無線LAN控制器和IPS整合指南

目錄

簡介 必要條件 需求 採用元件 慣例 Cisco IDS概觀 Cisco IDS和WLC — 整合概觀 IDS迴避 網路架構設計 配置Cisco IDS感測器 設定WLC Cisco IDS感測器示例配置 為IDS配置ASA <u>配置用於流量檢測的AIP-SSM</u> 配置WLC輪詢客戶端塊的AIP-SSM 向AIP-SSM新增阻止簽名 使用IDM監視阻止和事件 無線控制器中的監控客戶端排除 監視WCS中的事件 Cisco ASA示例配置 思科入侵防禦系統感測器示例配置 驗證 疑難排解 相關資訊

<u>簡介</u>

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。

<u>必要條件</u>

<u>需求</u>

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。

<u>採用元件</u>

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。

<u>Cisco IDS和WLC — 整合概觀</u>

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。



<u>IDS迴避</u>

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	Туре	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 dotlq
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<u>圖只</u>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。<u>架構圖表</u>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<u>內嵌模式</u>。

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#
```

<u>配置Cisco IDS感測器</u>

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:

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

NOTICE

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 <u>https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet</u> (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 10.0.0/8
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。

Cisco IDM 5.0 - 192.168.5.2				0
File Help				
🐺 🔳 🔇 🖸	0 0 1		Cisce S	*****
Configuration Monitoring Back Forwa	ed Refresh He	P	.db.	<u>_h_</u>
Contrare Setup G. G. Senior Setup G. G. Senior Setup G. G. Senior Setup G. G. Certificatos G. Certificatos G. G. Certificatos G. Certificatos Certificatos Certificatos G. Certificatos G. Certificatos G. Certificatos Certificatos Certificatos G. Certificatos G. Certificatos Certificatos Certificatos Certificatos G. Certificatos G. Certificatos Certificato	Noticest Performance Noticest Performance Specify the network Hostname: IP Address: Network Mask: Default Route: FTP Timeout Web Server Betts Practice TLSRS Web Server port:	Active Reset	seconds	
IDM is initialized successfully.			cisco administrator	1

5. 新增WLC用於訪問IPS感測器事件的使用者。

File Help						Citte Setting
Configuration Monitoring Back Forward	d Retresh Help					A. A.
Q. Sensor Setup Setup Network Setup Allowed Hosts B Q. SSH	Users Specify the users that have	e access to the sensor. The se	ervice role is a special ro	le that allows you to bypass	the CLI if needed. Only one service account is allowed.	
D Q Certificates	Us	emame		Role	Status	1
- Witney	cisco		Administrator		Active	Add
Q. Interface Configuration Pointerfaces						Edt
- Ninterface Pairs - NBypass						Delete
Q Analysis Engine		. 1.44 Day			3	
- Nintual Sensor		A KOD USET			2	
- Dolobal Variables		Usemame:	controller			
 Signature Definition Signature Variables 						
- Signature Configuration - Ocustom Signature Wizard		User Role:	Viewer	•		
G Q Event Action Rules						
- Devent Variables		- Password				
Sevent Action Overnoes		Password:	*****			
Doeneral Settings						
G Blocking						
- Sollocking Properties		Confirm Password	E 1			
Device Login Profiles						
Restar Blocking Device Interfaces						
- Cat 6K Blocking Device Interfaces		04	Cancel	Halp		
Staster Blocking Sensor		<u> </u>				
C CAMP					-	
敌用監控介面 。						
- Cisco IDM 5.0 - 197,168.5.7 Tile Help						
						Cisco Sester
Configuration Monitoring Back Forwar	d Refresh Help					A. A.
4 G. Sansor Salan	Interfaces					
Network						
- Allowed Hosts	A sensing interface mus	t be enabled and assigned to	a virtual sensor before t	e sensor will monitor that in	terface. You can enable/disable the available sensing interfaces	by selecting the row(s)
B Q SSH	and circking chadle or D	19.000				
B Q Certificates					1	
- SUsers	Interface Name	Enabled Media Type	Duplex Spee	d Atternate TCP Reset Interface	Description	Select All
Q Interface Configuration	GigabitEthemethith	Yes TX (concer)	Auto Auto	-None-		Edit
Sunterfaces	GigabitEthemet0/1	No TX (copper)	Auto Auto	None		
- Decass	OlgabitEthemet0/2	No TX (copper)	Auto Auto	None		Enable
Traffic Flow Notifications	OlgabitEthemet0/3	No TX (copper)	Auto Auto	None		Disable
						Putable

必須將監控介面新增到分析引擎,如以下視窗所示

Eile Male												
Configuration Monitoring Back	O Retrest	? Help										Casca Sr
Q Sensor Setup Network Sensor Setup Q, Network Q, SSH Q, Centicutes Continues	Virtual Ser The sens assign ar	nsor Ior monitors nd remove in	traffic that traverses interfaces o interfaces (or pains). You cannot s	r interface p idd a new v	airs assigned to a itual sensor or ch	virtual sensor ange the virtual	Click Edit 1 sensor nar	o change l me.	he properties of the de	rfault virtual sensor, You car	h change	the description
Dusers	Name		ssioned Interfaces (or Interface F	Pairs's	1			r	hescription			Edit
Q Interface Configuration Sinterfaces Sinterface Pairs Noteface Pairs Sinterface Pairs Sinterface Fourier Sources	vs0	Oigabit Oigabit Oigabit Oigabit	Ethermet0/0 Ethermet0/1 Ethermet0/2 Ethermet0/3		default virtual	ientior						
	ICMP回	應請	「求)以執行	·快速	記定駁	證。						
Configuration Montoring Seck Se	Forward Retrest Select Dy:	Pelp Configuratio	on bures 💽 Belect Criteria: 🖡	-100								Cisco S
File Help Configuration Monitoring Configuration G. Sensor Setup G. Sensor Setup Monitoring Configuration Configuratio Configur	Forward Reteat	Pelp Configuration All Eignat SubSig ID	on hures 💽 Belect Criteria: 🗍 Name	NUA- •	Action	Sevently	Fidelity Rating	Туре	Engine	Refired	•	Select A
Configuration Mattering Deck Configuration Mattering Deck Configuration	Forward Reteat	Pelp Configuration All Signat SubSig ID 2	on hures 💌 Belect Onteria: 🗍 Name TCP Drop - Ungent Pointer Wil.	NUA	Action Modify Packet I	Seventy Informatio.	Fidelity Rating 100	Type Default	Engine	Retired		Select A
The Help Configuration Config	Forward Reteat Signsture Belect By: Sig ID 1330 1330	P Help Configuratio All Signal SubSig ID 2 11	Name TCP Drop - Urgent Pointer Wil. TCP Drop - Urgent Pointer Wil.	Non- Yes	Action Modify Packet I. Deny Packet In	Seventy Informatio	Fidelity Rating 100 100	Type Default Default	Engine Normalizer Normalizer	Retired No		Select A NSDB LJ
Aliperation Aliperation Aliperation Aliperation Aliperation Aliperation Aliperation Aliperation Aliperatic Configuration Aliperatic Configuration Aliperatic Configuration	Forward Reteat	P Help Configuratio All Signat SubSig ID 2 11 9	n hures Belect Ordenia: Name TCP Drop - Ungent Pointer WI. TCP Drop - Timestamp Not A. TCP Drop - Data in SYMACK.	No Yes	Action Modify Packet I Deny Packet In Deny Packet In	Seventy Informatio Informatio	Fidelity Rating 100 100	Type Default Default	Engine Normalizer Normalizer	Retired No No	-	Select / NSDB LJ
Re Help Configuration Montoring Back Configuration Sheet Sheetwork	Forward Retreat Signature Signature Signo 1330 1330 1330	Peep Configuration All Signal SubSig ID 2 11 9 3	on Name CP Drop - Urgent Pointer WI. TCP Drop - Data in SYNACK TCP Drop - Data in SYNACK TCP Drop - Data in SYNACK	No Yes Yes	Action Modify Packet I Deny Packet In Deny Packet In	Severity Informatio Informatio Informatio	Fidelity Rating 100 100	Type Default Default Default	Engine Normalizer Normalizer Normalizer	Retired No No No	-	Crisce S Select/ NSDB Li Add Clone
Alip Alip Configuration Montoring Back Configuration Astrono Setup	Forward Reteat Reteat Belect by: 5 g (D) 1330 1330 1330	P Help Configuratio All Eignat SubSig ID 2 11 9 3	on hures Select Onteria: Name TCP Drop - Urgent Pointer WI. TCP Drop - Data in SYNACK TCP Drop - Data in SYNACK TCP Drop - Bad Option List MVIR Ench Denois	NOA-	Action Modity Packet I Deny Packet In Deny Packet In Deny Packet In	Severity Informatio Informatio Informatio Informatio	Fidelity Rating 100 100 100	Type Default Default Default Default	Engine Normalizer Normalizer Normalizer Normalizer	Retired No No No No		Select A NSDB L Add Clone Edit
Rev Help Configuration Monitoring Configuration Monitoring Configuration Sensor Setup Set	Forward Reheat Forward Reheat Signature Select by 1330 1330 1330 1330 1330	P Help Configuratio All Dignate SubSig ID 2 11 9 3 0 0	on Name Name TCP Drop - Urgent Pointer Wi. TCP Drop - Timestamp Not A. TCP Drop - Data in SYNACK TCP Drop - Data in SYNACK TCP Drop - Bad Option List ICMP Ecto Reply	NoA-	Action Modify Packet IL Deny Packet In. Deny Packet In. Deny Packet In. Produce Alert	Severity Informatio Informatio Informatio High	Fidelity Rating 100 100 100 100	Type Default Default Default Default Tuned	Engine Normalizer Normalizer Normalizer Normalizer Adomic IP	Retired No No No No No	-	Cisce S Select A NSDB LJ Add Cione Edit
Re Help Rec	Forward Reteat Signature S	P Hep Configuratio All Eignat SubSig ID 2 11 9 3 0 0 0	n hures Belect Oriteria: Name TCP Drop - Uspert Pointer WI. TCP Drop - Distantism NMA. TCP Drop - Bad Option List TCP Drop - Bad Option List NCMP Echo Reply KCMP Host Ukreachable	NoA	Action Modity Packet II. Deny Packet In. Deny Packet In. Deny Packet In. Produce Alert Produce Alert	Seventy Informatio Informatio Informatio High High	Fidelity Rating 100 100 100 100 100	Type Default Default Default Default Tuned Tuned	Engine Normalizer Normalizer Normalizer Normalizer Adomic IP Adomic IP	Retired No No No No No No		SelectA SelectA NSOB U Add Clone Eda
File Help Configuration G Sensor Setup G Sensor Setup G Sensor Setup G Centificates Susers G Literface Configuration Fontentaces Fontentac	Forward Reteat	P Help Configuratio All Eignat SubSig ID 2 11 9 3 0 0 0 0	n Name Name TCP Drop - Urgent Pointer VII. TCP Drop - Timestamp Not A. TCP Drop - Data in SYNACK TCP Drop - Data in SYNACK	NoA	Action Modify Packet I Deny Packet In Deny Packet In Produce Alert Produce Alert Produce Alert	Seventy Informatio. Informatio. Informatio. Informatio. High High High	Fidelity Rating 100 100 100 100 100 100 100	Type Default Default Default Default Tuned Tuned Tuned	Engine Normalizer Normalizer Normalizer Adomic IP Adomic IP Adomic IP	Retired No No No No No No No		Cesce S Select A NSDB LJ Add Ctone Edit Enable Disable
Rev Help Configuration Monitoring Beck Configuration Monitoring Beck	Forward Reteat Reteat Signature Select By: Sign D 1330 1330 1330 1330 1330 1330 1330 133	P Help Configuratio All Eignat SubSig ID 2 11 9 3 0 0 0 0 0 0	n Name Name TCP Drop - Urgent Pointer WI. TCP Drop - Data in SrNACK TCP Drop - Data in SrNACK TCP Drop - Data in SrNACK TCP Drop - Data Option List KCMP Echo Reply ICMP Host Unreschable ICMP Source Quench ICMP Redirect	No Yes Yes Yes Yes Yes Yes Yes Yes	Action Modify Packet I. Deny Packet In. Deny Packet In. Deny Packet In. Produce Act Produce Act Produce Act Produce Act	Severity Informatio Informatio Informatio Informatio High High High High	Fidelity Rating 100 100 100 100 100 100 100 100	Type Default Default Default Default Tuned Tuned Tuned	Engine Normalizer Normalizer Normalizer Normalizer Adomic IP Adomic IP Adomic IP Adomic IP	Retired No No No No No No No No No		Select A Select A NSDB LJ Add Clone Edit Enable Disable
Rev Help Configuration Montoring Beack Configuration Montoring Beack Sensor Setup Sensor Setup	Forward Retear Signature Select By: Sig ID 1330 1330 1330 1330 1330 1330 1330 2000 200	A Help Configuration All Eignat SubSig ID 2 11 9 3 0 0 0 0 0 0 0 0	n Name Name TCP Drop - Urgent Pointer VM. TCP Drop - Timestamp Not A. TCP Drop - Data in SrNACK: TCP Drop - Timestamp - Data in SrNACK: TCP Drop - Data in SrNACK:	No Yes Yes Yes Yes Yes Yes Yes Yes	Action Modify Packet I Deny Packet In Deny Packet In Deny Packet In Deny Packet In Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert	Severity Informatio Informatio Informatio High High High High High High	Fidelity Rating 100 100 100 100 100 100 100 100 100	Type Default Default Default Default Tuned Tuned Tuned	Engine Normalizer Normalizer Normalizer Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP	Retired No No No No No No No No No		Select A NEOB L Add Clone Edit Enable Disable Actions Restore De
Rev Help Configuration Monitoring Beack Monitoring Beack Sensor Setup Sensor Setup Sensor Setup Setup Sensor Setup Se	Forward Reteat Reteat Signature Select By: Sign D 1330 1330 1330 1330 1330 1330 1330 133	A Help Configuration All Eignat SubSig ID 2 11 9 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	n Name Name TCP Drop - Urgent Pointer WI. TCP Drop - Data in SrNACK TCP Drop - Data in SrNACK TC	Non- Personal Provided Allowing Allowin	Action Modify Packet I. Deny Packet In. Deny Packet In. Deny Packet In. Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert	Severity Informatio Informatio Informatio Informatio High High High High High High High High	Fidelity Rading 100 100 100 100 100 100 100 100 100 10	Type Default Default Default Default Tuned Tuned Tuned Tuned Tuned Default	Engine Normalizer Normalizer Normalizer Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP	Retired No No No No No No No No No No No		Cesco S Select A NSDB LJ Add Clone Edit Enable Disable Actions Restore Del
Arabite Engine Analogy Analog	Forward Reteat Select By: 1330 1330 1330 1330 1330 1330 1330 133	All Eignat SubSig ID 2 11 9 3 0 0 0 0 0 0 0 0 0 0 0 0 0	District Criteria: Name Name TCP Drop - Urgent Pointer Will, TCP Drop - Data in SYNACK, TCP Drop - Data in SYNACK, TCP Drop - Bad Option List KCMP Point Chreachable ICMP Factor Reput ICMP Factor Reput ICMP Echo Reput ICMP Time Exceeded for a D ICMP Pacenter Problem on D	NUA- Enabled No Yes Yes Yes Yes Yes Yes No No No	Action Modify Packet I. Deny Packet In. Deny Packet In. Deny Packet In. Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert	Seventy Informatio Informatio Informatio Informatio High High High High High Informatio	Fidelity Rading 100 100 100 100 100 100 100 100 100 10	Type Default Default Default Default Tuned Tuned Tuned Tuned Tuned Default Default Default	Engine Normalizer Normalizer Normalizer Normalizer Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP	Retired No No No No No No No No No No No No No		Cesce S Select A NEDE Li Add Clone Edit Enable Disable Actions Restore Der
A A	Forward Reteat Signature Select By: Sig ID 1330 1330 1330 1330 1330 1330 1330 133	P Help Configuration All Eignat SubSig ID 2 11 3 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Anne Belect Ordenia: Name TCP Drop - Usgent Pointer WI. TCP Drop - Usgent Pointer WI. TCP Drop - Bad Option List TCP Drop - Bad	No Yes Yes Yes Yes Yes Yes Yes Yes No No	Action Modify Packet I. Deny Packet In. Deny Packet In. Deny Packet In. Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert	Seventy Informatio Informatio Informatio High High High High High High High High	Fidelity Fading 100 100 100 100 100 100 100 100 100 10	Type Default Default Default Default Tuned Tuned Tuned Tuned Tuned Default Default Default Default	Engine Normalizer Normalizer Normalizer Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP Adomic IP	Retired No No No No No No No No No No No No No		Cesco S Select A NSCR Lo Add Clone Edit Enable Disable Actions Restore Del Deside
Tare Help Configuration Mandoring Beak Mandoring Beak Sensor Setup	Forward Retear Signature Select By: Sig ID 1330 1330 1330 1330 1330 1330 1330 133	All Eignat SubSig ID 2 11 9 3 0 0 0 0 0 0 0 0 0 0 0 0 0	on Name Name TCP Drop - Urgent Pointer VM. TCP Drop - Timestamp Not A. TCP Drop - Data in SYNACK TCP Drop - Data in SYNACK	Non- Enabled No Yes Yes Yes Yes Yes Yes No	Action Modify Packet II Deny Packet III Deny Packet III Deny Packet III Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert Produce Alert	Severity Informatio . Informatio . Informatio . High High High High High High High High	Fidelity Rating 100 100 100 100 100 100 100 100 100 10	Type Default Default Default Default Tuned Tuned Tuned Tuned Tuned Default Default Default	Engine Normalizer Normalizer Normalizer Adomic IP	Retired No No No No No No No No No No No No No		Select A NEOB U Add Cloce Edit Disable Actions Restore Der Conde

.

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。

Value			
2004			
0			
High			
100			
0			
Signature Name: ICMP Echo	Request		
Alert Notes:			
User Comments:			
Alert Traits:	<u></u>		
Release.			
Atomic IP			
 Fragment Status: Specify Layer 4 Protocol: 	Request Block Connection Request Block Host Request Snmb Trac		
	🛛 🔳 Layer 4 Protocol:	ICMP Protocol	
		Specify ICMP Sequence:	No 💌
		Specify ICMP Type:	Yes 👻
			ICMP Type: 8
		Specify ICMP Code:	No v
		Specify ICMP Identifier:	No
		Specify ICMP Total Length:	No 👻
	Value 2004 0 High Image: CMP Echo Alert Notes: User Comments: Alert Traits: Alert Traits: Exert Action: Fragment Status: Stat	Value 2004 0 High Image: Incomplete cho Request Alert Notes: Alert Notes: Alert Traits: Alert Traits: Alert Traits: Alert Traits: Event Action: Produce Alert Request Block Host Reques	Value 2004 0 High

<u>設定WLC</u>

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

Cinco Statema	A CONTRACTOR OF THE OWNER	Service and the service of the	A Section States	un bring and	And the second second	Save Co	nfiguration f	ing Logout Refresh
A. A.	MONITOR WLAN	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security 👱	CIDS Sensor Add						< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Index	1.	_					
MAC Filtering Disabled Clients User Login Policies AP Policies	Server Address	443						
Access Control Lists	Username	controller						
Network Access Control	Password	•••••						
IPSec Certificates CA Certificate ID Certificate	Confirm Password							
Web Auth Certificate Wireless Protection	Query Interval	15 500	onds					
Policies Trusted AP Policies Roque Policies	State	S						
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hash)	1662E996362A9	41EF08899A7C	1645F5C856A	8842 40 he	x chars		
Web Login Page								
CIDS Sensors Shunned Clients								

3. 檢查IPS感測器和WLC之間的連線狀態。

Conta Statute								Ping Logout R
A A.	MONITOR WI	LANS CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMM	ANDS HELP		
Security	CIDS Sensors	List						New
AAA	Index	Server Address	Port	State	Query Interval	Last Query (count)		
RADIUS Authentication RADIUS Accounting Local Net Users MAC Ribering Disabled Clients User Login Policies AP Policies	1	192.168.5.2	443	Enabled	15	Success (6083)	Ostail Semone	
Access Control Lists								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Palicies Trutsbed AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Simmary Client Exclusion Policies AP Authentication Nanagement Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

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。

Cores Deserves									Save Configu	ration Ping	Logout Refre
A.A. MON	NETOR WEANS C	ONTROLLER WI	RELESS SECUR	ITY MANAGEMENT	COMMANDS	HELP					
WLANS WL	ANs > Edit								1	< Back	Apply
WLANS WL WLANS AP Groups VLAN WL	AN ID AN SSID	1 IPS									
Ger	veral Policies						Security Policies				
R	adio Policy	All	*				IPv6 Enable				
A	dmin Status ession Timeout (secs)	Enabled					Layer 2 Security	WPA1+WPA2 MAC Filtering	×		
Q W	wality of Service (QoS)) Silver (best effo	rt) 💌				Layer 3 Security	None	v		
71	920 Phone Support readcast SSID	Client CAC Li	mit 🗋 AP CAC Li	nt				🔛 Web Policy *			
A E	llow AAA Override xternal Policy Validatio	n Cnabled					* Web Policy cannot be	used in combination	with IPsec		
¢	Sent Exclusion	Enabled **	600 Timeout Value (se) (3)			** When client exclusion	n is enabled, a timec require administratio	out value of		
D	HCP Server	🖸 Override					reset excluded clients)				
D	HCP Addr. Assignment	Required									
11	nterface Name	management V	1								
M	IFP Version Required IFP Signature	1									
G	eneration -REAP Local Switching										
	H-REAP Local Switchin	g not supported wit	h IPSEC, L2TP, PPT	P, CRANITE and FORT	TRESS authenticat	ions.					
CIS	CO Client ension (CCX)										
Vers	sion 1E	Enabled									
Airo	net IE										
Grat	tuitous Probe Response										
Rad	lius Servers										
		Authentication Se	rvers Account	ing Servers							
\$	erver 1	1P:10.1.1.12, Po	rt:1812 👻 none	*							

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。

Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	Peop Peop
Norried Attackers Notwork Blocks Notwork Blocks Notwork Blocks Notwork Blocks Notworks	Active Host Blocks
SP & Support Information Statistics Statistics System Information	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 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。

Cores Bremers	HOUTOD		004/7801158	w1961 666	SECURITY.	MANAGEMENT		100
Security	CIDS Shur	n List	CONTROLLER	WINELESS	SECONT	MPRE-UEWER1	0000000	HED?
General RADBUS Authentication	Re-sync		at NAC Address	Expire	Sec	or IP / Index		
RADIUS Accounting Local Net Users	10.10.99.21	1 00	-40:96:ad:0d:1b	326979296	192.	168.5.2 / 1		
MAC Filtering Disabled Clients User Login Policies AP Policies								
Access Control Lists								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

被新增到「客戶端排除」清單中。

A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS SE	CURITY M	ANAGEMENT C	OMMANDS HEU	p	
Monitor	Excluded	Clients							
Summary	Search by	MAC add	iress	Sear	rch				
Statistics Controller	Client MA	C Addr	AP Name	AP MAC Adde	WLAN	Туре	Exclusion Reas	on Port	
Wireless	00:40:95:4	106:06:1b	AP1242-2	00:14:15:59:3e:1	0 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。

A.A.	MON	ITOR WLAN	IS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Management	32	14:41:00 2006	Rogue AP : 00:15: no:0(802.11b/g)	c7:02:03:c2 d with R551: -03	etected on t and SNR: 6	lase Radio MAC :	00:14:1b:59:3	e:10 Interface
iummary	33	Tue Apr 11 14:40:16 2006	New client at 10.3	0.99.21 requ	ested to be	shunned by Sens	or at 192.168.	.5.2
NMP General SNMP V3 Users	34	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85: no:0(802.11b/g)	54:de:5d rem	oved from B	ase Radio MAC :	00:14:1b:59:3e	e:10 Interface
Communities Trap Receivers Trap Controls	35	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85: no:0(802.11b/g)	54:de:Se rem	oved from B	ase Radio MAC :	00:14:1b:59:3e	e:10 Interface
Trap Logs	36	Tue Apr 11 14:39:44	Reque : 00:05:85: no:0/802.11b/a)	54:de:Sf remo	wed from B	ase Radio MAC :	00:14:1b:59:3e	:10 Interface

件生成消息日誌。

Core Brancos	MONITOR WLA	Ns CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Management	Message Logs						
Summary SNMP	Message Log L	evel Significant	System events	*			
General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs HTTP	Tue Apr 11 14/56 00:40:96:ad:0d:1 10.10.99.21 Tue Apr 11 14:55: admin user "admin Mon Apr 10 13:11 mmDbMgmtVlanPv NULL pointer. Mon Apr 10 13:10	01 2006 [SECURITY b to exclusion list as 59 2006 [SECURITY 06 2006 [CRITICAL ortUpdate() @ mm_d 158 2006 [CRITICAL] mm_listen.c 3/ a result of an ID] asa.c 661: Aut] osapi_sem.c 7 r.c:982: ERROR] timerlib.c 442:	638: Adding IS shun event f thentication suc 77: : '(dbMead)->n Task 3227309	for Coeeded for nutex' is a 152 unable to		
Teinet-SSH Serial Port	acquire timer lock Mon Apr 10 13:10	58 2006 [CRITICAL] osapi_sem.c 7	77: csepiBsnTi	merCreate()		
Local Management Users	Mon Apr 10 13:10 acquire timer lock	ERROR: UmerSema 157 2006 [CRITICAL 57 2006 [CRITICAL	is a NULL pointe] timerlib.c 442:] osasi sem c 7	r. Task 3227309 77: anatiBanTi	52 unable to		
User Sessions	@ timerlib.c:442:1 Mon Apr 10 13:10	ERROR: 'timerSema' 157 2006 [CRITICAL	is a NULL pointe] hwutils.c 2014	r. Security Mod	ule not found		
Sysleg	Mon Apr 10 13:10	56 2006 [CRITICAL] bootos.c 825:	Starting code			
Message logs							

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。

Winfingerprint 0.6.2			
Input Options C IP Range C IP List Single Host C Neighborhood IP Address: 10-1.1.12	Scan Options © Domain C Active Director Win32 OS Version Users Null IPC\$ Sessions S Service NetBIOS Shares Disks Date and Time Group Ping Host(s) RPC Bindin	ry C WMI API	Scan Exit Clear Save Help
General Options Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conne P Address: 10.11.12 NAC-AC-3 Computername: WORKGROUP/NAC- ID: S-1-5-21-790525476-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Member Server Role: NT Morkstation Role: LAN Manager Workstat		ortscan Range: 1 ortscan Range: 1 Community String: Pu	1024 1024 ublic
Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho KB824105 Windows 2000 Ho KB824105 Windows 2000 Ho KB825119 Windows 2000 Ho KB828035 Windows 2000 Ho KB828035 Windows 2000 Ho	tfix - KB329115 tfix - KB823182 tfix - KB823559 tfix - KB824105 tfix - KB824151 tfix - KB824151 tfix - KB828119 tfix - KB828035 tfix - KB828035 tfix - KB828741		-

Cisco IPS感測器中生成的事件。

Confurnation Macantoring Macantor	Obol Forward Retreak	Prep Events Vou can display the events in th on event type and/or time, selec Sihow alert events: I inf Bhow error events: I Will	e local Event Store. By default all events are displayed. To fille If the appropriate check boxes. formational IP Low IP Medium IP High arrang IP Error IP Fatal	,	
- Ditatistics	G Event Viewer				
- Provision manufactor	Tupe Ben	sorUTC TI Event ID	Events	Sie D	
	17 alerthigh:100 April	111,200 1144003216861913654	ICMP Echo Reply	2000	
	16 alerthigh:100 April	111,200 1144003216861913652	ICMP Echo Request	2004	
	19 alertiow 32 April	11,200 1144003216861913656	SMD: ADMINE Hidden Share Access Attempt	3329	
	18 alertinformat. April	111,200. 1144003210001913055	SMD. Windows Share Enumeration	3322	
	20 alertinformat April	1144003216861913660	SMB: Windows Share Enumeration	3322	
	21 entrentir April	1144003216661913665	Unable to execute a host block timeout [10.10.99.2] because blocking is disabled		
	22 alertinformals. April	111,200 1144083216861913696	TCP SYN Host Sweep	3030	
	23 alertinformals. April	1144083218861913706	TCP SYN Host Sweep	3030	
	25 alerthigh:100 April	1144003216661913712	ICMP Echo Reply	2000	
	26 error error April	111, 200 1144063216661913714	Unable to execute a host block [10.10.99.22] because blocking is disabled		
	24 alerthigh:100 April	1144083216861913710	ICMP Echo Request	2004	
	27 aletmedium April	1144003216061913715	IOS UDP Bomb	4600	
	29 aletmedium April	1144083216861913717	Back Orifice Ping	4060	
	30 aletmedium Apri	1144063216661913718	IOS UDP Bomb	4600	
	31 aletmedium April	11,200 1144003216061913719	Back Orifice Ping	4060	
	32 aletmedium April	1144083216861913720	IOS UDP Bomb	4600 . Re	hesh
	32 aletmedium Apri	e 11, 200 1144063216661913720	IDE UDP Bomb	4600 . Re Last Updated: 4/11/06 2.5	8 2

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 10.0.0/8
access-list 40.0.0/8
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#
```



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。



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

-	<u></u>	12	0	0 1	0	0		2							Cor
Home C	Configuration	Monitoring	Deck /	Forward	Search	Retresh	Save	Help							
erfaces	Contractor	× testantiaces BS ² 1 ∰ 1 Å -		64								 		 	
Lange Policy		Interface	Name	Enabled	Security Level	IP Address	Gub	met Masik	Management	MTU		 Description	ion	 	
協	Chemeto	0	outside	Yes	0	10.10.102.2	255.25	95.255.0 55.255.0	No	1500		 			-
<u></u>	Ethernetto	2		No	100				No						
VPN	Managem	er/0/0	manage	Ves	100	192.168.1.1	255.25	55 255 0	Yes	1500					
Manager															
12															
PS															
*25															
louting															
80															
ol Objects															
bel Objects															
operties															
operties															
oel Objecto Operties															
operties															
tel Objecto Toperties															
tel Objects															
oel Otgecto															
operties															
bel Objects															
oul Objects															
od Otjects															
ol Otyects															
ni Otgects															
el Objects															
ni Otgects															
on Organita operation	T Enable	ballic babween	two or more in	đerfacës wi	hich are co	unigured with	same seco	unity lervels							
ou Otaects	T" Enable	kafic kelween	bug or more in	derfaces wi	hich are co	unliquired with 1	same secu	unity levels							
bei Objects	T" Enable	kafic belween	two or more in	derfaces wi	hich are co	anfigured with s	samé sécu	urity levels	Astr		Reset				

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。

Cisco ASDM	1 for ASA - 172.16.26.2	
A A		Cesco Sosreas
Home	and guration Monitoring Black Forward Search Refresh Save Help	A. A.
-	Configuration > Security Policy > Benice Policy Rules	
Piterfaces	◆ 金 辛 (図 (図) ふ 物 総 約 () 図 (Christel Deles, C Alal Deles, C Resta Deles Deles Deles Deles	
6.	Show Rules for Interface: All Interfaces	
Security Policy	Traffic Classification	Add
100	Name Enabled Match Source Destination Service Time Range Rule Actions Description	Edt
0	B Atlenface: Inglide, Policy: Inside-policy ID9-Inside-policy ID9-Inside-policy ID9-Inside-policy	Delete
VPN		
<u>a</u>		
CSD Manager		
PS		
-23		
Routing		
Giubai Objects		
Properties		
	Da Match Do not match 🕫 Show Summary C S	how Detail
	Apply Reset Advanced	
	*admin> NA(15) 🎲 🔜 🔤	/31/06 3:02:47 PM UTC

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。

🞼 Add Service Policy R	ule Wizard - Service Policy									
Adding a new service po	plicy rule requires three steps:									
Step 1: Configure a service policy.										
Step 2: Configure the tra	Step 2: Configure the traffic classification criteria for the service policy rule.									
Step 3: Configure actior	ns on the traffic classified by the service policy rule.									
Create a service policy	y and apply to:									
Interface:	inside - (create new service policy)									
Policy Name:	inside-policy									
Description:	DS-inside-policy									
C Global - applies to) all interfaces									
Policy Name:	global-policy									
Description:										
	< Back Next > Cancel	Help								

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)	
J Tunnel Group	
FICP or ODP Destination Port	
F ID Differen Code Deinte (DOCD)	
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.	
< Back Next >	Cancel Help

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 Ad	ctions		
Protocol Inspection	Intrusion Prevention	Connection Settings	QoS)
🖂 Enekle IDO fer	this tyseffs flam.			
Mada	this traffic flow			
C Inline Mode				
In this mode as a result o	e, a packet is directed to of IPS operation.	IPS and the packet may	be dropped	
• Promiscous	Mode			
In this mode be dropped	e, a packet is duplicated by IPS.	for IPS and the original p	acket cannot	
If IPS card fails	s, then			
Permit traffic				
C Close traffic				
			< Back Finish	Cancel Help

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。

🛱 Cinco ASDM	5.1 fer ASA - 172.16	.26.2							and the second	
File Rules Si Hove	Configuration Voite	ing Eack	C C	Ch Detreals	an ?					time Stories
iterfaces	Continue C	C AAA Rules C AAA Rules C	olice Fluice El Gi Filler Rules Siller Bules	- Service Policy R:	Jies					
Security Policy	P Name	Enabled Mate	Traffic C h Bource	assification Destination	Service	Tims Range	Ru e Actions	IDS inside policy	Description	Add Edit
VTN	inside class	i De	i any	🕸 are	🖈 avy traffic		iĝi jos promiscuous, permititafio			Delete
1000 A										
Finaling Global Objects										
Properties										
	Dig Welch	Donal ma	4ch						Show Summary	C Bitow Detail
			Apply	Reset	Access	ced .		Laster		0
Configuration sh	anges saved successfi	liγ.						*admin*	NA (15)	3 7/31/06 2:54 #7 PM UTC

<u>配置用於流量檢測的AIP-SSM</u>

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。

Cisco IDM 5.0 - 172.16.26.10				. 🖉 🕻
File Help				
🐺 🔳 🗿 🗯) 💿 📍		Crise	e Statena
Configuration Montoring Dack Forw	ard i Netresh Per			
Configuration Montoring Disk Forw Configuration Image: Second Se	erd Retrect Her Network Specify the network Hostname: IP Address: Network Mask Default Route: FTP Timeout Web Server Settin IP Enable TLS/ISS Web server port	nd communication parameters for the sensor.	seconds	
		Apply Reset		
IDM is initialized successfully.	L		cisco administrator	1 1 16

2. 新增至少具有檢視器許可權的使用者。

The Help
Without Without Without Without Service Without Without Without Service Without Without Service Without Service<
Contract State Contract

3. 啟用介面。

Cisco IDM 5.0 - 172.16.26.10						
File Help						
	0 0					Casco Systems
Configuration Monitoring Back Forw	ard Retresh Help					A.A.
Configuration National Setup Configuration Attorney Configuration Attorney Configuration	erd Pretenh Hop Interfaces A sensing interface m and clicking Einable o Interface Name OrgabitEthernet071	ust be enabled and assigned 1 Disable. Media Type Yes Backplane in	o a vitual sensor befo Duplex Si Auto A	e the sensor will monitor that in beed Alternate TCP Reset Interface utb -łkónłe-	terface. You can enable/disable the available sensing interfaces by sele	Citic States
				Apply 1	Reset	
IDM is initialized successfully.					cisco adm	inistrator 6
and a second sec						

4. 檢查虛擬感測器配置。



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

Cites Statist	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Serv	sor Edit						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering	Index Server Ac	Idress	2 172.16.26.10					
Disabled Clients User Login Policies AP Policies	Port		443					
Access Control Lists	Usemani	e.	controller.					
IPSec Certificates CA Certificate ID Certificate	Password		•••••					
Web Auth Certificate	State		V					
Wireless Protection Policies	Query Int	erval	10 sec	onds				
Rogue Policies Standard Signatures Custom Signatures	Fingerpri (SHA1 ha	nt sh)	98C996984EFA74 (hash key is alre	iF0528092666C ady set)	483C458487	40 her	< chars	
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Last Quer (count)	Γ¥	Success (1400)					
Web Login Page								
CIDS Sensors Shunned Clients								

4. 檢查AIP-SSM和WLC之間的連線狀態。

And Server	MONITOR	WLANS CONTRO	OLLER WIRELES	S SECURITY	MANAGEMENT COMM	IANDS HELP		
Security	CIDS Sens	ors List						
AAA	Index	Server Add	ress Port	State	Query Interval	Last Query (count)		
RADIUS Authentication	1	192.168.5.2	443	Enabled	15	Unauthorized (1)	Detail	Remove
RADJUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	2	172.16.26.1	443	Enabled	10	Success (1444)	Detail	Estrave
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Standard Signatures Custom Signatures Signature Events Summary Client Events AP Authentication / MFP Management Preme Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

<u>向AIP-SSM新增阻止簽名</u>

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。

File Help											
Configuration Monitoring Dack F	orward Retres	n Help									Cisco Sesti
G. Sensor Setup Sensor Setup Setu	Signature Select By	Configuration	on tures 💌 Select Criteria: 🖡	-NIA- 💌							
B Q SSH B Q Centificates	Sig ID	SubSig ID	Name	Enabled	Action	Seventy	Fidelity Rating	Type	Engine	Retired	Select All
- Witting	1330	2	TCP Drop - Urgent Pointer WL.	No	Modify Packet I	informatio	100	Default	Normalizer	No	NSDØ Link
D G Interface Configuration	1330	11	TCP Drop - Timestamp Not A	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Ninterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	informatio	100	Default	Normalizer	No	Clone
- Sovers	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Eqt
Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
Ciobal Variables	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
D 9 Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	
- Signature Variables - Signature Configuration	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Alomic IP	No	Restore Default
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	
C Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Adormic IP	No	Levense.
- DEvent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	informatio	100	Default	Atomic IP	No	Activate
- Sevent Action Overrides	2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio	100	Default	Atomic IP	No	Retre
-Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Adormic 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。

Name Value	🗣 Edit Signature				iteriteriteriteriteriteriteriteriteri
Signature ID: 2064 ButSignature ID: 0 Aut Signature ID: 0 Big Fidels Rather: 100 Promissious Data: 100 Promissious Data: 100 Big Fidels Rather: 100 Avent Notes: 100 Promissious Data: 100 Big Description: Bigmature Name: ColP Ector Registed Avent Notes: 100 Provide Commenta: 100 Signature Documenta: 100 Bigeody ICMP Sequence: 100 Bigeody ICMP Code: 100 Bigeody ICMP Code: 100 Bigeody ICMP Total Length: 100 Bigeody ICMP Code: 100	Name	Value			
SubSignature ID: 0 Attert Seventy: Hugn :: Big Fidels / Halms: 100 Promissous Datts: 0 Sig Description: Signature Name: Signature Name: Signature Name: User Comments: User Comments: User Comments: 0 Response 0 Programmet Distation: Produce Vehicles Auf .: Pragment Distation: Request Bool Commentor: Big Extify Liver 4 Protocol: Signetify ICMP Type:: Big Beckly ICMP Type: Dispeckly ICMP Type: Big Beckly ICMP Type: Big Beckly ICMP T	Signature ID:	2004			
Avant Seventy: High:	SubSignature ID:	0			
Big Fideling Rading: Promissouss Delta Sig Description: Biggnature Name: MOP Ector Request User Comments: User Comments: User Comments: User Comments: Engine: Momission: Produce Vehices Aler: Produce Vehices Aler: Produce Vehices Aler: Produce Vehices Aler: Produce Vehices Aler: Produce Veh	🔶 Alert Severity:	High			
Promiscuous Detta: Sig Description: Sig Description: Sig Description: Sig Adurt Name: Sig Comments: Adurt Trads: Release: Sig Comments: Adurt Trads: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments: Sig Comments	Sig Fidelity Rating:	100			
 Sig Description: Signature Name: CMP Echo Properts Arent Nobe: User Comments: Arent Traits: Berniese: Testameter uses the Default Value. Click the icon to reditte the default value. 	Promiscuous Delta:	0			
Signalare Name: WP Esho Pequest User Comments: User Comments: Extra later Notes: Extra later Notes: Extra later Notes: Extra later Notes: Extra later Issue: Extra later Issue: Extra later Issue: Extra later Verbese Aler Request Book Connector Request Book Protocol: Expensive: Issue: Issue: Arr Issue: Request Book Connector Request Book Protocol: Issue: Issue: Request Book Protocol: Issue: Request Book Protocol: Issue: Issue: Request Book Protocol: Issue: Issue: Request Book Protocol: Issue: Book Book ISI ISMP Code: Issue: Book Book Book Book Book Book Book Boo	Sig Description:				
Alert Note::::::::::::::::::::::::::::::::::::		Signature Name: IOMP Echo	Request		
 User Comments: Alert Trade: Reisase: Reisase: Respire: Atomic IP Event Action: Produce Area Respire: Atomic IP Event Action: Produce Area Respire: Atomic IP Event Action: Produce Mode Acting Produce Book Connector Respire: Fragment Status: Respire: Specify Layer 4 Protocol: Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: Specify ICMP Type: Specify ICMP Type: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: Respire: 		Alert Notes:			
Alert Trait: Release: Image: Alert Trait: Release: Image: Ima		User Comments:	<u> </u>		
Produce Vert Halls. Preisase: Engine: Abmic IP Evend Action: Produce Verboes Avert Specify ICMP Sequence: If I avert 4 Produce Specify ICMP Type: If I avert Parameter uses the Default Value. Click the icon to restore the default value. OK Cancel Halp		Alari Traiter	<u></u>		
Preveste: 1 Atomic IP Event Action: Produce Aleft Produce Aleft Produce State Prequest Stock Connector Request Stock Connector					
Nomic P Engine: Nomic P Event Action: Produce Verbage Aleri Request Block Denotion Fragment Btabus: Any		Release:			
Preduce Vertes event Action: Produce Vertes event Action: Produce Vertes event Action: Produce Vertes event Action: Produce Vertes event Action: Preduce Block Avent Arry Fragment Bladus: Arry Pragment Bladus: Preducet Bonn Tab Producet Bo	Engine:	Alomic IP			
Fragment Status: Any Specify Layer 4 Protocol: Specify ICMP Sequence: No Specify ICMP Type: Specify ICMP Typ		Event Action:	Produce Alert Produce Verbose Alert Request Block Connector Request Block Host Perquest Book Host		
Fragment Blabus: Fragment Blabus: Specify Layer 4 Protocol: Specify ICMP Protocol: Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: Specify ICMP Code: No w Specify ICMP Code: No w Specify ICMP Total Length: No w Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Halp			< >		
Parameter uses the Default Value. Click the icon to edit the value. OK Cancel OK Cancel		Fragment Status:	Any		
CMP Protocol Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: Specify ICMP Code: No Specify ICMP Code: No Specify ICMP Code: No Specify ICMP Identifier: No Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP		Specify Layer 4 Protocol:	Yes 💌		
Specify ICMP Sequence: Specify ICMP Type: Specify ICMP Type: ICMP Type: ICMP Type: Specify ICMP Code: Specify ICMP Code: Specify ICMP Identifier: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: Specify ICMP Total Length: OK Cancel Halp			E Layer 4 Protocol:	ICMP Protocol	
Specify ICMP Type: ICMP Typ				Specify ICMP Sequence:	No
ICMP Type: ICMP Type: 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				Specify ICMP Type:	Yes
Specity ICMP Code: No Specity ICMP Identifier: No Specity ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Help			$[b] \in \{1,2,3,3,4,5,4,5,4,5,4,5,4,5,4,5,4,5,4,5,4,5$	8.8.8.8.8.8.8.8	ICMP Type:
Specify ICMP Identifier: No Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Help				Coacily ICMD Code:	
Aprices rower administer. 1980 Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Halp				Opecity ICMP Identifier	
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				Concilia I CMP Total Landth:	
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				apecity town rotal Lengin.	
Parameter uses are certain yaue. Once the icon to earl the value. Parameter uses a User-Defined Value. Click the icon to restore the default value. OK Cancel Help	Paramalar uses the D	afaultitalas. Citabilas isan la addition	unium.		
OK Cancel Help	 Parameter uses the U Parameter uses a Us 	er-Defined Value. Click the icon to rest	tore the default value.		
			OK Cancel	Help	

S Ed	lit Signature		X
	Name	Value	-
	Signature ID:	2004	
	SubSignature ID:	0	
	Alert Severity:	Informational 👻	
•	Sig Fidelity Rating:	100	
	Promiscuous Delta:	0	
Θ	Sig Description:		
		Signature Name: ICMP Echo Reguest	
		Alert Notes:	
		User Comments:	
		Alert Traits: 0	
		Release: 81	
Θ	Engine:	Atomic IP	
		Event Action: Request Block Connection Request Block Host Request Snmp Trap Reset Tcp Connection Y	
-		Eranment Status'	-
•	Parameter uses the D Parameter uses a Use	efault Value. Click the icon to edit the value. er-Defined Value. Click the icon to restore the default value.	
		OK Cancel Help	

- 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**。

Cisco IDM 5.0 - 172.16.26.10		🖬 🖉 🔀
File Help		
Configuration Monitoring Back Forward Retresh	📍 Peip	Cosco Svercas
- Deried Attackers	Active Host Blocks	
- NACIVE Host Blocks	Const. Bar address to black and Bar desides for Bulletin.	
- SPP Logging	opeciny the address to block and the duration for that block.	
- Sevents		
E 4, Support Information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable	Add
-NStatistics	1010.99.26 10.10.102.1 0.1 30 30 0 failse	Datata [
- System Information		Desete
	Refresh	
	Last Updated: 7/3	1/06 3:21:04 PM
IDM is initialized successfully.	cisco admi	nistrator 👔

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**

Configuration Monitoring	Back	Forward	Refresh	📍 Help
Cenied Attackers Active Host Blocks CActive Host Blocks CP Logging Counters Counter				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: Image: Down of Medium of High Show Network Access Controller events Select the number of the rows per page Show status events 100 • Show all events: 1 Show all events: 1 Show status events 100 • Show status events: 1 Show status events: 1 Show all events: 1 Show status events: 1 Show all events: 1 Show all events: 1 Show status events: 1 Show status events: 1 Show status events: 1 Show all events: 1 Show past events: 1 Form: 1 Show events from the following time range 1 From the oldest event forward 1 End Time (UTC) 1 1 To now: 0 1 Wew Network 0 Wew

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。

Evi	ent Viewer					
+	Туре	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
1					— Last Updated: 7/	31/06 3:22:39 PM
			<back nex<="" td=""><td>Close Help</td><td></td><td></td></back>	Close Help		

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

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。

Cinco Sentron	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication	Re-sync	. La	st MAC Address	Expire	Sens	or IP / Index		
NACTUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	10.10.99.2	6 00	:40:96:ad:0d:1b	27	172.3	16.26.10 / 2		
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MPP Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

該使用者將被新增到「客戶端排除」清單中。

A. A.	MONITOR WLAN	CONTROLLER	WIRELESS SE	CURITY MANAGEM	ENT COMMANDS H	€Þ	
Monitor Summary Statistics Controller Ports Wireless Rogue APs Known Rogue APs Rogue Clients Adhoc Rogues 802.116 Radios 802.115/g Radios Clients RADBUS Servers	Excluded Clients Search by MAC ad Client MAC Addr 00:40:96:ad:0d:1b	AP Name AP0014.6940.81ce	5ean AP NAC Addr 00:14:15:5a:16:40	WLAN UPS	Type Exclusion R 802.11a UnknownEnu	eason Port m.5 29	Detail LinkTest Disable Remove

<u> 監視WCS中的事件</u>

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」。

Cisce Wireless Control System Username: root Logout Refresh Print View												
Location - Administration - Help -												
Alarms			Select a command 💌 🐻									
Severity Eailure_Dhiect Critical Radio_ADE-AF1242AG-A/1 Critical Radio_ADE-AF1242AG-A/2 Critical Radio_ADE-AF1242AG-A/2 Critical Radio_ADE-AF1242AG-A/2 Critical Radio_ADE-AF1242AG-A/2 Critical Radio_ADE-S1212(eD/2 Critical Radio_ADE-S1212(eD/2 Critical Radio_ADE-S1212(eD/2 Critical Radio_ADE-S1212(eD/2 Critical Radio_ADE-S1212(eD/2) Critical AP_ADE-S1212(eD/2) Critical AP_ADE-S1212(eD/2)	Renter	Date/Time 6/1/06 9:02 AM 6/1/06 9:02 AM 7/21/06 1:51 PM 7/21/06 1:51 PM 7/21/06 1:51 PM 7/21/06 1:51 PM 7/21/06 1:52 PM 7/21/06 5:25 PM 7/21/06 5:25 PM 7/26/06 2:02 PM 7/26/06 2:02 PM	Pressance AP 'AIR-LAP1242AG-A', interface '302.11b/g' is AP 'AIR-LAP1242AG-A', interface '302.11b/g' is down. AP 'AIR-LAP1242AG-A', interface '302.11b/g' is down. AP 'aIR-1751:12:0', interface '302.11b/g' is down. AP 'aIR-160:10000000000000000000000000000000000									
	Severity Eallure_Object Ortiscal Redix AB:LAP1242AG:A/1 Cettical Redix AB:LAP1242AG:A/2 Cettical Redix BB:T5:L2:e0/2 Cettical Redix AB:25:2:E0/20:L3:L5:L2:e0/2 Cettical ReB:R2:E2:E0/20:L3:L5:L2:E0/20:L3:L5:	Alarms Alarms Cetteral Redio: ABI:ABI:2422436:AQ2 Cetteral Redio: ABI:ABI:2422436:AQ2 Cetteral Redio: ABI:25121:e0Q2 Cetteral Redio: ABI:25121:e0Q2 Cetteral Redio: ABI:25121:e0Q2 Cetteral Redio: ABI:25121:e0Q2 Cetteral AP:ABI:25121:e0Q2 Cetteral AP:ABI:252243 AP:ABI:25121:e0Q2 Cetteral AP:ABI:252243 AP:ABI:252243 AP:ABI:252 Cetteral AP:ABI:2522 AP:ABI:252 AP:ABI:25 AP:ABI:25	Operation Addressing and a second secon									

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。

Cisco Wireless Cont	rol Sy	rstem					Username: roo	t Logout	Refresh	Print \	
Monitor • Configure • Location • Administration • Help •											
Alarms		Alar	ms					Select	a commi	and	
Severity Minor			Severity	Failure Object	Owner	Date/Time	Message				
Num Cutum			Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr				
Security			Minor	Client 00:40:95: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				
Search			Minor	Client 00:40:96:ad:0d:15		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated				
		Client 100.40.96:ad.0d.1b" which which which socialized with AP 100:14:1b:5a:16.40", interface 10" is excluded. The reason code is "S(Unkinowen)".									

<u>Cisco ASA示例配置</u>

```
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
1
interface Management0/0
nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
1
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
1
class-map inside-class
match any
!
!
policy-map inside-policy
 description IDS-inside-policy
 class inside-class
  ips promiscuous fail-open
1
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 10.0.0/8
access-list 40.0.0/8
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#

<u>驗證</u>

目前沒有適用於此組態的驗證程序。

<u>疑難排解</u>

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
- <u>無線 LAN 控制器 (WLC) 常見問題</u>
- 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