

Configurazione del firewall PIX e dei client VPN con PPTP, MPPE e IPSec

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Cisco VPN 3000 Client 2.5.x o Cisco VPN Client 3.x e 4.x](#)

[Installazione di Windows 98/2000/XP PPTP Client](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Comandi per la risoluzione dei problemi](#)

[Problemi correlati a Microsoft](#)

[Informazioni correlate](#)

[Introduzione](#)

In questa configurazione di esempio, quattro tipi diversi di client connettono e crittografano il traffico con Cisco Secure PIX Firewall come endpoint del tunnel:

- Utenti che eseguono Cisco Secure VPN Client 1.1 su Microsoft Windows 95/98/NT
- Utenti che eseguono Cisco Secure VPN 3000 Client 2.5.x su Windows 95/98/NT
- Utenti che eseguono client PPTP (Point-to-Point Tunneling Protocol) Windows 98/2000/XP nativi
- Utenti che eseguono Cisco VPN Client 3.x/4.x su Windows 95/98/NT/2000/XP

Nell'esempio, viene configurato un singolo pool per IPsec e PPTP. Tuttavia, i pool possono anche essere separati.

[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:

- Software PIX release 6.3.3
- Cisco Secure VPN Client 1.1
- Cisco VPN 3000 Client versione 2.5
- Cisco VPN Client 3.x e 4.x
- Client Microsoft Windows 2000 e Windows 98

Nota: questo è stato testato sul software PIX versione 6.3.3 ma dovrebbe funzionare sulle versioni 5.2.x e 5.3.1. Il software PIX versione 6.x è richiesto per Cisco VPN Client 3.x e 4.x. Il supporto per Cisco VPN 3000 Client 2.5 è stato aggiunto al software PIX versione 5.2.x. La configurazione funziona anche per il software PIX versione 5.1.x, ad eccezione della parte client Cisco VPN 3000.) È necessario configurare IPsec e PPTP/MPPE (Microsoft Point-to-Point Encryption) in modo che funzionino separatamente. Se non lavorano separatamente, non possono interagire.

Nota: PIX 7.0 utilizza il comando **inspect rpc** per gestire i pacchetti RPC. Il comando [inspect sunrpc](#) attiva o disattiva l'ispezione delle applicazioni per il protocollo Sun RPC. I servizi Sun RPC possono essere eseguiti su qualsiasi porta del sistema. Quando un client tenta di accedere a un servizio RPC su un server, deve individuare la porta su cui viene eseguito il servizio specifico. A tale scopo, eseguire una query sul processo portmapper sul numero di porta conosciuto 111. Il client invia il numero di programma RPC del servizio e recupera il numero di porta. A partire da questo punto, il programma client invia le query RPC alla nuova porta.

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.

[Convenzioni](#)

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

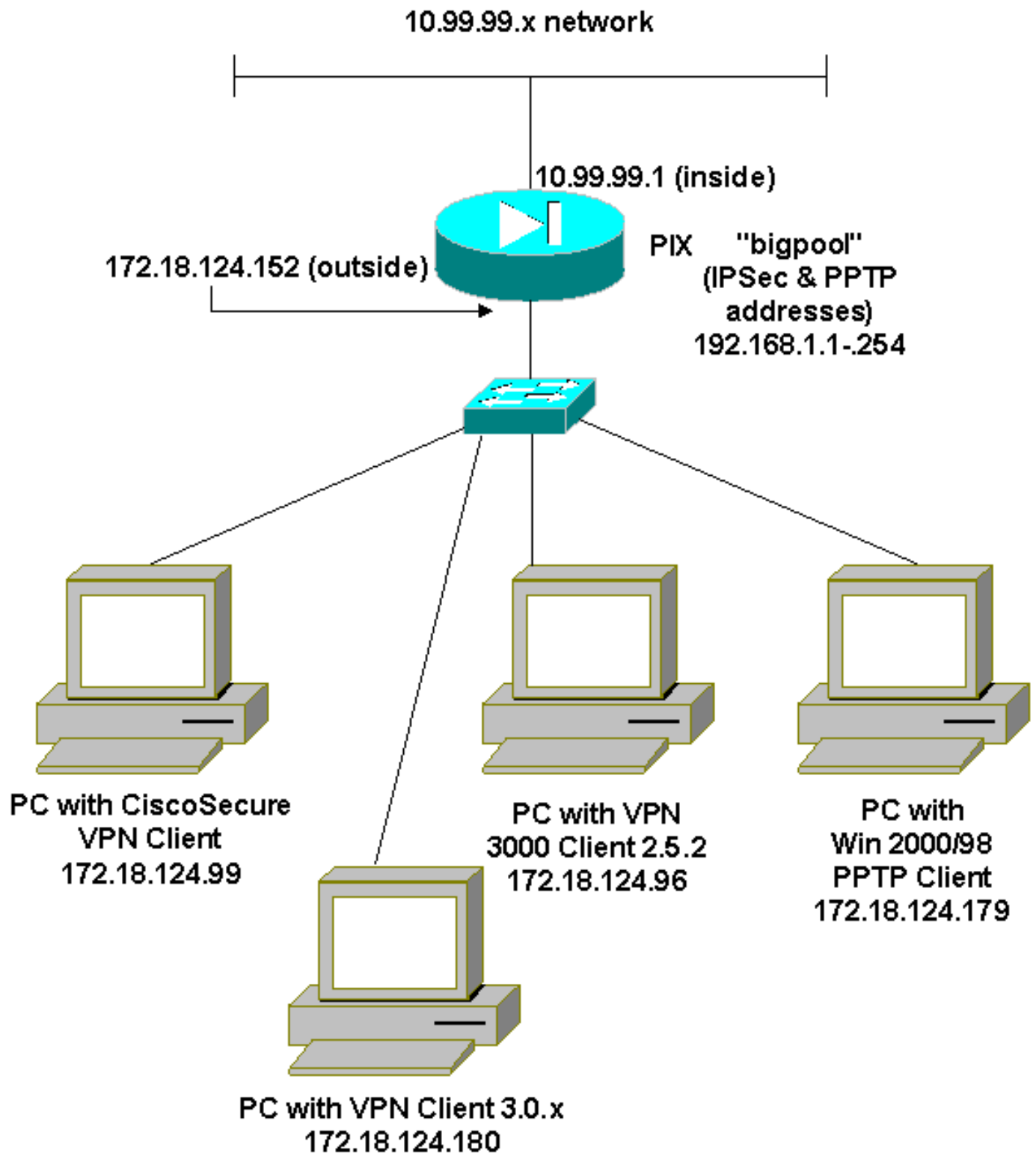
[Configurazione](#)

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](#)).

[Esempio di rete](#)

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate queste configurazioni.

- [Cisco Secure PIX Firewall](#)
- [Cisco Secure VPN Client 1.1](#)

Cisco Secure PIX Firewall

```
PIX Version 6.3(3)
interface ethernet0 auto
```

```
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname goss-515A
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names
access-list 101 permit ip 10.99.99.0 255.255.255.0
192.168.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.152 255.255.255.0
ip address inside 10.99.99.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool bigpool 192.168.1.1-192.168.1.254
pdm history enable
arp timeout 14400
nat (inside) 0 access-list 101
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 uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
sysopt connection permit-pptp
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
!--- Cisco Secure_VPNClient_key. isakmp key *****
address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local bigpool
outside

!--- ISAKMP Policy for Cisco VPN Client 2.5 or !---
Cisco Secure VPN Client 1.1. isakmp policy 10
authentication pre-share
```

```

isakmp policy 10 encryption des
isakmp policy 10 hash md5

!--- The 1.1 and 2.5 VPN Clients use Diffie-Hellman (D-
H) !--- group 1 policy (PIX default). isakmp policy 10
group 1
isakmp policy 10 lifetime 86400

!--- ISAKMP Policy for VPN Client 3.0 and 4.0. isakmp
policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5

!--- The 3.0/4.0 VPN Clients use D-H group 2 policy !---
and PIX 6.0 code. isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup vpn3000-all address-pool bigpool
vpngroup vpn3000-all dns-server 10.99.99.99
vpngroup vpn3000-all wins-server 10.99.99.99
vpngroup vpn3000-all default-domain password
vpngroup vpn3000-all idle-time 1800

!--- VPN 3000 group_name and group_password. vpngroup
vpn3000-all password *****
telnet timeout 5
ssh timeout 5
console timeout 0
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe auto
vpdn group 1 client configuration address local bigpool
vpdn group 1 pptp echo 60
vpdn group 1 client authentication local

!--- PPTP username and password. vpdn username cisco
password *****
vpdn enable outside
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
goss-515A#

```

Cisco Secure VPN Client 1.1

```

1- TACconn
  My Identity
    Connection security: Secure
    Remote Party Identity and addressing
    ID Type: IP subnet
    10.99.99.0
    255.255.255.0
    Port all Protocol all

  Connect using secure tunnel
    ID Type: IP address
    172.18.124.152

  Pre-shared Key=CiscoSecure_VPNClient_key

  Authentication (Phase 1)
  Proposal 1

```

```
Authentication method: pre-shared key
Encryp Alg: DES
Hash Alg: MD5
SA life: Unspecified
Key Group: DH 1
```

```
Key exchange (Phase 2)
Proposal 1
Encapsulation ESP
Encrypt Alg: DES
Hash Alg: MD5
Encap: tunnel
SA life: Unspecified
no AH
```

```
2- Other Connections
Connection security: Non-secure
Local Network Interface
Name: Any
IP Addr: Any
Port: All
```

[Cisco VPN 3000 Client 2.5.x o Cisco VPN Client 3.x e 4.x](#)

Selezionare **Opzioni > Proprietà > Autenticazione**. Il nome del gruppo e la password del gruppo corrispondono al nome_gruppo e alla password_del_gruppo sul PIX come mostrato nella:

```
vpngroup vpn3000-all password *****
Host-name = 172.18.124.152
```

[Installazione di Windows 98/2000/XP PPTP Client](#)

È possibile contattare il fornitore che crea il client PPTP. Per informazioni su come configurare questa funzionalità, consultare il documento sulla [configurazione di Cisco Secure PIX Firewall per l'utilizzo di PPTP](#).

[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 alla configurazione.

[Comandi per la risoluzione dei problemi](#)

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

Nota: consultare le [informazioni importanti sui comandi di debug](#) prima di usare i comandi di **debug**.

[Debug 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.

[Debug PIX PPTP](#)

- **debug ppp io**: visualizza le informazioni sul pacchetto per l'interfaccia virtuale PPTP PPP.
- **debug ppp error**: visualizza i messaggi di errore dell'interfaccia virtuale PPTP PPP.
- **debug vpdn error**: visualizza i messaggi di errore del protocollo PPTP.
- **debug vpdn packets**: visualizza le informazioni sui pacchetti PPTP relative al traffico PPTP.
- **debug vpdn events**: visualizza le informazioni sulla modifica degli eventi del tunnel PPTP.
- **debug ppp auth**: visualizza i messaggi di debug dell'autenticazione utente AAA dell'interfaccia virtuale PPTP PPP.

[Problemi correlati a Microsoft](#)

- [Come mantenere attive le connessioni RAS dopo la disconnessione](#) - Quando si esegue la disconnessione da un client di Servizio di accesso remoto Windows (RAS), tutte le connessioni RAS vengono disconnesse automaticamente. Per rimanere connessi dopo la disconnessione, abilitare la chiave KeepRasConnections nel Registro di sistema del client RAS.
- [L'Utente Non Viene Avvisato Quando Accede Con Credenziali Memorizzate Nella Cache](#) —Sintomi - Quando si tenta di accedere a un dominio da una workstation basata su Windows o da un server membro e non è possibile individuare un controller di dominio, non viene visualizzato alcun messaggio di errore. È stato invece eseguito l'accesso al computer locale utilizzando le credenziali memorizzate nella cache.
- [Come scrivere un file LMHOSTS per la convalida del dominio e altri problemi di risoluzione dei nomi](#) —In alcuni casi possono verificarsi problemi di risoluzione dei nomi sulla rete TCP/IP ed è necessario utilizzare i file Lmhosts per risolvere i nomi NetBIOS. In questo articolo viene descritto il metodo corretto per la creazione di un file Lmhosts per semplificare la risoluzione dei nomi e la convalida del dominio.

[Informazioni correlate](#)

- [Pagine di supporto per la negoziazione IPsec/protocolli IKE](#)
- [Informazioni di riferimento sui comandi PIX](#)
- [Cisco PIX serie 500 Security Appliance - Pagina di supporto](#)
- [RFC \(Requests for Comments\)](#)
- [Configurazione della protezione di rete IPsec](#)
- [Configurazione del protocollo di protezione di Internet Key Exchange](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)