

# Configuration Professional を使用した Easy VPN サーバとしての IOS ルータの設定例

## 目次

[概要](#)

[前提条件](#)

[使用するコンポーネント](#)

[Cisco CP のインストール](#)

[Cisco CP を実行するためのルータの設定](#)

[要件](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[Cisco CP : Easy VPN サーバの設定](#)

[CLI 設定](#)

[確認](#)

[Easy VPN サーバ : show コマンド](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、[Cisco Configuration Professional \( Cisco CP \)](#) および CLI を使用して、Cisco IOS® ルータを Easy VPN ( EzVPN ) サーバとして設定する方法について説明します。Easy VPN サーバ機能は、リモート エンド ユーザが IP Security ( IPsec ) を使用して任意の Cisco IOS バーチャル プライベート ネットワーク ( VPN ) ゲートウェイと通信できるようにします。集中管理された IPsec ポリシーはサーバによってクライアントデバイスに「プッシュ」されるため、エンド ユーザによる設定を最小化できます。

Easy VPN サーバの詳細は、『[安全な接続設定ガイド ライブラリ、Cisco IOS リリース 12.4T](#)』の「[Easy VPN サーバ](#)」セクションを参照してください。

## 前提条件

### [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 2.1

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。

## [Cisco CP のインストール](#)

次の手順を実行して、Cisco CP をインストールします。

1. Cisco CP V2.1 を [Cisco Software Center](#)（[登録ユーザ専用](#)）からダウンロードし、ローカル PC にインストールします。Cisco CP の最新バージョンは、[Cisco CP Web サイト](#) にあります。
2. ローカル PC で [Start] > [Programs] > [Cisco Configuration Professional (CCP)] の順に選択して Cisco CP を起動し、設定するルータを含む [Community] を選択します。
3. 設定するデバイスを見つけるには、ルータを強調表示して [Discover] をクリックします。

注: Cisco CP v2.1 と互換性がある Cisco ルータ モデルおよび IOS のリリースの詳細は、「[互換性のある Cisco IOS リリース](#)」セクションを参照してください。

注: Cisco CP v2.1 が稼働する PC の要件の詳細は、「[システム要件](#)」セクションを参照してください。

## [Cisco CP を実行するためのルータの設定](#)

Cisco ルータで Cisco CP を稼働させるには、次の設定手順を実行します。

1. Telnet、SSH、またはコンソールを使用してルータに接続します。次のコマンドを使用して、グローバル設定モードに入ります。Router(config)#enable Router(config)#
2. HTTP および HTTPS が有効で、標準外のポート番号を使用するように設定されている場合は、この手順をスキップして、そのまま設定済みのポート番号を使用してください。次の Cisco IOS ソフトウェア コマンドを使用して、ルータの HTTP または HTTPS サーバを有効にします。Router(config)# ip http server Router(config)# ip http secure-server  
Router(config)# ip http authentication local
3. 権限レベル 15 を持つユーザを作成します。Router(config)# username <username> privilege 15 password 0 <password> 注: 設定したいと思うユーザ名 および パスワードと <username> および <password> を取り替えて下さい。
4. SSH および Telnet にローカル ログインおよび権限レベル 15 を設定します。  
Router(config)# line vty 0 4 Router(config-line)# privilege level 15 Router(config-line)# login local Router(config-line)# transport input telnet Router(config-line)# transport input telnet ssh Router(config-line)# exit
5. (任意) ローカル ログインをイネーブルにして、ログ モニタリング機能をサポートします。  
o Router(config)# logging buffered 51200 warning

## [要件](#)

このドキュメントでは、Cisco ルータが完全に動作しており、Cisco CP で設定変更できるように設定されていることを想定しています。

Cisco CP の使用を開始する方法については、『[Cisco Configuration Professional 入門](#)』を参照してください。

## [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、ネットワーク内にあるルータの基本的な設定を行うための情報を提供します。

注: このセクション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。

## Cisco CP : Easy VPN サーバの設定

Cisco IOS ルータを Easy VPN サーバとして設定するには、次の手順を実行します。

1. [Configure] > [Security] > [VPN] > [Easy VPN Server] > [Create Easy VPN Server] の順に選択し、[Launch Easy VPN Server Wizard] をクリックして、Cisco IOS ルータを Easy VPN サーバとして設定します。
2. [Next] をクリックして、Easy VPN サーバの設定を続行します。
3. 表示されたウィンドウで、**仮想インターフェイス** が Easy VPN サーバ設定の一部として設定されます。 **仮想トンネル インターフェイスの IP アドレス**を指定し、VPN クライアントの認証に使用する **認証方法**も選択します。ここで使用している認証方法は [Pre-shared Keys] です。[Next] をクリックします。
4. このルータがリモート デバイスとのネゴシエート時に使用する **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**を指定します。ルータにはデフォルトの IKE ポリシーがあり、必要な場合にはこれを使用できます。新しい IKE ポリシーを追加する場合は、[Add] をクリックします。
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**を次のように指定し、[OK] をクリックします。
6. この例では、**デフォルトの IKE ポリシー**を使用します。このため、デフォルトの IKE ポリシーを選択して [Next] をクリックします。
7. 新しいウィンドウで、**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設定します。[Add] をクリックして詳細情報を指定して、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。注: Cisco CP を使用して設定した場合、ルータにはデフォルトで **CP デフォルト トランスフォーム セット**が存在します。
8. **トランスフォーム セット**の詳細情報 ( **暗号化アルゴリズム**と **認証アルゴリズム** ) を指定して、[OK] をクリックします。
9. この例では、**CP デフォルト トランスフォーム セット**という名前の **デフォルト トランスフォーム セット**を使用します。このため、デフォルトのトランスフォーム セットを選択して [Next] をクリックします。

10. 新しいウィンドウで、グループ ポリシーを設定するサーバを [Local]、[RADIUS]、または [Local and RADIUS] のいずれかから選択します。この例では、ローカルサーバを使用してグループ ポリシーを設定します。[Local] を選択して [Next] をクリックします。
11. この新しいウィンドウで、ユーザ認証に使用するサーバを [Local Only]、[RADIUS]、または [Local Only and RADIUS] のいずれかから選択します。この例では、ローカルサーバを使用して、認証用のユーザ クレデンシャルを設定します。必ず [Enable User Authentication] の横にあるチェックボックスにチェックマークを入れます。[Local Only] を選択して、[Next] をクリックします。
12. [Add] をクリックして新しいグループ ポリシーを作成し、リモート ユーザをこのグループに追加します。
13. [Add Group Policy] ウィンドウの、[Name of This Group] の入力スペースにグループ名 (この例では「cisco」) を入力し、[Pre-shared key] および IP プール ([Starting IP address] と [Ending IP address]) の情報を次に示すように入力して、[OK] をクリックします。注: 新しい IP プールを作成することも、既存の IP プールがある場合はそれを使用することもできます。
14. 続いて、cisco という名前で作成した新しいグループ ポリシーを選択し、必要に応じて [Configure Idle Timer] の横にあるチェックボックスをクリックして、アイドル タイマーを設定します。[Next] をクリックします。
15. 必要に応じて [Cisco Tunneling Control Protocol ( cTCP )] を有効にします。有効にしない場合は、[Next] をクリックします。
16. [Summary of the Configuration] を確認します。[Finish] をクリックします。
17. [Deliver Configuration to Router] ウィンドウで [Deliver] をクリックして、設定をルータに配信します。[Save to file] をクリックすれば、設定をファイルとして PC に保存できます。
18. [Command Delivery Status] ウィンドウには、ルータへのコマンドの配信ステータスが表示されます。[Configuration delivered to router] と表示されます。[OK] をクリックします。
19. 新しく作成した Easy VPN サーバを確認できます。[Edit Easy VPN Server] を選択して、既存のサーバを編集できます。これで、Cisco IOS ルータでの Easy VPN サーバの設定は完了です。

## CLI 設定

### ルータの設定

```
Router#show run Building configuration... Current
configuration : 2069 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption hostname
Router boot-start-marker boot-end-marker no logging
buffered enable password cisco !---AAA enabled using aaa
newmodel command. Also AAA Authentication and
Authorization are enabled---! aaa new-model ! ! aaa
authentication login ciscovpn_xauth_ml_1 local aaa
authorization network ciscovpn_group_ml_1 local ! !
aaa session-id common ip cef ! ! ! ! ip domain name
cisco.com ! multilink bundle-name authenticated ! ! !---
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 1 encr 3des authentication pre-share group
2 crypto isakmp keepalive 10 ! crypto isakmp client
```

```

configuration group cisco key cisco123 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1 match
identity group cisco client authentication list
ciscocp_vpn_xauth_ml_1 isakmp authorization list
ciscocp_vpn_group_ml_1 client configuration address
respond virtual-template 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 ESP-3DES-SHA
esp-3des esp-sha-hmac ! crypto ipsec profile
CiscoCP_Profile1 set security-association idle-time
86400 set transform-set ESP-3DES-SHA set isakmp-profile
ciscocp-ike-profile-1 ! ! ! !--- RSA certificate
generated after you enable the !--- ip http secure-
server command. crypto pki trustpoint TP-self-signed-
1742995674 enrollment selfsigned subject-name cn=IOS-
Self-Signed-Certificate-1742995674 revocation-check none
rsakeypair TP-self-signed-1742995674 !--- Create a user
account named cisco123 with all privileges. username
cisco123 privilege 15 password 0 cisco123 archive log
config hidekeys ! ! !--- Interface configurations are
done as shown below--- interface Loopback0 ip address
10.10.10.10 255.255.255.0 ! interface FastEthernet0/0 ip
address 10.77.241.111 255.255.255.192 duplex auto speed
auto ! interface Virtual-Templatel type tunnel ip
unnumbered Loopback0 tunnel mode ipsec ipv4 tunnel
protection ipsec profile CiscoCP_Profile1 ! !--- VPN
pool named SDM_POOL_1 has been defined in the below
command--- ip local pool SDM_POOL_1 192.168.1.1
192.168.1.254 !--- This is where the commands to enable
HTTP and HTTPS are configured. ip http server ip http
authentication local ip http secure-server ! ! ! !
control-plane ! line con 0 line aux 0 !--- Telnet
enabled with password as cisco. line vty 0 4 password
cisco transport input all scheduler allocate 20000 1000
! ! ! ! end
```

## 確認

### Easy VPN サーバ : show コマンド

ここでは、設定が正常に動作していることを確認します。

- **show crypto isakmp sa** : 現在ピアにあるすべての IKE SA を表示します。Router#show crypto isakmp sa IPv4 Crypto ISAKMP SA dst src state conn-id slot status 10.77.241.111 172.16.1.1 QM\_IDLE 1003 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。Router#show crypto ipsec sa interface: Virtual-Access2 Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0) current\_peer 172.16.1.1 port 1086 PERMIT, flags={origin\_is\_acl,} #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28 #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36 #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 2 local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0 current outbound spi: 0x186C05EF(409732591) inbound esp sas: spi: 0x42FC8173(1123844467) transform: esp-3des esp-sha-hmac

# トラブルシューティング

[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 コマンドを使用する前に、『[デバッグ コマンドの重要な情報](#)』を参照してください。

## 関連情報

- [IPSec ネゴシエーション/IKE プロトコル](#)
- [Cisco Configuration Professional クイック スタート ガイド](#)
- [Cisco 製品に関するサポートページ : ルータ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)