Client-to-Site VPN

https://campus.barracuda.com/doc/46209143/

With client-to-site VPNs, mobile workers can remotely access corporate information resources. VPNs provide access without the bandwidth, scalability, and manageability limitations of RAS implementations.

With the Barracuda NextGen Firewall F-Series, you can set up the following types of client-to-site VPNs:

Barracuda TINA

TINA is a Barracuda Networks proprietary VPN protocol. It offers a secure end-to-end solution that does not require additional third-party software or input. Every F-Series Firewall includes a root-level Certificate Authority (CA), letting you create, delete, and renew X.509 certificates for strong authentication. TINA offers substantial improvement over the IPsec protocol. It provides the following:

- High level of security. For supported encryption standards, see Authentication, Encryption, Transport, and VPN Routing.
- A full-featured Certificate Authority (CA) for TINA VPNs on every F-Series Firewall.
- X.509 certificate-based VPN authentication with password request.
- Immunity to NAT or proxy (HTTPS, SOCKS) traversal.

Supported VPN Clients

The following VPN clients are supported for use with Barracuda VPNs:

- Barracuda VPN Client (Windows)
- Barracuda VPN Client for macOS
- Barracuda VPN Client for Linux

Setting Up a Barracuda Client-to-Site VPN

For instructions on how to set up a Barracuda VPN, see the following articles:

- How to Configure a Client-to-Site TINA VPN with Personal Licenses
- How to Configure a Client-to-Site TINA VPN with Client Certificate Authentication
- Getting Started with the Barracuda VPN and Network Access Client

IPsec IKEv1 and IKEv2

IPsec is the most widely used secure cross-platform VPN protocol. The F-Series Firewall supports IPsec IKEv1 and IKEv2.

- High level of security. For supported encryption standards, see Authentication, Encryption, Transport, and VPN Routing.
- Multiple VPN authentication methods:
  - Pre-shared keys for iOS and Android devices
  - External X.509 certificate.
  - External X.509 certificate with username and password request using an external authentication server.
  - External X.509 certificate with username and password request. The username must match the one contained in the X.509 certificate. It can also be combined with external authentication.
- Support for multiple external authentication methods (MSAD, MSNT, LDAP, RADIUS, RSA-ACE, TACACS+).

Limitations

IPsec VPNs have the following limitations:

- Not every vendor adheres to the IPsec standard, so compatibility issues might be a problem.
- Certificate management requires more effort (external CA or self-signed certificates).
- Additional configuration might be needed if the client is behind a NAT router, which does not support IKEv1 IPsec passthrough or NAT traversal.

Supported IPsec IKEv1 VPN Clients

Every IPsec IKEv1 client adhering to the IKEv1 IPsec standard should work. Barracuda Networks uses the following VPN clients to test connectivity:

- How to Configure Apple iOS Devices for Client-to-Site VPN Connections with Certificate Authentication
- How to Configure Apple iOS Devices for Client-to-Site IPsec VPNs with PSK
- How to Configure Android Devices for Client-to-Site IPsec VPN Connections
- How to Configure Android Devices for Client-to-Site IPsec VPNs with PSK

Supported IPsec IKEv2 VPN Clients

Every IKEv2 IPsec client adhering to the IKEv2 IPsec standard should work. Barracuda Networks uses the following clients to test connectivity:

- Windows 8 / 8.1 / 10

Multiple Concurrent VPN Connections per User

A Remote Access Premium subscription is required for a user to connect to the Barracuda NextGen Firewall F-Series via Client-to-Site VPN with multiple devices simultaneously. The base license only allows one concurrent client-to-site connection per user.

For more information, see Licensing.

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 IKEv1 IPsec VPN with Client Certificate Authentication
- How to Configure a Client-to-Site VPN Group Policy
- How to Configure a Client-to-Site IKEv1 IPsec VPN with PSK
- How to Configure a Client-to-Site IPsec IKEv2 VPN

L2TP/IPsec

Layer 2 Transport Protocol over IPsec (L2TP/IPsec) is a Layer 2 protocol that uses IPsec for authenticating and securing the payload of the data. It provides the following:

- Native support in many modern operating systems (macOS, Linux, iOS, and Android).
- IPsec used to secure data and VPN authentication.
- Pre-shared X.509 certificates.
- Support for external authentication over MS-CHAP-v2 or a local user database.

Limitation

With L2TP VPNs, additional configuration might be needed if the client is behind a NAT router.

Setting Up an L2TP Client-to-Site VPN

For instructions on how to set up an L2TP VPN, see How to Configure a Client-to-Site L2TP/IPsec VPN.

PPTP

As of 2012, PPTP is no longer considered secure. It is highly recommended that you switch 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 PPTP VPN.