

# PIX/ASA 7.x y posteriores: Ejemplo de Configuración de Easy VPN con Tunelización Dividida ASA 5500 como Servidor y Cisco 871 como Easy VPN Remote

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

[Resolución de Problemas en el Router](#)

[Resolución de Problemas e ASA](#)

[Información Relacionada](#)

## [Introducción](#)

Este documento proporciona un ejemplo de configuración para IPsec entre un Cisco Adaptive Security Appliance (ASA) 5520 y Cisco 871 router con una Easy VPN. El ASA 5520 actúa como Servidor Easy VPN y el Cisco 871 router actúa como Cliente Easy VPN Remote. Mientras que esta configuración utiliza un dispositivo ASA 5520 que ejecuta la versión de software ASA 7.1(1), también puede utilizar esta configuración para los dispositivos de firewall PIX que ejecutan la versión del sistema operativo 7.1 del PIX y posterior.

Para configurar un Cisco IOS® router como EzVPN en el [Modo de Extensión de Red \(NEM\) que se conecta a un Cisco VPN 3000 Concentrator](#), consulte [Configuración de Cisco EzVPN Client en Cisco IOS con un VPN 3000 Concentrator](#).

Para configurar el IPsec entre el Cisco IOS Easy VPN Remote del Cisco IOS y el Easy VPN Server PIX, consulte Ejemplo de Configuración de IOS [Easy VPN Remote hardware Client a un PIX Easy VPN Server](#) .

Para configurar un Cisco 7200 Router como EzVPN y Cisco 871 Router como Easy VPN Remote, consulte Ejemplo de Configuración de [7200 Easy VPN Server a 871 Easy VPN Remote](#).

# Prerequisites

## Requirements

Asegúrese de tener conocimientos básicos del [IPSec y de los sistemas operativos ASA 7.x](#).

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El Easy VPN Server es un ASA 5520 que ejecuta la versión 7.1(1).
- The Easy VPN Remote Hardware Client es un Cisco 871 router que ejecuta Cisco IOS® Software Release 12.4(4)T1.

**Nota:** Cisco ASA serie 5500 versión 7.x ejecuta una versión de software similar que se ve en la versión 7.x de PIX. Las configuraciones en este documento son aplicables a ambas líneas de producto.

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.

## Convenciones

Consulte [Convenciones de Consejos Técnicos Cisco para obtener más información sobre las convenciones del documento](#).

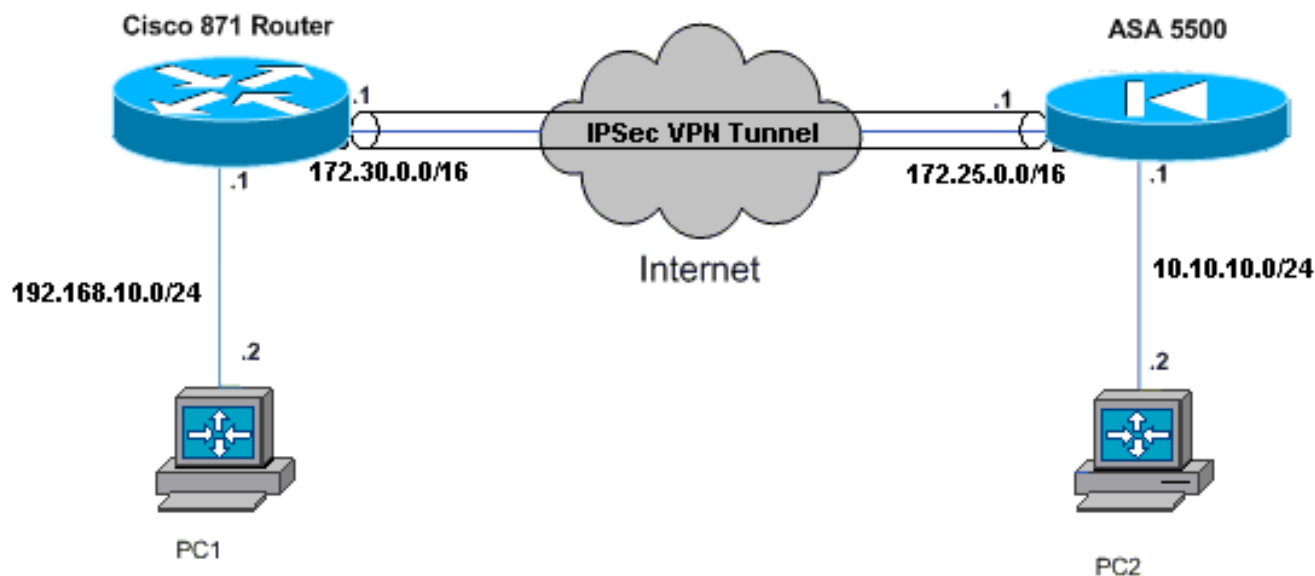
## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Use la [Command Lookup Tool](#) (sólo [clientes registrados](#)) para obtener más información sobre los comandos utilizados en este documento.

## Diagrama de la red

En este documento, se utiliza esta configuración de red:



## Configuraciones

En este documento, se utilizan estas configuraciones:

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

### 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#

```

## Cisco 871 Router

```

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#
```

## Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

Una vez que configuró ambos dispositivos, el Cisco 871 Router intenta instalar el túnel VPN al establecer contacto con ASA 5520 automáticamente usando la dirección IP par. Después de intercambiar los parámetros ISAKMP iniciales, el router visualiza este mensaje:

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

Debe ingresar el comando **crypto ipsec client ezvpn xauth** que le pide un nombre de usuario y contraseña. Éstos deben coincidir con el nombre de usuario y contraseña configurados en el ASA 5520. Una vez que el nombre de usuario y contraseña es acordado entre los pares, el resto de los parámetros se establece el resto de los parámetros y el túnel del IPsec VPN se conecta.

```
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**

Utilice estos comandos para verificar si el túnel funciona correctamente en el ASA 5520 y el Cisco 871 Router:

- [show crypto isakmp sa](#) : muestra todas las asociaciones de seguridad actuales IKE (SA) en un par. El estado del QM\_IDLE indica que el SA sigue autenticada con su par y se puede utilizar para los intercambios subsiguientes de modo rápido.

```
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](#) — **Muestra la configuración actual utilizada por las SA actuales**  
Verifique la dirección IP par, las redes accesibles en los extremos remotos y locales y la transformación fijada que se utiliza. Hay dos SAs de Encapsulating Security Protocol (ESP), uno en cada dirección. Puesto que el Authentication Header (AH) transforma los conjuntos que no se utilizan, está vacío.

```
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](#) —Muestra la configuración utilizada por las SAs actuales. Verifique la dirección IP par, las redes accesibles en los extremos remotos y locales y los conjuntos de la transformación que se utilizan. Hay dos ESP SA, uno en cada dirección.

```
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](#) —Muestra todas las SA IKE actuales en un par. El estado AM\_ACTIVE indica que el modo Aggressive se usó para el intercambio de parámetros.

```
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
```



## Troubleshoot

Use esta sección para resolver problemas de configuración.

- [Resolución de Problemas en el Router](#)
- [Resolución de Problemas e ASA](#)

[La herramienta Output Interpreter Tool \(clientes registrados solamente\) \(OIT\) soporta ciertos comandos show.](#) Utilice la OIT para ver un análisis del resultado del comando show.

**Nota:** Consulte [Información Importante sobre Comandos Debug](#) antes de utilizar los comandos debug.

### Resolución de Problemas en el Router

- `debug crypto isakmp`: muestra las negociaciones ISAKMP de la fase IKE 1.
- `debug crypto ipsec`: muestra las negociaciones IPsec de la fase IKE 2.

### Resolución de Problemas e ASA

- `debug crypto isakmp 127`—Muestra las negociaciones ISAKMP de la fase IKE 1.
- `debug crypto ipsec 127`—Muestra las negociaciones IPsec de la fase IKE 2.

## Información Relacionada

- [Ejemplo de Configuración de Easy VPN con ASA 5500 como Servidor y PIX 506E como Cliente \(NEM\)](#)
- [Soporte de producto para dispositivos de seguridad adaptable Cisco ASA de la serie 5500](#)
- [Soporte de Productos de Cisco 800 Series Routers](#)
- [Negociación IPsec/Protocolos IKE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)