

Configuring the Cisco VPN Client to the VPN 3000 Concentrator with Microsoft Windows NT Domain Authentication

Document ID: 14110

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure the VPN 3000 Concentrator

- Tasks Performed
- Network Diagram
- Step-by-Step Instructions
- Configure Authentication Server on a Per-Group Basis

Verify

Troubleshoot

- Good Debug – VPN 3000 Concentrator to NT
- Bad Debug – VPN 3000 Concentrator to NT

Related Information

Introduction

This document demonstrates how to configure the Cisco VPN 3000 Concentrator to authenticate Cisco VPN Clients to an external Microsoft Windows NT domain server. If multiple NT domain servers are specified, the first server listed is the primary server. The rest are backup servers in the event the primary server is inoperative after a configurable number of retries (0–10) and seconds (1–30). Set up a trust relationship in NT, with one NT domain server listed in the VPN 3000 to have authentication to multiple NT domains. All requests go to the single NT domain server, which forwards the request to the appropriate trusted primary domain controller (PDC) in the specified domain.

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 VPN 3000 Concentrator 2.5.2 and later
- Windows NT server 4.0

Note: This example from the lab shows the authentication PDCs outside the VPN Concentrator. In an actual network environment, and for maximum security, the PDCs would be inside the VPN Concentrator.

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

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

Configure the VPN 3000 Concentrator

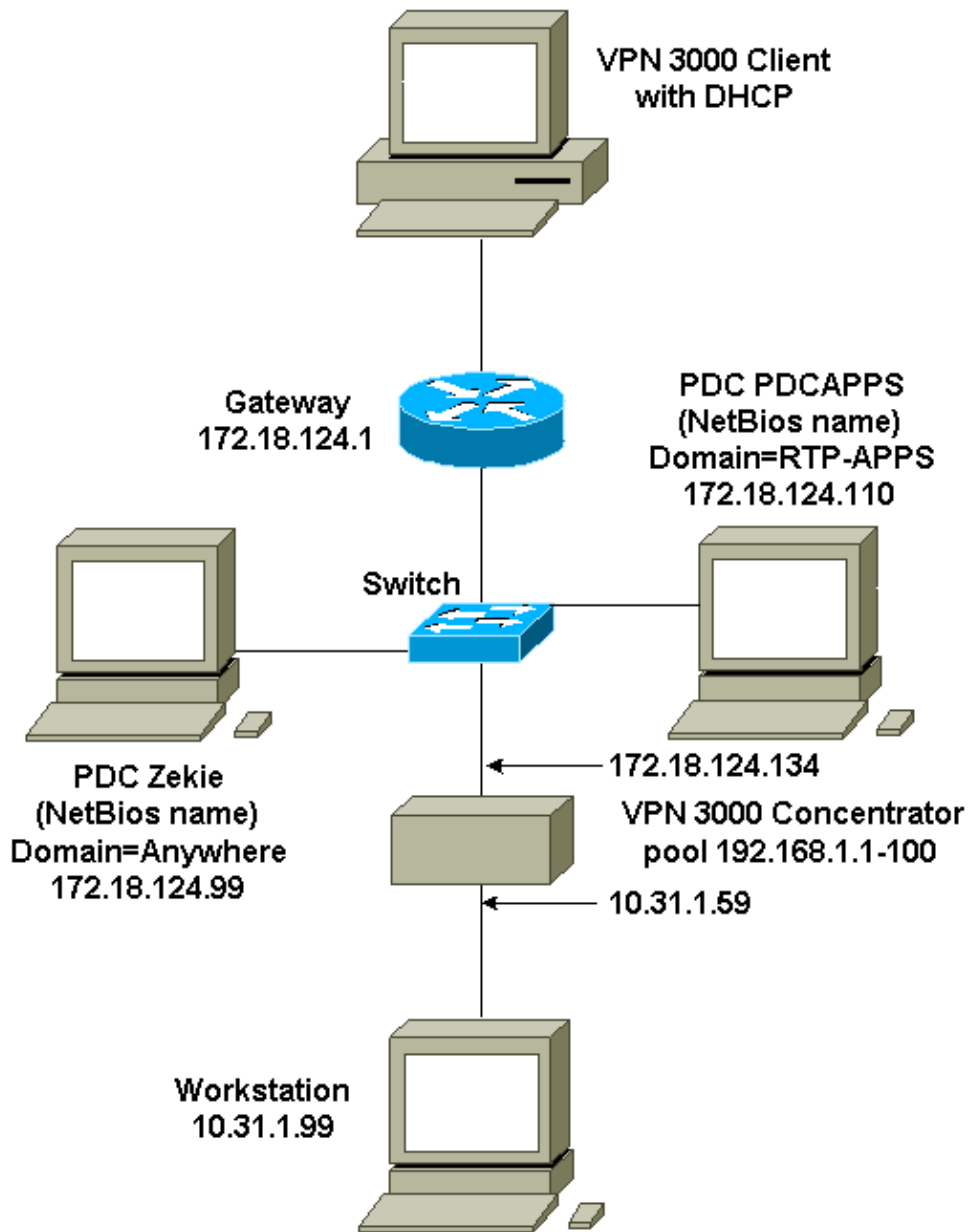
Tasks Performed

This section describes how to configure the VPN Concentrator to authenticate clients to an external Windows NT server.

1. Test with local authentication.
2. Add the Windows NT domain server to the VPN Concentrator.
3. Test the VPN Concentrator to the Windows NT domain server.
4. Change the group to point to the Windows NT domain server.
5. Test the VPN Client to the VPN 3000 Concentrator with Windows NT.

Network Diagram

This document uses the network setup shown in this diagram:



In this example:

- If both NT domain servers:

172.18.124.99 (ZEKIE=netbios name, domain=ANYWHERE)

172.18.124.110 (PDCAPPS=netbios name, domain=RTP-APPS)

are listed in the VPN 3000 Concentrator, requests go to 172.18.124.99 (ZEKIE); if 172.18.124.99 is unreachable, requests go to 172.18.124.110 (PDCAPPS).

- If only one NT domain server:

172.18.124.99 (ZEKIE=netbios name, domain=ANYWHERE)

is listed in the VPN 3000 Concentrator, but a trust relationship is set up in Windows NT, requests go to 172.18.124.99 (ZEKIE), which services user requests itself or forwards requests for other users to 172.18.124.110 (PDCAPPS).

Step-by-Step Instructions

Complete these steps:

1. Test to be sure that the VPN Client authentication and encryption to the internal VPN 3000 database works before you add authentication to a Windows NT domain server.
2. Add the NT domain server to the VPN 3000 Concentrator authentication server list. For a trust relationship, you might need to increase the timeout (the default is a 4-second timeout and two retries).

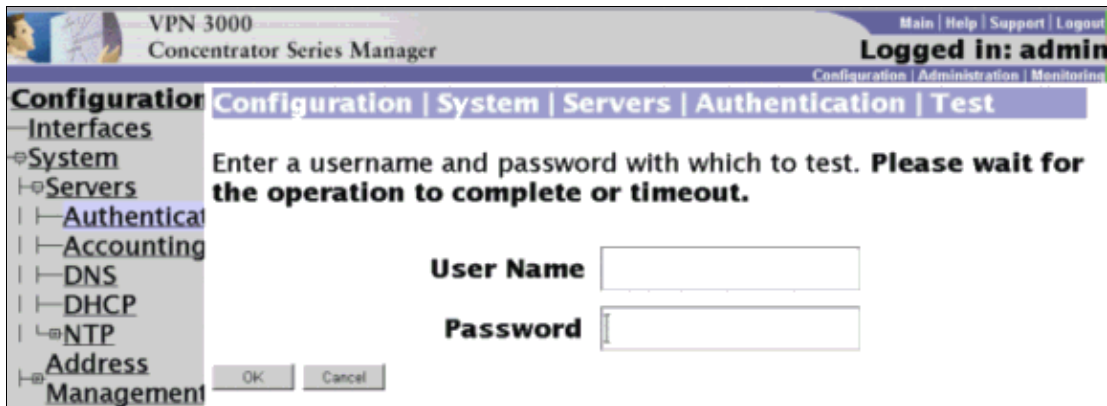
The screenshot shows the 'VPN 3000 Concentrator Series Manager' interface. The title bar includes 'Main | Help | Support | Logout' and 'Logged in: admin'. The main window title is 'Configure and add a user authentication server.' The left sidebar has 'Configuration' selected, with 'Administratic' and 'Monitoring' also visible. The 'Server Type' dropdown is set to 'NT Domain'. A note states: 'Selecting *Internal Server* will let you add users to the internal user database.' The 'Authentication Server Address' field contains '172.18.124.99'. The 'Server Port' field contains '0'. The 'Timeout' field contains '4'. The 'Retries' field contains '2'. The 'Domain Controller Name' field contains 'izekie'. On the right side, there are instructions: 'Enter the IP address.', 'Enter 0 for default port (139).', 'Enter the timeout for this server (seconds).', 'Enter the number of retries for this server.', and 'Enter the NT Primary Domain Controller name for this authentication server.' At the bottom, there are 'Add' and 'Cancel' buttons.

3. Test the NT domain server authentication from the VPN 3000 Concentrator. For example, we formed an NT trust relationship between 172.18.124.99 and 172.18.124.110 with one server listed. We tested authentication by entering:

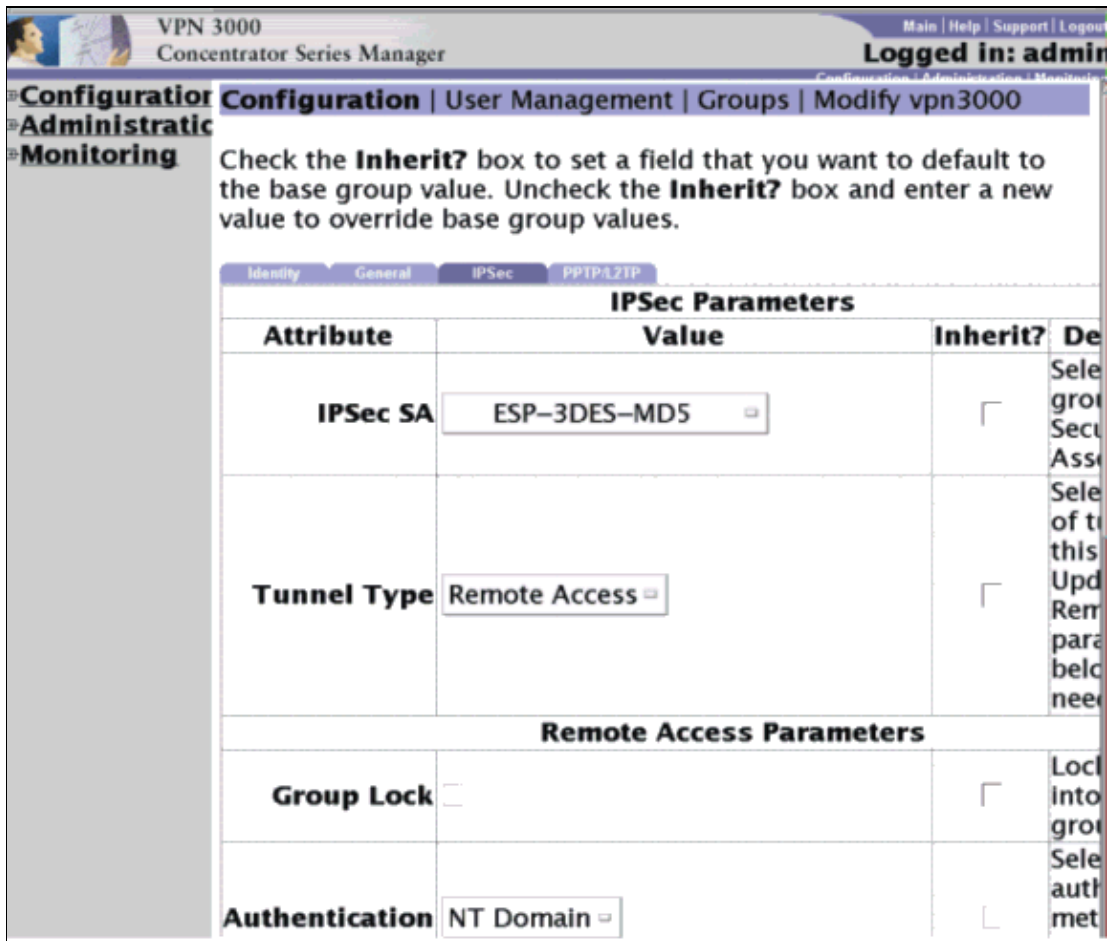
```
(user on 172.18.124.99)
  User Name: vpnuser
  Password: *****

  User Name: ANYWHERE\vpnuser
  Password: *****

(user on 172.18.124.110)
  User Name: RTP-APPS\appsuser
  Password: *****
```



4. Configure the VPN 3000 group to point to the NT domain for authentication.

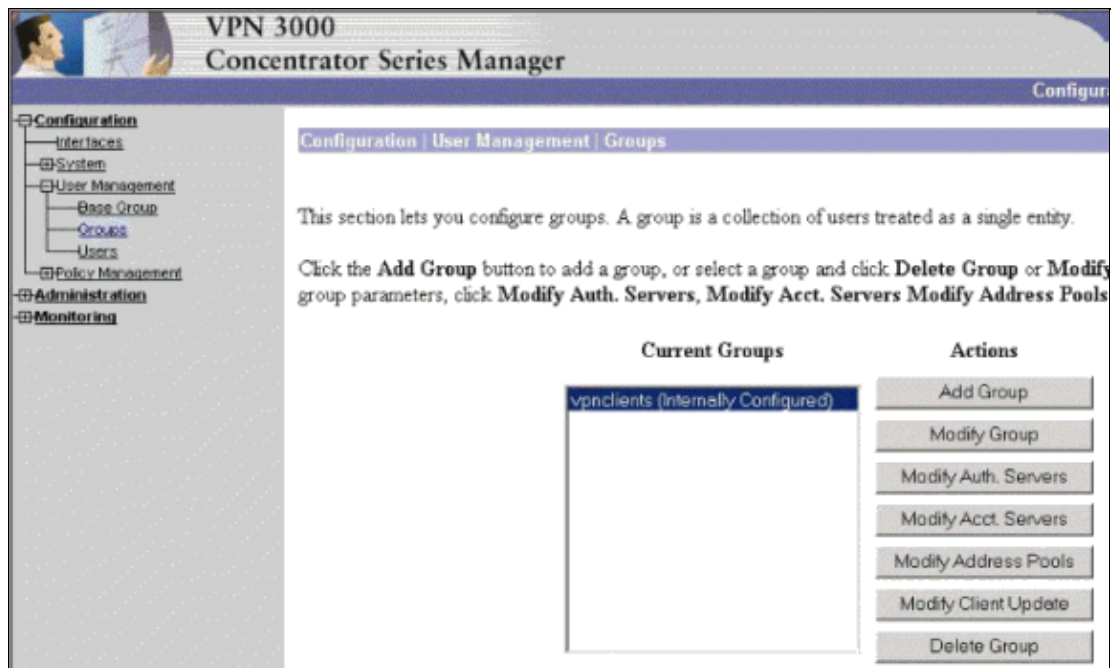


5. Test the VPN Client to the VPN 3000 Concentrator.

The VPN Client should be able to connect to the VPN 3000 Concentrator at this point. If there are problems, see the troubleshooting and debugging the configuration section.

Configure Authentication Server on a Per-Group Basis

On the Cisco VPN 3000 Concentrator versions 3.0 and later, it is possible to define the authentication server on a per-group basis (instead of defining it on a global basis for the whole VPN Concentrator). Select **Configuration > User Management > Groups** and click **Add Group**.



Verify

There is currently no verification procedure available for this document.

Troubleshoot

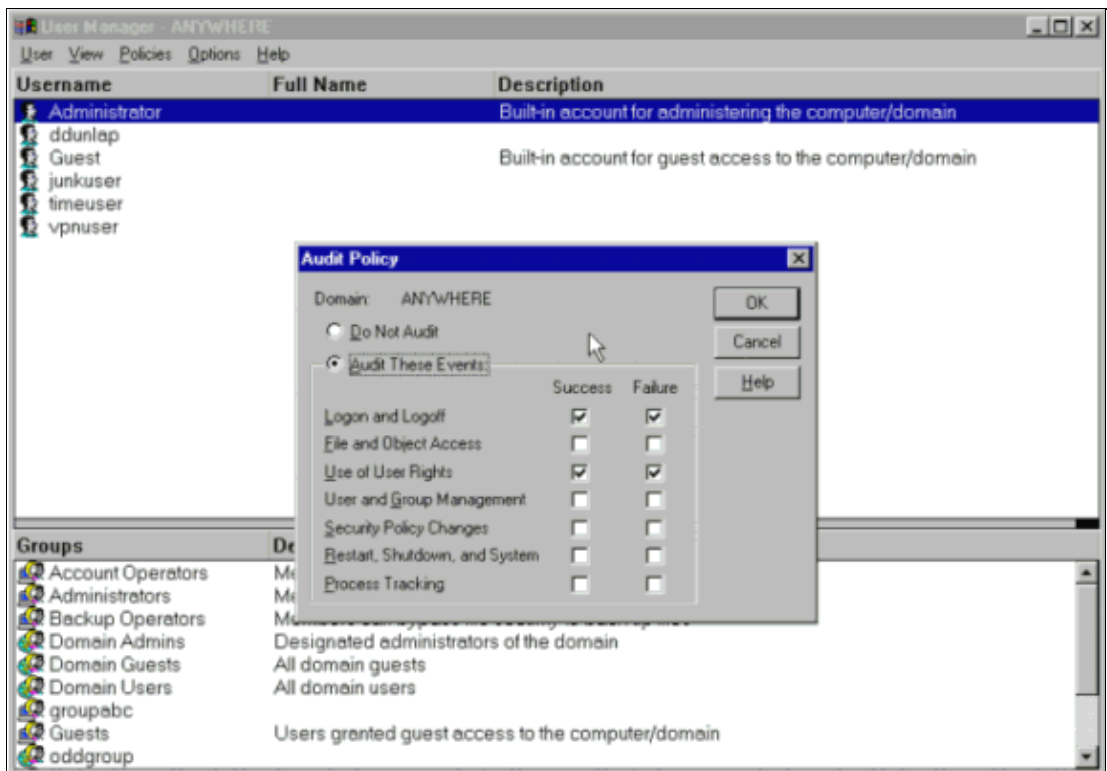
This section provides information that you can use to troubleshoot your configuration.

1. Select **Configuration > System > Events > Classes > Add** to turn on VPN 3000 Concentrator debugging. Include AUTH, AUTHDBG, AUTHDECODE with these settings.

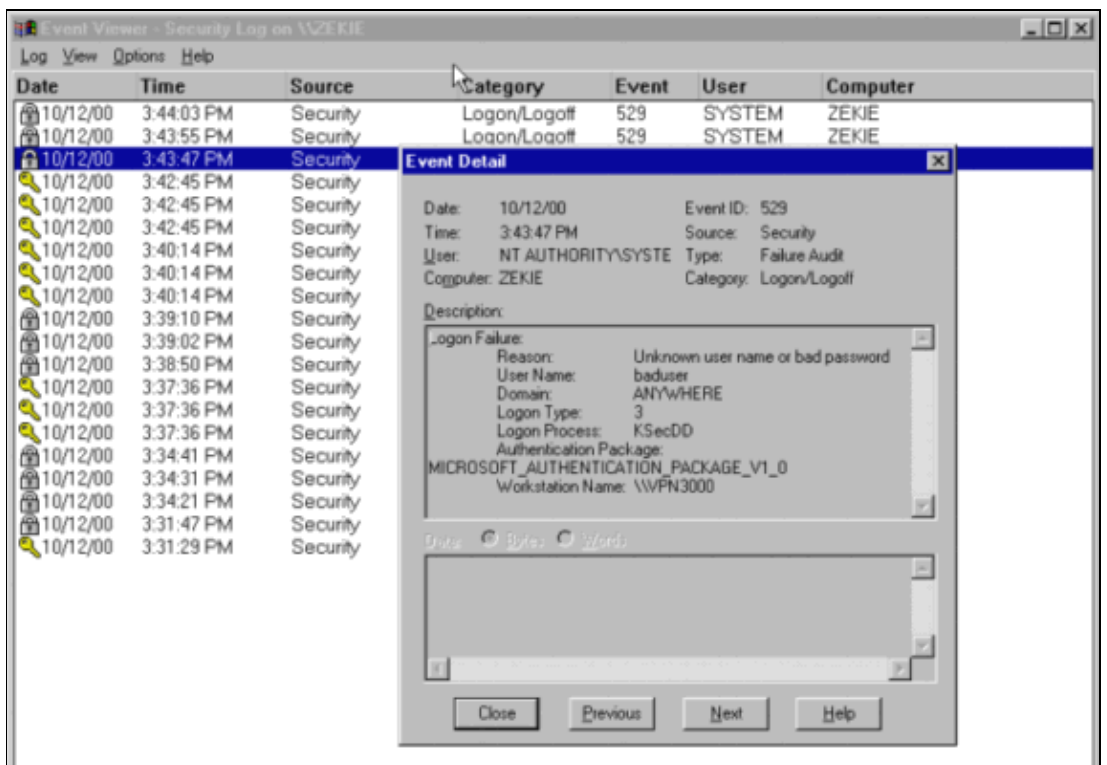
Severity to Log = 1–9

Severity to Console = 1–3

2. In Windows NT, enable the audit facility.



3. Select **Monitoring > Event Log** to examine the VPN 3000 Concentrator debug.
4. View successful and failed attempts for Windows NT.



Note: Be aware of one of the common errors for authentication failure for VPN users. The cause of the error can be due to the non-synchronization of the Clock between the VPN Concentrator and the AD server. Synchronize the time for authentication to work.

Good Debug – VPN 3000 Concentrator to NT

```
1 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/1 RPT=20
AUTH_Open() returns 62

2 10/12/2000 15:32:10.340 SEV=7 AUTH/12 RPT=20
Authentication session opened: handle = 62

3 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/3 RPT=29
AUTH_PutAttrTable(62, 5b6a3c)

4 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/5 RPT=14
AUTH_Authenticate(62, 5007b5c, 47540c)

5 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/59 RPT=29
AUTH_BindServer(71e3004, 0, 0)

6 10/12/2000 15:32:10.340 SEV=9 AUTHDBG/69 RPT=29
Auth Server 649ab4 has been bound to ACB 71e3004, sessions = 1

7 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/65 RPT=29
AUTH_CreateTimer(71e3004, 0, 0)

8 10/12/2000 15:32:10.340 SEV=9 AUTHDBG/72 RPT=29
Reply timer created: handle = AC0012

9 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/61 RPT=29
AUTH_BuildMsg(71e3004, 0, 0)

10 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/39 RPT=14
Smb_Build(71e3004)

11 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/77 RPT=14 161.44.17.135
SMB_Connect_Server(71e3004)

12 10/12/2000 15:32:10.340 SEV=8 AUTHDBG/91 RPT=14
RFCNB_Call(649ab4, ZEKIE, VPN 3000)

13 10/12/2000 15:32:10.350 SEV=7 AUTH/16 RPT=14
TCP session established: socket = 12, server = 172.18.124.99

14 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/92 RPT=14
RFCNB_Session_Req(649ab4, 2e7ea54, ZEKIE, VPN 3000)

15 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/93 RPT=46
RFCNB_Put_Pkt(2e7ea54, 2e79fb8, 72)

16 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/94 RPT=33
RFCNB_Get_Pkt(2e7ea54, fe36a0, 16)

17 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/89 RPT=14
SMB_Negotiate(71e3004)

18 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/93 RPT=47
RFCNB_Put_Pkt(2e7ea54, 2e7e414, 51)

19 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/94 RPT=34
RFCNB_Get_Pkt(2e7ea54, 2e7e414, 260)

20 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/79 RPT=14 161.44.17.135
SMB_Build_Request(71e3004)

21 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/64 RPT=29
AUTH_StartTimer(71e3004, 0, 0)

22 10/12/2000 15:32:10.350 SEV=9 AUTHDBG/73 RPT=29
```

Reply timer started: handle = AC0012, timestamp = 1650164, timeout = 4000

23 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/62 RPT=29
AUTH_SndRequest(71e3004, 0, 0)

24 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/43 RPT=27
Smb_Decode(2e79fb8, 0)

25 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/40 RPT=14 161.44.17.135
Smb_Xmt(71e3004)

26 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/80 RPT=14 161.44.17.135
SMB_Send_Request(71e3004)

27 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/93 RPT=48
RFCNB_Put_Pkt(2e7ea54, 2e7e414, 166)

28 10/12/2000 15:32:10.350 SEV=9 AUTHDBG/71 RPT=29
xmit_cnt = 1

29 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/63 RPT=29
AUTH_RcvReply(71e3004, 0, 0)

30 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/43 RPT=28
Smb_Decode(50076e0, 128)

31 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/41 RPT=14 161.44.17.135
Smb_Rcv(71e3004)

32 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/81 RPT=14 161.44.17.135
SMB_Receive_Reply(71e3004)

33 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/90 RPT=7
SMB_Logoff(71e3004, 4096)

34 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/93 RPT=49
RFCNB_Put_Pkt(2e7ea54, 2e7e9f0, 43)

35 10/12/2000 15:32:10.350 SEV=8 AUTHDBG/94 RPT=35
RFCNB_Get_Pkt(2e7ea54, 2e7e9f0, 43)

36 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/78 RPT=14 161.44.17.135
SMB_Disconnect_Server(71e3004)

37 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/66 RPT=29
AUTH_DeleteTimer(71e3004, 0, 0)

38 10/12/2000 15:32:10.360 SEV=9 AUTHDBG/74 RPT=29
Reply timer stopped: handle = AC0012, timestamp = 1650165

39 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/58 RPT=29
AUTH_Callback(71e3004, 0, 0)

40 10/12/2000 15:32:10.360 SEV=6 AUTH/4 RPT=22 161.44.17.135
Authentication successful: handle = 62, server = 172.18.124.99, user = vpnuser

41 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/3 RPT=30
AUTH_PutAttrTable(62, fe3764)

42 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/60 RPT=29
AUTH_UnbindServer(71e3004, 0, 0)

43 10/12/2000 15:32:10.360 SEV=9 AUTHDBG/70 RPT=29
Auth Server 649ab4 has been unbound from ACB 71e3004, sessions = 0

44 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/59 RPT=30

AUTH_BindServer(71e3004, 0, 0)

45 10/12/2000 15:32:10.360 SEV=9 AUTHDBG/69 RPT=30
Auth Server 6498bc has been bound to ACB 71e3004, sessions = 1

46 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/65 RPT=30
AUTH_CreateTimer(71e3004, 0, 0)

47 10/12/2000 15:32:10.360 SEV=9 AUTHDBG/72 RPT=30
Reply timer created: handle = AD0012

48 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/61 RPT=30
AUTH_BuildMsg(71e3004, 0, 0)

49 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/64 RPT=30
AUTH_StartTimer(71e3004, 0, 0)

50 10/12/2000 15:32:10.360 SEV=9 AUTHDBG/73 RPT=30
Reply timer started: handle = AD0012, timestamp = 1650165, timeout = 30000

51 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/62 RPT=30
AUTH_SndRequest(71e3004, 0, 0)

52 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/50 RPT=31
IntDB_Decode(2e79fb8, 41)

53 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/47 RPT=31
IntDB_Xmt(71e3004)

54 10/12/2000 15:32:10.360 SEV=9 AUTHDBG/71 RPT=30
xmit_cnt = 1

55 10/12/2000 15:32:10.360 SEV=8 AUTHDBG/47 RPT=32
IntDB_Xmt(71e3004)

56 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/49 RPT=16
IntDB_Match(71e3004, 50076e0)

57 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/63 RPT=30
AUTH_RcvReply(71e3004, 0, 0)

58 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/50 RPT=32
IntDB_Decode(50076e0, 98)

59 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/48 RPT=16
IntDB_Rcv(71e3004)

60 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/66 RPT=30
AUTH_DeleteTimer(71e3004, 0, 0)

61 10/12/2000 15:32:10.460 SEV=9 AUTHDBG/74 RPT=30
Reply timer stopped: handle = AD0012, timestamp = 1650175

62 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/58 RPT=30
AUTH_Callback(71e3004, 0, 0)

63 10/12/2000 15:32:10.460 SEV=6 AUTH/4 RPT=23 161.44.17.135
Authentication successful: handle = 62, server = Internal, user = vpn3000

64 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/4 RPT=16
AUTH_GetAttrTable(62, 5b6a84)

65 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/2 RPT=19
AUTH_Close(62)

66 10/12/2000 15:32:10.460 SEV=4 IKE/52 RPT=10 161.44.17.135

```

User [ ANYWHERE\vpnuser ]
User (ANYWHERE\vpnuser) authenticated.

67 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/60 RPT=30
AUTH_UnbindServer(71e3004, 0, 0)

68 10/12/2000 15:32:10.460 SEV=9 AUTHDBG/70 RPT=30
Auth Server 6498bc has been unbound from ACB 71e3004, sessions = 0

69 10/12/2000 15:32:10.460 SEV=8 AUTHDBG/10 RPT=19
AUTH_Int_FreeAuthCB(71e3004)

70 10/12/2000 15:32:10.460 SEV=9 AUTHDBG/19 RPT=19
instance = 63, clone_instance = 0

71 10/12/2000 15:32:10.460 SEV=7 AUTH/13 RPT=19
Authentication session closed: handle = 62

72 10/12/2000 15:32:10.470 SEV=4 AUTH/21 RPT=18
User ANYWHERE\vpnuser connected

73 10/12/2000 15:32:10.470 SEV=5 IKE/25 RPT=17 161.44.17.135
User [ ANYWHERE\vpnuser ]
Received remote Proxy Host data in ID Payload:
Address 161.44.17.135, Protocol 0, Port 0

76 10/12/2000 15:32:10.470 SEV=5 IKE/24 RPT=9 161.44.17.135
User [ ANYWHERE\vpnuser ]
Received local Proxy Host data in ID Payload:
Address 172.18.124.134, Protocol 0, Port 0

79 10/12/2000 15:32:10.470 SEV=5 IKE/66 RPT=17 161.44.17.135
User [ ANYWHERE\vpnuser ]
IKE Remote Peer configured for SA: ESP-3DES-MD5

80 10/12/2000 15:32:10.490 SEV=4 IKE/49 RPT=17 161.44.17.135
User [ ANYWHERE\vpnuser ]
Security negotiation complete for User (ANYWHERE\vpnuser)
Responder, Inbound SPI = 0x00686e15, Outbound SPI = 0x0a6587d9

```

Bad Debug – VPN 3000 Concentrator to NT

- Enter a bad username

```

73 10/12/2000 15:33:12.330 SEV=3 AUTH/5 RPT=13 161.44.17.135
Authentication rejected: Reason = Unspecified
handle = 64, server = 172.18.124.99, user = baduser

```

- Disconnect the PDC from the network

```

44 10/12/2000 15:35:01.370 SEV=2 AUTH/17 RPT=1
Unable to establish connection: server = 172.18.124.99

```

```

56 10/12/2000 15:35:01.370 SEV=4 AUTH/9 RPT=6 161.44.17.135
Authentication failed: Reason = No active server found
handle = 66, server = 172.18.124.99, user = vpnuser

```

Related Information

- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- IPSec Negotiation/IKE Protocols
- Technical Support & Documentation – Cisco Systems

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

Updated: Jul 05, 2006

Document ID: 14110
