

Auth-proxy Authentication Outbound (Cisco IOS Firewall – Routers/Switches, no NAT) Configuration

Document ID: 13886

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Troubleshoot

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This sample configuration initially blocks traffic from a host device (at 40.31.1.47) on the internal network to all devices on the Internet until you perform browser authentication 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 116 that temporarily allow access from the host device to the Internet.

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 12.0.7.T
- Cisco 3640 router

Note: The **ip auth-proxy** command was 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.

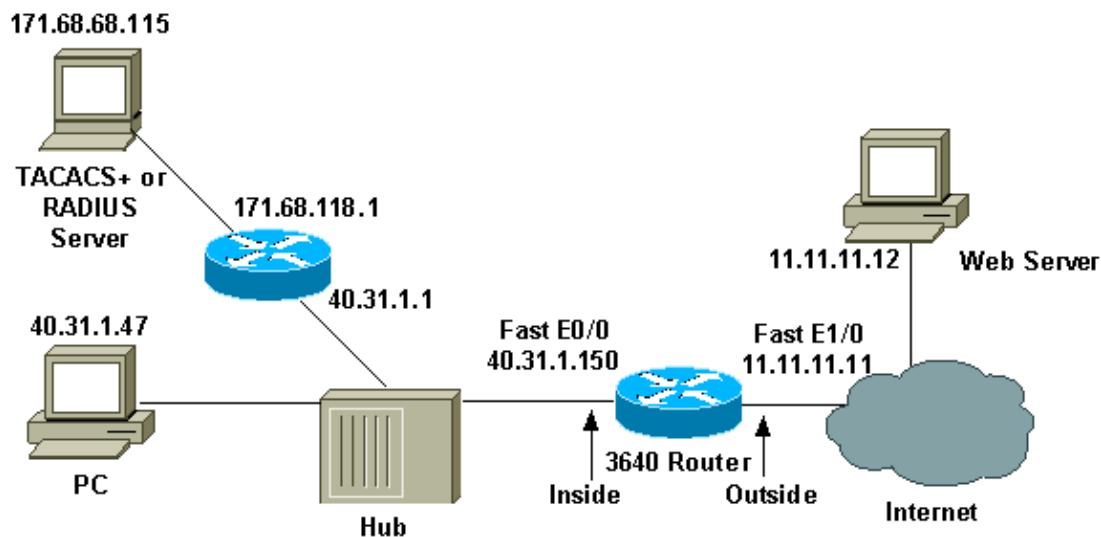
Configure

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:



Configurations

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+|radius 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
cns event-service server
!
process-max-time 200
!

!--- Inside interface.

interface FastEthernet0/0
 ip address 40.31.1.150 255.255.255.0
 ip access-group 116 in
 no ip directed-broadcast
 ip inspect myfw in
 ip auth-proxy list_a
 no ip route-cache
 no ip mroute-cache
 no mop enabled
!

!--- Outside interface.

interface FastEthernet1/0
 ip address 11.11.11.11 255.255.255.0
 ip access-group 101 in
 no ip directed-broadcast
 no mop enabled
!
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 deny ip 40.31.1.0 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 40.31.1.0 0.0.0.255 administratively-prohibited
access-list 101 permit icmp any 40.31.1.0 0.0.0.255 echo
access-list 101 permit icmp any 40.31.1.0 0.0.0.255 echo-reply
access-list 101 permit icmp any 40.31.1.0 0.0.0.255 packet-too-big
access-list 101 permit icmp any 40.31.1.0 0.0.0.255 time-exceeded
access-list 101 permit icmp any 40.31.1.0 0.0.0.255 traceroute
access-list 101 permit icmp any 40.31.1.0 0.0.0.255 unreachable
access-list 101 deny ip any any
access-list 116 permit tcp host 40.31.1.47 host 40.31.1.150 eq www
access-list 116 deny tcp host 40.31.1.47 any
access-list 116 deny udp host 40.31.1.47 any
access-list 116 deny icmp host 40.31.1.47 any

```

```

access-list 116 permit tcp 40.31.1.0 0.0.0.255 any
access-list 116 permit udp 40.31.1.0 0.0.0.255 any
access-list 116 permit icmp 40.31.1.0 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

```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

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

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

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

| |
|--|
| NetPro Discussion Forums – Featured Conversations for Security |
| Security: Intrusion Detection [Systems] |
| Security: AAA |
| Security: General |
| Security: Firewalling |

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**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 15, 2006

Document ID: 13886
