Cisco ルータへの Cisco VPN 3000 コンセントレータの設定

目次

はじめに

この設定例では、Cisco IOS® ソフトウェアを実行するルータの背後にあるプライベート ネットワークを Cisco VPN 3000 コンセントレータの背後にあるプライベート ネットワークに接続する方法を示します。 ネットワーク上のデバイスは、プライベート アドレスによって互いを認識します。

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 12.3.(1)a の Cisco 2611 ルータ**注:** Cisco 2600 シリーズ ル

ータが VPN 機能をサポートする暗号 IPSec VPN IOSイメージとインストールされていることを確かめて下さい。

- 4.0.1 B の Cisco VPN 3000 コンセントレータ

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。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメント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。

設定

このドキュメントでは次の設定を使用します。

ルータの設定

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
```

```
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
```

```
line con 0
line aux 0
line vty 0 4
!
end
```

VPN コンセントレータの設定

この試験的セッティングでは、VPN コンセントレータはコンソールポートを通して最初にアクセスされ、それ以上の設定がグラフィカル ユーザ インターフェイス（GUI）によってすることができるように最小コンフィギュレーションは追加されます。

VPN コンセントレータに現在のコンフィギュレーションがないことを確認するために > **System Reboot > Schedule reboot > Reboot with ファクトリ/デフォルト 設定** 『管理』 を選択 して下さい。

VPN コンセントレータは Quick Configuration に現われ、これらの項目はリブートの後で設定されます:

- 時間/日付
- Configuration Interfaces（パブリック アドレス = 200.1.1.2/24、プライベート アドレス = 192.168.10.1/24）でのインターフェイス/マスク
- Configuration > System > IP routing > Default_Gateway（200.1.1.1）のデフォルト ゲートウェイ

この段階で、VPN コンセントレータは、内部ネットワークから HTML を介してアクセスできます。

注: VPN コンセントレータが外部でから管理されるので、また選択しなければなりません:

- **Configuration > Interfaces** > 2 **パブリックは > IPフィルタを > 私用 1.選択します（デフォルト）**。
- *外部*マネージャの IP アドレスを追加する **Administration > Access Rights > Access Control List** > Add Manager Workstation。

これは*外部*から VPN コンセントレータを管理しなければ必要ではないです。

1. インターフェイスを再確認するために後始動 GUI Configuration > Interfaces の順に選択 しました。
2. IPsec のための**デフォルト**（インターネット）**ゲートウェイ**および**トンネル デフォルト**（中）**ゲートウェイを**プライベート ネットワークの他のサブネットに到達するために設定するように > IP Routing > Default Gateways を Configuration > System の順に選択 して下さい。
3. 暗号化されるべきトラフィックを定義するネットワークリストを作成するために > Network Lists を Configuration > Policy Management の順に選択 して下さい。これらはローカルネットワークです:これらはリモートネットワークです:
4. 完了時の 2 つのネットワーク リストは次のとおりです。**注:** IPSecトンネルが起動しない場合、関連 トラフィックが両側で一致するかどうか確認するため。 関連 トラフィックはルータおよび PIX ボックスのアクセス リストによって定義されます。 彼らは VPN コンセントレータのネットワークリストによって定義されます。
5. **LAN-to-LAN** Configuration > System > Tunneling Protocols > IPsec の順に選択 し、LAN-to-LAN トンネルを定義して下さい。

6. 『Apply』 をクリック した後、このウィンドウは LAN-to-LAN トンネル設定の結果として自動的に作成される他の設定と表示されます。以前に 作成された LAN-to-LAN IPSec パラメータは **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** で表示または修正することができます。
7. アクティブIKE 提案を確認するために Configuration > System > Tunneling Protocols > IPSec > IKE Proposals の順に選択 して下さい。
8. セキュリティ結合のリストを表示するために Configuration > Policy Management > Traffic Management > Security Associations の順に選択 して下さい。
9. Security Associationの名前をクリックし、次にセキュリティ結合を確認するために『Modify』 をクリック して下さい。

確認

このセクションはこの設定で使用される **show コマンドを**リストします。

インターフェイス設定です。

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

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。

- show crypto ipsec sa ：現在の SA が使用する設定を表示します。
- **show crypto isakmp sa** —ピアですべての現在のインターネット 鍵 交換 セキュリティ アソシエーションを示します。
- **show crypto engine connection active** —すべての暗号化エンジンのための現在のアクティブな暗号化されたセッション接続を表示します。

特殊なコマンドについての詳細を見るのに IOS Command Lookup Tool （登録ユーザのみ）を使用できます。

VPN コンセントレータ上で使用する場合

記録を回すために Configuration > System > Events > Classes > Modify の順に選択 して下さい。次のオプションを使用できます。

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

ログに対する重大度 = 1 ～ 13

コンソールに対する重大度 = 1 ～ 3

>イベントログを取得する**イベントログ** 『Monitoring』 を選択 して下さい。

トラブルシューティング

インターフェイス設定です。

debug コマンドを試みる前に Debug コマンドの重要な情報を参照して下さい。

- **debug crypto engine**：暗号化されたトラフィックを表示します。
- **debug crypto ipsec**：フェーズ 2 の IPSec ネゴシエーションを表示します。
- **debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。

問題-トンネルを開始することが不可能

エラー メッセージ

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
```

```
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

解決策

同時ログオンの望ましい 番号を設定するか、またはこの SA のための 5 に同時ログオンを設定するためにこの操作を完了して下さい:

10.19.187.229 > 全般 > Simultaneouts ログインを Configuration > User Management > Groups > Modify の順に進み、5.にログインの数を変更して下さい。

PFS

IPSec のネゴシエーションでは、Perfect Forward Secrecy（PFS; 完全転送秘密）によって、それぞれの新しい暗号鍵が以前の鍵とは独立したものであることが保証されます。 両方のトンネルピアの PFS を有効に するか、または無効に して下さい。 さもなければ、LAN-to-LAN（L2L）IPSecトンネルはルータで確立されません。

新しいセキュリティ結合のための要求を受け取る時 IPsec が PFS を必要とすること新しいセキュリティ結合がこの暗号マップエントリのために要求される、またはとき IPsec が PFS を頼む必要があること規定 するために、クリプト マップ コンフィギュレーションモードで **set pfs コマンドを**使用して下さい。 IPsec が PFS を要求するべきではないこと規定 するためにこのコマンドの **no 形式を**使用して下さい。

```
set pfs [group1 | group2]
no set pfs
```

set pfs コマンドについて：

- *group1* —新しい Diffie-Hellman交換が実行された時 IPsec が 768-bit Diffie Hellman プライム

記号係数グループを使用する必要があること規定 します。
- *group2* —新しい Diffie-Hellman交換が実行された時 IPsec が 1024 ビット Diffie Hellman プライム記号剰余グループを使用する必要があること規定 します。

デフォルトでは、PFS は要求されません。 このコマンドでグループを指定しない場合は、デフォルトで group1 が使用されます。

例：

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

set pfs コマンドに関する詳細については Cisco IOSセキュリティ コマンドレファレンスを参照して下さい。

関連情報

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- Cisco VPN 3000 シリーズ コンセントレータ
- Cisco VPN 3002 Hardware Client
- IPSec ネゴシエーション/IKE プロトコル
- テクニカル サポートとドキュメント – Cisco Systems