Esempio di configurazione L2TP over IPsec tra Windows 2000 e VPN 3000 Concentrator con certificati digitali

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Obiettivi Convenzioni Ottenere un certificato radice Ottenere un certificato di identità per il client Creare una connessione a VPN 3000 utilizzando la Connessione guidata alla rete Configurazione di VPN 3000 Concentrator Ottenere un certificato radice Ottenere un certificato di identità per VPN 3000 Concentrator Configurare un pool per i client Configurare una proposta IKE Configurazione dell'associazione di protezione Configurare il gruppo e l'utente Informazioni di debug Informazioni sulla risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene illustrata la procedura dettagliata utilizzata per connettersi a un concentratore VPN 3000 da un client Windows 2000 utilizzando il client L2TP/IPSec incorporato. Si presuppone che per autenticare la connessione al concentratore VPN vengano utilizzati i certificati digitali (CA radice autonoma senza il protocollo CEP). In questo documento viene utilizzato il servizio certificati Microsoft a scopo illustrativo. Per la documentazione su come configurarlo, consultare il sito Web <u>Microsoft</u>.

Nota: questo è un esempio solo perché l'aspetto delle schermate di Windows 2000 può cambiare.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento sono relative alla serie Cisco VPN 3000 Concentrator.

<u>Obiettivi</u>

In questa procedura, effettuare le seguenti operazioni:

- 1. Ottenere un certificato radice.
- 2. Ottenere un certificato di identità per il client.
- 3. Creare una connessione a VPN 3000 con l'aiuto della Connessione guidata di rete.
- 4. Configurare VPN 3000 Concentrator.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici</u>.

Ottenere un certificato radice

Per ottenere un certificato radice, completare le istruzioni seguenti:

- 1. Aprire una finestra del browser e digitare l'URL di Microsoft Certificate Authority (in genere http://servername o l'indirizzo IP di CA/certsrv).Viene visualizzata la finestra iniziale per il recupero e la richiesta dei certificati.
- Nella finestra Benvenuti in Selezionare un'operazione, scegliere Recupera il certificato CA o l'elenco di revoche di certificati e fare clic su Avanti.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Favorites Iools Help	
Address 2 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 other the web, sign your e-mail messages, encrypt your e-mail messages, and more depending of of certificate you request. Select a task: Retrieve the CA certificate or certificate revocation list Request a certificate Check on a pending certificate 	icure ar people over ipon the type
	Next>
🖉 Done	ernet //

3. Nella finestra Recupera il certificato CA o l'elenco di revoche di certificati fare clic su **Installa il percorso di certificazione CA** nell'angolo sinistro.Il certificato CA verrà aggiunto all'archivio Autorità di certificazione radice attendibili. Tutti i certificati rilasciati da questa CA al client sono pertanto attendibili.

Example Example Forward for the provided of the second forward of the second forward of the second for the	Microsoft Certificate Se	vices - Microsoft Internet Explaner	
But Retroit Now Seach Fourier Harry Har Par Her //132102250/cetur/cet/cate ap Control Certificate Services — win2know there there //132102250/cetur/cet/cate Revocation List there //132102250/cetur/cet/cate or Certificate Revocation List tal this CA certification path to allow your computer to trust certificates issued from this certificate from this certification authority so one file to download: Certificate OER encoded or C Base 64 encoded Download CA certificate Der encoded or C Base 64 encoded Download CA certificate Der encoded or C Base 64 encoded Download CA certificate Der encoded or C Base 64 encoded Download CA certificate Der encoded or C Base 64 encoded Download CA certificate Download CA certificate Der encoded or C Base 64 encoded Download CA certificate Download Downl	Ede Edi Meni Favia	er Toop Heb	
In the ANTECTED 2 Statement of the Antected 2 Stateme	↓ . + Ret		
travel Certificate Services - with services -	gidenen 💽 hatas //1322.168.	SU/cedux/ceduar.ap	💌 🖓 Ga Lania
tal this CA certificate Or Certificate Revocation List tal this CA certification path to allow your computer to trust certificates issued from this certification authority. s not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the certification path will be installed for you automatically. toose file to download: Certificate Output Demoded or C Base 64 encoded Download CA certification path Certificate Download CA certificate Download CA certification path Certificate Cateroficate Download CA certification path	Microsoft Certificate S	wees windenstwo	Hame
tal this CA certification path to allow your computer to trust certificates issued from this certification authority s not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the s certification path will be installed for you automatically. noose file to download: V Certificate: @ DER encoded or @ Base 64 encoded Download CA certificate Download CA certification path	Retrieve The CA C	artificate Or Certificate Revocation List	
tal this CA certification path to allow your computer to trust certificates issued from this certification authority. Is not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the certification path will be installed for you automatically. Noose file to download: Is Certificate: Certificate: Certificate: Certificate: Demonded or C Base 64 encoded Download CA certification path Download CA certification path			an a
s not necessary to manually install the CA certification path if you request and install a certificate from this certification authority, because the A certification path will be installed for you automatically.	istal this CA certific	ation path to allow your computer to trust certificates issue	d from this certification authority
A certification path will be installed for you automatically.	is not necessary to	manually install the CA certification path if you request and	install a certificate from this certification authority, because the
Certificate: Cuerrificate: Commond CA certificate Download CA certification path Certificate Commond CA certification path Cer	CA certification path	will be installed for you automatically.	
Certificate: ExerciteinScorver PER encoded or C Base 64 encoded Download CA certificate Download CA certification path	hoose file to dow	nload:	
OER encoded or C Base 64 encoded Download CA certificate Download CA certification path	A Certificate: Cue	nt[ein2kserver]	
OER encoded or C Base 64 encoded Download CA certificate Download CA certification path			
DER encoded or Devenload CA certificate Download CA certification path			
Download CA certificate Download CA certification path	۹D	Rencoded or Base 64 encoded	
Download CA certification path	Daw	load CA certificate	
	Dow	fload CA certification path	
Libring and rest certificate revocation rst	Llow	load latest certificate revocation list	
	200		and produced and an
	Stone		😰 kitesset

Ottenere un certificato di identità per il client

Per ottenere un certificato di identità per il client, completare i seguenti passaggi:

- 1. Aprire una finestra del browser e immettere l'URL di Microsoft Certificate Authority (in genere http://servername o l'indirizzo IP di CA/certsrv).Viene visualizzata la finestra iniziale per il recupero e la richiesta dei certificati.
- Nella finestra Benvenuti, in Selezionare un'operazione, scegliere Richiedi un certificato, quindi fare clic su Avanti.

Microsoft Certificate Services - Microsoft Internet Explorer	
Elle Edit View Fgvorites Icols Help	
Back Forward Stop Refresh Home Search Favorites History Mail Print	
Address C http://10.10.102.42/certsrv/	
Microsoft Certificate Services winZkserver	Home
Welcome	
You use this web site to request a certificate for your web browser, e-mail client, or other program. Once you acquire a certificate, you will be able to securely identify yourself to ot 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 C Retrieve the CA certificate C Check on a pending certificate	secure her people over g upon the type
	Next>
🛃 Done	Internet

3. Dalla finestra Scegli tipo di richiesta, selezionare Richiesta avanzata e fare clic su

Microsoft Certificate Services - Microsoft Internet Explores	
Elle Edi Yew Favories Inch Help	
Back I Stop Refeat Hane Seatch Fercetes Hatoy Hall Pint	
Researched with the rest of th	- C.00
Microsoft Conflictus Benicos: + wrDowner	Es.
Choose Request Type	
Disace color; the time of regrestion would like to make:	
Prease serecture type of request you would like to make.	
O User certificate request.	
Web Elevador Costá opto	
E-Mail Protection Certificate	
Advanced request	
	Next >
Done	internet

4. Nella finestra Richieste avanzate di certificati selezionare Invia una richiesta di certificato alla CA utilizzando un

Ad	vanced Certificate Requests
Yo me ob	u can request a certificate for yourself, another user, or a computer using one of the following thods. Note that the policy of the certification authority (CA) will determine the certificates that yo tain.
e	Submit a certificate request to this CA using a form.
c	Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using base64 encoded PKCS #7 file.
c	Request a certificate for a smart card on behalf of another user using the Smart Card Enrollmer Station.
	You must have an enrollment agent certificate to submit a request for another user.

5. Compilare i campi come in questo esempio.Il valore di Reparto (unità organizzativa) deve corrispondere al gruppo configurato nel concentratore VPN. Non specificare una dimensione della chiave maggiore di 1024. Assicurarsi di selezionare la casella di controllo **Usa archivio computer locale**. Al termine, fare clic su

ficate Request	×
ation	1
win2kdientid	
ahiga	
support	
marklin	
ma	
US	
ĸ	
Client Authentication Certificate	
Microsoft Base Cryptographic Provider v1.0	
C Exchange IF Signature C Both	
512 Max 10204 Beermon key sizes (02 2025 2008 0008 2008 0008 0008 0008 00	
6 Create new key set	
E Set the container name	
C Use existing key set	
Enable strong private key protection	
T Mark keys as exportable	
E Use local machine store	
You must be an administrator to gaveraite	
	ficate Request

seconda della configurazione del server CA, questa finestra viene talvolta visualizzata. In caso affermativo, contattare l'amministratore della

Certific	ile Pending
Your ce	fficate request has been received. However, you must wait for an administrator to issue the certificate you requested.
Please	etum to this web site in a day or two to retrieve your certificate.
Note: Yo	must return with this web browser within 10 days to retrieve your certificate

6. Fare clic su **Home page** per tornare alla schermata principale, selezionare **Controlla certificato in sospeso** e fare clic su

Please select the certificate	requestyou want to check:	
Otion Authentication Cert	CEW (02/19/2000 09:50:59)	
		Fag

7. Nella finestra Certificato rilasciato fare clic su Installa il

Aliconnali Certificate Services - witChosmer	. Bane
Certificate issued	
The certificate you requested was issued to you.	
THE TIME DIS CHIDCHE	
).[

- 8. Per visualizzare il certificato client, selezionare **Start > Esegui** ed eseguire Microsoft Management Console (MMC).
- 9. Fare clic su **Console** e scegliere **Aggiungi/Rimuovi snap-in**.
- 10. Fare clic su Add (Aggiungi) e selezionare Certificate (Certificato) dall'elenco.
- 11. Quando viene visualizzata una finestra in cui viene richiesto l'ambito del certificato, scegliere **Account computer**.
- 12. Verificare che il certificato del server CA si trovi nelle Autorità di certificazione radice attendibili. Verificare inoltre di disporre di un certificato selezionando Console Root > Certificate (Local Computer) > Personal > Certificates (Radice console > Certificato (Computer locale) > Personal > Certificates), come mostrato

ien minagine.				
Console1				-IQI ×
<u>⊆</u> onsole <u>Window</u> <u>H</u> elp				
Console Root\Certificate	es (Local Computer)\Person	nal\Certificates		
Action yew Eavorites	+ + 5 00 00	🖸 🖳 🔡		
Tree Favorites	Essued To /	Issued By	Expiration	
Console Root Certificates (Local Com Personal Certificates Certificate	(and the second secon	witt2kserver	3(1/2001_	
Personal store contains 1 certifi	ate.			

Creare una connessione a VPN 3000 utilizzando la Connessione guidata alla rete

Completare questa procedura per creare una connessione alla VPN 3000 con l'aiuto della connessione guidata di rete:

- 1. Fare clic con il pulsante destro del mouse su **Risorse di rete**, scegliere **Proprietà** e fare clic su **Crea nuova connessione**.
- Nella finestra Tipo di connessione di rete scegliere Connetti a una rete privata tramite Internet e quindi fare clic su Avanti.

You you	i can choose the type of network connection you want to create, based on r network configuration and your networking needs.
C	Dial-up to private network
	Connect using my phone line (modem or ISDN).
С	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
100	Let other computers connect to mine by phone line, the Internet, or direct cable.
C	Connect directly to another computer
100	Connect using my serial, parallel, or infrared port.
	< Back Next> Cance

3. Immettere il nome host o l'indirizzo IP dell'interfaccia pubblica del concentratore VPN e fare clic su

Avanti.

twork Connection Wizard		
Destination Address What is the name or address of the	edestination?	Í.
Type the host name or IP address of connecting.	of the computer or network to which you are	
Host name or IP address (such as n	nicrosoft.com or 123.45.6.78):	
64.67.72.180		
2		
	20	
	Z Back Neuts	Cancel

4. Nella finestra Disponibilità connessione selezionare **Personale** e fare clic su **Avanti**.

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

 Nella finestra Rete pubblica, selezionare se comporre automaticamente la connessione iniziale (l'account ISP).

Network Connection Wizard	
Public Network Windows can make sure the public network is connected first.	I)
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 >	Cancel

 Nella schermata Indirizzo di destinazione, immettere il nome host o l'indirizzo IP del concentratore VPN 3000 e fare clic su Avanti.

twork Connection Wizard		
Destination Address What is the name or address of the	destination?	S
Type the host name or IP address o connecting.	f the computer or network to which yo	ou are
Host name or IP address (such as r	nicrosoft.com or 123.45.6.78):	
64.67.72.180		
2		
	< Back Next >	Cancel

7. Nella finestra Connessione guidata di rete, immettere un nome per la connessione e fare clic su **Fine**.Nell'esempio, la connessione è denominata "Cisco corporate VPN".



8. Nella finestra Connessione privata virtuale fare clic su

Connect Virtua	l Private Conne	ection	<u>?×</u>
			N/
User name:	jedgaruser		
Password:	*****		
	Save Pass	word	
Connect	Cancel	Properties	Help

Proprietà.

- 9. Nella finestra Proprietà selezionare la scheda Rete.
- 10. In Tipo di server VPN chiamato scegliere L2TP dal menu a discesa, selezionare Protocollo Internet TCP/IP, quindi fare clic su

Cisco corporate VPN	? ×				
General Options Security Networking					
Type of VPN server Lam calling:					
Layer-2 Tunneling Protocol (L2TP)	•				
Settings					
Components checked are used by this connection:					
 Internet Protocol (TCP/IP) File and Printer Sharing for Microsoft Networks Client for Microsoft Networks 					
Install Uninstall Properties					
Description					
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.					
OK Can	icel				

Proprietà.

- 11. Selezionare **Avanzate > Opzioni > Proprietà**.
- 12. Nella finestra Protezione IP scegliere Utilizza questo criterio di protezione



- 13. Scegliere il criterio **Client (solo risposta)** dal menu a discesa e fare clic su **OK** più volte fino a tornare alla schermata Connetti.
- 14. Per avviare una connessione, immettere il nome utente e la password e fare clic su **Connetti**.

Configurazione di VPN 3000 Concentrator

Ottenere un certificato radice

Completare questi passaggi per ottenere un certificato radice per VPN 3000 Concentrator:

- 1. Posizionare il browser sulla CA, ad esempio http://ip_add_of_ca/certsrv/, **Recuperare il** certificato CA o l'elenco di revoche di certificati e fare clic su Avanti.
- 2. Fare clic su Scarica certificato CA e salvare il file nel disco locale.
- 3. Sul concentratore VPN 3000, selezionare Amministrazione > Gestione certificati, quindi fare clic su Fare clic qui per installare un certificato e Installare un certificato CA.
- 4. Fare clic su Upload File from Workstation.
- 5. Fare clic su Sfoglia e selezionare il file del certificato CA appena scaricato.
- 6. Evidenziare il nome del file e fare clic su **Installa**.

Configuration	Administration Certificate	e Management			Tuesday, 12 February
Administration					
-Administer Sessions					
Software Update	This section lets you view a	and manage certificates on the \	/PN 3000 Concentrator	C	
System Reboot					
Ping	 Click here to enroll y 	with a Certificate Authority			
-Monitoring Refresh	 <u>Click here to install</u> 	a certificate			
- CO-Access Rights	Cartificate Authorities	forward 1 montaneous Ph			
- @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	Assessmentstermenter		navalues and a subscription of	housessee	and a constant of the second
⊖ Monitoring	Identity Certificates (cu	urrent: 0, maximum: 2)			
	Subject	Issuer	Exp	iration	Actions
	No Identity Certificates				
Sessions	Enter that out you have put at \$1,000 at \$1,0000 at \$1,0000 at \$1,0000 at \$1,0000 at \$1,0000 at		an an daar dad oo daa ay Karana ay ka	and the second second second provide the	
and the second s	001 0-016-01	and a set and the set of the set of the		and the second second second	

Ottenere un certificato di identità per VPN 3000 Concentrator

Completare questi passaggi per ottenere un certificato di identità per VPN 3000 Concentrator:

 Selezionare ConfAdministration > Certificate Management > Enroll > Identity Certificate, quindi fare clic su Enroll via PKCS10 Request (Manual). Compilare il modulo come mostrato di seguito e fare clic su

regisiia.			
B-Configuration	Administration Certificate Management	it Enroll Mentity Certificate PKCS	10
3-Administration			
<u>Administer Sessions</u>	Enter the information to be included in th	e certificate request. The CA's certificati	must be installed as a Certificate Authority before installing the
- BSoftware Update	certificate you requested. Please wait for	the operation to finish.	
-System Reboot			
Ping			Enter the common name for the VPN 3000 Concentrator
Monitoring Refresh	Common Name (CN)	vpn3000-nase	to be used in this PKI
BACCess Rights			
- BElle Management	Ormanizational Unit (OU)	and	Enter the department
GCertificate Management	organization and (ob)	and	Enter the superment.
Enrolment			The second secon
Installation	Organization (O)	cisco	Enter the Organization or company.
paratoring			
	Locality (1)	borli	Enter the city or town
	carrier (c)	and	child die day of total.
	State/Province (SP)	1	Enter the State or Province.
	Country (C)	be	Enter the two-letter country abbreviation (e.g. United
			states = US).
	Chief Manual and Contain		Enter the Fully Qualified Domain Name for the VPN 3000
	Subject AlternativeName (FGDN)	vpn3000-name.cisco.com	Concentrator to be used in this PKI.
			Fritzense Fritzense fritzense fritzense sonne
	Subject AlternativeName (E-Mail	*	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI
	(Annuss)		Concentration to be used to this Pro.
	Kou Olas	DCA F12 bits	Calend the how size for the approximated DCA FICA have any
	key size	ROR DIZ DIS D	belect the key size for the generated HSH/DSH key pair.
	Enroll Cancel		
	t t		

Viene visualizzata una finestra del browser con la richiesta di certificato. Deve contenere testo simile a questo output:

-----BEGIN NEW CERTIFICATE REQUEST----MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu czEOMAwGA1UEChMFY21zY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG SIb3DQEJDjE1MCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW11LmNpc2NvLmNvbTAN BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak= -----END NEW CERTIFICATE REQUEST----

- 2. Posizionare il browser sul server CA, selezionare **Richiedi certificato**, quindi fare clic su **Avanti**.
- 3. Selezionare Advanced Request, fare clic su Next, quindi selezionare Submit a certificate request using a base64 encoded PKCS #10 file or a RENEWATE REQUEST using a base64 encoded PKCS #7 file.

- 4. Fare clic su **Next** (Avanti). Tagliare e incollare il testo della richiesta di certificato visualizzato in precedenza nell'area di testo. Fare clic su **Invia**.
- 5. In base alla configurazione del server CA, è possibile fare clic su **Scarica certificato CA**. Oppure, non appena il certificato è stato rilasciato dalla CA, tornare al server CA e selezionare **Controlla un certificato in sospeso**.
- 6. Fare clic su Avanti, selezionare la richiesta e fare di nuovo clic su Avanti.
- 7. Fare clic su **Scarica certificato CA** e salvare il file sul disco locale.
- 8. Sul concentratore VPN 3000, selezionare Amministrazione > Gestione certificati > Installa e fare clic su Installa certificato ottenuto tramite registrazione.La richiesta in sospeso verrà visualizzata con lo stato "In corso", come illustrato in questa

<u>Confic</u> ent	Logged quration Administration Mr
Confic ent	ouration Administration Mr
ent	
fathod Status	Artime
section Sectors	Pacimonis
anual In Progress	[[Merce:] Install, Delete:]
	Aethod Status anual In Progress

- 9. Fare clic su Installa, quindi su Carica file dalla workstation.
- 10. Fare clic su Sfoglia e selezionare il file contenente il certificato rilasciato dalla CA.
- 11. Evidenziare il nome del file e fare clic su Installa.
- 12. Selezionare **Amministrazione > Gestione certificati**. Verrà visualizzata una schermata simile all'immagine.

							Co	onfigurat	
Configuration	Administration Ce	artificate Mar	nagement					Wednes	
Administer Sessions Software Update System Reboot Ping Monitoring Refresh DAccess Rights	This section lets you view and manage certificates on the VPN 3000 Concentrator.								
- Certificate Management	Subjec	t	Issuer			Expiration	SCEP Issuer	1	
Installation Monitoring	snsvpc7-ca at cis	co	snsvpc7-ca at cisco			02/14/2004	No	[Mew	
	Identity Certificates (current: 1, maximum: 2)								
	Subject			Iss	uer	Expiration			
	vpn3000-name at cisco snsvpc7-ca at cisco						02/14/2003	[View]	
	SSL Certificate [Generate] Note: The public key in the SSL certificate is also used for the SSH host key.								
	Subjec	ct	1	ssuer		E	quiration	1	
	No SSL Certificate								
	Enrollment State	US [Remove A	II: Errored Tim	ed-Out Rei	ected (Cancelled In-Progres) (current: 0 availa)	ble: 2)	
	Subject	Issuer	Date	U	se	Reason	Method	Sta	
	No Enrollment Red	quests							

Configurare un pool per i client

Completare questa procedura per configurare un pool per i client:

- Per assegnare un intervallo disponibile di indirizzi IP, puntare un browser all'interfaccia interna di VPN 3000 Concentrator e selezionare Configurazione > Sistema > Gestione indirizzi > Pool > Aggiungi.
- 2. Specificare un intervallo di indirizzi IP che non sia in conflitto con altri dispositivi nella rete

interna e fare clic su Aggiungi

<u>, aguangn</u>			
			Configuration Administration
⊖ <u>Configuration</u>	Configuration	System Address k	Aanagement Pools Add
<u>Interfaces</u>			
- D System	Add an addres	s pool.	
Address Management	Dance Start	10 1 1 100	Enter the start of the IP need address range
<u>Assignment</u>	Range Start	10.1.1.100	Enter the start of the IP pool address range.
Pools			
Tunneling Protocols	Range End	10.1.1.200	Enter the end of the IP pool address range.
	-	-	
Protocols			
I ImEvents	Add	Cancel	
General			
- Client Update			
Load Balancing			
User Management			
Policy Management			
Administration			
Monitoring			

 Per indicare a VPN 3000 Concentrator di utilizzare il pool, selezionare Configurazione > Sistema > Gestione indirizzi > Assegnazione, selezionare la casella Usa pool di indirizzi e fare clic su Applica, come in questa

٠					
I	m	m	20	un	
I			au		10.
_			<u> </u>	,	

			Configuration Administration Monitoring				
<u> ← Configuration</u>	Configuration System Address Ma	Configuration System Address Management Assignment					
- Content	This section presents Address Assignment options. Each of the following methods are tried, in order,						
- El Servers	until an address is found.						
Address Management							
Assignment Pools	Use Client Address		Check to use the IP address supplied by the client. This can be overridden by user/group configuration.				
Tunneling Protocols	Use Address from Authentication	-	Check to use an IP address retrieved from an				
- IP Routing	Server	-	authentication server for the client.				
<u>⊢⊞ Management</u> Protocols	Use DHCP		Check to use DHCP to obtain an IP address for the client.				
<u> </u>	Use Address Pools		Check to use internal address pool configuration to obtain an IP address for the client.				
Client Update							
Load Balancing							
- Buser Management	Apply Cancel						
Belicy Management							
⊕ Administration							
Monitoring							

Configurare una proposta IKE

Per configurare una proposta IKE, completare i seguenti passaggi:

 Selezionare Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE, fare clic su Aggiungi e selezionare i parametri, come mostrato nell'immagine.

	Concernation of the second sec	Anna Mars Marsley etc. 1 1000 and 1 100	F. Electronic	1.0.0
General	Configuration [system] 1	unneling Protocols IP-sec IK	a: mopo:	rais 24dd
	Contains and a state of the second	E Burnard		
Load Balancing	Configure and add a new IK	E Proposal.		
- E-User Management	- · · · · · · · · · · · · · · · · · · ·			
Base Group		Station Street		 A. A. A
Groups	Proposal Name	IKE-for-win2M		Specify the name of this IKE Proposal.
Users	and the second second second second		_	
- Policy Management	Authentication Mode	RSA Digital Certificate		Select the authentication mode to use.
Access Hours				
GTraffic Management				
-Network Lists	Authentication Algorithm	MD5/HMAC-128 🗆		Select the packet authentication algorithm to use.
Bules		the second s		
SAs				
Filters	Encryption Algorithm	DES-56 🗆		Select the encryption algorithm to use.
TINAT	and the second second			
Administration				
Administor Soccions	Diffie-Heliman Group	Group 1 (768-bits)		Select the Diffie Heliman Group to use
Administer Sessions	Dirite Heining Group	anash (tee and)		beleet the bine rieman aroup to ave.
- (e) Software Update				
-System Reboot	Lifetime Meanument	Time		Colort the Matine measurement of the N/E hours
-Ping	Lifetime Measurement	-ume -		Select the measurement of the PCE keys.
-Monitoring Refresh				
- Access Rights	Data Lifetime	10000		Constitution data Matima in bilabutan (VD)
- EFile Management	Data Lifetine	70000		opecity the data metime in knobytes (KD).
Certificate				
Management	Time Lifetime	196400		Specify the time lifetime in seconds
-Enrolment	This create	100400		opecity the time method in seconds.
Installation				
Monitoring				
- Routing Table	Add Cancel			
Eliterable Event Loc				
CPF and able Event Lod		7		

2. Fare clic su **Aggiungi**, evidenziare la nuova proposta nella colonna di destra e fare clic su **Attiva**.

Configurazione dell'associazione di protezione

Completare questa procedura per configurare l'associazione di sicurezza (SA):

- Selezionare Configurazione > Gestione delle policy > Gestione del traffico > SA e fare clic su ESP-L2TP-TRANSPORT.Se l'associazione di protezione non è disponibile o viene utilizzata per altri scopi, crearne una nuova simile a questa. Sono accettabili impostazioni diverse per l'associazione di protezione. Modificare questo parametro in base ai criteri di protezione.
- 2. Selezionare il certificato digitale configurato in precedenza nel menu a discesa Certificato digitale. Selezionare la proposta IKE (Internet Key Exchange) IKE-for-win2k.Nota: non è obbligatorio. Quando il client L2TP/IPSec si connette al concentratore VPN, tutte le proposte IKE configurate nella colonna attiva della pagina Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE vengono tentate in ordine.L'immagine mostra la configurazione necessaria per l'associazione di protezione:

Configuration				
	IPSec Parameters			
- Policy Management	Authentication Algorithm	ESP/MD5/HMAC-128 🗆		Select the packet authentication algorithm to use.
Network Lists Rules	Encryption Algorithm	DES-56 🗆		Select the ESP encryption algorithm to use.
	Encapsulation Mode	Transport 🗆		Select the Encapsulation Mode for this SA.
Administration Administer Sessions	Perfect Ferward Secrecy	Disabled 🗆		Select the use of Perfect Forward Secrecy.
	Lifetime Measurement	Time 🗆		Select the lifetime measurement of the IPSec keys.
	Data Lifetime	10000		Specify the data lifetime in kilobytes (KB).
-@ <u>Certificate Management</u> 9 Monitoring	Time Lifetime]3e00		Specify the time lifetime in seconds.
	IKE Parameters			
	IKE Peer	0.0.0.0		Specify the IKE Peer for a LAN-to-LAN IPSec connection.
	Negotiation Mode	Main 🗀		Select the IKE Negotiation mode to use.
	Digital Certificate	vpn3000-name]	Select the Digital Certificate to use.
	Certificate Transmission	 Entire certificate chain Identity certificate only 		Choose how to send the digital certificate to the IKE peer.
Cisco Systems	IKE Proposal	IKE-for-win2k	Ξ.	Select the IKE Proposal to use as IKE initiator.

Configurare il gruppo e l'utente

Completare questa procedura per configurare il gruppo e l'utente:

- 1. Selezionare Configurazione > Gestione utente > Gruppo base.
- 2. Nella scheda General (Generale), verificare che L2TP over IPSec sia selezionato.
- 3. Nella scheda IPSec, selezionare la scheda ESP-L2TP-TRANSPORT SA.
- 4. Nella scheda PPTP/L2TP, deselezionare tutte le opzioni di crittografia L2TP.
- 5. Selezionare Configurazione > Gestione utente > Utenti e fare clic su Aggiungi.
- 6. Immettere il nome e la password utilizzati per la connessione dal client Windows 2000. Assicurarsi di selezionare **Gruppo base** in Selezione gruppo.
- 7. Nella scheda General (Generale), controllare il protocollo di tunneling L2TP over IPSec.
- 8. Nella scheda IPSec, selezionare la scheda ESP-L2TP-TRANSPORT SA.
- 9. Nella scheda PPTP/L2TP, deselezionare tutte le opzioni di crittografia L2TP, quindi fare clic su Aggiungi.Èora possibile connettersi con l'aiuto del client L2TP/IPSec Windows 2000.Nota: si è scelto di configurare il gruppo di base per accettare la connessione L2TP/IPSec remota. È inoltre possibile configurare un gruppo che corrisponda al campo Unità organizzativa (OU, Organization Unit) dell'associazione di sicurezza per accettare la connessione in ingresso. La configurazione è identica.

Informazioni di debug

```
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
```

Informazioni sulla risoluzione dei problemi

In questa sezione vengono illustrati alcuni problemi comuni e i relativi metodi di risoluzione.

Impossibile avviare il



X

Èmolto probabile che il servizio IPSec non sia stato avviato. Selezionare Start > Programmi > Strumenti di amministrazione > Servizio e verificare che il servizio IPSec sia abilitato.

Errore 786: Nessun certificato computer

Error Cor	nnecting to l2tp over ip	sec to vpn3k		? ×
A	Connecting to 10.48.66.	109		
<u></u>	Error 786: The L2TP cor valid machine certificate authentication.	nnection attempt faile on your computer fo	ed because there r security	is no
	Redial = 45	Cancel	More Info	1

valido.

errore indica un problema con il certificato nel computer locale. Per esaminare facilmente il certificato, selezionare Start > Esegui ed eseguire MMC. Fare clic su Console e scegliere Aggiungi/Rimuovi snap-in. Fare clic su Add (Aggiungi) e selezionare Certificate (Certificato) dall'elenco. Quando viene visualizzata una finestra in cui viene richiesto l'ambito del certificato, scegliere Account computer A questo punto è possibile verificare che il certificato del server CA si trovi nelle Autorità di certificazione radice attendibili. È inoltre possibile verificare di disporre di un certificato selezionando Directory principale della console >

Certificato (computer locale) > Personale > Certificati, come illustrato in questa immagine.

Console Root\Certificates (Loc	al Computer)\Personal\Ce	rtificates	
Action View Eavorites	→ 🗈 💽 🛤 🖗 🛛	3 3	
Tree Favorites	Issued To 🕢	Issued By	
Console Root Certificates (Local Computer) Certificates C		ывүрс/-са	
ersonal store contains 2 certificates.			11.

Fare clic sul **certificato**. Verificare che tutto sia corretto. In questo esempio è presente una chiave privata associata al certificato. Il certificato è scaduto. Questa è la causa del

Cert	ificate	3
Ge	eneral Details Certification Path	
	Certificate Information	
	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	
	\mathscr{P} You have a private key that corresponds to this certificat	e,
	Issuer Sta	tement

 Errore 792: Timeout della negoziazione di sicurezza.Questo messaggio viene visualizzato dopo un lungo



periodo.

relativi debug come spiegato nelle <u>domande frequenti su Cisco VPN 3000 Concentrator</u>. Leggete attraverso di loro. È necessario visualizzare un risultato simile a questo:

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

```
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
```

Ciò indica che la proposta IKE non è stata configurata correttamente. Verificare le informazioni nella sezione <u>Configurazione di una proposta IKE</u> di questo documento.

• Errore 789: Il livello di protezione rileva un errore di



elaborazione. Attivize i relativi debug come spiegato nelle domande frequenti su Cisco VPN 3000 Concentrator.

Leggete attraverso di loro. È necessario visualizzare un risultato simile a questo: 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! Versione utilizzataSelezionare Monitoraggio > Stato sistema per visualizzare questo output: 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

Informazioni correlate

- Negoziazione IPSec/protocolli IKE Supporto dei prodotti
- <u>Supporto tecnico Cisco Systems</u>

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).