Esempio di configurazione dell'autenticazione proxy di autenticazione in entrata (Cisco IOS Firewall - Router/switch e NAT)

Sommario

Introduzione

Questa configurazione di esempio blocca inizialmente il traffico dagli host esterni a tutti i dispositivi della rete interna finché l'autenticazione del browser non viene eseguita utilizzando il proxy di autenticazione. Dopo l'autorizzazione, l'elenco degli accessi passato dal server (**consenti tcp|ip|icmp any**) aggiunge voci dinamiche all'elenco degli accessi 116 che consentono temporaneamente l'accesso alla rete interna dal PC esterno.

Nota: la configurazione AAA usata in questo documento è applicabile anche agli switch Catalyst con software Cisco IOS®.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS Software Release 12.2.23

- Cisco 3640 router

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

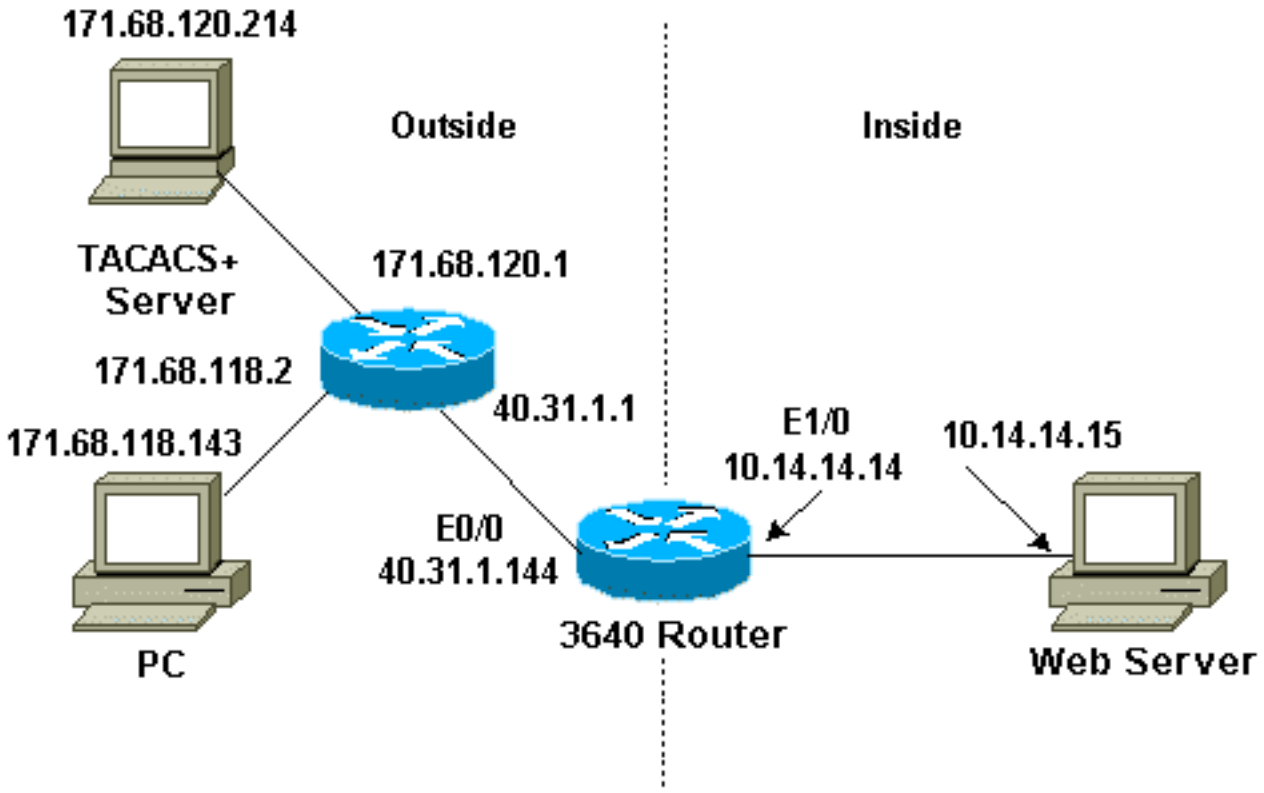
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento viene usata questa configurazione:

- 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
```

Verifica

consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Per informazioni sul comando e sulla risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi del proxy di autenticazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco IOS Firewall
- Sicurezza e supporto della tecnologia VPN
- Documentazione e supporto tecnico – Cisco Systems