Authentication, Encryption, Transport, IP Version and VPN Routing

https://campus.barracuda.com/doc/95258763/

VPN clients must authenticate themselves to the VPN server. A valid certificate is required for the client to verify the identity of the VPN server. To meet the security needs of your network, you can define username/password authentication and strict certificate requirements.

The Barracuda CloudGen Firewall supports multiple encryption algorithms for VPN connections. For TINA VPNs, multiple transport types are also available.

VPN Authentication Certificates

X.509 certificates are used by IPsec, L2TP/IPsec, and TINA (the Barracuda proprietary transport protocol). The certificates contain the following information:

- Public key.
- Some data signed by the private key for verification.
- Identity of the the CA.
- Identity of the owner.
- Key usage. Depending on what type of VPN and which clients you use, certain X.509 extensions might be required when creating the certificate.

For PPTP VPNs, external certificates are not needed because certificates are generated by the server at runtime.

Special settings might be required when creating the following types of certificates:

- L2TP/IPsec VPN service certificates. For more information, see How to Configure a Client-to-Site L2TP/IPsec VPN.
- Certificates for iOS devices used as a VPN client. For more information, see How to Set Up External CA VPN Certificates.

Certificate CA (PKI)

Use an external CA (PKI) for firewalls that are standalone.

Depending on the certificate, you must export it in one of the following formats after it is created and

signed:

Certificate	File Format
Root Certificate	PEM or CER
Server Certificate	PKCS12, CER, or CRT
Service Certificate/Key	PEM
Client Certificate (if needed)	PEM

Example Certificates for IPsec, L2TP, and iOS Clients

If you encounter any problems with your certificates, compare your settings to those of the example certificates. Especially verify the **X509 Basic Constraints** and **X509v3 Key Usage** settings.

Root Certificate

Tab	Setting	Value
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Basic Constraints**	CA:TRUE
	X509v3 Key Usage	Digital Signature, Key Agreement, Certificate Sign

Server Certificate

Tab	Setting	Value
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=docu,O=Barracuda Network AG,L=Innsbruck,ST=Tyrol,C=AT
	Hash	cc0460b5
Issuer	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374

Extensions	**X509v3 Key Usage**	Digital Signature, Key Agreement, Certificate Sign
	X509v3 Subject Alternative Name	DNS:vpnserver.yourdomain.com

Client Certificate

Tab	Setting	Values
Status	**Signature Algorithm**	sha1WithRSAEncryption
Subject	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tyrol,C=AT
	Hash	c2b06d20
Issuer	**RFC 2253**	emailAddress=support@barracuda.com,OU=documentation,O=Barracuda Networks,L=Innsbruck,ST=Tirol,C=AT
	Hash	7b6d2374
Extensions	**X509v3 Key Usage**	Digital Signature

Supported Encryption Algorithms

The Barracuda CloudGen Firewall supports the following encryption algorithms for TINA, IPsec, and L2TP/IPsec VPN connections:

Algorithm	Description
AES256	Advanced Encryption Standard with 256-bit encryption.
AES	Advanced Encryption Standard with 128-bit encryption. AES is often chosen because it provides a good performance and security ratio.
3DES	Triple DES. This algorithm is considered most secure but results in high system loads and lower VPN performance.
Blowfish	A keyed, symmetric block cipher developed to replace DES.
CAST	A 128-bit block cipher.
DES	Digital Encryption Standard. DES is the only export restricted algorithm available. DES is not recommended because it is considered unsafe.
NULL	No encryption.

TINA Transport Protocols

For TINA VPNs, the following transport types are available:

Transport Protocol	Description
UDP	Stateless protocol that is best used for response-optimized tunnels. UDP is not recommended for unstable Internet connections.
TCP	Stateful protocol that is used if the tunnel runs over a proxy server. Higher protocol overhead limits the response time. TCP is preferred for unstable Internet connections.
UDP & TCP	Hybrid mode that creates two transport tunnels. To compensate for the weakness of both protocols, UDP is used for TCP connections, and TCP is used for stateless connections.
ESP	The tunnel uses ESP (IP protocol 50). ESP is best for performance-optimized tunnels, but it does not work if NAT routers must be traversed.

IPv6 Support



The VPN service supports IPv6 for the VPN envelope. This means that the site-to-site and client-to-site VPN tunnels can be created between two IPv6 endpoints, but only IPv4 traffic can be sent through the tunnel. IPv6 is not supported for:

- Dynamic Mesh
- L2TP
- PPTP
- SSL VPN

VPN Routing Tables

You can configure how the VPN routes are introduced into the firewall's routing table.

- **Separate Routing Table** – By default, the CloudGen Firewall uses source-based routing and creates separate premain routing tables for every VPN tunnel.
- **Single Routing Table** – All VPN routes are inserted into the main routing table. VPN routes are inserted with a preference of **10**.

Handling of Duplicate Routes

- When a duplicate route to an existing VPN route in the main routing table is announced to the CloudGen Firewall via RIP, OSPF, or BGP, a duplicate routing entry is created and the route that was added last is used.
- Creating a direct or gateway route with the same metric and destination as a VPN route in the main routing table results in duplicate routes. The route added last is used.

Enable the Single Routing Table for VPN Routes

If you are using source-based VPN routing tables, you have the option of moving the entries to the main routing table. Because entries with identical destination addresses in the main routing table are aggregated regardless of their source address, you must be aware that when moving source-based VPN routing entries to the main routing table, the source address of a VPN routing entry will be ignored.

Using this option without a proper migration plan may break your current setup, forward traffic into wrong tunnels and cause loss of connectivity!

Therefore, if you want to route VPN traffic based on a special source address, it is recommended not to use this option.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. In the left menu, select **General**.
3. Click **Lock**.
4. Set **Add VPN routes to main routing table** to **Yes**.
5. Click **Send Changes** and **Activate**.

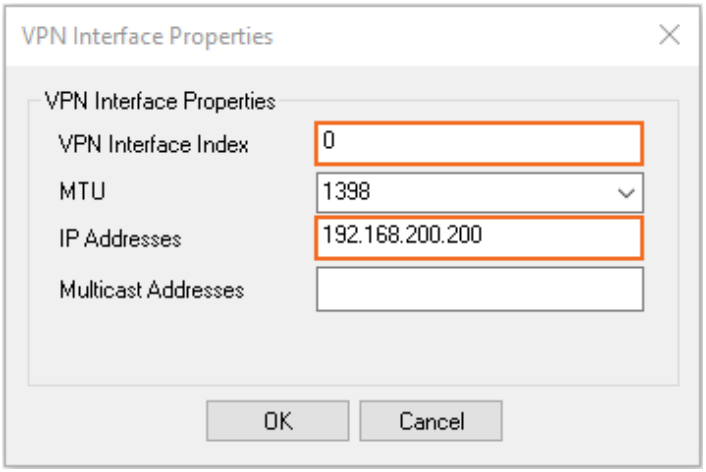
Enabling Local Out Traffic when using a Single Routing Table for VPN Routes

To send the local out traffic through the VPN tunnel, you must configure an IP address from the source network for the VPN interface.

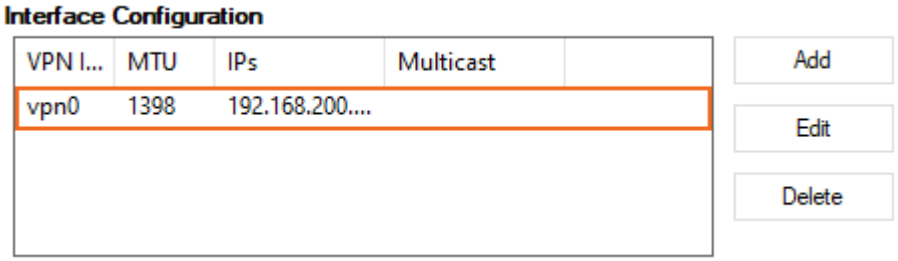
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service**

> VPN Settings.

2. Click **Lock**.
3. In the left menu, select **Routed VPN**.
4. Next to the **Interface Configuration** table, click **Add**.
5. In the **VPN Interface Properties** window, configure the following settings and then click **OK**.
   - In the **VPN Interface Index** field, enter the number of the VPN interface. E.g., `0` for vpn0
   - In the **IP Addresses** field, enter a box IP address that is also part of a published VPN network. E.g., `192.168.200.200` if one of the **Local Networks** of the VPN tunnel is 192.168.200.0/24.



   - Click **OK**. The interface is now listed in the **Interface Configuration** table.



6. Click **Send Changes** and **Activate**.

Local Out traffic is now sent and received correctly through the Site-to-Site VPN tunnel.

Figures

1. s_to_s_ipv6_tina-01.png
2. maintable_routing_01.png
3. maintable_routing_02.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.