

Esempio di configurazione del tunnel IPsec tra i protocolli PIX 7.x e VPN 3000 Concentrator

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione del PIX](#)

[Configurazione di VPN 3000 Concentrator](#)

[Verifica](#)

[Verificare il PIX](#)

[Verificare VPN 3000 Concentrator](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi relativi a PIX](#)

[Risoluzione dei problemi di VPN 3000 Concentrator](#)

[PFS](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene fornita una configurazione di esempio per come stabilire un tunnel VPN IPsec da LAN a LAN tra un firewall PIX 7.x e un concentratore Cisco VPN 3000.

Per ulteriori informazioni sullo scenario in cui il tunnel LAN-LAN tra i PIX consente anche a un client VPN di accedere al PIX spoke tramite il PIX dell'hub, fare riferimento all'[esempio di configurazione dell'autenticazione TACACS+ 7.x Enhanced Spoke-to-Client VPN](#) con autenticazione TACACS+.

Per ulteriori informazioni sullo scenario in cui il tunnel LAN-LAN tra il PIX/ASA e un router IOS, fare riferimento all'[esempio di configurazione del tunnel IPsec da LAN a LAN di un'appliance di sicurezza PIX/ASA 7.x su un router IOS](#).

[Prerequisiti](#)

[Requisiti](#)

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

- Questo documento richiede una comprensione di base del protocollo IPsec. per ulteriori informazioni su IPsec, fare riferimento a [Introduzione alla crittografia IPsec](#).

Componenti usati

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

- Cisco PIX serie 500 Security Appliance con software versione 7.1(1)
- Cisco VPN 3060 Concentrator con software versione 4.7.2(B)

Nota: PIX 506/506E non supporta 7.x.

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.

Per configurare il protocollo PIX 6.x, fare riferimento agli [esempi di configurazione del tunnel IPsec da LAN a LAN tra Cisco VPN 3000 Concentrator e PIX Firewall](#).

Convenzioni

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

Configurazione

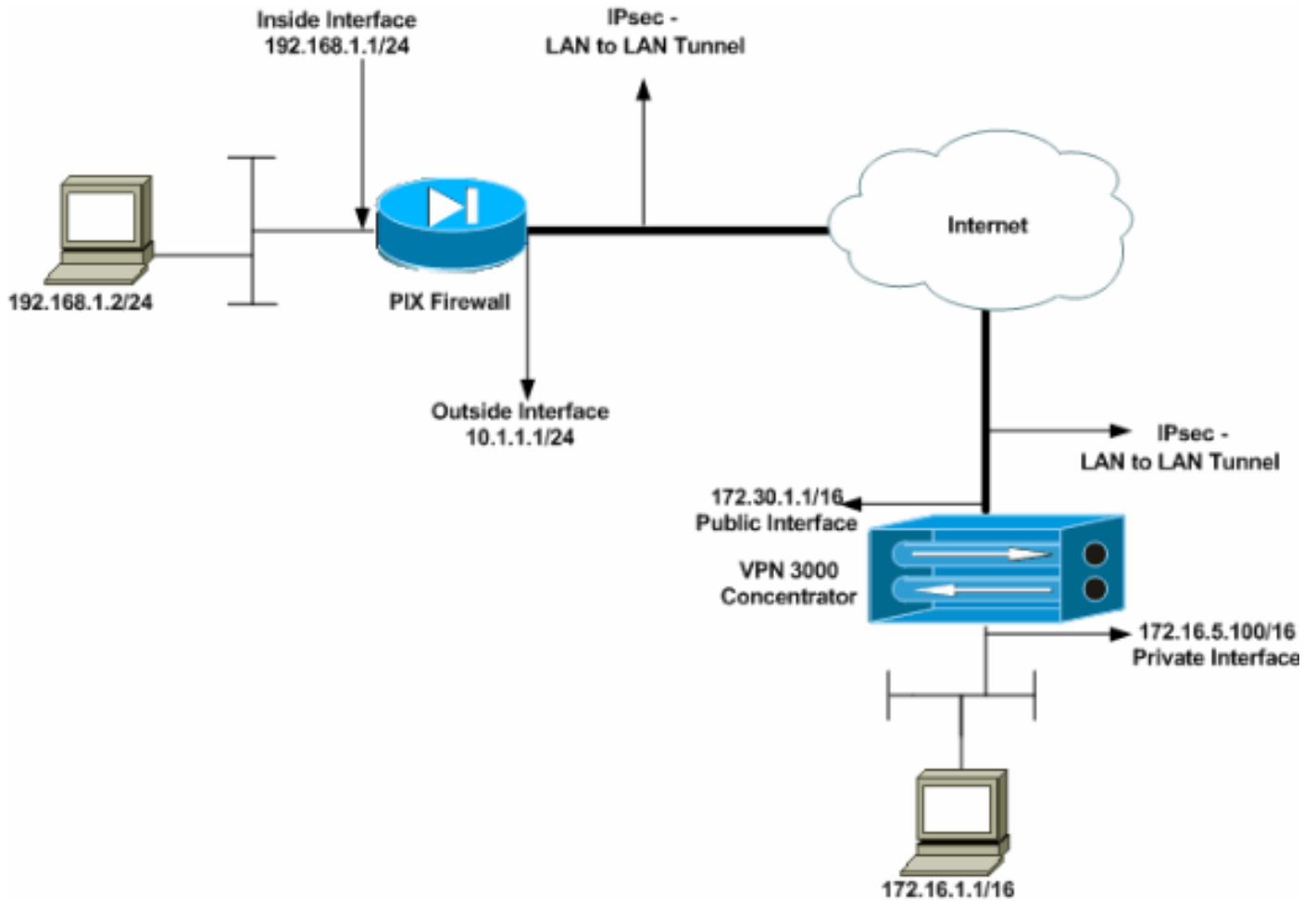
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

- [Configurazione del PIX](#)
- [Configurazione di VPN 3000 Concentrator](#)

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 questa impostazione di rete:



Configurazione del PIX

PIX

```

PIX7#show running-config
: Saved
:
PIX Version 7.1(1)
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside interface of the PIX. !---
By default, the security level for the outside interface
is 0. interface Ethernet0
  nameif outside
  security-level 0
  ip address 10.1.1.1 255.255.255.0
!
!--- Configures the inside interface of the PIX. !--- By
default, the security level for the inside interface is
100. interface Ethernet1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
!--- Defines the IP addresses that should not be NATed.
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any

```

```

!--- Defines the IP addresses that can communicate via
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!--- Output is suppressed. !--- These are the IPsec
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
!--- These are the Phase I parameters negotiated by the
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- A tunnel group consists of a set of records !---
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-l2l
tunnel-group 172.30.1.1 ipsec-attributes
pre-shared-key *
!--- Output is suppressed. ! : end PIX7#

```

Configurazione di VPN 3000 Concentrator

I concentratori VPN non sono pre-programmati con indirizzi IP nelle impostazioni di fabbrica. È necessario usare la porta della console per configurare le configurazioni iniziali che sono un'interfaccia della riga di comando (CLI) basata su menu. Per informazioni su come configurare i concentratori VPN tramite la console, consultare il documento sulla [configurazione dei concentratori VPN](#) tramite la console.

Dopo aver configurato l'indirizzo IP sull'interfaccia Ethernet 1 (privata), è possibile configurare il resto con la CLI o tramite l'interfaccia del browser. L'interfaccia del browser supporta sia HTTP che HTTPS su SSL (Secure Sockets Layer).

Questi parametri vengono configurati tramite la console:

- **Ora/data:** la data e l'ora corrette sono molto importanti. Garantiscono l'accuratezza delle voci di registrazione e di accounting e la possibilità di creare un certificato di protezione valido.
- **Ethernet 1 (private) interface:** indirizzo IP e maschera (della topologia di rete 172.16.5.100/16).



VPN Concentrator è ora accessibile tramite un browser HTML dalla rete interna. Per informazioni

su come configurare VPN Concentrator in modalità CLI, consultare il documento sull'[uso dell'interfaccia della riga di comando](#) per la [configurazione rapida](#).

Digitare l'indirizzo IP dell'interfaccia privata dal browser Web per abilitare l'interfaccia GUI.

Fare clic sull'icona **Save needed** (Salva le modifiche necessarie) per salvare le modifiche in memoria. Il nome utente e la password predefiniti sono **admin**, con distinzione tra maiuscole e minuscole.

1. Avviare la GUI e selezionare **Configuration > Interfaces** per configurare l'indirizzo IP dell'interfaccia pubblica e del gateway predefinito.


Configuration | Interfaces Sunday, 19 February 2006 16:54:00
Save Needed  Refresh 

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.5.100	255.255.0.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	172.30.1.1	255.255.0.0	00.03.A0.89.BF.D1	172.30.1.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- [Power Supplies](#)



2. Selezionare **Configurazione > Gestione delle policy > Gestione del traffico > Elenchi di rete > Aggiungi o modifica** per creare gli elenchi di rete che definiscono il traffico da crittografare. Aggiungere qui le reti locali e remote. Gli indirizzi IP devono rispecchiare quelli nell'elenco degli accessi configurato sul PIX remoto. Nell'esempio, i due elenchi di reti sono **remote_network** e **VPN Client Local LAN**.

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

3. Selezionare **Configurazione > Sistema > Protocolli di tunneling > IPSec LAN-to-LAN > Aggiungi** per configurare il tunnel LAN-to-LAN IPsec. Al termine, fare clic su **Apply** (Applica). Immettere l'indirizzo IP del peer, gli elenchi delle reti create nel passaggio 2, i parametri IPsec e ISAKMP e la chiave già condivisa. Nell'esempio, l'indirizzo IP del peer è **10.1.1.1**, gli elenchi delle reti sono **rete_remota** e **LAN locale del client VPN** e **cisco** è la chiave già condivisa.

Modify an IPSec LAN-to-LAN connection.

Enable <input checked="" type="checkbox"/>	Check to enable this LAN-to-LAN connection.
Name <input type="text" value="Test"/>	Enter the name for this LAN-to-LAN connection.
Interface <input type="text" value="Ethernet 2 (Public) (172.30.1.1)"/>	Select the interface for this LAN-to-LAN connection.
Connection Type <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
Peers <input type="text" value="10.1.1.1"/>	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.
Digital Certificate <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key <input type="text" value="cisco"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication <input type="text" value="ESP/SHA/HMAC-160"/>	Specify the packet authentication mechanism to use.
Encryption <input type="text" value="AES-256"/>	Specify the encryption mechanism to use.
IKE Proposal <input type="text" value="IKE-AES256-SHA"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List <input type="text" value="VPN Client Local LAN (Default)"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List <input type="text" value="remote_network"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	

- Selezionare **Configurazione > Gestione utente > Gruppi > Modifica 10.1.1.1** per visualizzare le informazioni sul gruppo generate automaticamente. **Nota:** non modificare queste impostazioni di gruppo.

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	10.1.1.1	Enter a unique name for the group.
Password	XXXXXXXXXX	Enter the password for the group.
Verify	XXXXXXXXXX	Verify the group's password.
Type	Internal	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Apply Cancel

Verifica

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

- [Verificare il PIX](#)
- [Verificare VPN 3000 Concentrator](#)

Verificare il PIX

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 isakmp sa](#): visualizza tutte le associazioni di sicurezza (SA) IKE correnti in un peer. Lo stato MM_ACTIVE indica che viene utilizzata la modalità principale per configurare il tunnel VPN IPsec. In questo esempio il firewall PIX avvia la connessione IPsec. L'indirizzo IP del peer è 172.30.1.1 e utilizza la modalità principale per stabilire la connessione.

```
PIX7#show 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: 172.30.1.1
   Type    : L2L                Role    : initiator
   Rekey   : no                State   : MM_ACTIVE
```

- [show ipsec sa](#): visualizza le impostazioni utilizzate dalle associazioni di protezione correnti. Verificare gli indirizzi IP dei peer, le reti accessibili sia a livello locale che remoto e il set di trasformazioni utilizzato. Esistono due associazioni di protezione ESP, una per ogni direzione.

```
PIX7#show ipsec sa
```

```
interface: outside
Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
```


current_peer: 172.30.1.1

```
#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: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
```

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

```
path mtu 1500, ipsec overhead 76, media mtu 1500
current outbound spi: 136580F6
```

inbound esp sas:

```
spi: 0xF24F4675 (4065281653)
transform: esp-aes-256 esp-sha-hmac
in use settings ={L2L, Tunnel,}
slot: 0, conn_id: 1, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (3824999/28747)
IV size: 16 bytes
replay detection support: Y
```

outbound esp sas:

```
spi: 0x136580F6 (325419254)
transform: esp-aes-256 esp-sha-hmac
in use settings ={L2L, Tunnel,}
slot: 0, conn_id: 1, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (3824999/28745)
IV size: 16 bytes
replay detection support: Y
```

Per ripristinare il tunnel, usare i comandi [clear ipsec sa](#) e [clear isakmp sa](#).

[Verificare VPN 3000 Concentrator](#)

Selezionare **Monitoraggio > Statistiche > IPSec** per verificare se il tunnel è arrivato nel concentratore VPN 3000. Contiene le statistiche per entrambi i parametri IKE e IPsec.

IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	5720
Sent Bytes	5576
Received Packets	57
Sent Packets	56
Received Packets Dropped	0
Sent Packets Dropped	0
Received Notifies	52
Sent Notifies	104
Received Phase-2 Exchanges	1
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	0
Phase-2 SA Delete Requests Sent	0
Initiated Tunnels	0
Failed Initiated Tunnels	0
Failed Remote Tunnels	0
Authentication Failures	0
Decryption Failures	0
Hash Validation Failures	0
System Capability Failures	0
No-SA Failures	0

IPsec (Phase 2) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	448
Sent Bytes	448
Received Packets	4
Sent Packets	4
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	4
Failed Inbound Authentications	0
Outbound Authentications	4
Failed Outbound Authentications	0
Decryptions	4
Failed Decryptions	0
Encryptions	4
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

È possibile monitorare attivamente la sessione in **Monitoraggio > Sessioni**. È possibile ripristinare il tunnel IPsec qui.

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group

Session Summary

Active LAN-to-LAN Sessions since Stats Reset	Active Remote Access Sessions since Stats Reset	Active Management Sessions since Stats Reset	Total Active Sessions since Stats Reset	Peak Concurrent Sessions since Stats Reset	Weighted Active Load since Stats Reset	Percent Session Load since Stats Reset	Concurrent Sessions Limit	Total Cumulative Sessions since Stats Reset
1	0	0	1	0	1	1.00%	100	2

NAC Session Summary

Accepted since Stats Reset		Rejected since Stats Reset		Exempted since Stats Reset		Non-responsive since Stats Reset		Hold-off since Stats Reset		N/A since Stats Reset	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions

[[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Test	10.1.1.1	IPSec/LAN-to-LAN	AES-256	Feb 19 17:02:01	0:06:02	448	448

Remote Access Sessions

[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
No Remote Access Sessions							

Management Sessions

[[LAN-to-LAN Sessions](#) | [Remote Access Sessions](#)]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	172.16.1.1	HTTP	3DES-168 SSLv3	Jan 01 05:45:00	0:11:30

Risoluzione dei problemi

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

- [Risoluzione dei problemi relativi a PIX](#)
- [Risoluzione dei problemi di VPN 3000 Concentrator](#)
- [PFS](#)

Risoluzione dei problemi relativi a PIX

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.

I comandi **debug** su PIX per i tunnel VPN sono:

- [debug crypto isakmp](#): esegue il debug delle negoziazioni della SA ISAKMP.
- [debug crypto ipsec](#): esegue il debug delle negoziazioni della SA IPsec.

Risoluzione dei problemi di VPN 3000 Concentrator

Analogamente ai comandi di debug sui router Cisco, è possibile configurare le classi di evento per visualizzare tutti gli allarmi. Selezionare **Configurazione > Sistema > Eventi > Classi > Aggiungi** per attivare la registrazione delle classi di evento.

Selezionare **Monitoraggio > Registro eventi filtrabili** per monitorare gli eventi attivati.

Select Filter Options

Event Class	<input type="text" value="All Classes"/>	Severities	<input type="text" value="ALL"/>
	<input type="text" value="AUTH"/>		<input type="text" value="1"/>
	<input type="text" value="AUTHDBG"/>		<input type="text" value="2"/>
	<input type="text" value="AUTHDECODE"/>		<input type="text" value="3"/>
Client IP Address	<input type="text" value="0.0.0.0"/>	Events/Page	<input type="text" value="100"/>
Group	<input type="text" value="-All-"/>	Direction	<input type="text" value="Oldest to Newest"/>

```

1 02/19/2006 17:17:00.080 SEV-5 IKEDBG/64 RPT-33 10.1.1.1
IKE Peer included IKE fragmentation capability flags:
Main Mode:      True
Aggressive Mode: True

3 02/19/2006 17:17:00.750 SEV-4 IKE/119 RPT-23 10.1.1.1
Group [10.1.1.1]
PHASE 1 COMPLETED

4 02/19/2006 17:17:00.750 SEV-4 AUTH/22 RPT-23 10.1.1.1
User [10.1.1.1] Group [10.1.1.1] connected, Session Type: IPSec/LAN-to-LAN

5 02/19/2006 17:17:00.750 SEV-4 AUTH/84 RPT-23
LAN-to-LAN tunnel to headend device 10.1.1.1 connected

6 02/19/2006 17:17:01.020 SEV-5 IKE/35 RPT-23 10.1.1.1
Group [10.1.1.1]
Received remote IP Proxy Subnet data in ID Payload:
  Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

9 02/19/2006 17:17:01.020 SEV-5 IKE/34 RPT-23 10.1.1.1
Group [10.1.1.1]
Received local IP Proxy Subnet data in ID Payload:
  Address 172.16.0.0, Mask 255.255.0.0, Protocol 0, Port 0

12 02/19/2006 17:17:01.020 SEV-5 IKE/66 RPT-13 10.1.1.1
Group [10.1.1.1]
IKE Remote Peer configured for SA: L2L: Test

13 02/19/2006 17:17:01.350 SEV-4 IKE/49 RPT-3 10.1.1.1
Group [10.1.1.1]
Security negotiation complete for LAN-to-LAN Group (10.1.1.1)
Responder, Inbound SPI = 0x136580f6, Outbound SPI = 0xf24f4675

16 02/19/2006 17:17:01.350 SEV-4 IKE/120 RPT-3 10.1.1.1
Group [10.1.1.1]
PHASE 2 COMPLETED (msgid=6b2795cd)

```

[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 il protocollo PFS su entrambi i peer del tunnel, altrimenti il tunnel IPsec LAN-LAN (L2L) non verrà stabilito nell'appliance 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
```

[Informazioni correlate](#)

- [Cisco PIX serie 500 Security Appliance - Pagina di supporto](#)
- [Cisco VPN serie 3000 Concentrator - Pagina di supporto](#)
- [Cisco PIX serie 500 Security Appliance - Guida di riferimento ai comandi](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)