Verwendung von RADIUS-Servern mit VPN 300-Produkten

Inhalt

Einführung

In diesem Dokument werden einige Probleme beschrieben, die bei der Verwendung einiger RADIUS-Server mit dem VPN 3000 Concentrator und VPN-Clients auftreten können.

- Der Windows 2000 RADIUS-Server benötigt für die Authentifizierung eines Cisco VPN-Clients das Password Authentication Protocol (PAP). (IPSec-Clients)
- Bei Verwendung eines RADIUS-Servers, der das MSCHAP (Microsoft Challenge Handshake Authentication Protocol) nicht unterstützt, müssen die MSCHAP-Optionen im VPN 3000-Concentrator deaktiviert werden. (Point-to-Point Tunneling Protocol [PPTP]-Clients)
- Für die Verwendung der Verschlüsselung mit PPTP ist das Rückgabeattribut MSCHAP-MPPE-Keys von RADIUS erforderlich. (PPTP-Clients)
- In Windows 2003 kann MS-CHAP v2 verwendet werden, die Authentifizierungsmethode sollte jedoch auf "RADIUS with Expiry" festgelegt werden.

Einige dieser Notizen sind in Produktversionsnotizen aufgeführt.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN 3000 Concentrator
- Cisco VPN-Client

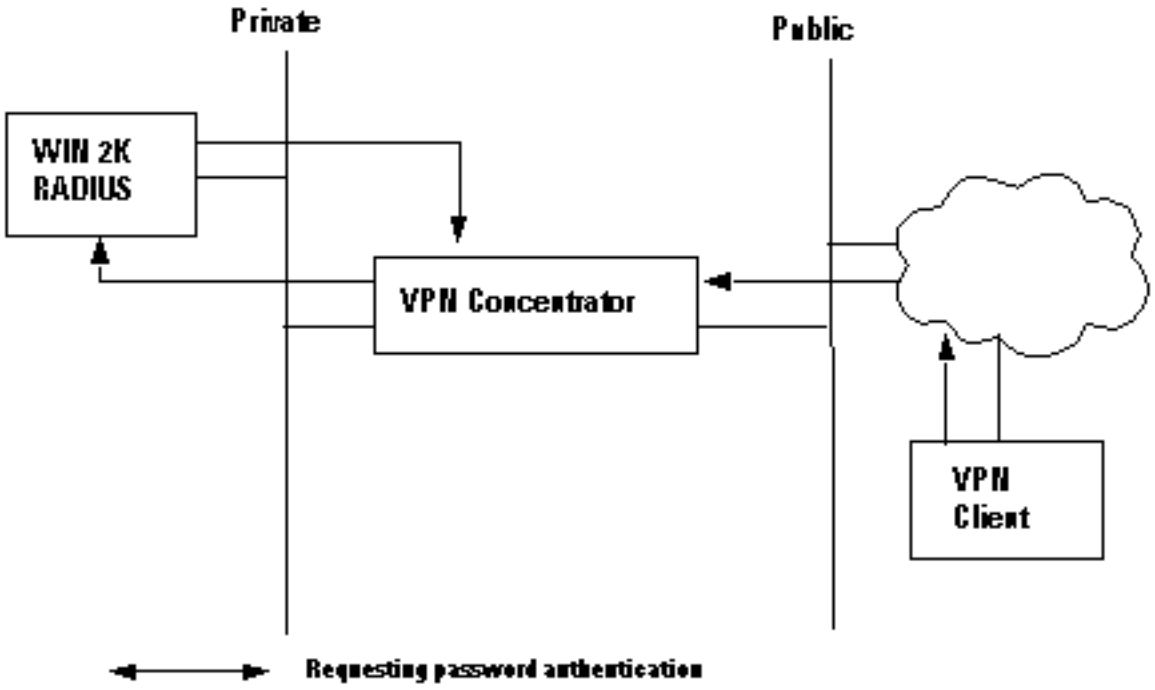
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Verwenden eines Windows 2000 RADIUS-Servers zum Authentifizieren eines Cisco VPN-Clients

Sie können einen VPN-Client-Benutzer mithilfe eines RADIUS-Servers in Windows 2000 authentifizieren. Im folgenden Szenario (der VPN-Client fordert eine Authentifizierung an) erhält der VPN 3000 Concentrator eine Anfrage vom VPN-Client, die den Benutzernamen und das Kennwort des Client-Benutzers enthält. Bevor der Benutzername/das Kennwort zur Überprüfung an einen RADIUS-Server von Windows 2000 im privaten Netzwerk gesendet wird, wird dieser vom VPN Concentrator mithilfe des HMAC/MD5-Algorithmus gehackt.

Der Windows 2000 RADIUS-Server benötigt PAP für die Authentifizierung einer VPN-Client-Sitzung. Damit der RADIUS-Server einen VPN-Client-Benutzer authentifizieren kann, aktivieren Sie im Fenster **Edit Dial-in Profile (Einwahlprofil bearbeiten**) den Parameter **Uncrypted Authentication (PAP, SPAP)** (**Unverschlüsselte Authentifizierung** (standardmäßig ist dieser Parameter nicht aktiviert). Um diesen Parameter festzulegen, wählen Sie die von Ihnen verwendete **Remote-Zugriffsrichtlinie aus**, wählen Sie **Eigenschaften aus**, und wählen Sie die Registerkarte **Authentifizierung aus**.

Beachten Sie, dass das Wort *Uncrypted* auf dem Namen dieses Parameters irreführend ist. Die Verwendung dieses Parameters führt *nicht* zu einer Sicherheitsverletzung, da der VPN Concentrator das Authentifizierungspaket an den RADIUS-Server sendet, das Kennwort nicht in clear sendet. Der VPN Concentrator empfängt Benutzername/Kennwort und verschlüsselte Pakete vom VPN-Client und führt einen HMAC/MD5-Hash für das Kennwort durch, bevor das Authentifizierungspaket an den Server gesendet wird.



Verwenden eines RADIUS-Servers, der MSCHAP nicht unterstützt

Einige RADIUS-Server unterstützen die MSCHAPv1- oder MSCHAPv2-Benutzerauthentifizierung nicht. Wenn Sie einen RADIUS-Server verwenden, der MSCHAP (v1 oder v2) nicht unterstützt, müssen Sie das PPTP-Authentifizierungsprotokoll der Basisgruppe so konfigurieren, dass es PAP und/oder CHAP verwendet und die MSCHAP-Optionen deaktiviert. Beispiele für RADIUS-Server, die MSCHAP nicht unterstützen, sind der Livingston v1.61 RADIUS-Server oder ein RADIUS-Server, der auf Livingston-Code basiert.

Hinweis: Ohne MSCHAP werden Pakete zu und von PPTP-Clients *nicht* verschlüsselt.

Verwenden der Verschlüsselung mit PPTP

Um die Verschlüsselung mit PPTP zu verwenden, muss ein RADIUS-Server die MSCHAP-Authentifizierung unterstützen und das Rückgabedatum MSCHAP-MPPE-Keys für jede Benutzerauthentifizierung senden. Nachfolgend sind Beispiele für RADIUS-Server aufgeführt, die dieses Attribut unterstützen.

- Cisco Secure ACS für Windows - Version 2.6 oder höher
- Funk Software Steel-Belted RADIUS
- Microsoft Internet Authentication Server für NT 4.0 Server Options Pack
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server - Internet-Authentifizierungsserver

Zugehörige Informationen

- RADIUS-Support-Seite
- Support-Seite für Cisco Secure ACS für Windows

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- Cisco VPN Client Support-Seite der Serie 3000
- IPSec-Support-Seite
- PPTP-Support-Seite
- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
- Anforderungen für Kommentare (RFCs)
- Technischer Support - Cisco Systems