LAN のサブネットが重複しているルータ間での IPSec トンネルの設定

目次

概要

このドキュメントでは、同じ IP アドレス方式を持つ 2 つの企業の統合をシミュレートするネットワーキング例を示します。 2 台のルータが VPN トンネルで接続され、各ルータの背後にあるネットワークは同じです。 あるサイトが他のサイトにあるホストにアクセスする場合、送信元アドレスと送信先アドレスの両方を異なるサブネットに変換するために、ルータ上でネットワークアドレス変換（NAT）が使用されます。

注: この設定は常置セットアップとしてネットワーク管理観点から複雑であるので推奨されません。

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。

- ルータ A： Cisco IOS® ソフトウェア リリース 12.3(4)T を実行する Cisco 3640 ルータ
- ルータ B： Cisco IOS® ソフトウェア リリース 12.3(5)を実行する Cisco 2621 ルータ

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。

背景説明

この例では、サイト A のホスト 172.16.1.2 がサイト B で同じ IP アドレスが指定されした ホストをアクセス したときに、それは 172.16.1.2 実際のアドレスによりもむしろ 172.19.1.2 にアドレスを接続します。 サイト B へのアクセス サイト A のホストが 172.18.1.2 に、それアドレスを接続する時。 ルータ A 上の NAT では、172.16.x.x のアドレスは、172.18.x.x のホスト エントリに一致するように変換されます。 ルータ B の NAT では、172.16.x.x を 172.19.x.x に変換します。

各ルータの暗号 機能はシリアルインターフェイスを渡る変換されたトラフィックを暗号化します。 NAT がルータの暗号化の*前*に発生することに注目して下さい。

注: この設定は 2 つのネットワークだけが通信するようにします。 インターネット接続には使用できません。 2 つのサイト以外場所への接続のためのインターネットに追加パスを必要とします; すなわち、ホストでいくつものルートが設定されている両方の側で別のルータかファイアウォールを、追加する必要があります。

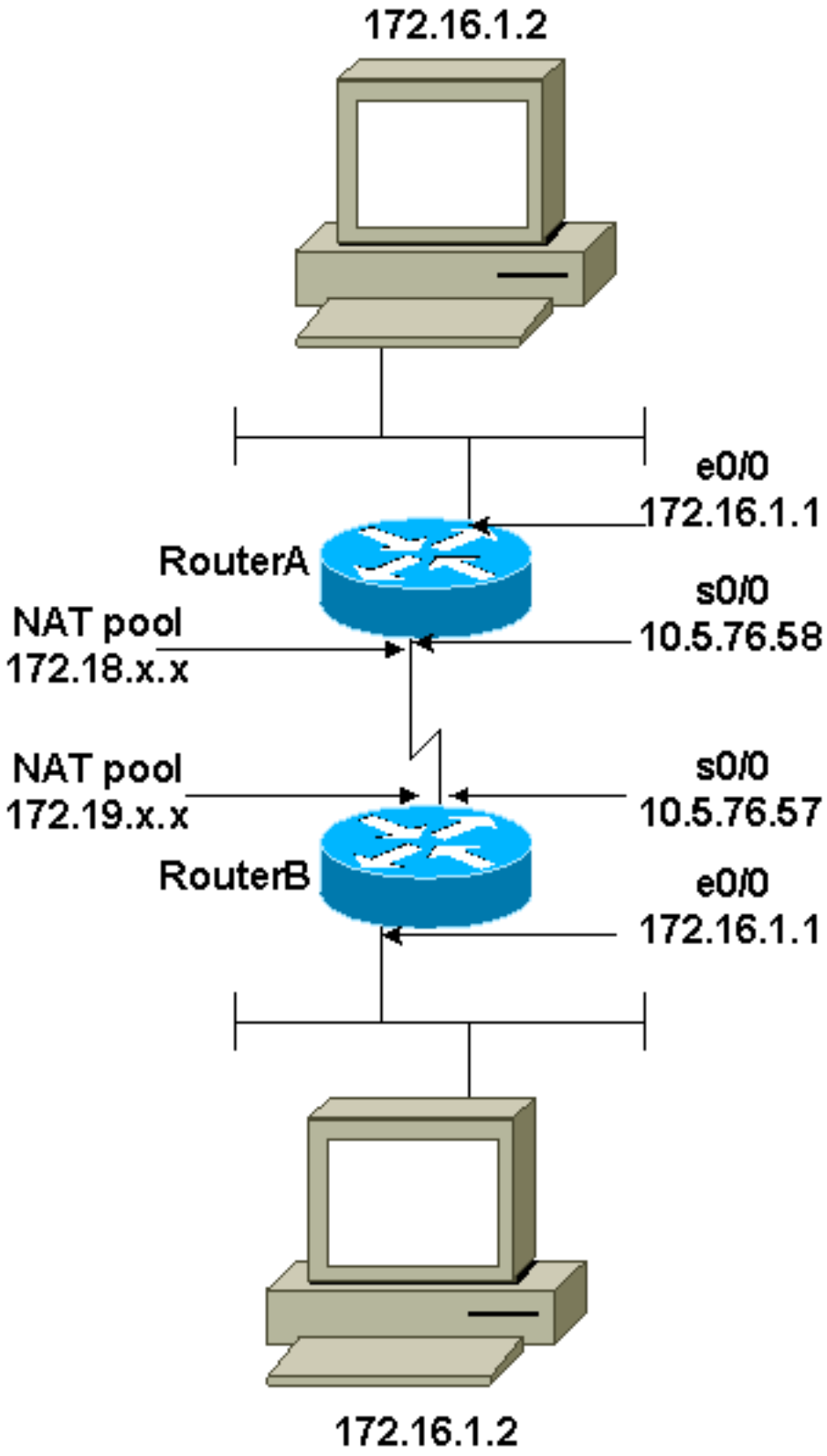
設定

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 A
- ルータ B

ルータ A
Current configuration : 1404 bytes

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10 encr 3des hash md5
authentication pre-share crypto isakmp key cisco123
address 10.5.76.57 ! !--- These are the IPSec
parameters. crypto ipsec transform-set myset1 esp-3des
esp-md5-hmac ! ! crypto map mymap 10 ipsec-isakmp set
peer 10.5.76.57 set transform-set myset1 !--- Encrypt
traffic to the other side. match address 100 ! ! !
interface Serial0/0 description Interface to Internet ip
address 10.5.76.58 255.255.0.0 ip nat outside clockrate
128000 crypto map mymap ! interface Ethernet0/0 ip
address 172.16.1.1 255.255.255.0 no ip directed-
broadcast ip nat inside half-duplex ! ! !--- This is the
NAT traffic. ip nat inside source static network
172.16.0.0 172.18.0.0 /16 no-alias ip http server no ip
http secure-server ip classless ip route 0.0.0.0 0.0.0.0
Serial0/0 ! !--- Encrypt traffic to the other side.
access-list 100 permit ip 172.18.0.0 0.0.255.255
172.19.0.0 0.0.255.255 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! ! end
```

ルータ B

```
Current configuration : 1255 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-15
!
boot-start-marker
boot-end-marker
!
!
memory-size iomem 15
no aaa new-model
ip subnet-zero
!
!
```

```
!
ip audit notify log
ip audit po max-events 100
!
!--- These are the IKE parameters. crypto isakmp policy
10 encr 3des hash md5 authentication pre-share crypto
isakmp key cisco123 address 10.5.76.58 ! !--- These are
the IPSec parameters. crypto ipsec transform-set myset1
esp-3des esp-md5-hmac ! crypto map mymap 10 ipsec-isakmp
set peer 10.5.76.58 set transform-set myset1 !---
Encrypt traffic to the other side. match address 100 ! !
interface FastEthernet0/0 ip address 172.16.1.1
255.255.255.0 ip nat inside duplex auto speed auto !
interface Serial0/0 description Interface to Internet ip
address 10.5.76.57 255.255.0.0 ip nat outside crypto map
mymap ! !--- This is the NAT traffic. ip nat inside
source static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server no ip http secure-server ip classless ip
route 0.0.0.0 0.0.0.0 Serial0/0 ! !--- Encrypt traffic
to the other side. access-list 100 permit ip 172.19.0.0
0.0.255.255 172.18.0.0 0.0.255.255 ! ! line con 0 line
aux 0 line vty 0 4 ! ! ! end
```

確認

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提供しています。

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show crypto ipsec sa**：フェーズ 2 のセキュリティ アソシエーションを表示します。
- **show crypto isakmp sa**：フェーズ 1 のセキュリティ アソシエーションを表示します。
- show ip nat translation - 現在使用されている NAT 変換を表示します。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

トラブルシューティングのためのコマンド

特定の **show** コマンドは、Output Interpreter Tool（登録ユーザ専用）によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- **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 Internet Security Association and Key Management Protocol（ISAKMP）ネゴシエーションを表示します。
- **debug crypto engine**：暗号化されたトラフィックを表示します。

関連情報

- IPSec に関するサポート ページ
- IPsec ネットワーク セキュリティの設定
- インターネット キー交換セキュリティ プロトコルの設定
- テクニカルサポート - Cisco Systems