Client-to-Site VPN

https://campus.barracuda.com/doc/95258764/

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. The VPN service on the CloudGen Firewall supports the following VPN protocols:

- TINA
- IPsec IKEv1
- IPsec IKEv2
- L2TP/IPsec
- PPTP

TINA and IPsec

Client-to-site protocols using TINA or IPsec VPN protocols are configured through VPN group policies using an external CA. TINA VPN connections can also be configured using personal license files generated on the firewall via the Barracuda VPN CA.

TINA VPN Protocol

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 CloudGen 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, IP Version and VPN Routing.
- A full-featured Certificate Authority (CA) for TINA VPNs on every CloudGen Firewall.
- X.509 certificate-based VPN authentication with password request.
- Immunity to NAT or proxy (HTTPS, SOCKS) traversal.
- Multi-Factor Authentication using Time-based One-time Password (TOTP)

IPsec IKEv1 and IKEv2 VPN Protocols

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

- High level of security. For supported encryption standards, see Authentication, Encryption, Transport, IP Version 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+).

Client Networks

When the VPN clients connects, it is assigned an IP address out of the VPN client network configured in the VPN profile. VPN client networks can be either:

- **routed (Static Route)** – The client network is a separate network. Routed networks can be extended more easily, but require access rules to be able to access the on-premises networks.
- **local (Proxy ARP)** – If you want to use a part of an existing local network for the VPN clients, use a local client network. The firewall automatically enables Proxy ARPs for the IP addresses in the local client network.

Authentication

To authenticate users, two types are offered:

- **External CA** – This authentication method uses external authentication schemes and/or X.509 certificates. VPN configuration is carried out in template-based VPN group policies. Since the VPN group policies match on the user group or certificate information, this is an easy way to configure client-to-site VPN policies for large user groups.
- **Barracuda VPN CA** – Proprietary authentication method that generates self-signed certificates for named users. Every user must be configured individually with a personal VPN license created and assigned to a custom policy.

VPN Group Policies

VPN group policies use the external CA and are made up of multiple small configuration snippets. These configuration snippets can then be combined to a VPN group policy. If multiple policies exist, VPN group policy conditions determine which policy is used. A policy consists of the following:

- **IPsec Settings** – Encryption, authentication hash settings, and lifetimes for IPsec clients.
- **TINA Settings** – Just like with IPsec, you must define the encryption settings for the clients connecting via the TINA protocol. If you are using the Access Control Service and the NAC client, these settings are also defined here.
- **Common Settings** – These settings contain the network information used by both the IPsec and TINA clients.
- **Policy** – The group policy combines the IPsec, TINA, and common settings into a single configuration. The network used for the VPN clients is also selected in the policy.

- **Rules** – Define user group and X.509 certificate patterns, the VPN client type, and the source IP address or network to determine which group policy is used. Policy rules are evaluated from top to bottom. The first group policy condition to match determines the common, TINA, and IPsec settings used for the client-to-site connection.

For more information, see How to Configure a Client-to-Site VPN Group Policy and How to Configure a Client-to-Site VPN Group Policy for a CloudGen Firewall Auto Scaling Cluster in AWS.

Personal Licenses

This type of TINA VPN configuration uses the internal Barracuda VPN CA to create self-signed certificates. Every user is assigned a custom policy and VPN license. This license file in combination with the password of the configured authentication scheme is used to authenticate when establishing a VPN connection. The Barracuda VPN client must be used as the VPN client.

For more information, see How to Configure a Client-to-Site TINA VPN with Personal Licenses.

Multiple Concurrent VPN Connections per User

The base license allows only one concurrent client-to-site connection per user. An Advanced Remote Access subscription is required for a user to connect with multiple devices simultaneously via VPN. Multiple VPN connections are not supported for TINA personal licenses.

For more information, see How to License a CloudGen Firewall.

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. Many operating systems have built-in VPN clients with L2TP support. The VPN connections use pre-shared X.509 certificates

- Native support in many modern operating systems (macOS, Linux, iOS, and Android).
- Pre-shared X.509 certificates.
- Support for external authentication schemes.

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