

Table of Contents

<u>Configuring IPsec Router-to-Router with NAT Overload and Cisco Secure VPN Client</u>	1
<u>Introduction</u>	1
<u>Prerequisites</u>	1
<u>Requirements</u>	1
<u>Components Used</u>	1
<u>Conventions</u>	1
<u>Configure</u>	2
<u>Network Diagram</u>	2
<u>Configurations</u>	2
<u>Verify</u>	8
<u>Troubleshoot</u>	8
<u>Troubleshooting Commands</u>	8
<u>NetPro Discussion Forums – Featured Conversations</u>	8
<u>Related Information</u>	8

Configuring IPsec Router-to-Router with NAT Overload and Cisco Secure VPN Client

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This sample configuration encrypts traffic from the network behind Light to the network behind House (the 192.168.100.x to 192.168.200.x network). Network Address Translation (NAT) overload is also done. Encrypted VPN Client connections are allowed into Light with wild-card, pre-shared keys and mode-config. Traffic to the Internet is translated, but not encrypted.

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 12.2.7 and 12.2.8T
- Cisco Secure VPN Client 1.1 (shown as 2.1.12 in the IRE client **Help > About** menu)
- Cisco 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 Cisco Technical Tips Conventions.

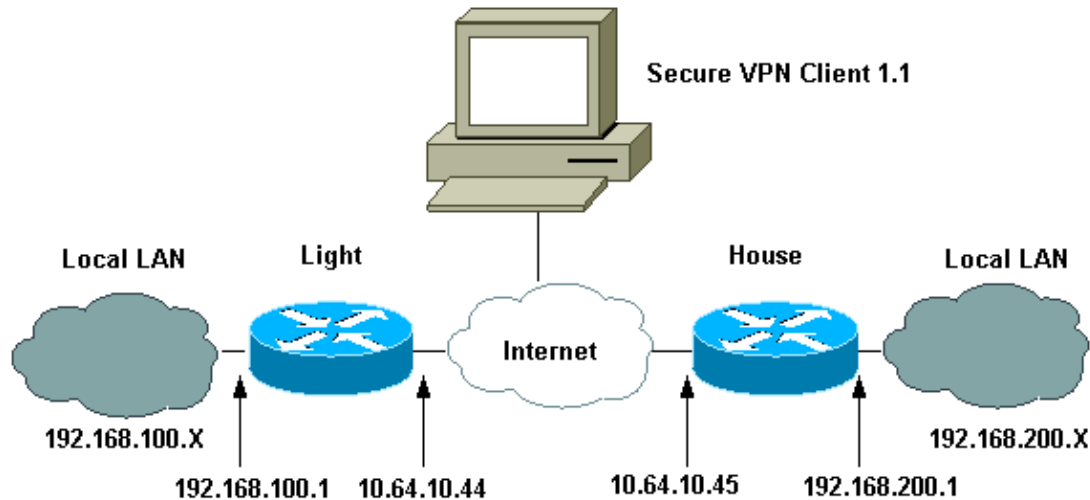
Configure

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

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations.

- Light Configuration
- House Configuration
- VPN Client Configuration

```
Light Configuration
Current configuration : 2047 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Light
!
boot system flash:c3660-ik9o3s-mz.122-8T
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
!---- IPsec Internet Security Association and
```

```

!--- Key Management Protocol (ISAKMP) policy.

crypto isakmp policy 5
  hash md5
  authentication pre-share

!--- ISAKMP key for static LAN-to-LAN tunnel
!--- without extended authenticaton (xauth).

crypto isakmp key cisco123 address 10.64.10.45 no-xauth

!--- ISAKMP key for dynamic VPN Client.

crypto isakmp key 123cisco address 0.0.0.0 0.0.0.0

!--- Assign IP address to the VPN Client.

crypto isakmp client configuration address-pool local test-pool
!
!
!
crypto ipsec transform-set testset esp-des esp-md5-hmac
!
crypto dynamic-map test-dynamic 10
  set transform-set testset
!
!

!--- VPN Client mode configuration negotiation,
!--- such as IP address assignment and xauth.

crypto map test client configuration address initiate
crypto map test client configuration address respond

!--- Static crypto map for the LAN-to-LAN tunnel.

crypto map test 5 ipsec-isakmp
  set peer 10.64.10.45
  set transform-set testset

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

  match address 115

!--- Dynamic crypto map for the VPN Client.

crypto map test 10 ipsec-isakmp dynamic test-dynamic
!

call rsvp-sync
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
controller E1 2/0
!
!
!

```

```

interface FastEthernet0/0
 ip address 10.64.10.44 255.255.255.224
 ip nat outside
 duplex auto
 speed auto
 crypto map test
!
interface FastEthernet0/1
 ip address 192.168.100.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface BRI4/0
 no ip address
 shutdown
!
interface BRI4/1
 no ip address
 shutdown
!
interface BRI4/2
 no ip address
 shutdown
!
interface BRI4/3
 no ip address
 shutdown
!

!--- Define IP address pool for the VPN Client.

ip local pool test-pool 192.168.1.1 192.168.1.254

!--- Exclude the private network and VPN Client
!--- traffic from the NAT process.

ip nat inside source route-map nonat interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
ip http server
ip pim bidir-enable
!

!--- Exclude the private network and VPN Client
!--- traffic from the NAT process.

access-list 110 deny ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

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

access-list 115 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
!

!--- Exclude the private network and VPN Client
!--- traffic from the NAT process.

route-map nonat permit 10
 match ip address 110
!
!

```

```
dial-peer cor custom
!
!
!
!
!
line con 0
line 97 108
line aux 0
line vty 0 4
!
end
```

House Configuration

Current configuration : 1689 bytes

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
boot system flash:c3660-jk8o3s-mz.122-7.bin
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!

!--- IPsec ISAKMP policy.

crypto isakmp policy 5
  hash md5
  authentication pre-share

!--- ISAKMP key for static LAN-to-LAN tunnel without xauth authenticaton.

crypto isakmp key cisco123 address 10.64.10.44 no-xauth
!
!
crypto ipsec transform-set testset esp-des esp-md5-hmac
!

!--- Static crypto map for the LAN-to-LAN tunnel.

crypto map test 5 ipsec-isakmp
  set peer 10.64.10.44
  set transform-set testset

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

  match address 115
!
call rsvp-sync
```

```

cns event-service server
!
!
!
!
!
fax interface-type modem
mta receive maximum-recipients 0
!
!
!
interface FastEthernet0/0
 ip address 10.64.10.45 255.255.255.224
 ip nat outside
 duplex auto
 speed auto
 crypto map test
!
interface FastEthernet0/1
 ip address 192.168.200.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface BRI2/0
 no ip address
 shutdown
!
interface BRI2/1
 no ip address
 shutdown
!
interface BRI2/2
 no ip address
 shutdown
!
interface BRI2/3
 no ip address
 shutdown
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex auto
 speed auto
!

!--- Exclude the private network traffic
!--- from the Dynamic (dynamic association to a pool) NAT process.

ip nat inside source route-map nonat interface FastEthernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.64.10.33
no ip http server
ip pim bidir-enable
!

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

access-list 110 deny ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 110 permit ip 192.168.200.0 0.0.0.255 any

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

```

```

access-list 115 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255

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

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

```

VPN Client Configuration

```

Network Security policy:
  1- TOLIGHT
  My Identity
  Connection security: Secure
  Remote Party Identity and addressing
  ID Type: IP subnet
  192.168.100.0
  255.255.255.0
  Port all Protocol all

Connect using secure tunnel
  ID Type: IP address
  10.64.10.44

Pre-shared Key=123cisco

Authentication (Phase 1)
  Proposal 1
  Authentication method: pre-shared key
  Encryp Alg: DES
  Hash Alg: MD5
  SA life: Unspecified
  Key Group: DH 1

Key exchange (Phase 2)
  Proposal 1
  Encapsulation ESP
  Encrypt Alg: DES
  Hash Alg: MD5
  Encap: tunnel
  SA life: Unspecified
  no AH

2- Other Connections

```



```
Connection security: Non-secure
Local Network Interface
Name: Any
IP Addr: Any
Port: All
```

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 (SAs).
- **show crypto isakmp sa** Shows the phase 1 SAs.

Troubleshoot

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

Troubleshooting Commands

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

- **debug crypto ipsec** Shows the IPSec negotiations of phase 2.
- **debug crypto isakmp** Shows the ISAKMP negotiations of phase 1.
- **debug crypto engine** Shows the traffic that is encrypted.
- **clear crypto isakmp** Clears the SAs related to phase 1.
- **clear crypto sa** Clears the SAs related to phase 2.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

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

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.