TINA VPN Tunnels

https://campus.barracuda.com/doc/96026155/

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 Barracuda CloudGen Firewalls. IPsec is only used for VPN tunnels between CloudGen Firewalls and a system from a different manufacturer.

The Barracuda CloudGen Firewall offers most of the advanced VPN features of the Barracuda CloudGen Firewall 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.

Example of TINA Tunnel Variations

Using different connection objects for the access rule matching the VPN traffic can control if and how the VPN network is visible from the other side of the VPN tunnel.

For more information, see Examples for TINA VPN Tunnels.

TINA Tunnel Settings

There are many settings and parameters for configuring TINA VPN tunnels. The TINA Tunnel settings include a description for each setting and configuration option.

For more information, see TINA Tunnel Settings.

SD-WAN

SD-WAN is the logical layer used to manage multiple parallel VPN tunnels (transports) in one VPN tunnel configuration. SD-WAN also handles load balancing, fail-over, and traffic routing for all transports of the VPN tunnel. Switching between different transports is completely transparent to the user.

For more information, see SD-WAN.

WAN Optimization

WAN Optimization reduces the amount of traffic sent through the tunnel by using deduplication. This means that the same data does not have to be sent repeatedly over the WAN since it is cached and delivered from the local cache of the branch site instead. In the beginning of the data transfer, the first system creates hashes for chunks of the TCP stream. This information, instead of the data, is sent to the other system. If the same data chunk has been transferred previously, the data can be found in the dictionary of the peer. Bandwidth is saved because only the reference must be transferred. If the peer recognizes that the data is not available, it sends a request for the RAW data from the first system to integrate this information into its own dictionary. The chunk size is 512 bytes. This is a hardcoded value that cannot be changed.

For more information, see WAN Optimization.