SSL VPN Client installation guide

in D-Link DSR router series

TABLE OF CONTENTS

1. Introduction

This document is a tip sheet for SSL VPN setup and configuration. SSL VPN support is provided for a variety of operating systems and browsers, and there are specific steps to debug interoperability issues when connectivity or client installation problems are encountered.

1.1. Intended Audience and Scope

This document is targeted towards SSL VPN users and Administrators of the D-Link VPN Firewall platform.

1.2. Acronyms, Abbreviations and Glossary

Term	Description
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network
JRE	Java Run-Time Environment

2. SSL VPN Client Installation

The D-Link VPN router product will prompt the SSL VPN user to download a Java or ActiveX client during the tunnel establishment process. ActiveX clients are offered when the user's PC host uses the Internet Explorer browser to access the router; all other browsers are offered Java Run-Time Environment (JRE) SSL clients. Usually a SSL VPN client installation is triggered from the D-Link platform router portal page. This client opens a SSL tunnel for secure communication between the host and VPN router.

SSL VPN client installation is not entirely straight forward. The user must follow a sequence of installation steps which can vary from operating systems and browsers. The following sections explain these installation steps and recommendations in detail.

```
The below installation instructions reference removal of previously
installed clients and the requirement to clear the host cache. This is
only applicable for connection attempts to SSL VPN routers from two
different manufacturers. Repeated connections to the same router or
routers from the same product family do not require the cache to be
cleared.
```

2.1. Windows Operating Systems

In order to download the SSL VPN ActiveX or JRE client, the browser (Internet Explorer, Mozilla, Firefox, Google Chrome, Opera, Netscape Navigator) must be run in Administrator mode. This is a requirement for all Microsoft Internet Explorer versions run on a Windows OS (XP, Vista, 7).

2.1.1 Internet explorer

- Always start the browser as administrator

- Browser cache must be cleared between connection attempts when connecting to different manufacturer's SSL VPN routers. Repeated connections to the same router do not require the cache to be cleared.

- For 64 bit machines install Visual C++ (VC++) 2005 (x64) since there is a conflict with the current version installed. Please restart the browser after installation. You can download VC++ from:
  http://www.microsoft.com/downloads/details.aspx?familyid=90548130-4468-4BBC-9673-D6ACABD5D13B&displaylang=en

- Clean up the previously existing files from the browser
    a. In Internet Explorer, on the Tools menu, select Internet Options.
    b. On the General tab, select Settings under browser history.
    c. Select View Objects.
    d. Delete all object files then re-launch the browser

- Cleanup the previous virtual adapter if they still exists
    a. Select Start and then select Control Panel. Double-click System.
    b. On the Hardware tab, select Device Manager.
    c. Double-click Network Adapters. Right-click the VPN Tunnel ssldrv adapter, click uninstall and restart the system

- When SSL VPN client installation is triggered a pop up blocker will appear to check if user wants to really install the ActiveX content. Click on the pop up and check "Install this Add-on for All users on this computer". Please refer to section 2.4 for further details.

- In Windows Services, check if the ActiveXInstaller service is running. If it is running stop or disable the service and try the connection again. If this works the ActiveXInstaller service is controlling how the ActiveX object are installed superseding the trusted zone settings on the browser and the user can follow-up with instructions on how to configure the "ActivexInstaller" service.

- If after executing the above steps the SSL VPN client is not installed, you will need to clean up installed SSL VPN client files manually if they still exist on the PC:
  - a. Under *C:/Windows* delete following files.
    - . ssldrv.cat
    - . SSLDrv.inf
    - . ssldrv.sys
    - . SSLDrv.txt
  - b. In C:\Windows\Downloaded Program Files, delete the following if they exist:
    - VPLaunchClass
    - XTunnel.dll
    - XTunnel.inf
  - c. C:\Windows\System32\ delete the following files:
    - SSLDrv.inf
    - ssldrv.sys
  - d. In explorer Click Tools -> Manage Add-ons and remove "VPLaunchClass" from the list of add-ons.
  - e. Enter "*regedit*" in command prompt and in the registry editor search for "*XTunnel*" and delete all listed files. The PC must be restarted after these registry changes.

```
Please be careful while deleting registry files; it is recommended that
back up of your current registry taken before this operation.
```

2.1.2   Mozilla Firefox, Chrome, Opera and Netscape Navigator

- Always start the browser as Administrator

- If Chrome make sure UAC is disabled for windows vista and later versions of windows

- In the Tools menu, select options -> Clear Private Data->Cache

- Navigate to Local Disk (C: drive typically) > Documents and Settings > Users and delete SSL VPN related folders

2.2. Apple MAC Operating Systems

The root user will have privileges to install the SSL VPN client from the D-Link router. Some Apple Mac operating systems do not enable root user by default. Since the SSL VPN tunnel can only be established as "root" user, the following method can be used to enable and login as a root user:

- Login as administrator

- Start the terminal: **Applications > Utilities > Terminal**

- At the command prompt enter these commands

```
% sudo passwd root
Enter Password:
Changing password for root
New password:
Verify password:
```

The first password asked for is the Administrator account password, to prove that you are authorized to make changes to this system.   After that, enter the new root password (twice for verification). The "root" account is enabled after these steps with the new password.

- Logout of the administrator account.   In the login prompt of the OS, select other and supply "root" as username and new password defined previous step

- Once logged in, SSL VPN client binaries can be downloaded to this operating system and SSL VPN tunnels can be established.

- In MAC-10.6 O.S (Snow Leopard) Safari can be run in two different modes. By default it will run in 64-bit mode. To enable 32-bit mode from MAC desktop options select Go -> Applications -> Safari. Right client on Safari icon -> Select Get Info and select Open in 32-bit mode.

- For Java Run-Time Environment JavaFrameEmbedding.framework needs to be installed. It is available in System -> Library -> Frameworks directory and should be installed if not present

- Cleanup the previous virtual adapter if they still exists
    a. First use the original router's SSL VPN client uninstaller to remove the Java client from the Mac machine
    b. Quit and restart the browser (Mac Safari or Firefox)
    c. From the browser's Tools menu, select options to Clear Private Data and Delete Cookies

```
In MAC 10.6.* and greater versions, Admin users can establish ssl
tunnels if special permissions are given in sudoers file. If a Admin
user john have to esatblish ssl tunnel then sudoers file should
contain the below entry.
john ALL=NOPASSWD: usr/sbin/chown,/bin/chmod,/bin/rm
```

2.3. Linux Operating Systems

2.3.1. Mozilla Firefox, Opera and Netscape Navigator

- Always start the browser as root
- Make sure browser cache is cleared between connection attempts.
- Previous files if any can be removed, which are present under root

![D-Link Building Networks for People logo]

- "rm –rf /vpclient"

2.4. Internet Explorer unknown publisher issues

When installing SSL VPN from Internet Explorer and if any issues related to unknown publisher as shown in Figure 1 follow these steps to overcome the issue:

- Add the portal address to the trusted sites
    Internet Options → Security →Trusted sites→Sites→Add

- Edit IE ActiveX settings
    Internet Options → Security →Trusted sites→ Custom Level
    →ActiveX controls and plugins →Download unsigned ActiveX controls
    →Check prompt.   Please refer to Figure 2

2.5. Appendix

Figure 1

Figure 2