VPN Tab

https://campus.barracuda.com/doc/73719535/

The Barracuda Firewall Admin **VPN** tab provides information on all VPN connections configured on the CloudGen Firewall. Go to the **VPN** tab in the ribbon bar for live information on all site-to-site and client-to-site VPN tunnels.

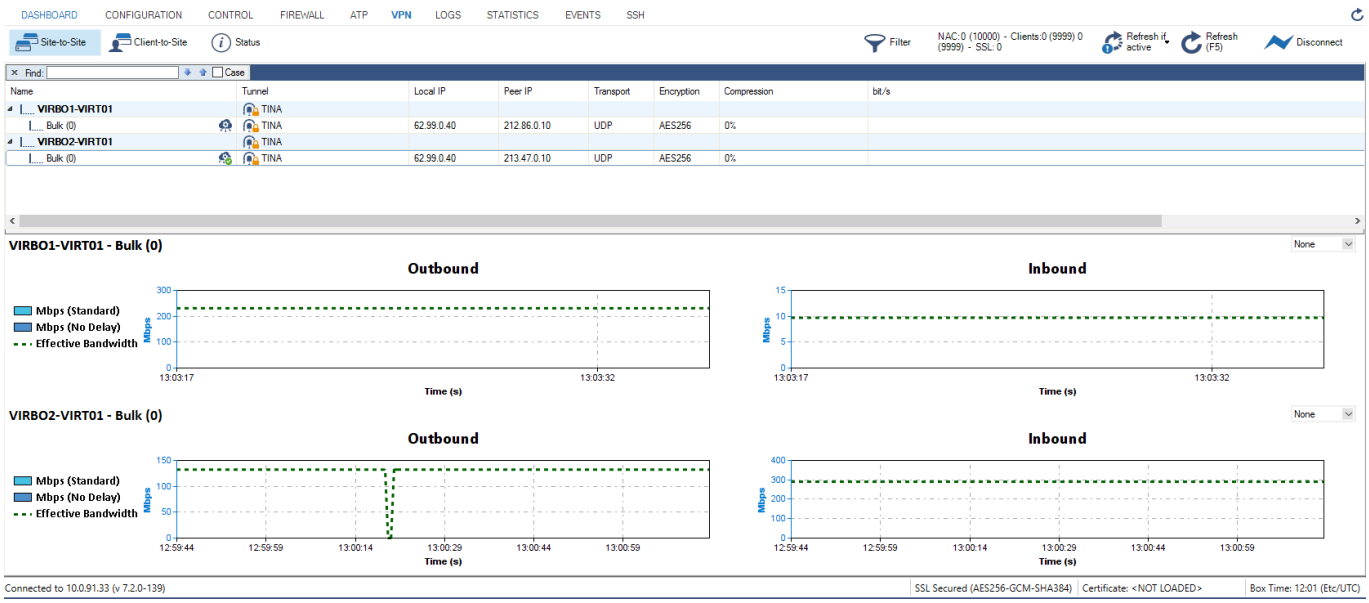
The VPN tab provides three separate pages:

- Site-to-Site
- Client-to-Site
- Status

Site-to-Site

The **Site-to-Site** page lists all TINA and IPsec site-to-site VPN tunnels.

Go to **VPN > Site-to-Site**.



The standard columns in the table provide the following information:

- **Name** – The name of the VPN tunnel.
- **Tunnel** – The type of VPN tunnel, either TINA or IPsec.
- **Local IP** – The local VPN point of entry.
- **Peer IP** – The remote VPN point of entry.

- **Transport** – The VPN tunnel transport protocol.
- **Compression** – The current compression rate and type of TINA VPN tunnel.
- **bit/s** – The current transfer speed in bits per second.
- **Start** – The duration of VPN connection in minutes (m) or days (d).

To show or hide additional columns, right-click in the window, select **Columns**, and then either select or deselect the columns you want displayed or hidden.

The following additional columns are available:

- **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)** is displayed. For group tunnels with a certificate, the x.509 subject is displayed.
- **Total (Byte)** – The total amount of traffic.
- **Key** – The age of issued key in minutes (m) or days (d).
- **Encryption** – The tunnel encryption method.
- **Duration** – Displays how long the tunnel is up and running.
- **Idle** – The time (in seconds) passed since the last activity within the connection.
- **Auth.** – The packet authentication method.
- **Internal** – Information about the tunnel name.
- **TI** – The traffic intelligence transport class IDs.
- **Latency** – The traffic latency (round-trip time) in seconds as measured by Dynamic Bandwidth and Latency Detection.
- **Dynamic Bandwidth State Local** – Last Dynamic Bandwidth and Latency Detection probing state for the firewall acting as the local VPN endpoint.
- **Dynamic Bandwidth State Peer** – Last Dynamic Bandwidth and Latency Detection probing state for the remote firewall.
- **Effective Bandwidth Inbound [bit/s]** – Effective bandwidth of inbound traffic in bits per second as measured by Dynamic Bandwidth an Latency Detection.
- **Effective Bandwidth Outbound [bit/s]** – Effective bandwidth of outbound traffic in bits per second as measured by Dynamic Bandwidth an Latency Detection.
- **Dynamic Bandwidth Detection** – This column shows if Dynamic Bandwidth and Latency Detection is enabled for the VPN transport.

To reset the columns to default, select **Default Columns**.

Context Menu

To open the context menu, right-click a VPN tunnel.

The following operations can be selected:

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

- (TINA only) **Last VPN Access** – Opens a window with a detailed VPN access and connection history.
- (TINA only) **Monitor Traffic** – Provides two monitors for Traffic Intelligence SD-WAN features for TINA UDP transports.
- (TINA only) **Trigger Active Probing** – Initiates probing for TINA UDP transports for which **Bandwidth and Latency Detection** is enabled..
- **Show VPN Run-Time Info** – Opens a window with details for the VPN service this VPN tunnel is using.
- **Show Sessions** – Displays information about the VPN sessions.
- **Show on Status Page** – Opens the VPN **Status** window and highlights the corresponding VPN tunnel.
- **Enable Tunnel** – Enables the selected VPN tunnel or transport.
- **Temporary Enable Tunnel** – Enter the desired time period in minutes for which the VPN tunnel or transport should be enabled.
- **Disable Tunnel** – Permanently disables the selected VPN tunnel or transport. Use **Enable Tunnel** to re-enable the VPN tunnel or transport.
- **Initiate Tunnel** – Manually re-establishes the selected VPN tunnel.
- (TINA only) **Terminate Tunnel** – This method kills Phase2 of the IPsec tunnel. Phase2 is re-initialized immediately.
- (IPsec only) **Terminate Phase 1** – 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.

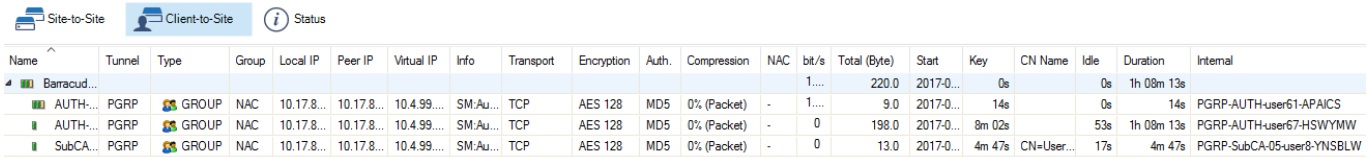
  Do not use the **Terminate Phase 1** function unless it is absolutely necessary. In case of doubt, please contact Barracuda Networks Technical Support to get assistance.
  After terminating Phase1, the tunnel can be re-initiated either manually or with the next re-keying.
- (IPsec only) **Terminate Phase 2** – This method kills Phase2 of the IPsec tunnel. Phase2 is re-initialized immediately.

For more information about the standard context menu, see Barracuda Firewall Admin.

Client-to-Site

The **Client-to-Site** page lists all client-to-site VPN tunnels configured on the firewall.

Go to **VPN > Client-to-Site**.



The standard columns in the table provide the following information:

- **Name** – The name of the VPN tunnel.
- **Tunnel** – The type of VPN tunnel, either PGRP, PPTP, L2TP, or IPsec.
- **Local IP** – The local VPN point of entry.
- **Peer IP** – The remote VPN point of entry.
- **Virtual IP** – The assigned virtual IP address.
- **Transport** – The VPN tunnel transport protocol.
- **Encryption** – The tunnel encryption method.
- **Compression** – The current compression rate and type of VPN tunnel.
- **bit/s** – The current transfer speed in bits per second.
- **Start** – The duration of VPN connection in minutes (m) or days (d).

To show or hide additional columns, right-click in the window, select **Columns**, and then select or unselect the columns you want displayed or hidden.

The following additional columns are available:

- **Type** – The type of network used for the VPN client.
- **Group** – The group that the logged-in VPN user belongs to.
- **Info** – Either a person's name (defined during configuration) and an IP address assigned by the license, separated by "@" (the "at" character), or the certificate subject.
- **Auth.** – The packet authentication method.
- **NAC** – Displays information if the VPN tunnel is established by the Barracuda Network Access Client.
- **Total (Byte)** – The total amount of traffic.
- **Key** – The age of issued key in minutes (m) or days (d).
- **CN Name** – Displays the certificate CN name.
- **Idle** – The time (in seconds) passed since the last activity within the connection.
- **Duration** – How long the tunnel is up and running.
- **Internal** – Information about the tunnel name.

For more information about the standard context menu, see Barracuda Firewall Admin.

Context Menu

To open the context menu, right-click on a VPN tunnel.

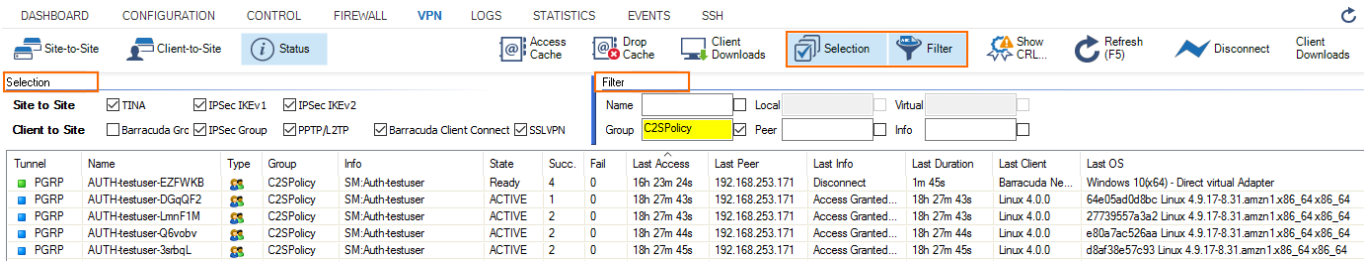
The following operations can be selected:

- **Show Transport Details** – Opens a window with detailed information about the selected VPN transport.
- **Show VPN Run-Time Info** – Opens a window with details for the VPN service this VPN tunnel is using.

- **Show Sessions** – Displays information about the VPN sessions.
- **Show on Status Page** – Opens the VPN **Status** window and highlights the corresponding 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.

Filter Options

The **VPN** page provides several filtering options.



Click the **Selection** icon to open the **Selection** menu, which provides the following options:

- **Site to Site** – Select the following options to filter for site-to-site tunnels:
  - **TINA** – Allows a filter to be set for TINA tunnels.
  - **IPSec IKEv1** – Allows a filter to be set for IPSec IKEv1 tunnels.
  - **IPSec IKEv2** – Allows a filter to be set for IPSec IKEv2 tunnels.
- **Client to Site** – Select the following options to filter for client-to-site tunnels:
  - **Barracuda Group** – Allows a filter to be set for Barracuda Group tunnels.
  - **IPSec Group** – Allows a filter to be set for IPSec tunnels.
  - **PPTP/LTPD** – Allows a filter to be set for PPTP/LTPD tunnels.
  - **Barracuda Client Connect** – Allows a filter to be set for Barracuda Client Connect tunnels.
  - **SSL VPN** – Allows a filter to be set for SSL VPN tunnels.

Click the **Filter** icon in the ribbon bar to open the **Filter** menu, which provides the following options:

- **Name** – Allows a filter to be set for a specific tunnel name.
- **Group** – Allows a filter to be set for a specific VPN group.
- **Local** – Allows a filter to be set for the local tunnel IP address.

- **Peer** – Allows a filter to be set for the local tunnel peer IP address.
- **Virtual** – Allows a filter to be set for a virtual server IP address.
- **Info** – Allows a filter to be set for content in the **Info** column.

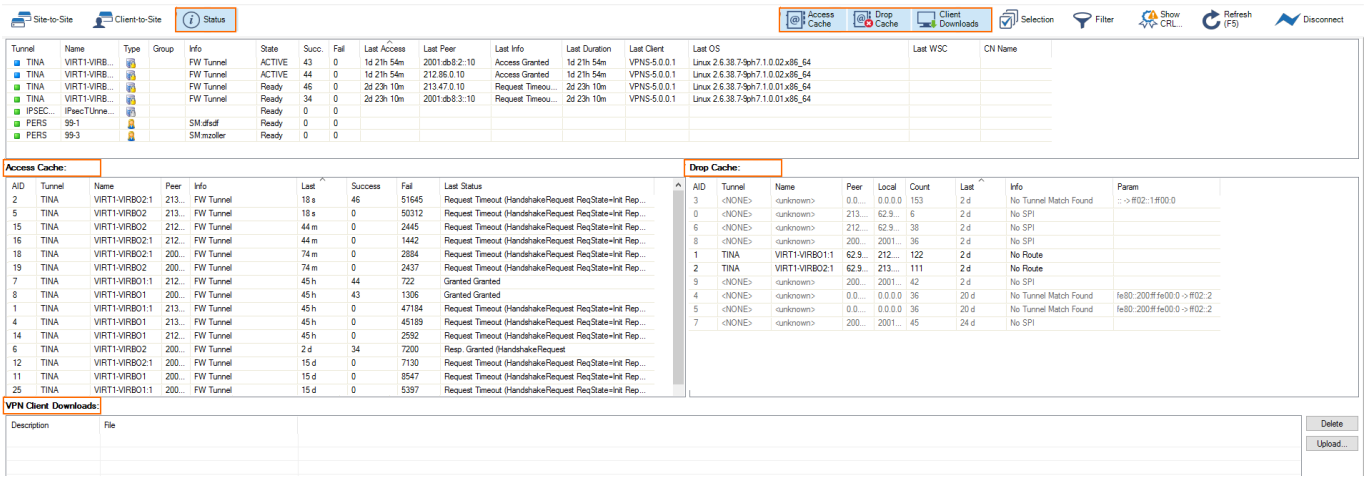
To apply a filter and / or selection, click the **Refresh** icon on the top right of the service bar.

Status

The **Status** page lists all configured VPN connections on the given system. It consists of four sections, which you can access via the main screen or by clicking the corresponding icons in the ribbon bar:

- Status section
- Access Cache section
- Drop Cache section
- VPN Client Downloads section

Go to **VPN > Status**.



Status Section

The Status section is the upper section of the **Status** page and lists the status of all configured VPN tunnels (site-to-site, client-to-site, and SSL VPN).

The table provides the following information:

- **Tunnel** – The description of the VPN tunnel.
- **Name** – The name of the VPN tunnel.
- **Type** – The type of the VPN tunnel.
- **Group** – The group that the VPN tunnel belongs to.

- **Info** – (optional) Displays additional information.
- **State** – The status of the VPN connection (ACTIVE, Ready, or Disabled).
- **Succ.** – The number of successful connections.
- **Fail** – The number of failed connections.
- **Last Access** – The time passed since the last access.
- **Last Peer** – The client IP address of the last connection.
- **Last Info** – The most recent information concerning the connection (e.g., Access Granted, Disconnect, etc.).
- **Last Duration** – The duration of the last connection.
- **Last Client** – The client (including version number) used for the last connection.
- **Last OS** – The operating system (including kernel number) used by the last connection's client.
- **Last WSC** – The WSC information.
- **CN Name** – The certificate CN name.

To enable, disable, or temporarily enable a tunnel, right-click a connection. The context menu opens. You can then select the option you need. If selecting "Temporarily Enable Tunnel", enter the period (in minutes) for which the tunnel should be enabled.

For each entry in the **Status** section, colored icons indicate the current status of a VPN tunnel:

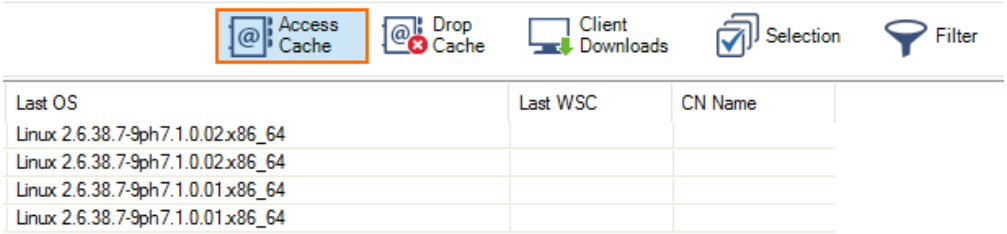
- **green** – Tunnel is terminated, but ready.
- **blue** – Tunnel is active.
- **gray** – Tunnel is disabled.

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

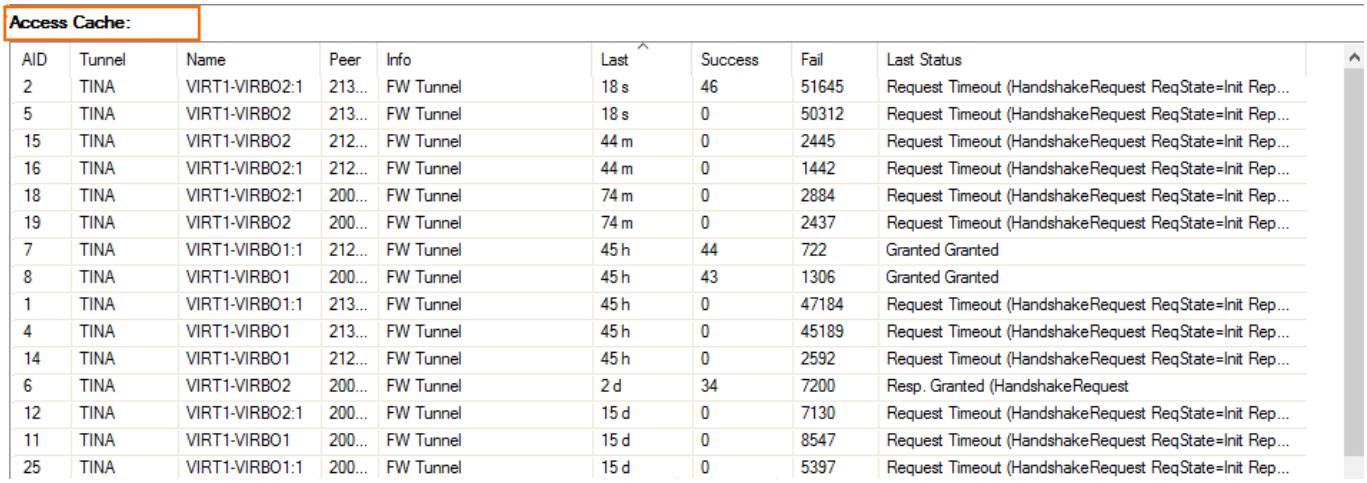
- **1 user** – Personal VPN tunnel.
- **2 users** – Group VPN tunnel.
- **Server lock** – Firewall-to-firewall VPN tunnel.
- **User global** – SSL VPN tunnel.

Access Cache Section

The **Access Cache** section displays the history of successful VPN connection attempts for site-to-site, client-to-site, and SSL VPN connections. To open the **Access Cache** section, click the **Access Cache** icon in the ribbon bar.



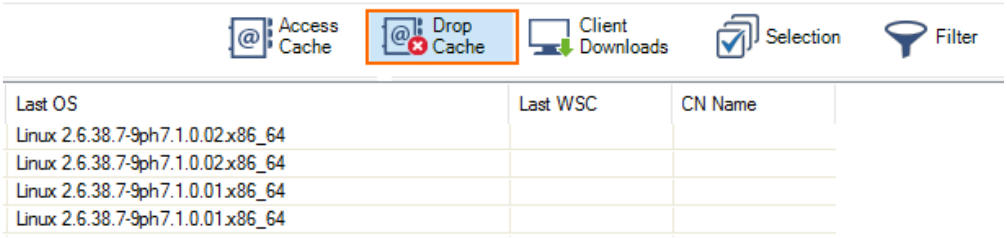
Double-click a specific VPN tunnel for detailed information.


Access Cache:

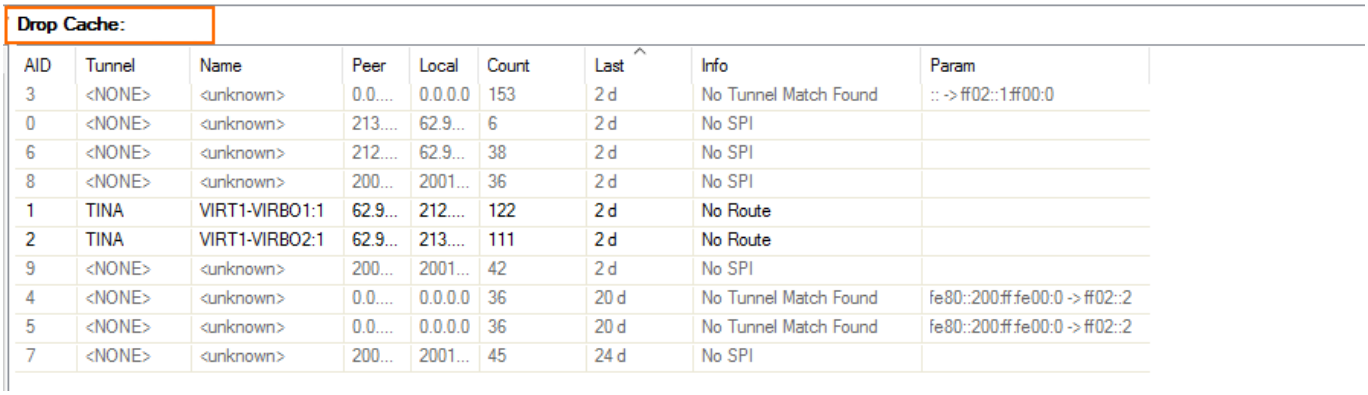
AID	Tunnel	Name	Peer	Info	Last	Success	Fail	Last Status
2	TINA	VIRT1-VIRBO2:1	213...	FW Tunnel	18 s	46	51645	Request Timeout (HandshakeRequest ReqState=Init Rep...
5	TINA	VIRT1-VIRBO2	213...	FW Tunnel	18 s	0	50312	Request Timeout (HandshakeRequest ReqState=Init Rep...
15	TINA	VIRT1-VIRBO2	212...	FW Tunnel	44 m	0	2445	Request Timeout (HandshakeRequest ReqState=Init Rep...
16	TINA	VIRT1-VIRBO2:1	212...	FW Tunnel	44 m	0	1442	Request Timeout (HandshakeRequest ReqState=Init Rep...
18	TINA	VIRT1-VIRBO2:1	200...	FW Tunnel	74 m	0	2884	Request Timeout (HandshakeRequest ReqState=Init Rep...
19	TINA	VIRT1-VIRBO2	200...	FW Tunnel	74 m	0	2437	Request Timeout (HandshakeRequest ReqState=Init Rep...
7	TINA	VIRT1-VIRBO1:1	212...	FW Tunnel	45 h	44	722	Granted Granted
8	TINA	VIRT1-VIRBO1	200...	FW Tunnel	45 h	43	1306	Granted Granted
1	TINA	VIRT1-VIRBO1:1	213...	FW Tunnel	45 h	0	47184	Request Timeout (HandshakeRequest ReqState=Init Rep...
4	TINA	VIRT1-VIRBO1	213...	FW Tunnel	45 h	0	45189	Request Timeout (HandshakeRequest ReqState=Init Rep...
14	TINA	VIRT1-VIRBO1	212...	FW Tunnel	45 h	0	2592	Request Timeout (HandshakeRequest ReqState=Init Rep...
6	TINA	VIRT1-VIRBO2	200...	FW Tunnel	2 d	34	7200	Resp. Granted (HandshakeRequest
12	TINA	VIRT1-VIRBO2:1	200...	FW Tunnel	15 d	0	7130	Request Timeout (HandshakeRequest ReqState=Init Rep...
11	TINA	VIRT1-VIRBO1	200...	FW Tunnel	15 d	0	8547	Request Timeout (HandshakeRequest ReqState=Init Rep...
25	TINA	VIRT1-VIRBO1:1	200...	FW Tunnel	15 d	0	5397	Request Timeout (HandshakeRequest ReqState=Init Rep...

Drop Cache Section

The **Drop Cache** section shows details about unsuccessful VPN connection attempts. To open the **Drop Cache** section, click the **Drop Cache** icon in the ribbon bar.



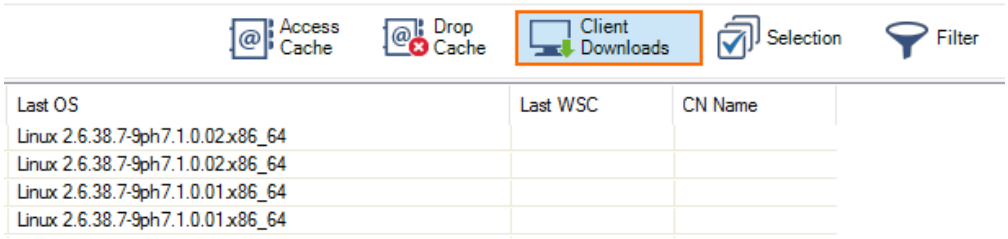
Last OS	Last WSC	CN Name
Linux 2.6.38.7-9ph7.1.0.02.x86_64		
Linux 2.6.38.7-9ph7.1.0.02.x86_64		
Linux 2.6.38.7-9ph7.1.0.01.x86_64		
Linux 2.6.38.7-9ph7.1.0.01.x86_64		


Drop Cache:

AID	Tunnel	Name	Peer	Local	Count	Last	Info	Param
3	<NONE>	<unknown>	0.0....	0.0.0.0	153	2 d	No Tunnel Match Found	:: -> ff02::1:ff00:0
0	<NONE>	<unknown>	213....	62.9...	6	2 d	No SPI	
6	<NONE>	<unknown>	212....	62.9...	38	2 d	No SPI	
8	<NONE>	<unknown>	200...	2001...	36	2 d	No SPI	
1	TINA	VIRT1-VIRBO1:1	62.9...	212....	122	2 d	No Route	
2	TINA	VIRT1-VIRBO2:1	62.9...	213....	111	2 d	No Route	
9	<NONE>	<unknown>	200...	2001...	42	2 d	No SPI	
4	<NONE>	<unknown>	0.0....	0.0.0.0	36	20 d	No Tunnel Match Found	fe80::200:ff:fe00:0 -> ff02::2
5	<NONE>	<unknown>	0.0....	0.0.0.0	36	20 d	No Tunnel Match Found	fe80::200:ff:fe00:0 -> ff02::2
7	<NONE>	<unknown>	200...	2001...	45	24 d	No SPI	

VPN Client Downloads Section

The **VPN Client Downloads** section allows you to copy Network Access Client update files to the firewall. To open the **VPN Client Downloads** section, click the **Client Downloads** icon in the ribbon bar. Please note that this feature is limited to the Barracuda Network Access Client and is not available with the Barracuda VPN Client only.



The next time a Network Access Client connects to the VPN server, you can download the uploaded version:

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 CloudGen Firewall.

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

Figures

1. vpn_s2s1.png
2. vpn_c2s.png
3. filter_select.png
4. vpn_status.png
5. ac_icon.png
6. vpn_ac.png
7. dc_icon.png
8. vpn_dc.png
9. cd_icon.png