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

Índice

Introdução

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 autenticado 3000 2.5 - Fora
- Embalagem segura autenticada (SSH) - Dentro ou fora

Nota: O DES ou o 3DES devem ser permitidos no PIX (emita um **comando show version** verificar) para os últimos três métodos. Na versão de software de PIX 6.0 e mais atrasado, o gerenciador de dispositivo pix (PDM) pode igualmente ser carregado para permitir o gerenciamento de GUI. Este documento não abrange o PDM.

Para obter mais informações sobre do comando da authentication e autorização para PIX 6.2, refira PIX 6.2: Exemplo do comando Configuration da authentication e autorização.

A fim criar (Corte-através do proxy) o acesso AAA-autenticado a um PIX Firewall que executa as versões de software de PIX 6.3 e mais atrasado, refira o PIX/ASA: Corte-através do proxy para o acesso de rede usando o TACACS+ e o exemplo da configuração de servidor RADIUS.

Pré-requisitos

Requisitos

Execute estas tarefas antes que você adicione a autenticação de AAA:

- Emita estes comandos a fim adicionar uma senha para o PIX:**passwd ww[<if_name>] do [<mask>] do <local_ip> do telnet**O PIX cifra automaticamente esta senha para formar uma série criptografada com a palavra-chave **cifrada**, como neste exemplo:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  Não é necessário adicionar a palavra-chave criptografada.
- Certifique-se que você pode telnet da rede interna à interface interna do PIX *sem* autenticação de AAA depois que você adiciona estas indicações.
- Tenha sempre uma conexão aberta ao PIX quando você adicionar instruções de autenticação caso suportando para fora os comandos é necessário.

Na autenticação de AAA (a não ser o SSH onde a sequência depende do cliente), o usuário vê um pedido para a senha de PIX (como no *<whatever> da senha*), a seguir um pedido para o nome de usuário e senha radius ou TACACS.

Nota: Você não pode telnet à interface externa do PIX. O SSH pode ser usado na interface externa se conectado de um cliente SSH exterior.

Componentes Utilizados

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

- Versão de software de PIX 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 exigido)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Portas RADIUS configuráveis (5.3 e posterior)

Alguns servidores RADIUS utilizam portas RADIUS diferentes de 1645/1646 (geralmente 1812/1813). Em PIX 5.3, a autenticação RADIUS e as portas de relatório podem ser mudadas a não ser ao padrão 1645/1646 com estes comandos:

aaa-server radius-authport #

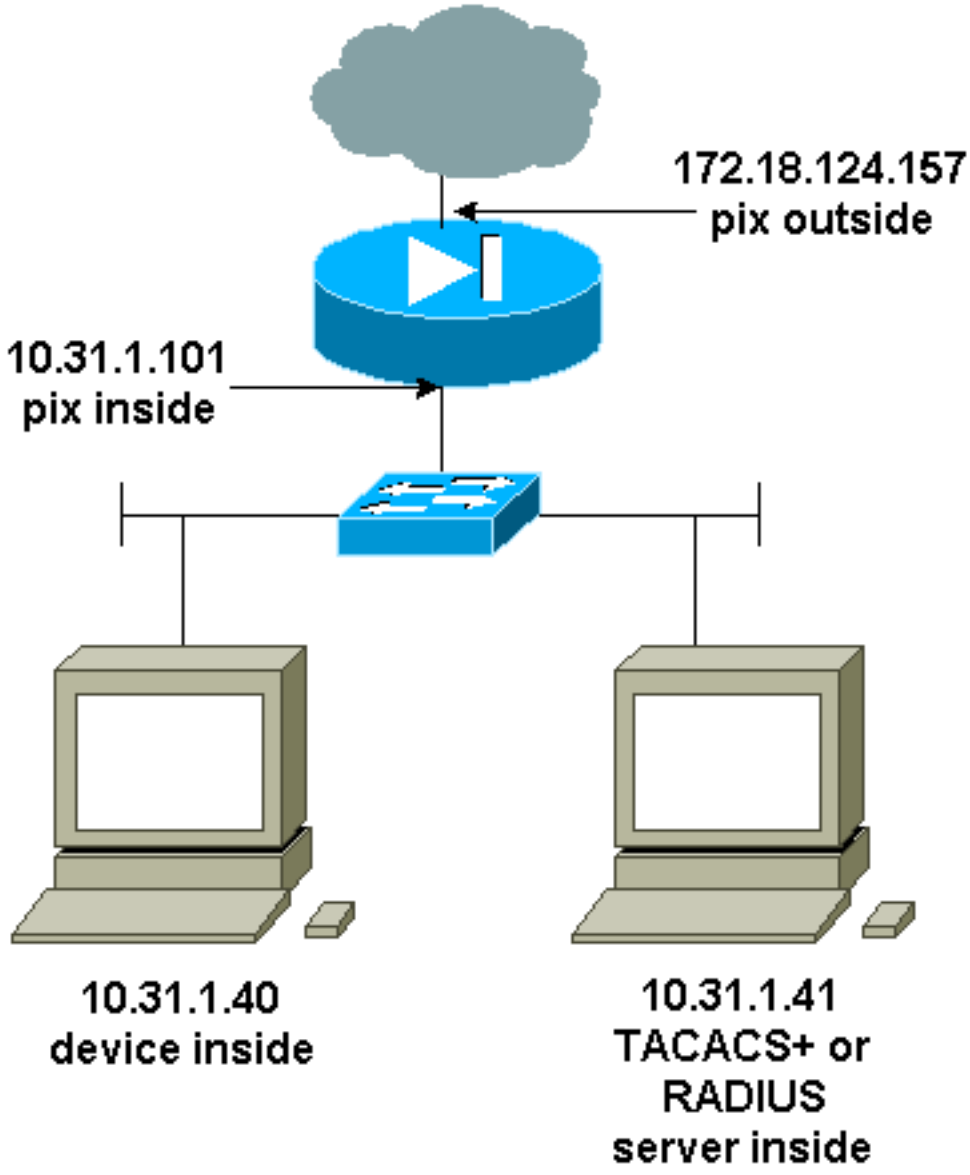
aaa-server radius-acctport #

Convenções

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

Adicionar estes comandos a sua configuração:

aaa-server topix protocol tacacs+

intervalo 5 de 10.31.1.41 Cisco do host topix de servidor AAA

topix do console Telnet de autenticação AAA

O usuário vê um pedido para a senha de PIX (como no `<whatever> da senha`), e então um pedido para o nome de usuário e senha radius ou TACACS (armazenado em 10.31.1.41 TACACS ou servidor Radius).

Autenticação da Porta do Console

Adicionar estes comandos a sua configuração:

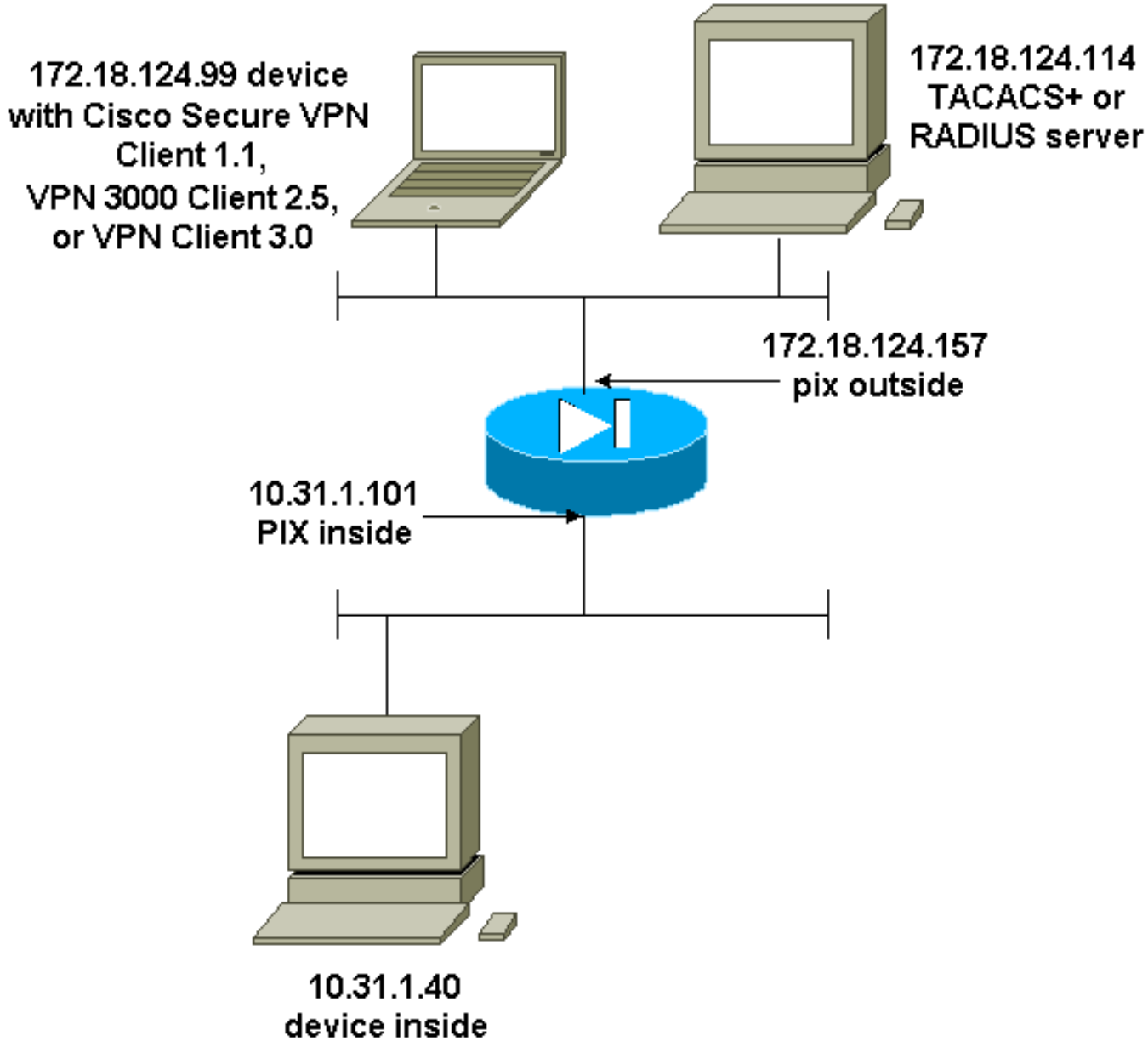
aaa-server topix protocol tacacs+

intervalo 5 de 10.31.1.41 Cisco do host topix de servidor AAA

Topix de console serial de autenticação AAA

O usuário vê um pedido para a senha de PIX (como no `<whatever> da senha`), a seguir um pedido para o username RADIUS/TACACS/senha (armazenados no server de 10.31.1.41 do radius or tacacs).

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 o **discador de VPN > as propriedades > o nome a conexão do** VPN3000.
2. Selecione a **autenticação > a informação de acesso de grupo**. O nome do grupo e a senha devem combinar o que está no PIX na indicação do ********** do <group_name > da senha do vpngroup**.

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 autenticado 3000 2.5 - Fora de - Configuração de PIX parcial

```
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
```

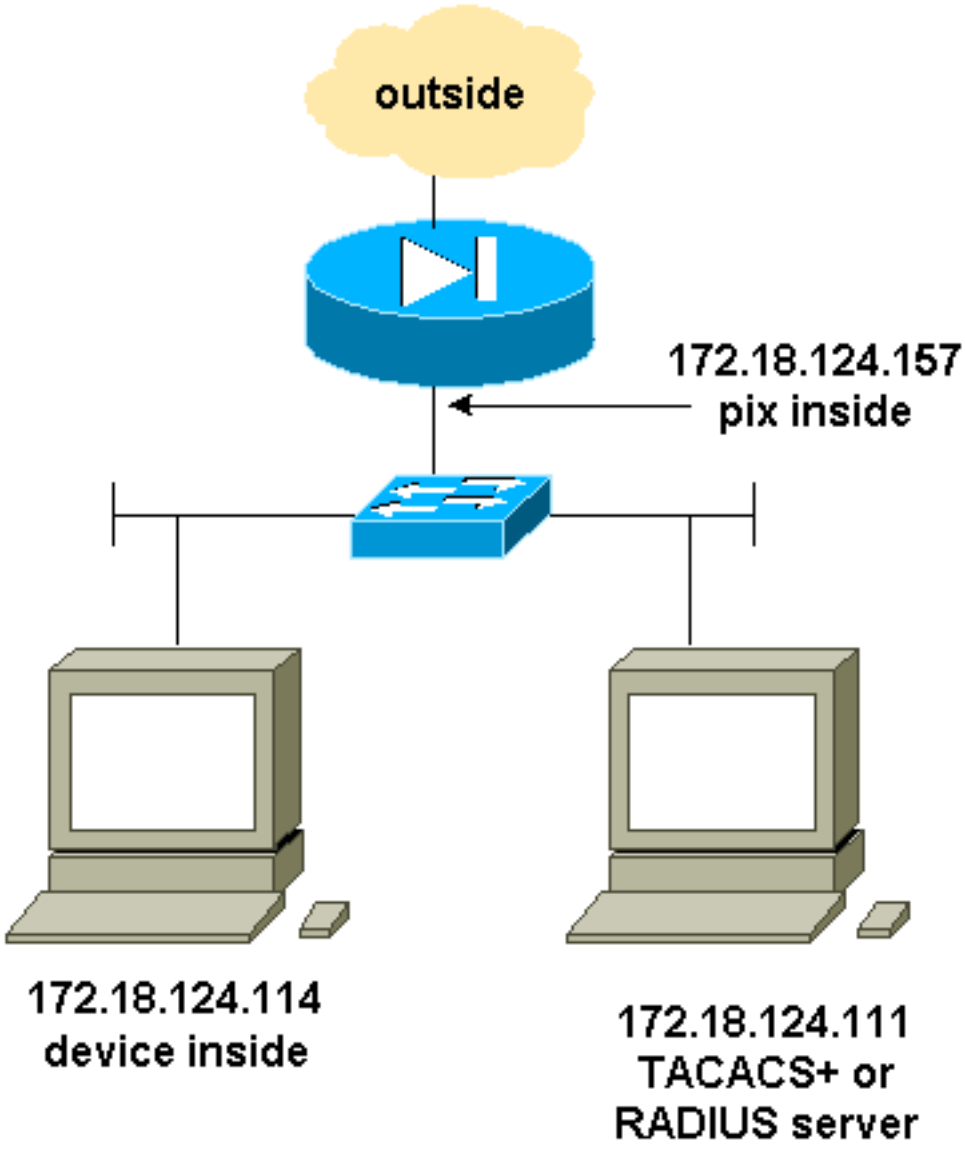
SSH - Dentro ou fora

Apoio adicionado da versão 1 do Shell Seguro (ssh) PIX 5.2. O SSH1 é baseado novembro, 1995, esboço de IETF. A versão de SSH 1 e 2 não é compatível um com o otro. Refira as perguntas mais frequentes do Shell Seguro (ssh) para obter mais informações sobre do SSH.

O PIX é considerado o servidor de SSH. O tráfego dos clientes SSH (isto é, caixas que executam o SSH) ao servidor de SSH (o PIX) é cifrado. 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 PIX 7.x, refira a seção reservando do acesso SSH controlando do acesso de sistema.

Diagrama de Rede



Configurar o SSH autenticado de AAA

Termine estas etapas para configurar o SSH autenticado de AAA:

1. Certifique-se que você pode telnet ao PIX com o AAA mas sem no SSH:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Nota: Quando o SSH é configurado, o comando de **172.18.124.114 255.255.255.255 do telnet** não está precisado porque o **interior de 172.18.124.114 255.255.255.255 do ssh** é emitido no PIX. Os comandos both são incluídos para propósitos testando.
2. Adicionar 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 da estação de Solaris:

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

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

Configurar SSH local (nenhuma autenticação de AAA)

Éigualmente possível estabelecer uma conexão de SSH ao PIX com autenticação local e nenhum servidor AAA. Contudo, não há nenhum nome de usuário discreto por usuário. O nome de usuário é sempre "pix".

Use estes comandos 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:

```
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
```

Depuração SSH

Debugar sem o comando debug ssh - 3DES e 512-cipher

```
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
```

Debugar 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"
```

Debugar - 3DES e 1024-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"
```

Debugar - DES e 1024-cipher

Nota: Essa saída é de um PC com SSH e não Solaris.

```
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"
```

Debugar - 3DES e 2048-cipher

Nota: Essa saída é de um PC com SSH e não Solaris.

```
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"
```

que pode dar errado

Solaris debuga - 2048-cipher e Solaris SSH

Nota: O Solaris não pode tratar o 2048-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"
```

Senha ruim ou username no server RADIUS/TACACS+

```
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"
```

Usuário não permitido por meio do comando:

ssh 172.18.124.114 255.255.255.255 para dentro

Tentativas de conectar:

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

```
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"
```

O servidor AAA está para baixo:

```
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"
```

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

Nota: O cliente era Solaris que não apoia o DES.

```
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"
```

e em nosso Solaris CLI:

```
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"
```

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:

a autenticação aaa permite o 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 informação nestas edições está disponível na identificação de bug Cisco CSCdm47044 (clientes registrados somente).

Informação 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 a informações de syslog se estabelece, a seguir as mensagens tais como estes estão indicadas no servidor de SYSLOG:

Nível de notificação de desvio de registro:

```
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"
```

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

307002: Sessão de login Telnet permitida a partir de 10.31.1.40

Aceda quando o servidor AAA estiver para baixo

Se o servidor AAA está para baixo, você pode incorporar o acesso da senha telnet o PIX inicialmente, a seguir **pix** para o username, e então a senha da possibilidade (**permita a senha *o que quer que***) para a senha. Caso a habilitação de senha não esteja na configuração PIX, digite pix como nome de usuário e pressione Enter. Se a senha da possibilidade é ajustada mas não sabida, você precisa um disco de recuperação de senha de restaurar a senha.

Informações a serem coletadas se você abrir um caso de TAC

Se você ainda precisa o auxílio após ter seguido os passos de Troubleshooting acima e o quer abrir um caso com o tac Cisco, seja certo incluir a informação seguinte.
• Descrição do problema e detalhes relevantes de topologia • Troubleshooting executado antes da abertura do 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 você não pode alcançar a ferramenta do

Case Query, você pode enviar a informação em um anexo de Email a attach@cisco.com com seu número de caso na linha de assunto de sua mensagem.

Informações Relacionadas

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