

# Configuring the Cisco VPN 3000 Concentrator for Blocking with Filters and RADIUS Filter Assignment

Document ID: 13834

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Network Diagram
- Conventions

### VPN 3000 Configuration

#### Filters for a LAN-to-LAN VPN Tunnel

#### VPN 3000 Configuration – RADIUS Filter Assignment

#### CSNT Server Configuration – RADIUS Filter Assignment

#### Debug – RADIUS Filter Assignment

#### Verify

#### Troubleshoot

#### NetPro Discussion Forums – Featured Conversations

#### Related Information

---

## Introduction

In this sample configuration, we want to use filters to allow a user to access only one server (10.1.1.2) inside the network and block access to all other resources. The Cisco VPN 3000 Concentrator can be set up to control IPsec, Point-to-Point Tunneling Protocol (PPTP), and L2TP client access to network resources with filters. Filters consist of rules, which are similar to access lists on a router. If a router was configured for:

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

the VPN Concentrator equivalent would be to set up a filter with rules.

Our first VPN Concentrator rule is **permit\_server\_rule**, which is equivalent to the router's **permit ip any host 10.1.1.2** command. Our second VPN Concentrator rule is **deny\_server\_rule** which is equivalent to the router's **deny ip any any** command.

Our VPN Concentrator filter is **filter\_with\_2\_rules**, which is equivalent to the router's 101 access list; it uses **permit\_server\_rule** and **deny\_server\_rule** (in that order). It is assumed that clients can connect properly prior to adding filters; they receive their IP addresses from a pool on the VPN Concentrator.

Refer to PIX/ASA 7.x ASDM: Restrict the Network Access of Remote Access VPN Users in order to learn more about the scenario where the PIX/ASA 7.x block the access from the VPN users.

## Prerequisites

## Requirements

There are no specific requirements for this document.

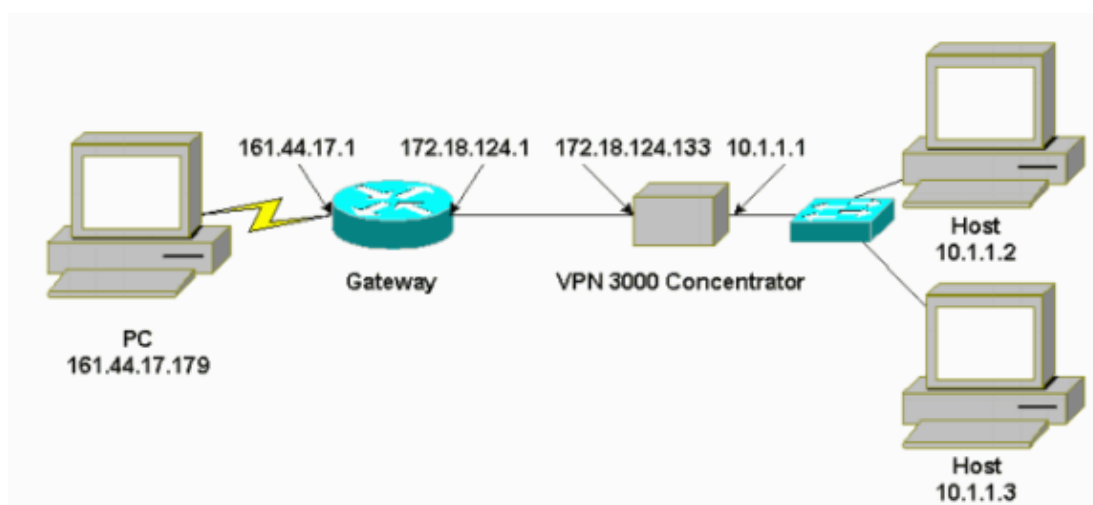
## Components Used

The information in this document is based on Cisco VPN 3000 Concentrator version 2.5.2.D.

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

This document uses this network setup:



## Conventions

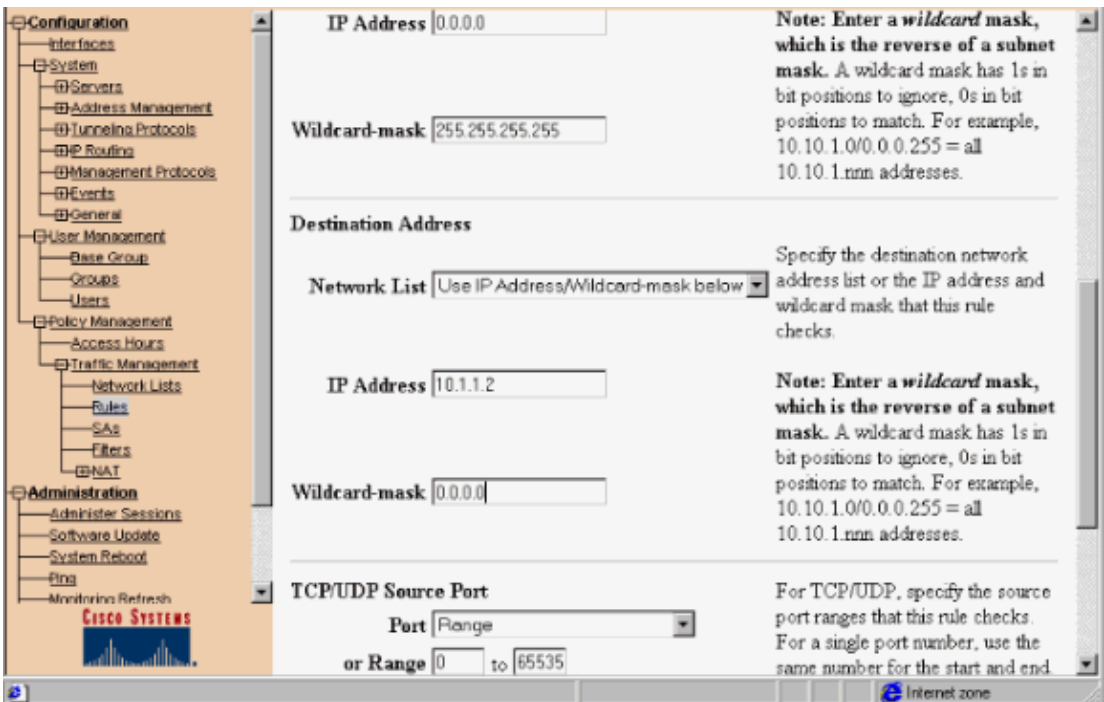
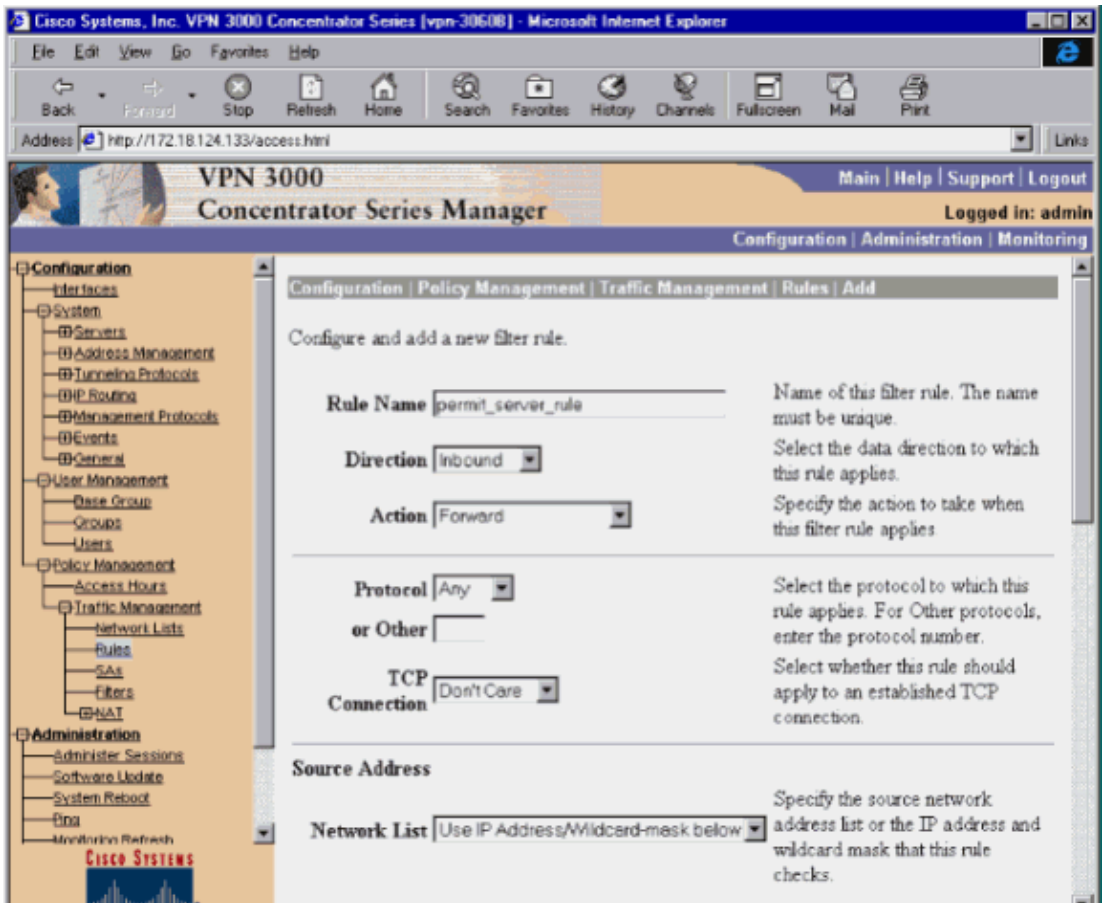
Refer to Cisco Technical Tips Conventions for more information on document conventions.

## VPN 3000 Configuration

Complete these steps in order to configure the VPN 3000 Concentrator.

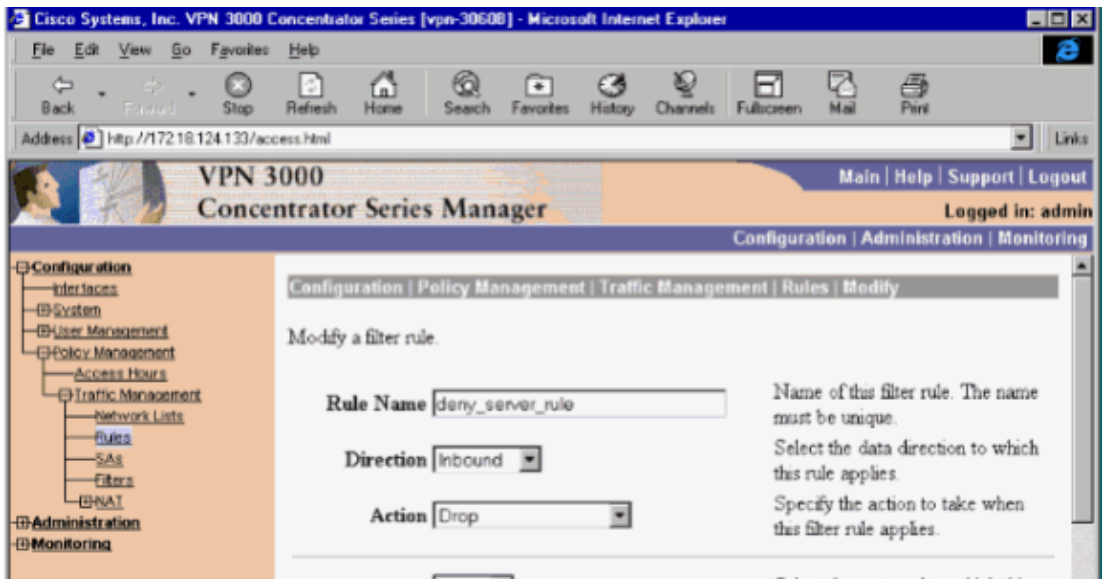
1. Choose **Configuration >Policy Management > Traffic Management > Rules > Add** and define the first VPN Concentrator rule called **permit\_server\_rule** with these settings:

- ◆ Direction **Inbound**
- ◆ Action **Forward**
- ◆ Source Address **255.255.255.255**
- ◆ Destination Address **10.1.1.2**
- ◆ Wildcard Mask **0.0.0.0**

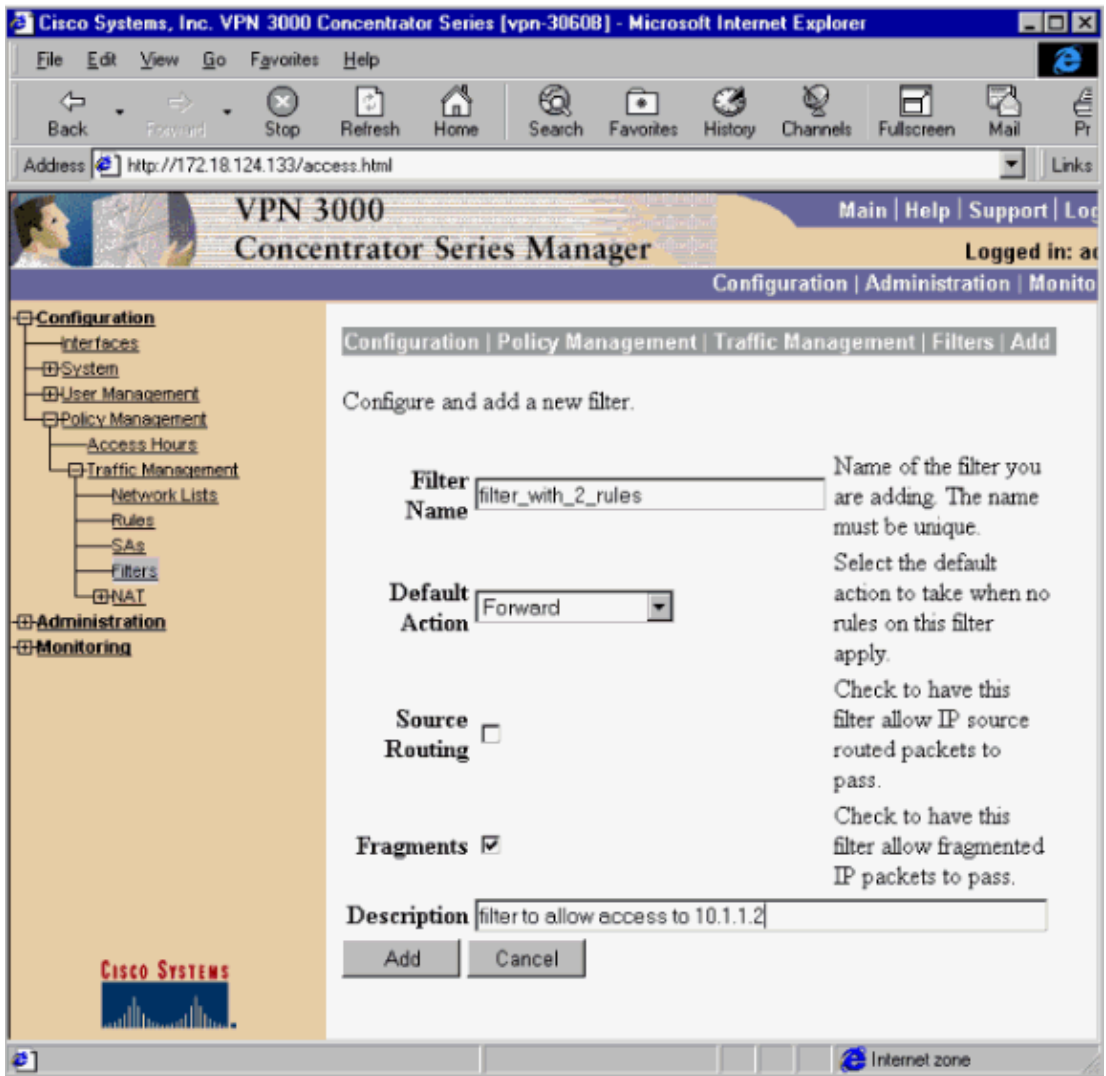


2. In the same area, define the second VPN Concentrator rule called **deny\_server\_rule** with these defaults:

- ◆ Direction **Inbound**
- ◆ Action **Drop**
- ◆ Source and Destination Addresses of anything (255.255.255.255):



3. Choose **Configuration > Policy Management > Traffic Management > Filters** and add your **filter\_with\_2\_rules** filter.



4. Add the two rules to filter\_with\_2\_rules:

Address: http://172.16.124.133/access.html

VPN 3000 Concentrator Series Manager

Logged in: admin

Configuration | Administration | Monitoring

Save Needed

Add, remove, prioritize, and configure rules that apply to a filter.

**Filter Name:** filter\_with\_2\_rules

Select an **Available Rule** and click **Add** to apply it to this filter.

Select a **Current Rule in Filter** and click **Remove**, **Move Up**, **Move Down**, or **Assign SA to Rule** as appropriate.

Select an **Available Rule**, then select a **Current Rule in Filter**, and click **Insert Above** to add the available rule above the current rule.

Current Rules in Filter	Actions	Available Rules
permit_server_rule (forward/in) deny_server_rule (drop/in)	<< Add << Insert Above Remove >> Move Up Move Down Assign SA to Rule Done	GRE In (forward/in) GRE Out (forward/out) IPSEC-ESP In (forward/in) IKE In (forward/in) IKE Out (forward/out) PPTP In (forward/in) PPTP Out (forward/out) L2TP In (forward/in) L2TP Out (forward/out) ICMP In (forward/in) ICMP Out (forward/out) RIP In (forward/in)

5. Choose **Configuration > User Management > Groups** and apply the filter to the group:

Configuration | User Management | Groups | Modify servergroup

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.

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow alphabetic-only passwords.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	filter_with_2_rules	<input type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
		<input type="checkbox"/>	Enter the IP address of the

## Filters for a LAN-to-LAN VPN Tunnel

From VPN Concentrator code 3.6 and later, you can filter traffic for each LAN-to-LAN IPsec VPN tunnel. For example, if you build a LAN-to-LAN tunnel to another VPN Concentrator with the address 172.16.1.1, and want to permit host 10.1.1.2 access to the tunnel while you deny all other traffic, you can apply **filter\_with\_2\_rules** when you choose **Configuration > System > Tunneling Protocols > IPsec > LAN-to-LAN > Modify** and select **filter\_with\_2\_rules** under **Filter**.

The screenshot shows the configuration interface for a VPN 3000 Concentrator. The left sidebar contains a tree view with categories: Configuration, Administration, and Monitoring. Under Configuration, the 'IPSec' sub-tree is expanded to show 'LAN-to-LAN' selected. The main content area is titled 'Modify an IPSec LAN-to-LAN connection' and contains the following fields:

- Name:** Test Lan to Lan
- Interface:** Ethernet 2 (Public) (172.18.124.133)
- Peer:** 172.16.1.1
- Digital Certificate:** None (Use Preshared Keys)
- Certificate Transmission:** Identity certificate only (selected)
- Preshared Key:** cisco123
- Authentication:** ESP/MD5/HMAC-128
- Encryption:** 3DES-168
- IKE Proposal:** IKE-3DES-MD5
- Filter:** filter\_with\_2\_rules

At the bottom, there is an unchecked checkbox for 'IPSec NAT-T'.

## VPN 3000 Configuration – RADIUS Filter Assignment

It is also possible to define a filter in the VPN Concentrator and then pass down the filter number from a RADIUS server (in RADIUS terms, attribute 11 is Filter-id), so that when the user is authenticated on the RADIUS server, the Filter-id is associated with that connection. In this example, the assumption is that RADIUS authentication for VPN Concentrator users is already operational and only the Filter-id is to be added.

Define the filter on the VPN Concentrator as in the previous example:

Modify a configured filter.

**Filter Name**

**Default Action**

**Source Routing**

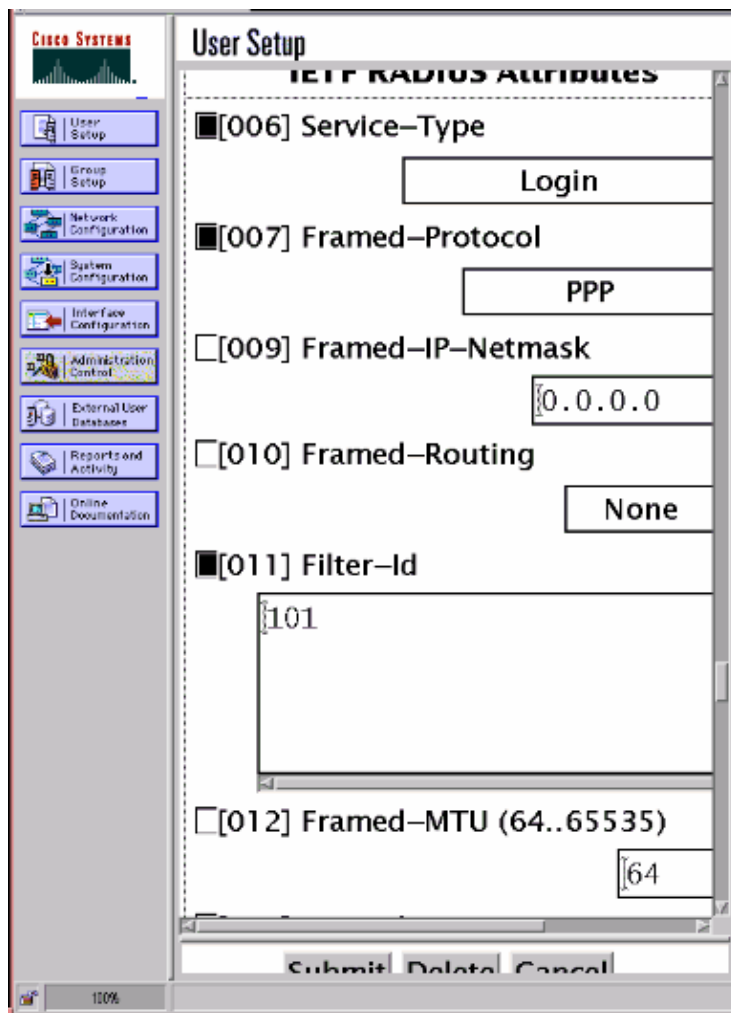
**Fragments**

**Description**

Name of the filters are modified. The filter name must be unique.  
Select the default action to take when no rules are applied.  
Check to allow source routing. This filter allows routed packets to pass.  
Check to allow fragmented packets. This filter allows IP packets to pass.

## CSNT Server Configuration – RADIUS Filter Assignment

Configure attribute 11, Filter-id on the Cisco Secure NT server to be **101**:



## Debug – RADIUS Filter Assignment

If AUTHDECODE (1–13 Severity) is on in the VPN Concentrator, the log shows that the Cisco Secure NT server sends down access-list 101 in attribute 11 (0x0B):

```

207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001 .v.....
0020: 0B053130 310806FF FFFFFFFF ..101.....

```

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

For troubleshooting purposes only, you can turn on filter debugging when you choose **Configuration > System > Events > Classes** and add **FILTERDBG** class with **Severity to Log = 13**. In the rules, change the Default action from Forward (or Drop) to **Forward and Log** (or Drop and Log). When the event log is retrieved at **Monitoring > Event Log**, it should show entries such as:

```

221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

```

## 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

- [IPsec Negotiation/IKE Protocols](#)
- [VPN 3000 Concentrator Frequently Asked Questions](#)
- [RADIUS Support](#)
- [Cisco VPN 3000 Concentrator Support](#)
- [Cisco VPN 3000 Client Support](#)
- [Cisco Secure ACS for Windows Support](#)
- [Request for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 07, 2007

Document ID: 13834