# Configuratievoorbeeld van Cisco AUTOMATISCHE AANVULLING (Cisco IOS-firewall) - Routers/Switches en NAT

## Inhoud



## Inleiding

Deze voorbeeldconfiguratie blokkeert aanvankelijk verkeer van externe hosts naar alle apparaten op het interne netwerk tot browser authenticatie wordt uitgevoerd met verificatieproxy. Na toestemming voegt de toegangslijst die van de server is doorgegeven (**laat tcp|ip|icmp elke**) dynamische items toe aan toegangslijst 116 die tijdelijk toegang van de externe pc tot het interne netwerk mogelijk maken.

**Opmerking:** de AAA-configuratie die in dit document gebruikt wordt, is ook van toepassing op Catalyst-switches die Cisco IOS® software gebruiken.

## 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

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.

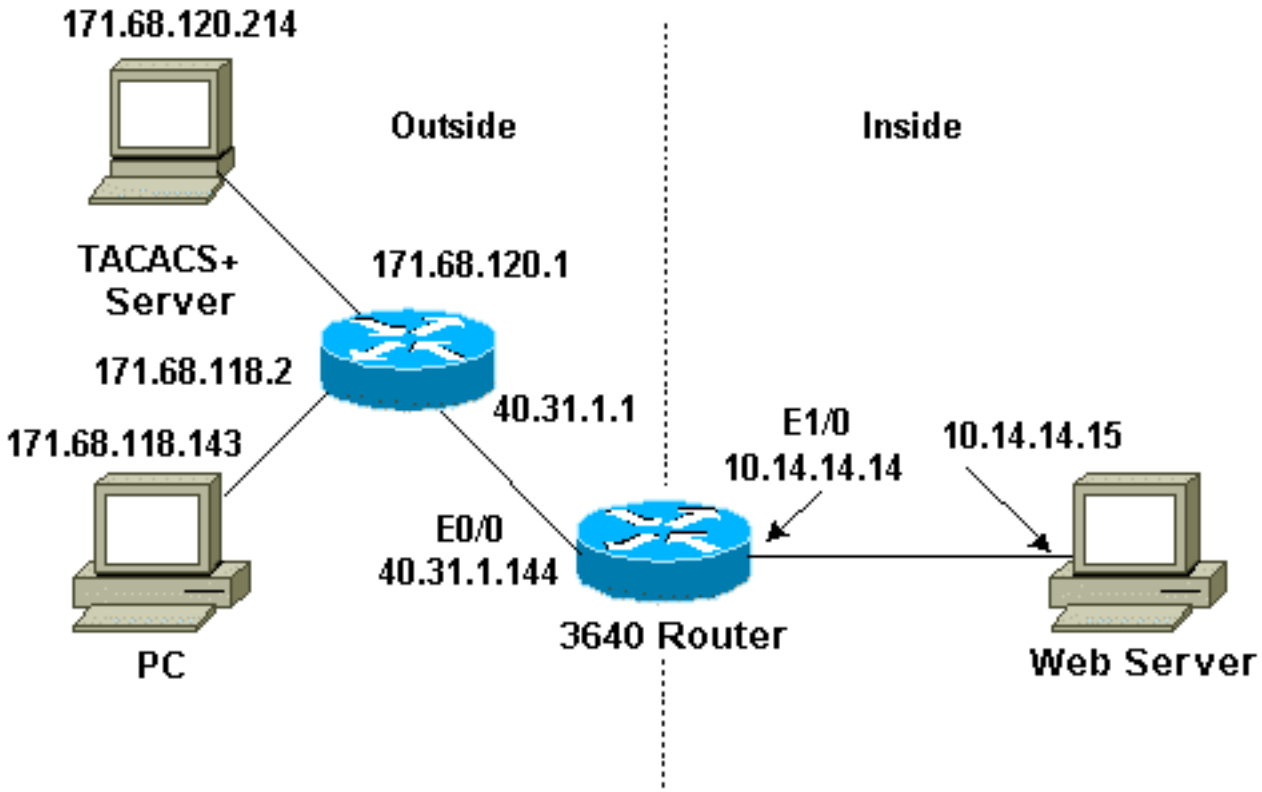
# Configureren

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:

- 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
```

## Verifiëren

Raadpleeg Belangrijke informatie over Debug Commands voordat u **debug**-opdrachten geeft.

Raadpleeg de verificatieproxy voor probleemoplossing voor opdracht- en probleemoplossing.

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

## Gerelateerde informatie

- Cisco IOS Firewall
- Ondersteuning van security en VPN-technologie
- Technische ondersteuning en documentatie – Cisco Systems