Troubleshooting

https://campus.barracuda.com/doc/75696495/

This page helps you solve some common issues concerning the Barracuda Network Access and VPN Client.

Issue: Connection errors shown in the Barracuda Health Agent

The Access Control Server cannot be reached at the IP addresses configured for health evaluation. A **Connection Error** message is shown in the Health Agent.

Solution

Configure a valid Access Control Server IP address locally. If the Access Control Server IP addresses are distributed by DHCP, use the operating system's built-in `ipconfig` tool to obtain a new IP address for the client computer that will include an Access Control Server IP address to connect to.

In order to verify whether an Access Control Server IP address was received through DHCP, look up the Barracuda Health Agent Access Control Server IPs dialog.

Issue: E_PENDING 0x8000000A The data necessary to complete the operation is not yet available.

Initialization of the Personal Firewall service takes very long, and thus the system's health state cannot be validated.

Debug Log output:

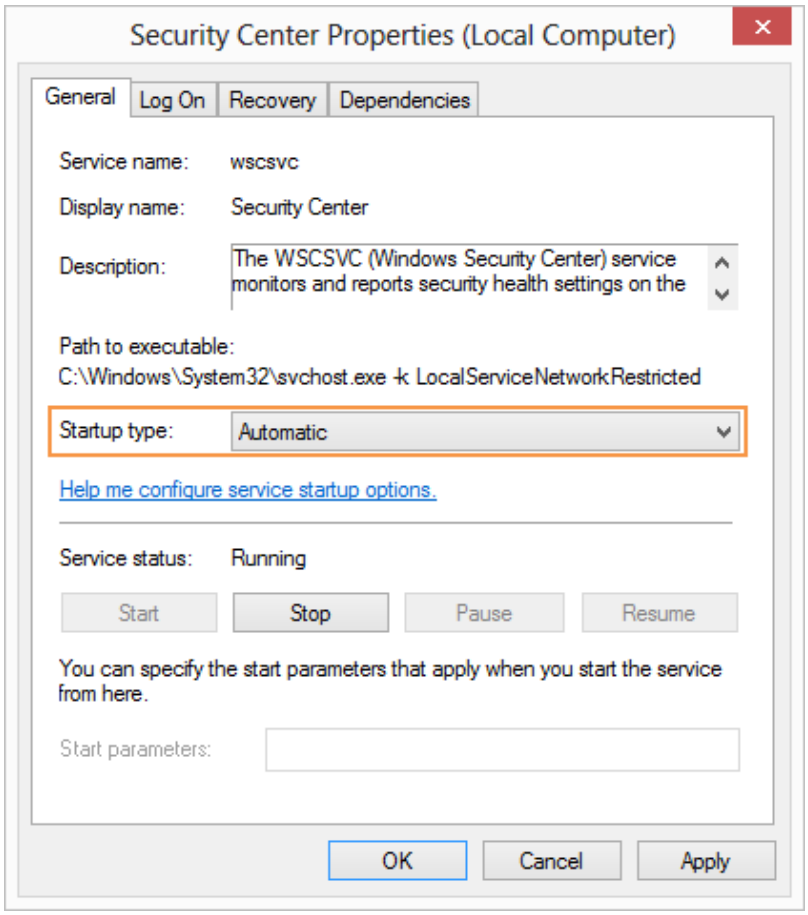
- `WMIXP2SecureCenter2.cpp(863)* Register FW Status Provider`
- `WMIXP2SecureCenter2.cpp(62)* RegisterFWStatusProvider`
- `WMIXP2SecureCenter2.cpp(112)* QueryInterface for Register failed Error: 0x8000000a`
- `WMIXP2SecureCenter2.cpp(870)* RegisterFWStatusProvider failed. wait 1000 ms...(0)`

Solution

The Personal Firewall's API registration takes too long because the required MS Windows Security Center service (WSCSVC) is not yet started. By default, MS Windows starts the WSCSVC service with

startup type: *Automatic (delayed Start)*

Set the **Startup type** value of WSCSVC to **Automatic**.



Issue: Connection to VPN server breaks immediately after establishing

Solution

An access ruleset may have been damaged during transfer from the VPN server to the client. Disconnect all applications and connect again to solve the issue. This behavior may also occur with slow connections. Increase the **Connect Timeout** parameter in the VPN Profile settings **Connect/Reconnect** tab if you encounter any problems.

Issue: Connection breaks if IP address assignment via DHCP is used

Solution

A connection problem occurs when the firewall slot is closed too early. Create a local firewall ruleset to solve the issue: **Action: Pass, Service: BOOTPS (out: UDP 67; in: UDP 68)**.

Issue: VPN Gateway not reachable via VPN tunnel is logged into the Events window

Solution

Open the **VPN Settings** tab and change the value for **Virtual Adapter Address Assignment (IPv4)**.

Issue: Session PHS: signature check failed (bad decrypt) is logged into the Events window

Solution

Deactivate **Private Encrypt** (see **Connection Entries > X.509 Authentication** above).

Issue: A VPN connection cannot be not established due to a Firewall Status mismatch error

The VPN Service on the CloudGen Firewall drops incoming connection requests by a Barracuda Network Access Client and generates the following error message in the VPN log:

- `Warning Session PGRP-AUTH-user01:`
- `reply unsuccesful handshake:`
- `100 36 Firewall Status mismatch`

Solution

Older Barracuda Network Access Client versions cannot interpret the VPN Service's **Firewall Always ON** Option, which therefore effectively prevents connection establishment for these clients.

To allow these older clients to connect to the VPN service, navigate in Barracuda Firewall Admin to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Client to Site > External CA > Group Policy** and clear the **Firewall Always ON** check box.

Issue: VPN Client cannot open a connection due to a timeout

The Barracuda Network Access Client breaks the VPN connection and generates the following error message in the client log:

- `Could not connect to serverConnectLib,`
- `Open() failed: could not open DIRECT connection,`
- `IOStreamSock: Connect(x.x.x.x:691): TIMEOUT`
- `Error while connect to x.x.x.x:691 (proto=TCP)`

Solution

This message appears only if the server's IP address is reachable, but at the same time no listen port (UDP/TCP 691) is available.

The VPN Service listens by default on the first and the second server IP address. For additional server IP addresses, it is necessary to bind the service manually to these additional IP addresses. In the CloudGen Firewall, navigate to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Access Control Service > Service Properties > Service Availability** in order to achieve this.

Issue: VPN Adapter has been removed after a Windows update

After installing certain updates to Windows 10 (e.g., upgrading to Windows 10 1809), the VPN Client is no longer able to establish a VPN connection because the "Barracuda Virtual Adapter" does not get migrated by Windows (see also %WINDIR%\INF\setupapi.dev.log), even though the driver has been fully certified for the corresponding version of Windows 10 as part of the Windows Hardware Compatibility Program.

As the “Barracuda Virtual Adapter” is a **virtual** (non-physical) network device, it will not get detected automatically and needs to be re-installed manually.

Solution

To fix the issue and to re-install the Virtual Adapter, run the following command:

For NAC 5.3.x:

- `msiexec.exe /fvomus {C222B45D-E81A-41E0-932D-6A6CFB21E817} /Lecumwvariox setup.log`

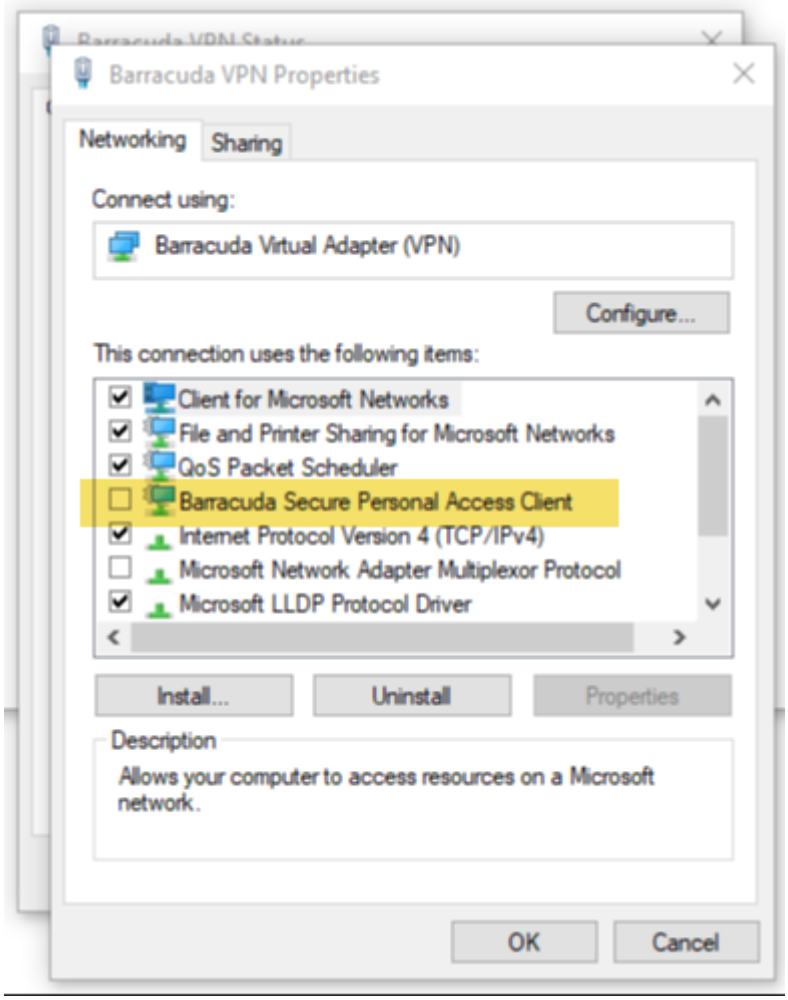
You may also choose **Troubleshooting > Repair VPN Adapter** from the tray icon menu instead.

Issue: VPN Client does not show routes or Virtual Adapter

When installed or updated, the VPN Client 5.1.x connects, but either there are no VPN routes or there is no Virtual Adapter shown as confirmed by `ipconfig/all` (Windows), or (on VPN Client 5.2.0) the client cannot connect due to the status error "Timeout waiting for Virtual Adapter".

Solution

- In the **Barracuda VPN Properties**, ensure that the entry **Internet Protocol Version 4 (TCP/IPv4)** is selected.
- Check for the presence of the Secure Personal Access Client (SPAC). If present, uninstall it from the Barracuda Virtual Adapter.



Figures

1. WSCSVC-Startup-type.png
2. sp_va.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.