

# Performing Authentication, Authorization, and Accounting of Users Through PIX Versions 5.2 and Later

Document ID: 8527

---

## **Introduction**

### **Prerequisites**

- Requirements
- Components Used
- Conventions
- Authentication, Authorization, and Accounting
- What the User Sees with Authentication/Authorization On
- Debugging Steps

### **Authentication Only**

- Network Diagram
- Server Setup – Authentication Only
- Configurable RADIUS Ports (5.3 and Later)
- PIX Authentication Debug Examples

### **Authentication Plus Authorization**

- Server Setup – Authentication plus Authorization
- PIX Configuration – Adding Authorization
- PIX Authentication and Authorization Debug Examples
- New Access List Feature
- PIX Configuration
- Server Profiles
- New Per–User Downloadable Access List With Version 6.2

### **Add Accounting**

- PIX Configuration – Add Accounting
- Accounting Examples

### **Use of the exclude Command**

### **Max–sessions and View Logged–in Users**

### **User Interface**

- Change the Prompt Users See
- Customize the Message Users See

### **Per–User Idle and Absolute Timeouts**

### **Virtual HTTP Outbound**

### **Virtual Telnet**

- Virtual Telnet Inbound
- Virtual Telnet Outbound
- Virtual Telnet Logout

### **Port Authorization**

- Network Diagram

### **AAA Accounting for Traffic Other Than HTTP, FTP, and Telnet**

- Example of TACACS+ Accounting Records

### **Authentication on the DMZ**

- Network Diagram
- Partial PIX Configuration

### **Information to Collect if You Open a TAC Case**

### **NetPro Discussion Forums – Featured Conversations**

### **Related Information**

---

# Introduction

RADIUS and TACACS+ authentication can be done for FTP, Telnet, and HTTP connections through the Cisco Secure PIX Firewall. Authentication for other less common protocols are usually made to work. TACACS+ authorization is supported. RADIUS authorization is not supported. Changes in PIX 5.2 authentication, authorization, and accounting (AAA) over the earlier version include AAA access list support to control who is authenticated and what resources the user accesses. In PIX 5.3 and later, the authentication, authorization, and accounting (AAA) change over earlier versions of code is that the RADIUS ports are configurable.

## Prerequisites

### Requirements

There are no specific prerequisites for this document.

### Components Used

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

- Cisco Secure PIX Firewall Software Versions 5.2.0.205 and 5.2.0.207

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.

**Note:** If you run PIX/ASA software version 7.x and later, refer to *Configuring AAA Servers and the Local Database*.

### Conventions

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

## Authentication, Authorization, and Accounting

Here is an explanation of Authentication, Authorization and Accounting:

- Authentication is who the user is.
- Authorization is what the user does.
- Authentication is valid without authorization.
- Authorization is not valid without authentication.
- Accounting is what the user did.

## What the User Sees with Authentication/Authorization On

When the user tries to go from inside to outside (or vice versa) with authentication/authorization on:

- **Telnet** The user sees a username prompt come up, then a request for password. If authentication (and authorization) is successful at the PIX/server, the user is prompted for username and password by the destination host beyond.

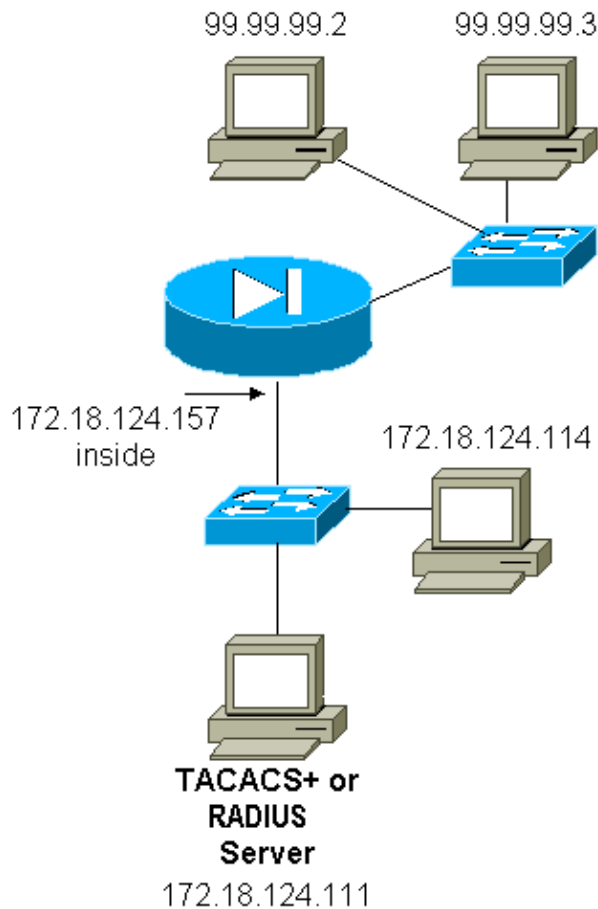
- **FTP** The user sees a username prompt come up. The user needs to enter "local\_username@remote\_username" for username and "local\_password@remote\_password" for password. The PIX sends the "local\_username" and "local\_password" to the local security server. If authentication (and authorization) is successful at the PIX/server, the "remote\_username" and "remote\_password" are passed to the destination FTP server beyond.
- **HTTP** A window is displayed in the browser requesting username and password. If authentication (and authorization) is successful, the user arrives at the destination web site beyond. Keep in mind that *browsers cache usernames and passwords*. If it appears that the PIX should time out an HTTP connection but does not do so, it is likely that re-authentication actually takes place with the browser "shooting" the cached username and password to the PIX. The PIX forwards this to the authentication server. PIX syslog and/or server debug shows this phenomenon. If Telnet and FTP seem to work "normally", but HTTP connections do not, this is the reason.

## Debugging Steps

- Make sure the PIX configuration works before you add AAA authentication and authorization. If you are unable to pass traffic before you institute authentication and authorization, you are unable to do so afterwards.
- Enable some kind of logging in the PIX.
  - ◆ Issue the **logging console debug** command to turn on logging console debugging.
    - Note:** Do not use logging console debugging on a heavily loaded system.
    - ◆ Use the **logging monitor debug** command to log a Telnet session.
    - ◆ Logging buffered debugging can be used, then execute the **show logging** command.
    - ◆ Logging can also be sent to a syslog server and examined there.
- Turn on debugging on the TACACS+ or RADIUS servers.

## Authentication Only

### Network Diagram



## Server Setup – Authentication Only

### Cisco Secure UNIX TACACS Server Configuration

```
User = cse {
password = clear "cse"
default service = permit
}
```

### Cisco Secure UNIX RADIUS Server Configuration

**Note:** Add the PIX IP address and key to the Network Access Server (NAS) list with the help of the advanced GUI.

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
}
}
}
```

### Cisco Secure Windows RADIUS

Use these steps to set up a Cisco Secure Windows RADIUS Sever.

1. Obtain a password in the **User Setup** section.
2. From the **Group Setup** section, set attribute 6 (Service–Type) to **Login** or **Administrative**.
3. Add the PIX IP address in the **NAS Configuration** section of the GUI.

## Cisco Secure Windows TACACS+

The user gets a password in the **User Setup** section.

## Livingston RADIUS Server Configuration

**Note:** Add PIX IP address and key to the *clients* file.

- bill Password="foo" User–Service–Type = Shell–User

## Merit RADIUS Server Configuration

**Note:** Add PIX IP address and key to the *clients* file.

- bill Password="foo" Service–Type = Shell–User

## TACACS+ Freeware Server Configuration

```
key = "cisco"
user = cse {
  login = cleartext "cse"
  default service = permit
}
```

## PIX Initial Configuration – Authentication Only

### PIX Initial Configuration – Authentication Only

```
PIX Version 5.2(0)205
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!

!--- These lines are necessary
!--- if the new feature in 5.2 is used to define which
!--- target/source IP addresses are to be authenticated.

access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
```

```
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask 255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114 netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
```

```
!--- For the purposes of illustration, the TACACS+ process is used
!--- to authenticate inbound users and RADIUS is used to authenticate outbound users.
```

```
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111 cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111 cisco timeout 5
!
```

```
!--- The next six statements are used to authenticate all inbound
!--- and outbound FTP, Telnet, and HTTP traffic.
```

```
aaa authentication include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    AuthInbound
aaa authentication include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    AuthOutbound
!
```

```
!--- OR the new 5.2 feature allows these two statements in
!--- conjunction with access-list 101 to replace the previous six statements.
!--- Note: Do not mix the old and new verbiage.
```

```
aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

## Configurable RADIUS Ports (5.3 and Later)

Some RADIUS servers use RADIUS ports other than 1645/1646 (usually 1812/1813). In PIX 5.3 and later, the RADIUS authentication and accounting ports can be changed to something other than the default 1645/1646 with these commands:

```
aaa-server radius-authport #
aaa-server radius-acctport #
```

## PIX Authentication Debug Examples

See Debugging Steps for information about how to turn on debugging. These are examples of a user at 99.99.99.2 that initiates traffic to inside 172.18.124.114 (99.99.99.99) and vice versa. Inbound traffic is TACACS+–authenticated and outbound is RADIUS–authenticated.

### Successful authentication – TACACS+ (inbound)

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
to 99.99.99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
gaddr 99.99.99.99/23 laddr 172.18.124.114/23 (cse)
```

### Unsuccessful authentication due to bad username/password – TACACS+ (inbound). The user sees "Error: Max number of tries exceeded."

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.124.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
to 99.99.99.2/11004 on interface outside
```

### Server not speaking to PIX – TACACS+ (inbound). User sees username once and the PIX never asks for a password (this is on Telnet). User sees "Error: Max number of tries exceeded."

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
(server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
(server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
(server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
to 99.99.99.2/11005 on interface outside
```

## Good authentication – RADIUS (outbound)

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
to 99.99.99.2/23 on interface inside
```

## Bad authentication (username or password) – RADIUS (outbound). User sees request for Username, then Password, has three opportunities to enter these, and if unsuccessful, see "Error: Max number of tries exceeded."

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
(server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
to 99.99.99.2/23 on interface inside
```

## Server pingable but daemon down, server not pingable, or key/client mismatch – will not communicate with PIX – RADIUS (outbound). User sees Username, then password, then "RADIUS server failed," and then finally "Error: Max number of tries exceeded."

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
(server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
(server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
(server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
to 99.99.99.2/23 on interface inside
```

## Authentication Plus Authorization

If you want to allow all authenticated users to perform all operations (HTTP, FTP, and Telnet) through the PIX, then authentication is sufficient and authorization is not needed. However, if you want to allow some subset of services to certain users or to limit users from going to certain sites, authorization is needed. RADIUS authorization is not valid for traffic through the PIX. TACACS+ authorization is valid in this case.

If authentication passes and authorization is on, the PIX sends the command the user is doing to the server. For example, "http 1.2.3.4." In version 5.2 of PIX, TACACS+ authorization is used in conjunction with access lists to control where users go.

If you want to implement authorization for HTTP (web sites visited), use software such as Websense since a single web site can have a large number of IP addresses associated with it.

## Server Setup – Authentication plus Authorization

### Cisco Secure UNIX TACACS Server Configuration

```
user = can_only_do_telnet {
password = clear "*****"
service = shell {
cmd = telnet {
permit .*
}
}
}
```

```

user = can_only_do_ftp {
password = clear "*****"
service = shell {
cmd = ftp {
permit .*
}
}
}

user = httponly {
password = clear "*****"
service = shell {
cmd = http {
permit .*
}
}
}

```

## Cisco Secure Windows TACACS+

Complete these steps to set up a Cisco Secure Windows TACACS+ server.

1. Click **Deny unmatched IOS commands** at the bottom of the Group Setup.
2. Click **Add/Edit New Command (FTP, HTTP, Telnet)**.

For example, if you want to allow Telnet to a specific site ("telnet 1.2.3.4"), the command is **telnet**. The argument is *1.2.3.4*. After filling in "command=**telnet**," fill in the "permit" IP address(es) in the Argument rectangle (for example, "permit 1.2.3.4"). If all Telnets are to be allowed, the command is still **telnet**, but click **Allow all unlisted arguments**. Then click **Finish editing command**.

3. Perform step 2 for each of the allowed commands (for example, Telnet, HTTP, and FTP).
4. Add the PIX IP address in the NAS Configuration section with the help of the GUI.

## TACACS+ Freeware Server Configuration

```

user = can_only_do_telnet {
login = cleartext "telnetonly"
cmd = telnet {
permit .*
}
}

user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

user = can_only_do_ftp {
login = cleartext "ftponly"
cmd = ftp {
permit .*
}
}

```

## PIX Configuration – Adding Authorization

Add commands to require authorization:

```

aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound

```

```
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

The new 5.2 feature allows this statement in conjunction with previously defined access list 101 to replace the previous three statements. The old and new verbiage should not be mixed.

```
aaa authorization match 101 outside AuthInbound
```

## PIX Authentication and Authorization Debug Examples

### Good authentication and authorization succeeds – TACACS+

```
109001: Auth start for user '???' from
99.99.99.2/11010 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 3
109005: Authentication succeeded for user
'cse' from 172.18.124.114/23 to 99.99.99.2/11010
on interface outside
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
from 99.99.99.2/11010 to 172.18.1 24.114/23
on interface outside
302001: Built inbound TCP connection 2 for faddr
99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
172.18.124.114/23 (cse)
```

### Good authentication but authorization fails – TACACS+. User also sees the message "Error: Authorization Denied."

```
109001: Auth start for user '???' from
99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
from 172.18.124.114/23 to 9 9.99.99.2/11011
on interface outside
109008: Authorization denied for user 'httponly'
from 172.18.124.114/23 to 99.99.99.2/11011
on interface outside
```

## New Access List Feature

In PIX software release 5.2 and later, define access lists on the PIX. Apply them on a per-user basis based on the user profile on the server. TACACS+ requires authentication and authorization. RADIUS requires authentication only. In this example, the outbound authentication and authorization to TACACS+ are changed. An access list on the PIX is set up.

**Note:** In PIX Version 6.0.1 and later, if you use RADIUS, the access lists are implemented by entering the list in standard IETF RADIUS attribute 11 (Filter-Id) [CSCdt50422]. In this example, attribute 11 is set to 115 in lieu of doing the vendor-specific "acl=115" verbiage.

## PIX Configuration

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
```

```
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

## Server Profiles

**Note:** The 2.1 version of the TACACS+ freeware does not recognize the "acl" verbiage.

### Cisco Secure UNIX TACACS+ Server Configuration

```
user = pixa{
  password = clear "*****"
  service=shell {
    set acl=115
  }
}
```

### Cisco Secure Windows TACACS+

In order to add authorization to the PIX to control where the user goes with access lists, check **shell/exec**, check the **Access control list** box, and fill in the number (matches the access list number on the PIX).

### Cisco Secure UNIX RADIUS

```
user = pixa{
  password = clear "*****"
  radius=Cisco {
    reply_attributes= {
      9,1="acl=115"
    }
  }
}
```

### Cisco Secure Windows RADIUS

RADIUS/Cisco is the device-type. The "pixa" user needs a username, a password, and a check and "acl=115" in the Cisco/RADIUS rectangular box where it says 009\001 AV-Pair (vendor-specific).

## Output

The outbound user "pixa" with "acl=115" in the profile authenticates and authorizes. The server passes down the acl=115 to the PIX, and the PIX shows this:

```
pixfirewall#show uauth
Current      Most Seen
Authenticated Users      1          2
Authen In Progress      0          2
user 'pixa' at 172.18.124.114, authenticated
  access-list 115
  absolute timeout: 0:05:00
  inactivity timeout: 0:00:00
```

When the user "pixa" tries to go to 99.99.99.3 (or any IP address except 99.99.99.2, because there is an implicit deny), the user sees this:

```
Error: acl authorization denied
```

## New Per-User Downloadable Access List With Version 6.2

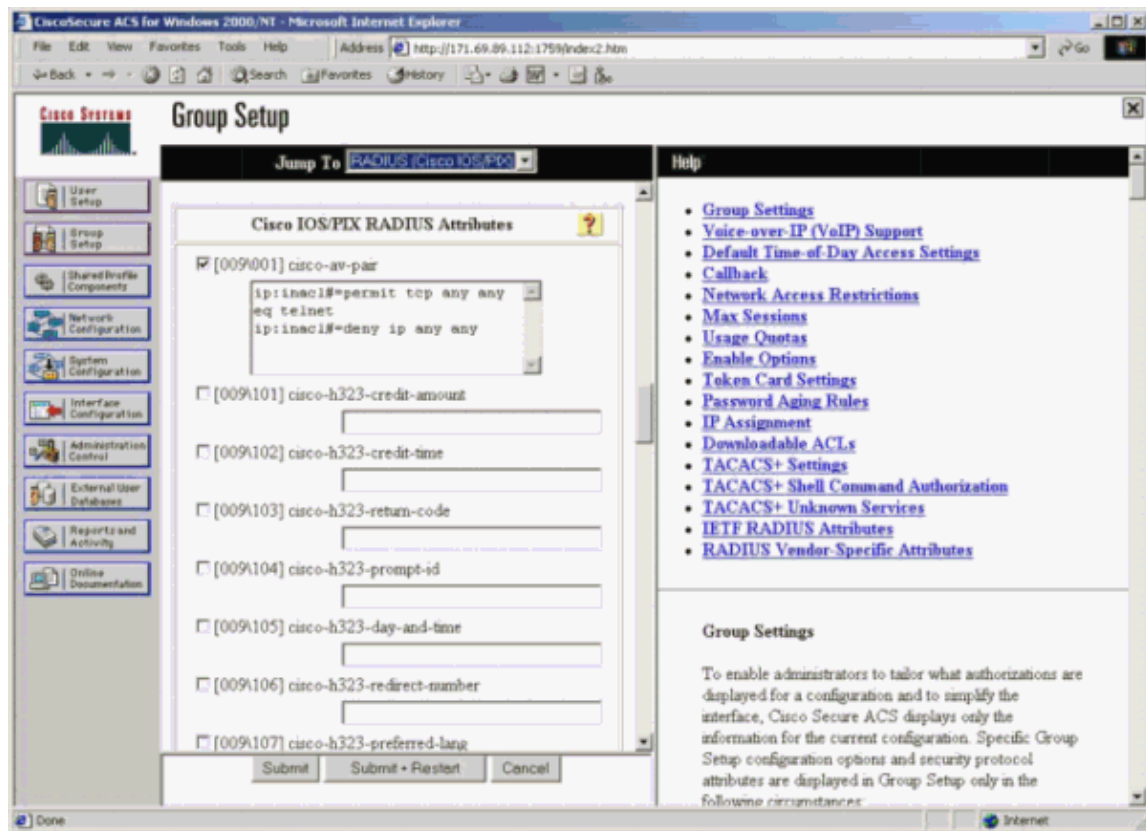
In software release 6.2 and later of the PIX Firewall, access lists are defined on an access control server (ACS) to download to the PIX after authentication. This works only with the RADIUS protocol. There is no need to configure the access list on the PIX itself. A group template is applied to multiple users.

In earlier versions, the access list is defined on the PIX. Upon authentication, the ACS pushed the access list name to the PIX. The new version allows the ACS to push the access list directly to the PIX.

**Note:** If failover occurs, the uauth table is not copied. Users are reauthenticated. The access list is downloaded again.

### ACS Setup

Click **Group Setup** and select the **RADIUS (Cisco IOS/PIX)** device type to set up a user account. Assign a username ("cse", in this example) and password for the user. From the Attributes list, select the option to configure **[009\001] vendor-av-pair**. Define the access list as illustrated in this example:



### PIX Debugs: Valid Authentication and Downloaded Access List

- Allows only Telnet and denies other traffic.

```
pix# 305011: Built dynamic TCP translation from inside:
      172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
      to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
      from 172.16.171.33/11063
      to 172.16.171.202/23 on interface inside
```

```
302013: Built outbound TCP connection 123 for outside:
172.16.171.202/23 (172.16.171.202/23) to inside:
172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

◆ Output from the **show uauth** command.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

◆ Output from the **show access-list** command.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- Denies only Telnet and allows other traffic.

```
pix# 305011: Built dynamic TCP translation from inside:
172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
from 172.16.171.33/11064
to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

◆ Output from the **show uauth** command.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

◆ Output from the **show access-list** command.

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

## New Per-User Downloadable Access List Using ACS 3.0

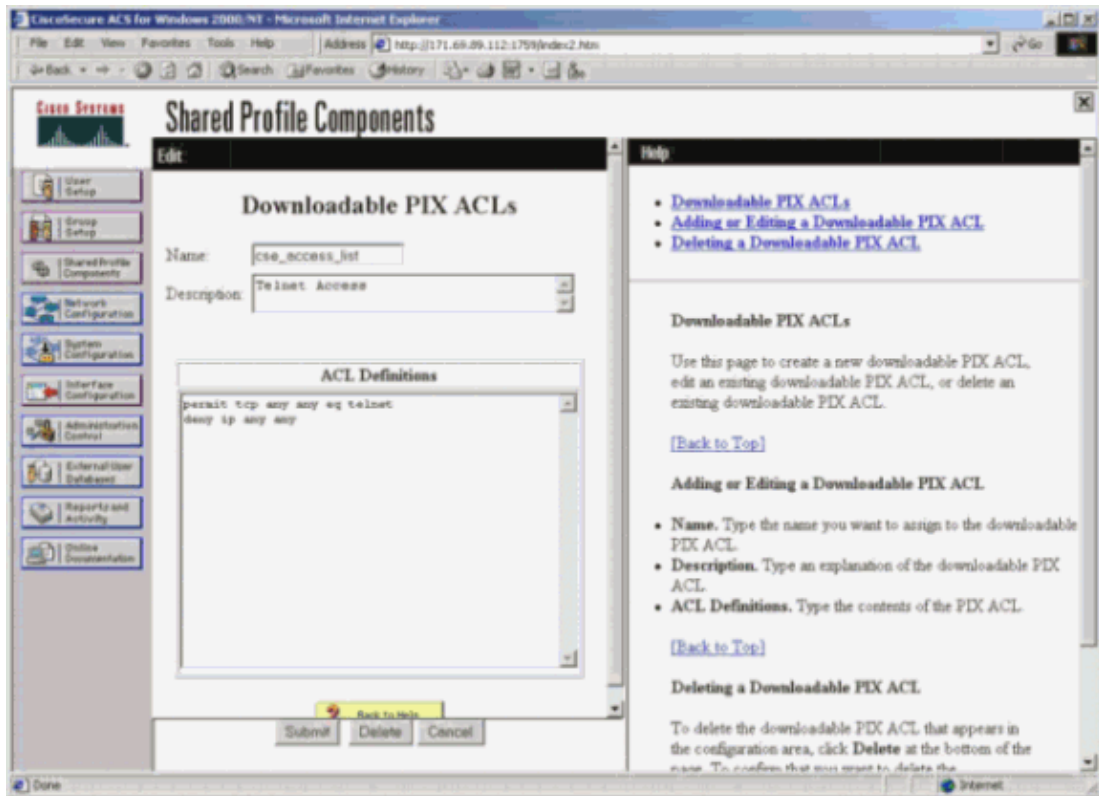
In ACS version 3.0, the shared profile component allows the user to create an access list template and define the template name to specific users or groups. The template name can be used with as many users or groups as needed. This eliminates the need to configure identical access lists for each user.

**Note:** If failover occurs, uauth is not copied to the secondary PIX. In the stateful failover, the session is sustained. However, the new connection must be reauthenticated and the access list must be downloaded again.

## Using Shared Profiles

Complete these steps when you use shared profiles.

1. Click **Interface Configuration**.
2. Check **User–Level Downloadable ACLs** and/or **Group–Level Downloadable ACLs**.
3. Click **Shared Profile Components**. Click **User–Level Downloadable ACLs**.
4. Define the Downloadable ACLs.
5. Click **Group Setup**. Under Downloadable ACLs, assign the PIX access list to the access list created earlier.



## PIX Debugs: Valid Authentication and Downloaded Access List Using Shared Profiles

- Allows only Telnet and denies other traffic.

```
pix# 305011: Built dynamic TCP translation from inside:
      172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
      172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
      172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
      172.16.171.202/23 (172.16.171.202/23) to inside:
      172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

- ◆ Output from the **show uauth** command.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
```

```
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

- ◆ Output from the **show access-list** command.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
    permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
    deny ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- Denies only Telnet and allows other traffic.

```
pix# 305011: Built dynamic TCP translation from inside:
    172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
    172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
    from 172.16.171.33/11066
    to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
    for user 'cse' from 172.16.171.33/11066
    to 172.16.171.202/23 on interface inside
```

- ◆ Output from the **show uauth** command.

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

- ◆ Output from the **show access-list** command.

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
    deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
    permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

## Add Accounting

### PIX Configuration – Add Accounting

#### TACACS (AuthInbound=tacacs)

Add this command.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

Or use the new feature in 5.2 to define what is to be accounted by access lists.

```
aaa accounting match 101 outside AuthInbound
```

**Note:** Access list 101 is defined separately.

## RADIUS (AuthOutbound=radius)

Add this command.

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

Or use the new feature in 5.2 to define what is to be accounted by access lists.

```
aaa accounting match 101 outside AuthOutbound
```

**Note:** Access list 101 is defined separately.

**Note:** Accounting records can be generated for administrative sessions on the PIX starting from PIX 7.0 code.

## Accounting Examples

- TACACS accounting example for Telnet from 99.99.99.2 outside to 172.18.124.114 inside (99.99.99.99).

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
local_ip=172.18.124.114
cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- RADIUS accounting example for connection from 172.18.124.114 inside to 99.99.99.2 outside (Telnet) and 99.99.99.3 outside (HTTP).

```
Sun Aug 6 03:59:28 2000
Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 172.18.124.114
Login-TCP-Port = 23
Acct-Session-Id = 0x00000004
User-Name = cse
Vendor-Specific = Source-IP=172.18.124.114
Vendor-Specific = Source-Port=35937
Vendor-Specific = Destination-IP=99.99.99.2
Vendor-Specific = Destination-Port=23
```

```
Sun Aug 6 03:59:32 2000
Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 172.18.124.114
Login-TCP-Port = 23
Acct-Session-Id = 0x00000004
Username = cse
Acct-Session-Time = 4
Acct-Input-Octets = 101
Acct-Output-Octets = 143
Vendor-Specific = Source-IP=172.18.124.114
Vendor-Specific = Source-Port=35937
Vendor-Specific = Destination-IP=99.99.99.2
Vendor-Specific = Destination-Port=23
```

```
Sun Aug 6 04:05:02 2000
Acct-Status-Type = Start
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 172.18.124.114
Login-TCP-Port = 80
Username = cse
Vendor-Specific = Source-IP=172.18.124.114
Vendor-Specific = Source-Port=35949
Vendor-Specific = Destination-IP=99.99.99.3
Vendor-Specific = Destination-Port=80
```

```
Sun Aug 6 04:05:02 2000
Acct-Status-Type = Stop
NAS-IP-Address = 172.18.124.157
Login-IP-Host = 172.18.124.114
Login-TCP-Port = 80
Acct-Session-Id = 0x0000000a
Username = cse
Acct-Session-Time = 0
Acct-Input-Octets = 1277
Acct-Output-Octets = 310
Vendor-Specific = Source-IP=172.18.124.114
Vendor-Specific = Source-Port=35949
Vendor-Specific = Destination-IP=99.99.99.3
Vendor-Specific = Destination-Port=80
```

## Use of the exclude Command

In this network, if you decide that a particular source or destination does not need authentication, authorization, or accounting, issue these commands.

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
99.99.99.3 255.255.255.255 AuthInbound
```

**Note:** You already have the **include** commands.

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

Or, with the new feature in 5.2, define what you want to exclude.

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
aaa accounting match 101 outside AuthInbound
```

**Note:** If you exclude a box from authentication and you have authorization on, you must also exclude the box from authorization.

## Max-sessions and View Logged-in Users

Some TACACS+ and RADIUS servers have "max-session" or "view logged-in users" features. The ability to

do max-sessions or check logged-in users is dependent on accounting records. When there is an accounting "start" record generated but no "stop" record, the TACACS+ or RADIUS server assumes the person is still logged in (that is, the user has a session through the PIX). This works well for Telnet and FTP connections because of the nature of the connections. However, this does not work well for HTTP. In this example, a different network configuration is used, but the concepts are the same.

User Telnets through the PIX, authenticating on the way.

```
(pix) 109001: Auth start for user '???' from
171.68.118.100/1200 to 9.9.9.25 /23
(pix) 109011: Authen Session Start: user 'cse', Sid 3
(pix) 109005: Authentication succeeded for user
'cse' from 171.68.118.100/1200 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for
faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 laddr
171.68.118.100/1200 (cse)
(server start account) Sun Nov 8 16:31:10 1998
rtp-pinecone.rtp.cisco.com cse
PIX 171.68.118.100 start task_id=0x3
foreign_ip=9.9.9.25
local_ip=171.68.118.100 cmd=telnet
```

Because the server has seen a "start" record but no "stop" record, at this point in time, the server shows that the "Telnet" user is logged in. If the user attempts another connection that requires authentication (perhaps from another PC), and if max-sessions is set to "1" on the server for this user (assuming the server supports max-sessions), the connection is refused by the server. The user goes about their Telnet or FTP business on the target host, then exits (spends ten minutes there).

```
(pix) 302002: Teardown TCP connection 5 faddr
9.9.9.25/80 gaddr 9.9.9.10/128 1 laddr
171.68.118.100/1281 duration 0:00:00 bytes
1907 (cse)
(server stop account) Sun Nov 8 16:41:17 1998
rtp-pinecone.rtp.cisco.com
cse PIX 171.68.118.100 stop task_id=0x3
foreign_ip=9.9.9.25 local_ip=171.68.118.100
cmd=telnet elapsed_time=5 bytes_in=98
bytes_out=36
```

Whether uauth is 0 (that is, authenticate every time) or more (authenticate once and not again during uauth period), an accounting record is cut for every site accessed.

HTTP works differently due to the nature of the protocol. Here is an example of HTTP where the user browses from 171.68.118.100 to 9.9.9.25 through the PIX.

```
(pix) 109001: Auth start for user '???' from
171.68.118.100/1281 to 9.9.9.25 /80
(pix) 109011: Authen Session Start: user 'cse', Sid 5
(pix) 109005: Authentication succeeded for user
'cse' from 171.68.118.100/12 81 to 9.9.9.25/80
(pix) 302001: Built TCP connection 5 for faddr
9.9.9.25/80 gaddr 9.9.9.10/12 81 laddr
171.68.118.100/1281 (cse)
(server start account) Sun Nov 8 16:35:34 1998
rtp-pinecone.rtp.cisco.com
cse PIX 171.68.118.100 start task_id=0x9
foreign_ip=9.9.9.25 local_ip=171.68.118.100 cmd=http
(pix) 302002: Teardown TCP connection 5 faddr
9.9.9.25/80 gaddr 9.9.9.10/128 1
laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)
(server stop account) Sun Nov 8 16:35.35 1998
```

```
rtp-pinecone.rtp.cisco .com
cse PIX 171.68.118.100 stop task_id=0x9
foreign_ip =9.9.9.25 local_ip=171.68.118.100
cmd=http elapsed_time=0 bytes_in=1907 bytes_out=223
```

The user reads the downloaded web page. The start record is posted at 16:35:34 and the stop record at 16:35:35. This download took one second (that is, there was less than one second between the start and the stop record). The user is not logged in to the web site. The connection is not open when the user is reading the web page. Max-sessions or view logged-in users do not work here. This is because the connection time (the time between the "Built" and "Teardown") in HTTP is too short. The "start" and "stop" record is sub-second. There is no "start" record without a "stop" record since the records occur at virtually the same instant. There is still a "start" and "stop" record sent to the server for every transaction whether uauth is set for 0 or something larger. However, max-sessions and view logged-in users do not work due to the nature of HTTP connections.

## User Interface

### Change the Prompt Users See

If you have the command:

```
auth-prompt prompt PIX515B
```

then users going through the PIX see this prompt.

```
PIX515B
```

### Customize the Message Users See

If you have the commands:

```
auth-prompt accept "GOOD_AUTHENTICATION"
auth-prompt reject "BAD_AUTHENTICATION"
```

then users see a message about authentication status on a failed/successful login.

```
PIX515B
Username: junk
Password:
"BAD_AUTHENTICATION"

PIX515B
Username: cse
Password:
"GOOD_AUTHENTICATION"
```

## Per-User Idle and Absolute Timeouts

The PIX **timeout uauth** command controls how often reauthentication is required. If TACACS+ authentication/authorization is on, this is controlled on a per-user basis. This user profile is set up to control the timeout (this is on the TACACS+ freeware server and the timeouts are in minutes).

```
user = cse {
default service = permit
login = cleartext "csecse"
service = exec {
timeout = 2
idletime = 1
```

```
}  
}
```

After authentication/authorization:

```
show uauth  
  
                Current      Most Seen  
Authenticated Users      1          2  
Authen In Progress       0          1  
user 'cse' at 99.99.99.3, authorized to:  
  port 172.18.124.114/telnet  
  absolute  timeout: 0:02:00  
  inactivity timeout: 0:01:00
```

At the end of two minutes:

Absolute timeout – session gets torn down:

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds  
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025  
      gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26  
      bytes 7547 (TCP FINs)
```

## Virtual HTTP Outbound

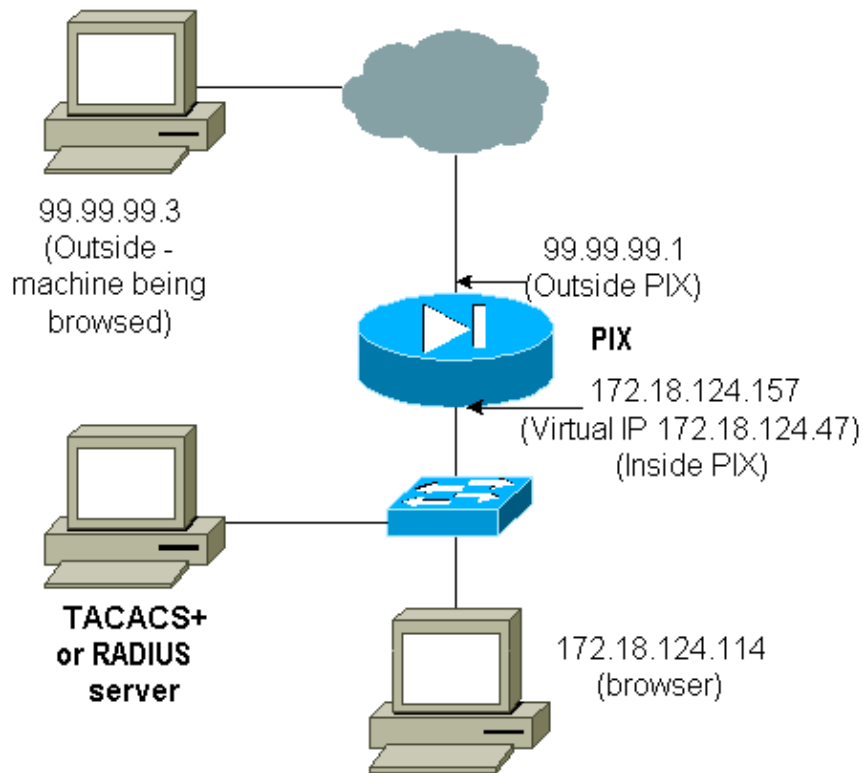
If authentication is required on sites outside the PIX as well as on the PIX itself, unusual browser behavior is sometimes observed, since browsers cache the username and password.

In order to avoid this, implement virtual HTTP by adding an RFC 1918 address (an address unroutable on the Internet, but valid and unique for the PIX inside network) to the PIX configuration in the format.

```
virtual http #.#.#.# <warn>
```

When the user tries to go outside the PIX, authentication is required. If the warn parameter is present, the user receives a redirect message. The authentication is good for the length of time in the uauth. As indicated in the documentation, do not set the **timeout uauth** command duration to 0 seconds with virtual HTTP. This prevents HTTP connections to the real web server.

**Note:** The virtual HTTP and virtual Telnet IP addresses must be included in the **aaa authentication** statements. In this example, specifying 0.0.0.0 does include these addresses.



In the PIX configuration add this command.

```
virtual http 172.18.124.47
```

The user points the browser at 99.99.99.3. This message is displayed.

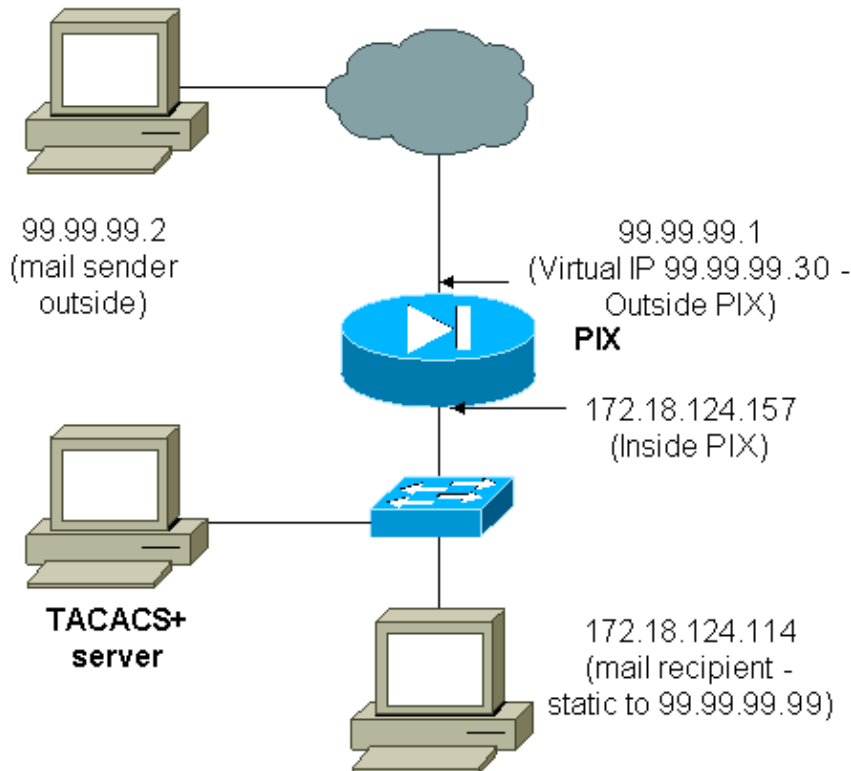
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

After authentication, the traffic is redirected to 99.99.99.3.

## Virtual Telnet

**Note:** The virtual HTTP and virtual Telnet IP addresses must be included in the **aaa authentication** statements. In this example, specifying 0.0.0.0 does include these addresses.

## Virtual Telnet Inbound



It is not a great idea to authenticate mail inbound since a window is not displayed for mail to be sent inbound. Use the **exclude** command instead. But for purpose of illustration, these commands are added.

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

```
!--- OR the new 5.2 feature allows these
!--- four statements to perform the same function.
!--- Note: The old and new verbiage should not be mixed.
```

```
access-list 101 permit tcp any any eq smtp
```

```
!--- The "mail" was a Telnet to port 25.
```

```
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
```

```
!--- plus
```

```
!
virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

The users (this is TACACS+ freeware):

```
user = cse {
```

```

default service = permit
login = cleartext "csecse"
}

user = pixuser {
login = cleartext "pixuser"
service = exec {
}
cmd = telnet {
permit .*
}
}
}

```

If only authentication is on, both users send mail inbound after authenticating on a Telnet to IP address 99.99.99.30. If authorization is enabled, user "cse" Telnets to 99.99.99.30, and enters the TACACS+ username/password. The Telnet connection drops. User "cse" then sends mail to 99.99.99.99 (172.18.124.114). Authentication succeeds for user "pixuser". However, when the PIX sends the authorization request for cmd=tcp/25 and cmd-arg=172.18.124.114, the request fails, as shown in this output.

```

109001: Auth start for user '???' from
99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
'cse' from 172.18.124.114/23 to
99.99.99.2/11036 on interface outside

```

```

pixfirewall#show uauth

```

	Current	Most Seen
Authenticated Users	1	1
Authen In Progress	0	1

```

user 'cse' at 99.99.99.2, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00

```

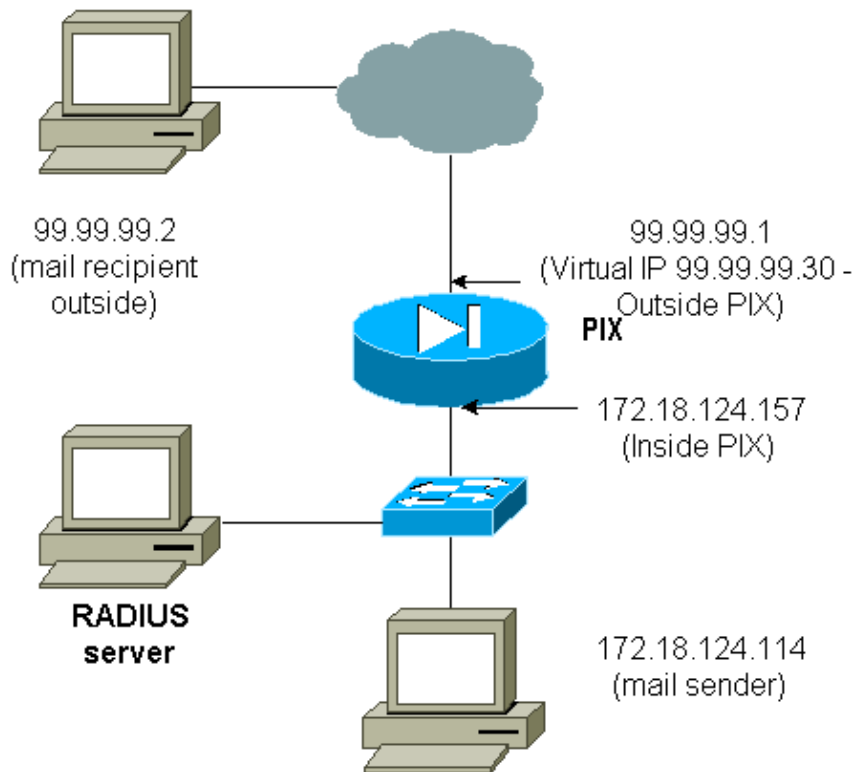
```

pixfirewall# 109001: Auth start for user '???' from
99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
to 172.18.124.30/23 on interface outside
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
to 172.18.124.114/11176 on interface outside

```

## Virtual Telnet Outbound



It is not a great idea to authenticate mail inbound since a window is not displayed for mail to be sent inbound. Use the **exclude** command instead. But for purpose of illustration, these commands are added.

It is not a great idea to authenticate mail outbound since a window is not displayed for mail to be sent outbound. Use the **exclude** command instead. But for purposes of illustration, these commands are added.

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

```
!--- OR the new 5.2 feature allows these three statements
!--- to replace the previous statements.
!--- Note: Do not mix the old and new verbiage.
```

```
access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
```

```
!--- plus
```

```
!
virtual telnet 99.99.99.30
```

```
!--- The IP address on the outside of PIX is not used for anything else.
```

In order to send mail from inside to outside, bring up a command prompt on the mail host and Telnet to 99.99.99.30. This opens the hole for mail to go through. Mail is sent from 172.18.124.114 to 99.99.99.2:

```
305002: Translation built for gaddr 99.99.99.99
to laddr 172.18.124.114
109001: Auth start for user '???' from
172.18.124.114/32860 to 99.99.99.30/23
109011: Authen Session Start: user 'cse', Sid 14
```

```
109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to 99.99.99.30/23
      on interface inside
302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)
```

```
pixfirewall#show uauth
Current      Most Seen
Authenticated Users      1          2
Authen In Progress      0          1
user 'cse' at 172.18.124.114, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

## Virtual Telnet Logout

When users Telnet to the virtual Telnet IP address, the **show uauth** command shows the time the hole is open. If the users want to prevent traffic from going through after their sessions are finished (when time remains in the uauth), they need to Telnet to the virtual Telnet IP address again. This toggles the session off. This is illustrated by this example.

### The first authentication

```
109001: Auth start for user '???'
      from 172.18.124.114/32862 to 99.99.99.30/23
109011: Authen Session Start: user 'cse', Sid 15
109005: Authentication succeeded for user
      'cse' from 172.18.124.114/32862 to
      99.99.99.30/23 on interface inside
```

### After the first authentication

```
pixfirewall#show uauth
Current      Most Seen
Authenticated Users      1          2
Authen In Progress      0          1
user 'cse' at 172.18.124.114, authenticated
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

### The second authentication

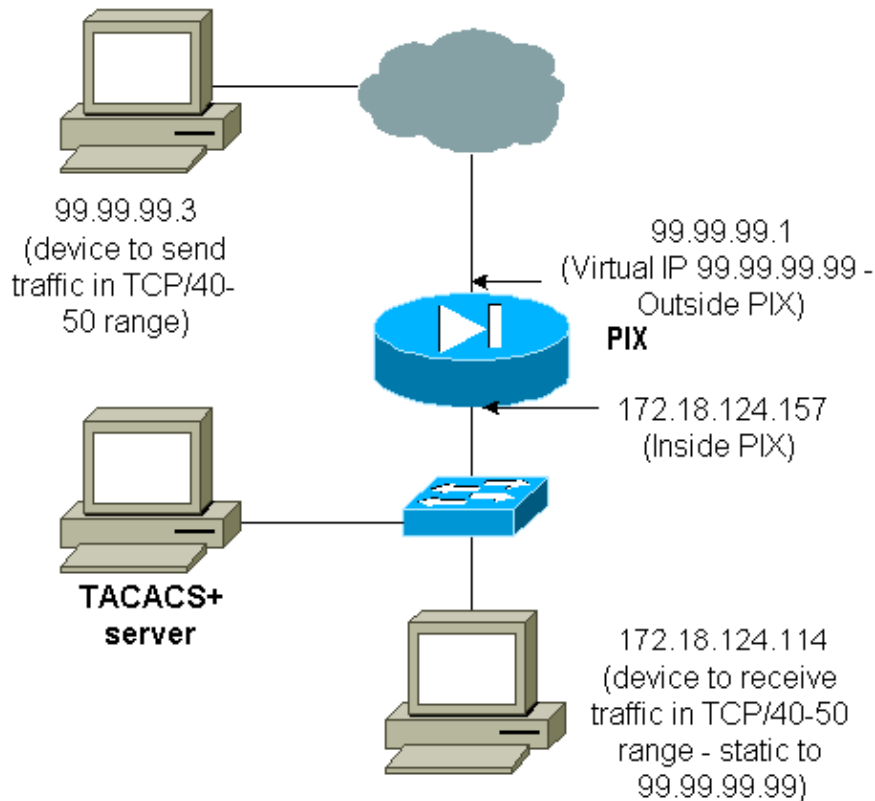
```
pixfirewall# 109001: Auth start for user 'cse'
      from 172.18.124.114/32863 to 99.99.99.30/23
109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to 99.99.99.30/23
      on interface inside
```

### After the second authentication

```
pixfirewall#show uauth
Current      Most Seen
Authenticated Users      0          2
Authen In Progress      0          1
```

## Port Authorization

## Network Diagram



Authorization is allowed for port ranges. If virtual Telnet is configured on the PIX, and authorization is configured for a range of ports, the user opens the hole with virtual Telnet. Then, if authorization for a port range is on and traffic in that range hits the PIX, the PIX sends the command to the TACACS+ server for authorization. This example shows inbound authorization on a port range.

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

```
!--- OR the new 5.2 feature allows these three statements
!--- to perform the same function as the previous two statements.
!--- Note: The old and new verbiage should not be mixed.
```

```
access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
aaa authorization match 116 outside AuthInbound
!

!--- plus

!
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

TACACS+ server configuration example (freeware):

```
user = cse {
login = cleartext "numeric"
cmd = tcp/40-50 {
permit 172.18.124.114
```

```
}  
}
```

The user must first Telnet to the virtual IP address 99.99.99.99. After authentication, when a user tries to push TCP traffic in the port 40–50 range through the PIX to 99.99.99.99 (172.18.124.114), cmd=tcp/40–50 is sent to the TACACS+ server with cmd-arg=172.18.124.114 as illustrated here:

```
109001: Auth start for user '???' from 99.99.99.3/11075  
      to 172.18.124.114/23  
109011: Authen Session Start: user 'cse', Sid 13  
109005: Authentication succeeded for user 'cse'  
      from 172.18.124.114/23 to 99.99.99.3/11075  
      on interface outside  
109001: Auth start for user 'cse' from 99.99.99.3/11077  
      to 172.18.124.114/49  
109011: Authen Session Start: user 'cse', Sid 13  
109007: Authorization permitted for user 'cse'  
      from 99.99.99.3/11077 to 172.18.124.114/49  
      on interface outside
```

## AAA Accounting for Traffic Other Than HTTP, FTP, and Telnet

After you make sure virtual Telnet works to allow TCP/40–50 traffic to the host inside the network, add accounting for this traffic with these commands.

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound  
  
!--- OR the new 5.2 feature allows these  
!--- two statements to replace the previous statement.  
!--- Note: Do not mix the old and new verbiage.  
  
aaa accounting match 116 outside AuthInbound  
access-list 116 permit ip any any
```

## Example of TACACS+ Accounting Records

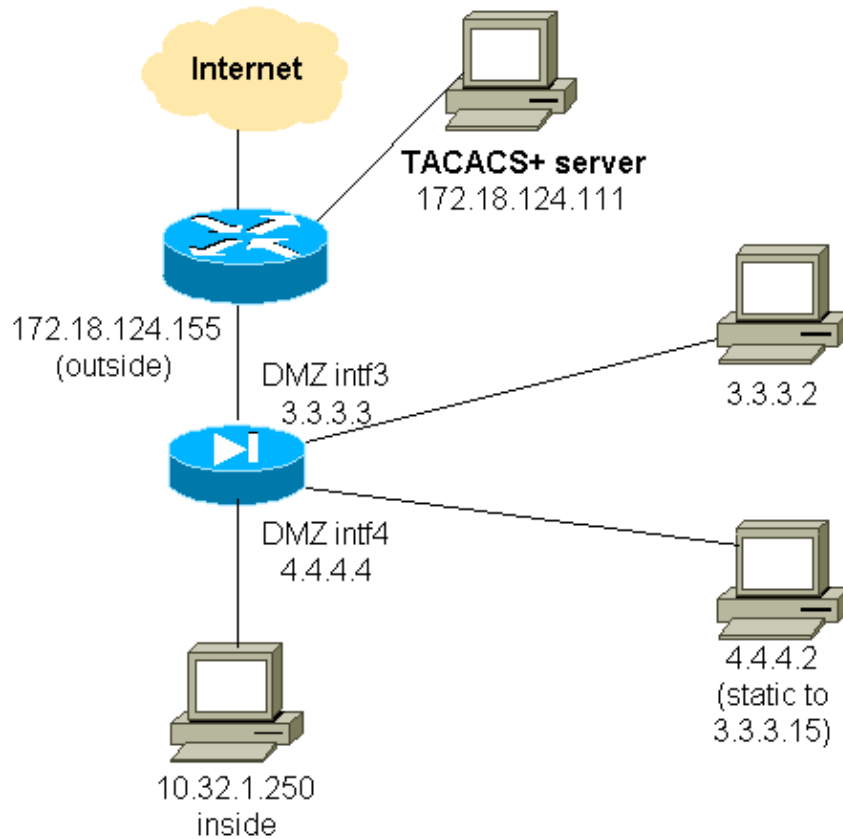
```
Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3  
start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114  
cmd=tcp/40-50  
Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3  
stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114  
cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

## Authentication on the DMZ

In order to authenticate users that go from one DMZ interface to another, tell the PIX to authenticate traffic for the named interfaces. On the PIX, the arrangement is like this:

```
least secure  
PIX outside (security0) = 172.18.124.155  
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2  
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)  
PIX inside (security100) = 10.32.1.250  
most secure
```

## Network Diagram



## Partial PIX Configuration

Authenticate Telnet traffic between pix/intf3 and pix/intf4, as demonstrated here.

### Partial PIX Configuration

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
(nameif ethernet2 pix/intf2 security10)
nameif ethernet3 pix/intf3 security15
nameif ethernet4 pix/intf4 security20
(nameif ethernet5 pix/intf5 security25)
interface ethernet0 auto
interface ethernet1 auto
(interface ethernet2 auto shutdown)
interface ethernet3 auto
interface ethernet4 auto
(interface ethernet5 auto shutdown)
ip address outside 172.18.124.155 255.255.255.0
ip address inside 10.32.1.250 255.255.255.0
ip address pix/intf3 3.3.3.3 255.255.255.0
ip address pix/intf4 4.4.4.4 255.255.255.0
static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask 255.255.255.255 0 0
conduit permit tcp host 3.3.3.15 host 3.3.3.2
aaa-server xway protocol tacacs+
aaa-server xway (outside) host 172.18.124.111 timeout 5
aaa authentication include telnet pix/intf4 4.4.4.0 255.255.255.0 3.3.3.0
255.255.255.0 3.3.3.0 255.255.255.0 xway
aaa authentication include telnet pix/intf3 4.4.4.0 255.255.255.0 3.3.3.0
255.255.255.0 3.3.3.0 255.255.255.0 xway
```

*!--- OR the new 5.2 feature allows these four statements*

```
!--- to replace the previous two statements.  
!--- Note: Do not mix the old and new verbiage.
```

```
access-list 103 permit tcp 3.3.3.0 255.255.255.0 4.4.4.0 255.255.255.0 eq telnet  
access-list 104 permit tcp 4.4.4.0 255.255.255.0 3.3.3.0 255.255.255.0 eq telnet  
aaa authentication match 103 pix/intf3 xway  
aaa authentication match 104 pix/intf4 xway
```

## Information to Collect if You Open a TAC Case

If you still need assistance after following the troubleshooting steps above and want to open a case with the Cisco TAC, be sure to include this information for troubleshooting your PIX Firewall.

- Problem description and relevant topology details
- Troubleshoot before you open the case
- Output from the **show tech-support** command
- Output from the **show log** command after you run with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available)

Attach the collected data to your case in non-zipped, plain text format (.txt). Attach information to your case by uploading it with the help of the Case Query Tool (registered customers only). If you are unable to access the Case Query Tool, send the information in an email attachment to [attach@cisco.com](mailto:attach@cisco.com) with your case number in the subject line of your message.

## 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

- [Cisco PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [Security Product Field Notices \(including PIX\)](#)
- [Requests for Comments \(RFCs\)](#)
- [Documentation for PIX Firewall](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Cisco Secure Access Control Server for UNIX](#)

- **Terminal Access Controller Access Control System (TACACS+)**
  - **Remote Authentication Dial-In User Service (RADIUS)**
  - **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: Oct 14, 2009

Document ID: 8527

---