ベルギーの elD カードを使った ASA 8.x Anyconnect の認証

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 表記法 背景説明 ローカル PC のセットアップ オペレーティング システム カード リーダー elD ランタイム ソフトウェア 認証証明書 AnyConnect のインストール ASA の要件 ASA の設定 <u>手順1:外部インターフェイスを有効にする</u> 手順2:ドメイン名、パスワード、システム時刻を設定する 手順 3: 外部インターフェイスで DHCP サーバを有効にする 手順4:elD VPN アドレス プールを設定する 手順 5: ベルギーのルート CA 証明書をインポートする 手順6:セキュア ソケット レイヤを設定する 手順7:デフォルトのグループポリシーを定義する <u>手順8:証明書マッピングを定義する</u> 手順 9: ローカル ユーザを追加する 手順 10: ASA を再起動する 微調整 簡単設定 関連情報

<u>概要</u>

このドキュメントでは、ASA 8.x の Anyconnect 認証を設定して、ベルギーの elD のカードを使 用する方法について説明します。

<u>前提条件</u>

このドキュメントに特有の要件はありません。

<u>使用するコンポーネント</u>

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。

• 適切な ASA 8.0 ソフトウェアを搭載する ASA 5505

AnyConnect Client

• ASDM 6.0

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、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『<u>シスコ テクニカル ティップスの表記法』を参照してください。</u>

<u>背景説明</u>

eID は、ユーザがリモート Windows PC 上で認証するために使用する必要のあるベルギー政府発行の PKI (公開キー インフラストラクチャ)カードです。AnyConnect ソフトウェア クライアントは、ローカル PC にインストールされ、リモート PC から認証クレデンシャルを取得します。認証が完了すると、リモート ユーザは完全な SSL トンネルを経由して中央にあるリソースにアクセスできます。リモート ユーザは ASA が管理するプールから取得される IP アドレスでプロビジョニングされます。

<u>ローカル PC のセットアップ</u>

<u>オペレーティング システム</u>

ローカル PC 上のオペレーティング システム(Windows、Mac OS、Unix、または Linux)は、必要なすべてのパッチがインストールされた最新の状態にしておく必要があります。

<u>カード リーダー</u>

eID カードを使用するためには、ローカル コンピュータに電子カード リーダーを設置する必要が あります。電子カード リーダーとは、コンピュータ上のプログラムと ID カード上のチップの間 に通信チャネルを確立するハードウェア デバイスのことです。

承認済みカード リーダーのリストについては、次の URL を参照してください。 <u>http://www.cardreaders.be/en/default.htm</u>

注:カードリーダを使用するには、ハードウェアベンダーが推奨するドライバをインストールす る必要があります。

elD ランタイム ソフトウェア

ベルギー政府が提供する elD ランタイム ソフトウェアをインストールする必要があります。この ソフトウェアを使用すると、リモート ユーザが elD カードのコンテンツを読み取り、検証し、印 刷することができます。このソフトウェアは、フランス語版とオランダ語版の Windows、Mac OS X、および Linux で使用できます。

詳細については、次の URL を参照してください。

http://www.belgium.be/zip/eid_datacapture_nl.html

認証証明書

ローカル PC で Microsoft Windows ストアに認証証明書をインポートする必要があります。証明 書をストアにインポートできない場合は、AnyConnect クライアントが ASA への SSL 接続を確 立できません。

手順

認証証明書を Windows ストアにインポートするには、次の手順を実行します。

1. elD をカード リーダーに挿入し、ミドルウェアを起動して、elD カードの内容にアクセスします。elD カードの内容が表示されます。

📫 Carte d'identité					
Centilicats Carte & PIN Options	: Info				
BELGIQUE CARTE D'IDENTITE	BELGIË IDENTITEITSKAART	BELGIEN PERSONALAUSWEIS	BEI IDE	LGIUM INTITY CARD	
	Identité Nom				
	Piénoms	Data da anticasa	fare	Matazalté	Е
	Lieu de naissance Titre	14/04/1963	M Numéro national	be	
Carte Numéro de la curse	Adresse		63.04.14-033.25		
534C494E336600296CFF27150718 Numéro de la carte	32C36 Code postal Commune			Pays	
590.5942800.24 Valide du Au 07/06/2007 07/06/2012	Statut spécial			De	
Commune d'émission	Canne jaune	- *			
			<u>*</u>	12 m	
				E.	
Fri				ACTA	1

2. [Certificats](フランス語)タブをクリックします。証明書の階層が表示されます。

📾 Carte d'identité		
6 □ 😂 🖬 🚳 🗙 Identité Certificats Carte & PIN Options Info		
Certificats		
BELPIC Belgium Root CA	Propriétaire (Authe	entication)
Citizen CA	Émetteur Citizen CA	
(Signature)	Longueur de clé 1024 bits	
	Valide du 15/06/2007	Au 08/06/2012
	Statut du certificat Non validé	
	Les certificats de la carte utiliser la carte d'identité i OpenOffice.org. Adobe R sélectionnez-le et cliquez	eID doivent être enregistrés dans Windows pour pouvoir électrorique dans Internet Explorer, Microsoft Office, leader, Outlook, Pour enregistrer un certificat, sur le bouton « Enregistrer ». Enregistrer Détails >>
Fn		

- 3. [Belgium Root CA] を展開し、[Citizen CA] を展開します。
- 4. 名前付き証明書の [Authentication] バージョンを選択します。
- 5. [Enregistrer](フランス語)ボタンをクリックします。証明書が Windows ストアにコピーされます。

注:[詳細]ボタンをクリックすると、証明書の詳細を表示するウィンドウが表示されます。 [Details] タブで [Subject] フィールドを選択して、[Serial Number] フィールドを表示します。 [Serial Number] フィールドには、ユーザ認証に使用される固有の値が表示されます。例えば、シ リアル番号「56100307215」は、生年月日が1956年10月3日で、シーケンス番号が072で小切手 番号が15のユーザーを表します。これらの番号を保存するには、連邦当局からの承認を要求する 必要があります。いずれかの国でベルギー市民のデータベースを維持する際は、所定の方法で公 式に通知してください。

確認

証明書が正常にインポートされたことを検証するには、次の手順を実行します。

- 1. Windows XP マシンで DOS ウィンドウを開き、**mmc コマンドを入力します。**Console アプ リケーションが表示されます。
- 2. [File] > [Add/Remove Snap-in] を選択します(または Ctrl を押した状態で M を押します)。 [Add/Remove Snap-in] ダイアログボックスが表示されます。
- 3. [Add] ボタンをクリックします。[Add Standalone Snap-in] ダイアログボックスが表示され ます。
- 4. [Available Standalone Snap-ins] リストから [Certificates] を選択し、[Add] をクリックします。
- 5. [My user account] **オプション ボタンをクリックし、[Finish] をクリックします。** [Add/Remove Snap-in] ダイアログボックスに [Certificate snap-in] が表示されます。

- 6. [Close] をクリックして [Add Standalone Snap-in] ダイアログボックスを閉じたら、 [Add/Remove Snap-in] ダイアログボックスで [OK] をクリックし、Console アプリケーショ ンに戻ります。
- 7. [Console Root] フォルダ下の [Certificates Current User] を展開します。
- 8. [Personal] を展開してから、[Certificates] を展開します。次の図のように、インポートされ た証明書が Windows ストアに表示されます。

🚡 Console1 - [Console Root\Certific	ates - Current User/Personal\Ce	rtificates]			X				
File Action View Favorites Window Help									
Console Root	Issued To /	Issued By	Expiration Date	Intended Purposes	Frier				
Certoricates - Current Oser Personal Certificates Trusted Root Certification Author Enterprise Trust Intermediate Certification Author Active Directory User Object Other Trusted People Other Other Certificate Enrolment Requests	(Authentication)	Citizen CA	8/06/2012	Client Authentication	Clé c				
	<				>				
Personal store contains 1 certificate.									

AnyConnect のインストール

リモート PC に AnyConnect クライアントをインストールする必要があります。AnyConnect ソフトウェアは、編集可能な XML 設定ファイルを使用して、使用可能なゲートウェイのリストを プリセットします。XML ファイルはリモート PC 上の次のパスに保存されます。

C:\Documents and Settings\%USERNAME%\Application Data\Cisco\Cisco AnyConnect VPN Client

ここで %USERNAME% は、リモート PC 上のユーザ名です。

XML ファイルの名前は preferences.xml です。以下はファイルの内容の例です。

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectPreferences> <DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences> ここで 192.168.0.1 は ASA ゲートウェイの IP アドレスです。



ASA が次の要件を満たしていることを確認します。

 AnyConnect と ASDM はフラッシュで実行する必要があります。このドキュメントの手順を 完了するには、適切な ASA 8.0 ソフトウェアがインストールされている ASA 5505 を使用し てください。AnyConnect および ASDM アプリケーションをフラッシュにプリロードする必 要があります。show flash コマンドを使用して、フラッシュの内容を確認します。
 ciscoasa#show flash:

-#	length	date/time	path
66	14524416	Jun 26 2007 10:24:02	asa802-k8.bin
67	6889764	Jun 26 2007 10:25:28	asdm-602.bin
68	2635734	T11 09 2007 07:37:06	anyconnect-win-2.0.0343-k9.pk

ASA は工場出荷時の初期状態で実行する必要があります。このドキュメントの手順を完了するために新しい ASA シャーシを使用する場合は、この要件を省略できます。それ以外の場合は、次の手順に従って、ASA を工場出荷時の初期状態にリセットします。ASDM アプリケーションで ASA シャーシに接続し、[File] > [Reset Device to the Factory Default Configuration]を選択します。



テンプレートのデフォルト値をそのまま使用します。イーサネット 0/1 内部インターフェイ スで PC を接続し、ASA の DHCP サーバによってプロビジョニングされる IP アドレスを更 新します。注:コマンド行からASAを工場出荷時のデフォルトにリセットするには、次のコ マンドを使用します。

ciscoasa#**conf** t

ciscoasa#config factory-default 192.168.0.1 255.255.255.0

<u>ASA の設定</u>

ASA を工場出荷時の初期状態にリセットしたら、192.168.0.1 で ASDM を開始して、イーサネット 0/1 の内部インターフェイスで ASA に接続します。

注:以前のパスワードは保持されます(デフォルトでは空白になります)。

デフォルトでは、ASAはサブネット192.168.0.0/24内の送信元IPアドレスを使用して着信管理セッションを受け入れます。ASAの内部インターフェイスで有効なデフォルトのDHCPサーバは、192.168.0.2 ~ 129/24の範囲のIPアドレスをを提供します。

ASA を設定するには、次の手順を実行します。

- 1. <u>外部インターフェイスを有効にする</u>
- 2. <u>ドメイン名、パスワード、システム時刻を設定する</u>
- 3. <u>外部インターフェイスで DHCP サーバを有効にする</u>
- 4. <u>eID VPN アドレス プールを設定する</u>
- 5. <u>ベルギーのルート CA 証明書をインポートする</u>
- 6. <u>セキュア ソケット レイヤを設定する</u>
- 7. <u>デフォルトのグループ ポリシーを定義する</u>
- 8. 証明書マッピングを定義する
- 9. <u>ローカル ユーザを追加する</u>
- 10. <u>ASA を再起動する</u>

<u>手順1:外部インターフェイスを有効にする</u>

この手順では、外部インターフェイスを有効にする方法について説明します。

- 1. ASDM アプリケーションで [Configuration] をクリックし、[Device Setup] をクリックします
- 2. [Device Setup] 領域で [Interfaces] を選択し、[Interfaces] タブをクリックします。

Cisco ASDM 6.0 for ASA - 192,168	.0.1								
File View Tools Wizards Window He	*	0		0	Look	For:		And +	ahaha
Home Og Configuration O Monitori	ng 🐻 Sa	re Q Refresh 😡	Back O Forward	- Help					cisco
Device List d ¹ P ×	Configural	ion > Device Setup > I	interfaces						0
Add Toelete S Connect	Interface	Switch Ports							
192.160.0.1	Name	Switch Ports	Enabled	Security	IP Address	Subnet Mask	Restrict	VLAN	
	inside	Ethernet0/1, Ethernet	10/2, Et Ves	Level	192.168.0.1	255,255,255,0	Traffic floer	vlant	Add
	outside	Ethernet0/0	Yes	0	197.0.100.1	255.255.255.0		vlan2	EdR
									Delete
Device Setup 57 Q ×									
g ⁹ Startup Wizard									
■ •§• Routing									
Povice Name/Password									
🗈 🎯 System Time	3								
B Device Setup									
Sig Firewal									
Remote Access VPN	-								
	Enable	traffic between two or	more interfaces which	are configure	d with same see	curity levels			
500-50-500 VPM	Enable	traffic between two or	more hosts connected	to the same in	nterface				
Device Management									
				App	NY R	eset			
······									
Device configuration loaded successfully.					<admin></admin>	15	🕺 🛃 🚮	27	/07/07 8:35:14 UTC

- 3. 外部インターフェイスを選択し、[Edit] をクリックします。
- 4. [General] タブの [IP address] セクションで [Use Static IP] オプションを選択します。
- 5. IP アドレスとして **197.0.100.1 と入力し、サブネット マスクとして 255.255.255.0 と入力** します。
- 6. [Apply] をクリックします。

<u>手順2:ドメイン名、パスワード、システム時刻を設定する</u>

この手順では、ドメイン名、パスワード、およびシステム時刻を設定する方法について説明しま す。

1. [Device Setup] 領域で [Device Name/Password] を選択します。

🛍 Cisco ASDM 6.0 for ASA - 192.168	.0.1			
File View Tools Wizards Window H	de	Look For:	End +	ahaha
Home 🔏 Configuration 📴 Monitor	ng 🔚 Save 💽 Refresh 🔇 Back 🚫	Forward 🧖 Help		CISCO
Device List of P ×	Configuration > Device Setup > Device Ram	e.Password		0
Add 📋 Delete 💕 Connect	Hostname and Domain Name			
A192.160.0.1	Hostname: ciscoasa			
	Domain Name: cisco.be			
	Enable Password			
	Change the privileged mode password.			
Device Setup 67 Q ×	Old Password:			
9 ⁹ Startup Wizard	New Password: *******			
Interfaces Interfaces Interfaces	Confirm New Password: *******			
Device Name/Password System Time	Teinet Password			
	Change the password to access the cons	ole of the security appliance.		
	Old Password:			
	New Password			
	Confirm New Password:			
- Device Setup				
Ermal				
OR Describe Access URM				
Concept Access with				
Ste-to-Ste VPN				
Device Management				
		Apply Reset		
Device configuration loaded successfully.		<admin> 15</admin>		7/07/07 8:36:04 UTC

- 2. ドメイン名としてcisco.beと入力し、[イネーブルパスワード]の値としてcisco123と入力しま す。注:デフォルトでは、パスワードは空白です。
- 3. [Apply] をクリックします。
- 4. [Device Setup] 領域で [System Time] を選択し、必要に応じてクロックの値を変更します。
- 5. [Apply] をクリックします。

<u>手順3:外部インターフェイスでDHCPサーバを有効にする</u>

この手順では、外部インターフェイスで DHCP サーバを有効にして、テストを効率よく実行する 方法について説明します。

- 1. Configuration をクリックし、次に Device Management をクリックします。
- 2. [Device Management] 領域で [DHCP] を展開し、[DHCP Server] を選択します。

G Cisco ASDM 6.0 for ASA - 192.168	.0.1							
File Wew Tools Wizards Window He	Np.			Look	For:		Find +	alada
Home 🔏 Configuration 🕖 Monitori	ng 📊 Save	Q Refresh	Back 🚫 Forward	💡 ныр				cisco
Device List an A ×	Configuration	n > Device Manag	ement > DHCP > DHCP S	erver				
🗣 Add 📋 Delete 🔊 Connect	Interface	DHCP Enabled	Address Pool	DNS Servers	WINS Servers	Domain Name	Ping Timeout U	Edk
192.160.0.1	inside	Yes	192.168.0.2 - 192.168.	0.129				
Device Management Imagement Access Imagement Access VPN Imagement Access VPN	Clobal DHCP Clobal DHCP Enables Enabling au tais proced DNS Server DNS Server Domain Nan Lease Lengi Ping Timeou Ping Timeou Dynamic DM Update	Yes Poptions auto-configuration ca fence over the auto file 22: 11 22: 12 12 13 14 15 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	from interface: Duts	00.30 Allow VPN override atomatically configure DNS, WINS Server:	, WINS and the d	efault domain na	me. The values in th	ve fields below
				Apply R	eset			
Running configuration successfully saved to flas	h memory.			<admin></admin>	15	😡 🛃	🙆 2	7/07/07 8:48:04 UTC

- 3. インターフェイス リストから外部インターフェイスを選択し、[Edit] をクリックします。 [Edit DHCP Server] ダイアログボックスが表示されます。
- 4. [Enable DHCP Server] チェックボックスをオンにします。
- 5. DHCP の [Address Pool] に IP アドレスとして 197.0.100.20 ~ 197.0.100.30 を入力します。
- 6. [Global DHCP Options] 領域の [Enable auto-configuration from interface] チェックボックス をオフにします。
- 7. [Apply] をクリックします。

<u> 手順 4:elD VPN アドレス プールを設定する</u>

この手順では、リモート AnyConnect クライアントをプロビジョニングするために使用する IP ア ドレスのプールを定義する方法について説明します。

- 1. Configuration をクリックし、次に Remote Access VPN をクリックする。
- 2. [Remove Access VPN] 領域で [Network (Client) Access] を展開し、[Address Assignment] を 展開します。
- 3. [Address Pools] を選択し、[Configure named IP Address pools] 領域にある [Add] **ボタンを クリックします。**[Add IP Pool] ダイアログボックスが表示されます。

📫 Cisco ASDM 6.0 for ASA - 192.168	.0.1					- C 🛛
File View Tools Wizards Window H	elp			Look For:	Find +	alada
Home Configuration D Monitor	ing 🔒 Save 🔇 Refre	sh 🔇 Back 🔘 Forwa	d 🥐 Help			cisco
Device List d ^a P ×	Configuration > Remote	Access VPH > Hetwork (Client) Access > Ad	dress Assignment >	Address Pools	
Add 📋 Delete 🖋 Connect	Configure named IP Add	tress pools.				
192.168.0.1	This second as is sefer					
	this parameter is enror	ced in eicher a ven proc co	DECEMPTOR, 2A. P.	A CONSCIONDRUME OF	2000 DORY COMPLETEDOR.	
	◆ Add @ Edt @	Delete				
	Pool Name	Starting Address		Ending Address	Subnet Mask	
						100
Remote Access VPN & P ×		Add IP Pool		×		
E Network (Client) Access						
SSL VPN Connection Profiles						
IPsec Connection Profiles			-	-		
Group Policies		Name:	eID-VPNPOOL			
Oynamic Access Polices						
Assignment Policy		Starting IP Address:	192.168.10.100			
Address Pools			-			
🖃 📆 Advanced		Ending IP Address:	192.168.10.110			
Clentless SSL VPN Access						
Easy VPN Remote		Subnet Mask:	255.255.255.0	~		
E Saura Daditro Managar				1000 0000 0000		
Certificate Management						
P DHCP Server						
		OK	Cancel Help			
Device Setup				_		30. BR (2. BR)
Frewal	1000 C					
Remote Access VPN						
Ste-to-Ste VPN						
Device Management						
			Apply	Reset		
			<8	dmin> 15	😡 🔐 🛛 🙆 2	7/07/07 8:53:04 UTC

- 4. [Name] フィールドに eID-VPNPOOL と入力します。
- 5. [Starting IP Address] フィールドと [Ending IP Address] フィールドに、IP アドレスの範囲 192.168.10.100 ~ 192.168.10.110 を入力します。
- 6. [Subnet Mask] ドロップダウン リストから [255.255.255.0] を選択し、[OK] をクリックして、[Apply] をクリックします。

<u>手順 5 : ベルギーのルート CA 証明書をインポートする</u>

この手順では、ベルギーのルート CA 証明書を ASA にインポートする方法について説明します。

- 1. ベルギーのルート CA 証明書(belgiumrca.crt および belgiumrca2.crt)を政府の Web サイト からローカル PC にダウンロードし、保存してインストールします。ベルギー政府の Web サイトは次の URL にあります。<u>http://certs.eid.belgium.be/</u>
- 2. [Remote Access VPN] 領域で [Certificate Management] を展開し、[CA Certificates] を選択 します。
- 3. [Add] をクリックして、[Install from file] をクリックします。
- 4. ベルギーのルートCA証明書(belgiumrca.crt)ファイルを保存した場所を参照し、[証明書のインストール]をクリ**ックします**。
- 5. 変更を保存するには、[適用(Apply)]をクリックします。
- 次の図は、ASA にインストールされた証明書です。



<u> 手順 6 : セキュア ソケット レイヤを設定する</u>

この手順では、安全な暗号化オプションに優先順位を付け、SSL VPN クライアント イメージを 定義し、接続プロファイルを定義する方法について説明します。

1. 最も安全な暗号化オプションを優先順位付けします。[Remote Access VPN] 領域で [Advanced] を展開し、[SSL Settings] を選択します。[Encryption] セクションで [Active Algorithms] が次のように上から順にスタックされます。AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1

Gisco ASDM 6.0 for ASA - 192.168	8.0.1	nerender og ekster, sje verstaderer i som som e	وجرائب مريشتين والمرابع فالشارية فريتي	en en senten el escontralmentrario de analismente de la mene de que el contro de	
File Wew Tools Wizards Window H	lelp			Look For: Find +	alada
Home 🖧 Configuration 🗾 Monitor	ing 🔚 Save 🔇 Refresh	😮 Back 🚫 Forward 🤺	? Help	and a set of a state of the set o	cisco
Device List d ¹ P ×	Configuration > Remote Ac	cess VPN > Advanced > SS	Settings		0
◆ Add Delete Ø Connect Delete Ø Connect	Configure SSL parameters. Th	ese parameters affect both AS	IOM and SSL VPN acc	ess.	
-	Server SSL Version: Any	Client 53, Versi	on: Any 💌		
	Encryption				
	Available Algorithms		C cc lbb	Active Algorithms	Novello
	RC4	I-MD5		AES256-5HA1	
	DES	-SHA1	<< Remove	AE5128-SHA1	Move Down
Remote Access VPN 🗗 🗘 🗡	100			30E5-SHA1	Contractor Contractor
Clentless SSL VPN Access	1.000			RC4-SHA1	
G Easy VPN Remote	12				
🗄 💣 AAA Setup	C 10-1-				
B Secure Desktop Manager	Certificates				1.000
Certificate Management	Specify which certificates, if	any, should be used for SSL a	uthentication on eac	h interface. The failback certificate will be used on interfa	ices not
DHCP Server	associaced with a ceronicate	or their own.			
E DNS	Interface		ID Certifical	te	Edk
E 123 Advanced	inside				
• Connection Gateway	outside				
Castificate to ED 1011 Cases					Section Section
NTTO Dedrest	100				
Maximum SQ VSN Servicer					
E-mail Provy					
< >					
Revice Setup					
🖏 Frowal					
Remote Access VPN					
Ste-to-Site VPN					
Device Management	Falbari Cartificata: 🔤 Kim	u]			
:			Apply	Reset	
Running configuration successfully saved to fla	sh memory.		cadmir	> 15 😡 🛃 🙆	27/07/07 8:57:34 UTC

 AnyConnect クライアントの SSL VPN クライアント イメージを定義します。[Remote Access VPN] 領域で [Advanced] を展開し、[SSL VPN] を展開し、[Client Settings] を選択し ます。[SSL VPN Client Images] 領域で [Add] をクリックします。フラッシュに保存される AnyConnect パッケージを選択します。次の図のように AnyConnect パッケージが [SSL VPN Client Images] リストに表示されます。

📫 Cisco ASDM 6.0 for ASA - 192.	168/100/254	
File View Tools Wizards Window	Help Look For: Find +	ahaha
Home 🖧 Configuration 📴 Mo	ntoring 🔚 Save 🔃 Refresh 🕓 Back 🚫 Forward 🧳 Help	cisco
Device List 51 9 ×	Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings	0
🗣 Add 📋 Delete 🖋 Connect	Identify SSL VPN Client (SVC) related files.	
A 192.168.0.1	SGLWIN Client Images	
a list list in the set	Minimize connection setup time by moving the image used by the nost commonly encountered operation system to the top of the list.	
	Add Di Replace Delete + Move UP & Move Down	
	Add Incompartment and 2 0 0243 July Na	
	na meno para prova a movem e nevera de constructiva para p	
Remote Access VPH 67 9 ×		
Network (Client) Access		
 SSL VPN Connection Profiles IPsec Connection Profiles 		
Group Policies		
Dynamic Access Policies	SSL WPN Client Profiles	<u></u>
Assignment Policy	💠 Add 🦉 Edt 🏢 Delete	
Address Pools	Name Package	
Kovanced Kovanced Kovanced Kovanced Kovanced		
🗃 🙀 SSL VPN		
Client Settings		
I Ing IPsec		
R Device Setup		
📆 Firewal	SSL VPN Client Localization File	
Remote Access VPN	To set the Localization file go to Language Localization,	
Ste-to-Site VPN	Cache File System (to hold CSD and SVC images)	
Device Management	Maximum Size: 20 MB	
	Apply Reset	
	<admin> 15 🔯 🔂 🔂 25/</admin>	07/07 23:20:54 UTC
🌆 start 🔰 📴 🕹 🥥 😣	🛐 🦈 🖆 a Wind 🛐 2003Ho 📷 CriwiteD 👩 Caso A5 🌺 2 Infan 🔂 TextRed 🤞	S # 10.00

3. DefaultWEBVPNGroup 接続プロファイルを定義します。[Remote Access VPN] 領域で [Network (Client) Access] を展開し、[SSL VPN Connection Profiles] を選択します。[Access Interfaces] 領域で [Enable Cisco AnyConnect VPN Client] チェックボックスをオンにします 。次の図のように、外部インターフェイスの [Allow Access]、[Require Client Certificate]、 および [Enable DTLS] チェックボックスをオンにします。

Cisco ASDM 6.0 for ASA - 192.168	.100.254								
File View Tools Wizards Window H	elp		And the second second	Look For:	Find +	alate			
😚 Home 🖧 Configuration 📴 Monitoring 🔚 Save 🗨 Refresh 🔇 Back 🚫 Porward 🦻 Help									
Device List a P ×	Configuration > Re	mote Access VPH > N	etwork (Client) Access > SSI	VPN Connection Profile	5	0			
🗣 Add 📋 Delete 🖋 Connect	dd 👔 Delete 🖉 Connect The security appliance automatically devices the Cisro AnnoConnect VPN Clert or lensery SSI VPN Clert to sample users us								
■ 192.160.0.1	deployment requir Security (DTLS) tu	es end-user administrati nneling options.	ve rights. The Cisco AnyConnect	VPN Client supports the HT	IPS/TCP (SSL) and Datagram Trans	sport Layer			
	(More client-relati	ed parameters, such as	client images and client profiles, o	an be found at a state of the	.)				
	Access Interfaces								
Remote Access VPN @ Q ×	Enable Cisco A	nvConnect VPN Client o	r legacy SSL VPN Client access on	the interfaces selected in t	he table below				
B Network (Client) Access	Tabulan .		Description Charle Contribute	Parkla P. D.	7				
39. VPN Connection Profiles	outside	Allow Access	Require Clerk Certificate	Enable DILS					
IPsec Connection Profiles	inside		m						
Group Policies									
Address Assignment									
Advanced	100								
Clentless SSL VPN Access	Access Port: 443	DTLS Por	t: 443						
Connection Profiles									
Portal	Click here to Asse	in Certificate to Interfac	2						
De Dupanic Access Dolicies									
Advanced	Connection Profile								
Encoding 💉	Connection profile	(tunnel group) table bel	ow contains records that determ	ine connection policies. A re	cord identifies a default group polic	cy for the			
C Internet Statements S	connection and co	ntains protocol-specific (connection parameters.			1.			
0	🗣 Add 🛃 Edit	T Delete							
Device Setup	Name	Alases	SSL VPN	Client Protocol	Group Policy	1			
Preval	DefaultWEBVPNG	roup	Enabled		OfItGrpPolicy				
	DefaultRAGroup		Enabled		DflbGrpPolicy				
Remote Access VFN									
Ste-to-Site VPN									
Device Management	Allow user to s	elect connection. ideniti	fied by alias in the table above. a	it loain bade					
:			Apply	Reset					
			ca	dmin> 15	😡 🚱 🛛 🙆 2	6/07/07 0:20:25 UTC			

[Connection Profiles] 領域で [DefaultWEBVPNGroup] を選択し、[Edit] をクリックします。 [Edit SSL VPN Connection Profile] ダイアログボックスが表示されます。

۵	🖆 Edit SSL VPN Connection Profile: DefaultWEBVPNGroup									
	Basic	Name: Aliases:	DefaultWEBVPNGroup							
		Authentication								
		Method:	◯ AAA ③ Certificate ◯ Both							
		AAA Server Group:	LOCAL	Manage						
			Use LOCAL If Server Group fails							
		Client Address Assigne	ent							
		DHCP Servers:								
		Client Address Pools:		Select						
		Default Group Policy -								
		Group Policy:	DfkGrpPolicy	Manage						
		SSL VPN Client Protocol:	C Enabled							
		ОК	Cancel Help							

ナビゲーション領域で [Basic] を選択します。[Authentication] 領域で [Certificate] オプショ

ンボタンをクリックします。[Default Group Policy] 領域で [SSL VPN Client Protocol] チェ ックボックスをオンにします。[Advanced] を展開し、[Authentication] を選択します。[Add] をクリックし、次の図のように外部インターフェイスをローカル サーバ グループとともに 追加します。

📬 Edit SSL VPN Connecti	on Profile: Default	WEBVPNGroup		×
Basic Advanced General	Interface-Specific	Authentication Server Group	15	
Client Addressing Authentication Accounting SSL VPN	Interface outside	Server Group LOCAL	Fallback to LOCAL	
	ОК	Cancel Hel	P	

ナビゲーション領域で [Authorization] を選択します。[Default Authorization Server Group] 領域で [Server Group] ドロップダウン リストから [LOCAL] **を選択し、[Users must exist in the authorization database to connect] チェックボックスをオンにします。**[User Name Mapping] 領域で [Primary DN Field] ドロップダウン リストから [SER (Serial Number)] **を選 択し、[Secondary DN Field] で [None]** を選択し、[OK] をクリックします。

🕵 Edit SSL VPN Connectio	ion Profile: DefaultWEBVPNGroup	×				
Basic Advanced General Client Addressing Authentication Authorization Accounting SSL VPN	Default Authorization Server Group Server Group: LOCAL Users must exist in the authorization database to connect Interface-specific Authorization Server Groups Add Content Content					
	Interface Server Group					
	User Name Mapping Use the entire DN as the username Specify individual DN fields as the username Primary DN Field: SER (Serial Number)					
	Secondary DN Field: None					

<u> 手順 7:デフォルトのグループ ポリシーを定義する</u>

この手順では、デフォルトのグループ ポリシーを定義する方法について説明します。

1. [Remote Access VPN] 領域で [Network (Client) Access] を選択し、[Group Policies] を選択 します。

Cisco ASDM 6.0 for ASA - 192.168	8.0.1							
File View Tools Wizards Window H	wp		Look Por:	Find -	ahaha			
Home Configuration Monitor	ring 🔚 Save 🔇 Refresh 🔇 8	Sack 🔘 Forward 🧳 He	P		cisco			
Device List 0 9 X	Configuration > Remote Access V	/PN > Network (Client) Acco	ss > Group Policies					
192.160.0.1	Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADBUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.							
	🗣 Add - 📑 Edit 🏢 Deiste							
	Name DRIGREPalicy (System Delay)	Type	Tunneling Protocol	AAA Server Group				
	and a surf of provide stated		ben a sederate sederately.					
Remote Access VPH & Q ×								
Network (Client) Access								
IPsec Connection Profiles								
Dynamic Access Policies								
Address Assignment Advanced								
Clentless SSL VPN Access Easy VPN Remote								
B AAA Setup								
Gertificate Management								
DHCP Server								
Advanced								
Bevice Setup								
🕄 Frowal								
Remote Access VPN								
Ste-to-Site VPN								
Device Management								
:			Apply Reset					
			cadmin> 15	27	07/07 15:23:14 UTC			

- 2. グループ ポリシーのリストから [DfltGrpPolicy] **を選択し、[Edit] を選択します。** 3. [Edit Internal Group Policy] ダイアログボックスが表示されます。

🜃 Edit Internal Group Po	licy: DfltGrpPoli	sy				X
General	Name:	OfltGrpPoli	CY			
⊟ Advanced	Banner:					
Split Tunneling IE Browser Proxy SSL VPN Client	Address Pools: eID-VPNPOOL					Select
Login Setting	More Options					۲
Dead Peer Detecti	Tunneling Proto	cols:	Clientless SSL VPN	SSL VPN Client	IPsec	L2TP/IPsec
Customization IPsec Client	Filter:		None		~	Manage
	NAC Policy:		None		~	Manage
	Access Hours:	Access Hours:	Unrestricted		~	Manage
	Simultaneous Logins: Restrict access to VLAI	gins:	3			
		to VLAN:	VLAN: Unrestricted		*	
	Maximum Conne	ct Time:	Unlimited	minutes		
	Idle Timeout:		Unlimited 30	minutes		
<						
		ОК	Cancel He	ip		

- 4. ナビゲーション領域で [General] を選択します。
- 5. [Address Pools] でアドレスのプールを選択するために [Select] をクリックして、[eID-VPNPOOL] を選択します。
- 6. [More Options] 領域で [IPsec] チェックボックスと [L2TP/IPsec] チェックボックスをオフに して、[OK] をクリックします。

<u>手順8:証明書マッピングを定義する</u>

この手順では、証明書のマッピング基準を定義する方法について説明します。

- 1. [Remote Access VPN] 領域で [Advanced] をクリックし、[Certificate to SSL VPN Connection Profile Maps] を選択します。
- 2. [Certificate to Connection Profile Maps] 領域で [Add] をクリックし、マップ リストから [DefaultCertificateMap] を選択します。このマップは [Mapped to Connection Profile] フィー ルドの [DefaultWEBVPNProfile] と一致する必要があります。
- 3. [Mapping Criteria] 領域で [Add] をクリックし、以下の値を追加します。Field : Issuer、 Country (C)、Equals、「be」Field : Issuer、Common Name (CN)、Equals、「citizen ca」 [Mapping Criteria] が次の図のようになります。

G Cisco ASDM 6.0 for ASA - 192,168	8,100.254							
File View Tools Wizards Window H	telp			Lo	ok For:		Find +	alada
Home 🔏 Configuration 📴 Monitor	ing 🔚 Save 🌘	🕽 Refresh 🔇 Back 🄇	Permand ? H	*				cisco
Device List d P ×	Configuration ?	Remote Access VPN > A	dvanced > Certifica	te to SSL VPH (Connection I	Profile Maps		0
🗣 Add 📋 Delete 🚿 Connect	Define rules to	map certificates to desired	connection profiles (h	nnel arouns). Us	e the bottom	table to configure certificat	e fields togethe	r with their
A 192.168.0.1	matching crite	ria for the selected rule.	construction provides (co	a a na group a , oa	e e le portori		e menur cogeone	THE T C IL
192.168.100.254	Certificate to	Connection Drofile Many						1.2.2.2.2.2.2.2
	Certificate to t	connection Prome Pages						
	🗣 Add 🛃	Edit 🚺 Delete						
	Map Name		Rule Priority	Mapped to	Connection P	rolie	12.6112.21	1.5 A. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.
	DefaultCertifi	cateMap		10 DefaultWE	BVPNGroup			
Remote Access VPN d ² Q ×								1.11
😑 🗊 Certificate Management								
Sta CA Certificates	1.3							
Identity Certificates	128							
Code Signer								1.00
Local Certificate Authority	100							
R rais	1.000			121434-614				
B Advanced	Mapping Crite	ria						and the second second
+2+ Connection Gateway	🗣 Add 🗹	Edt 📋 Delete						
SSL Settings	Fuld	Component		Onerator		Walkan		
P Certificate to SSL VPN Conne	Issuer	Country (C)		Equals		be		
HTTP Redrect	Issuer	Common Name (CN)		Equals		citizen ca		
Maximum SSL VPN Sessions	13							
a ag c-mai Proxy								
Bevice Setup	132							
A								
E Frewal								
Remote Access VPN								
Ste-to-Site VPN								
Device Management								
5				Apply	Reset			
Configuration changes saved successfully.				<admin></admin>	15	😡 😂 🔂	🙆 25(07/07 23:20:54 UTC

4. [Apply] をクリックします。

<u> 手順 9 : ローカル ユーザを追加する</u>

この手順では、ローカル ユーザを追加する方法について説明します。

1. [Remote Access VPN] 領域で [AAA Setup] を展開し、[Local Users] を選択します。

- 2. [Local Users] 領域で [Add] をクリックします。
- 3. [Username] フィールドにユーザ証明書のシリアル番号を入力します。たとえば、
 56100307215 と入力します(このドキュメントのセクション「認証証明書」を参照してく

Circus ASUM 6.0 for ASUM 6.0 for ASUM 5.0 for ASUM 10.0 For Asuma 10 for ASUM 6.0 for Asuma 10	<u>たさい)。</u>						
Provide Versition Versition Versition Versition Versition Vers	🐔 Cisco ASDM 6.0 for ASA - 192.168	.100.254					
Interest Using Interest View Interest View Interest View Interest View Interest View Interest View Interest View <th>File View Tools Wizards Window He</th> <th>slo</th> <th></th> <th></th> <th>Look For:</th> <th>Find +</th> <th>alada</th>	File View Tools Wizards Window He	slo			Look For:	Find +	alada
Device Let Image: Contract Image: Contract Image: Contract Image: Cont Image: Contract <td< th=""><th>Home Configuration D Monitoria</th><th>ng 🔚 Save 🤇</th><th>Refresh 🙆 Back 🚫 Fi</th><th>stward 🤣 Help</th><th></th><th></th><th>CISCO</th></td<>	Home Configuration D Monitoria	ng 🔚 Save 🤇	Refresh 🙆 Back 🚫 Fi	stward 🤣 Help			CISCO
Add	Desice List De X	Configuration > P	emote Access VPH > AAA 1	etun > Local lisers			0
Remote Access VPN Image: Sector Sector VPN Group Lock Add Image: Sector Sector VPN Group Sector Edd Image: Sector Sector VPN Group Lock Add Image: Sector Sector	Add Delete Ø Connect 192.168.0.1 192.168.100.254	Create entries i Command author AAA authentica go to <u>Authentica</u>	n the ASA local user database. orization must be enabled in ord tion console commands must be atlon.	er for the user account privile enabled in order for certain a	ges to be enforced. To enabl	e command authorization, go b ced. To enable AAA authentic	a Windows .
Bernote Access VPH 0 x Application Hebrer Application Hebrer Application Hebrer Pul Partice Struct Booky Struct Booky B AAA Server Groups B AAA Server Groups B AAA Server Groups B AAA Server Groups B Contributed Management Advanced Advanced Advanced Advanced Contributed Management Contr		Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add
Acple ation Higher Image: Signon Servers Image: Signon Servers<	Remote Access VPN 🗗 🔍 🛛	enable_15	15	Full	N/A	N/A	
Running configuration successfully saved to flash memory. def 26/07/07 0:22:25 UTC	Application Helper Single Signon Servers Single Signon Servers AAAA Server Groups AAAAA Server Groups			Apply	Reset		Delete
	Running configuration successfully saved to flas	h memory.		<adm< td=""><td>in> 15</td><td>🕼 🎱 📔 🙆 2</td><td>6/07/07 0:22:25 UTC</td></adm<>	in> 15	🕼 🎱 📔 🙆 2	6/07/07 0:22:25 UTC

4. [Apply] をクリックします。

<u>手順 10:ASA を再起動する</u>

ASA を再起動して、システム サービスにすべての変更が適用されていることを確認します。

<u>微調整</u>

テスト中に、一部の SSL トンネルが正しく閉じないことがあります。ASA は AnyConnect クラ イアントが切断してから再接続する可能性があることを想定しているため、トンネルはドロップ されません。そのため接続し直すことができます。ただし基本ライセンス(デフォルトでは 2 つ の SSL トンネル)を使用したラボのテスト中には、SSL トンネルが正しく閉じていないとライ センスを使い尽くしてしまう可能性があります。この問題が発生したら、vpn-sessiondb logoff <option> コマンドを使用して、すべてのアクティブな SSL セッションからログオフします。

<u>簡単設定</u>

動作する設定を素早く作成するには、ASA を工場出荷時の設定にリセットし、設定モードでこの 設定を貼り付けます。

CiscoASA

```
ciscoasa#conf t
ciscoasa#clear configure all
ciscoasa#domain-name cisco.be
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
interface Vlan1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
interface Vlan2
nameif outside
security-level 0
ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
switchport access vlan 2
no shutdown
interface Ethernet0/1
no shutdown
1
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
enrollment terminal
crl configure
crypto ca certificate map DefaultCertificateMap 10
issuer-name attr c eq be
issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
   16060355 0403130f 42656c67 69756d20 526f6f74
20434130 le170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
```

30e8efc4 ab935e07 de328f12 74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf 6ce3841d de872e33 0b3c74e2 21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b a7210687 1d27d3c4 a1c94cb0 6f020301 0001a381 bb3081b8 300e0603 551d0f01 01ff0404 03020106 300f0603 551d1301 01ff0405 30030101 ff304206 03551d20 043b3039 30370605 60380101 01302e30 2c06082b 06010505 07020116 20687474 703a2f2f 7265706f 7369746f 72792e65 69642e62 656c6769 756d2e62 65301d06 03551d0e 04160414 10f00c56 9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609 60864801 86f84201 01040403 02000730 1f060355 1d230418 30168014 10f00c56 9b61ea57 3ab63597 6d9fddb9 148edbe6 300d0609 2a864886 f70d0101 05050003 82010100 c86d2251 8a61f80f 966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59 48a74c49 37d773a1 6a01655e 32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9 5d0f37ba 76d240bd cc2d3fd3 4441499c fd5b29f4 0223225b 711bbf58 d9284e2d 45f4dae7 b5634544 110d2a7f 337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1 60f2d787 f6572e7a 7e6a1380 1ddce3d0 631e3d71 31b160d4 9e08caab f094c748 755481f3 1bad779c e8b28fdb 83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636 ba218c97 1a21d4ea 2d3bacba eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297 fff26e87 7d46c974 d6efeb3d 7de6596e 069404e4 a2558738 286a225e e2be7412 b004432a quit no crypto isakmp nat-traversal dhcpd address 192.168.0.2-192.168.0.129 inside dhcpd enable inside dhcpd address 197.0.100.20-197.0.100.30 outside dhcpd enable outside 1 service-policy global_policy global ssl encryption aes256-shal aes128-shal 3des-shal rc4sha1 ssl certificate-authentication interface outside port 443 webvpn enable outside svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1 svc enable certificate-group-map DefaultCertificateMap 10 DefaultWEBVPNGroup group-policy DfltGrpPolicy attributes vpn-tunnel-protocol svc webvpn address-pools value eID-VPNPOOL username 63041403325 nopassword tunnel-group DefaultWEBVPNGroup general-attributes authentication-server-group (outside) LOCAL authorization-server-group LOCAL authorization-required authorization-dn-attributes SER tunnel-group DefaultWEBVPNGroup webvpn-attributes

<u>関連情報</u>

- ・<u>Cisco PIX Firewall ソフトウェア</u>
- <u>Cisco Secure PIX ファイアウォール コマンド リファレンス</u>
- ・<u>セキュリティ製品に関する Field Notice(PIX を含む)</u>
- Requests for Comments (RFCs)
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>