Esempio di configurazione di ACL su controller LAN wireless

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni ACL su WLC Considerazioni sulla configurazione degli ACL nei WLC Configurazione di ACL sui WLC Configura regole per consentire servizi utente guest Configurazione degli ACL della CPU Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritto come configurare gli Access Control List (ACL) sui Wireless LAN Controller (WLAN) per filtrare il traffico attraverso la WLAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione del WLC e del Lightweight Access Point (LAP) per un funzionamento di base
- Conoscenze base di LWAPP (Lightweight Access Point Protocol) e metodi di sicurezza wireless

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2000 WLC con firmware 4.0
- Cisco serie 1000 LAP
- Cisco 802.11a/b/g Adattatore client wireless con firmware 2.6
- Cisco Aironet Desktop Utility (ADU) versione 2.6

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 Cisco sulle convenzioni nei suggerimenti tecnici.

ACL su WLC

Gli ACL sul WLC hanno lo scopo di limitare o permettere ai client wireless di accedere ai servizi sulla propria WLAN.

Prima della versione 4.0 del firmware del WLC, gli ACL vengono ignorati sull'interfaccia di gestione, quindi non è possibile influenzare il traffico destinato al WLC. È possibile solo impedire ai client wireless di gestire il controller con l'opzione **Gestione tramite wireless**. Pertanto, gli ACL possono essere applicati solo alle interfacce dinamiche. Nel firmware WLC versione 4.0, sono disponibili ACL della CPU in grado di filtrare il traffico destinato all'interfaccia di gestione. Per ulteriori informazioni, vedere la sezione <u>Configurazione degli ACL della CPU</u>.

Èpossibile definire fino a 64 ACL, ciascuno con un massimo di 64 regole (o filtri). Ogni regola dispone di parametri che influiscono sulla relativa azione. Quando un pacchetto soddisfa tutti i parametri di una regola, l'azione impostata per tale regola viene applicata al pacchetto. Gli ACL possono essere configurati dalla GUI o dalla CLI.

Di seguito sono elencate alcune delle regole che è necessario comprendere prima di configurare un ACL sul WLC:

- Se l'origine e la destinazione sono **qualsiasi**, la direzione in cui questo ACL viene applicato può essere **qualsiasi**.
- Se sourceordestination **non** è **any**, è necessario specificare la direzione del filtro e creare un'istruzione inversa nella direzione opposta.
- La nozione WLC di "in entrata" e "in uscita" non è intuitiva. È dalla prospettiva del WLC rivolto verso il client wireless, piuttosto che dal punto di vista del client. Dunque, per direzione in entrata si intende un pacchetto che entra nel WLC dal client wireless, per direzione in uscita si intende un pacchetto che esce dal WLC in direzione del client wireless.
- Alla fine dell'ACL, è presente un rifiuto implicito.

Considerazioni sulla configurazione degli ACL nei WLC

Gli ACL nei WLC funzionano in modo diverso rispetto ai router. Di seguito sono riportati alcuni aspetti da ricordare quando si configurano gli ACL nei WLC:

- L'errore più comune è selezionare IP quando si intende negare o consentire i pacchetti IP. Selezionando il contenuto del pacchetto IP, i pacchetti IP-in-IP vengono negati o consentiti.
- Gli ACL dei controller non possono bloccare l'indirizzo IP virtuale del WLC e quindi i pacchetti DHCP per i client wireless.
- Gli ACL del controller non possono bloccare il traffico multicast ricevuto da reti cablate

destinate a client wireless. Gli ACL del controller vengono elaborati per il traffico multicast avviato da client wireless, destinato a reti cablate o altri client wireless sullo stesso controller.

- A differenza di un router, l'ACL controlla il traffico in entrambe le direzioni quando applicato a un'interfaccia, ma non esegue il firewall con stato. Se si dimentica di aprire un buco nell'ACL per il traffico di ritorno, si verifica un problema.
- Gli ACL dei controller bloccano solo i pacchetti IP. Non è possibile bloccare ACL di livello 2 o pacchetti di livello 3 diversi da IP.
- Gli ACL dei controller non usano maschere inverse come i router. In questo caso, 255 indica esattamente la corrispondenza con l'ottetto dell'indirizzo IP.
- Gli ACL sul controller vengono eseguiti tramite software e influiscono sulle prestazioni di inoltro.

Nota: se si applica un ACL a un'interfaccia o a una WLAN, la velocità di trasmissione wireless diminuisce e può causare una perdita potenziale dei pacchetti. Per migliorare la velocità di trasmissione, rimuovere l'ACL dall'interfaccia o dalla WLAN e spostarlo su un dispositivo cablato adiacente.

Configurazione di ACL sui WLC

In questa sezione viene descritto come configurare un ACL sul WLC. L'obiettivo è configurare un ACL che consenta ai client guest di accedere ai seguenti servizi:

- Protocollo DHCP (Dynamic Host Configuration Protocol) tra client wireless e server DHCP
- Protocollo ICMP (Internet Control Message Protocol) tra tutti i dispositivi della rete
- DNS (Domain Name System) tra i client wireless e il server DNS
- Telnet su una subnet specifica

Tutti gli altri servizi devono essere bloccati per i client wireless. Completare questi passaggi per creare l'ACL con l'interfaccia utente grafica del WLC:

 Andare alla GUI del WLC e scegliere Sicurezza > Access Control Lists. Viene visualizzata la pagina Access Control Lists. In questa pagina vengono elencati gli ACL configurati sul WLC. Inoltre, permette di modificare o rimuovere gli ACL. Per creare un nuovo ACL, fare clic su Nuovo

G · O · 🗷 🖬 :	🐔 🔎 👷 🧐 🍰 🕺 Address 🕘 https://172.16.1.40/screens,fire 🔤 🔂 Go 🛛 Linis 🦷 Norton Additious 😣 • 🛛 🖉 – 6 🗙
Cases Statema	Save Configuration Ping Logout Refresh
A. A.	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	Access Control Lists
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Name
Access Control Lists	
Web Auth Certificate	
Wireless Protection Policies Trusted AP Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	
Web Login Page CIDS Sensors Shunned Clients	
8	Internet

Access Control Lists

 Immettere il nome dell'ACL e fare clic su Apply (Applica).Èpossibile immettere un massimo di 32 caratteri alfanumerici. Nell'esempio, il nome dell'ACL è Guest-ACL. Dopo aver creato l'ACL, fare clic su Edit (Modifica) per creare le regole dell'ACL.



Immettere il nome dell'ACL

 Quando viene visualizzata la pagina Access Control Lists > Modifica, fare clic su Aggiungi nuova regola. Viene visualizzata la pagina Access Control Lists > Rules > New.

3 · 5	🏠 🔎 👷 🥝 🍰 🎽 Address 🕘 https://172.16.1.40/screens/fire 📉 🔁 Go 🛛 Linis 🤴 Norton Anklikrus 🤬 - 🖉 🥌 🦉
Casco Statema	Save Configuration Ping Logout Refresh
A. A. Martine	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	Access Control Lists > Edit Add New Rule
AAA General	General
RADIUS Authentication RADIUS Accounting Local Net Users	Access List Name Guest-ACL
MAC Filtering Disabled Clients	Seq Action Source IP/Mask Destination Protocol Source Dest DSCP Direction IP/Mask Port Port
User Login Policies AP Policies	
Access Control Lists	
Web Auth Certificate	
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection Web Login Page CIDS Sensors	
Shunned Clients	
and the second s	Uncernet

Aggiungi nuove regole ACL

4. Configurare le regole che consentono a un utente guest di utilizzare i seguenti servizi:DHCP tra client wireless e server DHCPICMP tra tutti i dispositivi della reteDNS tra i client wireless e il server DNSTelnet su una subnet specifica

Configura regole per consentire servizi utente guest

In questa sezione viene illustrato un esempio di configurazione delle regole per questi servizi:

- DHCP tra client wireless e server DHCP
- ICMP tra tutti i dispositivi della rete
- DNS tra i client wireless e il server DNS
- Telnet su una subnet specifica
- Per definire la regola per il servizio DHCP, selezionare gli intervalli IP di origine e destinazione. In questo esempio viene utilizzato any come origine, il che significa che qualsiasi client wireless può accedere al server DHCP. Nell'esempio, il server 172.16.1.1 funge da server DHCP e DNS. L'indirizzo IP di destinazione è 172.16.1.1/255.255.255.255 (con una maschera host). Poiché DHCP è un protocollo basato su UDP, selezionare UDP dal campo a discesa Protocollo. Se nel passaggio precedente è stato scelto TCP o UDP, vengono visualizzati due parametri aggiuntivi: Porta di origine e Porta di destinazione. Specificare i dettagli delle porte di origine e di destinazione. Per questa regola, la porta di origine è client DHCP e la porta di destinazione è server DHCP.Selezionare la direzione in cui applicare l'ACL. Poiché questa regola viene applicata dal client al server, in questo esempio viene utilizzato il protocollo In entrata. Dalla casella di riepilogo a discesa Azione,

scegliere **Permit** per fare in modo che l'ACL consenta ai pacchetti DHCP dal client wireless al server DHCP. Il valore predefinito è Deny. Fare clic su **Apply**





Selezionare Permit per fare in modo che ACL consenta i pacchetti DHCP Se l'origine o la destinazione non sono **qualsiasi**, è necessario creare un'istruzione inversa nella direzione opposta. Ecco un esempio.

G · O · 🖻 🖻	6 2 * 8 6	👌 - 🍓 🎽 Address 🔬 https:	//172.16.1.40/screens,fre 🎽 🛃 G	io Links Norton Ar	killirus 🚱 •	🥂 – 8 ×
Circo Station				Save Confi	juration Ping	Logout Refresh
Alexandra and a second	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HE	LP	
Security	Access Control Lists	s > Rules > New			< Back	Apply
AAA General	Sequence	2	IP Address	Netmask		
RADIUS Authentication RADIUS Accounting	Source	IP Address	172.10.1.1	230.230.230.235		
Local Net Users MAC Filtering	Destination	Any 👻				
Disabled Clients User Login Policies AP Policies	Protocol	UDP 💌				
Access Control Lists	Source Port	DHCP Server 👻				
Web Auth Certificate	Destination Port	DHCP Client				
Wireless Protection Policies Trusted AP Policies	DSCP	Any 🗸				
Rogue Policies Standard Signatures	Direction	Outbound 🛩				
Custom Signatures Signature Events Summery	Action	Permit 💌				
AP Authentication / MFP Management Frame Protection						
Web Login Page						
CIDS Sensors Shunned Clients						
۵					🕲 Inte	rnet

Origine o destinazione impostata su Qualsiasi

2. Per definire una regola che autorizzi i pacchetti ICMP tra tutti i dispositivi, selezionare any (qualsiasi) nei campi Source (Origine) e Destination (Destinazione). Questo è il valore predefinito.Selezionare ICMP dal campo a discesa Protocollo. Poiché in questo esempio viene utilizzata qualsiasi per i campi Origine e Destinazione, non è necessario specificare la direzione. Può essere lasciato sul valore predefinito di any . Inoltre, non è richiesta l'istruzione inversa nella direzione opposta.Dal menu a discesa Azione, scegliere Permit per fare in modo che questo ACL consenta i pacchetti DHCP dal server DHCP al client wireless. Fare clic su Apply (Applica).

3 · 0 · 2	6 P * 0 0	Address 🔬 http	:://172.16.1.40/sc	reens,lfrz 🎽 🔁 Go	Links Nort	on AnkiWrus 😣 🔹	🦉 – 8 ×
Cince Stattun					Save C	onfiguration Ping	Logout Refresh
A. A. Deservices	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	Access Control Lists	s > Rules > New				< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Sequence Source	3 Any 💌					
MAC Filtering Disabled Clients User Login Policies AP Policies	Protocol	ICMP					
Access Control Lists	DSCP	Any 📉					
Web Auth Certificate	Direction	Any 💌					
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary	Action	Permit					
Client Exclusion Policies AP Authentication / MFP Management Frame Protection							
Web Login Page							
CIDS Sensors Shunned Clients							
Done			I TELEVISION AND			🌍 Inte	ernvet

Autorizzazione affinché ACL consenta l'invio di pacchetti DHCP dal server DHCP al client wireless

3. Analogamente, creare regole che consentano l'accesso del server DNS a tutti i client wireless e l'accesso del server Telnet per il client wireless a una subnet specifica. Ecco gli esempi.

	U PX O	Non-cos Sal uct			we Configuration 1. Since	
ite Station					we configuration Ping	Logout Kei
	MONITOR WEARS	CONTROLLER WIRELES	S SECURITY MANAGEM	ENT COMMAI	VDS HELP	
ecurity	Access Control Lists	s > Rules > New			< Back	Apply
AA	Sequence	3				
RADIUS Authentication	Source	Any 💌				
Local Net Users MAC Filtering	Destination	Any 💌				
Disabled Clients User Login Policies	Protocol	ICMP 👻				
AP Policies	DSCP	Any 💌				
teh Auth Certificate	Direction					
vireless Protection	Direction	Any				
olicies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MPP Magnatemat Exerce	Action	Permit 💌				
Protection						
Veb Login Page						
CIDS						
Shunned Clients						
Dama.						
Done					•	nternet
trea regole che con	sentono l'accesso	al server DNS per tu	tti i client wireless		•	nternet
rea regole che con	sentono l'accesso	al server DNS per tu	tti i client wireless	9 Go Links	Norton Antiliirus 🙆 •	nternet
rea regole che con	sentono l'accesso 🚳 🔎 🗙 🥹 👔	al server DNS per tu	tti i client wireless ps://172.16.1.40/screens/fic 💙 🚦	Go Linis	Norton Antilikrus 😵 -	nternet
Done rea regole che con C · C · M C	sentono l'accesso 💰 🔎 🚖 🥹 👔	al server DNS per tui	tti i client wireless ps://172.16.1.40/screens/fre 💙 🕻	€ Go Linis	Norton Antilikrus 🛞 -	nternet 1 Logout Re
Done rea regole che con C • C E E C E Surrer A A	sentono l'accesso 🟠 🔎 🚖 🥹 👔 MONITOR WLANS	al server DNS per tur - S Madres Madres	tti i client wireless 95:]/172-16-1.40]screens,fire 💙 🕻 5 SECURITY MANAGEM	о Linis » Si IENT COMMA	Notion Antilikrus 🛞 • ave Configuration Ping VDS HELP	nternet 27 – 1 Logout Ref
i bone rea regole che con Corresti i con Internet Anne de Recurity	Sentono l'accesso	al server DNS per tui Addres @http: CONTROLLER WIRELES	tti i client wireless ss://172.16.1.40/screens/fre 🗙 s security managem	S Go Linis " S. IENT COMMA	Norton Antilikus 🛞 - ave Configuration Ping NDS HELP < Back	nžemet 200 – 1 Logout Re Apply
Done rea regole che con C C C C C C C C C C C C C	Sentono l'accesso	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New	tti i client wireless ps://172.16.1.40/screens.frz 🗙	S Go Linis " S. IENT COMMAI	Norton Antilikus 🛞 - Ave Configuration Ping NDS HELP < Back	nbernet Apply
Done rea regole che con	Sentono l'accesso	al server DNS per tur Address Address Address CONTROLLER WIRELESS S > Rules > New 4	tti i client wireless ss://172.16.1.40/screens.frz 🗙	S. Linis " S. IENT COMMAI	Norton Antilivrus 😵 - sve Configuration Ping VDS HELP <back< td=""><td>nternet</td></back<>	nternet
Done rea regole che con C C C C C C C C C C C C C C C C C C C	Sentono l'accesso	al server DNS per tui Address The CONTROLLER WIRELES S > Rules > New Any	tti i client wireless ps://172.16.1.40/screens/fre 💙 🕻 s security managem	€ Linis S. IENT COMMA	Norton Antilikrus 🛞 • we Configuration Pino NDS HELP < Back	nternet Logout Re Apply
Done rea regole che con	Sentono l'accesso	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New Any IP Address V	tti i client wireless ps://172.16.1.40/screens.frz Y	So Linis So So IENT COMMAN	Norton Antilikus 🛞 - ave Configuration Ping NDS HELP < Back	nbernet Logout Re Apply:
Cone rea regole che con • • • • • • • • • • • • • • • • • • •	Sentono l'accesso	al server DNS per tur Address Meters CONTROLLER WIRELES S > Rules > New Any IP Address V	tti i client wireless s://172.16.1.40/screens/fite s security MANAGEM IP Address 172.16.1.1	So Linis Si IENT COMMA Netmask 255.255.255	Norton Antilikrus 🛞 - eve Configuration Pino NDS HELP < Back	nternet Logout Re Apply
Cone rea regole che con Cone	Sentono l'accesso	al server DNS per tur Address Address Address Address S > Rules > New Any IP Address UDP	tti i client wireless ss://172.16.1.40/screens/fre v S SECURITY MANAGEM IP Address 172.16.1.1	Comman Silent Comman Netmask 255.255.255	Notion Antilikus 🛞 - eve Configuration Ping VDS HELP <back< td=""><td>nbernet</td></back<>	nbernet
Done rea regole che con Control Marcon Recurity RAA General RADIUS Authentication RADIUS Authentication RA	Sentono l'accesso MONITOR WLANS Access Control Liste Sequence Source Destination Protocol Source Port	al server DNS per tur Address The CONTROLLER WIRELESS S > Rules > New Any IP Address V UDP V Any V	tti i client wireless ss://172.16.1.40/screens,firz Y	So Linis So So IENT COMMAN Netmask 255.255.255	Norton Antilikus 🛞 - Ave Configuration Ping NDS HELP < Back	nbernet
Done rea regole che con Con Con Con Con Con Con Con	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port	al server DNS per tur Address Meters CONTROLLER WIRELES S > Rules > New Any IP Address V UDP Any V DNS V	tti i client wireless ps://172.16.1.40/screens/fite V	So Unis So So IENT COMMA Netmask 255.255.251	Norton Antilikrus 🛞 - even Configuration Pino VDS HELP < Back	nternet
Cone rea regole che con C - C - C - C - C - C - C - C - C - C -	Sentono l'accesso MONITOR WLANS Access Control Liste Sequence Source Destination Protocol Source Port Destination Port Destination Port	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New Any V IP Address V UDP V Any V Any V	tti i client wireless ss://172.16.1.40/screens,fire 🗙 💽 S SECURITY MANAGEM IP Address 172.16.1.1	So Linis S.	Norton Antiliveus 🛞 - Ave Configuration Ping NDS HELP S.255	nbernet
Done rea regole che con Con Control Cont	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction	al server DNS per tur Address Meters CONTROLLER WIRELES S > Rules > New Any IP Address V UDP Any NUS Any Inbound V	tti i client wireless ps://172.16.1.40/screens/fite V	Comman Si IENT COMMA Netmask 255.255.255	Notion Antilikus 🛞 - eve Configuration Pino VDS HELP < Back	nbernet
Done rea regole che con rea regole che con reaction of the con reaction of the con reaction of the con RADIUS Authentication RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Logn Policies AP Policies Viroless Protection rusted AP Policies Rogue Policies Standard Signatures Signature Events Signature Events Signature Events Signature Events Signature Events Signature Events Signature Events Signature Events Signature Events Com Custom Signatures Com Custom Signatures Com Custom Signatures Com Custom Signatures Com Custom Signatures Custom Signa	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Part DSCP Direction Action	al server DNS per tur Address Address Address Address Address Address Source Any Address Addr	tti i client wireless ss://172.16.1.40/screens.frz Y	So Linis S.	Norton Antiliveus So - Ave Configuration Pino NDS H€LP <back< td=""><td>nbernet</td></back<>	nbernet
Done rea regole che con Con Con Con Con Con Con Con	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address Meters CONTROLLER WIRELES S > Rules > New 4 Any IP Address V UDP Any New Any Permit V	tti i client wireless ps://172.16.1.40/screens/fite V	Comman Silent Comman Netmask 255.255.255	Norton Antilikus 🛞 - eve Configuration Pino VDS HELP < Back	nžemet Logout Re Apply
Done rea regole che con con con con con con con con	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address Meters S > Rules > New Any IP Address V UDP Any Permit Permit	tti i client wireless ps://172.16.1.40/screens/fite V	COMMA SIENT COMMA Netmask 255.255.255	Norton Antilikus So • Norton Antilikus So • NDS HELP <back< td=""><td>nžemet Logout Re Apply</td></back<>	nžemet Logout Re Apply
Done Prea regole che con Prea regole che con Preserei Rapius Authentication RADIUS Aut	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELESS S > Rules > New Any IP Address V UDP V Any Permit V Permit V	tti i client wireless ss://172.16.1.40/screens,fit v	Comman Si IENT COMMA Netmask 255.255.255	Norton Antilikus 🛞 - Ave Configuration Pino VDS HELP < Back 3.255	nbernet
Done Crea regole che con Creation of the con C	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELESS S > Rules > New Any V IP Address V UDP V Any V Inbound V Permit V	tti i client wireless ss://172.16.1.40/screens,fit Y	So Linis So So Linis So Linis So Linis So So Linis So	Norton Antilikus 🛞 - Ave Configuration Pino NDS HELP <back 3.255</back 	nžemet
Crea regole che con Crea	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELESS S > Rules > New Any IP Address V UDP Any NP Permit V	tti i client wireless ss://172.16.1.40/screens,fit Y	So Linis So Sent COMMA Netmask 255.255.255	Norton Antilikus 🛞 - Ave Configuration Pino NDS HELP < Back 3.255	nbernet
Crea regole che con Crea	Sentono l'accesso MONITOR VLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New 4 Any V IP Address V UDP V Any V Inbound V Permit V	tti i client wireless ss://172.16.1.40/screens,fit Y	So Linis S SALENT COMMAN	Norton Antilikus 🛞 - Ave Configuration Pino NDS HELP S.255	nžemet
Crea regole che con Crea regole che con Crea regole che con Crea regole che con Creation con Creation con Creation con Creation con Creation con Creation con Creation con Creation con Creation con Con Con Con Con Con Con Con C	Sentono l'accesso MONITOR VLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New 4 Any V IP Address V UDP V Any V DNS V Inbound V Permit V	tti i client wireless ss://172.16.1.40/screens,fit Y	So Linis S SALENT COMMAN	Norton Antiliveus 🛞 - Ave Configuration Pino NDS HELP S.255	nbernet
Crea regole che con Crea regole che con Crea regole che con Crea regole che con Creation Control con Control con Control con Con Con Con Con Con Con Con C	Sentono l'accesso MONITOR VLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New 4 Any W 1P Address W UDP W Any W DNS W Inbound W Permit W	tti i client wireless ss://172.16.1.40/screens,fit Y	So Linis S So IENT COMMAI	Norton Antiliveus So - Ave Configuration Pino NDS HELP S.255	nžemet
Crea regole che con Crea regole che con Crea regole che con Crea regole che con Creation de la constant Creation de la constant Creation de la constant Creation de la constant Co	Sentono l'accesso MONITOR VLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New 4 Any V IP Address V UDP V Any V Inbound V Permit V	tti i client wireless ss://172.16.1.40/screens.fr: S SECURITY MANAGEM IP Address 172.16.1.1	So Linis S So IENT COMMAI	Autor Antiliveus So - Norton Antiliveus So - NDS HELP <back< td=""><td>nžemet</td></back<>	nžemet
Done Trea regole che con Trea regole che con Control con Control Contr	Sentono l'accesso MONITOR VLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address The CONTROLLER WIRELES S > Rules > New 4 Any IP Address UDP Any NS Permit Permit	tti i client wireless ss://172.16.1.40/screens.fr: S SECURITY MANAGEM IP Address 172.16.1.1	So Linis So So IENT COMMAN	Autor Antiliveus Sort Norton Antiliveus Sort NDS HELP <back 5.255</back 	nžemet
Done rea regole che con rea regole che con Con Con Con Con Con Con Con	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address Meters S > Rules > New 4 Any IP Address UDP Any Permit Permit V	tti i client wireless s://172.16.1.40/screens/fit S SECURITY MANAGEM IP Address 172.16.1.1	Comman Supervisional Netmask 295.255.251	Auston Antiliaus 🛞 - Ave Configuration Pino VDS HELP C Back	nžemet
Done rea regole che con rea regole che con Con Con Con Con Con Con Con	Sentono l'accesso MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	al server DNS per tur Address Meters S > Rules > New Any IP Address V UDP Any Permit Permit	tti i client wireless ps://172.16.1.40/screens/fit V	Co Linis S.	Autorian Antibility S - Ave Configuration Prince VDS HELP C Back	Apply

۵

Creazione di regole che consentono l'accesso del client wireless a una subnet da parte del server Telnet Definire questa regola per consentire al client wireless di accedere al servizio





Consenti accesso del client wireless al servizio Telnet

G · O · 🖻 🖻	6 🔎 🛠 🛛 🙆	Address 🔬 Ht	tps://172.16.1.40/screens,fre 🎽 🧧	Go Links Norton A	intilirus 🚷 •	AY - 8 3
area Stattan	HANKSHAR			Save Conf	iguration Ping	Logout Refres
A. alt. In provide the	MONITOR WLANS	CONTROLLER WIRELE	SS SECURITY MANAGEMI	ENT COMMANDS H	ELP	
Security	Access Control Lists	s > Rules > New			< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Access Control Lists Web Auth Certificate Wireless Protection Policies	Sequence Source Destination Protocol Source Port Destination Port	6 Any V IP Address V TCP V Any V Telnet V	IP Address 172.18.0.0	Netmask 255.255.0.0		
Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	DSCP Direction Action	Any V Inbound V Permit V				
Web Login Page						
CIDS Sensors Shunned Clients						
https://172.16.1.40/screench	arcer.html#				Inte	met

Un altro esempio di accesso client wireless al servizio Telnet La pagina ACL > Modifica elenca tutte le

regole definite per l'ACL.

curity	Acce	ss Contre	ol Lists > Edit						< Back		Add New	Rule
NA General	Gene	ral										
RADIUS Authentication RADIUS Accounting Local Net Users	Acces	s List Nam	e Guest-	ACL	Dectiontion				Devit.			
MAC Filtering Disabled Clients	Seq	Action	Source IP/Mas	ik	IP/Mask		Protocol	Port	Port	DSCP	Direction	
Jser Login Policies AP Policies	1	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	<i>'</i>	UDP	DHCP Client	DHCP Server	Any	Inbound	Edit Remove
cess Control Lists	2	Permit	172.16.1.1 255.255.255.255	1	0.0.0	1	UDP	DHCP Server	DHCP Client	Any	Outbound	Edit Remove
ireless Protection licies	з	Permit	0.0.0.0	/	0.0.0	1	ICMP	Any	Any	Any	Any	Edit Remove
Trusted AP Policies Rogue Policies	4	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	1	UDP	Any	DNS	Any	Inbound	Edit Remove
Standard Signatures Custom Signatures Signature Events	5	Permit	172.16.1.1 255.255.255.255	/	0.0.0.0	/	UDP	DNS	Any	Any	Outbound	Edit Remove
Summary Client Exclusion Policies UP Authentication / MFP	6	Permit	0.0.0.0	/	172.18.0.0 255.255.0.0	/	TCP	Any	Teinet	Any	Inbound	Edit Remove
tanagement Frame rotection	7	Permit	172.18.0.0 255.255.0.0	1	0.0.0	1	TCP	Teinet	Any	Any	Outbound	Edit Remove
DS ensors hunned Clients												

Modifica pagina: elenca tutte le regole definite per l'ACL

- 4. Dopo aver creato l'ACL, occorre applicarlo a un'interfaccia dinamica. Per applicare l'ACL, scegliere **Controller > Interfacce** e modificare l'interfaccia a cui applicare l'ACL.
- Nella pagina Interfacce > Modifica per l'interfaccia dinamica, scegliere l'ACL appropriato dal menu a discesa Access Control Lists. Ecco un esempio.

G · O 🗷 🖬 (🕼 🔎 🛧 🚱 🙆 🖉	Address Address //172.16.1.40/so	reens,lfra 🖌 🛃 Go	Links Norb	on AntiVirus 🚯 🔹	A
inen Stattens				Save C	onfiguration Ping	Logout Refres
<u></u>	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	Interfaces > Edit				< Back	Apply
General Inventory	General Information					
Interfaces	Interface Name G	uest				
Internal DHCP Server Mobility Management	Interface Address					
Mobility Groups Mobility Statistics	VLAN Identifier	1				
Ports	IP Address	172.19.1.10				
Master Controller Mode	Netmask	255.255.0.0				
Network Time Protocol	Gateway	172.19.1.50				
QoS Profiles	Physical Information					
	Port Number	1				
	Configuration					
	Quarantine					
	DHCP Information					
	Primary DHCP Server	172.16.1.1				
	Secondary DHCP Server					
	Access Control List					
	ACL Name	Guest-ACL				
	Note: Changing the Interface pa temporarily disabled and thus m some clients.	arameters causes the WLANs to be hay result in loss of connectivity for				
0					(Å) 101	ernet

Selezionare l'ACL appropriato dal menu Access Control List

Al termine, l'ACL autorizza e nega il traffico (in base alle regole configurate) sulla WLAN che usa questa interfaccia dinamica. Interface-ACL può essere applicato solo agli access point H-Reap in modalità connessa, ma non in modalità standalone.

Nota: in questo documento si presume che le WLAN e le interfacce dinamiche siano configurate. Per informazioni su come creare interfacce dinamiche sui WLC, fare riferimento a <u>Configurazione delle VLAN sui controller LAN wireless</u>.

Configurazione degli ACL della CPU

In precedenza, gli ACL sui WLC non disponevano di un'opzione per filtrare il traffico di dati LWAPP/CAPWAP, il traffico di controllo LWAPP/CAPWAP e il traffico di mobilità destinato alle interfacce di gestione e di gestione dei punti di accesso. Per risolvere questo problema e filtrare il traffico LWAPP e di mobilità, gli ACL della CPU sono stati introdotti con il firmware WLC versione 4.0.

La configurazione degli ACL della CPU prevede due passaggi:

- 1. Configurare le regole per l'ACL della CPU.
- 2. Applicare l'ACL CPU sul WLC.

Le regole per l'ACL della CPU devono essere configurate in modo simile agli altri ACL.

Verifica

Cisco consiglia di verificare le configurazioni degli ACL con un client wireless per verificare che siano state configurate correttamente. Se l'ACL non funziona correttamente, verificare gli ACL sulla pagina Web dell'ACL e verificare che le modifiche all'ACL siano state applicate all'interfaccia del controller.

Per verificare la configurazione, è possibile anche utilizzare i seguenti comandi show:

• show acl summary: per visualizzare gli ACL configurati sul controller, usare il comando show acl summary.Di seguito è riportato un esempio:

(Cisco Controller) >show acl summary

ACL	Name	Applied
Gues	st-ACL	Yes

 show acl detailedACL_Name: visualizza informazioni dettagliate sugli ACL configurati.Di seguito è riportato un esempio:

(Cisco Controller) >show acl detailed Guest-ACL

	Source	Destination		Source Port
Dest Por	t			
I Dir	IP Address/Netmask	IP Address/Netmask	Prot	Range
Range	DSCP Action			
1 In	0.0.0/0.0.0.0	172.16.1.1/255.255.255.255	17	68-68
67-67	Any Permit			
2 Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	67-67
68-68	Any Permit			
3 Any	0.0.0/0.0.0.0	0.0.0/0.0.0.0	1	0-65535
0-65535	Any Permit			
4 In	0.0.0/0.0.0.0	172.16.1.1/255.255.255.255	17	0-65535
53-53	Any Permit			
5 Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	53-53
0-65535	Any Permit			
6 In	0.0.0/0.0.0.0	172.18.0.0/255.255.0.0		60-65535
23-23	Any Permit			
7 Out	172.18.0.0/255.255.0.0	0.0.0/0.0.0.0	6	23-23
0-65535	Any Permit			

 show acl cpu: per visualizzare gli ACL configurati sulla CPU, usare il comando show acl cpu.Di seguito è riportato un esempio:

(Cisco Controller) >show acl cpu

CPU Acl Name..... CPU-ACL Wireless Traffic..... Enabled Wired Traffic.... Enabled

Risoluzione dei problemi

Il software controller versione 4.2.x o successive consente di configurare i contatori ACL. I contatori ACL possono aiutare a determinare quali ACL sono stati applicati ai pacchetti trasmessi tramite il controller. Questa funzione è utile per la risoluzione dei problemi del sistema.

I contatori ACL sono disponibili su questi controller:

• Serie 4400

- Cisco WiSM
- Switch controller LAN wireless integrato Catalyst 3750G

Per abilitare questa funzione, attenersi alla seguente procedura:

- 1. Per aprire la pagina Access Control Lists, scegliere Sicurezza > Access Control Lists > Access Control Lists.In questa pagina vengono elencati tutti gli ACL configurati per il controller.
- 2. Per verificare se i pacchetti hanno raggiunto uno degli ACL configurati sul controller, selezionare la casella di controllo **Abilita contatori** e fare clic su **Applica**. In caso contrario, lasciare deselezionata la casella di controllo. Questo è il valore predefinito.
- 3. Per cancellare i contatori di un ACL, posizionare il cursore sulla freccia di selezione blu dell'ACL e scegliere **Cancella contatori**.

Informazioni correlate

- Guida alla configurazione di Cisco Wireless LAN Controller, versione 6.0
- <u>Configurazione delle VLAN sui controller LAN wireless</u>
- <u>Risoluzione dei problemi in seguito a un errore di connessione di Lightweight Access Point</u>
 (LAP) a un WLC
- <u>Supporto tecnico e download Cisco</u>

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).