# & Configureer beveiligde client IKEv2/ASA in ASDM met AAA Cert Auth

## Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten **Netwerkdiagram** Configuraties Configuratie in ASDM Stap 1. VPN-wizards openen Stap 2. Identificatie van verbindingsprofiel Stap 3. VPN-protocollen Stap 4. Clientafbeeldingen Stap 5. Verificatiemethoden Stap 6. SAML-configuratie Stap 7. Toewijzing van clientadres Stap 8. Netwerknaamoplossingsservers Stap 9. NAT-vrijstelling Stap 10. Beveiligde clientimplementatie Stap 11. Instellingen opslaan Stap 12. Beveiligd clientprofiel bevestigen en exporteren Stap 13. Bevestig details van beveiligd clientprofiel Stap 14. Instellingen in ASA CLI bevestigen Stap 15. Cryptografisch algoritme toevoegen Configuratie in Windows-server Configuratie in ISE Stap 1. Apparaat toevoegen Stap 2. Actieve map toevoegen Stap 3. Identiteitsbroncode toevoegen Stap 4. Beleidsset toevoegen Stap 5. Verificatiebeleid toevoegen Stap 6. Toepassingsbeleid toevoegen **Verifiëren** Stap 1. Kopieer een beveiligd clientprofiel naar Win10 PC1 Stap 2. VPN-verbinding starten Stap 3. Syslog op ASA bevestigen Stap 4. IPsec-sessie voor ASA bevestigen Stap 5. Radius live log bevestigen Problemen oplossen Stap 1. VPN-verbinding starten Stap 2. Syslog in CLI bevestigen **Referentie** 

## Inleiding

Dit document beschrijft de stappen die nodig zijn om een beveiligde client via IKEv2 op ASA te configureren met behulp van ASDM met AAA en certificaatverificatie.

## Voorwaarden

## Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie van Cisco Identity Services Engine (ISE)
- Configuratie van Cisco adaptieve security virtuele applicatie (ASAv)
- Configuratie van Cisco Adaptieve Security Device Manager (ASDM)
- VPN-verificatiestroom

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine virtuele 3.3-patch 1
- Adaptieve security virtuele applicatie 9.20(2)21
- Adaptieve security apparaatbeheer 7.20(2)
- Cisco Secure-client 5.1.3.62
- Windows Server 2016
- Windows 10

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.

De domeinnaam ingesteld op Windows Server 2016 is ad.rem-system.com, die wordt gebruikt als voorbeeld in dit document.



Netwerkdiagram

## Configuraties

## Configuratie in ASDM

### Stap 1. VPN-wizards openen

Navigeer naar Wizards > VPN Wizards, klik op Secure Client VPN Wizard.



## Klik op Next (Volgende).

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 protecte using either the IPsec or the SSL protocol. The ASA will automatically upload the Secure VPN Client to the end user's device	be
100 to	when a VPN connection is established.	
	Local e Remote	
Corporate		
sector to		
THUM HIM		
TIT		
	< gack Next > Rifl Help	

Klik op Volgende knop

Stap 2. Identificatie van verbindingsprofiel

Voer informatie in voor het verbindingsprofiel. Naam verbindingsprofiel: vpn-ipsec-tunnel-grp VPN-toegangsinterface: buiten

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	

Identificatie van verbindingsprofiel

## Stap 3. VPN-protocollen

Selecteer IPsec en klik op de knop Add om een nieuw zelfondertekend certificaat toe te voegen.

Secure Client VPN Connection Setup Wizard	X Same Analysis and Analysis an
Steps     VPN Protocols       1. Introduction     Secure Client can use either the IPsec or SS, protocol to protect the data traffic. Please select which protocol or prot would like this connection profile to support.       2. Connection Profile Identification     SSL       3. VPN Protocols     SSL       4. Clent Images     Prec       5. Authentication Methods     Device Certificate       6. SAML Configuration     Device Certificate identifies the ASA to the remote access clents. Certain Secure clerk feature (Many-On, IPsec/IJE-V2) require that valid device certificate be available on the ASA.       9. NAT Exempt 10. Secure Clent Deployment     Device Certificate:None	atocols you           Issued To         Issued By         Expiry Date         Associated Trustpoints         Usage         Public Key Type         Add           Show Details         Delete         Export         Install         Re-Erroll
< Back [Bent> R:II]	Eind: <ul> <li>Batch Case</li> <li>Certificate Expiration Alerts</li> <li>Send the first alert before:</li> <li>(days)</li> <li>(days)</li> <li>Set Default</li> <li>Repeat Alert Interval:</li> <li>7 (days)</li> </ul> Weak Crypto Configurations <ul> <li>Permit Weak key sizes and Hash Algorithms</li> <li>Public CA Enrolment</li> <li>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.</li> <li>Enroll ASA SSL certificate with Entrust.</li> <li>Using a previously saved certificate Wizard</li> <li>The Cisco ASM Identity Certificate Wizard assists you in creating a self-signed certificate that is required for launching ASDM through launcher.</li> <li>Launch ASDM Identity Certificate Wizard</li> </ul>

Voer informatie in voor een zelfondertekend certificaat.

Trustpoint Naam: vpn-ipsec-trustpoint

## Toetsenpaar: ipsec-kp

Add Identity Certificate X	To Add Key Pair	×
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: O RSA O 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	Enter new key pair name: ipsec-kp	
• Add a new identity certificate:	Size: 4096 v	
Key Pair: Ipsec-kp    Show New	Usage: O General purpose O Special	
Certificate Subject DN: CN=ciscoasa Select		
Generate self-signed certificate     Generate Now     Cancel     Help		
Advanced		
Enable CA flag in basic constraints extension		
Add Certificate Cancel Help		

Details van het zelfondertekende certificaat

Bevestig de instellingen van VPN-protocollen en klik op Volgende.

Secure Client VPN Conne	ction Setup Wizard	×
Steps         1. Introduction         2. Connection Profile Identification         J. 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 SSL Device Certificate 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 V Manage	u
	< Back Next > It in Help	

Instellingen VPN-protocol bevestigen

#### Stap 4. Clientafbeeldingen

Klik op de knop Add om een beveiligd cliëntbeeld toe te voegen en klik op Next.

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Client Images	
Introduction     Connection Profile     Identification     VPN Protocols     Client Images     Authentication Methods	ASA can automatically upload the latest Secure Client package to the of A regular expression can be used to match the user-agent of a browse You can also minimize connection setup time by moving the image used the top of the list.	lient device when it accesses the enterprise network. If to an image. By the most commonly encountered operation system to
<ol> <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-k9.pkg	Regular expression to match user-agent
	You can download Secure Client packages from Cisco by searching 'Se	cure Mobility Client' or <u>click here</u> ,
	< gack Next >	Riff Help

Clientafbeeldingen

## Stap 5. Verificatiemethoden

Klik op de knop Nieuw om een nieuwe server toe te voegen en klik op Volgende.

Naam servergroep : radius-grp

Verificatieprotocol: RADIUS

IP-adres server: 1.x.x.191

#### Interface: binnen

Secure Client VPN Conn	ection Setup Waard X	To New Authentication Server Group	Secure Client VPN Conner	tion Setup Wizard X
29a 1. bitsdator 2. Greentian hylle 2. Greentian hylle 3. With Protoch 3. Anthenatic attem Methods 6. Stat Configuration 7. Circle Address Assignme 5. Halt Configuration 5. Halt Configuration 16. Secure Circle Exployme 11. Samary	Alchertosans Helladi The dar bit on good the schertosation more: The card all on the Tables. "Subtin to cards a new server grace. AAA Server Grage (IKC)	Create a new authentication server group containing one authentication server. To add more servers to the group or drampe other AAA server etitings, go to Configuration Device Hanagemet > Users/AAA > AAA Server Group. Server Group Name: Authentication Protocol: Server IP Address: Interface: Interface:	9495 1. Information Public 2. Constitution Public Information 3. WHP Interacted 3. WHP Interacted 5. Authornal Assignment 5. Safe Configuration 7. Other Address Assignment 5. Natroak Same Beaution 5. Sammary	Alferticizen hiteled Tea dag letz you geeff, hite bioloxie of the authentication same. Aut forme Grapp I make op Team. Aut forme Grapp I make op Team. Aut forme Grapp I make op form. Aut forme Grapp Team.
	444 (942) (942) (94)	Server Secret Key: Confirm Server Secret Key:		494 943 0.0 Http://www.com/auto-auto-auto-auto-auto-auto-auto-auto-

## Stap 6. SAML-configuratie

## Klik op de knop Volgende.

Secure Client VPN Conne	action 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 authenticaion method. Authentication Method: AAA Server Group: radius-grp Use LOCAL if Server Group fails SAML Identity Provider SAML Server : None Manage	
	< Back Next > It in Help	

SAML-configuratie

#### Stap 7. Toewijzing van clientadres

Klik op Nieuwe knop om een nieuwe IPv4-pool toe te voegen en klik op Volgende knop.

Naam : vpn-ipsec-pool

IP-startadres: 172.16.1.20

EindIP-adres: 172.16.1.30

Subnetmasker: 255.255.255.0

Secure Client VPN Conne	ction Setup Wizard		×	Secure Client VPN Conne	nection Setup Wizard	×
Steps  I. Introduction Connection Profile Identification VPN Protocols 4. Clent Tunges 5. Authentication Methods	Clerk Address Assignment This step allows you to create a new address pool or be assigned addresses from the pools when they cor IPv6 address pool is only supported for 55L connects IPv6 address Pool Pv4 Address Pool Address Pool: Select Verv	select an existing addres nect. m.	s pool for IPv4 and IPv6. The Secure Clents will	Steps   I. Introduction Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods	Client Address Assignment         This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The Secure Client be assigned address pool is only supported for SSL connection.         IPv6 address pool is only supported for SSL connection.         IP v4 Address Pool         Address Pool         Address Pool         Address Pool	s will
G. SAML Configuration     Cilient Address     Assignment     Network Name Resolutio     Servers     NAT Exempt     Servers     Server Client Deployme     11. Summary	Details of the selected address pool	Name: Starting IP Address Ending IP Address: Subnet Mask: OK	Vpn-ipsec-pool 172.16.1.20 - 172.16.1.30 - 255.255.255.25.0 - Cancel Help	6. SAML Configuration 7. Client Address Assignment 8. Network Name Resolutio Servers 9. NAT Exempt 10. Secure Client Deployme 11. Summary	Details of the selected address pool Starting IP Address: Ending IP Address: 172:16:1.30 Subnet Mask: 255:255.255.0 V	
	<back next=""></back>		I(cif) Help		<back [jext="">] 取消 H</back>	elp

Clientadrestoewijzing

## Stap 8. Netwerknaamoplossingsservers

Invoerinformatie voor DNS en domein, klik op Volgende knop.

DNS-servers : 1.x.x.57

## Domeinnaam: 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	
	< gack Next > It if He	slp

Netwerknaamoplossingsservers

Stap 9. NAT-vrijstelling

Klik op de knop Volgende.

Secure Client VPN Conn	ection Setup Wizard	×
Steps	NAT Exempt	
<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>	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.	
	< Back Next > 現初	Help

NAT-vrijstelling

## Stap 10. Beveiligde clientimplementatie

## Selecteer Toestaan dat het web wordt gestart en klik op Volgende.

Secure Client VPN Conne	ction Setup Wizard X
Steps	Secure Client Deployment
Steps     I. Introduction     Connection Profile     Identification     VPN Protocols     Clent Images     Authentication Methods     SAML Configuration     Clent Address Assignme     Network Name Resolutio     Servers     NAT Exempt     IO. Secure Client     Deployment     II. Summary	Secure Client Deployment Secure Client program can be installed to a client device by one of the following two methods: 1) Web launch - On accessing the ASA using a Web Browser, the Secure Client package will be automatically installed; 2) Pre-deployment - Manually install the Secure Client package.  Allow Web Launch Caution: Web launch is global setting, it affects all connections. Secure Client SSL connections and clientless SSL connections will NOT work if it is turned off.  For pre-deployment, please remember to include the client profile 'disk0:/vpn-ipsec-tunnel-grp_client_profile.xml' from the ASA in your Secure Client package, otherwise IPsec connection will NOT work.
	< Back Next > 現初 Help

### Stap 11. Instellingen opslaan

Klik op Finish (Voltooien) en sla de instellingen op.

Secure Client VPN Conne	ction Setup Wizard		X 🖾 Warning X	2
VPN Wizard	Summary		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	
	Here is the summary of the configuration.		[OK] ip local pool vpn-ipsec-pool 172.16.1.20-172.16.1.30 mask 255.255.255.0	1
EDIT	Name	Value	[OK] ! write client profile "disk0:/vpn-ipsec-tunnel-grp_client_profile.xml" to ASA [OK] webvpn	
	Summary Name/Alias of the Connection Profile	vpn-ipsec-tunnel-grp	[OK] anyconnect profiles vpn-ipsec-tunnel-grp_client_profile disk0:/vpn-ipsec-tunnel-grp_client_profile.xml [OK] exit	
(corporate)	VPN Access Interface Device Digital Certificate	outside vpn-ipsec-trustpoint:unstructuredName=ciscoasa, CN	[OK] aaa-server radius-grp protocol radius [OK] aaa-server radius-grp (inside) host 1.[i.J.191	
Network	VPN Protocols Enabled Secure Client Images	IPsec only 1 package	aaa-server radus-grp (inside) host 1.1"	
I A	Authentication Server Group	radus-grp Server:	[OK] vsy [OK] exit [OK] group-policy GroupPolicy vpn-ipsec-tunnel-grp internal	
	Address Pool for the Client	Authentication Method: asa 172.16.1.20 - 172.16.1.30	[OK] group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes	
1 Trantill	DNS	Server: Domain Name:	[OK] vpn-tunnel-protocol lkev2 [OK] webvpn	
TTT	Network Address Translation	The protected traffic can be subjected to network address translation	group-policy GroupPolicy_vpn-ipsec-tunnel-grp attributes webypn	
6 A-			[Ux] anyconnect prortees value symplexe-cunnel-grp_sterk_prortie type user [Uk] gext [Uk] group-policy GroupPolicy_ypn-ipsec-tunnel-grp attributes aroup-policy GroupPolicy von-ipsec-tunnel-grp attributes	
	< Back Einish	- 取詞 He	Close	

Instellingen opslaan

#### Stap 12. Beveiligd clientprofiel bevestigen en exporteren

Navigeer naar Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile, klik op Edit knop.

File View Iools Wigards Window Help	re 🔇 Refresh 🔾 Back 💭 Forward 🦻 Help			Type topic to search Go	cisco
Device List Bookmarks	Configuration > Remote Access VPN > Network (Client) Acce	ss > Secure Client Profile			
Boolmarks <u>a</u> a <u>a</u> a <u>x</u> To boolmark a page, right-click on a node in the navigation tree and select. "Add to boolemarks". Go <u>to</u> Delete	This panel is used to manage Secure Client Profiles and perform grou upload and download of client profiles between local machine and de The profile Usage field is introduced with the Secure Mobility Solution	p assignment for Secure Client version 2.5 or later. You can select a pr vice. . This field contains different profile usage in Secure Client version 3.0	offe to edit, change group or to delete. You can select the 'Add' butt and later.	on to add a new profile. Pressing the Import or Export bu	tton is for
Remote Access VPN 67 0	🗣 Ada 🗭 Edit 🔀 Change Group Policy 📋 Delete 🐺 Import	The Export 🔊 Valdate			
Introduction     Introduction	Profile Name Ispri-pisec-tunnel-grp_clenet_profile	Profile Usage AnyConnect VPN Profile	Group Policy GroupPolicy_upn-ipsec-tunnel-grp	Profile Location disk0:/vpn-psec-turnel-grp_ckent_profile.xml	

Beveiligd clientprofiel bewerken

Bevestig de details van het profiel.

- Display naam (verplicht): ciscoasa (IPsec) IPv4
- FQDN- of IP-adres: 192.168.1.1
- Primair protocol: IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grp	client_profile					Server List Entry					×
Profile: vpn-ipsec-tunnel-grp_client_profile				Server Load Balancing Servers SCEP Hoble Certificate Pinning								
Preferences (Part 1) Preferences (Part 2) References (Part 2)	Server List						Primary Server Connec Display Name (inquired) (coccase (Prec) Pref			Connection Informatio	on [Pec ∵]	
Centrate Having Centrate Having Centrate Having Centrate Market Ender Having	Houtmanne Researce (Direct & a Note: it is highly of	Hot Address - 192-546-1-1 ecommended that at	Uber Group	Backap Server List	SCIP Mobile	Setting	Poper P Add 190, 548-1.1 Group URL	Backup Servers		Auth Hethod D	uring B/E Registration 05 gateway only) Add Move Up Move Up Move Down Delete	[AP-AryCorrect ->
									OK.	Carcel		

Beveiligd clientprofiel bevestigen

### Klik op de knop Exporteren om het profiel naar een lokale pc te exporteren.

File View Tools Wizards Window Help				Type topic to search
🚮 Home 🙈 Configuration 😥 Monitoring 🔚 Sar	we 🔇 Refresh 🔇 Back 🕥 Forward 🧳	Help		
Device List Realmonder	Conferentiate & Description & Annual Mathematica	much (Claub) Assess & Course Claub Deeffe		
Perfection Doormans	Configuration > Remote Access VPN > Net	WORK (CHERK) ACCESS > Secure Cherk Prome		
Boomaris D' 4 ×	J			
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 Pro	iles and perform group assignment for Secure Client version 2.5 or later.Yo	u can select a profile to edit, change group or to delete. You can sele	ect the 'Add' button to add a new profile. Pressing the Import or Expo
	and download of client profiles between local m	achine and device.	interest in a selector	
Go Delete	The profile Usage field is introduced with the Se	cure Mobility Solution. This field contains different profile usage in Secure (	lient version 3.0 and later.	
Remote Access VPN d <sup>3</sup> Q	Add 2 Edt S Change Group Policy	Delete Timort & Export A Validate		
-? Introduction				
Network (Client) Access	Profile Name	Profile Usage	Group Policy	Profile Location
Secure Client Connection Profiles	vpn-ipsec-tunnel-grp_client_profile	Any Connect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
Secure Client Customization/Localization				
Resources				
Binary		Expert Secure Client Brofile	~	
Cill Text and Mass and		Export Secure Client Pronie	^	
Customized Installer Transforms		This namel is used to expect Secure Client profile from devi	ra to the local file system	
I ocalized Installer Transforms		The particle data to expert secore client prove from den	te to the local the system	
- Secure Client Profile				
Secure Client Software				
Secure Client External Browser		Profile Name: vpn-ipsec-tunnel-grp_client_profile		
- Dynamic Access Policies				
Group Policies		Local Bables Colliferentic et 2126, Dec Oreal Date	Itaalumo in Resure Leval	
IPsec(I):Ev1) Connection Profiles		colorestant colorestantes and colorest	cop/vprinp browse coca	
Psec(II:Ev2) Connection Profiles				
- Secure Mobility Solution				
Address Assignment				
H S Advanced				
Clericess SSL WTN Access		Export Cancel	Help	
Average of the Section and Section an				

Beveiligd clientprofiel exporteren

#### Stap 13. Bevestig details van beveiligd clientprofiel

Open een beveiligd clientprofiel via de browser en bevestig dat het primaire protocol voor de host IPsec is.

```
\u00ed 
\u00ed <
```

Details van beveiligd clientprofiel

#### Stap 14. Instellingen in ASA CLI bevestigen

Bevestig de IPsec-instellingen die door ASDM in de ASA CLI zijn gemaakt.

```
// 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

Stap 15. Cryptografisch algoritme toevoegen

In ASA CLI voegt u groep 19 toe aan het IKEv2-beleid.



Opmerking: voor IKEv2/IPsec-verbindingen ondersteunt Cisco Secure Client vanaf versie 4.9.00086 niet langer Diffie-Hellman (DH) groepen 2, 5, 14 en 24. Deze verandering kan in verbindingsmislukkingen resulteren toe te schrijven aan cryptografische algoritmemismatches.

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

Configuratie in Windows-server

U moet een domeingebruiker toevoegen voor een VPN-verbinding. Navigeer naar Active Directory-gebruikers en -computers, klik op Gebruikers. Voeg vpnuser toe als domeingebruiker.

Active Directory Users and Computers						
File Action View Help						
수	🐮 🕼 🍸 🗾 🐍					
Active Directory Users and Computers winserver.ad.rem-system.com Saved Quenes Gomputers Computers Domain Controllers Compain SecurityPrincipals Mananed Service Accounts Users	Name Administrator Allowed RODC Passwor Cert Publishers Cloneable Domain Con Cert Publishers Cloneable Domain Con DefaultAccount Denied RODC Passwore Denied RODC Passwore Denied RODC Passwore Domain Gousts Domain Controllers Domain Guests Domain Guests Domain Guests Domain Users Enterprise Read-only Di Coup Policy Creator O Coup Policy Creator O	vpn user Properties Member Of Remote control General Address vpn user Bint name: Last name: Digplay name: Recorption: Office: Telephone number:	Dial-In Envi Remote Desktop Se Account Profile	vonment envices Profile Telephones	? × Sessions COM+ Organization	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 ators 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 s group are Read-Only Domain Controllers in t s group are modify group policy for the domain t for quest access to the sense the foremain
	Image: Guest         Image: Guest	Islephone number: Email: Web page:	DK Cancel	ésoly	@her Déher	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

Domeingebruiker toevoegen

## Voeg de domeingebruiker toe aan het lid van Domeinbeheerders en Domeingebruikers.

pn user Properties				?	$\times$	vpn user Pr	operties				?	$\times$
Remote control	Remote [	Desktop Se	arvices Profile	CO	M+	Remote	control	Remote	Desktop S	ervices Profile	CO	M+
Member Of	Dial-in	Env	ironment	Sessio	ns	General	Address	Account	Profile	Telephones	Organia	zation
General Address	Account	Profile	Telephones	Organi	zation	Membe	er Of	Dial-in	Env	vironment	Sessio	ns
User logon name:						Member o	£					
vpnuser		@ad.re	m-system.com		$\sim$	Name		Active Direct	tory Domai	n Services Folder	r	
User logon name (pre-	Windows 200	0):				Domain	Admins	ad.rem-syste	m.com/Us	ers		
AD\		vpnuser	r			Domain	Users	ad.rem-syste	m.com/Us	ers		
User must chan     User cannot chi     Password never     Store password     Account expires	ge password a ange password rexpires using reversib	it next logo d le encryptic	n		~	Add. Primary gr	oup: D	Remove omain Users There is r	no need to	change Primary	group unle	
Never						<u>Set Fu</u>	mary droup	you have application	Macintosh ons.	n clients or POSI)	(-complian	t
⊖ <u>E</u> nd of:	Monday .	June	10, 2024	Ţ	]							
0	ĸ	Cancel	Apply	Н	elp		0	K	Cancel	Apply	Н	elp

Domain Admins en domeingebruikers

## Configuratie in ISE

### Stap 1. Apparaat toevoegen

Navigeer naar Beheer > Netwerkapparaten, klik op de knop Toevoegen om ASAv-apparaat toe te voegen.

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS	Servers RA	DIUS Server Sequences
Network Devices Default Device Device Security Settings	Network Devic Network I Name Description	ASAv	51 / 32 👳		
	Device Pro Model Nar	file 🗰 Cisco	~ ©		
	Software \ Network D	evice Group	~		
	Location	All Locations	~	Set To Default	
	IPSEC	No	~	Set To Default	
	Device Typ	All Device Types	~	Set To Default	
	C V R4 Pre	RADIUS Authentication	n Settings		
	Sh	ared Secret cisco123		Hide	

Apparaat toevoegen

#### Stap 2. Actieve map toevoegen

Navigeer naar Beheer > Externe Identiteitsbronnen > Active Directory, klik op Connectiontab, voeg Active Directory toe aan ISE.

- Lid worden: AD\_Join\_Point
- Active Directory-domein: ad.rem-system.com



Actieve map toevoegen

#### Navigeer naar het tabblad Groepen, selecteer Groepen uit directoraat uit vervolgkeuzelijst.

dentity Services E	e Administration / identity Management	
okmarks	tities Groups External Identity Sources Identity Source Sequences Settings	
shboard		
ontext Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings	
perations	C BS Cattless Automation Update SID Values	
licy	Certificate Auditenciat      Select Groups From Directory      SiD	
Iministration	AD_Join_Point Add Group Control Assist ad.rem-system.com/S-1-5-32-579	
	Identity Services Engin kmarks Iden hboard http://www.initiality http://wwww.initiality http://www.initiality http://www.initiality http://www.initiality http://www.initiality http://wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwww	Identity Services Engine     Administration / Identity Management       wkmarks     Identities     Groups     External Identity Sources     Identity Sources       ukboard     Identities     Groups     External Identity Sources     Identities       ukboard     Identities     Groups     Attributes     Advanced Settings       arations     Connection     Allowed Domains     PassiveID     Groups       is Certificate Authenticat     Certificate Authenticat     SID       is Select Groups     Control Assist     add Group     Control Assist

Selecteer Groepen uit map

Klik op Groepen ophalen in de vervolgkeuzelijst. Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Gebruikers en klik op OK.

×	
. 1	
1	
1.1	
1 1	
0.1	
DK	

Domeincomputers en -gebruikers toevoegen

#### Stap 3. Identiteitsbroncode toevoegen

Navigeer naar Beheer > Identity Source Sequences, voeg een Identity Source Sequence toe.

• Naam: Identity\_AD

• Verificatie Zoeklijst: AD\_Join\_Point

≡	dentity Services I	Engine		Administration / Id	lentity Management
н	Bookmarks	Identities Group	s External Identity Sources	Identity Source Sequences	Settings
51	Dashboard	Identity Source Seau	nces List ) Identity_AD		
명	Context Visibility	Identity Source	Sequence		
*	Operations				
-0	Policy	<ul> <li>Identity So</li> </ul>	irce Sequence		
2.	Administration	-	Identity_AD		
đ	Work Centers	Description			
					A
(?)	Interactive Help	✓ Certificate	Based Authentication		
		Select Cr	rtificate Authentication Profile	~	
		✓ Authentica	tion Search List		
		A set of	dentity sources that will be accesse	d in sequence until first authentication se	ucceeds
		Avail	ble	Selected	
		Interr	al Endpoints	AD_Join_Point ^	
		Interr	al Users		
		Gues All A	D Join Points		
					슬
			>>		
			<b></b>	0	Σ]
Iden	tity Source Sequence	es toevoegen			

#### Stap 4. Beleidsset toevoegen

Navigeer naar Policy > Policy Sets, klik op + om een policy set toe te voegen.

- Naam reeks beleid: VPN\_Test
- Voorwaarden: Apparaattype komt overeen met alle apparaattypen
- Toegestane protocollen/serverreeks: standaard netwerktoegang

≡	dentity Services Er	gine Policy / Policy Sets	🔺 Evaluation Mode = Cays Q 💩 💿 📮 🛛 R
Щ	Bookmarks	Policy Sets	Reset Reset Policyset Hitcounts Save
	Dashboard	Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
망	Context Visibility	Q Search	
*	Operations	VPN Test     DEVICE Device Type I	EQUALS All Default Network Access
0	Policy	Device Types	
Bele	eidsset toevoegen		

## Stap 5. Verificatiebeleid toevoegen

Navigeer naar Beleidssets, klik op VPN\_Test om een verificatiebeleid toe te voegen.

• Regelnaam: VPN\_Verificatie

- Voorwaarden: IP-adres voor netwerktoegangsapparaat is gelijk aan 1.x.x.61
- Gebruik: Identity\_AD

∨Authentication Policy(2)				
(+) Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
		Identity_AD		-0-
VPN_Authentication	Retwork Access-Device IP Address EQUALS 1.171.1.61	> Options	10	ţÇž
√erificatiebeleid toevoegen				

Stap 6. Toepassingsbeleid toevoegen

Navigeer naar Beleidssets, klik op VPN\_Test om een autorisatiebeleid toe te voegen.

- Regel Naam: VPN\_Authorisation
- Voorwaarden: Network\_Access\_Authentication\_Passed
- Resultaten: PermitAccess

	Results			
Conditions	Profiles	Security Groups	Hits	Actions
Network_Access_Authentication_Passed	PermitAccess			ŝ
	Conditions Network_Access_Authentication_Passed	Results       Conditions     Profiles       Network_Access_Authentication_Passed     PermitAccess	Results         Conditions       Profiles       Security Groups         Network_Access_Authentication_Passed       PermitAccess	Results       Profiles       Security Groups       Hits         Network_Access_Authentication_Passed       PermitAccess       2 +       Select from list       2 +       10

Toepassingsbeleid toevoegen

## Verifiëren

Stap 1. Kopieer een beveiligd clientprofiel naar Win10 PC1

Kopieer het beveiligde clientprofiel naar de map C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile.

← → • ↑ 📙	> This PC > Local Disk (C:) > ProgramData > Cisco	> Cisco Secure Client	t > VPN > Profile >
1 Ouistansee	Name	Date modified	Туре
Quick access	MgmtTun	5/17/2024 8:42 AM	File folder
Desktop 🖈	vpn-ipsec-tunnel-grp_client_profile	5,173/2024 12:48 AM	XML Document
	AnyConnectProfile.xsd	/1./2024 1:12 PM	XSD File

Profiel naar PC kopiëren

Stap 2. VPN-verbinding starten

Voer in het eindpunt Cisco Secure Client uit en voer de gebruikersnaam en het wachtwoord in en controleer vervolgens of de verbindingen met Cisco Secure Client zijn geslaagd.



Verbinding geslaagd

### Stap 3. Syslog op ASA bevestigen

In syslog, bevestig dat de verbinding IKEv2 slaagde.

#### <#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

## Stap 4. IPsec-sessie voor ASA bevestigen

voer de opdracht uitshow vpn-sessiondb detail anyconnect om de IKEv2/IPsec-sessie op ASA te bevestigen.

#### <#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

Stap 5. Radius live log bevestigen

Navigeer naar Operations > RADIUS > Live Logs in ISE GUI en bevestig het live log voor VPN-verificatie.

≡	dentity Services E	Engine			Operations / RADI	US			🛦 Evalue	ation Mode 🥌 Days	۵ ۵	• • I	۹
н	Bookmarks	Live Logs Live Sessions											
	Dashboard												
N	Context Visibility	Misconfigured Supplicants		Misconfigured Network	Devices 📀	RADIUS Drops		<b>Client Stopped Re</b>	sponding 💿		Re	peat Counter	
*	Operations	0		0		0		0				0	
Ð	Policy								Refresh	Show	Wei	in	
8.	Administration								Never	V Latest 20 rec	cords 🗸 Las	t 3 hours	ŕ
ก็เ	Work Centers	C for Reset Repeat Counts	🕁 Export To 🗸								FØ	w V O	
		Time	Status Details	Repeat Endpoint Ide	tity Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Port	Identity Gro	u
(?)	Interactive Help	×	~	Endpoint ID Ide	tity Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address V	Network Devic	Device Port	Identity Grou	2
		May 28, 2024 05:13:42	• a	0 00.50.5 vpm	ser Windows10-Workstation	${\tt VPN}_{\rm a}{\tt Test} \mapsto {\tt VPN}_{\rm a}{\tt Authentication}$	VPN_Test >> VPN_Authorization	PermitAccess					
		May 28, 2024 05:13:42	a a	00:50:5 vpm	ser Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Workstation	

Radius live log

#### Klik op Status om de details van het bewegend logbestand te bevestigen.

Cisco ISE				
		1		
Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
LIGHT		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
		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	00:50:56:98:77:A4	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	Windows10-Workstation	15036	Evaluating Authorization Policy	1
Authentication Identity	AD_Join_Point	24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
Store		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 ASCI	22081	Max sessions policy passed	6
		22080	New accounting session created in Session cache	0
Authentication Protocol	PAP_ASCII	11002	Returned RADIUS Access-Accept	2
Network Device	ASAv			

Detail van bewegend logboek

#### Problemen oplossen

De cryptografische algoritmen mismatch kan resulteren in verbindingsfouten. Dit is een voorbeeld van een probleem waarbij algoritmen niet overeenkomen. Het uitvoeren van Stap 15 van de sectie Configuration in ASDM kan het probleem oplossen.

Stap 1. VPN-verbinding starten

Voer op het eindpunt de Cisco Secure Client uit en bevestig dat de verbinding is mislukt vanwege een verkeerde match van cryptografische

algoritmen.

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

Sisco Secure Client		-		×	Cisco Secure Client	$\times$
AnyConnect VPII: Ready to connect. ciscoasa (IPsec) IPv4	~	~] Cor	Connect		The cryptographic algorithms required by the secure gateway do not match those supported by Cisco Secure Client. Please contact your network administrator.	
					ОК	

Verbinding is mislukt

Stap 2. Syslog in CLI bevestigen

Bevestig in syslog dat de IKEv2-onderhandeling is mislukt.

#### <#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

Referentie

AnyConnect over IKEv2 naar ASA met AAA- en certificaatverificatie

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.