

Autenticación de Proxy de Autenticación Entrante - Sin Firewall Cisco IOS ni Configuración 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 un dispositivo host (en 11.11.11.12) en la red externa a todos los dispositivos de la red interna hasta que se realiza la autenticación del explorador con el uso del proxy de autenticación. La lista de acceso transmitida desde el servidor (**permit tcp|ip|icmp any any**) agrega entradas dinámicas después de la autorización a la lista de acceso 115 que permiten temporalmente el acceso desde el dispositivo host a la red interna.

[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 de software del IOS® de Cisco 12.0.7.T
- Cisco 3640 router

Nota: El comando **ip auth-proxy** se introdujo en la versión 12.0.5.T del software del IOS de Cisco.

Esta configuración se probó con Cisco IOS Software Release 12.0.7.T.

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.

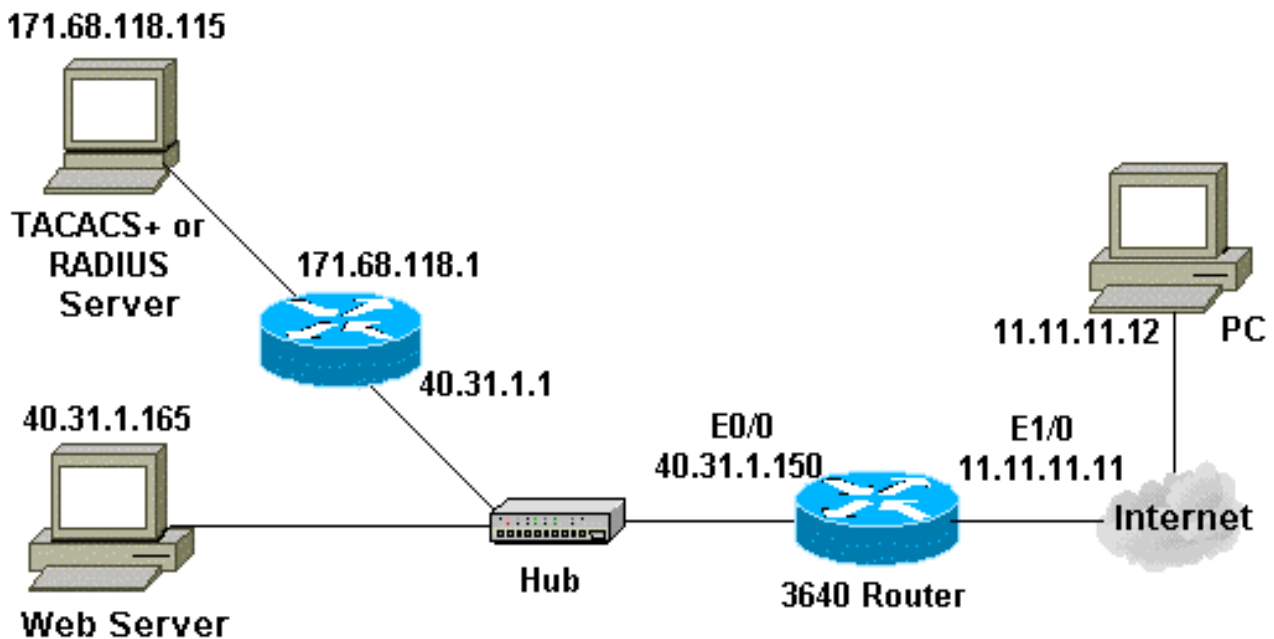
Configurar

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:

Router 3640

```
Current configuration:  
!  
version 12.0
```

```

service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname security-3640
!
!--- Turn on authentication. aaa new-model
!--- Define the server group and servers for TACACS+ or
RADIUS. aaa group server tacacs+|radius RTP
  server 171.68.118.115
!
!--- Define what you need to authenticate. 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
!
!--- You want the router name to appear as banner. ip
auth-proxy auth-proxy-banner
!--- You want the access-list entries to timeout after
10 minutes. ip auth-proxy auth-cache-time 10
!--- You define the list-name to be associated with the
interface. 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
  no ip directed-broadcast
  no mop enabled
!
interface FastEthernet1/0
  ip address 11.11.11.11 255.255.255.0
!--- Apply the access-list to the interface. ip access-
group 115 in
  no ip directed-broadcast
!--- Apply the auth-proxy list-name. ip auth-proxy
list_a
!
ip classless
ip route 171.68.118.0 255.255.255.0 40.31.1.1
!--- Turn on the http server and authentication. ip http
server
ip http authentication aaa
!
!--- This is our access-list for auth-proxy testing - !-
-- it denies only one host, 11.11.11.12, access - to
minimize disruption !--- to the network during testing.
access-list 115 permit tcp host 11.11.11.12 host
11.11.11.11 eq www
access-list 115 deny icmp host 11.11.11.12 any
access-list 115 deny tcp host 11.11.11.12 any
access-list 115 deny udp host 11.11.11.12 any
access-list 115 permit udp any any
access-list 115 permit tcp any any
access-list 115 permit icmp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit

```

```
!  
!--- Define the server(s). 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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para estos comandos, junto con otra información de resolución de problemas, consulte [Resolución de problemas del Proxy de autenticación](#).

Nota: Consulte [Información Importante sobre Comandos Debug](#) antes de ejecutar los comandos debug.

Información Relacionada

- [Página de soporte de firewall de IOS](#)
- [Página de soporte de TACACS/TACACS+](#)
- [TACACS+ en documentación de IOS](#)
- [Página de soporte de RADIUS](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)