Cisco VPN 5000 Concentrator の初期およびリモート・クライアント・アクセス用セットアップ

内容

概要

このガイドでは、Cisco VPN 5000コンセントレータの初期設定、特にIPを使用してネットワークに接続し、リモートクライアント接続を提供するための設定方法について説明します。

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。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ある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の間を通過する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特有の要件はありません。

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。

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。Ethernet 0ポートのIPアドレスを設定したら、Telnetを使用してコンセントレータに接続し、設定を完了できます。また、適切なテキストエディタでコンフィギュレーションファイルを生成し、TFTPを使用して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以下のようになります：

```
*[ 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

Ethernet 1ポートのTCP/IPアドレス情報は、コンセントレータに割り当てた外部のインターネットルーティング可能な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。VPNコンセントレータでは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以下のようになります：

```
*[ 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、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

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。後で、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を設定します。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以下のようになります：

```
*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#
```

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

IPSecゲートウェイは、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、設定した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以下のようになります：

```
* 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#
```

次に、IKEポリシーを設定します。

IKE ポリシー

コンセントレータのInternet Security Association Key Management Protocol(ISAKMP/IKE)パラメータを設定します。これらの設定は、トンネルセッションを確立するために、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は関連付けられていません。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クライアント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クライアントのフェーズ2 IKEネゴシエーションパラメータは、[VPN Group <Name>]デバイスで設定されます

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クライアント間の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、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。クライアントは、ネゴシエーションのオプションの1つを受け入れます。各オプションの最初の部分であるMD-5(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。

```
* 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#
```

基本が設定されたので、グループパラメータを入力します。

VPNグループ設定

グループパラメータを入力する際には、コマンドラインパーサーでVPNグループ名にスペースを入力できる場合でも、VPNグループ名にスペースを含めることはできません。VPNグループ名には、文字、数字、ダッシュ、およびアンダースコアを使用できます。

各VPNグループでIP操作に必要な4つの基本パラメータがあります。

- Maxconnections
- StartIPaddressまたはLocalIPNet
- Transform
- IPNet

Maxconnectionsパラメータは、この特定のVPNグループ設定で許可される同時クライアントセッションの最大数です。この数値はStartIPAddressまたはLocalIPNetパラメータと組み合わせて動作するので、注意してください。

VPNコンセントレータは、StartIPAddressとLocalIPNetという2つの異なる方式でリモートクライアントにIPアドレスを割り当てます。StartIPAddressは、接続されているクライアントのEthernet 0とproxy-arpsに接続されているサブネットのIP番号を割り当てます。LocalIPNetは、VPNクライアントに固有のサブネットからリモートクライアントにIP番号を割り当てます。そのため、ネットワークの残りの部分は、スタティックルーティングまたはダイナミックルーティングを通じてVPNサブネットの存在を認識する必要があります。StartIPAddressを使用すると設定が簡単になりますが、アドレス空間のサイズが制限されることがあります。LocalIPNetは、リモートユーザに対するアドレス指定の柔軟性を高めますが、必要なルーティングを設定するには少し作業が必要です。

StartIPAddressでは、着信クライアントトンネルセッションに割り当てられた最初のIPアドレスを使用します。基本設定では、これは内部TCP/IPネットワーク（イーサネット0ポートと同じネットワーク）のIPアドレスである必要があります。 次の例では、最初のクライアントセッションに192.168.233.50アドレスが割り当てられ、次の同時クライアントセッションに192.168.233.51が割り当てられます。Maxconnectionsの値を30に割り当てました。つまり、使用されていないIPアドレスが30個あるブロック（DHCPサーバがある場合は含む）は、192.168.233.50で始まり、192.168.233.79で終わる必要があります。異なるVPNグループ設定で使用するIPアドレスを重複しないでください。

LocalIPNetは、LAN上の他の場所で使用されていないサブネットからリモートクライアントにIPアドレスを割り当てます。たとえば、VPNグループ設定でパラメータ「LocalIPNet=182.168.1.0/24」を指定すると、コンセントレータは192.168.1.1で始まるクライアントにIPアドレスを割り当てます。そのため、LocalIPNetを使用してIP番号を割り当る際時に「Maxconnections=255444224540000000000000000000000000000000000000000000000000000

Transformキーワードは、コンセントレータがIKEクライアントセッションに使用する保護タイプとアルゴリズムを指定します。オプションは次のとおりです。

```
Transform = [ 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) ]
```

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部分です。このキーワードは、このセクション内で複数回表示される場合があります。この場合、コンセントレータは、指定された保護部分をセッション中にクライアントが使用できるように受け入れるまで、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。

ESP(SHA,DES)、ESP(SHA,3DES)、ESP(MD5,DES)、およびESP(MD5,3DES)は、パケットを暗号化および認証するためのEncapsulating Security Payload(ESP)ヘッダーを表します。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、SHAはSecure Hash Algorithm(SHA)であり、MD5よりもややセキュアと見なされます。

ESP(MD5,DES)はデフォルト設定であり、ほとんどのインストールで推奨されます。
ESP(MD5)およびESP(SHA)は、ESPヘッダーを使用して、暗号化のないパケットを認証します。
AH(MD5)およびAH(SHA)は、認証ヘッダー(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認証ヘッダーを使用します。

注： Mac OS ClientソフトウェアはAHオプションをサポートしていません。Mac OSクライアントソフトウェアを使用する場合は、少なくとも1つのESPオプションを指定する必要があります。

IPNetフィールドは、コンセントレータクライアントの移動先を制御するため、重要です。このフィールドに入力する値によって、どのTCP/IPトラフィックがトンネル接続されるか、あるいはより一般的に、このVPNグループに属するクライアントがネットワーク上を通過できるかが決まります。

内部ネットワーク(この例では192.168.233.0/24)を設定することを推奨します。これにより、内部ネットワークに向かうクライアントからのすべてのトラフィックがトンネルを介して送信され、認証および暗号化されます（暗号化を有効にした場合）。 このシナリオでは、他のトラフィックはトンネリングされません。通常どおりルーティングされます。単一またはホストアドレスを含む複数のエントリを持つことができます。形式はアドレス(この例ではネットワークアドレス192.168.233.0)で、そのアドレスに関連付けられたマスクはビット(/24)で表されます。これはクラスCマスクです。

configure VPN group basic-userコマンドを入力して設定のこの部分を開始し、システム情報を入力してプロンプトに応答します。設定シーケンス全体の例を次に示します。

```
*IntraPort2+_A56CB700# configure VPN group basic-user
      Section 'VPN Group basic-user' 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 "?"
      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
                                   or
      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24
      *[ VPN Group "basic-user" ]# maxconnections=30
      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)
      *[ VPN Group "basic-user" ]# ipnet=192.168.233.0/24
      *[ VPN Group "basic-user" ]# exit
      Leaving section editor.
      *IntraPort2_A51EB700#
```

次に、ユーザのデータベースを定義します。

VPN ユーザコンフィギュレーション

設定のこのセクションでは、VPNユーザデータベースを定義します。各行は、VPNユーザとそのユーザのVPNグループの設定およびパスワードを定義します。複数行のエントリには、バックスラッシュで終わる改行が必要です。ただし、二重引用符で囲まれた改行は保持されます。

VPNクライアントがトンネルセッションを開始すると、クライアントのユーザ名がデバイスに送信されます。デバイスはこのセクションでユーザを検出すると、エントリの情報を使用してトンネルをセットアップします。（RADIUSサーバをVPNユーザの認証に使用することもできます）。 デバイスでユーザ名が見つからず、認証を実行するようにRADIUSサーバを設定していない場合、トンネルセッションが開かず、クライアントにエラーが返されます。

edit config VPN usersコマンドを入力して、設定**を開始**します。VPNグループ「basic-user」に「User1」という名前のユーザを追加する例を見てみましょう。

```
*IntraPort2+_A56CB700# edit config VPN users
      Section 'VPN users' not found in the config.
      Do you want to add it to the config? y
      <Name> <Config> <SharedKey>
      Editing "[ VPN Users ]"...
      1: [ VPN Users ]
      End of buffer
      Edit [ VPN Users ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> User1 Config="basic-user" SharedKey="Burnt"
      Append> .
      Edit [ VPN Users ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

このユーザーのSharedKeyは「Burnt」です。 これらの設定値はすべて大文字と小文字が区別されます。「User1」を設定する場合は、クライアントソフトウェアに「User1」と入力する必要があります。「user1」と入力すると、「invalid or unauthorized user」エラーメッセージが表示されます。エディタを終了する代わりにユーザの入力を続行できますが、エディタを終了するにはピリオドを入力する必要があります。そうしないと、設定に無効なエントリが発生する可能性があります。

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、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