

# Configuring IPsec Router-to-Router Fully Meshed

Document ID: 14134

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Configure

- Network Diagram
- Configurations

### Verify

### Troubleshoot

- Troubleshooting Commands

### Related Information

---

## Introduction

This sample configuration shows fully-meshed encryption between three routers through the use of one crypto map on each router to the networks behind each of its two peers.

Encryption is to be done from:

- 160.160.160.x network to 170.170.170.x network
- 160.160.160.x network to 180.180.180.x network
- 170.170.170.x network to 180.180.180.x network

## 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:

- Cisco IOS® Software Release 12.2.7C and 12.2.8(T)4
- Cisco 2500 and 3600 routers

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 the Cisco Technical Tips Conventions .

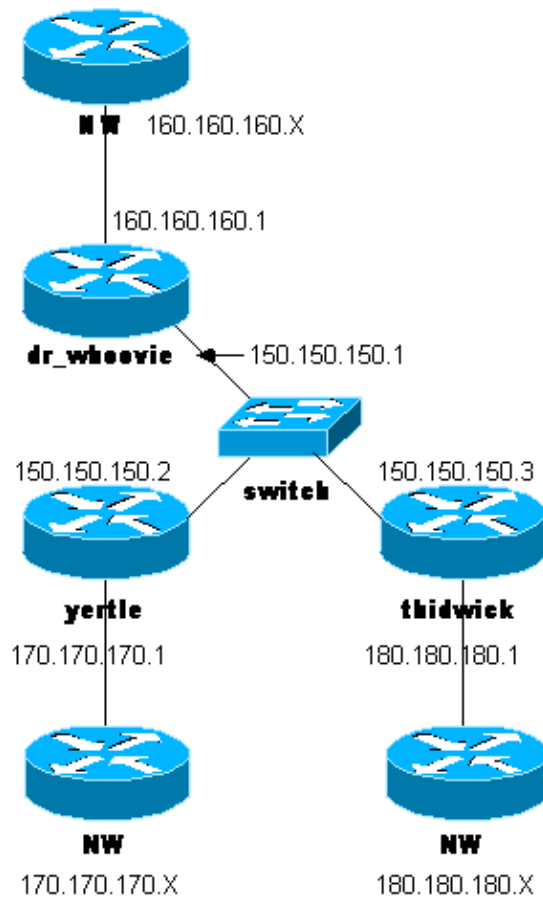
# Configure

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 the network setup shown in this diagram.



## Configurations

This document uses these configurations.

- Dr\_Whoovie Configuration
- Yertle Configuration
- Thidwick Configuration

**Note:** These configurations were recently tested with the current code (November 2003) within the document.

### Dr\_Whoovie Configuration

```
Current configuration:
!
version 12.2
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGN.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!

!--- Internet Key Exchange (IKE) Policies:

crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.3
crypto isakmp key cisco123 address 150.150.150.2
!

!--- IPSec Policies:

crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
!
crypto map ETH0 17 ipsec-isakmp
set peer 150.150.150.2
set transform-set 170cisco

!--- Include the 160.160.160.x to 170.170.170.x network
!--- in the encryption process.

match address 170
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco

!--- Include the 160.160.160.x to 180.180.180.x network
!--- in the encryption process.

match address 180
!
interface Ethernet0
ip address 150.150.150.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Ethernet1
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0
ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface Serial1
no ip address
no ip directed-broadcast
clockrate 4000000
```

```

!
ip classless
ip route 170.170.170.0 255.255.255.0 150.150.150.2
ip route 180.180.180.0 255.255.255.0 150.150.150.3
no ip http server
!

!--- Include the 160.160.160.x to 170.170.170.x network
!--- in the encryption process.

access-list 170 permit ip 160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255

!--- Include the 160.160.160.x to 180.180.180.x network
!--- in the encryption process.

access-list 180 permit ip 160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end

```

### Yertle Configuration

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!

!--- IKE Policies:

crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.3
crypto isakmp key cisco123 address 150.150.150.1
!

!--- IPSec Policies:

crypto ipsec transform-set 160cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
!
crypto map ETH0 16 ipsec-isakmp
set peer 150.150.150.1
set transform-set 160cisco

!--- Include the 170.170.170.x to 160.160.160.x network

```

```

!--- in the encryption process.

match address 160
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco

!--- Include the 170.170.170.x to 180.180.180.x network
!--- in the encryption process.

match address 180
!
interface Ethernet0
ip address 150.150.150.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
no fair-queue
!
interface Serial1
ip address 170.170.170.1 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
ip route 180.180.180.0 255.255.255.0 150.150.150.3
no ip http server
!

!--- Include the 170.170.170.x to 160.160.160.x network
!--- in the encryption process.

access-list 160 permit ip 170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255

!--- Include the 170.170.170.x to 180.180.180.x network
!--- in the encryption process.

access-list 180 permit ip 170.170.170.0 0.0.0.255 180.180.180.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end

```

### Thidwick Configuration

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime

```

```
no service password-encryption
!
hostname thidwick
!
enable secret 5 $1$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!

!--- IKE Policies:

crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.1
crypto isakmp key cisco123 address 150.150.150.2
!

!--- IPsec Policies:

crypto ipsec transform-set 160cisco esp-des esp-md5-hmac
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
!
crypto map ETH0 16 ipsec-isakmp
set peer 150.150.150.1
set transform-set 160cisco

!--- Include the 180.180.180.x to 160.160.160.x network
!--- in the encryption process.

match address 160
crypto map ETH0 17 ipsec-isakmp
set peer 150.150.150.2
set transform-set 170cisco

!--- Include the 180.180.180.x to 170.170.170.x network
!--- in the encryption process.

match address 170
!
interface Ethernet0
ip address 150.150.150.3 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
no fair-queue
clockrate 4000000
!
interface Serial1
ip address 180.180.180.1 255.255.255.0
no ip directed-broadcast
clockrate 4000000
!
interface BRI0
no ip address
```

```

no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
ip route 170.170.170.0 255.255.255.0 150.150.150.2
no ip http server
!

!--- Include the 180.180.180.x to 160.160.160.x network
!--- in the encryption process.

access-list 160 permit ip 180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255

!--- Include the 180.180.180.x to 170.170.170.x network
!--- in the encryption process.

access-list 170 permit ip 180.180.180.0 0.0.0.255 170.170.170.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
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 settings used by current [IPSec] security associations.
- **show crypto isakmp sa** Shows all current IKE security associations at a peer.

## Troubleshoot

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

### Troubleshooting Commands

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

- **debug crypto ipsec** Displays the IPSec negotiations of phase 2.
  - **debug crypto isakmp** Displays the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.
  - **debug crypto engine** Displays the traffic that is encrypted.
  - **clear crypto isakmp** Clears the security associations related to phase 1.
  - **clear crypto sa** Clears the security associations related to phase 2.
-

## Related Information

- [IPSec Support Page](#)
  - [Configuring IPSec Network Security](#)
  - [Configuring Internet Key Exchange Security Protocol](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Feb 17, 2005

Document ID: 14134

---