

Autenticação de saída de proxy automático (Cisco IOS Firewall e NAT)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

Esta configuração de exemplo inicialmente bloqueia o tráfego de um dispositivo de host (em 10.31.1.47) na rede interna para todos os dispositivos na Internet até que você execute a autenticação do navegador com o uso do proxy de autenticação. A lista de acesso passada do servidor (**permit tcp|ip|icmp any any**) adiciona entradas dinâmicas pós-autorização à lista de acesso 116 que permitem temporariamente o acesso desse dispositivo à Internet.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco IOS® versão 12.2.23
- Cisco 3640 Router

Observação: o comando **ip auth-proxy** foi introduzido no Cisco IOS Software Release 12.0.5.T. Esta configuração foi testada com o 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.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

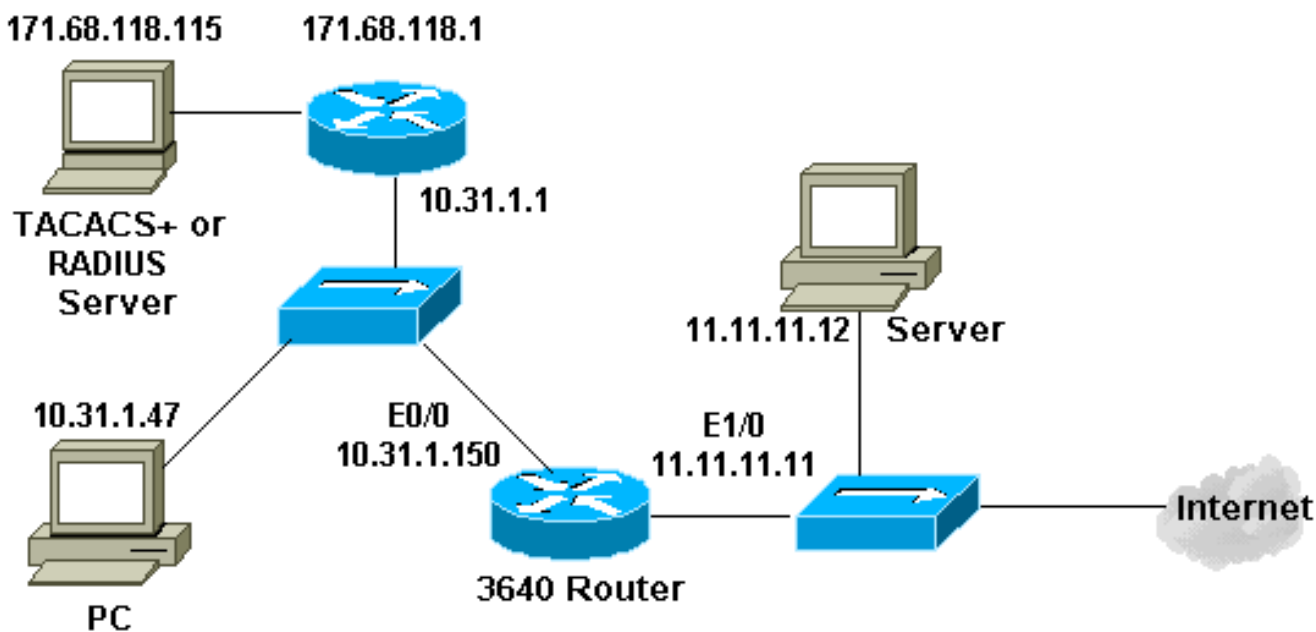
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza esta configuração:

3640 Router

```
Current configuration:
!
version 12.2
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 local group RTP none  
aaa authorization exec default group RTP none  
aaa authorization auth-proxy default group RTP  
enable secret 5 $1$Vcfr$RkuU6HLmpbNgLTg/JNM6e1  
enable password ww  
!  
username john password 0 doe  
!  
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  
!  
process-max-time 200  
!  
interface Ethernet0/0  
  ip address 10.31.1.150 255.255.255.0  
  ip access-group 116 in  
  ip nat inside  
  ip inspect myfw in  
  ip auth-proxy list_a  
  no ip route-cache  
  no ip mroute-cache  
!  
interface Ethernet1/0  
  ip address 11.11.11.11 255.255.255.0  
  ip access-group 101 in  
  ip nat outside  
!  
ip nat pool outsidepool 11.11.11.20 11.11.11.30 netmask  
255.255.255.0  
ip nat inside source list 1 pool outsidepool  
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 10.31.1.1  
ip http server  
ip http authentication aaa  
!  
access-list 1 permit 10.31.1.0 0.0.0.255  
access-list 101 deny ip 10.31.1.0 0.0.0.255 any  
access-list 101 deny ip 127.0.0.0 0.255.255.255 any  
access-list 101 permit icmp any 11.11.11.0 0.0.0.255  
unreachable  
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
```

```
echo-reply
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
packet-too-big
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
time-exceeded
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
traceroute
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
administratively-prohibited
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
echo
access-list 116 permit tcp host 10.31.1.47 host
10.31.1.150 eq www
access-list 116 deny tcp host 10.31.1.47 any
access-list 116 deny udp host 10.31.1.47 any
access-list 116 deny icmp host 10.31.1.47 any
access-list 116 permit tcp 10.31.1.0 0.0.0.255 any
access-list 116 permit udp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 171.68.118.0 0.0.0.255 any
access-list 116 permit tcp 171.68.118.0 0.0.0.255 any
access-list 116 permit udp 171.68.118.0 0.0.0.255 any
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 auth-port 1645 acct-
port 1646
radius-server key cisco
!
line con 0
  transport input none
line aux 0
line vty 0 4
  exec-timeout 0 0
  password ww
!
end
```

[Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

[Troubleshoot](#)

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para obter comandos **debug**, juntamente com outras informações de solução de problemas, consulte [Proxy de Autenticação de Troubleshooting](#).

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos debug.

[Informações Relacionadas](#)

- [Página de suporte de firewall do IOS](#)
- [Página de Suporte do TACACS/TACACS+](#)
- [TACACS+ na Documentação do IOS](#)
- [Página de suporte RADIUS](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)