

Configuring IPSec Router-to-Router, Pre-Shared, NAT Overload Between Private Networks

Document ID: 7276

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This sample configuration shows how to encrypt traffic between two private networks (10.50.50.x and 10.103.1.x) using IPSec. The networks know each other by their private addresses.

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 12.3.1a
- Cisco 2691 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

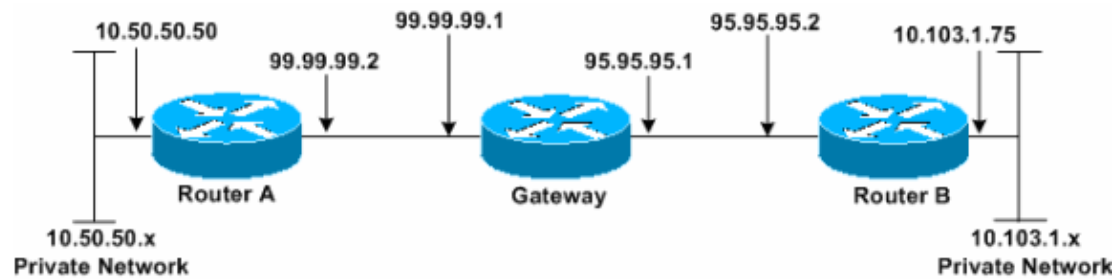
In this section, you are presented with the information to configure the features described in this document.

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 the network setup shown in this diagram.



Configurations

This document uses these configurations.

- Router A
- Router B

```
Router A
Router_A#write terminal
Building configuration...
Current configuration : 1638 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_A
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 95.95.95.2
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 95.95.95.2
set transform-set rtpset

!--- Include the private network to private network traffic
!--- in the encryption process.

match address 115
!
no voice hpi capture buffer
no voice hpi capture destination
```

```

!
interface FastEthernet0/0
ip address 99.99.99.2 255.255.255.0
ip nat outside
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
ip address 10.50.50.50 255.255.255.0
ip nat inside
duplex auto
speed auto
!

!--- Except the private network traffic from the
!--- Network Address Translation (NAT) process.

ip nat inside source route-map nonat interface FastEthernet0/0 overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.1
!

!--- Except the private network traffic from the NAT process.

access-list 110 deny ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
access-list 110 permit ip 10.50.50.0 0.0.0.255 any

!--- Include the private network to private network traffic
!--- in the encryption process.

access-list 115 permit ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
!

!--- Except the private network traffic from the NAT process.

route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
Router_A#

```

Router B

```

Router_B#write terminal
Building configuration...
Current configuration : 1394 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_B

```

```
!  
boot system flash:c2691-ik9o3s-mz.123-1a.bin  
!  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
no ftp-server write-enable  
!  
crypto isakmp policy 1  
hash md5  
authentication pre-share  
crypto isakmp key cisco123 address 99.99.99.2  
!  
crypto ipsec transform-set rtpset esp-des esp-md5-hmac  
!  
crypto map rtp 1 ipsec-isakmp  
set peer 99.99.99.2  
set transform-set rtpset  
  
!--- Include the private network to private network traffic  
!--- in the encryption process.  
  
match address 115  
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
interface FastEthernet0/0  
ip address 95.95.95.2 255.255.255.0  
ip nat outside  
duplex auto  
speed auto  
crypto map rtp  
!  
interface FastEthernet0/1  
ip address 10.103.1.75 255.255.255.0  
ip nat inside  
duplex auto  
speed auto  
!  
!--- Except the private network traffic from the NAT process.  
  
ip nat inside source route-map nonat interface FastEthernet0/0 overload  
ip http server  
no ip http secure-server  
ip classless  
ip route 0.0.0.0 0.0.0.0 95.95.95.1  
!  
!--- Except the private network traffic from the NAT process.  
  
access-list 110 deny ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255  
access-list 110 permit ip 10.103.1.0 0.0.0.255 any  
  
!--- Include the private network to private network traffic  
!--- in the encryption process.  
  
access-list 115 permit ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255  
!  
!--- Except the private network traffic from the NAT process.  
  
route-map nonat permit 10  
match ip address 110
```

```
!  
dial-peer cor custom  
!  
line con 0  
exec-timeout 0 0  
line aux 0  
line vty 0 4  
login  
!  
end  
Router_B#
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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 sa** Displays the IPSec negotiations of phase 2.
- **debug crypto isakmp sa** Displays the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.
- **debug crypto engine** Displays the encrypted sessions.

Related Information

- [IP Security Troubleshooting – Understanding and Using debug Commands](#)
- [IPSec Support Page](#)
- [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: Jan 14, 2008

Document ID: 7276
