スプリット トンネリング ASA 5500 をサーバとして、Cisco 871 を Easy VPN として使った Easy VPN のリモート設定例

内容

概要

このドキュメントでは、Easy VPN を使用した Cisco Adaptive Security Appliance (ASA) 5520 と Cisco 871 ルータ の間の IPsec 設定例を紹介します。ASA 5520 は Easy VPN サーバ、Cisco 871 ルータは Easy VPN Remote クライアントとして動作します。この設定には ASA ソフトウェア バージョン 7.1(1)が稼働する ASA 5520 デバイスを使用しますが、PIX オペレーティング システム バージョン 7.1 以降が稼働する PIX Firewall デバイスでもこの設定を使用できます。

Cisco VPN 3000コンセントレータに接続するNetwork Extension Mode(NEM)でCisco IOS®ルータをEzVPNとして設定するには、『VPN 3000コンセントレータを使用するCisco IOS上のCisco EzVPNクライアントののの設定』を。

Cisco IOS Easy VPNリモートハードウェアクライアントとPIX Easy VPNサーバ間のIPsecを設定するには、『IOS Easy VPNリモートハードウェアクライアントからPIX Easy VPNサーバへの設定例』を参照してください。

Cisco 7200ルータをEzVPNとして設定し、Cisco 871ルータをEasy VPNリモートとして設定するには、『7200 Easy VPNサーバから871 Easy VPNリモートへの設定例』を参照してください。

前提条件

要件

IPsec と ASA 7.x オペレーティング システムに関する基本的な知識があることを確認してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Easy VPN サーバは、バージョン 7.1(1) が稼働する ASA 5520 です。
- Easy VPNリモートハードウェアクライアントは、Cisco IOS®ソフトウェアリリース12.4T1が稼働するCisco 871ルータです。

注：Cisco ASA 5500シリーズバージョン7.xでは、PIXバージョン7.xと同様のソフトウェアバージョンが稼働しています。このドキュメントで使用する設定は、両方の製品ラインに適用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

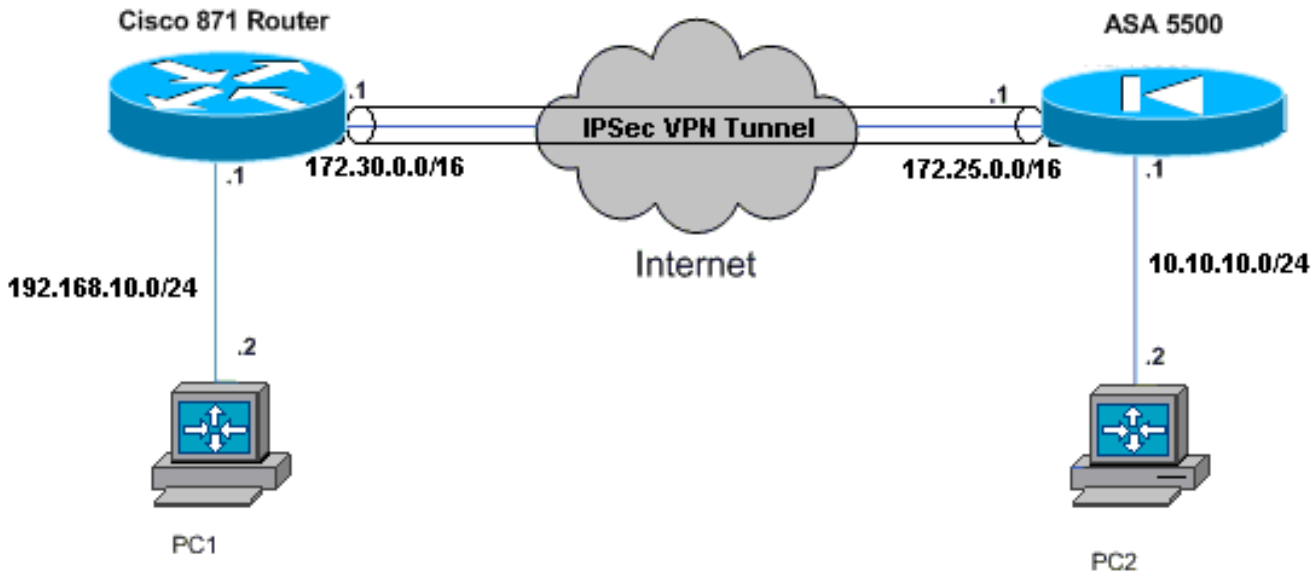
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注： このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- Cisco ASA 5520
- Cisco 871 ルータ

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 ルータ

```
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#
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

両方のデバイスを設定すると、Cisco 871 ルータはピア IP アドレスを使用して ASA 5520 に自動的に接触し、VPN トンネルの設定を試みます。最初の ISAKMP パラメータが交換されると、ルータは次のメッセージを表示します。

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

crypto ipsec client ezvpn xauth コマンドを入力する必要があり、入力するとユーザ名とパスワードが求められます。これは、ASA 5520で設定されているユーザ名とパスワードと一致する必要があります。ユーザ名とパスワードが両方のピアで合意されると、残りのパラメータが一致し、IPsec VPNトンネルが起動します。

```
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
```

次のコマンドを使用して、ASA 5520 と Cisco 871 ルータの両方でトンネルが正しく動作していることを確認します。

- **show crypto isakmp sa：ピア上の現在の IKE セキュリティ アソシエーション（SA）をすべて表示します。**QM_IDLE 状態は、SA がピアと認証された状態であり、後続のクイック モードの交換に使用できることを示します。

```
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：現在の SA で使用されている設定を表示します。**ピア IP アドレス、ローカルとリモートの両端のアクセスが可能なネットワーク、および使用されている変換セットをチェックします。2 つの Encapsulating Security Protocol（ESP）SA が、各方向に 1 つずつあります。Authentication Header（AH; 認証ヘッダ）変換セットは使用されないため、空の状態です。

```
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](): **現在の SA で使用されている設定を表示します。**ピア IP アドレス、ローカルとリモート両端のアクセス可能なネットワーク、および使用されている変換セットをチェックします。2 つの ESP SA が、各方向に 1 つずつあります。

```
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](): ピアにおける現在のIKE SAをすべて表示します。AM_ACTIVE 状態は、パラメータの交換にアグレッシブ モードが使用されたことを示します。

```
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
```

トラブルシュート

このセクションは、設定のトラブルシューティングを行う際に参照してください。

- ルータのトラブルシューティング
- ASA のトラブルシューティング

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

ルータのトラブルシューティング

- **debug crypto isakmp**:IKEフェーズ1のISAKMPネゴシエーションを表示します。
- **debug crypto ipsec**:IKEフェーズ2のIPSecネゴシエーションを表示します。

ASA のトラブルシューティング

- **debug crypto isakmp 127**:IKEフェーズ1のISAKMPネゴシエーションを表示します。
- **debug crypto ipsec 127**:IKEフェーズ2のIPSecネゴシエーションを表示します。

関連情報

- **ASA 5500 をサーバ、PIX 506E をクライアント（NEM）として使用する Easy VPN の設定例**
- **Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス製品のサポート**
- **Cisco 800 シリーズ ルータ製品に関するサポート ページ**
- **IPSec ネゴシエーション/IKE プロトコル**
- **テクニカル サポートとドキュメント – Cisco Systems**