Auth−proxy Authentication Inbound (Cisco IOS Firewall, no NAT) Configuration

Document ID: 13888

Contents

Introduction

This sample configuration initially blocks traffic from external hosts to all devices on the internal network until browser authentication is performed with the use of authentication proxy. The access list passed down from the server (**permit tcp|ip|icmp any any**) adds dynamic entries post−authorization to access−list 115 that temporarily allow access from the external PC to the internal network.

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 12.0.7.T
- Cisco 3640 router

Note: The **ip auth−proxy** command is introduced in Cisco IOS Software Release 12.0.5.T. This configuration was tested with Cisco IOS Software Release 12.0.7.T.

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.

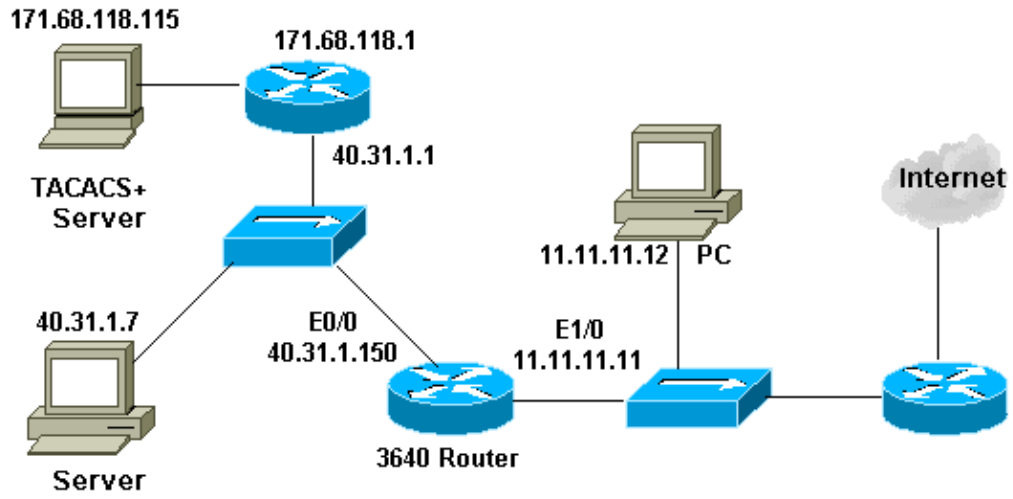
Configure

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:



Configuration

This document uses this configuration:

3640 Router

```
Current configuration:
!
version 12.0
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 group RTP none
aaa authorization exec default group RTP none
aaa authorization auth-proxy default group RTP
enable secret 5 $1$H9zZ$z9bu5HMy4NTtjsvIhltGT0
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 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
cns event-service server
!
process-max-time 200
!
interface FastEthernet0/0
 ip address 40.31.1.150 255.255.255.0
 ip access-group 101 in
 no ip directed-broadcast
 ip inspect myfw in
 no mop enabled
!
interface FastEthernet1/0
 ip address 11.11.11.11 255.255.255.0
 ip access-group 115 in
 no ip directed-broadcast
 ip auth-proxy list_a
!
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 40.31.1.1
ip http server
ip http authentication aaa
!
access-list 101 permit icmp 40.31.1.0 0.0.0.255 any
access-list 101 permit tcp 40.31.1.0 0.0.0.255 any
access-list 101 permit udp 40.31.1.0 0.0.0.255 any
access-list 101 permit icmp 171.68.118.0 0.0.0.255 any
access-list 101 permit tcp 171.68.118.0 0.0.0.255 any
access-list 101 permit udp 171.68.118.0 0.0.0.255 any
access-list 115 permit tcp host 11.11.11.12 host 11.11.11.11 eq www
access-list 115 deny   tcp any any
access-list 115 deny   udp any any
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 echo
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 echo-reply
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 packet-too-big
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 time-exceeded
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 traceroute
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 unreachable
access-list 115 permit icmp any 40.31.1.0 0.0.0.255 administratively-prohibited
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
radius-server key cisco

!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
!
```

```
!
end
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

For these commands, along with other troubleshooting information, refer to Troubleshooting Authentication Proxy.

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

Related Information

- **IOS Firewall Support Page**
- **IOS Firewall in IOS Documentation**
- **TACACS/TACACS+ Support Page**
- **TACACS+ in IOS Documentation**
- **RADIUS Support Page**
- **RADIUS in IOS Documentation**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 15, 2006 Document ID: 13888