Authentification des utilisateurs sortants par proxy d'authentification – Ni pare-feu Cisco IOS, ni NAT

Contenu

Introduction

La fonction Authentication Proxy permet aux utilisateurs de se connecter au réseau ou d'accéder à Internet via HTTP, avec leurs profils d'accès spécifiques automatiquement récupérés et appliqués à partir d'un serveur RADIUS ou TACACS+. Les profils utilisateur sont actifs uniquement lorsqu'il y a du trafic actif en provenance des utilisateurs authentifiés.

Cet exemple de configuration bloque le trafic du périphérique hôte (à l'adresse 40.31.1.47) sur le réseau interne vers tous les périphériques sur Internet jusqu'à ce que l'authentification du navigateur soit effectuée avec l'utilisation du proxy d'authentification. La liste de contrôle d'accès (ACL) transmise depuis le serveur (**permit tcp|ip|icmp any any**) ajoute des entrées dynamiques après autorisation à la liste d'accès 116 qui permettent temporairement l'accès à Internet depuis le PC hôte.

Référez-vous à Configuration du proxy d'authentification pour plus d'informations sur le proxy d'authentification.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Logiciel Cisco IOS® Version 12.2(15)T
- Routeur Cisco 7206

Remarque : La commande **ip auth-proxy** a été introduite dans le logiciel Cisco IOS Firewall Version 12.0.5.T.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

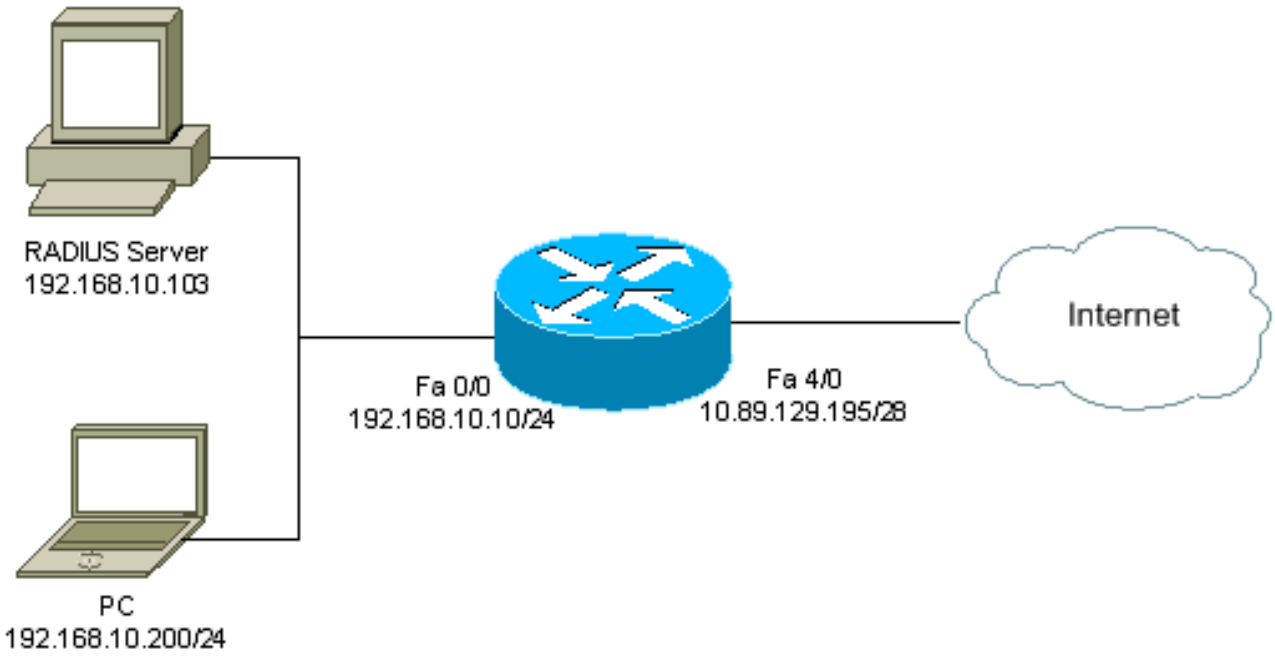
Configuration

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

Remarque : Utilisez l'outil de recherche de commandes (clients inscrits seulement) pour en savoir plus sur les commandes figurant dans le présent document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

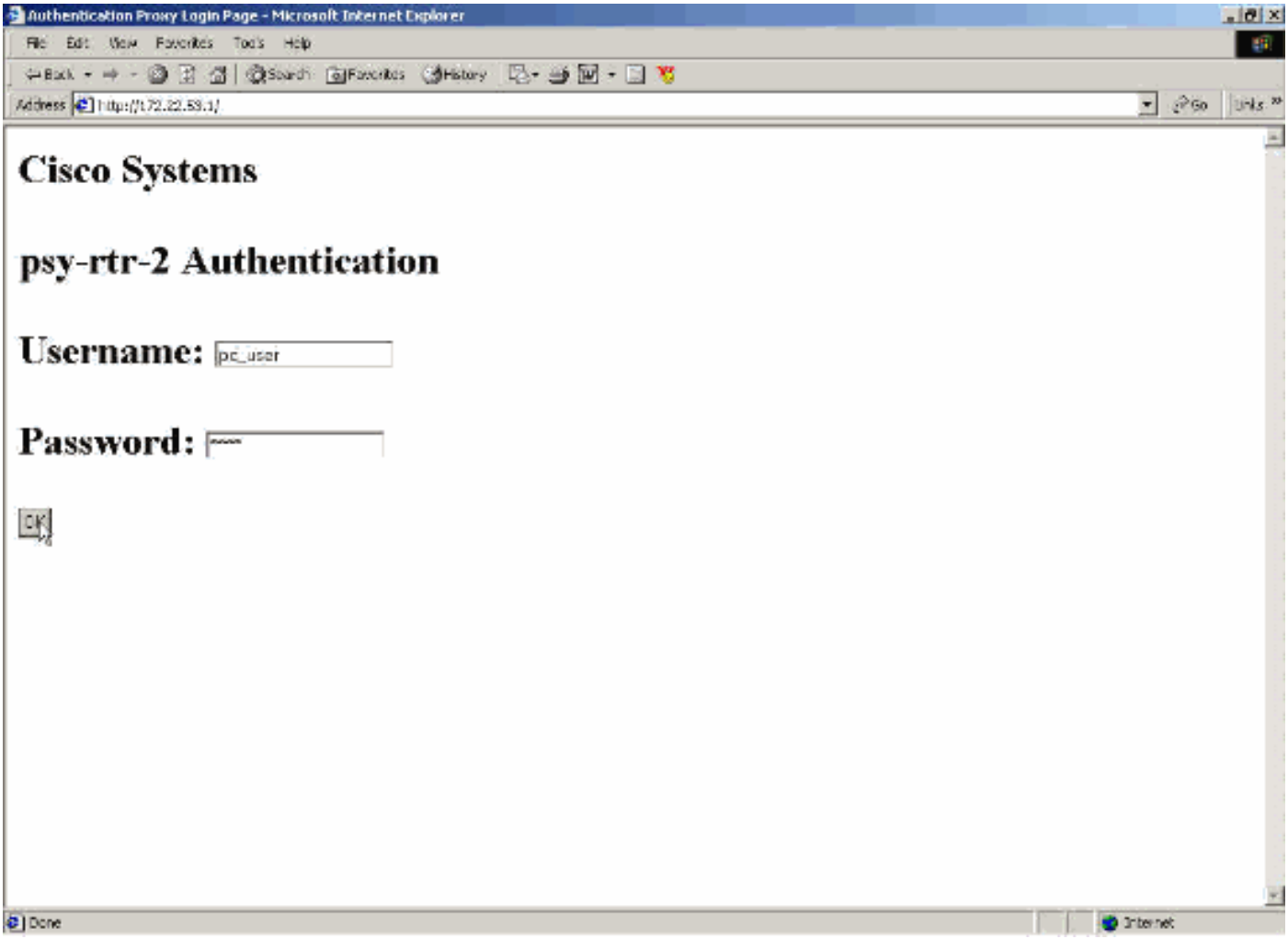
Ce document utilise la configuration suivante :

Routeur 7206

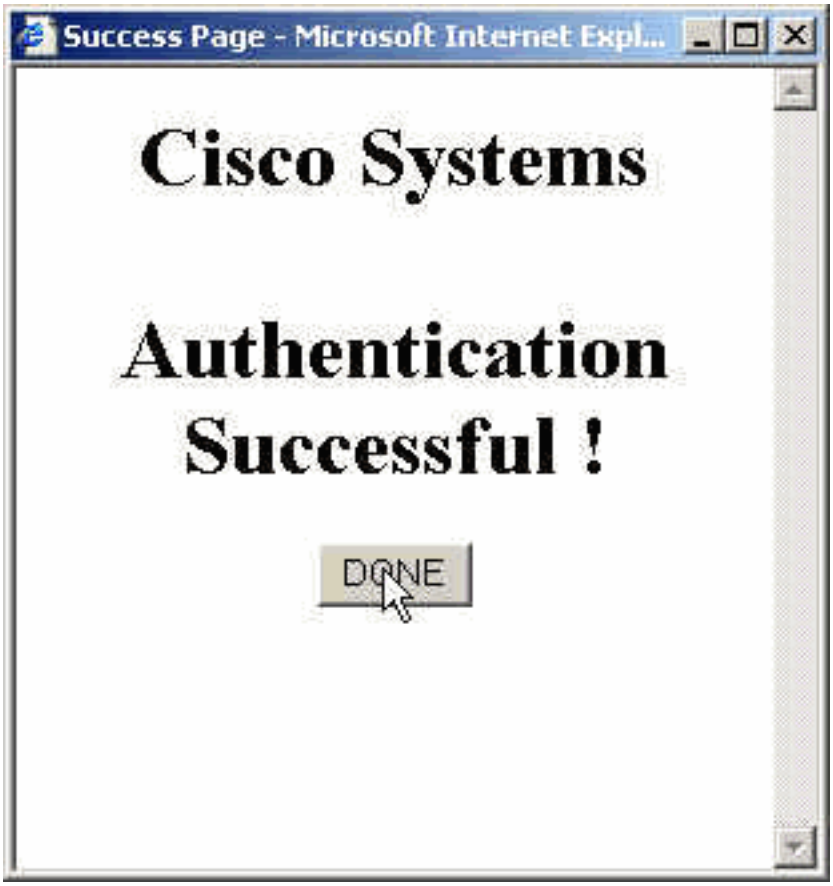
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- Enable AAA. aaa authentication login default group
radius none !--- Use RADIUS to authenticate users. aaa
authorization exec default group radius none aaa
authorization auth-proxy default group radius !---
Utilize RADIUS for auth-proxy authorization. aaa
session-id common ip subnet-zero ! ip cef ! ip auth-
proxy auth-proxy-banner !--- Displays the name of the
firewall router !--- in the Authentication Proxy login
page. ip auth-proxy auth-cache-time 10 !--- Sets the
global Authentication Proxy idle !--- timeout value in
minutes. ip auth-proxy name restrict_pc http !---
Associates connections that initiate HTTP traffic with
!--- the "restrict_pc" Authentication Proxy name. ip
audit notify log ip audit po max-events 100 ! no voice
hpi capture buffer no voice hpi capture destination !
mta receive maximum-recipients 0 ! ! interface
FastEthernet0/0 ip address 192.168.10.10 255.255.255.0
ip access-group 116 in !--- Apply access list 116 in the
inbound direction. ip auth-proxy restrict_pc !--- Apply
the Authentication Proxy list !--- "restrict_pc"
configured earlier. duplex full ! interface
FastEthernet4/0 ip address 10.89.129.195 255.255.255.240
duplex full ! ip classless ip http server !--- Enables
the HTTP server on the router. !--- The Authentication
Proxy uses the HTTP server to communicate !--- with the
client for user authentication. ip http authentication
aaa !--- Sets the HTTP server authentication method to
AAA. ! access-list 116 permit tcp host 192.168.10.200
host 192.168.10.10 eq www !--- Permit HTTP traffic (from
the PC) to the router. access-list 116 deny tcp host
192.168.10.200 any access-list 116 deny udp host
192.168.10.200 any access-list 116 deny icmp host
192.168.10.200 any !--- Deny TCP, UDP, and ICMP traffic
from the client by default. access-list 116 permit tcp
192.168.10.0 0.0.0.255 any access-list 116 permit udp
192.168.10.0 0.0.0.255 any access-list 116 permit icmp
192.168.10.0 0.0.0.255 any !--- Permit TCP, UDP, and
ICMP traffic from other !--- devices in the
192.168.10.0/24 network. ! radius-server host
192.168.10.103 auth-port 1645 acct-port 1646 key 7
<deleted> !--- Specify the IP address of the RADIUS !---
server along with the key. radius-server authorization
permit missing Service-Type call rsvp-sync ! ! line con
0 stopbits 1 line aux 0 stopbits 1 line vty 0 4 ! end
```

Authentification sur le PC

Cette section fournit des captures d'écran prises à partir du PC qui montrent la procédure d'authentification. La première capture montre la fenêtre dans laquelle un utilisateur entre le nom d'utilisateur et le mot de passe pour l'authentification et appuie sur **OK**.



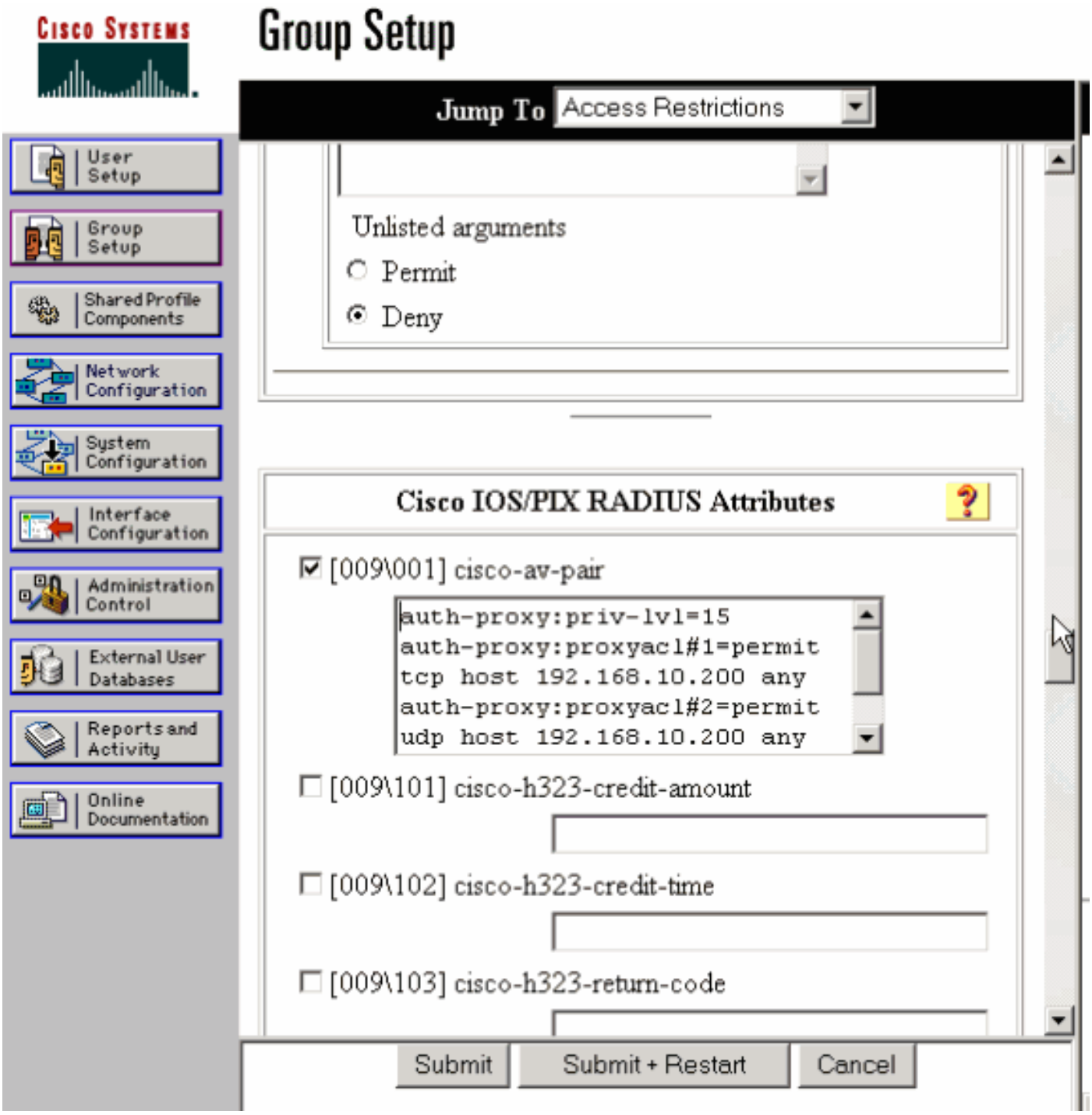
Si l'authentification réussit, cette fenêtre s'affiche.



Le serveur RADIUS doit être configuré avec les listes de contrôle d'accès proxy appliquées. Dans cet exemple, ces entrées de liste de contrôle d'accès sont appliquées. Cela permet au PC de se connecter à n'importe quel périphérique.

```
permit tcp host 192.168.10.200 any
permit udp host 192.168.10.200 any
permit icmp host 192.168.10.200 any
```

Cette fenêtre Cisco ACS indique où entrer les listes de contrôle d'accès proxy.



Remarque : référez-vous à Configuration du proxy d'authentification pour plus d'informations sur la configuration du serveur RADIUS/TACACS+.

Vérification

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show ip access-lists** - Affiche les listes de contrôle d'accès standard et étendues configurées sur le pare-feu (inclut les entrées de liste de contrôle d'accès dynamique). Les entrées de la liste de contrôle d'accès dynamique sont ajoutées et supprimées périodiquement selon que

l’utilisateur s’authentifie ou non.
- **show ip auth-proxy cache** - Affiche les entrées du proxy d'authentification ou la configuration du proxy d'authentification en cours. Mot clé cache permettant de répertorier l'adresse IP de l'hôte, le numéro de port source, la valeur de délai d'attente du proxy d'authentification et l'état des connexions qui utilisent le proxy d'authentification. Si l'état du proxy d'authentification est HTTP_ESTAB, l'authentification de l'utilisateur est une réussite.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour ces commandes, ainsi que d'autres informations de dépannage, référez-vous à Dépannage du proxy d'authentification.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d’utiliser les commandes de **débogage**.

Informations connexes

- Page de support pour le pare-feu d'IOS
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Page d'assistance RADIUS
- RADIUS dans la documentation d'IOS
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems