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

Document ID: 13884

Contents

Introduction

The Authentication Proxy feature allows users to log in to the network or access the Internet via HTTP, with their specific access profiles automatically retrieved and applied from a RADIUS, or TACACS+ server. The user profiles are active only when there is active traffic from the authenticated users.

This sample configuration blocks traffic from the host device (at 40.31.1.47) on the internal network to all devices on the Internet until browser authentication is performed with the use of Authentication Proxy. The access control list (ACL) 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 PC to the Internet.

Refer to Configuring Authentication Proxy for more information on Authentication Proxy.

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(15)T
- Cisco 7206 router

Note: The **ip auth−proxy** command was introduced in Cisco IOS Firewall Software Release 12.0.5.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 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 find more information on the commands used in this document.

Network Diagram

This document uses this network setup:
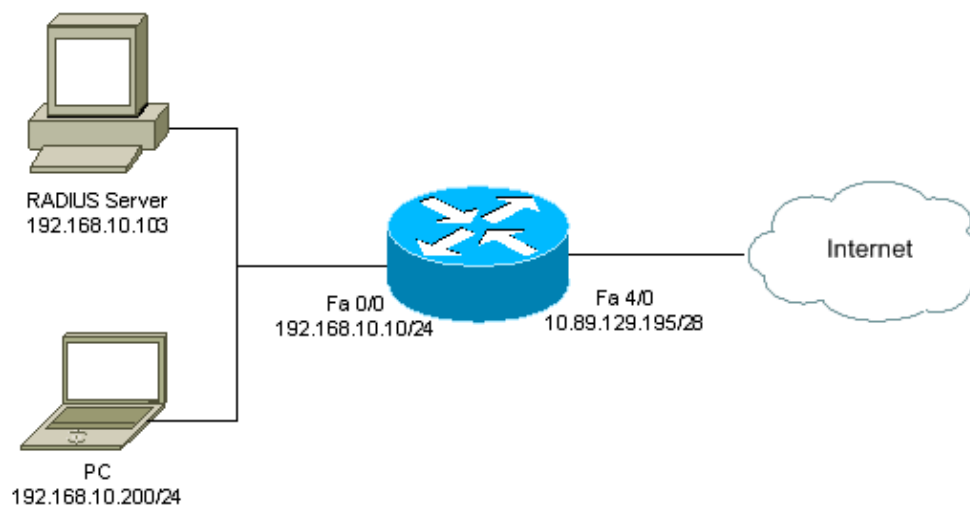
Configuration

This document uses this configuration:

7206 Router

```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model


!--- Enable AAA.


aaa authentication login default group radius none
```

```
!--- Use RADIUS to authenticate users.

aaa authorization exec default group radius none
aaa authorization auth-proxy default group radius


!--- Utilize RADIUS for auth-proxy authorization.

aaa session-id common
ip subnet-zero
!
ip cef
!
ip auth-proxy auth-proxy-banner


!--- Displays the name of the firewall router
!--- in the Authentication Proxy login page.

ip auth-proxy auth-cache-time 10


!--- Sets the global Authentication Proxy idle
!--- timeout value in minutes.


ip auth-proxy name restrict_pc http


!--- Associates connections that initiate HTTP traffic with
!--- the "restrict_pc" Authentication Proxy name.


ip audit notify log
ip audit po max-events 100
!
no voice hpi capture buffer
no voice hpi capture destination
!
mta receive maximum-recipients 0
!
!
interface FastEthernet0/0
 ip address 192.168.10.10 255.255.255.0
 ip access-group 116 in


!--- Apply access list 116 in the inbound direction.

 ip auth-proxy restrict_pc


!--- Apply the Authentication Proxy list
!--- "restrict_pc" configured earlier.


 duplex full
!
interface FastEthernet4/0
 ip address 10.89.129.195 255.255.255.240
 duplex full
!
ip classless
ip http server
```

```
!--- Enables the HTTP server on the router.


!--- The Authentication Proxy uses the HTTP server to communicate
!--- with the client for user authentication.


ip http authentication aaa


!--- Sets the HTTP server authentication method to AAA.


!
access-list 116 permit tcp host 192.168.10.200 host 192.168.10.10 eq www


!--- Permit HTTP traffic (from the PC) to the router.


access-list 116 deny tcp host 192.168.10.200 any
access-list 116 deny udp host 192.168.10.200 any
access-list 116 deny icmp host 192.168.10.200 any


!--- Deny TCP, UDP, and ICMP traffic from the client by default.


access-list 116 permit tcp 192.168.10.0 0.0.0.255 any
access-list 116 permit udp 192.168.10.0 0.0.0.255 any
access-list 116 permit icmp 192.168.10.0 0.0.0.255 any


!--- Permit TCP, UDP, and ICMP traffic from other
!--- devices in the 192.168.10.0/24 network.

!
radius-server host 192.168.10.103 auth-port 1645 acct-port 1646 key 7 <deleted>


!--- Specify the IP address of the RADIUS
!--- server along with the key.


radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
end
```
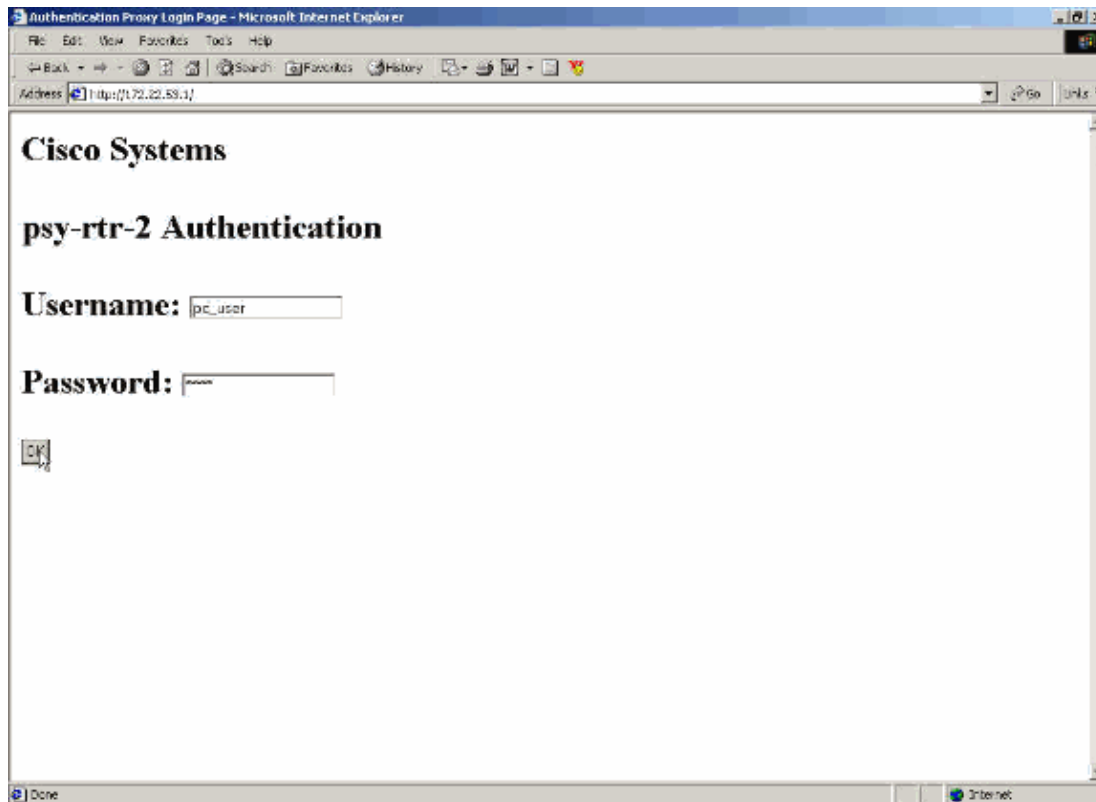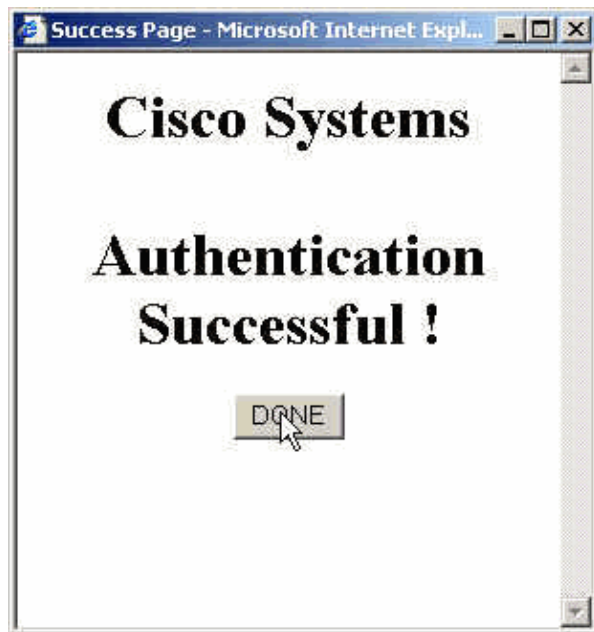
Authentication on the PC

This section provides screen captures taken from the PC that show the authentication procedure. The first capture shows the window where a user enters the username and password for authentication and presses **OK**.

If authentication is successful, this window appears.

The RADIUS server must be configured with the proxy ACLs that are applied. In this example, these ACL entries are applied. This permits the PC to connect to any device.

```
permit tcp host 192.168.10.200 any
permit udp host 192.168.10.200 any
permit icmp host 192.168.10.200 any
```

This Cisco ACS window shows where to enter the proxy ACLs.
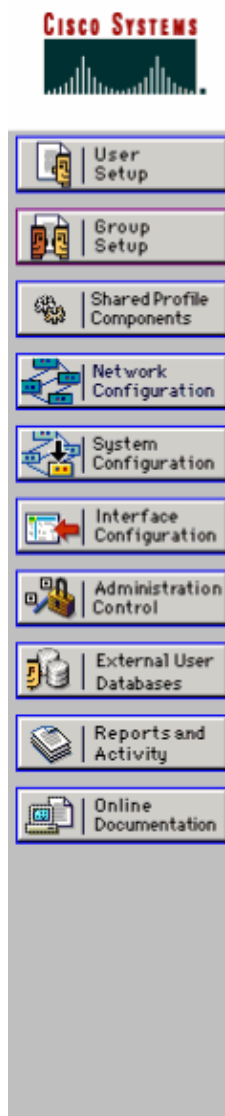
Group Setup

Jump To Access Restrictions

Unlisted arguments
- ○ Permit
- ⊙ Deny

Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

```
auth-proxy:priv-lvl=15
auth-proxy:proxyacl#1=permit
tcp host 192.168.10.200 any
auth-proxy:proxyacl#2=permit
udp host 192.168.10.200 any
```

☐ [009\101] cisco-h323-credit-amount

☐ [009\102] cisco-h323-credit-time

☐ [009\103] cisco-h323-return-code

Submit   Submit + Restart   Cancel

Note: Refer to Configuring Authentication Proxy for more information on how to configure the RADIUS/TACACS+ server.

Verify

This section provides information you can use to confirm your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show ip access−lists** Displays the standard and extended ACLs configured on the firewall (includes dynamic ACL entries). The dynamic ACL entries are added and removed periodically based on whether the user authenticates or not.
- **show ip auth−proxy cache** Displays either the Authentication Proxy entries or the running Authentication Proxy configuration. The cache keyword to list the host IP address, the source port number, the timeout value for the Authentication Proxy, and the state for connections that use Authentication Proxy. If the Authentication Proxy state is HTTP_ESTAB, the user authentication is a success.

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 use **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**