Guida all'integrazione di Controller LAN wireless e IPS

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Panoramica di Cisco IDS Cisco IDS e WLC - panoramica sull'integrazione Shun IDS Progettazione dell'architettura di rete Configurazione del sensore Cisco IDS Configurare il WLC Esempio di configurazione del sensore Cisco IDS Configurazione di un'ASA per IDS Configurazione di AIP-SSM per l'ispezione del traffico Configurare un WLC per eseguire il polling di AIP-SSM per i blocchi client Aggiungere una firma di blocco a AIP-SSM Monitoraggio del blocco e degli eventi con IDM Monitorare l'esclusione dei client in un controller wireless Monitoraggio eventi in WCS Esempio di configurazione di Cisco ASA Esempio di configurazione del sensore Cisco Intrusion Prevention System Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

Il Cisco Unified Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) fa parte di Cisco Self-Defending Network ed è la prima soluzione di sicurezza wireless e cablata integrata del settore. Cisco Unified IDS/IPS adotta un approccio completo alla sicurezza: ai limiti wireless, cablati, WAN e attraverso il centro dati. Quando un client associato invia traffico dannoso attraverso la Cisco Unified Wireless Network, un dispositivo IDS cablato Cisco rileva l'attacco e invia richieste shun ai Cisco Wireless LAN Controller (WLC), che quindi dissociano il dispositivo client.

Cisco IPS è una soluzione inline basata su rete progettata per identificare, classificare e arrestare in modo accurato il traffico dannoso, inclusi worm, spyware/adware, virus di rete e abusi delle

applicazioni, prima che influiscano sulla business continuity.

Utilizzando il software sensore Cisco IPS versione 5, la soluzione Cisco IPS combina servizi di prevenzione in linea con tecnologie innovative per migliorare l'accuratezza. Il risultato è una totale fiducia nella protezione fornita della soluzione IPS, senza il timore di perdere il traffico legittimo. La soluzione Cisco IPS offre anche una protezione completa della rete grazie alla possibilità unica di collaborare con altre risorse di sicurezza della rete e fornisce un approccio proattivo alla protezione della rete.

La soluzione Cisco IPS consente agli utenti di bloccare un numero maggiore di minacce con maggiore sicurezza grazie all'utilizzo di queste funzionalità:

- Tecnologie di prevenzione in linea accurate: offrono la massima sicurezza per intraprendere azioni preventive contro una più ampia gamma di minacce senza il rischio di far cadere il traffico legittimo. Queste tecnologie uniche offrono un'analisi contestuale intelligente, automatizzata dei dati e consentono di ottenere il massimo dalla soluzione di prevenzione delle intrusioni.
- Identificazione delle minacce multi-vettoriali: protegge la rete da violazioni delle policy, sfruttamento delle vulnerabilità e attività anomale attraverso un'ispezione dettagliata del traffico nei livelli da 2 a 7.
- Collaborazione unica in rete: migliora la scalabilità e la resilienza attraverso la collaborazione in rete, incluse tecniche efficienti di acquisizione del traffico, funzionalità di bilanciamento del carico e visibilità nel traffico crittografato.
- Soluzioni di installazione complete: fornisce soluzioni per tutti gli ambienti, dalle piccole e medie imprese (PMI) alle filiali, dalle grandi aziende alle installazioni di provider di servizi.
- Potenti servizi di gestione, correlazione degli eventi e supporto: offrono una soluzione completa che include configurazione, gestione, correlazione dei dati e servizi di supporto avanzati. In particolare, il sistema MARS (Security Monitoring, Analysis, and Response System) di Cisco identifica, isola e consiglia la rimozione precisa degli elementi dannosi per una soluzione di prevenzione delle intrusioni a livello di rete. Inoltre, il Cisco Incident Control System previene la diffusione di nuovi worm e virus consentendo alla rete di adattarsi rapidamente e fornire una risposta distribuita.

Se combinati, questi elementi offrono una soluzione di prevenzione in linea completa e consentono di rilevare e arrestare la più ampia gamma di traffico dannoso prima che influisca sulla business continuity. L'iniziativa Cisco Self-Defending Network richiede una sicurezza integrata e integrata per le soluzioni di rete. Gli attuali sistemi WLAN basati su LWAPP (Lightweight Access Point Protocol) supportano solo le funzionalità IDS di base, in quanto si tratta essenzialmente di un sistema di layer 2 e ha una potenza di elaborazione di linea limitata. Cisco rilascia tempestivamente il nuovo codice per includere nuove funzionalità avanzate nei nuovi codici. La versione 4.0 offre le funzionalità più recenti che includono l'integrazione di un sistema WLAN basato su LWAPP con la linea di prodotti Cisco IDS/IPS. In questa versione, l'obiettivo è quello di consentire al sistema Cisco IDS/IPS di istruire i WLC di bloccare alcuni client dall'accesso alle reti wireless quando viene rilevato un attacco dal layer 3 al layer 7 che interessa il client in questione.

Prerequisiti

Requisiti

Assicurarsi di soddisfare i seguenti requisiti minimi:

- Firmware WLC versione 4.x e successive
- Èconsigliabile avere a disposizione informazioni su come configurare Cisco IPS e Cisco WLC.

Componenti usati

Cisco WLC

Questi controller sono inclusi nella versione software 4.0 per le modifiche IDS:

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

Access point

- Cisco Aironet serie 1100 AG Lightweight Access Point
- Cisco Aironet serie 1200 AG Lightweight Access Point
- Cisco Aironet serie 1300 Lightweight Access Point
- Cisco Aironet serie 1000 Lightweight Access Point

Gestione

- Cisco Wireless Control System (WCS)
- Cisco serie 4200 Sensor
- Gestione Cisco IDS Cisco IDS Device Manager (IDM)

Piattaforme Cisco Unified IDS/IPS

- Cisco IPS serie 4200 Sensori con software sensore Cisco IPS 5.x o versioni successive.
- SSM10 e SSM20 per Cisco ASA serie 5500 Adaptive Security Appliance con software sensore Cisco IPS 5.x
- Cisco ASA serie 5500 Adaptive Security Appliance con software sensore Cisco IPS 5.x
- Cisco IDS Network Module (NM-CIDS) con software sensore Cisco IPS 5.x
- Cisco Catalyst serie 6500 Intrusion Detection System Module 2 (IDSM-2) con software sensore Cisco IPS 5.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

Panoramica di Cisco IDS

I componenti principali di Cisco IDS (versione 5.0) sono:

- Applicazione sensore: consente di acquisire e analizzare i pacchetti.
- Modulo Event Storage Management and Actions: fornisce lo storage delle violazioni delle regole.
- Imaging, Install and Startup Module: carica, inizializza e avvia tutto il software di sistema.
- User Interfaces and UI Support Module: fornisce una CLI incorporata e IDM.
- Sistema operativo sensore: sistema operativo host (basato su Linux).



L'applicazione sensore (software IPS) è costituita da:

- Applicazione principale: inizializza il sistema, avvia e arresta altre applicazioni, configura il sistema operativo ed è responsabile degli aggiornamenti. Contiene i seguenti componenti:Control Transaction Server: consente ai sensori di inviare transazioni di controllo utilizzate per abilitare la funzionalità Master Blocking Sensor di Attack Response Controller (precedentemente nota come Controller di accesso alla rete).Event Store: archivio indicizzato utilizzato per memorizzare gli eventi IPS (errori, messaggi di stato e di sistema di allarme) accessibile tramite CLI, IDM, Adaptive Security Device Manager (ASDM) o Remote Data Exchange Protocol (RDEP).
- Applicazione interfaccia (Interface App) Gestisce le impostazioni di bypass e fisiche e definisce le interfacce accoppiate. Le impostazioni fisiche sono costituite dallo stato di velocità, duplex e amministrativo.
- Log App: scrive i messaggi di log dell'applicazione nel file di log e i messaggi di errore nell'archivio eventi.
- Attack Response Controller (ARC) (noto in precedenza come Network Access Controller): gestisce dispositivi di rete remoti (firewall, router e switch) per fornire funzionalità di blocco quando si verifica un evento di avviso. ARC crea e applica elenchi di controllo di accesso (ACL) sul dispositivo di rete controllato o utilizza il comando shun (firewall).
- Notification App: invia trap SNMP quando vengono attivate da un evento di avviso, stato ed errore. A tale scopo, l'app di notifica utilizza un agente SNMP di dominio pubblico. I comandi GET di SNMP forniscono informazioni sullo stato di un sensore.Server Web (server HTTP)

RDEP2): fornisce un'interfaccia utente Web. Consente inoltre di comunicare con altri dispositivi IPS tramite RDEP2 utilizzando diversi servlet per fornire servizi IPS.**Authentication App**: verifica che gli utenti siano autorizzati a eseguire azioni CLI, IDM, ASDM o RDEP.

- Applicazione sensore (motore di analisi): acquisisce e analizza i pacchetti.
- CLI: l'interfaccia eseguita quando gli utenti riescono ad accedere al sensore tramite Telnet o SSH. Tutti gli account creati tramite la CLI utilizzano la CLI come shell (ad eccezione dell'account del servizio - è consentito un solo account del servizio). I comandi CLI consentiti dipendono dai privilegi dell'utente.

Tutte le applicazioni IPS comunicano tra loro tramite una API (Application Program Interface) comune denominata IDAPI. Le applicazioni remote (altri sensori, applicazioni di gestione e software di terze parti) comunicano con i sensori tramite i protocolli RDEP2 e Security Device Event Exchange (SDEE).

Si noti che il sensore dispone delle seguenti partizioni del disco:

- Partizione applicazioni: contiene l'immagine completa del sistema IPS.
- **Partizione di manutenzione**: un'immagine IPS per scopi speciali utilizzata per ricreare l'immagine della partizione applicativa di IDSM-2. Una nuova immagine della partizione di manutenzione comporta la perdita delle impostazioni di configurazione.
- Partizione di ripristino: immagine speciale utilizzata per il ripristino del sensore. L'avvio nella partizione di ripristino consente agli utenti di ricreare completamente l'immagine della partizione applicativa. Le impostazioni di rete vengono mantenute, ma tutte le altre configurazioni vengono perse.

Cisco IDS e WLC - panoramica sull'integrazione

La versione 5.0 di Cisco IDS introduce la capacità di configurare le azioni di negazione quando vengono rilevate violazioni dei criteri (firme). In base alla configurazione utente sul sistema IDS/IPS, è possibile inviare una richiesta shun a un firewall, un router o un WLC per bloccare i pacchetti da un particolare indirizzo IP.

Con il software Cisco Unified Wireless Network versione 4.0 per i controller wireless Cisco, è necessario inviare una richiesta shun a un WLC per attivare il comportamento di esclusione o blacklist del client disponibile su un controller. L'interfaccia usata dal controller per ottenere la richiesta shun è l'interfaccia di comando e controllo su Cisco IDS.

- Il controller consente di configurare fino a cinque sensori IDS su un determinato controller.
- Ogni sensore IDS configurato viene identificato dal relativo indirizzo IP o nome di rete qualificato e dalle credenziali di autorizzazione.
- Ogni sensore IDS può essere configurato su un controller con una frequenza di query univoca in secondi.



Shun IDS

Il controller esegue una query sul sensore alla frequenza di query configurata per recuperare tutti gli eventi shun. Una determinata richiesta shun viene distribuita in tutto il gruppo di mobilità del controller che recupera la richiesta dal sensore IDS. Ogni richiesta di shun per un indirizzo IP client è attiva per il valore di timeout dei secondi specificato. Se il valore di timeout indica un tempo infinito, l'evento shun termina solo se la voce shun viene rimossa dall'IDS. Lo stato del client ignorato viene mantenuto su ogni controller nel gruppo di mobilità anche se uno o tutti i controller vengono reimpostati.

Nota: la decisione di evitare un client viene sempre presa dal sensore IDS. Il controller non rileva attacchi di livello 3. È un processo molto più complesso determinare che il client sta lanciando un attacco dannoso al layer 3. Il client viene autenticato al layer 2, che è sufficiente al controller per concedere l'accesso al layer 2.

Nota: ad esempio, se a un client viene assegnato un indirizzo IP che causa un errore precedente (non utilizzato), è possibile sbloccare l'accesso di layer 2 per questo nuovo client solo dopo il timeout del sensore. Anche se il controller consente l'accesso al layer 2, il traffico del client potrebbe comunque essere bloccato sui router del layer 3, perché il sensore informa anche i router dell'evento shun.

Si supponga che un client abbia l'indirizzo IP A. Ora, quando il controller esegue il polling dell'IDS per individuare gli eventi shun, l'IDS invia la richiesta shun al controller con l'indirizzo IP A come indirizzo IP di destinazione. Ora, il controller nero elenca questo client A. Sul controller, i client sono disabilitati in base a un indirizzo MAC.

Si supponga ora che il client cambi il proprio indirizzo IP da A a B. Durante il polling successivo, il controller ottiene un elenco di client esclusi in base all'indirizzo IP. Anche in questo caso, l'indirizzo IP A è ancora nell'elenco degli indirizzi non utilizzati. Tuttavia, poiché il client ha modificato il proprio indirizzo IP da A a B (che non è incluso nell'elenco degli indirizzi IP esclusi), questo client con un nuovo indirizzo IP di B viene rilasciato una volta raggiunto il timeout dei client in lista nera sul controller. A questo punto, il controller inizia a consentire al client di utilizzare il

nuovo indirizzo IP di B (ma l'indirizzo MAC del client rimane lo stesso).

Pertanto, anche se un client rimane disabilitato per la durata del tempo di esclusione del controller e viene riescluso se acquisisce nuovamente l'indirizzo DHCP precedente, tale client non viene più disabilitato se l'indirizzo IP del client ignorato viene modificato. Ad esempio, se il client si connette alla stessa rete e il timeout del lease DHCP non è scaduto.

I controller supportano solo la connessione all'IDS per le richieste di shun client che utilizzano la porta di gestione del controller. Il controller si connette all'IDS per l'ispezione dei pacchetti tramite le interfacce VLAN applicabili che trasportano il traffico client wireless.

Sul controller, la pagina Disabilita client mostra ciascun client che è stato disabilitato tramite una richiesta del sensore IDS. Il comando **show** della CLI visualizza anche una lista nera dei client.

In Sistema colori Windows i client esclusi vengono visualizzati nella scheda secondaria Protezione.

Di seguito viene riportata la procedura per completare l'integrazione dei sensori Cisco IPS e dei WLC di Cisco.

- 1. Installare e collegare l'accessorio IDS sullo stesso switch su cui risiede il controller wireless.
- 2. Eseguire il mirroring (SPAN) delle porte WLC che trasportano il traffico client wireless all'accessorio IDS.
- 3. L'appliance IDS riceve una copia di ogni pacchetto e controlla il traffico dal layer 3 al layer 7.
- 4. L'accessorio IDS offre un file di firma scaricabile che può anche essere personalizzato.
- 5. L'accessorio IDS genera un allarme con un'azione evento shun quando viene rilevata una firma di attacco.
- 6. Il WLC analizza l'IDS per rilevare eventuali allarmi.
- 7. Quando viene rilevato un allarme con l'indirizzo IP di un client wireless associato al WLC, il client viene inserito nell'elenco di esclusione.
- 8. Il WLC genera una trap e il WCS ne riceve notifica.
- 9. L'utente viene rimosso dall'elenco di esclusione dopo il periodo di tempo specificato.

Progettazione dell'architettura di rete



Il Cisco WLC è collegato alle interfacce gigabit del Catalyst 6500. Creare un canale di porta per le interfacce Gigabit e abilitare il protocollo LAG (Link Aggregation) sul 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

Il controller è collegato all'interfaccia gigabit 5/1 e gigabit 5/2 sullo switch Catalyst 6500.

```
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
1
interface GigabitEthernet5/2
switchport
```

```
switchport trunk encapsulation dot1q
switchport trunk native vlan 99
switchport mode trunk
no ip address
channel-group 99 mode on
end
cat6506#show run interface port-channel 99
Building configuration...
Current configuration : 153 bytes
1
interface Port-channel99
switchport
switchport trunk encapsulation dotlq
switchport trunk native vlan 99
switchport mode trunk
no ip address
end
```

Le interfacce di rilevamento del sensore IPS possono funzionare singolarmente in **modalità promiscua** oppure è possibile accoppiarle per creare interfacce in linea per la **modalità di rilevamento in linea**.

In modalità promiscua, i pacchetti non passano attraverso il sensore. Il sensore analizza una copia del traffico monitorato anziché il pacchetto inoltrato. Il vantaggio di operare in modalità promiscua è che il sensore non influisce sul flusso del pacchetto con il traffico inoltrato.

Nota: il <u>diagramma dell'architettura</u> è solo un esempio di configurazione dell'architettura integrata WLC e IPS. L'esempio di configurazione qui mostrato spiega l'interfaccia di rilevamento IDS che agisce in modalità promiscua. Il <u>diagramma dell'architettura</u> mostra le interfacce di rilevamento accoppiate per funzionare in modalità Inline Pair. Per ulteriori informazioni sulla modalità interfaccia in linea, fare riferimento a <u>Modalità in linea</u>.

In questa configurazione, si presume che l'interfaccia di rilevamento agisca in modalità promiscua. L'interfaccia di monitoraggio del sensore Cisco IDS è collegata all'interfaccia 5/3 Gigabit del Catalyst 6500. Creare una sessione di monitoraggio sullo switch Catalyst 6500 quando l'interfaccia del canale della porta è l'origine dei pacchetti e la destinazione è l'interfaccia Gigabit a cui è connessa l'interfaccia di monitoraggio del sensore Cisco IPS. In questo modo tutto il traffico in entrata e in uscita dalle interfacce cablate del controller viene replicato negli IDS per l'ispezione di layer 3-7.

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#

Configurazione del sensore Cisco IDS

La configurazione iniziale del sensore Cisco IDS viene effettuata dalla porta della console o

collegando un monitor e una tastiera al sensore.

- 1. Accedere all'accessorio:Collegare una porta console al sensore.Collegare un monitor e una tastiera al sensore.
- Digitare il nome utente e la password al prompt di accesso.Nota: il nome utente e la password predefiniti sono entrambi cisco. Al primo accesso all'accessorio verrà richiesto di modificarli. È necessario prima immettere la password UNIX, ovvero cisco. Immettere quindi la nuova password due volte.

```
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. Configurare l'indirizzo IP, la subnet mask e l'elenco degli accessi sul sensore.Nota: questa è l'interfaccia di comando e controllo sull'IDS utilizzata per comunicare con il controller. Questo indirizzo deve poter essere indirizzato all'interfaccia di gestione del controller. Le interfacce di rilevamento non richiedono indirizzamento. L'elenco degli accessi deve includere l'indirizzo dell'interfaccia di gestione del controller e gli indirizzi consentiti per la gestione dell'IDS. sensor#configure terminal

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

4. Èquindi possibile configurare il sensore IPS dalla GUI. Puntare il browser all'indirizzo IP di gestione del sensore. L'immagine mostra un esempio di sensore configurato con 192.168.5.2.

Cisco IDM 5.0 - 192.168.5.2				C 🖉 🛛
File Help				
				Cisco Sestems
Configuration Monitoring Back Forward	d Retrests Hei			de de
Configuration Motion Dock Provide Technology Configuration Excellence Excellence Configuration	Remesh Performance Remesh Performanc	and communication parameters for the sensor.	Flemste Access Tateits not a secure access service and is disabled by defaut. P Enable Teinet Reset	seconds
IDM is initialized successfully.				cisco administrator

5. Aggiungere un utente usato dal WLC per accedere agli eventi del sensore

IPS.				
4 Clines DM 5.0 - 192.168.5.2				- 6 8
File Help				
Configuration Monitoring Back Forward Retrest	? 1 Help			Cisco Sestius
G Sensor Setup Users Shotwork Sectify the Sectify the Sectify the Sectify the	i users that have access to the sensor. The	service role is a special role that allows you to bypass th	e CLJ if needed. Only one service account is allowed.	
-STime	Usemame	Role	Status	
Susers cisco		Administrator	Active	
G. Interface Configuration Sinterfaces				Edit
-Ninterface Pairs -Nexpass				Delete
Traffic Flow Notifications				
E Q Analysis Engine	S Add User	x		
- Nitual Sensor			1	
- Dolobal Variables	Usemame:	controller		
Sincuture Unintion				
- Signature Configuration	11000 8010	La constante de		
- Custom Signature Wizard	User Role:	Alemen		
- Miscellaneous				
D Q Event Action Rules				
- Devent Variables	- Password			
- Target Value Rating				
- Nevert Action Overrides	Passwort			
Devent Action Fibers	T and the			
C C Direction				
-Stillocking Properties	Confirm Passwo	48 T		
- Device Login Profiles				
- 18 Blocking Devices	i			
- SRouter Blocking Device Interfaces				
- Cat 6K Blocking Device Interfaces	OF	Cancel Help		
- Master Blocking Sensor				
in C comp			-	

6. Abilitare le interfacce di monitoraggio.

Cisco IDM 5.0 - 192.168.5.2							
File Help							
Configuration Monitoring Eack Forward	d Refresh Help						Cisco Systems
G. Sensor Selup Sensor Selup Selup Allowed Hosts G. SisH G. Certificates	A sensing interface mus and clicking Enable or D	It be enabled and assigned to visable.	a virtual senso	r before the se	nsor will monitor that int	erface. You can enable/disable the available sensing interfaces by selectin	ig the row(s)
-DTime Dusers	Interface Name	Enabled Media Type	Duplex	Speed	Atternate TCP Reset Interface	Description	Select All
E Q Interface Configuration	OigabitEthemet0/0	Yes TX (copper)	Auto	Auto	None		Edit
- Dinterface Pairs	GigabitEthemet0/1	No TX (copper)	Auto	Auto	-None-		Eastin
- Depars	OlgabitEthemet0/2	No TX (copper)	Auto	Auto	None		Chatte
Traffic Flow Notifications	OigabitEthemet0/3	No TX (copper)	Auto	Auto	None		Disable

Le interfacce di monitoraggio devono essere aggiunte al motore di analisi, come mostrato in questa

finestra:

finestra:				
Cisco IDM 5.0 - 192,168.5.2				
File Help				
Configuration Montoring Eack Forward	nd Refresh	nep		Core Services
E Q Sensor Setup - Nivebook - National Q SSH Q Centificates - Nitime	- Virtual 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 wal sensor or change the virtual sensor name.	description or
Users	Name	Assigned Interfaces (or Interface Pairs)	Description	Edit
G. Interface Configuration Dinterfaces Noterfaces Noterface Pairs Noterface Pairs Noterface Pairs Noterface Pairs Noterface	vs0	OlgabitElthernet0/0 OlgabitElthernet0/1 OlgabitElthernet0/2 OlgabitElthernet0/3	default virtual sensor	
Ca Analysis Engine				

7. Per eseguire una rapida verifica della configurazione, selezionare la firma 2004 (ICMP Echo Request).

Cisco IDM 5.0 - 192,168.5.2											
File Help											
Configuration Montoring Dack Fi	orward Retrest	? h Help									Cisco Sesters
Q. Sensor Setup - Network - Netwo	Signature Select Dy	Configuration	on tures 💌 Select Criteria: 🖡	-104							
B Q SSH B Q Certificates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	Select All
- SUIsers	1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	informatio	100	Default	Normalizer	No	NSDB Link
D Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Ninterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Clone
- Striberace Pairs	1330	3	TCP Drop - Bad Option List	Yes	Deny Packet In	informatio	100	Default	Normalizer	No	
Traffic Flow Notifications	2000	0	ICMP Echo Reply	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Edt
G Q Analysis Engine	2001	0	ICMP Host Unreachable	Yes	Produce Alert	High	100	Tuned	Adomic IP	No	Enable
Cichal Sensor	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
() 9 Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
- Signature Variables	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	180	Tuned	Atomic IP	No	Actions Data da
Custom Signature Wzard Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	Pressore L'enauts
D Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Dente.
- Sevent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Activate
Super Value Rating Super Lating	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	

Affinché la fase di verifica venga completata, è necessario abilitare la firma, impostare la gravità dell'avviso su **Alta** e impostare l'azione evento su **Produzione host avvisi** e **host richieste di blocco**.



Configurare il WLC

Per configurare il WLC, completare i seguenti passaggi:

- 1. Una volta configurato l'accessorio IPS e pronto per essere aggiunto al controller, scegliere Sicurezza > CIDS > Sensori > Nuovo.
- Aggiungere l'indirizzo IP, il numero di porta TCP, il nome utente e la password creati in precedenza.Per ottenere l'impronta digitale dal sensore IPS, eseguire questo comando nel sensore IPS e aggiungere l'impronta digitale SHA1 sul WLC (senza i due punti). Utilizzato per proteggere la comunicazione di polling da controller a 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	Sand States States	and an a state of the	Minister and	un brindling	And the second	Save Co	nfiguration	Ping Logout Refresh
A. A.	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	CIDS Sensor Add						< Back	Apply
General RADIUS Authentication RADIUS Accounting	Index	1.						
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 Wireless Protection	Query Interval	15 sec	onds					
Policies Trusted AP Policies	State	3						
Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Management Frame Protection	Fingerprint (SHA1 hash)	1662E996362A9J	1EF08899A7C	1645F5C856A	8842 40 he:	« chars		
Web Login Page								
CIDS Sensors Shunned Clients								

3. Controllare lo stato della connessione tra il sensore IPS e il

VVLC.									
Conta Brattant									Logout Re
A.A.	MONITOR W	ALANS CONTROL	ER WIRELESS	SECURITY I	MANAGEMENT COMM	WNDS HELP			
Security	CIDS Sensor	s List						1	New
AAA	Index	Server Addre	ss Port	State	Query Interval	Last Query (count)			
Ceneral RADUIS Authentication RADUIS Accounting Local Net Users MAC Ribering Disabled Clients User Login Policies AP Policies	1	192.168.5.2	443	Enabled	15	Success (6083)	Ostail Esmons		
Access Control Lists									
Network Access Control									
IPSec Certificates CA Certificate ID Certificate									
Web Auth Certificate									
Wireless Protection Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication Nanagement Prame Protection									
Web Login Page									
CIDS Sensors Shunned Clients									

4. Una volta stabilita la connettività con il sensore Cisco IPS, verificare che la configurazione WLAN sia corretta e che sia abilitata l'esclusione del client.Il valore predefinito del timeout di esclusione dei client è 60 secondi. Si noti inoltre che, indipendentemente dal timer di esclusione dei client, l'esclusione dei client persiste finché il blocco client richiamato da IDS rimane attivo. Il tempo di blocco predefinito nell'IDS è 30 minuti.

Conce Deutens									Save Config	puration Ping	Logout Refre
A.A.	MONITOR WEARS CO	ONTROLLER WIRELESS	SECURITY N	MANAGEMENT	COMMANDS	HELP					
WLANs	WLANs > Edit									< Back	Apply
WLANS WLANS AP Groups VLAN	WLAN ID WLAN SSID	1 1PS									
	General Policies						Security Policies				
	Radio Policy	All 💌					IPv6 Enable				
	Admin Status Session Timeout (secs)	Enabled					Layer 2 Security	WPA1+WPA2	×		
	Quality of Service (QoS)	Silver (best effort)						MAC Filtering			
	WMM Policy 7920 Phone Support	Client CAC Limit A	P CAC Limit				Layer 3 Security	None	*		
	Broadcast SSID	Cnabled						- was hourd			
	Allow AAA Override	Enabled					* Web Policy cannot be	used in combination	with IPsec		
	Client Exclusion	Enabled ** 600					and L2TP.	a is eachied a time.	and and and and		
	DHCP Server	Timeout V	/alue (secs)				zero means infinity(will reset excluded clients)	require administrati-	re override to		
	DHCP Addr. Assignment	Required									
	Interface Name	management 💌									
	MFP Version Required	1									
	MFP Signature Generation										
	H-REAP Local Switching										
	* H-REAP Local Switching	p not supported with IPSEC, i	2TP, PPTP, CRA	NETE and FORTR	ESS authenticat	ions.					
	CISCO Client Extension (CCX)										
	Version 1E	Enabled									
	Aironet IE	2									
	Gratuitous Probe Response										
	Radius Servers										
		Authentication Servers	Accounting Ser	vers							
	Server 1	1P/10.1.1.12, Port:1812	none 💌								

5. Èpossibile attivare un evento nel sistema Cisco IPS quando si esegue una scansione NMAP su determinati dispositivi della rete o quando si esegue un ping su alcuni host monitorati dal sensore Cisco IPS. Dopo aver attivato un allarme nell'IPS Cisco, passare a Monitoraggio e blocchi host attivi per verificare i dettagli

sull'host.	
Cisco IDM 5.0 - 192.168.5.2	
File Help	
Configuration Monitoring Back Forward Refresh	Y Halp
Deried Attackers Dictive Hose Blocks Divetwork Blocks Dickes Dickes	Active Host Blocks Specify the address to block and the duration for that block.
Support information Support information 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

Nell'elenco Shun Client del controller vengono ora inseriti gli indirizzi IP e MAC

A.A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shur	n List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Re-sync IP Addres 10.10.99.25	s L	ast NAC Address 0:40:96:ad:0d:1b	Expire 326979296	5 192.3	or IP / Index 660.5.2 / 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 Authentisation Management Frame Protection								
Web Login Page								
CIDS Sensors Shunned Clients								

dell'host.

ente viene aggiunto all'elenco di esclusione

client.

Corre Brennen A. A.	MONITOR WLA	NS CONTROLLER	WIRELESS SEC	URITY MANAGEMENT	COMMANDS HELP	
Monitor	Excluded Cliente	5				
Summary	Search by MAC	address	Search	h		
Statistics Controller	Client MAC Adds	AP Name	AP NAC Adde	WLAN Typ	e Exclusion Reason	Port
Wireless	00:40:96:ad:0d:1	b AP1242-2	00:14:15:59:3e:10	IPS 802	11b UnknownEnum:5	29 Detail LinkTest Disable Remove

Quando un client viene aggiunto all'elenco dei file condivisi, viene generato un registro delle

	MONITO	OR WLAN	CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Management	32 1	4:41:00	Rogue AP : 00:15x2:02:02:c2 detected on Base Radio MAC : 00:14:1b:59:3e:10 Interface no:0(002.11b/g) with RSSI: -03 and SNR: 6
Summary SNMP General SNMP V3 Users	33 1-22	ue Apr 11 4:40:16 006	New client at 10.10.99.21 requested to be shunned by Sensor at 192.168.5.2
	34 1-2	ue Apr 11 4:39:44 106	Rogue : 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	35 1-22	ue Apr 11 4:39:44 106	Rogue : 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	36 1	ue Apr 11 4:39:44	Rogue: 00:0b:05:54:de:Sf removed from Base Radio MAC: 00:14:16:59:3e:10 Interface

l'evento viene inoltre generato un registro

L'ut



messaggi.

Qua

ndo si esegue una scansione NMAP su un dispositivo monitorato, nel sensore Cisco IPS vengono generati alcuni eventi

IP Range □ IP List Single Host Neighborhood Address: Win32 OS Version Users Patch Level Null IPC\$ Sessions Services MAC Address I0.1.1.12 Null IPC\$ Sessions Services MAC Address I0.1.1.12 Null IPC\$ Sessions Services MAC Address IV NetBIOS Shares Disks Sessions S ID ate and Time Groups Event Log H Image Ping Host(s) RPC Show Bindings S Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image Image </th <th>API Exit Address Clear ions t Log S Help</th> <th>Patch Lev MAC Add</th> <th>Directory Users Services</th> <th>in32 OS Version</th> <th>IP List Neighborhood</th> <th>IP Range C</th>	API Exit Address Clear ions t Log S Help	Patch Lev MAC Add	Directory Users Services	in32 OS Version	IP List Neighborhood	IP Range C
Single Host C Neighborhood Address: 10.1.1.1.2 10.1.1.2 10.1.2 10.1.1.2 10.1.1.2 10.1.2 10.1.2 10.1.2	Address Clear ions Save t Log Help	Patch Lev MAC Add	Users Services	in32 OS Version	Neighborhood	
10.1.1.12 Image: Solution of the second	Address Clear ons Save t Log Help	Sessions	Services	JI 10C4 Saccione		 Single Host C IP Address:
Image: State in the image: State in	t Log Help	C Sessions		an third h substants		10.1.1.12
□ Date and Time □ Groups □ Event Log □ Ping Host(s) □ RPC □ Show □ Traceroute Host □ Traceroute Host weral Options □ TCP Portscan Range: 1 meout for TCP/UDP/ICMP/SNMP: 5 □ UDP Portscan Range: 1 ntries: 3 Max Connections: 1024 □ SNMP Community String: □ ublic 00096b8d51c2 Networkstation Role: NT Workstation Role: IAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server Role: LAN Manager Server KB823182 KB823182 KB823182	t Log Help		Disks	tBIOS Shares		
Ping Host(s) RPC Bindings Show Errors H weral Options Traceroute Host I meout for TCP/UDP/ICMP/SNMP: 5 UDP Portscan Range: 1 ytries: 3 Max Connections: 1024 SNMP Community String: Public ourses: 10.1.1.12 INAC-ACS SNMP Community String: Public ourses: 11.1.2 INAC-ACS SNMP Community String: SNMP Community String: <tr< th=""><th>s Help</th><th>Event Lo</th><th>Groups</th><th>ate and Time</th><th></th><th></th></tr<>	s Help	Event Lo	Groups	ate and Time		
Traceroute Host Traceroute Host Traceroute Host TCP Portscan Range: TCP Portscan Range: TCP Portscan Range: TCP Portscan Range: DUDP Portscan Range: DUDP Portscan Range: DUDP Portscan Range: public DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range: DUP Portscan Range		Errors	RPC Bindings	ng Host(s)		
TCP Portscan Range: 1 meout for TCP/UDP/ICMP/SNMP: 5 UDP Portscan Range: 1 ptries: 3 Max Connections: 1024 SNMP Community String: public public ourress: 10.1.1.12 nmc-ACS putername: WORKGROUP/NAC-ACS : S-1-S-21-790525478-1580436667-1343024091 : Addresses: 00096b8d451c2 h Level: Operating System: 5.0 Role: NT Momber Server Role: MT Manager Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB923182				aceroute Host		
TCP Portscan Range: 1						ieneral Options
meout for TCP/UDP/ICMP/SNMP: 5 UDP Portscan Range: 1 public tries: 3 Max Connections: 1024 SNMP Community String: public convest: 10:1:1:12 NAC-ACS public SNMP Community String: 00096b8d51c2 h Level: 00096b8d51c2 h Level: 00perating System: 5.0 Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB32915	e: 1 1024	can Range:	TCP Ports			
etries: 3 Max Connections: 1024 SNMP Community String: public ourress: 10.1.1.12 NHC-ACS putername: WORKGROUPNAC-ACS : S-1-S-21-790525478-1580436667-1343024091 : Addresses: 00096b8d51c2 h Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182	e: 1 1024	can Range:	UDP Ports	5	UDP/ICMP/SNMP:	Timeout for TCP/
etries: 3 Max Connections: 1024 Constitution, 5547	String: public	nmunity Strip	SNMP Con			
upress: 10.1.1.12 NAC-ACS iputername: WORKGROUPNAC-ACS : S-1-S-21-790525478-1580436667-1343024091 : Addresses: 00096b8d51c2 h Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Workstation Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182	and. It			1024	Max Conne	Retries: 3
Gures: 101.112 NRCACS is 0.1-12 NRCACS is -1-5-21-790525478-1580436667-1343024091 Addresses: 00096668d51c2 h Level: Operating System: 5.0 Role: NT Workstation Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182						
S-1-5-21-790525478-1580436667-1343024091 Addresses: 00096b8d51c2 h Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Workstation Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					ORKGROUP\NAC-	moutername: W
Addresses: 00096b8d5lc2 h Level: Operating System: 5.0 Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182				024091	525478-15804366	D: S-1-5-21-790
00096063102 h Level: Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182						AC Addresses:
Operating System: 5.0 Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					5162	0009668d5
Role: NT Member Server Role: NT Workstation Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					System: 5.0	Operation 1
Role: NT Workstation Role: LAN Manager Workstation Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					lember Server	Role: NT M
Role: LAN Manager Workstation Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					forkstation	Role: NT W
Role: LAN Manager Server Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					Manager Workstat	Role: LAN I
Role: Master Browser Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					Manager Server	Role: LAN I
Comment: Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					er Browser	Role: Maste
Service Pack 4 KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182						Comment:
KB329115 Windows 2000 Hotfix - KB329115 KB823182 Windows 2000 Hotfix - KB823182					ick 4	Service Pa
KB823182 Windows 2000 Hotfix - KB823182				329115	Windows 2000 Ho	KB329115
1.18.8.8.8.8.8.8.5.1.1				823182	Windows 2000 Ho	KB823182
KB823559 Windows 2000 Hothx - KB823559				823559	Windows 2000 Ho	KB823559
KB824105 Windows 2000 Hotfix - KB824105				824105	Windows 2000 Ho	KB824105
KB024151 Windows 2000 Hoffix - KB024151				824151	Windows 2000 Ho	KB824151
KB025119 Windows 2000 Hottix - KB025119				025119	Windows 2000 Ho	KB825119
KB026232 Windows 2000 Hotix - KB026232				020232	windows 2000 Ho	KB026232
KB828035 WINDOWS 2000 PODIX - KB828035				828035	and the second sec	120 0 0 0 0 0 0 0 0

aggiuntivi.

esta finestra mostra gli eventi generati nel sensore Cisco IPS.

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

Esempio di configurazione del sensore Cisco IDS

Questo è l'output dello script di installazione:

```
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#
```

Configurazione di un'ASA per IDS

A differenza di un sensore di rilevamento delle intrusioni tradizionale, un'ASA deve sempre trovarsi nel percorso dati. In altre parole, invece di estendere il traffico da una porta dello switch a

una porta di sniffing passivo sul sensore, l'ASA deve ricevere i dati su un'interfaccia, elaborarli internamente e quindi inoltrarli su un'altra porta. Per gli IDS, usare la struttura policy modulare (MPF) per copiare il traffico che l'ASA riceve sul modulo interno dei servizi di sicurezza per l'ispezione avanzata e la prevenzione (AIP-SSM) per l'ispezione.



Nell'esempio, l'appliance ASA è già configurata e trasmette il traffico. In questa procedura viene illustrato come creare una regola per l'invio di dati a AIP-SSM.

 Accedere all'ASA utilizzando ASDM. Dopo aver eseguito correttamente l'accesso, viene visualizzata la finestra ASA Main System (Sistema principale ASA).



2. Fare clic su **Configuration** (Configurazione) nella parte superiore della pagina. La finestra mostra le interfacce

ASA.														510	
File Roles 1	Depricts	Options	Tools Wiz	ards H	elp									(=)(B	ľ
Since North	Confi	-G paration	Monitoring	0) 	O	Gearch	Retresh	Save	2				Casco Svar	į
Interfaces		2.¥		1 95 B	5 5 5 R	6 4									
Security Policy		-	Inderface		Name	Enabled	Security Level	IP Address		ubnet Mask	Management	MTU	U Description	Add	
645		Ethernet0	ю 	6 4	dside	Yes	0	10.10.102.2	255	265,255.0	No	1500		Edit	
NAT		Etherneto	0		side	Yes	100	172.16.26.2	255	255,255.0	Pio	1500		<u>Colete</u>	1
VPN		Manager	er/0/0	m	an age	Ves	100	192.160.1.1	255	255 255 0	Ves	1500			
							195								
CSD Manager															
<u> </u>															
Routing															
- 89															
Global Objects															
Properties															
		Enable	traffic betwee	in two or	more int	terfaces w	hich are co	onfigured with I	same se	curity levels	•				
											Adata	1 F	Reset		
													admas NA (15) 💣 🕺 7/27/0	6 5 07 52 PM U	1

 Fare clic su Criteri di protezione sul lato sinistro della finestra. Nella finestra risultante, scegliere la scheda Regole dei criteri di servizio.

📫 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 Palicy + Senice Policy Rules	
bierfaces	• • • • • •	3 時 8 影 8 (9)	
8	C Access Rules	AAA Rules Pilter Rules Pilter 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. Per creare un nuovo criterio, fare clic su Add (Aggiungi). L'Aggiunta guidata regole dei criteri del servizio verrà avviata in una nuova finestra.Fare clic su Interface (Interfaccia), quindi selezionare l'interfaccia corretta dall'elenco a discesa per creare un nuovo criterio associato a una delle interfacce che attraversano il traffico.Assegnare al criterio un nome e una descrizione dell'operazione eseguita utilizzando le due caselle di testo.Per passare alla fase successiva, fare clic su Next (Avanti).

Add Service Policy F	Rule Wizard - Service Policy									
Adding a new service p	olicy rule requires three steps:									
Step 1: Configure a service policy.										
Step 2: Configure the 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								

 Creare una nuova classe di traffico da applicare al criterio.Sebbene sia consigliabile creare classi specifiche per l'analisi di tipi di dati specifici, nell'esempio riportato viene selezionata l'opzione Any Traffic per semplicità. Per continuare, fare clic su Next (Avanti).

🚰 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	ı
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. Tuse class-default as the traffic class.	
< Back Next >	Cancel Help

6. Completare questi passaggi perindicare all'ASA di indirizzare il traffico sul suo server AIP-SSM.Per abilitare il rilevamento delle intrusioni, selezionare Abilita IPS per questo flusso di traffico.Impostare la modalità su Promiscua in modo che una copia del traffico venga inviata al modulo fuori banda anziché posizionare il modulo in linea con il flusso di dati.Fare clic su Permit traffic (Autorizza traffico) per verificare che l'ASA passi allo stato fail-open in caso di errore dell'AIP-SSM.Per eseguire il commit della modifica, fare clic su Fine.

🖆 Add Service Policy	y Rule Wizard - Rule Ad	ctions		
Protocol Inspection	Intrusion Prevention	Connection Settings	QoS)
	u lle in the Configuration			
JY Enable IPS to	ir this traffic flow			
C Inline Mode)			
In this mod as a result	de, a packet is directed to t of IPS operation.	IPS and the packet may	be dropped	
	s Mode			
In this mod be droppe	de, a packet is duplicated d by IPS.	for IPS and the original p	oacket cannot	
If IPS card fai	ls, then			
Permit traff	ic			
C Close traffi	c			
			< Back Finish	Cancel Help

7. L'ASA è ora configurata per inviare il traffico al modulo IPS. Per salvare le modifiche sull'appliance ASA, fare clic su **Save** nella riga superiore.

🖆 Cinco ASDW	5.1 for ASA - 172.16.	.26.2				·····			- I X
File Rules S	sarch Options Tools	Wittands Help							
Gin Howe	Configuration Monitor	ing Back Forward S	Refeat	🔜 🥐 Зама Нар				1	discality.
	Configuration + Babur	it/ Policy + Service Policy Rules							
Ξ,	🗣 🚊 🖗 🖬 🚺	125666814							
interfaces	C Access Rules	C AAA Rules C Filler Rules	Genice Policy Rule	lets					
Security Policy	Bhow Rules for Inte	riace: All Interfaces 💌 👔	iew All				1		
14	2	To Re	Classification			Ru e Actions		Description	Add
NAT	Name	Enabled Match Bourba	Dast nation	Device	Timi Ranga		OR inside exiles		Edit
<u> 28</u>	inside-class	any 🕹 🖓 🖓	🎱 are	🖈 any traffic		🥥 ipo promiscuous, permit traffic	Do mana policy		Dalete
VPN									
CSO Hanager									
12									
15									
- Touting									
80									
Global Objects									
3									
Properties									
	1								
	1								
	1								
	Dig Watch	and match						@ Show Summary C Show Detail	
		Apply	Reset	Assessed	al.				
Configuration sh	anges saved successfu	lik.					sedmine INA (15	0 🔒 🔂 🔒 7/31/08 2:54	47 PM UTC

Configurazione di AIP-SSM per l'ispezione del traffico

Mentre l'ASA invia i dati al modulo IPS, associare l'interfaccia AIP-SSM al motore dei sensori virtuali.

1. Accedere a AIP-SSM utilizzando IDM.

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

2. Aggiungere un utente con almeno privilegi di

visualizzatore.



3. Abilitare

l'interfaccia.

S Cisco IDM 5.0 - 172.16.26.10							
File Help							
Configuration Hardwise) 💽 🥐						Casco Systems
Configuration Montoring Configuration Montoring Configuration Configuration	ed Retreat Hop Interfaces A sensing interface my and clicking Enable of Interface Name OugubitEthernetOrt	t be enabled and assigned 5 Visable. Enabled Media Type Yos Elackplane in	D a virtual sensor I Duplex	Speed Auto	Abernate TCP Resel Interface None	erface. You can enable/disable the available sensing interfaces by s	electing the row(s) Select All Est Enable Disable
					Acoly R	eset	
IDM is initialized successfully.						l cisco a	dministrator 🙆

4. Controllare la configurazione del sensore virtuale.



Configurare un WLC per eseguire il polling di AIP-SSM per i blocchi client

Completare questi passaggi quando il sensore è configurato e pronto per essere aggiunto nel controller:

- 1. Scegliere Sicurezza > CIDS > Sensori > Nuovo nel WLC.
- 2. Aggiungere l'indirizzo IP, il numero di porta TCP, il nome utente e la password creati nella sezione precedente.
- 3. Per ottenere l'impronta digitale dal sensore, eseguire questo comando nel sensore e aggiungere l'impronta digitale SHA1 sul WLC (senza i due punti). Utilizzato per proteggere la comunicazione di polling da controller a 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

Cinco Srerens											
A.A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP			
Security	CIDS Sens	sor Edit									
AAA General RADIUS Authentication RADIUS Accounting	Index		2								
Local Net Users	Server Ad	Idress	172.16.26.10								
Disabled Clients User Login Policies	Port		443								
Access Control Lists	Username	e.	controller								
IPSec Certificates CA Certificate ID Certificate	Password		•••••								
Web Auth Certificate	State		2								
Wireless Protection Policies	Query Int	erval	10 sec	onds							
Rogue Policies	Fingerprin	3n	90C996984EFA74F0528092888C483C4584876C55 40 hex chars								
Standard Signatures Custom Signatures	(SHA1 ha	sh)	(hash key is already set)								
Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Last Quer (count)	Y	Success (1400)								
Web Login Page											
CIDS Sensors Shunned Clients											

4. Controllare lo stato della connessione tra l'AIP-SSM e il

WLC.								
Cross Street and	MONITOR WL	ANS CONTROLLE	R WIRELESS	SECURITY M	ANAGEMENT COMM	ANDS HELP		
Security	CIDS Sensors	List						
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Index 1 2	Server Address 192.168.5.2 172.16.26.10	Port 443 443	State Enabled Enabled	Query Interval 15 10	Last Query (count) Unauthorized (1) Success (1444)	Detail Detail	Bemave Bemave
Access Centrol Lists IPSec Certificates CA Certificate ID Certificate								
Web Auth Certificate Wireless Protection Policies Trusted AP Policies Reque Policies Standard Signatures Custom Signatures Signature Events Sumary Client Exclusion Policies AP Authentication / MFP Management Frame Protection								
Web Login Page CIDS Sensors Shunned Clients								

Aggiungere una firma di blocco a AIP-SSM

Aggiungere una firma di ispezione per bloccare il traffico. Sebbene siano presenti molte firme che possono eseguire il processo in base agli strumenti disponibili, in questo esempio viene creata una firma che blocca i pacchetti ping.

1. Selezionare la **firma 2004 (ICMP Echo Request)** per eseguire una rapida verifica della configurazione.

Cisco IDM 5.0 - 192,168.5.2											
File Help											
Configuration Monitoring Back Forward	d Retre	📍 sh Help									Casco System
G. Sensor Setup Sensor Setup Setwork SAllowed Hosts	Signatur Select D	e Configurati r. All Signa	on Aures 💽 Select Criteria: 🖡	-NA- 💌							
B Q SSH B Q Centicates	Sig ID	SubSig ID	Name	Enabled	Action	Sevenity	Fidelity Rating	Type	Engine	Retired	Select All
Clart	1330	2	TCP Drop - Urgent Pointer WI	No	Modify Packet I	Informatio	100	Default	Normalizer	No	NSDB Link
D Q Interface Configuration	1330	11	TCP Drop - Timestamp Not A.	Yes	Deny Packet In	Informatio	100	Default	Normalizer	No	Add
- Dinterfaces	1330	9	TCP Drop - Data in SYNACK	Yes	Deny Packet In	informatio	100	Default	Normalizer	No	Clone
- Stypess	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
Clobal Variables	2002	0	ICMP Source Quench	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	Disable
G. Signature Definition	2003	0	ICMP Redirect	Yes	Produce Alert	High	100	Tuned	Atomic IP	No	
- Signature Variables	2004	0	ICMP Echo Request	Yes	Produce Alert Request Block	High	100	Tuned	Atomic IP	No	Actions Restore Defaults
Miscellaneous	2005	0	ICMP Time Exceeded for a D	No	Produce Alert	informatio	100	Default	Atomic IP	No	
O Q Event Action Rules	2006	0	ICMP Parameter Problem on	No	Produce Alert	Informatio	100	Default	Atomic IP	No	Departies
- Devent Variables	2007	0	ICMP Timestamp Request	No	Produce Alert	informatio .	100	Default	Atomic IP	No	Activate
ToTarpet Value Rating Sevent Action Oversides	2008	0	ICMP Timestamp Reply	No	Produce Alert	informatio	100	Default	Atomic IP	No	Retre
-Sevent Action Filters	2009	0	ICMP Information Request	No	Produce Alert	Informatio	100	Default	Adormic IP	No	

2. Per completare la procedura di verifica, abilitare la firma, impostare la gravità dell'avviso su Alta e impostare Azione evento su **Produzione host avvisi** e **host blocchi richieste**. L'azione Host blocco richiesta è la chiave per segnalare il WLC e creare eccezioni client.

🔍 Edit Signature				negative contraction of the second
Name	Value			a an an an an an an an a <u>s</u>
Signature ID:	2004			
SubSignature ID:	0			
🔶 Alert Severity:	High •			
Big Fidelity Rating:	100			
Promiscuous Delta:	0			
Sig Description:				
	Signature Name: IOMP Echo	Request		
	Alert Notes:			
	User Comments:			
	Alert Traits:			
	Palasea			
	Therease.			
Engine:	Alomic IP			
	Event Action:	Produce Alert Produce Verbose Alert Request Block Connector Request Block Host Request Snmp Trao		
	Fragment Status:	Any		
	🛇 📕 Specify Layer 4 Protocol:	Yes		
		S Layer 4 Protocol:	ICMP Protocol	
			Specify ICMP Sequence:	No 👻
			Specify ICMP Type:	Yes v
			2003333	ICMP Type: 8
			Constitution Contes	
			OperativiCMP Code:	
			Constitution	
			apecily ICMP Total Lengin.	NO 2
				P
 Parameter uses the D Parameter uses a Us 	eraum value. Click the icon to edit the v er-Defined Value. Click the icon to rest	tore the default value.		
		0K Cancel	Halp	
		CALL CALLER	(log	

S. Ed	lit Signature				X				
	Name	Value			<u>-</u>				
	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 Statu	Ann -		<u>*</u>				
•	 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 He	p					

- 3. Per salvare la firma, fare clic su OK.
- 4. Verificare che la firma sia attiva e impostata per eseguire un'azione di blocco.
- 5. Per eseguire il commit della firma nel modulo, fare clic su Applica.

Monitoraggio del blocco e degli eventi con IDM

Attenersi alla seguente procedura:

 Quando la firma viene attivata correttamente, in IDM sono disponibili due posizioni in cui annotare questa condizione.Il primo metodo mostra i blocchi attivi installati da AIP-SSM. Fare clic su Monitoraggio nella riga superiore delle azioni. Nell'elenco di elementi visualizzato sul lato sinistro, selezionare Blocchi host attivi. Ogni volta che viene attivata la firma ping, nella finestra Blocchi host attivi vengono visualizzati l'indirizzo IP del trasgressore, l'indirizzo del dispositivo da attaccare e il tempo rimanente per il quale il blocco è attivo. Il tempo di blocco predefinito è di 30 minuti ed è regolabile. La modifica di questo valore non viene tuttavia illustrata in questo documento. Per informazioni su come modificare questo parametro, consultare la documentazione della configurazione dell'ASA. Rimuovere il blocco immediatamente, selezionarlo dall'elenco e fare clic su Elimina.



Il secondo metodo per visualizzare le firme attivate utilizza il buffer degli eventi AIP-SSM. Dalla pagina Monitoraggio IDM, selezionare **Eventi** nell'elenco degli elementi a sinistra. Viene visualizzata l'utilità di ricerca Eventi. Impostare i criteri di ricerca appropriati e fare clic su

Visualizza

Cisca IDM 5.0 - 172.16.26.10	
le Help	
Configuration Monitoring Dack Forward Refresh	Y Help
Denied Atlackers Active Host Blocks PLogging Diagnostics Report Diagnostics Report Statistics Dystem Information	Puends Show a died events in the local Event Store. By default all events are displayed. To filter over event type and/or time, select the appropriate check boxes. Show all events: 'Pranting 'Proc' 'Pradie'' Boxes the number of the rows per page. Show Network Access Controller events Show status events: 'Prace'' Boxes the sensor'' Show past events: 'Prace'' Prace'' Show status events: 'Prace'' Show past events: 'Prace'' Show status events: 'Prace'' Show past events: 'Prace'' Show events from the following time range: Show from the oldeest event forward End Time (JTC) Prace'' Prace'' Yww. Reset

2. Viene quindi visualizzato il Visualizzatore eventi con un elenco di eventi che corrispondono ai criteri specificati. Scorrere l'elenco e cercare la firma della richiesta echo ICMP modificata nei passaggi di configurazione precedenti.Cercare nella colonna Eventi il nome della firma oppure il numero di identificazione della firma nella colonna Signature

ID.

# Type Sensor UTC Time Event ID Events 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 1145383740954941577 ICMP Echo Request 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 3:19:16 PM U 1145383740954941577 ICMP Echo Request	Sig ID 2004	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 alertinformati July 31, 2006 3:19:16 PM U 1145383740954941574 ICMP Echo Request 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 alertinformati July 31, 2006 3:19:46 PM U 1145383740954941597 ICMP Echo Request	2004	
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 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 alertinformati July 31, 2006 3:19:16 PM U 1145383740954941574 ICMP Echo Request 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 alertinformati July 31, 2006 3:19:46 PM U 1145383740954941597 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		
5 alert informati July 31, 2006 3:19:46 PM U 1145383740954941597 ICMP Echo Request		
	2004	
		Reliesh
	Last Updated: 7/	/31/06 3:22:39 PM

3. Dopo aver individuato la firma, fare doppio clic sulla voce per aprire una nuova finestra. La nuova finestra contiene informazioni dettagliate sull'evento che ha attivato la firma.

```
Details for 1145383740954941597
evIdsAlert: eventId=1145383740954941597 vendor=Cisco severity=informational
  originator:
   hostId: sensor
    appName: sensorApp
   appInstanceId: 341
  time: July 31, 2006 3:19:46 PM UTC offset=0 timeZone=UTC
             description=ICMP Echo Request id=2004 version=S1
  signature:
   subsigId: 0
  interfaceGroup:
 vlan: 0
 participants:
   attacker:
     addr: 10.10.99.26 locality=OUT
    target:
      addr: 10.10.102.1 locality=OUT
 summary: 4 final=true initialAlert=1145383740954941574 summaryType=Regular
  alertDetails: Regular Summary: 4 events this interval ;
 riskRatingValue: 25
 interface: ge0_1
 protocol: icmp
```

Monitorare l'esclusione dei client in un controller wireless

A questo punto, nell'elenco dei client esclusi del controller vengono inseriti gli indirizzi IP e MAC dell'host.

Constantion A. A.	MONITOR	WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP
Security	CIDS Shu	n List						
AAA General RADIUS Authentication	Re-sync	. L	st MAC Address	Expire	Sent	ior IP / Index		
RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	10.10.99.2	6 00	0:40:96:ad:0d:1b	27	172.1	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								

L'utente viene aggiunto all'elenco di esclusione client.

Core Bronnen	MONITOR WL	ANS CONTROLLER	WIRELESS SI	ECURITY MAN	AGEMENT CO	OMMANDS HELP		
Monitor Summary Statistics Centroller Ports Wireless Rogue APs Known Rogue APs Rogue Clents Adhoe Clents	Excluded Client Search by MAC Client NAC Add 00:40:96:ad:0d	ts address Ir AP Name 1b APD014.6940.814	AP NAC Addr te 00:14:15:5a:16:4	WLAN WLAN 10 IPS	Type 802.11a	Exclusion Reason UnknownEnum:5	Port 29	Detail Link Test Disable Remove
802.11a Radios 802.11b/g Radios Clients RADIUS Servers								

Monitoraggio eventi in WCS

Gli eventi di sicurezza che attivano un blocco all'interno di AIP-SSM fanno in modo che il controller aggiunga l'indirizzo del trasgressore all'elenco di esclusione dei client. In WCS viene inoltre generato un evento.

- Per visualizzare l'evento di esclusione, utilizzare l'utilità Monitor > Alarms del menu principale di Sistema colori Windows. WCS visualizza inizialmente tutti gli allarmi non cancellati e presenta inoltre una funzione di ricerca sul lato sinistro della finestra.
- 2. Modificare i criteri di ricerca per trovare il blocco client. In Gravità scegliere **Minore** e impostare anche la categoria di allarme su **Sicurezza**.
- 3. Fare clic su

Cerca

4. La finestra Allarme elenca quindi solo gli allarmi di sicurezza con un livello di gravità minore. Puntare il mouse sull'evento che ha attivato il blocco all'interno di AIP-SSM.In particolare, WCS mostra l'indirizzo MAC della stazione client che ha causato l'allarme. Posizionando il puntatore del mouse sull'indirizzo appropriato, viene visualizzata una piccola finestra con i dettagli dell'evento. Fare clic sul collegamento per visualizzare gli stessi dettagli in un'altra finestra.

Cisco Wireless Co	introl S	ystem					Username: roo	t Logout Refresh Print \
Monitor • Configu	re 🕶 🕴	ocation	n 🔻 <u>A</u> dminis	stration = Help =				
Alarms		Alar	rms					Select a command
Severity Minor	~		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 Security	~		Minor	Client 00:40:96:ad:0d:1b		7/26/06 2:47 PM	The WEP Key configured at the station may be wr	
Jocomy			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:1b		7/31/06 4:25 PM	Client '00:40:96:ad:0d:1b' which was associated,	
				Client 100:40:96:ad:0dt 100:14:1b:5a:16:40', into code is 'S(Unknown)'.	b' which was as inface 'O' is exclu	sociated with AP ded. The reason		

Esempio di configurazione di Cisco ASA

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(2)
!
hostname ciscoasa
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif outside
```

```
security-level 0
 ip address 10.10.102.2 255.255.255.0
1
interface Ethernet0/1
nameif inside
 security-level 100
ip address 172.16.26.2 255.255.255.0
Ţ
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#
```

Esempio di configurazione del sensore Cisco Intrusion Prevention System

```
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#
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Installazione e utilizzo di Cisco Intrusion Prevention System Device Manager 5.1
- Appliance Cisco ASA serie 5500 Adaptive Security Guide alla configurazione
- Configurazione del sensore Cisco Intrusion Prevention System con l'interfaccia della riga di comando 5.0 - Configurazione delle interfacce
- Guida alla configurazione WLC 4.0
- <u>Supporto tecnico wireless</u>
- Domande frequenti sui Wireless LAN Controller (WLC)
- Esempio di configurazione base di Wireless LAN Controller e Lightweight Access Point
- Configurazione delle soluzioni di sicurezza
- Documentazione e supporto tecnico Cisco Systems