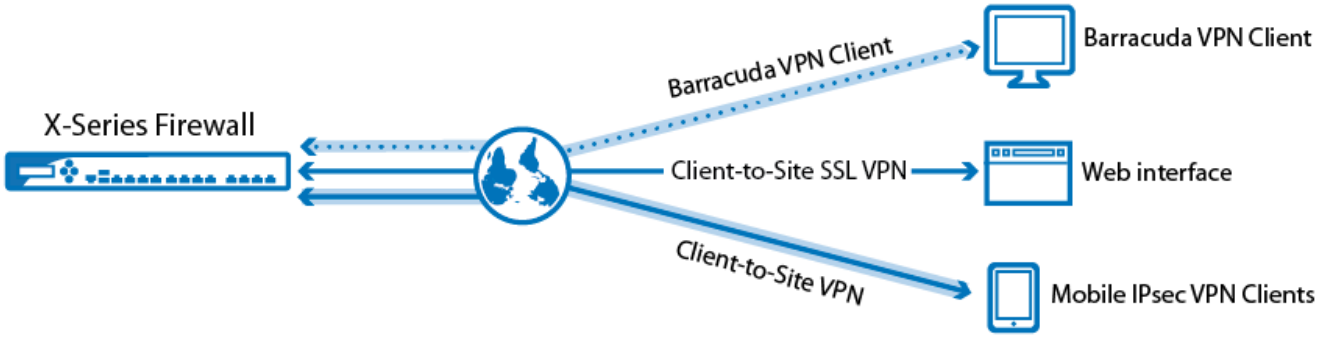
# Client-to-Site VPN

https://campus.barracuda.com/doc/30114049/

Client-to-site VPNs connect remote users to the corporate network.




## Client-to-Site IPsec VPN

There are three 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.
- **Client Certificate** – X.509 certificates are generated by an external CA. These certificates are used to authenticate the client. This method is more secure.
- **Shared Key or Client Certificate –** Client and server require either a shared key or valid client certificate to authenticate the remote device.

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 How to Configure an External Authentication Service.

#### 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 the following articles:

- How to Configure a Client-to-Site VPN with Shared Key Authentication
- How to Configure a Client-to-Site VPN with Certificate Authentication
- How to Configure the Apple iOS VPN Client for IPsec Shared Key VPN
- How to Configure Apple iOS VPN Client for IPsec VPN with Certificate Authentication
- How to Configure the Android VPN Client for IPsec Shared Key VPN

## 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 a SSL VPN

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

## PPTP

> As of 2012, PPTP is no longer considered secure. It is highly recommended that you switch away from PPTP because of the security risks involved.

Point-to-Point-Tunnel-Protocol (PPTP) is offered with up to 128-bit of MPPE encryption. It provides the following:

- Long standing widespread support across many platforms.
- Use if no other VPN client is available for client platform.
- Use if VPN performance is more important than security.
- Support for external authentication over MS-CHAP-v2 or a local user database.

#### Limitations

PPTP VPNs have the following limitations:

- No data integrity verification.
- Weak encryption using only a 128-bit key.

#### Supported VPN Clients

Almost every modern operating system includes a PPTP client. The following clients are officially

supported by Barracuda Networks:

- Native VPN clients included in Windows, macOS, and Linux.
- Native VPN clients included in iOS and Android.

**Setting Up a PPTP Client-to-Site VPN**

For instructions on how to set up a PPTP VPN, see How to Configure a Client-to-Site VPN with PPTP.

## Figures

1. c_to_s_overview.png