Configuring an IPSec Tunnel Between Routers with Duplicate LAN Subnets

Document ID: 14143

Contents

Introduction

This document provides a networking example that simulates two merging companies with the same IP addressing scheme. Two routers are connected with a VPN tunnel, and the networks behind each router are the same. For one site to access hosts at the other site, Network Address Translation (NAT) is used on the routers to change both the source and the destination addresses to different subnets.

Note: This configuration is not recommended as a permanent setup because it would be confusing from a network management standpoint.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Router A: Cisco 3640 router running Cisco IOS® Software Release 12.3(4)T
- Router B: Cisco 2621 router running Cisco IOS® Software Release 12.3(5)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Background Information

In this example, when host 172.16.1.2 at Site A accesses the same IP−addressed host at Site B, it connects to a 172.19.1.2 address rather than to the actual 172.16.1.2 address. When the host at Site B to accesses Site A, it connects to a 172.18.1.2 address. NAT on Router A translates any 172.16.x.x address to look like the matching 172.18.x.x host entry. NAT on Router B changes 172.16.x.x to look like 172.19.x.x.

The crypto function on each router encrypts the translated traffic across the serial interfaces. Note that NAT occurs *before* encryption on a router.

Note: This configuration only allows the two networks to communicate. It does not allow for Internet connectivity. You need additional paths to the Internet for connectivity to locations other than the two sites; in other words, you need to add another router or firewall on each side, with multiple routes configured on the hosts.
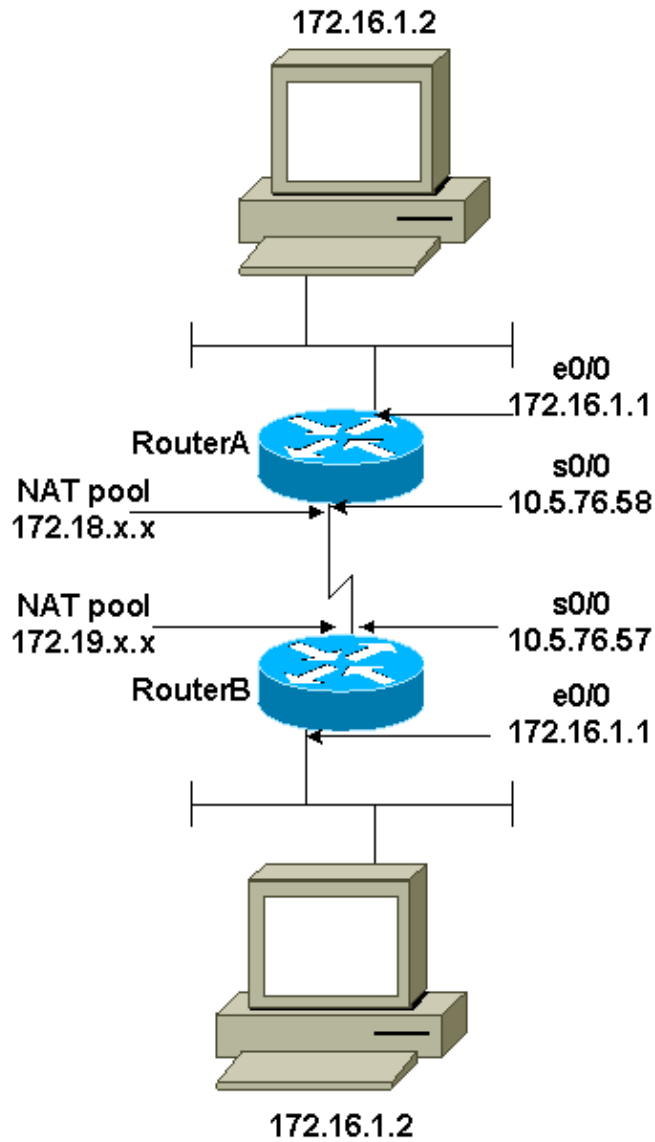
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup:

172.16.1.2

RouterA
e0/0
172.16.1.1
s0/0
10.5.76.58

NAT pool
172.18.x.x

NAT pool
172.19.x.x

s0/0
10.5.76.57

RouterB
e0/0
172.16.1.1

172.16.1.2

Configurations

This document uses these configurations:

- Router A
- Router B

Router 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
```

Router 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
```

Verify

This section provides information you can use to confirm your configuration is working properly.

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show crypto ipsec sa** Shows the phase 2 security associations.
- **show crypto isakmp sa** Shows the phase 1 security associations.
- **show ip nat translation** Shows the current NAT translations in use.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

- **debug crypto ipsec** Shows the IPSec negotiations of phase 2.
- **debug crypto isakmp** Shows the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.
- **debug crypto engine** Shows the traffic that is encrypted.

Related Information

- **IPSec Support Page**
- **Configuring IPSec Network Security**

- **Configuring Internet Key Exchange Security Protocol**
- **Technical Support – Cisco Systems**

Updated: Jan 14, 2008 Document ID: 14143