Ejemplo de Configuración de L2TP sobre IPsec entre Windows 2000 y el Concentrador VPN 3000 Usando Certificados Digitales

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Objetivos Convenciones** Obtener un certificado raíz Obtener un certificado de identidad para el cliente Creación de una conexión a VPN 3000 mediante el Asistente de conexión de red Configurar el concentrador VPN 3000 Obtener un certificado raíz Obtenga un certificado de identidad para el concentrador VPN 3000 Configurar un grupo para los clientes Configurar una propuesta IKE Configuración de SA Configuración del grupo y el usuario Información acerca de la depuración Información de Troubleshooting Información Relacionada

Introducción

Este documento muestra el procedimiento paso a paso utilizado para conectarse a un Concentrador VPN 3000 desde un cliente Windows 2000 mediante el cliente integrado L2TP/IPSec. Se supone que utiliza certificados digitales (entidad emisora de certificados raíz (CA) independiente sin protocolo de inscripción de certificados (CEP)) para autenticar la conexión con el concentrador VPN. Este documento utiliza el Servicio de certificados de Microsoft como ejemplo. Consulte el sitio web de <u>Microsoft</u> para obtener documentación sobre cómo configurarlo.

Nota: Este es un ejemplo sólo porque la apariencia de las pantallas de Windows 2000 puede cambiar.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento es para el Cisco VPN 3000 Concentrator series.

Objetivos

En este procedimiento, debe completar estos pasos:

- 1. Obtenga un certificado raíz.
- 2. Obtenga un certificado de identidad para el cliente.
- 3. Cree una conexión a VPN 3000 con la ayuda del Asistente de conexión de red.
- 4. Configurar el concentrador VPN 3000.

Convenciones

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

Obtener un certificado raíz

Complete estas instrucciones para obtener un certificado raíz:

- Abra una ventana del explorador y escriba la dirección URL de Microsoft Certificate Authority (normalmente http://servername o la dirección IP de CA/certsrv).Se muestra la ventana Bienvenido para las solicitudes y recuperaciones de certificados.
- En la ventana Bienvenido, en Seleccionar una tarea, elija Recuperar el certificado de CA o la lista de revocación de certificados y haga clic en Siguiente.

Microsoft Certificate Services - Microsoft Internet Explorer	
<u>Elle E</u> dit ⊻iew Fgvorites Iools <u>H</u> elp	
(→ . ↔ . ⊗	
Address http://10.10.102.42/certsrv/	j∂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 secure program. Once you acquire a certificate, you will be able to securely identify yourself to other p the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upo of certificate you request. Select a task: © Retrieve the CA certificate or certificate revocation list © Request a certificate © Check on a pending certificate	re eople over on the type
	Next>
E Done	(<u> </u>

3. En la ventana Recuperar el certificado de CA o la lista de revocaciones de certificados, haga clic en **Instalar esta ruta de certificación de CA** en la esquina izquierda.Esto agrega el certificado de CA al almacén de autoridades de certificados raíz de confianza. Esto significa que todos los certificados que esta CA emite a este cliente son de confianza.

Fe Ed Yes Fanker Jok Heb For Star Star Star Star Star Star Star Sta	Revocation List	es issued from this certific	E 260 Links tissues ication authority
Agine Contricute Services - win2knewe Adicrosoft Contricute Services - win2knewe Adicrosoft Contricute Services - win2knewe Retrieve The CA Certificate Or Certificate Install this CA certification path to allow your It is not necessary to manually install the CA CA certification path will be installed for you Choose file to download:	Revocation List computer to trust certificate certification path if you requ	es issued from this certific	ی ک∂ی العقد tiame ication authority
Against Contribute Services - win2leastner Retrieve The CA Certificate Or Certificate Install this CA certification path to allow your t is not necessary to manually install the CA CA certification path will be installed for you Choose file to download:	Revocation List computer to trust certificate certification path if you requ automatically.	es issued from this certifi uest and install a certifica	ड ्रिका । Crea Hame ication authority
Microsoft Certificate Services - win2knamer Retrieve The CA Certificate Or Certificate Install this CA certification path to allow your It is not necessary to manually install the CA CA certification path will be installed for you Choose file to download:	Revocation List computer to trust certificate certification path if you requ automatically.	es issued from this certifice	Earne Contraction authority
Retrieve The CA Certificate Or Certificate Install this CA certification path to allow your It is not necessary to manually install the CA CA certification path will be installed for you Choose file to download:	Revocation List computer to trust certificate certification path if you requ automatically.	es issued from this certifice	ication authority
Install this CA certification path to allow your It is not necessary to manually install the CA CA certification path will be installed for you Choose file to download:	computer to trust certificate certification path if you requ automatically.	es issued from this certifi uest and install a certifica	ication authority
t is not necessary to manually install the CA CA certification path will be installed for you Choose file to download:	certification path if you requ automatically.	uest and install a certifica	and the second
Choose file to download:			are from this centrication authority, because the
CA Certificate: Cusent[ein2kserver]			
@ DER encoded or . C Bas	a 64 encoded		
Download CA certificate	0.01000000		
Download CA certification p	th		
Download latest certificate ry	vocation list		

Obtener un certificado de identidad para el cliente

Complete estos pasos para obtener un certificado de identidad para el cliente:

- 1. Abra una ventana del explorador e introduzca la URL de Microsoft Certificate Authority (normalmente http://servername o la dirección IP de CA/certsrv).Se muestra la ventana Bienvenido para las solicitudes y recuperaciones de certificados.
- 2. En la ventana Bienvenido, en Seleccionar una tarea, elija **Solicitar un certificado** y haga clic en

Siguiente.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Favorites Icols Help	80) 810
Image: Constraint of the second se	
Address @ http://10.10.102.42/certsrv/	
Microsoft Certificate Services win2kserver	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other se program. Once you acquire a certificate, you will be able to securely identify yourself to othe the web, sign your e-mail messages, encrypt your e-mail messages, and more depending of certificate you request. Select a task:	ecure er people over upon the type
	Next>
🛃 Done	ternet

3. En la ventana Elegir tipo de solicitud, seleccione Solicitud avanzada y haga clic en

De Sit See Facetes Lock Heb Back Sop Refrect Harry Stack Sop Refrect Harry Agtest Imp.//10.10.102.42/centur/centup.a.ap Attorney Imp.//10.102.102.102.102.102.102.102.102.102.1
Back Sono Refresh Harres Search Parceles Harres
Back Private Step Reference Human Search Parceles Human Hall Private Priv
Attoreed Contracts Benaces - Anchore Even
Microsoft Cost Sciences Microsoft Microsoft Microsoft Choose Request Type Please select the type of request you would like to make: C User certificate request: E-Mel Protection Certificate
Choose Request Type Please select the type of request you would like to make: C User certificate request E-Mel Protector Certificate
Please select the type of request you would like to make: C User certificate request E-Mel Protection Certificate
User certificate request: E-Mel Protection Certificate
E-Mail Protection Centricate
A holomore and an exception
M Advanced request
Piezd >
el Done el transmit

4. En la ventana Advanced Certificate Requests, seleccione Submit a certificate request to this CA using a



 Rellene los campos como en este ejemplo.El valor de Department (unidad organizativa) debe coincidir con el grupo configurado en el concentrador VPN. No especifique un tamaño de clave superior a 1024. Asegúrese de seleccionar la casilla de verificación Use local machine store. Cuando haya finalizado, haga clic en Next (Siguiente)

Advanced Certif	z ficale Request	-
Identifying Inform	ation	
Name	win2kclientid	
E-Mail:		1
Company	eliga	
Department	support	
City	i franklin	1
State	ma	
CountryRegion	US	1
Intended Purpose	ĸ	
	Client Authentication Certificate	
Key Options:		
CSP	Microsoft Base Cryptographic Pravider v1.0	
Key Usage:	C Exchange @ Signature C Both	2
Key Bize:	512 Max 1924 Max 19214 Wermen Key stress (20. 2024 2018) 1028 2018, 10285 3	
	@ Create new key set	
	E Set the container name	
	C Use existing key set	
	Enable strong private key protection	144
	T Mark keys as expotable	1.5
	E Use local machine store You rout be an administrator to generate a key in the local machine alore.	-

n función de la configuración del servidor de la CA, a veces aparece esta ventana. Si es así, póngase en contacto con el administrador de la

Your certificate re	quest has been received. However, you must wait for an administrator to issue the certificate you requested.
Please return to t	his web site in a day or two to retrieve your certificate.
Note: You must retu	m with this web browser within 10 days to retrieve your certificate

6. Haga clic en **Home** para volver a la pantalla principal, seleccione **Check on pending certificate** y haga clic en

Please select the certification	request you want to check:		
Quer Aufreickenen Ger	iicew (62/18/200009-50.59)		
			Next

7. En la ventana Certificado emitido, haga clic en Instalar este

Alicro	and Certificate Services — with server
Certif	loate issued
The co	ettificate you requested was issued to you.
	Eroud
	test at this certificate
).[

- 8. Para ver su certificado de cliente, seleccione **Start > Run**, y realice Microsoft Management Console (MMC).
- 9. Haga clic en Console y elija Add/Remove Snap-in.
- 10. Haga clic en Agregar y elija Certificado en la lista.
- 11. Cuando aparezca una ventana que le pregunte el alcance del certificado, elija **Cuenta de** equipo.
- 12. Compruebe que el certificado del servidor de la CA se encuentra en Entidades de certificación raíz de confianza. También verifique que tiene un certificado seleccionando Console Root > Certificate (Local Computer) > Personal > Certificates, como se muestra en esta

٠						
I	m	а	a	е	n.	
•		-		-	• • •	

Console1				_0 ×
<u>⊆</u> onsole <u>W</u> indow <u>H</u> elp	0 📽 🖬 🔟 🗌			
Console Root Certificat	es (Local Computer)\Perso	nal\Certificates		
Action yew Eavorites	+ + 1 1 1	🖸 🖳 😭	10	
Tree Favorites	Essued To /	Issued By	Expiration	
Console Root Certificates (Local Com Certificates (Local Com Certificates Certific	Wein2ficlientid	whäserver	3(1/2001	

Creación de una conexión a VPN 3000 mediante el Asistente de conexión de red

Complete este procedimiento para crear una conexión a VPN 3000 con la ayuda del asistente de conexión de red:

- 1. Haga clic con el botón derecho en **Mis sitios de red**, elija **Propiedades** y haga clic en **Realizar nueva conexión**.
- En la ventana Network Connection Type (Tipo de conexión de red), seleccione Connect to a private network through the Internet (Conectarse a una red privada a través de Internet) y, a continuación, haga clic en Next.

You can choose t your network con	ne type of network connec guration and your network	tion you want to ing needs.	create, based on	8
C Dial-up to g	rivate network			
Connect using	my phone line (modem or	ISDN).		
C Dial-up to t	e Internet			
Connect to th	Internet using my phone	line (modem or IS	DN).	
• Connect to	a private network thro	ugh the Intern	et	
Create a Virtu	I Private Network (VPN) c	connection or 'tun	nel' through the Intern	net.
C Accent inc	ming connections			
Let other corr	outers connect to mine by	phone line, the Ir	ternet, or direct cable	
C Connect di	ectly to another comm	uter		
Connect usin	my serial, parallel, or infra	red port.		

 Introduzca el nombre de host o la dirección IP de la interfaz pública del concentrador VPN y haga clic en Next.

Destination Address What is the name or address	s of the destination?	۵Ż
Type the host name or IP add connecting.	ldress of the computer or network to which you are	
Host name or IP address (suc	ch as microsoft.com or 123.45.6.78):	
64.67.72.180		
3		
	Carl Newty Car	

4. En la ventana Disponibilidad de la conexión, seleccione **Solo para mí** y haga clic en **Siguiente**.

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. En la ventana Red pública, seleccione si desea marcar la conexión inicial (la cuenta ISP) automáticamente.

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

 En la pantalla Destination Address (Dirección de destino), introduzca el nombre de host o la dirección IP del concentrador VPN 3000 y haga clic en Next (Siguiente).

twork Cor	nection Wizard				
Destinat Wha	ion Address is the name or ac	ldress of the des	ination?		S
Type conn	the host name or ecting.	IP address of the	computer or netwo	ork to which you ar	e
<u>H</u> ost	name or IP addres	ss (such as micro	soft.com or 123.45.	6.78):	
64.6	7.72.180				
-					
			and a second	Í North	
			< Back	Nevts I	Cancel

7. En la ventana Asistente para conexión de red, escriba un nombre para la conexión y haga clic en **Finalizar**.En este ejemplo, la conexión se denomina "Cisco corporate VPN".



8. En la ventana Conexión privada virtual, haga clic en



Propiedades.

- 9. En la ventana Propiedades, seleccione la ficha Redes.
- 10. En Type of VPN server I am calling, elija L2TP en el menú desplegable, resalte Internet Protocol TCP/IP y haga clic en

Cisco corporate VPN		? ×
General Options Sec	urity Networking	,
Type of VPN server La	ım calling:	
Layer-2 Tunneling Pro	itocol (L2TP)	
		Settings
Components checked	are used by this conne	ection:
 ✓ Internet Protoc ✓ ₽ ₽ File and Printe ✓ ₽ ₽ Client for Micro 	ol (TCP/IP) Sharing for Microsoft soft Networks	Networks
Install	Uninstall	Properties
Description Transmission Contro wide area network p across diverse inter	I Protocol/Internet Pro protocol that provides o connected networks.	tocol. The default communication
		DK Cancel

Properties.

- 11. Seleccione Advanced > Options > Properties.
- 12. En la ventana IP Security, elija Use this IP security



- 13. Elija la política **Client (Respond Only)** del menú desplegable y haga clic en **OK** varias veces hasta que regrese a la pantalla Connect.
- 14. Para iniciar una conexión, ingrese su nombre de usuario y contraseña, y haga clic en **Connect**.

Configurar el concentrador VPN 3000

Obtener un certificado raíz

Complete estos pasos para obtener un certificado raíz para el Concentrador VPN 3000:

- Señale en el explorador su CA (normalmente algo como http://ip_add_of_ca/certsrv/), Recupere el certificado de CA o la lista de revocación de certificados y haga clic en Siguiente.
- 2. Haga clic en Descargar certificado de CA y guarde el archivo en algún lugar del disco local.
- 3. En el Concentrador VPN 3000, seleccione Administration > Certificate Management, y haga clic en Click here to install a certificate e Install CA Certificate.
- 4. Haga clic en Cargar archivo desde estación de trabajo.
- 5. Haga clic en Browse y seleccione el archivo de certificado de CA que acaba de descargar.
- 6. Resalte el nombre de archivo y haga clic en **Install**.

Configuration	Administration Certificate	e Management			Tuesday, 12 February
Administration Administer Sessions					
	This section lets you view a	and manage certificates on the \	/PN 3000 Concentrato	r.	
Ping 	 Click here to enroll v Click here to install 	with a Certificate Authority a certificate			
- GRACCESS Rights - GREile Management	Certificate Authorities	(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	[Vev Configure Delete]
- Monitoring	Identity Certificates (cu	urrent: 0, maximum: 2)			
mEilerable Event Los	Subject	Issuer	Exp	iration	Actions
System Status	No Identity Certificates				
Sessions	0.01 0 110 110				

Obtenga un certificado de identidad para el concentrador VPN 3000

Complete estos pasos para obtener un certificado de identidad para el Concentrador VPN 3000:

 Seleccione ConfAdministration > Certificate Management > Enroll > Identity Certificate, luego haga clic en Enroll via PKCS10 Request (Manual). Rellene el formulario como se muestra aquí y haga clic en lucentition

INSCRIDIT.			
Configuration	Administration Certificate Management	it Enroll Identity Certificate PKCS1	0
>Administration			
Administer Sessions	Enter the information to be included in th	e certificate request. The CA's certificate i	must be installed as a Certificate Authority before installing the
-B-Software Update	certificate you requested. Please wait for	the operation to finish.	
Ding			
Atopitoring Befresh	Common Name (CN)	ma 2000 and	Enter the common name for the VPN 3000 Concentrator
-Báccess Biobts	contraint (crt)	Altragon transf	to be used in this PKI.
-BFile Management			7
-G-Certificate Management	Organizational Unit (OU)	ana	Enter the department.
-Enrollment			
Installation	Organization (O)	ciacá	Enter the Organization or company
© Monitoring			
		L	The second se
	Locality (L)	pull	Enter the city or town.
	State/Province (SP)	1	Enter the State or Province.
			4 (
	Country (C)	57	Enter the two-letter country abbreviation (e.g. United
	country (c)	D.d.	States = US).
		- 10-0.0	Enter the Fully Qualified Domain Name for the VEN 3000
	Subject AlternativeName (FQDN)	vpn3000-name.cisco.com	Concentrator to be used in this PKI.
	Subject AlternativeName (E-Mail	1	Enter the E-Mail Address for the VPN 3000
	Address)		Concentrator to be used in this PKL
		and all and and a second	
	Key Size	RSA 512 bits 🗆	Select the key size for the generated RSA/DSA key pair.
	Enroll Cancel		
	F		

Aparece una ventana del navegador con la solicitud de certificado. Necesita contener texto similar a este resultado:

-----BEGIN NEW CERTIFICATE REQUEST-----MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu czEOMAwGA1UEChMFY21zY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW11LmNpc2NvLmNvbTAN BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak= -----END NEW CERTIFICATE REQUEST-----

- 2. Señale el explorador al servidor de la CA, marque **Solicitar un certificado** y haga clic en **Siguiente**.
- 3. Marque Advanced Request, haga clic en Next y seleccione Submit a certificate request using a base64 encoded PKCS #10 file or a renew request using a base64 encoded PKCS #7 file.
- 4. Haga clic en Next (Siguiente). Corte y pegue el texto de la solicitud de certificado que se

muestra anteriormente en el área de texto. Haga clic en Submit (Enviar).

- Según la configuración del servidor de la CA, puede hacer clic en Descargar certificado de la CA. O bien, cuando la CA haya emitido el certificado, vuelva al servidor de la CA y active Comprobar un certificado pendiente.
- 6. Haga clic en Next, seleccione su solicitud y haga clic en Next nuevamente.
- 7. Haga clic en **Descargar certificado de CA** y guarde el archivo en el disco local.
- 8. En el Concentrador VPN 3000, seleccione Administration > Certificate Management > Install y haga clic en Install certificate received via enrollment. A continuación, verá la solicitud pendiente con el estado "En curso", como en esta

imagen.

VPN	3000							Main Help Support	Legeu
Conc	entrator Series Mana	iger						Logged	in: admi
							Configu	ation Administration M	onitorin
HITP/HITPS —IETP —Teinet —SNMP SNMP	Select a enrolment request to Enrollment Status	install.	Install certifica	ale obta	ned via enr	sliment			
Communities	Subject	Issuer	Date	Use	Reason	Method	Status	Actions	
SSH SSH	vpn3000-name at cisco	NóR	02/13/2002	ID	Initial	Manual	In Progress	[Mew.] Install Delete]	
-BEvents	<< Go back and choose a diffe	rent type of c	ertificate						

- 9. Haga clic en Install, seguido de Upload File from Workstation.
- 10. Haga clic en Examinar y seleccione el archivo que contiene el certificado emitido por la CA.
- 11. Resalte el nombre de archivo y haga clic en Install.
- 12. Seleccione Administration > Certificate Management. Aparece una pantalla similar a esta imagen.

inagen.						Co	nfigura			
Configuration	Administration Ce	ertificate Ma	anagement				Wednes			
Administration Administer Sessions 	This section lets you view and manage certificates on the VPN 3000 Concentrator.									
Certificate Management	t Subject Issuer Expirat		Expiration	SCEP Issuer						
Enrollment	snsvpc7-ca at cisco snsvpc7-ca at cisco 02/14/2004				No	[Mew				
Monitoring	Identity Certificates (current: 1, maximum: 2)									
	S	ubject			Issuer	Expiration	1			
	vpn3000-name at	vpn3000-name at cisco snsvpc7-ca at cisco					[View]			
	SSL Certificate	Generate] No	de: The public l	ey in the SSL	certificate is also use	d for the SSH host key	y.			
	Subjec	ct	ls	suer	E	xpiration				
	No SSL Certificat	e								
	Enrollment State	US [Remove /	All: Errored Time	d-Out Rejecte	d Canceled In-Progre	(current: 0 available)	ble: 2)			
	Subject	Issuer	Date	Use	Reason	Method	Sta			
	No Enrollment Red	quests								
	and the second s	and a second sec								

Configurar un grupo para los clientes

Complete este procedimiento para configurar un pool para los clientes:

- Para asignar un rango disponible de direcciones IP, dirija un navegador a la interfaz interna del Concentrador VPN 3000 y seleccione Configuration > System > Address Management > Pools > Add.
- 2. Especifique un intervalo de direcciones IP que no entre en conflicto con ningún otro dispositivo de la red interna y haga clic en

Agregar.	
	Configuration Administration
⊖ <u>Configuration</u>	Configuration System Address Management Pools Add
- D System	Add an address pool.
- Chorace Management	
Assignment	Range Start 10.1.1.100 Enter the start of the IP pool address range.
Pools	
- Tunneling Protocols	Paper End 10.1.1.000 Enter the and of the IP need address range
- BIP Routing	Range End 10.1.1.200 Enter the end of the iP poor address range.
Management	
L Drotocois	Add
General	
- Client Update	
Load Balancing	
- El User Management	
Policy Management	
Administration	
<u>Monitoring</u>	

 Para decirle al concentrador VPN 3000 que utilice el conjunto, seleccione Configuration > System > Address Management > Assignment, marque la casilla Use Address Pools y haga clic en Apply, como en esta

imagen.

	Configuration Administration Monitoring
<u> Configuration </u>	Configuration System Address Management Assignment
<u>Interfaces</u>	
- D System	This section presents Address Assignment options. Each of the following methods are tried, in order,
Servers	until an address is found.
Address Management	
Assignment	Use Client Address
	can be overhousen by usergroup configuration.
Tunneling Protocols	Use Address from Authentication
	Server authentication server for the client.
Protocols	Use DHCP Check to use DHCP to obtain an IP address for the client.
- Events	Use Address Profe Check to use internal address pool configuration to obtain
- @ <u>General</u>	an IP address for the client.
<u>Elient Update</u>	
Load Balancing	Apply Consta
User Management	Apply Cancer
<u> Policy Management</u>	
Administration	
Monitoring	

Configurar una propuesta IKE

Complete estos pasos para configurar una propuesta IKE:

 Seleccione Configuration > System > Tunneling Protocols > IPSec > IKE Proposals, haga clic en Add y seleccione los parámetros, como se muestra en esta imagen.

- General f	Configuration System T	unneling Protocols IPSec IK	di Propos	iais Add
l oad Balancing	Configure and add a new IK	E Proposal.		
Filling Management				
-teruser management				
Base Group	Proposal Name	IKE-for-win2M		Specify the name of this IKE Proposal
Groups				
Users				
- Policy Management	Authentication Mode	RSA Digital Certificate	1.1	Select the authentication mode to use
Access Hours	raturettacauon mone	Horr Dignar Certificate		select the authentication mode to see.
El Traffic Managament				
		LUDEAU AND ADD		And the second se
Network Lists	Authentication Algorithm	MD5/HMAC-128		Select the packet authentication algorithm to use.
Bules				
-SAs	the second second	A CONTRACTOR OF A CONTRACTOR OFTA CONTRACTOR O		
Filters	Encryption Algorithm	DES-56 🗆		Select the encryption algorithm to use.
-mNAT				and the second
Administration				
Administer Sessions	Diffie-Hellman Group	Group 1 (768-bits)		Select the Diffie Heliman Group to use.
The Setting and the set of the se		marks from any		
-ter-Soltware update				
-System Reboot	Lifetime Measurement	Time III		Salart the Matine measurement of the IVE your
-Ping	Lifetime measurement	1100		delect the methic measurement of the rice keys.
-Monitoring Refresh				
- Access Rights	Data Lifetime	10000		Cooper, the data Maline is bilabutes (VD)
-IBFile Management	Data Lifetine	70000		Specify the data metime in kilopytes (KB).
Certificate				
- Management	Time Lifetime	10000		Coacify the time lifetime in seconds
-Enrolment	Tanie Lifetanie	199400		specify the time metime in seconds.
Installation				
Lingitaring		1		
-MOLITORING	Add Cancel			
-GFilterable Event Log				

2. Haga clic en **Agregar**, resalte la nueva propuesta en la columna de la derecha y haga clic en **Activar**.

Configuración de SA

Complete este procedimiento para configurar la Asociación de seguridad (SA):

- Seleccione Configuration > Policy Management > Traffic Management > SA y haga clic en ESP-L2TP-TRANSPORT.Si esta SA no está disponible o si la utiliza para algún otro propósito, cree una nueva SA similar a esta. Se aceptan diferentes configuraciones para la SA. Cambie este parámetro en función de su política de seguridad.
- Seleccione el certificado digital que ha configurado previamente en el menú desplegable Certificado digital. Seleccione la propuesta IKE-for-win2k Internet Key Exchange (IKE).Nota: No es obligatorio. Cuando el cliente L2TP/IPSec se conecta con el Concentrador VPN, todas las propuestas IKE configuradas bajo la columna activa de la página Configuration > System > Tunneling Protocols > IPSec > IKE Proposals se prueban en orden.Esta imagen muestra la configuración necesaria para SA:

∋Configuration				
	IPSec Parameters			
- Policy Management	Authentication Algorithm	ESP/MD5/HMAC-128 🗆		Select the packet authentication algorithm to use.
Access Hours				
Traffic Management	Encryption Appritum	DES-56		Select the ESP encryption algorithm to use.
	citer ypoon regenerati	223.30		Select the Construction argument to select
-SA1		a constant and		
-Eitters	Encapsulation Mode	Transport 🗆		Select the Encapsulation Mode for this SA.
-BNAT				
Administer Sessions	Perfect Forward Secrecy	Disabled 🗆		Select the use of Perfect Forward Secrecy.
-B-Software Lipdate				
-System Reboot	Lifetime Measurement	Time 🗆		Select the lifetime measurement of the IPSec keys.
Ping Monitorion Referation				,
-montoring Henesit	Data Lifetime	30000		Spacify the data lifetime in kilobytes (KR)
- Elle Management	Contraction Contraction	Terista		absent the assentation in measures forth
- Certificate Management	Time Lifetime	Tacoo.		Specify the time lifetime is seconds
e-Monitoring	rine creane	79999		specify the time metine in seconds.
	IKE Parameters			
	IVE Door	0.0.0		Creation the IVE Deep for a Links to Links IDCan expendence
	INE Peer	0.0.0.0		specily the IKE Peer for a LAN-10-LAN IPsec connection.
	Negotiation Mode	Main 🗆		Select the IKE Negotiation mode to use.
	Digital Certificate	vpn3000-name		Select the Digital Certificate to use.
		A		
	Certificate Transmission	Entire certificate chain		Choose how to send the digital certificate to the IKE peer.
		Identity certificate only		-
Cores Sections	IKE Proposal	IKE_for_win7k	- mil	Select the IKE Protocol to use as IKE initiator
	the trapeste			active and a report to and an out initially

Configuración del grupo y el usuario

Complete este procedimiento para configurar el Grupo y el Usuario:

- 1. Seleccione Configuration > User Management > Base Group.
- 2. En la ficha General, asegúrese de que la casilla L2TP sobre IPSec esté marcada.
- 3. En la ficha IPSec, seleccione la SA ESP-L2TP-TRANSPORT.
- 4. En la pestaña PPTP/L2TP, desmarque todas las opciones de L2TP Encryption.
- 5. Seleccione Configuration > User Management > Users y haga clic en Add.
- 6. Introduzca el nombre y la contraseña que utiliza para conectarse desde el cliente de Windows 2000. Asegúrese de seleccionar **Grupo base** en Selección de grupo.
- 7. En la ficha General, verifique el protocolo de tunelización L2TP sobre IPSec.
- 8. En la ficha IPSec, seleccione la SA ESP-L2TP-TRANSPORT.
- 9. En la ficha PPTP/L2TP, desmarque todas las opciones de L2TP Encryption y haga clic en Add.Ahora puede conectarse con la ayuda de L2TP/IPSec Windows 2000 Client.Nota: Ha elegido configurar el grupo base para aceptar la conexión L2TP/IPSec remota. También es posible configurar un grupo que coincida con el campo Unidad organizativa (OU) de la SA para aceptar la conexión entrante. La configuración es idéntica.

Información acerca de la depuración

```
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
```

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 Alq:
   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) ... 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 IKEDBG/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 certreg 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
```

Información de Troubleshooting

Esta sección ilustra algunos problemas comunes y los métodos de solución de problemas para cada uno.

• No se puede iniciar el

servidor.



Lo más probable es que el servicio IPSec no esté iniciado. Seleccione **Inicio > Programas >** Herramientas administrativas > Servicio y asegúrese de que el servicio IPSec está habilitado.

• Error 786: No hay certificado de equipo

⚠	Connecting to 10.48.66.109				
	Error 786: The L2TP connection attempt failed because there is no valid machine certificate on your computer for security authentication.				
1	Padial = 15	Cancel	More Info	1	

válido.

indica un problema con el certificado en el equipo local. Para ver fácilmente su certificado, seleccione **Start > Run**, y ejecute MMC. Haga clic en **Console** y elija **Add/Remove Snap-in**. Haga clic en **Agregar** y elija **Certificado** en la lista. Cuando aparezca una ventana que le pregunte el alcance del certificado, elija **Cuenta de equipo**. Ahora puede comprobar que el certificado del servidor de la CA se encuentra en las **entidades emisoras raíz de confianza**. También puede verificar que tiene un certificado seleccionando **Console Root > Certificate** (Local Computer) > Personal > Certificates, como se muestra en esta

imagen.

Console1 ∫ ⊆onsole Window Help] [) 🚅 🛃 🔲		
Console Root\Certificates (I	.ocal Computer)\Personal\Ce ← → 🗈 💽 💼 🔮 [rtificates	
Tree Favorites	Issued To 🕖	Issued By	
Console Root Certificates (Local Computer Certificates Ce	my_name	snsvpc7-ca	
Personal store contains 2 certificates	5,		

Haga clic en el **certificado**. Compruebe que todo es correcto. En este ejemplo, hay una clave privada asociada al certificado. Sin embargo, este certificado ha caducado. Esta es la causa

This certificate has expired or is not yet valid. Issued to: my_name Issued by: snsvpc7-ca Valid from 2/14/2002 to 2/14/2003 You have a private key that corresponds to this certificate.	Certificate Infor	mation
Issued to: my_name Issued by: snsvpc7-ca Valid from 2/14/2002 to 2/14/2003 You have a private key that corresponds to this certificate.	This certificate has exp	pired or is not yet valid.
Issued to: my_name Issued by: snsvpc7-ca Valid from 2/14/2002 to 2/14/2003 You have a private key that corresponds to this certificate.		
Issued to: my_name Issued by: snsvpc7-ca Valid from 2/14/2002 to 2/14/2003 You have a private key that corresponds to this certificate.		
Issued by: snsvpc7-ca Valid from 2/14/2002 to 2/14/2003 Vou have a private key that corresponds to this certificate.	Issued to: my_nar	me
Valid from 2/14/2002 to 2/14/2003 P You have a private key that corresponds to this certificate.	Issued by: snsvpc	7-ca
\mathscr{W} You have a private key that corresponds to this certificate.	Valid from 2/14/20)02 to 2/14/2003
	1990 C	ev that corresponds to this certificate

- del problema.
- Error 792: Tiempo de espera de negociación de seguridad.Este mensaje aparece después de un período



prolongado.

las depuraciones relevantes como se explica en las Preguntas Frecuentes sobre el

<u>Concentrador VPN 3000 de Cisco</u>. Lean a través de ellos. Debe ver algo similar a este resultado:

```
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
```

Esto indica que la propuesta IKE no se ha configurado correctamente. Verifique la información de la sección <u>Configuración de una Propuesta IKE</u> de este documento.

Error 789: La capa de seguridad encuentra un error de



ve las depuraciones relevantes como se explica en las <u>Preguntas Frecuentes sobre el</u> <u>Concentrador VPN 3000 de Cisco</u>. Lean a través de ellos. Debe ver algo similar a este

resultado:

procesamiento

```
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!
• Versión utilizadaSeleccione Monitoring > System Status para ver este resultado:
    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

Información Relacionada

- Soporte de Productos de Negociación IPSec/Protocolos IKE
- Soporte Técnico Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).