Configurazione dell'autenticazione proxy di autenticazione in uscita (Cisco IOS Firewall e NAT)

Sommario

Introduzione

Questa configurazione di esempio blocca inizialmente il traffico proveniente da un dispositivo host (versione 10.31.1.47) sulla rete interna e diretto a tutti i dispositivi su Internet finché non si esegue l'autenticazione del browser con l'utilizzo del proxy di autenticazione. L'elenco degli accessi passato dal server (**consenti tcp|ip|icmp any any**) aggiunge voci dinamiche post-autorizzazione all'elenco degli accessi 116 che consentono temporaneamente l'accesso a Internet da tale dispositivo.

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:

- Software Cisco IOS® versione 12.2.23
- Cisco 3640 router

Nota: il comando **ip auth-proxy** è stato introdotto nel software Cisco IOS versione 12.0.5.T. Questa

configurazione è stata testata con il software Cisco IOS versione 12.0.7.T.

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.

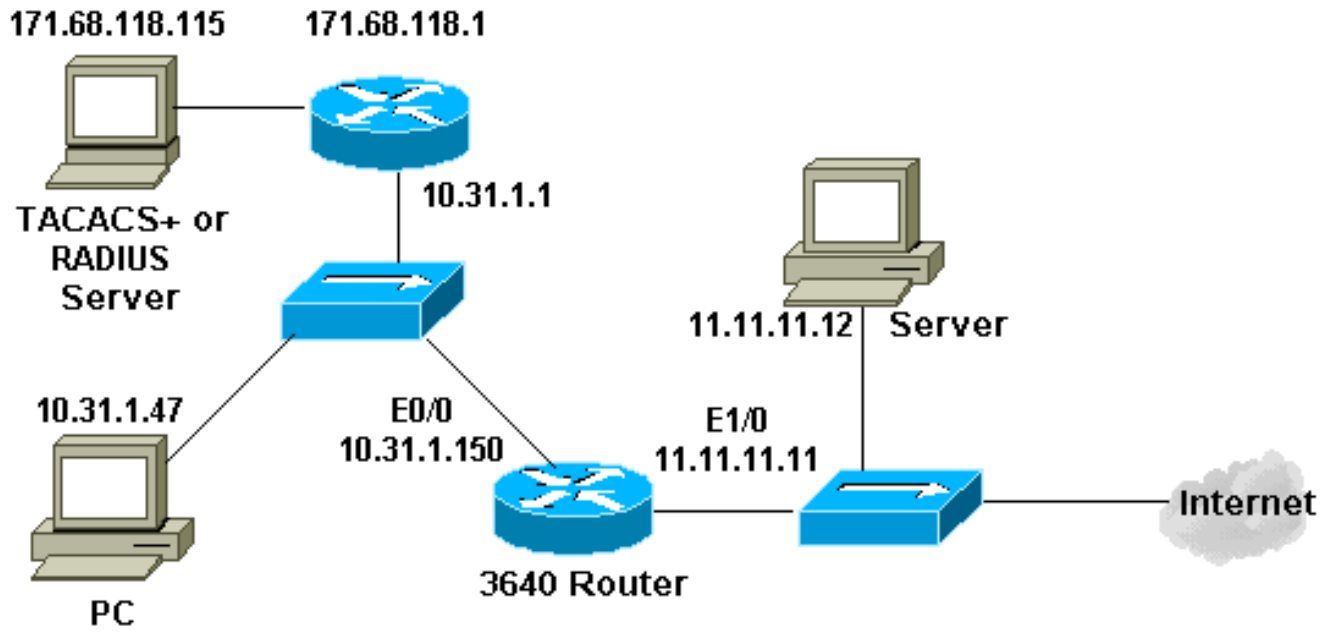
Configurazione

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:

3640 Router
`Current configuration:` `!`

```
version 12.2
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 local group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$vCfr$rkuU6HLmpbNgLTg/JNM6e1
enable password ww
!
username john password 0 doe
!
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
!
process-max-time 200
!
interface Ethernet0/0
 ip address 10.31.1.150 255.255.255.0
 ip access-group 116 in
 ip nat inside
 ip inspect myfw in
 ip auth-proxy list_a
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet1/0
 ip address 11.11.11.11 255.255.255.0
 ip access-group 101 in
 ip nat outside
!
ip nat pool outsidepool 11.11.11.20 11.11.11.30 netmask
255.255.255.0
ip nat inside source list 1 pool outsidepool
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 10.31.1.1
ip http server
ip http authentication aaa
!
```

```
access-list 1 permit 10.31.1.0 0.0.0.255
access-list 101 deny   ip 10.31.1.0 0.0.0.255 any
access-list 101 deny   ip 127.0.0.0 0.255.255.255 any
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
unreachable
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
echo-reply
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
packet-too-big
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
time-exceeded
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
traceroute
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
administratively-prohibited
access-list 101 permit icmp any 11.11.11.0 0.0.0.255
echo
access-list 116 permit tcp host 10.31.1.47 host
10.31.1.150 eq www
access-list 116 deny   tcp host 10.31.1.47 any
access-list 116 deny   udp host 10.31.1.47 any
access-list 116 deny   icmp host 10.31.1.47 any
access-list 116 permit tcp 10.31.1.0 0.0.0.255 any
access-list 116 permit udp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 10.31.1.0 0.0.0.255 any
access-list 116 permit icmp 171.68.118.0 0.0.0.255 any
access-list 116 permit tcp 171.68.118.0 0.0.0.255 any
access-list 116 permit udp 171.68.118.0 0.0.0.255 any
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 auth-port 1645 acct-
port 1646
radius-server key cisco
!
line con 0
 transport input none
line aux 0
line vty 0 4
 exec-timeout 0 0
 password ww
!
end
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per i comandi **debug** e altre informazioni sulla risoluzione dei problemi, consultare il documento sulla risoluzione dei problemi del proxy di autenticazione.

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

Informazioni correlate

- Pagina di supporto di IOS Firewall
- Pagina di supporto TACACS/TACACS+
- Documentazione relativa a TACACS+ in IOS
- Pagina di supporto RADIUS
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems