VPN 3000 제품과 함께 RADIUS 서버 사용

목차

소개

이 문서에서는 VPN 3000 Concentrator 및 VPN 클라이언트에서 일부 RADIUS 서버를 사용할 때 발견되는 특정 주의 사항에 대해 설명합니다.

- Windows 2000 RADIUS 서버에는 Cisco VPN 클라이언트 인증을 위한 PAP(Password Authentication Protocol)가 필요합니다.(IPSec 클라이언트)
- MSCHAP(Microsoft Challenge Handshake Authentication Protocol)를 지원하지 않는 RADIUS 서버를 사용하려면 VPN 3000 Concentrator에서 MSCHAP 옵션을 비활성화해야 합니다 .(PPTP(Point-to-Point Tunneling Protocol) 클라이언트)
- PPTP와 함께 암호화를 사용하려면 RADIUS의 반환 특성 MSCHAP-MPPE-Keys가 필요합니다 (PPTP 클라이언트).
- Windows 2003에서는 MS-CHAP v2를 사용할 수 있지만 인증 방법은 "RADIUS with Expiry"로 설정해야 합니다.

이러한 참고 사항 중 일부는 제품 릴리스 노트에 나와 있습니다.

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco VPN 3000 Concentrator
- Cisco VPN 클라이언트

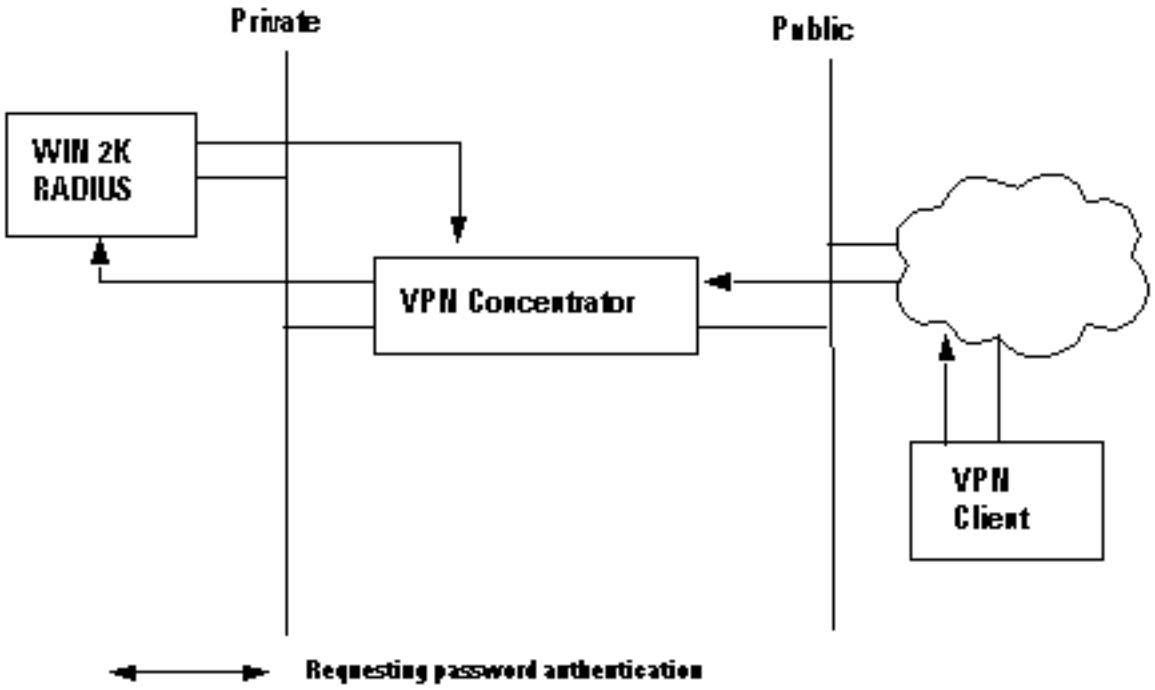
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Windows 2000 RADIUS 서버를 사용하여 Cisco VPN 클라이언트 인증

Windows 2000 RADIUS 서버를 사용하여 VPN 클라이언트 사용자를 인증할 수 있습니다.다음 시나리오(VPN 클라이언트가 인증을 요청하고 있음)에서 VPN 3000 Concentrator는 클라이언트 사용자의 사용자 이름 및 비밀번호를 포함하는 VPN 클라이언트로부터 요청을 받습니다.확인을 위해 개인 네트워크의 Windows 2000 RADIUS 서버에 사용자 이름/비밀번호를 보내기 전에 VPN Concentrator는 HMAC/MD5 알고리즘을 사용하여 이를 해시합니다.

Windows 2000 RADIUS 서버에는 VPN 클라이언트 세션을 인증하기 위한 PAP가 필요합니다 .RADIUS 서버가 VPN 클라이언트 사용자를 인증하도록 하려면 **Edit Dial-in Profile(다이얼인 프로필 수정)** 창에서 **Unencrypted Authentication (PAP, SPAP)** 매개변수를 선택합니다(기본적으로 이 매개변수는 선택되지 않음). 이 매개 변수를 설정하려면 사용 중인 **원격 액세스 정책**을 선택하고 **속성**을 선택한 다음 **인증** 탭을 선택합니다.

이 매개 변수 이름의 *Unencrypted* 단어는 잘못된 것입니다.VPN Concentrator가 인증 패킷을 RADIUS 서버로 전송할 때 암호화되지 않은 상태로 비밀번호를 전송하지 않으므로 이 매개변수를 사용해도 보안이 침해되지 *않습니다*.VPN Concentrator는 VPN 클라이언트에서 사용자 이름/비밀번호 및 암호화된 패킷을 수신하고 인증 패킷을 서버로 전송하기 전에 비밀번호에 대해 HMAC/MD5 해시를 수행합니다.



MSCHAP를 지원하지 않는 RADIUS 서버 사용

일부 RADIUS 서버는 MSCHAPv1 또는 MSCHAPv2 사용자 인증을 지원하지 않습니다 .MSCHAP(v1 또는 v2)를 지원하지 않는 RADIUS 서버를 사용하는 경우 PAP 및/또는 CHAP를 사용하도록 기본 그룹의 PPTP 인증 프로토콜을 구성하고 MSCHAP 옵션을 비활성화해야 합니다 .MSCHAP를 지원하지 않는 RADIUS 서버의 예로는 Livingston v1.61 RADIUS 서버 또는 Livingston 코드를 기반으로 하는 RADIUS 서버가 있습니다.

참고: MSCHAP가 없으면 PPTP 클라이언트에서 보내고 받는 패킷은 암호화되지 않습니다.

PPTP에서 암호화 사용

PPTP에서 암호화를 사용하려면 RADIUS 서버가 MSCHAP 인증을 지원해야 하며 모든 사용자 인증에 대한 반환 특성 MSCHAP-MPPE-Keys를 전송해야 합니다.이 특성을 지원하는 RADIUS 서버의 예는 다음과 같습니다.

- Cisco Secure ACS for Windows - 버전 2.6 이상
- 펑크 소프트웨어 스틸 벨트드 RADIUS
- NT 4.0 서버 옵션 팩의 Microsoft Internet Authentication Server
- Microsoft Commercial Internet System(MCIS 2.0)
- Microsoft Windows 2000 Server — 인터넷 인증 서버

관련 정보

- RADIUS 지원 페이지
- Cisco Secure ACS for Windows 지원 페이지
- Cisco VPN 3000 Series Concentrator 지원 페이지
- Cisco VPN 3000 Series 클라이언트 지원 페이지
- IPSec 지원 페이지
- PPTP 지원 페이지
- RFC 2637:PPTP(Point-to-Point Tunneling Protocol)
- RFC(Request for Comments)
- Technical Support - Cisco Systems