Operation and Monitoring

https://campus.barracuda.com/doc/75696484/

The Barracuda Network Access Client implements a client-server-based access control and authentication process preventing unauthorized clients from connecting to a LAN through publicly accessible ports unless they are authenticated. The credentials for authentication are obtained by the client computer from the Access Control Service, based on the client computer's health evaluation result, restricting or granting network access to the client computer. Policies, such as applicable firewall ruleset or access rights, can be machine-specific, and must be selected according to both identity and system health state.

The Barracuda Network Access Client's policy matching capabilities include:

- ID-based policies and support for ID-based exemptions (health condition and/or software update)
- Date and time conditions
- Access type (internal and external category supported)
- Separate machine and quarantine policies
- Machine properties (Microsoft operating system time, Microsoft SID, x.509 certificate for LocalMachine account with subject, issues, alt name conditions, host name, MAC address, network ACL, NetBIOS name)
- User properties (all of the above plus login name and work group affiliation)
- Antivirus (AV) and AntiSpyware realtime protection status and update
- Personal firewall ruleset (not available for Barracuda VPN Client)
- Registry entries (not available for Barracuda VPN Client)
- Gateway network access roles

For more information, see: Network Access Client Monitoring on the CloudGen Firewall

The Barracuda Health Agent

The Barracuda Health Agent is the key component of the Barracuda Network Access Client. This software is responsible for sending the endpoint health status to the Access Control Service for baselining. Health Agent access monitors are dynamically downloaded and updated as required, supporting same full and delta updates. They are extremely light, only occupying 340 KB in memory.

For more information, see: How to Use the Barracuda Health Agent.

The Barracuda Personal Firewall

Being a centrally managed host firewall, the Barracuda Personal Firewall can handle up to four different firewall rulesets at once. Which rulesets are available to the firewall engine and which one of these is currently enforced depends on the policy applicable to user, machine, date, and time.

For more information, see: How to Use the Barracuda Personal Firewall.

The Barracuda VPN Client

The Barracuda VPN client establishes a secure connection to a VPN service. The Health Agent then communicates through the VPN tunnel with the responsible System Health Validator (SHV). After installing and configuring the Barracuda VPN Client, you can initiate VPN connections with the settings from your configured VPN profiles. For more information, see:

- How to Establish a VPN Connection Using Barracuda VPN Client for Windows
- How to Establish a VPN Connection Using Barracuda VPN Client for macOS
- How to Establish a VPN Connection Using Barracuda VPN Client for Linux

© 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.