

# Configuring the Cisco VPN 5000 Client to the Cisco VPN 5000 Concentrator with Cisco Secure UNIX (RADIUS) Authentication

Document ID: 10132

---

**Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End-of-Sales Announcement.**

---

## **Introduction**

### **Prerequisites**

- Requirements
- Components Used
- Conventions

### **Configure**

- Network Diagram
- Configurations

### **Change to PAP Authentication**

- VPN 5000 RADIUS Profile Change
- Cisco Secure User Profile
- VPN 5000 PAP Debug

### **Add IP Address Assignment**

#### **Add Accounting**

- Accounting Records From Cisco Secure UNIX

### **Debug – Good Authentication**

- VPN 5000 Concentrator
- Cisco Secure UNIX

### **What Can Go Wrong**

- Cisco Secure UNIX Server Unreachable
- Authentication Fails
- VPNgroup Password Entered by User Does Not Agree with VPNPassword
- Group Name Sent Down by the RADIUS Server Does Not Exist on the VPN 5000 Concentrator

### **NetPro Discussion Forums – Featured Conversations**

#### **Related Information**

---

## **Introduction**

The Cisco VPN 5000 Concentrator can be configured to authenticate VPN 5000 Clients through Cisco Secure UNIX (CSUNIX) RADIUS. This document assumes that local authentication works prior to adding RADIUS authentication (hence our user localuser in group ciscolocal). Authentication is then added to Cisco Secure UNIX RADIUS for users that do not exist in the local database (user csunixuser is assigned to group csunix by virtue of the attributes returned from the Cisco Secure UNIX RADIUS server).

The VPN 5000 Concentrator uses Vendor-Specific RADIUS attributes by default:

- VPNGroupInfo
- VPNPassword

Since these are not native to Cisco Secure UNIX, the choice was made to have Cisco Secure return non-vendor-specific attributes instead:

VPN5000	attribute	CiscoSecure UNIX
-----	-----	-----
VPNGroupInfo	67	Tunnel-Client-Endpoint
VPNPassword	66	Tunnel-Server-Endpoint

## 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 Secure UNIX 2.3.5.1
- VPN 5000 Concentrator 5.2.16.0005
- VPN 5000 Client 4.2.7

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 the Cisco Technical Tips Conventions.

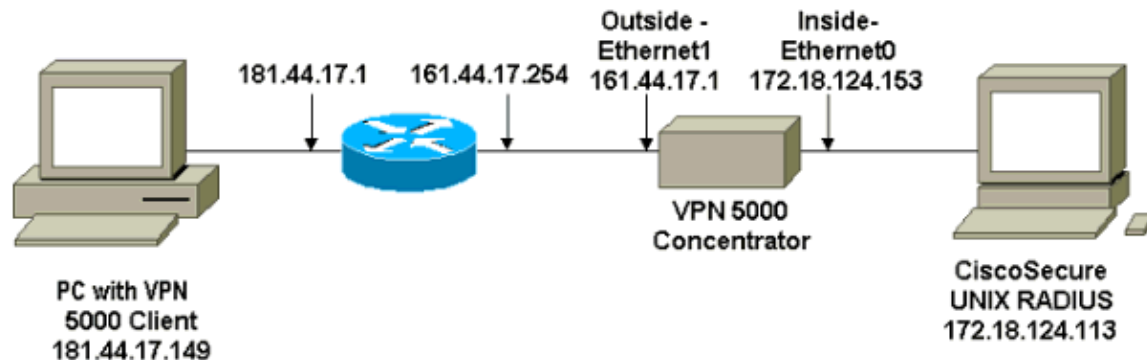
## Configure

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:

- VPN 5000 Concentrator
- VPN 5000 Client
- Cisco Secure UNIX

**Note:** If the RADIUS server supports either VPN 5000 vendor-specific attributes or the default attribute 69 for VPNPassword and 77 for VPNGroupInfo, the configuration does not need to include those parameters.

VPN 5000 Concentrator	
[ IP Ethernet 0 ]	
SubnetMask	= 255.255.255.0
Mode	= Routed
IPAddress	= 172.18.124.153
[ IP Ethernet 1 ]	
Mode	= Routed
SubnetMask	= 255.255.255.0
IPAddress	= 161.44.17.1
[ VPN Group "ciscolocal" ]	
IPNet	= 172.18.124.0/24
Transform	= esp(md5,des)
StartIPAddress	= 172.18.124.250
MaxConnections	= 4
BindTo	= "ethernet0"
[ General ]	
EthernetAddress	= 00:00:a5:f0:c9:00
DeviceType	= VPN 5001 Concentrator
ConfiguredOn	= Timeserver not configured
ConfiguredFrom	= Command Line, from 172.18.124.99
IPSecGateway	= 161.44.17.254
[ Logging ]	
Level	= 7
Enabled	= On
LogToAuxPort	= On
LogToSysLog	= On
SyslogIPAddress	= 172.18.124.114
SyslogFacility	= Local5
[ IKE Policy ]	
Protection	= MD5_DES_G1
[ VPN Users ]	
localuser Config="ciscolocal" SharedKey="locallike"	
[ Radius ]	
VPNGroupInfo	= 67
VPNPassword	= 66
PrimAddress	= "172.18.124.113"
Secret	= "CSUnix"
ChallengeType	= CHAP
BindTo	= "ethernet0"
Authentication	= On
[ VPN Group "csunix" ]	
Transform	= ESP(md5,des)
BindTo	= "ethernet0"

```

StartIPAddress          = 172.18.124.243
IPNet                   = 172.18.124.0/24

MaxConnections          = 3

Configuration size is 2202 out of 65500 bytes.

```

**Note:** For the VPN 5000 Client configuration, none of the defaults are changed. Two users are added, and the appropriate passwords entered when prompted after clicking Connect.

VPN 5000 Client		
username	password	radius_password
-----	-----	-----
localuser	localike	N/A
csunixuser	grouppass	csunixpass

**Note:** For the Cisco Secure UNIX configuration, any RADIUS reply-attribute in the 64–191 range with a string value works. This must agree with those values configured on the VPN 5000 by the VPNPassword and VPNGroupInfo values.

```

Cisco Secure UNIX

User Profile
# ../CLI/ViewProfile -p 9900 -u csunixuser
User Profile Information
user = csunixuser{
profile_id = 56
profile_cycle = 1
radius=IETF {
check_items= {
2=csunixpass
}
reply_attributes= {
66=grouppass
67=csunix
}
}
}

VPN 5000 Concentrator Profile
# ../CLI/ViewProfile -p 9900 -u NAS.172.18.124.153
User Profile Information
user = NAS.172.18.124.153{
profile_id = 48
profile_cycle = 1
NASNAME="172.18.124.153"
SharedSecret="CSUnix"
RadiusVendor="Cisco"
Dictionary="DICTIONARY.IETF"
}

```

## Change to PAP Authentication

Based on the assumption that Challenge Handshake Authentication Protocol (CHAP) authentication works, the decision is made to change to Password Authentication Protocol (PAP).

## VPN 5000 RADIUS Profile Change

```
[ Radius ]
PAPAuthSecret          = "abcxyz"
ChallengeType          = PAP
```

## Cisco Secure User Profile

```
# ./ViewProfile -p 9900 -u csunix1102
User Profile Information
user = csunix1102{
profile_id = 60
profile_cycle = 1
radius=IETF {
check_items= {
2=abc
}
}
reply_attributes= {
66=csunixpass
67=csunix
}
}
}
```

What the user sees (three password boxes):

```
Shared Secret = csunixpass
RADIUS Login box - Password = abc
RADIUS Login box - Authentication Secret = abcxyz
```

## VPN 5000 PAP Debug

```
show sys log buffer
Notice 68795.42 seconds New IKE connection:
  [181.44.17.149]:1034:csunix1102
Debug 68795.48 seconds Sending RADIUS PAP challenge
  to csunix1102 at 181.44.17.149
Debug 68806.12 seconds Received RADIUS PAP response
  from csunix1102 at 181.44.17.149,
  contacting server
Notice 68806.36 seconds VPN 0 opened for csunix1102
  from 181.44.17.149.
Debug 68806.38 seconds Client's local broadcast
  address = 181.44.17.255
Notice 68806.41 seconds User assigned IP address 172.18.124.243
```

## Add IP Address Assignment

If RADIUS attribute 8, Framed-IP-Address is sent down from the Cisco Secure UNIX RADIUS server:

```
8=172.18.124.240
```

and the VPN 5000 Concentrator group is set for:

```
AssignIPRADIUS = On
```

this assigns that IP address to the client.

# Add Accounting

In order to have session accounting records sent to the Cisco Secure UNIX RADIUS server, add to the VPN 5000 Concentrator RADIUS configuration:

```
[ Radius ]
Accounting = On
```

Then **apply**, **write**, and **boot** the VPN 5000 Concentrator for this to take effect.

## Accounting Records From Cisco Secure UNIX

```
NAS-IP-Address = 172.18.124.153
NAS-Port-Type = Virtual
NAS-Port = 268435456
User-Name = "csunixuser"
Acct-Status-Type = Start
Acct-Session-Id = "78a8dd45-00000000"
Acct-Authentic = RADIUS
Tunnel-Server-Endpoint = "csunix"
Tunnel-Client-Endpoint = "181.44.17.149"
Tunnel-Server-Endpoint = "172.18.124.243"
```

```
NAS-IP-Address = 172.18.124.153
NAS-Port-Type = Virtual
NAS-Port = 268435456
Username = "csunixuser"
Acct-Status-Type = Stop
Acct-Session-Id = "78a8dd45-00000000"
Acct-Authentic = RADIUS
Tunnel-Server-Endpoint = "csunix"
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 84
Acct-Input-Octets = 208
Acct-Output-Octets = 104
Acct-Input-Packets = 2
Acct-Output-Packets = 1
```

## Debug – Good Authentication

Certain **show** commands are supported by the Output Interpreter Tool ( registered customers only) , which allows you to view an analysis of **show** command output.

## VPN 5000 Concentrator

**show sys log buffer** (CHAP authentication)

```
Notice 2422.30 seconds New IKE connection:
  [181.44.17.149]:1072:csunixuser
Debug 2422.32 seconds Sending RADIUS CHAP challenge to csunixuser
  at 181.44.17.149
Debug 2427.30 seconds Received RADIUS challenge resp. from csunixuser
  at 181.44.17.149, contacting server
Notice 2427.54 seconds VPN 0 opened for csunixuser from 181.44.17.149.
Debug 2427.56 seconds Client's local broadcast address = 181.44.17.255
Notice 2427.59 seconds User assigned IP address 172.18.124.243
```

**vpn trace dump all**

```
VPN5001_A5F0C900#vpn trace dump all
6 seconds -- stepmngtr trace enabled --
new script: ISAKMP primary responder script for (start)
manage @ 2422 seconds :: [181.44.17.149]:1072 (start)
2422 seconds doing irpri_new_conn, (0 @ 0)
2422 seconds doing irpri_pkt_1_recd, (0 @ 0)
new script: ISAKMP Resp Aggr Shared Secret script
  for [181.44.17.149]:1072 (start)
2422 seconds doing irsass_process_pkt_1, (0 @ 0)
2422 seconds doing irsass_build_rad_pkt, (0 @ 0)
2422 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 2422 seconds :: [181.44.17.149]:1072 (done)
manage @ 2424 seconds :: [181.44.17.149]:1072:csunixuser (start)
2424 seconds doing irsass_radius_wait, (0 @ 0)
2424 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 2424 seconds :: [181.44.17.149]:1072:csunixuser (done)
manage @ 2426 seconds :: [181.44.17.149]:1072:csunixuser (start)
2426 seconds doing irsass_radius_wait, (0 @ 0)
2426 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 2426 seconds :: [181.44.17.149]:1072:csunixuser (done)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (start)
2427 seconds doing irsass_radius_wait, (0 @ 0)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (done)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (start)
2427 seconds doing irsass_rad_serv_wait, (0 @ 0)
2427 seconds doing irsass_build_pkt_2, (0 @ 0)
2427 seconds doing irsass_send_pkt_2, (0 @ 0)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (done)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (start)
2427 seconds doing irsass_check_timeout, (0 @ 0)
2427 seconds doing irsass_check_hash, (0 @ 0)
2427 seconds doing irsass_last_op, (0 @ 0)
end script: ISAKMP Resp Aggr Shared Secret script
  for [181.44.17.149]:1072:csunixuser, (0 @ 0)
next script: ISAKMP primary responder script
  for [181.44.17.149]:1072:csunixuser, (0 @ 0)
2427 seconds doing irpri_phase1_done, (0 @ 0)
2427 seconds doing irpri_phase1_done, (0 @ 0)
2427 seconds doing irpri_start_phase2, (0 @ 0)
new script: phase 2 initiator
  for [181.44.17.149]:1072:csunixuser (start)
2427 seconds doing iph2_init, (0 @ 0)
2427 seconds doing iph2_build_pkt_1, (0 @ 0)
2427 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (done)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (start)
2427 seconds doing iph2_pkt_2_wait, (0 @ 0)
2427 seconds doing ihp2_process_pkt_2, (0 @ 0)
2427 seconds doing iph2_build_pkt_3, (0 @ 0)
2427 seconds doing iph2_config_SAs, (0 @ 0)
2427 seconds doing iph2_send_pkt_3, (0 @ 0)
2427 seconds doing iph2_last_op, (0 @ 0)
end script: phase 2 initiator for
  [181.44.17.149]:1072:csunixuser, (0 @ 0)
next script: ISAKMP primary responder script
  for [181.44.17.149]:1072:csunixuser, (0 @ 0)
2427 seconds doing irpri_open_tunnel, (0 @ 0)
2427 seconds doing irpri_start_i_maint, (0 @ 0)
new script: initiator maintenance for
  [181.44.17.149]:1072:csunixuser (start)
2427 seconds doing imnt_init, (0 @ 0)
manage @ 2427 seconds :: [181.44.17.149]:1072:csunixuser (done)
manage @ 2457 seconds :: [181.44.17.149]:1072:csunixuser (start)
2457 seconds doing imnt_maintenance, (0 @ 0)
2457 seconds doing imnt_maint_inform, (0 @ 0)
2457 seconds doing imnt_last_op, (0 @ 0)
```

```
end script: initiator maintenance for
  [181.44.17.149]:1072:csunixuser, (0 @ 0)
next script: ISAKMP primary responder script
  for [181.44.17.149]:1072:
csunixuser, (0 @ 0)
2457 seconds doing irpri_report_err, (0 @ 0)
2457 seconds doing irpri_last_op, (0 @ 0)
end script: ISAKMP primary responder script
  for [181.44.17.149]:1072:csunixuser, (0 @ 0)
next script: for [181.44.17.149]:1072:csunixuser, (0 @ 0)
manage @ 2457 seconds :: [181.44.17.149]:1072:csunixuser (done)
new script: ISAKMP primary responder script for (start)
manage @ 2485 seconds :: [181.44.17.149]:1073 (start)
2485 seconds doing irpri_new_conn, (0 @ 0)
2485 seconds doing irpri_pkt_1_recvd, (0 @ 0)
new script: ISAKMP Resp Aggr Shared Secret script
  for [181.44.17.149]:1073 (start)
2485 seconds doing irsass_process_pkt_1, (0 @ 0)
2485 seconds doing irsass_build_rad_pkt, (0 @ 0)
2485 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 2485 seconds :: [181.44.17.149]:1073 (done)
manage @ 2487 seconds :: [181.44.17.149]:1073:csunixuser (start)
2487 seconds doing irsass_radius_wait, (0 @ 0)
2487 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 2487 seconds :: [181.44.17.149]:1073:csunixuser (done)
manage @ 2489 seconds :: [181.44.17.149]:1073:csunixuser (start)
2489 seconds doing irsass_radius_wait, (0 @ 0)
2489 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 2489 seconds :: [181.44.17.149]:1073:csunixuser (done)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (start)
2492 seconds doing irsass_radius_wait, (0 @ 0)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (done)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (start)
2492 seconds doing irsass_rad_serv_wait, (0 @ 0)
2492 seconds doing irsass_build_pkt_2, (0 @ 0)
2492 seconds doing irsass_send_pkt_2, (0 @ 0)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (done)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (start)
2492 seconds doing irsass_check_timeout, (0 @ 0)
2492 seconds doing irsass_check_hash, (0 @ 0)
2492 seconds doing irsass_last_op, (0 @ 0)
end script: ISAKMP Resp Aggr Shared Secret script
  for [181.44.17.149]:1073:csunixuser, (0 @ 0)
next script: ISAKMP primary responder script for [181.44.17.149]:
1073:csunixuser, (0 @ 0)
2492 seconds doing irpri_phase1_done, (0 @ 0)
2492 seconds doing irpri_phase1_done, (0 @ 0)
2492 seconds doing irpri_start_phase2, (0 @ 0)
new script: phase 2 initiator for
  [181.44.17.149]:1073:csunixuser (start)
2492 seconds doing iph2_init, (0 @ 0)
2492 seconds doing iph2_build_pkt_1, (0 @ 0)
2492 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (done)
manage @ 2492 seconds :: [181.44.17.149]:1073:csunixuser (start)
2492 seconds doing iph2_pkt_2_wait, (0 @ 0)
2492 seconds doing ihp2_process_pkt_2, (0 @ 0)
2492 seconds doing iph2_build_pkt_3, (0 @ 0)
2492 seconds doing iph2_config_SAs, (0 @ 0)
2492 seconds doing iph2_send_pkt_3, (0 @ 0)
2492 seconds doing iph2_last_op, (0 @ 0)
end script: phase 2 initiator for [181.44.17.149]:1073:
csunixuser, (0 @ 0)
next script: ISAKMP primary responder script
  for [181.44.17.149]:1073:csunixuser, (0 @ 0)
2492 seconds doing irpri_open_tunnel, (0 @ 0)
```

VPN5001\_A5F0C900#

## Cisco Secure UNIX

```
CiscoSecure DEBUG - RADIUS ; Request from host ac127c99 nas
(172.18.124.153) coe=1 id=1 length=69
CiscoSecure DEBUG - RADIUS ; Incoming Packet id=1 (172.18.124.153)
NAS-IP-Address = 172.18.124.153
NAS-Port-Type = Virtual
NAS-Port = 268435456
Username = "csunixuser"
CHAP-Password = "\254E\227A\347\026\302MvJ\013\206>\214IVT"
CiscoSecure DEBUG - RADIUS ; Authenticate (172.18.124.153)
CiscoSecure DEBUG - RADIUS ; User PASSWORD type is Normal
CiscoSecure DEBUG - RADIUS ; authChapPwd (172.18.124.153)
CiscoSecure DEBUG - RADIUS ; Sending Ack of id 1 to ac127c99
(172.18.124.153)
CiscoSecure DEBUG - RADIUS ; Outgoing Accept Packet id=1
(172.18.124.153)
Tunnel-Client-Endpoint = "grouppass"
Tunnel-Server-Endpoint = "csunix"
```

## What Can Go Wrong

**Note:** Before issuing **debug** commands, refer to Important Information on Debug Commands.

## Cisco Secure UNIX Server Unreachable

### VPN 5000 Concentrator Debug

```
Oct 31 15:11:07 [172.18.124.153.2.2] New IKE connection:
[181.44.17.149]:1025:csunixuser
Oct 31 15:11:07 [172.18.124.153.2.2] Sending RADIUS CHAP
challenge to csunixuser at 181.44.17.149
Oct 31 15:11:18 [172.18.124.153.2.2] Received RADIUS challenge
resp. from csunixuser at 181.44.17.149, contacting server
Oct 31 15:12:17 [172.18.124.153.2.2] (csunixuser) reset:
RADIUS server never responded.
```

What the user sees:

```
VPN Server Error (14) User Access Denied
```

## Authentication Fails

The username or password on Cisco Secure UNIX is bad.

### VPN 5000 Concentrator Debug

```
Oct 31 15:14:45 [172.18.124.153.2.2] New IKE connection:
[181.44.17.149]:1027:csunixuser
Oct 31 15:14:45 [172.18.124.153.2.2] Sending RADIUS CHAP challenge
to csunixuser at 181.44.17.149
Oct 31 15:14:48 [172.18.124.153.2.2] Received RADIUS challenge resp.
from csunixuser at 181.44.17.149, contacting server
Oct 31 15:14:48 [172.18.124.153.2.2] Auth request for csunixuser
rejected by RADIUS server
Oct 31 15:14:49 [172.18.124.153.2.2] (csunixuser) reset
due to RADIUS authentication failure.
```

What the user sees:

```
VPN Server Error (14) User Access Denied
```

## VPNgroup Password Entered by User Does Not Agree with VPNPassword

In this example, attribute 66= VPNPassword.

### VPN 5000 Concentrator Debug

```
Oct 31 15:17:01 [172.18.124.153.2.2] New IKE connection:
[181.44.17.149]:1029:csunixuser
Oct 31 15:17:01 [172.18.124.153.2.2] Sending RADIUS CHAP challenge
to csunixuser at 181.44.17.149
Oct 31 15:17:05 [172.18.124.153.2.2] Received RADIUS challenge resp.
from csunixuser at 181.44.17.149, contacting server
```

The Cisco Secure log shows access=accept, but the VPN 5000 Concentrator log stops there.

What the user sees:

```
IKE ERROR: Authentication Failed.
```

## Group Name Sent Down by the RADIUS Server Does Not Exist on the VPN 5000 Concentrator

### VPN 5000 Concentrator Debug

```
Oct 31 15:22:10 [172.18.124.153.2.2] New IKE connection:
[181.44.17.149]:1032:csunixuser
Oct 31 15:22:10 [172.18.124.153.2.2] Sending RADIUS CHAP challenge
to csunixuser at 181.44.17.149
Oct 31 15:22:14 [172.18.124.153.2.2] Received RADIUS challenge resp.
from csunixuser at 181.44.17.149, contacting server
Oct 31 15:22:14 [172.18.124.153.2.2] User, "csunixuser", has an invalid
VPN Group config, "no_group_there"
Oct 31 15:22:14 [172.18.124.153.2.2] (csunixuser) reset:
connection script finished.
Oct 31 15:22:14 [172.18.124.153.2.2] -- reason: S_NO_POLICY (220@772)
```

The Cisco Secure log shows access=accept, but the VPN 5000 Concentrator log shows a problem.

What the user sees:

```
VPN Server Error (6): Bad user configuration on IntraPort server.
```

## 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

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
  - [VPN 5000 Concentrator Documentation](#)
  - [Cisco VPN 5000 Concentrator Support Page](#)
  - [Cisco VPN 5000 Client Support Page](#)
  - [IPSec Support Page](#)
  - [Technical Support – Cisco Systems](#)
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: May 02, 2008

Document ID: 10132

---