Guia de integração de controlador de LAN sem fio e IPS

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados **Conventions** Visão geral do Cisco IDS Cisco IDS e WLC - Visão geral da integração **Desconexão IDS** Projeto de arquitetura de rede Configurar o Cisco IDS Sensor **Configurar o WLC** Exemplo de configuração do sensor Cisco IDS Configurar um ASA para IDS Configurar o AIP-SSM para a inspeção de tráfego Configurar uma WLC para pesquisar o AIP-SSM para blocos de clientes Adicionar uma assinatura de bloqueio ao AIP-SSM Monitorar bloqueio e eventos com IDM Monitorar a exclusão do cliente em um controlador sem fio Monitorar eventos no WCS Exemplo de configuração do Cisco ASA Exemplo de configuração do sensor do sistema de prevenção de intrusão da Cisco Verificar Troubleshoot Informações Relacionadas

Introduction

O Sistema de Detecção de Intrusão (IDS) e o Sistema de Prevenção de Intrusão (IPS) da Cisco são parte da Cisco Self-Defending Network e é a primeira solução integrada de segurança de rede com e sem fio na indústria. O Cisco Unified IDS/IPS adota uma abordagem abrangente à segurança — na borda da rede sem fio, borda da rede com fio, borda da WAN e através do data center. Quando um cliente associado envia tráfego mal-intencionado através da Cisco Unified Wireless Network, um dispositivo IDS com fio da Cisco detecta o ataque e envia solicitações shun para os Cisco Wireless LAN Controllers (WLCs), que então desassociam o dispositivo cliente.

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

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

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

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

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

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

Prerequisites

Requirements

Certifique-se de atender a estes requisitos mínimos:

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

Componentes Utilizados

WLC da Cisco

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

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

Pontos de acesso

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

Gerenciamento

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

Plataformas Cisco Unified IDS/IPS

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

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

Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Visão geral do Cisco IDS

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

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



O aplicativo de sensor (software IPS) consiste em:

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

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

- Aplicativo Sensor (Analysis Engine) Executa captura e análise de pacotes.
- CLI —A interface que é executada quando os usuários fazem login com êxito no Sensor por meio de Telnet ou SSH. Todas as contas criadas através da CLI usam a CLI como shell (exceto a conta de serviço - somente uma conta de serviço é permitida). Os comandos CLI permitidos dependem do privilégio do usuário.

Todos os aplicativos IPS se comunicam entre si por meio de uma API (Application Program Interface, interface de programa de aplicativos) comum chamada IDAPI. Os aplicativos remotos (outros sensores, aplicativos de gerenciamento e software de terceiros) comunicam-se com os sensores por meio dos protocolos RDEP2 e Security Device Event Exchange (SDEE).

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

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

Cisco IDS e WLC - Visão geral da integração

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

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

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



Desconexão IDS

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

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

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

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

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

endereço MAC do cliente permanece o mesmo).

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

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

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

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

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

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

Projeto de arquitetura de rede



O Cisco WLC está conectado às interfaces gigabit no Catalyst 6500. Crie um canal de porta para as interfaces gigabit e ative a LAG (Link Aggregation, Agregação de links) na WLC.

(Cisco Controller) >show interface summary

Interface Name	Port	Vlan Id	IP Address	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

O controlador está conectado à interface gigabit 5/1 e gigabit 5/2 no Catalyst 6500.

```
cat6506#show run interface gigabit 5/1
Building configuration...
Current configuration : 183 bytes
1
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
1
interface GigabitEthernet5/2
switchport
```

```
switchport trunk encapsulation dotlg
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
1
interface Port-channel99
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

As interfaces de detecção do sensor IPS podem operar individualmente no modo Promiscutivo ou você pode combiná-las para criar interfaces em linha para o modo de detecção em linha.

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

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

Nesta configuração, supõe-se que a interface de detecção atue no modo Promiscutivo. A interface de monitoramento do Cisco IDS Sensor está conectada à interface gigabit 5/3 no Catalyst 6500. Crie uma sessão de monitor no Catalyst 6500 onde a interface do canal de porta é a origem dos pacotes e o destino é a interface gigabit onde a interface de monitoração do Cisco IPS Sensor está conectada. Isso replica todo o tráfego de entrada e saída das interfaces com fio do controlador para o IDS para inspeção de Camada 3 a Camada 7.

```
cat6506#show run | inc monitor
monitor session 5 source interface Po99
monitor session 5 destination interface Gi5/3
cat6506#show monitor session 5
Session 5
------
Type : Local Session
Source Ports :
Both : Po99
Destination Ports : Gi5/3
cat6506#
```

Configurar o Cisco IDS Sensor

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

- Faça login no equipamento:Conecte uma porta de console ao sensor.Conecte um monitor e um teclado ao sensor.
- 2. Digite seu nome de usuário e senha no prompt de login. Observação: o nome de usuário e a senha padrão são cisco. Você será solicitado a alterá-los na primeira vez em que fizer login no aplicativo. Você deve primeiro inserir a senha UNIX, que é cisco. Em seguida, você deve digitar a nova senha duas vezes.

login: cisco

```
Password:
  ***NOTICE***
  This product contains cryptographic features and is subject to
  United States and local country laws governing import, export,
  transfer and use. Delivery of Cisco cryptographic products does
  not imply third-party authority to import, export, distribute or
  use encryption. importers, exporters, distributors and users are
  responsible for compliance with U.S. and local country laws.
  By using this product you agree to comply with applicable laws
  and regulations. If you are unable to comply with U.S. and local laws,
  return this product immediately.
  A summary of U.S. laws governing Cisco cryptographic products may
  be found at:
  http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
  If you require further assistance please contact us by sending
  email to export@cisco.com.
  ***LICENSE NOTICE***
  There is no license key installed on the system.
  Please go to <a href="https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet">https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet</a> (registered
  customers only) to obtain a new license or install a license.
3. Configure o endereço IP, a máscara de sub-rede e a lista de acesso no sensor. Observação:
```

essa é a interface de comando e controle no IDS usada para se comunicar com o controlador. Esse endereço deve ser roteável para a interface de gerenciamento do controlador. As interfaces de detecção não exigem endereçamento. A lista de acesso deve incluir o endereço da interface de gerenciamento da(s) controladora(s), bem como endereços permitidos para o gerenciamento do IDS.

```
sensor#configure terminal
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#host-ip 192.168.5.2/24,192.168.5.1
sensor(config-hos-net)#access-list 10.0.0.0/8
sensor(config-hos-net)#access-list 40.0.0.0/8
sensor(config-hos-net)#telnet-option enabled
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes: ?[yes]: yes
sensor(config)#exit
sensor#
sensor#ping 192.168.5.1
PING 192.168.5.1 (192.168.5.1): 56 data bytes
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=1 ttl=255 time=0.9 ms
64 bytes from 192.168.5.1: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 192.168.5.1: icmp_seq=3 ttl=255 time=1.0 ms
--- 192.168.5.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.6/1.0 ms
sensor#
```

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

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

192.100.3.2.				
A Cloco IDM 5.0 - 192.168.5.2				S 6 🛛
File Help				
				Casco Sestems
Configuration Montoring Back Form	and Retrach He			A A.
E G. Sensor Setup	Network			
- Shiebwork	Theory and			
-SAllowed Hosts	Specify the network	and communication parameters for the sensor.		
D Q SSH				
Time	Hostname:	Bensor		
SUsers				
E 9 Interface Configuration	IP Address:	192.168.5.2		
Solinderfaces				
- Sunterface Pairs	Network Mask:	255.255.255.0		
Traffic Flow Notifications				
D Q Analysis Engine	Default Route	192160.51		
-Svinual Sensor	Energia roomana.			
-Solobal Variables	CTO Towards	[200		
E G Signature Definition	FIP TIMEOUE	1 miles		seconds
- Selanabre Confouration				
- Socution Signature Wizard	-Web Server Sets	ngs	Remote Access	
*SMiscellaneous	P Enable TLS/55	A.	and is disabled by default.	
D 9, Event Action Rules				
- Sillword Variables	Web server port.	443	M Enable Telnet	
Sent Action Oversities				
- Sevent Action Filters				
- Doneral Settings				
B Q Blocking				
- SABlocking Properties				
Blacking Devices				
-SRouter Blocking Device Interfaces				
-SCat 6K Blocking Device Interfaces				
Staster Blocking Sensor				
B Q SNMP				
Configuration				
- NAuto Update				
- Restore Defaults				
- NReboot Sensor				
- Distidown Sensor				
Dupdate Sensor				
- percenting				
		Apply	Reset	
IDM is initialized successfully.				cisco administrator 🙆

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

IPS				
4. Cises EW 5.0 - 197.168.5.7				- 0 2
File Help				
Configuration Monitoring Configuration Monitoring	? Heb			Casco Sestion
Q Sensor Setup Sensor Setup Diversork Shortwork Specify the user Q Q SSH	s that have access to the sensor. The service	role is a special role that allows you to bypass the	CLI if needed. Only one service account is allowed.	
ID Q Certificates	Usemame	Role	Status	
SUpers cisco	Adri	inistrator	Active	A00
G. Interface Configuration				Edt
- Noterfaces				
- Shreats				Delete
Traffic Flow Notifications				
E Q Analysis Engine	S Add User	X		
Dividual Sensor				
E G. Signature Definition	Usemame:	controller		
- Signature Variables				
- Signature Configuration	User Role:	Viewer		
- DCustom Signature Wizard				
D G. Event Action Rules				
- Sevent Variables	Password			
- Target Value Rating				
- NEvent Action Overrides	Passwort			
Concerning Settions				
B Q Blocking				
- Stocking Properties	Confirm Password:			
- Device Login Profiles				
- NBlocking Devices				
Cat Bic Biocking Device Interfaces				
Master Blocking Sensor	OK	Cancer Help		
m C cump				

6. Ative as interfaces de monitoramento.



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

mostra:

mosua.				
Clisco IDM 5.0 - 192,168.5.2				
File Help				
Configuration Montoring Back Forward	nd Retresh	nep		Cisco Systems
E Q. Sensor Setup I Nietwork I Nietwork B Q. SSH B Q. Centificates I Nitrine	-Vitual Sens The sensor assign and	or monitors traffic that traverses interfaces or interface pa remove interfaces (or pains). You cannot add a new vit	irs assigned to a virtual sensor. Click Edit to change the properties of the default virtual sensor. You can change the wal sensor or change the virtual sensor name.	description or
DUsers	Name	Assigned Interfaces (or Interface Pairs)	Description	Edit
B. Interface Configuration Dinterfaces Nontrace Pairs Dinterface D	vs0	Olgabili: Enemet00 Olgabili: Enemet01 Olgabili: Enemet02 Olgabili: Enemet02 Olgabili: Enemet02	default witual sensor	
Q. Analysis Engine -				

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

configuração.											
*. Cisco IDM 5.0 - 192.168.5.2											- 8 X
File Help											
Configuration Monitoring Dack Form	erd Retres	en 1980									Cisco System
Q. Sensor Setup	Select By	Configuration	on tures 💌 Select Criteria: 🖡	-NA- •							
B Q SSH B 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
() Q 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	Cione
Dinterface Pairs	1330	э	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
D Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
- Nirtual Sensor	2002	0	ICMP Source Quench	Ves	Produce Alert	High	100	Tuned	Atomic IP	No	Diversity
- Solobal Variables	2002	0	ICMP Redeert	Vec	Produce Alart	Minh	100	Tuned	Altomic ID	No	Disable
-Signature Variables	1000		TOWP POPULATION	165	P TODOUCH PRETL	r nge-	100	Tomes	Page 14 IP		Actions
- Signature Configuration	2004		ICMP Echo Request		Request Block					No	Restore Defaults
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	
G Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Adornic IP	No	University.
- 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	Adormic IP	No	Rates
- Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	

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



Configurar o WLC

Conclua estes passos para configurar a WLC:

- 1. Depois que o aplicativo IPS estiver configurado e pronto para ser adicionado ao controlador, escolha Security > CIDS > Sensors > New (Segurança > CIDS > Sensores > Novo).
- Adicione o endereço IP, o número da porta TCP, o nome de usuário e a senha que você criou anteriormente.Para obter a impressão digital do sensor IPS, execute esse comando no sensor IPS e adicione a impressão digital SHA1 na WLC (sem dois-pontos). Isso é usado para proteger a comunicação de polling de controlador para IDS. sensor#show tls fingerprint MD5: 1A:C4:FE:84:15:78:B7:17:48:74:97:EE:7E:E4:2F:19 SHA1: 16:62:E9:96:36:2A:9A:1E:F0:8B:99:A7:C1:64:5F:5C:B5:6A:88:42

Cases Systems	A work in the second second		A Marine Marine St.	with the state of the	Suid Chair Suid &	Save Co	nfiguration	Ping	Logout P	Refresh
A. A.	MONITOR WLAN	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Contraction of the		
Security 🛓	CIDS Sensor Add						< Back		Apply	
General RADIUS Authentication RADIUS Accounting	Index	1.								
Local Net Users MAC Filtering Disabled Clients	Server Address	192.168.5.2								
User Login Policies AP Policies	Port	443								
Access Control Lists	Username	controller								
Network Access Control	Password	•••••								
IPSec Certificates CA Certificate ID Certificate	Confirm Password	•••••								
Web Auth Certificate	Query Interval	15 500	onds							
Policies Trusted AP Policies	State	R								
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hash)	1662E996362A94	1EF08899A7C	1645FSCB56AI	8842 40 he	chars				
Web Login Page CIDS										
Sensors Shunned Clients										

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

Come Section								Save Configuration	Fing	Logout Re
A.A.	MONETOR WL	ANS CONTROLLER	WIRELESS	SECURITY M	ANAGEMENT COMM	WNDS HELP				
Security	CIDS Sensors	List							1	New
AAA	Index	Server Address	Port	State	Query Interval	Last Query (count)				
RADIUS Authentication	1	192.168.5.2	443	Enabled	15	Success (6083)	Detail Remove			
NADUS Accounting Local Net Users 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 Palicies Trutted AP Policies Rogue Policies Standard Signatures Signatures Events Summary Client Exclusion Policies AP Authentication Nanagement Frame Protection										
Web Login Page										
CIDS Sensors Shunned Clients										

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

Const Descent									Save Carfig	uration Ping	Logout Refre
A. A.	MONITOR WLANS CO	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP					
WLANS	WLANs > Edit									< Back	Apply
WLANS	WLAN ID	1									
AP Groups VLAN	WLAN SSID	1PS									
	General Policies						Security Policies				
	Radio Policy	All 💌					IPv6 Enable				
	Admin Status	💽 Enabled									
	Session Timeout (secs)	1800					Layer 2 Security	WFA1+WFA2	×		
	Quality of Service (QoS)	Silver (best effort)						MAC hitening			
	WMM Policy	Disabled 🐱					Laver 3 Security	None	~		
	7920 Phone Support	🖸 Client CAC Limit 📋	AP CAC Limit					Web Policy *			
	Breadcast SSID	💽 Enabled									
	Allow AAA Override	Enabled									
	External Policy Validation	n 🔲 Enabled					 Web Policy cannot be and L2TP. 	used in combination	with IPsec		
	Client Exclusion	Enabled ** 600 Timeou	t Value (secs)				** When client exclusion zero means infinity/will	s is enabled, a times require administrativ	ut value of re override to		
	DHCP Server	Override					reset excluded clients)				
	DHCP Addr. Assignment	Required									
	Interface Name	management 🛩									
	MFP Version Required	1									
	MFP Signature Generation										
	H-REAP Local Switching										
	* H-REAP Local Switching	g not supported with IPSEC	, L2TP, PPTP, C	RANITE and FORTI	RESS authentical	ions.					
	CISCO Client Extension (CCX)		_								
	Version IE	Enabled									
	Aironet IE										
	Gratuitous Probe Response										
	Radius Servers										
		Authentication Servers	Accounting	Servers							
	Server 1	IP:10.1.1.12, Port:1812	✓ none ✓								

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

host.	
Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	9 Hap
- NDeried Attackers - Notething Act Blocks - Notething Act Blocks - Notething Act Blocks - Notething - N	Active Host Blocks Specify the address to block and the duration for that block.
Support information Support information Support S	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable 10.10.99.21 10.10.99.1 0 1 10 10 0 failse

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

Core former	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shun List						
AAA General RADIUS Authentication	Re-sync	st MAC Address	Expire	Sense	r IP / Index		
RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	10.10.99.21 00	:40:96:ad:0d:1b	326979296	192.14	0.5.2/1		
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							

usuário é adicionado à lista de exclusões de

clientes.

A. A.	MONITOR WLANS	CONTROLLER	WIRELESS SEC	URITY MANAGEMENT	COMMANDS HELP		
Monitor	Excluded Clients						
Summary	Search by MAC ad	fress	Search	N			
Statistics Controller	Client MAC Addr	AP Name	AP MAC Adde	WLAN Type	Exclusion Reason	Port	
Wireless	00:40:95:ad:0d:1b	AP1242-2	00:14:15:59:3e:10	IPS 802.1	1b UnknownEnum:5	29	Detail LinkTest Disable Remove

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

A. A.	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
Management	32 14:41:00 32 006 Rogue AP : 00:15:c7:82:03:c2 detected on Base Radio MAC : 00:14:10:59:3e:10 Interfu no:0(802.11b/g) with RSSE: -83 and SNR: 6	9C6
Summary	Twe Apr 11 33 1404016 New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2 2006	
General SNMP V3 Users	Twe Apr 11 34 14:39:44 Rogue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interfa no:0(002.11b/g)	ce
SNMP V3 Users Communities Trap Receivers 35 Trap Controls	Twe Apr 11 35 14:39:44 Rogue : 00:0b:85:54:de:Se removed from Base Radio MAC : 00:14:1b:59:3e:10 Interfa no:0(002.11b/g)	ce
Trap Logs	Twe Apr 11 36 14:39:44 Regue : 00:0b:05:54:de:5f removed from Base Radio MAC : 00:14:1b:59:3e:10 Interfa med/802 11b/a)	ce

registro de mensagens também é gerado para o

Core Station	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Management	Message Logs						
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Legs HTTP Telnet-SSH Serial Port Local Management Users User Sessions Syslog	Message Log Level Tue Apr 11 14/56/01 2 00:40/96:46/06/16 to e 10:10.99.21 Tue Apr 11 14/55/59 21 admin user "admin" Mon Apr 10 13:11/05 2 mmObMgmtVlerAPortUp NUL pointer. Mon Apr 10 13:10/58 2 e timerib.cc.442: ERRO Mon Apr 10 13:10/57 2 adquire timer lock. Mon Apr 10 13:10/57 2 d timerib.cc.442: ERRO Mon Apr 10 13:10/57 2 0 timerib.cc.442: ERRO Mon Apr 10 13:10/57 2 0 timerib.cc.442: ERRO Mon Apr 10 13:10/57 2	Significant S 006 (SECURITY) 006 (SECURITY) 006 (CRITICAL) 006 (CRITICAL)	ystem events mm_ksten.c 3 result of an ID asa.c 651: Aut osapi_sem.c 7 .c:902: ERROR timerib.c 442: osapi_sem.c 7 s a NULL points timerib.c 442: osapi_sem.c 7 s a NULL points timerib.c 2014 bootos.c 825:	S38: Adding S38: Adding S shun event ! thentication su 77: ' (dbhead)->r Task 3227309 77: osapi8snT r. Task 3227309 77: osapi8snT r. : Seourity Mod Starting code.	for coseded for mutex' is a MS2 unable to imerCreate() MS2 unable to imerCreate() ule not found		
Syslog Mgmt Via Wireless Message logs	Mon Apr 10 13:10:56 2	006 [CRITICAL]	beotos.c 825:	Starting code.			

evento.

Alguns

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

subar obnous	Scan Options			Scan
C IP Range C IP List	Domain C Activ	e Directory	WMI API	scan
Single Host C Neighborhood IP Address:	₩in32 OS Version	Users 🔽	Patch Level	Exit
10.1.1.12	□ Null IPC\$ Sessions	Services	MAC Address	Clear
	I✓ NetBIOS Shares	Disks [Sessions	Save
	Date and Time	Groups 🗖	Event Log -	5970
	Ping Host(s)	Bindings	Show Errors	Help
	1 Traceroute Host			
General Options				
		TCP Portscan	Range: 1	1024
Timeout for TCP/UDP/ICMP/SNMP	s	UDP Portscan	Range: 1	1024
Retries: 3 Max Conn	ections: 1024	SNMP Commu	nity String: P	ublic
Computername: WORKGROUP\NAC	ACS			-
SID: S-1-5-21-790525478-15804364 MAC Addresses:	67-1343024091			
00096b8d51c2				
Ontob Lawals				
Patch Level: Operating System: 5.0				
Patch Level: Operating System: 5.0 Role: NT Member Server				
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta	tion			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server	tion			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment:	tion			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB292115 Windows 2000 M	tion			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hi KB823182 Windows 2000 Hi	tion tfix - KB329115 tfix - KB823182			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hi KB823182 Windows 2000 Hi KB823182 Windows 2000 Hi	tion tfix - KB329115 tfix - KB823182 tfix - KB82359			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hi KB823182 Windows 2000 Hi KB824105 Windows 2000 Hi KB824105 Windows 2000 Hi	tfix - KB329115 dfix - KB329115 dfix - KB823182 dfix - KB823159 dfix - KB824105 dfix - KB824105			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hi KB823182 Windows 2000 Hi KB824105 Windows 2000 Hi KB824105 Windows 2000 Hi KB824151 Windows 2000 Hi	tion tfix - KB329115 tfix - KB323182 tfix - KB823559 tfix - KB824151 tfix - KB824151 tfix - KB824151			
Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Worksta Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hi KB823182 Windows 2000 Hi KB824105 Windows 2000 Hi KB824105 Windows 2000 Hi KB824151 Windows 2000 Hi KB824151 Windows 2000 Hi KB825119 Windows 2000 Hi KB826232 Windows 2000 Hi KB826035 Windows 2000 Hi	tion tfix - KB329115 tfix - KB823182 tfix - KB823559 tfix - KB824151 tfix - KB824151 tfix - KB025119 tfix - KB025232 tfix - KB025035			

a janela mostra os eventos gerados no Cisco IPS Sensor.

Aguration Mentioning Denied Attackers Ductive Host Blocks Divervork Blocks DP-Logging DP	Back Forward Re	etresh Pley	vents u can display the events in t event type and/or time, sele how alert events: P in how error events: P W	he local Event Bore. Dy default all events are displayed. To file of the appropriate check boxes. formational IP Low IP Medium IP High anning IP Error IP Fatal	r	
- Statistics Stratistics	G Event Viewer					
	F Type	Sensor UTC Te	Event ID	Events	Sig ID .	
	17 alerthigh 100	April 11, 200	1144003216861913654	ICMP Echo Reply	2000	
	16 alerthigh:100	April 11, 200	1144083216861913652	ICMP Echo Request	2004	
	19 alertiow 32	April 11, 200	1144003216861913656	SMB: ADMINS Hidden Share Access Attempt	3320	
	18 alertinformati	April 11, 200	1144083216861913655	SMB: Windows Share Enumeration	3322	
	20 alertinformati	April 11, 200	1144003216861913660	SMB: Windows Share Enumeration	3322	
	21 entrentr	April 11, 200	1144003216061913665	Unable to execute a host block timeout [10.10.99.2] because blocking is disabled		
	22 alert information	April 11, 200	1144083216861913696	TOP BYN Host Sweep	3030	
	23 alert information	April 11, 200	1144083216661913706	TCP SYN Host Sweep	3030	
	25 alerthigh:100	April 11, 200	1144063216661913712	ICMP Echo Reply	2000	
	26 empriembr	April 11, 200	1144003216861913714	Unable to execute a host block [10.10.99.22] because blocking is disabled		
	24 alerthigh:100	April 11, 200	1144083216861913710	ICMP Echo Request	2004	
	27 aletmedium	April 11, 200	1144083216861913715	IOS UDP Bomb	4600	
	29 alertmedium	April 11, 200	1144063216661913717	Back Onlice Ping	4060	
	30 aletmedium	April 11, 200	1144083216861913718	IOS UDP Bomb	4600	
	31 aletmedium	April 11, 200	1144003216061913719	Back Onlice Ping	4060	
	27 212 22 20 20 20 20 20	April 11, 200	1144083216861913720	IOS UDP Bomb	4600 .	Refresh

Exemplo de configuração do sensor Cisco IDS

Esta é a saída do script de configuração da instalação:

sensor#**show config**

```
! ------
! Version 5.0(2)
! Current configuration last modified Mon Apr 03 15:32:07 2006
! ------
service host
network-settings
host-ip 192.168.5.2/25,192.168.5.1
host-name sensor
telnet-option enabled
access-list 10.0.0/8
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#
```

Configurar um ASA para IDS

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

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



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

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

📫 Cisco ASDM 5.1 for ASA - 17	2.16.26.2					imteriestesiestesies
File Rules Search Options	Tools Wizards Help					
Home Configuration	Monitoring Back	Forward Search	Refresh	Save Help		
- Device Information			-Interface Stat	us		
General License			Interface	IP Address/Mask	Line Link	Current Kbps
Host Name: ciscoasa ASA Version: 7.1(2) ASDM Version: 5.1(2)	Device Uptime:	2d 5h 24m 51s ASA5510	inside management outside	172.16.26.2/24 192.168.1.1/24 10.10.102.2/24	Oup Oup down Odown Oup Oup	3 0 0
Firewall Mode: Routed Total Flash: 256 MB	Context Mode: Total Memory:	Single 256 MB	Select an interf	ace to view input and	output Kbps	
VPN Status	Obi Tunnala: 0 0	Tunnala: 0	Connections I	Per Second Usage		
System Resources Status CPU CPU Uzage () 15 00	ercent)		1 0.6 1907.02	TCP- 0	Tatat: 0	· · · · ·
17.07.72 12.02.02						
Memory Usa	ya (MB)			race Tramic Usage (Köps		

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

5A.																
Roles Dear	Coptions To	ils Wizards	Help													(e.)(P)
5 Car	-	() ntorng	O .	Convert 1	Search	Retresh	Gave	?								Cinco Stata
•	◆ <u>·</u> ···································	anteres Eff 1 A - Pa	0.65	6 9												
y Policy	inte	face	Name	Enabled	Security Level	IP Address	Su	briet Masik	Management	MTU		Descri	ption			Add
k	Cthemet0/0		outside	Yes	0	10.10.102.2	255.2	55.255.0	No	1500	Î.					Edit
î	Ethernet0/1		knolde	Yes	1001	172.16.26.2	255.2	55,255.0	140	1500						Delete
	Ethernet0/2			No					No							
	Management0	0	manage	Yes	100	92.160.1.1	255.2	55 255 0	Yes	1500						
ben i																
	Enable traff	c between tw	o or more in	terfaces w	hich are co	infigured with s	iame sec	urity levels								
									Adoty		Reset					
												+admin+	NA (15)	1 1 I	A 7/27/06	5.07.52 PM U

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

📫 Cisco ASDM 1	5.1 for ASA - 172.16.26.2	
File Rules Se	arch oppons Tools Weards Hep	a Sectors
Si Home C	Configuration Montoring Black Forward Search Refresh Save Help	
	Condisuration = Nexualy Policy = Bentos Policy Rules	
	◆ 全 平 (d) () × № 色 色 範 (4)	
Herfaces	C Access Rules C AMA Rules C Filter Rules C Storice Policy Rules	
<u> </u>	Show Rules for Indenface: All Interfaces Show All Show All	
Security Policy	Traffic Classification	Add
NAT	Name Enables Match Source Destination Service Time Range Plue Actions Descapeon	Edit
03	Patrice: Inside policy CP-Inside-policy CP-Inside-policy CP-Inside-policy CP-Inside-policy	Delete
VPN		
<u>a</u>		
CSD Manager		
١,		
PS 		
Routing		
8		
Giubal Objects		
2		
Properties		
	Do not match @ Show Summary @ Show Detail	
	Apply Reset Advanced	
	* admin* NA(15) 👔 🖬 👘 7/31/06.3.02-	7 PM UTC

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

Add Service Policy	Rule Wizard - Service Policy	
Adding a new service	policy rule requires three steps:	
Step 1: Configure a s	ervice policy.	
Step 2: Configure the	traffic classification criteria for the service policy rule.	
Step 3: Configure acti	ions on the traffic classified by the service policy rule.	
Create a service pol	icy 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. Crie uma nova classe de tráfego para aplicar à política.Érazoável criar classes específicas para inspecionar tipos de dados específicos, mas neste exemplo, Qualquer tráfego é selecionado para simplificar. Clique em **Avançar** para continuar.

鱰 Add Service Policy Rule Wi	zard - Traffic Classificatio	on Criteria			×
Create a new traffic class:	inside-class				
S Ofcate a flew frame class.					
Description (optional):					
Traffic match criteria					
🔲 Default Inspection 1	raffic				
🔲 Source and Destina	tion IP Address (uses ACL)				
🗖 Tunnel Group					
TCP or UDP Destin	ation Port				
🗖 RTP Range					
🔲 IP DiffServ CodePoi	nts (DSCP)				
IP Precedence					
Any traffic					
If traffic does not match a exist Class-default can be used in o C Use class-default as the tra	ing traffic class, then it will m atch all situation. ffic class.	atch the class-default traffi	c class.		
		< Park	Next >	Cancel	Heln
		- Dack	HOM -		norp

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

鱰 Add Service Policy	Rule Wizard - Rule Ad	ctions		
Protocol Inspection	Intrusion Prevention	Connection Settings	QoS	1
I⊻ Enable IPS for	this traffic flow			
C 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.	for IPS and the original p	acket cannot	
If IPS card fails	s, then			
Permit traffic	:			
C Close traffic				
			< Back Finish	Cancel Help

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

🖆 Cinco ASDM	5.1 for ASA - 172,16.3	26.2							- I ×
File Rules Se	sarch Options Tools	Wittends_Help							
Howe -	Configuration Monitoria	ng Back Forward S	anch Refresh	🗐 ? Save Help				51	te serras
	Configuration + Baburd	V Folicy - Service Policy Rules							
	 	人生的现在分词							
C.	C Access Rules	C AAA Rules C Filler Rules	G Service Policy Ru	les					
Security Policy	Bhow Rules for Inter	face: All Interfaces 💌 🔠	iow All				-		
14	7	Tofic	Classification			Ru e Actions	D	seristion	Add
NAT	Name	Enalyed Match Source	Destination	Service	Tims Ranga				Edit
<u>88</u>	inside-class	De lang	🎱 any	🛪 any traffic		🗐 jos promiscuous, permit traffic	DS HSRD PORY		Delete
VPN									
CSD Marcader									
1									
190									
noting									
80									
Giolad Objects									
5.									
Properties									
	1								
	Den Walch	and match						@ Show Summary C. Show Detail	
		Apply	Reset	A16993	d .				
Configuration sh	anges saved successful	¥					sadmine (NA (15)	a 713108 2:54	47 PM UTC

Configurar o AIP-SSM para a inspeção de tráfego

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

1. Faça login no AIP-SSM usando IDM.

Cisco IDM 5.0 - 172.16.26.10				
File Help				
		•		Cisco System
Configuration Montoring Back Forw	ard Retresh He	p.		A A
E Q Sensor Setup	- Network			
- Network				
- Allowed Hosts	Specify the network	and communication parameters for the sensor.		
B Q SSH				
Br & Cenncates	Hostname:	sensor		
Dutert				
D Q Interface Configuration	IP Address:	172.16.26.10		
- Sinterfaces				
- Dypass	All and a second second second	265 265 265 0		
- Traffic Flow Notifications	Network Mask:	12322322330		
D Q Analysis Engine		[-
- Svetual Sensor	Default Route:	172.16.26.1		
E G. Signature Definition				
-Signature Variables	FTP Timeout	300		seconds
- Signature Configuration				
- DCustom Signature Wizard	Web Server Settin	105	Remote Access	
Miscellaneous	Enable TI GIGG		Telnet is not a secure access service	
E Q Event Action Rules	in children i coro o	-	and is disabled by default.	
INEvent Variables IT send Value Patient	Web server port	443	Finable Tainet	
- Sevent Action Overrides	The store part			
- Devent Action Filters				
Someral Settings				
E Q Blocking				
- NBlocking Properties				
Device Login Profiles				
Bouter Blocking Device Interfaces				
- Cat 6K Blocking Device Interfaces				
- Master Blocking Sensor				
D Q SNMP				
- Noeneral Configuration				
- Traps Configuration				
Paulo Update Pastace Defaulte				
- Rebot Sensor				
- Shutdown Sensor				
- Dupdate Sensor				
Licensing				
		Jop/y	Reset	
			L	
IDM is initialized successfully.				cisco administrator

2. Adicione um usuário com pelo menos privilégios de

visualizador.



3. Ative a

interface.

4. Verifique a configuração do sensor virtual.



Configurar uma WLC para pesquisar o AIP-SSM para blocos de clientes

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

- 1. Escolha Security > CIDS > Sensors > New na WLC.
- Adicione o endereço IP, o número da porta TCP, o nome de usuário e a senha que você criou na seção anterior.
- 3. Para obter a impressão digital do sensor, execute esse comando no sensor e adicione a impressão digital SHA1 à WLC (sem dois-pontos). Isso é usado para proteger a comunicação de polling de controlador para IDS. sensor#show tls fingerprint MD5: 07:7F:E7:91:00:46:7F:BF:11:E2:63:68:E5:74:31:0E SHA1: 98:C9:96:9B:4E:FA:74:F8:52:80:92:BB:BC:48:3C:45:B4:87:6C:55

Cores Section	MONITOR	WLANE	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Serve	ior Edit						
AAA General RADUUS Authentication	Index		2					
RADIUS Accounting Local Net Users MAC Filtering	Server Ad	Idress	172.16.26.10					
Disabled Clients User Login Policies	Port		443					
Access Control Lists	Usernam	0	controller					
IPSec Certificates CA Certificate ID Certificate	Password		•••••					
Web Auth Certificate	State		2					
Wireless Protection Policies	Query Int	erval	10 sec	onds				
Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures	Fingerprin (SHA1 ha	nt sh)	98C9969B4EFA74 (hash key is alre	4F05280926660 ady set)	483C458487	40 he	chars	
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Last Quer (count)	nr.	Success (1400)					
Web Login Page								
CIDS Sensors Shunned Clients								

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

WLC.								
Conce Streeting	MONITOR V	VLANS CONTROLLS	R WIRELESS	SECURITY M	ANAGEMENT COMM	ANDS HELP		
Security	CIDS Sensor	's List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AB Policies	Index 1 2	Server Addres 192.168.5.2 172.16.26.10	443 443	State Enabled Enabled	Query Interval 15 10	Last Query (count) Unauthorized (1) Success (1444)	Detail Detail	Remove Remove
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 Sumary Client Exclusion Policies AP Authentication / MEP Management Frame Protection								
Web Login Page CIDS Sensors Shunned Clients								

Adicionar uma assinatura de bloqueio ao AIP-SSM

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

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

configuração.											
. Cisco IDM 5.0 - 192.168.5.2											T 🖉 🖸
File Help											
Configuration Monitoring Eack Forward	Rete	n Help									Cisco Sesties
E Q Sensor Setup	Signatur	e Configurati	01								
- Network	Dalast D	-	terre al estadouter [A							
SAllowed Hosts	Detect D	r. Ive signa	entes in perior cuteria: 1-	-104- 1							_
D Q SSH D Q Centicates	Sig ID	SubSig ID	Name	Enabled	Action	Seventy	Fidelity Rating	Type	Engine	Retired	Select All
- S there	1330	2	TCP Drop - Urgent Pointer WI.	No	Modify Packet I	Informatio	100	Default	Normalizer	No	NSDB Link
D Q 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	Cinca
- Noterface Pairs	1330	1	TCP Drop - Bad Ontion List	Ves	Deny Packet In	Informatio	100	Default	Normalizer	Nin	Cione
Traffic Flow Motor shops	1000		MMP Echo Dank	Var	Produce Mart	High	100	Tuned	Atomic ID	No	Edt
C G Analysis Engine	2000		POMP Ecno Reply	105	Produce Aven	righ	100	Tuneo	Approx P	140	Enable
- Wintual Sensor	2001	Q	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adormic IP*	No	Enacie
- Olobal Variables	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
B Q Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
- Signature Variables	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High		Tuned	Atomic IP	No	Restore Defaults
- DCustom Signature Wizard	2005	0	ICMP Time Exceeded for a D_	No	Produce Alert	Informatio	100	Default	Atomic IP	No	
G Event Artion Bulan	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Defete.
- Severt Variables	1007		MD Timestano Desuet	No	Produce Alast	Information	100	Darlaut	Atomic ID	ted Min	Activate
- Target Value Rating	2007	0	rumer intestant product	140	Produce Aven	ampril 1900	100	C-enaut	Peperints IP	140	
- Revent 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	Atomic IP	No	

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

A ron signature				hitektektektektektektek
Name Value				
Signature ID: 2004				
SubSignature ID: 0				
Alert Severity: High	•			
Sig Fidelity Rating: 100				
Promiscuous Deita:				
Sig Description:				
Signature	Name: ICMP Echo Request			
Alert Note:	8			
User Com	nments:			
alart Traits	er [0			
Selection and	× 10			
Release.	181			
Engine: Atomic IP				
Event A	uction: Produce Al Produce Ve Request B Repuest B	tose Alert sck Connector		
	<	>		
Fragme	ent Status: Any	v		
😔 🔳 Specify	Layer 4 Protocol: Yes 💌			
	🖯 🖬 Laya	r 4 Protocol: ICMP. Protocol	-	
		Specify	CMP Sequence: No -	
		🕒 🔳 Specify	CMP Type: Yes 💌	
				Type:
		Specify 1	CMP Code: No	
		Specify	CMP Identifier.	
		Specify	CMP Total Length: No. V	
Parameter uses the Default Value. Clin	ck the icon to edit the value			
Parameter uses a User-Defined Value	a. Click the icon to restore the defau	tvalue.		
	0K	Cancel Help	1	

S Ed	lit Signature		E Contraction of the second	ĸ
	Name	Value	-	1
	Signature ID:	2004		
	SubSignature ID:	0		
	Alert Severity:	Informational 💌		
	Sig Fidelity Rating:	100	-	
	Promiscuous Delta:	0	-	
Θ	Sig Description:			ſ
		Signature Name:	ICMP Echo Request	
		Alert Notes:		l
		User Comments:		l
		Alert Traits:	0	
		Release:	81	
Θ	Engine:	Atomic IP		
		Event Action:	Request Block Connection	
1		Eranment Statu	P Anno Incl	
•	Parameter uses the D Parameter uses a Use	efault Value. Click the icc er-Defined Value. Click th	n to edit the value. e icon to restore the default value.	
			OK Cancel Help	

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

Monitorar bloqueio e eventos com IDM

Conclua estes passos:

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

Excluir.



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





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

moremor		Event ID	Events	Sig ID	Details.
anon.emon	July 31, 2006 2:59:52 PM U	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
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]		
lert informati	July 31, 2006 3:19:16 PM U	1145383740954941574	ICMP Echo Request	2004	
mor: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		
lert informati	July 31, 2006 3:19:46 PM U	1145383740954941597	ICMP Echo Request	2004	
	rror:warning lert.informati rror.error lert.informati	Intron.warning July 31, 2006 3:16:51 PM U Iert.informati July 31, 2006 3:19:16 PM U Intronemor July 31, 2006 3:19:16 PM U Iert.informati July 31, 2006 3:19:46 PM U	rror:warning July 31, 2006 3:16:51 PM U 1145383740954941447 Iert.informati July 31, 2006 3:19:16 PM U 1145383740954941574 rror:error July 31, 2006 3:19:16 PM U 1145383740954941577 Iert.informati July 31, 2006 3:19:46 PM U 1145383740954941597	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] lert.informati July 31, 2006 3:19:16 PM U 1145383740954941574 ICMP Echo Request 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 lert.informati July 31, 2006 3:19:46 PM U 1145383740954941597 ICMP Echo Request	Intro: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] Iert.informati July 31, 2006 3:19:16 PM U 1145383740954941574 ICMP Echo Request 2004 Iror: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 2004 Iertinformati July 31, 2006 3:19:16 PM U 1145383740954941577 Unable to execute a host block [10.10.99.26] because blocking is not configured 2004

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

```
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
             description=ICMP Echo Request id=2004 version=S1
  signature:
   subsigId: 0
 interfaceGroup:
 vlan: 0
 participants:
   attacker:
     addr: 10.10.99.26 locality=OUT
   target:
      addr: 10.10.102.1 locality=OUT
 summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
  alertDetails: Regular Summary: 4 events this interval ;
 riskRatingValue: 25
 interface: ge0_1
 protocol: icmp
```

Monitorar a exclusão do cliente em um controlador sem fio

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

Cinto Stattan								
AA	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering	Re-sync IP Addres 10.10.99.20	s La 6 00	st MAC Address :40:96:ad:0d:1b	Expire 27	Sen: 172.:	tor IP / Index 16.26.10 / 2		
User Login Policies AP Policies								
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								

O usuário é adicionado à lista de exclusões de clientes.

	MONITOR WI	LANS CONTROLLER	WIRELESS S	ECURITY MAN	AGEMENT CO	MMANDS HELP		
Monitor Summary Statistics Controller Ports Wireless Rogue APs Rogue Cients Adhoc Rogues 802.116 Radios 802.116 Radios 802.116 Radios 802.116 Radios 802.116 Radios 802.116 Radios	Excluded Clien Search by NAI Client NAC Ad	nts Caddress Idr AP Name	AP NAC Addr	WLAN	Туре	Exclusion Reason	Port	
	00:40:96:ad:0d	1:15 AP5014.6940.81c	e 00:14:15:5a:16:	40 IPS	802.11a	UnknownEnum:S	29	Detail LinkTest Disable Remove

Monitorar eventos no WCS

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

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

3. Clique em

. Buscar

Cisco Wireless Control S	ystem			Username: root Logout Refresh Print View
Monitor • Configure •	Alarms			Select a command 💌 GO
Saverty Critical v Alarm Category Al Types v Scarch	Severity Failure_Object Critical Radio_ADR-LAPL262AG-A/1 Critical Radio_ADR-LAPL262AG-A/2 Critical Radio_ADR-LAPL262AG-A/2 Critical Radio_ADR-LAPL262AG-A/2 Critical Radio_ADR-LAPL262AG-A/2 Critical Radio_ADR-LAPL262AG-A/2 Critical Radio_ADR-DS1212:e0/2 Critical Radio_ADR-DS122:e0/2 Critical AP_ABID231.2:e0/00:05:057:12:e0 Critical AP_ABID31.0:e92.e0/00:13:55:75:14:e0 Critical AP_APD031.0:e92.e0/00:13:55:75:14:e0 Critical AP_APD031.0:e92.e0/00:13:55:75:14:e0 Critical AP_APD031.0:e92.e0/00:13:55:75:14:e0 Critical AP_APD031.0:e92.e0/00:13:55:75:14:e0 Critical AP_APD031.0:e92.e0/00:13:55:75:14:e0 Critical AP_APD031.0:e92.e0/00:13:55:21:e0:e0 Critical AP_APD002:e0/00:13:e1:FE1:0:1/1 Critical AP_APD002:e0/00:13:e1:FE1:0:1/1 Critical AP_APD002:e0/07:00:45:17:E1:0:1/2 Critical AP_APD002:e0/07:00:45:17:E1:0:1/2	Daner	Date/Time 6/1/05 9:02 AM 6/1/05 9:02 AM 6/1/05 9:02 AM 7/21/06 1:51 PM 7/21/06 1:51 PM 7/21/06 4:32 PM 7/21/06 4:32 PM 7/21/06 4:32 PM 7/21/06 4:32 PM 7/21/06 5:31 PM 7/21/06 5:32 PM 7/26/06 2:02 PM 7/26/06 2:02 PM	AP 'AIR-LAP1242AG-A', interface '802.11b'g' is AP 'AIR-LAP1242AG-A', interface '802.11b'g' is AP 'AIR-LAP1242AG-A', interface '802.11b'g' is down AP 'AIR-LAP1242AG-A', interface '802.11b'g' is down AP 'ap1751121e0', interface '802.11b'g' is down AP 'ap-aco-c3750-48-1-FE1-0-3', interface '802 AP 'AP-aco-c3750-48-1-FE1-0-3', interface '802
Regues 0 242 Coverage 0 Security 2 0 4 Centrollers 1 0 0 Access Points 0 0 0				

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

janeia.											
Cisco Wireles	s Control S	ystem						Username: roo	at Logout	Refresh	Print V
Monitor ▼ Configure ▼ Location ▼ Administration ▼ Help ▼											
Alarms		Alar	ms						Select	t a comm	and
Severity Minor	~		Severity	Failure Object	Owner	Date/Time		Message			
(Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 P	PM	The WEP Key configured at the station may be wr			
Alarm Category			Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 P	PM	The WEP Key configured at the station may be wr			
Security			Minor	Client 00:90:7a:04:6d:04		7/31/06 2:36 P	PM	Client '00:90:7a:04:6d:04' which was associated			
Search			Minor	Client 00:40:95:ad:0d:15		7/31/06 4:25 P	PM	Client '00:40:96:ad:0d:1b' which was associated			
				Client 100.40.96 ac 100.14.1brSo:16.40 code is 'S(Unknow	10d:16° which was asso 3°, interface 10° is exclude m)°.	ciated with AP ed. The reason					

Exemplo de configuração do Cisco ASA

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
```

```
interface Ethernet0/0
 nameif outside
 security-level 0
ip address 10.10.102.2 255.255.255.0
!
interface Ethernet0/1
nameif inside
 security-level 100
 ip address 172.16.26.2 255.255.255.0
1
interface Ethernet0/2
 shutdown
no nameif
 no security-level
no ip address
!
interface Management0/0
nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
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
class-map inside-class
match any
1
!
```

```
policy-map inside-policy
description IDS-inside-policy
class inside-class
ips promiscuous fail-open
!
service-policy inside-policy interface inside
Cryptochecksum:699d110f988e006f6c5c907473939b29
: end
ciscoasa#
```

Exemplo de configuração do sensor do sistema de prevenção de intrusão da Cisco

sensor#show config | _____ ! Version 5.0(2) ! Current configuration last modified Tue Jul 25 12:15:19 2006 | _____ service host network-settings host-ip 172.16.26.10/24,172.16.26.1 telnet-option enabled access-list 10.0.0/8 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#

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

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

Informações Relacionadas

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