

ASA 8.x: AnyConnect VPN Client Troubleshooting Tech Note

Document ID: 100597

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Troubleshooting Process

- Installation and Virtual Adapter Issues
- Disconnection or Inability to Establish Initial Connection
- Problems with Passing Traffic
- AnyConnect Crash Issues
- Fragmentation / Passing Traffic Issues
- Uninstall Automatically

AnyConnect: Corrupt Driver Database Issue

- Repair
- If Repair Fails
- Analyze the Database

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This troubleshooting scenario applies to applications that do not work through the Cisco AnyConnect VPN Client.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on ASA Security Appliance that runs version 8.x.

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 Cisco Technical Tips Conventions for more information on document conventions.

Troubleshooting Process

This typical troubleshooting scenario applies to applications that do not work through the Cisco AnyConnect VPN Client for end-users with Microsoft Windows-based computers. These sections address and provide solutions to the problems:

- Installation and Virtual Adapter Issues
- Disconnection or Inability to Establish Initial Connection
- Problems with Passing Traffic
- AnyConnect Crash Issues
- Fragmentation / Passing Traffic Issues

Installation and Virtual Adapter Issues

Complete these steps:

1. Obtain the device log file:

- ◆ Windows XP / Windows 2000:

```
\Windows\setupapi.log
```

- ◆ Windows Vista:

Note: Hidden folders must be made visible in order to see these files.

```
\Windows\Inf\setupapi.app.log  
\Windows\Inf\setupapi.dev.log
```

If you see errors in the setupapi log file, you can turn up verbosity to 0x2000FFFF as described in this Windows KB article . Note the article says to set it to 0xFFFF, but if you add the high order value of 0x2, it makes the logging faster.

2. Obtain the MSI installer log file:

If this is an initial web deploy install, this log is located in the per-user temp directory.

- ◆ Windows XP / Windows 2000:

```
\Documents and Settings\\Local Settings\Temp\
```

- ◆ Windows Vista:

```
\Users\\AppData\Local\Temp\
```

If this is an automatic upgrade, this log is in the temp directory of the system:

```
\Windows\Temp
```

The filename is in this format:

anyconnect-win-x.x.xxxx-k9-install-yyyyyyyyyyyyyy.log. Obtain the most recent file for the version of the client you want to install. The x.xxxx changes based on the version, such as 2.0.0343, and yyyy-yyyy-yyyy is the date and time of the install.

3. Obtain the PC system information file:

- a. From a Command Prompt/DOS box, type this:

- ◇ Windows XP / Windows 2000:

```
winmsd /nfo c:\msinfo.nfo
```

◇ Windows Vista:

```
msinfo32 /nfo c:\msinfo.nfo
```

Note: After you type this prompt, wait. It can take between two to five minutes for the file to complete.

b. Obtain a systeminfo file dump from a Command Prompt:

Windows XP and Windows Vista:

```
systeminfo c:\sysinfo.txt
```

See AnyConnect: Corrupt Driver Database Issue in order to debug the driver issue.

Disconnection or Inability to Establish Initial Connection

If you experience connection problems with the AnyConnect Client, such as disconnections or the inability to establish an initial connection, obtain these files:

- The configuration file from the ASA in order to determine if anything in the configuration causes the connection failure:

From the console of the ASA, type `write net x.x.x.x:ASA-Config.txt` where `x.x.x.x` is the IP address of a TFTP server on the network.

OR

From the console of the ASA, type `show running-config`. Let the configuration complete on the screen, then cut-and-paste into a text editor and save.

- The ASA event logs:
 1. In order to enable logging on the ASA for auth, webvpn, ssl, and svc events, issue these CLI commands:

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class svc console debugging
```
 2. Originate an Anyconnect session, and ensure that the failure can be reproduced. Capture the logging output from the console into a text editor and save.
 3. In order to disable logging, issue `no logging enable`.
- The Cisco AnyConnect VPN Client log from the Windows Event Viewer of the client PC:

1. Choose **Start > Run**.
2. Enter:

```
eventvwr.msc /s
```

3. Right-click the **Cisco AnyConnect VPN Client** log, and select **Save Log File As AnyConnect.evt**.

Note: Always save it as the **.evt file** format.

Problems with Passing Traffic

When problems are detected with passing traffic to the private network with an Anyconnect session through the ASA, complete these data gathering steps:

1. Obtain the output of the **show vpn-sessiondb detail svc filter name <username>** ASA command from the console, and if the output shows `Filter Name: XXXXX`, then gather the output for **show access-list XXXXX**. Verify that the access-list XXXXX does not block the intended traffic flow.
2. Export the Anyconnect statistics from the AnyConnect VPN Client > Statistics > Details > Export (AnyConnect-ExportedStats.txt).
3. Check the ASA configuration file for **nat** statements. If NAT is enabled, these must exempt data that returns to the client as a result of NAT. As an example, to NAT exempt (nat 0) the IP addresses from the AnyConnect pool, use this on the CLI:

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

4. Determine if the tunneled default gateway needs to be enabled for the setup. The traditional default gateway is the gateway of last resort for non-decrypted traffic.

Example

```
!--- Route outside 0 0 is an incorrect statement.

route outside 0 0 10.145.50.1
route inside 0 0 10.0.4.2 tunneled
```

As an example, if the VPN Client needs to access a resource which is not in the routing table of the VPN Gateway, the packet is routed through the standard default gateway. The VPN gateway does not need the complete internal routing table in order to resolve this. The **tunneled** keyword can be used in this instance.

AnyConnect Crash Issues

Complete these data gathering steps:

1. Ensure that the Microsoft Utility Dr Watson is enabled. In order to do this, choose **Start > Run**, and run **Drwtsn32.exe**. Configure this and click OK:

```
Number of Instructions      : 25
Number of Errors To Save   : 25
Crash Dump Type            : Mini
Dump Symbol Table         : Checked
Dump All Thread Contexts   : Checked
Append To Existing Log File : Checked
Visual Notification       : Checked
Create Crash Dump File     : Checked
```

When the crash occurs, gather the .log and .dmp files from **C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson**. If these files appear to be in use, then use `ntbackup.exe`.

2. Obtain the Cisco AnyConnect VPN Client log from the Windows Event Viewer of the client PC:
 - a. Choose **Start > Run**.
 - b. Enter:

eventvwr.msc /s

c. Right-click the **Cisco AnyConnect VPN Client** log, and select Save Log File As **AnyConnect.evt**.

Note: Always save it as the **.evt file** format.

Fragmentation / Passing Traffic Issues

Some applications, such as Microsoft Outlook, do not work but the tunnel is able to pass other traffic such as small pings.

This can provide clues as to a fragmentation issue in the network. Consumer routers are particularly poor at packet fragmentation and reassembly.

Try a scaling set of pings to see if it fails at a certain size. For example, ping 1 500, ping 1 1000, ping 1 1500, ping 1 2000.

It is recommended that you configure a special group for users that experience fragmentation, and set the svc mtu for this group to 1200. This allows you to remediate users who experience this issue but not impact the broader user base.

Uninstall Automatically

Problem:

The AnyConnect VPN Client uninstalls by itself once the connection terminates.

The client logs show that keep installed is set to disabled.

Solution:

Anyconnect uninstalls itself despite that the **keep installed** option is selected on ASDM. In order to resolve this issue, configure the **svc keep-installer installed** command under group-policy.

AnyConnect: Corrupt Driver Database Issue

This entry in the SetupAPI.log file suggests that the catalog system is corrupt:

```
W239 driver signing class list " C:\WINDOWS\INF\certclas.inf" was missing or
invalid. Error 0xfffffde5: Unknown Error. Assuming all device classes are subject to driver
signing policy.
```

You can also receive this error message and log message

```
Error(3/17): Unable to start VA, setup shared queue, or VA gave up shared queue"
```

And this log on the client

```
"The VPN client driver has encountered an error"
```

Repair

This issue is due to Cisco bug ID CSCsm54689 (registered customers only) . In order to resolve this issue, make sure that Routing and Remote Access Service is disabled before you start anyconnect. If this does not resolve the issue, complete these steps:

1. Open a command prompt as an Administrator on the PC (elevated prompt on Vista).
2. Run `net stop CryptSvc`.
3. Run `esentutl /p`
`%systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catd`
4. When prompted, choose OK to attempt the repair.
5. Exit the command prompt.
6. Reboot.

If Repair Fails

If the repair fails, complete these steps:

1. Open a command prompt as an Administrator on the PC (elevated prompt on Vista).
2. Run `net stop CryptSvc`.
3. Rename the `%WINDIR%\system32\catroot2` to `catroot2_old` directory.
4. Exit the command prompt.
5. Reboot.

Analyze the Database

You can analyze the database at any time in order to determine if it is valid.

1. Open a command prompt as an Administrator on the PC.
2. Run `esentutl /g`
`%systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catd`

Refer to System Catalog Database Integrity for more information.

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 Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Technical Support & Documentation – Cisco Systems](#)

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 24, 2008

Document ID: 100597
