Configuratievoorbeeld van ACL-filters op Aironet AP's

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Waar ACLâ€TMs moeten worden gemaakt MAC-adresfilters IP-filters Ethertype-filters

Inleiding

Dit document beschrijft hoe u op ACL-filters (Access Control List) kunt configureren op basis van Cisco Aironet access points (AP's) met gebruik van de GUI.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van deze onderwerpen:

- De configuratie van een draadloze verbinding met gebruik van een Aironet AP en een Aironet 802.11 a/b/g clientadapter
- ACL's

Gebruikte componenten

Dit document maakt gebruik van Aironet 1040 Series AP's waarop Cisco IOS[®]-softwarerelease 15.2(2)JB wordt uitgevoerd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

U kunt filters op AP's gebruiken om deze taken uit te voeren:

- Toegang tot het draadloze LAN (WLAN)-netwerk beperken
- Een extra beveiligingslaag voor draadloos LAN bieden

U kunt verschillende soorten filters gebruiken om verkeer te filteren op basis van:

- Specifieke protocollen
- Het MAC-adres van het clientapparaat
- Het IP-adres van het clientapparaat

U kunt filters ook inschakelen om verkeer van gebruikers op het bekabelde LAN te beperken. IP-adres en MAC-adresfilters maken het doorsturen van unicast- en multicast-pakketten die naar of van specifieke IP- of MAC-adressen worden verzonden, mogelijk of verbieden.

Op protocollen gebaseerde filters bieden een korreliger manier om de toegang tot specifieke protocollen via de Ethernet- en radio-interfaces van het toegangspunt te beperken. U kunt deze methoden gebruiken om de filters op de toegangspunten te configureren:

- Web GUI
- CLI

Dit document legt uit hoe ACL's moeten worden gebruikt om filters via de GUI te configureren.

Opmerking: Raadpleeg voor meer informatie over de configuratie door het gebruik van de CLI het <u>Cisco-artikel_Voorbeeld van configuratie van ACL-filter voor access point</u>.

Configureren

In deze sectie wordt beschreven hoe u op ACL gebaseerde filters kunt configureren op Cisco Aironet AP's met gebruik van de GUI.

Waar ACL's moeten worden gemaakt

Ga naar **Beveiliging** > **Geavanceerde beveiliging**. Kies het tabblad **Associatietoegangslijst** en klik op **Filter definiëren**:

cisco	HOME	<u>N</u> ETWORK	ASSOCIATION	W <u>I</u> RELI	ess <u>s</u> e	CURITY <u>S</u> ER	vices <u>s</u> oftw	ARE <u>E</u> VENT	LOG	
Security	Но	stname Auton	omous							
Encryption Manager SSID Manager	s	ecurity Sumr	nary							
Server Manager AP Authentication	A U	dministrators sername				Read-Only				
Intrusion Detection Local RADIUS Server	ntrusion Detection Cisco					1				
Advance Security	S	ervice Set Iden SID	tifiers (SSIDs)		VLAN	BandSelect	Radi	o	BSSID/Gues	t Mode√
սիսիս cisco	Номе	NETWORK	ASSOCIATION	WIRELES	5 SECI	IRITY <u>S</u> ERVICI	es <u>s</u> oftware	EVENT LOG	;	
Security	AU	MAC ADDRESS		TIMERS	3	ASSOC	LIST			
Admin Access Encryption Manager	Hos	stname Autono	mous aced Security- As	sociation A	ccess Lis	1		•		
Server Manager AP Authentication Intrusion Detection Local RADIUS Server	F	ilter client as	sociation with M	AC address	access li	st:		< NONE >	Define Fill	er

MAC-adresfilters

U kunt op MAC-adres gebaseerde filters gebruiken om clientapparaten te filteren op basis van het hardgecodeerde MAC-adres. Wanneer een client toegang wordt geweigerd via een op MAC gebaseerd filter, kan de client geen koppeling maken met het toegangspunt. Met MAC-adresfilters kan of kan het doorsturen van unicast- en multicast-pakketten die zijn verzonden van of zijn gericht aan specifieke MAC-adressen, worden verboden.

Dit voorbeeld illustreert hoe u een op MAC gebaseerd filter kunt configureren via de GUI om de client te filteren met een MAC-adres van **0040.96a5.b5d4**:

1. Maak het MAC-adres ACL 700. Met deze ACL kan de client 0040.96a5.b5d4 niet aan het AP worden gekoppeld.

curity	E APPLY F	ILTERS	MAC ADDRESS FILT	ERS	IP FILTERS	i i	ETHERTYPE FILTERS	
dmin Access	Hostname Autono	auom					Autonomous uptima	is 4 weeks, 16 hours, 6 minut
cryption Manager								
ID Manager	Services: Filter	s - MAC Address Filter	•					
rver Manager	Create/Edit Filt	er Index: < NEW >	-					
rusion Detection								
cal RADIUS Server	Filter Index:	700	(700-799)					
vance Security								
	Add MAC Adds	ese: 0040 96x5 b5d4	Mask- 0000.0000	Action:	Black - Add			
	Prop marco Proven			ALLIAND.				
		(1010-000-002	n) (nnan.nna	in anany				
	Date in Landau							
	Dangun ALUGN.	TYDE 2						
	Elhor Classer							
	Fillers Cidoec							
				^				
				- Delete Class	1			

- 2. Klik op Add om dit filter toe te voegen aan de Filterklassen. U kunt de standaardactie ook definiëren als Alles doorsturen of Alles weigeren.
- 3. Klik op Apply (Toepassen). ACL 700 wordt nu gemaakt.
- 4. Als u ACL 700 op een radio-interface wilt toepassen, navigeert u naar het gedeelte Filters toepassen. U kunt deze ACL nu toepassen op een inkomende of uitgaande radio of Gigabit Ethernet-interface.

iiliiilii cisco	HOME NETWORK	ASSOCIATION WIRE	LESS SECURITY S	SERVICES SOFTWARE	EVENT LOG		Sage Conf	gunation (Sing Logout Bafree						
Security Admin Access	JE ADDLY	FLTERS	MAC ADDRESS FLT	ERS	IP FILTERS	Ĭ	ETHERTYPE RLTERS Autonomous uptim	e is 4 weeks, 16 hours, 11 minutes						
SSID Manager	Services: Filte	Services: Filters - Apply Filters												
Server Manager		Radio	0.802.11N ^{2.4GHz}		Radio1-802.11N ^{5GHz}		Gig	abitEthernet0						
Intrusion Detection	Incoming	MAC	< NONE >		MAC < NO	NE > 💌	MAC	< NONE >						
Local RADIUS Server		EtherType	< NONE >	Ett	erType <no< td=""><td>NE > 💌</td><td>EtherType</td><td>< NONE > •</td></no<>	NE > 💌	EtherType	< NONE > •						
		IP	< NONE > •		IP <no< td=""><td>NE > •</td><td>P</td><td>< NONE > •</td></no<>	NE > •	P	< NONE > •						
	Outgoing	MAC	< NONE > 💌		MAC <no< td=""><td>NE > 💌</td><td>MAC</td><td>< NONE > m</td></no<>	NE > 💌	MAC	< NONE > m						
		EtherType	< NONE > •	Eb	erType <no< td=""><td>NE > .</td><td>EtherType</td><td>< NONE > .</td></no<>	NE > .	EtherType	< NONE > .						
		IP	< NONE > 💌		IP <n0< td=""><td>NE > 💌</td><td>P</td><td>< NONE > .</td></n0<>	NE > 💌	P	< NONE > .						
		Inse Wadow					Constant (c) 1982-3	Apply. Cancel						

IP-filters

U kunt standaard of uitgebreide ACL's gebruiken om de toegang van clientapparaten tot het WLANnetwerk toe te staan of te verbieden op basis van het IP-adres van de client.

Dit configuratievoorbeeld gebruikt uitgebreide ACLâ€TMs. Uitgebreide ACL moet Telnet-toegang tot de clients toestaan. U moet alle andere protocollen op het WLAN-netwerk beperken. Ook gebruiken de clients DHCP om het IP-adres te verkrijgen. U moet een uitgebreide ACL maken die:

- Maakt DHCP- en Telnet-verkeer mogelijk
- Ontkent alle andere verkeerstypen

Voltooi de volgende stappen om een bestand te maken:

1. Geef het filter een naam en selecteer **Alles blokkeren** in de vervolgkeuzelijst **Standaardactie**, omdat het resterende verkeer moet worden geblokkeerd:

սիսիս	And the second se			Silve Lonn	dination Fuld redort Paul
cisco	HOME NETWORK ASSO	CIATION WIRELESS GEOURITY SERVICES	SOFTWARE EVENTLOG		
Security	APPLY FILTERS	I MAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
Admin Access	Hostname Autonomous			Autonomous uptime is	4 weeks, 16 hours, 14 minutes
Encryption Manager					
SSID Manager	Services: Filters - IP Fi	iters			
Server Manager AP Authentication	Create/Edit Filter Nam	< NEW > •			
Intrusion Detection	5 h H				
Advance Security	Filter Name:	Allow_DHCP_Telnet			
	Default Action:	Block Al			
	IP Address				
	Destination Address:		Mask: 0.0.0.0		
	Source Address:	0.0.0.0	Mask: 255.255.255.255		
				Action:	Forward * Add
	IP Protocol				
	IP Protocol:	 Authentication Header Protocol (51) 		Action:	Forward . Add
		Custom (0-255)			

2. Selecteer Telnet in de vervolgkeuzelijst **TCP-poort** en **BOOTP-client-** en **BOOTP-server** in de **vervolgkeuzelijst UDP**-poort:

cisco	HOM	E NETWORK	ASSOCIATION	wigeness groue	RITY SERVICES	SOFTWARE	EVENTLOG			ante composition Eud	regers Ferre
Security		IP Protocol:	 Author Custor 	ntication Header Prot	(0-255)	•			Action:	Forward .	Add
Admin Access Encryption Manager SSID Manager					(****)						
Server Manager		UDP/TCP Port									
AP Authentication Intrusion Detection		TCP Port:	Teinet (23))]			Action:	Forward .	Add
Local RADIUS Server Advance Security			© Custom	0	0-66535)	_					
		JDP Port:	 Bootstrap 	Protocol (BOOTP) s	erver (67)				Action:	Forward 💌	Add
			© Custom	0	0-65535)						
		Filters Classes									
		TCP part: Telline UDP part: Boot UDP part: Boot Default - Block	t (23) - Ferward strap Protocol (BOO) strap Protocol (BOO) All	TP) client (68) - Ferwi TP) server (67) - Ferw	ard Aard			- Delete Cl	855		
	_	-							_		
										Apply De	lete Cancel

3. Klik op **Apply** (**Toepassen**). Het IP-filter **Allow_DHCP?_Telnet** is nu gemaakt en u kunt deze ACL toepassen op een inkomende of uitgaande radio of Gigabit Ethernet-interface.

cisco	HOME NETWOR	K ASSOCIATION	WIRELESS SECURITY	SERVICES SOFTWARE	EVENT LOG	Say	e Configuration (Eing Logout Befreuh						
Security	APP	LYFILTERS	BINC ADDRESS FIL	TERS	IP FLITERS	ETHERTYPE PLTER	4						
Admin Access	Hostname Aut	Hostname Autonomous uptime is 4 weeks, 16 hours, 25 minutes											
Encryption Manager SSID Menager	Services: Filters - Apply Filters												
Server Manager			Radio0-802.11N ^{2.4GHz}		Radio1-802.11NSGHz		GigabitEthernet0						
Intrusion Detection	Incoming	MAC	< NONE > .	MAC	< NONE > .	MAC	< NONE > .						
Local RADIUS Server		EtherType	<none> .</none>	EtherType	< NONE > m	EtherType	< NONE > x						
Automatic Sector by		IP	< NONE >	P	< NONE >	P	< NONE >						
	Outgoing	MAC	Allow_DHCP_Telnet	MAC	< NONE >	MAC	< NONE > *						
		EtherType	< NONE > •	EtherType	< NONE > •	EtherType	< NONE > •						
		IP	< NONE >	P	< NONE >	P	< NONE >						
							Apply. Cancel						

Ethertype-filters

U kunt Ethertype-filters gebruiken om IPX-verkeer (Internetwork Packet Exchange) op Cisco Aironet AP te blokkeren. Een typische situatie waar dit nuttig is, is wanneer IPX-server uitzendt de draadloze verbinding verstikken, wat soms gebeurt op een groot ondernemingsnetwerk.

Voltooi deze stappen om een filter te configureren en toe te passen dat IPX-verkeer blokkeert:

- 1. Klik op het tabblad **Filters Ethernet**.
- 2. Noem het filter in het veld **Filter Index** met een nummer van 200 tot 299. Het nummer dat u toewijst, maakt een ACL voor het filter.
- 3. Typ **8137** in het veld **Add Ethertype**.
- 4. Laat het masker voor het Ethertype in het veld Masker staan op de standaardwaarde.
- 5. Selecteer **Blok** in het actiemenu en klik op **Toevoegen**.

cisco	HOME DETWORK ASSOCIAT	ION WIRELESS SECURITY SE	ERVICES SOFTWARE EVENTLOG	Saye Configu	nation <u>B</u> ing Logout Befreah
Security Admin Access Encryption Manager SSTD Manager Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	Hostname Autonomous Services: Filters - EtherTyp Create/Edit Filter Index:	Eliters CNEW > CNEW >	Invites governmante enternation In 17 In Printerna	ETHERTYPE FILTERS Autonomous uptime is 4	weeks, 19 hours, 35 minutes
	Filter Index: Add EtherType: Default Action:	200 (200-29 (8137 (0.#FFF) Hana •	99) Mask: 0000 (0-FFFE)	Action: Block 💌	[Add] =
	Filters Classes: EiterType: 8137 Mask: 000 Dafaut - None	0 - Block			

6. Om Ethertype uit de lijst van de Klassen van Filters te verwijderen, selecteer het, en klik de Klasse van de Schrapping. Herhaal de vorige stappen en voeg de typen 8138, 00ff en 00e0 aan het filter toe. U kunt deze ACL nu toepassen op een inkomende of uitgaande radio of Gigabit Ethernet-interface.

cisco	HOME NETWORK	ASSOCIATION	WIRELESS SECURITY	SERVICES SOFTWARE	EVENT LOG	Say	e Configuration Eng	Logout Befreah						
Security	APPL	Y FILTERS	MAC ADDRESS	FILTERS	IP FILTERS	ETHERTYPE PLTER	B							
Admin Access	Hostname Auto	Hostname Autonsmous Autonsmous uptime is 4 weeks, 16 hours, 37 minutes												
Encryption Manager SSID Manager	Services: Filt	Services: Filters - Apply Filters												
Server Manager			Radio0.802.11N ^{2.4GHz}		Radio1-802.11N ^{5GHz}		GigabitEthernet®							
Intrusion Detection	Incoming	MAC	< NONE > •	MAC	< NONE > •	MAC	< NONE > •							
Local RADIUS Server		EtherType	< NONE > IN	EtherType	< NONE > x	EtherType	< NONE > .							
		IP	200 •	P	< NONE >	P	< NONE >	•						
	Outgoing	MAC	< NONE > .	MAC	< NONE > x	MAC	< NONE > *							
		EtherType	< NONE > •	EtherType	< NONE > .	EtherType	< NONE > x							
		IP	< NONE >	P	< NONE >	P	< NONE >							
								Apply Cancel						
						_								

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.