# Utilisation de serveurs RADIUS avec des produits VPN 3000

## Contenu



# Introduction

Ce document décrit certaines mises en garde trouvées à l'aide de quelques serveurs de RAYON avec le concentrateur VPN 3000 et les clients vpn.

- Le serveur de RAYON de Windows 2000 a besoin du Password Authentication Protocol (PAP) pour authentifier un Client VPN Cisco. (Clients d'IPSec)
- Utilisant un serveur de RAYON qui ne le prend en charge pas la Microsoft Challenge Handshake Authentication Protocol (MSCHAP) exige des options MSCHAP d'être désactivé sur le concentrateur VPN 3000. (Clients de Protocol de canalisation en tunnel point-à-point [PPTP])
- Utilisant le cryptage avec PPTP exige les MSCHAP-MPPE-clés de retour d'attribut du RAYON. (Clients PPTP)
- Avec Windows 2003, MS-CHAP v2 peut être utilisé, mais la méthode d'authentification devrait être placée en tant que « RAYON avec l'échéance ».

Certaines de ces notes sont apparues dans les notes de distribution du produit.

# 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.

### Composants utilisés

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

- Concentrateur Cisco VPN 3000
- **Client VPN Cisco**

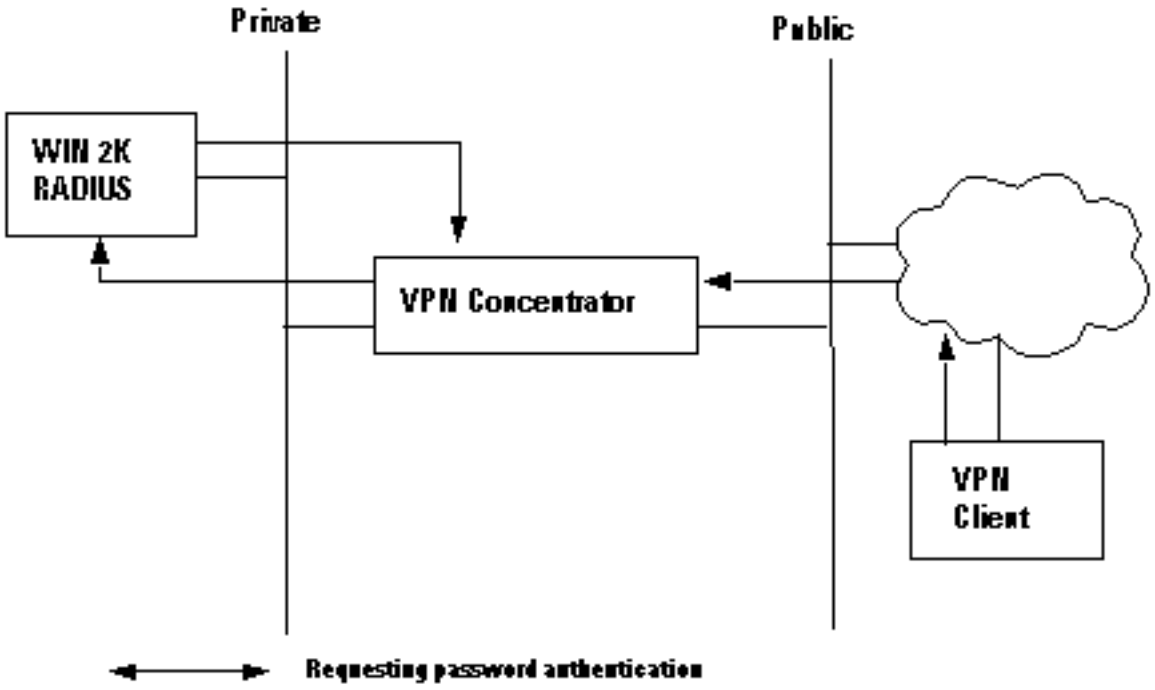
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Utilisant un serveur de RAYON de Windows 2000 pour authentifier un Client VPN Cisco

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

Le serveur de RAYON de Windows 2000 a besoin du PAP pour authentifier une session de client vpn. Pour permettre au serveur de RAYON d'authentifier un utilisateur de client vpn, vérifiez le paramètre **décrypté de l'authentification (PAP, SPAP)** sur la fenêtre de **profil d'accès distant d'éditer** (par défaut, ce paramètre n'est pas vérifié). Pour placer ce paramètre, sélectionner la **stratégie d'accès à distance que** vous utilisez, **Properties** choisi, et sélectionnent l'onglet d'**authentification**.

Notez que le mot *décrypté* sur ce nom de paramètre est fallacieux. Utilisant ce paramètre n'entraîne pas une brèche de sécurité, parce que quand le concentrateur VPN envoie le paquet d'authentification au serveur de RAYON, il n'envoie pas le mot de passe en clair. Le concentrateur VPN reçoit le nom d'utilisateur/mot de passe et les paquets chiffrés du client vpn, et exécute des informations parasites HMAC/MD5 sur le mot de passe avant d'envoyer le paquet d'authentification au serveur.




## Utilisant un serveur de RAYON qui ne prend en charge pas MSCHAP

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

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

## Utilisant le cryptage avec PPTP

Pour utiliser le cryptage avec PPTP, un serveur de RAYON doit prendre en charge l'authentification MSCHAP et doit envoyer les MSCHAP-MPPE-clés de retour d'attribut pour chaque authentification de l'utilisateur. Des exemples des serveurs de RAYON qui prennent en charge cet attribut sont affichés ci-dessous.

- Cisco Secure ACS pour Windows - version 2.6 ou ultérieures
- RAYON Acier-ceinturé par logiciel de trouille
- Microsoft Internet Authentication Server sur le paquet d'options de serveur de NT 4.0
- Système commercial d'Internet de Microsoft (MCIS 2.0)
- Microsoft Windows 2000 Server -- Serveur d'authentification d'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