Configurer un routeur Cisco pour l'authentification de numérotation à l'aide de TACACS+

Contenu

Introduction

Ce document décrit comment configurer un routeur Cisco pour l'authentification par numérotation avec TACACS+ qui s'exécute sur UNIX. TACACS+ ne propose pas autant de fonctionnalités que Cisco Secure ACS pour Windows ou Cisco Secure ACS pour UNIX disponible dans le commerce.

Le logiciel TACACS+ précédemment fourni par Cisco Systems a été discontinué et n'est plus pris en charge par Cisco Systems.

Aujourd'hui, vous pouvez trouver beaucoup de versions gratuites de TACACS+ quand vous recherchez « logiciel gratuit TACACS+ » sur votre moteur de recherche préféré sur Internet. Cisco ne recommande spécifiquement aucune implémentation particulière de logiciel gratuit TACACS+.

Le Cisco Secure Access Control Server (ACS) est disponible pour l'achat par des ventes de Cisco et des canaux réguliers de distribution dans le monde entier. Le Cisco Secure ACS pour des Windows inclut tous les composants nécessaires requis pour une installation indépendante sur une station de travail de Microsoft Windows. Le moteur de solution de Cisco Secure ACS est expédié avec une licence logicielle préinstallée de Cisco Secure ACS. Reportez-vous au Bulletin produit Cisco Secure ACS 4.0 pour obtenir les numéros de produit. Visitez la page d'accueil de commande Cisco (clients enregistrés seulement) pour passer une commande.

Note: Vous avez besoin d'un compte CCO associé à un contrat de service pour obtenir la version d'évaluation de 90 jours de Cisco Secure ACS pour Windows (clients enregistrés uniquement).

La configuration du routeur dans ce document a été développée sur un routeur qui exécute la version software 11.3.3 de Cisco IOS®. Les versions 12.0.5.T et ultérieures du logiciel Cisco IOS utilisent **group tacacs+** au lieu de **tacacs+**. Les instructions telles que **aaa authentication login default tacacs+ enable** apparaissent comme **aaa authentication login default group tacacs+ enable**.

Vous pouvez télécharger le logiciel gratuit TACACS+ et le Guide de l'utilisateur par ftp anonyme vers ftp-eng.cisco.com dans le répertoire /pub/tacacs.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Configurations

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour trouver des informations supplémentaires sur les commandes utilisées dans ce document.

Ce document utilise les configurations suivantes :

- Configuration du routeur
- Fichier de configuration TACACS+ sur le serveur gratuit

Configuration du routeur

```
!
aaa new-model
aaa authentication login default tacacs+ enable
aaa authentication ppp default if-needed tacacs+
aaa authorization exec default tacacs+ if-authenticated
aaa authorization commands 1 default tacacs+ if-
authenticated
aaa authorization commands 15 default tacacs+ if-
```

```
authenticated
aaa authorization network default tacacs+
enable password ww
!
chat-script default "" at&fls0=1&h1&r2&c1&d2&b1e0q2 OK
!
interface Ethernet0
 ip address 10.6.1.200 255.255.255.0
!
 !--- Challenge Handshake Authentication Protocol !---
(CHAP/PPP) authentication user. interface Async1 ip
unnumbered Ethernet0 encapsulation ppp async mode
dedicated peer default ip address pool async no cdp
enable ppp authentication chap ! !--- Password
Authentication Protocol (PAP/PPP) authentication user.
interface Async2 ip unnumbered Ethernet0 encapsulation
ppp async mode dedicated peer default ip address pool
async no cdp enable ppp authentication pap ! !---
Authentication user with autocommand PPP. interface
Async3 ip unnumbered Ethernet0 encapsulation ppp async
mode interactive peer default ip address pool async no
cdp enable ! ip local pool async 10.6.100.101
10.6.100.103 tacacs-server host 171.68.118.101 tacacs-
server timeout 10 tacacs-server key cisco ! line 1
session-timeout 20 exec-timeout 120 0 autoselect during-
login script startup default script reset default modem
Dialin transport input all stopbits 1 rxspeed 115200
txspeed 115200 flowcontrol hardware ! line 2 session-
timeout 20 exec-timeout 120 0 autoselect during-login
script startup default script reset default modem Dialin
transport input all stopbits 1 rxspeed 115200 txspeed
115200 flowcontrol hardware ! line 3 session-timeout 20
exec-timeout 120 0 autoselect during-login autoselect
ppp script startup default script reset default modem
Dialin autocommand ppp transport input all stopbits 1
rxspeed 115200 txspeed 115200 flowcontrol hardware ! end
```

Fichier de configuration TACACS+ sur le serveur gratuit

```
!--- Handshake with router !--- AS needs 'tacacs-server
key cisco'. key = "cisco" !--- User who can Telnet in to
configure. user = admin { default service = permit login
= cleartext "admin" } !--- CHAP/PPP authentication line
1 - !--- password must be cleartext per CHAP
specifications. user = chapuser { chap = cleartext
"chapuser" service = ppp protocol = ip { default
attribute = permit } } !--- PPP/PAP authentication line
2. user = papuser { login = file /etc/passwd service =
ppp protocol = ip { default attribute = permit } } !---
Authentication user line 3. user = authauto { login =
file /etc/passwd service = ppp protocol = ip { default
attribute = permit } }
```

Configuration de Microsoft Windows

Configuration de Microsoft Windows pour les utilisateurs 1 et 2

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Step-by-Step Instructions

Procédez comme suit :

Remarque : La configuration du PC peut varier légèrement en fonction de la version du système d'exploitation que vous utilisez.

1. Sélectionnez **Start > Programs > Accessories > Dial-Up Networking** pour ouvrir la fenêtre Dial-Up Networking.
2. Choisissez **Make New Connection** dans le menu Connections, puis entrez un nom pour votre connexion.
3. Entrez les informations spécifiques à votre modem et cliquez sur **Configurer**.
4. Dans la page Propriétés générales, sélectionnez la vitesse la plus élevée de votre modem, mais ne vérifiez pas la **connexion Uniquement à cette vitesse**... de la boîte de dialogue.
5. Sur la page Configurer/Propriétés de connexion, utilisez 8 bits de données, aucune parité et 1 bit d'arrêt. Les préférences d'appel à utiliser sont **Attendre la tonalité avant de composer le numéro** et **Annuler l'appel s'il n'est pas connecté après 200 secondes**.
6. Sur la page Connexion, cliquez sur **Avancé**. Dans Paramètres de connexion avancés, sélectionnez uniquement **Contrôle de flux matériel** et **Type de modulation Standard**.Sur la page des propriétés Configurer/Options, rien ne doit être coché sauf la case sous Contrôle d'état.
7. Cliquez sur **OK**, puis sur **Suivant**.
8. Entrez le numéro de téléphone de la destination, cliquez à nouveau sur **Suivant**, puis cliquez sur **Terminer**.
9. Une fois que l'icône de nouvelle connexion apparaît, cliquez dessus avec le bouton droit et choisissez **Propriétés > Type de serveur**.
10. Choisissez **PPP : WINDOWS 95, WINDOWS NT 3.5, Internet** et ne cochez aucune option avancée.
11. Cochez **TCP/IP** sous Protocoles réseau autorisés.
12. Sous Paramètres TCP/IP..., sélectionnez **Adresse IP attribuée au serveur**, **Adresses serveur de noms attribuées au serveur**, et **Utiliser la passerelle par défaut sur le réseau distant**, puis cliquez sur **OK**.
13. Lorsque l'utilisateur double-clique sur l'icône pour afficher la fenêtre Se connecter à afin de composer un numéro, il doit remplir les champs Nom d'utilisateur et Mot de passe, puis cliquez sur **Se connecter**.

Configuration Microsoft Windows pour l'utilisateur 3

La configuration de l'utilisateur 3 (utilisateur d'authentification avec autocommand PPP) est identique à celle des utilisateurs 1 et 2, avec les exceptions suivantes :

- Sur la page des propriétés Configurer/Options (étape 6), cochez la case **Monter la fenêtre du terminal après avoir composé le numéro**.
- Lorsque l'utilisateur double-clique sur l'icône pour ouvrir la fenêtre Se connecter à à composer (étape 13), il ne remplit pas les champs Nom d'utilisateur et Mot de passe. L'utilisateur clique sur **Connect**. Une fois la connexion établie au routeur, l'utilisateur entre le nom d'utilisateur et le mot de passe dans la fenêtre noire qui s'affiche. Après authentification, l'utilisateur appuie sur **Continuer (F7)**.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Routeur

Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **debug.**

- **terminal monitor** - Affiche la sortie de la commande **debug** et les messages d'erreur système pour le terminal et la session en cours.
- **debug ppp negotiation** - Affiche les paquets PPP envoyés lors du démarrage PPP, où les options PPP sont négociées.
- **debug ppp packet** : affiche les paquets PPP qui sont envoyés et reçus. (Cette commande affiche les vidages de paquets de bas niveau.)
- **debug ppp chap** : affiche des informations sur l'authentification d'un client (pour les versions du logiciel Cisco IOS antérieures à 11.2).
- **debug aaa authentication** - Affiche des informations sur l'authentification, l'autorisation et la comptabilité (AAA)/l'authentification TACACS+.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/TACACS+.

Serveur

Remarque : ceci suppose le code de serveur gratuit TACACS+ de Cisco.

```
tac_plus_executable -C config.file -d 16
  tail -f /var/tmp/tac_plus.log
```

Informations connexes

- Page d'assistance TACACS+
- TACACS+ dans la documentation d'IOS
- Serveur Cisco Secure Access Control
- Configuration et débogage de CiscoSecure 2.x TACACS+
- Support et documentation techniques - Cisco Systems