Come eseguire l'autenticazione e l'attivazione sul firewall Cisco Secure PIX (da 5.2 a 6.2)

Sommario

Introduzione

In questo documento viene descritto come creare un accesso con autenticazione AAA a un firewall PIX con software PIX versione 5.2-6.2 e vengono fornite informazioni su come abilitare l'autenticazione, il syslog e ottenere l'accesso quando il server AAA non è attivo. In PIX 5.3 e versioni successive, l'autenticazione, l'autorizzazione e l'accounting (AAA) vengono modificati rispetto alle versioni precedenti del codice in quanto le porte RADIUS sono configurabili.

Nel software PIX versione 5.2 e successive, è possibile creare un accesso autenticato AAA al PIX in cinque modi diversi:

- Autenticazione Telnet - Interno
- Autenticazione porta console
- Autenticato Cisco Secure VPN Client 1.1 - Esterno
- Authenticated VPN 3000 2.5 - Esterno
- SSH (Authenticated Secure Shell) - Interno o esterno

Nota: DES o 3DES devono essere abilitati sul PIX (per verificare, eseguire un comando **show version**) per gli ultimi tre metodi. Nel software PIX versione 6.0 e successive, è possibile anche caricare PIX Device Manager (PDM) per abilitare la gestione GUI. PDM non è compreso nell'ambito di questo documento.

Per ulteriori informazioni sull'autenticazione e il comando di autorizzazione per PIX 6.2, fare riferimento a PIX 6.2 : Esempio di configurazione dei comandi di autenticazione e autorizzazione.

Per creare un accesso autenticato AAA (proxy cut-through) a un firewall PIX con software PIX versione 6.3 e successive, fare riferimento a PIX/ASA : Proxy Cut-through per l'accesso alla rete con esempio di configurazione server TACACS+ e RADIUS.

Prerequisiti

Requisiti

Prima di aggiungere l'autenticazione AAA, eseguire i seguenti task:

- Per aggiungere una password per PIX, eseguire questi comandi:**passwdtelnet <ip_locale> [<maschera>] [<nome_if>]**Il PIX cripta automaticamente questa password per formare una stringa crittografata con la parola chiave **encrypted**, come nell'esempio seguente:
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  non è necessario aggiungere la parola chiave **encrypted**.
- Dopo aver aggiunto queste istruzioni, accertarsi di poter passare dalla rete interna all'interfaccia interna del PIX *senza* autenticazione AAA.
- Mantenere sempre una connessione aperta al PIX durante l'aggiunta delle istruzioni di autenticazione nel caso in cui sia necessario eseguire il backup dei comandi.

Con l'autenticazione AAA (diversa da SSH, la cui sequenza dipende dal client), l'utente riceve una richiesta di password PIX (come nella *password <any>*), quindi una richiesta di nome utente e password RADIUS o TACACS.

Nota: non è possibile eseguire la connessione Telnet all'interfaccia esterna di PIX. Se collegato da un client SSH esterno, il protocollo SSH può essere usato sull'interfaccia esterna.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software PIX versione 5.2, 5.3, 6.0, 6.1 o 6.2
- Cisco Secure VPN Client 1.1

- Cisco VPN 3000 Client 2.5
- Cisco VPN Client 3.0.x (è richiesto il codice PIX 6.0)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Porte RADIUS configurabili (5.3 e successive)

Alcuni server RADIUS utilizzano porte RADIUS diverse da 1645/1646 (generalmente 1812/1813). In PIX 5.3, le porte di autenticazione e accounting RADIUS possono essere modificate in modalità diversa da quella predefinita 1645/1646 con questi comandi:

aaa-server radius-authport #

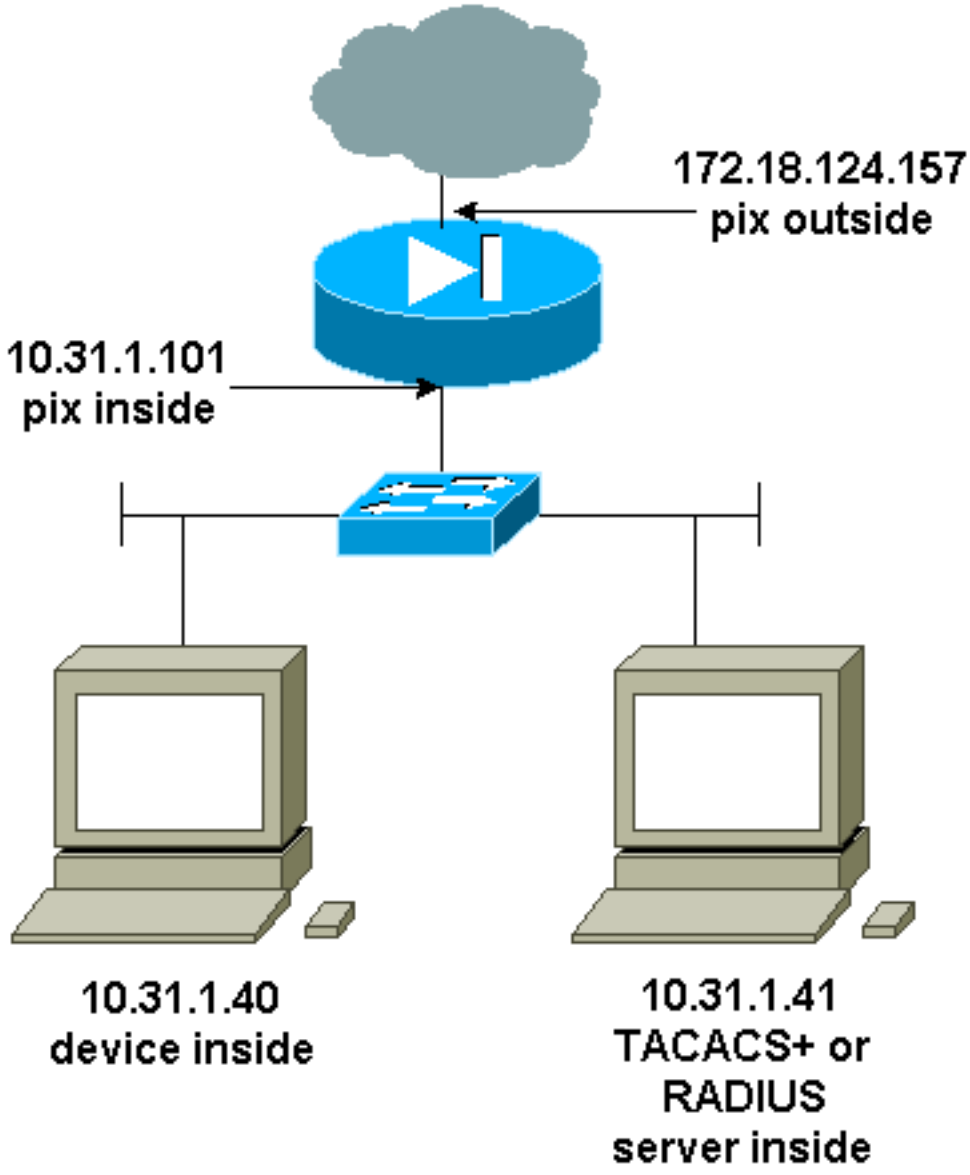
n. radius-acctport aaa-server

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Autenticazione Telnet - Interno

Esempio di rete



Comandi aggiunti alla configurazione PIX

Aggiungere i seguenti comandi alla configurazione:

tacacs+ protocollo topix aaa-server

host topix aaa-server 10.31.1.41 cisco timeout 5

topix console telnet autenticazione aaa

L'utente vede una richiesta per la password PIX (come nella `password <any>`), quindi una richiesta per il nome utente e la password RADIUS o TACACS (memorizzati sul server 10.31.1.41 TACACS o RADIUS).

Autenticazione porta console

Aggiungere i seguenti comandi alla configurazione:

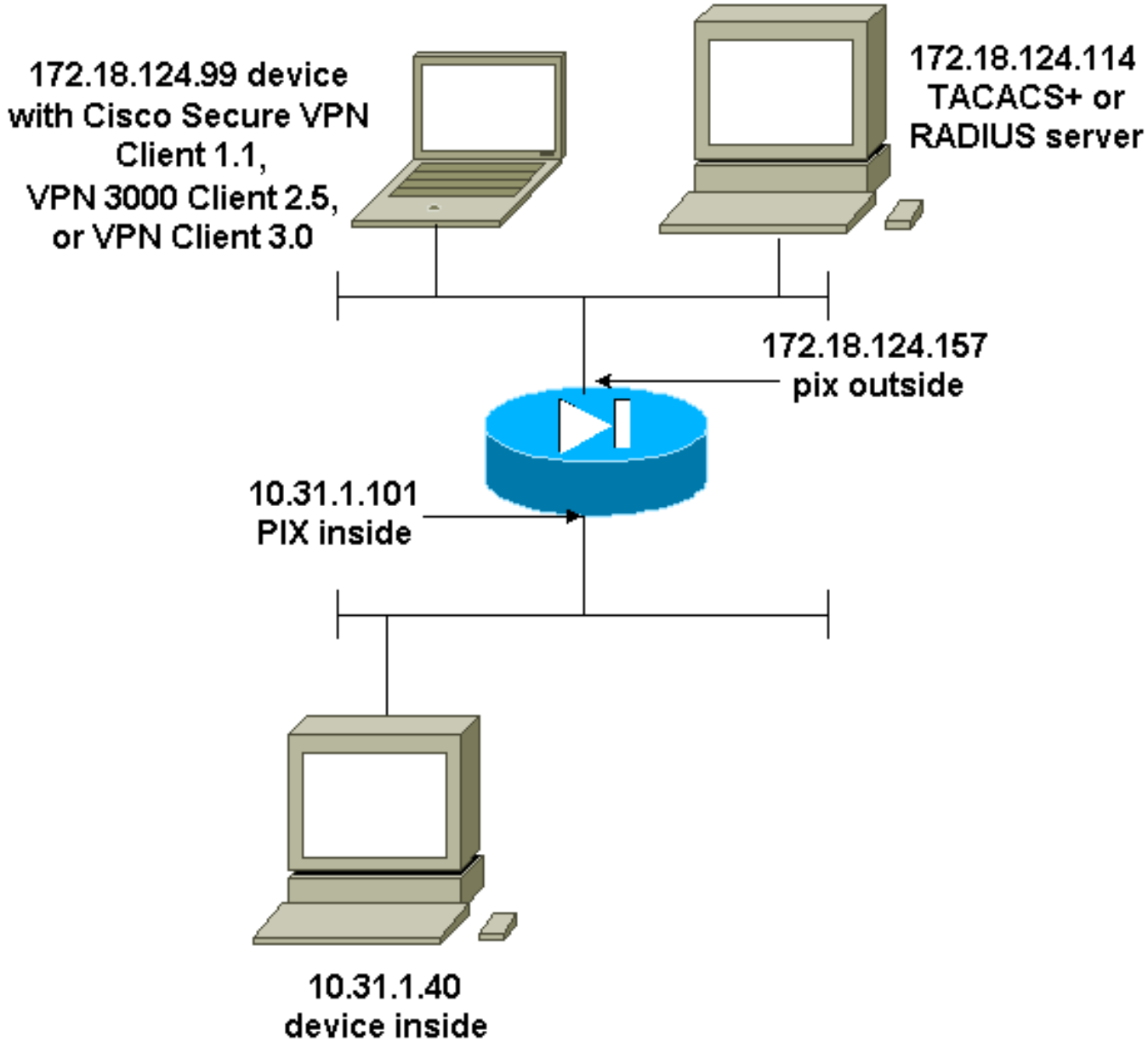
tacacs+ protocollo topix aaa-server

host topix aaa-server 10.31.1.41 cisco timeout 5

topix console seriale autenticazione aaa

L'utente vede una richiesta per la password PIX (come nella `password <any>`), quindi una richiesta per il nome utente/la password RADIUS/TACACS (memorizzata sul server RADIUS o TACACS 10.31.1.41).

Diagramma - VPN Client 1.1, VPN 3000 2.5 o VPN Client 3.0 - Esterno



Autenticato Cisco Secure VPN Client 1.1 - Esterno

Autenticato Cisco Secure VPN Client 1.1 - Esterno - Configurazione client
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
```

Autenticato Cisco Secure VPN Client 1.1 - Esterno - Configurazione PIX parziale

```
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
```

Autenticato VPN 3000 2.5 o VPN Client 3.0 - Esterno

Authenticated VPN 3000 2.5 o VPN Client 3.0 - Esterno - Configurazione client

1. Selezionare **VPN Dialer > Proprietà > Nome connessione** dalla VPN 3000.
2. Selezionare **Autenticazione > Informazioni accesso gruppo**. Il nome e la password del gruppo devono corrispondere a quelli presenti nel PIX nell'istruzione **vpngroup <*nome_gruppo*> password *********.

Quando si fa clic su **Connect**, viene visualizzato il tunnel crittografico e il PIX assegna un indirizzo IP dal pool di test (solo la configurazione in modalità è supportata con il client VPN 3000). Quindi, è possibile visualizzare una finestra del terminale, Telnet su 172.18.124.157, e autenticare il server AAA. Il comando **telnet 192.168.1.x** sul PIX consente le connessioni dagli utenti del pool all'interfaccia esterna.

Authenticated VPN 3000 2.5 - Esterno - Configurazione PIX parziale

```
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
```

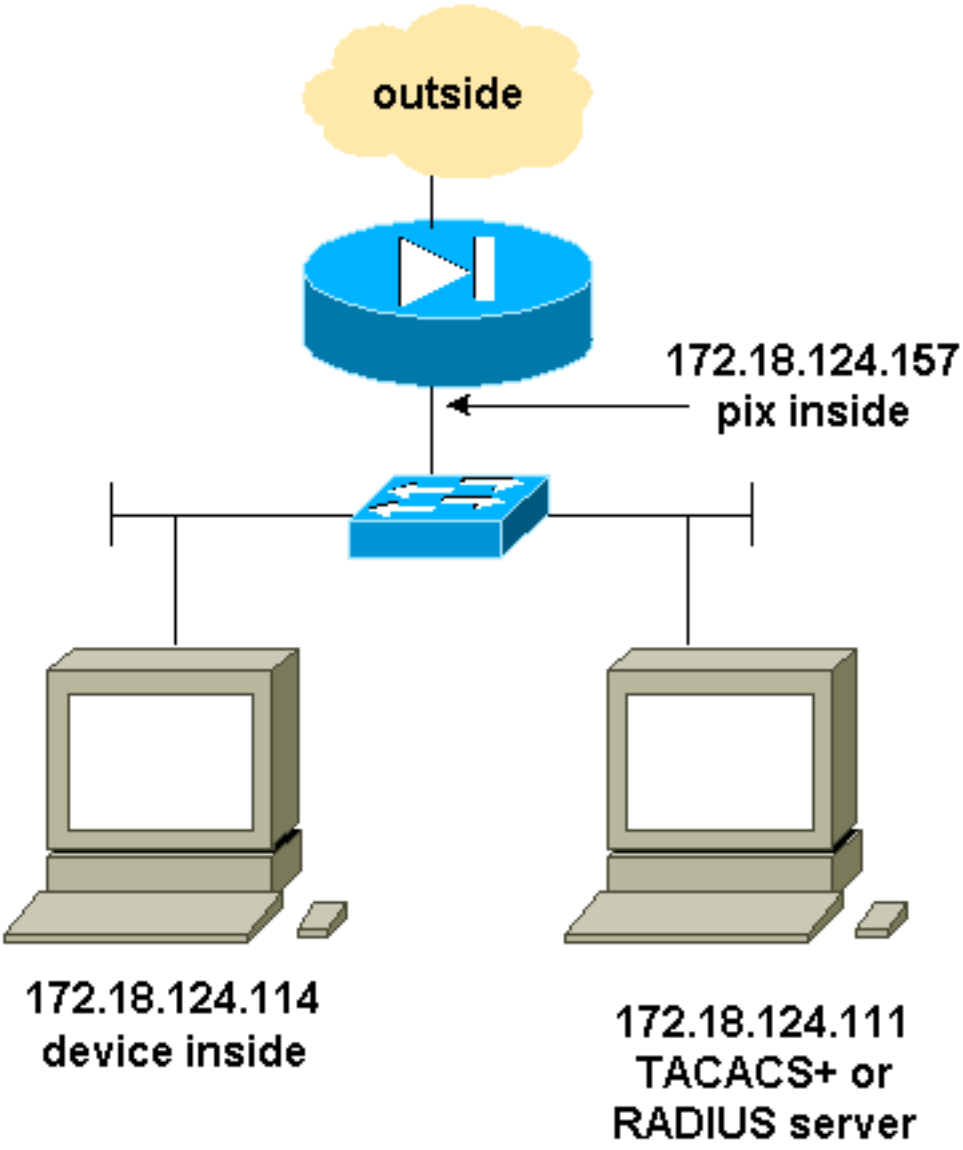
SSH - Interno o esterno

PIX 5.2 ha aggiunto il supporto Secure Shell (SSH) versione 1. Il protocollo SSH 1 si basa sul progetto dell'IETF del novembre 1995. SSH versione 1 e 2 non sono compatibili tra loro. Per ulteriori informazioni sul protocollo SSH, fare riferimento alle domande frequenti su SSH (Secure Shell).

Il PIX è considerato il server SSH. Il traffico tra i client SSH (ossia, le scatole con SSH) e il server SSH (il PIX) è crittografato. Alcuni client SSH versione 1 sono elencati nelle note sulla versione PIX 5.2. I test sono stati eseguiti con F-secure SSH 1.1 su NT e versione 1.2.26 per Solaris.

Nota: per PIX 7.x, fare riferimento alla sezione Autorizzazione dell'accesso SSH in Gestione dell'accesso al sistema.

Esempio di rete



Configurazione di AAA Authenticated SSH

Completare la procedura seguente per configurare il protocollo SSH autenticato AAA:

1. Accertarsi di poter usare Telnet to PIX con AAA attivo ma senza SSH:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   Nota: quando il protocollo SSH è configurato, il comando **telnet 172.18.124.114.255.255.255.255** non è necessario perché il comando **ssh 172.18.124.114.255.255.255.255** è emesso sul PIX. Entrambi i comandi sono inclusi a scopo di test.
2. Aggiungere SSH utilizzando i seguenti comandi:
   ```
   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. Eseguire il comando **show ca mypubkey rsa** in modalità di configurazione.

```
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. Provare a usare una connessione Telnet dalla stazione Solaris:

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

Nota: "cisco" è il nome utente sul server RADIUS/TACACS+ e la destinazione è 172.18.124.157.

Configurazione del protocollo SSH locale (senza autenticazione AAA)

Èanche possibile configurare una connessione SSH al PIX con l'autenticazione locale e senza server AAA. Non sono tuttavia disponibili nomi utente distinti per utente. Il nome utente è sempre "pix".

Utilizzare questi comandi per configurare il protocollo SSH locale sul 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
```

Poiché il nome utente predefinito in questa disposizione è sempre "pix", il comando per connettersi al PIX (3DES da una finestra di Solaris) è:

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

Debug SSH

Debug senza il comando debug ssh - 3DES e cifratura 512

```
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
```

Eseguire il debug con il 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"
```

Debug - cifratura 3DES e 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"
```

Debug - DES e cifratura 1024

Nota: questo output viene generato da un PC con SSH, non da 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"
```

Debug - cifratura 3DES e 2048

Nota: questo output viene generato da un PC con SSH, non da 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"
```

Problemi che possono verificarsi

Solaris debug - cifratura 2048 e Solaris SSH

Nota: Solaris non è in grado di gestire la cifratura 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).
```

Password o nome utente non valido sul server 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
```

Utente non autorizzato tramite il comando:

interno ssh 172.18.124.114.255.255.255.255

Tentativi di connessione:

315001: Sessione SSH negata da 161.44.17.151 sull'interfaccia interna

Con chiave rimossa da PIX (con il comando **ca zero rsa**) o non salvata con il 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)
```

Server AAA inattivo:

```
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
```

Il client è impostato per 3DES ma in PIX è presente solo la chiave DES:

Nota: Solaris non supporta 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 sulla CLI di Solaris:

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

Come rimuovere la chiave RSA da PIX

rsa ca zero

Come salvare la chiave RSA in PIX

può salvare tutto

Come consentire il protocollo SSH dall'esterno del client SSH

ssh_ip esterno *255.255.255.255* all'esterno

Abilita autenticazione

Con il comando:

topix console abilitazione autenticazione aaa

(dove *topix* è il nostro elenco di server), viene richiesto all'utente di immettere un nome utente e una password da inviare al server TACACS o RADIUS. Poiché il pacchetto di autenticazione per enable è lo stesso del pacchetto di autenticazione per login, se l'utente può accedere al PIX con TACACS o RADIUS, lo può abilitare tramite TACACS o RADIUS con lo stesso nome utente/password.

Per ulteriori informazioni su questi problemi, consultare l'ID bug Cisco CSCdm47044 (solo utenti registrati).

Informazioni sul syslog

Mentre l'accounting AAA è valido solo per le connessioni attraverso il PIX, non al PIX, se il syslog è configurato, le informazioni sull'operazione eseguita dall'utente autenticato vengono inviate al server syslog (e al server di gestione della rete, se configurato, tramite il MIB syslog).

Se syslog è impostato, messaggi come questi vengono visualizzati sul server syslog:

Livello di notifica registrazione trap:

```
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.
```

Livello informativo registrazione trap (che include il livello di notifica):

307002: Sessione di accesso Telnet consentita da 10.31.1.40

Ottenere l'accesso quando il server AAA è inattivo

Se il server AAA non è attivo, è possibile immettere la password Telnet per accedere inizialmente al PIX, quindi al **pix** per il nome utente e infine alla password enable (**enable password, *a prescindere dalla password***) per la password. Se si **abilita la password** a *prescindere da quale* sia la configurazione PIX, immettere **pix** come nome utente e premere **Invio**. Se la password di abilitazione è impostata ma non è nota, è necessario un disco di recupero della password per reimpostarla.

Informazioni da raccogliere se si apre una richiesta TAC

Se dopo aver eseguito le procedure di risoluzione dei problemi sopra descritte si desidera continuare a ricevere

assistenza e si desidera aprire una richiesta con Cisco TAC, includere le seguenti informazioni.
• Descrizione del problema e dettagli sulla topologia • Risoluzione dei problemi eseguita prima dell'apertura della richiesta • Output del comando **show tech-support** • Output del comando **show log** dopo l'esecuzione con il comando **logging buffered debugging** o acquisizioni della console che dimostrano il problema (se disponibili) Allegare i dati raccolti alla richiesta in formato testo normale non compresso (txt). È possibile allegare informazioni alla richiesta caricandola tramite lo strumento Case Query Tool (solo clienti registrati). Se non è possibile accedere allo strumento Case Query, inviare le informazioni in un allegato e-mail a attach@cisco.com con il numero della richiesta in oggetto.

Informazioni correlate

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- PIX RAGGIO TACACS+