Cisco Secure PIX Firewall（5.2～6.2）で認証と有効化を行う方法

内容

概要

このドキュメントでは、PIX ソフトウェア バージョン 5.2 ～ 6.2 が稼働する PIX Firewall に AAA 認証を使用してアクセスする方法について説明し、イネーブル認証、syslog、および AAA サーバのダウン時のアクセス方法に関する情報を示します。PIX 5.3 以上における、認証、許可、会計（AAA）の旧バージョンのコードからの変更点は、RADIUS ポートが設定可能なことです。

PIX ソフトウェア バージョン 5.2 以上では、次の 5 通りの方法で PIX への AAA 認証アクセスを

実行できます。

- Telnet 認証 - 内部
- コンソール ポート認証
- 認証された Cisco Secure VPN Client 1.1 - 外部
- VPN 3000 2.5 の認証 - 外部
- Secure Shell（SSH）の認証 - 内部または外部

注：最後の3つの方法では、PIXでDESまたは3DESを有効にする(確認するには**show version**コマンドを発行して)必要があります。PIXソフトウェアバージョン6.0以降では、PIX Device Manager(PDM)をロードしてGUI管理を有効にすることもできます。PDM はこのドキュメントの適用範囲外です。

PIX 6.2のauthenticationおよびauthorizationコマンドの詳細については、『PIX 6.2:認証および認可コマンドの設定例.

PIXソフトウェアバージョン6.3以降が稼働するPIXファイアウォールへのAAA認証（カットスループロキシ）アクセスを作成するには、『PIX/ASA:TACACS+ および RADIUS サーバを使用したネットワーク アクセスのカットスルー プロキシの設定例.

前提条件

要件

AAA認証を追加する前に、次の作業を実行します。

- PIXのパスワードを追加するには、次のコマンドを発行します。**passwd wwtelnet <local_ip> [<mask>] [<if_name>]**PIXは、このパスワードを自動的に暗号化し、キーワード**encrypted**を使用して暗号化された文字列を形成します。次に例を示します。
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  encrypted キーワードを追加する必要はありません。
- これらの文を追加した後は、AAA認証なしで内部ネットワークからPIXの内部インターフェイスにTelnetできることを確認してください。
- コマンドのバックアウトが必要な場合は、認証文を追加する間は、必ずPIXへの接続を開いてください。

AAA認証（クライアントに依存するSSH以外）では、ユーザはPIXパスワードの要求(*passwd <which>*など)を確認し、次にRADIUSまたはTACACSのユーザ名とパスワードの要求を確認します。

注：PIXの外部インターフェイスにはTelnetできません。外部SSHクライアントから接続されている場合、外部インターフェイスでSSHを使用できます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PIX ソフトウェア バージョン 5.2、5.3、6.0、6.1、6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5
- Cisco VPN Client 3.0.x（PIX 6.0 のコードが必要）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定可能な RADIUS ポート（5.3 以降）

一部の RADIUS サーバは、1645/1646 以外の RADIUS ポート（通常は 1812/1813）を使用します。 PIX 5.3では、次のコマンドを使用して、RADIUS認証ポートとアカウンティングポートをデフォルトの1645/1646以外に変更できます。

aaa-server radius-authport #

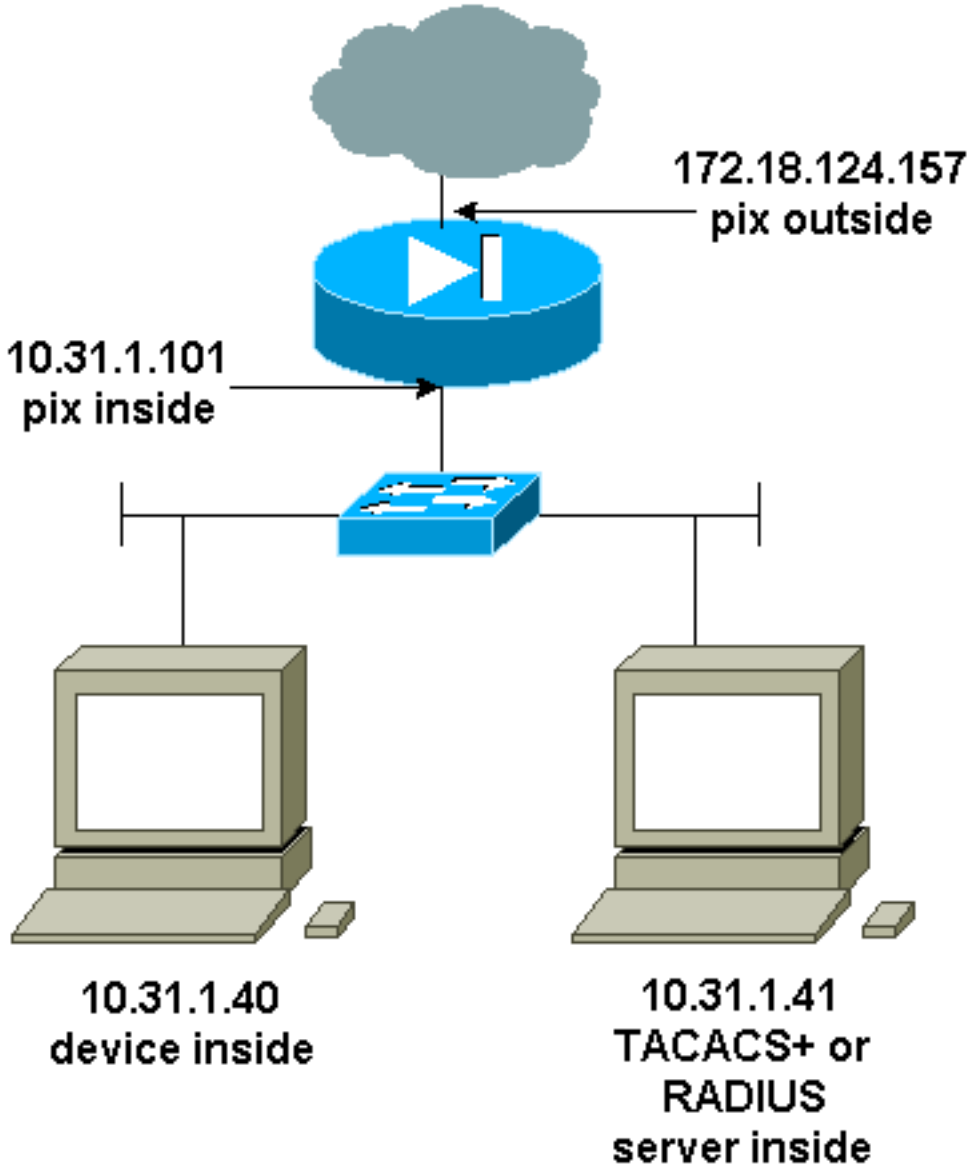
aaa-server radius-acctport #

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

Telnet 認証 - 内部

ネットワーク図



PIX 設定に追加されるコマンド

次のコマンドを設定に追加します。

aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication telnet console topix

ユーザには、PIXパスワードの要求(`passwd <why>`など)が表示され、次にRADIUSまたはTACACSのユーザ名とパスワードの要求(10.31.1.41 TACACSまたはRADIUSサーバに保存)が表示されます。

コンソール ポート認証

次のコマンドを設定に追加します。

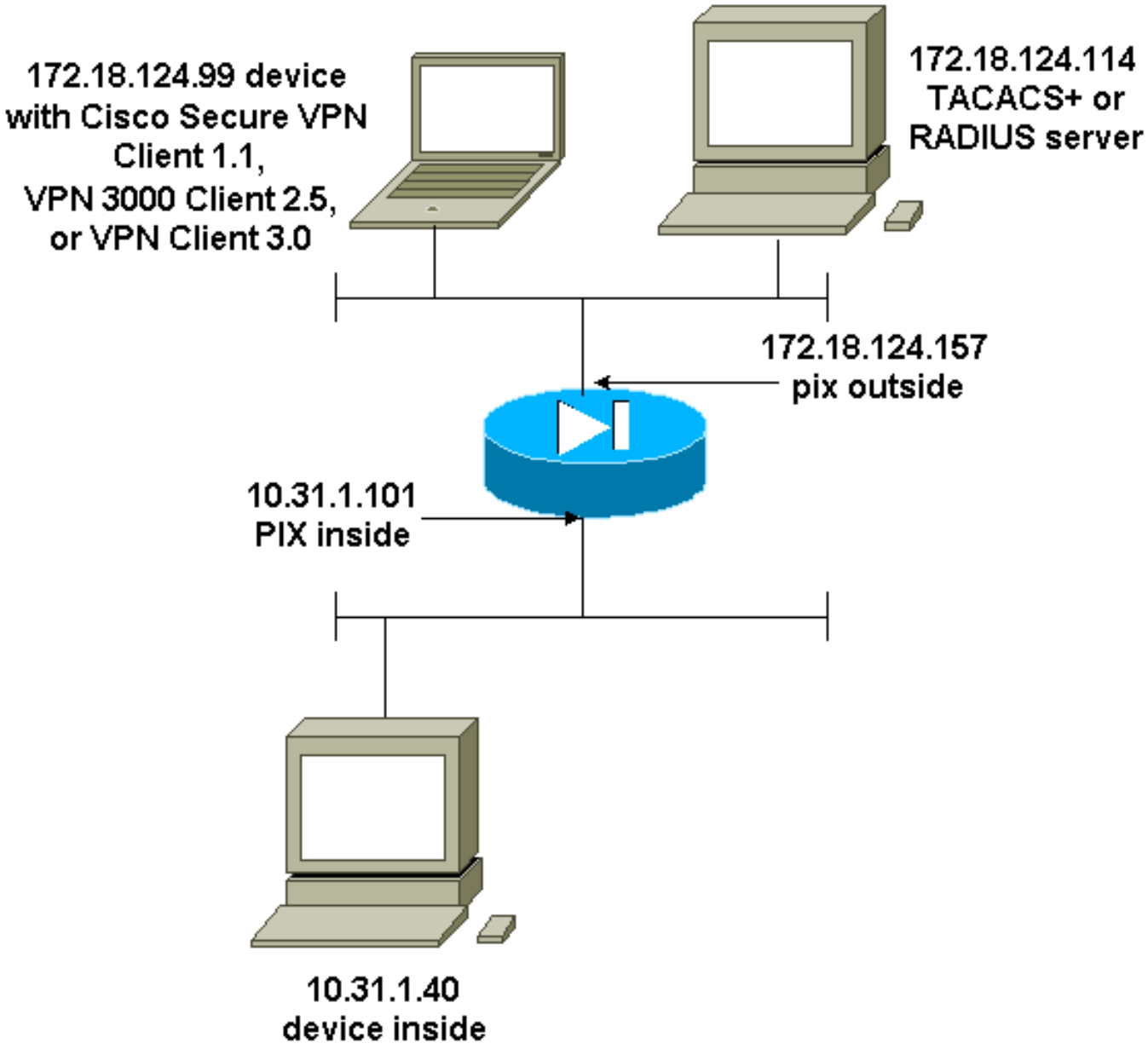
aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication serial console topix

ユーザにPIXパスワードの要求(passwd <why>など)が表示され、次にRADIUS/TACACSユーザ名/パスワードの要求(RADIUSまたはTACACS 10.31.1.41サーバに保存)が表示されます。

図 - VPN Client 1.1、VPN 3000 2.5、または VPN Client 3.0 - 外部



認証された Cisco Secure VPN Client 1.1 - 外部

Cisco Secure VPN Client 1.1 の認証 - 外部 - クライアント設定

```
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
```

Cisco Secure VPN Client 1.1 の認証 - 外部 - PIX 設定（一部）

```
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
```

認証された VPN 3000 2.5 あるいは VPN クライアント 3.0 - 外部

VPN 3000 2.5 または VPN Client 3.0 の認証 - 外部 - クライアント設定

1. VPN 3000からVPN Dialer > Properties > Name the connectionを選択します。
2. [Authentication] > [Group Access Information]を選択します。グループ名とパスワードは、vpngroup <*group_name*> password ********文のPIX上のものと一致する必要があります。

Connect をクリックすると、暗号化トンネルが作成され、PIX によって test プールからの IP アドレスが割り当てられます (VPN 3000 クライアントでは mode-config のみがサポートされます)。 これで、ターミナル ウィンドウを起動して 172.18.124.157 に Telnet し、AAA 認証を受けることができます。このプールのユーザから外部インターフェイスへの接続は、PIX 上の telnet 192.168.1.x コマンドによって許可されます。

VPN 3000 2.5 の認証 - 外部 - PIX 設定 (一部)

```
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
```

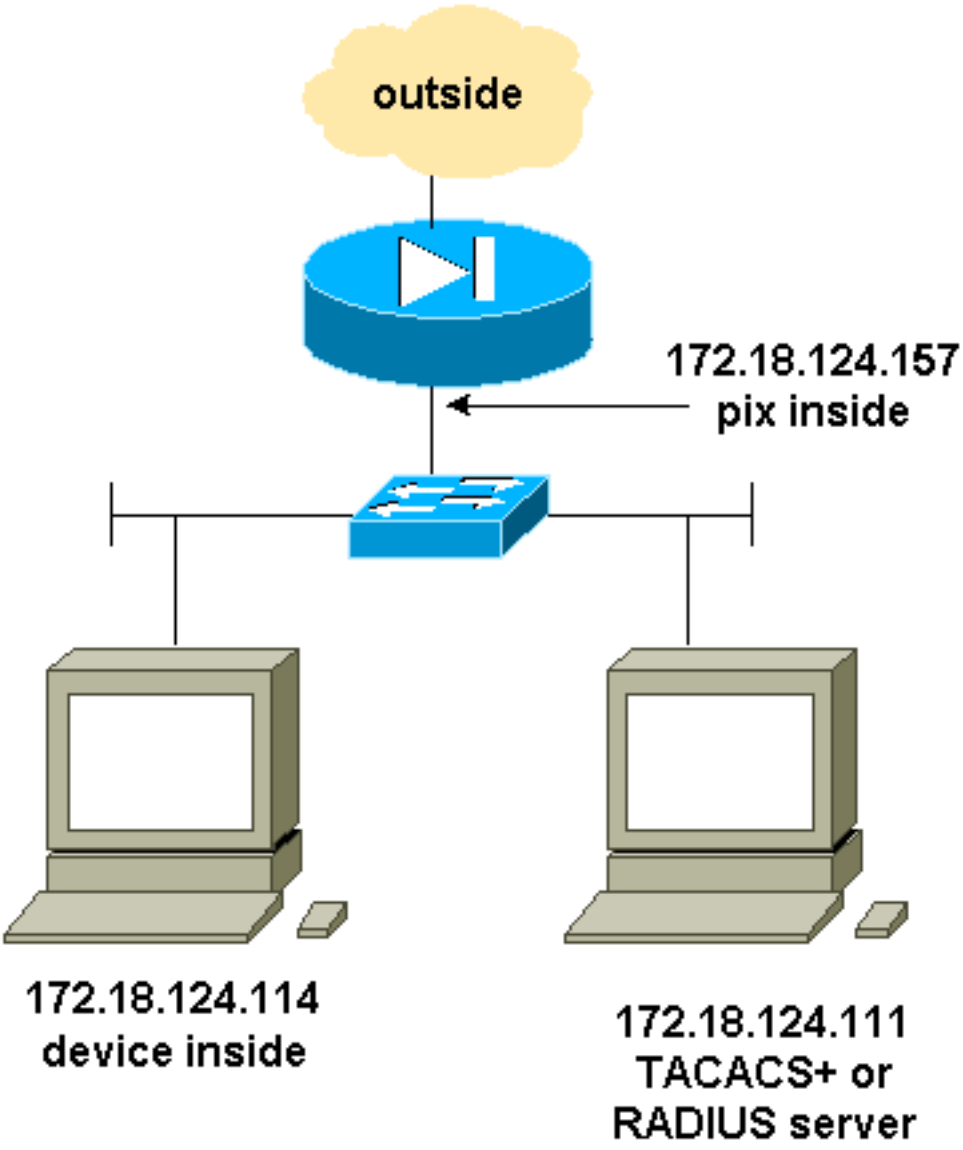
SSH - 内部または外部

PIX 5.2 では、Secure Shell (SSH; セキュア シェル) バージョン 1 のサポートが追加されています。SSH 1 は、1995 年 11 月の IETF ドラフトに基づいています。SSH バージョン 1 と 2 には互換性がありません。SSHの詳細については、SSH(Secure Shell)に関するFAQを参照してください 。

PIX は SSH サーバとしてみなされます。SSH クライアント (つまり、SSH を実行しているボックス) から SSH サーバ (PIX) へのトラフィックは暗号化されます。一部の SSH バージョン 1 クライアントは、PIX 5.2 リリース ノートに掲載されています。ラボでのテストは、NT 用の F-secure SSH 1.1 と、Solaris 用のバージョン 1.2.26 を使用して行われました。

注：PIX 7.xの場合は、『システムアクセスの管理』の「SSHアクセスの許可」セクションを参照してください。

ネットワーク図



AAA認証SSHの設定

AAA認証SSHを設定するには、次の手順を実行します。

1. SSHを使用せずに、AAAをオンにしてPIXにTelnetできることを確認します。
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   注：SSHが設定されている場合、PIXで**ssh 172.18.124.114 255.255.255.255 inside**が発行されるため、**telnet 172.18.124.114 255.255.255.255コマンドは必要ありません。**どちらのコマンドもテスト目的のために取り込まれています。
2. 次のコマンドを使用してSSHを追加します。
   ```
   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. configモードで**show ca mypubkey rsa**コマンドを発行します。

```
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 dcdcda34 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. SolarisステーションからTelnetを試します。

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

注：「cisco」はRADIUS/TACACS+サーバのユーザ名、172.18.124.157は宛先です。

ローカルSSHの設定（AAA認証なし）

ローカル認証を使用し、AAAサーバを使用せずに、PIXへのSSH接続を設定することもできます。ただし、ユーザごとの個別のユーザ名はありません。ユーザ名は常に「pix」です。

PIXでローカルSSHを設定するには、次のコマンドを使用します。

```
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
```

この仕組みでは、デフォルトのユーザ名が常に「pix」であるため、この PIX（これは Solaris ボックスからは 3DES でした）への接続コマンドは次のようになります。

```
./ssh -c 3des -1 pix -v <ip_of_pix>
```

SSH のデバッグ

debug sshコマンドを使用しないでのデバッグ – 3DESおよび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 sshコマンドを使用したデバッグ – 3DESおよび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"
```

デバッグ – 3DESおよび1024暗号

```
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 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"
```

デバッグ – DESおよび1024暗号

注：この出力は、Solarisではなく、SSHがインストールされたPCからのものです。

```
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_SMSG_PUBLIC_KEY message sent
SSH0: SSH_CMSG_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"
```

デバッグ – 3DESおよび2048暗号

注：この出力は、Solarisではなく、SSHがインストールされたPCからのものです。

```
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_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_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"
```

不具合の原因

Solarisデバッグ – 2048暗号およびSolaris SSH

注： Solarisは2048暗号を処理できませんでした。

```
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).
```

RADIUS/TACACS+サーバのパスワードまたはユーザ名が正しくありません。

```
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_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_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
```

次のコマンドでユーザが許可されない：

ssh 172.18.124.114 255.255.255.255 inside

接続の試行：

315001:Denied SSH session from 161.44.17.151 on interface inside

（ca zero rsa コマンドを使用して）PIX からキーが削除された、または ca save all コマンドでキーが保存されていない

```
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 サーバのダウン

```
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
```

クライアントには 3DES が設定されているが、PIX には DES キーしか設定されていない

注：クライアントはSolarisでDESをサポートしていませんでした。

```
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)
```

Solaris CLI の出力

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

PIX から RSA キーを削除する方法

ca zero rsa

RSA キーを PIX に保存する方法

ca save all

外部 SSH クライアントからの SSH を許可する方法

ssh outside_ip 255.255.255.255 outside

認証を有効にする方法

次のコマンドを使用すると

aaa authentication enable console topix

（topix はサーバ リスト）、ユーザは TACACS または RADIUS サーバに送信するユーザ名とパスワードの入力を求められます。イネーブル用の認証パケットはログイン用の認証パケットと同じであるため、TACACS または RADIUS が設定された PIX にログインできるユーザは、同じユーザ名/パスワードで TACACS または RADIUS を通じてその PIX をイネーブルにすることができます。

これらの問題の詳細は、Cisco Bug ID CSCdm47044(登録ユーザ専用)を参照してください。

Syslog情報

AAA アカウンティングが、PIX への接続ではなく、PIX を経由した接続に対してのみ有効な場合は、syslog を設定することで、認証ユーザによる操作についての情報を syslog サーバに送信できます（ネットワーク管理サーバを設定すれば、syslog MIB を通じてネットワーク管理サーバにも送信できます）。

syslogが設定されている場合、次のようなメッセージがsyslogサーバに表示されます。

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

AAAサーバがダウンした場合のアクセス権の取得

AAAサーバがダウンしている場合は、最初にPIXにアクセスするTelnetパスワードを入力し、次にユーザ名に**pix**を、次にパスワードにイネーブルパスワード(**enable password *whatever)*を入力できます**。enable password whatever が PIX 設定に含まれていない場合は、ユーザ名として pix を入力して Enter キーを押します。イネーブルパスワードが設定されているが不明な場合は、パスワードをリセットするためにパスワード回復ディスクが必要です。

TAC サービス リクエストをオープンする場合に収集する情報

上記のトラブルシューティング手順に従ってもサポートが必要で、Cisco TACでケースをオープンする場合は、必ず次の情報を含めてください。
• 問題の説明と関連するトポロジの詳細 • サービス リクエストをオープンする前に実行したト

ラブルシューティング

- show tech-support コマンドの出力
- **logging buffered debugging コマンド実行後の show log コマンドの出力、あるいは、問題を示すコンソール キャプチャ（採取されている場合）**

収集したデータは、圧縮しないプレーンなテキスト形式（.txt）でサービス リクエストに添付してください。 情報をサービス リクエストに添付するには、TAC Service Request Tool（登録ユーザ専用）を使用してアップロードします。 Service Request Tool にアクセスできない場合は、電子メールへの添付で、attach@cisco.com に情報を送信できます。この場合は、メッセージの件名（Subject）行にサービス リクエスト番号を記入してください。

関連情報

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- PIX RADIUS TACACS+