出站的认证代理认证-没有Cisco IOS防火墙或NAT配置

目录

简介

认证代理功能允许用户登录到网络或通过 HTTP 访问 Internet，并会自动从 RADIUS 或 TACACS+ 服务器检索和应用其特定的访问配置文件。只有验证的用户有活动的流量时，用户配置文件才是有效的。

在使用认证代理执行浏览器身份验证之前，此配置示例会阻塞从内部网络上的主机设备（地址为 40.31.1.47）到 Internet 上的所有设备的流量。从服务器传送的访问控制列表 (ACL)(**permit tcp|ip|icmp any any**) 会将动态条目后授权添加到暂时允许从主机 PC 访问 Internet 的访问列表 116 中。

有关认证代理的详细信息，请参阅配置认证代理。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS® 软件版本 12.2(15)T

- Cisco 7206 路由器

注意： **ip auth-proxy** 命令在 Cisco IOS 防火墙软件版本 12.0.5.T 中引入。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

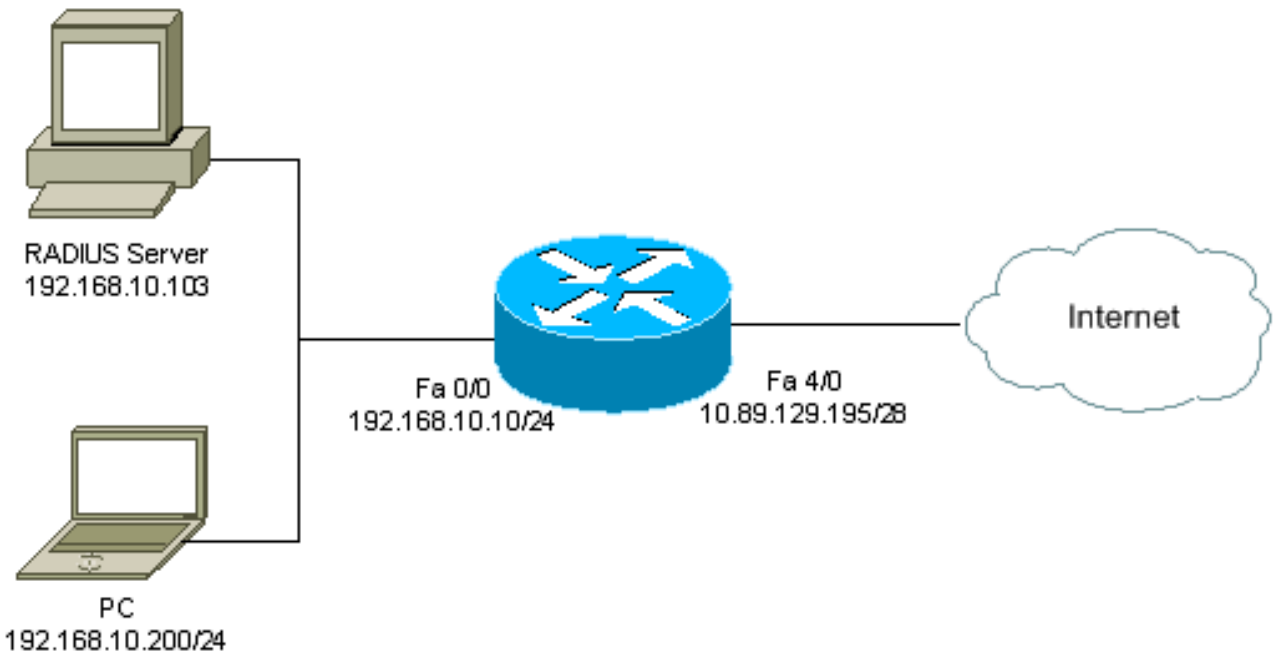
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

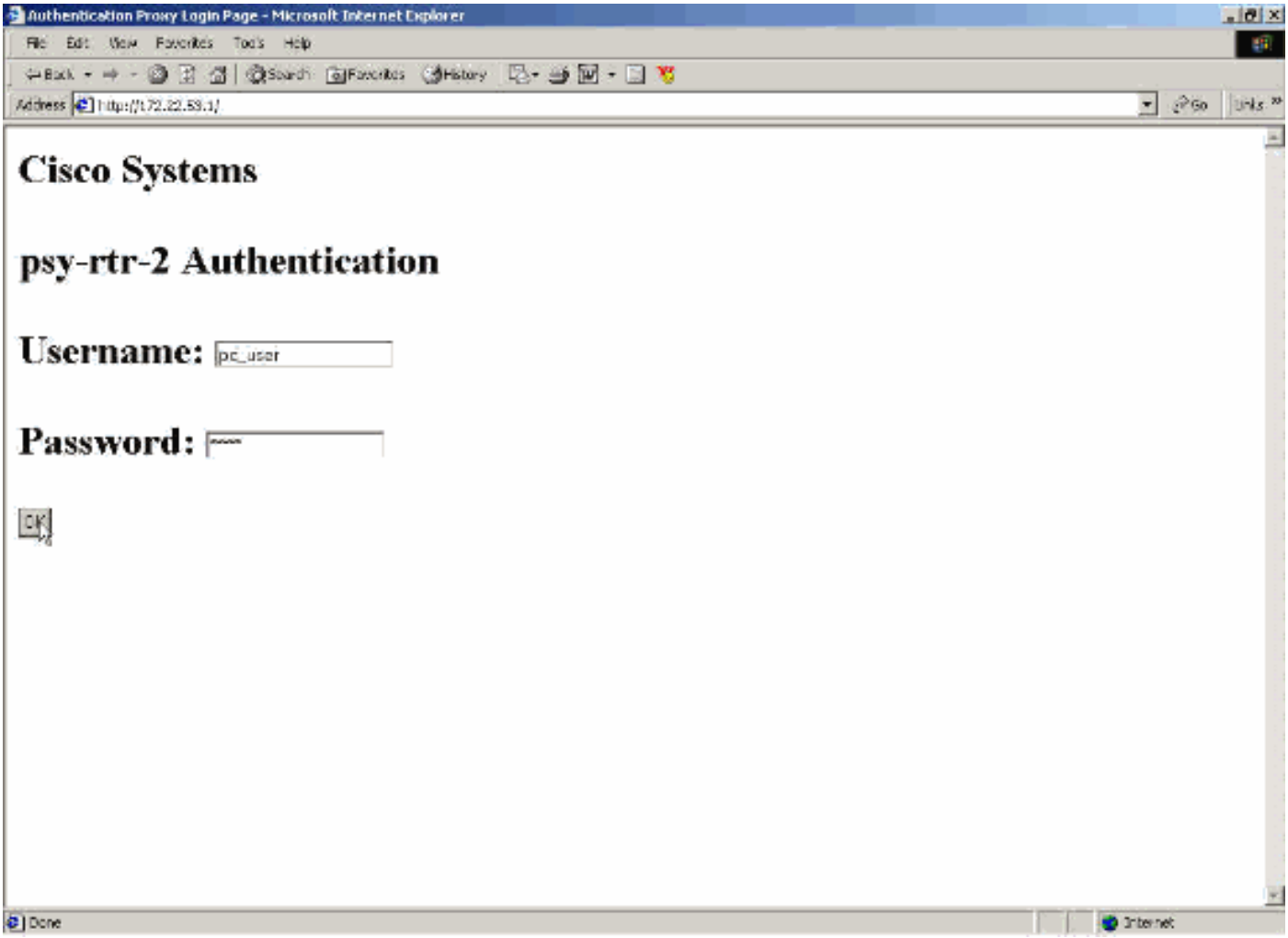
7206 路由器

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
```

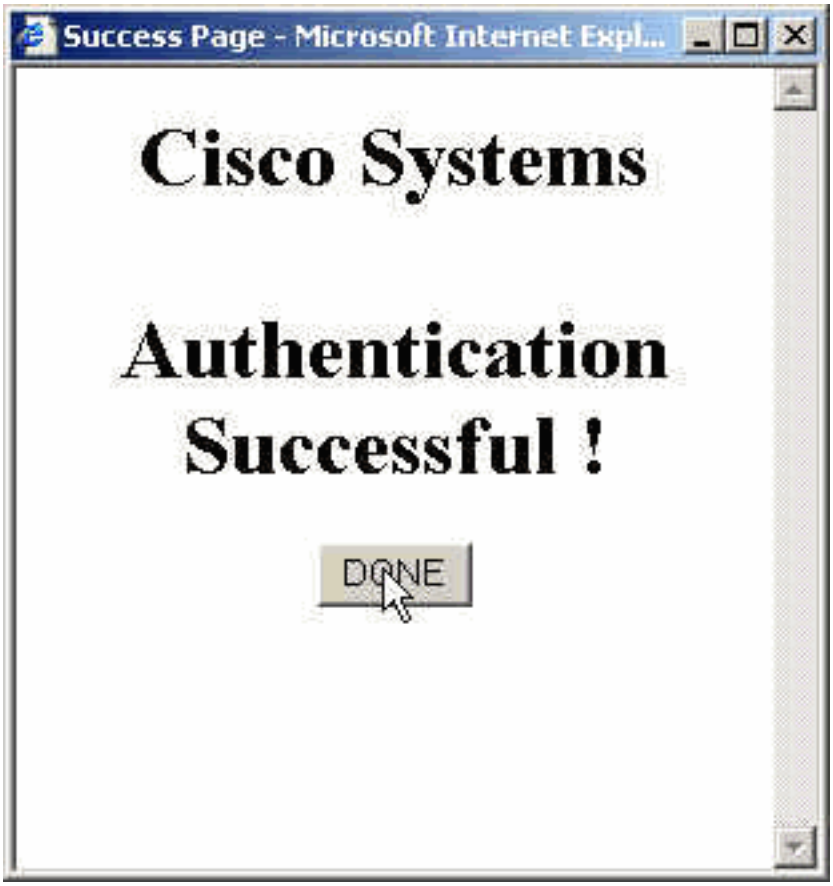
```
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

PC 上的身份验证

本部分提供了从显示身份验证过程的 PC 中获取的屏幕截图。第一个截图显示了一个窗口，用户在这里可以输入用户名和口令进行身份验证，然后按 OK。



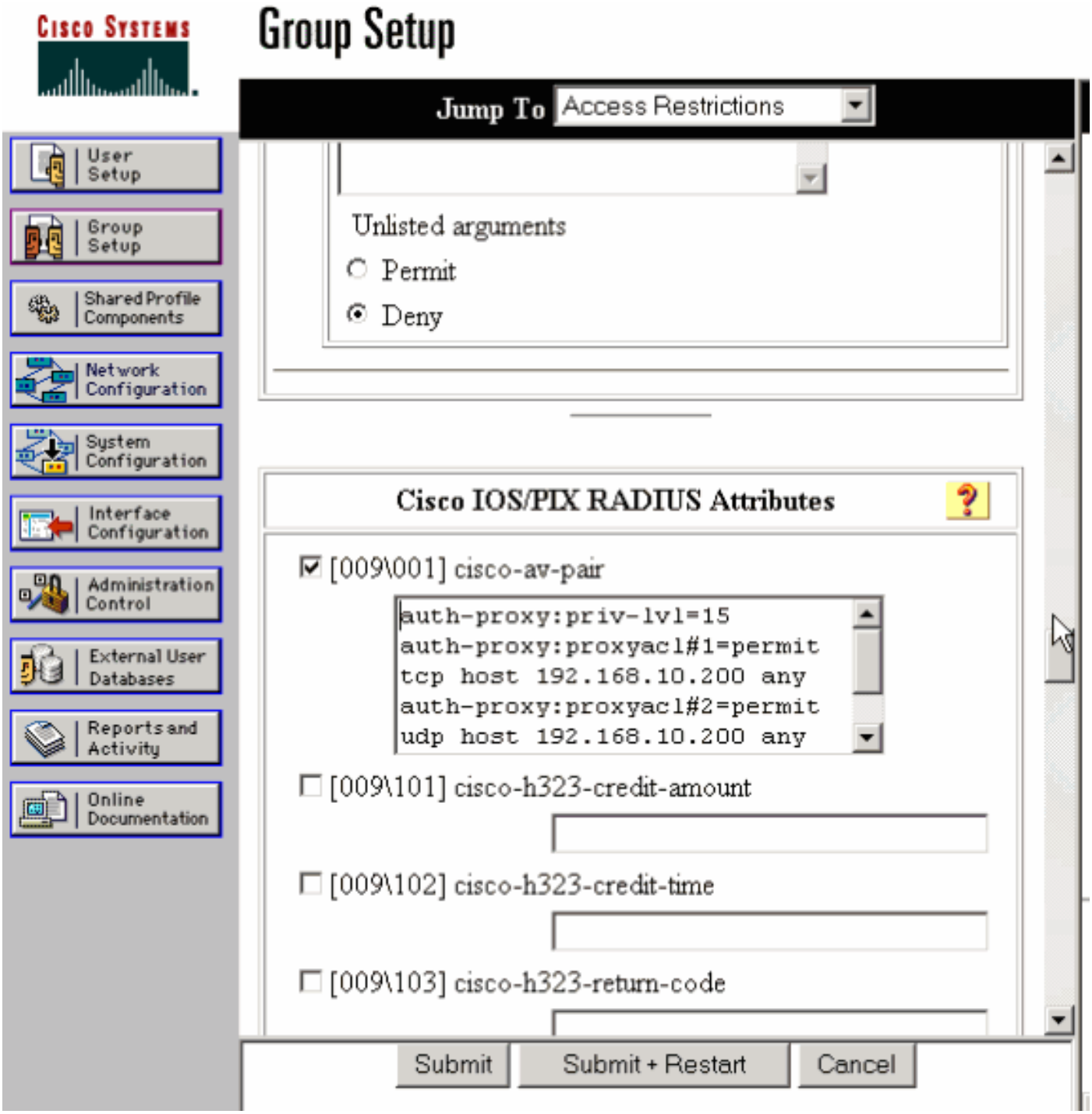
如果身份验证成功，会显示此窗口。



必须使用所应用的代理 ACL 配置 RADIUS 服务器。在本示例中，会应用这些 ACL 条目。这就可以让 PC 连接到任何设备。

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

此 Cisco ACS 窗口显示了代理 ACL 的输入位置。



注意： 有关如何配置 RADIUS/TACACS+ 服务器的详细信息，请参阅配置认证代理。

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show ip access-lists** - 显示在防火墙上配置的标准和扩展 ACL（包括动态 ACL 条目）。动态 ACL 条目会根据是否进行用户身份验证来定期添加和删除。
- **show ip auth-proxy cache** - 显示认证代理条目或运行中的认证代理配置。缓存关键字，用于列出主机 IP 地址、源端口号、认证代理超时值以及使用认证代理的连接的状态。如果认证代理状态是 HTTP_ESTAB，则用户身份验证成功。

故障排除

本部分提供的信息可用于对配置进行故障排除。

对于这些指令和其他故障排除信息，请参见排错认证代理。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

相关信息

- **IOS防火墙支持页面**
- **TACACS/TACACS+支持页面**
- **IOS 文档中的 TACACS+**
- **RADIUS 支持页**
- **IOS 文档中的 RADIUS**
- **请求注解 (RFC)**
- **技术支持和文档 - Cisco Systems**