

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

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[VPN コンセントレータの設定](#)

[確認](#)

[インターフェイス設定です。](#)

[VPN コンセントレータ上で使用する場合](#)

[トラブルシューティング](#)

[インターフェイス設定です。](#)

[問題-トンネルを開始することが不可能](#)

[PFS](#)

[関連情報](#)

概要

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

一々が 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

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、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分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。

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
<pre>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</pre>

```
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) によって行う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、これらの項目は再度ブートするの後に設定されます:

- 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 > 1. Private (デフォルト) 選択します。

- 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、LAN-to-LAN トンネル設定の結果として自動的に作成されるこのウィンドウは他の設定と表示する。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

用できません。

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

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

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、またはディセーブルにして下さい。さもなければ、LAN-to-LAN な (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 デフィーヘルマン 主な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 デフィーヘルマン 主な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](#)