

How To Perform Authentication and Enabling on the Cisco Secure PIX Firewall (5.2 Through 6.2)

Document ID: 8505

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Configurable RADIUS Ports (5.3 and later)
- Conventions

Telnet Authentication – Inside

- Network Diagram
- Commands Added to PIX Configuration

Console Port Authentication

Authenticated Cisco Secure VPN Client 1.1 – Outside

Authenticated VPN 3000 2.5 or VPN Client 3.0 – Outside

- Authenticated VPN 3000 2.5 or VPN Client 3.0 – Outside – Client Configuration

SSH – Inside or Outside

- Network Diagram
- Configure AAA Authenticated SSH
- Configure Local SSH (No AAA Authentication)
- SSH Debug
- What Can Go Wrong
- How to Remove RSA Key from PIX
- How to Save RSA Key to PIX
- How to Allow SSH from Outside SSH Client

Enable Authentication

Syslogg Information

Gain Access When the AAA Server is Down

Information to Collect if You Open a TAC Case

Related Information

Introduction

This document describes how to create AAA–authenticated access to a PIX Firewall that runs PIX Software version 5.2 through 6.2, and also provides information about enable authentication, syslogging, and gaining access when the AAA server is down. In PIX 5.3 and later, the authentication, authorization, and accounting (AAA) change over previous versions of code is that the RADIUS ports are configurable.

In PIX Software versions 5.2 and later, you can create AAA–authenticated access to the PIX in five different ways:

- Telnet Authentication – Inside
- Console Port Authentication
- Authenticated Cisco Secure VPN Client 1.1 – Outside
- Authenticated VPN 3000 2.5 – Outside
- Authenticated Secure Shell (SSH) – Inside or Outside

Note: DES or 3DES must be enabled on the PIX (issue a **show version** command to verify) for the last three methods. In PIX Software version 6.0 and later, PIX Device Manager (PDM) can also be loaded to enable GUI management. PDM is outside the scope of this document.

For more information about the authentication and authorization command for PIX 6.2, refer to PIX 6.2 : Authentication and Authorization Command Configuration Example.

In order to create AAA–authenticated (Cut–through Proxy) access to a PIX Firewall that runs PIX Software versions 6.3 and later, refer to PIX/ASA : Cut–through Proxy for Network Access using TACACS+ and RADIUS Server Configuration Example.

Prerequisites

Requirements

Perform these tasks before you add AAA authentication:

- Issue these commands to add a password for the PIX:

```
passwd ww
```

```
telnet <local_ip> [<mask>] [<if_name>]
```

The PIX automatically encrypts this password to form an encrypted string with the keyword **encrypted**, as in this example:

```
passwd OnTrBUG1Tp0edmkr encrypted
```

You do not need to add the **encrypted** keyword.

- Make sure you can Telnet from the inside network to the inside interface of the PIX *without* AAA authentication after you add these statements.
- Always have a connection open to the PIX while you add authentication statements in the event that backing out the commands is necessary.

On AAA authentication (other than SSH where the sequence depends on the client), the user sees a request for the PIX password (as in *passwd <whatever>*), then a request for the RADIUS or TACACS username and password.

Note: You cannot Telnet to the outside interface of PIX. SSH can be used on the outside interface if connected from an outside SSH client.

Components Used

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

- PIX Software version 5.2, 5.3, 6.0, 6.1, or 6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5
- Cisco VPN Client 3.0.x (PIX 6.0 code required)

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.

Configurable RADIUS Ports (5.3 and later)

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

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

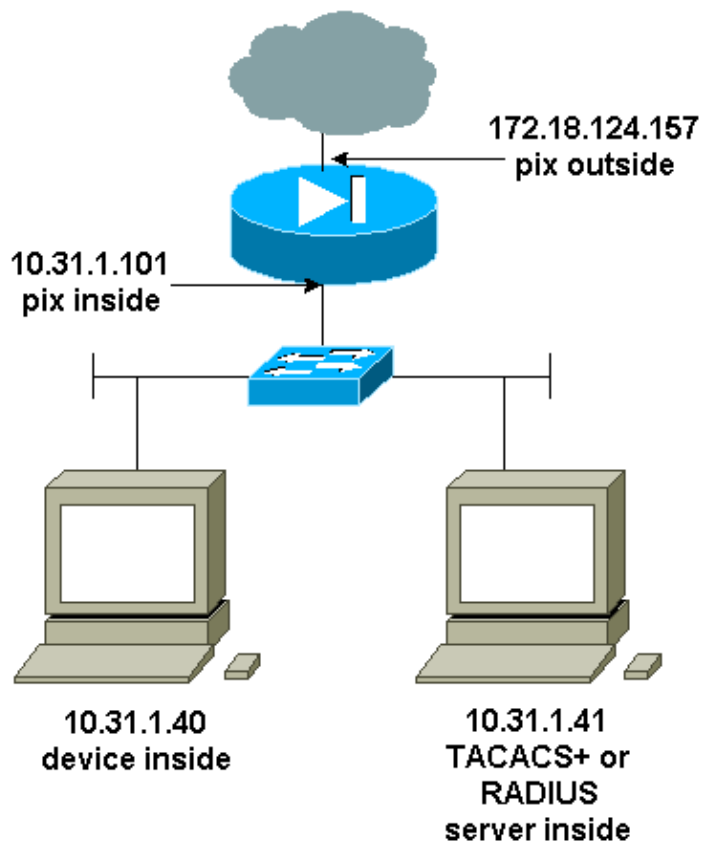
```
aaa-server radius-acctport #
```

Conventions

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

Telnet Authentication – Inside

Network Diagram



Commands Added to PIX Configuration

Add these commands to your configuration:

```
aaa-server topix protocol tacacs+
```

```
aaa-server topix host 10.31.1.41 cisco timeout 5
```

```
aaa authentication telnet console topix
```

The user sees a request for the PIX password (as in `passwd <whatever>`), and then a request for the RADIUS or TACACS username and password (stored on the 10.31.1.41 TACACS or RADIUS server).

Console Port Authentication

Add these commands to your configuration:

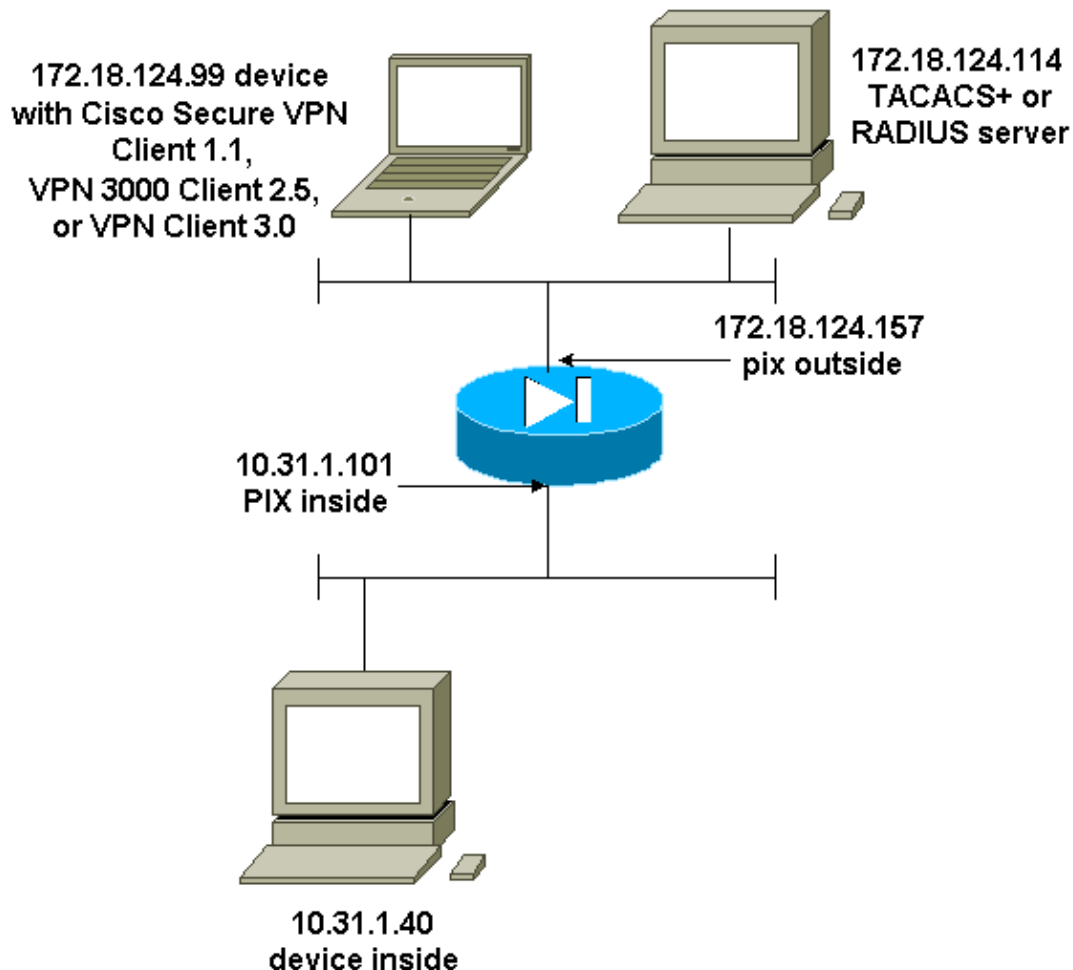
```
aaa-server topix protocol tacacs+
```

```
aaa-server topix host 10.31.1.41 cisco timeout 5
```

```
aaa authentication serial console topix
```

The user sees a request for the PIX password (as in `passwd <whatever>`), then a request for the RADIUS/TACACS username/password (stored on the RADIUS or TACACS 10.31.1.41 server).

Diagram – VPN Client 1.1, VPN 3000 2.5, or VPN Client 3.0 – Outside



Authenticated Cisco Secure VPN Client 1.1 – Outside

Authenticated Cisco Secure VPN Client 1.1 – Outside – Client Configuration

```
1- Myconn
   My Identity
```

```
Connection security: Secure
Remote Party Identity and addressing
ID Type: IP address
Port all Protocol all
Pre-shared key (matches that on PIX)
```

```
Connect using secure tunnel
ID Type: IP address
172.18.124.157
```

```
Authentication (Phase 1)
Proposal 1
```

```
Authentication method: Preshared key
Encryp Alg: DES
Hash Alg: MD5
SA life: Unspecified
Key Group: DH 1
```

```
Key exchange (Phase 2)
Proposal 1
Encapsulation ESP
Encrypt Alg: DES
Hash Alg: MD5
Encap: tunnel
SA life: Unspecified
no AH
```

2- Other Connections

```
Connection security: Non-secure
Local Network Interface
Name: Any
IP Addr: Any
Port: All
```

Authenticated Cisco Secure VPN Client 1.1 – Outside – Partial PIX Configuration

```
ip address outside 172.18.124.157 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside

!--- If you know the IP address of the outside client, use that
!--- IP address in this statement.

isakmp key ***** address 0.0.0.0 netmask 0.0.0.0
!
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400

!--- We knew our client would access the PIX from this
!--- network. If you know the IP address of the client, use that IP address
!--- in this statement.

telnet 172.18.124.0 255.255.255.0 outside
```

Authenticated VPN 3000 2.5 or VPN Client 3.0 – Outside

Authenticated VPN 3000 2.5 or VPN Client 3.0 – Outside – Client Configuration

1. Select **VPN Dialer > Properties > Name the connection** from the VPN 3000.
2. Select **Authentication > Group Access Information**. The group name and password should match what is on the PIX in the **vpngroup <group_name> password ******* statement.

When you click **Connect**, the crypto tunnel comes up, and the PIX assigns an IP address from the test pool (only mode-config is supported with the VPN 3000 client). Then you can bring up a terminal window, Telnet to 172.18.124.157, and be AAA-authenticated. The **telnet 192.168.1.x** command on the PIX allows connections from users in the pool to the outside interface.

Authenticated VPN 3000 2.5 – Outside – Partial PIX Configuration

```
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.31.1.101 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
!
!--- ISAKMP Policy for VPN 3000 Client runs 2.5 code.

isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5

!--- The 2.5 client uses group 1 policy (PIX default).

isakmp policy 10 group 1
isakmp policy 10 lifetime 86400

!--- ISAKMP Policy for VPN Client runs 3.0 code.

isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5

!--- The 3.0 clients use D-H group 2 policy and require PIX 6.0 code.

isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
!
vpngroup vpn3000 address-pool test
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password *****
telnet 192.168.1.0 255.255.255.0 outside
```

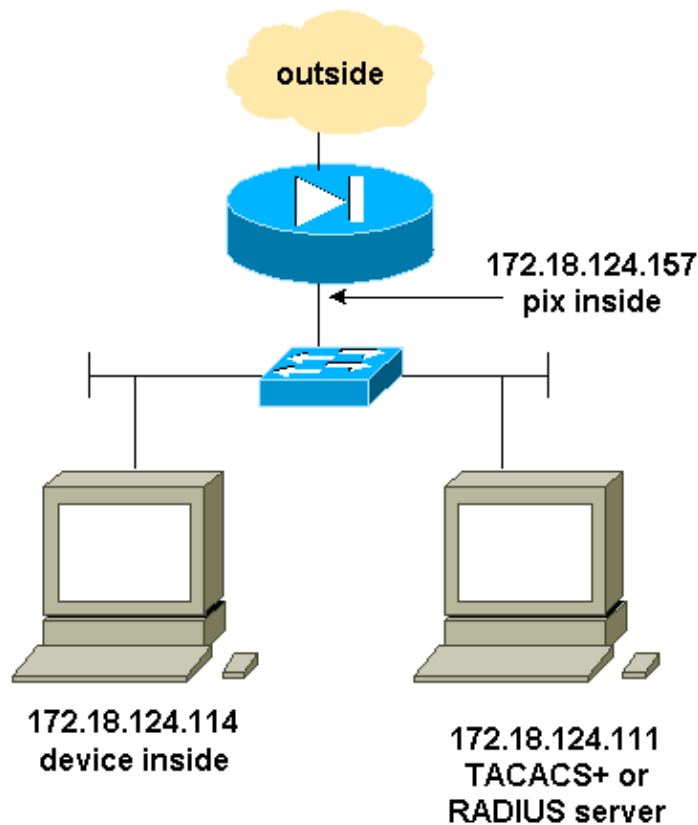
SSH – Inside or Outside

PIX 5.2 added Secure Shell (SSH) version 1 support. SSH 1 is based on a November, 1995, IETF draft. SSH version 1 and 2 are not compatible with each other. Refer to the Secure Shell (SSH) Frequently Asked Questions for more information about SSH.

The PIX is considered the SSH server. Traffic from SSH clients (that is, boxes running SSH) to the SSH server (the PIX) is encrypted. Some SSH version 1 clients are listed in the PIX 5.2 release notes. Tests in our lab were done with F-secure SSH 1.1 on NT and Version 1.2.26 for Solaris.

Note: For PIX 7.x, refer to the Allowing SSH Access section of Managing System Access.

Network Diagram



Configure AAA Authenticated SSH

Complete these steps to configure AAA authenticated SSH:

1. Make sure you can Telnet to PIX with AAA on but without SSH:

```
aaa-server AuthOutbound protocol radius (or tacacs+)
aaa authentication telnet console AuthOutbound
aaa-server AuthOutbound host 172.18.124.111 cisco
```

Note: When SSH is configured, the **telnet 172.18.124.114 255.255.255.255** command is not needed because the **ssh 172.18.124.114 255.255.255.255 inside** is issued on the PIX. Both commands are included for testing purposes.

2. Add SSH using these commands:

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024
```

```
!--- Caution: The RSA key is not be saved without
!--- the ca save all command.
!--- The write mem command does not save it.
!--- In addition, if the PIX has undergone a write erase
!--- or has been replaced, then cutting and pasting
!--- the old configuration does not generate the key.
!--- You must re-enter the ca gen rsa key command.
!--- If there is a secondary PIX in a failover pair, the write standby
!--- command does not copy the key from the primary to the secondary.
!--- You must also generate and save the key on the secondary device.
```

```
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
aaa authen ssh console AuthOutbound
logging trap debug
logging console debug
```

3. Issue the **show ca mypubkey rsa** command in config mode.

```
goss-d3-pix(config)#show ca mypubkey rsa
% Key pair was generated at: 08:22:25 Aug 14 2000
Key name: goss-d3-pix.rtp.cisco.com
Usage: General Purpose Key
Key Data:
 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ad4bcb
 e9c174d5 0657a0f3 c94e4b6d 32ac8500 6b84e754 59e20df4 f28c257d 131af21d
 4c0a8f4c e79d8b6d a3520faa 1a42d577 c6adfe51 9d96fa62 f3be07fb 01e082d7
 133cecff bf24f653 bc690b11 ee222070 413c1920 d02321f8 4fc3c5f1 f0c6e077
 81e93184 af55438b dcdca34 c0a5f5ad 87c435ef
    67170674 4d5ba51e 6d020301 0001
% Key pair was generated at: 08:27:18 Aug 14 2000
Key name: goss-d3-pix.rtp.cisco.com.server
Usage: Encryption Key
Key Data:
 307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00d4f61b ec45843a
 4ad9266d b125ee26 efc63cc4 e5e9cda4 9418ee53 6e4d16cf 3d0dc864 4d4830c8
 fa7f110e 8a5761ed 4ca73ea7 5d405862 6f3150df 9eb0d11e 9c4d3563 95ff51ae
 6711d60b 9a1415e4 19201d3f 03b455ea c1df9a41 b3a5a73f 4f020301 0001
```

4. Try a Telnet from the Solaris station:

```
rtp-evergreen#./ssh -c 3des -l cisco -v 172.18.124.157
```

Note: "cisco" is the username on the RADIUS/TACACS+ server and 172.18.124.157 is the destination.

Configure Local SSH (No AAA Authentication)

It is also possible to set up an SSH connection to the PIX with local authentication and no AAA server. However, there is no discrete per-user username. The username is always "pix."

Use these commands to configure local SSH on the PIX:

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024
```

```
!--- Caution: The RSA key is not saved without
!--- the ca save all command.
!--- The write mem command does not save it.
!--- In addition, if the PIX has undergone a write erase
```

```
!--- or has been replaced, then cutting and pasting
!--- the old configuration does not generate the key.
!--- You must re-enter the ca gen rsa key command.
!--- If there is a secondary PIX in a failover pair, a write standby
!--- command does not copy the key from the primary to the secondary.
!--- You must also generate and save the key on the secondary device.
```

```
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
passwd cisco123
```

Since the default username in this arrangement is always "pix," then the command to connect to the PIX (this was 3DES from a Solaris box) is:

```
./ssh -c 3des -l pix -v <ip_of_pix>
```

SSH Debug

Debug without the debug ssh command – 3DES and 512-cipher

```
109005: Authentication succeeded for user 'cse' from 0.0.0.0/0
      to 172.18.124.114/0 on interface SSH
109011: Authen Session Start: user 'cse', sid 0
315002: Permitted SSH session from 172.18.124.114 on interface inside
      for user "cse"
315011: SSH session from 172.18.124.114 on interface inside
      for user "cse" terminated normally
```

Debug with the debug ssh command – 3DES and 512-cipher

```
goss-d3-pix#debug ssh
SSH debugging on
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 112
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
      and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
      from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
      for user "cse"
```

Debug – 3DES and 1024-cipher

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
```

```

SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_MSG_PUBLIC_KEY message sent
SSH1: SSH_MSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
        and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
        from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
        for user "cse"

```

Debug – DES and 1024–cipher

Note: This output is from a PC with SSH, not Solaris.

```

Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.99' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-W1.0
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_MSG_PUBLIC_KEY message sent
SSH0: SSH_MSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests DES cipher: 2
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid ssh
SSH(ssh): user authen method is 'use AAA', aaa server group ID = 4
SSH(ssh): starting user authentication request,
        and waiting for reply from AAA server
SSH(ssh): user 'ssh' is authenticated
SSH(ssh): user authentication request completed
SSH0: authentication successful for ssh109
SSH0: invalid request - 0x2500
SSH0: starting exec shell5: Authentication succeeded for user 'ssh'
        from 0.0.0.0/0 to 172.18.124.99/0 on interface SSH
109011: Authen Session Start: user 'ssh', sid 1
315002: Permitted SSH session from 172.18.124.99 on interface outside
        for user "ssh"

```

Debug – 3DES and 2048–cipher

Note: This output is from a PC with SSH, not Solaris.

```

goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_MSG_PUBLIC_KEY message sent
SSH1: SSH_MSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3.
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,

```

```
and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse10900
SSH1: invalid request - 0x255:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
      from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
109011: Authen Session Start: user 'cse', Sid 2
315002: Permitted SSH session from 161.44.17.151 on interface inside
      for user "cse"
```

What Can Go Wrong

Solaris debug – 2048–cipher and Solaris SSH

Note: Solaris could not handle the 2048–cipher.

```
rtp-evergreen.cisco.com: Initializing random;
seed file /export/home/cse/.ssh/random_seed
RSA key has too many bits for RSAREF to handle (max 1024).
```

Bad password or username on RADIUS/TACACS+ server

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_MSG_PUBLIC_KEY message sent
SSH1: SSH_MSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
      and waiting for reply from AAA serverss-d3-pix#
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH1: password authentication failed for cse
109006: Authentication failed for user 'cse'
      from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

User not permitted via the command:

ssh 172.18.124.114 255.255.255.255 inside

Attempts to connect:

315001: Denied SSH session from 161.44.17.151 on interface inside

With key removed from PIX (using the **ca zero rsa** command) or not saved with the **ca save all** command

```
Device opened successfully.
SSH: unable to retrieve host public key for 'goss-d3-pix.rtp.cisco.com',
      terminate SSH connection.
SSH-2145462416: Session disconnected by SSH server - error 0x00 "Internal error"
315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
315011: SSH session from 0.0.0.0 on interface outside for user ""
      disconnected by SSH server, reason: "Internal error" (0x00)
```

AAA server is down:

```
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: SSH_SMSG_PUBLIC_KEY message sent302010: 0 in use, 0 most used
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests 3DES cipher: 3
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
        and waiting for reply from AAA server1090
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH0: password authentication failed for cse0
SSH0: authentication failed for cse
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
2: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
    (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
    (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
    (server 172.18.124.111 failed) on interface outside
109006: Authentication failed for user 'cse' from 0.0.0.0/0
    to 172.18.124.114/0 on interface SSH
315003: SSH login session failed from 172.18.124.114 (1 attempts)
    on interface outside by user "cse"
315011: SSH session from 172.18.124.114 on interface outside for user "cse"
    disconnected by SSH server, reason: "status code: 0x03" (0x03)
109012: Authen Session End: user 'cse', Sid 0, elapsed 352 seconds
```

Client is set up for 3DES but there is only DES key in PIX:

Note: Client was Solaris not supporting DES.

```
GOSS-PIX# Device opened successfully.
SSH: host key initialised
SSH: license supports DES: 1.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
315011: SSH session from 172.18.124.114 on interface outside for user ""
    disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

and on our Solaris CLI:

```
Selected cipher type 3DES not supported by server.
```

How to Remove RSA Key from PIX

ca zero rsa

How to Save RSA Key to PIX

`ca save all`

How to Allow SSH from Outside SSH Client

`ssh outside_ip 255.255.255.255 outside`

Enable Authentication

With the command:

`aaa authentication enable console topix`

(where *topix* is our server list), the user is prompted for a username and password which is sent to the TACACS or RADIUS server. Since the authentication packet for enable is the same as the authentication packet for login, if the user can log into the PIX with TACACS or RADIUS, they can enable through TACACS or RADIUS with the same username/password.

More information on these issues are available in Cisco bug ID CSCdm47044 (registered customers only) .

Syslog Information

While AAA accounting is only valid for connections through the PIX, not to the PIX, if syslogging is set up, information on what the authenticated user did is sent to the syslog server (and to the network management server, if configured, through the syslog MIB).

If syslogging is set up, then messages such as these are displayed at the syslog server:

Logging trap notification level:

```
111006: Console Login from pixuser at console
111007: Begin configuration: 10.31.1.40 reading from terminal
111008: User 'pixuser' executed the 'conf' command.
111008: User 'pixuser' executed the 'hostname' command.
```

Logging trap informational level (which includes notification level):

```
307002: Permitted Telnet login session from 10.31.1.40
```

Gain Access When the AAA Server is Down

If the AAA server is down, you can enter the Telnet password access the PIX initially, then **pix** for the username, and then the enable password (**enable password whatever**) for the password. If **enable password whatever** is not in the PIX configuration, enter **pix** for the username and press **Enter**. If the enable password is set but not known, you need a password recovery disk to reset the password.

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 the following information.

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

Please attach the collected data to your case in non-zipped, plain text format (.txt). You can attach information to your case by uploading it using the Case Query Tool (registered customers only) . If you cannot access the Case Query Tool, you can send the information in an email attachment to attach@cisco.com with your case number in the subject line of your message.

Related Information

- [Cisco Secure PIX Firewall Command References](#)
- [PIX RADIUS TACACS+](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

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

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 26, 2006

Document ID: 8505
