Configuring IPSec Between Three Routers Using Private Addresses

Document ID: 14124

Contents

Introduction

This document describes a fully meshed configuration with three routers that use private addresses. The example illustrates these features:

- Encapsulating Security Payload (ESP) − Data Encryption Standard (DES) only
- Pre−shared keys
- Private networks behind each router: 192.168.1.0, 192.168.2.0, and 192.168.3.0
- isakmp policy and crypto map configuration
- Tunnel traffic defined with the **access−list** and **route−map** commands. In addition to Port Address Translation (PAT), route maps can be applied to a one−to−one static Network Address Translation (NAT) on Cisco IOS® Software Release 12.2(4)T2 and later. For more information refer to NAT − Ability to Use Route Maps with Static Translations Feature Overview.

Note: Encryption technology is subject to export controls. It is your responsibility to know the law regarding export of encryption technology. If you have any questions regarding export control, please send an email to export@cisco.com.

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 12.3.(7)T.
- Cisco routers configured with IPSec.

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.

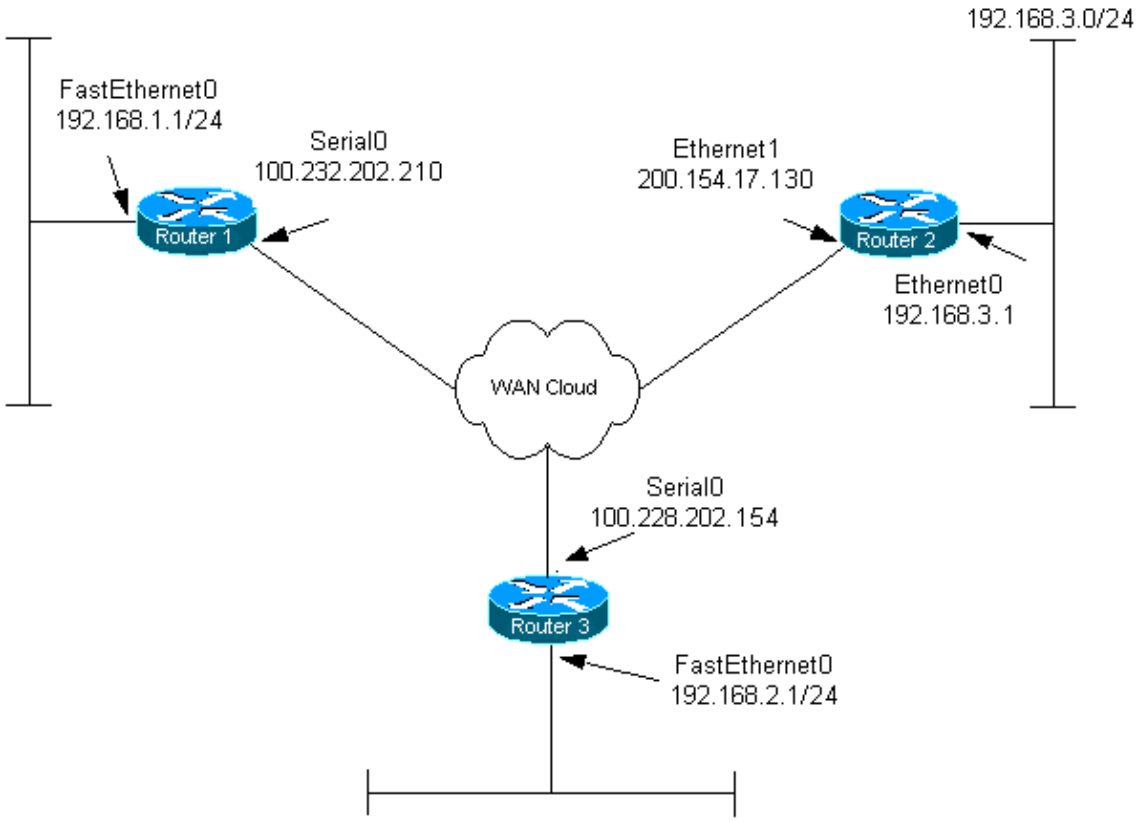
Configure

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:

- Router 1
- Router 2
- Router 3

Router 1

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router1
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!


!--- Configure Internet Key Exchange (IKE) policy and
!--- pre-shared keys for each peer.



!--- IKE policy defined for peers.


crypto isakmp policy 4
authentication pre-share


!--- Pre-shared keys for different peers.


crypto isakmp key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!


!--- IPSec policies:


crypto ipsec transform-set encrypt-des esp-des
!
!
crypto map combined local-address Serial0


!--- Set the peer, transform-set and encryption traffic for tunnel peers.


crypto map combined 20 ipsec-isakmp
   set peer 100.228.202.154
   set transform-set encrypt-des
   match address 106
crypto map combined 30 ipsec-isakmp
   set peer 200.154.17.130
   set transform-set encrypt-des
   match address 105
!
!
```

```
interface Serial0
   ip address 100.232.202.210 255.255.255.252
   ip nat outside
   serial restart-delay 0


!--- Apply the crypto map to the interface.


   crypto map combined
!
interface FastEthernet0
   ip address 192.168.1.1 255.255.255.0
   ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.232.202.209
no ip http server
no ip http secure-server
!


!--- Define traffic for NAT.


ip nat inside source route-map nonat interface Serial0 overload


!--- Access control list (ACL) that shows traffic to encrypt over the tunnel.


access-list 105 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255


!--- ACL to avoid the traffic through NAT over the tunnel.


access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 150 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255


!--- ACL to perform NAT on the traffic that does not go over the tunnel.


access-list 150 permit ip 192.168.1.0 0.0.0.255 any


!--- Do not perform NAT on the IPSec traffic.


route-map nonat permit 10
  match ip address 150
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Router 2

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!


!--- Configure IKE policy and pre-shared keys for each peer.




!--- IKE policy defined for peers.


crypto isakmp policy 4
    authentication pre-share


!--- Pre-shared keys for different peers.


crypto isakmp key xxxxxx1234 address  100.228.202.154
crypto isakmp key xxxxxx1234 address  100.232.202.210
!
!


!--- IPSec policies.


crypto ipsec transform-set encrypt-des esp-des
!
!
crypto map combined local-address Ethernet1


!--- Set the peer, transform-set and encryption traffic for tunnel peers.


crypto map combined 7 ipsec-isakmp
      set peer 100.232.202.210
      set transform-set encrypt-des
      match address 105

crypto map combined 8 ipsec-isakmp
      set peer 100.228.202.154
      set transform-set encrypt-des
      match address 106
!
```

```
!
!
interface Ethernet0
      ip address 192.168.3.1 255.255.255.0
      ip nat inside
!
interface Ethernet1
      ip address 200.154.17.130 255.255.255.224
      ip nat outside


!--- Apply the crypto map to the interface.


      crypto map combined
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.154.17.129
no ip http server
no ip http secure-server
!


!--- Define traffic for NAT.


ip nat inside source route-map nonat interface Ethernet1 overload


!--- ACL shows traffic to encrypt over the tunnel.


access-list 105 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 106 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255


!--- ACL to avoid the traffic through NAT over the tunnel.


access-list 150 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 150 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255


!--- ACL to perform NAT on the traffic that does not go over the tunnel.


access-list 150 permit ip any any


!--- Do not perform NAT on the IPSec traffic.


route-map nonat permit 10
  match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
```

Router 3 Configuration

```
Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!


!--- Configure IKE policy and pre-shared keys for each peer.



!--- IKE policy defined for peers.


crypto isakmp policy 4
  authentication pre-share



!--- Pre-shared keys for different peers.


crypto isakmp key xxxxxx1234 address 100.232.202.210
crypto isakmp key xxxxxx1234 address 200.154.17.130
!
!


!--- IPSec policies:


crypto ipsec transform-set encrypt-des esp-des
!
!


!--- Set the peer, transform-set and encryption traffic for tunnel peers.


crypto map combined local-address Serial0
crypto map combined 7 ipsec-isakmp
  set peer 100.232.202.210
  set transform-set encrypt-des
  match address 106
crypto map combined 8 ipsec-isakmp
  set peer 200.154.17.130
  set transform-set encrypt-des
  match address 105
```

```
!
!
interface Serial0
  ip address 100.228.202.154 255.255.255.252
  ip nat outside
  serial restart-delay 0


!--- Apply the crypto map to the interface.


  crypto map combined
!
  interface FastEthernet0
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153
no ip http server
no ip http secure-server
!


!--- Define traffic for NAT.


ip nat inside source route-map nonat interface Serial0 overload


!--- ACL that shows traffic to encrypt over the tunnel.


access-list 105 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 106 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255


!--- ACL to avoid the traffic through NAT over the tunnel.


access-list 150 deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 150 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255


!--- ACL to perform NAT on the traffic that does not go over the tunnel.


access-list 150 permit ip 192.168.2.0 0.0.0.255 any


!--- Do not perform NAT on the IPSec traffic.


route-map nonat permit 10
  match ip address 150
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
 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 engine connections active** Shows encrypted and decrypted packets between IPSec peers.
- **show crypto isakmp sa** Shows all current IKE security associations (SAs) at a peer.
- **show crypto ipsec sa** Shows the settings used by current (IPSec) SAs.

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, please see Important Information on Debug Commands.

Note: The following debugs must be running on both IPSec routers (peers). Clearing SAs must be done on both peers.

- **debug crypto isakmp** Displays errors during Phase 1.
- **debug crypto ipsec** Displays errors during Phase 2.
- **debug crypto engine** Displays information from the crypto engine.
- **clear crypto connection** *connection−id [slot | rsm | vip]* Terminates an encrypted session currently in progress. Encrypted sessions normally terminate when the session times out. Use the **show crypto cisco connections** command to learn the connection−id value.
- **clear crypto isakmp** Clears the Phase 1 SAs.
- **clear crypto sa** Clears the Phase 2 SAs.

Related Information

- **IPSec Support Page**
- **Technical Support − Cisco Systems**

Updated: Jan 14, 2008 Document ID: 14124