身份驗證代理身份驗證出站 — 無Cisco IOS防火牆或NAT配置

目錄

簡介

驗證代理功能允許使用者登入網路或透過HTTP存取網際網路，並自動從RADIUS或TACACS+伺服器擷取和應用其特定存取設定檔。僅當存在來自已驗證使用者的活動流量時，使用者配置檔案才處於活動狀態。

此示例配置阻止從內部網路上的主機裝置(40.31.1.47)到Internet上的所有裝置的流量，直到使用身份驗證代理執行瀏覽器身份驗證。從伺服器向下傳遞的訪問控制清單(ACL)(**permit tcp|ip|icmp any any**)會在授權後向訪問清單116新增動態條目，這些條目暫時允許從主機PC訪問Internet。

如需驗證代理的詳細資訊，請參閱設定驗證代理。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS®軟體版本12.2(15)T
- 思科7206路由器

注意：ip auth-proxy指令是在Cisco IOS防火牆軟體版本12.0.5中匯入，

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

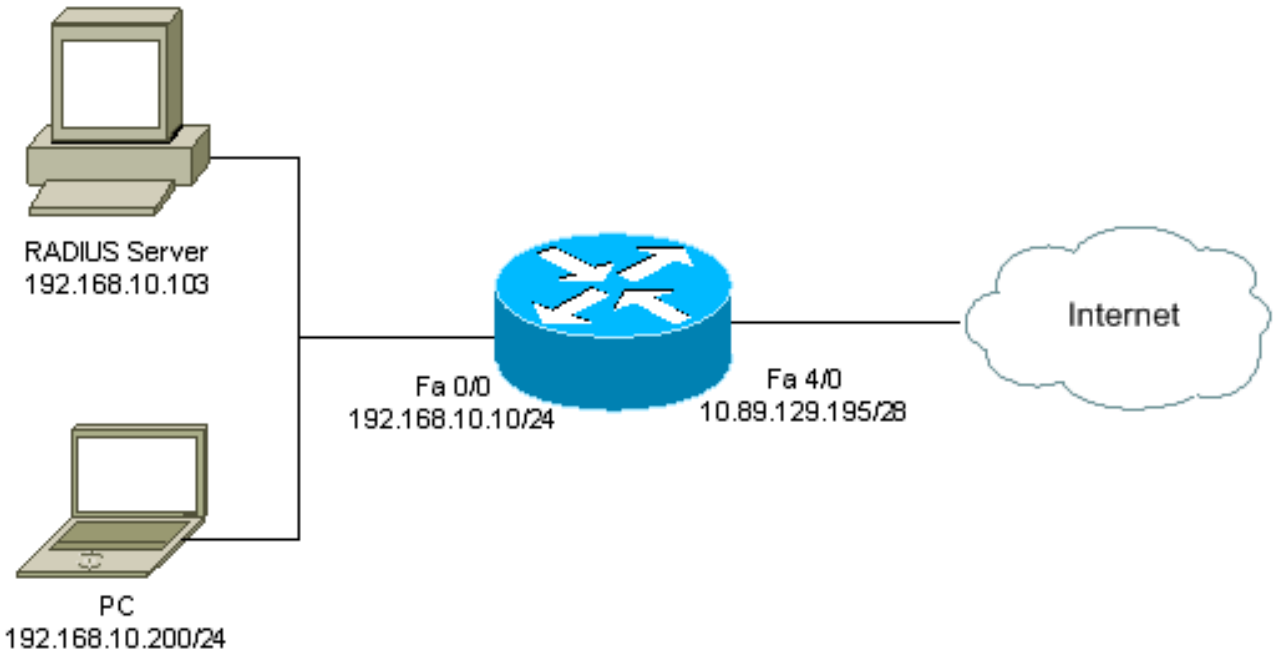
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



組態

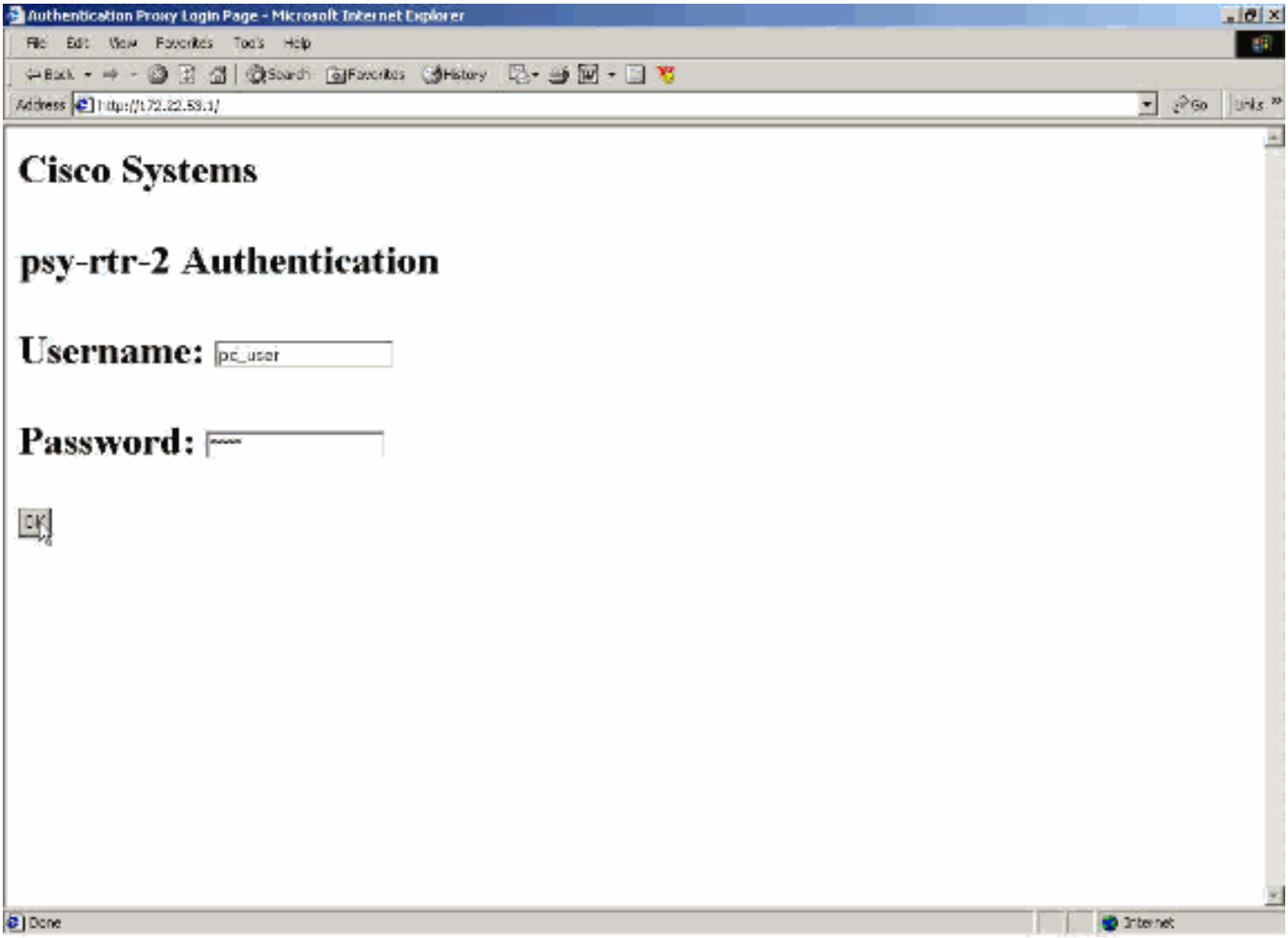
本檔案會使用以下設定：

7206路由器
version 12.2 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! hostname psy-rtr-2 !

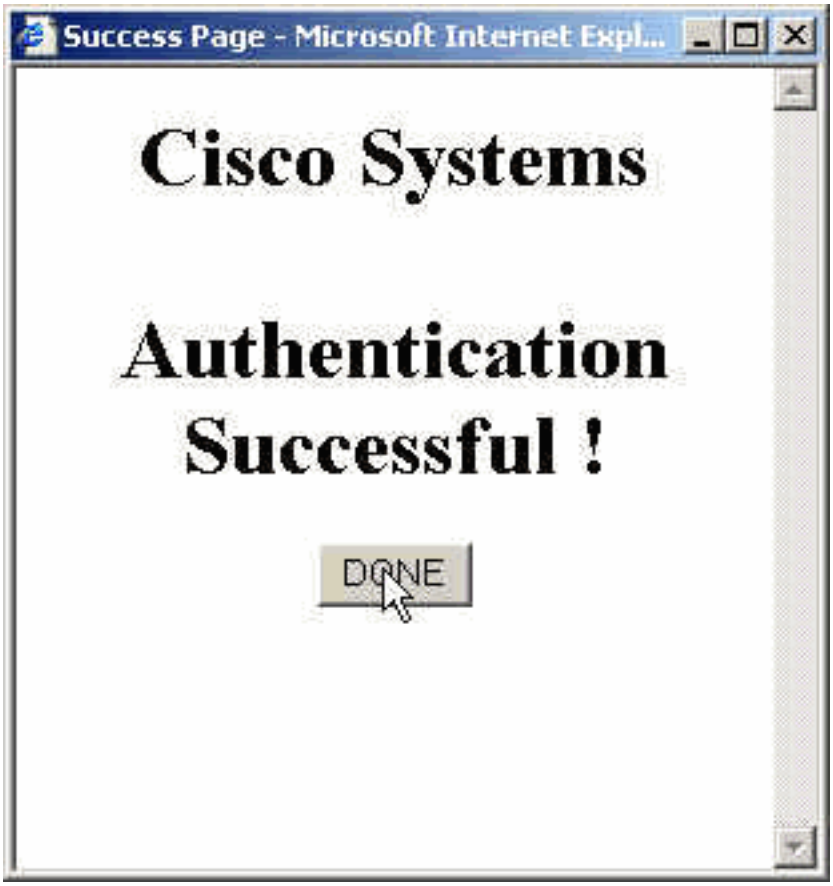
```
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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上的身份驗證

本節提供從PC獲取的螢幕截圖，其中顯示了身份驗證過程。第一個捕獲顯示一個視窗，使用者在該視窗中輸入使用者名稱和密碼進行身份驗證，然後按**確定**。



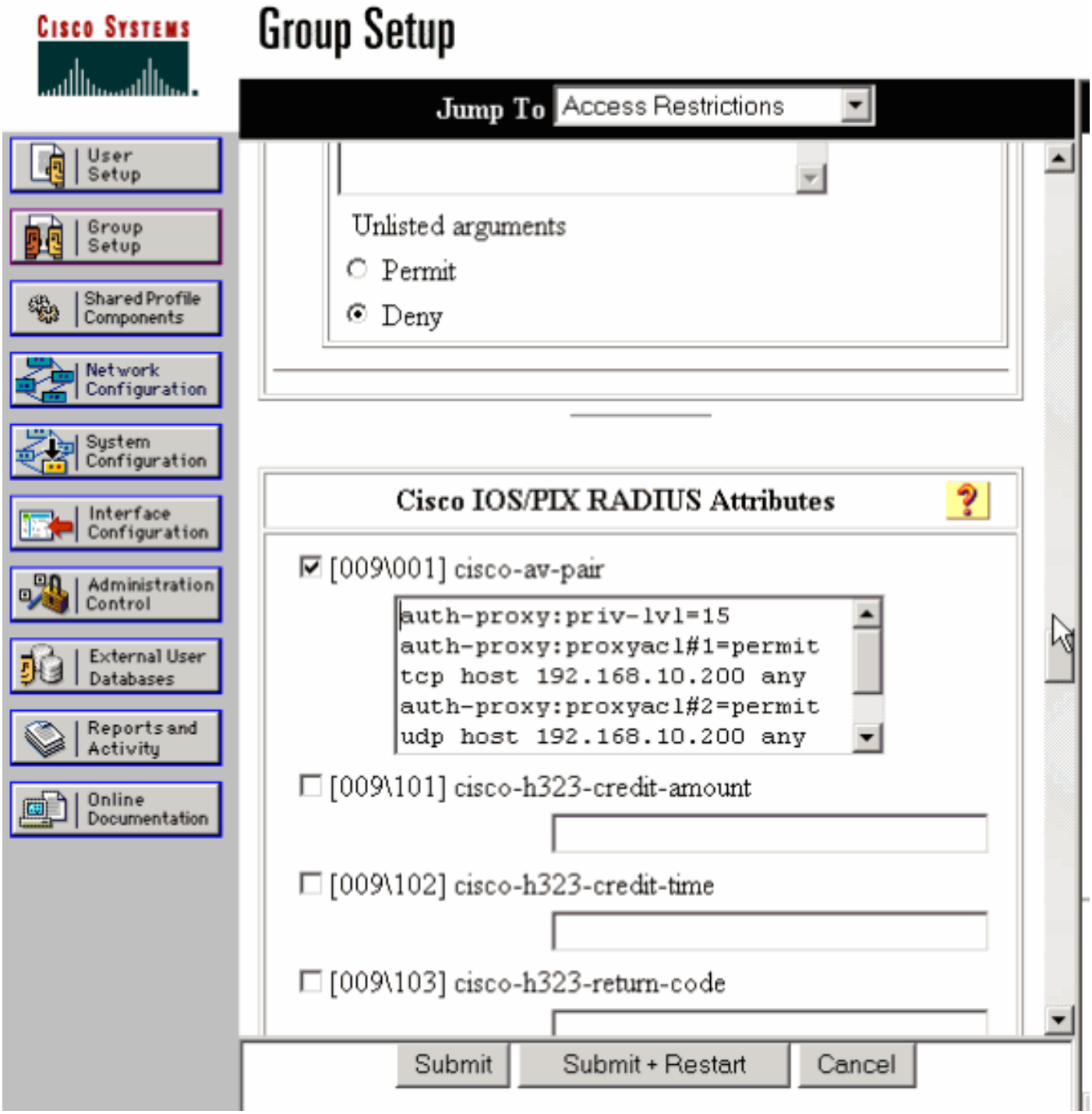
如果驗證成功，則出現此視窗。



必須使用應用的代理ACL配置RADIUS伺服器。在此範例中，將套用這些ACL專案。這允許PC連線到任何裝置。

```
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視窗顯示代理ACL的輸入位置。



註：有關如何配置RADIUS/TACACS+伺服器的詳細資訊，請參閱配置身份驗證代理。

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show ip access-lists** — 顯示防火牆上配置的標準型和延伸型ACL（包括動態ACL條目）。 動態ACL條目將根據使用者是否進行身份驗證定期新增和刪除。
- **show ip auth-proxy cache** — 顯示驗證代理條目或執行中的驗證代理配置。cache關鍵字，用於列出主機IP地址、源埠號、身份驗證代理的超時值和使用身份驗證代理的連線狀態。如果身份驗證代理狀態為HTTP_ESTAB，則使用者身份驗證成功。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

如需這些命令以及其他疑難排解資訊，請參閱驗證代理疑難排解。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

相關資訊

- **IOS防火牆支援頁面**
- **TACACS/TACACS+ 支援頁面**
- **IOS 文件中的 TACACS+**
- **RADIUS 支援頁面**
- **IOS檔案中的RADIUS**
- **要求建議 (RFC)**
- **技術支援與文件 - Cisco Systems**