

Authentifizierungsproxyauthentifizierung eingehend - Keine Cisco IOS-Firewall oder NAT- Konfiguration

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

[Einführung](#)

Diese Beispielkonfiguration blockiert zunächst den Datenverkehr von einem Hostgerät (bei 11.11.11.12) im externen Netzwerk zu allen Geräten im internen Netzwerk, bis Sie die Browser-Authentifizierung mithilfe eines Authentifizierungsproxys durchführen. Die vom Server übergebene Zugriffsliste (**permit tcp|ip|icmp any any**) fügt der Zugriffsliste 115 nach der Autorisierung dynamische Einträge hinzu, die vorübergehend den Zugriff vom Host-Gerät auf das interne Netzwerk erlauben.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.0.7.T
- Cisco Router 3640

Hinweis: Der Befehl `ip auth-proxy` wurde in Version 12.0.5.T der Cisco IOS-Software eingeführt.

Diese Konfiguration wurde mit Version 12.0.7.T der Cisco IOS-Software getestet.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

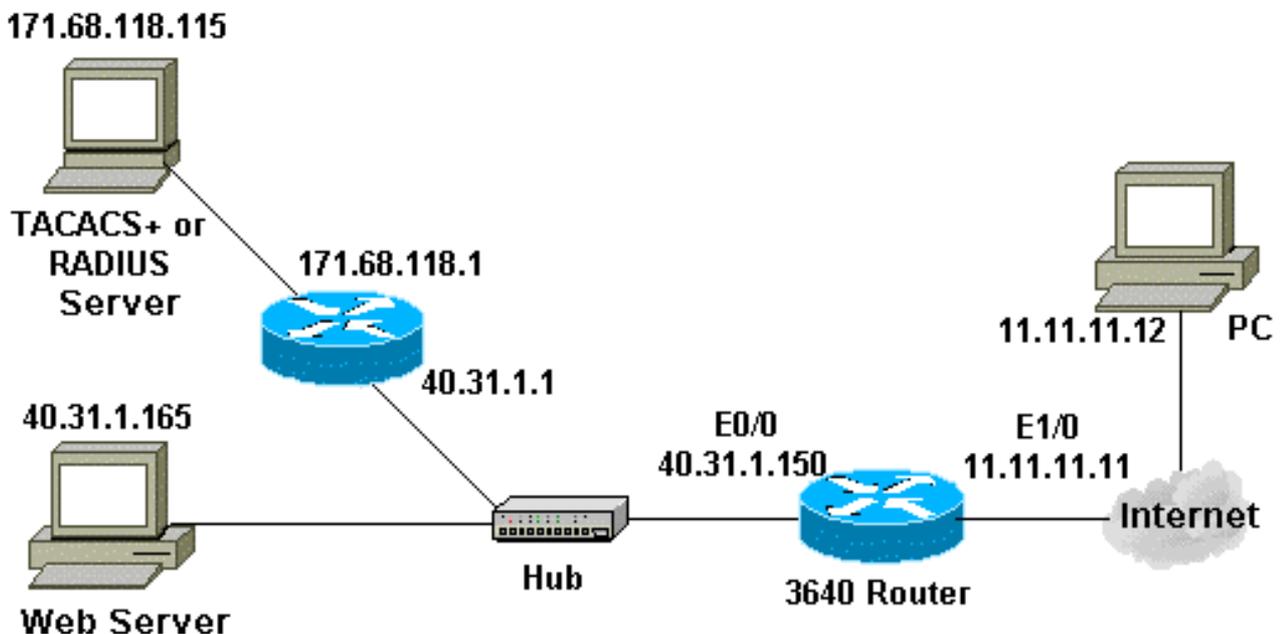
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument wird diese Konfiguration verwendet:

Router 3640
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Weitere Informationen zu diesen Befehlen sowie weitere Informationen zur Fehlerbehebung finden Sie unter [Troubleshooting Authentication Proxy](#).

Hinweis: Lesen Sie [vor dem](#) Ausgabe von **Debug**-Befehlen unter [Wichtige Informationen zu Debug-Befehlen nach](#).

Zugehörige Informationen

- [Support-Seite für IOS-Firewall](#)
- [Support-Seite für TACACS/TACACS+](#)
- [TACACS+ in der IOS-Dokumentation](#)
- [RADIUS-Support-Seite](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)