Implémentation du proxy d'authentification

Contenu

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 astuces générales pour l'implémentation du proxy d'authentification, fournit quelques profils de serveur Cisco Secures pour le proxy authentique, et décrit ce que l'utilisateur voit quand le proxy d'authentification est en service.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Comment implémenter le Seveur mandataire d'authentification

Procédez comme suit :

1. Assurez-vous que la circulation correctement par le Pare-feu avant que vous configuriez le proxy d'authentification.
2. Pour l'interruption minimum du réseau pendant le test, modifiez la liste d'accès existante pour refuser l'accès à un client de test.
3. Assurez-vous que l'un client de test ne peut pas obtenir par le Pare-feu et que les autres hôtes peuvent obtenir.
4. Turn on mettent au point avec l'**exec-timeout 0 0** sous le port de console ou les terminaux de type virtuel (VTYs), alors que vous ajoutez les commandes et le test de **proxy d'authentification**.

Profils de serveur

Notre test a été fait avec Cisco Secure UNIX et Windows. Si le RAYON est en service, le serveur de RAYON doit prendre en charge des attributs de constructeur-particularité (attribut 26). Les exemples spécifiques de serveur suivent :

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"
}
}
```

Windows Cisco Secure (TACACS+)

Suivez cette procédure.

1. Écrivez le nom d'utilisateur et mot de passe (base de données Cisco Secure ou de Windows).
2. Pour la configuration d'interface, **TACACS+** choisi.
3. Sous de nouveaux services, sélectionnez l'option de **groupe** et tapez le **proxy d'authentification** dans la colonne de service. Laissez le blanc de colonne de Protocol.
4. - Viseur pour chaque service - attributs personnalisés avancés.
5. Dans des configurations de groupe, vérifiez le **proxy d'authentification** et écrivez 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 (RAYON)

```
# ./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"
}
}

}
```

Windows Cisco Secure (RAYON)

Suivez cette procédure.

1. Configuration réseau de réseau ouvert. Le NAS devrait être RAYON de Cisco.
2. Si le RAYON de configuration d'interface est disponible, vérifiez les cases **VSA**.
3. Dans les paramètres utilisateurs, entrez dans le nom d'utilisateur/mot de passe.
4. Dans des configurations de groupe, sélectionnez l'option pour des Cisco-poids du commerce-**paires [009/001]**. Dans la zone de texte 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

Les tentatives d'utilisateur de parcourir quelque chose de l'autre côté du Pare-feu.

Affichages d'une fenêtre avec ce message :

```
Cisco <hostname> Firewall
Authentication Proxy
Username:
Password:
```

Si le nom d'utilisateur et mot de passe sont bon, 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