Implémentation du proxy d'authentification

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Conventions](#)
[Comment implémenter le proxy d'authentification](#)
[Profils de serveur](#)
[Cisco Secure UNIX (TACACS+)](#)
[Cisco Secure Windows (TACACS+)](#)
[Ce que l'utilisateur voit](#)
[Informations connexes](#)

Introduction

Le proxy d'authentification, offert avec le pare-feu du logiciel Cisco IOS® versions 12.0.5.T et ultérieures, sert à authentifier les utilisateurs entrants, sortants ou les deux. Ces utilisateurs sont généralement bloqués au moyen d'une liste d'accès. Cependant, grâce au proxy d'authentification, les utilisateurs lancent un navigateur afin d'outrepasser le pare-feu et d'être authentifiés sur un serveur TACACS+ ou RADIUS. Le serveur transfère des entrées supplémentaires de la liste d'accès vers le routeur afin de donner accès aux utilisateurs après leur authentification.

Ce document donne à l'utilisateur des conseils généraux pour la mise en oeuvre de auth-proxy, fournit quelques profils de serveur Cisco Secure pour le proxy d'auth et décrit ce que l'utilisateur voit quand auth-proxy est en cours d'utilisation.

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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Comment implémenter le proxy d'authentification

Procédez comme suit :

1. Assurez-vous que le trafic traverse correctement le pare-feu avant de configurer auth-proxy.
2. Pour une interruption minimale du réseau pendant le test, modifiez la liste d'accès existante pour refuser l'accès à un client de test.
3. Assurez-vous que le client de test ne peut pas passer par le pare-feu et que les autres hôtes peuvent passer.
4. Activez debug avec **exec-timeout 0 0** sous le port de console ou les terminaux de type virtuel (VTY), tandis que vous ajoutez les commandes **auth-proxy** et testez.

Profils de serveur

Nos tests ont été réalisés avec Cisco Secure UNIX et Windows. Si RADIUS est utilisé, le serveur RADIUS doit prendre en charge des attributs spécifiques au fournisseur (attribut 26). Voici quelques exemples de serveurs :

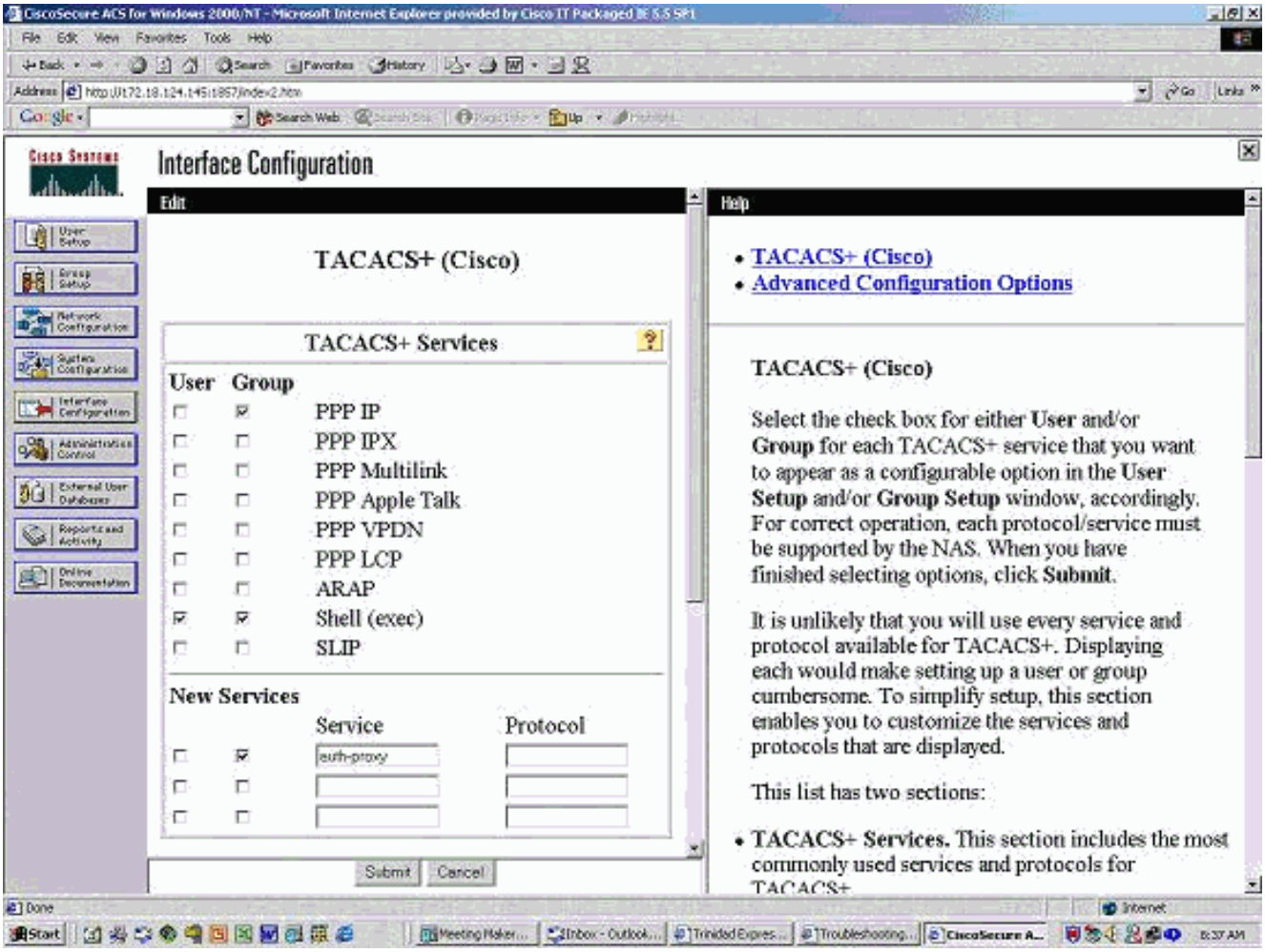
Cisco Secure UNIX (TACACS+)

```
# ./ViewProfile -p 9900 -u proxyonly
User Profile Information
user = proxyonly{
profile_id = 57
set server current-failed-logins = 1
profile_cycle = 2
password = clear "********"
service=auth-proxy {
set priv-lvl=15
set proxyacl#1="permit icmp any any"
set proxyacl#2="permit tcp any any"
set proxyacl#3="permit udp any any"
}
}
```

Cisco Secure Windows (TACACS+)

Suivez la procédure suivante .

1. Saisissez le nom d'utilisateur et le mot de passe (base de données Cisco Secure ou Windows).
2. Pour Configuration d'interface, sélectionnez **TACACS+**.
3. Sous Nouveaux services, sélectionnez l'option **Groupe** et tapez **auth-proxy** dans la colonne Service. Laissez la colonne Protocole
   vide.



4. Avancé - fenêtre d'affichage pour chaque service - attributs personnalisés.
5. Dans Paramètres du groupe, cochez **auth-proxy** et entrez ces informations dans la fenêtre :

```
priv-lvl=15
proxyacl#1=permit icmp any any
proxyacl#2=permit tcp any any
proxyacl#3=permit udp any any
```

Cisco Secure UNIX (RADIUS)

```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit udp any any"
}
}

}
```

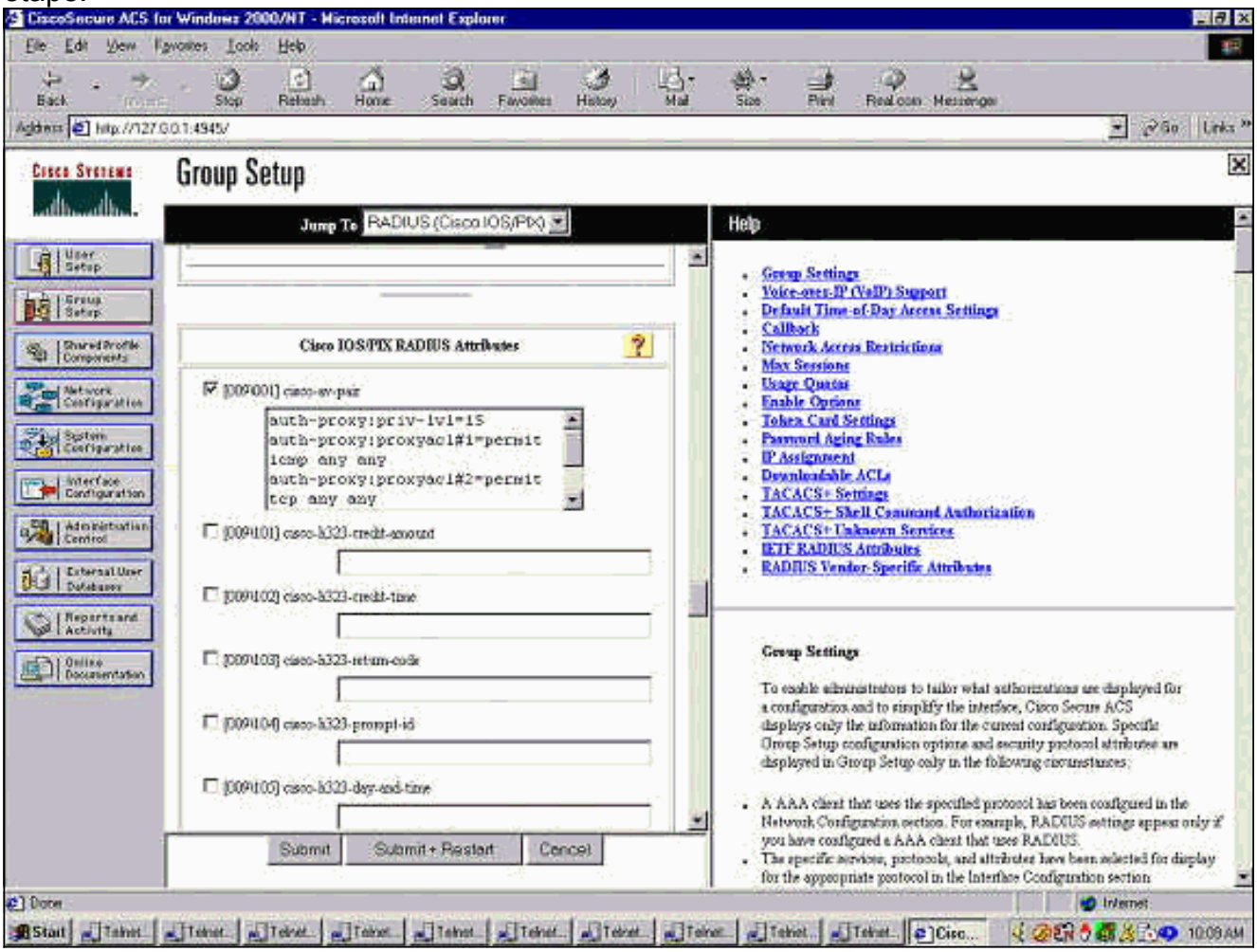
Cisco Secure Windows (RADIUS)

Suivez la procédure suivante .

1. Ouvrez Configuration du réseau. Le NAS doit être Cisco RADIUS.
2. Si l'option RADIUS de configuration d'interface est disponible, cochez les cases **VSA**.
3. Dans Paramètres utilisateur, saisissez le nom d'utilisateur/mot de passe.
4. Dans Paramètres du groupe, sélectionnez l'option pour **[009/001] cisco-av-pair**. Dans la zone de texte située sous la sélection, tapez ceci :

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit icmp any any
auth-proxy:proxyacl#2=permit tcp any any
auth-proxy:proxyacl#3=permit udp any any
```

Cette fenêtre est un exemple de cette étape.



Ce que l'utilisateur voit

L'utilisateur tente de parcourir quelque chose de l'autre côté du pare-feu.

Une fenêtre s'affiche avec ce message :

```
Cisco <hostname> Firewall
```

```
Authentication Proxy
Username:
Password:
```

Si le nom d'utilisateur et le mot de passe sont corrects, l'utilisateur voit :

```
Cisco Systems
Authentication Successful!
```

Si l'authentification échoue, le message est :

```
Cisco Systems
Authentication Failed!
```

Informations connexes

- Page de support pour le pare-feu d'IOS
- Support et documentation techniques - Cisco Systems