Configuring IPSec Router−to−Router Hub and Spoke

Document ID: 14133

Contents

Introduction

This document shows hub and spoke encryption from one router (the "hub") to three other routers (the "spokes"). There is one crypto map on the hub router that specifies the networks behind each of its three peers. The crypto maps on each of the spoke routers specify the network behind the hub router.

Encryption is done between these networks:

- 160.160.160.x network to 170.170.170.x network
- 160.160.160.x network to 180.180.180.x network
- 160.160.160.x network to 190.190.190.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 12.0.7.T or later
- Cisco 2500 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 Cisco Technical Tips Conventions.

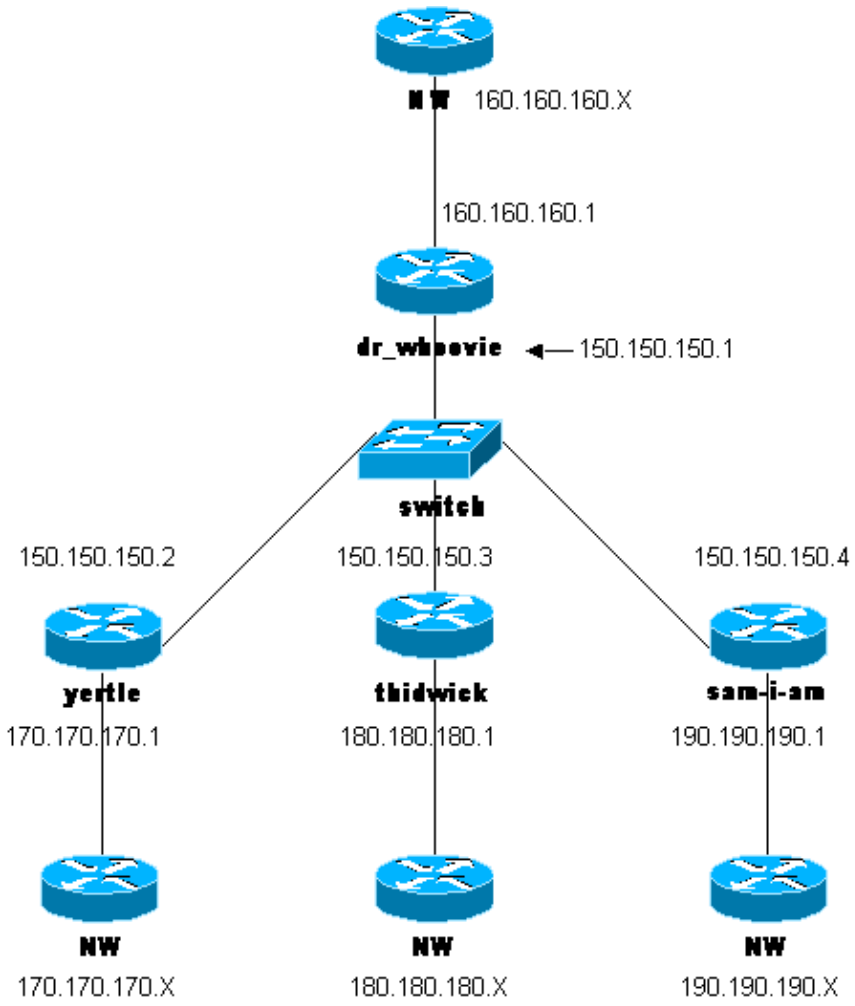
Configure

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 this network setup:



Configurations

This document uses these configurations:

- dr_whoovie Configuration
- sam−I−am Configuration
- thidwick Configuration
- yertle Configuration

dr_whoovie Configuration

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPN.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server

!--- Configure the Internet Key Exchange (IKE)
!--- policy and preshared key for each peer:
!--- IKE policy defined for peers.

crypto isakmp policy 1
authentication pre-share

!--- Preshared keys for different peers.

crypto isakmp key cisco170 address 150.150.150.2
crypto isakmp key cisco180 address 150.150.150.3
crypto isakmp key cisco190 address 150.150.150.4

!--- Configure the IPSec parameters:
!--- IPSec transform sets.

crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
crypto ipsec transform-set 190cisco esp-des esp-md5-hmac
!
crypto map ETH0 17 ipsec-isakmp

!--- Set the peer.

set peer 150.150.150.2

!--- The IPSec transform set is used for this tunnel.

set transform-set 170cisco

!--- Interesting traffic for peer 150.150.150.2.

match address 170
crypto map ETH0 18 ipsec-isakmp

!--- Set the peer.

set peer 150.150.150.3

!--- The IPSec transform set is used for this tunnel.

set transform-set 180cisco

!--- Interesting traffic for peer 150.150.150.3.

match address 180
crypto map ETH0 19 ipsec-isakmp
```

```
!--- Set the peer.

set peer 150.150.150.4

!--- The IPSec transform set is used for this tunnel.

set transform-set 190cisco

!--- Interesting traffic for peer 150.150.150.4.

match address 190
!
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

!--- Apply crypto map on the interface.

crypto map ETH0
!
interface Serial0
ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
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
ip route 190.190.190.0 255.255.255.0 150.150.150.4
no ip http server
!

!--- Access list that shows traffic to encryption from yertle.

access-list 170 permit ip 160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255

!--- Access list that shows traffic to encryption from thidwick.

access-list 180 permit ip 160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255

!--- Access list that shows traffic to encryption from sam-i-am.

access-list 190 permit ip 160.160.160.0 0.0.0.255 190.190.190.0 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
```

sam-I-am Configuration

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Sam-I-am
!
enable secret 5 $1$HDyw$qubSJdqfIC0f1VLvHmg/P0
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server

!--- Configure the IKE policy and preshared key for the hub:

crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco190 address 150.150.150.1

!--- Configure the IPSec parameters:
!--- IPSec transform set.

crypto ipsec transform-set 190cisco esp-des esp-md5-hmac

!--- Crypto map definition for the hub site.

crypto map ETH0 19 ipsec-isakmp

!--- Set the peer.

set peer 150.150.150.1

!--- IPSec transform set.

set transform-set 190cisco

!--- Interesting traffic for peer 150.150.150.1 (hub site).

match address 190
!
interface Ethernet0
ip address 150.150.150.4 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled

!--- Apply crypto map on the interface.

crypto map ETH0
!
interface Serial0
ip address 190.190.190.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
no ip http server

!--- Access list that shows traffic to encryption
!--- for the hub site (dr_whoovie).

access-list 190 permit ip 190.190.190.0 0.0.0.255 160.160.160.0 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 12.0
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

!--- Configure the IKE policy and preshared key for the hub:

crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco180 address 150.150.150.1

!--- Configure the IPSec parameters:
!--- IPSec transform set.

crypto ipsec transform-set 180cisco esp-des esp-md5-hmac

!--- Crypto map definition for the hub site.

crypto map ETH0 18 ipsec-isakmp

!--- Set the peer.

set peer 150.150.150.1

!--- IPSec transform set.

set transform-set 180cisco

!--- Interesting traffic for peer 150.150.150.1 (hub site).

match address 180
!
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
```

```
!--- Apply crypto map on the interface.

crypto map ETH0
!
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
no ip http server

!--- Access list that shows traffic to encryption
!--- for the hub site (dr_whoovie).

access-list 180 permit ip 180.180.180.0 0.0.0.255 160.160.160.0 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 12.0
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

!--- Configure the IKE policy and preshared key for the hub:

crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco170 address 150.150.150.1

!--- Configure the IPSec parameters:
!--- IPSec transform set.

crypto ipsec transform-set 170cisco esp-des esp-md5-hmac

!--- Crypto map definition for the hub site.
```

```
crypto map ETH0 17 ipsec-isakmp

!--- Set the peer.

set peer 150.150.150.1

!--- IPSec transform set.

set transform-set 170cisco

!--- Interesting traffic for peer 150.150.150.1 (hub site).

match address 170
!
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

!--- Apply crypto map on the interface.

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
no ip http server

!--- Access list that shows traffic to encryption for
!--- the hub site (dr_whoovie).

access-list 170 permit ip 170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
tftp-server flash:/c2500-jos56i-l.120-7.T
tftp-server flash:c2500-jos56i-l.120-7.T
tftp-server flash:
!
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 phase 2 security associations.
- **show crypto isakmp sa** Shows the phase 1 security associations.

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 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

- **Configure IPSec Network Security**
- **Configure Internet Key Exchange Security Protocol**
- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 14, 2008 Document ID: 14133