RADIUS-servers met VPN 3000-producten gebruiken

Inhoud

Inleiding

Dit document beschrijft bepaalde voorbehouden die gevonden worden bij het gebruik van bepaalde RADIUS-servers met de VPN 3000 Concentrator en VPN-clients.

- Windows 2000 RADIUS-server vereist Wachtwoordverificatie Protocol (PAP) voor verificatie van een Cisco VPN-client. (IPsec-klanten)
- Gebruik van een RADIUS-server die Microsoft Challenge Handshake Authentication Protocol (MSCHAP) niet ondersteunt, vereist dat de MSCHAP-opties worden uitgeschakeld aan de VPN 3000 Concentrator. (Point-to-Point Tunneling Protocol [PPTP]-clients)
- Het gebruik van encryptie met PPTP vereist de terugkeereigenschap MSCHAP-MPPE-Keys van RADIUS. (PPTP cliënten)
- Met Windows 2003 kan MS-CHAP v2 worden gebruikt, maar de authenticatiemethode moet worden ingesteld als "RADIUS met verloop van tijd".

Een aantal van deze opmerkingen zijn opgenomen in de opmerkingen over het product.

Voordat u begint

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VPN 3000 Concentrator
- Cisco VPN-client

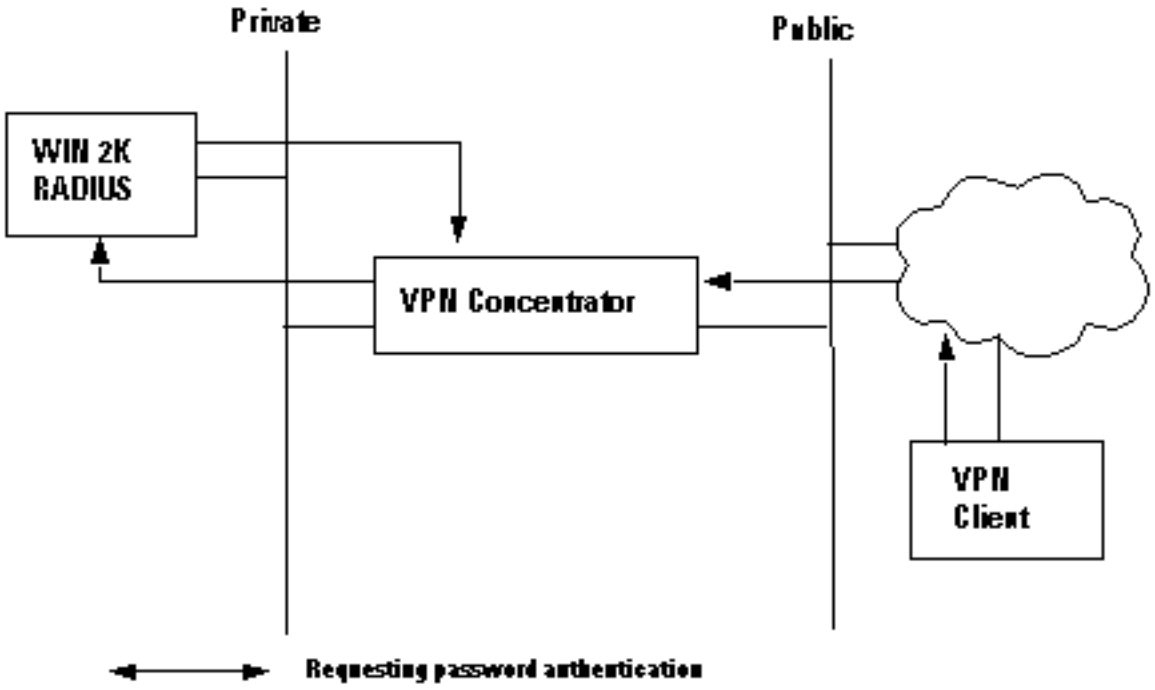
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Gebruik van een Windows 2000 RADIUS-server om een Cisco VPN-client voor verificatie te zorgen

U kunt een Windows 2000 RADIUS-server gebruiken om een VPN-clientgebruiker te authentiseren. In het volgende scenario (de VPN-client vraagt om verificatie) ontvangt de VPN 3000 Concentrator een verzoek van de VPN-client met daarin de gebruikersnaam en het wachtwoord van de client. Alvorens de gebruikersnaam/het wachtwoord naar een Windows 2000 RADIUS-server in het privénetwerk te verzenden ter verificatie, slaat de VPN-Concentrator het wachtwoord op met behulp van het HMAC/MD5-algoritme.

De Windows 2000 RADIUS-server heeft PAP nodig voor het authenticeren van een VPN-clientsessie. Om de RADIUS-server in staat te stellen om een VPN-clientgebruiker voor authentiek te verklaren, controleert u de parameter **Niet-versleutelde verificatie (PAP, SPAP)** in het venster **Dial-in-profiel bewerken** (standaard wordt deze parameter niet ingeschakeld). Om deze parameter in te stellen, selecteert u het **Remote Access Policy** dat u gebruikt, selecteert u **Eigenschappen** en selecteert u het tabblad **Verificatie**.

Let op dat het woord *Unencryptie* op de naam van deze parameter misleidend is. Deze parameter veroorzaakt *geen* schending van de veiligheid, omdat wanneer de VPN Concentrator het authenticatiepakket naar de RADIUS-server stuurt het wachtwoord niet in het duidelijke versturen. De VPN Concentrator ontvangt de gebruikersnaam/het wachtwoord en versleutelde pakketten van de VPN-client en voert een HMAC/MD5-hash op het wachtwoord uit voordat u het verificatiepakket naar de server stuurt.



Een RADIUS-server gebruiken die MSCHAP niet ondersteunt

Sommige RADIUS-servers ondersteunen MSCHAPv1 of MSCHAPv2-gebruikersverificatie niet. Als u een RADIUS-server gebruikt die MSCHAP (v1 of v2) niet ondersteunt, moet u het PPTP-verificatieprotocol van de Base Group configureren om PAP en/of CHAP te gebruiken en ook de MSCHAP-opties uitschakelen. Voorbeelden van RADIUS-servers die MSCHAP niet ondersteunen zijn de Livingston v1.61 RADIUS-server of een RADIUS-server die is gebaseerd op Livingston-code.

N.B.: Zonder MSCHAP zullen pakketten naar en van PPTP-clients *niet* worden versleuteld.

Encryptie met PPTP gebruiken

Om encryptie met PPTP te gebruiken, moet een RADIUS-server MSCHAP-verificatie ondersteunen en de return attribuut MSCHAP-MPPE-Keys voor elke gebruikersverificatie verzenden. Voorbeelden van RADIUS-servers die deze eigenschap ondersteunen worden hieronder weergegeven.

- Cisco Secure ACS voor Windows - versie 2.6 of hoger
- Funk Software Steel-Belted RADIUS
- Microsoft Internet-verificatieserver voor NT 4.0-serveropties - pack
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server — Internet-verificatieserver

Gerelateerde informatie

- RADIUS-ondersteuningspagina
- Cisco Secure ACS voor Windows-ondersteuningspagina
- Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina
- Cisco VPN 3000 Series clientondersteuningspagina

- IPsec-ondersteuningspagina
- PPTP-ondersteuningspagina
- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning - Cisco-systemen