# 在具有AAA &;證書身份驗證的ASDM中配置安 全客戶端IKEv2/ASA

目錄
· · · · · · · · · · · · · · · · · · ·
<u>必要條件</u>
<u>需求</u>
<u>採用元件</u>
<u>網路圖表</u>
 ASDM中的配置
步驟 1.開放式VPN嚮導
步驟 2.連線設定檔辨識
步驟 3.VPN通訊協定
步驟 4.客戶端映像
<u>步驟 5.驗證方法</u>
步驟 6.SAML配置
<u> </u>
步骤 9.NAT免除
步驟 10.安全客戶端部署
步驟 12.確認並匯出安全使用者端設定檔
步驟 13.確認安全客戶端配置檔案的詳細資訊
步驟 14.在ASA CLI中確認設定
<u>步驟 15.增加加密演算法</u>
<u>Windows Server中的配置</u>
<u>ISE中的配置</u>
<u>步驟 1.增加裝置</u>
步驟 2.新增Active Directory
<u>步驟 3.增加身份源隔離</u>
<u> </u>
<u> </u>
步驟 1.將安全客戶端配置檔案複製到Win10 PC1
步驟 4.確認ASA上的IPsec會話
步驟 5.確認Radius即時日誌
<u>疑難排解</u>
步驟 1.啟動VPN連線
步驟 2.在CLI中確認系統日誌
參考

# 簡介

本文檔介紹在ASA上使用帶AAA和證書身份驗證的ASDM配置IKEv2上的安全客戶端所需的步驟。

# 必要條件

# 需求

思科建議您瞭解以下主題:

- 思科身份服務引擎(ISE)的配置
- 思科自適應安全虛擬裝置(ASAv)的配置
- 思科自適應安全裝置管理器(ASDM)的配置
- VPN身份驗證流程

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 身分辨識服務引擎虛擬3.3修補程式1
- 調適型安全虛擬裝置9.20(2)21
- 調適型安全裝置管理器7.20(2)
- 思科安全使用者端5.1.3.62
- Windows Server 2016
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

# 網路圖表

下圖顯示本文檔示例中使用的拓撲。

在Windows Server 2016上配置的域名是ad.rem-system.com,本文檔中用作示例。



網路圖表

# 組態

# ASDM中的配置

### 步驟 1.開放式VPN嚮導

# 導航到Wizards > VPN Wizards,按一下Secure Client VPN Wizard。



# 按「Next」(下一步)。

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 when a VPN connection is established.	bd
Conter -	VPN Remote Access	
Corporate Network	Local P Remote	
	< Back 版ext > 取引 Help	

按一下「下一步」按鈕

步驟 2.連線設定檔辨識

輸入連線配置檔案的資訊。 連線配置檔名稱:vpn-ipsec-tunnel-grp VPN訪問介面:outside

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		
5. Authentication Methods	VPN Access Interface: outside 🗸	
6. SAML Configuration		
7. Client Address Assignme		
<ol> <li>Network Name Resolutio Servers</li> </ol>		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	< Back Next > It if Help	

連線設定檔辨識

### 步驟 3.VPN通訊協定

# 選擇IPsec,按一下Add按鈕以增加新的自簽名證書。

Conne Client VPN Conne	ection Setup Wizard	Ta Manage Identity Certificates
Steps   I. Introduction  C. Connection Profile Identification  VPN Protocols  C. Cent Images  Authentication Methods  S. SANE Configuration  C. Clent Address Assignme  B. Network Name Resolutio Servers  N. NAT Exempt  S. Socure Clent Deployme  S. Socure Clent Deployme	VPN Protocols         Secure Cleart 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 support.         SSL         Prec         Device Certificate         Device Certificate identifies the ASA to the remote access clearts. Certain Secure Cleart features (Always-On, IPsec/IB/EV2) require that valid device certificate be available on the ASA.         Device Certificate:       - None         Manage	Issued To Issued By Expiry Date Associated Trustpoints Usage Public Key Type Add Show Details Delete Export Install Re-Erroll
	<back bent=""> Rin Help</back>	End: <ul> <li>Match Case</li> <li>Certificate Expiration Alerts</li> <li>Send the first alert before : 60 (days)</li> <li>Set Default</li> <li>Repeat Alert Interval : 7 (days)</li> </ul> Weak Crypto Configurations <ul> <li>(days)</li> <li>Weak Key sizes and Hash Algorithms.</li> </ul> Public CA Enrollment <ul> <li>Get your Cisco ASA security applance 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 besting.             <ul> <li>Enroll ASA SSL certificate with Entrust.</li> <li>Using a previously saved certificate signing request, encol with Entrust.</li> <li>4STMI Identity: Certificate Ward</li> </ul></li></ul>
		The Clisco 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

# 輸入自簽名證書的資訊。

# 信任點名稱:vpn-ipsec-trustpoint

# 金鑰對:ipsec-kp

Ta Add Identity Certificate X	Ta 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	Enter new key pair name: psec-#p
• 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	

自簽名證書的詳細資訊

# 確認VPN協定的設定,按一下Next按鈕。

Secure Client VPN Conne	ection 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         Manage	u
	< Back Next > Ikin Help	

確認VPN協定的設定

### 按一下Add按鈕增加安全客戶端映像,然後按一下Next按鈕。

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 bro 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 substantial distantial of a	
5. Authentication Methods	TAdd Add Replace Delete T	
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 searching	g 'Secure Mobility Client' or <u>click here</u> ,
	< gack Next >	Ikin Help

客戶端映像

#### 步驟 5.驗證方法

按一下New按鈕增加新的aaa伺服器,按一下Next按鈕。

伺服器組名稱:radius-grp

身份驗證協定:RADIUS

伺服器IP地址:1.x.x.191

介面:inside

Secure Client VPN Connect	ion Setup Wizard	× Ta New Authentication Server Group	×	Secure Client VPN Connection Setup	Wizard	×
Dag 1. Simolaction 2. Connotion hullin Sentration 3. With Protocols 4. Card Inages 5. Add-backation Hetbool 6. Stef Configuration 7. Clerit Ablesi Alargine 8. Secure Clerit Deployme 10. Secure Clerit Deployme 11. Summary	Alternisment Mehnde Marken der Alter von eine Alternisme einen Texa and als der Versum-, Statien tei under anner anner greuze. AAA Server Greuz (1004) : Texa Land kater Laded (1004) : Alter 2004 Dienen eine Alded (1004) : Alter 2004 Presentel (1004) : Dienen eine Alter 2004 Presentel (1004) : Dienen eine Alter 2004 Presentel (1004) : Dienen eine Alter 2004 Dienen einen eine Alter 2004 Dienen einen einen einen einen einen einen einen einen einen einter 2004 Dienen eine	Create a new authentication server group containing one authentication server. To add more server to the group or change other AAA server restringing to to Configuration > Denice Hamagement > > Usergroup AAA Server Groups. Server Group Name: Authentication Protocol: Server IP Address: Littin_191 Interface: Interface:		Steps         Althoritic           1. Ditrokation         This step is biofedication         This step is biofedication           3. With House         Althoritic           3. With House         Althoritic           6. Ball confearation         Althoritic           6. Ball confearation         Althoritic           7. Clinet Address Asigner         Althoritic           8. Marc Confearation         State Confearation           9. Marc Confearation         State Confearation           10. Source Clinet Deployme         11. Summary	kon Mehoda In sou used y status of the authentication server, sou used y status of the authentication server, sous petal. If call the status of the status of the status of the status of the status of the status	
	 RA Bet> RA He	Server Secret Key:		< ĝak	Bet> R.A	Help
		OK Cancel Hep				

# 步驟 6.SAML配置

# 按一下Next按鈕。

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         AAA Server Group:       radus-grp         Use LOCAL if Server Group fails         SAML Identity Provider         SAML Server :       None	
	< gack Next > Rifl	Help

SAML配置

步驟 7.客戶端地址分配

按一下New按鈕增加新的IPv4池,然後按一下Next按鈕。

名稱:vpn-ipsec-pool

- 起始IP地址:172.16.1.20
- 結束IP地址:172.16.1.30
- 子網掩碼:255.255.255.0

Secure Client VPN Conne	ection Setup Wizard	×	Secure Client VPN Conne	nection Setup Wizard	×
Concre Client VPN Connor Seps 1. Introduction 2. Connection Profe Identification 3. VPN Protocols 4. Clerk Images 5. Authentication Nethods 6. SANL Configuration 7. Client Address Assignment 9. NAT Exempt 10. Secure Client Deployme 11. Summary	Clent Address Assignment. This step allows you to create a new address pool or select an exis be assigned addresses from the pools when they connect. IPV6 address pool is only supported for SSL connection. IPV6 address pool Address Pool: Select New Raddess Pool Details of the selected address pool Submet I Submet	ting address pool for IP+4 and IP+6. The Secure Clents will  v4 Pool V4 Pool V P Address IP2.16.1.30 P Address I255.255.6 V OK Cancel Help	Secure Client VPN Comm Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Client Images 5. Authentication Methods 6. SAML Configuration 7. Client Address Assignment 8. Network Name Resolutio Servers 9. NAT Exempt 10. Secure Client Deployme 11. Summary	nection Setup Wizard  Clerk Address Assignment  This site allows you to create a new address pool or select an existing address pool for IP+4 and IP+6. The Secure Clerks w be assigned address pool is only supported for SSL connection.  IP+4 address Pool P+4 Address Pool Address Pool Starting IP Address:  172.16.1.30  Charles I 172.16.1.30  Subnet Mask:  255.255.255.0  ✓	× ndl
	< Back Next >	Rcii) Help		<gadk next=""> Riff Heb</gadk>	2

客戶端地址分配

# 步驟 8.網路名稱解析伺服器

# 輸入DNS和域的資訊,然後按一下Next按鈕。

DNS伺服器:1.x.x.57

# 域名:ad.rem-system.com

Secure Client VPN Conne	ection Setup Wizard	×
Steps	Network Name Resolution Servers	
1. Introduction	This step lets you specify how domain names are resolved for the remote user when accessing the internal network.	
2. Connection Profile Identification	DNS Servers: 1.102.0.57	
3. VPN Protocols	WINS Servers:	
4. Client Images	Domain Name: ad.rem-system.com	
5. Authentication Methods		
6. SAML Configuration		
7. Client Address Assignme		
8. Network Name Resolution Servers		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	< Back Next >	Help

網路名稱解析伺服器

# 步驟 9.NAT免除

按一下Next按鈕。

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

NAT免除

# 步驟 10.安全客戶端部署

# 選擇允許Web啟動,然後按一下「下一步」按鈕。

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 CURRED 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 > 現前 Help

### 步驟 11.儲存設定

### 按一下Finish按鈕並儲存設定。

Secure Client VPN Conne	ction 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 fallure, [INFO] means information and [WARNING] means warning
	Name Summary Name/Alas of the Connection Profile VPN Access Interface Device Digital Cettificate VPN Protocols Enabled Secure Clenk Images Authentication Server Group SAML Address Pool for the Clenk	Value vpn-ipsec-tunnel-grp outside vpn-ipsec-trustpoint:unstructuredName=ciscoasa, CN IPsec only 1 package radur-grp Server: Authentication Method: aaa 172.16.1.30 - 172.16.1.30	[O(:) p local pool spr-ipsec-pool 172:16.1.20-172:16.1.30 mask 295.255.255.0         [O(:) I write client profile "disi0:/prn-ipsec-tunnel-gp_client_profile.xml" to ASA         [O(:) anyconnect profiles vpn-ipsec-tunnel-gp_client_profile.xml" to ASA         [O(:) anyconnect profiles vpn-ipsec-tunnel-gp_client_profile.xml" to ASA         [O(:) anyconnect profiles vpn-ipsec-tunnel-gp_client_profile.xml         [O(:) any-server radue-gp (mide) host 1.1.1
	DNS Network Address Translation <back enish<="" td=""><td>erver: Domain Name: The protected traffic can be subjected to network address translation</td><td>[Ok] upin-turner-protocol wev2         [Ok] upin-turner-protocol wev2         [Ok] upin-turner-protocol wev2         [Ok] any-context profiles value vpn-ipsec-turnel-grp attributes         webynn         [Ok] any-context profiles value vpn-ipsec-turnel-grp_clent_profile type user         [Ok] group-policy GroupPolicy_vpn-ipsec-turnel-grp attributes         aroup-policy GroupPolicy von-ipsec-turnel-grp attributes         GK] group-policy GroupPolicy von-ipsec-turnel-grp attributes         Glose</td></back>	erver: Domain Name: The protected traffic can be subjected to network address translation	[Ok] upin-turner-protocol wev2         [Ok] upin-turner-protocol wev2         [Ok] upin-turner-protocol wev2         [Ok] any-context profiles value vpn-ipsec-turnel-grp attributes         webynn         [Ok] any-context profiles value vpn-ipsec-turnel-grp_clent_profile type user         [Ok] group-policy GroupPolicy_vpn-ipsec-turnel-grp attributes         aroup-policy GroupPolicy von-ipsec-turnel-grp attributes         GK] group-policy GroupPolicy von-ipsec-turnel-grp attributes         Glose

儲存設定

#### 步驟 12.確認並匯出安全使用者端設定檔

導航到Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile,按 一下Edit按鈕。

Ele View Iools Wigards Window Help	e 🔇 Refresh 🔇 Back 💭 Forward 🦻 Help			Type topic to search Go	cisco
Device List Boolmarks	Configuration > Remote Access VPN > Network (Client) Acce	ss > Secure Client Profile			
Boolmanis         20         P           To boolmark a page, right-click on a node in the navigation tree and select "Add to boolmarks".         To boolmarks".           Image: Select and the page right-click on a node in the navigation tree and select "Add to boolmarks".         To boolmarks".           Image: Select and the page right-click on a node in the navigation tree and select "Add to boolmarks".         To boolmarks".	point and set with the page, right-click on a node in the navigation and setist. Table to boolmains <sup>2</sup> .       This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add button to add a new profile. Pressing the Import or Export button is for upbad and download of deet profiles between local machine and device.         In and select add to boolenaris <sup>2</sup> .       Delete         Delete       This panel is used to manage Secure Client Profiles and perform group assignment for Secure Client version 2.0 or later. You can select the 'Add button to add a new profile. Pressing the Import or Export button is for upbad and download of deet profile Usage held is httpoduced with the Secure Pholicy Solution. This field contains different profile usage in Secure Client version 3.0 and later.				
Remote Access VPN D: 4	Add G Edit M Change Group Policy Delete M Import	txport 付 Valdate			
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	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml	
Secure Clent Customization/Localization     Secure Clent Profile     Secure Clent Profile     Secure Clent Software					

編輯安全客戶端配置檔案

### 確認設定檔的詳細資訊。

- 顯示名稱(必填): ciscoasa (IPsec) IPv4
- FQDN或IP地址: 192.168.1.1
- 主要協定: IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grp	client_profile				Server	List Entry				×	
Profile: vpn-ipsec-tunne	Profile: vpn-ipsec-tunnel-grp_client_profile						Server Load Balancing Servers SCEP Moble Certificate Priving					
Vite Preferences (Part 1) Preferences (Part 2) References (Part 2)	Server List					Pr. 1	mary Server Xiplay Name (required)	(SCORER (Proc.) Prof.	Connection Information Primary Protocol	к v)		
Cenfricate Priving Cenfricate Matching Cenfricate Envolvent Cenfricate Envolvent Hobie Policy Server List	Hostname Sectors (Short) 2	Host Address	User Group	Backup Server List	SCIP Mobile Se		QDN or IP Address 192:368.1.1 Jone URL	Uter Group	Auth Method During BLE Identity (305 ga	DE Negotiation [	EAP-AnyConnect 🗸	
	moon is a regres		aac one jorver pe	annei n'sprine.	Add	]	Backup 5 Host J	kvæs	Cancel	Add Plave Up Plave Down Delete		

確認安全客戶端配置檔案

# 按一下Export按鈕將配置檔案導出到本地PC。

File View Tools Wizards Window Help				Type topic to search
🛞 Home 🗞 Configuration 🔯 Monitoring 🕁 Sa	we 🔇 Refresh 🔇 Back 🔘 Forward 💈	Help		
Device List Bookmarks	Configuration > Remote Access VPN > Ne	twork (Client) Access > Secure Client Profile		
Bookmarks 🗗 🕂 🗙				
To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks". Go marks Delete	This panel is used to manage Secure Client Pro and download of client profiles between local The profile Usage field is introduced with the S	rfies and perform group assignment for Secure Clent version 2.5 or la nachine and device. ecure Mobility Solution. This field contains different profile usage in S	ter. You can select a profile to edit, change group or to delete. You can scure Client version 3.0 and later.	select the 'Add' button to add a new profile. Pressing the Import or Expo
Remote Access VPN di P	🗣 Add 🛃 Edit 🔀 Change Group Policy	👕 Delete 🐷 Impert 🐻 Export 🔏 Validate		
? Introduction	Draffle Marrie	Braffalleran	Come Below	Braffe Laustian
Secure Clent Connection Profiles	Prome wante	Prome osage	Group Policy	High from been been door wheth model and
Secure Client Customization Provides	vpn-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-psec-tunnel-grp_client_profile.xml
Resources				
Binary				
- Script		Export Secure Client Profile	×	
GUI Text and Messages				
Customized Installer Transforms		This panel is used to export Secure Client profile fro	m device to the local file system	
Localized Installer Transforms				
- If Secure Clent Profile				
Secure Client Software				
Secure Client External Browser		Profile Name: vpn-ipsec-tunnel-grp_client_prof	ile	
Dvnamic Access Policies				
- Group Policies				
IPsec(IKEv1) Connection Profiles		Local Path: C:\Users\j.u L", 2LDr / Cis	colDesktoplvpn-ip: Browse Local	
IPsec(IEV2) Connection Profiles				
- Secure Mobility Solution				
Address Assignment				
Advanced				
Clientless SSL VPN Access		Event Cancel	tiala	
AAA/Local Users		Export Cancer	map	
A Docture (for Secure Frewall)				

導出安全客戶端配置檔案

#### 步驟 13.確認安全客戶端配置檔案的詳細資訊

透過瀏覽器打開Secure Client Profile,確認主機的主要協定是IPsec。

```
\u00ed 
\u00ed <
```

安全客戶端配置檔案的詳細資訊

#### 步驟 14.在ASA CLI中確認設定

在ASA CLI中確認ASDM建立的IPsec設定。

// 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

步驟 15.增加加密演算法

在ASA CLI中,將組19增加到IKEv2策略。



注意:對於IKEv2/IPsec連線,自版本4.9.00086起,Cisco Secure Client不再支援Diffie-Hellman (DH)組2、5、14和24。此更改可能導致由於加密演算法不匹配而導致連線失敗。

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

Windows Server中的配置

您需要為VPN連線增加域使用者。 導覽至Active Directory Users and Computers,然後按一下 Users。將vpnuser新增為網域使用者。

Active Directory Users and Computers						
File Action View Help						
💠 🔶 🙍 📅 🥇 🖬 🗶 🗑 🖉 📷 🖏 🕸	i i i 😗 🧕 🔌					
Active Directory Users and Computers vinserver.ad.rem-s Saved Quenes Saved Quenes Source Sou	lame Administrator Allowed RODC Passwor Cert Publishers Cloneable Domain Con DefaultAccount Denied RODC Passwore DnsAdmins Domain Admins Domain Computers Domain Computers Domain Computers Domain Computers Domain Controllers Domain Ouests Domain Users Enterprise Admins Enterprise Read-only Di Group Policy Creator O & Guest Key Admins MAR User Admins Read-only Domain Con Schema Admins text user yon user	vpn user Properties Member Of Remote control General Address Vpn use Dist name: Last name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Web page:	Disi-in Remote Deskto Account Prof vpni user vpn user	Environment pp Services Profile file Telephones jntials:	? × 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 stors Group o are permitted to perform dynamic updates o ninistrators of the domain trollers in the domain trollers in the domain sts 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 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

新增網域使用者

# 將域使用者增加到域管理員和域使用者的成員。

vpn user Properties			?	$\times$	vpn user Pro	operties				?	$\times$
Remote control Member Of General Address	Remote Dial-In Account	Pesktop Services Profile Environment Profile Telephones	CO Sessio Organi	)M+ ons ization	Remote General Membe	control Address r Of	Remote Account Dial-in	Desktop Se Profile Envi	rvices Profile Telephones ironment	COI Organiz Session	M+ ation
User logon name: Vpnuser User logon name (pre- AD\ Logon Hours	Windows 200	@ad.rem-system.com 0): vpnuser		~	Member of Name Domain Domain	f: Admins Users	Active Direct ad rem-system ad rem-system	ory Domain m.com/Use m.com/Use	n Services Folder ns		
Account gptions:	ge password a ange password expires using reversib	t next logon f		< >	Add Primary gru	. <u>f</u> pup: D	Remove omain Users				_
Account expires Never End of:	Monday .	June 10, 2024		]	<u>S</u> et Prin	nary Group	There is r you have applicatio	no need to ( Macintosh ns.	change Primary clients or POSID	roup unle (-complian	55 t
0	K (	Cancel Apply	Н	lelp		0	K (	Cancel	Apply	He	dp.

# ISE中的配置

### 步驟 1.增加裝置

# 導航到管理>網路裝置,點選增加按鈕,增加ASAv裝置。

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS	Servers RADIU	S Server Sequences
Network Devices Default Device Device Security Settings	Network Device Network Device Name Description	s List > ASAv evices ASAv			
	IP Addres	s v *IP: 1.000,061	/ 32 🚳		
	Device Prof	ile 🏥 Cisco	× ()		
	Model Nam		~		
	Software Ve	rsion	~		
	Network De	vice Group			
	Location	All Locations	~	Set To Default	
	IPSEC	No	~	Set To Default	
	Device Type	All Device Types	~	Set To Default	
	RAI Prot	RADIUS Authentication S DIUS UDP Settings	Settings		
	Sha	red Secret cisco123		Hide	

增加裝置

步驟 2.新增Active Directory

導航到管理>外部身份源> Active Directory,點選連線頁籤,將Active Directory增加到ISE。

- 連線點名稱: AD\_Join\_Point
- Active Directory網域: ad.rem-system.com



新增Active Directory

# 導覽至Groups索引標籤,選取從目錄選取群組從下拉式清單。

	=	dentity Services	Engine Administration / Identity Management
	Ц	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
		Dashboard	
	0	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
	%	Operations	Contribution     P Edit     + Add     Delete Group     Update SID Values
	U	Policy	Select Groups From Directory     Select Groups From Directory     Select Groups From Directory
<b></b> 金曜	20	Administration	AD_Join_Point Ontrol Assist ad.rem-system.com/S-1-5-32-579
組			

按一下「擷取群組」下拉式清單。Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain Userand clickOK。

≡		Engine					×	4
н	Bookmarks	Identities Groups E	Sel	ect Directory Groups				
53	Dashboard	Ceroncate AD     Cative Directo	This di	alog is used to select groups from the Direct	ory.			
넝	Context Visibility	AD_Join_Poin	N	lame SID	Type ALL			
×	Operations	C LDAP		Peter Peter	ricer			
0	Policy			Hedrove Groups] a Groups Retrieve	2.			
20	Administration	RSA SecuriD		Name ^	Group SID	Group Type		
-	Work Centers	SAML Id Provide	0	ad.rem-system.com/Users/DnsAdmins	5-1-5-21-4190742415-4130520026-20462399	DOMAIN LOCAL	^	
		🖿 Social Login	-	ad.rem-system.com/Users/DosUpdateProxy	5-1-5-21-4193/42415-4133520026-20462399	CLOBAL CLOBAL		
	Interactive Help			ad.rem-system.com/Users/Domain Computers	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ad.rem-system.com/Users/Domain Controllers	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ad.rem-system.com/Users/Domain Guests	5+1+5+21+4190742415+4130520026+20462099	GLOBAL		
				ad.rem-system.com/Users/Domain Users	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ed.rem-system.com/Users/Enterprise Admins	5+1+5+21+4190742415+4133520026+20462399	UNIVERSAL	1	
				ad.rem-system.com/Users/Enterprise Key Admins	5-1-5-21-4190742415-4130520026-20462399	UNIVERSAL		
			0	ad.rem-system.com/Users/Enterprise Read-only.	5+1+5+21+4193742415+4133520026+20462399	UNIVERSAL		
			0	ad.rem-system.com/Users/Group Policy Creator .	. 5-1-5-21-4190742415-4133520026-20462399	GLOBAL	-	
			<				•	
						Cancel	ок	
						L		

增加域電腦和使用者

#### 步驟 3.增加身份源隔離

導航到管理>身份源序列,增加身份源序列。

• 名稱: Identity\_AD

### • 身份驗證搜尋清單: AD\_Join\_Point

=	dentity Services	Engine		Administration / Id	lentity Management
Л	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
51	Dashboard	Identity Source Sequence	s List > Identity_AD		
명	Context Visibility	Identity Source Se	equence		
×	Operations	Lidentitu Course	Coguanaa		
-0	Policy	* Name	testile AD		
80	Administration	Description	eenery_vel		
d.	Work Centers				
٢	Interactive Help	<ul> <li>Certificate Ba</li> <li>Select Certific</li> <li>Authentication</li> <li>A set of idem</li> </ul>	sed Authentication are Authentication Profile n Search List tity sources that will be accessed	in sequence until first authentication se	ucceeds
		Available		Selected	
		Internal E Internal U Guest Use All_AD_J,	ndpoints  sers ers oin_Points	AD_Join_Point	-1
				Ĕ	
			>>> >>>	8	
增加	身份源序列				

### 步驟 4.增加策略集

導航到策略>策略集,點選+增加策略集。

- 策略集名稱: VPN\_Test
- 條件:裝置裝置型別等於所有裝置型別
- 允許的協定/伺服器序列:預設網路訪問

≡	dentity Services Eng	ine Policy / Policy Sets	🔺 Evaluation Mode = Cays Q 🛕 🎯 📮   ႙
Щ	Bookmarks	Policy Sets	Reset Policyset Hitcounts Save
	Dashboard	🕒 Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hits Actions View
10	Context Visibility	Q Search	
×	Operations	VPN Test     DEVICE-Device Type EQUALS A	Default Network Access     A + 30     A
0	Policy	Device Types	
增加	策略集		

#### 步驟 5.增加身份驗證策略

導航到策略集,點選VPN\_Test增加身份驗證策略。

• 規則名稱: VPN\_Authentication

- 條件:網路訪問裝置IP地址等於1.x.x.61
- 使用:Identity\_AD

```
✓Authentication Policy(2)
```

+ Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
VPN_Authentication	Network Access-Device IP Address EQUALS 1.1771.1.61	Identity_AD //	10	ŝ
增加身份驗證策略				

#### 步驟 6.增加授權策略

#### 導航到策略集,點選VPN\_Test增加授權策略。

- 規則名稱: VPN\_Authorization
- 條件:Network\_Access\_Authentication\_Passed
- 結果: PermitAccess

✓Authorization Policy(2)					
		Results			
+ Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
VPN_Authorization [	Network_Access_Authentication_Passed	PermitAccess	Select from list	10	ŝ
曾加授權策略					

# 驗證

# 步驟 1.將安全客戶端配置檔案複製到Win10 PC1

將安全客戶端配置檔案複製到C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile目錄。

← → • ↑ 📙	> This PC > Local Disk (C:) > ProgramData > Cisco	> Cisco Secure Client	t > VPN > Profile >
1 Ouistansee	Name	Date modified	Туре
P Quick access	MgmtTun	5.117/2024 8:42 AM	File folder
Desktop	vpn-ipsec-tunnel-grp_client_profile	5,173/2024 12:48 AM	XML Document
- Downloads	AnyConnectProfile.xsd	'1./2024 1:12 PM	XSD File

將設定檔複製到PC

# 步驟 2.啟動VPN連線

在終端上,運行Cisco Secure Client並輸入使用者名稱和密碼,然後確認Cisco Secure Client連線成

功。

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

連線成功

### 步驟 3.確認ASA上的系統日誌

在系統日誌中,確認IKEv2連線成功。

#### <#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

### 步驟 4.確認ASA上的IPsec會話

運行show vpn-sessiondb detail anyconnect命令以確認ASA上的IKEv2/IPsec會話。

#### <#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

步驟 5.確認Radius即時日誌

在ISE GUI中導航到操作> RADIUS >即時日誌,確認vpn身份驗證的即時日誌。

≡	dentity Services E	Engine			Operations / RADIU	JS			A trans	rlion Mode 💶 Days	۵ ۵	© 0	18
н	Bookmarks	Live Logs Live Sessions											
	Dashboard												
N	Context Visibility	Misconfigured Supplicants		Misconfigured Network Devic	es 📀	RADIUS Drops		<b>Client Stopped Res</b>	ponding 🕕			lepeat Cour	ster 📀
*	Operations	0		0		0		0				0	
Ð	Policy								Refresh	Show	W	intin	
8.	Administration								Never	V Latest 20 re	cords 🗸 L	ast 3 hours	×
đ	Work Centers	C for Reset Repeat Counts	🕁 Екроп То 🗸									Filter 🗸	0
		Time	Status Details	Repeat Endpoint Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Port	Identit	y Grou
٢	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. vpruser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess					
		May 28, 2024 05:13:42	a a	00:50:5 vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Worksta	rtion

Radius即時日誌

#### 按一下[狀態]以確認即時記錄檔的詳細資訊。

Cisco ISE				
		L. L		
Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
Username	vpnuser	11001	Received RADIUS Access-Request	
	(pridda)	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
Authentication Policy	VPN_Test >> VPN_Authentication	15048	Queried PIP - DEVICE.Device Type	6
		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 authoritication 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 - vonuser	0
Store	Ab_oon_ronk	24211	Found Endpoint in Internal Endpoints IDStore	9
Identity Group	Workstation	15048	Oueried PIP - Network Access AuthenticationStatus	2
Audit Session Id	01aa003d0001700066559220	15016	Selected Authorization Profile - PermitAccess	7
		22081	Max sessions policy passed	6
Authentication Method	PAP_ASCII	22080	New accounting session created in Session cache	0
Authentication Protocol	PAP_ASCII	11002	Returned RADIUS Access-Accept	2
Network Device	ASAv			

即時日誌的詳細資訊

#### 疑難排解

密碼編譯演演算法不相符可能會導致連線失敗。這是發生演演算法不相符問題的範例。在ASDM中執行Configuration部分的第15步可 解決此問題。

步驟 1.啟動VPN連線

在終端上,運行Cisco Secure Client並確認由於加密演算法不匹配導致連線失敗。

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

() Cisco Secure Client	-		×	Cisco Secure Client	×
AnyConnect VPII: Ready to connect. ciscoasa (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.	
				ОК	

連線失敗

#### 步驟 2.在CLI中確認系統日誌

在系統日誌中,確認IKEv2協商失敗。

#### <#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

#### 參考

透過IKEv2到具有AAA和證書身份驗證的ASA的AnyConnect

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。