

Allow Local LAN Access for VPN Clients on the VPN 3000 Concentrator Configuration Example

Document ID: 70775

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

Background Information

Configure Local LAN Access for VPN Clients

- Configure the VPN Concentrator
- Configure the VPN Client

Verify

- Connect with the VPN Client
- View the VPN Client Log
- Test Local LAN Access with Ping
- View Sessions on the Concentrator

Troubleshoot

- Unable to Print or Browse by Name

Related Information

Introduction

This document provides step-by-step instructions on how to allow VPN Clients to **only** access their local LAN while tunneled into a VPN 3000 Series Concentrator. This configuration allows VPN Clients secure access to corporate resources via IPsec and still gives the client the ability to carry out activities like printing wherever the client is located. If it is permitted, traffic destined for the Internet is still tunneled to the VPN Concentrator.

Note: This is not a configuration for split tunneling, where the client has unencrypted access to the Internet while connected to the VPN Concentrator. Refer to [Split Tunneling for VPN Clients on the VPN 3000 Concentrator Configuration Example](#) for information on how to configure split tunneling on the VPN 3000 Series Concentrators.

Prerequisites

Requirements

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

Components Used

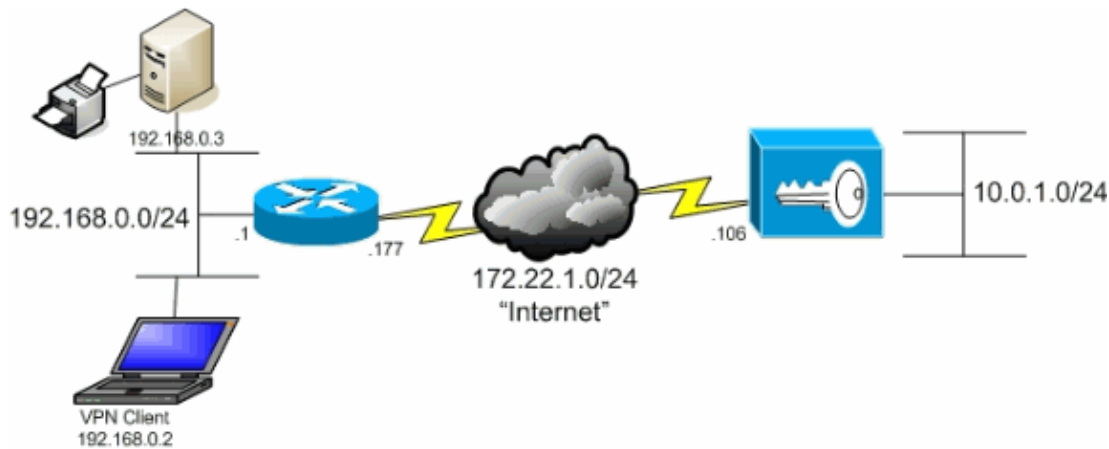
The information in this document is based on these software and hardware versions:

- 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

Unlike a classic split tunneling scenario in which all Internet traffic is sent unencrypted, enabling local LAN access for VPN Clients permits those clients to communicate unencrypted with only devices on the network on which they are located. For example, a VPN Client who is allowed local LAN access while connected to the VPN Concentrator from home is able to print to their own printer, but not access the Internet without first sending the traffic over the tunnel.

A network list is used in order to allow local LAN access in much the same way that split tunneling is configured on the VPN Concentrator. However, instead of defining which networks *should be* encrypted, the network list in this case defines which networks *should not be* encrypted. Moreover, unlike the split tunneling scenario, the actual networks in the list do not need to be known. Instead, the VPN Concentrator supplies a default network of 0.0.0.0/0.0.0.0 which is understood to mean the local LAN of the VPN Client.

Note: When the VPN Client is connected and configured for local LAN access, you *cannot print or browse by name* on the local LAN. However, you can browse or print by IP address. See the Troubleshooting section of this document for more information as well as workarounds for this situation.

Configure Local LAN Access for VPN Clients

Complete these two tasks in order to allow VPN Clients access to their local LAN while connected to the VPN Concentrator:

- Configure the VPN Concentrator

- Configure the VPN Client

Configure the VPN Concentrator

Complete these steps on the VPN Concentrator in order to allow VPN Clients to have local LAN access while connected:

1. Choose **Configuration > Policy Management > Traffic Management > Network Lists**.

The screenshot shows the web interface of the VPN 3000 Concentrator Series Manager. The top navigation bar includes 'Main | Help | Support | Logout' and 'Logged in: admin'. The breadcrumb trail is 'Configuration | Policy Management | Traffic Management | Network Lists'. A 'Save Needed' indicator is present in the top right. The left sidebar shows a tree view with 'Configuration' expanded to 'Traffic Management' > 'Network Lists'. The main content area contains the following text:

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List	Actions
VPN Client Local LAN (Default)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Copy"/> <input type="button" value="Delete"/>

The Cisco Systems logo is visible in the bottom left corner of the interface.

2. Verify that the VPN Client Local LAN (Default) list is present and click **Modify** to verify that the default network of 0.0.0.0/0.0.0.0 is present.

Alternatively, you can type in a new network address and wildcard mask in order to define the network at this point. Click **Apply** when you are done.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name: VPN Client Local LAN (Default)

Network List: 0.0.0.0/0.0.0.0

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

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (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, 10.10.1.0/0.0.255 = 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.

Apply Cancel Generate Local List

- Once you confirm that the network list is present, you must 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
<p>Add Group</p> <p>Modify Group</p> <p>Delete Group</p>	<p>ipsecgroup (Internally Configured)</p>	<p>Authentication Servers</p> <p>Authorization Servers</p> <p>Accounting Servers</p> <p>Address Pools</p> <p>Client Update</p> <p>Bandwidth Assignment</p> <p>WebVPN Servers and URLs</p> <p>WebVPN Port Forwarding</p>

- Select the **Client Config** tab of the group that you have chosen to modify.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

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.

Identity | 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

5. Scroll down to the sections labeled Split Tunneling Policy and Split Tunneling Network List.
6. Check **Allow the networks in the list to bypass the tunnel**. Then, select the list from step 1 in the drop-down.

In this case it is **VPN Client Local LAN (Default)**. 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

- Interfaces
- System
- User Management
 - Base Group
 - Groups
 - Users
- Policy Management
- Tunneling and Security
- Administration
- Monitoring

Banner	<input checked="" type="checkbox"/>	Enter the banner for this group.
Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input checked="" type="checkbox"/> Allow the networks in list to bypass the tunnel <input 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. <input type="checkbox"/> 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. <input type="checkbox"/> 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	<input type="checkbox"/> VPN Client Local LAN (Default) <ul style="list-style-type: none"> VPN Client Local LAN (Default) -None- VPN Client Local LAN (Default) 	<input type="checkbox"/> Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Default Domain Name	<input type="text"/>	<input checked="" type="checkbox"/> Enter the default domain name given to users of this group.
Split DNS Names	<input type="text"/>	<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

CISCO SYSTEMS

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

Configure the VPN Client

Complete these steps in the VPN Client in order to allow the client to have local LAN access while connected to the VPN Concentrator.

1. Choose your existing connection entry and click **Modify**.

VPN Client - Version 4.0.5 (Rel)

Connection Entries | Status | Certificates | Log | Options | Help

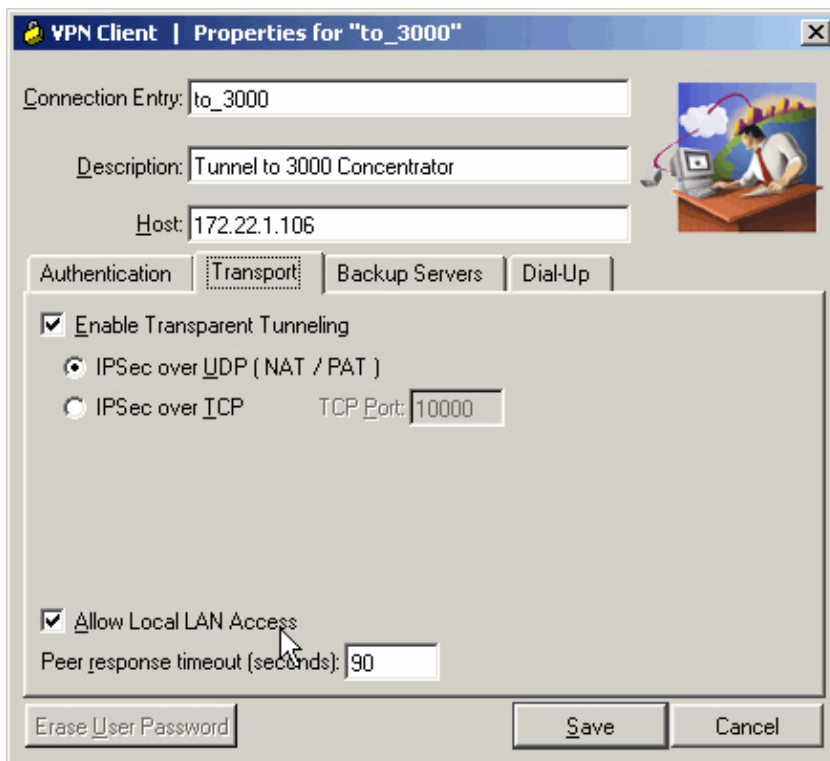
Connect | New | Import | **Modify** | Delete

CISCO SYSTEMS

Connection Entry	Host	Transport
to_3000	172.22.1.106	IPSec/UDP

Not connected.

2. Go to the Transport tab and check **Allow Local LAN Access**. Click **Save** when you are done.



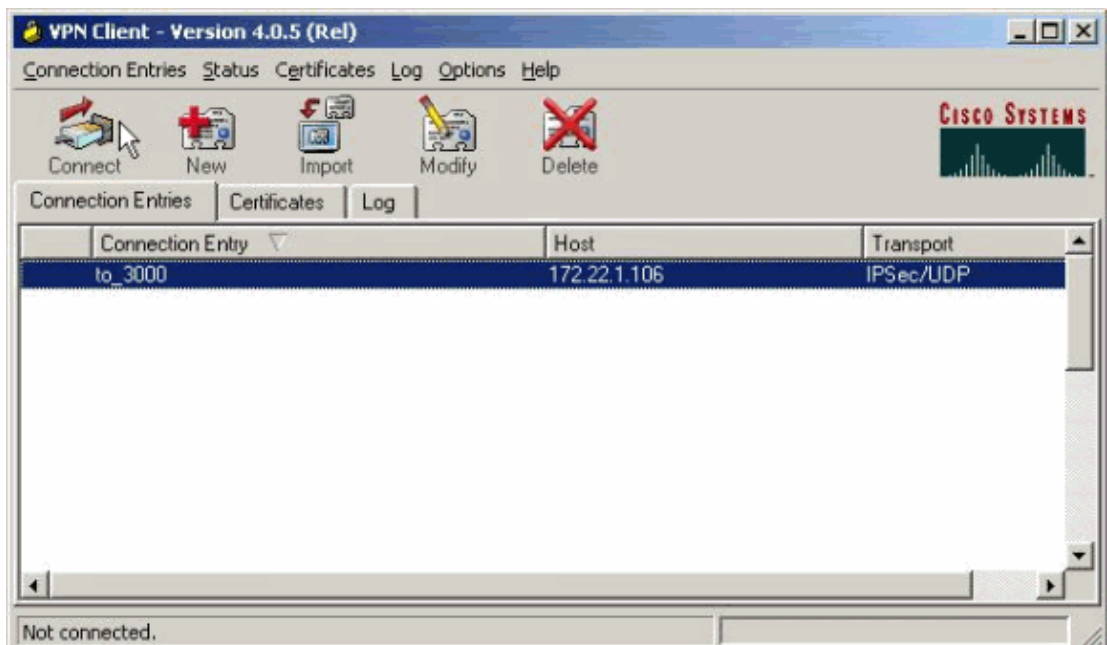
Verify

Follow the steps in these sections in order to verify your configuration.

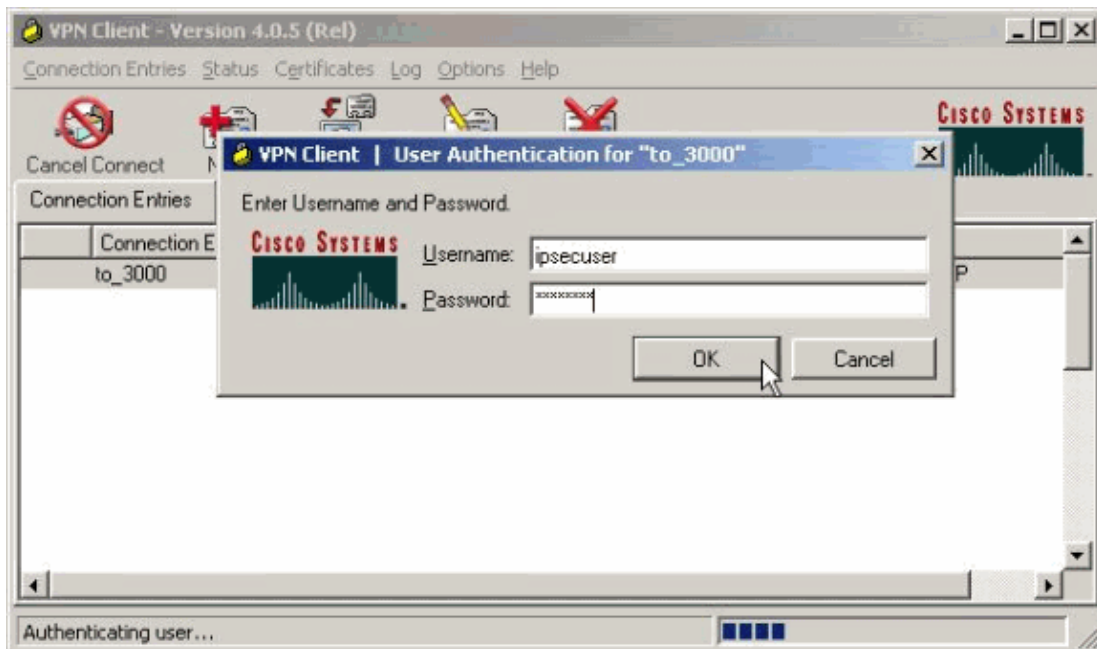
Connect with the VPN Client

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

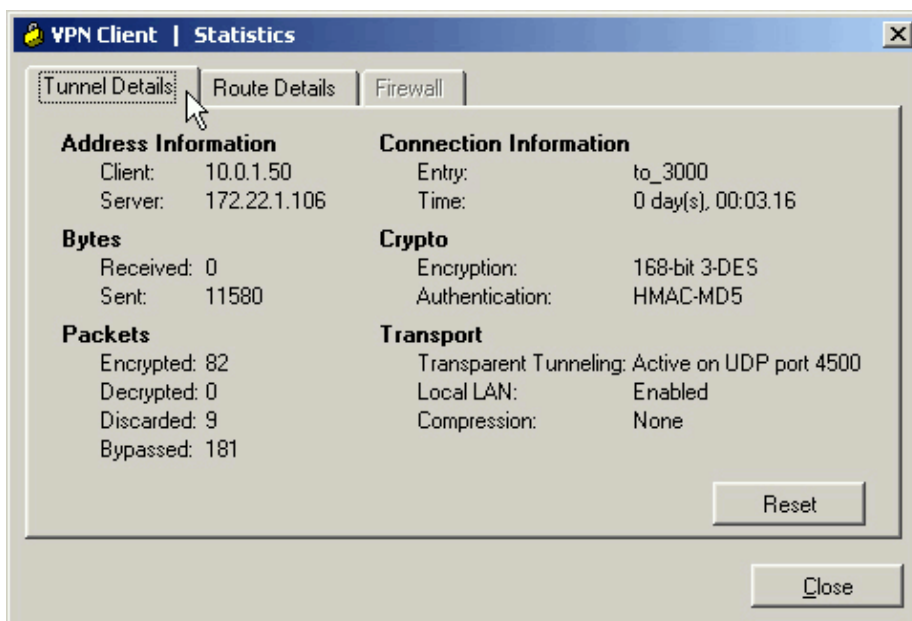
1. Choose your connection entry from the list and click **Connect**.



2. Enter your credentials.

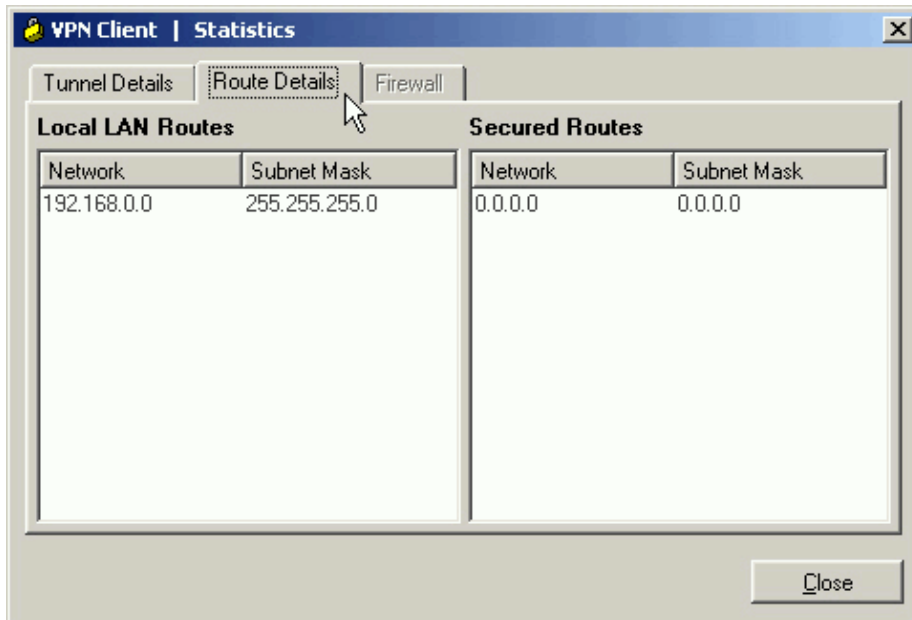


3. Choose **Status > Statistics...** in order to display the Tunnel Details window where you can inspect the particulars of the tunnel and see traffic flowing.



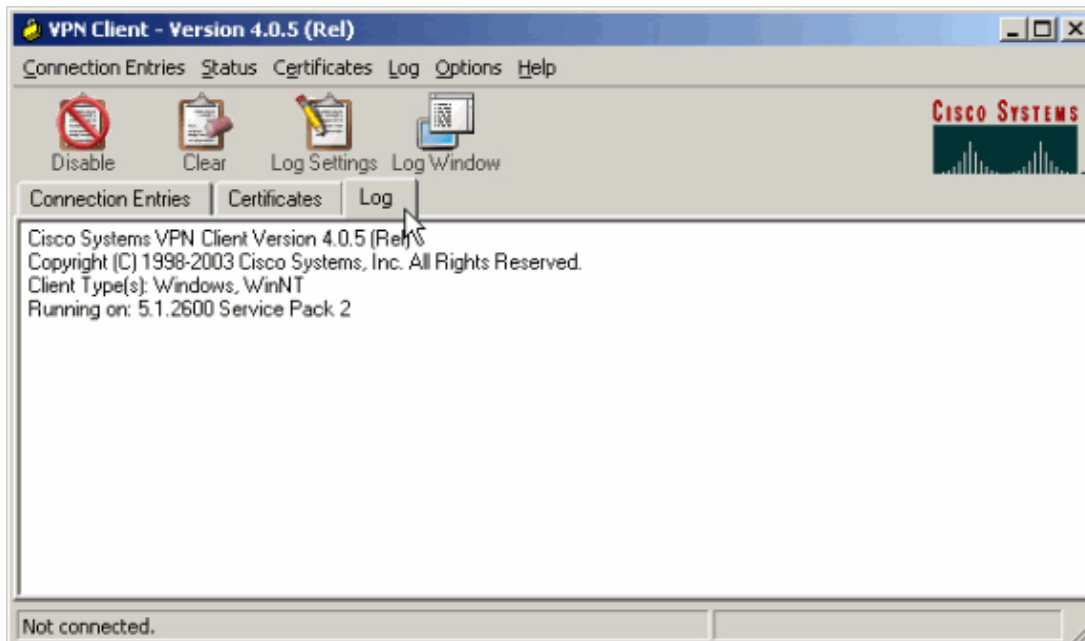
4. Go to the Route Details tab in order to see which routes the VPN Client still has local access to.

In this example, the VPN Client is allowed local LAN access to 192.168.0.0/24 while all other traffic is encrypted and sent across the tunnel.



View the VPN Client Log

When you examine the VPN Client log, you can determine whether or not the parameter that allows local LAN access is set. In order to view the log, go to the Log tab in the VPN Client. Then click on **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      16:22:08.214 07/19/06 Sev=Info/6      IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.
```

!--- Output is suppressed.

```

26      16:22:39.338  07/19/06  Sev=Info/5      IKE/0x6300005D
Client sending a firewall request to concentrator

27      16:22:39.338  07/19/06  Sev=Info/5      IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).

28      16:22:39.338  07/19/06  Sev=Info/5      IKE/0x6300005C
Firewall Policy: Product=Cisco Intrusion Prevention Security Agent,
Capability= (Are you There?).

29      16:22:39.348  07/19/06  Sev=Info/4      IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106

30      16:22:39.348  07/19/06  Sev=Info/6      IKE/0x63000054
Sent a keepalive on the IPSec SA

31      16:22:40.200  07/19/06  Sev=Info/5      IKE/0x6300002F
Received ISAKMP packet: peer = 172.22.1.106

32      16:22:40.200  07/19/06  Sev=Info/4      IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.106

33      16:22:40.200  07/19/06  Sev=Info/5      IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50

34      16:22:40.200  07/19/06  Sev=Info/5      IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0

35      16:22:40.200  07/19/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000

36      16:22:40.200  07/19/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000

37      16:22:40.210  07/19/06  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

!--- Local LAN access is permitted and the local LAN defined.

38      16:22:40.230  07/19/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_INCLUDE_LOCAL_LAN (# of local_nets),
value = 0x00000001

39      16:22:40.230  07/19/06  Sev=Info/5      IKE/0x6300000F
LOCAL_NET #1
    subnet = 192.168.0.0
    mask = 255.255.255.0
    protocol = 0
    src port = 0
    dest port=0

40      16:22:40.230  07/19/06  Sev=Info/5      IKE/0x6300000D
MODE_CFG_REPLY: Attribute = Received and using NAT-T port number , value = 0x00001194

!--- Output is suppressed.

```

Test Local LAN Access with Ping

An additional way to test that the VPN Client still has local LAN access while tunneled to the VPN Concentrator is to use the **ping** command at the Windows command line. The local LAN of the VPN Client is

192.168.0.0/24 and another host is present on the network with an IP address of 192.168.0.3.

```
C:\>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data:

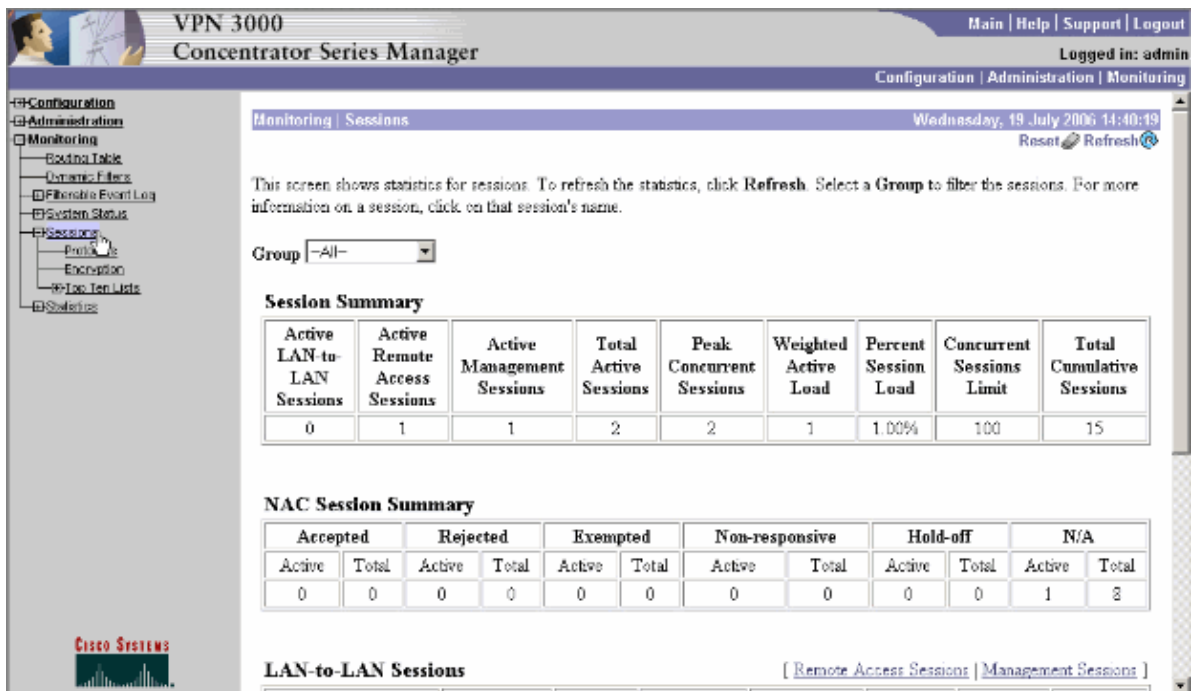
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

View Sessions on the Concentrator

You can also view the session(s) on the VPN Concentrator in order to verify that the tunnel is up.

1. Choose **Monitoring > Sessions** in order to see active sessions on the VPN Concentrator.



The screenshot shows the web interface of a VPN 3000 Concentrator Series Manager. The page title is "Monitoring | Sessions" and the date is "Wednesday, 19 July 2006 14:40:49". The user is logged in as "admin". The left sidebar shows a navigation tree with "Monitoring" selected. The main content area displays session statistics and summary tables.

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Weighted Active Load	Percent Session Load	Concurrent Sessions Limit	Total Cumulative Sessions
0	1	1	2	2	1	1.00%	100	15

NAC Session Summary

Accepted		Rejected		Exempted		Non-responsive		Hold-off		N/A	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	1	2

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

2. Scroll down to see more information about connected sessions.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring

NAC Session Summary

Accepted		Rejected		Exempted		Non-responsive		Hold-off		N/A	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	1	8

LAN-to-LAN Sessions [Remote Access Sessions | Management Sessions]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
No LAN-to-LAN Sessions							

Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
ipsecuser	10.0.1.50 172.22.1.177	ipsecgroup	IPSec/NAT-T 3DES-168	Jul 19 14:35:47 004:32	WinNT 4.0.5 (Rel)	206928 43432	N/A

Management Sessions [LAN-to-LAN Sessions | Remote Access Sessions]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	10.0.1.50	HTTP	None	Jul 19 14:39:38	0:00:41

Troubleshoot

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

Unable to Print or Browse by Name

When the VPN Client is connected and configured for local LAN access, you *cannot print or browse by name* on the local LAN. There are two options available to work around this situation:

- Browse or print by IP address.
 - ◆ In order to browse, instead of using the syntax `\\sharename`, use the syntax `\\x.x.x.x` where `x.x.x.x` is the IP address of the host computer.
 - ◆ In order to print, change the properties for the network printer to use an IP address instead of a name. For example, instead of the syntax `\\sharename\printername`, use `\\x.x.x.x\printername`, where `x.x.x.x` is an IP address.
- Create or modify the VPN Client LMHOSTS file. An LMHOSTS file on a Windows PC allows you to create static mappings between hostnames and IP addresses. For example, an LMHOSTS file might look like this:

```
192.168.0.3 SERVER1
192.168.0.4 SERVER2
192.168.0.5 SERVER3
```

In Windows XP Professional Edition, the LMHOSTS file is located in `%SystemRoot%\System32\Drivers\Etc`. Refer to your Microsoft documentation or Microsoft KB Article 314108 for more information.

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](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Nov 14, 2007

Document ID: 70775
