# Esempio di configurazione di VPN tra i prodotti Sonicwall e Cisco Security Appliance

## Sommario



## Introduzione

In questo documento viene illustrato come configurare un tunnel IPsec con chiavi già condivise per comunicare tra due reti private utilizzando sia la modalità aggressiva che la modalità principale. Nell'esempio, le reti in comunicazione sono la rete privata 192.168.1.x all'interno di Cisco Security Appliance (PIX/ASA) e la rete privata 172.22.1.x all'interno di SonicwallTM TZ170 Firewall.

## Prerequisiti

### Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Prima di avviare la configurazione, il traffico tra Cisco Security Appliance e Sonicwall TZ170 deve passare a Internet (rappresentato qui dalle reti 10.x.x.x).
- Gli utenti devono avere familiarità con la negoziazione IPSec. Questo processo può essere suddiviso in cinque fasi, incluse due fasi di IKE (Internet Key Exchange).Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.Nella fase 1 di IKE, i peer IPsec negoziano il criterio di associazione di sicurezza (SA) IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando

Internet Security Association and Key Management Protocol (ISAKMP).In IKE fase 2, i peer IPsec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni di associazione di sicurezza IPsec. La negoziazione del criterio condiviso determina la modalità di definizione del tunnel IPSec.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.Il tunnel IPsec termina quando le associazioni di protezione IPsec vengono eliminate o quando scade la loro durata.

### Componenti usati

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

- Cisco PIX 515E versione 6.3(5)
- Cisco PIX 515 versione 7.0(2)
- Sonicwall TZ170, SonicOS Standard 2.2.0.1

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.

### Prodotti correlati

Questa configurazione può essere utilizzata anche con le seguenti versioni hardware e software:

- La configurazione PIX 6.3(5) può essere utilizzata con tutti gli altri prodotti Cisco PIX firewall che eseguono tale versione del software (PIX 501, 506 e così via)
- La configurazione PIX/ASA 7.0(2) può essere utilizzata solo su dispositivi con il gruppo di software PIX 7.0 (ad eccezione degli switch 501, 506 e probabilmente alcuni degli switch 515 meno recenti) e su ASA Cisco serie 5500.

### Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

## Configurazione

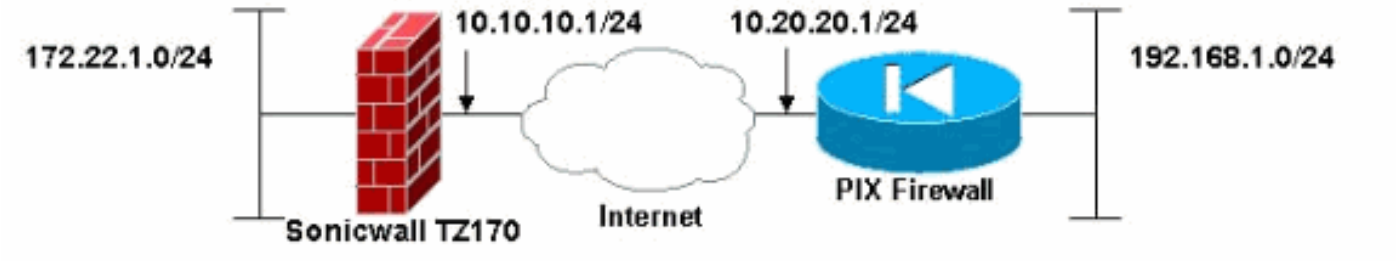
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

**Nota:** in modalità IPSec Accective, è necessario che Sonicwall avvii il tunnel IPSec verso il PIX. Ciò si verifica quando si analizzano i debug per questa configurazione. Questa condizione è inerente al funzionamento della modalità aggressiva di IPSec.

### Esempio di rete

Nel documento viene usata questa impostazione di rete:

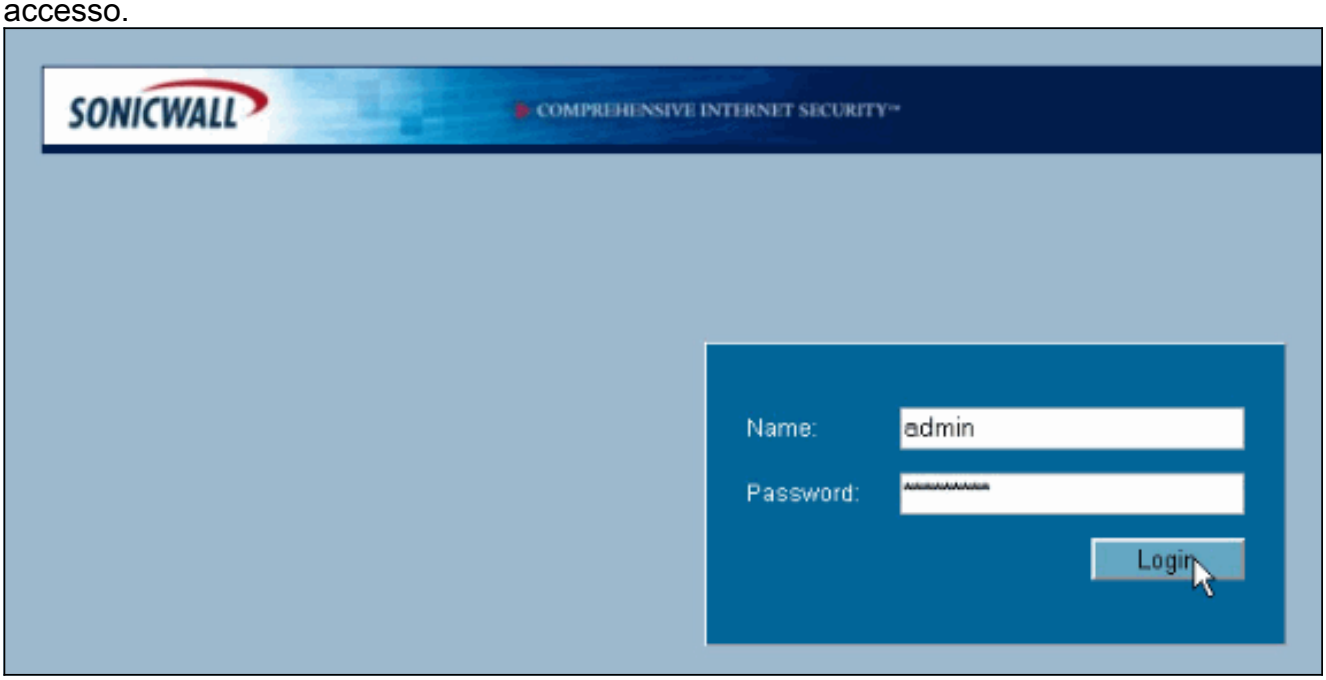



## Configurazione di Sonicwall

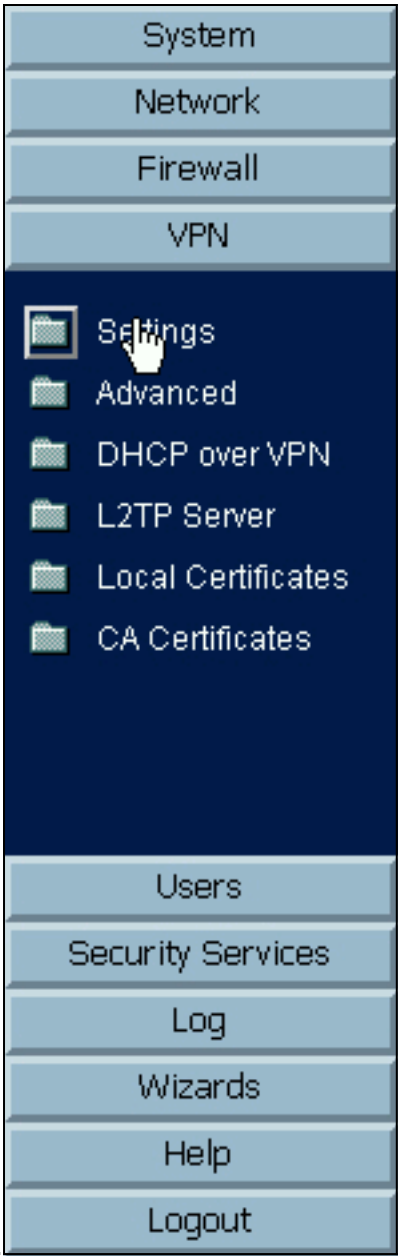
La configurazione di Sonicwall TZ170 viene effettuata attraverso un'interfaccia basata su web.

Attenersi alla seguente procedura:

1. Connettersi all'indirizzo IP del router su una delle interfacce interne utilizzando un browser Web standard.Verrà visualizzata la finestra di accesso.

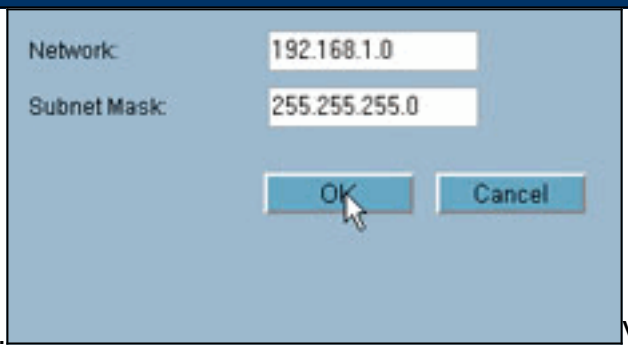



2. Accedere al dispositivo Sonicwall e selezionare **VPN >**

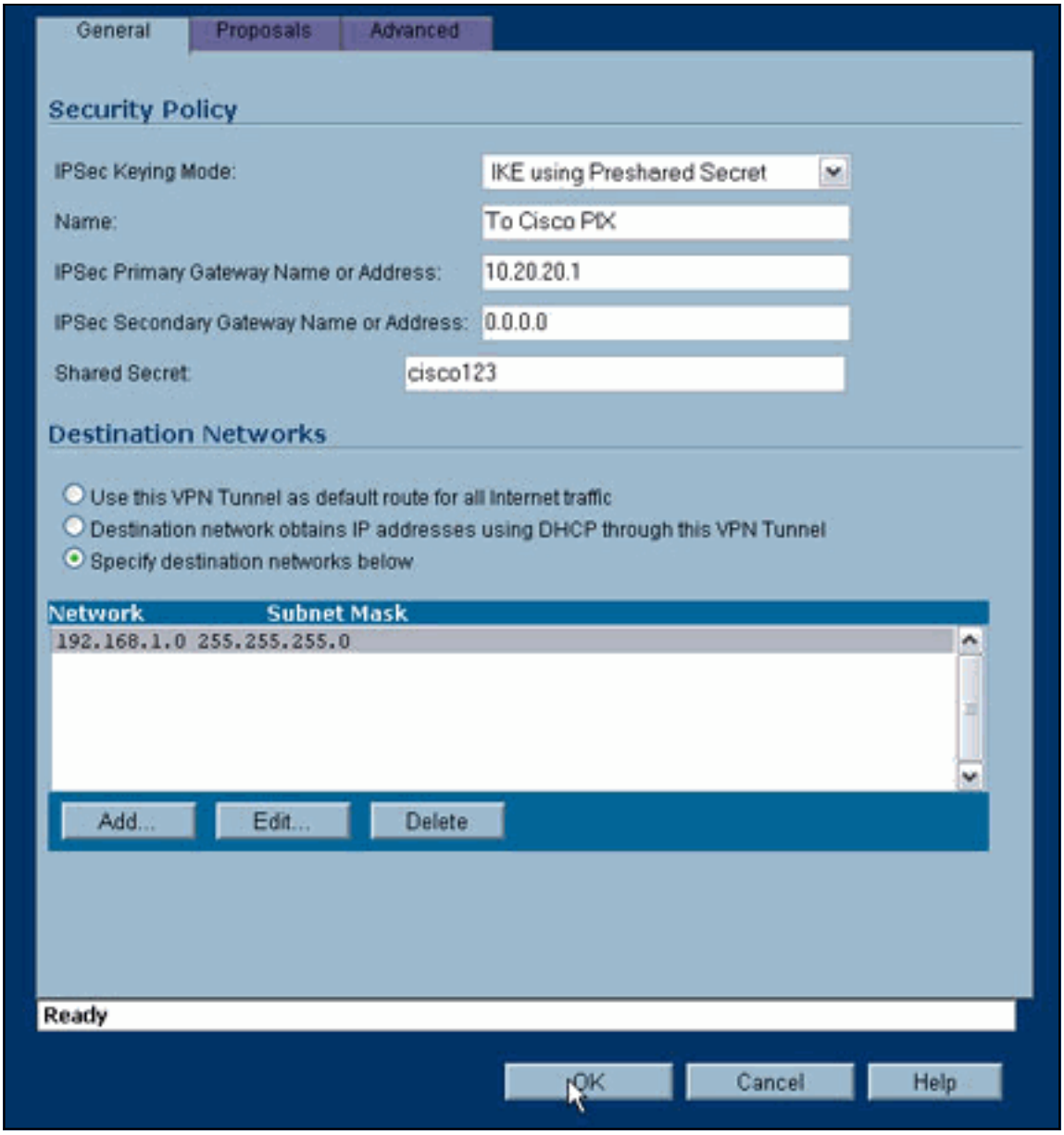



**Impostazioni**.

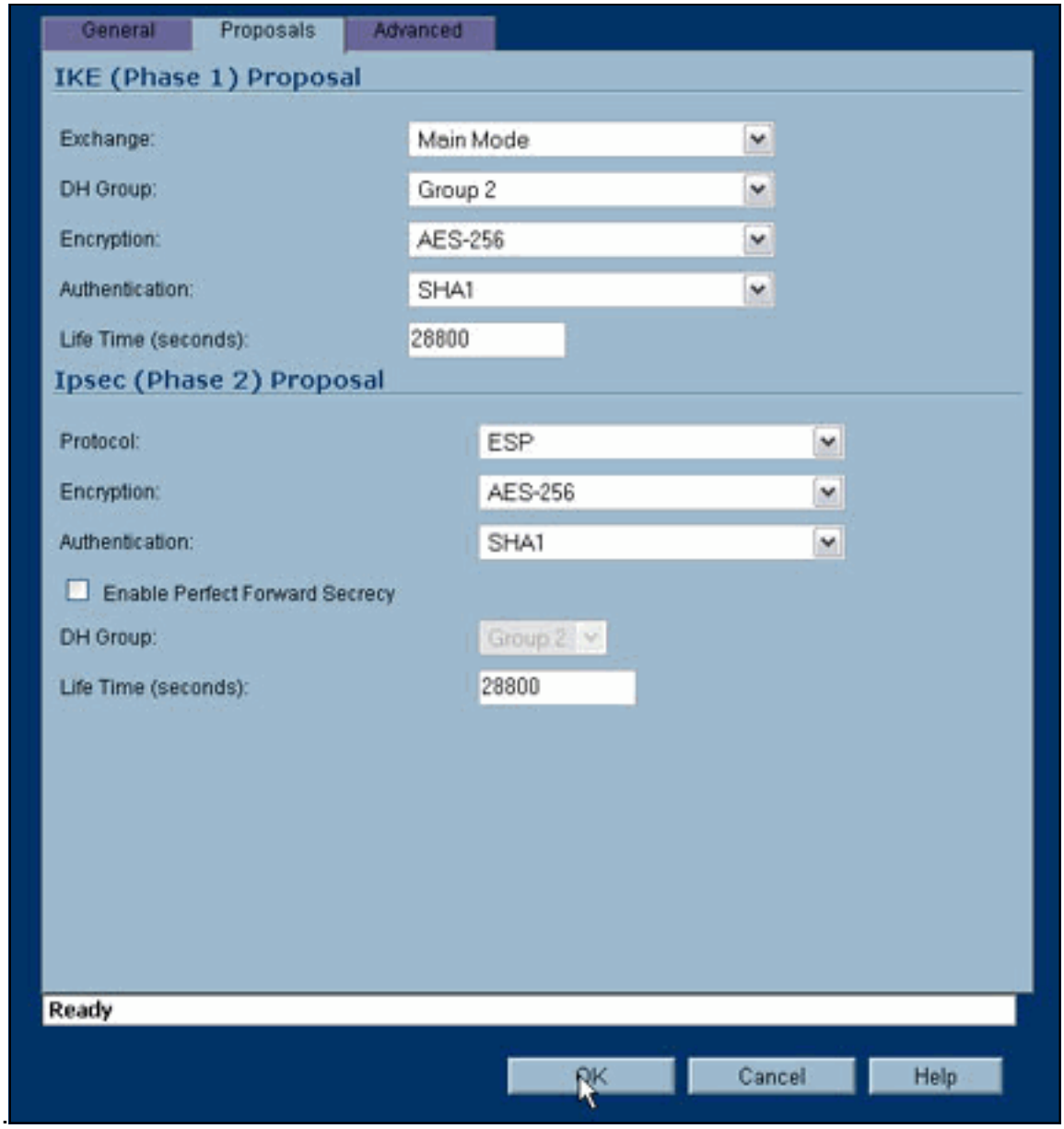
3. Immettere l'indirizzo IP del peer VPN e il segreto già condiviso che verrà utilizzato. Fare clic su **Add** (Aggiungi) in Destination Networks (Reti di destinazione).


4. Immettere la rete di destinazione. Viene visualizzata la finestra Settings (Impostazioni).

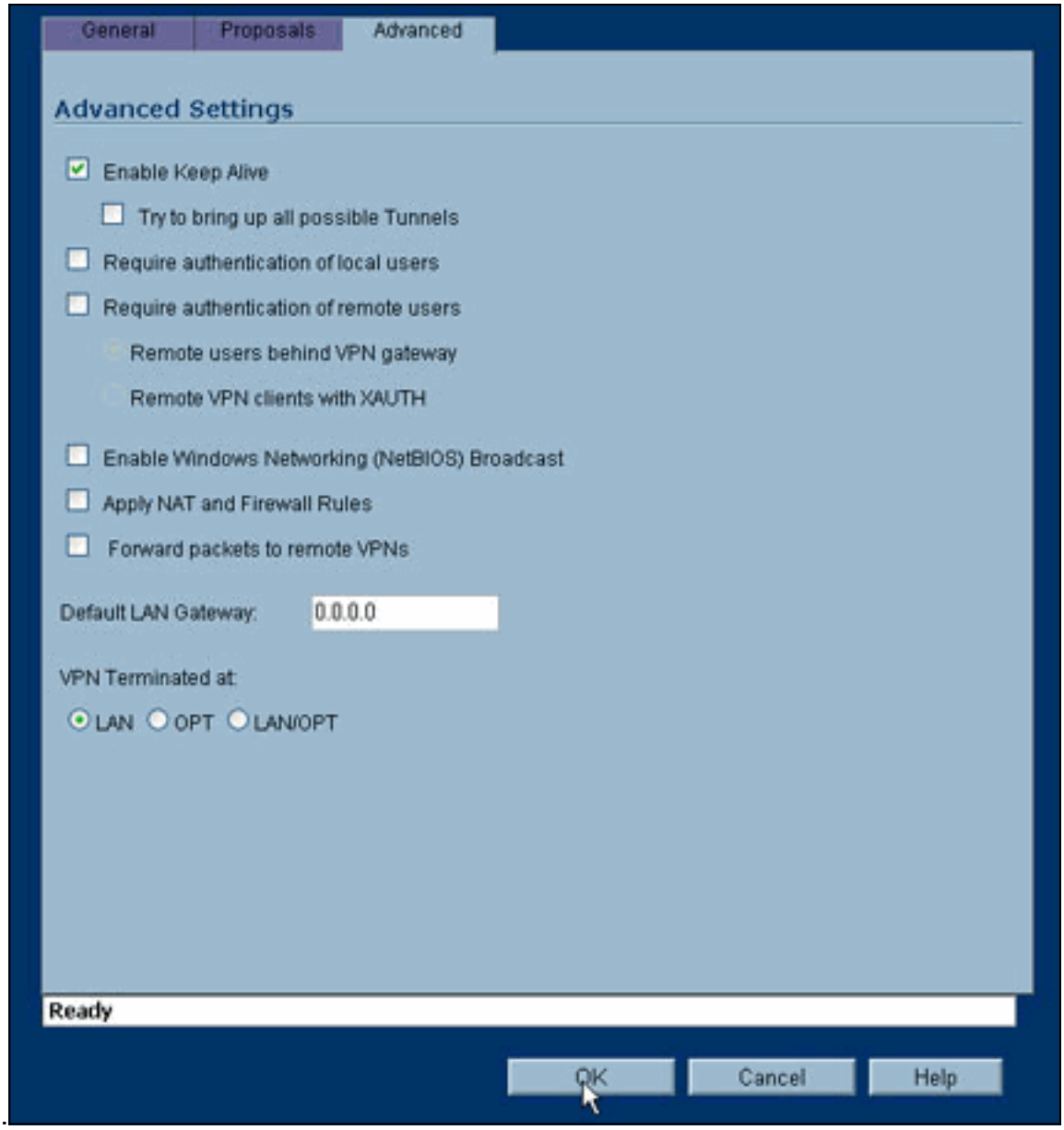



5. Fare clic sulla scheda Proposte nella parte superiore della finestra Impostazioni.
6. Selezionare lo scambio che si intende utilizzare per questa configurazione (modalità principale o modalità aggressiva) insieme alle altre impostazioni di Fase 1 e Fase 2.In questa configurazione di esempio viene utilizzata la crittografia AES-256 per entrambe le fasi con l'algoritmo hash SHA1 per l'autenticazione e il gruppo Diffie-Hellman 2 a 1024 bit per i criteri



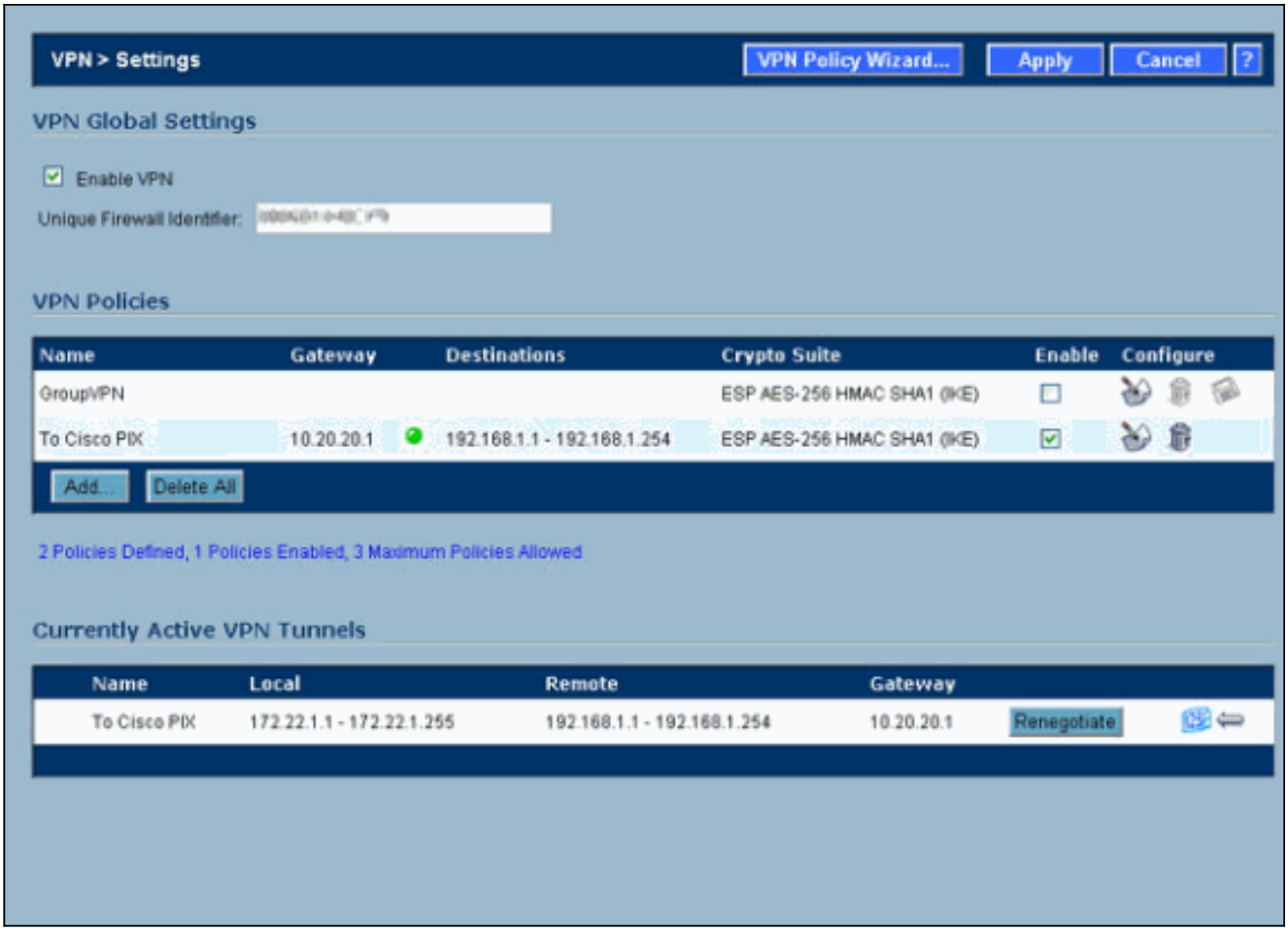

IKE.

7. Fare clic sulla scheda Avanzate.In questa scheda è possibile configurare altre opzioni. Impostazioni utilizzate per la configurazione di



esempio.

8. Fare clic su **OK**.Una volta completata questa configurazione e la configurazione sul PIX remoto, la finestra Settings (Impostazioni) dovrebbe essere simile a quella di esempio.




## Configurazione modalità principale IPSec

Questa sezione utilizza le seguenti configurazioni:

- Cisco PIX 515e versione 6.3(5)
- Cisco PIX 515 versione 7.0(2)

**Cisco PIX 515e versione 6.3(5)**

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
```

```
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION: !--- Defines the transform set
for Phase 2 encryption and authentication. !---
Austinlab is the name of the transform set that uses
aes-256 encryption !--- as well as the SHA1 hash
algorithm for authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies IKE is used to establish the IPsec SAs
for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
map . crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map. crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Specifies the interface
to use for the IPsec tunnel.

isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used with the preshared key cisco123. isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

## Cisco PIX 515 versione 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS®. !--- This output configures the IP
address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies the ACL pixtosw to use with this map.
crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Defines how the PIX
```

```
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration !--- settings specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

## Configurazione modalità aggressiva IPsec

Questa sezione utilizza le seguenti configurazioni:

- Cisco PIX 515e versione 6.3(5)
- Cisco PIX 515 versione 7.0(2)

### Cisco PIX 515e versione 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
```

```
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 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 !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
the name of the transform set that uses aes-256
encryption !--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map ciscopix for the transform
set. crypto dynamic-map ciscopix 1 set transform-set
austinlab !--- Specifies the IKE that should be used to
establish SAs !--- for the dynamic map. crypto map
dynmaptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
the settings above to the outside interface. crypto map
dynmaptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
.
isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used as the preshared key "cisco123". isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

## Cisco PIX 515 versione 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS. !--- This output configures the IP
```

```
address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map "ciscopix" for the defined
transform set. crypto dynamic-map ciscopix 1 set
transform-set austinlab !--- Specifies that IKE should
be used to establish SAs !--- for the defined dynamic
map. crypto map dynmaptosw 66 ipsec-isakmp dynamic
ciscopix !--- Applies the settings to the outside
interface. crypto map dynmaptosw interface outside !---
PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
```

```
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

# Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show crypto isakmp sa**: visualizza tutte le SA IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di protezione correnti.

Queste tabelle mostrano gli output di alcuni debug per la modalità principale e aggressiva sia in PIX 6.3(5) che in PIX 7.0(2) dopo che il tunnel è stato completamente stabilito.

**Nota:** queste informazioni sono sufficienti per stabilire un tunnel IPsec tra questi due tipi di hardware. Per inviare commenti, utilizzare il modulo sul lato sinistro del documento.

- Cisco PIX 515e versione 6.3(5) - Modalità principale
- Cisco PIX 515 versione 7.0(2)- Modalità principale
- Cisco PIX 515e versione 6.3(5) - Modalità aggressiva
- Cisco PIX 515 versione 7.0(2) - Modalità aggressiva

**Cisco PIX 515e versione 6.3(5) - Modalità principale**

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.10.10.1       10.20.20.1    QM_IDLE         0
1
pix515e-635#



pix515e-635#show crypto ipsec sa


           interface: outside
           Crypto map tag: maptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={origin_is_acl,}
```

```
           #pkts encaps: 4, #pkts encrypt: 4, #pkts
digest 4
           #pkts decaps: 4, #pkts decrypt: 4, #pkts
verify 4
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
           #send errors 1, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
           path mtu 1500, ipsec overhead 72, media mtu
1500
           current outbound spi: ed0afa33

 inbound esp sas:
           spi: 0xac624692(2892121746)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 1, crypto map: maptosw
           sa timing: remaining key lifetime (k/sec):
(4607999/28718)
           IV size: 16 bytes
           replay detection support: Y


           inbound ah sas:


           inbound pcp sas:


           outbound esp sas:
           spi: 0xed0afa33(3976919603)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 2, crypto map: maptosw
           sa timing: remaining key lifetime (k/sec):
(4607999/28718)
           IV size: 16 bytes
           replay detection support: Y


           outbound ah sas:


           outbound pcp sas:

pix515e-635#
```

## Cisco PIX 515 versione 7.0(2)- Modalità principale

```
pix515-702#show crypto isakmp sa

 Active SA: 1
           Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
           Total IKE SA: 1

1 IKE Peer: 10.10.10.1
           Type : L2L Role : initiator
           Rekey : no State : MM_ACTIVE
           pix515-702#
```

```
pix515-702#show crypto ipsec sa
interface: outside
    Crypto map tag: maptosw, local addr: 10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: 2D006547

 inbound esp sas:
           spi: 0x309F7A33 (815757875)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28739)
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0x2D006547 (755000647)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28737)
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

## Cisco PIX 515e versione 6.3(5) - Modalità aggressiva

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.20.20.1       10.10.10.1    QM_IDLE         0
1

pix515e-635#show crypto ipsec sa



           interface: outside
           Crypto map tag: dynmaptosw, local addr.
10.20.20.1
```

```
 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={}
           #pkts encaps: 0, #pkts encrypt: 0, #pkts
digest 0
           #pkts decaps: 0, #pkts decrypt: 0, #pkts
verify 0
           #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.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
           path mtu 1500, ipsec overhead 72, media mtu
1500
           current outbound spi: efb1149d

 inbound esp sas:
           spi: 0x2ad2c13c(718455100)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 2, crypto map: dynmaptosw
           sa timing: remaining key lifetime (k/sec):
(4608000/28736)
           IV size: 16 bytes
           replay detection support: Y


           inbound ah sas:


           inbound pcp sas:


           outbound esp sas:
           spi: 0xefb1149d(4021359773)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 1, crypto map: dynmaptosw
           sa timing: remaining key lifetime (k/sec):
(4608000/28727)
           IV size: 16 bytes
           replay detection support: Y


           outbound ah sas:


           outbound pcp sas:

pix515e-635#
```

## Cisco PIX 515 versione 7.0(2) - Modalità aggressiva

```
pix515-702#show crypto isakmp sa

 Active SA: 1
           Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
```

```
           Total IKE SA: 1

1 IKE Peer: 10.10.10.1
           Type : L2L Role : responder
           Rekey : no State : AM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
           interface: outside
           Crypto map tag: ciscopix, local addr:
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: D7E2F5FD

 inbound esp sas:
           spi: 0xDCBF6AD3 (3703532243)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28703
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0xD7E2F5FD (3621975549)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28701
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

## Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems