TINA VPN Tunnels

https://campus.barracuda.com/doc/72516595/

TINA, the Barracuda VPN protocol, is a proprietary extension of the IPsec protocol developed to improve VPN connectivity and availability over the standard IPsec protocol.

Because the TINA protocol offers more advantages than IPsec, it is the main protocol that is used for VPN connections between CloudGen Firewalls. IPsec is used only for VPN tunnels between a CloudGen Firewall and a system from a different manufacturer.

The firewall offers most of the advanced VPN features based on our proprietary TINA VPN protocol:

- Modified initial handshake improving denial-of-service protection for X.509-certificate-based authentication.
- Multiple encapsulation transports: ESP, UDP, TCP, TCP/UDP hybrid mode, or routing (no encapsulation).
- Heartbeat monitoring and fast failover support.
- Continuous bandwidth and throughput evaluation.
- Immunity to NAT devices or proxies (HTTPS, SOCKS) between two tunnel endpoints.

Creating TINA Site-to-Site VPN Tunnels

To connect two networks protected by CloudGen Firewalls, TINA site-to-site VPN tunnels are used. An active site-to-site TINA VPN tunnel transparently connects the published networks.

For more information, see How to Create a TINA VPN Tunnel between CloudGen Firewalls.