

Split Tunneling for VPN Clients on the VPN 3000 Concentrator Configuration Example

Document ID: 70799

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Background Information

Configure Split Tunneling on the VPN Concentrator

Verify

- Connect with the VPN Client
- View the VPN Client Log

Troubleshoot

Related Information

Introduction

This document provides step-by-step instructions on how to allow VPN Clients access to the Internet while they are tunneled into a VPN 3000 Series Concentrator. This configuration allows VPN Clients secure access to corporate resources via IPsec while giving unsecured access to the Internet.

Note: Split tunneling can potentially pose a security risk when configured. Because VPN Clients have unsecured access to the Internet, they can be compromised by an attacker. That attacker might then be able to access the corporate LAN via the IPsec tunnel. A compromise between full tunneling and split tunneling can be to allow VPN Clients local LAN access only. Refer to Allow Local LAN Access for VPN Clients on the VPN 3000 Concentrator Configuration Example for more information.

Prerequisites

Requirements

This document assumes that a working remote access VPN configuration already exists on the VPN Concentrator. Refer to IPsec with VPN Client to VPN 3000 Concentrator Configuration Example if one is not already configured.

Components Used

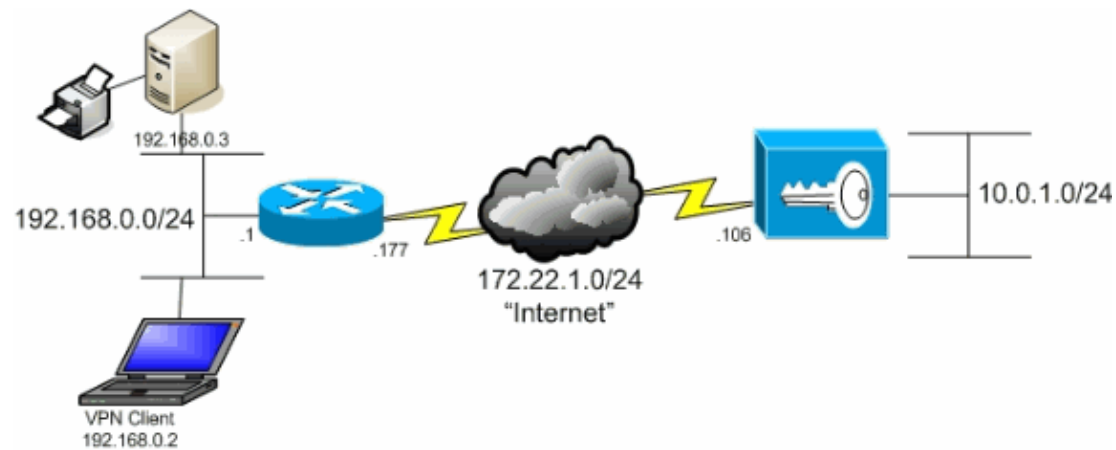
The information in this document is based on these software and hardware versions:

- Cisco VPN 3000 Concentrator Series Software version 4.7.2.H
- Cisco VPN Client version 4.0.5

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.

Network Diagram

The VPN Client is located on a typical SOHO network and connects across the Internet to the main office.



Conventions

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

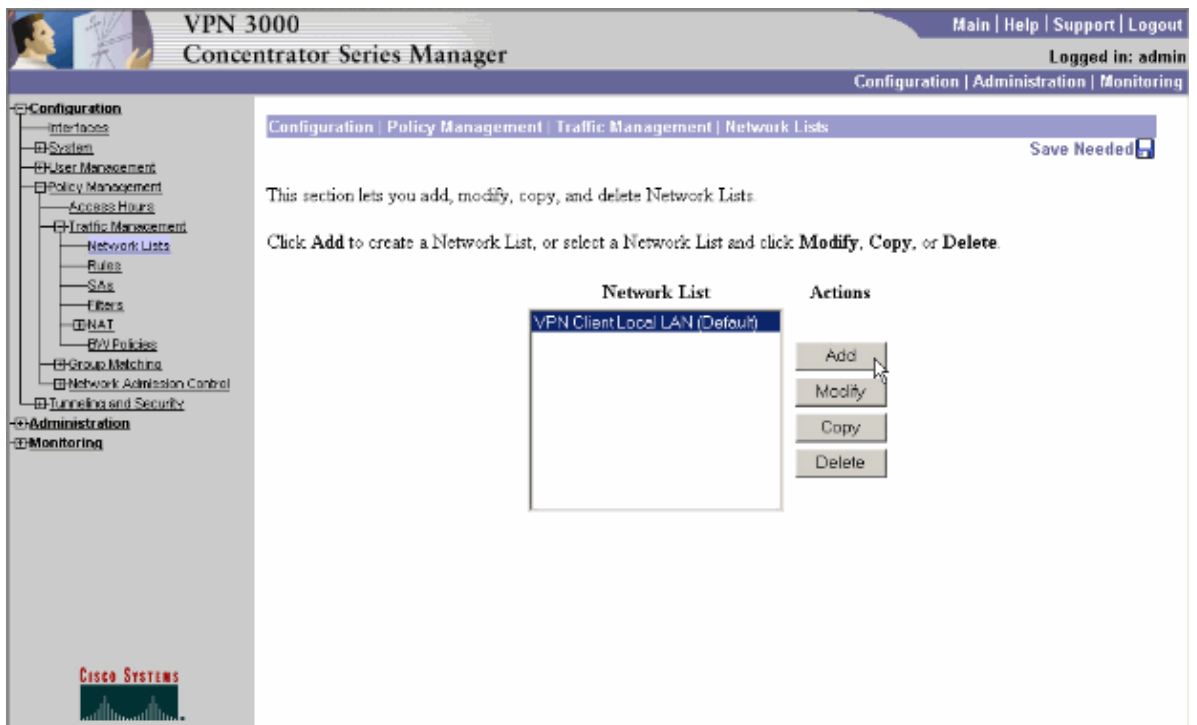
Background Information

In a basic VPN Client to VPN Concentrator scenario, all traffic from the VPN Client is encrypted and sent to the VPN Concentrator no matter what the destination. Based on your configuration and the number of users supported, such a setup can become bandwidth intensive. Split tunneling can work to alleviate this problem by allowing users to send only that traffic which is destined for the corporate network across the tunnel. All other traffic such as IM, email, or casual browsing is sent out to the Internet via the local LAN of the VPN Client.

Configure Split Tunneling on the VPN Concentrator

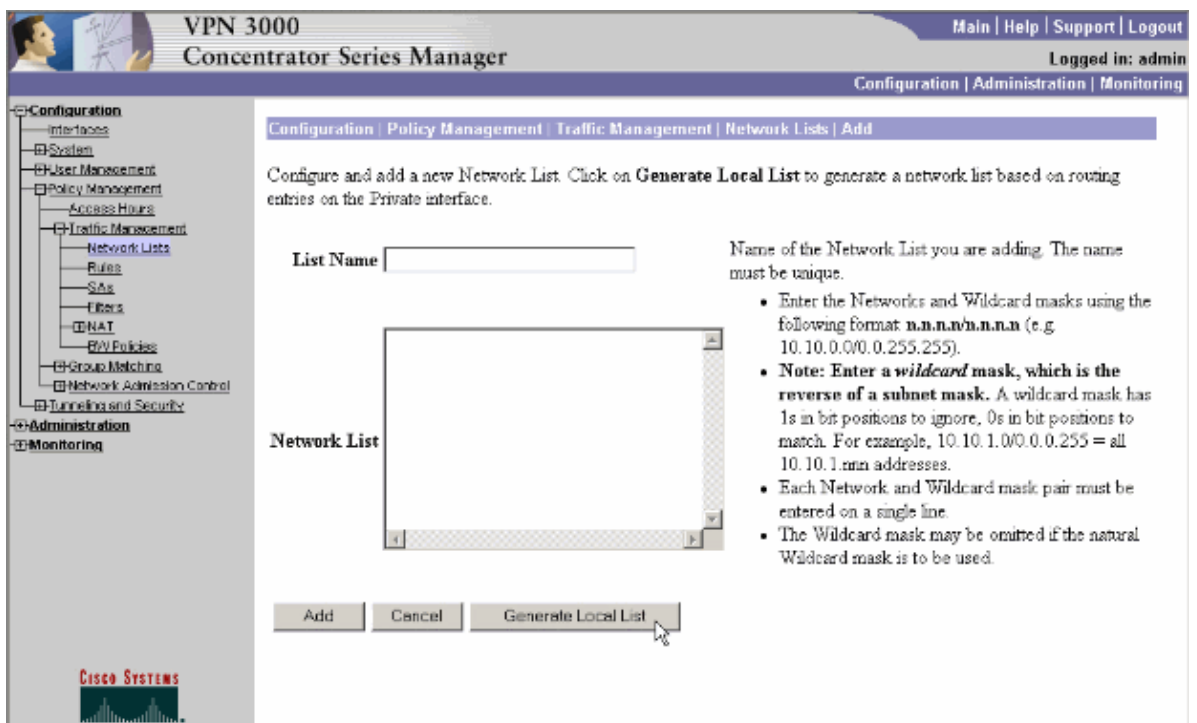
Complete these steps in order to configure your tunnel group to allow split tunneling for users in the group. First create a Network List. This list defines the destination networks to which the VPN Client sends encrypted traffic. Once the list is created, add the list to the split tunneling policy of the client tunnel group.

1. Choose **Configuration > Policy Management > Traffic Management > Network Lists** and click **Add**.



2. This list defines the destination networks to which the VPN Client sends encrypted traffic. Either enter these networks manually, or click **Generate Local List** in order to create a list based on routing entries on the private interface of the VPN Concentrator.

In this example, the list was created automatically.



3. Once it is created or populated, provide a name for the list and click **Add**.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name:

Network List:

Buttons: Add, Cancel, Generate Local List

Name of the Network List you are adding. The name must be unique.

- Enter the Network and Wildcard masks using the following format **n.n.n.n/w.w.w.w** (e.g. 10.10.0.0/0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/w.w.w.w = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

CISCO SYSTEMS

4. Once you create the network list, assign it to a tunnel group. Choose **Configuration > User Management > Groups**, select the group you wish to change, and click **Modify Group**.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups

Save Needed

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	<input type="text" value="ipsecgroup (Internally Configured)"/>	<input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

CISCO SYSTEMS

5. Go to the Client Config tab of the group that you have chosen to modify.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify ipsecgroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identify | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

Client Configuration Parameters

Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPsec backup server addresses/names starting from high priority to low. Enter each IPsec backup server address/name on a single line.

6. Scroll down to the Split Tunneling Policy and Split Tunneling Network List sections and click **Only tunnel networks in the list**.
7. Choose the list created earlier from the drop-down. In this case it is **Main Office**. The Inherit? checkboxes are automatically emptied in both cases.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify ipsecgroup

Split Tunneling Policy	<input type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input checked="" type="radio"/> Only tunnel networks in the list	<input type="checkbox"/>	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Split Tunneling Network List	Main Office	<input type="checkbox"/>	
Default Domain Name		<input checked="" type="checkbox"/>	Enter the default domain name given to users of this group.
Split DNS Names		<input checked="" type="checkbox"/>	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel. The Default Domain Name must be explicitly included in Split DNS Names list if it is to be resolved through the tunnel.

Apply Cancel

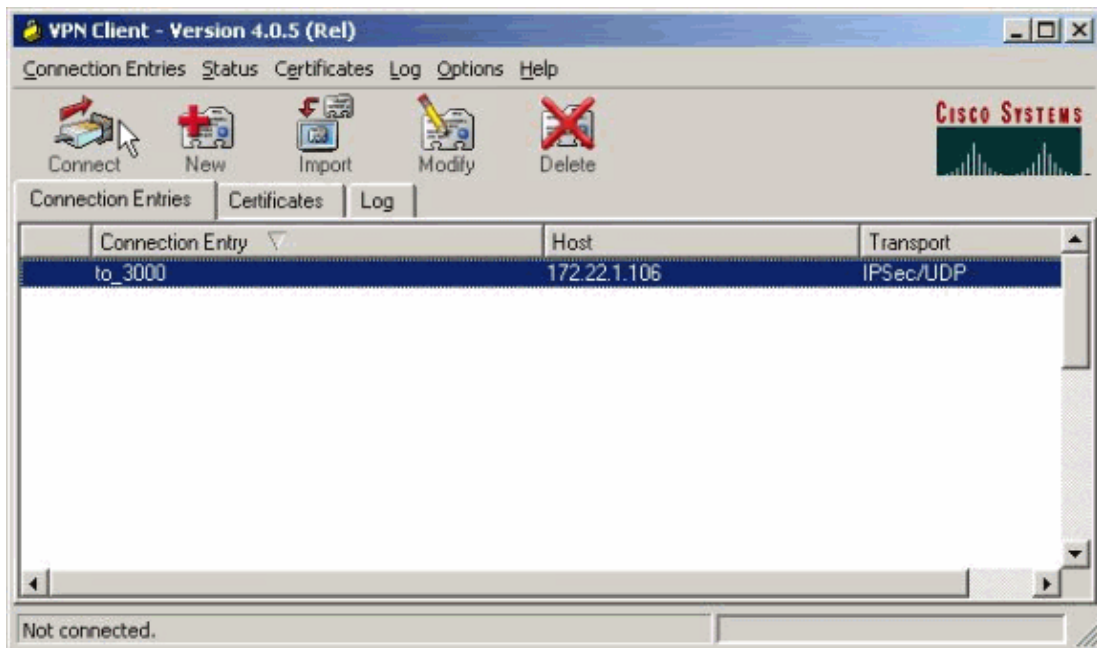
8. Click **Apply** when you are done.

Verify

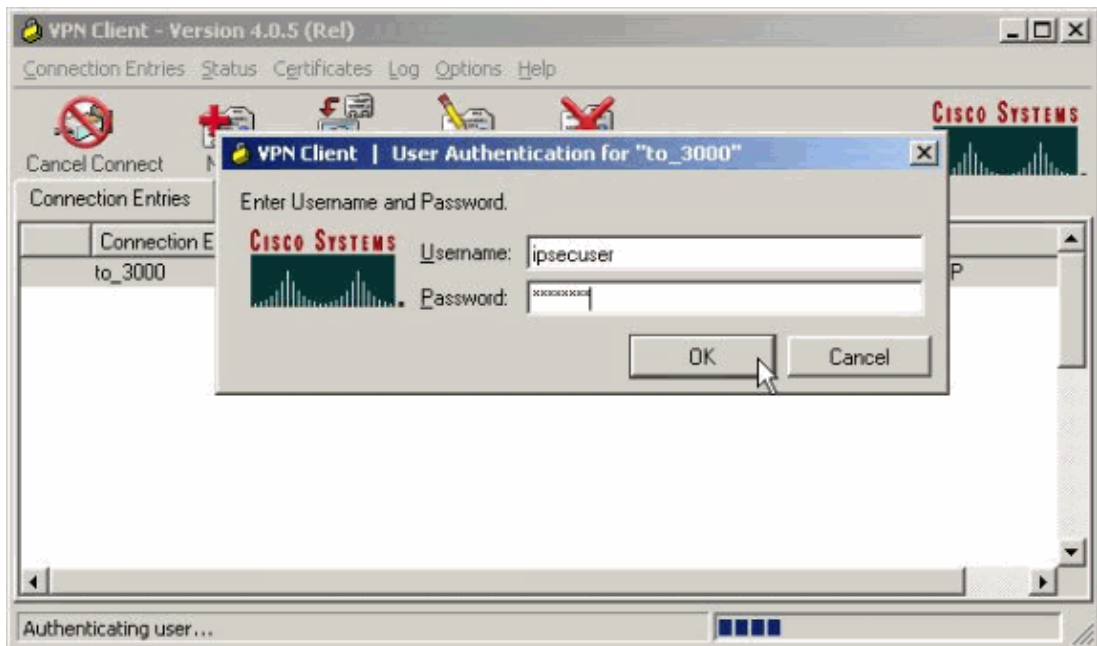
Connect with the VPN Client

Connect your VPN Client to the VPN Concentrator in order to verify your configuration.

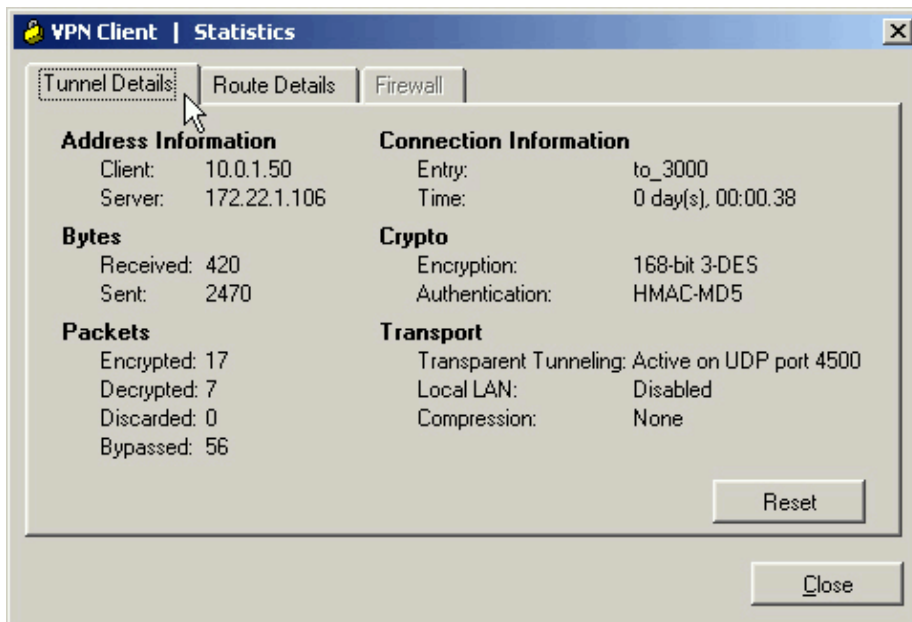
1. Choose your connection entry from the list and click **Connect**.



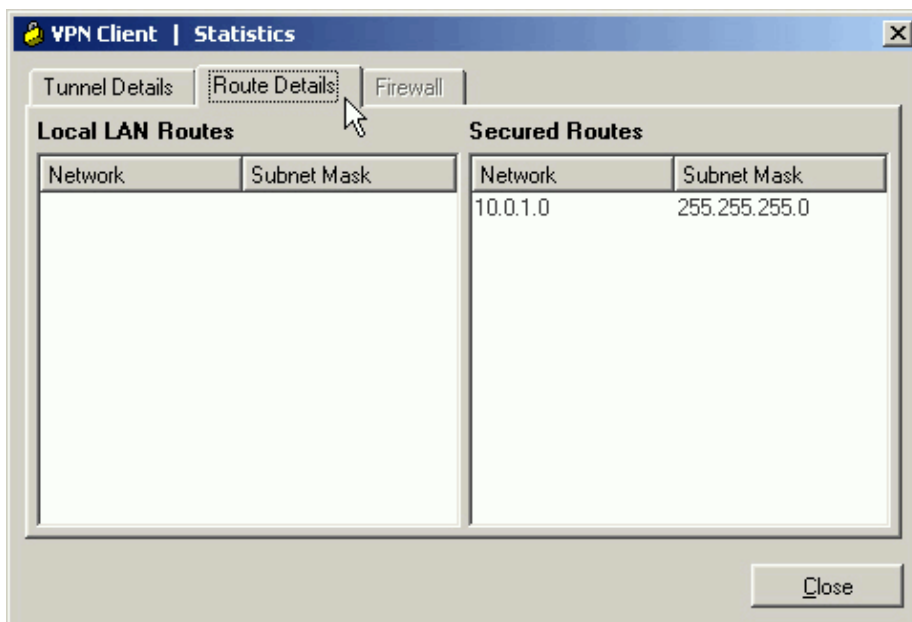
2. Enter your credentials.



3. Choose **Status > Statistics...** in order to display the Tunnel Details window where you can inspect the particulars of the tunnel and see traffic flowing.

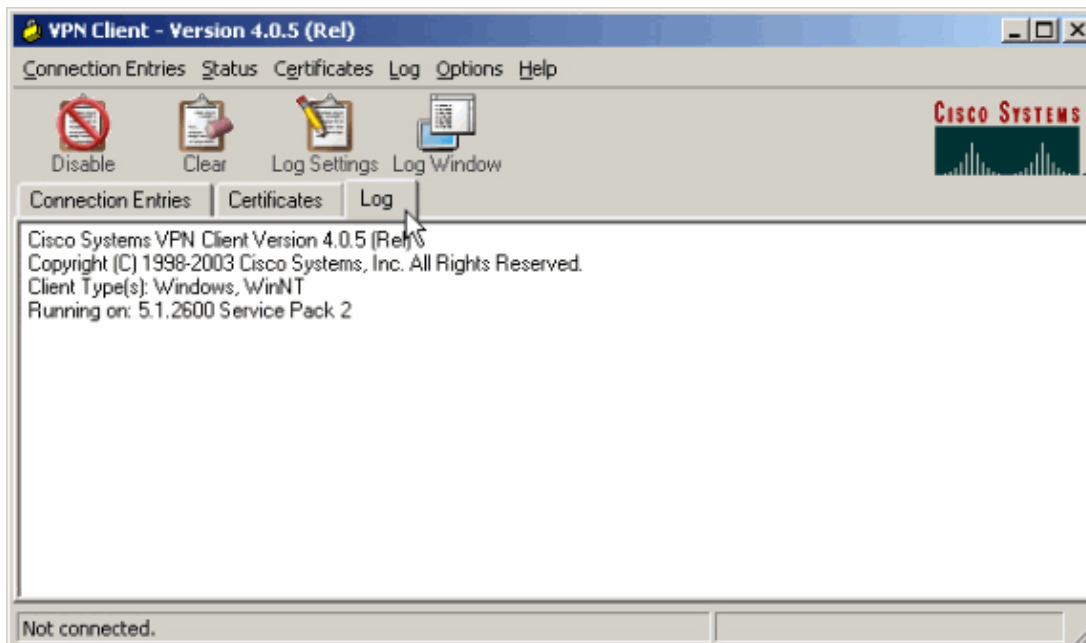


- Go to the Route Details tab in order to see which networks the VPN Client sends encrypted traffic to. In this example, the VPN Client communicates securely with 10.0.1.0/24 while all other traffic is sent unencrypted to the Internet.



View the VPN Client Log

When you examine the VPN Client log, you can determine whether or not the parameter that allows split tunneling is set. Go to the Log tab in the VPN Client in order to view the log. Click **Log Settings** in order to adjust what is logged. In this example, IKE and IPsec are set to **3– High** while all other log elements are set to **1 – Low**.



```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
```

```
1      14:21:43.106  07/21/06  Sev=Info/6      IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.
```

!--- Output is suppressed.

```
28     14:21:55.151  07/21/06  Sev=Info/5      IKE/0x6300005D
Client sending a firewall request to concentrator
```

```
29     14:21:55.151  07/21/06  Sev=Info/5      IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).
```

```
30     14:21:55.151  07/21/06  Sev=Info/5      IKE/0x6300005C
Firewall Policy: Product=Cisco Intrusion Prevention Security Agent,
Capability= (Are you There?).
```

```
31     14:21:55.171  07/21/06  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106
```

```
32     14:21:56.114  07/21/06  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 172.22.1.106
```

```
33     14:21:56.114  07/21/06  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.106
```

```
34     14:21:56.114  07/21/06  Sev=Info/5      IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50
```

```
35     14:21:56.114  07/21/06  Sev=Info/5      IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0
```

```
36     14:21:56.114  07/21/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000
```

!--- Split tunneling is configured.

```
37      14:21:56.114  07/21/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x00000001

38      14:21:56.114  07/21/06  Sev=Info/5      IKE/0x6300000F
SPLIT_NET #1
    subnet = 10.0.1.0
    mask = 255.255.255.0
    protocol = 0
    src port = 0
    dest port=0

39      14:21:56.124  07/21/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000

40      14:21:56.124  07/21/06  Sev=Info/5      IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems,
Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29 2006 20:21:56

41      14:21:56.124  07/21/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = Received and using NAT-T port number , value = 0x00001194
```

!--- Output is suppressed.

Troubleshoot

Refer to IPsec with VPN Client to VPN 3000 Concentrator Configuration Example – Troubleshooting for general information on troubleshooting this configuration.

Related Information

- [IPsec with VPN Client to VPN 3000 Concentrator Configuration Example](#)
- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN Client](#)
- [Technical Support & Documentation – 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: Nov 14, 2007

Document ID: 70799
