Comment configurer le PPTP du concentrateur VPN 3000 avec l'authentification locale

Contenu

Introduction

Le concentrateur de Cisco VPN 3000 prend en charge la méthode point par point de perçage d'un tunnel de Protocol de tunnel (PPTP) pour les clients Windows indigènes. Il y a la prise en charge du chiffrement 40-bit et de 128-bit disponible sur ces concentrateurs VPN pour une connexion fiable sécurisée.

Référez-vous à configurer le concentrateur VPN 3000 PPTP avec le Cisco Secure ACS pour l'authentification de RAYON de Windows afin de configurer le concentrateur VPN pour des utilisateurs PPTP avec l'authentification étendue utilisant le Cisco Secure Access Control Server (ACS).

Conditions préalables

Conditions requises

Assurez-vous que vous rencontrez les conditions préalables mentionnées dans quand est le cryptage PPTP pris en charge sur un concentrateur de Cisco VPN 3000 ? avant que vous tentiez cette configuration.

Composants utilisés

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

- Concentrateur VPN 3015 avec la version 4.0.4.A
- PC Windows avec le client PPTP

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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Conventions

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

Configurez le concentrateur VPN 3000 avec l'authentification locale

Terminez-vous ces étapes pour configurer le concentrateur VPN 3000 avec l'authentification locale.

1. Configurez les adresses IP respectives dans le concentrateur VPN et assurez-vous que vous avez la Connectivité.
2. Assurez-vous que l'**authentification PAP** est sélectionnée dans le **Configuration > User Management >** onglet du **groupe de base** PPTP/L2TP.
3. **La configuration > les protocoles de système > de Tunnellisation > les PPTP** choisis et s'assurent que qui **ont activé** est vérifié.
4. **Le Configuration > User Management > Groups** choisi **> ajoutent**, et configurent un groupe PPTP. Dans cet exemple, le nom de groupe est « pptpgroup » et le mot de passe (et vérifiez le mot de passe) est "cisco123".
5. Sous l'onglet Général du groupe, assurez-vous que l'option **PPTP** est activée dans les Protocoles d'authentification.
6. Sous l'onglet PPTP/L2TP, l'**authentification PAP d'**enable, et le **cryptage de** débronchement (le cryptage peut être activé à tout moment à l'avenir).
7. **Le Configuration > User Management > les utilisateurs** choisis **> ajoutent**, et configurent un utilisateur local (appelé le « pptpuser ») avec le mot de passe **cisco123** pour l'authentification

PPTP. Mettez l'utilisateur dans le « pptpgroup » précédemment défini :
8. Sous l'onglet Général pour l'utilisateur, assurez-vous que l'option **PPTP** est activée dans des protocoles de Tunnellisation.
9. **Configuration > système > gestion d'adresses > groupes** choisis pour définir un pool d'adresses pour la gestion d'adresses.
10. **La configuration > le système > la gestion d'adresses > l'affectation** choisis et dirigent le concentrateur VPN utiliser le pool d'adresses.

Configuration de client de Microsoft PPTP

Remarque: Aucune des informations disponibles ici sur configurer le logiciel Microsoft n'est livré avec n'importe quelle garantie ou logiciel de support pour microsoft. Le logiciel de support pour microsoft est fourni par Microsoft .

Windows 98 - Installez et configurez la caractéristique PPTP

Installez

Terminez-vous ces étapes pour installer la caractéristique PPTP.

1. **Le Start > Settings > Control Panel > Add New Hardware** choisi **(prochain) > choisissent parmi la liste > l'adaptateur réseau (ensuite)**.
2. **Microsoft** choisi dans le panneau et l'**adaptateur** gauches de **Microsoft VPN** sur le panneau de droite.

Configurez

Terminez-vous ces étapes pour configurer la caractéristique PPTP.

1. **Le Start > Programs > Accessories > Communications > Dial Up Networking** choisi **> établissent le nouveau rapport**.
2. Connectez utilisant l'adaptateur de Microsoft VPN au choisi une demande de périphérique. L'IP de serveur VPN est le périphérique du tunnel 3000.

L'authentification par défaut de Windows 98 utilise le cryptage de mot de passe (par exemple, CHAP ou MSCHAP). Afin de désactiver au commencement ce cryptage, sélectionnez le **Properties > Server types**, et décochez les cases de **mot de passe chiffré** et de **Require Data Encryption**.

Windows 2000 - Configurer la caractéristique PPTP

Terminez-vous ces étapes pour configurer la caractéristique PPTP.

1. **Le Start > Programs > Accessories > Communications > Network and Dialup connections** choisi **> établissent le nouveau rapport**.
2. Cliquez sur Next, et choisi **connectez à un réseau privé par l'Internet > le cadran une connexion antérieurement** (ne sélectionnez pas ceci si vous utilisez un RÉSEAU LOCAL).
3. Cliquez sur Next de nouveau, et écrivez l'adresse Internet ou l'IP du périphérique du tunnel,

qui est l'interface extérieure du concentrateur VPN 3000. Dans cet exemple l'adresse IP est 161.44.17.1.

Properties > Security for the connection > Advanced choisi pour ajouter un type de mot de passe comme PAP. Le par défaut est MSCHAP et MSCHAPv2, pas CHAP ou PAP.

Le chiffrement de données est configurable dans cette zone. Vous pouvez le désactiver au commencement.

Windows NT

Vous pouvez les informations d'accès au sujet d'installer des clients de Windows NT pour PPTP au site Web de Microsoft .

Windows Vista

Terminez-vous ces étapes pour configurer la caractéristique PPTP.

1. Dès le début le bouton, choisissent **se connectent à**.
2. Choisissez **installent une connexion ou un réseau**.
3. Choisissez **se connectent à un lieu de travail** et cliquent sur Next.
4. Choisissez l'**utilisation ma connexion Internet (VPN)**.**Remarque:** S'incité pour « vous voulez utiliser une connexion que vous avez déjà, » choisissez l'**aucun, créez une nouvelle connexion** et cliquez sur Next.
5. Dans le domaine d'**adresse Internet**, type **pptp.vpn.univ.edu**, par exemple.
6. Dans la zone d'**identification de destination**, type **UNIVVPN**, par exemple.
7. Dans le **champ User Name**, tapez votre ID de connexion UNIV. Votre ID de connexion UNIV est la partie de votre adresse e-mail avant **@univ.edu.**
8. Dans le domaine de **mot de passe**, tapez votre mot de passe d'ID de connexion UNIV.
9. Cliquez sur le bouton de **création** et puis cliquez sur le bouton **étroit**.
10. Afin de se connecter au serveur VPN après que vous créiez la connexion VPN, cliquez sur le début, et puis **connectez à**.
11. Choisissez la connexion VPN dans la fenêtre et le clic **se connectent**.

Ajoutez MPPE (le cryptage)

Assurez-vous que la connexion PPTP fonctionne sans cryptage avant que vous ajoutiez le cryptage. Par exemple, cliquez sur le **bouton Connect** sur le client PPTP pour s'assurer que la connexion se termine. Si vous décidez d'avoir besoin du cryptage, l'authentification MSCHAP doit être utilisée. Sur le VPN 3000, **Configuration > User Management > Groups** choisi. Puis, sous l'onglet PPTP/L2TP pour le groupe, décochez le **PAP**, vérifiez **MSCHAPv1**, et vérifiez **requis pour le cryptage PPTP**.

Le client PPTP devrait être modifié pour l'encrytption de données et le MSCHAPv1 facultatifs ou priés (si c'est une option).

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre

configuration fonctionne correctement.

Vérifiez le concentrateur VPN

Vous pouvez commencer la session PPTP par composer la forme que le client PPTP a créée plus tôt dans la section de configuration de client de Microsoft PPTP.

Employez la fenêtre de sessions de >Administer de gestion sur le concentrateur VPN pour visualiser les paramètres et les statistiques pour toutes les sessions actives PPTP.

Vérifiez le PC

Émettez la **commande ipconfig** dans le mode de commande du PC de voir que le PC a deux adresses IP. On est sa propre adresse IP et l'autre est assigné par le concentrateur VPN du groupe d'adresse IP. Dans cet exemple l'adresse IP 172.16.1.10 est l'adresse IP assignée par le concentrateur VPN.

Debug

Si la connexion ne fonctionne pas, la classe d'événement PPTP mettent au point peut être ajoutée au concentrateur VPN. **La configuration > le système > les événements > les classes** choisis **> modifient** ou **ajoutent** (affiché ici). Les classes d'événement PPTPDBG et PPTPDECODE sont également disponibles, mais pourraient fournir trop d'informations.

Le journal d'événements peut être récupéré de la **surveillance > du journal d'événements filtrables**.

Debug VPN 3000 - Bonne authentification

```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129
   User [pptpuser]
   Authenticated successfully with MSCHAP-V1

4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22
   User [pptpuser] Group [Base Group] connected, Session Type: PPTP
```

Cliquez sur en fonction la fenêtre de **détails d'**état d'utilisateur PPTP pour vérifier les paramètres sur le PC Windows.

Dépannez

Ce sont des erreurs possibles que vous pouvez rencontrer :

- **Mauvais nom d'utilisateur ou mot de passe**Sortie de débogage de concentrateur VPN 3000 :1
```
09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 established
```

```
2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129
   Authentication rejected: Reason = User was not found
   handle = 44, server = (none), user = pptpusers, domain = <not specified>

5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129
   User [pptpusers]
   disconnected.. failed authentication ( MSCHAP-V1 )

6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129
   Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761),
   reason: Error (No additional info)

8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)
```

Le message que l'utilisateur voit (du Windows 98) :`Error 691: The computer you have dialed in to has denied access because the username and/or password is invalid on the domain.`Le message que l'utilisateur voit (du Windows 2000) :`Error 691: Access was denied because the username and/or password was invalid on the domain.`

- **Le « cryptage exigé » est sélectionné sur le PC, mais pas sur le concentrateur VPN**Le message que l'utilisateur voit (du Windows 98) :`Error 742: The computer you're dialing in to does not support the data encryption requirements specified. Please check your encryption settings in the properties of the connection. If the problem persists, contact your network administrator.`Le message que l'utilisateur voit (du Windows 2000) :`Error 742: The remote computer does not support the required data encryption type`
- **Le « cryptage exigé » (128-bit) est sélectionné sur le concentrateur VPN avec un PC qui prend en charge seulement le cryptage 40-bit**Sortie de débogage de concentrateur VPN 3000 :`4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [ pptpuser ] disconnected. PPTP Encryption configured as REQUIRED.. remote client not supporting it.`Le message que l'utilisateur voit (du Windows 98) :`Error 742: The remote computer does not support the required data encryption type.`Le message que l'utilisateur voit (du Windows 2000) :`Error 645 Dial-Up Networking could not complete the connection to the server. Check your configuration and try the connection again.`
- **Le concentrateur VPN 3000 est configuré pour MSCHAPv1 et le PC est configuré pour le PAP, mais ils ne peuvent pas convenir sur une méthode d'authentification**Sortie de débogage de concentrateur VPN 3000 :`8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129 User [pptpuser] disconnected. Authentication protocol not allowed.` Le message que l'utilisateur voit (du Windows 2000) :`Error 691: Access was denied because the username and/or password was invalid on the domain.`

Questions possibles de Microsoft à dépanner

- Comment maintenir des connexions RAS actives après fermeture de sessionQuand vous vous fermez une session d'un client de Windows Remote Access Service (RAS), toutes les connexions RAS sont automatiquement déconnectées. Permettez à la clé de **KeepRasConnections** dans le registre sur le client RAS de demeurer connectée après que vous vous fermiez une session. Référez-vous à l'article de base de connaissances de

Microsoft - 158909 pour en savoir plus.

- **L'utilisateur n'est pas alerté en ouvrant une session avec les qualifications cachées**Les symptômes de cette question sont quand vous tentez d'ouvrir une session à un domaine d'un poste de travail basé sur Windows ou le serveur membre et un contrôleur de domaine ne peuvent pas se trouvent et aucun message d'erreur n'est affiché. Au lieu de cela, vous ouvrez une session sur l'ordinateur local à l'aide des informations d'identification mises en cache. Référez-vous à l'article de base de connaissances de Microsoft - 242536 pour en savoir plus.
- **Procédures pour écrire un fichier LMHOSTS pour la validation de domaine et autres problèmes de résolution de noms**Il peut y avoir des exemples quand vous éprouvez des questions de résolution de noms sur votre réseau TCP/IP et vous devez utiliser des fichiers lmhosts pour résoudre des noms NetBIOS. Cet article discute la méthode appropriée utilisée pour créer un fichier lmhosts pour faciliter la validation de résolution de noms et de domaine. Référez-vous à l'article de base de connaissances de Microsoft - 180094 pour en savoir plus.

Informations connexes

- RFC 2637 : Protocole de tunnellisation point à point (PPTP)
- Cisco Secure ACS pour des pages de support de Windows
- Quand le cryptage PPTP est-il pris en charge sur un concentrateur de Cisco VPN 3000 ?
- Configurer le concentrateur VPN 3000 et le PPTP avec le Cisco Secure ACS pour l'authentification de RAYON de Windows
- Pages de support de concentrateur de Cisco VPN 3000
- Pages de support de Cisco VPN 3000 Client
- Pages de support produit de sécurité IP (IPSec)
- Pages de support produit PPTP
- Support et documentation techniques - Cisco Systems