인증 프록시 인증 아웃바운드 - Cisco IOS 방화벽 또는 NAT 컨피그레이션 없음

목차

소개

인증 프록시 기능을 사용하면 사용자가 RADIUS 또는 TACACS+ 서버에서 자동으로 검색 및 적용되는 특정 액세스 프로필을 사용하여 네트워크에 로그인하거나 HTTP를 통해 인터넷에 액세스할 수 있습니다. 사용자 프로필은 인증된 사용자로부터 활성 트래픽이 있는 경우에만 활성화됩니다.

이 샘플 컨피그레이션은 인증 프록시를 사용하여 브라우저 인증이 수행될 때까지 내부 네트워크의 호스트 디바이스(40.31.1.47)에서 인터넷의 모든 디바이스로 트래픽을 차단합니다. 서버에서 전달된 ACL(Access Control List)은 호스트 PC에서 인터넷으로 일시적으로 액세스를 허용하는 액세스 목록 116에 동적 **항목**(permit tcp|ip|icmp any any)을 추가합니다.

인증 프록시에 대한 자세한 내용은 인증 프록시 구성을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 소프트웨어 릴리스 12.2(15)T

- Cisco 7206 라우터

참고: ip auth-proxy 명령은 Cisco IOS Firewall Software 릴리스 12.0.5.T에 도입되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

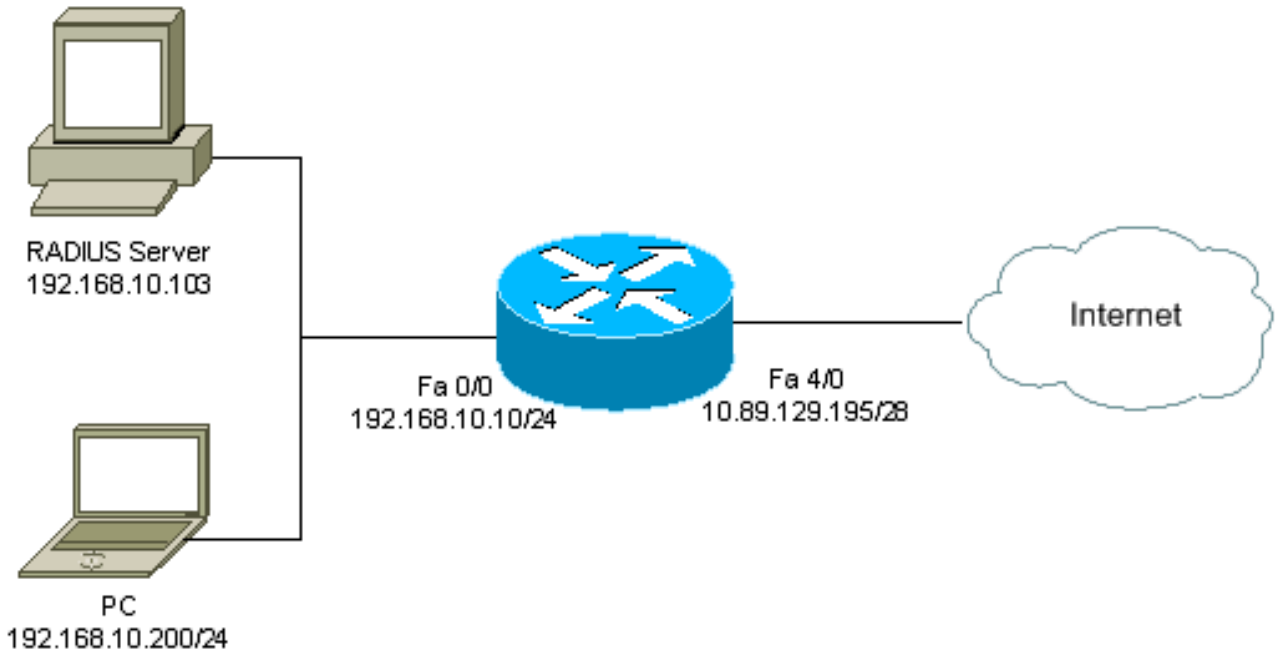
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

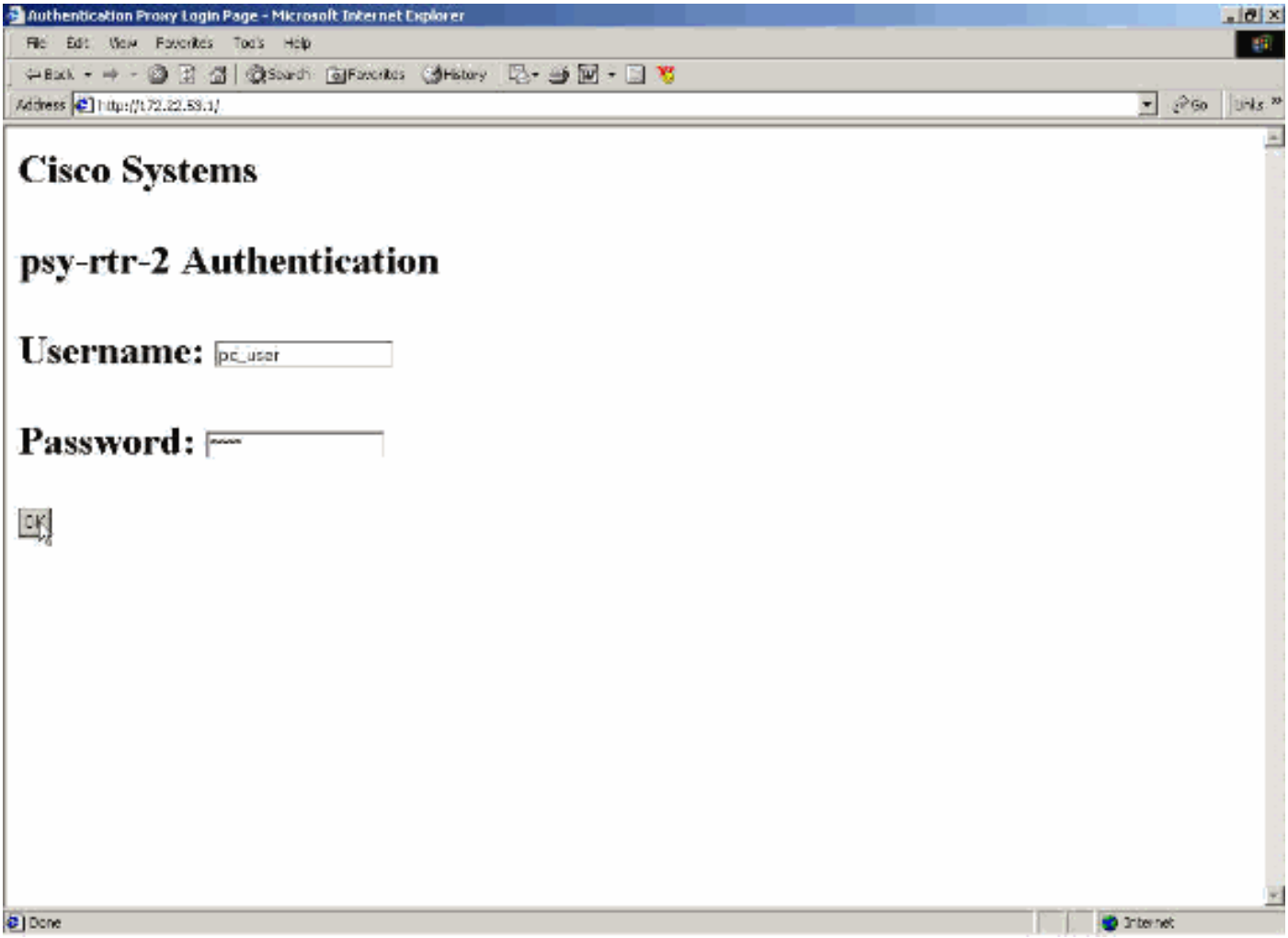
이 문서에서는 다음 구성을 사용합니다.

7206 라우터
version 12.2 service timestamps debug datetime msec service timestamps log datetime msec

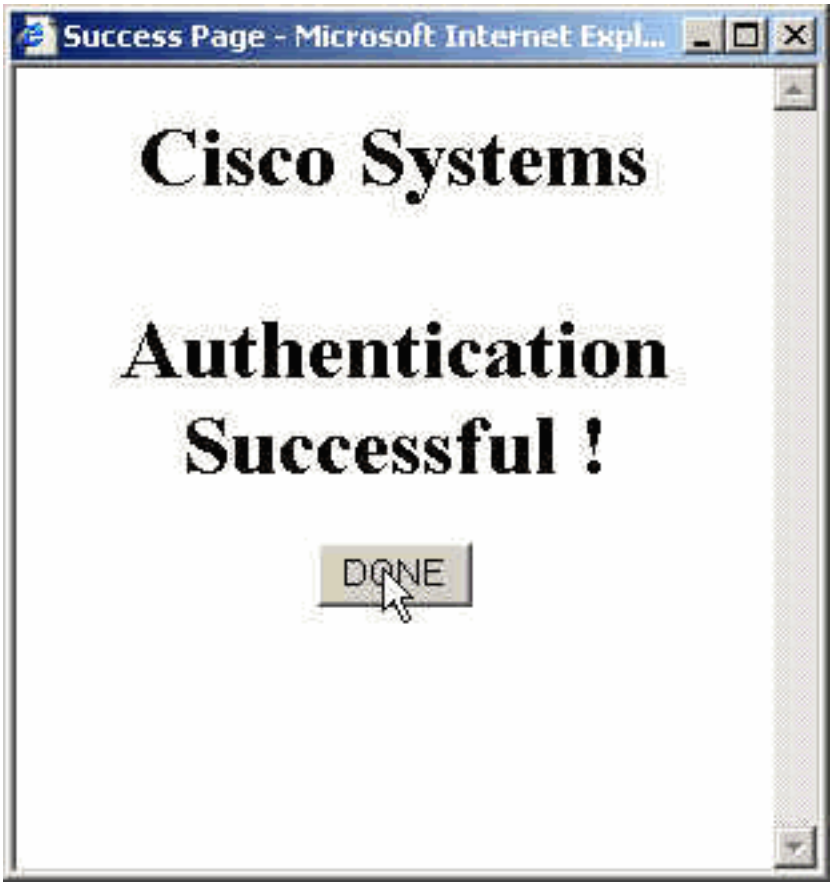
```
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

PC에서 인증

이 섹션에서는 인증 절차를 보여 주는 PC의 화면 캡처를 제공합니다. 첫 번째 캡처는 사용자가 인증을 위해 사용자 이름 및 비밀번호를 입력하고 **OK**를 누르는 창을 표시합니다.



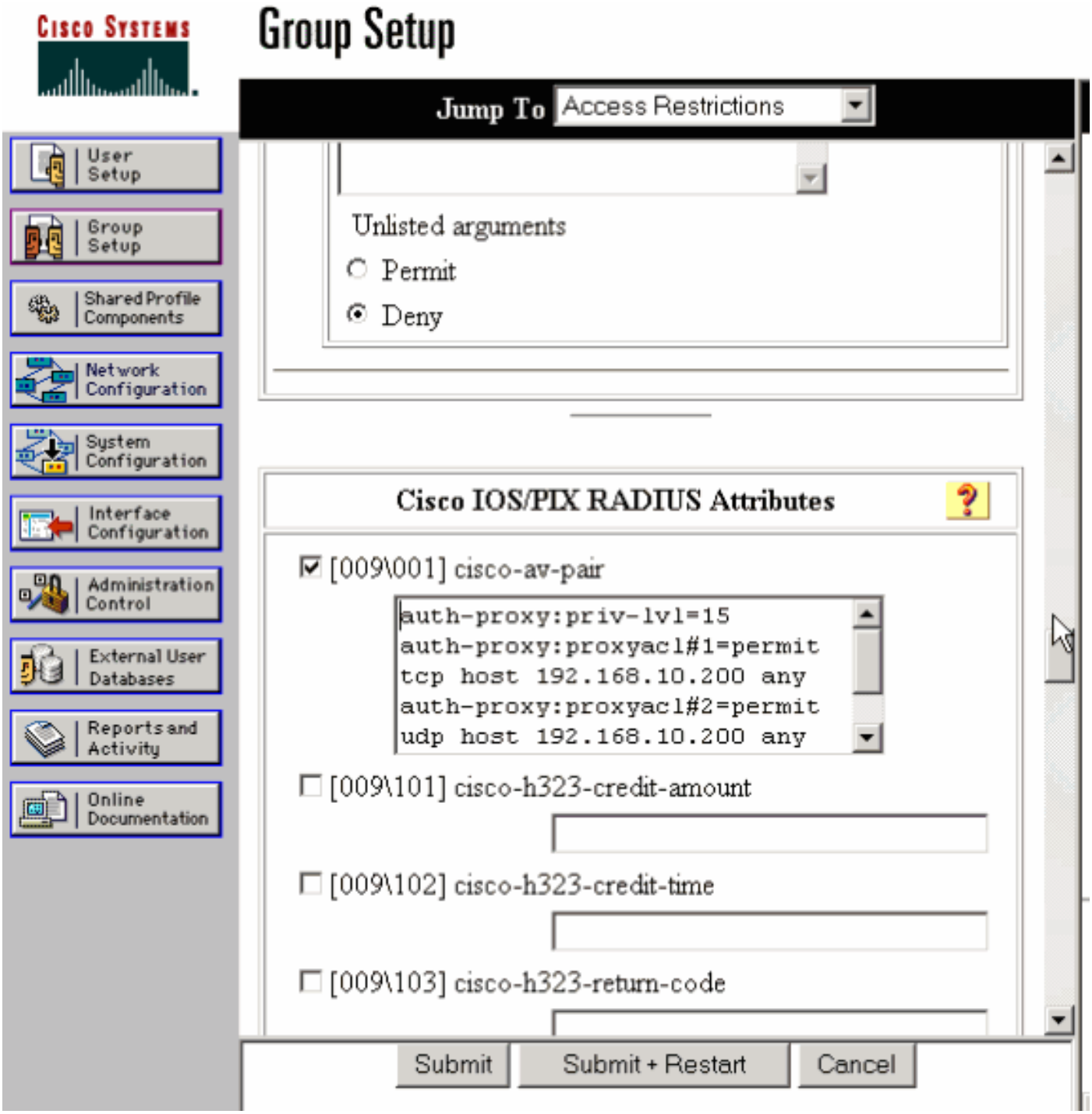
인증에 성공하면 이 창이 나타납니다.



RADIUS 서버는 적용되는 프록시 ACL로 구성되어야 합니다. 이 예에서는 이러한 ACL 항목이 적용됩니다. 이렇게 하면 PC가 모든 장치에 연결할 수 있습니다.

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

이 Cisco ACS 창은 프록시 ACL을 입력할 위치를 보여줍니다.



참고: RADIUS/TACACS+ 서버 구성 방법에 대한 자세한 내용은 인증 프록시 구성을 참조하십시오.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show ip access-lists** - 방화벽에 구성된 표준 및 확장 ACL을 표시합니다(동적 ACL 항목 포함). 사용자가 인증하는지 여부에 따라 동적 ACL 항목이 정기적으로 추가되고 제거됩니다.
- **show ip auth-proxy cache**—인증 프록시 항목 또는 실행 중인 인증 프록시 컨피그레이션을 표시합니다. 호스트 IP 주소, 소스 포트 번호, 인증 프록시의 시간 제한 값 및 인증 프록시를 사용하는 연결의 상태를 나열하는 cache 키워드. 인증 프록시 상태가 HTTP_ESTAB이면 사용자 인증이 성공합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

이러한 명령과 다른 문제 해결 정보는 인증 프록시 문제 해결을 참조하십시오.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- IOS 방화벽 지원 페이지
- TACACS/TACACS+ 지원 페이지
- IOS 설명서의 TACACS+
- RADIUS 지원 페이지
- IOS 설명서의 RADIUS
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems