

PIX/ASA 7.x及更高版本：使用分割隧道ASA 5500的Easy VPN作为服务器并且使用Cisco 871作为Easy VPN远端配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[排除路由器故障](#)

[排除 ASA 故障](#)

[相关信息](#)

简介

本文档提供了使用 Easy VPN 在 Cisco 自适应安全设备 (ASA) 5520 和 Cisco 871 路由器之间配置 IPsec 的示例配置。ASA 5520 充当 Easy VPN 服务器，Cisco 871 路由器充当 Easy VPN 远程客户端。此配置使用运行 ASA 软件版本 7.1(1) 的 ASA 5520 设备，您也可以对运行 PIX 操作系统版本 7.1 及更高版本的 PIX 防火墙设备使用此配置。

要在[网络扩展模式 \(NEM\) 下将 Cisco IOS® 路由器配置为连接到 Cisco VPN 3000 集中器的 EzVPN](#)，请参阅[使用 VPN 3000 集中器在 Cisco IOS 上配置 Cisco EzVPN Client](#)。

要在 Cisco IOS Easy VPN Remote Hardware Client 和 PIX Easy VPN 服务器之间配置 IPsec，请参阅[IOS Easy VPN Remote Hardware Client 到 PIX Easy VPN 服务器配置示例](#)。

要将 Cisco 7200 路由器配置为 EzVPN 并将 Cisco 871 路由器配置为 Easy VPN Remote，请参阅[7200 Easy VPN 服务器到 871 Easy VPN Remote 配置示例](#)。

先决条件

要求

请确保您对 [IPsec](#) 和 [ASA 7.x 操作系统](#) 有基本的了解。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Easy VPN 服务器是运行版本 7.1(1) 的 ASA 5520。
- Easy VPN Remote Hardware Client 是运行 Cisco IOS® 软件版本 12.4(4)T1 的 Cisco 871 路由器。

注意： Cisco ASA 5500系列版本7.x运行PIX版本7.x中的类似软件版本。本文档中的配置适用于这两个产品系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

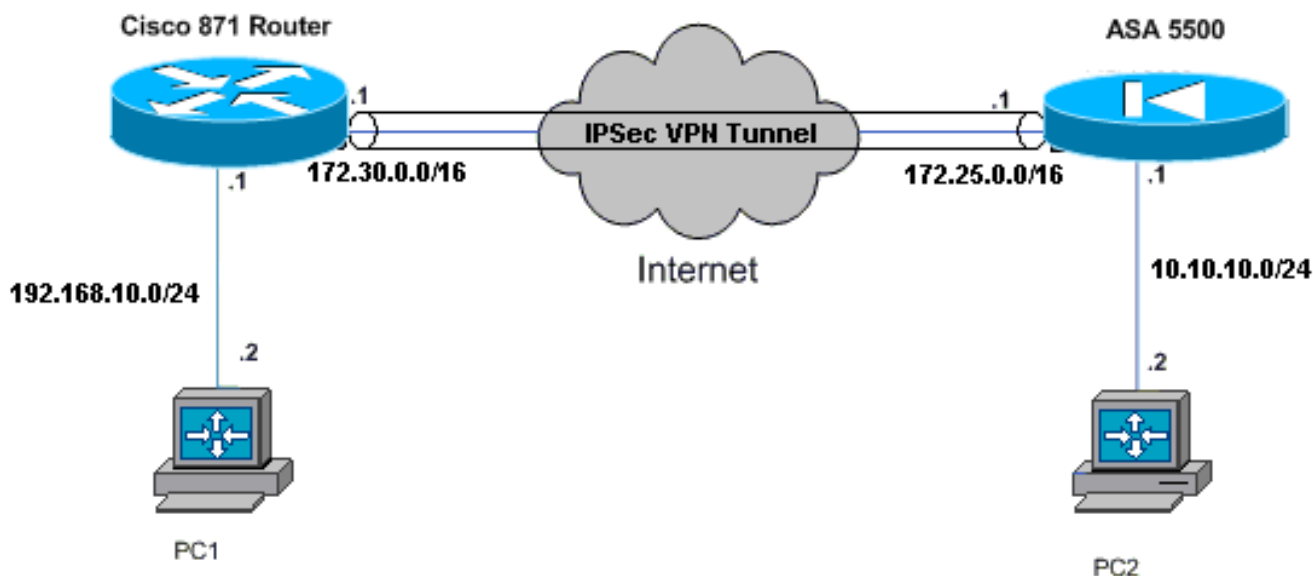
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用[命令查找工具](#)(仅限注册客户)可查找有关本文档中使用的命令的详细信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- [Cisco ASA 5520](#)
- [Cisco 871 路由器](#)

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 路由器

```
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 unreachablees
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 unreachablees 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#

```

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

配置这两个设备后，Cisco 871 路由器将尝试通过使用对等 IP 地址自动与 ASA 5520 联系来设置 VPN 隧道。在交换最初的 ISAKMP 参数后，路由器显示以下消息：

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

您必须输入提示您输入用户名和口令的 **crypto ipsec client ezvpn xauth** 命令。此用户名和口令应该与在 ASA 5520 上配置的用户名和口令匹配。两个对等体都同意用户名和口令后，其余参数也将被同意，IPSec VPN 隧道启动。

```
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
```

在 ASA 5520 和 Cisco 871 路由器上使用以下命令验证隧道是否正常运行：

- [show crypto isakmp sa](#) - 显示对等体上的所有当前 IKE 安全关联 (SA)。QM_IDLE 状态表示 SA 已通过其对等体的身份验证，并且可用于随后的快速模式交换。

```
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](#) - 显示当前 SA 使用的设置。检查对等 IP 地址、本地和远程端都可访问的网络，以及所使用的转换集。有两个封装安全协议 (ESP) SA，每个方向一个。由于未使用身份验证报头 (AH) 转换集，因此它是空的。

```
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](#) - 显示当前 SA 使用的设置。检查对等 IP 地址、本地和远程端都可访问的网络，以及所使用的转换集。有两个 ESP SA，每个方向一个。

```
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](#) - 显示对等体上的所有当前 IKE SA。AM_ACTIVE 状态表示使用了主动模式进行参数交换。

```
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
```

故障排除

使用本部分可排除配置故障。

- [排除路由器故障](#)
- [排除 ASA 故障](#)

[命令输出解释程序 \(仅限注册用户\) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

注意：在使用[debug命令之前](#)，请[参阅](#)有关Debug命令的重要信息。

排除路由器故障

- debug crypto isakmp - 显示 IKE 第 1 阶段的 ISAKMP 协商。
- debug crypto ipsec - 显示 IKE 第 2 阶段的 IPsec 协商。

排除 ASA 故障

- debug crypto isakmp 127 - 显示 IKE 第 1 阶段的 ISAKMP 协商。
- debug crypto ipsec 127 - 显示 IKE 第 2 阶段的 IPsec 协商。

相关信息

- [使用 ASA 5500 作为服务器并使用 PIX 506E 作为客户端 \(NEM\) 的 Easy VPN 配置示例](#)
- [Cisco ASA 5500 系列自适应安全设备产品支持](#)
- [Cisco 800 系列路由器产品支持](#)
- [IPsec 协商/IKE 协议](#)
- [技术支持和文档 - Cisco Systems](#)