無線LAN控制器和IPS整合指南

目錄

簡介

Cisco Unified Intrusion Detection System(IDS)/Intrusion Prevention System(IPS)是Cisco Self-Defending Network的一部分，是業界第一個整合的有線和無線安全解決方案。Cisco Unified IDS/IPS在無線邊緣、有線邊緣、廣域網邊緣和資料中心採用全面的安全方法。當關聯的客戶端通過Cisco統一無線網路傳送惡意流量時，Cisco有線IDS裝置會檢測到該攻擊，並向Cisco無線LAN控制器(WLC)傳送shun請求，然後WLC將解除客戶端裝置的關聯。

Cisco IPS是一種基於網路的內聯解決方案，旨在準確識別、分類和阻止惡意流量（包括蠕蟲、間諜軟體/廣告軟體、網路病毒和應用濫用），使它們不影響業務連續性。

利用Cisco IPS感測器軟體版本5,Cisco IPS解決方案將內聯防禦服務與創新技術相結合，以提高準確性。這樣可以完全信任為您的IPS解決方案提供的保護，而不必擔心合法流量被丟棄。Cisco IPS解決方案還通過其與其他網路安全資源進行合作的獨特能力，為您的網路提供全面保護，並提

供主動網路保護方法。

Cisco IPS解決方案可通過使用以下功能幫助使用者以更大的信心阻止更多威脅：

- **準確的內聯防禦**技術 — 提供無與倫比的信心，能夠針對更廣泛的威脅採取防範措施，而不會有丟棄合法流量的風險。這些獨特的技術提供了智慧、自動化、情景分析資料，有助於確保您從入侵防禦解決方案中獲得最大收益。
- **多向量威脅識別 —** 通過對第2層到第7層的流量進行詳細檢查，保護您的網路免受策略違規、漏洞利用和異常活動的影響。
- **獨特的網路協**作 — 通過網路合作增強可擴充性和恢復能力，包括高效的流量捕獲技術、負載平衡功能以及加密流量的可視性。
- **全面的部署解**決方案 — 為所有環境(從中小型企業(SMB)和分支機構辦公室位置，到大型企業和服務提供商安裝)提供解決方案。
- **強大的管理、事件關聯和支援服**務**—**支援完整的解決方案，包括配置、管理、資料關聯和高級支援服務。特別是思科安全監控、分析和響應系統(MARS)可識別、隔離違規元素，並建議精確刪除這些元素，以便實現網路範圍的入侵防禦解決方案。思科事件控制系統使網路能夠快速適應並提供分散式響應，從而防止新的蠕蟲和病毒爆發。

結合使用時，這些元素可提供全面的內聯防護解決方案，並使您有信心在影響業務連續性之前檢測和阻止最廣泛的惡意流量。思科自防禦網路計畫要求為網路解決方案提供整合和內建安全性。目前基於輕量型存取點通訊協定(LWAPP)的WLAN系統僅支援基本IDS功能，因為此系統本質上是一個第2層系統，且線路處理能力有限。思科會及時發佈新代碼，在新代碼中包含新的增強功能。4.0版具有最新功能，包括基於LWAPP的WLAN系統與Cisco IDS/IPS產品系列的整合。在此版本中，目標是允許Cisco IDS/IPS系統指示WLC在從第3層到第7層任意位置檢測到涉及所考慮客戶端的攻擊時，阻止特定客戶端訪問無線網路。

必要條件

需求

確保滿足以下最低要求：

- WLC韌體版本4.x及更高版本
- 最好瞭解如何配置Cisco IPS和Cisco WLC。

採用元件

Cisco WLC

IDS修改軟體版本4.0中包含以下控制器：

- Cisco 2000系列WLC
- Cisco 2100系列WLC
- Cisco 4400系列WLC
- 思科無線服務模組(WiSM)
- Cisco Catalyst 3750G系列整合存取交換器
- Cisco無線LAN控制器模組(WLCM)

存取器

- Cisco Aironet 1100 AG系列輕量型存取點
- Cisco Aironet 1200 AG系列輕量型存取點
- Cisco Aironet 1300系列輕量型存取點
- Cisco Aironet 1000系列輕量型存取點

管理

- 思科無線控制系統(WCS)
- Cisco 4200系列感應器
- Cisco IDS Management - Cisco IDS Device Manager(IDM)

Cisco整合IDS/IPS平台

- 採用Cisco IPS感測器軟體5.x或更高版本的Cisco IPS 4200系列感測器。
- 適用於採用Cisco IPS感應器軟體5.x的Cisco ASA 5500系列調適型安全裝置的SSM10和SSM20
- 採用Cisco IPS感應器軟體5.x的Cisco ASA 5500系列調適型安全裝置
- 採用Cisco IPS感應器軟體5.x的Cisco IDS網路模組(NM-CIDS)
- 採用Cisco IPS感應器軟體5.x的Cisco Catalyst 6500系列入侵偵測系統模組2(IDSM-2)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

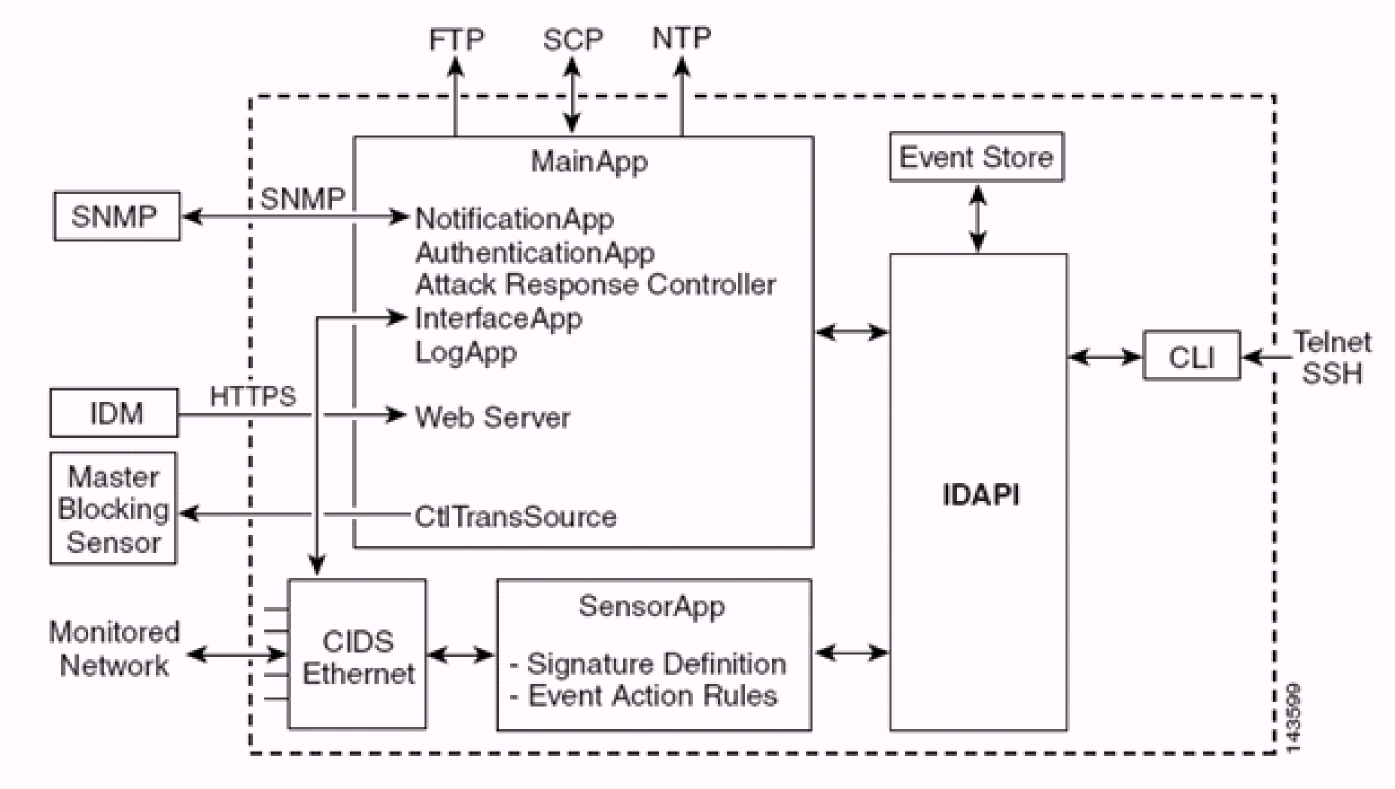
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

Cisco IDS概觀

Cisco IDS（5.0版）的主要元件包括：

- **Sensor App** — 執行資料包捕獲和分析。
- **Event Storage Management and Actions Module** — 提供策略違規的儲存。
- **映像、安裝和啟動模組** — 載入、初始化並啟動所有系統軟體。
- **使用者介面和UI支援模**塊 — 提供嵌入式CLI和IDM。
- **感測器操**作系統 — 主機作業系統（基於Linux）。



感測器應用（IPS軟體）包括：

- **主應用** — 初始化系統、啟動和停止其他應用程式、配置作業系統並負責升級。它包含以下元件：**Control Transaction Server** — 允許感測器傳送用於啟用攻擊響應控制器（以前稱為網路訪問控制器）主阻止感測器功能的控制事務。**Event Store** — 一個索引儲存，用於儲存可通過CLI、IDM、自適應安全裝置管理器(ASDM)或遠端資料交換協定(RDEP)訪問的IPS事件（錯誤、狀態和警報系統消息）。
- **Interface App** — 處理旁路和物理設定並定義配對介面。物理設定包括速度、雙工和管理狀態。
- **Log App** — 將應用程式的日誌消息寫入日誌檔案，將錯誤消息寫入事件儲存。
- **Attack Response Controller(ARC)（以前稱為網路訪問控制器）** — 管理遠端網路裝置（防火牆、路由器和交換機），在發生警報事件時提供阻止功能。ARC在受控網路裝置上建立並套用存取控制清單(ACL)或使用**shun**指令（防火牆）。
- **通知應**用 — 由警報、狀態和錯誤事件觸發時傳送SNMP陷阱。通知應用為此使用公共域SNMP代理。SNMP GET提供有關感測器健康狀態的資訊。**Web伺服器（HTTP RDEP2伺服器）** — 提供Web使用者介面。它還提供使用多個Servlet來提供IPS服務，通過RDEP2與其他IPS裝置通訊的方法。**Authentication App** — 驗證使用者是否有權執行CLI、IDM、ASDM或RDEP操作。
- **Sensor App(Analysis Engine)** — 執行資料包捕獲和分析。
- **CLI** — 使用者通過Telnet或SSH成功登入感測器時運行的介面。通過CLI建立的所有帳戶都使用CLI作為其外殼（服務帳戶除外 — 只允許使用一個服務帳戶）。 允許的CLI命令取決於使用者的許可權。

所有IPS應用通過稱為IDAPI的通用應用程式介面(API)相互通訊。遠端應用程式（其他感測器、管理應用程式和第三方軟體）通過RDEP2和安全裝置事件交換(SDEE)協定與感測器通訊。

必須注意的是，感測器具有以下磁碟分割槽：

- **Application Partition** — 包含完整的IPS系統映像。
- **維護分**區 — 用於重新映像IDSM-2的應用程式分割槽的特殊用途IPS映像。重新映像維護分割槽會導致配置設定丟失。

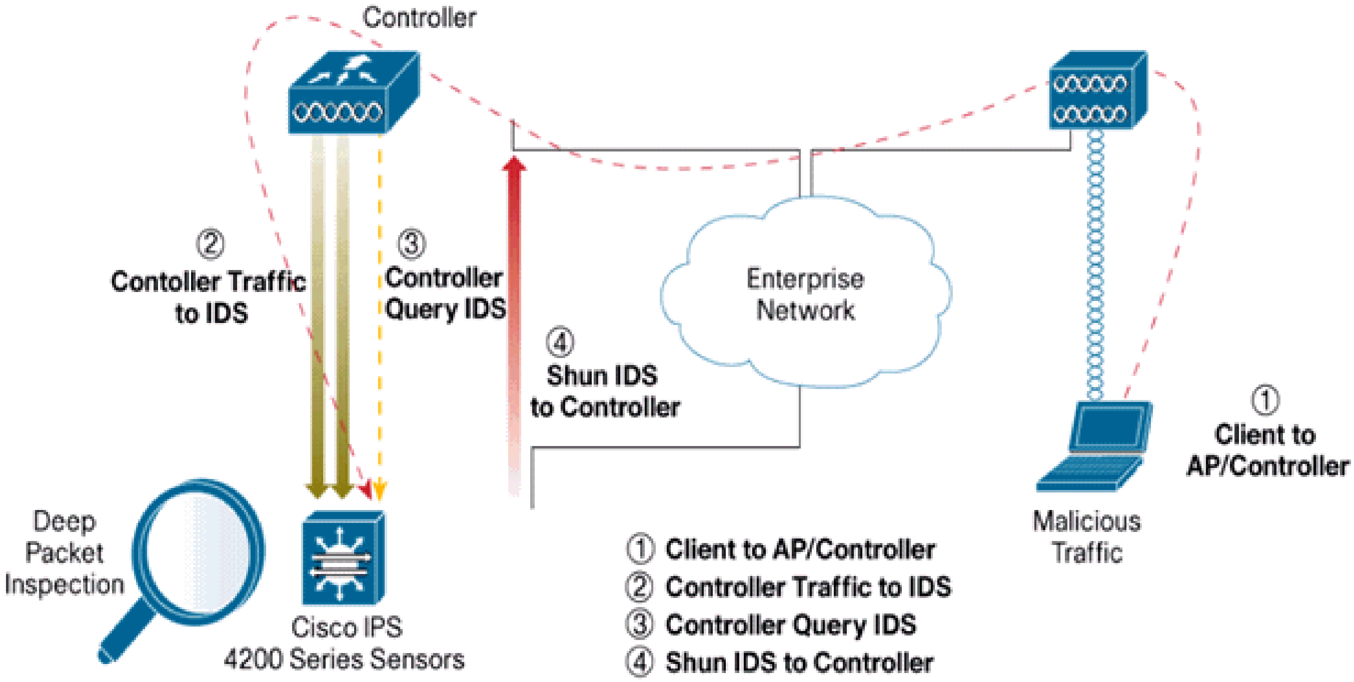
- **恢復分**區 — 用於恢復感測器的特殊用途映像。引導至恢復分割槽使使用者能夠完全重新映像應用程式分割槽。網路設定被保留，但所有其它配置都將丟失。

Cisco IDS和WLC — 整合概觀

Cisco IDS版本5.0引入了在檢測到違反策略（簽名）時配置拒絕操作的功能。根據IDS/IPS系統上的使用者組態，可以將shun要求傳送到防火牆、路由器或WLC，以阻擋來自特定IP位址的封包。

使用適用於思科無線控制器的思科整合無線網路軟體版本4.0時，需要向WLC傳送shun要求，才能觸發控制器上可用的使用者端黑名單或排除行為。控制器用來取得shun要求的介面是Cisco IDS上的指令和控制介面。

- 控制器允許在給定控制器上配置最多五個IDS感測器。
- 每個配置的IDS感測器由其IP地址或合格的網路名稱和授權憑證標識。
- 可以在控制器上配置每個IDS感測器，其唯一查詢速率以秒為單位。



IDS迴避

控制器以配置的查詢速率查詢感測器，以便檢索所有shun事件。給定的shun請求分佈在整個控制器的移動組中從IDS感測器檢索請求。客戶端IP地址的每個shun請求對指定的超時秒值有效。如果超時值指示無限時間，則只有在IDS上刪除shun條目時，shun事件才會結束。即使移動組中的任何或全部控制器被重置，迴避客戶端狀態仍會在每個控制器上保留。

注意：避開客戶端的決策始終由IDS感測器決定。控制器未檢測到第3層攻擊。判斷使用者端是否在第3層發動惡意攻擊是一個複雜得多的過程。使用者端在第2層進行驗證，這足以讓控制器授予第2層存取許可權。

注意：例如，如果客戶端獲得分配的上一個違規（迴避）IP地址，則直到感測器超時，才能取消阻止此新客戶端的第2層訪問。即使控制器在第2層提供訪問許可權，客戶端通訊量仍可能在第3層路由器上被阻止，因為感測器也會將迴避事件通知路由器。

假設客戶端具有IP地址A。現在，當控制器輪詢Shun事件的IDS時，IDS會將Shun請求傳送到控制器，並將IP地址A作為目標IP地址。現在，控制器黑名單中列出了此客戶端A。在控制器上，基於MAC地址禁用了客戶端。

現在，假設使用者端將其IP位址從A變更為B。在下一次輪詢期間，控制器會根據IP位址獲得一個迴避使用者端的清單。這一次，IP地址A仍然位於迴避清單中。但是由於使用者端已將其IP位址從A變更為B（不在IP位址的避免清單中），因此一旦控制器上達到黑名單使用者端的逾時，就會釋放具有新IP位址B的使用者端。現在，控制器開始允許此客戶端使用新的IP地址B（但客戶端MAC地址保持不變）。

因此，雖然客戶端在控制器排除時間期間保持禁用狀態，並且如果重新獲取其以前的DHCP地址則會重新排除該客戶端，但如果被迴避的客戶端的IP地址發生更改，該客戶端將不再被禁用。例如，如果客戶端連線到同一網路，並且DHCP租用超時未過期。

控制器僅支援連線到IDS，以便客戶端迴避使用控制器上的管理埠的請求。控制器通過傳輸無線客戶端流量的相應VLAN介面連線到IDS以進行資料包檢測。

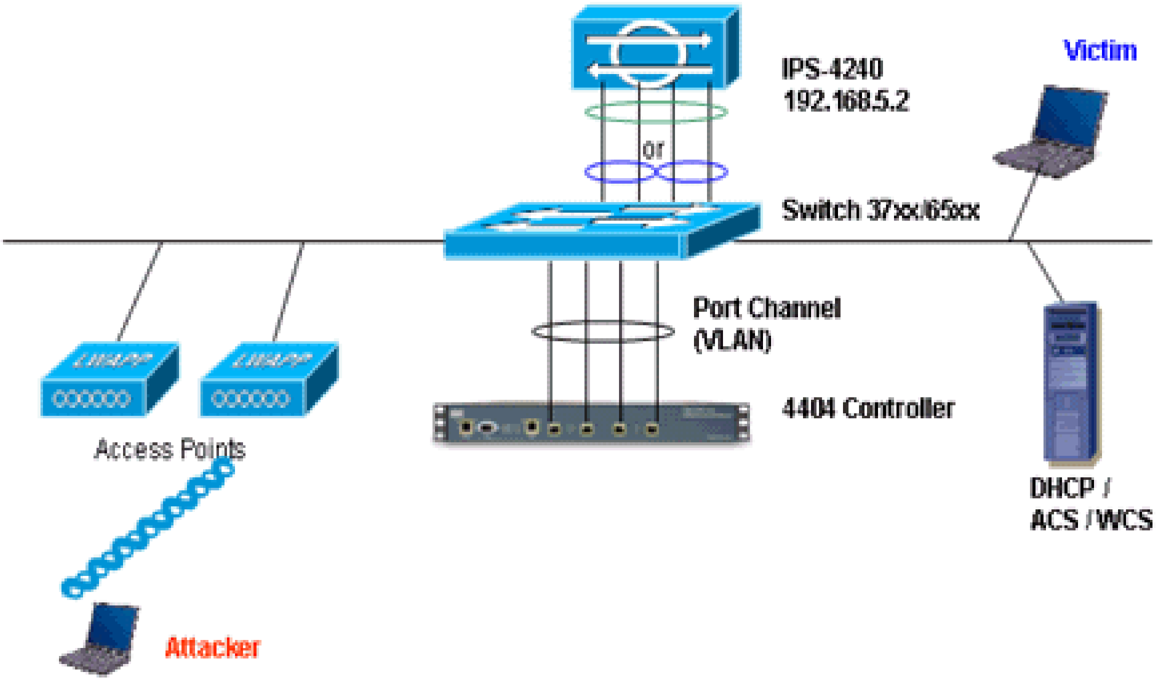
在控制器上，Disable Clients頁面顯示已通過IDS感測器請求禁用的每個客戶端。CLI **show**命令也會顯示已列入黑名單的客戶端的清單。

在WCS上，排除的客戶端顯示在Security子頁籤下。

以下是完成Cisco IPS感測器和Cisco WLC的整合需遵循的步驟。

1. 在無線控制器所在的交換機上安裝和連線IDS裝置。
2. 將承載無線使用者端流量的WLC連線埠映象(SPAN)到IDS裝置。
3. IDS裝置收到每個資料包的副本，並檢查第3層至第7層的流量。
4. IDS裝置提供可下載的簽名檔案，也可進行自定義。
5. 當檢測到攻擊特徵碼時，IDS裝置會生成事件操作shun的警報。
6. WLC輪詢IDS以查詢警報。
7. 當偵測到與WLC相關聯的無線使用者端的IP位址的警報時，會將使用者端列入排除清單。
8. 陷阱由WLC生成並通知WCS。
9. 在指定的時間段之後，使用者將從排除清單中刪除。

網路架構設計



Cisco WLC連線到Catalyst 6500上的gigabit介面。為gigabit介面建立連線埠通道，並在WLC上啟用連結彙總(LAG)。

```
(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
```

控制器已連線到Catalyst 6500上的gigabit 5/1和gigabit 5/2介面。

```
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感測器的檢測介面可以在**混雜模式**下單獨運行，也可以將它們配對，為內聯檢測模式創**建內聯介面**。

在混雜模式下，資料包不會流經感測器。感測器分析受監控流量的副本，而不是實際轉發的資料包。在混雜模式下運行的優勢在於感測器不會影響轉發通訊量的資料包流。

註：架構圖只是WLC和IPS整合架構的示例設定。此處顯示的示例配置說明了IDS感應介面在混雜模式下工作。架構圖表顯示配對在一起的感應介面，以在內嵌配對模式下運作。有關內嵌介面模式的詳細資訊，請參閱內嵌模式。

在此配置中，假設感測介面以混雜模式工作。Cisco IDS感應器的監控介面連線到Catalyst 6500上的gigabit介面5/3。在Catalyst 6500上建立一個監控作業階段，其中連線埠通道介面是封包的來源，目的地是連線到Cisco IPS感應器的監控介面的gigabit介面。這會將控制器有線介面的所有入口和出口流量複製到IDS，以便進行第3層到第7層檢查。

```
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#
```

配置Cisco IDS感測器

Cisco IDS感測器的初始配置是通過控制檯埠或通過將顯示器和鍵盤連線到感測器來完成的。

1. 登入裝置：將控制檯埠連線到感測器。將顯示器和鍵盤連線到感測器。
2. 在登入提示符下鍵入使用者名稱和密碼。**注意：**預設使用者名稱和密碼均為cisco。首次登入裝置時，系統會提示您更改它們。您必須首先輸入UNIX密碼，即cisco。然後必須輸入新密碼兩次。

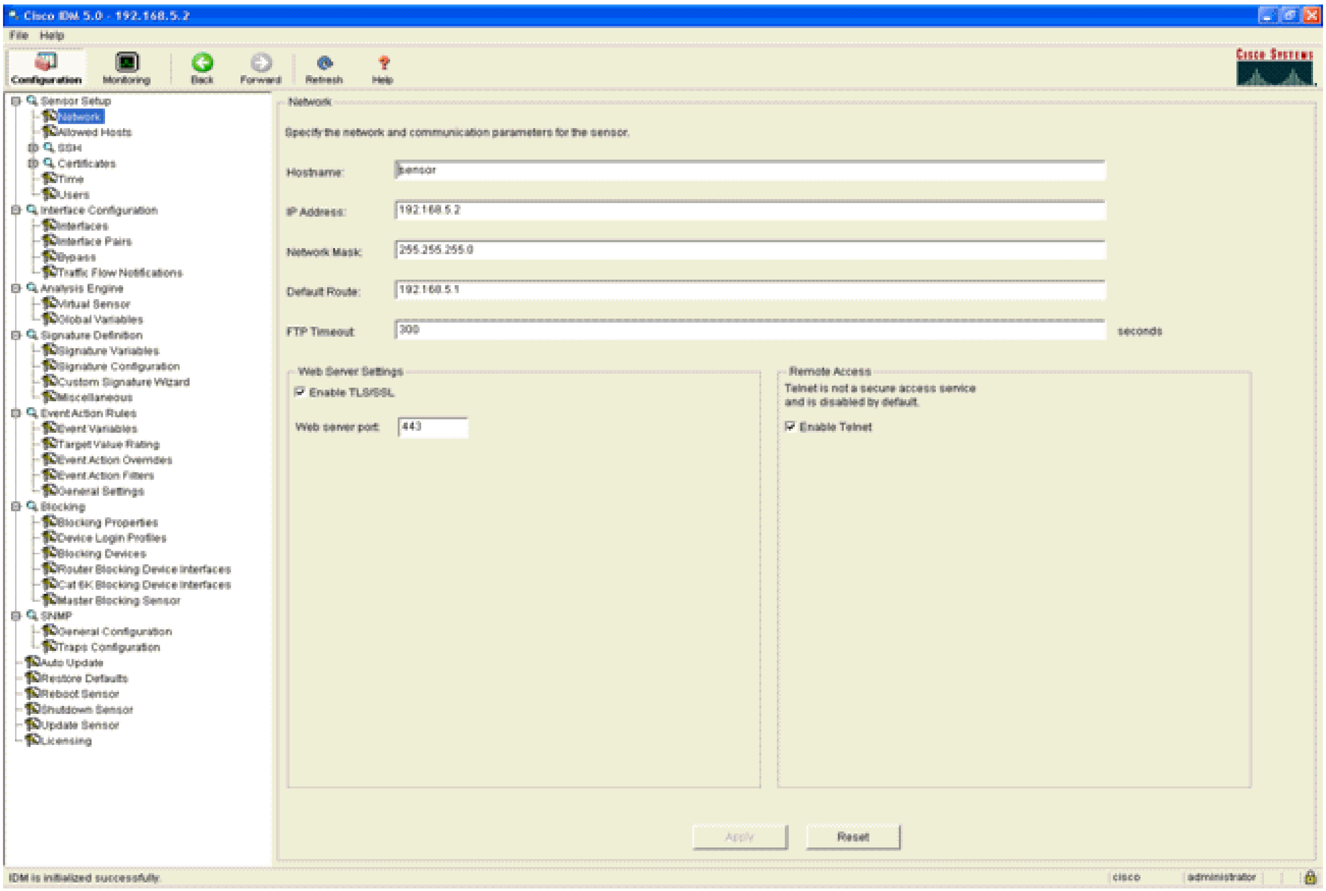
   ```
   login: cisco
   Password:
   ```

```
***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. 配置感測器上的IP地址、子網掩碼和訪問清單。**注意：**這是IDS上用於與控制器通訊的命令和控制介面。此位址應可路由到控制器管理介面。感應介面不需要定址。存取清單應包括控制器管理介面位址，以及管理IDS的允許位址。

   ```
   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. 現在，您可以通過GUI配置IPS感測器。將瀏覽器指向感測器的管理IP地址。此圖顯示一個示例，其中感測器配置了192.168.5.2。



Network

Specify the network and communication parameters for the sensor.

Hostname: sensor

IP Address: 192.168.5.2

Network Mask: 255.255.255.0

Default Route: 192.168.5.1

FTP Timeout: 300 seconds

Web Server Settings

☑ Enable TLS/SSL

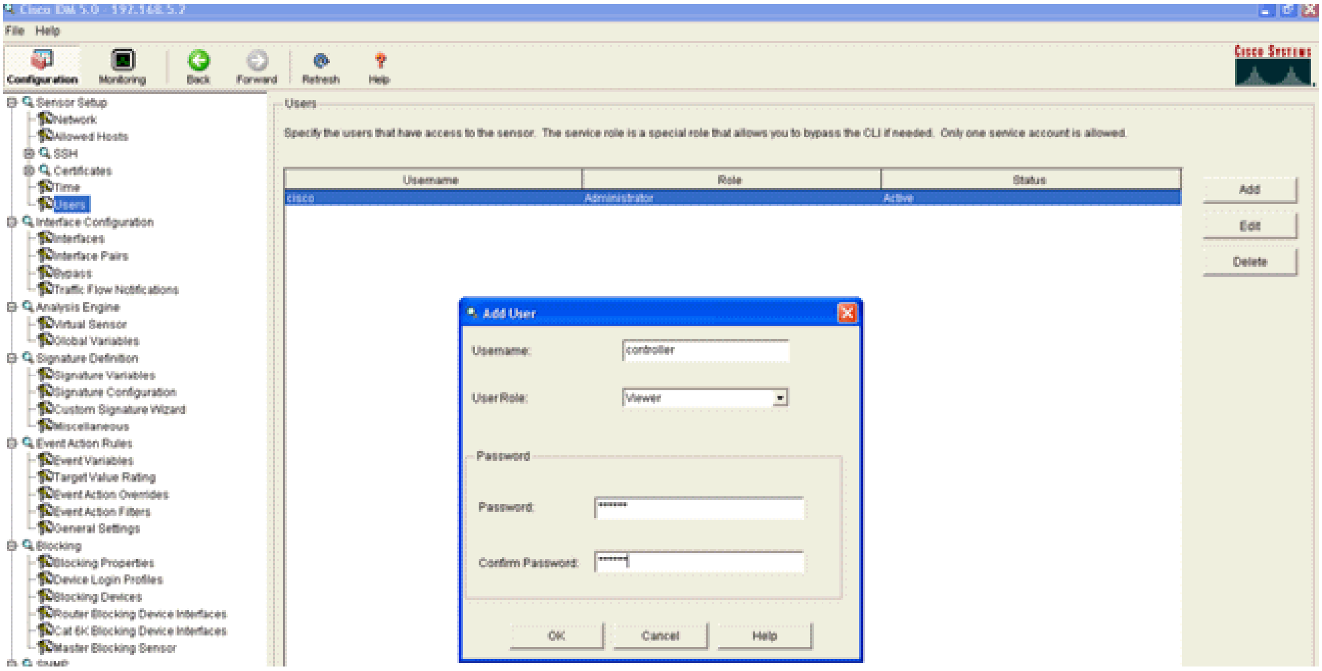
Web server port: 443

Remote Access

Telnet is not a secure access service and is disabled by default.

☑ Enable Telnet

5. 新增WLC用於訪問IPS感測器事件的使用者。



Users

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
cisco	Administrator	Active

Add User

Username: controller

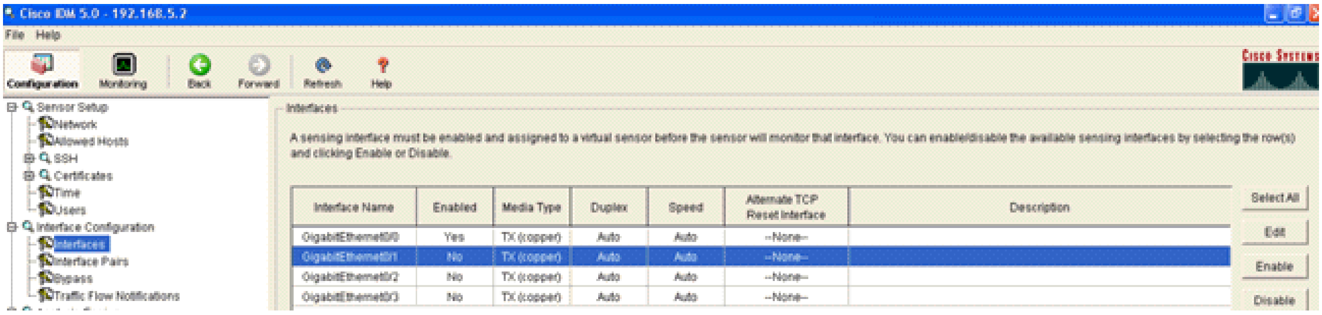
User Role: Viewer

Password

Password: *******

Confirm Password: *******

6. 啟用監控介面。



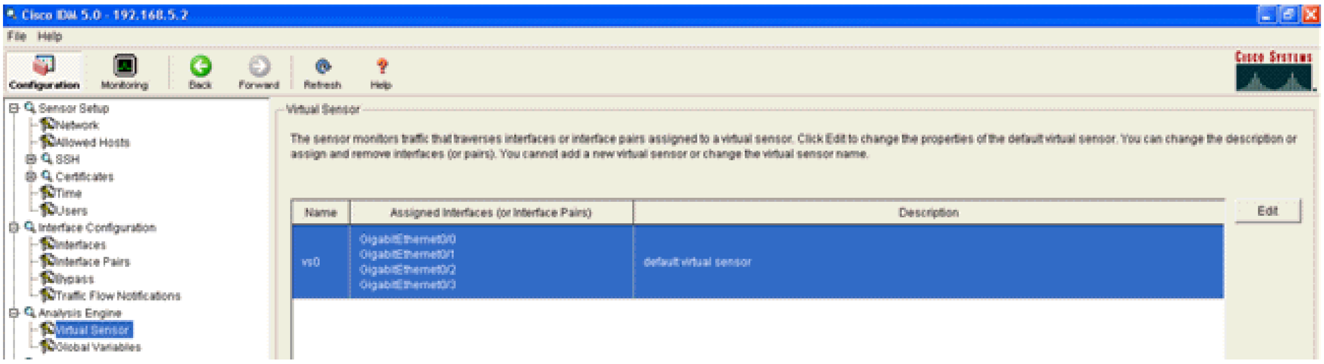
Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Media Type	Duplex	Speed	Alternate TCP Reset Interface	Description
GigabitEthernet0/0	Yes	TX (copper)	Auto	Auto	--None--	
GigabitEthernet0/1	No	TX (copper)	Auto	Auto	--None--	
GigabitEthernet0/2	No	TX (copper)	Auto	Auto	--None--	
GigabitEthernet0/3	No	TX (copper)	Auto	Auto	--None--	

必須將監控介面新增到分析引擎，如以下視窗所示

:

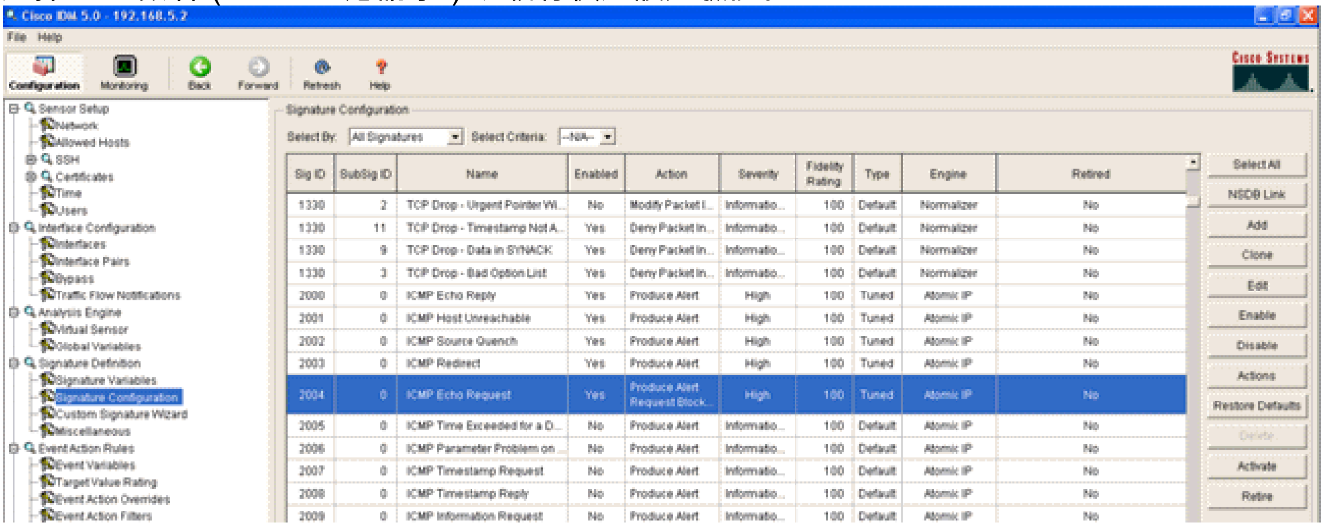


Virtual Sensor

The sensor monitors traffic that traverses interfaces or interface pairs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the description or assign and remove interfaces (or pairs). You cannot add a new virtual sensor or change the virtual sensor name.

Name	Assigned Interfaces (or Interface Pairs)	Description
vs0	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	default virtual sensor

7. 選擇2004簽名（ICMP回應請求）以執行快速設定驗證。

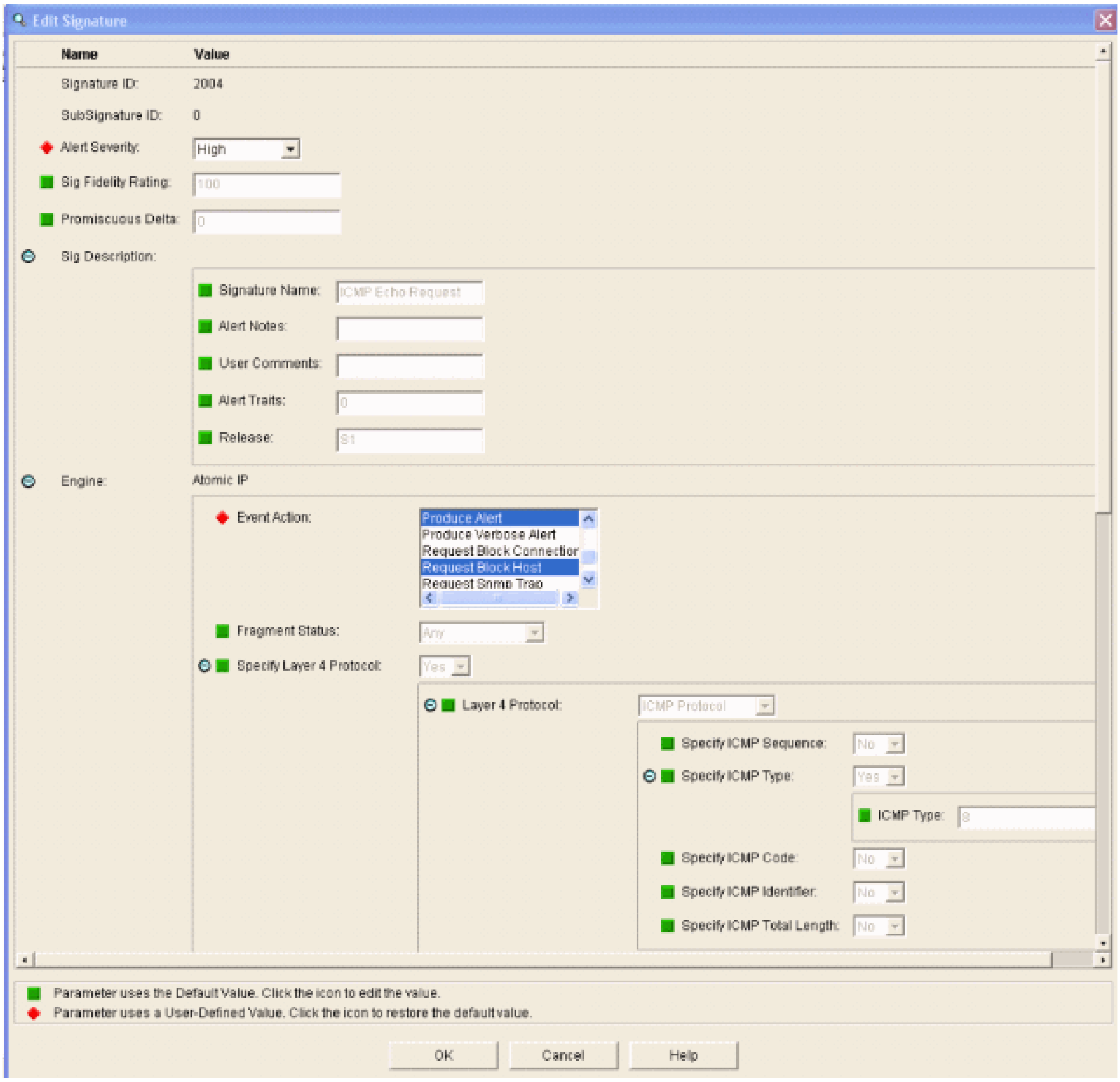


Signature Configuration

Select By: All Signatures Select Criteria: --N/A--

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired
1330	2	TCP Drop - Urgent Pointer Wi...	No	Modify Packet I...	Informatio...	100	Default	Normalizer	No
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informatio...	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	Informatio...	100	Default	Atomic IP	No
2006	0	ICMP Parameter Problem on ...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2009	0	ICMP Information Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No

在完成此驗證步驟時，應啟用特徵碼，將警報嚴重性設定為**High**，將事件操作設定為**Produce Alert**和**Request Block Host**。



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

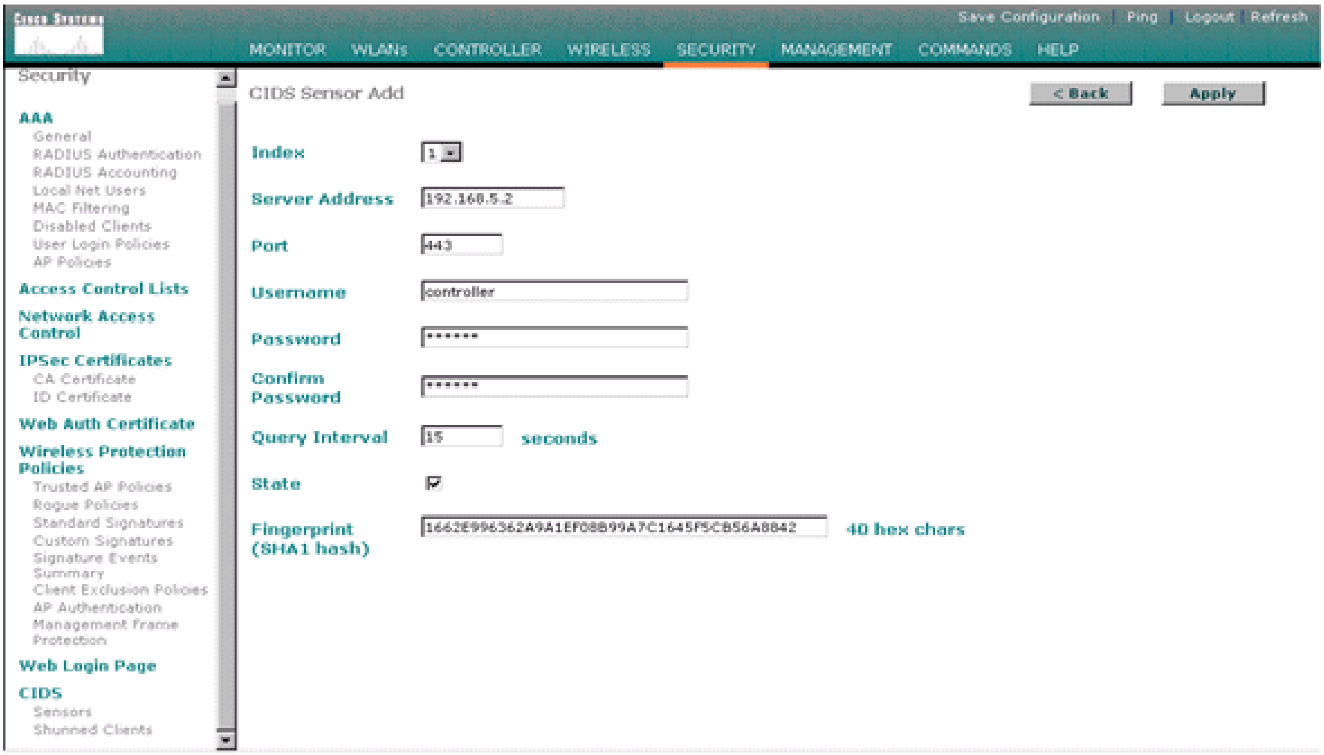
🟩 Parameter uses the Default Value. Click the icon to edit the value.
◆ Parameter uses a User-Defined Value. Click the icon to restore the default value.

設定WLC

完成以下步驟即可設定WLC:

1. 配置好IPS裝置並準備將其新增到控制器後，請選擇**Security > CIDS > Sensors > New**。
2. 新增之前建立的IP地址、TCP埠號、使用者名稱和密碼。為了從IPS感測器獲取指紋，請在IPS感測器中執行此命令，然後在WLC上新增SHA1指紋（不帶冒號）。 這用於保護控制器到IDS的輪詢通訊。

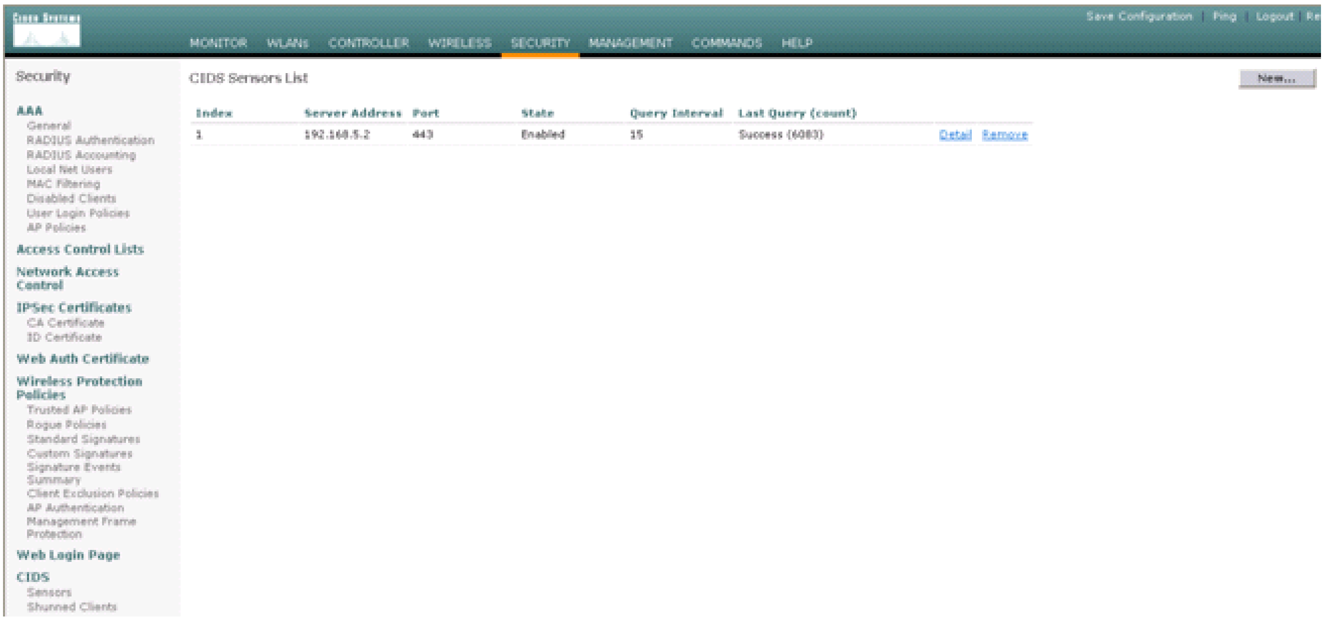
```
sensor#show tls fingerprint
MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19
SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42
```



CIDS Sensor Add

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

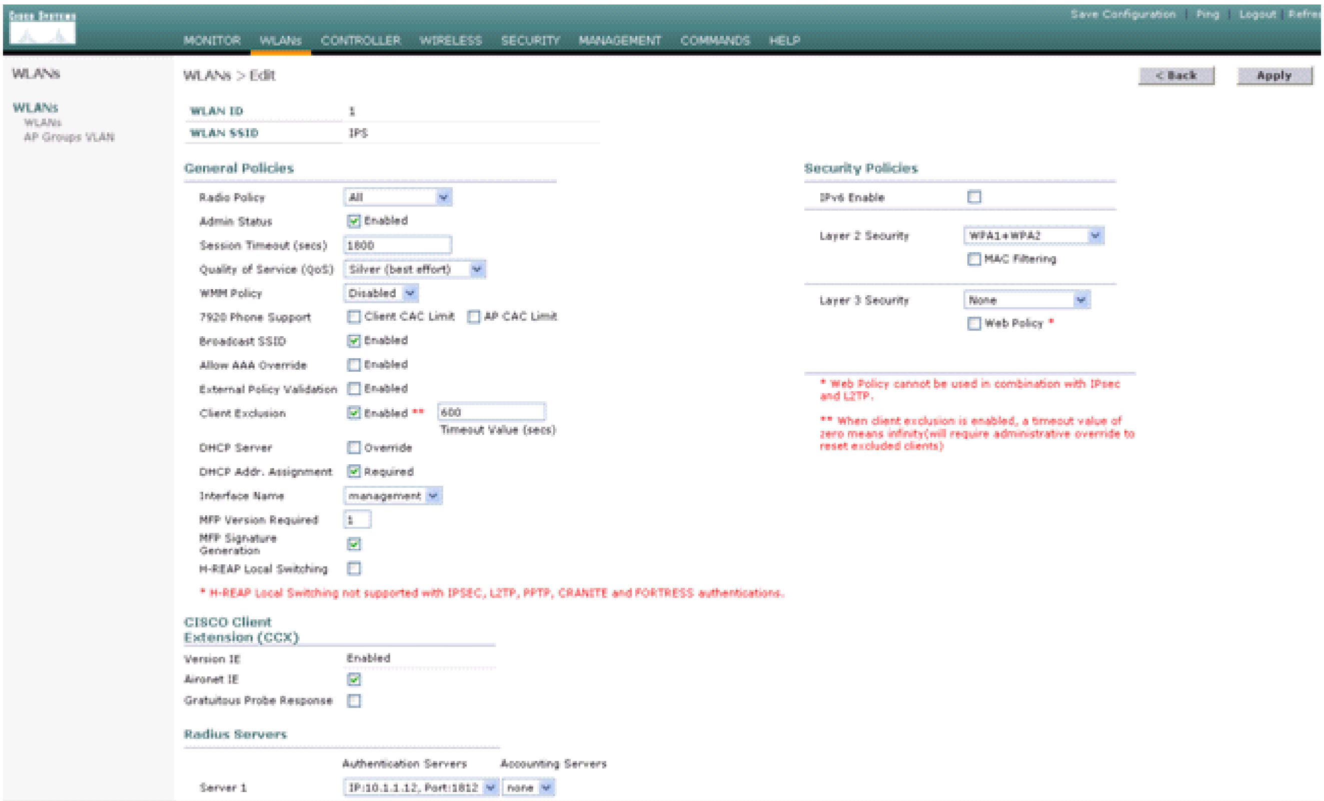
3. 檢查IPS感測器和WLC之間的連線狀態。



CIDS Sensors List

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

4. 建立與Cisco IPS感測器的連線後，請確保WLAN配置正確並且啟用**Client Exclusion**。預設客戶端排除超時值為60秒。另請注意，無論客戶端排除計時器如何，只要IDS呼叫的客戶端塊保持活動狀態，客戶端排除就會繼續存在。IDS中的預設阻止時間為30分鐘。



WLANs > Edit

WLAN ID 1
WLAN SSID IPS

General Policies

Radio Policy All
Admin Status ☑ Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support □ Client CAC Limit □ AP CAC Limit
Broadcast SSID ☑ Enabled
Allow AAA Override □ Enabled
External Policy Validation □ Enabled
Client Exclusion ☑ Enabled ** 600 Timeout Value (secs)
DHCP Server □ Override
DHCP Addr. Assignment ☑ Required
Interface Name management
MFP Version Required 1
MFP Signature Generation ☑
H-REAP Local Switching □

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

CISCO Client Extension (CCX)

Version IE Enabled
Aironet IE ☑
Gratuitous Probe Response □

Radius Servers

Authentication Servers Accounting Servers
Server 1 IP:10.1.1.12, Port:1812 none

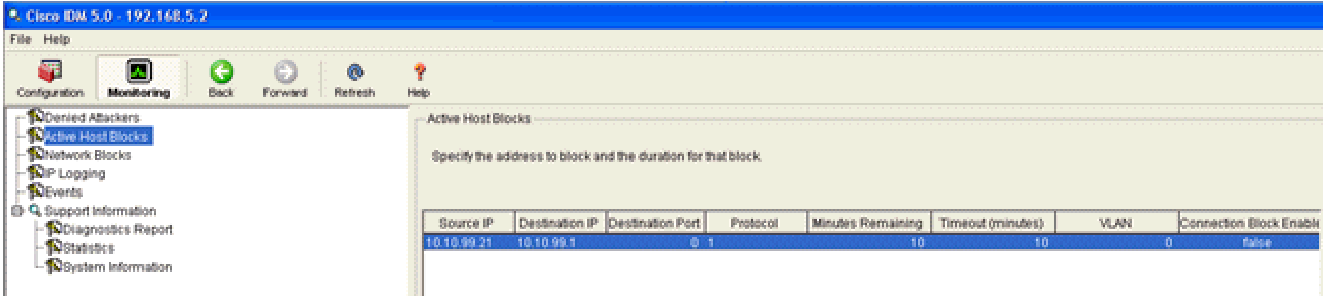
Security Policies

IPv6 Enable □
Layer 2 Security WPA1+WPA2
□ MAC Filtering
Layer 3 Security None
□ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

5. 當您對網路中的某些裝置執行NMAP掃描時，或者當您對Cisco IPS感測器監控的某些主機執行ping操作時，都可以觸發Cisco IPS系統中的事件。在Cisco IPS中觸發警報後，請轉到**Monitoring and Active Host Blocks**以檢查有關主機的詳細資訊。

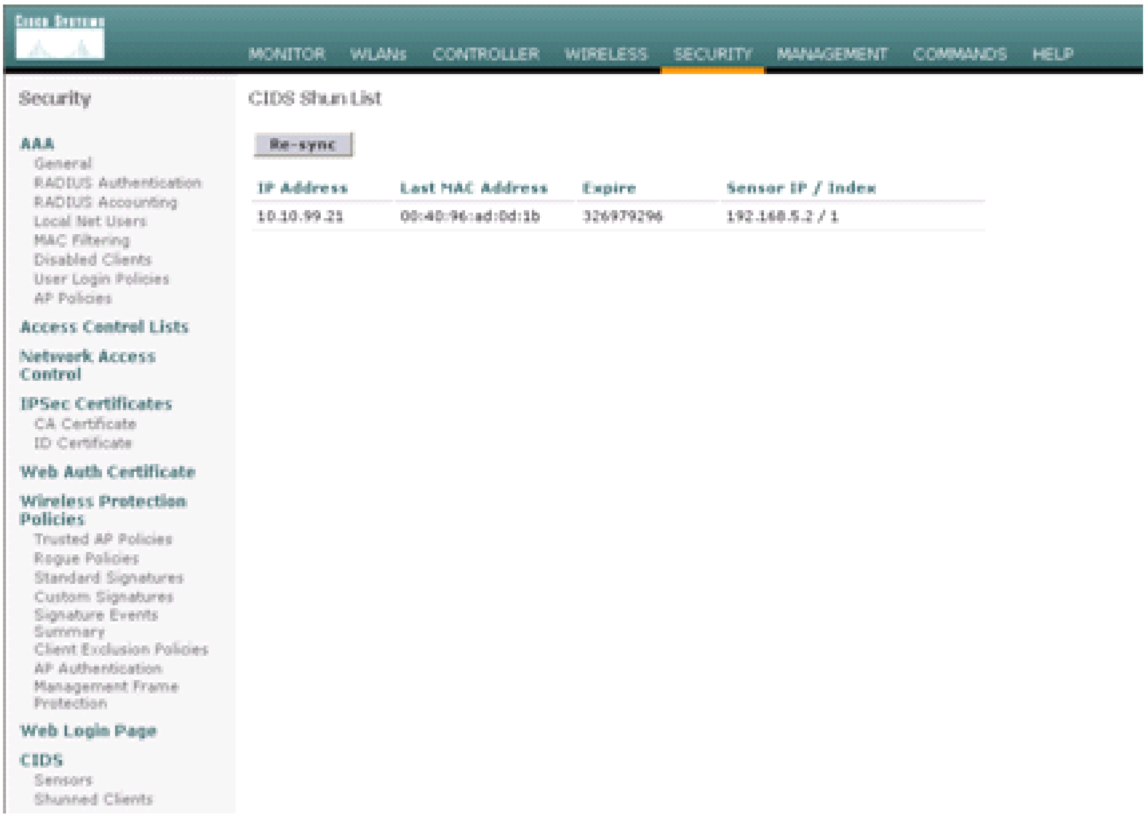


Active Host Blocks

Specify the address to block and the duration for that block.

Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	VLAN	Connection Block Enable
10.10.99.21	10.10.99.1	0	1	10	10	0	false

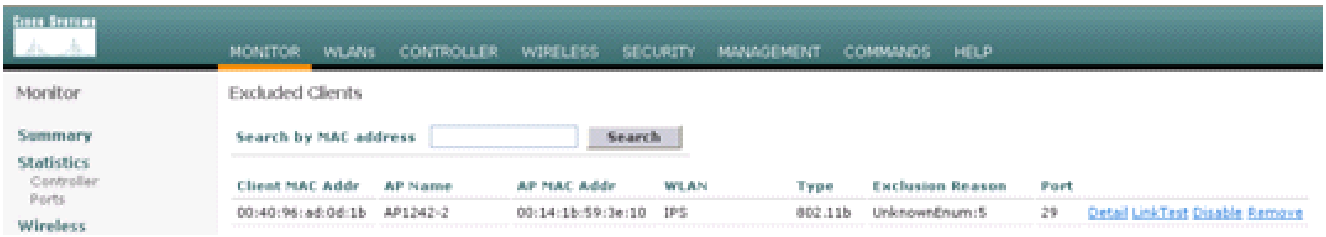
控制器中的「迴避客戶端」清單現在會填充主機的IP和MAC地址。



CIDS Shun List

IP Address	Last MAC Address	Expire	Sensor IP / Index
10.10.99.21	00:40:96:ad:0d:1b	326979296	192.168.5.2 / 1

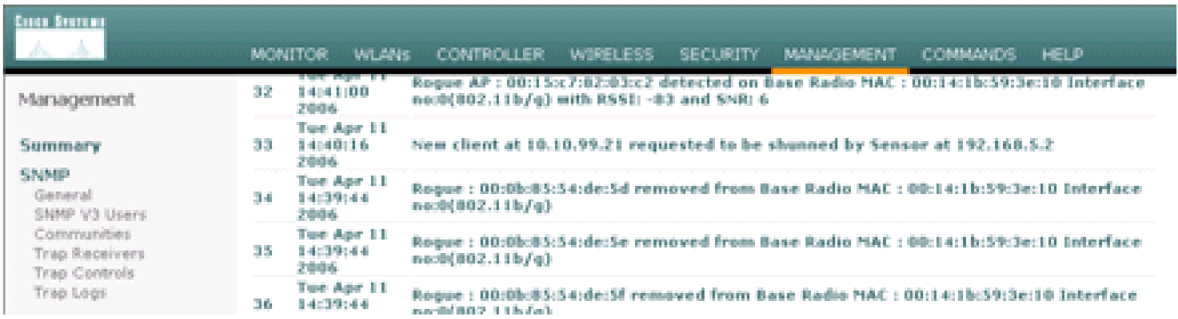
該使用者將被新增到「客戶端排除」清單中。



Excluded Clients

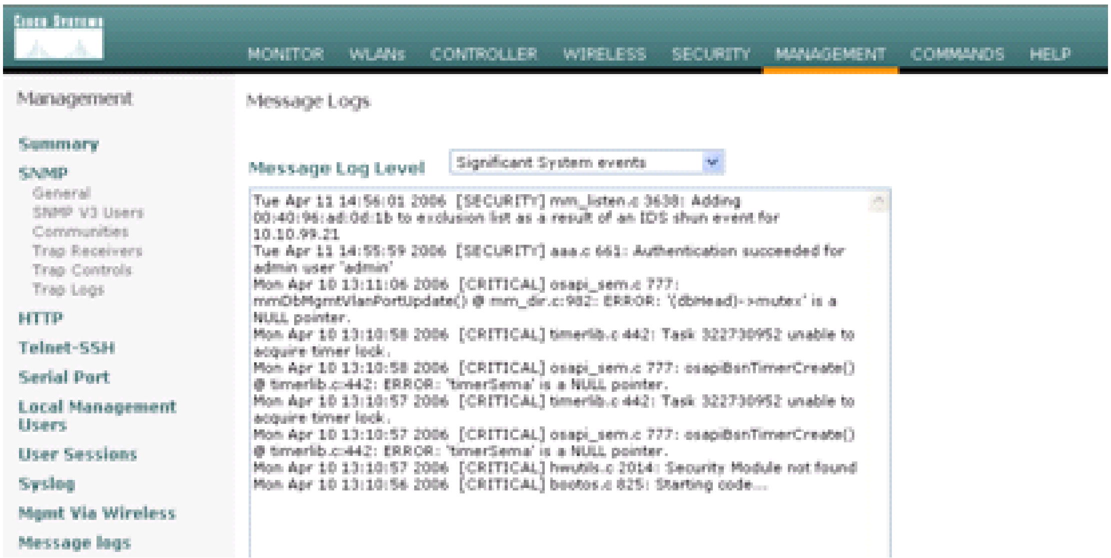
Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Exclusion Reason	Port	
00:40:96:ad:0d:1b	AP1242-2	00:14:1b:59:3e:10	IPS	802.11b	UnknownEnum:5	29	Detail LinkTest Disable Remove

在將客戶端新增到規避清單中時，生成陷阱日誌。



32	Tue Apr 11 14:41:00 2006	Rogue AP : 00:15:c7:82:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g) with RSSI: -83 and SNR: 6
33	Tue Apr 11 14:40:16 2006	New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2
34	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
35	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:5e removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
36	Tue Apr 11 14:39:44	Rogue : 00:0b:85:54:de:5f removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)

還將為事件生成消息日誌。

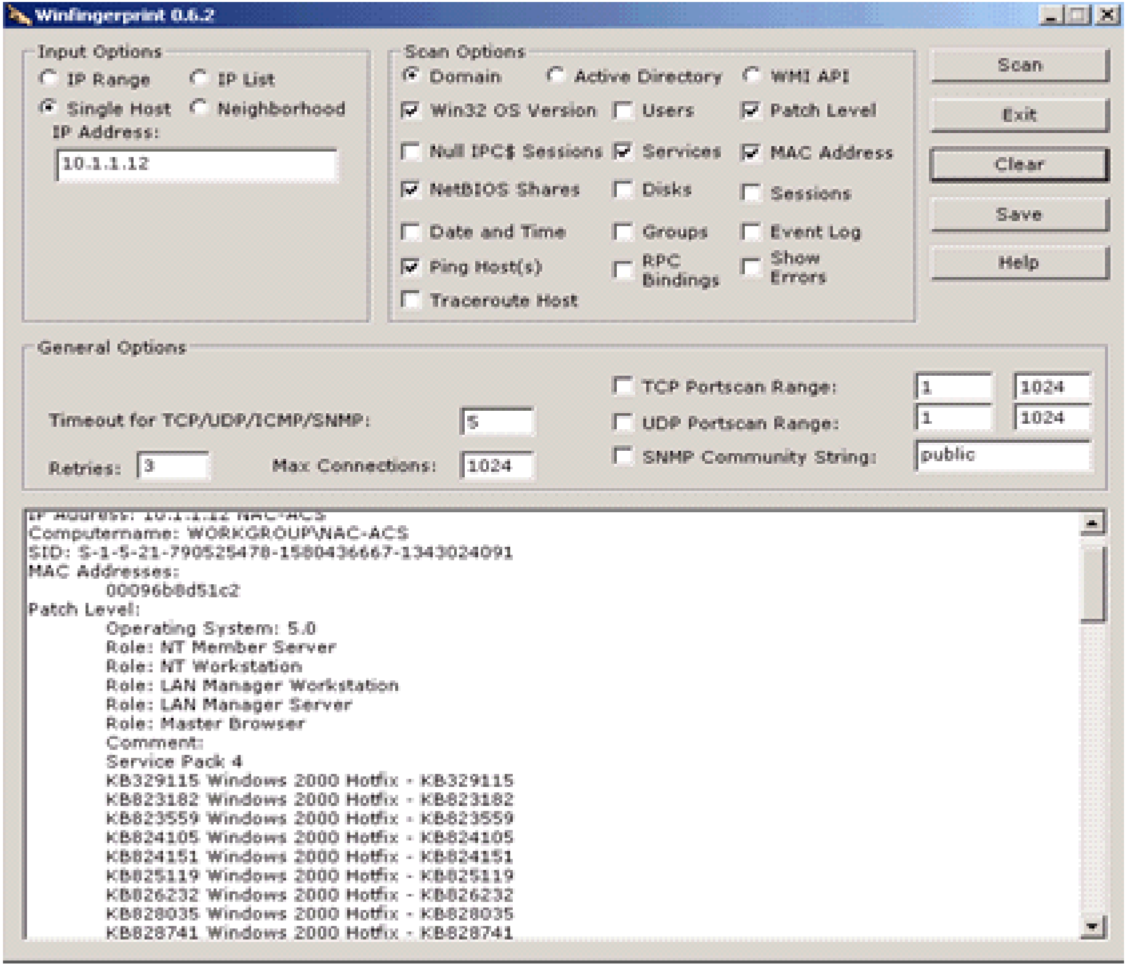


Message Logs

Message Log Level: Significant System events

```
Tue Apr 11 14:56:01 2006  [SECURITY] mm_listen.c 3638: Adding
00:40:96:ad:0d:1b to exclusion list as a result of an IDS shun event for
10.10.99.21
Tue Apr 11 14:55:59 2006  [SECURITY] aaa.c 661: Authentication succeeded for
admin user 'admin'
Mon Apr 10 13:11:06 2006  [CRITICAL] osapi_sem.c 777:
mmDbMgmtVlanPortUpdate() @ mm_dir.c:982: ERROR: '(dbHead)->mutex' is a
NULL pointer.
Mon Apr 10 13:10:58 2006  [CRITICAL] timerlib.c 442: Task 322730952 unable to
acquire timer lock.
Mon Apr 10 13:10:58 2006  [CRITICAL] osapi_sem.c 777: osapiBsnTimerCreate()
@ timerlib.c:442: ERROR: 'timerSema' is a NULL pointer.
Mon Apr 10 13:10:57 2006  [CRITICAL] timerlib.c 442: Task 322730952 unable to
acquire timer lock.
Mon Apr 10 13:10:57 2006  [CRITICAL] osapi_sem.c 777: osapiBsnTimerCreate()
@ timerlib.c:442: ERROR: 'timerSema' is a NULL pointer.
Mon Apr 10 13:10:57 2006  [CRITICAL] hwutils.c 2014: Security Module not found
Mon Apr 10 13:10:56 2006  [CRITICAL] bootos.c 825: Starting code...
```

當NMAP掃描在其監控的裝置上完成時，Cisco IPS感測器中會生成一些其他事件。



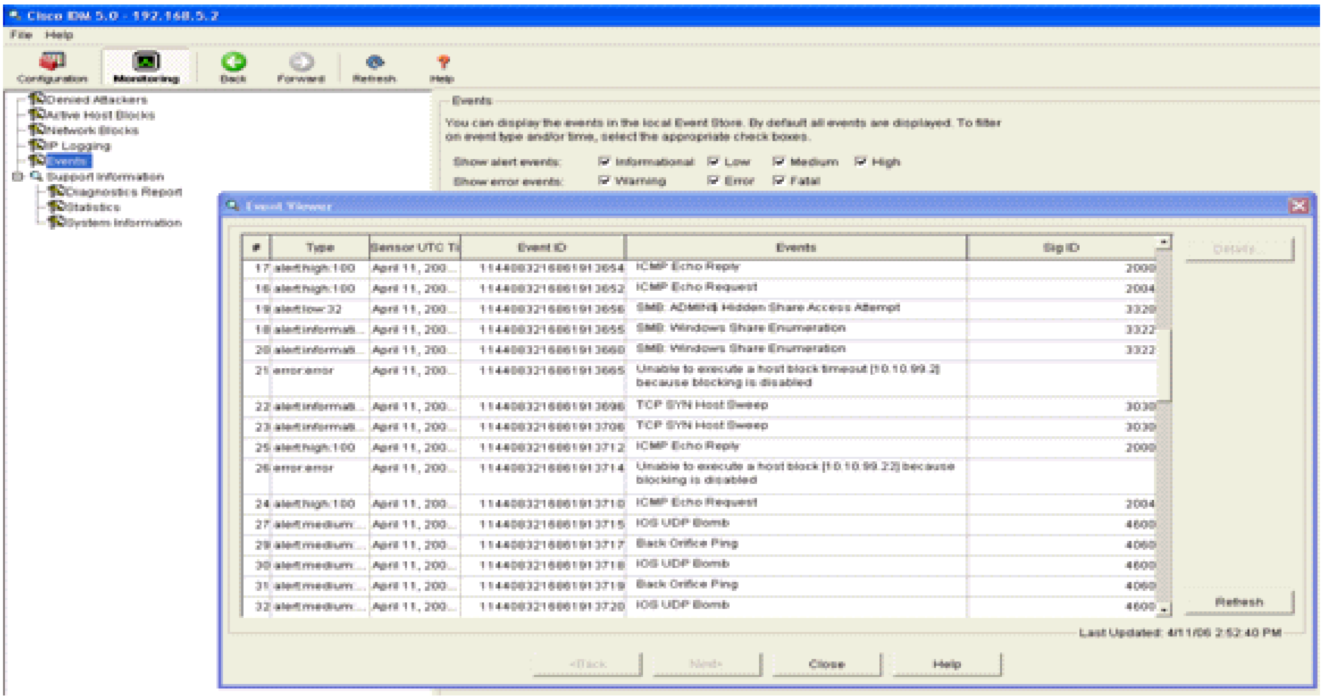
Input Options
○ IP Range ○ IP List
● Single Host ○ Neighborhood
IP Address: 10.1.1.12

Scan Options
● Domain ○ Active Directory ○ WMI API
☑ Win32 OS Version □ Users ☑ Patch Level
□ Null IPC$ Sessions ☑ Services ☑ MAC Address
☑ NetBIOS Shares □ Disks □ Sessions
□ Date and Time □ Groups □ Event Log
☑ Ping Host(s) □ RPC Bindings □ Show Errors
□ Traceroute Host

General Options
□ TCP Portscan Range: 1 1024
□ UDP Portscan Range: 1 1024
Timeout for TCP/UDP/ICMP/SNMP: 5
□ SNMP Community String: public
Retries: 3 Max Connections: 1024

```
IP Address: 10.1.1.12 NAC-ACS
Computername: WORKGROUP\NAC-ACS
SID: S-1-5-21-790525478-1580436667-1343024091
MAC Addresses:
        00096b8d51c2
Patch Level:
        Operating System: 5.0
        Role: NT Member Server
        Role: NT Workstation
        Role: LAN Manager Workstation
        Role: LAN Manager Server
        Role: Master Browser
        Comment:
        Service Pack 4
        KB329115 Windows 2000 Hotfix - KB329115
        KB823182 Windows 2000 Hotfix - KB823182
        KB823559 Windows 2000 Hotfix - KB823559
        KB824105 Windows 2000 Hotfix - KB824105
        KB824151 Windows 2000 Hotfix - KB824151
        KB825119 Windows 2000 Hotfix - KB825119
        KB826232 Windows 2000 Hotfix - KB826232
        KB828035 Windows 2000 Hotfix - KB828035
        KB828741 Windows 2000 Hotfix - KB828741
```

此視窗顯示Cisco IPS感測器中生成的事件。



You can display the events in the local Event Store. By default all events are displayed. To filter on event type and/or time, select the appropriate check boxes.

Show alert events: ☑ Informational ☑ Low ☑ Medium ☑ High

Show error events: ☑ Warning ☑ Error ☑ Fatal

#	Type	Sensor UTC Ti	Event ID	Events	Sig ID
17	alert:high:100	April 11, 200...	1144083216861913654	ICMP Echo Reply	2000
16	alert:high:100	April 11, 200...	1144083216861913652	ICMP Echo Request	2004
19	alert:low:32	April 11, 200...	1144083216861913656	SMB: ADMIN$ Hidden Share Access Attempt	3320
18	alert:informati...	April 11, 200...	1144083216861913655	SMB: Windows Share Enumeration	3322
20	alert:informati...	April 11, 200...	1144083216861913660	SMB: Windows Share Enumeration	3322
21	error:error	April 11, 200...	1144083216861913665	Unable to execute a host block timeout [10.10.99.2] because blocking is disabled	
22	alert:informati...	April 11, 200...	1144083216861913698	TCP SYN Host Sweep	3030
23	alert:informati...	April 11, 200...	1144083216861913706	TCP SYN Host Sweep	3030
25	alert:high:100	April 11, 200...	1144083216861913712	ICMP Echo Reply	2000
26	error:error	April 11, 200...	1144083216861913714	Unable to execute a host block [10.10.99.22] because blocking is disabled	
24	alert:high:100	April 11, 200...	1144083216861913710	ICMP Echo Request	2004
27	alert:medium:...	April 11, 200...	1144083216861913715	IOS UDP Bomb	4600
29	alert:medium:...	April 11, 200...	1144083216861913717	Back Orifice Ping	4060
30	alert:medium:...	April 11, 200...	1144083216861913718	IOS UDP Bomb	4600
31	alert:medium:...	April 11, 200...	1144083216861913719	Back Orifice Ping	4060
32	alert:medium:...	April 11, 200...	1144083216861913720	IOS UDP Bomb	4600

Last Updated: 4/11/06 2:52:40 PM

Cisco IDS感測器示例配置

以下是安裝指令碼的輸出：

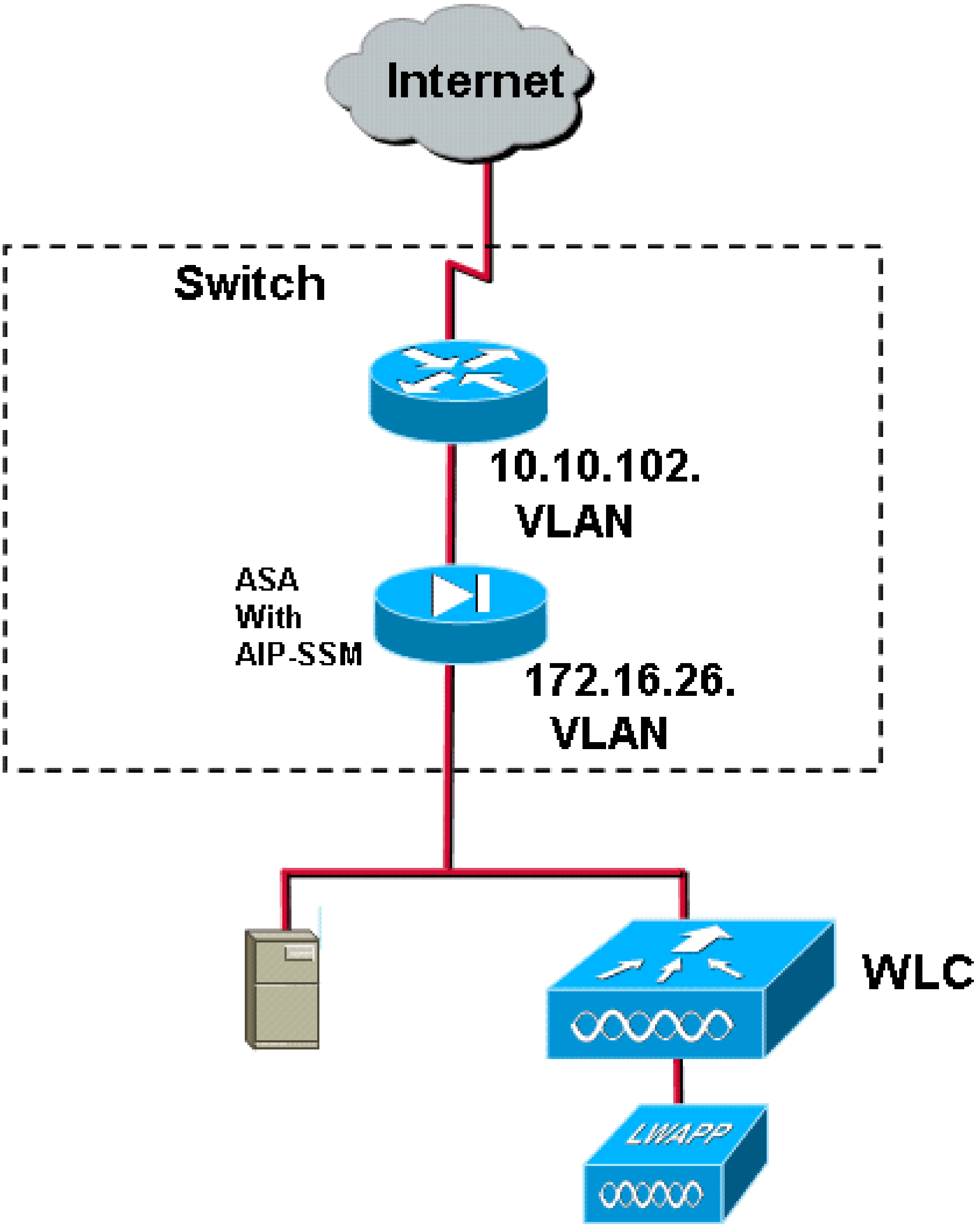
```
sensor#show config
! ------------------------------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------------------------------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list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

為IDS配置ASA

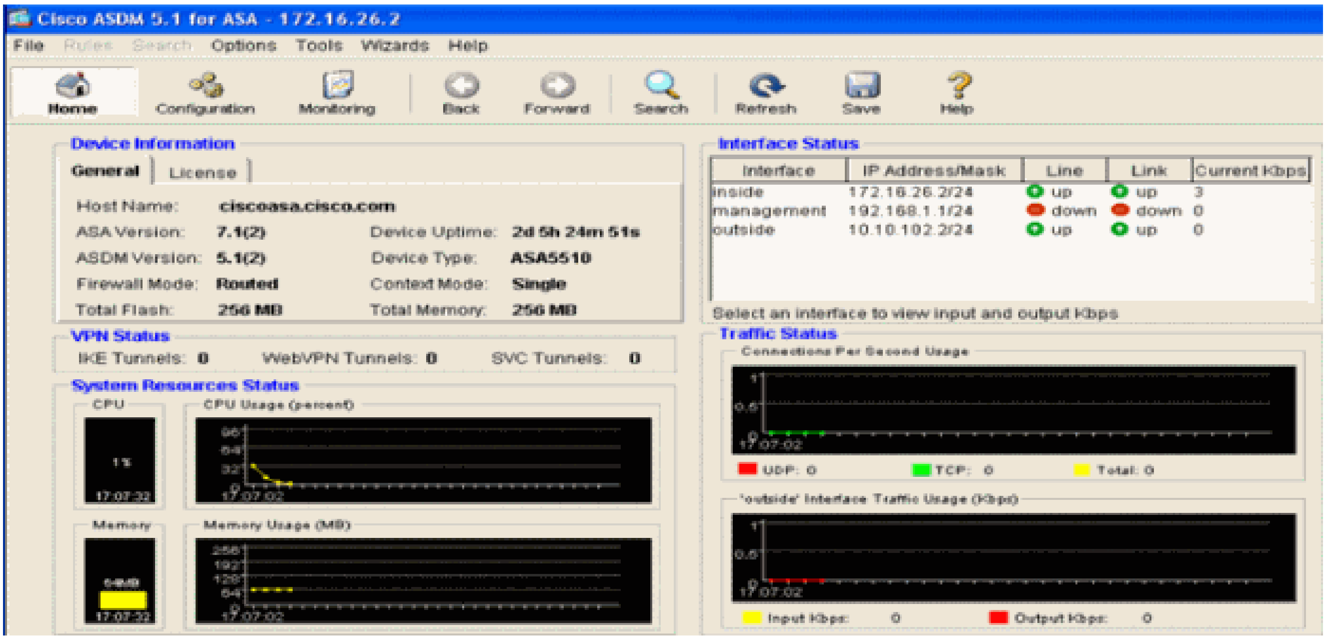
與傳統入侵檢測感測器不同，ASA必須始終位於資料路徑中。換句話說，ASA必須在一個介面上接收資料，進行內部處理，然後將其轉發到另一個埠，而不是將通訊量從交換機埠跨接到感測器上的

被動監聽埠。對於IDS，使用模組化策略框架(MPF)將ASA接收的流量複製到內部高級檢測和防禦安全服務模組(AIP-SSM)以進行檢測。



在此示例中，使用的ASA已經設定並傳遞流量。以下步驟演示如何建立將資料傳送到AIP-SSM的策略。

1. 使用ASDM登入到ASA。成功登入後，出現ASA主系統視窗。



Cisco ASDM 5.1 for ASA - 172.16.26.2
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Device Information
General License
VPN Status
System Resources Status
CPU
CPU Usage (percent)
Memory
Memory Usage (MB)
Interface Status
Traffic Status
Connections Per Second Usage
'outside' Interface Traffic Usage (Kbps)

Host Name: ciscoasa.cisco.com

ASA Version:	7.1(2)	Device Uptime:	2d 5h 24m 51s
ASDM Version:	5.1(2)	Device Type:	ASA5510
Firewall Mode:	Routed	Context Mode:	Single
Total Flash:	256 MB	Total Memory:	256 MB

IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0

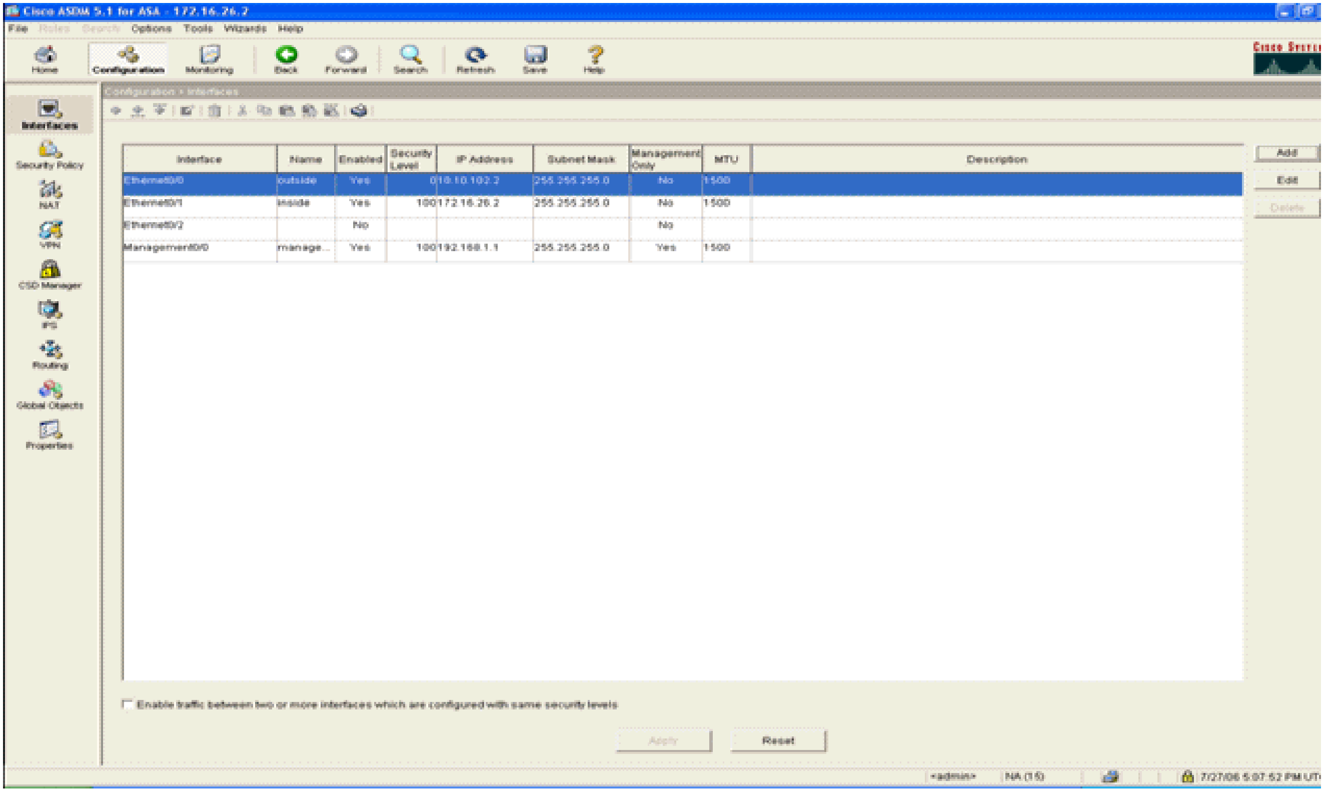
Interface	IP Address/Mask	Line	Link	Current Kbps
inside	172.16.26.2/24	● up	● up	3
management	192.168.1.1/24	● down	● down	0
outside	10.10.102.2/24	● up	● up	0

Select an interface to view input and output Kbps

🟥 UDP: 0 🟩 TCP: 0 🟨 Total: 0

🟨 Input Kbps: 0 🟥 Output Kbps: 0

2. 按一下頁面頂部的Configuration。該視窗切換到ASA介面的檢視。

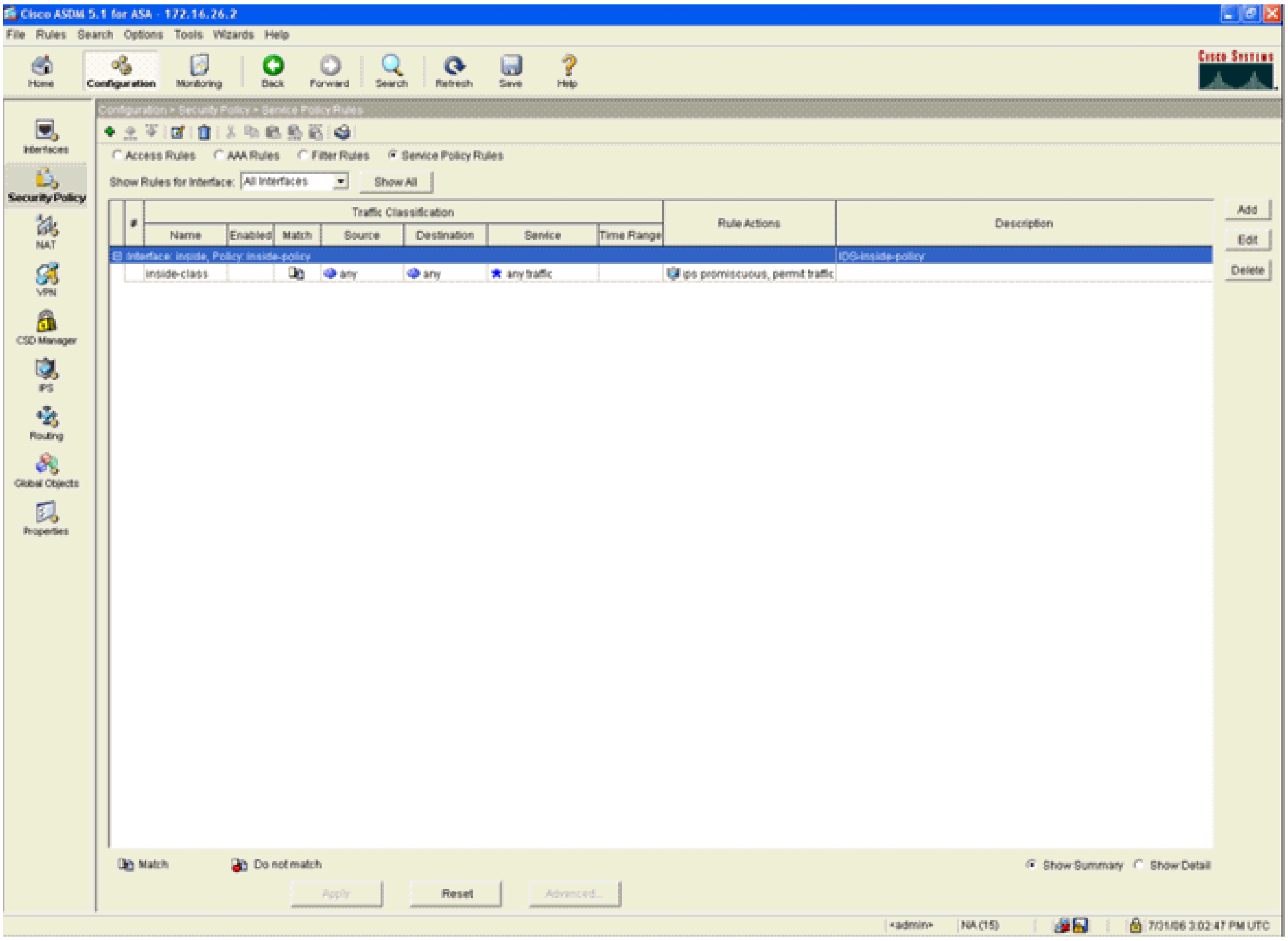


Cisco ASDM 5.1 for ASA - 172.16.26.2
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Configuration > Interfaces
Interfaces
Security Policy
NAT
VPN
CSD Manager
IPS
Routing
Global Objects
Properties
Add
Edit
Delete
Apply
Reset
<admin>
NA (15)
7/27/06 5:07:52 PM UTC

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Management Only	MTU	Description
Ethernet0/0	outside	Yes	0	10.10.102.2	255.255.255.0	No	1500	
Ethernet0/1	inside	Yes	100	172.16.26.2	255.255.255.0	No	1500	
Ethernet0/2		No				No		
Management0/0	manage...	Yes	100	192.168.1.1	255.255.255.0	Yes	1500	

□ Enable traffic between two or more interfaces which are configured with same security levels

3. 按一下視窗左側的Security Policy。在生成的視窗中，選擇Service Policy Rules選項卡。



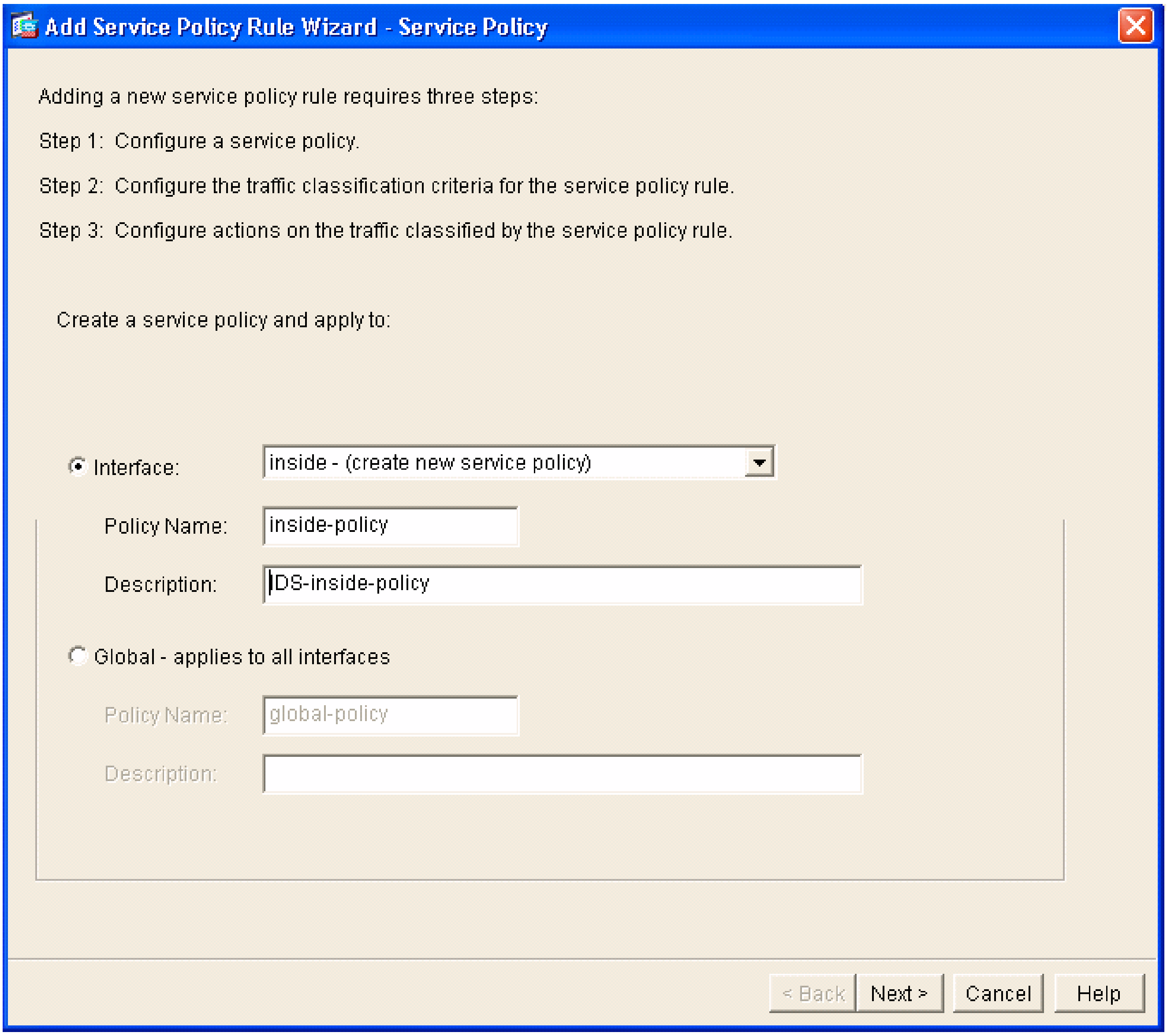
○ Access Rules ○ AAA Rules ○ Filter Rules ● Service Policy Rules

Show Rules for Interface: All Interfaces ▾ Show All

#	Traffic Classification							Rule Actions	Description
	Name	Enabled	Match	Source	Destination	Service	Time Range		
⊟ Interface: inside, Policy: inside-policy									IDS-inside-policy
	inside-class			any	any	★ any traffic		ips promiscuous, permit traffic	

● Show Summary ○ Show Detail

4. 按一下**Add**以建立新策略。將在新視窗中啟動新增服務策略規則嚮導。按一下**Interface**，然後從下拉選單中選擇正確的介面，以便建立繫結到傳遞流量的某個介面的新策略。使用兩個文本框為策略指定一個名稱並描述策略執行的操作。按一下「**Next**」以進入下一個步驟。



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: inside - (create new service policy)

Policy Name: inside-policy

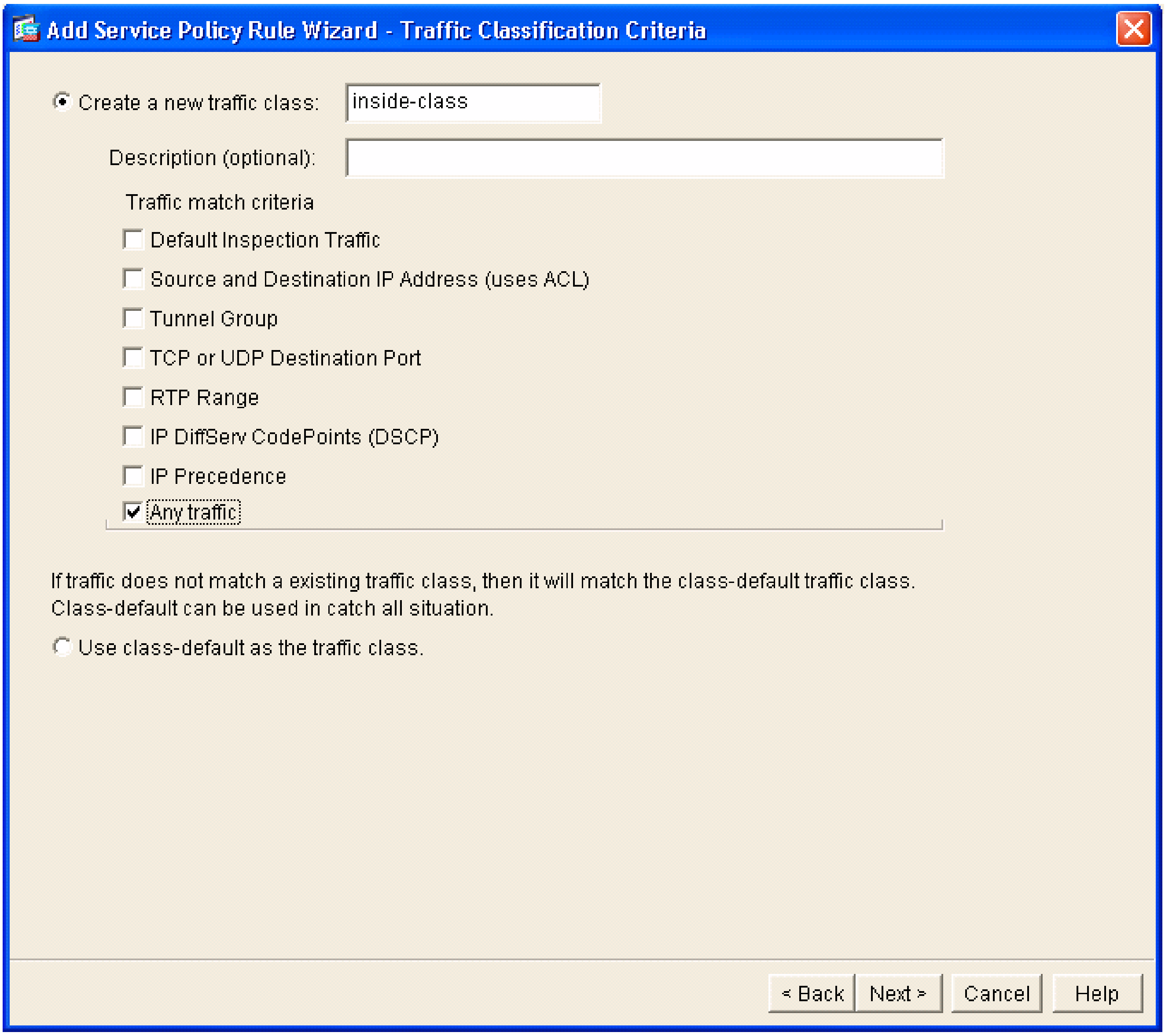
Description: IDS-inside-policy

○ Global - applies to all interfaces

Policy Name: global-policy

Description:

5. 構建要應用於策略的新流量類。為了檢查特定資料型別，構建特定類是合理的，但在此示例中，為簡化起見，選擇了Any Traffic。按一下「**Next**」以繼續。



Add Service Policy Rule Wizard - Traffic Classification Criteria

● Create a new traffic class: inside-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)

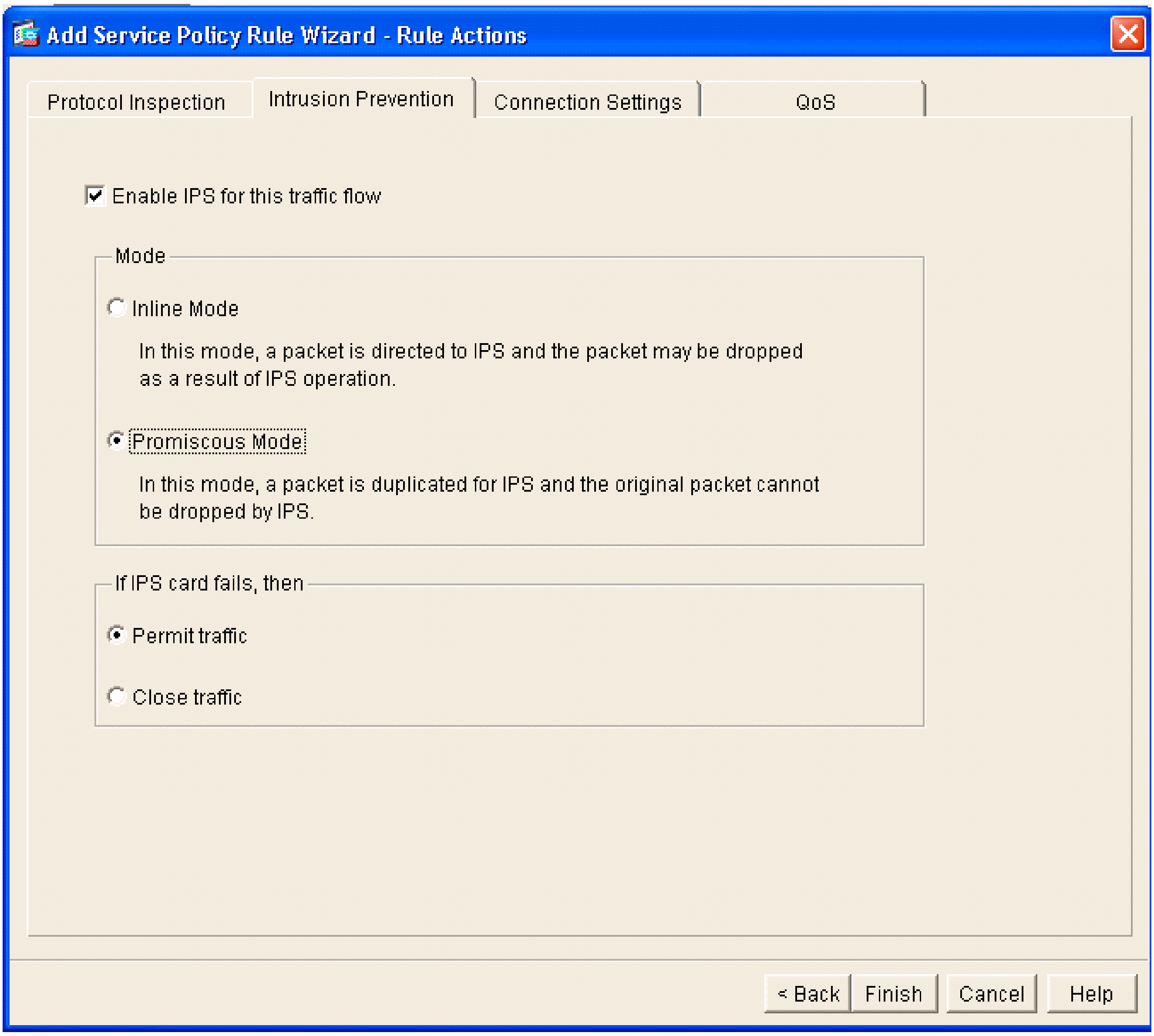
□ IP Precedence

☑ 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.

6. 完成以下步驟，以便指示ASA將流量定向到其AIP-SSM。選中**Enable IPS for this traffic flow**以啟用入侵檢測。將模式設定為**混雜**，以便流量的副本在帶外傳送到模組，而不是將模組與資料流內聯。按一下**Permit traffic**以確保ASA交換機在AIP-SSM發生故障時進入失效開放狀態。按一下**完成**以提交更改。



Add Service Policy Rule Wizard - Rule Actions

☑ Enable IPS for this traffic flow

Mode

○ Inline Mode

In this mode, a packet is directed to IPS and the packet may be dropped as a result of IPS operation.

● Promiscous Mode

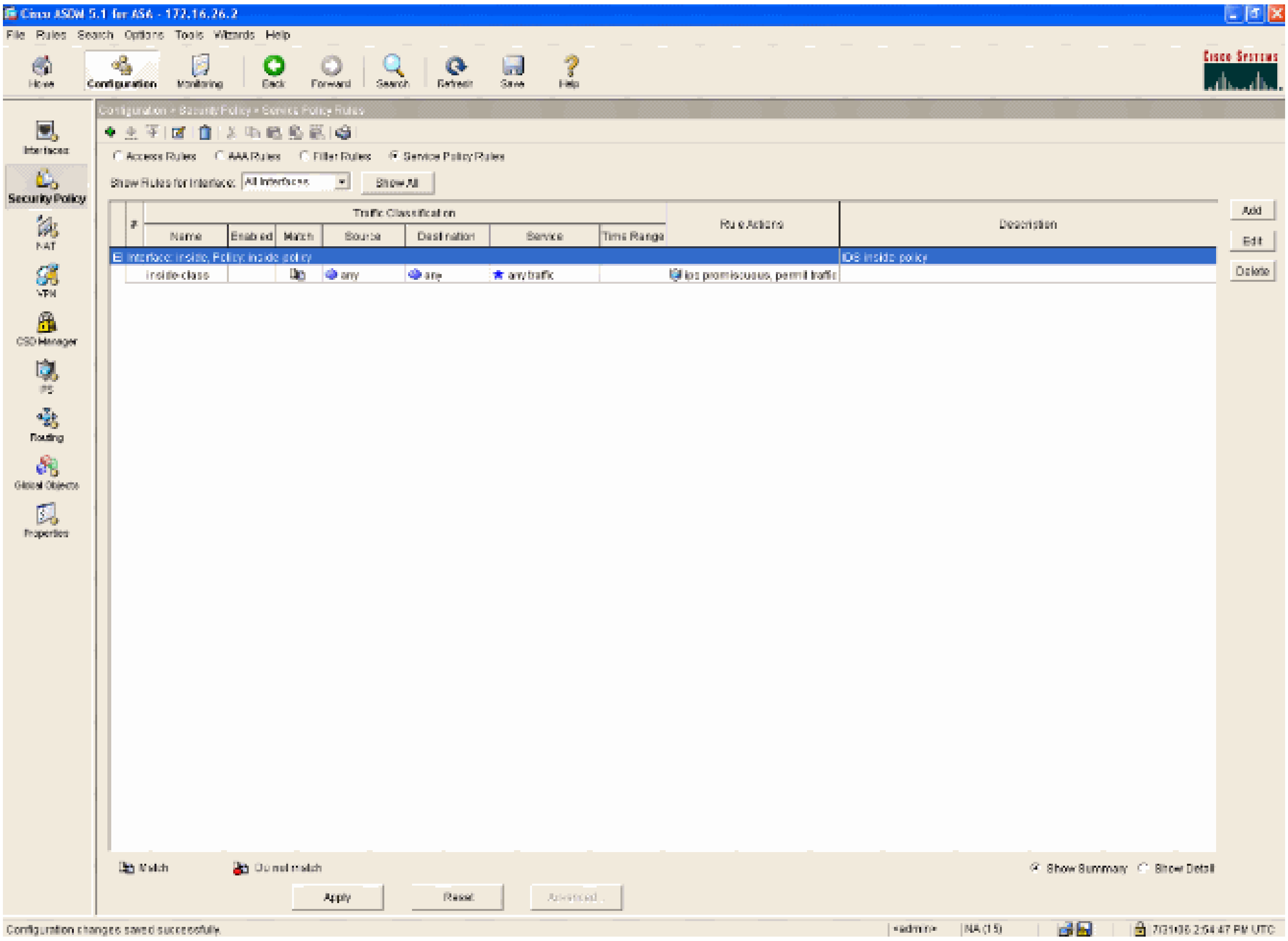
In this mode, a packet is duplicated for IPS and the original packet cannot be dropped by IPS.

If IPS card fails, then

● Permit traffic

○ Close traffic

7. ASA現在配置為將流量傳送到IPS模組。按一下頂行上的**Save**以將更改寫入ASA。


Cisco ASDM 5.1 for ASA - 172.16.26.2
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Cisco Systems
Interfaces
Security Policy
NAT
VPN
CSD Manager
IPS
Routing
Global Objects
Properties
Configuration > Security Policy > Service Policy Rules
Add
Edit
Delete
Match
Do not match
Apply
Reset
Advanced...

○ Access Rules ○ AAA Rules ○ Filter Rules ● Service Policy Rules

Show Rules for Interface: All Interfaces Show All

#	Traffic Classification							Rule Actions	Description
	Name	Enabled	Match	Source	Destination	Service	Time Range		
⊟ Interface: inside, Policy: inside-policy									IDS inside policy
	inside-class			any	any	any traffic		ips promiscuous, permit traffic	

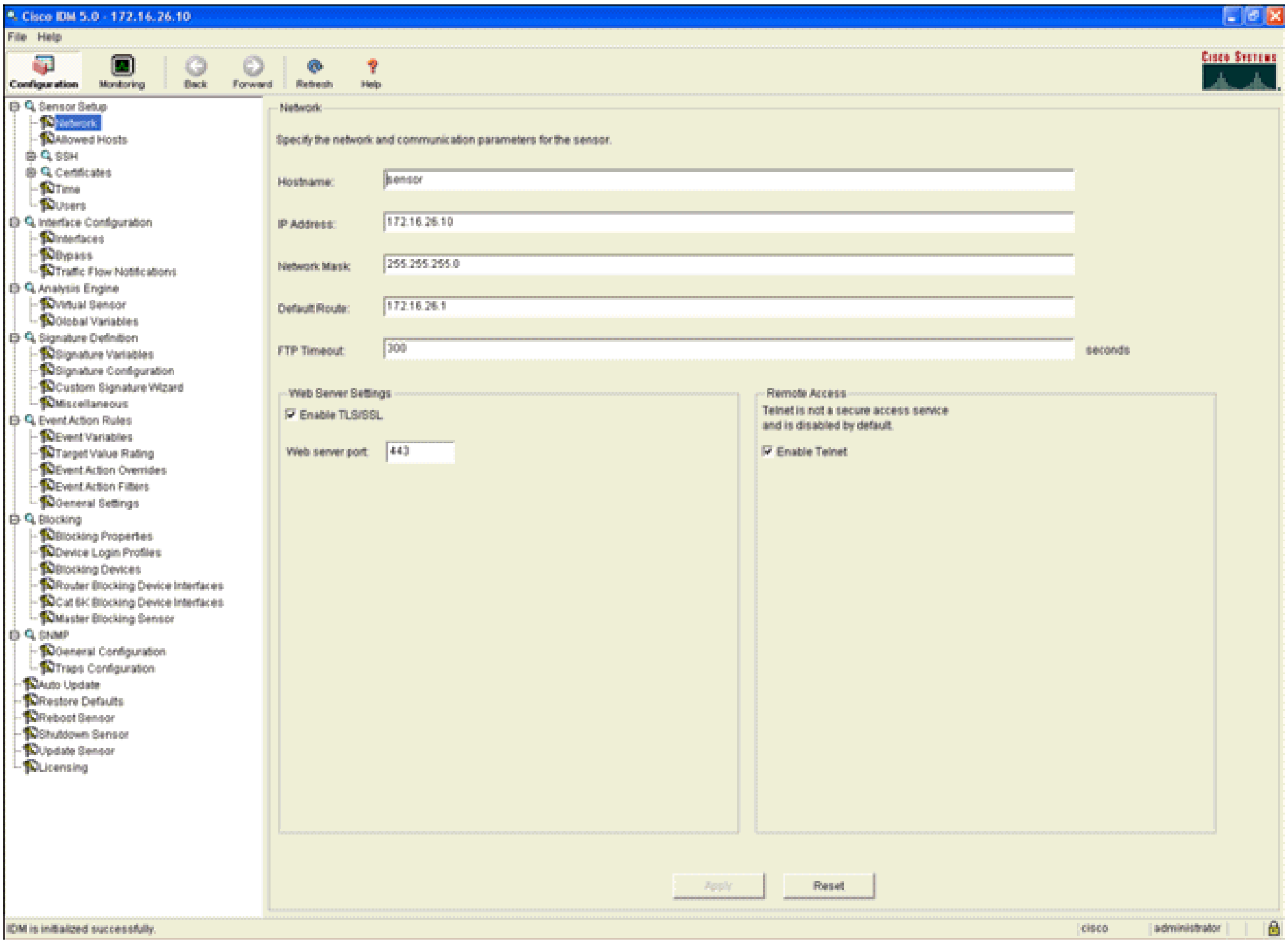
● Show Summary ○ Show Detail

Configuration changes saved successfully. <admin> NA (15) 7/31/06 2:54:47 PM UTC

配置用於流量檢測的AIP-SSM

當ASA向IPS模組傳送資料時，請將AIP-SSM介面與其虛擬感測器引擎關聯。

1. 使用IDM登入AIP-SSM。



Network

Specify the network and communication parameters for the sensor.

Hostname: sensor

IP Address: 172.16.26.10

Network Mask: 255.255.255.0

Default Route: 172.16.26.1

FTP Timeout: 300 seconds

Web Server Settings

☑ Enable TLS/SSL

Web server port: 443

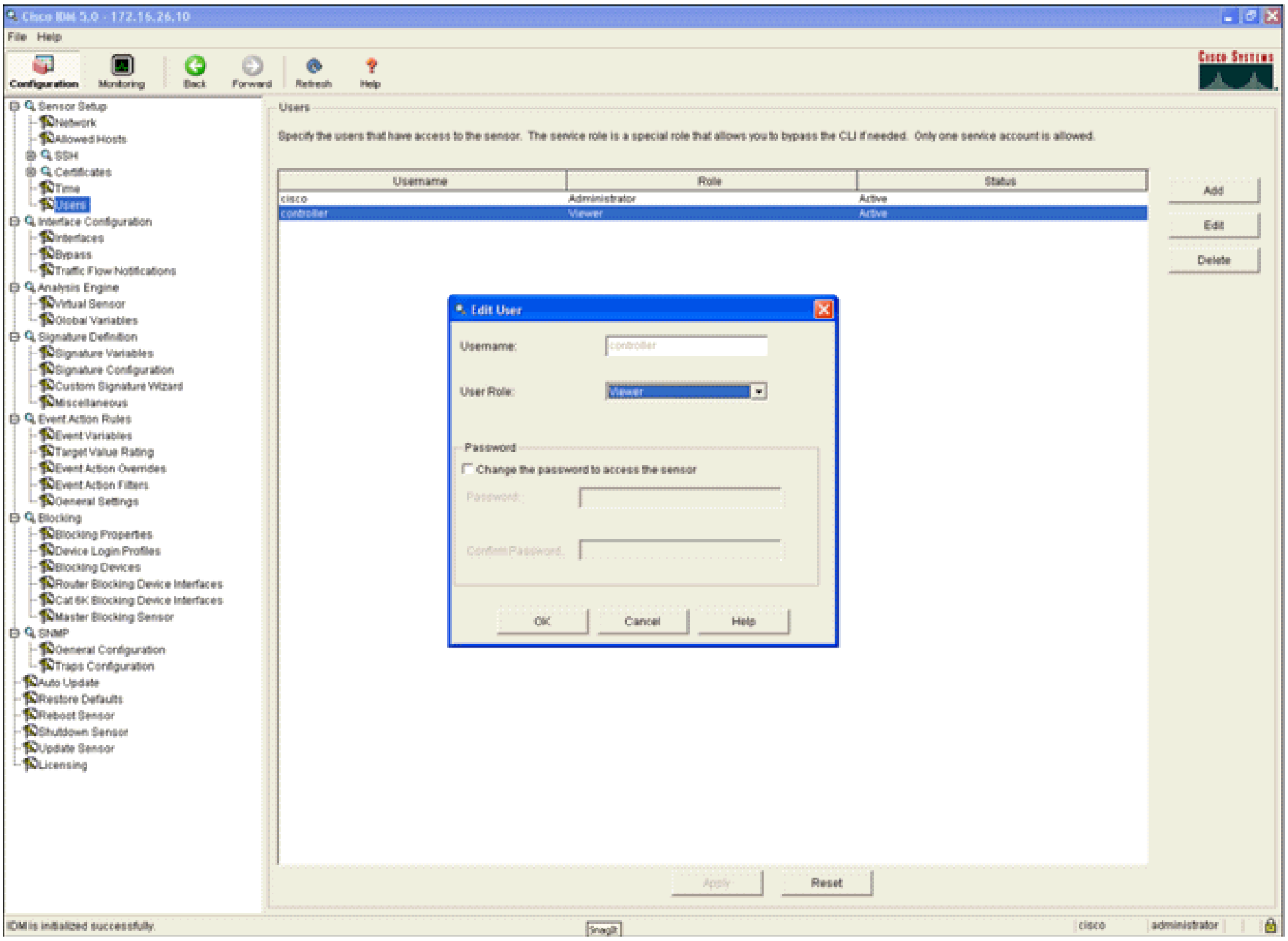
Remote Access

Telnet is not a secure access service and is disabled by default.

☑ Enable Telnet

IDM is initialized successfully.

2. 新增至少具有檢視器許可權的使用者。



Users

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
cisco	Administrator	Active
controller	Viewer	Active

Edit User

Username: controller

User Role: Viewer

Password

☐ Change the password to access the sensor

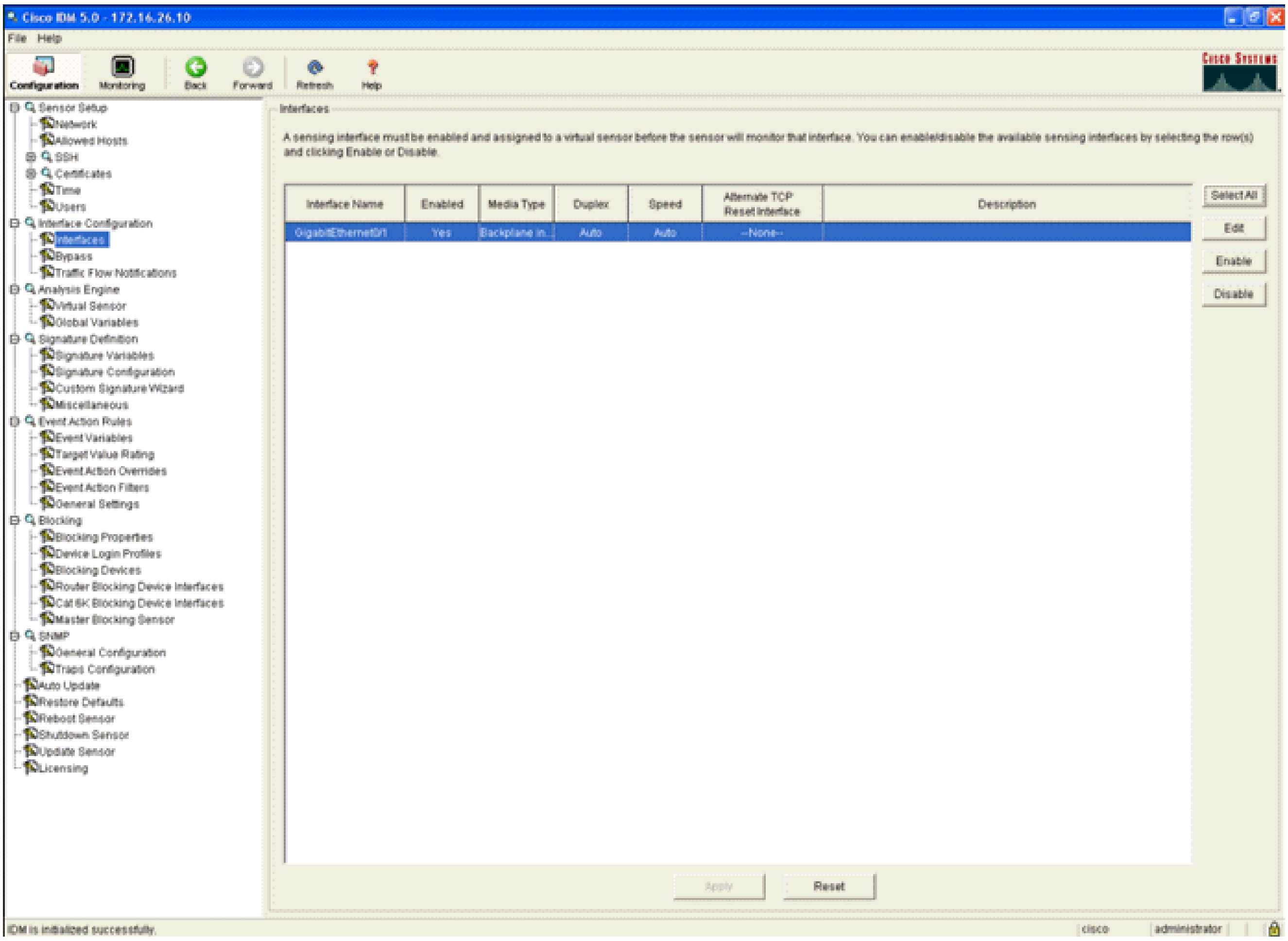
Password:

Confirm Password:

OK Cancel Help

IDM is initialized successfully.

3. 啟用介面。



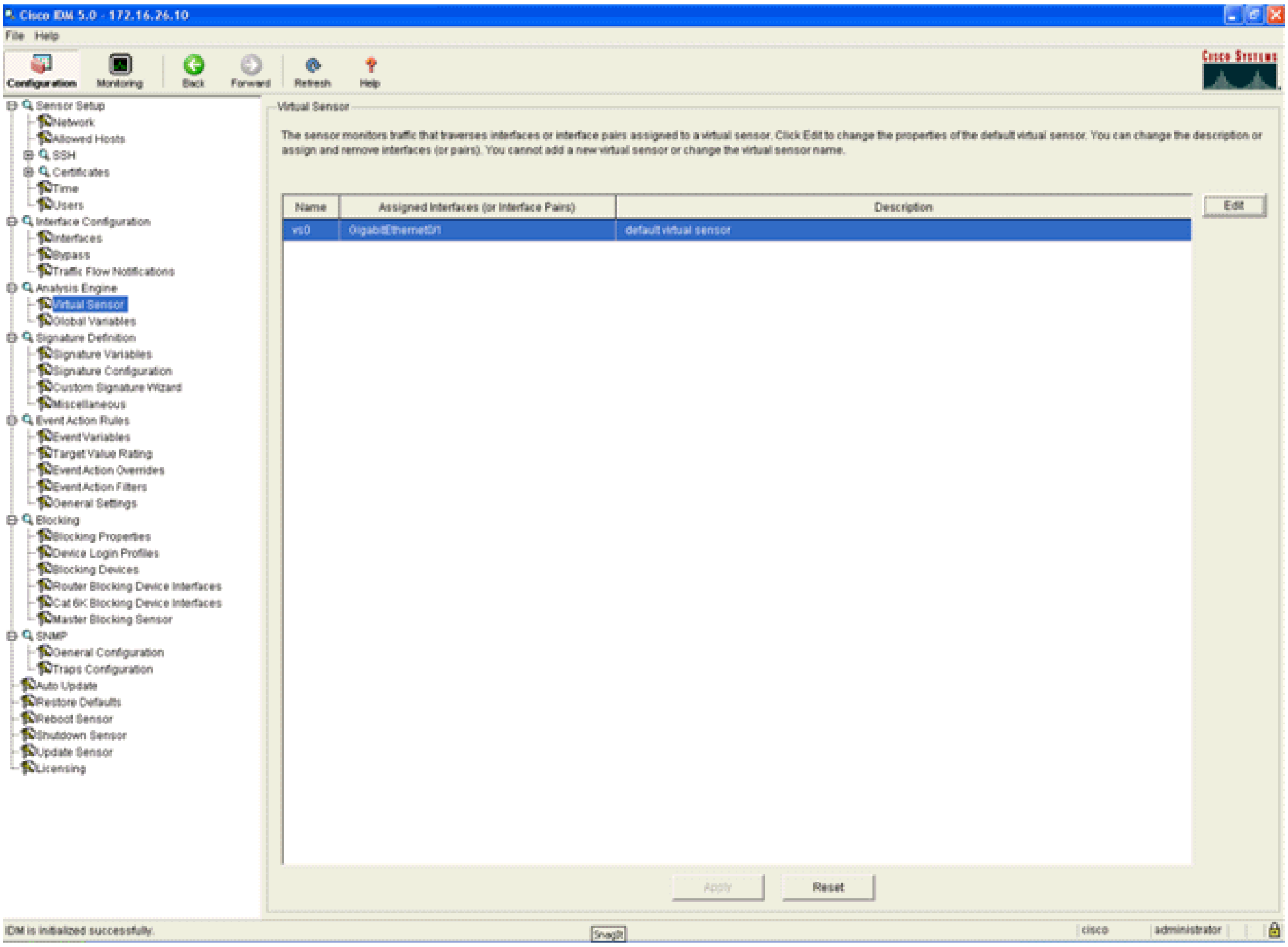
Interfaces

A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Media Type	Duplex	Speed	Alternate TCP Reset Interface	Description
GigabitEthernet0/1	Yes	Backplane in...	Auto	Auto	--None--	

IDM is initialized successfully.

4. 檢查虛擬感測器配置。



Virtual Sensor

The sensor monitors traffic that traverses interfaces or interface pairs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the description or assign and remove interfaces (or pairs). You cannot add a new virtual sensor or change the virtual sensor name.

Name	Assigned Interfaces (or Interface Pairs)	Description
vs0	GigabitEthernet0/1	default virtual sensor

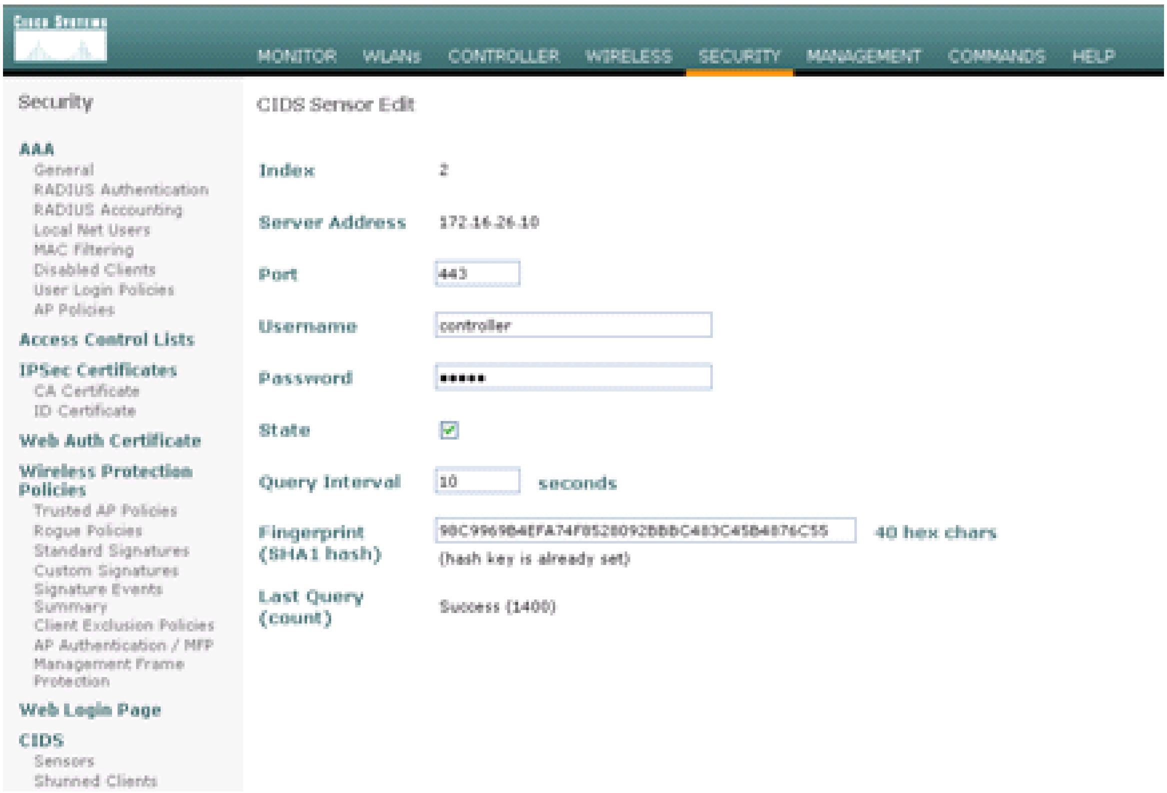
IDM is initialized successfully.

配置WLC輪詢客戶端塊的AIP-SSM

設定好感測器並準備將其新增至控制器後，請完成以下步驟：

1. 在WLC中選擇**Security > CIDS > Sensors > New**。
2. 新增您在上一部分中建立的IP地址、TCP埠號、使用者名稱和密碼。
3. 若要從感應器取得指紋，請在感應器中執行此命令，然後在WLC上新增SHA1指紋（不含冒號）。 這用於保護控制器到IDS的輪詢通訊。

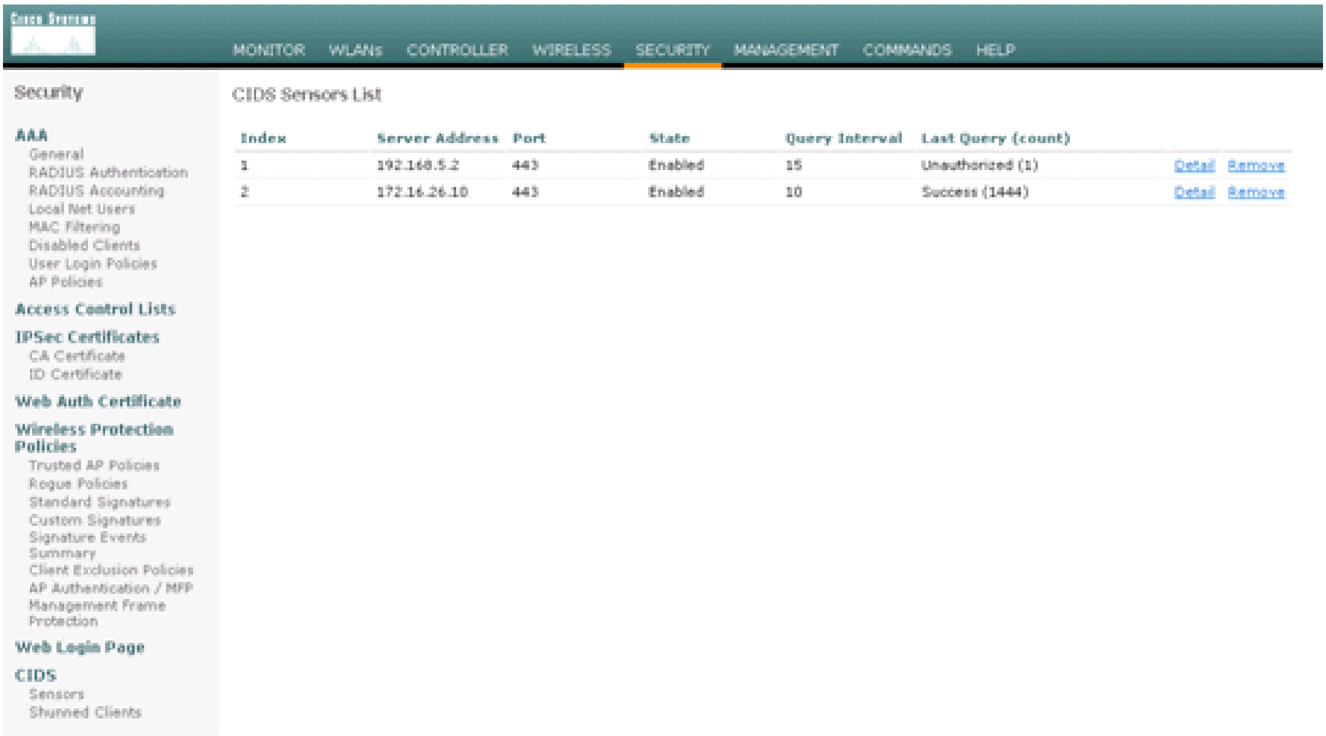
```
sensor#show tls fingerprint
MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E
SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55
```



CIDS Sensor Edit

Index	2
Server Address	172.16.26.10
Port	443
Username	controller
Password	●●●●●
State	☑
Query Interval	10 seconds
Fingerprint (SHA1 hash)	98C9969B4EFA74F8528092BBBC483C45B4876C55 40 hex chars (hash key is already set)
Last Query (count)	Success (1400)

4. 檢查AIP-SSM和WLC之間的連線狀態。



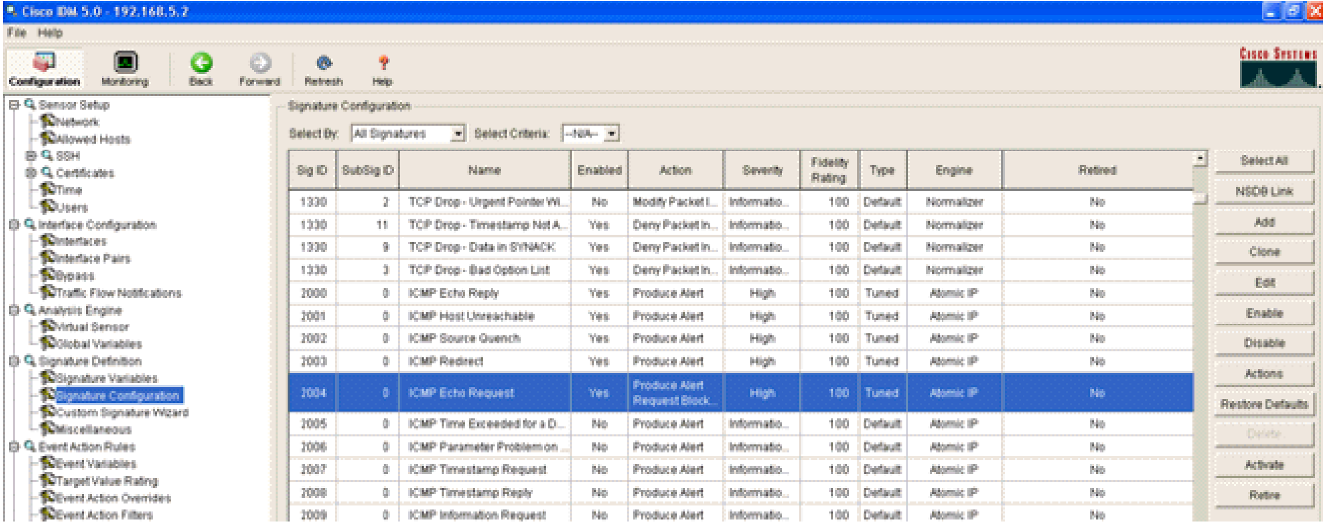
CIDS Sensors List

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

向AIP-SSM新增阻止簽名

新增檢查簽名以阻止流量。雖然有許多簽名可以根據可用的工具執行作業，但本示例建立一個阻止ping資料包的簽名。

1. 選擇2004**簽名（ICMP回應請求）**，以執行快速設定驗證。

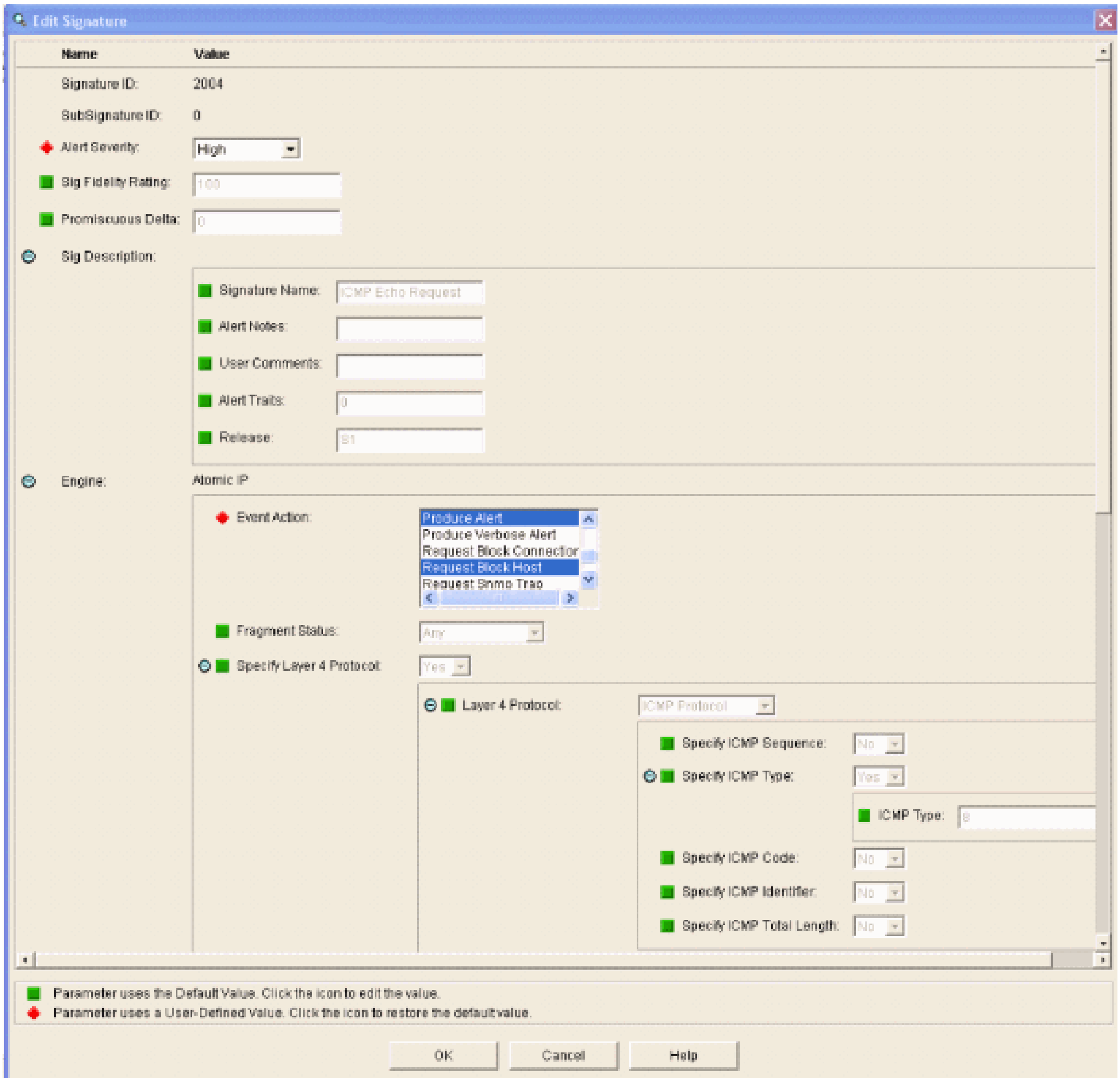


Signature Configuration

Select By: All Signatures   Select Criteria: --N/A--

Sig ID	SubSig ID	Name	Enabled	Action	Severity	Fidelity Rating	Type	Engine	Retired
1330	2	TCP Drop - Urgent Pointer Wi...	No	Modify Packet I...	Informatio...	100	Default	Normalizer	No
1330	11	TCP Drop - Timestamp Not A...	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In...	Informatio...	100	Default	Normalizer	No
1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In...	Informatio...	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	Informatio...	100	Default	Atomic IP	No
2006	0	ICMP Parameter Problem on ...	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio...	100	Default	Atomic IP	No
2009	0	ICMP Information Request	No	Produce Alert	Informatio...	100	Default	Atomic IP	No

2. 啟用特徵碼，將Alert Severity（警報嚴重性）設定為**High**，並將Event Action（事件操作）設定為**Produce Alert**（生成警報）和**Request Block Host**，以完成此驗證步驟。請注意，Request Block Host操作是向WLC發出訊號以建立客戶端異常的關鍵。

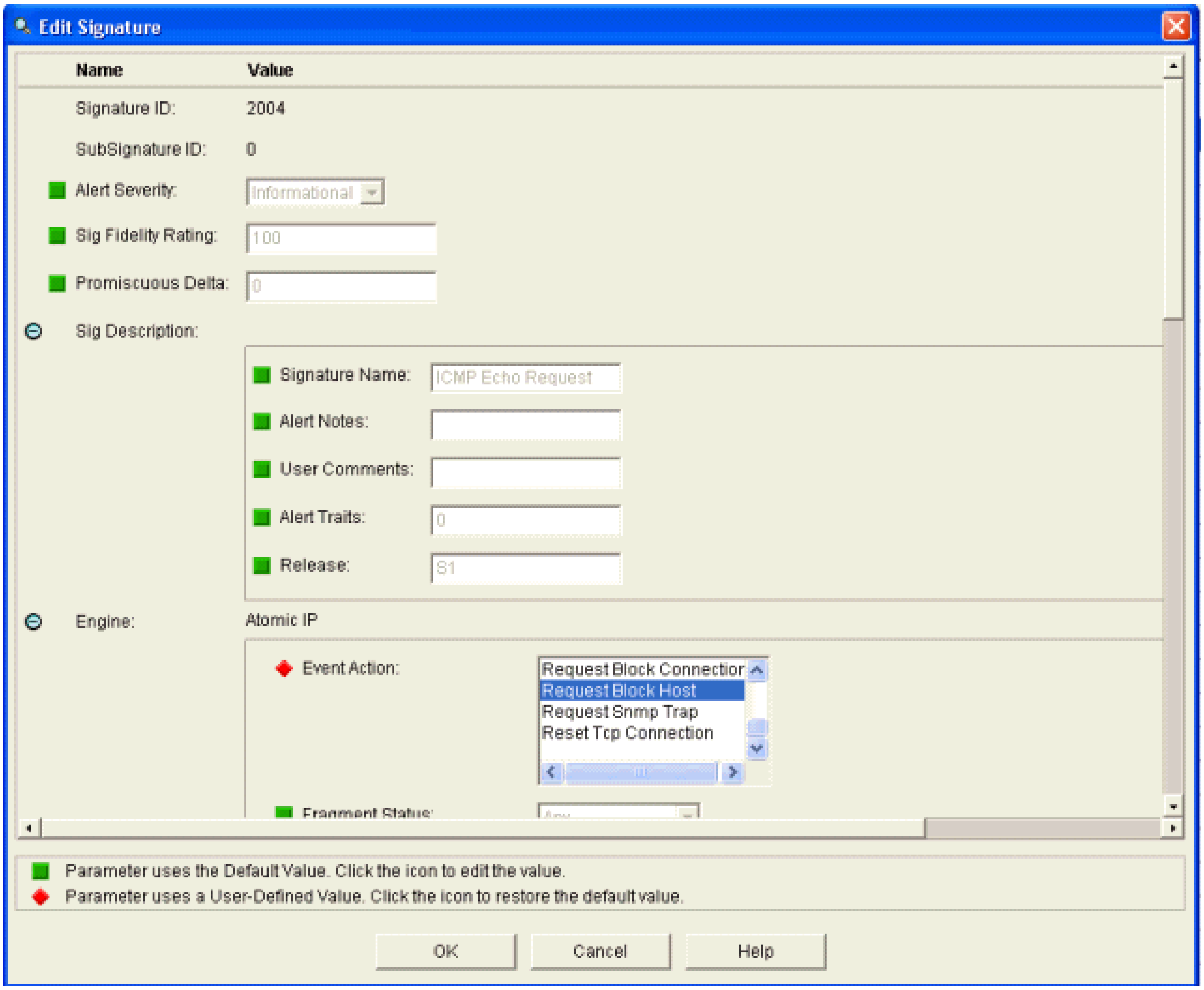


Edit Signature

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.



Edit Signature

Name	Value
Signature ID:	2004
SubSignature ID:	0
🟩 Alert Severity:	Informational
🟩 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:	Request Block Connection Request Block Host Request Snmp Trap Reset Tcp Connection
🟩 Fragment Status:	Any

🟩 Parameter uses the Default Value. Click the icon to edit the value.

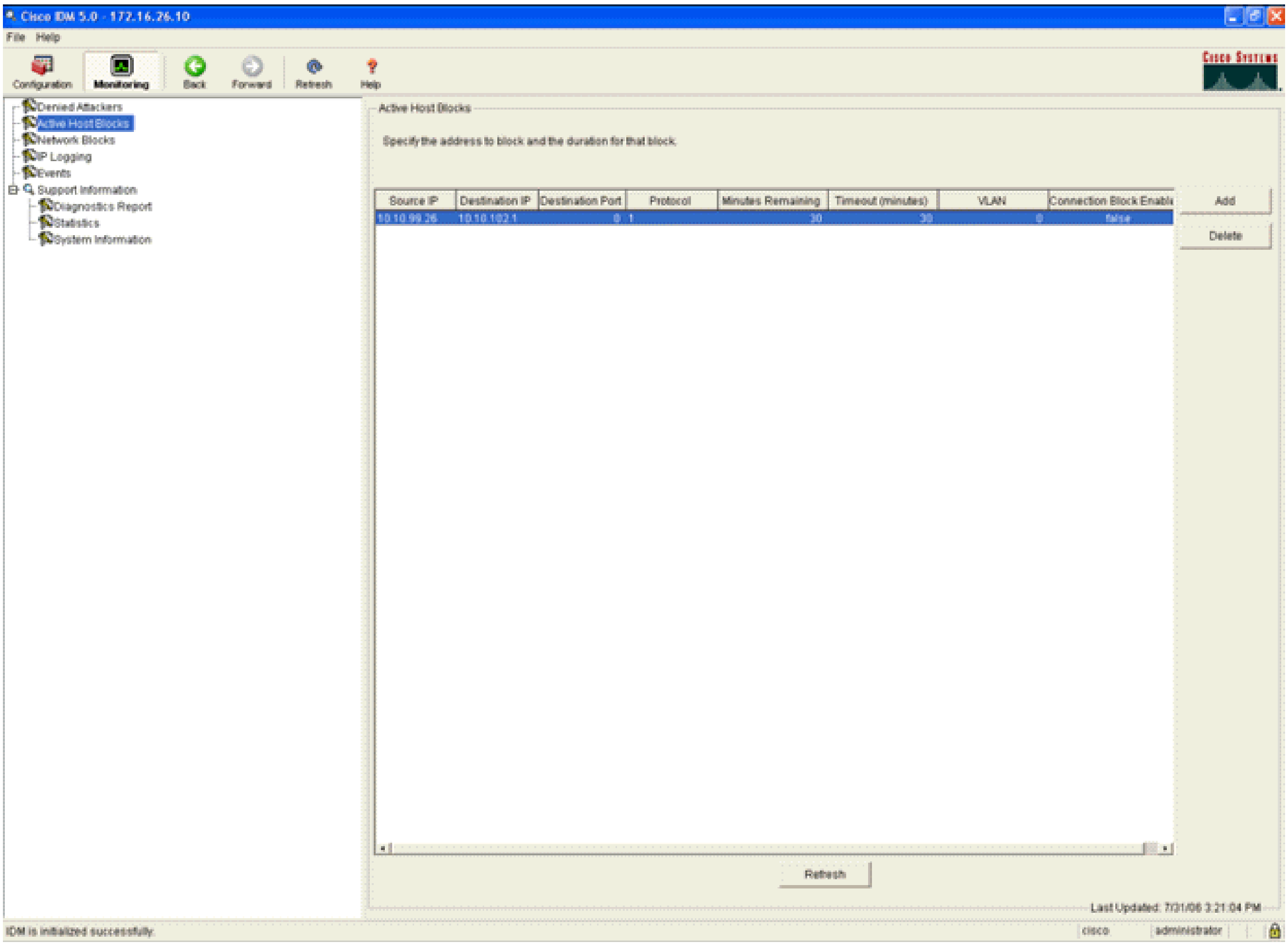
♦ Parameter uses a User-Defined Value. Click the icon to restore the default value.

3. 按一下「**OK**」以儲存簽名。
4. 驗證簽名是否處於活動狀態，以及是否將其設定為執行阻止操作。
5. 按一下**Apply**以將簽名提交到模組。

使用IDM監視阻止和事件

請完成以下步驟：

1. 成功觸發簽名後，IDM中有兩個地方可以注意這一點。第一種方法顯示AIP-SSM已安裝的活動塊。按一下頂部操作行上的**Monitoring**。在左側顯示的項清單中，選擇**Active Host Blocks**。每當ping簽名觸發時，「活動主機塊」視窗都會顯示違規者的IP地址、受攻擊裝置的地址以及阻止生效所剩餘的時間。預設阻塞時間為30分鐘，並且是可調節的。但是，本文不討論更改此值。有關如何更改此引數的資訊，請根據需要參閱ASA配置文檔。立即刪除該阻止，從清單中選擇它，然後按一下**刪除**。



Active Host Blocks

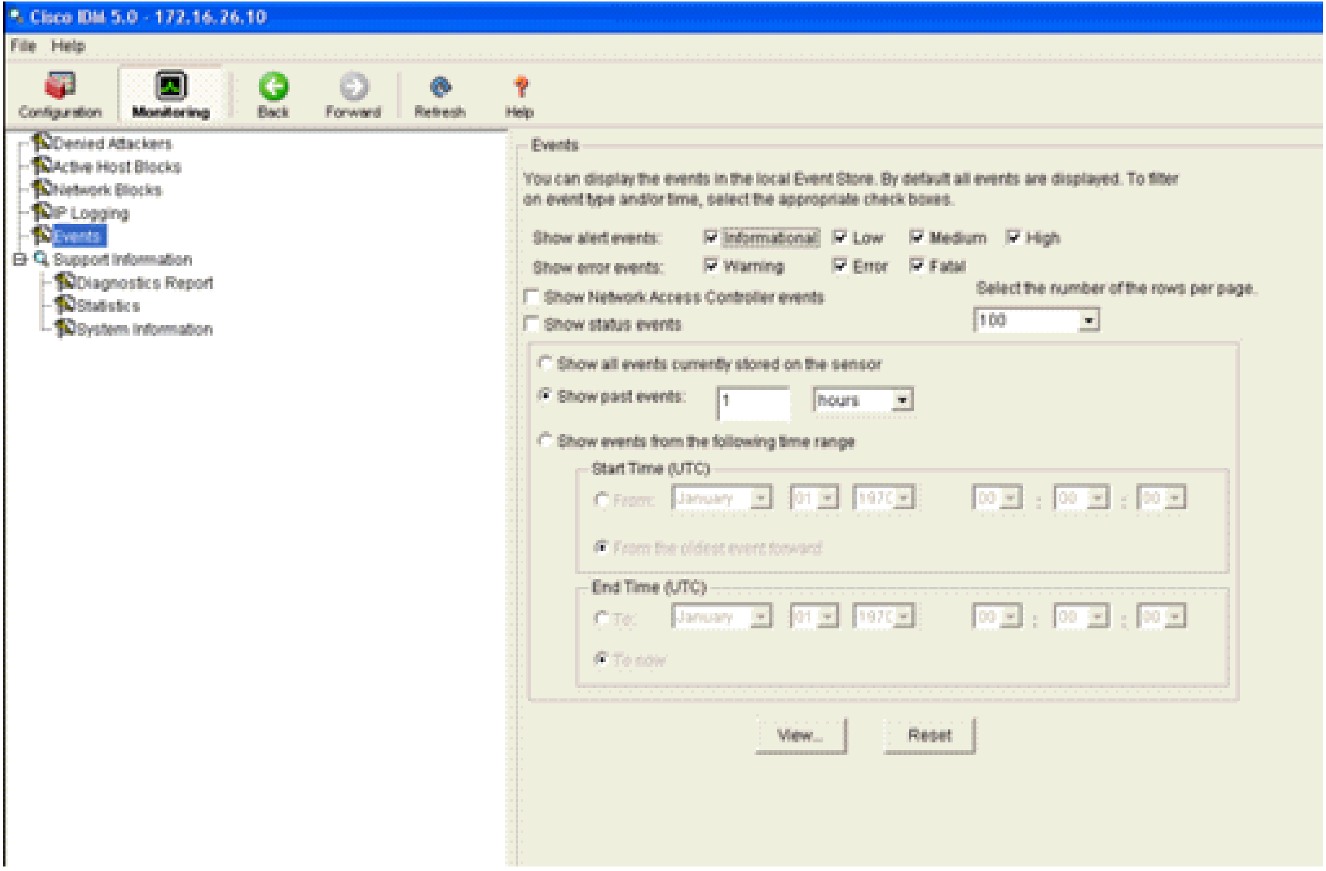
Specify the address to block and the duration for that block.

Source IP	Destination IP	Destination Port	Protocol	Minutes Remaining	Timeout (minutes)	VLAN	Connection Block Enabl
10.10.99.26	10.10.102.1	0	1	30	30	0	false

Last Updated: 7/31/06 3:21:04 PM

IDM is initialized successfully.

檢視觸發簽名的第二種方法使用AIP-SSM事件緩衝區。在「IDM監視」頁中，在左側的專案清單中選擇**事件**。系統將顯示Events搜尋實用程式。設定相應的搜尋條件，然後單**擊「檢視……」**
(View...).



Events

You can display the events in the local Event Store. By default all events are displayed. To filter on event type and/or time, select the appropriate check boxes.

Show alert events: ☑ Informational ☑ Low ☑ Medium ☑ High

Show error events: ☑ Warning ☑ Error ☑ Fatal

☐ Show Network Access Controller events

☐ Show status events

Select the number of the rows per page. 100

○ Show all events currently stored on the sensor

● Show past events: 1 hours

○ Show events from the following time range

Start Time (UTC)

○ From: January 01 1970 00 : 00 : 00

● From the oldest event forward

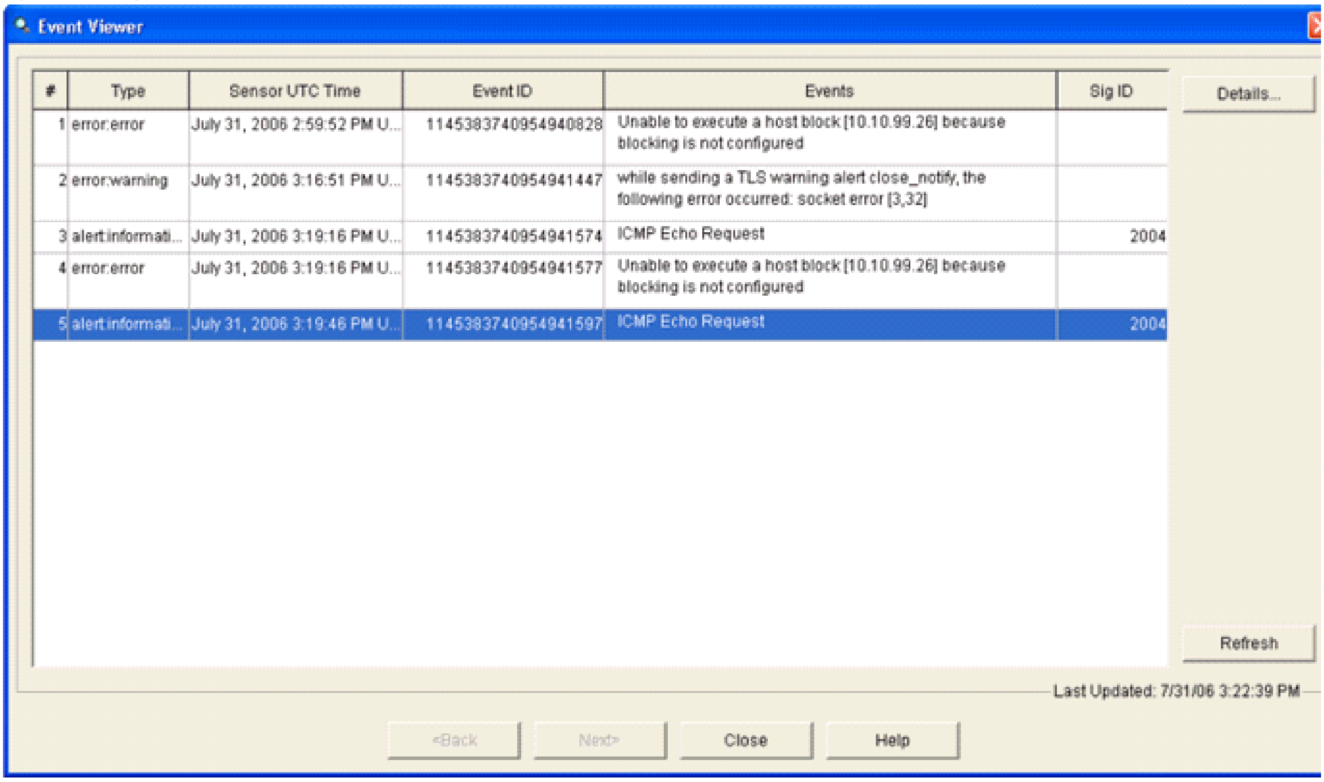
End Time (UTC)

○ To: January 01 1970 00 : 00 : 00

● To now

2. 此時將出現事件檢視器，其中包含符合給定條件的事件的清單。滾動清單並找到在先前配置步

驟中修改的ICMP回應請求簽名。在「事件」列中查詢簽名的名稱，或者在「簽名ID」列下搜尋簽名的標識號。

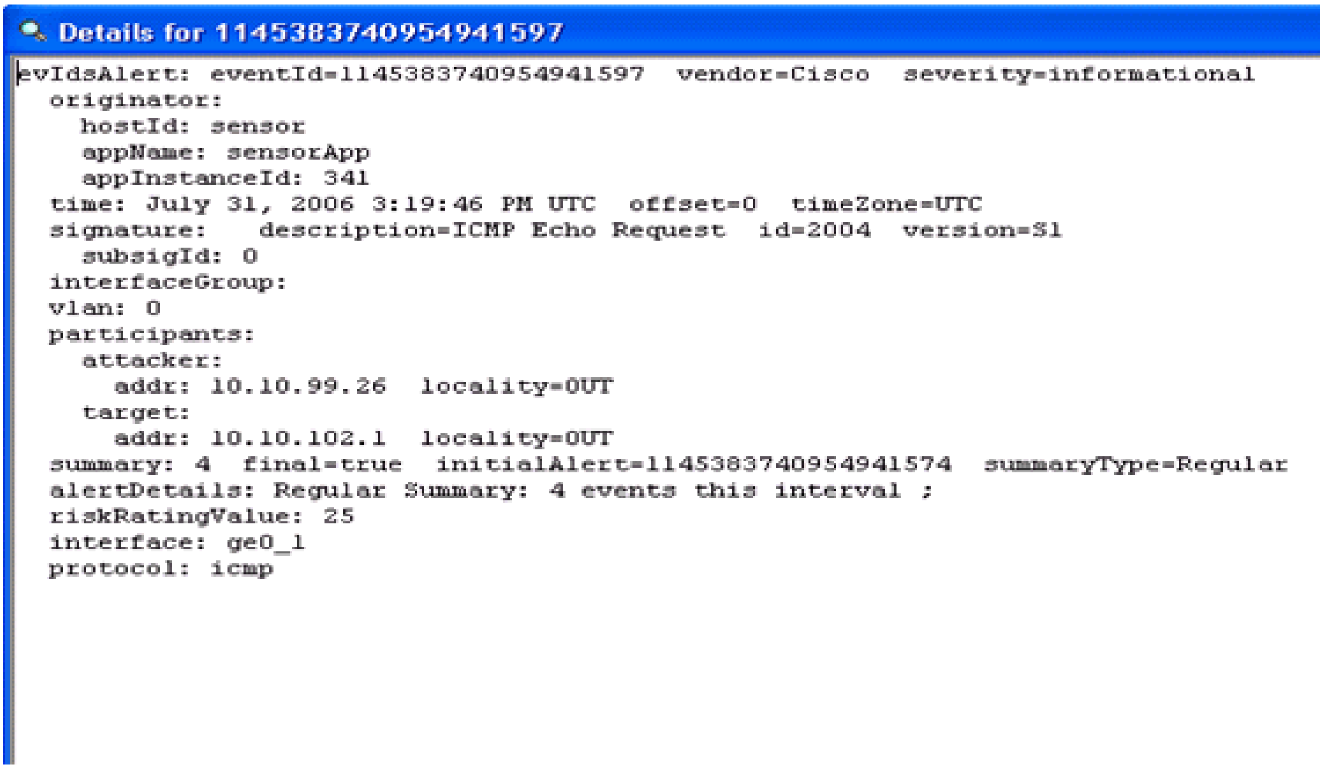


Event Viewer

#	Type	Sensor UTC Time	Event ID	Events	Sig ID
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

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

3. 找到簽名後，按兩下該條目以開啟一個新視窗。新視窗包含有關觸發特徵碼的事件的詳細資訊。

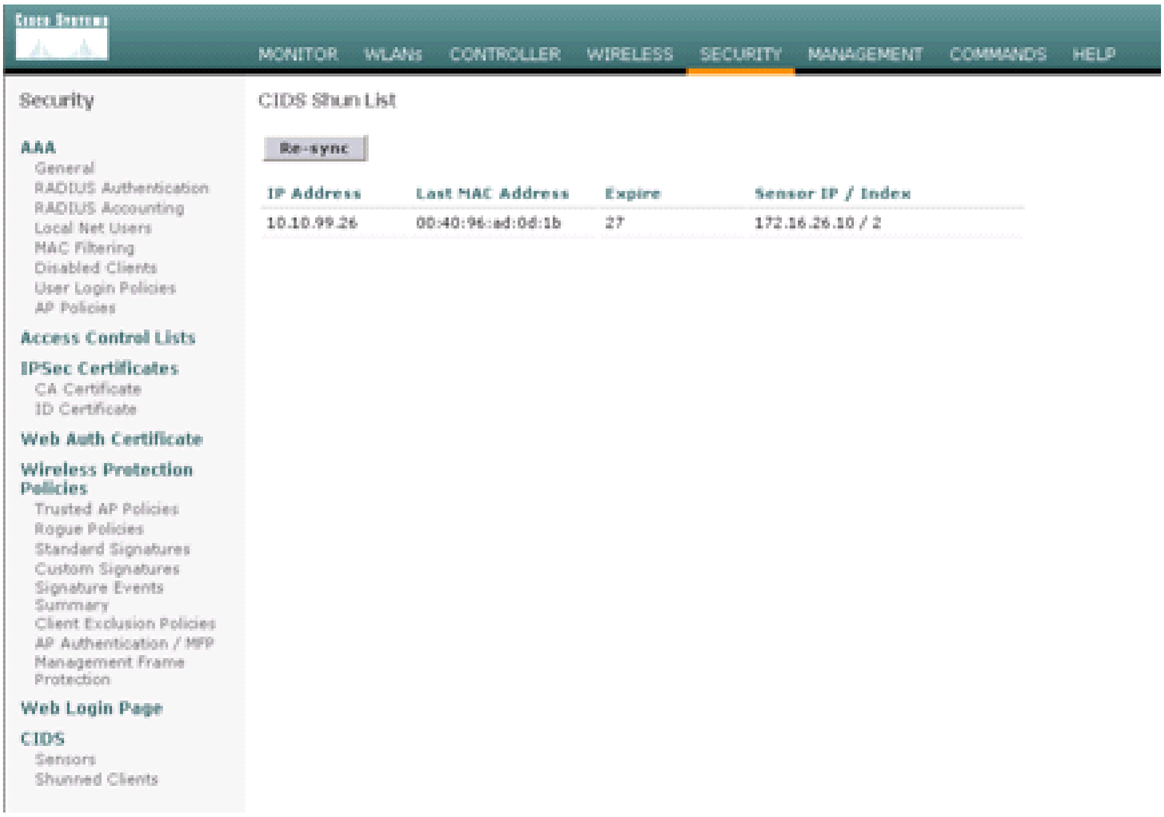


Details for 1145383740954941597

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

無線控制器中的監控客戶端排除

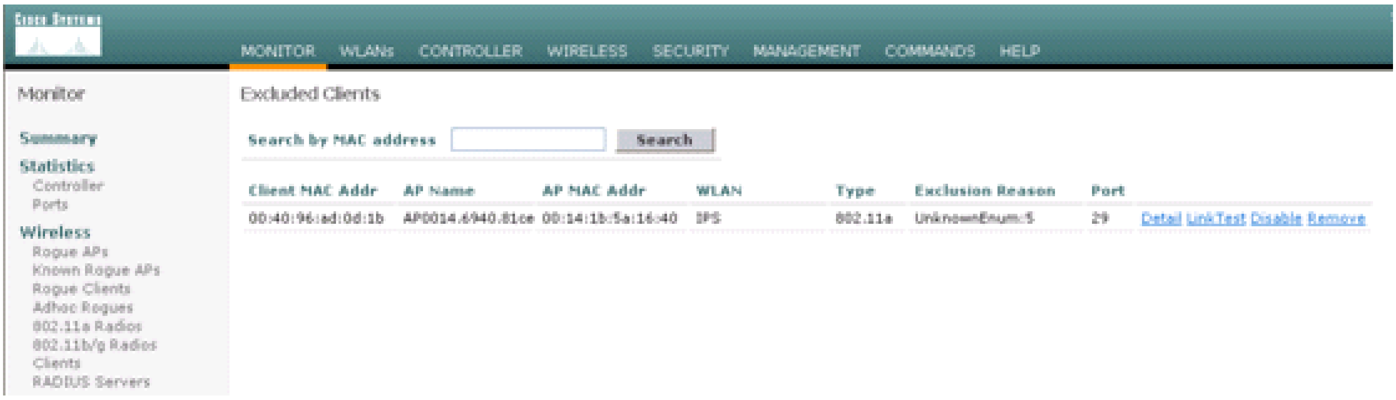
此時控制器中的Shunned Clients清單會填充主機的IP和MAC地址。



CIDS Shun List

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

該使用者將被新增到「客戶端排除」清單中。



Excluded Clients

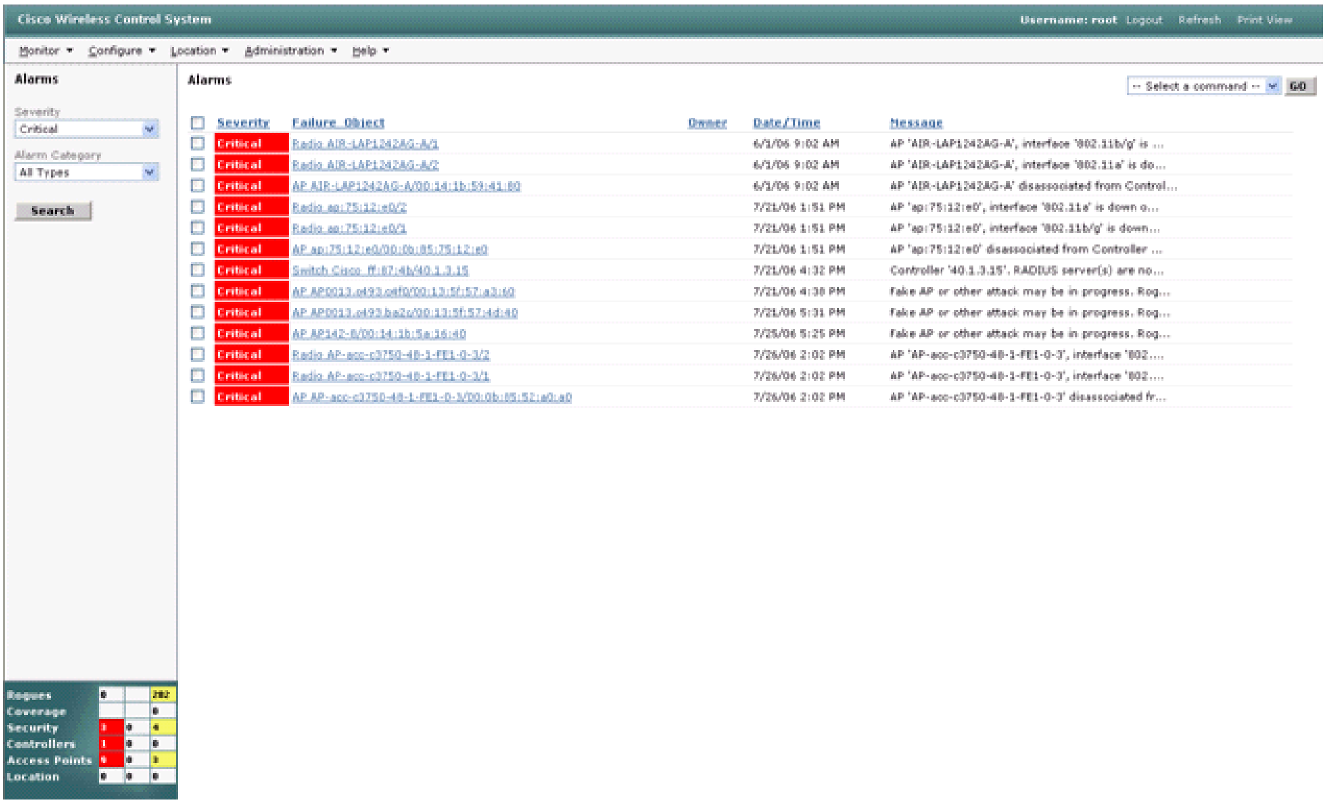
Search by MAC address

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 LinkTest Disable Remove

監視WCS中的事件

在AIP-SSM內觸發阻止的安全事件導致控制器將違規者的地址新增到客戶端排除清單中。在WCS中也會生成事件。

1. 使用WCS主選單中的**Monitor > Alarms**實用程式檢視排除事件。WCS最初顯示所有未清除的警報，並在視窗的左側顯示搜尋功能。
2. 修改搜尋條件以查詢客戶端塊。在Severity下，選擇**Minor**，並將Alarm Category設定為**Security**。
3. 按一下「**Search**」。



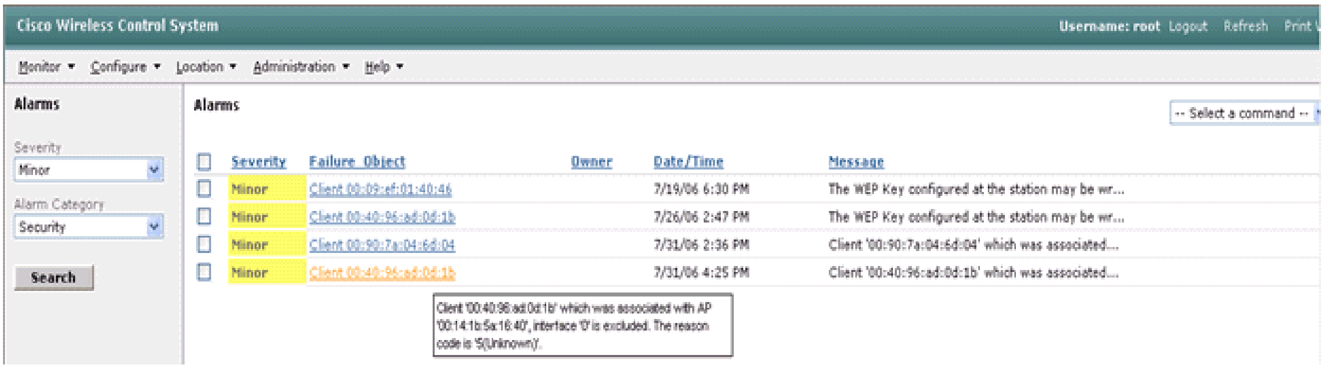
Severity: Critical

Alarm Category: All Types

□	Severity	Failure Object	Owner	Date/Time	Message
□	Critical	Radio AIR-LAP1242AG-A/1		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11b/g' is ...
□	Critical	Radio AIR-LAP1242AG-A/2		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11a' is do...
□	Critical	AP AIR-LAP1242AG-A/00:14:1b:59:41:80		6/1/06 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_ff:87:4b/40.1.3.15		7/21/06 4:32 PM	Controller '40.1.3.15'. RADIUS server(s) are no...
□	Critical	AP AP0013.c493.c4f0/00:13:5f:57:a3:60		7/21/06 4:38 PM	Fake AP or other attack may be in progress. Rog...
□	Critical	AP AP0013.c493.ba2c/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:16:40		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...

Rogues	0		282
Coverage			0
Security	1	0	4
Controllers	1	0	0
Access Points	9	0	3
Location	0	0	0

4. 然後，「警報」視窗僅列出嚴重性為次要的安全警報。將滑鼠指向在AIP-SSM內觸發該塊的事件。特別是，WCS顯示導致警報的客戶端工作站的MAC地址。通過指向相應的地址，WCS會彈出一個包含事件詳細資訊的小視窗。按一下該連結可在另一個視窗中檢視這些相同的詳細資訊。



Severity: Minor

Alarm Category: Security

□	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 '5(Unknown)'.

Cisco ASA示例配置

```
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#
```

思科入侵防禦系統感測器示例配置

```
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#
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 安裝和使用思科入侵防禦系統裝置管理器5.1
- Cisco ASA 5500系列自適應安全裝置 — 配置指南
- 使用命令列介面5.0配置思科入侵防禦系統感測器 — 配置介面
- WLC組態設定指南4.0
- 無線技術支援
- 無線 LAN 控制器 (WLC) 常見問題
- 無線LAN控制器和輕量型存取點基本組態範例
- 配置安全解決方案
- 技術支援與文件 - Cisco Systems