

VPN Tab

<https://campus.barracuda.com/doc/43847180/>

The Barracuda NG Admin **VPN** tab provides information on all VPN connections that are configured on the Barracuda NG Firewall. Selecting the icons in the ribbon bar under the **VPN** tab takes you to the Site-to-Site and Client-to-Site VPN pages.

In this article:

Site-to-Site

The first page accessed when clicking the **VPN** tab is the **Site-to-Site** page.

Name	Tunnel	Local	Peer	Info	Transport	Encryption	Auth.	Compression	bps10	Total	Idle
S1-Zurich-borderS1 (2)											
S1-Zurich-borderS1	TINA	62.99.0.200	213.47.0.200		TCP & UDP	AES 128	MD5	0%	0 B	0 K	44 f
Fallback (0)		62.99.0.200	213.47.0.200		TCP & UDP	AES 128	MD5	0%	0 B	0 K	43 f
/ single transport tunnel (1)											
S1-Munich-borderS1-10.0.6...	IPSEC	66.99.0.200	212.86.0.200	DOWN(passive)	ESP	3DES	MD5	0%	0 B	0 K	2 d

The **Site-to-Site** page lists all firewall-to-firewall VPN tunnels that are configured on the Barracuda NG Firewall. These can either be VPN tunnels based on the Barracuda Networks proprietary TINA protocol or IPsec VPN tunnels (for more information, see [Site-to-Site VPN](#)).

Tunnel Information

The information details are displayed as follows:

- **Name** – Displays the name of the VPN tunnel.
- **Tunnel** – Displays the type of VPN tunnel. This can either be TINA or IPSEC.
- **Group** – Displays the group the VPN tunnel belongs to.
- **Local** – Displays the local VPN point of entry.
- **Peer** – Displays the remote VPN point of entry.
- **Info** – Depending on the tunnel type, this column displays either the tunnel type, the state, or the certificate subject. As soon as a tunnel is passive and down, DOWN (passive) will be displayed. For group tunnels with certificate, the x.509 subject is displayed.
- **Transport** – Displays the VPN tunnel transport protocol used.
- **Encryption** – Displays the tunnel encryption method used.

- **Auth.** - Displays the used packet authentication method.
- **Compression** - Current compression rate and type of a TINA VPN tunnel.
- **bps10** - Current transfer speed in bytes per 10 seconds.
- **Total** - Total amount of traffic in KB/key.
- **Idle** - Time (in seconds) passed since the last activity within the connection.
- **Start** - Duration of VPN connection in minutes (m) or days (d).
- **Key** - Age of issued key in minutes (m) or days (d).

Double-clicking an entry opens a new window with detailed information about the selected VPN tunnel.

Context Menu

Right-clicking a VPN tunnel opens a context menu where the following tunnel operations can be selected:

- **Show Details** - Opens a new window with detailed information about the selected VPN tunnel.
- **Show Transport Details** - Opens a new window with detailed information about the selected VPN transport.
- **Last VPN Access** - Opens a new window with a detailed VPN access and connection history.
- **Show on Status Page** - Opens the VPN **Status** window and highlights the according VPN tunnel.
- **Enable Tunnel** - Enables the selected VPN tunnel.
- **Temporary Enable Tunnel** - Enter the desired time period in minutes for which the VPN tunnel should be enabled.
- **Disable Tunnel** - Permanently disables the selected VPN tunnel. The VPN tunnel will be established again, by clicking **Enable Tunnel** within the context menu.
- **Terminate Tunnel** - This method kills Phase2 of the IPSEC tunnel. Phase2 is re-initialized immediately.
- **Initiate Tunnel** - Manually re-establishes the selected VPN tunnel.
- **Hard kill Tunnel** - This method kills Phase1 of the VPN tunnel. Because there is no exchange between the tunnel partners, Phase1 can only be re-established if the partner kills its own Phase 1.

Do not use the **Hard kill Tunnel** function unless it is absolutely necessary. In case of doubt, please contact Barracuda Networks Technical Support to get assistance.

- **Show VPN Run-Time Info** - Opens a window with details for the used VPN service this VPN tunnel is using.
- **Show Sessions** - Displays information about the VPN sessions.
- **Show grouped** - Groups the list entries according to the amount of transports.
- **Save Traffic Selection Policy** - Remembers the **Selection** settings and makes the selected settings available when reconnecting to a unit.
- **Tools** - Opens the **Tools** context menu.

Client-to-Site

The **Client-to-Site** page lists all client-to-site VPN tunnels that are configured on the Barracuda NG Firewall. These can either be VPN tunnels established by the [Barracuda Network Access Client](#), L2TP/IPsec or PPTP clients (for more information, see [Client-to-Site VPN](#)). To access the **Client-to-Site** page, select the **Client-to Site** icon under the **VPN** tab.

Tunnel Information

The information details are displayed as follows:

- **Name** - Displays the name of the VPN tunnel.
- **Tunnel** - The type of VPN tunnel. This can either be PGRP, PPTP, L2TP, or IPSEC.
- **Type** - The type of network that is used for the VPN client.
- **Group** - Displays the group the logged in VPN user belongs to.
- **Local** - Displays the local VPN point of entry.
- **Peer** - Displays the remote VPN point of entry.
- **Virtual IP** - Displays the assigned virtual IP address.
- **Info** - Either a person name (defined during configuration) and an IP address assigned by the license, separated by "@" (the "at" character), or the certificate subject.
- **Transport** - Displays the VPN tunnel transport protocol used.
- **Encryption** - Displays the tunnel encryption method used.
- **Auth.** - Displays the packet authentication method used.
- **Compression** - Current compression rate and type of a VPN tunnel.
- **NAC** - Displays information if the VPN tunnel is established by the Barracuda Network Access Client.
- **bps10** - Current transfer speed in bytes per 10 seconds.
- **Total** - Total amount of traffic in KB/key.
- **Idle** - Time (in seconds) passed since the last activity within the connection.
- **Start** - Duration of VPN connection in minutes (m) or days (d).
- **Key** - Age of issued key in minutes (m) or days (d).

Double-clicking an entry opens a new window with detailed information about the selected VPN tunnel.

Context Menu

Right-clicking a VPN tunnel opens a context menu where the following tunnel operations can be selected:

- **Show Details** - Opens a new window with detailed information about the selected VPN tunnel.
- **Show Transport Details** - Opens a new window with detailed information about the selected VPN transport.

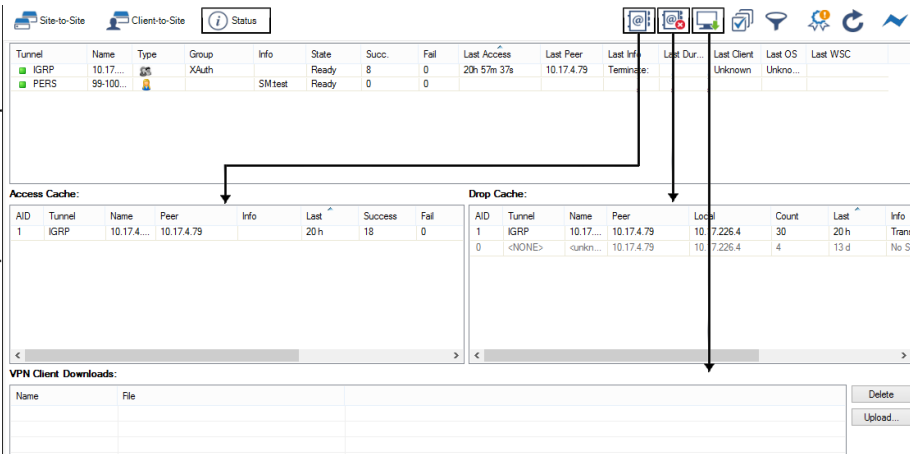
- **Last VPN Access** – Displays information about the last VPN access.
- **Show on Status Page** – Opens the VPN **Status** window and highlights the according VPN tunnel.
- **Enable Tunnel** – Enables the selected VPN tunnel.
- **Temporary Enable Tunnel** – Enter the desired time period in minutes for which the VPN tunnel should be enabled.
- **Disable Tunnel** – Permanently disables the selected VPN tunnel. The VPN tunnel will be established again, by clicking **Enable Tunnel** within the context menu.
- **Terminate Tunnel** – This method kills Phase2 of the IPSEC tunnel. Phase2 can be re-initialized immediately.
- **Initiate Tunnel** – Manually re-establishes the selected VPN tunnel.
- **Hard kill Tunnel** – This method kills Phase1 of the VPN tunnel. Because there is no exchange between the tunnel partners ,Phase1 can only be re-established if the partner kills his own Phase 1.

Do not use the **Hard kill Tunnel** function unless it is absolutely necessary. In case of doubt, please contact Barracuda Networks Technical Support to get assistance.

- **Show VPN Run-Time Info** – Opens a window with details for the used VPN service this VPN tunnel is using.
- **Show Sessions** – Displays information about the VPN sessions.
- **Show grouped** – Groups the list entries according to the amount of transports.
- **Save Traffic Selection Policy** – Remembers the **Selection** settings and makes the selected settings available when reconnecting to a unit.
- **Tools** – Opens the **Tools** context menu.

Status

The **Status** page provides information on all configured VPN connections on the given system. To access the page, select the **Status** icon under the **VPN** tab. The page consists of four sections which are accessible via the main screen or by clicking the corresponding icons in the ribbon bar:



The screenshot shows the VPN Status page with the following sections and data:

- Status Section:** A table listing VPN tunnels.

Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last F...	Last Dur...	Last Client	Last OS	Last WSC
IGRP	10.17...	IPsec	XAuth		Ready	8	0	20h 57m 37s	10.17.4.79			Unknown	Unkno...	
PERS	99-100...			SMtest	Ready	0	0							
- Access Cache:** A table showing VPN sessions.

AID	Tunnel	Name	Peer	Info	Last	Success	Fail
1	IGRP	10.17.4...	10.17.4.79		20 h	18	0
- Drop Cache:** A table showing dropped sessions.

AID	Tunnel	Name	Peer	Local	Count	Last	Info
1	IGRP	10.17...	10.17.4.79	10.7.226.4	30	20 h	
0	<NONE>	<unkn...	10.17.4.79	10.7.226.4	4	13 d	No S
- VPN Client Downloads:** A table for managing client files.

Name	File

Status Section

In the upper section of the **Status** page, the status of all configured VPN tunnels (site-to-site, client-to-site and SSL VPN) is listed. The information details are displayed as follows:

- **Tunnel** - Description of the VPN Tunnel.
- **Name** - Displays the name of the VPN Tunnel.
- **Type** - Displays the type of the VPN Tunnel.
- **Group** - Displays the group the VPN Tunnel belongs to.
- **Info** - (optional) Displays additional information.
- **State** - Status of the VPN connection (ACTIVE, Ready or Disabled).
- **Succ.** - Number of successful connections.
- **Fail** - Number of failed connections.
- **Last Access** - Time passed since the last access.
- **Last Peer** - Client IP address of the last connection.
- **Last Info** - Last information concerning the connection (e.g. Access Granted, Disconnect, etc.).
- **Last Duration** - Duration of the last connection.
- **Last Client** - Client (including version number) used for the last connection.
- **Last OS** - Operating system (including kernel number) used by the last connection's client.
- **Last WSC** - WSC information.

You can enable, disable, or temporarily enable configured connections by selecting the corresponding entry in the right-click context menu. If selecting "temporarily enable", enter the period (in minutes) for which the tunnel should be enabled. For each entry of the **Status** window, colored icons indicate the current status of a VPN tunnel:

- **green** - Tunnel is terminated, but ready.
- **blue** - Tunnel is active.
- **gray** - Tunnel is disabled.

Within the **Type** column, the type of VPN tunnel is indicated. The icons indicate information as follows:

- **1 user** - Personal VPN tunnel.
- **2 users** - Group VPN tunnel.
- **Server lock** - Firewall-to-firewall VPN tunnel.
- **User global** - SSL VPN tunnel.

Access Cache

The **Access Cache** section, if opened via the corresponding icon, displays the history of successful VPN connection attempts for Site-to-Site, Client-to-Site and SSL VPN connections. Double-click on a VPN tunnel to display detailed information on this connection.

Drop Cache

The **Drop Cache** section, if opened via the corresponding icon, shows details about unsuccessful VPN connection attempts to a Barracuda NG Firewall.

VPN Client Downloads

You can copy Barracuda Network Access Client update files onto the Barracuda NG Firewall system. The next time a Barracuda Network Access Client connects to the VPN server, it will be offered this installation file for download.

1. Click **Upload** on the right of the section to open the uploading window.
2. Use the **Browse** option within this window to select the desired installation file.
3. Click **Upload** to store the update file on the Barracuda NG Firewall.

If an uploaded file has become obsolete, select it and click **Delete** to remove the file from the VPN client downloads list.

Figures

1. vpn_tab.png
2. status_pg.png

© Barracuda Networks Inc., 2019 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.