# Configurazione di Secure Client IKEv2/ASA in ASDM con AAA & Cert Auth

# Sommario

Introduzione
Prerequisiti
Requisiti
<u>Componenti usati</u>
Esempio di rete
Conligurazione in ASDM Responsibilità Aprilia respondure quidate V/PN
Passaggio 2. Identificazione profile di connecsione
Passargio 3. Protocolli VPN
Passaggio 4. Immagini client
Passaggio 5. Metodi di autenticazione
Passaggio 6. Configurazione SAML
Passaggio 7. Assegnazione indirizzo client
Passaggio 8. Server di risoluzione dei nomi di rete
Passaggio 9. Esente da NAT
Passaggio 10. Installazione client sicura
Passaggio 11. Salva impostazioni
Passaggio 12. Conferma ed esporta profilo client protetto
Passaggio 13. Conferma dettagli profilo client protetto
Passaggio 14. Conferma impostazioni nella CLI di ASA
Passaggio 15. Aggiungi algoritmo di crittografia
Configurazione in Windows Server
Configurazione in ISE
Passaggio 1. Aggiungi dispositivo
Passaggio 2. Aggiungi Active Directory
Passaggio 3. Aggiungi sequenza di origine identità
Passaggio 4. Aggiungi set di criteri
Passaggio 5. Aggiungi criterio di autenticazione
Passaggio 6. Aggiungi criterio di autorizzazione
Verifica
Passaggio 1. Copia profilo client sicuro in Win10 PC1
Passaggio 2. Avvia connessione VPN
Passaggio 3. Conferma syslog su ASA
Passaggio 4. Conferma sessione IPsec su ASA
Passaggio 5. Conferma registro dinamico Radius
Risoluzione dei problemi
Passaggio 1. Avvia connessione VPN
Passaggio 2. Conferma syslog nella CLI
Riferimento

# Introduzione

In questo documento viene descritto come configurare un client sicuro su IKEv2 su un'appliance ASA usando ASDM con AAA e autenticazione dei certificati.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco Identity Services Engine (ISE)
- Configurazione di Cisco Adaptive Security Virtual Appliance (ASAv)
- Configurazione di Cisco Adaptive Security Device Manager (ASDM)
- Flusso di autenticazione VPN

## Componenti usati

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

- Patch 1 di Identity Services Engine Virtual 3.3
- Adaptive Security Virtual Appliance 9.20(2)21
- Adaptive Security Device Manager 7.20(2)
- Cisco Secure Client 5.1.3.62
- Windows Server 2016
- Windows 10

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.

# Esempio di rete

Nell'immagine è illustrata la topologia utilizzata per l'esempio del documento.

Il nome di dominio configurato in Windows Server 2016 è ad.rem-system.com, utilizzato come esempio in questo documento.



Esempio di rete

# Configurazioni

## Configurazione in ASDM

Passaggio 1. Apri procedure guidate VPN

Passare a Creazioni guidate > Creazioni guidate VPN, fare clic su Creazione guidata VPN client sicura.



#### Fare clic su Next (Avanti).

Secure Client VPN Conne	ction Setup Wizard	$\times$
VPN Wizard	Introduction	
	Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Client. The connections will be protector using either the IPsec or the SSL protocol. The ASA will automatically upload the Secure VPN Client to the end user's device when a VPN connection is established. VPN Remote Access	rd
	< Back Next > Right Help	

Fare clic sul pulsante Avanti

Passaggio 2. Identificazione profilo di connessione

Immettere le informazioni per il profilo di connessione. Nome profilo connessione : vpn-ipsec-tunnel-grp Interfaccia di accesso VPN : esterna

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Connection Profile Identification	
1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN	
2. Connection Profile	connections.	
3. VPN Protocols	Connection Profile Name: vpn-ipsec-tunnel-grp	
4. Client Images	UTM Access Takedaces	
5. Authentication Methods	VPN Access Likelitace:	
6. SAML Configuration		
7. Client Address Assignme		
<ol> <li>Network Name Resolutio Servers</li> </ol>		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	< gack Next > Help	

Identificazione profilo di connessione

#### Passaggio 3. Protocolli VPN

Selezionare IPsec, fare clic su Aggiungi pulsante per aggiungere un nuovo certificato autofirmato.

Secure Client VPN Conn	ection Setup Wizard	Manage Identity Certificates
Steps	VPN Protocols	Tequed To Tequed By Evolv Date Associated Trustrophy I kane Duble Vev Type Add
1. Introduction	Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you	Associated in associated in angle in a social of the participation of th
2. Connection Profile Identification	would like this connection profile to support.	Show Decas
3. VPN Protocols 4. Client Images	SSL Prec	Export
5. Authentication Methods		Install
6. SAML Configuration	Device certificate identifies the ASA to the remote access clients. Certain Secure	De Forel
7. Client Address Assignme	Client features (Always-On, IPsec/IKEv2) require that valid device certificate be	Kechton
8. Network Name Resolutio	available on one ASA.	
9. NAT Exempt	Device Certificate: None V Manage	
10. Secure Client Deployme		
11. Summary		
		Find: Match Case
		Certificate Expiration Alerts
		Send the first alert before : 60 (days) Set Default
	<back next=""> 現初 Heb</back>	Repeat Alert Interval : 7 (days)
		Weak Crypto Configurations
		Permit Weak key sizes and Hash Algorithms
		Public CA Enrolment
		Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.
		Enroll ASA SSL certificate with Entrust
		Liston a reavisuativ saved certificate circles request, errol with Entrust
		owing a promotion of the original sequence and the second s
		ASDM Identity Certificate Wizard The Circo ASDM Identity Certificate Wizard enricht you in creation a cellicioned certificate that is required for launching
		ASDM through launcher.
		Launch ASDM Identity Certificate Wizard
		OK Cancel Help

Immettere le informazioni per il certificato autofirmato.

Nome punto di fiducia : vpn-ipsec-trustpoint

#### Coppia di chiavi: ipsec-kp

Add Identity Certificate X	📧 Add Key Pair	×
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: ORSA OECDSA OEDDSA	
Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):		
Decryption Passphrase:	Name: Use default key pair name	
File to Import From: Browse	Enter new key pair name: psec-kp	
• Add a new identity certificate:	Size: 4096 V	
Key Pair: ipsec-lip V Show New	Usage: O General purpose O Special	
Certificate Subject DN: CN=ciscoasa Select		
Generate self-signed certificate     Generate self-signed certificate     Act as local certificate authority and issue dynamic certificates to TLS-Proxy	Generate Now Cancel Help	
_		
Advanced		
C Enable CA flag in basic constraints extension		
Add Certificate Cancel Help		

Dettagli del certificato autofirmato

## Confermare le impostazioni dei protocolli VPN, quindi fare clic su Next button.

Secure Client VPN Conne	ection Setup Wizard	×
Steps         1. Introduction         2. Connection Profile Identification         JUPN Protocols         4. Client Images         5. Authentication Methods         6. SAML Configuration         7. Client Address Assignme         8. Network Name Resolutio Servers         9. NAT Exempt         10. Secure Client Deployme         11. Summary	VPN Protocols Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols yo would like this connection profile to support. SSL Prvice Certificate Device Certificate Device certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/B:Ev2) require that valid device certificate be available on the ASA. Device Certificate: vpn-ipsec-trustpoint:unstructuredNamv Manage	u
	< Back Next > It if) Help	

Conferma impostazioni protocollo VPN

#### Passaggio 4. Immagini client

Fare clic su Add button per aggiungere un'immagine client sicura, quindi fare clic su Next button.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Client Images	
Introduction     Connection Profile     Identification     VPN Protocols     Client Images	ASA can automatically upload the latest Secure Client package to the A regular expression can be used to match the user-agent of a brow You can also minimize connection setup time by moving the image up the top of the list.	he client device when it accesses the enterprise network. wser to an image. sed by the most commonly encountered operation system to
<ol> <li>S. Authentication Methods</li> <li>SAML Configuration</li> <li>Client Address Assignme</li> <li>Network Name Resolutio Servers</li> <li>NAT Exempt</li> <li>Secure Client Deployme</li> <li>Summary</li> </ol>	Image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-49.pkg	Regular expression to match user-agent
	You can download Secure Client packages from <u>Cisco</u> by searching	'Secure Mobility Client' or <u>click here</u> ,
	< gack Mext >	Ikin Help

Immagini client

#### Passaggio 5. Metodi di autenticazione

Fare clic su Nuovo pulsante per aggiungere un nuovo server aaa, fare clic su Avanti pulsante.

Nome gruppo server : radius-grp

Protocollo di autenticazione : RADIUS

Indirizzo IP server : 1.x.x.191

#### Interfaccia : interna

Secure Client VPN Cons	ection Setup Witard X	To New Authentication Server Group	< 1	Secure Client VPN Connec	tion Setup Wizard X
Page 1. Pithology 2. Conversion In Yells Selections 3. Mithological 4. Other Langest 5. Static-Information 7. Cert Addess Anapone 6. Selec Configuration 7. Cert Addess Anapone 6. Selec Configuration 7. Cert Addess Anapone 5. Mat Lossey 19. Secure Cert Deployme 11. Sammary	Auf detections Vehicles The care days our week access access are erg aga, AAA Server Grag. 1004 End Server States Codes Load Server States Code to Adade Code to Adade Code to Adade Code to Code	Create a new authentication server group containing one authentication server. To add more servers to the group or drange other AAA server settings, go to Configuration Device Hanagemet > Users/AAA > AAA Server Group. Server Group Name: Authentication Protocol: Server IP Address: Interface: Interface:		Args 1. Ho to dutton 2. Ko to dutton 3. Mon to dutton 1. Mon to dutton 1. Mon to dutton Mon to dutton Mon to dutton 1. Markon Same Realized Servers 1. Markon Stand 1. Samendo 1. Same Configuration 1. Markon Stand 1. Samendo 1. Same	Aufwertscheinen Heiholds Hen keine bester ung werden Heiholdsen eineren: Hau der der der einer Aufwertscheinen Besternen graupe. Auß Gerein Graupe Indeen gerichten
	64 (94) (94)	Server Secret Key: Confirm Server Secret Key:		(	(b)
		OK Cancel Help			

#### Passaggio 6. Configurazione SAML

#### Fare clic sul pulsante Avanti.

Secure Client VPN Conne	ection Setup Wizard	×
Steps	SAML Configuration	
<ol> <li>Introduction</li> <li>Connection Profile Identification</li> <li>VPN Protocols</li> <li>Client Images</li> <li>Authentication Methods</li> <li>SAML Configuration</li> <li>Client Address Assignme</li> <li>Network Name Resolutio Servers</li> <li>NAT Exempt</li> <li>Secure Client Deployme</li> <li>Summary</li> </ol>	This step allows you to configure a SAML and the authentication method. Authentication Method: AAA Arr AAAA Arr AAAAA Arr AAAAA Arr AAAAA Arr AAAAA Arr AAAA Arr AAAA Arr AAAAAAA Arr AAAAAAAA	
	< gack Next > Rifl Help	

Configurazione SAML

Passaggio 7. Assegnazione indirizzo client

Fare clic sul pulsante New (Nuovo) per aggiungere un nuovo pool IPv4, fare clic sul pulsante Next (Avanti).

Nome : vpn-ipsec-pool

Indirizzo IP iniziale: 172.16.1.20

Indirizzo IP finale : 172.16.1.30

Subnet mask: 255.255.255.0

Secure Client VPN Connection	ection Setup Wizard	X	Secure Client VPN Conne	ection Setup Wizard	×
Steps  I. Introduction  C. Connection Notife Identification  VPN Protocols  A Uthert Images  Authentication Nethods  S. Auth-entication Nethods  S. Auth-entication Nethods  N. Client Address Assignment  N. Network Name Resolutio Servers  N. Nat Secure Client Deployme  S. Summary	Clerk Address Assignment This step allows you to create a new address pool or select an be assigned addresses from the pools when they correct. IPv6 address pool is only supported for SSL connection. Address Pool:Select	existing address pool for IPv4 and IPv6. The Secure Clients will dd IPv4 Pool X ne: tring IP Address: I72.16.1.20 net Mask: S55.255.255.0 OK Cancel Help	Steps   I. Introduction  C. Connection Profile Identification  VPN Protocols  C. Carlinguration  S. Authentication Nethods  S. Authentication  S. Authenti	Clerk Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The Secure Clerks be assigned address pool is only supported for SSL connection. IPv6 address pool Address Pool Address Pool Clerk address Details of the selected address pool Starting IP Address: IP2-16-1.30 Submet Masi: 255-255-255-0	i vol
	< Back Next >	Riff Help		<back next=""> 限的 He</back>	tip 📄

Assegnazione indirizzo client

Passaggio 8. Server di risoluzione dei nomi di rete

Immettere le informazioni per il DNS e il dominio, fare clic su Avanti pulsante.

Server DNS : 1.x.x.57

#### Nome dominio: ad.rem-system.com

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Network Name Resolution Servers	
<ol> <li>Introduction</li> <li>Connection Profile Identification</li> <li>VPN Protocols</li> <li>Client Images</li> <li>Authentication Methods</li> <li>SAML Configuration</li> <li>Client Address Assignme</li> <li>Network Name Resolution Servers</li> <li>NAT Exempt</li> <li>Secure Client Deployme</li> <li>Summary</li> </ol>	This step lets you specify how domain names are resolved for the remote user when accessing the internal network. DNS Servers: Domain Name: ad.rem-system.com	
	< Back Next > It if He	de la

Server di risoluzione dei nomi di rete

#### Passaggio 9. Esente da NAT

Fare clic sul pulsante Avanti.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	NAT Exempt	
Introduction     Connection Profile     Identification     VPN Protocols     Client Images     Authentication Methods     SAML Configuration     Client Address Assignme     Network Name Resolutio     Servers     NAT Exempt     Summary	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.	
	< Back Next >	Help

Esente da NAT

## Passaggio 10. Installazione client sicura

## Selezionare Consenti avvio Web, quindi fare clic su Pulsante Avanti.

Secure Client VPN Conne	ction Setup Wizard X
Steps	Secure Client Deployment
1. Introduction	Secure Client program can be installed to a client device by one of the following two methods:
<ol> <li>Connection Profile Identification</li> </ol>	<ol> <li>Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed;</li> <li>Pre-deployment - Manually install the Secure Client package.</li> </ol>
3. VPN Protocols	
4. Client Images	Allow Web Launch
5. Authentication Methods	Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will
7. Client Address Assignme	NOT work if it is turned off.
8. Network Name Resolutio Servers	For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA
9. NAT Exempt	in your Secure Client package, otherwise IPsec connection will NOT work.
10. Secure Client Deployment	
11. Summary	
	< gack Next > 現初 Help

#### Passaggio 11. Salva impostazioni

Fare clic su Fine per salvare le impostazioni.

Secure Client VPN Conne	ection Setup Wizard		× 🖾 Warning ×
VPN Wizard	Summary Here is the summary of the configuration.		ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning
	Name Summary Name/Alas of the Connection Profile VPN Access Interface Device Digital Certificate VPN Protocols Enabled Secure Client Images Authentication Server Group SAML Address Pool for the Client DNS Network Address Translation	Value       vpn-ipsec-trustpointcunstructuredName=ciscoasa, CN       Psec only       1 package       radus-orp       Server:       Authentication Method: asa       1 72.16.1.20 - 172.16.1.30       Server:       Domain Name:       The subjected to fific can be subjected to network address translation	<ul> <li>[Oil] p local pool ypn-ipsec-pool 172.16.1.30-172.16.1.30 mask 255.255.355.05</li> <li>[Oil] p local pool ypn-ipsec-tunnel-grp_clerk_profile_xml to ASA</li> <li>[Oil] webvyn</li> <li>[Oil] avy connect profiles vpn-ipsec-tunnel-grp_clerk_profile_kml (bill)</li> <li>[Oil] awy connect profiles vpn-ipsec-tunnel-grp_clerk_profile_kml</li> <li>[Oil] awa -server raduu-grp protocol radus</li> <li>[Oil] awa -server raduu-grp (inside) host 1.1:191</li> <li>[Oil] is wr</li> <li>[Oil] is wr</li> <li>[Oil] group-polky GroupFolky_ypn-ipsec-tunnel-grp attributes</li> <li>[Oil] you-polky GroupFolky_ypn-ipsec-tunnel-grp attributes</li> <li>[Oil] you-polky GroupFolky_ypn-ipsec-tunnel-grp attributes</li> <li>[Oil] you-polky GroupFolky_ypn-ipsec-tunnel-grp_clerk_profile type user</li> <li>[Oil] wr</li> <li>[Oil] wr on profiles value vpn-ipsec-tunnel-grp_clerk_profile type user</li> <li>[Oil] you-polky GroupFolky_vpn-ipsec-tunnel-grp_clerk_profile type user</li> <li>[Oil] you-polky GroupFolky vpn-ipsec-tunnel-grp_clerk_profile type user</li> <li>[Oil] you-polky GroupFolky vpn-ipsec-tunnel-grp_profile type user</li> <li>[Oil] you-polky GroupFolky vpn-ipsec-tunnel-grp_profile type user</li> </ul>

Salva impostazioni

#### Passaggio 12. Conferma ed esporta profilo client protetto

Selezionare Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profilo client protetto, quindi fare clic sul pulsante Modifica.

Eile View Iools Wigards Window Help	re 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help			Type topic to search Ge	cisco
Device List Bookmarks	Configuration > Remote Access VPN > Network (Client)	Access > Secure Client Profile			
Boolmarks <u>a</u> Q X X To boolmark a page, right-click on a node in the navigation bree and select "Add to boolmarks". G G Delete	This panel is used to manage Secure Client Profiles and perfor upload and download of client profiles between local machine. The profile Usage field is introduced with the Secure Mobility S	m group assignment for Secure Clent version 2.5 or later and device. olution. This field contains different profile usage in Secur	You can select a profile to edit, change group or to delete. You can sele e Client version 3.0 and later.	xt the 'Add' button to add a new profile. Pressing the Import or Export butto	n is for
Remote Access VPN 🗗 🖗	🗣 Adc 🗭 Edt 🔀 Change Group Policy 🏦 Delete 👪	Import 🖏 Export 🔊 Validate			
Introduction     Metwork (Client) Access	Profile Name	Profile Usage	Group Policy	Profile Location	
Secure Client Connection Profiles	vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	dsk0:/vpn-ipsec-tunnel-grp_client_profile.xml	
Secure Client Profile					

Modifica profilo client protetto

Confermare il dettaglio del profilo.

- Nome visualizzato (obbligatorio) : ciscoasa (IPsec) IPv4
- FQDN o indirizzo IP : 192.168.1.1
- Protocollo primario: IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grp	o_client_profile					Server List Entry					×	
Profile: vpn-ipsec-tunne	l-grp_client_pr	ofile					Server Load Balancin	gServers SCEP M	ble Certificate Pinning				
UPs - (Part 1)	Server List						Primary Server	_		Connection Information	n		
							Display Name (H	quired) (iscome)	Prec) Pv4	Primary Protocol	Primary Protocol Princ 🗸		
- Certificate Planing - E Certificate Matching	Hostname	Host Address	User Group	Backup Server List	SCEP 1	Hoble Setting	FQDN or IP Add	ess	User Group	ASA.gateway			
- Certificate Envolment B Hubble Policy	CREATER (Protec) 1.	. 192-198-1-1		- 276 012 -		_	192.168.1.1		1	Auth Method Du	ring 3/E Negotiation	EAP-AnyConnect. v	
Server List							Group UPL			3/E Identity (30	5 gateway only)		
	<u></u>	-	-	-									
	Note: it is highly a	recommended that at i	east one server be a	Sefined in a profile.	A	M							
					E	\$		Backup Servers					
								Host Address			Add		
											Marca 100		
											Playe op		
											Move Down		
											Delete		
									OK	Carcel			

Conferma profilo client protetto

#### Fare clic sul pulsante Esporta per esportare il profilo sul PC locale.

File View Tools Wizards Window Help				Type topic to search
🚳 Home 🦓 Configuration 🔯 Monitoring 🔲 Si	ave 🔇 Refresh 🔇 Back 🔘 Forward 🢡	Help		
Device List Bookmarks	Configuration > Remote Access VPN > Net	work (Client) Access > Secure Client Profile		
Bookmarks d P X				
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks". Go Delete	This panel is used to manage Secure Client Prol and download of client profiles between local m The profile Usage field is introduced with the Se	iles and perform group assignment for Secure Client version 2.5 or later achine and device. scure Mobility Solution. This field contains different profile usage in Secu	.You can select a profile to edit, change group or to delete. You can re Client version 3.0 and later.	select the 'Add' button to add a new profile. Pressing the Import or Expor
Remote Access VPN dP Q	🗣 Add 🧭 Edit 🔀 Change Group Policy 👔	Delete 🛃 Impert 🖶 Export 🔏 Validate		
2 Introduction	D. (1. 1)	De file linear	Com Balan	P. distanting
Potwork (Client) Access	Pronie Name	Prone Usage	Group Policy	Pronie Location
Secure Client Connection Promes	vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
Baroureas				
Biowy				
Cruint		Export Secure Client Profile	×	
Cliff Text and Messaver		Capare Second Caterio Frome	~	
Customized Installer Transforms		This papel is used to export Secure Client profile from d	levice to the local file system	
I or aized Installer Transforms				
- 16 Secure Clent Profile				
Secure Client Software				
Secure Client External Browser		Profile Name: vpn-ipsec-tunnel-grp_client_profile		
- Dynamic Access Policies				
Group Policies				
IPsec(I)(Ev1) Connection Profiles		Local Path: C:\Users\j.u L, Dr i - Cisco)	Desktop\vpn-ip: Browse Local	
IPsec(IEv2) Connection Profiles				
- Secure Mobility Solution				
Address Assignment				
Advanced				
Clientless SSL VPN Access		Envit Court	tinh	
AAA/Local Users		Export Cancel	nep	
Duchura (for Secure Frendal)				

Esporta profilo client protetto

#### Passaggio 13. Conferma dettagli profilo client protetto

Aprire Secure Client Profile tramite browser, verificare che il protocollo primario per l'host sia IPsec.

```
\u00ed 
\u00ed <
```

Dettagli di Secure Client Profile

#### Passaggio 14. Conferma impostazioni nella CLI di ASA

Confermare le impostazioni IPsec create da ASDM nella CLI dell'ASA.

```
// Defines a pool of addresses
ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0
// Defines radius server
aaa-server radius-grp protocol radius
aaa-server radius-grp (inside) host 1.x.x.191
timeout 5
// Define the transform sets that IKEv2 can use
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption aes
protocol esp integrity sha-256 sha-1
// Configures the crypto map to use the IKEv2 transform-sets
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map outside_map interface outside
// Defines trustpoint
crypto ca trustpoint vpn-ipsec-trustpoint
enrollment self
subject-name CN=ciscoasa
keypair ipsec-kp
crl configure
// Defines self-signed certificate
crypto ca certificate chain vpn-ipsec-trustpoint
certificate 6651a2a2
308204ed 308202d5 a0030201 02020466 51a2a230 0d06092a 864886f7 0d01010b
ac76f984 efd41d13 073d0be6 f923a9c6 7b
quit
// IKEv2 Policies
crypto ikev2 policy 1
encryption aes-256
integrity sha256
group 5
prf sha256
lifetime seconds 86400
crypto ikev2 policy 10
```

encryption aes-192 integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 20 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 crypto ikev2 policy 40 encryption aes integrity sha256 group 5 prf sha256 lifetime seconds 86400 // Enabling client-services on the outside interface crypto ikev2 enable outside client-services port 443 // Specifiies the certificate the ASA uses for IKEv2 crypto ikev2 remote-access trustpoint vpn-ipsec-trustpoint // Configures the ASA to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside enable anyconnect image disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 anyconnect profiles vpn-ipsec-tunnel-grp\_client\_profile disk0:/vpn-ipsec-tunnel-grp\_client\_profile.xml anyconnect enable tunnel-group-list enable // Configures the group-policy to allow IKEv2 connections and defines which Cisco Secure Client profile group-policy GroupPolicy\_vpn-ipsec-tunnel-grp internal group-policy GroupPolicy\_vpn-ipsec-tunnel-grp attributes wins-server none dns-server value 1.x.x.57 vpn-tunnel-protocol ikev2 default-domain value ad.rem-system.com webvpn anyconnect profiles value vpn-ipsec-tunnel-grp\_client\_profile type user // Ties the pool of addressess to the vpn connection tunnel-group vpn-ipsec-tunnel-grp type remote-access tunnel-group vpn-ipsec-tunnel-grp general-attributes address-pool vpn-ipsec-pool authentication-server-group radius-grp default-group-policy GroupPolicy\_vpn-ipsec-tunnel-grp tunnel-group vpn-ipsec-tunnel-grp webvpn-attributes group-alias vpn-ipsec-tunnel-grp enable

Passaggio 15. Aggiungi algoritmo di crittografia

Nella CLI di ASA, aggiungere il gruppo 19 ai criteri IKEv2.



Nota: per le connessioni IKEv2/IPsec, Cisco Secure Client non supporta più i gruppi Diffie-Hellman (DH) 2, 5, 14 e 24 alla versione 4.9.00086. Questa modifica può causare errori di connessione dovuti a mancata corrispondenza dell'algoritmo di crittografia.

ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# group 19
ciscoasa(config-ikev2-policy)#

Configurazione in Windows Server

È necessario aggiungere un utente di dominio per la connessione VPN. Passare a Utenti e computer di Active Directory, quindi fare clic su Utenti. Aggiungere vpnuser come utente di dominio.

Active Directory Users and Computers						
File Action View Help						
🗢 🔿 📶 🦨 🖬 🗙 🗊 🖻 🕞 📓 📷 🗏 👟	ia 🐨 🧕 🔽					
Active Directory Users and Computers winserver.ad.rem-s     Saved Quenes     Saved Que	Name Administrator Allowed RODC Passwork Cert Publishers Cioneable Domain Con ConfaultAccount Denied RODC Passwore Denied RODC Passwore DonsAdmins DonsAdmins DonsAdmins Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Domain Guests Domain Users Scherprise Admins Enterprise Read-only De	vpn user Properties     ?     >       Member Of     Dial-in     Environment     Sessions       Remote control     Remote Desktop Services Profile     COM+       General     Address     Account     Profile     Telephones     Organization       vpn user     vpn user				t for administering the computer/domain s group can have their passwords replicated to s group are permitted to publish certificates to s group that are domain controllers may be cl managed by the system. s group cannot have their passwords replicate tors Group o are permitted to perform dynamic updates o ninistrators of the domain trollers in the domain sts rs ninistrators of the enterprise s group can perform administrative actions on s group can modify group policy for the domain t
200 第二 第二 100 100 100 100 100 100 100 100 100 10	Vale volus y creator o Yaka User Ndes_user Protected Users RAS and IAS Servers Read-only Domain Con Johema Admins est user	Telephone number: Eggal: Web page:	K Cancel	<u>a</u> pply	Qther Other	s group can recess to the computer/domain s group can perform administrative actions on s group are afforded additional protections ag roup can access remote access properties of u s group are Read-Only Domain Controllers in t ninistrators of the schema

Aggiungi utente di dominio

## Aggiungere l'utente di dominio al membro di Domain Admins e Domain Users.

vpn user Properties			?	$\times$	vpn user Pro	operties				?	×
Remote control Member Of	Remote [	Desktop Services Profile Environment	CO	M+	Remote	control Address	Remote	Desktop Se Profile	ervices Profile Telephones	CO	M+ zation
General Address	Account	Profile Telephones	Organi	zation	Membe	r Of	Dial-in	Env	rironment	Sessio	ns
User logon name:					Member of	ł:					
vpnuser		@ad.rem-system.com		$\boldsymbol{\boldsymbol{\sim}}^{\prime}$	Name		Active Direct	tory Domain	n Services Folder		
User logon name (pre-	Windows 200	0):			Domain	Admins	ad.rem-syste	m.com/Use	ers		
AD\		vpnuser			Domain	Users	ad.rem-syster	m.com/Use	ers		
Unjock account Account gotions: User must chang User cannot cha Password never Store password Account expires	ge password a ange password expires using reversibl	t next logon j le encryption		< >	Add Primary gr	. <u>F</u> oup: D	Gemove omain Users	to condito	chance Primary		
Never     End of:	Monday ,	June 10, 2024	Ţ	]	<u>S</u> et Prir	nary Group	There is r you have applicatio	no need to Macintosh ms.	change Primary ( ) clients or POSID	group unle (-complian	t t
0	K C	Cancel Apply	Н	elp		0	K	Cancel	Apply	He	slp

Domain Admins e Domain Users

## Configurazione in ISE

#### Passaggio 1. Aggiungi dispositivo

Selezionare Amministrazione > Dispositivi di rete, quindi fare clic su Aggiungi per aggiungere un dispositivo ASAv.

Network Devices	Network Device Groups	Network Device Profil	es External RADIUS	Servers R/	ADIUS Server Sequences
Network Devices Default Device Device Security Settings	Network Dev Network Name Descriptio	Devices ASAv ASAv			
	IP Add	ress - * IP : 1.000	61 <sup>/</sup> 32 🐵		
	Device Pr	ofile 📅 Cisco	<u> </u>		
	Model Na	me	~		
	Software	Version	~		
	Network	Device Group			
	Location	All Locations	~	Set To Default	
	IPSEC	No	~	Set To Default	
	Device Ty	All Device Types	~	Set To Default	
	<b>~</b>	RADIUS Authentication	on Settings		
	R	ADIUS UDP Settings			
	p	rotocol RADIUS			
	S	hared Secret cisco12	3	Hide	

Aggiungi dispositivo

Passaggio 2. Aggiungi Active Directory

Selezionare Amministrazione > Origini identità esterne > Active Directory, fare clic sulla scheda Connessione, quindi aggiungere Active Directory ad ISE.

- Nome punto di join: AD\_Join\_Point
- Dominio Active Directory: ad.rem-system.com

≡	dentity Services I	e Administration / Identity Management
н	Bookmarks	titles Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
명	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	> Certificato Authenticat  Join Point Name AD_Join_Point 0
-0	Policy	Active Directory * Active Directory ad.rem-system.com
3.	Administration	AD_Join_Point

Aggiungi Active Directory

Passare alla scheda Gruppi, selezionare Seleziona gruppi dalla directory dall'elenco a discesa.

	dentity Services	Engine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
22	Dashboard	
1d o	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Cartificate Authorities
0	Policy	Select Groups From Directory     Select Groups From Directory     Select Groups From Directory
<b>a</b> o -	Administration	Add Group Control Assist ad.rem-system.com/S-1-5-32-579

Seleziona gruppi dalla directory

Selezionate Recupera gruppi (Retrieve Groups) dall'elenco a discesa. Checkad.remsystem.com/Users/Domain Computersandad.rem-system.com/Users/Domain Utenti e fare clic su OK.

=		Engine						×	A trees
	Restaurates	Identities Groups F	Sele	ect Directory Groups	S				
	Dookmarks		This dial	log is used to select groups from the Dir	irectory				
24	Dashboard	Active Directo	Dom	ain ad.rem-system.com					
18	Context Visibility	AD_Join_Poin	Na	ine S Iter Fil	SID . Iter	Type ALL Filter			
*	Operations	E LDAP		Retrieve Groups 9 Groups Retri	leved.				
0	Policy	RADIUS Token							
10	Administration	RSA SecuriD	0	Name	^	Group SID	Group Type		
-	Work Centers	SAML Id Provide	0	ad.rem-system.com/Users/DrsAdmins		5-1-5-21-4193742415-4133520026-20462399	DOMAIN LOCAL	^	
_		🖾 Social Login	0	ad rem-system com/Users/DisciplatePricky		5-1-5-21-4193742415-4133520020-20402390	CLOBAL		
•	Interactive Help			ad rem-system.com/Users/Domain Computer		5-1-5-21-4193742415-4133520028-20462399	GLOBAL		
			0	ad.rem+system.com/Users/Domain Controller	ra -	5+1+5+21+4193742415+4133520026+20462399	GLOBAL		
			0	ad.rem+system.com/Users/Domain Guests		5-1-5-21-4193742415-4133520026-20482399	GLOBAL		
				ad.rem-system.com/Users/Domain Users		5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ad.rem+system.com/Users/Enterprise Admins	9	5-1-5-21-4193742415-4133520026-20462399	UNIVERSAL	1	
			0	ad.rem-system.com/Users/Enterprise Key Ad	pning	5-1-5-21-4193742415-4133520026-20462399	UNIVERSAL		
			0	ad.rem+system.com/Users/Enterprise Read+o	only	5+1+5+21+4193742415+4133520026+20462399	UNIVERSAL		
				ad.rem+system.com/Users/Group Policy Crea	Mor	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			4					>	
								<b>C</b> 14	
_								UN	

Aggiungi computer e utenti del dominio

#### Passaggio 3. Aggiungi sequenza di origine identità

Passare ad Amministrazione > Sequenze origine identità, quindi aggiungere una sequenza origine

identità.

- Nome: Identity\_AD
- Elenco di ricerca autenticazione: AD\_Join\_Point

≡	dualse Identity Services I	ngine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
51	Dashboard	Identity Source Sequences List > Identity_AD
명	Context Visibility	Identity Source Sequence
*	Operations	
0	Policy	<ul> <li>Identity Source Sequence</li> <li>Name</li> </ul>
<b>a</b> 0	Administration	Identity_AD
đ	Work Centers	Leschpion
?	Interactive Help	Certificate Based Authentication
		Select Certificate Authentication Profile
		Authentication Search List A set of identity sources that will be accessed in sequence until first authentication succeeds
		Available Selected
		Internal Endpoints ^ AD_Join_Point ^
		Internal Users
		Guest Users

Aggiungi sequenze origine identità

#### Passaggio 4. Aggiungi set di criteri

Passare a Criterio > Set di criteri, fare clic su + per aggiungere un set di criteri.

- Nome set di criteri : VPN\_Test
- · Condizioni : Tipo di dispositivo dispositivo uguale a Tutti i tipi di dispositivo
- · Protocolli consentiti/sequenza server: accesso alla rete predefinito

≡	diada Identity Services Eng	gine	Policy / Policy Set	S	Leveluation Mode	Days Q (	0 Q	Ф I А
н	Bookmarks	Policy Sets			Reset P	olicyset Hitcoun	ts	Save
	Dashboard	🕒 Status Policy Set Name	Description	Conditions	Allowed Protocols / Server S	Sequence Hits	Actions	View
10	Context Visibility	Q Search						
*	Operations	A VIDA Text		DEVICE-Device Type EQUALS AI	Default Network Access	<i>e</i> + <i>m</i>	iêi.	
0	Policy	VPN_1051	l	Device Types			(Ç)	<u> </u>

Aggiungi set di criteri

Passaggio 5. Aggiungi criterio di autenticazione

Passare a Set di criteri e fare clic su VPN\_Test per aggiungere un criterio di autenticazione.

- Nome regola : VPN\_Authentication
- Condizioni : Indirizzo IP dispositivo di accesso alla rete UGUALE A 1.x.x.61
- Usa: Identity\_AD

VAuthentication Policy(2)				
+ Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
		Identity_AD		
VPN_Authentication	P Network Access-Device IP Address EQUALS 1.1711.61	> Options	10	\$ <u>}</u>

Aggiungi criterio di autenticazione

Passaggio 6. Aggiungi criterio di autorizzazione

Passare a Set di criteri e fare clic su VPN\_Test per aggiungere un criterio di autorizzazione.

- Nome regola : VPN\_Authorization
- Condizioni : Network\_Access\_Authentication\_Passed
- Risultati : PermitAccess

Authoriza	ation Policy(2)					
			Results			
+ Sta	atus Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q s	earch					
•	VPN_Authorization	Network_Access_Authentication_Passed	PermitAccess	Select from list	- 10	ŝ
giungi	criterio di autorizz	zazione				

# Verifica

Passaggio 1. Copia profilo client sicuro in Win10 PC1

Copiare il profilo client sicuro nella directory C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.



#### Passaggio 2. Avvia connessione VPN

Sull'endpoint, eseguire Cisco Secure Client e immettere il nome utente e la password, quindi verificare che Cisco Secure Client si connetta correttamente.

♦ Cisco Secure Client — 🗌 🗠 🗙	Scisco Secure Client   ciscoasa (IPsec) IPv4 ×	O Cisco Secure Client
AnyConnect VPI: Please enter your username and password. ciscoasa (IPsec) IPv4 V Connect	Please enter your username and password. Group: vpn-psec-tunnel-grp  Username: vpnuser	AnyConnect VPIt: Connected to discoasa (IPsec) IPv4. discoasa (IPsec) IPv4 V Disconnect
	Password: ******	00:00:05 IPv4
	OK Cancel	

Connessione riuscita

#### Passaggio 3. Conferma syslog su ASA

Nel syslog, verificare che la connessione IKEv2 sia riuscita.

#### <#root>

```
May 28 20xx 08:xx:20: %ASA-5-750006: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
New Connection Established
```

```
May 28 20xx 08:xx:20: %ASA-6-751026: Local:192.168.1.1:4500 Remote:192.168.1.11:50982 Username:vpnuser
```

#### Passaggio 4. Conferma sessione IPsec su ASA

eseguire show vpn-sessiondb detail anyconnect il comando per confermare la sessione IKEv2/IPsec sull'appliance ASA.

#### <#root>

ciscoasa#

show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : vpnuser Index : 23 Assigned IP : 172.16.1.20 Public IP : 192.168.1.11 Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent License : AnyConnect Premium Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES256 AnyConnect-Parent: (1)none Hashing : IKEv2: (1)SHA256 IPsecOverNatT: (1)SHA256 AnyConnect-Parent: (1)none Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy\_vpn-ipsec-tunnel-grp Tunnel Group : vpn-ipsec-tunnel-grp Login Time : 08:13:20 UTC Tue May 28 2024 Duration : 0h:10m:10s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 01aa003d0001700066559220 Security Grp : none IKEv2 Tunnels: 1 IPsecOverNatT Tunnels: 1 AnyConnect-Parent Tunnels: 1 AnyConnect-Parent: Tunnel ID : 23.1 Public IP : 192.168.1.11 Encryption : none Hashing : none Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 19 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : 5.1.3.62 IKEv2: Tunnel ID : 23.2 UDP Src Port : 50982 UDP Dst Port : 4500 Rem Auth Mode: userPassword Loc Auth Mode: rsaCertificate Encryption : AES256 Hashing : SHA256 Rekey Int (T): 86400 Seconds Rekey Left(T): 85790 Seconds PRF : SHA256 D/H Group : 19 Filter Name : Client OS : Windows Client Type : AnyConnect IPsecOverNatT: Tunnel ID : 23.3 Local Addr : 0.0.0.0/0.0.0.0/0/0 Remote Addr : 172.16.1.20/255.255.255.255/0/0 Encryption : AES256 Hashing : SHA256 Encapsulation: Tunnel Rekey Int (T): 28800 Seconds Rekey Left(T): 28190 Seconds Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Bytes Tx : 840 Bytes Rx : 52408 Pkts Tx : 21 Pkts Rx : 307

Passaggio 5. Conferma registro dinamico Radius

Selezionare Operations > RADIUS > Live Login nell'interfaccia utente di ISE, quindi confermare il log attivo per l'autenticazione VPN.

≡	the intervices in the intervic	ngine Operations / RADIUS										<b>A</b> ••	aluation Mode 💭 Days	۵ ۵	۲	<b>Q</b>   2	a
н	Bookmarks	Live Logs Live Sessions															
	Dashboard																
N	Context Visibility	Misconfigured Supplicants			Mis	configured Ne	twork Devic	es 📀	RADIUS Drops		<b>Client Stopped Re</b>	sponding 💿			Repeat C	ounter 📀	
*	Operations	0				(	)		0		0					C	
Ð	Policy											Refresh	Show		Michin		
2.	Administration											Never	V Latest 20 M	cords 🗸	Last 3 ho	urs v	
ส์เ	Work Centers	C 10 Reset Repeat Counts	d) Export To N	×											Filter 🗸	۰	
		Time	Status	Details	Repeat	Endpoint	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Por	t Ide	ntity Grou	
	Interactive Help	×	~			Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	V Network Devic	Device Port	Ide	ntity Group	
		May 28, 2024 05:13:42	•	0	0	00.50.5	vpruser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess						
		May 28, 2024 05:13:42		0		00:50:5	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Wor	kstation	

Registro Radius Live

Fare clic su Stato per confermare	i dettagli del registro attivo.
-----------------------------------	---------------------------------

Cisco ISE				
Overview		Steps		
		Step ID	Description	Latency (ms)
Event	5200 Authentication succeeded	11001	Received RADIUS Access-Request	
Username	vpnuser	11017	RADIUS created a new session	1
Endpoint Id	00:50:56:98:77:A4 ⊕	15049	Evaluating Policy Group	36
Endpoint Profile	Windows10-Workstation	15008	Evaluating Service Selection Policy	1
Endpoint Prome	WIRKOWS I C-WORKSLOUDI	15048	Queried PIP - DEVICE.Device Type	6
Authentication Policy	VPN_Test >> VPN_Authentication	15041	Evaluating Identity Policy	20
Authorization Policy	VPN_Test >> VPN_Authorization	15048	Queried PIP - Network Access.Device IP Address	2
Authorization Result	PermitAccess	22072	Selected identity source sequence - Identity_AD	6
		15013	Selected Identity Source - AD_Join_Point	1
		24430	Authenticating user against Active Directory - AD_Join_Point	4
Authentication Details		24325	Resolving identity - vpnuser	38
Source Timestamp	2024-05-28 17:13:42.897	24313	Search for matching accounts at join point - ad.rem- system.com	0
Received Timestamp	2024-05-28 17:13:42.897	24319	Single matching account found in forest - ad.rem- system.com	0
Policy Server	ise33-01	24323	Identity resolution detected single matching account	0
Event	5200 Authentication succeeded	24343	RPC Logon request succeeded - vpnuser@ad.rem- system.com	23
Username	vpnuser	24402	User authentication against Active Directory succeeded - AD_Join_Point	3
Endpoint id	00:50:50:98:77:44	22037	Authentication Passed	1
Calling Station Id	192.168.1.11	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
Endpoint Profile	windows i 0-workstation	15036	Evaluating Authorization Policy	1
Authentication Identity Store	AD_Join_Point	24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
0.010		24211	Found Endpoint in Internal Endpoints IDStore	9
Identity Group	Workstation	15048	Queried PIP - Network Access.AuthenticationStatus	2
Audit Session Id	01aa003d0001700066559220	15016	Selected Authorization Profile - PermitAccess	7
Authentication Method	PAP_ASCII	22081	Max sessions policy passed	6
Authoritization Droto	DAD ACON	22080	New accounting session created in Session cache	0
Authentication Protocol	PAF_AGUN	11002	Returned RADIUS Access-Accept	2
Network Device	ASAv			

Dettagli del registro attivo

#### Risoluzione dei problemi

La mancata corrispondenza degli algoritmi di crittografia può causare errori di connessione. Questo è un esempio di quando si verifica un problema di mancata corrispondenza degli algoritmi. Per risolvere il problema, eseguire il passo 15 della sezione Configurazione in ASDM.

Passaggio 1. Avvia connessione VPN

Sull'endpoint, eseguire Cisco Secure Client e confermare che la connessione non è riuscita a causa di una mancata corrispondenza degli

The cryptographic algorithms required by the secure gateway do not match those supported by AnyConnect.Please contact your network administrator.

S Cisco Secure Client	-		×	Cisco Secure Client	×
AnyConnect VPN: Ready to connect.	~ [	Connec	t	The cryptographic algorithms required by the secure gateway do not match those supported by Cisco Secure Client. Please contact your network administrator.	
				ОК	

Connessione non riuscita

Passaggio 2. Conferma syslog nella CLI

Nel syslog, confermare che la negoziazione IKEv2 non è riuscita.

#### <#root>

May 28 20xx 08:xx:29: %ASA-5-750002: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Received a IKE\_INIT\_SA requ May 28 20xx 08:xx:29: %ASA-4-750003: Local:192.168.1.1:500 Remote:192.168.1.11:57711 Username:Unknown IKEv2 Negotiation aborted due to ERI

Failed to find a matching policy

Riferimento

AnyConnect over IKEv2 su ASA con autenticazione AAA e certificato

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).