Autenticação de entrada de proxy de autenticação (Cisco IOS Firewall, sem NAT) Configuração

Contents

Introduction

Essa configuração de exemplo inicialmente bloqueia o tráfego de hosts externos para todos os dispositivos na rede interna até que a autenticação do navegador seja executada 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 115 que permitem temporariamente o acesso do PC externo à rede interna.

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 12.0.7.T
- Cisco 3640 Router

Observação: o comando **ip auth-proxy** é apresentado 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.

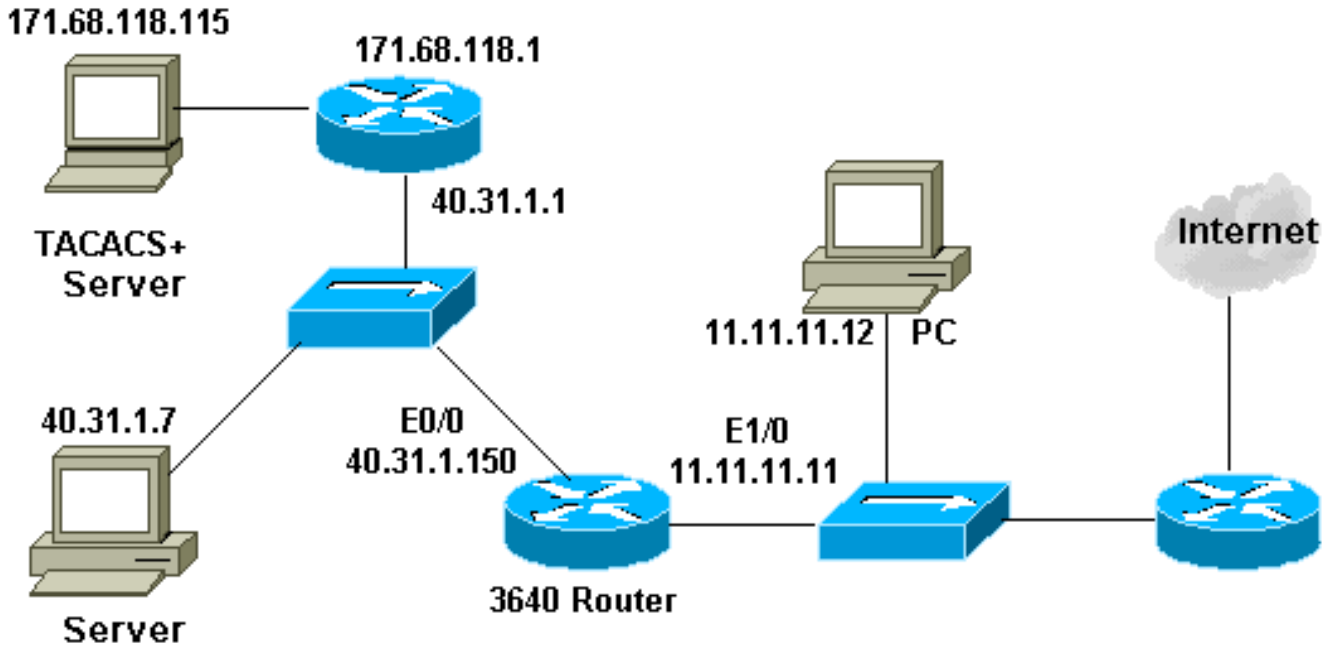
Configurar

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:



Configuração

Este documento utiliza esta configuração:

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$z9bu5HMy4NTtjsvIhltGT0
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
```

Verificar

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

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para esses comandos, juntamente com outras informações de troubleshooting, 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