ArubaOS8 RAP Deployment
Non-Cluster

Marcel Koedijk
Airheads MVP Expert
@mkk

11 April 2020
Agenda

- Introduction
- Installation two VMC controllers in DMZ zone
- Add VRRP Redunancy
- Add VPN Service
  - Configure IKE Pre-Shared Key *
  - Configure AP user accounts *
- Provision an Campus AP to Remote AP
- Verify redundancy

* Only needed for PSK based authentication
What is a Remote Access Point

– A “normal” Campus Access Point (CAP) use unencrypted GRE tunnels to transfer client data to the Mobility Controllers over the customer network infrastructure.

   **Note:** When using WPA2/3 encryption the client traffic is AES encrypted in the GRE tunnels, and de-crypt at the controllers by default.

– A Remote Access Point (RAP) use a encrypted IPSEC tunnels to transfer client data to the Mobility Controllers over the internet.

– Any modern Aruba Access Point can be provisioned as RAP.
ArubaOS8 Cluster vs Non-Cluster

- A ArubaOS8 cluster RAP deployment is high redundant and support hitless failover.

- A ArubaOS8 non-cluster RAP deployment is (VRRP) redundant, GRE tunnels must re-established on the second controller and clients must re-authenticate.

- When using ArubaOS8 in a cluster configuration each node must assigned a public (WAN) IP in the cluster configuration when using Network Address Translation (NAT) for connect Remote Access Points (RAP).

- When having only one public IP available, you can’t use clustering.

  – A cluster is the recommened setup if you have enough public IP addressed available.
Certificate vs PSK based authentication

– Any Access Point and hardware Mobility Controller (MC) have a Trust Platform Module (TPM) that can be used for certificate based authentication.

– A virtual Mobility Controller (VMC) don’t have a TPM chip, and therefore can’t used certificate based authentication.

– Certificate based authentication is recommended if you can use it.
Remote AP Communication

– For both MC or VMC it’s recommended to deploy two dedicated controllers in the DMZ zone of your firewall.

– In this setup we use VMC controllers in the DMZ with a single Public IP available.
Pre-Installation of two VMC controllers
Add VMC controllers to the Mobility Master
Create a new Managed Device Group

– Add a new managed device group “Remote”.
– Add the VMC controllers to this group
Create VRRP Redundancy
Test VRRP Redundancy (CLI)

– Show vrrp
Create VPN Service

- The chosen IP pool must be unique/non-routed in your infrastructure, this addresses are assigned as inner IP to the Remote Access Points after establishment of the IPSEC tunnel.
Add IKE Pre-Shared Key

– Only needed for PSK based authentication!
Add RAP User Account

– Only needed for PSK based authentication!
Provision CAP to RAP

– Provision a existing CAP to a RAP
– After provisioning place the RAP on a external internet connection / location.
Test RAP connectivity

- Show datapath session table | include 4500
- Show crypto isakmp sa
- Show crypto ipsec sa
Test RAP failover
Test RAP Failover

– After HomeLAB-RC01 fails, HomeLAB-RC02 becomes the VRRP master and the RAP has re-connect its GRE tunnels to the second controllers within 10 seconds.
Thank you