# ローカル CA サーバおよび AnyConnect ヘッド エンドとしての ASA の設定

# 目次

はじめに 前提条件 要件 <u>使用するコンポーネント</u> 背景説明 設定 ネット<u>ワーク図</u> ローカル CA サーバとしての ASA 手順1: ローカル CA サーバを ASA 上で設定し、有効にする 手順2:ユーザを作成し、ASA データベースに追加する 手順3:WAN インターフェイスで WebVPN を有効にする ステップ4:証明書をクライアントマシンにインポートする AnyConnect クライアント用の SSL ゲートウェイとしての ASA ASDM AnyConnect 構成ウィザード AnyConnect 用の CLI の設定 確認 トラブルシューティング 関連情報

## 概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス(ASA)を認証局(CA)サー バおよび Cisco AnyConnect セキュア モビリティ クライアント用のセキュア ソケット レイヤ (SSL)ゲートウェイとしてセットアップする方法説明します。

## 前提条件

### 要件

次の項目に関する知識が推奨されます。

- ソフトウェア バージョン 9.1.x を実行する基本的な ASA 設定
- ASDM 7.3 以降

### 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くものです。

・ソフトウェア バージョン 9.1(6) が稼働する Cisco 5500 シリーズ ASA

- AnyConnect セキュア モビリティ クライアント バージョン 4.x (Windows 用)
- ・<u>互換性チャート</u>ごとにサポートされている OS が稼働する PC。
- Cisco Adaptive Security Device Manager (ASDM) バージョン 7.3

注: シスコの「<u>ソフトウェア ダウンロード</u>」ページ(登録ユーザ専用)から、AnyConnect VPN Client パッケージ(anyconnect-win\*.pkg)をダウンロードします。 AnyConnect VPN Client を ASA のフラッシュ メモリにコピーします。これは、ASA との SSL VPN 接続を確 立するためにリモート ユーザ コンピュータにダウンロードされます。 詳細については、 ASA のコンフィギュレーション ガイドの「<u>AnyConnect Client のインストール</u>」セクショ ンを参照してください。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメン トで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています。 稼働中 のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してくだ さい。

## 背景説明

ASA の認証局は次の機能を提供します。

- •ASAの基本的な認証局の動作を統合する。
- •証明書を導入する。
- 発行済み証明書のセキュアな失効チェックを実行する。
- ブラウザベース(WebVPN)とクライアントベース(AnyConnect)の両方で SSL VPN 接続とともに、ASA 上に認証局を提供する。
- •外部の証明書認証に依存することなく、ユーザに信頼できるデジタル証明書を提供する。
- 証明書認証のためのセキュアな内部認証局を提供し、Web サイト ログインを使用した簡単な ユーザ登録を実現する。

#### 注意事項と制約事項

- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポ ートされています。
- 一度に 1 つのローカル CA サーバのみ ASA に常駐できます。
- ローカル CA サーバ機能としての ASA は、フェールオーバー設定ではサポートされません。
- ローカル CA サーバとして機能する ASA は現在、SHA1 証明書の生成のみサポートします。
- ローカル CA サーバは、ブラウザ ベースとクライアント ベースの両方の SSL VPN 接続に使用することができます。 現在、IPSec にはサポートされていません。
- ローカル CA の VPN ロード バランシングをサポートしていません。
- ローカル CA は別の CA に従属することはできません。 ルート CA としてのみ機能できます。
- •現在、ASA はアイデンティティ証明書のローカル CA サーバに登録することはできません。
- 証明書の登録が完了すると、ASA により、ユーザのキーペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約2KBのフラッシュメモリまた はディスク領域が必要です。実際のディスク領域の量は、設定されているRSA キーサイズ と証明書フィールドによって異なります。使用できるフラッシュメモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してくださ い。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシ ュメモリに保存されます。

# 設定

このセクションでは、Cisco ASA をローカル CA サーバとして設定する方法について説明します。

**注:** このセクションで使用されているコマンドの詳細を調べるには、<u>Command Lookup</u> <u>Tool(登録</u>ユーザ専用)を使用してください。

### ネットワーク図



### ローカル CA サーバとしての ASA

### ステップ1: ローカル CA サーバを ASA 上で設定し、有効にする

- [Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [CA Server] の順に移動します。 [Enable Certificate Authority server] オプション をチェックします。
- パスフレーズを設定します。パスフレーズは最低7文字にする必要があります。これは、ローカル CA 証明書とキーペアを含む PKCS12 ファイルのエンコードと保存のために使用されます。 CA 証明書またはキーペアが失われた場合は、パスフレーズを使用して PKCS12 アーカイブをロック解除します。
- •発行元名を設定します。 このフィールドは、ルート証明書 CN として表示されます。 次の形 式で指定できます。 CN(共通名)、OU(組織ユニット)、O(組織)、L(地名)、S(州 )、C(国)
- オプション設定: [SMTP Server and Email Server settings] を、OTP がメールを介してエンドクライアントに受信されて登録が完了するように設定します。 ローカル Email/SMTP サーバのホスト名または IP アドレスを設定することができます。 また、クライアントが受信する電子メールの [From address] および [Subject] フィールドを設定することもできます。 デフォルトでは、[From Address] は admin@<ASA hostname>.null で、[Subject] は Certificate Enrollment Invitation.です。

# オプション設定: Client key size、CA server key size、Ca Certificate Lifetime、および Client certificate lifetime などのオプション パラメータを設定できます。

ce List 🗗 🛱 兴 Configuration > Remote Access VPN > Certificate Management > Local Certificate Authori

🖨 Add 🏛 Delete 🚿 Connect		
Add Delete Sp connect	Configure the Local Certificate Au	uthority. To make configuration changes after it has been configured for the first time, disable the Local Certificate Authority.
Find: Go	Enable Certificate Authority S	Server
10.105.130.69:4443	Passphrase:	
	Confirm Passphrase:	••••••• Specify the Passphrase
	Issuer Name:	CN=ASA.local Specify the CN which will show as Issuer nam
	CA Server Key Size:	1024 🗸
	Client Key Size:	1024 V Specify the Server/Client key-size to
	CA Certificate Lifetime:	1095 days
		The CA certificate lifetime change will take effect after existing CA certs expire.
Remote Access VPN	Client Certificate Lifetime:	365 days
? Introduction	SMTP Server & Email Settings	
Cliently Access	Server Name/IP Address:	
AAA/Local Users	From Address:	admin@ciscoasa.null
Secure Desktop Manager	Subject:	Certificate Enrolment Invitation
Certificate Management	Subject	
The Identity Certificates	More Options	
Trusted Certificate Pool		
- 2 Code Signer		
- E Local Certificate Authority		
CA Server		
Manage User Database		
Manage User Certificates		

### CLIの同等の設定:

ASA(config)# crypto ca server ASA(config-ca-server)# issuer-name CN=ASA.local ASA(config-ca-server)# subject-name-default CN=ASA.local ASA(config-ca-server)# lifetime certificate 365 ASA(config-ca-server)# lifetime ca-certificate 1095 ASA(config-ca-server)# passphrase cisco123 ASA(config-ca-server)# no shutdown % Some server settings cannot be changed after CA certificate generation. Keypair generation process begin. Please wait...

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete

これらは、ローカル CA サーバの設定で構成できる追加のフィールドです。

これは ASA での CRL の場所です。
デフォルトの場所は、 <u>http://hostname.domain/+CSCOCA+/asa_ca.crl</u> ですが、URL に
特定のインターフェイスおよびポートで、CRL に HTTP ダウンロードできるようにす
publish-CRL インターフェイスを選択します。次に、1~65535の任意のポート番号
TCP ポート 80 です。
ローカル CA は、ユーザ証明書が無効化または無効化解除されるたびに、CRL を更新
更がない場合、CRL ライフタイム 1 回ごとに、CRL が自動的に再発行されます。ライ
lifetime crl コマンドで指定した期間です。 CRL のライフタイムを指定しない場合、ラ
ASA では、ユーザ情報、発行済み証明書、および失効リストへのアクセスと実装にL
このデータベースは、デフォルトでローカル フラッシュ メモリに存在するか、または
外部のファイル システム上に設定することもできます。
発行された証明書のユーザ名に追加されるデフォルト サブジェクト(DN 文字列)を
指定できます。
• CN(共通名)SN(姓)
• O(組織名)
• L(地名)

C(国) OU(組織ユニット) EA(電子メール アドレス) • ST(州/都道府県) • T(タイトル) ユーザが ASA から PKCS12 ファイルを取得できる登録制限時間を設定します(時間 Enrollment Period デフォルト値は 24 時間です。 : ユーザ証明書が含まれる PKCS12 ファイルを取得する前に登録の有効期間が切れた: One Time OTP のユーザ登録有効期間を定義します(時間単位)。 この期間は、ユーザが登録を Password 値は 72 時間です。 Expiration Certificate 証明書の有効期限までの日数を指定します。この日数が経過すると、再登録に関する Expiration Reminder

### 手順2:ユーザを作成し、ASA データベースに追加する

• [Configuration] > [Remote Access VPN] > [Certificate Management] > [Local Certificate Authority] > [Manage User Database] に移動します。[Add] をクリックします。



• ユーザの詳細を指定します。次の画像に示すように、ユーザ名、電子メール ID、件名を指定

🔄 Add User		×	
Username:	user1		
Email ID:	user 1@cisco.com		
Subject (DN String):	CN=user1,OU=TAC Select		
Allow enrollment			
	Add User Cancel Help		

- 認証のための登録ができるように、[Allow Enrollment] がチェックされていることを確認します。
- ・[Add User] をクリックして、ユーザ設定を完了します。

CLI の同等の設定:

- ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com
  - ユーザがユーザ データベースに追加されると、登録ステータスは [Allowed to Enroll] として 示されます。

Configuration > Remote Acc	cess VPN > Certificate Management >	Local Certificate Authority > Manage	<u>User Database</u>		
Manage the users in the user of	database for Local Certificate Authority Ser	ver.			
Username	Email	Subject Name	Enrollment Status	Certificate Holder	Add
user1	user 1@cisco.com	CN=user1,OU=TAC	allowed	yes	Edit
					Delete
					Allow Enrollment
					Errel OTD
					Email OTP
					View/Re-generate OTP

ユーザのステータスを確認するための CLI:

#### ASA# show crypto ca server user-db

username: user1
email: user1@cisco.com
dn: CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll

 ユーザがユーザ データベースに追加されると、ユーザが登録を完了できるように、次のいず れかの方法で One Time Password (OTP)を提供できます。

OTP に電子メールを送信する(CA サーバ設定で [SMTP server and Email Settings] が必要)。

#### または

OTP を直接表示し、[View/Re-generate OTP] をクリックしてユーザと共有する。 これは、OTP の再生成にも使用できます。

nfiguration :	> Remote Access VPN >	<u>Certificate Management</u> > <u>L</u>	ocal Certificate Authority > M	anage User Database	ſ
Manage the us	ers in the user database for	Local Certificate Authority Server			
Username	Email	Subject Name	Enrollment Status	Certificate Holder	Add
user 1	user 1@gmail.com	CN=user1,OU=TAC	allowed	yes	Edit
					Delete
					Allow Enrollment
					Email OTP
					View/Re-generate OTP

#### CLI の同等の設定:

ASA# show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll

手順3:WAN インターフェイスで WebVPN を有効にする

・クライアントが登録を要求できるように、ASA で Web アクセスを有効にします。

ASA# show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll

#### 手順4:証明書をクライアント マシンにインポートする

- クライアント ワークステーションでブラウザを開き、登録を完了するためにリンクに移動します。
- このリンクで使用される IP/FQDN は、前の手順で webvpn が有効にされたインターフェイス
   、つまり インターフェイス Internet の IP である必要があります。

https://<ASA IP/FQDN>/+CSCOCA+/enroll.html

 ユーザ名(手順2、オプションAのASAで設定したもの)およびOTP(電子メールまたは 手動で提供されたもの)を入力します。

C DInPrivate C https:	/10.105.130.69/+CSCOCA+/login.html	D 🗸 😵 Certificate error C 🧭 10.105.130.69	×
alialia cisco	ASA - Local Certificate Authority		
454 Loost	Cartificato Authority		
Username	user1		
One-time Password	it Reset	Enter the User-Name and OTP provided	
NOTE: On successful au	thentication:		
Open or Save the     Install the certific     Close all the brow     Restart the SSL	generated certificate ate in the browser store vser windows, and /PN connection		

[Open] をクリックして、ASA から受け取ったクライアント証明書を直接インストールします。
 クライアント証明書をインストールするパスフレーズは、前に受け取った OTP と同じです。

File Down	load 🗾 🔀
Do you	want to open or save this file?
	Name: user1.p12 Type: Personal Information Exchange From: 10.105.130.214 Open Save Cancel
2	While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

• [Next] をクリックします。

### Certificate Import Wizard



•パスはデフォルト値のままにして、[Next] をクリックします。

Certificate Import Wizard	x
File to Import Specify the file you want to import.	
File name:           s\Temporary Internet Files\Content.IE5\SQT1AUGH\user1[1].p12         Browse	
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange-PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)	
Learn more about <u>certificate file formats</u>	
< Back Next > Cance	2

- [Password] フィールドに OTP を入力します。
- 必要に応じて、将来、キーをワークステーションからエクスポートできるようにするために 、[Mark this key as exportable] オプションを選択できます。
- [Next] をクリックします。

Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Include all extended properties.
Learn more about protecting private keys
< Back Next > Cancel

- 特定の証明書ストアに手動で認証をインストールするか、またはそのままにして自動的にストアを選択することができます。
- [Next] をクリックします。

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Output Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel

• [Finish] をクリックして、インストールを完了します。

### Certificate Import Wizard



# Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

### You have specified the following settings:







- •証明書が正常にインストールされたら、これを確認できます。
- IE を開き、[Tools] > [Internet Options] に移動します。

🏠 👻 (	<u>م</u>	🔻 🖃 🖶 🔻 Page 🕶 Safe	ty 🕶 🛛 Tools 💌
		Diagnose Connection Proble	ms
	<b>t</b>	Reopen Last Browsing Session	n
		Pop-up Blocker	•
	٢Ÿ	Manage Add-ons	
	€	Work Offline	
		Compatibility View	
		Compatibility View Settings	
	<b>1</b>	Full Screen	F11
		Toolbars	+
		Explorer Bars	•
	<⊳>	Developer Tools	F12
		Suggested Sites	
	1	Internet Options	

• 次の画像に示すように、[Content] タブに移動して、[Certificates] をクリックします。

Internet Options
General Security Privacy Content Connections Programs Advanced
Parental Controls
be viewed.
Ratings help you control the Internet content that can be viewed on this computer.
Enable 💿 Settings
Certificates
Use certificates for encrypted connections and identification.
Clear SSL state Certificates Publishers
AutoComplete
AutoComplete stores previous entries on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
OK Cancel Apply

• [Personal] ストアでは、ASA から受信した証明書を表示できます。

Certificates							x
Intended pu	urpose: (	<al ></al >					•
Personal	Other Peop	le Int	termediate Certification	Authorities	Trusted Ro	ot Certification 4	•
Issued	То		Issued By	Expiratio	Friend	ly Name	
user	.1		asa.local	1/8/2017	7 ou=TA	AC, cn = user 1	
Import Certificate	. Exp	ort urposes	Remove			Advance	d
Learn more	e about <u>certif</u>	<u>îcates</u>				Close	

AnyConnect クライアント用の SSL ゲートウェイとしての ASA

### ASDM AnyConnect 構成ウィザード

AnyConnect 構成ウィザード/CLI は、AnyConnect セキュア モビリティ クライアントを設定する ために使用できます。 先に進む前に、AnyConnect クライアント パッケージが ASA ファイアウ ォールのフラッシュまたはディスクにアップロードされていることを確認します。

構成ウィザードを使用して AnyConnect セキュア モビリティ クライアントを設定するために、次の手順を実行します。

1. ASDM にログインし、[Wizards] > [VPN Wizards] > [AnyConnect VPN Wizard] に移動して設 定ウィザードを起動し、[Next] をクリックします。

TanyConnect VPN Connection	on Setup Wizard	23
VPN Wizard	Introduction	
Branch Home Corporate Network	Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the user's device when a VPN connection is established.	end
	< Back Next > Cancel H	(elp

2. [Connection Profile Name] を入力し、VPN から終端されるインターフェイスを [VPN Access Interface] ドロップダウン メニューから選択して、[Next] をクリックします。

a AnyConnect VPN Connection 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 connections		
2. Connection Profile Identification			
3. VPN Protocols	Connection Profile Name: SSL_GRP		
4. Client Images	VPN Access Interface:		
5. Authentication Methods			
6. Client Address Assignme			
<ol> <li>Network Name Resolutio Servers</li> </ol>			
8. NAT Exempt			
<ol> <li>AnyConnect Client Deployment</li> </ol>			
10. Summary			
	< Back Next > Cancel Help		

3. セキュア ソケット レイヤ(SSL)を有効にするために、[SSL] チェックボックスにチェックを 入れます。 デバイス証明書は、信頼できるサードパーティの認証局(CA)によって発行された 証明書(Verisign、Entrust など)や自己署名証明書にすることができます。 証明書がすでに ASA にインストールされている場合、ドロップダウン メニューから選択できます。  注:この証明書は ASA によって SSL クライアントに提示されるサーバ側の証明書です。 ASA に現在インストールされているサーバ証明書がない場合、自己署名証明書を生成する 必要があります。その後、[Manage] をクリックします。サードパーティの証明書をインス トールするために、シスコの <u>ASA 8.x WebVPN で使用するサードパーティ ベンダーの証明</u> 書を手動でインストールする設定例の資料で説明されている手順を実行します。[VPN

X

Protocols] と [Device Certificate] を有効にします。[Next] をクリックします。

Steps	VPN Protocols
<ol> <li>Introduction</li> <li>Connection Profile Identification</li> </ol>	AnyConnect 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.
3. VPN Protocols	SSL SSL
4. Client Images	IPsec
5. Authentication Methods	Device Certificate
6. Client Address Assignme	Device certificate identifies the ASA to the remote access clients. Certain
<ol> <li>Network Name Resolutio Servers</li> </ol>	AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.
8. NAT Exempt	
<ol> <li>AnyConnect Client Deployment</li> </ol>	Device Certificate: None
10. Summary	
	< Back Next > Cancel Help

4. ローカル ドライブまたは ASA のフラッシュ/ディスクから AnyConnect クライアント パッケー ジ(.pkg ファイル)を追加するために、[Add] をクリックします。

フラッシュ ドライブから画像を追加するには、[Browse Flash] をクリックし、ホスト マシンのロ ーカル ドライブから画像を追加するには、[Upload] をクリックします。

AnyConnect VPN Connec	tion Setup Wizard	L	23
Steps	Client Images		
1. Introduction	ASA can automatically upload the latest AnyConnect package to the dier	nt device when it accesses the enterprise network.	,
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser You can also minimize connection setup time by moving the image used b	to an image. y the most commonly encountered operation syste	em to
3. VPN Protocols	the top of the list.	,,,,,,,,,,	
4. Client Images			
5. Authentication Methods	Add      Replace Delete      T		
6. Client Address Assignme	Image	Regular expression to match user-agent	
7. Network Name Resolutio Servers			
8. NAT Exempt			
<ol> <li>AnyConnect Client Deployment</li> </ol>			
10. Summary			
	You can download AnyConnect Client packages from Cisco by searching	'AnyConnect VPN Client' or click here	
	Too can domined Any connect client packages non <u>cisto</u> by searching	any connect that digite or <u>clearing c</u> a	
	< Back Next >	Cancel Hel	p

- AnyConnect.pkg ファイルは、ASA フラッシュ/ディスク(パッケージがすでに存在する場合)またはローカル ドライブのいずれかからアップロードできます。
- Browse flash: AnyConnect パッケージを ASA フラッシュ/ディスクから選択します。
- Upload : AnyConnect パッケージをホスト マシンのローカル ドライブから選択します。
- [OK] をクリックします。

add AnyConnect Client Image	23
AnyConnect Image: disk0:/anyconnect-win-4.2.00096-k9.pkg	Browse Flash
	Upload
Regular expression to match user-agent	*
OK Cancel Help	

• [Next] をクリックします。

AnyConnect VPN Connect	ion Setup Wizard	×
Steps	Client Images	
1. Introduction	ASA can automatically upload the latest AnyConnect package to the clien	t device when it accesses the enterprise network.
2. Connection Profile Identification	A regular expression can be used to match the user-agent of a browser to You can also minimize connection setup time by moving the image used by	to an image. y the most commonly encountered operation system to
3. VPN Protocols	the top of the list.	
4. Client Images		
5. Authentication Methods		
6. Client Address Assignme	Image	Regular expression to match user-agent
<ol> <li>Network Name Resolutio Servers</li> </ol>	disk0:/anyconnect-win-4.2.00096-k9.pkg	
8. NAT Exempt		
9. AnyConnect Client Deployment		
10. Summary		
	You can download AnyConnect Client packages from Circo by searching	'AnyConnect VPN Client' or click here
	Tou can domitoad Anyconnect Client packages from CISCO by Searching	Any connect very client of <u>click here</u> .
	< Back Next >	Cancel Help

5. ユーザ認証は認証、許可、およびアカウンティング(AAA)サーバ グループを介して実行でき ます。 ユーザがすでに設定されている場合、[LOCAL] を選択して、[Next] をクリックします。 そ の他に、ユーザをローカル ユーザ データベースに追加して、[Next] をクリックします。

**注:** この例では、**ローカル認証**が設定されています。これは、ASA のローカル ユーザ デー タベースが認証に使用されることを示します。

AnyConnect VPN Connection	on Setup Wizard	23
Steps 1. Introduction	Authentication Methods This step lets you specify the location of the authentication server.	
<ol> <li>Connection Profile Identification</li> <li>VPN Protocols</li> </ol>	You can click on the "New" button to create a new server group.	
4. Client Images 5. Authentication Methods	Local User Database Details	
<ol> <li>Client Address Assignme</li> <li>Network Name Resolutio Servers</li> <li>NAT Exempt</li> <li>AnyConnect Client Deployment</li> <li>Summary</li> </ol>	User to be Added Username: user1 Add >> Password: ••••• Delete Confirm Password: •••••	
(	< Back Next > Cancel H	elp

6. VPN クライアントのアドレス プールが設定されていることを確認します。 ip プールがすでに 設定されている場合、ドロップダウン メニューから選択します。 設定されていない場合、[New] をクリックして設定します。 完了したら [next] をクリックします。

AnyConnect VPN Connect	tion Setup Wizard
Steps         1. Introduction         2. Connection Profile Identification         3. VPN Protocols         4. Client Images         5. Authentication Methods         6. Client Address Assignment         7. Network Name Resolutio Servers         8. NAT Exempt         9. AnyConnect Client Deployment         10. Summary	Client Address Assignment This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect. IPv6 address pool is only supported for SSL connection. IP v4 Address Pool IP v6 Address Pool Address Pool: Select New Details of the selected address pool
	< Back Next > Cancel Help

Add IPv4 Pool	
Name:	VPN_Pool
Starting IP Address:	10.10.10.1
Ending IP Address:	10.10.200
Subnet Mask:	255.255.255.0 ▼
ОК	Cancel Help

• [Next] をクリックします。

7. 必要に応じて、ドメイン ネーム システム(DNS)サーバと DN を [DNS Servers] および [Domain Name] フィールドに設定し、[Next] をクリックします。

a AnyConnect VPN Connection 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:	
3. VPN Protocols	WINS Servers:	
4. Client Images	Domain Name:	
5. Authentication Methods		
6. Client Address Assignme		
7. Network Name Resolution Servers		
8. NAT Exempt		
<ol> <li>AnyConnect Client Deployment</li> </ol>		
10. Summary		
	< Back Next > Cancel Help	

8. クライアントと内部のサブネット間のトラフィックは動的ネットワーク アドレス変換 (NAT)の適用が除外される必要があります。 [Exempt VPN traffic from network address translation] チェック ボックスを有効にし、適用の除外に使用される LAN インターフェイスを設 定します。 また、適用が除外されるローカル ネットワークを指定して、[Next] をクリックします

a AnyConnect VPN Connection Setup Wizard					
Steps	NAT Exempt				
1. Introduction	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.				
2. Connection Profile Identification	Exempt VPN traffic from network address translation				
3. VPN Protocols	Inside Interface is the interface directly connected to your internal				
4. Client Images	network.				
5. Authentication Methods	Inside Interface: Inside				
6. Client Address Assignme	Local Network is the network address(es) of the internal network that				
7. Network Name Resolutio	dient can access.				
Servers	Local Network: 192.168.10.0/24				
8. NAT Exempt					
<ol> <li>AnyConnect Client Deployment</li> </ol>	The traffic between AnyConnect client and internal network will be				
10. Summary	exempt from network address translation.				
< Back Next > Cancel Help					

# 9. [Next] をクリックします。

<u>a</u> /	a AnyConnect VPN Connection Setup Wizard					
Steps AnyConnect Client Deployment						
1.	1. Introduction AnyConnect client program can be installed to a client device by one of the following two methods:					
2.	<ul> <li>2. Connection Profile Identification</li> <li>1) Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed;</li> <li>2) Pre-deployment - Manually install the AnyConnect client package.</li> </ul>					
3.	VPN Protocols					
4.	Client Images					
5.	Authentication Methods					
6.	Client Address Assignme					
7.	Network Name Resolutio Servers					
8.	NAT Exempt					
9.	AnyConnect Client Deployment					
10	. Summary					
		< Back Next > Cancel He	lp			

10. 最後の手順は要約を示します。設定を完了するには、[Finish] をクリックします。

TanyConnect VPN Connecti	on Setup Wizard	X		
VPN Wizard	Summary			
Branch	Here is the summary of the configuration.			
SET I	Name	Value		
Toot ISP	Summary			
	Name/Alias of the Connection Profile	SSL_GRP		
Home	VPN Access Interface	Internet		
emorate	Device Digital Certificate	none		
Network	VPN Protocols Enabled	SSL only		
	AnyConnect Client Images	1 package		
CLARK IN ME	Authentication Server Group	LOCAL		
and the second second	Address Pool for the Client	10.10.10.1 - 10.10.10.200		
	DNS	Server: Domain Name:		
	Network Address Translation	The protected traffic is not subjected to network address translation		
[	< Back Finish	Cancel Help		

これで、AnyConnect クライアントの設定が完了しました。 ただし、構成ウィザードで AnyConnectを設定すると、認証方式が AAA にデフォルトで設定されます。 証明書およびユーザ 名とパスワードでクライアントを認証するには、認証方式として証明書と AAA を使用するように トンネル グループ(接続プロファイル)を設定する必要があります。

• [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。

•新規追加された接続プロファイル SSL\_GRP が一覧表示されます。

Device List $\Box + \times$	Configuration >	Remote Access VP	N > Network (Client)	<u>) Access</u> > <u>AnyConn</u>	ect Connection Profiles				
	The security app tunnel with Data	oliance automatically d agram Transport Layer	eploys the Cisco AnyCo Security (DTLS) tunneli	nnect VPN Client to ren ing options.	note users upon connection. The	initial die	nt deployment requires (	end-user administrative rights. The Cisco AnyConnect	VPN Client supports IPsec (IKEv2) tunnel as well as SSL
37 L	Ccess Interfaces	AnyConnect VPN Clie t be enabled if you allo	nt access on the interfa w AnyConnect client to	aces selected in the tab be launched from a bro	le below owser (Web Launch) .				
		SSL Access		IPsec (IKEv2) Access					
	Interface	Allow Access	Enable DTLS	Allow Access	Enable Client Services		Device Certificate		
Remote Access VPN 🗗 🖗	Inside					-	Port Settings		
-? Introduction	Internet		<b>V</b>			-			
Clisice Outside									
SanyConnect Customization/Localization     AnyConnect Clent Profile     AnyConnect Clent Profile     AnyConnect Clent Software     Dynamic Access Policies     Secure Policies     Secure Volitiy Solution     Secure Wolthy Solution	Corpose interface access is as for infloating why seapons Access lists for mount why seapons Access lists for group policy and user policy always apply to the traffic. Login Page Setting      Corpose access as a for infloating page.								
Advanced	Connection Profiles								
AnyConnect Essentials	Connection profile (turnel group) specifies how user is authenticated and other parameters. You can configure the mapping from certificate to connection profile here.								
AnyConnect Custom Attributes     AnyConnect Custom Attributes     AnyConnect Custom Attributes	🗣 Add 🗹 Edit 👔 Delete								
ACL Manager	Name		SSL Enabled	IP	sec Enabled		Aliases	Authentication Method	Group Policy
Clientless SSL VPN Access	DefaultRAGroup	p						AAA(LOCAL)	DfltGrpPolicy
Connection Profiles	DefaultWEBVPN	Group						AAA(LOCAL)	DfltGrpPolicy
VDI Access	ssl-grp						ssl-grp	AAA(LOCAL)	DfltGrpPolicy
	SSL_GRP		₹				SSL_GRP	AAA(LOCAL)	GroupPolicy_SSL_GRP

- AAA と証明書認証を設定するために、接続プロファイルに [SSL\_GRP] を選択して、[Edit] を クリックします。
- [Authentication Method] で、[Both] を選択します。

Edit AnyConnect Connection Profile: SSL_GRP						
Basic	Name:	SCI (CDD				
Advanced	Alassa					
	Allases:	SSL_GKP				
	Authentication					
	Method:	AAA Certificate Soth				
	AAA Server Group:	LOCAL	Manage			
		Use LOCAL if Server Group fails				
	Client Address Assignment –					
1	DHCP Servers:					
		None      DHCP Link      DHCP Subnet				
	Client Address Pools:	VPN_Pool	Select			
	Client IPv6 Address Pools:		Select			
	Default Group Policy					
	Group Policy:	GroupPolicy_SSL_GRP -	Manage			
	(Following field is an attribu	ute of the group policy selected above.)				
Enable SSL VPN dient protocol     Enable IPsec(IKEv2) dient protocol						
	WINS Servers:					
	Domain Name:					
Find:	Ne	ext OPrevious				
OK Cancel Help						

### AnyConnect 用の CLI の設定

#### !! \*\*\*\*\*Configure the VPN Pool\*\*\*\*\*

ip local pool VPN\_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0

#### !! \*\*\*\*\*Configure Address Objects for VPN Pool and Local Network\*\*\*\*\*

object network NETWORK\_OBJ\_10.10.10.0\_24
subnet 10.10.10.0 255.255.255.0
object network NETWORK\_OBJ\_192.168.10.0\_24 subnet 192.168.10.0 255.255.255.0 exit !!
\*\*\*\*\*Configure WebVPN\*\*\*\*\*

webvpn enable Internet anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1 anyconnect enable tunnel-group-list enable exit !! \*\*\*\*\*Configure User\*\*\*\*\* username user1 password mb02jYs13AX1IAGa encrypted privilege 2

#### !! \*\*\*\*\*Configure Group-Policy\*\*\*\*\*

group-policy GroupPolicy\_SSL\_GRP internal group-policy GroupPolicy\_SSL\_GRP attributes vpntunnel-protocol ssl-client dns-server none wins-server none default-domain none exit !! \*\*\*\*\*Configure Tunnel-Group\*\*\*\*\*

tunnel-group SSL\_GRP type remote-access tunnel-group SSL\_GRP general-attributes authentication-server-group LOCAL default-group-policy GroupPolicy\_SSL\_GRP address-pool VPN\_Pool tunnel-group SSL\_GRP webvpn-attributes authentication aaa certificate group-alias SSL\_GRP enable exit

#### !! \*\*\*\*\*Configure NAT-Exempt Policy\*\*\*\*\*

nat (Inside,Internet) 1 source static NETWORK\_OBJ\_192.168.10.0\_24 NETWORK\_OBJ\_192.168.10.0\_24 destination static NETWORK\_OBJ\_10.10.10.0\_24 NETWORK\_OBJ\_10.10.10.0\_24 no-proxy-arp route-lookup

### 確認

このセクションでは、設定が正常に機能していることを確認します。

**注:** 特定の show コマンドが<u>アウトプット インタープリタ ツール(登録ユーザ専用</u>)でサポ ートされています。 show コマンド出力の分析を表示するには、アウトプット インタープ リタ ツールを使用します。

CA サーバが有効であることを確認します。

#### show crypto ca server

ASA(config)# show crypto ca server Certificate Server LOCAL-CA-SERVER: Status: enabled State: enabled Server's configuration is locked (enter "shutdown" to unlock it) Issuer name: CN=ASA.local CA certificate fingerprint/thumbprint: (MD5) 32e868b9 351a1b07 4b59cce5 704d6615 CA certificate fingerprint/thumbprint: (SHA1) 6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d Last certificate issued serial number: 0x1 CA certificate expiration timer: 19:25:42 UTC Jan 8 2019 CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016 Current primary storage dir: flash:/LOCAL-CA-SERVER/

Auto-Rollover configured, overlap period 30 days Autorollover timer: 19:25:42 UTC Dec 9 2018

WARNING: Configuration has been modified and needs to be saved!! 追加後に、ユーザが登録を許可されていることを確認します。

#### \*\*\*\*\*Before Enrollment\*\*\*\*\*

ASA# show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:03:11 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Allowed to Enroll >>> Shows the status "Allowed to Enroll"

#### \*\*\*\*\*After Enrollment\*\*\*\*\*

username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: 19:05:14 UTC Thu Jan 14 2016 notified: 1 times enrollment status: Enrolled, Certificate valid until 19:18:30 UTC Tue Jan 10 2017, Renewal: Allowed CLI または ASDM のいずれかを介して AnyConnect 接続の詳細を確認できます。

#### CLI の場合

#### show vpn-sessiondb detail anyconnect

#### ASA# show vpn-sessiondb detail anyconnect

```
Session Type: AnyConnect Detailed
                                   Public IP : 1'
Username
           : user1
Assigned IP : 10.10.10.1
                                               : 10.142.189.181
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Essentials
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx
           : 13822
                                    Bytes Rx
                                             : 13299
Pkts Tx
                                    Pkts Rx
           : 10
                                                : 137
Pkts Tx Drop : 0
                                   Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSL_GRP Tunnel Group : SSL_GRP
Login Time : 19:19:10 UTC Mon Jan 11 2016
Duration
           : 0h:00m:47s
Inactivity : 0h:00m:00s
NAC Result
           : Unknown
VLAN Mapping : N/A
                                    VLAN
                                              : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
 Tunnel ID : 1.1
             : 10.142.189.181
 Public IP
 Encryption : none
                                     Hashing
                                                : none
 TCP Src Port : 52442
                                     TCP Dst Port : 443
 Auth Mode
           : Certificate and userPassword
 Idle Time Out: 30 Minutes
                                     Idle TO Left : 29 Minutes
             : Windows
 Client OS
 Client Type : AnyConnect
 Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096
 Bytes Tx : 6911
                                     Bytes Rx : 768
```

Pkts Tx : 5 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 1.2 

 Assigned IP : 10.10.10.1
 Public IP : 10.142.189.181

 Encryption : RC4
 Hashing : SHA1

 TCP Src Port : 52443 Encapsulation: TLSv1.0 Auth Mode : Certificate and userPassword TCP Dst Port : 443 Idle TO Left : 29 Minutes Idle Time Out: 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 Bytes Tx : 6911 Bytes Rx : 152 Pkts Tx : 5 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 1.3 Assigned IP : 10.10.10.1 Public IP : 10.142.189.181 Hashing : SHA1 Encryption : AES128 UDP Src Port : 59167 Encapsulation: DTLSv1.0 UDP Dst Port : 443Auth Mode: Certificate and userPasswordIdle Time Out: 30 MinutesIdle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096 : 0 Bytes Rx : 12907 Bytes Tx : 0 Pkts Tx Pkts Rx : 142 Pkts Tx Drop : 0 Pkts Rx Drop : 0 NAC: Reval Left(T): 0 Seconds EoU Age(T) : 51 Seconds Reval Int (T): 0 Seconds SQ Int (T) : 0 Seconds Hold Left (T): 0 Seconds Posture Token: Redirect URL :

#### ASDM の場合

- [モニタリング(Monitoring)] > [VPN] > [VPN 統計情報(VPN Statistics)] > [セッション (Sessions)] の順に移動します。
- [Filter By] に [All Remote Access].を選択します。
- ・選択した AnyConnect クライアントについていずれかの操作を実行できます。

Details:セッションに関する詳細情報が表示されます。

Logout : ヘッドエンドからユーザを手動でログアウトします。

Ping: ヘッドエンドから AnyConnect クライアントを ping します。

# トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

**注**: <u>debug</u> コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください 。

注意: ASA では、さまざまなデバッグ レベルを設定できます。 デフォルトでは、レベル 1 が使用されます。 デバッグ レベルを変更すると、デバッグの冗長性が高くなる場合があり ます。 特に実稼働環境では、注意して実行してください。

- debug crypto ca
- debug crypto ca server
- debug crypto ca messages
- debug crypto ca transactions
- debug webvpn anyconnect

次のデバッグ出力は、CA サーバが no shut コマンドを使用して有効にされている場合に示されま す。

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255

CRYPTO\_CS: input signal enqueued: no shut >>>> Command issued to Enable the CA server Crypto CS thread wakes up!

CRYPTO\_CS: enter FSM: input state disabled, input signal no shut CRYPTO\_CS: starting enabling checks CRYPTO\_CS: found existing serial file. CRYPTO\_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019 CRYPTO\_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate CRYPTO\_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO\_CS: DB version 1 CRYPTO\_CS: last issued serial number is 0x4 CRYPTO\_CS: closed ser file CRYPTO\_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl CRYPTO\_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl CRYPTO\_CS: CRL file LOCAL-CA-SERVER.crl exists. CRYPTO\_CS: Read 220 bytes from crl file. CRYPTO\_CS: closed crl file CRYPTO\_PKI: Storage context locked by thread Crypto CA Server

CRYPTO\_PKI: inserting CRL CRYPTO\_PKI: set CRL update timer with delay: 20250 CRYPTO\_PKI: the current device time: 18:05:17 UTC Jan 16 2016

CRYPTO\_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016 CRYPTO\_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016 CRYPTO\_PKI: CRL cache delay being set to: 20250000 CRYPTO\_PKI: Storage context released by thread Crypto CA Server

CRYPTO\_CS: Inserted Local CA CRL into cache!

CRYPTO\_CS: shadow not configured; look for shadow cert CRYPTO\_CS: failed to find shadow cert in the db CRYPTO\_CS: set shadow generation timer CRYPTO\_CS: shadow generation timer has been set CRYPTO\_CS: Enabled CS. CRYPTO\_CS: exit FSM: new state enabled CRYPTO\_CS: cs config has been locked.

Crypto CS thread sleeps!

次のデバッグ出力はクライアントの登録を示します。

ASA# debug crypto ca 255 ASA# debug crypto ca server 255 ASA# debug crypto ca message 255 ASA# debug crypto ca transaction 255

CRYPTO\_CS: writing serial number 0x2. CRYPTO\_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO\_CS: Writing 32 bytes to ser file CRYPTO\_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

#### 次の条件が発生している場合、クライアントの登録が失敗する場合があります。

#### シナリオ 1.

#### ・ユーザは、登録する許可なしで CA サーバ データベースに作成されます。

<sub>1</sub> Add User		×
Username:	user 1	
Email ID:	user 1@cisco.com	
Subject (DN String):	CN=user 1,OU=TAC	Select
Allow enrollment		
L	Add User Cancel Help	

### CLIの同等の設定:

ASA(config) # show crypto ca server user-db username: user1 email: user1@cisco.com dn: CN=user1,OU=TAC allowed: <not allowed> notified: 0 times enrollment status: Not Allowed to Enroll

• ユーザが登録を許可されていない場合、ユーザの OTP を生成するかまたは電子メールで送信 しようとすると、このエラー メッセージが出されます。



#### シナリオ 2.

- show run webvpn コマンドを使用して、登録ポータルが使用可能になっているポートおよび インターフェイスを確認します。 デフォルト ポートは 443 ですが、変更可能です。
- クライアントが、登録ポータルへのアクセスを成功させるために使用されるポートで、 webvpn が有効になっているインターフェイスの IP アドレスへのネットワーク到達可能性が あることを確認します。

次のような場合、クライアントは ASA の登録ポータルにアクセスできないことがあります。

- 1. 中間デバイスが、クライアントから指定されたポート上の ASA の webvpn IP への着信接続 をブロックする場合。
- 2. webvpn が有効になっているインターフェイスの状態がダウンしている場合。
- この出力は、登録ポータルをカスタム ポート 4433 のインターフェイス Internet の IP アドレ スで使用できることを示しています。

```
ASA(config) # show run webvpn
webvpn
port 4433
enable Internet
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

### シナリオ 3.

- CA サーバ データベース ストレージのデフォルトの場所は、ASA のフラッシュ メモリです
- •登録時にユーザの pkcs12 ファイルを生成して保存する空き領域がフラッシュ メモリにある ことを確認します。
- フラッシュメモリに十分な空き領域がない場合、ASA はクライアントの登録プロセスの完了
   に失敗し、次のデバッグログが生成されます。

ASA(config)# debug crypto ca 255 ASA(config)# debug crypto ca server 255 ASA(config)# debug crypto ca message 255 ASA(config)# debug crypto ca transaction 255 ASA(config)# debug crypto ca trustpool 255 CRYPTO\_CS: writing serial number 0x2. CRYPTO\_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser CRYPTO\_CS: Writing 32 bytes to ser file CRYPTO\_CS: Generated and saving a PKCS12 file for user user1 at flash:/LOCAL-CA-SERVER/user1.p12

CRYPTO\_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.

CRYPTO\_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO\_CS: Failed to process enrollment in-line for user user1. status: -1

# 関連情報

- <u>Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス</u>
- AnyConnect VPN クライアントのトラブルシューティング ガイド 一般的な問題
- AnyConnect セッションの管理、モニタリング、およびトラブルシューティング
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>