# Configurazione di un concentratore Cisco VPN 5000 con autenticazione esterna per un server Microsoft Windows 2000 IAS RADIUS

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Cisco VPN 5000 Concentrator Configuration Configurazione di Microsoft Windows 2000 IAS RADIUS Server Verifica del risultato Configurare il client VPN Registri concentratore Risoluzione dei problemi Informazioni correlate

## **Introduzione**

In questo documento vengono descritte le procedure utilizzate per configurare un concentratore Cisco VPN 5000 con autenticazione esterna per un server Microsoft Windows 2000 Internet Authentication Server (IAS) con RADIUS.

**Nota: il protocollo** CHAP (Challenge Handshake Authentication Protocol) non funziona. Utilizzare solo il protocollo PAP (Password Authentication Protocol). Per ulteriori informazioni, fare riferimento all'ID bug Cisco <u>CSCdt96941</u> (solo utenti <u>registrati</u>).

## **Prerequisiti**

#### **Requisiti**

Nessun requisito specifico previsto per questo documento.

#### Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

Cisco VPN 5000 Concentrator Software versione 6.0.16.0001

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

#### **Convenzioni**

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

# **Cisco VPN 5000 Concentrator Configuration**

VPN5001_4B9CBA80				
VPN5001_4B9CBA80> <b>show config</b> Enter Password:				
Edited Configuration not	Present, using Running			
[ General ] EthernetAddress DeviceType ConfiguredOn ConfiguredFrom EnablePassword Password	<pre>= 00:02:4b:9c:ba:80 = VPN 5001 Concentrator = Timeserver not configured = Command Line, from Console = =</pre>			
[ 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	<pre>= "ethernet0" = PAP = "pappassword" = "172.18.124.108" = "radiuspassword" = Off = On</pre>			
[ Logging ] Level Enabled Configuration size is 106	= 7 = On 55 out of 65500 bytes.			
VPN5UU1_4B9CBA80#				

## Configurazione di Microsoft Windows 2000 IAS RADIUS Server

La procedura descritta di seguito consente di eseguire in modo semplificato la configurazione di un server RADIUS Microsoft Windows 2000 IAS.

 Nelle proprietà IAS di Microsoft Windows 2000, selezionare Client e creare un nuovo client.Nell'esempio viene creata una voce denominata VPN5000. L'indirizzo IP di Cisco VPN 5000 Concentrator è 172.18.124.223. Nella casella a discesa Client-Vendor, selezionare Cisco. Il segreto condiviso è il segreto presente nella sezione [ RADIUS ] della configurazione di <u>VPN</u>

	VPN5000 Properties
	Settings
	Friendly name for client:
	VPN5000
	- Client address
	Address (IP or DNS):
	172 18 124 223
	Verify
	Client-Vendor: Cisco
	Client must always send the signature attribute in the request
	Shared secret:
	Confirm shared secret:
	OK Cancel Apply
tor	

2. Nelle proprietà dei criteri di accesso remoto selezionare **Concedi autorizzazione di accesso remoto** nella sezione "Se un utente soddisfa le condizioni" e quindi fare clic su **Modifica** 

Policy name:	Allow acc	ess if dial-in permissio	n is enabled
Specify the con	ditions to match:		
Day-And-Time-	Restrictions match	es "Sun 00:00-24:00,	; Mon 00:00-24
-			
Add	Remove	Edit	
- If a user match			
Grant rem	iote access permis	sion	
C Damage			
U Deny rem	ote access permis	sion	
Access w is override	ill be granted with ten on a per-user l	the profile you specify pasis.	y, unless acce
Stor.			
Edit Profile			

3. Fare clic sulla scheda Autenticazione e verificare che sia selezionata solo l'opzione Autenticazione non crittografata (PAP,

Dial-in Profile		
Dial-in Constraints	IP	Multilink
Authentication	Encryption	Advanced
Check the authentication m	ethods which are allowe	ed for this connecti
Extensible Authenticat	ion Protocol	
Select the EAP type which	h is acceptable for this p	olicy.
MD5-Challenge	į	Configure
a second preservation for the		
Unauthenticated Access-		
Allow remote PPP clies	nts to connect without r thod.	negotiating
Allow remote PPP clie any authentication me	nts to connect without r thod.	negotiating
Allow remote PPP clie any authentication me	nts to connect without r thod.	negotiating

4. Selezionare la scheda Advanced (Avanzate), fare clic su **Add** (Aggiungi), quindi selezionare **Vendor-Specific** (Specifico del fornitore).

Dial-in Constraints		IP Multiink	Order	
Authentication	Enci	yption Advance	d   1	
pecity additional connects	ion attributes	to be returned to the Remote		
CCESS DEIVER.		Add Attributes		
arameters:				
Name	Vendo	To add an attribute to the Pro	file, select the attribut	e and click Add.
		DADUUC and day		
		HADIUS attributes:	1	
		Name	Vendor	Description
		Hepty-Message	RADIUS Standard	Message to be displayed to user when authentical
		Service-Type	RADIUS Standard	Type of service user has requested
		Tunnet-Assignment-ID	RADIUS Standard	I unnel to which a session is to be assigned
		Tunnel-Client-Auth-ID	RADIUS Standard	Name used by the tunnel initiator during the auther
		Tunnel-Lient-Endpt	RADIUS Standard	IP address of the initiator end of the tunnel
		Tunnel-Medium-Type	PADIUS Standard	Parameter and the second
		Tunnel-Password	PADIUS Standard	Password for aumenticating to a remote server
		Tunnel Put Group ID	DADILIC Standard	Group ID for a particular hanneled session
•		Tunnel-Server AuthJD	RADIUS Standard	Name used by the tunnel terminator during the auth
Add Dema	1	Tunnel-Server-Endnt	RADIUS Standard	IP address of the server end of the tunnel
Aug., Tieno	we .	Tunnel-Tune	RADIUS Standard	Tunneling protocols to be used
		Vendor-Specific	RADIUS Standard	Used to support proprietary NAS features
		Cisco-AV-Pair	Cisco	Cisco AV Pair VSA
		USR-ACCM-Type	U.S. Robotics, I	Description not available
		USR-AT-Call-Input-Filter	U.S. Robotics, I	Description not available
		USR-AT-Call-Output-Filter	U.S. Robotics, I	Description not available
		USR-AT-Input-Filter	U.S. Robotics, I	Description not available
	OK	USR-AT-Output-Filter	U.S. Robotics, I	Description not available
		USR-AT-RTMP-Input-Filter	U.S. Robotics, I	Description not available

5. Nella finestra di dialogo Informazioni attributi multivalore relativa all'attributo specifico del fornitore, fare clic su Add per accedere alla finestra di dialogo Informazioni attributi specifici del fornitore. Selezionare Enter Vendor Code (Immetti codice fornitore) e immettere 255 nella casella adiacente. Quindi, selezionare Sì. È conforme e fare clic su Configura attributo.

Aultivalued Attribute Information	? ×	Vendor-Specific Attribut	e Information	<u>?  ×</u>
Attribute name:		Attribute name:		
Vendor-Specific		Vendor-Specific		
Attribute number:		Specify network access se	erver vendor.	
26		C Select from list	<b>FIADIUS Standard</b>	<b>T</b>
Attribute format:		Enter Vendor Code:	255	
OctetString	1			
Attribute values:		Specify whether the attribut vendor specific attributes	te conforms to the RADIUS RFC sp	ecification for
Vendor Value	Move Up	( Yes It conforms		
	Move Down			
	Add	C No. It does not conform	<b>`</b>	
		Configure Attribute		
	Remove			
	Edi			
•	•		OK	Cancel
	OK. Cancel			

6. Nella finestra di dialogo Configure VSA (RFC compliant), immettere **4** per il numero di attributo assegnato dal fornitore, **String** (Stringa) per il formato dell'attributo e **rtp-group** 

(nome del gruppo VPN nel Cisco VPN 5000 Concentrator) per il valore dell'attributo. Fare clic su **OK** e ripetere il passaggio

4	
Attribute format:	
String	
Attribute value:	
rtp-group	

7. Nella finestra di dialogo Configure VSA (RFC compliant), immettere **4** per il numero di attributo assegnato dal fornitore, **String** per il formato dell'attributo e **cisco123** (il segreto condiviso del client) per il valore dell'attributo. Fare clic su

Attribute format: String Attribute value: cisco123	5	
String Attribute value: cisco123	Attribute format:	
Attribute value: cisco123	String	
cisco123	Attribute value:	
	cisco123	

8. L'attributo Specifico del fornitore contiene due valori (gruppo e password

Authentication       Encryption       Advanced         Specify additional connection attributes to be returned to the Remote Access Server.       Parameters:         Parameters:       Vendor       Value         Vendor-Specific       RADIUS Standard       rtp-group, cisco12         Image: Add       Remove       Edit	Dial-in Constrai	nts IP	Multilink
Specify additional connection attributes to be returned to the Remote Access Server.         Parameters:         Name       Vendor         Vendor-Specific       RADIUS Standard         rtp-group, cisco12         Add       Remove         Edit	Authentication	Encryption	Advanced
Name     Vendor     Value       Vendor-Specific     RADIUS Standard     rtp-group, cisco12       Image: standard standard     rtp-group, cisco12       Image: standard standard     Remove     Edit	Specify additional co Access Server. Parameters:	nnection attributes to be retu	rned to the Remote
Vendor-Specific RADIUS Standard rtp-group, cisco12  Add Remove Edit	Name	Vendor	Value
Add Remove Edit	Vendor-Specific	RADIUS Standard	rtp-group, cisco12

9. In Proprietà utente fare clic sulla scheda Connessione remota e verificare che l'opzione Controlla accesso tramite Criteri di accesso remoto sia

	?
General 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</li> </ul>	s Policy
Verify Caller-ID:	
Callback Options	·
No Callback	
C Set by Caller (Routing and Remote Ac	cess Service only)
C Always Callback to:	
🦳 Assign a Static IP Address	1 GC 14 40 1
Assign a Static IP Address	

#### Verifica del risultato

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** <u>strumento Output Interpreter (solo utenti</u> <u>registrati); lo</u> <u>strumento permette di visualizzare un'analisi dell'output del comando</u> **show.** 

- **show radius statistics**: visualizza le statistiche dei pacchetti per la comunicazione tra il concentratore VPN e il server RADIUS predefinito identificato dalla sezione RADIUS.
- show radius config Visualizza le impostazioni correnti per i parametri RADIUS.

Questo è l'output del comando show radius statistics.

VPN5001	_4B9CBA80> <b>show</b>	radius	statistics
RADIUS	Stats		

Accounting	Primary	Secondary
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	Primary	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>

#### Questo è l'output del comando show radius config.

RADIUS		State	UDP	CHAP16	;
Authenticat	ion	On	1812	No	
Accounting		Off	1813	n/a	
Secret		'radiusp	asswoi	rd '	
Server	IP add	lress	Atte	empts	AcctSecret
Primary	172.18	8.124.108	3	5	n/a
Secondary	Off				

## Configurare il client VPN

Questa procedura guida l'utente nella configurazione del client VPN.

 Dalla finestra di dialogo VPN Client, selezionare la scheda Configurazione. Quindi, dalla finestra di dialogo VPN Client-Prompt for Secret, immettere il segreto condiviso nel server VPN. Il segreto condiviso del client VPN è il valore immesso per la password VPN dell'attributo 5 in Concentrator

Name	Partner	Login Method	Add
omar omar	172.18.124.215	Manual Shared Key	Remov
			Edit
VPN Client -	Prompt for Secre	t.	
Login Name	e: omar		OK
VPN Server	: 172.18	3.124.223	Cancel
Shared Sec	rret:		
1. <sup>6</sup>			
•			Advance
	un Dataulturkan Oa	-	

2. Dopo aver immesso il segreto condiviso, vengono richiesti una password e un segreto di autenticazione. La password è la password RADIUS per l'utente e il segreto di autenticazione è il segreto di autenticazione PAP nella sezione [ RADIUS ] di <u>VPN</u> <u>Concentrator</u>.

Name	Partner Login Method	Add
omar	172.18.124.215 Manual	
amar 🚰	172.18.124.223 Shared Key	Remove
		Edit
Passwo	ord:	OK Cancel
( Auto-Conn	ect to Default when Opened	Advanced

### **Registri concentratore**

Notice 4080.11 seconds New IKE connection: [172.18.124.108]:1195:omar 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. 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

### Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

# Informazioni correlate

Cisco VPN serie 5000 concentrator: annuncio di fine vendita

- Pagina di supporto per Cisco VPN 5000 Concentrator
  Pagina di supporto per i client Cisco VPN 5000
- Pagina di supporto per IPSec
- Supporto tecnico Cisco Systems