Operating System	WinSock Support	Aventail Connect Version Installed
Windows 98, Windows NT 4.0	WinSock 2.0	Aventail Connect 3.01
Windows 95	With Microsoft patch: WinSock 2.0	Aventail Connect 3.01
	Without Microsoft patch: WinSock 1.1	Aventail Connect 2.51
Windows 3.1, Windows for Workgroups 3.11, Windows NT 3.51	WinSock 1.1	Aventail Connect 2.51

You can create custom packages that include one or both versions of Aventail Connect (3.01 and 2.51) Setup will determine which version to install on each workstation. (For more information, see "Customizer.")

Windows 95 and WinSock

The Microsoft Windows 95 WinSock 2.0 Update upgrades WinSock 1.1 to WinSock 2.0 in Windows 95. This patch (filename `w95ws2setup.exe`) is available from the Microsoft Web site, at **http://www.microsoft.com/windows/downloads/contents/Updates/W95Sockets2/default.asp**. Unless you need specific Aventail Connect 3.01 features, Aventail recommends that you do not upgrade from WinSock 1.1 to WinSock 2.0. If you do not upgrade to WinSock 2.0, Aventail Connect 2.51 will be installed.

If you do need to install the Microsoft Windows 95 WinSock 2.0 Update, follow the instructions provided by Microsoft. Reboot your computer after upgrading, prior to installing Aventail Connect.

How Does Aventail Connect Work?

The following three steps are identical to standard WinSock communications steps described above; however, nested inside them are additional actions and options introduced by Aventail Connect.

1. The application does a DNS lookup to convert the hostname to an IP address. If the application already knows the IP address, this entire step is skipped. Otherwise, Aventail Connect does the following:
   - If the hostname matches a local domain string or does not match a redirection rule, Aventail Connect passes the name resolution query through to the TCP/IP stack on the local workstation. The TCP/IP stack performs the lookup as if Aventail Connect were not running.
   - If the destination hostname matches a redirection rule domain name (i.e., the host is part of a domain we are proxying traffic to) then Aventail Connect creates a false DNS entry (HOSTENT) that it can recognize

during the connection request. Aventail Connect will forward the hostname to the extranet (SOCKS) server in step 2 and the SOCKS server performs the hostname resolution.

- If the DNS proxy option is enabled and the domain cannot be looked up directly, Aventail Connect creates a fake DNS entry that it can recognize later, and returns this to the calling application. The false entry tells Aventail Connect that the DNS lookup must be proxied, and that it must send the fully qualified hostname to the SOCKS server with the SOCKS connection request.

2. The application requests a connection to the remote host. This causes the underlying stack to begin the TCP handshake. When the handshake is complete, the application is notified that the connection is established and that data may now be transmitted and received. Aventail Connect does the following:

   a. Aventail Connect checks the connection request.

   - If the request contains a false DNS entry (from step 1), it will be proxied.
   - If the request contains a routable IP address, and the rules in the configuration file say it must be proxied, Aventail Connect will call WinSock to begin the TCP handshake with the server designated in the configuration file.
   - If the request contains a real IP address and the configuration file rule says that it does not need to be proxied, the request will be passed to WinSock and processing jumps to step 3 as if Aventail Connect were not running.

   b. When the connection is completed, Aventail Connect begins the SOCKS negotiation.

   - It sends the list of authentication methods enabled in the configuration file.
   - Once the server selects an authentication method, Aventail Connect executes the specified authentication processing.
   - It then sends the proxy request to the extranet (SOCKS) server. This includes either the IP address provided by the application or the DNS entry (hostname) provided in step 1.

   c. When the SOCKS negotiation is completed, Aventail Connect notifies the application. From the application's point of view, the entire SOCKS negotiation, including the authentication negotiation, is merely the TCP handshaking.

3 The application transmits and receives data.

If an encryption module is enabled and selected by the SOCKS server, Aventail Connect encrypts the data on its way to the server on behalf of the application. If data is being returned, Aventail Connect decrypts it so that the application sees cleartext data.