Microsoft Windows 2000 IAS RADIUS 서버에 대 한 외부 인증을 사용하여 Cisco VPN 5000 Concentrator 구성

목차

소개 <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>표기 규칙</u> <u>Cisco VPN 5000 Concentrator 컨피그레이션</u> <u>Microsoft Windows 2000 IAS RADIUS 서버 구성</u> <u>결과 확인</u> <u>VPN 클라이언트 구성</u> <u>Concentrator 로그</u> 문제 해결 관련 정보

<u>소개</u>

이 문서에서는 RADIUS를 사용하는 Microsoft Windows 2000 IAS(Internet Authentication Server)에 대한 외부 인증을 사용하여 Cisco VPN 5000 Concentrator를 구성하는 데 사용되는 절차에 대해 설 명합니다.

참고: CHAP(Challenge Handshake Authentication Protocol)가 작동하지 않습니다. PAP(Password Authentication Protocol)만 사용합니다. 자세한 내용은 Cisco 버그 ID <u>CSCdt96941(등록된</u> 고객만 해당)을 참조하십시오.

<u>사전 요구 사항</u>

<u>요구 사항</u>

이 문서에 대한 특정 요건이 없습니다.

<u>사용되는 구성 요소</u>

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

• Cisco VPN 5000 Concentrator Software 버전 6.0.16.0001 이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

<u>표기 규칙</u>

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 표기 규칙</u>을 참조하십시오.

<u>Cisco VPN 5000 Concentrator 컨피그레이션</u>

VPN5001_4B9CBA80			
VPN5001_4B9CBA80> show con Enter Password:	Eig		
Edited Configuration not Pr	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 =	Routed 255.255.255.0 172.18.124.223		
[IP Ethernet I] Mode =	Off		
[IKE Policy] Protection =	MD5_DES_G1		
<pre>[VPN Group "rtp-group"] BindTo = Transform = LocalIPNet = MaxConnections = IPNet =</pre>	<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		
Configuration size is 1065 VPN5001_4B9CBA80#	out of 65500 bytes.		

<u>Microsoft Windows 2000 IAS RADIUS 서버 구성</u>

- 이 단계는 간단한 Microsoft Windows 2000 IAS RADIUS 서버 구성을 안내합니다.
 - 1. Microsoft Windows 2000 IAS 속성에서 **Clients를** 선택하고 새 클라이언트를 만듭니다.이 예에 서는 VPN5000이라는 항목이 생성됩니다. Cisco VPN 5000 Concentrator의 IP 주소는 172.18.124.223입니다. Client-Vendor 드롭다운 상자에서 **Cisco를** 선택합니다. 공유 비밀은 <u>VPN Concentrator</u> 컨피그레이션의 [RADIUS] 섹션에 있는 암호입니다

VPN5000 Properties		<u>'</u> ×
Settings		
Friendly name for client:		
VPN5000		
Client address		
172.18.124.223		
Verify		
Client-Vendor: Cisco	•]
Client must always send the s	signature attribute in the request	
Shared secret:	******	
Confirm shared secret:	******	1
	OK Cancel Apply	

2. Remote Access Policy(원격 액세스 정책)의 속성 아래에서 "If a user matches the conditions(사용자가 조건과 일치할 경우)" 섹션 아래에서 **Grant remote access permission(원 격 액세스 권한 부여)**을 선택한 다음 Edit Profile(프로필 수정)을 클릭합니다

ow access if dia	l-in permission	is enabled	Properties	?>
Settings				
Policy name: Specify the cond	Allow acce itions to match: estrictions match	ess if dial-in p	ermission is en 0-24:00: Mon I	abled
		7 Ja	-1	Þ
Add	Remove	E.dit		
If a user match Grant remo Deny remo	es the conditions Ite access permis Ite access permis	sion sion		
Access wi	I be granted with	the profile yo	u specify, unle	ss access
Edit Profile				
		ок	Cancel	Apply

3. Authentication(인증) 탭을 클릭하고 Unencrypted Authentication(암호화되지 않은 **인증)(PAP,** SPAP)만 선택되었는지 확인합니다

Dial-in Profile		
Dial-in Constraints	IP IP	Multilink
Authentication	Encryption	Advanced
Check the authentication	methods which are allow	ed for this connection.
Extensible Authentic	ation Protocol	
Select the EAP type whi	ch is acceptable for this r	policy.
MD5-Challenge		Configure
Treeschenenge	9	
Microsoft Encrypted	Authentication version 2	(MS-CHAP v2)
Microsoft Encrypted	Authentication (MS-CHA	P)
	ation (CHAP)	
	vication (PAP_SPAP)	
I Onencippied Addrei	incation (FAF, 5FAF)	
11 (11) (1 (1 (1 1))		
Unauthenticated Acces	S	
Allow remote PPP cl any authentication m	ients to connect without r nethod.	negotiating
		annel Acelu

4. Advanced(고급) 탭을 선택하고 Add(**추가**)를 클릭하고 Vendor**-Specific(벤더별)을 선택합니다**

.

Authentication	Enco	rtion Advanc	ed U .	
Authentication	Enci	Abaou		
necilu additional connect	ion attributes	to be rehand to the Bernot		
coess Server	our dimession	to be retained to the rienton	·	
	1	dd Attributes		
arameters:		a state of the second sec		
Name	Vendo	To add an attribute to the P	hofile, select the attribut	e and click Add.
		RADIUS attributes:		
		Name	Vendor	Description
		Benki-Message	BADILIS Standard	Message to be displayed to user when authentical
		Service-Tupe	RADIUS Standard	Tune 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 typnel 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 fr
		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 aut
Add. Remo	we	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
	01	USR AT Input Filter	U.S. Robotics, I	Description not available
	UK	USR-AT-Output-Filter	U.S. Robotics, I	Description not available
	-	USR-AT-RTMP-Input-Filte	r U.S. Robotics, I	Description not available
		•		,

5. 공급업체별 특성에 대한 다중값 속성 정보 대화 상자에서 추가를 클릭하여 판매업체별 특성 정보 대화 상자로 이동합니다. Enter Vendor Code(공급업체 코드 입력)를 선택하고 인접한 상 자에 255를 입력합니다. 그런 다음 예를 선택합니다. 이를 준수하고 특성 구성을 클릭합니다

Multivalued Attribute Information	? X	Vendor-Specific Attribut	e Information	? X
Attribute name:		Attribute name:		
Vendor-Specific		Vendor-Specific		
Attribute number:		Specify network access se	rver vendor.	
26		C Select from list	RADIUS Standard	7
Attribute format:		Enter Vendor Code:	255	
OctetString				
Attribute values:		Specify whether the attribute	te conforms to the RADIUS RFC spe	scification for
Vendor Value	Move Up	Yes It conforms		
	Move Down	-		
	bhd	No. It does not conform	L	
		Configure Attribute		
	Bemoye			
	Edit			
I	Ŀ		OK	Cancel
	1			
OK.	Cancel			

6. Configure VSA (RFC compliant)(VSA(RFC 호환) 구성) 대화 상자에서 Vendor-assigned attribute number에 4를 입력하고 Attribute 형식에 대한 String을 입력하고 Attribute 값에 대해 rtp-group(Cisco VPN 5000 Concentrator에 있는 VPN 그룹의 이름)을 입력합니다. 확인을 클

릭하고 5단계를 반복합니다

	? ×
	•
OK	Cancel
	OK

7. Configure VSA (RFC compliant)(VSA(RFC 호환) 구성) 대화 상자에서 판매업체 지정 특성 번 호에 4를 입력하고 Attribute(특성) 형식에 **String**(문자열)을 입력하고 Attribute 값에 대해 cisco123(클라이언트 공유 암호)을 입력합니다. 확인을 클릭합니다

onfigure VSA (RFC compliant)			? ×
Vendor-assigned attribute number:			
5			
Attribute format:			
String			•
Attribute value:			
cisco123			
	OK	Car	icel
		Years.	10

8. Vendor-Specific 속성에는 두 개의 값(그룹 및 VPN 비밀번호)이 포함되어 있습니다

Dial-in Constraints	Í IP	Multilink
Authentication	Encryption	Advanced
Specify additional connecti Access Server. 'arameters:	on attributes to be returr	ned to the Remote
Name	Vendor	Value
vendor-specific	navius standard	rtp-group, cisco i 23
Add Remor	ve Edit	F

9. 사용자 속성에서 전화 접속 탭을 클릭하고 원격 액세스 정책을 통한 제어 액세스가 선택되었

nar 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	s Policy
Verify Caller-ID:	
Callback Options	
No Callback	
C Set by Caller (Routing and Remote Acc	cess Service only)
Always Callback to:	
C Assign a Static IP Address	
Apply Static Routes	, <u> </u>
Define routes to enable for this Dial-in	Static Routes

<u>결과 확인</u>

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 show 명령은 <u>출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면</u> show 명 령 출력의 분석 결과를 볼 수 있습니다.

• show radius statistics - RADIUS 섹션에서 식별된 VPN Concentrator와 기본 RADIUS 서버 간 의 통신에 대한 패킷 통계를 표시합니다.

• show radius config - RADIUS 매개변수에 대한 현재 설정을 표시합니다.

show radius statistics 명령의 출력입니다.

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

Primary	Secondary
3	na
3	na
0	na
	Primary 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0

VPN5001_4B9CBA80>

show radius config 명령의 출력입니다.

RADIUS		State	UDP	CHAP1	б
Authentica	tion	On	1812	No	
Accounting		Off	1813	n/a	
Secret		'radius	passwo	ord'	
Server	IP ad	dress	Att	empts	AcctSecret
Primary	172.1	8.124.10	8	5	n/a
Secondary	Off				

VPN 클라이언트 구성

이 절차에서는 VPN 클라이언트의 컨피그레이션을 안내합니다.

1. VPN Client 대화 상자에서 Configuration 탭을 선택합니다. 그런 다음 VPN Client-Prompt for Secret 대화 상자에서 VPN Server 아래에 공유 암호를 입력합니다. VPN Client 공유 비밀은 VPN Concentrator에서 특성 5의 VPN 비밀번호에 입력한 값입니다

lame	Partner	Login Method	Add
omar omar	172.18.124.215	Manual Shared Key	Remove
			Edit
VPN Client -	Prompt for Secre	t.	
Login Name	: omar		ОК
VPN Server	: 172.18	3.124.223	Cancel
Shared Sec	ret: 📗		
-			
			Advanced
	ta Default when Oe	and the second se	

2. 공유 암호를 입력하면 암호 및 인증 암호를 입력하라는 메시지가 표시됩니다. 비밀번호는 해 당 사용자의 RADIUS 비밀번호이며 인증 비밀은 <u>VPN Concentrator</u>의 [RADIUS] 섹션에 있는 PAP 인증<u>비밀번호입니다</u>

Name	Partner	Login Method	Add
omar ¹¹ omar	172.18.124.215 172.18.124.223	Manual Shared Key	Remove
000 1977			Edit
RADIUS	Login		×
Passwo	ord:		ОК
Authen	itication Secret:		Cancel
1			
		ig all the	Advanced
			Advanced

<u>Concentrator 로그</u>

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
Debug	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

<u>문제 해결</u>

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

<u>관련 정보</u>

- <u>Cisco VPN 5000 Series Concentrator 판매 중단 발표</u>
- <u>Cisco VPN 5000 Concentrator 지원 페이지</u>

- <u>Cisco VPN 5000 클라이언트 지원 페이지</u> <u>IPSec 지원 페이지</u>
- Technical Support Cisco Systems