Como executar a autenticação e ativação no Cisco Secure PIX Firewall (5.2 a 6.2)

Contents

Introduction

Este documento descreve como criar acesso autenticado AAA para um Firewall PIX executando PIX Software, versão 5.2 a 6.2. Além disso, fornece informações sobre como habilitar a autenticação, informações de SYSLOG e sobre como obter acesso quando o servidor AAA está sem conexão. No PIX 5.3 e posterior, a mudança de AAA (autenticação, autorização e relatório) em relação às versões anteriores do código é que as portas RADIUS são configuráveis.

No software PIX versões 5.2 e posteriores, é possível criar um acesso autenticado por AAA para o PIX de cinco modos diferentes:

- Autenticação de Telnet - Interna
- Autenticação da Porta do Console
- Cisco Secure VPN Client 1.1 autenticado - Fora
- VPN 3000 2.5 autenticado - externo
- Shell Seguro Autenticado (SSH - Authenticated Secure Shell) - Interno ou Externo

Observação: DES ou 3DES devem ser ativados no PIX (emita um comando **show version** para verificar) para os três últimos métodos. No PIX Software versão 6.0 e posterior, o PIX Device Manager (PDM) também pode ser carregado para ativar o gerenciamento da GUI. Este documento não abrange o PDM.

Para obter mais informações sobre o comando authentication e authorization para PIX 6.2, consulte o PIX 6.2 : Exemplo de configuração do comando de autenticação e autorização.

Para criar acesso autenticado por AAA (Cut-through Proxy) a um PIX Firewall que execute o software PIX versões 6.3 e posteriores, consulte PIX/ASA : Proxy Cut-through para Acesso à Rede usando o Exemplo de Configuração de Servidor TACACS+ e RADIUS.

Prerequisites

Requirements

Execute estas tarefas antes de adicionar a autenticação AAA:

- Execute estes comandos para adicionar uma senha para o PIX:**passwd wwtelnet <local_ip> [<mask>] [<if_name>]**O PIX criptografa automaticamente esta senha para formar uma string criptografada com a palavra-chave **criptografada**, como neste exemplo:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  Não é necessário adicionar a palavra-chave criptografada.
- Certifique-se de que é possível executar telnet da rede interna para a interface interna do PIX *sem* autenticação AAA depois de adicionar essas instruções.
- Sempre tenha uma conexão aberta ao PIX enquanto adiciona instruções de autenticação caso seja necessário fazer o backup dos comandos.

Na autenticação AAA (diferente do SSH em que a sequência depende do cliente), o usuário vê uma solicitação para a senha do PIX (como na *senha <what>*) e, em seguida, uma solicitação para o nome de usuário e a senha do RADIUS ou TACACS.

Observação: você não pode executar telnet para a interface externa do PIX. O SSH pode ser usado na interface externa se conectado de um cliente SSH externo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software PIX versão 5.2, 5.3, 6.0, 6.1 ou 6.2
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client 2.5

- Cisco VPN Client 3.0.x (código PIX 6.0 necessário)

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.

Portas RADIUS configuráveis (5.3 e posterior)

Alguns servidores RADIUS utilizam portas RADIUS diferentes de 1645/1646 (geralmente 1812/1813). No PIX 5.3, as portas de autenticação e tarifação RADIUS podem ser alteradas para outras que não o padrão 1645/1646 com estes comandos:

aaa-server radius-authport #

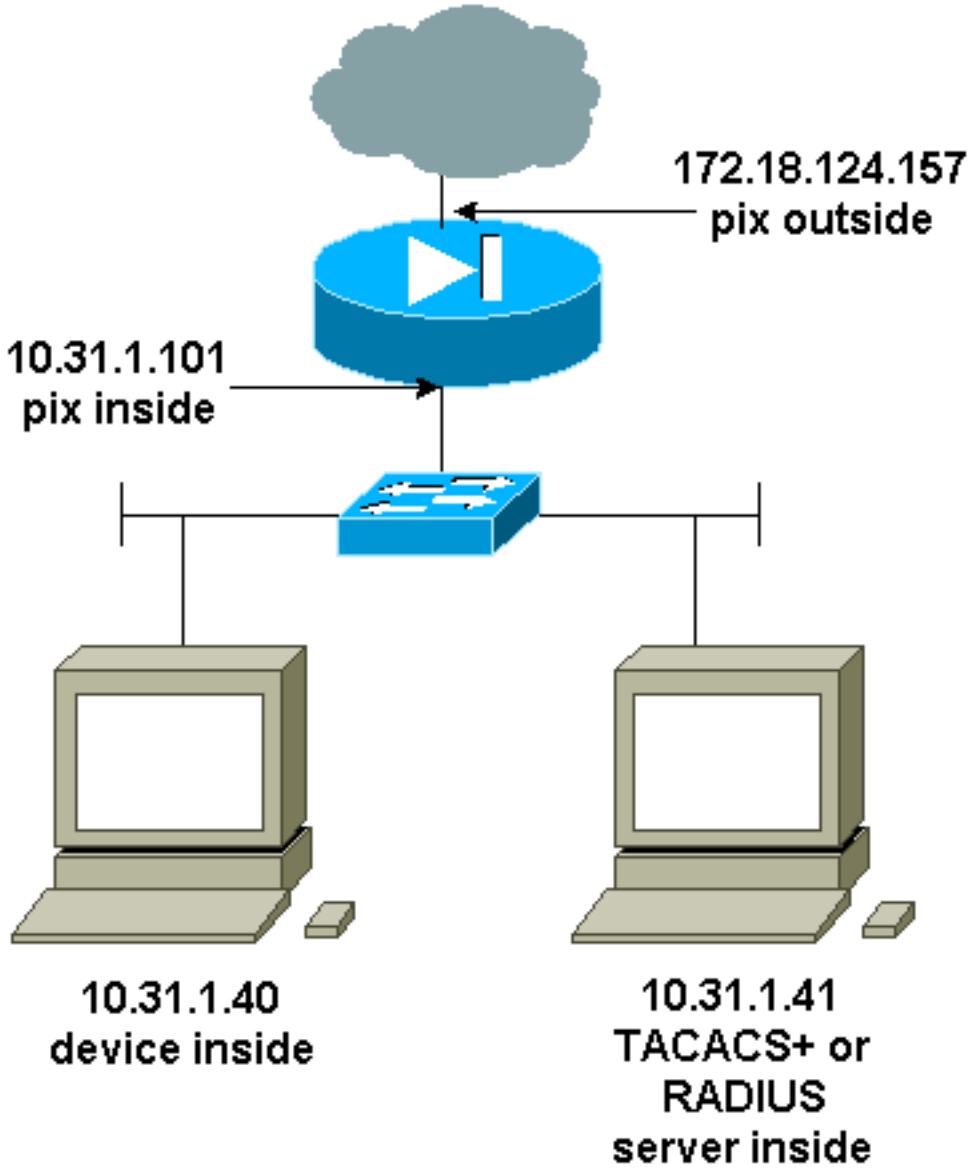
aaa-server radius-acctport #

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Autenticação de Telnet - Interna

Diagrama de Rede



Comandos adicionados à configuração PIX

Adicione estes comandos à sua configuração:

aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication telnet console topix

O usuário vê uma solicitação para a senha do PIX (como em `passwd <what>`) e, em seguida, uma solicitação para o nome de usuário e a senha do RADIUS ou TACACS (armazenados no servidor 10.31.1.41 TACACS ou RADIUS).

Autenticação da Porta do Console

Adicione estes comandos à sua configuração:

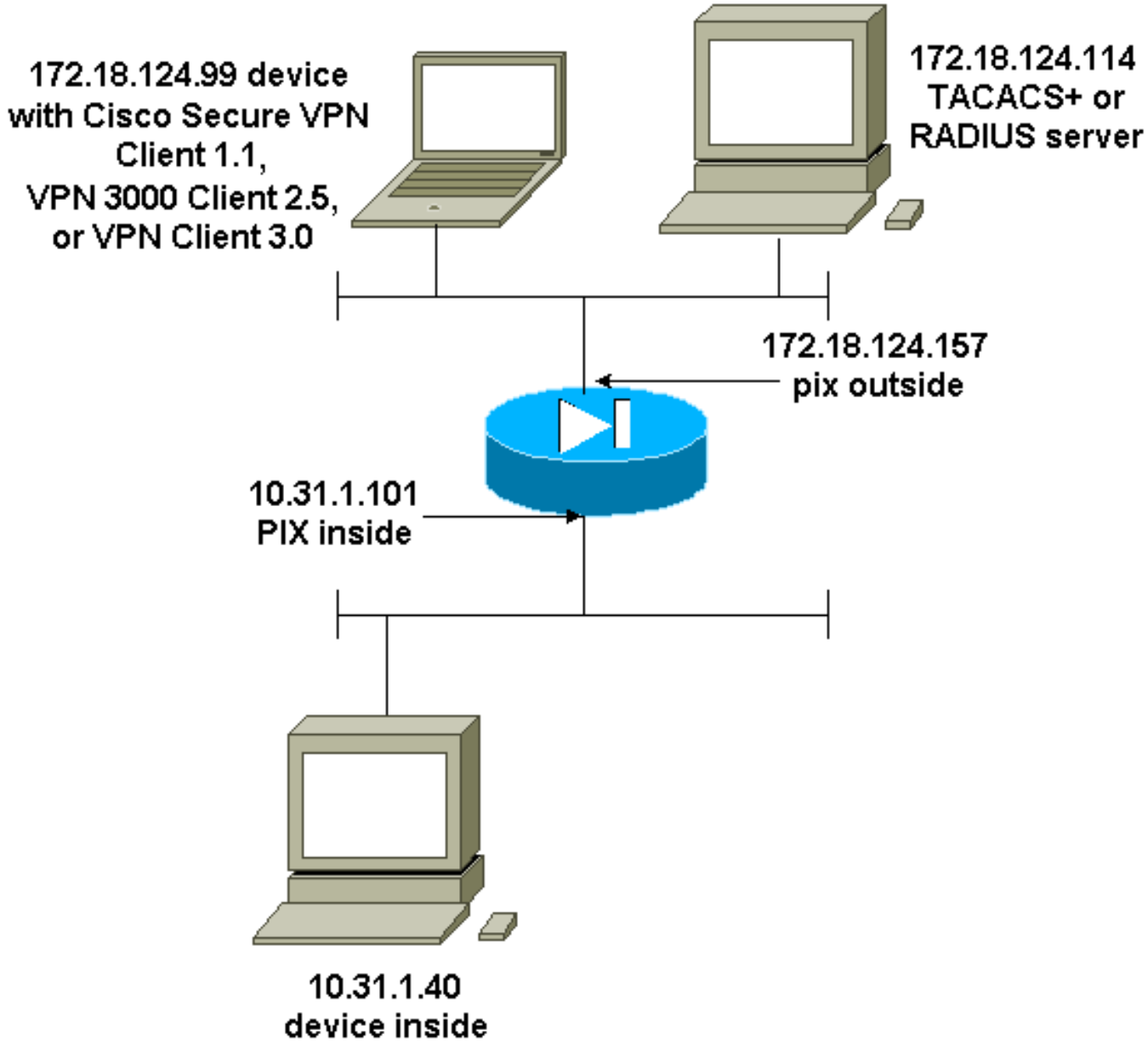
aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication serial console topix

O usuário vê uma solicitação para a senha do PIX (como na `senha <o que>`) e, em seguida, uma solicitação para o nome de usuário/senha do RADIUS/TACACS (armazenado no servidor RADIUS ou TACACS 10.31.1.41).

Diagrama - VPN Client 1.1, VPN 3000 2.5 ou VPN Client 3.0 – Lado externo



Cisco Secure VPN Client 1.1 autenticado - Fora

Cisco Secure VPN Client 1.1 autenticado Fora Configuração do cliente
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 autenticado - fora - configuração parcial de PIX

```
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
```

VPN 3000 2.5 ou VPN Client 3.0 autenticado - Externo

VPN 3000 2.5 ou VPN Client 3.0 autenticado – Externo – Configuração cliente

1. Selecione **VPN Dialer > Properties > Name the connection (Discador VPN > Propriedades > Nomear a conexão** do VPN 3000).
2. Selecione **Authentication > Group Access Information**. O nome do grupo e a senha devem corresponder ao que está no PIX na declaração **vpngroup <*group_name*> password **********.

Ao clicar em Connect (Conectar), o túnel de criptografia é ativado e o PIX atribui um endereço IP do conjunto de teste (somente mode-config é suportado com o cliente VPN 3000). Em seguida, você pode abrir uma janela de terminal, acessar o endereço 172.18.124.157 via empresa de telecomunicações e ser autenticado por AAA. O comando telnet 192.168.1.x no PIX permite conexões a partir de usuários no pool com a interface externa.

VPN 3000 2.5 autenticado - Externo - Configuração parcial de PIX

```
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
```

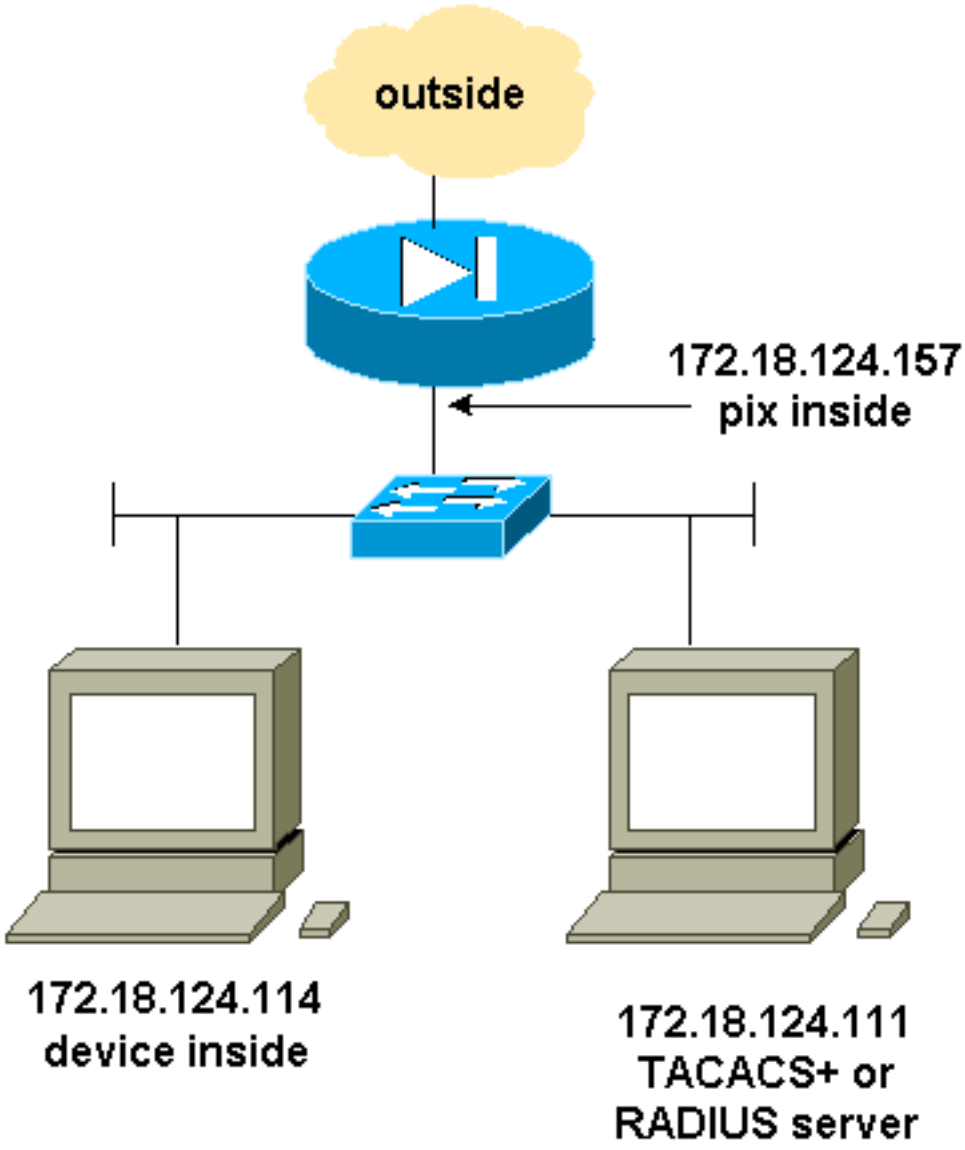
SSH – Dentro ou fora

O PIX 5.2 adicionou suporte a Secure Shell (SSH) versão 1. O SSH 1 é baseado em uma versão preliminar de novembro de 1995 da IETF. As versões 1 e 2 do SSH não são compatíveis entre si. Consulte as Perguntas Frequentes do Shell Seguro (SSH) para obter mais informações sobre o SSH.

O PIX é considerado o servidor SSH. O tráfego de clientes SSH (ou seja, caixas executando SSH) para o servidor SSH (o PIX) é criptografado. Alguns clientes SSH versão 1 estão listados nas notas de versão do PIX 5.2. Os testes em nosso laboratório foram feitos com o F-secure SSH 1.1 no NT e versão 1.2.26 para Solaris.

Nota:Para o PIX 7.x, consulte a seção Permitindo o Acesso de SSH de Gerenciando o Acesso ao Sistema.

Diagrama de Rede



Configurar SSH autenticado por AAA

Conclua estes passos para configurar o SSH autenticado AAA:

1. Certifique-se de que é possível executar telnet para PIX com AAA ligado, mas sem SSH:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Observação: quando o SSH é configurado, o comando **telnet 172.18.124.114 255.255.255** não é necessário porque o **ssh 172.18.124.114 255.5 255.255.255 inside** é emitido no PIX. Ambos os comandos são incluídos para fins de teste.
2. Adicione o SSH usando estes comandos:
   ```
   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. Emita o comando **show ca mypubkey rsa** no modo de configuração.

```
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. Tente um Telnet a partir da estação Solaris:

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

Observação: "cisco" é o nome de usuário no servidor RADIUS/TACACS+ e 172.18.124.157 é o destino.

Configurar SSH local (sem autenticação AAA)

Também é possível configurar uma conexão SSH para o PIX com autenticação local e nenhum servidor AAA. No entanto, não há um nome de usuário discreto por usuário. O nome de usuário é sempre "pix".

Use estes comandos para configurar o SSH local no 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
```

Como o nome de usuário padrão nesta organização é sempre "pix," o comando para conexão ao PIX (este era 3DES de uma caixa Solaris) é:

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

Depuração SSH

Depurar sem o comando debug ssh - 3DES e 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
```

Depurar com o comando debug ssh - 3DES e 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"
```

Depuração - 3DES e cifra 1024

```
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"
```

Depuração - DES e cifra 1024

Observação: esta saída é de um PC com SSH, não 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_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"
```

Depuração - 3DES e 2048-cipher

Observação: esta saída é de um PC com SSH, não 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_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"
```

[que pode dar errado]

Solaris debug - 2048-cipher e Solaris SSH

Observação: o Solaris não pôde lidar com a cifra 2048.

```
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).
```

Senha ou nome de usuário inválido no servidor RADIUS/TACACS+

```
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
```

Usuário não permitido por meio do comando:

ssh 172.18.124.114 255.255.255.255 inside

Tentativas de conexão:

315001 : Sessão SSH negada de 161.44.17.151 em interface interna

Com a chave removida do PIX (com o uso do comando ca zero rsa) ou não salva com o comando ca save all

```
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)
```

O servidor AAA está inoperante:

```
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
```

O cliente é configurado para o 3DES, mas há uma única chave DES no PIX:

Observação: o cliente Solaris não suportava 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)
```

e no Solaris CLI:

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

Como remover a chave RSA do PIX

ca zero rsa

Como salvar a chave RSA do PIX

ca save all

Como permitir o SSH de fora do cliente SSH

ssh outside_ip 255.255.255.255 outside

Habilitar autenticação

Com o comando:

aaa authentication enable console topix

(em que topix é a nossa lista de servidores), o usuário utiliza um prompt para nome de usuário e senha, que é enviado para o servidor TACACS ou RADIUS. Como o pacote de autenticação para habilitação é o mesmo que o pacote de autenticação para login, se o usuário puder efetuar login no PÌX com o TACACS ou o RADIUS, poderá habilitar por meio do TACACS ou do RADIUS com o mesmo nome de usuário/senha.

Mais informações sobre esses problemas estão disponíveis na ID de bug da Cisco CSCdm47044 (somente clientes registrados) .

Informações de syslogg

Enquanto o relatório de AAA só é válido para conexões pelo PIX, não para o PIX, se syslogging for configurado, as informações sobre o que o usuário autenticado fez serão enviadas ao servidor syslog (e ao servidor de gerenciamento de rede, se configurado, por meio de syslog MIB).

Se syslogging estiver configurado, mensagens como essas serão exibidas no Servidor syslog:

Nível de notificação de desvio de registro:

```
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.
```

Nível informativo da armadilha de registro (que inclui o nível de notificação):

307002 : Sessão de login Telnet permitida a partir de 10.31.1.40

Obtenha acesso quando o servidor AAA estiver inoperante

Se o servidor AAA estiver inoperante, você pode digitar a senha Telnet para acessar o PIX inicialmente, depois **pix** para o nome de usuário e, em seguida, a senha de ativação (**enable password *what***) da senha. Caso a habilitação de senha não esteja na configuração PIX, digite pix como nome de usuário e pressione Enter. Se a senha de ativação estiver definida, mas não for conhecida, você precisará de um disco de recuperação de senha para redefini-la.

Informações a serem coletadas se você abrir um caso de TAC

Se você ainda precisar de assistência após seguir as etapas de solução de problemas acima e quiser abrir um caso no Cisco TAC, inclua as seguintes informações.
• Descrição do problema e detalhes relevantes de topologia

- Troubleshooting executado antes de abrir o caso
- Saída do comando **show tech-support**
- Saída do comando show log após a execução com o comando de depuração de registro colocado em buffer ou capturas do console que demonstram o problema (se disponível)

Anexe os dados coletados para o seu caso em um formato não compactado e texto simples (.txt). Você pode anexar informações para o seu caso, carregando-o com o uso da Case Query Tool (somente clientes registrados). Se não conseguir acessar a Case Query Tool, você poderá enviar as informações em um anexo de e-mail para attach@cisco.com com o número do caso na linha de assunto da sua mensagem.

Informações Relacionadas

- Referências do comando Cisco Secure PIX Firewall
- PIX RADIUS TACACS+