Uso di server RADIUS con prodotti VPN 3000

Sommario

Introduzione

In questo documento vengono descritte alcune avvertenze rilevate durante l'utilizzo di alcuni server RADIUS con il concentratore VPN 3000 e i client VPN.

- Per autenticare un client VPN Cisco, il server RADIUS Windows 2000 richiede il protocollo PAP (Password Authentication Protocol). (client IPSec)
- Se si utilizza un server RADIUS che non supporta MSCHAP (Microsoft Challenge Handshake Authentication Protocol), è necessario che le opzioni MSCHAP siano disabilitate in VPN 3000 Concentrator. (client Point-to-Point Tunneling Protocol [PPTP])
- L'utilizzo della crittografia con PPTP richiede l'attributo restituito MSCHAP-MPPE-Keys da RADIUS (client PPTP).
- Con Windows 2003 è possibile utilizzare MS-CHAP v2, ma il metodo di autenticazione deve essere impostato su "RADIUS con scadenza".

Alcune di queste note sono state inserite nelle note di rilascio del prodotto.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco VPN 3000 Concentrator
- Cisco VPN Client

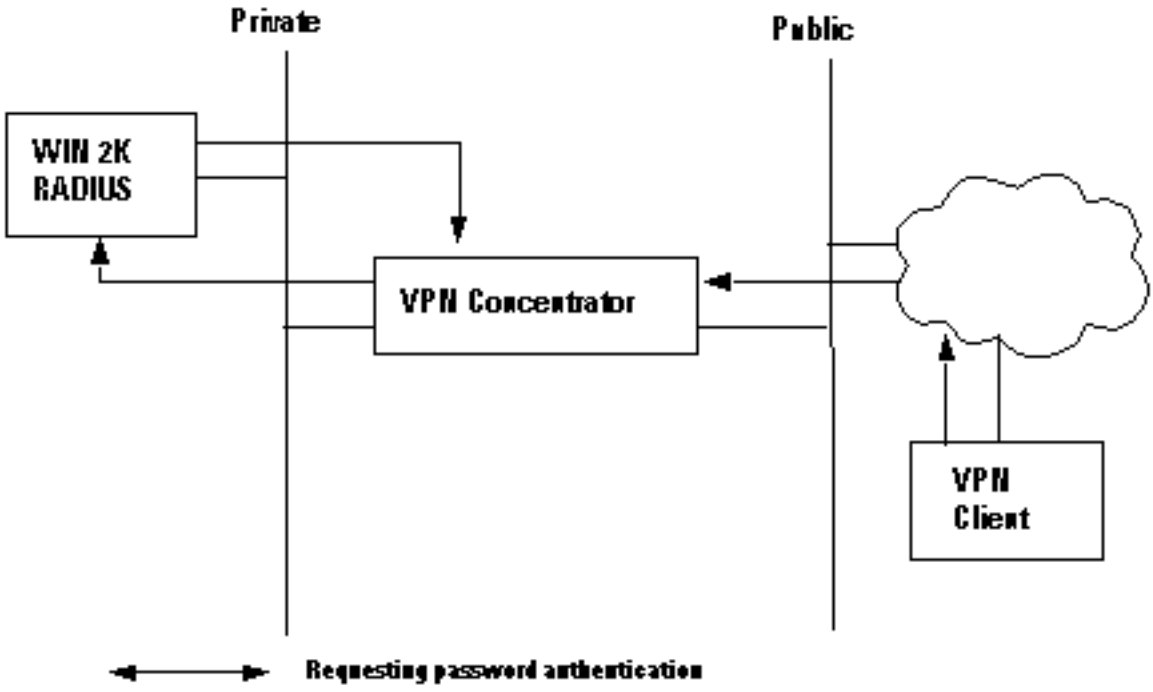
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Utilizzo di un server RADIUS Windows 2000 per autenticare un client VPN Cisco

Èpossibile utilizzare un server RADIUS Windows 2000 per autenticare un utente client VPN. Nello scenario seguente (il client VPN richiede l'autenticazione), il concentratore VPN 3000 riceve una richiesta dal client VPN contenente il nome utente e la password dell'utente client. Prima di inviare il nome utente e la password a un server RADIUS Windows 2000 nella rete privata per la verifica, VPN Concentrator esegue l'hashing del server utilizzando l'algoritmo HMAC/MD5.

Il server RADIUS Windows 2000 richiede PAP per l'autenticazione di una sessione client VPN. Per consentire al server RADIUS di autenticare un utente client VPN, controllare il parametro **Unencrypted Authentication (PAP, SPAP)** nella finestra **Modifica profilo chiamata in ingresso** (per impostazione predefinita, questo parametro non è selezionato). Per impostare questo parametro, selezionare il **criterio di accesso remoto** in uso, selezionare **Proprietà**, quindi selezionare la scheda **Autenticazione**.

Si noti che la parola *Unencrypted* nel nome del parametro è fuorviante. L'utilizzo di questo parametro *non* causa una violazione della sicurezza, in quanto quando il concentratore VPN invia il pacchetto di autenticazione al server RADIUS, non invia la password in chiaro. VPN Concentrator riceve il nome utente/password e i pacchetti crittografati dal client VPN ed esegue un hash HMAC/MD5 sulla password prima di inviare il pacchetto di autenticazione al server.



Utilizzo di un server RADIUS che non supporta MSCHAP

Alcuni server RADIUS non supportano l'autenticazione utente MSCHAPv1 o MSCHAPv2. Se si utilizza un server RADIUS che non supporta MSCHAP (v1 o v2), è necessario configurare il protocollo di autenticazione PPTP del gruppo di base per l'utilizzo di PAP e/o CHAP e inoltre disattivare le opzioni MSCHAP. Esempi di server RADIUS che non supportano MSCHAP sono il server Livingston v1.61 RADIUS o qualsiasi server RADIUS basato su codice Livingston.

Nota: senza MSCHAP, i pacchetti da e verso i client PPTP *non* verranno crittografati.

Utilizzo della crittografia con PPTP

Per utilizzare la crittografia con PPTP, un server RADIUS deve supportare l'autenticazione MSCHAP e inviare l'attributo restituito MSCHAP-MPPE-Keys per ogni autenticazione utente. Di seguito sono riportati alcuni esempi di server RADIUS che supportano questo attributo.

- Cisco Secure ACS per Windows - versione 2.6 o successiva
- Funk Software Steel-Belted RADIUS
- Pacchetto di opzioni di Microsoft Internet Authentication Server su NT 4.0 Server
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server - Server di autenticazione Internet

Informazioni correlate

- Pagina di supporto RADIUS
- Pagina di supporto di Cisco Secure ACS per Windows
- Cisco VPN serie 3000 Concentrator Support Page
- Cisco VPN serie 3000 Client Support Page
- Pagina di supporto per IPSec
- Pagina di supporto PPTP
- RFC 2637: Protocollo PPTP (Point-to-Point Tunneling Protocol)
- RFC (Requests for Comments)
- Supporto tecnico – Cisco Systems