PIX/ASA 7.x及更高版本：將分割隧道ASA 5500作為伺服器並將思科871作為Easy VPN Remote配置的Easy VPN示例

目錄

簡介
必要條件
需求
採用元件
慣例
設定
網路圖表
組態
驗證
疑難排解
路由器故障排除
排除ASA故障
相關資訊

簡介

本文檔提供使用Easy VPN的Cisco自適應安全裝置(ASA)5520和Cisco 871路由器之間的IPsec配置示例。ASA 5520充當Easy VPN伺服器，Cisco 871路由器充當Easy VPN Remote客戶端。雖然此配置使用運行ASA軟體版本7.1(1)的ASA 5520裝置，但您也可以將此配置用於運行PIX作業系統7.1及更高版本的PIX防火牆裝置。

要將Cisco IOS®路由器配置為連線到Cisco VPN 3000集中器的網路擴展模式(NEM)下的EzVPN，請參閱使用VPN 3000集中器在Cisco IOS上配置Cisco EzVPN客戶端。

要在Cisco IOS Easy VPN遠端硬體客戶端和PIX Easy VPN伺服器之間配置IPsec，請參閱IOS Easy VPN遠端硬體客戶端到PIX Easy VPN伺服器配置示例。

要將Cisco 7200路由器配置為EzVPN，將Cisco 871路由器配置為Easy VPN Remote，請參閱7200 Easy VPN Server to 871 Easy VPN Remote配置示例。

必要條件

需求

確保您對IPsec和ASA 7.x操作系統有基本瞭解。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Easy VPN伺服器是運行版本7.1(1)的ASA 5520。
- Easy VPN遠端硬體客戶端是運行Cisco IOS®軟體版本12.4(4)T1的Cisco 871路由器。

註：Cisco ASA 5500系列版本7.x運行與PIX版本7.x類似的軟體版本。本文檔中的配置適用於這兩種產品系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

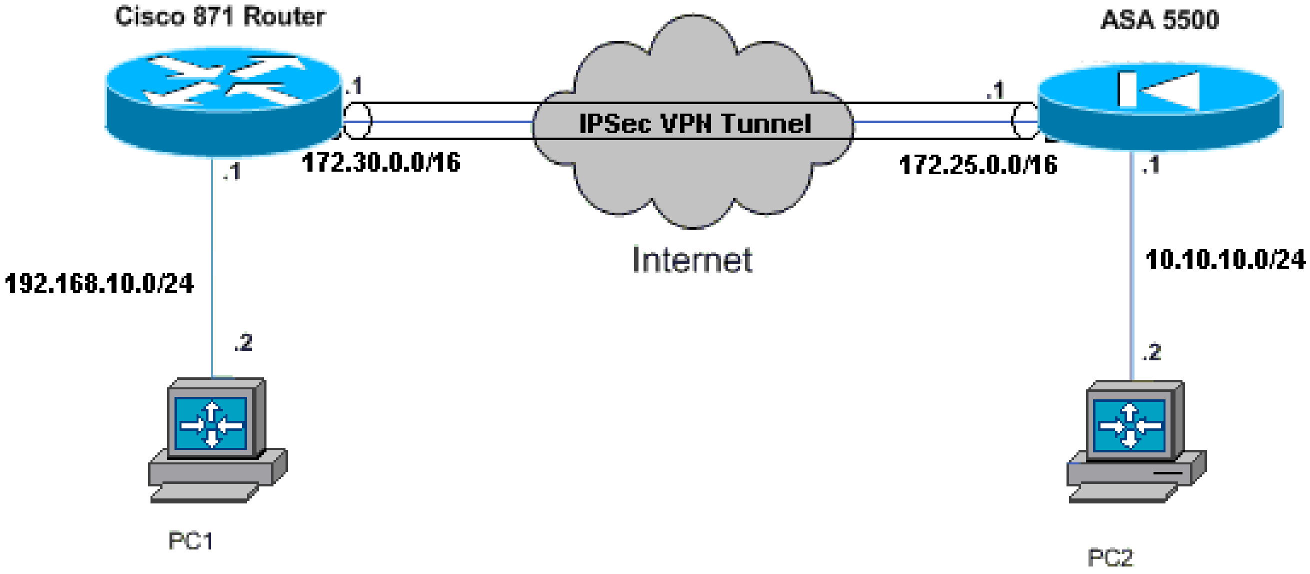
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- Cisco ASA 5520
- 思科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#
```

思科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 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#
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

配置兩台裝置後，Cisco 871路由器會嘗試使用對等IP地址自動聯絡ASA 5520來設定VPN隧道。交換初始ISAKMP引數後，路由器會顯示以下訊息：

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

您必須輸入**crypto ipsec client ezvpn xauth**命令，該命令會提示您輸入使用者名稱和密碼。這應該與ASA 5520上配置的使用者名稱和密碼匹配。一旦兩個對等體同意使用者名稱和密碼，則同意其餘引數並啟動IPsec VPN隧道。

```
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
```

使用以下命令驗證隧道在ASA 5520和Cisco 871路由器上是否正常工作：

- show crypto isakmp sa — 顯示對等體上的所有當前IKE安全關聯(SA)。QM_IDLE狀態表示SA保持其對等體的身份驗證，可用於後續的快速模式交換。

  ```
  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 — 顯示當前SA使用的設定。檢查對等IP地址、可在本地和遠端端訪問的網路，以及使用的轉換集。有兩個封裝安全通訊協定(ESP)SA，每個方向一個。由於不使用身份驗證報頭(AH)轉換集，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](#) — 顯示當前SA使用的設定。檢查對等IP地址、可在本地和遠端端訪問的網路，以及使用的轉換集。有兩個ESP SA，每個方向一個。

```
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** — 顯示對等體上的所有當前IKE SA。AM_ACTIVE狀態表示使用主動模式進行引數交換。

```
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
```

疑難排解

使用本節內容，對組態進行疑難排解。

- 路由器故障排除
- 排除ASA故障

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

路由器故障排除

- **debug crypto isakmp** — 顯示IKE第1階段的ISAKMP協商。
- **debug crypto ipsec** — 顯示IKE第2階段的IPsec協商。

排除ASA故障

- **debug crypto isakmp 127** — 顯示IKE第1階段的ISAKMP協商。
- **debug crypto ipsec 127** — 顯示IKE第2階段的IPsec協商。

相關資訊

- **將ASA 5500作為伺服器並將PIX 506E作為客戶端(NEM)的Easy VPN配置示例**
- **Cisco ASA 5500系列自適應安全裝置產品支援**
- **Cisco 800系列路由器產品支援**
- **IPSec 協商/IKE 通訊協定**
- **技術支援與文件 - Cisco Systems**