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

Contenu

Introduction

La caractéristique de Seveur mandataire d'authentification permet à des utilisateurs pour ouvrir une session au réseau ou accéder à l'Internet par l'intermédiaire du HTTP, avec leur accès spécifique profile automatiquement récupéré et appliqué à partir d'un serveur de RAYON, ou TACACS+. Les profils utilisateurs sont en activité seulement quand il y a du trafic actif des utilisateurs authentifiés.

Les blocs de cette configuration d'échantillon trafiquent du périphérique hôte (chez 40.31.1.47) sur le réseau interne à tous les périphériques sur l'Internet jusqu'à ce que l'authentification du navigateur soit exécutée avec l'utilisation du Seveur mandataire d'authentification. La liste de contrôle d'accès (ACL) passée vers le bas du serveur (**TCP d'autorisation|IP|l'ICMP tout**) en ajoute la POST-autorisation d'entrées dynamiques à la liste d'accès 116 qui permettent temporairement l'accès du PC d'hôte à l'Internet.

Référez-vous à configurer le Seveur mandataire d'authentification pour plus d'informations sur le Seveur mandataire d'authentification.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

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

Remarque: La commande de **proxy d'authentification d'IP** a été introduite dans la version de logiciel 12.0.5.T de Pare-feu Cisco IOS.

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.

Conventions

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

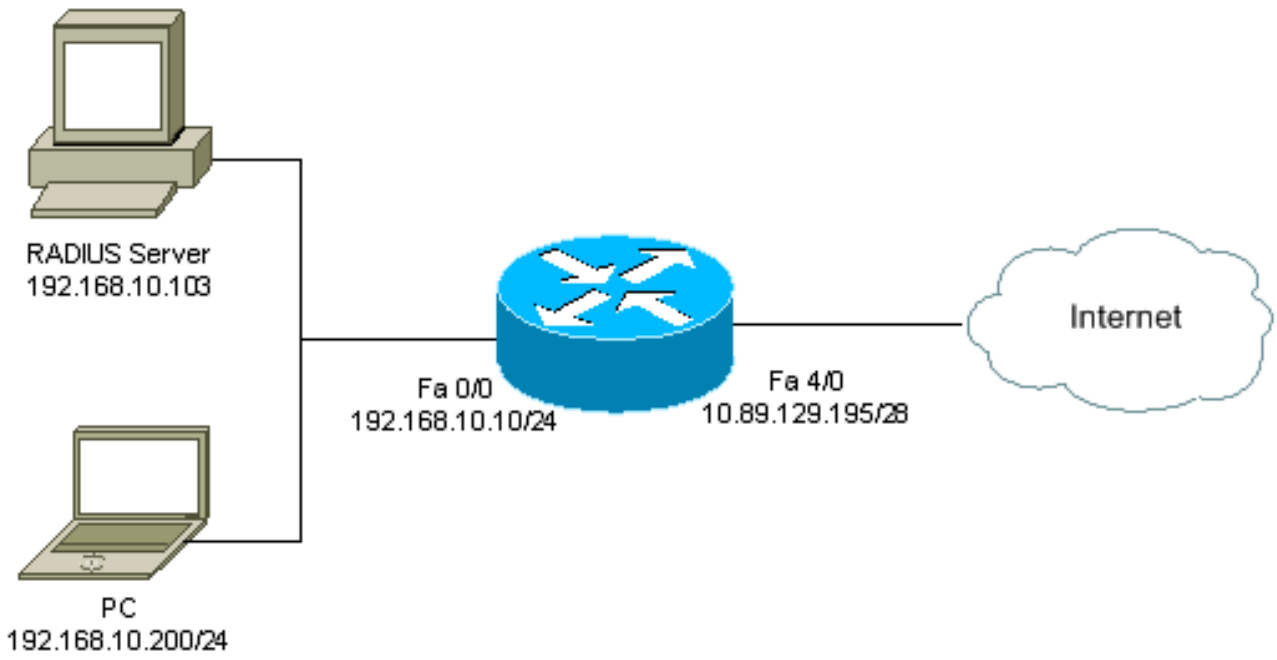
Configurez

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

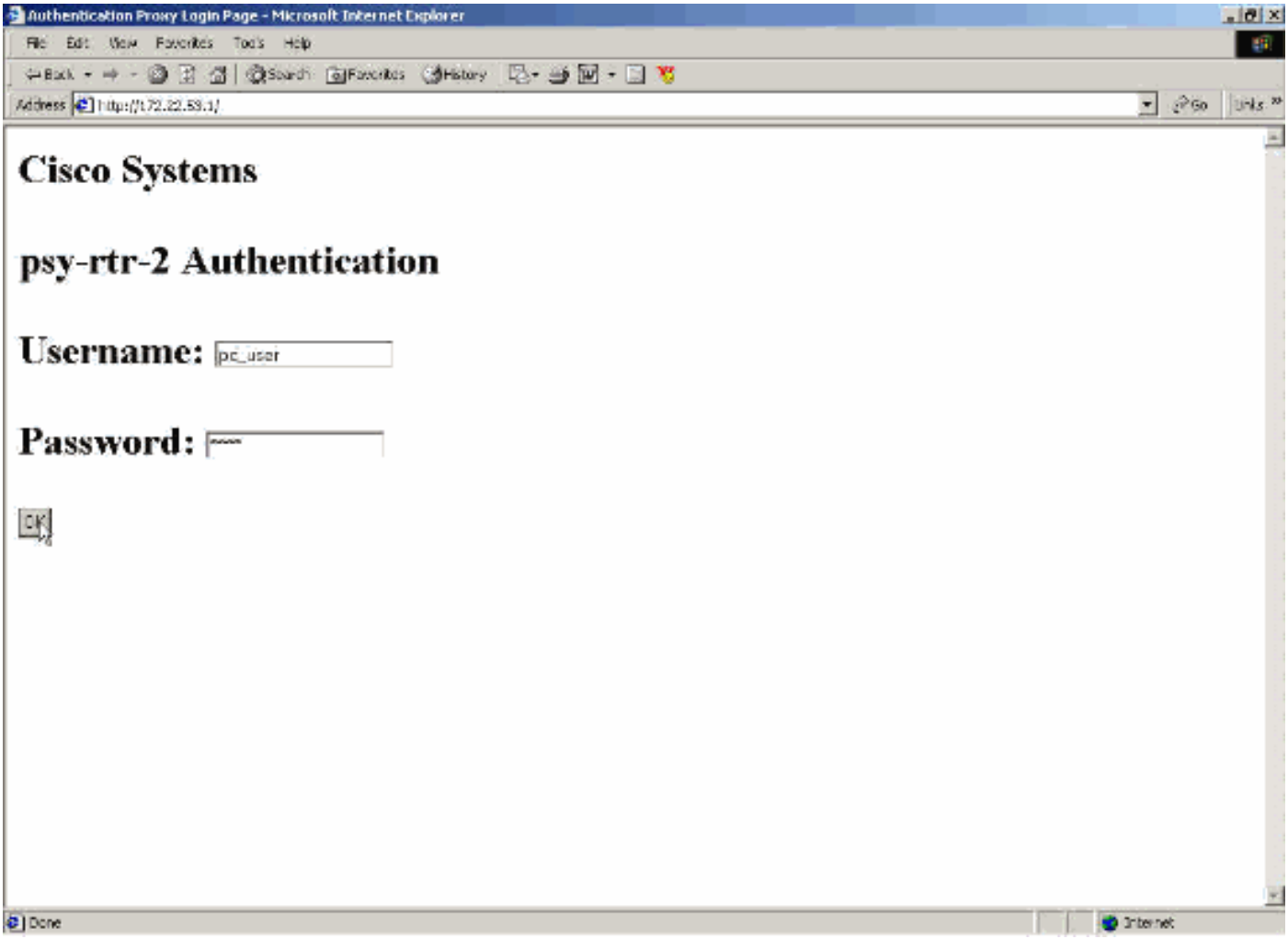
Ce document utilise la configuration suivante :

Routeur 7206

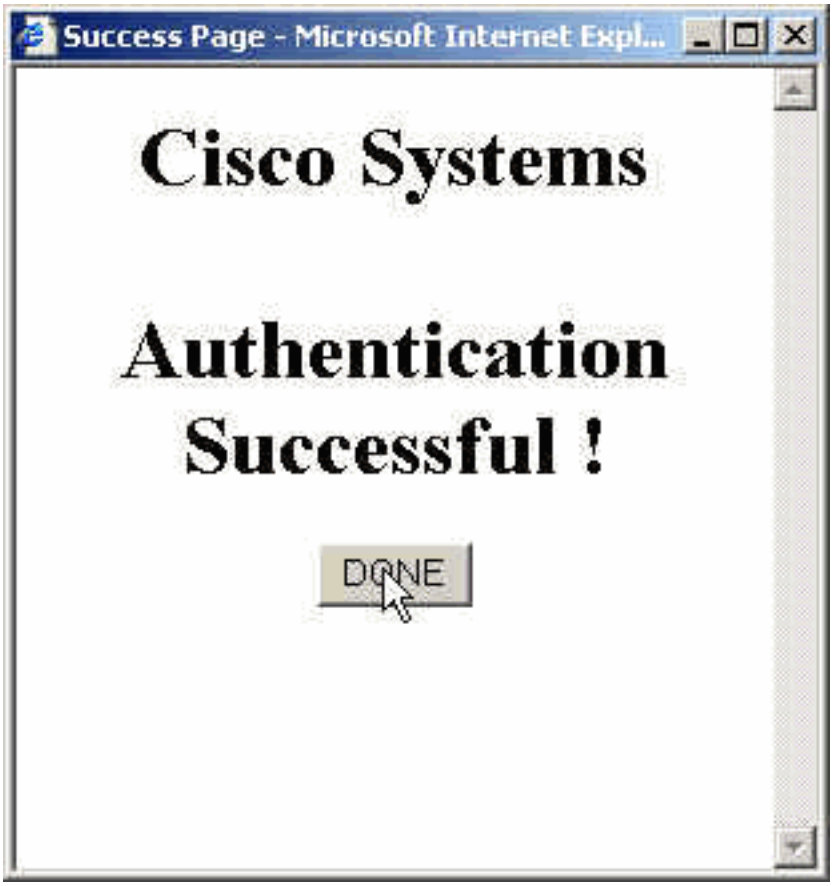
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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 les captures d'écran prises du PC qui affichent la procédure d'authentification. La première capture affiche à la fenêtre où un utilisateur écrit le nom d'utilisateur et mot de passe pour l'authentification et l'appuie sur **CORRECT**.



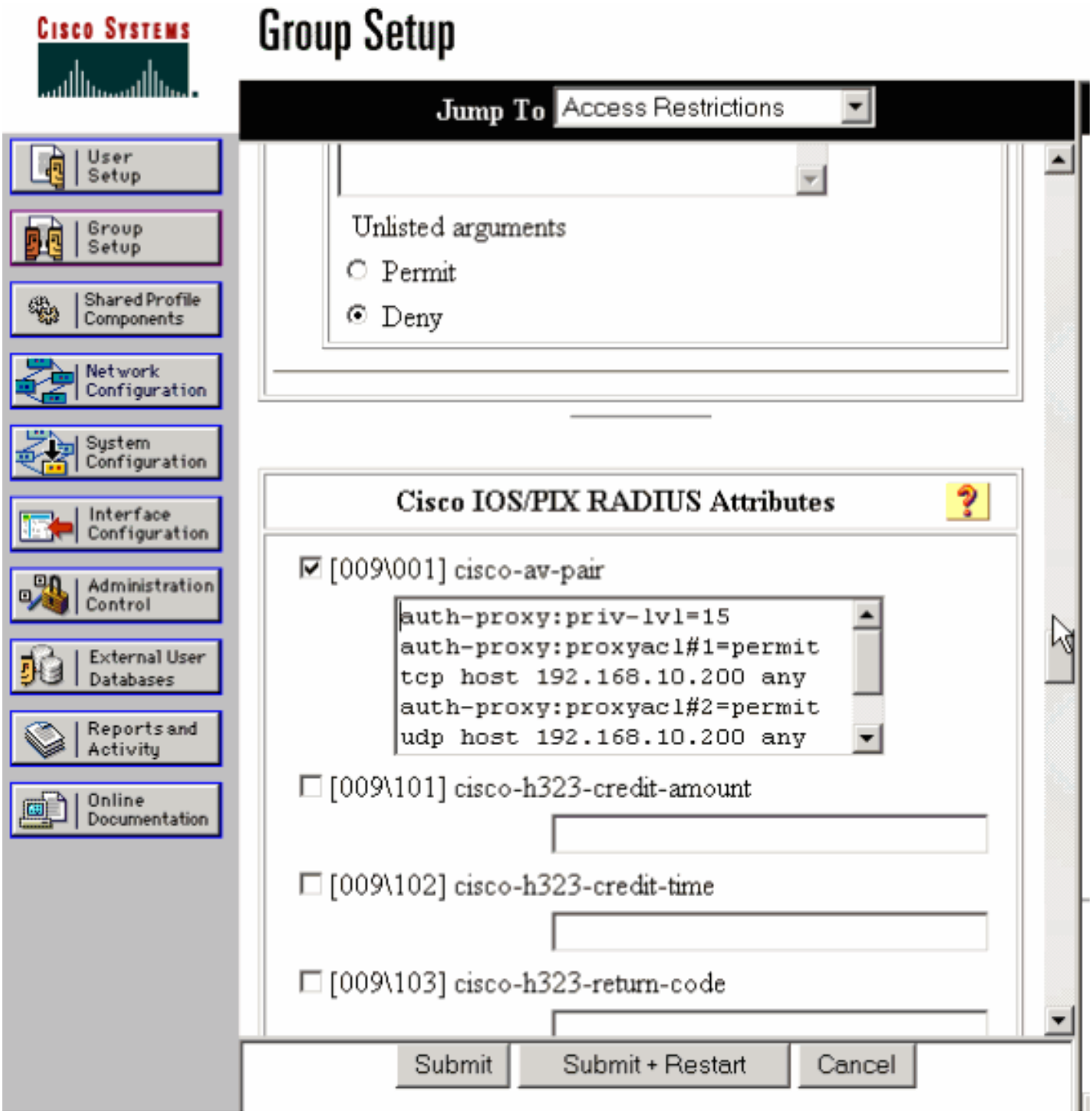
Si l'authentification est réussie, cette fenêtre apparaît.



Le serveur de RAYON doit être configuré avec le proxy ACLs qui sont appliqué. Dans cet exemple, ces rubriques de liste ACL sont appliqués. Ceci permet au PC pour 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 de Cisco ACS affiche où écrire le proxy ACLs.



Remarque: Référez-vous à configurer le Seveur mandataire d'authentification pour plus d'informations sur la façon configurer le serveur RADIUS/TACACS+.

Vérifiez

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 la norme et l'ACLs étendu configurés sur le Pare-feu (inclut les rubriques de liste ACL dynamiques). Les rubriques de liste ACL dynamiques sont ajoutés et retirés périodiquement basé en fonction, que l'utilisateur authentifie ou pas.

- **cache de show ip auth-proxy** — Affiche les entrées de Seveur mandataire d'authentification ou la configuration du proxy d'authentification courante. Le mot clé de cache pour répertorier l'adresse IP d'hôte, le numéro de port de source, la valeur du dépassement de durée pour le Seveur mandataire d'authentification, et l'état pour les connexions qui utilisent le Seveur mandataire d'authentification. Si l'état de Seveur mandataire d'authentification est HTTP_ESTAB, l'authentification de l'utilisateur est un succès.

Dépannez

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

Pour ces commandes, avec l'autre information de dépannage, référez-vous au Seveur mandataire d'authentification de dépannage.

Remarque: Référez-vous aux informations importantes 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