

# Autenticazione proxy in uscita - senza configurazione Cisco IOS Firewall o NAT

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Autenticazione sul PC](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

La funzionalità Proxy di autenticazione consente agli utenti di accedere alla rete o a Internet tramite HTTP, con i relativi profili di accesso specifici recuperati e applicati automaticamente da un server RADIUS o TACACS+. I profili utente sono attivi solo quando è attivo il traffico proveniente dagli utenti autenticati.

In questa configurazione di esempio viene bloccato il traffico tra il dispositivo host (versione 40.31.1.47) sulla rete interna e tutti i dispositivi su Internet finché non viene eseguita l'autenticazione del browser con il proxy di autenticazione. L'elenco di controllo di accesso (ACL) passato dal server (**consenti tcp|ip|icmp any**) aggiunge voci dinamiche post-autorizzazione all'elenco di accesso 116 che consentono temporaneamente l'accesso a Internet dal PC host.

Per ulteriori informazioni sul proxy di autenticazione, consultare il documento sulla [configurazione del proxy di autenticazione](#).

## Prerequisiti

### Requisiti

Nessun requisito specifico previsto per questo documento.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software Cisco IOS® versione 12.2(15)T
- Cisco 7206 router

**Nota:** il comando **ip auth-proxy** è stato introdotto nel software Cisco IOS Firewall versione 12.0.5.T.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

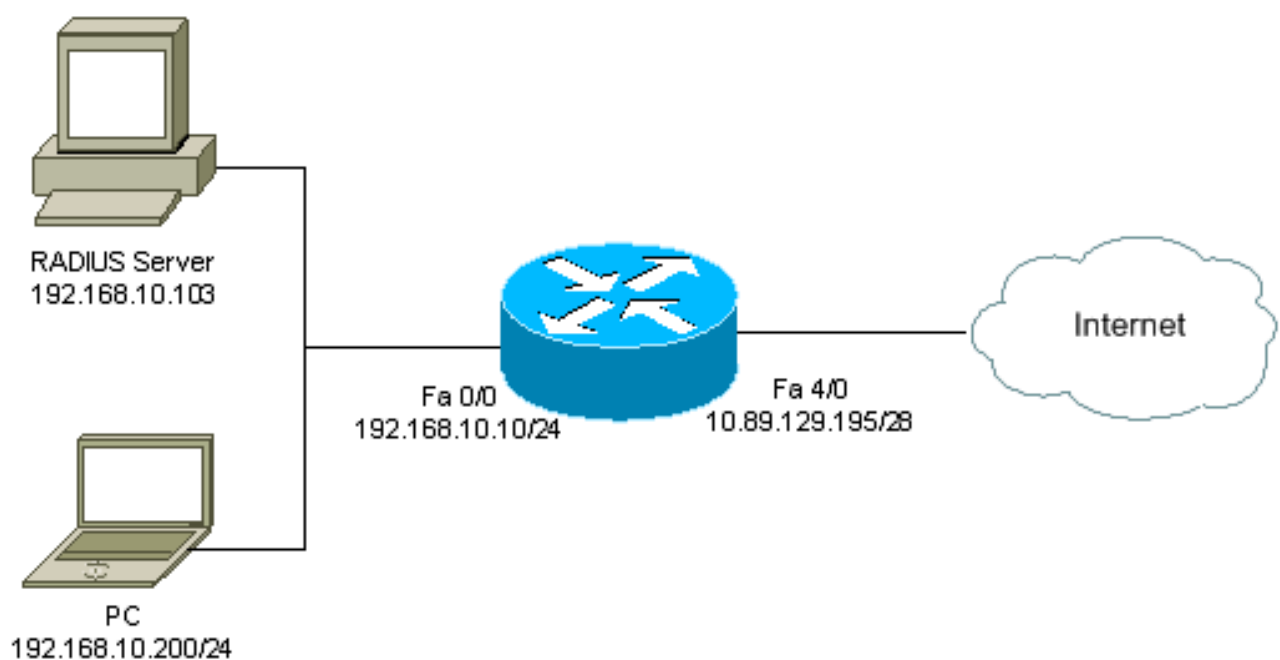
## Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

**Nota:** per ulteriori informazioni sui comandi menzionati in questo documento, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



## Configurazione

Nel documento viene usata questa configurazione:

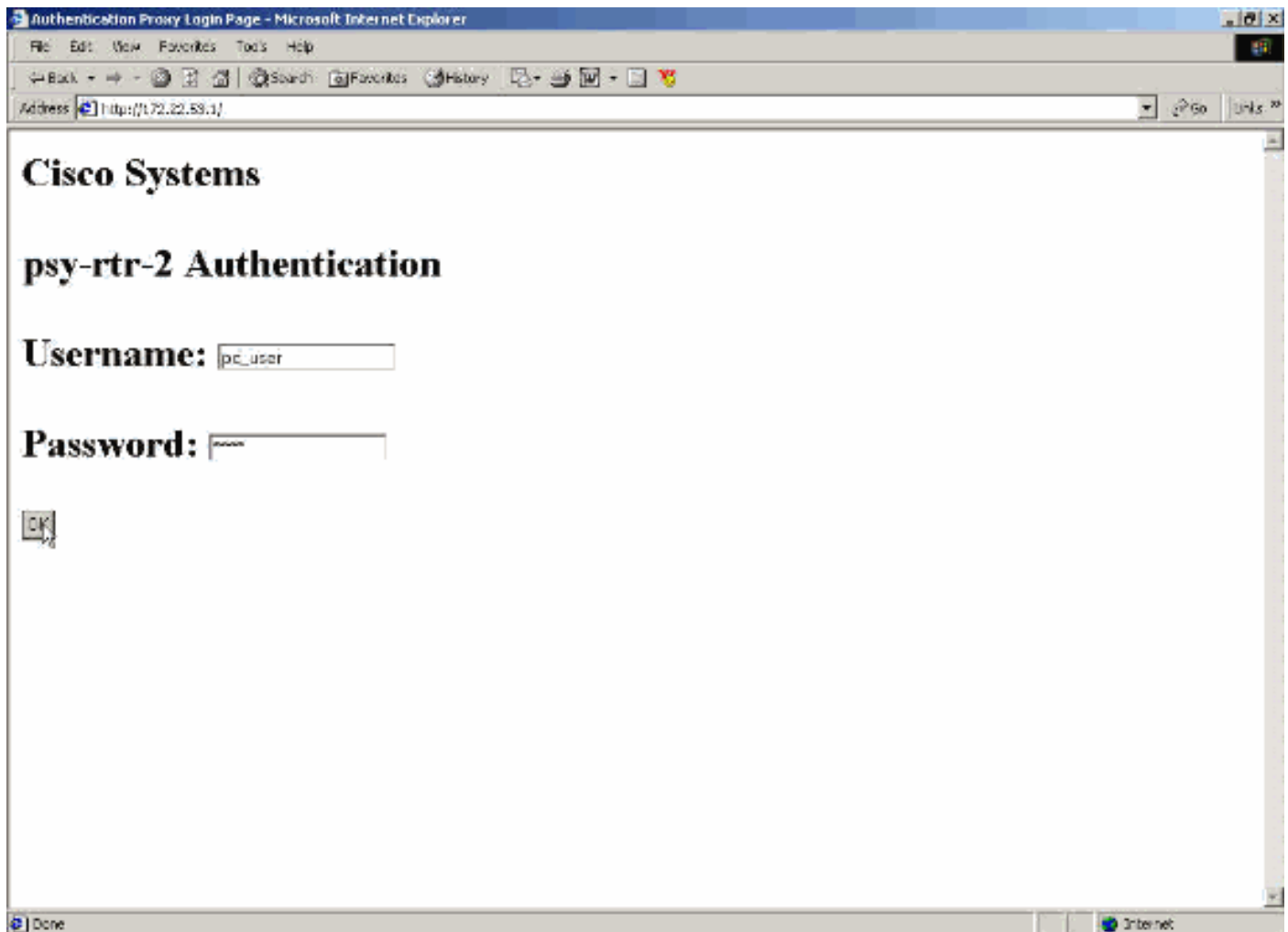
## 7206 Router

```
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

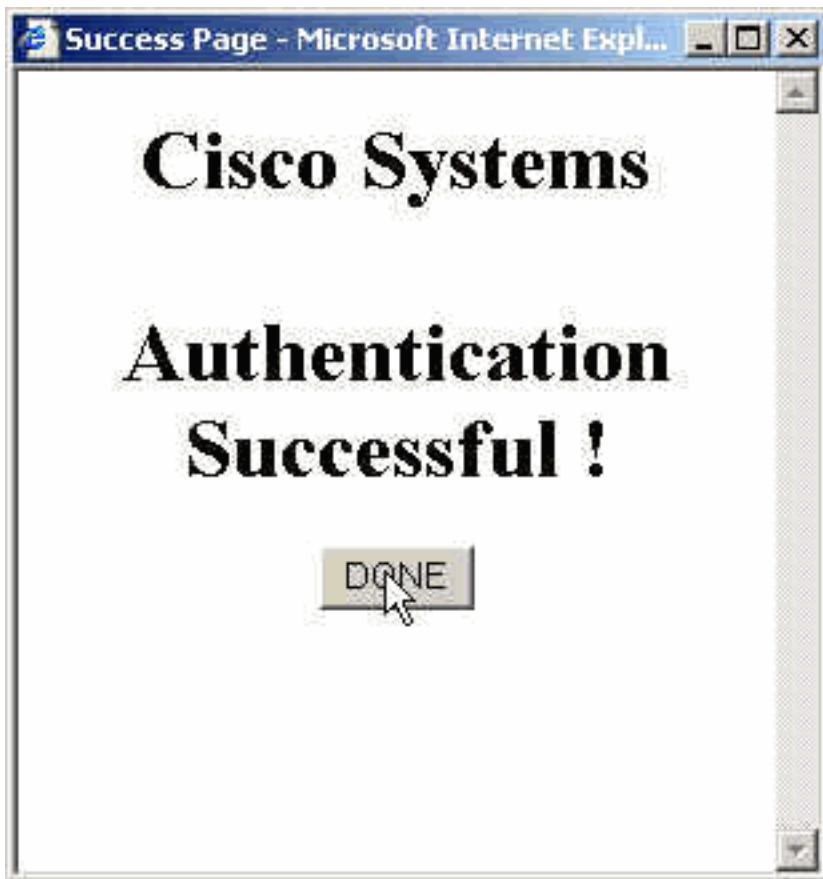
!--- Enable AAA. aaa authentication login default group
radius none !--- Use RADIUS to authenticate users. aaa
authorization exec default group radius none aaa
authorization auth-proxy default group radius !---
Utilize RADIUS for auth-proxy authorization. aaa
session-id common ip subnet-zero ! ip cef ! 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
```

## [Autenticazione sul PC](#)

In questa sezione vengono fornite immagini acquisite dal PC che mostrano la procedura di autenticazione. La prima acquisizione mostra la finestra in cui un utente immette il nome utente e la password per l'autenticazione e preme OK.



Se l'autenticazione ha esito positivo, viene visualizzata questa finestra.



Il server RADIUS deve essere configurato con gli ACL proxy applicati. Nell'esempio, vengono applicate queste voci ACL. Consente al PC di connettersi a qualsiasi 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
```

In questa finestra Cisco ACS viene mostrato dove accedere agli ACL proxy.



# Group Setup

Jump To Access Restrictions

Unlisted arguments

Permit

Deny

---

**Cisco IOS/PIX RADIUS Attributes** ?

[009\001] cisco-av-pair

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit
tcp host 192.168.10.200 any
auth-proxy:proxyacl#2=permit
udp host 192.168.10.200 any
```

[009\101] cisco-h323-credit-amount

[009\102] cisco-h323-credit-time

[009\103] cisco-h323-return-code

**Nota:** per ulteriori informazioni su come configurare il server RADIUS/TACACS+, consultare il documento sulla [configurazione del proxy di autenticazione](#).

## Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show ip access-lists:** visualizza gli ACL standard ed estesi configurati sul firewall (include le voci ACL dinamiche). Le voci ACL dinamiche vengono aggiunte e rimosse periodicamente a seconda che l'utente esegua o meno l'autenticazione.

- **show ip auth-proxy cache**: visualizza le voci del proxy di autenticazione o la configurazione del proxy di autenticazione in esecuzione. La parola chiave cache per elencare l'indirizzo IP dell'host, il numero della porta di origine, il valore di timeout per il proxy di autenticazione e lo stato delle connessioni che utilizzano il proxy di autenticazione. Se lo stato del proxy di autenticazione è HTTP\_ESTAB, l'autenticazione utente ha esito positivo.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per questi comandi e altre informazioni sulla risoluzione dei problemi, consultare il documento sulla [risoluzione dei problemi del proxy di autenticazione](#).

**Nota:** consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di debug.

## Informazioni correlate

- [Pagina di supporto di IOS Firewall](#)
- [Pagina di supporto TACACS/TACACS+](#)
- [Documentazione relativa a TACACS+ in IOS](#)
- [Pagina di supporto RADIUS](#)
- [Documentazione di RADIUS in IOS](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)