ASA 8.3 y más adelante: Autorización de RADIUS (ACS 5.x) para el acceso VPN usando ACL descargable con el ejemplo de la configuración CLI y ASDM

Contenido

Introducción prerrequisitos Requisitos **Componentes Utilizados Convenciones Antecedentes** Configurar Diagrama de la red Configure el VPN de acceso remoto (IPsec) Configure el ASA con el CLI Configure ACS para ACL descargable para el usuario individual Configure ACS para ACL descargable para el grupo Configure ACS para ACL descargable para un grupo de dispositivos de red Configure las configuraciones IETF RADIUS para un grupo de usuarios Configuración de Cliente Cisco VPN Verificación Comandos show crypto ACL descargable para el usuario/el grupo Filtro-identificación ACL **Troubleshooting** Borre las asociaciones de seguridad Comandos para resolución de problemas Información Relacionada

Introducción

Este documento describe cómo configurar el dispositivo de seguridad para autenticar a los usuarios para el acceso a la red. Puesto que usted puede activar implícito las autorizaciones de RADIUS, este documento no contiene ninguna información sobre la configuración de la autorización de RADIUS en el dispositivo de seguridad. Proporciona información sobre cómo gestiona el dispositivo de seguridad la información de la lista de acceso recibida de los servidores RADIUS.

Usted puede configurar a un servidor de RADIUS para descargar una lista de acceso al dispositivo de seguridad o un nombre de la lista de acceso a la hora de la autenticación. Autorizan al usuario a hacer solamente qué se permite en la lista de acceso usuario-específica.

Las Listas de acceso transferibles son los medios más escalables cuando usted utiliza el Cisco Secure Access Control Server (ACS) para proporcionar a las Listas de acceso apropiadas para cada usuario. Para más información sobre las funciones de lista de acceso transferibles y Cisco ACS seguro, refiera a configurar a un servidor de RADIUS para enviar las listas de control de acceso transferibles y IP transferible ACL.

Refiera a <u>ASA/PIX 8.x</u>: <u>Autorización de RADIUS (ACS) para el acceso a la red usando ACL</u> <u>descargable con el ejemplo de la configuración CLI y ASDM</u> para la configuración idéntica en Cisco ASA con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

Este documento asume que el dispositivo de seguridad adaptante (ASA) está completamente - operativo y configurado para permitir que el Cisco Adaptive Security Device Manager (ASDM) o el CLI realice los cambios de configuración.

Nota: Refiera a <u>permitir el acceso HTTPS para ASDM</u> para permitir que el dispositivo sea configurado remotamente por el ASDM o el Secure Shell (SSH).

Componentes Utilizados

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

- Versión de software 8.3 de Cisco ASA y más adelante
- Versión 6.3 y posterior de Cisco ASDM
- Cliente VPN de Cisco versión 5.x y más adelante
- Cisco ACS seguro 5.x

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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco</u> para obtener más información sobre las convenciones del documento.

<u>Antecedentes</u>

Usted puede utilizar IP transferible ACL para crear los conjuntos de las definiciones ACL que usted puede aplicar a muchos usuarios o grupos de usuarios. Estos conjuntos de las definiciones ACL se llaman contenido ACL.

El IP transferible ACL actúa esta manera:

- 1. Cuando ACS concede un acceso del usuario a la red, ACS determina si un IP transferible ACL está asignado al perfil de la autorización en la sección del resultado.
- 2. Si ACS localiza un IP transferible ACL que se asigne al perfil de la autorización, ACS envía un atributo (como parte de la sesión del usuario, en el RADIUS acceso-valide el paquete) que especifica ACL mencionado, y la versión del ACL mencionado.
- 3. Si responde el cliente AAA que no tiene la versión actual del ACL en su caché (es decir, el ACL es nuevo o ha cambiado), ACS envía el ACL (nuevo o actualizado) al dispositivo.

El IP transferible ACL es una alternativa a la configuración de los ACL en el atributo [26/9/1] del cisco av-pair RADIUS Cisco de cada usuario o grupo de usuarios. Usted puede crear un IP transferible ACL una vez, le da un nombre, y después asigna el IP transferible ACL a cualquier perfil de la autorización si usted se refiere a su nombre. Este método es más eficiente que si usted configura el atributo del cisco av-pair RADIUS Cisco para el perfil de la autorización.

Cuando usted ingresa las definiciones ACL en la interfaz Web ACS, no utilice la palabra clave o las entradas de nombre; por lo demás, utilice el sintaxis del comando acl y la semántica estándar para el cliente AAA en quien usted se prepone aplicar el IP transferible ACL. Las definiciones ACL que usted ingresa en ACS comprenden uno o más comandos acl. Cada comando acl debe estar en una línea aparte.

En ACS, usted puede definir IP transferible múltiple ACL y utilizarlo en diversos perfiles de la autorización. De acuerdo con las condiciones en las reglas de la autorización del servicio del acceso, usted puede enviar diversos perfiles de la autorización que contienen IP transferible ACL a diversos clientes AAA.

Además, usted puede cambiar la orden del contenido ACL en un IP transferible ACL. ACS examina el contenido ACL, a partir del top de la tabla, y descarga el primer contenido ACL que encuentra. Cuando usted fija la orden, usted puede asegurar la eficiencia del sistema si usted coloca lo más extensamente posible el contenido aplicable ACL más arriba en la lista.

Para utilizar un IP transferible ACL en un cliente AAA determinado, el cliente AAA debe adherirse a estas reglas:

- Utilice RADIUS para la autenticación
- Utilice IP transferible ACL

Éstos son ejemplos de los dispositivos de Cisco que utilizan IP transferible ACL:

• ASA

• Dispositivos de Cisco que funcionan con la versión 12.3(8)T y posterior IOS

Éste es un ejemplo del formato que usted debe utilizar para ingresar ASA ACLs en el rectángulo de las definiciones ACL:

permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1 permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255 permit 0 any host 10.159.1.22 deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log permit TCP any host 10.160.0.1 eq 80 log permit TCP any host 10.160.0.2 eq 23 log permit TCP any host 10.160.0.3 range 20 30 permit 6 any host HOSTNAME1 permit UDP any host HOSTNAME2 neq 53 deny 17 any host HOSTNAME3 lt 137 log deny 17 any host HOSTNAME4 gt 138 deny ICMP any 10.161.0.0 0.0.255.255 log permit TCP any host HOSTNAME5 neg 80

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:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que fueron utilizadas en un entorno de laboratorio.

Configure el VPN de acceso remoto (IPsec)

Procedimiento ASDM

Complete estos pasos para configurar el VPN de acceso remoto:

 Seleccione los Asisitente > a los Asisitente VPN > IPsec(IKEv1) Asisitente del VPN de acceso remoto de la ventana casera.

File	View	Tools V	Vizards Window	Help				Look	
24	Home	S cor	Startup Wizard		ĩ	Back C Forward	🤊 Help		
-			VPN Wizards	•		Site-to-site VPN Wizard	L		
vice List	Home Hig Device Uni		High Availability Unified Commu	High Availability and Scalability Wizard Unified Communication Wizard		AnyConnect VPN Wizar Clientless SSL VPN Wiza	rd ard		
B	Device Infc Packet Capture Wizard				IPsec (IKEv1) Remote Access VPN Wizard				
	Ge	eneral Lice	anse		-	15	Interface	IP Address/Ma	
				A 4			dmz	192.168.26.13/24	
	н	lost Name:	ciscoasa.dera	Jic.domain.invalid	-		inside	10.1.1.1/24	
	A	5A Version	8.4(3)	Device Optime: Ud Zh 2	Um	13/5	outside	172.16.1.1/24	
	A	SDM Versio	n: 6.4(7)	Context Mode: Single	10		test	no ip address	
	Т	otal Flash:	64 MB	Total Memory: 256 MB	1				
		or a second s					Select an interface to	view input and output	

 Seleccione la interfaz del túnel VPN como sea necesario (afuera, en este ejemplo), y también asegúrese de que el checkbox al lado de las sesiones del permiso IPSec entrante para desviar las Listas de acceso del interfaz está controlado.



 Elija el tipo de cliente VPN como Cliente Cisco VPN, la versión 3.x o más arriba. Haga clic en Next (Siguiente).

VPN Wizard	Remote Access Client (Step 2 of)
and a second	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
Corporate Network	VPN Client Type: C Elisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product
	 C Microsoft Windows client using L2TP over IPsec Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it. □ PAP □ CHAP □ MS-CHAP-V1 □ MS-CHAP-V2 □ EAP-PROXY Specify if the client will send tunnel group name as - username@tunnelgroup. □ Client will send tunnel group name as username@tunnelgroup. If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next Finish Cancel Help

4. Elija el método de autenticación y proporcione a la información de autenticación. El método de autenticación usado aquí es clave previamente compartida. También, proporcione a un nombre de grupo de túnel en el espacio proporcionado. La clave previamente compartida usada aquí es cisco123 y el nombre de grupo de túnel usado aquí es Cisco-túnel. Haga clic en Next

(Siguiente).

🔂 VPN Wizard	×
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
unand Unand Unand Unand	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client. - Authentication Method • Pre-shared key
Corporato	Pre-Shared Key: cisco123
Contraction of the second seco	Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Certificate Name: Challenge/response authentication (CRACK) Tunnel Group Tunnel Group Tunnel Group Name: Cisco-Tunnel
	< Back Next > Finish Cancel Help

5. Elija si desea que los usuarios remotos sean autenticados en las bases de datos de usuarios locales o en un grupo de servidores AAA externo. Aquí, elegimos autenticamos usando un Grupo de servidores AAA. Haga clic nuevo al lado del campo de nombre del Grupo de servidores AAA para crear un nuevo nombre de Grupo de servidores AAA.

🔂 VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window. Authenticate using the local user database Authenticate using an AAA server group AAA Server Group Name: Image Server Group Name Server Server Group Name Server Group N
	<back next=""> Finish Cancel Help</back>

6. Proporcione al nombre de grupo de servidores, al protocolo de autenticación, al nombre de la dirección IP del servidor, del interfaz, y a la clave del Secreto de servidor en los espacios respectivos proporcionados, y la **AUTORIZACIÓN del** tecleo.

Creace a new authentication s To add more servers to the gr Configuration > Device Manag	erver group containing one authentication serv oup or change other AAA server settings, go t gement > Users/AAA > AAA Server Groups.	ver. D
Server Group Name:	ACS5	
Authentication Protocol:	RADIUS	
Server IP Address:	192.168.26.51	
Interface:	dmz	
Server Secret Key:	****	
Confirm Server Secret Key:	****	

7. Haga clic en Next (Siguiente).

🚮 VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
Brandi Brandi SP Brandi Homo Nativerk	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.
	Authenticate using an AAA server group AAA Server Group Name: ACS5 New
	<back next=""> Finish Cancel Help</back>

8. Defina un pool de las direcciones locales que se asignarán dinámicamente a los clientes de VPN remotos cuando se conectan. Haga clic **nuevo** para crear un nuevo pool de la dirección local.

📸 VPN Wizard		×
VPN Wizard Briefstein	Address Pool Enter a po clients.	(Step 5 of 10)
Corporatio Nertwork		Tunnel Group Name : Clisco-Tunnel Pool Name: Pool Settings Range Start Address: Range End Address: Subnet Mask;
		< Back Next > Finish Cancel Help

9. En la ventana del grupo de direcciones IP del agregar, proporcione al nombre del pool, comenzando la dirección IP, terminando la dirección IP, y a la máscara de subred. Click

Name:	Sample-Pool	
Starting IP Address:	10.2.2.1	1
Ending IP Address:	10.2.2,254	1
Subnet Mask:	255.255.255.0	1

Seleccione el nombre del pool de la lista desplegable, y haga clic después. El nombre del pool por este ejemplo es Muestra-pool que fue creado en el paso
 9.

🚰 VPN Wizard	1			2
VPN Wizard	Address Pool	(Step 5 of 10)		
	Enter a po clients.	ol of local addresses to be us	ed for assigning dynamic IP ad	dresses to remote VPN
Corporate Natwork		Tunnel Group Name :	Dișco-Tunnel	
Techte		Pool Name:	Sample-Pool	New
A CAR	a the	Pool Settings		
T-HUIM		Range Start Address:	10.2.2.1	
Terret	4	Range End Address:	10.2.2.254	
		Subnet Mask:	255.255.255.0	
			<back next=""> Fir</back>	Cancel Help

11. *Opcional:* Especifique la información de servidor DNS y WINS y un Nombre de Dominio Predeterminado que se avanzará a los clientes de VPN remotos.

🚰 VPN Wizard	×
VPN Wizard	Attributes Pushed to Client (Optional) (Step 6 of 10)
	Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.
Home	Tunnel Group: Disco-Tunnel
Corporate Network	Primary DNS Server:
1 Alter	Secondary DNS Server:
	Primary WINS Server:
and the state	Secondary WINS Server:
S.P-	Default Domain Name: cisco.com
4	
	<back cancel="" finish="" help<="" next="" th=""></back>

12. Especifique qué host internos (de haber alguno) o redes deben exponerse a los usuarios de VPN remotos. Haga clic después después de proporcionar al nombre del interfaz y las redes que se eximirán en las redes exentas colocan. Si deja esta lista vacía, permita que los usuarios de VPN remotos acceden a la red interna completa del ASA. Puede también habilitar la tunelización dividida en esta ventana. La tunelización dividida encripta el tráfico a los recursos definidos anteriormente en este procedimiento y proporciona el acceso no cifrado a Internet en general al no tunelizar ese tráfico. Si la tunelización dividida no se habilita, todo el tráfico de los usuarios de VPN remotos se tuneliza al ASA. Éste puede convertirse en un gran ancho de banda y hacer un uso intensivo del procesador, sobre la base de su

configuración.

📸 VPN Wizard		4
VPN Wizard	IPsec Settings (Optional) (Step 7 of 10)	
Brench Brench SP Honm	Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the Exempt Networks field blank.	
Corporate	Interface:	
Nam	Exempt Networks: 10.1.1.0/24 -	
	Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet. Enable Perfect Porwarding Secrecy (PFS) Diffie Hellman Group:	
	<back cancel="" help<="" next="" th="" trinsh=""><th></th></back>	

13. Esta ventana muestra un resumen de las acciones que ha realizado. Haga clic en **Finalizar** si está satisfecho con la configuración.



Configure el ASA con el CLI

Ésta es la configuración CLI:

Configuración corriente en el dispositivo ASA
ASA# sh run
ASA Version 8.4(3)
!
! Specify the hostname for the Security Appliance.
hostname ciscoasa enable password y.tvDXf6yFbMTAdD
encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !
Configure the outside and inside interfaces. interface
Ethernet0/0 nameif dmz security-level 50 ip address
192.168.26.13 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface Ethernet0/2 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
<pre>! Output is suppressed. boot system disk0:/asa843-</pre>
k8.bin ftp mode passive object network
NETWORK_OBJ_10.1.1.0_24 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_10.2.2.0_24 subnet 10.2.2.0
255.255.255.0 access-list OUTIN extended permit icmp any
any ! This is the Access-List whose name will be sent
by ! RADIUS Server(ACS) in the Filter-ID attribute.
access-list new extended permit ip any host 10.1.1.2
access-list new extended deny ip any any
pager lines 24
logging enable

logging asdm informational mtu inside 1500 mtu outside 1500 mtu dmz 1500 ip local pool Sample-Pool 10.2.2.1-10.2.2.254 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 !--- Specify the location of the ASDM image for ASA !--to fetch the image for ASDM access. asdm image disk0:/asdm-647.bin no asdm history enable arp timeout 14400 !--- Specify the NAT from internal network to the Sample-Pool. nat (inside,outside) source static NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24 destination static NETWORK_OBJ_10.2.2.0_24 NETWORK_OBJ_10.2.2.0_24 no-proxy-arp route-lookup access-group OUTIN in interface outside !--- Create the AAA server group "ACS5" and specify the protocol as RADIUS. !--- Specify the ACS 5.x server as a member of the "ACS5" group and provide the !--- location and key. aaa-server ACS5 protocol radius aaa-server ACS5 (dmz) host 192.168.26.51 timeout 5 key ***** aaa authentication http console LOCAL http server enable 2003 http 0.0.0.0 0.0.0.0 inside !--- PHASE 2 CONFIGURATION ---! !--- The encryption & hashing types for Phase 2 are defined here. We are using !--- all the permutations of the PHASE 2 parameters. crypto ipsec ikev1 transform-set ESP-AES-256-MD5 espaes-256 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-192-MD5 espaes-192 esp-md5-hmac crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac crypto ipsec ikev1 transform-set ESP-AES-256-SHA espaes-256 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-192-SHA espaes-192 esp-sha-hmac crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac !--- Defines a dynamic crypto map with !--- the specified transform-sets created earlier. We are specifying all the !--- transform-sets. crypto dynamicmap SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transformset

ESP-AES-128-SHA ESP-AES-128-MD5

```
ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-
256-MD5 ESP-3DES-SHA
   ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
!--- Binds the dynamic map to the IPsec/ISAKMP process.
crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. crypto map
outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policies defined with all the permutation !-
-- of the 5 ISAKMP parameters. The configuration
commands here define the !--- Phase 1 policy parameters
that are used. crypto ikev1 enable outside
crypto ikev1 policy 10
authentication crack
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 20
authentication rsa-sig
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 30
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
crypto ikev1 policy 40
authentication crack
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 50
authentication rsa-sig
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 60
authentication pre-share
encryption aes-192
hash sha
group 2
lifetime 86400
crypto ikev1 policy 70
authentication crack
encryption aes
hash sha
```

group 2 lifetime 86400 crypto ikev1 policy 80 authentication rsa-sig encryption aes hash sha group 2 lifetime 86400 crypto ikev1 policy 90 authentication pre-share encryption aes hash sha group 2 lifetime 86400 crypto ikev1 policy 100 authentication crack encryption 3des hash sha group 2 lifetime 86400 crypto ikev1 policy 110 authentication rsa-sig encryption 3des hash sha group 2 lifetime 86400 crypto ikev1 policy 120 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 crypto ikev1 policy 130 authentication crack encryption des hash sha group 2 lifetime 86400 crypto ikev1 policy 140 authentication rsa-sig encryption des hash sha group 2 lifetime 86400 crypto ikev1 policy 150 authentication pre-share encryption des hash sha group 2 lifetime 86400 webvpn group-policy Cisco-Tunnel internal group-policy Cisco-Tunnel attributes vpn-tunnel-protocol ikev1



Configure ACS para ACL descargable para el usuario individual

Usted puede configurar las Listas de acceso transferibles en Cisco ACS seguro 5.x pues Permissions Nombrados Object y después lo asigna a un perfil de la autorización que sea elegido en la sección del resultado de la regla en el Acceso-servicio.

En este ejemplo, el usuario de VPN **Cisco de** IPsec autentica con éxito, y el servidor de RADIUS envía una lista de acceso transferible al dispositivo de seguridad. El usuario "Cisco" puede tener acceso solamente al servidor de 10.1.1.2 y niega el resto del acceso. Para verificar el ACL, vea <u>ACL descargable para el usuario/la sección de grupo</u>.

Complete estos pasos para configurar al cliente RADIUS en Cisco ACS seguro 5.x:

 Elija los recursos de red > los dispositivos de red y a los clientes AAA, y el tecleo crea para agregar una entrada para el ASA en la base de datos del servidor RADIUS.

 My Workspace 	Network Resources > Network Devices and AAA Clents
🔹 🤯 Network Resources	Network Devices
 Network Device Groups Location 	Filter: Match if: Go 🗢
Dence Type Network Dences and Ava Clients Default Network Device External Proxy Servers	 Name IP Address Description NDG:Location NDG:Device Type No data to display
	Create Duplicate Edit Delete File Operations Export

 Ingrese el nombre significativo a localmente - para el ASA (muestra-asa, en este ejemplo), después ingrese 192.168.26.13 en el campo del IP address. Elija el RADIO en la sección de las opciones de autenticación controlando el checkbox del RADIO y ingrese cisco123 para el campo secreto compartido. Haga clic en Submit (Enviar).

Description:	5	
Location	All Locations	Select
Device Type	All Device Types	Select
Gingle IP Addr Single IP Addr IP: 192.168.26.13	ess CIPRange(s) By Mask CIPRange(s)	Authentication Options
- Dogukod Onlde		Kayinputromiai ~ Aocii ~ Mexabechikat

3. El ASA se agrega con éxito a la base de datos del servidor de RADIUS (ACS).

Filter:		Match if.	•	G0 🔻	
	Name 🔺	IP Address	Description	NDG:Location	NDG:Device Type
	sample-asa	192.168.26.13/32		All Locations	All Device Types

4. Elija a los usuarios y la identidad salva > identidad interna salva > los usuarios, y el tecleo crea para crear a un usuario en la base de datos local del ACS para la autenticación VPN.

 My Workspace 	Users and identity Stores > Internal identity Stores > Users
Network Resources	Internal Users
Source and Identity Stores Identity Groups	Filter: Match if. Go 🗢
Internal Identity Stores	Status User Name Identity Group Description No data to display Create Duplicate Edit Detete [Change Password] File Operations Export

 Ingrese el nombre de usuario cisco. Seleccione el tipo de contraseña como usuarios internos, y ingrese la contraseña (cisco123, en este ejemplo). Confirme la contraseña, y el tecleo

Name:	cisco Status	Enabled 💌 😑				
Description:	48.00000					
Password Inform Password must Contain 4 Password Typ Password: Confirm Pass Confirm Pass Change pass There are no a	nation I - 32 characters pe: Internal Users word: ••••••• assword on next login dditional identity attributes defined for u	ser records	Enable Passw Select Enat Cont Passw	Password Informa ord must Contain 4 - 32 char ile Password:	dion nacters	

6. Crean al usuario Cisco con

,	
AY	′It∩
07	ιιυ

Filter	:	Match if:	Go	-
Г	Status	User Name	Identity Group	Description
	0	cisco	All Groups	

 Para crear ACL descargable, elegir los elementos de la directiva > la autorización y los permisos > nombró a Permission Objects > los ACL transferibles, y el tecleo crea.

er:		3	Match if:	•	G0 🔻	
	Name		Description			
	No data	to disp	lay			

8. Proporcione al **nombre** para ACL descargable, así como al **contenido ACL**. Haga clic en Submit

(Enviar).

Periorai			
Name:	Sample-DACL		
Description			
ownloadable	a ACL Content		
permit jp s	any host 10.1.1.2		
deny ip an	y any		
= Required	fields		

9. ACL descargable la muestra-DACL se crea con

é	Х	it	0	•
		-		

itter. Match it Go 🕶	
Name - Description	
Sample-DACL	

10. Para configurar las políticas de acceso para la autenticación VPN, elija las políticas de acceso > el acceso mantiene > las reglas de selección del servicio, y determina qué servicio está abasteciendo al protocolo RADIUS. En este ejemplo, las coincidencias RADIUS de la regla 1, y el acceso a la red del valor por defecto abastecerán al pedido de RADIUS.



11. Elija el servicio del acceso determinado del paso 10. En este ejemplo, se utiliza el acceso a la red del valor por defecto. Elija la tabulación permitida de los protocolos, y asegúrese de que permita PAP/ASCII y permita MS-CHAPv2 estén seleccionados. Haga clic en Submit (Enviar).

Aut	thentication Protocols		
•	Allow PAP/ASCI		
•	Allow CHAP		
٠	C Allow MS-CHAPv1		
۲	Allow MS-CHAPv2		
•	Allow EAP-MD5		
	Allow EAP-TLS		
	C Allow LEAP		
+	Allow PEAP		
٠	Allow EAP-FAST		
	Preferred EAP protocol	P	

12. Haga clic en la **sección de la identidad de los servicios del acceso**, y asegúrese de que seleccionan a los **usuarios internos** como la fuente de la identidad. En este ejemplo, hemos tomado el acceso a la red del valor por defecto.



13. Elija las políticas de acceso > los servicios del acceso > el acceso a la red > la autorización del valor por defecto, y el tecleo

	Pol	CVI Excer	rtion Poli	24							
twork	k Acı	cess Aut	horization	Policy							
tter:	Stat	15		Match if: Equ	uals	* Enabled	٠	Clear Filter Co	~		
1		Status	Name	NDG:Location	Cond	iitions Time And Date		Results Authorization Profile	Hit Count		
		No data	to display	1							
		Default		If no rules defin	ted or no	o enabled rule ma	iches	PermitAccess	0		

 Sistema del movimiento: Username de la columna disponible a la columna seleccionada, y AUTORIZACIÓN del tecleo.



15. El tecleo crea para crear una nueva

Netwo	rk Ac	cess Aut	horizatio	n Policy				annan annan	
Filter:	Stat	us		Match it Equa	als 💽 Enabled 💌	Clear Filter	00 🗢		
		Status	Name	NDG:Location	Conditions System:UserName Identi	ty Group Autho	Results rization Profiles	Hit Count	
		No data	to displa	y .					
	F	Default		If no rules define	d or on enabled rule matche	s Permi	tAcress	0	
Treste	1.	Dunles	10 1-	Frit Daleta	Move to 1			-	Customire Hit Count

 Asegúrese de que el checkbox al lado del sistema: El username se selecciona, elige los iguales de la lista del descenso-abajo, y ingresa el nombre de usuario cisco.

o Secure ACS - Mozilla Fir	efox	
192.168.26.51 https://192	.168.26.51/acsadmin/PolicyInputAction.do	
General Name: Rule-2 The Custom policy condi	Status: Enabled Status	
Conditions	AND	
NDG:Location:		
Identity Group: Results Authorization Profiles:	-ANY-	
	defined in multiple profiles will use the value from the firm profile defined.	st
Select Deselect		
OK Cancel		Hel

17. Tecleo selecto.

o Secure ACS - Mozilla Fi	efox	
192.168.26.51 https://19	2:168.26.51/acsadmin/PolicyInputAction.do	-
General Name: Rule-2 The Custon policy cond	Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Enable of the policy rules screen controls which status and results are available here for use in policy rules.	
Conditions		
NDG:Location:	-ANY-	
System:UserName:	equals cisco	
Authorization Profiles:	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
Select Deselect		
Cancel		Hel

18. El tecleo **crea** para crear un nuevo perfil de la autorización.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.ds	(h)
Authorization Profiles	Showing 1-2 of 2 50 🝸 per pageGo
Filter: Match if. Oo 🔻	
Name Description	
DerwAccess	
Permit Access	
Create Duplicate Edit Delete	Page 1 of 1 milled
Un Cancer	Heip
	33

19. Proporcione a un nombre para el **perfil de la autorización**. **El ejemplo de perfil** se utiliza en este

mplo.		
o Secure ACS - Mo	zilla Firefox	NAMES OF TAXABLE PARTY OF TAXABLE PARTY.
] 192.168.26.51 ht	ps://192.168.26.51/acsadmin/NetworkAccessIPInputAction.do	WHAT INSTALLS IN THE PARTY OF THE PARTY OF
General Com	non Tasks RADIUS Attributes	
Name: 8	ample-Profile	
Description:		
F = Required field	8	
	R	
	10 x	
	1	
Ibmit Cancel	-	

20. Elija la tabulación **común de las tareas**, y seleccione los **parásitos atmosféricos de la** lista desplegable para **ACL descargable el nombre**. Elija el **DACL** creado recientemente **(la**

muestra - DACL) de la lista desplegable de

valores.

ACLS						
Downloadable ACL Name:						
Downloadable Nor Name. Te	Static	٠	Value Sample-DAQ	*		
Filter-ID ACL:	Not in Use	٠			-	
Proxy ACL:	Not in Use	-				
Voice VLAN						
Permission to Join:	Not in Use	-				
VLAN						
VLAN ID/Name:	Not in Use	*				
Reauthentication						
Reauthentication Timer.	Not in Use	٠				
Maintain Connectivity during Reauthentication:						
005						
Input Policy Map:	Not in Use	•				
Output Policy Map:	Not in Use	+				
802.1X-REV		_				
LinkSec Security Policy:	Not in Use	*				
		_				

21. Haga clic en Submit

General Common Tasks	RADIUS A	tribute	s	
ACLS	-			
Downloadable ACL Name:	Static	٠	Value Sample-DACL	
Filter-ID ACL:	Not in Use	*		
Proxy ACL:	Not in Use	-		
Voice VLAN		_		
Permission to Join:	Not in Use	-		
VLAN		_		
VLAN ID/Name:	Not in Use	*		
Reauthentication				
Reauthentication Timer:	Not in Use	٠		
Maintain Connectivity during Reauthentication:	1			
QOS				
Input Policy Map:	Not in Use	•		
Output Policy Map:	Not in Use	*		
802.1X-REV				
LinkSec Security Policy:	Not in Use	*		
URL Redirect				
When a URL is defined for I	Redirect an AC	1 mus	st also be defined	

22. Asegúrese de que el checkbox al lado del ejemplo de perfil (el perfil creado recientemente

de la autorización) esté controlado, y haga clic la **AUTORIZACIÓN**.

withorization Profiles	Showing 1-3 of 3 50 T per page
Filter: Match if: Go 🔻	
Name Description	
DemyAccess	
Permit Access	
Sample-Profile	

23. Una vez que usted ha verificado que el **ejemplo de perfil** creado recientemente está seleccionado en la **autorización perfila el** campo, haga clic la **AUTORIZACIÓN**

General		
Name: Rule-2	Status: Enabled 💌 🔿	
The Custor policy cond	mize button in the lower right area of the policy rules screen controls which ditions and results are available here for use in policy rules.	
NDG:Location:	-ANY-	
System:UserName	equals cisco	
Identity Group:	-ANY-	
Sample-Profile	Tou may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the firs profile defined.	t

24. Verifique que la nueva regla (**Rule-2**) esté creada con el sistema: El username **iguala las**

condiciones y el **ejemplo de perfil de Cisco** como el resultado. **Cambios de la salvaguardia del** tecleo. La regla 2 se crea con

etwo	rk Act	ess Auth	orization	Policy					
iter:	Statu	IS		Match it Equal	is 💌 Enabled	Ciear Fi	ter 00 🔻		
	Г	Status	Name	NDG:Location	Conditions System:UserName	Identity Group	Results Authorization Profiles	Ht Count	
1	0	0	Rule-2	-ANY-	equals cisco	-ANY-	Sample-Profile	0	
•	Г	Default		If no rules define	ed or no enabled rule r	natches.	PermitAccess	Ð	
eat		Doplicat	E. [-] 3	Edit Delate	Move to:				Customize Hit Coun

Configure ACS para ACL descargable para el grupo

Complete los pasos 1 a 12 del <u>configurar ACS para ACL descargable para el usuario individual</u> y realice estos pasos para configurar ACL descargable para el grupo en Cisco ACS seguro.

En este ejemplo, el usuario de VPN "Cisco" de IPsec pertenece al Muestra-grupo.

El usuario **Cisco del Muestra-grupo** autentica con éxito, y el servidor de RADIUS envía una lista de acceso transferible al dispositivo de seguridad. El usuario "Cisco" puede tener acceso solamente al servidor de 10.1.1.2 y niega el resto del acceso. Para verificar el ACL, refiera a <u>ACL</u> <u>descargable para el usuario/la sección de grupo</u>.

 En la barra de navegación, haga clic a los usuarios y la identidad salva > los grupos de la identidad, y el tecleo crea para crear a un nuevo



2. Proporcione a un nombre del grupo (Muestra-**grupo**), y el tecleo **somete**.

General	Rampla Group		
Descriptio	n:		
o Parent:	All Groups	Select	
= Required	fields		

3. Elija los **almacenes de la Identificación del usuario > identidad interna salva >** los **usuarios**, y selecciona al usuario **Cisco**. El tecleo **corrige** para cambiar la membresía del grupo de este

sternal Users				Showing 1-1 of 1 50 💌 g	er page Go
Filter:	Match #	•			
🕫 Status	User Name	Identity Group	Description		
9 0	01800	Al Oroups			

4. Tecleo **selecto** al lado del grupo de la identidad

Description:	cisco	Status; Enabled 🗾 🥹	
Identity Group:	All Groups	Selept	
er Information	iditional identity attrib	butes defined for user records	
eation Modifica	tion Information		
Date Created: 1	Wed Feb 15 16:32:2	5 IST 2012	
Date Modified: V	Wed Feb 15 16:32:2	5 IST 2012	
= Required field	le	5151 2012	

5. Seleccione al grupo creado recientemente (es decir, Muestra-**grupo**), y haga clic la **AUTORIZACIÓN**.

isco Secure ACS - Mozilla Firefox
192.168.26.51 https://192.168.26.51/acsadmin/IdentityGroupsLPInputAction.do
Identity Groups
Filter: Match if. Go 🗢
Name Description C * All Groups Identity Group Root
Sample-Group
Create Duplicate File Operations Export
LQK Cancel Help

6. Haga clic en Submit

ocherai			
🧧 Name:	cisco	Status	Enabled 👱 😔
Description:			
🗧 Identity Group	All Groups:Samp	le-Group	Select
User Information			
There are no a	dditional identity at	tributes defined for u	user records
20,000,000,000	an a an air		
Creation/Modific:	ation Information		
Date Created	Wed Feb 15 16:32	:25 IST 2012	
Date created.			
Date Modified:	Wed Feb 15 16:32	:25 IST 2012	
Date Modified: Date Enabled:	Wed Feb 15 16:32 Wed Feb 15 16:32	:25 IST 2012 :25 IST 2012	
Date Modified: Date Enabled: = Required fiel	Wed Feb 15 16:32 Wed Feb 15 16:32 <mark>Js</mark>	:25 IST 2012 :25 IST 2012	
Date Modified: Date Enabled: # = Required fiel	Wed Feb 15 16:32 Wed Feb 15 16:32 Js	:25 IST 2012 :25 IST 2012	
Date Modified: Date Enabled: F = Required field	Wed Feb 15 16:32 Wed Feb 15 16:32 ds	:25 IST 2012 :25 IST 2012	

7. Elija las políticas de acceso > los servicios del acceso > el acceso a la red > la autorización del valor por defecto, y el tecleo crea para crear una nueva

andan	d Poli	 Access 1 cvi Excent 	tion Policy	betault Network Acc	ess > Authorization				
letwor	k Acr	cess Auth	orization P	Policy					
itter:	Stat.	us.	*	Match if Equals	Enabled	Clear Fa	ter Go 🗢		
	Г	Status	Name	NDGLocation	Conditions System UserName	Identity Group	Results Authorization Profiles	Hit Count	
		No data	to display						
-	Г	Default		If no rules define	d or no enabled rule n	natches.	Permit Access	0	
++	Г	Default	e[•] E	If no rules define	d or no enabled rule n Xéova to	natches.	Permit Access	0	Customize Hit Cour
ti Trente	- 	Default Duplicat	e(▼ _ E	If no rules define	d or no enabled rule n Move to	natches.	Permit Access	0	Custombe Hit Cour

8. Asegúrese de que el checkbox al lado del **grupo de la identidad** esté controlado, y haga clic **selecto**.

Support of the suppor	rerox		
192.168.26.51 https://1	92.168.26.51/ac	sadmin/PolicyInput	Action.do
General			
Name: Rule-1	Stat	us: Enabled	
The Custo policy cond	mize button ir ditions and re	n the lower righ sults are avail	nt area of the policy rules screen controls which able here for use in policy rules.
Conditions	[450/		
NDG:Location:	LAND		
V Identity Group	lin	-	Select
		K C N	defined in multiple profiles will use the value from the first profile defined.
Select Deselec	5	*	

9. Elija al Muestra-grupo, y haga clic la

AUTORIZACIÓN.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDevceGroupLPInputAction.do?contextData.externalFilter=IdentityGroup=IdentityGroup=	the C
Network Device Groups	C BOOM STATE
Filter: Match if: Go 🗢	
Name Description	
C * All Groups Identity Group Root	
C Sample-Group	
Create Duplicate Edit Delete File Operations Export	
OK Cancel	Help
- Le	weip

10. Haga clic **selecto**, en la sección de los perfiles de la autorización.

o Secure ACS - Mozilla F	irefox			and the second second	
192.168.26.51 https://1	92.168.26.51/acs	admin/PolicyInput	Action do		REMONANCE PRO
General Name: Rule-1 The Custo policy cond	Statu mize button in ditions and res	s: Enabled the lower righ sults are avail	■ ● ht area of the policy rule able here for use in pol	es screen controls wi icy rules.	nich
Conditions	-ANY-				
System:UserName	-ANY-				
Identity Group:	in	II G	roups:Sample-Group	Select	
			You may select multiple a defined in multiple profile profile defined.	uthorization profiles. Attr s will use the value from	butes the first
Select Deselec	1	×			
DK Cancel					Hel

11. El tecleo **crea** para crear un nuevo perfil de la autorización.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.de	
Authorization Profiles	Showing 1-2 of 2 50 💌 per pageGo
Filter: Match if: 00 💌	
T Name Description	
DerwAccess	
Permit Access	
Creans, Duplicate Edit Delete	Page 1 of 1
OK Cancel	Help

12. Proporcione a un nombre para el **perfil de la autorización**. **El ejemplo de perfil** es el nombre usado en este

ejemplo.	Internet and a second second second
Cisco Secure ACS - Mozilla Firefox	2 Construction of the second sec
192,168,26.51 https://192,168,26.51/acsadmin/NetworkAccessLPInputAction.do	
General Common Tasks RADIUS Attributes	
Name: Sample-Profile	
Description:	
Required fields	
5	
- 10	
Submit Cancel	

13. Elija la tabulación **común de las tareas**, y seleccione los **parásitos atmosféricos de la** lista desplegable para **ACL descargable el nombre**. Elija el **DACL** creado recientemente **(la**

muestra - DACL) de la lista desplegable de

valores.

General Common Tasks	RADIUS A	tribut	es	
ACLS	1			
Downloadable ACL Name:	Static	٠	Sample-DAQ	3
Filter-ID ACL:	Not in Use	٠		
Proxy ACL:	Not in Use	-		
Voice VLAN				
Permission to Join:	Not in Use	-		
VLAN				
VLAN ID/Name:	Not in Use	*		
Reauthentication				
Reauthentication Timer:	Not in Use	٠		
Maintain Connectivity during Reauthentication:	1			
QOS				
Input Policy Map:	Not in Use			
Output Policy Map:	Not in Use	*		
802.1X-REV				
LinkSec Security Policy.	Not in Use	*		
URL Redirect				
		a line	et also he defined	

14. Haga clic en Submit

General Common Tasks	RADIUS At	ributes	1		
ACLS					1
Downloadable ACL Name:	Static		Value Sample-DACL	 *	
Filter-ID ACL:	Not in Use	-			
Proxy ACL:	Not in Use	-			
Voice VLAN	1	-			
Permission to Join:	Not in Use	-			
VLAN		_			
VLAN ID/Name:	Not in Use	*			
Reauthentication		_			
Reauthentication Timer:	Not in Use	٠			
Maintain Connectivity during Reauthentication:	1				
QOS					
Input Policy Map:	Not in Use	*			
Output Policy Map:	Not in Use	*			
802.1X-REV					
LinkSec Security Policy:	Not in Use	•			
URL Redirect					
the an a LIDI is shafing a day i	Dadiract on AC	must	t sich he defined		

15. Elija el ejemplo de perfil del perfil de la autorización creado anterior, y haga clic la

AUTORIZACIÓN.

Cisco Secure ACS - Mozilla Firefox	X
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessi/PinputAction.do	合 ()
Authorization Profiles	Showing 1-3 of 3 50 🗾 per pageGo
Filter: Match if. Oo 🔻	
Name Description	
DerwAccess	
Permit Access	
Sample-Proble	
Create Duplicate Edit Delete	Page 1 of 1 💌 💓
OK Cancel	Help

16. Click

OK.

o Secure ACS - Mozilla Fi	refox				
192.168.26.51 https://19	2.168.26.51/acsadm	in/PolicyInp	utAction.do	The Party of the P	MAUERN
General Name: Rule-1 The Custon policy cond	Status: Status: Nize button in the itions and result	Enabled e lower rig s are ava	ght area of the policy rules	s screen controls which y rules.	
Conditions				5	
NDG:Location:	-ANY-				
System:UserName:	-ANY-				
Identity Group:	in	- All	Groups:Sample-Group	Select	
Sample-Frome			You may select multiple aut defined in multiple profiles profile defined.	horization profiles. Attribute will use the value from the t	s Arst
Select Deselect	1				
Cancel					Hel

17. Verifique que **Rule-1** esté creado con el Muestra-**grupo del** grupo de la identidad como la condición y el **ejemplo de perfil** como el resultado. Haga clic los **cambios de la salvaguardia**.

two	rk Acc	cess Auth	erization	Policy						
Her:	Statu	JŚ	-	Match if: Equal	s 💌 Enabled	Clear Filter Go	*			
	Г	Status	Name	NDG:Location	Condition System UserName	s Identity Group	Results Authorization Profiles	Hit Count		
1	C	0	Rule-1	-ANS	-ANY-	in All Oroups:Sample-Group	Sample-Profile	0]	
	C C	Defect	Rule-1	-ANF	-ANF	in All Oroups:Sample-Oroup	Sample-Profile	0]	

Configure ACS para ACL descargable para un grupo de dispositivos de red

Complete los pasos 1 a 12 del configurar ACS para ACL descargable para el usuario individual y

realice estos pasos para configurar ACL descargable para un grupo de dispositivos de red en Cisco ACS seguro.

En este ejemplo, el cliente RADIUS (ASA) pertenece al grupo de dispositivos de red que la petición de la autenticación VPN-Gateways.The VPN que viene del ASA para el usuario "Cisco" autentica con éxito, y el servidor de RADIUS envía una lista de acceso transferible al dispositivo de seguridad. El usuario "Cisco" puede tener acceso solamente al servidor de 10.1.1.2 y niega el resto del acceso. Para verificar el ACL, refiera a <u>ACL descargable para el usuario/la sección de grupo</u>.

 Elija los recursos de red > los grupos de dispositivos de red > el tipo de dispositivo, y el tecleo crea para crear a un nuevo grupo de dispositivos de red

🚭 My Workspace	Network Resources > Network Device Groups > Device Type
💱 Network Resources	Network Device Groups
Network Device Groups Location	Filter: Match If. Go 💌
Network Devices and AAA Cilents Default Network Device	Name Description
External Proxy Servers	I All Device Types All Device Types
Users and Identity Stores	
Se Policy Elements	
🔂 Access Policies	
Monitoring and Reports	
🍓 System Administration	
	Create Duplicate Edit Delete File Operations Export

2. Proporcione a un nombre de **grupo de dispositivos de red** (**gatewayes de VPN** en este ejemplo), y el tecleo

Device Group) - General	
🧒 Name:	VPN-Gateways	
Descriptio	in:	
👩 Parent:	All Device Types	Select
= Required	Ifields	

 Elija los recursos de red > los dispositivos de red y a los clientes AAA, y seleccione al cliente muestra-asa RADIUS creado anterior. El tecleo corrige para cambiar la calidad de miembro de grupo de dispositivos de red de este cliente RADIUS (asa).

		Match if:		00 🔻		
me		IP Address	Description	NDG:Location	NDG:Device Type	
mpie-er	18	192108-2610/02		All Locations	All Device Types	
	me mpie-er	me 🔺	Match if. Me IP Address Mote-esa 192 19526 1972	Match if, Match if, PAddress Description mote-sta 192.105.26.1302	Match If: Go Match If: IP Address Description NDG:Location numeress 192,195,26,1972 Al:Locations	Match if: Oo Match if: Oo Match if: Oo Match if: Oo Match if: Oo Match if: Oo Match if: Oo Match if: Oo Match if: Oo

4. Tecleo **selecto** al lado del tipo de

Description:	sample-asa	
etwork Device	Groups	
ocation	All Locations	Select
Device Type	All Device Types	Select
© Single IP: 192.16	P Address C IP Range(s) By Mask C IP Range(s)	Authentication Options ► TACACS+ ► RADIUS ►

5. Seleccione el grupo de dispositivos de red creado recientemente (que es **gatewayes de** VPN), y haga clic la AUTORIZACIÓN.

Cisco Secure ACS - Mozilla Firefox	×
192-168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do	合
Network Device Groups	
Filter: Match if: Go 💌	
Name Description C *All Device Types All Device Types	
C VPN-Gateways	
Create Duplicate Edit Delete File Operations Export	
9K Cancel	Help

6. Haga clic en Submit

Name: Description:	sample-asa	
Network Device	Groups	
Location	All Locations	Select
Device Type	All Device Types: VPN-Gateways	Select
G Single	P Address C IP Range(s) By Mask C IP Range(s)	Authentication Option ► TACACS+ Г ► RADIUS Γ

7. Elija las políticas de acceso > los servicios del acceso > el acceso a la red > la autorización del valor por defecto, y el tecleo personaliza.

etwor	k Acc	ess Auth	orization	Policy				
iter.	Statu	IS		Match if Equals Finabled	Clear Filter Go 🔻			
	C	Status	Name	Conditions NDG:Location System:UserName identity	Group .	Results Authorization Profiles	Hit Count	
		Default		If no rules defined or no enabled rule matches.	F	ermit Access	0	
eate	.1-	Dunlicat	0E	dit Delete Move to				Sustemize Hit C

8. Movimiento NDG: Tipo de dispositivo de la sección disponible a la sección seleccionada, y AUTORIZACIÓN del

tecleo.



9. El tecleo crea para crear una nueva

	K Aci	cess Auti	norization	Policy					
Filter:	Stat	15	-	Match if Equal	s 💽 Enabled	Clear Filter Go	*		
	F	Status	Name	NDG:Location	System/UserName	Conditions Identity Group	NDO:Device Type	Results Authorization Profiles	Hit Count
-		Default		lf no rules define	ed or no enabled rule r	natches.		PermitAccess	0

10. Asegúrese de que el checkbox al lado de **NDG:** Seleccionan y elige al **tipo de dispositivo adentro de la** lista desplegable. Tecleo

selecto.

o Secure ACS - Mozilla Fi	refox	
General	22:168.26.51/acsadmin/PolicyInputAction.do	4.021 (29
Name: Rule-1 The Custor policy cond	Status: Enabled Status: Enable	
Conditions	LANN	
System:UserName	-ANY-	
Identity Group:	-ANY-	
NDG:Device Type:	in Select	
Authorization Profiles:	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the fi profile defined.	rst
Select Deselect		
K Cancel		Hel

11. Elija los **gatewayes de VPN del** grupo de dispositivos de red creados anterior, y haga clic la **AUTORIZACIÓN**.

Cisco Secure ACS - Mozilla Firefox	×
192,168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFilter=Device 7/pe=Device 7	/pe=string 🏠
Network Device Groups	COLLE OF SHALL STRATE
Filter: Match if: Go 💌	
Name Description	
C * All Device Types All Device Types	
C <u>VPN-Gateways</u>	
Create Duplicate Edit Datate I File Operations Dipart	
Create Dupincate COIL Delete I File Operations Export	
OX Cancel	Help
	1071

12. Haga clic selecto.

o Secure ACS - Mozilla Fi	refox	
192.168.26.51 https://19	2.168.26.51/acsadmin/PolicyInputAction.do	
General Name: Rule-1	Status: Enabled 💌 😔	
policy cond	nize button in the lower right area of the policy rules screen controls which itions and résults are available here for use in policy rules.	
Conditions	LANY	
System: LiserName	-ANY-	
Identity Group	-ANY-	
NDG:Device Type	in All Device Types VPN-Gateways Select	
Authorization Profiles:	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
OK Cancel		Не

13. El tecleo **crea** para crear un nuevo perfil de la autorización.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do	
Authorization Profiles	Showing 1-2 of 2 50 💌 per pageGo
Filter: Match if: 30 👻	
T Name - Description	
DerwAccess	
Permit Access	
Create, Duplicate Edit Delete	Page 1 of 1
OK Cancel	Help
	100

14. Proporcione a un nombre para el **perfil de la autorización**. **El ejemplo de perfil** es el nombre usado en este

ejemplo.	Internet and a second second second
Cisco Secure ACS - Mozilla Firefox	2 Construction of the second sec
192,168,26.51 https://192,168,26.51/acsadmin/NetworkAccessLPInputAction.do	
General Common Tasks RADIUS Attributes	
Name: Sample-Profile	
Description:	
Required fields	
5	
- 10	
Submit Cancel	

15. Elija la tabulación **común de las tareas**, y seleccione los **parásitos atmosféricos de la** lista desplegable para ACL descargable el nombre. Elija el **DACL** creado recientemente

(muestra-DACL) de la lista desplegable de

valores.

General Common Tasks	RADIUS A	ttribut	es	
ACLS	1			
Downloadable ACL Name:	Static	٠	Sample-DAQ	×
Filter-ID ACL:	Not in Use	٠		
Proxy ACL:	Not in Use	-		
Voice VLAN				
Permission to Join:	Not in Use	-		
VLAN				
VLAN ID/Name:	Not in Use	*		
Reauthentication				
Reauthentication Timer:	Not in Use	*		
Maintain Connectivity during Reauthentication:	1			
QOS				
Input Policy Map:	Not in Use	-		
Output Policy Map:	Not in Use	*		
802.1X-REV				
LinkSec Security Policy.	Not in Use	*		
URL Redirect When a URL is defined for f	Redirect an AC	L mu	ist also be defined	
LIPI for Podirost	Not in Lleo	-		

16. Haga clic en Submit

General Common Tasks	RADIUS At	ributes			
ACLS					
Downloadable ACL Name:	Static	Value Sa	imple-DACL	*	
Filter-ID ACL:	Not in Use				
Proxy ACL:	Not in Use	*			
Voice VLAN		_			
Permission to Join:	Not in Use	-			
VLAN					
VLAN ID/Name:	Not in Use	*			
Reauthentication					
Reauthentication Timer:	Not in Use	*			
Maintain Connectivity during Reauthentication:	1				
QOS					
Input Policy Map:	Not in Use	-			
Output Policy Map:	Not in Use	*			
802.1X-REV					
LinkSec Security Policy:	Not in Use	*			
URL Redirect					
When a LIRL is defined for I	Redirect an AC	must also be det	fined		

17. Seleccione el ejemplo de perfil creado anterior, y haga clic la

AUTORIZACIÓN.

wtho	rization Profiles	Showing 1-4 of 4 50 💌 per page 🧾
Filter:	Match if. 00 🔻	
	Name Description	
	DenvAccess	
	Filter-Id	
	Permit Access	
2	Sample-Profile	

18. Click

o Secure ACS - Mozilla Fir	efox Παραγολικά το αναγγοριστικό το το διαδολογιστικού του	-
192.168.26.51 https://19	:168.26.51/acsadmin/PolicyInputAction.do	-
General Name: Rule-1 The Custom	Status: Enabled 💽 💿	
policy condi	tions and results are available here for use in policy rules.	
NDG Location	-ANY-	
System:UserName	-ANY-	
Lidentity Group:	-ANY-	
NDG:Device Type:	in All Device Types VPN-Gateways Select	
Results Authorization Profiles: Sample-Profile	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first	t
Select Deselect	profile defined.	
Cancel		Hel

 Verifique que Rule-1 esté creado con los gatewayes de VPN como NDG: Tipo de dispositivo como condición, y ejemplo de perfil como resultado. Cambios de la salvaguardia del

etwo	rk Ac	cess A	thorization	Policy						
itter:	State	us	-	Match if Equa	Is 💌 Enabled	Clear F	itter Ga 🔫			
	-	Status	Name	NDGLocation	System UserName	Conditions Identity Group	NDG:Device Type]	Results Authorization Profiles	Hit Count
1	Γ.	0	Rule-1	-ANY-	-ANY-	-ANY	in All Device Types VPN	+O alleways	Sample-Profile	4
	Г	Defa	8	If no rules defin	ed or no enabled rule	matches.			Permit Access	0

Configure las configuraciones IETF RADIUS para un grupo de usuarios

Para descargar un nombre para una lista de acceso que usted ha creado ya en el dispositivo de seguridad del servidor de RADIUS cuando un usuario autentica, configure el atributo filtroidentificación IETF RADIUS (número de atributo 11):

filter-id=acl_name

El usercisco del Muestra-grupo autentica con éxito, y el servidor de RADIUS descarga un nombre ACL (nuevo) para una lista de acceso que usted ha creado ya en el dispositivo de seguridad. El usuario "Cisco" puede tener acceso a todos los dispositivos que estén dentro de la red del ASA **excepto el** servidor de 10.1.1.2. Para verificar el ACL, vea la sección Filtro-<u>identificación ACL</u>.

Según el ejemplo, el **nuevo** nombrada ACL se configura para filtrar en el ASA:

```
access-list new extended deny ip any host 10.1.1.2
access-list new extended permit ip any any
```

Estos parámetros aparecen solamente cuando éstos son verdades. Usted ha configurado:

- Cliente AAA para utilizar uno de los protocolos RADIUS en configuración de red
- Un perfil de la autorización con la Filtro-identificación RADIUS (IETF) se selecciona bajo

sección del resultado de la regla en el Acceso-servicio.

Los atributos de RADIUS se envían como perfil para cada usuario de ACS al cliente AAA solicitante.

Los pasos completos 1 a 6 y 10 a 12 del <u>configurar ACS para ACL descargable para el usuario</u> <u>individual</u>, seguido por los pasos 1 a 6 del <u>configurar ACS para ACL descargable para el grupo</u>, y realizan estos pasos en esta sección para configurar la Filtro-identificación en Cisco ACS seguro.

Para configurar las configuraciones del **atributo de RADIUS IETF** para aplicarse como en el perfil de la autorización, realice estos pasos:

1. Elija los **elementos de la directiva >** la **autorización y los permisos >** los **perfiles del acceso a la red >** de la **autorización**, y el tecleo **crea** para crear un nuevo perfil de la

	auon Promes	F.		Showing 1-2 of 2 50 💌 per page
ilter:	1	Match if:	💌 Ga 🔻	
N	ame 4	Description		
P	ermit Access			
3	ample-Profile	t.		

2. Proporcione a un nombre para el **perfil de la autorización**. La Filtro-identificación es el nombre del perfil de la autorización elegido en este ejemplo con el fin de simplificar.

Seneral C	ommon Tasks RADIUS Atti	ibutes
Name:	Filter-Id	
Descriptio	n:	
= Required	ïelds	

 Haga clic la tabulación común de las tareas, y elija los parásitos atmosféricos de la lista desplegable para la Filtro-identificación ACL. Ingrese el nombre de la lista de acceso como nuevo en el campo de valor, y el tecleo somete.

General Common Tasks	RADIUS At	tribute	s
ACLS Downloadable ACL Name:	Not in Use	•	
Filter-ID ACL:	Static	¥	Ø Value new
Proxy ACL:	Not in Use	٠	
Voice VLAN			
Permission to Join:	Not in Use	-	
VLAN			
VLAN ID/Name:	Not in Use	+	
Reauthentication			
Reauthentication Timer:	Not in Use	-	
Maintain Connectivity during Reauthentication: QOS			
Input Policy Map:	Not in Use	+	
Output Policy Map:	Not in Use	-	
802.1X-REV			
LinkSec Security Policy:	Not in Use	-	
URL Redirect When a URL is defined for R	edirect an AC	L mus	t also be defined
URL for Redirect	Not in Use	+	
URL Redirect ACL:	Not in Use	+	
= Required fields			

4. Elija las políticas de acceso > los servicios del acceso > el acceso a la red > la autorización del valor por defecto, y el tecleo crea para crear una nueva

oess P	folicies :	Access S	Services > 1	Detault Network Acc	ess > Authorization				
anda	rd Poli	cyl Excest	tion Pelicy						
ietwo	ork Acc	cess Auth	orization	Policy	State Management				
Filter	State	18	*	Match if: Equals	s 💌 Enabled	ClearFiter 00	-		
	Г	Status	Name	NDG Location	Condition System:UserName	is Identity Group	Results Authorization Profiles	Hit Count	
		No data	to display						
-	Г	Default		If no rules define	ed or no enabled rule r	natches.	Permit Access	0	
-	e. 1+	Duplicat		dit Delete	Move to				Customize Hit Cour

5. Asegúrese de que el checkbox al lado del **grupo de la identidad** esté controlado, y haga clic **selecto**.

100 100 00 01 100	0 160 DC E1	and up the loss of the set of the	ALL NOT A CARDINE ALL ADDRESS OF ADDRESS OF ALL ADDRESS OF ALL ADDRESS OF ALL ADD	NO CHE
192.168.26.51 https://19	2.168.26.51/a	sadmin/PolicyInputAction.do	TARA BURNING STRATE MARK - ANT CRIMIN	-
General				
Name: (Rule-1	Stal	tus: Enabled 🔄 🔮		
The Custon	nize button i	n the lower right area o	of the policy rules screep controls which	
policy cond	itions and re	esults are available her	re for use in policy rules.	
C				
NDG:Location:	-ANY-			
System:LicerName	-AND-			
V Identity Group:	lin	-	Select	
Desutte	1			
Autorization Deathan				
Authorization Profiles.				
		-		
		Ybu may	/ select multiple authorization profiles. Attributes	
		defined	in multiple profiles will use the value from the fin	st
		profile d	efined.	
		2		
1		×		
Select Deselect	1			
	-			

6. Elija al Muestra-**grupo**, y haga clic la AUTORIZACIÓN.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFiker=IdentityGroup=IdentityGroup=Stir *	
Network Device Groups	
Filter: Match if: Go 🗸	
Name Description	
ICK Cancel	

7. Haga clic **selecto** en la sección de los perfiles de la autorización.

Secure ACS - Mozilla Fi	refox		LAND NEWSFILM PROPERTY AND	Not Name of P
192.168.26.51 https://19	2.168.26.51/acsad	Min/PolicyInpi	rAction.do	
General				
Name: Rule-1	Status:	Enabled	1 •	
The Custor policy cond	nize button in th itions and resul	e lower riç ts are ava	ht area of the policy rules screen controls w lable here for use in policy rules.	hich
Conditions				
NDG:Location:	-ANY-			
System:UserName:	-ANY-			
Identity Group:	in	All	Groups:Sample-Group Select	
Authorization Profiles:		× ×	You may select multiple authorization profiles. Att defined in multiple profiles will use the value from profile defined.	ributes n the first
Select Deselect	1	*		
				1000

8. Elija la Filtro-**identificación del** perfil de la autorización creada anterior, y haga clic la **AUTORIZACIÓN**.

Cisco Secure ACS - Mozilla Firefox	X
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do	(A)
Authorization Profiles	Showing 1-4 of 4 50 💌 per page Go
Filter: Match if. 💽 Go 🗢	
T Name Description	
DerwAccess	
Eilter-Id	
Permit Access	
Sample-Profile	
Create Duplicate Edit Delete	Page 1 of 1
<u>gk</u> Cancel	Help

9. Click OK.

Secure ACS	5 - Mozilla Fii	efox			
192.168.26.5	51 https://19	2.168.26.51/ə	sadmin/Policy1r	nputAction.do	
General					
Name: Rule	e-1	Stat	tus: Enabled		
Conditions	The Custom policy condi	nize button i tions and re	n the lower esults are av	right area of the policy rule vallable here for use in poli	es screen controls which icy rules.
NDG:Lo	cation:	-ANY-			
System	UserName:	-ANY-			
V Identity	Group:	in	- A	II Groups:Sample-Group	Select
Select	Deselect]	K CON	defined in multiple profile: profile defined.	s will use the value from the first
K Cance	a 1				He

10. Verifique que **Rule-1** esté creado con el Muestra-**grupo del** grupo de la identidad como la condición y Filtro-**identificación** como resultado. Haga clic los **cambios de la salvaguardia**.

30900	rk Aci	cess Aut	orization	Policy					
iller	Statu	US	*	Match if Equal	s 💌 Enabled	Clear Filter 00	♥		
	Г	Status	Name	NDG:Location	Conditions System UserName	s Identity Group	Results Authorization Profiles	HitCount	
1		0	Rule-1	-ANY-	-ANY	in All Groups:Sample-Group	Filter-Id	0	
-	F	Certault		f no rules define	d or no enabled rule m	natches.	PermitAccess	0	

Configuración de Cliente Cisco VPN

Conecte con Cisco ASA con el Cliente Cisco VPN para verificar que el ASA está configurado con éxito.

Complete estos pasos:

- 1. Elija el Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN.
- 2. Haga clic **nuevo** para lanzar la nueva ventana de la entrada de la conexión VPN del crear.

∂ status: Disconnected ¥PN Client - ¥ersio	n 5.0.07.0410	_ 🗆 ×
Connection Entries Status Certificates Log Op	tions Help	
Connect New Import Modify) Delete	cisco
Connection Entry	Host	Transport
Not connected.		

3. Complete los detalles de su nueva conexión:Ingrese el nombre del Entrada de conexión junto con una descripción.Ingrese el IP address exterior del ASA en el rectángulo del host.Ingrese el nombre de grupo de túnel VPN (Cisco-túnel) y la contraseña (clave previamente compartida - cisco123) como está configurado en el ASA.Click

				aluali
Description:				CISCO
Host:	172.16.1.1			
Authentication	Transport E	ackup Servers	Dial-Up	
Group Authen	tication		C Mutual Gro	oup Authenticatio
Name:	Cisco-Tunn	el		
Password:	*****			
Confirm Passw	ord: *******			
C. Cottificate Aut	hantiastian			
Namer	nerication	*	Í	
Send CA C	ertificate Chain	1		
00110010	oranioado cariani			

4. Haga clic la conexión que usted quiere utilizar, y el tecleo **conecta de la** ventana principal del cliente

5. Cuando está incitado, ingrese el nombre de usuario cisco y la contraseña **cisco123** como está configurado en el ASA para la autenticación, y haga clic la **AUTORIZACIÓN** para conectar con la red

The server has reque authentication.	sted the following	information to complete	the user
uluulu, Username:	cisco		
Password:			
		OK	Canad

remota.
6. Una vez que la conexión se establece con éxito, elija las estadísticas del menú del estatus para verificar los detalles del

Connection Entrie	Status Certificates Log Optio	ons Help	
in .	Ratistics Ctrl+5		ahah
Connect	N N	Delete	CISCO
Connection Entrie	s Reset Stats		
0	nnection Entry	Host	Transport
Sa	mple-Connection	172.16.1.1	IPSec/UDP

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la **salida del comando show**.

Comandos show crypto

 show crypto isakmp sa: muestra todas las asociaciones actuales de seguridad IKE (SA) de un par.

```
ciscoasa# sh crypto isakmp sa
 IKEv1 SAs:
    Active SA: 1
     Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
 Total IKE SA: 1
 1
     IKE Peer: 172.16.1.50
     Type : user
                             Role : responder
                             State : AM_ACTIVE
     Rekey : no
 ciscoasa#

    muestre ipsec crypto sa - Muestra las configuraciones usadas por el SAs actual.

 ciscoasa# sh crypto ipsec sa
 interface: outside
     Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
        172.16.1.1
       local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
       remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
       current_peer: 172.16.1.50, username: cisco
       dynamic allocated peer ip: 10.2.2.1
       #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
       #pkts decaps: 333, #pkts decrypt: 333, #pkts verify: 333
       #pkts compressed: 0, #pkts decompressed: 0
       #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
       #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
       #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly:
         Ω
       #send errors: 0, #recv errors: 0
       local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.1.50/0
       path mtu 1500, ipsec overhead 74, media mtu 1500
       current outbound spi: 9A06E834
       current inbound spi : FA372121
     inbound esp sas:
       spi: 0xFA372121 (4197916961)
          transform: esp-aes esp-sha-hmac no compression
          in use settings ={RA, Tunnel, }
          slot: 0, conn id: 16384, crypto-map: SYSTEM DEFAULT_CRYPTO_MAP
          sa timing: remaining key lifetime (sec): 28678
          IV size: 16 bytes
          replay detection support: Y
          Anti replay bitmap:
           OxFFFFFFFF OxFFFFFFF
     outbound esp sas:
```

ACL descargable para el usuario/el grupo

Verifique ACL descargable para el usuario Cisco. Los ACL se descargan del CSACS.

Filtro-identificación ACL

La Filtro-identificación [011] ha solicitado el grupo - filtran al Muestra-grupo, y a los usuarios del grupo según el ACL (nuevo) definido en el ASA.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración. También se muestra un ejemplo de salida del debug.

Nota: Para más información sobre el Acceso Remoto IPsec VPN del troubleshooting, refiera a <u>la</u> mayoría de las soluciones comunes del troubleshooting de IPsec VPN L2L y del Acceso Remoto.

Borre las asociaciones de seguridad

Cuando usted resuelve problemas, asegúrese de borrar el SAs existente después de que usted realice un cambio. En el modo privilegiado del PIX, utilice estos comandos:

- borre ipsec sa del [crypto] Suprime el IPSec activo SAs. La palabra clave crypto es opcional.
- borre isakmp sa del [crypto] Suprime el IKE activo SAs. La palabra clave crypto es opcional.

Comandos para resolución de problemas

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la **salida del comando show**.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

- ponga a punto el ipsec crypto 7 Visualiza los IPSec Negotiations de la fase 2.
- isakmp crypto 7 de la depuración Visualiza negociaciones ISAKMP de la fase 1.

Información Relacionada

- Página de Soporte de Cisco ASA 5500 Series Adaptive Security Appliances
- Referencias del comando del Dispositivos de seguridad adaptable Cisco ASA de la serie
 <u>5500</u>
- <u>Cisco Adaptive Security Device Manager</u>
- Página de soporte de la Negociación IPSec/Protocolos IKE
- Página de soporte del Cliente Cisco VPN
- <u>Cisco Secure Access Control System</u>
- Pedidos los comentarios (RFC)
- Soporte Técnico y Documentación Cisco Systems