How to Authenticate VPN 5000 Client to the VPN 5000 Concentrator with Cisco Secure NT 2.5 and Later (RADIUS)

Document ID: 10133

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the End−of−Sales Announcement.

Contents

Introduction

Cisco Secure NT (CSNT) 2.5 and later (RADIUS) is capable of returning Virtual Private Network (VPN) 5000 vendor−specific attributes for VPN GroupInfo and VPN Password to authenticate a VPN 5000 Client to the VPN 5000 Concentrator. The following document assumes that local authentication is working before adding RADIUS authentication (hence our user, "localuser," in group "ciscolocal"). Then authentication is added to CSNT RADIUS for users not existing in the local database (user "csntuser" is assigned to group "csntgroup" by virtue of the attributes returned from the CSNT RADIUS server).

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 NT 2.5
- Cisco VPN 5000 Concentrator 5.2.16.0005
- Cisco 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.

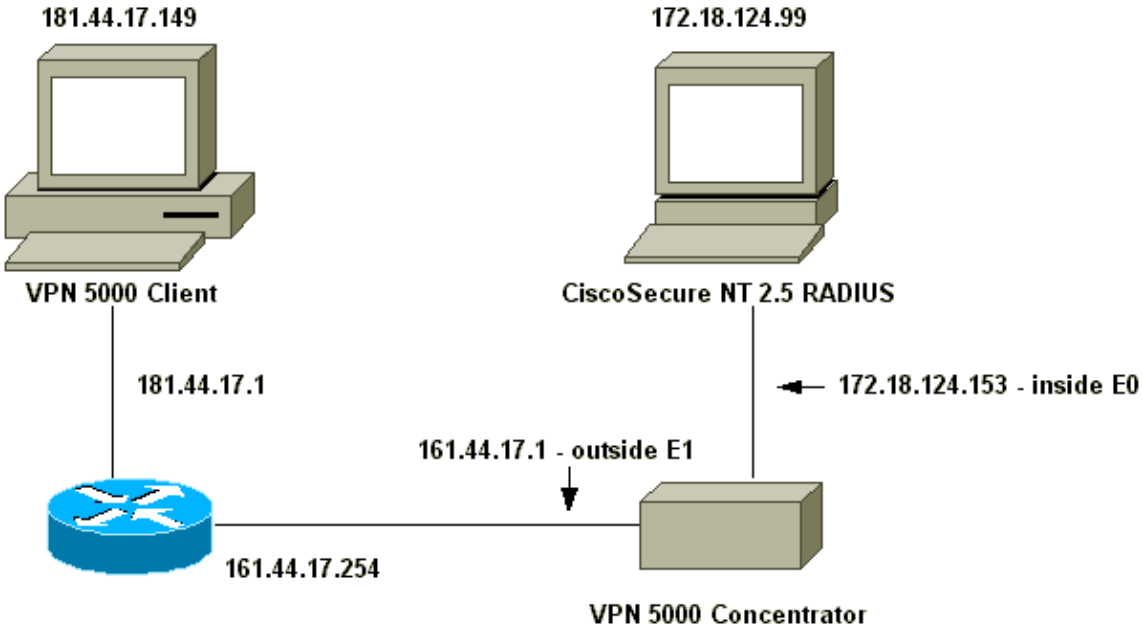
Configure

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

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="localike"

[ Radius ]
Accounting               = Off
PrimAddress              = "172.18.124.99"
Secret                   = "csntkey"
ChallengeType            = CHAP
BindTo                   = "ethernet0"
Authentication           = On

[ VPN Group "csnt" ]
BindTo                   = "ethernet0"
Transform                = ESP(md5,Des)
MaxConnections           = 2
IPNet                    = 172.18.124.0/24
StartIPAddress           = 172.18.124.245

AssignIPRADIUS           = Off
BindTo                   = "ethernet0"
StartIPAddress           = 172.18.124.243
IPNet                    = 172.18.124./24
StartIPAddress           = 172.18.124.242
Transform                = ESP(md5,Des)
BindTo                   = "ethernet0"
MaxConnections           = 1

[ VPN Group "csntgroup" ]
MaxConnections           = 2
StartIPAddress           = 172.18.124.242
```

```
BindTo                    = "ethernet0"
Transform                 = ESP(md5,Des)
IPNet                     = 172.18.124.0/24

Configuration size is 2045 out of 65500 bytes.
```

VPN 5000 Client

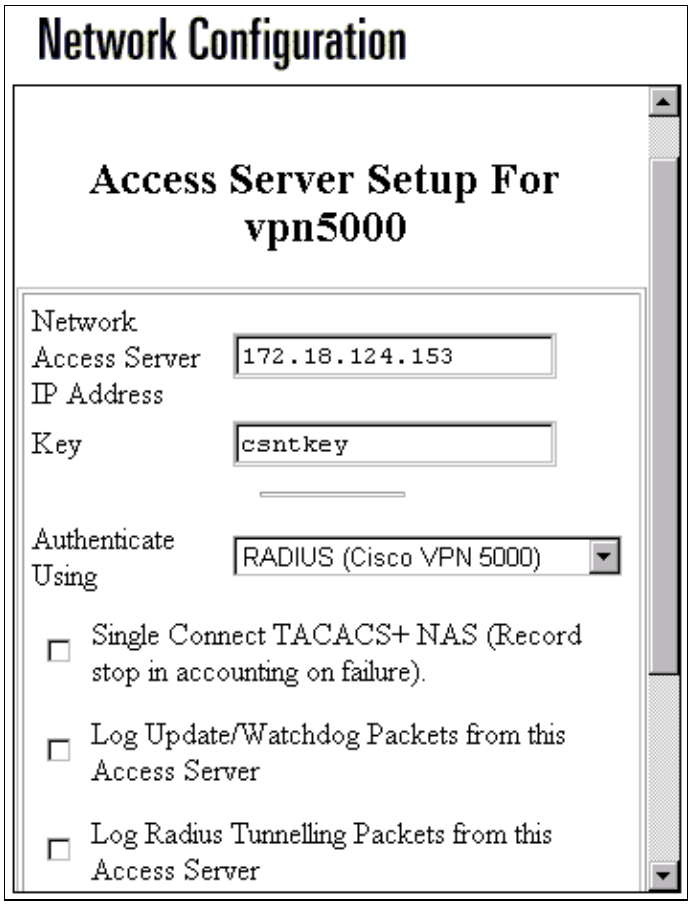
Note: None of the defaults have been changed. Two users were added, and the appropriate passwords were entered when prompted after clicking Connect:

username	password	radius_password
localuser	localike	N/A
csntuser	grouppass	csntpass

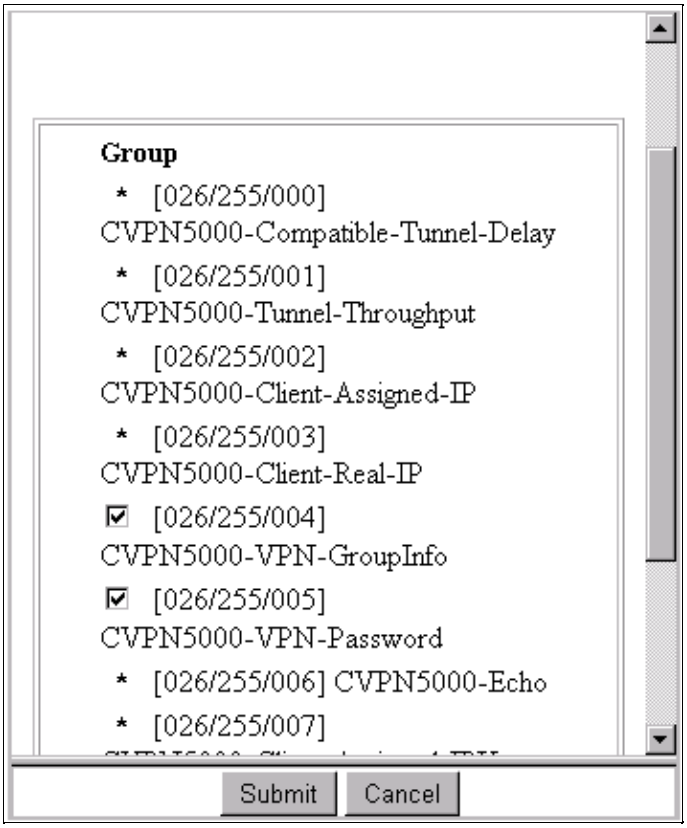
Cisco Secure NT 2.5 Configuration

Follow this procedure.

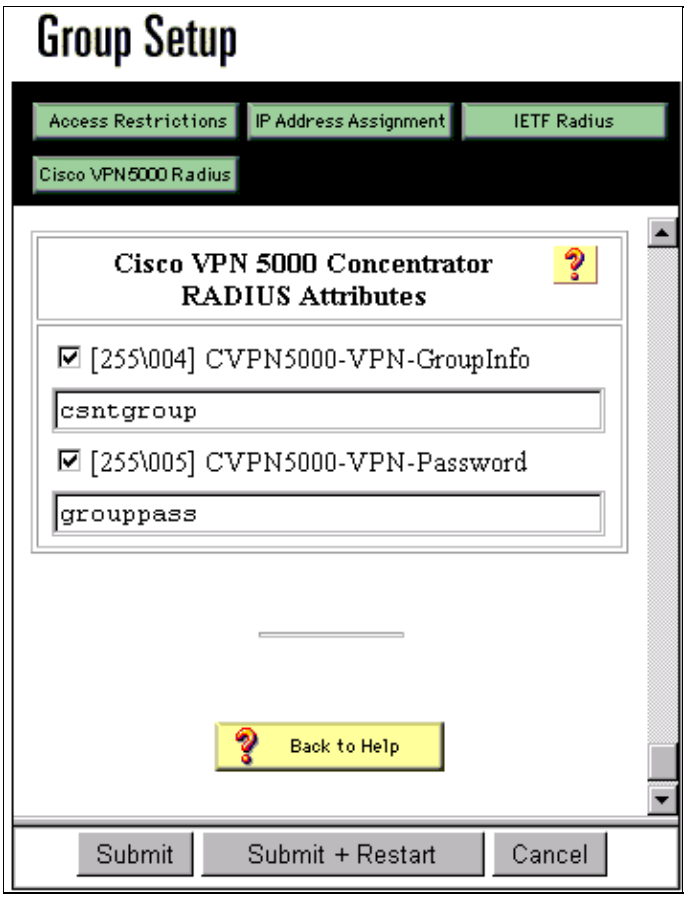
1. Configure the server to speak to the Concentrator:



2. Go to **Interface Configuration** > **RADIUS (VPN 5000)** and check VPN GroupInfo and VPN Password:



3. After configuring the user ("csntuser") with a password ("csntpass") in the User Setup and putting the user in Group 13, configure the VPN 5000 attributes in **Group Setup | Group 13**:



Changing to PAP Authentication

Assuming Challenge Handshake Authentication Protocol (CHAP) authentication works, you may wish to change to Password Authentication Protocol (PAP), which enables you to have CSNT use the user's password from the NT database.

VPN 5000 RADIUS Profile Change

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

Note: CSNT would also be configured to use the NT database for that user's authentication.

What the user sees (three password boxes):

```
Shared Secret = grouppass
RADIUS Login box − Password = csntpass
RADIUS Login box − Authentication Secret = abcxyz
```

Adding IP Address Assignment

If the user's CSNT profile is set in "Assign static IP Address" to a particular value, and if the VPN 5000 Concentrator group is set for:

```
AssignIPRADIUS = On
```

Then, the RADIUS IP Address is sent down from CSNT and applied to the user on the VPN 5000 Concentrator.

Adding Accounting

If you want session accounting records sent to the Cisco Secure RADIUS server, then add to the VPN 5000 Concentrator RADIUS configuration:

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

You must use the **apply** and **write** commands, and then the **boot** command on the VPN 5000 for this change to take effect.

Accounting Records From CSNT

```
11/06/2000,16:02:45,csntuser,Group 13,,Start,077745c5−00000000,,,,,,,,,
   268435456,172.18.124.153
11/06/2000,16:03:05,csntuser,Group 13,,Stop,077745c5−00000000,20,,,
   104,0,1,0,,268435456,172.18.124.153
```

Verify

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

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

- **show system log buffer**

```
Info 7701.12 seconds Command loop started from 172.18.124.99
on PTY1

Notice 7723.36 seconds New IKE connection: [181.44.17.149]:1041:csntuser
Debug 7723.38 seconds Sending RADIUS CHAP challenge to
   csntuser at 181.44.17.149
Debug 7729.0 seconds Received RADIUS challenge resp. from
   csntuser at 181.44.17.149, contacting server
Notice 7729.24 seconds VPN 0 opened for csntuser from 181.44.17.149.
Debug 7729.26 seconds Client's local broadcast address = 181.44.17.255
Notice 7729.29 seconds User assigned IP address 172.18.124.242
```

- **vpn trace dump all**

```
VPN5001_A5F0C900# vpn trace dump all
         6 seconds -- stepmngr trace enabled --
   new script: ISAKMP primary responder script for <no id> (start)
manage @ 91 seconds :: [181.44.17.149]:1042 (start)
         91 seconds doing irpri_new_conn, (0 @ 0)
         91 seconds doing irpri_pkt_1_recd, (0 @ 0)
   new script: ISAKMP Resp Aggr Shared Secret script for
      [181.44.17.149]:1042 (start)
         91 seconds doing irsass_process_pkt_1, (0 @ 0)
         91 seconds doing irsass_build_rad_pkt, (0 @ 0)
         91 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 91 seconds :: [181.44.17.149]:1042 (done)
manage @ 93 seconds :: [181.44.17.149]:1042:csntuser (start)
         93 seconds doing irsass_radius_wait, (0 @ 0)
         93 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 93 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
         95 seconds doing irsass_radius_wait, (0 @ 0)
         95 seconds doing irsass_send_rad_pkt, (0 @ 0)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
         95 seconds doing irsass_radius_wait, (0 @ 0)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 95 seconds :: [181.44.17.149]:1042:csntuser (start)
         95 seconds doing irsass_rad_serv_wait, (0 @ 0)
         95 seconds doing irsass_build_pkt_2, (0 @ 0)
         96 seconds doing irsass_send_pkt_2, (0 @ 0)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (start)
         96 seconds doing irsass_check_timeout, (0 @ 0)
         96 seconds doing irsass_check_hash, (0 @ 0)
         96 seconds doing irsass_last_op, (0 @ 0)
   end script: ISAKMP Resp Aggr Shared Secret script for
      [181.44.17.149]:1042:csntuser, (0 @ 0)
   next script: ISAKMP primary responder script for
      [181.44.17.149]:1042:csntuser, (0 @ 0)
         96 seconds doing irpri_phase1_done, (0 @ 0)
         96 seconds doing irpri_phase1_done, (0 @ 0)
         96 seconds doing irpri_start_phase2, (0 @ 0)
   new script: phase 2 initiator for [181.44.17.149]:1042:csntuser (start)
         96 seconds doing iph2_init, (0 @ 0)
         96 seconds doing iph2_build_pkt_1, (0 @ 0)
         96 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (start)
         96 seconds doing iph2_pkt_2_wait, (0 @ 0)
         96 seconds doing ihp2_process_pkt_2, (0 @ 0)
         96 seconds doing iph2_build_pkt_3, (0 @ 0)
         96 seconds doing iph2_config_SAs, (0 @ 0)
         96 seconds doing iph2_send_pkt_3, (0 @ 0)
```

```
            96 seconds doing iph2_last_op, (0 @ 0)
      end script: phase 2 initiator for [181.44.17.149]:1042:csntuser, (0 @ 0)
      next script: ISAKMP primary responder script for
         [181.44.17.149]:1042:csntuser, (0 @ 0)
            96 seconds doing irpri_open_tunnel, (0 @ 0)
            96 seconds doing irpri_start_i_maint, (0 @ 0)
      new script: initiator maintenance for [181.44.17.149]:1042:csntuser (start)
            96 seconds doing imnt_init, (0 @ 0)
   manage @ 96 seconds :: [181.44.17.149]:1042:csntuser (done)
   <vpn trace dump done, 55 records scanned>
```

Troubleshoot

The following are possible errors you may encounter.

Cisco Secure NT Server is Unreachable

VPN 5000 Debug

```
Notice 359.36 seconds New IKE connection: [181.44.17.149]:1044:csntuser
Debug 359.38 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 363.18 seconds Received RADIUS challenge resp. From
   csntuser at 181.44.17.149, contacting server
Notice 423.54 seconds <no ifp> (csntuser) 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 NT is bad.

VPN 5000 Debug

```
Notice 506.42 seconds New IKE connection: [181.44.17.149]:1045:csntuser
Debug 506.44 seconds Sending RADIUS CHAP challenge to csntuser
   at 181.44.17.149
Debug 511.24 seconds Received RADIUS challenge resp. From csntuser
  at 181.44.17.149, contacting server
Debug 511.28 seconds Auth request for csntuser rejected by RADIUS server
Notice 511.31 seconds <no ifp> (csntuser) reset due to RADIUS authentication
failure.
```

What the user sees:

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

Cisco Secure:

Go to **Reports** and **Activity**, and the failed attempts log shows the failure.

VPN Group Password Entered by User Does Not Agree With VPNPassword

VPN 5000 Debug

```
Notice 545.0 seconds New IKE connection: [181.44.17.149]:1046:csntuser
Debug 545.6 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 550.6 seconds Received RADIUS challenge resp. From csntuser at 181.44.17.149,
contacting server
```

What the user sees:

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

Cisco Secure:

Go to **Reports** and **Activity**, and the failed attempts log does not show the failure.

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

VPN 5000 Debug

```
Notice 656.18 seconds New IKE connection: [181.44.17.149]:1047:csntuser
Debug 656.24 seconds Sending RADIUS CHAP challenge to csntuser at 181.44.17.149
Debug 660.12 seconds Received RADIUS challenge resp. From csntuser at 181.44.17.149,
contacting server
Warnin 660.16 seconds User, "csntuser", has an invalid VPN Group config, "junkgroup"
Notice 660.20 seconds  (csntuser) reset: connection script finished.
Notice 660.23 seconds -- reason: S_NO_POLICY (220@772)
```

What the user sees:

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

Cisco Secure:

Go to **Reports** and **Activity**, and the failed attempts log does *not* show the failure.

Related Information

- **Cisco Secure ACS for Windows Support Page**
- **Cisco VPN 5000 Series Concentrators End−of−Sales Announcement**
- **Cisco VPN 5000 Concentrator Support Page**
- **Cisco VPN 5000 Client Support Page**
- **IPsec Support Page**
- **RADIUS Support Page**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map
© 2014 − 2015 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

Updated: Apr 04, 2008 Document ID: 10133