

Verificatieproxy-verificatie inkomende - geen Cisco IOS-firewall of NAT-configuratie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Deze voorbeeldconfiguratie blokkeert aanvankelijk verkeer van een host-apparaat (op 11.11.11.12) op het externe netwerk naar alle apparaten op het interne netwerk 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 items na autorisatie toe aan toegangslijst 115 die tijdelijk toegang van het host-apparaat 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** 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.

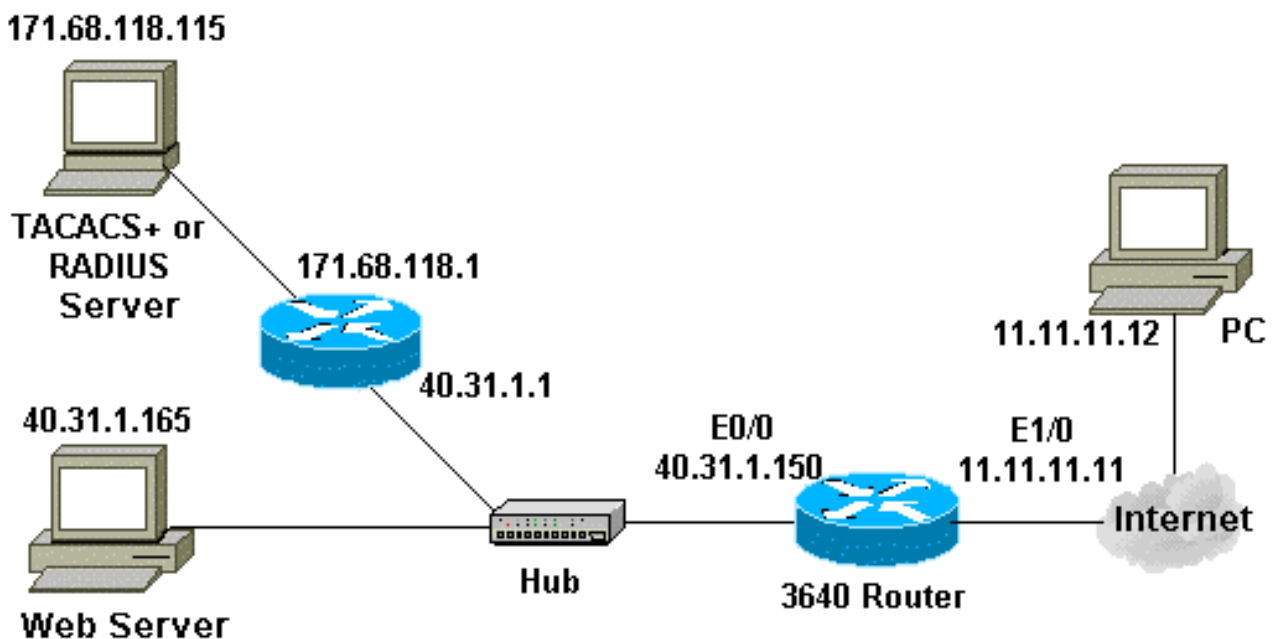
Configureren

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.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

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
!
!--- Turn on authentication. aaa new-model
!--- Define the server group and servers for TACACS+ or
RADIUS. aaa group server tacacs+|radius RTP
server 171.68.118.115
!
!--- Define what you need to authenticate. 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$z9bu5HMy4NTtjstvIhltGT0
enable password ww
!
ip subnet-zero
!
!--- You want the router name to appear as banner. ip
auth-proxy auth-proxy-banner
!--- You want the access-list entries to timeout after
10 minutes. ip auth-proxy auth-cache-time 10
!--- You define the list-name to be associated with the
interface. 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
no ip directed-broadcast
no mop enabled
!
interface FastEthernet1/0
ip address 11.11.11.11 255.255.255.0
!--- Apply the access-list to the interface. ip access-
group 115 in
no ip directed-broadcast
!--- Apply the auth-proxy list-name. ip auth-proxy
list_a
!
ip classless
ip route 171.68.118.0 255.255.255.0 40.31.1.1
!--- Turn on the http server and authentication. ip http
server
ip http authentication aaa
!
!--- This is our access-list for auth-proxy testing - !-
-- it denies only one host, 11.11.11.12, access - to
minimize disruption !--- to the network during testing.
access-list 115 permit tcp host 11.11.11.12 host
11.11.11.11 eq www
access-list 115 deny icmp host 11.11.11.12 any
access-list 115 deny tcp host 11.11.11.12 any
access-list 115 deny udp host 11.11.11.12 any
access-list 115 permit udp any any
access-list 115 permit tcp any any
access-list 115 permit icmp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
!--- Define the server(s). 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 verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

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](#)