PIX/ASA 7.x e versioni successive: Esempio di configurazione del tunnel VPN da PIX a PIX

Sommario

Introduzione

Questo documento descrive la procedura per configurare i tunnel VPN tra due firewall PIX con Cisco Adaptive Security Device Manager (ASDM). ASDM è uno strumento di configurazione basato su applicazioni progettato per semplificare la configurazione, la configurazione e il monitoraggio del firewall PIX con un'interfaccia utente grafica. I firewall PIX si trovano in due siti diversi.

Tunnel formato tramite IPsec. IPsec è una combinazione di standard aperti che forniscono riservatezza, integrità e autenticazione dell'origine dei dati tra peer IPsec.

Nota: in PIX 7.1 e versioni successive, il comando **syspot connection allow-ipsec** viene modificato in **syspot connection allow-vpn**. Questo comando consente al traffico che entra nell'appliance di sicurezza attraverso un tunnel VPN e viene quindi decriptato, di ignorare gli elenchi degli accessi all'interfaccia. I Criteri di gruppo e gli elenchi degli accessi con autorizzazione per utente sono ancora applicabili al traffico. Per disabilitare questa funzione, usare la forma **no** di questo comando. questo comando non è visibile nella configurazione CLI.

Per ulteriori informazioni, fare riferimento al documento PIX 6.x: Esempio di configurazione

semplice del tunnel VPN da PIX a PIX per ulteriori informazioni sullo stesso scenario in cui Cisco PIX Security Appliance esegue la versione software 6.x.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni in questo documento specificano che questo peer avvia il primo scambio proprietario per determinare il peer appropriato a cui connettersi.

- Cisco PIX serie 500 Security Appliance con versione 7.x e successive
- ASDM versione 5.x.1 e successive

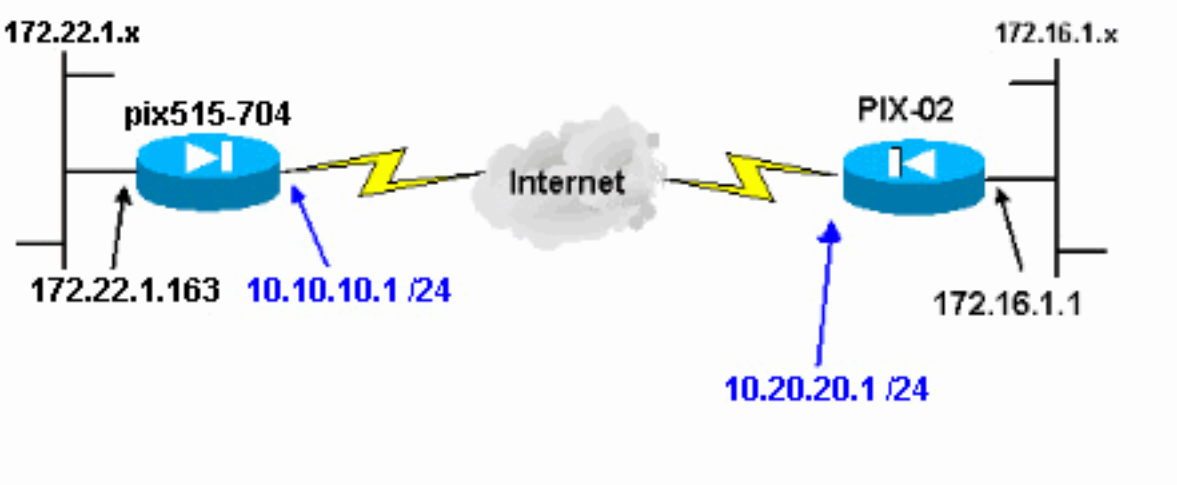
Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

Nota: ASA serie 5500 versione 7.x/8.x esegue lo stesso software mostrato nella versione 7.x/8.x di PIX. Le configurazioni riportate in questo documento sono applicabili a entrambe le linee di prodotti.

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.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

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

Premesse

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

1. Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene 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. 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.
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 quando scade la loro durata.**Nota:** la negoziazione IPSec tra i due PIX non ha esito positivo se le associazioni di protezione su entrambe le fasi IKE non corrispondono sui peer.

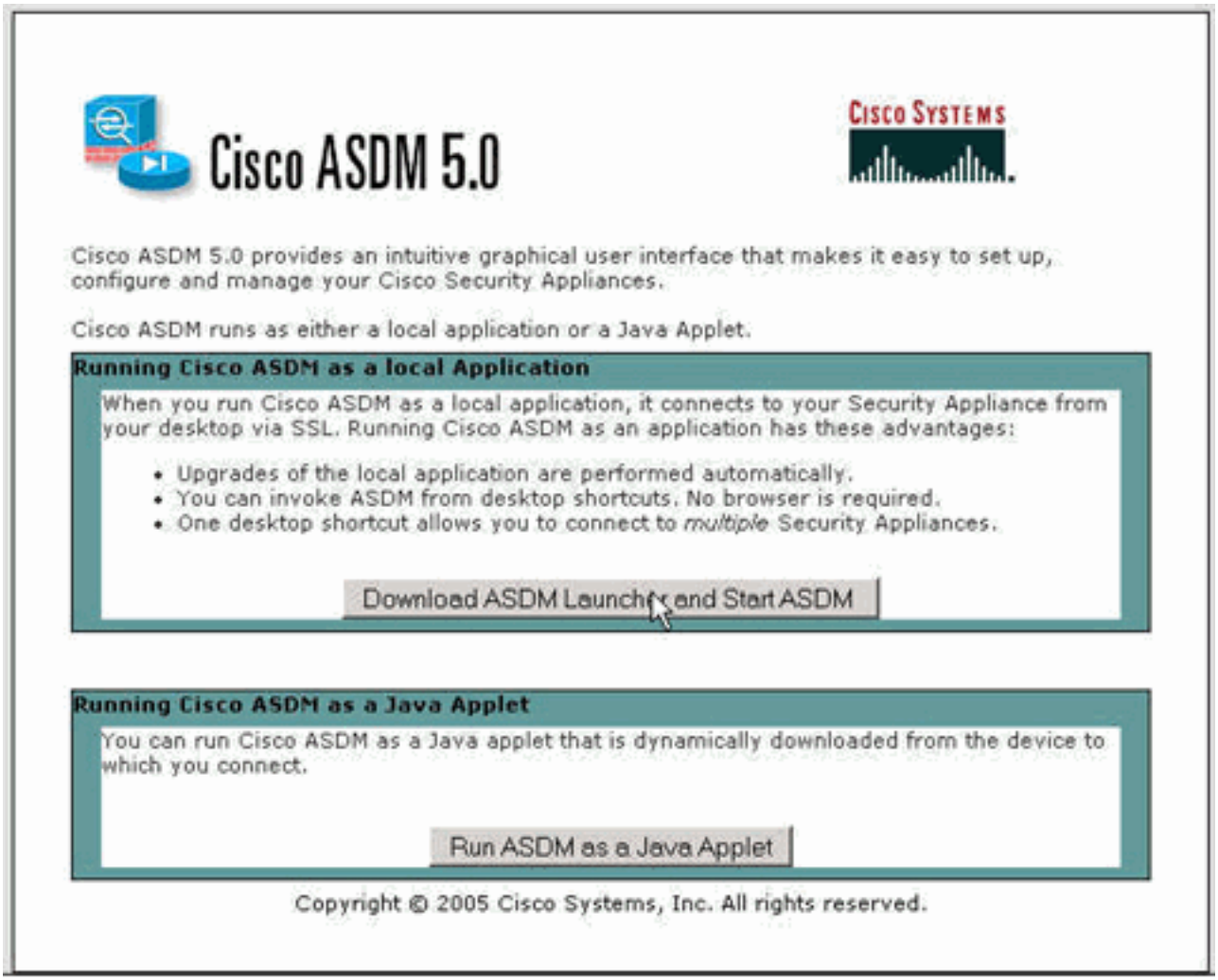
Configurazione

- Configurazione ASDM
- Configurazioni PIX CLI

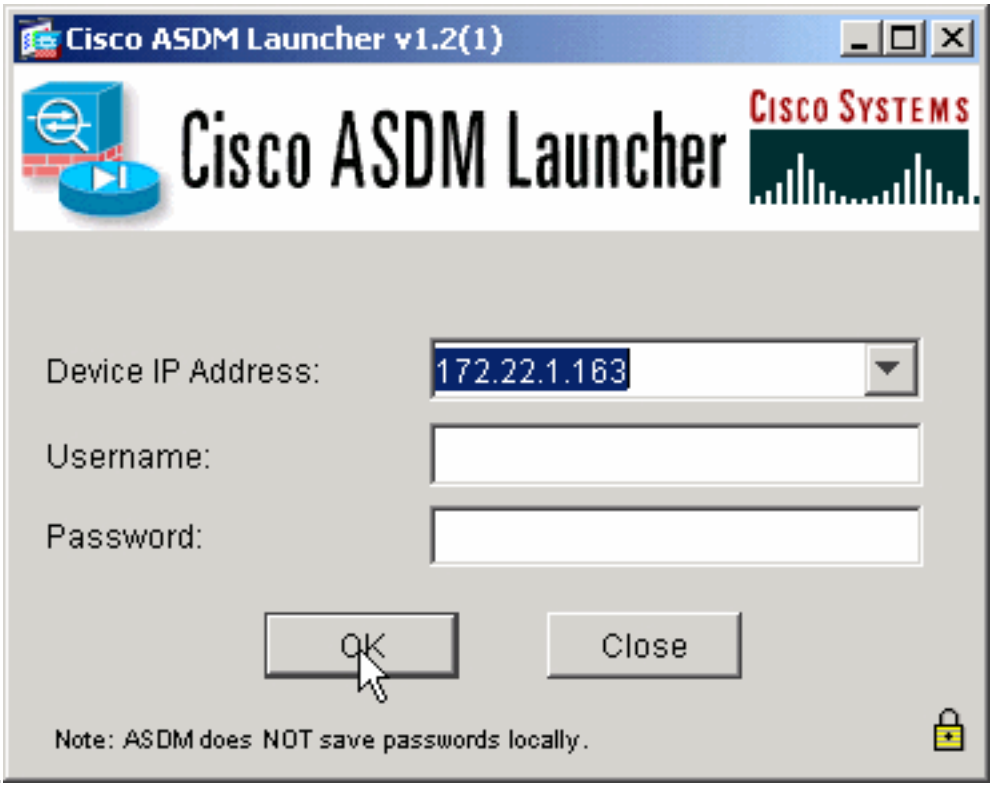
Configurazione ASDM

Attenersi alla seguente procedura:

1. Aprire il browser e digitare **https://<Inside_IP_Address_of_PIX>** per accedere ad ASDM sul PIX.Assicurarsi di autorizzare tutti gli avvisi che il browser visualizza relativi all'autenticità del certificato SSL. Il nome utente e la password predefiniti sono entrambi vuoti.Il PIX visualizza questa finestra per consentire il download dell'applicazione ASDM. In questo esempio l'applicazione viene caricata nel computer locale e non viene eseguita in un'applet Java.

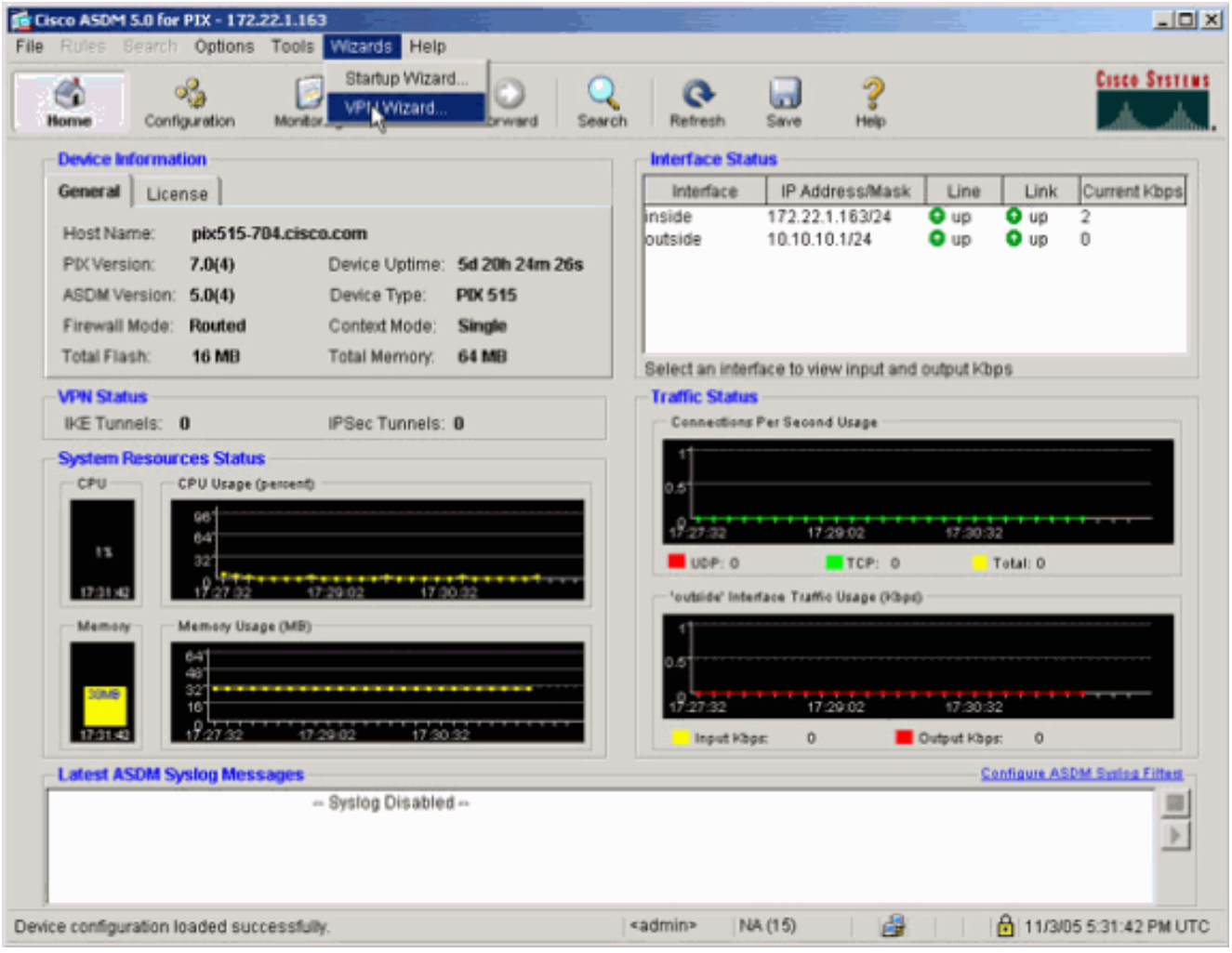


2. Fare clic su **Download ASDM Launcher e Avvia ASDM** per scaricare il programma di installazione dell'applicazione ASDM.
3. Una volta scaricato l'utilità di avvio ASDM, seguire le istruzioni per installare il software ed eseguire l'utilità di avvio Cisco ASDM.
4. Immettere l'indirizzo IP per l'interfaccia configurata con il comando **http -**, nonché un nome utente e una password, se specificati.In questo esempio vengono utilizzati il nome utente e la password vuoti

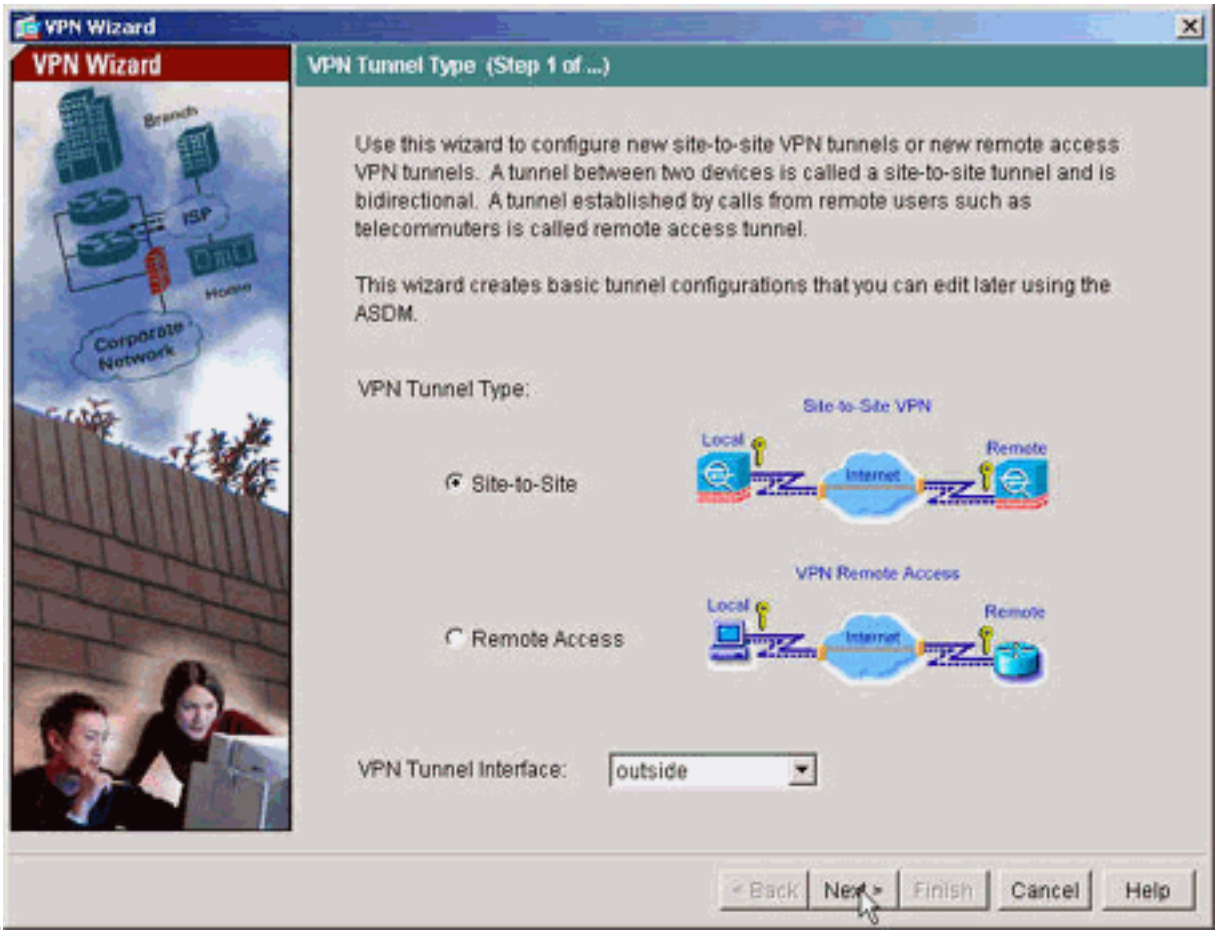


predefiniti.

5. Eseguire la Creazione guidata VPN una volta che l'applicazione ASDM si connette al PIX.

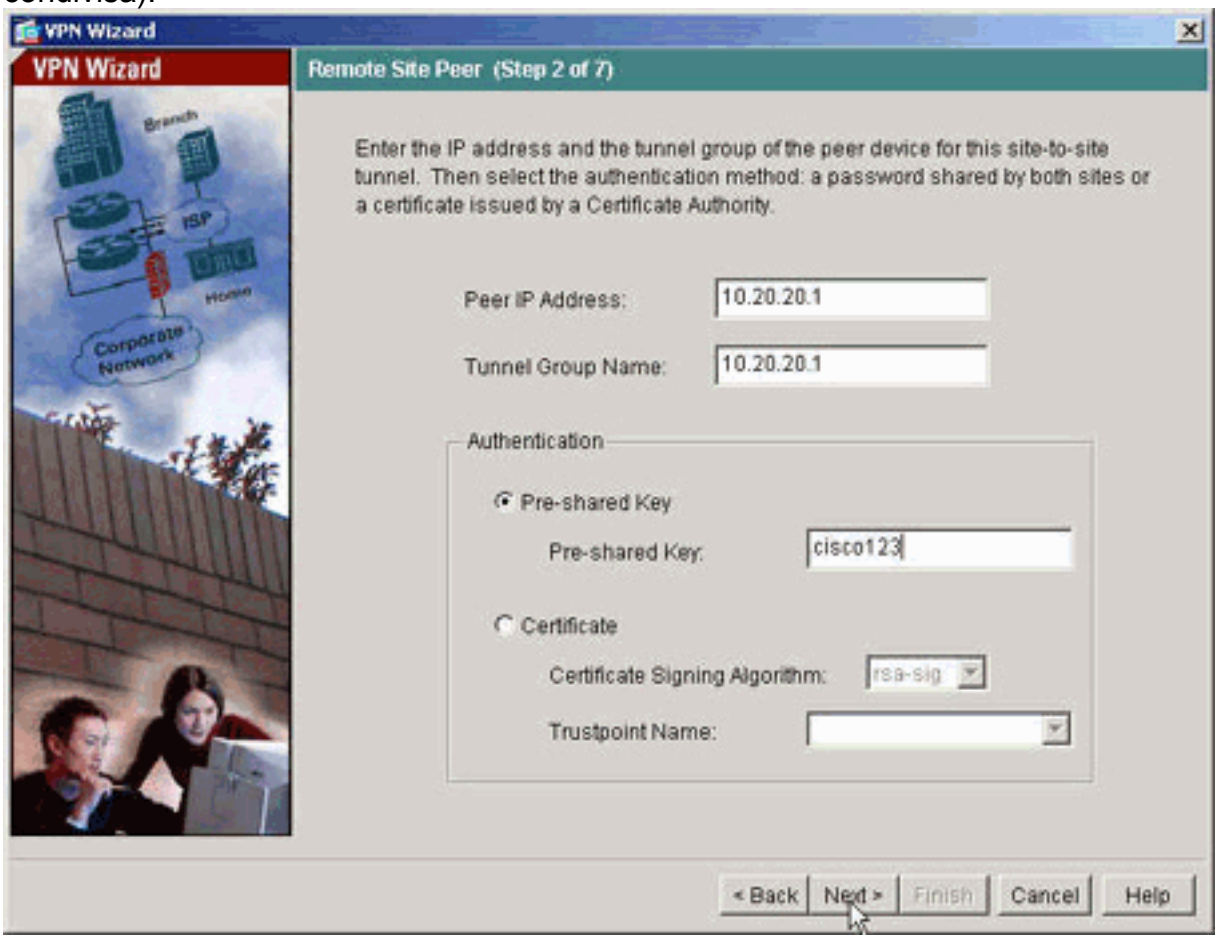


6. Scegliere il tipo di tunnel VPN **da sito a**



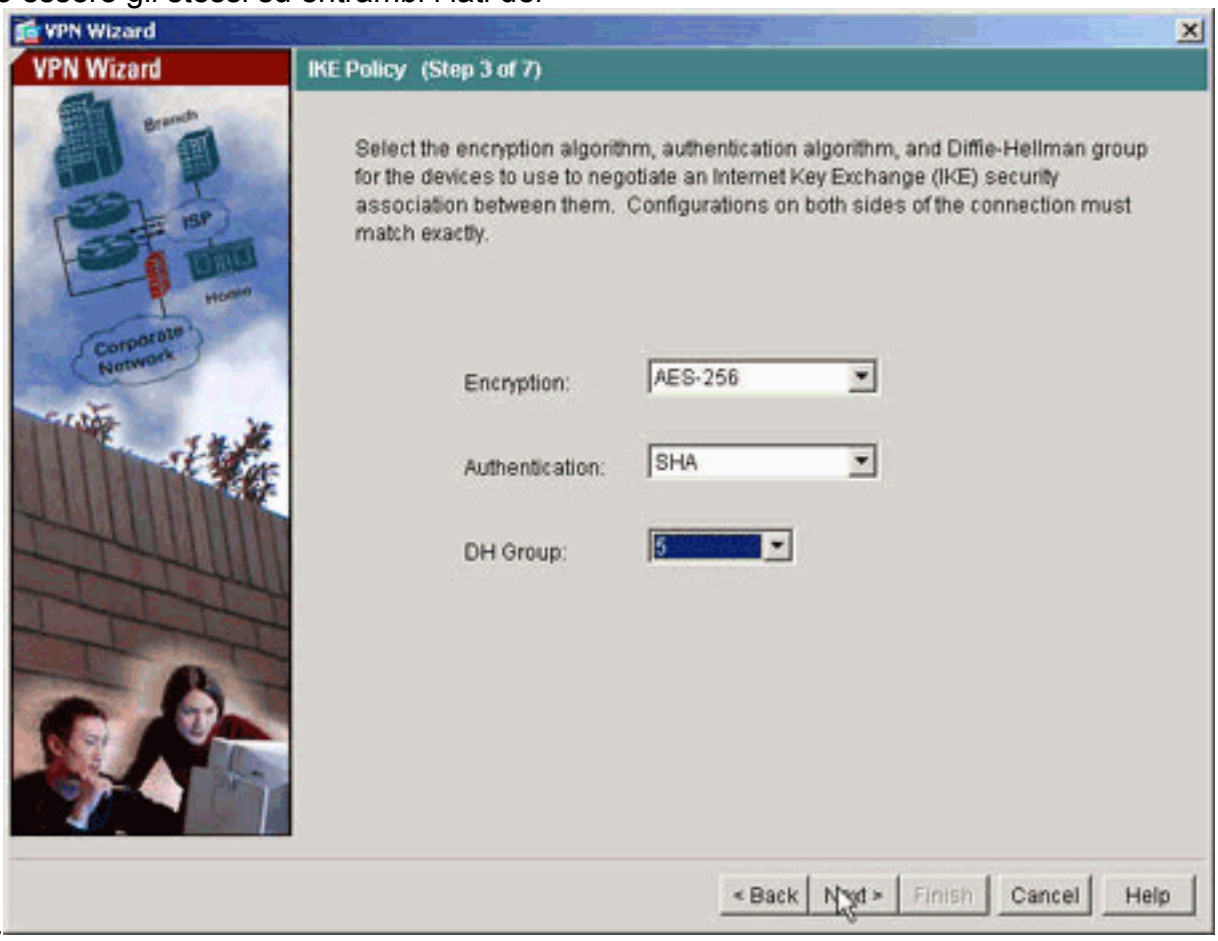
sito.

7. Specificare l'indirizzo IP esterno del peer remoto. Immettere le informazioni di autenticazione da utilizzare (in questo esempio, la chiave già condivisa).

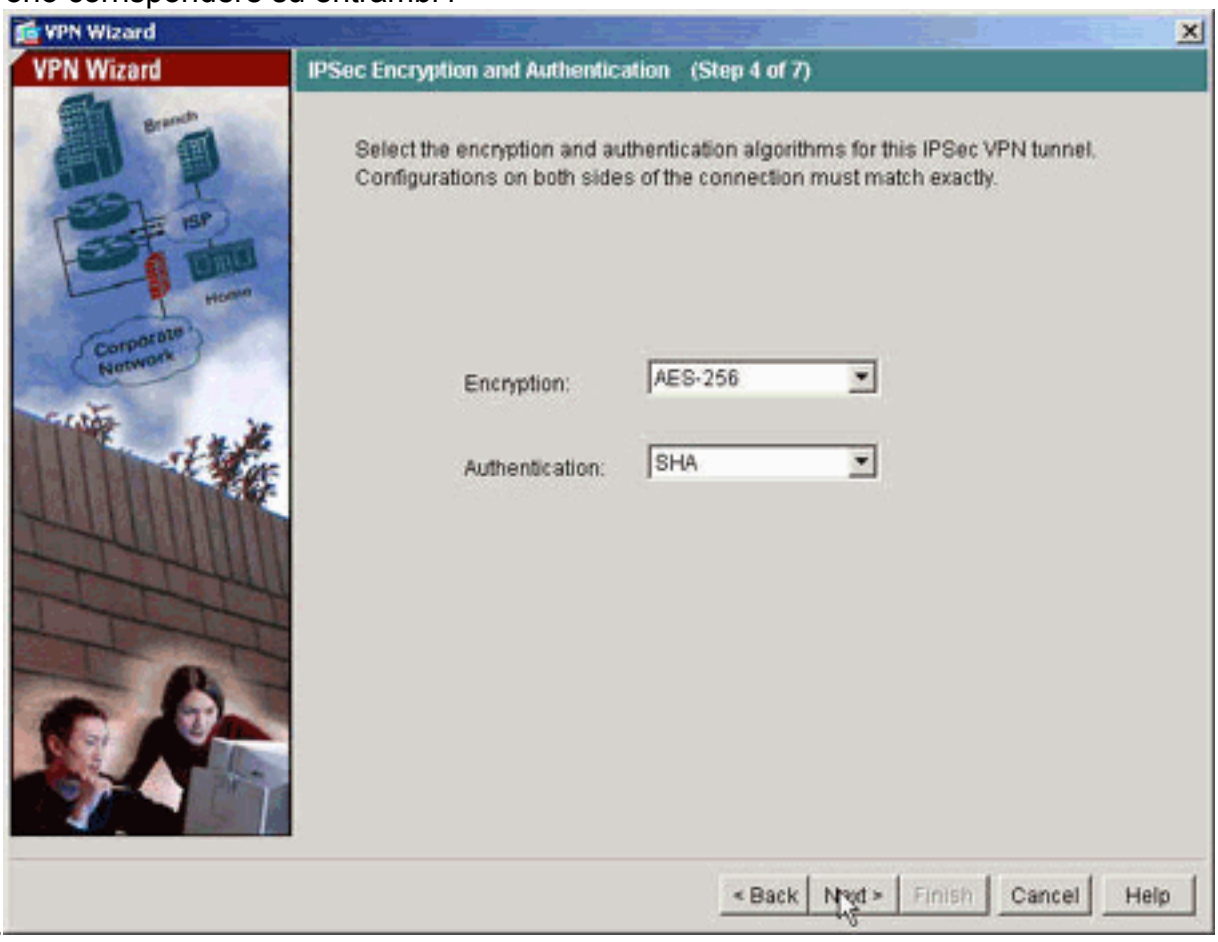


8. Specificare gli attributi da utilizzare per IKE, noto anche come "Fase 1". Questi attributi

devono essere gli stessi su entrambi i lati del tunnel.

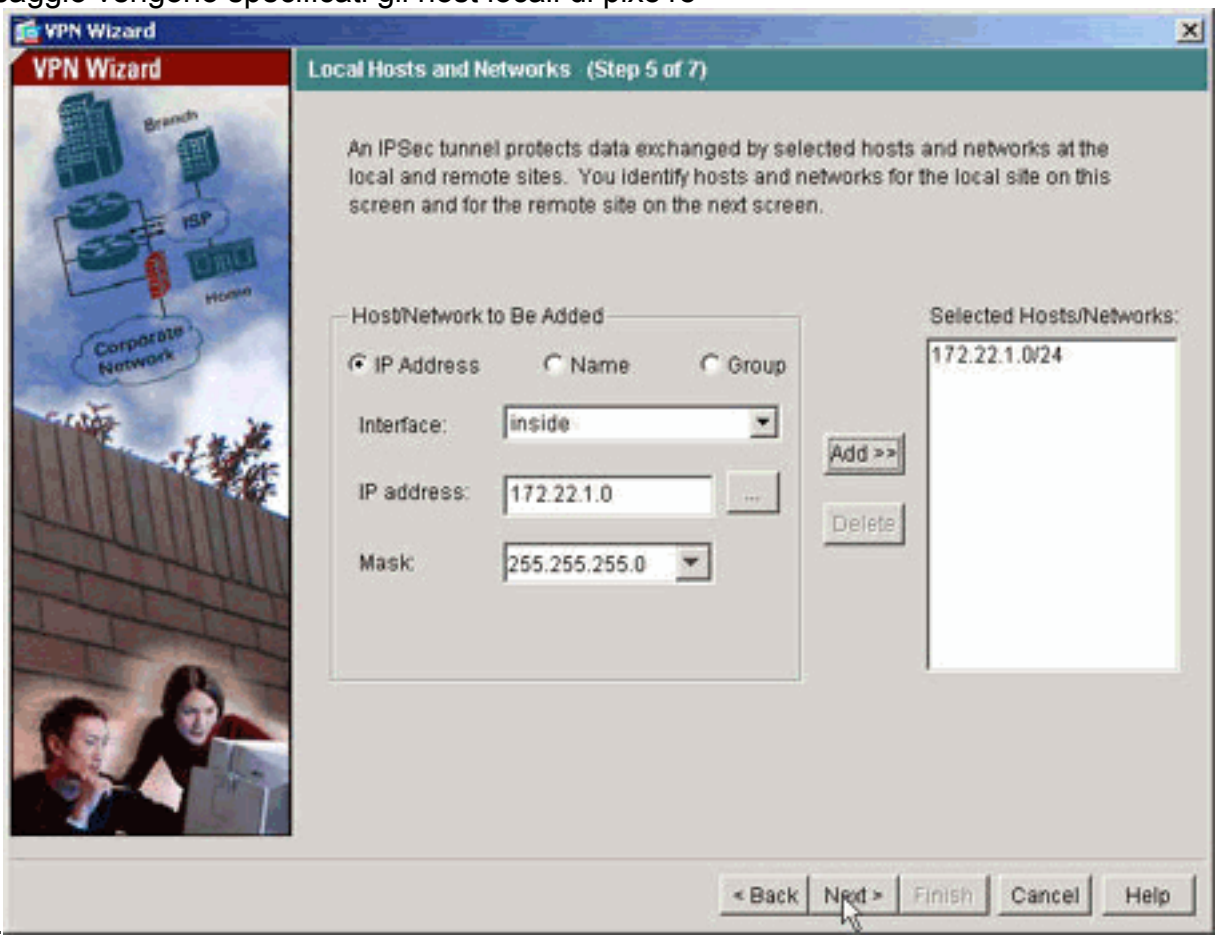


9. Specificare gli attributi da utilizzare per IPSec, noti anche come "Fase 2". Questi attributi devono corrispondere su entrambi i lati.



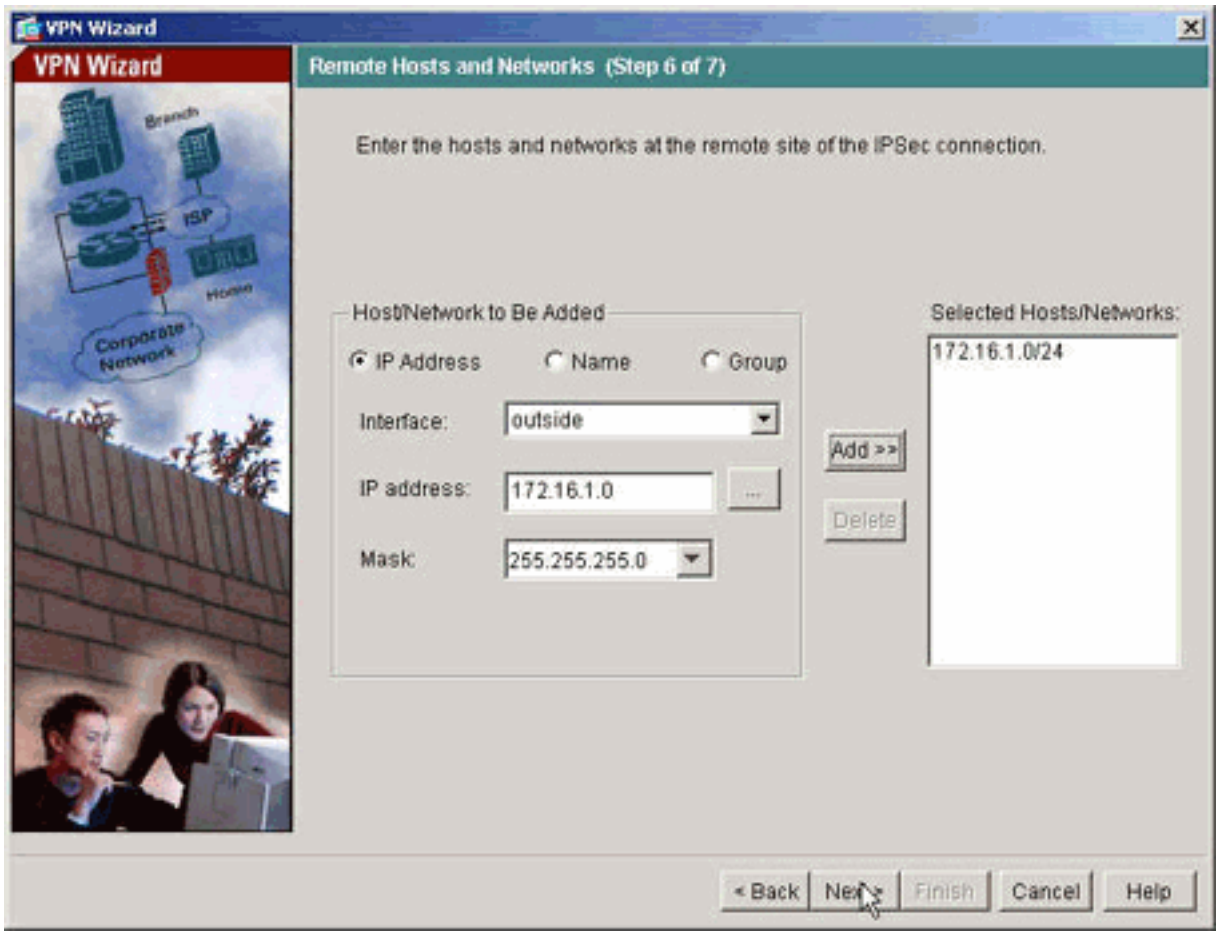
10. Specificare gli host il cui traffico deve poter passare attraverso il tunnel VPN. In questo

passaggio vengono specificati gli host locali di pix515-



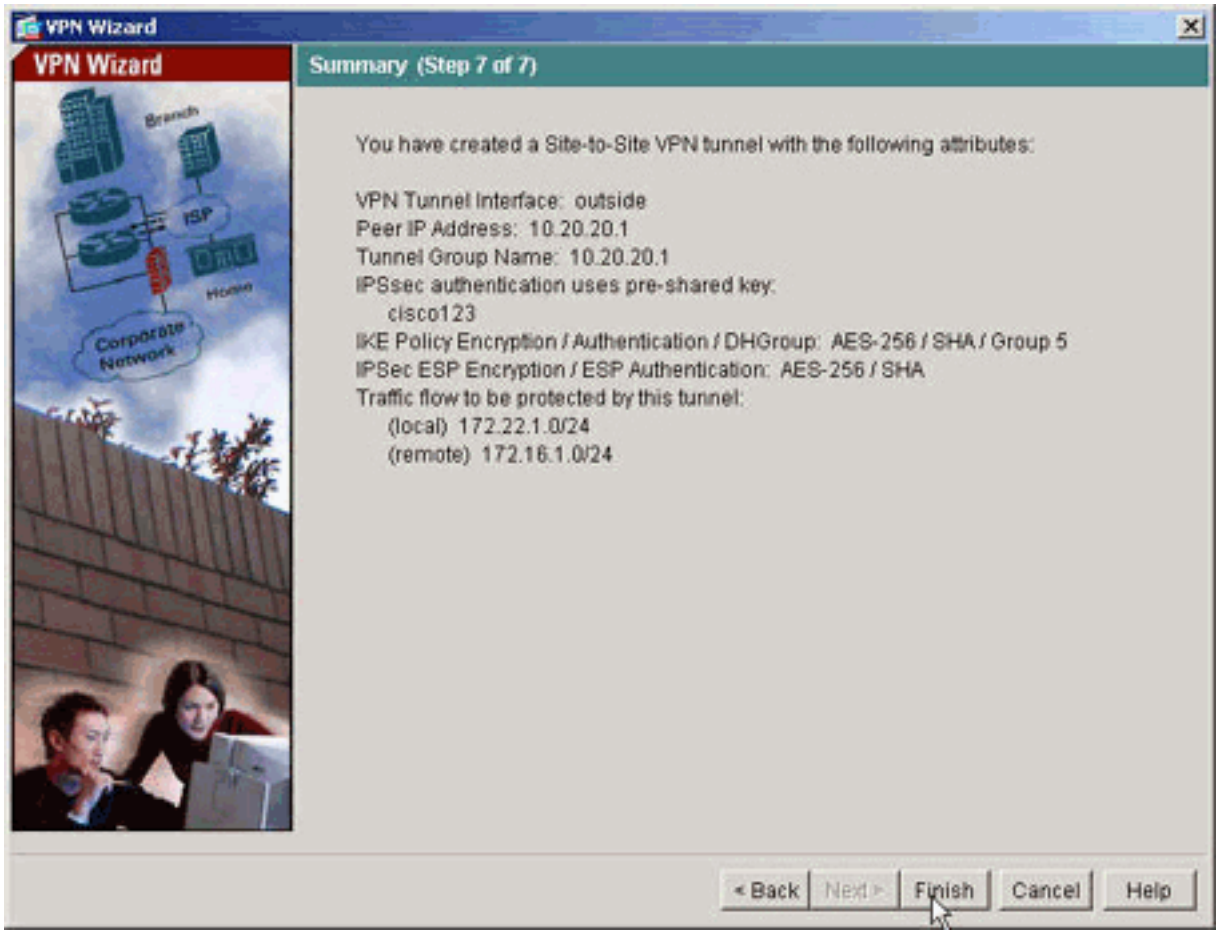
704.

11. Vengono specificati gli host e le reti sul lato remoto del tunnel.



12. In questo riepilogo vengono visualizzati gli attributi definiti dalla Creazione guidata VPN.

Verificare la configurazione e fare clic su **Finish** (Fine) quando le impostazioni sono corrette.



Configurazione PIX CLI

pix515-704

```
pixfirewall#show run
: Saved
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.10.10.1 255.255.255.0
!--- Configure the outside interface. ! interface
Ethernet1 nameif inside security-level 100 ip address
172.22.1.163 255.255.255.0 !--- Configure the inside
interface. ! !-- Output suppressed ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name default.domain.invalid
access-list inside_nat0_outbound extended permit ip
172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !---
This access list (inside_nat0_outbound) is used with the
nat zero command. !--- This prevents traffic which
matches the access list from undergoing !--- network
```

```
address translation (NAT). The traffic specified by this
ACL is !--- traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_cryptomap_20 extended permit ip
172.22.1.0 255.255.255.0 172
.16.1.0 255.255.255.0
!--- This access list (outside_cryptomap_20) is used
with the crypto map !--- outside_map to determine which
traffic should be encrypted and sent !--- across the
tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover

asdm image flash:/asdm-511.bin
!--- Enter this command to specify the location of the
ASDM image. asdm history enable arp timeout 14400 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound.

route outside 0.0.0.0 0.0.0.0 10.10.10.2 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


http server enable
!--- Enter this command in order to enable the HTTPS
server for ASDM. http 172.22.1.1 255.255.255.255 inside
!--- Identify the IP addresses from which the security
appliance !--- accepts HTTPS connections. no snmp-server
location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. crypto ipsec transform-set ESP-AES-
256-SHA esp-aes-256 esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 20
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
```

```
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
l2l !--- In order to create and manage the database of
connection-specific records !--- for ipsec-l2l—IPsec
(LAN-to-LAN) tunnels, use the tunnel-group !--- command
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 10.20.20.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
authentication method. telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

PIX-02

```
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704.

access-list outside_cryptomap_20 extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
outside_cryptomap_20 !--- ACL on pix515-704.
```

```
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
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
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256
esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-
SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874
```

```
: end
pixfirewall#
```

Tunnel di backup da sito a sito

Per specificare il tipo di connessione per la funzione da sito a sito di backup per questa voce della mappa crittografica, utilizzare il comando **crypto map set connection-type** in modalità di configurazione globale. Utilizzare la forma `no` di questo comando per tornare all'impostazione predefinita.

Sintassi:

crypto map *map-name seq-num set* **connection-type {answer-only | originate-only | bidirectional}**

- **solo risposta**: specifica che questo peer risponde solo alle connessioni IKE in entrata per prime durante lo scambio proprietario iniziale per determinare il peer appropriato a cui connettersi.
- **bidirezionale**: per specificare che il peer può accettare e creare connessioni basate su questa voce della mappa crittografica. Si tratta del tipo di connessione predefinito per tutte le connessioni da sito a sito.
- **originate-only** - Specifica che questo peer avvia il primo scambio proprietario per determinare il peer appropriato a cui connettersi.

Il comando **crypto map set connection-type** specifica i tipi di connessione per la funzione di backup da LAN a LAN. Consente di specificare più peer di backup a un'estremità della connessione. Questa funzione funziona solo tra le seguenti piattaforme:

- Due appliance di sicurezza Cisco ASA serie 5500
- Cisco ASA serie 5500 security appliance e Cisco VPN 3000 Concentrator
- Cisco ASA serie 5500 appliance di sicurezza e appliance di sicurezza con software Cisco PIX Security Appliance versione 7.0 o successive

Per configurare una connessione di backup da LAN a LAN, Cisco consiglia di configurare un'estremità della connessione come sola origine con la parola chiave `originate-only` e l'estremità con più peer di backup come sola risposta con la parola chiave `answer-only`. Sul lato solo dell'origine, usare il comando **crypto map set peer** per ordinare la priorità dei peer. L'accessorio di protezione di sola origine tenta di negoziare con il primo peer dell'elenco. Se il peer non risponde, l'appliance di sicurezza scorre verso il basso fino a quando un peer non risponde o non ci sono altri peer nell'elenco.

Se configurato in questo modo, il peer di sola origine tenta inizialmente di stabilire un tunnel proprietario e negoziare con un peer. In seguito, entrambi i peer possono stabilire una normale connessione LAN a LAN e i dati di entrambe le estremità possono avviare la connessione del tunnel.

Nota: se per una voce di crittografia è stata configurata una VPN con più indirizzi IP peer, la VPN viene stabilita con l'indirizzo IP peer di backup quando il peer primario non funziona. Tuttavia, una volta che il peer primario ritorna, la VPN non ha diritto di priorità sull'indirizzo IP primario. È necessario eliminare manualmente l'associazione di protezione esistente per riavviare la negoziazione VPN e passare all'indirizzo IP primario. Come si deduce dalla conclusione, l'interruzione anticipata della VPN non è supportata nel tunnel da sito a sito.

Tipi di connessione LAN a LAN di backup supportati

Lato remoto	Lato centrale
`Originate-Only`	`Answer-Only`
`Bi-Directional`	`Answer-Only`
`Bi-Directional`	`Bi-Directional`

Esempio

Questo esempio, immesso in modalità di configurazione globale, configura la **mappa crittografica mymap** e imposta il tipo di connessione su *originate-only*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

Cancella associazioni di sicurezza

In modalità di privilegio di PIX, utilizzare i seguenti comandi:

- **clear [crypto] ipsec sa**: elimina le SA IPsec attive. la parola chiave *crypto* è facoltativa.
- **clear [crypto] isakmp sa**: elimina le SA IKE attive. la parola chiave *crypto* è facoltativa.

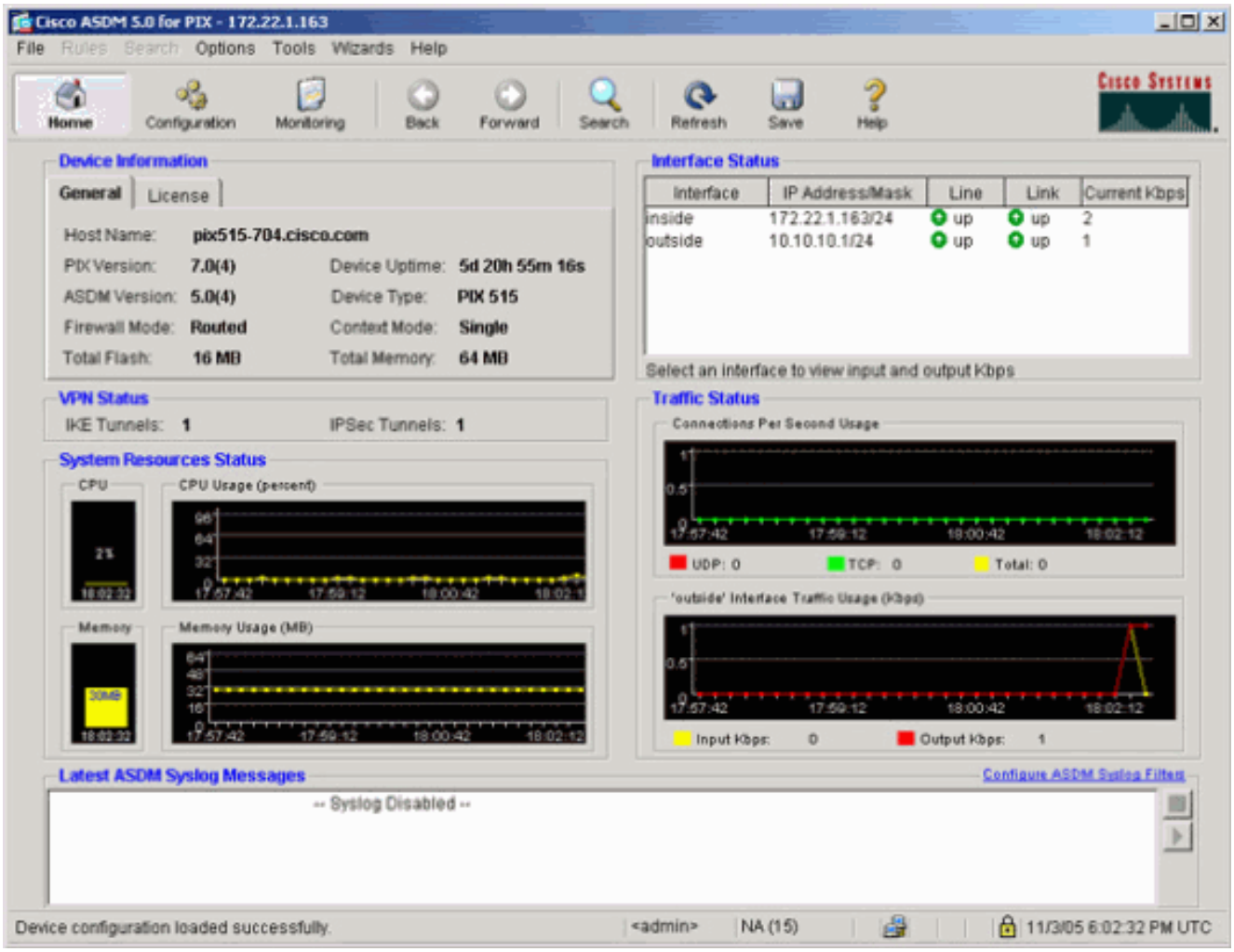
Verifica

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

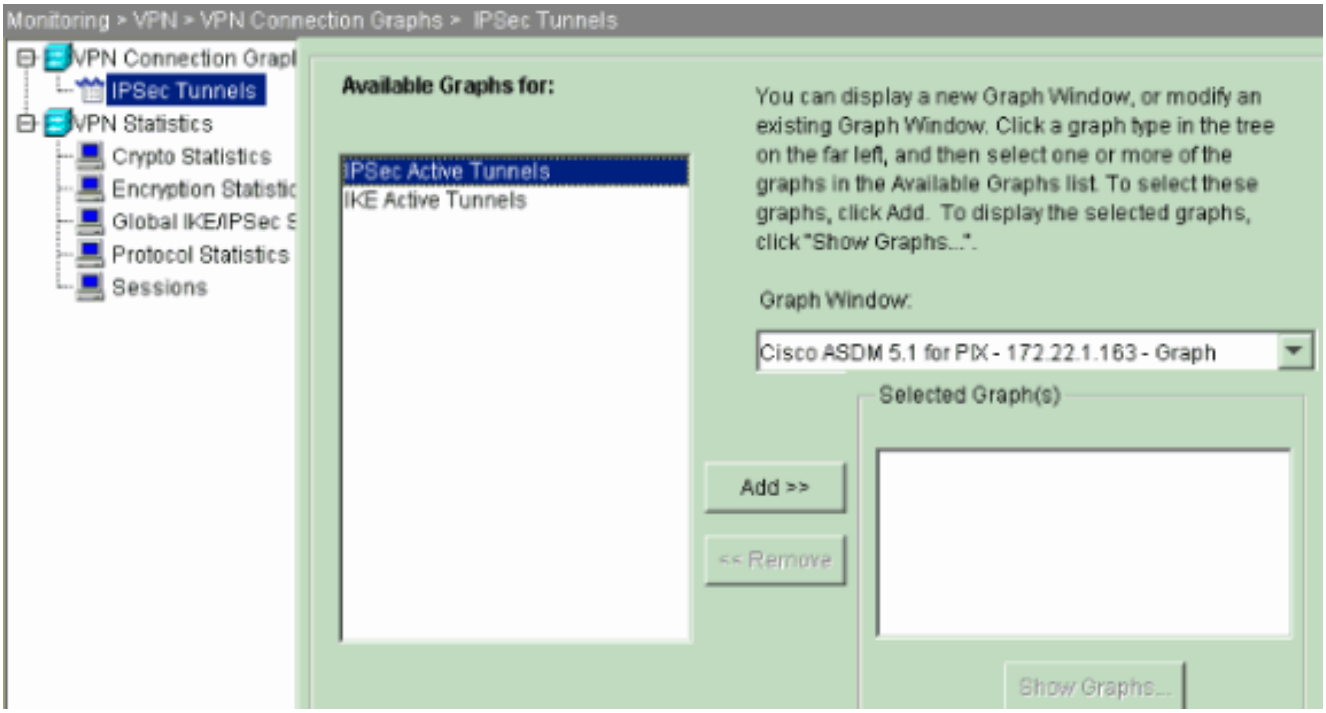
Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Se è presente traffico interessante verso il peer, il tunnel viene stabilito tra pix515-704 e PIX-02.

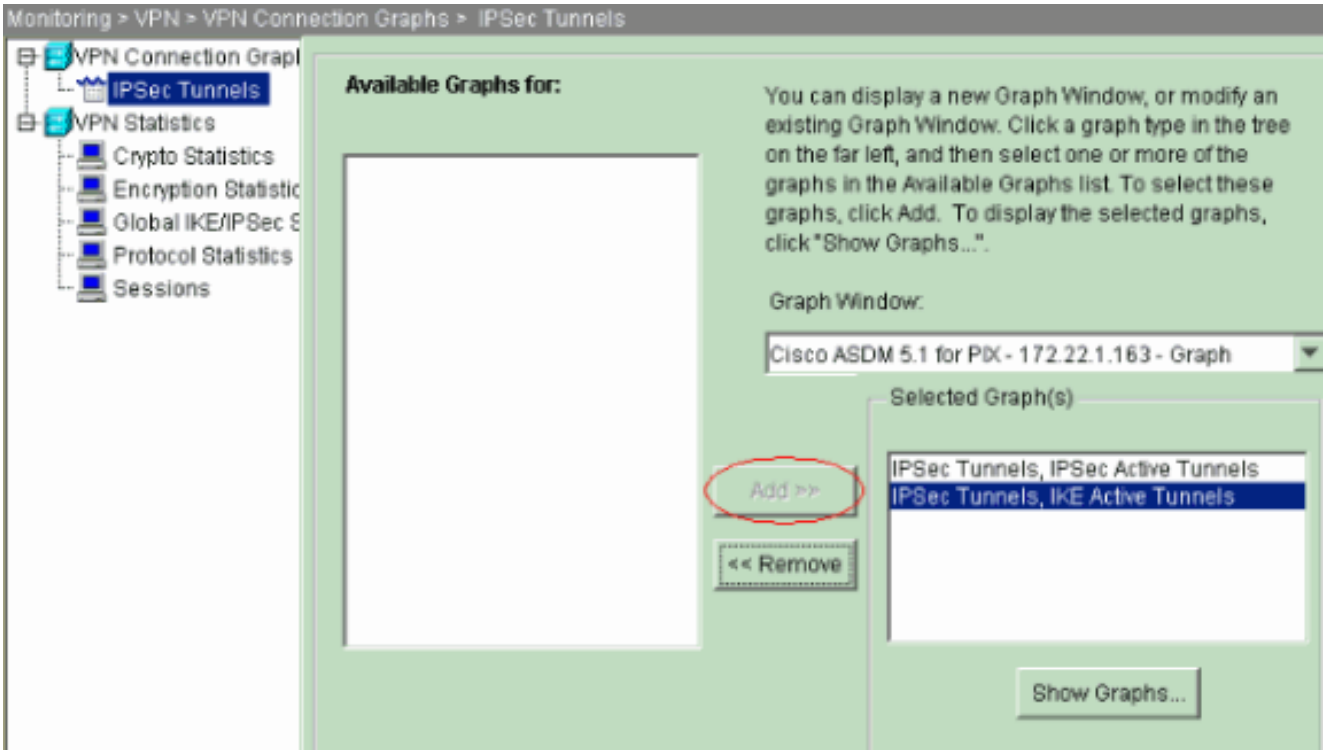
1. Per verificare la formazione del tunnel, visualizzare lo stato VPN in **Home** (Home) in ASDM.



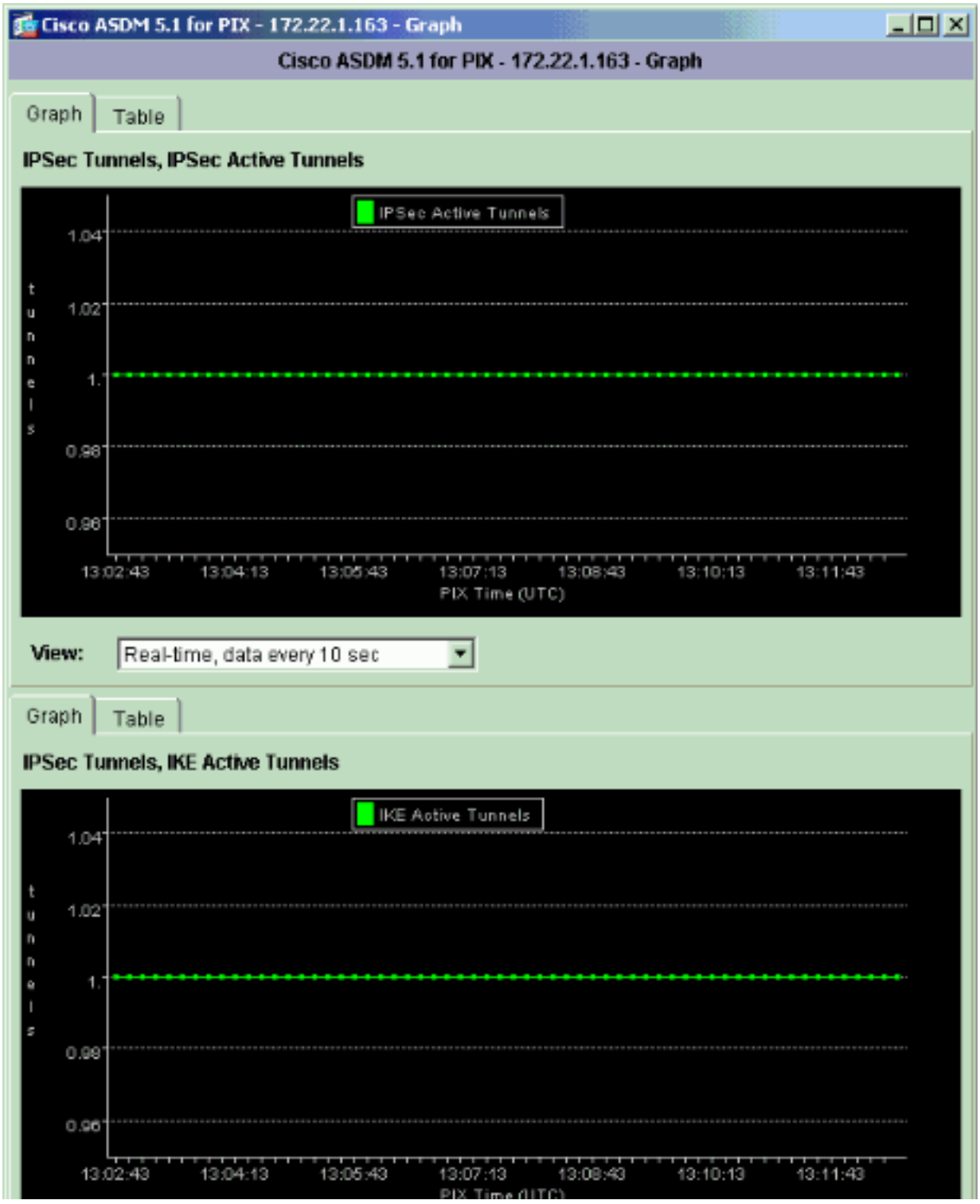
2. Per verificare i dettagli sulla definizione del tunnel, scegliere **Monitoraggio > VPN > Grafici connessione VPN > Tunnel IPSec**.



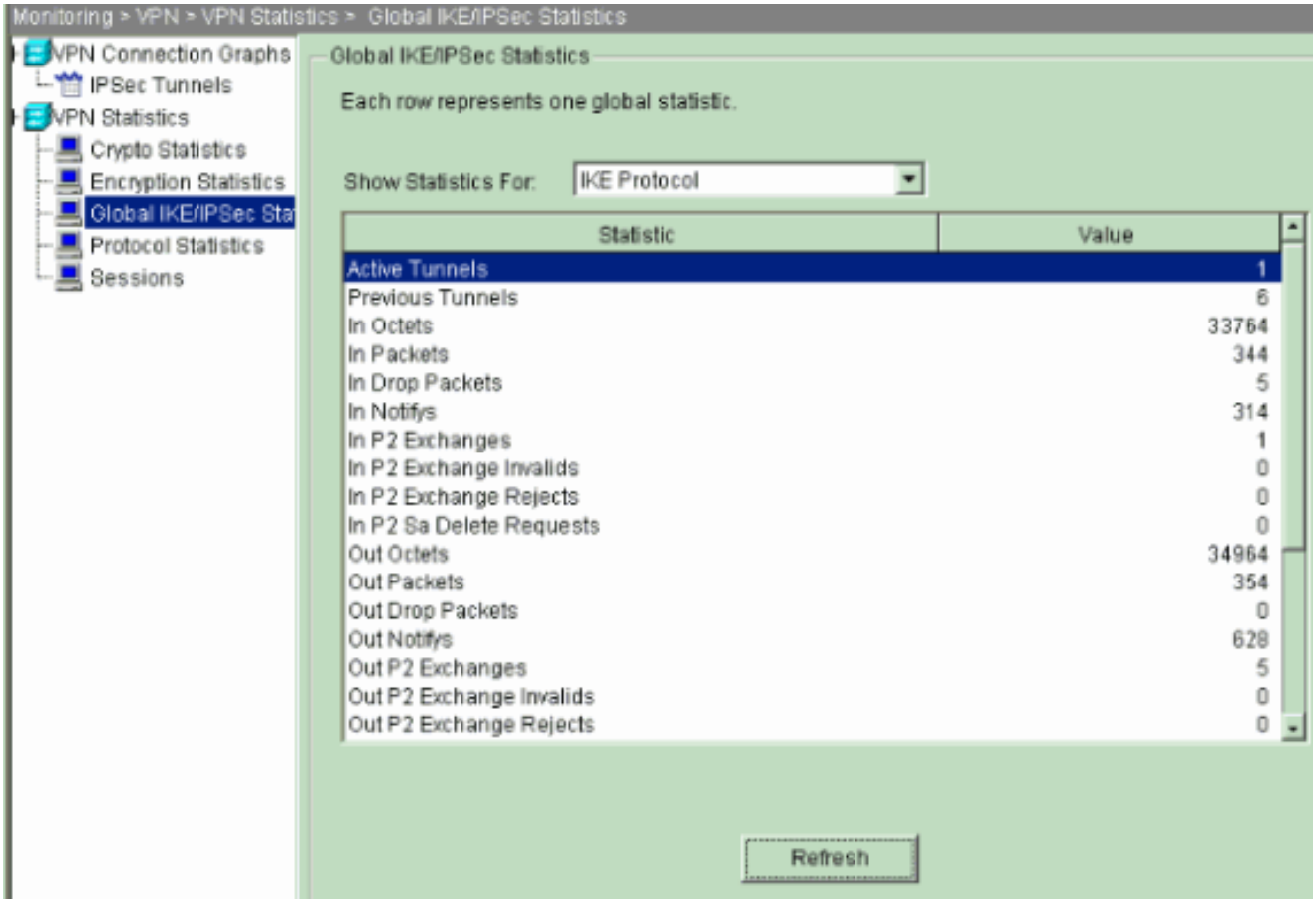
3. Fate clic su **Aggiungi (Add)** per selezionare i grafici disponibili da visualizzare nella finestra del grafico.



4. Per visualizzare i grafici dei tunnel attivi IKE e IPsec, fare clic su **Show Graphs**.



5. Per conoscere le informazioni statistiche del tunnel VPN, scegliere **Monitoraggio > VPN > Statistiche VPN > Statistiche globali IKE/IPSec**.



èpossibile anche verificare la formazione dei tunnel usando la CLI. Utilizzare il comando **show crypto isakmp sa** per controllare la formazione dei tunnel e il comando **show crypto ipsec sa** per osservare il numero di pacchetti incapsulati, crittografati e così via.

pix515-704

```
pixfirewall(config)#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: 10.20.20.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

pix515-704

```
pixfirewall(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1

     access-list outside_cryptomap_20 permit ip
172.22.1.0
       255.255.255.0 172.16.1.0 255.255.255.0
     local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
     current_peer: 10.20.20.1

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest:
```

```
20
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify:
20
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #pkts comp failed: 0,
#pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

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

      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 44532974

    inbound esp sas:
      spi: 0xA87AD6FA (2826622714)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824998/28246)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x44532974 (1146300788)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824998/28245)
         IV size: 16 bytes
         replay detection support: Y
```

Risoluzione dei problemi

PFS

Nelle negoziazioni IPsec, PFS (Perfect Forward Secrecy) garantisce che ogni nuova chiave di crittografia non sia correlata a nessuna chiave precedente. Abilitare o disabilitare PFS su entrambi i peer del tunnel, altrimenti il tunnel IPsec L2L non verrà stabilito in PIX/ASA.

PFS è disattivato per impostazione predefinita. Per abilitare PFS, utilizzare il comando **pfs** con la parola chiave *enable* in modalità di configurazione Criteri di gruppo. Per disabilitare PFS, immettere la parola chiave *disable*.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Per rimuovere l'attributo PFS dalla configurazione in esecuzione, immettere la forma **no** di questo comando. Un criterio di gruppo può ereditare un valore per PFS da un altro criterio di gruppo. Immettere la forma **no** di questo comando per impedire che un valore venga ereditato.

```
hostname(config-group-policy)#no pfs
```

Accesso alla gestione

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

Non è possibile eseguire il ping dell'interfaccia interna del PIX dall'altra estremità 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
```

Comandi debug

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

debug crypto isakmp: visualizza le informazioni di debug sulle connessioni IPsec e mostra il primo set di attributi negati a causa di incompatibilità su entrambi i lati.

debug crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7
Nov 27 12:01:59 [IKEv1 DEBUG]: Pitcher: received a key
acquire message,
spi 0x0
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE Initiator:
New Phase 1,
Intf 2, IKE Peer 10.20.20.1  local Proxy Address
172.22.1.0, remote
Proxy Address 172.16.1.0,  Crypto map (outside_map)
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing ISAKMP SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing Fragmentation
VID + extended capabilities payload
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=0) with payloads : HDR +
 SA (1) + VENDOR (13) + NONE (0) total length : 148
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0)
total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley
proposal is acceptable
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Fragmentation VID
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer
included
IKE fragmentation capability flags
:  Main Mode:        True  Aggressive Mode:  True
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing nonce payload
```

```
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing Cisco Unity VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing xauth V6 VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS
VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities:
20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send
Altiga/
Cisco VPN3000/Cisco ASA GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13)
+ VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) total length
 : 320
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message
(msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) +
NONE (0) total length : 320
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing ISA_KE payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Cisco Unity client VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
xauth V6 VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing VPN3000/ASA
spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Altiga/Cisco VPN3000/Cisco ASA
GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection
landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, Generating keys
for Initiator...
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
```

```
10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing dpd vid payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE
(14) + VENDOR (13) +
NONE (0) total length : 119
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE
(14) + VENDOR (13) +
NONE (0) total length : 96
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing IOS keep alive payload: proposal=32767/32767
sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Received DPD VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection
landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Oakley begin quick mode
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1, PHASE 1 COMPLETED
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive
type for this connection: DPD
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Starting phase 1 rekey timer: 73440000 (ms)
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, IKE got
SPI from key engine: SPI = 0x44ae0956
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
oakley constucting quick mode
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing blank hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing IPSec SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing IPSec nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
```

```
10.20.20.1,
constructing proxy ID
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Transmitting Proxy Id:
  Local subnet:  172.22.1.0  mask 255.255.255.0 Protocol
0  Port 0
  Remote subnet: 172.16.1.0  Mask 255.255.255.0 Protocol
0  Port 0
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing qm hash payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NOTIFY (11) +
NONE (0) total length : 200
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message
(msgid=d723766b) with payloads
 : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID
(5) + NONE (0)
 total length : 172
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
loading all IPSEC SAs
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
Security negotiation complete for LAN-to-LAN Group
(10.20.20.1)
Initiator, Inbound SPI = 0x44ae0956, Outbound SPI =
0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
oakley constructing final quick mode
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
IKE got a KEY_ADD msg for SA: SPI = 0x4a6429ba
```

```
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Pitcher: received KEY_UPDATE, spi 0x44ae0956
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
 Starting P2 Rekey timer to expire in 24480 seconds
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
PHASE 2 COMPLETED (msgid=d723766b)
```

debug crypto ipsec: visualizza le informazioni di debug sulle connessioni IPsec.

debug crypto ipsec

```
pix1(config)#debug crypto ipsec 7

exec mode commands/options:
  <1-255>  Specify an optional debug level (default is
1)
  <cr>
pix1(config)# debug crypto ipsec 7
pix1(config)# IPSEC: New embryonic SA created @
0x024211B0,
    SCB: 0x0240AEB0,
    Direction: inbound
    SPI      : 0x2A3E12BE
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0,
    SCB: 0x0240B710,
    Direction: outbound
    SPI      : 0xB283D32F
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xB283D32F
IPSEC: Updating outbound VPN context 0x02422618, SPI
0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: New outbound permit rule, SPI 0xB283D32F
    Src addr: 10.10.10.1
    Src mask: 255.255.255.255
    Dst addr: 10.20.20.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
```

```
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0xB283D32F
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: Completed host IBSA update, SPI 0x2A3E12BE
IPSEC: Creating inbound VPN context, SPI 0x2A3E12BE
    Flags: 0x00000006
    SA   : 0x024211B0
    SPI  : 0x2A3E12BE
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x02422618
    SCB  : 0x0240AEB0
    Channel: 0x014A45B0
IPSEC: Completed inbound VPN context, SPI 0x2A3E12BE
    VPN handle: 0x0240BF80
IPSEC: Updating outbound VPN context 0x02422618, SPI
0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0240BF80
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: New inbound tunnel flow rule, SPI 0x2A3E12BE
    Src addr: 172.16.1.0
    Src mask: 255.255.255.0
    Dst addr: 172.22.1.0
    Dst mask: 255.255.255.0
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 0
    Use protocol: false
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI
0x2A3E12BE
    Rule ID: 0x0240B108
IPSEC: New inbound decrypt rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
```

```
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x2A3E12BE
    Rule ID: 0x02406E98
IPSEC: New inbound permit rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x2A3E12BE
    Rule ID: 0x02422C78
```

Informazioni correlate

- Creazione di tunnel ridondanti tra firewall tramite PDM
- Software Cisco PIX Firewall
- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- 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