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

内容

概要

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。

VPNコンセントレータは、ファイアウォールに関連してネットワークに接続する場所に応じて、2つの設定のいずれかでインストールできます。VPNコンセントレータには2つのイーサネットポートがあり、そのうちの1つ(Ethernet 1)はIPSecトラフィックのみを渡します。他のポート(Ethernet 0)はすべてのIPトラフィックをルーティングします。ファイアウォールと並行してVPNコンセントレータをインストールする場合は、Ethernet 0が保護されたLANに面し、Ethernet 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介してインターネットに面するように、両方のポートを使用する必要があります。また、保護されたLANにファイアウォールの背後にVPNコンセントレータをインストールし、Ethernet 0ポートを介して接続することで、インターネットとコンセントレータ間を通過するIPSecトラフィックがファイアウォールを通過するようにすることもできます。

前提条件

要件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco VPN 5000コンセントレータに基づくものです。

このマニュアルの情報は、特定のラボ環境に置かれた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。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について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、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、ターミナルソフトウェアを使用してイーサネット0ポートのIPアドレスを設定することです。イーサネット0ポートのIPアドレスを設定した後、Telnetを使用してVPNコンセントレータに接続し、設定を完了できます。適切なテキストエディタで設定ファイルを生成し、TFTPを使用してVPNコンセントレータに送信することもできます。

コンソールポートからターミナルソフトウェアを使用すると、最初にパスワードの入力を求められます。パスワード「letmein」を使用します。 パスワードで応答した後、**configure ip ethernet 0**コマンドを発行し、システム情報をプロンプトに応答します。プロンプトのシーケンスは、次の例のようになります。

```
*[ 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 ]#
```

これで、イーサネット1ポートを設定する準備ができました。

イーサネット 1 ポートの設定

Ethernet 1ポートのTCP/IPアドレス情報は、VPNコンセントレータに割り当てた、インターネットでルーティング可能な外部TCP/IPアドレスです。Ethernet 0と同じTCP/IPネットワークでアドレスを使用することは避けてください。これは、コンセントレータでTCP/IPが無効になるためです。

configure ip ethernet 1コマンドを入力し、システム情報とプロンプトに応答します。プロンプトのシーケンスは、次の例のようになります。

```
*[ 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 ]#
```

次に、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

IPSecゲートウェイは、VPNコンセントレータがすべてのIPSec（トンネル化された）トラフィックを送信する場所を制御します。これは、後で設定するデフォルトルートとは無関係です。**configure general**コマンドを入力し、**シス**テム情報を含むプロンプトに応答します。プロンプトのシーケンスは、次の例のようになります。

```
* 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以降では、ipsecgatewayコマンドが**vpngateway**コマンドに変更さ**れま**した。

次に、インターネットキーエクスチェンジ(IKE)ポリシーを設定します。

IKE ポリシーの設定

Internet Security Association Key Management Protocol(ISAKMP)/IKEパラメータは、VPNコンセントレータとクライアントが互いを識別して認証し、トンネルセッションを確立する方法を制御します。この初期ネゴシエーションはフェーズ1と呼ばれます。フェーズ1パラメータはデバイスに対してグローバルであり、特定のインターフェイスに関連付けられません。このセクションで認識されるキーワードを次に示します。LAN-to-LANトンネルのフェーズ1ネゴシエーションパラメータは、[Tunnel Partner <Section ID>]セクションで設定できます。フェーズ2 IKEネゴシエーションは、VPNコンセントレータとVPN Clientが個々のトンネルセッションを処理する方法を制御します。VPNコンセントレータとVPN Clientのフェーズ2 IKEネゴシエーションパラメータは、[VPN Group <Name>]デバイスで設定します。

IKEポリシーの構文は次のとおりです。

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```

protectionキーワードは、VPNコンセントレータとVPN Client間のISAKMP/IKEネゴシエーションの保護スイートを指定します。この項では、このキーワードが複数回表示される場合があります。この場合、VPNコンセントレータは指定されたすべての保護スイートを提案します。VPN Clientは、ネゴシエーションのオプションのいずれかを受け入れます。各オプションの最初の部分であるMD5(Message Digest 5)は、ネゴシエーションに使用される認証アルゴリズムです。

SHAはSecure Hash Algorithm（SHA；セキュアハッシュアルゴリズム）を意味し、MD5よりも安全であると見なされます。各オプションの2番目の部分は暗号化アルゴリズムです。DES(Data Encryption Standard)は56ビットの鍵を使用してデータをスクランブルする。各オプションの3番目の部分は、キー交換に使用されるDiffie-Hellmanグループです。グループ2(G2)アルゴリズムで使用される数が多いため、グループ1(G1)よりも安全です。

設定を開始するには、システム情報を含むプロン**プトに応答**して、configure IKE policyコマンドを入力します。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#
```

基本的な設定が完了したので、トンネルとIP通信パラメータを定義します。

主要モードサイト間の設定

LAN-to-LAN接続をサポートするようにVPNコンセントレータを設定するには、トンネル設定と、トンネルで使用するIP通信パラメータを定義する必要があります。これは、[Tunnel Partner VPN x]セクションと[IP VPN x]セクションの2つのセクションで行います。特定のサイト間設定の場合、トンネル設定がプロトコル設定に適切に関連付けられるように、この2つのセクションで定義されている*x*が一致している必要があります。

これらの各セクションを詳しく見てみましょう。

トンネル・パートナー・セクションの設定

トンネルパートナーセクションでは、少なくとも次の8つのパラメータを定義する必要があります。

- Transform
- パートナー
- KeyManage
- 共有キー
- モード
- ローカルアクセス
- ピア
- バインド

Transform

Transformキーワードは、IKEクライアントセッションに使用される保護タイプとアルゴリズムを指定します。このパラメータに関連付けられている各オプションは、認証と暗号化のパラメータを指定する保護ピースです。このセクションでは、Transformパラメータが複数回表示される場合があります。この場合、VPNコンセントレータは、セッション中にクライアントによって使用が

許可されるまで、指定された保護部分を解析された順序で提示します。ほとんどの場合、必要なTransformキーワードは1つだけです。

Transformキーワードのオプションは次のとおりです。

```
[ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES) | ESP(MD5) |
ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES) |
AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]
```

ESPはEncapsulating Security Payload（カプセル化セキュリティペイロード）を表し、AHは認証ヘッダーを表します。これらのヘッダーは両方とも、パケットの暗号化と認証に使用されます。DES(Data Encryption Standard)は56ビットの鍵を使用してデータをスクランブルする。3DESは3つの異なるキーとDESアルゴリズムの3つのアプリケーションを使用して、データをスクランブルします。MD5は、message-digest 5(MD5)ハッシュアルゴリズムです。SHAはSecure Hash Algorithm（SHA；セキュアハッシュアルゴリズム）であり、MD5よりもややセキュアであると見なされます。

ESP(MD5,DES)はデフォルト設定であり、ほとんどのセットアップで推奨されます。ESP(MD5)およびESP(SHA)は、ESPを使用してパケットを認証します（暗号化なし）。AH(MD5)およびAH(SHA)はAHを使用してパケットを認証します。AH(MD5)+ESP(DES)、AH(MD5)+ESP(3DES)、AH(SHA)+ESP(DES)、およびAH(SHA)+ESP(3DES)は、パケットを認証するためにAHを使用します。

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終端装置のIPアドレスを定義します。この番号は、ローカルVPNコンセントレータがIPSec接続を作成できる、パブリックでルーティング可能なIPアドレスである必要があります。

KeyManage

KeyManageキーワードは、トンネルパートナーシップ内の2つのVPNコンセントレータが、どのデバイスがトンネルを開始し、どのタイプのトンネル確立手順に従うかを決定する方法を定義します。オプションは、[自動(Auto)]、[開始(Initiate)]、[応答(Respond)]、[手動(Manual)]です。最初の3つのオプションを使用してIKEトンネルを設定し、Manualキーワードを使用して固定暗号化トンネルを設定できます。このドキュメントでは、固定暗号化トンネルの設定方法については説明しません。[自動(Auto)]は、トンネルパートナーがトンネル設定要求を開始および応答できることを指定します。[開始(Initiate)]は、トンネルパートナーがトンネル設定要求のみを送信し、それに応答しないことを指定します。[応答(Respond)]は、トンネルパートナーがトンネル設定要求に応答することを指定しますが、トンネルを開始しません。

共有キー

SharedKey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で同じSharedKey値を設定する必要があります。

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[Aggressive]であるため、VPNコンセントレータを相互運用モードに設定するには、Modeキーワードを[Main]に設定する必要があります。

ローカルアクセス

LocalAccessは、ホストマスクからデフォルトルートまで、トンネルを通じてアクセスできるIP番号を定義します。LocalProtoキーワードは、ICMP(1)、TCP(6)、UDP(17)など、トンネル経由でアクセスできるIPプロトコル番号を定義します。すべてのIP番号を渡す場合は、LocalProto=0を設定する必要があります。LocalPortは、どのポート番号にトンネル経由で到達できるかを決定します。LocalProtoとLocalPortの両方がデフォルトで0またはall-accessに設定されます。

ピア

Peerキーワードは、トンネルを介して検出されるサブネットを指定します。PeerProtoは、リモートトンネルエンドポイントを介して許可されるプロトコルを指定し、PeerPortは、トンネルのもう一方の端でアクセスできるポート番号を設定します。

バインド

BindToは、サイト間接続を終端するイーサネットポートを指定します。このパラメータは、VPNコンセントレータがシングルポートモードで実行されている場合を除き、常にEthernet 1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には、configure Tunnel Partner VPN 1コマンドを入力し、システム情報を含むプロンプトに応答します。

プロンプトのシーケンスは、次の例のようになります。

```
*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.
```

次に、IPセクションを設定します。

IP セクションの設定

各トンネルパートナーシップのIP設定セクションでは、（WAN接続のIP設定のように）番号付きまたは非番号接続を使用できます。ここでは、アンナンバードを使用しました。

非番号サイト間接続の最小設定には、次の2つの文が必要です。numbered=falseおよびmode=routed。configure ip vpn 1コマンドを入力し、次のようにシステムプロンプトに応答しま

す。

```
*[ 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
```

次に、デフォルトルートを設定します。

デフォルト ルート (TCP/IP ルート テーブル) の設定

VPNコンセントレータが直接接続されているネットワーク以外のネットワークまたはダイナミックルートを持つネットワーク宛てのすべてのTCP/IPトラフィックを送信するために使用できるデフォルトルートを設定する必要があります。デフォルトルートは、内部ポートで検出されたすべてのネットワークを指し示します。IPSecゲートウェイパラメータを使用してインターネットとの間でIPSecトラフィックを送信するように、Intraportを既に設定しています。デフォルトルート設定を開始するには、edit config ip staticコマンドを入力し、システム情報を含むプロンプトに応答します。プロンプトのシーケンスは、次の例のようになります。

```
*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

最後の手順は、設定を保存することです。構成をダウンロードしてデバイスを再起動するかどうかを確認するメッセージが表示されたら、**yと入力して**Enterキーを**押します**。ブートプロセス中はVPNコンセントレータをオフにしないでください。コンセントレータのリブート後、ユーザはコンセントレータのVPN Clientソフトウェアを使用して接続できます。

設定を保存するには、次のように**save**コマンドを入力します。

```
*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している場合は、上記の出力がすべて表示されます。コンソール経由で接続している場合は、次のような出力が表示されますが、表示される時間ははるかに長くなります。この出力の最後に、VPNコンセントレータは「Hello Console...」を返します パスワードを要求します。これが自分が終わったことを知る方法です。

```
Codesize => 0 pfree => 462
      Updating Config variables...
      Adding section '[ General ]' to config
      Adding -- ConfiguredFrom = Command Line, from Console
      Adding -- ConfiguredOn = Timeserver not configured
      Adding -- DeviceType = IntraPort2
      Adding -- SoftwareVersion = IntraPort2 V4.5
      Adding -- EthernetAddress = 00:00:a5:6c:b7:00
      Not starting command loop: restart in progress.
      Rewriting Flash....
```

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お知らせ
- 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 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