ASA 8.3 e mais atrasado: Autorização RADIUS (ACS 5.x) para a utilização do acesso VPN ACL baixável com CLI e exemplo da configuração ASDM

Índice

Introdução **Pré-requisitos** Requisitos Componentes Utilizados Convenções Informações de Apoio Configurar Diagrama de Rede Configurar o acesso remoto VPN (IPsec) Configurar o ASA com CLI Configurar ACS para ACL baixável para o usuário individual Configurar ACS para ACL baixável para o grupo Configurar ACS para ACL baixável para um grupo de dispositivo de rede Configurar ajustes do RADIUS IETF para um grupo de usuário Configuração de Cisco VPN Client Verificar Comandos show crypto ACL baixável para o usuário/grupo ID de filtro ACL Troubleshooting Cancele associações de segurança Comandos para Troubleshooting Informações Relacionadas

Introdução

Este documento descreve como configurar o mecanismo de segurança para autenticar usuários para o acesso de rede. Desde que você pode implicitamente permitir autorizações RADIUS, este original não contém nenhuma informação sobre a configuração da autorização RADIUS na ferramenta de segurança. Ela fornece informações sobre como o mecanismo de segurança lida com as informações da lista de acesso recebidas dos servidores RADIUS.

Você pode configurar um servidor Radius para transferir uma lista de acessos à ferramenta de

segurança ou um nome da lista de acessos na altura da autenticação. O usuário é autorizado fazer somente o que é permitido na lista de acessos USER-específica.

As Listas de acesso carregável são os meios os mais escaláveis quando você usa o Serviço de controle de acesso Cisco Secure (ACS) para fornecer as Listas de acesso apropriadas para cada usuário. Para obter mais informações sobre dos recursos de lista de acesso carregável e do Cisco Secure ACS, refira <u>configurar um servidor Radius para enviar as listas de controle de acesso carregável e IP carregável ACL</u>.

Refira <u>ASA/PIX 8.x: Autorização RADIUS (ACS) para a utilização do acesso de rede ACL baixável</u> <u>com CLI e exemplo da configuração ASDM</u> para a configuração idêntica em Cisco ASA com versões 8.2 e anterior.

Pré-requisitos

Requisitos

Este original supõe que a ferramenta de segurança adaptável (ASA) é plenamente operacional e configurada para permitir que o Cisco Adaptive Security Device Manager (ASDM) ou o CLI façam alterações de configuração.

Nota: Refira <u>permitir o acesso HTTPS para o ASDM</u> a fim permitir que o dispositivo seja configurado remotamente pelo ASDM ou pelo Shell Seguro (ssh).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software 8.3 de Cisco ASA e mais atrasado
- Versão ASDM Cisco 6.3 e mais atrasado
- Versão Cliente VPN Cisco 5.x e mais tarde
- Cisco Secure ACS 5.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as <u>Convenções de Dicas Técnicas da Cisco</u> para obter mais informações sobre convenções de documentos.

Informações de Apoio

Você pode usar IP carregável ACL a fim criar grupos de definições de ACL que você pode aplicar a muitos usuários ou grupos de usuário. Estes grupos de definições de ACL são chamados índices ACL.

O IP carregável ACL opera esta maneira:

- 1. Quando ACS concede um acesso de usuário à rede, ACS determina se um IP carregável ACL está atribuído ao perfil da autorização na seção do resultado.
- Se ACS encontra um IP carregável ACL que esteja atribuído ao perfil da autorização, ACS envia um atributo (como parte da sessão do usuário, no pacote de aceitação acesso do RAIO) que especifica o ACL nomeado, e a versão do ACL nomeado.
- 3. Se o cliente de AAA responde que não tem a versão atual do ACL em seu esconderijo (isto é, o ACL é novo ou mudou), ACS envia o ACL (novo ou actualizado) ao dispositivo.

O IP carregável ACL é uma alternativa à configuração dos ACL no atributo [26/9/1] do Cisco-avpair de Cisco do RAIO de cada usuário ou grupo de usuário. Você pode criar um IP carregável ACL uma vez, dá-lhe um nome, e atribui-o então o IP carregável ACL a todo o perfil da autorização se você provê seu nome. Este método é mais eficiente do que se você configura o atributo do Cisco-av-pair de Cisco do RAIO para o perfil da autorização.

Quando você incorpora as definições de ACL à interface da WEB ACS, não use a palavra-chave ou as entradas de nome; em todos respeitos restantes, sintaxe e semântica padrão de comando acl do uso para o cliente de AAA em que você pretende aplicar o IP carregável ACL. As definições de ACL que você incorpora em ACS compreendem uns ou vários comandos acl. Cada comando acl deve estar em uma linha separada.

Em ACS, você pode definir IP carregável múltiplo ACL e usá-lo em perfis diferentes da autorização. Baseado nas condições nas regras da autorização do serviço do acesso, você pode enviar os perfis diferentes da autorização que contêm IP carregável ACL aos clientes de AAA diferentes.

Mais, você pode mudar a ordem dos índices ACL em um IP carregável ACL. ACS examina os índices ACL, partindo da parte superior da tabela, e transfere o primeiro índice ACL que encontra. Quando você ajusta a ordem, você pode assegurar a eficiência de sistema se você posiciona o mais extensamente os índices aplicáveis ACL mais altamente sobre a lista.

A fim usar um IP carregável ACL em um cliente de AAA particular, o cliente de AAA deve aderir a estas regras:

- Use o RAIO para a autenticação
- Apoie IP carregável ACL

Estes são exemplos dos dispositivos Cisco que apoiam IP carregável ACL:

• ASA

• Dispositivos Cisco que executam a Versão do IOS 12.3(8)T e mais tarde Este é um exemplo do formato que você deve usar a fim incorporar ASA ACL à caixa das definições de 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

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configurar o acesso remoto VPN (IPsec)

Procedimento ASDM

Termine estas etapas a fim configurar o acesso remoto VPN:

 Selecione assistentes > wizard VPN > IPsec(IKEv1) assistente do acesso remoto VPN do indicador home.

File	View	Tools V	Vizards Window	Help				Look
4	Home	Cor	Startup Wizard		1	Back C Forward	🤣 Help	
			VPN Wizards	,		Site-to-site VPN Wizard	I	
vice List	Home High Availability and Scalability Wizard Unified Communication Wizard		AnyConnect VPN Wizard Clientless SSL VPN Wizard					
B	Dev	Device Info Packet Capture Wizard			IPsec (IKEv1) Remote	Access VPN Wizard		
	G	eneral Lice	inse		1	12	Interface	IP Address/Ma
							dmz	192.168.26.13/24
		lost Name:	ciscoasa.defa	ult.domain.invalid			inside	10.1.1.1/24
	4	45A Version	8.4(3)	Device Uptime: 0d 2h 2	On	375	outside	172.16.1.1/24
		ASDM Versio	n: 6.4(7)	Device Type: ASA 55	10		test	no ip address
		irewall Mod	e: Routed	Context Mode: Single				
	T	fotal Flash:	64 MB	Total Memory: 256 MB				
							Select an interface to	o view input and output

- Selecione a interface de túnel VPN como necessário (fora, neste exemplo), e igualmente certifique-se de que a caixa de seleção ao lado do permite sessões do IPSec de entrada contornear Listas de acesso da relação está verificada.
 - verificada.



 Escolha o tipo do cliente VPN como o Cisco VPN Client, a liberação 3.x ou mais altamente. Clique em Next.

LIDAL LACTOR OF	
VPN Wizard	Remote Access Client (Step 2 of)
	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
Home	VPN Client Type:
Corporate Network	 Cisco VPN Client, Release 3.x or higher; or other Easy VPN Remote product
The state	C Microsoft Windows client using L2TP over IPsec
	specified on the remote client, do not specify it.
THIN	T PAP T CHAP T MS-CHAP-VI T MS-CHAP-V2 T EAP-PROXY
THI	Specify if the client will send tunnel group name as - username@tunnelgroup.
- 6	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. Escolha o método de autenticação e forneça a informação da autenticação. O método de autenticação usado aqui é chave pré-compartilhada. Também, forneça um nome de grupo de túneis no espaço fornecido. A chave pré-compartilhada usada aqui é cisco123 e o nome de grupo de túneis usado aqui é Cisco-túnel. Clique em Next.

🔂 YPN Wizard		4
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)	
unner United Street	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	
Homo	Pre-shared key	
Corporate	Pre-Shared Key: cisco123	
	Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Certificate Name: Certificate Name: Certificate Name: Certificate Name: Section (CRACK)	
J T J J	Tunnel Group	
- The state	Tunnel Group Name: Cisco-Tunnel	
	< Back Next > Finish Cancel Help	

5. Escolha se você quer usuários remotos ser autenticado à base de dados de usuário local ou a um Grupo de servidores AAA externo. Aqui, nós escolhemos autenticamos usando um Grupo de servidores AAA. Clique novo ao lado do campo de nome do Grupo de servidores AAA a fim criar um nome de Grupo de servidores AAA novo.

🔂 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:
	<back next=""> Finish Cancel Help</back>

 Forneça o nome de grupo de servidor, o nome do protocolo de autenticação, do endereço IP do servidor, da relação, e a chave do segredo de servidor nos espaços respectivos fornecidos, e na APROVAÇÃO do clique.

To add more servers to the gr Configuration > Device Manag	oup or change other AAA server settings, go gement > Users/AAA > AAA Server Groups.	to
Server Group Name:	ACS5	
Authentication Protocol:	RADIUS	
Server IP Address:	192.168.26.51	
Interface:	dmz	
Server Secret Key:	*****	
Confirm Server Secret Key:	*****	

7. Clique em Next.

🚮 VPN Wizard	x
VPN Wizard	Client Authentication (Step 4 of)
Brendi Brendi Brendi Brendi Homo Network	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: AC55 New
	<back next=""> Finish Cancel Help</back>

8. Defina um pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos quando conectam. Clique **novo** a fim criar um pool novo do endereço local.

📬 VPN Wizard		×
VPN Wizard	Address Pool Enter a po clients.	(Step 5 of 10) of local addresses to be used for assigning dynamic IP addresses to remote VPN
Corporation Nertowarts		Tunnel Group Name : Cisco-Tunnel Pool Name: Pool Settings Range Start Address: Range End Address: Subnet Mask;
		<back next=""> Finish Cancel Help</back>

9. No indicador do IP pool adicionar, forneça o nome do pool, começando o IP address, terminando o IP address, e a máscara de sub-rede. Clique em

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

 Selecione o nome do pool da lista de drop-down, e clique-o em seguida. O nome do pool para este exemplo é Amostra-pool que foi criado na etapa
 9.

🚰 VPN Wizard				×
VPN Wizard	Address Pool	(Step 5 of 10)		
	Enter a po clients.	ol of local addresses to be us	ed for assigning dynamic IP addr	esses to remote VPN
Corporato Network		Tunnel Group Name :	Cisco-Tunnel	
Territor in		Pool Name:	Sample-Pool 📉	New
		Pool Settings		
I HUUMIN		Range Start Address:	10.2.2.1	
T		Range End Address:	10.2.2.254	
- Londa		Subnet Mask:	255.255.255.0	
			<back next=""> Fins</back>	6 Cancel Help

11. *Opcional:* Especifique o DNS e GANHE a informação do server e um Domain Name do padrão a ser empurrado para clientes VPN remotos.

🔂 VPN Wizard	×
VPN Wizard	Attributes Pushed to Client (Optional) (Step 6 of 10)
Barnet	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
Corporato Network	Primary DNS Server:
A State	Secondary DNS Server:
TIM	Primary WINS Server:
- I - LI	Secondary WINS Server:
6	Diefer & Demain Name
	Jasco, com
	< Back Next Finish Cancel Help

12. Especifique qual, eventualmente, os host internos ou as redes devem ser expostos aos usuários remotos VPN. Clique **em seguida** após ter fornecido o nome da relação e as redes a ser isentadas nas redes isentas colocam.Se você deixa esta lista vazia, permite que os usuários remotos VPN alcancem a rede interna inteira do ASA.Você pode igualmente permitir o Split Tunneling neste indicador. O Split Tunneling cifra o tráfego aos recursos definidos mais cedo neste procedimento e fornece acesso unencrypted ao Internet em grande não escavando um túnel esse tráfego. Se o Split Tunneling não é permitido, todo o tráfego dos usuários remotos VPN está escavado um túnel ao ASA. Esta pode transformarse muito largura de banda e utilização de processador, com base em sua configuração.

📸 VPN Wizard	
VPN Wizard	IPsec Settings (Optional) (Step 7 of 10)
Brench Brench Brench Brench Brench	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:
FINTE 10	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 Forwarding Secrecy (PFS) Diffie Hellman Group:
	<back cancel="" help<="" next="" th="" trinsh=""></back>

13. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.



Configurar o ASA com CLI

Esta é a configuração de CLI:

Configuração running no 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



Configurar ACS para ACL baixável para o usuário individual

Você pode configurar Listas de acesso carregável no Cisco Secure ACS 5.x porque umas Permissões Nomeados Objeto e o atribui então a um perfil da autorização que seja escolhido na seção do resultado da regra no Acesso-serviço.

Neste exemplo, o usuário **Cisco do** IPSec VPN autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário "Cisco" pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, veja o <u>ACL</u> <u>baixável para o usuário/seção de grupo</u>.

Termine estas etapas a fim configurar o cliente RADIUS em um Cisco Secure ACS 5.x:

 Escolha recursos de rede > dispositivos de rede e clientes de AAA, e o clique cria a fim adicionar uma entrada para o ASA na base de dados do servidor radius.

🕨 🚭 My Workspace	Network Resources > Network Devices and AAA Clients
- 😝 Network Resources	Network Devices
 Network Device Groups Location 	Filter: 💽 Match if: 💽 Go 🔻
Device Type	Name . IP Address Description NDG:Location NDG:Device Typ
Default Network Device External Proxy Servers	No data to display
	Create Duplicate Edit Delete File Operations Export

 Dê entrada com o nome significativo a localmente - para o ASA (amostra-ASA, neste exemplo), a seguir inscreva 192.168.26.13 no campo do IP address. Escolha o RAIO na seção das opções de autenticação verificando a caixa de seleção do RAIO e entre no cisco123 para o campo secreto compartilhado. Clique em Submit.

Loration All Lorations Select Device Type All Device Types Select IP Address C IP Range(s) By Mask P Range(s) IP: 192.168.20.13 TACACS+ Shared Secret ISingle Connect Device ISingle Connect Device E Legacy TACACS+ Single Connect Support IP Address FACACS+ Drat Compliant Single Connect Support IP: 192.168.20.13 IP Range(s)	Network Device Group	s	
Device Type All Device Types Select IP Address Single IP Address IP: 192:168:26.13 IP: 192:168:26.13 IP: 192:168:26.1	Location	All Locations	Select
P Address IP Range(s) By Mask IP Range(s) TACACS+ Shared Secret Legacy TACACS+ Single Connect Support TACACS+ Drat Compliant Single Connect Support RADUS Shared Secret Sha	Device Type	All Device Types	Select
TACACS+ Draft Compliant Single Connect Support RADIUS RADIUS RADIUS Shared Secret Show CoA part 1700 Enable KeyWrap Key Encryption Key Message Authenticator Code Key Key Incryption Key Key Incry Key Incryption Key Key Incryption Key Key Incry	IP Address © Single IP Addn IP: 192.168.26.13	ess ⊂ IP Range(s) By Mask ⊂ IP Range(s)	Authentication Options
Nej squaronnat Hoos Habebboland			TACACS+ Draft Compliant Single Connect Support RADIUS R Shared Secret Shared Secret CoA port 1700 Enable KeyWrap Key Encryption Key: Message Authenticator Code Key: Key input Format ASCII HEXADECIMAL

3. O ASA é adicionado com sucesso ao base de dados do servidor 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. Escolha **usuários e a identidade armazena > identidade interna armazena > usuários**, e o clique **cria** a fim criar um usuário no base de dados local do ACS para a autenticação VPN.

• 🕀 My Workspace	Users and Identity Stores > Internal Identity Stores > Users
Network Resources	Internal Users
Gale Users and Identity Stores Identity Groups	Filter: Match if: Go 🗢
Hosts	Status User Name Identity Group Description No data to display Create Duplicate Edit Detete Change Password File Operations Export

5. Incorpore o username **Cisco**. Selecione o tipo de senha como **usuários internos**, e incorpore a senha (**cisco123**, neste exemplo). Confirme a senha, e o clique **submete-**

General						
Name:	cisco Statu	Enabled				
Description:						
Identity Group:	All Groups	Select				
Dassword before	vation			Enable Decement late	rmation	
Password must	191011			Password must		
Contain 4	 32 characters 			Contain 4 - 32	characters	
Password Typ	e: Internal Users		Select	Enable Password:		
Password:				Confirm		
Confirm Pass	werent:			Password:	1	
E change	nana. permeter					
Change pa	assword on next login					
Iser Information						
There are no ad	iditional identity attributes defined for	user records				

6. O usuário Cisco é criado com

ilter:		Match if:	• G	▼	
-	Status	User Name	 Identity Group 	Description	
0	0	cisco	All Groups		

7. A fim criar um ACL baixável, para escolher **elementos da política > autorização e permissões** > **nomeou Permissão Objeto > ACL carregável**, e o clique

ter:		
Name	 Description 	
No data	to display	

8. Forneça o **nome** para o **índice** ACL baixável, assim como **ACL**. Clique em Submit.

Jener al			
S Name:	Sample-DACL		
Description			
ownloadable	ACL Content		
permit jp a	ny host 10.1.1.2	 -	
deny ip any	/ any		
		171	
		1	
= Required f	ields		

9. A amostra-DACL ACL baixável é criada com

10. A fim configurar as políticas de acesso para a autenticação VPN, escolha políticas de acesso > acesso presta serviços de manutenção > regras de seleção do serviço, e determinam que serviço está abastecendo ao protocolo de raio. Neste exemplo, ordene 1 RAIO dos fósforos, e o acesso de rede padrão abastecerá à requisição RADIUS.



11. Escolha o serviço do acesso determinado da etapa 10. Neste exemplo, o acesso de rede padrão é usado. Escolha a aba permitida dos protocolos, e certifique-se de que permita PAP/ASCII e permita MS-CHAPv2 estão selecionados. Clique em Submit.

Auth	entication Protocols
+ 1	Allow PAP/ASCI
• 1	Allow CHAP
• 1	Allow MS-CHAPv1
• 1	Allow MS-CHAPv2
• 1	Allow EAP-MD5
• 1	Allow EAP-TLS
• 1	Allow LEAP
• 1	Allow PEAP
• 1	Allow EAP-FAST
1	Preferred EAP protocol

12. Clique sobre a **seção da identidade dos serviços do acesso**, e certifique-se de que os **usuários internos** estão selecionados como a fonte da identidade. Neste exemplo, nós tomamos o acesso de rede padrão.



 Escolha políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão, e o clique

indari	d Pol	CALEXCEL	vtion Poli	X								
etwor	k Ac	cess Aut	horizatio	Policy								
iller:	Stat	15		Match if: Ec	anala	 Enabled 	*	Clear Fitter	60 🔻			
	Г	Status	Name	NDO:Location	Conc	titions Time And Da	te	Resu Authorizatio	its n Profiles	Hit Count		
		No data	to displa	1								
	F	Default		If no rules def	Ined or n	o enabled rule	matches	PermitAcce	55	0		

 Sistema do movimento: Username da coluna disponível à coluna selecionada, e APROVAÇÃO do clique.



15. O clique **cria** a fim criar uma regra

tandar	rd Pol	icy Excer	stion Poli	sy.					
letwo	irk Ac	cess Aut	horizatio	n Policy					
Filter	Stat	US		• Match if: Equ	als 💌 Enabled	Clear	Filter 00 🔻		
		Status	Name	NDG:Location	Conditions System:UserName	Identity Group	Results Authorization Profiles	Hit Count	
		No data	to displa	y .					
	-	Default		Hee pulse date	ad as an anabled ada	matches	Darmit Losses		
rest	e	Duplica	te_1-	Edit Delete	Move to		PenalPoless	u	Customize Hit Count
	-	-			·				
			Incored Cit						

 Certifique-se de que a caixa de seleção ao lado do sistema: O username é selecionado, escolhe iguais da lista de drop-down, e incorpora o username Cisco.

192.168.26.51 https://19	
	2.168.26.51/acsadmin/PolicyInputAction.do
General Name: Rule-2 The Custor policy cond	Status: Enabled Status: Enab
Conditions	
NDG:Location:	-ANY-
Results Authorization Profiles:	You may salect multiple authorization profiles. Attributes
	defined in multiple profiles will use the value from the first profile defined.

17. Clique seleto.

Secure ACS - Mozilla Fi	efox	
192.168.26.51 https://19	2.168.26.51/acsadmin/PolicyInputAction.do	
General Name: Rule-2 The Custom policy condi	Status: Enabled	
Conditions NDG:Location: System:UserName:	-ANY-	
Results Authorization Profiles:	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
Select Deselect		
K Cancel		Не

 O clique cria a fim criar um perfil novo da autorização.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessI.PinputAction.do	金
Authorization Profiles	Showing 1-2 of 2 50 🝸 per pageGo
Filter: Match if: 00 V	
Name Description	
DerwAccess	
Permit Access	
Create Duralizate Call Davide	
Creat Colucity For Delan	rays i oli
OK Cancel	Help

19. Forneça um nome para o **perfil da autorização**. **O exemplo de perfil** é usado neste exemplo.

o Secure AES - Mozilla Firefox	
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessIPInputAction.	da
General Common Tasks RADIUS Attributes	
Name: Sample-Profile	
Description:	
e Required fields	
R	
ubmit Cancel	

20. Escolha a aba **comum das tarefas**, e selecione a **estática da** lista de drop-down para o **nome ACL baixável**. Escolha o **DACL** recém-criado **(a amostra - DACL) da** lista de drop-down de

valor.

General Common Tasks	RADIUS A	tribute	25		
ACLS					
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					
18 Avera a 1 (P) I is shadin a diday (Dedirection AC	i main	st alon he defined		

21. Clique em

Submit.

General Common Tasks	RADIUS Attri	butes		
ACLS	1.			
Downloadable ACL Name:	Static	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	•		
Maintain Connectivity during Reauthentication:	í.			
00S				
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 E	Redirect an ACL	must also he defined		

22. Certifique-se de que a caixa de seleção ao lado do **exemplo de perfil** (o perfil recém-criado da autorização) está verificada, e clique-se a

APROVAÇÃO.

uthorization Profiles	Showing 1-3 of 3 50 ref page G
iller. 💽 Match if. 💽 🕜 🔻	
Name Description	
DenvAccess	
PermitAccess	
Sample-Profile	

23. Uma vez que você verificou que o **exemplo de perfil** recém-criado está selecionado no campo dos **perfis da autorização**, clique a

o Secure ACS - Mozilla Fir	бох		-
192.168.26.51 https://192	168.26.51/acsadmin/PolicyInputA	iction ido	K
General Name: Rule-2	Status: Enabled	I area of the policy rules screen controls which	
Conditions	ons and results are availa	ble here for use in policy rules.	
System:UserName:	equalscisco		
Identity Group:	ANY		
Sample-Profile Select Deselect		rou may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
Cancel			leip

24. Verifique que a regra nova (**Rule-2**) está criada com o sistema: O username **iguala** condições e **exemplo de perfil de Cisco** como o resultado. **Mudanças da salvaguarda do**

clique. A regra 2 é criada com

etwo	rk Aci	cess Auti	horization	Policy					
iter	Stat.	19	2	Match it Equal	s 💌 Enabled	Chear FE	ter 00 🔻		
	Г	Status	Name	NDG:Location	Conditions System: UserName	Identity Group	Results Authorization Profiles	Ht Count	
1	0	•	Bule-2	-ANY-	equals cisco	-ANY-	Sample-Profile	0	
	Г	Default		If no rules define	d or no enabled rule r	natches.	PermitAccess	0	
reat	1.1-	Duplicat	te[+]	Edit Delate	Move to	1			Customize Hit Coun

Configurar ACS para ACL baixável para o grupo

Termine etapas 1 a 12 <u>configurar ACS para ACL baixável para o usuário individual</u> e execute estas etapas a fim configurar ACL baixável para o grupo em um Cisco Secure ACS.

Neste exemplo, o usuário "Cisco" do IPSec VPN pertence ao Amostra-grupo.

O usuário **Cisco do Amostra-grupo** autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário "Cisco" pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, refira o <u>ACL baixável para o usuário/seção de grupo</u>.

 Na barra de navegação, clique usuários e a identidade armazena > grupos da identidade, e o clique cria a fim criar um grupo novo

* C. with convergence	Users and identity Stores > identity Groups
Network Resources	Identity Groups
 Users and Identity Stores Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Identity Store Sequences 	Filter: Match if Go 🗢

2. Forneça um nome do grupo (Amostra-**grupo**), e o clique **submetese**.

oeneral Name:	Sample-Group	
Descriptio	in:	
👷 Parent:	All Groups	Select
= Required	fields	

3. Escolha lojas da identidade do usuário > identidade interna armazena > usuários, e selecionam o usuário Cisco. O clique edita a fim mudar a membrasia do clube deste

nternal Users				Showing 1-1 of 1 50 T per page Go
Filter:	Match if:	• 00		
Status	User Name	 Identity Group 	Description	
v	51500	All Oreups		

4. Clique seleto ao lado do grupo da

IC	en	ntin	lad	
IU.		iuv	au	i

Name: Description:	cisco	Status;	Enabled 💌 🥥	
Identity Group:	All Groups		Select	
lser Information				
There are no a	dditional identity attri	butes defined for us	er records	
Croation Madifia:	tion Information			
Date Created	Wed Feb 15 16:32:2	5 IST 2012		
Date Modified:	Wed Feb 15 16:32:2	5 IST 2012		
Date Enabled:	Wed Feb 15 16:32:2	5 IST 2012		
= Required field	de la			

5. Selecione o grupo recém-criado (isto é, Amostra-**grupo**), e clique a **APROVAÇÃO**.

Cisco Secure ACS - Mozilla Firefox	x
192.168.26.51 https://192.168.26.51/acsadmin/IdentityGroupsLPInputAction.do	合
Identity Groups	Contract Product of States
Filter: Match if: Go 🗢	
Name Description	
C * All Groups Identity Group Root	
Sample-Group	
Create Duplicate File Operations Export	
Cancel	Help
	8 N 440 N

6. Clique em

Submit.

den an			
S Name:	cisco	Status: Er	nabled 📩 😔
Description:			
🗯 Identity Group:	All Groups:Sample-G	roup	Select
User Information	N.		
There are no a	dditional identity attribu	tes defined for user	records
en ster berdens			
Creation/Modifica	ation Information		
Date Created:	Wed Feb 15 16:32:25 I	ST 2012	
Date Madified.	Wed Feb 15 16:32:25	IST 2012	
Date modified:	Wood Each 15 18-22-251	ST 2012	
Date Modified: Date Enabled:	Wed Feb 10 10.52.201		
Date Modified: Date Enabled: = Required field	38 38		
Date Modified: Date Enabled: # = Required field	99 10 10 10 10 10 10 10 10 10 10 10 10 10		
Date Modified: Date Enabled: = Required field	99 10 10 10 10 10 10 10 10 10 10 10 10 10		
Date Modified: Date Enabled: # = Required field	19		

7. Escolha **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**, e o clique **cria** a fim criar uma regra

diama a		and Burds	and a set of the set of	The Real of Control of					
two	statu	ess Auth	erization P	Match if: Equals	Enabled	Clear Fa	tar Go 🔻		
	Г	Status	Name	NDGLocation	Conditions System.UserName	Identity Group	Results Authorization Profiles	Hit Count	
		No data	to display						
			1.50						
	Г	Default		If no rules define	d or no enábled rule m	natches.	Permit Access	0	

8. Certifique-se de que a caixa de seleção ao lado do **grupo da identidade** está verificada, e clique-se

Secure ACS - Mozilla Fi	refox			CONTRACT OF ANY	
192.168.26.51 https://19	92.168.26.51/acsadmi	n/PolicyInputAction.d		-	Ribbert and en
General Name: Rule-1 The Custor policy cond	Status: Nize button in the litions and results	Enabled 💽 : lower right area s are available h) i of the policy rule ere for use in polic	s screen controls wh cy rules.	nich
Conditions	-ANY-	_			
 System OserName. Identity Group: 	in	-		Seject	
		You m define profile	ay select multiple au d in multiple profiles defined.	thorization profiles. Attri will use the value from	ibutes the first
Select Deselect	1	2			

9. Escolha o Amostra-**grupo**, e clique a **APROVAÇÃO**.

192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFilter=IdentityGrou atwork Device Groups	up=IdentikyGroup=strir
etwork Device Groups	
ilter: Match if. Go 🕶	
Name - Description	
* All Groups Identity Group Root	
Sample-Group	
<u>Dample Oroup</u>	
Create Duelleste Edit Delete I File Operations Execut	
The second	
Create Dupincate Eon Devete Frie Operations Export	
K Cancel	Hels

10. Clique **seleto**, na seção dos perfis da autorização.

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. O clique **cria** a fim criar um perfil novo da autorização.

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 page Go
Filter: Match if: 00 💌	
T Name Description	
DerwAccess	
Permit Access	
Create, Duplicate Edit Delete	Page 1 of 1 IF
OK Cancel	Help

12. Forneça um nome para o **perfil da autorização**. **O exemplo de perfil** é o nome usado neste exemplo.

co Secure ACS - Mozilla Firefox	
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessiPInputAction.do	
General Common Tasks RADIUS Attributes	
Name: Sample-Profile	
Description:	
Required fields	
2	
ubmit Cancel	

13. Escolha a aba **comum das tarefas**, e selecione a **estática da** lista de drop-down para o **nome ACL baixável**. Escolha o **DACL** recém-criado **(a amostra - DACL) da** lista de dropdown de valor.

General Common Tasks	RADIUS A	tribute	25		
ACLS					
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					
18 Avera a 1 (P) I is shadin a diday (Dedirection AC	i main	st alon he defined		

14. Clique em

Submit.

General Common Tasks	RADIUS Attri	butes			
ACLS	1	and a second sec			
Downloadable ACL Name:	Static	💌 🌼 Value Samp	le-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:	í.				
005					
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	edirect an ACL	must also be define	d		

15. Escolha o **exemplo de perfil do** perfil da autorização criado mais cedo, e clique a **APROVAÇÃO**.

	CONTRACTOR OF A DECISION OF A DECISIONO OF A DECI		N		H. STERAMOR	
] 192-168.26.51 https://	192.168.26.51/acsadmir	n/NetworkAccess/PInputAction.do	A CONTRACTOR OF SHE			5
Authorization Profiles			Showing 1-3 of :	3 50 💌	per page	Go
Filter:	Match if:	▼ 00 ▼				
T Name 🔺	Description					
DerwAccess						
Permit Access						
Sample-Profile						
Create Duplicate	Edit Delete	1	<u>•••</u> •	°age	1 of 1	

16. Clique em **OK**.

o Secure ACS - Mozilla Fi	refox			
192.168.26.51 https://19	2.168.26.51/acsadm	in/PolicyInp	utAction.do	
General				
Name: Rule-1	Status:	Enabled	• •	
The Custon policy cond	nize button in th itions and résult	e lower rij s are ava	ght area of the policy rule: illable here for use in polic	s screen controls which cy rules.
Conditions				
NDG:Location:	-ANY-			
System:UserName:	-ANY-			
Identity Group:	in	All	Groups:Sample-Group	Select
Sample-Profile			You may select multiple au defined in multiple profiles profile defined.	thorization profiles. Attributes will use the value from the first
Select Deselect		_		
K Cancel				He

17. Verifique que **Rule-1** está criado com o Amostra-**grupo do** grupo da identidade como a circunstância e o **exemplo de perfil** como o resultado. Clique **mudanças da salvaguarda**.

stwor	K ACC	ess Auth	orization F	olicy						
itter:	Statu	ś	-	Match if: Equals	Enabled	Clear Filter Go	*			
	Г	Status	Name	NDG1 acotion	Condition	S Identity Convers	Results Authorization Profiles	Hit Count		
				Disco Eucandei	oystem osemante	Identity Oroup	Paginonitasioniti nomes			
1		0	Rule-1	-ANY	-ANY	in All Groups:Sample-Group	Sample-Profile	0]	
1	C	Defect	Rule-1	-ANE	-ANY	in All Oroups:Sample-Group	Sample-Profile	0]	

Configurar ACS para ACL baixável para um grupo de dispositivo de rede

Termine etapas 1 a 12 configurar ACS para ACL baixável para o usuário individual e execute

estas etapas a fim configurar ACL baixável para um grupo de dispositivo de rede em um Cisco Secure ACS.

Neste exemplo, o cliente RADIUS (ASA) pertence ao grupo de dispositivo de rede o pedido de autenticação VPN-Gateways. The VPN que que vem do ASA para o usuário "Cisco" autentica com sucesso, e o servidor Radius envia uma lista de acessos carregável à ferramenta de segurança. O usuário "Cisco" pode alcançar somente o server de 10.1.1.2 e nega todo acesso restante. A fim verificar o ACL, refira o <u>ACL baixável para o usuário/seção de grupo</u>.

1. Escolha **recursos de rede > grupos de dispositivo de rede > tipo de dispositivo**, e o clique **cria** a fim criar um grupo de dispositivo de rede

2010

🎝 Network Resources	Network Device Groups	
Network Device Groups Location	Filter: Match If: Go 💌	
Network Devices and AAA Cilents	T Name - Description	
Default Network Device External Proxy Servers	All Device Types All Device Types	
35 Users and Identity Stores		
Se Policy Elements		
🔓 Access Policies		
S Monitoring and Reports		
System Administration		

2. Forneça um nome de **grupo de dispositivo de rede** (**gateways de VPN n**este exemplo), e o clique **submete-**

Device Group	- General	
o Name:	VPN-Gateways	
Descriptio	n:	
🙍 Parent:	All Device Types	Selec
= Required	fields	ananananananananananananananananananan

 Escolha recursos de rede > dispositivos de rede e clientes de AAA, e selecione o cliente RADIUS amostra-ASA criado mais cedo. O clique edita a fim mudar a sociedade de grupo de dispositivo de rede deste cliente RADIUS (asa).

		Match if.		90 🗢		
me		IP Address	Description	NDG:Location	NDG:Device Type	
morie-esa		192.168.26.13932		Al: Locations	All Device Types	
0	ne note esa	NC •	Match if. IP Address 192.145.26.1312	Match If: Match If: IP Address Description IDE-108-28 102108-28 1032	Match If: Go V Ne IP Address Description NDG:Location NDG:Location NDG:Location A& Locations	Match if: Oo Match if: IP Address Description NDG:Location NDG:Device Type I02:100:26:13/32 Al: Locations Al: Device Types

4. Clique **seleto** ao lado do tipo de

Description	sample-asa	
letwork Devic	e Groups	
Location	All Locations	Select
Device Type	All Device Types	Select
 Single IP: 192.16 	IP Address C IP Range(s) By Mask C IP Range(s) 8.26.13	► TACACS+ T ► RADIUS T

5. Selecione o grupo de dispositivo de rede recém-criado (que é **gateways de VPN**), e clique a **APROVAÇÃO**.

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

6. Clique em

Submit.

Name: Description:	sample-asa	
Network Device	Groups	
Location	All Locations.	Select
Device Type	All Device Types:VPN-Gateways	Select
 Single I IP: 192.168 	Address C IP Range(s) By Mask C IP Range(s)	► TACACS+ F

 Escolha políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão, e o clique personaliza.

etwor	k Aci	cess Auth	orization	Policy			
iter.	Statu	IS	-	Match if Equals 💌 Enabled 💌 Clear Filter	Go 🔻		
	Status	Status Name		Conditions NDG:Location System:UserName Identity Group	Results Authorization Profiles	Hit Count	
-		Default		If no rules defined or no enabled rule matches.	PermitAccess	0	
eate		Duplicat	0 E	dit. Delete Move to			Sustomize Hit Count

8. Movimento NDG: Tipo de dispositivo da seção disponível à seção selecionada, e APROVAÇÃO do

clique.



9. O clique cria a fim criar uma regra

0000

Netwo	rk Aci	cess Auth	norization	Policy					
Filter:	Stat.	15	2	Match it Equals	Enabled	Clear Filter G			
	L.	Status	Name	NDG:Location	System UserName	Conditions Identify Group	NDO:Device Type	Results Authorization Profiles	Hit Count
**	Г	Default		lf no rules define	d or no enabled rule r	natches.		PermitAccess	0
reate		Duplicat	10	Edit Delate	Move to.				Customize Hit Cour

10. Certifique-se de que a caixa de seleção ao lado de NDG: O tipo de dispositivo é selecionado e escolhe dentro da lista de drop-down. Clique

seleto

Conditions NDG:Location: -ANY4 System:UserName: -ANY4 Identity Group: -ANY4 MDG:Device Type: in Select Results Authorization Profiles: You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	suits are available fiere for use in policy fules.	ton in the lower rig	The Custom
Image: NDG:Device Type: in Select Results Authorization Profiles: You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.			nditions NDG:Location:
Authorization Profiles: You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	Seler		NDG:Device Type:
Select Deselect	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.		Select Deselect

11. Escolha os **gateways de VPN do** grupo de dispositivo de rede criados mais cedo, e clique a **APROVAÇÃO**.

isco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFilter=DeviceType=DeviceType=string	合
Network Device Groups	
Filter: Match if: Go 🗢	
Name Description	
C * All Device Types All Device Types	_
VPN-Gateways	
Create Duplicate Edit Delete File Operations Export	
OX Cancel Hel	p
	-

12. Clique seleto.

o Secure ACS - Mozilla Fi	refox	
192.168.26.51 https://19	2.168.26.51/acsadmin/PolicyInputAction.do	-
General Name: Rule-1 The Custon policy cond	Status: Enabled 💽 💿 hize button in the lower right area of the policy rules screen controls which tions and results are available here for use in policy rules.	
Conditions		
NDG:Location:	-ANY-	
System:UserName:	-ANY-	
Identity Group:	-ANY-	
NDG:Device Type:	in All Device Types.VPN-Gateways Select	
Select Deselect	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
K Cancel		Hel

13. O clique **cria** a fim criar um perfil novo da autorização.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessi/PinputAction.de	<u></u>
Authorization Profiles	Showing 1-2 of 2 50 🝸 per pageGo
Filter: Match if: 00 🔻	
T Name - Description	
DerwAccess	
Permit Access	
Creats, Duplicate Edit Delete	Page 1 of 1
OK Cancel	Help
	Contraction of the second s

14. Forneça um nome para o **perfil da autorização**. **O exemplo de perfil** é o nome usado neste exemplo.

o Secure ACS - Mozilla Firefox	
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do	
General Common Tasks RADIUS Attributes	
Name: Sample-Profile	
Description:	
Required fields	
54	
ubmit Cancel	

15. Escolha a aba **comum das tarefas**, e selecione a **estática da** lista de drop-down para o nome ACL baixável. Escolha o **DACL** recém-criado **(amostra-DACL) da** lista de drop-down de

valor.

General Common Tasks	RADIUS AN	tribute	IS		
ACLS					
Downloadable ACL Name:	Static	٠	Value Sample-DAR	*	
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:	3				
QOS					
Input Policy Map:	Not in Use				
Output Policy Map:	Not in Use	*			
802.1X-REV					
LinkSec Security Policy:	Not in Use	*			
URL Redirect					
184 an a LIDI is defined for	Dedirect on AC	i maine	t alon he defined		

16. Clique em

Submit.

General Common Tasks	RADIUS Att	ibutes			
ACLS					
Downloadable ACL Name:	Static	Val	lue 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	*			
Maintain Connectivity during Reauthentication:	l.				
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 ACI	must also	be defined		

17. Selecione o **exemplo de perfil** criado mais cedo, e clique a **APROVAÇÃO**.

uthorization Profiles	Showing 1-4 of 4 50 👱 per page
liter: Match if. 00 V	
Name Description	
DenvAccess	
Filter-Id	
Permit Access	
Sample-Profile	

18. Clique em

		-
192.168.26.51 https://19	2:168.26.51/acsadmin/PolicyInputAction.do	
General		
Name: Rule-1	Status: Enabled 💽 💿	
-		
The Custor	nize button in the lower right area of the policy rules screen controls which itions and results are available here for use in policy rules.	
policy cond	sons and results are available nere for use in policy fules.	
Conditions		
NDG:Location:	-ANY-	
System:UserName:	-ANY-	
Identity 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 profile defined.	
	<u>*</u>	
Select Deselect	1	
	2	

19. Verifique que **Rule-1** está criado com os **gateways de VPN** como NDG: Tipo de dispositivo como a circunstância, e **exemplo de perfil** como o resultado. **Mudanças da salvaguarda do**

clique.

	IK AC	cess Auto	orization	Policy					
itter:	Statu	3L	•	Match if: Equal	s 💌 Enabled	· Clear Fi	fler Ga 🔻		
	-	Status	Name	NDGLocation	System/UserName	Conditions Identity Group	NDG Device Type	Results Authorization Profiles	Hit Count
1	Π.	۲	Rule-1	-ANY-	-ANY-	-ANY	in All Device Types:VPN-Galeways	Sample-Profile	4
	Г	Default		If no rules define	ad or no enabled rule r	matches.		Permit Access	0

Configurar ajustes do RADIUS IETF para um grupo de usuário

A fim transferir um nome para uma lista de acessos que você já crie na ferramenta de segurança do servidor Radius quando um usuário autentica, configurar o atributo do ID de filtro do RADIUS IETF (número de atributo 11):

filter-id=acl_name

O usercisco do Amostra-grupo autentica com sucesso, e o servidor Radius transfere um nome ACL (novo) para uma lista de acessos que você já crie na ferramenta de segurança. O usuário "Cisco" pode alcançar todos os dispositivos que são dentro da rede do ASA **exceto o** server de 10.1.1.2. A fim verificar o ACL, veja a <u>seção ACL do ID de filtro</u>.

Conforme o exemplo, o novo nomeado ACL é configurado filtrando no ASA:

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

Estes parâmetros aparecem somente quando estes são verdadeiros. Você configurou:

- Cliente de AAA para usar um dos protocolos de raio na configuração de rede
- Um perfil da autorização com o ID de filtro do RAIO (IETF) é selecionado sob a seção do resultado da regra no Acesso-serviço.

Os atributos RADIUS são enviados como um perfil para cada usuário de ACS ao cliente de AAA de pedido.

Termine etapas 1 com 6 e 10 com 12 <u>configurar ACS para ACL baixável para o usuário individual</u>, seguido por etapas 1 com 6 <u>configurar ACS para ACL baixável para o grupo</u>, e execute estas etapas nesta seção a fim configurar o ID de filtro no Cisco Secure ACS.

A fim configurar ajustes do **atributo de raio de IETF** para aplicar-se como no perfil da autorização, execute estas etapas:

1. Escolha elementos da política > autorização e permissões > perfis do acesso de rede > da autorização, e o clique cria a fim criar um perfil novo da

Authorization Profiles	Showing 1-2 of 2 50 💌 per page Go
Filter: Match if: Go 🗸	
Name Description	
Permit Access	
Sample-Profile	

 Forneça um nome para o perfil da autorização. O ID de filtro é o nome de perfil da autorização escolhido neste exemplo para a simplicidade.

General	offittion lasks RADIOS Autobules	
Name:	Filter-Id I	
Descriptio	n:	
= Required	fields	

 Clique a aba comum das tarefas, e escolha a estática da lista de drop-down para o ID de filtro ACL. Dê entrada com o nome da lista de acessos como novo no campo de valor, e o clique submete-

se.

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	5 mm m m m m m m m m m m m m m m m m m		
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. Escolha **políticas de acesso > acesso presta serviços de manutenção > acesso > autorização de rede padrão**, e o clique **cria** a fim criar uma regra

				and the second second					
andar	d Pob	TYI Excess	tion Policy	1					
ietwo	rk Aci	ess Auth	orization	Policy					
Filter:	Statu	18	*	Match if: Equals	Enabled	Clear Filter 00	*		
	Г	Status	Name	NDGLocation	Condition System:UserName	is Identity Group	Results Authorization Profiles	Hit Count	
		No data	to display						
**	Г	Default		If no rules define	d or no enabled rule r	natches.	Permit Access	0	
Tro the		Duplicat	0.1• E	dit Delete	Move to				Customize Hit Cour
	_		suminal sum	a ferrenerate ferrener		-			

5. Certifique-se de que a caixa de seleção ao lado do **grupo da identidade** está verificada, e clique-se **seleto**.

	irelox		CONTRACT STREET, STREE	
192.168.26.51 https://19	92.168.26.51/ə	sadmin/PolicyInputAction.do		
General				
Name: Rule-1	Stat	tus: Enabled 🗾 🔵		
CA The Custor	mize button i	n the lower right area of	of the policy rules screen controls which	
Dolicy cond	titions and re	esults are available here	e for use in policy rules.	
Conditions				
NDG:Location:	-ANY-			
System:UserName	-ANY-			
Identity Group:	in		Select	
		defined in profile de	n multiple profiles will use the value from the firs afined.	st
Select Deselect	1	<u></u>		

6. Escolha o Amostra-**grupo**, e clique a **APROVAÇÃO**.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.doTcontextData.externalFiker=IdentityGroup=IdentityGroup=structure	(A)
Network Device Groups	
Filter: Match if. Go 🗸	
Name Description C * All Groups Identity Group Root	
C Sample-Group	
Create Duplicate Edit Delete File Operations Export	
K Cancel He	ip

7. Clique **seleto na** seção dos perfis da autorização.

Secure ACS - Mozilla I	irefox			
192.168.26.51 https://1	92.168.26.51/acsadm	n/PolicyInp	put Action , do	
General				
Name: Rule-1	Status:	Enabled	⊻ ♥	
The Custo policy con	mize button in the ditions and result	e lower ri s are ava	ight area of the policy rules screen controls which allable here for use in policy rules.	
Conditions				
NDG:Location:	-ANY-			
System:UserName	-ANY-		and the second se	
Identity Group:	in		I Groups:Sample-GroupSelect	
Select Deselect			You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the firs profile defined.	t

 Escolha o ID de filtro do perfil da autorização criado mais cedo, e clique a APROVAÇÃO.

Cisco Secure ACS - Mozilla Firefox	X
192.168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do	
Authorization Profiles	Showing 1-4 of 4 50 💌 per pageGo
Filter: Match if. 00 🔻	
Name Description	
DerwAccess	
Filter-Id	
Permit Access	
Sample-Profile	
Create Duplicate Edit Delete	Page 1 of 1
<u>PK</u> Cancel	Help

9. Clique em OK.

Secure ACS - Mozilla F	irefox		A LON NO.	
192.168.26.51 https://1	92.168.26.51/a	csadmin/PolicyInp	outAction, do	STREET BOOK STREET
General Name: Rule-1 The Custo policy con	Sta mize button ditions and r	itus: Enabled in the lower ri esults are ava	ight area of the policy rule	es screen controls which icy rules
Conditions	Line			
NDG:Location: System:UserName	-ANY-			
Identity Group:	in	All	l Groups:Sample-Group	Select
			defined in multiple profile profile defined.	s will use the value from the first
Select Deselec	t	×		
K Cancel				н

10. Verifique que **Rule-1** está criado com o Amostra-**grupo do** grupo da identidade como a circunstância e o **ID de filtro** como o resultado. Clique **mudanças da salvaguarda**.

etwork Access Authorization Policy											
iller	ter: Status Match It Equals Tenabled Clear Filter 00 V						▽				
	Г	Status	Name	NDG:Location	Conditions System UserName	s Identity Group	Results Authorization Profiles	Hit Count			
1		•	Rule-1	-ANY	-ANIX	in All Group's Sample-Group	Filter-Id	0			
-	F	Default		If no rules define	d or no enabled rule m	natches	PermitAccess	0			

Configuração de Cisco VPN Client

Conecte a Cisco ASA com o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

Conclua estes passos:

- 1. Escolha o Start > Programs > o cliente VPN de Cisco Systems > o cliente VPN.
- 2. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.

👶 status: Disconnected VPN Client - Version	n 5.0.07.0410	_ 🗆 ×
Connection Entries Status Certificates Log Opt	tions Help	
Connect New Import Modify) Delete	cisco
Connection Entry	Host	Transport
Not connected.		
		1

3. Preencha os detalhes de sua nova conexão:Dê entrada com o nome da entrada de conexão junto com uma descrição.Incorpore o endereço IP externo do ASA à caixa do host.Incorpore o nome de grupo de túneis VPN (Cisco-túnel) e a senha (chave pré-compartilhada - cisco123) como configurado no ASA.Click

Connocion Enklys	15 ample-Conn	ection		4.4
Description:				CISCO
Host:	172.16.1.1			cibeo
Authentication	Transport	Backup Servers	Dial-Up	
Group Authe	entication		C Mutual Gro	up Authenticatio
Name:	Cisco-Tu	innel		
Password:	*****			
Confirm Passy	word:			
C Certificate A Name: Send CA	uthentication Certificate Cha	in .	ſ	

4. Clique a conexão que você quer usar, e o clique **conecta da** janela principal do cliente VPN.

Status: D Connection E	Isconne ntries	acted VPN	Client -	Version 5. og Option	0.07.0410 s Help	1	
Confect	Ne		 I port	Modify	Delete		cisco
Connection E	Entries	Certificates	Log			Hort	Transport
F	Samp	le-Connect	ion			172 16 1 1	IPSec/UDP
4							
Not connecte	d.						

5. Quando alertado, entre no **cisco123** username **Cisco** e da senha como configurado no ASA para a autenticação, e clique a **APROVAÇÃO** a fim conectar à rede

The server has reque authentication.	sted the following i	nformation to complete	the user
uluit. Username:	cisco		
CISCO Password:	*****		
		οκ	Cano

6. Uma vez que a conexão é estabelecida com sucesso, escolha **estatísticas do** menu de status a fim verificar os detalhes do

Connection Entries	Status Certificates Log Option	ns Help	
Connect N	Ratistics Ctrl+5 Notifications Ctrl+N	Delete	cisco
Connection Entries	Reset Stats		
Conn	ection Entry	Host	Transport
Samp	ole-Connection	172.16.1.1	IPSec/UDP

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Comandos show crypto

 show crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.
 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#

    mostre ipsec cripto sa - Mostra os ajustes usados pelo SAs atual.

 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 baixável para o usuário/grupo

Verifique o ACL baixável para o usuário Cisco. Os ACL são transferidos do CSACS.

ID de filtro ACL

O ID de filtro [011] aplicou-se para o grupo - o Amostra-grupo, e os usuários do grupo são filtrados conforme o ACL (novo) definido no ASA.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. O exemplo de debug é mostrado igualmente.

Nota: Para obter mais informações sobre do IPSec VPN do Acesso remoto do Troubleshooting, refira <u>a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções</u>.

Cancele associações de segurança

Quando você pesquisa defeitos, certifique-se cancelar o SAs existente depois que você faz uma mudança. No modo privilegiado do PIX, use estes comandos:

- clear [crypto] ipsec sa Suprime do IPSec ativo SAs. As palavras-chave crypto são opcionais.
- clear [crypto] isakmp sa Suprime do IKE ativo SAs. As palavras-chave crypto são opcionais.

Comandos para Troubleshooting

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte <u>Informações Importantes sobre Comandos de Depuração</u> antes de usar comandos **debug**.

- ipsec 7 do debug crypto Indica as negociações de IPSEC de fase 2.
- isakmp 7 do debug crypto Indica as negociações de ISAKMP de fase 1.

Informações Relacionadas

- Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances
- Referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- <u>Cisco Adaptive Security Device Manager</u>
- Página de suporte da Negociação IPSec/Protocolos IKE
- Página de suporte do Cisco VPN Client
- <u>Cisco Secure Access Control System</u>
- <u>Request for comments (RFC)</u>
- <u>Suporte Técnico e Documentação Cisco Systems</u>