Configuring IPSec – Cisco Secure VPN Client to Central Router Controlling Access

Document ID: 14141

Contents

Introduction

The following configuration would not be commonly used, but was designed to allow Cisco Secure VPN Client IPSec tunnel termination on a central router. As the tunnel comes up, the PC receives its IP address from the central router's IP address pool (in our example, the router is named "moss"), then the pool traffic can reach the local network behind moss or be routed and encrypted to the network behind the outlying router (in our example, the router is named "carter"). In addition, traffic from private network 10.13.1.X to 10.1.1.X is encrypted; the routers are doing NAT overload.

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 12.1.5.T (c3640–io3s56i–mz.121–5.T)
- Cisco Secure VPN Client 1.1

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.
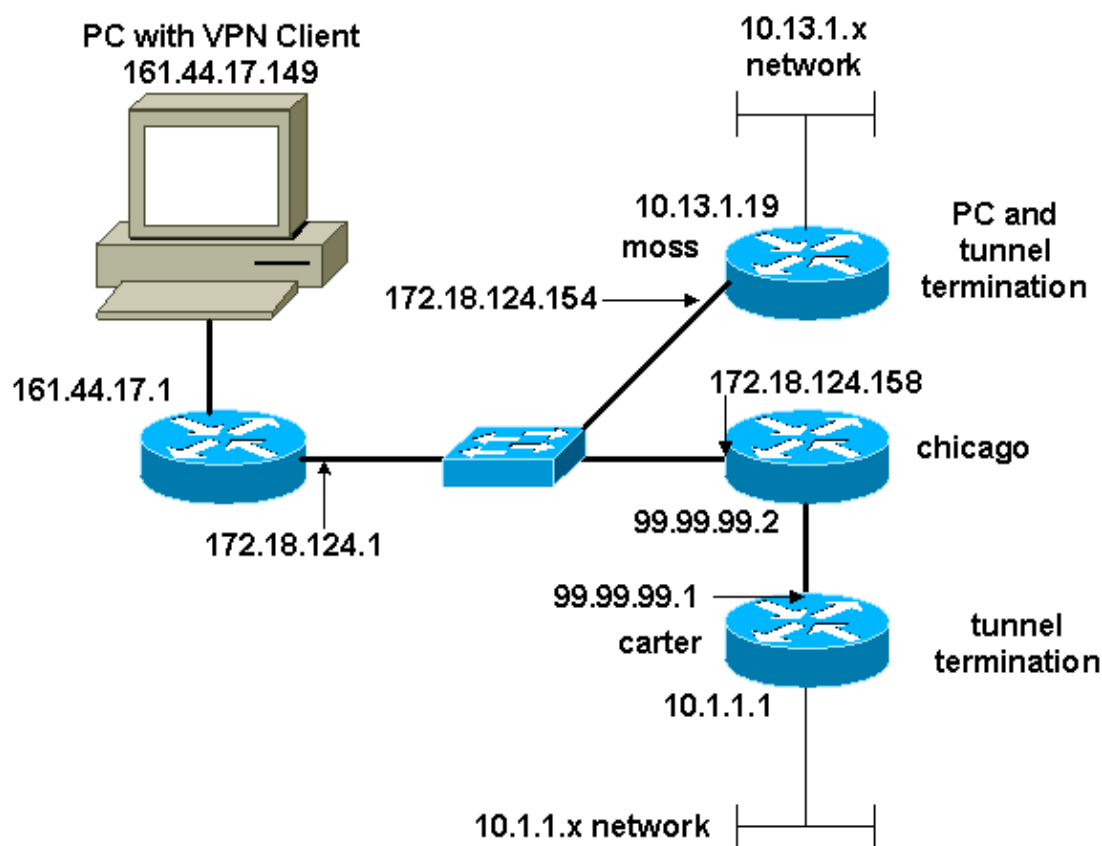
Configure

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:

- moss Configuration
- carter Configuration

moss Configuration

```
Version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
enable password ww
```

```
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.1
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp client configuration address-pool local RTP-POOL
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto dynamic-map rtp-dynamic 20
set transform-set rtpset
!
crypto map rtp client configuration address initiate
crypto map rtp client configuration address respond
!crypto map sequence for network to network traffic
crypto map rtp 1 ipsec-isakmp
set peer 99.99.99.1
set transform-set rtpset
match address 115

!--- crypto map sequence for VPN Client network traffic.

crypto map rtp 10 ipsec-isakmp dynamic rtp-dynamic
!
call rsvp-sync
!
interface Ethernet2/0
ip address 172.18.124.154 255.255.255.0
ip nat outside
no ip route-cache
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Serial2/0
no ip address
shutdown
!
interface Ethernet2/1
ip address 10.13.1.19 255.255.255.0
ip nat inside
half-duplex
!
ip local pool RTP-POOL 192.168.1.1 192.168.1.254
ip nat pool ETH20 172.18.124.154 172.18.124.154 netmask 255.255.255.0
ip nat inside source route-map nonat pool ETH20 overload
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.1
ip route 10.1.1.0 255.255.255.0 172.18.124.158
ip route 99.99.99.0 255.255.255.0 172.18.124.158
no ip http server
!

!--- Exclude traffic from NAT process.

access-list 110 deny ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 110 deny ip 10.13.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 10.13.1.0 0.0.0.255 any
```

```
!--- Include traffic in encryption process.

access-list 115 permit ip 10.13.1.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 115 permit ip 192.168.1.0 0.0.0.255 10.1.1.0 0.0.0.255
route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

carter Configuration

```
Current configuration : 2059 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname carter
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 172.18.124.154
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!

!--- crypto map sequence for network-to-network traffic.

crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.154
set transform-set rtpset
match address 115
!
call rsvp-sync
!
interface Ethernet0/0
ip address 99.99.99.1 255.255.255.0
ip nat outside
half-duplex
crypto map rtp
!
interface FastEthernet3/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
```

```
duplex auto
speed 10
!
ip nat pool ETH00 99.99.99.1 99.99.99.1 netmask 255.255.255.0
ip nat inside source route-map nonat pool ETH00 overload
ip classless
ip route 0.0.0.0 0.0.0.0 99.99.99.2
no ip http server
!

!--- Exclude traffic from NAT process.

access-list 110 deny ip 10.1.1.0 0.0.0.255 10.13.1.0 0.0.0.255
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any

!--- Include traffic in encryption process.

access-list 115 permit ip 10.1.1.0 0.0.0.255 10.13.1.0 0.0.0.255
access-list 115 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
route-map nonat permit 10
match ip address 110
!
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

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** 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 security associations related to phase 1.
- **clear crypto sa** Clears the security associations related to phase 2.

Related Information

- **Configuring IPSec Network Security**
- **Configuring Internet Key Exchange Security Protocol**
- **Cisco VPN Client Support Page**
- **IPSec Support Page**
- **Technical Support – Cisco Systems**

Updated: Jan 14, 2008   Document ID: 14141