Configuration Professional： 2 つの IOS ルータ間のサイト間 IPSec VPN の設定例

目次

概要

このドキュメントでは、Cisco Configuration Professional（Cisco CP）を使用して、2 台の Cisco IOS® ルータ間に LAN-to-LAN（サイトツーサイト）IPSec トンネルを設定する例を説明します。話を簡単にするため、スタティック ルートを使用します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認します。

- この設定を開始する前に、エンドツーエンドの IP 接続を確立する必要があります。

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くものです。

- Cisco IOS ソフトウェア リリース 12.4(15T) が稼働する Cisco 1841 ルータ
- Cisco CP バージョン 2.5

注: Cisco CP でルータを設定できるようにする方法については、『Cisco Configuration

Professional を使用した基本的なルータ設定』を参照してください。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 のアドレスです。

- ルータ A の Cisco CP 設定
- ルータ B の Cisco CP 設定
- ルータ B の CLI 設定

ルータ A の Cisco CP 設定

Cisco IOS ルータでサイトツーサイト VPN トンネルの設定を行うには、次の手順を実行します。

1. [Configure] > [Security] > [VPN] > [Site-to-Site VPN] の順に選択し、[Create a Site-to-Site VPN] の横にあるオプション ボタンをクリックします。 [Launch the selected task] をクリックします。
2. [Step by step wizard] を選択して設定を続行し、[Next] をクリックします。
3. 次のウィンドウのそれぞれの部分で、VPN 接続情報を指定します。 VPN トンネルのインターフェイスを、ドロップ ダウン メニューから選択します。 ここでは、[FastEthernet0] を選択しています。 [Peer Identity] セクションでは、[Peer with static IP address] を選択し、リモート ピアの IP アドレスを指定しています。 続いて、[Authentication] セクションで [Pre-shared Keys]（この例では *cisco123*）を指定します。 最後に、[Next] をクリックします。
4. [Add] をクリックして、暗号化アルゴリズム、認証アルゴリズム、およびキー交換方法を指定する IKE プロポーザルを追加します。
5. 暗号化アルゴリズム、認証アルゴリズム、およびキー交換方法を指定して、[OK] をクリックします。 暗号化アルゴリズム、認証アルゴリズム、およびキー交換方法の値は、ルータ B で指定するデータと一致している必要があります。
6. [Next] をクリックします。
7. 次の新しいウィンドウではトランスフォーム セットの詳細情報を指定します。 トランスフォーム セットでは、VPN トンネルのデータを保護するのに使用する暗号化アルゴリズムと認証アルゴリズムを指定します。 [Add] をクリックして、これらの詳細情報を指定します。 この方法を使用して、必要に応じて任意の数のトランスフォーム セットを追加できます。
8. トランスフォーム セットの詳細情報（整合性アルゴリズムおよび暗号化アルゴリズム）を

指定して、[OK] をクリックします。
9. 使用する必要な**トランスフォーム セット**をドロップダウン メニューから選択し、[Next] をクリックします。
10. 次のウィンドウで、VPN トンネルによって保護するトラフィックの詳細情報を指定します。 保護するトラフィックの送信元ネットワークおよび宛先ネットワークを指定し、指定した送信元ネットワーク~宛先ネットワーク間のトラフィックが保護されるようにします。 次の例の場合、送信元ネットワークは *10.10.10.0*、宛先ネットワークは *10.20.10.0* です。 [Next] をクリックします。
11. 次のウィンドウで [Finish] をクリックして、ルータ A の設定を完了します。

ルータ B の Cisco CP 設定

Cisco IOS ルータ（ルータ B）でサイトツーサイト VPN トンネルの設定を行うには、次の手順を実行します。

1. [Configure] > [Security] > [VPN] > [Site-to-Site VPN] の順に選択し、[Create a Site-to-Site VPN] の横にあるオプション ボタンをクリックします。 [Launch the selected task] をクリックします。
2. [Step by step wizard] を選択して設定を続行し、[Next] をクリックします。
3. 次のウィンドウのそれぞれの部分で、VPN 接続情報を指定します。 VPN トンネルのインターフェイスを、ドロップ ダウン メニューから選択します。 ここでは、[FastEthernet0] を選択しています。 [Peer Identity] セクションでは、[Peer with static IP address] を選択し、リモート ピアの IP アドレスを指定しています。 続いて、[Authentication] セクションで [Pre-shared Keys]（この例では *cisco123*）を指定します。 最後に、[Next] をクリックします。
4. [Add] をクリックして、暗号化アルゴリズム、認証アルゴリズム、およびキー交換方法を指定する IKE プロポーザルを追加します。
5. 暗号化アルゴリズム、認証アルゴリズム、およびキー交換方法を指定して、[OK] をクリックします。 暗号化アルゴリズム、認証アルゴリズム、およびキー交換方法の値は、ルータ A で指定したデータと一致している必要があります。
6. [Next] をクリックします。
7. 次の新しいウィンドウではトランスフォーム セットの詳細情報を指定します。 トランスフォーム セットでは、VPN トンネルのデータを保護するのに使用する暗号化アルゴリズムと認証アルゴリズムを指定します。 [Add] をクリックして、これらの詳細情報を指定します。 この方法を使用して、必要に応じて任意の数のトランスフォーム セットを追加できます。
8. トランスフォーム セットの詳細情報（整合性アルゴリズムおよび暗号化アルゴリズム）を指定して、[OK] をクリックします。
9. 使用する必要な**トランスフォーム セット**をドロップダウン メニューから選択し、[Next] をクリックします。
10. 次のウィンドウで、VPN トンネルによって保護するトラフィックの詳細情報を指定します。 保護するトラフィックの送信元ネットワークおよび宛先ネットワークを指定し、指定した送信元ネットワーク~宛先ネットワーク間のトラフィックが保護されるようにします。 次の例の場合、送信元ネットワークは *10.20.10.0*、宛先ネットワークは *10.10.10.0* です。 [Next] をクリックします。
11. 次のウィンドウは、サイトツーサイト VPN 設定の要約を示しています。 VPN の接続をテストする場合は、[Test VPN Connectivity after configuring] チェックボックスにチェックマークを入れてください。 今の場合は、VPN の接続をチェックする必要があるので、該当するチェックボックスにチェックマークを入れています。 **[Finish] をクリックします。**
12. [Start] をクリックして、VPN の接続をチェックします。

13. 次のウィンドウに、VPN 接続テストの結果が表示されます。 このウィンドウを見ると、該当トンネルが稼働している（Up）かしていない（Down）かがわかります。 この設定例では、該当トンネルが「Up」になっており、緑色で表示されています。これで Cisco IOS ルータ B の設定が完了し、トンネルが稼働していることがわかります。

ルータ B の CLI 設定

ルータ B

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden !--- as the default values are
chosen. crypto isakmp policy 2 authentication pre-share
!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1 ! ! !--- Configuration for
IPsec policies. !--- Enables the crypto transform
configuration mode, !--- where you can specify the
transform sets that are used !--- during an IPsec
negotiation. crypto ipsec transform-set Router-IPSEC
esp-des esp-sha-hmac ! !--- Indicates that IKE is used
to establish !--- the IPsec Security Association for
protecting the !--- traffic specified by this crypto map
entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description
Tunnel to172.16.1.1 !--- Sets the IP address of the
remote end. set peer 172.16.1.1 !--- Configures IPsec to
use the transform-set !--- "Router-IPSEC" defined
earlier in this configuration. set transform-set Router-
IPSEC !--- Specifies the interesting traffic to be
```

```
encrypted. match address 100 ! ! ! !--- Configures the
interface to use the !--- crypto map "SDM_CMAP_1" for
IPsec. interface FastEthernet0 ip address 172.17.1.1
255.255.255.0 duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet1 ip address
10.20.10.2 255.255.255.0 duplex auto speed auto !
interface FastEthernet2 no ip address ! interface Vlan1
ip address 10.77.241.109 255.255.255.192 ! ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2 ip route
10.77.233.0 255.255.255.0 10.77.241.65 ip route
172.16.1.0 255.255.255.0 172.17.1.2 ! ! ip nat inside
source route-map nonat interface FastEthernet0 overload
! ip http server ip http authentication local ip http
secure-server ! !--- Configure the access-lists and map
them to the Crypto map configured. access-list 100
remark SDM_ACL Category=4 access-list 100 remark IPSec
Rule access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255 ! ! ! !--- This ACL 110 identifies
the traffic flows using route map access-list 110 deny
ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255 access-list
110 permit ip 10.20.10.0 0.0.0.255 any route-map nonat
permit 10 match ip address 110 ! control-plane ! ! line
con 0 login local line aux 0 line vty 0 4 privilege
level 15 login local transport input telnet ssh ! end
```

確認

ここでは、設定が正常に動作していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- IOS ルータ：show コマンド

IOS ルータ：show コマンド

- **show crypto isakmp sa**：現在ピアにあるすべての IKE SA を表示します。`RouterB# show crypto isakmp sa dst src state conn-id slot status 172.17.1.1 172.16.1.1 QM_IDLE 3 0 ACTIVE`
- **show crypto ipsec sa**：現在ピアにあるすべての IPSec SA を表示します。`RouterB# show crypto ipsec sa interface: FastEthernet0 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) current_peer 172.16.1.1 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68 #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68 #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.: 172.17.1.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500 current outbound spi: 0xB7C1948E(3082917006) inbound esp sas: spi: 0x434C4A7F(1129073279) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3004) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xB7C1948E(3082917006) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3002) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`
- **show crypto engine connections active**：現在の接続と、暗号化および復号化されたパケットの情報を表示します。`RouterB#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 3 FastEthernet0 172.17.1.1 set HMAC_SHA+DES_56_CB 0 0 2001`

```
FastEthernet0 172.17.1.1 set DES+SHA 0 59 2002 FastEthernet0 172.17.1.1 set DES+SHA 59 0
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

注: 『debug コマンドの重要な情報』および『IP Security のトラブルシューティング： debug コマンドの理解と使用』を参照してから、**debug** コマンドを使用するようにしてください。

- **debug crypto ipsec 7**：フェーズ 2 の IPSec ネゴシエーションを表示します。**debug crypto isakmp 7**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- **debug crypto ipsec**：フェーズ 2 の IPSec ネゴシエーションを表示します。**debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。

関連情報

- Cisco Configuration Professional クイック スタート ガイド
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems