# Configurando um Cisco VPN 5000 Concentrator com autenticação externa para um servidor RADIUS de IAS do Microsoft Windows 2000.

### Contents

Introduction Prerequisites Requirements Componentes Utilizados Conventions Configuração do concentrador Cisco VPN 5000 Configurar o Microsoft Windows 2000 IAS RADIUS Server Verificar o resultado Configurar o VPN Client Registros do concentrador Troubleshoot Informações Relacionadas

# **Introduction**

Este documento descreve os procedimentos usados para configurar um Cisco VPN 5000 Concentrator com autenticação externa em um Microsoft Windows 2000 Internet Authentication Server (IAS) com RADIUS.

**Observação:** o Challenge Handshake Authentication Protocol (CHAP) não funciona. Use somente o PAP (Password Authentication Protocol Protocolo de Autenticação de Senha). Consulte o bug da Cisco ID <u>CSCdt96941</u> (somente clientes <u>registrados</u>) para obter mais detalhes.

# **Prerequisites**

#### **Requirements**

Não existem requisitos específicos para este documento.

#### **Componentes Utilizados**

As informações aqui são baseadas nesta versão de software:

Software Cisco VPN 5000 Concentrator versão 6.0.16.0001

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

#### **Conventions**

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

### Configuração do concentrador Cisco VPN 5000

<pre>VPN5001_4B9CEA80&gt; show config Enter Password: Edited Configuration not Present, using Running [ General ] EthernetAddress = 00:02:4b:9c:ba:80 DeviceType = VPN 5001 Concentrator ConfiguredOn = Timeserver not configured ConfiguredFrom = Command Line, from Console EnablePassword = Password = [ IP Ethernet 0 ] Mode = Routed SubnetMask = 255.255.255.0 IPAddress = 172.18.124.223 [ IP Ethernet 1 ] Mode = Off [ IKE Policy ] Protection = MD5_DES_G1 [ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0</pre>
Edited Configuration not Present, using Running [ General ] EthernetAddress = 00:02:4b:9c:ba:80 DeviceType = VPN 5001 Concentrator ConfiguredOn = Timeserver not configured ConfiguredFrom = Command Line, from Console EnablePassword = Password = [ IP Ethernet 0 ] Mode = Routed SubnetMask = 255.255.0 IPAddress = 172.18.124.223 [ IP Ethernet 1 ] Mode = Off [ IKE Policy ] Protection = MD5_DES_G1 [ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0
<pre>[ General ] EthernetAddress = 00:02:4b:9c:ba:80 DeviceType = VPN 5001 Concentrator ConfiguredOn = Timeserver not configured ConfiguredFrom = Command Line, from Console EnablePassword = Password = [ IP Ethernet 0 ] Mode = Routed SubnetMask = 255.255.0 IPAddress = 172.18.124.223 [ IP Ethernet 1 ] Mode = Off [ IKE Policy ] Protection = MD5_DES_G1 [ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0</pre>
<pre>[ IP Ethernet 0 ] Mode = Routed SubnetMask = 255.255.0 IPAddress = 172.18.124.223 [ IP Ethernet 1 ] Mode = Off [ IKE Policy ] Protection = MD5_DES_G1 [ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0</pre>
<pre>Mode = OII [ IKE Policy ] Protection = MD5_DES_G1 [ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0</pre>
Protection = MD5_DES_G1 [ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0
<pre>[ VPN Group "rtp-group" ] BindTo = "ethernet0" Transform = esp(md5,des) LocalIPNet = 10.1.1.0/24 MaxConnections = 10 IPNet = 0.0.0.0/0</pre>
<pre>[ RADIUS ] BindTo = "ethernet0" ChallengeType = PAP PAPAuthSecret = "pappassword" PrimAddress = "172.18.124.108" Secret = "radiuspassword" UseChap16 = Off Authentication = On [ Logging ] Level = 7 Erechlad = 07</pre>
Configuration size is 1065 out of 65500 bytes.

### Configurar o Microsoft Windows 2000 IAS RADIUS Server

Estas etapas o guiam por uma configuração simples do servidor Microsoft Windows 2000 IAS RADIUS.

 Nas propriedades IAS do Microsoft Windows 2000, selecione Clients e crie um novo cliente.Neste exemplo, uma entrada chamada VPN5000 é criada. O endereço IP do Cisco VPN 5000 Concentrator é 172.18.124.223. Na caixa suspensa Client-Vendor, selecione Cisco. O segredo compartilhado é o segredo na seção [ RADIUS ] da configuração do <u>VPN</u>

PN5000 Properties				?
Settings				
Friendly name for clien	t			
VPN5000				
- Client address				
Address (IP or DNS	<b>)</b> .			
172 18 124 223	Je			
Verify				
Client-Vendor:	Cisco			•
_	1			
Client must always	send the	signature att	ribute in the requ	est
Shared secret:		******		
Confirm shared secret:		******		
		1		
		ок I	Canaal	Apple
		UN	Cancer	HUDA

- Concentrator.
- 2. Nas propriedades da Política de acesso remoto, selecione **Conceder permissão de acesso remoto** na seção "Se um usuário corresponder às condições" e clique em **Editar**

Policu name:	Allow acc	ess if dial-in permissi	ion is enabled
r olloy hamo.			
Specify the con	ditions to match:	<sup>11</sup> C 00.00 34.0	0
Day-And-Time-	nestrictions match	es Sun 00:00-24:0	U; MON UU:UU-24:
•			
Add	Bemove	Edit	
If a user match	nes the conditions		
<ul> <li>Grant rem</li> </ul>	iote access permis	sion	
C Deny rem	ote access permis	sion	
Access w	ill be granted with	the profile you spec	ify, unless access
is override	den on a per-user l	basis.	
Edit Profile			

3. Clique na guia Authentication (Autenticação) e verifique se Unencrypted Authentication (PAP, SPAP) está

t Dial-in Profile		?
Dial-in Constraints Authentication	IP Encryption	Multilink   Advanced
Check the authentication in Check the authentication in Check the Extensible Authentication in Check the EAP type which	' methods which are allow ation Protocol ch is acceptable for this ;	ed for this connection. policy.
MD5-Challenge		Configure
<ul> <li>Microsoft Encrypted.</li> <li>Encrypted Authentic.</li> <li>Unencrypted Authentic.</li> </ul>	Authentication (MS-CHA ation (CHAP) tication (PAP, SPAP)	PJ
- Unauthenticated Access - Allow remote PPP cli	ents to connect without	negotiating
any authentication m	ethod.	
	ок с	ancel Apply

selecionado.

4. Selecione a guia Avançado, clique em Adicionar e selecione Específico do fornecedor.

Dial-in Constraints	Enn	IP   Multiir	k Order	
Authentication	Encig	ypuon wuvanu	1	
and additional compact	an all the days	to be returned to the Demote		
ccess Server	on annoules	to be returned to the Helliote		
occorron.		Add Attributes		
arameters:		and street a street of the street		
Name	Vendo	To add an attribute to the P	rofile, select the attribut	e and click Add.
		RADIUS attributes		
		Name	Mandar	Description
		Reply Message	PADILIS Standard	Message to be deplayed to user when a therefeat
		Senarce Turne	RADIUS Standard	Tune of service user bac requested
		TunnelAssignment/D	RADIUS Standard	Turnel 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-Endot	BADIUS 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
( )		Tunnel-Pyt-Group-ID	RADIUS Standard	Group ID for a particular tunneled session
and the second second		Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the auth
Add Remo	ve	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	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
		USH-AT-Call-Input-Filter	U.S. Hobotics, I	Description not available
		USH-AT-Call-Output-Filter	U.S. Hobotics, I	Description not available
	OK	USP-AT-Input-Filter	U.S. HODORCS, I	Description not available
		LICO AT DTMD Innut Eiker	U.S. Piccolics, I	Description not available
		ist and the second seco	0.5. h0000cs, I	Description flot available
		-		

5. Na caixa de diálogo Informações de atributo com vários valores para o atributo Específico do fornecedor, clique em Adicionar para ir para a caixa de diálogo Informações de atributo específicas do fornecedor. Selecione Inserir código do fornecedor e digite 255 na caixa adjacente. Em seguida, selecione Sim. Ele está em conformidade e clique em Configurar atributo.

Multivalued Attribu	te Information	? >	Vendor-Specific Attribut	te Information	<u>? ×</u>
Attribute name:			Attribute name:		
Vendor-Specific			Vendor-Specific		
Attribute number:			Specify network access se	erver vendor.	
26			C Select from list	RADIUS Standard	Ŧ
Attribute format:			· Enter Vendor Code:	255	
OctetString					
Attribute values:			Specify whether the attribut vendor specific attributes.	te conforms to the RADIUS RFC sp	pecification for
Vendor	Value	Move Up	Yes It conforms		
		Move Down			
		Add	C No. It does not conform	n.	
			Configure Attribute		
		Hemove			
		Edit			
•		2		OK	Cancel
			-		
	_	OK. Cancel			

6. Na caixa de diálogo Configurar VSA (compatível com RFC), insira **4** para o número de atributo atribuído pelo Fornecedor, digite **String** para o formato do Atributo e digite **rtp-group** 

(nome do grupo VPN no Cisco VPN 5000 Concentrator) para o valor do Atributo. Clique em **OK** e repita a etapa

4		
Attribute format:		
String		
Attribute value:		
rtp-group		

7. Na caixa de diálogo Configurar VSA (compatível com RFC), insira **4** para o número de atributo atribuído pelo fornecedor, digite **String** para o formato Attribute e digite **cisco123** (o segredo compartilhado do cliente) para o valor Attribute. Click

Vendor-assigned attribute number:	
5	
Attribute format:	
String	
Attribute value:	
cisco123	

8. Você vê que o atributo Vendor-Specific contém dois valores (grupo e senha de

Dial-in Constrai	nts 📔 🗌	IP	Multilink
Authentication	Encry	ption	Advanced
Specify additional co Access Server, <sup>D</sup> arameters;	onnection attributes	to be returned	to the Remote
Name	Vendor	V	alue
Vendor-Specific	RADIUS	Standard rt	p-group, cisco12
▲ Add	Remove	J Edit	

9. Em suas propriedades de usuário, clique na guia Discar e verifique se o **acesso de controle por meio da Diretiva de acesso remoto** está

omar Properties	<u>?</u> ×
General Member Of Profile Dial-in	
Remote Access Permission (Dial-in or VPN)	
C Allow access	
C Deny access	
Control access through Remote Access Policy	
Verify Caller-ID:	
Callback Options	
• No Callback	
C Set by Caller (Routing and Remote Access Service on	(y)
C Always Callback to:	
Assign a Static IP Address	
- Apply Statia Paytes	
Define routes to enable for this Dial-in Static Ro	outes

#### Verificar o resultado

Esta seção fornece informações que você pode usar para confirmar se a sua configuração funciona corretamente.

A <u>Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados</u> comandos show, o que permite exibir uma análise da saída do comando show.

- show radius statistics Exibe estatísticas de pacotes para comunicação entre o VPN Concentrator e o servidor RADIUS padrão identificado pela seção RADIUS.
- show radius config Mostra as configurações atuais dos parâmetros RADIUS.

Esta é a saída do 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>

#### Esta é a saída do comando show radius config.

RADIUS		State	UDP	CHAP16	
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				

### **Configurar o VPN Client**

Este procedimento o orienta na configuração do VPN Client.

 Na caixa de diálogo Cliente VPN, selecione a guia Configuração. Em seguida, na caixa de diálogo VPN Client-Prompt for Secret, digite o segredo compartilhado no VPN Server. O segredo compartilhado do VPN Client é o valor inserido para a senha VPN do atributo 5 no VPN

Concentrator.

ime	Partner	Login Method	Add
omar	172.18.124.215	Manual	
omar	172.18.124.223	Shared Key	Hemove
			Edit
Shared Secr	et		
			Advanced.

 Depois de inserir o segredo compartilhado, você será solicitado a fornecer uma senha e um segredo de autenticação. A senha é sua senha RADIUS para esse usuário, e o segredo da autenticação é o segredo da autenticação PAP na seção [ RADIUS] do <u>VPN</u> <u>Concentrator</u>.

rame	Partner	Login Method	Add
omar	172.18.124.215	Manual	
an omar	172.18.124.223	Shared Key	Remove
			Edit
RADIUS	Login		×
Passwo	ord:		ОК
Authen	tication Secret:	]	Cancel
2.0			
			Advanced
			Advanced

#### Registros do concentrador

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 d087.52 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

#### **Troubleshoot**

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

# Informações Relacionadas

Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series

- Página de suporte do Cisco VPN 5000 Concentrator
  Página de suporte do Cisco VPN 5000 Client
- Página de suporte do IPSec
- Suporte Técnico Cisco Systems