Autenticación de Proxy de Autenticación Saliente - Sin Firewall Cisco IOS ni Configuración NAT

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Configurar](#)
[Diagrama de la red](#)
[Configuración](#)
[Autenticación en el PC](#)
[Verificación](#)
[Troubleshoot](#)
[Información Relacionada](#)

Introducción

La función Authentication Proxy permite a los usuarios iniciar sesión en la red o acceder a Internet a través de HTTP, con sus perfiles de acceso específicos recuperados y aplicados automáticamente desde un servidor RADIUS o TACACS+. Los perfiles de usuario están activos sólo cuando hay tráfico activo de los usuarios autenticados.

Esta configuración de ejemplo bloquea el tráfico desde el dispositivo host (en 40.31.1.47) en la red interna a todos los dispositivos en Internet hasta que se realice la autenticación del explorador con el uso de Authentication Proxy. La lista de control de acceso (ACL) transmitida desde el servidor (**permit tcp|ip|icmp any any**) agrega entradas dinámicas después de la autorización a la lista de acceso 116 que permiten temporalmente el acceso desde el equipo host a Internet.

Consulte Configuración del Proxy de Autenticación para obtener más información sobre el Proxy de Autenticación.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 12.2(15)T del software del IOS® de Cisco
- Cisco 7206 router

Nota: El comando **ip auth-proxy** se introdujo en la versión 12.0.5.T del software de firewall del IOS de Cisco.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

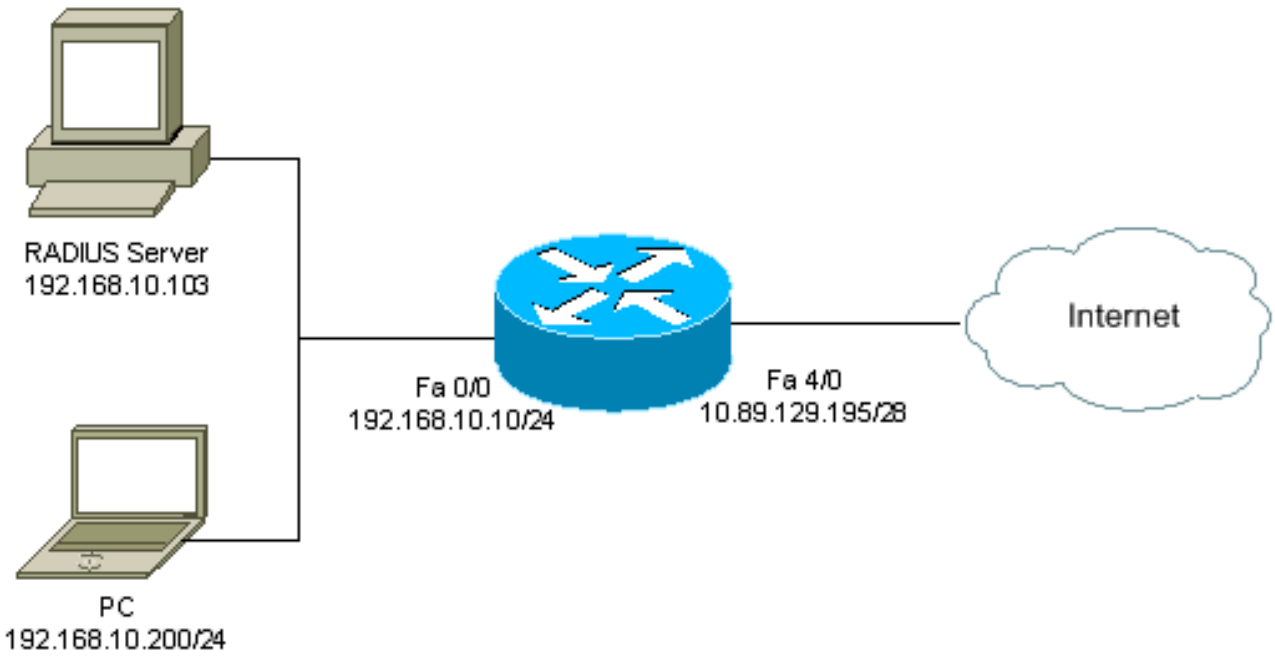
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración

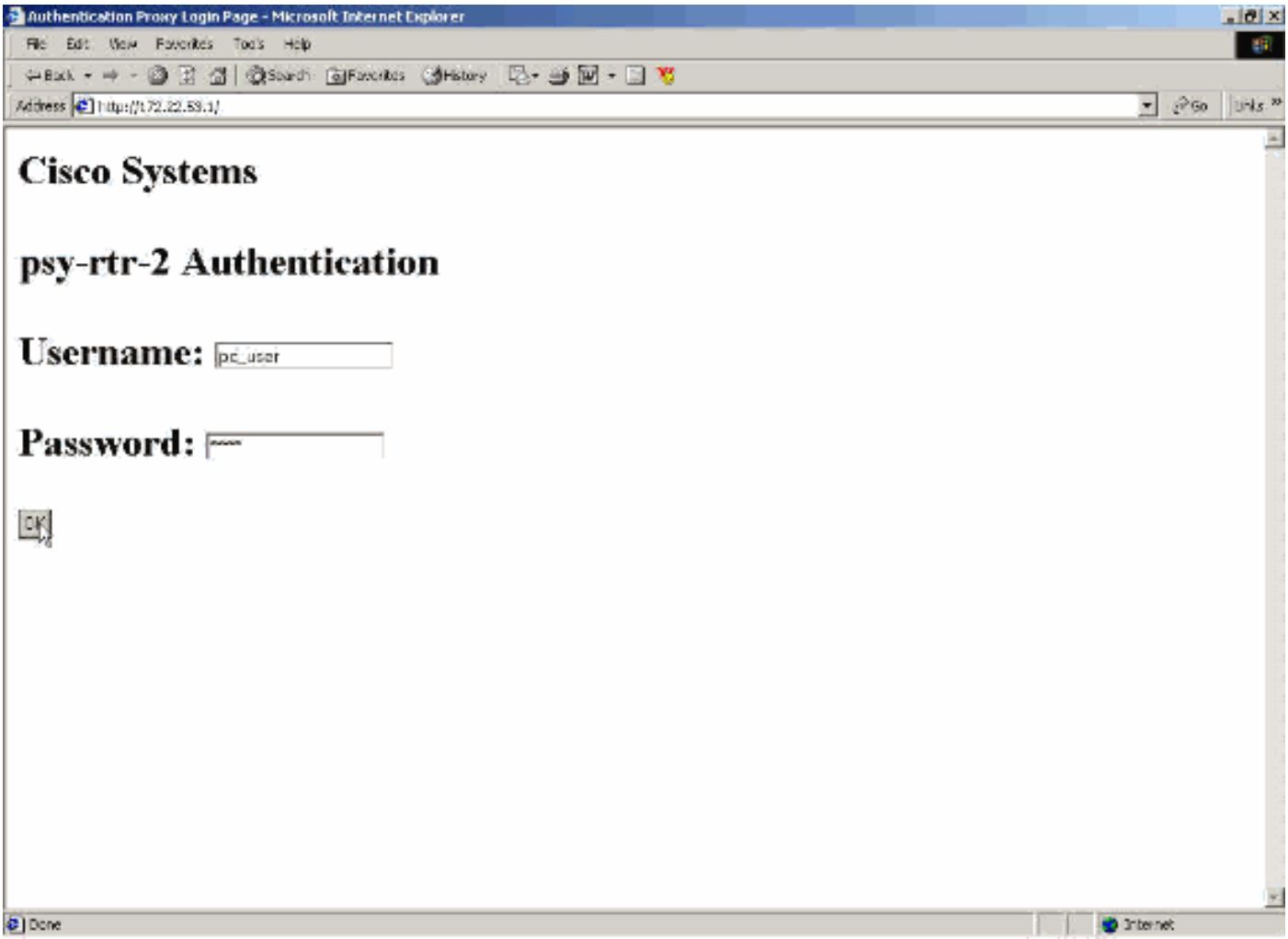
Este documento usa esta configuración:

Router 7206

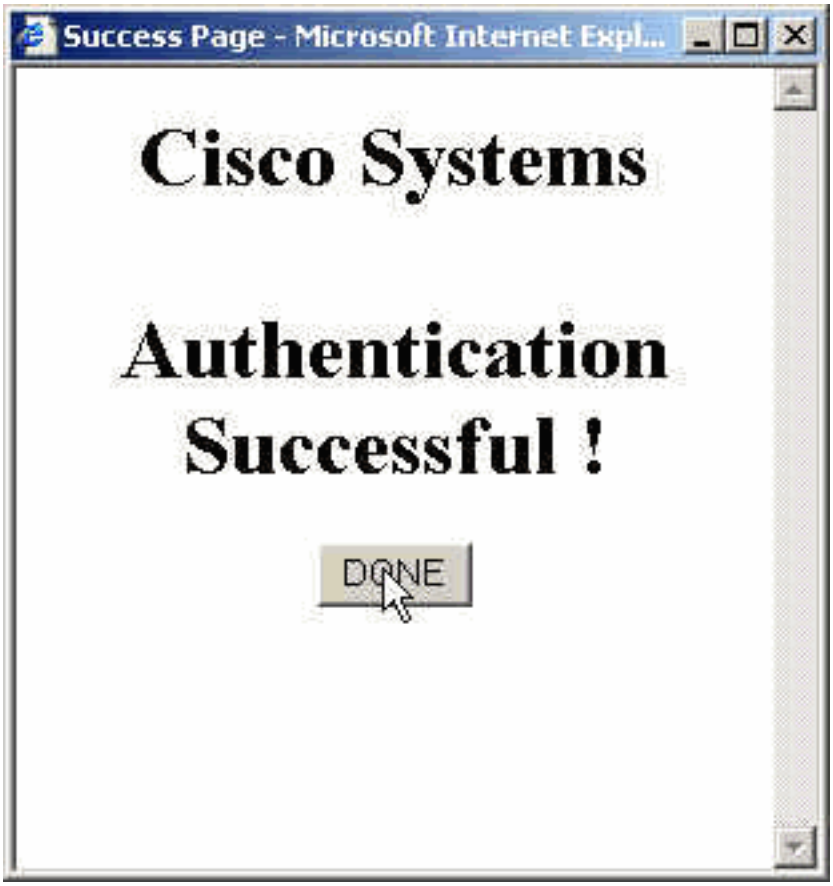
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

Autenticación en el PC

Esta sección proporciona capturas de pantalla tomadas del PC que muestran el procedimiento de autenticación. La primera captura muestra la ventana donde un usuario ingresa el nombre de usuario y la contraseña para la autenticación y presiona **OK**.



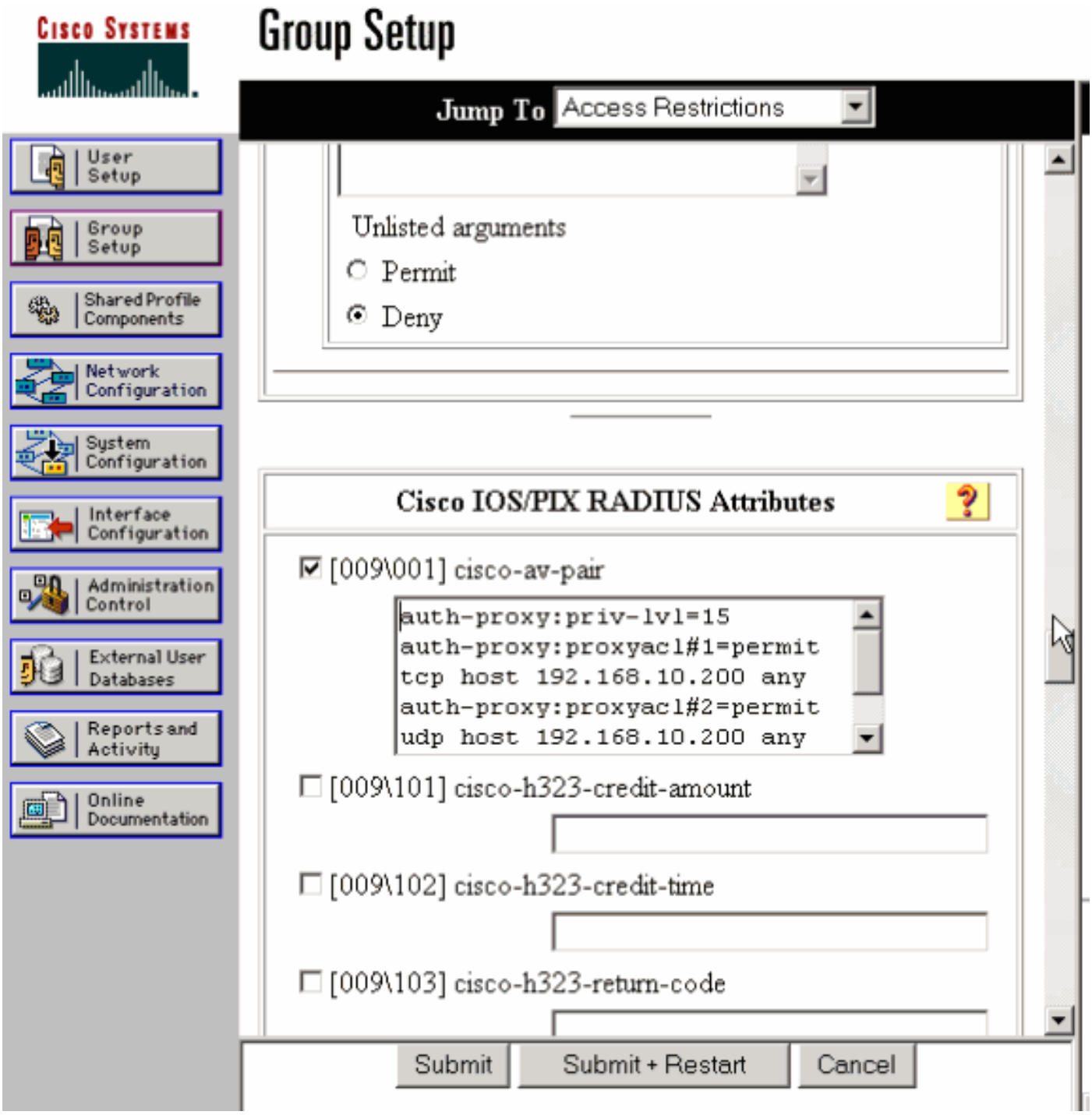
Si la autenticación es correcta, aparece esta ventana.



El servidor RADIUS debe configurarse con las ACL de proxy que se aplican. En este ejemplo, se aplican estas entradas de ACL. Esto permite que el PC se conecte a cualquier 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 ventana de Cisco ACS muestra dónde ingresar las ACL de proxy.



Nota: Consulte Configuración del Proxy de Autenticación para obtener más información sobre cómo configurar el servidor RADIUS/TACACS+.

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show ip access-lists**: muestra las ACL estándar y extendidas configuradas en el firewall (incluye entradas de ACL dinámicas). Las entradas de ACL dinámicas se agregan y eliminan periódicamente en función de si el usuario se autentica o no.

- **show ip auth-proxy cache**: muestra las entradas del Proxy de autenticación o la configuración del Proxy de autenticación en ejecución. La palabra clave cache para enumerar la dirección IP del host, el número de puerto de origen, el valor de tiempo de espera para el Proxy de autenticación y el estado para las conexiones que utilizan el Proxy de autenticación. Si el estado Proxy de autenticación es HTTP_ESTAB, la autenticación de usuario es correcta.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Para estos comandos, junto con otra información de resolución de problemas, consulte Resolución de problemas del Proxy de autenticación.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

Información Relacionada

- Página de soporte de firewall de IOS
- Página de soporte de TACACS/TACACS+
- TACACS+ en documentación de IOS
- Página de soporte de RADIUS
- RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) en documentación de IOS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems