TINA Tunnel Settings

https://campus.barracuda.com/doc/96026156/

The following provides a complete list of all TINA tunnel settings.

Basic

Setting	Description
Name	The tunnel name. You can enter a maximum of 64 characters.
Disabled	To manually disable the tunnel, select this check box.
Endpoint Type	Enable to use **IPv4** or **IPv6** addresses for the VPN tunnel envelope.
Transport	The transport type for the tunnel. You can select one of the following options: • **UDP** – The tunnel uses UDP port 691 to communicate. This connection type is suited best for response-optimized tunnels. It allows fast transport and generates the least overhead. • **TCP** – The tunnel uses TCP connection on port 691 or 443 (for HTTP proxies). This mode is required for connection over SOCKS4 or HTTP proxies. It is useful for unreliable lines where packet loss is common. • **UDP & TCP** – The tunnel uses TCP and UDP connections. The tunnel engine uses the TCP connection for UDP requests and the UDP connection for TCP requests and ICMP-based applications. • **ESP** – The tunnel uses ESP (IP protocol 50) to communicate. This connection type is best suited for performance-optimized tunnels. This option is useful for a private link such as MPLS, or when ESP is not blocked by NAT. ◦ Do not select *ESP* if there are filtering or NAT interfaces in between. ◦ Some routers, especially DSL routers for home accounts and cable modems, block ESP traffic. In this case, select **TCP** or **UDP**. • **Routing** – Use this option with SD-WAN. It disables data payload encryption within the tunnel and should only be used for uncritical bulk traffic on private lines. With this option, you can also specify the next hop address for the routed data packets when configuring the SD-WAN traffic transport classification.

Encryption	The data encryption algorithm. You can select one of the following options: • **AES | AES256** – The Advanced Encryption Standard (default). AES works with 128-bit key length and AES256 works with 256-bit long keys. With AES 256, the security of the encrypted data is increased, but more CPU capacity is required. Only use AES256 when required. Represents a very good compromise between key length and encryption speed. AES encryption speed can also be improved with hardware acceleration. (Recommended.) • **3DES** – Further developed DES encryption. Three keys each having a 56-bit length are used sequentially, providing a key length of 168-bit. (Not recommended.) Avoid using 3DES because this algorithm works very slowly and only offers acceptable performance with the help of special hardware acceleration cards. • **CAST** – Algorithm similar to DES with a key length of 128-bit. • **Blowfish** – Works with a variable key length up to 128-bit. • **DES** – Digital Encryption Standard. Because DES is only capable of a 56-bit key length, it can no longer be considered safe. (Not recommended.) • **Null** – No encryption.
Authentication	The hashing algorithm for the VPN tunnel. You can select one of the following options: • **MD5** – Message Digest 5. Hash length is 128-bit. (Not recommended. High performance, but theoretically vulnerable.) • **SHA** – Secure Hash Algorithm. Hash length is 160-bit. (Not recommended. High performance, but theoretically vulnerable.) • **NOHASH** – Use NOHASH for systems with hardware encryption support because it allows for hardware-accelerated high encryption performance on these systems. • **RIPEMD160** – RACE Integrity Primitives Evaluation Message Digest. Hash length is 160-bit. (Highly recommended.) • **SHA256** – Secure Hash Algorithm. Hash length is 256-bit. (Highly recommended.) • **SHA512** – Secure Hash Algorithm. Hash length is 512-bit. • **GCM** – Galois/Counter Mode (GCM). Hash length is 128-bit. Provides assurance of confidential data authenticity up to about 64 GB per invocation using a universal hash function defined over a binary Galois field.
SD-WAN Classification	The VPN transport classification for this tunnel. The first VPN tunnel is always classified as bulk-0. For more information, see SD-WAN. • Bulk • Quality • Fallback
SD-WAN-ID	The SD-WAN transport ID.
Compression	Enable to compress traffic transmitted through the VPN tunnel. VPN compression is not compatible with WAN Optimization.
Use Dynamic Mesh	Enable to allow this CloudGen Firewall to create and accept dynamic VPN tunnels. For more information, see Dynamic Mesh VPN Networks.

Dynamic Mesh Timeout [s]	Dynamic tunnels are terminated after the timeout (in seconds) passes without traffic being sent through the VPN tunnel.
Dynamic Mesh on Dynamic Interface	Enable if Dynamic Mesh is used in combination with dynamic interfaces. For more information, see Dynamic Mesh VPN Networks.

SD-WAN

From the **SD-WAN - Bandwidth Protection** and **SD-WAN - VPN Envelope Policy** tabs, configure the SD-WAN settings for the tunnel. For more information, see SD-WAN.

SD-WAN - Bandwidth Protection

Setting	Description
Dynamic Bandwidth Detection	When using traffic shaping, select the monitoring policy: • **Disabled** • **Active Probing and Passive Monitoring** • **Active Probing Only** • **No Probing - use Estimated Bandwidth** For more information, see SD-WAN.
Bandwidth Policy	Policy defining how Traffic Shaping is applied: • **None** • **Assign QoS Profile** – Apply a QoS • **Static Bandwidth** – Static outbound shaping based on the **Estimated Bandwidth**. Cannot be used in combination with **Dynamic Bandwidth and Latency Detection**. • **TCP Buffer Shaping** – Only for TCP transports using the TCP protocol for ingress shaping. Cannot be used in combination with **Dynamic Bandwidth and Latency Detection**.
Consolidated Shaping	Enable to shape VPN twice: Once on a per-transport basis and the second time for all VPN traffic.
Assigned QoS Profile	Select the QoS profile for transports not using **Dynamic Bandwidth and Latency Detection**. The **Bandwidth Policy** must be set to **Assign QoS Profile**.
Estimated Bandwidth	Enter the outbound bandwidth in kps.
Inbound/Reverse	Enter the inbound bandwidth in kps or -1 to use the same value as the outbound bandwidth.
FEC Level	Forward Error Correction Level. Possible values are: • **Off** • **Low** • **Medium** • **High** For more information, see Forward Error Correction (FEC) in TINA Tunnels.

SD-WAN - VPN Envelope Policy

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>TOS Policy</td><td>This policy setting specifies how Type of Service (ToS) information contained within a packet’s IP header is handled. In networks, the ToS may be used to define the handling of the datagram during transport. If the ToS is enveloped, this information is lost. You can select one of the following options:
• Copy TOS From Payload to Envelope – Use this option with non-TCP transports. The packet’s original ToS information is copied onto the envelope, so that it stays available for use.
• Fixed Envelope TOS – The ToS information is masked by enveloping it without consideration.</td></tr>
<tr><td>Envelope TOS Value</td><td>Enter the fixed ToS value. The same ToS information is then assigned to all packets. For example:
<table>
<tr><th>DSCP</th><th>Precedence</th><th>Purpose</th></tr>
<tr><td>0</td><td>0</td><td>Best effort</td></tr>
<tr><td>8</td><td>1</td><td>Class 1</td></tr>
<tr><td>16</td><td>2</td><td>Class 2</td></tr>
<tr><td>24</td><td>3</td><td>Class 3</td></tr>
<tr><td>32</td><td>4</td><td>Class 4</td></tr>
<tr><td>40</td><td>5</td><td>Express forwarding</td></tr>
<tr><td>48</td><td>6</td><td>Control</td></tr>
<tr><td>56</td><td>7</td><td>Control</td></tr>
</table>
For more information about precedence values, see http://www.bogpeople.com/networking/dscp.shtml and http://www.tucny.com/Home/dscp-tos.</td></tr>
<tr><td>QoS Policy</td><td>The QoS Policy settings rely on connection objects that are assigned to bands in the firewall rulesets and specify bandwidth assignment to transports as a whole. Multiple transports can share a single band if they are processed by the same interface.
You can select one of the following options:
• Use Band According to Rule Set – Use the band from the firewall rule, allowing traffic between the tunnel endpoints.
• Copy Band From Payload To Envelope – Use the band from the firewall rule, redirecting traffic to the VPN tunnel entry point. The band setting for the rule that configures traffic between the tunnel endpoints is then ignored.
• Fixed Envelope Band – Use a static band. From the Envelope Band Value list, select one of the available bands (System, Band A to Band G).</td></tr>
<tr><td>QoS Connector ID</td><td>The unique access ID for the connection.</td></tr>
</table>

Replay Window Size	If ToS policies assigned to VPN tunnels or transport packets are not forwarded instantly according to their sequence number, you can configure the replay window size for sequence integrity assurance and to avoid IP packet "replaying." The window size specifies a maximum number of IP packets that can be on hold until it is assumed that packets have been sent repeatedly and sequence integrity has been violated. Individual window size settings are configurable per tunnel and transport, overriding any global policy settings. Set to -1 to disable Replay Protection. • To view or edit the global replay window size, see the VPN server settings. • To view the replay window size for a tunnel, double-click the tunnel on the **VPN** page to open the **Transport Details** window (attribute: transport_replayWindow).

Advanced

Setting	Description
HW Acceleration	Specifies if HW acceleration or CPU acceleration should be used. You can select one of the following options: • **Use Acceleration Card** – If a crypto accelerator hardware board is in use, select this option. • **Use CPU** – Use CPU acceleration.
Packet Balancing	Enables/disables packet-based traffic balancing. Select **Cycle with a transport class** when using packet-based traffic shaping. For more information, see How to Configure Packet-Based Balancing for VPN Tunnels with SD-WAN.
WANOpt Policy	Select one of the configured WAN OPT policies. For more information, see How to Configure WAN Optimization Policies.
Key Time Limit	The period of time after which the re-keying process is started. You can select **5, 10 (default), 30,** or **60** minutes.
Key Traffic Limit	The key traffic limit. You can select **No Limit, 1 GB, 500 MB, 100 MB, 50 MB, 10 MB (default), 5 MB,** or **1 MB**.
Tunnel Probing	The interval between tunnel probes. If probes are not answered in the time period specified by the **Tunnel Timeout** setting, the tunnel is terminated. You can select **Silent** (no probes are sent), **1 secs, 10 secs, 20 secs, 30 secs** (default), or **60 secs**.
Tunnel Timeout	The length of time in which tunnel probes must be correctly answered before the tunnel is terminated. If, for some reason, the enveloping connection breaks down, the tunnel must be re-initialized. This is extremely important in setups with redundant possibilities to build the enveloping connection. You can select **3 secs, 10 secs, 20 secs** (default), **30 secs,** or **60 secs**.
High Performance Settings	To allow multiple CPUs and cores to be assigned to a single VPN tunnel to increase VPN performance, select this check box.
Routing Next-Hop	The routing next-hop address or interface, if used.

Scripts

From the **Scripts** tab, add scripts in the following sections to start or stop processes:

- **Start Script** – This script is executed when connecting via VPN.
- **Stop Script** – This script is executed when disconnecting from VPN.

Local Networks

Setting	Description
Call Direction	From this list, you can select one of the following options to specify if the local network is active or passive: • **Active** – An active VPN server accepts tunnel requests and initiates the tunnel connection. When the tunnel is down for a defined time, it cleans its state to accept retries from its partner. Furthermore, it tries to initiate the connection by itself. • **Passive** – A passive VPN server does not build up the tunnel. It merely accepts requests from its partner. If the tunnel is down for a defined time, it cleans its state to accept retries from its partner. • **OnDemand** – Use this option with SD-WAN. The VPN server actively builds up a connection and terminates it during the time-outs specified by the **On Demand Transport Timeout** setting from the **SD-WAN - VPN Envelope Policy** tab.
Local Network Scheme	Select a **Local Network** object configured in the **Local Networks** tab, or use **explicit** to enter the local networks directly.
Network Address	The local networks that should be able to reach the partner networks. You can enter a list of networks or single IP addresses. Because this setting is typically shared by several tunnels, it may be defined from the **Local Networks** setting and referenced within the single tunnel configurations. After entering an address, click **Add**.

Local

Setting	Description
Tunnel Parameter Template	From this list, you can select a template that has been configured from the **Parameter Templates** tab on the **Site to Site** page. To explicitly configure the settings, select **-explicit-** .

IP Address or Device used for Tunnel Address	From this list, you can select one of the following options: • **First Server IP** – The first server IP address is used. • **Second Server IP** – The second server IP address is used. • **Dynamic (via routing)** – The IP address is specified by the routing table. • **Explicit (ordered list)** – To explicitly specify the IP addresses or devices used, select this option. This option is important to ensure redundancy on the active side of the tunnel.
Proxy Type	From this list, you can select one of the following options: • **Direct (no Proxy)** – The standard connection. • **HTTP Proxy** – An HTTP proxy server with optional user/password authentication is used. • **Socks 4 Proxy** – A SOCKS4 server is used. • **Socks 5 Proxy** – A SOCKS5 server is used. • **Like System Settings** – Use the proxy settings configured on the CloudGen Firewall.

Identify

From the **Identification Type** list, you can select one of the following options to specify if a public key or certificate is to be used:

- **Public Key**
- **X509 Certificate (CA signed)**
- **X509 Certificate (explicit)**
- **Box SCEP Certificate (CA signed)**

For certificates, configure the **Server Certificate** and/or **Server Protocol Key** settings to select the certificate and protocol key.

Remote Networks

From this tab, specify the partner networks that are accessible through the VPN tunnel.

Setting	Description
VPN Interface Index	By default, the tunnel is fed through **vpn0**. To use another VPN interface, enter it in this field.
Remote Network	The partner networks that are accessible through the VPN tunnel. Enter the network address, and then click **Add**.

Advertise Route	To propagate routes to the partner networks using OSPF or RIP, select this check box. For more information, see Dynamic Routing Protocols (OSPF/RIP/BGP).

Remote

From this tab, specify the IP addresses and host names of the VPN partner system.

Setting	Description
Remote Peer Tunnel Name	The name of the VPN partner.
Remote Peer IP Addresses	The IP addresses, hostname, or, if the call direction is passive, enter the subnet of the VPN partner. Enter the network address, and then click **Add**. When using a hostname as the destination, the VPN service caches the resolved IP address for the TTL of the DNS record. This may result in problems with DynDNS domains using a long TTL. For more information on how to clear the cache manually, see **Clearing the DNS Cache of the VPN Service** below.
Port (TCP only)	The port used for the VPN tunnel. The default port is 691. If you have configured a different port in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings, Local VPN listen port**, then this port will be used instead.
Accepted Encryption Algorithms	The encryption ciphers that can be used to establish the connection.
Accepted Authentication Algorithms	The authentication ciphers that can be used to establish the connection.

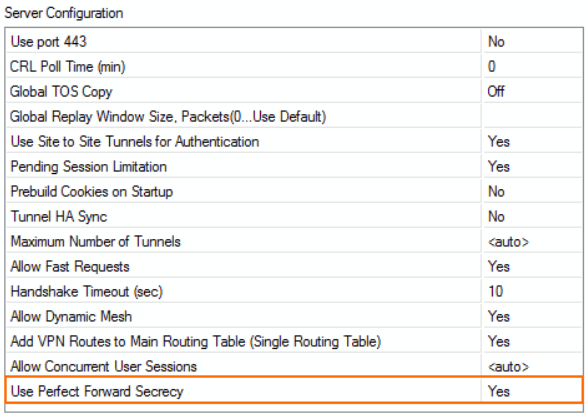
Peer Identification

Depending on whether the tunnel direction is passive or active, the partner server may be a whole subnet (passive mode) or may need to be defined by single IP addresses (active and bi-directional mode). Import the public key of the tunnel partner via clipboard or file. Principally, the public key is not needed. However, it is highly recommended to use strong authentication to build up the tunnel enveloping connection. If you have two different tunnel connections configured between the same two peers, the keys are mandatory.

Perfect Forward Secrecy for TINA Tunnels

By default, firewalls running 6.2.0 or higher support Perfect Forward Secrecy (PFS) and Elliptic Curve Cryptography (ECC). The VPN service sends and responds to PFS/EC requests and uses ECC if it is also supported by the remote firewall. To determine if PFS/EC is used, go to the VPN logs and check for the following log messages:

- DH attributes found in request, generating new key
- DH attributes found in response, deriving shared secret



Server Configuration

Use port 443	No
CRL Poll Time (min)	0
Global TOS Copy	Off
Global Replay Window Size, Packets(0...Use Default)	
Use Site to Site Tunnels for Authentication	Yes
Pending Session Limitation	Yes
Prebuild Cookies on Startup	No
Tunnel HA Sync	No
Maximum Number of Tunnels	<auto>
Allow Fast Requests	Yes
Handshake Timeout (sec)	10
Allow Dynamic Mesh	Yes
Add VPN Routes to Main Routing Table (Single Routing Table)	Yes
Allow Concurrent User Sessions	<auto>
Use Perfect Forward Secrecy	Yes

Clearing the DNS Cache of the VPN Service

Using Barracuda Firewall Admin

To clear the cache and manually trigger a DNS lookup, open the **VPN** page. Right-click on the VPN tunnel and select **Show Runtime information.** Right-click on the **IKE** entry in the **Worker** section, and select **Flush DNS Cache**.

Command Line

Log in as root and enter**:**

```
/opt/phion/bin/ipsecctrl isa flushdns
```

Figures