Autenticação de Proxy de Autenticação de Saída - Sem Firewall do Cisco IOS ou Configuração de NAT

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configuração](#)
[Autenticação no PC](#)
[Verificar](#)
[Troubleshoot](#)
[Informações Relacionadas](#)

Introduction

O recurso Proxy de Autenticação permite que os usuários façam login na rede ou acessem a Internet via HTTP, com seus perfis de acesso específicos automaticamente recuperados e aplicados de um servidor RADIUS ou TACACS+. Os perfis de usuário estão ativos somente quando há tráfego ativo dos usuários autenticados.

Esta configuração de exemplo bloqueia o tráfego do dispositivo de host (em 40.31.1.47) na rede interna para todos os dispositivos na Internet até que a autenticação do navegador seja executada com o uso do proxy de autenticação. A lista de controle de acesso (ACL) passada do servidor (**permit tcp|ip|icmp any any**) adiciona entradas dinâmicas pós-autorização à lista de acesso 116 que permitem temporariamente o acesso do PC host à Internet.

Consulte Configuração do Proxy de Autenticação para obter mais informações sobre o Proxy de Autenticação.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS® versão 12.2(15)T
- Cisco 7206 Router

Observação: o comando **ip auth-proxy** foi introduzido no Cisco IOS Firewall Software Release 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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

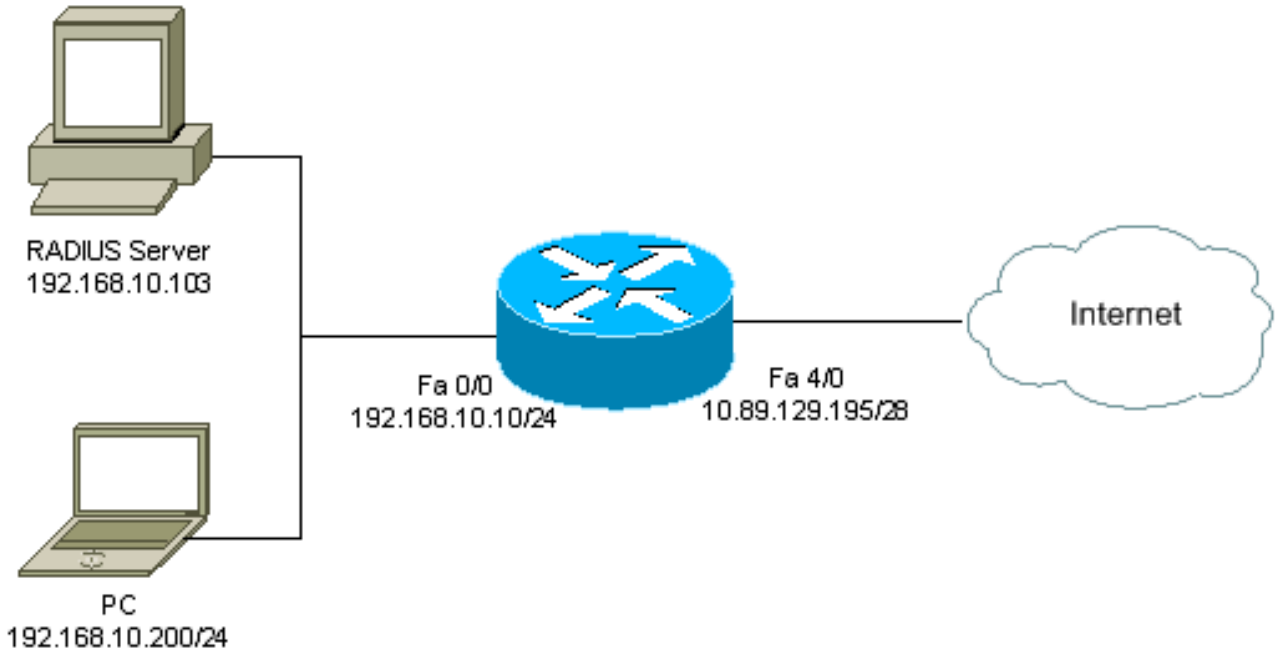
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração

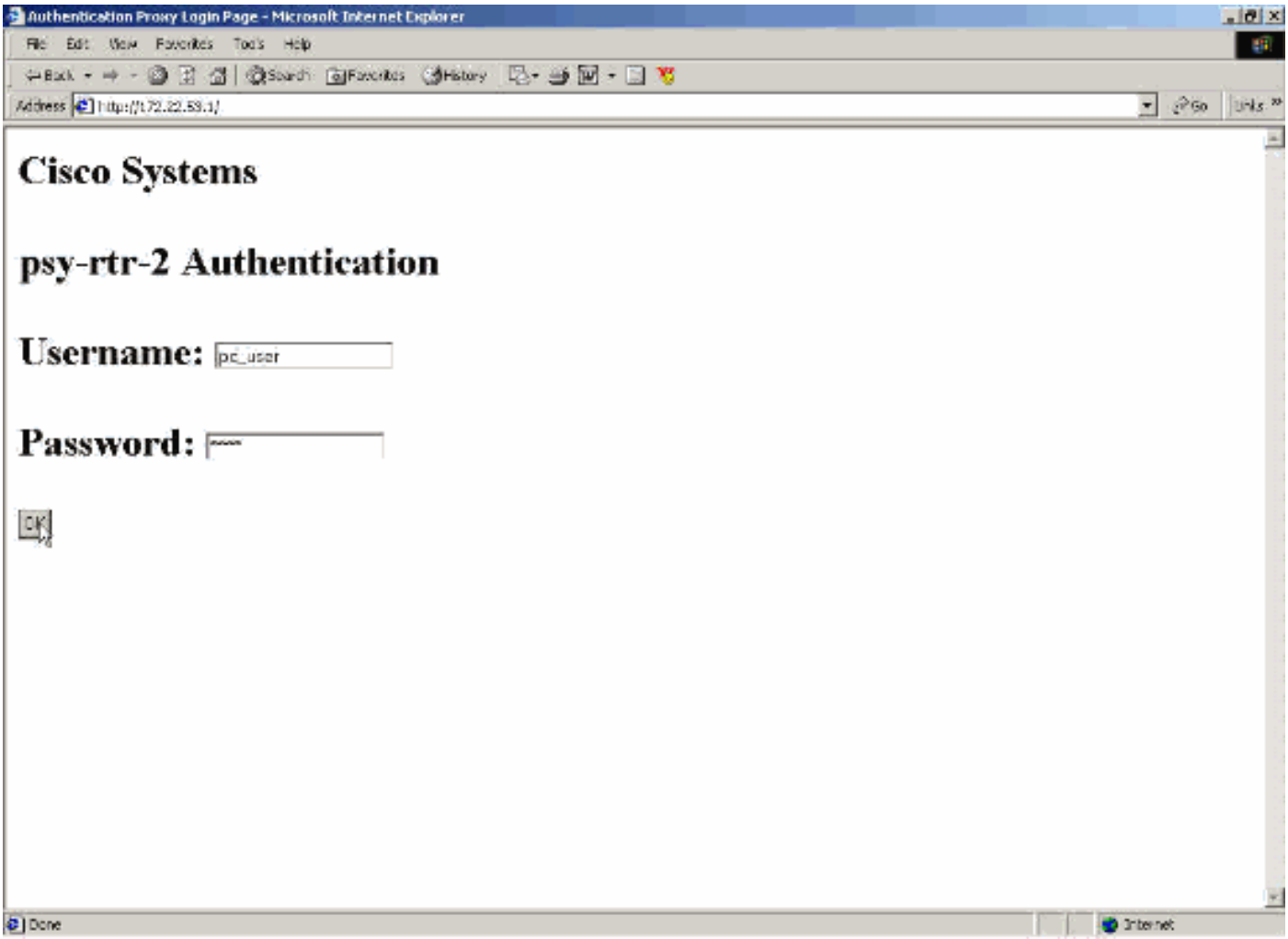
Este documento utiliza esta configuração:

7206 Router

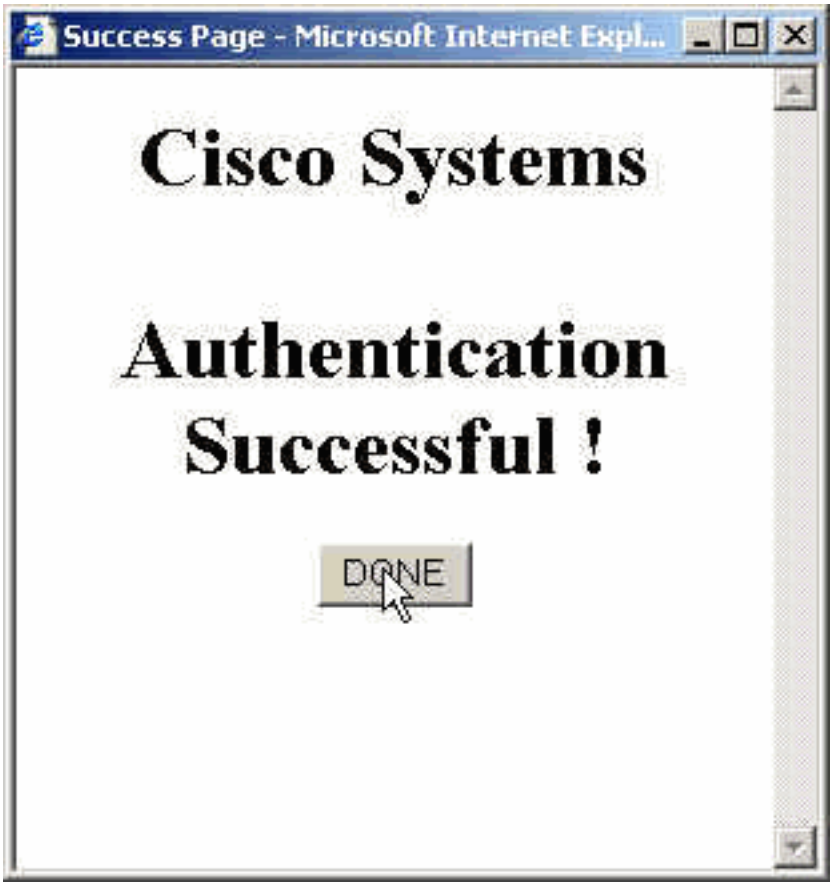
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

Autenticação no PC

Esta seção fornece capturas de tela tiradas do PC que mostram o procedimento de autenticação. A primeira captura mostra a janela onde um usuário insere o nome de usuário e a senha para autenticação e pressiona **OK**.



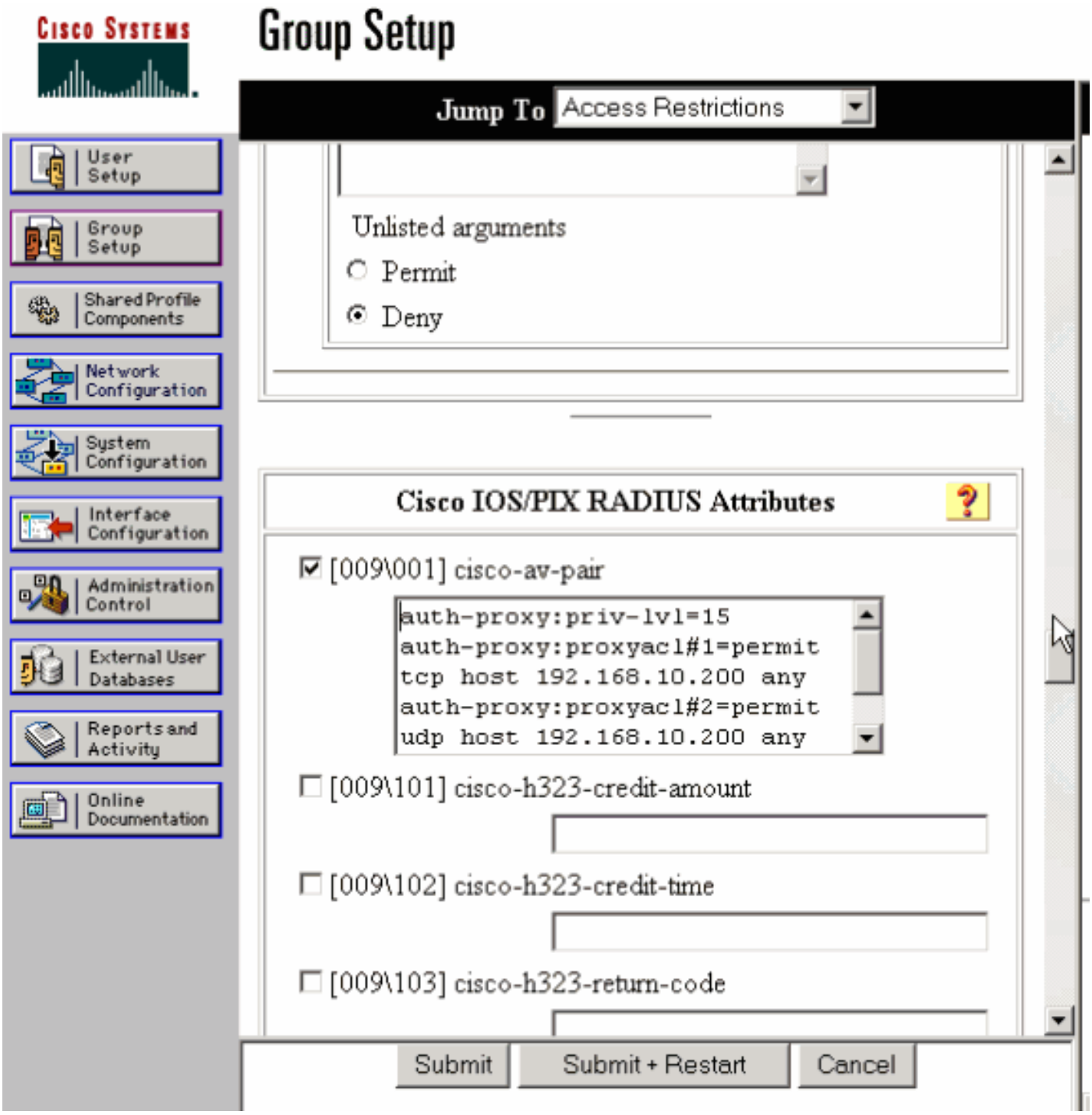
Se a autenticação for bem-sucedida, esta janela será exibida.



O servidor RADIUS deve ser configurado com as ACLs de proxy aplicadas. Neste exemplo, essas entradas da ACL são aplicadas. Isso permite que o PC se conecte a qualquer dispositivo.

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

Esta janela do Cisco ACS mostra onde inserir as ACLs de proxy.



Observação: consulte Configurando o proxy de autenticação para obter mais informações sobre como configurar o servidor RADIUS/TACACS+.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **show ip access-lists** —Exibe as ACLs padrão e estendidas configuradas no firewall (inclui entradas de ACL dinâmicas). As entradas dinâmicas da ACL são adicionadas e removidas periodicamente com base na autenticação ou não do usuário.

- **show ip auth-proxy cache** — Exibe as entradas do Proxy de Autenticação ou a configuração do Proxy de Autenticação em execução. A palavra-chave cache para listar o endereço IP do host, o número da porta de origem, o valor de tempo limite para o Proxy de Autenticação e o estado das conexões que usam o Proxy de Autenticação. Se o estado do Proxy de Autenticação for HTTP_ESTAB, a autenticação do usuário será um sucesso.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para esses comandos, juntamente com outras informações de troubleshooting, consulte Proxy de Autenticação de Troubleshooting.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Informações Relacionadas

- Página de suporte de firewall do IOS
- Página de Suporte do TACACS/TACACS+
- TACACS+ na Documentação do IOS
- Página de suporte RADIUS
- RADIUS em Documentação de IOS
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems