# Konfigurieren von Secure Client IKEv2/ASA im ASDM mit AAA & Zertifizierungsauthentifizierung

## Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konfigurationen Konfiguration in ASDM Schritt 1: Offene VPN-Assistenten Schritt 2: Verbindungsprofilidentifizierung Schritt 3: VPN-Protokolle Schritt 4: Client-Images Schritt 5: Authentifizierungsmethoden Schritt 6: SAML-Konfiguration Schritt 7. Client-Adressenzuweisung Schritt 8: Server für die Netzwerknamensauflösung Schritt 9. NAT-Ausnahme Schritt 10. Sichere Client-Bereitstellung Schritt 11. Einstellungen speichern Schritt 12: Sicheres Clientprofil bestätigen und exportieren Schritt 13: Details des sicheren Clientprofils bestätigen Schritt 14: Bestätigen der Einstellungen in der ASA CLI Schritt 15: Verschlüsselungsalgorithmus hinzufügen Konfiguration in Windows Server Konfiguration in der ISE Schritt 1: Gerät hinzufügen Schritt 2: Active Directory hinzufügen Schritt 3: Identitätsguelltext hinzufügen Schritt 4: Policy Set hinzufügen Schritt 5: Authentifizierungsrichtlinie hinzufügen Schritt 6: Autorisierungsrichtlinie hinzufügen Überprüfung Schritt 1: Kopieren des sicheren Clientprofils auf Win10 PC1 Schritt 2: VPN-Verbindung initiieren Schritt 3: Syslog auf ASA bestätigen Schritt 4: IPsec-Sitzung auf ASA bestätigen Schritt 5: RADIUS-Live-Protokoll bestätigen Fehlerbehebung Schritt 1: VPN-Verbindung initiieren Schritt 2: Syslog in CLI bestätigen

#### Referenz

## Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration eines sicheren Clients über IKEv2 auf ASA mit ASDM mit AAA und Zertifikatsauthentifizierung beschrieben.

## Voraussetzungen

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Identity Services Engine (ISE)
- Konfiguration der Cisco Adaptive Security Virtual Appliance (ASAv)
- Konfiguration des Cisco Adaptive Security Device Manager (ASDM)
- VPN-Authentifizierungsablauf

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Identity Services Engine Virtual 3.3 Patch 1
- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.

Der unter Windows Server 2016 konfigurierte Domänenname ist ad.rem-system.com. Dies wird in diesem Dokument als Beispiel verwendet.



Netzwerkdiagramm

## Konfigurationen

## Konfiguration in ASDM

### Schritt 1: Offene VPN-Assistenten

Navigieren Sie zu Wizards > VPN Wizards, und klicken Sie auf Secure Client VPN Wizard.



## Klicken Sie auf Next (Weiter).

Secure Client VPN Conne	ction Setup Wizard	$\times$
Secure Client VPN Connect VPN Wizard	tion Setup Wizard Introduction Use this wizard to configure the ASA to accept VPN connections from the Secure VPN Client. The connections will be protecte 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 Cool Cool Cool Cool Cool Cool Cool Cool	× d
	< Back Next > 現初 Help	

Klicken Sie auf Weiter

Schritt 2: Verbindungsprofilidentifizierung

Eingabeinformationen für das Verbindungsprofil. Name des Verbindungsprofils: vpn-ipsec-tunnel-grp VPN-Zugriffsschnittstelle: außen

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Connection Profile Identification	
<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 Connection Profile Name and the Interface the remote access users will access for VPN connections. Connection Profile Name: vpn-ipsec-tunnel-grp VPN Access Interface: outside v	
	< Back Next > Ikin Help	

Verbindungsprofilidentifizierung

#### Schritt 3: VPN-Protokolle

Wählen Sie IPsec aus, und klicken Sie auf Hinzufügen, um ein neues selbstsigniertes Zertifikat hinzuzufügen.

Secure Client VPN Conne	ction Setup Wizard X		The Manage Identity Certificates
Steps	VPN Protocols		Issued To Issued By Expiry Date Associated Trustpoints Usage Public Key Type Add
1. Introduction	Secure Clent can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to a most		Show Details
<ol> <li>Connection Profile Identification</li> </ol>			Delete
3. VPN Protocols	Diss.		Export
5. Authentication Methods			Instal
6. SAML Configuration	Device Certificate Device certificate identifies the ASA to the remote access clants. Certain Secure		
7. Client Address Assignme	Client Features (Always-On, IPsec/II/Ev2) require that valid device certificate be	1	Kechioa
8. Network Name Resolutio	araidate on one ASA.	ł.	
9. NAT Exempt	Device Certificate: None V Manage		
10. Secure Client Deployme			
11. Summary			
		1	
			Eind: 💿 💿 🗋 Match Case
			Certificate Expiration Alerts
		-	Send the first alert before : 60 (days) Set Default
	< gack Next > R(I) Help		Repeat Alert Interval : 7 (days)
		1	Weak Crypto Configurations
			Permit Weak key sizes and Hash Algorithms
			Duble CA Encolmant
		1	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
			Using a previously saved certificate signing request, enrol with Entrust,
			ASDM Identity Certificate Wizard
			The Cisco ASDM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.
			Launch ASDM Identity Certificate Wizard
			OK Cancel Help

Eingabeinformationen für selbstsigniertes Zertifikat.

Vertrauenspunktname: vpn-ipsec-trustpoint

### Schlüsselpaar: ipsec-kp

Add Identity Certificate X	🖸 Add Key Pair X			
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: ORSA OECDSA EDDSA			
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	O Enter new key pair name: lpsec-kp			
• Add a new identity certificate:	Size: 4096 ~			
Key Pair: Ipsec-lip 🧹 Show New	Usage: O General purpose O Special			
Certificate Subject DN: CN=ciscoasa Select				
Generate self-signed certificate     Act as local certificate authority and issue dynamic certificates to TLS-Proxy	Generate Now Cancel Help			
Advanced				
Enable CA flag in basic constraints extension				
Add Certificate Cancel Help				

Detail des selbstsignierten Zertifikats

Bestätigen Sie die Einstellungen der VPN-Protokolle, und klicken Sie auf die Schaltfläche Weiter.

Secure Client VPN Conne	ction Setup Wizard	×
Steps         1. Introduction         2. Connection Profile Identification         3. VPN 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         Image: SSL         Device Certificate         Device Certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/ID:Ev2) require that valid device certificate be available on the ASA.         Device Certificate : vpn-ipsec-trustpoint:unstructuredNam	20
	< Back Next > Rifl Help	

Einstellungen des VPN-Protokolls bestätigen

#### Schritt 4: Client-Images

Klicken Sie auf die Schaltfläche Hinzufügen, um ein sicheres Client-Image hinzuzufügen, und klicken Sie auf die Schaltfläche Weiter.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Client Images	
1. Introduction	ASA can automatically upload the latest Secure Client package to	the client device when it accesses the enterprise network.
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a br You can also minimize connection setup time by moving the image	owser to an image. used by the most commonly encountered operation system to
3. VPN Protocols	the top of the list.	
4. Client Images	A 44 2 and a C a 44	
5. Authentication Methods	* Add 🖉 Replace 🚺 Delete 🖵 🔶	
6. SAML Configuration	Image	Regular expression to match user-agent
7. Client Address Assignme	disk0:/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg	
8. Network Name Resolutio Servers		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	You can download Secure Client packages from <u>Cisco</u> by searchin	ig 'Secure Mobility Client' or <u>click here</u> ,
	< gack Next >	R iff Help

**Client-Images** 

Schritt 5: Authentifizierungsmethoden

Klicken Sie auf die Schaltfläche Neu, um einen neuen AAA-Server hinzuzufügen, und klicken Sie auf die Schaltfläche Weiter.

Server-Gruppenname: radius-grp

Authentifizierungsprotokoll: RADIUS

Server-IP-Adresse: 1.x.x.191

Schnittstelle : innen

Secure Client VPN Core	ection Setup Witard	× 🔯 New Au	thentication Server Gr	oup	×	Secure Client VPN Conn	ection Setup Wizard	×
Stee 1. Broketion 2. Convector hritike Identification 3. With Inducid 4. Get Langes 5. StAL Configuration 7. Get Address Assignment 5. StAL Configuration 10. Status Configuration 9. Nat Longel 10. Status Conf. Deployment 11. Status Que Deployment 12. Status Que Deployment 13. Status Que Deployment 14. Status Que Deployment 15.	Addretication: Mithods Mithod & Mithod	Create To add Configu Server Authen Server Interfa	Server Group Name:     2005       Authentication Protocol:     RADRUS       Server Group Name:     1. bit Address:       Authentication Protocol:     RADRUS       Server Group Name:     1.11:1:1:1:1:1:1:1:1:1:1:1:1:1:1:1:1:1:		Authentication Helholds The sample is use used by the factors of the authentication server. Tou can do the MH-M-M-Mattin to end a sine server groups. AAA Server Group Teaching Teaching Teaching AAA Server Group Teaching Teaching AAA Server Group Teaching Teaching Server Same of 20 Address Detailers Teaching Teaching Teaching Teaching Servers			
	<\$ak (bet> 0.1	Heb Server	Secret Key:					
		Confirm	n Server Secret Key:				<bok bet=""></bok>	
			OK	Cancel Help				

Authentifizierungsmethoden

#### Schritt 6: SAML-Konfiguration

#### Klicken Sie auf die Schaltfläche Weiter.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	SAML Configuration	
Introduction     Connection Profile     Identification     VPN Protocols     Client Images     Authentication Methods <b>6. SAML Configuration</b> Client Address Assignme     Network Name Resolutio     Servers	This step allows you to configure a SAML and the authenticaion method.  Authentication  Method: AAA   AAA Server Group: radus-grp   Use LOCAL if Server Group fails  SAML Identity Provider  SAML Server : None   Manage	
9. NAT Exempt 10. Secure Client Deployme 11. Summary		
	< Back Next > 同時 Next > 目時 Next > 同時 Next > 同	db

SAML-Konfiguration

Schritt 7. Client-Adressenzuweisung

Klicken Sie auf die Schaltfläche Neu, um einen neuen IPv4-Pool hinzuzufügen, und klicken Sie auf die Schaltfläche Weiter.

Name: vpn-ipsec-pool

Start-IP-Adresse: 172.16.1.20

End-IP-Adresse: 172.16.1.30

### Subnetzmaske: 255.255.255.0

Secure Client VPN Conne	ction Setup Wizard			×	Secure Client VPN Conne	ction Setup Wizard		×
Steps   I. Introduction  C. Correction Profile Identification  WHI Protocols  A. Clerk Timages  S. Authentication Methods  6. SAML Configuration  7. Client Address Assignment  8. Network Name Resolutio Servers  9. NAT Exempt  10. Secure Clerk Deployme  11. Summary	Clerk Address Assignment This step allows you to create a new address pool or s be assigned addresses from the pools when they conn BV-6 address Pool is only supported for SSL connection Address Pool - Select New Details of the selected address pool	elect an existing address ect. h Add IPv4 Pool Name: Starting IP Address Ending IP Address: Subnet Masil: OK	vpn-ipsec-pool 172.16.1.20 172.16.1.30 255.255.55.0 Cancel	The Secure Clents will	Steps	Clerk Address Assignm This step allows you to be assigned addresses IPv6 address pool is ori IPv6 address Pool Address Pool yon-pop Details of the select Starting IP Address: Ending IP Address: Submet Mask:	ent create a new address pool or select an existing address pool for IPv4 and IPv6. The Se from the pools when they connect. w supported for SSL connection. ed address pool	ure Clerts will
	< Back Next >			Ikil) Help		< gack Next >	- R/A	Help

Client-Adresse zuweisen

#### Schritt 8: Server für die Netzwerknamensauflösung

Geben Sie Informationen für DNS und Domäne ein, und klicken Sie auf die Schaltfläche Weiter.

#### DNS-Server: 1.x.x.57

#### Domänenname: ad.rem-system.com

$\sim$

Server für die Netzwerknamensauflösung

#### Schritt 9. NAT-Ausnahme

Klicken Sie auf die Schaltfläche Weiter.

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     Secure Client Deployme     In. Summary	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.	
	< Back Next >	Help

NAT-Ausnahme

## Schritt 10. Sichere Client-Bereitstellung

Wählen Sie Web-Start zulassen aus, und klicken Sie auf die Schaltfläche Weiter.

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:
2. Connection Profile Identification	<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	
5. Authentication Methods	Z Allow Web Launch
6. SAML Configuration	Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will
7. Client Address Assignme	NUT WORK I'R IS CARDED 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 > It in Help

Sichere Client-Bereitstellung

### Schritt 11. Einstellungen speichern

Klicken Sie auf Fertig stellen, und speichern Sie die Einstellungen.

VPN Wizer         Summary         Here is the summary of the configuration.         Name       Value         Summary         Name/Alas of the Connection Profile       Value         Summary       Name/Alas of the Connection Profile       Value         Summary       Name/Alas of the Connection Profile       Value         Summary       Name/Alas of the Connection Profile       Value         Summary       Name/Alas of the Connection Profile       Value         Device Digital Certificate       Value       (0) as a server radue-gp protocol radue         Secure Clerk       Device Digital Certificate       Value-gp         Secure Clerk       Address Poil for the Clerk       (1) as a server radue-gp protocol radue         Secure Clerk       Address Poil for the Clerk       (2) as a server radue-gp protocol radue         ONS       Device Digital Certificate       Value-gp         Secure Clerk       1 package       (2) as a server radue-gp protocol radue         ONS       Device Digital Certificate       (2) as a server radue-gp protocol radue         ONS       Device Digital Certificate       (2) as a server radue-gp protocol radue         ONS       Device Digital Certificate       (2) as a server radue-gp protocol radue         ONS       Device Digi	Secure Client VPN Conne	ction Setup Wizard		K 🖾 Warning 🛛 🕹
Name       Value         Summary       Name/Alas of the Connection Profile       yn-pisec-tunnel-gr         WM Access Interface       outside         Device Digital Cettificate       yn-pisec-tunnel-gr         Distance       Distance         Address Pool for the Clent       127.16.1.30         Distance       Distance         Distance       Distance         Distance       Distance	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
aroue-ookv GrouePokv von-iosec-turnel-aro attributes		Name Summary Name/Alas of the Connection Profile VPN Access Interf are Device Digital Certificate VPN Protocols Enabled Secure Clerk Images Authentication Server Group SAPL Address Pool for the Clent DNS Network Address Translation	Value vpn-ipsec-tunnel-grp outside vpn-ipsec-trustpoint:unstructuredName= <iscoasa, cn<br="">Pisec only 1 package radius-grp Server: Server: Server: Domain Name: The protected traffic can be subjected to network address translation</iscoasa,>	[Ok] p local pool ym-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.255.35         [Ok] j webypn         [Ok] webypn         [Ok] webypn         [Ok] avconnett profile signification of the profile disk0:/ym-ipsec-tunnel-grp_clent_profile.xml         [Ok] avconnett profiles vpn-ipsec-tunnel-grp_clent_profile disk0:/ym-ipsec-tunnel-grp_clent_profile.xml         [Ok] avconnett profiles vpn-ipsec-tunnel-grp_clent_profile.xml         [Ok] avs-server radux-grp (inside) host 1.1.1

Einstellungen speichern

#### Schritt 12: Sicheres Clientprofil bestätigen und exportieren

Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile, und klicken Sie auf die Schaltfläche Edit.

File View Tools Wigards Window Help	efresh 🕟 Back 🔘 Forward 🦻 Help		Type topic to search Go	cisco
Device List Boolmarks Config	iration > Remote Access VPN > Network (Client) Access > Secure Client Profile			
Bodimarks ∂ 0 0 × To bodimark apage, right-click on a node in the navigation tree and select 7.46d to boolenarks".	anel is used to manage Secure Clerct Profiles and perform group assignment for Secure Clerct version 2.5 or d and download of clerct profiles between local machine and device. order Usage India is stranduced with this Secure Holdity Solution. The field contains different profile usage in Add Clerct Local Change Group Policy (1) Delete (1) Import (1) Export (2) Validate	r låter. You can select a profile to edit, change group or to delete. You can select Secure Clent version 3.0 and later.	the 'Add' button to add a new profile. Pressing the Import or Export by	Æton is for
Info Douccon     I	le Name Profile Usage seecturnel-gp_tlent_srofile AnyConnect VNN Profile	Group Policy GroupPolicy_upn-tpsec-tunnel-grp	Profile Location  dsk0:/vpn-bsecturnel-grp_dient_profile.uml	

Sicheres Clientprofil bearbeiten

Bestätigen Sie die Profildetails.

- Anzeigename (erforderlich): Cisco ASA (IPsec) IPv4
- FQDN oder IP-Adresse: 192.168.1.1
- Primäres Protokoll: IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grp	client_profile					Server List Entry					×	
Profile: vpn-ipsec-tunne	l-grp_client_pro	ofile					Server Load Balancing	Servers SCIP M	able Certificate Pinning				
Unix Other ences (Part 1) Preferences (Part 2) Other Earliep Cenvers	Server List						Primary Server Display Name (required) Occoace (Piver) Pive(			Connection Information Primary Protocol	Connection Information Primary Protocol Presc		
Centrate Harring Centrate Harring Centrate Harring Centrate Toulanet Light Harring Server Liet	Hothame	Host Address 192 Std. 1.1	User Group	Backup Server List	SCDP P	d	PQEN or IP Addr	Backup Servers Host Address	Uter Group	Auth Hethod Ly	Add Add Move Up Move Down Delete	EAP-AnyConnett ->	
									OK.	Canod			

Sicheres Clientprofil bestätigen

Klicken Sie auf die Schaltfläche Exportieren, um das Profil auf den lokalen PC zu exportieren.

File View Tools Wizards Window Help				Type topic to search
🚳 Home 🦓 Configuration 🔯 Monitoring 🔒 Sav	re 💽 Refresh 🔇 Back 🔘 Forward 🢡	Help		
Device List Bookmarks	Configuration > Remote Access VPN > Netw	ork (Client) Access > Secure Client Profile		
Bookmarks d <sup>a</sup> Q ×				
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".	This panel is used to manage Secure Client Profil and download of client profiles between local ma The profile Usage field is introduced with the Sec	es and perform group assignment for Secure Client version 2.5 or later. chine and device. ure Mobility Solution. This field contains different profile usage in Secure	You can select a profile to edit, change group or to delete. You can selec e Client version 3.0 and later.	ct the 'Add' button to add a new profile. Pressing the Import or Expo
Remote Access VPN 🗗 🖗	🗣 Add 🧭 Edit 🞇 Change Group Policy 📋	Delete 🛃 Impert 🔹 Export 👩 Validate		
-? Introduction	Droffie Name	Profile Lisane	Group Ballou	Profile Location
Secure Cleant Connection Profiler	provide manife	In Control 1741 Profile	Council and a second se	del éstere base barrel en electerentie en
Secure Clent Customization   oralization	vpr-psec-curine-grp_clienc_prone	AnyConnect why Prone	GroupPoicy_vpn-psec-cunnel-grp	asiv:/vpn-psec-curnel-grp_cienc_prone.xm
Resources				
Binary				
- Script		Export Secure Client Profile	×	
GLII Text and Messages				
Customized Installer Transforms		This papel is used to export Secure Client profile from de	wice to the local file system	
Localized Installer Transforms				
Serve Clerk Public				
Service Clerk Software				
Secure Clent External Browser		Profile Name: vpn-ipsec-tunnel-grp_client_profile		
De Dunamir Arraes Dokrias				
Group Policies				
Different (1) Evit) Connection Profiler		Local Path: C:\Users\j.u.L."; DrDr /u - Cisco\D	esktop\vpn-ip: Browse Local	
Direc(DEv2) Connection Profiles				
Carrie Mahibu Calitico				
C Address Assistment				
Address Assignment				
Charles CO 104 Anna				
Chertoess 55 min Access		Export Cancel	Help	
Avoilocal Users     Avoilocal Users     Avoilocal Users				

Sicheres Clientprofil exportieren

Schritt 13: Details des sicheren Clientprofils bestätigen

Öffnen Sie Secure Client Profile by browser, und stellen Sie sicher, dass das primäre Protokoll für den Host IPsec ist.

```
\u00ed 
\u00ed <
```

Details zum sicheren Clientprofil

#### Schritt 14: Bestätigen der Einstellungen in der ASA CLI

Bestätigen Sie die von ASDM in der ASA CLI erstellten IPsec-Einstellungen.

```
// 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

Schritt 15: Verschlüsselungsalgorithmus hinzufügen

Fügen Sie in der ASA CLI Gruppe 19 zur IKEv2-Richtlinie hinzu.



Hinweis: Für IKEv2/IPsec-Verbindungen unterstützt der Cisco Secure Client seit Version 4.9.00086 nicht mehr die Diffie-Hellman (DH)-Gruppen 2, 5, 14 und 24. Diese Änderung kann aufgrund von nicht übereinstimmenden kryptografischen Algorithmen zu Verbindungsfehlern führen.

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

Konfiguration in Windows Server

Sie müssen einen Domänenbenutzer für die VPN-Verbindung hinzufügen. Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Benutzer. Fügen Sie vpnuser als Domänenbenutzer hinzu.

Active Directory Users and Computers						
File Action View Help						
💠 🔿 📶 🦨 🛍 🗙 🖾 🙆 📴 🖏	🐮 🖹 🍸 🗾 🐍					
Active Directory Users and Computers winserver.ad.rem-s Saved Queries Ad.rem-system.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Users	Name Administrator Allowed RODC Passwor Cert Publishers Cloneable Domain Con Coneable Domain Con DefaultAccount Denied RODC Passwore	vpn user Properties Member Of Remote control General Address	Dial-in Remote Deskt Account Pro	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		
	DonsAdmins DonsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Enterprise Admins Enterprise Read-only D Group Policy Creator O Group Poli	Eint name: Last name: Digolay name: Qescription: Offige:	vpn  user vpn user	jntals:		etors Group o are permitted to perform dynamic updates o ninistrators of the domain s and servers joined to the domain trollers in the domain sts rs ninistrators of the enterprise s group can perform administrative actions on
		Ţelephone number: E @al: Web page:			Qther Other	s group are Read-Only Domain Controllers in t s group can modify group policy for the domain t for guest access 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
	🖔 test user 💍 vpn user		OK Cano	el <u>é</u> pply	Help	

Domänenbenutzer hinzufügen

Fügen Sie den Domänenbenutzer einem Mitglied von Domänenadministratoren und Domänenbenutzern hinzu.

vpn user Properties		?	×	vpn user Properties				?	×
Remote control	Remote Desktop Services Profile	CC	M+	Remote control	Remote I	Desktop Se	rvices Profile	CON	4+
Member Of	Dial-in Environment	Sessi	ons	General Address	Account	Profile	Telephones	Organiz	ation
General Address	Account Profile Telephones	Organ	ization	Member Of	Dial-in	Envi	ronment	Session	IS
User logon name: Member of:									
vpnuser	@ad.rem-system.com		$\sim$	Name	Active Direct	ory Domain	Services Folder		
User logon name (pre-	Windows 2000):			Domain Admins	ad.rem-syster	m.com/Use	rs		
AD\	vpnuser			Domain Users	ad.rem-system	m.com/Use	rs		
									55
Never     End of:	Monday , June 10, 2024		]	Set minaly Group	you have applicatio	Macintosh ns.	clients or POSIX	compliant	
OF	Cancel Apply	H	lelp	0	K (	Cancel	Apply	He	lp 🛛

Domänenadministratoren und Domänenbenutzer

## Konfiguration in der ISE

### Schritt 1: Gerät hinzufügen

Navigieren Sie zu Administration > Network Devices, und klicken Sie auf Add (Hinzufügen), um ein ASAv-Gerät hinzuzufügen.

Network Devices	Network Dev	ice Groups	Network Device Pro	files External R	ADIUS Serve	rs RADIUS Se	erver Sequences
Network Devices Default Device Device Security Settings		Network Devices Network De Name Description	List > ASAv vices ASAv				
					_		
		IP Address	<ul> <li>* IP : 1.00</li> </ul>	0.1.61 <sup>/</sup> 32	۲		
		Device Profil	e 🏥 Cisco	~	0		
		Model Name			-		
		Software Ver	sion		~		
		Network Dev	ice Group				
		Location	All Locations		Y Set T	o Default	
		IPSEC	No		Y Set T	o Default	
		Device Type	All Device Types		Y Set T	o Default	
		🔽 🗸 R	ADIUS Authentica	tion Settings			
		Proto	col RADIU	s			
		Shar	ed Secret cisco	123		Hide	

Gerät hinzufügen

Schritt 2: Active Directory hinzufügen

Navigieren Sie zu Administration > External Identity Sources > Active Directory, klicken Sie aufRegisterkarte Connection, und fügen Sie Active Directory zur ISE hinzu.

- Verknüpfungspunkt-Name: AD\_Join\_Point
- · Active Directory-Domäne: ad.rem-system.com

≡	dentity Services	Engine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Settings
11	Dashboard	
15	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat
-0	Policy	Active Directory ad.rem-system.com
20	Administration	AD_Join_Point

Active Directory hinzufügen

Navigieren Sie zur Registerkarte Gruppen, und wählen SieGruppe auswählen aus Verzeichnis aus Dropdown-Liste.

dentity Services E	Engine Administration / identity Management
Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
Dashboard	
Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
Operations	Cast Control C
Policy	Select Groups From Directory     Select Groups From Directory     StD
Administration	Add Group Control Assist ad.rem-system.com/S-1-5-32-579
	elede identity Services Bookmarks Dashboard Context Visibility Operations Policy Administration

Gruppe auswählen aus Verzeichnis

Klicken Sie auf Gruppen aus der Dropdown-Liste abrufen. Checkad.remsystem.com/Users/Domain Computersandad.rem-system.com/Users/Domain Benutzer und klicken auf OK.

=	dentity Services	Engine						×	A tono
		Identities Orever F	Sel	ect Directory Groups	S				
	BOOKMARKS		This di	ialog is used to select groups from the D	irectory.				
-	Dashboard	Active Directo	Do	main ad.rem-system.com					
18	Context Visibility	AD_Join_Poin	Ň	iame	SID . Iter	Type ALL Filter			
×	Operations	C LDAP		Retrieve Groups	ieved.				
0	Policy	C RADIUS Token							
10	Administration	C RSA SecuriD	0	Name	~ Gro	sup SID	Group Type		
-	Work Centers	SAML Id Provide	-	ad rem-system com/Users/DeallocateProve	5+1	-5-21-4193742415-4133520026-20462399	CLOBAL	1	
_		Social Login	0	ad.rem-system.com/Users/Domain Admins	5-1	+5+21+4193742415+4133520026+20462399	GLOBAL		
•	Interactive Help			ad.rem-system.com/Users/Domain Compute	rs 5-1	-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ad.rem+system.com/Users/Domain Controlle	rs 5+1	+5+21+4193742415+4133520026+20462399	GLOBAL		
			0	ad.rem-system.com/Users/Domain Guests	S+1	-5-21-4193742415-4133520026-20462399	GLOBAL		
			•	ad.rem-system.com/Users/Domain Users	5-1	-5-21-4193742415-8133520026-20462399	GLOBAL		
			0	ad.rem-system.com/Users/Enterprise Admin	o 5+1	+5+21+4193742415+4133520026+20462399	UNIVERSAL	1	
				ad.rem-system.com/Users/Enterprise Key Ad	dmins S+1	-5-21-4193742415-4133520026-20462399	UNIVERSAL		
			0	ad.rem-system.com/Users/Enterprise Read-	only S+1	+5+21+4193742415+8133520026+20462399	UNIVERSAL		
			0	ad.rem-system.com/Users/Group Policy Cre	etor S+1	+5+21+4193742415+4133520026+20462399	GLOBAL		
			<				,	•	
							Cancel	ок	

Domänencomputer und -benutzer hinzufügen

Schritt 3: Identitätsquelltext hinzufügen

Navigieren Sie zu Administration > Identity Source Sequences, und fügen Sie eine Identity Source Sequence hinzu.

- Name: Identity\_AD
- Authentifizierungs-Suchliste: AD\_Join\_Point

≡	dentity Services	Engine		Administration / Id	lentity Management
н	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
18	Dashboard Context Visibility	Identity Source Sequence	equence		
* 0 <b>4</b> 0 eli	Operations Policy Administration Work Centers	V Identity Source * Name I Description	e Sequence dentity_AD		
(?)	Interactive Help	Certificate Bi     Select Certifi	ased Authentication	~	
		<ul> <li>Authentication</li> <li>A set of identification</li> <li>Available</li> <li>Internal I</li> <li>Internal I</li> <li>Guest Us</li> <li>All_AD_</li> </ul>	n Search List ntity sources that will be accessed in indpoints Jaers lers loin_Points	n sequence until first authentication su Selected AD_Join_Point	ucceeds

Identitätsquellensequenzen hinzufügen

#### Schritt 4: Policy Set hinzufügen

Navigieren Sie zu Policy > Policy Sets, und klicken Sie auf +, um einen Policy Set hinzuzufügen.

- Richtliniensatzname: VPN\_Test
- Bedingungen : GERÄTETYP ENTSPRICHT ALLEN GERÄTETYPEN
- Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff

≡	dentity Services Engin	ne	Policy / Policy Sets		🔺 Evaluation Mode = Days Q 🛕 😨 📮   🔎				
Щ	Bookmarks	Policy Sets			Reset	Reset Policyset Hite	counts	Sa	ve
51	Dashboard	+ Status Policy Set Name	Description	Conditions	Allowed Protocols	/ Server Sequence	Hits Ad	ctions V	liew
10	Context Visibility	Q Search							
×	Operations	NON Test	Г	DEVICE-Device Type EQUALS AII	Default Network Ar	reess 2 .L	~ 1	rên	
0	Policy	VPW_IOSI	L	Device Types			30 Ş	.Ş?	

```
Policy Set hinzufügen
```

Schritt 5: Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf VPN\_Test, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: VPN\_Authentication
- Bedingungen: IP-Adresse des Netzwerkzugriffsgeräts ENTSPRICHT 1.x.x.61
- Verwenden: Identity\_AD

		nits	Actions
Q Search			
	Identity_AD		
VPN_Authentication	> Options	10	ŝ

Authentifizierungsrichtlinie hinzufügen

#### Schritt 6: Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf VPN\_Test, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: VPN\_Authorization
- Bedingungen: Network\_Access\_Authentication\_Passed
- Ergebnisse : PermitAccess

		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
VPN_Authorization	Network_Access_Authentication_Pass	ed			ŝ

## Überprüfung

Schritt 1: Kopieren des sicheren Clientprofils auf Win10 PC1

Kopieren Sie das sichere Clientprofil in das Verzeichnis C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.

🗧 🕆 🗧 🕂	> This PC > Local Disk (C:) > ProgramData > Cisco	> Cisco Secure Client	> VPN > Profile >
	Name	Date modified	Туре
Quick access	MgmtTun	5/17/2024 8:42 AM	File folder
Desktop	vpn-ipsec-tunnel-grp_client_profile	5,123/2024 12:48 AM	XML Document
Downloads	AnyConnectProfile.xsd	'1./2024 1:12 PM	XSD File

### Schritt 2: VPN-Verbindung initiieren

Führen Sie auf dem Endgerät den Cisco Secure Client aus, geben Sie den Benutzernamen und das Kennwort ein, und bestätigen Sie dann, dass die Verbindung mit dem Cisco Secure Client erfolgreich hergestellt wurde.

Sisco Secure Client – 🗆 🗙	S Cisco Secure Client   ciscoasa (IPsec) IPv4 ×	S Cisco Secure Client − □ ×
AnyConnect VPN: Please enter your username and password. dscoasa (IPsec) IPv4 V Connect	Please enter your username and password. Group: vpn-ipsec-tunnel-grp Username: vpnuser	AnyConnect VPII: Connected to discoasa (IPsec) IPv4. discoasa (IPsec) IPv4 V Disconnect
	Password: ******	00:00:05 IPv4
	OK Cancel	

Verbindung erfolgreich

## Schritt 3: Syslog auf ASA bestätigen

Überprüfen Sie im Syslog, ob die IKEv2-Verbindung erfolgreich war.

#### <#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

## Schritt 4: IPsec-Sitzung auf ASA bestätigen

Führen Sie einen Befehl ausshow vpn-sessiondb detail anyconnect, um die IKEv2/IPsec-Sitzung auf der ASA zu bestätigen.

#### <#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 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

Schritt 5: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle) in der ISE-GUI, und bestätigen Sie das Live-

#### Protokoll für die VPN-Authentifizierung.

≡ dentity Services	s Engine			Operations / RA	DIUS			🛦 Evaluati	on Mode 📻 Days	۹ ۵ ۵	୭ <b>୦</b> ∣ ୧
JI Bookmarks	Live Logs Live Sessions										
E Dashboard											
1d Context Visibility	Misconfigured Supplicants		Misconfigured N	etwork Devices 📀	RADIUS Drops		<b>Glient Stopped Resp</b>	onding 🕓		Rep	seat Counter 📀
× Operations	0		(	0	0		0				0
() Policy								lafrash	Show	With	in
Administration								Never	Latest 20 re	cords 🗸 Last	t 3 hours 🗸
Work Centers	🕄 🐀 Reset Repeat Counts	$\pm$ Export To $\sim$								Filte	# Y 0
	Time	Status Details	Repeat Endpoint	Identity Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Port	Identity Grou
③ Interactive Help	×	~	Endpoint ID	Identity Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address V	Network Devic	Device Port	Identity Group
	May 28, 2024 05:13:42	• •	0 00.50.5	vpnuser Windows10-Workstat	on VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess				
	May 28, 2024 05:13:42	a o	00:50:5	vpruser Windows10-Workstati	on VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Workstation

Radius-Live-Protokoll

Klicken Sie auf Status, um die Details des Live-Protokolls zu bestätigen.

Cisco ISE					
Overview		Ste	eps		
Event	5200 Authentication succeeded	Ste	ep ID	Description	Latency (ms)
		110	001	Received RADIUS Access-Request	
Username	vpnuser	110	017	RADIUS created a new session	1
Endpoint Id	00:50:56:98:77:A4 ⊕	150	049	Evaluating Policy Group	36
Endpoint Profile	Windows10-Workstation	150	800	Evaluating Service Selection Policy	1
Authentiestics Delieu	VDN Test as VDN Authentication	150	048	Queried PIP - DEVICE.Device Type	6
Authentication Policy	VPN_lest >> VPN_Authentication	150	041	Evaluating Identity Policy	20
Authorization Policy	VPN_Test >> VPN_Authorization	150	048	Queried PIP - Network Access.Device IP Address	2
Authorization Result	PermitAccess	220	072	Selected identity source sequence - Identity_AD	6
		150	013	Selected Identity Source - AD_Join_Point	1
		244	430	Authenticating user against Active Directory - AD_Join_Point	4
Authentication Details		243	325	Resolving identity - vpnuser	38
Source Timestamp	2024-05-28 17:13:42.897	243	313	Search for matching accounts at join point - ad.rem- system.com	0
Received Timestamp	2024-05-28 17:13:42.897	243	319	Single matching account found in forest - ad.rem- system.com	0
Policy Server	ise33-01	243	323	Identity resolution detected single matching account	0
Event	5200 Authentication succeeded	243	343	RPC Logon request succeeded - vpnuser@ad.rem- system.com	23
Username	vpnuser	244	402	User authentication against Active Directory succeeded - AD_Join_Point	3
Enapoint la	00:50:56:98:77:A4	220	037	Authentication Passed	1
Calling Station Id	192.168.1.11	247	715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	1
Endpoint Profile	windows10-workstation	150	036	Evaluating Authorization Policy	1
Authentication Identity	AD_Join_Point	242	209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
Store		242	211	Found Endpoint in Internal Endpoints IDStore	9
Identity Group	Workstation	150	048	Queried PIP - Network Access.AuthenticationStatus	2
Audit Session Id	01aa003d0001700066559220	150	016	Selected Authorization Profile - PermitAccess	7
Authentication Method	PAP ASCI	220	081	Max sessions policy passed	6
- automotion motiou		220	080	New accounting session created in Session cache	0
Authentication Protocol	PAP_ASCII	110	002	Returned RADIUS Access-Accept	2
Network Device	ASAv				

Details zum Live-Protokoll

#### Fehlerbehebung

Die Nichtübereinstimmung der kryptografischen Algorithmen kann zu Verbindungsfehlern führen. Dies ist ein Beispiel dafür, wenn ein Problem mit einer Nichtübereinstimmung der Algorithmen auftritt. Durch Ausführen von Schritt 15 des Abschnitts "Konfiguration" in ASDM kann das Problem behoben werden.

#### Schritt 1: VPN-Verbindung initiieren

Führen Sie auf dem Endgerät den Cisco Secure Client aus, und vergewissern Sie sich, dass die Verbindung aufgrund einer nicht übereinstimmenden kryptografischen Algorithmen fehlgeschlagen ist.

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. discoasa (IPsec) IPv4		Connect		The cryptographic algorithms required by the secure gateway do not match those supported by Cisco Secure Client. Please contact your network administrator.	
				OK	

#### Verbindung fehlgeschlagen

#### Schritt 2: Syslog in CLI bestätigen

Bestätigen Sie im Syslog, dass die IKEv2-Aushandlung fehlgeschlagen ist.

#### <#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

#### Referenz

AnyConnect über IKEv2 zu ASA mit AAA und Authentifizierung von Zertifikaten

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.