Overview

https://campus.barracuda.com/doc/75696486/

The Barracuda Network Access and VPN clients provide an effective and cost-efficient end-user solution that combines administered remote endpoint security with a network access control (NAC) framework without the need to implement major changes to your existing network infrastructure. The Barracuda Network Access Client integrates with the Access Control service of the Barracuda CloudGen Firewall and lets you configure access policies and rules depending on various criteria such as identity and client health state. The Barracuda VPN Client lets you configure and establish client-to-site virtual private networks (VPNs) using the stand-alone client or integrated directly in CudaLaunch to allow mobile workers remote access to corporate resources. Suitable server-side functionality is included with the Barracuda CloudGen Firewall.

The Barracuda VPN Client

The Barracuda VPN Client secures remote and mobile desktops connecting to the corporate LAN through the Internet. The VPN Client establishes a secure connection to a VPN service. The Barracuda VPN Client is available for Windows, and as a separate client for macOS and Linux.

The Barracuda Network Access Client

The Barracuda Network Access Client is a suite of applications available for Windows (Windows 7, Windows 8.1, and Windows 10) that lets you control network and VPN client access based on rules and policies.

Access Policies

The Barracuda Network Access Client provides a managed personal firewall solution with periodic health assessments. Both the outcome of the assessment and the identity of the machine and/or current user will influence the policy applicable to the endpoint. The Barracuda Network Access Client lets you easily distinguish between visitors and guest network users and can allow or deny network access attempts based on date and time, identity, health state, and type of network access. For example, different policies can be configured for users that connect from within a corporate network or users that access WLAN hotspots to build a secure VPN connection.

Health Monitoring

The Barracuda Network Access Client consists of client-side (Windows 32-bit or 64-bit) and server-side components that the client software periodically communicates with to have the health state of its underlying operating system verified and its network access rights assessed. The client's health state

is evaluated prior to initial network connection; afterwards, system health assessments are carried out periodically to detect changes.

Available Software Components

The Barracuda Network Access Client contains the following subsystems that can be installed all-in-one or separately:

- **Barracuda Health Agent** – Monitors software and is responsible for sending the endpoint health status to the Access Control Service for baselining. The Barracuda Health Agent Access Monitor is dynamically downloaded and updated as required.
- **Barracuda Personal Firewall** – A centrally managed host firewall that can handle up to four different rulesets at once, depending on the policy applicable to user, machine, date, and time.
- **Barracuda VPN Client** – VPN Client that secures mobile desktops connecting to the corporate LAN through the Internet.

The VPN Client establishes a secure connection to a VPN service. The Barracuda Health Agent then communicates with the responsible System Health Validator (SHV) through the VPN tunnel. In this case, the VPN server fully controls the virtual connection.

Barracuda TINA

With the Barracuda VPN Client, you can set up client-to-site TINA VPNs. TINA is a Barracuda Networks proprietary VPN protocol that offers a secure end-to-end solution without requiring additional third-party software or input. TINA offers substantial improvement over the IPsec protocol, providing:

- High level of security. For supported encryption standards, see Authentication, Encryption, Transport, IP Version and VPN Routing.
- A full-featured Certificate Authority (CA) for TINA VPNs on every Barracuda CloudGen Firewall, for use with self-signed certificates.
- X.509 certificate-based VPN authentication with password request.
- Immunity to NAT or proxy (HTTPS, SOCKS) traversal.

Available Software Components

The following VPN clients are supported for use with Barracuda VPNs:

- **Barracuda VPN Client for Windows** – Standard VPN client that is included with the Barracuda Network Access Client, but can also be installed or uninstalled separately.

Features and Benefits

The Barracuda Network Access and VPN clients offer support for numerous authentication methods

(user/password, X.509, X509 + user/password, LIC files, and SAML), quick restoration of VPN tunnels after dropped connections, 'Always On' VPN connections for PCs, support for redundant VPN gateways, selective routing of network traffic through the tunnel, automatic selection of the optimal VPN gateway based on the client's location, and much more. When using a Barracuda CloudGen Firewall as the VPN gateway, you can also deploy and manage the Windows clients centrally. Every Barracuda CloudGen Firewall includes a root-level Certificate Authority (CA), letting you create, delete, and renew X.509 certificates for strong authentication.

For information on how to configure the Barracuda CloudGen Firewall for client-to-site VPN, see Client-to-Site VPN.

Downloading the VPN Client

Go to the Barracuda Download Portal or visit the Microsoft App Store to download the Network Access and VPN clients for you operating system.

© 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.