Konfiguration der eingehenden Auth-Proxy-Authentifizierung (Cisco IOS Firewall, kein NAT)

Inhalt

Einführung

Diese Beispielkonfiguration blockiert zunächst den Datenverkehr von externen Hosts zu allen Geräten im internen Netzwerk, bis die Browser-Authentifizierung mithilfe des Authentifizierungsproxys erfolgt. 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 externen PC 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** wird 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).

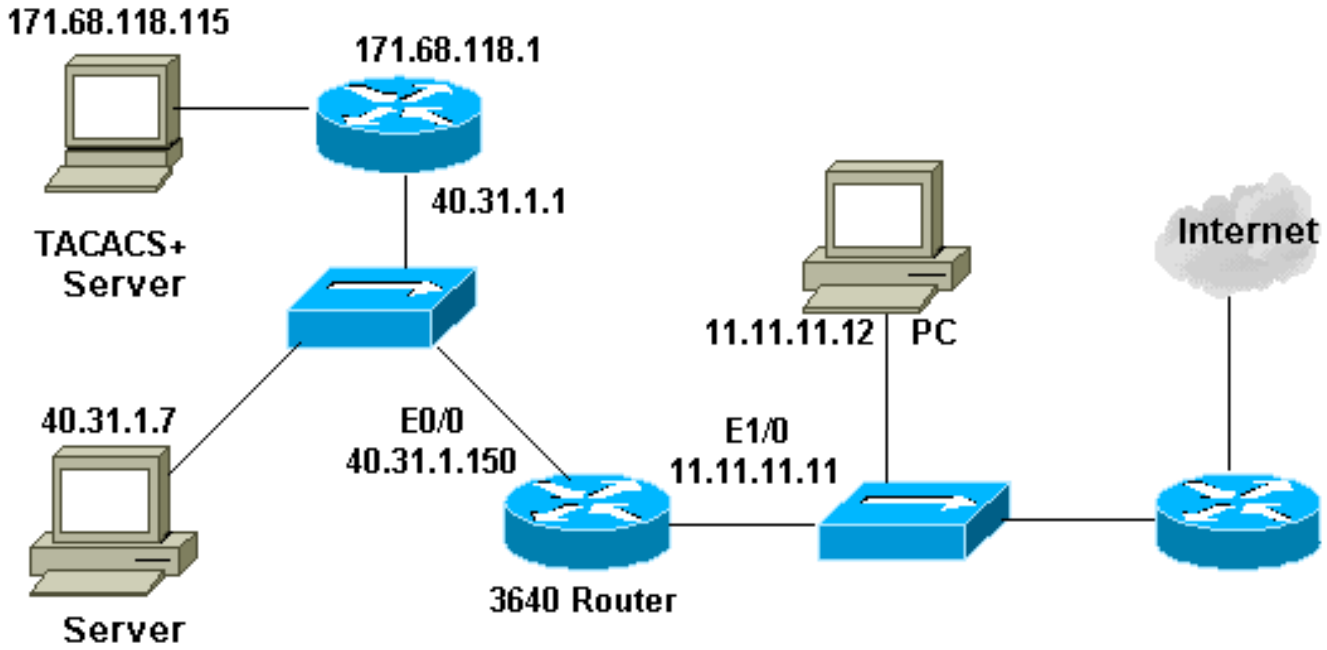
Konfigurieren

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:



Konfiguration

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
!
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

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