# Configuratie van automatische proxy-verificatie (Cisco IOS-firewall en NAT)

## Inhoud



## Inleiding

Deze voorbeeldconfiguratie blokkeert aanvankelijk het verkeer van een host device (op 10.31.1.47) op het interne netwerk naar alle apparaten op het internet totdat u browser-verificatie uitvoert 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 waarden toe na de vergunningverlening aan toegangslijst 116 die tijdelijk toegang van dat apparaat tot het internet toestaan.

## 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 12.2.2
- Cisco 3640 router

**Opmerking:** de **ip-opdracht** voor **automatische proxy** is 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.

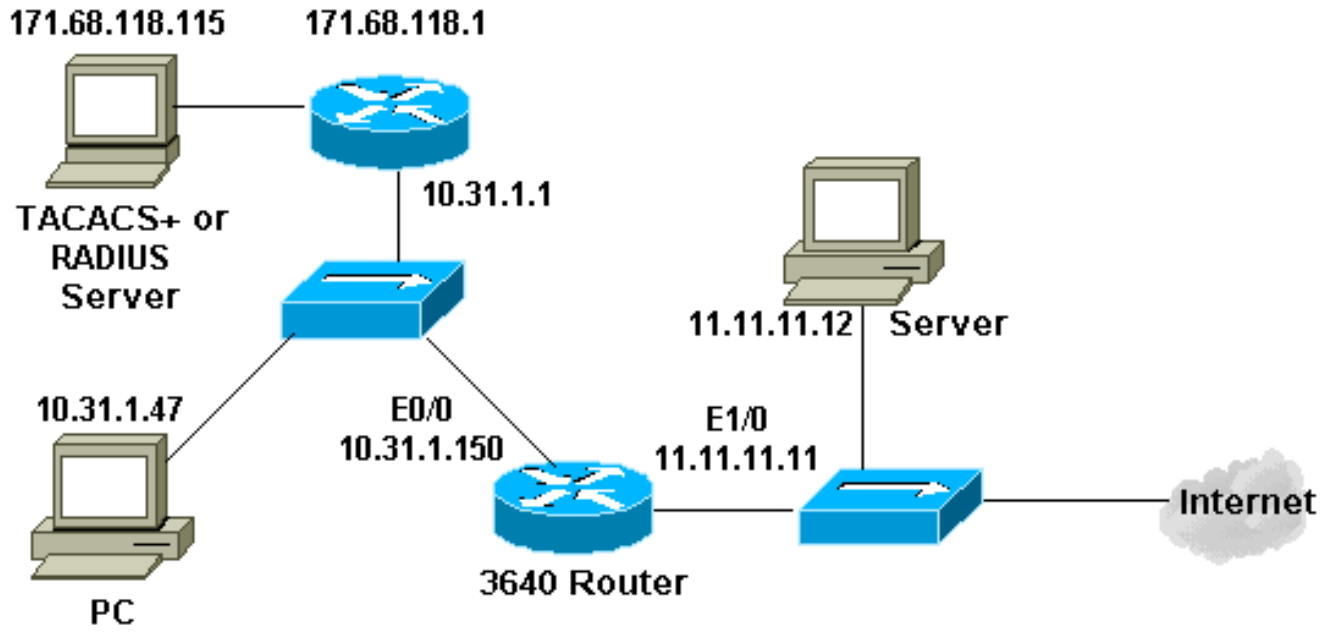
## Configureren

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:




### Configuraties

Dit document gebruikt deze configuratie:

| 3640 router |
| --- |
| Current configuration:<br>!<br>version 12.2<br>service timestamps debug uptime<br>service timestamps log uptime<br>no service password-encryption<br>! |

```
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
```

# Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

# Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Raadpleeg voor **debug** opdrachten, naast 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