Configuración saliente de la autenticación auth-proxy (Firewall Cisco IOS y NAT)

Contenido

Introducción

Esta configuración de muestra bloquea inicialmente el tráfico de un dispositivo host (en 10.31.1.47) en la red interna a todos los dispositivos en Internet hasta que usted realice la autenticación de buscador con el uso del Proxy de autenticación. La lista de acceso se transmitió desde el servidor (permit tcp**|ip|el ICMP cualquier ninguno**) agrega el poste authorization de las entradas dinámicas a la lista de acceso 116 que permite temporalmente el acceso de ese dispositivo a Internet.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Release 12.2.23 de Cisco IOS®
- Cisco 3640 Router

Nota: Se introdujo el comando ip auth-proxy en el software IOS de Cisco versión 12.0.5.T. Esta configuración fue probada con el Cisco IOS Software Release 12.0.7.T.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

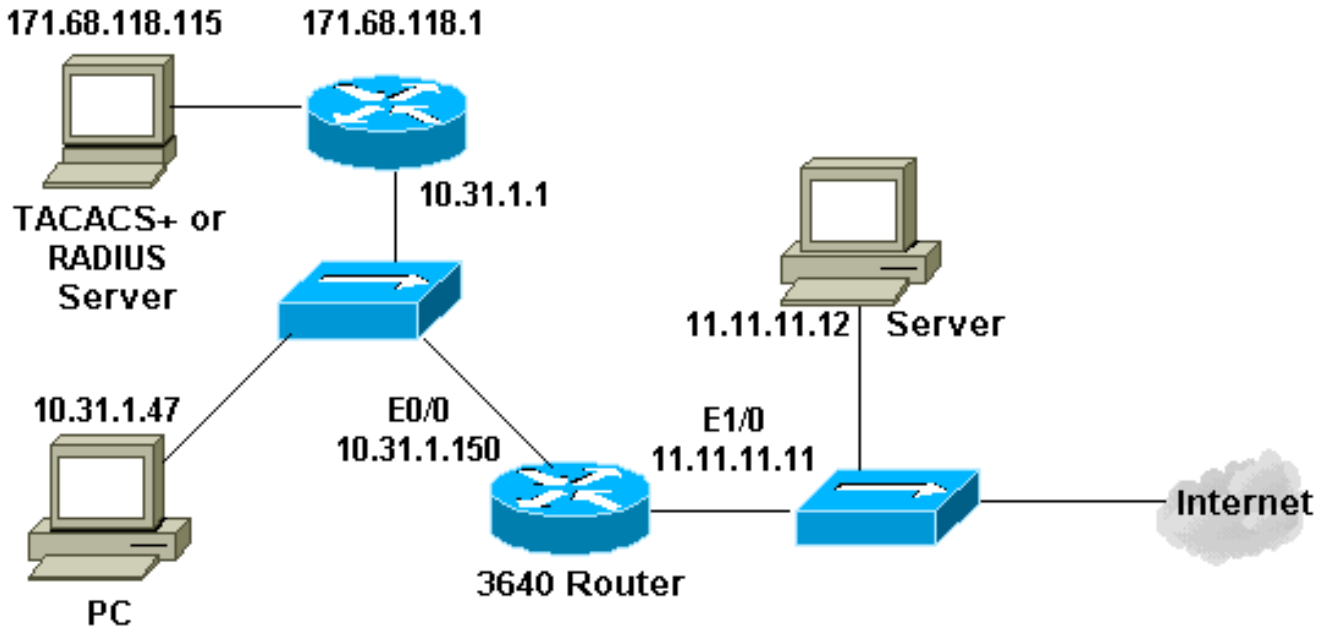
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

Este documento usa esta configuración:

Router 3640

```
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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Para los **comandos debug**, junto con la otra información de Troubleshooting, refiera al Proxy de autenticación del troubleshooting.

Nota: Consulte información importante en los comandos debug antes de ejecutar los comandos debug.

Información Relacionada

- Página de soporte de firewall de IOS
- Página de soporte de TACACS/TACACS+
- TACACS+ en documentación de IOS
- Página de soporte de RADIUS
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems