Leitfaden zur Integration von Wireless LAN-Controllern und IPS

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Cisco IDS im Überblick Cisco IDS und WLC - Integrationsübersicht **IDS-Shunding** Netzwerkarchitekturdesign Konfigurieren des Cisco IDS-Sensors Konfigurieren des WLC Beispielkonfiguration für Cisco IDS-Sensoren Konfigurieren einer ASA für IDS Konfigurieren des AIP-SSM für die Datenverkehrsüberprüfung Konfigurieren eines WLC zum Abrufen des AIP-SSM für Client-Blöcke Hinzufügen einer Blockierungssignatur zum AIP-SSM Überwachung von Blockierung und Ereignissen mit IDM Überwachung des Client-Ausschlusses in einem Wireless-Controller Überwachung von Ereignissen in WCS **Cisco ASA - Beispielkonfiguration Cisco Intrusion Prevention System - Beispielkonfiguration** Überprüfung Fehlerbehebung Zugehörige Informationen

Einführung

Das Cisco Unified Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) ist Teil des Cisco Self-Defending Network und die erste integrierte kabelgebundene und Wireless-Sicherheitslösung der Branche. Cisco Unified IDS/IPS verfolgt einen umfassenden Sicherheitsansatz - am Wireless-Edge, am kabelgebundenen Edge, am WAN-Edge und im Rechenzentrum. Wenn ein verbundener Client schädlichen Datenverkehr über das Cisco Unified Wireless Network sendet, erkennt ein kabelgebundenes Cisco IDS-Gerät den Angriff und sendet keine Anfragen an Cisco Wireless LAN Controller (WLCs), die dann das Client-Gerät trennen.

Das Cisco IPS ist eine netzwerkbasierte Inline-Lösung, die schädlichen Datenverkehr, einschließlich Würmern, Spyware/Adware, Netzwerkviren und Anwendungsmissbrauch, genau

identifizieren, klassifizieren und stoppen kann, bevor sie die Geschäftskontinuität beeinträchtigen.

Mit der Cisco IPS Sensor Software Version 5 kombiniert die Cisco IPS-Lösung Inline-Prevention-Services mit innovativen Technologien, um die Genauigkeit zu erhöhen. Das Ergebnis ist uneingeschränktes Vertrauen in den Schutz Ihrer IPS-Lösung, ohne dass der legitime Datenverkehr verloren geht. Die Cisco IPS-Lösung bietet darüber hinaus einen umfassenden Schutz Ihres Netzwerks durch die einzigartige Möglichkeit, mit anderen Netzwerksicherheitsressourcen zusammenzuarbeiten, und bietet einen proaktiven Ansatz für den Schutz Ihres Netzwerks.

Mit der Cisco IPS-Lösung können Benutzer mehr Bedrohungen mit größerer Sicherheit stoppen, indem sie die folgenden Funktionen nutzen:

- Präzise Inline-Präventionstechnologien Bietet beispielloses Vertrauen, um vorbeugende Maßnahmen gegen eine Vielzahl von Bedrohungen zu ergreifen, ohne dass das Risiko besteht, legitimen Datenverkehr zu verwerfen. Diese einzigartigen Technologien ermöglichen eine intelligente, automatisierte, kontextbezogene Analyse Ihrer Daten und stellen sicher, dass Sie Ihre Intrusion Prevention-Lösung optimal nutzen können.
- Multi-Vector Threat Identification Schützt Ihr Netzwerk durch detaillierte Überprüfung des Datenverkehrs in Layer 2 bis 7 vor Richtlinienverletzungen, Schwachstellen-Exploitationen und ungewöhnlichen Aktivitäten.
- Einzigartige Zusammenarbeit im Netzwerk: Verbessert Skalierbarkeit und Ausfallsicherheit durch Netzwerkzusammenarbeit, einschließlich effizienter Techniken zur Erfassung des Datenverkehrs, Funktionen zum Lastenausgleich und Transparenz für verschlüsselten Datenverkehr.
- Umfassende Bereitstellungslösungen Bietet Lösungen für alle Umgebungen, von kleinen und mittleren Unternehmen (KMUs) und Zweigstellen bis hin zu Installationen großer Unternehmen und Service Provider.
- Leistungsstarke Management-, Ereigniskorrelations- und Support-Services Ermöglicht eine Komplettlösung mit Konfigurations-, Management-, Datenkorrelations- und erweiterten Support-Services. Das Cisco Security Monitoring, Analysis, and Response System (MARS) identifiziert, isoliert und empfiehlt die präzise Entfernung von Angriffselementen für eine netzwerkweite Intrusion Prevention-Lösung. Das Cisco Incident Control System verhindert neue Würmer- und Virenangriffe, indem es das Netzwerk in die Lage versetzt, sich schnell anzupassen und eine verteilte Reaktion darauf zu ermöglichen.

In Kombination bieten diese Elemente eine umfassende Inline-Präventionslösung, mit der Sie die größte Bandbreite an schädlichem Datenverkehr erkennen und stoppen können, bevor er die Geschäftskontinuität beeinträchtigt. Die Cisco Self-Defending Network-Initiative erfordert integrierte und integrierte Sicherheitsfunktionen für Netzwerklösungen. Aktuelle LWAPP-basierte WLAN-Systeme (Lightweight Access Point Protocol) unterstützen nur grundlegende IDS-Funktionen, da es sich im Wesentlichen um ein Layer-2-System handelt und die Verarbeitungsleistung für Leitungen begrenzt ist. Cisco veröffentlicht neuen Code zeitnah, um neue erweiterte Funktionen in die neuen Codes aufzunehmen. Version 4.0 bietet die neuesten Funktionen, darunter die Integration eines LWAPP-basierten WLAN-Systems in die Cisco IDS/IPS-Produktlinie. In dieser Version soll das Cisco IDS/IPS-System die WLCs anweisen, den Zugriff auf Wireless-Netzwerke für bestimmte Clients zu sperren, wenn ein Angriff auf Layer 3 bis Layer 7 erkannt wird, an dem der Client beteiligt ist.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Mindestanforderungen erfüllen:

- WLC-Firmware Version 4.x und höher
- Kenntnisse zur Konfiguration von Cisco IPS und Cisco WLC sind wünschenswert.

Verwendete Komponenten

Cisco WLC

Diese Controller sind in der Softwareversion 4.0 für IDS-Änderungen enthalten:

- Cisco WLC der Serie 2000
- Cisco WLC der Serie 2100
- Cisco WLC der Serie 4400
- Cisco Wireless Services Module (WiSM)
- Cisco Catalyst Unified Access Switch der Serie 3750G
- Cisco Wireless LAN Controller-Modul (WLCM)

Access Points

- Cisco Aironet Lightweight Access Points der Serie 1100 AG
- Cisco Aironet Lightweight Access Points der Serie 1200 AG
- Cisco Aironet Lightweight Access Points der Serie 1300
- Cisco Aironet Lightweight Access Points der Serie 1000

Management

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

Cisco Unified IDS/IPS-Plattformen

- Cisco IPS Sensoren der Serie 4200 mit Cisco IPS Sensor Software 5.x oder höher
- SSM10 und SSM20 für die Cisco Adaptive Security Appliances der Serie ASA 5500 mit Cisco IPS Sensor Software 5.x
- Cisco Adaptive Security Appliances der Serie ASA 5500 mit Cisco IPS Sensor Software 5.x
- Cisco IDS Network Module (NM-CIDS) mit Cisco IPS Sensor Software 5.x
- Cisco Catalyst Intrusion Detection System Module 2 (IDSM-2) der Serie 6500 mit Cisco IPS Sensor Software 5.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions (Technische Tipps von Cisco zu Konventionen).</u>

Cisco IDS im Überblick

Die wichtigsten Komponenten des Cisco IDS (Version 5.0) sind:

- Sensor-App Führt die Paketerfassung und -analyse durch.
- Event Storage Management and Actions Module Ermöglicht das Speichern von Richtlinienverletzungen.
- Imaging, Install and Startup Module (Imaging, Installation und Startmodul) Laden, Initialisieren und Starten der gesamten Systemsoftware.
- Benutzeroberflächen und UI-Support-Modul Stellt eine integrierte CLI und das IDM bereit.
- Sensor OS Host-Betriebssystem (basierend auf Linux).



Die Sensor Application (IPS Software) besteht aus:

- Main App: Initialisiert das System, startet und stoppt andere Anwendungen, konfiguriert das Betriebssystem und ist für Upgrades verantwortlich. Es enthält folgende Komponenten:Control Transaction Server - Ermöglicht es den Sensoren, Steuerungstransaktionen zu senden, die zum Aktivieren der Master-Sperrsensorfunktion des Attack Response Controllers (ehemals Network Access Controller) verwendet werden.Event Store - Ein indizierter Speicher zum Speichern von IPS-Ereignissen (Fehler, Status- und Warnsystemmeldungen), auf die über CLI, IDM, Adaptive Security Device Manager (ASDM) oder Remote Data Exchange Protocol (RDEP) zugegriffen werden kann.
- Interface App: Behandelt Umgehungs- und physische Einstellungen und definiert paarweise Schnittstellen. Die physischen Einstellungen bestehen aus Geschwindigkeits-, Duplex- und Verwaltungsstatus.
- Log App (Protokollanwendung): Schreibt die Protokollmeldungen der Anwendung in die Protokolldatei und die Fehlermeldungen in den Event Store.
- Attack Response Controller (ARC) (ehemals Network Access Controller) Verwaltet Remote-Netzwerkgeräte (Firewalls, Router und Switches), um Blockierungsfunktionen bereitzustellen,

wenn ein Warnereignis aufgetreten ist. ARC erstellt und wendet Zugriffskontrolllisten (ACLs) auf dem kontrollierten Netzwerkgerät an oder verwendet den Befehl **shun** (Firewalls).

- Notification App: Sendet SNMP-Traps, wenn sie durch Warn-, Status- und Fehlerereignisse ausgelöst werden. Die Benachrichtigungs-App verwendet dazu einen SNMP-Agent für eine öffentliche Domäne. Die SNMP GETs liefern Informationen zum Zustand eines Sensors.Webserver (HTTP RDEP2-Server) - Stellt eine Webbenutzeroberfläche bereit. Es bietet auch die Möglichkeit, über RDEP2 mit anderen IPS-Geräten zu kommunizieren, indem mehrere Servlets verwendet werden, um IPS-Dienste bereitzustellen.Authentifizierungsanwendung: Überprüft, ob Benutzer zur Ausführung von CLI-
 - , IDM-, ASDM- oder RDEP-Aktionen autorisiert sind.
- Sensor App (Analysis Engine) Führt die Paketerfassung und Analyse durch.
- CLI Die Schnittstelle, die ausgeführt wird, wenn sich Benutzer über Telnet oder SSH erfolgreich beim Sensor anmelden. Alle über die CLI erstellten Konten verwenden die CLI als Shell (mit Ausnahme des Dienstkontos - nur ein Dienstkonto ist zulässig). Zulässige CLI-Befehle hängen von der Berechtigung des Benutzers ab.

Alle IPS-Anwendungen kommunizieren miteinander über eine gemeinsame API (Application Program Interface), die IDAPI genannt wird. Remote-Anwendungen (andere Sensoren, Verwaltungsanwendungen und Software von Drittanbietern) kommunizieren über RDEP2- und SDEE-Protokolle (Security Device Event Exchange) mit Sensoren.

Beachten Sie, dass der Sensor über folgende Datenträgerpartitionen verfügt:

- Anwendungspartition: Enthält das vollständige IPS-Systemabbild.
- Maintenance Partition (Wartungspartition) Ein spezielles IPS-Image, das verwendet wird, um die Anwendungspartition von IDSM-2 neu zu formatieren. Ein Re-Image der Wartungspartition führt zu Verlust der Konfigurationseinstellungen.
- Wiederherstellungspartition Ein spezielles Abbild, das zur Wiederherstellung des Sensors verwendet wird. Durch das Starten in die Wiederherstellungspartition können Benutzer die Anwendungspartition vollständig neu abbilden. Die Netzwerkeinstellungen bleiben erhalten, aber alle anderen Konfigurationen gehen verloren.

Cisco IDS und WLC - Integrationsübersicht

Version 5.0 des Cisco IDS ermöglicht die Konfiguration von Ablehnungsaktionen, wenn Richtlinienverletzungen (Signaturen) erkannt werden. Je nach Benutzerkonfiguration im IDS/IPS-System kann eine Shun-Anfrage an eine Firewall, einen Router oder einen WLC gesendet werden, um die Pakete von einer bestimmten IP-Adresse zu blockieren.

Mit der Cisco Unified Wireless Network Software Version 4.0 für Cisco Wireless Controller muss eine Shun-Anfrage an einen WLC gesendet werden, um das auf einem Controller verfügbare Blacklisting oder Ausschlussverhalten der Clients auszulösen. Die Schnittstelle, die der Controller zum Abrufen der Shun-Anforderung verwendet, ist die Command-and-Control-Schnittstelle des Cisco IDS.

- Der Controller ermöglicht die Konfiguration von bis zu fünf IDS-Sensoren auf einem bestimmten Controller.
- Jeder konfigurierte IDS-Sensor wird durch seine IP-Adresse oder einen qualifizierten Netzwerknamen und Autorisierungsanmeldeinformationen identifiziert.
- Jeder IDS-Sensor kann auf einem Controller mit einer eindeutigen Abfragerate in Sekunden

konfiguriert werden.



IDS-Shunding

Der Controller fragt den Sensor mit der konfigurierten Abfragerate ab, um alle Shun-Ereignisse abzurufen. Eine gegebene Shun-Anforderung wird über die gesamte Mobilitätsgruppe des Controllers verteilt, der die Anfrage vom IDS-Sensor abruft. Jede Shun-Anforderung für eine Client-IP-Adresse gilt für den angegebenen Wert für die Timeout-Sekunden. Wenn der Timeout-Wert eine unbegrenzte Zeit anzeigt, endet das Shun-Ereignis nur, wenn der Shun-Eintrag auf dem IDS entfernt wird. Der gemiedete Client-Status wird auf jedem Controller in der Mobilitätsgruppe auch dann beibehalten, wenn einer oder alle Controller zurückgesetzt werden.

Hinweis: Die Entscheidung, einen Client zu sperren, wird immer vom IDS-Sensor getroffen. Der Controller erkennt keine Layer-3-Angriffe. Es ist weitaus komplizierter festzustellen, ob der Client einen bösartigen Angriff auf Layer 3 auslöst. Der Client wird auf Layer 2 authentifiziert, sodass der Controller den Layer-2-Zugriff gewähren kann.

Hinweis: Wenn einem Client z. B. eine IP-Adresse zugewiesen wird, die bereits einen Angriff auslöst (gelöscht), ist es an der Sensor-Zeitüberschreitung, den Layer-2-Zugriff für diesen neuen Client zu deaktivieren. Selbst wenn der Controller den Zugriff auf Layer 2 gewährt, kann der Client-Datenverkehr ohnehin an Routern in Layer 3 blockiert werden, da der Sensor auch Router über das Shun-Ereignis informiert.

Angenommen, ein Client hat die IP-Adresse A. Wenn der Controller das IDS auf Shun-Ereignisse abfragt, sendet das IDS jetzt die Shun-Anforderung an den Controller, wobei die IP-Adresse A die Ziel-IP-Adresse ist. Der Controller schwarz listet diesen Client A auf. Auf dem Controller werden Clients basierend auf einer MAC-Adresse deaktiviert.

Nehmen Sie nun an, dass der Client seine IP-Adresse von A in B ändert. Bei der nächsten Abfrage erhält der Controller eine Liste mit Clients, die auf der IP-Adresse basieren. Auch dieses Mal befindet sich die IP-Adresse A noch immer in der Liste "Shunned" (Shunned). Da der Client jedoch seine IP-Adresse von A nach B geändert hat (die nicht in der gefälschten Liste der IP-Adressen enthalten ist), wird dieser Client mit einer neuen IP-Adresse von B freigegeben, sobald die Zeitüberschreitung der in Blacklists aufgeführten Clients auf dem Controller erreicht ist. Der Controller lässt diesem Client nun die neue IP-Adresse von B zu (die MAC-Adresse des Clients bleibt jedoch gleich).

Obwohl ein Client während der Ausschlusszeit des Controllers deaktiviert bleibt und beim erneuten Abruf seiner vorherigen DHCP-Adresse wieder ausgeschlossen wird, wird dieser Client nicht mehr deaktiviert, wenn sich die IP-Adresse des Clients ändert, der nicht aufgerufen wird. Wenn der Client beispielsweise eine Verbindung mit demselben Netzwerk herstellt und das DHCP-Lease-Timeout nicht abgelaufen ist.

Controller unterstützen nur die Verbindung mit dem IDS für Client-Shunning-Anfragen, die den Management-Port des Controllers verwenden. Der Controller stellt über die entsprechenden VLAN-Schnittstellen, die Wireless-Client-Datenverkehr übertragen, eine Verbindung zum IDS für die Paketprüfung her.

Auf der Seite "Disable Clients" (Clients deaktivieren) wird auf dem Controller jeder Client angezeigt, der über eine IDS-Sensor-Anfrage deaktiviert wurde. Der Befehl CLI **show** zeigt auch eine Liste von Clients an, die auf Blacklists gesetzt sind.

Im WCS werden die ausgeschlossenen Clients unter der Unterregisterkarte "Sicherheit" angezeigt.

Im Folgenden finden Sie die erforderlichen Schritte, um die Integration von Cisco IPS-Sensoren und Cisco WLCs abzuschließen.

- 1. Installieren Sie die IDS-Appliance auf demselben Switch, auf dem sich der Wireless Controller befindet, und schließen Sie sie an.
- 2. Spiegelung (SPAN) der WLC-Ports, die den Wireless-Client-Datenverkehr zur IDS-Appliance übertragen.
- 3. Die IDS-Appliance empfängt eine Kopie aller Pakete und prüft den Datenverkehr auf Layer 3 bis 7.
- 4. Die IDS-Appliance bietet eine herunterladbare Signaturdatei, die auch angepasst werden kann.
- 5. Die IDS-Appliance generiert den Alarm mit einer Ereignisaktion "Shun", wenn eine Signatur eines Angriffs erkannt wird.
- 6. Der WLC fragt das IDS nach Alarmen ab.
- 7. Wenn ein Alarm mit der IP-Adresse eines Wireless-Clients, der dem WLC zugeordnet ist, erkannt wird, wird der Client in die Ausschlussliste aufgenommen.
- 8. Ein Trap wird vom WLC generiert, und WCS wird benachrichtigt.
- 9. Der Benutzer wird nach dem angegebenen Zeitraum aus der Ausschlussliste entfernt.

Netzwerkarchitekturdesign



Der Cisco WLC ist mit den Gigabit-Schnittstellen des Catalyst 6500 verbunden. Erstellen Sie einen Port-Channel für die Gigabit-Schnittstellen, und aktivieren Sie Link Aggregation (LAG) auf dem 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

Der Controller ist an die Schnittstelle Gigabit 5/1 und Gigabit 5/2 auf dem Catalyst 6500 angeschlossen.

cat6506#**show run interface gigabit 5/1** Building configuration...

```
Current configuration : 183 bytes
!
interface GigabitEthernet5/1
switchport
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
```

cat6506#show run interface gigabit 5/2
Building configuration...

Current configuration : 183 bytes !

```
interface GigabitEthernet5/2
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
cat6506#show run interface port-channel 99
Building configuration...
Current configuration : 153 bytes
interface Port-channel99
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

Die Sensorschnittstellen des IPS-Sensors können einzeln im **Promiscuous-Modus** betrieben werden oder Sie können sie zu Inline-Schnittstellen für den **Inline-Sensing-Modus** kombinieren.

Im Promiscuous-Modus fließen Pakete nicht durch den Sensor. Der Sensor analysiert eine Kopie des überwachten Datenverkehrs und nicht das tatsächlich weitergeleitete Paket. Der Vorteil des Promiscuous-Modus besteht darin, dass der Sensor den Paketfluss mit dem weitergeleiteten Datenverkehr nicht beeinträchtigt.

Hinweis: Das <u>Architekturdiagramm</u> ist nur eine Beispieleinrichtung der integrierten WLC- und IPS-Architektur. Die hier gezeigte Beispielkonfiguration erklärt die IDS-Sensorschnittstelle, die im Promiscuous-Modus arbeitet. Das <u>Architekturdiagramm</u> zeigt die Sensorschnittstellen, die zusammengefasst werden, um im Inline-Paarmodus zu agieren. Weitere Informationen zum Inline-Schnittstellenmodus finden Sie unter <u>Inline-Modus</u>.

Bei dieser Konfiguration wird davon ausgegangen, dass die Sensorschnittstelle im Promiscuous-Modus arbeitet. Die Überwachungsschnittstelle des Cisco IDS-Sensors ist an die Gigabit-Schnittstelle 5/3 des Catalyst 6500 angeschlossen. Erstellen Sie eine Überwachungssitzung auf dem Catalyst 6500, wobei die Port-Channel-Schnittstelle die Quelle der Pakete ist und das Ziel die Gigabit-Schnittstelle ist, an die die Überwachungsschnittstelle des Cisco IPS-Sensors angeschlossen ist. Dadurch wird der gesamte ein- und ausgehende Datenverkehr von den kabelgebundenen Schnittstellen des Controllers zum IDS für die Layer-3- bis Layer-7-Überprüfung repliziert.

```
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#

Konfigurieren des Cisco IDS-Sensors

Die Erstkonfiguration des Cisco IDS-Sensors erfolgt über den Konsolenport oder durch den Anschluss eines Monitors und einer Tastatur an den Sensor.

- 1. Melden Sie sich bei der Appliance an: Verbinden Sie einen Konsolenport mit dem Sensor.Schließen Sie einen Monitor und eine Tastatur an den Sensor an.
- 2. Geben Sie Ihren Benutzernamen und Ihr Kennwort an der Eingabeaufforderung ein. Hinweis: Der Standardbenutzername und das Standardkennwort sind beide Cisco. Bei der ersten Anmeldung bei der Appliance werden Sie aufgefordert, diese zu ändern. Sie müssen zuerst das UNIX-Kennwort (cisco) eingeben. Dann müssen Sie das neue Passwort zweimal eingeben.

```
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. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und die Zugriffsliste auf dem Sensor. Hinweis: Dies ist die Command-and-Control-Schnittstelle auf dem IDS, die für die Kommunikation mit dem Controller verwendet wird. Diese Adresse sollte an die Controller-Verwaltungsschnittstelle weitergeleitet werden können. Die Sensorschnittstellen erfordern keine Adressierung. Die Zugriffsliste sollte die Management-Schnittstellenadresse des/der Controller sowie zulässige Adressen für die Verwaltung des IDS enthalten.

```
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. Sie können den IPS-Sensor jetzt über die Benutzeroberfläche konfigurieren. Zeigen Sie den Browser auf die Management-IP-Adresse des Sensors. Dieses Bild zeigt ein Beispiel, in dem der Sensor mit 192.168.5.2 konfiguriert

ist.				
Cisco EM 5.0 - 192.168.5.2				C (# 🛛
File Help				Lained Research Barrier
				Cisco Secreus
Configuration Monitoring Back Forwar	d Retresh He			4.4
(D) Q, Sensor Setup	Network			
- Phatwork				
ID G. SSH	specity the network	and communication parameters for the sensor.		
(D G, Certificates	Line to serve	Teamor		
- STime	Hospanie.	press.		
- DUsers	10.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	102168 6.2		
- Sinterfaces	IP Address:	harvest		
- Dinterface Pairs		These have have a		
- Seypass	Network Mask:	1239.239.239.0		
ELC Apalenia Engine		1001000.6.1		
SVirtual Sensor	Default Route:	harmen		
-Solobal Variables		[305		
G. Signature Definition	FTP Timeout	low		seconds
- Signature Configuration			Provents Access	
- SCustom Signature Wittand	Web berver bebr		Teinet is not a secure access service	
- Somiscellaneous	P Enable TLS/SS	L	and is disabled by default.	
D S Event Action Rules	Web server port	443	Enable Teinet	
- STarpet Value Rating				
- Sevent Action Overrides				
- SNEvent Action Filters				
B Q Blocking				
- Selocking Properties				
- SOevice Login Profiles				
Selecting Devices Selecting Devices				
-SCat 6K Blocking Device Interfaces				
- Master Blocking Sensor				
© Q SNMP				
Trace Configuration				
- NAuto Update				
- Restore Defaults				
Silvetices Sensor				
- Dupdate Sensor				
DLicensing				
		Apply	Reset	
This is initialized assessed the				(alore (administrative) (

5. Fügen Sie einen Benutzer hinzu, den der WLC verwendet, um auf die IPS-Sensorereignisse zuzugreifen.

CIRCLEW 3.0 - 197.108.3.7				
File Help				
Configuration Monitoring Back Forward Ri	💽 📍 stresh Help			Cisco Sesti
B Q Sensor Setup	9			
- DNetwork	if the upers that have access to the sensor. The s	avira mia is a spacial mia that allows you to humans the	Ci Liferented. Only one service account is allowed	
- ThAllowed Hosts Open	wy sile opera shacmare access to she sensor. The s	entre role is a special role that anows you to oppass the	CD is needed. Only one service account is anower.	
B Q Contraine				
STime	Usemame	Role	Status	
Cisco Cisco	0	Administrator	Active	. 400
9 G. Interface Configuration				6.0
- Dinterfaces				601
- Ninterface Pairs				Datata
- Depass				Unine
Traffic Flow Notifications				
3 Q Analysis Engine	S Add ther			
- Ninual Sensor				
- Soliobal Variables	Usemame:	controller		
- Q Signature Definition				
- Signature Variables				
Designature Comparation	User Role:	Viewer		
Chiral status				
G Event Articio Rules				
- DEvert Variables	- Password			
- Target Value Rating				
- Devent Action Overrides				
- Sevent Action Filters	Password:			
- Someral Settings				
Q. Blocking				
- Sollocking Properties	Confirm Password	£ 11		
- Device Login Profiles				
- TwBlocking Devices				
Device Blocking Device Interfaces				
Muster Discking Device Interfaces	OK	Cancel Help		
C caluto				

6. Aktivieren Sie die Überwachungsschnittstellen.



Die Überwachungsschnittstellen müssen der Analysis Engine hinzugefügt werden, wie in diesem Fenster Folgendes angezeigt

wird:				
 Cisco IDM 5.0 - 192.168.5.2 				
File Help				
Configuration Monitoring Back Forward	nd Retresh	e Nep		Cosce Systems
 C Sensor Setup Nietwork Nietwork Hosts Q SSH Q Centificates Sittime 	Vitual Senso The sensor assign and	or monitors traffic that traverses interfaces or interface pa remove interfaces (or pairs). You cannot add a new vit	ers assigned to a vidual sensor. Click Edit to change the properties of the default vidual sensor. You can change the buai sensor or change the vidual sensor name.	description or
LNUsers	Name	Assigned Interfaces (or Interface Pains)	Description	Edit
G A interface Configuration Sinterfaces Notefface Pairs Noteffaces Noteffaces Noteffaces Noteffaces	vs0	OlgabitEthernet0/0 OlgabitEthernet0/1 OlgabitEthernet0/2 OlgabitEthernet0/2	default Wrbual sensor	
Q. Analysis Engine Nindust Bansar Diobal Variables				

7. Wählen Sie die 2004-Signatur (ICMP Echo Request) aus, um eine schnelle Einrichtungsüberprüfung

durchzufuhren.											
Cisco IDM 5.0 - 192,168.5.2											
File Help											
Configuration Monitoring Back Forms	nd Retres	n Help									Cisco Systems
Q Sensor Setup - Nvietwork - SAllowed Hosts	Select By	Configurati	on tures 💌 Select Criteria: 🖡	-N8A							
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 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	Clone
- Severas	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	Adomic IP	No	Enable
PMitual Sensor Solicitud Viciables	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					Produce Alert	1.1.1		-			Actions
- Signature Configuration	2004		ICMP Echo Request		Request Block			Tuned	Abornic IP	No	Restore Defaults
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	Contrato I
© Q. Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	
- Sevent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	informatio	100	Default	Atomic IP	No	Activate
Target Value Rating Scient Action Contribut	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	

Die Signatur sollte aktiviert sein, der Alert-Schweregrad auf **Hoch** und die Event Action (Ereignisaktion) auf **Produce Alert** and **Request Block Host** gesetzt sein, damit dieser Verifizierungsschritt abgeschlossen werden kann.



Konfigurieren des WLC

Gehen Sie wie folgt vor, um den WLC zu konfigurieren:

- 1. Wenn die IPS-Appliance konfiguriert ist und im Controller hinzugefügt werden kann, wählen Sie Security > CIDS > Sensors > New aus.
- Fügen Sie die IP-Adresse, die TCP-Portnummer, den Benutzernamen und das Kennwort hinzu, die Sie zuvor erstellt haben. Um den Fingerabdruck vom IPS-Sensor abzurufen, führen Sie diesen Befehl im IPS-Sensor aus, und fügen Sie den SHA1-Fingerabdruck auf dem WLC hinzu (ohne Doppelpunkt). Diese Funktion dient zum Sichern der Abfragekommunikation zwischen Controller und 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 Stateme	And States	Section of the Section	A Minister Street	un bring and	Sundal States Towners	Save Co	nfiguration	Ping Logour	Refresh
A. A.	MONITOR WLAN	S CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security 💌	CIDS Sensor Ad	1					< Back	Apply	/
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients	Index Server Address	1 .							
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 Wireless Protection	Query Interval	15 50	conds						
Policies Trusted AP Policies Rome Policies	State	R							
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection Web Login Page	Fingerprint (SHA1 hash)	1662E996362A9	A1EF08899A7C	1645F5CB56A	8842 40 he	x chars			
CIDS Sensors Shunned Clients									

3. Überprüfen Sie den Status der Verbindung zwischen dem IPS-Sensor und dem WI C

Sam Service A	MONETOR W	LANS CONTROLLER	WIRELESS	SECURITY M	NAGEMENT COMM	ANDS HELP		Save Configuration Ping	Logout Re
Security	CIDS Sensors	List							New
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Pitering Disabled Clients	Index 1	Server Address 192.160.5.2	Port 443	State Enabled	Query Interval	Last Query (count) Success (6083)	Ostail Remove		
AP Policies Access Control Lists									
Network Access Central IPSec Certificates CA Certificate									
Web Auth Certificate									
Pelicies Trusted AP Policies Rogue Policies Standard Signatures Signature Events Summery Client Exclusion Policies AP Authentication Nanagement Frame Protection									
Web Login Page CIDS Sensors Shuroad Clients									

4. Wenn Sie die Verbindung mit dem Cisco IPS-Sensor hergestellt haben, stellen Sie sicher, dass die WLAN-Konfiguration korrekt ist und dass Sie die Client-Ausschluss aktivieren.Der Timeout-Standardwert für Clientausschlüsse ist 60 Sekunden. Beachten Sie außerdem, dass der Client-Ausschluss unabhängig vom Client-Ausschlusszeitgeber so lange andauert, wie der vom IDS aufgerufene Clientblock aktiv bleibt. Die standardmäßige Blockierungszeit im IDS beträgt 30

Minuten.

Conce Destrone									Save Config.	ration Ping	Logout Refre
AA	MONITOR WLANS CO	ONTROLLER WIRELE	SS SECURITY	MANAGEMENT	COMMANDS	HELP					
WLANS	WLANs > Edit								1	< Back	Apply
WLANS	WLAN ID	1									
AP Groups VLAN	WLAN SSID	1PS									
	General Policies						Security Policies				
	Radio Policy	All 💌					1Pv6 Enable				
	Admin Status	💽 Enabled									
	Session Timeout (secs)	1800					Layer 2 Security	WPA1+WPA2	~		
	Quality of Service (QoS)	Silver (best effort)	~					MAC hitering			
	WMM Policy	Disabled 🐱					Layer 3 Security	None	¥		
	7920 Phone Support	Client CAC Limit	🗌 AP CAC Limit					Web Policy *			
	Broadcast 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	out Value (cerci)				** When client exclusion	n is enabled, a time:	out value of		
	DHCP Server	C Override	and a serie (reces)				reset excluded clients)	require administrati	ve overnde to		
	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 IPS	EC, LZTP, PPTP, O	RANITE and FORT	RESS authentical	ions.					
	CISCO Client Extension (CCX)										
	Version IE	Enabled									
	Aironet IE	X									
	Gratuitous Probe Response										
	Radius Servers										
		Authentication Server	Accounting	Servers							
	Server 1	1P:10.1.1.12, Port:18	12 🛩 none 🛩								

5. Sie können ein Ereignis im Cisco IPS-System auslösen, wenn Sie eine NMAP-Prüfung auf bestimmte Geräte im Netzwerk durchführen oder wenn Sie einen Ping an einige Hosts senden, die vom Cisco IPS-Sensor überwacht werden. Sobald ein Alarm im Cisco IPS ausgelöst wird, gehen Sie zu Monitoring und Active Host Blocks, um die Details zum Host zu überprüfen.

Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	₽ Help
Norried Abackers Norried Abackers Norrier Hass Blocks Norrier Hass Blocks Norrier Block	Active Host Blocks Specify the address to block and the duration for that block.
B & Support Internation Diagnostics Report Statistics System Information	Source IP Destination IP Destination Port Protocol Minutes Remaining Timeout (minutes) VLAN Connection Block Enable 10.10.99.21 10.10.95.1 0 1 10 10 0 failse

Die Liste "Shunned Clients" im Controller ist jetzt mit der IP- und MAC-Adresse des Hosts

Luce Former	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	CIDS Shu	n List							
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Re-sync IP Addres 10.10.99.2	s La L 00	st MAC Address	Expire 326979296	Ser 192	isor IP / Index 160.5.2 / 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									
иц. И И И АН			. ,						
itzer wird der Clier	ntaussch	nlussl	iste						

hinzugefügt.

A. A.	MONITOR WU	ANS CONTROLLER	WIRELESS SEC	URITY MANAGEMENT	COMMANDS HELP		
Monitor	Excluded Client	ts					
Summary	Search by MAC	address	Search	h			
Controller	Client MAC Add	dr AP Name	AP MAC Adde	WLAN Type	Exclusion Reason	Port	
Wireless	00:40:96:66:06	1b AP1242-2	00:14:15:59:3e:10	IPS 802.1	1b UnknownEnum:5	29	Detail LinkTest Disable Remove

Ein Trap-Protokoll wird generiert, während ein Client der Shun-Liste hinzugefügt

	32	14:41:00	Rogue AP : 00:15:c7:02:03:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface
Management		2006	no:0(802.11b/g) with R551: -83 and SNR: 6
Summary	33	Tue Apr 11 14:40:16 2006	New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2
General SNMP V3 Users	34	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:54 removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(802.11b/g)
Communities Trap Receivers Trap Controls	35	Tue Apr 11 14:39:44 2006	Rogue : 00:0b:85:54:de:Se removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(002.11b/g)
Trap Logs	36	Tue Apr 11 14:39:44	Reque : 00:0b:85:54:de:Sf removed from Base Radio MAC : 00:14:1b:59:3e:10 Interface

das Ereignis wird auch ein Meldungsprotokoll



generiert.

Im

Cisco IPS-Sensor werden einige zusätzliche Ereignisse generiert, wenn eine NMAP-Prüfung auf einem überwachten Gerät durchgeführt

Input options	Scan Options		-	Scan
C IP Range C IP List	Domain Ac	tive Directory	C WMI API	Goar
Single Host C Neighborhood IP Address:	₩in32 OS Version	Users	Patch Level	Exit
10.1.1.12	Null IPC\$ Sessions	s 🔽 Services	MAC Address	Clear
	✓ NetBIOS Shares	Disks	C Sessions	Save
	Date and Time	Groups	Event Log	
	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:	ublic
Retries: 5 Plax Conne	ecoons: 11024			
DP AUDITESS TO LET 17 MALTER S				
Computername: WORKGROUPWAC-	ACS			
1P A001955: 10:1-1:12 NAC-ACS Computername: WORKGROUP/NAC- SID: S-1-5-21-790525478-15804366	ACS 67-1343024091			
TP AGUTESS: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses:	ACS 67-1343024091			
IP AGUIISS: 10:1:1:12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096b8d51c2	ACS 67-1343024091			
IP AGUINSS: 10:1:1:1 NAC-ACS Computername: WORKGROUPWAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009668d51c2 Patch Level:	ACS 67-1343024091			
Computername: WORKGROUPNAC- SID: S-1-S-21-790525478-15804366 MAC Addresses: 0009668d51c2 Patch Level: Operating System: 5.0	A⊂S 67-1343024091			
TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Member Server	ACS 67-1343024091			
IP 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 Role: NT Workstation	ACS 67-1343024091			
IP 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 Role: NT Workstation Role: LAN Manager Workstat	ACS 67-1343024091 tion			
TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666d51c2 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 tion			
TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser	ACS 67-1343024091 tion			
IP 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 Role: LAN Manager Vorkstal Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Comment:	ACS 67-1343024091 tion			
IP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009668d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Member Server Role: LAN Manager Workstal Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KD229215, Windows 2000 Mo	ACS 67-1343024091 tion			
TP Aduress: 10.1.1.12 NAC-ACS Computername: WORKGROUPVAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096668d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: NT Member Server Role: LAN Manager Workstat Role: LAN Manager Server Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115			
TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666851c2 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: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823182			
IP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009668d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Workstat Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823182 Windows 2000 Ho KB823559 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823559			
IP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: IAN Manager Workstal Role: LAN Manager Workstal Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823559 Windows 2000 Ho KB824105 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823182 tfix - KB824161			
TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPVAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666d51c2 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: Service Pack 4 KB329115 Windows 2000 Ho KB823559 Windows 2000 Ho KB824105 Windows 2000 Ho KB824105 Windows 2000 Ho KB824151 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823182 tfix - KB823151 tfix - KB824105 tfix - KB824151 tfix - KB824151			
IP AGUNDS: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-S-21-790525478-15804366 MAC Addresses: 00096b8d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstaf Role: LAN Manager Workstaf Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB323182 Windows 2000 Ho KB823182 Windows 2000 Ho KB823182 Windows 2000 Ho KB824151 Windows 2000 Ho KB824151 Windows 2000 Ho KB824151 Windows 2000 Ho KB825119 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823182 tfix - KB824151 tfix - KB824151 tfix - KB824151 tfix - KB824151			
IP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 0009666d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: LAN Manager Workstal Role: LAN Manager Workstal Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823559 Windows 2000 Ho KB823559 Windows 2000 Ho KB824105 Windows 2000 Ho KB825119 Windows 2000 Ho KB825119 Windows 2000 Ho KB8251219 Windows 2000 Ho KB826232 Windows 2000 Ho	ACS 67-1343024091 tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB823155 tfix - KB824105 tfix - KB824105 tfix - KB824105 tfix - KB824105 tfix - KB824105			
TP Address: 10.1.1.12 NAC-ACS Computername: WORKGROUPNAC- SID: S-1-5-21-790525478-15804366 MAC Addresses: 00096668d51c2 Patch Level: Operating System: 5.0 Role: NT Member Server Role: IAN Manager Workstal Role: LAN Manager Workstal Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Ho KB823162 Windows 2000 Ho KB823159 Windows 2000 Ho KB824105 Windows 2000 Ho KB824105 Windows 2000 Ho KB824151 Windows 2000 Ho KB824151 Windows 2000 Ho KB824351 Windows 2000 Ho KB826323 Windows 2000 Ho KB828035 Windows 2000 Ho KB828035 Windows 2000 Ho	ACS 67-1343024091 tion tfix - KB329115 tfix - KB823182 tfix - KB823182 tfix - KB824105 tfix - KB824151 tfix - KB824151 tfix - KB824151 tfix - KB824151 tfix - KB828155 tfix - KB828035 tfix - KB828035			

diesem Fenster werden die im Cisco IPS-Sensor generierten Ereignisse angezeigt.

Monitoring Monitoring Denied Attackers Durtwe host Blocks Divervork Blocks Divervork Blocks Divervork Blocks Divervork Blocks Divervork Blocks	Option Option Peep Events Events Events You can display the events in the local Event Blore. By default all events are displayed. To fits on event type and/or time, select the appropriate check toxes. Show alert events: P informational P Low P Medure P High Bhow error events: P informational P Low P Medure P High	or .
- Distatutics	Q. Lincol Warmer	
Solystem Information		•
	If the part of the second	1000 DEMOL.
	16 ale4blab 100 Anril 11 200 1144003216061613642 ICMP Echo Request	2004
	19 abertiow 32 April 1 200 1144003216851013656 SMB ADMINE Hidden Share Access Atempt	1329
	18 alertinformati, April 11, 200, 1144003216861013655 SMR Windows Share Enumeration	3322
	20 alertinformati. April 11, 200 1144003216861913660 SMB: Windows Share Enumeration	3322
	21 empremor April 11, 200 1144003216861913665 Unable to execute a host block timeout (10.10.99.2) because blocking is disabled	
	22 alertinformati. April 11, 200 1144063216661913696 TCP SYN Host Sweep	30.30
	23 alertinformati. April 11, 200 1144003216661913706 TCP SYN Host Sweep	3030
	25 alerthigh:100 April 11, 200 1144003216661913712 ICMP Echo Reply	2000
	26 error error April 11, 200 1144503216861913714 Unable to execute a host block [10.10.99.22] because blocking is disabled	
	24 alerthigh:100 April 11, 200 1144003216861913710 ICMP Echo Request	2004
	27 alertmedium April 11, 200 1144003216861913715 IOS UDP Bomb	4600
	29 aleftmedium April 11, 200	4060
	30 aletmedium April 11, 200 1144003216861913718 IOS UDP Bomb	4600
	31 alertmedium April 11, 200 1144003216661913719 Back Orifice Ping	4060
	32 aletmedium April 11, 200 1144003216661913720 IOG UDP Bomb	4600 - Rebesh

Beispielkonfiguration für Cisco IDS-Sensoren

Dies ist die Ausgabe des Setup-Skripts für die 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#
```

Konfigurieren einer ASA für IDS

Anders als bei einem herkömmlichen Angriffserkennungssensor muss sich eine ASA immer im Datenpfad befinden. Anders ausgedrückt: Anstatt den Datenverkehr von einem Switch-Port über

einen passiven Sniffing-Port am Sensor zu verteilen, muss die ASA Daten über eine Schnittstelle empfangen, intern verarbeiten und dann an einen anderen Port weiterleiten. Für IDS verwenden Sie das Modular Policy Framework (MPF), um Datenverkehr, den die ASA empfängt, zur Überprüfung an das interne Advanced Inspection and Prevention Security Services Module (AIP-SSM) zu kopieren.



In diesem Beispiel ist die verwendete ASA bereits eingerichtet und leitet den Datenverkehr weiter. Diese Schritte veranschaulichen die Erstellung einer Richtlinie, die Daten an das AIP-SSM sendet.

 Melden Sie sich mit ASDM bei der ASA an. Nach erfolgreicher Anmeldung wird das Fenster "ASA Main System" angezeigt.

📫 Cisco ASDM 5.1 for ASA - 172.16.26.2		tieletieletieletie
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 Li	nk Current Kbps
Host Name: ciscoasa.cisco.com	Inside 172.16.26.2/24 O up O u management 192.168.1.1/24 O down O d	p 3 own 0
ASA Version: 7.1(2) Device Optime: 2d 5h 24m 51s ASDM Version: 5.1(2) Device Type: ASA5510 Firewall Mode: Routed Context Mode: Single	0019109 10.10.102.2724 U up U u	
Total Flash: 256 MB Total Memory: 256 MB	Select an interface to view input and output kthrs	
VPN Status IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels: 0	Traffic Status Connections Per Second Usage	1
System Resources Status CPU CPU Uzage (percent)	1 ⁴	
15 00 04 02	49 07-02 ■ UDP: 0 ■ TCP: 0 ■ Total: (
17.07.32 17.07.02	- 'outside' Interface Traffic Usage (K0-ps)	
Memory Usage (MB) 250 192 64.0 64	0.6 19 07.02	
17:07:32 17:07:02	Input Kbps: 0 E Output Kbps: ()

2. Klicken Sie oben auf der Seite auf Konfiguration. Das Fenster zeigt die ASA-Schnittstellen

digur ation	Montoring	Dack Pr	·····	Search	Retresh	Save He						4.4
+ <u>+</u> 3	(1 11 2) (111) (113) (113)	10. 55 R	9						 		 	
	interface	Name	Enabled	Security Level	IP Address	Gubnet M	ask Managemer	MTU	 De	escription	 	Add
Etherne	apio	outside	Yes	Q	10.10.102.2	255 255 255	i0 No	1500				Edit
Etherne	10/1	Inside	Yes	100	172.16.26.2	255 255 255	0 No	1500	 			Delete
Etherne	40/2		No				No					
Manage	iment0/0	manage	Yes	100	192.160.1.1	255 255 255	0 Yes	1500				

3. Klicken Sie links im Fenster auf **Sicherheitsrichtlinie**. Wählen Sie im sich daraus ergebenden Fenster die Registerkarte **Service Policy Rules (Servicebestimmungen**) aus.

📫 Cisco ASDM	5.1 for ASA - 172.16.26.2	
File Rules Se	rarch Options Tools Wizards Help	Cotto Sections
Home	Configuration Montoring Back Forward Search Ratherh Save Help	A. A.
	Condustation > Security Palicy > Servera Palicy Rules	
Ξ,	◆ 魚 平 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
Interfaces	C Access Rules C AAA Rules C Filter Rules C Sterice Policy Rules	
<u> </u>	Show Rules for Interface: All Interfaces 💌 Show All	
Security Policy	Traffic Classification	Add
NAT	Name Enabled Match Source Destination Service Time Range Huber Closes Destination	Edt
03	Debetice: Inguise Policy Inside-policy Debetice: Inguise Policy Inside-policy Debetice: Inguise Policy Inside-policy	Delete
VPN		
<u>a</u>		
CSD Manager		
۵,		
P5		
*25 Routing		
CRUBH Objects		
5		
Properties		
	Cab Match 🚯 Do not match 🕫 Show Summary C Show Summary	etail
	Apply Reset Advanced	
		20247 PM UTC

4. Klicken Sie auf Hinzufügen, um eine neue Richtlinie zu erstellen. Der Assistent zum Hinzufügen von Service Policy-Regeln wird in einem neuen Fenster gestartet.Klicken Sie auf Interface (Schnittstelle), und wählen Sie dann in der Dropdown-Liste die richtige Schnittstelle aus, um eine neue Richtlinie zu erstellen, die an eine der Schnittstellen gebunden ist, die den Datenverkehr weiterleiten.Geben Sie der Richtlinie einen Namen und eine Beschreibung der Vorgehensweise in den beiden Textfeldern.Klicken Sie auf Weiter, um mit dem nächsten Schritt

fortzufahren.

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

5. Erstellen Sie eine neue Datenverkehrsklasse, die auf die Richtlinie angewendet werden soll.Es ist sinnvoll, spezifische Klassen zu erstellen, um bestimmte Datentypen zu überprüfen. In diesem Beispiel wird jedoch Any Traffic (Beliebiger Datenverkehr) aus Gründen der Einfachheit ausgewählt. Klicken Sie auf Weiter, um fortzufahren.

🖆 Add Service Policy Rule Wiz	zard - Traffic Classificatio	on Criteria	
	[· · · ·	1	
 Create a new traffic class: 	Inside-class		
Description (optional):			
Traffic match criteria			
🗌 Default Inspection T	raffic		
🗌 Source and Destina	tion IP Address (uses ACL)		
🔲 Tunnel Group			
TCP or UDP Destination	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 c C Use class-default as the tra	ing traffic class, then it will m atch all situation. ffic class.	atch the class-default traffic clas	s.
		< Back Ne	kt > Cancel Help

6. Führen Sie diese Schritte aus, umWeisen Sie die ASA an, den Datenverkehr an ihr AIP-SSM weiterzuleiten. Aktivieren Sie IPS für diesen Datenverkehrsfluss aktivieren, um die Angriffserkennung zu aktivieren. Legen Sie den Modus auf Promiscuous fest, sodass eine Kopie des Datenverkehrs an das Out-of-Band-Modul gesendet wird, anstatt das Modul in Übereinstimmung mit dem Datenfluss zu platzieren. Klicken Sie auf Datenverkehr zulassen, um sicherzustellen, dass die ASA bei Ausfall des AIP-SSM in den Fail-Open-Zustand wechselt. Klicken Sie auf Fertig stellen, um die Änderung zu bestätigen.

🖆 Add Service Policy Rule Wizard - Rule Actions	
Protocol Inspection Intrusion Prevention Connection Settings QoS	
Mode	
C Inline Mode	
In this mode, a packet is directed to IPS and the packet may be dropped as a result of IPS operation.	
Promiscous Model	
In this mode, a packet is duplicated for IPS and the original packet cannot be dropped by IPS.	
If IPS card fails, then	
Permit traffic	
C Close traffic	
< Back Finish	Cancel Help

7. Die ASA ist jetzt so konfiguriert, dass Datenverkehr an das IPS-Modul gesendet wird. Klicken Sie in der obersten Zeile auf **Speichern**, um die Änderungen in die ASA zu schreiben.

🖆 Cinco ASDM 🤉	5.1 for ASA - 172.16	.26.2							_ I 🛛 🗙
File Rules Se	arch Options Tools	Wittands Help							
ik ve	Configuration Monitor	ing Dack Forward Sa	kich Retresit	🔜 🢡 Save Hep				1	nte Serrier Absorbs
	Configuration + Babur	IV Policy - Service Policy Rules							
	🔹 🚊 🐨 🖬 🚺	12 時間島高岡()							
Interfaces	C Access Rules	C AAA Rules C Filter Rules	Service Policy Rule	ies -					
Security Policy	Show Rules for Inte	riace: All Interfaces 💌 Bit	ow All						
24	2	TOPIC	Sassification			Ru e Actions		Description	A00
NAT	Name	Enabled Match Source	Destination	Bervice	Tims Ranga				Edit
68	E menace inside inside class	Policy: incide policy	🎱 are	🔹 arvitafic		🗑 jos promiscuous, permit traffic	IDE INSIGE DOLKY		Dalete
VPN						de la la seconda la seconda de la second			
<u> 6</u>									
CSD Hanager									
1 75									
- 28 Forder									
(Contraction)									
Girland Chinema									
2-0									
	De Malch	🎦 Oonal risich							
		Apply	Reset	A19990	al.				
Configuration sha	l Inges saved successfu	lk					sadmine NA (1	0 📑 🔂 🔒 7/31/06 2:5	147 PM UTC

Konfigurieren des AIP-SSM für die Datenverkehrsüberprüfung

Während die ASA Daten an das IPS-Modul sendet, ordnen Sie die AIP-SSM-Schnittstelle der virtuellen Sensor-Engine zu.

1. Melden Sie sich mit IDM beim AIP-SSM an.

File Help	Cisco IDM 5.0 - 172.16.26.10				
With With With With With With With With	File Help				
Control Mathematical Stress Control Control Contro Control					Cisco System
Image: State	Configuration Montoring Back Forward	and Retresh He			
Notes Notes </td <td>E Q Sensor Setup</td> <td>- Network</td> <td></td> <td></td> <td></td>	E Q Sensor Setup	- Network			
• Store Store • Store Store • Others Contracts • Others Contres <t< td=""><td>- Notwork</td><td></td><td></td><td></td><td></td></t<>	- Notwork				
B & G + GH B & G + GH B & G + GH B + GH B + GH	- Allowed Hosts	Specify the network	and communication parameters for the sensor.		
Image: State Configuration Hotshamme: Juncor Image: State Configuration Products Configuration Products Configuration Image: State Configuration Products Configuration Products Configuration Products Configuration Image: State Configuration Products Configuration Products Configuration Products Configuration Products Configuration Image: State Configuration Product Configuration Products Configuration Products Configuration Products Configuration Image: State Configuration Products Configuration	B 4,88H				
Constrained P Address: 1/216.26.10 Constrained Constrained 1/2216.26.10 Constrained Constrained Constrained Con	B Q Centricates	Hostname:	sensor		
Q marks - configuration IP Address: [17216.26.10 Notations: Particle - Strate - Configuration Period: Marks: [252.255.255.0 Q marks in Engine Output: Road: [17216.26.10 seconds P marks: [17216.26.10 seconds seconds Q marks: [17216.26.10 seconds seconds Q marks: [17216.26.10 seconds seconds P marks: [17216.26.10 seconds seconds Q marks: [17216.26.10 seconds seconds P marks: [12216.26.10 seconds seconds P marks: [12216.26.10 seconds seconds P marks: [12216.26.10 seconds seconds <td>Siltari</td> <td></td> <td></td> <td></td> <td></td>	Siltari				
- Chronics Network Mask: 255.255.255.0 - Chronics - Chronics - Chronics	D Q Interface Configuration	IP Address:	172.16.26.10		
Impriss Number for Notifications Imprise Tow Notifications Outwalk Roads Imprise Tow Notifications PTP Timeout:	- Sinterfaces	IF PROFESS.			
Image: Spring Properties Particle Trans Notice Spring Image: Spring Properties Point Assister Transmission Image: Spring Properties Properties	- Dypass		246 266 266 0		
Q. Anylas Engine Default Rode: 17219.281 P. Sipulare Configuration Configuration secondB P. Sipulare Configuration Web Server Settings secondB P. Sipulare Configuration Web Server Settings secondB P. Sipulare Configuration Web Server Settings Tends Access P. Sipulare Configuration Web Server Settings Tends Access P. Sipulare Configuration Web Server Settings Web server port P. Sipulare Configuration Web server port ¥43 P. Sipulare Configuration Sigurative Settings Tends Access P. Sipulare Configuration Web server port ¥43 P. Sipulare Configuration Sigurative Settings Tends Access P. Sigurative Settings Sigurative Settings Tends Access P. Sigurative Settings Sigurative Settings Tends Tends Configuration P. Sigurative Settings Sigurative Settings Sigurative Settings	Traffic Flow Notifications	Network Mask:	120.10110		
Outwall Second Dividual Visables Outwall Second Seconds Seconds Second Second Seconds Second Second Outwall Second Second Seconds Second Second Second Outwall Second	D Q Analysis Engine				
→ Discission Versitations PTP Timeout: 300 secondo → Objecture Configuration PVED Server Settings secondo secondo → Discission Properties PVED Server Settings PVED Server Settings secondo → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Server Settings PVED Server Settings → Discission Properties PVED Server Settings PVED Settings PVED Settings → Discission Properties PVED Settings PVED Settings PVED Setings	- Writual Sensor	Default Route:	172.16.26.1		
Image: Control of Contro	- Distantian Defection				
Subjects Control Signature Witzeld Control Control Provide Interfaces Control Control Control Provide Interfaces Control Control Control Provide Interfaces Control Control Provide Interfaces Control Control Provide Interfaces Control Disorder Interfaces Contend Disorder Interfaces <	- Signature Variables	FTP Timeout	300		seconds
Content Spaniar Washed Web Barver Stellings Web Server John Provert Attion Prives Content Stellings Provert Values Provet Values P	-Signature Configuration		-		
C Note: Name See Service Note: Service Service Note: Service Service Note: Service	- Custom Signature Wizard	Web Canada Callin	ar	Damate Arrange	
Q Peret Aston Rules P Enable TLUSSL - NDeret Visibles Web server pot: - NDeret Aston Cornides P Enable TLUSSL - NDeret Aston Cornides P Enable TLUSSL - NDeret Aston Falses P Enable TLUSSL - NDeret Aston Falses P Enable TLUSSL - NDeret Aston Falses P Enable Tussue - NDeret Aston Falses P Enable Tussue - NDeret Aston Falses P Enable Teinet - NDeret Aston Falses P Enable Teinet - NDeret Aston Falses P Enable Teinet - NDeret Confluction P Enable Teinet - NDeret Confluction P Enable Teinet - Note the Teinet Description P Enable Teinet	Miscellaneous	Theo berver bear	gs.	Tabat is not a service process service	
• Deterministication Overrides • Deterministication Contracts • Deterministication •	E Q Event Action Rules	Chable TUSISS	L	and is disabled by default.	
Number 1 Weis server port **3 Number 1 Number 1 Number 1 Number 1 <t< td=""><td>- DEvent Variables</td><td></td><td>140</td><td>C. C. M. B. M.</td><td></td></t<>	- DEvent Variables		140	C. C. M. B. M.	
Devent Action Overlaes Devent Action Contracts Devent Action Contracts <	- SuTarget Value Rating	vieo server port.	***	P Enable leinet	
Poweres Bettings Publicities Publicities <	Event Action Overnoes Event Action Eillers				
Geosting Gooding Properties Nowing Power list Nover Logar Poties Nover list Blocking Device Interfaces Noveral Configuration Noveral Configuratin Noveral Configuratin Noveral Configuration	- Oeneral Settings				
Nilocking Properties Nilocking Properties Nilocking Properties Nilocking Device Interfaces Nilocking Properties	E Q Blocking				
Obervel Loge Protes Stocking Device Interfaces Novelete Interface Novelete Novelete Interface Novelete Novelete	- Blocking Properties				
Nicosing Device Interfaces Notester Blocking Device Interfaces Nutaster Defaults Nitebotts Bensor Nutating Bensor Nutaster Blocking Nutaster Blocking Device Interfaces Nutaster Defaults Directors Bensor Nutaster Blocking Nutaster Defaults Directors Bensor Nutaster Blocking Nutaster Defaults Directors Bensor Nutaster Blocking Nutaster Bensor Reset	- Device Login Profiles				
Note interfaces Note interface Note interfa	- NBlocking Devices				
Wister Bocking Device Interfaces Q G type Notester Notester Straps Configuration Notester N	Knower Blocking Device Interfaces				
Q. DivatP P. Divate Notaceal Configuration Nation Update Director Densities Nicotor Sensor Notate Sensor Nuclear Sensor Nuclea	Master Blocking Sensor				
Noteneral Configuration Nato Update Nestore Defaults Nestore Defaults Netwood Sensor Nubulate S	D Q SNMP				
Withous Configuration Direstore Defaults Network Defaults Nothodown Sensor Duddate Sensor Reset	- Deneral Configuration				
Nado Uddel Nester Defuits Neter Defuits Noter Sensor Notersing	Traps Configuration				
Nestero Defaults Nestero Rensor Nototato Sensor Nutrining	- Auto Update				
Noteensing	- Restore Defaults				
Notation Subdate Sensor Nuccensing	- DReboot Sensor				
Apply Reset	- Si Indala Santor				
Apply Reset	- Dicensing				
Apply Reset					
Apply Reset					
Apply Reset					
Apply Reset					
Zoply Reset					
7995				Reset	
1			1994		
DM is initialized successfully.	IDM is initialized successfully				cisco [administrator]

2. Fügen Sie einen Benutzer mit mindestens Anzeigeberechtigungen





3. Aktivieren Sie die

Schnittstelle.

Cisco IDM 5.0 - 172.16.26.10									
File Help									
Configuration Montoring Back For	e e e e e e e e e e e e e e e e e e e	Retresh Help							Casco Sessions
Configuration Monitoring Configuration Monitoring Back For Monitoring Seck For Monitoring Seck For Seck Seck Seck Seck Seck	Wind I	Retresh Holp Interfaces A sensing interface m and clicking Enable or Interface Name Giglab/IEthernet//1	ust be enabled i Crisable. Enabled Yes	Ind assigned to Media Type Biockplane in	a virtual senso Duplex Auto	r before the se Speed Auto	nsor will monitor that int Atternate TCP Reset Interface Nonis-	erface. You can enabledisable the available sensing interfaces by Description	Selecting the row(s) Select All Esste Disable
p uscensing									
							Apply R	leset	
IDM is initialized successfully.								cisco	administrator

4. Überprüfen Sie die Konfiguration des virtuellen Sensors.



Konfigurieren eines WLC zum Abrufen des AIP-SSM für Client-Blöcke

Führen Sie die folgenden Schritte aus, sobald der Sensor konfiguriert und zum Hinzufügen im Controller bereit ist:

- 1. Wählen Sie Security > CIDS > Sensors > New in the WLC aus.
- 2. Fügen Sie die IP-Adresse, die TCP-Portnummer, den Benutzernamen und das Kennwort hinzu, die Sie im vorherigen Abschnitt erstellt haben.
- 3. Um den Fingerabdruck vom Sensor abzurufen, führen Sie diesen Befehl im Sensor aus, und fügen Sie den SHA1-Fingerabdruck auf dem WLC hinzu (ohne Doppelpunkt). Diese Funktion dient zum Sichern der Abfragekommunikation zwischen Controller und 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

Conce Sections	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Sen	sor Edit						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Index Server Ac	idress	2					
MAC Filtering Disabled Clients User Login Policies AP Policies	Port		443					
Access Control Lists	Usernam	0	controller					
IPSec Certificates CA Certificate ID Certificate	Password		•••••					
Web Auth Certificate	State		V					
Wireless Protection Policies Trusted AP Policies	Query Int	erval	10 sec	onds				
Roque Policies Standard Signatures Custom Signatures	Fingerpri (SHA1 ha	nt sh)	98C996984EFA74 (hash key is alre	edy set)	483C458487	40 he	< chars	
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Last Quer (count)	rv.	Success (1400)					
Web Login Page								
CIDS Sensors Shunned Clients								

4. Überprüfen Sie den Status der Verbindung zwischen dem AIP-SSM und dem

WLC.									
Cinco Stores									
A.A.	MONITOR	WLANS	CONTROLLER	R WIRELESS	SECURITY	MANAGEMENT COMM	IANDS HELP		
Security	CIDS Serve	sors List							
AAA	Index	54	erver Address	Port	State	Query Interval	Last Query (count)		
General RADIUS Authentication	1	19	2.168.5.2	443	Enabled	15	Unauthorized (1)	Detail	Remove
RADIUS Accounting	2	17	2.16.26.10	443	Enabled	10	Success (1444)	Detail	Remove
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies									
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									

Hinzufügen einer Blockierungssignatur zum AIP-SSM

Fügen Sie eine Überprüfungssignatur hinzu, um Datenverkehr zu blockieren. Obwohl es viele Signaturen gibt, die diese Aufgabe auf der Grundlage der verfügbaren Tools ausführen können, wird in diesem Beispiel eine Signatur erstellt, die Ping-Pakete blockiert.

1. Wählen Sie die **2004-Signatur (ICMP-Echo-Anforderung)**, um eine schnelle Einrichtungsüberprüfung

durchzuführen.

Cisco IDM 5.0 - 192.168.5.2												
File Help												
Configuration Montoring Dack Fo	Contract of the second	(Retresh	? Help									Cisco System
Q. Sensor Setup Sensor Setup Shlowerk Shlowed Hosts	- Sig Se	phature C Nect By:	All Signal	on ures 💌 Select Criteria: 🖡	-NRA- 💌							
B Q SSH B Q Centicates	8	Big ID S	lubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	Select All
- Suttime		1330	2	TCP Drop - Urgent Pointer WL.	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
- Dinterfaces		1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	informatio	100	Default	Normalizer	No	Clone
- Soverace 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	Eot
Q Analysis Engine		2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
Circhal Variables		2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
E 9 Signature Definition		2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Adormic IP	No	
- Signature Variables				1740 Colo Danuari		Produce Alert		100	R	Alternation (1970)		Actions
Signature Configuration Since A set Without		2004		NUMP ECTIO Request	195	Request Block	riign	100	TUNKO	Automatic art	**	Restore Defaults
Miscellaneous		2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	Decete
E Q Event Action Rules		2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Adomic IP	No	
- Devent Variables		2007	0	ICMP Timestamp Request	No	Produce Alert	informatio	100	Default	Atomic IP	No	Activate
Performance Rating Performance Rating Performance Rating		2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio	100	Default	Adomic IP	No	Retire
- Sevent Action Filters		2009	0	ICMP Information Reguest	No	Produce Alert	Informatio	100	Default	Atomic IP	No	

2. Aktivieren Sie die Signatur, legen Sie den Alert Severity (Schweregrad der Warnung) auf High (Hoch) fest, und legen Sie die Event Action (Ereignisaktion) auf Produce Alert and Request Block Host fest, um diesen Verifizierungsschritt abzuschließen. Beachten Sie, dass die Aktion "Request Block Host" der Schlüssel für die Signalisierung des WLC zum Erstellen von Clientausnahmen ist.

A roit 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	

🤏 Edit Signature					×			
Name	Value				<u>.</u>			
Signature ID	2004							
SubSignatu	re ID: 0							
Alert Severit	Y: Informational 💌							
Sig Fidelity F	Rating: 100							
Promiscuou	us Delta: 0							
Sig Descript	tion:							
	Signature Nam	e: ICMP Echo Request						
	Alert Notes:		-					
	User Commer	ts:	_					
	Alert Traits:	0	-					
	Release:	81	_					
Engine:	Atomic IP							
	Event Action	Request Request Reset To	Block Connection					
•	Eranment S	tatue:	=		-			
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 Can	cel Help					

- 3. Klicken Sie auf **OK**, um die Signatur zu speichern.
- 4. Überprüfen Sie, ob die Signatur aktiv ist und für eine Blockierungsaktion festgelegt ist.
- 5. Klicken Sie auf Apply, um die Signatur auf das Modul zu übertragen.

Überwachung von Blockierung und Ereignissen mit IDM

Führen Sie diese Schritte aus:

 Wenn die Signatur erfolgreich feuert, gibt es innerhalb von IDM zwei Stellen, um dies zu beachten.Die erste Methode zeigt die aktiven Blöcke, die vom AIP-SSM installiert wurden. Klicken Sie in der oberen Aktionszeile auf Monitoring. Wählen Sie in der Liste der Elemente, die links angezeigt wird, Active Host Blocks aus. Wenn die Ping-Signatur auslöst, zeigt das Fenster Active Host Blocks (Aktive Host-Blöcke) die IP-Adresse des Angreifers, die Adresse des Geräts, gegen das ein Angriff stattfindet, und die Zeit, für die der Block noch gültig ist. Die Standardblockierungszeit beträgt 30 Minuten und kann eingestellt werden. Die Änderung dieses Werts wird in diesem Dokument jedoch nicht behandelt. Weitere Informationen zum Ändern dieses Parameters finden Sie in der ASA-Konfigurationsdokumentation (falls erforderlich). Entfernen Sie den Block sofort, wählen Sie ihn aus der Liste aus, und klicken Sie dann auf Löschen.



Die zweite Methode zum Anzeigen ausgelöster Signaturen verwendet den AIP-SSM-Ereignispuffer. Wählen Sie auf der Seite IDM Monitoring (IDM-Überwachung) **Events** (**Ereignisse**) in der Liste Items (Elemente) auf der linken Seite aus. Das Dienstprogramm für die Veranstaltungssuche wird angezeigt. Legen Sie die gewünschten Suchkriterien fest, und klicken Sie auf

Anzeigen....

Cisco IDM 5.0 - 172.16.26.10	
e Help	
anfiguration Manifering Back Forward Refresh	Personal Antonio Anton
Denied Atlackers Active Host Blocks Network Blocks DP Logging C Support Information Statistics System Information	Events You can display the events in the local Event Store. By default all events are displayed. To filter on event type and/or time, select the appropriate check boass. Show aller events: Imformational Cow Medium P High Show error events: Wilarning Error Fatal Show Network Access Combolier events Select the number of the rows per page. Show status events: 100 Image: Show status events Show status events: 1 nours Image: Show status events Show weats from the following time range Start Time (UTC) Image: Ima

2. Die Ereignisanzeige wird dann mit einer Liste von Ereignissen angezeigt, die den angegebenen Kriterien entsprechen. Blättern Sie durch die Liste, und suchen Sie nach der Signatur für die ICMP-Echo-Anforderung, die in den vorherigen Konfigurationsschritten geändert wurde.Suchen Sie in der Spalte Events (Ereignisse) nach dem Namen der Signatur, oder suchen Sie in der Spalte Sig ID (Signatur-ID) nach der Identifikationsnummer der

rror July 3 rarning July 3 formati July 3 rror July 3	11, 2006 2:59:52 PM U 11, 2006 3:16:51 PM U 11, 2006 3:19:16 PM U	J 1145383740954940828 J 1145383740954941447	Unable to execute a host block [10.10.99.26] because blocking is not configured while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
formati July 3 formati July 3 rror July 3	1, 2006 3:16:51 PM U	J 1145383740954941447	while sending a TLS warning alert close_notify, the following error occurred: socket error [3,32]		
formati July 3 rror July 3	1, 2006 3:19:16 PM U				
rror July 3		J 1145383740954941574	ICMP Echo Request	2004	
	1, 2006 3:19:16 PM U	J 1145383740954941577	Unable to execute a host block [10.10.99.26] because blocking is not configured		
formati July 3	1, 2006 3:19:46 PM L	J 1145383740954941597	ICMP Echo Request	2004	
					Ped
	cormaa. _j ouly s	ormaa juury 31, 2006 3,13(46 PM (rormas juliy 31, 2000 3.19.46 PM 0 1145383740954941597	Cormas July 31, 2006 3.19.46 PM 0	COTTRABI JUly 31, 2006 3.19.46 PM O 1145383740934941597 Pomr Ecro Request 2004

3. Nachdem Sie die Signatur gefunden haben, doppelklicken Sie auf den Eintrag, um ein neues Fenster zu öffnen. Das neue Fenster enthält detaillierte Informationen zum Ereignis, das die Signatur ausgelöst hat.

```
Details for 1145383740954941597
evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
  originator:
   hostId: sensor
    appName: sensorApp
    appInstanceId: 341
  time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
  signature: description=ICMP Echo Request id=2004 version=S1
   subsigId: 0
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
     addr: 10.10.99.26 locality=OUT
   target:
     addr: 10.10.102.1 locality=0UT
  summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
  alertDetails: Regular Summary: 4 events this interval ;
  riskRatingValue: 25
  interface: ge0 1
  protocol: icmp
```

Überwachung des Client-Ausschlusses in einem Wireless-Controller

Die Liste "Shunned Clients" im Controller wird zu diesem Zeitpunkt mit der IP- und MAC-Adresse des Hosts ausgefüllt.

	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADUS Authoritication	Re-sync							
RADIUS Accounting	IP Addres	5 L	ast MAC Address	Expire	Sen	sor IP / Index		
Local Net Users MAC Piltering Disabled Clients User Login Policies AP Policies	10.10.99.24	6 0	0:40:96:ad:0d:1b	27	172.	16.26.10 / 2		
Access Control Lists								
IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate								
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MPP Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

Der Benutzer wird der Clientausschlussliste hinzugefügt.



Überwachung von Ereignissen in WCS

Sicherheitsereignisse, die einen Block im AIP-SSM auslösen, veranlassen den Controller, die Adresse des Straftäters der Ausschlussliste des Clients hinzuzufügen. Ein Ereignis wird auch in WCS generiert.

- Verwenden Sie das Dienstprogramm Monitor > Alarms im WCS-Hauptmenü, um das Ausschlussereignis anzuzeigen. WCS zeigt zunächst alle nicht gelesenen Alarme an und zeigt auch eine Suchfunktion auf der linken Seite des Fensters an.
- Ändern Sie die Suchkriterien, um den Clientblock zu suchen. Wählen Sie unter Severity (Schweregrad) die Option Minor (Gering) aus, und legen Sie die Alarmkategorie auch auf Security (Sicherheit) fest.
- 3. Klicken Sie auf

Suchen.

Monitor · Configure · L	coation - Administration - Help -			
larms	Alarms			Select a command 💌 🕻
leverity Cróteal v Jarm Category All Types v Search	Severity Eailure_Object Critical Radio_ABS_LAF1242AG_A/2 Critical Radio_ABS_LAF1242AG_A/2 Critical Radio_ABS_LAF1242AG_A/2 Critical Radio_ABS_LAF1242AG_A/2 Critical Radio_ABS_LAF1242AG_A/2 Critical Radio_ABS_LAF1242AG_A/2001015155141160 Critical Radio_ABS_L5121460/2 Critical Radio_ABS_L5121460/2 Critical Radio_ABS_L5121460/20101515151460 Critical AF_AP0031_0433_04700011315157143140 Critical AF_AP032_0433_04700011315157143140 Critical AF_AP142-R00141105_5315140 Critical Radio_AF_acc-0750-48-1-FE1-0-3/2 Critical Radio_AF_acc-0750-48-1-FE1-0-3/2 Critical Radio_AF_acc-0750-48-1-FE1-0-3/1	Owner	Date/Time 6/2/06 9:02 AM 6/2/06 9:02 AM 7/2L/06 1:51 PM 7/2L/06 1:51 PM 7/2L/06 1:51 PM 7/2L/06 4:32 PM 7/2L/06 4:32 PM 7/2L/06 5:31 PM 7/2L/06 5:32 PM 7/2L/06 5:22 PM 7/26/06 2:02 PM 7/26/06 2:02 PM	Nessance AP 'AIR-LAP1242AG-A', interface '802.11b/g' is AP 'AIR-LAP1242AG-A', interface '802.11b/g' is AP 'AIR-LAP1242AG-A', interface '802.11a' is down AP 'AIR-LAP1242AG-A' disessociated from Controller AP 'aIR-151121e0' disessociated from Controller Controller '40.13.15', RADIUS server(s) are no Fake AP or other attack may be in progress. Rog Fake AP or other attack may be in progress. Rog Fake AP or other attack may be in progress. Rog Fake AP or other attack may be in progress. Rog AP 'AP-aco-c3750-40-1-FE1-0-3', interface '802 AP 'AP-aco-c3750-40-1-FE1-0-3' disassociated fr
gues 0 282 rerage 0 0 certy 0 0 atrollers 1 0 0				

4. Im Fenster Alarm werden dann nur Sicherheitswarnungen mit geringem Schweregrad angezeigt. Zeigen Sie mit der Maus auf das Ereignis, das den Block innerhalb des AIP-SSM

ausgelöst hat. Insbesondere zeigt WCS die MAC-Adresse der Client-Station an, die den Alarm ausgelöst hat. Durch den Verweis auf die entsprechende Adresse öffnet WCS ein kleines Fenster mit Ereignisdetails. Klicken Sie auf den Link, um die gleichen Details in einem anderen Fenster

anzuzeigen.

Cisco Wireless Con	Cisco Wireless Control System Username: root Logout Refresh Print V									
Monitor • Configure • Location • Administration • Help •										
Alarms		Alar	ms					Select a command		
Severity Minor	v		Severity	Failure Object	Owner	Date/Time	Message			
Alarm Catagory			Minor	Client 00:09:ef:01:40:46		7/19/06 6:30 PM	The WEP Key configured at the station may be wr			
Security	v		Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr			
			Minor	Client 00:90:7a:04:6d:04		7/31/06 2:36 PM	Client '00:90:7a:04:6d:04' which was associated			
Search			Minor	Client 00:40:95:ad:0d:15		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated			
				Client 100.40.96 ad 00 100.14.1b:Sa:16.40', ir code is S(Uninnown)	11b" which was as: iterface '안 is exclu '.	sociated with AP ded. The reason				

Cisco ASA - Beispielkonfiguration

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
1
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
1
interface Ethernet0/1
nameif inside
security-level 100
ip address 172.16.26.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif management
 security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
pager lines 24
logging asdm informational
mtu inside 1500
mtu management 1500
```

mtu outside 1500 asdm image disk0:/asdm512-k8.bin no asdm history enable arp timeout 14400 nat-control global (outside) 102 interface nat (inside) 102 172.16.26.0 255.255.255.0 nat (inside) 102 0.0.0.0 0.0.0.0 route inside 0.0.0.0 0.0.0.0 172.16.26.1 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute http server enable http 10.1.1.12 255.255.255.255 inside http 0.0.0.0 0.0.0.0 inside http 192.168.1.0 255.255.255.0 management no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart telnet 0.0.0.0 0.0.0.0 inside telnet timeout 5 ssh timeout 5 console timeout 0 dhcpd address 192.168.1.2-192.168.1.254 management dhcpd lease 3600 dhcpd ping_timeout 50 dhcpd enable management class-map inside-class match any ! 1 policy-map inside-policy description IDS-inside-policy class inside-class ips promiscuous fail-open 1 service-policy inside-policy interface inside Cryptochecksum: 699d110f988e006f6c5c907473939b29 : end ciscoasa#

Cisco Intrusion Prevention System - Beispielkonfiguration

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
exi+
! ------
service analysis-engine
virtual-sensor vs0
description default virtual sensor
physical-interface GigabitEthernet0/1
exit
exit
! _____
service interface
exit.
| _____
service trusted-certificates
exit
sensor#
```

<u>Überprüfung</u>

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Installation und Verwendung von Cisco Intrusion Prevention System Device Manager 5.1
- <u>Cisco Adaptive Security Appliances der Serie ASA 5500 Konfigurationsleitfäden</u>
- Konfigurieren des Cisco Intrusion Prevention System-Sensors mithilfe der Befehlszeilenschnittstelle 5.0 - Konfigurieren von Schnittstellen

- WLC-Konfigurationsleitfaden 4.0
- Technischer Support für Wireless
- Häufig gestellte Fragen zum Wireless LAN Controller (WLC)
- <u>Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access</u>
 <u>Point</u>
- Konfigurieren von Sicherheitslösungen
- Technischer Support und Dokumentation für Cisco Systeme