Auth−proxy Authentication Inbound (Cisco IOS Firewall − Routers/Switches and NAT) Configuration Example

Document ID: 13890

Contents

Introduction

This sample configuration initially blocks traffic from external hosts to all devices on the internal network until browser authentication is performed using authentication proxy. After authorization, the access list passed down from the server (**permit tcp|ip|icmp any any**) adds dynamic entries to access list 116 that temporarily allow access from the external PC to the internal network.

Note: The AAA configuration used in this document is also applicable to Catalyst switches that run Cisco IOS® software.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS Software Release 12.2.23
- Cisco 3640 router

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

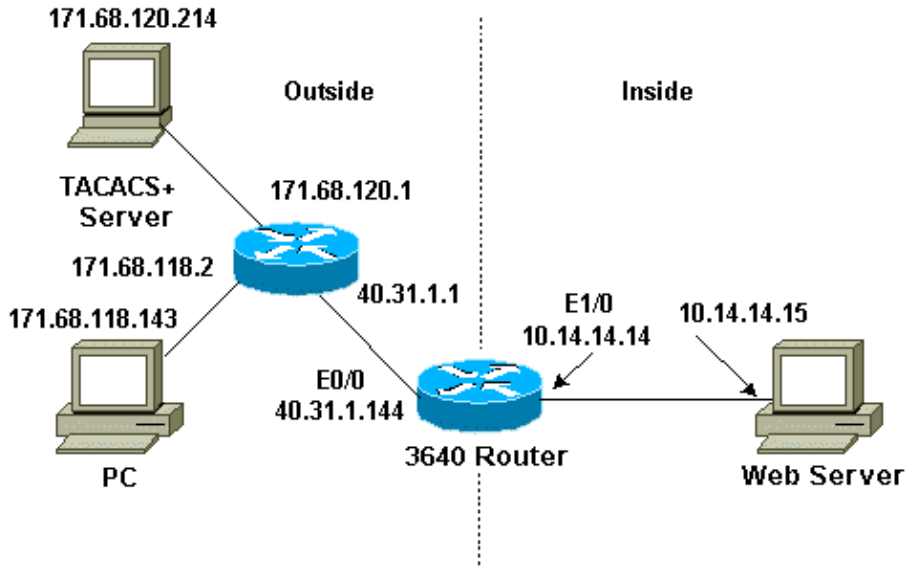
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses this configuration:

- 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
```

Verify

Refer to Important Information on Debug Commands before you issue **debug** commands.

Refer to Troubleshooting Authentication Proxy for command and troubleshooting information.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Cisco IOS Firewall**
- **Security and VPN Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 15, 2006 Document ID: 13890