Router and VPN Client for Public Internet on a Stick Configuration Example

Document ID: 71461

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure
Network Diagram
Configurations
VPN Client 4.8 Configuration
Verify
Troubleshoot
Troubleshooting Commands
Related Information

Introduction

This document describes how to set up a central site router to perform IPsec traffic on a stick. This setup applies to a specific case where the router, without enabling split tunneling, and Mobile users (Cisco VPN Client) can access the Internet via the central site router. In order to achieve this, configure the policy map in the router to point all the VPN traffic (Cisco VPN Client) to a loopback interface. This allows the Internet traffic to be port address translated (PATed) to the outside world.

Refer to PIX/ASA 7.x and VPN Client for Public Internet VPN on a Stick Configuration Example in order to complete a similar configuration on a central site PIX Firewall.

Note: In order to avoid the overlapping of IP addresses in the network, assign the entirely different pool of IP addresses to the VPN Client (for example, 10.x.x.x , 172.16.x.x, 192.168.x.x). This IP addressing scheme helps you to troubleshoot your 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 Router 3640 with Cisco IOS® Software Release 12.4
- Cisco VPN Client 4.8

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

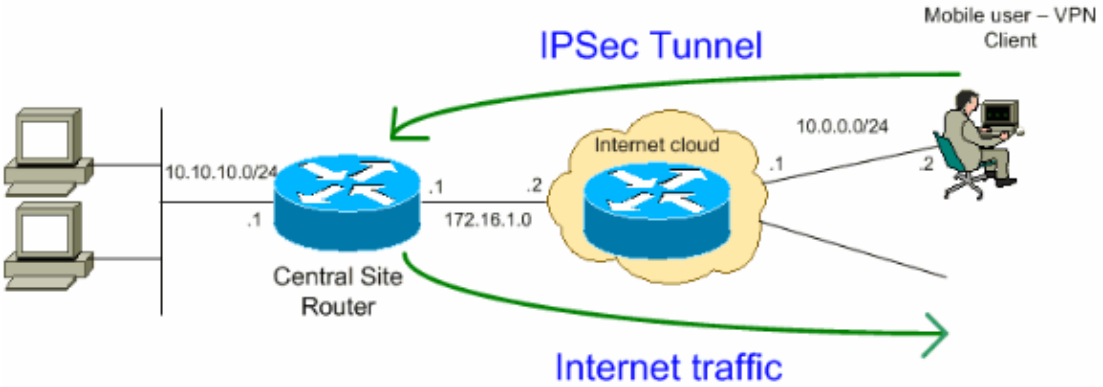
Configure

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

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Configurations

This document uses these configurations:

- Router
- Cisco VPN Client

Router
VPN#**show run** Building configuration... Current configuration : 2170 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname VPN ! boot-start-marker boot-end-marker !

```
!

!--- Enable authentication, authorization and accounting (AAA)
!--- for user authentication and group authorization.


aaa new-model
!

!--- In order to enable Xauth for user authentication,
!--- enable the aaa authentication commands.


aaa authentication login userauthen local


!--- In order to enable group authorization, enable
!--- the aaa authorization commands.

aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!

!--- For local authentication of the IPsec user,
!--- create the user with a password.


username user password 0 cisco
!
!
!

!--- Create an Internet Security Association and
!--- Key Management Protocol (ISAKMP) policy for Phase 1 negotiations.



crypto isakmp policy 3
 encr 3des
 authentication pre-share
 group 2


!--- Create a group that is used to specify the
!--- WINS and DNS server addresses to the VPN Client,
!--- along with the pre-shared key for authentication.


crypto isakmp client configuration group vpnclient
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
!

!--- Create the Phase 2 Policy for actual data encryption.



crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
```

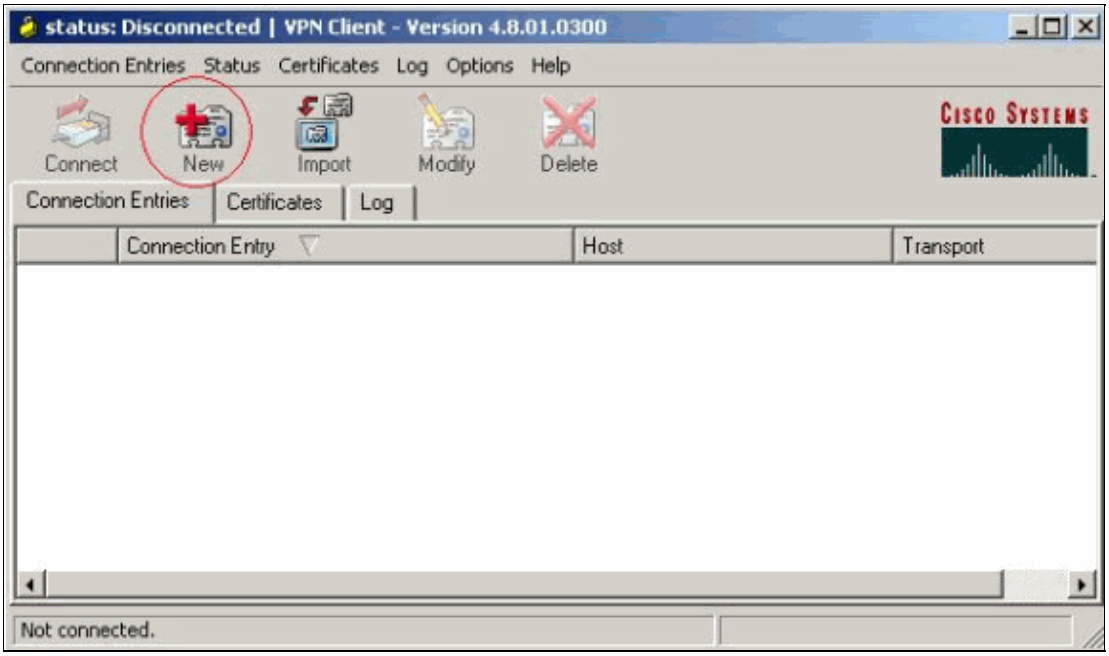
```
!--- Create a dynamic map and apply
!--- the transform set that was created earlier.


crypto dynamic-map dynmap 10
 set transform-set myset
 reverse-route
!


!--- Create the actual crypto map,
!--- and apply the AAA lists that were created earlier.


crypto map clientmap client authentication list userauthen
crypto map clientmap isakmp authorization list groupauthor
crypto map clientmap client configuration address respond
crypto map clientmap 10 ipsec-isakmp dynamic dynmap
!
!
!
!

!--- Create the loopback interface for the VPN user traffic
.
interface Loopback0
 ip address 10.11.0.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 half-duplex
 ip nat inside


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


interface FastEthernet1/0
 ip address 172.16.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip policy route-map VPN-Client
 duplex auto
 speed auto
 crypto map clientmap
!
interface Serial2/0
 no ip address
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown

!--- Create a pool of addresses to be
```

```
!--- assigned to the VPN Clients.


!
ip local pool ippool 192.168.1.1 192.168.1.2
ip http server
no ip http secure-server
!
ip route 10.0.0.0 255.255.255.0 172.16.1.2

!--- Enables Network Address Translation (NAT)
!--- of the inside source address that matches access list 101
!--- and gets PATed with the FastEthernet IP address.


ip nat inside source list 101 interface FastEthernet1/0 overload
!

!--- The access list is used to specify which traffic is to be translated for the
!--- outside Internet.

access-list 101 permit ip any any


!--- Interesting traffic used for policy route.

access-list 144 permit ip 192.168.1.0 0.0.0.255 any


!--- Configures the route map to match the interesting traffic (access list 144)
!--- and routes the traffic to next hop address 10.11.0.2.

!
route-map VPN-Client permit 10
 match ip address 144
 set ip next-hop 10.11.0.2
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
end
```

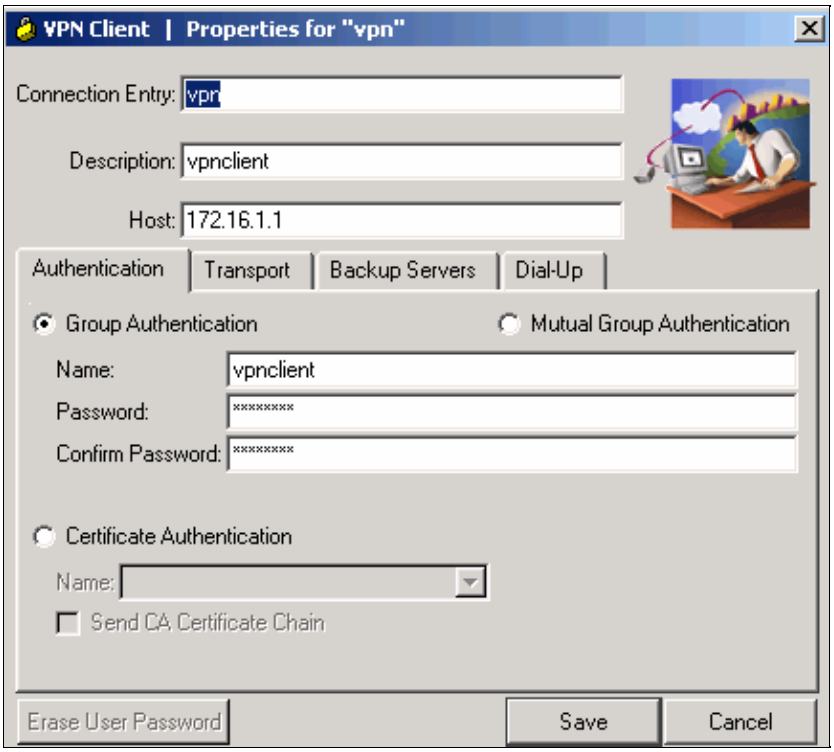
VPN Client 4.8 Configuration

Complete these steps in order to configure the VPN Client 4.8.

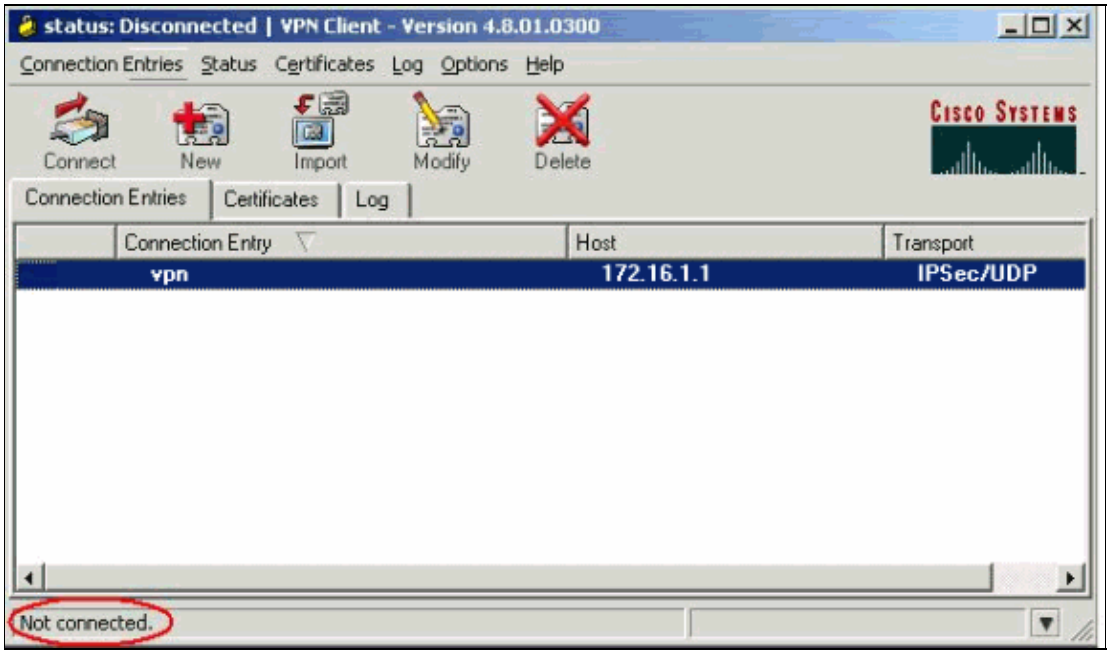
1. Choose **Start > Programs > Cisco Systems VPN Client > VPN Client**.
2. Click **New** in order to launch the Create New VPN Connection Entry window.



3. Enter the name of the Connection Entry along with a description, enter the outside IP address of the router in the Host box, and enter the VPN Group name and password. Click **Save**.

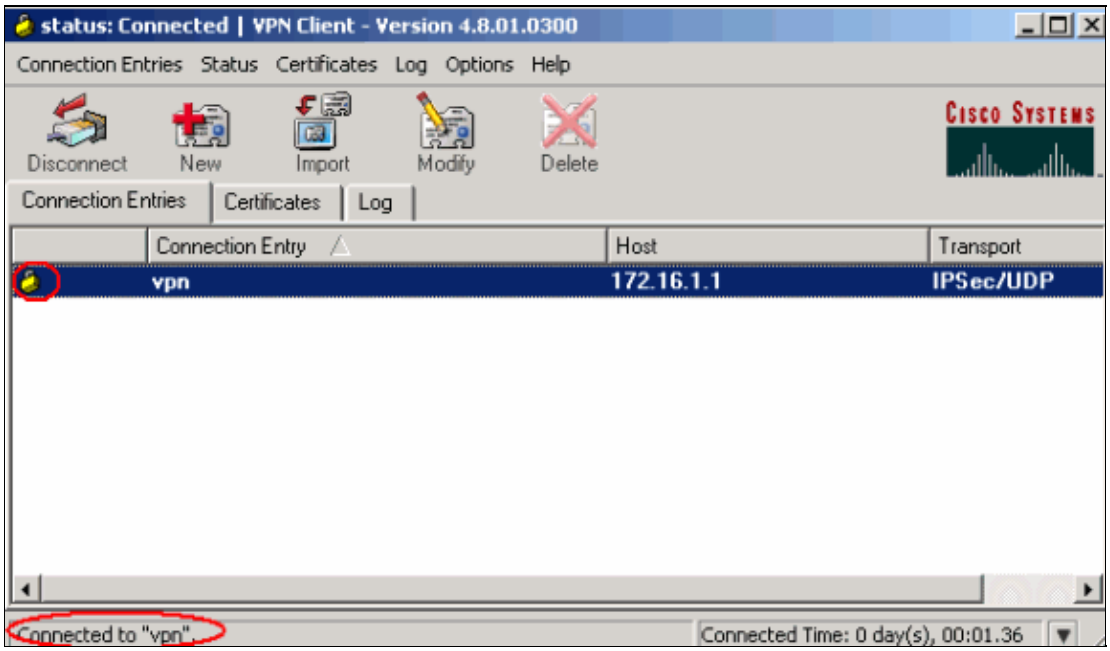


4. Click on the connection you would like to use and click **Connect** from the VPN Client main window.

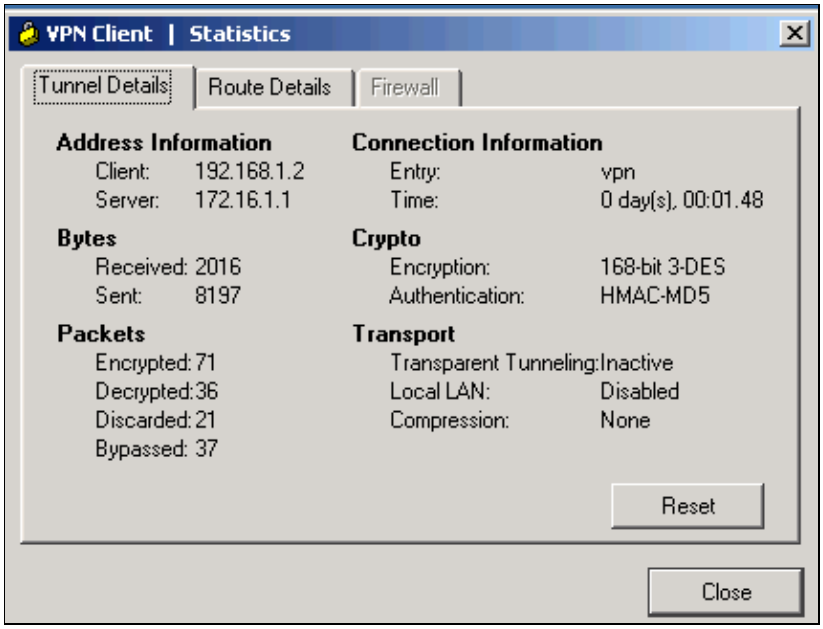


5. When prompted, enter the Username and Password information for Xauth and click **OK** in order to connect to the remote network.

6. The VPN Client gets connected with the router at the central site.



7. Choose **Status** > **Statistics** in order to check the tunnel statistics of the VPN Client.



Verify

This section provides information you can use to confirm your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto isakmp sa** Shows all current IKE Security Associations (SAs) at a peer.

```
VPN#show crypto ipsec sa

interface: FastEthernet1/0
    Crypto map tag: clientmap, local addr 172.16.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0)
   current_peer 10.0.0.2 port 500
     PERMIT, flags={}
    #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270
    #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0
     current outbound spi: 0xEF7C20EA(4017889514)

     inbound esp sas:
      spi: 0x17E0CBEC(400608236)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: clientmap
        sa timing: remaining key lifetime (k/sec): (4530341/3288)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:
```

```
inbound pcp sas:

outbound esp sas:
 spi: 0xEF7C20EA(4017889514)
   transform: esp-3des esp-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2002, flow_id: SW:2, crypto map: clientmap
   sa timing: remaining key lifetime (k/sec): (4530354/3287)
   IV size: 8 bytes
   replay detection support: Y
   Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

- **show crypto ipsec sa** Shows the settings used by current SAs.

```
VPN#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.1      10.0.0.2        QM_IDLE              15    0 ACTIVE
```

Troubleshoot

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of Phase 1.

Related Information

- **IPsec Negotiation/IKE Protocols**
- **Cisco VPN Client − Product support**
- **Cisco Router − Product Support**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2013 − 2014 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Jun 24, 2008 Document ID: 71461