

Autenticação do proxy de autenticação de partida - Nenhuma Cisco IOS Firewall ou configuração de NAT

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração](#)

[Autenticação no PC](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

A característica do Proxy de autenticação permite que os usuários entrem à rede ou alcançar o Internet através do HTTP, com seu acesso específico perfila recuperado automaticamente e aplicado de um server do RAIO, ou TACACS+. Os perfis de usuário são ativos somente quando há um tráfego ativo dos usuários autenticados.

Esta configuração de exemplo obstrui o tráfego do dispositivo host (em 40.31.1.47) na rede interna a todos os dispositivos no Internet até que a autenticação de navegador esteja executada com o uso do Proxy de autenticação. O Access Control List (ACL) passado para baixo do server (**licença tcp|ip|o ICMP todo o algum**) adiciona as entradas dinâmica pós-autorização à lista de acessos 116 que permitem temporariamente o acesso do host PC ao Internet.

Refira [configurar o Proxy de autenticação](#) para obter mais informações sobre do Proxy de autenticação.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

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

Nota: O comando `ip auth-proxy` foi introduzido no Software Release 12.0.5.T do Cisco IOS Firewall.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

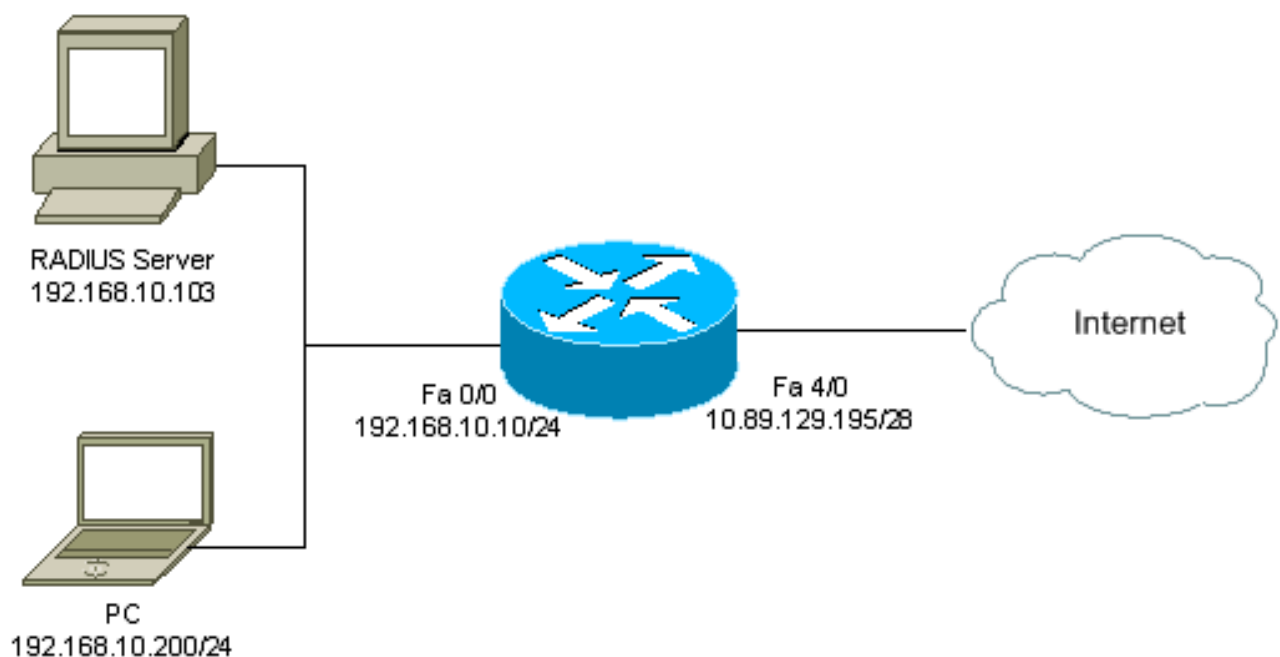
Configurar

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

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para 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:

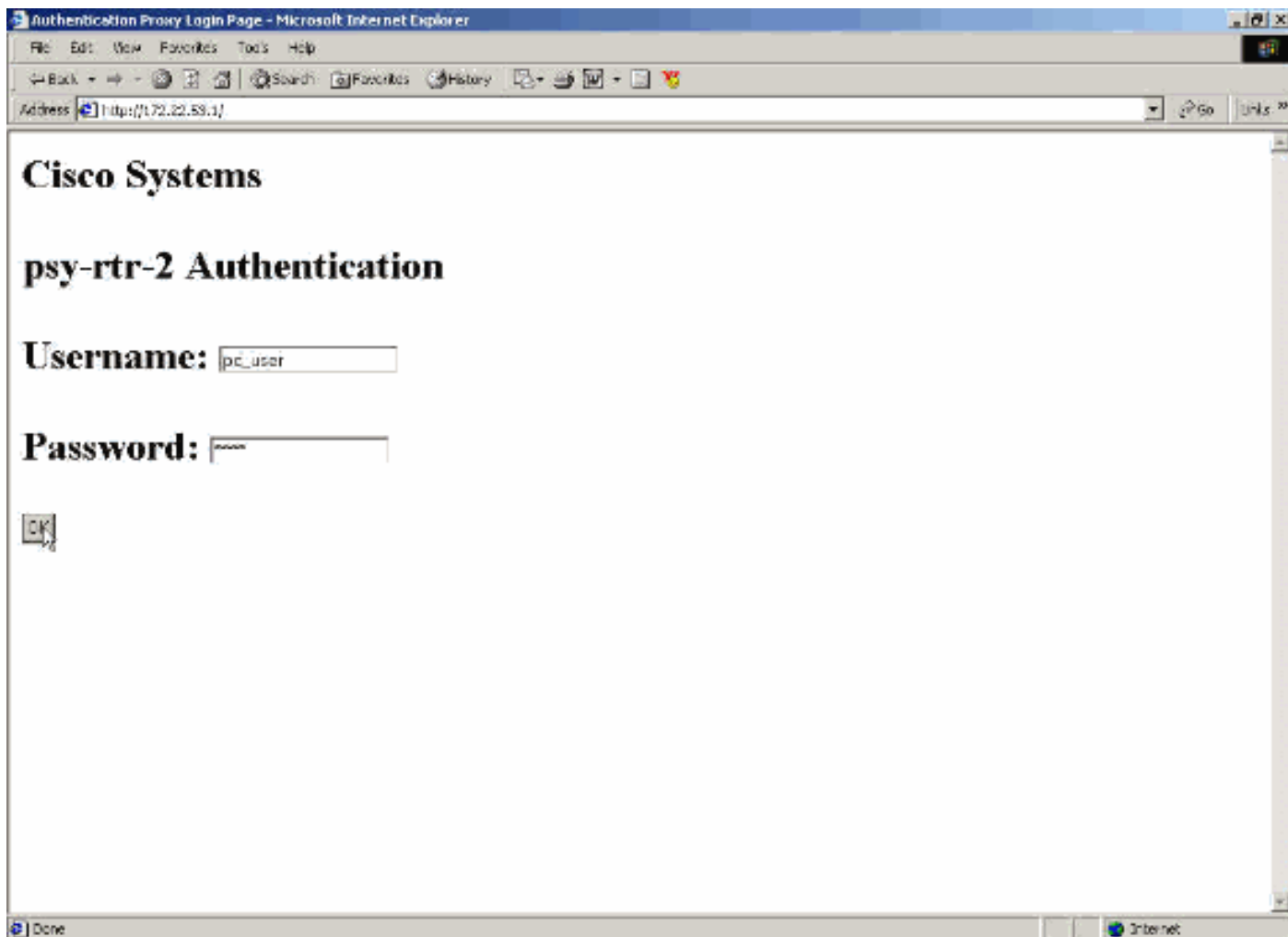
7206 Router

```
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

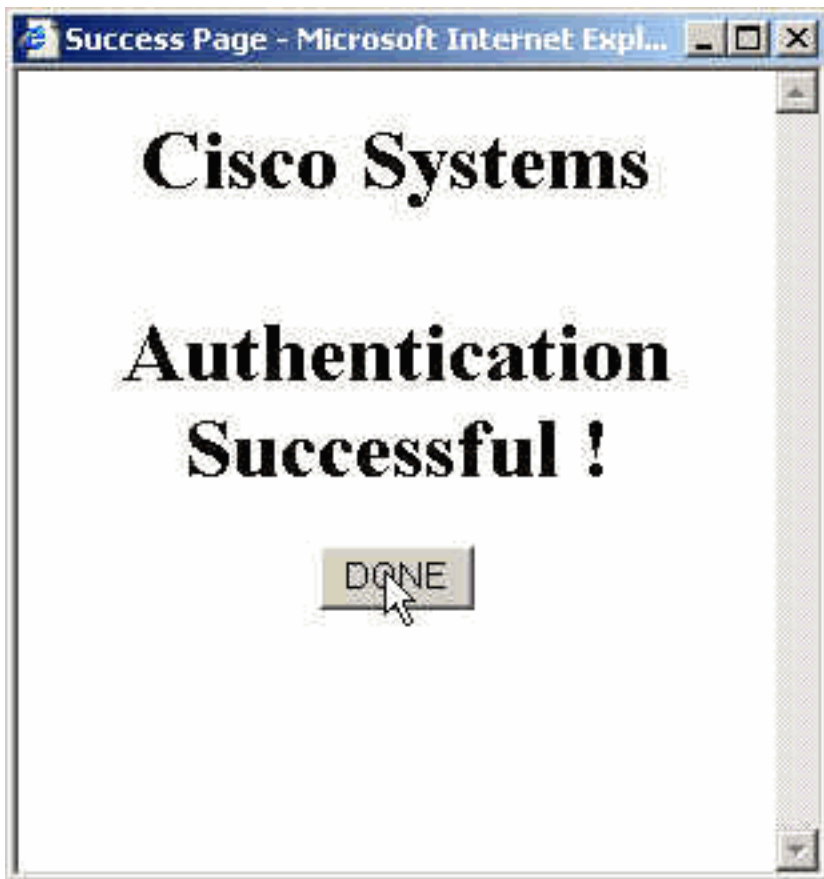
!--- Enable AAA. aaa authentication login default group
radius none !--- Use RADIUS to authenticate users. aaa
authorization exec default group radius none aaa
authorization auth-proxy default group radius !---
Utilize RADIUS for auth-proxy authorization. aaa
session-id common ip subnet-zero ! ip cef ! 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 as capturas de tela tomadas do PC que mostram o procedimento de autenticação. A primeira captura mostra ao indicador onde um usuário incorpora o nome de usuário e senha para a autenticação e o pressiona **ESTÁ BEM**.



Se a autenticação é bem sucedida, este indicador aparece.



O servidor Radius deve ser configurado com o proxy ACL que é aplicado. Neste exemplo, estas entradas ACL são aplicadas. Isto permite o PC conectar a todo o 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 de ACS de Cisco mostra onde entrar no proxy ACL.



Group Setup

Jump To Access Restrictions

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Unlisted arguments

Permit

Deny

Cisco IOS/PIX RADIUS Attributes ?

[009\001] cisco-av-pair

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit
tcp host 192.168.10.200 any
auth-proxy:proxyacl#2=permit
udp host 192.168.10.200 any
```

[009\101] cisco-h323-credit-amount

[009\102] cisco-h323-credit-time

[009\103] cisco-h323-return-code

Submit Submit + Restart Cancel

Nota: Refira [configurar o Proxy de autenticação](#) para obter mais informações sobre de como configurar o server RADIUS/TACACS+.

Verificar

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

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre listas de acesso IP** — Indica o padrão e os ACL estendido configurados no Firewall (inclui entradas ACL dinâmicas). As entradas ACL dinâmicas são adicionadas e removidas baseado periodicamente sobre se o usuário autentica ou não.

- **mostre o esconderijo do ip auth-proxy** — Indica as entradas do Proxy de autenticação ou a configuração do proxy de autenticação running. A palavra-chave do esconderijo para alistar o endereço IP de Um ou Mais Servidores Cisco ICM NT do host, o número de porta de origem, o valor de timeout para o Proxy de autenticação, e o estado para as conexões que usam o Proxy de autenticação. Se o estado do Proxy de autenticação é HTTP_ESTAB, a autenticação de usuário é um sucesso.

Troubleshooting

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

Para estes comandos, junto com a outra informação de Troubleshooting, refira [pesquisando defeitos o Proxy de autenticação](#).

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](#)