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

目次

はじめに

このガイドは IP を使用してネットワークに接続するために Cisco VPN 5000 コンセントレータの初期設定を、とりわけそれを設定する方法を説明しリモートクライアント接続を提供します。

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コンセントレータを、できます。 コンセントレータに 2 つのイーサネットポートが、そのうちの一つあります (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 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しては個別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。

本書の情報は、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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。

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、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。 ：

```
*[ 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

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 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 VPN 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。 ：

```
*[ 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

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。 以降、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 を設定します。 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。 :

```
*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#
```

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

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。 これはちょうど設定したデフォルト・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。 :

```
* 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 ポリシーを設定して下さい。

IKE ポリシー

Internet Security Association Key Management Protocol を/Internet Key Exchange（IKE）（コンセントレータのための ISAKMP/IKE）パラメータ設定して下さい。 これらの設定はトンネルセッションを設定するために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、認証するか制御します。 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。

フェーズ 2 IKE ネゴシエーション制御どのように VPN コンセントレータおよびクライアントハンドル個々のトンネルセッション。 VPN コンセントレータおよび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。 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、MD-5（5） message-digest 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。

```
* 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#
```

基本が設定されるので、グループ パラメータを入力して下さい。

VPNグループ設定

グループ パラメータを入力した場合、コマンド・ライン パーサーが VPNグループ名で領域を入力することを可能にするのに VPNグループ名は領域がはいらないはずであることを覚えて下さい。 VPNグループ名は文字、数、ダッシュおよびアンダースコアが含まれている場合があります。

IP オペレーションに各 VPNグループに必要となる 4 つの基本的なパラメータがあります:

- Maxconnections
- StartIPaddress か LocalIPNet
- トランスフォーム
- 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。 StartIPAddress または LocalIPNet パラメータと共にはたらくように、この数に留意して下さい。

VPN コンセントレータは 2 方式、StartIPAddress および LocalIPNet によってリモートクライアントに IP アドレスを割り当てます。 StartIPAddress は接続されたクライアントにイーサネット 0 およびプロキシARP に接続されるサブネットからの IP 数を割り当てます。 LocalIPNet は VPN クライアントにユニークなサブネットからのリモートクライアントに IP 数を割り当てネットワークの他がスタティック または ダイナミック ルーティングによる VPN サブネットのプロシージャを認識されていることを必要とします。 StartIPAddress はより容易な設定を提供しましたり、アドレス スペースのサイズを制限するかもしれません。 LocalIPNet はリモートユーザ向けのアドレッシングの柔軟性を提供しますが、わずかにより多くの作業を必要なルーティングを設定するように要求します。

StartIPAddress に関しては、着信クライアント トンネル セッションに割り当てられる最初の IP アドレスを使用して下さい。 基本設定コンフィギュレーションセットアップでは、これは内部 TCP/IP ネットワーク（イーサネットと同じネットワーク 0 ポート）の IP アドレスであるはずです。 下記の例では、最初のクライアントセッション 192.168.233.50 アドレスは、次の同時クライアントセッション割り当てられます 192.168.233.51 を、等割り当てられます。 ある場合 192.168.233.50 から開始するおよび 192.168.233.79 で終了する 30 未使用 IP アドレスのブロックが（を含む DHCP サーバ）ある必要があることを意味する 30 という Maxconnections 値を割り当てました。 異なる VPNグループ設定で使用される IP アドレスとオーバーラップすることを避けて下さい。

LocalIPNet は LAN で他の所で未使用である必要があるサブネットからの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グループ設定のパラメータ "LocalIPNet=182.168.1.0/24" を規定 すれば、コンセントレータは 192.168.1.1 から開始しているクライアントに IP アドレスを割り当てます。 従って、"Maxconnections=254" を割り当てる必要がありまコンセントレータがサブネット境界に番号が付いている注意しないので割り当てた場合 IP を LocalIPNet を使用します。

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のために使用する保護タイプをおよびアルゴリズムを規定 します。 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#
```

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。 このキーワードは 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、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。

ESP （SHA、DES ）、ESP(SHA,3DES)、ESP(MD5,DES)、および ESP(MD5,3DES) はパケットを暗号化し、認証するために Encapsulating Security Payload （ESP ）ヘッダを表示します。 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 アルゴリズムであり、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、ほとんどのインストールのために推奨されます。 暗号化無しでパケットを認証する ESP(MD5) および ESP（SHA ）使用 ESP ヘッダ。 パケットを認証する AH(MD5) および AH（SHA ）使用 Authentication Header （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 ヘッダを認証する使用認証ヘッダー。

注: Mac OS クライアントソフトウェアは AH オプションをサポートしません。 Mac OS クライアントソフトウェアを使用する場合少なくとも 1 つの ESP オプションを規定 する必要があります。

IPNet フィールドはコンセントレータ クライアントがどこに行くことができるか制御するので、重要です。 このフィールドで入力する値はこの VPNグループに属するクライアントがネットワークで行くことができるところでどんな TCP/IP トラフィックがトンネル伝送される、または一般にはか判別します。

Cisco は（この例 192.168.233.0/24 で ）内部ネットワークを設定することを推奨します、従って（暗号化を有効に すれば ）内部ネットワークに行っているトンネルを通してクライアントからのすべてのトラフィックは送信 され、従って認証され、暗号化されます。 このシナリオでは、他のトラフィックはトンネル伝送されません; その代り、ずっとそれは正常にルーティングしています。 単一かホスト アドレスを含む複数のエントリが、あることができます。 形式はアドレスです（次に例、ネットワーク アドレスで 192.168.233.0 ）およびビット（クラス C マスクである ）/24 のそのアドレスと関連付けられるマスク。

設定のこの一部を**設定 VPNグループ基本ユーザ** コマンドの入力から開始し、次にシステム情報を用いるプロンプトに応答して下さい。 コンフィギュレーション全体シーケンスの例はここにあります:

```
*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#
```

次のステップはユーザ データベースを定義することです。

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。 各行はそのユーザの VPNグループ設定およびパスワードと共に VPN ユーザを定義します。 マルチライン エントリはバックスラッシュで終了する改行がなければなりません。 ただし、二重引用符で囲まれている改行は維持されます。

VPN クライアントがトンネルセッションを始めるとき、クライアントのユーザ名はデバイスに送信されます。 デバイスがこのセクションでユーザを見つける場合、エントリで情報をトンネルを設定するのに使用します。 （ また VPN ユーザの認証のために RADIUSサーバを使用できます ）。 デバイスがユーザ名を見つけないし、認証を行うために RADIUSサーバを設定しなかったら場合トンネルセッションは開かないし、エラーはクライアントに返されます。

edit config vpn users コマンドの入力から設定を開始して下さい。 VPNグループ「基本ユーザ」に名前を挙げられるユーザを "User1" 追加する例を示します。

```
*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#
```

このユーザの Shared-key は「焼き付けられます」。 これらの設定値すべては大文字/小文字の区別があります; "User1" を設定する場合、ユーザはクライアントソフトウェアで "User1" を入力する必要があります。 "user1" を入力することは無効なまたは許可されていないユーザ エラーメッセージという結果に終ります。 エディタを終了するかわりにユーザを入力し続けることができます覚えるために、エディタを終了するために期間に入って下さい。 そうする失敗により設定で無効なエントリを引き起こす場合があります。

仕上げ

最後のステップは設定を保存しています。 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 をタイプし、入力 キー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 VPN クライアント ソフトウェアを使用して接続できます。

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

```
*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、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