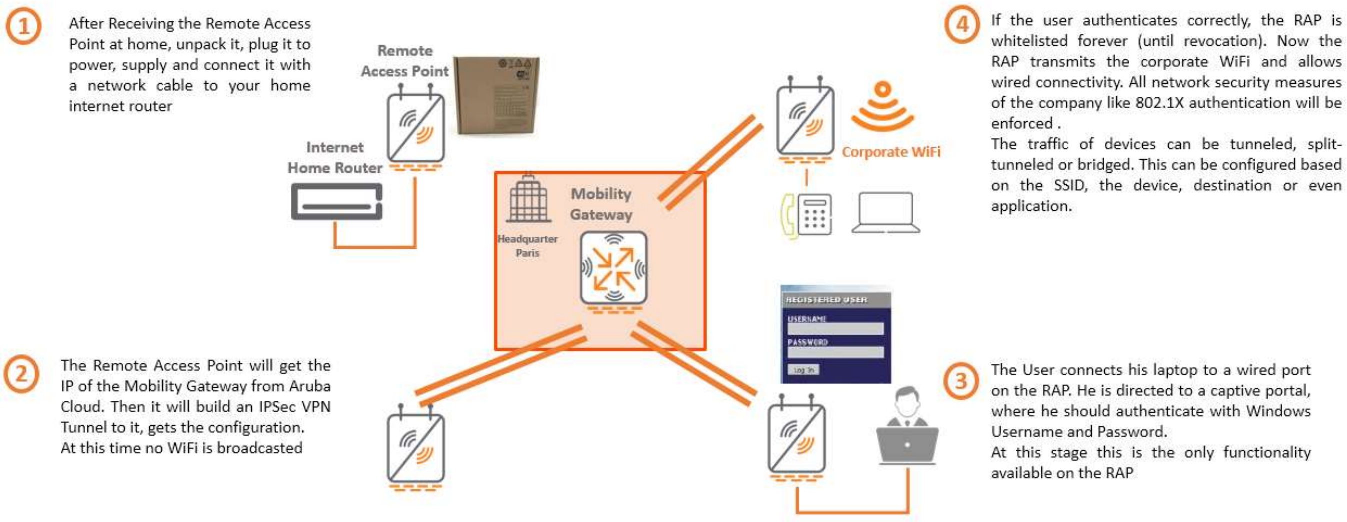
SECURE REMOTE ACCESS POINT PROVISIONING

For customers wishing to distribute Remote Access Points (RAP) to their employees there are concerns of overhead and security.

They are looking for a zero-touch method where the remote access points will get their configuration automatically and at the same time the distribution, authentication and connectivity is done securely. For instance how to deal with the case, when a RAP is sent via post to an employee at home and this RAP is lost or gets in unauthorized hands?

Aruba provides a *secure provisioning solution* for it Remote Access Points. This is described in the figure below:



① After Receiving the Remote Access Point at home, unpack it, plug it to power, supply and connect it with a network cable to your home internet router

② The Remote Access Point will get the IP of the Mobility Gateway from Aruba Cloud. Then it will build an IPSec VPN Tunnel to it, gets the configuration.
At this time no WiFi is broadcasted

③ The User connects his laptop to a wired port on the RAP. He is directed to a captive portal, where he should authenticate with Windows Username and Password.
At this stage this is the only functionality available on the RAP

④ If the user authenticates correctly, the RAP is whitelisted forever (until revocation). Now the RAP transmits the corporate WiFi and allows wired connectivity. All network security measures of the company like 802.1X authentication will be enforced .
The traffic of devices can be tunneled, split-tunneled or bridged. This can be configured based on the SSID, the device, destination or even application.

As seen in the figure, the key element here is that the RAP allows no wired or wireless connectivity until the user connects his laptop to a wired port on the RAP and authenticates on the captive portal using his Active Directory or Windows username and password. The user does it once; after that the RAP is whitelisted and will allow the configured settings like WiFi and Wired connectivity. This step prevents the RAP from coming under unauthorized hands before it reaches its destination.

The provisioning of the RAP is simple, zero-touch and secure. This scenario was implemented by large German customer in the transportation business as well as many other security-aware customers.

Also worth to mention is that the IPSec VPN is established through a certificate built into a TPM (Trusted Platform Module) chipset that exist on the RAP. This certificate cannot be tampered with. This ensures confidentiality of data transmitted over the internet.

This kind of secure provisioning is unique to Aruba.

AT ARUBA WE ADVANCE HOW PEOPLE LIVE AND WORK

aruba
a Hewlett Packard
Enterprise company
www.arubanetworks.com

3333 Scott Blvd. | Santa Clara, CA 95054
1.844.472.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com