# Getting Started

https://campus.barracuda.com/doc/75696481/

The Barracuda VPN Client secures mobile desktops connecting to the corporate LAN through the Internet. With the Barracuda VPN Client, you can set up TINA client-to-site VPNs, the Barracuda Networks proprietary VPN protocol. TINA offers a secure end-to-end solution that does not require additional third-party software or input. The Barracuda Network Access Client provides enhanced protection against malicious software and attackers, improved network access control for employees and guests, superior resource usage tracking, and a powerful policy adherence mechanism. The Barracuda Network Access Client offers access control, using a combination of client-agent-based and DHCP-based address assignment. Policies, such as applicable access rulesets or access rights, are selectable according to both client identity and system health state. For a general understanding of the client-server interaction processes, health states, and rules selection, see Rules and Policy Matching.

## Before You Begin

- Establishing client-to-site VPN connections using the Barracuda VPN Client requires a working client-to-site VPN configuration on the firewall. For instructions on how to set up a Barracuda VPN on the Barracuda CloudGen Firewall, see:
  - How to Configure a Client-to-Site TINA VPN with Personal Licenses.
  - Example - Client-to-Site TINA VPN with Client Certificate Authentication.

  For instructions on how to set up a Barracuda VPN on the Barracuda NextGen Firewall X-Series, see Client-to-Site VPN.
- Before configuring the Barracuda Network Access Client, you must introduce the Access Control Service on your CloudGen Firewall. For more information, see Access Control Service.

## Configure the Barracuda VPN Client

Configure your VPN settings and create VPN profiles on the Barracuda VPN Client. The client establishes a secure connection to the VPN service on the firewall. The Barracuda Health Agent then communicates through the VPN tunnel with the responsible System Health Validator (SHV). In this case, the VPN server fully controls the virtual connection.

For instructions on how to configure the Barracuda VPN Client for Windows, macOS, or Linux, see:

- How to Configure the Barracuda VPN Client for Windows
- How to Configure the Barracuda VPN Client for macOS
- How to Configure the Barracuda VPN Client for Linux

## Configure the Barracuda Network Access Client

The Barracuda Network Access Client consists of client software components and server-side components that the client software periodically communicates with in order to have the health state of its underlying operating system verified and its network access rights assessed. Barracuda firewalls can interpret that information and subsequently allow or deny network access attempts by the respective client. Access policies can be machine-specific, based on address context, and can contain ID-based exceptions. Client system health assessments are carried out prior to initial connection to the network, and periodically afterwards, to detect changes in the client health state.

The Barracuda Network Access Client software consists of the following subsystems:

#### Barracuda Health Agent

This software is responsible for sending the endpoint health status to the Access Control Service for baselining. Barracuda Health Agents are dynamically downloaded and updated as required, supporting the same full and delta updates. They are extremely light, occupying only 340 KB in memory. For more information, see: How to Use the Barracuda Health Agent and How to Configure the Barracuda Health Agent.

#### Barracuda Personal Firewall

Being a centrally managed Host Firewall, this advanced firewall engine 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 Configure the Barracuda Personal Firewall.

#### Barracuda VPN Client

The VPN Client establishes a secure connection to the VPN service on the CloudGen Firewall. The Barracuda Health Agent then communicates through the VPN tunnel with the responsible System Health Validator (SHV). In this case, the VPN server fully controls the virtual connection. The Barracuda VPN Client can be implemented together with the Network Access Client, or separately, for Windows, macOS, and Linux.

## VPN Client Integration with CudaLaunch

VPN connections can be initiated directly in the VPN client interface and also in CudaLaunch by clicking a VPN group policy in the **VPN Connection** tab. The VPN group policy must be made available to the user by the admin of the SSL VPN service.

For more information, see CudaLaunch and CudaLaunch for Windows and macOS.