无线 LAN 控制器和 IPS 集成指南

目录

简介 先决条件 要求 使用的组件 规则 思科IDS概述 <u>Cisco IDS和WLC</u>—集成概述 IDS顺宁 网络架构设计 配置Cisco IDS传感器 配置 WLC Cisco IDS传感器配置示例 为IDS配置ASA 配置AIP-SSM以进行流量检测 配置WLC轮询客户端块的AIP-SSM 向AIP-SSM添加阻塞签名 使用IDM监控阻止和事件 无线控制器中的监控客户端排除 监控WCS中的事件 Cisco ASA配置示例 思科入侵防御系统传感器示例配置 验证 故障排除 相关信息

<u>简介</u>

思科统一入侵检测系统(IDS)/入侵防御系统(IPS)是思科自防御网络的一部分,是业内首款集成有线 和无线安全解决方案。Cisco Unified IDS/IPS采用全面的安全方法 — 在无线边缘、有线边缘、广域 网边缘以及通过数据中心。当关联的客户端通过思科统一无线网络发送恶意流量时,思科有线 IDS设备会检测攻击并向思科无线局域网控制器(WLC)发送避开请求,然后将客户端设备取消关联。

Cisco IPS是基于网络的内联解决方案,旨在在恶意流量(包括蠕虫、间谍软件/广告软件、网络病 毒和应用滥用)影响业务连续性之前,准确识别、分类和阻止它们。

借助Cisco IPS传感器软件版本5,Cisco IPS解决方案将内联防御服务与创新技术相结合,以提高准确性。结果是您完全放心地提供IPS解决方案保护,而无需担心合法流量被丢弃。Cisco IPS解决方案还通过其与其他网络安全资源协作的独特能力,为您的网络提供全面保护,并提供主动的网络保护方法。

Cisco IPS解决方案通过以下功能帮助用户更自信地阻止更多威胁:

- 准确的内联防御技术 提供无与伦比的信心,能够针对范围更广的威胁采取预防措施,而不会 丢失合法流量。这些独特的技术可提供对数据的智能、自动的情景分析,并帮助确保您从入侵 防御解决方案中获得最大收益。
- 多向量威胁识别 通过详细检查第2层到第7层的流量,保护您的网络免受策略违规、漏洞攻击 和异常活动的影响。
- •独特的网络协作 通过网络协作(包括高效的流量捕获技术、负载均衡功能和对加密流量的可 视性)增强可扩展性和恢复能力。
- **全面的部署解**决方案 为所有环境提供解决方案,从中小型企业(SMB)和分支机构位置到大型 企业和服务提供商安装。
- 强大的管理、事件关联和支持服务 支持完整的解决方案,包括配置、管理、数据关联和高级 支持服务。特别是思科安全监控、分析和响应系统(MARS)可识别、隔离并建议精确删除违规元 素,以实现网络范围的入侵防御解决方案。思科事件控制系统通过使网络快速适应并提供分布 式响应来防止新的蠕虫和病毒爆发。

这些元素结合起来后,可提供全面的内联防御解决方案,让您有信心在最广泛的恶意流量影响业务 连续性之前检测并阻止它们。思科自防御网络计划要求为网络解决方案提供集成和内置的安全性。 当前基于轻量接入点协议(LWAPP)的WLAN系统仅支持基本的IDS功能,因为它本质上是第2层系统 ,并且线路处理能力有限。思科及时发布新代码,将新的增强功能包括到新代码中。版本4.0具有最 新功能,包括将基于LWAPP的WLAN系统与Cisco IDS/IPS产品系列集成。在此版本中,目标是允 许Cisco IDS/IPS系统指示WLC在从第3层到第7层的任何位置检测到攻击时阻止某些客户端访问无 线网络,该攻击涉及客户端。

<u>先决条件</u>

<u>要求</u>

确保满足以下最低要求:

- •WLC固件版本4.x及更高版本
- •需要了解如何配置Cisco IPS和Cisco WLC。

使用的组件

思科WLC

这些控制器随软件版本4.0一起提供,用于IDS修改:

- Cisco 2000 系列 WLC
- Cisco 2100 系列 WLC
- Cisco 4400 系列 WLC
- 思科无线服务模块(WiSM)
- 思科Catalyst 3750G系列统一接入交换机
- •思科无线局域网控制器模块(WLCM)

访问点

- 思科Aironet 1100 AG系列轻量接入点
- 思科Aironet 1200 AG系列轻量接入点

- 思科Aironet 1300系列轻量接入点
- Cisco Aironet 1000系列轻量接入点

管理

- Cisco Wireless Control System (WCS)
- 思科4200系列传感器
- 思科IDS管理 思科IDS设备管理器(IDM)

思科统一IDS/IPS平台

- Cisco IPS 4200系列传感器,带Cisco IPS传感器软件5.x或更高版本。
- •适用于Cisco ASA 5500系列自适应安全设备的SSM10和SSM20,带Cisco IPS传感器软件5.x
- •带Cisco IPS传感器软件5.x的Cisco ASA 5500系列自适应安全设备
- •带Cisco IPS传感器软件5.x的Cisco IDS网络模块(NM-CIDS)
- •带Cisco IPS传感器软件5.x的Cisco Catalyst 6500系列入侵检测系统模块2(IDSM-2)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

<u>规则</u>

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

<u>思科IDS概述</u>

思科IDS(版本5.0)的主要组件包括:

- •传感器应用 执行数据包捕获和分析。
- •事件存储管理和操作模块 提供违反策略的存储。
- 映像、安装和启动模块 加载、初始化和启动所有系统软件。
- •用户界面和UI支持模块 提供嵌入式CLI和IDM。
- •传感器OS 主机操作系统(基于Linux)。



传感器应用(IPS软件)包括:

- 主应用 初始化系统、启动和停止其他应用、配置操作系统并负责升级。它包含以下组件
 : Control Transaction Server 允许传感器发送控制事务,这些事务用于启用攻击响应控制器 (以前称为网络访问控制器)主阻塞传感器功能。事件存储 — 用于存储IPS事件(错误、状态 和警报系统消息)的索引存储,可通过CLI、IDM、自适应安全设备管理器(ASDM)或远程数据 交换协议(RDEP)访问。
- 接口应用 处理旁路和物理设置并定义配对接口。物理设置包括速度、双工和管理状态。
- Log App 将应用程序的日志消息写入日志文件,将错误消息写入事件存储。
- 攻击响应控制器(ARC)(以前称为网络访问控制器) 管理远程网络设备(防火墙、路由器和 交换机),以在发生警报事件时提供阻止功能。ARC在受控网络设备上创建并应用访问控制列 表(ACL),或使用shun命令(防火墙)。
- 通知应用 当由警报、状态和错误事件触发时发送SNMP陷阱。为此,通知应用使用公共域SNMP代理。SNMP GET提供有关传感器运行状况的信息。Web服务器(HTTP RDEP2服务器) 提供Web用户界面。它还提供了通过RDEP2与其他IPS设备通信的方法,使用多个Servlet来提供IPS服务。Authentication App 验证用户是否获得执行CLI、IDM、ASDM或RDEP操作的授权。
- •传感器应用(分析引擎)—执行数据包捕获和分析。
- CLI 用户通过Telnet或SSH成功登录传感器时运行的接口。通过CLI创建的所有帐户都使用 CLI作为其外壳(服务帐户除外 — 仅允许一个服务帐户)。 允许的CLI命令取决于用户的权限 。

所有IPS应用都通过称为IDAPI的通用应用程序接口(API)相互通信。远程应用(其他传感器、管理应 用和第三方软件)通过RDEP2和安全设备事件交换(SDEE)协议与传感器通信。

必须注意,传感器具有以下磁盘分区:

- Application Partition 包含完整的IPS系统映像。
- 维护分区 用于重新映像IDSM-2的应用程序分区的特殊用途IPS映像。维护分区的重新映像会 导致配置设置丢失。

• **恢复分**区 — 用于恢复传感器的特殊用途映像。通过引导到恢复分区,用户可以完全重新映像应 用程序分区。网络设置将保留,但所有其他配置都将丢失。

<u>Cisco IDS和WLC — 集成概述</u>

Cisco IDS的5.0版引入了在检测到策略违规(签名)时配置拒绝操作的功能。根据IDS/IPS系统中的 用户配置,可以向防火墙、路由器或WLC发送避开请求,以阻止来自特定IP地址的数据包。

对于适用于思科无线控制器的思科统一无线网络软件版本4.0,需要向WLC发送避开请求,以触发 控制器上可用的客户端黑名单或排除行为。控制器用于获取shun请求的接口是Cisco IDS上的命令 和控制接口。

- •控制器允许在给定控制器上配置最多五个IDS传感器。
- 每个已配置的IDS传感器都由其IP地址或限定网络名称和授权凭证来标识。
- 每个IDS传感器都可以在控制器上配置唯一的查询速率(以秒为单位)。



<u>IDS顺宁</u>

控制器以配置的查询速率查询传感器以检索所有避开事件。给定的避开请求分布在从IDS传感器检 索请求的控制器的整个移动组中。对客户端IP地址的每个shun请求对指定的超时秒数值有效。如果 超时值指示无限时间,则只有在IDS上删除了shun条目时,shun事件才会结束。即使重置任何或所 有控制器,被避开的客户端状态也会在移动组中的每个控制器上保持。

注意:IDS传感器始终决定避开客户端。控制器不检测第3层攻击。确定客户端在第3层发起恶意攻 击的过程要复杂得多。客户端在第2层进行身份验证,这足以让控制器授予第2层访问权限。

注意:例如,如果客户端分配了以前违规(被回避)的IP地址,则直到传感器超时才会取消阻止此 新客户端的第2层访问。即使控制器在第2层提供访问,客户端流量仍可能在第3层路由器上被阻止 ,因为传感器也会通知路由器避开事件。

假设客户端有IP地址A。现在,当控制器轮询IDS以查找避开事件时,IDS会将避开请求发送到IP地

址为A的控制器作为目标IP地址。现在,控制器黑色列出此客户端A。在控制器上,客户端根据 MAC地址禁用。

现在,假设客户端将其IP地址从A更改为B。在下一次轮询中,控制器将根据IP地址获取避开的客户 端列表。这一次,IP地址A仍在被回避的列表中。但是,由于客户端已将其IP地址从A更改为B(不 在被回避的IP地址列表中),因此,当控制器上达到黑名单客户端的超时时间后,会释放此IP地址 为B的客户端。现在,控制器开始允许此客户端使用新的IP地址B(但客户端MAC地址保持不变)。

因此,尽管客户端在控制器排除时间的持续时间内保持禁用状态,并且如果它重新获取其先前的 DHCP地址,则重新排除该客户端,但如果被避开的客户端的IP地址发生更改,则不再禁用该客户 端。例如,如果客户端连接到同一网络且DHCP租用超时未过期。

控制器仅支持与IDS的连接,以便客户端避开使用控制器上管理端口的请求。控制器通过传输无线 客户端流量的适用VLAN接口连接到IDS进行数据包检测。

在控制器上,Disable Clients页面显示已通过IDS传感器请求禁用的每个客户端。CLI **show**命令还显 示列入黑名单的客户端列表。

在WCS上,排除的客户端显示在Security子选项卡下。

以下是完成Cisco IPS传感器和Cisco WLC集成的步骤。

- 1. 在无线控制器所在的交换机上安装并连接IDS设备。
- 2. 镜像(SPAN)将无线客户端流量传输到IDS设备的WLC端口。
- 3. IDS设备接收每个数据包的副本并检查第3层到第7层的流量。
- 4. IDS设备提供可下载的签名文件,也可以自定义。
- 5. 当检测到攻击签名时,IDS设备生成警报,事件操作为shun。
- 6. WLC轮询IDS以获取警报。
- 7. 当检测到与WLC关联的无线客户端的IP地址的警报时,它会将客户端放入排除列表。
- 8. WLC生成陷阱,并通知WCS。
- 9. 在指定的时间段后,用户将从排除列表中删除。

<u>网络架构设计</u>



Cisco WLC连接到Catalyst 6500上的千兆接口。为千兆接口创建端口通道,并在WLC上启用链路聚 合(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					

控制器连接到Catalyst 6500上的千兆5/1和千兆5/2接口。

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传感器的感应接口可以在混杂模式下单独**运行,**或者您可以将它们配对,为内联感应模式创**建 内联接口**。

在混合模式下,数据包不会通过传感器。传感器会分析受监控流量的副本,而不是实际转发的数据 包。在混合模式下运行的优点是传感器不会影响转发流量的数据包流。

注意:体<u>系结</u>构图只是WLC和IPS集成架构的一个示例设置。此处显示的示例配置说明了IDS感应接 口在混杂模式下工作。架构<u>图显</u>示了成对在内联对模式下工作的感应接口。有关内联接口模式的详 细信息,请参阅<u>内联模式。</u>

在此配置中,假设传感接口在混杂模式下工作。Cisco IDS传感器的监控接口连接到Catalyst 6500的 千兆接口5/3。在Catalyst 6500上创建监控会话,其中端口通道接口是数据包的源,目的地是连接 Cisco IPS传感器监控接口的千兆接口。这会将所有入口和出口流量从控制器有线接口复制到 IDS,以便进行第3层到第7层检查。

```
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传感器

Cisco IDS传感器的初始配置是从控制台端口完成的,或通过将显示器和键盘连接到传感器完成的。

1. 登录设备:将控制台端口连接到传感器。将显示器和键盘连接到传感器。

2. 在登录提示符下键入用户名和密码。注意:默认用户名和密码均为cisco。首次登录设备时 ,系统会提示您更改它们。您必须先输入UNIX密码,即cisco。然后您必须输入两次新密码。 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 <u>https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet</u> (registered
customers only) to obtain a new license or install a license.

3. 在传感器上配置IP地址、子网掩码和访问列表。注意:这是IDS上用于与控制器通信的命令和 控制接口。此地址应可路由到控制器管理接口。感应接口不需要编址。访问列表应包括控制器 管理接口地址以及用于管理IDS的允许地址。

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. 现在,您可以从GUI配置IPS传感器。将浏览器指向传感器的管理IP地址。此图显示传感器配置了192.168.5.2的示例。

S Cisco IDM 5.0 - 192.168.5.2				- I I I I
File Help				
🐺 🔳 🔇 🔿	0 1			Cisco Sestens
Configuration Monitoring Back Forward	rd Retresh Hei	þ		db. db.
Configuration Monitoring Disk Porvio Image: Sensor Setup Image: Sensor Se	ed Rebech Hel Network Specify the network Hostname: IP Address: Network Mask Default Route: FTP Timeout Web Server Bettin IP Enable TLB/IS Web server port.	Activ Reset	seconds	
IDM is initialized successfully.			cisco administ	nator 🕅

5. 添加WLC用于访问IPS传感器事件的用户。

File Help						face former
Configuration Monitoring Back Forward	Retresh Help					
E Q Sensor Setup	Users					
- SAlowed Hosts	Specify the users that have	e access to the sensor. The se	rvice role is a special	ole that allows you to bypass	the CLI if needed. Only one service account is allowed.	
B Q SSH						
(0 Q Certificates	U	emame		Role	Status	I
- D'lime	cisco		Administrator		Active	Add
G Interface Configuration						
- Pinterfaces						604
- Ninterface Pairs						Delete
- NBygass						
Q Analysis Engine		0		6	7	
- Ninual Sensor		A Add User			2	
- Dolobal Variables		Usemame:	controller			
Signature Definition		Contractory.				
Signature Configuration						
- Custom Signature Wizard		User Note:	Lyewer			
Miscellaneous						
Q Event Action Rules		- Password				
- Dicvert Variables						
Sevent Action Overrides						
- Revent Action Filters		Password:				
Seneral Settings						
Eliocking Evolution		Confirm Password				
Device Login Profiles						
- Blocking Devices		i				
-NRouter Blocking Device Interfaces						
Master Blocking Device Interfaces		OK.	Cancel	Help		
C CAUD						
日出监控接口。						
Cisco IDM 5.0 - 192.168.5.2						
lie Help						t
🥥 🔳 🔇 🔘	® ?					CISCO SPETE
nfiguration Monitoring Back Forward	I Refresh Help					Abredby
Q Sensor Setup	Interfaces					
- Network	A sensing interface mus	t be enabled and assigned to a	a virtual sensor before	the sensor will monitor that in	ferface. You can enable/disable the available sensing interfaces	by selecting the row(s)
B Q SSH	and clicking Enable or D	isable.				,
B Q Certificates						
- STime		5		Alternate TCP		Select All
	Index Sector Manager	Enabled Media Hype	DUDHEX Spr	EG	Description	
- Dusers	Interface Name			Reset interface		
Susers Guterface Configuration Summerfaces	OlgabitEthernetD/D	Yes TX (copper)	Auto Au	0None		Edit
Supers Configuration Configur	Interface Name OlgabitEthemet0/0 OlgabitEthemet0/1	Yes TX (copper) No TX (copper)	Auto Au Auto Au	Reset Interface None- None-		Edit
- Dusers 9-Q Interface Configuration - Difference - Directrace Pairs - Dispass	Interface Name OlgabitEthomet0/0 OlgabitEthomet0/1 OlgabitEthomet0/2	Yes TX (copper) No TX (copper) No TX (copper)	Auto Au Auto Au Auto Au	Reset Interface None None None None		Edit

监控接口必须添加到分析引擎,如以下窗口所示

Cisco DM 5.0 - 192.168.5.2				
Configuration Montoring Dack Forward	nd Refresh	9 Нер		Cosce Sectors
 C Sensor Setup Nietwork Nietwork Hosts Q SSH Q Centificates Sittime 	Virtual Sen The sense assign an	or r monitors traffic that traverses interfaces or interface p remove interfaces (or pairs). You cannot add a new vir	airs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the tual sensor or change the virtual sensor name.	description or
Duters Critiguration Directore Configuration Directore Pairs Directore Pairs Directore Pairs Directore Flow Notifications	Name vs0	Assigned interfaces (or interface Pains) OrgabitEmemet00 OrgabitEmemet01 OrgabitEmemet02 OrgabitEmemet02	Description default virbal sensor	Edit
Analysis Engine Minual Genster Solobal Variables				

7. 选择2004签名(ICMP回应请求)以执行快速设置验证。

.

ile Help													
Configuration Montoring Dack	O Forward	Retres	n Help										Cisco Sest
3 9, Sensor Setup - Nitetwork - Nitetwork	ſ	Signature Belect By	Configurati	on 🔹 Belect Criteria: 🖡	-188								
B Q SSH B Q Centricates		Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	-	Select All
Dusers		1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	informatio	100	Default	Normalizer	No	2.	NSDB Link
Q Interface Configuration		1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No		Add
- Dinterfaces		1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No		Clone
- Notestace Pairs		1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	1.2	
Traffic Flow Notifications		2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No		Edt
Q Analysis Engine		2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No		Enable
- Mitual Sensor		2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No		Disable
Q Signature Definition		2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Adomic IP	No		
- Signature Variables		2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Alomic IP	No		Actions Restore Defa
Custom Signature W2ard Startegius		2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No		
Q Event Action Rules		2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio_	100	Default	Atomic IP	No		Criotal.
- Sevent Variables		2007	0	ICMP Timestamp Request	No	Produce Alert	informatio	100	Default	Atomic IP	No		Activate
Target Value Rating		2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio	100	Default	Adomic IP	No		Retre
Sound Action Differen		1000		1740 Information Demonst	R.L.	Free days a black	Induces all a	4.00	Darden (B)	Advancia (D)		-	10464

应启用签名,将警报严重性设置为**高**,将事件操作设置为**生成警报和请求阻止主机**,以完成此 验证步骤。

dit Signature				
Name	Value			
Signature ID:	2004			
SubSignature ID:	0			
Alert Severity:	High			
Sig Fidelity Rating:	100			
Promiscuous Delta:	0			
Sig Description:				
	Bignature Name: ICMP Echo	Request		
	Alert Notes:			
	User Comments:	<u></u>		
	Alert Traits:	<u></u>		
	Releaser	<u></u>		
Engine:	Atomic IP			
	 Fragment Status: Specify Layer 4 Protocol: 	Request Block Connection Request Block Host Request Snmp Trace		
		🕒 🔳 Layer 4 Protocol:	ICMP Protocol	
			Specify ICMP Sequence:	No
			Specify ICMP Type:	Yes 👻
				ICMP Type:
			Specify ICMP Code:	No
			Specify ICMP Identifier:	No 💌
			Specify ICMP Total Length:	No 💌
Parameter uses the D	efault Value. Click the icon to edit the	value.		
Parameter uses a Us	er-Defined Value. Click the icon to res	tore the default value.		

配置 WLC

要配置WLC,请完成以下步骤:

- 1. 配置IPS设备并准备好在控制器中添加后,选择Security > CIDS > Sensors > New。
- 添加您之前创建的IP地址、TCP端口号、用户名和密码。要从IPS传感器获取指纹,请在IPS传感器中执行此命令,并在WLC上添加SHA1指纹(不带冒号)。这用于保护控制器到IDS的轮询通信。

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 Second Land	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. 检查IPS传感器和WLC之间连接的状态。

Conce Sections								Ping Logout Re
A.A.	MONITOR WL	ANS CONTROLLER	WIRELESS	SECURITY MAN	AGEMENT COMM	ANDS HELP		
Security	CIDS Sensors	List						New
AAA	Index	Server Address	Port	State	Query Interval	Last Query (count)		
ACOUS Authentication RACOUS Accounting Local Net Users MAC Ribering Disabled Clients User Login Policies AP Policies	1	192.160.5.2	443	Enabled	15	Success (6083)	Qetail Semone	
Access Control Lists								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trustod AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summery Client Exclusion Policies AP Authentication Nanagement Prame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

4. 与Cisco IPS传感器建立连接后,请确保WLAN配置正确并启用"客户端排除"。默认客户端排除 超时值为60秒。另请注意,无论客户端排除计时器如何,只要IDS调用的客户端块保持活动状态,客户端排除就会持续。IDS中的默认阻止时间为30分钟。

Case Instant					Save Configuration Ping	Logout Refre
MONITOR WLANS	CONTROLLER WIRELESS SECURI	TY MANAGEMENT COMM	NDS HELP			
WLANS WLANS > Edit					< Back	Apply
WLANS WLAN ID	1					
AP Groups VLAN	11.9					
General Policies			Security P	Policies		
Radio Policy	All 💌		IPv6 Enab	ble 🔲		
Admin Status	Enabled		Lavar 2.5	weat awaa		
Session Timeout (se	(s) 1800		Caper 2 5	MAC Eltering		
Quality of Service (Q	oS) Silver (best effort) 💌					
WMM Policy	Disabled 💙		Layer 3 S	lecurity None	¥	
7920 Phone Support	Client CAC Limit AP CAC Lin	nit.		Web Policy *		
Broadcast SSID	Chabled					
Allow AAA Override	Enabled			For an end of the second second		
External Policy Valid	ation 🔲 Enabled		and L2TP.	licy cannot be used in combination w	in Paec	
Client Exclusion	Enabled ** 600 Timeout Value (sec	s)	** When	client exclusion is enabled, a timeout os infinity(will require administrative	t value of override to	
DHCP Server	C Override		reset exc	luded clients)		
DHCP Addr. Assignm	ent 🗹 Required					
Interface Name	management 🛩					
MFP Version Require	d 1					
MFP Signature Generation						
H-REAP Local Switch	ing 🔲					
* H-REAP Local Switt	thing not supported with IPSEC, L2TP, PPT	P, CRANITE and FORTRESS auth	intications.			
CISCO Client Extension (CCX)						
Version 1E	Enabled					
Aironet IE	2					
Gratuitous Probe Respo	nse 🔲					
Radius Servers						
	Authentication Servers Account	ing Servers				
Server 1	IP:10.1.1.12, Part:1812 V none	e				

5. 当您对网络中的某些设备执行NMAP扫描或对Cisco IPS传感器监控的某些主机执行ping操作时 ,可以触发Cisco IPS系统中的事件。在Cisco IPS中触发警报后,请转至**监控和活动主机块**以 检查有关主机的详细信息。

S Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	₹ •op
- NDeried Attackers - NAttive Rook Blocks - Nhetwork Blocks - NH - Dogsing - NEvents	Active Host Blocks Specify the address to block and the duration for that block.
Support Internation Support Internation Support Support Support Support Support	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
- pesystem information	

控制器中的Sived Clients列表现在填充了主机的IP和MAC地址。

Care Server								
Security	CIDS Shu	wLANs n List	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HEUP
AAA General RADIUS Authentication RADIUS Accounting	Re-sync	. La	ist MAC Address	Expire	Sen	ior IP / Index		
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	10.10.992	. 0	0.40196180100120	320939290	196.			
Access Control Lists								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signetures Custom Signetures Signeture Events Summary Client Exclusion Policies AP Authentication Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

到客户端排除列表。

da da	MONITOR WLANS	CONTROLLER WIRE	LESS SECURITY	MANAGEMENT CO	MMANDS HELP		
Monitor	Excluded Clients						
Summary	Search by MAC addres	\$\$	Search				
Controller	Client MAC Adde AP	Name AP NA	C Adde WLAN	Туре	Exclusion Reason	Port	
Wireless	00:40:96:ad:0d:1b AP	1242-2 00:14:	1b:59:3e:10 IPS	802.11b	UnknownEnum:5	29	Detail LinkTest Disable Remove

当客户端添加到避开列表时,会生成陷阱日志。

A.A.	MON	ITOR WLAN	s CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Management	32	14:41:00 2006	Rogue AP : 00:11 no:0(802.11b/g)	0c7:02:03:c2 0 with RSSI: -0	letected on i 3 and SNR: 6	Base Radio MAC :	00:14:1b:59:3	e:10 Interface
mmary	33	Tue Apr 11 14:40:16 2006	New client at 10	.10.99.21 requ	ested to be	shunned by Sens	vor at 192.168	.5.2
SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls	34	Tue Apr 11 14:39:44 2006	Regue : 00:0b:85 no:0(802.11b/g)	:54:de:5d rem	oved from B	lase Radio MAC :	00:14:1b:59:3	e:10 Interface
	35	Tue Apr 11 14:39:44 2006	Reque : 00:0b:85 no:0(802.11b/g)	:54:de:Se rem	oved from B	lase Radio MAC :	00:14:1b:59:3	e:10 Interface
Trap Logs	36	Tue Apr 11 14:39:44	Reque : 00:05:83	i:54:de:Sf.rem	oved from B	ase Radio MAC :	00:14:1b:59:3e	:10 Interface

件生成消息日志。

Core Statement	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management	Message Logs
Summary	Message Log Level Significant System events
General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs	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] asa.c 661: Authentication succeeded for admin user "admin" Mon Apr 10 13:11:06 2006 [CRITICAL] osepi_sem.c 777: mmCHearthUnderTitedate() @ mm_dir ::027_ERCOP: V/detacd).sem/ercor' is a
HTTP	NULL pointer. Mon Apr 10 13:10:58 2004 [COTTON] himselik c.442: Task 322230652 unable to
Telnet-SSH	acquire timer lock.
Serial Part	Mon Apr 10 13:10:58 2006 [CRITICAL] osapi_sem.c 777: osapi8shTimerCreate() @ timerlb.c:442: ERROR: 'timerSema' is a NULL pointer.
Local Management Users	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] opanic semic 277: csacibanTimer("crafter)]
User Sessions	@ timerib.c:442: ERROR: 'timerSema' is a NULL pointer.
Syslog	Mon Apr 10 13:10:57 2006 [CRITICAL] hwotes.c 2014: Security Module not found Mon Apr 10 13:10:56 2006 [CRITICAL] bootos.c 825: Starting code
Mgmt Via Wireless	
Message logs	

当在Cisco

IPS传感器监控的设备上完	成NMAP扫描时	,会在Cis	sco IPS传感	器中生成一些其	他事件。
Winfingerprint 0.6.2					1
Input Options C IP Range C IP List G Single Host C Neighborhood IP Address: 10-1-1-12	Scan Options Domain C Ac Win32 OS Version Null IPC\$ Session NetBIOS Shares Date and Time Ping Host(s) Traceroute Host	tive Directory Users S Services Disks Groups RPC Bindings	C WMI API Patch Level MAC Address Sessions Event Log Show Errors	Scan Exit Clear Save Help	
General Options Timeout for TCP/UDP/ICMP/SNMP: Retries: 3 Max Conner Max Computername: WORKGROUP/NAC-A SID: S-1-5-21-790525478-158043666 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB23182 Windows 2000 Hot KB823182 Windows 2000 Hot KB823181 Windows 2000 Hot KB823151 Windows 2000 Hot KB823035 Windows 2000 Hot KB823035 Windows 2000 Hot KB823411 Windows 2000 Hot KB824114 Windows 2000 Hot KB824141 Windows 2000 Hot KB824141 Windows 2000 Hot KB824141 Wind	5 etions: 1024 CS 7-1343024091 fix - KB329115 fix - KB823182 fix - KB823182 fix - KB824105 fix - KB82411	TCP Port	scan Range: scan Range: mmunity String:	1 1024 1 1024 public	此窗口显示在

Cisco IPS传感器中生成的事件。

To create Adactars Dents Multipe Host Blocks For displayment and status of the second in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Events in the local Events in the local Event Bhose. Bry defauld all events are displayed. To Status on events for events in the local Events i	Monitoring	O Dack Forward Re	etrech Pleas				
Copystems information Tage Benace UTC Th Events Stig ID Tope 1 Taleettringh: 100 April 11, 200. 111.4409321686191364 ICMP Echo Request 2004 18 alextingh: 100 April 11, 200. 111.44093216861913654 ICMP Echo Request 2004 18 alextingh: 100 April 11, 200. 111.44093216861913655 GMB: AdMinds Hadden Share Access Attempt 33220 18 alextinformatil. April 11, 200. 114.4093216861913655 GMB: Windows Share Enumeration 33220 18 alextinformatil. April 11, 200. 114.4093216861913655 GMB: Windows Share Enumeration 33220 21 entramet April 11, 200. 114.4093216861913765 CDP STVI Host Sheep 30302 22 alextinformatil. April 11, 200. 114.4093216861913705 CDP STVI Host Sheep 30302 23 alextinformatil. April 11, 200. 114.4093216861913705 CDP STVI Host Sheep 30302 24 alextinformatil. April 11, 200. 114.4093216861913715 ICMP Echo Repty 2004	Openied Attackers SActive Host Blocks Shrietwork Blocks DiP Logging Covers Cover Covers Covers Cover	Q. Excel Viewer	- D Yes On S	ents u can display the events in t event type and/or time, sele how alert events: how error events: W	he local Event Bore. By default all events are displayed. To filter cl file appropriate check boxes. formational P Low P Medium P High faming P Error P Fatal		
1 1 0.0113 0.0113 0.0113 0.0113 0.0113 10 alerthigh:100 April 11, 200. 114.408321688191365 ICMP Echo Request 2004 16 alerthigh:100 April 11, 200. 114.408321688191365 ICMP Echo Request 2004 16 alerthigh:100 April 11, 200. 114.408321688191365 ICMP Echo Request 2004 16 alerthigh:100 April 11, 200. 114.408321688191365 ICMP Windows Bhare Enumeration 33322 21 alertiinformali. April 11, 200. 114.408321688191366 ILMB: Windows Bhare Enumeration 33322 21 alertiinformali. April 11, 200. 114.408321688191366 ILMB: Windows Bhare Enumeration 33322 22 alertiinformali. April 11, 200. 114.408321688191306 TCP EVN Host Elwestp 3030 23 alertiinformali. April 11, 200. 114.408321688191371 ICMP Echo Rept 2009 24 alert 11, 200. 114.4083216881913715 ICMP Echo Rept 2004 29 alertinformali. April	- Soldystem Information	Tree	Renaur UTC T	Event ID	Events	Sec .	
16 aled high: 100 April 11, 200. 114 400321686191305 ICMP Echo Request 2004 19 aled:now:32 April 11, 200. 114 400321680191305 SMB: ADMIN¢ Hodon Share Access Attempt 3320 19 aled:normath April 11, 200. 114 400321680191305 SMB: ADMIN¢ Hodon Share Enumeration 3322 20 aled:normath April 11, 200. 114 400321680191305 SMB: Windows Share Enumeration 3322 21 error.mor April 11, 200. 114 400321680191306 Unable to execute a host block firmout [10 10.99.2]		17 aled high 100	April 11, 200	1144083216861913654	ICMP Echo Reply	2000	. Arrenta
11 allettion:32 April 11, 200. 114.480321686191365 SMB: ADMIN§ Hidden Share Access Attempt 3328 12 allettinformatil. April 11, 200. 114.400321686191365 SMB: Windows Share Enumeration 3322 21 allettinformatil. April 11, 200. 114.400321686191365 SMB: Windows Share Enumeration 3322 21 allettinformatil. April 11, 200. 114.400321686191366 Unable to execute a host block timesul [10.10.99.2] 3030 22 allettinformatil. April 11, 200. 114.400321686191376 TCP BYN Host Bloeke 3030 23 allettinformatil. April 11, 200. 114.400321686191371 TCP BYN Host Bloeke 3030 24 allettinformatil. April 11, 200. 114.400321686191371 TCP BYN Host Bloeke 3030 25 allettinformatil. April 11, 200. 114.400321686191371 TCM BYN Host Bloekee 3030 26 allettinformatil. April 11, 200. 114.4003216861913716 TCM BYN Host Bloekee 3030 26 allettingh:100 April 11, 200. 114.4003216861913716 TCM BYN Hos		16 alerthigh 100	April 11, 200	1144083216861913652	ICMP Echo Request	2004	
16 alettinformati. April 11, 200. 1144083216861913655 SMB: Windows Share Enumeration 3322 28 alettinformati. April 11, 200. 1144083216861913650 SMB: Windows Share Enumeration 3322 29 emmark April 11, 200. 1144083216861913660 Unable to exercise a host block timeout [10.10.09.2] 3322 22 eterinformati. April 11, 200. 1144083216861913690 TCP BYN Host Sweep 3030 23 alettinformati. April 11, 200. 1144083216861913706 TCP BYN Host Sweep 3030 24 alettingh:100 April 11, 200. 1144083216861913706 TCP BYN Host Sweep 3030 25 alettingh:100 April 11, 200. 1144083216861913712 ICMP Echo Rept 2000 26 error error April 11, 200. 1144093216861913714 Unable to execute a host block [10.10.99.22] because 2004 27 alettinetium. April 11, 200. 1144093216861913716 ICMP Echo Rept 3040 28 alettinetium. April 11, 200. 1144093216861913716 IOS UDP Bomb 4000 29 alettinetium. April 11, 200. 114409321686		19 alertics 32	April 11, 200	1144003216861913656	SMD: ADMIN\$ Hidden Share Access Attempt	3320	
20 alettinformali April 11, 200. 114409321686191366 BMB: Windows Share Enumeration 3322 21 emoranor April 11, 200. 114409321686191366 Unable to execute a host black timeout (10.10.09.2) 22 electinformalia April 11, 200. 114409321686191369 TCP BYN Host Sweep 3038 23 alettinformalia April 11, 200. 114409321686191376 TCP BYN Host Sweep 3039 25 alettingention April 11, 200. 114409321686191376 TCP BYN Host Sweep 3039 26 error.entor April 11, 200. 1144093216861913712 ICMP Echn Repty 20000 26 error.entor April 11, 200. 1144093216861913714 Under to execute a host black (10.10.99.22) because 2004 24 alettingen:100 April 11, 200. 1144093216861913716 ICMP Echn Repty 2004 27 alettingen:100 April 11, 200. 1144093216861913716 IOS UDP Bomb 4600 28 alettinedium. April 11, 200. 1144093216861913716 IOS UDP Bomb 4600 38		18 alert information	April 11, 200	1144003216061913655	SMB: Windows Share Enumeration	3322	
21 emocranor April 11, 200. 1144893216861913865 Unable to execute a host block timeout [0,10,99,2] 22 electinformatic April 11, 200. 114469321686191306 TCP SYN Host Biweep 3039 23 electinformatic April 11, 200. 114469321686191306 TCP SYN Host Biweep 3039 24 electings: host block timeout [0,10,99,2] electings: host block timeout [0,10,99,2] 3039 25 electings: host block timeout [0,10,99,2] alectings: host block timeout [0,10,99,2] 3039 26 error ener April 11, 200. 1144093216861913712 ICMP Etino Repty 2000 26 error ener April 11, 200. 1144093216861913714 Unable to execute a host block [10,10,99,22] because 2004 27 electroeter April 11, 200. 1144093216861913716 ICMP Etino Repty 2004 27 electroeter April 11, 200. 1144093216861913716 ICMP Etino Repty 2004 28 electroeter April 11, 200. 1144093216861913717 ICMP Etino Repty 2004 39 electroeter April 11, 200. 1144093216861913717 Biok Orifice Pinp 4009 39 electroeter April 11, 200. 1144093216801913718 Biok Orifice Pinp 4069		20 alert information	April 11, 200	1144003216861913660	SMB: Windows Share Enumeration	3322	
22 alektinformaß. April 11, 200. 1144003216601913096 TCP BYN Host Bweep 3030 23 alektinformaß. April 11, 200. 114400321660191370 TCP BYN Host Bweep 3030 25 alektinformaß. April 11, 200. 114400321660191371 CMB Ethon Rept 2000 26 alektings.100 April 11, 200. 1144003216601913714 Unable to execute a host block [10.10.99.22] because 2000 26 alektings.100 April 11, 200. 1144003216601913714 Unable to execute a host block [10.10.99.22] because 2004 24 alektings.100 April 11, 200. 1144003216601913716 ICLMP Ethon Request 2004 27 alektingedium. April 11, 200. 1144003216601913716 ICLMP Ethon Request 4600 29 alektings.100 April 11, 200. 1144003216601913716 ICLMP Ethon Request 4600 30 alektings.110 Intervedium. April 11, 200. 1144003216601913716 ICLMP Ethon Request 4600 31 alektingduum. April 11, 200. 1144003216601913718 ICLMP Ethon Request 4600 32 alektingduum. April 11, 200. 1144003216601913719 ICLMP Ethon Request		21 enorientir	April 11, 200	1144003216861913665	Unable to execute a host block timeout [10.10.99.2] because blocking is disabled		
23 alettinformal. April 11, 200. 11144083216861913706 TCP SYN Host Bweep 3030 25 alettingh:100 April 11, 200. 11144083216861913712 ICMP Echo Reply 2000 26 erscampr April 11, 200. 11144083216861913712 Unable to execute a host block (10.10.99.22) because 2000 26 erscampr April 11, 200. 11144083216861913716 Unable to execute a host block (10.10.99.22) because 2004 27 alettmedium. April 11, 200. 11144083216861913716 ICMP Echo Request 2004 27 alettmedium. April 11, 200. 11144083216861913716 ICMP Echo Request 4000 28 alettmedium. April 11, 200. 11144083216861913717 IDS UDP Bomb 4000 39 alettmedium. April 11, 200. 11144083216861913718 IDS UDP Bomb 4000 39 alettmedium. April 11, 200. 11144083216861913718 Bask Onfice Ping 4000 31 alettmedium. April 11, 200. 11144083216801913718 Bask Onfice Ping 4000 32 alettmedium. April 11, 200. 11144083216801913719 Bask Onfice Ping 4000 32		22 alert information	April 11, 200	1144083216861913696	TCP SYN Host Sweep	3030	
25 alettholgh:160 Agril 11, 200. 1144093216861913712 ICMP Echo Reply 2000 26 error amor April 11, 200. 1144093216861913714 Unable to execute a host block (10.10.99.22) because block (10.10.99.22) block (10.10.9		23 alert information	April 11, 200	1144083216661913706	TCP SYN Host Sweep	3030	
26 error anor April 11, 200. 1144093216861913714 Unable to execute a host block (10.10.99.22) because blocking is disabled 24 alerthigh:100 April 11, 200. 1144093216861913716 ICMP Etho Request 2004 27 alertmedium. April 11, 200. 1144093216861913716 ICMP Etho Request 2004 28 alertmedium. April 11, 200. 1144093216861913716 ICMP Etho Request 2004 28 alertmedium. April 11, 200. 1144093216861913716 ICMU Etho Request 4000 30 alertmedium. April 11, 200. 1144093216861913718 IOS UDP Bomb 4600 31 alertmedium. April 11, 200. 1144093216861913719 Back Onlice Ping 4000 32 alertmedium. April 11, 200. 1144093216861913719 Back Onlice Ping 4000 32 alertmedium. April 11, 200. 1144093216861913720 IOS UDP Bomb 4600 Refer		25 alerthigh:100	April 11, 200	1144063216661913712	ICMP Echo Reply	2000	
24 alert high:100 April 11, 200. 1144093216601913710 ICMP Etho Request 2004 27 alertmedium April 11, 200. 1144093216601913710 IOS UDP Bomb 4600 29 alertmedium April 11, 200. 1144093216601913717 Bask Onflice Pinp 4000 39 alertmedium April 11, 200. 1144093216601913718 Bask Onflice Pinp 4000 30 alertmedium April 11, 200. 1144093216601913718 Bask Onflice Pinp 4000 31 alertmedium April 11, 200. 1144093216601913718 Bask Onflice Pinp 4000 32 alertmedium April 11, 200. 1144093216601913719 Bask Onflice Pinp 4000 32 alertmedium April 11, 200. 1144093216601913720 IOS UDP Bomb 4000		26 error error	April 11, 200	1144003216061913714	Unable to execute a host block [10.10.99.22] because blocking is disabled		
27 aletmedium: Aert 11, 200. 1144093216861913715 IOS UDP Bomb 4600 28 aletmedium: Aert 11, 200. 1144093216861913717 Back Onlice Ping 4000 30 aletmedium: Aert 11, 200. 1144093216861913717 Back Onlice Ping 4000 30 aletmedium: Aert 11, 200. 1144093216861913718 IOS UDP Bomb 4600 31 aletmedium: Aert 11, 200. 1144093216861913719 Back Onlice Ping 4600 32 aletmedium: Aert 11, 200. 1144093216861913720 IOS UDP Bomb 4600		24 alerthigh:100	April 11, 200	1144083216861913710	ICMP Echo Request	2004	
29 aletmedium April 11, 200. 11144003216861913717 Back Onfice Ping 4060 30 aletmedium April 11, 200. 11144003216861913718 IOS UDP Bomb 4600 31 aletmedium April 11, 200. 11144003216861913718 IOS UDP Bomb 4600 32 aletmedium April 11, 200. 11144003216861913719 Back Onfice Ping 4600 32 aletmedium April 11, 200. 11144003216861913720 IOS UDP Bomb 4600		27 alert medium	April 11, 200	1144083216861913715	IOS UDP Bomb	4600	
30 aleftmedium April 11, 200 1144093216861913718 IOS UDP Bomb 4600 31 aleftmedium April 11, 200 1144093216861913719 Back Orticle Pinp 4060 32 aleftmedium April 11, 200 1144093216861913720 IOS UDP Bomb 4060		29 aletmedium	April 11, 200	1144083216861913717	Back Orifice Ping	4060	
31 alettmedium: April 11, 200 1144003216801913719 Back Orifice Pinp 4060 32 alettmedium: April 11, 200 1144003216801913720 IOS UDP Bomb 4600 Retin		30 aletmedium	April 11, 200	1144063216661913718	IOS UDP Bomb	4600	
32 alettmedium: April 11, 200 1144083216861913720 IOS UDP Bomb 4600 Refe		31 aletmedium	April 11, 200	1144083216861913719	Back Orifice Ping	4060	
		32 aletmedium	April 11, 200	1144083216861913720	IOS UDP Bomb	4600 .	Refresh
Last Updated: 4/11/06 2.52/						Last Updated: 4/1	1/06 2:52:40

<u>Cisco IDS传感器配置示例</u>

以下是安装脚本的输出:

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#
```



与传统的入侵检测传感器不同,ASA必须始终在数据路径中。换句话说,ASA必须在一个接口上接 收数据,在内部进行处理,然后将数据从另一个端口转发出去,而不是将流量从交换机端口传输到 传感器上的被动嗅探端口。对于IDS,请使用模块化策略框架(MPF)将ASA接收的流量复制到内部高级检测和防御安全服务模块(AIP-SSM)进行检测。



在本例中,使用的ASA已设置并传递流量。这些步骤演示如何创建将数据发送到AIP-SSM的策略。 1. 使用ASDM登录ASA。成功登录后,系统将显示ASA Main System窗口。

📫 Cisco ASDM 5.1 for ASA - 172.16.26.2	
File Rules Search Options Tools Wizards Help	
Mome Configuration Monitoring Back Forward Sea	Refresh Save Help
Device Information	Interface Status
General License	Interface IP Address/Mask Line Link Current 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 Sizewall Mode: Bender Context Mode: Sizeda	Inside 172.16.26.2/24 O up O up 3 management 192.168.1.1/24 O down O down 0 outside 10.10.102.2/24 O up O up 0
Total Easty 256 MD Total Marrony 256 MD	
VPN Status IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0	Traffic Status Connections Per Second Usage
System Resources Status CPU CPU Uzage (percent)	0.5 19 07-02
17.97.32 19.97.92	OUDP: 0 TCP: 0 Total: 0 'outside' Interface Traffic Usage (K3ps)
Memory Usage (MB) 256 192 120 17.07-32 Memory Usage (MB) 256 102 120	1 0.0 17 07:02 Input Kbps: 0 Output Kbps: 0

2. 单击页面顶部的**Configuration**。窗口切换到ASA接口的视图。

Config	San Monitoring	Deck r	orward	Search	Retresh	Save Help			
1000	Aguration + Interfaces								
		10 ES 80 4	6 9						
	Interface	Name	Enabled	Security	IP Address	Subnet Mask	Management	MTU	Description
	Citremet0/0	outside	Yes	01	0.10.102.2	255 255 255 0	No	1500	
	Ethernet0/1	Inside	Yes	1001	72.16.26.2	255 255 255 0	140	1500	
	Ethernet0/2		No				No		
	Management0/0	manage	Yes	1001	92.168.1.1	255 255 255 0	Yes	1500	

3. 单击窗口左侧的Security Policy。在结果窗口中,选择服务策**略规则选**项卡。

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. 单击Add以创建新策略。添加服务策略规则向导将在新窗口中启动。单击Interface,然后从下 拉列表中选择正确的接口,以创建一个新策略,该策略绑定到传递流量的接口之一。使用两个 文本框为策略指定名称和说明。单击Next以转到下一步。

🞼 Add Service Policy F	Rule Wizard - Service Policy								
Adding a new service p	olicy rule requires three steps:								
Step 1: Configure a service policy.									
Step 2: Configure the tr	raffic classification criteria for the service policy rule.								
Step 3: Configure actio	ins on the traffic classified by the service policy rule.								
Create a service polic	y and apply to:								
Interface:	inside - (create new service policy)								
Policy Name:	inside-policy								
Description:	DS-inside-policy								
C Global - applies t	o all interfaces								
Deliau Memor									
Policy Name.	gional-holicy								
Description:									
	< Back Next > Cancel	Help							

5. 构建新的流量类以应用到策略。构建特定类以检查特定数据类型是合理的,但在本例中,为简 单起见,选择Any Traffic。单击**Next**以继续。

🖆 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	1
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. C Use class-default as the traffic class.	
< Back Next >	Cancel Help

6. 完成以下步骤以指示ASA将流量转发到其AIP-SSM。选中Enable IPS for this traffic flow以启用 入侵检测。将模式设置为Promiscuous,以便流量的副本以带外方式发送到模块,而不是将模 块与数据流内联。单击Permit traffic以确保ASA在AIP-SSM发生故障时切换到失效开放状态。 单击Finish以提交更改。

🚰 Add Service Policy	Rule Wizard - Rule A	ctions		
Protocol Inspection	Intrusion Prevention	Connection Settings	QoS]
🔽 Enable IPS for	r this traffic flow			
Mode				1
🔿 Inline Mode				
In this mod as a result	e, a packet is directed to of IPS operation.) IPS and the packet may	be dropped	
(Promiscous	Mode			
In this mod be dropped	e, a packet is duplicated I by IPS.	l for IPS and the original p	oacket cannot	
If IPS card fails	s, then			
 Permit traffic 	:			
C Close traffic				
				-
			< Back Finish	Cancel Help

7. 现在,ASA已配置为将流量发送到IPS模块。单击顶行上的**Save**,将更改写入ASA。

🖆 Cinco ASDW	5.1 for ASA - 172,16.2	6.2							and the second	
File Rules a	Configuration Monitoring	a Eack	Conversion Gene	ch Betresit						Cisco Statues
iterisce:	● 史 平 团 自 C Access Rules	A Th IB IS I	Alcy Franco El I 🍏 I Filler Rules – G	Service Policy Ro	les					
Security Policy	Show Hules for Interio	ce: All Interfaces	Traffic C	wAI lassification			Pue tritoro		Description	Add
NAT	Name El Interface: Inside, P	Enabled Match clicy: incide policy	Bource	Destination	Bervice	Timi Ranga		OS inside poliky		Edit
NAN NAN	insitte-class	up.	🥥 any	san⊭ San⊭	🐨 any traffic		igi (os promiscuous, permitiraño			<u> </u>
CSD Hanager										
Routing										
Gibiad Objects										
Properties										
	Dig Watch	a Donal mat	dt						Show Summary	C Bitow Detail
			Αερίγ	Reset	A1996	ced				
Configuration a	hanges saved successfully							<admine [<="" td=""><td>NA (15) 📑 🔂</td><td>2 7/31/06 2:54 47 PM UTC</td></admine>	NA (15) 📑 🔂	2 7/31/06 2:54 47 PM UTC

配置AIP-SSM以进行流量检测

当ASA向IPS模块发送数据时,将AIP-SSM接口关联到其虚拟传感器引擎。

1. 使用IDM登录AIP-SSM。

Cisco IDM 5.0 - 172.16.26.10					e (
File Help					
Configuration Manfaring Back Form	and Referation 19			Cisco S	
E C Sensor Setup	Natural				
- Nietwork - NAllowed Hosts	Specify the network	and communication parameters for the sensor.			
B Q SSH					
Er & Cenncates	Hostname:	sensor			
DUsers					
D Q Interface Configuration	IP Address:	172.16.26.10			
- Sunterfaces					
Traffe Flow Notifeations	Network Mask:	255.255.255.0			
D Q Analysis Engine					
- SVirtual Sensor	Default Route:	172.16.26.1			
L-Solobal Variables					
Er 4, Signature Definition	FTP Timeout	200		seconds	
- Signature Configuration					
- Custom Signature Wizard	Web Server Setti	05	Remote Access		
- Miscellaneous	Enable TI SIGS		Telnet is not a secure access service		
B Q Event Action Rules			and is disabled by default.		
Tarpet Value Rading	Web server port	443	F Enable Teinet		
- DEvent Action Overrides					
- DEvent Action Filters					
Discharge Contract Settings					
- BBlocking Properties					
- Device Login Profiles					
- DBlocking Devices					
NRouter Blocking Device Interfaces					
Master Blocking Sensor					
D Q SNMP					
- Deneral Configuration					
Traps Configuration					
Restore Defaults					
- Rebot Sensor					
- Shutdown Sensor					
- DUpdate Sensor					
- SLicensing					
			Reset		
IDM is initialized successfully.				cisco administrator	1 16

2. 添加至少具有查看器权限的用户。

<pre>File Hete The Hete</pre>	9, Cisco ID4 5.0 - 172.16.26.10					- 0
Control There Control Th	File Help					
Original Configuration Original Configu	Configuration Montoring Each Forw	ard Refeats Hop				Casco System
Apply Reset	G Sensor Betap Sensor Sensor Sensor Sensor Sensor Sensor Sensor Sensor Sensor Sensor Sensor	Users Specify the users that have acc Userna Crisco Controller	Edit User Username: User Role: Password Password Confernt Password OK	vice role is a special role that allows you to bypass the C Administrator Vicewer	U If needed. Only one service account is allowed.	Add Edd Delate
				Apply Reset		

3. 启用该接口。

Cisco IDM 5.0 - 172.16.26.10						
File Help						
	0 0 9					Casco Systems
Configuration Monitoring Back Forw	ard Retresh Help					A.A.
Configuration National Setup Configuration Attorney Configuration Configurat	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 uto -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. 检查虚拟传感器配置。



配置WLC轮询客户端块的AIP-SSM

配置好传感器并准备好添加到控制器中后,请完成以下步骤:

- 1. 在WLC中选择Security > CIDS > Sensors > New。
- 2. 添加您在上一节中创建的IP地址、TCP端口号、用户名和密码。
- 3. 要从传感器获取指纹,请在传感器中执行此命令,并在WLC上添加SHA1指纹(不带冒号)。 这用于保护控制器到IDS的轮询通信。

```
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:7	4:F8:	52:80:92:E	BB:BC:48:	3C:45:B	4:87:6C:55					
Circo Section	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP			
Security	CIDS Sens	or Edit									
General RADIUS Authentication	Index		2								
RADIUS Accounting Local Net Users	Server Ad	dress	172.16.26.10								
Disabled Clients User Login Policies	Port		443								
AP Policies Access Control Lists	Username	,	controller								
IPSec Certificates CA Certificate	Password		•••••								
Web Auth Certificate	State										
Wireless Protection Policies	Query Int	erval	10 sec	onds							
Rogue Policies	Fingerprin	1t	90C996984EFA74	F0528092888	C483C458487	6C55 40 her	x chars				
Standard Signatures Custom Signatures	(SHA1 ha	sh)	(hash key is already set)								
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Last Quer (count)	Y	Success (1400)								
Web Login Page											
CIDS											

- Shunned Clients
- 4. 检查AIP-SSM和WLC之间连接的状态。

A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT COMM	ANDS HELP		
Security	CIDS Sens	sors List							
AAA	Index	s	erver Address	Port	State	Query Interval	Last Query (count)		
RADIUS Authentication	1	19	2.168.5.2	443	Enabled	15	Unauthorized (1)	Detail	Remov
RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	2	17	2.16.26.10	443	Enabled	10	Success (1444)	Detail	Remov
Access Control Lists									
IPSec Certificates CA Certificate ID Certificate									
Web Auth Certificate									
Wireless Protection Policies Trusted AP Policies Reque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection									
Web Login Page									
CIDS Sensors Shunned Clients									

<u>向AIP-SSM添加阻塞签名</u>

添加检查签名以阻止流量。虽然有许多签名可以根据可用工具执行此工作,但此示例创建的签名会 阻止ping数据包。

1. 选择2004**签名(ICMP回应请求)**以执行快速设置验证。

Cisco IDM 5.0 - 192,168.5.2												
File Help												
Configuration Monitoring Each For	ered Retres	n Help										Cisco Sesti
Q. Sensor Setup Sensor Setup Shitework Shitework Shitework	Select By	Configurati	on 💽 💌 Select Criteria: 🖡	-NR- ¥								
B Q SSH D Q Centicates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	÷	Select All
- DUsers	1330	2	TCP Drop - Urgent Pointer WI	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
- Sevense Pars	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	-	Edt
© Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No		Enable
Colobal Variables	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No		Disable
(3 Q Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	-	
- Signature Variables - Signature Configuration	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Atomic IP	No	-	Actions Restore Default
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	-	Contraction of the second
E Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	-	
- NEvent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	_	Activate
Contrarget value Hating Sevent Action Overrides	2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio	100	Default	Atomic IP	No		Retre
- Devent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	-	

2. 启用签名,将Alert Severity设置为**High**,并将Event Action设置为**Produce Alert**和**Request Block Host**,以完成此验证步骤。请注意,Request Block Host操作是向WLC发出信号以创建 客户端异常的关键。

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 Total Length: 100 Bigeody ICMP Total Length: 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: Request Book Book Protocol: Request Book Book Protocol: Re	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 Produce Verboes Avert Produce Verboes Avert Produce Verboes Avert Avert Produce Verboes Avert Produce Verboes Avert Produce Verboes Avert Avert Produce Verboes Avert		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			$[b] \in \{1,2,3,3,4,5,3,5,1,5,1,5,1,5,1,5,1,5,1,5,1,5,1,5,1$	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				Coocily ICMP Total Longth:	
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				×
	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 Request		
		Alert Notes:			
		User Comments:			
		Alert Traits:	0		
		Release:	81		
Θ	Engine:	Atomic IP			
		Event Action:	Request B Request B Request S Reset Top	ock Connectior	
•		Eranment Statu	e' Daw	-	<u>*</u>
•	Parameter uses the D Parameter uses a Use	efault Value. Click the icc er-Defined Value. Click th	in to edit the value. In icon to restore the defau	It value.	
			OK Cancel	Help	

- 3. 单击OK以保存签名。
- 4. 验证签名是否处于活动状态且已设置为执行阻止操作。
- 5. 单击Apply将签名提交到模块。

使用IDM监控阻止和事件

请完成以下步骤:

1. 当签名成功触发时,IDM中有两个位置可以注意这一点。第一种方法显示AIP-SSM已安装的活动块。单击顶行Monitoring。在左侧显示的项目列表中,选择"活动主机块"。每当触发ping签名时,Active Host Blocks窗口都会显示违规者的IP地址、受攻击设备的地址以及阻止生效的剩余时间。默认阻塞时间为30分钟,可调。但是,本文档不讨论更改此值。有关如何更改此参数的信息,请根据需要查阅ASA配置文档。立即删除该块,从列表中选择该块,然后单击"删除"。

Cisco IDM 5.0 - 172.16.26.10		🖬 🗖 🔀
File Help		
Configuration Monitoring Back Forward Retresh	♥ Pep	Cisco Svercos
Cherried Attackers Control Attacker	Active Host Blocks Specify the address to block and the duration for that block.	
Support Information Support Information Support Information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable	Add
- Statistics System Information	1010.99.26 10.10.102.1 0 1 20 30 0 failse	Delete
	Retesh	106321104 PM
IDM is initialized successfully.	cisco admir	nistrator 👘 🔂

查看触发签名的第二种方法使用AIP-SSM事件缓冲区。从"IDM监控"页中,在左侧的"项目"列 表中选择"事件"。系统将显示Events搜索实用程序。设置适当的搜索条件,然**后单击查看**

Configuration Monitoring Back Forward Refresh	Y Help
Denied Attackers Active Host Blocks Network Blocks Network Blocks Network Blocks Norther Statistics Support Information Statistics Norther Statistics Norther Information	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 bases. Show alert events: Informational Low Medium High Show error events: Warning Error Fatal Show Network Access Controller events Select the number of the rows per page Show status events 100 Image: Control on the sensor Show past events: To prove Image: Control on the sensor
	Show events from the following time range Start Time (UTC) From: Danuary > 01 > 197C > 00 > : 00 > : 00 > From: the oldest event toward
	End Time (UTC) C To: Uservary # 01 # 1970 # 00 # ; 00 # ; 00 # @ To now
	ViewReset

2. 然后,系统将显示事件查看器,其中包含符合给定条件的事件列表。滚动列表,查找在前面的 配置步骤中修改的ICMP回应请求签名。在"事件"列中查找签名的名称,或在"签名ID"列下搜索

	Type	Sensor UTC Time	Event ID	Events	Sig ID	Detai
1 er	rror: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 er	rror: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 al	lert.informati	July 31, 2006 3:19:16 PM U	1145383740954941574	ICMP Echo Request	2004	
4 er	rror: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 al	lert informati	July 31, 2006 3:19:46 PM U	1145383740954941597	ICMP Echo Request	2004	

3. 找到签名后,双击该条目以打开新窗口。新窗口包含有关触发签名的事件的详细信息。

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=0UT summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular alertDetails: Regular Summary: 4 events this interval ; riskRatingValue: 25 interface: ge0_1 protocol: icmp

<u>无线控制器中的监控客户端排除</u>

此时,控制器中的Sived Clients列表会填充主机的IP和MAC地址。

Case Brannes	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Re-sync IP Addres 10.10.99.24	5 La	st MAC Address :40:96:ad:0d:1b	Expire 27	Sens 172.1	or IP / Index 16.26.10 / 2		
Access Control Lists								
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 / MPP Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

用户将添加到客户端排除列表。

Loss Fernan A. A.	MONITOR WLAN	s CONTROLLER	WIRELESS SEC	URITY MANAGEME	NT COMMANDS HELP		
Monitor Summary Statistics Centroller Ports Wireless Rogue APs Rogue Clents Adhoc Rogues 802.118 Radios 802.118 Radios 802.11b/g Radios Clents RADDJS Servers	Excluded Clients Search by MAC a Client MAC Addr 00:40:96:ad:0d:1b	AP Name AP0014.6940.81ce	Searc AP MAC Addr 00:14:15:5a:16:40	MLAN IPS 0	Fype Exclusion Reaso 02.11a UnknownEnum:5	n Part 29	Detail LinkTest Disable Remove

<u>监控WCS中的事件</u>

触发AIP-SSM内块的安全事件导致控制器将违规者的地址添加到客户端排除列表。WCS中也会生成事件。

- 使用WCS主菜单中的Monitor > Alarms实用程序查看排除事件。WCS最初显示所有未清除的 警报,还在窗口左侧显示搜索功能。
- 2. 修改搜索条件以查找客户端块。在"严重性"下,选择**次要**,并将"警报类别"设置为"**安全"**。
- 3. 单击搜索。

Cisce Wireless Control System Username: root Logout Refresh Print View									
Monitor • Configure • L	ocation - Administration - Belo -								
Alarms	Alarms			Select a command 💌 GO					
Alerms Severity Critical Alarm Category All Types Search	Severity Enline_Object Critical Endio_ABE-LAP12422AG-A/2 Critical Endio_ABE-LAP12422AG-A/2 Critical AP_ABE-LAP12422AG-A/2 Critical Badio_ABE-TS121202 Critical Endio_ADE-TS121202 Critical AP_ABE-LAP12422AG-A/001431b159:41180 Critical Badio_ADE-TS1212002 Critical AP_ABE-LAP1242AG-A/001431b159:41180 Critical AP_AD012513120020 Critical AP_AD012513120020 Critical AP_AP001131551511410 Critical AP_AP0012.0493.04000131315512143160 Critical AP_AP0012.0493.04000131315512143160 Critical AP_AP0012.0493.041000131315512143160 Critical AP_AP0012.0493.041000131315512143160 Critical AP_AP0012.0493.041000131315512143160 Critical Radio_AP-acc-c3750-48-1-FE1-0-3/2 Critical Radio_AP-acc-c3750-48-1-FE1-0-3/1 Critical AP_AP-acc-c3750-48-1-FE1-0-3/00100185152140140	Dwner	Date/Time 6/1/06 9:02 AM 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 4:32 PM 7/21/06 4:33 PM 7/21/06 5:33 PM 7/25/06 5:25 PM 7/26/06 2:02 PM 7/26/06 2:02 PM	Select a command Select a command					
Coverage 0 Security 1 0 4 Controllers 1 0 0 Access Points 0 0 0									

4. 然后,"警报"窗口仅列出严重性次要的安全警报。将鼠标指向触发AIP-SSM内块的事件。特别 是,WCS显示导致警报的客户端站的MAC地址。通过指向适当的地址,WCS会弹出一个包含 事件详细信息的小窗口。单击该链接可查看其他窗口中的这些相同详细信息。

Cisco Wireless Control System Username: root Logout Refresh Print V									
Monitor - Configure - Location - Administration - Help -									
Alarms	Alarms					Select a command			
Severity		Severity	Failure Object	Owner	Date/Time	Message			
Minor		Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr			
Alarm Category Security		Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr			
(actor)		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 00:40:95:ad:0d:1b		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated			
			Client '00:40:96:ad:0: '00:14:1b:5a:16:40', i code is '5(Unknown)	21b" which was ass interface '안 is exclud /.	lociated with AP led. The reason				

<u>Cisco ASA配置示例</u>

```
ciscoasa#show run
: Saved
•
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
1
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
Т
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
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
!
1
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# **思科入侵防御系统传感器示例配置**

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
```

<u>验证</u>

当前没有可用于此配置的验证过程。

<u>故障排除</u>

目前没有针对此配置的故障排除信息。

相关信息

- 安装和使用思科入侵防御系统设备管理器5.1
- Cisco ASA 5500系列自适应安全设备 配置指南
- 使用命令行界面5.0配置Cisco入侵防御系统传感器 配置接口
- WLC配置指南4.0
- •<u>无线技术支持</u>
- 无线局域网控制器(WLC)常见问题
- 无线 LAN 控制器和轻量接入点基本配置示例
- 配置安全解决方案
- <u>技术支持和文档 Cisco Systems</u>