

# PIX/ASA 7.x et versions ultérieures : Exemple de configuration d'Easy VPN à l'aide d'un dispositif ASA 5500 avec transmission tunnel partagée en tant que serveur et d'un routeur Cisco 871 en tant que client distant Easy VPN

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépanner le routeur](#)

[Dépanner l'ASA](#)

[Informations connexes](#)

## [Introduction](#)

Ce document fournit un exemple de configuration pour IPsec entre Cisco Adaptive Security Appliance (ASA) 5520 et un routeur Cisco 871 utilisant Easy VPN. L'ASA 5520 joue le rôle de serveur Easy VPN et le routeur Cisco 871, celui de client distant Easy VPN. Bien que cette configuration utilise un périphérique ASA 5520 qui exécute la version du logiciel ASA 7.1(1), vous pouvez également utiliser cette configuration pour les périphériques du pare-feu PIX qui exécutent la version de système d'exploitation 7.1 et ultérieure.

Afin de configurer un routeur Cisco IOS® comme EzVPN en [mode d'extension réseau \(NEM\) qui se connecte à un concentrateur Cisco VPN 3000](#), consultez [Configuration du client Cisco EzVPN sur Cisco IOS avec le concentrateur VPN 3000](#).

Afin de configurer IPsec entre le client matériel distant Cisco IOS Easy VPN et le serveur PIX Easy VPN, consultez [Exemple de configuration de client matériel IOS Easy VPN Remote sur un serveur PIX Easy VPN](#).

Afin de configurer un routeur Cisco 7200 comme EzVPN et le routeur Cisco 871 comme Easy VPN distant, consultez [Exemple de configuration distante du serveur Easy VPN 7200 sur Easy](#)

[VPN 871](#).

## Conditions préalables

### Conditions requises

Assurez-vous que vous comprenez les bases d'[IPsec et des systèmes d'exploitation ASA 7.x](#).

### Components Used

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

- Le serveur Easy VPN Server est un ASA 5520 qui exécute la version 7.1(1).
- Le client matériel distant Easy VPN est un routeur Cisco 871 qui exécute la version logicielle 12.4(4)T1 de Cisco IOS®.

**Remarque** : la gamme Cisco ASA 5500 version 7.x exécute une version logicielle similaire vue dans PIX version 7.x. Les configurations présentées dans ce document s'appliquent aux deux gammes de produits.

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.

### Conventions

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

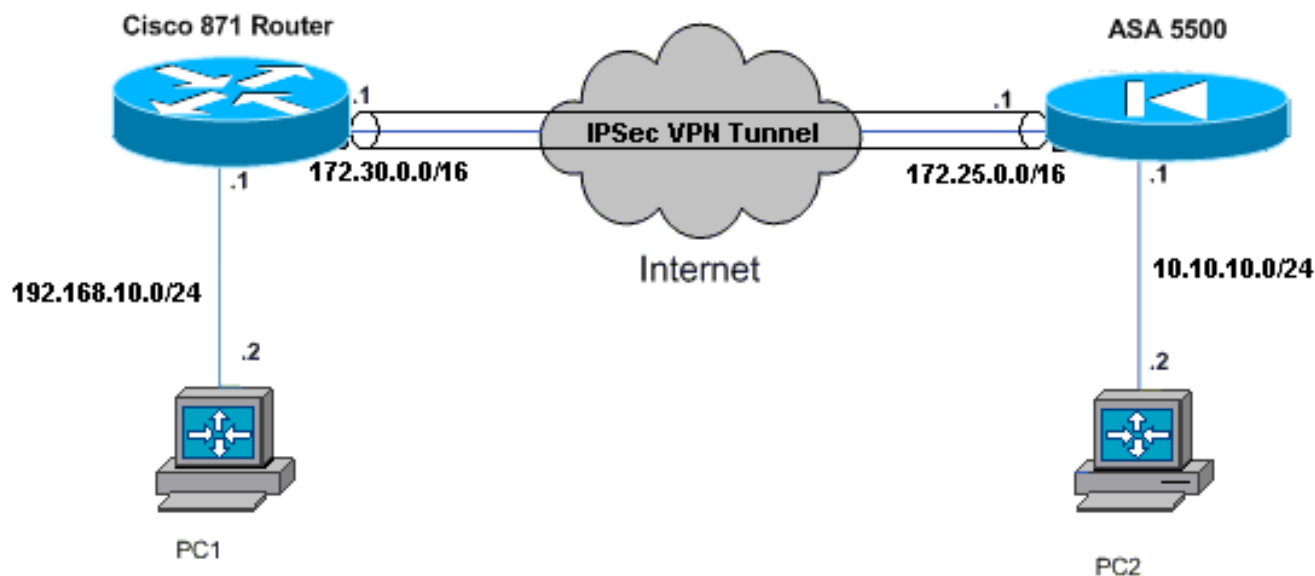
## Configuration

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

**Remarque** : Utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement) pour en savoir plus sur les commandes figurant dans le présent document.

### Diagramme du réseau

Ce document utilise la configuration réseau suivante :



## Configurations

Ce document utilise les configurations suivantes :

- [Cisco ASA 5520](#)
- [Routeur Cisco 871](#)

### Cisco ASA 5520

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(1)
!
hostname ciscoasa
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.25.171.1 255.255.0.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!--- Output is suppressed. access-list no-nat extended
```

```
permit ip 10.10.10.0 255.255.255.0 192.168.10.0
255.255.255.0 access-list ezvpn extended permit ip
10.10.10.0 255.255.255.0 192.168.10.0 255.255.255.0

access-list Split_Tunnel_List remark The corporate
network behind the ASA
access-list Split_Tunnel_List standard permit 10.10.10.0
255.255.255.0
nat (inside) 0 access-list no-nat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 172.25.171.2 1
!--- Use the group-policy attributes command in !---
global configuration mode to enter the group-policy
attributes mode.

group-policy DfltGrpPolicy attributes
  banner none
  wins-server none
  dns-server none
  dhcp-network-scope none
  vpn-access-hours none
  vpn-simultaneous-logins 3
  vpn-idle-timeout 30
  vpn-session-timeout none
  vpn-filter none
  vpn-tunnel-protocol IPSec
  password-storage enable
  ip-comp disable
  re-xauth disable
  group-lock none
  pfs disable
  ipsec-udp enable
  ipsec-udp-port 10000

split-tunnel-policy tunnelspecified

split-tunnel-network-list value Split_Tunnel_List
  default-domain none
  split-dns none
  secure-unit-authentication disable
  user-authentication disable
  user-authentication-idle-timeout 30
  ip-phone-bypass disable
  leap-bypass disable
  !--- Network Extension mode allows hardware clients to
  present a single, !--- routable network to the remote
  private network over the VPN tunnel. nem enable
  backup-servers keep-client-config
  client-firewall none
  client-access-rule none
username cisco password 3USUCOPFUIMCO4Jk encrypted
  http server enable
  no snmp-server location
  no snmp-server contact
  snmp-server enable traps snmp authentication linkup
  linkdown coldstart
  !--- These are IPsec Phase I and Phase II parameters. !-
  -- The parameters have to match in order for !--- the
  IPsec tunnel to come up. crypto ipsec transform-set
mySET esp-des esp-md5-hmac
crypto dynamic-map myDYN-MAP 5 set transform-set mySET
crypto map myMAP 60 ipsec-isakmp dynamic myDYN-MAP
crypto map myMAP interface outside
isakmp identity address
```

```

isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400

tunnel-group DefaultRAGroup general-attributes
 default-group-policy DfltGrpPolicy

tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
!
: end
ciscoasa#

```

## Routeur Cisco 871

```

C871#show running-config
Current configuration : 1639 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C871
!
boot-start-marker
boot-end-marker
!
!
ip cef
!
!--- Creates a Cisco Easy VPN Remote configuration and
enters the !--- Cisco Easy VPN Remote configuration
mode. crypto ipsec client ezvpn ASA
!--- The IPsec VPN tunnel is automatically connected
when the Cisco !--- Easy VPN Remote feature is
configured on an interface. connect auto
!--- The group name should match the remote group name.
group DefaultRAGroup key cisco
!--- Specifies that the router should become a remote
extension of the !--- enterprise network at the other
end of the VPN connection. mode network-extension
!--- Sets the peer IP address or hostname for the VPN
connection. peer 172.25.171.1
!--- Specifies how the Easy VPN Client handles extended
authentication (Xauth) requests. xauth userid mode
interactive
!--- Output is suppressed. ! interface FastEthernet0 !
interface FastEthernet1 ! interface FastEthernet2 !
interface FastEthernet3 ! !--- Assigns a Cisco Easy VPN
Remote configuration to an outside interface. interface
FastEthernet4 ip address 172.30.171.1 255.255.0.0 ip
access-group 101 in no ip redirects no ip unreachable
no ip proxy-arp ip nat outside ip virtual-reassembly ip
route-cache flow duplex auto speed auto crypto ipsec

```

```

client ezvpn ASA
!
!--- Assigns a Cisco Easy VPN Rremote configuration to
an outside interface. interface Vlan1 ip address
192.168.10.1 255.255.255.0 ip access-group 100 out no ip
redirects no ip unreachable no ip proxy-arp ip nat
inside ip virtual-reassembly ip route-cache flow ip tcp
adjust-mss 1452 crypto ipsec client ezvpn ASA inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.30.171.2
!
!--- Enables NAT on the inside source address. ip nat
inside source route-map EzVPN1 interface FastEthernet4
overload
!
access-list 100 permit ip any any
access-list 101 permit ip any any
access-list 103 permit ip 192.168.10.0 0.0.0.255 any
!
route-map EzVPN1 permit 1
  match ip address 103
!
end
C871#

```

## Vérification

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

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`.

Une fois que vous avez configuré les deux périphériques, le routeur Cisco 871 tente d'installer le tunnel VPN en contactant l'ASA 5520 automatiquement à l'aide de l'adresse IP de l'homologue. Une fois les paramètres ISAKMP initiaux permutés, le routeur affiche ce message :

```

Pending XAuth Request, Please enter the
following command: crypto ipsec client ezvpn xauth

```

Vous devez entrer la commande de `crypto ipsec client ezvpn xauth` qui demande un nom d'utilisateur et mot de passe. Ceci devrait correspondre au nom d'utilisateur et au mot de passe configurés sur l'ASA 5520. Une fois que les deux homologues sont d'accord sur le nom d'utilisateur et le mot de passe, les autres paramètres sont convenus et le tunnel IPsec VPN apparaît.

```

EZVPN(ASA): Pending XAuth Request, Please enter the following command:

```

```

EZVPN: crypto ipsec client ezvpn xauth

```

```

!--- Enter the crypto ipsec client ezvpn xauth command.

```

```

crypto ipsec client ezvpn xauth

```

Enter Username and Password.: **cisco**  
Password: : **test**

Utilisez ces commandes pour vérifier si le tunnel fonctionne correctement sur l'ASA 5520 et le routeur Cisco 871 :

- [show crypto isakmp sa](#) - Affiche toutes les associations de sécurité actuelles d'IKE (SA) sur un pair. L'état QM\_IDLE indique que le SA reste authentifié avec son homologue et peut être utilisé pour des échanges de mode rapides ultérieurs.

```
show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
172.25.171.1 172.30.171.1 QM_IDLE        1011     0 ACTIVE
```

```
IPv6 Crypto ISAKMP SA
```

- [show crypto ipsec sa](#) — Affiche les paramètres utilisés par les SA. 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 SA ESP (Encapsulating Security Protocol), une dans chaque direction. Puisque les jeux de transformations AH (Authentication Header) ne sont pas utilisés, ils sont vides.

```
show crypto ipsec sa
```

```
interface: FastEthernet4
  Crypto map tag: FastEthernet4-head-0, local addr 172.30.171.1

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 172.25.171.1 port 500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: 172.30.171.1, remote crypto endpt.: 172.25.171.1
  path mtu 1500, ip mtu 1500
  current outbound spi: 0x2A9F7252(715092562)

inbound esp sas:
  spi: 0x42A887CB(1118341067)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    conn id: 39, flow_id: C87X_MBRD:39, crypto map: FastEthernet4-head-0
    sa timing: remaining key lifetime (k/sec): (4389903/28511)
    IV size: 8 bytes
    replay detection support: Y
    Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x2A9F7252(715092562)
    transform: esp-des esp-md5-hmac ,
```

```
in use settings ={Tunnel, }
conn id: 40, flow_id: C87X_MBRD:40, crypto map: FastEthernet4-head-0
sa timing: remaining key lifetime (k/sec): (4389903/28503)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
```

outbound ah sas:

outbound pcp sas:

- [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 les jeux de transformations utilisés. Il y a deux SAS ESP, une dans chaque direction.

```
ciscoasa#show ipsec sa
interface: outside
Crypto map tag: myDYN-MAP, seq num: 5, local addr: 172.25.171.1

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 172.30.171.1, username: cisco
dynamic allocated peer ip: 0.0.0.0

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.25.171.1, remote crypto endpt.: 172.30.171.1

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 42A887CB
```

inbound esp sas:

```
spi: 0x2A9F7252 (715092562)
transform: esp-des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 8, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28648
IV size: 8 bytes
replay detection support: Y
```

outbound esp sas:

```
spi: 0x42A887CB (1118341067)
transform: esp-des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 8, crypto-map: myDYN-MAP
sa timing: remaining key lifetime (sec): 28644
IV size: 8 bytes
replay detection support: Y
```

- [show isakmp sa](#) — Affiche toutes les SA IKE en cours au niveau d'un homologue. L'état AM\_ACTIVE indique que le mode agressif a été utilisé pour l'échange de paramètres.

```
ciscoasa#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: 172.30.171.1
  Type      : user           Role      : responder
  Rekey     : no           State     : AM_ACTIVE
```



# Dépannage

Utilisez cette section pour dépanner votre configuration.

- [Dépanner le routeur](#)
- [Dépanner l'ASA](#)

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.

## Dépanner le routeur

- `debug crypto isakmp` — Affiche les négociations ISAKMP de la phase IKE 1.
- `debug crypto ipsec` — Affiche les négociations IPsec de la phase IKE 2.

## Dépanner l'ASA

- `debug crypto isakmp 127` — Affiche les négociations ISAKMP de la phase IKE 1.
- `debug crypto ipsec 127` — Affiche les négociations IPsec de la phase IKE 2.

## Informations connexes

- [Exemple de configuration d'Easy VPN avec un dispositif ASA 5500 en tant que serveur et ASA 506E en tant que client \(NEM\)](#)
- [Assistance produit des dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500](#)
- [Assistance produit des routeurs de la gamme Cisco 800](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)