# PIX/ASA 7.x and Later : Easy VPN with Split Tunneling ASA 5500 as the Server and Cisco 871 as the Easy VPN Remote Configuration Example

## Document ID: 68815

## Contents

## Introduction

This document provides a sample configuration for IPsec between a Cisco Adaptive Security Appliance (ASA) 5520 and a Cisco 871 router using Easy VPN. The ASA 5520 acts as the Easy VPN Server and the Cisco 871 router acts as the Easy VPN Remote Client. While this configuration uses an ASA 5520 device that runs ASA software version 7.1(1), you can also use this configuration for PIX Firewall devices that run PIX operating system version 7.1 and later.

In order to configure a Cisco IOS® router as an EzVPN in Network Extension Mode (NEM) that connects to a Cisco VPN 3000 Concentrator, refer to Configuring the Cisco EzVPN Client on Cisco IOS with the VPN 3000 Concentrator.

In order to configure IPsec between the Cisco IOS Easy VPN Remote Hardware Client and the PIX Easy VPN Server, refer to IOS Easy VPN Remote Hardware Client to a PIX Easy VPN Server Configuration Example.

In order to configure a Cisco 7200 Router as an EzVPN and the Cisco 871 Router as the Easy VPN Remote, refer to 7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example.

## Prerequisites

### Requirements

Ensure that you have a basic understanding of IPsec and the ASA 7.x operating systems.

## Components Used

The information in this document is based on these software and hardware versions:

- The Easy VPN Server is an ASA 5520 that runs version 7.1(1).
- The Easy VPN Remote Hardware Client is a Cisco 871 router that runs Cisco IOS® Software Release 12.4(4)T1.

**Note:** Cisco ASA 5500 series version 7.x runs a similar software version seen in PIX version 7.x. The configurations in this document are applicable to both product lines.

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

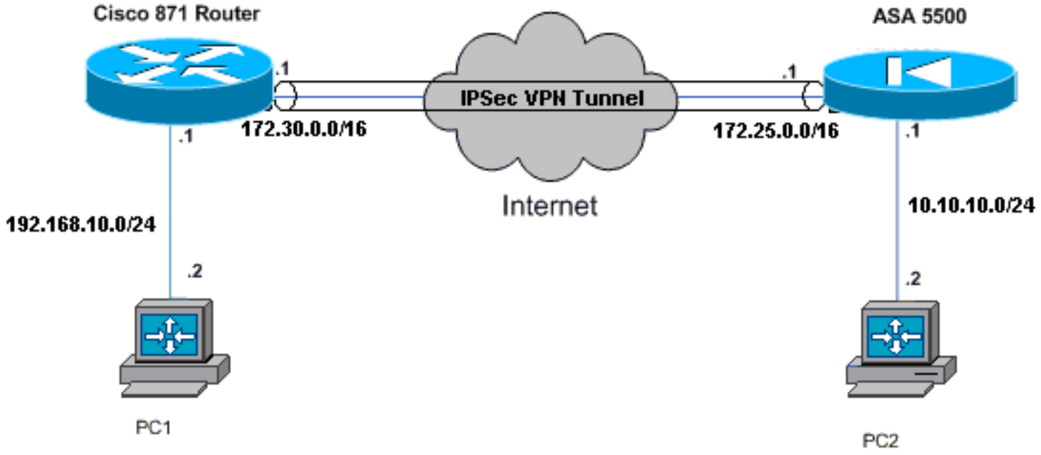
# Configure

In this section, you are presented with the information to configure the features described in this document.

**Note:** Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

## Network Diagram

This document uses this network setup:



## Configurations

This document uses these configurations:

- 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 unreachables
 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 unreachables
 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#
```

## Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Once you configure both devices, the Cisco 871 router attempts to setup the VPN tunnel by contacting ASA 5520 automatically using the peer IP address. After the initial ISAKMP parameters are exchanged, the router displays this message:

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

You have to enter the **crypto ipsec client ezvpn xauth** command which prompts you for a username and password. This should match the username and password configured on the ASA 5520. Once the username and password is agreed by both peers, the rest of the parameters are agreed and the IPsec VPN tunnel comes up.

```
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
```

Use these commands to verify if the tunnel works properly on both the ASA 5520 and the Cisco 871 router:

- **show crypto isakmp sa** Displays all current IKE security associations (SAs) at a peer. The QM_IDLE state denotes that the SA remains authenticated with its peer and can be used for subsequent quick mode exchanges.

```
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** Displays the settings used by current SAs. Check for the peer IP addresses, the networks accessible at both the local and remote ends, and the transform set that is used. There are two Encapsulating Security Protocol (ESP) SAs, one in each direction. Since Authentication Header (AH) transform sets are not used, it is empty.

```
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**  Displays the settings used by current SAs. Check for the peer IP addresses, the networks accessible at both the local and remote ends, and the transform sets that are used. There are two ESP SAs, one in each 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**  Displays all current IKE SAs at a peer. The AM_ACTIVE state denotes that Aggressive mode was used for the exchange of parameters.

```
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 this section to troubleshoot your configuration.

- Troubleshoot the Router
- Troubleshoot the ASA

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

### Troubleshoot the Router

- **debug crypto isakmp** Displays the ISAKMP negotiations of IKE phase 1.
- **debug crypto ipsec** Displays the IPsec negotiations of IKE phase 2.

### Troubleshoot the ASA

- **debug crypto isakmp 127** Displays the ISAKMP negotiations of IKE phase 1.
- **debug crypto ipsec 127** Displays the IPsec negotiations of IKE phase 2.

## Related Information

- **Easy VPN with an ASA 5500 as the Server and PIX 506E as the Client (NEM) Configuration Example**
- **Cisco ASA 5500 Series Adaptive Security Appliances Product Support**
- **Cisco 800 Series Routers Product Support**
- **IPSec Negotiation/IKE Protocols**
- **Technical Support & Documentation − Cisco Systems**