

Exemple de configuration d'un tunnel IPSec entre PIX 7.x et un concentrateur VPN 3000

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurer le PIX](#)

[Configurer le concentrateur VPN 3000](#)

[Vérification](#)

[Vérifier le PIX](#)

[Vérification du concentrateur VPN 3000](#)

[Dépannage](#)

[Dépannage du PIX](#)

[Dépannage du concentrateur VPN 3000](#)

[PFS](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration pour établir un tunnel VPN IPsec LAN à LAN entre un pare-feu PIX 7.x et un concentrateur VPN Cisco 3000.

Référez-vous à [Exemple de configuration de VPN satellite à client amélioré avec authentification TACACS+ PIX/ASA 7.x](#) afin d'en savoir plus sur le scénario où le tunnel LAN à LAN entre les PIX permet également à un client VPN d'accéder au PIX satellite via le PIX concentrateur.

Référez-vous à [Exemple de configuration de tunnel IPsec LAN à LAN du dispositif de sécurité PIX/ASA 7.x d'un routeur IOS](#) afin d'en savoir plus sur le scénario où le tunnel LAN à LAN entre le PIX/ASA et un routeur IOS.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Ce document exige une connaissance de base du protocole IPSec. Consultez la section [Introduction au chiffrement IPSec pour de plus amples renseignements sur IPSec.](#)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Dispositif de sécurité de la gamme Cisco PIX 500 avec version logicielle 7.1(1)
- Concentrateur VPN Cisco 3060 avec version logicielle 4.7.2(B)

Remarque : PIX 506/506E ne prend pas en charge 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Afin de configurer PIX 6.x, référez-vous à [Exemple de configuration du tunnel IPSec LAN à LAN entre le concentrateur VPN 3000 de Cisco et le pare-feu PIX.](#)

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco.](#)

Configuration

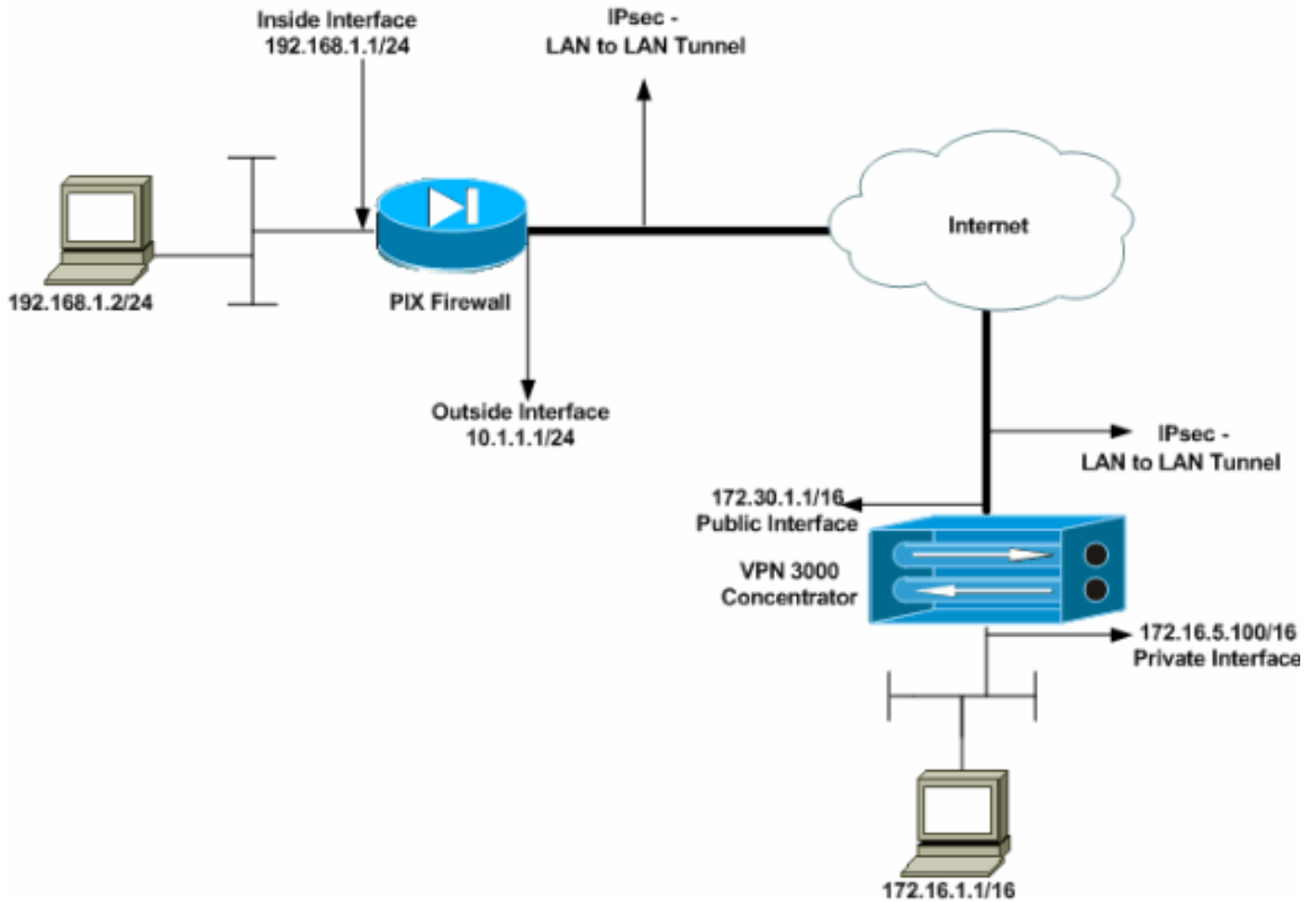
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

- [Configurer le PIX](#)
- [Configurer le concentrateur VPN 3000](#)

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurer le 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#

```

Configurer le concentrateur VPN 3000

Dans leurs paramètres d'usine, les concentrateurs VPN préprogrammés ne comportent aucune adresse IP. Vous devez utiliser le port de console afin de configurer les configurations initiales qui sont une interface de ligne de commande (CLI) basée sur des menus. Pour en savoir plus sur la [configuration des concentrateurs VPN par la console, consultez la section correspondante.](#)

Après avoir configuré l'adresse IP sur l'interface Ethernet 1 (privée), vous pouvez configurer le reste avec l'interface de ligne de commande ou via l'interface du navigateur. L'interface du navigateur prend en charge les protocoles HTTP et HTTPS sur SSL (Secure Socket Layer).

Les paramètres suivants sont configurés par la console :

- **Heure/Date** : l'heure et la date correctes sont très importantes. Elles permettent l'exactitude des entrées de journalisation et de gestion des comptes et la création par le système d'un certificat de sécurité valide.
- **Interface Ethernet 1 (privée)** : adresse IP et masque (de la topologie réseau 172.16.5.100/16).



Le concentrateur VPN est désormais accessible via un navigateur HTML à partir du réseau interne. Référez-vous à [Utilisation de l'interface de ligne de commande pour la configuration](#)

[rapide](#) pour plus d'informations sur la façon de configurer le concentrateur VPN en mode CLI.

Tapez l'adresse IP de l'interface privée à partir du navigateur Web afin d'activer l'interface utilisateur graphique.

Cliquez sur l'icône **Enregistrer les modifications nécessaires** pour enregistrer les modifications apportées à la mémoire. Le nom d'utilisateur et le mot de passe par défaut sont **admin**, ce qui est sensible à la casse.

1. Lancez l'interface utilisateur graphique et sélectionnez **Configuration > Interfaces** pour configurer l'adresse IP de l'interface publique et de la passerelle par défaut.


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. Sélectionnez **Configuration > Policy Management > Traffic Management > Network Lists > Add or Modify** pour créer les listes réseau qui définissent le trafic à chiffrer. Ajoutez ici les réseaux locaux et distants. Les adresses IP doivent refléter celles de la liste d'accès configurée sur le PIX distant. Dans cet exemple, les deux listes réseau sont **remote_network** et **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. Sélectionnez **Configuration > System > Tunneling Protocols > IPsec LAN-to-LAN > Add** pour configurer le tunnel IPsec LAN-to-LAN. Cliquez sur **Apply** lorsque vous avez terminé. Saisissez l'adresse IP de l'homologue, les listes réseau créées à l'étape 2, les paramètres IPsec et ISAKMP et la clé pré-partagée. Dans cet exemple, l'adresse IP de l'homologue est 10.1.1.1, les listes réseau sont **remote_network** et **VPN Client Local LAN**, et **cisco** est la clé pré-partagée.

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"/>	

4. Sélectionnez **Configuration > User Management > Groups > Modify 10.1.1.1** pour afficher les informations de groupe générées automatiquement. **Remarque :** Ne modifiez pas ces paramètres de groupe.

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	*****	Enter the password for the group.
Verify	*****	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

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- [Vérifier le PIX](#)
- [Vérification du concentrateur VPN 3000](#)

Vérifier le PIX

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- [show isakmp sa](#) : affiche toutes les associations de sécurité IKE (SA) actuelles sur un homologue. L'état MM_ACTIVE indique que le mode principal est utilisé pour configurer le tunnel VPN IPsec. Dans cet exemple, le pare-feu PIX initie la connexion IPsec. L'adresse IP homologue est 172.30.1.1 et utilise le mode principal pour établir la connexion.

```
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](#) — Affiche les paramètres utilisés par les SA en cours. Recherchez les adresses IP de l'homologue, les réseaux accessibles aux niveaux local et distant et le jeu de transformations utilisé. Il y a deux SAS ESP, une dans chaque direction.

```
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
```

Utilisez les commandes [clear ipsec sa](#) et [clear isakmp sa](#) pour réinitialiser le tunnel.

[Vérification du concentrateur VPN 3000](#)

Sélectionnez **Monitoring > Statistics > IPsec** pour vérifier si le tunnel est apparu dans le concentrateur VPN 3000. Ce champ contient les statistiques des paramètres IKE et 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

Vous pouvez surveiller activement la session à l'adresse **Monitoring > Sessions**. Vous pouvez réinitialiser le tunnel IPsec ici.

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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- [Dépannage du PIX](#)
- [Dépannage du concentrateur VPN 3000](#)
- [PFS](#)

Dépannage du PIX

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines [commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

Les commandes **debug** sur PIX pour les tunnels VPN sont les suivantes :

- [debug crypto isakmp](#) - Débogue les négociations ISAKMP SA.
- [debug crypto ipsec](#) - Débogue les négociations de SA IPsec.

Dépannage du concentrateur VPN 3000

À l'instar des commandes de débogage des routeurs Cisco, vous pouvez configurer des classes d'événements pour afficher les alarmes. Sélectionnez **Configuration > System > Events > Classes > Add** pour activer la journalisation des classes d'événements.

Sélectionnez **Monitoring > Filterable Event Log** pour surveiller les événements activés.

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](#)

Dans des négociations IPsec, le Perfect Forward Secrecy (PFS) assure que chacune nouvelle clé

cryptographique est indépendante de toute clé précédente. Activez ou désactivez PFS sur les deux homologues de tunnel, sinon le tunnel IPsec LAN à LAN (L2L) n'est pas établi dans PIX/ASA.

PFS est désactivé par défaut. Afin d'activer PFS, utilisez la commande **pfs** avec le mot clé **enable** en mode de configuration de stratégie de groupe. Afin de désactiver PFS, saisissez le mot clé **disable**.

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

Afin de retirer l'attribut PFS de la configuration en cours, saisissez la forme no de cette commande. Une stratégie de groupe peut hériter d'une valeur pour PFS d'une autre stratégie de groupe. Saisissez la forme no de cette commande afin d'éviter d'hériter d'une valeur.

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

[Informations connexes](#)

- [Page d'assistance des appliances de sécurité de la gamme Cisco PIX 500](#)
- [Page d'assistance du concentrateur Cisco VPN 3000](#)
- [Référence des commandes des dispositifs de sécurité de la gamme Cisco PIX 500](#)
- [Support et documentation techniques - Cisco Systems](#)