Configurazione di IPSec tra un server Microsoft Windows 2000 e un dispositivo Cisco

Sommario

Introduzione

In questo documento viene illustrato come formare un tunnel IPSec con chiavi già condivise per collegarsi a 2 reti private: una rete privata (192.168.I.X) all'interno di un dispositivo Cisco e una rete privata (10.32.50.X) all'interno di Microsoft 2000 Server. Si presume che il traffico tra il dispositivo Cisco e l'interno del server 2000 e Internet (rappresentato qui dalle reti 172.18.124.X) scorra prima di iniziare questa configurazione.

Per informazioni dettagliate sulla configurazione del server di Microsoft Windows 2000, visitare il sito Web Microsoft: http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

Operazioni preliminari

Convenzioni

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

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

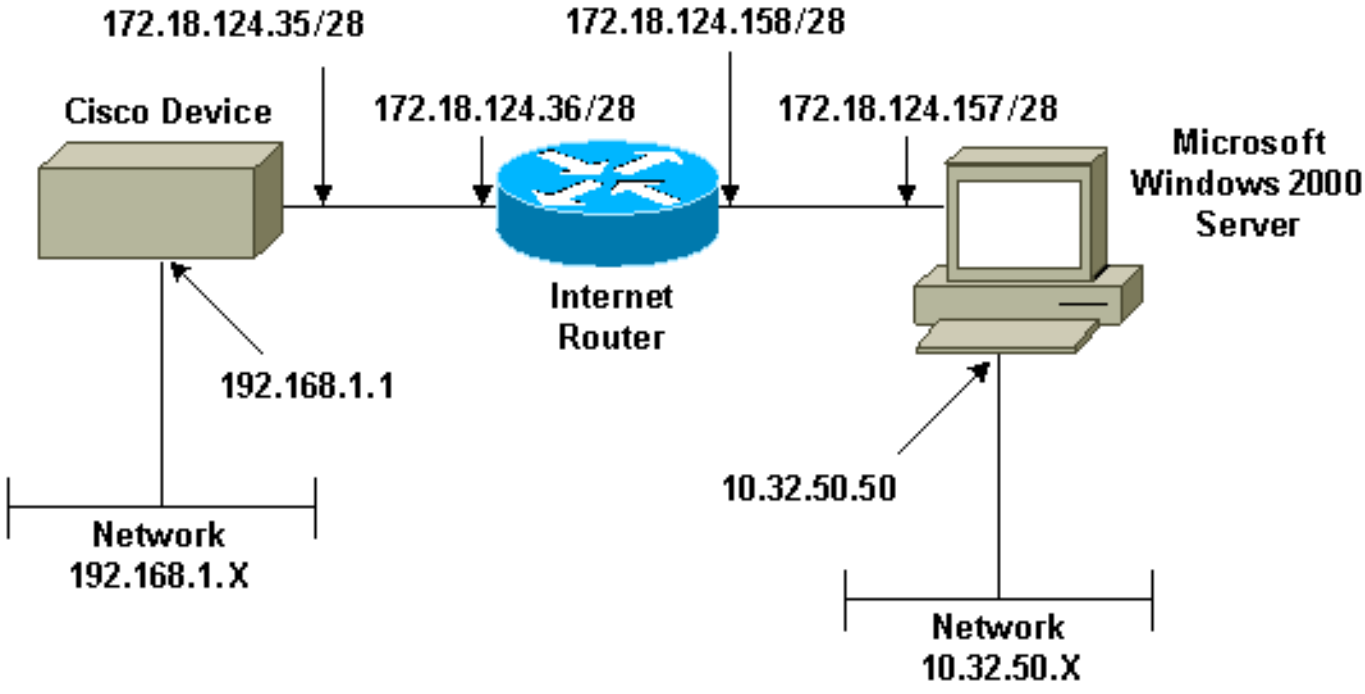
Queste configurazioni sono state sviluppate e testate utilizzando le versioni software e hardware riportate di seguito.

- Microsoft Windows 2000 Server 5.00.2195
- Router Cisco 3640 con software Cisco IOS® versione c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall con software PIX versione 5.2.1
- Cisco VPN 3000 Concentrator con software VPN 3000 Concentrator versione 2.5.2.F
- Cisco VPN 5000 Concentrator con software VPN 5000 Concentrator versione 5.2.19

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

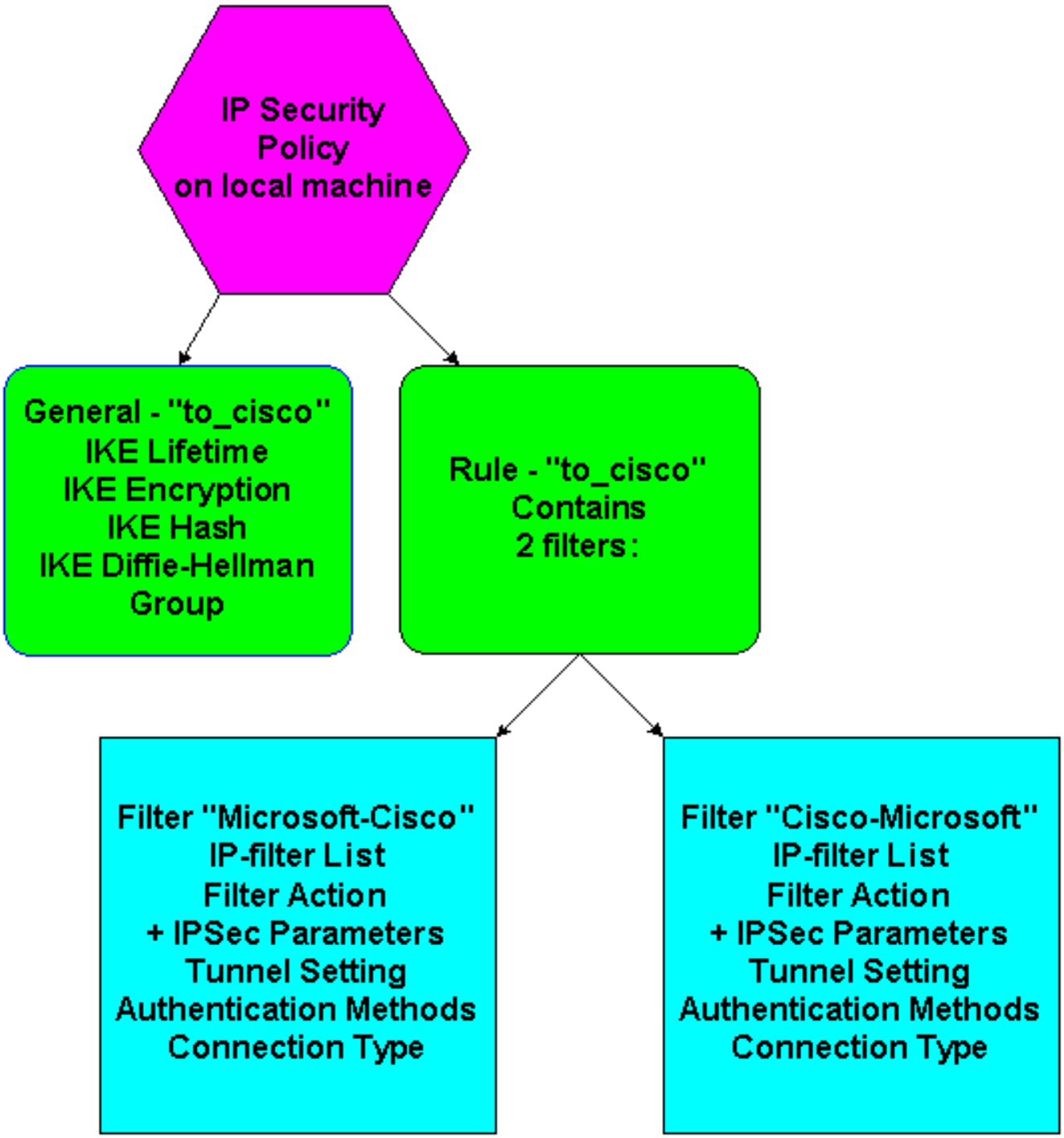
Questo documento utilizza le impostazioni di rete mostrate nel diagramma sottostante.



Configurazione di Microsoft Windows 2000 Server per l'utilizzo con i dispositivi Cisco

Attività eseguite

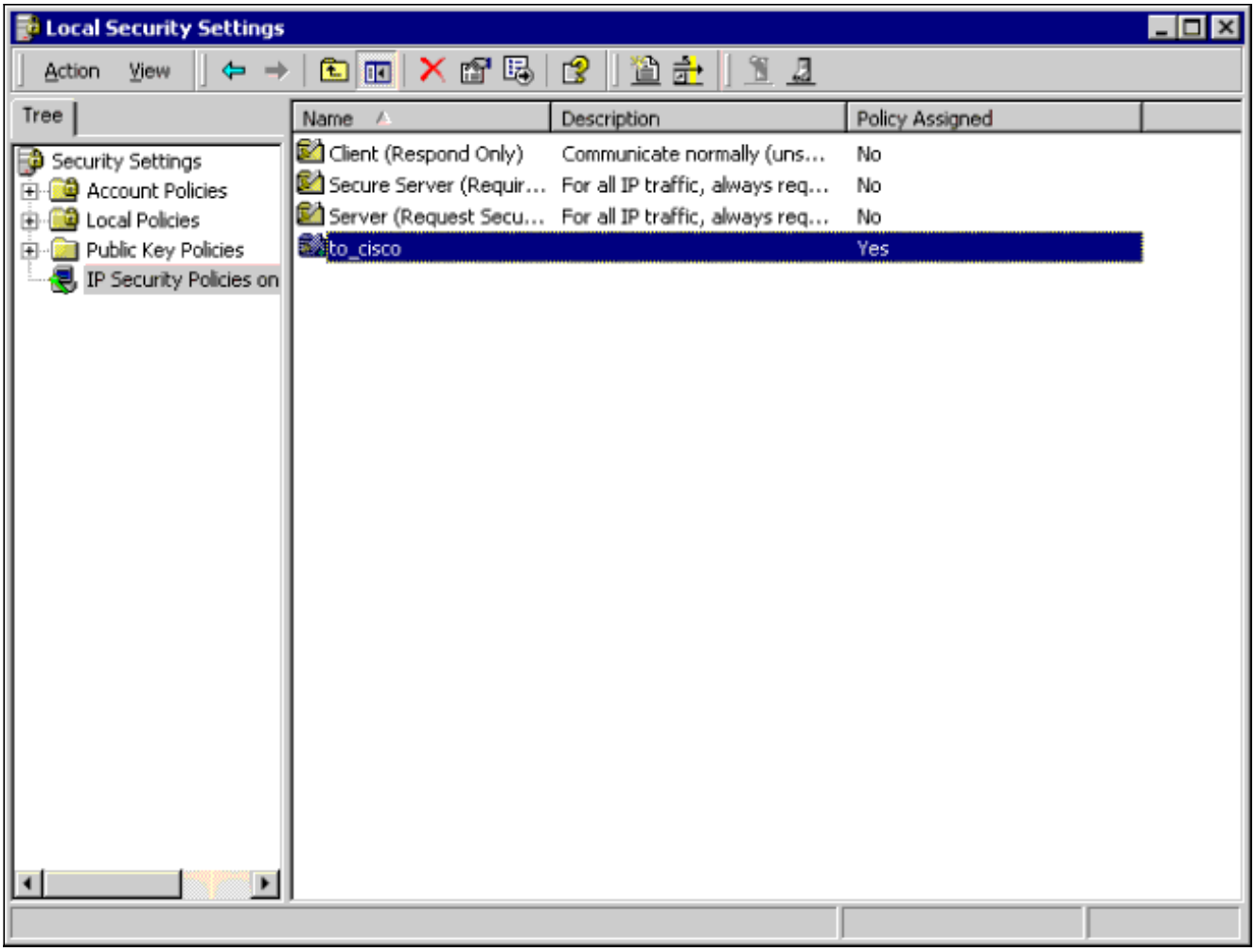
Il diagramma mostra le attività eseguite nella configurazione del server di Microsoft Windows 2000:



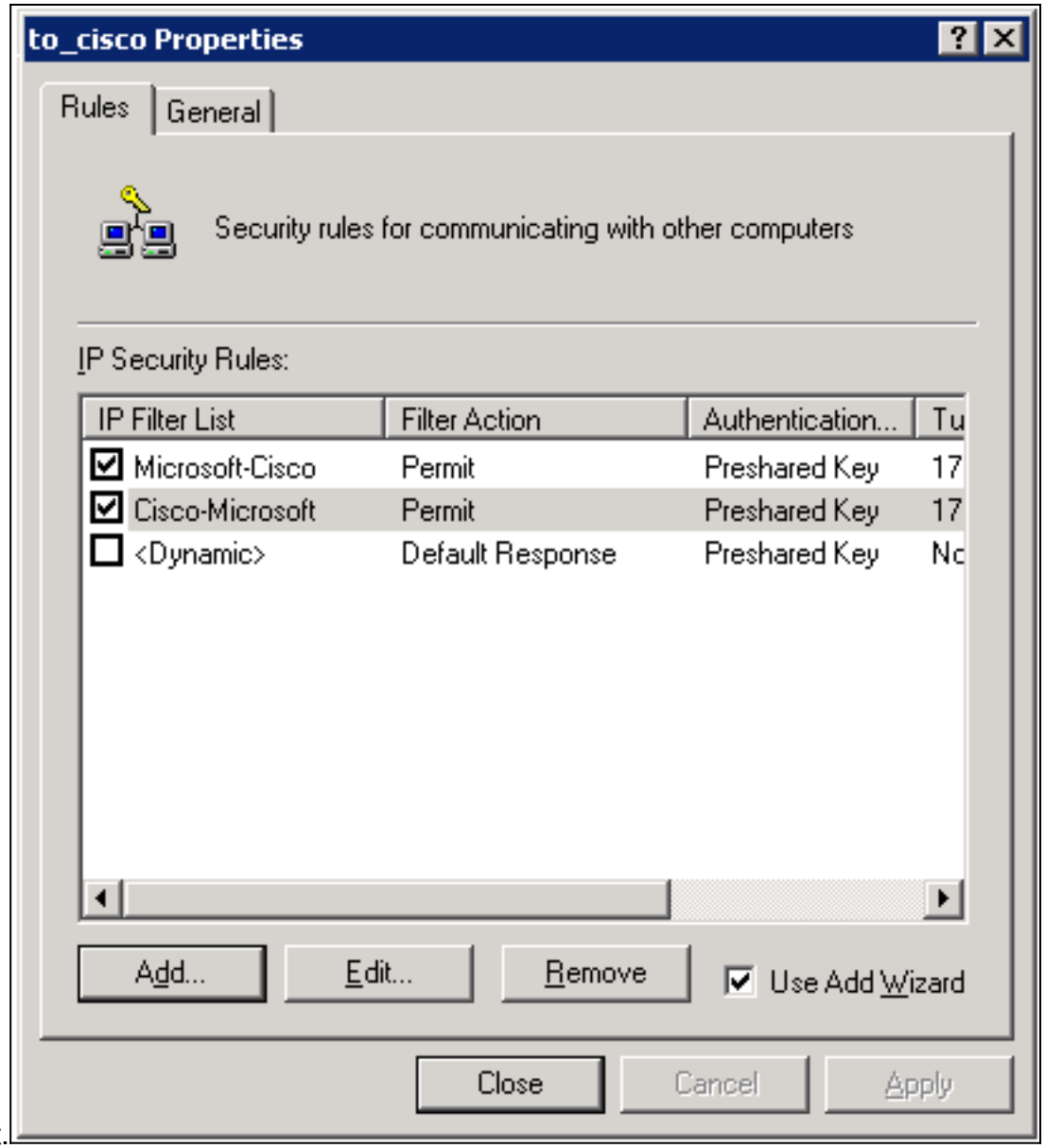
Istruzioni dettagliate

Dopo aver seguito le istruzioni di configurazione sul sito Web Microsoft, eseguire la procedura seguente per verificare che la configurazione funzioni con i dispositivi Cisco. I commenti e le modifiche vengono annotati con le immagini acquisite.

1. Fare clic su **Start > Esegui > secpol.msc** in Microsoft Windows 2000 Server e verificare le informazioni nelle schermate seguenti.Dopo aver utilizzato le istruzioni sul sito Web Microsoft per configurare un server 2000, sono state visualizzate le seguenti informazioni sul tunnel.**Nota:** la regola di esempio è chiamata "to_cisco".

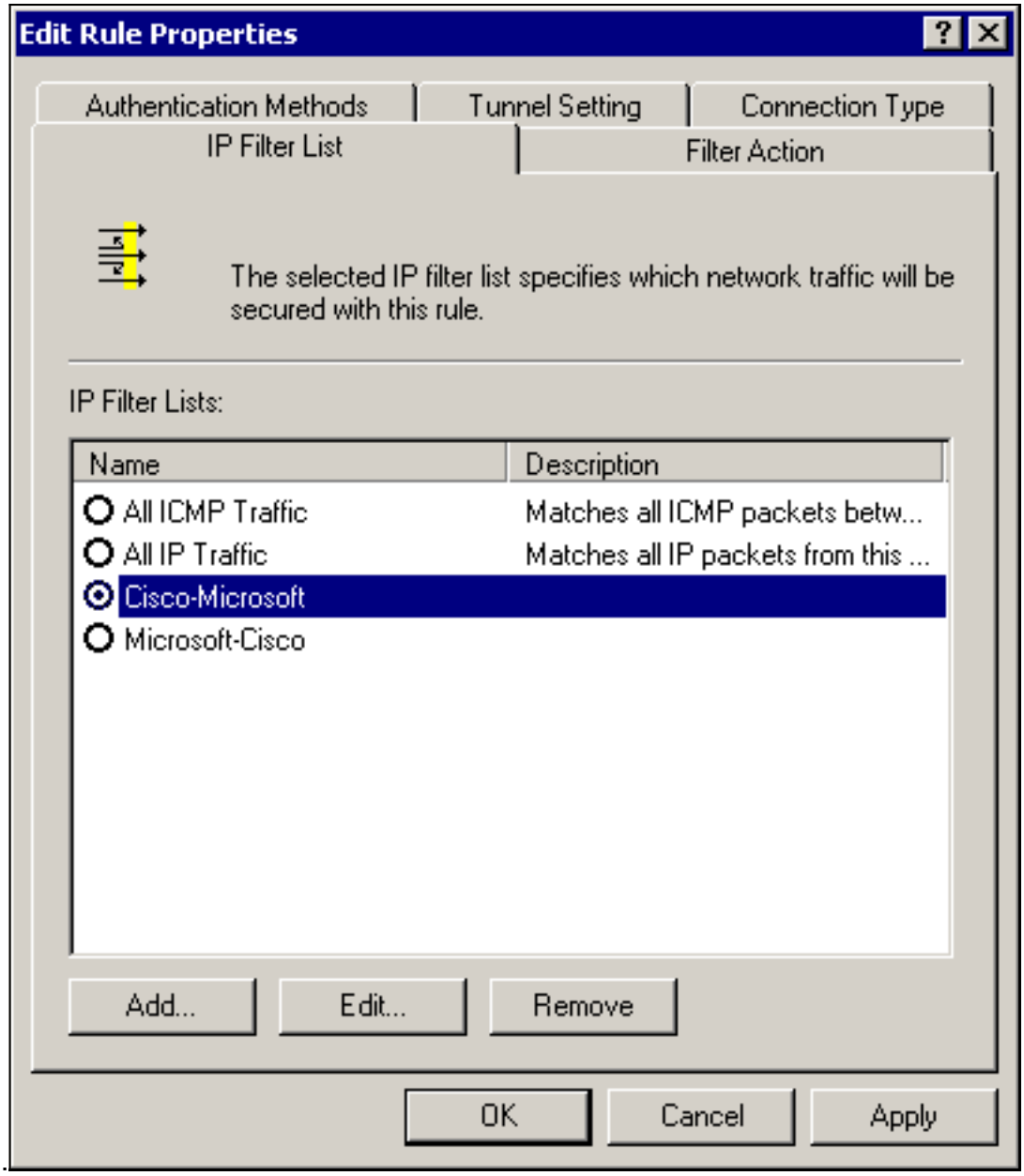


2. Questa regola di esempio contiene due filtri: Microsoft-Cisco e Cisco-



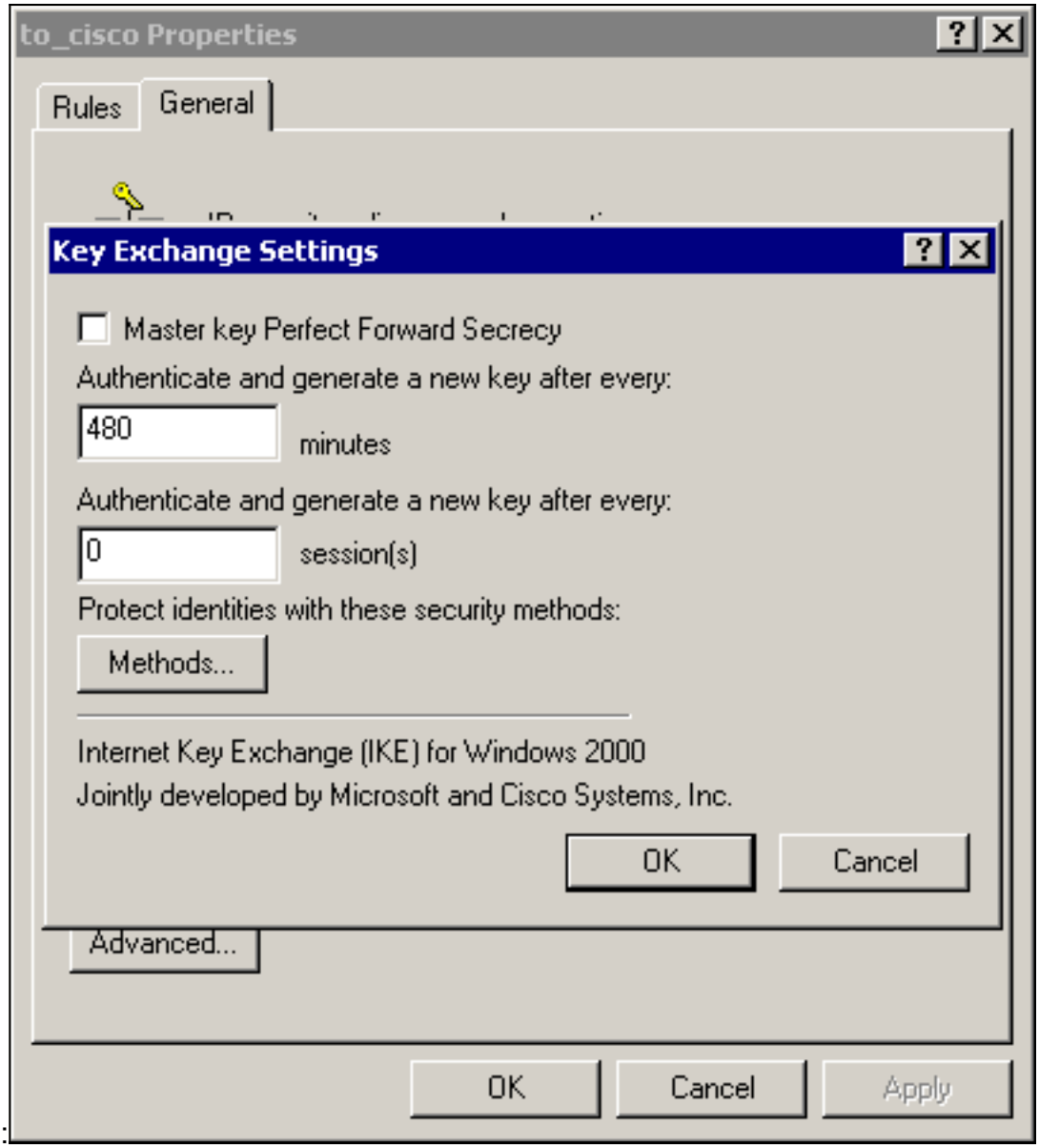
Microsoft.

3. Selezionare la regola di sicurezza IP Cisco-Microsoft, quindi fare clic su **Modifica** per visualizzare/aggiungere/modificare gli elenchi filtri



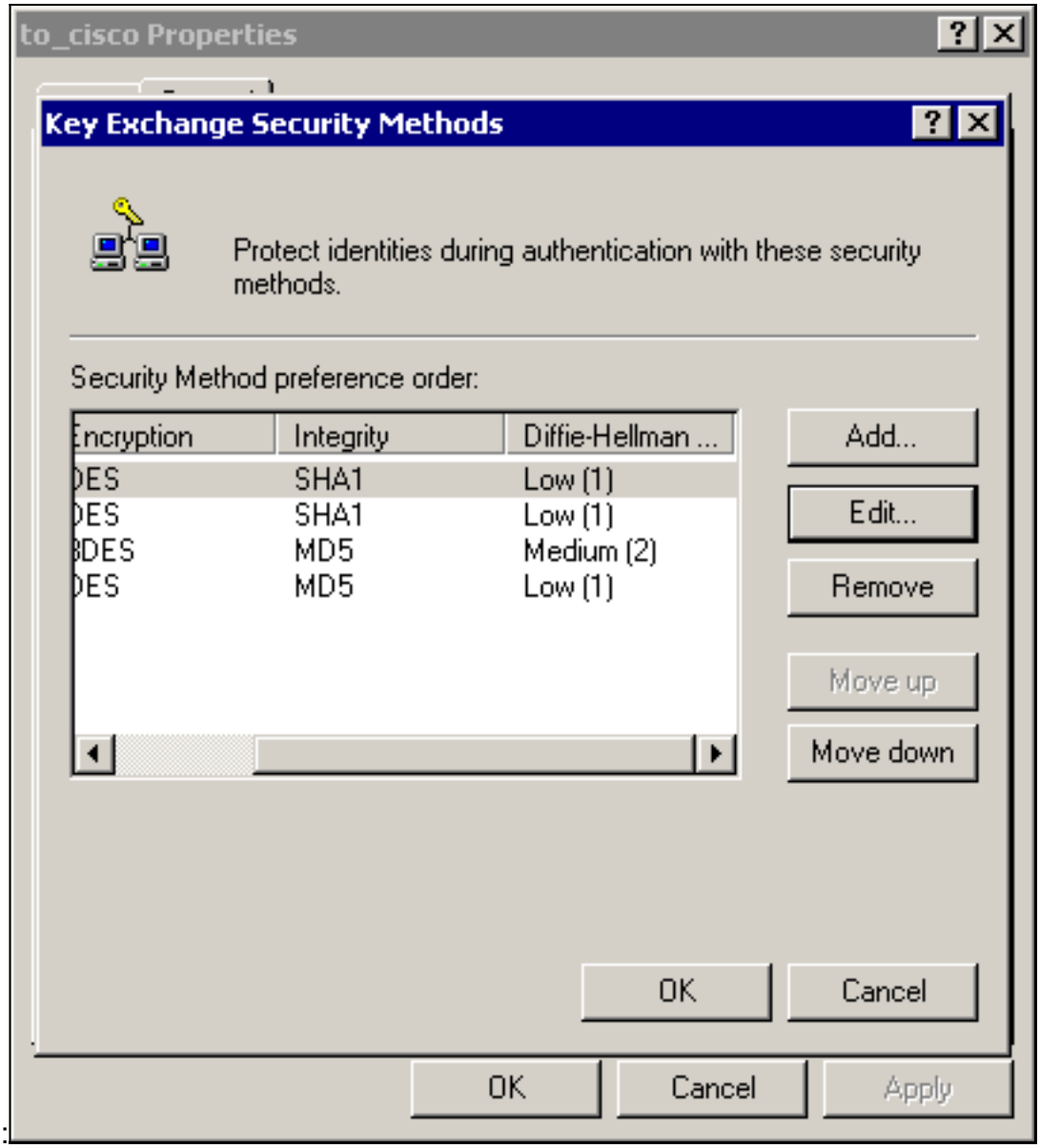
IP.

4. La scheda **Generale > Avanzate** della regola ha la **durata IKE** (480 minuti = 28800



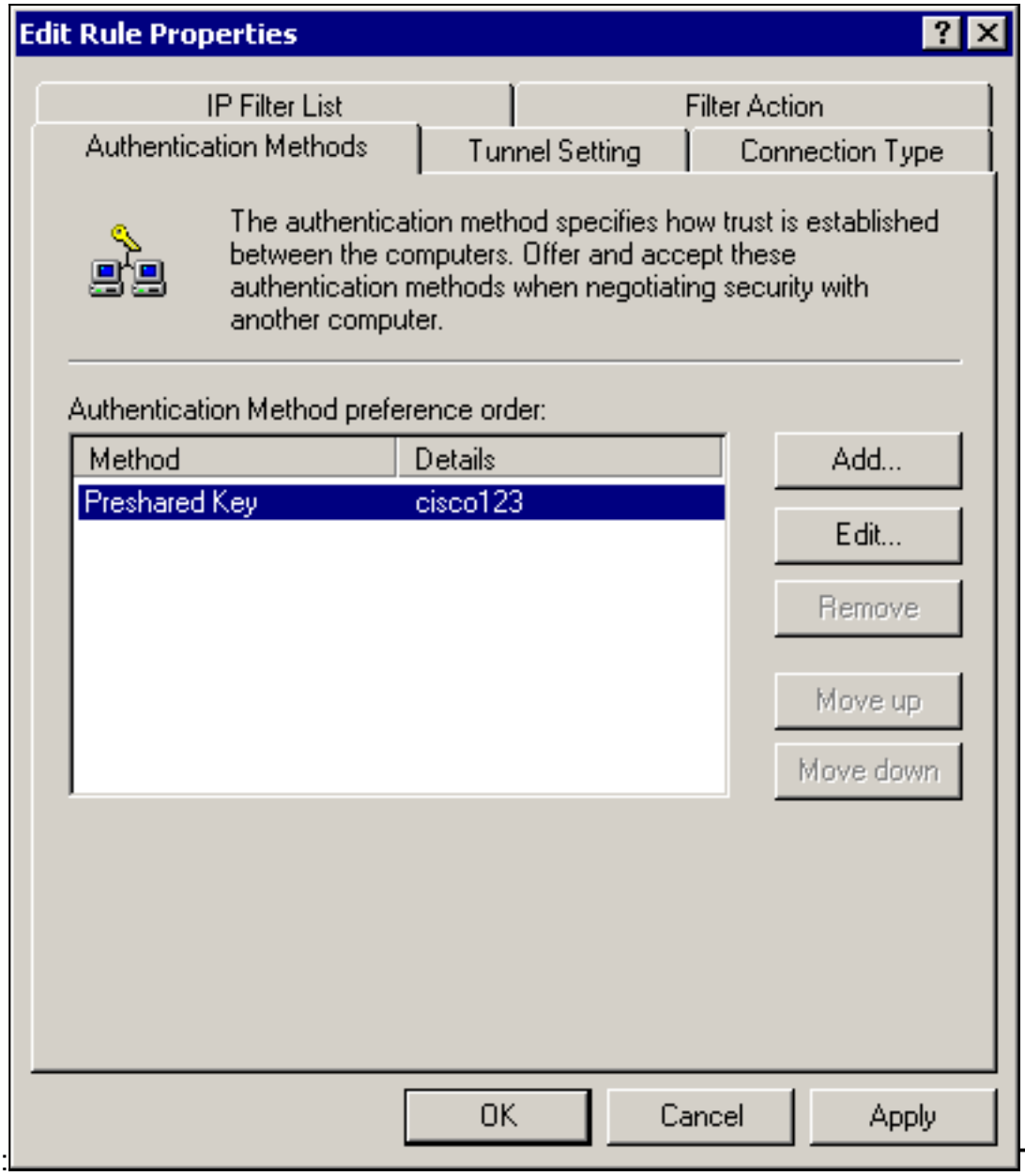
secondi):

5. La scheda **Generale > Avanzate > Metodi** della regola contiene il **metodo di crittografia IKE** (DES), l'**hashing IKE** (SHA1) e il gruppo **Diffie-Helman**

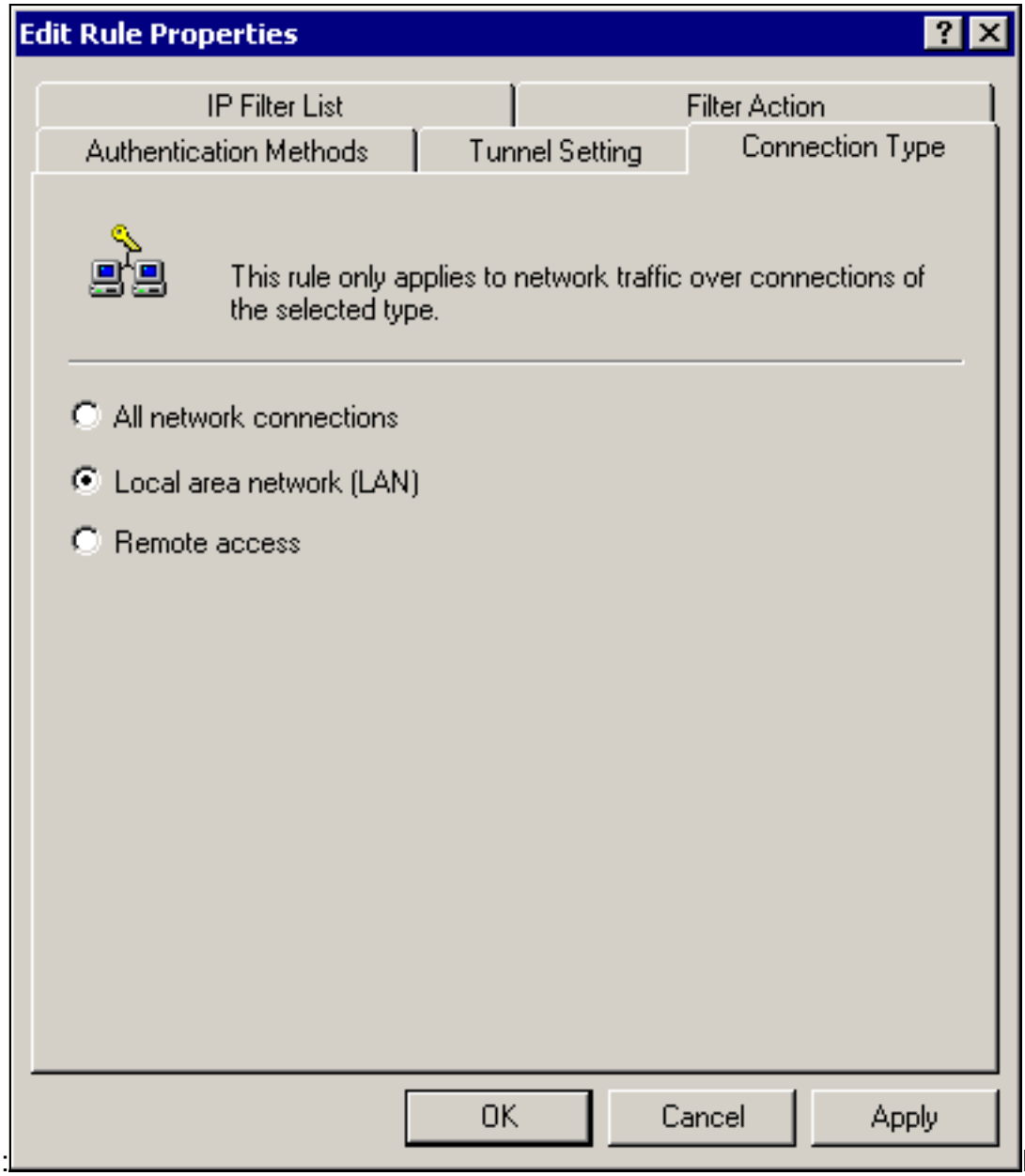


(Low(1)):

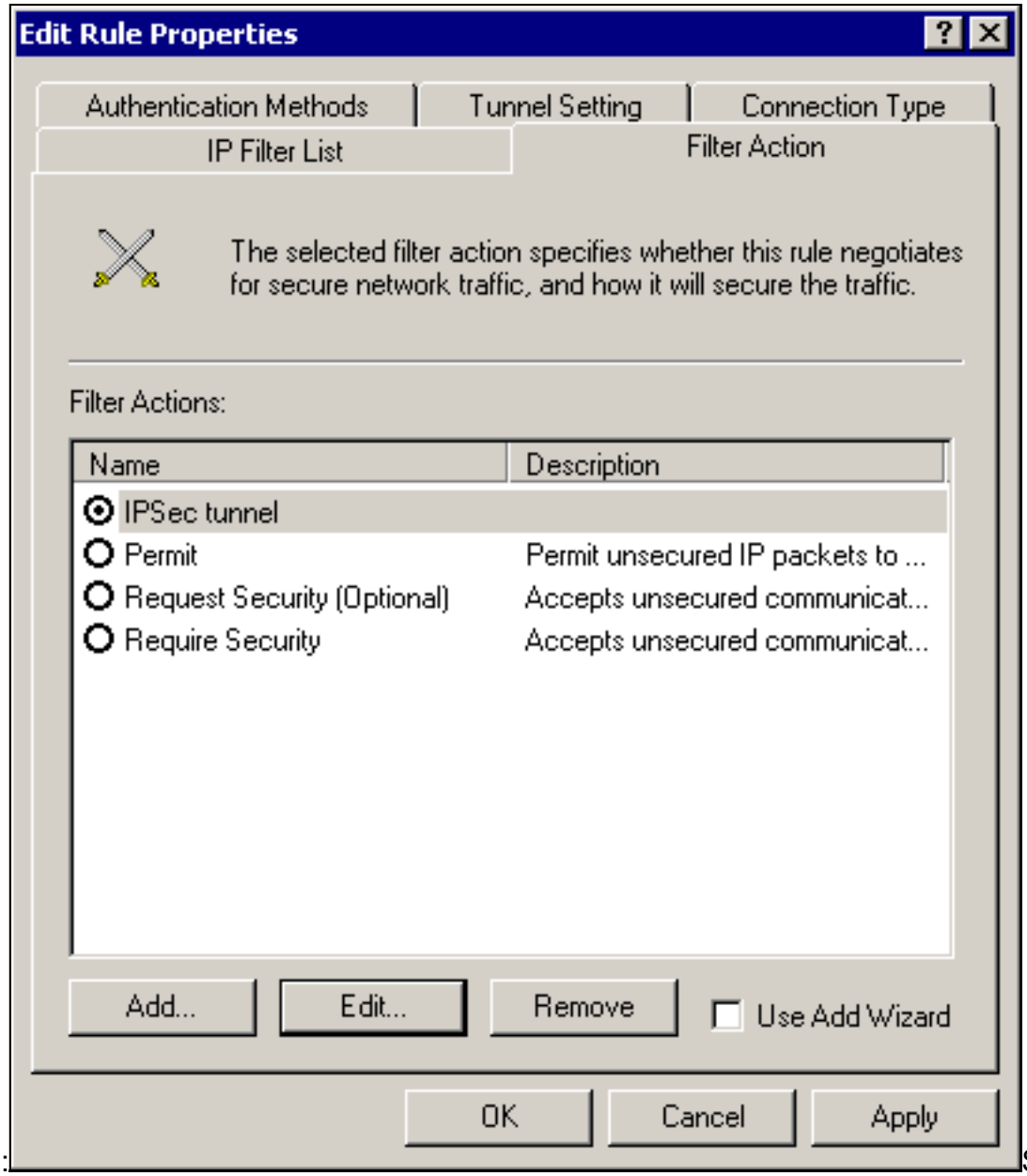
6. Ogni filtro dispone di 5 schede:**Metodi di autenticazione** (chiavi già condivise per IKE [Internet Key



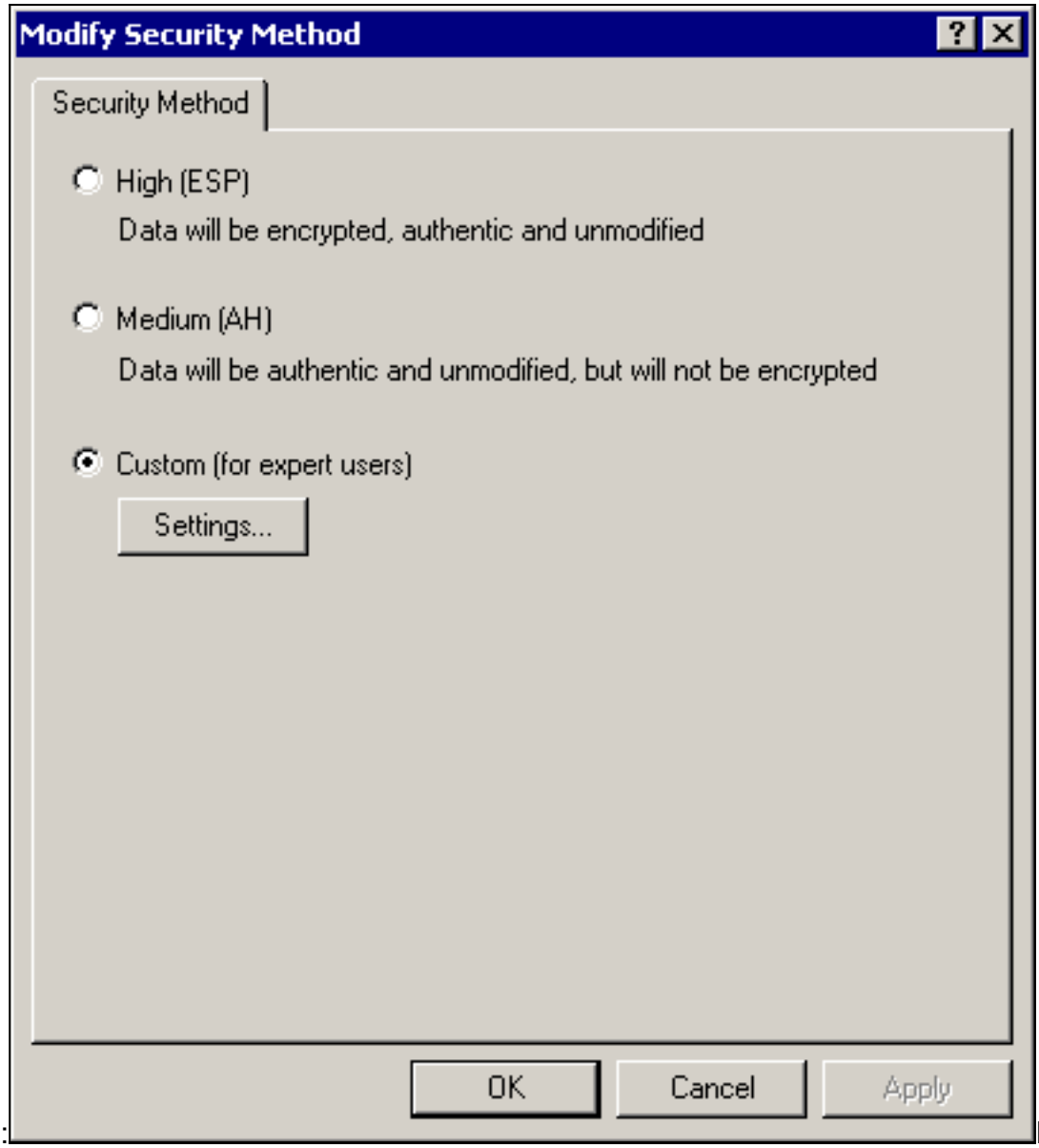
Exchange]): **Tipo di connessione**



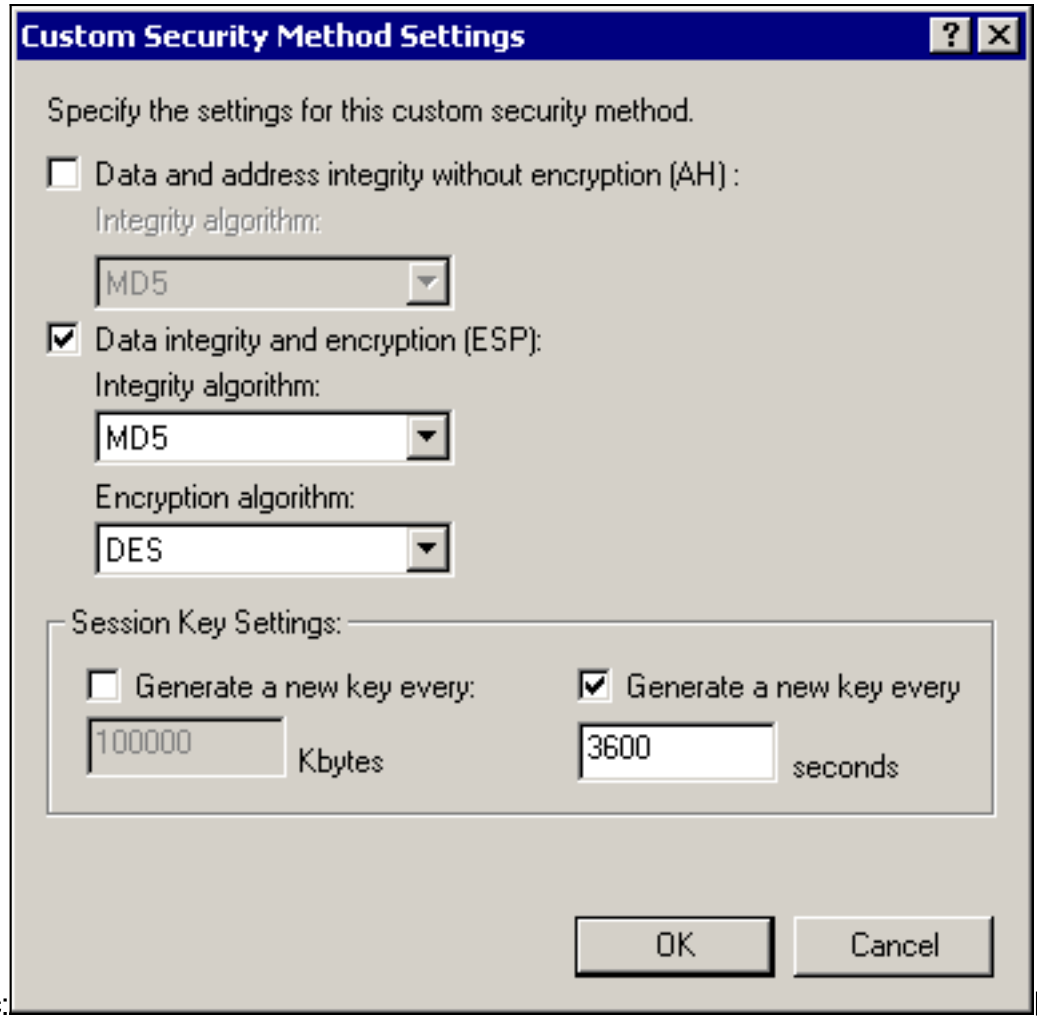
(LAN): IPSec (**Filter**



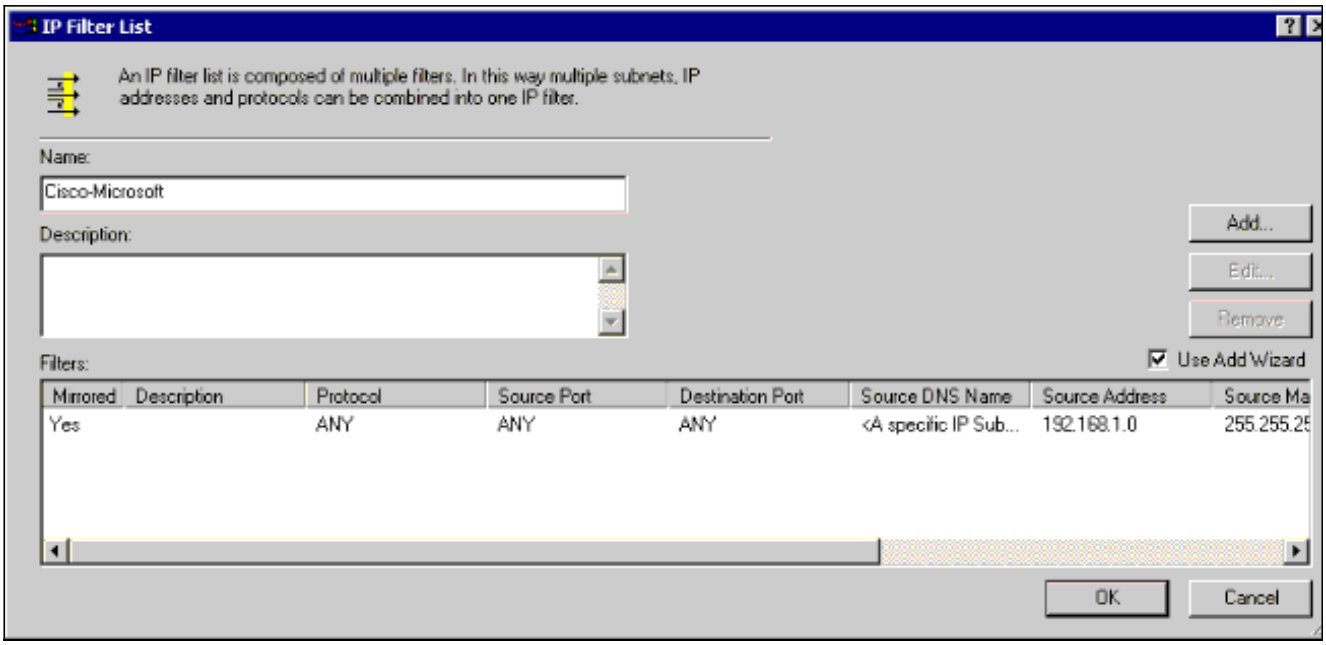
Action):Selezionare **Operazione filtro > Tunnel IPSec > Modifica > Modifica**, quindi fare clic su



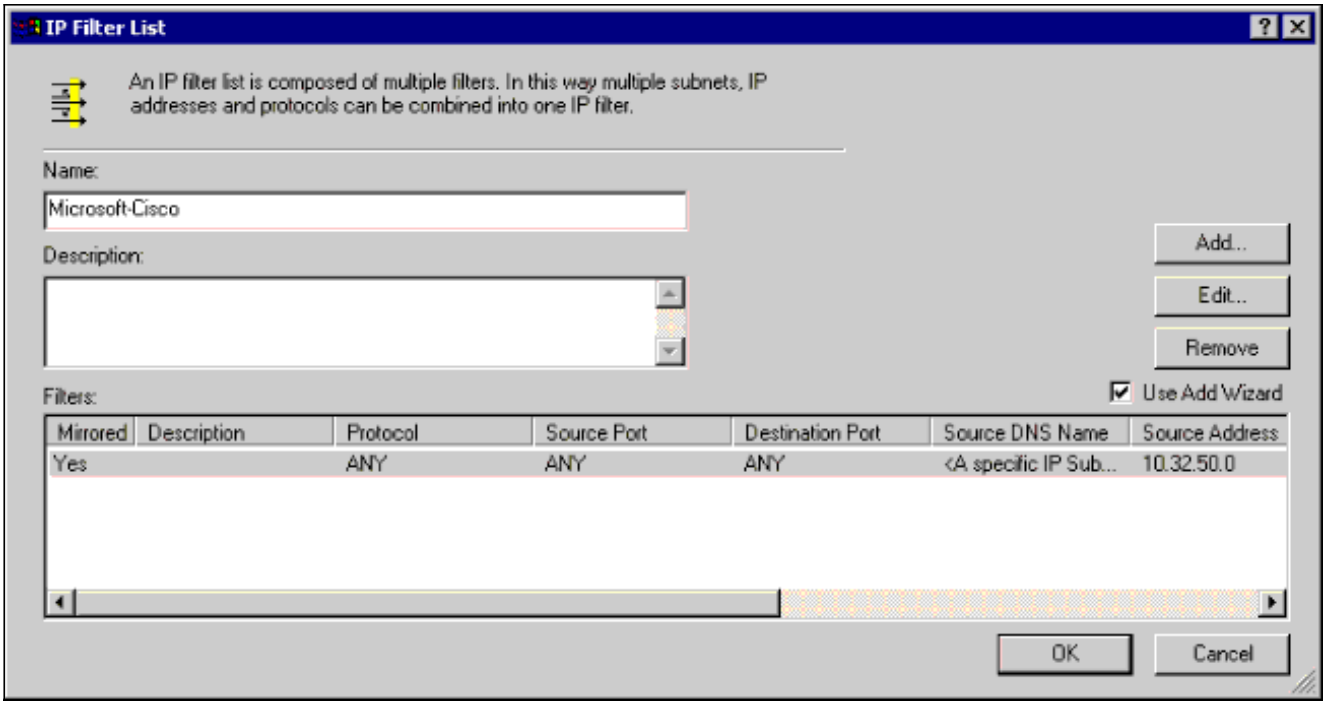
Personalizzato: F
are clic su **Impostazioni - Trasformazioni IPSec** e **Durata**



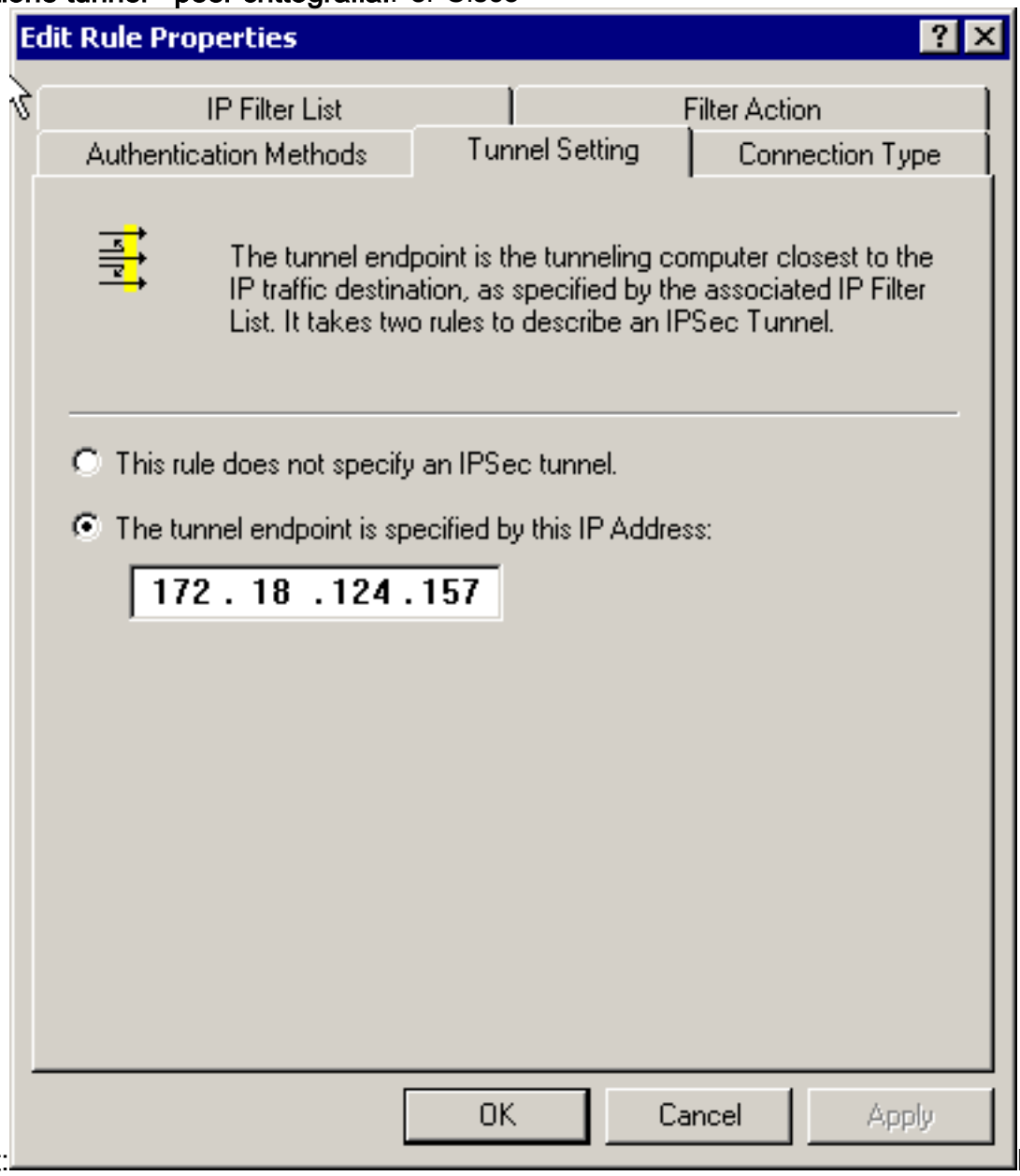
IPSec: **Elenco filtri IP** - reti di **origine** e **destinazione** da crittografare:Per Cisco-Microsoft:



Per Microsoft-Cisco:

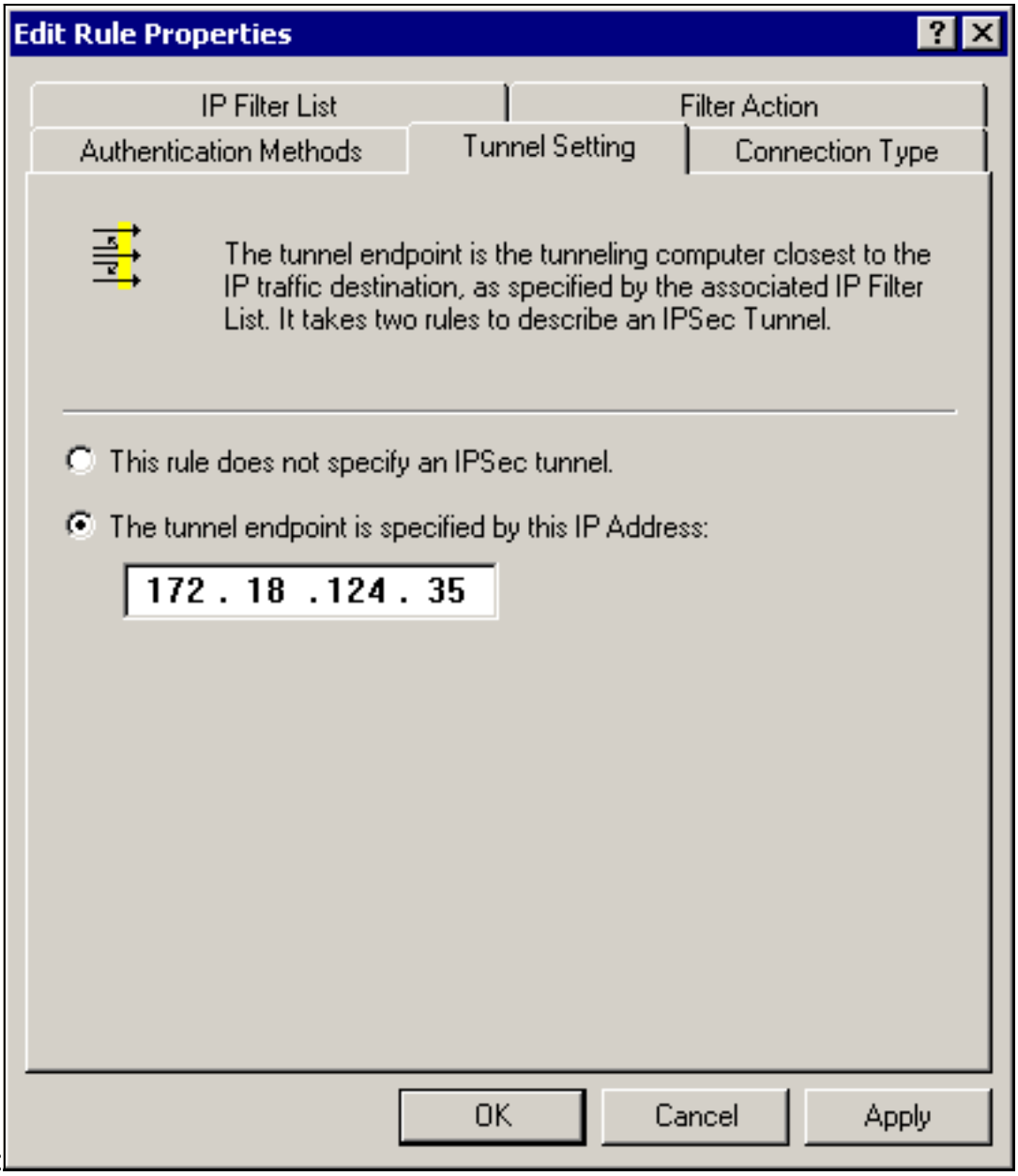


Impostazione tunnel - peer crittografia: Per Cisco-



Microsoft:Per

Microsoft-Cisco:



Configurazione dei dispositivi Cisco

Configurare i Cisco router, PIX e VPN concentrator come mostrato negli esempi seguenti.

- Cisco 3640 Router
- PIX
- VPN 3000 Concentrator
- VPN 5000 Concentrator

Configurazione del router Cisco 3640

Cisco 3640 Router
Current configuration : 1840 bytes ! version 12.1 no service single-slot-reload-enable service timestamps debug uptime

```
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
!
call rsvp-sync
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
!
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
```

```
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

Configurazione di PIX

PIX

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 255.255.255.0 10.32.50.0
255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
!--- Except Source/Destination from Network Address
Translation (NAT): nat (inside) 0 access-list 115
route outside 0.0.0.0 0.0.0.0 172.18.124.36 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
```

```
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPSec transforms crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- IPSec lifetime crypto ipsec security-association
lifetime seconds 3600
crypto map rtpmap 10 ipsec-isakmp
!--- Source/Destination networks crypto map rtpmap 10
match address 115
!--- Encryption peer crypto map rtpmap 10 set peer
172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap interface outside
isakmp enable outside
!--- Encryption peer isakmp key ******** address
172.18.124.157 netmask 255.255.255.240
isakmp identity address
!--- Authentication method isakmp policy 10
authentication pre-share
!--- IKE encryption method isakmp policy 10 encryption
des
!--- IKE hashing isakmp policy 10 hash sha
!--- Diffie-Hellman group isakmp policy 10 group 1
!--- IKE lifetime isakmp policy 10 lifetime 28800
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08
: end
```

Configurazione di VPN 3000 Concentrator

Utilizzare le opzioni di menu e i parametri mostrati di seguito per configurare VPN Concentrator in base alle esigenze.

- Per aggiungere una proposta IKE, selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec > Proposte IKE > Aggiungi proposta.**

  ```
  Proposal Name = DES-SHA
  !--- Authentication method Authentication Mode = Preshared Keys !--- IKE hashing
  Authentication Algorithm = SHA/HMAC-160 !--- IKE encryption method Encryption Algorithm =
  DES-56 !--- Diffie-Hellman group Diffie Hellman Group = Group 1 (768-bits) Lifetime
  Measurement = Time Date Lifetime = 10000 !--- IKE lifetime Time Lifetime = 28800
  ```

- Per definire il tunnel da LAN a LAN, selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec da LAN a LAN.**

  ```
  Name = to_2000
  Interface = Ethernet 2 (Public) 172.18.124.35/28
  !--- Encryption peer Peer = 172.18.124.157 !--- Authentication method Digital Certs = none
  (Use Pre-shared Keys) Pre-shared key = cisco123 !--- IPSec transforms Authentication =
  ESP/MD5/HMAC-128 Encryption = DES-56 !--- Use the IKE proposal IKE Proposal = DES-SHA
  Autodiscovery = off !--- Source network defined Local Network Network List = Use IP
  Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 !---
  ```

```
Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below
IP Address 10.32.50.0 Wildcard Mask 0.0.0.255
```

- Per modificare l'associazione di protezione, selezionare **Configurazione > Gestione criteri > Gestione traffico > Associazioni di protezione > Modifica.**

```
SA Name = L2L-to_2000
Inheritance = From Rule
IPSec Parameters
!--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm =
DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime
= 10000 !--- IPSec lifetime Time Lifetime = 3600 Ike Parameters !--- Encryption peer IKE
Peer = 172.18.124.157 Negotiation Mode = Main !--- Authentication method Digital Certificate
= None (Use Preshared Keys) !--- Use the IKE proposal IKE Proposal DES-SHA
```

Configurazione di VPN 5000 Concentrator

VPN 5000 Concentrator

```
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35

[ General ]
IPSecGateway = 172.18.124.36
DeviceName = "cisco"
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console

[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 192.168.1.1

[ Tunnel Partner VPN 1 ]
 !--- Encryption peer Partner = 172.18.124.157 !---
IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet
1:0" !--- Authentication method SharedKey = "cisco123"
KeyManage = Auto !--- IPSec transforms Transform =
esp(md5,des) Mode = Main !--- Destination network
defined Peer = "10.32.50.0/24" !--- Source network
defined LocalAccess = "192.168.1.0/24" [ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1 [ IP VPN 1 ] Mode =
Routed Numbered = Off [ IKE Policy ] !--- IKE hashing,
encryption, Diffie-Hellman group Protection = SHA_DES_G1
Configuration size is 1088 out of 65500 bytes.
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alle configurazioni.

Comandi per la risoluzione dei problemi

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

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

Cisco 3640 Router

- **debug crypto engine**: visualizza i messaggi di debug sui motori di crittografia, che eseguono la crittografia e la decrittografia.
- **debug crypto isakmp**: visualizza i messaggi relativi agli eventi IKE.
- **debug crypto ipsec** - Visualizza gli eventi IPSec.
- **show crypto isakmp sa**: visualizza tutte le associazioni di sicurezza IKE correnti in un peer.
- **show crypto ipsec sa**: visualizza le impostazioni utilizzate dalle associazioni di sicurezza correnti.
- **clear crypto isakmp** - (dalla modalità di configurazione) Cancella tutte le connessioni IKE attive.
- **clear crypto sa** - (dalla modalità di configurazione) Elimina tutte le associazioni di protezione IPSec.

PIX

- **debug crypto ipsec**: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp**: visualizza le negoziazioni ISAKMP (Internet Security Association and Key Management Protocol) della fase 1.
- **debug crypto engine**: visualizza il traffico crittografato.
- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.
- **clear crypto isakmp** - (dalla modalità di configurazione) Cancella le associazioni di protezione IKE (Internet Key Exchange).
- **clear crypto ipsec sa** - (dalla modalità di configurazione) Cancella le associazioni di protezione IPSec.

VPN 3000 Concentrator

- - Avviare il debug di VPN 3000 Concentrator selezionando **Configurazione > Sistema > Eventi > Classi > Modifica** (gravità da registro=1-13, gravità da console=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - Il registro eventi può essere cancellato o recuperato selezionando **Monitoraggio > Registro eventi**.
- - Il traffico del tunnel LAN-LAN può essere monitorato in **Monitoraggio > Sessioni**.
- - Il tunnel può essere cancellato in **Amministrazione > Amministra sessioni > Sessioni LAN-to-LAN > Azioni - Disconnessione.**

VPN 5000 Concentrator

- **vpn trace dump all**: visualizza le informazioni su tutte le connessioni VPN corrispondenti, incluse le informazioni sull'ora, il numero VPN, l'indirizzo IP reale del peer, gli script eseguiti e, in caso di errore, la routine e il numero di riga del codice software in cui si è verificato l'errore.
- **show vpn statistics**: visualizza le informazioni seguenti per Users, Partners e il totale per entrambi. Per i modelli modulari, il display include una sezione per ogni slot del modulo. Corrente attiva - Le connessioni attive correnti. In Negot - Connessioni attualmente in fase di negoziazione. High Water - Numero massimo di connessioni attive simultanee dall'ultimo riavvio. Totale in esecuzione: il numero totale di connessioni riuscite dall'ultimo riavvio. Avvio del tunnel: numero di avvii del tunnel. Tunnel OK: il numero di tunnel per i quali non sono stati rilevati errori. Errore tunnel: numero di tunnel con errori.
- **show vpn statistics verbose**: visualizza le statistiche di negoziazione ISAKMP e molte altre statistiche di connessione attive.

Informazioni correlate

- Cisco VPN serie 5000 concentrator: annuncio di fine vendita
- Configurazione di IPSec Network Security
- Configurazione del protocollo di protezione di Internet Key Exchange
- Supporto tecnico – Cisco Systems