# 外部認証を使用する Cisco VPN 5000 コンセン トレータを Microsoft Windows 2000 IAS RADIUS サーバに設定する方法

### 内容

 概要

 前提条件

 要件

 使用するコンポーネント

 表記法

 Cisco VPN 5000 Concentrator 設定

 Microsoft Windows 2000 IAS RADIUSサーバの設定

 結果の確認

 VPN クライアントの設定

 コンセントレータ ログ

 トラブルシュート

 関連情報

### <u>概要</u>

このドキュメントでは、外部認証を使用する Cisco VPN 5000 コンセントレータを RADIUS を使用する Microsoft Windows 2000 Internet Authentication Server(IAS)に設定する手順について説明します。

**注:チャレンジハンドシ**ェーク認証プロトコル(CHAP)は機能しません。パスワード認証プロトコ ル(PAP)のみを使用します。 詳細については、Cisco Bug ID <u>CSCdt96941</u>(登録<u>ユーザ</u>専用)を参照 してください。

# <u>前提条件</u>

#### <u>要件</u>

このドキュメントに特有の要件はありません。

#### 使用するコンポーネント

このドキュメントの情報は次のソフトウェア バージョンに基づいています。

• Cisco VPN 5000 コンセントレータ ソフトウェア バージョン 6.0.16.0001 このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

### <u>表記法</u>

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

### <u>Cisco VPN 5000 Concentrator 設定</u>

VPN5001_4B9CBA80	
VPN5001_4B9CBA80> <b>show cc</b> Enter Password:	onfig
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	<pre>= Routed = 255.255.255.0 = 172.18.124.223</pre>
[ IP Ethernet 1 ] 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.
VPN5001_4B9CBA80#	

### <u>Microsoft Windows 2000 IAS RADIUSサーバの設定</u>

次の手順に従って、簡単なMicrosoft Windows 2000 IAS RADIUSサーバ設定を行います。

1. Microsoft Windows 2000 IASのプロパティで、[Clients]を選択し、新しいクライアントを作 成します。この例では、VPN5000という名前のエントリが作成されます。Cisco VPN 5000コンセントレータのIPアドレスは172.18.124.223です。[Client-Vendor]ドロップダウン ボックスで、[Cisco]を選択します。共有秘密は、VPNコンセントレータの設定の[RADIUS] ョンにある秘密です。

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

2. リモートアクセスポリシーのプロパティで、[ユーザーが条件に一致する場合]セクションの [リモートアクセス許可の付与]を選択し、[プロファイルの編集]をクリ**ックします**。

w access if dia	al-in permission	is enabled	l Properties	?
ettings   Policy name: Specify the cont	Allow acco ditions to match:	ess if dial-in p	permission is er	nabled
Day-And-Time-f	Restrictions match	es ''Sun 00:0	00-24:00; Mon	00:00-24:00; 1
Add	Remove	Edit		
If a user match Grant rem Deny rem Access w is overrido	nes the conditions ote access permis ote access permis ill be granted with len on a per-user t	sion sion the profile yo pasis,	u specify, unle	ess access
Edit Profile				
		OK	Connel	A sector.

3. 「認証」タブをクリックし、「非暗号化認証(PAP、SPAP)」のみが選択されていることを

onstraints       IP       Multilink         cation       Encryption       Advanced         uthentication methods which are allowed for this connection       ble Authentication Protocol       EAP type which is acceptable for this policy.         EAP type which is acceptable for this policy.       Image       Image       Image         oft Encrypted Authentication version 2 (MS-CHAP v2)       oft Encrypted Authentication (MS-CHAP)       oft Encrypted Authentication (MS-CHAP)         ted Authentication (CHAP)       ted Authentication (PAP, SPAP)       cated Access         emote PPP clients to connect without negotiating hentication method.       Image Ima	dit Dial-in Profile			
Sation       Encryption       Advanced         uthentication methods which are allowed for this connection       Second S	Dial-in Constraints	IP	Mult	ilink
uthentication methods which are allowed for this connectible Authentication Protocol EAP type which is acceptable for this policy. enge Configure oft Encrypted Authentication version 2 (MS-CHAP v2) oft Encrypted Authentication (MS-CHAP) ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Authentication	Encryption	Advar	nced
ble Authentication Protocol EAP type which is acceptable for this policy. enge Configure off Encrypted Authentication version 2 (MS-CHAP v2) off Encrypted Authentication (MS-CHAP) ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Check the authentication	methods which are al	lowed for this conr	nection.
EAP type which is acceptable for this policy.  enge Configure oft Encrypted Authentication version 2 (MS-CHAP v2) oft Encrypted Authentication (MS-CHAP) ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Extensible Authentic	ation Protocol		
enge Configure oft Encrypted Authentication version 2 (MS-CHAP v2) oft Encrypted Authentication (MS-CHAP) ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Select the EAP type whi	ch is acceptable for t	his policy.	
oft Encrypted Authentication version 2 (MS-CHAP v2) oft Encrypted Authentication (MS-CHAP) ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	MD5-Challenge		Configur	e
oft Encrypted Authentication (MS-CHAP) ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Microsoft Encrunted	Authentication versio	n 2 (MS-CHAP v2)	
ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Microsoft Encrupted	Authentication (MS-C	шлр)	
ted Authentication (CHAP) ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Microsoft Encrypted	Addrendeadon (MS-C	(IAC)	
ypted Authentication (PAP, SPAP) cated Access emote PPP clients to connect without negotiating hentication method.	Encrypted Authentic	ation (CHAP)		
cated Access emote PPP clients to connect without negotiating hentication method.	🔽 Unencrypted Auther	itication (PAP, SPAP)		
cated Access emote PPP clients to connect without negotiating hentication method.				
emote PPP clients to connect without negotiating hentication method.	Unauthenticated Acces	8		
hentication method.	Allow comete DDD at	ionto to compact with a	aut pogotisting	
OK Cancel Ar	any authentication m	iethod.	Juc negotiating	
Πκ	Unauthenticated Access Allow remote PPP cl any authentication m	; ients to connect wit iethod.	ho	hout negotiating
014				

4. [Advanced]タブを選択し、[Add]をクリックし、[Vendor-Specific]を選択します。

Diarin Constraints	-	IP   Multin	nk   Order	
Authentication	Enci	yption Muvane	0 1	
nacily additional compact	ing attribution	to be rehand to the Demote		
ccess Server	on annoues	to be retained to the Hellion	2	
	4	Add Attributes		
rameters:		and the second second second second	where the second second second	
lame	Vendo	To add an attribute to the P	rofile, select the attribut	e and click Add.
		RADIUS attributes:		
		Name	Vendor	Description
		Beolu-Message	BADIUS Standard	Message to be displayed to user when authentica
		Service-Tupe	BADIUS 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	BADIUS Standard	Name used by the tunnel initiator during the auther
		Tunnel-Client-Endpt	BADIUS Standard	IP address of the initiator end of the tunnel
		Tunnel-Medium-Tune	RADIUS Standard	Transport medium to use when creating a tunnel f
		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
		Tunnel-Server-Auth-ID	RADIUS Standard	Name used by the tunnel terminator during the au
Add. Berno	Ne	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
		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-Filte	r U.S. Robotics, I	Description not available
		4		,

5. Vendor-Specific属性の[Multivalued Attribute Information]ダイアログボックスで、[Add]をク リックして、[Vendor-Specific Attribute Information]ダイアログボックスに移動します。 [Enter Vendor Code]を選択し、横のボックスに255と入力します。次に、[はい]を選択しま す。一致し、[属性の構成]をクリックします。

Multivalued Attribute	Information	? ×	Vendor-Specific Attribute Informa	ation	<u>? ×</u>
Attribute name:			Attribute name:		
Vendor-Specific			Vendor-Specific		
Attribute number:			Specify network access server vendo	II.	
26			C Select from list RADI	US Standard	Ŧ
Attribute format:			Enter Vendor Code: 255		
OctetString					
Attribute values:			Specify whether the attribute conforms vendor specific attributes.	to the RADIUS RFC sp	ecification for
Vendor	Value	Move Up	Yes It conforms		
		Move Down	C N N I N I N I		
		Add	<ul> <li>No. It does not conform.</li> </ul>		
		Parana	Configure Attribute		
		Demoye			
		Edit			
•	<u> </u>	1		OK _	Cancel
		1			
	OK.	Cancel			

6. [Configure VSA (RFC compliant)]ダイアログボックスで、[Vendor-assigned attribute number]に4と入力し、[Attribute format]にStringと入力し、[Attribute value]にrtpgroup (Cisco VPN 5000コンセントレータのVPNグループののグループの名)とです。 [OK]をクリックし、手順5を繰り返します。

Vendor-assigned attribute number:	
4	
Attribute format:	
String	•
Attribute value:	
rtp-group	

7. [Configure VSA (RFC compliant)]ダイアログボックスで、[Vendor-assigned attribute number]に4と入力し、[Attribute format]にStringと入力し、[Attribute value]にcisco123 (client shared secret)と入力します。[OK] をクリックします。

Configure VSA (RFC compliant)		? ×
Vendor-assigned attribute number:		
5		
Attribute format:		1
String		•
Attribute value:		
cisco123		
3		
	OK Ca	ncel

8. ベンダー固有属性に2つの値(グループとVPNパスワード)が含まれていることがわかりま

Dial-in Constraints	IP	Multilink
Authentication	Encryption	Advanced
Specify additional conn Access Server. Parameters:	ection attributes to be retu	ned to the Remote
Name	Vendor	Value
Vendor-Specific	RADIUS Standard	rtp-group, cisco12
•		
Add Re	move Edit	l,

9. ユーザーのプロパティの下で、[ダイヤルイン]タブをクリックし、[リモート**アクセスポリシ** ーによるアクセスの制御]が選択されていることを確認します。

	?
4)	
s Policy	
cess Service (	only)
1.0	1. B.
1	
	۹) ss Policy cess Service (

#### 結果の確認

このセクションでは、設定が正しく動作していることを確認するために使用できる情報を提供しています。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています(登録ユーザ専用)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- show radius statistics: VPNコンセントレータとRADIUSセクションで識別されるデフォルトの RADIUSサーバ間の通信に関するパケット統計情報を表示します。
- show radius config:RADIUSパラメータの現在の設定を表示します。

次に、show radius statisticsコマンドの出力を示します。

VPN5001\_4B9CBA80>**show 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>

#### 次に、show radius configコマンドの出力を示します。

RADIUS	State	UDP	CHAP16
Authentication	On	1812	No
Accounting	Off	1813	n/a
Secret	'radiusp	asswor	rd '

Server IP address Attempts AcctSecret Primary 172.18.124.108 5 n/a Secondary Off

# <u>VPN クライアントの設定</u>

この手順では、VPN Clientの設定について説明します。

1. [VPN Client]ダイアログボックスで、[Configuration]タブを選択します。次に、[VPN Client-Prompt for Secret]ダイアログボックスで、VPN Serverの下に共有秘密を入力します。VPN Clientの共有秘密は、VPNコンセントレータで属性5のVPNパスワードに入力した値です。

ame	Partner	Login Method	Add
omar omar	172.18.124.215	Manual Shared Key	Remove
			Edit
VPN Client -	Prompt for Secr	et	
Login Name	: omar		ОК
VPN Server	: 172.1	8.124.223	Cancel
Shared Sec	ret:		
		24 A.M.	21 - 1998 - 194
			Advanced

2. 共有秘密を入力すると、パスワードと認証秘密の入力を求められます。パスワードはそのユ ーザのRADIUSパスワードで、認証シークレットはVPNコンセントレータの[RADIUS]セクシ ョンにあるPAP認証シークレット<u>です</u>。

8.124.215 Manu 8.124.223 Share	ial ed Key	Remove
8.124.223 Share	ed Key	Remove
		Edit
		X
		ОК
pret:		Cancel
	in the	
		Advanced
ult when Opened		
c	cret:	cret:

# <u>コンセントレータ ログ</u>

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

<u>トラブルシュート</u>

現在、この設定に関する特定のトラブルシューティング情報はありません。

# 関連情報

- <u>Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ</u>
- <u>Cisco VPN 5000 コンセントレータに関するサポートページ</u>

- ・<u>Cisco VPN 5000 クライアントに関するサポート ページ</u> ・<u>IPSec に関するサポート ページ</u>
- ・<u>テクニカルサポート Cisco Systems</u>