PIX 6.x Esempio di configurazione semplice del tunnel VPN da PIX a PIX

Sommario

Introduzione

Questa configurazione consente a due Cisco Secure PIX Firewall di eseguire un tunnel VPN (Virtual Private Network) semplice da PIX a PIX su Internet o su qualsiasi rete pubblica che utilizzi la protezione IP (IPSec). IPSec è una combinazione di standard aperti che fornisce riservatezza, integrità e autenticazione dell'origine dei dati tra peer IPSec.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA 7.x: Esempio di configurazione semplice del tunnel VPN da PIX a PIX per ulteriori informazioni sullo stesso scenario in cui l'appliance di sicurezza Cisco esegue la versione software 7.x.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- Cisco Secure PIX 515E Firewall con software versione 6.3(5)
- Cisco Secure PIX 515E Firewall con software versione 6.3(5)

Convenzioni

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

Premesse

La negoziazione IPSec può essere suddivisa in cinque fasi, incluse due fasi IKE (Internet Key Exchange).

1. Un tunnel IPSec viene avviato da traffico interessante. Il traffico è considerato interessante quando viene effettuato tra peer IPSec.
2. Nella fase 1 di IKE, i peer IPSec negoziano il criterio SA (Security Association) IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando Internet Security Association and Key Management Protocol (ISAKMP).
3. Nella fase 2 di IKE, i peer IPSec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni della SA IPSec. La negoziazione del criterio condiviso determina la modalità di definizione del tunnel IPSec.
4. Il tunnel IPSec viene creato e i dati vengono trasferiti tra i peer IPSec in base ai parametri IPSec configurati nei set di trasformazioni IPSec.
5. Il tunnel IPSec termina quando le associazioni di protezione IPSec vengono eliminate o alla scadenza della relativa durata.

Nota: la negoziazione IPSec tra i due PIX non riesce se le associazioni di protezione su entrambe le fasi IKE non corrispondono sui peer.

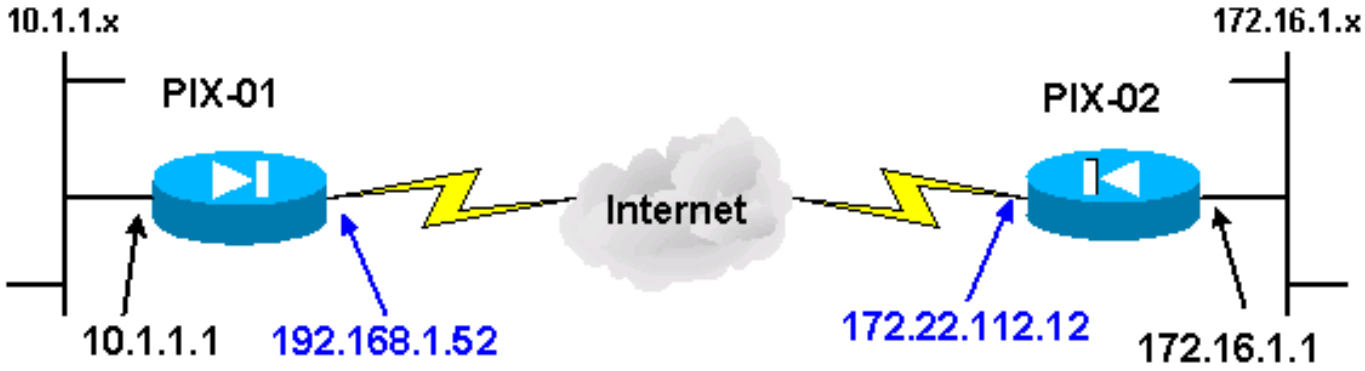
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usato questo diagramma di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Questi sono indirizzi RFC 1918 usati in un ambiente lab.

Configurazione IKE e IPSec

La configurazione IPSec di ogni PIX varia solo quando si inseriscono le informazioni peer e la convenzione di denominazione scelta per le mappe crittografiche e i set di trasformazioni. La configurazione può essere verificata con il terminale **write** o con i comandi **show**. I comandi appropriati sono show isakmp, **show isakmp policy**, **show access-list**, **show crypto IPSec transform-set** e **show crypto map**. Per ulteriori informazioni su questi comandi, consultare i riferimenti ai comandi di Cisco Secure PIX Firewall.

Per configurare IPSec, completare la procedura seguente:

1. Configura IKE per chiavi già condivise
2. Configurare IPSec
3. Configurazione di NAT (Network Address Translation)
4. Configurazione delle opzioni di sistema PIX

Configura IKE per chiavi già condivise

Per abilitare il protocollo IKE sulle interfacce terminali IPSec, usare il comando **isakmp enable**. In questo scenario, l'interfaccia esterna è l'interfaccia terminale IPSec su entrambi i PIX. IKE è configurato su entrambi i PIX. Questi comandi mostrano solo PIX-01.

```
isakmp enable outside
```

Èinoltre necessario definire i criteri IKE utilizzati durante le negoziazioni IKE. A tale scopo, eseguire il comando **isakmp policy**. Quando si esegue questo comando, è necessario assegnare un livello di priorità in modo che i criteri vengano identificati in modo univoco. In questo caso, al criterio viene assegnata la priorità massima 1. Il criterio è inoltre impostato per utilizzare una chiave già condivisa, un algoritmo di hashing MD5 per l'autenticazione dei dati, un DES per Encapsulating Security Payload (ESP) e un gruppo Diffie-Hellman1. Il criterio è inoltre impostato per utilizzare la durata SA.

```
isakmp policy 1 authentication pre-share
```

```
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

La configurazione IKE può essere verificata con il comando **show isakmp policy**:

```
PIX-01#show isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 1000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

Infine, usare il comando **isakmp key** per configurare la chiave già condivisa e assegnare un indirizzo peer. Quando si utilizzano chiavi già condivise, è necessario che la stessa chiave già condivisa corrisponda nei peer IPSec. L'indirizzo è diverso e dipende dall'indirizzo IP del peer remoto.

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

Il criterio può essere verificato con il comando **write terminal** o **show isakmp**:

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

Configurare IPSec

IPSec viene avviato quando uno dei PIX riceve il traffico destinato all'altro PIX all'interno della rete. Questo traffico è ritenuto interessante e deve essere protetto con IPSec. L'elenco degli accessi viene utilizzato per determinare il traffico che avvia le negoziazioni IKE e IPSec. Questo elenco degli accessi consente di inviare il traffico dalla rete 10.1.1.x alla rete 172.16.1.x tramite il tunnel IPSec. L'elenco degli accessi nella configurazione PIX opposta rispecchia tale elenco. Ciò è appropriato per PIX-01.

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

Il set di trasformazioni IPSec definisce il criterio di protezione utilizzato dai peer per proteggere il flusso di dati. La trasformazione IPSec viene definita utilizzando il comando **crypto IPSec**

transform-set. È necessario scegliere un nome univoco per l'impostazione di trasformazione ed è possibile selezionare fino a tre trasformazioni per definire i protocolli di protezione IPSec. Questa configurazione utilizza solo due trasformazioni: **esp-hmac-md5** e **esp-des**.

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

Le mappe crittografiche configurano le associazioni di protezione IPSec per il traffico crittografato. Per creare una mappa crittografica, è necessario assegnare un nome e un numero di sequenza alla mappa. Quindi, vengono definiti i parametri della mappa crittografica. Il trasferimento della mappa crittografica visualizzato utilizza IKE per stabilire le associazioni di protezione IPSec, crittografa tutti gli elementi che corrispondono all'access-list 101, ha un peer impostato e utilizza **chevelle** transform-set per applicare i criteri di protezione per il traffico.

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

Dopo aver definito la mappa crittografica, applicarla a un'interfaccia. L'interfaccia scelta deve essere l'interfaccia di terminazione IPSec.

```
crypto map transam interface outside
```

Utilizzare il comando **show crypto map** per verificare gli attributi della mappa crittografica.

```
PIX-01#show crypto map

Crypto Map: "transam" interfaces: { outside }

Crypto Map "transam" 1 IPSec-isakmp
Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
Current peer: 172.22.112.12
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ chevelle, }
```

Configurazione NAT

Questo comando indica al PIX di non inviare a NAT alcun traffico ritenuto interessante per IPSec. Pertanto, tutto il traffico che corrisponde alle istruzioni del comando **access-list** è esente dai servizi NAT.

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0
nat (inside) 0 access-list NoNAT
```

Configurazione delle opzioni di sistema PIX

Poiché tutte le sessioni in entrata devono essere consentite in modo esplicito da un elenco degli accessi o da un canale, il comando **sysopt connection allow-IPSec** viene utilizzato per consentire tutte le sessioni di crittografia autenticate IPSec in entrata. Con il traffico IPSec protetto, il controllo del canale secondario può essere ridondante e causare il mancato completamento della creazione del tunnel. Il comando **sysopt** ottimizza diverse funzioni di sicurezza e configurazione del firewall PIX.

```
sysopt connection permit-IPSec
```

Configurazioni

se il dispositivo Cisco restituisce i risultati di un comando **write terminal**, è possibile usare Output Interpreter (solo utenti registrati) per visualizzare i potenziali errori e correggerli. Per utilizzare Output Interpreter (solo utenti registrati) è necessario aver eseguito l'accesso e avere JavaScript abilitato.

PIX-01 at 192.68.1.52

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-01
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
```

```
!--- Sets the outside address on the PIX Firewall. ip
address outside 192.168.1.52 255.255.255.0
!--- Sets the inside address on the PIX Firewall. ip
address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2: !--- The IPSec transform-set
"chevelle" uses esp-md5-hmac to provide !--- data
authentication.

crypto IPSec transform-set chevelle esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map transam 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 172.22.112.12.
crypto map transam 1 match address 101
!--- Sets the IPSec peer. crypto map transam 1 set peer
172.22.112.12
!--- Sets the IPSec transform set "chevelle" !--- to be
used with the crypto map entry "transam". crypto map
transam 1 set transform-set chevelle
!--- Assigns the crypto map transam to the interface.
crypto map transam interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate the IPSec tunnel

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the pre-shared key between the IPSec peers. !--- The
```

```
same preshared key must be configured on the !--- IPSec
peers for IKE authentication. isakmp key ********
address 172.22.112.12 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the
differences in !--- the default and configured policy.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX-02 at 172.22.12.12

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 172.22.112.12 255.255.255.0
```

```
!--- Sets the inside address on the PIX Firewall. ip
address inside 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2:  !--- The IPSec transform set defines
the negotiated security policy !--- that the peers use
to protect the data flow. !--- The IPSec transform-set
"toyota" uses hmac-md5 authentication header !--- and
encapsulates the payload with des.

crypto IPSec transform-set toyota esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map bmw 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 192.168.1.52.
crypto map bmw 1 match address 101
!--- Sets IPSec peer. crypto map bmw 1 set peer
192.168.1.52
!--- Sets the IPSec transform set "toyota" !--- to be
used with the crypto map entry "bmw". crypto map bmw 1
set transform-set toyota
!--- Assigns the crypto map bmw to the interface. crypto
map bmw interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate IPSec tunnel.

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the preshared key between the IPSec peers. !--- The same
```

```
preshared key must be configured on the !--- IPSec peers
for IKE authentication. isakmp key ******** address
192.168.1.52 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Alcuni comandi **show sono supportati dallo** strumento Output Interpreter (solo utenti registrati); lo strumento permette di visualizzare un'analisi dell'output del comando show.

- **show crypto IPSec sa**: questo comando visualizza lo stato corrente delle associazioni di protezione IPSec ed è utile per determinare se il traffico viene crittografato.
- **show crypto isakmp sa**: questo comando visualizza lo stato corrente delle associazioni di protezione IKE.

PIX-01 show Commands

PIX-01 show Commands

```
PIX-01#show crypto IPSec sa
interface: outside
Crypto map tag: transam, local addr. 192.168.1.52

local ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
current_peer: 172.22.112.12
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are being sent
!--- and received without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0
#send errors 2, #recv errors 0
```

```
local crypto endpt.: 192.168.1.52, remote crypto endpt.:
172.22.112.12
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 6f09cbf1
!--- Shows inbound SAs that are established. inbound esp
sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:
!--- Shows outbound SAs that are established. outbound
ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-01#show
crypto isakmp sa
     dst             src           state      pending
created
172.22.112.12    192.168.1.52    QM_IDLE         0
1Maui-PIX-01#
```

PIX-02 show Commands

PIX-02 show Commands

```
PIX-02#show crypto IPSec sa

interface: outside
Crypto map tag: bmw, local addr. 172.22.112.12

local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.52
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are !--- being
sent and recede without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
```

```
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts
decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.22.112.12, remote crypto
endpt.: 192.168.1.52
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 70be0c04
!--- Shows inbound SAs that are established. Inbound ESP
sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:
!--- Shows outbound SAs that are established. Outbound
ESP sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-02#show
crypto isakmp sa
     dst             src          state      pending
created
172.22.112.12    192.168.1.52    QM_IDLE          0
PIX-02#
```

Non è possibile eseguire il ping dell'interfaccia interna del PIX per la formazione del tunnel a meno che il comando management-access non sia configurato in modalità di configurazione globale.

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Nota: i comandi **clear** devono essere eseguiti in modalità di configurazione.

- **clear crypto IPSec sa**: questo comando reimposta le associazioni di protezione IPSec dopo tentativi non riusciti di negoziare un tunnel VPN.
- **clear crypto isakmp sa**: questo comando reimposta le associazioni di sicurezza ISAKMP dopo i tentativi non riusciti di negoziare un tunnel VPN.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto IPSec**: questo comando mostra se un client sta negoziando la parte IPSec della connessione VPN.
- **debug crypto isakmp**: questo comando mostra se i peer stanno negoziando la parte ISAKMP della connessione VPN.

Una volta completata la connessione, è possibile verificarla utilizzando i comandi **show**.

Informazioni correlate

- Pagina di supporto PIX
- Informazioni di riferimento sui comandi PIX
- RFC (Request for Comments)
- Negoziazione IPSec/pagina di supporto del protocollo IKE
- Documentazione e supporto tecnico – Cisco Systems