Aruba Virtual Intranet Access Solution Guide for Teleworkers and Home Offices

a Hewlett Packard
Enterprise company

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett Packard Enterprise Company
6280 America Center Drive
San Jose, CA 95002
USA

The following table lists the revisions of this document.

Table 1: *Revision History*

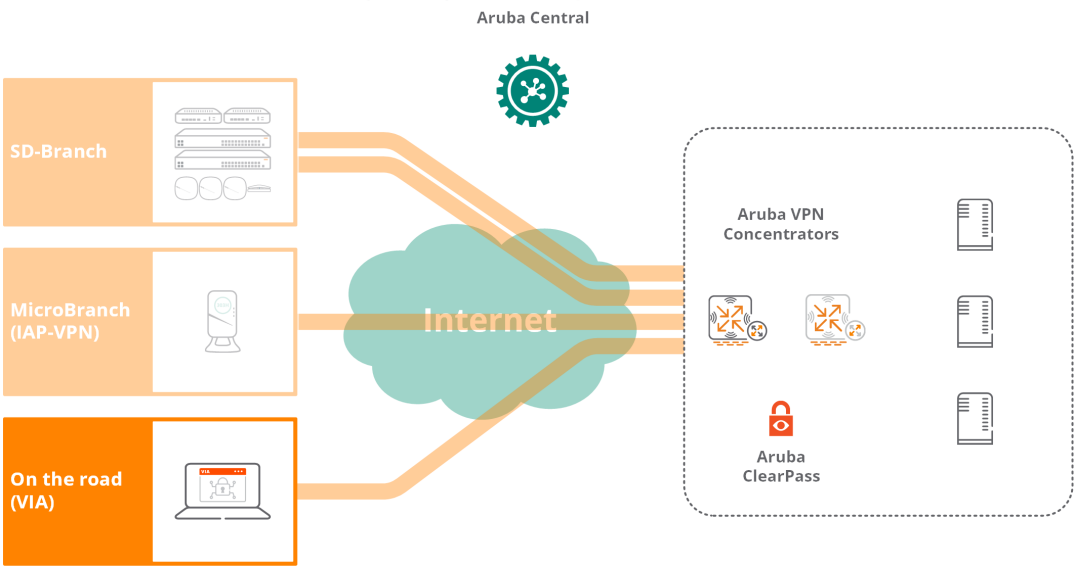
Revision	Change Description
Revision 01	Initial release.

The following topics are discussed in this chapter:

The Aruba SD-Branch solution provides a complete suite of solution for all the needs in a distributed enterprise. From larger branches requiring SD-WAN technology and redundant gateways, as well as the complete cloud-managed LAN or WLAN; to the micro-branches, where the branch network could be built with just an AP. However, SD-WAN and APs cannot be used for secure corporate access from mobile hotspots that provide only wireless access, such as those in airports, hotels, and coffee shops.

To address the demands of the current mobile workforce, which requires corporate access from these mobile hotspots, Aruba leverages the Virtual Intranet Access (VIA) solution. The Aruba VIA solution is designed to provide secure corporate access to employee computers and smart phones from anywhere.

Figure 1 *VIA Solution*



VIA Architecture

The VIA architecture is aligned to that of SD-WAN or IAP-VPN because the same VPN Concentrators (VPNCs) that participate in the SD-WAN networks are capable of terminating tunnels from VIA clients.

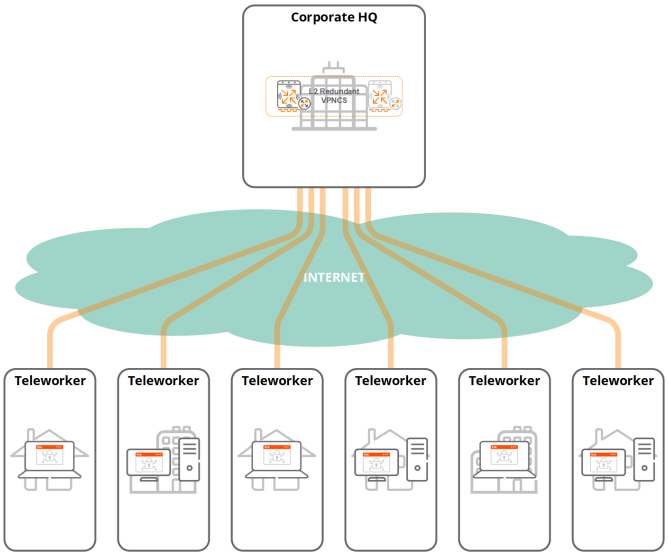
Network Architectures

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 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. Each data center (or hub) consisting of an appliance-based VPNC depending on the number of remote access users that need to be supported and redundancy needs.

All VIA deployments require at least one hub site with a single VPNC installed. Optionally, Layer 2 redundancy can be provided by installing a second VPNC, if required as described in Figure 2.

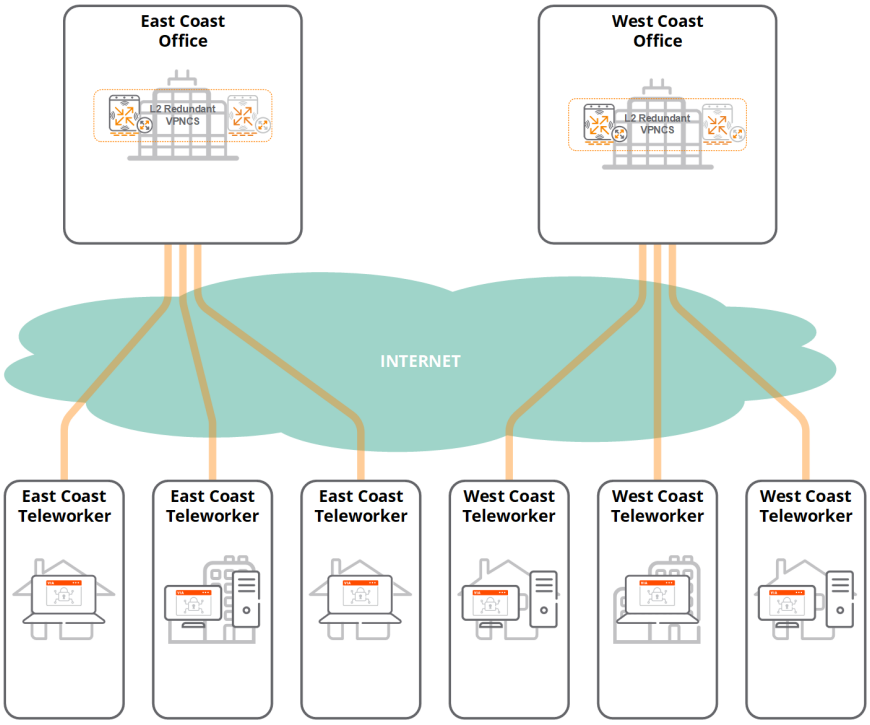
Figure 2 *Single Hub*



Larger VIA deployments generally include multiple hub sites providing additional connection options to teleworkers if the primary hub is unreachable or fails.

A larger VIA deployment may include a secondary hub site or multiple hub sites that are geographically distributed based on teleworker population. Teleworkers connect to their closest hub first and then, to alternative hubs, if the preferred hub is not available.

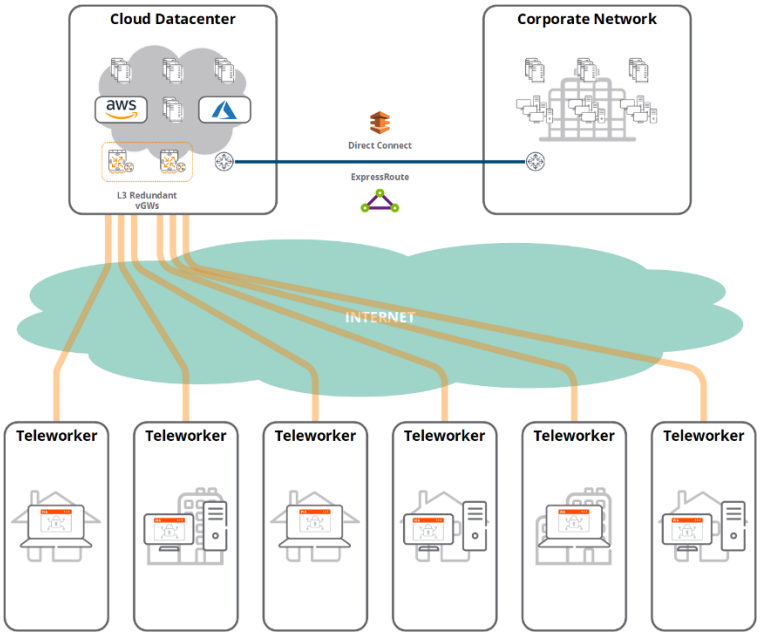
Figure 3 *Multiple Hubs*



A VIA remote access solution may also leverage Virtual Gateways (vGW) deployed in a public cloud environment such as AWS or Azure. The vGW behaves like appliance-based VPNCs in a physical data center but deployed in the customers public cloud environment. A public cloud deployment may consist of a single vGW or multiple

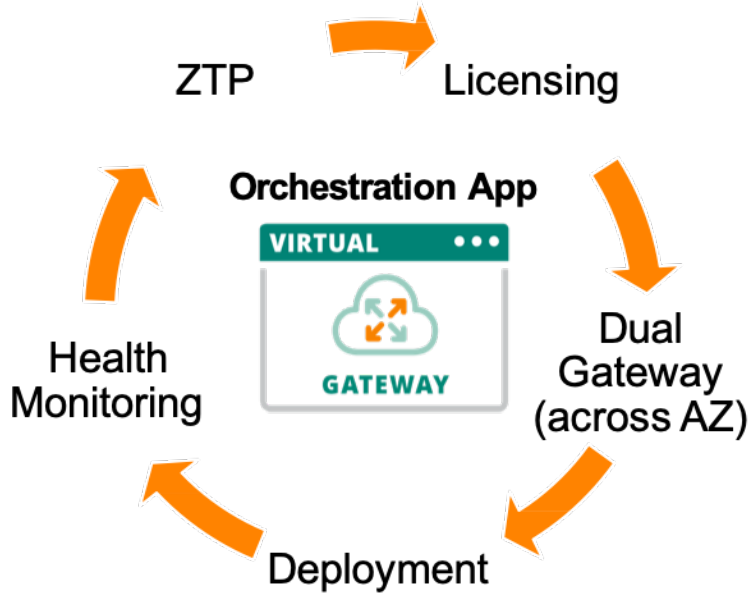
vGWs but unlike physical appliances does not support L2 redundancy. Redundancy is instead provided by distributing vGWs between different Availability Zones (AZ). Figure 4 is an example of a public cloud deployment.

Figure 4 *Public Cloud*



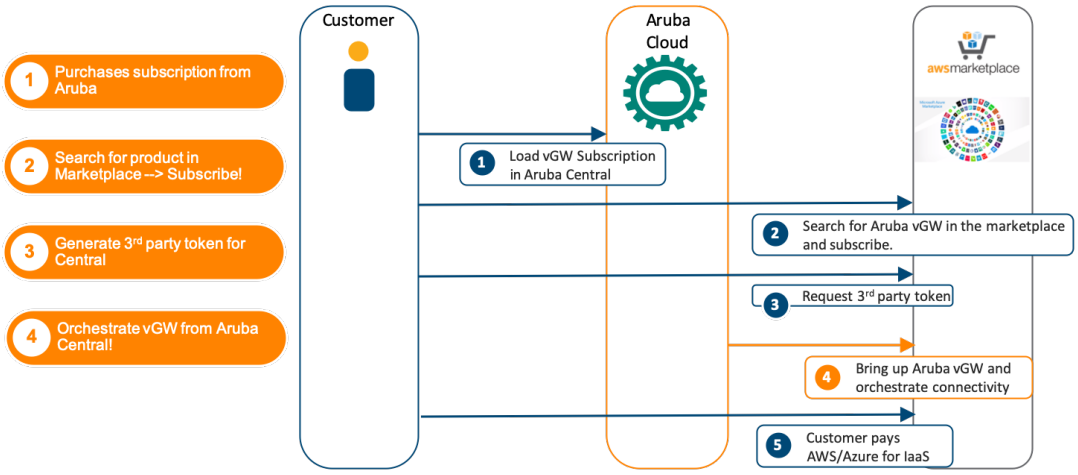
In public cloud environments, Aruba Central can handle the full life cycle of the Aruba Virtual Gateways, that is Aruba VPNCs in AWS or Azure. From the initial bring up and provisioning through the regular management (as if it were another VPNC in the network) to handling failover in HA scenarios.

Figure 5 *Aruba vGW Orchestration*



Therefore, Aruba Central connects to the customer AWS or Azure account to have visibility over it and provision the vGW, together with the necessary interfaces, subnets, elastic-IP mappings, etc. This provides an accelerated mechanism to enable connectivity, as any hardware is not installed in the Data Center and all actions can be done through APIs that are connected from Aruba Central to AWS or Azure.

Figure 6 *Aruba vGW Provisioning*



NOTE

Additional details on vGW Orchestration and Public Cloud integration can be found in *Tech Notes* and *Aruba Central documentation*.

High Availability

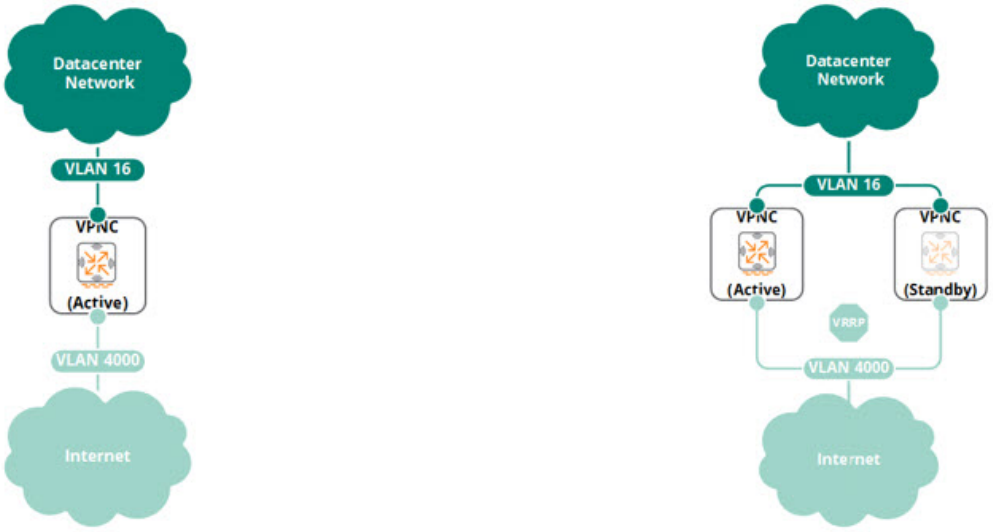
Each hub site can consist of a standalone VPNC or a layer 2 redundant pair of VPNCs. When layer 2 redundancy is enabled, one VPNC operates in an active role while the second VPNC operates in a standby role. The standby

VPNC will become active in the event of an active VPNC failure. Virtual Router Redundancy Protocol (VRRP) provides failover capabilities where the active VPNC is assigned the highest VRRP priority.

NOTE

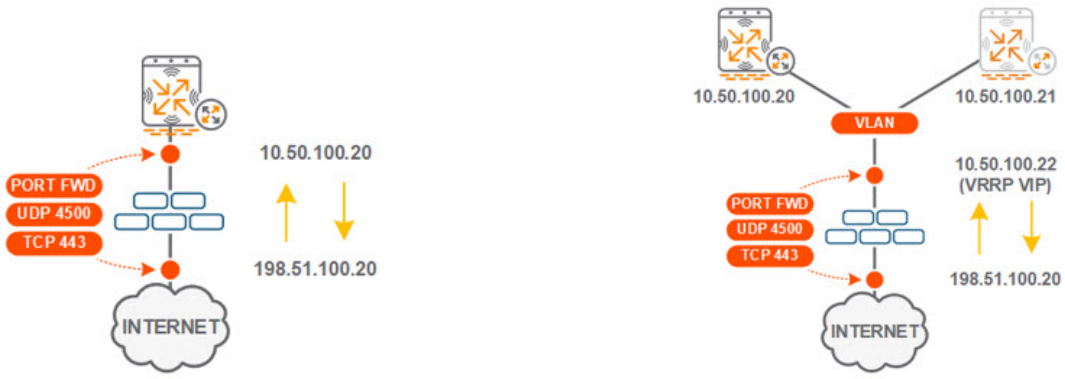
The standby VPNC does not terminate any VPN tunnels or advertise branch routes via OSPFv2 or BGP4 until it transitions to an active state. If a L2 failover occurs, all the VPN tunnels from the VIA clients are torn down and re-established to the standby VPNC (typically 20 – 30 tunnels / second).

Figure 7 *VPNC Redundancy*



When L2 redundant VPNCs are deployed, the VPN tunnels from the VIA clients are terminated on the VRRP virtual IP address rather than the VPNC's actual IP address. The VPNC, that is, the VRRP master terminates the VPN tunnels and forwards the traffic during normal operation. As most VPNCs are deployed behind an Internet edge firewall, a port-forwarding rule is configured to permit UDP 4500 and TCP port 443 traffic from an outside public IP address to the VRRP virtual IP address. An example is shown in figure 8:

Figure 8 *Port Forwarding Examples*



VIA Connection Flowchart

When a remote user connects to a VPNC using the VIA client application, the remote user will go through authentication and download a VPN profile. This will include all the VPN connection information configured under VIA connection profile.

The VPN client will first download the connection profile, which would be cached for future use, and then establish the VPN connection, which will automatically failover between L3 redundant VPN Concentrators and will automatically fallback to SSL when needed.

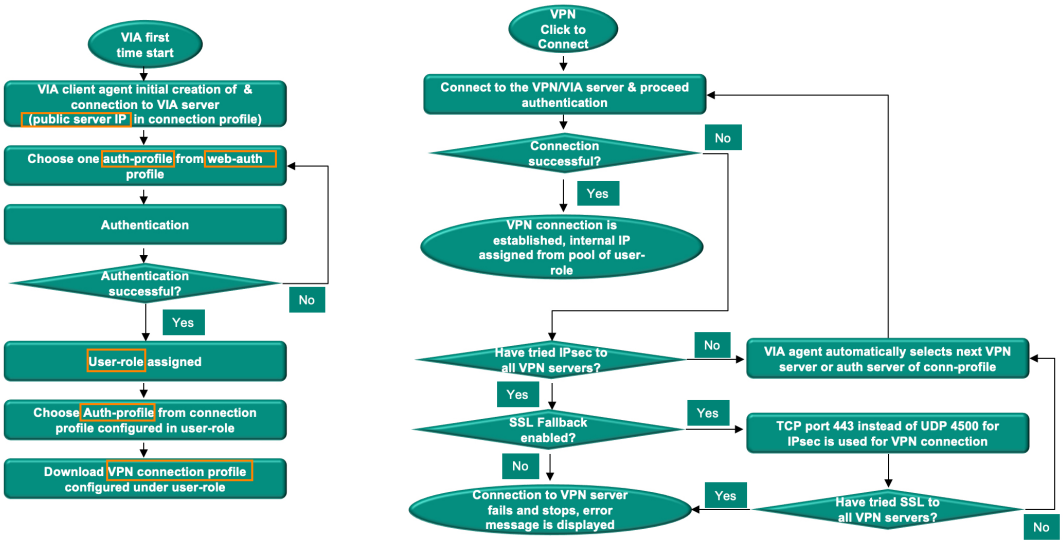
Listed below are the steps to download the connection profile:

1. The client will ping the Web Server, which is tied to a Web Authentication profile. Each authentication server profile may have one or more authentication servers configured for redundancy.
2. The user authenticates and, if the authentication succeeds, is assigned a user role.
3. The user role includes the Inner IP Pool and the VIA Connection Profile assigned to that user.
4. The VIA connection profile associated to the user role is downloaded to the VIA Client with all the parameters like VIA server list, authentication server list, tunnel subnets, authentication methods, IKE protocol policies, client WLAN profile, etc., configured in the connection profile. These will then be applied to the user.
5. The user will initiate the connection to the VIA server(s) defined in the connection profile, in order of precedence.
6. VPN profile is cached in the VIA VPN application after it is downloaded for the first time. After the first download, the VPN access will skip the first four steps and start from step 5 directly if you want to initiate a connection.

After the connection profile is downloaded, follow the steps below to connect to the VPN:

1. Connect to the VPN server and authenticate. If that is successful, the client will be online.
2. If the first connection is not successful, the VIA client will try to connect to other VPN Concentrators defined in the connection profile, if an IPsec tunnel can be established to any of the VPNCs, the client will be online. Else, the client will fall back to SSL (provided SSL fallback is enabled).
3. The VIA client will try to connect to the VPNCs in the Connection Profile using SSL, if SSL connection can be established to any of the VPNCs, the client will be online. Else, the connection to the VPN will stop and an error message will be displayed.

Figure 9 *VIA Connection Flowchart*



Web Authentication Profile

The VIA web authentication consists of a list of VIA authentication profiles. The web authentication list allows the users to login to the VIA download page <https://<VPNC FQDN>/via> to download the VIA client. To successfully login to the VIA download page, the user must authenticate successfully against the VIA authentication profile in the list. If more than one VIA authentication profile is configured in the web authentication list, the user can view the list and select one authentication profile before authenticating to the VIA installer download page.

The web authentication list also is used during the initial user authentication process that determines the VIA user role. The VIA users are authenticated against the authentication server defined by the VIA authentication profile in the VIA web authentication list. If more than one VIA authentication profile is configured in the web authentication list, the users can view the list and select one authentication profile during the VIA bootstrap process.

Authentication Profile

VIA clients connect to the VPNC through Internet. This communication between VIA clients and the VPNC across Internet is secured using the VPN technology. In the VIA solution, the VPNC acts as the VPN server and the VIA clients that are installed on the end-user devices behave as the VPN clients. Secure communication between the VPNC and VIA clients is achieved using IPsec, by default, and it can fallback to SSL when IPsec is blocked by the firewall.

The following flexible authentication methods are supported in the VIA solution:

- Tunnel authentication options: PSK or digital certificate
- User authentication options: Username/password, token, or digital certificate
- Supports RSA SecurID Suite with new/next PIN mode
- Supports 2-Factor/Multi-Factor Authentication. For more details, contact Aruba technical support.

The VIA authentication profile defines the authentication server group used and the default role assigned to the authenticated users. Multiple authentication profiles can be created. When multiple authentication profiles are available, the VIA client prompts the user to select an authentication profile.

The VIA authentication profile is a critical part of VIA configuration and it is used for the following purposes:

- To determine the authentication server for the XAUTH authentication phase of IKEv1 and EAP authentications of IKEv2.
- To determine the authentication server for the VIA web authentication. The VIA authentication profile is an integral part of the VIA web authentication, which determines the authentication sever used for VIA bootstrap process and for authenticating users on the VIA installer download page of the VPNC.
- VIA authentication profile has two parts of configuration:
  - **VIA user role** - It is assigned to the users who successfully authenticate through their VIA client. The user role defines the access rights of the users that connect using VIA.
  - **Authentication server group** - It is a collection of servers that are used for authentication. By default, the first server on the list is used for authentication unless it is unavailable. A server group can have different types of authentication servers.

Connection Profile

The VIA connection profile is a collection of all the configurations required by a VIA client. The VIA connection profile contains all the details required for the VIA client to establish a secure IPsec connection to the VPNC. A VIA connection profile also defines other optional parameters. Such optional parameters can be client auto-login, split-tunnel settings, and Content Security Services (CSS) settings. You can configure multiple VIA connection profiles.

A VIA connection profile is always associated to a user role, and all the users that belong to that role use the configured settings. When a user authenticates successfully to a server in an authentication profile, the VIA client downloads the VIA connection profile that is attached to the role assigned to that user.

The table summarizes the various parameters of a VIA connection profile and shows example settings for different IKEv1 and IKEv2 client authentication methods.

Table 2: *Parameters of a VIA connection profile*

Parameters	Purpose
VIA Servers	■ **Address**: Add the public IP or DNS hostname of the VPNC. This is the host name or IP address that the VIA users enter as the VIA server information on the VIA client. ■ **Internal_IP**: Add the IP address of any of the internal VLAN interfaces of the controller. This IP address should not be reachable from the public Internet. The VIA client uses this IP address to determine whether the user is connected to a trusted network. ■ **Description**: Add a readable description of the controller. More than one VIA controller can be added to the list. ■ **Position**: It decides the priority of the VIA server, that is, VPNCs which will terminate the VIA users. The top one is the VPNC that the VIA users will try to connect to first. If it is not available, the VIA users will try others in the list sequentially.
Client auto-login	It allows VIA users to auto login after the first successful authentication is complete. Enabled by default.
VIA authentication profiles to provision	Used to determine the authentication server used for the IKE authentication process. If more than one VIA authentication profile is added to this list, the users can choose the VIA authentication profile to be used during IKE authentication. If no VIA authentication profile is defined, the users are authenticated against the server group that is specified by the default VIA authentication profile (pre-defined).
VIA tunneled networks	When split-tunneling is enabled, traffic to the subnets configured here from VIA users will be tunneled to the VIA server-VPNC, other traffic will be forwarded locally to the default gateways of the VIA users
Enable split tunneling	Enable this parameter if split-tunneling is required. Disabled by default.
Enable IKEv2	Enable this parameter if IKEv2 is used for authentication. Disabled by default.
IKEv2 authentication method	The following four methods are supported: ■ User certification ■ EAP-TLS ■ EAP-MSCHAPV2 ■ EAP-GTC
VIA domain name profile	This parameter allows you to add VIA domain name profiles. **NOTE:** If a hyphen (-) is entered as input after a parameter, the Controller and VIA ignore that parameter. Example: `aaa authentication via connection-profile "via" (VIA Connection Profile "via") #dn-profile CN VIA-EXAMPLE.ACME.COM ORG IT OU - Country USA`

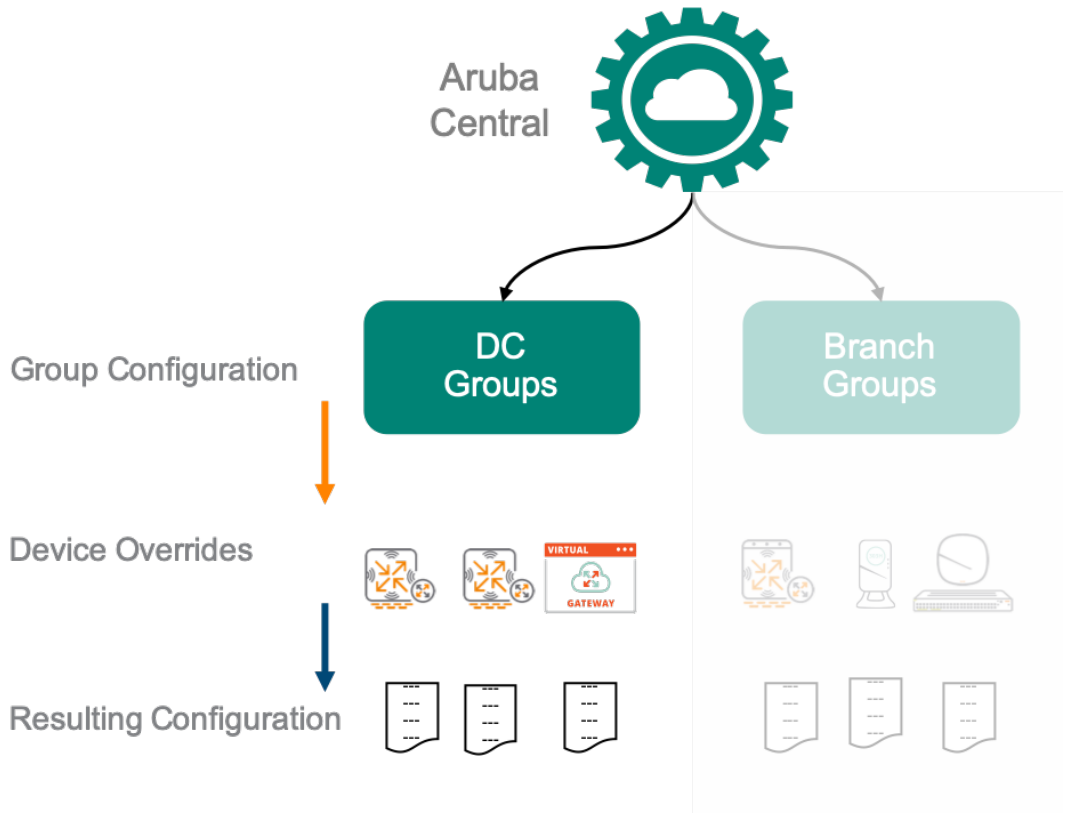
The following topics are discussed in this chapter:

The features and configuration of VIA through Aruba Central is similar to the configuration of VIA in ArubaOS 8 controllers. This section provides guidance on how to set up the most common scenarios. The complete set of options are described in the *Aruba Central documentation portal*.

Aruba Central Group-based Configuration

Aruba Central uses a hierarchical configuration model where configurations applied at the group level filter down to all the devices in the group. Specific overrides, like hostnames, IP addresses, or specific routing configurations are generally overridden at the device level.

Figure 10 *Central Configuration Hierarchy*

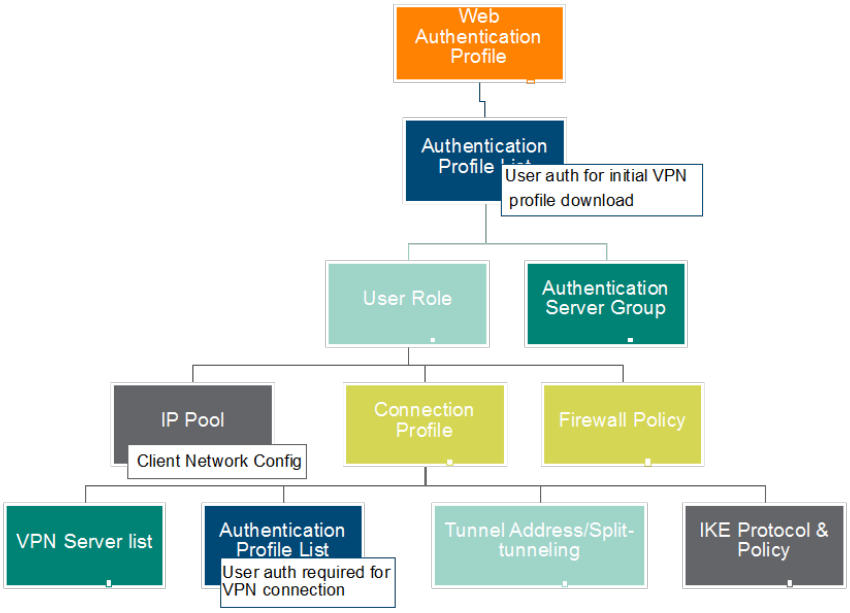


In the context of VIA, the general recommendation is to have different groups for each Data Center (Branch groups do not have relevance in this context). Common configurations that would be consistent across a single data center (DC) would then be done at the group level to facilitate administration.

Client Profiles

The Aruba VIA configuration gravitates around client connection profiles and the use they make of other configuration constructs such Authentication, User Roles, IP pools, etc.

Figure 11 *VIA Configuration Flow Chart*



The flowchart above provides a complete view of the steps to be taken. This document focuses on the following main configuration steps:

- Authentication
- Creating the Connection Profile
- Client IP Routing
- Applying the Connection Profile to the User-Role

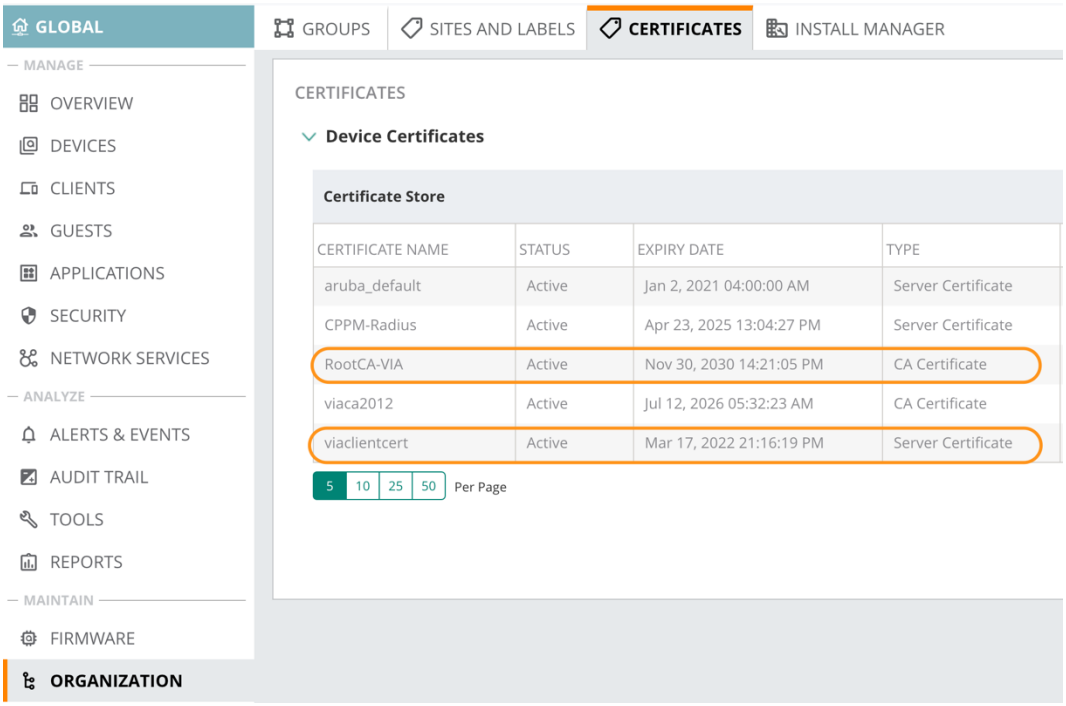
Authentication

Unless IKEv1 with pre-shared keys is used (not recommended), the VIA configuration requires server certificates that are loaded in the VPNCs. This is required for the HTTPS communication to download the profile and for the VPN. If client-devices use cert-based authentication, the trusted CA certificates should be loaded to the VPNCs.

Load Certificates through Aruba Central

Each VPNC should have a server certificate signed by a CA that is trusted by the client devices to identify itself. You can use different certificates per VPNC or the same certificate with multiple SANs tied to the FQDNs used by the VPN service. Certificates can be loaded into all devices through Aruba Central by navigating to **Global > Organization > Certificates**.

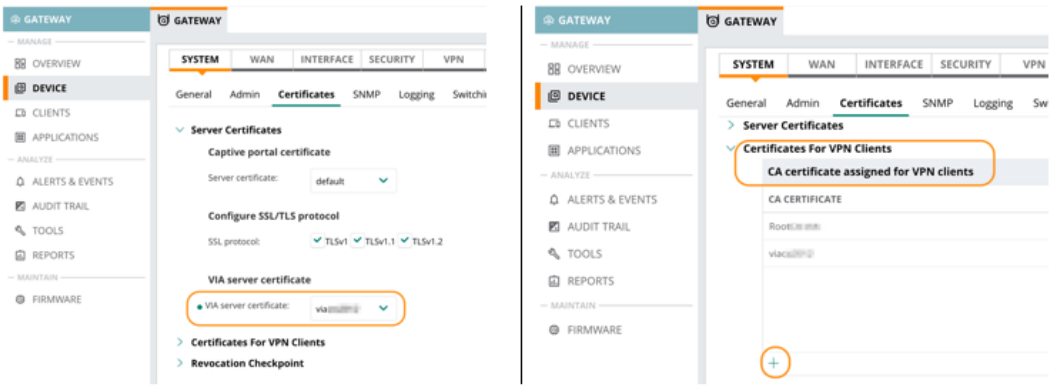
Figure 12 *Certificate Management in Central*



Apply Certificates

Once the certificates are loaded using the certificate store in Aruba Central, configure the devices to use the correct one for each service. You can navigate to **System > Certificates** under **Devices > Gateway > Management** and select the correct Server Certificate or CA for each use-case.

Figure 13 *Apply Certificates*



Authentication Profiles

To define the authentication scheme to be used by the VIA service, perform the following steps:

1. In the **Network Operations** app, use the filter to select a group in which gateways are configured.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the Configuration icon. The gateway configuration page is displayed.
4. Under **Security > Auth Servers**, create the RADIUS server to be used for VPN client authentication.

5. Navigate to **Security > L3 Authentication > VIA authentication** and create a new VIA authentication profile.
6. Assign the appropriate Server Groups, Accounting server, and RFC3576 Server.
7. Navigate to **Security > L3 Authentication > VIA Web Authentication > default**. to associate the VIA authentication profile to the default VIA Web Authentication profile. This ensures that the users download the correct VIA profile.

As opposed to what happens with ArubaOS 8.x controllersmanaged by a Mobility Master, the internal DB cannot be used for VIA client authentication when the VPNC is managed by Aruba Central.

Creating the Connection Profile

The next step is to configure the Connection Profile(s) to be used. When multiple VPNCs are in use, either because there is a global VPN Service or for redundancy purposes, ensure that there is consistency across all VPNCs. Configure the Connection Profile at the group level to handle the multiple VPNCs with ease.

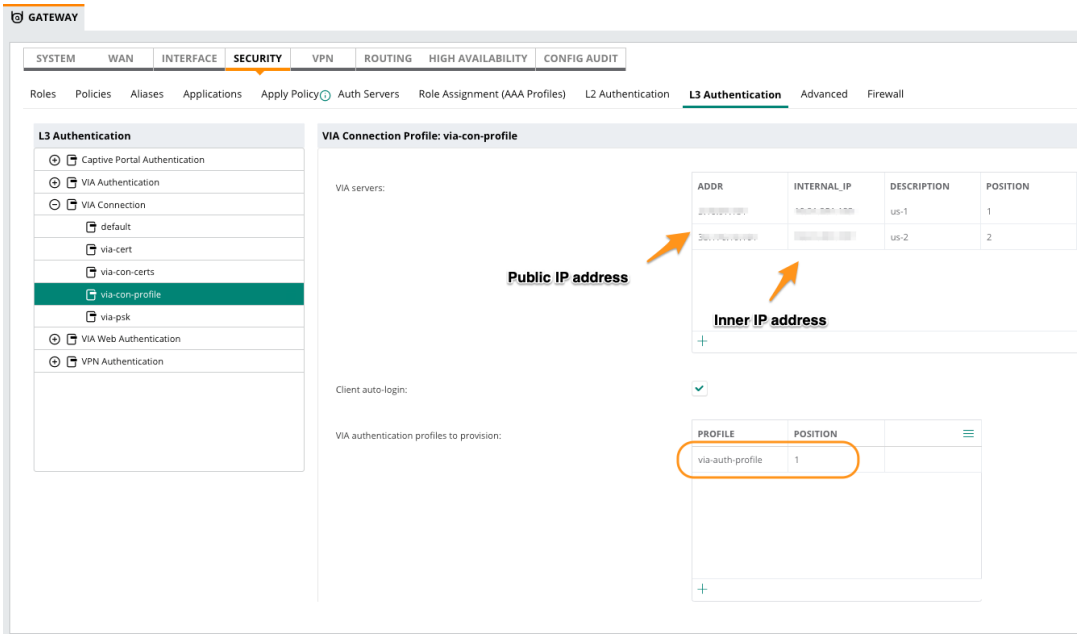
To configure the VIA profile, perform the following steps:

1. In the **Network Operations** app, use the filter to select a group in which gateways are configured.
2. Under **Manage**, click **Devices > Gateways**.
3. Click the  Configuration icon. The gateway configuration page is displayed.
4. Click **Security > L3 Authentication > VIA connection**.

For more details, see Aruba Central documentation, but the most common options are the following:

- **VIA Servers** - Configure the Public-facing as well as the internal IP address of the VPN concentrators in this profile. When using multiple L3 VPNC servers, make sure all VPNCs have all VIA servers defined.
- **VIA authentication profiles to provision** - Select the authentication profile to be used.
- **Enable split-tunneling** - Decide whether clients should be full-tunneled or if split-tunnel should be allowed.
- **VIA tunneled networks** - In case split-tunnel is selected, define the destinations that are to be reached through the tunnel.
- **VIA client DNS suffix list** – In case split-tunnel is in use, select the domains (comma separated) for which the corporate DNS servers (defined with the Inner IP Pools) will be used.
- **Enable IKEv2** – This is the recommended value, as it's more secure and resilient.
- **IKE2 authentication method** – Select the authentication method to be used.

Figure 14 *VIA Connection Profile*



Client IP Configuration

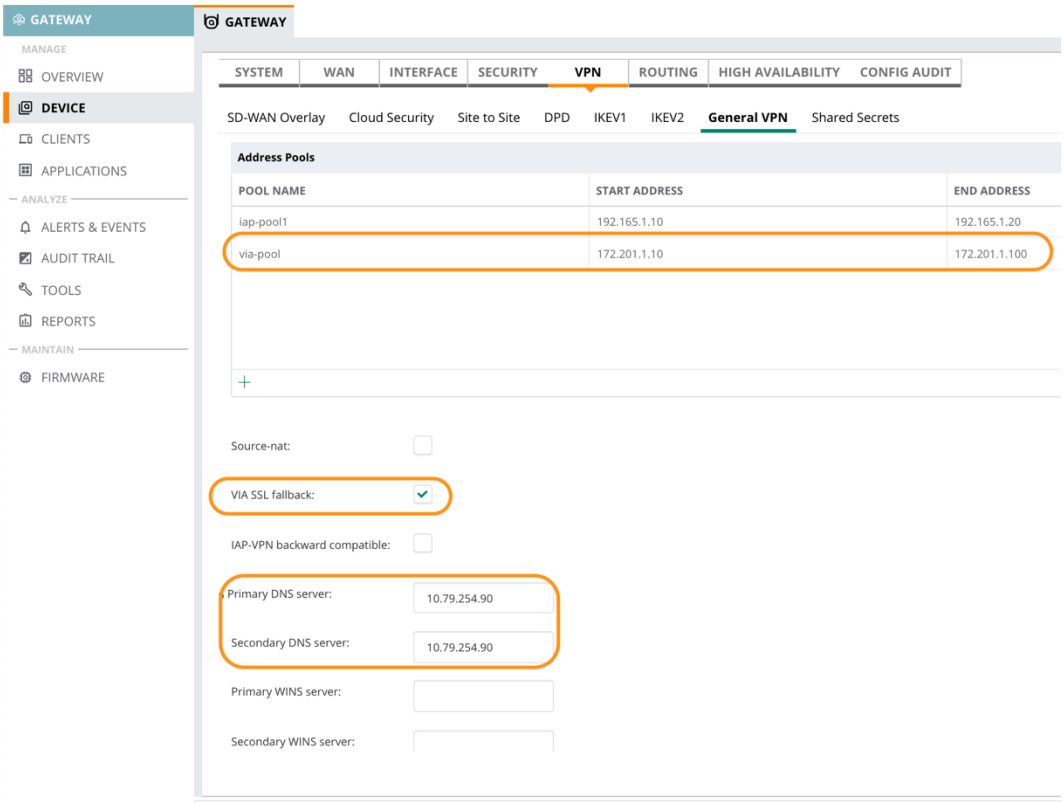
The next step is to create the network configurations that will be associated with the client devices. These will be the Inner IP pool associated to the VPN clients as well as other parameters such as SSL Fallback, internal DNS to be provided to the VPN clients, etc.

To create the network configuration settings, perform the following steps:

1. In the **Network Operations** app, use the filter to select a group in which gateways are configured.
2. Under **Manage**, click **Devices > Gateways**. The gateway page is displayed.
3. Click **VPN > General VPN**.

If the provided Source-NAT is not enabled, the inner IP addresses will have to be routable through the network. To ensure network consistency, the Inner IP Pools should be the same across L2-redundant peers and different across L3 peers (more details in the Client IP Routing section).

Figure 15 *Client IP configuration*



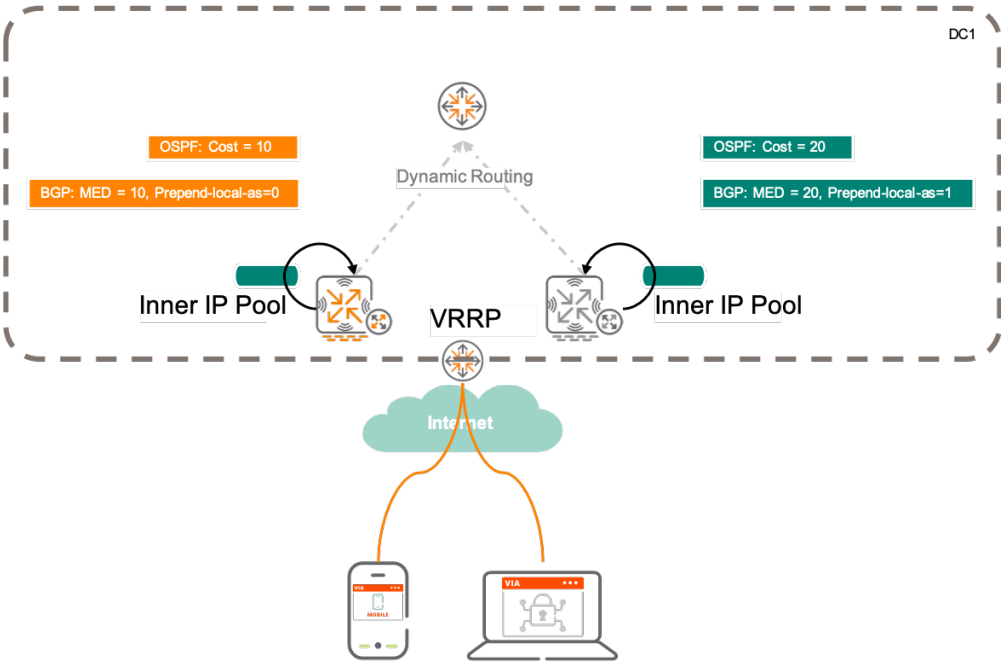
In case IKEv1 is used (not recommended), a shared secret must be set under **VPN > Shared Secrets** for the phase 0 authentication.

Client IP Routing

The Inner IP Pool will have to be routable through the corporate network. This can be achieved by using static routes in the northbound routers pointing to the VPNCs or by redistributing the Inner IP pool subnets into the dynamic routing protocol in use. Based on whether there is L2 or L3 redundancy, different strategies should be adopted.

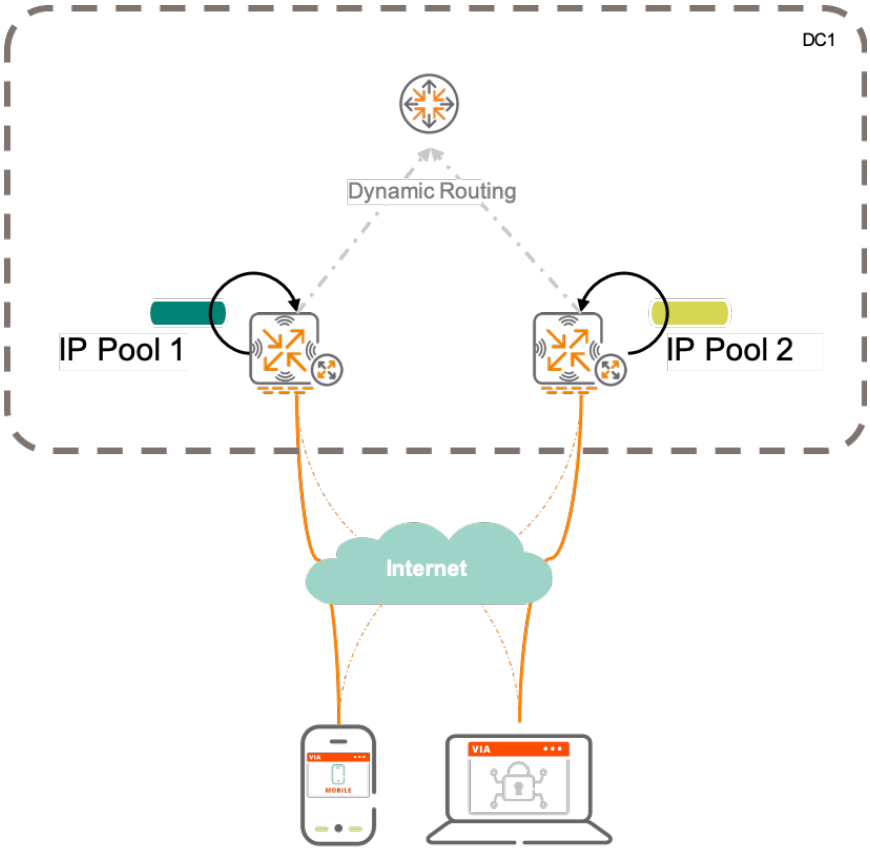
In the case of L2 redundancy in a single data center, the same IP pool should be used in both VPNCs, redistributing with a lower cost on the active VPNC than on the backup VPNC. To do this, both VPNCs would have the same Public/Private servers defined in the Connection Profile, both attached to a VRRP address between the two of them.

Figure 16 *HA Configuration - L2 Single DC*



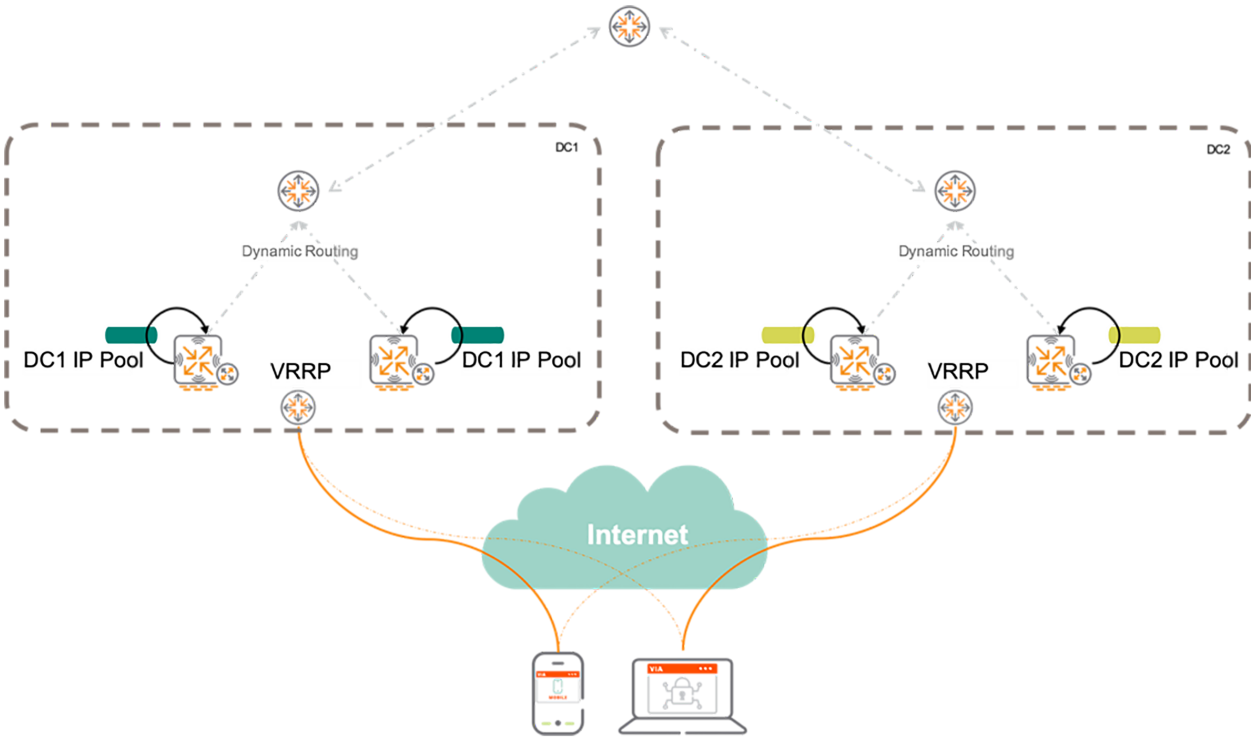
In the case of L3 redundancy in a single data center (as in the case of Virtual Gateways in Public Cloud), different IP pools should be used in each VPNC, allowing active-active VPN termination. To do this, simply create multiple VIA servers in the Connection Profile, as described above:

Figure 17 *Active-Active L3 VPNCs*



A combination of both is also possible, by having multiple active DCs with active/backup pairs in each one:

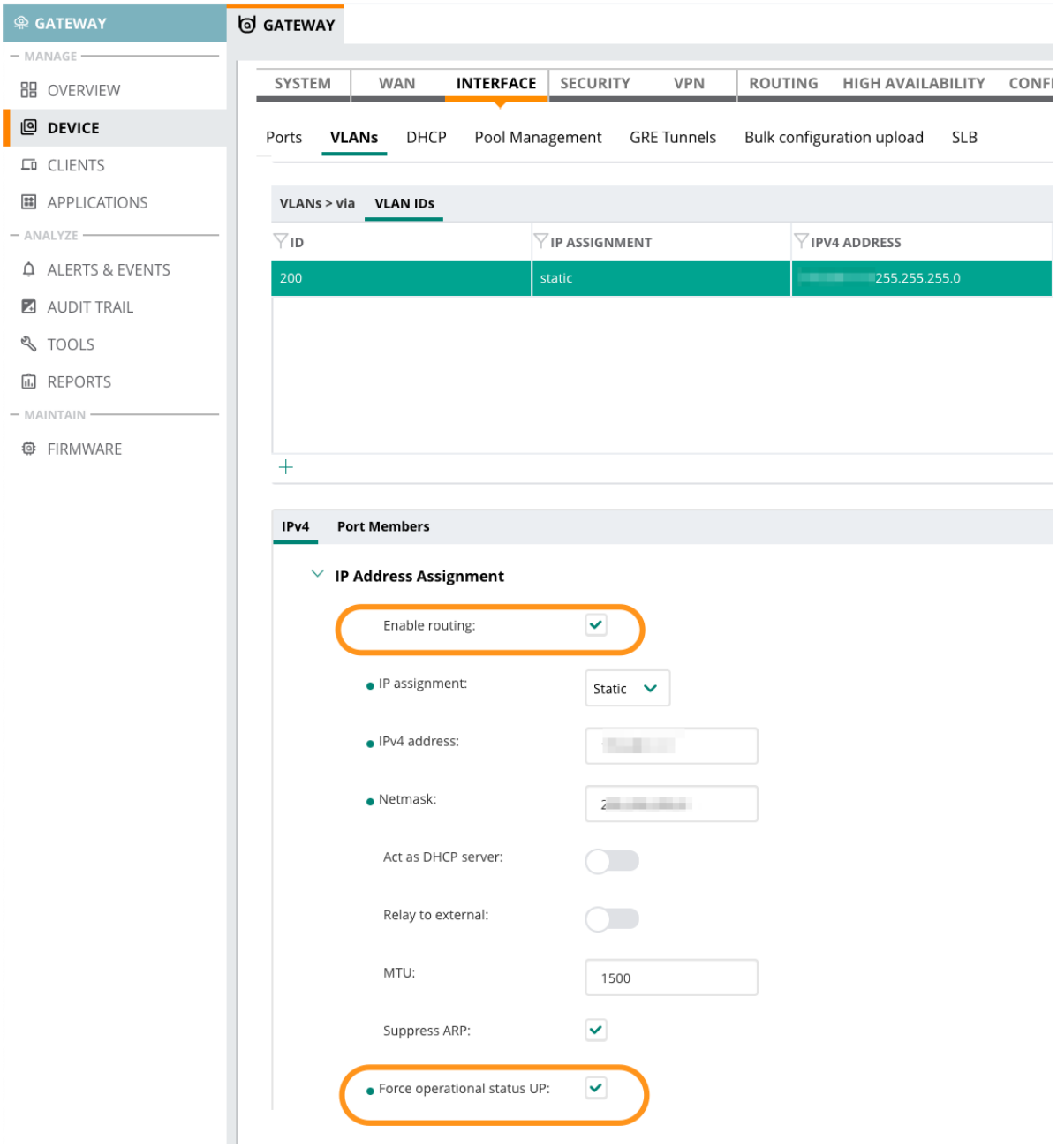
Figure 18 *Multiple active DCs with HA Pairs*



To advertise the subnet with the VIA clients, create a VLAN interface with IP/netmask in the same subnet as the inner IP Pool (when using L2 redundancy, use the same IP/netmask on both peers) and redistribute it into the dynamic routing protocol being used. Perform the following steps:

1. In the **Network Operations** app, use the filter to select a group in which gateways are configured.
2. Under **Manage**, click **Devices > Gateways**. The gateway page is displayed.
3. Click **Interface > VLANs**.
4. Click **VLAN IDs**.
5. Click the **Force operational status UP** checkbox, to ensure that L3 interface is always up.

Figure 19 *VIA VLAN Interface*



To redistribute the VIA subnet(s):

- For OSPF
  1. Enable OSPF and set the area to be used with the upstream router.
  2. Enable the interface VLANs to be used in the OSPF Process.
  3. Redistribute Connected > VLAN X routes into OSPF.
- For BGP

1. Enable BGP Globally and set the AS number.
2. Create the necessary BGP neighbors. Note: ArubaOS follows RFC8112, which describes that, in absence of a route-map, no routes should be learnt from a neighboring eBGP router.
3. Redistribute Connected > VLAN X routes into BGP.

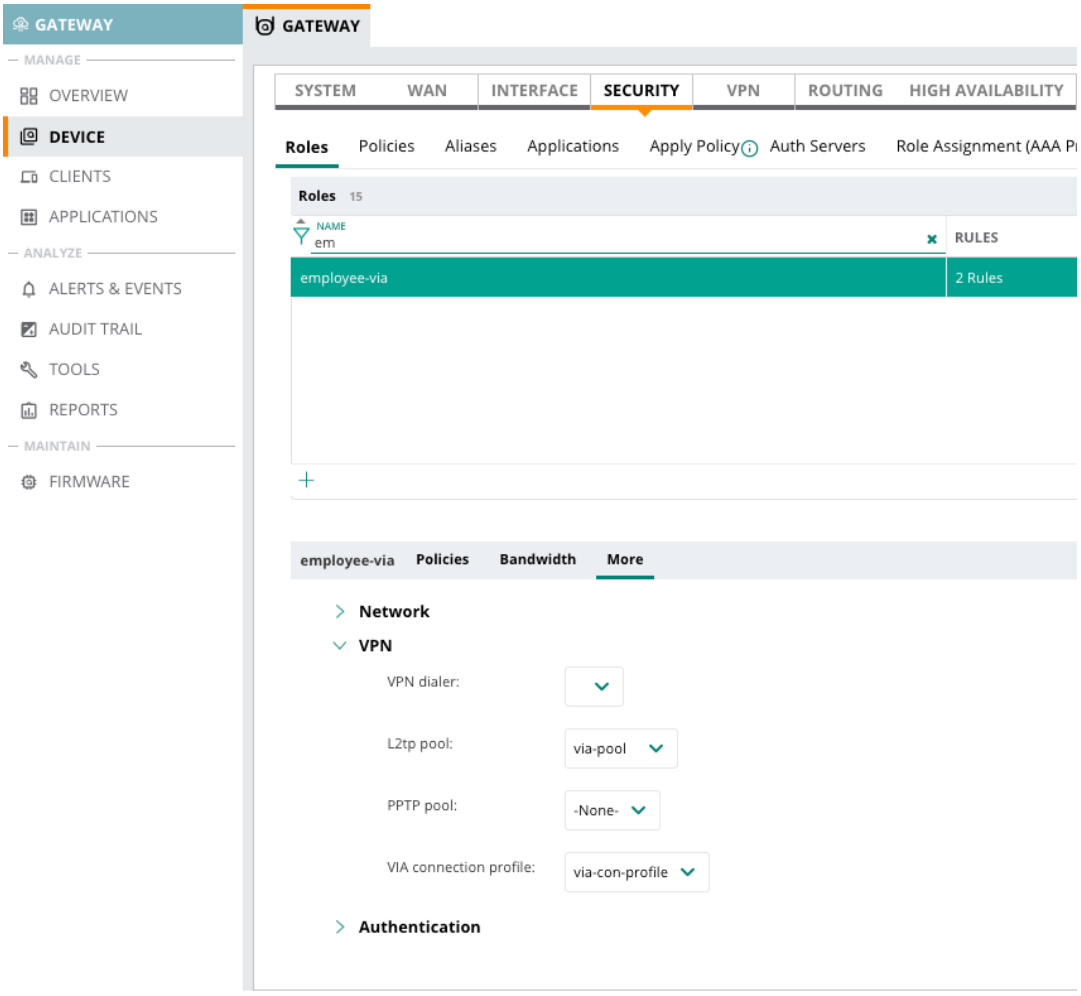
Applying the Connection Profile to the User-Role

Once a VPN Client has gone through the authentication process, it will be associated with a role that will have a certain connection profile.

Perform the following steps to apply the connection profile to the user roles:

1. In the **Network Operations** app, use the filter to select a group in which gateways are configured.
2. Under **Manage**, click **Devices > Gateways**. The gateway page is displayed.
3. Click **Security > Roles** and select the correct role.
4. Set the VIA connection profile and the L2TP pool by navigating to **Advanced View > More > VPN**.

Figure 20 *Applying VIA Configuration to User-Role*

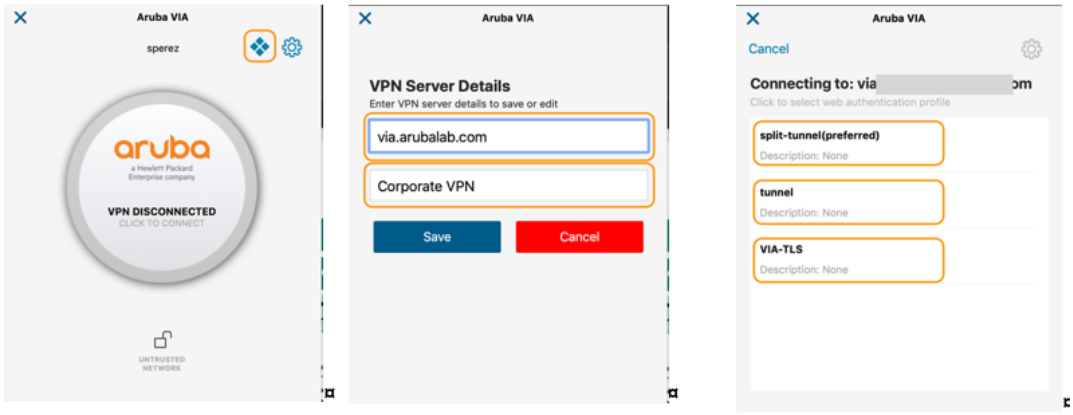


As described in this document, VIA is a software-based VPN Client that can be installed in most modern operating systems. The software can be downloaded from the Aruba Support Portal as well as from the respective application stores.

Once the end-user has downloaded the application, the application is designed to guide the user through the whole process. If it's the first time, the user will have to download the VPN Profile, by following the steps listed below:

1. Open the application and click the diamonds icon on the top right corner. You will be prompted to download a VIA profile.
2. Enter the URL and provide a name for the VPN Connection Profile (this is only relevant for the end-user).
3. Select one of the available profiles.

Figure 21 *VIA Client*

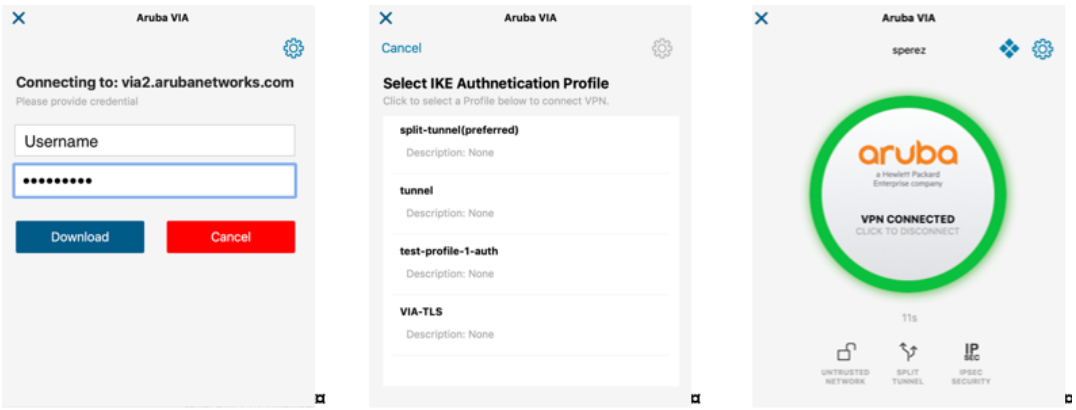


The steps above only have to be done once, as the profile will be cached in the VIA client.

After downloading the profile, the VIA client will be ready to connect:

1. Enter the username and password.
2. Select the VIA authentication profile to be uses, in case multiple profiles are available. You will be online and can proceed further.

Figure 22 *VIA Client*



From this point on, the user credentials will be cached, and as long as the same profile is used, the VIA client will automatically connect to the VPN every time it's outside the corporate network.

Table 3: *Supported Operating System*

Platform	Download From	User Limit
Windows	Aruba Support Portal	Windows Vista
		Windows 7
		Windows 10
MAC OS X	Apple App Store	10.6-10.12
Apple iOS	Apple App Store	4.2-10.x
Android	Google Play	4.0.2 and above
Linux	Aruba Support Portal	RHEL 6
		CentOS 6
		Debian 7
		Ubuntu (>12.04)

Recommended Software Versions

Listed below is the recommended software versions to be used in a remote access solution, as of March 2020:

- For headend gateways, the recommended version is ArubaOS 8.5.0.0-2.0.0.3.
- For the VIA clients:
  - For Android, iOS and MAC OS X – The images available in the Google Play or the Apple App Store
  - For Windows – 3.4.2
  - For Linux – 3.1.1

Software updates for the headend gateways can be managed from Aruba Central. To guarantee that a consistent software image is deployed across all sites, it is recommended to set a Compliant Software Image using the **Firmware Management** page in Aruba Central.

Central Subscriptions

When devices are managed by Central, the only subscriptions required for the remote access service are the Gateway Foundation Subscription, applied to all the VPNCs.

Headend Gateway Sizing

The following table describes the user limit for controllers and supported operating systems:

Table 4: *VPN Concentrator Sizing*

Platform	User Limit
7200 Series	
7210	16384
7220	24576
7240XM	32768
7280	32768
7000 Series	
7005	1024
7008	1024
7010	2048
7024	2048
7030	4096