Exemple de configuration de L2TP sur IPsec entre Windows 2000 et le concentrateur VPN 3000 à l'aide de certificats numériques

Contenu

Introduction Conditions préalables **Conditions requises Components Used Objectifs** Conventions Obtenir un certificat racine Obtenir un certificat d'identité pour le client Création d'une connexion au VPN 3000 à l'aide de l'Assistant de connexion réseau Configuration du concentrateur VPN 3000 Obtenir un certificat racine Obtenir un certificat d'identité pour le concentrateur VPN 3000 Configurer un pool pour les clients Configurer une proposition IKE Configuration de la SA Configurer le groupe et l'utilisateur Informations de débogage Informations de dépannage Informations connexes

Introduction

Ce document montre la procédure pas à pas utilisée pour se connecter à un concentrateur VPN 3000 à partir d'un client Windows 2000 utilisant le client intégré L2TP/IPSec. Nous supposons que vous utilisez des certificats numériques (autorité de certification racine autonome sans protocole CEP (Certificate Enrollment Protocol)) pour authentifier votre connexion au concentrateur VPN. Ce document utilise le service de certificats Microsoft pour l'illustration. Reportez-vous au site Web de <u>Microsoft</u> pour obtenir de la documentation sur la façon de le configurer.

Remarque : il s'agit d'un exemple uniquement car l'apparence des écrans de Windows 2000 peut changer.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document concernent la gamme de concentrateurs Cisco VPN 3000.

Objectifs

Dans cette procédure, vous effectuez les étapes suivantes :

- 1. Obtenir un certificat racine.
- 2. Obtenez un certificat d'identité pour le client.
- 3. Créez une connexion au VPN 3000 à l'aide de l'Assistant de connexion réseau.
- 4. Configurez le concentrateur VPN 3000.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Obtenir un certificat racine

Complétez ces instructions afin d'obtenir un certificat racine :

- Ouvrez une fenêtre de navigateur et tapez l'URL de l'autorité de certification Microsoft (généralement http://servername ou l'adresse IP de CA/certsrv).La fenêtre Bienvenue pour les demandes et les extractions de certificats s'affiche.
- Dans la fenêtre Bienvenue, sous Sélectionner une tâche, choisissez Récupérer le certificat de l'autorité de certification ou la liste de révocation de certificats et cliquez sur Suivant.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Favorites Icols Help	
Address 🖉 http://10.10.102.42/certsrv/	∂Go Links »
Microsoft Certificate Services win2kserver	<u>Home</u>
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other per the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upor of certificate you request. Select a task: Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate 	e ∋ople over n the type
1	lext>
E Done	

3. Dans la fenêtre Récupérer le certificat de l'autorité de certification ou la liste de révocation de certificats, cliquez sur Installer ce chemin de certification de l'autorité de certification dans le coin gauche.Le certificat CA est ajouté au magasin des autorités de certification racine de confiance. Cela signifie que tous les certificats que cette autorité de certification émet pour ce client sont approuvés.

	ficale Services - Microsoft Internet Explorer			
Elle Edil Mer	w Favoulles Ioole Help			
41 . H	Sim Retrict House Sound Faculty House	E Bur		
gåner 💽 http:/	/1921682550/ceture/cetcarc.aup			• 260 Links
Microsoft Cort	žicate Services — wisZkoarwer			Hame
Retrieve The	e CA Certificate Or Certificate Revocation Lis	it		
nstal this CA	certification path to allow your computer to trust	certificates issued from t	his certification authority	
t is not neces CA certificati	sary to manually install the CA certification path on path will be installed for you automatically.	if you request and install	a certificate from this certification author	ity, because the
Choose file	to download:			
CA Certificat	0 Current [win2kserver]			
	CER encoded or CBase 64 encoded			
	Download CA certificate			
	Download CA certification path			
	and the second of the second o			

Obtenir un certificat d'identité pour le client

Complétez ces étapes afin d'obtenir un certificat d'identité pour le client :

- 1. Ouvrez une fenêtre de navigateur et entrez l'URL de l'autorité de certification Microsoft (généralement http://servername ou l'adresse IP de CA/certsrv).La fenêtre Bienvenue pour les demandes et les extractions de certificats s'affiche.
- Dans la fenêtre de bienvenue, sous Sélectionner une tâche, choisissez Demander un certificat, puis cliquez sur Suivant.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Fgvorites Iools Help	10 M
Back Forward Stop Refresh Home Search Favorites History Mail Print	
Address C http://10.10.102.42/certarv/	▼ @Go Links *
Microsoft Certificate Services win2kserver	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other s program. Once you acquire a certificate, you will be able to securely identify yourself to oth the web, sign your e-mail messages, encrypt your e-mail messages, and more depending of certificate you request. Select a task: C Retrieve the CA certificate or certificate revocation list Request a certificate C Check on a pending certificate	secure her people over g upon the type
	Next>
🖉 Done	Internet

3. Dans la fenêtre Choisir un type de demande, sélectionnez Demande avancée et cliquez sur

Differendit Certificate Services - Microsoft Internet Explores	F
Elle Edit View Farvaltes Lack Help	1.
Address 0 Max //18 10.102 42/cetar/ceta.a.ao	▼ ,≥6. 10
Trend a t	-
Microsoft Configure Services - wirZksamer	Home
Choose Request Type	
Choose Request Type	
Please select the type of request you would like to make:	
C Liner confidente request	
Cost Contractorequest.	
E-Meil Protection Centricate	
R	
Advanced request	
	Next >
	a harrest

4. Dans la fenêtre Demandes de certificat avancées, sélectionnez Envoyer une demande de certificat à cette autorité de certification à l'aide d'un



5. Renseignez les champs comme dans cet exemple.La valeur de Department (unité d'organisation) doit correspondre au groupe configuré sur le concentrateur VPN. Ne spécifiez pas une taille de clé supérieure à 1024. Veillez à cocher la case Utiliser le magasin de machines locales. Lorsque vous avez terminé, cliquez sur

Next

Advanced Certif	ificate Request	*
Identifying Inform	vation:	
Name	: win2kdientid	
E-Mail:		
Company	eliga .	
Department	support	
City	c (hanklin	1
State	E ma	
CountryRegion	us	
Intended Purpose	8	
	Client Authentication Certificate	
Key Options:		
CSP	Microsoft Base Cryptographic Provider v1.0	
Key Usage:	: C Eschange ∉ Signature C Both	1
Key Bize:	1: 512 Max 304 Max 19294 Boormon Rey steel 512 2025 2020 2020 3	
	@ Create new key set	
	E Set the container name	
	C Use existing key set	
	Enable strong private key protection	15
	🗁 Mark keys as exportable	
	Vise local machine store You must be an administrator to generate a say to the local machine store.	-10

elon la configuration du serveur AC, cette fenêtre apparaît parfois. Dans ce cas, contactez l'administrateur de l'autorité de

Certificate Pending	
Your cartificate remust has been received	However, you must wait for an administrator to issue the cartificate you remested
Please entry to this web site is a day actu	n in moren, you make male male an annihitati anni prioduk ink centricate you requested.
Prease return to dits web site in a day of be	io to retrave your certificate.
Note: You must return with this web browser within	n 10 days to retrieve your certificate

6. Cliquez sur **Home** pour revenir à l'écran principal, sélectionnez **Check on pending certificate**, puis cliquez sur

Please select the certif	icate request you want to check		
Clark Mathematication	Carliceso (82/15/2000 09 50:59)		
			Next

7. Dans la fenêtre Certificat émis, cliquez sur Installer ce

Microsofi Catalinate Services — witCharane	. Horn
Certificate issued	
The certificate you requested was issued to you.	
Install this certificate	

- 8. Afin d'afficher votre certificat client, sélectionnez **Démarrer > Exécuter**, et exécutez Microsoft Management Console (MMC).
- 9. Cliquez sur Console et choisissez Add/Remove Snap-in.
- 10. Cliquez sur Add et choisissez Certificate dans la liste.
- 11. Lorsqu'une fenêtre apparaît et vous demande l'étendue du certificat, sélectionnez **Computer Account**.
- 12. Vérifiez que le certificat du serveur AC se trouve sous Autorités de certification racine de confiance. Vérifiez également que vous avez un certificat en sélectionnant Console Root > Certificate (Local Computer) > Personal > Certificates, comme indiqué dans cette image.

Console1	a dia mandri di secondo di second		
<u>⊆</u> onsole <u>Wi</u> ndow <u>H</u> elp			
🚡 Console Root\Certificate	es (Local Computer)\Personal\Certil	Irates	
Action yew Eavorites	+ + [] [] [] [] []	13	12
Tree Favorites	Essued To /	Issued By	Expiration
Console Root Certificates (Local Com Personal Trusted Root Certif Enterprise Trust Enterprise Trust Enterpri	22 win2kclientid	win2kserver	3(1(2001
Personal store contains 1 certific			1

<u>Création d'une connexion au VPN 3000 à l'aide de l'Assistant de</u> <u>connexion réseau</u>

Complétez cette procédure afin de créer une connexion au VPN 3000 à l'aide de l'assistant de connexion réseau :

- 1. Cliquez avec le bouton droit sur **Favoris réseau**, choisissez **Propriétés** et cliquez sur **Créer une connexion**.
- Dans la fenêtre Network Connection Type, choisissez Connect to a private network through the Internet, puis cliquez sur Next.

Networ You you	k Connection Type I can choose the type of network connection you want to create, based on I network configuration and your networking needs.
~	
C.	Dial-up to private network
	Connect using my phone line (modern of 15DM).
0	Dial-up to the Internet
	Connect to the Internet using my phone line (modem or ISDN).
œ	Connect to a private network through the Internet
	Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
C	Accept incoming connections
	Let other computers connect to mine by phone line, the Internet, or direct cable
-	
0	<u>Connect directly to another computer</u>
	Connect using my serial, parallel, or infrared port.
	Z Rack Neut Cancel

3. Entrez le nom d'hôte ou l'adresse IP de l'interface publique du concentrateur VPN, et cliquez sur

Next.

etwork Connectio	n Wizard				
Destination Add What is the n	Iress ame or address of the	e destination?			Ĩ
Type the host connecting.	name or IP address	of the computer or	network to wh	ich you are	
<u>H</u> ost name or	IP address (such as	microsoft.com or 12	23.45.6.78):		
64.67.72.180	Č.				
2					
		Z Pa	ok 🕅	aut x	Cancel

 Dans la fenêtre Disponibilité de la connexion, sélectionnez Uniquement pour moi-même et cliquez sur Suivant.

Network Connection Wizard
Connection Availability You may make the new connection available to all users, or just yourself.
You may make this connection available to all users, or keep it only for your own use. A connection stored in your profile will not be available unless you are logged on.
Create this connection:
O For all users
Only for myself
< Back Next > Cancel

5. Dans la fenêtre Public Network (Réseau public), indiquez si la connexion initiale (le compte FAI) doit être établie automatiquement.

Network Connection Wizard	
Public Network Windows can make sure the public network is connected first.	S)
Windows can automatically dial the initial connection to the Internet or other public network, before establishing the virtual connection.	
O Do not dial the initial connection.	
Automatically dial this initial connection:	
Cisco corporate VPN	•
< Back Next > 0	Cancel

 Dans l'écran Destination Address, entrez le nom d'hôte ou l'adresse IP du concentrateur VPN 3000, puis cliquez sur Next.

work Connection Wizard	
Destination Address What is the name or address of	f the destination?
Type the host name or IP addres connecting.	ess of the computer or network to which you are
Host name or IP address (such a	as microsoft.com or 123.45.6.78):
64.67.72.180	
	< Back Next > Cancel

7. Dans la fenêtre Assistant Connexion réseau, entrez un nom pour la connexion et cliquez sur **Terminer**.Dans cet exemple, la connexion est nommée « Cisco corporate VPN ».



8. Dans la fenêtre Connexion privée virtuelle, cliquez sur

Connect Virtua	Private Connection	<u>? ×</u>
		P P
User name:	jedgaruser	
Password:	******	
	Save Password	
Connect	Cancel Properties	Help

Propriétés.

- 9. Dans la fenêtre Propriétés, sélectionnez l'onglet Mise en réseau.
- 10. Sous Type de serveur VPN que j'appelle, choisissez L2TP dans le menu déroulant, sélectionnez Internet Protocol TCP/IP, puis cliquez sur

Cisco corporate VPN		<u>? ×</u>
General Options Secu	rity Networking	
Type of VPN server I am	calling:	
Layer-2 Tunneling Proto	col (L2TP)	_
		Settings
Components checked a	re used by this conne	ection:
 ✓ Internet Protocol ✓ ↓ ✓ ↓	(TCP/IP) Sharing for Microsoft I oft Networks	Networks
Install	Uninstall	Properties
Description Transmission Control F wide area network pro across diverse interco	Protocol/Internet Pro stocol that provides c nnected networks.	tocol. The default
		IK Cancel

- Properties. 11. Sélectionnez Avancé > Options > Propriétés.
- 12. Dans la fenêtre IP Security, sélectionnez Use this IP security



- 13. Sélectionnez la stratégie **Client (Répondre uniquement)** dans le menu déroulant, puis cliquez sur **OK** plusieurs fois jusqu'à ce que vous reveniez à l'écran Connect.
- 14. Afin de lancer une connexion, entrez votre nom d'utilisateur et votre mot de passe, et cliquez sur **Connect**.

Configuration du concentrateur VPN 3000

Obtenir un certificat racine

Complétez ces étapes afin d'obtenir un certificat racine pour le concentrateur VPN 3000 :

- Pointez votre navigateur vers votre autorité de certification (généralement http://ip_add_of_ca/certsrv/), récupérez le certificat de l'autorité de certification ou la liste de révocation de certificats, puis cliquez sur Suivant.
- 2. Cliquez sur **Download CA certificate** et enregistrez le fichier quelque part sur votre disque local.
- 3. Sur le concentrateur VPN 3000, sélectionnez Administration > Certificate Management, et cliquez sur Click here to install a certificate and Install CA Certificate.
- 4. Cliquez sur Upload File from Workstation.
- 5. Cliquez sur Browse et sélectionnez le fichier de certificat CA que vous venez de télécharger.
- 6. Sélectionnez le nom du fichier et cliquez sur **Install**.

Configuration	Administration Certificate	Idministration Certificate Management				
Administration						
-Administer Sessions						
	This section lets you view a	and manage certificates on the \	/PN 3000 Concentrator	C		
-System Reboot		-				
Ping	 <u>Click here to enroll</u> 	with a Certificate Authority				
-Monitoring Refresh	 <u>Click here to install</u> 	a certificate				
- CO-Access Rights	Cartificate Authorities	former and the sector sector and				
- @File Management	Certificate Authonties	(current: 1, maximum: 6)				
Certificate Management	Subject	Issuer	Expiration	SCEP Issuer	Actions	
Enrollment	snsvpc7-ca at cisco	snsvpc7-ca at cisco	02/11/2004	No	[View Configure Delete]	
Installation	Assessments	sentration of the second s	nanagen and a state of the stat	havennessee		
⇒ Monitoring	Identity Certificates (cu	urrent: 0, maximum: 2)				
	Subject	Issuer	Exp	iration	Actions	
	No Identity Certificates					
				warmen der ein ben und en bei		
	001 0 10 10					

Obtenir un certificat d'identité pour le concentrateur VPN 3000

Complétez ces étapes afin d'obtenir un certificat d'identité pour le concentrateur VPN 3000 :

 Sélectionnez ConfAdministration > Certificate Management > Enroll > Identity Certificate, puis cliquez sur Enroll via PKCS10 Request (Manual). Remplissez le formulaire comme indiqué ici et cliquez sur

B-Configuration	Administration Certificate Managemen	it Enroll Mentity Certificate PKCS1	0
Administration			
Administer Sessions	Enter the information to be included in th	e certificate request. The CA's certificate	must be installed as a Certificate Authority before installing the
B Software Update	certificate you requested. Please wait for	the operation to finish.	
System Meboot			
Alandoring Refeet	Common Name (CN)	ma 2000	Enter the common name for the VPN 3000 Concentrator
Báccass Rights	common name (CH)	oburger-unit	to be used in this PKI.
-BFile Management			
- G-Certificate Management	Organizational Unit (OU)	ana	Enter the department.
-Enrollment			
Installation	Organization (O)	ciaco	Enter the Organization or company
B-Monitoring			
		- <i>W</i>	The second se
	Locality (L)	pul	Enter the city or town.
	State/Province (SP)	2	Enter the State or Province.
	Country (C)	ha	Enter the two-letter country abbreviation (e.g. United
	country (c)	2.6	States = US).
	tation million and so meanwhile	- 200 K	Enter the Fully Qualified Domain Name for the VPN 3000
	Subject AlternativeName (FQDN)	vpn3000-name.cisco.com	Concentrator to be used in this PKI.
	Subject AlternativeName (E-Mail	8	Enter the E-Mail Address for the VPN 3000
	Address)	-	Concentrator to be used in this PNL
		Providence in the second second	
	Key Size	RSA 512 bits 🗆	Select the key size for the generated RSA/DSA key pair.
	Enroll Cancel		
	t t		

Une fenêtre de navigateur apparaît avec la demande de certificat. Il doit contenir un texte similaire à celui-ci :

-----BEGIN NEW CERTIFICATE REQUEST----MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu czEOMAwGA1UEChMFY21zY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW11LmNpc2NvLmNvbTAN BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNflQDi+D7w8dxPu74b/BRHn9fsKI X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak= -----END NEW CERTIFICATE REQUEST----

- 2. Pointez votre navigateur vers votre serveur AC, cochez **Demander un certificat**, puis cliquez sur **Suivant**.
- 3. Cochez Advanced Request, cliquez sur Next, et sélectionnez Submit a certificate request using a base64 encoded PKCS #10 file or a renew request using a base64 encoded PKCS #7 file.

- 4. Cliquez sur **Next** (Suivant). Coupez et collez le texte de la demande de certificat précédemment affiché dans la zone de texte. Cliquez sur Submit.
- 5. Selon la configuration du serveur AC, vous pouvez cliquer sur Télécharger le certificat AC. Ou dès que le certificat a été émis par l'autorité de certification, revenez à votre serveur d'autorité de certification et cochez Vérifier un certificat en attente.
- 6. Cliquez sur Next, sélectionnez votre demande, puis cliquez à nouveau sur Next.
- 7. Cliquez sur Download CA certificate, et enregistrez le fichier sur le disque local.
- 8. Sur le concentrateur VPN 3000, sélectionnez Administration > Certificate Management > Install et cliquez sur Install certificate obtain via enrollment.Votre demande en attente s'affiche alors avec l'état En cours, comme dans cette

VPT	N 3000							Main Help Support
Con	centrator Series Mana	ager						Logged i
							Configur	ation Administration Mor
IEIP Teinet	Select a enrollment request to	install.						
SNMP.	Enrollment Status							
SNMP Communities	Enrollment Status Subject	Issuer	Date	Use	Reason	Method	Status	Actions
SNMP Communities	Enrollment Status Subject vpn3000-name at cisco	Issuer Not	Date 02/13/2002	Use	Reason	Method	Status In Progress	Actions [Very Instal, Delete.]

- 9. Cliquez sur Install, puis sur Upload File from Workstation.
- Cliquez sur Browse et sélectionnez le fichier qui contient votre certificat émis par l'autorité de certification.
- 11. Sélectionnez le nom du fichier et cliquez sur Install.
- 12. Sélectionnez Administration > Certificate Management. Un écran similaire à cette image

s'affiche.									
Configuration	Administration I Certificate Management.								
Administration Administer Sessions 	This section lets yo <u>Click here to</u> <u>Click here to</u> Certificate Author	u view and m enroll with a install a cer orities (curr	nanage certifi <u>a Certificate /</u> tifi <u>cate</u> ent: 1, maxim	icates o Authorit ium: 6)	n the VP	N 3000 Concentra	tor.		
	Subject	t	Issuer			Expiration	SCEP Issuer		
	snsvpc7-ca at cis	co	snsvpc7-ca	at cisc	0	02/14/2004	No	[Mew]	
Monitoring	Identity Certificates (current: 1, maximum: 2)								
	3	ubject			ls	Issuer Expira			
	vpn3000-name at	cisco	5	nsvpc7	-ca at ci	sco	02/14/2003	[View]]	
	SSL Certificate	Generate] No	te: The public	key in t	he SSL c	ertificate is also use	d for the SSH host k	iy.	
	Subjec	:t	1	Issuer		E	xpiration	1	
	No SSL Certificate								
	Enrollment State	US [Remove A	III: Errored Tin	ned-Out	Rejected	Cancelled In-Progre	22] (current: 0 availa	ble: 2)	
	Subject	Issuer	Dat	8	Use	Reason	Method	Sta	
	No Enrollment Red	quests							

Configurer un pool pour les clients

Effectuez cette procédure afin de configurer un pool pour les clients :

 Afin d'attribuer une plage disponible d'adresses IP, pointez un navigateur vers l'interface interne du concentrateur VPN 3000 et sélectionnez Configuration > System > Address Management > Pools > Add. 2. Spécifiez une plage d'adresses IP qui ne sont pas en conflit avec d'autres périphériques sur le réseau interne, et cliquez sur

Add.			
			Configuration Administration
<u> ← Configuration</u>	Configuration	System Address N	Aanagement Pools Add
- D System	Add an addres	is pool.	
Servers			
Assignment	Range Start	10.1.1.100	Enter the start of the IP pool address range.
Pools			
- Tunneling Protocols	Dongo Fod	10 1 1 000	Enter the and of the ID need address young
- IP Routing	Range End	10.1.1.200	Enter the end of the IP pool address range.
Management			
Protocols		Connel	
Events The Constraint	Add	Cancer	
- Client Undate			
l oad Balancing			
- III-User Management			
Policy Management			
Administration			
Monitoring			

 Afin de demander au concentrateur VPN 3000 d'utiliser le pool, sélectionnez Configuration > System > Address Management > Assignment, cochez la case Use Address Pools, et cliquez sur Apply, comme dans cette

image. Configuration | Administration | Monitoring Configuration -Interfaces This section presents Address Assignment options. Each of the following methods are tried, in order, ⊖System until an address is found. - Servers - Address Management Use Client Address -Assignment can be overridden by user/group configuration. -Pools Use Address from Authentication Server Check to use an IP address retrieved from an Server authentication server for the client. Tunneling Protocols -P Routing Management
 Protocols Use DHCP
Check to use DHCP to obtain an IP address for the client. - Events Use Address Pools E Check to use internal address pool configuration to obtain an IP address for the client. - General - Client Update -Load Balancing Cancel Apply Policy Management ⊕Administration Monitoring

Configurer une proposition IKE

Complétez ces étapes afin de configurer une proposition IKE :

 Sélectionnez Configuration > System > Tunneling Protocols > IPSec > IKE Proposal, cliquez sur Add et sélectionnez les paramètres, comme indiqué dans cette image.

m General 1	Configuration Sustain 7	montion Declarate 108ac 16	E Departure	ala 1 Add
	Comiguration System 1	unneing moucois [Insec] in	c rropo:	ias Luon
	Configure and add a new IV	E Despecial		
Load Balancing	Conligure and add a new ik	E Proposal		
- Ouser Management				
Base Group	Descourd House	THE for minal		Specify the same of this IVE Despected
Groups	rtoposai name	IKE-TOT-WINZM		opecity the name of this INE Proposal.
Users				
- Policy Management	Authentication Mode	RSA Digital Certificate	11	Select the authentication mode to use
Access Hours	Faranettacauon mone	Hori bighar certificate		select the authentication mode to use.
ETraffic Management				
Natwork Lists	Authentication Algorithm	MD54444C-128 m		Salast the nackat authentication algorithm to use
Redes	Autoentication Augoritani	MD0/HMMC=120 CJ		Select the packet authentication algorithm to use.
<u>Enviros</u>				
<u>- 545</u>	From the Almost the	0.55 54		Colored the successful alreading to use
Filters	Encryption Augorithm	DE3-36 L		Select the encryption algorithm to use.
UAL				
Administration	and the second se	Contract of the state of the state		many states and a second second second second
Administer Sessions	Diffie-Hellman Group	Group 1 (768-bits)		Select the Diffie Heliman Group to use.
- CO-Software Update				
-System Reboot				
-Ping	Lifetime Measurement	Time 🗆		Select the lifetime measurement of the IKE keys.
-Monitoring Refresh				
- Access Rights		Transa.		A CONTRACTOR AND A CONTRACTOR
BEIg Management	Data Lifetime	10000		Specify the data lifetime in kilobytes (KB).
Certificate				
• Management	Time Lifetime	105400		Concilly the time lifetime in seconds
Enrolment	Tane Lifetine	196400		specify the time metime in seconds.
Installation				
Monitoring		1		
Dauding Tabla	Add Cancel			
rating late				
-C-Filterable Event Lod				

2. Cliquez sur **Add**, mettez en surbrillance la nouvelle proposition dans la colonne de droite, puis cliquez sur **Activate**.

Configuration de la SA

Complétez cette procédure afin de configurer l'association de sécurité (SA) :

- Sélectionnez Configuration > Policy Management > Traffic Management > SA et cliquez sur ESP-L2TP-TRANSPORT.Si cette association de sécurité n'est pas disponible ou si vous l'utilisez à d'autres fins, créez une nouvelle association de sécurité similaire à celle-ci. Différents paramètres sont acceptables pour la SA. Modifiez ce paramètre en fonction de votre stratégie de sécurité.
- 2. Sélectionnez le certificat numérique que vous avez configuré précédemment dans le menu déroulant Certificat numérique. Sélectionnez la proposition IKE-for-win2k Internet Key Exchange (IKE).Remarque : ceci n'est pas obligatoire. Lorsque le client L2TP/IPSec se connecte au concentrateur VPN, toutes les propositions IKE configurées dans la colonne active de la page Configuration > System > Tunneling Protocols > IPSec > IKE Proposal sont essayées dans l'ordre.Cette image montre la configuration requise pour l'association de sécurité

3 Configuration				
-mSystem	IPSec Parameters			
CPolicy Management	Authentication Algorithm	ESP/MD5/HMAC-128 🗆		Select the packet authentication algorithm to use.
Access Hours				
Traffic Management	Encryption Algorithm	DES-SA CT		Select the ESP encruption algorithm to use
Rules	cherypoon regorium	00000		ounce the con energy on against to une.
-SA1		land the second s		
-Eitters	Encapsulation Mode	Transport 🗆		Select the Encapsulation Mode for this SA.
- ID-NAT				
Administration	Perfect Ferward Secrecy	Disabled 🗆		Select the use of Perfect Forward Secrecy.
-m-Software Lindate				
-System Reboot	Lifetime Measurement	Time		Select the lifetime measurement of the IPSec keys
-Ping	Lifetime medsurement	Time C1		Select the methic measurement of the in Sec keys.
Monitoring Refresh		2		without the standard standard in the standard standard standard standard standard standard standard standard st
DEile Management	Data Lifetime	10000		Specify the data lifetime in kilobytes (KB).
- Certificate Management				
Monitoring	Time Lifetime	3900		Specify the time lifetime in seconds.
	IKE Parameters			
	INC Dear	2.0.0.0		Constanting The Second State and the Second State
	IKE Peer	0.0.0.0		specify the IRE Peer for a LAN-10-LAN IPSec connection.
		1		
	Negotiation Mode	Main 🖵		Select the IKE Negotiation mode to use.
	Digital Certificate	vpn3000-name	1	Select the Digital Certificate to use.
	Conditionales Temporales Inc.	Entire certificate chain		Channel have be used the district contribute to the WF ways
	Certificate Transmission	Identity certificate only		Choose now to send the digital certificate to the IKE peer.
Cisco Systems	IKE Proposal	IKE-for-win2k	-	Select the IKE Proposal to use as IKE initiator.
	2			

Configurer le groupe et l'utilisateur

Effectuez cette procédure afin de configurer le groupe et l'utilisateur :

- 1. Sélectionnez Configuration > User Management > Base Group.
- 2. Sous l'onglet Général, assurez-vous que L2TP sur IPSec est coché.
- 3. Sous l'onglet IPSec, sélectionnez la SA ESP-L2TP-TRANSPORT.
- 4. Sous l'onglet PPTP/L2TP, décochez toutes les options L2TP Encryption.
- 5. Sélectionnez Configuration > User Management > Users et cliquez sur Add.
- 6. Entrez le nom et le mot de passe que vous utilisez pour vous connecter à partir de votre client Windows 2000. Veillez à sélectionner **Groupe de base** sous Sélection de groupe.
- 7. Sous l'onglet Général, vérifiez le protocole de tunnellisation L2TP sur IPSec.
- 8. Sous l'onglet IPSec, sélectionnez la SA ESP-L2TP-TRANSPORT.
- 9. Sous l'onglet PPTP/L2TP, décochez toutes les options L2TP Encryption, puis cliquez sur Add.Vous pouvez maintenant vous connecter à l'aide du client L2TP/IPSec Windows 2000.Remarque : vous avez choisi de configurer le groupe de base pour accepter la connexion L2TP/IPSec distante. Il est également possible de configurer un groupe qui correspond au champ Unité d'organisation (OU) de l'association de sécurité pour accepter la connexion entrante. La configuration est identique.

Informations de débogage

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7
```

271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76 Phase 1 failure against global IKE proposal # 16: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76 Proposal # 1, Transform # 2, Type ISAKMP, Id IKE Parsing received transform: Phase 1 failure against global IKE proposal # 1: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76 Phase 1 failure against global IKE proposal # 2: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76 Phase 1 failure against global IKE proposal # 3: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76 Phase 1 failure against global IKE proposal # 4: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76 Phase 1 failure against global IKE proposal # 5: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 2 Cfg'd: Oakley Group 1 291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76 Phase 1 failure against global IKE proposal # 6: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76 Phase 1 failure against global IKE proposal # 7: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76

```
Phase 1 failure against global IKE proposal # 10:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 2
   Cfg'd: Oakley Group 1
306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
 Phase 1 failure against global IKE proposal # 11:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 2
   Cfg'd: Oakley Group 1
309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
 Phase 1 failure against global IKE proposal # 12:
 Mismatched attr types for class Encryption Alg:
   Rcv'd: DES-CBC
   Cfg'd: Triple-DES
312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
 Phase 1 failure against global IKE proposal # 13:
 Mismatched attr types for class Encryption Alg:
   Rcv'd: DES-CBC
   Cfg'd: Triple-DES
315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
 Phase 1 failure against global IKE proposal # 14:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1
318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
 Phase 1 failure against global IKE proposal # 15:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 2
   Cfg'd: Oakley Group 7
321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
 Phase 1 failure against global IKE proposal # 16:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1
324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
 Phase 1 failure against global IKE proposal # 1:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 2
329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
 Phase 1 failure against global IKE proposal # 2:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
 Phase 1 failure against global IKE proposal # 3:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
 Phase 1 failure against global IKE proposal # 4:
 Mismatched attr types for class Encryption Alg:
```

Rcv'd: DES-CBC Cfg'd: Triple-DES 338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76 Phase 1 failure against global IKE proposal # 5: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76 Phase 1 failure against global IKE proposal # 6: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76 Phase 1 failure against global IKE proposal # 7: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76 Phase 1 failure against global IKE proposal # 8: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76 Phase 1 failure against global IKE proposal # 9: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76 Phase 1 failure against global IKE proposal # 10: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76 Phase 1 failure against global IKE proposal # 11: Mismatched attr types for class Hash Alg: Rcv'd: SHA Cfg'd: MD5 358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76 Phase 1 failure against global IKE proposal # 12: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76 Phase 1 failure against global IKE proposal # 13: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76 Phase 1 failure against global IKE proposal # 14: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76

```
Phase 1 failure against global IKE proposal # 15:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 7
370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
 Phase 1 failure against global IKE proposal # 16:
 Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
   Cfg'd: MD5
372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
 Phase 1 failure against global IKE proposal # 1:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 2
377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
 Phase 1 failure against global IKE proposal # 2:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 2
380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
 Phase 1 failure against global IKE proposal # 3:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 2
383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
 Phase 1 failure against global IKE proposal # 4:
 Mismatched attr types for class Encryption Alg:
   Rcv'd: DES-CBC
   Cfg'd: Triple-DES
386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
 Phase 1 failure against global IKE proposal # 5:
 Mismatched attr types for class Encryption Alg:
   Rcv'd: DES-CBC
    Cfg'd: Triple-DES
389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
 Phase 1 failure against global IKE proposal # 6:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 2
392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
 Phase 1 failure against global IKE proposal # 7:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
 Phase 1 failure against global IKE proposal # 8:
 Mismatched attr types for class DH Group:
   Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2
398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
 Phase 1 failure against global IKE proposal # 9:
 Mismatched attr types for class DH Group:
```

Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76 Phase 1 failure against global IKE proposal # 10: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76 Phase 1 failure against global IKE proposal # 11: Mismatched attr types for class Auth Method: Rcv'd: RSA signature with Certificates Cfg'd: Preshared Key 407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76 Phase 1 failure against global IKE proposal # 12: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76 Phase 1 failure against global IKE proposal # 13: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 2 413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76 Phase 1 failure against global IKE proposal # 14: Mismatched attr types for class Encryption Alg: Rcv'd: DES-CBC Cfg'd: Triple-DES 416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76 Phase 1 failure against global IKE proposal # 15: Mismatched attr types for class DH Group: Rcv'd: Oakley Group 1 Cfg'd: Oakley Group 7 419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76 IKE SA Proposal # 1, Transform # 4 acceptable Matches global IKE entry # 16 420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76 constructing ISA_SA for isakmp 421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76 SENDING Message (msgid=0) with payloads : HDR + SA (1) + NONE (0) ... total length : 80 423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76 RECEIVED Message (msgid=0) with payloads : $HDR + KE (4) + NONCE (10) + NONE (0) \dots total length : 152$ 425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76 RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152 427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76 processing ke payload 428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76 processing ISA_KE

429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76 processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76 constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDEG/1 RPT=105 10.48.66.76 constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76 constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76 Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76 constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76 constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76 Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76 Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76 constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76 Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76 Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76 SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76 RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0) ... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76 Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76 processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76 processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76 computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76 processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76 Storing cert request payload for use in MM msg 4

454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76 Starting group lookup for peer 10.48.66.76 455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76 No Group found by matching IP Address of Cert peer 10.48.66.76 456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76 No Group found by matching OU(s) from ID payload: ou=sns, 457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76 Group [VPNC_Base_Group] No Group name for IKE Cert session, defaulting to BASE GROUP 459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76 Group [VPNC_Base_Group] Found Phase 1 Group (VPNC_Base_Group) 460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76 Group [VPNC_Base_Group] Authentication configured for Internal 461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76 Group [VPNC_Base_Group] IKEGetUserAttributes: default domain = fenetwork.com 462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76 Group [VPNC_Base_Group] Validation of certificate successful (CN=my_name, SN=6102861F0000000000) 464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76 Group [VPNC_Base_Group] peer ID type 9 received (DER_ASN1_DN) 465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76 Group [VPNC_Base_Group] constructing ID 466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76 Group [VPNC_Base_Group] constructing cert payload 467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76 Group [VPNC_Base_Group] constructing RSA signature 468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76 Group [VPNC_Base_Group] computing hash 469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76 Group [VPNC_Base_Group] constructing dpd vid payload 470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76 SENDING Message (msgid=0) with payloads : HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0) ... total length : 1112 473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76 Group [VPNC Base Group] PHASE 1 COMPLETED

474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76 Keep-alive type for this connection: None 475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76 Keep-alives configured on but peer does not support keep-alives (type = None) 476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76 Group [VPNC_Base_Group] Starting phase 1 rekey timer: 21600000 (ms) 477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76 RECEIVED Message (msgid=781ceadc) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) ... total length : 1108 480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76 Group [VPNC_Base_Group] processing hash 481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76 Group [VPNC_Base_Group] processing SA payload 482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76 Group [VPNC_Base_Group] processing nonce payload 483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76 Group [VPNC_Base_Group] Processing ID 484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76 Group [VPNC_Base_Group] Received remote Proxy Host data in ID Payload: Address 10.48.66.76, Protocol 17, Port 1701 487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76 Group [VPNC_Base_Group] Processing ID 488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76 Group [VPNC_Base_Group] Received local Proxy Host data in ID Payload: Address 10.48.66.109, Protocol 17, Port 0 491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942 QM IsRekeyed old sa not found by addr 492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76 Group [VPNC_Base_Group] IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT 493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76 Group [VPNC_Base_Group] processing IPSEC SA 494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76 Group [VPNC Base Group] IPSec SA Proposal # 1, Transform # 1 acceptable 495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76 Group [VPNC_Base_Group] IKE: requesting SPI!

496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4 IKE got SPI from key engine: SPI = 0x10d19e33 497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76 Group [VPNC_Base_Group] oakley constucting quick mode 498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76 Group [VPNC_Base_Group] constructing blank hash 499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76 Group [VPNC_Base_Group] constructing ISA_SA for ipsec 500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76 Group [VPNC_Base_Group] constructing ipsec nonce payload 501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76 Group [VPNC_Base_Group] constructing proxy ID 502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76 Group [VPNC_Base_Group] Transmitting Proxy Id: Remote host: 10.48.66.76 Protocol 17 Port 1701 Local host: 10.48.66.109 Protocol 17 Port 0 506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76 Group [VPNC_Base_Group] constructing qm hash 507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76 SENDING Message (msgid=781ceadc) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)... total length : 156 510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76 RECEIVED Message (msgid=781ceadc) with payloads : HDR + HASH (8) + NONE (0) ... total length : 48 512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76 Group [VPNC_Base_Group] processing hash 513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76 Group [VPNC_Base_Group] loading all IPSEC SAs 514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76 Group [VPNC_Base_Group] Generating Quick Mode Key! 515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76 Group [VPNC_Base_Group] Generating Quick Mode Key! 516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76 Group [VPNC_Base_Group] Loading host: Dst: 10.48.66.109 Src: 10.48.66.76

517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76 Group [VPNC_Base_Group] Security negotiation complete for User () Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4 IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955 pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76 Group [VPNC_Base_Group] PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956 pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957 KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0

Informations de dépannage

Cette section présente certains problèmes courants et les méthodes de dépannage de chacun d'eux.

Impossible de démarrer le



Il est très probable que le service IPSec ne soit pas démarré. Sélectionnez **Démarrer > Programmes > Outils d'administration > Service** et vérifiez que le **service IPSec** est activé.

Erreur 786 : Aucun certificat d'ordinateur

Error Cor	nnecting to l2tp over ip	sec to vpn3k		? ×
A	Connecting to 10.48.66.1	109		
<u>.</u>	Error 786: The L2TP con valid machine certificate authentication.	nection attempt faile on your computer for	d because there security	is no
	Redial = 45	Cancel	More Info	1
				Cette erreur

valide.

indique un problème avec le certificat sur l'ordinateur local. Afin de consulter facilement votre certificat, sélectionnez **Démarrer > Exécuter**, et exécutez MMC. Cliquez sur **Console** et choisissez **Add/Remove Snap-in**. Cliquez sur **Add** et choisissez **Certificate** dans la liste. Lorsqu'une fenêtre apparaît et vous demande l'étendue du certificat, sélectionnez **Computer Account**.Vous pouvez maintenant vérifier que le certificat du serveur AC est situé sous les **Autorités de certification racines de confiance**. Vous pouvez également vérifier que vous avez

un certificat en sélectionnant **Racine de la console > Certificat (Ordinateur local) > Personnel > Certificats**, comme illustré dans cette

image.

🚡 Console1								
Console Window Help □ 🛱 🖬 💷								
🚡 Console Root\Certificates (Loca	l Computer)\Personal\Ce	ertificates	1					
Action View Eavorites 🛛 🗢 🔿 💽 💽 💼 😰 🚱								
Tree Favorites	Issued To 🔥	Issued By						
Console Root Certificates (Local Computer) Certificates Certificates Certificates Certificates Certificates Certificates	my_name	snsvpc7-ca	1					
Personal store contains 2 certificates.			2					

Cliquez sur le **certificat**. Vérifiez que tout est correct. Dans cet exemple, une clé privée est associée au certificat. Cependant, ce certificat a expiré. C'est la cause du

Certificate	
General Details Certification Pa	ath
Certificate Informa	ation
This certificate has expire	ed or is not yet valid.
Issued to: my_name	
Issued by: snsvpc7-ca	3
Valid from 2/14/2002	to 2/14/2003
¶ [∞] You have a private key t	hat corresponds to this certificate.
	Issuer Stateme
	Issuer Stateme

• Erreur 792 : Temporisation de négociation de sécurité.Ce message apparaît après une longue



débogages appropriés comme expliqué dans la FAQ sur le <u>concentrateur Cisco VPN 3000</u>.

```
Lisez-les. Vous devez voir quelque chose de similaire à cette sortie :
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
Phase 1 failure against global IKE proposal # 6:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 1
Cfg'd: Oakley Group 2
9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
```

```
Phase 1 failure against global IKE proposal # 7:
```

```
Mismatched attr types for class Auth Method:
   Rcv'd: RSA signature with Certificates
   Cfg'd: Preshared Key
9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
 Phase 1 failure against global IKE proposal # 8:
 Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
   Cfg'd: Oakley Group 7
9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable
9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1
9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0
9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```

Cela indique que la proposition IKE n'a pas été configurée correctement. Vérifiez les informations de la section <u>Configuration d'une proposition IKE</u> de ce document.

• Erreur 789 : La couche de sécurité rencontre une erreur de

rror Co	nnecting to l2tp over ip	sec to vpn3k		? ×
	Connecting to 10.48.66.	109		
ف	Error 789: The L2TP con layer encountered a proc the remote computer.	nection attempt faile essing error during in	d because the secu nitial negotiations wit	irity h
	Redial = 37	Cancel	More Info	

traitement.L

les débogages appropriés comme expliqué dans la FAQ sur le <u>concentrateur Cisco VPN</u> <u>3000</u>. Lisez-les. Vous devez voir quelque chose de similaire à cette sortie :

```
11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686
 Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
 Parsing received transform:
   Phase 2 failure:
   Mismatched attr types for class Encapsulation:
     Rcv'd: Transport
     Cfg'd: Tunnel
 11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
 AH proposal not supported
 11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
 Group [VPNC_Base_Group]
 All IPSec SA proposals found unacceptable!

    Version utiliséeSélectionnez Monitoring > System Status pour afficher cette sortie :

 VPN Concentrator Type: 3005
 Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
 Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
 Up For: 44:39:48
 Up Since: 02/13/2002 15:49:59
 RAM Size: 32 MB
```

Informations connexes

- <u>Assistance produit Négociation IPSec/Protocoles IKE</u>
- <u>Support technique Cisco Systems</u>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.