DATA SHEET

HPE ARUBA NETWORKING VIRTUAL INTRANET ACCESS CLIENT (VIA)

Secure Remote Network Connectivity

The HPE Aruba Networking Virtual Intranet Access (VIA) client is a secure VPN service for users who need corporate connectivity at home, temporary sites, or while they're mobile.

Available as a software download for Google Android, Apple iOS, MacOS, Linux and Windows, VIA is a hybrid IPsec/SSL VPN client that automatically scans and selects the best, secure connection to terminate traffic destined for public or private workloads. Unlike traditional VPNs which require dedicated hardware, VIA integrates VPN services directly on our existing secure infrastructure to simplify architecture and management.

GOVERNMENT USE CASE

VIA operates under strict adherence to international and U.S. government computer security standards in order to meet or exceed the demands and requirements of national agencies, organizations, and other publicly-funded institutions. Note: this page is updated quarterly. A summary of this information can be accessed here.

VIA ARCHITECTURE

The VIA remote access solution provides secure authenticated remote access to teleworkers to resources on the corporate network over the public Internet. A VPN tunnel is established from an employee's PC or mobile device to a VPN concentrator (VPNC) deployed in a corporate office. The VPN tunnels are used to securely transport traffic between the employee's device and resources in the corporate network.

VPNCs are typically deployed in data centers in the corporate headquarters where the applications and network resources reside.

KEY FEATURES

- Provides VPN connectivity to public or private clouds.
- Delivers Unified management of VPN services with WLAN, and SD-WAN.
- Leverages existing gateways or controllers (physical or virtual) as VPN concentrators.
- Allows users to use their same corporate credentials when authenticating.
- Dynamically apply and enforce policies using ClearPass integration.

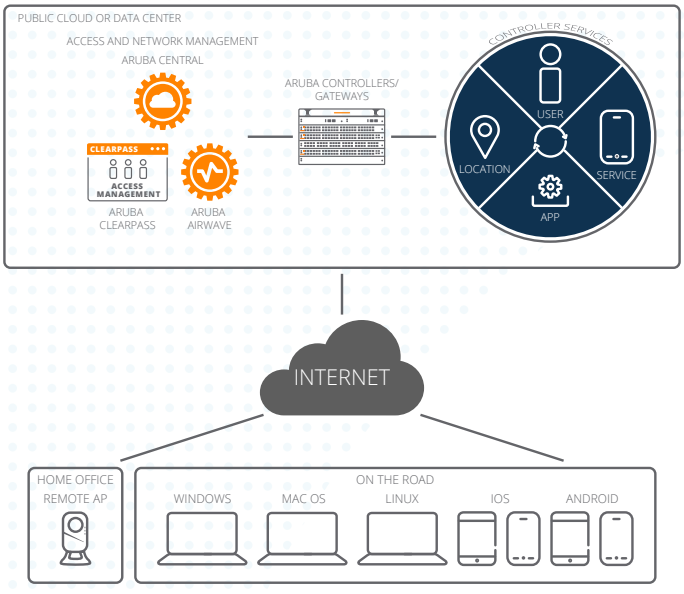

Figure 1. Remote Networking Solution

Each data center (or hub) includes one or more appliance-based or virtual VPNC depending on the number of remote access users that need to be supported and redundancy needs. Optionally, Layer 2 redundancy can be provided by installing a second VPNC, if required.

VIA MANAGEMENT

VIA can be managed using cloud-native HPE Aruba Networking Central. VIA provides split and full tunnel connections to an Aruba VPN Concentrator managed by Central, a cloud-based networking solution that empowers IT with AI-powered insights, intuitive visualizations, workflow automation, and edge-to-cloud security to manage campus, branch, remote, data center, and IoT networks from one dashboard. VIA can also be managed using HPE Aruba Networking AirWave.

AUTOMATIC IPSEC CONNECTIONS

Frequent business travelers often connect through hotels, airports, coffee shops, cellular networks, which require secure links to access internal corporate resources. Legacy VPNs often require users to start additional software and undergo a complicated login process.

However, Aruba VIA is completely Wi-Fi-aware. From a noncorporate network – such as a home WLAN, 5G/LTE, 3G or public Wi-Fi network – VIA automatically launches a VPN-ondemand connection to the data center. Connectivity and authentication occur transparently with no complicated logins.

IPSEC WITH SSL FALLBACK ENCAPSULATION

VIA uses the standard IPsec protocol suite to secure communications between VIA-enabled devices and a VPN concentrator (a gateway or controller). This ensures the fastest connections possible where clients connect via native IPsec. If a firewall blocks direct IPsec connections, VIA can wrap IPsec packets in an SSL header to allow secure connectivity through corporate firewalls.

SEAMLESS SINGLE SIGN-ON EXPERIENCE

The same mobile device credentials that authenticate users to wireless LANs (WLANs) can also be used to authenticate VIA users. Leveraging these credentials, VIA automatically connects users in the background without prompting them for a username and password.

When coupled with the automatic connection capability, users get a consistent connection and authentication experience without changing their work habits. Organizations that require additional authentication methods can employ traditional user name and password or token schemes.

EXTENDED ROLE-BASED ACCESS

VIA client software leverages the same role-based and stateful firewall policies for local and remote network access to ensure a consistent end-user experience, regardless of location. It can also be configured to allow separate access roles and policies on the same end point, depending on where the user logs into the network.

EXTENSIVE TROUBLESHOOTING SUPPORT

VIA's built-in logging and diagnostic capabilities enable remote troubleshooting of connectivity issues without requiring users to navigate through a complex set of tools. If required, client logs can be emailed to support teams for more detailed troubleshooting. The diagnostic tools include connection logs, system info, detected WLAN networks, and detailed connectivity tests.

SECURITY PROTOCOLS SUPPORTED

- Encryption: AES-GCM-256, AES-GCM-128, AES256, AES192, AES128, 3DES
- Hash: SHA2-384-192, SHA2-256-128, SHA-384, SHA-256, SHA1-96
- Authentication: Pre-shared Key, RSA, RSA & ECDSA, Smart Card
- Diffie-Hellman Group: Group 1, Group 2, Group 14, ECDH Group 19, ECDH Group 20
- IPSec KEv2, IKEv1, IKEv1 with XAUTH

AUTHENTICATION OPTIONS

- Username/password and certificate multi-factor authentication
- Smart card

FORWARDING MODES

- Tunnel mode: All traffic terminates on an Aruba controller.
- Split-tunnel mode: Non-corporate (e.g. Internet-bound) traffic bypasses the controller directly to its destination.

SUPPORTED CLIENT OPERATING SYSTEMS

Refer to VIA release notes for client OS support.

HARDWARE REQUIREMENTS

- Minimum 1GHz 64-bit processor
- 2 GB of RAM
- 250 MB of available drive space

SUPPORTED GATEWAYS AND CONTROLLERS

- Virtual Gateways
- 9000 Series
- 7200 Series
- 7000 Series
- 6000 with M3 controller module
- 3000 Series
- 600 Series

CERTIFICATIONS

For a full set of certifications, including common criteria see: https://www.arubanetworks.com/solutions/government/certifications/

HOW TO BUY

VIA is included Central licenses for SD-Branch. You can reference the ordering guide here.

In addition, VIA is included with controller policy enforcement firewall (PEF) licenses or it can be ordered on a per user/per session capability: JZ148AAE Aruba LIC-VIA per VIA Client License E-LTU. This license enables per user/session firewall services for VPN termination from Aruba VIA VPN client[1].

[1] PEFV license can also be used for VIA VPN termination. But PEFV is tied to a particular controller and the license capacity scales to the controller user capacity.

On the other hand, LIC-VIA license is per VIA user license and is not tied to any particular controller. It can be transferred from one controller to another. Unlike PEFV, LIC-VIA supports centralized licensing and can be managed by Mobility Conductor or a Conductor Controller in AOS 8.x deployment.

a Hewlett Packard Enterprise company

DS_ArubaVIA_RVK_080523 a00134039enw

Contact us at www.arubanetworks.com/contact