Guide d'intégration du contrôleur de réseau local sans fil et du système IPS

Contenu

Introduction Conditions préalables **Conditions requises** Components Used Conventions Présentation de Cisco IDS Cisco IDS et WLC - Présentation de l'intégration Arrêt IDS Conception de l'architecture réseau Configuration du capteur Cisco IDS Configurer le WLC Exemple de configuration du capteur Cisco IDS Configurer un ASA pour IDS Configurer AIP-SSM pour l'inspection du trafic Configurer un WLC pour interroger l'AIP-SSM pour les blocs de clients Ajouter une signature de blocage à AIP-SSM Blocage et événements de surveillance avec IDM Contrôle de l'exclusion du client dans un contrôleur sans fil Surveiller les événements dans WCS Exemple de configuration de Cisco ASA Exemple de configuration du capteur du système de prévention des intrusions Cisco Vérification Dépannage Informations connexes

Introduction

Le système de détection des intrusions Cisco Unified Intrusion Detection System (IDS)/système de prévention des intrusions (IPS) fait partie du réseau à capacité d'autodéfense Cisco et est la première solution de sécurité câblée et sans fil intégré de l'industrie. Cisco Unified IDS/IPS adopte une approche complète de la sécurité, à la périphérie sans fil, à la périphérie filaire, à la périphérie WAN et à travers le data center. Lorsqu'un client associé envoie du trafic malveillant via le réseau sans fil unifié de Cisco, un périphérique IDS câblé de Cisco détecte l'attaque et envoie des requêtes d'annulation aux contrôleurs de réseau local sans fil (WLC) de Cisco, qui dissocient ensuite le périphérique client.

Cisco IPS est une solution en ligne basée sur le réseau, conçue pour identifier, classer et arrêter

avec précision le trafic malveillant, y compris les vers, les logiciels espions/publicitaires, les virus réseau et les utilisations abusives des applications, avant qu'ils n'affectent la continuité de l'activité.

Grâce à l'utilisation du logiciel Cisco IPS Sensor version 5, la solution Cisco IPS associe des services de prévention en ligne à des technologies innovantes pour améliorer la précision. Il en résulte une confiance totale dans la protection fournie de votre solution IPS, sans crainte de perte de trafic légitime. La solution Cisco IPS offre également une protection complète de votre réseau grâce à sa capacité unique à collaborer avec d'autres ressources de sécurité réseau et offre une approche proactive de la protection de votre réseau.

La solution Cisco IPS aide les utilisateurs à arrêter davantage de menaces en toute confiance grâce à l'utilisation des fonctionnalités suivantes :

- Technologies de prévention en ligne précises : offre une confiance inégalée pour prendre des mesures préventives contre un plus large éventail de menaces sans risque de perte de trafic légitime. Ces technologies uniques offrent une analyse intelligente, automatisée et contextuelle de vos données et vous aident à tirer le meilleur parti de votre solution de prévention des intrusions.
- Identification des menaces multivecteurs Protège votre réseau contre les violations de politiques, les exploitations de vulnérabilité et les activités anormales grâce à une inspection détaillée du trafic des couches 2 à 7.
- Collaboration réseau unique Améliore l'évolutivité et la résilience grâce à la collaboration réseau, notamment des techniques efficaces de capture du trafic, des fonctionnalités d'équilibrage de charge et une visibilité sur le trafic chiffré.
- Solutions de déploiement complètes : fournit des solutions pour tous les environnements, des petites et moyennes entreprises (PME) aux filiales en passant par les grandes entreprises et les fournisseurs de services.
- Puissants services de gestion, de corrélation d'événements et d'assistance : offre une solution complète comprenant des services de configuration, de gestion, de corrélation de données et d'assistance avancée. En particulier, Cisco Security Monitoring, Analysis, and Response System (MARS) identifie, isole et recommande la suppression précise des éléments offensants, pour une solution de prévention des intrusions à l'échelle du réseau. De plus, le système de contrôle des incidents Cisco empêche les nouveaux vers et virus de se propager en permettant au réseau de s'adapter rapidement et de fournir une réponse distribuée.

Combinés, ces éléments constituent une solution complète de prévention en ligne et vous donnent la confiance nécessaire pour détecter et arrêter le trafic malveillant le plus étendu avant qu'il n'affecte la continuité de l'activité. L'initiative Cisco Self-Defending Network préconise une sécurité intégrée et intégrée pour les solutions réseau. Les systèmes WLAN actuels basés sur le protocole LWAPP (Lightweight Access Point Protocol) prennent uniquement en charge les fonctions IDS de base, car il s'agit essentiellement d'un système de couche 2 et sa puissance de traitement de ligne est limitée. Cisco publie le nouveau code en temps opportun pour inclure de nouvelles fonctionnalités améliorées dans les nouveaux codes. La version 4.0 présente les dernières fonctionnalités qui incluent l'intégration d'un système WLAN basé sur LWAPP à la gamme de produits Cisco IDS/IPS. Dans cette version, l'objectif est de permettre au système Cisco IDS/IPS de demander aux WLC de bloquer certains clients d'accès aux réseaux sans fil lorsqu'une attaque est détectée entre les couches 3 et 7 et implique le client en question.

Conditions préalables

Conditions requises

Assurez-vous de respecter les conditions minimales suivantes :

- Microprogramme WLC version 4.x et ultérieure
- Il est souhaitable de savoir comment configurer Cisco IPS et Cisco WLC.

Components Used

WLC Cisco

Ces contrôleurs sont inclus avec la version logicielle 4.0 pour les modifications IDS :

- WLC Cisco, série 2000
- WLC de la gamme Cisco 2100
- WLC de la gamme Cisco 4400
- Module de services sans fil Cisco (WiSM)
- Commutateur d'accès unifié Cisco Catalyst 3750G
- Module de contrôleur LAN sans fil Cisco (WLCM)

Points d'accès

- Points d'accès légers de la gamme Cisco Aironet 1100 AG
- Points d'accès légers de la gamme Cisco Aironet 1200 AG
- Points d'accès légers de la gamme Cisco Aironet 1300
- Points d'accès légers de la gamme Cisco Aironet 1000

Gestion

- Cisco Wireless Control System (WCS)
- Capteur de la gamme Cisco 4200
- Cisco IDS Management Cisco IDS Device Manager (IDM)

Plates-formes Cisco Unified IDS/IPS

- Capteurs de la gamme Cisco IPS 4200 avec logiciel Cisco IPS Sensor 5.x ou version ultérieure.
- SSM10 et SSM20 pour les appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 avec le logiciel Cisco IPS Sensor 5.x
- Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 avec logiciel Cisco IPS Sensor 5.x
- Module de réseau Cisco IDS (NM-CIDS) avec logiciel Cisco IPS Sensor 5.x
- Module IDSM-2 (Intrusion Detection System Module 2) de la gamme Cisco Catalyst 6500 avec logiciel Cisco IPS Sensor 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

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Présentation de Cisco IDS

Les principaux composants de Cisco IDS (version 5.0) sont les suivants :

- Application de capteur : effectue la capture et l'analyse des paquets.
- Event Storage Management and Actions Module Permet le stockage des violations de stratégie.
- Module d'imagerie, d'installation et de démarrage : charge, initialise et démarre tous les logiciels système.
- User Interfaces and UI Support Module : fournit une interface de ligne de commande intégrée et l'IDM.
- Sensor OS : système d'exploitation hôte (basé sur Linux).



L'application de détection (logiciel IPS) se compose des éléments suivants :

- Application principale : initialise le système, démarre et arrête d'autres applications, configure le système d'exploitation et est responsable des mises à niveau. Il contient les composants suivants :Control Transaction Server : permet aux capteurs d'envoyer des transactions de contrôle utilisées pour activer la fonctionnalité de capteur de blocage principal du contrôleur de réponse aux attaques (anciennement appelé contrôleur d'accès au réseau).Event Store -Magasin indexé utilisé pour stocker les événements IPS (erreurs, messages d'état et d'alerte) accessibles via l'interface de ligne de commande, IDM, Adaptive Security Device Manager (ASDM) ou le protocole RDEP (Remote Data Exchange Protocol).
- Application d'interface : gère les paramètres physiques et de contournement et définit les interfaces associées. Les paramètres physiques comprennent les états de vitesse, de duplex et d'administration.
- Log App : écrit les messages de journal de l'application dans le fichier journal et les messages

d'erreur dans le magasin d'événements.

- Contrôleur de réponse aux attaques (ARC) (anciennement appelé contrôleur d'accès réseau)

 gère les périphériques réseau distants (pare-feu, routeurs et commutateurs) afin de fournir
 des fonctionnalités de blocage lorsqu'un événement d'alerte s'est produit. ARC crée et
 applique des listes de contrôle d'accès (ACL) sur le périphérique réseau contrôlé ou utilise la
 commande shun (pare-feu).
- Notification App : envoie des interruptions SNMP lorsqu'elles sont déclenchées par des événements d'alerte, d'état et d'erreur. L'application de notification utilise un agent SNMP de domaine public à cette fin. Les GET SNMP fournissent des informations sur l'état d'un capteur.Serveur Web (serveur HTTP RDEP2) : fournit une interface utilisateur Web. Il fournit également un moyen de communiquer avec d'autres périphériques IPS via RDEP2 en utilisant plusieurs servlets pour fournir des services IPS.Authentication App : vérifie que les utilisateurs sont autorisés à exécuter des actions CLI, IDM, ASDM ou RDEP.
- Application de capteur (Analysis Engine) : effectue la capture et l'analyse des paquets.
- CLI : interface exécutée lorsque les utilisateurs se connectent correctement au capteur via Telnet ou SSH. Tous les comptes créés via l'interface de ligne de commande utilisent l'interface de ligne de commande comme interpréteur de commandes (à l'exception du compte de service - un seul compte de service est autorisé). Les commandes CLI autorisées dépendent des privilèges de l'utilisateur.

Toutes les applications IPS communiquent entre elles via une API (Application Program Interface) commune appelée IDAPI. Les applications distantes (autres capteurs, applications de gestion et logiciels tiers) communiquent avec les capteurs via les protocoles RDEP2 et SDEE (Security Device Event Exchange).

Notez que le capteur possède les partitions de disque suivantes :

- Application Partition : contient l'image système IPS complète.
- **Partition de maintenance** : image IPS spéciale utilisée pour refaire l'image de la partition d'application de l'IDSM-2. Une nouvelle image de la partition de maintenance entraîne la perte des paramètres de configuration.
- partition de récupération : image spéciale utilisée pour la récupération du capteur. L'amorçage dans la partition de récupération permet aux utilisateurs de refaire complètement l'image de la partition d'application. Les paramètres réseau sont préservés, mais toutes les autres configurations sont perdues.

Cisco IDS et WLC - Présentation de l'intégration

La version 5.0 de Cisco IDS introduit la possibilité de configurer des actions de refus lorsque des violations de stratégie (signatures) sont détectées. En fonction de la configuration utilisateur au niveau du système IDS/IPS, une requête d'arrêt peut être envoyée à un pare-feu, un routeur ou un WLC afin de bloquer les paquets d'une adresse IP particulière.

Avec le logiciel Cisco Unified Wireless Network Version 4.0 pour les contrôleurs sans fil Cisco, une demande de désactivation doit être envoyée à un WLC afin de déclencher la liste noire ou le comportement d'exclusion du client disponible sur un contrôleur. L'interface que le contrôleur utilise pour obtenir la requête shun est l'interface de commande et de contrôle sur le système Cisco IDS.

• Le contrôleur permet de configurer jusqu'à cinq capteurs IDS sur un contrôleur donné.

- Chaque capteur IDS configuré est identifié par son adresse IP ou son nom de réseau qualifié et ses informations d'autorisation.
- Chaque capteur IDS peut être configuré sur un contrôleur avec un taux de requête unique en secondes.



Arrêt IDS

Le contrôleur interroge le capteur à la vitesse de requête configurée afin de récupérer tous les événements shun. Une requête shun donnée est distribuée dans tout le groupe de mobilité du contrôleur qui récupère la requête du capteur IDS. Chaque requête de suppression d'une adresse IP client est en vigueur pour la valeur de délai d'attente spécifiée en secondes. Si la valeur de délai d'attente indique une heure infinie, l'événement shun ne se termine que si l'entrée shun est supprimée sur le système IDS. L'état du client ignoré est maintenu sur chaque contrôleur du groupe de mobilité, même si tous les contrôleurs ou l'un d'entre eux sont réinitialisés.

Remarque : La décision de ne pas utiliser un client est toujours prise par le capteur IDS. Le contrôleur ne détecte pas les attaques de couche 3. Il est beaucoup plus compliqué de déterminer que le client lance une attaque malveillante au niveau de la couche 3. Le client est authentifié au niveau de la couche 2, ce qui est suffisant pour que le contrôleur accorde l'accès à la couche 2.

Remarque : Par exemple, si un client reçoit une adresse IP (ignorée) offensante précédente, il est possible de débloquer l'accès de couche 2 pour ce nouveau client jusqu'au délai d'expiration du capteur. Même si le contrôleur donne accès à la couche 2, le trafic client peut être bloqué sur les routeurs de la couche 3 de toute façon, car le capteur informe également les routeurs de l'événement shun.

Supposez qu'un client a l'adresse IP A. Maintenant, lorsque le contrôleur interroge le système IDS pour les événements de shun, le système IDS envoie la requête de shun au contrôleur avec l'adresse IP A comme adresse IP cible. Maintenant, le contrôleur noir répertorie ce client A. Sur le contrôleur, les clients sont désactivés en fonction d'une adresse MAC.

Maintenant, supposez que le client change son adresse IP de A à B. Au cours du prochain

sondage, le contrôleur obtient une liste de clients ignorés en fonction de l'adresse IP. Cette fois encore, l'adresse IP A figure toujours dans la liste des adresses ignorées. Mais comme le client a changé son adresse IP de A à B (qui ne figure pas dans la liste des adresses IP ignorées), ce client avec une nouvelle adresse IP de B est libéré une fois que le délai d'expiration des clients noirs répertoriés est atteint sur le contrôleur. Maintenant, le contrôleur commence à autoriser ce client avec une nouvelle adresse IP de B (mais l'adresse MAC du client reste la même).

Par conséquent, bien qu'un client reste désactivé pour la durée du délai d'exclusion du contrôleur et soit réexclu s'il acquiert de nouveau son adresse DHCP précédente, ce client n'est plus désactivé si l'adresse IP du client ignoré change. Par exemple, si le client se connecte au même réseau et que le délai de bail DHCP n'est pas expiré.

Les contrôleurs prennent uniquement en charge la connexion au système IDS pour les demandes de mise en garde de clients qui utilisent le port de gestion sur le contrôleur. Le contrôleur se connecte à l'IDS pour l'inspection des paquets via les interfaces VLAN applicables qui transportent le trafic client sans fil.

Sur le contrôleur, la page Désactiver les clients affiche chaque client qui a été désactivé via une demande de capteur IDS. La commande CLI **show** affiche également une liste de clients inscrits sur une liste noire.

Sur le WCS, les clients exclus sont affichés sous le sous-onglet Sécurité.

Voici les étapes à suivre pour terminer l'intégration des capteurs Cisco IPS et des WLC Cisco.

- 1. Installez et connectez l'appareil IDS sur le même commutateur que celui où réside le contrôleur sans fil.
- 2. Mettre en miroir (SPAN) les ports WLC qui transportent le trafic du client sans fil vers l'appareil IDS.
- 3. L'appareil IDS reçoit une copie de chaque paquet et inspecte le trafic des couches 3 à 7.
- 4. L'appliance IDS offre un fichier de signature téléchargeable, qui peut également être personnalisé.
- 5. L'appareil IDS génère l'alarme avec une action d'évitement d'événement lorsqu'une signature d'attaque est détectée.
- 6. Le WLC interroge l'IDS pour les alarmes.
- 7. Lorsqu'une alarme avec l'adresse IP d'un client sans fil, associé au WLC, est détectée, elle place le client dans la liste d'exclusion.
- 8. Un déroutement est généré par le WLC et WCS est averti.
- 9. L'utilisateur est supprimé de la liste d'exclusion après la période spécifiée.

Conception de l'architecture réseau



Le contrôleur de réseau local sans fil Cisco est connecté aux interfaces gigabit du Catalyst 6500. Créez un port-channel pour les interfaces gigabit et activez l'agrégation de liaisons (LAG) sur le WLC.

(Cisco Controller) >show interface summary

Port	Vlan Id	IP Address	Туре	Ap Mgr
LAG	untagged	10.10.99.3	Static	Yes
LAG	untagged	10.10.99.2	Static	No
N/A	N/A	192.168.1.1	Static	No
N/A	N/A	1.1.1.1	Static	No
LAG	101	10.10.101.5	Dynamic	No
	Port LAG LAG N/A N/A LAG	Port Vlan Id LAG untagged LAG untagged N/A N/A N/A N/A LAG 101	Port Vlan Id IP Address LAG untagged 10.10.99.3 LAG untagged 10.10.99.2 N/A N/A 192.168.1.1 N/A N/A 1.1.1.1 LAG 101 10.10.101.5	PortVlan IdIP AddressTypeLAGuntagged10.10.99.3StaticLAGuntagged10.10.99.2StaticN/AN/A192.168.1.1StaticN/AN/A1.1.1.1StaticLAG10110.10.101.5Dynamic

Le contrôleur est connecté aux interfaces gigabit 5/1 et gigabit 5/2 sur le Catalyst 6500.

cat6506#show run interface gigabit 5/1 Building configuration... Current configuration : 183 bytes ! interface GigabitEthernet5/1 switchport switchport trunk encapsulation dotlq switchport trunk native vlan 99 switchport mode trunk no ip address channel-group 99 mode on end cat6506#show run interface gigabit 5/2 Building configuration... Current configuration : 183 bytes 1 interface GigabitEthernet5/2

```
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
cat6506#show run interface port-channel 99
Building configuration...
Current configuration : 153 bytes
1
interface Port-channel99
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

Les interfaces de détection du capteur IPS peuvent fonctionner individuellement en **mode Promiscuité** ou vous pouvez les jumeler pour créer des interfaces en ligne pour le **mode Inline Sensing**.

En mode Promiscuité, les paquets ne transitent pas par le capteur. Le capteur analyse une copie du trafic surveillé plutôt que le paquet transféré réel. L'avantage d'un fonctionnement en mode Promiscuité est que le capteur n'affecte pas le flux de paquets avec le trafic transféré.

Remarque : Le <u>diagramme d'architecture</u> n'est qu'un exemple de configuration de l'architecture intégrée WLC et IPS. L'exemple de configuration présenté ici explique l'interface de détection IDS agissant en mode Promiscuité. Le <u>diagramme d'architecture</u> montre les interfaces de détection en cours d'association pour agir en mode Paire en ligne. Référez-vous à <u>Mode en ligne</u> pour plus d'informations sur le mode Interface en ligne.

Dans cette configuration, on suppose que l'interface de détection agit en mode Promiscuité. L'interface de surveillance du Cisco IDS Sensor est connectée à l'interface Gigabit 5/3 du Catalyst 6500. Créez une session de surveillance sur le Catalyst 6500 où l'interface port-channel est la source des paquets et la destination est l'interface gigabit où l'interface de surveillance du capteur IPS Cisco est connectée. Ceci répliquera tout le trafic d'entrée et de sortie des interfaces filaires du contrôleur vers le système IDS pour l'inspection des couches 3 à 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#
```

Configuration du capteur Cisco IDS

La configuration initiale du Cisco IDS Sensor est effectuée à partir du port de console ou en

connectant un moniteur et un clavier au capteur.

- 1. Connectez-vous à l'appliance :Connectez un port de console au capteur.Connectez un moniteur et un clavier au capteur.
- 2. Tapez votre nom d'utilisateur et votre mot de passe à l'invite de connexion. Remarque : le nom d'utilisateur et le mot de passe par défaut sont tous deux cisco. Vous êtes invité à les modifier la première fois que vous vous connectez à l'appliance. Vous devez d'abord saisir le mot de passe UNIX, cisco. Ensuite, vous devez saisir le nouveau mot de passe deux fois. 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. Configurez l'adresse IP, le masque de sous-réseau et la liste d'accès sur le capteur. Remarque : Il s'agit de l'interface de commande et de contrôle sur le système IDS utilisé pour communiquer avec le contrôleur. Cette adresse doit être routable vers l'interface de gestion du contrôleur. Les interfaces de détection ne nécessitent pas d'adressage. La liste d'accès doit inclure l'adresse de l'interface de gestion du ou des contrôleurs, ainsi que les adresses autorisées pour la gestion du système 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 10.0.0/8
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. Vous pouvez maintenant configurer le capteur IPS à partir de l'interface utilisateur graphique. Pointez le navigateur vers l'adresse IP de gestion du capteur. Cette image affiche un exemple dans lequel le capteur est configuré avec

192.168.5.2.	-		
Cisco IDM 5.0 - 192.168.5.2			50
File Help			Constanting of the second s
Configuration Monitoring Dack Forward	nd Refresh Hel		Cisco Sester
G. Sensor Setup Notweel Hots: G. Sensor Setup Notweel Hots: G. Centicates State Setup Contractes State Setup Contractes State Setup Contractes State Flow Notifications Notweel Hots: Notweel	Network Dipecify the network a Hostname: P Address: Network Mask: Default Route: FTP Timeout: Web Server Bettin P Enable TLSESS Web server port:	Activ Reset	seconds
ILM IS HIGHZED SUCCESSIUNY.			cieco agrianos acor

5. Ajoutez un utilisateur que le WLC utilise pour accéder aux événements IPS Sensor.

Ciscs DM 5.0 / 192.168.5.2				- * 🛛
File Help				
Configuration Monitoring Back Forward Retresh	? Heb			Cisco Sestion
G Q Sensor Setup Shetwork Quest Quest	ers that have access to the sensor. The se	nice role is a special role that allows you to bypass the	CLI if needed. Only one service account is allowed.	τ
- Time	Usemame	Noie	Utatus Artica	Add
L-10Lisers		Participation	PLUTT.	
G Interface Configuration Sinterfaces				E6t
- Negrats				Delete
E Q Analysis Engine	a section			
- Nintual Sensor	A KOD CONT			
-Solobal Variables	Usemame:	controller		
E 4 Signature Definition				
Signature variables				
- Dustom Signature Wizard	User Role:	Animatic		
Miscellaneous				
Q Event Action Rules	Parameter			
- DEvent Variables	Passadro			
Supplement action (hearing)				
- Sevent Action Filters	Password:	*****		
- Deneral Settings				
E Q Blocking				
- NBlocking Properties	Confirm Password			
Device Login Protes				
Router Blocking Device Interfaces				
-SCat 6K Blocking Device Interfaces		Cancel Help		
Master Blocking Sensor				
rh G cump			1	

6. Activez les interfaces de surveillance.

Cisco IDM 5.0 - 192.168.5.2							
File Help							
Configuration Monitoring Eack Forward	d Refresh Help						Cisco Systems
E Q Sensor Selup - Network - Network Hosts B Q SSH B Q Centificates	A sensing interface must and clicking Enable or Di	be enabled and assigned to sable.	a virtual sensor	before the se	nsor will monitor that int	erface. You can enableidisable the available sensing interfaces by selectin	g the row(s)
- Dusers	Interface Name	Enabled Media Type	Duplex	Speed	Atternate TCP Reset Interface	Description	SelectAll
Q Interface Configuration	OlgabitEthemet0/0	Yes TX (copper)	Auto	Auto	None		Edit
Sinterface Pairs	OigabitEthemet0/1	No TX (copper)	Auto	Auto	None		Eastin
- Departs	OigabitEthemet0/2	No TX (copper)	Auto	Auto	None		Chatre
Traffic Flow Notifications	OigabitEthemet0/3	No TX (copper)	Auto	Auto	None		Disable

Les interfaces de surveillance doivent être ajoutées au moteur d'analyse, comme le montre cette fenêtre

 Cisco IDM 5.0 - 192.168.5.2 File Help 							
Configuration Montoring Eack Forwa	and Retresh	₽ Heb		Cisco Systems			
E Q Sensor Setup - Nivetwork - Nivetwork B Q SSH B Q Centificates - ©Time	Vitual Sensor 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 ual sensor or change the virtual sensor name.	description or			
Users	Name	Assigned Interfaces (or Interface Pairs)	Description	Edit			
G. Interface Configuration Sonterfaces Sonterface Pairs Noterface Pairs Sonterface Pairs Sonterface Pairs Sonterface Pairs	vs0	OlgabitEthemet00 OlgabitEthemet00 OlgabitEthemet00 OlgabitEthemet00 OlgabitEthemet00	defaut virtual sensor				
Q. Analysis Engine Strats Engine School Variables							

7. Sélectionnez la signature 2004 (ICMP Echo Request) afin d'effectuer une vérification de configuration

rapide.											
*. Cisco IDM 5.0 - 192.168.5.2											- C 🛛
File Help											
Configuration Monitoring Dack Forward	nd Retres	n Help									Cisco Systems
Q. Sensor Setup Notwork SAlowed Hosts	Select By	Configurati	on tures 💌 Select Criteria: 🖡	-104							
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	NSDB Dink
D 9 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
- Bevoass	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	Eot
© Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Enable
District Vision	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
D 9 Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	
- Signature Variables - Signature Configuration	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	Hiph	100	Tuned	Atomic IP	No	Actions Data At
- Custom Signature Wizard	2005	0	KMP Time Exceeded for a D	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Pressore Cenaults
C. C. Event Artisis Dulan	2006		ICMP Parameter Problem on	No	Produce Alart	Informatio	100	Defect	Atomic ID	No	Deixte.
-Sevent Variables	1000	0	MAD Transitions Desugat	No	Produce Alast	informatio.	100	Darlaut	Atomic ID	No.	Activate
- Target Value Rating	2007	0	numer intrestants roequest	140	Produce Alen	PHQ111300	100	Denaut	Paymic IP	PRU	
-Sevent Action Overrides	2008	0	ICMP Timestamp Reply	NO	Produce Alert	informatio	100	Default	Adomic IP	NO	Retre
- Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	

La signature doit être activée, la gravité de l'alerte définie sur **Élevé** et l'action d'événement définie sur **Produire l'alerte** et l'**hôte de bloc de demande** pour que cette étape de vérification soit

terminée.



Configurer le WLC

Complétez ces étapes afin de configurer le WLC :

- 1. Une fois l'appareil IPS configuré et prêt à être ajouté au contrôleur, sélectionnez **Security >** CIDS > Sensors > New.
- 2. Ajoutez l'adresse IP, le numéro de port TCP, le nom d'utilisateur et le mot de passe que vous avez précédemment créés. Afin d'obtenir l'empreinte du capteur IPS, exécutez cette commande dans le capteur IPS et ajoutez l'empreinte SHA1 sur le WLC (sans les deuxpoints). Cette option permet de sécuriser la communication d'interrogation contrôleur/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	and the second second	and the second states	Surd and	in the second	And the second second	Save Co	nfiguration	Ping	Logout Refresh
March The Part of the	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		a she san and
Security	CIDS Sensor Add						< Back		Apply
General RADIUS Authentication RADIUS Accounting	Index	11							
Local Net Users MAC Filtering	Server Address	192.168.5.2							
Disabled Clients 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 sec	onds						
Policies Trusted AP Policies Rogue Policies	State	R							
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hash)	1662E996362A9A	1EF08899A7C	1645F5C856A	8842 40 he	(chars			
Web Login Page									
CIDS Sensors Shunned Clients									

3. Vérifiez l'état de la connexion entre le capteur IPS et le

WLC.								
Core Server	MONITOR WU	ANE CONTROLLE	e wielless	SECURITY	MANAGEMENT COMM	ANDS HELP		Logout Re
Carpelly	0100.0000000							
seconcy	GIDS Servors I	LISE						 Pog av
AAA	Index	Server Address	Port	State	Query Interval	Last Query (count)		
ADUUS Authentication RADUUS Accounting Local Net Users MAC Fibering Disabled Clients User Login Policies AP Policies	1	192.160.5.2	443	Enabled	15	Success (6083)	Detail Esmore	
Access Control Lists								
Network Access Control								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trutbed AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summery Client Exclusion Policies AP Authonication Nanagement Prame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								
		_				_		

4. Une fois que vous avez établi la connectivité avec le Cisco IPS Sensor, assurez-vous que la configuration WLAN est correcte et que vous activez l'exclusion du client.La valeur par défaut du délai d'exclusion du client est de 60 secondes. Notez également que, indépendamment du compteur d'exclusion du client, l'exclusion du client persiste tant que le bloc client appelé par le système IDS reste actif. La durée de blocage par défaut dans le système IDS est de 30 minutes.

Conce Deserves									Save Config	uration Ping	Logout Refre
AA	MONITOR WEARS CO	ONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP					
WLANS	WLANs > Edit									< Back	Apply
WLANS WLANS AR Groups VLAN	WLAN ID WLAN SSID	1 IPS									
HE GEORGE ELSER	General Policies						Security Policies				
	Radio Policy	All 🗸					IPv6 Enable				
	Admin Status Session Timeout (secs)	Enabled					Layer 2 Security	WPA1+WPA2	×		
	Quality of Service (QoS) WMM Policy	Silver (best effort) V Disabled V					Laver 3 Security	None	~		
	7920 Phone Support	Client CAC Limit A	IP CAC Limit				and a second	Web Policy *			
	Allow AAA Overvide	Enabled									
	External Policy Validation	Enabled					* Web Policy cannot be	used in combination	with IPsec		
	Client Exclusion	Enabled ** 600 Timeout	Value (secs)				and L2TP. ** When client exclusion	n is enabled, a time:	out value of		
	DHCP Server	C Override					reset excluded clients)	require auministrati	re overnae w		
	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, CP	ANITE and FORTE	RESS authenticat	ions.					
	CISCO Client Extension (CCX)		_								
	Version IE	Enabled									
	Aironet IE										
	Gratuitous Probe Response										
	Radius Servers										
		Authentication Servers	Accounting S	lervers							
	Server 1	IP:10.1.1.12, Port:1812	v none v								

5. Vous pouvez déclencher un événement dans le système IPS Cisco, soit lorsque vous effectuez une analyse NMAP sur certains périphériques du réseau, soit lorsque vous envoyez une requête ping à certains hôtes surveillés par le capteur IPS Cisco. Une fois qu'une alarme est déclenchée dans le système de prévention des intrusions Cisco, accédez à **Surveillance et blocs d'hôtes actifs** afin de vérifier les détails relatifs à l'hôte

mole.	
Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Retresh	₽ Nap
NDeried Abackers Notebook Asstallacks Notebook Asstallacks Notebook Asstallacks Notebook Security Notebook Notebook	- Active Host Blocks Specify the address to block and the duration for that block.
Source Statistics Statistics System Information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable 10.10.99.21 10.10.99.1 0.1 10 10 0 failse

La liste des clients désactivés du contrôleur contient désormais les adresses IP et MAC de

<u></u>	MONITOR WIL	WIS CONTROLLER	WIRELESS SE	CURITY MANAGEMENT	COMMANDS	HELP
Security	CIDS Shun List					
AAA General	Re-sync					
RADBUS Authentication RADBUS Accounting	IP Address	Last MAC Address	Expire	Sensor IP / Index		
Local Net Users	10.10.99.21	00:40:96:ad:0d:1b	326979296	192.168.5.2 / 1		
MAC Filtering Disabled Clients User Login Policies AP Policies						
Access Control Lists						
Network Access Control						
IPSec Certificates CA Certificate ID Certificate						
Web Auth Certificate						
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection						
Web Login Page						
CIDS Sensors						

ateur est ajouté à la liste Exclusion du

client.

Const Branner A. A.	MONITOR V	ALANS	CONTROLLER	WIRELESS SE	CURITY	MANAGEMENT	COMMINDS	HELP		
Monitor	Excluded Cli	ents								
Summary	Search by M	IAC addre		Sea	rch					
Statistics Controller	Client MAC A	Addr A	P Name	AP MAC Adde	WLAN	Туре	Exclusion	Reason	Port	
Wireless	00:40:96:ad:	06:15 A	P1242-2	00:14:15:59:3e:1	0 IPS	802.1	1b Unknown8	num:5	29	Detail LinkTest Disable Remove

Un journal de déroutement est généré lorsqu'un client est ajouté à la liste de déroutement.

Anna Brinnen	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management	32 14:41:00 2006 Regue AP : 00:15:c7:82:93:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface ne:0(802.11b/g) with RSSI: -83 and SNR: 6
Summary	Twe Apr 11 33 14:4016 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 14:39144 2006 Regue : 00:0b:85:54:de:5d removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
Communities Trap Receivers Trap Controls	Twe Apr 11 35 14:3744 2006 Regue : 00:0b:85:54:de:Se removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
Trap Logs	Twe Apr 11 36 14:39:44 Regue : 00:0b:05:55:54:de:5f removed from Base Radio NAC : 00:14:1b:59:3e:10 Interface an-bf802 11b.fa3

journal des messages est également généré pour



l'événement.

ertains événements supplémentaires sont générés dans le Cisco IPS Sensor lorsqu'une analyse NMAP est effectuée sur un périphérique qu'il

Input Options	Scan Options		-	Scan
C IP Range C IP List	Domain C Ac	tive Directory	C WMI API	
Single Host C Neighborhood IP Address:	Win32 OS Version	Users	Patch Level	Exit
10.1.1.12	Null IPC\$ Session	s 🖓 Services	MAC Address	Clear
	VetBIOS Shares	Disks	Sessions	Sava
	Date and Time	☐ Groups	Event Log	
	I Ping Host(s)	E Bindings	Errors	Help
	Traceroute Host			
General Options				
		TCP Ports	ican Range:	1 1024
Timeout for TCP/UDP/ICMP/SNMP:	5	UDP Port	scan Range:	1 1024
		E SNMP Co	mmunity String:	public
Retries: 3 Max Conne	rotions: 1024	1 900 00		1.
Retries: 3 Max Conne	ections: 1024			r
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP\NAC-/ SID: S-1-5-21-790525478-15804366	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP'NAC-J SID: S-1-5-21-790525478-15804366 MAC Addresses: MAC Addresses:	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP'NAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level:	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPVNAC-, SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC-, SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Pole: WT Workstation	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP\NAC-, SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Member Server Role: IAN Manager Workstat	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP\NAC SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Member Server Role: LAN Manager Workstat Role: LAN Manager Server	ACS 67-1343024091			
Retries: 3 Max Conne P Address: 10.1.1.11 NAC-ACS Computername: WORKGROUP/NAC-, SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Morkstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser	ACS 67-1343024091			
Retries: 3 Max Conne TP Address: 10.1111 NAC-ACS Computername: WORKGROUP/NAC- SID: S-1-S-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Sensite Rack d	ACS 67-1343024091			
Retries: 3 Max Conne TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP/NAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Morkstation Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Server Role: Comment: Service Pack 4 KB329115 Windows 2000 Hot	ACS 67-1343024091 ion			
Retries: 3 Max Conne TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUP/NAC-, SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho	tion tfix - KB329115 tfix - KB823182			
Retries: 3 Max Connection IP Address: IO.1.1.12 NAC-ACS Computername: WORKGROUP/NAC SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: Operating System: S.0 Role: NT Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB229115 Windows 2000 Hoi KB823559 Windows 2000 Hoi	tfix - KB329115 tfix - KB823182 tfix - KB823559			
Retries: 3 Max Conne IP Address: 007640000000000000000000000000000000000	tion tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823182			
Retries: 3 Max Connection IP Address: 10.1.1.11 NAC-ACS Computername: WORKGROUP/NAC SID: 5-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB23182 Windows 2000 Hot KB23182 Windows 2000 Hot KB24105 Windows 2000 Hot KB231319 Windows 2000 Hot	tions: 1024 ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823559 tfix - KB824105 tfix - KB824151 tfix - KB824151 tfix - KB824151			
Retries: 3 Max Connection TP Address: 10.1.1.11 NAC-AC3 Computername: WORKGROUP/NAC SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: Operating System: S.0 Role: NT Member Server Role: LAN Manager Workstation Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB23182 Windows 2000 Hot KB23182 Windows 2000 Hot KB23182 Windows 2000 Hot KB24105 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot	tfix - KB329115 fix - KB329115 fix - KB823182 fix - KB823182 fix - KB823559 fix - KB823559 fix - KB824105 fix - KB824151 fix - KB824151 fix - KB824151			
Retries: 3 Max Connection TP Address: 10.1.1.11 NAC-ACS Computername: WORKGROUP/NAC SID: S-1-S-21-790525478-15804366 MAC Addresses: 00096bd51c2 Patch Level: Operating System: Operating System: S.0 Role: NT Member Server Role: NAmager Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB23182 Windows 2000 Hot KB23182 Windows 2000 Hot KB231915 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot KB25119 Windows 2000 Hot KB25319 Windows 2000 Hot KB25232 Windows 2000 Hot	tfix - KB329115 tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823182 tfix - KB824105 tfix - KB824105 tfix - KB824151 tfix - KB824151 tfix - KB82635			

e fenêtre affiche les événements générés dans le Cisco IPS Sensor.

С

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

Exemple de configuration du capteur Cisco IDS

Voici le résultat du script de configuration de l'installation :

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#
```

Configurer un ASA pour IDS

Contrairement à un capteur de détection d'intrusion traditionnel, un ASA doit toujours se trouver dans le chemin de données. En d'autres termes, au lieu d'étendre le trafic d'un port de

commutateur à un port de reniflage passif sur le capteur, l'ASA doit recevoir des données sur une interface, les traiter en interne, puis les transférer vers un autre port. Pour IDS, utilisez le cadre de politique modulaire (MPF) afin de copier le trafic que l'ASA reçoit vers le module interne AIP-SSM (Advanced Inspection and Prevention Security Services Module) pour inspection.



Dans cet exemple, l'ASA utilisé est déjà configuré et transmet le trafic. Ces étapes montrent comment créer une stratégie qui envoie des données à AIP-SSM.

 Connectez-vous à l'ASA à l'aide d'ASDM. Une fois la connexion établie, la fenêtre Système principal ASA s'affiche.

📫 Cisco ASDM 5.1 for ASA - 172.16.26.2		deletetetetetete
File Rules Search Options Tools Wizards Help		
Home Configuration Monitoring Back Forward Search	Refresh Save Help	
Device Information	- Interface Status	
General License	Interface IP Address/Mask Line	Link Current Kbps
Host Name: ciscoasa.cisco.com	inside 172.16.26.2/24 O up O management 192.168.1.1/24 O down	up 3 down 0
ASA Version: 7.1(2) Device Uptime: 2d 5h 24m 51s ASDM Version: 5.1(2) Device Type: ASA5510 Firewall Mode: Routed Context Mode: Single	outside 10.10.102.224 Up	up u
Total Flash: 256 MB Total Memory: 256 MB	Reject an interface to view input and output kines.	
VPN Status IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0	Traffic Status Connections Per Decond Usage	
CPU CPU Usage (percent)	0.5	
00	+9 07:02	
17:07:32 19:07:02	- 'outside' Interface Traffic Usage (Kbps)	ii: 0
Memory Uzage (MB)	1	
64 192 64 17 07 32 19 07 02	0.0 17 07.02 Input Kbps: 0 Output Kbps:	0

2. Cliquez sur **Configuration** en haut de la page. La fenêtre bascule vers une vue des interfaces ASA.

Non-Kinning Dack Portward Samo Network abbn = Manapaces	8	0	0	0	0	2					
2500 5 8 10 11 21 13 1 3 10 원 왕 같이 2015 Interface Name Enabled <u>Becurty IP Address</u> <u>Bubnet Mask Management Only</u> <u>Description</u> metb00 <u>votate</u> <u>Yes</u> <u>010 10 10 2 2 55 255 25 0 No 1500</u> net0개 <u>ksinde</u> <u>Yes</u> <u>100 172 10 20 2 255 255 0 No 1500</u> net002 <u>No 100 172 10 20 2 255 255 0 No 1500</u> net002 <u>No 100 192 100 192 100 11 255 255 255 0 Yes 1500</u>	paration Montoring	Eack I	Forward	Search	Retresh	Save Help					
Interface Name Enabled Gaturity Level IP Address Bubnet Mask Only MTU Description Interface Name Enabled Gaturity Level IP Address Bubnet Mask Only MTU Description Interface Ves 010:10:10:27 255:255:55.0 No 1500 Interface No Ves 100:172:16:26.2 255:255:25.0 No 1500 Interface No Ves 100:192:16:81.1 255:255:25.0 Yes 1500	viguration + Interfaces								 		
Interface Name Enabled Baculty Level IP Address Bubnet Mask Only Management Only MTU Description med00 outside Yes 010.10.10.22 255.255.05 Mo 1500 med001 Mside Yes 100.17.216.2.0 255.255.05 Mo 1500 met002 No No No No 100 gement000 manage. Yes 100.192.168.1.1 255.255.05 Yes 1500	生辛(略)前;8	小的粉粉	6 9								
Interface Name Enabled Groups BP Address Bubnet Mark MTU Description met0/0 outside Yes 010.10.10.22 255.255.0 No 1500 met0/0 image Yes 100.17.2.16.26.2 255.255.0 No 1500 met0/2 No No No No No No gemen0/0 manage Yes 100.192.16.8.1.1 255.255.0 Yes 1500				Decurby			Macanerat		 		
Mactical Ves Otor 10.10/2 255.255.25.0 Mol Mol Vest011 Molde Ves 100172.16.26.2 255.255.25.0 Mol 1500 met0/2 No No No No No No germer#0/0 manage Ves 100192.168.1.1 255.255.255.0 Ves 1500	Interface	Name	Enabled	Level	IP Address	Subnet Mask	Only	MTU	Description	on	
Instant Instant <thinstant< th=""> <thinstant< th=""> <thi< td=""><td>c stemestro</td><td>putside</td><td>100</td><td>10017</td><td>10.102.2</td><td>255 255 255 0</td><td>No</td><td>500</td><td> </td><td></td><td></td></thi<></thinstant<></thinstant<>	c stemestro	putside	100	10017	10.102.2	255 255 255 0	No	500	 		
gemer#0/0 manage. Ves 100192.168.1.1 255.255.25.0 Ves 1500	Enemetari	ingide	Nes	199177	2.10.20.2	250.250.250.0	Peo his	1500			
	Management00	TO 30 808	Ves	10010	216811	0.845 555 545	Ved	500			
	and regentier solo			19919	al target to t	1001001000					
able braffic bedween two or more interfaces which are configured with same security levels	Enable traffic betwee	n two or more in	derfaces w	hich are confi	figured with is	ame security level					

3. Cliquez sur **Stratégie de sécurité** dans la partie gauche de la fenêtre. Dans la fenêtre résultante, sélectionnez l'onglet **Règles de stratégie de service**.

📫 Cisco ASDM 1	5.1 for ASA - 172,16.2	26.2	
File Rules Se	arch Options Tools	Wizards Help	fores foresas
Home C	configuration Monitorin	ng Back Forward Search Refresh Seve Hep	
-	Configuration + Security	y Policy + Senice Policy Rules	
bierfaces	• 👷 🖗 🖬 📋	3 時 8 影 8 (9)	
8	Access Rules	AAA Rules Piller Rules Piller Rules	
Security Policy	Show Rules for Interf	tace: All Interfaces Show All	
24		Traffic Classification Rule Actions Description	Add
NAT	E interface: inside, i	Enaded Match Source Lestination Service Inne Hange Policy Inside policy DO-Inside-policy	Edt
SK VEN	inside-class	Db @ any @ any ★ any traffic U\$ los promiscuous, permit traffic	Delete
<u>a</u>			
CSD Manager			
PS			
Routing			
A Constants			
Properties			
	De Match	🚯 Do not match 🕫 Show Summary 🔿 S	Show Detail
		Apply Reset Advanced	
	,		131/06 3:02:47 PM UTC

4. Cliquez sur Ajouter afin de créer une nouvelle stratégie. L'Assistant Ajout de règle de stratégie de service s'ouvre dans une nouvelle fenêtre.Cliquez sur Interface, puis choisissez l'interface correcte dans la liste déroulante afin de créer une nouvelle stratégie liée à l'une des interfaces qui transmettent le trafic.Donnez à la stratégie un nom et une description de ce qu'elle fait à l'aide des deux zones de texte.Cliquez sur Suivant pour passer à l'étape suivante.

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. Créez une nouvelle classe de trafic à appliquer à la stratégie.Il est raisonnable de créer des classes spécifiques afin d'inspecter des types de données spécifiques, mais dans cet exemple, Any Traffic est sélectionné pour la simplicité. Cliquez sur **Suivant** pour continuer.

📧 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	I
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. Complétez ces étapes afin dedemander à l'ASA de diriger le trafic vers son AIP-SSM.Cochez Enable IPS pour ce flux de trafic afin d'activer la détection des intrusions.Définissez le mode sur Promiscuité afin qu'une copie du trafic soit envoyée au module hors bande au lieu de placer le module en ligne avec le flux de données.Cliquez sur Autoriser le trafic afin de vous assurer que l'ASA passe à l'état d'ouverture en cas de défaillance de l'AIP-SSM.Cliquez sur Terminer afin de valider la modification.

🖆 Add Service Policy	Rule Wizard - Rule A	ctions		
Protocol Inspection	Intrusion Prevention	Connection Settings	QoS	1
Enable IPS for	this traffic flow			
Mode				
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

7. L'ASA est maintenant configuré pour envoyer le trafic au module IPS. Cliquez sur **Enregistrer** sur la ligne supérieure afin d'écrire les modifications dans l'ASA.

🛱 Cinco ASDM	5.1 for ASA - 172.16.	26.2							- 17 🗵
File Rules S	earch Options Tools	Wittards Help							
en e	Configuration Monto	ing Eack Forward S	Q Detresit	🗐 ? Save Help				91	disa disa.
	Configuration + Bacun	& Policy - Service Policy Rules							
	🔹 🕾 🐨 🖬 🛍	1246666							
10	C Access Rules	C AAA Rules C Filler Rules	 Service Policy Pall 	les					
Security Policy	Show Rules for Inter	riace: All Interfaces	hew Al						
24	7	ToR	Classification			Ru e Actions	D	escription	Add
NAT	Name	Enabled Match Source	Destination	Bervice	Tims Ranga		CO local de contra		Edit
<u>88</u>	inside-class	Line any	ia ang	🖈 ary traffic		🥥 jos promiscuous, permit traffic	De inside porky		Dalete
VPN									
<u> 8</u>									
CSD Hanager									
<u>,</u>									
Touting									
80									
Global Objects									
54									
Properties									
	1								
	Den Walds	Donal risksh						@ Show Summary C. Show Detail	
		Apply	Reset	Assess	al. [
Configuration sh	angee saved successful	De.					sadmine (NA (15)	213106 254	47 PM UTC

Configurer AIP-SSM pour l'inspection du trafic

Pendant que l'ASA envoie des données au module IPS, associez l'interface AIP-SSM à son moteur de capteur virtuel.

1. Connectez-vous à AIP-SSM à l'aide d'IDM.

Cisco IDM 5.0 - 172.16.26.10					e 🛯
File Help					
				Cisco Si	TETERS
Configuration Montoring Back Forwa	and Retresh He	•			\mathbf{A}
Configuration Montening Disk Form Configuration Status Disk Form Configuration Mitoweal Hosts Disk Form Configuration National Status Disk Form Configuration National Status Disk Form Configuration National Status Disk Status Configuration National Status Disk Status Configuration National Status Disk Status Disk Configuration National Status Disk Disk	vid Retresh He Network Specify the network Hostname: IP Address: Network Mask Default Route: FTP Timeout Vieb Server Setti IP Enable TLSISS Web server port.	ind communication parameters for the sensor. #ensor 172:16:26:10 1255:255:255:0 172:16:26:1 100 98	Remote Access Telnet is not a secure access service and is disabled by default. ✓ Enable Telnet	seconds	
IDM is initialized successfully.				cisco administrator	1 16

2. Ajoutez un utilisateur avec au moins des privilèges de

visionneuse.



3. Activez

l'interface.

Cisco IDM 5.0 - 172.16.26.10							
File Help							
🖓 🔳 🔇 🖸) 💿 🥊						Casco Systems
Configuration Monitoring Back Forwa	ed Retresh Help						A.A.
Configuration Kontoring Configuration Configurati	ed Retresh Hop Interfaces A sensing interface my and clicking Enable of Interface Name OrgabilEthernetS/1	st be enabled and assigned to Disable. Enabled Media Type Yes Backplane in	a virtual sensor	Before the set	Abernate TCP Reset interface -Noni	erface. You can enabledisable the available sensing interfaces by sele Description	ting the row(s)
Cleansing					Apply R	eset	
PM is in Walland our can of the						Idiana Jacket	inistrator A
num is initialized successibility.						cisco adm	10198-8001 (U

4. Vérifiez la configuration du capteur virtuel.



Configurer un WLC pour interroger l'AIP-SSM pour les blocs de clients

Effectuez ces étapes une fois que le capteur est configuré et prêt à être ajouté au contrôleur :

- 1. Choisissez Security > CIDS > Sensors > New in the WLC.
- 2. Ajoutez l'adresse IP, le numéro de port TCP, le nom d'utilisateur et le mot de passe que vous avez créés dans la section précédente.
- 3. Afin d'obtenir l'empreinte du capteur, exécutez cette commande dans le capteur et ajoutez l'empreinte SHA1 sur le WLC (sans le deux-points). Cette option permet de sécuriser la communication d'interrogation contrôleur/IDS.

```
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	WLANK	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)	98C9969B4EFA7- (hash key is alre	4F05280926660 ady set)	04830458487	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. Vérifiez l'état de la connexion entre AIP-SSM et le

WLC.								
Circo Station	MONITOR W	LANS CONTROLLE	R WIRELESS	SECURITY MAN	AGEMENT COMM	ANDS HELP		
Security	CIDS Sensor	s List						
AAA General	Index	Server Address 192.168.5.2	Port 443	State	Query Interval	Last Query (count) Unauthorized (1)	Detail	Remove
RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	2	172.16.26.10	443	Enabled	10	Success (1444)	Detail	Remove
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

Ajouter une signature de blocage à AIP-SSM

Ajoutez une signature d'inspection pour bloquer le trafic. Bien qu'il existe de nombreuses signatures pouvant effectuer le travail en fonction des outils disponibles, cet exemple crée une signature qui bloque les paquets ping.

1. Sélectionnez la **signature 2004 (requête d'écho ICMP)** afin d'effectuer une vérification de configuration

rapide.											
Cisco IDM 5.0 - 192,168.5.2											E 8 🛛
File Help											
Configuration Monitoring Eack Forward	d Retro	n Help									Cisco Sestius
⊕ Q, Sensor Setup	- Signature	Configuration	08								
- SNetwork	Calast D	All Piece	Anna al Relationaria	100.00							
- SAlowed Hosts	Devectory	r. Ive signa	enes To search outerne 1-								_
B G Centificates	Sig ID	SubSig ID	Name	Enabled	Action	Seventy	Fidelity	Type	Engine	Retired	Select All
- STime	-						Hating				NSDB Link
- Dusers	1330	2	TCP Drop - Urgent Pointer WL.	No	Modify Packet I	informatio	100	Default	Normalizer	No	
D 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
- Ninterface Pairs	1330	c	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
- Nitual Sensor	2002	0	KMP Source Queerb	Vas	Produce Alart	High	100	Tuned	Altomic IP	Nin	
- Wolobal Variables	2002		Mar Dource opening	hing	Propose Aven	right .	100	Turnera .	Page 10	140	Disable
Sissature Verlahlas	2003	0	ICMP Redirect	Tes	Produce Alert	High	100	Tuned	Adomic IP	NO	Actions
- Signature Configuration	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Atomic IP	No	Restore Defaults
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	Durate 1
Q. Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	
- Severt Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio.	100	Default	Atomic IP	No	Activate
- SuTarget Value Rating	2008	0	ICMP Timestamp Reply	No	Produce Alert	Informatio.	100	Default	Atomic IP	No	Rates
-Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	

 Activez la signature, définissez la gravité de l'alerte sur Élevé et définissez l'action d'événement sur Produire l'alerte et l'hôte de bloc de requête afin de terminer cette étape de vérification. Notez que l'action Hôte de bloc de requête est la clé pour signaler au WLC de créer des exceptions client.

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 Double 100 Bigeody ICMP Sequence: 100 Bigeody ICMP Tope: 100 Bigeody ICMP Tope: 100 Bigeody ICMP Tope: 100 Bigeody ICMP Tope: 100 Bige	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 Attert Trats: 0 Programe I Status: 0 Pragment Status: 0 Status: 0 Superity Layer 4 Protocol: Specify Layer 4 Protocol: Specify Layer 4 Protocol: Specify Layer 4 Protocol: Specify Layer 4 Protocol: Specify Layer 4 Protocol: Specify Layer 5 The Default Value. Click the icon to edithe value. Parameter uses a User-Defined Value. Click the icon to restore the default value.	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 4 Produce If I aver		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				8.8.8.8.8.8.8.8	ICMP Type:
Specify ICMP Identifier: No Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Help				Coacily ICMD Code:	
Aprices rower administer. 1980 Specify ICMP Total Length: No Parameter uses the Default Value. Click the icon to edit the value. OK Cancel Halp				Opecity ICMP Identifier	
Parameter uses the Default Value. Click the icon to edit the value. Parameter uses a User-Defined Value. Click the icon to restore the default value. OK Cancel Help				Concilia I CMP Total Langth:	
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	

🔍 Ed	it 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 Block Connection Request Block Host Request Snmp Trap Reset Tcp Connection	
-		Eranment Status	e' l'Anno III	•
•	Parameter uses the D Parameter uses a Use	efault Value. Click the ico rr-Defined Value. Click th	on to edit the value. The icon to restore the default value.	
			OK Cancel Help	

- 3. Cliquez sur **OK** pour enregistrer la signature.
- 4. Vérifiez que la signature est active et qu'elle est configurée pour effectuer une action de blocage.
- 5. Cliquez sur **Apply** afin de valider la signature sur le module.

Blocage et événements de surveillance avec IDM

Procédez comme suit :

 Lorsque la signature est correctement déclenchée, il y a deux endroits dans IDM pour le noter.La première méthode montre les blocs actifs installés par AIP-SSM. Cliquez sur Surveillance le long de la ligne supérieure des actions. Dans la liste des éléments qui s'affiche à gauche, sélectionnez Blocs d'hôtes actifs. À chaque fois que la signature ping se déclenche, la fenêtre Blocs d'hôte actif affiche l'adresse IP du contrevenant, l'adresse du périphérique attaqué et l'heure pour laquelle le blocage est en vigueur. La durée de blocage par défaut est de 30 minutes et est réglable. Cependant, la modification de cette valeur n'est pas abordée dans ce document. Consultez la documentation de configuration ASA si nécessaire pour plus d'informations sur la façon de modifier ce paramètre. Supprimez le bloc immédiatement, sélectionnez-le dans la liste, puis cliquez sur Supprimer.



La deuxième méthode d'affichage des signatures déclenchées utilise le tampon d'événements AIP-SSM. Dans la page Surveillance IDM, sélectionnez **Événements** dans la liste des éléments située sur le côté gauche. L'utilitaire de recherche Événements s'affiche. Définissez les critères de recherche appropriés et cliquez sur

Afficher....



2. L'Observateur d'événements apparaît ensuite avec une liste d'événements correspondant aux critères donnés. Faites défiler la liste et recherchez la signature ICMP Echo Request modifiée lors des étapes de configuration précédentes.Recherchez dans la colonne Événements le nom de la signature ou recherchez le numéro d'identification de la signature dans la colonne ID de

-	.,,	Sensor UTC Time	Event ID	Events	Sig ID	Details.
1	error:error	July 31, 2006 2:59:52 PM U	1145383740954940828	Unable to execute a host block [10.10.99.26] because blocking is not configured		
2	error:warning	July 31, 2006 3:16:51 PM U	1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
3	alert informati	July 31, 2006 3:19:16 PM U	1145383740954941574	ICMP Echo Request	2004	
4	error.error	July 31, 2006 3:19:16 PM U	1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
5	alert informati	July 31, 2006 3:19:46 PM U	1145383740954941597	ICMP Echo Request	2004	

3. Après avoir localisé la signature, double-cliquez sur l'entrée afin d'ouvrir une nouvelle fenêtre. La nouvelle fenêtre contient des informations détaillées sur l'événement qui a déclenché la

		1	
n n	nat	tur	D
Siu	ı la	เนเ	с.
- 0			

Section 1145383740954941597
<pre>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:</pre>
<pre>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</pre>

Contrôle de l'exclusion du client dans un contrôleur sans fil

La liste des clients désactivés du contrôleur est renseignée à ce stade avec l'adresse IP et MAC de l'hôte.

Core Server	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Fibering Disabled Clients User Login Policies AP Policies	Re-sync IP Addres 10.10.99.2	5 DC	ist MAC Address 0:40:96:ad:0d:1b	Expire 27	Sen: 172.	tor IP / Index 16.26.10 / 2		
Access Control Lists IPSec Certificates CA 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								

L'utilisateur est ajouté à la liste Exclusion du client.

Kora Barran	MONITOR WLAN	CONTROLLER	WIRELESS SEC	URITY MANAGEM	ENT COMMANDS H	εı₽	
Monitor Summary Statistics Controller Ports Wireless Ropue APs Known Rogue APs Ropue Clients Adhoc Rogues 802.3116 Radios 802.3116/g Radios Clients RADUS Servers	Excluded Clients Search by MAC ad Client MAC Addr 00:40:96:ad:0d:1b	AP Name AP0014.6940.81ce	Search AP NAC Addr 00:14:1b:5a:16:40	WLAN IPS	Type Exclusion R 802.11a UrknownEnu	eason Port n.5 29	Detail LinkTest Disable Remove

Surveiller les événements dans WCS

Les événements de sécurité qui déclenchent un blocage dans AIP-SSM font que le contrôleur ajoute l'adresse du délinquant à la liste d'exclusion du client. Un événement est également généré dans WCS.

 Utilisez l'utilitaire Monitor > Alarms du menu principal de WCS afin d'afficher l'événement d'exclusion. WCS affiche initialement toutes les alarmes non effacées et présente également une fonction de recherche sur le côté gauche de la fenêtre.

- 2. Modifiez les critères de recherche pour trouver le bloc client. Sous Gravité, sélectionnez **Mineur**, puis définissez la catégorie d'alarme sur **Sécurité**.
- 3. Cliquez sur Rechercher

Access Points 9 0 3 Location 0 0 0

Rechercher	•			
Cisco Wireless Control	System			Username: root Logout Refresh Print View
Monitor · Configure ·	Location - Administration - Help -			
Alarms	Alarms			- Select a command - ¥ 60
Record Rec				and a second sec
Critical	Severity Failure_Object	Owner	Date/Time	Message
Harm Calanary	Critical Radio AIR-LAP1242AG-A/1		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11b/g' is
All Types	Critical Radio_AIR-LAP1242AG-A/2		6/1/05 9:02 AM	AP 'AIR-LAP1242AG-A', interface '802.11a' is do
	Critical AP.AIR-LAP1242AG-A/00:14(1b)59:41:80		6/1/06 9:02 AM	AP 'AIR-LAP1242AG-A' disassociated from Control
Search	Critical Radio.api/75:12:e0/2		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11a' is down o
	Critical Radio.ao;75;12;e0/1		7/21/06 1:51 PM	AP 'ap:75:12:e0', interface '802.11b/g' is down
	Critical AP.ap.75:12:e0/00:0b:85:75:12:e0		7/21/06 1:51 PM	AP 'ap:75:12:e0' disassociated from Controller
	Critical Smitch Cisco, #187:4b/40.1.3.15		7/21/06 4:32 PM	Controller '40.1.3.15'. RADIUS server(s) are no
	Critical AP_AP2013.0493.04f0/00:13:5f:57:a3:60		7/21/06 4:38 PM	Fake AP or other attack may be in progress. Rog
	Critical AP.AP0013.0493.ba20/00:13:5f:57:4d:40		7/21/06 5:31 PM	Fake AP or other attack may be in progress. Rog
	Critical AP.AP142-0/00:14:10:5a:16:40		7/25/06 5:25 PM	Fake AP or other attack may be in progress. Rog
	Critical Radio AP-acc-c0750-48-1-FE1-0-3/2		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802
	Critical Radio AP-acc-c0750-48-1-FE1-0-3/1		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3', interface '802
	Critical AP.AP-acc-c3750-40-1-FE1-0-3/00:0b:05:52:a0:a0		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3' disassociated fr
	Critical AP_AP_acc-c3750-48-1-FE1-0-3/0018b:851521a01a0		7/26/06 2:02 PM	AP 'AP-acc-c3750-48-1-FE1-0-3' disassociated fr
Regues 0 28 Coverage				
Security 1 0 4				
Controllers 1 0 0				

4. La fenêtre Alarm répertorie ensuite uniquement les alarmes de sécurité avec une gravité mineure. Pointez la souris sur l'événement qui a déclenché le blocage dans AIP-SSM.En particulier, WCS affiche l'adresse MAC de la station client qui a déclenché l'alarme. En pointant l'adresse appropriée, WCS affiche une petite fenêtre avec les détails de l'événement. Cliquez sur le lien pour afficher ces mêmes détails dans une autre fenêtre.

Cisco Wireless C	Cisco Wireless Control System Username: root Logout Refresh Print V										
Monitor • Config	Monitor • Configure • Location • Administration • Help •										
Alarms		Alar	ms					Select a command			
Severity	v		Severity	Failure Object	Owner	Date/Time	Message				
			Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr				
Alarm Category			Minor	Client 00:40:95:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr				
Jocarity			Minor	Client 00:90:7a:04:6d:04		7/31/06 2:36 PM	Client '00:90:7a:04:6d:04' which was associated				
Search			Minor	Client 00:40:96:ad:0d:15		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated				
				Client '00:40:96.ad.0d.1 '00:14:16:56:16:40', htt code is '5(Unknown)'.	b' which was as rface 안 is exclu	sociated with AP ded. The reason					

Exemple de configuration de Cisco ASA

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

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

Exemple de configuration du capteur du système de prévention des intrusions 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#
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Installation et utilisation de Cisco Intrusion Prevention System Device Manager 5.1
- Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 Guides de configuration
- Configuration du capteur Cisco Intrusion Prevention System à l'aide de l'interface de ligne de commande 5.0 Configuration des interfaces
- Guide de configuration WLC 4.0
- <u>Assistance technique sans fil</u>
- Contrôleur de réseau local sans fil (WLC) Forum Aux Questions
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- <u>Configuration des solutions de sécurité</u>
- Support et documentation techniques Cisco Systems