ASA/PIX 7.x and VPN クライアント Microsoft CA によるデジタル証明書を使用した IPSec 認 証の設定例

目次

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント 関連製品 表記法 設定 ネットワーク図 設定 ASA の設定 ASA の設定 ASA の設定の概要 VPN Client の設定 確認 トラブルシューティング 関連情報

<u>概要</u>

このドキュメントでは、Cisco セキュリティ アプライアンス(ASA/PIX)7.x および VPN Client にサード パーティ ベンダーのデジタル証明書を手動でインストールして、Microsoft の認証局 (CA)サーバで IPSec ピアの認証を行う方法について説明します。

前提条件

<u>要件</u>

このドキュメントでは、証明書を登録するために Certificate Authority(CA; 認証局)にアクセス する必要があります。 サポートされるサードパーティ CA ベンダーは、Baltimore、Cisco、 Entrust、iPlanet/Netscape、Microsoft、RSA、および VeriSign です。

注: このドキュメントは、シナリオに CA サーバとして Windows 2003 Server を使用しています 。

注: このドキュメントは、ASA/PIX に既存の VPN 設定がないことを前提としています。

<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くものです。

・ソフトウェア バージョン 7.2(2) および ASDM バージョン 5.2(2) が稼働する ASA 5510

・ソフトウェア バージョン 4.x 以降が稼働する VPN Client

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、クリアな(デフォルト)設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

ASA の設定は、ソフトウェア バージョン 7.x が稼働する Cisco 500 シリーズ PIX にも適用できます。

<u>表記法</u>

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</u>』を参照してください。

<u>設定</u>

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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 Tool</u>(<u>登</u> <u>録</u>ユーザ専用)を使用してください。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

<u>設定</u>

このドキュメントでは、次の設定を使用します。

- <u>ASA の設定</u>
- <u>ASA の設定の概要</u>
- ・<u>VPN Client の設定</u>

<u>ASA の設定</u>

ASA にサードパーティ ベンダーのデジタル証明書をインストールするには、次の手順を実行します。

<u>ステップ1:日付、時刻、および時間帯(Time Zone)の値が正しいことを確認する</u>

<u>ステップ 2. RSA キー ペアを生成する</u>

ステップ 3. トラストポイントを作成する

ステップ 4. 証明書登録を生成する

<u>ステップ 5. トラストポイントを認証する</u>

<u>ステップ 6. 証明書をインストールする</u>

<u>ステップ 7. 新しくインストールした証明書を使用するようにリモート アクセス</u> <u>VPN(IPSec)を設定する</u>

ステップ1:日付、時刻、および時間帯(Time Zone)の値が正しいことを確認する

ASDM の手順

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Device Administration] を展開し、[Clock] を選択します。
- 3. 表示されている情報が正しいことを確認します。証明書の検証が適切に行われるために、 Date、Time、および Time Zone の値は正確である必要があります。



コマンドラインの例

CiscoASA

OISCOROR				
CiscoASA#show clock	16:25:49.580	IST Fri	Dec 2	8 2007

<u>ステップ 2. RSA キー ペアを生成する</u>

生成された RSA 公開キーは、ASA からの ID 情報と結合され、PKCS#10 証明書要求が形成され ます。 キー ペアを作成するトラストポイントでキー名を明確に特定する必要があります。

ASDM の手順

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Key Pair] を選択します。
- 3. [Add] をクリックします。

Configuration > Properties > Certifi	tate > Key Pair			
Startup Wizard	ry Pair			
🗄 🚮 AAA Setup	Configure the key pairs to be used in cert	ificates		
	configure the key pairs to be used in cen	nicales.		
🟵 🐻 ARP				
	Note: Operations on this screen are appli	ed immediately upon o	completion and are irreve	rsible.
E- Certificate				
Authentication				
Enrolment	Key Pair Name	Usage	Modulus Size	Add
mport Certificate				
Key Pair				Circuit Data Za
Manage Certificat				Show Details
Add Key Pa				
Device Acce				Delete
- 30 Device Admi	C. Lise default key name			
(B) Banner Hame.				Refresh
Boot Ima	my.CA.key			
CLI Prom				
Clock Size	1024			
Console Size.	1024			
Davice				
ETP Moc	General Purpose C Special			
ICMP Ru				
Manager				
O NTP	laws Cancel H	In 1		
Passwo	Cancel He	4P		
1000110				

- 4. キー名を入力し、モジュール サイズを選択し、使用タイプを選択します。**注:** 推奨されるキ ー ペアのサイズは 1024 です。
- 5. [Generate Now] をクリックします。作成したキー ペアが [Key Pair Name] 列に表示されます。
- コマンドラインの例

CiscoASA



<u>ステップ 3. トラストポイントを作成する</u>

トラストポイントは、ASA が使用する認証局(CA)を宣言する必要があります。

ASDM の手順

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Trustpoint] を展開します。
- 3. [Configuration] を選択し、[Add] をクリックします。

Configuration > Properties > 0)er	tificate >	Trustpoint > Config	guration		
🖂 🚽 🖉 Startup Wizard	ľ	Configure	ation			
🗈 💼 AAA Setup	1	Confi	www.a.Cartificata.A.d	hority (CA) as a trustmoint		
		Comi	gure a certificate Aut	nonty (CA) as a trustpoint.		
🖭 🐯 ARP						
Client Update		,				
😑 🔂 Certificate			Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add
Authentication						
Enrolment						Edit
Import Certificate						
Key Pair						
Manage Certificat						Delete
E-22 Trustpoint						
Configuration						Request (
Export						

- 4. 以下の値を設定します。**トラストポイント名**: トラストポイント名は目的の用途に関連す る名前にします (この例では *CA1*)。**キー ペア**: <u>ステップ 2.</u> で生成したキー ペア (my.CA.key)を選択します。
- 5. [Manual Enrollment] を選択していることを確認します。
- 6. [Certificate Parameters] をクリックします。[Certificate Parameters] ダイアログ ボックスが 表示されます。
- 7. [Edit] をクリックし、次の表に示す属性を設定します。これらの値を設定するために、 Attribute ドロップダウン リストから値を選択し、値を入力して、Add をクリックします

		マトンし言	を選択し、直と、		<u>・</u> ノノノレみ 9。
🚰 Edit DN					
				Attribute	Value
				Common Name (CN)	CiscoASA.cisco.com
DN Attribute	to be Added			Department (OU)	TSWEB
			Redelana	Company Name (O)	Cisco Systems
Attribute:	Select Attribute	· 💌	Add PP	Country (C)	US
			[State (St)	North Carolina
Value:			Delete	Location (L)	Raleigh
	<u></u>				
				1	
		ок	Cancel	Help	

- 8. 適切な値を追加したら、OK をクリックします。
- 9. [Certificate Parameters] ダイアログボックスで、[Specify FQDN] フィールドに FQDN を入 力します。この値は、Common Name(CN)に使用したものと同じ FQDN である必要があ

	💼 Certificate Parameters
	Enter the values for the parameters that are to be included in the certi
	Subject DN: Systems,C=US,St=North Carolina,L=Raleigh
	Subject Alternative Name (FQDN)
	C Use FQDN of the device
	Specify FQDN CiscoASA.cisco.com
	O Use none
	E-mail:
	IP Address:
	Include device serial number
ります。	OK Cancel Help

- 10. [OK] をクリックします。
- 11. 正しいキー ペアが選択されていることを確認し、[Use manual enrollment] オプション ボタ ンをクリックします。
- 12. [OK] をクリックして、[Apply] をクリックします。

🗯 Add Trustpoint Configu	Iration		
Trustpoint Name:	A1		
☐ Generate a self-sign	ed certificate on e	enrollment	
If this option is enabl	ed, only Key Pair	and Certificate Parameters	s can be specified.
Enrollment Settings Re	vocation Check	CRL Retrieval Policy CR	L Retrieval Method OCSP
Key Pair: my.C	A.key	Show Details	New Key Pair
Challenge Password:		Confirm Challenge Password:	
Enrollment Mode can	only be specified	if there are no certificates	s associated with this trust
Enrollment Mode			
💽 Use manual	enrollment		
C Use automa	tic enrollment		
Enrollment UR	L: http://		
Retry Period:	1	minutes	
Retry Count:	0	Use 0 to indicate u	nlimited retries)
			Contificante Domentou
			Certificate Parameter
	ок	Cancel	Help

コマンドラインの例

CiscoASA
CiscoASA(config)#crypto ca trustpoint CA1 ! Creates
the trustpoint. CiscoASA(config-ca-
trustpoint)#enrollment terminal ! Specifies cut and
paste enrollment with this trustpoint. CiscoASA(config-
ca-trustpoint)# subject-name
CN=wepvpn.cisco.com,OU=TSWEB, O=Cisco
Systems, C=US, St=North Carolina, L=Raleigh ! Defines
x.500 distinguished name. CiscoASA(config-ca-
trustpoint)#keypair my.CA.key ! Specifies key pair
generated in <u>Step 2</u> . CiscoASA(config-ca-trustpoint)# fqdn
CiscoASA.cisco.com ! Specifies subject alternative
<pre>name (DNS:). CiscoASA(config-ca-trustpoint)#exit</pre>

<u>ステップ 4. 証明書登録を生成する</u>

ASDM の手順

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Enrollment] を選択します。
- 3. <u>ステップ 3</u> で作成したトラストポイントが選択されていることを確認して、[Enroll] をクリックします。ダイアログ ボックスに証明書登録要求(証明書署名要求とも呼ばれる)が一覧表示されます。

nrollment Request	
To complete the enrollment proces management interface of the CA.	ss, please paste the following PKCS10 enrollment request into
You will need to install the certific	ate after receiving it.
Go to Configuration > Properties >	 Certificate > Import Certificate to do so.
Certificate Request:	
Certificate Request:	SteWBrbWFrbi SieYNibrSib20rrc28rrD0YJKoZTbroN
Certificate Request: hvcNAQkCFhtDaXNjb0FTQS AQEBBQADqY0AMIGJAoGBAL	5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN 5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm
Certificate Request: hvcNAQkCFhtDaXNjb0FTQS AQEBBQADgY0AMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn	5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKo2IhvcN 5YNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY
Certificate Request: hvcNAQkCFhtDaXNjb0FTQS AQEBBQADgY0AMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX61	5teWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvcN 5YNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0QlFzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS AQEBBQADgYOAMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX6 AgMBAAGgRjBEBgkqhkiG9w	SteWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvcN SYNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0QlFzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF 0BCQ4xNzAlMAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS AQEBBQADgYOAMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX6J AgMBAAGgRjBEBgkqhkiG9w ghtDaXNjbOFTQSSteWRvbW	5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN 5YNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF 0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd Fpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS AQEBBQADgYOAMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX6 AgMBAAGgRjBEBgkqhkiG9w ghtDaXNjbOFTQS5teWRvbW gmoBmSRVnLOqyDtpS1bveK	SteWRvbWFpbi5jaXNjby5jb20wg28wDQYJKo2IhvcN SYNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0QlFzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJ2vdqCgq+xR404/1YP0oeKKfq7apCHvVHF 0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd Fpbi5jaXNjby5jb20wDQYJKo2IhvcNAQEEBQADgYEA ew0AdG5/fxnJRYU2UunllW6sG0KaJYCiFH//eaewF3
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS AQEBBQADgYOAMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX6J AgMBAAGgRjBEBgkqhkiG9w ghtDaXNjbOFTQS5teWRvbW gmoBmSRVnL0qyDtpS1bveK gEjVABVhB7Ni6N29710mDAJ	SteWRvbWFpbi5jaXNjby5jb20wg28wDQYJKo2IhvcN SYNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0QlFzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJ2vdqCgq+xR404/1YP0oeKKfq7apCHvVHF 0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd Fpbi5jaXNjby5jb20wDQYJKo2IhvcNAQEEBQADgYEA ew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 bnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS AQEBBQADgYOAMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX6 AgMBAAGgRjBEBgkqhkiG9w ghtDaXNjbOFTQS5teWRvbW gmoBmSRVnL0qyDtpS1bveK gEjVABVhB7Ni6N29710mDA gonnkGTJ11vZCSDXz4BXm4	SteWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN SYNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF 0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd Fpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA ew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 bnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 sXAqrwZCDdj0/S5BiQJGc=
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS AQEBBQADgYOAMIGJAoGBAL psMFP7DeKPIQ+RdthaRBzn mAH40WUXbi18BHZSSgxPX6J AgMBAAGgRjBEBgkqhkiG9w ghtDaXNjbOFTQS5teWRvbW gmoBmSRVnLOqyDtpS1bveK gEjVABVhB7Ni6N29710mDAJ gonnkGTJ11vZCSDXz4BXm4; D	SteWRvbWFpbi5jaXNjby5jb20wg28wDQYJKo2IhvcN SYNIxlzkfo80ziV7xJdfA7jRtkHXx2Npmr9A0QlFzm gSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY BGeiC9BjJ2vdqCgq+xR404/1YP0oeKKfq7apCHvVHF 0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd Fpbi5jaXNjby5jb20wDQYJKo2IhvcNAQEEBQADgYEA ew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 bnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 sXAqrwZCDdj0/S5BiQJGc=

4. 次の手順に示すように、PKCS#10 登録要求をテキスト ファイルにコピーし、保存した CSR をサードパーティ ベンダー(Microsoft CA など)に送信します。VPN サーバに提供さ れたユーザ クレデンシャルを使用して、CA サーバ 172.16.5.1 にログインします。

🐐 about:blank - Microsoft I	nternet Exploi	er provided by	y Cisco Sys	tems, Inc.		
File Edit View Favorites	Tools Help					
🖨 Back 🔻 🔿 👻 🙋 🖞	🖞 🛛 🧟 Search	😹 Favorites	Media	🎯 🖏 •	90	
Address (http://172.16.5.1)	'certsry					
						_
Enter Net	work Passwor	ď			?	×1
9-2	Diana tura un		d			
	Flease (ype yc	our user name and	u passworu.			
	Site:	172.16.5.1				
	User Name	vpnuser				
	Password	******)		
	Domain					
	🔲 Save this p	password in your	password lis	t		
			ОК		Cancel	
						'

注: CA サーバで、ASA(VPN サーバ)のユーザ アカウントを所有していることを確認して ください。[Request a certificate] > [advanced certificate request] の順にクリックし、 [Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file or submit a renewal request by using a base-64-encoded PKCS#7 file] を選択します。

Address 🕘 http://172.16.5.1/certsrv/certrqad.asp	*	260	Lin
Microsoft Certificate Services CAT		Ho	<u>me</u>
Advanced Certificate Request			
The policy of the CA determines the times of eartifactor you can request. Click one of the following entions to			
The policy of the CA determines the types of certificates you can request. Click one of the following options in	0.		
Create and submit a request to this CA			
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal re-	auest	t by us	sind
a base 64-encoded PKCS #7 file			
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollm	ient s'	tation	l
Note: You must have an enrollment agent certificate to submit a request on behalf of another user.			-

符号化された情報を [Saved Request] ボックスにコピー アンド ペーストし、[Submit] をク リックします。

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded (source (such as a Web server) in the Saved Request box.

Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	vQVNBLmNpc2NvLmNvbTANBgkqhkiG9wOBAQQ 4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mAT D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgR 8Ux9emhFHpGHnQ/MpSfUOdQ== not part of the certificate request- ■ Browse for a file to insert.	PFAAO AsG8 JGh+
Certificate Temp	late:	
	IPSEC -	
Additional Attribu	ites:	
Attributes:		
	Submi	it > Base
64 encoded オプショ	ョン ボタンをクリックし、次に Download certificate を	クリックします 1
Microsoft Certi	ficate Services CA1	
Certificate Is	sued	
The certificate	e you requested was issued to you.	
0	DER encoded or <a>• Base 64 encoded	
	<u>ownload certificate</u> ownload certificate chain	File Download

ダイアログ ボックスが表示されたら、ASA にインストールする ID 証明書として cert_client_id.cer という名前で保存します。

File Dowr	nload 🗙
?	Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.
	File name: certnew.cer
	File type: Security Certificate
	From: 172.16.5.1
	This type of file could harm your computer if it contains malicious code.
	Would you like to open the file or save it to your computer?
	Open Save Cancel More Info
	Always ask before opening this type of file

コマンドラインの例

CiscoASA
CiscoASA(config)#crypto ca enroll CA1 ! Initiates
CSR. This is the request to be submitted ! via web or
email to the 3rd party vendor. % Start certificate
enrollment % The subject name in the certificate will
be: CN=CiscoASA.cisco.com,OU=TSWEB, O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh % The fully-
qualified domain name in the certificate will be:
CiscoASA.cisco.com % Include the device serial number in
the subject name? [yes/no]: no ! Do not include the
device's serial number in the subject. Display
Certificate Request to terminal? [yes/no]: yes !
Displays the PKCS#10 enrollment request to the terminal.
! You will need to copy this from the terminal to a
text ! file or web text field to submit to the 3rd
party CA. Certificate Request follows:
MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3 oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX01uBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7Se0
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BM051ulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5Q1Kx2Y/vrqs+Hg5SLHpbhj/

Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not part of the certificate request--- Redisplay enrollment request? [yes/no]: no ciscoasa(config)#

<u>ステップ 5. トラストポイントを認証する</u>

サードパーティ ベンダーから ID 証明書を受信したら、引き続きこのステップを実行します。

ASDM の手順

- 1. ID 証明書をローカル コンピュータに保存します。
- 2. ファイル形式ではない Base64 で符号化された証明書が提供された場合、Base64 メッセージをコピーし、テキスト ファイルに貼り付ける必要があります。
- 3..cer 拡張子を使用してファイルの名前を変更します。注:.cer 拡張子を使用してファイルの



名前を変更すると、ファイルのアイコンは証明書として表示されます。 4. 証明書ファイルをダブルクリックします。

Ge	eneral Details Certification Path
	Certificate Information
	This tertificate is intended for the following purpose(s):
	 Ensures the identity of a remote computer Proves your identity to a remote computer 2.16.840.1.113733.1.7.21

__注: General タブに「

Windows does not have enough information to verify this certificate」というメッセージが表示された場合、この手順を継続する前に、サードパーティ ベンダーのルート CA または中間 CA 証明書を入手する必要があります。 ルート CA または中間 CA 証明書を入手するには、サードパーティ ベンダーまたは CA 管理者に問い合せてください。

- 5. [Certificate Path] タブをクリックします。
- 6. 発行された ID 証明書の上にある CA 証明書をクリックし、[View Certificate] をクリックし

Certificate	? >
General Details Certification Path	
Certification path	
	View Certificate
Certificate <u>s</u> tatus:	
This certificate is OK.	
f。	OK CA 証明

に関する詳細情報が表示されます。

7. Details をクリックして、ID 証明書の詳細情報を確認します。

Certificate	<u>?</u> ×
General Details Certification Path	
Show: <all></all>	
Field	Value
E Version	V3
E Serial number	611E E59B 0000 0000 0007
Signature algorithm	sha1RSA
Valid from	CA1, ISWeb, cisco, com Saturday, December 15, 2007
	Monday, December 15, 2007
E Subject	CiscoASA.cisco.com OU=TSW
E Public key	RSA (1024 Bits)
1	
Ec	lit Properties
	ОК

8. ID 証明書をインストールする前に、CA 証明書を CA サーバからダウンロードし、ASA にイ ンストールする必要があります。 次の手順を実行して、*CA1* という名前の CA サーバから CA 証明書をダウンロードします。VPN サーバに提供されたユーザ クレデンシャルを使用 して、CA サーバ 172.16.5.1 にログインします。

🖹 abo	out:blar	nk - M	icrosoft	Internet	Explor	er				
Eile	<u>E</u> dit	<u>V</u> iew	F <u>a</u> vorite	s <u>T</u> ools	<u>H</u> elp					
🕒 Ba	ick 🔻 🍯	•	× 2	🏠 🛛 🔎 s	5earch	Fa	vorites	e		
A <u>d</u> dre:	ss 🙆 H	http://1	72.16.5.	1/certsrv						
									1	
	Conne	ct to	172.16.5	.1				?×		
	E.	2								
	222									
	C		- 170 10							
	Conn	ecting	to 172.16	0.5.1						
	<u>U</u> ser	name:		🙎 vpnse	erver		-	·		
	Passv	word:		•••••	••					
					nber my	passwo	rd			
					OK		Cano	:el		
									l[Download	a (

certificate, certificate chain or CRL] をクリックし、[Base 64] オプション ボタンを選択して 符号化方式を指定します。[Download CA certificate] をクリックします。

Downloa	ad a CA Certificate, Certificate Chain, or CRL
To trust o	ertificates issued from this certification authority, install this CA c
0 1.001 0	entineatee recard mentining contineation admonty, <u>metantine erre</u>
o downl	oad a CA certificate, certificate chain, or CRL, select the certifica
A certific	cate:
	Current [CA1]
ncoding	method:
	O DER ● Base 64
Downloa	d CA certificate
Downloa	d CA certificate chain
Downloa	d latest base CRL
<u>)ownloa</u>	d latest delta CRL
certnew.ce	er という名前で、CA 証明書をコンピュータに保存します。
ile Down	oad - Security Warning 🛛 🔀
Danau	went to spen as some this GlaD
DO YOU	want to open or save this mer
	Name: certnew.cer
	Type: Security Certificate, 1.64 KB
	From: 172.16.5.1
	Open Save Cancel
1	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>

- 10. メモ帳などのテキスト エディタでファイルを開きます。 (ファイルを右クリックし、 [Send To] > [Notepad] の順に選択します)。
- 11. Base64 で符号化されたメッセージは、次の画像の証明書のようになります。

📝 certnew.cer - Notepad <u>File E</u>dit F<u>o</u>rmat <u>H</u>elp ---BEGIN CERTIFICATE-MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT Bqojkiajk/IszaezFqvuu1dlyjeMMAoGA1uEAxMDQ0ExMB4xDTA3MTIxNDA2MDE0 MĪoXDTEyMTIXNDA2MTAXNVowUTETMBEGCqmSJomT8ixkARkWA2NvbTEVMBMGCqmS jomT8ixkARkwBwNpc2NvMRUwEwYKCZImiŹPyLGQBGRYFVFNXZWIXDDAKBgNVBĀMT AONBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuvvyiLmA9 BSGzMz3sCtR9TCMwOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vŴeMijcQnŵdOq+ Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI //3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXwKh4uC04xxQmr//Sct1tdwQcvk2V µBwCsptW7C1akTqfm5×K/d//z2eUu×rHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDh×x wPXR018CAwEAAa0CAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQE AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZr58I8jqI8RRDL3mYfNQJ pAP1wDccAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdwJsawm]MjBLZXk]MjBTZXJ2aWN]cyxD Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD ÞŴNvbT9jZXJ0aŴZpYŹF0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9 Y1JMRG]zdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50c3d]Yi5j aXNjby5jb20vQ2vydEvucm9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MičbXJeKr L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHqHUCD9/BZWAqfmGUm++HMljnW8liyIF bcNwxlqxsDT+n9Yok6bnG6uof4sgETNrN8EyYVrsGK0lE+oC5L+ytJvw19GZhlzE [Ovufpa+pt47dmar6uo2v2zbw5kGavLu8GsrFd8wZbpBvMkCqFwNcNItcufu0x]b 1××c68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2ÉwGPn149zp×v5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1vD+p85at ---END CERTIFICATE-----

- 12. ASDM で [Configuration] をクリックし、[Properties] をクリックします。
- 13. [Certificate] を展開し、[Authentication] を選択します。
- 14. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックします。
- 15. Base64 形式で作成された CA 証明書をテキスト エディタからテキスト領域に貼り付けます。
- 16. [Authenticate] をクリックします。

Configuration > Properties > Ce	rtificate > Authentication
🖂 💁 Startup Wizard	Authentication
🕀 🚮 AAA Setup	Sutheritinate a CA cartificate. As the result of sutheritination, the CA cartificate will be assor
	hustonint and installed on the device
🕀 🐻 ARP	a desponit and instance of the device.
	Trustnoint Name: Edit New
E Certificate	
Authentication	Fingerprint (optional):
Enrollment	
Import Certificate	The certificate text can be specified if the selected trustpoint is configured for manua
Key Pair	
	Certificate Text
🖃 🔯 Trustpoint	Church from a flat
Configuration	Comport from a file.
Export	
- A Import	 Enter the certificate text in hexadecimal or base64 format:
Device Access	L6Z86JGW1Rbf5VYnITrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMlin//
E OP Device Administration	CSL+ytJvw1
Banner (B) Banner	MKCgFWNct
Boot Image/Config	wGPn149zpi
Clark	
Clock	The trustpoint CA1 has been authenticated.
Console	
Device	
FTP Mode	OK
ICMP Rules	
Management Acc	
- O NTP	
Password	
Secure Copy	
- 🚰 SMTP	
SNMP 1	Authenticate

17. [OK] をクリックします。 **コマンドラインの例**

CiscoASA
CiscoASA(config)#crypto ca authenticate CA1 !
Initiates the prompt to paste in the base64 CA root !
or intermediate certificate. Enter the base 64 encoded
CA certificate. End with the word "quit" on a line by
itselfBEGIN CERTIFICATE
MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B
AQUFADBR
${\tt MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21z}$
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK
BgNVBAMT
${\tt A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu}$
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI

y3GoFGmn8zGx6yS1DEaUQxRVwnDbM1vwqYBXwKn4uC04xxQmr//Sctlt
uwgcvkzv
ubwcsptw/clakiqim5xk/d//zzeouxiniySgclorykivE0/glotigeSS
WPAROIOCAWEAAAUCAWowggFIMDMGCSSGAQQDgJCUAgQGHGQAQWDDMASG
AWIBHJAPBGNVHRMBALOEBTADAQH/MBUGALUGDGQWBBTZIDOIOJQIORRD
$D_{\text{CM}} = D_{\text{CM}} = D_{C$
DAPINDCCAQMGAIUGHWSB+2CD+DCB9aCBoqCB/4aBCWXKIXAOLY0VQ049
QUEXLENU
FVKILVCYSZMCQUNILENOFUNEUCZDI JIQUWUSAWMIMJBLZZKIMJBIZZUZ
c2Ny1.FPD
PWNvbr9jZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jbc2U/b2JcZWN0
02xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnSGNWh0dHA6Lv90cv13MmszLWFicv50
c3dlyi5j
aXNibv5ib20v02VvdEVucm9sbC9D0TEuY3JsMBAGCSsGA00BgicVA00D
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYn1TrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HM1j
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw
19GZhlzE
10VUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
cufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
END CERTIFICATE quit ! Manually pasted
certificate into CLI. INFO: Certificate has the
following attributes: Fingerprint: 98d66001 f65d98a2
b455fbce d672c24a Do you accept this certificate?
[yes/no]: yes Trustpoint CA certificate accepted. %
Certificate successfully imported CiscoASA(config)#

<u>ステップ 6. 証明書をインストールする</u>

ASDM の手順

次の手順を実行するには、サードパーティ ベンダーにより提供された ID 証明書を使用します。

- 1. [Configuration]、[Properties] の順にクリックします。
- 2. [Certificate] を展開し、[Import Certificate] を選択します。
- 3. [Enter the certificate text in hexadecimal or base64 format] オプション ボタンをクリックし 、テキスト フィールドに Base64 ID 証明書を貼り付けます。



4. [Import] をクリックし、[OK] をクリックします。 コマンドラインの例

CiscoASA CiscoASA(config)#crypto ca import CA1 certificate !---Initiates prompt to paste the base64 identity certificate !--- provided by the 3rd party vendor. % The fully-qualified domain name in the certificate will be: CiscoASA.cisco.com Enter the base 64 encoded certificate. End with the word "quit" on a line by itself !--- Paste the base 64 certificate provided by the 3rd party vendor. ----BEGIN CERTIFICATE-----MIIFpzCCBI+gAwIBAgIKYR71mwAAAAAABzANBgkqhkiG9w0BAQUFADBR MRMwEOYK CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT BgoJkiaJ k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz OVoXDTA5 MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo IENhcm9s aW5hMRAwDgYDVQQHEwdSYWx1aWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0 ZW1zMSQw IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ KoZIhvcN AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C qB9j3HpX BmfXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCO sS8iqxq0 2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/ CaeqnGRN AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ21z Y29BU0Eu Y21zY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf BONVHSME GDAWgBTZrb818jq18RRDL3mYfNQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB 9aCB8qCB 74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD Tj1QdWJs aWM1MjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1 cmF0aW9u

LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJ1dm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWN1cnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1d1Yi5jaXNjby5jb21f
Q0ExLmNy
${\tt dDahbgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud}$
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/02xDB
7wXQaGph
${\tt zRq4dxAL111JkIjhfeQY+7VSkZ1GEpuBnENTohdhthz5vBjG1cROXIs8}$
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/034wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc lL5nuPsd8MaexBc=END CERTIFICATE quit
INFO: Certificate successfully imported
CiscoASA(config)#

<u>ステップ 7. 新しくインストールした証明書を使用するようにリモート アクセス</u> VPN(IPSec)を設定する

ASDM の手順

リモート アクセス VPN を設定するには、次の手順を実行します。

1. [Configuration] > [VPN] > [IKE] > [Policies] > [Add] の順に選択し、この図のように ISAKMP ポリシー 65535 を作成します。

🗯 Add IKE Policy				
Priority:	65535	Authentication:	rsa-sig 💌	
Encryption:	3des 💌	D-H Group:	2 💌	
Hash:	md5 💌	Lifetime:	C Unlimited	seconds 💌
	ок	Cancel	Help	

- 2. [OK] をクリックして、[Apply] をクリックします。
- 3. [Configuration] > [VPN] > [IPSec] > [Transform Sets] > [Add] の順に選択し、この図のように トランスフォーム セット(*myset*)を作成します。

付 Add Transform Set		
Set Name:	yset	
Properties		
Mode: ESP Encryption: ESP Authentication	Tunnel JDES on: MD5	○ Transport
ок	Cancel	Help

- 4. [OK] をクリックし、[Apply] をクリックします。
- 5. [Configuration] > [VPN] > [IPSec] > [IPSec Rules] > [Add] の順に選択し、この図のように、 ダイナミック ポリシーのプライオリティが 10 であるクリプト マップを作成します。

🚰 Create IPSec Rule	
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selec	tion
Interface: outside 💌 Policy Type: dynamic 💌	Priority: 10
Transform Sets	
Transform Set to Be Added:	Move Up
ESP-DES-SHA	· · · ·
Remove	Move Down

- 6. [OK] をクリックし、[Apply] をクリックします。
- 7. [Configuration] > [VPN] > [General] > [Group Policy] > [Add Internal Group Policy] の順に選 択し、以下の図に示すようにグループ ポリシー **Defaultgroup** を作成します。

🚰 Add Internal Group Policy					
Name: Defa	ultgroup				
General IPSec C	lient Configur:	ation Client Fi	rewall Ha		
Check an Inherit (checkbox to le	et the correspo	onding settin		
Tunneling Protoc	ols:	🔽 Inherit	🗖 IPSe		
Filter:		🔽 Inherit			
Connection Settin Access Hours	igs	🔽 Inherit			

i 📩 A	dd Internal Group Poli	c y	
	Name: Defaultg	oup	
	General IPSec Client	Configuration Client Firewall	Hardware Client
	Check an Inherit chec	kbox to let the corresponding s	etting take its value from the def
	General Client Param	eters Cisco Client Parameters	Microsoft Client Parameters
	Banner:		✓ Inherit
	Default Domain:		🗆 Inherit 🔤 cisco.com

- 8. [OK] をクリックし、[Apply] をクリックします。
- 9. [Configuration] > [VPN] > [IP Address Management] > [IP Pools] > [Add] の順に選択し、VPN クライアント ユーザが動的に割り当てられるようにアド<u>レ</u>ス プール vpnpool を設定します

Add IP Pool				
Name:		vpnpool		
Starting ID 4 a	ldrooo:	105510		
Starting in Ad	uress.	10.5.5.10		
Ending IP Add	dress:	10.5.5.20		
Subnet Mask	:	255.255.25	5.0	•
ок	C	ancel	ł	Help

10. [OK] をクリックし、[Apply] をクリックします。

o

11. [Configuration] > [VPN] > [General] > [Users] > [Add] の順に選択し、VPN クライアント ア クセス用のユーザ アカウント **vpnuser** を作成します。

F	Add User Account		
	(Identity) VPN Policy VVebVPN		
	Username:	vpnuser	
	Provide		
	Password:		
	Confirm Passwor	'd:	
	🗖 User aut	henticated using MSCHAP	
	Privilege level is u	used with command authorization.	
	Privilege Level:	2 💌	
2. <u> </u>	のユーザを DefaultRAGroup に追加しま	ます。	
1	Add User Account		
	Identity VPN Policy VebVPN		
	Check an Inherit checkbox to let the c	orresponding setting take its value from t	he gro
	Group Policy:	Minherit	
	Tunneling Protocols:	🗹 Inherit 🔲 IPSec 🔲 We	sbVPN
	Filter:	Inherit	
	Tunnel Group Lock:		
	Store Password on Client System:	✓ Inherit C Yes C No	

- 13. [OK] をクリックし、[Apply] をクリックします。
- 14. 次の手順を実行して DefaultRAGroup を編集します。[Configuration] > [VPN] > [General] > [Tunnel Group] > [Edit] の順に選択します。[Group Policy] ドロップダウン リストから [Defaultgroup] を選択します。

🕵 Edit Tunnel Group
Name: DefaultRAGroup Type: jpsec-ra
General IPSec PPP
Configure general access attributes from the following sub-tabs.
Basic Authentication Authorization Accounting Client Address .
Group Policy: Defaultgroup [Authentication]
Server Group] ドロップダウン リストから [LOCAL] を選択します。
🖆 Edit Tunnel Group
Name: DefaultRAGroup Type: ipsec-ra
General PPP
Configure general access attributes from the following sub-tabs. Basic Authentication Authorization Accounting Client Address Assig
To set authentication server group per interface, go to the Advanced ta
Authentication Server Group:

Assignment] ドロップダウン リストから [vpnpool] を選択します。

🔂 Edit Tunnel Group	
Name: DefaultRAGroup	Type: jpsec-ra
General IPSec PPP	
Configure general access attributes from the	following sub-tabs.
Basic Authentication Authorization Acco	unting Client Address Assignmer
To specify whether to use DHCP or ad > IP Address Management > Assignme	ldress pools for address assignme ent.
DHCP Servers	
ID Addresses	
in Address.	Add >>
	Delete
Address Pools	
To configure interface-specific add	iress pools, go to the Advanced ta
Available Pools	Assigned
	vpnpool
	Add >>

15. [OK] をクリックし、次に [Apply] をクリックします。 **コマンドラインの例**

CiscoASA
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5 CiscoASA(config-
isakmp-policy)# group 2 CiscoASA(config-isakmp-
policy)#lifetime 86400 CiscoASA(config-isakmp-
<pre>policy)#exit CiscoASA(config)#crypto isakmp identity</pre>
<pre>auto ! Phase 1 Configurations CiscoASA(config)#crypto</pre>
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map outside_dyn_map 10
<pre>set transform-set myset CiscoASA(config)#crypto map</pre>
outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
CiscoASA(config)#crypto map outside_map interface

outside !--- Phase 2 Configurations CiscoASA(config)#group-policy defaultgroup internal CiscoASA(config) #group-policy defaultgroup attributes CiscoASA(config-group-policy)#default-domain value cisco.com CiscoASA(config-group-policy) #exit !--- Create a group policy "Defaultgroup" with domain name !--cisco.com CiscoASA(config)#username vpnuser password password123 CiscoASA(config)#username vpnuser attributes CiscoASA(config-username) #group-lock value **DefaultRAGroup** CiscoASA(config-username) #exit !---Create an user account "vpnuser" and added to "DefaultRAGroup" CiscoASA(config) #tunnel-group DefaultRAGroup general-attributes !--- The Security Appliance provides the default tunnel groups !--- for remote access (DefaultRAGroup). CiscoASA(config-tunnelgeneral) #address-pool vpnpool !--- Associate the vpnpool to the tunnel group using the address pool. CiscoASA(config-tunnel-general)#default-group-policy **Defaultgroup** !--- Associate the group policy "Defaultgroup" to the tunnel group. CiscoASA(configtunnel-general)#exit CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-attributes CiscoASA(config-tunnelipsec)#trust-point CA1 CiscoASA(config-tunnelipsec)#exit !--- Associate the trustpoint CA1 for IPSec peer authentication

<u>ASA の設定の概要</u>

CiscoASA

CiscoASA#**show running-config** : Saved : ASA Version 7.2(2) ! hostname CiscoASA domain-name cisco.com enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif outside security-level 0 ip address 192.168.1.5 255.255.255.0 ! interface Ethernet0/1 shutdown nameif inside security-level 100 ip address 10.2.2.1 255.255.255.0 ! interface Ethernet0/2 nameif DMZ security-level 90 ip address 10.77.241.142 255.255.255.192 ! interface Ethernet0/3 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa722-k8.bin ftp mode passive dns server-group DefaultDNS domain-name cisco.com access-list 100 extended permit ip 10.2.2.0 255.255.255.0 10.5.5.0 255.255.255.0 pager lines 24 mtu outside 1500 mtu inside 1500 mtu DMZ 1500 ip local pool vpnpool 10.5.5.10-10.5.5.20 mask 255.255.255.0 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no asdm history enable arp timeout 14400 nat (inside) 0 access-list 100 route outside 10.1.1.0 255.255.255.0 192.168.1.1 1 route outside 172.16.5.0 255.255.255.0 192.168.1.1 1 route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute group-policy Defaultgroup internal group-policy Defaultgroup attributes default-domain value cisco.com username vpnuser password TXttW.eFqbHusJQM encrypted username vpnuser attributes group-lock value DefaultRAGroup http

server enable http 0.0.0.0 0.0.0.0 outside http 0.0.0.0 0.0.0 DMZ no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set myset esp-3des esp-md5-hmac crypto dynamic-map outside_dyn_map 10 set transform-set myset crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map crypto map outside_map interface outside crypto ca trustpoint CA1 enrollment terminal subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco Systems, C=US, St=North Carolina, L=Raleigh keypair my.CA.key crl configure crypto ca certificate chain CA1 certificate 3f14b70b0000000001f 308205eb 308204d3 a0030201 02020a3f 14b70b00 00000000 1f300d06 092a8648 86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31 15301306 0a099226 8993f22c 64011916 05636973 636f3115 3013060a 09922689 93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 1e170d30 37313232 37313430 3033365a 170d3038 31323236 31343030 33365a30 67311330 11060a09 92268993 f22c6401 19160363 6f6d3115 3013060a 09922689 93f22c64 01191605 63697363 6f311530 13060a09 92268993 f22c6401 19160554 53576562 310e300c 06035504 03130555 73657273 31123010 06035504 03130976 706e7365 72766572 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7 545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905 5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2 d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001a382 03313082 032d300b 0603551d 0f040403 02052030 34060355 1d11042d 302ba029 060a2b06 01040182 37140203 a01b0c19 76706e73 65727665 72405453 5765622e 63697363 6f2e636f 6d301d06 03551d0e 04160414 2c242ddb 490cde1a fe2d63e3 1e1fb28c 974c4216 301f0603 551d2304 18301680 14d9adbf 08f23a88 f114432f 79987cd4 09a403e5 58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081 ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453 2d57324b 332d4143 532c434e 3d434450 2c434e3d 5075626c 69632532 304b6579 25323053 65727669 6365732c 434e3d53 65727669 6365732c 434e3d43 6f6e6669 67757261 74696f6e 2c44433d 54535765 622c4443 3d636973 636f2c44 433d636f 6d3f6365 72746966 69636174 65526576 6f636174 696f6e4c 6973743f 62617365 3f6f626a 65637443 6c617373 3d63524c 44697374 72696275 74696f6e 506f696e 74863568 7474703a 2f2f7473 2d77326b 332d6163 732e7473 7765622e 63697363 6f2e636f 6d2f4365 7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06 01050507 01010482 010f3082 010b3081 a906082b 06010505 07300286 819c6c64 61703a2f 2f2f434e 3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230 4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143 65727469 66696361 74653f62 6173653f 6f626a65 6374436c 6173733d 63657274 69666963 6174696f 6e417574 686f7269 7479305d 06082b06 01050507 30028651 68747470 3a2f2f74 732d7732 6b332d61 63732e74 73776562 2e636973 636f2e63 6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b 332d4143 532e5453 5765622e 63697363 6f2e636f 6d5f4341 312e6372 74301506 092b0601 04018237 14020408 1e060045 00460053 300c0603 551d1301 01ff0402 30003015 0603551d 25040e30 0c060a2b 06010401 82370a03 04304406 092a8648 86f70d01 090f0437 3035300e 06082a86 4886f70d 03020202 0080300e 06082a86 4886f70d 03040202 00803007 06052b0e 03020730 0a06082a 864886f7

0d030730	0d06092a	864886f7	0d010105	05000382	010100bf	
99b9daf2	e24f1bd6	ce8271eb	908fadb3	772df610	0e78b198	
£945£379	5d23a120	7c38ae5d	8f91b3ff	3da5d139	46d8fb6e	
20d9a704	b6aa4113	24605ea9	4882d441	09f128ab	4c51a427	
fa101189	b6533eef	adc28e73	fcfed3f1	f4e64981	0976b8a1	
2355c358	a22af8bb	e5194b42	69a7c2f6	c5a116f6	d9d77fb3	
a7f3d201	e3cff8f7	48f8d54e	243d2530	31a733af	0e1351d3	
9c64a0f7	4975fc66	a017627c	cfd0ea22	2992£463	9412b388	
84bf8b33	bd9f589a	e7087262	a4472e69	775ab608	e5714857	
4£887163	705220e3	aca870be	b107ab8d	73faf76d	b3550553	
1a2b873f	156f9dff	5386c839	1380fda8	945a7f6c	c2e9d5c8	
83e2e761	394dd4da	63eaefc6	a44df5 qu	uit certif	Eicate ca	
7099f1994	4764e09c46	551da80a16	5b749c 308	32049d 308	320385	
a0030201	02021070	99£19947	64e09c46	51da80a1	6b749c30	
0d06092a	864886f7	0d010105	05003051	31133011	060a0992	
268993f2	2c640119	1603636f	6d311530	13060a09	92268993	
f22c6401	19160563	6973636f	31153013	060a0992	268993£2	
2c640119	16055453	57656231	0c300a06	03550403	13034341	
31301e17	0d303731	32313430	36303134	335a170d	31323132	
31343036	31303135	5a305131	13301106	0a099226	8993f22c	
64011916	03636f6d	31153013	060a0992	268993£2	2c640119	
16056369	73636f31	15301306	0a099226	8993£22c	64011916	
05545357	6562310c	300a0603	55040313	03434131	30820122	
300d0609	2a864886	f70d0101	01050003	82010f00	3082010a	
02820101	00ea8fee	c7ae56fc	a22e603d	0521b333	3dec0ad4	
7d4c2316	3b1eea33	c9a6883d	28ece906	02902f9a	d1eb2b8d	
f588cb9a	78a069a3	965de133	6036d8d7	6ede9ccd	ale906ec	
88b32a19	38e5353e	6c0032e8	8c003fa6	2fd22a4d	b9dda2c2	
5fcbb621	876bd678	c8a37109	f074eabe	2b1fac59	a78d0a3b	
35af17ae	687a4805	3b9a34e7	24b9e054	063c60a4	9b8d3c09	
351bc630	05£69357	833b9197	f875b408	cb71a814	69a1f331	
b1eb2b35	0c469443	1455c210	db308bf0	a9805758	a878b82d	
38c71426	afffd272	dd6d7564	1cbe4d95	b81c02b2	9b56ec2d	
5a913a9t	9b95caid	difici67	94b9'/ac'/	63249009	ta05ca4d	
6f13afd0	96819141	e492cie4	e50e15f1	cU15d13b	51020301	
0001a382	01613082	01603013	13050404	01040182	3/140204	
061e0400	43004130	00060355	10010404	03020186	30010603	
551d1301	01II0405	30030101 14422570	II301006	03551dUe	04160414	
06025514	12320011	144321/9	987CQ409	4403e558	30820103	
64617020	1104011D	102212010	0113dU01	12a001e1	0001D30C	
0401/03a	21212143	40304341	12102350	75626960	62252220	
20414555 46657025	20434630	43443020	45465050	102020209	77766967	
4D037923	1034136f	60666967	75726174	4054505	12100903	
53576562	20111333	63697363	6f2c///3	34636f64	3f636572	
74696669	63617465	5265766f	63617469	6f6e4c69	73743f62	
6173653f	6f626a65	6374436c	6173733d	63524c44	69737472	
69627574	696f6e50	6f696e74	86356874	74703a2f	2f74732d	
77326b33	2d616373	2e747377	65622e63	6973636f	2e636f6d	
2f436572	74456e72	6f6c6c2f	4341312e	63726c30	1006092b	
06010401	82371501	04030201	00300d06	092a8648	86f70d01	
01050500	03820101	001abc5a	40b32112	22da80fb	bb228bfe	
4bf8a515	df8fc3a0	4e0c89c6	d725e2ab	2fa67ce8	9196d516	
dfe55627	953aea47	2e871289	6b754e9c	1e01d408	3f7f0595	
8081f986	526fbe1c	c9639d6f	258b2205	0dc370c6	5431b034	
fe9fd60e	93a6e71b	ab8e7f84	a011336b	37c13261	5ad218a3	
a513e382	e4bfb2b4	9bf0d7d1	99865cc4	94e5547c	f03e3d3e	
3b766011	e94a3657	6cc35b92	860152d4	f06b2b15	df306433	
c1bcc282	80558d70	d22d72e7	eed3195b	d575dceb	c0caa196	
34f693ea	f3beee4d	aa2ef1c2	edba288f	3a678ecb	3809d0df	
b1699c76	13018f9f	5e3dce95	efe6da93	f4cb3b00	102efa94	
48a22fc4	7e342031	2406165e	39edc207	eddc6554	3fa9f396	ad
quit cryp	pto isakmp	o enable d	outside ci	rypto isał	<pre>xmp policy</pre>	Į
65535 aut	henticati	ion rsa-st	ia encrypt	ion 3des	hash md5	

group 2 lifetime 86400 crypto isakmp identity auto tunnel-group DefaultRAGroup general-attributes addresspool vpnpool default-group-policy Defaultgroup tunnelgroup DefaultRAGroup ipsec-attributes trust-point CA1 telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspectiontraffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! servicepolicy global_policy global prompt hostname context Cryptochecksum:e150bc8bab11b41525784f68d88c69b0 : end CiscoASA#

<u>VPN Client の設定</u>

次の手順を実行して、VPN Client を設定します。

1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択し、VPN クラ イアント ソフトウェアを起動します。

nal	Į.	Programs	•	- 	Accessories Internet Explorer	•	
S.	\bigcirc	Documents	•	6	Cisco Systems VPN Client	•	🔄 Uninstall VPN Client
ofes	5	Settings	+-		¥		VPN Client
ΩPr		Search	•				Cisco Systems Inc. VPN Client
S 200	۲	Help					
ð	<u>7</u>	Run					
Win	Ì	Shut Down					
1	Start	🖸 🥭 🚾 🔂 🔤 🔤 🕐	NNT\;	sys	Prabu	ا (Microsoft Certi 🖓 untitled - Paint 🛛 🖉

2. 次の手順を実行して、CA1 という名前の CA サーバから CA 証明書をダウンロードし、 Cisco VPN Client にインストールします。vpnuser に提供されたユーザ クレデンシャルを使 用して、CA サーバ 172.16.5.1 にログインします。

File Edit View Favorites Tools Help Hack
🛏 Back 👻 🤿 🗸 🙆 🖓 🖓 Search 💿 Favorites 🛞 Media 🧭 🗄
ddress 🚳 http://172.16.5.1/certsrv
Enter Network Password
Please type your user name and password. Site: 172.16.5.1 User Name vpnuser Password ******* Domain
OK Carth: CA のサ
バで、VPN Client ユーザのユーザ アカウントを持っていることを確認してください。

タンを選択して符号化方式を指定します。[Download CA certificate] をクリックします。

Download a CA Certificate, Certificate Chain, or CRL
Fo trust certificates issued from this certification authority, <u>install this CA cer</u>
o download a CA certificate, certificate chain, or CRL, select the certificate
CA certificate:
Encoding method:
O DER
• Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL
oortnow oor という夕前で CA 証明書をコンピュータに保存します。 デフォルトでけ フ

certnew.cer という名前で、CA 証明書をコンピュータに保存します。 デフォルトでは、フ <u>アイルは C:\Program Files\Cisco Systems\VPN Client に保存されます。</u>

File Dowr	nload	
?	Some files can h looks suspicious save this file.	arm your computer. If the file information below , or you do not fully trust the source, do not open or
	File name:	certnew.cer
	File type:	Security Certificate
	From:	172.16.5.1
	🔥 This type o malicious c	f file could harm your computer if it contains ode.
	Would you like t	o open the file or save it to your computer?
	<u>O</u> pen	<u>Save</u> Cancel <u>M</u> ore Info VPN Client で
[Certificat	tes] タブをクリ	ックし、[Import] を選択します。[Import from File] オプション ボタ

[Certificates] タブをクリックし、[Import] を選択します。[Import from File] オプション ボタ ンをクリックし、[Browse] をクリックして、保存場所の C:\Program Files\Cisco Systems\VPN Client から CA 証明書をインポートします。[Import] をクリックします。証明 書が正常にインポートされたことを示すダイアログ ボックスが表示されます。

👌 sta	atus: Discor	nnected	VPN Clien	it - Vers	sion 4.8	.02.00	10			
Conne	ection Entries	; Status	Certificates	s Log	Options	Help				
() Vi	iew I	mport	Export	Er] → iroll	Yerif	y y	X Delete		
Conne	ection Entrie	s Certif	icates L	og						
Numb	er	Certif	icate				Store	Δ		Key Size
0	👌 VPN Cli	ent In	nport Cert	ificate						
	Import	from <u>F</u> ile								
	Im	port <u>P</u> ath	ram Files\C	isco Sys	tems\VF	'N Client	\certne	w.cer	B	rowse
	Import F	o <u>a</u> ssword:								
	C Import	from <u>M</u> icro		Certific	ate succ	essfully	importe	ed.		
Not co	Import (Certificate:			ОК				word r	
	identity	certificate:) 3.					por	word t	NOCECC
	<u>N</u> ew	Password	:							
	<u>C</u> onfirm	Password	:							
						Γ	<u>I</u> mp	port		Cancel
ficates Connectio] タブに [C on Entries Stal	A Certific	ates CA1] Ites Log Opt	と表示す tions Help	<u>されます</u>	- <u> </u>				
View		Export	€ +		siifu					ili Ci

	View	Impo	rt Expor	t	Enroll	Verif	У	Delete		CISC	0
C	Connection Ent	tries	Certificates	Log							
N	umber		Certificate				Store	Δ	Key Size	Validity	J
)			CA1				CA		2048	until Dec 14, 2012 1	14

注: [Show CA/RA Certificates] オプションを選択していることを確認します。 選択されてい ないと、証明書ウィンドウに CA 証明書が表示されません。

🔕 status: Disconnect	ted	VPN Client	- Ver	sion 4.8.	.02.0010
Connection Entries Sta	atus 🛛	C <u>e</u> rtificates	Log	Options	Help
		<u>⊻</u> iew…			
View Import		<u>I</u> mport			
Connection Entries	Certif	E <u>x</u> port			
Number	Certif_	E <u>n</u> roll			
0 C	:A1	Verify			
		D <u>e</u> lete			
		⊆hange	Certif	icate Pas	sword,,
		<u>R</u> etrieve	: Appr	oved Cer	tificate
		✓ Show CA	A/RA 🤇	Certificate	es

3. 次の手順を実行して、ID 証明書をダウンロードし、VPN Client にインストールします。CA のサーバ CA1 で、[Request a Certificate] > [advanced certificate request] > [Create and submit a request to this CA] の順に選択し、ID 証明書を登録します。[Submit] をクリックし ます。

Certificate Temp	ilate:
	User
Key Options:	
	O Create new key set O Use existing key set
CSP:	Microsoft Enhanced Cryptographic Provider v1.0
Key Usage:	Exchange
Key Size:	1024 Min: 384 (common key sizes: <u>512</u> <u>1024</u> <u>2048</u> <u>4096</u> <u>8192</u> <u>16384</u>) Max:16384
	 Automatic key container name O User specified key container na
	✓ Mark keys as exportable □ Export keys to file
	Enable strong private key protection
	Store certificate in the local computer certificate store Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.
Additional Optio	ns:
Request Format:	OCMC ©PKCS10
Hash Algorithm:	MD5 Conly used to sign request.
	Save request to a file
 [Yes] をクリックし	って次に進みます。
otential Scripting Viola	tion 2
This Web site is Do you want to	requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you request a certificate now?
	Yes No
[Install this certific	ate] をクリックします。
Microsoft Certifi	cate Services CA1
Certificate Is:	sued
The certificate	you requested was issued to you.
Est Inst	t <u>all this certificate</u> [Yes] をクリックして次に進み

Potential S	icripting Violat	ion								2
⚠	This Web site is security risk. Th computer and ga	adding one or Web site co ain access to	r more certifi uld install te your data	icates to this rtificates yo	s computer. A ou do not trus	Allowing an u t, which coul	ntrusted We Id allow proj	eb site to up grams that v	date your cer ou do not tru	tificates is a st to run on this
	Do you want this	; program to	add the cert	ificates now	7 Click Yes if	you trust thi	s Web site.	Otherwise, c	lick. No.	
				Yes	;	No				
次の図の	りように、	証明書が	インスト	ヽールさ	れたこと	とを示す	メッセ-	−ジが表	示されま	ミす。
Micros	oft Certific	ate Sei	vices -	- CA1						
Certifi	cate ins	talled								
		canva								
							- 111			
′our n	ew certif	cate h	as be	en suc	cessfu	Illy inst	alled.	VPN Cli	ient を終	了して再
[/] our ni 起動し、	ew certif インスト・	cate h -ルされ	as bee	en suc 明書が、	cessfu 、次の図	Illy inst に示すよ	alled. 、うに v	VPN Cli PN Clie	ient を終 nt の [Ce	了して再 ertificates]
[′] our n _' 起動し、 タブにま	ew certif インスト・ 長示される。	cate h ールされ ょうにし	as be た ID 証 ます。	en suc 明書が、	:cessfu 、次の図	Illy inst に示すよ	alled. 、うに v	VPN Cli PN Clie	ient を終 nt の [Ce	了して再 ertificates]
OUT N 起動し、 タブに引	ew certif インスト・ 気示される。 Entries Statu:	cate h ールされ ょうにし	asbeo たID証 ます。	ƏN SUC 明書が、 Options Hi	Cessfu 、次の図 elp	Illy inst に示すよ	alled. 、うに v	VPN Cli PN Clie	ient を終 nt の [Ce	了して再 ertificates]
OUT N 起動し、 タブに引 Connection	ew certif インスト・ 気示される。 Entries Statu:	cate h ールされ ようにし	as be た ID 証 ます。 s Log (en suc 明書が、 Options Hi	ccessfu 、次の図 响	Illy inst に示すよ	alled. こうに V	VPN Cli PN Clie	ient を終 nt の [Ce	了して再 ertificates]
YOUIT In 起動し、 タブに引 onnection View	ew certif インスト・ 表示される。 Entries Status 「 Import	cate h ールされ ようにし ; Certificat	asber たID証 ます。 です Log (Enr	en suc 明書が、 Options H	COURT 、次の図 elp Verify	Illy inst に示すよ Delete	alled. 、うに V	VPN Cli PN Clie	ient を終 nt の [Ce	了して再 ertificates] ・
OUT No 起動し、 タブに引 Connection	ew certif インスト・ 長示される。 Entries Status Import	icate h ールされ ようにし Certificat	asber たID証 ます。 es Log (Enr	en suc 明書が、 ⊃ptions H	cessfL 、次の図 elp Verify	ully inst に示すよ Delete	alled. くうに V	VPN Cli PN Clie	ient を終 nt の [Ce	了して再 ertificates] IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
OUT Pr 起動し、 タブに引 onnection View Connection	ew certif インスト・ 気示される。 Entries Statu: Import	icate h ールされ ようにし ; Certificat Export tificates	asbeo たID証 ます。 ですいので Enr	en suc 明書が、 ⊃ptions Hi	COURTS	Illy inst に示すよ Delete	alled. こうに V	VPN Cli PN Clie	ient を終 nt の [Ce Validity	了して再 ertificates] ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

4. 次の手順を実行して、接続エントリ(*vpnuser*)を作成します。[Connection Entries] タブを クリックし、[New] をクリックします。Host フィールドにルーティング可能なリモート ピ アの IP アドレスを入力します。[Certificate Authentication] オプション ボタンを選択し、ド ロップダウン リストから ID 証明書を選択します。[Save] をクリックします。

Description:					
Host:	192.168.1.5)		cisco	
Authentication	Transport	Backup Servers	Dial-Up		
C Group Authe	entication		O Mutual Gro	up Authentication	1
Name:					
Password:					
Confirm Pass	word:				
			<u>_</u>		
 Certificate Ar 	uthentication				
Name: 0-U	sers + vpnuser ((Microsoft)	J		
🔽 Send CA	Certificate Chair	n			
Erase User Pass	word		Save	Cancel	
Erase User Pass Connectl をクリ	word リックします。		Save	Cancel	-
Erase User Pass [Connect] をクリ 3 status: Disconne	word リックします。 ccted VPN Client	t - Version 4.8.02.00	Save	Cancel	
Erase User Pass [Connect] をクリ status: Disconne Connection Entries	word リックします。 ected VPN Client Ratus Certificates	t - Version 4.8.02.00 Log Options Help	Save	Cancel	
Erase User Pass Connect] をクリ status: Disconne Connection Entries S	word リックします。 ected VPN Client Ratus Certificates	t - Version 4.8.02.00 Log Options Help	Save	Cancel	
Erase User Pass Connect] をクリ status: Disconne Connection Entries S Cancel Connect N Connection Entries	word リックします。 cted VPN Client Ratus Certificates New Import	t - Version 4.8.02.00 Log Options Help	Save	Cancel	 cisco
Erase User Pass Connect] をクリ status: Disconne Connection Entries S Cancel Connect N Connection Entries	word リックします。 cted VPN Client Ratus Certificates New Import Certificates Lo ection Entry △	t - Version 4.8.02.00 Log Options Help Modify D	Save	Cancel	

6. ダイアログボックスが表示されたら、xauth のユーザ名とパスワード情報を入力して、[OK] をクリックし、リモート ネットワークに接続します。

CISCO SYSTEMS Username:	vpnuser		
Aniiiiiinaaniiiiina Password.		OK	Cancel
次の図に示すように、VPN Cli 参fstatus: Connected VPN Cli	ent が ASA に ent - Version 4	接続されま .8.01.0300	ਰ .

Connection Entries Status Certificates Log Options Help

<u>確認</u>

ASA では、コマンドラインで各種の show コマンドを使用して、証明書の状況を確認できます。

ここでは、設定が正常に動作していることを確認します。

• show crypto ca trustpoint — 設定されているトラストポイントを表示します。CiscoASA#show crypto ca trustpoints Trustpoint CA1: Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com Serial Number: 7099f1994764e09c4651da80a16b749c Certificate configured.

• show crypto ca certificate — システムにインストールされているすべての証明書を表示しま

f • CiscoASA#show crypto ca certificates Certificate Status: Available Certificate Serial Number: 3f14b70b0000000001f Certificate Usage: Encryption Public Key Type: RSA (1024 bits) Issuer Name: cn=CA1 dc=TSWeb dc=cisco dc=com Subject Name: cn=vpnserver cn=Users dc=TSWeb dc=cisco dc=com PrincipalName: vpnserver@TSWeb.cisco.com CRL Distribution Points: [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services, CN=Services,CN=Configuratio n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass= cRLDistributionPoint [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl Validity Date: start date: 14:00:36 UTC Dec 27 2007 end date: 14:00:36 UTC Dec 26 2008 Associated Trustpoints: CA1 CA Certificate Status: Available Certificate Serial Number: 7099f1994764e09c4651da80a16b749c Certificate Usage: Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=CA1 dc=TSWeb dc=cisco dc=com Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com CRL Distribution Points: [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services, CN=Services,CN=Configuratio n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass= cRLDistributionPoint [2] http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl Validity Date: start date: 06:01:43 UTC Dec 14 2007 end date: 06:10:15 UTC Dec 14 2012 Associated Trustpoints: CA1

- show crypto ca crls キャッシュされている Certificate Revocation List (CRL; 証明書失効リ スト)を表示します。
- show crypto key mypubkey rsa 生成されたすべての暗号鍵ペアを表示します。
 CiscoASA#show crypto key mypubkey rsa Key pair was generated at: 01:43:45 UTC Dec 11 2007
 Key name: <Default-RSA-Key> Usage: General Purpose Key Modulus Size (bits): 1024 Key Data: 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509 99e95d6c b5bdaa25
 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541 f5a66eb1 6d337c70 29031b76 e58c3c6f
 36229b14 fefd3298 69f9123c 37f6c43b 4f8384c4 a736426d 45765cca 7f04cba1 29a95890 84d2c5d4
 adeeb248 a10b1f68 2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301
 0001 Key pair was generated at: 06:36:00 UTC Dec 15 2007 Key name: my.CA.key Usage: General
 Purpose Key Modulus Size (bits): 1024 Key Data: 30819f30 0d06092a 864886f7 0d010101 05000381
 8d003081 89028181 00b8e20a a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a
 570667d7 545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905 5ab94b18
 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2 d903f722 bd414b0a 3205aa05
 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001 Key pair was generated at: 07:35:18 UTC
 Dec 21 2007 CiscoASA#
- show crypto isakmp sa IKE 1 トンネル情報を表示します。CiscoASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total

IKE SA: 1 1 IKE Peer: 10.1.1.5 Type : user Role : responder Rekey : no State : MM_ACTIVE

• show crypto ipsec sa — IPSec トンネル情報を表示します。CiscoASA#show crypto ipsec sa interface: outside Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0) current_peer: 10.1.1.5, username: vpnuser dynamic allocated peer ip: 10.5.5.10 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0 #pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #prefrag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: FF3EEE7D inbound esp sas: spi: 0xEFDF8BA9 (4024404905) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 4096, crypto-map: dynmap sa timing: remaining key lifetime (sec): 28314 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xFF3EEE7D (4282314365) transform: esp-3des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 4096, crypto-map: dynmap sa timing: remaining key lifetime (sec): 28314 IV size: 8 bytes replay detection support: Y

<u>Output Interpreter Tool</u>(OIT)(<u>登録</u>ユーザ専用)では、特定の show コマンドがサポートされ ています。 OIT を使用して、show コマンド出力の解析を表示できます。

<u>トラブルシューティング</u>

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

発生する可能性のあるエラーを次に示します。

- ERROR: Failed to parse or verify imported certificateこのエラーが発生する可能性があるのは、 、ID 証明書をインストールしたけれども、関連付けられたトラストポイントで認証された正しい中間証明書またはルート CA 証明書がない場合です。 正しい中間証明書またはルート CA 証明書を使用して削除と再認証を行う必要があります。 正しい CA 証明書を受け取っていることを確認するには、サードパーティ ベンダーに問い合せてください。
- Certificate does not contain general purpose public keyこのエラーが発生する可能性があるの は、正しくないトラストポイントに ID 証明書をインストールしようとした場合です。 無効 な ID 証明書をインストールしようとしているか、トラストポイントと関連付けられた鍵ペア が ID 証明書に含まれている公開鍵と合致しません。 正しいトラストポイントに ID 証明書を インストールしたことを確認するには、show crypto ca certificates trustpointname コマンド を使用します。 Associated Trustpoints がある行を探します。 正しくないトラストポイント が表示されている場合は、このドキュメントで説明されている手順に従って、トラストポイ ントを削除して適切なトラストポイントを再インストールします。 また、CSR が生成されて から鍵ペアが変更されていないことを確認します。
- ERROR : ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:認証中に証 明書の問題が発生した場合に、VPN Client でこのエラーが表示される場合があります。 この 問題を解決するには、ASA/PIX 設定で crypto isakmp identity auto コマンドを使用します。

<u>関連情報</u>

- Cisco 適応型セキュリティ アプライアンスに関するサポート ページ(英語)
- <u>Cisco VPN Client に関するサポート ページ</u>
- Cisco PIX 500 シリーズ セキュリティ アプライアンス
- <u>Cisco Secure PIX ファイアウォール コマンド リファレンス</u>
- セキュリティ製品に関する Field Notice (PIX を含む)

- Requests for Comments (RFC)
 テクニカルサポートとドキュメント Cisco Systems