Exemple de configuration d'authentification IPSec sur ASA/PIX 7.x et clients VPN à l'aide de certificats numériques avec une autorité de certification Microsoft

Contenu

Introduction Conditions préalables Conditions requises Composants utilisés Produits connexes Conventions Configurez Diagramme du réseau Configurations Configuration ASA Résumé de configuration ASA Configuration du client VPN Vérifiez Dépannez Informations connexes

Introduction

Ce document décrit comment installer manuellement un certificat numérique de constructeur de tiers sur l'appliance de sécurité Cisco (ASA/PIX) 7.x, aussi bien que des clients vpn, afin d'authentifier les pairs d'IPSec avec le serveur de Microsoft Certificate Authority (CA).

Conditions préalables

Conditions requises

Ce document exige que vous avez accès à un Autorité de certification (CA) pour l'inscription de certificat. Tiers pris en charge des constructeurs que CA incluent Baltimore, Cisco, confient, iPlanet/Netscape, Microsoft, RSA, et Verisign.

Remarque: Ce document utilise le serveur Windows 2003 en tant que serveur CA pour le scénario.

Remarque: Ce document suppose qu'il n'y a aucune configuration VPN préexistante dans l'ASA/PIX.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5510 qui exécute la version de logiciel 7.2(2) et la version 5.2(2) ASDM.
- Client VPN qui exécute la version de logiciel 4.x et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

La configuration ASA peut également être utilisée avec la gamme Cisco 500 PIX qui exécute la version de logiciel 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco</u>.

<u>Configurez</u>

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil <u>Command Lookup Tool</u> (clients <u>enregistrés</u> seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

- Configuration ASA
- <u>Résumé de configuration ASA</u>
- <u>Configuration du client VPN</u>

Configuration ASA

Terminez-vous ces étapes afin d'installer un certificat numérique de constructeur de tiers sur l'ASA

Étape 1. Vérifiez que les valeurs Date, Heure et Fuseau Horaire soient exactes

Étape 2. Générez la paire de clés RSA

Étape 3. Créez le point de confiance.

Étape 4. Générez l'inscription de certificat.

Étape 5. Authentifiez le point de confiance

Étape 6. Installez le certificat

Étape 7. Configurez l'Accès à distance VPN (IPSec) pour utiliser le certificat nouvellement installé

Étape 1. Vérifiez que les valeurs Date, Heure et Fuseau Horaire soient exactes

Procédure ASDM

1. Cliquez sur **Configuration**, et ensuite sur **Properties**.

- 2. Développez la gestion de périphérique, et choisissez l'horloge.
- Vérifiez que les informations répertoriées sont correctes.Les valeurs pour la date, le temps, et le fuseau horaire doivent être précises pour que la validation appropriée de certificat se produise.

Configuration > Properties > De	evice Adminis	tration >	Clock					
Stort up Witzerd	Clock	and the second	CIGOR					
E C A A & Setur	- CADOM							
Anti Specifing	Use this s	creen to (configure	the ASA	A clock.			
Anti-Spooning								
Auto Lindete	Time Zone	; (GI	VIT+05:30)) Calcutt	а			
Client Lindate								
	Date							
			П			-	-	
	Decemi	oer 💌	1			200	7 💌	T 1
Banner	<u>م</u>	М	т	VAC.	т	F	~	Time
Boot Image/Confir							Ŭ	hh ∶mm ∶ss
CLI Prompt							1	
Clock								16 25 41
Console	2	3	4	5	6	7	8	
CSD Setup								Undete D
Device	9	10	11	12	13	14	15	Opdate D
FTP Mode	16	17	18	10	20	21	22	
ICMP Rules	.0	17	10	15	20	21	~~	
	23	24	25	26	27	28	29	
O NTP								
Password	30	31						
Secure Copy								
- 🙀 SMTP								
SNMP								
TFTP Server					Ap	olv		Reset
User Accounts				_	- 1*			

Exemple de ligne de commande

CiscoASA					
CiscoASA#show clock	16:25:49.580	IST Fr	i Dec	28	2007

Étape 2. Générez la paire de clés RSA

La clé publique générée RSA est combinée avec les informations d'identité de l'ASA pour former une demande du certificat PKCS#10. Vous devriez distinctement identifier le nom de clé avec le point de confiance pour lequel vous créez la paire de clés.

Procédure ASDM

- 1. Cliquez sur Configuration, et ensuite sur Properties.
- 2. Développez le certificat, et choisissez la paire de clés.
- 3. Cliquez sur

Add.

Configuration > Properties > Certific	ate > Key Pair			
	y Pair			
🗄 🖬 AAA Setup	Configure the loss pairs to be used in and	idiantan		
	configure the key pairs to be used in cen	incates.		
E-B ARP				
	Note: Operations on this screen are appli	ed immediately upon	completion and are irrev	ersible.
😑 🐼 Certificate				
Authentication				
an Enrolment	Key Pair Name	Usage	Modulus Size	a da
- El Import Certificate	rvey r di rvaine	Usago	mounus size	Add
- 🚟 Key Pair				1
Manage Certificat				Show Details
🗄 🙀 Trustpoi 🚺 Add Key Pai		×		
E 👔 Device Acce				Delete
E-So Device Admi	C the defendition of the			
Banner Name:	 Use default key name 			Refrech
Boot Ime	G my CA key			Tron con
CLI Prom	(* my cackey)			
Clock				
Console Size:	1024			
CSD Set				
Device Usage:	General Purpose C Specia			
FTP Moc				
ICMP Ru				
Manager				
Senerate N	ow Cancel He	ip di		
Passwo				

- 4. Écrivez le nom de clé, choisissez la taille de module, et sélectionnez le type d'utilisation. **Remarque:** La taille recommandée de paire de clés est 1024.
- 5. Cliquez sur **Generate Now**.La paire de clés que vous avez créée devrait être répertoriée dans la colonne de nom de paire de clés.

Exemple de ligne de commande



Étape 3. Créez le point de confiance

Des points de confiance sont exigés pour déclarer l'Autorité de certification (CA) que votre ASA utilisera.

Procédure ASDM

- 1. Cliquez sur Configuration, et ensuite sur Properties.
- 2. Développez le certificat, et puis développez le point de confiance.
- 3. Choisissez la **configuration**, et puis cliquez sur Add.

Configuration > Properties > Certificate > Trustpoint > Configuration					
Startup Wizard	Configur	ation			
🗈 💼 AAA Setup	1	in ma a Cardificata Ard	havity (CA) as a trustmaint		
	Coni	igure a Certificate Aut	nonty (CA) as a trustpoint.		
🖭 🐻 ARP					
E- Certificate		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add
Authentication					
Enrolment					Edit
Import Certificate					
					Dutit
Manage Certificat					Delete
E-162 Trustpoint					
Configuration					Request (
Export					

- Configurez ces valeurs : Nom de point de confiance : Le nom de point de confiance devrait être approprié à l'utilisation destinée. (Cet exemple utilise *CA1*.)Paire de clés : Sélectionnez la paire de clés générée dans l'<u>étape 2.</u> (my.CA.key)
- 5. Assurez que l'Inscription manuelle est sélectionnée.
- 6. Paramètres de certificat de clic.La boîte de dialogue de paramètres de certificat apparaît.
- 7. Cliquez sur Edit, et configurez les attributs répertoriés dans cette table :Pour configurer ces valeurs, choisissez une valeur dans la liste déroulante Attribute, entrez la valeur, puis cliquez sur

Add.			
🔂 Edit DN			
		Attribute	Value
		Common Name (CN)	CiscoASA.cisco.com
DN Attribute to be Added		Department (OU)	TSWEB
		Company Name (O)	Cisco Systems
Attribute: Select Attribute	Add >>	Country (C)	US
	[State (St)	North Carolina
Value:	Delete	Location (L)	Raleigh
ок	Cancel	Help	

- 8. Une fois que les valeurs appropriées ont été ajoutées, cliquez sur OK.
- 9. Dans la boîte de dialogue de paramètres de certificat, écrivez le FQDN dans le domaine FQDN de spécifier.Cette valeur devrait être le même FQDN que vous avez utilisé pour le

	🔂 Certificate Parameters		
	Enter the values for the para	ameters that are to be inc	luded in the certif
	Subject DN:	C=US,St=North Carolina,	L=Raleigh
	Subject Alternative Name (I	FQDN)	
	C Use FQDN of the dev	vice	
	Specify FQDN	CiscoASA.cisco.com	
	C Use none		
	E-mail:		
	IP Address:		
	🔲 Include device serial nu	mber	
nom commun (NC).	ок	Cancel	Help

- 10. Cliquez sur OK.
- 11. Vérifiez la paire de clés correcte est sélectionné, et clique sur la case d'option d'**Inscription manuelle d'utilisation**.
- 12. Cliquez sur **OK**, puis sur **Apply**.

🇯 Add Trustpoint Configur	ation		
Trustpoint Name:	1)	
🗌 Generate a self-signed	d certificate on en	rollment	
If this option is enabled	l, only Key Pair an	d Certificate Parameters	can be specified.
Enrollment Settings Rev	ocation Check C	RL Retrieval Policy CRL	. Retrieval Method OCSP
Key Pair: my.CA	.key	Show Details	New Key Pair
Challenge Password:		Confirm Challenge Password:	
Enrollment Mode can or	nly be specified if f	there are no certificates	associated with this trust
Enrollment Mode			
💿 Use manual er	nrollment		
C Use automatic	enrollment		
Enrollment URL:	http://		
Retry Period:	1	minutes	
Retry Count:	0	(Use 0 to indicate un	limited retries)
			Certificate Parameter
	ок	Cancel	Help

Exemple de ligne de commande

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-
<pre>trustpoint)#keypair my.CA.key ! Specifies key pair</pre>
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>

Étape 4. Générez l'inscription de certificat

Procédure ASDM

- 1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
- 2. Développez le certificat, et choisissez l'inscription.
- Vérifiez le point de confiance créé dans l'étape 3 est sélectionné, et le clic s'inscrivent. Une boîte de dialogue apparaît qui répertorie la demande d'inscription de certificat (également désignée sous le nom d'une demande de signature de certificat)

Enrollment Request To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA. You will need to install the certificate after receiving it. Go to Configuration > Properties > Certificate > Import Certificate to do so. Certificate Request: hvcNAQkCFhtDaXNjb0FTQSSteWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN AQEEBQADgYOANIGJAoGEALSYNIX1zk fo80z1V7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaREzngSgm1kmNYoMx6taicY9pbTVgFcfvJH2dsBoLSCh1KY mAH400UXb118BH2SSgxPX6BCe1C9BjJ2vdqCgqtxR404/1YP0oeKKfq7apCHvVHF AgmBAACgRjBEBgkqhkiG9w0BCQ4xNzA1MAsCA1UdbwQEAwIFoDAmBgNVHREHzAd qhtDaXNjb0FTQSSteWRvbWFpb15jaXNjby5jb20wDQYJKoZIhvcNQEEBQADgYEA gmoBmSRVhL0qyDtpS1bveKew0AdG5/fxnJRYU2Um11W6sG0KaJYCiFH//eaewF3 gjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4BXm4sXAqrw2CDdj0/SSEiQJGc= End - This line not part of the certificate request	ertificat).	
To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA. You will need to install the certificate after receiving it. Go to Configuration > Properties > Certificate > Import Certificate to do so. Certificate Request: hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN AQEBEQADgYOAMIGJAoCBAL5YNIx1zkf080z1V7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaPBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoLSGhIKY mAH40WUXbi18BH2SSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAACgrjBEBgkqhkiC9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 gEjVABVhP7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gomnkGTJ11v2CSDXz4EXm4sXAqrw2CDdj0/S5EiQJGc= End - This line not part of the certificate request	🛊 Enrollment Request	
To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA. You will need to install the certificate after receiving it. Go to Configuration > Properties > Certificate > Import Certificate to do so. Certificate Request: hvcNAQkCFhtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKoZIhvcN AQEBBQADgY0AMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaRBzngSgm1kmNY0Mx6taicY9pbTVgFcfvJH2dsBoL5Gh1KY mAH40WUXbi18BH2SSgxPX6BCeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAACgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDvQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSEVnL0qyDtpS1bveKev0AdG5/fxnJRYU2Uun11W6sC0KaJYC1FH//eaewF3 gBjVAEVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4EXm4sXAqrw2CDdj0/S5BiQJGc= End - This line not part of the certificate request		
You will need to install the certificate after receiving it. Go to Configuration > Properties > Certificate > Import Certificate to do so. Certificate Request: hvcNAQkCFhtDaXNjbOFTQSSteWRvbWFpbiSjaXNjby5jb2Owg28wDQYJKoZIhvcN AQEBBQADgYOAMIGJAoCBALSYNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psNFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoLSChlKY mAH40WUXbi18BH2SSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzAlMAsGA1UdDwQBAwIFoDAmBgNVHREHzAd ghtDaXNjb0FTQSSteWRvbWFpbi5jaXNjby5jb2OwDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4BXm4sXAqrw2CDdj0/SSBiQJGc= End - This line not part of the certificate request	To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA.	;
Go to Configuration > Properties > Certificate > Import Certificate to do so. Certificate Request: hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb2Owg28wDQYJKo2IhvcN AQEBBQADgYOAMIGJAoGBALSYNIX1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psNFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY mAH40WUXbi18BH2SSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb2OwDQYJKo2IhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpSlbveKew0AdC5/fxnJRYU2Uun11W6sGORaJYCiFH/eaewF3 gEjVABVhB7Ni6N29710mDAbnPsOR3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4EXm4sXAqrw2CDdj0/S5BiQJGc= End - This line not part of the certificate request	You will need to install the certificate after receiving it.	
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb2Owg28wDQYJKoZIhvcN AQEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaRBzngSgm1kmNYoMx6taicY9pbTVgFcfvJH2dsBoL5Ch1KY mAH40WUXbi18BH2SSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAACgRjBEBgkqhkiC9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjbOFTQSSteWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4EXm4sXAqrw2CDdj0/S5BiQJCc=	Go to Configuration > Properties > Certificate > Import Certificate to do so.	
Certificate Request: hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wg28wDQYJKo2IhvcN AQEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY mAH40WUXbi18BH2SSgxPX6BGeiC9BjJ2vdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKo2IhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4BXm4sXAqrw2CDdj0/S5BiQJGc=		
hvcNAQkCFhtDaXNjbOFTQS5teWRvbWFpbi5jaXNjby5jb2Owg28wDQYJKoZIhvcN AQEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY mAH4OWUXbi18BH2SSgxPX6BGeiC9BjJZvdqCgq+xR404/1YPOoeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 gonnkGTJ11vZCSDXz4BXm4sXAqrw2CDdj0/S5BiQJGc=	Certificate Request:	
AQEBBQADgYOAMIGJAoGBALSYNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm psMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY mAH40WUXbi18BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11vZCSDXz4BXm4sXAqrw2CDdj0/S5BiQJGc=	bycNAOkCEptDaXNibOETOS5teWEybWEpbi5iaXNiby5ib20wgZ8wD0YJKoZIbycN	7
psMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY mAH40WUXbi18BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/1YP0oeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uun11W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4BXm4sXAqrw2CDdj0/S5BiQJGc=	AOEBBOAD gYOAMIGJA oGBAL 5YNIx 1 zk fo80 zi V7x JdfA7 i RtkHXx2Npmr9A001 Fzm	-
mAH4OWUXbi18BHZSSgxPX6BGeiC9BjJZvdqCgq+xR4O4/1YPOoeKKfq7apCHvVHF AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb2OwDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnLOqyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwk2jBTwoe9LuR0gefWfyAH0 gonnkGTJ11v2CSDXz4BXm4sXAqrw2CDdj0/S5BiQJGc= D End - This line not part of the certificate request	psMFP7DeKPI0+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY	
AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzAlMAsGAlUdDwQEAwIFoDAmBgNVHREEHzAd ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= End - This line not part of the certificate request	mAH40WUXbil8BHZSSgxPX6BGeiC9BjJZvdgCgg+xR404/lYP0oeKKfg7apCHvVHF	1
ghtDaXNjbOFTQSSteWRvbWFpbi5jaXNjby5jb2OwDQYJKoZIhvcNAQBEBQADgYEA gmoBmSRVnLOqyDtpSlbveKewOAdG5/fxnJRYU2Uunl1W6sGOKaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPsOR3IyMwbr3eChIFwkZjBTwoe9LuROgefWfyAH0 gonnkGTJ11v2CSDXz4BXm4sXAqrw2CDdj0/S5BiQJGc= D End - This line not part of the certificate request	AqMBAAGqRjBEBqkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBqNVHREEHzAd	
gmoBmSRVnLOqyDtpSlbveKewOAdG5/fxnJRYU2UunllW6sGOKaJYCiFH//eaewF3 gEjVABVhB7Ni6N29710mDAbnPsOR3IyMwbr3eChIFwkZjBTwoe9LuROgefWfyAHO gonnkGTJllvZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= End - This line not part of the certificate request	ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA	
gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0 gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= D End - This line not part of the certificate request	gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3	
gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc= 0End - This line not part of the certificate request	gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0	
O End - This line not part of the certificate request	gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=	
End - This line not part of the certificate request		
	End - This line not part of the certificate request	-
ок	ОК	

4. Copiez la demande de l'inscription PKCS#10 sur un fichier texte, et puis soumettez le CSR enregistré à votre constructeur de tiers (tel que Microsoft CA) suivant les indications de cette procédure :Ouvrez une session au serveur 172.16.5.1 CA avec les credantials d'utilisateur fournis au serveur de vpn.

👰 about:blank - Microsoft I	nternet Explore	r provided by	' Cisco Sys	tems, Inc.	
File Edit View Favorites	Tools Help				
🖛 Back 🔻 🔿 👻 🙆 🐔	ථු 🛛 🔕 Search	🚡 Favorites	Media	🎯 🖏 -	4 e e
Address (http://172.16.5.1)	certsry				
Enter Net	work Password				? ×
00					
P 20	Please type you	r user name and	l password.		
V	Site:	172.16.5.1			
	User Name	vpnuser			
	Password	******)	
	Domain				
	🔲 Save this pa	assword in your p	password list	t	
			ОК		Cancel

Remarque: Veillez-vous pour faire expliquer à un utilisateur l'ASA (serveur de vpn) avec le serveur CA.La demande de clic un certificat > a avancé la demande de certificat, et puis la sélectionne soumettent une demande de certificat à l'aide d'un fichier CMC ou PKCS#10 base-64-encoded ou soumettent une demande de renouvellement à l'aide d'un fichier base-64-encoded

PKCS#7.

Address 🗃 http://172.16.5.1/certsrv/certrqad.asp	i∂Go Lin
Microsoft Certificate Services CA1	<u>Home</u>
Advanced Certificate Request	
The policy of the CA determines the types of certificates you can request. Click one of the following options to:	
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 request a base-64-encoded PKCS #7 file.	by using
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment st Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	ation.
Copiez et collez les informations encodées dans le champ texte enregistré de demande	e. et

Copiez et collez les informations encodées dans le champ texte **enregistré de demande**, et cliquez sur

Submit a Certi	ificate Request or Renewal Request
To submit a sav source (such as	ved request to the CA, paste a base-64-encode s a Web server) in the Saved Request box.
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	VQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAC 4BfcXd20LCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8 D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+ 8Ux9emhFHpGHnQ/MpSfU0dQ== not part of the certificate request Browse for a file to insert.
Certificate Temp	late:
	IPSEC -
Additional Attrib	utes:
Attributes:	
	Submit >

Cliquez sur la case d'option Codé en base 64, puis sur Télécharger le

Cortificate leaved	1	
The certificate you	requested wa	is issued to you.
O DER	encoded or	● Base 64 encoded
📷 Downlo	ad certificate	
1999 December	ad a artificato	abain

case de dialob de téléchargement de fichier apparaît, sauvegardez-la avec le nom **cert_client_id.cer**, qui est le certificat d'identité à installer sur

File D	ownload 🔀
	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
SA.	Always ask before opening this type of file

Exemple de ligne de commande

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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
30MXSNPO
mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
FIISY21z
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm

```
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uol3yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no ciscoasa(config)#
```

Étape 5. Authentifiez le point de confiance

Une fois que vous recevez le certificat d'identité du constructeur de tiers, vous pouvez poursuivre cette étape.

Procédure ASDM

- 1. Enregistrez le certificat d'identité sur votre ordinateur local.
- 2. Si vous étiez fourni un certificat base64-encoded qui n'a pas été livré comme fichier, vous devez copier le message base64, et le collez dans un fichier texte.
- 3. Renommez le fichier avec une extension de .cer.**Remarque:** Une fois le fichier est renommé avec l'extension de .cer, l'icône de fichier devrait afficher comme certificat comme



4. Double-cliquez sur le fichier de

Certificate	
General Details Certification Path	
Certificate Information	
Thizertificate 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	
	Remarque:

certificat.

« Windows n'a pas assez d'informations pour vérifier ce certificat » le message apparaît dans l'onglet Général, vous devez obtenir la racine CA de constructeur de tiers ou le certificat de CA intermédiaire avant que vous continuiez cette procédure. Contactez votre constructeur de tiers ou administrateur CA afin d'obtenir la racine émettante CA ou le certificat de CA intermédiaire.

- 5. Cliquez sur l'onglet de chemin de certificat
- 6. Cliquez sur le certificat de CA situé au-dessus de votre certificat d'identité délivré, et cliquez sur le certificat de

Certification gath	В
	⊻iew Certificate
Certificate <u>s</u> tatus:	
This contificate is OV	

informations détaillées au sujet du certificat d'authentification apparaissent.

7. Cliquez sur **Details** afin d'en savoir plus sur le certificat

Certificate		? X
General Details Certification Pa	th	
Show: All>		
Field	Value	<u> </u>
 Version Serial number Signature algorithm Issuer Valid from Valid to Subject Public key 	V3 611E E59B 0000 0000 0007 sha1RSA CA1, TSWeb, cisco, com Saturday, December 15, 2007 Monday, December 14, 2009 CiscoASA.cisco.com OU=TSW RSA (1024 Bits)	
	Edit Properties	
	ОК	

d'identité.
8. Avant que vous installiez le certificat d'identité, le certificat de CA doit être téléchargé du serveur CA et être installé dans l'ASA. Terminez-vous ces étapes afin de télécharger le certificat de CA du serveur CA nommé *CA1* :Ouvrez une session au serveur 172.16.5.1 CA avec des credantials d'utilisateur fournis au serveur de

🖹 abo	ut:blank - Micro	soft Internet Explo	rer	
File	<u>E</u> dit <u>V</u> iew F <u>a</u> v	orites <u>T</u> ools <u>H</u> elp		
🕒 Bao	k 🔻 🕘 👻 📕	😰 🏠 🔎 Search	ጵ Favorites	🛛 🖉
A <u>d</u> dres	s 🥘 http://172.1	6.5.1/certsrv		
	C 11- 170	46 5 4		0 1
	Lonnect to 172.	16.5.1	200	<u> </u>
	30 W		The second	
	Connecting to 17	2.16.5.1		
	<u>U</u> ser name:	🕵 vpnserver	-	·
	Password:	•••••		
		🔲 <u>R</u> emember m	y password	

Download un **certificat de CA, une chaîne de certificat ou un CRL**, et puis sélectionnez la case d'option de la **base 64** afin de spécifier la méthode de codage.Cliquez sur le **certificat de CA de**

téléchargement.

Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, <u>install this CA cer</u>
To download a CA certificate, certificate chain, or CRL, select the certificate
CA certificate:
Current [CA1]
ncoding method:
O DER
• Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Sauvegardez le certificat de CA à votre ordinateur avec le nom

	File Download - Security Warning	1
	Do you want to open or save this file?	
	Name: certnew.cer Type: Security Certificate, 1.64 KB From: 172.16.5.1 <u>O</u> pen <u>Save</u> Cancel	
certnew.cer.	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>	

- 9. Naviguez jusqu'à l'emplacement où vous avez enregistré le certificat d'autorité de certification.
- 10. Ouvrez le fichier avec un éditeur de texte, tel que le Bloc-notes. (Cliquez avec le bouton droit le fichier, et choisissez **envoient à > Notepad**.)
- 11. Le message base64-encoded devrait ressembler au certificat dans cette image

:

🛿 certnew.cer - Notepad <u>File E</u>dit F<u>o</u>rmat <u>H</u>elp ----BEGIN CERTIFICATE--MIIEnTCCA4WqAwIBAqIQcJnxmUdk4JxGUdqAoWt0nDANBqkqhkiG9w0BAQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT Bqojkiajk/IszaezFqvuu1dlyjeMMAoGA1uEAxMDQ0ExMB4xDTA3MTIxNDA2MDE0 MÍoXDTEVMTIXNDA2MTAXNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEVMBMGCgmS DomT8ixkARkwBwNpc2NvMRUwEwYKCZImiŹPyLGQBGRYFVFNXZWIXDDAKBgNVBĀMT AONBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuvvyiLmA9 BSGzMz3sCtR9TCMwOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5zd4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vŴeMijcQnŵdOq+ kx+sWaeNCjš1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI y3GoFGmh8zGx6ys1DEaUQxRvwhDbMIvwqYBXwKh4uC04xxQmr//Sct1tdwQcvk2v µBwCsptw7c1akTqfm5xK/d//z2eUuxrHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDhXx wPXR018CAwEAAa0CAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQE AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZr58I8jqI8RRDL3mYfNQJ pAP1wDccAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWM]MjBLZXk]MjBTZXJ2aWN]cyxD Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD PŴNvbT9jZXJ0aŴZpYŹF0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9 Y1JMRGlźdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j aXNjby5jb20vQ2vydEvucm9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sij/5L+KUV34/DoE4MicbXJeKr L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHqHUCD9/BZWAqfmGUm++HMljnW8liyIF bcNwxlQxsDT+n9Y0k6bnG6u0f4SgETNrN8EyYVrSGK0lE+0C5L+ytJvw19GZhlzE 10VUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCqFWNcNItcufu0x1b 1xxc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2ÉwGPn149zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1vD+p85at ---END CERTIFICATE----

- 12. Dans l'ASDM, la configuration de clic, et cliquent sur alors Properties.
- 13. Développez le certificat, et choisissez l'authentification.
- 14. Cliquez sur l'entrer le texte de certificat dans la case d'option d'hexadécimal ou de format base64.
- 15. Collez le certificat de CA base64-formatted de votre éditeur de texte dans la zone de texte.
- 16. Le clic

authentifient.

Configuration > Properties > Ce	ertificate > Authentication
🖂 🔊 Startup Wizard	Authentication
🕀 🚽 🖌 🖌 🖬	Authenticate a CA cartificate. As the year it of authentication, the CA cartificate will be account
	hustroint and installed on the device
😟 🐻 ARP	a dapoint and installou of the device.
	Tructuoint Name:
	CA1
E Certificate	
Authentication	Fingerprint (optional):
Enrollment	
	The certificate text can be specified if the selected trustpoint is configured for manual
🚟 Key Pair	
Manage Certificat	Certificate Text
🖻 🔯 Trustpoint	
Configuration	C Import from a file: Drowse,
🔂 Export	
- 🖗 Import	Enter the certificate text in hexadecimal or base64 format:
E f Device Access	6786.IGW/IRbf5//YpiTraRy6HEpirdLi6cHpHLiCD9/B70/ActmGLim++HMin/A
E 🛞 Device Administration	
- 🗐 Banner	Authentication Successful
Boot Image/Config	wGPn149zp:
CLI Prompt	
Clock -	The trustpoint CA1 has been authenticated.
Console	
CSD Setup	
Device	
FTP Mode	OK
On MP Rules	
Management Acc	
UNIP	
ALL Password	
Secure Copy	
SMIP	
SNMP -	Authenticate

17. Cliquez sur **OK**.

Exemple de ligne de commande

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
$\tt MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B$
AQUFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgmS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK
BgNVBAMT
${\tt A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu}$
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI

v3GoFGmh8zGx6vs1DEaUOxRVwhDbMIvwgYBXWKh4uC04xxOmr//Sct1t
dWOcvk2V
uBwCsptW7ClakTgfm5XK/d//z2eUuXrHYvS0CfoFvk1vE6/0lo+f0eSS
z+TlDhXx
wPXR018CAwEAAaOCAW8wggFrMBMGCSsGAOOBgicUAgOGHgOAOwBBMAsG
A1UdDwOE
AWIBH JAPBGNVHRMBAF8EBTADAOH/MB0GA1UdDgOWBBT7rb8I8jgI8RBD
L.3mYfNOJ
DAP1WDCCAOMGA1UdHwSB+zCB+DCB9aCB8gCB74aBtWxkYXA6Lv8vO049
PVRTLVcvSzMtOUNTLENOPUNEUCxDTilOdWJsaWMlMiBLZXklMiBTZXJ2
aWN1cvxD
TilTZXJ2aWNlcyxDTilDb25maWdlcmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
Q2xhc3M9
Y1JMRG1zdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMlj
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
cufu0x1b
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+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)#

Étape 6. Installez le certificat

Procédure ASDM

Utilisez le certificat d'identité fourni par le constructeur de tiers pour exécuter ces étapes :

- 1. Cliquez sur Configuration, et ensuite sur Properties.
- 2. Développez le certificat, et puis choisissez le certificat d'importation.
- 3. Cliquez sur l'entrer le texte de certificat dans la case d'option d'hexadécimal ou de format base64, et collez le certificat d'identité base64 dans le champ texte.



4. Cliquez sur l'importation, et puis cliquez sur OK.

Exemple de ligne de commande



LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJ1dm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/02xDB
7wXQaGph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/034wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc 1L5nuPsd8MaexBc=END CERTIFICATE quit
INFO: Certificate successfully imported
CiscoASA(config)#

Étape 7. Configurez l'Accès à distance VPN (IPSec) pour utiliser le certificat nouvellement installé

Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

 Choisissez la configuration > le VPN > l'IKE > les stratégies > ajoutent afin de créer une stratégie ISAKMP 65535 suivant les indications de cette image.

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

- 2. Cliquez sur **OK**, puis sur **Apply**.
- 3. Choisissez la **configuration > le >Add VPN > d'IPSec > de jeux de transformations** afin de créer un jeu de transformations (*myset*) suivant les indications de cette image

付 Add Transform Set		
Set Name:	/set	
Properties		
Mode:	• Tunnel	C Transport
ESP Encryption:	3DES	-
ESP Authenticatio	on: MD5	
ок	Cancel	Help

4. Cliquez sur OK, et puis appliquez

:

5. Choisissez la **configuration > le >Add VPN > d'IPSec > de règles IPSecs** afin de créer un crypto map avec la stratégie dynamique de la priorité 10 suivant les indications de cette image

Crea	te IPSec R	tule					
Tunn	el Policy (Cr	rypto Map) - Ba	isic Tunnel I	Policy (Crypto Ma	ap) - Advancec	I Traffic Selec	ction
	Interface:	outside	T	Policy Type	e: dynamic	T	Priority: 10
	Transform	Sets					
	Transform ESP-DES	n Set to Be Add		Add >>	myset		Move Up
	-			Remove			Move Down

- 6. Cliquez sur OK, et puis **appliquez**
- 7. Choisissez le Configuration > VPN > General > Group Policy > l'Add Internal Group Policy afin de créer une stratégie de groupe Defaultgroup suivant les indications de ces

	🚰 Add Internal Group Policy						
	Name: Defaultgroup						
	General IPSec Client Cor	nfiguration Client Fin	ewall Ha				
	Check an Inherit checkbox to let the corresponding se						
	Tunneling Protocols:	🔽 Inherit	🗖 IPSe				
	Filter:	🔽 Inherit					
	Connection Settings	🔽 Inherit					
images.							

🚺 Ad	d Internal G	iroup Policy				
	Name:	Defaultgroup				
Ĺ	General IPS	ec Client Confi	guration Client	Firewall I	Hardware Client	NAC VVebV
	Check an I	nherit checkbox	to let the corres	oonding se	tting take its valu	e from the def
	General C	lient Parameters	Cisco Client Pa	rameters	Microsoft Client	Parameters
	Banner	:			🔽 Inherit	
	Default	Domain:			🗆 Inherit 🤇	cisco.com

- 8. Cliquez sur OK, et puis appliquez
- 9. Choisissez la configuration > le VPN > la gestion d'adresse IP > les groupes IP > ajoutent afin de configurer le vpnpool de pool d'adresses pour que les utilisateurs de client vpn soient

	🗯 Add IP Pool	
	Name:	vpnpool
	Starting IP Address:	10.5.5.10
	Ending IP Address:	10.5.5.20
	Subnet Mask:	255.255.255.0
	OK	Canaal Hain
assignés dynamiquement.	UN	Cancer Help

- 10. Cliquez sur OK, et puis **appliquez**
- 11. Choisissez la configuration > le VPN > le général > les utilisateurs > ajoutent afin de créer un vpnuser de compte utilisateur pour l'accès de client

🗯 Add User Account		
(Identity) VPN Policy	WebVPN	
	Username:	vpnuser
	Password:	*****
	Confirm Password:	****
	🗌 User authenticat	ed using MSCHAP
	Privilege level is used with	h command authorization.
vpn.	Privilege Level:	2 💌
. Ajoutez cet utilisateur à		
DefaultRAGroup.		

Add User Account			
Identity VPN Policy VVebVPN	rresponding settir	ng take its valı	ue from the group
Group Policy:	🔽 Inherit		<u>-</u>
Tunneling Protocols:	🔽 Inherit	🗖 IPSec	VVebVPN
Filter:	🔽 Inherit		
Tunnel Group Lock:	🗌 Inherit	DefaultRA	Group
Store Password on Client System:	🔽 Inherit	C Yes	C No

- 13. Cliquez sur OK, et puis appliquez
- 14. Éditez le DefaultRAGroup comme décrit dans cette procédure :Choisissez la configuration
 > le VPN > le groupe de général > de tunnel > éditent.Choisissez Defaultgroup de la liste déroulante de stratégie de

	🕵 Edit Tunnel Group	
	Name: DefaultRAGroup Type: ipsec-ra	
	General IPSec PPP	
	Configure general access attributes from the following sub-tabs.	
	Basic Authentication Authorization Accounting Client Address .	
roupe.	Group Policy: Defaultgroup	oisissez

les **GENS DU PAYS de la** liste déroulante de groupe de serveurs d'authentification.

auuun	entineation				
🚺 Edi	t Tunnel G	roup			
	Name:	DefaultRAGroup		Type:	ipsec-ra
- (General 川	Sec PPP			
	Configure	general access attributes	from the follov	ving sub)-tabs.
	Basic	uthentication Authorizatic		Client	Address Assic
		Autorization Autorizatio	in p Accounting		. Auuress Assig
	To set	authentication server grou	n per interface	an to th	ne Advanced ta
		autronitoutor correr grou	p por interrition	, go to ti	
	Authe	ntication Server Group:			
	Addito	nicalori ociver oroup.	LECCHE	\mathcal{I}_{-}	

vpnpool de la liste déroulante d'affectation d'adresse du

🔂 Edit Tunnel	Group		
Name:	DefaultRAGroup	Type: ipsed	⊳ra
Genera	IPSec PPP		
Configur	e general access attributes from th	e following sub-tabs.	
Basic /	Authentication Authorization Acc	counting Client Addre	ss Assignmer
T(>	o specify whether to use DHCP or a IP Address Management > Assignm	address pools for addr nent.	ress assignme
ſ	DHCP Servers		
	IP Address:	Add >> Delete	
	Address Pools		
	To configure interface-specific ad	ddress pools, go to the	e Advanced ta
	Available Pools		Assigned
			Vpnpool
client.		Add >>	

15. Cliquez sur OK, et puis **appliquez**.

Cisc	coASA
Cisc	oASA(config)#crypto isakmp enable outside
Cisc	oASA(config)#crypto isakmp policy 65535
Cisc	oASA(config-isakmp-policy)#authentication rsa-sig
Cisc	oASA(config-isakmp-policy)#encryption 3des
Cisc	oASA(config-isakmp-policy)#hash md5 CiscoASA(config-
isakı	<pre>mp-policy)#group 2 CiscoASA(config-isakmp-</pre>
poli	cy)#lifetime 86400 CiscoASA(config-isakmp-
poli	cy)#exit CiscoASA(config)#crypto isakmp identity
auto	! Phase 1 Configurations CiscoASA(config)#crypt
ipse	c transform-set myset esp-3des esp-md5-hmac
Cisc	oASA(config)#crypto dynamic-map outside_dyn_map 10
set	transform-set myset CiscoASA(config)#crypto map
outs	ide_map 65535 ipsec-isakmp dynamic outside_dyn_map
Cisc	oASA(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

Résumé de configuration ASA

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 le170d30 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 lelfb28c 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	
4f887163	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	268993f2	
2c640119	16055453	57656231	0c300a06	03550403	13034341	
31301e17	0d303731	32313430	36303134	335a170d	31323132	
31343036	31303135	5a305131	13301106	0a099226	8993f22c	
64011916	03636f6d	31153013	060a0992	268993f2	2c640119	
16056369	73636f31	15301306	0a099226	8993f22c	64011916	
05545357	6562310c	300a0603	55040313	03434131	30820122	
300d0609	2a864886	f70d0101	01050003	82010£00	3082010a	
02820101	00ea8fee	c7ae56fc	a22e603d	0521b333	3dec0ad4	
7d4c2316	3bleea33	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	£875b408	cb71a814	69a1f331	
bleb2b35	0c469443	1455c210	db308bf0	a9805758	a878b82d	
38c71426	afffd272	dd6d7564	1cbe4d95	b81c02b2	9b56ec2d	
5a913a9f	9b95cafd	dfffcf67	94b97ac7	63249009	fa05ca4d	
6f13afd0	968f9f41	e492cfe4	e50e15f1	c0f5d13b	5£020301	
0001a382	016f3082	016b3013	06092b06	01040182	37140204	
061e0400	43004130	0b060355	1d0f0404	03020186	300£0603	
551d1301	01ff0405	30030101	ff301d06	03551d0e	04160414	
d9adbf08	f23a88f1	14432f79	987cd409	a403e558	30820103	
0603551d	1f0481fb	3081£830	81f5a081	f2a081ef	8681b56c	
6461703a	2f2f2f43	4e3d4341	312c434e	3d54532d	57324b33	
2d414353	2c434e3d	4344502c	434e3d50	75626c69	63253230	
4b657925	32305365	72766963	65732c43	4e3d5365	72766963	
65732c43	4e3d436f	6e666967	75726174	696f6e2c	44433d54	
53576562	2c44433d	63697363	6f2c4443	3d636f6d	3£636572	
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	
8081£986	526fbelc	c9639d6f	258b2205	0dc370c6	5431b034	
fe9fd60e	93a6e71b	ab8e7f84	a011336b	37c13261	5ad218a3	
a513e382	e4bfb2b4	9bf0d7d1	99865cc4	94e5547c	f03e3d3e	
3b766011	e94a3657	6cc35b92	860152d4	f06b2b15	df306433	
clbcc282	80558d70	d22d72e7	eed3195b	d575dceb	c0caa196	
34f693ea	f3beee4d	aa2ef1c2	edba288f	3a678ecb	3809d0df	
b1699c76	13018f9f	5e3dce95	efe6da93	f4cb3b00	102efa94	_
48a22fc4	/e342031	2406165e	39edc207	eddc6554	3ta9f396	ad
quit cryp	pto isakmp	p enable d	outside ci	rypto isal	<pre>cmp policy</pre>	7
165535 aut	nenticati	ion rsa-si	la encrypt	lon 3des	nash md5	

```
group 2 lifetime 86400 crypto isakmp identity auto
tunnel-group DefaultRAGroup general-attributes address-
pool vpnpool default-group-policy Defaultgroup tunnel-
group DefaultRAGroup ipsec-attributes trust-point CA1
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! 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 ! service-
policy global_policy global prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0 : end
CiscoASA#
```

Configuration du client VPN

Terminez-vous ces étapes afin de configurer le client vpn :

1. Sélectionnez le **début > les programmes > le client vpn de Cisco Systems > le client vpn** afin de lancer le logiciel de client



 Terminez-vous ces étapes afin de télécharger le certificat de CA du serveur CA nommé CA1 et l'installer dans le Client VPN Cisco :Ouvrez une session au serveur 172.16.5.1 CA avec les credantials d'utilisateur fournis au

🛏 Back 👻 🔿 👻 🖄) 😰 🚮 🔯 Search 📾 Favorites 🚳 Media 🎯 🗌
ddress 🙆 http://172	2.16.5.1/certsrv
Enter Nel	twork Password
	 Please type your user name and password.
গ	Site: 172.16.5.1
	User Name Vpnuser
	User Name
	User Name Password
	User Name Password Domain
	User Name vpnuser Password xxxxxx Domain Save this password in your password list

que: Veillez-vous pour faire expliquer à un utilisateur l'utilisateur de client vpn avec le serveur CA.Cliquez sur Download un **certificat de CA, une chaîne de certificat ou un CRL**, et puis sélectionnez la case d'option de la **base 64** afin de spécifier la méthode de codage.Cliquez sur le **certificat de CA de téléchargement**.

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:
Current [CA1]
ncoding method:
ODER Base 64
<u>Download CA certificate</u>
<u>Download CA certificate chain</u>
Download latest base CRL
Download latest delta CRL

Sauvegardez le certificat de CA à votre ordinateur avec le nom **certnew.cer**. Par défaut, le fichier enregistre à C:\Program Files\Cisco des systèmes \ client

chi <u>ler enreg</u> i	Sile a C. (Progra	am Files/Cisco des	systemes (CI	Tent
File Dowi	nload			J
?	Some files can looks suspiciou save this file.	harm your computer s, or you do not fully	. If the file inform trust the source	ation below , do not open or
	File name:	certnew.cer		
	File type:	Security Certificate	•	
	From:	172.16.5.1		
	A This type of malicious of	of file could harm yo code.	ur computer if it c	contains
	Would you like	to open the file or sa	ave it to your con	nputer?
on	<u>O</u> pen	Save	Cancel	<u>M</u> ore Info

vpn, cliquez sur l'onglet de **Certificats**, et puis choisissez l'**importation**.Cliquez sur l'**importation en provenance de la** case d'option de **fichier**, et puis cliquez sur **parcourent** afin d'importer le certificat de CA des _{systèmes} de C:\Program Files\Cisco d'emplacement de mémoire \ client vpn.Cliquez sur **Import**.Une boîte de dialogue est évident qu'énonce que le certificat a été avec succès importé.

👌 sta	itus: Discor	nnected	VPN Clier	it - Ye	rsion 4.8	.02.00	10		
Conne	ection Entries	: Status	Certificate	s Log	Options	Help			
6	Ş (F 📑	1 4	†	⊒ → •⊡3	Ś		X	
Vi	iew li	mport	Export	E	nroll	Veril	fy	Delete	
Conn	ection Entries	s Certif	ricates L	og					
Numb	er	Certif	ficate				Store	Δ	Key Size
0	👌 VPN Cli	ent In	nport Cert	ificate					
	Import	from <u>F</u> ile							
	Imp	port <u>P</u> ath	ram Files\C	isco Sy	stems\VP	N Clien	t\certne	w.cer	<u>B</u> rowse
	Import F	assword:							
			👌 VPN C	lient				×	
	C Import	from <u>M</u> icro	í 🕕	Certifi	cate succi	essfully	importe	ed.	
Not co	Import C	<u>e</u> rtificate:		_					v
					OK				
	Entering identity () a new pa certificate:	a S.					ssv	vord protect
	<u>N</u> ew	Password	:						
	<u>C</u> onfirm	Password	:						
						г			
							<u>I</u> mp	ort	Cancel

Certificats CA CA1 apparaissent dans l'onglet de Certificats

Certificats.						
Connection Entries S	tatus Certificates	Log Options	Help			
View Impo	nt Export	Enrol	Kang Verify	XX Delete		cisco
Connection Entries	Certificates Log	,				
Number	Certificate		Store	\triangle	Key Size	Validity
)	CA1		CA		2048	until Dec 14, 2012 11 4

Remarque: Assurez-vous que l'option de **Certificats de l'exposition CA/RA** est sélectionnée ; autrement, les Certificats CA n'apparaîtront pas dans la fenêtre de

	🤪 status: Disconne	ected	VPN Client	- Ver	sion 4.8	.02.0010	
	Connection Entries	<u>s</u> tatus	C <u>e</u> rtificates	Log	Options	Help	
		3	<u>⊻</u> iew…				
	View Imp) ort	<u>I</u> mport.				
		Certif	E <u>x</u> port.				
	Number	Certif	E <u>n</u> roll				ŀ
	0	CA1	Verify				
			D <u>e</u> lete				
			⊆hange	Certi	ficate Pas	sword	
			<u>R</u> etrieva	е Арр	roved Cer	tificate,,,	
certificat		(Show C	A/RA	Certificati	es 🔵	

3. Terminez-vous ces étapes afin de télécharger le certificat d'identité et l'installer dans le client vpn :Dans le serveur d'autorité de certification CA1, choisissez Demander un certificat > demande de certificat avancée > Créer et soumettre une demande de requête auprès de cette Autorité de certification afin de s'inscrire pour le certificat d'identité.Cliquez sur Submit.

Certificate Template:
User
Key Options:
Ocreate new key set Ocreate new key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0 💌
Key Usage: 🔎 Exchange
Key Size: 1024 Min: 384 (common key sizes: <u>512 1024 2048 4096 8192 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 Options:
Request Format: © CMC © PKCS10
Hash Algorithm: MD5 Only used to sign request.
Save request to a file
Cliquez sur oui pour
POURSUIVRE. Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you Do you want to request a certificate now?
Yes No
Le clic installent ce Microsoft Certificate Services CA1 Certificate Issued
The certificate you requested was issued to you.
certificat. Install this certificate Cliquez sur oui pour

poursu	ivre.
Potential	Scripting Violation
⚠	This Web site is adding one or more certificates to this computer. Allowing an untrusted Web site to update your certificates is a security risk. The Web site could install certificates you do not trust, which could allow programs that you do not trust to run on this computer and gain access to your data
	Do you want this program to add the certificates now? Click Yes if you trust this Web site. Otherwise, click No.
	Yes No
Vous d	levez recevoir le message installé par certificat suivant les indications de cette image
Micro	osoft Certificate Services CA1
Certi	ficate Installed
four	new certificate has been successfully installed. Quittez et puis relancez
le clien Certific	It vpn afin de permettre au certificat d'identité installé pour apparaître dans l'onglet de cats du client vpn suivant les indications de cette image

Connection Entries S	itatus Certificat	es Log Options	Help Venil) ly	Delete		ululu CISCO
Connection Entries	Certificates	Log					
Number	Certificate			Store	Δ	Key Size	Validity
	CA1			CA		2048	until Dec 14, 2012 11:40:
	Users + vpnuse	r		Microso	ft	1024	until Dec 26, 2008 18:27:

4. Terminez-vous ces étapes afin de créer une entrée de connexion (*vpnuser*) :Cliquez sur l'onglet d'entrées de connexion, et puis cliquez sur New.Entrez l'adresse IP du partenaire distant (routable) dans le champ Host.Sélectionnez la case d'option d'**authentification de certificat**, et choisissez le certificat d'identité de la liste déroulante.Cliquez sur

Description:	192.168.1.5			 cisco
Authentication	Transport	Backup Servers	Dial-Up	
C Group Auther	ntication		C Mutual (Group Authentication
Name:				
Password:				
Confirm Passw	ord:			
Certificate Au	thentication)	
Name: 0-Us	ers + vpnuser	(Microsoft)		
🔽 Send CA C	Certificate Cha	iin		

a status: Disconnect	ed VPN Client - Ver	sion 4.8.02.0010		_	
Connection Entries Sta	tus Certificates Log	Options Help			
Cancel Connect Net	v Import	Modify Delet	e	ulu CIS	(). CO
Connection Entries (Certificates Log				
Connect	ion Entry 🛆		Host	Transport	
vpnuser	ſ		192.168.1.5	IPSec/UDP	
.1					
1				 	•
Contacting the security (gateway at 192.168.1.5	5			

6. Une fois incité, écrivez les informations de nom d'utilisateur et de mot de passe pour le Xauth, et cliquez sur OK afin de se connecter au réseau

Enter Username an Cisco Systems	d Password. Username: vpnus Password: *******	er	
distant.		OK	Cancel
7. Le client vpn se connecte	à l'ASA suivant les 'PN Clienty - Version	s indications de cette 4.8.01.0300	e image

Vérifiez

Connection Entries

Sur l'ASA vous pouvez employer plusieurs commandes show à la ligne de commande afin de vérifier l'état d'un certificat.

Log

Options

Help

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

• crypto ca trustpoint d'exposition - Les affichages ont configuré des points de

Status Certificates

CONFIANCE.CiscoASA#**show crypto ca trustpoints** Trustpoint CA1: Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com Serial Number: 7099f1994764e09c4651da80a16b749c Certificate configured.

• affichez le crypto certificat Ca — Affiche tous les Certificats installés sur le

SyStème.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 crl Les affichages ont caché les listes des révocations de certificat (CRL).
- show crypto key mypubkey rsa Affiche toutes les cryptos paires de clés

Générées.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** Affiche l'IKE les 1 informations de tunnel.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 Dislays les informations de tunnel d'IPSec.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

L'<u>Outil Interpréteur de sortie</u> (clients <u>enregistrés</u> uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Voici quelques erreurs possibles que vous pourriez rencontrer :

- ERREUR : Failed to parse or verify imported certificateCette erreur peut se produire quand vous installez le certificat d'identité et que vous n'avez pas le certificat d'autorité de certification racine ou intermédiaire correct authentifié avec le point de confiance associé. Vous devez supprimer et réauthentifier avec le certificat d'autorité de certification racine ou intermédiaire correct. Contactez votre constructeur de tiers afin de vérifier que vous avez reçu le certificat de CA correct.
- Certificate does not contain general purpose public keyCette erreur peut se produire quand vous essayez d'installer votre certificat d'identité sur le point de confiance incorrect. Vous essayez d'installer un certificat d'identité non valide ou la paire de clés associée au point de confiance ne correspond pas à la clé publique contenue dans le certificat d'identité. Employez la commande de trustpointname de show crypto ca certificat afin de vous vérifier a installé votre certificat d'identité sur le point de confiance correct. Recherchez la ligne énonçant des points de confiance associés. si le point de confiance incorrect est répertorié, utilisez les procédures décrites dans ce document afin de supprimer et de réinstaller le point de confiance approprié. Vérifiez également que la paire de clés n'a pas changé depuis que la CSR a été générée.
- ERREUR : ASA/PIX. Sev=Warning/3 IKE/0xE3000081 Invalid remote certificate id:Vous pourriez recevoir cette erreur dans le client vpn si un problème se pose avec les Certificats pendant l'authentification. Afin de résoudre ce problème, utilisez la commande auto de crypto isakmp identity dans la configuration ASA/PIX.

Informations connexes

- Page d'assistance pour Serveur de sécurité adaptatif Cisco
- <u>Cisco VPN Client Support Page</u>
- Dispositifs de sécurité de la gamme Cisco PIX 500
- <u>Références des commandes du pare-feu Cisco Secure PIX</u>
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques Cisco Systems