# 在具有AAA &;证书身份验证的ASDM中配置安 全客户端IKEv2/ASA

目录
<u>简介</u>
<u>先决条件</u>
要求
——— 使用的组件
ASDM中的配置 ASDM中的配置
<u>弗二罗:VPN协议</u> 签四些,安白 <del>泄</del> 师渔
<u>弗巴沙,各广场峡</u> 像 第五步,身份验证方法
第五 <u>ジ・月田</u> 金田力広 第六 <u>坊・</u> SAMI 配置
步骤 7.客户端地址分配
<del></del>
步骤 9NAT免除
步骤 10安全客户端部署
<u>步骤 11保存设置</u>
步骤 12确认并导出安全客户端配置文件
步骤 13确认安全客户端配置文件的详细信息
步骤 14确认ASA CLI中的设置
<u>步骤 15添加加密算法</u>
<u>Windows Server中的配置</u>
ISE中的配置
<u>步骤1:添加设备</u>
<u>第二步:添加Active Directory</u>
<u>第三步:添加身份源隔离</u>
<u>第四步:添加策略集</u>
<u>第五步:添加身份验证策略</u> ————————————————————————————————————
<u>第六步:添加授权策略</u>
<u>验证</u>
步骤1:将安全客户端配置文件复制到Win10 PC1
<u>第二步:启动VPN连接</u>
<u>第三步:确认ASA上的系统日志</u>
<u>第四步:确认ASA上的IPsec会话</u>
<u>第五步:确认Radius实时日志</u>
<u>故障排除</u>
步骤1:启动VPN连接
<u>第二步:在CLI中确认系统日志</u>

#### <u>参考</u>

## 简介

本文档介绍在ASA上使用带AAA和证书身份验证的ASDM配置IKEv2上的安全客户端所需的步骤。

## 先决条件

## 要求

Cisco 建议您了解以下主题:

- 思科身份服务引擎(ISE)的配置
- 思科自适应安全虚拟设备(ASAv)的配置
- 思科自适应安全设备管理器(ASDM)的配置
- VPN身份验证流程

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 身份服务引擎虚拟3.3补丁1
- 自适应安全虚拟设备9.20(2)21
- 自适应安全设备管理器7.20(2)
- 思科安全客户端5.1.3.62
- Windows Server 2016
- Windows 10

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

## 网络图

下图显示本文档示例中使用的拓扑。

在Windows Server 2016上配置的域名是ad.rem-system.com,本文档中将其用作示例。



#### 网络图

## 配置

## ASDM中的配置

#### 步骤1:打开VPN向导

### 导航到Wizards > VPN Wizards,单击Secure Client VPN Wizard。



### 单击 Next。



单击"下一步"按钮

第二步:连接配置文件标识

输入连接配置文件的信息。 连接配置文件名称:vpn-ipsec-tunnel-grp VPN访问接口: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 Identification	connectors.	
3. VPN Protocols	Connection Profile Name: vpn-ipsec-tunnel-grp	
4. Client Images	VPN Access Interface: outside	
5. Authentication Methods		
6. SAML Contiguration 7. Client Address Assimme		
8. Network Name Resolutio Servers		
9. NAT Exempt		
10. Secure Client Deployme		
11. Summary		
	< gack Next > It if Help	

连接配置文件标识

## 第三步:VPN协议

## 选择IPsec,单击Add按钮以添加新的自签名证书。

Conne Client VPN Conne	ection Setup Wizard X	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

## 输入自签名证书的信息。

## 信任点名称:vpn-ipsec-trustpoint

## 密钥对:ipsec-kp

Ta Add Identity Certificate X	Ta Add Key Pair ×
Trustpoint Name: vpn-ipsec-trustpoint	Key Type: ORSA OECDSA OEDDSA
Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):	
Decryption Passphrase:	Name: Use default key pair name
File to Import From: Browse	O Enter new key pair name: lpsec-kp
Add a new identity certificate:	Size: 4096 V
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	

自签名证书的详细信息

## 确认VPN协议的设置,单击Next按钮。

Secure Client VPN Conne	ction Setup Wizard	$\times$
Secure Client VPN Connel Steps	VPN Protocols Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols y 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/INEv2) require that valid device certificate be available on the ASA.	× ou
9. NAT Exempt 10. Secure Client Deployme 11. Summary	Device Certificate:       vpn-ipsec-trustpoint:unstructuredNam       Manage         Kack       Manage       Manage	

## 单击Add按钮添加安全客户端映像,然后单击Next按钮。

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 A regular expression can be used to match the user-agent of a brow You can also minimize connection setup time by moving the image up the top of the list.	e client device when it accesses the enterprise network. wser to an image. Just 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         You can download Secure Client packages from Cisco by searching	Regular expression to match user-agent
	< gack Next >	likin Help

客户端映像

第五步:身份验证方法

单击New按钮添加新的AAA服务器,单击Next按钮。

服务器组名称:radius-grp

身份验证协议:RADIUS

服务器IP地址:1.x.x.191

接口:内部

Secure Client VPN Conn	ection Setup Witand	×	To New Authentication Server Group	×	×	Secure Client VPN Conn	ection Setup Wizard	×
Page 1. Strikkolov 2. Corvection Prikle Schröckolov 3. Strikholski 4. Gelt Sanger Petitekolov 6. SARL Configuration 7. Gelt Addense Alexynete Schröder Same Projektion 5. Natt Compt 10. Secure Clief Deployme 11. Samary	Authoritorean Helinka Helin oping king using each for handmir of the authoritis data serves are regioned. AAA Serve Grage: [ICA]		Create a new authentication server group containing one authent To add more servers to the group or dhange other AAA server Configuration - Device Managemet > Users(AAA > AAA Server Server Group Name: Authentication Protocol: Server IP Address: Interface: Interface:	kation server. tings, go to Groups.		Steps 1. Drobaction 2. Connection Wells <u>Methods</u> 3. With Hotosh 3. With Hotosh 3. With Hotosh 4. Gatel Jongsa 5. Mathematication <b>Methods</b> 6. Stable Configuration 7. Gatel Address Anapyres 8. Natures Hamel 10. Secure Cleve Deployme 11. Summary	Authentication Hellocki The step by support Phase* Judica is used a new prove use on this hell hellocking of the supervergence. AAA Server Grapp Stable AAA Server Grapp Stable AAA Server Grapp Stable AAA Server Grapp Stable Server Saver S PA Server Star Server Servergence Server Saver S PA Servergence Servergence Server Saver S PA Servergence Servergence Servergence S PA Servergence Servergence Servergence Servergence S PA Servergence Servergence Servergence S PA Servergence Servergence Servergence S Servergence Servergenc	
	<pre> (px bet&gt; 0.0 )</pre>	10	Server Secret Key:				 (put>) 001 Hel	
			Confirm Server Secret Key: OK Cancel Help	1				

## 第六步:SAML配置

## 单击Next按钮。

Secure Client VPN Conne	ection Setup Wizard	×
Steps	SAML Configuration	
<ol> <li>Introduction</li> <li>Connection Profile Identification</li> <li>VPN Protocols</li> <li>Client Images</li> <li>Authentication Methods</li> <li>SAML Configuration</li> <li>Client Address Assignme</li> <li>Network Name Resolutio Servers</li> <li>NAT Exempt</li> <li>Secure Client Deployme</li> <li>Summary</li> </ol>	This step allows you to configure a SAML and the authentication method. Authentication Method: AAA AAA Server Group: radius-grp  Use LOCAL if Server Group fails SAML Identity Provider SAML Server : None Manage	
	< Back Next > Rifl	Help

SAML配置

步骤 7.客户端地址分配

单击New按钮以添加新的IPv4池,然后单击Next按钮。

名称:vpn-ipsec-pool

- 起始IP地址:172.16.1.20
- 结束IP地址:172.16.1.30
- 子网掩码: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:	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  V	× ndl
	< Back Next >	Rcii) Help		<gadk next=""> Riff Heb</gadk>	2

客户端地址分配

## 步骤 8网络名称解析服务器

## 输入DNS和域的信息,单击Next按钮。

### DNS服务器:1.x.x.57

## 域名:ad.rem-system.com

Secure Client VPN Conn	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

网络名称解析服务器

步骤 9NAT免除

单击Next按钮。

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

NAT免除

## 步骤 10安全客户端部署

## 选择允许Web启动,然后单击"下一步"按钮。

Secure Client VPN Conne	ection 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	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 FIR 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	
	< Back Next > It if Help

#### 步骤 11保存设置

### 单击Finish按钮并保存设置。

Can Secure Client VPN Connection Setup Wizard	X 🔯 Warning X
VPN Wizard         Summary           Grandhin         Here is the summary of the configuration.	ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning
Name     Value       Summary     Nume/Alas of the Connection Profile     ypn-ipsec-tunnel-gp       VMA Access Interface     outside       Device Digital Certificate     ypn-ipsec-trustpoint:unstructuredName=ciscoasa, CN       VMP Notocols Enabled     DPisec only       Secure Clear Images     1 package       Authentication Server Group     radus-gp       SAML     Authentication Method: asa       Address Pool for the Cleart     172.16.1.20       DNS     Domain Name:       Network Address Translation     The publicited of affic can be subjected to network address       Verwick Address Translation     The publicited of affic can be subjected to network address	[Ok] bit all point projection rules in the transmission of the second

保存设置

步骤 12确认并导出安全客户端配置文件

导航到Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profile,单击Edit按钮。

File View Iools Wigards Window Help	e 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help			Type topic to search Go	cisco				
Device List Bookmarks	Configuration > Remote Access VPN > Network (Clie	nt) Access > Secure Client Profile							
Boolmarks         dP Q ×           To boolmark a page, right-click on a node in the navigation tree and select. "Add to boolmarks".           ● Go III Delete	warks       20       0       X         immark appr, right-clack on a node in the navigation of select. "Add to boolewarks".       This panel is used to manage Secure Clerk Profiles and perform group assignment for Secure Clerk 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 upload and download of clerk profiles between local machine and device.         The profile Usage Field is introduced with the Secure Mobility Solution. This field contains different profile usage in Secure Clerk version 3.0 and later.								
Remote Access VPN 🗗 🖗	🗣 Adc 🖪 Edit 🔀 Change Group Policy 👔 Delete 🚦	🛃 Import 🖏 Export 🚳 Validate							
Introduction     Introduction     Introduction     Introduction	Profile Name	Profile Usage	Group Policy	Profile Location					
Secure Clent Connection Profiles     Secure Clent Customication(Localization     Secure Clent Notice     Secure Clent Software	von-ipsec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-lpsec-turinel-grp	disk0;/vpn-basec-tunnel-grp_client_profile.vml					

编辑安全客户端配置文件

## 确认配置文件的详细信息。

- •显示名称(必填): ciscoasa (IPsec) IPv4
- FQDN或IP地址:192.168.1.1
- 主协议:IPsec

Secure Client Profile Editor - v	Secure Client Profile Editor - spin-psec-tunnel-grp_client_profile											×	
Profile: vpn-ipsec-tunne	l-grp_client_pr	ofile					Server Load Balancing Servers SCIP Hoble Certificate Pinning						
Preferences (Part 1) Preferences (Part 2) References (Part 2)	Server List						Primary Server Display Name (required) Occuses (Proc) Pv4			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	Backup Server List	SCIP Mobil	Setting	Poper P Add 190,044 P Add 190,046 L1	Backup Servers		Auth Hethod D	uring B/E Registration 05 gateway only) Add Move Up Move Up Move Down Delete	[AP-AryCorrect ->	
									OK .	Carcel			

确认安全客户端配置文件

## 单击Export按钮将配置文件导出到本地PC。

	File View Tools Wizards Window Help				Type topic to search
Cardware Access VPX ->https://conder.com/com/com/com/com/com/com/com/com/com/	🚳 Home 🚳 Configuration 🔯 Monitoring 🔚 Sav	re 🔇 Refresh 🔇 Back 🔘 Forward 🢡	Help		
Decimate       O       E         Toolomska population       Pit-do       Add Columba population       Financial Sector Control Into analysis         Toolomska population       Pit-do       Toolomska population       Financial Sector Control Into analysis       Toolomska population       Financial Sector Control Into and Cont	Device List Bookmarks	Configuration > Remote Access VPN > Net	work (Client) Access > Secure Client Profile		
To bolomata's appe, right-did to oan node in the nangdol the manage Secure Chert Profiles and perform group assignment for Secure Clert version 2.5 or later. You can select a profile to edd, change group or to deleter. You can select the "Add button to add a new profile. Pressing the laport or Export and obstring add chert profiles boloweasi's.	Bookmarks d <sup>a</sup> Q ×				
Remote Access VM Cl Q     In troduction     In troduction     Score Clerk Connection Profes     Score Clerk Score Profes     Score Score Profes     Score Score Profes     Score Profes     Score Profes     Score Score Profes     Score Profes <td< td=""><td>To bookmark a page, right-click on a node in the navigation tree and select "Add to bookmarks".</td><td>This panel is used to manage Secure Client Prof and download of client profiles between local m The profile Usage field is introduced with the Se</td><td>les and perform group assignment for Secure Client version 2.5 or later.Yo schine and device. cure Mobility Solution. This field contains different profile usage in Secure (</td><td>u can select a profile to edit, change group or to delete. You can selec Bent version 3.0 and later.</td><td>t the 'Add' button to add a new profile. Pressing the Import or Expo</td></td<>	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 Prof and download of client profiles between local m The profile Usage field is introduced with the Se	les and perform group assignment for Secure Client version 2.5 or later.Yo schine and device. cure Mobility Solution. This field contains different profile usage in Secure (	u can select a profile to edit, change group or to delete. You can selec Bent version 3.0 and later.	t the 'Add' button to add a new profile. Pressing the Import or Expo
Profile Name       Profile Usage       Group Polcy       Profile Location         Store Clerk Currentsion Profiles       Socie Clerk Currentsion Profiles       Socie Clerk Currentsion Profile       X         Socie Clerk Currentsion Profiles       X       This panel is used to export Secure Client Profile       X         Socie Clerk Schwae       Currentsion Profiles       X       This panel is used to export Secure Client Profile       X         Socie Clerk Schwae       Socie Client Profile       X         Socie Clerk Schwae       Socie Clerk Sch	Remote Access VPN	🗣 Add 📝 Edit 🔛 Change Group Policy 🥤	Delete 🛃 Impart 🚳 Export 🗿 Validate		
<ul> <li>Prote Nation</li> <li>Chard Nation</li> <li>Secure Clerk Contention Profes</li> <li>Contention Profes</li> <li>Contention Profes</li> <li>Contention Profes</li> <li>Secure Clerk Contention Profes</li> <li>Contention Profes</li> <li>Secure Clerk Contention Profes</li> <li>Secure Clerk Contention Profes</li> <li>Secure Clerk Contention Profes</li> <li>Secure Clerk Contention Profes</li> <li>Secure Clerk Software</li> <li>Profe Name:</li> <li>Secure Clerk Software</li> <li>Secure Clerk Software</li></ul>	-? Introduction	Profile Name	Drofile Linean	Group Policy	Decide Location
Source Cent Cutomic Contract Profile     Source Cent Cutomic Contract Profile     Source Cent Cutomic Contract Profile     Source Cent Software     Source Cent Softwa	Service Cleant Connection Profiler	Provide Harris	In Company 1991 Due Sta	Council and the second se	del Charachera hand an dest auffe and
Image: Secure Client Profile         Societ Secure Client Profile         Societ Client And Messages         Contacted Installer Transforms         Societ Client Andler Transforms         Societ Client Stroking         Dispect Stroking         Dispect Stroking         Societ Client Stroking         Dispect Stroking	Secure Client Customization Profiles	vpn-psec-tunnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_vpn-ipsec-tunnel-grp	disk0:/vpn-ipsec-tunnel-grp_client_profile.xml
Stope     S	Resources				
Source	Boary				
GUI Text and Messages       Customized installer transforms         Customized Installer transforms       Customized Installer transforms         Secure Clerk Software       Profile Name: vpr-psec-tunnel-gp_clerk_profile         Secure Clerk Software       Profile Name: vpr-psec-tunnel-gp_clerk_profile         Description       Description         Description       Profile Name: vpr-psec-tunnel-gp_clerk_profile         Description       Description       Description         Description       Description       Description         Description       Description       Description         Description       Description       Description         Description       Description       Description </td <td>String String</td> <td></td> <td>Export Secure Client Profile</td> <td>×</td> <td></td>	String String		Export Secure Client Profile	×	
Controlled Installer Transforms Controlled Installer Controlled C	GIII Text and Messager				
Localed Instaler Tranforms     Localed Instaler Tranforms     Succe Card Databet Tranforms     Profile Name: vpn-ipsec-turnel-gp_clert_profile     Succe Card Databet Tranforms     Profile Name: vpn-ipsec-turnel-gp_clert_profile     Succe Card Databet Tranforms     Profile Name: vpn-ipsec-turnel-gp_clert_profile     Desc(ExV) Connection Profiles     Succe Card Databet Tranforms     Profile Name: vpn-ipsec-turnel-gp_clert_profile     Desc(ExV) Connection Profiles     Succe Card Databet Tranforms     Profile Name: vpn-ipsec-turnel-gp_clert_profile     Desc(ExV) Connection Profiles     Succe Card Databet Tranforms     Desc(ExV) Connection Profiles     Succe Card Databet Tranforms     Desc(ExV) Connection Profiles	Customized Installer Transforms		This namel is used to export Secure Client profile from devi	ra to the local file system	
Concern and the second of the and the second of the and the second of the second of the and the second of the	to a sheet that the Transforms		The particle about to expert secure cash, prome from dem		
Stouce Clerk Software     Profile Name:     vpn-psec-turnel-gp_clerk_profile       Stouce Clerk Software     Profile Name:     vpn-psec-turnel-gp_clerk_profile       Stouce Clerk Software     Discretion Profiles     Local Path:       Discretic Profile Name:     Vpn-psec-turnel-gp_clerk_profile       Discretic Profile Name:     Vpn-psec-turnel-gp_clerk_profile       Discretic Profile Name:     Local Path:     C:[Uters[j_i_i_],",",Dr v Cisco]Desktop vpn-p       Response Local     Discretion Profiles       Discretic Profile     Export     Cancel       Help     Advanced	Cocated Distaler mansforms				
Stude Units Sortical Browser     Socie Cent External Browser     Dynamic Access Policies     Dynamic Access Policies     Direc(1)E/v1 Connection Policies	The Second Clerk Fellowing				
Source Cleric Extends Browser     Source Cleric Extends     Browser Local     Source Cleric Extends     Source Cleric Extends     Browser Local     Source Cleric Extends     Browser Local     Source Cleric Extends	Secure Client Software		Profile Name: unp-insec-tunnel-orp client profile		
Contract Access Storess     Contraction Profiles     Prec(1)Exv1 Connection Profiles     Profile     Prec(1)Exv1 Connection Profiles     Profile	Secure Client External Browser		The second		
Good Pathers     Good Pathers     Good Pathers     Good Pathers     Good Pathers     Cool (Users) Good Cool (Users)	Dynamic Access Policies				
Pisc(12-V) Connection Profess     Pisc(12-V) Connection Profess     Pisc(12-V) Connection Profess     Social Mobility Solution     Advanced     Advanced     Advanced     Concell Help     Cancell Help	Group Policies		Local Path: C:\Users\iu_L_"OrDr u - Cisco\Des	itop\vpn-ipr Browse Local	
Byse(1E-V2) Connection Profiles     Source class Profiles     Source class Profiles     Source class Profile     Book Address     Export     Cancel Help     Cancel Help	Psec(IKEV1) Connection Promes				
By Advanced       By Advanced       By Advanced       Concellent       Concellent       Concellent	IPsec(IKEv2) Connection Profiles				
Big Address Assignment       Big Address Assignment       Big Address SQ, WHA Access       Big Address SQ, WHA Access SQ, WHA Access       Big Address SQ, WHA Access       Big Address SQ, WHA Access       Big Address SQ, WHA Access SQ, WHA Access SQ, WHA Access       Big Address SQ, WHA Access	- Secure Mobility Solution				
Big Advanced     Genetics SUMMAccess     Dig Contents SUMMAccess     Dig Contents SUMMAccess     Dig Contents Summaria     Cancel Help	Address Assignment				
Barge Carries SS, WM Access     Burge Carries SS, WM Access     Burge Carries State State State     Cancel Help	H to Advanced				
B and Adalacial Users	Clientless SSL VPN Access		Export Cancel	Help	
An Dechara Freedail	AAA/Local Users				
	Ph Doch ine (For Service Firewall)				

导出安全客户端配置文件

#### 步骤 13确认安全客户端配置文件的详细信息

通过浏览器打开"安全客户端配置文件",确认主机的主要协议为IPsec。

```
\u00ed 
AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/">

\u00ed 
\u00ed </p
```

安全客户端配置文件的详细信息

#### 步骤 14确认ASA CLI中的设置

确认ASDM在ASA CLI中创建的IPsec设置。

// 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

步骤 15添加加密算法

在ASA CLI中,将组19添加到IKEv2 Policy。



注意:对于IKEv2/IPsec连接,自版本4.9.00086起,思科安全客户端不再支持Diffie-Hellman (DH)组2、5、14和24。此更改可能会导致由于加密算法不匹配而导致连接失败。

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

Windows Server中的配置

您需要为VPN连接添加域用户。 导航到Active Directory用户和计算机,然后单击用户。将 vpnuser添加为域用户。

Active Directory Users and Computers						
File Action View Help						
💠 🔶 📶 🤾 🖬 🗙 🖾 🔒 📓 📷 😤 👟	গ্রি 🍸 🗾 🔽					
Active Directory Users and Computers I vinserver.ad.rem-r Active Directory Users and Computers I vinserver.ad.rem-r ad.rem-system.com Domain Controllers ForeignSecurityPrincipals Mananel Service Accounts Users Salar Sa	Administrator Administrator Allowed RODC Password Cert Publishers Cloneable Domain Con DefaultAccount Denied RODC Password OnsUpdateProxy Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Admins Enterprise Read-only Du Group Policy Creator O Guest Key Admins MAR User Inde_user Protected Users RAS and IAS Servers Read-only Domain Con Schema Admins test user	Vpn user Properties Member Of Remote control General Address Vpn use Brit name: Last name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Digplay name: Web page:	Dial-in Remote De Account	Environment sktop Services Profile Profile Telephone intels:	? X Sessions COM+ is Cryanization	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 ntors Group o are permitted to perform dynamic updates o ninistrators of the domain trollers in 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 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

添加域用户

## 将域用户添加到域管理员和域用户的成员。

vpn user Properties				?	×	vpn user Pr	operties				?	$\times$
Remote control	Remote I	Desktop Servic	es Profile	CO	M+	Remote	control	Remote	Desktop Se	ervices Profile	CO	M+
Member Of	Dial-in	Environ	ment	Sessio	ons	General	Address	Account	Profile	Telephones	Organia	tation
General Address	Account	Profile T	elephones	Organi	ization	Membe	r Of	Dial-in	Env	vironment	Sessio	ns
User logon name:						Member of	f:					
vpnuser		@ad.rem-sy	ystem.com		$\sim$	Name		Active Direct	tory Domair	n Services Folder		٦.
User logon name (pre-	Windows 200	0):				Domain	Admins	ad.rem-syste	m.com/Use	ers		
AD\		vpnuser				Domain	Users	ad.rem-syste	m.com/Use	ers		
Account gotions:	ge password a ange passwor expires using reversib	st next logon d le encryption			< ×	Add. Primary gr	I oup: D	Remove		change Primany		
Ne <u>v</u> er <u>End of:</u>	Monday ,	June 10,3	2024		]	<u>S</u> et Pri	mary Group	you have applicatio	Macintosh ms.	clients or POSI	(-complian	t
0	K (	Cancel	Apply	Н	lelp		0	K	Cancel	Apply	He	elp

域管理员和域用户

## ISE中的配置

### 步骤1:添加设备

## 导航到管理>网络设备,点击添加按钮以添加ASAv设备。

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS S	Servers RADIUS Ser	ver Sequences
Network Devices Default Device Device Security Settings	Network Device Network D Name Description	s List > ASAv evices ASAv			
	IP Addres	s ~ <sup>11P</sup> : 1.070.061	/ 32 🚳		
	Device Prof Model Nam Software Ve Network De	e Cisco	~ 0 ~ ~		
	Location	All Locations	~	Set To Default	
	IPSEC	No	~	Set To Default	
	Device Type	All Device Types	~	Set To Default	
	RAI Pro Sha	RADIUS Authentication S DIUS UDP Settings tocol RADIUS red Secret cisco123	Settings	Hide	

添加设备

第二步:添加Active Directory

导航到管理>外部身份源> Active Directory,点击连接选项卡,将Active Directory添加到ISE。

- 加入点名称: AD\_Join\_Point
- Active Directory域: ad.rem-system.com



添加Active Directory

## 导航到组选项卡,选择从目录选择组从下拉列表。

$\equiv \frac{-1}{cosce}$ Identity Services	Engine Administration / Identity Management
I Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
E Dashboard	
14 Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
ℜ Operations	Cartificate Authoritiest     // Edit + Add -      Delete Group Update SID Values
Dolicy	C Centrado Adominicatura     Select Groups From Directory     Select Groups From Directory     Select Groups From Directory
1 Administration	AD_Join_Point Control Assist ad.rem-system.com/5-1-5-32-579

从目录选择组

单击Retrieve Groupsfrom下拉列表。Checkad.rem-system.com/Users/Domain Computersandad.rem-system.com/Users/Domain 用户并单击OK。

≡	dentity Services	Engine						×	A toba
		Identities Groups F	Sel	ect Directory Groups	S				
14	Bookmarks	Ceronicate AD	This di	alog is used to select groups from the Di	irectory.				
22	Dashboard	Active Directo	Dor	main ad.rem-system.com					
성	Context Visibility	AD_Join_Poin	N	lame . 5 Filter Fil	SID . Iter	Type ALL Filter			
×	Operations	D LDAP		Retrieve Groups 9 Groups Retr	ieved.				
0	Policy								
10	Administration	RSA SecuriD		Name	~ 6	iroup SID	Group Type		
, fil	Work Centers	SAML Id Provide	0	ad.rem-system.com/Users/DnsAdmins	2	-1-5-21-4193742415-4133520026-20462399	DOMAIN LOCAL	1	
		🖾 Social Login	0	ad rem-system com/Users/Domoio Admine		-1-5-21-4103742415-413352028-20482399	CLOBAL		
	Interactive Help			ad.rem-system.com/Users/Domain Compute	a 5	-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			0	ad.rem+system.com/Users/Domain Controlle	n s	+1+5+21+4190742415+4130520026+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	s	-1-5-21-4193742415-4133520026-20462399	GLOBAL		
				ad.rem-system.com/Users/Enterprise Admin	a 5	+1+5+21+4193742415+4133520026+20462399	UNIVERSAL	1	
				ad.rem-system.com/Users/Enterprise Key Ad	pnins S	-1-5-21-4193742415-4133520026-20462399	UNIVERSAL		
				ad.rem+system.com/Users/Enterprise Read+	only S	+1+5+21+4190742415+4130520026+20462399	UNIVERSAL		
				ad.rem+system.com/Users/Group Policy Crea	etor S	+1+5+21+4193742415+4133520026+20462399	GLOBAL		
			4				,	•	
							Cancel	ox	

添加域计算机和用户

### 第三步:添加身份源隔离

导航到管理>身份源序列,添加身份源序列。

• 名称 : Identity\_AD

## • 身份验证搜索列表:AD\_Join\_Point

≡	dentity Services I	ingine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
51	Dashboard	Identity Source Sequences List > Identity_AD
뱅	Context Visibility	Identity Source Sequence
×	Operations	V Identini Course Conuenee
-0	Policy	* Name
80	Administration	identity_AL]
di.	Work Centers	Lescription
9	Interactive Help	Certificate Based Authentication     Select Certificate Authentication Profile     Y     Authentication Search List     A set of identity sources that will be accessed in sequence until first authentication succeeds
		Available Selected
		Internal Endpoints ^ AD_Join_Point ^
		Internal Users
		All_AD_Join_Points
添加	身份源序列	

### 第四步:添加策略集

导航到策略>策略集,点击+添加策略集。

- 策略集名称: VPN\_Test
- 条件:设备设备类型等于所有设备类型
- 允许的协议/服务器序列:默认网络访问

=	المانية، Identity Services Engine			Policy / Policy	Sets	🔺 Evaluation Mode = Days Q 🎄 🕐 📮   S	R	
н	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 All	Default Network Access 2 + 30 273	
U	Policy					Device Types	121	
添加	策略集							

### 第五步:添加身份验证策略

导航到策略集,点击VPN\_Test添加身份验证策略。

• 规则名称: VPN\_Authentication

- 条件:网络接入设备IP地址等于1.x.x.61
- 使用:Identity\_AD

```
✓Authentication Policy(2)
```

+ Status Rule Name	Conditions	Use	Hits	Actions
Q Search				
_		Identity_AD		- 0-
VPN_Authentication	Network Access-Device IP Address EQUALS 1.000000161	> Options	10	٢ <u>٢</u>

添加身份验证策略

### 第六步:添加授权策略

导航到策略集,点击VPN\_Test添加授权策略。

- 规则名称: VPN\_Authorization
- 条件:Network\_Access\_Authentication\_Passed
- 结果: PermitAccess

✓Authorization Policy(2)	)							
			Results					
+ Status Rule N	lame	Conditions	Profiles		Security Groups		Hits	Actions
Q Search								
VPN_Au	thorization	Network_Access_Authentication_Passed	PermitAccess	0 +	Select from list	0 +	10	ŝ
添加授权策略								

## 验证

## 步骤1:将安全客户端配置文件复制到Win10 PC1

将安全客户端配置文件复制到C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile目录。

← → × ↑ 📙	> This PC > Local Disk (C:) > ProgramData > Cisco	<ul> <li>Cisco Secure Client</li> </ul>	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

将配置文件复制到PC

## 第二步:启动VPN连接

在终端上,运行Cisco Secure Client并输入用户名和密码,然后确认Cisco Secure Client连接成功。

O 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 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	

连接成功

## 第三步:确认ASA上的系统日志

在系统日志中,确认IKEv2连接成功。

#### <#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

## 第四步:确认ASA上的IPsec会话

运行show vpn-sessiondb detail anyconnect命令以确认ASA上的IKEv2/IPsec会话。

#### <#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

第五步:确认Radius实时日志

导航到操作> RADIUS >实时日志 ISE GUI中,确认vpn身份验证的实时日志。

≡	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								Befresh	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实时日志

#### 点击Status以确认实时日志的详细信息。

Cisco ISE				
Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
		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 Store	AD_Join_Point	24209	Looking up Endpoint in Internal Endpoints IDStore - vpnuser	0
		24211	Found Endpoint in Internal Endpoints IDStore	9
Identity Group	Workstation	15048	Queried PIP - Network Access.AuthenticationStatus	2
Audit Session Id	01aa003d0001700066559220	15016	Selected Authorization Profile - PermitAccess	7
Authentication Method	PAP_ASCII	22081	Max sessions policy passed	6
Authentication Destant		22080	New accounting session created in Session cache	0
Authentication Protocol	PAP_ASUI	11002	Returned RADIUS Access-Accept	2
Network Device	ASAv			

实时日志的详细信息

#### 故障排除

#### 加密算法不匹配可能导致连接故障。这是出现算法不匹配问题的示例。在ASDM中执行Configuration部分的第15步可以解决此问题。

步骤1:启动VPN连接

在终端上,运行Cisco Secure Client并确认由于加密算法不匹配导致连接失败。

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



连接失败

第二步:在CLI中确认系统日志

在系统日志中,确认IKEv2协商失败。

#### <#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

#### 参考

通过IKEv2的AnyConnect连接到ASA,进行AAA和证书身份验证

#### 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。