L2TP über IPsec zwischen Windows 2000 und VPN 3000 Concentrator unter Verwendung digitaler Zertifikate - Konfigurationsbeispiel

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Ziele Konventionen Abrufen eines Stammzertifikats Abrufen eines Identitätszertifikats für den Client Erstellen einer Verbindung mit dem VPN 3000 mithilfe des Netzwerkverbindungs-Assistenten Konfigurieren des VPN 3000 Concentrator Abrufen eines Stammzertifikats Erhalt eines Identitätszertifikats für den VPN 3000 Concentrator Konfigurieren eines Pools für die Clients Konfigurieren eines IKE-Angebots Konfigurieren der SA Konfigurieren der Gruppe und des Benutzers Debuginformationen Informationen zur Fehlerbehebung Zugehörige Informationen

Einleitung

Dieses Dokument zeigt die schrittweise Vorgehensweise für die Verbindung mit einem VPN 3000 Concentrator von einem Windows 2000-Client mithilfe des integrierten L2TP/IPSec-Clients. Es wird davon ausgegangen, dass Sie digitale Zertifikate (Standalone Root Certification Authority (CA) ohne Certificate Enrollment Protocol (CEP)) verwenden, um Ihre Verbindung mit dem VPN Concentrator zu authentifizieren. In diesem Dokument wird der Microsoft-Zertifikatdienst zur Veranschaulichung verwendet. Informationen zur Konfiguration finden Sie auf der <u>Microsoft</u> -Website.

Hinweis: Dies ist nur ein Beispiel, weil sich die Darstellung der Windows 2000-Bildschirme ändern kann.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument bezieht sich auf die Cisco VPN 3000 Concentrator-Serie.

<u>Ziele</u>

In diesem Verfahren führen Sie folgende Schritte aus:

- 1. Rufen Sie ein Stammzertifikat ab.
- 2. Abrufen eines Identitätszertifikats für den Client
- 3. Erstellen Sie mithilfe des Netzwerkverbindungs-Assistenten eine Verbindung zum VPN 3000.
- 4. Konfigurieren Sie den VPN 3000 Concentrator.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps von Cisco zu Konventionen).

Abrufen eines Stammzertifikats

Führen Sie die folgenden Anweisungen aus, um ein Stammzertifikat zu erhalten:

- Öffnen Sie ein Browserfenster, und geben Sie die URL f
 ür die Microsoft-Zertifizierungsstelle ein (normalerweise http://servername oder die IP-Adresse von CA/certsrv).Das Willkommensfenster f
 ür Zertifikatabrufe und -anforderungen wird angezeigt.
- Wählen Sie im Fenster Willkommen unter Aufgabe auswählen die Option Zertifizierungsstellenzertifikat oder Zertifikatsperrliste abrufen aus, und klicken Sie auf Weiter.

Microsoft Certificate Services - Microsoft Internet Explorer	
Ele Edit View Favorites Icols Help	8 0
Address @ http://10.10.102.42/certsrv/	▪ ∂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 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. Klicken Sie im Fenster zum Abrufen des Zertifizierungsstellenzertifikats oder der Zertifikatsperrliste in der linken Ecke auf Diesen Zertifizierungsstellenzertifizierungspfad installieren. Dadurch wird das Zertifizierungsstellenzertifikat dem Speicher der vertrauenswürdigen Stammzertifizierungsstellen hinzugefügt. Das bedeutet, dass alle Zertifikate, die diese Zertifizierungsstelle für diesen Client ausstellt, vertrauenswürdig sind.

General Certificate Services - Microsoft Internet Captorer	1.6
Ele Ed Ven Fanales Iook Heb	
Agáres el hay://132162.550/ceture/ceture.ap	· Pos Links
El Remain B. Cast Scate. Coming a la cast de la c	thereas a
And and a state of the state of	
Retrieve The CA Certificate Or Certificate Revocation List	
instal this CA certification path to allow your computer to trust certificates issued from this certificat	ion authority
It is not necessary to manually install the CA certification path if you request and install a certificate CA certification path will be installed for you automatically.	from this certification authority, because the
Choose file to download:	
CA Certificate: Cunant[win2liserver]	
COED second of an C Data 64 second of	
M DER elicited of Y Base of allcoded	
Download CA certification path	
Download latest certificate revocation list	
T make	NACION.

Abrufen eines Identitätszertifikats für den Client

Führen Sie die folgenden Schritte aus, um ein Identitätszertifikat für den Client zu erhalten:

- 1. Öffnen Sie ein Browserfenster, und geben Sie die URL für die Microsoft-Zertifizierungsstelle ein (normalerweise http://servername oder die IP-Adresse von CA/certsrv).Das Willkommensfenster für Zertifikatabrufe und -anforderungen wird angezeigt.
- Wählen Sie im Willkommensfenster unter Wählen Sie eine Aufgabe aus die Option Zertifikat anfordern, und klicken Sie auf Weiter.

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

3. Wählen Sie im Fenster "Anforderungstyp auswählen" die Option "**Erweiterte Anforderung**" aus, und klicken Sie auf

Microsoft Certificate Services - Microsoft Internet Explorer	2 S S S
Elle Edit View Favorites Lack Help	
Back France State Honey Hand P	
Agdenie 🕑 Mip.//10.10.242/certurv/certique.aup	💌 🖓 🛈 a 🛛 Unita 🍽
Microsoft Contificate Services Welchsonner	El Italia Hanna
Choose Request Type	
Please select the type of request you would like to make:	
C User certificate request:	
E-Mail Protection Centificate	
Advanced request	
	Next>
(oitor" Riter	all been

4. Wählen Sie im Fenster "Erweiterte Zertifikatanforderungen" die Option Zertifikatanforderung mit einem Formular an diese Zertifizierungsstelle senden



5. Füllen Sie die Felder wie in diesem Beispiel aus.Der Wert für die Abteilung (Organisationseinheit) muss mit der im VPN Concentrator konfigurierten Gruppe übereinstimmen. Geben Sie keine Schlüssellänge größer als 1024 an. Aktivieren Sie das Kontrollkästchen Lokalen Computerspeicher verwenden. Wenn Sie fertig sind, klicken Sie auf

Waitar

Advanced Certif	ficate Request	
Identifying information:		
Name	win2kdientid	
E-Mail:		
Company.	aliga	
Department	support	
City:	franklin	
State:	ma	
CountryRegion	US	
Intended Purpose	c	
	Client Authentication Certificate	
Key Options:		
CSP:	Microsoft Base Cryptographic Pravider v1.0	
Key Usage:	C Eschange ∉ Signature C Both	
Key Size:	512 Marc 304 Marc 10204 Reserves Rep stees: 552 2028 2028 doll 2028 10205 1	
	Create new key set	
	E Set the container name	
	C Use existing key set	
	E Enable strong private key protection	
	Mark keys as exportable	
	You must be an achimototator to generate a key in the local machine alone.	

e nach Konfiguration des CA-Servers wird dieses Fenster manchmal angezeigt. Wenden Sie sich andernfalls an den CA-

	Numeral Contractory and Associate	N.
	Certificate Pending	
	Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.	
	Please return to this web site in a day or two to retrieve your certificate.	
	Hate: You must return with this web braves within 10 days to retrieve your certificate	
A		
Administrator.		1

6. Klicken Sie auf **Startseite**, um zum Hauptbildschirm zurückzukehren, wählen Sie **Ausstehendes Zertifikat überprüfen aus**, und klicken Sie auf

Please select the certificate request you want to check:	
Chart Auffrenkon Cartilicate (62/18/2800.08.50.58)	
	10

7. Klicken Sie im Fenster Certificate Issued (Von Zertifikat ausgestellt) auf Install this

	Microsoft Cariflete Services - without the
	Certificate issued
	The cettificate you requested was issued to you.
	ter the certificate
ricate.	

- 8. Um das Client-Zertifikat anzuzeigen, wählen Sie **Start > Ausführen**, und führen Sie die Microsoft Management Console (MMC) aus.
- 9. Klicken Sie auf Konsole, und wählen Sie Snap-In hinzufügen/entfernen aus.
- 10. Klicken Sie auf Hinzufügen, und wählen Sie Zertifikat aus der Liste aus.
- 11. Wenn ein Fenster angezeigt wird, in dem Sie nach dem Umfang des Zertifikats gefragt werden, wählen Sie **Computerkonto**.
- 12. Überprüfen Sie, ob sich das Zertifikat des Zertifizierungsstellenservers unter den vertrauenswürdigen Stammzertifizierungsstellen befindet. Überprüfen Sie außerdem, ob Sie über ein Zertifikat verfügen, indem Sie Konsolenstamm > Zertifikat (Lokaler Computer) > Personal > Zertifikate auswählen, wie in diesem Bild



Erstellen einer Verbindung mit dem VPN 3000 mithilfe des Netzwerkverbindungs-Assistenten

Gehen Sie wie folgt vor, um mithilfe des Netzwerkverbindungs-Assistenten eine Verbindung zum VPN 3000 herzustellen:

- 1. Klicken Sie mit der rechten Maustaste auf **Netzwerkumgebung**, wählen Sie **Eigenschaften aus**, und klicken Sie auf **Neue Verbindung herstellen**.
- Wählen Sie im Fenster Netzwerkverbindungstyp die Option Über das Internet mit einem privaten Netzwerk verbinden aus, und klicken Sie dann auf Weiter.

letwor You you	k Connection Type I can choose the type of network connection you want to create, based on I network configuration and your networking needs.
с	Dial-up to private network
~	Connect using my phone line (modern or 15DN).
0	Dial-up to the Internet
	Connect to the internet using my phone line (modern of 15DN).
۲	Connect to a private network through the Internet
	Create a Virtual Private Network (VPN) connection or 'tunnel' through the Internet.
C	Accept incoming connections
	Let other computers connect to mine by phone line, the Internet, or direct cable.
C	Connect directly to another computer
	Connect using my serial, parallel, or infrared port.
	< <u>B</u> ack <u>N</u> ext> Cance

 Geben Sie den Hostnamen oder die IP-Adresse der öffentlichen Schnittstelle des VPN Concentrator ein, und klicken Sie auf Weiter.

wo	ork Connection Wizard
De	estination Address What is the name or address of the destination?
	Type the host name or IP address of the computer or network to which you are connecting.
	Host name or IP address (such as microsoft.com or 123.45.6.78):
	64.67.72.180
	<back next=""> Cancel</back>

 Wählen Sie im Fenster Verbindungsverfügbarkeit die Option Nur für mich aus, und klicken Sie auf Weiter.

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. Wählen Sie im Fenster Public Network (Öffentliches Netzwerk) aus, ob die ursprüngliche Verbindung (das ISP-Konto) automatisch gewählt werden soll.

I)
·
,
ncel

6. Geben Sie im Bildschirm Destination Address (Zieladresse) den Hostnamen oder die IP-Adresse des VPN 3000 Concentrator ein, und klicken Sie auf **Next** (Weiter).

	rrk Connection Wizard
De	estination Address
	Type the host name or IP address of the computer or network to which you are connecting.
	Host name or IP address (such as microsoft.com or 123,45,6,78);
	64.67.72.180

7. Geben Sie im Fenster Netzwerkverbindungs-Assistent einen Namen für die Verbindung ein, und klicken Sie auf **Fertig stellen**. In diesem Beispiel heißt die Verbindung "Cisco Corporate VPN".



8. Klicken Sie im Fenster Virtuelle private Verbindung auf



Eigenschaften.

- 9. Wählen Sie im Fenster Eigenschaften die Registerkarte Netzwerk aus.
- 10. Wählen Sie unter Type of VPN server I am call aus dem Pulldown-Menü L2TP aus, markieren Sie Internet Protocol TCP/IP, und klicken Sie auf

Cisco corporate VPN	<u>? ×</u>
General Options Security Networking	
Type of VPN server I am calling:	
Layer-2 Tunneling Protocol (L2TP)	•
Se	ettings
Components checked are used by this connection:	
 Internet Protocol (TCP/IP) File and Printer Sharing for Microsoft Networks Client for Microsoft Networks 	
Install Uninstall Prope	erties
Transmission Control Protocol/Internet Protocol. The de wide area network protocol that provides communicatio across diverse interconnected networks.	efault on
ОК	Cancel

- Properties.

 11. Wählen Sie Erweitert > Optionen > Eigenschaften aus.
- 12. Wählen Sie im Fenster "IP Security" die Option Use this IP security policy (Diese IP-Sicherheitsrichtlinie

Do not use IPSEC	
Jse this IP security policy:	
Client (Respond Only)	
Communicate normally (un	secured). Use the default response rule
negotiate with servers that	request security. Only the requested
Communicate normally (un	secured). Use the default response rule
negotiate with servers that	request security. Only the requested
protocol and port traffic wit	th that server is secured.
Communicate normally (un	secured). Use the default response rule
negotiate with servers that	request security. Only the requested
protocol and port traffic wit	th that server is secured.

verwenden).

- 13. Wählen Sie im Pulldown-Menü die **Client (Response Only)**-Richtlinie aus, und klicken Sie mehrmals auf **OK**, bis Sie zum Bildschirm "Connect" zurückkehren.
- 14. Um eine Verbindung herzustellen, geben Sie Ihren Benutzernamen und Ihr Kennwort ein, und klicken Sie auf **Verbinden**.

Konfigurieren des VPN 3000 Concentrator

Abrufen eines Stammzertifikats

Gehen Sie wie folgt vor, um ein Root-Zertifikat für den VPN 3000 Concentrator zu erhalten:

- Zeigen Sie in Ihrem Browser auf Ihre Zertifizierungsstelle (normalerweise etwas wie http://ip_add_of_ca/certsrv/), rufen Sie das Zertifizierungsstellenzertifikat oder die Zertifikatsperrliste ab, und klicken Sie auf Weiter.
- 2. Klicken Sie auf **CA-Zertifikat herunterladen**, und speichern Sie die Datei auf der lokalen Festplatte.
- 3. Wählen Sie im VPN 3000 Concentrator Administration > Certificate Management aus, und klicken Sie auf Click here (Hier klicken), um ein Zertifikat zu installieren und CA-Zertifikat zu installieren.
- 4. Klicken Sie auf Datei von Workstation hochladen.
- 5. Klicken Sie auf **Durchsuchen**, und wählen Sie die Zertifikatsdatei aus, die Sie gerade heruntergeladen haben.
- 6. Markieren Sie den Dateinamen, und klicken Sie auf Installieren.

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	t.	
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				

Erhalt eines Identitätszertifikats für den VPN 3000 Concentrator

A mmaldam

Gehen Sie wie folgt vor, um ein Identitätszertifikat für den VPN 3000 Concentrator zu erhalten:

 Wählen Sie ConfAdministration > Certificate Management > Enroll > Identity Certificate aus, und klicken Sie dann auf Enroll via PKCS10 Request (Manual). Füllen Sie das Formular wie hier gezeigt aus und klicken Sie auf

Anneuen.			
B-Configuration	Administration Certificate Management	it Enroll Mentity Certificate PKC	510
Administration			
 Administer Sessions 	Enter the information to be included in th	e certificate request. The CA's certifica	te must be installed as a Certificate Authority before installing the
- B Software Update	certificate you requested. Please wait for	the operation to finish.	
-System Reboot			
Ping	and the second sec	•	Enter the common name for the VPN 3000 Concentrator
Monitoring Refresh	Common Name (CN)	vpn3000-nawe	to be used in this PKI.
- BAccess Rights			
-Brie Management	Organizational Unit (OU)	ana	Enter the department
Greeningate Management		1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.	and
Enrolment	10 10		and the second second second
	Organization (O)	cisco	Enter the Organization or company.
C THE REAL PROPERTY OF THE PRO			
	Locality (L)	bell	Enter the city or town.
		1.1.2	and a state of the
	Dista Designed (DD)		Palastic Palaster State
	atalentivince (ar)	A.	Enter the state of Province.
			False the loss letter country obtaining to a United
	Country (C)	be	States = US)
			energy - proj
	Subject AlternativeName (FODN)	von3000-name ciaco.com	Enter the Fully Qualified Domain Name for the VPN 3000
	conference (ranny	division and a second	Concentrator to be used in this PKI.
	Subject AlternativeName (E-Mail	×	Enter the E-Mail Address for the VPN 3000
	Address)	â.	Concentrator to be used in this PKI.
	Key Size	RSA 512 bits 🖂	Select the key size for the generated RSA/DSA key pair.
	,		the section of a barrier formula provide the section of a first section of a sectio
	Enroll Cancel		

Die Zertifikatsanforderung wird in einem Browserfenster angezeigt. Es muss Text enthalten, der dieser Ausgabe ähnlich ist:

-----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. Zeigen Sie in Ihrem Browser auf den CA-Server, aktivieren Sie **Zertifikat anfordern,** und klicken Sie auf **Weiter**.
- 3. Aktivieren Sie Erweiterte Anforderung, klicken Sie auf Weiter, und wählen Sie eine Zertifikatsanforderung mit einer Base64-codierten PKCS #10-Datei oder eine Verlängerungsanforderung mit einer Base64-codierten PKCS #7-Datei senden aus.

- 4. Klicken Sie auf **Next** (Weiter). Schneiden Sie den Text der zuvor im Textbereich angezeigten Zertifikatsanforderung aus, und fügen Sie ihn ein. Klicken Sie auf **Senden**.
- 5. Je nach Konfiguration des Zertifizierungsstellenservers können Sie auf Zertifizierungsstellenzertifikat herunterladen klicken. Wenn das Zertifikat von der Zertifizierungsstelle ausgestellt wurde, kehren Sie zum Zertifizierungsstellenserver zurück, und aktivieren Sie die Option Auf ausstehendes Zertifikat überprüfen.
- 6. Klicken Sie auf Weiter, wählen Sie Ihre Anfrage aus, und klicken Sie erneut auf Weiter.
- 7. Klicken Sie auf **CA-Zertifikat herunterladen**, und speichern Sie die Datei auf dem lokalen Datenträger.
- Wählen Sie im VPN 3000 Concentrator die Optionen Administration > Certificate Management > Install aus, und klicken Sie auf Install certificate received via enrollment (Zertifikat installieren).Sie sehen dann Ihre ausstehende Anfrage mit dem Status "In Bearbeitung", wie in diesem



- 9. Klicken Sie auf Installieren, gefolgt von Datei von Workstation hochladen.
- 10. Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei aus, die das von der Zertifizierungsstelle ausgestellte Zertifikat enthält.
- 11. Markieren Sie den Dateinamen, und klicken Sie auf Installieren.
- 12. Wählen Sie Administration > Certificate Management aus. Ein Bildschirm, der diesem Bild ähnelt, wird

angezeigt.								
						Co	onfigurat	
Configuration Administration —Administer Sessions	Administration Ce	artificate Ma	nagement				Wednes	
Boftware Update System Reboot Ping Monitoring Refresh BAccess Rights File Management	This section lets yo <u>Click here to</u> <u>Click here to</u> Certificate Author	u view and m enroll with a install a cert orities (cum	nanage certifi a <u>Certificate A</u> <u>tificate</u> ent: 1, maxim	cates on the \ outhority um: 6)	/PN 3000 Concentra	tor.		
- Certificate Management	Subjec	t	Contraction of the local data	ssuer	Expiration	SCEP Issuer	1	
Enrollment	snsvpc7-ca at cis	co	snsvpc7-ca	at cisco	02/14/2004	No	[Mew]	
Monitoring	Identity Certificates (current: 1, maximum: 2)							
	3	ubject		1	ssuer	Expiration	1	
	vpn3000-name at	cisco	s	nsvpc7-ca at	cisco	02/14/2003	[<u>View</u>]	
	SSL Certificate	Generate] No	te: The public	key in the SSL	. certificate is also use	d for the SSH host ke	y.	
	Subjec	ct	1	ssuer	E	xpiration	1	
	No SSL Certificat	e						
	Enrollment State	US [Remove A	III: Errored Tim	ed-Out Rejecte	d Cancelled In-Progre	ss] (current: 0 availa	ble: 2)	
	Subject	Issuer	Date	e Use	Reason	Method	Sta	
	No Enrollment Re	quests						

Konfigurieren eines Pools für die Clients

Gehen Sie wie folgt vor, um einen Pool für die Clients zu konfigurieren:

- Um einen verfügbaren IP-Adressbereich zuzuweisen, zeigen Sie in einem Browser auf die interne Schnittstelle des VPN 3000 Concentrator, und wählen Sie Configuration > System > Address Management > Pools > Add aus.
- 2. Geben Sie einen IP-Adressbereich an, der nicht mit anderen Geräten im Netzwerk in Konflikt steht, und klicken Sie auf Hinzufügen

r inizaragon:					
				Configuration A	dministration
<u> ← Configuration</u>	Configuration	System Address N	lanagement Pools	Add	
<u>Interfaces</u>					
- D System	Add an addres	s pool.			
Servers .					
Address Management	Ranne Start	10 1 1 100	Enter the start of th	e IP nool address r	ongo
-Assignment Reals	mange ovare	10.1.1.100	Enter the start of th	ie ir poor address it	ange.
Tunneling Protocols		-			
BIP Routing	Range End	10.1.1.200	Enter the end of the	e IP pool address ra	nge.
Management					
Protocols					
Events	Add	Cancel			
- Ceneral					
Client Update					
Load Balancing					
User Management					
- Management					
-ter-Monitoring					

 Um den VPN 3000 Concentrator anzuweisen, den Pool zu verwenden, wählen Sie Configuration > System > Address Management > Assignment, aktivieren Sie das Kontrollkästchen Use Address Pools (Adresspools verwenden), und klicken Sie wie in diesem Bild auf Apply (Anwenden)

	Configuration Administration Monitoring
<u>Configuration</u>	Configuration System Address Management Assignment
Interfaces	
- D System	This section presents Address Assignment options. Each of the following methods are tried, in order,
Servers	until an address is found.
- C-Address Management	
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
I Her 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>Events</u>	Use Address Prote E Check to use internal address pool configuration to obtain
General	an IP address for the client.
- Elient Update	
Load Balancing	
User Management	Apply Cancel
Policy Management	
Administration	
Monitoring	

Konfigurieren eines IKE-Angebots

Gehen Sie wie folgt vor, um ein IKE-Angebot zu konfigurieren:

 Wählen Sie Configuration > System > Tunneling Protocols > IPSec > IKE Proposals aus, klicken Sie auf Add und wählen Sie die Parameter aus, wie in diesem Bild dargestellt.

- General 1	Configuration System 1	unneling Protocols IPSec IK	E Propos	als (Add
Client Update	a martine second second second			
Load Balancing	Configure and add a new IK	E Proposal.		
CHIser Management				
Pate Group		A STATE AND A STATE		
Crawer,	Proposal Name	IKE-for-win2M		Specify the name of this IKE Proposal.
Groups		the second state of the second		
<u>Users</u>				
- 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				
SAc				
Filton	Encreation Algorithm	DES-56		Select the encruntion election to use
E INLEIS	Linerypoon regorium	DE3-30 L		beleet the energyboon algonium to use.
-waar				
Administration	Diffe Hallman Course	Crown I (200 bills)		Colord the Diffe Linkson Group to use
Administer Sessions	Dime-Hellman Group	Group I (766-bits)		Select the Dime Helman Group to use.
- CSoftware Update				
-System Reboot	· · · · · · · · · · · · · · · · · · ·	Concernant of the second se		All and second literation does not free with reaction 10 and only a
-Ping	Lifetime Measurement	Time 🗔		Select the lifetime measurement of the IKE keys.
-Monitoring Refresh				
- Access Rights		The second		
- Management	Data Lifetime	10000		Specify the data lifetime in kilobytes (KB).
Certificate				
Phanagement		To cross		
Englinent	Time Lifetime	186400		specify the time inetime in seconds.
Installation		5		
Instanation				
Monicoring	Add Cancel			
-Routing Table				
-GFilterable Event Log				

2. Klicken Sie auf **Hinzufügen**, markieren Sie den neuen Vorschlag in der rechten Spalte, und klicken Sie auf **Aktivieren**.

Konfigurieren der SA

Gehen Sie wie folgt vor, um die Sicherheitszuordnung (Security Association, SA) zu konfigurieren:

- Wählen Sie Configuration > Policy Management > Traffic Management > SA aus, und klicken Sie auf ESP-L2TP-TRANSPORT.Wenn diese SA nicht verfügbar ist oder Sie sie für einen anderen Zweck verwenden, erstellen Sie eine neue SA, die dieser ähnelt. Unterschiedliche Einstellungen für die SA sind akzeptabel. Ändern Sie diesen Parameter entsprechend Ihrer Sicherheitsrichtlinie.
- 2. Wählen Sie das zuvor konfigurierte digitale Zertifikat im Pulldown-Menü Digitales Zertifikat aus. Wählen Sie das Angebot IKE-for-win2k Internet Key Exchange (IKE) aus.Hinweis: Dies ist nicht obligatorisch. Wenn der L2TP/IPSec-Client eine Verbindung mit dem VPN Concentrator herstellt, werden alle IKE-Vorschläge, die in der aktiven Spalte der Seite Konfiguration > System > Tunneling-Protokolle > IPSec > IKE-Vorschläge konfiguriert wurden, der Reihe nach ausprobiert.Dieses Bild zeigt die erforderliche Konfiguration für die SA:

Configuration			
	IPSec Parameters		
GPolicy Management	Authentication Algorithm	ESP/MD5/HMAC-128 🗆	Select the packet authentication algorithm to use.
Access Hours			
Traffic Management	Encryption Algorithm	DE5-56 (7)	Select the ESP encruption algorithm to use
Pulot	cuci ypaon regonann	DE3-30 L	beloct the Cor entrypoon algorithm to use.
SAs			
-Eitters	Encapsulation Mode	Transport 🗀	Select the Encapsulation Mode for this SA.
- ID-NAT			
Administration	Perfect Ferward Secrecy	Disabled 🗆	Select the use of Perfect Forward Secrecy.
-@Software Lipdate			
System Reboot	Lifetime Measurement	Time 🗔	Select the lifetime measurement of the IPSec keys
Ping	Circuite Provider Circuite	Take a	condition include include in the incode negative
Monitoring Refresh	Data Lifetime	30000	Council, the data lifetime is block day of the
-@File Management	Data Lifetime	310000	Specify the data intrime in kilopytes (KB).
- Certificate Management	had the shakes of	had the second s	
-Monitoring	Time Lifetime	13e00	Specify the time lifetime in seconds.
	NE Deservations		
	IKE Parameters		
	IKE Peer	0.0.0.0	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
	Neoptiation Mode	Main 🖂	Select the IKE Neoptiation mode to use
	District Confederate	100000000000000000000000000000000000000	Fried the District Coddinate to use
	Digital Certificate	vpn3000-name 🖾	Select the Digital Certificate to use.
		O Entire certificate chain	
	Certificate Transmission	A literate contract contract	Choose how to send the digital certificate to the IKE peer.
		 identity certificate only 	
Cores Sections	IKE Procesal	IKE-for-win2k	Select the IKE Proposal to use as IKE initiator
	the composed		

Konfigurieren der Gruppe und des Benutzers

Gehen Sie wie folgt vor, um die Gruppe und den Benutzer zu konfigurieren:

- 1. Wählen Sie Configuration > User Management > Base Group aus.
- 2. Vergewissern Sie sich auf der Registerkarte Allgemein, dass L2TP über IPSec aktiviert ist.
- 3. Wählen Sie auf der Registerkarte IPSec die ESP-L2TP-TRANSPORT SA aus.
- 4. Deaktivieren Sie auf der Registerkarte PPTP/L2TP alle Optionen für die L2TP-Verschlüsselung.
- 5. Wählen Sie Konfiguration > Benutzerverwaltung > Benutzer aus, und klicken Sie auf Hinzufügen.
- 6. Geben Sie den Namen und das Kennwort ein, die Sie für die Verbindung mit dem Windows 2000-Client verwenden. Stellen Sie sicher, dass Sie unter "Gruppenauswahl" die Option **Basisgruppe** auswählen.
- 7. Aktivieren Sie auf der Registerkarte General (Allgemein) das L2TP over IPSec-Tunneling-Protokoll.
- 8. Wählen Sie auf der Registerkarte IPSec die ESP-L2TP-TRANSPORT SA aus.
- 9. Deaktivieren Sie auf der Registerkarte PPTP/L2TP alle L2TP-Verschlüsselungsoptionen, und klicken Sie auf Hinzufügen. Sie können nun mithilfe des L2TP/IPSec Windows 2000 Clients eine Verbindung herstellen. Hinweis: Sie haben sich entschieden, die Basisgruppe so zu konfigurieren, dass sie die Remote-L2TP/IPSec-Verbindung akzeptiert. Es ist auch möglich, eine Gruppe zu konfigurieren, die dem Feld für die Organisationseinheit (OU) des SA entspricht, um die eingehende Verbindung zu akzeptieren. Die Konfiguration ist identisch.

Debuginformationen

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 Alq:
   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) ... 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 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

Informationen zur Fehlerbehebung

In diesem Abschnitt werden einige häufige Probleme und die jeweiligen Fehlerbehebungsmethoden erläutert.

• Der Server kann nicht gestartet



Höchstwahrscheinlich wird der IPSec-Dienst nicht gestartet. Wählen Sie **Start > Programme > Verwaltung > Dienst aus,** und stellen Sie sicher, dass der **IPSec-Dienst** aktiviert ist.

• Fehler 786: Kein gültiges



Computerzertifikat.

Dieser Fehler weist auf ein Problem mit dem Zertifikat auf dem lokalen Computer hin. Um Ihr

Zertifikat einfach anzuzeigen, wählen Sie **Start > Ausführen**, und führen Sie MMC aus. Klicken Sie auf **Konsole**, und wählen Sie **Snap-In hinzufügen/entfernen aus**. Klicken Sie auf **Hinzufügen**, und wählen Sie **Zertifikat** aus der Liste aus. Wenn ein Fenster angezeigt wird, in dem Sie nach dem Umfang des Zertifikats gefragt werden, wählen Sie **Computerkonto**.Jetzt können Sie überprüfen, ob sich das Zertifikat des Zertifizierungsstellenservers unter den **vertrauenswürdigen Stammzertifizierungsstellen** befindet. Sie können auch überprüfen, ob Sie über ein Zertifikat verfügen, indem Sie **Konsole Root > Certificate (Local Computer) > Personal > Certificates (Konsolenstamm > Zertifikat (Lokaler Computer) > Personal > Zertifikate) auswählen**, wie in diesem Bild



Klicken Sie auf das **Zertifikat**. Überprüfen Sie, ob alles korrekt ist. In diesem Beispiel ist dem Zertifikat ein privater Schlüssel zugeordnet. Dieses Zertifikat ist jedoch abgelaufen. Das ist die Ursache des

	📆 Certific	ate Informatio	n.	
ī	his certificat	e has expired o	r is not yet va	alid.
	Iccurd to			
	Issued to	r: my_name		
	Issued by	y: snsvpc7-ca		
	Valid fror	n 2/14/2002 to	2/14/2003	
	🌮 You have a	a private key that	corresponds to	this certificate.

• Fehler 792: Timeout bei Sicherheitsaushandlung.Diese Meldung wird nach längerer Zeit



angezeigt.

n Sie die entsprechenden Debugging-Funktionen, wie in den <u>Häufig gestellten Fragen</u> zum <u>Cisco VPN 3000 Concentrator</u> erläutert. Lies sie durch. Sie müssen etwas Ähnliches wie diese Ausgabe sehen:

```
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
```

Dies weist darauf hin, dass das IKE-Angebot nicht richtig konfiguriert wurde. Überprüfen Sie die Informationen im Abschnitt Konfigurieren eines IKE-Angebots in diesem Dokument.

• Fehler 789: Auf der Sicherheitsschicht tritt ein Verarbeitungsfehler

	Connecting to 10.48.66.	109		
E la	rror 789: The L2TP cor ayer encountered a proc ne remote computer.	nnection attempt faile cessing error during in	d because the sec itial negotiations w	urity vith
	Redial = 37	Cancel	More Info	ř.

die entsprechenden Debugging-Funktionen, wie in den <u>Häufig gestellten Fragen</u> zum <u>Cisco</u> <u>VPN 3000 Concentrator</u> erläutert. Lies sie durch. Sie müssen etwas Ähnliches wie diese

```
Ausgabe sehen:
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!

Verwendete VersionWählen Sie Überwachung > Systemstatus, um diese Ausgabe anzuzeigen:

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

Zugehörige Informationen

- IPSec-Aushandlung/IKE-Protokolle Produktsupport
- Technischer Support Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.