AAA &;証明書認証を使用したASDMでのセキ ュアクライアントIKEv2/ASAの設定

内容
<u>はじめに</u>
<u>前提条件</u>
<u>要件</u>
使用するコンポーネント
ネットワーク図
コンフィギュレーション
ー ASDMでの設定
 ステップ 1:VPNウィザードを開く
ーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーーー
<u>ステップ 5 : 認証方式</u>
<u>手順 6:SAML設定</u>
<u>手順7:クライアントアドレス割り当て</u>
<u>ステップ8: ネットワーク名前解決サーバ</u>
<u>ステップ 9:NAT免除</u>
<u>ステップ 10:セキュアなクライアント展開</u>
<u>ステップ 11設定の保存</u>
<u>ステップ 12セキュアクライアントプロファイルの確認とエクスポート</u>
<u>ステップ 13セキュアクライアントプロファイルの詳細の確認</u>
<u>ステップ 14:ASA CLIでの設定の確認</u>
<u>ステップ 15:暗号化アルゴリズムの追加</u>
<u>Windows Serverでの設定</u>
<u>ISEでの設定</u>
<u>ステップ1: デバイスの追加</u>
<u>ステップ 2:Active Directoryの追加</u>
<u>ステップ3:アイデンティティソースシーケンスの追加</u>
<u>ステップ4:ポリシーセットの追加</u>
<u>ステップ5: 認証ポリシーの追加</u>
<u>手順6: 許可ポリシーの追加</u>
<u>ステップ1:セキュアクライアントプロファイルのWin10 PC1へのコピー</u>
<u>ステップ2:VPN接続の開始</u>
<u>ステップ3: ASAでのSyslogの確認</u>
<u>ステップ4:ASAでのIPsecセッションの確認</u>
<u>ステップ5: Radiusライブログの確認</u>
トラブルシュート
<u>ステップ1:VPN接続の開始</u>
<u>ステップ2:CLIでのSyslogの確認</u>
<u>参考</u>

はじめに

このドキュメントでは、ASDMとAAAおよび証明書認証を使用して、ASA上でIKEv2を介したセキ ュアクライアントを設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ・ Cisco Identity Services Engine(ISE)の設定
- Cisco適応型セキュリティ仮想アプライアンス(ASAv)の設定
- ・ Cisco Adaptive Security Device Manager(ASDM)の設定
- VPN認証のフロー

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Identity Services Engine仮想3.3パッチ1
- ・ 適応型セキュリティ仮想アプライアンス9.20(2)21
- Adaptive Security Device Manager(ASDM)7.20
- Cisco Secureクライアント5.1.3.62
- Windows Server 2016
- Windows 10

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

ネットワーク図

次の図は、このドキュメントの例で使用するトポロジを示しています。

Windows Server 2016で設定されるドメイン名は、このドキュメントの例で使用するad.remsystem.comです。



ネットワーク図

コンフィギュレーション

ASDMでの設定

ステップ1:VPNウィザードを開く

Wizards > VPN Wizardsの順に移動し、Secure Client VPN Wizardをクリックします。



[Next] をクリックします。



[次へ]ボタンをクリックします

ステップ2:接続プロファイルID

接続プロファイルの情報を入力します。 接続プロファイル名:vpn-ipsec-tunnel-grp VPNアクセスインターフェイス: outside

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Connection Profile Identification	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme Summary 	This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections. Connection Profile Name: vpn-ipsec-tunnel-grp VPN Access Interface: outside v	
	< Back Next > 現別 Help	

接続プロファイルID

ステップ 3: VPN プロトコル

IPsecを選択し、Addボタンをクリックして、新しい自己署名証明書を追加します。

Secure Client VPN Conn	ection Setup Wizard X	Ta Manage Identity Certificates X
Secure Client VPN Conn Steps 1. Introduction 2. Connection Profile Identification 3. VPN Protocols 4. Clent Images 5. Authentication Methods 6. SAML Configuration 7. Client Address Assignme 8. Network Name Resolutio Servers	VPN Protocols Secure Clerk 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 SSL Device Certificate Device Certificate - Device Certificate identifies the ASA to the remote access clerks. Certain Secure Clerk features (Always-On, IPsec/IBEV2) require that valid device certificate be available on the ASA.	Issued To Issued By Expiry Date Associated Trustpoints Usage Public Key Type Add Show Details Delete Export Install Re-Erroll
9. NAT Exempt 10. Secure Clent Deployme 11. Summary	Device Certricate:None ✓ Manage < Back Next > Rain Help	End: Certificate Expiration Alerts Send the first alert before : 60 (days) Set Default Repeat Alert Interval : 7 (days)
		Weak Crypto Configurations Permit Weak key sizes and Hash Algorithms Public CA Enrollment Get your Cisco A5A 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 testing. Enroll ASA SSL certificate with Entrust Using a previously saved certificate signing request, erroll with Extrust. ASDM Identity Certificate Ward The Cisco ASDM Identity Certificate Ward assists you in creating a self-signed certificate that is required for launching ASDM through launcher. Launch ASDM Identity Certificate Wizard OK Cancel

自己署名証明書の情報を入力します。

トラストポイント名:vpn-ipsec-trustpoint

キーペア:ipsec-kp

Ta Add Identity Certificate X	🔁 Add Key Pair X	<
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		

自己署名証明書の詳細

VPNプロトコルの設定を確認し、Nextボタンをクリックします。

Secure Client VPN Conne	ction Setup Wizard	×
Steps	VPN Protocols Secure Client can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols would like this connection profile to support. SSL SSL Device Certificate Device Certificate identifies the ASA to the remote access clients. Certain Secure Client features (Always-On, IPsec/IXEV2) require that valid device certificate be available on the ASA. Device Certificate: vpn-ipsec-trustpoint:unstructuredNam Manage	you
	< gack Next > I(1) He	P

VPNプロトコルの設定の確認

ステップ4:クライアントイメージ

Addボタンをクリックしてセキュアなクライアントイメージを追加し、Nextボタンをクリックします。

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Client Images	
Introduction Connection Profile Identification VPN Protocols	ASA can automatically upload the latest Secure Client package to the cl 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.	ient device when it accesses the enterprise network. r to an image. by the most commonly encountered operation system to
4. Client Images 5. Authentication Methods	🕈 Add 🗹 Replace 📋 Delete 🛧 🗲	
 SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt Secure Client Deployme Summary 	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 <u>Cisco</u> by searching 'Sec	ure Mobility Client' or <u>click here</u> ,
	< gack Next >	Ikin Help

クライアントイメージ

ステップ 5:認証方式

Newボタンをクリックして新しいaaaサーバを追加し、Nextボタンをクリックします。

サーバグループ名:radius-grp

認証プロトコル:RADIUS

- サーバIPアドレス:1.x.x.191
- インターフェイス:内部

Secure Client VPN Cone	rection Setup Witard	×	Diversion Server Gr	oup	×	Secure Client VPN Conn	ection Setup Wizard	>
9 Seas 1. Selesaton 2. Convotion Hulle Detertion 3. Hill Industria 4. Cher Sungel 4. Cher Sungel 5. Satz Carlgarion 7. Clert Adhess Anapone 5. Natt Carlly 18. Searc Clert Deployee 11. Search	Alchertostas Hellok The dark bis van de holdstas of de aufbestudion norme The and all on the Theur." butten to creat a sine array grap. AAA form Ginag: [004]		Create a new adhertication server group containing one adhertication server. To add more server its the group or dhange other AAA server settings, go to Configuration > Denice Homesener > Usergl(AA > AA Server Groups. Server Group Name: Authertication Protocol: Server IP Address: Interface: Interface: Interface:		29ge Authorization Mellodi 1. beokatim Excellantin 1. Secon Cellantim Excellantin 1. Secon Cellantim Excellantin 1. Secon Cellantim Excellantim 1. Secon Cellantim Excellantim		Authentization Methods The step by support Phase* Authon to used a new prove use call due half by Real* Authon to used a new prove AAA Server Graup Catals AAA Server Graup Catals AAA Server Graup Catals AAA Server Graup Catals AAA Server Graup Catals Server Server or IP Address : Defange Termon. Termon.	
		BUT Hep	Server Secret Key: Confirm Server Secret Key: OK	Cancel Help			c(pá (jot)	RIT HO

認証方式

手順 6:SAML設定

Nextボタンをクリックします。

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

SAML設定

手順7:クライアントアドレス割り当て

Newボタンをクリックして新しいIPv4プールを追加し、Nextボタンをクリックします。

名前:vpn-ipsec-pool

開始IPアドレス:172.16.1.20

終了IPアドレス:172.16.1.30

サブネットマスク:255.255.255.0

Secure Client VPN Conne	ection Setup Wizard			×	Secure Client VPN Conne	ction Setup Wizard				×
Steps I. Introduction C. Connection Profile Identification VPM Protocols C. Carlen Images S. Authentication Nethods S. Authentication Nethods S. SAVIL Configuration N. Clictent Address Assignment N. Nat's Lempt N. Nat's Lempt S. Nat's Lempt S. Secure Client Deployme S. Summary S. Summary S. Summary S. Summary S. Secure Client Deployme S. Summary S. Summary S. Summary S. Secure Client Deployme S. Summary S. Summary S. Secure Client Deployme S. Summary S. Summary S. Secure Client Deployme S. Secure Client S. Secure Cli	Clerk Address Assignment This step allows you to create a new address pool or be assigned address from the pools when they cor IPv6 address pool is only supported for SSL connects IPv6 address Pool IPv6 address	select an existing address nect. Add IPv4 Pool Name: Starting IP Address: Subnet Mask: OK	vpn-ipsec-pool 172.16.1.20 172.16.1.30 255.255.255.0	5. The Secure Clents will	Steps	Clerk Address Assignm This step allows you to be assigned addresses IPv6 address pool is on IP v4 Address Pool Address Pool Details of the select Starting IP Address: Ending IP Address: Subnet Masis:	ent create a new address pool or select from the pools when they connect. W w upported for SSL connection. ool exc-pool New ed address pool 172.16.1.30 255.255.255.0	t an existing address pool for IPv4 a	nd IPv6. The Secure Cle	nts will
	<back next=""></back>			Riff Help		< gack Next >			Rif	Help

クライアントアドレスの割り当て

ステップ8:ネットワーク名前解決サーバ

DNSとドメインの情報を入力し、Nextボタンをクリックします。

DNSサーバ:1.x.x.57

ドメイン名:ad.rem-system.com

Secure Client VPN Conne	ction Setup Wizard	×
Steps	Network Name Resolution Servers	
 Introduction Connection Profile Identification VPN Protocols Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolution Servers NAT Exempt Secure Client Deployme Summary 	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 > I(i) He	þ

ネットワーク名前解決サーバ

ステップ 9:NAT免除

Nextボタンをクリックします。

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

NAT免除

ステップ 10:セキュアなクライアント展開

Allow Web Launchを選択し、Nextボタンをクリックします。

Secure Client VPN Conne	ction Setup Wizard X
Steps	Secure Client Deployment
Introduction Connection Profile Identification VPN Protocols	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.
 Client Images Authentication Methods SAML Configuration Client Address Assignme Network Name Resolutio Servers NAT Exempt 	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.
10. Secure Client Deployment 11. Summary	
	< gack Next > It if Help

ステップ 11設定の保存

Finishボタンをクリックして、設定を保存します。

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 failure, [INPO] means information and [WARNING] means warning [OK] in local nod von-inser-nool 172.16.1.20-172.16.1.30 mask 255.255.255.0
	Name Summary Name/Allas of the Connection Profile VPN Access Interface Device Digital Certificate VPN Proceos Enabled Secure Clent Images Authentication Server Group SAML Address Pool for the Clent DNS Network Address Translation	Value vpn-ipsec-tunnel-grp outside vpn-ipsec-turspoint:unstructuredName=ciscoasa, CN IPsec only 1 package radius-grp Server: Authentication Method: asa 172:16.1.30 Server: Domain Name: The protected traffic can be subjected to network address translation	[01] 9 Kolajson spredse toppinger-tunnel-grap_clent_profile_mith_to ASA [02] 1 wite cleart profile "dialo/typn-ipsec-tunnel-grap_clent_profile_straft to ASA [03] webugin [04] any connect profiles syn-ipsec-tunnel-grap_clent_profile_dialo(typn-ipsec-tunnel-grap_clent_profile_straft [05] asa-server radus-grap protocol radus [05] asa-server radus-grap (nside) host 1.1 ·
	< Back Einish	Rin He	Close

設定の保存

ステップ 12セキュアクライアントプロファイルの確認とエクスポート

Configuration > Remote Access VPN > Network (Client) Access > Secure Client Profileの順に移動 し、Editボタンをクリックします。

Ele Verw Tools Wigards Window Help								
Device List Boolemarks	Configuration > Remote Access VPN > Network (Client) Acce	ss > Secure Client Profile						
Boltmarks OP A To boltmark sop, right-dation a node in the nanigation tree and select "Add to boltmarks". This panel is used to manage Secure Clert Profess and perform group assignment for Secure Clert version 2.5 or later. You can select a profe to edit, change group or to delete. You can select the "Add button to add a new profile. Pressing the limport or Export button is for igoad and download of clert profess between local mathew and device. Image field a introduced with the Secure Molity Solution. This field contains different profile usage field as introduced with the Secure Molity Solution. This field contains different profile usage in Secure Clert version 3.0 and later. Remote Access VM Image Group Policy (intege Group Po								
Network (Client) Access	Profile Name	Profile Usage	Group Policy	Profile Location				
Secure Clent Connection Profiles Secure Clent Customization(Localization Secure Clent Profile Secure Clent Strikere	vpn-psec-turnel-grp_client_profile	AnyConnect VPN Profile	GroupPolicy_upn-ipsec+unnel-grp	(disk0:/vpn-ipsec-tunnel-grp_client_sxofile.xml				

セキュアクライアントプロファイルの編集

プロファイルの詳細を確認します。

- 表示名(必須):ciscoasa(IPsec)IPv4
- FQDNまたはIPアドレス:192.168.1.1
- ・ プライマリプロトコル:IPsec

Secure Client Profile Editor - v	pn-ipsec-tunnel-grj	p_client_profile					Server List Entry)	×
Profile: vpn-ipsec-tunne	el-grp_client_pr	rofile					Server Load Balanci	ngServers SCEP M	ible Certificate Pinning				
Uts - O Preferences (Part 1) - O Preferences (Part 2)	Server List	Server List					Primary Server Display Name (required) Occasia (Proc) IPv4			Connection Information	an I≫ac √		
Centrate Servers Centrate Priving Centrate Having Centrate Having Centrate Having Server Lief	Hodname Contains (1974)	Hot Address	User Group	Backup Serve List	SCDP	Moble Satting	Poplay Name Poplar of JP Ad 192,048-1-1 Group UPL	Backsp Servers Host Address	Uter Group	Primary Protocol	Prec rrng 3/2 Negotiation (5 gateway only) Add Phore Up Phore Down Delate	[AP-AnyConnett]	
									OK.	Canoel			

セキュアクライアントプロファイルの確認

Exportボタンをクリックして、プロファイルをローカルPCにエクスポートします。



セキュアクライアントプロファイルのエクスポート

ステップ 13セキュアクライアントプロファイルの詳細の確認

ブラウザでセキュアクライアントプロファイルを開き、ホストのプライマリプロトコルがIPsecで あることを確認します。

```
\u00ed 
\u00ed
```

セキュアクライアントプロファイルの詳細

ステップ14:ASA CLIでの設定の確認

ASA CLIでASDMによって作成されたIPsec設定を確認します。

// 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

ステップ15:暗号化アルゴリズムの追加

ASA CLIで、グループ19をIKEv2ポリシーに追加します。



注:IKEv2/IPsec接続に関して、Cisco Secure Clientではバージョン4.9.00086以降、Diffie-Hellman(DH)グループ2、5、14、および24をサポートしていません。この変更により、 暗号化アルゴリズムの不一致が原因で接続エラーが発生する可能性があります。

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

Windows Serverでの設定

VPN接続用のドメインユーザを追加する必要があります。 Active Directory Users and Computersに移動し、Usersをクリックします。ドメインユーザとしてvpnuserを追加します。

Active Directory Users and Computers						
File Action View Help						
💠 🔶 📶 🤾 🗂 🗙 🗊 🕢 🕞 🖬 🗂 % % 🖤 i	2 🔌					
Active Directory Users and Computers winserver.ad.rem-s Active Directory Users and Computers winserver.ad.rem-s Administra	ator ODC Passwor shers Domain Con count DDC Passwor count DDC Passwor Ser Proxy dmins omputers ontrollers wests sers Admins Key Admins Read-only Di icy Creator O ns Users Domain Con dmins	In user Properties Member Of Remote control General Address Von user Inst name: Last name: Digolay name: Digolay name: Cescription: Offige: Lecpal: Lecpal: Web page:	Dial-in Env Remote Desktop Sr Account Profile	viorment envices Profile Telephones	? X 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

```
ドメインユーザの追加
```

Domain AdminsとDomain Usersのメンバにドメインユーザを追加します。

vpn user Properties			?	×	vpn user Properties				?	\times
Remote control	Remote [Desktop Services Profile	00	M+	Remote control	Remote Desktop Services Profile			CON	M+
Member Of General Address	Dial-in Account	Profile Telephones	Organization		General Address Member Of	Account Dial-in	Profile	Telephones	Organiz Session	ation
Liter locon name:					Mambar of:		_			-
vpnuser		@ad.rem-system.com		~	Name	Active Direct	tory Domain	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 gptions:	je password a inge password expires using reversib	t next logon d le encryption		~	Add Primary group:	Remove Domain Users There is r	no need to	change Primary	group unle	55
Ne <u>v</u> er <u>End of:</u>	Monday .	June 10, 2024]	Set Filling's Group	you have applicatio	Macintosh	clients or POSID	(-compliant	t
O	((Cancel Apply	Н	elp	()K	Cancel	Apply	He	ф

ドメイン管理者とドメインユーザー

ISEでの設定

ステップ1:デバイスの追加

Administration > Network Devicesの順に移動し、AddbuttonをクリックしてASAvデバイスを追加 します。

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS S	ervers RA	DIUS Server Sequences
Network Devices Default Device Device Security Settings	Network Device Network D Name Description	evices			
	IP Addre	is ∨ * IP : 1.0000.61	√ 32 ⊗ ∽ (j		
	Model Nam	e	Ŷ		
	Network De	vice Group			
	Location	All Locations	~	Set To Default Set To Default	
	Device Typ	e All Device Types	~	Set To Default	
		RADIUS Authentication	Settings		
	Pro	tocol RADIUS		Hide	

デバイスの追加

ステップ 2: Active Directoryの追加

Administration > External Identity Sources > Active Directoryの順に移動し、Connectiontabをクリックし、Active DirectoryをISEに追加します。

- ・ 結合ポイント名: AD_Join_Point
- ・ Active Directoryドメイン:ad.rem-system.com

≡	tesce Identity Services	Administration / Identity Management	
н	Bookmarks	S Groups External Identity Sources Settings	
11	Dashboard		
1H	Context Visibility	ixternal Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings	
*	Operations	Certificate Authenticat	
-0	Policy	Active Directory ad.rem-system.com	
80	Administration	AD_Join_Point	

Active Directoryの追加

=	diada Identity Services	Engine Administration / Identity Management
н	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
11	Dashboard	
15 0	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
- %	Operations	Certificate Authenticat
-0	Policy	Select Groups From Directory
80	Administration	AD_Join_Point Add Group Control Assist ad.rem-system.com/S-1-5-32-579

Groupsタブに移動し、Select Groups From Directoryドロップダウンリストからグループを選択します。

Select Groups from Directory

[グループの取り出し]ドロップダウンリストをクリックします。Checkad.rem-

system.com/Users/Domain Computersandad.rem-system.com/Users/Domain ユーザを選択し、 [OK] をクリックします。

=	dentity Services	Engine						×	A type
		Identifies Groups F	Sel	lect Directory Group	S				
	Bookmarks	> Li Geroncare Ab	This di	ialog is used to select groups from the I	Directory	γ.			
12	Dashboard	Active Directo	Do	main ad.rem-system.com					
15	Context Visibility	AD_Join_Poin		Name . Filter F	SID .	Type ALL Filter			
×	Operations	C LDAP		Petrime Groups	trieved				
-0	Policy								
10	Administration	RSA SecuriD		Name	^	Group SID	Group Type		
-	Work Centers	SAML Id Provide	0	ad.rem-system.com/Users/DnsAdmins		\$-1-5-21-4193742415-4133520026-20462399	DOMAIN LOCAL	^	
		C Social Login	-	ad.rem-system.com/Users/DnsUpdateProx	Ý	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
•	Interactive Help			ad.rem+system.com/Users/Domain Admins	_	5+1+5+21+4193742415+4133520026+20462399	GLOBAL		
				ad rem-system.com/Users/Domain Compo	ers.	5-1-5-21-4193742415-4133520028-20482399	CLOBAL CLOBAL		
			-	ad rem-system com/Users/Domain Guests		5-1-5-21-4193742415-4133520026-20442399	CLOBAL		
				ad.rem-system.com/Users/Domain Users		5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
				ad.rem+system.com/Users/Enterprise Adm	ina.	5-1-5-21-4193742415-4133520026-20462399	UNIVERSAL	10.00	
			0	ad.rem-system.com/Users/Enterprise Key J	Admins	5-1-5-21-4193742415-4133520026-20462399	UNIVERSAL		
			0	ad.rem+system.com/Users/Enterprise Read	-only	5+1+5+21+4193742415+4133520026+20462399	UNIVERSAL	1	
				ad.rem+system.com/Users/Group Policy Cr	eator	5-1-5-21-4193742415-4133520026-20462399	GLOBAL		
			<		-			• Ť	
							Cancer	ur .	

ドメインコンピューターとユーザーの追加

ステップ3:アイデンティティソースシーケンスの追加

Administration > Identity Source Sequencesの順に移動し、Identity Source Sequenceを追加します。

- 名前: Identity_AD
- ・ 認証検索リスト:AD_Join_Point

≡	dentity Services	Engine		Administration / Id	lentity Management
Щ	Bookmarks	Identities Groups	External Identity Sources	Identity Source Sequences	Settings
10 10	Dashboard Context Visibility	Identity Source Sequence	equence		
* U 40 El	Operations Policy Administration Work Centers	V Identity Source	e Sequence dentity_AD		
9	Interactive Help	Certificate Ba Select Certific	ased Authentication	~	
		 Authenticatio A set of ider Available Internal E Internal C Guest Us All_AD_J 	n Search List tity sources that will be accessed i indpoints Isers ers oin_Points	n sequence until first authentication se Selected AD_Join_Point	ucceeds

アイデンティティソースシーケンスの追加

ステップ4:ポリシーセットの追加

Policy > Policy Setsの順に移動し、+ をクリックしてポリシーセットを追加します。

- ・ポリシーセット名:VPN_Test
- 条件:DEVICE Device Type はすべてのデバイスタイプと同じ
- •許可されるプロトコル/サーバシーケンス:デフォルトのネットワークアクセス

≡	dentity Services Engineer	ne	Policy / Policy Set		A Evaluation	Mode = Days Q	۵	0	Ф А
Щ	Bookmarks	Policy Sets			Reset	Reset Policyset Hit	counts		Save
51	Dashboard	+ Status Policy Set Name	Description	Conditions	Allowed Protocols / S	Server Sequence	Hits	Actions	View
10	Context Visibility	Q Search							
×	Operations	VDN Test		DEVICE-Device Type EQUALS AI	Default Network Acce	P55 0 1	20	sêt.	
0	Policy	ALIATION		The Device Types		<i>v</i> +	50	£\$1	·

```
ポリシーセットの追加
```

ステップ5:認証ポリシーの追加

Policy Setsに移動し、VPN_Testをクリックして認証ポリシーを追加します。

- ルール名:VPN_Authentication
- 条件:ネットワークアクセスデバイスのIPアドレスが1.x.x.61と等しい
- 使用:Identity_AD

∨Authenticati	ion Policy(2)				
🕂 Statu	is Rule Name	Conditions	Use	Hits	Actions
Q Sear	ch				
	r		Identity_AD		
0	VPN_Authentication	Network Access Device IP Address EQUALS 1.171.1.61	> Options		Ś
認証ポリシ	一の追加				

手順6:許可ポリシーの追加

Policy Setsに移動し、VPN_Testをクリックして認可ポリシーを追加します。

- ルール名:VPN_Authorization
- 条件:Network_Access_Authentication_Passed
- 結果:PermitAccess

∨Autho	rization	Policy(2)								
					Results					
ŧ	Status	Rule Name		Conditions	Profiles		Security Groups		Hits	Actions
Q	Searc	h								
	0	VPN_Authorization	=	Network_Access_Authentication_Passed	PermitAccess	0 +	Select from list	0 +	10	ŝ
許可ポ	リシ-	ーの追加								

確認

ステップ1:セキュアクライアントプロファイルのWin10 PC1へのコピー

セキュアクライアントプロファイルをC:\ProgramData\Cisco\Cisco Secure Client\VPN\Profileディ レクトリにコピーします。

← → • ↑ 📙	> This PC > Local Disk (C:) > ProgramData > Cisco	> Cisco Secure Client	t > VPN > Profile >
1 O ist server	Name	Date modified	Туре
Quick access	MgmtTun	5/17/2024 8:42 AM	File folder
Desktop	vpn-ipsec-tunnel-grp_client_profile	5,773/2024 12:48 AM	XML Document
	AnyConnectProfile.xsd	,'1./2024 1:12 PM	XSD File

ステップ2:VPN接続の開始

エンドポイントで、Cisco Secure Clientを実行し、ユーザ名とパスワードを入力して、Cisco Secure Clientが正常に接続されていることを確認します。

Sisco Secure Client - 🗆 🗙				Sisco Secure Client ciscoasa (IPsec) IPv4	S Cisco Secure Client	-		×	
AnyConnect VPI: Please enter your username and pa discoasa (IPsec) IPv4	issword.	Connect		Please enter your username and password. Group: vpn-ipsec-tunnel-grp Username: vpnuser	~	AnyConnect VPH: Connected to discoasa (IPsec) IPv4. discoasa (IPsec) IPv4		Disconnect	_
			_	Password:		00:00:05		I	Pv4
				OK Canc	el				

Connection succeeded

ステップ3:ASAでのSyslogの確認

syslogで、IKEv2接続が成功したことを確認します。

<#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

ステップ4:ASAでのIPsecセッションの確認

show vpn-sessiondb detail anyconnectコマンドを実行して、ASAでのIKEv2/IPsecセッションを確認します。

<#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

ステップ 5:Radiusライブログの確認

ISE GUIでOperations > RADIUS > Liveの順に移動し、vpn認証のライブログを確認します。

≡	dentity Services E	Engine						Operations / RADIL	JS			ه ۵	aluation Mode 🥅 Days	۵ ۵	۲	۹ ۹
н	Bookmarks	Live Logs Live Sessions														
	Dashboard															
N	Context Visibility	Misconfigured Supplicants			Mis	configured Ne	twork Device	es 📀	RADIUS Drops		Client Stopped Re	sponding 🔘			Repeat C	ounter 📀
*	Operations	0				0)		0		0				(0
Ð	Policy											Refresh	Show		Michin	
8.	Administration											Never	V Latest 20 m	cords 🗸	Last 3 ho	urs v
ก็เ	Work Centers	🕄 🎂 Reset Repeat Counts	₫ Export To ∨												Filter 🗸	0
		Time	Status	Details	Repeat	Endpoint	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network De	Device Por	t Ide	ntity Grou
(?)	Interactive Help	×				Endpoint ID	Identity	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	V Network Devic	Device Port	Ide	ntity Group
		May 28, 2024 05:13:42	٠	ō.	0	00.50.5	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess					
		May 28, 2024 05:13:42		ò		00:50:5	vpnuser	Windows10-Workstation	VPN_Test >> VPN_Authentication	VPN_Test >> VPN_Authorization	PermitAccess		ASAv		Wor	kstation

Radiusライブログ

[ステータス]をクリックして、ライブログの詳細を確認します。

Cisco ISE				
Overview		Steps		
		Step ID	Description	Latency (ms)
Event	5200 Authentication succeeded	11001	Received RADIUS Access-Request	
Username	vpnuser	11017	RADIUS created a new session	1
Endpoint Id	00:50:56:98:77:A4 ⊕	15049	Evaluating Policy Group	36
Endpoint Profile	Windows10-Workstation	15008	Evaluating Service Selection Policy	1
Lingpoint Frome		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			

ライブログの詳細

トラブルシュート

暗号化アルゴリズムのミスマッチにより、接続障害が発生する可能性があります。これは、アルゴリズムの不一致の問題が発生す る場合の例です。ASDMでセクション「設定」のステップ15を実行すると、この問題を解決できます。

ステップ1:VPN接続の開始

エンドポイントでCisco Secure Clientを実行し、暗号化アルゴリズムの不一致が原因で接続が失敗したことを確認します。

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	×
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	

接続に失敗しました。

ステップ2:CLIでのSyslogの確認

syslogで、IKEv2ネゴシエーションが失敗したことを確認します。

<#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

AAA 認証と証明書認証を使用した、IKEv2 による ASA への AnyConnect

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。