Exemple de configuration des filtres ACL sur les AP Aironet

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Où créer des listes de contrôle d'accès Filtres d'adresses MAC Filtres IP Filtres Ethertype

Introduction

Ce document décrit comment configurer des filtres basés sur une liste de contrôle d'accès (ACL) sur des points d'accès Cisco Aironet à l'aide de l'interface utilisateur graphique.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration d'une connexion sans fil à l'aide d'un AP Aironet et d'un adaptateur client Aironet 802.11 a/b/g
- ACL

Components Used

Ce document utilise les points d'accès de la gamme Aironet 1040 qui exécutent le logiciel Cisco IOS[®] version 15.2(2)JB.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

Vous pouvez utiliser des filtres sur les points d'accès afin d'effectuer ces tâches :

- Restreindre l'accès au réseau sans fil LAN (WLAN)
- Fournir une couche supplémentaire de sécurité sans fil

Vous pouvez utiliser différents types de filtres afin de filtrer le trafic en fonction de :

- de protocoles spécifiques ;
- Adresse MAC du périphérique client
- Adresse IP du périphérique client

Vous pouvez également activer des filtres afin de restreindre le trafic des utilisateurs sur le réseau local câblé. Les filtres d'adresse IP et d'adresse MAC permettent ou rejettent le transfert des paquets de monodiffusion et de multidiffusion qui sont envoyés vers ou depuis des adresses IP ou MAC spécifiques.

Les filtres basés sur des protocoles fournissent une façon plus précise de restreindre l'accès aux protocoles spécifiques par les interfaces Ethernet et radios de l'AP. Vous pouvez utiliser l'une de ces méthodes afin de configurer les filtres sur les AP :

- GUI Web
- CLI

Ce document explique comment utiliser des listes de contrôle d'accès afin de configurer des filtres via l'interface utilisateur graphique.

Note: Pour plus d'informations sur la configuration via l'utilisation de l'interface de ligne de commande, reportez-vous à l'article <u>Exemple de configuration de filtre de liste de contrôle</u> <u>d'accès de point d'accès</u> Cisco.

Configuration

Cette section décrit comment configurer des filtres basés sur ACL sur les points d'accès Cisco Aironet à l'aide de l'interface utilisateur graphique.

Où créer des listes de contrôle d'accès

Accédez à Security > Advance Security. Sélectionnez l'onglet Liste d'accès à l'association, puis cliquez sur Définir le filtre :

cisco	
Security Admin Access	Hostname Autonomous
SSID Manager	Security Summary
Server Manager AP Authentication	Username Read-Only
Intrusion Detection Local RADIUS Server	Cisco 🗸
Advance Security	Service Set Identifiers (SSIDs) SSID VLAN BandSelect Radio BSSID/Guest Mode
.ı ı.ı ı. cısco	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENT LOG
Security	AUTHENTICATION
Admin Access Encryption Manager	Hostname Autonomous
SSID Manager Server Manager	Security: Advanced Security- Association Access List
AP Autoentication Intrusion Detection Local RADIUS Server Advance Security	Filter client association with MAC address access list:

Filtres d'adresses MAC

Vous pouvez utiliser des filtres basés sur les adresses MAC afin de filtrer les périphériques clients en fonction de l'adresse MAC codée en dur. Quand un client se voit refuser l'accès par un filtre basé sur l'adresse MAC, il ne peut pas s'associer à l'AP. Les filtres d'adresses MAC permettent ou interdisent le transfert de paquets de monodiffusion et de multidiffusion envoyés depuis des adresses MAC spécifiques ou adressés à ces adresses.

Cet exemple montre comment configurer un filtre basé sur MAC via l'interface utilisateur graphique afin de filtrer le client avec l'adresse MAC **0040.96a5.b5d4** :

1. Créez l'adresse MAC ACL 700. Cette ACL ne permet pas au client 0040.96a5.b5d4 de s'associer à l'AP.

ululu cisco	HOME NETWORK ASSOCIATION WIRELESS SECURITY SERVICES SOFTWARE EVENT LOG	Sage Configuration Bing Logout Bafne									
Security		ETHERTYPE FILTERS									
Admin Access	Hostname Autonomous	Autonomous uptime is 4 weeks, 16 hours, 6 minutes									
Encryption Manager SSID Manager	Services: Filters - MAC Address Filters										
Server Nanager AP Authentication	Creata/Edit Filter Index: < NEW > •										
Local RADIUS Server Advance Security	Filter Index: 700 (700-799)										
	Add MAC Address: 0040.9655.5543 Mesk: 0000.0000 0000 Action: Block x Add (H4844.H484.44844) 044444 H4844										
	Default Action: None -										
	Filters Classes:										
	- Delete Class										
		Apply Delete Cancel									

- 2. Cliquez sur Add afin d'ajouter ce filtre aux classes de filtres. Vous pouvez également définir l'action par défaut Forward All ou Deny All.
- 3. Cliquez sur Apply. ACL 700 est maintenant créé.
- 4. Afin d'appliquer **la liste de contrôle d'accès 700** à une interface radio, accédez à la section **Appliquer les filtres**. Vous pouvez maintenant appliquer cette liste de contrôle d'accès à une interface radio ou GigabitEthernet entrante ou sortante.

rity	APPLY FR.T	ERS	MAC ADDRESS FILTERS	II IPFL	TERS II	ETHERTYPE PLTERS						
Admin Access Encryption Manager SSID Manager Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	lindane luterene					Autonomous uptin	ne is 4 weeks, 16 hours, 11 n					
	Services: Filters - Apply Filters											
		Radio	0-802.11N ^{2.4GHz}	Radi	io1-802.11N ^{SGHz}	Gig	GigabitEthernet0					
	Incoming	MAC	< NONE >	MAC	< NONE >	MAC	< NONE > .					
		EtherType	<none></none>	EtherType	< NONE > *	EtherType	< NONE > .					
		IP	< NONE > •	IP	<none> •</none>	P	< NONE >					
	Outgoing	MAC	< NONE > .	MAC	<none> *</none>	MAC	< NONE > x					
		EtherType	< NONE >	EtherType	< NONE >	EtherType	< NONE > .					
		IP	< NONE > .	IP	< NONE > .	P	< NONE > .					
							Apply					

Filtres IP

Vous pouvez utiliser des listes de contrôle d'accès standard ou étendues afin d'autoriser ou de refuser l'entrée de périphériques clients dans le réseau WLAN en fonction de l'adresse IP du client.

Cet exemple de configuration utilise des listes de contrôle d'accès étendues. La liste de contrôle d'accès étendue doit autoriser l'accès Telnet aux clients. Vous devez restreindre tous les autres protocoles sur le réseau WLAN. En outre, les clients utilisent DHCP afin d'obtenir l'adresse IP. Vous devez créer une liste de contrôle d'accès étendue qui :

- permet le trafic DHCP et Telnet ;
- refuse tous les autres types de trafic.

Complétez ces étapes afin de le créer :

1. Nommez le filtre et sélectionnez **Bloquer tout** dans la liste déroulante **Action par défaut**, car le trafic restant doit être bloqué :

	HOME NETWORK ASSOCIATION	WIRLISS SECURITY SERVICE	S SOFTWARE EVENTLOG	Saige Lon	ngunation Find redore Fam
Security	APPLY FILTERS	1 NAC ADDRESS FILTERS	IP FILTERS	ETHERTYPE FILTERS	
Admin Access Encryption Manager SSID Manager Server Manager AP Authentication Intrusion Detaction Local RADIUS Server Advance Security	Services: Filters - IP Filters			Autonomous uptime i	s 4 weeks, 16 hours, 14 minutes
	Create/Edit Filter Name:	< NEW > •			
	Filter Name: Default Action:	Allow_DHCP_Telnet			
	IP Address				
	Destination Address: Source Address:	0.0.0.0	Mosk: 0.0.0 Mosk: 265.255.255		
				Action:	Forward Add
	IP Protocol				
	IP Protocol:	thentication Header Photocol (51)	×	Action:	Forward Add

2. Sélectionnez Telnet dans la liste déroulante **Port TCP** et **client BOOTP** & **serveur BOOTP** dans la liste **déroulante Port UDP** :

cisco	HOME	NETWORK	ASSOCIATION	WIRELESS	SECURITY	SERVICES	SOFTWARE	EVENTLOG	Salfa	Comparison ging	rogont Rewo
Security Admin Access Encryption Manager SSID Monager Server Manager AP Authentication Intrusion Detection Local RADIUS Server Advance Security	P	Protocol:	 A Cu 	thentication He dom	ader Protocol	(51) 1-255)			Action:	Forward •	Add
	rc	P/TCP Port	 Telnet Custor 	(23)	(0-665	1			Action:	Forward	Add
	æ	OP Port:	 Boots Custor 	rap Protocol (B	OOTP) server	(67) 535)	•		Action:	Forward	Add
		ters Classes CP port: Teinet DP port: Boots CP port: Boots efsuit - Block /	(23) - Forward trep Protocol (B trop Protocol (I)	00TP) client (6 00TP) senser ((8) - Forward 7) - Forward				Delete Class	Apply: De	lete Cancel

3. Cliquez sur Apply. Le filtre IP **Allow_DHCP ?_Telnet** est maintenant créé et vous pouvez appliquer cette liste de contrôle d'accès à une interface radio ou GigabitEthernet entrante ou sortante.

uluulu cisco	HOME NETWOR		WIRELESS SECURITY	SERVICES SOFTWARE	EVENTLOG	Sa	e Configuration Eing Logout Befred						
Security	APPI	YFLTERS	I MAC ADDRESS FI		IP FILTERS	ETHERTYPE PLTER	8						
Admin Access	Hostname Auto	Hostname Autonomous autonomous uptime is 4 weeks, 16 hours, 25 minutes											
Encryption Manager SSID Manager	Services: Fil	Services: Filters - Apply Filters											
Server Manager			Radio0-802.11N ^{2.4GHz}		Radio1-802.11NSGHz		GigabitEthernet0						
AP Authentication Intrusion Detection	Incoming	MAC	< NONE > m	MAC	< NONE >	MAC	< NONE >						
Local RADIUS Server		EtherType	< NONE > m	EtherType	< NONE > 💌	EtherType	< NONE > .						
		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 Gencel						

Filtres Ethertype

Vous pouvez utiliser des filtres Ethertype afin de bloquer le trafic IPX (Internetwork Packet Exchange) sur le point d'accès Cisco Aironet. Une situation typique dans laquelle cela est utile est lorsque les diffusions de serveur IPX étouffent la liaison sans fil, ce qui se produit parfois sur un réseau de grande entreprise.

Complétez ces étapes afin de configurer et d'appliquer un filtre qui bloque le trafic IPX :

- 1. Cliquez sur l'onglet Ethertype Filters.
- 2. Dans le champ **Index de filtre**, nommez le filtre avec un nombre compris entre 200 et 299. Le numéro que vous attribuez crée une liste de contrôle d'accès pour le filtre.
- 3. Entrez 8137 dans le champ Ajouter un type d'Ethernet.
- 4. Laissez le masque de l'Ethernet dans le champ Masque à la valeur par défaut.
- 5. Sélectionnez **Bloquer** dans le menu d'action, puis cliquez sur **Ajouter**.

urity	APPLY FILTERS	H MAC ADDR	ESS FILTERS	ĺ.	IP FILTERS	ETHERTYPE FILTERS	
nin Access	Hostname Autonomous					Autonomous uptim	e is 4 weeks, 16 hours, 35 minute
yption Manager	F	-					
Manager	Services: Filters - EtherTyp	e Fillers					
er Manager	Create/Edit Filter Index:	4	: NEW > 💌				
usion Detection							
I RADIUS Server	Filter Index:	200	(200-299)				
Idvance Security			- Lass and				
	Add EtherType:	8137		Mark: 0	000	Action: Black	
	Non Calci (Jbc.	0.07		magnin [CEEP.	Headen Chock	× (***
		(04999)		10	Perre)		
	Default Action:	Nees					
		TRATIN E					
	Filters Classes:						
	EtherType: 8137 Mask: 000	- Flack					
	Default - None	British					
			- Dekat	te Class			

6. Afin de supprimer l'Ethernet de la liste Classes de filtres, sélectionnez-le, puis cliquez sur Supprimer la classe. Répétez les étapes précédentes et ajoutez les types 8138, 00ff et 00e0 au filtre. Vous pouvez maintenant appliquer cette liste de contrôle d'accès à une interface radio ou GigabitEthernet entrante ou sortante.

սիսիս								Say	e Configuration	jing Logout Befreah			
CISCO	HOME NETWOR	ASSOCIATION	WDELESS SEC	UKITY SERVICES	SOFTWARE	EVENTLOG							
Security	APPL	YFILTERS	MAC ADD	RESS FILTERS	Ye	IP FILTERS	Ý	ETHERTYPE FILTERS	1				
Admin Access	Hostname Autonomous uptime is 4 weeks, 16 hours, 37 minutes												
Encryption Manager													
SSID Manager	Services: Filters - Apply Filters												
Server Manager AP Authentication Intrusion Detection			Radio0.802.11N ^{2.4GR}			Radio1-802.11N ^{5GHz}			GigabitEthernet	0			
	Incoming	MAC	< NONE > •		MAC	< NONE > •		MAC	< NONE > •				
Local RADIUS Server		EtherType	< NONE > IN		EtherType	< NONE > (m)		EtherType	< NONE > .				
		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 >				
								_					
										Apply Cancel			

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.