Autorização de autenticação proxy de entrada (Cisco IOS Firewall - Roteadores/Switches e exemplo de configuração NAT)

Índice

Introdução

Esta configuração de exemplo inicialmente bloqueia o tráfego de hosts externos para todos os dispositivos na rede interna até que a autenticação do navegador esteja executada usando um proxy de autenticação. Após a autorização, a lista de acesso vinda do servidor (permit tcp|ip|icmp any any) adiciona as entradas dinâmicas à lista de acesso 116 que permitem temporariamente o acesso do PC externo à rede interna.

Nota: A configuração de AAA usada neste documento é igualmente aplicável aos Catalyst Switches esse software do ® do Cisco IOS da corrida.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS Software Release 12.2.23
- Cisco 3640 Router

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

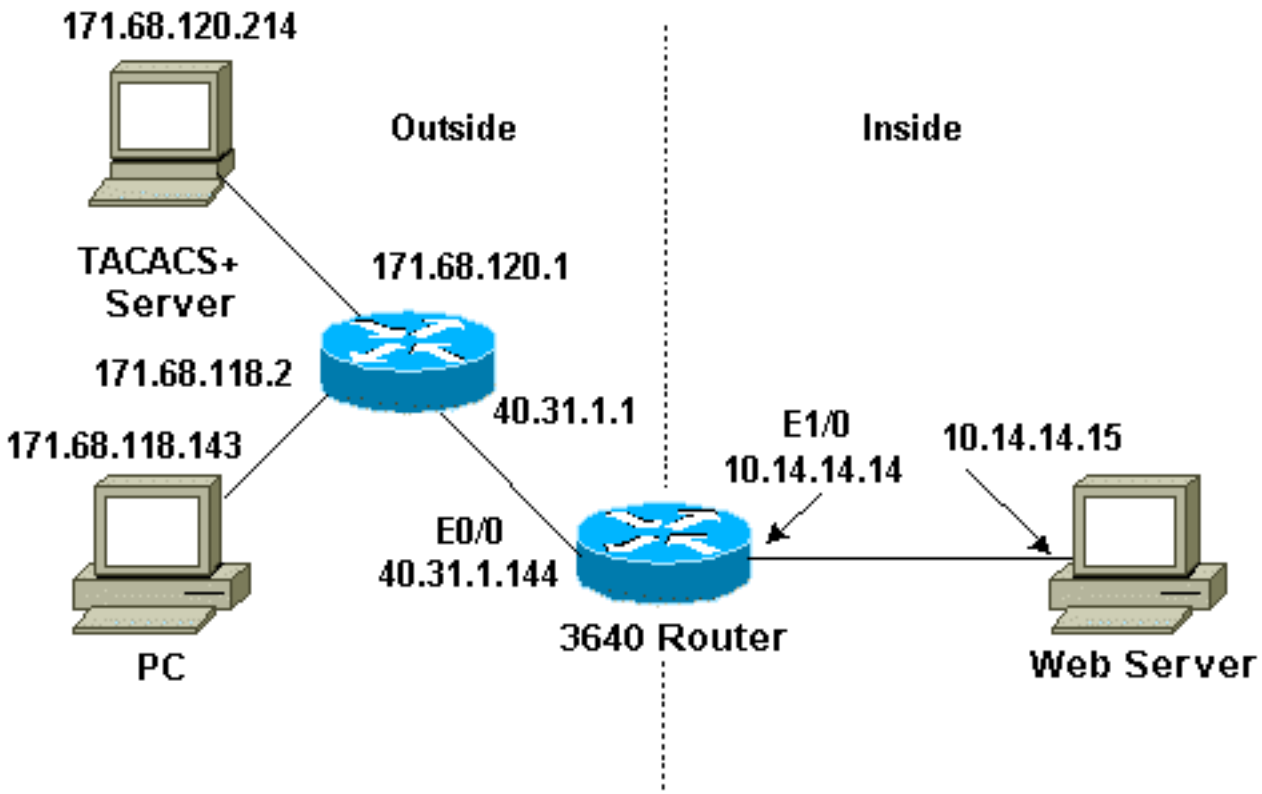
Configurar

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:

- 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
```

Verificar

Consulte Informações Importantes sobre Comandos de Debugação antes de usar comandos **debug**.

Refira pesquisando defeitos o Proxy de autenticação para o comando e a informação de Troubleshooting.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Cisco IOS Firewall
- Suporte por tecnologia da Segurança e VPN
- Suporte Técnico e Documentação - Cisco Systems