PIX/ASA 7.x 이상:Easy VPN with Split Tunneling ASA 5500 as the Server 및 Cisco 871 as the Easy VPN Remote Configuration 예

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance) 5520과 Easy VPN을 사용하는 Cisco 871 라우터 간의 IPsec에 대한 샘플 컨피그레이션을 제공합니다.ASA 5520은 Easy VPN Server의 역할을 하며 Cisco 871 라우터는 Easy VPN Remote Client의 역할을 합니다.이 컨피그레이션에서는 ASA 소프트웨어 버전 7.1(1)을 실행하는 ASA 5520 디바이스를 사용하지만 PIX 운영 체제 버전 7.1 이상을 실행하는 PIX 방화벽 디바이스에 대해서도 이 컨피그레이션을 사용할 수 있습니다.

Cisco VPN 3000 Concentrator에 연결되는 NEM(Network Extension Mode)에서 Cisco IOS® 라우터를 EzVPN으로 구성하려면 VPN 3000 Concentrator를 사용하여 Cisco IOS에서 Cisco EzVPN 클라이언트 구성을 참조하십시오.

Cisco IOS Easy VPN Remote Hardware Client와 PIX Easy VPN Server 간에 IPsec을 구성하려면 PIX Easy VPN Remote Hardware Client to a PIX Easy VPN Server Configuration Example을 참조하십시오.

Cisco 7200 라우터를 EzVPN으로 구성하고 Cisco 871 라우터를 Easy VPN Remote로 구성하려면 7200 Easy VPN Server to 871 Easy VPN Remote Configuration Example을 참조하십시오.

사전 요구 사항

요구 사항

IPsec 및 ASA 7.x 운영 체제에 대한 기본적인 이해가 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Easy VPN Server는 버전 7.1(1)을 실행하는 ASA 5520입니다.
- Easy VPN Remote Hardware Client는 Cisco IOS® Software Release 12.4(4)T1을 실행하는 Cisco 871 라우터입니다.

참고: Cisco ASA 5500 Series 버전 7.x는 PIX 버전 7.x와 유사한 소프트웨어 버전을 실행합니다.이 문서의 구성은 두 제품 라인에 모두 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

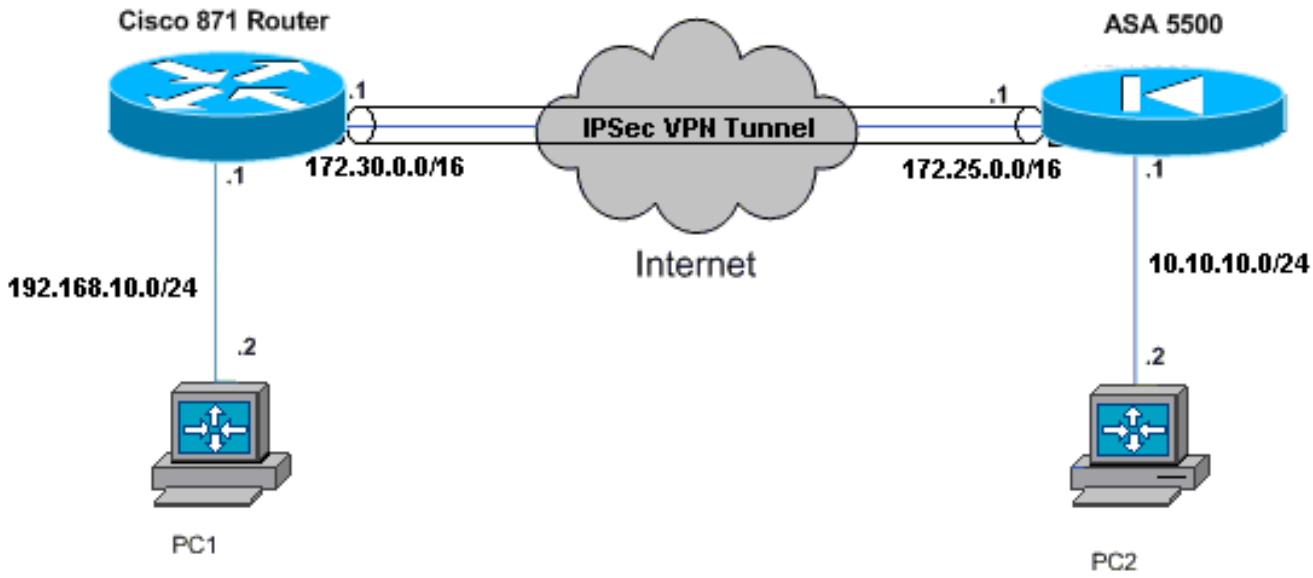
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- 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#
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

두 디바이스를 모두 구성하면 Cisco 871 라우터는 피어 IP 주소를 사용하여 ASA 5520에 자동으로 연결하여 VPN 터널을 설정하려고 시도합니다.초기 ISAKMP 매개변수가 교환되면 라우터에 다음 메시지가 표시됩니다.

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

사용자 이름 및 비밀번호를 입력하라는 **메시지를 표시하는 crypto ipsec client ezvpn xauth** 명령을 입력해야 합니다.이는 ASA 5520에 구성된 사용자 이름과 비밀번호와 일치해야 합니다.사용자 이름과 비밀번호가 두 피어에서 모두 동의하면 나머지 매개변수가 동의되고 IPsec VPN 터널이 나타납니다.

```
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
```

ASA 5520 및 Cisco 871 라우터에서 터널이 제대로 작동하는지 확인하려면 다음 명령을 사용합니다.

- **show crypto isakmp sa** - 피어에 있는 현재 IKE SA(보안 연결)를 모두 표시합니다.QM_IDLE 상태는 SA가 피어로 인증되고 후속 빠른 모드 교환에 사용할 수 있음을 나타냅니다.

```
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** - 현재 SA에서 사용하는 설정을 표시합니다.피어 IP 주소, 로컬 및 원격 모두에서 액세스할 수 있는 네트워크, 사용되는 변형 집합을 확인합니다.ESP(Encapsulating Security Protocol) SA는 각 방향마다 하나씩 2개 있습니다.AH(Authentication Header) 변환 세트는 사용되지 않으므로 비어 있습니다.

```
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 - 현재 SA에서 사용하는 설정을 표시합니다.피어 IP 주소, 로컬 및 원격 끝에서 모두 액세스할 수 있는 네트워크, 사용되는 변형 집합을 확인합니다.ESP SA는 각 방향에 하나씩 2개 있습니다.

```
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 - 피어의 현재 모든 IKE SA를 표시합니다.AM_ACTIVE 상태는 매개변수 교환에 Aggressive 모드가 사용되었음을 나타냅니다.

```
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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

- 라우터 문제 해결
- ASA 문제 해결

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

라우터 문제 해결

- **debug crypto isakmp** - IKE 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto ipsec** - IKE 2단계의 IPsec 협상을 표시합니다.

ASA 문제 해결

- **debug crypto isakmp 127** - IKE 1단계의 ISAKMP 협상을 표시합니다.
- **debug crypto ipsec 127** - IKE 2단계의 IPsec 협상을 표시합니다.

관련 정보

- Easy VPN with an ASA 5500 as the Server, PIX 506E as the Client (NEM) 컨피그레이션 예
- Cisco ASA 5500 Series Adaptive Security Appliances 제품 지원
- Cisco 800 Series 라우터 제품 지원
- IPSec 협상/IKE 프로토콜
- 기술 지원 및 문서 – Cisco Systems