ACL pro Benutzer mit Wireless LAN-Controllern und Konfigurationsbeispiel für Cisco Secure ACS

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Netzwerkdiagramm Konfigurieren Konfigurieren des Wireless LAN-Controllers Erstellen eines VLAN für die Wireless-Benutzer Konfigurieren des WLC für die Authentifizierung mit Cisco Secure ACS Erstellen eines neuen WLAN für Wireless-Benutzer Definieren der ACLs für die Benutzer Konfigurieren des Cisco Secure ACS-Servers Konfigurieren des Wireless LAN-Controllers als AAA-Client auf dem Cisco Secure ACS Konfigurieren von Benutzern und Benutzerprofil auf dem Cisco Secure ACS Überprüfung Fehlerbehebung **Tipps zur Fehlerbehebung** Zugehörige Informationen

Einleitung

In diesem Dokument wird anhand eines Beispiels erläutert, wie Zugriffskontrolllisten (ACLs) für die WLCs erstellt und auf Benutzer angewendet werden, die von der RADIUS-Autorisierung abhängig sind.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

 Grundkenntnisse der Konfiguration eines Cisco Secure ACS-Servers zur Authentifizierung von Wireless-Clients

- Kenntnis der Konfiguration von Cisco Aironet Lightweight Access Points (LAPs) und Cisco Wireless LAN Controllern (WLCs)
- Kenntnisse der Cisco Unified Wireless Security-Lösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Wireless LAN Controller der Serie 4400 mit Version 5.0.148.0
- Cisco Aironet Lightweight Access Points (LAPs) der Serie 1231
- Cisco Aironet 802.11 a/b/g Cisco Wireless LAN-Client-Adapter mit Version 3.6
- Cisco Aironet Desktop Utility Version 3.6
- Cisco Secure ACS Server Version 4.1
- Cisco Integrated Services Router der Serie 2800 mit IOS[®] Version 12.4(11)T
- Cisco Catalyst Switch der Serie 2900XL mit Version 12.0(5)WC3b

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.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Die Zugriffskontrollliste pro Benutzer (ACL) ist Teil des Cisco Identity Networking. Die Cisco Wireless LAN-Lösung unterstützt Identitätsnetzwerke, die es dem Netzwerk ermöglichen, eine einzelne SSID anzukündigen, es bestimmten Benutzern aber auch ermöglichen, je nach ihren Benutzerprofilen unterschiedliche Richtlinien zu erben.

Die Funktion für benutzerspezifische ACLs ermöglicht die Anwendung einer auf dem Wireless LAN Controller konfigurierten ACL auf einen Benutzer, der auf der RADIUS-Autorisierung basiert. Dies wird mithilfe des anbieterspezifischen Attributs (VSA) für die ASA-ACL-Name erreicht.

Dieses Attribut gibt den ACL-Namen an, der auf den Client angewendet werden soll. Wenn das ACL-Attribut im RADIUS Access Accept vorhanden ist, wendet das System den ACL-Namen nach der Authentifizierung auf die Client-Station an. Dadurch werden alle der Schnittstelle zugewiesenen ACLs außer Kraft gesetzt. Er ignoriert die zugewiesene Schnittstelle-ACL und wendet die neue an.

Im Folgenden finden Sie eine Zusammenfassung des Attributformats "ACL-Name". Die Felder werden von links nach rechts übertragen.

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
+	+	+	+ - •	+	+	+	+	+	+	+ - +	+ - +	+-+	+-+	+ - +	+ - +	+ - +	+-+	⊢ — +	+-+	+	+ - +	+ - +	⊢ — +	+	+ - +	+ - +	+-+	⊢ — +	+-+	++	⊦-+

	Туре	Length		Vend	dor-Id			
+-+-+	-+-+-+-+-+-+	-+-+-+-+-+-+-	+-+-+-+-	-+-+-+	+-+-+-	-+-+-	+-+-+	
	Vendor-Id (c	ont.)	Vendor f	type	Vendoi	c len	gth	
+-+-+	-+-+-+-+-+	-+-+-+-+-+-+-	+-+-+-+-	-+-+-+	+-+-+-	-+-+-	+-+-+	
	ACL Name	•••						
+-+-+	+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-	-+-+-+-+-+-						
• Typ	be - 26 for V	endor-Specific						
• Ler	ngth - >7							
• Ver	ndor-Id - 141	79						
• Ver	ndor type – 6							
• Ver	ndor length -	>0						
• Val Tł	lue – A strin Ne string is	g that includes case sensitive.	the name	of the	ACL to	use	for the	client.

Weitere Informationen zum Cisco Unified Wireless Network Identity Networking finden Sie im Abschnitt Konfigurieren von Identitätsnetzwerken im Dokument Konfigurieren von Sicherheitslösungen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

In dieser Konfiguration werden die Wireless LAN Controller WLC und LAP verwendet, um Wireless-Services für die Benutzer in Abteilung A und Abteilung B bereitzustellen. Alle Wireless-Benutzer verwenden eine gemeinsame WLAN-Niederlassung (SSID), um auf das Netzwerk zuzugreifen, und befinden sich im VLAN Office-VLAN.



Der Cisco Secure ACS-Server dient zur Authentifizierung von Wireless-Benutzern. Die EAP-Authentifizierung dient zur Authentifizierung von Benutzern. Der WLC-, LAP- und Cisco Secure ACS-Server sind wie gezeigt mit einem Layer-2-Switch verbunden.

Router R1 verbindet die Server auf der kabelgebundenen Seite wie gezeigt über den Layer-2-Switch. Router R1 fungiert auch als DHCP-Server, der Wireless-Clients IP-Adressen aus Subnetz 172.16.0.0/16 zur Verfügung stellt.

Sie müssen die Geräte so konfigurieren, dass dies geschieht:

Benutzer1 aus Abteilung A hat nur Zugriff auf Server 172.16.1.100

Benutzer2 aus Abteilung B hat nur Zugriff auf Server 172.16.1.50

Um dies zu erreichen, müssen Sie im WLC zwei ACLs erstellen: eine für User1 und die andere für User2. Nachdem die ACLs erstellt wurden, müssen Sie den Cisco Secure ACS-Server so konfigurieren, dass das ACL-Namensattribut nach erfolgreicher Authentifizierung des Wireless-Benutzers an den WLC zurückgegeben wird. Der WLC wendet dann die ACL auf den Benutzer an, sodass der Zugriff auf das Netzwerk je nach Benutzerprofil eingeschränkt wird.

Hinweis: Dieses Dokument verwendet die LEAP-Authentifizierung zur Benutzerauthentifizierung. Cisco LEAP ist anfällig für Wörterbuchangriffe. In Echtzeit-Netzwerken sollten sicherere Authentifizierungsmethoden wie EAP FAST verwendet werden. Da im Dokument die Konfiguration der benutzerspezifischen ACL-Funktion im Mittelpunkt steht, wird LEAP zur Vereinfachung verwendet.

Der nächste Abschnitt enthält eine schrittweise Anleitung zum Konfigurieren der Geräte für diese Konfiguration.

Konfigurieren

Bevor Sie die Funktion für benutzerspezifische ACLs konfigurieren, müssen Sie den WLC für den Basisbetrieb konfigurieren und die LAPs beim WLC registrieren. In diesem Dokument wird davon ausgegangen, dass der WLC für den Basisbetrieb konfiguriert ist und dass die LAPs beim WLC registriert sind. Wenn Sie ein neuer Benutzer sind, der versucht, den WLC für den Basisbetrieb mit LAPs einzurichten, finden Sie weitere Informationen unter Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Führen Sie nach der Registrierung der LAPs die folgenden Schritte aus, um die Geräte für diese Einrichtung zu konfigurieren:

- 1. Konfigurieren Sie den Wireless LAN-Controller.
- 2. Konfigurieren Sie den Cisco Secure ACS-Server.
- 3. Überprüfen Sie die Konfiguration.

Hinweis: In diesem Dokument wird die erforderliche Wireless-Konfiguration beschrieben. Im Dokument wird davon ausgegangen, dass die kabelgebundene Konfiguration vorhanden ist.

Konfigurieren des Wireless LAN-Controllers

Gehen Sie auf dem Wireless LAN Controller wie folgt vor:

- Erstellen Sie ein VLAN für die Wireless-Benutzer.
- Konfigurieren Sie den WLC für die Authentifizierung von Wireless-Benutzern mit Cisco Secure ACS.
- Erstellen Sie ein neues WLAN für die Wireless-Benutzer.
- Definieren Sie die ACLs für die Wireless-Benutzer.

Erstellen eines VLAN für die Wireless-Benutzer

Führen Sie die folgenden Schritte aus, um ein VLAN für die Wireless-Benutzer zu erstellen.

- Rufen Sie die WLC-GUI auf, und wählen Sie Controller > Interfaces (Controller > Schnittstellen) aus. Das Fenster Schnittstellen wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten Schnittstellen aufgeführt.
- 2. Klicken Sie auf Neu, um eine neue dynamische Schnittstelle zu erstellen.
- Geben Sie im Fenster Interfaces > New (Schnittstellen > Neu) den Schnittstellennamen und die VLAN-ID ein. Klicken Sie anschließend auf Übernehmen. In diesem Beispiel wird die dynamische Schnittstelle Office-VLAN und die VLAN-ID 20 zugewiesen.

🖸 • 🗇 • 🖻 🗟 🏠 🔎	🕈 🕘 🎅	- & G				2823838383838				9 - 8 ×
iliilii cisco	MONITOR	WLANS		WIRELESS	SECURITY	MANAGEMENT	Saya C C <u>O</u> MMANDS	onfiguration HELP	Ping Logou	rt <u>R</u> efresh
Controller	Interface	s > New						< 8.a	ck A	pply
Controller General Inventory Interfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protacol QoS CDP	Interface Interface VLAN Id	s > New Nome 0 2	ffice-VLAN 0					< Ba	ck As	pply

4. Geben Sie im Fenster Schnittstellen > Bearbeiten die IP-Adresse, die Subnetzmaske und das Standard-Gateway für die dynamische Schnittstelle ein. Weisen Sie ihn einem physischen Port des WLC zu, und geben Sie die IP-Adresse des DHCP-Servers ein. Klicken Sie anschließend auf Übernehmen.

cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	Saya C COMMANDS	onfiguration <u>P</u> ing Logout <u>R</u> efres HELP
CISCO Controller General Inventory Interfaces Internal DHCP Server Mobility Management Ports Master Controller Mode Network Time Protocol QOS CDP	MONITOR WLANS Interfaces > Edit General Informatio Interface Name MAC Address Interface Address Interface Address VLAN Identifier IP Address Netmask Gateway Physical Informatio Port Number Configuration	CONTROLLER an Office-V 00:0b:0 20 172 255 172 00 1 255 172 00 1 255 172 00 1 1 1 1 1 1 1 1 1 1 1 1 1	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	KELP
	DHCP Information Primary DHCP Serve Secondary DHCP Serve Access Control List ACL Name Note: Changing the Intel temporaryly disabled an some clients.	r 177 nver nor t mface parameters d thus mey result	ne 💌 s causes the Wi] LANS to be nectivity for			

In diesem Beispiel werden diese Parameter für die Office-VLAN-Schnittstelle verwendet: $_{\tt Office-VLAN}$

```
IP address: 172.16.1.25
Netmask: 255.255.0.0
Default gateway: 172.16.1.75 (sub-interface on Router R1)
Port on WLC: 1
DHCP server: 172.16.1.75
```

Konfigurieren des WLC für die Authentifizierung mit Cisco Secure ACS

Der WLC muss konfiguriert werden, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server (in diesem Fall Cisco Secure ACS) weiterzuleiten. Der RADIUS-Server validiert die Benutzeranmeldeinformationen und gibt das ACL-Namensattribut nach erfolgreicher Authentifizierung des Wireless-Benutzers an den WLC zurück.

Gehen Sie wie folgt vor, um den WLC für den RADIUS-Server zu konfigurieren:

- 1. Wählen Sie **Sicherheit** und **RADIUS Authentication (RADIUS-Authentifizierung)** in der Controller-GUI aus, um die Seite **RADIUS-Authentifizierungsserver** anzuzeigen. Klicken Sie anschließend auf **Neu**, um einen RADIUS-Server zu definieren.
- Definieren Sie die RADIUS-Serverparameter auf der Seite RADIUS Authentication Servers > New (RADIUS-Authentifizierungsserver > Neu). Zu diesen Parametern gehören die IP-Adresse des RADIUS-Servers, der Shared Secret, die Portnummer und der Serverstatus.

cisco	MONITOR WLANS CON	Sage Configuration Bing Logout Befre ROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Security	RADIUS Authentication	Servers > New < Back Apply
Security AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Usors MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Priority Order Access Control Lists IPSec Certs Wireless Protection Policies Wireless Protection Policies	RADIUS Authentication Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Retransmit Timeout Network User Management IPSec	Servers > New C Back Apply

 Die Kontrollkästchen Netzwerkbenutzer und -verwaltung bestimmen, ob die RADIUSbasierte Authentifizierung für Verwaltungs- und Netzwerkbenutzer gilt. In diesem Beispiel wird Cisco Secure ACS als RADIUS-Server mit der IP-Adresse 10.77.244.196 verwendet. Klicken Sie auf Apply (Anwenden).

Erstellen eines neuen WLAN für Wireless-Benutzer

Als Nächstes müssen Sie ein WLAN erstellen, mit dem die Wireless-Benutzer eine Verbindung herstellen können. Gehen Sie wie folgt vor, um ein neues WLAN zu erstellen:

- 1. Klicken Sie in der GUI des Wireless LAN-Controllers auf **WLANs**. Auf dieser Seite werden die WLANs aufgelistet, die auf dem Controller vorhanden sind.
- Wählen Sie Neu, um ein neues WLAN zu erstellen. Geben Sie die WLAN-ID, den Profilnamen und die WLAN-SSID f
 ür das WLAN ein, und klicken Sie auf Apply. Erstellen Sie f
 ür diese Konfiguration ein WLAN Office.

🖸 • 😳 • 🖻 🖻 🐔 .	A 🛧 🙆 🔕 🖗 -				al experience		HERE BEER BEER	🧗 – 8 ×
ululu cisco	MONITOR MLANS		WIRELESS	SECURITY	MANAGEMENT	Sage C COMMANDS	onfiguration Bin HELP	g i Logout <u>R</u> efresh
WLANs	WLANs > New						< Back	Apply
VLANS	WLAN ID	1 1						
AP Groups VLAN	Profile Name	Office						
	WLAN SSID	Office						
							1	

3. Sobald Sie ein neues WLAN erstellt haben, wird die Seite WLAN > Bearbeiten für das neue WLAN angezeigt. Auf dieser Seite können Sie verschiedene Parameter für dieses WLAN definieren, die allgemeine Richtlinien, Sicherheit, QoS und erweiterte Parameter enthalten.

cisco	Sa <u>v</u> e Configuration <u>B</u> ing Logout Be MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP
VLANS VLANS WLANS AP Groups VLAN	WLANS CONTROLLER WLENS SECURITY MEMAGEMENT COMMANDS HED WLANS > Edit Back Apply General Security QoS Advanced Profile Name Office WLAN SSID Office MLAN SSID Office WLAN SSID Office WLAN SSID Office WLAN SSID Office WLAN SSID Office <t< td=""></t<>
	Foot Notes I CKUP is not supported by 10xx model APs 3 M-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MPP is not active unless WPA2 is configured

Überprüfen Sie den **WLAN-Status** unter Allgemeine Richtlinien, um das WLAN zu aktivieren. Wählen Sie die entsprechende Schnittstelle aus dem Dropdown-Menü aus. Verwenden Sie in diesem Beispiel die Schnittstelle **Office-vlan**. Die anderen Parameter auf dieser Seite können je nach Anforderung des WLAN-Netzwerks geändert werden.

4. Wählen Sie die Registerkarte Sicherheit aus. Wählen Sie 802.1x aus dem Security-Dropdown-Menü für Layer 2 aus (da es sich um eine LEAP-Authentifizierung handelt). Wählen Sie unter 802.1x-Parametern die entsprechende WEP-Schlüssellänge aus.

Ns	WLANs > Edit < Bac	k Apply
	General Security QoS Advanced	
LANS /LANS P Groups VLAN	Layer 2 Layer 3 AAA Servers	
	Layer 2 Security 802.1X	
	802.1X Parameters	
	602-11 Data Encryption Type Key Size	
	I CKIP is not supported by 10xx model APs	
	3 II-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to res	set excluded client
	5 Client MFP is not active unless WPA2 is configured	

5. Wählen Sie auf der Registerkarte Sicherheit die Unterregisterkarte **AAA-Server** aus. Wählen Sie den AAA-Server aus, der zur Authentifizierung von Wireless-Clients verwendet wird. Verwenden Sie in diesem Beispiel den ACS-Server 10.77.244.196, um Wireless-Clients zu authentifizieren.



6. Wählen Sie die Registerkarte Erweitert aus. Aktivieren Sie AAA Override zulassen, um die Überschreibung von Benutzerrichtlinien über AAA in einem Wireless-LAN zu konfigurieren.

cisco	Saye Configuration Eing Logout Be MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS WLANS WLANS AP Groups VLAN	WLANs > Edit <back< td=""> Apply General Security QoS Advanced Allow AAA Override Imabled DHCP H-REAP Local Switching * Enabled DHCP Aironet IE Imabled DHCP Addr. Assignment Required Diagnostic Channel Enabled DHCP Addr. Assignment Required Override Interface ACL None Imabled Infrastructure MEP Imabled Client Exclusion * Imabled Merecut Value (secs) MFP Client Protection * Optional * Optional *</back<>
	Foot Notes 1 CKIP is not supported by 10xx model APs 3 H-REAP Local Switching is not supported with IPsec, CRANITE and FORTRESS authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MPP is not active unless WPA2 is configured

Wenn AAA-override aktiviert ist und ein Client AAA- und Cisco Wireless LAN-Controller-Authentifizierungsparameter in Konflikt miteinander bringt, wird die Client-Authentifizierung vom AAA-Server durchgeführt. Im Rahmen dieser Authentifizierung verschiebt das Betriebssystem Clients vom Standard-WLAN-VLAN der Cisco Wireless LAN-Lösung zu einem VLAN, das vom AAA-Server zurückgegeben und in der Schnittstellenkonfiguration des Cisco Wireless LAN-Controllers vordefiniert ist. Dies geschieht nur bei der Konfiguration für MAC-Filterung, 802.1X und/oder WPA-Betrieb. In allen Fällen verwendet das Betriebssystem außerdem QoS-, DSCP-, 802.1p-Prioritäts-Tag-Werte und die vom AAA-Server bereitgestellte ACL, sofern diese in der Schnittstellenkonfiguration des Cisco Wireless LAN-Controllers vordefiniert sind.

7. Wählen Sie die anderen Parameter basierend auf den Netzwerkanforderungen aus. Klicken Sie auf **Apply** (Anwenden).

Definieren der ACLs für die Benutzer

Für diese Konfiguration müssen zwei ACLs erstellt werden:

- ACL1: Nur 172.16.1.100, um Zugriff auf Benutzer1 für den Server bereitzustellen
- ACL2: Nur 172.16.1.50, um Zugriff auf Benutzer2 für den Server bereitzustellen

Gehen Sie wie folgt vor, um die ACLs auf dem WLC zu konfigurieren:

 Wählen Sie in der WLC-GUI Security > Access Control Lists (Sicherheit > Zugriffskontrolllisten) aus. Die Seite Zugriffskontrolllisten wird angezeigt. Auf dieser Seite werden die auf dem WLC konfigurierten ACLs aufgelistet. Außerdem können Sie ACLs bearbeiten oder entfernen. Klicken Sie zum Erstellen einer neuen Zugriffskontrollliste auf Neu.

- 2. Auf dieser Seite können Sie neue Zugriffskontrolllisten erstellen. Geben Sie den Namen der Zugriffskontrollliste ein, und klicken Sie auf **Übernehmen**. Wenn die ACL erstellt wurde, klicken Sie auf **Bearbeiten**, um Regeln für die ACL zu erstellen.
- Benutzer1 muss nur auf Server 172.16.1.100 zugreifen können und muss keinen Zugriff auf alle anderen Geräte haben. Dazu müssen Sie diese Regeln definieren.Weitere Informationen zur Konfiguration von Zugriffskontrolllisten auf Wireless LAN-Controllern finden Sie im <u>Konfigurationsbeispiel</u> für<u>ACLs</u> unter<u>Konfigurationsbeispiel</u> für<u>Wireless LAN-</u> Controller.

cisco	MONE	TOR W	LANS CONTR	OLLE	R WIRELESS	SE	CURITY M	ANAGEMENT	Saya C COMMANDS	onfiguration HELP	Eing	.ogout <u>R</u> i	
Security	Acce	ss Con	trol Lists > E	dit					< 8	ack	Add Nev	Rule	
General	Gene	ral											
RADIUS Authentication	Access	i List Nam	ve User1	L									
Accounting + TACACS+	Seq	Action	Source IP/M	urce IP/Mask Destination			Protocol	Source Port	Dest Port	DSCP	Direction	on	
Local Net Users MAC Filtering	٦	Permit	172.16.0.0 255.255.0.0	1	172.16.1.100 255.255.255.255	1	Any	Any	Any	Any	Inbound		
Disabled Clients User Login Policies AP Policies	2	Permit	172.16.1.100 255.255.255.2	55	172.16.0.0 255.255.0.0	′	Any	Any	Απγ	Any	Outbound	۵	
Local EAP	L												
Priority Order													
Access Control Lists Access Control Lists CPU Access Control Lists													
IPSec Certs													
Wireless Protection Policies													
Web Auth													
CIDS													

4. Ebenso müssen Sie eine ACL für User2 erstellen, die nur User2-Zugriff auf Server 172.16.1.50 zulässt. Dies ist die für Benutzer2 erforderliche ACL.

Control Lists > Edi Name User2 In Source IP/Mas it 172.16.0.0 255.255.0.0 it 172.16.1.50 255.255.255.255.255	it / /	Destination IP/Mask 172.16.1.50 255.255.255.255 172.16.0.0 255.255.0.0	/ ; /	Protocol Any Any	Source Port Any Any	Cest Port Any Any	k DSCP Any Any	Add New Direction Inbound Outbound	e Rule
Name User2 an Source IP/Mas 172.16.0.0 255.255.0.0 it 172.16.1.50 255.255.255.255.255	k / /	Destination 1P/Nask 172.16.1.50 255.255.255.255 172.16.0.0 255.255.0.0	/	Protocol Any Any	Source Port Any Any	Dest Port Any Any	DSCP Any Any	Direction Inbound Outbound	0
Name User2 00 Source IP/Nas 172.16.0.0 255.255.0.0 172.16.1.50 255.255.255.255	k /	Destination IP/Mask 172.16.1.50 255.255.255.255 172.16.0.0 255.255.0.0	/	Protocol Any Any	Source Port Any Any	Dest Port Any Any	DSCP Any Any	Direction Inbound Outbound	0
an Source IP/Mas 172.16.0.0 255.255.0.0 172.16.1.50 255.255.255.255	k /	Destination IP/Mask 172.16.1.50 255.255.255.255 172.16.0.0 255.255.0.0	/	Protocol Any Any	Source Port Any Any	Dest Port Any Ány	DSCP Any Any	Direction Inbound Outbound	0
it 172.16.0.0 255.255.0.0 172.16.1.50 it 255.255.255.255	/	172.16.1.50 255.255.255.255 172.16.0.0 255.255.0.0	/	Any Any	Ατιγ Ατιγ	Απγ Απγ	Απγ Απγ	Inbound Outbound	•
iit 172-16-1.50 255-255-255-255	1	172.16.0.0 255.255.0.0	'	Any	Any	Αογ	Any	Outbound	
	eless I AN (eless LAN Cor	eless LAN Controller fü	eless LAN Controller für d	eless LAN Controller für diese E	eless LAN Controller für diese Einrichtur	eless LAN Controller für diese Einrichtung konfigu	eless I AN Controller für diese Finrichtung konfiguriert	eless I AN Controller für diese Einrichtung konfiguriert. Der n

Sie haben jetzt den Wireless LAN Controller für diese Einrichtung konfiguriert. Der nächste Schritt besteht in der Konfiguration des Cisco Secure Access Control-Servers zur Authentifizierung der Wireless-Clients und der Rückgabe des ACL Name-Attributs an den WLC nach erfolgreicher Authentifizierung.

Konfigurieren des Cisco Secure ACS-Servers

Damit der Cisco Secure ACS Wireless-Clients authentifizieren kann, müssen Sie die folgenden Schritte ausführen:

- Konfigurieren Sie den Wireless LAN Controller auf dem Cisco Secure ACS als AAA-Client.
- Konfigurieren Sie die Benutzer und Benutzerprofile auf dem Cisco Secure ACS.

Konfigurieren des Wireless LAN-Controllers als AAA-Client auf dem Cisco Secure ACS

Gehen Sie wie folgt vor, um den Wireless LAN Controller auf dem Cisco Secure ACS als AAA-Client zu konfigurieren:

 Klicken Sie auf Netzwerkkonfiguration > AAA-Client hinzufügen. Die Seite AAA-Client hinzufügen wird angezeigt. Definieren Sie auf dieser Seite den WLC-Systemnamen, die IP-Adresse der Verwaltungsschnittstelle, den gemeinsamen geheimen Schlüssel und die Authentifizierung mithilfe der Radius-Schnittstelle. Hier ein Beispiel:

Cisco Systems	Network Configuration	×
	Edit	Help
User Setup Setup Setup Setup Setup Setup Setur Configuration System Configuration	Add AAA Client Hostname wlc AAA Client IP Address 10.77.244.210 Shared Secret Cisco	AAA Client Hesthame AAA Client Hesthame Shared Secret Network Device Group BADIUS Key Wran Authenticate Using Single Cennert TACACS - AAA Client Log Update/Watchdeg Pathets from this AAA Client Log Update/Watchdeg Pathets from this AAA Client Log Update/Watchdeg Pathets from this AAA Client Log RADIUS Transfer Pathets from this AAA Client Beplace RADIUS Part info with Username from this AAA Client Match Framewith P-Address with user IP addre for second for a with user IP
Administration Centrel Databases Pestere Validation Validation Profile:	RADIUS Key Wrap Key Encryption Key Message Authenticator Code Key Key Input Format O ASCII @ Hexadecimal Authenticate Using RADIUS (Cisco Airespace)	AAA Client Hestname The AAA Client Hostname is the name assigned to the AAA client. [Back to Tee]
Activity Dedine Documentation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	AAA Client IP Address
	Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client Match Framed-IP-Address with user IP address for accounting packets from this AAA Client Submit Submit + Apply Cancel	If you want to designate more than one AAA client with a single AAA client entry in ACB, you can specify the IP address for each AAA client to be represented by this AAA client to be represented by this AAA client to be represented by this AAA client to be represented by the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the set of the Enter.
	P Back to Help	You can use the vildcard asterisk (*) for an octet in the IP address. For example, if you vant every AAA clent in your 192,160,13,1

Hinweis: Der auf dem Cisco Secure ACS konfigurierte geheime Schlüssel muss mit dem auf dem WLC unter **RADIUS Authentication Servers > New** konfigurierten gemeinsamen geheimen Schlüssel übereinstimmen.

2. Klicken Sie auf Senden+Übernehmen.

Konfigurieren von Benutzern und Benutzerprofil auf dem Cisco Secure ACS

Gehen Sie wie folgt vor, um Benutzer auf dem Cisco Secure ACS zu konfigurieren:

 Wählen Sie User Setup (Benutzereinrichtung) aus der ACS-GUI aus, geben Sie den Benutzernamen ein, und klicken Sie auf Hinzufügen/Bearbeiten. In diesem Beispiel ist der Benutzer User1.



 Wenn die Seite User Setup (Benutzereinrichtung) angezeigt wird, definieren Sie alle f
ür den Benutzer spezifischen Parameter. In diesem Beispiel werden Benutzername, Kennwort, Zus
ätzliche Benutzerinformationen und die RADIUS-Attribute konfiguriert, da Sie nur diese Parameter f
ür die EAP-Authentifizierung ben
ötigen.

Cisco Systems	User Setup	×
adhaadhaa	Edit	Help
User Setup	User: UserA (New User)	Account Disabled Deletina a Usernane Supernentary User Info
Shared Profile Components	Account Disabled	Password Authentication Group to which the user is assigned Calback
Network Configuration	Supplementary User Info	Client IP Address Assignment Advanced Settings Network Access Restrictions
Configuration	Description	Max Sessions Mage Oustas Account Disable Downloadable ACLs
Administration Centrel	User Setup	Advanced TACACS= Settings TACACS+ Enable Control TACACS+ Enable Parsword TACACS+ Until Parsword TACACS+ Outbound Parsword
Pestere Validation	Password Authentication: ACS Internal Database	InCACS + Shell Command Authorization Command Authorization for Network Device Hanagement Applications TACACS + Unknown Services IET BADIUS Attributes
Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	RADUS Yeador-Specific Attailutes
Activity	Confirm	Account Disabled Status
Documentation	Password Separate (CHAP/MS-CHAP/ARAP)	Select the Account Disabled check box to disable this account; clear the check how to enable the account.
	Password	[Back to Tap]
	Password	Deleting a Username
	When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token carbino is enabled	The Deltte button appears only when you are adding an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete . When asked to confirm your action, click DK .
		[Back to Top]
	Group to which the user is assigned:	Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information boves that appear. To add or change fields, click Interface

Blättern Sie nach unten, bis die für den Benutzer spezifischen Cisco Airespace RADIUS-Attribute angezeigt werden. Aktivieren Sie den **Aire-ACL-Namen**, damit der ACS den ACL-Namen zusammen mit der erfolgreichen Authentifizierungsantwort an den WLC zurückgeben kann. Erstellen Sie für User1 eine ACL User1 auf dem WLC. Geben Sie den ACL-Namen als Benutzer1

ein.

😋 • 😒 • 💽 🗐	🏟 🖍 🔅 🗢 🗔 - 🌭 🗖	🥂 – 8 ×
Cisco Systems	User Setup	X
	Date exceeds:	Help
User Setup Setup Setup Setup Setup Setup Seture Components Retwork Configuration Set Configuration Set Configuration	Sep 9 2007 Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Clisce Alirespace RADIUS Attributes (141794002) Aitr-QoS-Level Bronze	Account Disabled Deleting a Username Supplementary User Info Pansword Authentication Group to which the user is assigned Calback Calb
Network Access Profile:	00	ILIT HADDUS Attributes RADUS Yeador-Specific Attributes
Online Documentation	0 [14179'005] Aize-Interface-Name	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account.
	V [14179/006] Aire-Acl-Name User1	[Rack to Tep] Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click DK.
	P Back to Help	[Back to Tap] Supplementary liser lafa
	Submit Cancel	Type the applicable information in any supplemental user information boses that appear. To add or chance fields, click laterface

3. Wiederholen Sie die gleiche Prozedur, um User2 zu erstellen, wie hier gezeigt.

Cisco Systems	User Setup					
-dlb-dlb-	Select	Help				
User Stared Profile Shared Profile </th <th>Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISS List all users Remove Dynamic Users 2 bek to Help</th> <th> Help Person and a factor of these Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person Rationant Rationant Rationants Person Rationant Rationants Person Rationant Rationant Rationants Person Rationants Person Rationants Person Rationant Rationants Person Rationants<!--</th--></th>	Select User: User2 Find Add/Edit List users beginning with letter/number: ABCPEFSSIIVYXXII QIIIISSIIVYXXII QIIIISS List all users Remove Dynamic Users 2 bek to Help	 Help Person and a factor of these Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rationant Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person a factor of the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person ACS and the ACS Internal Rational Rationants Person Rationant Rationant Rationants Person Rationant Rationants Person Rationant Rationant Rationants Person Rationants Person Rationants Person Rationant Rationants Person Rationants<!--</th-->				
0 · O · E E ·	 A ≠ € ⊗ 5 B 	🕅 - 5 ×				
Cisco Systems	User Setup	×				
adbad ba	Edit	Help E				
User Setup Group Setup Setup Setup Setup Setup Setup Configuration Setup Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	User: UserA (New User) Account Disabled Supplementary User Info Real Name User2 Description User Setup Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-	Account Disabled Beletima a Distributed Supplementary User Info Supplementary User Info Destroard Authentication Comp to which the user is assigned Calback Client IP Address Assignment Advanced Settings Network Access Restrictions Max Sessions Unage Quetas Network Access Restrictions Max Sessions Disable Aftact Advanced TACACS - Settings TACACS - Inable Password TACACS - Inable Password TACACS - Undersmod Password TACACS - RADIUS Attributes				
Reports and Activity Documentation	Password Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password Confirm Password Confirm Password When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled. Group to which the user is assigned: Submit Cancel	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [hack to Tee] Deleting a Username The Delete buttos appears only when you are editing as existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When added to certifing your action, click OK. [hack to Tee] Supplementary User Info Type the applicable information in any supplemental user information				

🔕 • 🕗 • 🖻 🖻	🏠 🖉 🕸 🕘 🎯 🖏 🖬	🦓 – 8 ×
Cisco Systems	User Setup	X
-dbdb	Date exceeds:	Help
User Setup Graup Setup Setup Setup Matwork Configuration Retwork Configuration Suptem Configuration	Sep 9 2007 Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit Clisce Alirespace RADIUS Attributes	Account Disabled Beforting a Uvernmen Supplementary Uver Info Descentary Uver Info Descent PL Address Assignment Client IP Address Assignment Advanced Settings Natural Settings Natural Settings Disag Durits Account Disable Developedat Account Disable Developedate Account Disable Developedate Account Disable TACACS - Enable Passured TACACS - Enable Passured TACACS - Enable Passured
Postare Validation Wetwork Access Profile:	[14179402] Aire-QoS-Level Bronze [14179403] Aire-DSCP [0	TACACS - Shell Command Authorization Economical Authorization for Network Device Hanagement Applications TACACS - Unknown Services I ETT RADBUS Athibutes RABBUS Yeador-Specific Athibutes
Reports and Activity Documentation	[14179404] Aire-802.1P-Tag [0 [14179405] Aire-Interface-Name	Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account. [Rack to Tao]
(User2	Deleting a Uremane The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the database, click Delete. When asked to confirm your action, click DK.
	2 Back to Malp	[Back to Tap] Supplementary User Info
	Submit Cancel	Type the applicable information in any supplemental user information benefits that answer. To add or channe fields, click interface

4. Klicken Sie auf Systemkonfiguration und Globales Authentifizierungs-Setup, um sicherzustellen, dass der Authentifizierungsserver so konfiguriert ist, dass er die gewünschte EAP-Authentifizierungsmethode ausführt. Wählen Sie unter den EAP-Konfigurationseinstellungen die entsprechende EAP-Methode aus. In diesem Beispiel wird die LEAP-Authentifizierung verwendet. Klicken Sie abschließend auf Senden.

0·0·2 2	合 🖓 🙊 🗵 🖏 🖪	M - 8 ×
Cisco Systems	System Configuration	X
	PEAP	Help
User	L Allow EAP-MSCHAPv2	
Clascop	Allow EAP-GTC	Use this page to specify settings for various authentication protocols.
Graup Setup	C Allow Posture Validation	EAD Configuration
Shared Profile	C Allow EAO-TLS	• EAP-FAST
- Icontrasto	Select one or more of the following options:	• EAP-TLS
Configuration	E Cartificate SAN comparison	• EAP-H05
Stad Sectors		AP SAP Request Timest
Configuration	M Certificate CN comparison	<u>MS-CHIP Configuration</u>
Interface	H Certificate Binary comparison	
Configuration	EAP-TLS session timeout (minutes): 120	
Administration Centrel		EAP Configuration
a L Febread Here	Cisco client initial message:	EAD is a flexible request-response protocol for arbitrary
91 Databases	PEAP session timeout (minutes): 120	authentication information (RFC 2204). EAP is layered on tap of another protocol such as UDP, 802.1x or RADIUS and supports
manal Pestare	Feable Fact Deconnect:	multiple "authentication" types.
Const Antennen	enable rast Reconnect.	[Back to Top]
Profilez	FAD-FAST	BEAD.
CR 1 Report and	EAP-EAST Configuration	PERF
Activity		PEAP is the euter layer protocel for the secure tunnel.
and 1 Online	EAP-TLS	
Documentation	Allow EAP-TLS	Notes IEAP is a certificate-based authentication protect. IEAP
	Select one or more of the following options:	to the ACS Certificate Setup page.
	R Certificate SAN comparison	· Allow FADALITHAD - Line to seable FAD-MICHAD - while his DEAD
	F Certificate CN comparison	authentication. Enable this protocol for any repository that supports MS-
	F Certificate Binary comparison	CHAPV2, such as Microsoft AD, and the ACS Internal Database.
	EAP-TLS session timeout (minutes): 120	 Allow EAP-GTC — Use to enable EAP-GTC within Ciscs PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
-	LEAP	Allow Restore Voldation - Use to scale at other (CAD / AD / TO)
\subseteq	Allow LEAP (For Aironet only)	 Answer Percent and a den - One to enable the PERP (EAP'TEV) protocol for posture validation of Network Admission Control (NAC) clients.
	Submit Submit + Restart Cancel	Allow EAP-TLS - Use to enable the EAP-TLS protocol as an additional inner method for PEAP. The PEAP/EAP-TLS feature strength lowerpage the existing T

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Versuchen Sie, einen Wireless-Client mit dem Lightweight AP der LEAP-Authentifizierung zu verknüpfen, um zu überprüfen, ob die Konfiguration wie erwartet funktioniert.

Hinweis: In diesem Dokument wird davon ausgegangen, dass das Clientprofil für die LEAP-Authentifizierung konfiguriert ist. Weitere Informationen zur Konfiguration des 802.11a/b/g-Wireless-Client-Adapters für die LEAP-Authentifizierung finden Sie unter <u>Verwenden der EAP-</u> <u>Authentifizierung</u>.

Wenn das Profil für den Wireless-Client aktiviert ist, wird der Benutzer aufgefordert, den Benutzernamen/das Kennwort für die LEAP-Authentifizierung einzugeben. Dies geschieht, wenn Benutzer1 versucht, sich bei der LAP zu authentifizieren.

Enter Wireless Network Password			
Please enter your LEAP username and password to log on to the wireless network			
User Name :	User1		
Password :	•••••		
Log on to :			
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter		
Profile Name :	Office OK Cancel		

Der Lightweight Access Point und anschließend der WLC geben die

Benutzeranmeldeinformationen an den externen RADIUS-Server (Cisco Secure ACS) weiter, um die Anmeldeinformationen zu validieren. Der RADIUS-Server vergleicht die Daten mit der Benutzerdatenbank und gibt nach erfolgreicher Authentifizierung den für den Benutzer konfigurierten ACL-Namen an den WLC zurück. In diesem Fall wird der ACL User1 an den WLC zurückgegeben.

Cisco Aironet Desktop Utility	y - Current Profile: Office	-TSWEB	2×
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
authumuthu Profile Name:	Office-TSWEB		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 64	
Server Based Authentication:	LEAP	Data Encryption: WEP	
IP Address:	172.16.0.14		
Signal Strength:		Excellent	
		Advanced	

Der Wireless LAN Controller wendet diese Zugriffskontrollliste auf Benutzer 1 an. Diese Ping-Ausgabe zeigt, dass User1 nur auf Server 172.16.1.100 zugreifen kann, aber nicht auf ein anderes Gerät.

D:\Documents and Settings\Administrator>ping 172.16.1.100 Pinging 172.16.1.100 with 32 bytes of data: Reply from 172.16.1.100: bytes=32 time=3ms TTL=255 Reply from 172.16.1.100: bytes=32 time=1ms TTL=255 Reply from 172.16.1.100: bytes=32 time=1ms TTL=255 Reply from 172.16.1.100: bytes=32 time=1ms TTL=255 Ping statistics for 172.16.1.100: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 3ms, Average = 1ms D:\Documents and Settings\Administrator>ping 172.16.1.50 Pinging 172.16.1.50 with 32 bytes of data: Request timed out. Request timed out. Request timed out. Request timed out. Ping statistics for 172.16.1.50: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Wenn User2 versucht, auf das WLAN zuzugreifen, gibt der RADIUS-Server nach erfolgreicher Authentifizierung die ACL User2 an den WLC zurück.

Enter Wireless N	etwork Password 🗙
Please enter your L network	EAP username and password to log on to the wireless
User Name :	User2
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11 a/b/g Wireless Adapter
Profile Name :	Office
	OK Cancel

AP Authentication Status	<u></u> :
Card Name: Cisco Aironet 802.1	1a/b/g Wireless Adapter
Profile Name: Office-TSWEB	
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Skipped because the domain name was not configured
r S⊦	now minimized next time (Cancel)

Der Wireless LAN Controller wendet diese Zugriffskontrollliste auf Benutzer 2 an. Diese Ping-Ausgabe zeigt, dass User2 nur auf Server 172.16.1.50 zugreifen kann, aber nicht auf ein anderes Gerät.

```
D:\Documents and Settings\Administrator>ping 172.16.1.50
Pinging 172.16.1.50 with 32 bytes of data:
Reply from 172.16.1.50: bytes=32 time=3ms TTL=255
Reply from 172.16.1.50: bytes=32 time=18ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Reply from 172.16.1.50: bytes=32 time=1ms TTL=255
Ping statistics for 172.16.1.50:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 18ms, Average = 5ms
D:\Documents and Settings\Administrator>ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 172.16.1.100:
   Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Auf dem Wireless LAN Controller können Sie diese Debugbefehle auch verwenden, um Fehler bei der AAA-Authentifizierung zu beheben.

• debug aaa all enable - Konfiguriert das Debuggen aller AAA-Nachrichten

- debug dot1x packet enable: Aktiviert das Debuggen aller dot1x-Pakete
- debug client <MAC-Adresse> Aktiviert das Debuggen von Wireless-Clients

Im Folgenden finden Sie ein Beispiel für den Befehl debug aaa all enable

Hinweis: Einige der Zeilen in der Ausgabe wurden aufgrund von Platzhaltern auf die zweite Zeile verschoben.

Thu Aug 16 14:42:54 2007: AuthenticationReguest: 0xblab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228 protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: Thu Aug 16 14:42:54 2007:

 Thu Aug 16 14:42:54 2007:
 proxyState.....00:40:96:AF:3E:93-03:01

 Thu Aug 16 14:42:54 2007:
 Packet contains 16 AVPs (not shown)

 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 01 00 d0 2d 34 f5 99 b4 19 27 28 eb 5f 35 9c-4.....'(._5. Thu Aug 16 14:42:54 2007: 00000010: 8f a9 00 dd 01 07 75 73 65 72 31 1f 13 30 30 2duser1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office-TSWEB.. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1aM....wlc. Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c..... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 13 40 06 00 = @ . . Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 00 06 51 04 32 30 4f 27 02Q.200'. Thu Aug 16 14:42:54 2007: 00000090: 01 00 25 11 01 00 18 1d 87 9d 0b f9 dd e5 39 0d Thu Aug 16 14:42:54 2007: 000000a0: 2e 82 eb 17 c6 23 b7 96 dc c3 55 ff 7c 51 4e 75 Thu Aug 16 14:42:54 2007: 000000b0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000c0: 1a d5 3b 35 5e 93 11 c0 c6 2f 5e f5 65 e9 3e 2d ..;5[^]..../[^].e.>-Thu Aug 16 14:42:54 2007: 00000000: 0b 01 00 36 8c 31 6a b4 27 e6 d4 0e 1b 8e 5d 19 ...6.1j.'....]. Thu Aug 16 14:42:54 2007: 00000010: 60 lc c2 16 4f 06 03 01 00 04 18 0a 53 56 43 3d Thu Aug 16 14:42:54 2007: 00000020: 30 2e 31 3b 50 12 6c fb 90 ec 48 9b fb d7 ce ca 0.1;P.1...H.... Thu Aug 16 14:42:54 2007: 00000030: 3b 64 93 10 fe 09 ;d.... Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=11 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=11 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....104 resultCode.....255 Thu Aug 16 14:42:54 2007: Thu Aug 16 14:42:54 2007: protocolUsed.....0x0000001 Thu Aug 16 14:42:54 2007: proxyState.... 00:40:96:AF:3E:93-03:01

Thu Aug 16 14:42:54 2007: Packet contains 3 AVPs (not shown) Thu Aug 16 14:42:54 2007: AuthenticationRequest: 0xblab104 Thu Aug 16 14:42:54 2007: Callback.....0x85ed228 Thu Aug 16 14:42:54 2007: protocolType.....0x00140001 Thu Aug 16 14:42:54 2007: proxyState..... 00:40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 16 AVPs (not shown) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Successful transmission of Authentication Packet (id 2) to 10.77.244.196:1812, proxy state 00:40:96:af:3e:93-00:00 Thu Aug 16 14:42:54 2007: 00000000: 01 02 00 c0 38 b6 b2 20 ff 5b f2 16 64 df 02 618....[..d..a Thu Aug 16 14:42:54 2007: 00000010: cf f5 93 4b 01 07 75 73 65 72 31 1f 13 30 30 2d ...K..User1..00-Thu Aug 16 14:42:54 2007: 00000020: 34 30 2d 39 36 2d 41 46 2d 33 45 2d 39 33 1e 20 40-96-AF-3E-93.. Thu Aug 16 14:42:54 2007: 00000030: 30 30 2d 30 42 2d 38 35 2d 35 42 2d 46 42 2d 44 00-0B-85-5B-FB-D Thu Aug 16 14:42:54 2007: 00000040: 30 3a 4f 66 66 69 63 65 2d 54 53 57 45 42 05 06 0:Office.. Thu Aug 16 14:42:54 2007: 00000050: 00 00 01 04 06 0a 4d f4 d2 20 05 77 6c 63 1aM....wlc. Thu Aug 16 14:42:54 2007: 00000060: 0c 00 00 37 63 01 06 00 00 01 06 06 00 00 00 ...7c.... Thu Aug 16 14:42:54 2007: 00000070: 02 0c 06 00 00 05 14 3d 06 00 00 01 13 40 06 00 = @ . . Thu Aug 16 14:42:54 2007: 0000080: 00 00 0d 41 06 00 00 06 51 04 32 30 4f 17 01 ...A....Q.200.. Thu Aug 16 14:42:54 2007: 00000090: 01 00 15 11 01 00 08 0f 14 05 65 1b 28 61 c9 75e.(a.u Thu Aug 16 14:42:54 2007: 000000a0: 73 65 72 31 18 0a 53 56 43 3d 30 2e 31 3b 50 12 ser1..SVC=0.1;P. Thu Aug 16 14:42:54 2007: 000000b0: 05 ba 6b af fe a4 b0 d1 a2 94 f8 39 80 ca 3c 96 Thu Aug 16 14:42:54 2007: 00000000: 02 02 00 ce c9 3d 5d c8 6c 07 8e fb 58 84 8d f6=].1...X... Thu Aug 16 14:42:54 2007: 00000010: 33 6d 93 21 08 06 ff ff ff ff 4f 27 02 01 00 25 3m.!...8 Thu Aug 16 14:42:54 2007: 00000020: 11 01 00 18 e5 e5 31 1e 33 b5 4e 69 90 e7 84 25% Thu Aug 16 14:42:54 2007: 00000030: 42 a9 20 ac 84 33 9f 87 ca dc c9 b3 75 73 65 72 B....3....user Thu Aug 16 14:42:54 2007: 00000040: 31 1a 3b 00 00 00 09 01 35 6c 65 61 70 3a 73 65 1.;....5leap:se Thu Aug 16 14:42:54 2007: 00000050: 73 73 69 6f 6e 2d 6b 65 79 3d 29 80 1d 2c 1c 85 ssion-key=).... Thu Aug 16 14:42:54 2007: 00000060: db 1c 29 7e 40 8a b8 93 69 2a 55 d2 e5 46 89 8b ...)~@...i*U..F.. Thu Aug 16 14:42:54 2007: 00000070: 2c 3b 65 49 3e 44 cf 7e 95 29 47 54 1a 1f 00 00 ,;eI>D.~.)GT.... Thu Aug 16 14:42:54 2007: 0000080: 00 09 01 19 61 75 74 68 2d 61 6c 67 6f 2d 74 79auth-algo-ty Thu Aug 16 14:42:54 2007: 00000090: 70 65 3d 65 61 70 2d 6c 65 61 70 1a 0d 00 00 37 pe=eap-leap....7 Thu Aug 16 14:42:54 2007: 000000a0: 63 06 07 55 73 65 72 31 19 14 43 41 43 53 3a 30 c..User1..CACS:0 Thu Aug 16 14:42:54 2007: 000000b0: 2f 39 2f 61 34 64 66 34 64 32 2f 31 50 12 9a 71 /9/a4df4d2/1P..q Thu Aug 16 14:42:54 2007: 000000c0: 09 99 7d 74 89 ad af e5 c8 b1 71 94 97 d1 ..}t....q... Thu Aug 16 14:42:54 2007: ****Enter processIncomingMessages: response code=2 Thu Aug 16 14:42:54 2007: ****Enter processRadiusResponse: response code=2 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93

Access-Accept received from RADIUS server

10.77.244.196 for mobile 00:40:96:af:3e:93 receiveId = 3 Thu Aug 16 14:42:54 2007: AuthorizationResponse: 0x9c27800 Thu Aug 16 14:42:54 2007: structureSize.....236 Thu Aug 16 14:42:54 2007: resultCode.....0 Thu Aug 16 14:42:54 2007: protocolUsed.....0x0 0000001 Thu Aug 16 14:42:54 2007: proxyState.....00: 40:96:AF:3E:93-03:02 Thu Aug 16 14:42:54 2007: Packet contains 6 AVPs: Thu Aug 16 14:42:54 2007: AVP[01] Framed-IP-Address.....0xffffffff (-1) (4 bytes) Thu Aug 16 14:42:54 2007: AVP[02] EAP-Message.....DATA (37 bytes) Thu Aug 16 14:42:54 2007: AVP[03] Cisco / LEAP-Session-Key...DATA (16 bytes) Thu Aug 16 14:42:54 2007: AVP[04] Airespace / ACL-Name.....User1 (5 bytes) Thu Aug 16 14:42:54 2007: AVP[05] Class.....CACS:0/9/a4df4d2/1 (18 bytes) Thu Aug 16 14:42:54 2007: AVP[06] Message-Authenticator.....DATA (16 bytes) Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Applying new AAA override for station 00:40:96:af:3e:93 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Override values for station 00:40:96:af:3e:93 source: 4, valid bits: 0x400 gosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName:User1 Thu Aug 16 14:42:54 2007: 00:40:96:af:3e:93 Inserting new RADIUS override into chain for station 00:40:96:af:3e:93

Sie können den Befehl **show wlan summary** verwenden, um zu erkennen, welches Ihrer WLANs RADIUS-Serverauthentifizierung verwendet. Anschließend können Sie den Befehl **show client summary** anzeigen, um festzustellen, welche MAC-Adressen (Clients) in den RADIUS-WLANs erfolgreich authentifiziert wurden. Sie können dies auch mit den von Cisco Secure ACS begangenen Versuchen oder fehlgeschlagenen Protokollen korrelieren.

Cisco empfiehlt, die ACL-Konfigurationen mit einem Wireless-Client zu testen, um sicherzustellen, dass Sie sie korrekt konfiguriert haben. Wenn sie nicht ordnungsgemäß funktionieren, überprüfen Sie die ACLs auf der ACL-Webseite und überprüfen Sie, ob Ihre ACL-Änderungen auf die Schnittstelle des Controllers angewendet wurden.

Sie können die folgenden Befehle auch verwenden, um Ihre Konfiguration zu überprüfen:

 show acl summary - Um die auf dem Controller konfigurierten ACLs anzuzeigen, verwenden Sie den Befehl show acl summary.

Hier ein Beispiel:

(Cisco	Controller)	<pre>>show acl</pre>	summary
ACL Nar	ne		Applied
User1			Yes
User2			Yes

• show acl detail <ACL_Name> —Zeigt detaillierte Informationen zu den konfigurierten ACLs

an.Hier ein Beispiel:**Hinweis:** Einige der Zeilen in der Ausgabe wurden aufgrund von Platzhaltern auf die zweite Zeile verschoben.

Cisco Controller) >show acl detailed User1

Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action __ ___ ____ _____ ____ 1 In 172.16.0.0/255.255.0.0 172.16.1.100/255.255.255.255 In 172.16.0.0/255.255.0.0 172. Any 0-65535 0-65535 Any Permit 2 Out 172.16.1.100/255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit (Cisco Controller) >show acl detailed User2 Source Destination Source Port Dest Port I Dir IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action __ ___ ____ ---- ----- ----- -----1 In 172.16.0.0/255.255.0.0 172.16.1.50/255.255.255.255 0-65535 0-65535 Any Permit Anv 2 Out 172.16.1.50/255.255.255.255 172.16.0.0/255.255.0.0 Any 0-65535 0-65535 Any Permit

 show client detail <MAC-Adresse des Clients> - Zeigt detaillierte Informationen zum Wireless-Client an.

Tipps zur Fehlerbehebung

Verwenden Sie diese Tipps zur Fehlerbehebung:

- Überprüfen Sie auf dem Controller, ob der RADIUS-Server im aktiven Zustand und nicht im Standby-Modus oder deaktiviert ist.
- Überprüfen Sie auf dem Controller, ob der RADIUS-Server im Dropdown-Menü des WLAN (SSID) ausgewählt wurde.
- Überprüfen Sie, ob der RADIUS-Server die Authentifizierungsanfrage vom Wireless-Client empfängt und validiert.
- Überprüfen Sie dazu die Berichte "Erfolgreiche Authentifizierung" und "Fehlgeschlagene Versuche" auf dem ACS-Server. Diese Berichte stehen unter "Berichte und Aktivitäten" auf dem ACS-Server zur Verfügung.

Zugehörige Informationen

- ACLs auf Wireless LAN-Controllern: Regeln, Einschränkungen und Beispiele
- Konfigurationsbeispiel für ACLs in Wireless LAN-Controllern
- Konfigurationsbeispiel f
 ür MAC-Filter mit WLCs (Wireless LAN Controller)
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 5.2
- Technischer Support und Dokumentation für Cisco Systeme