Konfigurationsbeispiel für ACL-Filter auf Aironet APs

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Erstellen von ACLs MAC-Adressfilter IP-Filter Ethertype-Filter

Einleitung

In diesem Dokument wird beschrieben, wie Sie ACL-basierte Filter (Access Control List) auf Cisco Aironet Access Points (APs) mithilfe der GUI konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Konfiguration einer Wireless-Verbindung unter Verwendung eines Aironet AP und eines Aironet 802.11 a/b/g Client Adapter
- ACLs

Verwendete Komponenten

In diesem Dokument werden APs der Serie Aironet 1040 verwendet, auf denen die Cisco IOS[®] Software, Version 15.2(2)JB, ausgeführt wird.

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

Hintergrundinformationen

Sie können auf den APs Filter verwenden, um folgende Aufgaben durchzuführen:

- Beschränken des Zugriffs auf das WLAN
- Zusätzliche Wireless-Sicherheit

Sie können verschiedene Arten von Filtern verwenden, um Datenverkehr auf der Grundlage von:

- Spezifische Protokolle
- Die MAC-Adresse des Client-Geräts
- Die IP-Adresse des Client-Geräts

Sie können auch Filter aktivieren, um den Datenverkehr von Benutzern im LAN einzuschränken. IP-Adressen- und MAC-Adressfilter erlauben oder verbieten die Weiterleitung von Unicast- und Multicast-Paketen, die von oder an bestimmte IP- oder MAC-Adressen gesendet werden.

Protokollbasierte Filter bieten eine detailliertere Möglichkeit, den Zugriff auf bestimmte Protokolle über die Ethernet- und Funkschnittstellen des Access Points zu beschränken. Sie können eine der folgenden Methoden verwenden, um die Filter auf den APs zu konfigurieren:

- Weboberfläche
- CLI

In diesem Dokument wird die Verwendung von ACLs zum Konfigurieren von Filtern über die GUI erläutert.

Hinweis: Weitere Informationen zur Konfiguration über die CLI finden Sie im Cisco Artikel <u>Access</u> <u>Point ACL Filter Configuration Example</u>.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie ACL-basierte Filter auf Cisco Aironet APs mithilfe der GUI konfigurieren.

Erstellen von ACLs

Navigieren Sie zu **Sicherheit** > **Erweiterte Sicherheit**. Wählen Sie die Registerkarte **Association Access List** aus, und klicken Sie auf **Define Filter**:

uluilu cisco	HOME	NETWORK	ASSOCIATION	WIRELESS	SECURIT	Y <u>s</u> ervice	S <u>S</u> OFTWARE	EVENT LOG	
Security Admin Access	Hos	stname Autono	mous						
Encryption Manager SSID Manager Server Manager	Se Ac	ecurity Summ Iministrators	ıary						
AP Authentication	U	sername					Read-Only		
Intrusion Detection	Ci	sco ervice SetIden	tifiers (SSIDs)				√		
Advance Security	S	SID		VL	AN Ban	dSelect	Radio	BSSID/Gu	est Mode√



MAC-Adressfilter

Sie können MAC-Adressbasierte Filter verwenden, um Client-Geräte anhand der hartcodierten MAC-Adresse zu filtern. Wenn einem Client der Zugriff über einen MAC-basierten Filter verweigert wird, kann der Client keine Verbindung zum AP herstellen. MAC-Adressfilter erlauben oder verhindern die Weiterleitung von Unicast- und Multicast-Paketen, die entweder von bestimmten MAC-Adressen gesendet oder an bestimmte MAC-Adressen adressiert werden.

In diesem Beispiel wird veranschaulicht, wie ein MAC-basierter Filter über die Benutzeroberfläche konfiguriert wird, um den Client mit der MAC-Adresse **0040.96a5.b5d4** zu filtern:

1. Erstellen Sie die ACL 700 für die MAC-Adresse. Mit dieser ACL kann der Client 0040.96a5.b5d4 keine Verbindung mit dem Access Point herstellen.

ı. cısco	Saya Carifiguration (Eng. Lagout (Enfre HOME NETWORK ASSOCIATION WRITERS SECURITY SERVICES SOFTWARE EVENTLOG
Security	
Admin Access	Hostname Autonomous uptime is 4 weeks, 16 hours, 6 minutes
Encryption Manager SSID Manager	Services: Filters - MAC Address Filters
Server Manager AP Authentication	Create/Edit Filter Index: < NEW > •
Intrusion Detection Local RADIUS Server Advance Security	Filter Index: 700 (700-799)
	Add MAC Address: 0040 96a5.55d4 Mask: 0000.0000 Action: Block Add (H4H4H H4H4H H4H4H H4H4H)
	Default Action: None -
	Filters Classes:
	- Delete Class
	Apply Delate Carcel

- 2. Klicken Sie auf **Hinzufügen**, um diesen Filter den Filterklassen hinzuzufügen. Sie können die Standardaktion auch als **Alle weiterleiten** oder **Alle verweigern** definieren.
- 3. Klicken Sie auf Apply (Anwenden). ACL 700 wurde erstellt.
- 4. Um ACL 700 auf eine Funkschnittstelle anzuwenden, navigieren Sie zum Abschnitt Filter anwenden. Sie können diese ACL jetzt auf eine Funkschnittstelle (Eingang oder Ausgang) oder eine GigabitEthernet-Schnittstelle anwenden.

uluulu cisco	HOME NET	TWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	SOFTWARE	EVEN	тіоб		Sage Conf	punation ging Logo	ut Befreah
Security Admin Access)i	APPLYF	L TERS	1	AC ADDRESS F	LTERS	H	IP FL.	TERS	li	ETHERTYPE RLTERS Autonomous uptim	e is 4 weeks, 16 hours, 1	1 minutes
SSID Menager Server Manager	Service	es: Filters	- Apply Filters	Radio0-80	2.11N ^{2.4GHz}			Radi	o1.802.11N ^{8GHz}		Gig	abitEthernet0	
AP Authentication Intrusion Detection Local RADIUS Server	Incomin	9	Ether	MAC <i< td=""><td>NONE > • NONE ></td><td></td><td>Ether</td><td>MAC Type</td><td>< NONE > •</td><td></td><td>MAC EtherType</td><td>< NONE ></td><td></td></i<>	NONE > • NONE >		Ether	MAC Type	< NONE > •		MAC EtherType	< NONE >	
Advance Security	Outoria				NONE > •			IP	< NONE > •		P	< NONE > •	
	ougan	9	Ether	Type <	NONE > .		Ether	Type	< NONE >		EtherType	< NONE > .	
				IP <	NONE > 💌			IP	< NONE > 💌		p	< NONE > .	
												Apply	Cancel
		CI	ose Window								Copyright (c) 1992-2	008, 2011-2012 by Cisco	Systems, Inc

IP-Filter

Sie können standardmäßige oder erweiterte Zugriffskontrolllisten verwenden, um den Zugriff von Client-Geräten auf das WLAN basierend auf der IP-Adresse des Clients zu erlauben oder zu verweigern.

In diesem Konfigurationsbeispiel werden erweiterte Zugriffskontrolllisten verwendet. Die erweiterte ACL muss den Telnet-Zugriff auf die Clients zulassen. Sie müssen alle anderen Protokolle im WLAN einschränken. Außerdem verwenden die Clients DHCP, um die IP-Adresse abzurufen. Sie müssen eine erweiterte ACL erstellen, die:

- Ermöglicht DHCP- und Telnet-Datenverkehr
- Verweigert alle anderen Datenverkehrstypen

Gehen Sie wie folgt vor, um die Datei zu erstellen:

1. Geben Sie dem Filter einen Namen, und wählen Sie **Block All (Alle blockieren**) in der Dropdown-Liste **Default Action (Standardaktion**) aus, da der verbleibende Datenverkehr blockiert werden muss:

cisco	HOME NETWORK ASS	OCIATION WIRELESS SECURITY SER	RVICES SOFTWARE EVENTLOG	Sage Low	udmumou Rud redon. R
Security	APPLY FILTER	IS I WAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
Admin Access	Hostname Autonomous			Autonomous uptime i	s 4 weeks, 16 hours, 14 minutes
Encryption Manager SSID Manager	Services: Filters - IP	Filters			
Server Manager AP Authentication	Create/Edit Filter Na	< NEW > •			
Intrusion Detection Local RADIUS Server Advance Security	Filter Name: Default Action:	Allow_DHCP_Teinet			
	IP Address				
	Destination Address Source Address:	0.0.0.0	Mask: 0.0.0.0 Mask: 255.255.255.255		
				Action:	Forward • Add
	IP Protocol				
	IP Protocel:	Authentication Header Protocol (51)	×	Action:	Forward Add
		© Custom (0-255)			

2. Wählen Sie Telnet aus der Dropdown-Liste **TCP Port** (**TCP-Port**) und **BOOTP Client** & **BOOTP Server** aus der Dropdown-Liste **UDP Port** (BOOTP-**Client** und **BOOTP-Server**) aus:

cisco	HOME NETWORK	ASSOCIATION WIRELESS SECURITY SERVICE	S SOFTWARE EVENTLOG	-sege	Toundration Find redon	e i Pana
Security Admin Access Encryption Manager	IP Protocol:	Authentication Header Protocol (51) Custom (0-255)		Action:	Forward • Ad	N
SSED Manager Server Nanager AP Authentication Intrusion Detection Local RADIUS Server	UDP/TCP Port	 Teinet (23) Custom (0-65535) 	1	Action:	Forward Ad	aa]
Advance Security	JDP Port:	Bootstap Protocol (BOOTP) server (67) Custom (0-6535)		Action:	Forward	sa l
	Filters Classes TCP port: Tell UDP port: Bot Histoporte Hos Default - Block	net (23) - Forward distrap Protocol (BCOTP) client (68) - Forward status Protocol (ISCOTP) server (67) - Forward c All		- Delete Class		
					Apply Delete (Cancel

3. Klicken Sie auf **Apply** (**Anwenden**). Der IP-Filter **Allow_DHCP?_Telnet** wurde erstellt, und Sie können diese ACL auf eine eingehende oder ausgehende Radio- oder GigabitEthernet-Schnittstelle anwenden.

սիսիս						Saya (Configuration Eing Logout Befreuh
CISCO	HOME NETWOR	ASSOCIATION	WIRELESS SECURITY	SERVICES SOFTWARE	EVENTLOG		
Security	JE APPL	YFILTERS	B WAC ADDRESS FILT	TERS I	IP FILTERS 1	ETHERTYPE PLTERS	
Admin Access	Hostname Auto	nomous				Autonomous u	ptime is 4 weeks, 16 hours, 25 minutes
Encryption Manager							
SSID Manager	Services: Filt	ers - Apply Filters					
Server Manager		1	Radio0-802.11N ^{2.4GHz}		Radio1-802.11NSGHz		sigabitEthernet0
Intrusion Detection	Incoming	MAC	< NONE > .	MAC	< NONE >	MAC	NONE >
Local RADIUS Server		EtherType	< NONE > x	EtherType	< NONE > .	EtherType	NONE > x
rature recently		IP	< NONE >	P	< NONE >	P	NONE >
	Outgoing	MAC	Allow_OHCP_Telnet	MAC	< NONE > .	MAC	NONE > *
		EtherType	< NONE >	EtherType	< NONE >	EtherType _	NONE >
		IP	< NONE >	P	< NONE >	P	NONE >
						_	
							Apply, Gencel

Ethertype-Filter

Sie können Ethertype-Filter verwenden, um IPX-Datenverkehr (Internetwork Packet Exchange) auf dem Cisco Aironet AP zu blockieren. Eine typische Situation, in der dies nützlich ist, ist, wenn die Wireless-Verbindung durch den IPX-Server unterbrochen wird, was manchmal in einem großen Unternehmensnetzwerk der Fall ist.

Gehen Sie wie folgt vor, um einen Filter zu konfigurieren und anzuwenden, der IPX-Datenverkehr blockiert:

- 1. Klicken Sie auf die Registerkarte Ethertype Filters (Ethertypfilter).
- 2. Geben Sie im Feld **Filterindex** dem Filter einen Namen mit einer Zahl zwischen 200 und 299. Durch die Nummer, die Sie zuweisen, wird eine ACL für den Filter erstellt.
- 3. Geben Sie in das Feld Ethertype hinzufügen den Wert 8137 ein.
- 4. Lassen Sie die Maske für den Ethertype im Maskenfeld auf dem Standardwert.
- 5. Wählen Sie im Menü Aktion die Option **Block** aus, und klicken Sie auf **Hinzufügen**.

rity	E APPLY FILTERS	H WAC ADDRESS FILTERS	IP FLTERS	ETHERTYPE FILTERS	
in Access	Hostname Autonomous			Autonomous uptime is 4 week	ks, 16 hours, 35 minute
yption Manager D Manager	Services: Filters - EtherTyp	e Filters			
ver Manager Authentication	Create/Edit Filter Index:	< NEW > •			
al RADIUS Server ance Security	Filter Index:	200 (200-299)			
	Add EtherType:	8137 (Q-FFFF)	Mask: 0000 (0.FFFE)	Action: Block 💌	Add
	Default Action:	None			
	Filters Classes:				
	EtherType: 8137 Mask: 000 Default - None	A Block			
		- Del	iste Class		

6. Um den Ethertype aus der Liste Filterklassen zu entfernen, wählen Sie ihn aus, und klicken Sie auf Klasse löschen. Wiederholen Sie die vorherigen Schritte, und fügen Sie dem Filter die Typen 8138, 00ff und 00e0 hinzu. Sie können diese ACL jetzt auf eine Funkschnittstelle (Eingang oder Ausgang) oder eine GigabitEthernet-Schnittstelle anwenden.

	APPL	Y FILTERS	WAC ADDRESS FILTS	ERS 1	IP FILTERS	ETHERTYPE FILTER	B
	Hostname Auto	nomous				Autonomou	s uptime is 4 weeks, 16 hours,
Manager sger	Services: Filt	ers - Apply Filters					
lager			Radio0.802.11N ^{2.4GHz}		Radio1-802.11N ^{SGHz}		GigabitEthernetD
Atection	Incoming	MAC	< NONE > •	MAC	< NONE > •	MAC	< NONE > •
US Server		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE > .
icarity		IP	200 •	P	< NONE >	P	< NONE >
	Outgoing	MAC	< NONE >	MAC	< NONE > .	MAC	< NONE > .
		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE > •
		IP	<none></none>	P	< NONE >	P	< NONE >

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.