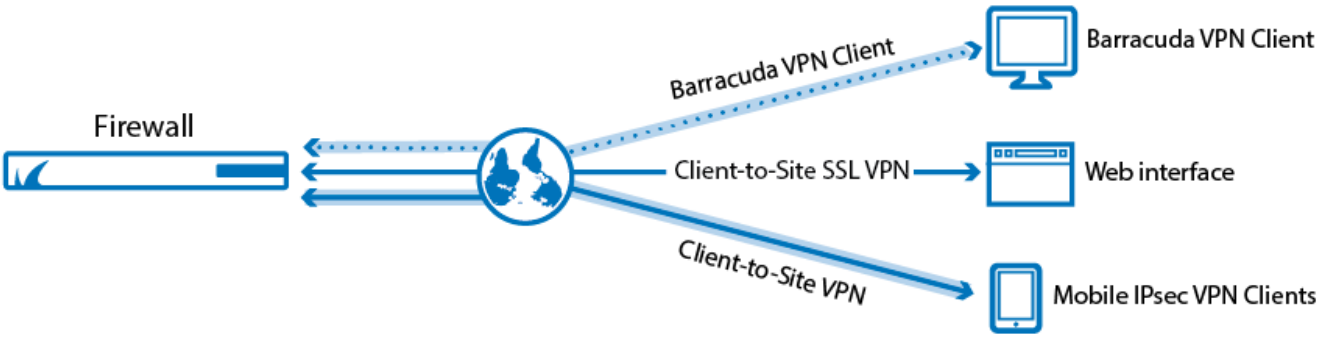
Client-to-Site VPN

https://campus.barracuda.com/doc/72516141/

VPN client-to-site connections are used to connect an individual device, such as a laptop or mobile phone, to the company network. The VPN client running on the client connects to the VPN service on the firewall.



Client-to-Site IPsec VPN

There are two types of IPsec VPNs available:

- **Shared Key** – No external CA is required. A passphrase (shared key) is entered on the server and the client. This passphrase is used to authenticate the connection.
- **Shared Key or Client Certificate** – Client and server require either a shared key or valid client certificate to authenticate the remote device. X.509 certificates are generated by an external CA. These certificates are used to authenticate the client. This method is more secure.

Additionally, every user must authenticate using a username and password. Usernames and passwords can be stored in external authentication services like Microsoft Active Directory, LDAP, or RADIUS. For more information, see Authentication.

Supported VPN Clients

The following VPN clients are supported:

- Barracuda VPN Client (Windows/macOS/Linux)
- Third-party IPsec VPN clients
- Apple iOS and Android devices

Setting Up an IPsec Client-to-Site VPN

For instructions on how to set up an IPsec VPN, see How to Configure a Client-to-Site VPN Group Policy.

SSL VPN Portal

The SSL VPN lets any user with a browser connect to published corporate resources - such as Exchange OWA, RDP connections to internal servers/computers, or internal Wikis. You can also use the My Network feature to initiate a full-routed network VPN from the SSL VPN portal.

Setting Up an SSL VPN

For instructions on how to set up SSL VPN, see SSL VPN.

PPTP

PPTP is no longer considered secure. Use TINA, IPsec, or L2TP/IPsec instead.

For compatibility and fallback purposes, client-to-site VPNs using the PPTP protocol are supported. The Point to Point Tunnel Protocol uses 40-, 56-, and 128-bit MPPE encryption. PPTP should only be used if no other VPN client is available on the client, or if VPN performance is more important than security, because the low overhead and weaker encryption allow for higher throughput. You can use the following authentication schemes with PPTP:

- Local Authentication
- MS-CHAPv2

For more information, see How to Configure a Client-to-Site PPTP VPN.

Remote Access Clients

Depending on the VPN protocol and the device, you must select the proper VPN client to match your client-to-site VPN configuration.

For more information, see Remote Access Clients.

Figures

1. c_to_s_overview.png