Utilisation de serveurs RADIUS avec des produits VPN 3000

Contenu

Introduction

Ce document décrit certaines mises en garde détectées lors de l'utilisation de certains serveurs RADIUS avec le concentrateur VPN 3000 et les clients VPN.

- Le serveur RADIUS Windows 2000 nécessite le protocole PAP (Password Authentication Protocol) pour authentifier un client VPN Cisco. (clients IPSec)
- L'utilisation d'un serveur RADIUS qui ne prend pas en charge le protocole MSCHAP (Microsoft Challenge Handshake Authentication Protocol) nécessite que les options MSCHAP soient désactivées sur le concentrateur VPN 3000. (Clients PPTP (Point-to-Point Tunneling Protocol)
- L'utilisation du chiffrement avec PPTP nécessite l'attribut de retour MSCHAP-MPPE-Keys de RADIUS. (clients PPTP)
- Avec Windows 2003, MS-CHAP v2 peut être utilisé, mais la méthode d'authentification doit être définie sur RADIUS avec Expiry.

Certaines de ces notes sont apparues dans les notes de mise à jour des produits.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur Cisco VPN 3000
- Client VPN Cisco

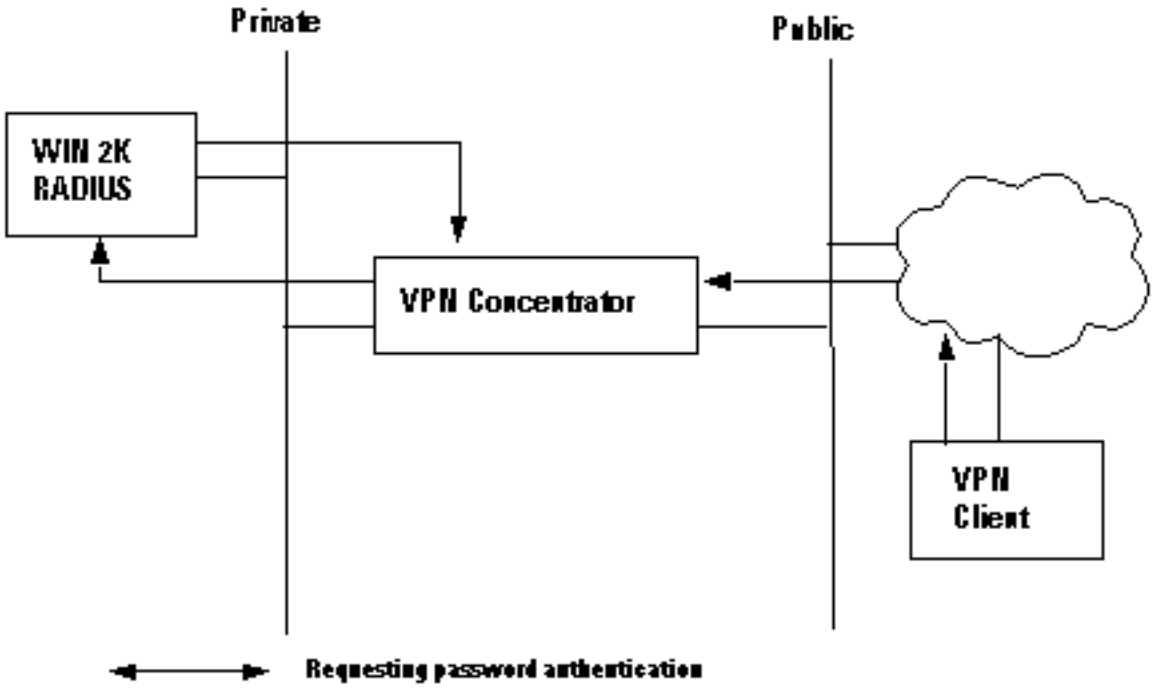
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Utilisation d'un serveur RADIUS Windows 2000 pour authentifier un client VPN Cisco

Vous pouvez utiliser un serveur RADIUS Windows 2000 pour authentifier un utilisateur client VPN. Dans le scénario suivant (le client VPN demande l'authentification), le concentrateur VPN 3000 reçoit une requête du client VPN contenant le nom d'utilisateur et le mot de passe de l'utilisateur client. Avant d'envoyer le nom d'utilisateur/mot de passe à un serveur RADIUS Windows 2000 sur le réseau privé pour vérification, le concentrateur VPN le hache, à l'aide de l'algorithme HMAC/MD5.

Le serveur RADIUS Windows 2000 nécessite PAP pour authentifier une session client VPN. Pour permettre au serveur RADIUS d'authentifier un utilisateur client VPN, vérifiez le **paramètre Unencryption Authentication (PAP, SPAP)** dans la fenêtre **Edit Dial-In Profile** (par défaut, ce paramètre n'est pas coché). Pour définir ce paramètre, sélectionnez la **stratégie d'accès à distance** que vous utilisez, sélectionnez **Propriétés** et l'onglet **Authentification**.

Notez que le mot *Unchiffré* sur le nom de ce paramètre est trompeur. L'utilisation de ce paramètre *ne* provoque *pas* de violation de sécurité, car lorsque le concentrateur VPN envoie le paquet d'authentification au serveur RADIUS, il n'envoie pas le mot de passe dans la zone clear . Le concentrateur VPN reçoit le nom d'utilisateur/mot de passe et les paquets chiffrés du client VPN, et effectue un hachage HMAC/MD5 sur le mot de passe avant d'envoyer le paquet d'authentification au serveur.



Utilisation d'un serveur RADIUS qui ne prend pas en charge MSCHAP

Certains serveurs RADIUS ne prennent pas en charge l'authentification utilisateur MSCHAPv1 ou MSCHAPv2. Si vous utilisez un serveur RADIUS qui ne prend pas en charge MSCHAP (v1 ou v2), vous devez configurer le protocole d'authentification PPTP du groupe de base pour utiliser PAP et/ou CHAP et également désactiver les options MSCHAP. Les serveurs RADIUS Livingston v1.61 ou tout autre serveur RADIUS basé sur le code Livingston sont des exemples de serveurs RADIUS qui ne prennent pas en charge MSCHAP.

Remarque : Sans MSCHAP, les paquets en provenance et à destination des clients PPTP *ne* seront *pas* chiffrés.

Utilisation du chiffrement avec PPTP

Pour utiliser le chiffrement avec PPTP, un serveur RADIUS doit prendre en charge l'authentification MSCHAP et doit envoyer l'attribut de retour MSCHAP-MPPE-Keys pour chaque authentification utilisateur. Des exemples de serveurs RADIUS prenant en charge cet attribut sont présentés ci-dessous.

- Cisco Secure ACS pour Windows - version 2.6 ou ultérieure
- Logiciel Funk Acier RADIUS
- Pack d'options Microsoft Internet Authentication Server sur NT 4.0 Server
- Microsoft Commercial Internet System (MCIS 2.0)
- Microsoft Windows 2000 Server — Serveur d'authentification Internet

Informations connexes

- Page d'assistance RADIUS

- Cisco Secure ACS pour la page d'assistance de Windows
- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Page de support PPTP
- RFC 2637 : Protocole de tunnellisation point à point (PPTP)
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems