Configuración de ACS 5.2 para la autenticación basada en puerto con un LAP

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados Convenciones** Antecedentes Configurar Diagrama de la red **Suposición Configuration Steps Configurar LAP** Configurar switch **Configurar servidor RADIUS** Configurar recursos de red **Configurar usuarios** Definición de elementos de política Aplicar políticas de acceso Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe cómo configurar un Lightweight Access Point (LAP) como supplicant 802.1x para autenticarse en un servidor RADIUS como un Access Control Server (ACS) 5.2.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar realizar esta configuración:

- Conocimiento básico del controlador de LAN inalámbrica (WLC) y los LAP.
- Tener conocimiento funcional del servidor AAA.
- Poseer un conocimiento profundo de las redes inalámbricas y de los problemas de seguridad inalámbrica.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

• Cisco 5508 WLC que ejecuta la versión 7.0.220.0 del firmware

- LAP de la serie 3502 de Cisco
- Cisco Secure ACS que ejecuta la versión 5.2
- Switch Cisco serie 3560

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Los LAP tienen instalados de fábrica certificados X.509 - firmados por una clave privada - que se queman en el dispositivo en el momento de la fabricación. Los LAP utilizan este certificado para autenticarse con el WLC en el proceso de unión. Este método describe otra manera de autenticar los LAPs. Con el software WLC, puede configurar la autenticación 802.1x entre un punto de acceso (AP) Cisco Aironet y un switch Cisco. En este caso, el AP actúa como el suplicante 802.1x y es autenticado por el switch contra un servidor RADIUS (ACS) que utiliza EAP-FAST con aprovisionamiento PAC anónimo. Una vez configurado para la autenticación 802.1x, el switch no permite que ningún tráfico que no sea el tráfico 802.1x pase a través del puerto hasta que el dispositivo conectado al puerto se autentique correctamente. Un AP se puede autenticar antes de que se una a un WLC o después de que se haya unido a un WLC, en cuyo caso usted configura 802.1x en el switch después de que el LAP se une al WLC.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Estos son los detalles de configuración de los componentes utilizados en este diagrama:

- La dirección IP del servidor ACS (RADIUS) es 192.168.150.24.
- La dirección de la interfaz de administración y del administrador AP del WLC es 192.168.75.44.
- Los servidores DHCP dirigen 192.168.150.25.
- LAP se coloca en VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Suposición

- Los switches se configuran para todas las VLAN de Capa 3.
- Al servidor DHCP se le asigna un ámbito DHCP.
- Existe conectividad de capa 3 entre todos los dispositivos de la red.
- El LAP ya está unido al WLC.
- Cada VLAN tiene una máscara /24.

• ACS 5.2 tiene instalado un certificado autofirmado.

Configuration Steps

Esta configuración se divide en tres categorías:

- 1. Configure el LAP.
- 2. <u>Configure el switch.</u>
- 3. Configure el servidor RADIUS.

Configurar LAP

Suposiciones

El LAP ya está registrado al WLC usando la opción 43, el DNS, o la IP estáticamente configurada de la interfaz de la administración del WLC.

Complete estos pasos:

1. Vaya a **Inalámbrico** > **Puntos de acceso** > **Todos los APs** para verificar el registro del LAP en el WLC.

 cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	Management op	24MANOS HELP (BEDBA	sak CX	e Configuration	Bing Log	put Befred
Wireless	All APs						Entries	1 - 1 of 1
	Current Filter	Rene	(Change Filte	d (Clear Riter)				
 Nadios 802.11a/n 802.11b/g/h Global Configuration 	Number of APs	1						
> Advanced	AP Name	AP Hodel	AP MAC	AP Up Time	Admin Status	Operational Statuc	Port	AP Mode
Mesh HREAP Groups	3502e	AIR-CAP3502E-A-K5	acie/;48:/a:53:19	1 d, 62 h 32 m 42 s	Enabled	REG	13	Local
▶ 802.11a/n								
▶ 902.11b/g/n								
Media Stream								
Country								
Timers								
+ Qo5								

2. Puede configurar las credenciales 802.1x (es decir, nombre de usuario/contraseña) para todos los LAP de dos maneras:

• Globalmente

Para un LAP ya unido, puede establecer las credenciales globalmente para que cada LAP que se une al WLC herede esas credenciales.

iliilii cisco	MONETOR WEARS GON	TROLLER WIRELESS SECUR	тү мауласмент	COMMANDS HELP EEED	Skyr BACK	Configuration Bing Legout B
e55	Global Configuration					Act
cess Points I APs atlos	CDP			High Availability		
102.135/0/h Robal Configuration devanced lesh REAP Groups 02.11e/n 02.135/g/m edia Stream	CDP State Ethernet Interface# 1 2 3 Rindio Slot# 0 1	IP COP State IP IP		AP Heartbest Timesur() Local Node AP Test Hear H REAP Mode AP Test He AP Primery Discovery T Back-up Primery Contro Back-up Secondary Con Back-up Secondary Con	(-33) (best Timer State cartbest Timer State (imeaul(30 to 3800) oller 3P Address oller name ntroter 19 Address ntroter me	30 Dias bis = Dias bis = 120
ountry	2 3	2		TCP MSS		
265	Login Credentials			Globel TCP Adjust MSS		
	Usemanie	[AP Retransmit Config	Parameters	
	Pessaord Bhable Password			AD Retransmit Count AD Retransmit Intercel		5
	802.1x Supplicant Cre 902.1x Authentication Usernama Password Canfirm Password	dentials				
	AP Failover Priority Gibbel AP Failover Prior	ty Diszbie 🔹				
	AP Image Pre-downlo Download Primary Interchange Image	ad Download Back				

• Individualmente

Configuración de perfiles 802.1 x por AP. En nuestro ejemplo, configuraremos las credenciales por AP.

- a. Vaya a Wireless > All APs, y seleccione el AP correspondiente.
- b. Agregue el nombre de usuario y la contraseña en los campos **802.1x Supplicant** Credentials.

alala		Sage Configuration Eng	Logout Befres
CISCO	MONETOR WLANE CONTROLLER WORLESS SECURITY MANAGEMENT COMMANDS HELP ERECRACK		
Wireless	All APs > Details for 3502e	< Beck	Apply
Access Points All APs Fados B02.118/n 002.118/n 002.118/n Obtal Carifystation Advanced Mesh HREAP Groups B02.118/n B02.118/n	General Credentials Interfaces High Availability Enventory Advanced Legis Credentials Visioname Size Visioname Size Size <td></td> <td></td>		
Media Stream Country Timers QoS	Over-ride Global ordentials (7) Username (850)e Peareont (****** Confirm Resevent (******		

Nota: Las credenciales de inicio de sesión se utilizan para Telnet, SSH o la consola en el AP.

3. Configure la sección High Availability y haga clic en Apply.

. cisco	HONITOR WLANS CONTROLLER WIRELESS SECURITY MIMAGEMENT COMMANDS HELP EEEDBACK	Bays Configuration Bing Logout Befree
Wireless	All APs > Details for 3502e	< Deck Apply
 Access Points All Ars Rodos S32.154/h S32.154/h S32.154/h Globel Configuration Advenced Mesh HREAP Groups B02.114/g B02.114/g Media Stream Country Timers Qe5 	General Credentials Interfaces High Availability Investory Advanced Name Memory Respondent UP Address Primary Castrollar Secondary Centreflar Secondary Centreflar	

Nota: Una vez guardadas, estas credenciales se retienen en el WLC y el AP se reinicia. Las credenciales cambian solamente cuando el LAP se une a un nuevo WLC. El LAP asume el nombre de usuario y la contraseña que fueron configurados en el nuevo WLC.

Si el AP aún no se ha unido a un WLC, debe iniciar la consola en el LAP para establecer las credenciales. Ejecute este comando CLI en el modo de habilitación:

LAP#lwapp ap dot1x username <username> password <password>

or

LAP#capwap ap dot1x username <username> password <password>

Nota: Este comando está disponible solamente para los AP que ejecutan la imagen de recuperación.

El nombre de usuario y la contraseña predeterminados para el LAP son cisco y Cisco, respectivamente.

Configurar switch

El switch actúa como un autenticador para el LAP y autentica el LAP contra un servidor RADIUS. Si el switch no tiene el software compatible, actualice el switch. En la CLI del switch, ejecute estos comandos para habilitar la autenticación 802.1x en un puerto del switch:

<#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)#

!--- 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.

Nota: Si tiene otros AP en el mismo switch y no desea que utilicen 802.1x, puede dejar el puerto sin configurar para 802.1x o ejecutar este comando:

<#root>

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

Configurar servidor RADIUS

El LAP se autentica con EAP-FAST. Asegúrese de que el servidor RADIUS que utiliza admite este método EAP si no utiliza Cisco ACS 5.2.

La configuración del servidor RADIUS se divide en cuatro pasos:

- 1. Configure los recursos de red.
- 2. Configurar usuarios.
- 3. Definir elementos de política.
- 4. Aplique políticas de acceso.

ACS 5.x es un ACS basado en políticas. En otras palabras, ACS 5.x utiliza un modelo de política basado en reglas en lugar del modelo basado en grupos utilizado en las versiones 4.x.

El modelo de políticas basadas en reglas ACS 5.x proporciona un control de acceso más potente y flexible

en comparación con el antiguo enfoque basado en grupos.

En el modelo basado en grupos más antiguo, un grupo define la política porque contiene y une tres tipos de información:

- **Información de identidad**: esta información puede estar basada en la pertenencia a grupos AD o LDAP o en una asignación estática para usuarios internos de ACS.
- Otras restricciones o condiciones: restricciones de tiempo, restricciones de dispositivos, etc.
- **Permisos**: VLAN o niveles de privilegio de Cisco IOS[®].

El modelo de políticas de ACS 5.x se basa en reglas con el formato:

Si la condición entonces resultado

Por ejemplo, utilizamos la información descrita para el modelo basado en grupos:

Si identity-condition, restricted-condition, authorization-profile.

Como resultado, esto nos da flexibilidad para limitar las condiciones en las que el usuario puede acceder a la red y también qué nivel de autorización se permite cuando se cumplen condiciones específicas.

Configurar recursos de red

En esta sección, configuramos el cliente AAA para el switch en el servidor RADIUS.

Este procedimiento explica cómo agregar el switch como cliente AAA en el servidor RADIUS para que el switch pueda pasar las credenciales de usuario del LAP al servidor RADIUS.

Complete estos pasos:

- 1. Desde la GUI de ACS, haga clic en Network Resources.
- 2. Haga clic en Network Device Groups.
- 3. Vaya a **Ubicación** > **Crear** (en la parte inferior).



4. Agregue los campos obligatorios y haga clic en Enviar.

cisco Cisco Secure A	Network Resources > Network Device Groups > Location > Create
An Hetwork Resources Network Device Groups Location Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers 20. Lisers and Identity Stores	Device Group - General Image: Image
Policy Elements Access Policies Monitoring and Reports System Administration	

5. La ventana se actualiza:

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	Name Description T <u>All Locations</u> All Locations
Big Users and Identity Stores	LAB LAB Devices
Sp Policy Elements	
+ 🔂 Access Policies	
Monitoring and Reports	
System Administration	

6. Haga clic en **Tipo de dispositivo** > **Crear**.

cisco Cisco Secure A	ICS	
+ 🕀 My Workspace	Network Resources > Network Device Groups > Device Type > Edit "Device	Type:Al Device Types:Switches*
🔹 🌆 Network Resources	Design Course Coursel	
 Network Device Groups Location 	e Name: Switches	
Device Type	Description: Switch where LAP is connected	
Network Devices and AAA Clients Default Network Device	Parent All Device Types	Select
External RADIUS Servers	• = Required fields	
Users and Identity Stores		
Policy Elements		
Access Policies		
Monitoring and Reports	1. 1. A. M	
🕨 🍕 System Administration		

7. Haga clic en Submit (Enviar). Una vez completada, la ventana se actualiza:



- 8. Vaya a Recursos de red > Dispositivos de red y clientes AAA.
- 9. Haga clic en Create y rellene los detalles como se muestra aquí:

cisco Cisco Secure A	CS			eccedmin SALIL-ACSS2 (Primery)
Any Workspace My Workspace Network Device Groups Location Device Trop My Honore Sole	Network Resources - Xetwork Devices and AAA Name: 2500-Description Description: Saltch where LAP is con Network Device Groups Location Al Locations LA	Clens - Create nected	Select	
	P Address P Single P Address O IP [102:168:153.10]	s Switches g8(s)	Select Authentication Options TXGACB+ T RADUS P Ghared Secret Coord	2
 Soldsau volumerication 	0 - Regurassis		CoApert 1790 Caapert 1790 Key Encryption Key Massage Authentica Key Input Format	br Ceda Key ASCII / [®] HEXADECIMAL

10. Haga clic en Submit (Enviar). La ventana se actualiza:

cisco Cisco Secure A	ICS					acamitrin	SALIL-AC
+ 💮 My Workspace	Network	Resources > Network	Devices and AAA Clent				
- An Network Resources	Retry	ork Devices					Showin
Network Device Groups Location	Filter	:	💌 Match it	7 60	-		
Index Devices and AM-Cherns Details Network Device Extensil EADURE Secure		Name + 3560-Switch-LAP	IP / Mask 192.168.153.10/32	NDG/Location All Locations:LAB	NDG,Device Type All Device Types:Switches	Description Switch where LAP is connected	1
+ 🔐 Lisers and identity Stores							
Policy Elements							
* 💭 Access Policies							
→ → Monitoring and Reports							
+ 🧟 System Administration							

Configurar usuarios

En esta sección, verá cómo crear un usuario en el ACS configurado previamente. Asignará el usuario a un grupo llamado "usuarios LAP".

Complete estos pasos:

1. Vaya a Usuarios y almacenes de identidad > Grupos de identidad > Crear.

Cisco Secure A MyWorkspace	VCS Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:Wir	cicas Users"
Comparing Courses Cou	General Name: LAP users Description: LAPs authenticating over wired Network Parent All Groups Required fields	Select
Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Certificate Authentication Profile Identity Store Sequences		

2. Haga clic en Submit (Enviar).

cisco Cisco Secure A	ICS
My Workspace	Users and Identity Stores > Identity Groups
► 🎲 Network Resources	Identity Groups
Busers and identity Stores Identity Groups	Filter: 💌 Match if: 💌 Go 🔫
 Internal Identity Stores External Identity Stores LDAP Active Directory RSA SecurID Token Servers 	Name Description * <u>All Groups</u> Identity Group Root <u>LAP users</u> LAPs authenticating over wired Network.
RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	

- 3. Cree **3502e** y asígnelo al grupo "usuarios LAP".
- 4. Vaya a Usuarios y almacenes de identidad > Grupos de identidad > Usuarios > Crear.

► 😤 My Workspace	Users and identity Stores > Internal identity Stores > Users > Create
Image: Book of the second s	Constal
B Users and Identity Stores	Name: 3502e Status: Enabled - 6
Identity Groups	Description: LAP 3502e in vian 253
Users	Identity Group: All Groups:LAP users Select
External Identity Stores Certificate Authorities Certificate Authorities Identity Store Sequences	Password Information Password must Contain 4 - 32 characters
Policy Elements	Password:
Access Policies	O Confirm Dependent
Monitoring and Reports	Change password on next login
Bystem Administration	User Information There are no additional identity attributes defined for user records

5. Verá la información actualizada:

😪 My Workspace	Users and	Identity Store	s > Internal identity Stor	res >	Users	
• 🚯 Network Resources	Interna	I Users				
👸 Users and Identity Stores	Eller	[a Nata a	1000 C		-
Identity Groups	Filid.	1		_		•
· Internal Identity Stores		Status	User Name	*	Identity Group	Description
U250TS			<u>3502a</u>		All Groups:LAP users	LAP 35020 in vian 253

Definición de elementos de política

Verifique que Permit Access esté configurado.

cisco Cisco Secure A	ICS
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and identity Stores	Filter Malefoit Ro V
🗸 🏇 Policy Elements	
Session Conditions Authorization and Permissions	Permit Access
 Network Access Authorization Profiles 	
Device Administration Named Permission Objects	
+ 🔂 Access Policies	
Monitoring and Reports	
🕨 🍇 System Administration	

Aplicar políticas de acceso

En esta sección, seleccionará EAP-FAST como el método de autenticación utilizado para los LAPs para autenticar. A continuación, creará reglas basadas en los pasos anteriores.

Complete estos pasos:

1. Vaya a Políticas de acceso > Servicios de acceso > Acceso a la red predeterminado > Editar: "Acceso a la red predeterminado".

cisco Cisco Secure A	CS
🕞 🕨 🛞 My Workspace	Access Policies > Access Services > Default Network Access > Edit "Default Network Access"
One the second secon	
Users and Identity Stores	General Allowed Protocols
► 🎭 Policy Elements	Name: Default Network Access
Access Policies	Description: Default Network Access Service
Access Services Access Services Access Selection Rules	Service Type : Network Access
Default Device Admin	Policy Structure
Default Network Access	✓ Identity
▶ Ø deleterne	Group Mapping
Monitoring and Reports	Authorization
🕨 🍓 System Administration	

2. Asegúrese de haber habilitado EAP-FAST y Anonymous In-Band PAC Provisioning.





- 3. Haga clic en Submit (Enviar).
- 4. Verifique el grupo de identidad que ha seleccionado. En este ejemplo, utilice **Internal Users** (que fue creado en ACS) y guarde los cambios.

cisco Cisco Secure A	CS academin SA
► 🚭 My Workspace	Access Policies > Access Sonices > Default Network Access > Identity
► ftp Network Resources	Spale result selection C Bule based result selection
+ 🐉 Users and Identity Stores	Identity Source. Internal Users Select
Policy Elements	T Advanted Patients
🖌 🏝 Access Policies	It is mention failed Read
Access Services Service Selection Rules O Detault Device Admin	If user not found Reject If process failed Drop
O Delaut Network Access	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will
Authorization Actional Authorization	on reprised
 Identifying and Reports 	
 New System Administration 	

5. Vaya a Access Policies > Access Services > Default Network Access > Authorization para verificar el perfil de autorización.

Puede personalizar en qué condiciones permitirá el acceso de un usuario a la red y qué perfil de autorización (atributos) pasará una vez autenticado. Esta granularidad sólo está disponible en ACS 5.x. En este ejemplo, se seleccionan Location, **Device Type**, **Protocol**, **Identity Group** y EAP Authentication Method.



- 6. Haga clic en Aceptar y Guardar cambios.
- 7. El siguiente paso consiste en crear una regla. Si no se define ninguna regla, el LAP se permite el acceso sin ninguna condición.
- 8. Haga clic en Create > Rule-1. Esta regla es para los usuarios del grupo "usuarios LAP".

cisco Cisco Secure At	CS .	cascimin S4
	Access Palcies > Access Services > Default Selvicet Access > Aufterization Standard Policy Exception Policy Net Cisco Secure ACS - Mozilla Finelice	×
Access Primes Access Services Service Selection Rules O Detast Device Admin O Detast Device Admin O Detast Device Admin Access Identity Access Access	File 192.468.450.24 https://192.468.450.24/ accadmin/PolicyInputAction.de I General General Itame: Rule-1 Status: Enabled Image: The Customize buttion in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	
 Note and the second seco	Cenditions Image: NDG Location: Image: NDG Device Type: Image: NDG Device Type: NDG Device Type: Image: NDG Device Type: NDG Device Type	5 51
	OK Cancel OK Cancel Destault Fino rules defined or no enabled rule matches. Oreate Duplicale Edit Detete Move to Save Changes Discard Changes	Help

9. Haga clic en **Guardar cambios**. Si desea que se denieguen los usuarios que no cumplan las condiciones, edite la regla predeterminada para que diga "Denegar acceso".

cisco Cisco Secure A	28	scaadmin SALB, AC302 (Pr	imery) Log Dut About Ne
► - Ny Werkspace	Access Psicies > Access Services > Defaul listeent Access > Autorization		State of the State
» (5) Network Resources	Standard Balant Consultan Balan		
· 🗿 Uoers and Identity Stores	Statement Process Anthenine Policy		
* 🕞 Policy Elements	The first Access without ston Policy		
• 🐁 Access Policies	Mac Islaus Watch It Islauss - Enabled - Calar Hills Go +		
Access Services El Service Selection Rules	Status Name NDGLocation NDG Device Type Protocol Identity Group	Eap Authentication Method	Results Hit Authorization Profiles
 Default Device Admin 	Bule: W Al Locations LAB In All Device Types Dwitches match Radius In All Droups LAP users	-4101-	PermitAccess 0
OPPRETRANSMENT ADDRESS IDENTIFY			
Ball cruster			
* 📄 Nontoring and Reports			
+ M Eystem Administration			
	Dolaut Ene rules defined ar no enabled rule matches.		Permit Access
	Create_1+ Dudicate_1+ Edit Detete A Nove to Y		Custerize Ht Court
	ALEND AND AND ALEND ALEND ALEND		
	Save Ohanges Discard Changes		

10. El último paso consiste en definir reglas de selección de servicios. Utilice esta página para configurar una política simple o basada en reglas para determinar qué servicio se debe aplicar a las solicitudes entrantes. Por ejemplo:

cisco Cisco Secure AC	cs		-				Notes in the		scsadmin	MU
* 🛃 My Workspace	Access P	tikies	> Access	Services	Service Selection R	ies				
* 🚯 Network Resources	C St	ncle re	sult sales	tion 🕫 i	Rule based result :	election				
38 Users and identity Stores	Servi	ce Sel	ection Po	licy						
+ 🥎 Policy Elements	Filter	Stat	us +	Natch it	Equals +	Enabled	Clear Filter	00 -		
Access Policies Access Renines		C	Status	Name	Protocal	Conditions		Resulta	Hit Count	
Senate Selector Pales Selector Pales Selector Pales	1			Rule-1	match Radius			Default Network Access	0	
O Default Network Access Identity Authorization Ø defeteme	2	Г	0	Rule-2	match Tacacs			Default Device Admin	0	
► S Monitoring and Reports										
* 🧏 System Administration										

Verificación

Una vez que 802.1x está habilitado en el puerto del switch, todo el tráfico, excepto el tráfico 802.1x, se bloquea a través del puerto. El LAP, que ya está registrado en el WLC, se desasocia. Sólo después de una autenticación 802.1x correcta se permite el paso de otro tráfico. El registro exitoso del LAP al WLC después de que 802.1x esté habilitado en el switch indica que la autenticación del LAP es exitosa.

Consola de AP:

<#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.

Registros de ACS:

1. Ver los recuentos de visitas:

Si está comprobando los registros en los 15 minutos siguientes a la autenticación, asegúrese de actualizar el número de visitas. En la misma página, en la parte inferior tiene una pestaña **Hit Count**.

cisco Cisco Secure Ad	CS		-	-			ace
+ 🔆 My Workspace	Access	Policies	» Access	Services >	Service Selection Rules		
+ 🎲 Network Resources	0 s	nole re	sult selec	ton 🖲 F	tule based result selection		
Users and Identity Stores	Servi	ce Sel	ection Pol	icy			
+ 🚱 Policy Elements	Filter	: Stat	us •	Match if:	Equals - Enabled - Clear Filter	G0 -	
 Access Policies 			_		Conditions	 Results	
 Access Services 			Status	Name	Protocol	Service	Hit Count
Belancescentini Antes Default Device Admin	1			Rule-1	match Radius	Default Network Access	1
 Ø Default Network Access 	2	Г	0	Rule-2	match Tacaca	Default Device Admin	0
Identity Authorization							
+ 📳 Monitoring and Reports							
🔸 🍓 System Administration							

cisco Cisco Secure Al	CS SALE AC	SAT (Primary) Log Out About Pr
 Statistics 	Access Pelities + Access Services + Calleut Halwort Access + Autheritation	
s (b) Network Resources	Standard Extinui Excerting Delice	
 Jusers and identity Stores 	Notwork Arrange Authoritation Desiry	
 So Policy Elements Access Policies 	Filter Dialas • Hatch ff, Equais • Enabled • Clear Filter Go •	
Access Services I Service Selection Rales	Name NDGLocation NDGDelice Type Protocol Identity Group Explositionity Method	Results Authorization Profiles HE Count
Orfault Device Admin Orfault Network Admin	Rule-1 In Al 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		
	•	л.
	If no rules defined or no enabled rule matches.	Permit Access 0
	Create. • Duplosh. I • Edt Delete A Nove to. Y	Customize Hit Gount
	Ban Changes Discard Changes	

2. Haga clic en **Supervisión e informes** y aparecerá una nueva ventana emergente. Haga clic en **Autenticaciones -RADIUS -Hoy**. También puede hacer clic en **Detalles** para verificar qué regla de selección de servicio se aplicó.

@ @										Launch Interact	live Warwar
Showing Page	1 1 of 1					I Geta	lage: Ge				
AAA Protocol > RAD	US Authe	ntication									
Authentication Status : Date :	Pass or Pail January 29,	2012 (<u>Las</u>	1.30 Nin	utes i Last Hi	uri Last 12 Hours (To	day i <u>Yesferdar i Last 7 Dax</u>	(Last30 Days)				
Generated on January 2	9, 2012 9.15	01 PM ES	st								
Rekel	-ciek for e	ietaile \$		e over item	for additional informat	tion					
Logged At	RADUS	S NAS Failure	Details	Usemame	MACIP Address	Access Senice	Authentication Method	Network Device	NAS IP Address	NAS Port ID	C1S Security Gr
Jan 29,12 9:11:12 966	FM 🖌		4	3502e	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-NSCHAP\2)	3590-Switch-LAP	192.168,153.10	GigabitEthemet0/11	

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- <u>Cisco Secure Access Control System</u>
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).