Configuración de un Concentrador VPN 5000 de Cisco con autenticación externa en un servidor IAS RADIUS de Microsoft Windows 2000.

## Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configuración del concentrador VPN 5000 de Cisco Configuración del servidor RADIUS IAS de Microsoft Windows 2000 Verificar el resultado Configure el cliente VPN "Registros del concentrador" Troubleshoot Información Relacionada

# **Introducción**

Este documento describe los procedimientos utilizados para configurar un Cisco VPN 5000 Concentrator con autenticación externa a un Microsoft Windows 2000 Internet Authentication Server (IAS) con RADIUS.

**Nota:** El protocolo de autenticación por desafío mutuo (CHAP) no funciona. Utilice solamente el protocolo de autenticación de contraseña (PAP). Consulte Cisco bug ID <u>CSCdt96941</u> (<u>sólo</u> clientes registrados) para obtener más detalles.

### **Prerequisites**

### **Requirements**

No hay requisitos específicos para este documento.

### **Componentes Utilizados**

La información de este documento se basa en esta versión del software:

• Software del concentrador VPN 5000 de Cisco versión 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.

#### **Convenciones**

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

# Configuración del concentrador VPN 5000 de Cisco

VPN5001_4B9CBA80			
VPN5001_4B9CBA80> <b>show con</b> Enter Password:	fig		
Edited Configuration not P	resent, 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>		
<pre>[ RADIUS ] BindTo = ChallengeType = PAPAuthSecret = PrimAddress = Secret = UseChap16 = Authentication = [ Logging ] Level = Enabled =</pre>	"ethernet0" PAP "pappassword" "172.18.124.108" "radiuspassword" Off On 7 On		
Configuration size is 1065 VPN5001_4B9CBA80#	out of 65500 bytes.		

# Configuración del servidor RADIUS IAS de Microsoft Windows 2000

Estos pasos le guiarán a través de una simple configuración del servidor IAS RADIUS de Microsoft Windows 2000.

1. En las propiedades de Microsoft Windows 2000 IAS, seleccione **Clientes** y cree un nuevo cliente.En este ejemplo, se crea una entrada denominada VPN5000. La dirección IP del Cisco VPN 5000 Concentrator es 172.18.124.223. En el cuadro desplegable Cliente-Proveedor, seleccione **Cisco**. El secreto compartido es el secreto en la sección [ RADIUS ] de la configuración del concentrador

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 si	gnature attrib	ute in the requ	iest
Shared secret:		*****		
Sharea seciel.		J		
Confirm shared secret:		*****		
				1
		ОК	Cancel	Appl

2. Bajo las propiedades de la política de acceso remoto, seleccione **Conceder permiso de acceso remoto** en la sección "Si un usuario coincide con las condiciones" y luego haga clic

olicy name:	Allow acce	ess if dial-in p	ermission is	enabled
necifu the conr	litions to match:			
ay-And-Time-F	Restrictions match	es ''Sun 00:0	0-24:00; Mo	n 00:00-24:00
	1			an a
<u>u</u>				
Add	Remove	Edit		
Combood				
Grant rem	ote access permis	sion		
C Deny remo	ote access permis	sion		
	II be granted with	the profile yo	u specify, ur	nless access
Access wi		the second s		

en Editar perfil.

3. Haga clic en la ficha Authentication (Autenticación) y asegúrese de que sólo **esté** seleccionada la autenticación no cifrada (PAP,

Cole D	al-in Profile		
	Dial-in Constraints	IP	Multilink
	Authentication	Encryption	Advanced
Cł	neck the authentication n	nethods which are allowe	d for this connection.
П	Extensible Authentica	ation Protocol	
-	Select the EAP type whic	h is acceptable for this p	olicy.
	MD5-Challenge	j	Configure
I	<ul> <li>Unencrypted Authent</li> </ul>	ication (PAP, SPAP)	
I	Jnauthenticated Access		

4. Seleccione la pestaña Advanced, haga clic en Add y seleccione Vendor-Specific.

Dial-in Constraints		IP Multiink	Order	
Authentication	Enciy	ption Advanced	1    1	
pecify additional connection	on attributes	to be returned to the Remote		
vccess Server.		dd Attributes		
arameters:				
Name	Venda	To add an attribute to the Pro	file, select the attribut	e and click Add
rigino	Terioo			
		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 authen
		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 fo
		Tunnel-Password	RADIUS Standard	Password for authenticating to a remote server
		Tunnel-Preference	RADIUS Standard	Relative preference assigned to each tunnel when
( <u>)</u>		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	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
		Lisco-AV-Pair	Lisco	Cisco AV Pair VSA
		USH-ALLM-Type	U.S. Hobolics, I	Description not available
		USH AT Call Input-Filter	U.S. Hobolics, I	Description not available
		USP AT loave Elba	U.S. HODOBCS, I	Description not available
	OK	USP AT Output Filter	U.S. HODORCS, I	Description not available
		LICD AT DTMD Incut Files	U.S. Hobolics, I	Description not available
	1	USH-AT-INT-INDUC-FILLET	0.3. h0000cs, I	Description hot available
		•		
				Add Class

5. En el cuadro de diálogo Información de atributo multivalor para el atributo específico del proveedor, haga clic en Agregar para ir al cuadro de diálogo Información de atributo específico del proveedor. Seleccione Introducir código del proveedor e introduzca 255 en el cuadro adyacente. A continuación, seleccione Yes (Sí). Se ajusta y hace clic en Configurar atributo.

Aultivalued Attr	ibute Information	<u>?  ×</u>	Vendor-Specific Attribut	te Information	? X
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 sp	ecification for
Vendor	Value	Move Up	( Ves It conforms		
		Move Down	i i conoma.		
		A44	C No. It does not conform	<b>1</b> .	
		All	Configure Attribute		
		Bemove			
		Edit			
-	-1.X. (S. 1.X.)			OK.	Cancel
		OK. Cancel			

6. En el cuadro de diálogo Configurar VSA (compatible con RFC), escriba **4** para el número de atributo asignado por el proveedor, escriba **String** para el formato de atributo e introduzca

**rtp-group** (nombre del grupo de VPN en el concentrador Cisco VPN 5000) para el valor de atributo. Haga clic en **Aceptar** y repita el paso

onfigure ¥SA (RFC compliant)	?
Vendor-assigned attribute number:	
4	
Attribute format:	
String	
Attribute value:	
rtp-group	
	OK Cancel

 En el cuadro de diálogo Configurar VSA (compatible con RFC), escriba 4 para el número de atributo asignado por el proveedor, escriba String para el formato de atributo e introduzca cisco123 (el secreto compartido del cliente) para el valor de atributo. Click

ute format: Ig	
ig No ov	
ute value:	
o123	

8. El atributo Específico del proveedor contiene dos valores (grupo y contraseña de

Dial-in Constrain	ts I IP	) Multilisk
Authentication	Encryption	Advanced
Specify additional cor Access Server. Parameters:	nnection attributes to be re	turned to the Remote
Name	Vendor	Value
•		

9. En las propiedades de usuario, haga clic en la ficha Marcar y asegúrese de que está seleccionado Control access through Remote Access Policy

nar Properties		?
General Member Of Profile Dial-in		
- Remote Access Permission (Dial-in or VPN)-		
C Allow access		
C Deny access		
Control access through Remote Access Po	olicy	
☐ Verify Caller-ID:		
Callback Options		
No Callback		
C Set by Caller (Routing and Remote Access	s Service only)	
C Always Callback to:		
Assign a Static IP Address	(i )i - i	<u> </u>
Apply Static Routes		
Define routes to enable for this Dial-in connection.	Static Routes	
8		

### Verificar el resultado

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

La herramienta <u>Output Interpreter</u> (sólo para clientes registrados) permite utilizar algunos comandos "show" y ver un análisis del resultado de estos comandos.

- **show radius statistics**—Muestra las estadísticas de paquetes para la comunicación entre el VPN Concentrator y el servidor RADIUS predeterminado identificado por la sección RADIUS.
- show radius config: muestra la configuración actual para los parámetros RADIUS.

Este es el resultado 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>

#### Este es el resultado 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				

## Configure el cliente VPN

Este procedimiento le guía a través de la configuración del VPN Client.

 En el cuadro de diálogo VPN Client, seleccione la ficha Configuration. A continuación, en el cuadro de diálogo Solicitud de cliente VPN para secreto, introduzca el secreto compartido en el servidor VPN. El secreto compartido de VPN Client es el valor ingresado para la contraseña VPN del atributo 5 en el VPN Concentrator.

me	Partner	Login Method	Add
omar	172.18.124.21	5 Manual	
omar	172.18.124.22	3 Shared Key	Remove
			E dit
Login Nam	e: oma	ar 10 101 000	ОК
VPN Serve	er: 172	.18.124.223	Cancel
Shared Se	cret:		
			Advanced.
		3	

 Después de introducir el secreto compartido, se le solicitará una contraseña y un secreto de autenticación. La contraseña es su contraseña RADIUS para ese usuario, y el secreto de autenticación es el secreto de autenticación PAP en la sección [ RADIUS] de <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 del 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 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

### **Troubleshoot**

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- Página de soporte del concentrador VPN 5000 de Cisco

- Página de soporte para Cisco VPN 5000 Client
- Página de soporte de IPSec
- Soporte Técnico Cisco Systems