

Configurazione di Auth-proxy Authentication Inbound (Cisco IOS Firewall, no NAT)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

[Introduzione](#)

Questa configurazione di esempio blocca inizialmente il traffico dagli host esterni a tutti i dispositivi della rete interna finché non viene eseguita l'autenticazione del browser con l'utilizzo del proxy di autenticazione. L'elenco degli accessi passato dal server (**consenti tcp|ip|icmp any**) aggiunge voci dinamiche post-autorizzazione all'elenco degli accessi 115 che consentono temporaneamente l'accesso alla rete interna dal PC esterno.

[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 12.0.7.T
- Cisco 3640 router

Nota: il comando **ip auth-proxy** è stato introdotto nel software Cisco IOS versione 12.0.5.T. Questa configurazione è stata testata con il software Cisco IOS versione 12.0.7.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

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

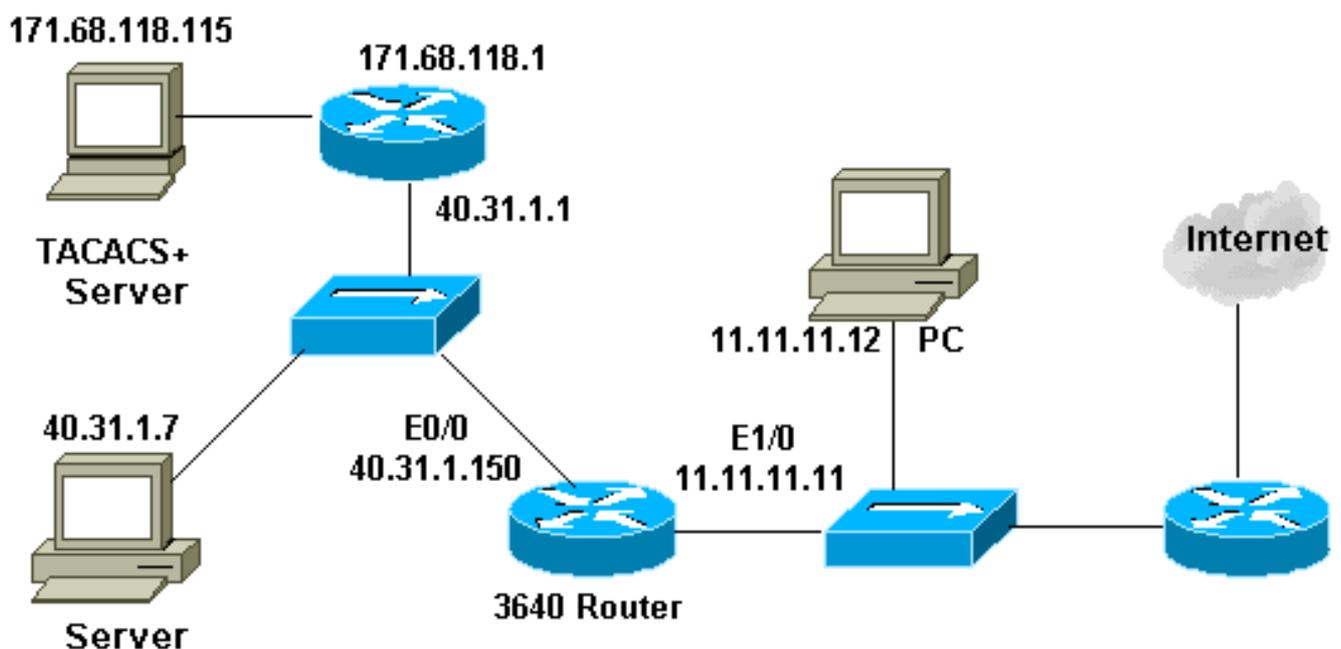
Configurazione

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 questa sezione, 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:

3640 Router

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname security-3640
!
aaa new-model
aaa group server tacacs+ RTP
  server 171.68.118.115
!
aaa authentication login default group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$H9zZ$z9bu5HMy4NTtjstvIhltGT0
enable password ww
!
ip subnet-zero
!
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip auth-proxy auth-proxy-banner
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
process-max-time 200
!
interface FastEthernet0/0
  ip address 40.31.1.150 255.255.255.0
  ip access-group 101 in
  no ip directed-broadcast
  ip inspect myfw in
  no mop enabled
!
interface FastEthernet1/0
  ip address 11.11.11.11 255.255.255.0
  ip access-group 115 in
  no ip directed-broadcast
  ip auth-proxy list_a
!
ip classless
ip route 0.0.0.0 0.0.0.0 11.11.11.1
ip route 171.68.118.0 255.255.255.0 40.31.1.1
ip http server
ip http authentication aaa
!
access-list 101 permit icmp 40.31.1.0 0.0.0.255 any
access-list 101 permit tcp 40.31.1.0 0.0.0.255 any
access-list 101 permit udp 40.31.1.0 0.0.0.255 any
access-list 101 permit icmp 171.68.118.0 0.0.0.255 any
access-list 101 permit tcp 171.68.118.0 0.0.0.255 any
access-list 101 permit udp 171.68.118.0 0.0.0.255 any
access-list 115 permit tcp host 11.11.11.12 host
11.11.11.11 eq www
access-list 115 deny tcp any any
```

```
access-list 115 deny    udp any any
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 echo
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
echo-reply
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
packet-too-big
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
time-exceeded
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
traceroute
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
unreachable
access-list 115 permit icmp any 40.31.1.0 0.0.0.255
administratively-prohibited
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tacacs-server host 171.68.118.115
tacacs-server key cisco
radius-server host 171.68.118.115
radius-server key cisco

!
line con 0
  transport input none
line aux 0
line vty 0 4
  password ww
!
!
end
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

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](#)
- [RFC \(Requests for Comments\)](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)