Autenticación de servidor alterno de autenticación saliente - Ningún Firewall Cisco IOS o configuración del NAT

Contenido

Introducción

La característica del Proxy de autenticación permite que los usuarios inicien sesión a la red o acceder Internet vía el HTTP, con su acceso específico perfila extraído automáticamente y aplicado de un servidor RADIUS, o TACACS+. Los perfiles del usuario son activos solamente cuando hay tráfico activo de los usuarios autenticados.

Esta configuración de muestra bloquea el tráfico del dispositivo host (en 40.31.1.47) en la red interna a todos los dispositivos en Internet hasta que la autenticación de buscador se realice con el uso del Proxy de autenticación. El Access Control List (ACL) pasajero abajo del servidor (**permiso tcp|ip|el ICMP cualquier ninguno**) agrega el poste authorization de las entradas dinámicas a la lista de acceso 116 que permite temporalmente el acceso del host PC a Internet.

Refiera a configurar el Proxy de autenticación para más información sobre el Proxy de autenticación.

prerrequisitos

Requisitos

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.

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

Nota: Presentaron al **comando ip auth-proxy** en el Software Release 12.0.5.T del Firewall Cisco IOS.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

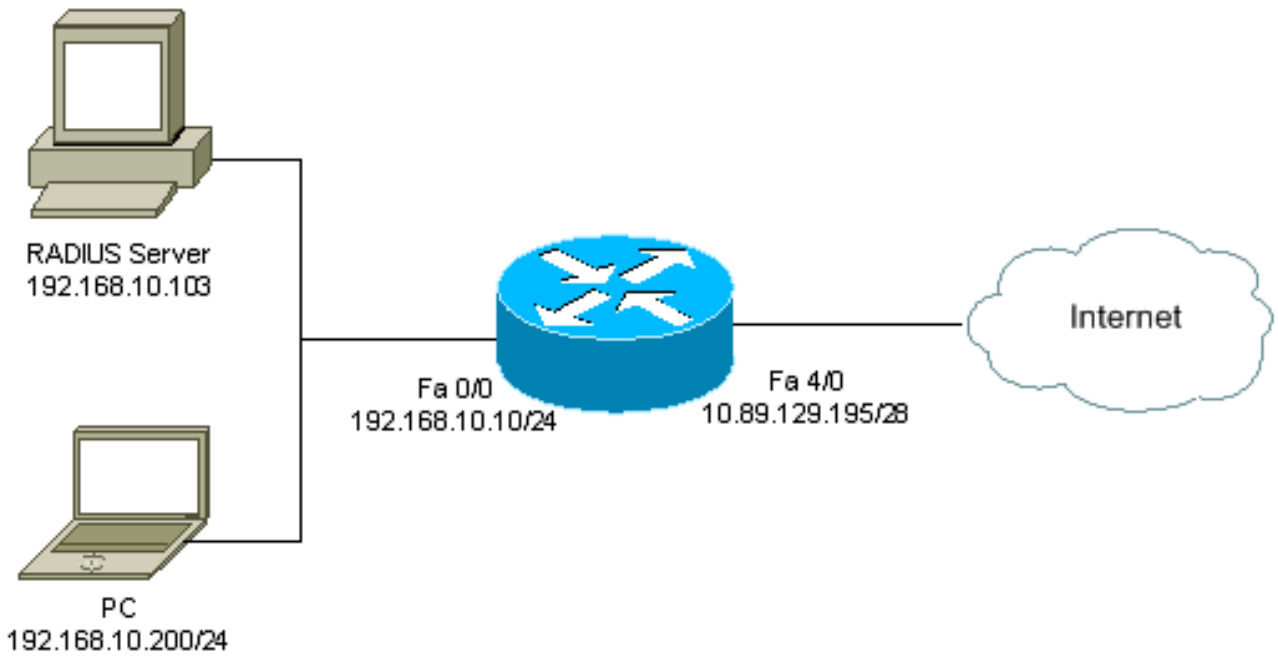
Configurar

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

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración

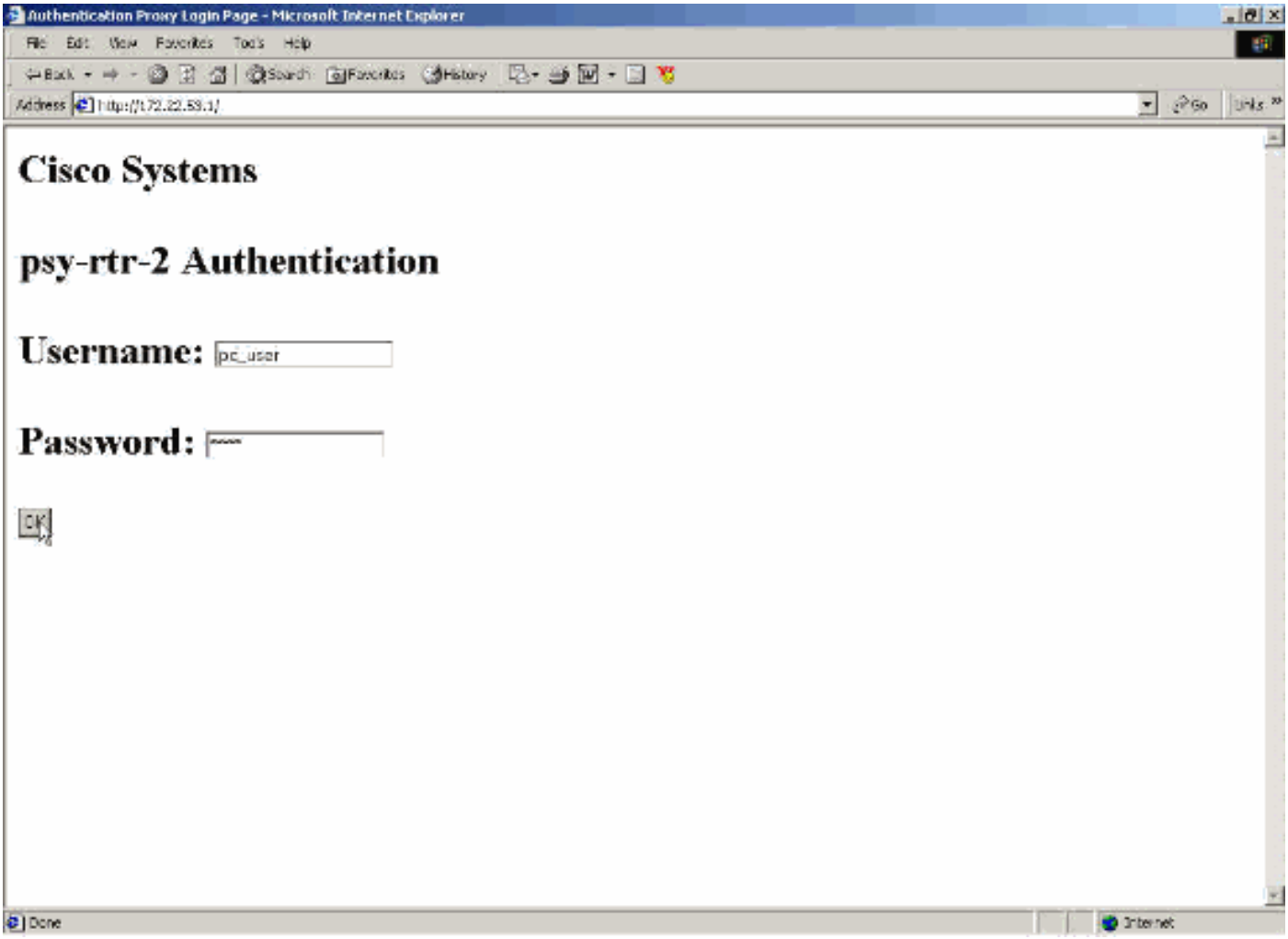
Este documento usa esta configuración:

7206 Router

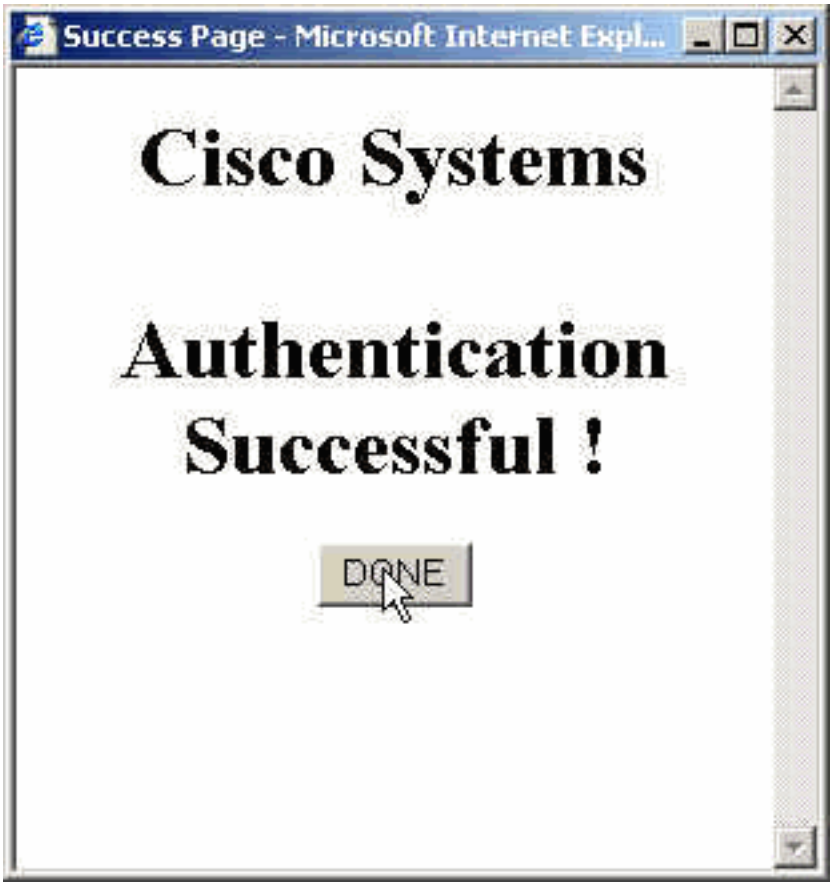
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

Autenticación en el PC

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



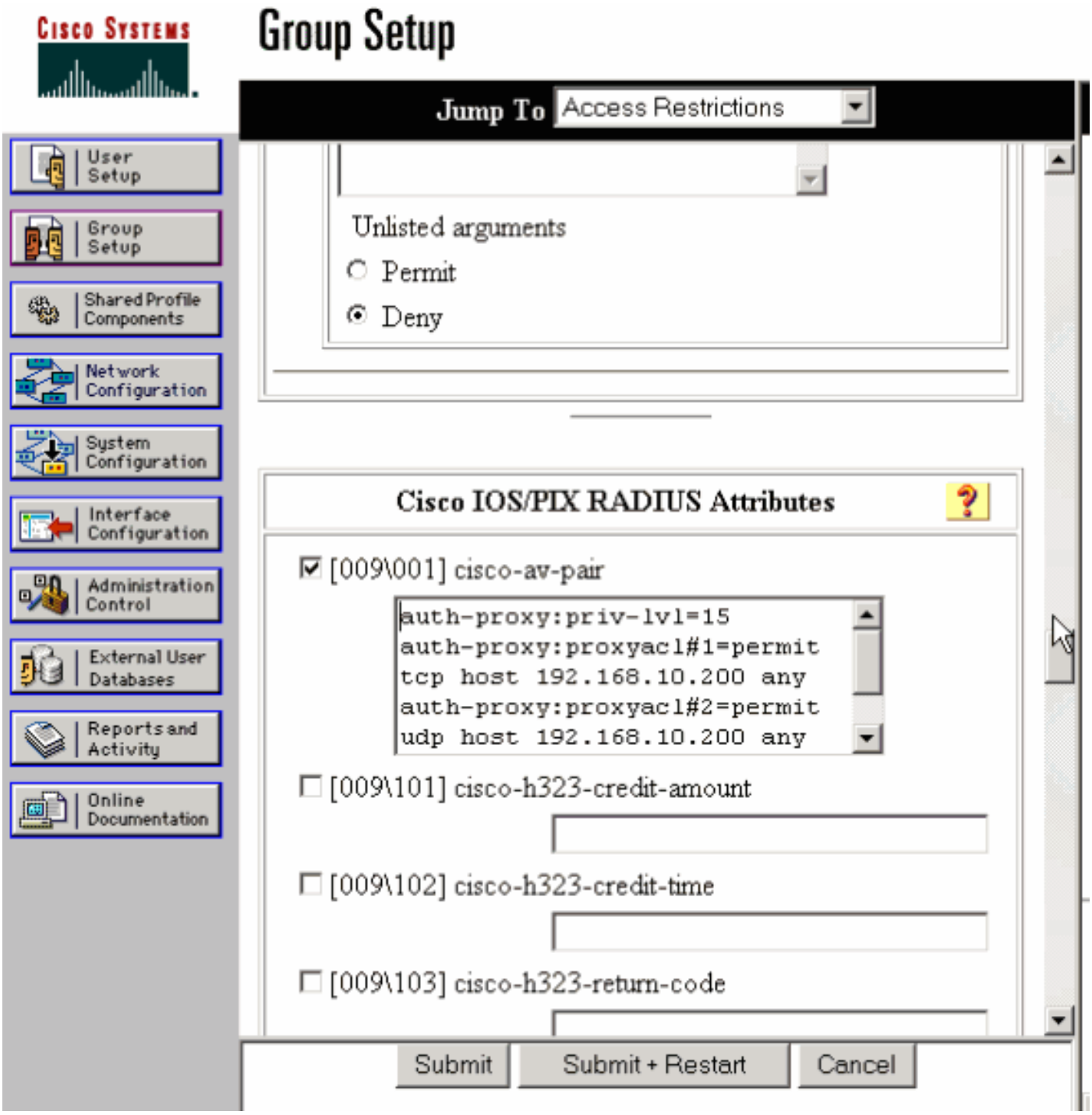
Si la autenticación es acertada, esta ventana aparece.



El servidor de RADIUS debe ser configurado con el proxy ACL que es aplicado. En este ejemplo, estas entradas ACL son aplicadas. Esto permite que el PC conecte con 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 ACS de Cisco muestra donde ingresar el proxy ACL.



Nota: Refiera a configurar el Proxy de autenticación para 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.

- **muestre las listas de acceso del IP** — Visualiza el estándar y los ACL ampliados configurados en el Firewall (incluye las entradas ACL dinámicas). Se agregan y se quitan las entradas ACL dinámicas basado periódicamente encendido si el usuario autentica o no.

- **muestre el caché del ip auth-proxy** — Visualiza las entradas del Proxy de autenticación o la configuración de proxy de autenticación corriente. La palabra clave del caché para enumerar la dirección IP del host, el número del puerto de origen, el valor de agotamiento del tiempo para el Proxy de autenticación, y el estado para las conexiones que utilizan el Proxy de autenticación. Si el estado del Proxy de autenticación está HTTP_ESTAB, la autenticación de usuario es un éxito.

Troubleshooting

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

Para estos comandos, junto con la otra información de Troubleshooting, refiera al Proxy de autenticación del troubleshooting.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando 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