

# Ejemplo de Configuración de Autenticación Entrante de Auth-Proxy (Cisco IOS Firewall - Routers/Switches y NAT)

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## [Introducción](#)

Esta configuración de ejemplo bloquea inicialmente el tráfico de los hosts externos a todos los dispositivos de la red interna hasta que se realice la autenticación del navegador mediante el proxy de autenticación. Después de la autorización, la lista de acceso transmitida desde el servidor (**permit tcp|ip|icmp any any**) agrega entradas dinámicas a la lista de acceso 116 que permiten temporalmente el acceso desde el equipo externo a la red interna.

**Nota:** La configuración AAA utilizada en este documento también es aplicable a los switches Catalyst que ejecutan el <sup>software</sup> Cisco IOS<sup>®</sup>.

## [Prerequisites](#)

## [Requirements](#)

No hay requisitos específicos para este documento.

## [Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 12.2.23 del software Cisco IOS

- Cisco 3640 router

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

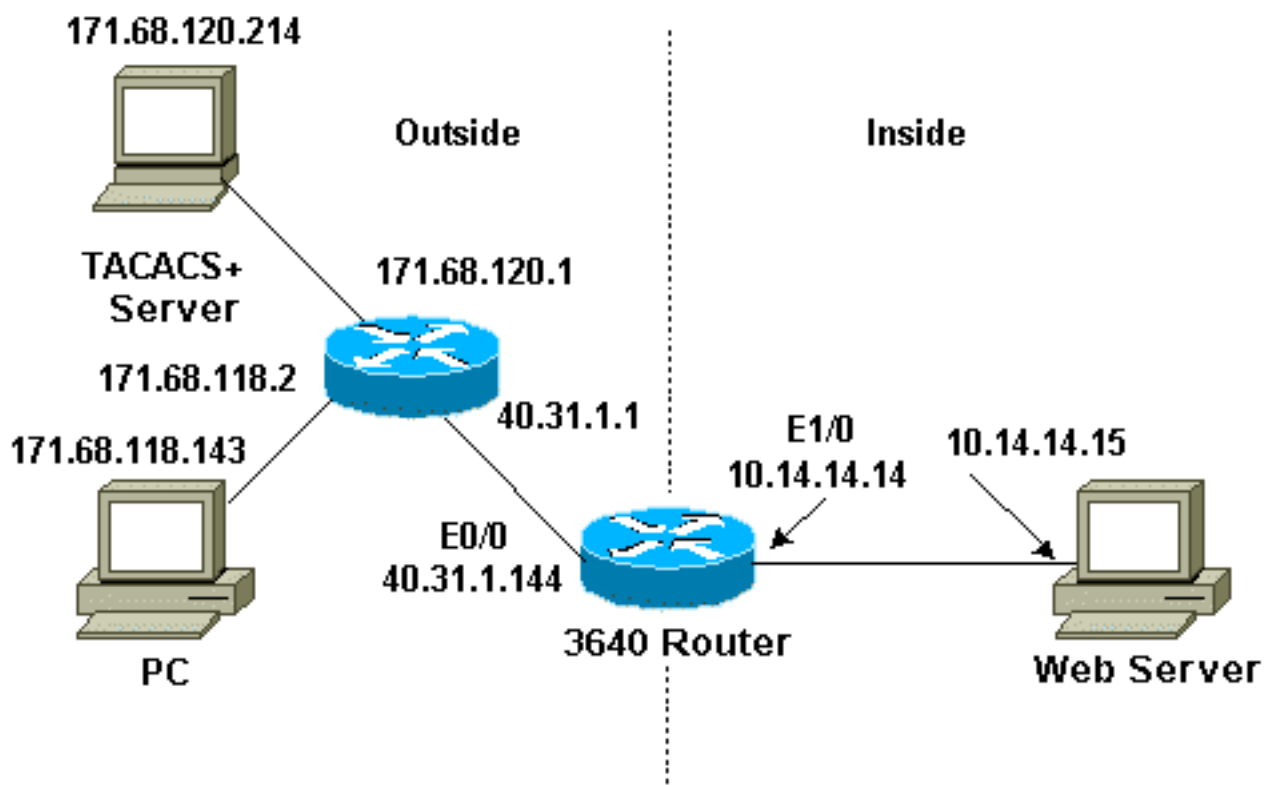
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Utilice la herramienta [Command Lookup](#) (sólo para clientes [registrados](#)) para obtener más información sobre los comandos utilizados en esta sección.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

Este documento usa esta configuración:

- Cisco 3640 Router

|                   |
|-------------------|
| Cisco 3640 Router |
|-------------------|

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname sec-3640
!

aaa new-model
aaa group server tacacs+ RTP
  server 171.68.120.214
!

aaa authentication login default group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$PqRI$3TDNFT9FdYT8Sd/q3S0VU1
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 inspect name myfw vdolive

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
!
interface Ethernet0/0
  ip address 40.31.1.144 255.255.255.0

ip access-group 116 in
  ip nat outside

ip auth-proxy list_a
  no ip route-cache
  no ip mroute-cache
  speed auto
  half-duplex
  no mop enabled
!
interface Ethernet1/0
  ip address 10.14.14.14 255.255.255.0
  ip nat inside
  ip inspect myfw in
  speed auto
  half-duplex
```

```
!  
!--- Interfaces deleted. ! nat pool outsidepool  
40.31.1.50 40.31.1.60 netmask 255.255.255.0 ip nat  
inside source list 1 pool outsidepool ip nat inside  
source static 10.14.14.15 40.31.1.77 ip classless ip  
route 0.0.0.0 0.0.0.0 40.31.1.1 ip route 171.68.118.0  
255.255.255.0 40.31.1.1 ip route 171.68.120.0  
255.255.255.0 40.31.1.1 no ip http server !  
access-list 116 permit tcp host 171.68.118.143 host  
40.31.1.144 eq www  
access-list 116 deny tcp host 171.68.118.143 any  
access-list 116 deny udp host 171.68.118.143 any  
access-list 116 deny icmp host 171.68.118.143 any  
access-list 116 permit icmp any any  
access-list 116 permit tcp any any  
access-list 116 permit udp any any  
dialer-list 1 protocol ip permit  
dialer-list 1 protocol ipx permit  
!  
tacacs-server host 171.68.120.214  
tacacs-server key cisco  
!  
line con 0  
  transport input none  
line aux 0  
line vty 0 4  
  password ww  
!  
end
```

## Verificación

Consulte [información importante en los comandos debug antes de ejecutar los comandos debug](#).

Consulte [Resolución de Problemas de Proxy de Autenticación](#) para obtener información sobre el comando y la resolución de problemas.

## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

## Información Relacionada

- [Cisco IOS Firewall](#)
- [Soporte de seguridad y tecnología VPN](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)