# Konfigurieren eines Cisco VPN 500 Concentrator mit externer Authentifizierung für einen Microsoft Windows 2000 IAS RADIUS Server

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfiguration des Cisco VPN 5000 Concentrator Konfigurieren des Microsoft Windows 2000 IAS RADIUS-Servers Überprüfen des Ergebnisses Konfigurieren des VPN-Clients Concentrator-Protokolle Fehlerbehebung Zugehörige Informationen

# **Einführung**

In diesem Dokument werden die Verfahren beschrieben, die zum Konfigurieren eines Cisco VPN 500 Concentrator mit externer Authentifizierung für einen Microsoft Windows 2000 Internet Authentication Server (IAS) mit RADIUS verwendet werden.

**Hinweis:** CHAP (Challenge Handshake Authentication Protocol) funktioniert nicht. Verwenden Sie ausschließlich das Password Authentication Protocol (PAP). Weitere Informationen finden Sie unter Cisco Bug ID <u>CSCdt96941</u> (nur <u>registrierte</u> Kunden).

# Voraussetzungen

#### **Anforderungen**

Für dieses Dokument bestehen keine speziellen Anforderungen.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dieser Softwareversion:

Cisco VPN 5000 Concentrator Software Version 6.0.16.0001

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten

Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u>.

# Konfiguration des Cisco VPN 5000 Concentrator

VPN5001_4B9CBA80				
VPN5001_4B9CBA80> <b>show config</b> Enter Password:				
Edited Configuration not Present, using Running				
[ General ] EthernetAddress = DeviceType = ConfiguredOn = ConfiguredFrom = EnablePassword = Password =	00:02:4b:9c:ba:80 VPN 5001 Concentrator Timeserver not configured Command Line, from Console			
[ IP Ethernet 0 ] Mode = SubnetMask = IPAddress = [ IP Ethernet 1 ]	Routed 255.255.255.0 172.18.124.223			
Mode =	Off			
[ IKE Policy ] Protection =	MD5_DES_G1			
[ VPN Group "rtp-group" ] BindTo = Transform = LocalIPNet = MaxConnections = IPNet =	<pre>"ethernet0" esp(md5,des) 10.1.1.0/24 10 0.0.0.0/0</pre>			
[ RADIUS ] BindTo = ChallengeType = PAPAuthSecret = PrimAddress = Secret = UseChap16 = Authentication =	"ethernet0" PAP "pappassword" "172.18.124.108" "radiuspassword" Off On			
<pre>[ Logging ] Level = Enabled = Configuration size is 1065 VPN5001 4B9CBA80#</pre>	7 On out of 65500 bytes.			

### Konfigurieren des Microsoft Windows 2000 IAS RADIUS-Servers

Diese Schritte führen Sie durch eine einfache RADIUS-Serverkonfiguration in Microsoft Windows 2000 IAS.

 Wählen Sie unter den Microsoft Windows 2000 IAS-Eigenschaften Clients aus, und erstellen Sie einen neuen Client. In diesem Beispiel wird ein Eintrag mit dem Namen VPN5000 erstellt. Die IP-Adresse des Cisco VPN 500 Concentrator lautet 172.18.124.223. Wählen Sie im Dropdown-Feld Client-Anbieter die Option Cisco aus. Der gemeinsam genutzte geheime Schlüssel ist der geheime Schlüssel im [ RADIUS] Abschnitt der <u>VPN Concentrator-</u>

VPN5000 Properties	? ×
Settings	
Friendly name for client:	
VPN5000	
Client address	
Address (IP or DNS):	
Verify	
Climit Vanden C	
Client must always send the s	ignature attribute in the request
Shared secret:	******
Confirm shared secret:	******
	OK Cancel Apply

Konfiguration.

2. Wählen Sie unter den Eigenschaften der Remote-Zugriffsrichtlinie im Abschnitt "Wenn ein Benutzer die Bedingungen erfüllt" die Option **Remotezugriffsberechtigung erteilen aus**, und klicken Sie dann auf **Profil** 

olicy name:	Allow acce	ess it dial-in permis:	sion is enabled	
pecify the cond	itions to match:			
) ay-And-Time-P	estrictions matche	es "Sun 00:00-24:	00; Mon 00:00	24:00
d	-			n.
а.				
Add	Remove	Edit		
lf a user match	es the conditions-			
6.0.1	nte access permis:	sion		
Intrant remo	,			
Grant remo		sion		
C Deny remo	te access permis:			
<ul> <li>Grant remo</li> <li>Deny remo</li> <li>Access will is overridd</li> </ul>	ite access permis: I be granted with t an on a per-user b	the profile you spe	cify, unless acc	cess
C Deny remo Access wi is overridd	ite access permiss I be granted with t en on a per-user b	the profile you spe lasis.	cify, unless acc	cess
C Deny remo Access wi is overridd	ite access permiss I be granted with t en on a per-user b	the profile you spe Jasis.	cify, unless acc	
C Deny remo Access wi is overridd	ite access permiss I be granted with I en on a per-user b	the profile you spe lasis.	cify, unless acc	

- bearbeiten.
- 3. Klicken Sie auf die Registerkarte Authentifizierung, und stellen Sie sicher, dass nur unverschlüsselte Authentifizierung (PAP, SPAP) ausgewählt

	ial-in Profile			
	Dial-in Constraints	IP	1	Multilink
	Authentication	Encrypti	on	Advanced
С	heck the authentication	methods which	are allowed fo	r this connection.
the second	Extensible Authentio	cation Protocol		
	Select the EAP type wh	nich is acceptable	e for this policy	ı.
	MD5-Challenge		<b>v</b>	Configure
	<ul> <li>Encrypted Authentio</li> <li>Unencrypted Authention</li> </ul>	cation (CHAP) ntication (PAP, S	PAP)	
F	Unauthenticated Acces	:5		

4. Wählen Sie die Registerkarte Erweitert aus, klicken Sie auf **Hinzufügen**, und wählen Sie **Anbieterspezifisch** aus.

Dial-in Constraints		P Multiink	Order	
Authentication	Encry	ption Advanced	1 1	
pecify additional connects	on attributes	to be returned to the Remote		
ccess Server.		dd Attributes		and the second
arameters:				-
Name	Vendo	To add an attribute to the Pro	file, select the attribut	e and click Add.
righte	Torido			
		RADIUS attributes:		
		Name	Vendor	Description
		Reply-Message	RADIUS Standard	Message to be displayed to user when authenticati
		Service-Type	RADIUS Standard	Type of service user has requested
		Tunnel-Assignment-ID	RADIUS Standard	Tunnel to which a session is to be assigned
		Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the auther
		Tunnel-Client-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
		Tunnel-Medium-Type	RADIUS Standard	Transport medium to use when creating a tunnel for
		Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
		Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
1		Tunnel-Pvt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
		Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth
Add Remov	VB	Tunnel-Server-Endpt	RADIUS Standard	IP address of the server end of the tunnel
		Tunnel-Type	RADIUS Standard	Tunneling protocols to be used
		Vendor/Specific	HADIUS Standard	Used to support proprietary NAS features
		Lisco-AV-Par	Lisco	Lisco AV Par VSA
		USD AT Calling & EBro	U.S. HODORCS, I	Description not available
		USP AT Call Order A Face	U.S. Hobolics, I	Description not available
		LICD AT Jose & Elbar	U.S. Hobolics, I	Description not available
	OK	USP.AT.Output.Eiter	U.S. Hobolics, I	Description not available
		LISB AT BTMPJ mut Filer	U.S. Robotice I	Description not available
		our state in the apportune	0.0. H000003, L.	Description from available
				A11 Ch.

5. Klicken Sie im Dialogfeld Mehrwertige Attributinformationen f
ür das anbieterspezifische Attribut auf Hinzuf
ügen, um zum Dialogfeld Herstellerspezifische Attributinformationen zu gelangen. W
ählen Sie Anbietercode eingeben und geben Sie 255 in das angrenzende Feld ein. W
ählen Sie anschlie
ßend Ja aus. Es entspricht und klickt auf Attribut konfigurieren.

iultivalued Attr	ibute Information	<u>?</u> ×	Vendor-Specific Attribut	e Information
Attribute name:			Attribute name:	
Vendor-Specific			Vendor-Specific	
Attribute number:			Specify network access se	erver vendor.
26			C Select from list	RADIUS Standard
Attribute format:			· Enter Vendor Code:	255
OctetString				
Attribute values:			Specify whether the attribut vendor specific attributes	te conforms to the RADIUS RFC specification for
Vendor	Value	Move Up	Yes It conforms	
		Move Down	C	
		Add	<ul> <li>No. It does not conform</li> </ul>	<b>k</b> . (1)
		Remove	Configure Attribute	
		Edi		OK Canad
•		1		UK Carbei
	0	Cancel		

6. Geben Sie im Dialogfeld Configure VSA (RFC-konform) (VSA konfigurieren) **4** für die vom Anbieter zugewiesene Attributnummer ein, geben Sie **String** für das Attributformat ein, und

geben Sie **rtp-group** (Name der VPN-Gruppe im Cisco VPN 5000 Concentrator) für den Attributwert ein. Klicken Sie auf **OK**, und wiederholen Sie Schritt

/endor-assigned attribute number	r.	
Attribute format:		
String		
Attribute value:		
rtp-group		

7. Geben Sie im Dialogfeld Configure VSA (RFC-kompatibel) (VSA konfigurieren) (RFC-kompatibel) 4 für die vom Anbieter zugewiesene Attributnummer ein, geben Sie String für das Attributformat ein, und geben Sie cisco123 (den Client Shared geheim) für den Attributwert ein. Klicken Sie auf

onfigure VSA (RFL compliant)	
Vendor-assigned attribute number:	
5	
Attribute format:	
String	
Attribute value:	
cisco123	
	K Cano

8. Sie sehen, dass das anbieterspezifische Attribut zwei Werte enthält (Gruppen- und VPN-

Dial-in Constraints       IP       Multilink         Authentication       Encryption       Advanced         Specify additional connection attributes to be returned to the Remote       Access Server.         Access Server.       *arameters:         Name       Vendor       Value         Vendor-Specific       RADIUS Standard       rtp-group, cisco123         Add       Remove       Edit	Dial-in Profile		
Authentication       Encryption       Advanced         Specify additional connection attributes to be returned to the Remote       Access Server.         Parameters:       Parameters:       Vendor       Value         Name       Vendor       Value       Vendor-Specific         Vendor-Specific       RADIUS Standard       rtp-group, cisco123         Add       Remove       Edit	Dial-in Constraints	IP	Multilink
Access Server.  Access Server.  Arameters:  Name Vendor Value Vendor-Specific RADIUS Standard rtp-group, cisco123  Add Remove Edit	Authentication	Encryption	Advanced
Name     Vendor     Value       Vendor-Specific     RADIUS Standard     rtp-group, cisco123       Image: Comparison of the standard standard     rtp-group, cisco123	Specify additional connecti Access Server. Parameters:	on attributes to be return	ned to the Remote
Vendor-Specific RADIUS Standard rtp-group, cisco123  Add Remove Edit	Name	Vendor	Value
Add Remove Edit	Vendor-Specific	RADIUS Standard	rtp-group, cisco123
	Add Remo	ve Edit	2

Kennwort).

9. Klicken Sie unter den Benutzereigenschaften auf die Registerkarte Einwählen, und stellen Sie sicher, dass die Option **Zugriffssteuerung über Remote-Zugriffsrichtlinie** ausgewählt

eneral Member Of Profile Dial-in	
Remote Access Permission (Dial-in or VPN)	
C Allow access	
C Deny access	
<ul> <li>Control access through Remote Access Poli</li> </ul>	cy
🗖 Verify Caller-ID:	
Callback Options	
No Callback	
C Set by Caller (Routing and Remote Access)	Service only)
C Always Callback to:	
Assign a Static IP Address	a. a. a.
Assign a Static IP Address     Apply Static Routes	(4 (4 a))
Assign a Static IP Address     Apply Static Routes     Define routes to enable for this Dial-in     connection.	Static Routes
Assign a Static IP Address     Apply Static Routes     Define routes to enable for this Dial-in     connection.	Static Routes

### Überprüfen des Ergebnisses

Dieser Abschnitt enthält Informationen, die Sie verwenden können, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom <u>Output Interpreter Tool</u> unterstützt (nur <u>registrierte</u> Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show radius statistics** Zeigt Paketstatistiken für die Kommunikation zwischen dem VPN Concentrator und dem im RADIUS-Abschnitt identifizierten RADIUS-Standardserver an.
- show radius config Zeigt die aktuellen Einstellungen für RADIUS-Parameter an.

Dies ist die Ausgabe des Befehls show radius statistics.

VPN5001_4B9CBA80> <b>show</b>	radius	statisti	lcs
RADIUS Stats			
Accounting	Primary	7 5	Secondary
Poguoata	0		200

0	-	
Requests	0	na
Responses	0	na

Retransmissions	0	na
Bad Authenticators	0	na
Malformed Responses	0	na
Packets Dropped	0	na
Pending Requests	0	na
Timeouts	0	na
Unknown Types	0	na

Authentication	Drimary	Secondary
Auchichicicación	FIIIIIII Y	Secondary
Requests	3	na
Accepts	3	na
Rejects	0	na
Challenges	0	na
Retransmissions	0	na
Bad Authenticators	0	na
Malformed Responses	0	na
Packets Dropped	0	na
Pending Requests	0	na
Timeouts	0	na
Unknown Types	0	na

VPN5001\_4B9CBA80>

#### Dies ist die Ausgabe des Befehls show radius config.

RADIUS		State	UDP	CHAP16	5
Authenticat	ion	On	1812	No	
Accounting		Off	1813	n/a	
Secret		'radiusp	asswor	rd '	
Server	IP add	lress	Atte	empts	AcctSecret
Primary	172.18	8.124.108	;	5	n/a
Secondary	Off				

### Konfigurieren des VPN-Clients

Dieses Verfahren führt Sie durch die Konfiguration des VPN-Clients.

 Wählen Sie im Dialogfeld VPN-Client die Registerkarte Konfiguration aus. Geben Sie anschließend im Dialogfeld VPN Client-Prompt for Secret (VPN-Client-Aufforderung zur Geheimhaltung) den gemeinsamen geheimen Schlüssel unter dem VPN-Server ein. Der gemeinsame geheime Schlüssel des VPN-Clients ist der Wert, der für das VPN-Kennwort des Attributs 5 im VPN-Konzentrator eingegeben

Name	Partner	Login Method	Add.
omar omar	172.18.124.21	o Manual 3 Shared Key	Remo
			Edit.
<b>VPN</b> Client	- Prompt for Sec	ret	
Login Nam	ne: oma	r.	OK
VPN Serve	er: 172.	18.124.223	Cancel
Shared Se	cret:		
-			
•			Advanc

2. Nachdem Sie den freigegebenen geheimen Schlüssel eingegeben haben, werden Sie zur Eingabe eines Kennworts und eines Authentifizierungsgeheimnisses aufgefordert. Das Kennwort ist Ihr RADIUS-Kennwort für diesen Benutzer, und der Authentifizierungsgeheimnis ist der geheime PAP-Authentifizierungsschlüssel im [ RADIUS] Abschnitt des <u>VPN</u> <u>Concentrator</u>.

Name	Partner	Login Method	Add
omar	172.18.124.215	Manual	
an omar	172.18.124.223	Shared Key	Remove
			Edit
RADIUS Passwo Authen	Login ord:		OK Cancel
			Advanced

### **Concentrator-Protokolle**

Notice 4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar Debug 4080.15 seconds Sending RADIUS PAP challenge to omar at 172.18.124.108 4087.52 seconds Received RADIUS PAP response from omar at 172.18.124.108, contacting server Notice 4088.8 seconds VPN 0:3 opened for omar from 172.18.124.108. Debug 4088.8 seconds Client's local broadcast address = 172.18.124.255 Notice 4088.8 seconds User assigned IP address 10.1.1.1 Info 4094.49 seconds Command loop started from 10.1.1.1 on PTY2

### **Fehlerbehebung**

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

# Zugehörige Informationen

Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes

- <u>Support-Seite für Cisco VPN 500 Concentrator</u>
- Support-Seite für Cisco VPN 5000-Client
- IPSec-Support-Seite
- Technischer Support Cisco Systems