# Cisco VPN 5000 コンセントレータの設定と IPSec メインモード LAN-to-LAN VPN 接続の実装

## 目次



## はじめに

このドキュメントでは、Cisco VPN 5000 コンセントレータの初期設定について説明し、IP を使用したネットワークへの接続方法、および IPSec メインモード LAN-to-LAN VPN 接続の提供方法を紹介します。

によってインストール ファイアウォールに関連してネットワークにそれを接続する 2 つの設定のどちらかに VPN コンセントレータを、できます。 VPN コンセントレータは 2 つのイーサネット ポートを、そのうちの一つ備えています ( イーサネットは IPSecトラフィックしか通過させません 1 ) 。 他のポート ( イーサネットは 0 ) すべての IP トラフィックをルーティングします。 ファイアウォールに平行して VPN コンセントレータをインストールすることを計画する場合イーサネット 0 が保護された LAN に直面し、イーサネット 1 がネットワークのインターネット ゲートウェイ ルータを通してインターネットに直面するように両方のポートを使用して下さい。 インターネットとコンセントレータの間で渡る IPSecトラフィックがファイアウォールによって通過するように、また保護された LAN でファイアウォールの後ろで 0 ポート VPN コンセントレータをインストールし、イーサネットによって接続できます。

## 前提条件

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

この 文書に記載されている 情報は Cisco VPN 5000 コンセントレータに基づいています。

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、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、どのような作業についても、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。

# 基本的な接続設定

基本的なネットワーク接続を確立する最も簡単な方法は 0 ポート シリアルケーブルを VPN コンセントレータのコンソールポートに接続し、イーサネットの IP アドレスを設定するのにターミナルソフトウェアを使用することです。 イーサネットの IP アドレスを設定した後 0 ポート設定を完了するために、VPN コンセントレータに接続するのに Telnet を使用できます。 また適切なテキストエディタのコンフィギュレーション ファイルを生成でき VPN コンセントレータに TFTP を使用してそれを送信 します。

コンソールポートを通したターミナルソフトウェアを使用する、パスワードのために最初にプロンプト表示されます。 使用して下さいパスワード「letmein」。を パスワードで応答の後で、システム情報を用いるプロンプトに応答する **configure ip ethernet 0 コマンドを**発行して下さい。プロンプトのシーケンスは次の例のように見える必要があります。

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

この場合イーサネットを設定して準備ができています 1 つのポート。

## イーサネット 1 ポートの設定

イーサネットの TCP/IP アドレッシング情報は 1 つのポート VPN コンセントレータに割り当てた外部、インターネットルート可能な TCP/IP アドレスです。 これがコンセントレータの TCP/IP を無効に するのでイーサネット 0 と同じ TCP/IP ネットワークでアドレスを使用することを避けて下さい。

システム情報を用いるプロンプトに応答する**設定 IP イーサネット 1** コマンドを入力して下さい。プロンプトのシーケンスは次の例のように見える必要があります。

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1
      *[ IP Ethernet 1 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
      *[ IP Ethernet 1 ]# mode=routed
      *[ IP Ethernet 1 ]#
```

この場合 IPSecゲートウェイを設定する必要があります。

## IPSec ゲートウェイの設定

VPN コンセントレータがすべての IPSec を送信 するところ IPSecゲートウェイ制御、またはトンネル伝送される、トラフィック。 これは以降を設定するデフォルト· ルートの依存しないです。システム情報を用いるプロンプトに応答する **configure general コマンドの**入力から開始して下さい。プロンプトのシーケンスは下記に示されている例のように見える必要があります。

```
* IntraPort2+_A56CB700# configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

**注:** リリース 6.x およびそれ以降では、**ipsecgateway コマンドは vpngateway コマンド**に変更されました。

この場合インターネット キー エクスチェンジ（IKE）ポリシーを設定しよう。

## IKE ポリシーの設定

トンネルセッションを設定するために VPN コンセントレータおよびクライアントがどのように互いを識別し、認証するか Internet Security Association Key Management Protocol（ISAKMP）/IKE パラメータ制御。 この最初のネゴシエーションはフェーズ 1.フェーズ 1 パラメータがデバイスにグローバルで、特定のインターフェイスと関連付けられないので参照されます。 このセクションで認識されるキーワードは下記です。 LAN-to-LAN トンネルのためのフェーズ 1 ネゴシエーション パラメータは[トンネルパートナー <Section ID>]セクションで設定されるかもしれません。 VPN コンセントレータおよび VPN クライアントが個々 トンネル セッションをどのように処理するかフェーズ 2 IKE ネゴシエーション制御。 VPN コンセントレータおよび VPN クライアントのためのフェーズ 2 IKE ネゴシエーション パラメータは[VPNグループ <Name>]デバイスで設定されます。

IKE ポリシーのための構文は次の通りです。

```
* IntraPort2+_A56CB700# configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Protection キーワードは VPN コンセントレータと VPN クライアント間の ISAKMP/IKE ネゴシエーションのためのプロテクションスイートを規定 します。 このキーワードは VPN コンセントレータが特定のプロテクションスイートすべてを提案すればこのセクション内の複数回を現われるかもしれません。 VPN クライアントはネゴシエーションのためのオプションの 1 つを受け入れます。 各オプションの最初のピース、MD5（5）メッセージ要約は、ネゴシエーションに使用する認証アルゴリズムです。 SHA は MD5 よりセキュアであると考慮されるセキュアハッシュアルゴリズムを意味します。 各オプションの第 2 ピースは暗号化アルゴリズムです。 DES（データ暗号規格）は 56 ビット キーをデータをスクランブルするのに使用します。 各オプションの第 3 ピースは鍵交換に使用する Diffie-Hellmanグループです。 大きい数がグループ 2（G2）アルゴリズムによって使用されるので、グループ 1（G1）よりセキュアです。

設定を開始するために、システム情報を用いるプロンプトに応答する**設定 IKE ポリシー** コマンドを入力して下さい。 次に例を示します。

```
* IntraPort2+_A56CB700# configure IKE Policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

基本を設定したので、それはトンネルおよび IPコミュニケーション パラメータを定義する時間です。

# 主要モードサイト間の設定

LAN-to-LAN接続をサポートするために VPN コンセントレータを設定するためにトンネル設定、またトンネルで使用されるべき IPコミュニケーション パラメータを定義する必要があります。 2 つのセクションでこれを、[トンネルパートナーVPN X]セクション、および[IP VPN x]セクションします。 ある特定のサイト間の設定に関しては、これら二つのセクションで定義される *x* はトンネル設定がプロトコル 設定ときちんと関連付けられるように一致する必要があります。

これらのセクションのそれぞれを詳しく検知 しよう。

## トンネル・パートナー・セクションの設定

Tunnel Partner セクションでは、少なくとも次の 8 つのパラメータを定義して下さい。

- トランスフォーム

- パートナー
- KeyManage
- Shared-key
- モード
- LocalAccess
- ピア
- BindTo

## トランスフォーム

Transform キーワードは IKE クライアントセッションに使用する保護タイプおよびアルゴリズムを規定 します。 このパラメータと関連付けられる各オプションは認証および暗号化パラメータを規定 する 保護部分です。 トランスフォーム パラメータは 1 つがセッションの間に使用のためのクライアントによって受け入れられるまで、VPN コンセントレータが彼らが解析される順序で指定された保護の部分を提案すればこのセクション内の複数回を現われるかもしれません。 ほとんどの場合、1 Transform キーワードだけ必要です。

Transform キーワードのためのオプションは次の通りです。

```
* IntraPort2+_A56CB700# configure IKE Policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

ESP は Encapsulating Security Payload を意味し、AH は認証ヘッダーを意味します。 これらのヘッダが両方ともパケットを暗号化し、認証するのに使用されています。 DES （データ暗号規格）は 56 ビット キーをデータをスクランブルするのに使用します。 トリプル DES は DES アルゴリズムの 3 つの異なるキーおよび 3 つのアプリケーションをデータをスクランブルするのに使用します。 MD5 は message-digest 5 ハッシュ アルゴリズムです。 SHA は MD5 より幾分セキュアの考慮されるセキュアハッシュアルゴリズムです。

ESP(MD5,DES) はデフォルト設定で、ほとんどの設定用の推奨されます。 パケットを認証する ESP(MD5) および ESP（SHA）使用 ESP （暗号化無しで）。 パケットを認証する AH(MD5) および AH（SHA）使用 AH。 AH(MD5)+ESP(DES)、AH(MD5)+ESP(3DES)、
AH（SHA）+ESP（DES）、および AH(SHA)+ESP(3DES) パケットを暗号化するためにパケットおよび ESP を認証する使用 AH。

## パートナー

Partner キーワードはトンネル パートナーシップの他のトンネル ターミネータの IP アドレスを定義します。 この数はローカル VPN コンセントレータが IPSec接続を作成できるルーティング可能IPアドレス パブリックである必要があります。

## KeyManage

KeyManage キーワードはどのデバイスがトンネルを開始し、続くべきかどのようなトンネル確

立の手順をトンネル パートナーシップの 2 つの VPN コンセントレータがどのように判別するか定義します。 オプションは Auto , Initiate , Respond および Manual です。 最初の 3 つのオプションおよび固定暗号化トンネルを設定するために IKE トンネルを設定するのに Manual キーワードを使用できます。 この資料は固定暗号化トンネルを設定する方法を取り扱っていません。 オートはトンネルパートナーがトンネルセットアップ要求に始まり、応答できること規定 します。 開始はトンネルパートナーがトンネルセットアップ要求だけを送信 すること、それ応答しません規定 しますそれらに。 トンネルパートナーがトンネル セットアップ要求に応答するが、決して始めませんそれらを応答しないで下さいこと規定 しましたり。

## Shared-key

SharedKey キー キーワードは IKE 共有秘密として使用されます。 両方のトンネルパートナーの同じ SharedKey値を設定して下さい。

## モード

Mode キーワードは IKE ネゴシエーション プロトコルを定義します。 デフォルト設定は積極的です、従ってインターオペラビリティ モードのための VPN コンセントレータを設定するために、本管に Mode キーワードを設定して下さい。

## LocalAccess

LocalAccess はトンネルを通してアクセスすることができるホスト マスクからデフォルト・ルートに IP 数を定義します。 IP プロトコル数がトンネルを通して、ICMP(1) のような、TCP(6) アクセスすることができる LocalProto キーワードは、UDP(17) を、等定義します。 すべての IP 数を渡したいと思う場合 LocalProto=0 を設定する必要があります。 LocalPort はどのポート番号がトンネルを通して達することができるか判別します。 LocalProto および LocalPort は両方 0、または all-access にデフォルトで設定されます。

## ピア

ピア キーワードはどのサブネットがトンネルを通してあるか規定 します。 PeerProto はどのポート番号がトンネルの反対側でアクセスすることができるかどのプロトコルがリモート トンネル エンドポイントによって許可される、PeerPort は設定しますか規定 し。

## BindTo

BindTo はどのイーサネットポートがサイト間接続を終えるか規定 します。 VPN コンセントレータがシングルポート モードで動作しているときイーサネット 1 にこのパラメータを、を除いて常に設定する必要があります。

## パラメータの設定

これらのパラメータを設定するために、**設定トンネルパートナーVPN を**システム情報を用いるプロンプトに応答する **1 つの**コマンド入力して下さい。

プロンプトのシーケンスは下記の例のように見える必要があります。

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
```

```
      Section ?config Tunnel Partner VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
      *[ Tunnel Partner VPN 1 ]# sharedkey=letmein
      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
      *[ Tunnel Partner VPN 1 ]# mode=main
      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
      *[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
      *[ Tunnel Partner VPN 1 ]# exit
      Leaving section editor.
```

この場合それは IP セクションを設定する時間です。

## IP セクションの設定

各トンネル パートナーシップの IPコンフィギュレーション セクションで番号付き または 非番号接続 ( WAN 接続の次 IPコンフィギュレーション ) を使用できます。 ここでは、非番号を使用しました。

非番号 サイト間 接続のための最低限の設定は 2 つの文を必要とします: numbered=false および mode=routed。 **configure ip vpn 1 コマンドの**入力から開始し、システム プロンプトに次の通り応答して下さい。

```
*[ IP Ethernet 0 ]# configure ip vpn 1
      Section ?IP VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP VPN 1 ]# mode=routed
      *[ IP VPN 1 ]# numbered=false
```

この場合それはデフォルト・ ルートを設定する時間です。

## デフォルト ルート (TCP/IP ルート テーブル) の設定

ダイナミックルートを持っているかどれのためにそれが直接接続されるか、またはネットワーク以外ネットワークに向かうすべての TCP/IP トラフィックを送信 するのに使用 VPN コンセントレータができるデフォルト・ ルートを設定する必要があります。 内部ポートで見つけられるすべてのネットワークに戻るデフォルト・ ルート ポイント。 既に IPSecゲートウェイパラメータを使用してインターネットに出入して IPSecトラフィックを送信 するために Intraport を設定しました。 デフォルト・ ルート設定を開始するために、システム情報を用いるプロンプトに応答する edit config ip static コマンドを入力して下さい。 プロンプトのシーケンスは下記の例のように見える必要があります。

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
```

```
End of buffer
Edit [ IP Static ]> append 1
Enter lines at the prompt. To terminate input, enter
a . on a line all by itself.
Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
Append> .
Edit [ IP Static ]> exit
Saving section...
Checking syntax...
Section checked successfully.
*IntraPort2+_A56CB700#
```

# 仕上げ

最後のステップは設定を保存することです。 設定をダウンロードし、デバイスを再起動したいと思い、**y を**入力し、『Enter』 を押すことを確かめるかどうか尋ねられた場合。 ブートプロセスの間に VPN コンセントレータを消さないで下さい。 コンセントレータがリブートした後、ユーザはコンセントレータの VPN クライアント ソフトウェアを使用して接続できます。

設定を保存するために、**save コマンドを**、次の通り入力して下さい。

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

Telnet を使用して VPN コンセントレータに接続される場合、上記の出力は表示されるすべてです。 コンソールを通して接続される場合、次と同じような出力が大いに長ただ表示されます。 この出力の端に、VPN コンセントレータは戻します「HELLO コンソール…」を そしてパスワードを頼みます。 これは終了することをどのように確認するかです。

```
*IntraPort2+_A56CB700# save
      Save configuration to flash and restart device? y
```

# 関連情報

- Cisco VPN 5000 シリーズ コンセントレータの販売終了の発表
- Cisco VPN 5000 コンセントレータに関するサポートページ
- Cisco VPN 5000 クライアントに関するサポート ページ
- IPsec に関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems