Konfigurationsbeispiel für die eingehende Auth-Proxy-Authentifizierung (Cisco IOS Firewall - Router/Switches und 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. Nach der Autorisierung fügt die vom Server übergebene Zugriffsliste (**permit tcp|ip|icmp any any any any**) dynamische Einträge zur Zugriffsliste 116 hinzu, die vorübergehend den Zugriff vom externen PC auf das interne Netzwerk erlauben.

Hinweis: Die in diesem Dokument verwendete AAA-Konfiguration gilt auch für Catalyst Switches, auf denen die Cisco IOS® Software ausgeführt wird.

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 12.2.23

- Cisco Router 3640

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).

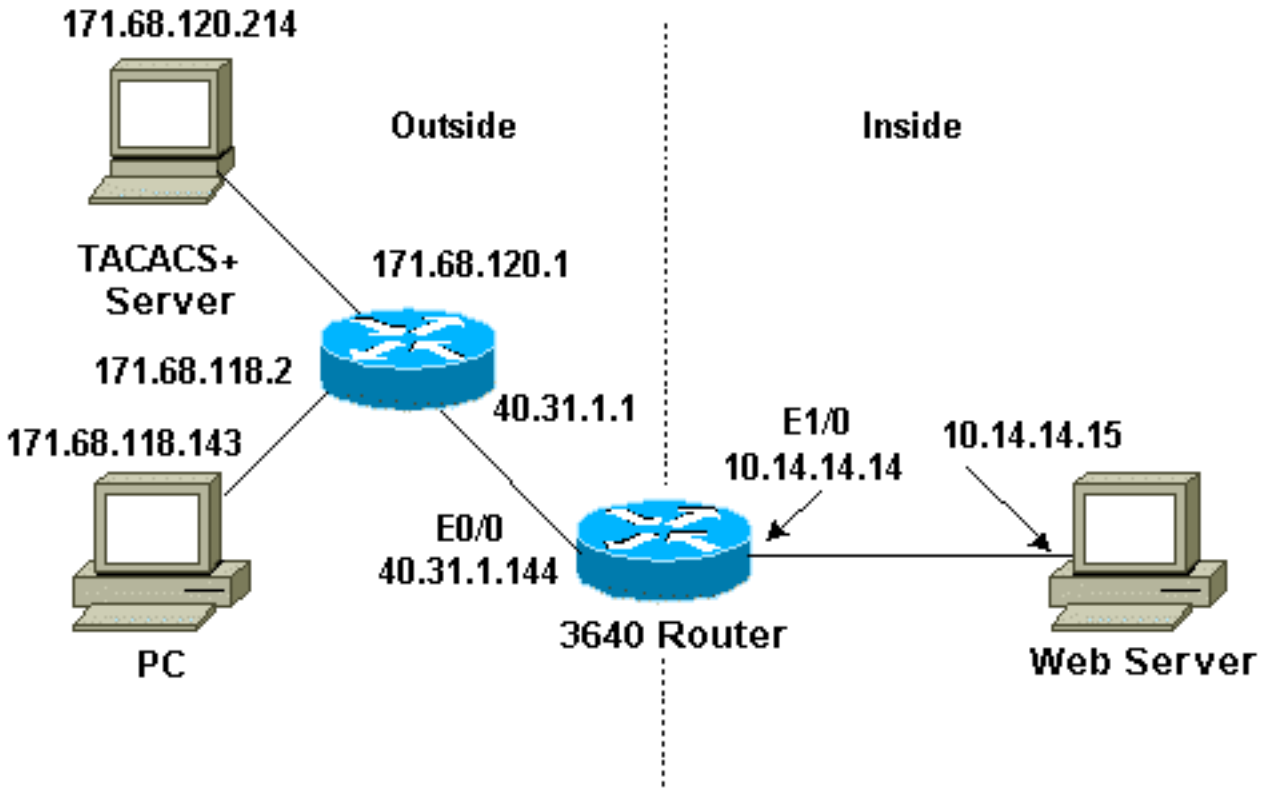
Konfigurieren

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:

- Cisco Router 3640

Cisco Router 3640

```
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
```

Überprüfen

Weitere Informationen zu Debug-Befehlen finden Sie vor dem Ausgeben von **Debug-**Befehlen unter Wichtige Informationen.

Informationen zu Befehlen und Fehlerbehebung finden Sie unter Troubleshooting Authentication Proxy (Fehlerbehebung bei Authentifizierungsproxys).

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco IOS-Firewall
- Unterstützung von Sicherheits- und VPN-Technologie
- Technischer Support und Dokumentation - Cisco Systems