# ASA 8.3 e versioni successive: Esempio di autorizzazione Radius (ACS 5.x) per l'accesso VPN con ACL scaricabile con CLI e ASDM

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Configura VPN di accesso remoto (IPsec) Configurazione dell'ASA con CLI Configurazione di ACS per ACL scaricabili per un singolo utente Configurazione di ACS per ACL scaricabili per gruppo Configurazione di ACS per ACL scaricabili per un gruppo di dispositivi di rete Configurare le impostazioni RADIUS IETF per un gruppo di utenti Configurazione client VPN Cisco Verifica Mostra comandi di crittografia ACL scaricabile per utente/gruppo ACL Filter-Id Risoluzione dei problemi Cancella associazioni di protezione Comandi per la risoluzione dei problemi Informazioni correlate

# **Introduzione**

In questo documento viene descritto come configurare l'appliance di sicurezza per autenticare gli utenti per l'accesso alla rete. Poiché le autorizzazioni RADIUS possono essere attivate in modo implicito, in questo documento non viene fornita alcuna informazione sulla configurazione dell'autorizzazione RADIUS sull'accessorio di sicurezza. Vengono fornite informazioni sul modo in cui l'accessorio di protezione gestisce le informazioni dell'elenco degli accessi ricevute dai server RADIUS.

Èpossibile configurare un server RADIUS in modo che al momento dell'autenticazione venga scaricato un elenco degli accessi all'accessorio di protezione o un nome di elenco degli accessi.

L'utente è autorizzato a eseguire solo le operazioni consentite nell'elenco degli accessi specifico.

Gli elenchi degli accessi scaricabili sono il metodo più scalabile quando si utilizza Cisco Secure Access Control Server (ACS) per fornire gli elenchi degli accessi appropriati per ogni utente. Per ulteriori informazioni sulle funzionalità delle liste di accesso scaricabili e su Cisco Secure ACS, consultare il documento sulla configurazione di un server RADIUS per inviare liste di controllo degli accessi scaricabili e ACL IP scaricabili.

Per ulteriori informazioni, fare riferimento al documento <u>ASA/PIX 8.x: Esempio di autorizzazione</u> <u>Radius (ACS) per l'accesso alla rete con ACL scaricabile con CLI e ASDM</u> per la stessa configurazione sull'appliance Cisco ASA con versioni 8.2 e precedenti.

# Prerequisiti

# **Requisiti**

In questo documento si presume che le appliance ASA (Adaptive Security Appliance) siano completamente operative e configurate per consentire a Cisco Adaptive Security Device Manager (ASDM) o alla CLI di apportare modifiche alla configurazione.

**Nota:** per consentire la configurazione remota del dispositivo da parte di ASDM o Secure Shell (SSH), consultare il documento sull'<u>autorizzazione</u> dell'<u>accesso HTTPS per ASDM</u>.

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco ASA versione 8.3 e successive
- Cisco ASDM versione 6.3 e successive
- Cisco VPN Client versione 5.x e successive
- Cisco Secure ACS 5.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## **Convenzioni**

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> nei suggerimenti tecnici.

# **Premesse**

Èpossibile usare gli ACL IP scaricabili per creare set di definizioni di ACL che possono essere applicate a molti utenti o gruppi di utenti. Questi set di definizioni ACL sono chiamati contenuti ACL.

Gli ACL IP scaricabili funzionano nel modo seguente:

- 1. Quando ACS concede a un utente l'accesso alla rete, ACS determina se un ACL IP scaricabile è assegnato al profilo di autorizzazione nella sezione dei risultati.
- 2. Se ACS individua un ACL IP scaricabile assegnato al profilo di autorizzazione, invia un attributo (come parte della sessione utente, nel pacchetto RADIUS access-accept) che specifica l'ACL con nome e la versione dell'ACL con nome.
- 3. Se il client AAA risponde che la versione corrente dell'ACL non è presente nella cache, ossia l'ACL è nuovo o è stato modificato, ACS invia l'ACL (nuovo o aggiornato) al dispositivo.

Gli ACL IP scaricabili sono un'alternativa alla configurazione degli ACL nell'attributo RADIUS Cisco cisco-av-pair [26/9/1] di ciascun utente o gruppo di utenti. È possibile creare un ACL IP scaricabile una volta sola, assegnargli un nome e quindi assegnare l'ACL IP scaricabile a qualsiasi profilo di autorizzazione se si fa riferimento al nome. Questo metodo è più efficiente di quello utilizzato per configurare l'attributo RADIUS Cisco cisco-av-pair per il profilo di autorizzazione.

Quando si immettono le definizioni degli ACL nell'interfaccia Web di ACS, non usare parole chiave o nomi; per tutti gli altri aspetti, usare la sintassi dei comandi ACL standard e la semantica del client AAA a cui si intende applicare l'ACL IP scaricabile. Le definizioni ACL immesse in ACS comprendono uno o più comandi ACL. Ogni comando ACL deve essere su una riga separata.

Negli ACS, è possibile definire più ACL IP scaricabili e usarli in diversi profili di autorizzazione. In base alle condizioni specificate nelle regole di autorizzazione dei servizi di accesso, è possibile inviare profili di autorizzazione diversi contenenti ACL IP scaricabili a client AAA diversi.

Inoltre, è possibile modificare l'ordine dei contenuti dell'ACL in un ACL IP scaricabile. ACS esamina il contenuto degli ACL, a partire dalla parte superiore della tabella, e scarica il primo contenuto trovato. Quando si imposta l'ordine, è possibile garantire l'efficienza del sistema posizionando più in alto nell'elenco i contenuti degli ACL applicabili.

Per utilizzare un ACL IP scaricabile su un particolare client AAA, il client AAA deve rispettare le seguenti regole:

- Utilizza RADIUS per l'autenticazione
- Supporto di ACL IP scaricabili

Di seguito sono riportati alcuni esempi di dispositivi Cisco che supportano ACL IP scaricabili:

• ASA

Dispositivi Cisco con IOS versione 12.3(8)T e successive

Questo è un esempio del formato da usare per immettere gli ACL ASA nella casella Definizioni 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 0.0.255
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 HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80

# **Configurazione**

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



**Nota:** gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

## Configura VPN di accesso remoto (IPsec)

### Procedura ASDM

Per configurare la VPN di accesso remoto, completare i seguenti passaggi:

 Selezionare Procedure guidate > Procedure guidate VPN > Procedura guidata VPN ad accesso remoto IPsec(IKEv1) dalla finestra 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	Device	High Availability and Scalability Wizard Unified Communication Wizard Packet Capture Wizard			AnyConnect VPN Wizard Clientless SSL VPN Wizard			
B	Dev	rice Infc				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	

2. Selezionare VPN Tunnel Interface come richiesto (Outside, in questo esempio) e verificare anche che la casella di controllo accanto a Abilita sessioni IPsec in entrata per ignorare gli elenchi degli accessi all'interfaccia sia

selezionata.



 Scegliere il tipo di client VPN come Cisco VPN Client, versione 3.x o successive. Fare clic su Next (Avanti).

👩 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
and and a	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
Corporato	VPN Client Type:
Nation	or other Easy VPN Remote product
the state	Microsoft Windows client using L2TP over IPsec     Specify the PPP authentication protocol. IF a protocol is not     coordinate on the second plant, do not coordinate.
	Specified on the remote client, do not specify it.
The	I PAP IM CHAP IM MERCHAPAT I MERCHAPAY
LILI	Specify if the client will send tunnel group name as - username@tunnelgroup.
A	Cient 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. Scegliere il Metodo di autenticazione e fornire le informazioni di autenticazione. Il metodo di autenticazione utilizzato è la chiave già condivisa. Inoltre, fornire un nome di gruppo di tunnel nello spazio fornito. La chiave precondivisa utilizzata è cisco123, il nome del gruppo di tunnel è Cisco-Tunnel. Fare clic su Next (Avanti).

🔂 VPN Wizard		×
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)	
and a second	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	
THE REAL	C Certificate Certificate Signing Algorithm: rsa-sig Certificate Name:	
- I HILLIN	Charlenge/response dutienticount (creacy)	
THIT	Tunnel Group	
and the second	Tunnel Group Name: Cisco-Tunnel	
	< Back Next > Finish Cancel Help	

5. Specificare se si desidera che gli utenti remoti vengano autenticati nel database degli utenti locale o in un gruppo di server AAA esterno. In questo caso, si sceglie Autentica utilizzando un gruppo di server AAA. Per creare un nuovo nome di gruppo di server AAA, fare clic su New (Nuovo) accanto al campo AAA Server Group Name (Nome gruppo server 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:
	<back next=""> Finish Cancel Help</back>

6. Specificare il nome del gruppo di server, il protocollo di autenticazione, l'indirizzo IP del server, il nome dell'interfaccia e la chiave privata del server negli spazi corrispondenti e fare clic su

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

7. Fare clic su **Next** (Avanti).

🛃 VPN Wizard	×
VPN Wizard	Client Authentication (Step 4 of)
Brench Brench ISP Homo Corporate 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: ACS5     New
	<back next=""> Finish Cancel Help</back>

 Definire un pool di indirizzi locali da assegnare dinamicamente ai client VPN remoti quando si connettono. Per creare un nuovo pool di indirizzi locali, fare clic su New (Nuovo).

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

9. Nella finestra Aggiungi pool IP, fornire il nome del pool, l'indirizzo IP iniziale, l'indirizzo IP finale e la subnet mask. Fare clic su

Name:	Sample-Pool	
Starting IP Address:	10.2.2.1	
Ending IP Address:	10.2.2.254	
Subnet Mask:	255.255.255.0	

 Selezionare il nome del pool dall'elenco a discesa e fare clic su Avanti. Il nome del pool per questo esempio è Sample-Pool, creato nel passaggio 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 addresses to remote VPN	_
Corporate Network		Tunnel Group Name :	Cișco-Tunnel		
THE THE		Pool Name:	Sample-Pool	▼	
		Pool Settings			
T-HUIM		Range Start Address:	10.2.2.1		
The second se		Range End Address:	10.2.2.254		
		Subnet Mask:	255.255.255.0		
		1		1	
			< Back Next >	Finish Cancel Hel	

11. *Facoltativo:* Specificare le informazioni sui server DNS e WINS e un nome di dominio predefinito da inserire nei client VPN remoti.

🚰 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
Corporato Network	Primary DNS Server:
the second	Secondary DNS Server:
	Primary WINS Server:
- I - LI	Secondary WINS Server:
S.R-	Default Domain Name: cisco.com
	<back next=""> Finish Cancel Help</back>

12. Specificare gli eventuali host interni o reti da esporre agli utenti VPN remoti. Fare clic su Avanti dopo aver fornito il nome dell'interfaccia e le reti a cui applicare l'esenzione nel campo Reti esenti.Se si lascia vuoto questo elenco, gli utenti VPN remoti possono accedere all'intera rete interna dell'appliance ASA.In questa finestra è anche possibile abilitare il tunneling suddiviso. Il tunneling ripartito cripta il traffico diretto alle risorse definite in precedenza in questa procedura e fornisce l'accesso non crittografato a Internet in senso lato evitando il tunneling del traffico. Se il tunneling suddiviso *non* è abilitato, tutto il traffico proveniente dagli utenti VPN remoti viene tunneling verso l'appliance ASA. In base alla configurazione, questa operazione può richiedere un uso intensivo della larghezza di banda e del

processore.

📬 VPN Wizard		×
VPN Wizard	IPsec Settings (Optional) (Step 7 of 10)	
Branch Branch Branch Branch Homes	Network Address Translation (NAT) is used to hide the internal network from outside users. You or make exceptions to NAT to expose the entire or part of the internal network to authenticated ren 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.	an note
(Corporate)	Interface:	
Nam	Exempt Networks: 10.1.1.0/24	
	Enable split tunneling to let remote users have simultaneous encrypted access to the resource defined above, and unencrypted access to the internet.     Enable Perfect Forwarding Secrecy (PFS)     Diffie-Hellman Group:	es
	< Back Next > Finish Cancel He	ib.

 Questa finestra mostra un riepilogo delle azioni intraprese. Se la configurazione è soddisfacente, fare clic su Fine.



# Configurazione dell'ASA con CLI

Questa è la configurazione CLI:

Esecuzione della configurazione sul dispositivo ASA
ASA# <b>sh run</b>
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



# Configurazione di ACS per ACL scaricabili per un singolo utente

Èpossibile configurare elenchi degli accessi scaricabili in Cisco Secure ACS 5.x come oggetti con autorizzazioni denominate e quindi assegnarli a un profilo di autorizzazione che verrà scelto nella sezione dei risultati della regola in Access-Service.

Nell'esempio, l'utente VPN IPsec **cisco** viene autenticato correttamente e il server RADIUS invia un elenco degli accessi scaricabili all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione <u>ACL</u> <u>scaricabili per utente/gruppo</u>.

Completare questa procedura per configurare il client RADIUS in un Cisco Secure ACS 5.x:

 Scegliere Risorse di rete > Dispositivi di rete e client AAA, quindi fare clic su Crea per aggiungere una voce per l'appliance ASA nel database del server RADIUS.

My Workspace	Network Resources > Network Devices and AAA Clients
- 💓 Network Resources	Network Devices
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: Match if. Go 🗢
Device Type Network Devices and AAA Clients Default Network Device External Proxy Servers	<ul> <li>Name          <ul> <li>IP Address Description</li> <li>NDG:Location</li> <li>NDG:Device Type</li> <li>No data to display</li> </ul> </li> </ul>
	Create Duplicate Edit Delete File Operations Export

 Immettere un nome localmente significativo per l'ASA (sample-asa, in questo esempio), quindi immettere 192.168.26.13 nel campo dell'indirizzo IP. Selezionare la casella di controllo RADIUS nella sezione Authentication Options (Opzioni di autenticazione) e immettere cisco123 come campo Shared Secret. Fare clic su Invia.

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       FACAUSF       Single Connect Device         IP:       192.168.20.13       Single Connect Device       E Legacy TACACS+ Single Connect Support         IP Address       C IP Range(s)       Single Connect Support       FACACS+ Drat Compliant Single Connect Support         IP RADIUS       IP       Shared Secret       Show       CoA port:         IP Radius       IP       Shared Secret       Show       CoA port:         IP       Shared Secret       Show       CoA port:       TOD         IP       Enable KeyWrap       Key Encryption Key       Message Authenticator Code Key       Key Encryption Key	Network Device Group	s	
Device Type       All Device Types       Select         IP Address <ul> <li>Single IP Address</li> <li>IP: 192:168:26.13</li> </ul> <ul> <li>IP: 192:168:26.13</li> <li>IP: 192:168:26.1</li></ul>	Location	All Locations	Select
P Address <ul> <li>IP Range(s) By Mask</li> <li>IP Range(s)</li> </ul> <ul> <li>TACACS+</li> <li>Shared Secret</li> <li>Legacy TACACS+ Single Connect Support</li> <li>TACACS+ Drat Compliant Single Connect Support</li> <li>RADUS</li> <li>Shared Secret</li> <li>Sha</li></ul>	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 Sec

3. L'appliance ASA viene aggiunta correttamente al database del server RADIUS (ACS).

evice Typ
ce Types

 Scegliere Utenti e archivi identità > Archivi identità interni > Utenti, quindi fare clic su Crea per creare un utente nel database locale del server ACS per l'autenticazione VPN.

<ul> <li>My Workspace</li> </ul>	Users and Identity Stores > Internal Identity Stores > Users
Network Resources	Internal Users
Gentily 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. Immettere il nome utente **cisco**. Selezionare il tipo di password **Internal Users** (Utenti interni), quindi immettere la password (**cisco123**, in questo esempio). Confermare la password e fare clic su

The second set and a		
Identity Group: All	Groups Select	
Password Informatio Password must • Contain 4 - 32	n I characters	Enable Password Information Password must • Contain 4 - 32 characters
Password Type: Password:	Internal Users	Select Enable Password:
Confirm Password	d:	Password.
ser Information	onal identity attributes defined for user records	

### 6. Creazione dell'utente cisco

#### completata.

ilter	:	Match if:	Go	_ ▼
Г	Status	User Name	<ul> <li>Identity Group</li> </ul>	Description
Γ	0	cisco	All Groups	

7. Per creare un ACL scaricabile, scegliere Elementi dei criteri > Autorizzazioni e autorizzazioni
 > Oggetti autorizzazioni con nome > ACL scaricabili, quindi fare clic su

JWIIIDau	able Act	Less Control	Lists				
ilter:		Match	fi	-	G0 🔻		
Nan	ne	- Descrip	tion				
No	data to d	lisplay					

8. Specificare il **nome** dell'ACL scaricabile e il **contenuto** dell'**ACL**. Fare clic su **Invia**.

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. Creazione dell'ACL scaricabile Sample-DACL

wnloadable Access Control Lists	Showing 1-1 of 1 50 Per page
ter: 💽 Match if 💽 🐨	
Name - Description	
Sample-DACL	

10. Per configurare i criteri di accesso per l'autenticazione VPN, scegliere Criteri di accesso > Servizi di accesso > Regole di selezione dei servizi e determinare il servizio che gestisce il protocollo RADIUS. Nell'esempio, la regola 1 corrisponde a RADIUS e Accesso alla rete predefinito soddisferà la richiesta RADIUS.



 Scegliere il servizio Access determinato dal passo 10. In questo esempio viene utilizzato Accesso di rete predefinito. Scegliere la scheda Protocolli consentiti e verificare che Consenti PAP/ASCII e Consenti MS-CHAPv2 siano selezionati. Fare clic su Invia.

Authe	ntication Protocols
• •	Allow PAP/ASCII
• □	Allow CHAP
• E	Allow MS-CHAPv1
• •	Allow MS-CHAPv2
• =	Allow EAP-MD5
•	Allow EAP-TLS
) E	Allow LEAP
• •	Allow PEAP
• 🔽	Allow EAP-FAST
Г	Preferred EAP protocol

12. Fare clic sulla **sezione Identità** di **Access Services** e verificare che **Internal Users** sia selezionato come Origine identità. Nell'esempio, è stato utilizzato l'accesso alla rete predefinito.



 Scegliere Criteri di accesso > Servizi di accesso > Accesso di rete predefinito > Autorizzazione, quindi fare clic su



14. Spostare **System:UserName** dalla colonna **Available** alla colonna **Selected** e fare clic su **OK**.



15. Per creare una nuova regola, fare clic su Create

andar	d Poli	cyl Excer	tion Poli	ex.					
ietwo	rk Ac	cess Aut	horizatio	n Policy		in a manufacture of the second		annanan annanan	
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	¥					
-	-								
	-	Detaun	-	If no fules define	ed of ho enabled rule	matches.	PermitAccess	0	in the second second
Create		Dupaca	te	Edit Delete	Move to	~			Customize Hit Coun

 Verificare che la casella di controllo accanto a System: UserName sia selezionata, scegliere uguale dall'elenco a discesa e immettere il nome utente 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. Fare clic su **Seleziona**.

o Secure ACS - Mozilla Fi	refox	
192.168.26.51 https://19	2:168.26.51/acsadmin/PolicyInputAction.do	-
General Name: Rule-2 The Custor policy cond	Status: Enabled	
Conditions		
NDG:Location:	ANY	
System:UserName:		
Authorization Profiles:	You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first profile defined.	
Select Deselect		
OK Cancel		Hel

18. Per creare un nuovo profilo di autorizzazione, fare clic su **Crea**.

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

19. Specificare un nome per il **profilo di autorizzazione**. Nell'esempio viene utilizzato **Sample-Profile**.

sco 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	
R	
Submit Cancel	

20. Scegliere la scheda **Common Tasks** e selezionare **Static** (Statica) dall'elenco a discesa per il valore **Downloadable ACL Name** (Nome ACL scaricabile). Scegliere il nuovo **DACL** (Sample -DACL) creato dall'elenco a discesa dei valori.

General Common Tasks	RADIUS A	tribute	25		
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					
18 Average 1 (P) I have been a state of	Dedirect on AC	i main	st also be defined		

### 21. Fare clic su

### Invia.

General Common Tasks	RADIUS Attrib	outes		
ACLS				
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:				
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	edirect an ACL r	must also be defined		

22. Verificare che la casella di controllo accanto a **Sample-Profile** (Profilo di autorizzazione appena creato) sia selezionata e fare clic su

OK.

uthorization Profiles	Showing 1-3 of 3 50 📩 per page G
illter: Match if: 00 🔻	
Name - Description	
DenvAccess	
Permit Access	
Sample-Profile	
Create Duplicate Edit Delete	Page 1 of 1

23. Dopo aver verificato che il nuovo **Profilo campione** sia selezionato nel campo **Profili di autorizzazione**, fare clic su

192.168.26.51 https://192	.168.26.51/acsadmin/PolicyInputAction.do	
Seneral Name: Rule-2	Status: Enabled	
The Custom policy condit	ize button in the lower right area of the policy rules screen controls whic ions and results are available here for use in policy rules.	h
NDG:Location:	-ANY-	
System:UserName:	equalscisco	
Results		
Authorization Profiles:		
Sample-Profile		
	defined in multiple suthorization profiles. Attributed authorization profiles. Attributed defined in multiple profiles will use the value from the profile defined.	ites e first
Select Deselect		
Cancel		

24. Verificare che la nuova regola (**Regola-2**) sia stata creata con System:UserName **uguale** alle condizioni **cisco** e **Sample-Profile** come risultato. Fare clic su **Salva modifiche**.

## Creazione della regola 2

Vetwo	rk Ac	cess Aut	horization	Policy					
Filter	Stat	15	2	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	Г		Bule-2	-ANY-	equals cisco	-ANY-	Sample-Profile	0	
	Г	Default		If no rules define	ed or no enabled rule r	natches.	PermitAccess	0	
 Creat	F	Default	te[•]	If no rules define	ed or no enabled rule r	natches.	PermitAccess	0	Customize

# Configurazione di ACS per ACL scaricabili per gruppo

Completare i punti da 1 a 12 di <u>Configure ACS for Downloadable ACL for Individual User</u> (Configura ACL scaricabili per un singolo utente) ed eseguire questa procedura per configurare un ACL scaricabile per un gruppo in un ACS Cisco Secure.

Nell'esempio, l'utente VPN IPsec "cisco" appartiene al gruppo di esempio.

L'utente **Sample-Group** cisco esegue l'autenticazione e il server RADIUS invia un elenco degli accessi scaricabile all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione <u>ACL scaricabili per utente/gruppo</u>.

 Nella barra di navigazione, fare clic su Utenti e archivi identità > Gruppi di identità, quindi fare clic su Crea per creare un nuovo





2. Fornire un nome di gruppo (**Sample-Group**) e fare clic su **Invia**.

General Mame:	Sample-Group		
Descriptio	n:		
👩 Parent:	All Groups	Select	
= Required	fields		

3. Scegliere Archivi identità utente > Archivi identità interni > Utenti, quindi selezionare l'utente cisco. Per modificare l'appartenenza ai gruppi di questo utente, fare clic su

nternal Use	ers				Showing 1-1 of 1 50 💌 pe	er page Go
Filter:		Match if:	•	0		
🗟 Statu	81	User Name 🔺	Identity Group	Description		
and the second second	1995	and the second se	All Shares and a			

4. Fare clic su **Seleziona** accanto al gruppo di identità

🗸 Name:	cisco	Status; E	nabled 💌	•	
Description					
Identity Gro	up: All Groups		Sele	Ly	
User Informat	on	uuune			
There are n	additional identity attrib	utes defined for use	r records		
Creation/Modi	ication Information				
Date Create	d: Wed Feb 15 16:32:25	IST 2012			
Date Modifie	d: Wed Feb 15 16:32:25	IST 2012			
Date Enable	d: Wed Feb 15 16:32:25	IST 2012			
Required t	elds				

5. Selezionate il gruppo appena creato (ovvero **Sample-Group**) e fate clic su **OK**.

Cisco Secure ACS - Mozilla Firefox	X
192.168.26.51 https://192.168.26.51/acsadmin/IdentityGroupsLPInputAction.do	
Identity Groups	Contract of the second s
Filter: Match if: Go 💌	
Name   Description	
C * All Groups Identity Group Root	
<ul> <li>Sample-Group</li> </ul>	
Create Duplicate File Operations Export	
POK Cancel	Help

6. Fare clic su

- Mamai	laiana	Ctature Enchlad	10
v Name.	[ciscu	Status, Enabled	10
Description:			
🤹 Identity Group:	All Groups:Sample-Group	Se	lect
User Information			
There are no a	dditional identity attributes d	lefined for user records	
an the later and			
Creation/Modifica	ation Information		
Date Created:	Wed Feb 15 16:32:25 IST 2	012	
Data Madified:	Wed Feb 15 16:32:25 IST 2	012	
Date woulded.		012	
Date Modified. Date Enabled:	Wed Feb 15 16:32:25 IST 2	~	
Date Modified: Date Enabled: = Required field	Wed Feb 15 16:32:25 IST 2 <mark>Is</mark>		
Date Modified: Date Enabled: # = Required field	Wed Feb 15 16 32:25 IST 2 Js		
Date Modified: Date Enabled: = Required field	Wed Feb 15 16:32:25 IST 2 Is		

Invia.

7. Scegliere Criteri di accesso > Servizi di accesso > Accesso di rete predefinito >

### Autorizzazione, quindi fare clic su Crea per creare una nuova

regola.

STANCE.	k Acc	ess Auth	iorization P	Policy		American and the second			
iter:	Statu	s	*	Match if: Equals	Enabled	Clear Fat	ter Go 🔻		
	Г	Status	Name	NDGLocation	Conditions System.UserName	Identity Group	Results Authorization Profiles	Hit Count	
			and the second						
		No data	to display						
	<b>C</b>	No data	to display	If no rules definer	d or no enabled rule n	natches.	Permit Access	0	

8. Verificare che la casella di controllo accanto a **Gruppo di identità** sia selezionata e fare clic su **Seleziona**.

Secure ACS - Mozilla Fi	irefox			
192.168.26.51 https://19	92.168.26.51/acsa	dmin/PolicyInputAc	tion.do	
General			_	
Name: Rule-1	Status	Enabled	<b>•</b> 0	
The Custor	nite butten in t	the lower dabt	area of the pollow	n loo paraon apatrola ubioh
policy cond	litions and resu	ults are availab	ile here for use in p	policy rules.
Conditions				
NDG:Location:	-ANY-			
System:UserName	-ANY-			
Identity Group:	lin			Select
			enned in multiple pro rofile defined.	nies will use the value from the first
Colori Decelori		~		
oelect Deselect				

9. Selezionate **Sample-Group**, quindi fate clic su **OK**.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFiter=IdentityGroup=IdentityGroup=	she fr
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	
OK Cancel	Help
	122

10. Fare clic su **Seleziona** nella sezione Profili di autorizzazione.

o Secure ACS - Mozilla F	irefox				
192.168.26.51 https://1	92.168.26.51/acs	admin/PolicyInput	Action.do		-
General Name: Rule-1	Statu mize button in	s: Enabled the lower righ	• of the policy rule	es screen controls which	
Conditions	-ANY-	uits are avail	able here for use in pol	icy rules.	
System:UserName	in -ANY-	▼ All G	roups:Sample-Group	Select	
			You may select multiple a defined in multiple profile profile defined.	uthorization profiles. Attribute s will use the value from the f	s Irst
Select Deselec		×			
OK Cancel					Hel

11. Per creare un nuovo profilo di autorizzazione, fare clic su **Crea**.

Cisco Secure ACS - Mozilla Firefox			×
192-168.26.51 https://192.168.26.51/acsadmin/NetworkAccessiPInputAction.do			
Authorization Profiles Show	ning 1-2 of 2 50	🔹 per page	Go
Filter: Match if. 00 🔻			
T Name - Description			
DerwAccess			
Permit Access			
Create Edit Delete	Page	1 of 1 💽	DAT
OK Cancel		н	elp

12. Specificare un nome per il **profilo di autorizzazione**. **Sample-Profile** è il nome utilizzato in questo

esempio.	
Lisco Secure ALS - Mozilla Firefox	
192-168.26.51 https://192.168.26.51/acsadmin/NetworkAccessDPInputAction.do	HAR STREET HOUSE - GUT & HARDARD HINNEY
General Common Tasks RADIUS Attributes	
Name: Sample-Profile	
Description:	
· = Required helds	
4	
Submit Cancel	

13. Scegliere la scheda **Common Tasks** e selezionare **Static** (Statica) dall'elenco a discesa per il valore **Downloadable ACL Name** (Nome ACL scaricabile). Scegliere il nuovo **DACL** 

# (Sample -DACL) creato dall'elenco a discesa

Valore.

ACLS Downloadable ACL Name: Static Value Sample-DAQ Filter-ID ACL: Not in Use Fromy ACL: Not in Use Voice VLAN Permission to Join: Not in Use VLAN VLAN ID/Name: Not in Use Reauthentication Reauthentication Reauthentication Reauthentication: QOS Input Policy Map: Not in Use QUIput Policy Map: Not in Use QU	General Common Tasks	RADIUS A	ttribut	es	
Downloadable ACL Name: Static   Static Value   Sample-DAQ Image: Static   Filter-ID ACL: Not in Use Proxy ACL: Not in Use Value Value Value Voice VLAN Permission to Join: Not in Use VLAN VLAN VLAN VLAN Reauthentication Reauthentication Timer: Not in Use Maintain Connectivity during Reauthentication: OOS Input Policy Map: Not in Use Solution Use Booluty Policy Map: Not in Use UBL Redirect URL Redirect	ACLS	1			
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  Accurate Accur	Downloadable ACL Name:	Static	٠	Sample-DAQ	
Proxy ACL: Not in Use   Voice VLAN   Permission to Join: Not in Use   VLAN   VLAN   VLAN ID/Name: Not in Use   Reauthentication   Reauthentication Timer:   Not in Use   Maintain Connectivity during Reauthentication:   QOS   Input Policy Map:   Not in Use   QOS   802.1X-REV   LinkSec Security Policy:   Not in Use   URL Redirect	Filter-ID 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:   Reauthentication:   QOS   Input Policy Map:   Not in Use   Output Policy Map:   Not in Use   B02.1X-REV   LinkSec Security Policy:   Not in Use   URL Redirect	Proxy ACL:	Not in Use	-		
Permission to Join: Not in Use   VLAN   VLAN ID/Name: Not in Use   Reauthentication   Reauthentication Timer: Not in Use   Maintain Connectivity during Reauthentication:   Reauthentication:   OOS   Input Policy Map:   Not in Use   Output Policy Map:   Not in Use   802.1X-REV   LinkSec Security Policy:   Not in Use	Voice VLAN				
VLAN   VLAN ID/Name:   Not in Use   Reauthentication   Reauthentication Timer:   Not in Use   Maintain Connectivity during Reauthentication:   Reauthentication:   Output Policy Map:   Not in Use   Output Policy Map:   Not in Use   802.1X-REV   LinkSec Security Policy:   Not in Use	Permission to Join:	Not in Use	-		
VLAN ID/Name: Not in Use   Reauthentication   Reauthentication Timer:   Not in Use   Maintain Connectivity during Reauthentication:   Reauthentication:   OOS   Input Policy Map:   Not in Use   Output Policy Map:   Not in Use   802.1X-REV   LinkSec Security Policy:   Not in Use	VLAN				
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	VLAN ID/Name:	Not in Use	*		
Reauthentication Timer: Not in Use  Maintain Connectivity during Reauthentication: OOS Input Policy Map: Not in Use  Output Policy Map: Not in Use  B02.1X-REV LinkSec Security Policy: Not in Use  URL Redirect URL Redirect	Reauthentication				
Maintain Connectivity during Reauthentication: QOS Input Policy Map: Not in Use BUL Not in Use UnkSec Security Policy: Not in Use URL Redirect	Reauthentication Timer:	Not in Use	*		
OOS         Input Policy Map:         Output Policy Map:         Not in Use         802.1X-REV         LinkSec Security Policy:         Not in Use         URL Redirect	Maintain Connectivity during Reauthentication:	1			
Input Policy Map: Not in Use  Output Policy Map: Not in Use  802.1X-REV LinkSec Security Policy: Not in Use  UBL Redirect	QOS				
Output Policy Map: Not in Use 802.1X-REV LinkSec Security Policy: Not in Use  UBL Redirect	Input Policy Map:	Not in Use	-		
802.1X-REV LinkSec Security Policy: Not in Use  URL Redirect	Output Policy Map:	Not in Use	*		
LinkSec Security Policy: Not in Use  URL Redirect	802.1X-REV				
URL Redirect	LinkSec Security Policy.	Not in Use	*		
When a URL is defined for Redirect an ACL must also be defined	URL Redirect When a URL is defined for f	Redirect an AC	Lmu	stalso be defined	

### 14. Fare clic su

#### Invia.

General Common Tasks	RADIUS Attributes	
ACLS		
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:		
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 P	edirect an ACL must also be defined	
IRI for Redirect	Natiollea	

15. Scegliere il profilo di autorizzazione Profilo di esempio creato in precedenza e fare clic su

OK.

New Contraction Designs	Charles d 2 at 2 at a second
unorization Profiles	Showing 7-3 or 3 [50 ] per page _
iller: Match if. 00 🔻	
Name A Description	
DerryAccess	
Permit Access	
Sample-Profile	
Create Durlicate Edit Delete	Page 1 of 1

16. Fare clic su

OK.

o Secure ACS - Mozilla Fi	irefox				
192.168.26.51 https://19	92.168.26.51/acs	admin/PolicyInput	tAction.do		UTAUX ES
General					
Name: Rule-1	Statu	s: Enabled	• •		
The Custor policy cond	mize button in Jitions and res	the lower rigi ults are avail	ht area of the policy rule lable here for use in pol	es screen controls which licy rules.	r
	-ANY-				
System:UserName	-ANY-				
Identity Group	lin	▼ All G	Foups:Sample-Group	Select	
Sample-Profile			You may select multiple a defined in multiple profile profile defined.	uthorization profiles. Attribut s will use the value from the	es first
Select Deselect	Ē	<u>×</u>			

17. Verificare che **Rule-1** sia stato creato con Identity Group **Sample-Group** come condizione e **Sample-Profile** come risultato. Fare clic su **Salva modifiche**.

Iwor	k Acc	ess Auth	erization F	Policy						
er.[	Statu	ś	-	Match if: Equals	Enabled	Clear Filter Go	*			
	F	Status	Name	NDGLocation	Condition System UserName	s Identity Group	Results Authorization Profiles	Hit Count		
-	100		,				October Destin	~		
			Rule-1	-ANY-	-#NF	in All Oroups: Sample-Group	Sample-Profile	0	]	
			Rule-1	-4016	-4015	in All Oroups: Sample-Group	Sample-Profile		]	

# Configurazione di ACS per ACL scaricabili per un gruppo di dispositivi di rete

Completare i punti da 1 a 12 di Configure ACS for Downloadable ACL for Individual User

(Configura ACL scaricabili per un singolo utente) ed eseguire questa procedura per configurare un ACL scaricabile per un gruppo di dispositivi di rete in un ACS sicuro Cisco.

Nell'esempio, il client RADIUS (ASA) appartiene al gruppo di dispositivi di rete **VPN-Gateway**.La richiesta di autenticazione VPN proveniente dall'ASA per l'utente "cisco" viene autenticata correttamente e il server RADIUS invia un elenco degli accessi scaricabili all'appliance di sicurezza. L'utente "cisco" può accedere solo al server 10.1.1.2 e nega tutti gli altri tipi di accesso. Per verificare l'ACL, consultare la sezione <u>ACL scaricabili per utente/gruppo</u>.

 Scegliere Risorse di rete > Gruppi di dispositivi di rete > Tipo di dispositivo, quindi fare clic su Crea per creare un nuovo gruppo di dispositivi di

Network Resources	Network Device Groups
Network Device Groups	
Location Device Type	Filter: Match if: Go 💌
Network Devices and AAA Cilients	F Name - Description
External Prox Servers	All Device Types All Device Types
3 Users and Identity Stores	
S Policy Elements	
🔓 Access Policies	
🔝 Monitoring and Reports	
🍓 System Administration	

2. Specificare il nome di un **gruppo di dispositivi di rete** (**gateway VPN** in questo esempio) e fare clic su

Device Group	- General	
o Name:	VPN-Gateways	
Descriptio	n.	
o Parent:	All Device Types	Sele
a = Required	fields	

 Scegliere Risorse di rete > Dispositivi di rete e client AAA, quindi selezionare il client RADIUS campione-asa creato in precedenza. Fare clic su Edit (Modifica) per modificare l'appartenenza al gruppo di dispositivi di rete del client RADIUS (asa).

Devices						Showing 1-1 of 1 50 💌 per page 0
		• Match if:		00 🗢		
lame		IP Address	Description	NDG:Location	NDG:Device Type	
emple-es	a	192,165,26,13/32		All Locations	All Device Types	
	Devices iame emole-es	ame •	Devices  Match If.  Match If.  P Address  P Address  P Address  P Address P Address P Address P A P A P A P A P A P A P A P A P A P A	Ame IP Address Description	ame ▲ IP Address Description NDG:Location ame ▲ 1921163:261:002 AFLocation	Devices  Match If:OO ▼ ameIP Address Description NDG:Location NDG:Device Type ampe-esa 192.1%5.26.13732 AF Locations AF Dence Types

4. Fare clic su **Seleziona** accanto al Tipo di dispositivo

Description:	imple-asa	
etwork Device G	roups	
ocation	All Locations	Select
evice Type	All Device Types	Select
© Single IP /	Address C IP Range(s) By Mask C IP Range(s) 6.13	► TACACS+ IT

5. Selezionare il gruppo di dispositivi di rete appena creato (ovvero **VPN-Gateway**) e fare clic su **OK**.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do	
Network Device Groups	
Filter: Match if: Go 🔻	
Name   Description	Ī
C *All Device Types All Device Types	
(• <u>VPN-Galleways</u>	
Create Dursteate Edit Delete L Site Operations Depart	
Creater Dupincate Euit Desete Fine Operations Export	
dk Cancel	Help

6. Fare clic su

#### Invia.

Name:	sample-asa	
Description:		
letwork Devic Location	All Locations	Select
Device Type	All Device Types:VPN-Gateways	Select
P Address Single IP: 192.16	P Address C IP Range(s) By Mask C IP Range(s) 3.26.13	Authentication Options TACACS+ RADIUS

 Scegliere Criteri di accesso > Servizi di accesso > Accesso di rete predefinito > Autorizzazione, quindi fare clic su Personalizza.

etwo	rk Aci	cess Auth	iorization	Policy							
iter:	Stat.	15	<u>×</u>	Match if Equals	Enabled	Clear Filter	90 V				
	<b>Г</b>	Status	Name	NDG:Location	Condition: System:UserName	s Identity Group	Resa Authorizatio	alts In Profiles	Hit Count		
**	Г	Default		If no rules define	d or no enabled rule n	atches.	PermitAcce	99	0		
eate		Dunlicat	0_1 = E	dit Delete	Move to	1				Sustemize	Hit Coun

8. Spostare NDG:Tipo di dispositivo dalla sezione Disponibile alla sezione Selezionato, quindi fare clic su

vailable:	Selected: NDG:Location	
Device Filler	System:UserName	
Eap Authentication Method	NDG:Device Type	
Eap Tunnel Building Method End Station Filter	24	
Protocol		
UseCase		
Nac Machina Authanticated 💦 🎽		

9. Per creare una nuova regola, fare clic su Create

Networ	rk Ac	cess Aut	norization P	Anticy					
Filter:	Stat	15	-	Match if Equals	Enabled	Ciear Fitter G	• •		
	<b>F</b>	Status	Name	NDG:Location	System:UserName	Conditions Identity Group	NDO:Device Type	Results Authorization Profiles	Hit Count
-	Г	Default		If no rules define	d or no enabled rule r	natches.		PermitAccess	0

10. Assicurarsi che la casella di controllo accanto a **NDG:Tipo di dispositivo** sia selezionata e scegliere **in** dall'elenco a discesa. Fare clic su

### Seleziona.

o Secure ACS - Mozilla Fi 192.168.26.51 https://19	efox 168.26.51/acsadmin/PolicyInputAct	non do
General Name: Rule-1 The Custor policy cond	Status: Enabled	area of the policy rules screen controls which le here for use in policy rules.
Conditions DDG:Location: System:UserName: Identity Group:	-ANY- -ANY- -ANY-	
NDG:Device Type:     Results     Authorization Profiles:	in 💌	Select
		u may select multiple authorization profiles. Attributes afined in multiple profiles will use the value from the first ofile defined.
Select Deselect	<u>_</u>	
DK Cancel		Hel

11. Scegliere il gruppo di dispositivi di rete **Gateway VPN** creato in precedenza e fare clic su **OK**.

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. Fare clic su **Seleziona**.

o Secure ACS - Mozilla Fi	efox	
192.168.26.51 https://19	2.168.26.51/acsadmin/PolicyInputAction.do	
General Name: Rule-1 The Custor policy condi	Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Enabled Status: Status	
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. Per creare un nuovo profilo di autorizzazione, fare clic su **Crea**.

Cisco Secure ACS - Mozilla Firefox	×
192-168.26.51 https://192.168.26.51/acsadmin/NetworkAccessLPInputAction.do	<u>(</u>
Authorization Profiles	Showing 1-2 of 2 50 💌 per page Go
Filter: Match if: 30 V	
T Name - Description	
DerwAccess	
Permit Access	
Create Developeda Call Datata	
Consert Contraction Content	Page 1 011
OK Cancel	Help
	31

14. Specificare un nome per il **profilo di autorizzazione**. **Sample-Profile** è il nome utilizzato in questo

sempio. sco 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	
N	
1-3	
ubmit Cancel	

15. Scegliere la scheda **Common Tasks** e selezionare **Static** (Statica) dall'elenco a discesa per il nome dell'ACL scaricabile. Selezionare il nuovo **DACL (Sample-DACL)** creato dall'elenco

### a discesa dei

#### valori.

General Common Tasks	RADIUS A	ttribute	28		
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 When a URL is defined for f	Redirect an AC	L mu	stalso be defined		
UDL for Dedirect	Not in Lloo	-			

### 16. Fare clic su

### Invia.

ACLS			
Downloadable ACL Name: St	latic 💌	Value Sample-DACL	
Filter-ID ACL:	ot in Use 👱	]	
Proxy ACL: N	ot in Use 💌	1	
Voice VLAN			
Permission to Join: No	ot in Use 💌	]	
VLAN			
VLAN ID/Name: N	ot in Use 💌	]	
Reauthentication			
Reauthentication Timer: No	ot in Use 💌	1	
Maintain Connectivity during Reauthentication:			
QOS			
Input Policy Map: No	ot in Use 💽 💌	]	
Output Policy Map:	ot in Use 💌	1	
802.1X-REV			
LinkSec Security Policy. No	ot in Use 💌	1	
URL Redirect		-	
When a LIRL is defined for Redi	rect an ACL m	ust also be defined	

17. Selezionate Sample-Profile creato in precedenza e fate clic su

OK.

utho	rization Profiles				Showing 1-4 of 4 50	T bei bage
liter.		Match if:	-	00 7		
	Name 🔺	Description				
	DemyAccess					
	Filter-Id					
	Permit Access					
7	Sample-Profile					
0	ata   Divellenta					

## 18. Fare clic su

Secure ACS - Mozilla F	irefox
192.168.26.51 https://1	
	92:168.26.51/acsadmin/PolicyInputAction.do
General	
Name: Rule-1	Status: Enabled 🗾 🥯
A The Custor	mize button in the lower right area of the policy rules screen controls which
policy cond	litions 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
Results	
Authorization Profiles:	
Sample-Profile	
	You may select multiple authorization profiles. Attributes
	defined in multiple profiles will use the value from the first
	prome desired.
	-
Outrus   Desiring	
Select Deselect	

19. Verificare che la **regola 1** venga creata con **VPN-Gateway** come condizione NDG:Device Type e come risultato **Sample-Profile**. Fare clic su **Salva** modifiche

two	rik Aci	cess Auth	orization	Policy					
ter:	Statu	uś	-	Match if: Equal	s 💌 Enabled	· Clear Fi	iller Ga 🔻		
	F	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
	F	Default		If no rules define	ad or no enabled rule (	matches.		PermtAccess	0

## Configurare le impostazioni RADIUS IETF per un gruppo di utenti

Per scaricare dal server RADIUS il nome di un elenco degli accessi già creato sull'accessorio di sicurezza durante l'autenticazione, configurare l'attributo IETF RADIUS filter-id (numero attributo 11):

#### filter-id=acl\_name

L'**utente** Sample-Group esegue l'autenticazione e il server RADIUS scarica un nome ACL (nuovo) per un elenco degli accessi già creato sull'appliance di sicurezza. L'utente "cisco" può accedere a tutti i dispositivi che si trovano all'interno della rete dell'ASA, **ad eccezione** del server 10.1.1.2. Per verificare l'ACL, consultare la sezione <u>ACL Filter-Id</u>.

Come mostrato nell'esempio, l'ACL con nome **new** è configurato per il filtro nell'appliance ASA:

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

Questi parametri vengono visualizzati solo quando sono veri. È stato configurato:

- Client AAA per utilizzare uno dei protocolli RADIUS in Configurazione rete
- Nella sezione dei risultati della regola in Access-Service viene selezionato un profilo di autorizzazione con ID filtro RADIUS (IETF).

Gli attributi RADIUS vengono inviati come profilo per ogni utente da ACS al client AAA richiedente.

Completare i passaggi da 1 a 6 e da 10 a 12 di <u>Configurazione di ACS per ACL scaricabili per un</u> <u>singolo utente</u>, quindi i passaggi da 1 a 6 di <u>Configurazione di ACS per ACL scaricabili per un</u> <u>gruppo</u>, quindi eseguire i passaggi descritti in questa sezione per configurare Filter-Id in Cisco Secure ACS.

Per configurare le impostazioni degli attributi **RADIUS IETF** da applicare come nel profilo di autorizzazione, eseguire la procedura seguente:

1. Scegliere Elementi dei criteri > Autorizzazioni e autorizzazioni > Accesso di rete > Profili di autorizzazione, quindi fare clic su Crea per creare un nuovo profilo di

2. Specificare un nome per il **profilo di autorizzazione**. **Filter-Id** è il nome del profilo di autorizzazione scelto in questo esempio per semplicità.

General	Common Tasks	RADIUS Attributes	
Name:	Filter-Id T		
Descri	ption:		
= Requir	ed fields		
1.1.1			

 Fare clic sulla scheda Attività comuni e scegliere Statico dall'elenco a discesa per ACL Filter-ID. Immettere il nome dell'elenco accessi come nuovo nel campo Valore e fare clic su Invia.

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	at also be defined
URL for Redirect	Not in Use	-	
URL Redirect ACL:	Not in Use	+	
= Required fields			

4. Scegliere Criteri di accesso > Servizi di accesso > Accesso di rete predefinito > Autorizzazione, quindi fare clic su Crea per creare una nuova

Indar	d Poli	Cyl Except	tion Policy	Y						
etwo	rk Aci	cess Auth	orization	Policy						
Filter:	Statu	18	*	Match if: Equals	s 💌 Enabled	Clear Filter 0	0 -			
	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	d or no enabled rule r	matches.	PermitAccess	0		
ret N		Duplicat	8. 1• E	Edit Delete	Move to				Customize	Hit Coun

5. Verificare che la casella di controllo accanto a **Gruppo di identità** sia selezionata e fare clic su **Seleziona**.

ins ins at st hit i			and the second	-
192.168.26.51 https://	192.168.26.51/a	tsadmin/PolicyInputAction.do	PART INTERIO IN CONTRACTOR INCOME IN CASE OF PRIMA	
General				
Name:  Rule-1	Sta	tus: Enabled 🗾 🔘		
The Cuet	omize button i	n the lower right area o	f the policy rules ecreen controls which	
policy cor	nditions and re	esults are available here	e for use in policy rules.	
Para Reference				
NDG:Location:	-ANY-			
C System LiserNam	ANY			
V Identity Group	lin	-	Select	
Decute	1			
Vesuits Authorization Drafiles:				
Autronzation Promes.				
		<u></u>		
		You may	select multiple authorization profiles. Attributes	
		defined in profile da	In multiple profiles will use the value from the first	
		prome de	sineu.	
		S.		
		-1		
	and a second			
	100 F			
Select Deseld	2.41			
Select Desele	264			
Select Desele	244			
Select Desele	244			
Select Desele	244			
Select Desele				

6. Selezionate **Sample-Group**, quindi fate clic su **OK**.

Cisco Secure ACS - Mozilla Firefox	×
192.168.26.51 https://192.168.26.51/acsadmin/NetworkDeviceGroupLPInputAction.do?contextData.externalFilter=IdentityGroup=IdentityGroup=stric	3
Network Device Groups	Г
Filter: Match if: Go 💌	
Name Description	
Create Duplicate Edit Delete File Operations Export	
RK Cancel Help	

7. Fare clic su **Seleziona** nella sezione Profili di autorizzazione.

) Secure ACS - Mozilla Fi	irefox				
192.168.26.51 https://19	92.168.26.51/ac	sadmin/PolicyInputA	ction.do		
General					
Name: Rule-1	Stat	us: Enabled	• •		
The Custor policy cond	nize button i litions and re	n the lower right sults are availa	area of the policy n ble here for use in p	ules screen controls which olicy rules.	r.
	-ANY-				
System UserName	-ANY-				
V Identity Group	lin	▼ All Gro	oups:Sample-Group	Select	
			You may select multiple defined in multiple profi profile defined.	authorization profiles. Attribut lies will use the value from the	es first
Select Deselect		2			

8. Scegliere l'**ID filtro del** profilo di autorizzazione creato in precedenza e fare clic su **OK**.

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 page Go
Filter. Match if. 30 💌	
Name      Description	
DemyAccess	
Filter-Id	
Permit Access	
Sample-Profile	
Create Duplicate Edit Delete	Page 1 of 1
<u>ek</u> Cancel	Help

9. Fare clic su **OK**.

Secure ACS - Mozilla	Firefox	MADE TO		
192.168.26.51 https://	192.168.26.51/	csadmin/Policy1	InputAction, do	STREET BOOK COMPANY
General Name: Rule-1 The Cust policy cor	Standard Sta	atus: Enable in the lower results are a	d right area of the policy rule wallable here for use in pol	es screen controls which icy rules.
Conditions	LANN			
System:UserNam	-ANT-			
Identity Group:	in	-	All Groups:Sample-Group	Select
			defined in multiple profile profile defined.	s will use the value from the first
Select Desele	ct	-	-	

 Verificare che Rule-1 sia stato creato con Identity Group Sample-Group come condizione e Filter-Id come risultato. Fare clic su Salva modifiche.

-two	rk Act	ess Auth	orization	Policy					
iller	Statu	8	*	Match if Equals	s 💌 Enabled	Clear Filter 00	<b>v</b>		
	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	
-	Г	Default		If no rules define	rd or no enabled rule m	natches	PermitAccess	0	

# Configurazione client VPN Cisco

Per verificare che l'ASA sia configurata correttamente, connettersi all'appliance Cisco ASA con il client VPN Cisco.

Attenersi alla seguente procedura:

- 1. Scegliere Start > Programmi > Cisco Systems VPN Client > VPN Client.
- Fare clic su New per avviare la finestra Create New VPN Connection Entry (Crea nuova voce di connessione VPN).

👌 status: Disconnected   VPN Client - Versio	n 5.0.07.0410	_ D ×
Connection Entries Status Certificates Log Op	tions Help	
Connect New Import Modify	Delete	cisco
Connection Entry	Host	Transport
Connection Entry	Host	I ransport
4		
Not connected.		
Account	Transfer	

3. Specificare i dettagli della nuova connessione:Immettere il nome della voce di connessione insieme a una descrizione.Immettere l'**indirizzo IP esterno dell'appliance ASA** nella casella Host.Immettere il nome del gruppo di tunnel VPN (**Cisco-Tunnel**) e la password (chiave già condivisa - **cisco123**) come configurato nell'ASA.Fare clic su

a finite second second				
Connection Entry;	Sample-Connec	otion		11. 11.
Description:				CISCO.
Host:	172.16.1.1			cisco
Authentication	Transport	Backup Servers	Dial-Up	
Group Auther	ntication		C Mutual Gr	oup Authenticatior
Name:	Cisco-Tun	nel		
Password:	******			
Confirm Passw	vord:			
C Certificate Au	thentication			
Name:		0.02.0		

4. Fare clic sulla connessione che si desidera utilizzare e fare clic su **Connetti** nella finestra principale del client

Connection Entry         Log           Connection Entry         Host         Transport           Sample-Connection         172.16.1.1         IPSec/UDP	Corf.ect	New New	∠i Ioa Import	Modify	Delete		cisco
Sample-Connection 172.16.1.1 IPSec/UDP	Connection Entrie	onnection	Entry /	· I		Host	Transport
	•						

5. Quando richiesto, immettere il nome utente **cisco** e la password **cisco123** come configurato nell'appliance ASA per l'autenticazione e fare clic su **OK** per connettersi alla rete

The server has reque	sted the following information to complete the user
aumenication.	
uluit, Username:	cisco
CISCO Password	
Fassword:	January 199

6. Una volta stabilita la connessione, scegliere **Statistics** dal menu Status per verificare i dettagli del

Connection Entries	Status Certificates Log O	ptions Help	
Connect N	Ratistics Ctrl+5 Notifications Ctrl+N		alialia
Connection Entries	Reset Stats		
Con	nection Entry	Host	Transport
Sam	ple-Connection	172.16.1.1	IPSec/UDP

# **Verifica**

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

## Mostra comandi di crittografia

• show crypto isakmp sa: visualizza tutte le associazioni di sicurezza IKE correnti in un peer. 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
     IKE Peer: 172.16.1.50
          eer: 1,2...
: user Role . ....
Role . ...
State : AM_ACTIVE
     Type
     Rekev
 ciscoasa#

    show crypto ipsec sa: visualizza le impostazioni utilizzate dalle associazioni di protezione

 correnti.
 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 scaricabile per utente/gruppo

Verificare l'ACL scaricabile per l'utente Cisco. Gli ACL vengono scaricati dai CSACS.

### **ACL Filter-Id**

L'ID filtro [011] è stato applicato al gruppo Group - Sample-Group e gli utenti del gruppo vengono filtrati in base all'ACL (nuovo) definito nell'ASA.

# Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione. Viene visualizzato anche l'output di esempio del comando **debug**.

Nota: per ulteriori informazioni sulla risoluzione dei problemi relativi alla VPN IPsec di accesso remoto, vedere <u>Soluzioni per la risoluzione dei problemi relativi alla VPN IPsec di accesso remoto e L2L più comuni</u>.

#### Cancella associazioni di protezione

Quando si esegue la risoluzione dei problemi, assicurarsi di cancellare le associazioni di

protezione esistenti dopo aver apportato una modifica. In modalità privilegiata di PIX, utilizzare i seguenti comandi:

- clear [crypto] ipsec sa Elimina le SA IPsec attive. La parola chiave crypto è facoltativa.
- clear [crypto] isakmp sa Elimina le associazioni di protezione IKE attive. La parola chiave crypto è facoltativa.

# Comandi per la risoluzione dei problemi

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

- debug crypto ipsec 7: visualizza le negoziazioni IPsec della fase 2.
- debug crypto isakmp 7: visualizza le negoziazioni ISAKMP della fase 1.

# Informazioni correlate

- <u>Cisco ASA serie 5500 Adaptive Security Appliance Pagina di supporto</u>
- Riferimenti per i comandi di Cisco ASA serie 5500 Adaptive Security Appliance
- <u>Cisco Adaptive Security Device Manager</u>
- Pagina di supporto per la negoziazione IPsec/i protocolli IKE
- Pagina di supporto per Cisco VPN Client
- <u>Cisco Secure Access Control System</u>
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems