

Authentication Proxy Authentication Inbound – No Cisco IOS Firewall or NAT Configuration

Document ID: 13885

Introduction

Prerequisites

Requirements

Components Used

Conventions

Configure

Network Diagram

Configurations

Verify

Troubleshoot

Related Information

Introduction

This sample configuration initially blocks traffic from a host device (at 11.11.11.12) on the external network to all devices on the internal network 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-authentication to access list 115 that temporarily allow access from the host device 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 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.

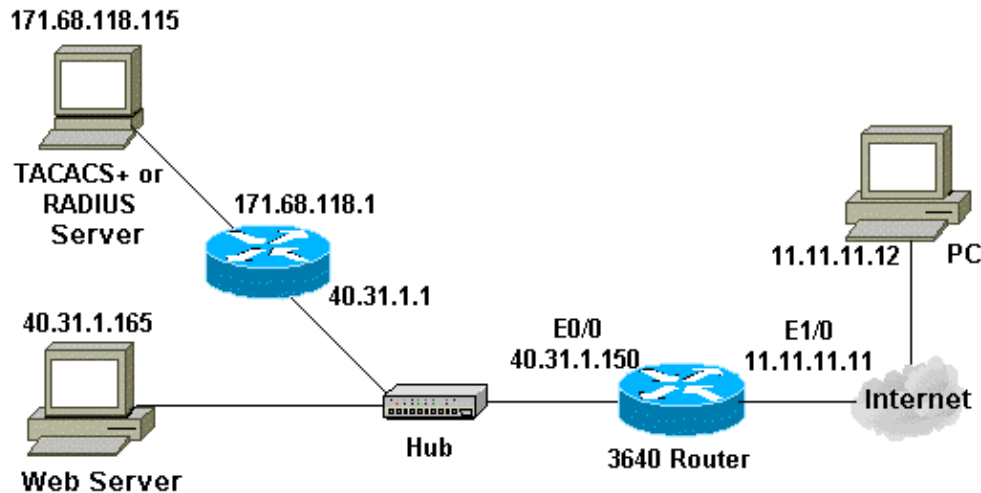
Configure

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
!
!--- Turn on authentication.
aaa new-model
!--- Define the server group and servers for TACACS+ or RADIUS.
aaa group server tacacs+|radius RTP
server 171.68.118.115
!
!--- Define what you need to authenticate.
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$z9bu5HMy4NTtjstvIhltGT0
enable password ww
!
ip subnet-zero
!

/--- You want the router name to appear as banner.

ip auth-proxy auth-proxy-banner

/--- You want the access-list entries to timeout after 10 minutes.

ip auth-proxy auth-cache-time 10

/--- You define the list-name to be associated with the interface.

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
 no ip directed-broadcast
 no mop enabled
!
interface FastEthernet1/0
 ip address 11.11.11.11 255.255.255.0

/--- Apply the access-list to the interface.

ip access-group 115 in
 no ip directed-broadcast

/--- Apply the auth-proxy list-name.

 ip auth-proxy list_a
!
ip classless
ip route 171.68.118.0 255.255.255.0 40.31.1.1

/--- Turn on the http server and authentication.

ip http server
ip http authentication aaa
!

/--- This is our access-list for auth-proxy testing -
/--- it denies only one host, 11.11.11.12, access - to minimize disruption
/--- to the network during testing.

access-list 115 permit tcp host 11.11.11.12 host 11.11.11.11 eq www
access-list 115 deny icmp host 11.11.11.12 any
access-list 115 deny tcp host 11.11.11.12 any
access-list 115 deny udp host 11.11.11.12 any
access-list 115 permit udp any any
access-list 115 permit tcp any any
access-list 115 permit icmp any any
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!

/--- Define the server(s).
```

```
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 in order 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](#)

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 15, 2006

Document ID: 13885
