Konfigurieren von ACS 5.2 für die portbasierte Authentifizierung mit einer LAP

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Konfigurieren Netzwerkdiagramm Annahmen Konfigurationsschritte Konfigurieren von LAP Switch konfigurieren Konfigurieren des RADIUS-Servers Netzwerkressourcen konfigurieren Benutzer konfigurieren Definieren von Richtlinienelementen Zugriffsrichtlinien anwenden Überprüfung Fehlerbehebung Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie ein Lightweight Access Point (LAP) als 802.1x-Komponente konfiguriert wird, um sich gegenüber einem RADIUS-Server wie einem Zugriffssteuerungsserver (ACS) 5.2 zu authentifizieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen, bevor Sie diese Konfiguration vornehmen:

- Grundkenntnisse der Wireless LAN Controller (WLC) und LAPs
- Besitzen funktionale Kenntnisse des AAA-Servers.
- Besitzen fundierte Kenntnisse über Wireless-Netzwerke und Wireless-Sicherheitsprobleme

Verwendete Komponenten

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

- Cisco 5508 WLC mit Firmware-Version 7.0.220.0
- Cisco Serie 3502 LAP
- Cisco Secure ACS mit Version 5.2
- Cisco Switch der Serie 3560

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 unter <u>Cisco Technical Tips Conventions</u> (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

LAPs verfügen über werkseitig installierte X.509-Zertifikate, die von einem privaten Schlüssel signiert und zum Zeitpunkt der Herstellung in das Gerät eingebrannt werden. LAPs verwenden dieses Zertifikat, um sich beim Join-Prozess beim WLC zu authentifizieren. Diese Methode beschreibt eine andere Methode zur Authentifizierung von LAPs. Mit der WLC-Software können Sie die 802.1x-Authentifizierung zwischen einem Cisco Aironet Access Point (AP) und einem Cisco Switch konfigurieren. In diesem Fall fungiert der Access Point als 802.1x-Komponente und wird vom Switch über einen RADIUS-Server (ACS) authentifiziert, der EAP-FAST mit anonymer PAC-Bereitstellung verwendet. Nach der Konfiguration für die 802.1x-Authentifizierung lässt der Switch den Datenverkehr, der nicht 802.1x-Datenverkehr ist, erst über den Port zu, wenn sich das mit dem Port verbundene Gerät erfolgreich authentifiziert hat. Ein AP kann authentifiziert werden, bevor er einem WLC beitritt, oder nachdem er einem WLC beigetreten ist. In diesem Fall konfigurieren Sie 802.1x auf dem Switch, nachdem der LAP dem WLC beigetreten ist.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Nachfolgend sind die Konfigurationsdetails der in diesem Diagramm verwendeten Komponenten aufgeführt:

- Die IP-Adresse des ACS (RADIUS)-Servers lautet 192.168.150.24.
- Die Management- und AP-Manager-Schnittstellenadresse des WLC lautet 192.168.75.44.
- Die DHCP-Server-Adresse lautet 192.168.150.25.
- Die LAP wird in VLAN 253 platziert.
- VLAN 253: 192.168.153.x/24 Gateway: +192 168 153 10
- VLAN 75: 192.168.75.x/24 Gateway: 192.168.75.1

Annahmen

- Switches werden für alle Layer-3-VLANs konfiguriert.
- Dem DHCP-Server wird ein DHCP-Bereich zugewiesen.
- Zwischen allen Geräten im Netzwerk bestehen Layer-3-Verbindungen.
- Die LAP ist bereits mit dem WLC verbunden.
- Jedes VLAN hat eine /24-Maske.

• In ACS 5.2 ist ein selbstsigniertes Zertifikat installiert.

Konfigurationsschritte

Diese Konfiguration ist in drei Kategorien unterteilt:

- 1. Konfigurieren der LAP
- 2. Konfigurieren Sie den Switch.
- 3. Konfigurieren Sie den RADIUS-Server.

Konfigurieren von LAP

Annahmen:

LAP ist bereits mithilfe von Option 43, DNS, oder der statisch konfigurierten WLC-Verwaltungsschnittstellen-IP beim WLC registriert.

Führen Sie diese Schritte aus:

1. Gehen Sie zu **Wireless** > **Access Points** > **All APs**, um die LAP-Registrierung auf dem WLC zu überprüfen.

cisco	MONITOR MLANS	CONTROLLER WIRELESS SECUR	UTY MANAGEMENT	COMMANDS HELP (EE	Sag DBACK	e Configuration	Bing Logout Befred
Wireless	All APs						Entries 1 - 1 of 1
* Access Points All APe * N880c0 882.11s/n 802.11b/g/h	Current Pilter Number of APs	Anne 1	(Change B	tar] (Clear Filter)			
Clobal Configuration Advanced Mesh HREAP Groups 002.11a/n 002.11b/g/n Media Stream Country Timers P QuS	AP Name 23628	AP Rodol Alt-CAPISOIE-AHS	AP HAC cc:ef:40.fe:33:1	AP Up Time 9 1 d, 62 h 32 m 42 s	Admin Status s Enabled	Operational Status REG	Port AP Hode 13 Local

- 2. Sie haben zwei Möglichkeiten, die 802.1x-Anmeldedaten (d. h. Benutzername/Kennwort) für alle LAPs zu konfigurieren:
 - Global

Bei einem bereits verbundenen LAP können Sie die Anmeldeinformationen global festlegen, sodass jeder dem WLC beitretende LAP diese Anmeldeinformationen übernimmt.

cisco	MONITOR WLAND CONTROLLER WIRELESS SECURITY MINAGEN	State Configuration Bing Legent & ENT COMMANDS HELP FEEDBACK
eless	Global Configuration	Act
Al APs Radios 802-11a/n	COP	High Aveilability
102.13Drom Could Configuration Advanced Hesh HREAP Groups 902.11A/n 902.211A/n Hedio Stream Country	CDP State P Ethernet Interfaces CDP State 0 P 1 P 2 P 1 Radio Slot# CDP State 0 P 1 CDP State 0 P 2 P 2 P 3 P 1 CDP State 0 P 1 CDP State 1 CDP State	Air Headfloot Timesuf(1-33) [20] Local Neels Air Fest HeartBeet Timer State HirtSAP Node Air Fest HeartBeet Timer State Bit SAP Node Air Fest HeartBeet Timer State Air Primery Discovery Timesuf(35 to 3500) [123] Back-up Primery Controller 2P Address Bisck-up Primery Controller anne Back-up Secondary Controller name Back-up Secondary Controller name
iners ieS	Looin Credentials	Global TCP Adjust MSS
	lisemene Fessiond	AP Retransmit Config Parameters
	Enable Password	AP Rainerant Interval
	AP Failover Priority Gibbel AP Fellover Priority Disable AP Image Pre-download	•
	Download Primary Download Backup Interchange Image	

• Individuell

Konfigurieren von 802.1 x-Profilen pro AP In unserem Beispiel werden Anmeldeinformationen pro Access Point konfiguriert.

- a. Gehen Sie zu **Wireless** > **All APs**, und wählen Sie den betreffenden Access Point aus.
- b. Fügen Sie den Benutzernamen und das Kennwort in den Feldern für die 802.1x-Anmeldeinformationen für die Komponente hinzu.

սիսիս								Sage Configuration Eng.	Logout Exfred
CISCO	MONITOR MLANE	CONTROLLER W	UPBLASS SECURITY	MANAGEMENT	COMMINDS	HELP	RECEACE		
Wireless	All APs > Details for	r 3502e						< Beck	Apply
Access Points All APs Eddos Eddos Eddos Gottallig/in Global Carrigutation Advanced Mesh HREAP Groups Aga Jula (n	General Credentials Over-ride Gobel ore Userneme Pressuord Enable Password	sdentiols	es High Aveilability	y Enventory	Advanced				
 002.11b/g/e Media Stream Country Timers QoS 	002.1x Supplicant Cr Over-ride Global on Usersme Password Confirm Possword	edentials adentials 8502e 	q						

Hinweis: Anmeldeinformationen werden für Telnet, SSH oder die Konsole beim AP verwendet.

3. Konfigurieren Sie den Abschnitt "Hohe Verfügbarkeit", und klicken Sie auf Anwenden.

. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MIMAGEMENT COMMANDS HELP EEEDBACK	Baye Configuration Bing La	ogout Beires
Wireless	All APs > Details for 3502e	< Back	Apply
 Access Points All Ars Radios B32:11a/n B32:11a/n B32:11a/n B32:11a/n B02:11b/g/n B02:11a/g/n B02:11b/g/n Media Stream Ceantry Timers Qu5 	General Credentials Interfaces High Availability Investory Advanced Name Memo Memogeneent 3P Address Memo Memogeneent 3P Address Primary Controller Secondary Controller Secondary Controller Secondary Controller Tertiary Controller Secondary Controller Secondary Controller Secondary Controller		

Hinweis: Nach dem Speichern werden diese Anmeldeinformationen im gesamten WLC beibehalten, und der Access Point wird neu gestartet. Die Anmeldeinformationen ändern sich nur, wenn der LAP einem neuen WLC beitritt. Die LAP übernimmt den Benutzernamen und das Kennwort, die auf dem neuen WLC konfiguriert wurden.

Wenn der Access Point noch keinem WLC beigetreten ist, müssen Sie in der LAP eine Konsole einrichten, um die Anmeldeinformationen festzulegen. Geben Sie diesen CLI-Befehl im privilegierten Modus ein:

LAP#lwapp ap dot1x Benutzername <Benutzername > Kennwort <Kennwort>

Oder

LAP#capwap ap dot1x Benutzername <Benutzername > Kennwort <Kennwort>

Hinweis: Dieser Befehl steht nur für APs zur Verfügung, die das Wiederherstellungs-Image ausführen.

Der Standardbenutzername und das Standardkennwort für die LAP sind cisco und Cisco.

Switch konfigurieren

Der Switch fungiert als Authentifizierer für die LAP und authentifiziert die LAP über einen RADIUS-Server. Wenn der Switch nicht über die entsprechende Software verfügt, führen Sie ein Upgrade des Switches durch. Geben Sie in der Switch-CLI die folgenden Befehle ein, um die 802.1x-Authentifizierung an einem Switch-Port zu aktivieren:

<#root>
switch#
configure terminal
switch(config)#
dot1x system-auth-control
switch(config)#
aaa new-model
!--- Enables 802.1x on the Switch.

switch(config)#

aaa authentication dot1x default group radius

```
switch(config)#
```

radius server host 192.168.150.24 key cisco

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#

ip radius source-interface vlan 253

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast

!--- gig0/11 is the port number on which the AP is connected.

```
switch(config-if)dot1x pae authenticator
```

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.

Hinweis: Wenn sich auf demselben Switch andere APs befinden, die 802.1x nicht verwenden sollen, können Sie den Port für 802.1x entweder unkonfiguriert lassen oder den folgenden Befehl ausführen:

<#root>

switch(config-if)authentication port-control force-authorized

Konfigurieren des RADIUS-Servers

LAP wird mit EAP-FAST authentifiziert. Stellen Sie sicher, dass der verwendete RADIUS-Server diese EAP-Methode unterstützt, wenn Sie Cisco ACS 5.2 nicht verwenden.

Die Konfiguration des RADIUS-Servers ist in vier Schritte unterteilt:

- 1. Netzwerkressourcen konfigurieren
- 2. Konfigurieren Sie Benutzer.
- 3. Definieren Sie Richtlinienelemente.
- 4. Wenden Sie Zugriffsrichtlinien an.

ACS 5.x ist ein richtlinienbasierter ACS. Anders ausgedrückt: ACS 5.x verwendet ein regelbasiertes Richtlinienmodell anstelle des in Version 4.x verwendeten gruppenbasierten Modells.

Das regelbasierte ACS 5.x-Richtlinienmodell bietet im Vergleich zum älteren gruppenbasierten Ansatz eine leistungsstärkere und flexiblere Zugriffskontrolle.

Im älteren gruppenbasierten Modell definiert eine Gruppe eine Richtlinie, da sie drei Informationstypen enthält und miteinander verknüpft:

- **Identitätsinformationen** Diese Informationen können auf der Mitgliedschaft in AD- oder LDAP-Gruppen oder einer statischen Zuweisung für interne ACS-Benutzer basieren.
- Andere Einschränkungen oder Bedingungen Zeitbeschränkungen, Gerätebeschränkungen usw.
- Berechtigungen VLANs oder Cisco IOS[®]-Berechtigungsebenen

Das ACS 5.x-Richtlinienmodell basiert auf folgenden Regeln:

Wenn Bedingung dann Ergebnis

Wir verwenden z. B. die für das gruppenbasierte Modell beschriebenen Informationen:

Wenn Identität-Bedingung, Restriktionsbedingung dann Autorisierungsprofil.

Dies gibt uns die Flexibilität, die Bedingungen, unter denen der Benutzer auf das Netz zugreifen darf, und auch die Berechtigungsstufe, die erlaubt ist, wenn bestimmte Bedingungen erfüllt sind, zu begrenzen.

Netzwerkressourcen konfigurieren

In diesem Abschnitt wird der AAA-Client für den Switch auf dem RADIUS-Server konfiguriert.

In diesem Verfahren wird erläutert, wie der Switch als AAA-Client auf dem RADIUS-Server hinzugefügt wird, damit der Switch die Benutzeranmeldeinformationen der LAP an den RADIUS-Server weitergeben kann.

Führen Sie diese Schritte aus:

- 1. Klicken Sie in der ACS-GUI auf Netzwerkressourcen.
- 2. Klicken Sie auf Netzwerkgerätegruppen.
- 3. Gehen Sie zu **Location** > **Create** (unten).



4. Fügen Sie die erforderlichen Felder hinzu, und klicken Sie auf Senden.

cisco Cisco Secure A	ICS
+ 🛞 My Workspace	Network Resources > Network Device Groups > Location > Create
In the twork Resources Network Device Groups Location Device Type Notwork Devices and AAA Clients Default Network Device External RADIUS Servers	Device Group - General • Name: LAB Description: LAB Devices • Parent All Locations • Required fields
 B Users and Identity Stores 	
Policy Elements	
Access Policies	
Monitoring and Reports	
🕞 🍓 System Administration	

5. Das Fenster wird aktualisiert:

cisco Cisco Secure A	CS
🕨 🦪 My Workspace	Network Resources > Network Device Groups > Location
👻 🐙 Network Resources	Network Device Groups
Network Device Groups Location	Filter: Match if: Go 🗢
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers Susers and Identity Stores	Name Description * <u>All Locations</u> LAB LAB Devices
Policy Elements	
Access Policies	
Monitoring and Reports	
🕨 🍓 System Administration	

6. Klicken Sie auf **Gerätetyp** > **Erstellen**.

cisco Cisco Secure A	ICS
+ 🕀 My Workspace	Network Resources > Network Device Groups > Device Type > Edit "Device Type: Al Device Types: Switches
Interview Resources	
Network Device Groups Location Device Type	Bovice Group - General Boviches Description: Control and is connected
Network Devices and AAA Clients Default Network Device External RADIUS Servers	Parent All Device Types Select Select
Users and Identity Stores	
Policy Elements	
Access Policies	
Monitoring and Reports	1. 1. 1. 111. 1. 3: 1 w
🖌 🍇 System Administration	

7. Klicken Sie auf Senden. Nach Abschluss des Vorgangs wird das Fenster aktualisiert:



- 8. Gehen Sie zu Network Resources > Network Devices and AAA Clients.
- 9. Klicken Sie auf Erstellen, und geben Sie die hier abgebildeten Details ein:

cisco Cisco Secure A	ICS	accadimin SALIL ACSIS (Primary)
+ 🛃 Ny Workspace	Network Resources > Network Devices and AUA Clerks > Create	
Jyn Network Resources Network Device Groups Location Device Tirps	Name: 2500 Switch LAP Description: Switch where LAP is connected Network Device Groups	
Defour Network Device	Location Al Locations LAB	Select
External RADIUS Servers	Device Type All Device Types Switches	Select
B Users and Identity Stores Q: Policy Elements C, Access Policies Si Nontaring and Reports	P Address P Single P Address C IP Range(s) • IP: [102:163.153.10	Authentication Options
 Ng System Administration 	R = Read of Salar	CoApert 1700

10. Klicken Sie auf Senden. Das Fenster wird aktualisiert:

cisco Cisco Secure A	cs	ecandren SALE AC
+ 💮 My Workspace	Network Resources > Network Devices and AAA Clents	
- La Network Resources	Retwork Devices	Showin
Network Device Groups Location	Filter: Vilatch if. V Go V	
Network Devices and AMACIENTS	Rame + IP/Mask NDGLacation NDGDevice Type	Description
Detaut Network Device External BADIUE Servers	3550-Switch-LAP 192 166 153 10/32 All Locations:LAB All Device Types:Switch	hes Switch where LAP is connected
+ 🎒 Lisers and identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports		
* 🍓 System Administration		

Benutzer konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie einen Benutzer auf dem zuvor konfigurierten ACS erstellen. Sie weisen den Benutzer einer Gruppe mit der Bezeichnung "LAP-Benutzer" zu.

Führen Sie diese Schritte aus:

1. Gehen Sie zu **Benutzer und Identitätsdaten** > **Identitätsgruppen** > **Erstellen**.



2. Klicken Sie auf Senden.



- 3. Erstellen Sie **3502e**, und weisen Sie es der Gruppe "LAP-Benutzer" zu.
- 4. Gehen Sie zu **Benutzer und Identitätsdaten** > **Identitätsgruppen** > **Benutzer** > **Erstellen**.

cisco Cisco Secure Ad	cs
► 🔆 My Workspace	Users and identity Stores > internal identity Stores > Users > Create
► 👸 Network Resources	Canada
🔹 🚳 Users and Identity Stores	o Name: 3502e Status: Enabled - 6
Identity Groups	Description: LAP 3502e in vian 253
Users	Identity Group: All Groups:LAP users Select
Fosts External Identity Stores Certificate Authonities Certificate Authonities Identity Store Sequences	Password Information Password must Contain 4 - 32 characters
Policy Elements	Password:
Access Policies	O Confirm Password
 Monitoring and Reports 	Change password on next login
► 🍓 System Administration	User Information There are no additional identity attributes defined for user records I = Required fields

5. Die aktualisierten Informationen werden angezeigt:



Definieren von Richtlinienelementen

Überprüfen Sie, ob Zugriffsberechtigung festgelegt ist.

cisco Cisco Secure A	CS
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and identity Stores	Elter - Match #
🗸 🗞 Policy Elements	
Session Conditions Authorization and Permissions	Name Description Permit Access
 Network Access Authorization Profiles 	
 Device Administration Named Permission Objects 	
+ 🔂 Access Policies	
► 🔝 Monitoring and Reports	
🕨 🍓 System Administration	

Zugriffsrichtlinien anwenden

In diesem Abschnitt wählen Sie EAP-FAST als Authentifizierungsmethode für LAPs für die Authentifizierung aus. Anschließend erstellen Sie Regeln, die auf den vorherigen Schritten basieren.

Führen Sie diese Schritte aus:

1. Gehen Sie zu Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Bearbeiten: ''Standard-Netzwerkzugriff''.



2. Stellen Sie sicher, dass Sie die EAP-FAST- und die anonyme In-Band-PAC-Bereitstellung aktiviert haben.





- 3. Klicken Sie auf Senden.
- 4. Überprüfen Sie die ausgewählte Identitätsgruppe. Verwenden Sie in diesem Beispiel **Internal Users** (die auf dem ACS erstellt wurde), und speichern Sie die Änderungen.

cisco Cisco Secure A	ecaninin SAL
 My Workspace 	Access Policies > Access Services > Default Network Access > Identity
 Br Network Resources 	Gingle result selection C Rule based result selection
+ 🐉 Users and Identity Stores	Mentity Source: Internal Users Select
Policy Elements	* Literard Cettons
🖌 🅵 Access Policies	it authentication failed React
Access Services Service Selection Rules O Detault Device Admin	If user notifound Reject
O Default Network Access	Note: For authemications using FEAP, LEAP, EAP-PAST or RADIUS MSCHAP it is not possible to continue processing when authemication fails or user is not found. If continue option is selected in these cases, requests will
Authorization	be rejected
 Identifying and Reports 	
 System Administration 	

5. Gehen Sie zu Access Policies > Access Services > Default Network Access > Authorization, um das Autorisierungsprofil zu überprüfen.

Sie können festlegen, unter welchen Bedingungen Sie einem Benutzer Zugriff auf das Netzwerk gewähren und welches Autorisierungsprofil (Attribute) Sie nach der Authentifizierung weitergeben. Diese Granularität ist nur in ACS 5.x verfügbar. In diesem Beispiel werden Location, **Device Type**, **Protocol**, **Identity Group** und **EAP Authentication Method** ausgewählt.



- 6. Klicken Sie auf **OK**, und **speichern Sie die Änderungen**.
- 7. Der nächste Schritt ist das Erstellen einer Regel. Wenn keine Regeln definiert sind, wird LAP der Zugriff ohne Bedingungen gewährt.
- 8. Klicken Sie auf Erstellen > Regel-1. Diese Regel ist für Benutzer in der Gruppe "LAP-Benutzer".

cisco Cisco Secure A	CS	ecandmin Si
+ 💮 My Workspace	Access Policies > Access Services > Default Velocity Access > Authorization	
+ 🎲 Network Resources	Standard Daley Evention Doley	
+ 🎎 Users and identity Stores	Mark Come Second 475 March Ender	VI
Policy Elements	Net Cace Secure ALS - Morals Tunnes	×
- 🕵 Access Policies	Filly 192.168.150.24 https://192.168.150.24/acsadmin/PolicyInputAction.do	<u> </u>
Monitoring and Reports		
Nel System Administration	Conditions	
	MDGLocation: In MILlocations:LAB Select	
	MDG Device Type: In All Device Types Switches Select	
	M Protocol: Manon Kapus Select	b
	Fine 6 the statute Matter ANK	۲
	Results Furtholization Profiles: Furtholization profile: Furtholization Furtholization profile: Furtholization Furtholization	65 frs1
	OK Cancel	Help
	T Default If no rules defined or no enabled rule matches.	
	Create I Duplicate I Edit Delete A Nove to V	
	O	
	Save Changes Discard Changes	

9. Klicken Sie auf Änderungen speichern. Wenn Benutzer, die nicht den Bedingungen entsprechen, abgelehnt werden sollen, ändern Sie die Standardregel so, dass "Zugriff verweigern" angezeigt wird.

cisco Cisco Secure A	C8	udmin SAUX-ACSO(Primary) Log Dur About the
► - Ny Werkspace	Access Psicies > Access Services > Default lietwork Access > Authorization	
» (5) Network Resources	Etandent Balant Excention Online	
· 🗿 Uoers and Identity Stores	Statement Automatical Printing	
Policy Elements	Site Contra antione into a Contra a Contra a Contra a	
• 🐁 Access Policies	Her Baus • Wath It House • Enabled • Case Her Go •	
Access Services Service Selection Rules @ Default Device Admin	Status Non-Location NOS Device Type Protocol Martinity Group Eth ID Sule::1 in All Locations LAB in All Device Types Diviticities match Radus in All Croups LAP users #	Results Hi Sp Authentication Method Authorization Profiles Hi MDP Permit Access 0
Contain Network Access		
	4	
	Dataut If no ruleo defined or no enabled rule matches.	Permit Access
	Create_i = Dusisate_i = ERI Defete A Move to V Save Changes Discard Changes	Custoria: HitCount

10. Der letzte Schritt besteht in der Definition von Serviceauswahlregeln. Auf dieser Seite können Sie eine einfache oder regelbasierte Richtlinie konfigurieren, um zu bestimmen, welcher Service auf eingehende Anfragen angewendet werden soll. Beispiele:

cisco Cisco Secure AC	s							acsadmin	SAL
My Workspace My Workspace Motiver: Resources Guess and identity Etores Gy Policy Elements	Access Pokies > Access Benkes > Service Selection Rules Single result selection Service Selection Policy Filter Stakes V Natch & Equals V Enabled V Clear Filter Go V								
Access Policies Constant Policies Constant Policies Constant Policies Constant Policies Constant Policies Identity Authorization Monitoling and Reports System Administration	1 2		Status 0 0	Name Rule-1 Rule-2	Conditions Protocal match Radius match Tacaca	3	Results Sentce Default Network Access Default Device Admin	Hit Count 0]

Überprüfung

Sobald 802.1x auf dem Switch-Port aktiviert ist, wird der gesamte Datenverkehr über diesen Port blockiert, mit Ausnahme des 802.1x-Datenverkehrs. Die LAP, die bereits beim WLC registriert ist, wird getrennt. Erst nach einer erfolgreichen 802.1x-Authentifizierung wird der andere Datenverkehr zugelassen. Wenn die LAP erfolgreich beim WLC registriert wurde, nachdem 802.1x auf dem Switch aktiviert wurde, ist die LAP-Authentifizierung erfolgreich.

AP-Konsole:

<#root>

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11.
*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29
```

!--- Authentication is successful and the AP gets an IP.

Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
 peer_ip: 192.168.75.44 peer_port: 5246

*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN *Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan wmmAC status is FALSEged state to CFG *Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down *Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset *Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP *Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller 5508-3 *Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake. Wireless client traffic will be blocked until DTLS tunnel is established. *Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up *Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0] *Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to down *Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset *Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up *Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down *Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset *Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up *Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS keys are plumbed successfully. *Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel established. *Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled !--- AP joins the 5508-3 WLC.

ACS-Protokolle:

1. Anzeige der Trefferanzahl:

Wenn Sie Protokolle innerhalb von 15 Minuten nach der Authentifizierung überprüfen, stellen Sie sicher, dass Sie die Trefferanzahl aktualisieren. Auf derselben Seite befindet sich unten die Registerkarte **Hit Count (Trefferanzahl**).

cisco Cisco Secure Ad	CS		-	-			ace		
+ 🔆 My Workspace	Access	Policies	» Access	Services >	Service Selection Rules				
+ 🎲 Network Resources	C Single result selection 🦉 Bule based result selection								
Users and Identity Stores	Servi	Service Selection Policy							
+ 🚱 Policy Elements	Filter	: Stat	us -	Match if:	Equals - Enabled - Clear Filter	G0 -			
 Access Policies 			_	-	Conditions	 Results			
 Access Services 			Status	Name	Protocol	Service	Hit Count		
Belaut Device Admin	1			Bule-1	match Radius	Default Network Access	1		
 Ø Default Network Access 	2	Г	0	Rule-2	match Tacacs	Default Device Admin	0		
Identity Authorization									
+ 📳 Monitoring and Reports									
🔸 🍓 System Administration									

cisco Cisco Secure Al	CS cadra 140.4	CSA2(Prinnery) Lig Out About M									
 S By Workspace 	Access Peleles + Access Centrol + Cafault Network Access + Authentitation										
+ 158 Network Resources	Instant Delical Excercise Delice										
 Jusers and identity Stores 	Network Access Authorization Policy										
So Policy Elements	Filter Blakes • Blakeh if Equaits • Enabled • Great Filter Go •										
Access Services T Service Selection Rales	Name NDGLocation HDGDevice Type Protocol Mently Group Explautientication Method	Authorization Profiles Hill Count									
Orfault Device Admin	Rule-1 in All Locations: LAB in All Device Types Switches match Radius in All Groups LAP users -ANY-	Permit Access 1									
Lécolt Americanie > 21 deleterre											
 Monitoring and Reports 											
» 🍓 Dyslem Administration											
	4	л.									
	If no rules defined or no enabled rule matches.	Permit Access 0 V									
	Create. I = Duplicate. I = Edt Delete A More to.	Castornize Hit Geunt									
100	Bare Changes Discard Changes										

2. Klicken Sie auf **Überwachung und Berichte**, um ein neues Popup-Fenster zu öffnen. Klicken Sie auf **Authentifizierungen -RADIUS -Heute**. Sie können auch auf **Details** klicken, um zu überprüfen, welche Serviceauswahlregel angewendet wurde.

_ 0 0									Launch Interact	ive Waxwar 🗄
Showing Page 1	of 1				I Geto	Pager Ge				
AAA Protocol > RADIU	S Authenti	cation								
Authentication Status : Pa Date : Jan	ss or Pail wary 29, 20	12 (<u>Last 30 Mi</u>	tuba i LastH	enci Lag <u>e 12 Hours</u> (70	day i <u>Yesferdar i Last 7 Dav</u>	s (Last30.Davs.)				
Generated on January 29, 3	2012 9 15:01	PM EST								
Relati	click for deta	ila 9-mo	as over item	for additional informat	ian					
Logged At	RADUS I Status F	NAS Details	Usemame	MACIP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Go
Jan 25,12 9 11:12 566 PM	· ·	4	3502e	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-NSCHAP\2)	3590-Switch-LAP	192.168.153.10	GicablEthemet0/11	

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- <u>Cisco Secure Access Control System</u>
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

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.