Configuratie van verificaties bij volmacht (Cisco IOS-firewall, geen NAT)

Inhoud

Inleiding

Deze voorbeeldconfiguratie blokkeert aanvankelijk verkeer van externe hosts naar alle apparaten op het interne netwerk tot browser authenticatie wordt uitgevoerd met het gebruik van authenticatie proxy. De toegangslijst die van de server is doorgegeven (**sta toe TCP|ip|icmp**, indien **er** dan **ook is**) voegt dynamische items na autorisatie toe aan toegangslijst 115 die tijdelijk toegang van de externe pc tot het interne netwerk mogelijk maken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS® softwarerelease 12.0.7.T
- Cisco 3640 router

Opmerking: De **ip** opdracht **voor automatische proxy** wordt geïntroduceerd in Cisco IOS-softwarerelease 12.0.5.T. Deze configuratie is getest met Cisco IOS-softwarerelease 12.0.7.T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

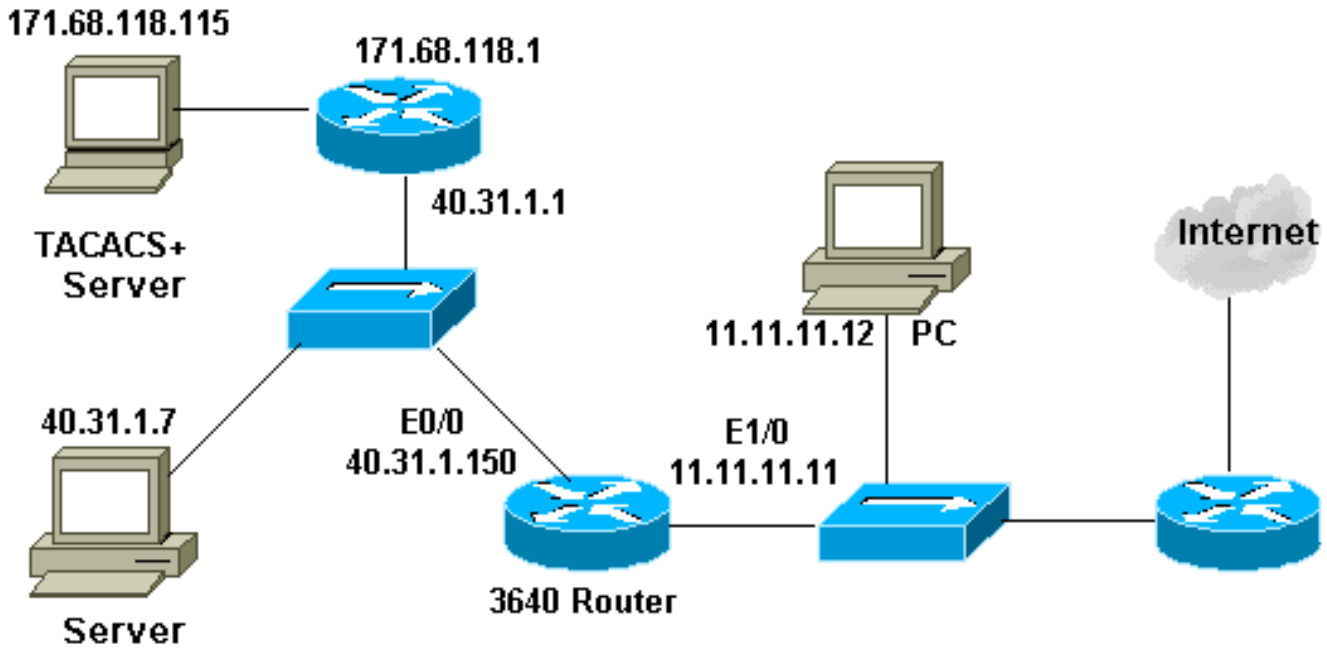
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie

Dit document gebruikt deze configuratie:

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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Raadpleeg voor deze opdrachten, samen met andere informatie over probleemoplossing, de verificatieproxy voor probleemoplossing.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug**-opdrachten afgeeft.

Gerelateerde informatie

- IOS-ondersteuningspagina
- Ondersteuningspagina voor TACACS/TACACS+
- TACACS+ in IOS-documentatie
- RADIUS-ondersteuningspagina
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems