC）（以前の Network Access Controller）**：リモート ネットワーク デバイス（ファイアウォール、ルータ、スイッチ）を管理し、アラート イベントの発生時にブロッキング機能を提供します。ARC は、アクセス コントロール リスト（ACL）を作成して制御対象ネットワーク デバイスに適用するか、または、**shun** コマンド（ファイアウォール）を使用します。
- **Notification App**：アラート、ステータスおよびエラー イベントによりトリガーされたときに SNMP トラップを送信します。Notification App は、このためにパブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的な状態に関する情報を提供し

ます。**Web サーバ（HTTP RDEP2 サーバ）**：Web ユーザ インターフェイスを提供します。また、いくつかのサーブレットを使用する RDEP2 を経由して他の IPS デバイスと通信し、IPS サービスを提供します。**Authentication App**：ユーザに CLI、IDM、ASDM または RDEP アクションの実行が許可されているか確認します。
- **Sensor App（分析エンジン）**：パケットのキャプチャと分析を行います。
- **CLI**：Telnet または SSH を通じてセンサーに正しくログインすると実行されるインターフェイスです。CLI を通じて作成されるすべてのアカウントは、シェルとして CLI を使用します（サービス アカウントは例外で、許可されるサービス アカウント 1 つだけです）。 使用できる CLI コマンドは、ユーザの権限により異なります。

すべての IPS は、IDAPI という共通のアプリケーション プログラム インターフェイス（API）を介して相互に通信します。リモート アプリケーション（その他のセンサー、管理アプリケーションおよびサードパーティ ソフトウェア）は、RDEP2 および Security Device Event Exchange（SDEE）プロトコルを介してセンサーと通信します。

センサーには、次のディスク パーティションがあります。

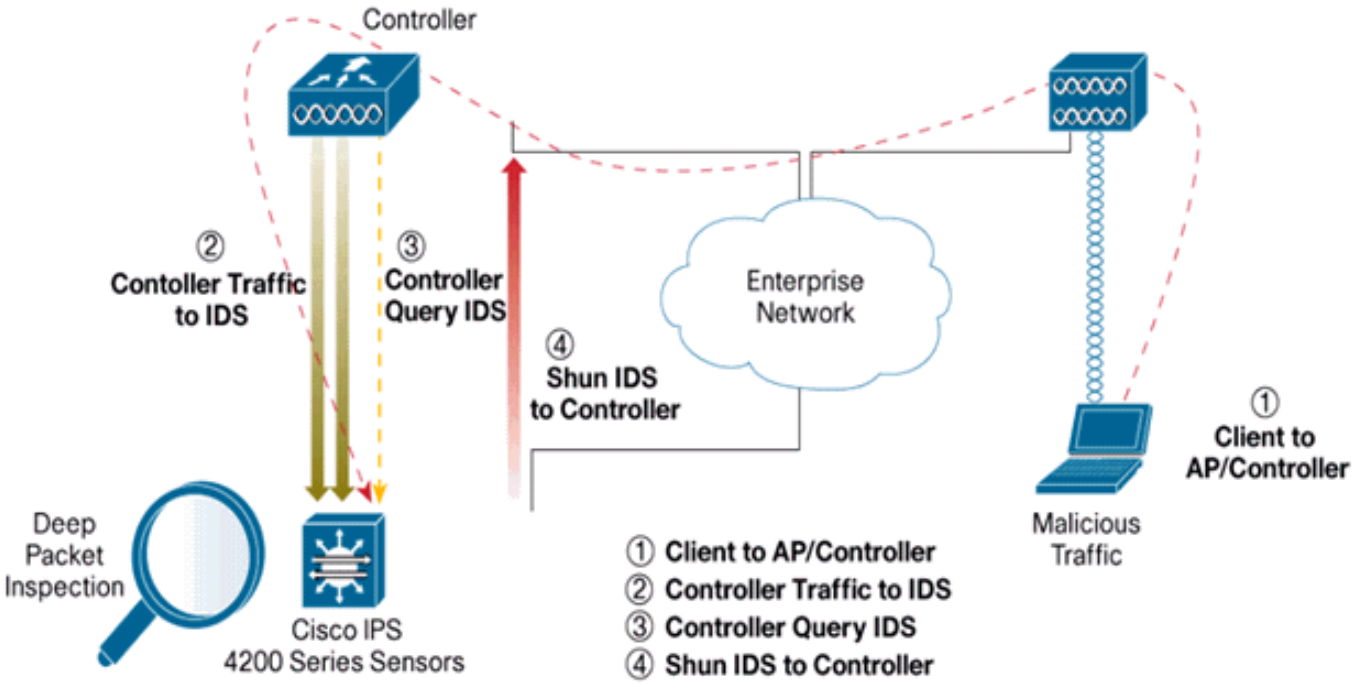
- **アプリケーション パーティション**：完全な IPS システム イメージを含みます。
- **メンテナンスパーティション**:IDSM-2のアプリケーションパーティションの再イメージ化に使用される特殊な目的のIPSイメージ。メンテナンスパーティションの再イメージ化により、設定が失われます。
- **リカバリ パーティション**：センサーのリカバリに使用される、特殊な目的のイメージ。リカバリ パーティションにブートすると、アプリケーション パーティションのイメージを完全に再作成できます。ネットワーク設定は保存されますが、それ以外のすべての設定は失われます。

Cisco IDS と WLC：統合の概要

Cisco IDS バージョン 5.0 では、ポリシー違反（シグニチャ）が検出されたときに拒否アクションを設定できます。IDS/IPS システムでのユーザ設定に基づいて、回避要求をファイアウォール、ルータまたは WLC に送信して、特定の IP アドレスから送られるパケットをブロックできます。

Cisco ワイヤレス コントローラの Cisco Unified Wireless Network ソフトウェア リリース 4.0 では、コントローラで使用できるクライアント ブラックリスト登録または除外動作をトリガーするには、回避要求を WLC に送信する必要があります。コントローラが回避要求の取得に使用するインターフェイスは、Cisco IDS のコマンドおよび制御インターフェイスです。

- コントローラでは、最大 5 つの IDS センサーを設定できます。
- 設定された各 IDS センサーは、その IP アドレスまたは修飾ネットワーク名および認可クレデンシャルにより識別されます。
- 各 IDS センサーは、秒単位での一意なクエリー レートを使用してコントローラに設定できます。



IDS 回避

コントローラは、設定されているクエリー レートでセンサーをクエリーし、すべての回避イベントを取得します。回避要求は、IDS センサーから要求を受け取るコントローラのモビリティ グループ全体で分散されます。クライアント IP アドレスの各回避要求は、秒単位で指定されたタイムアウト値の間、有効です。タイムアウト値が無限の期間を示す場合、回避イベントは、回避エントリが IDS で削除されるまで終了しません。回避クライアント ステータスは、いずれか、またはすべてのコントローラがリセットされた場合でも、モビリティ グループの各コントローラで維持されます。

注：クライアントを排除する決定は、常にIDSセンサーによって行われます。コントローラはレイヤ 3 攻撃を検出しません。クライアントがレイヤ3で悪意のある攻撃を開始していると判断するのは、はるかに複雑なプロセスです。クライアントはレイヤ2で認証され、コントローラがレイヤ2アクセスを許可するのに十分です。

注：例えば、クライアントに以前の問題の（シャントされた）IPアドレスが割り当てられている場合、この新しいクライアントのレイヤ2アクセスのブロックを解除するには、センサーのタイムアウトが発生します。コントローラがレイヤ 2 でのアクセスを提供する場合でも、クライアントトラフィックは、レイヤ 3 のルータでブロックされることがあります。これは、センサーが、ルータに回避イベントを通知するためです。

クライアントにIPアドレスAがあると仮定します。ここで、コントローラがIDSをポーリングして回避イベントを検出すると、IDSはターゲットIPアドレスとしてIPアドレスAを持つ回避要求をコントローラに送信します。これで、コントローラの黒いリストにこのクライアントAが表示されます。コントローラでは、クライアントはMACアドレスに基づいて無効になります。

ここで、クライアントのIPアドレスがAからBに変更されたと仮定します。次のポーリングの間、コントローラはIPアドレスに基づいて回避されたクライアントのリストを取得します。この場合も、IP アドレス A はまだ回避リストに登録されています。ただし、クライアントはその IP アドレスを A から B（IP アドレスの回避リストに登録されていない）に変更しているため、ブラックリストに登録されているクライアントがタイムアウトになると、新しい IP アドレス B を使用するこのクライアントは解放されます。コントローラは、新しい IP アドレス B（ただし、同じクラ

イアント MAC アドレス）を使用するクライアントを許可します。

そのため、クライアントがコントローラの除外期間で無効になり、以前の DHCP アドレスを再取得すると再び除外されますが、このクライアントは、回避クライアントの IP アドレスが変更されると、無効ではなくなります。たとえば、クライアントが同じネットワークに接続した場合、DHCP リース タイムアウトは失効しません。

コントローラは、コントローラの管理ポートを使用するクライアント回避要求の IDS への接続だけをサポートします。コントローラは、ワイヤレス クライアント トラフィックを送信する適切な VLAN インターフェイスを介して、IDS に接続しパケットを検査します。

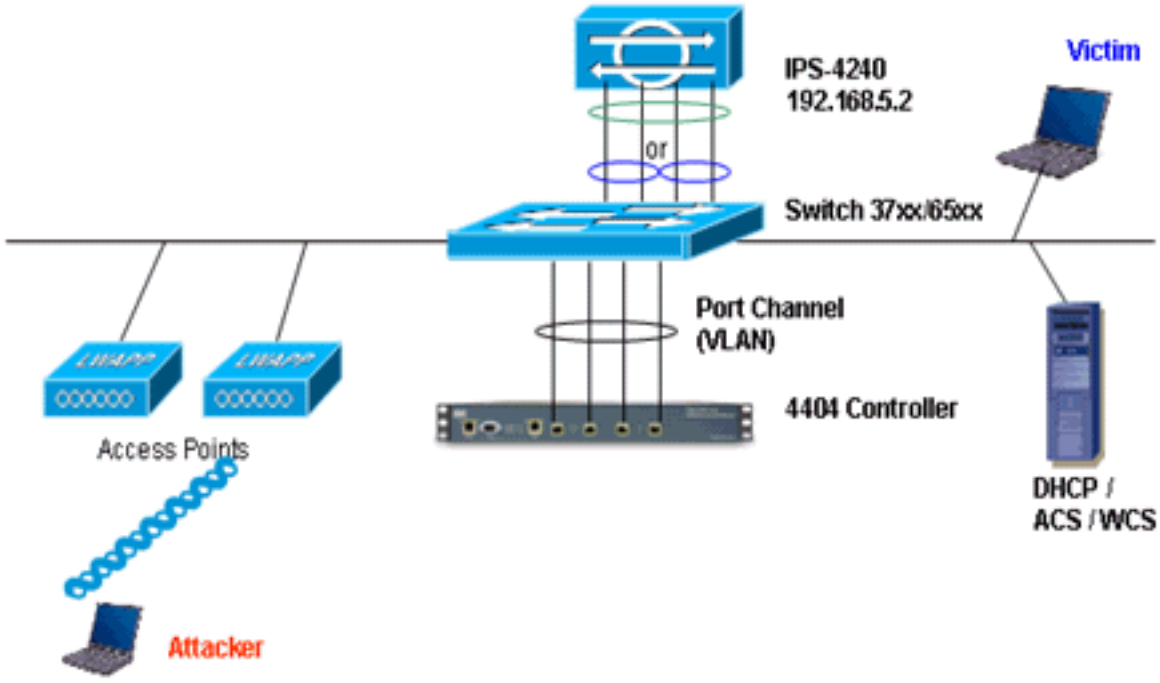
コントローラでは、[Disable Clients] ページに、IDS センサー要求を介して無効にされた各クライアントが表示されます。CLI **show** コマンドを使用し、ブラックリストに登録されているクライアントのリストを表示することできます。

WCS では、除外クライアントは、[Security] サブタブに表示されます。

次に、Cisco IPS センサーと Cisco WLC を統合する手順を示します。

1. ワイヤレス コントローラが常駐するスイッチに IDS アプライアンスをインストールして接続します。
2. ワイヤレス クライアント トラフィックを IDS アプライアンスに送信する WLC ポートをミラー化（SPAN）します。
3. IDS アプライアンスは、すべてのパケットのコピーを取得して、レイヤ 3 ~ 7 でトラフィックを検査します。
4. IDS アプライアンスは、ダウンロード可能なシグニチャ ファイルを提供します。これは、カスタマイズできます。
5. IDS アプライアンスは、攻撃シグニチャが検出されると、回避のイベント アクションでアラームを生成します。
6. WLC は、IDS をポーリングしてアラームを生成します。
7. WLC にアソシエートされるワイヤレス クライアントの IP アドレスでアラームが検出されると、クライアントは除外リストに追加されます。
8. トラップが WLC で生成され、WCS に通知されます。
9. ユーザは、指定期間が経過すると、除外リストから削除されます。

ネットワーク アーキテクチャ設計



Cisco WLC は、Catalyst 6500 のギガビット インターフェイスに接続されます。ギガビット インターフェイスのポート チャネルを作成し、WLC のリンク集約（LAG）を有効にします。

```
(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
```

コントローラは、Catalyst 6500 のインターフェイス ギガビット 5/1 およびギガビット 5/2 に接続されます。

```
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
```

IPS センサーのセンシング インターフェイスは、無差別モードで個別に稼働したり、これらをペアにしてインライン インターフェイス モードのインライン インターフェイスを作成したりできます。

無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されるパケットではなく、モニタ対象のトラフィックのコピーを分析します。無差別モードで運用する利点は、転送されるトラフィックでパケットのフローにセンサーが影響を与えないことです。

注：アーキテクチャダイアグラムは、WLCとIPS統合アーキテクチャの設定例にすぎません。この設定例は、無差別モードで稼働する IDS センシング インターフェイスについて説明します。次の構造図では、インライン ペア モードで稼働するためにペアにされたセンシング インターフェイスを示します。インライン インターフェイス モードの詳細については、『インライン モード』を参照してください。

この設定では、センシング インターフェイスは無差別モードで稼働しています。Cisco IDS センサーのモニタリング インターフェイスは、Catalyst 6500 のギガビット インターフェイス 5/3 に接続されます。Catalyst 6500 のモニタ セッションを作成します。このセッションでは、ポートチャネル インターフェイスをパケットの送信元として、Cisco IPS センサーのモニタリング インターフェイスが接続されるギガビット インターフェイスを宛先とします。これは、レイヤ 3 ~ 7 の検査のために、コントローラ接続インターフェイスから IDS へのすべての入出力トラフィックを複製します。

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3

cat6506#show monitor session 5
Session 5
---------
Type                   : Local Session
Source Ports           :
    Both               : Po99
Destination Ports      : Gi5/3
cat6506#
```

Cisco IDS センサーの設定

Cisco IDS センサーの初期設定は、コンソール ポートから実行するか、モニタおよびキーボードをセンサーに接続して実行します。

1. アプライアンスにログインします。コンソール ポートをセンサーに接続します。モニタおよびキーボードをセンサーに接続します。
2. ログイン プロンプトに対してユーザ名とパスワードを入力します。**注：デフォルト**のユーザ名とパスワードは両方ともciscoです。初めてアプライアンスにログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード (cisco) を入力してください。次に、新しいパスワードを 2 回入力します。

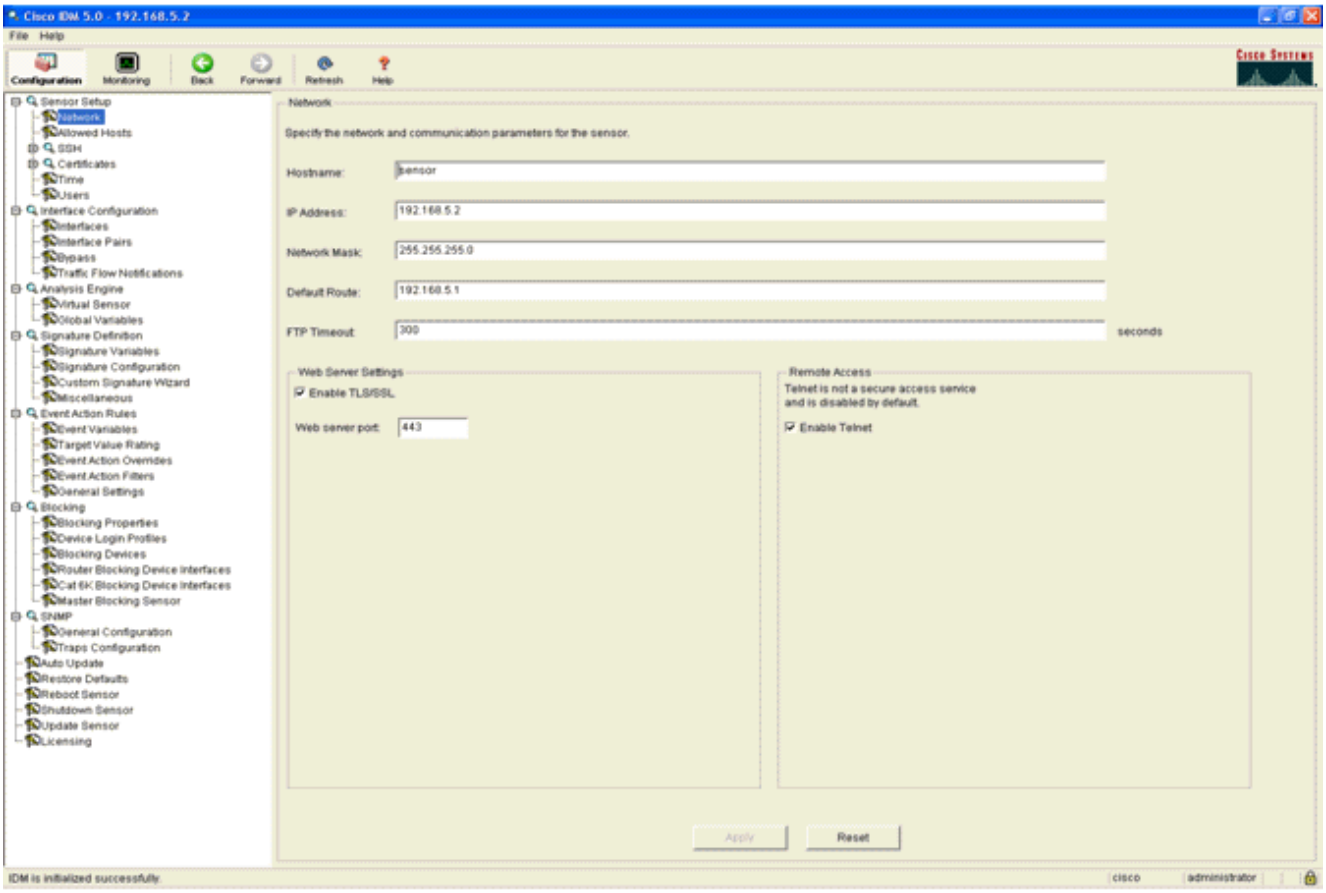
```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute or
use encryption. 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. センサーの IP アドレス、サブネット マスクおよびアクセス リストを設定します。**注：これ**は、コントローラとの通信に使用されるIDSのコマンドおよび制御インターフェイスです。このアドレスは、コントローラ管理インターフェイスにルーティングされます。センシング インターフェイスでは、アドレッシングは不要です。アクセス リストには、コントローラ管理インターフェイス アドレスおよび IDS 管理のための可能なアドレスが含まれます。

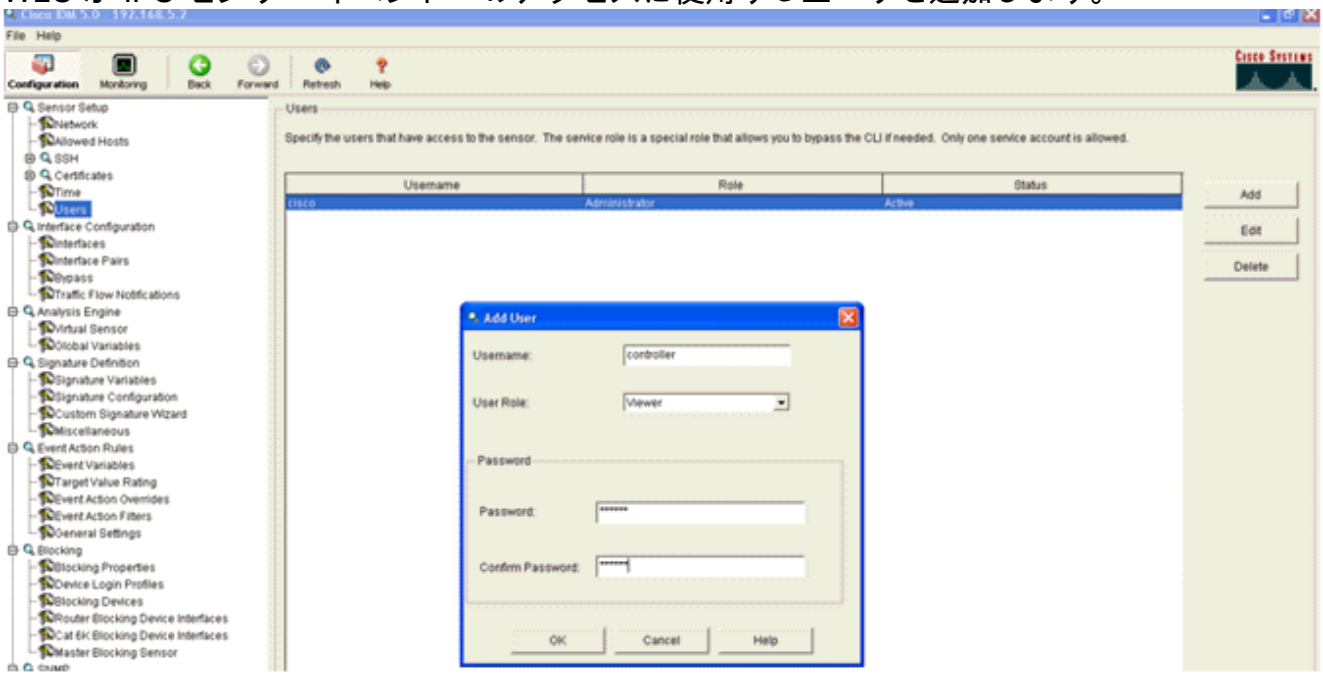
```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit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

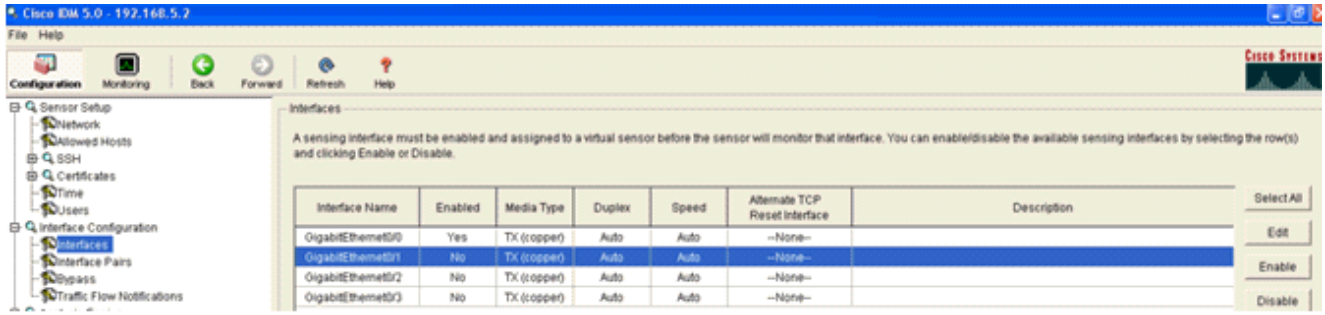
4. IPS センサーは GUI から設定できます。ブラウザを使用して、センサーの管理 IP アドレスを示します。次の例では、センサーは 192.168.5.2 で設定されます。



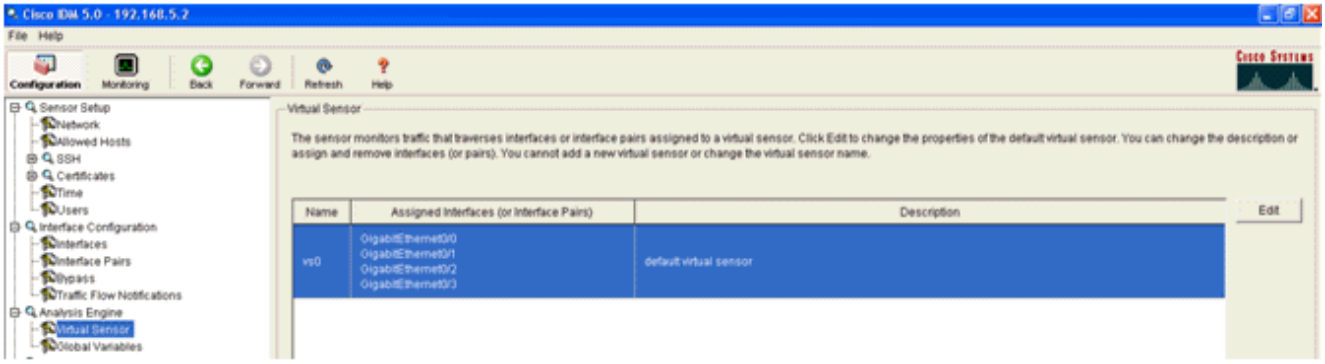
5. WLC が IPS センサー イベントへのアクセスに使用するユーザを追加します。



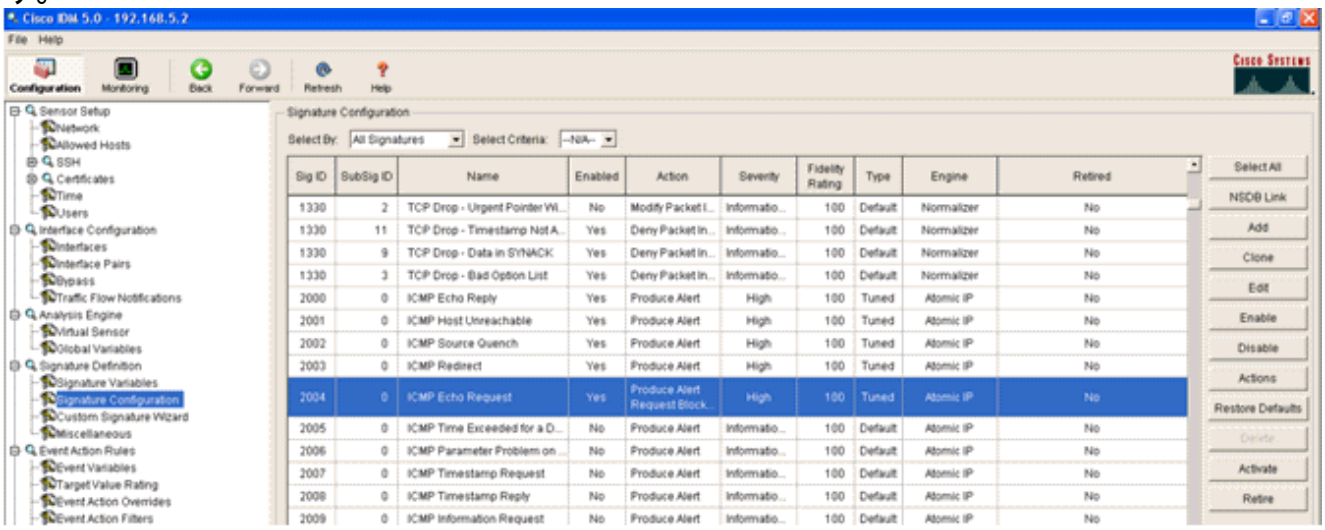
6. モニタリング インターフェイスを有効にします。



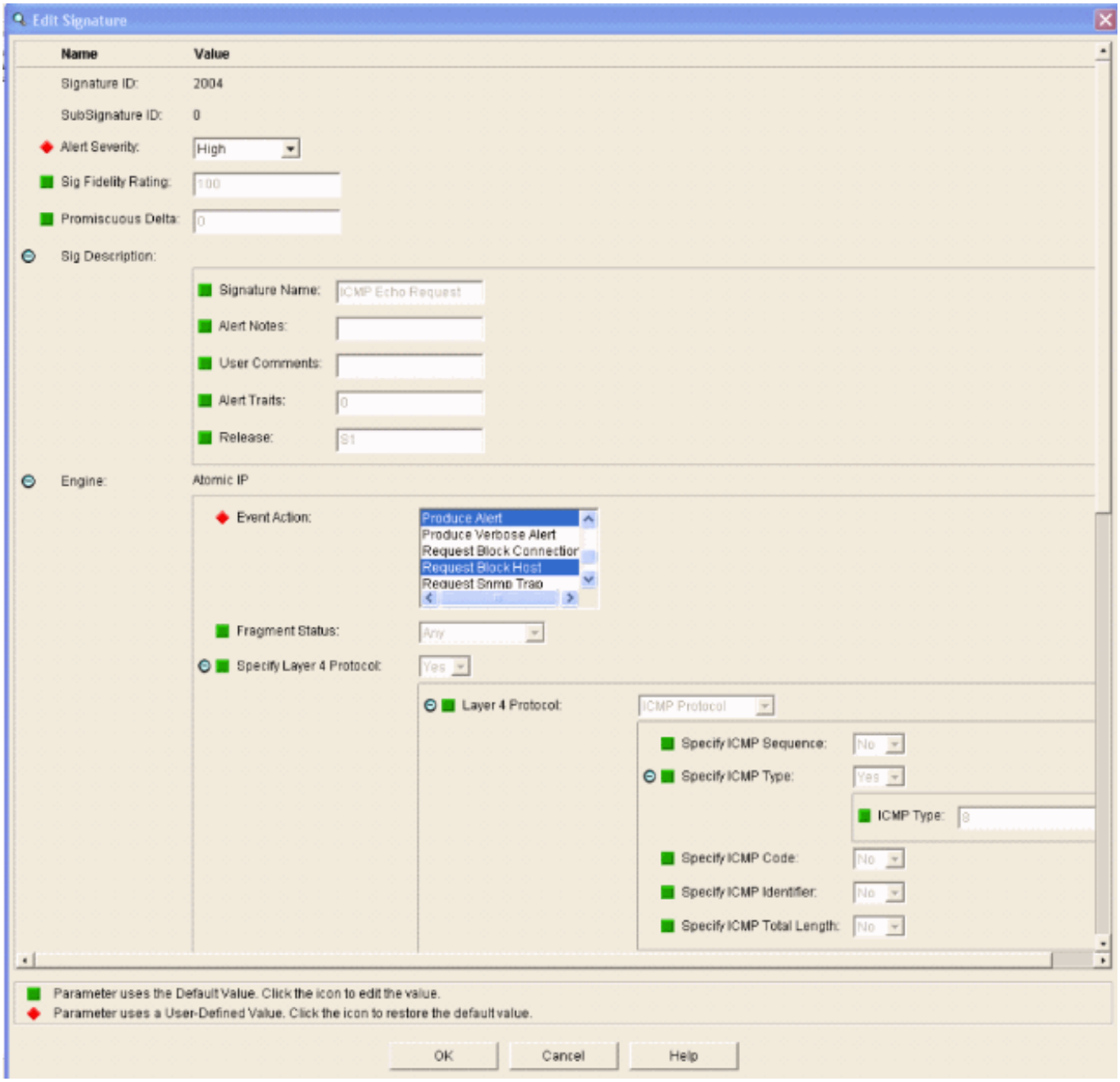
モニタリング インターフェイスは、次の例に示すように、分析エンジンに追加する必要があります。



7. クイック設定検査を実行するために 2004 シグニチャ（[ICMP Echo Request]）を選択します。



シグニチャを有効にし、[Alert Severity] を [High] に設定し、[Event Action] を [Produce Alert] および [Request Block Host] に設定し、検証手順を完了します。

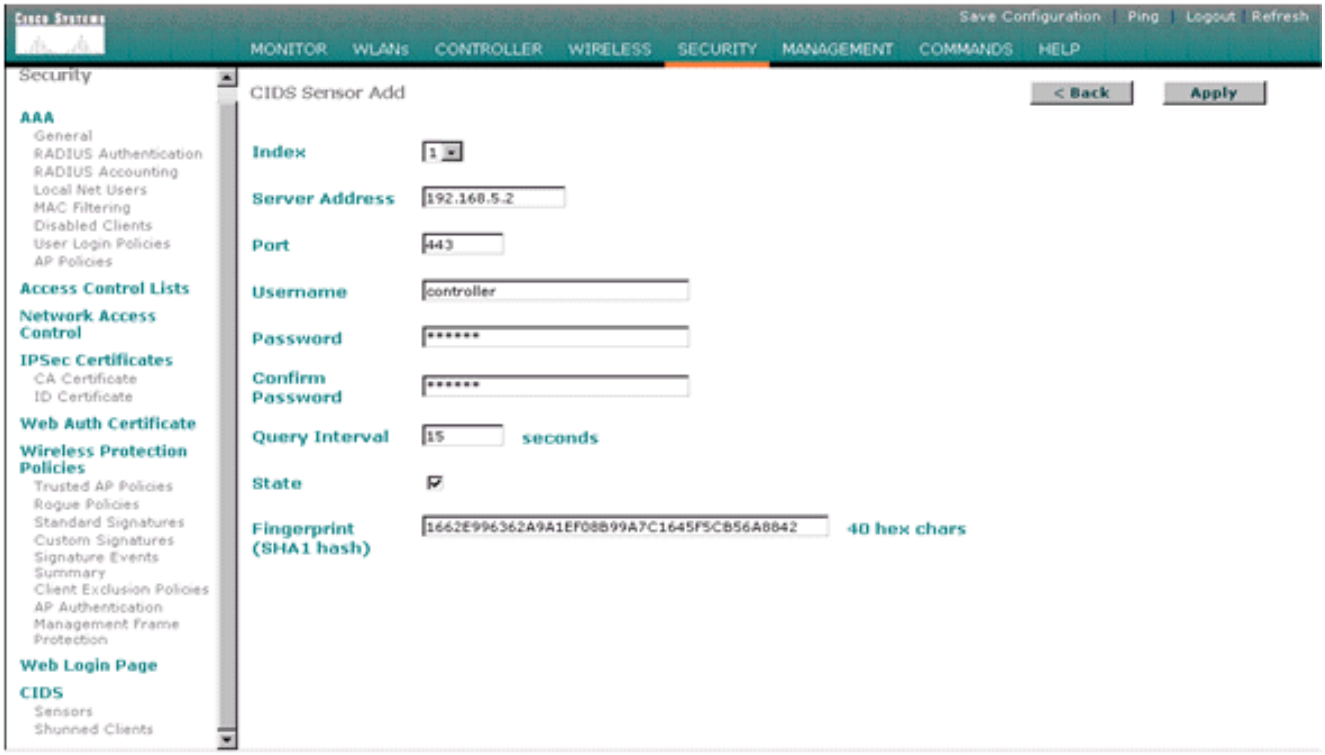


WLC の設定

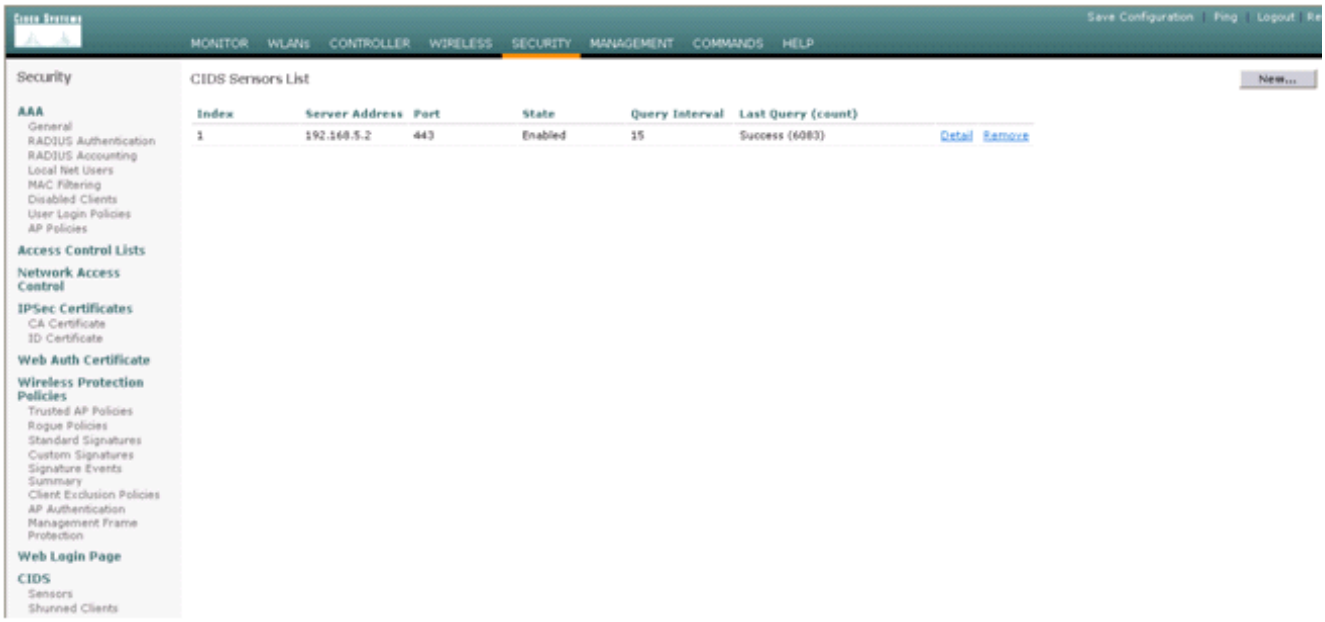
WLC を設定するには、次の手順を実行します。

1. IPS アプライアンスを設定し、コントローラに追加できるようになったら、[Security] > [CIDS] > [Sensors] > [New] を選択します。
2. 以前作成した IP アドレス、TCP ポート番号、ユーザ名およびパスワードを追加します。IPS センサーからフィンガープリントを取得するには、IPS センサーで次のコマンドを実行して、SHA1 フィンガープリントを WLC に追加します（コロンは使用しません）。 これはコントローラと IDS のポーリング通信のセキュリティを確保するために使用します。

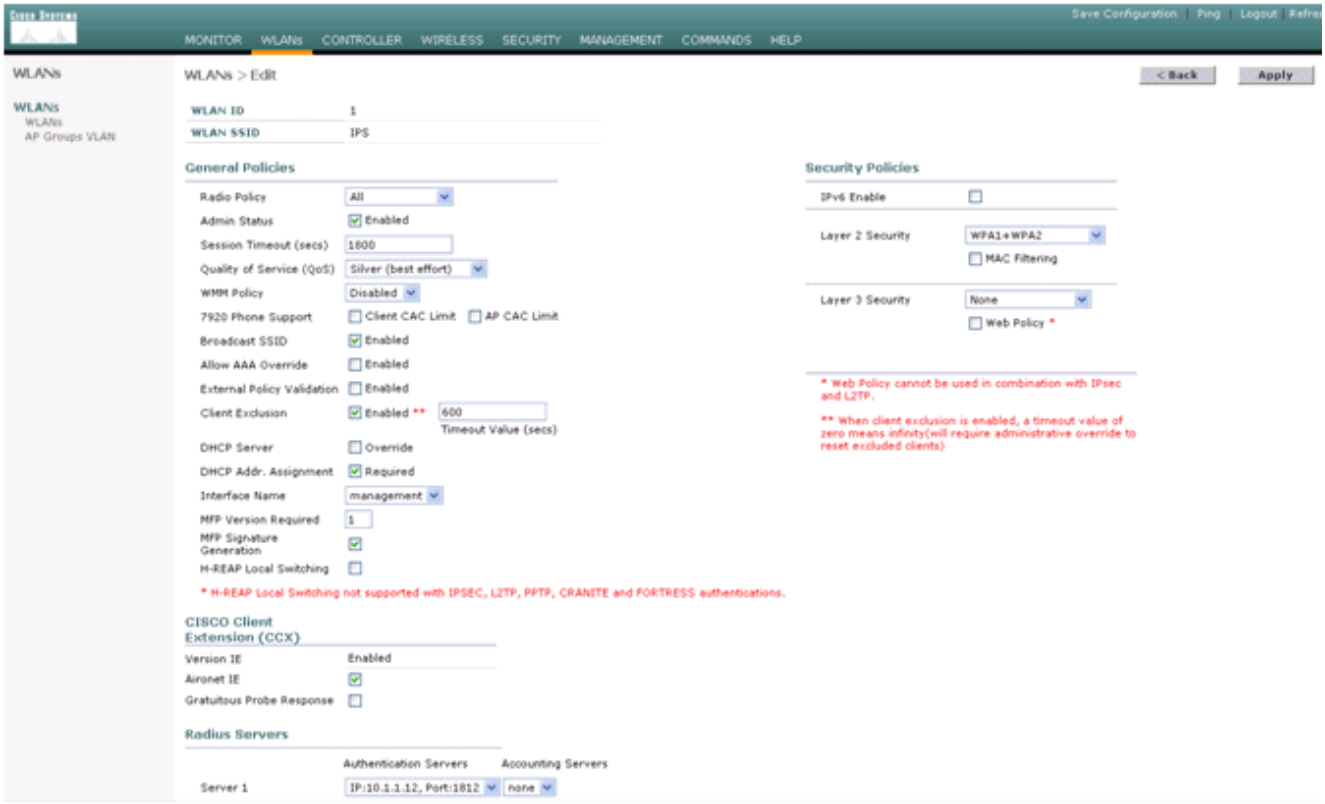
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



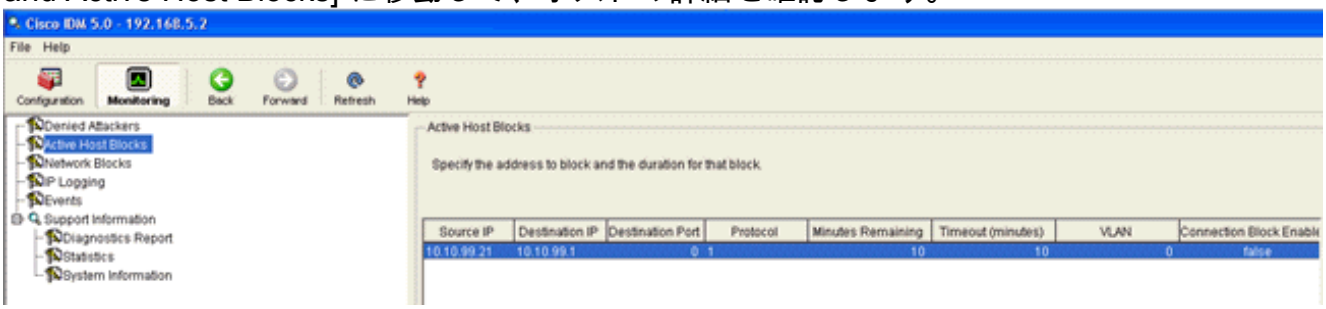
3. IPS センサーと WLC 間の接続のステータスを確認します。



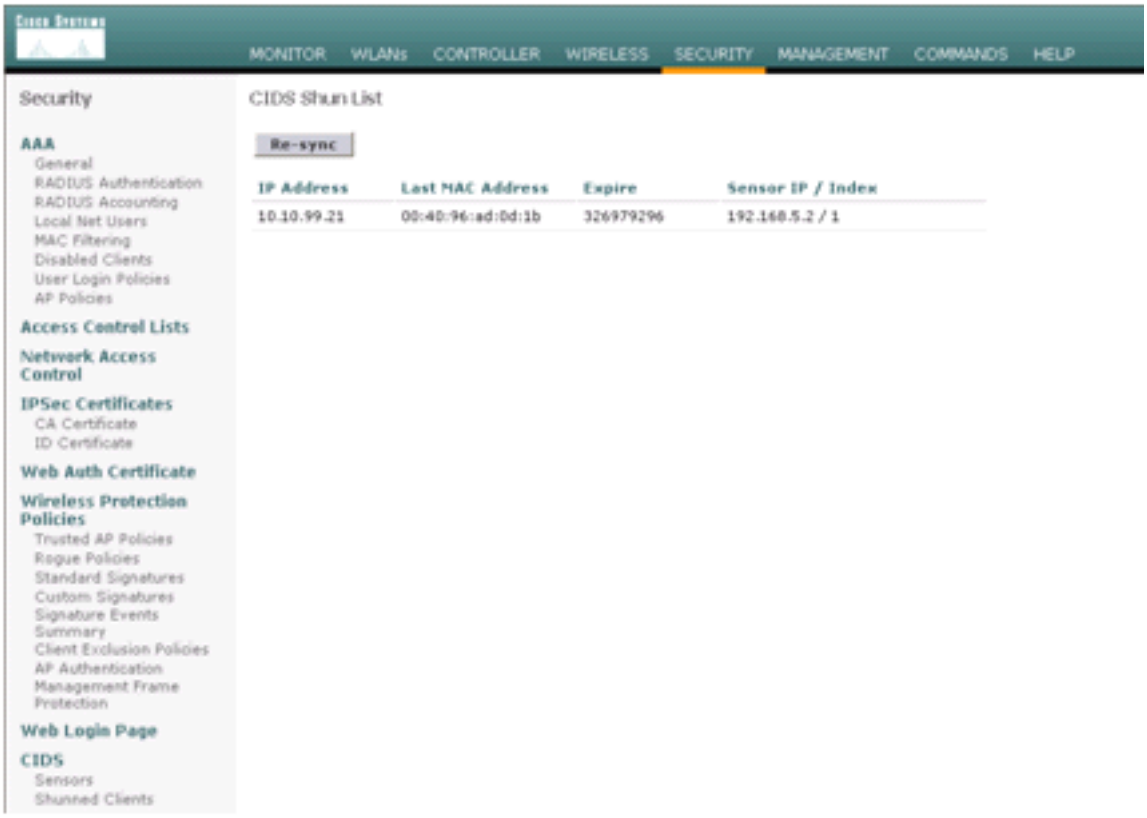
4. Cisco IPS センサーとの接続を確立したら、WLAN 設定が正しいか確認し、[Client Exclusion] を有効にします。デフォルトのクライアント除外タイムアウト値は 60 秒です。また、クライアントの除外タイマーに関係なく、IDS により呼び出されるクライアント ブロックがアクティブである限り、クライアント除外は維持されるので注意してください。IDS のデフォルトのブロック時間は 30 分です。



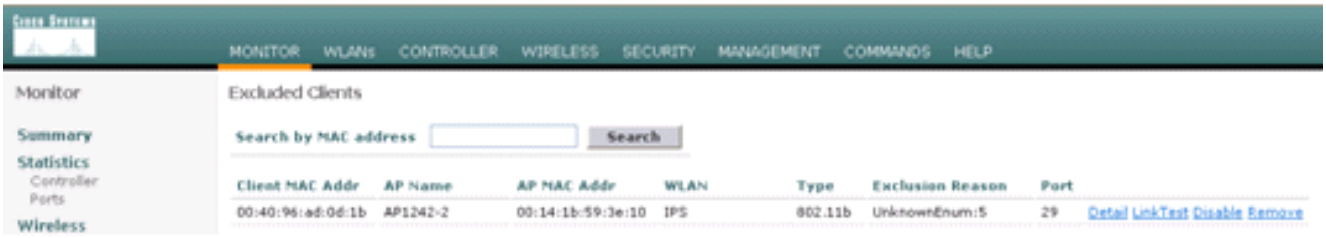
5. ネットワークの特定のデバイスに対して NMAP スキャンを実行するとき、または Cisco IPS センサーによりモニタされるいくつかのホストに ping を実行するときに、Cisco IPS システムのイベントをトリガーできます。Cisco IPS でアラームがトリガーされたら、[Monitoring and Active Host Blocks] に移動して、ホストの詳細を確認します。



コントローラの [Shunned Clients] リストは、ホストの IP および MAC アドレスが表示され

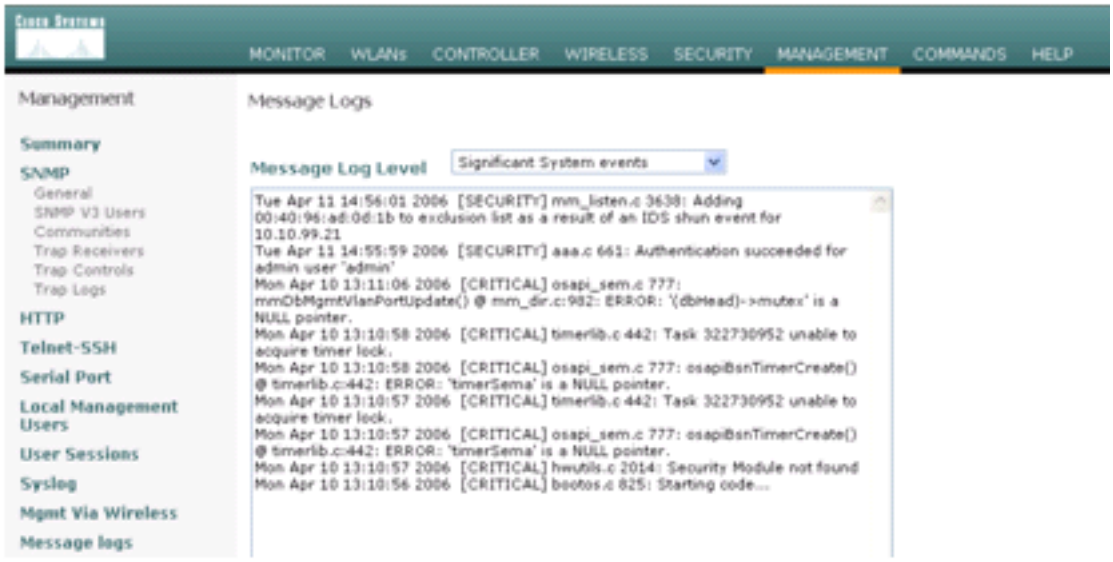


ます。ユーザはクライアント除外リストに追加されます。

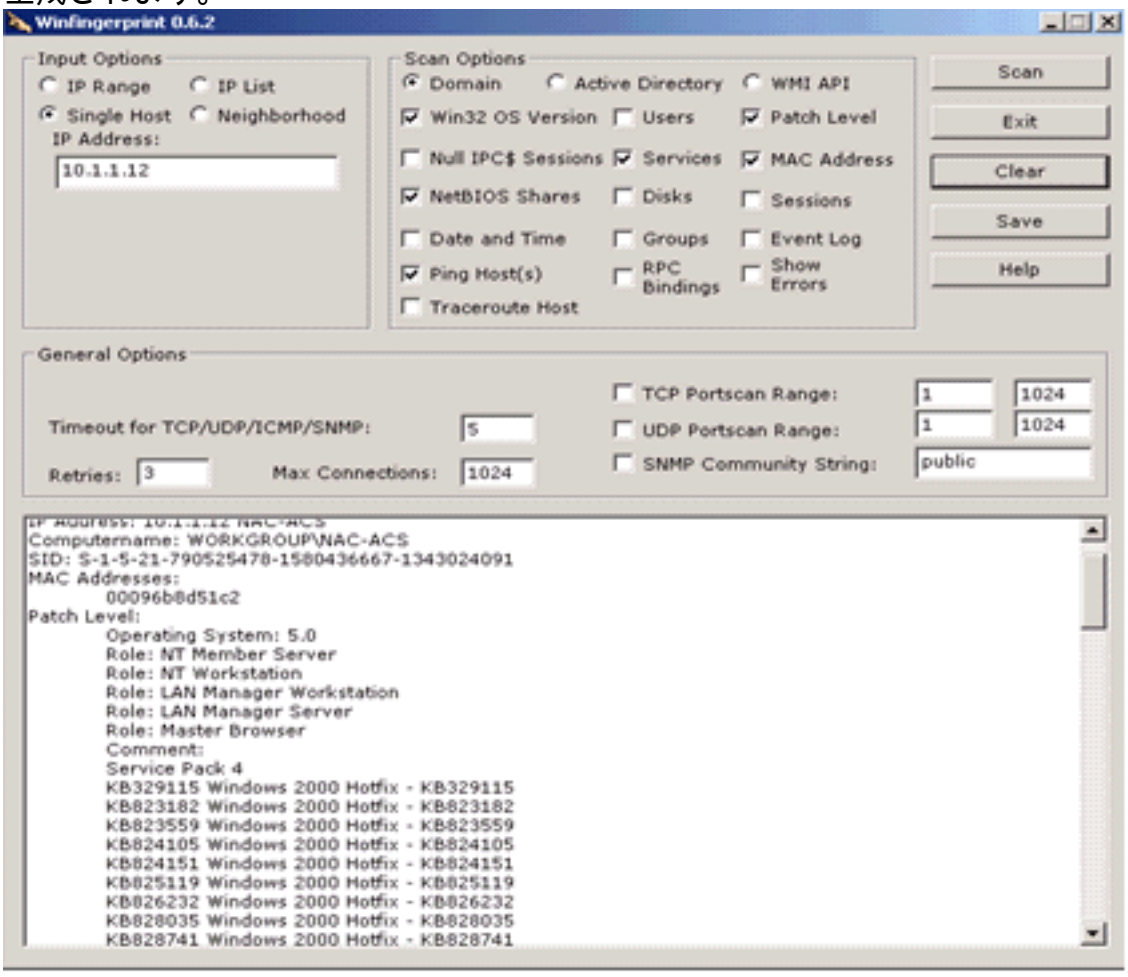


クライアントが回避リストに追加されると、トラップ ログが生成されます。

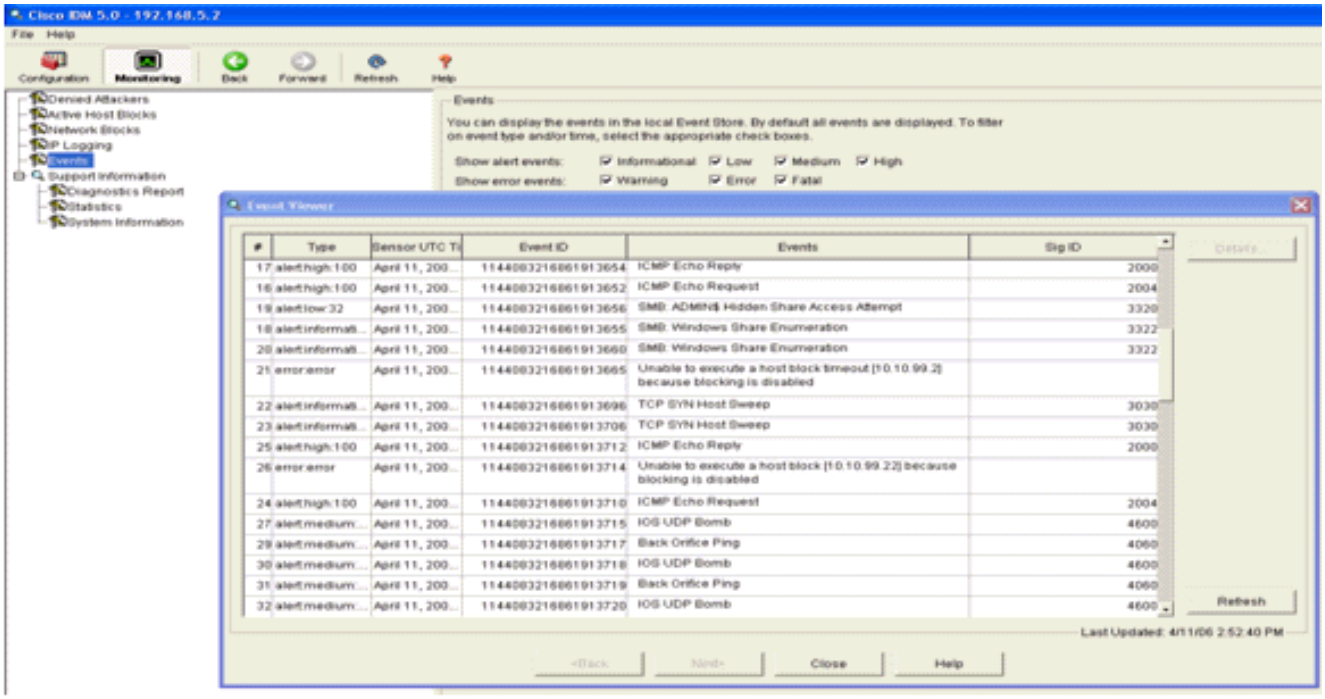
イベントのメッセージ ログも生成されます。



モニタするデバイスで NMAP スキャンが実行されると、Cisco IPS センサーでいくつかの追加イベントが生成されます。



次の例では、Cisco IPS センサーで生成されたイベントを示します。



Cisco IDS センサーの設定例

次に、インストールからのセットアップ スクリプトの出力例を示します。

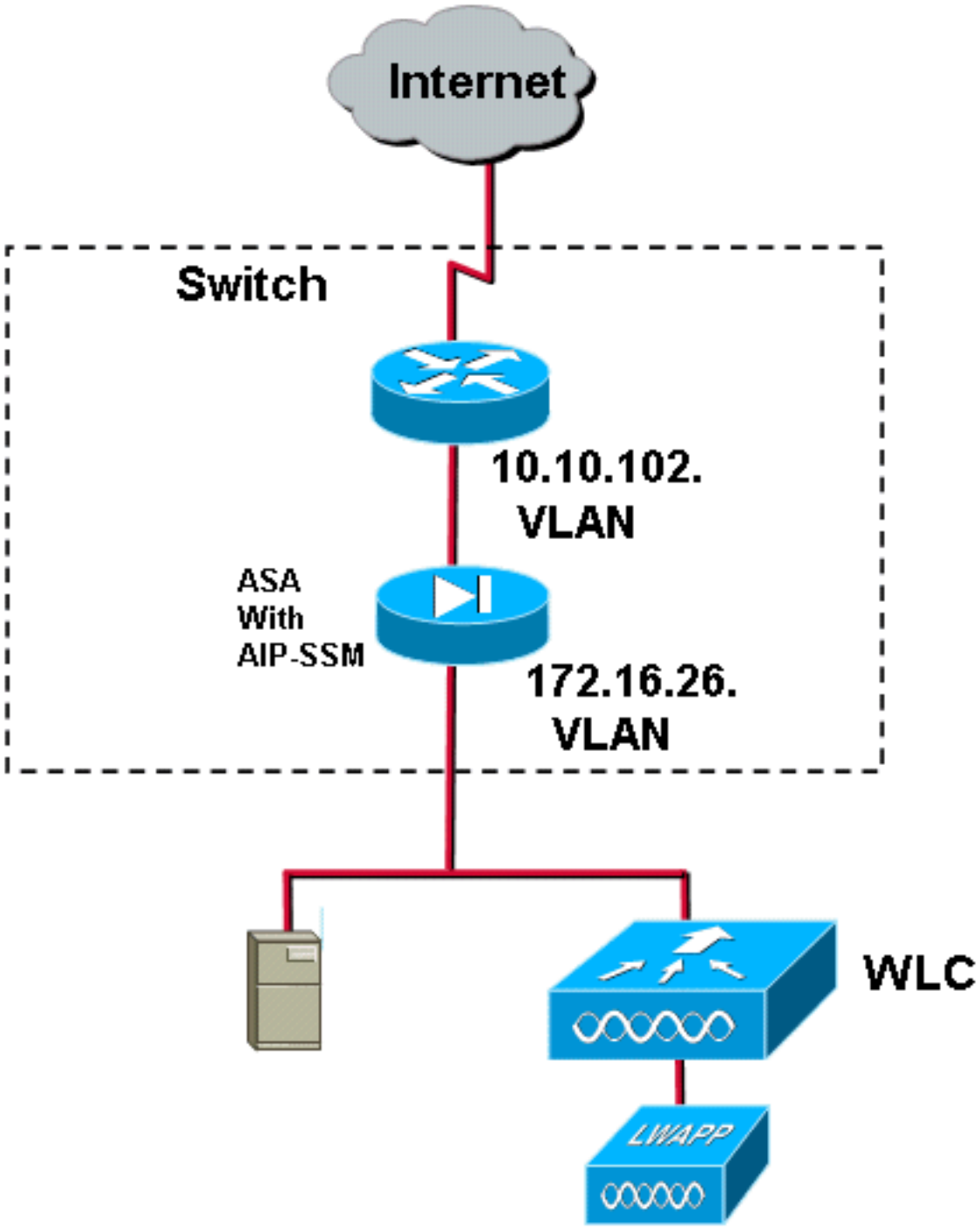
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list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

IDS のための ASA の設定

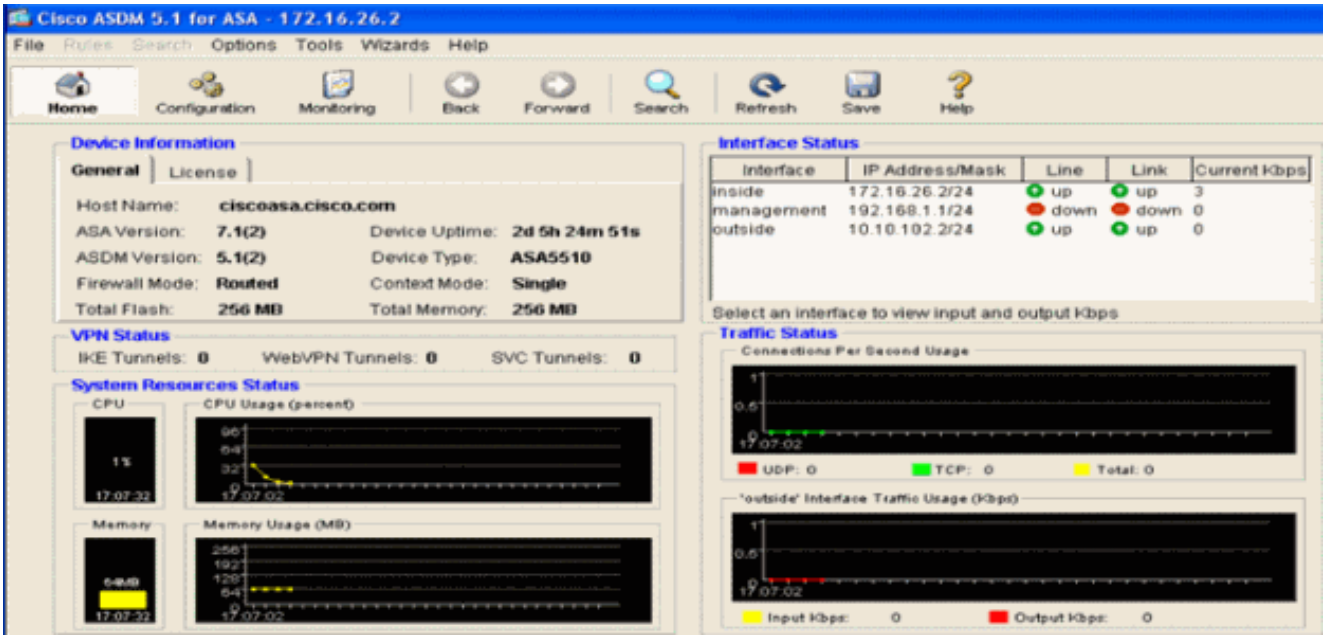
従来の侵入検知センサーとは異なり、ASA は必ずデータ パス上にある必要があります。つまり、スイッチ ポートからセンサーのパッシブ スニフィング ポートにトラフィックをスパニングせず

に、ASA は、インターフェイスでデータを受信し、内部的に処理をしてから、別のポートに転送する必要があります。IDS では、モジュラ ポリシー フレームワーク（MPF）を使用して、ASA が受信するトラフィックを internal Advanced Inspection and Prevention Security Services Module（AIP-SSM）にコピーして検査します。

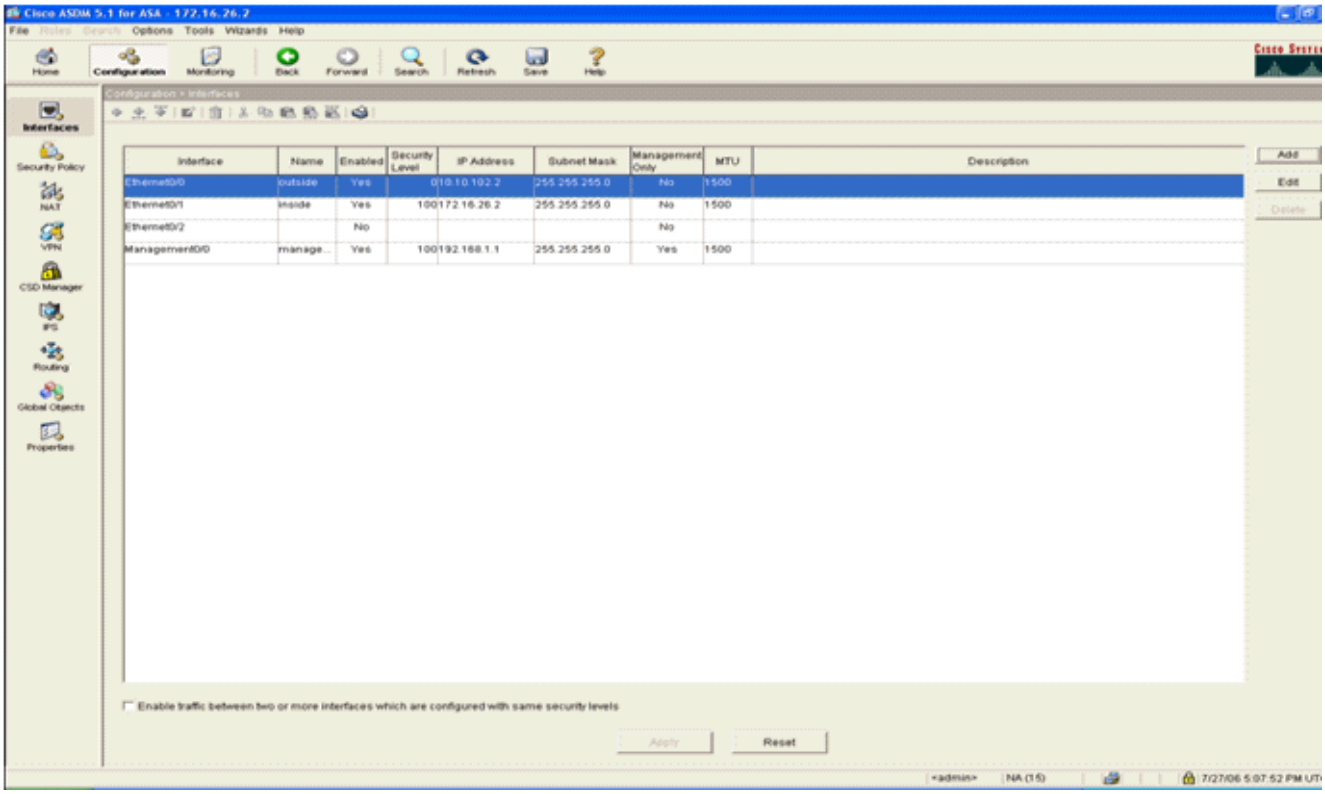


この例では、使用される ASA は、設定済みで、トラフィックを渡します。次の手順は、データを AIP-SSM に送信するポリシーの作成例を示します。

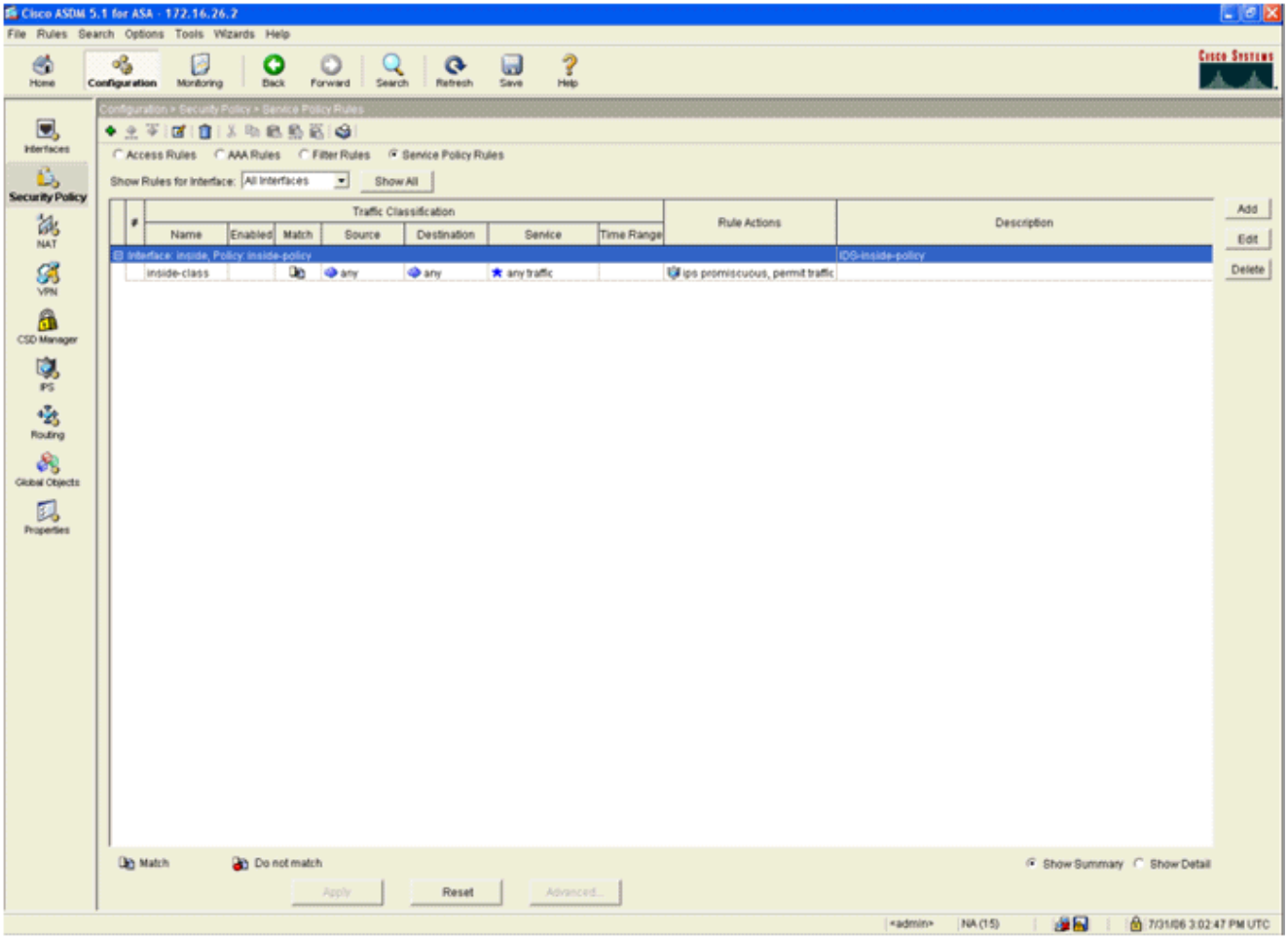
1. ASDM を使用して ASA にログインします。ログインに成功すると、[ASA Main System] ウィンドウが表示されます。



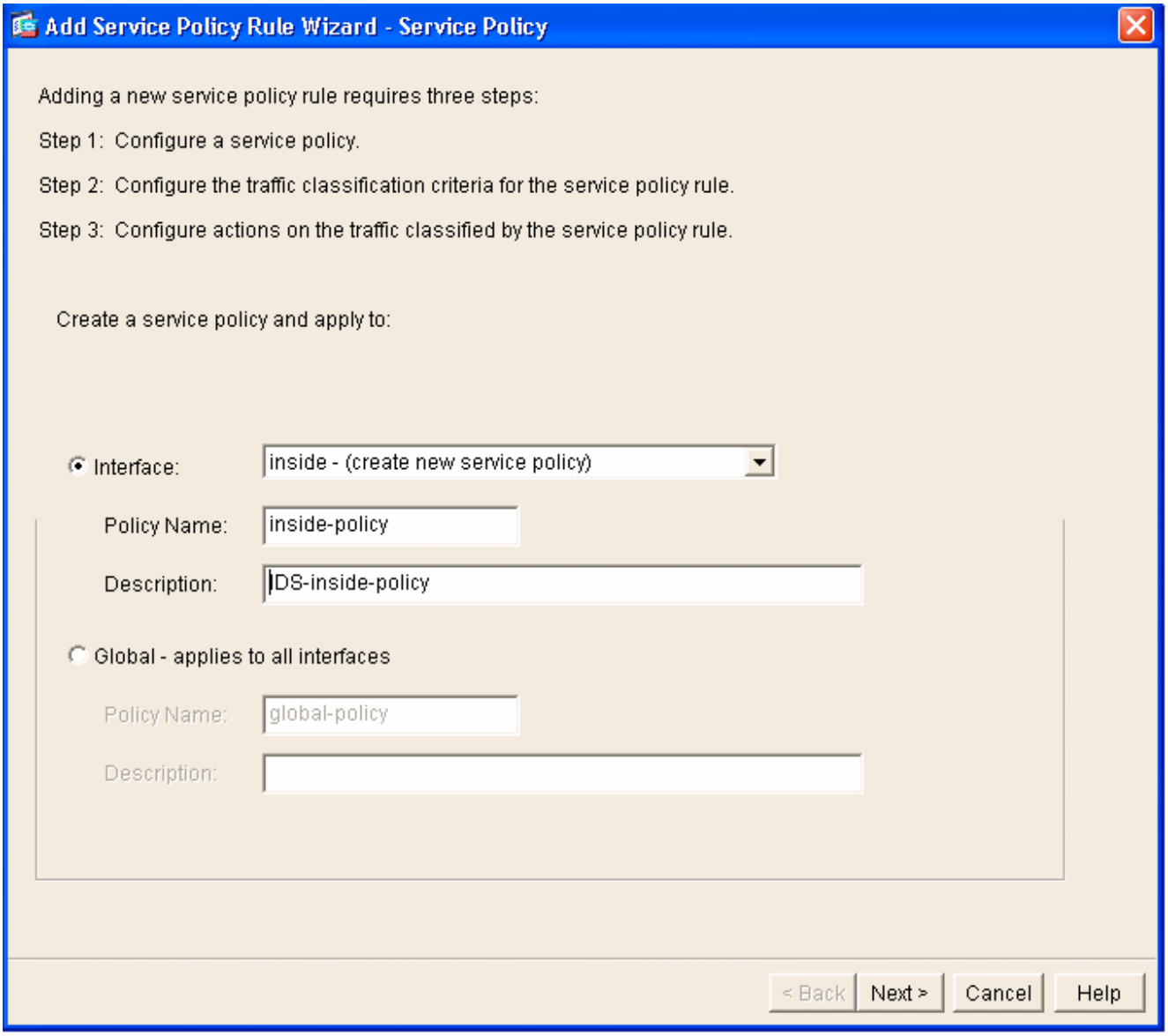
2. ページ上部の [Configuration] をクリックします。ウィンドウが ASA インターフェイスに切り替わります。



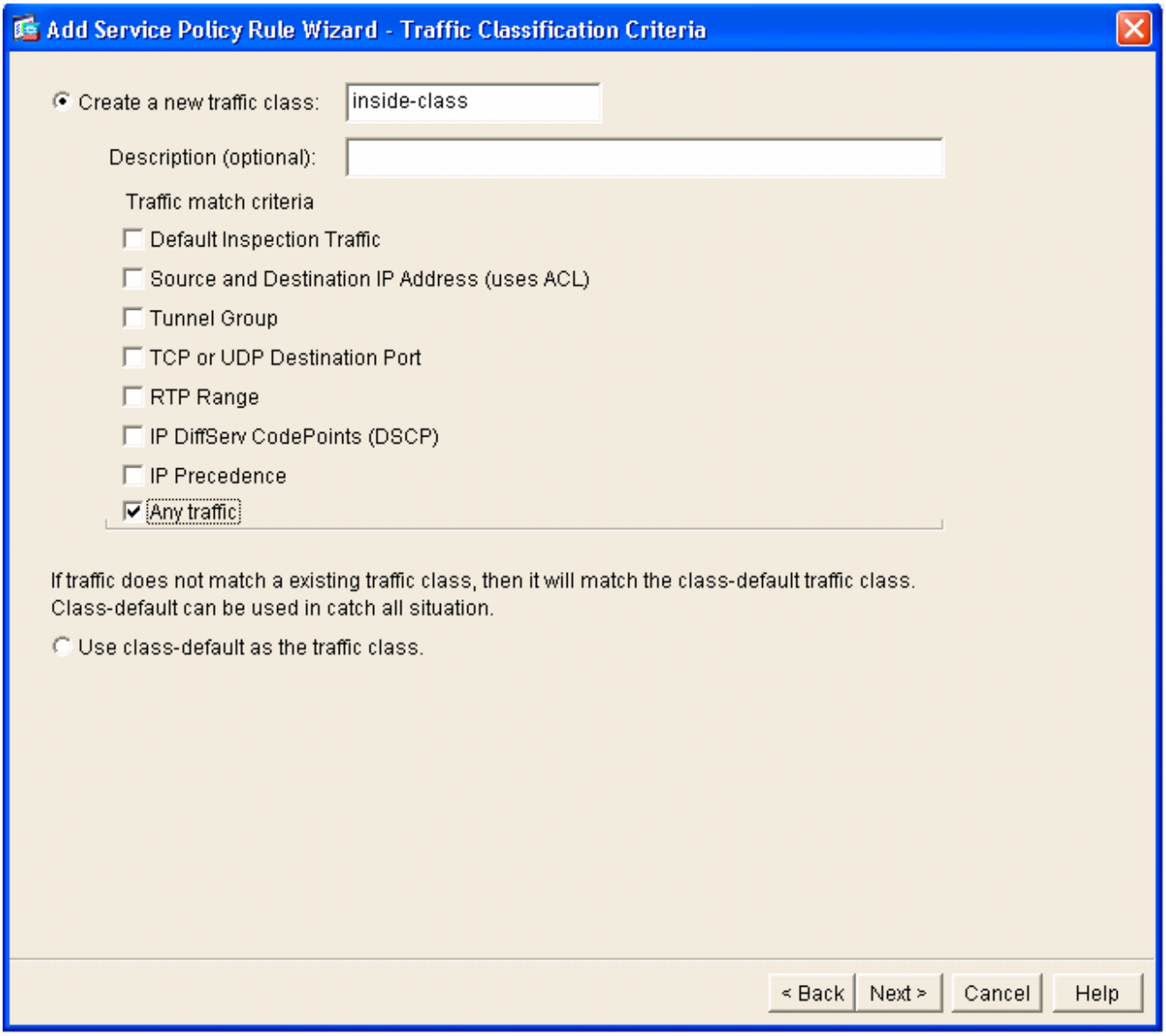
3. ウィンドウ左側の [Security Policy] をクリックします。結果のウィンドウで、[Service Policy Rules] タブを選択します。



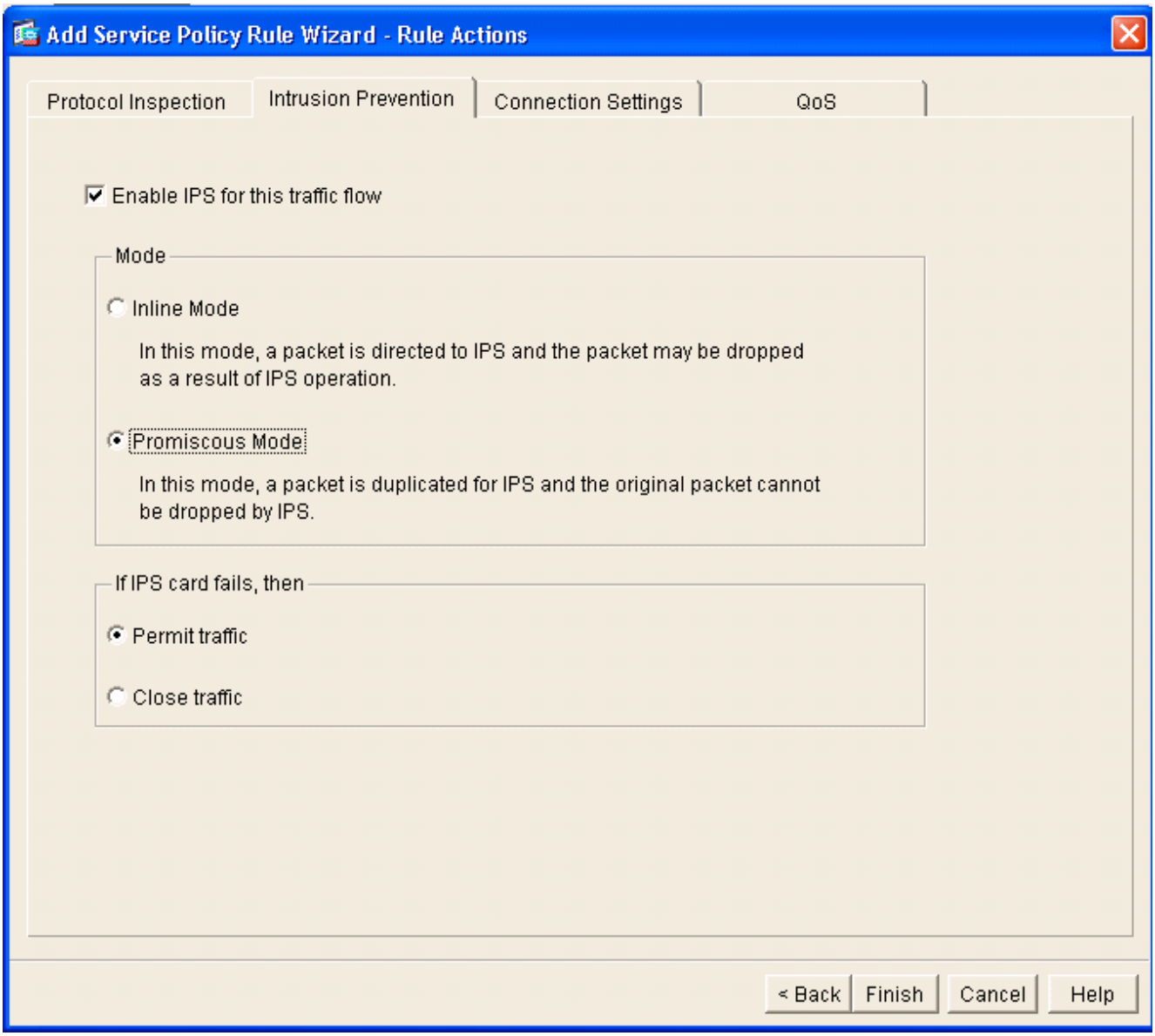
4. [Add] をクリックして、新しいポリシーを作成します。[Add Service Policy Rule Wizard] が新しいウィンドウで起動します。[Interface] をクリックし、ドロップダウン リストから正しいインターフェイスを選択して、トラフィックを渡すいずれかのインターフェイスにバインドされる新しいポリシーを作成します。2 つのテキスト ボックスを使用して、ポリシーに名前付け、ポリシーの内容を入力します。[Next] をクリックして、次の手順に進みます。



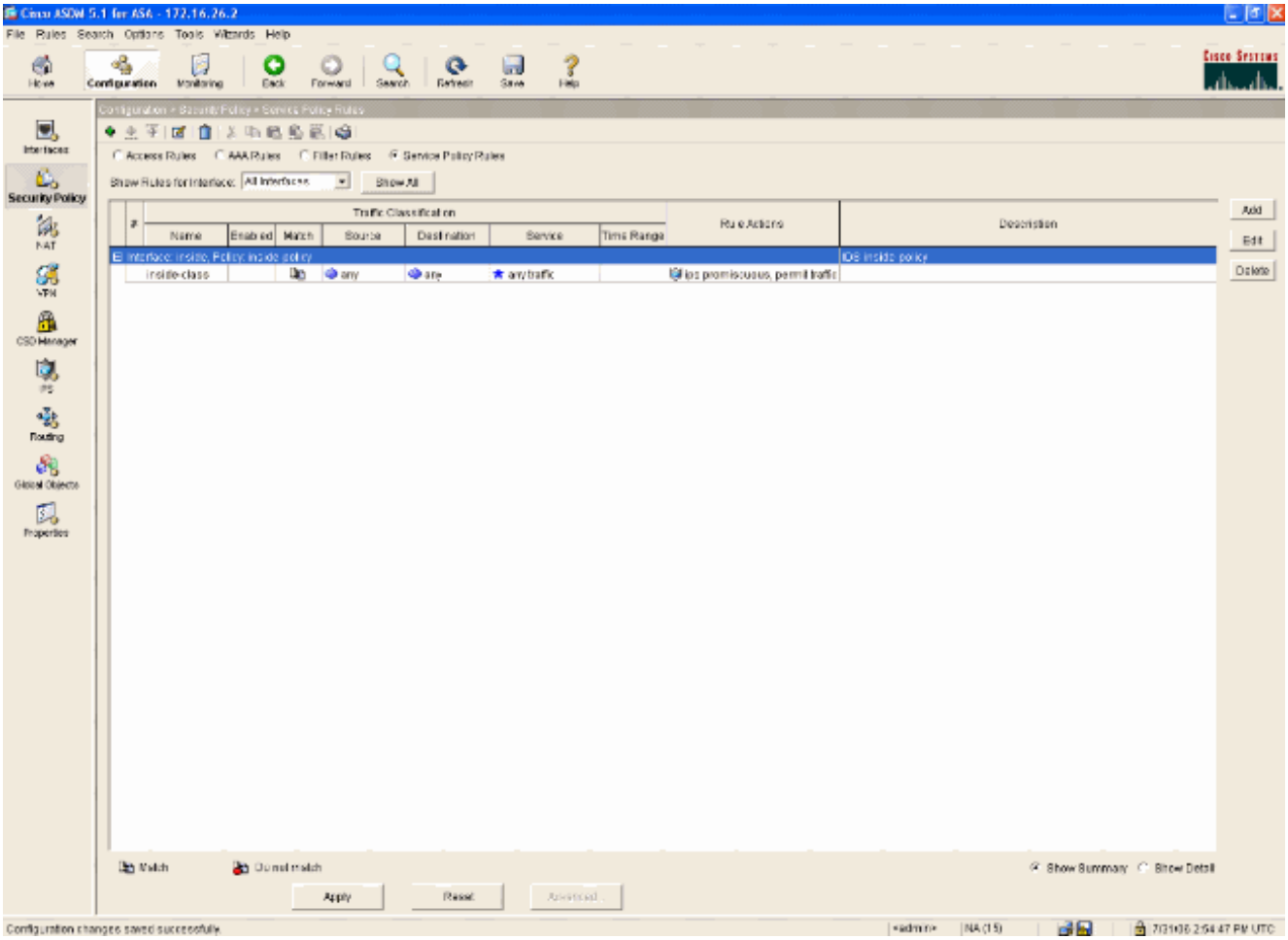
5. ポリシーに適用する新しいトラフィック クラスを構築します。通常は特定のデータ タイプを検査するために特定のクラスを構築しますが、この例では、説明のために [Any Traffic] を選択します。[Next] をクリックして、続行します。



6. 次の手順を実行します。トラフィックを AIP-SSM に送るように ASA を設定します。[Enable IPS for this traffic flow] チェックボックスをオンにして、侵入検知を有効にします。モジュールをデータ フローでインラインにせずに、モードを [Promiscuous] に設定して、トラフィックのコピーをアウトオブバンド モジュールに送信します。[Permit traffic] をクリックします。これにより、AIP-SSM で障害が発生した場合に ASA がフェールオープン状態に切り替わります。[Finish] をクリックして、変更を確認します。



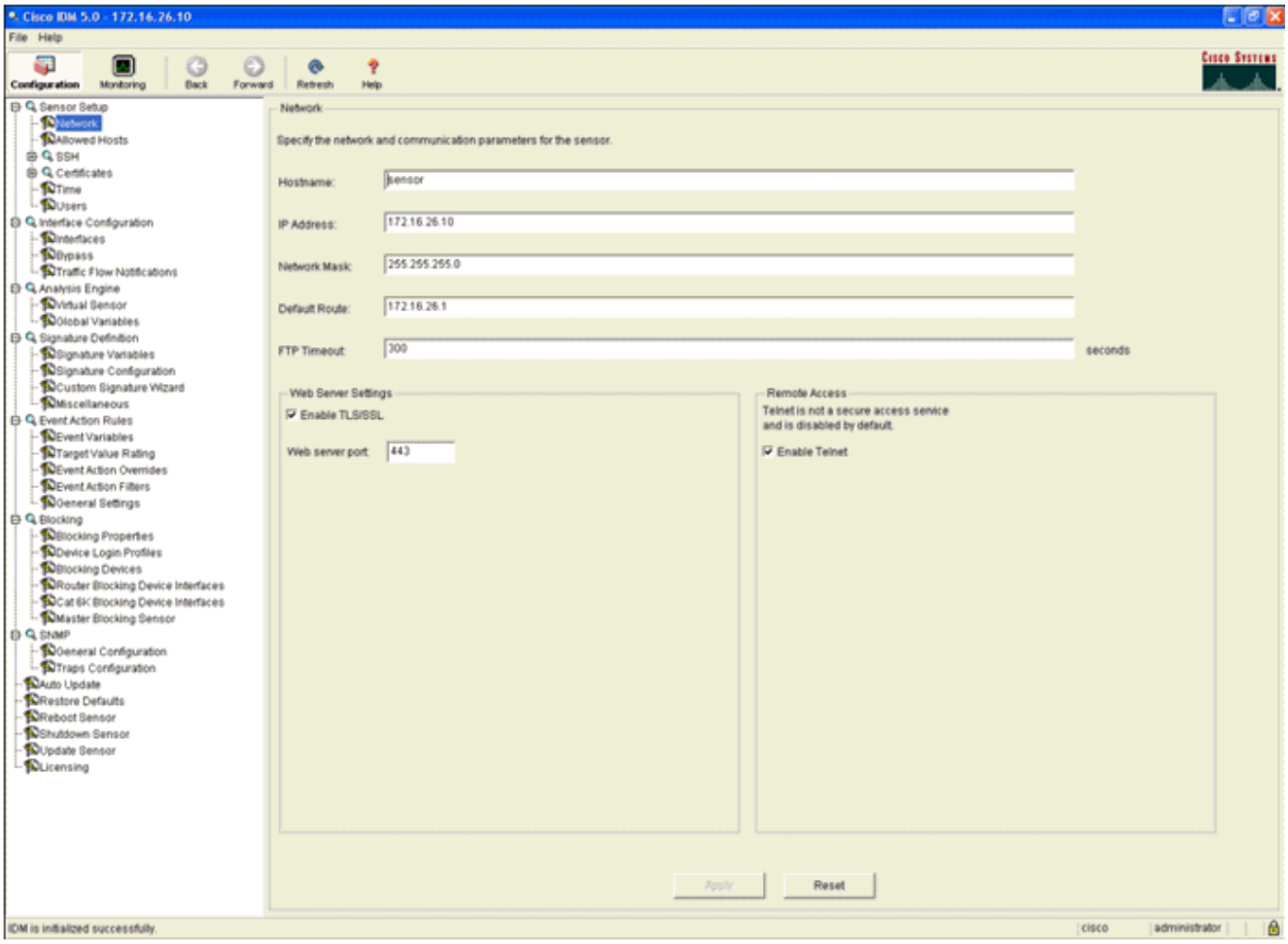
7. これで、トラフィックを IPS モジュールに送信するように、ASA が設定されました。上部の行で [Save] をクリックして、変更を ASA に書き込みます。



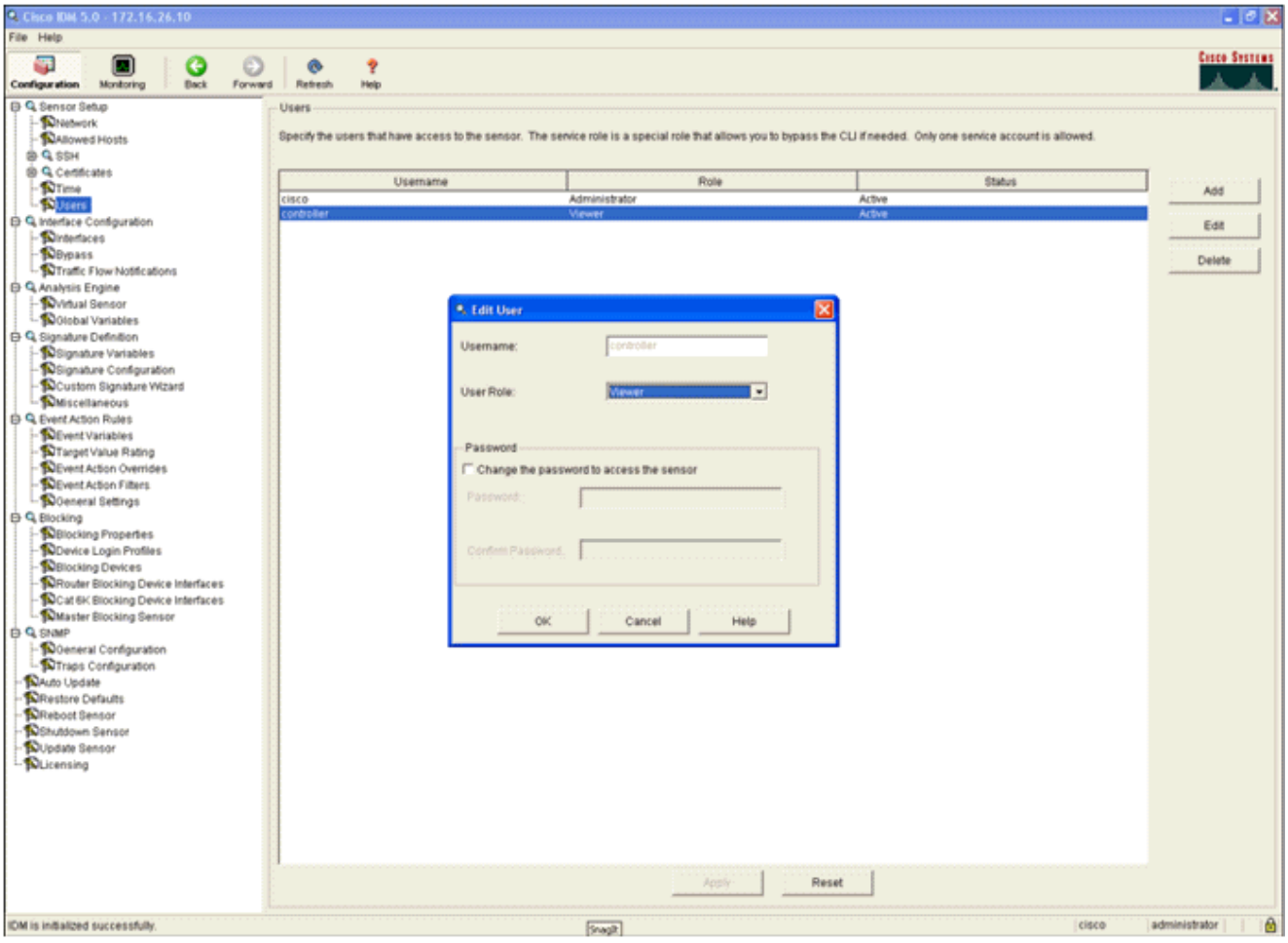
トラフィック検査のための AIP-SSM の設定

ASA はデータを IPS モジュールに送信しますが、AIP-SSM インターフェイスを仮想センサー エンジンにアソシエートします。

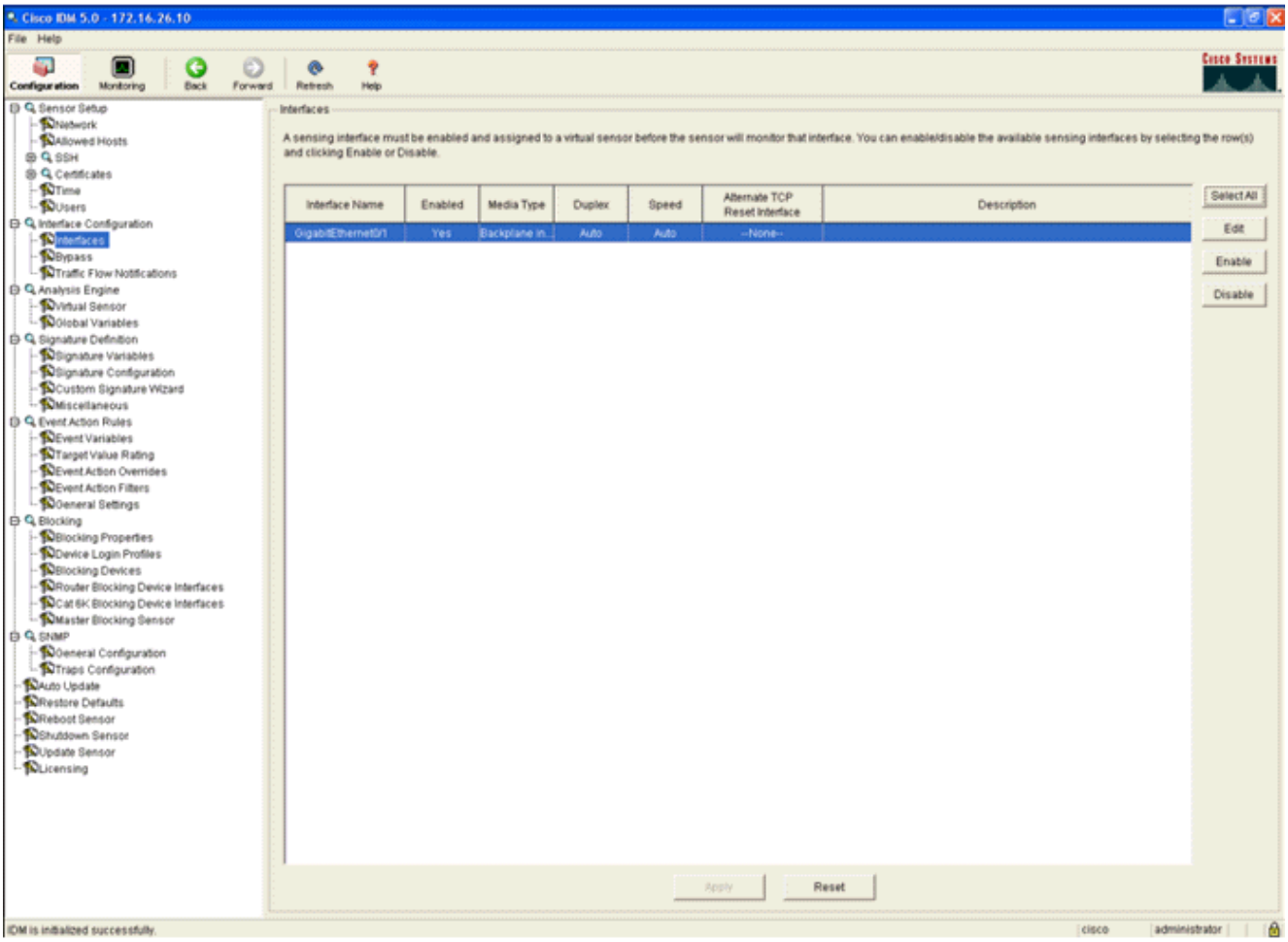
1. IDM を使用して AIP-SSM にログインします。



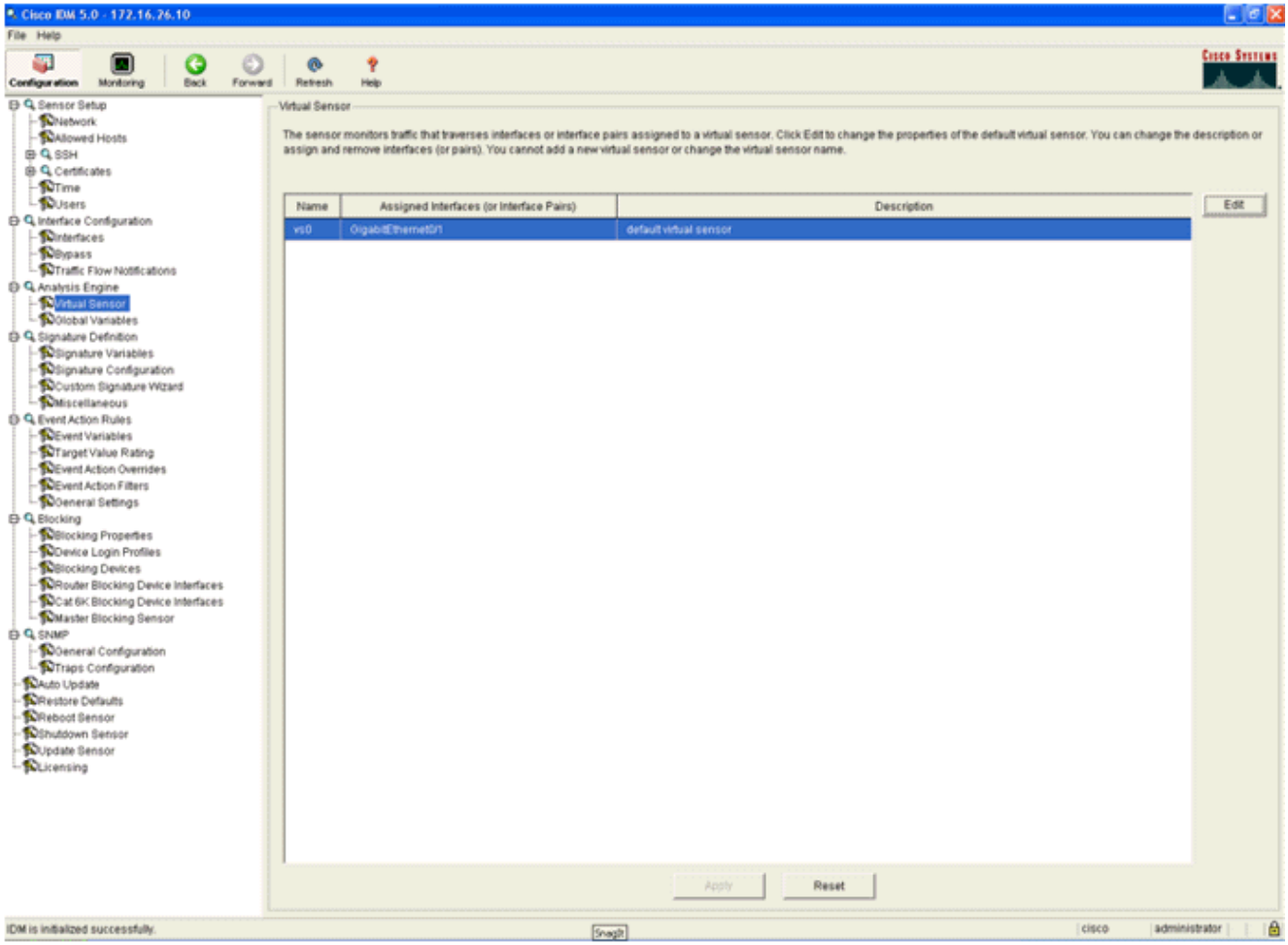
2. 表示以上の権限を持つユーザを追加します。



3. インターフェイスを有効にします。



4. 仮想センサー設定を確認します。

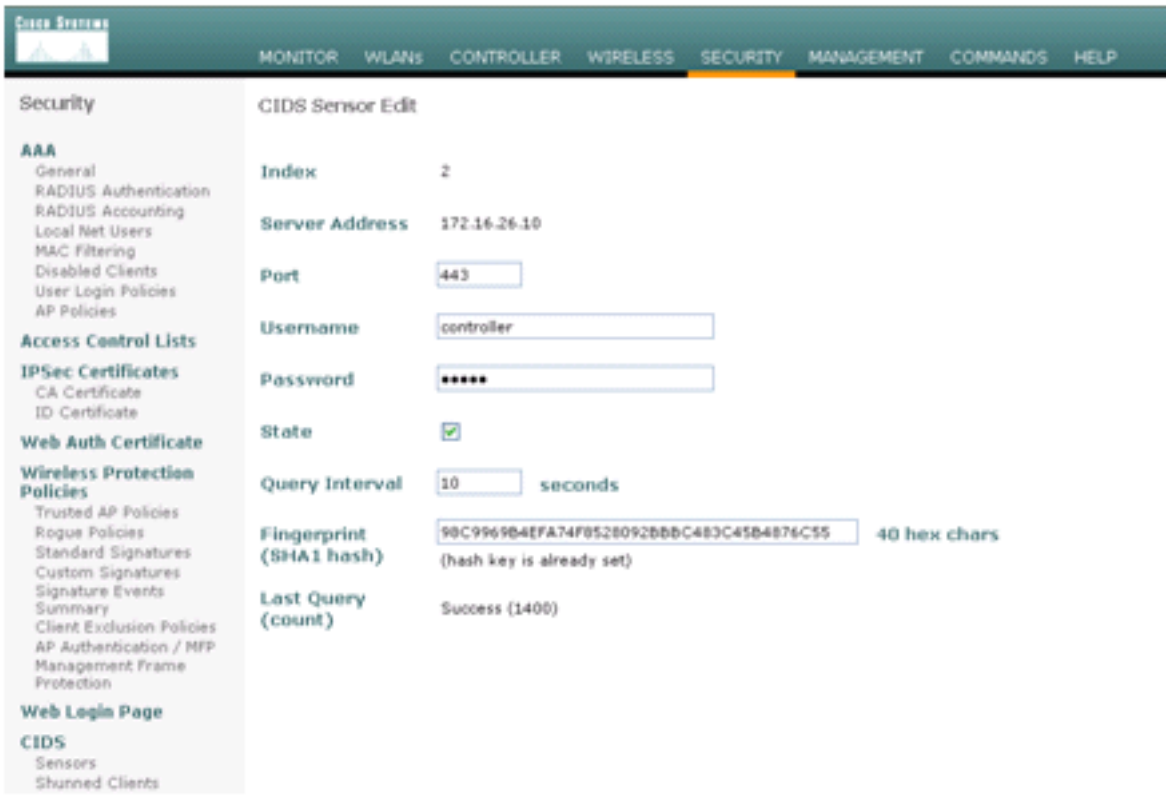


クライアント ブロックのために AIP-SSM をポーリングするための WLC の設定

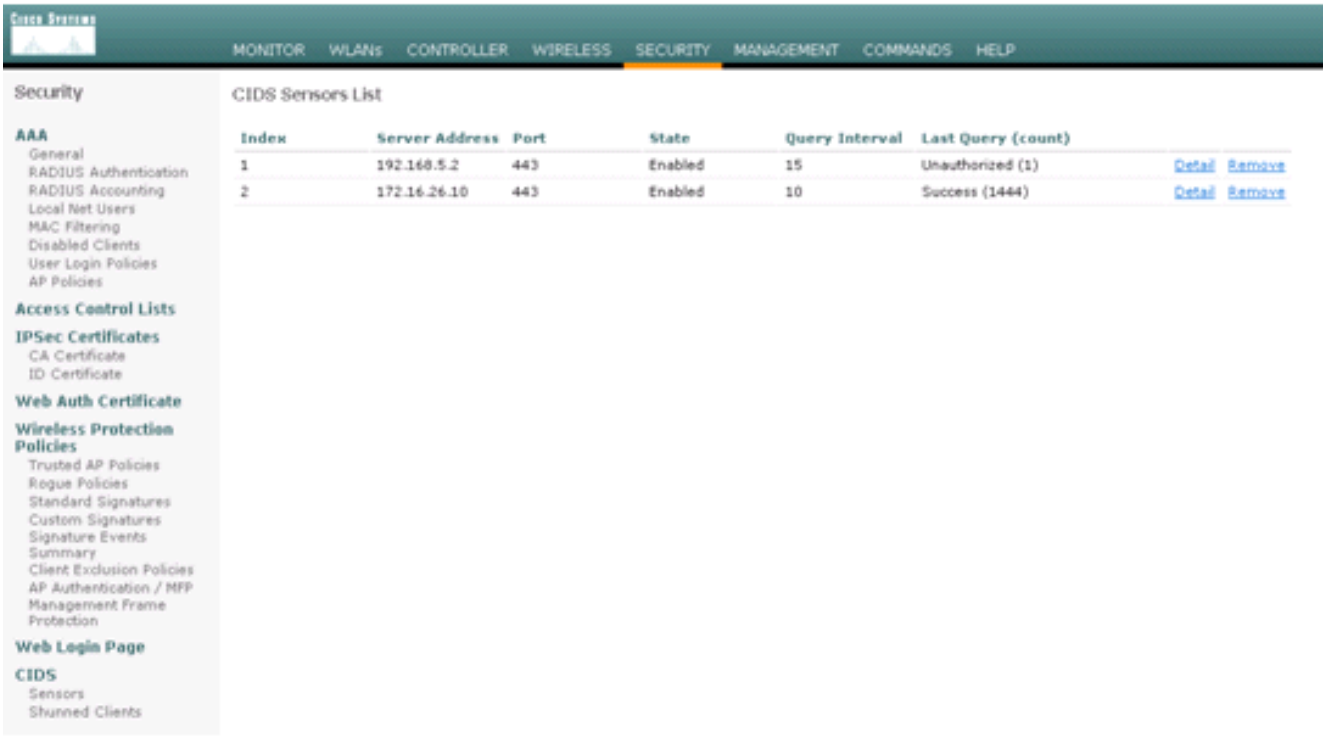
センサーを設定して、コントローラに追加できるようになったら、次の手順を実行します。

1. WLC で [Security] > [CIDS] > [Sensors] > [New] を選択します。
2. 前述のセクションで作成した IP アドレス、TCP ポート番号、ユーザ名およびパスワードを追加します。
3. センサーからフィンガープリントを取得するには、センサーで次のコマンドを実行して、SHA1 フィンガープリントを WLC に追加します（コロンは使用しません）。 これはコントローラと IDS のポーリング通信のセキュリティを確保するために使用します。

```
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
```



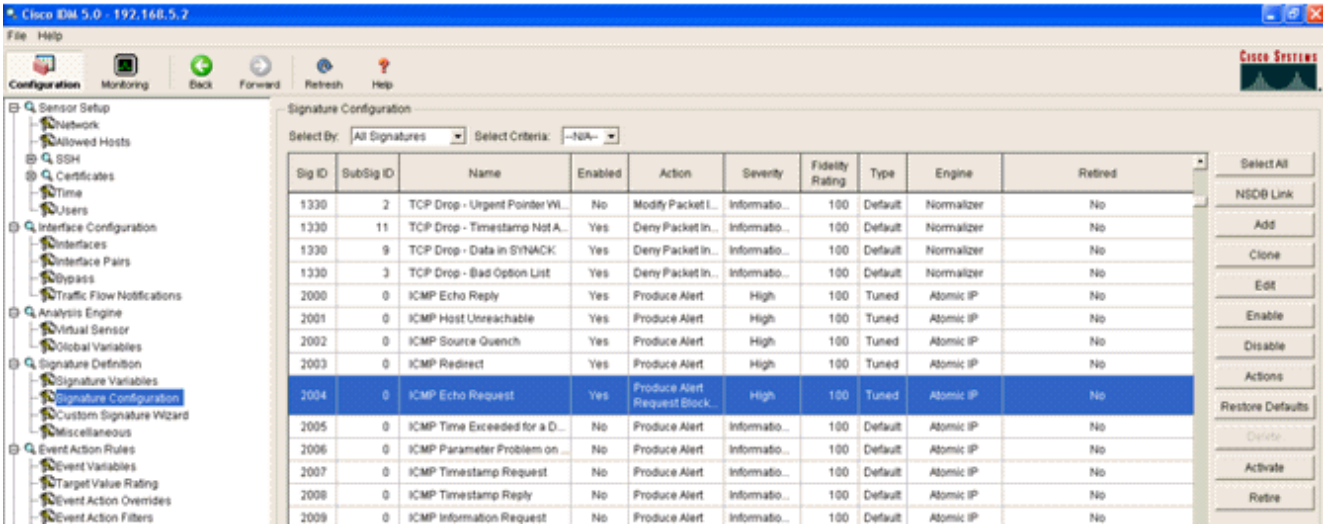
4. AIP-SSM と WLC 間の接続のステータスを確認します。



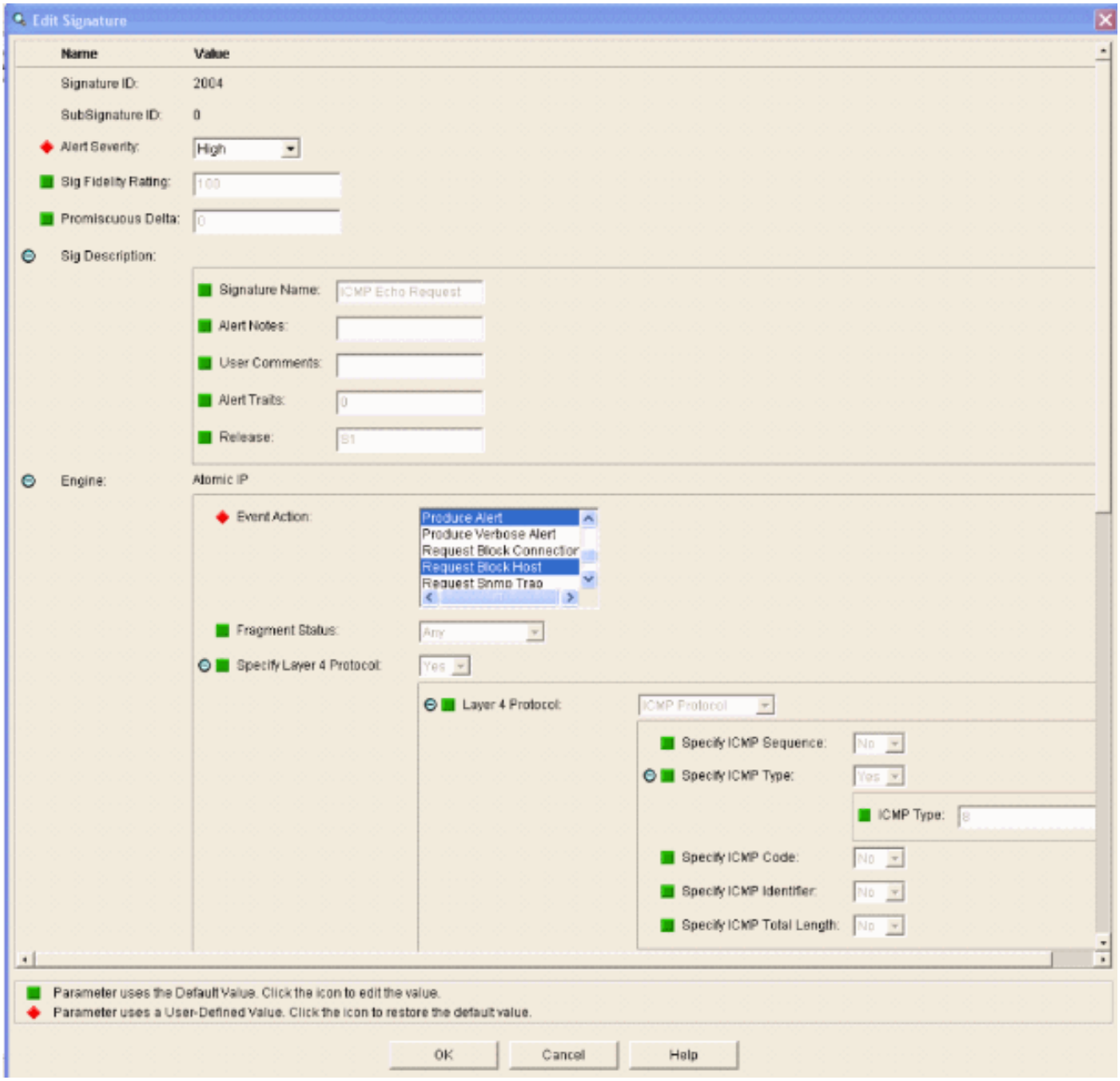
AIP-SSM へのブロッキング シグニチャの追加

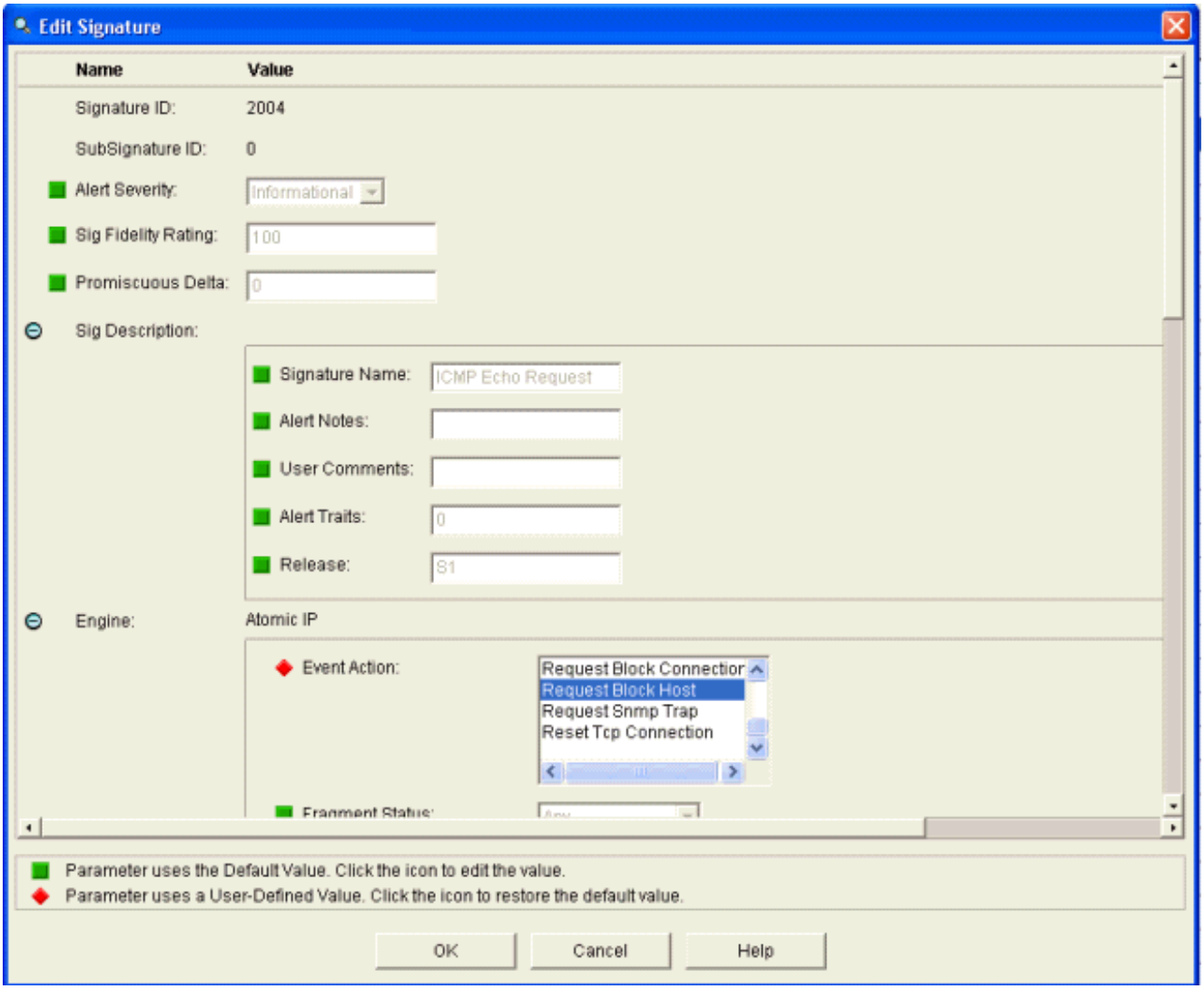
トラフィックをブロックする検査シグニチャを追加します。使用できるツールに基づいてジョブを実行できるシグニチャはたくさんありますが、この例では、ping パケットをブロックするシグニチャを作成します。

1. クイック設定検査を実行するために 2004 シグニチャ（[ICMP Echo Request]）を選択します。



2. シグニチャを有効にし、[Alert Severity] を [High] に設定し、[Event Action] を [Produce Alert] および [Request Block Host] に設定し、検証手順を完了します。[Request Block Host] アクションは、WLC でクライアント除外を作成するときに重要です。


Edit Signature
Name
Value
Signature ID:
2004
SubSignature ID:
0
Alert Severity:
High
Sig Fidelity Rating:
100
Promiscuous Delta:
0
Sig Description:
Signature Name:
ICMP Echo Request
Alert Notes:
User Comments:
Alert Traits:
0
Release:
S1
Engine:
Atomic IP
Event Action:
Produce Alert
Produce Verbose Alert
Request Block Connection
Request Block Host
Request Snmp Trap
Fragment Status:
Any
Specify Layer 4 Protocol:
Yes
Layer 4 Protocol:
ICMP Protocol
Specify ICMP Sequence:
No
Specify ICMP Type:
Yes
ICMP Type:
8
Specify ICMP Code:
No
Specify ICMP Identifier:
No
Specify ICMP Total Length:
No
Parameter uses the Default Value. Click the icon to edit the value.
Parameter uses a User-Defined Value. Click the icon to restore the default value.
OK
Cancel
Help

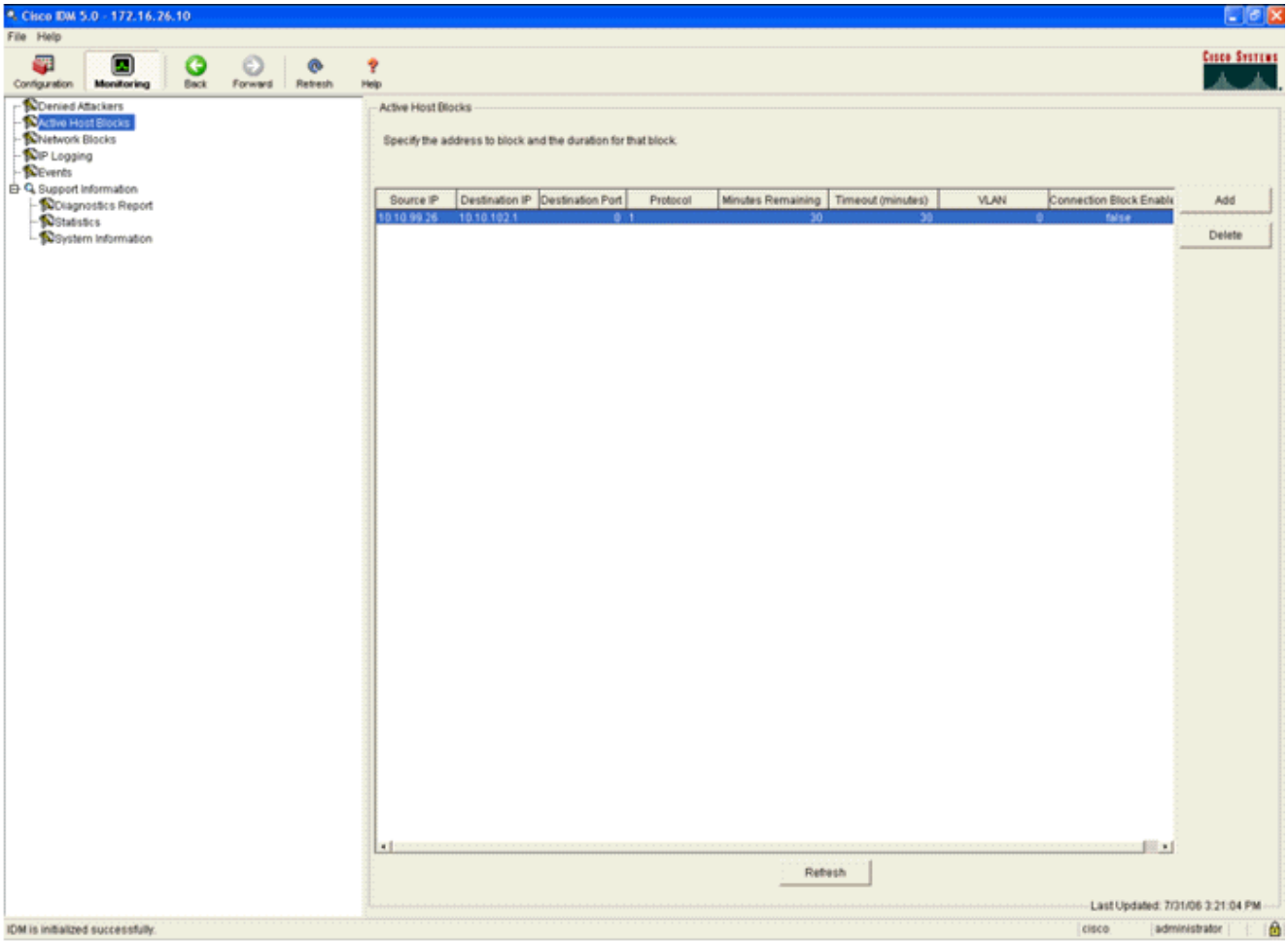


3. [OK] をクリックして、シグニチャを保存します。
4. シグニチャがアクティブで、ブロック アクションを実行するように設定されていることを確認します。
5. [Apply] をクリックして、シグニチャをモジュールに確定します。

IDM によるブロッキングおよびイベントのモニタ

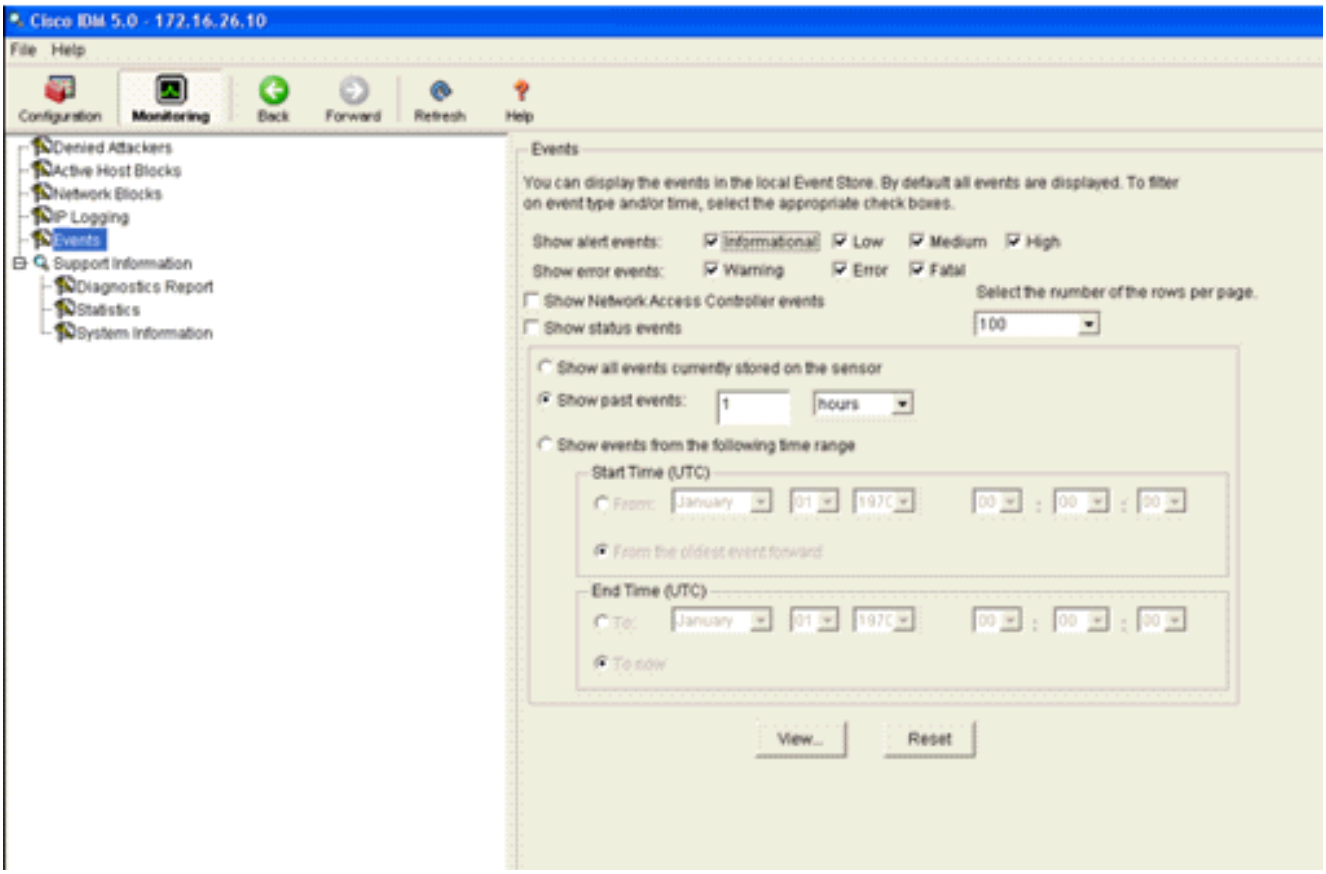
次のステップを実行します。

1. IDM 内では、2 つの場所から、シグニチャが正常に起動したかどうかを確認できます。最初の方式では、AIP-SSM がインストールしたアクティブ ブロックが示されます。アクションの上部行の [Monitoring] をクリックします。左側に表示される項目リストで、[Active Host Blocks] を選択します。ping シグニチャがトリガーされると、[Active Host Blocks] ウィンドウに、攻撃者の IP アドレス、攻撃を受けたデバイスのアドレス、ブロックの適用期間が表示されます。デフォルトのブロック時間は、30 分ですが、これは調整可能です。ただし、この値の変更については、このドキュメントでは説明していません。このパラメータの変更方法については、ASA の設定マニュアルを参照してください。ブロックをすぐに削除し、リストから選択して、[Delete] をクリックします。

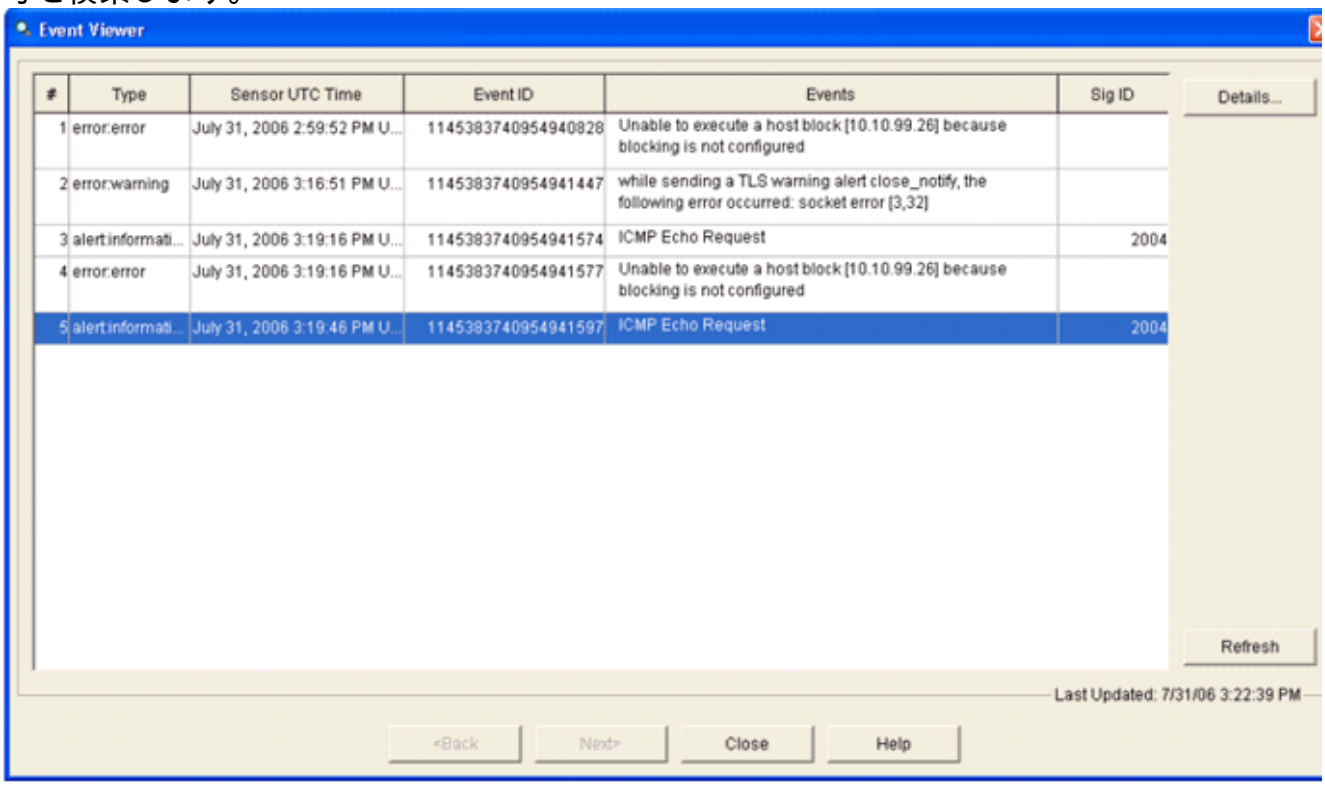


トリガーされるシグニチャを表示する 2 つめの方式では、AIP-SSM イベント バッファを使用します。[IDM Monitoring] ページから、左側の項目リストで [Events] を選択します。イベント検索ユーティリティが表示されます。適切な検索条件を設定し、**[View...]をクリックします。**

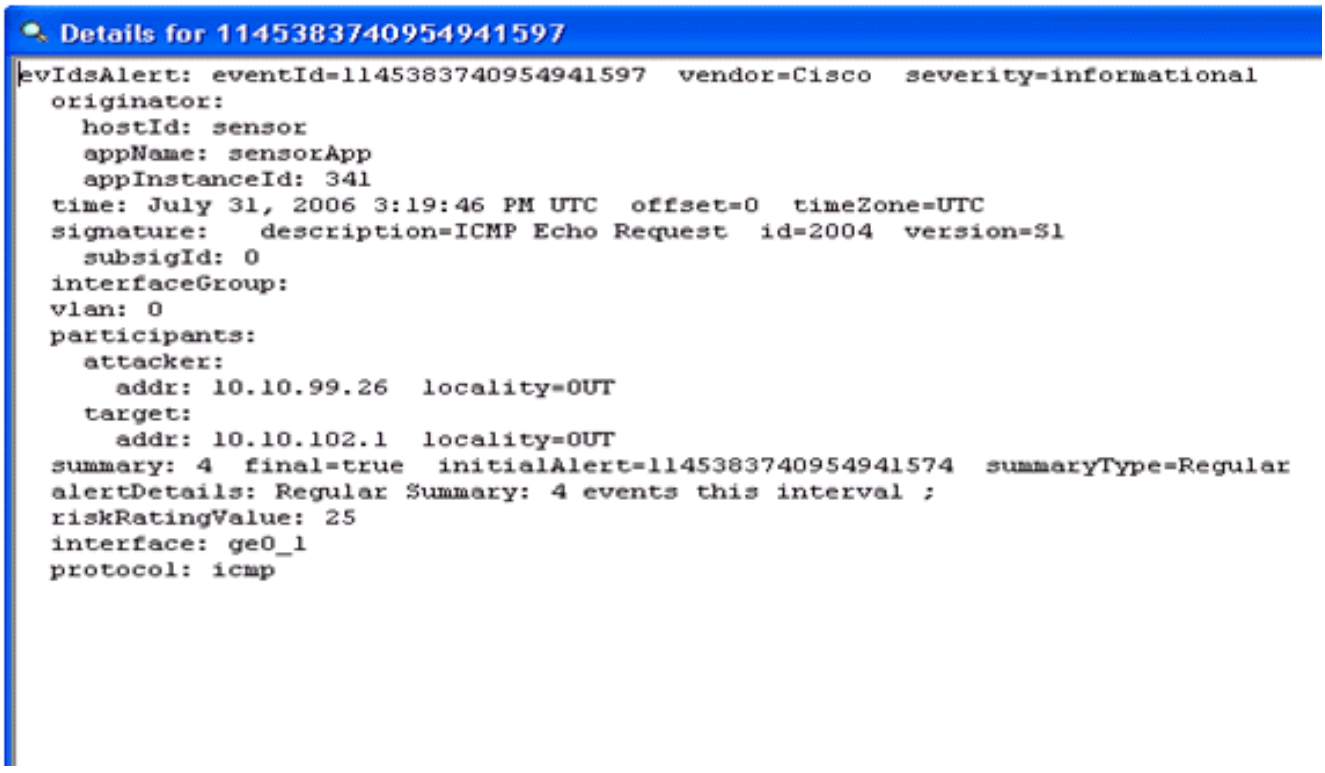
.



2. イベント ビューアが表示され、指定された条件と一致するイベントのリストが表示されます。リストをスクロールして、以前の設定手順で変更した [ICMP Echo Request] シグニチャを探します。[Events] 列でシグニチャの名前を検索するか、[Sig ID] 列でシグニチャの ID 番号を検索します。



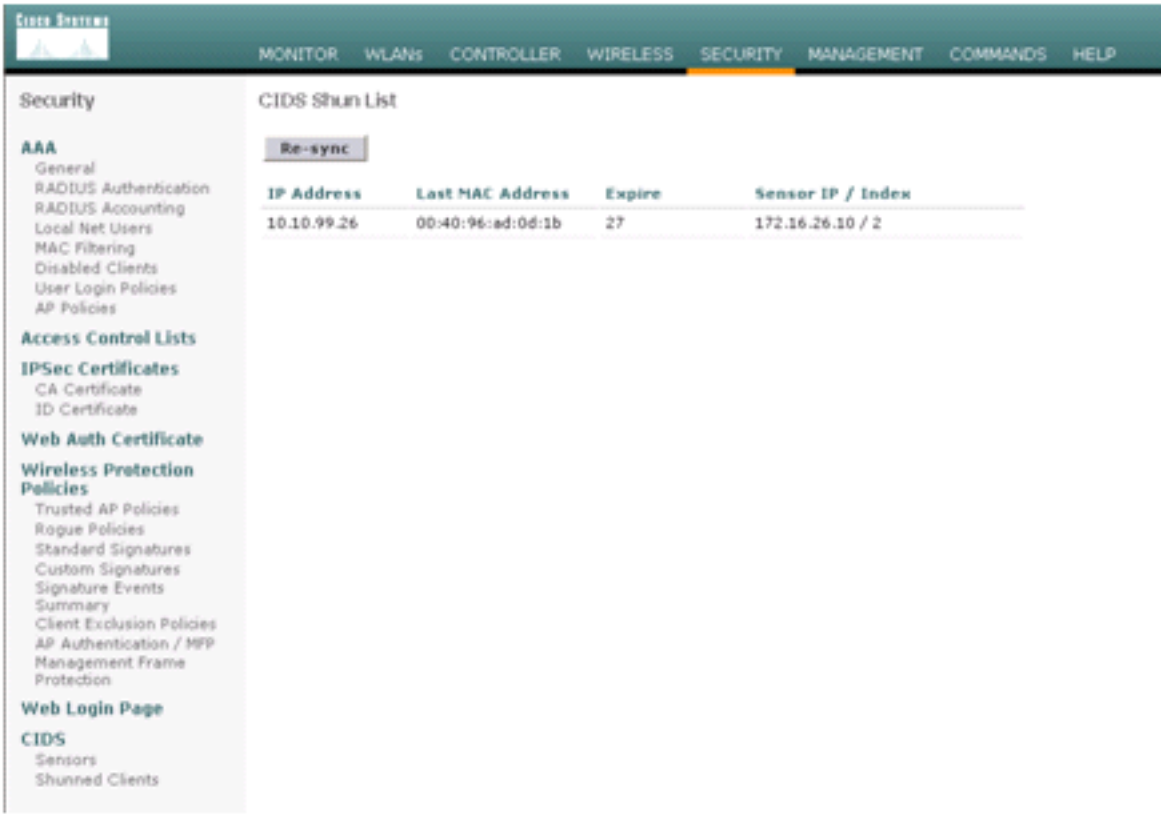
3. シグニチャを検索したら、エントリをダブルクリックして、新しいウィンドウを開きます。この新しいウィンドウには、シグニチャをトリガーしたイベントに関する詳細情報が表示されます。



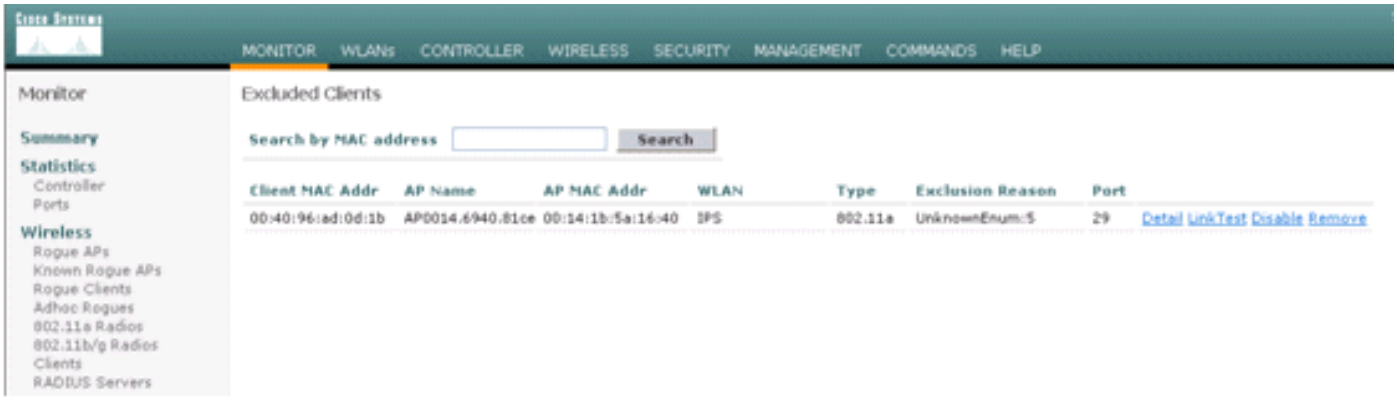
ワイヤレス コントローラでのクライアント除外のモニタ

この時点で、コントローラの [Shunned Clients] リストには、ホストの IP および MAC アドレス

が入力されます。



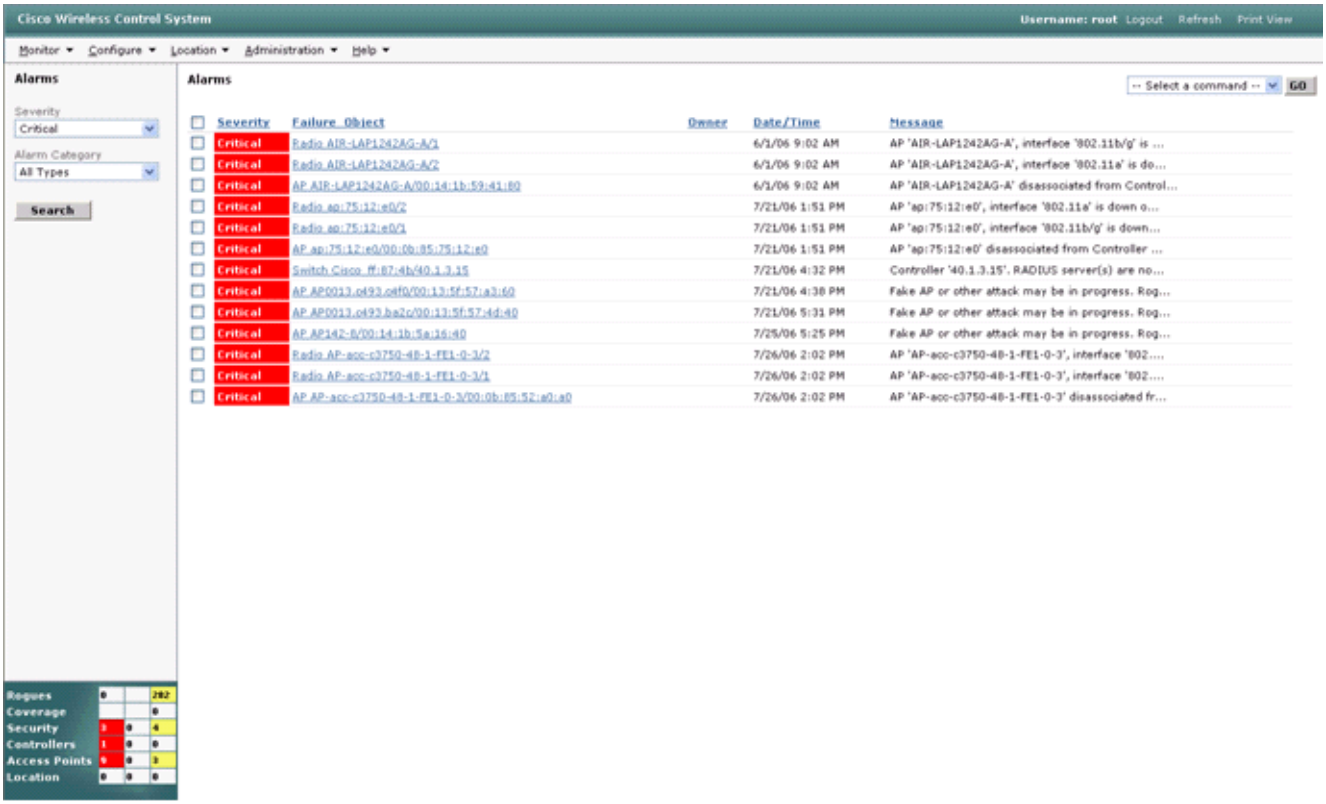
ユーザはクライアント除外リストに追加されます。



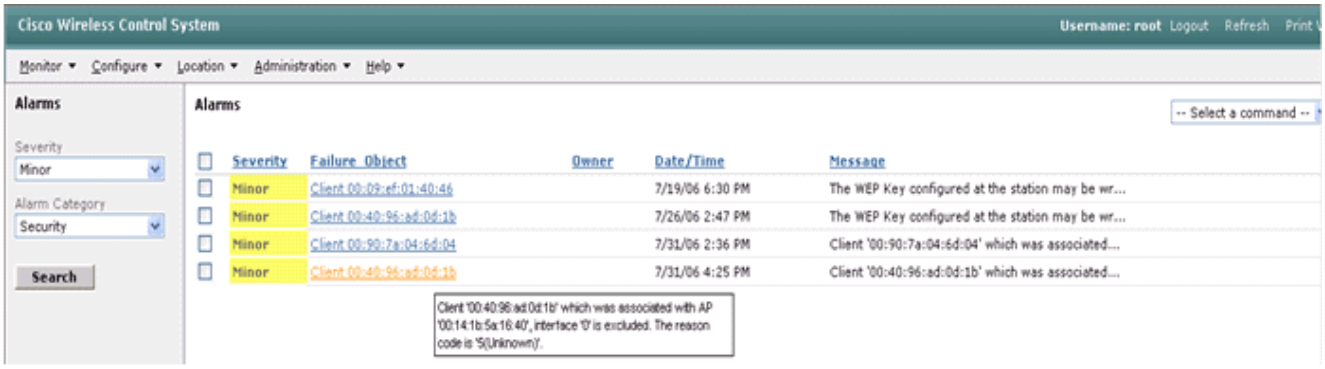
WCS でのイベントのモニタ

AIP-SSM 内でブロックをトリガーするセキュリティ イベントにより、コントローラは、攻撃者のアドレスをクライアント除外リストに追加します。また、WCS 内でイベントが生成されます。

1. WCS メイン メニューから [Monitor] > [Alarms] ユーティリティを使用し、除外イベントを表示します。WCS は最初に、不明なすべてのアラームを表示し、ウィンドウ左側に検索機能を提供します。
2. 検索条件を変更して、クライアント ブロックを検索します。[Severity] で [Minor] を選択し、[Alarm Category] を [Security] に設定します。
3. [Search] をクリックします。



4. [Alarm] ウィンドウに、重大度が低いセキュリティ アラームだけがリストされます。AIP-SSM 内でブロックをトリガーしたイベントにマウスを合わせます。特に、WCS は、アラームの原因となったクライアント ステーションの MAC アドレスを示します。適切なアドレスを示すと、WCS により、イベントの詳細を示す小さいウィンドウが表示されます。リンクをクリックして、別のウィンドウでこれらと同じ詳細を表示します。



Cisco ASA の設定例

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 10.10.102.2 255.255.255.0
!
```

```
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.26.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
mtu outside 1500
asdm image disk0:/asdm512-k8.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 102 interface
nat (inside) 102 172.16.26.0 255.255.255.0
nat (inside) 102 0.0.0.0 0.0.0.0
route inside 0.0.0.0 0.0.0.0 172.16.26.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.12 255.255.255.255 inside
http 0.0.0.0 0.0.0.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 50
dhcpd enable management
!
class-map inside-class
 match any
!
!
policy-map inside-policy
 description IDS-inside-policy
 class inside-class
  ips promiscuous fail-open
!
```

```
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Cisco 侵入防御システム センサーの設定例

```
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#
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Installing and Using Cisco Intrusion Prevention System Device Manager 5.1
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス：コンフィギュレーション ガイド
- Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.0：インターフェイスの設定
- WLC Configuration Guide 4.0
- ワイヤレスに関するテクニカルサポート
- Wireless LAN Controller（WLC）に関する FAQ
- ワイヤレス LAN コントローラと Lightweight アクセス ポイントの基本設定例
- セキュリティ ソリューションの設定
- テクニカル サポートとドキュメント – Cisco Systems