DATA SHEET

ARUBA MULTIZONE

Aruba's centralized architecture provides a more secure Wi-Fi environment that is different from any other Wi-Fi vendor on the market today. Among the key security advantages of this architecture are:

- Client to core controller encryption, where thin APs do not perform encryption and perform a pass-through by tunneling encrypted Wi-Fi traffic between itself and the controller across the wired infrastructure.
- Role-based authentication and access to users and devices, centrally within the controller.
- Integrated policy enforcement firewall capability based on assigned roles of users and devices.
- Enhanced security in that there are no encryption keys present on any Aruba AP (unlike most other vendor solution).
- With Aruba's centralized architecture, there are no encryption session keys or certificates present on the AP that are used for user data transmissions.

Because traffic is tunneled between the AP and controller, all configuration and security mechanisms are implemented centrally on the controller.

Up to this point, the AP has authenticated to the controller and establishes a GRE tunnel with that controller. APs only communicate to that single controller. However, environments exist that need additional separation due to security requirements.

Aruba's centralized architecture makes it possible to provide additional separation and security by designing and creating separate "zones" for each separation instance. Examples of this kind of separation are:

- Federal unclassified networks vs classified networks
- Separate operating networks (unclassified or classified) within a single environment
- Department/Contractor/Visitor/Guest access
- Multi-tenant facilities

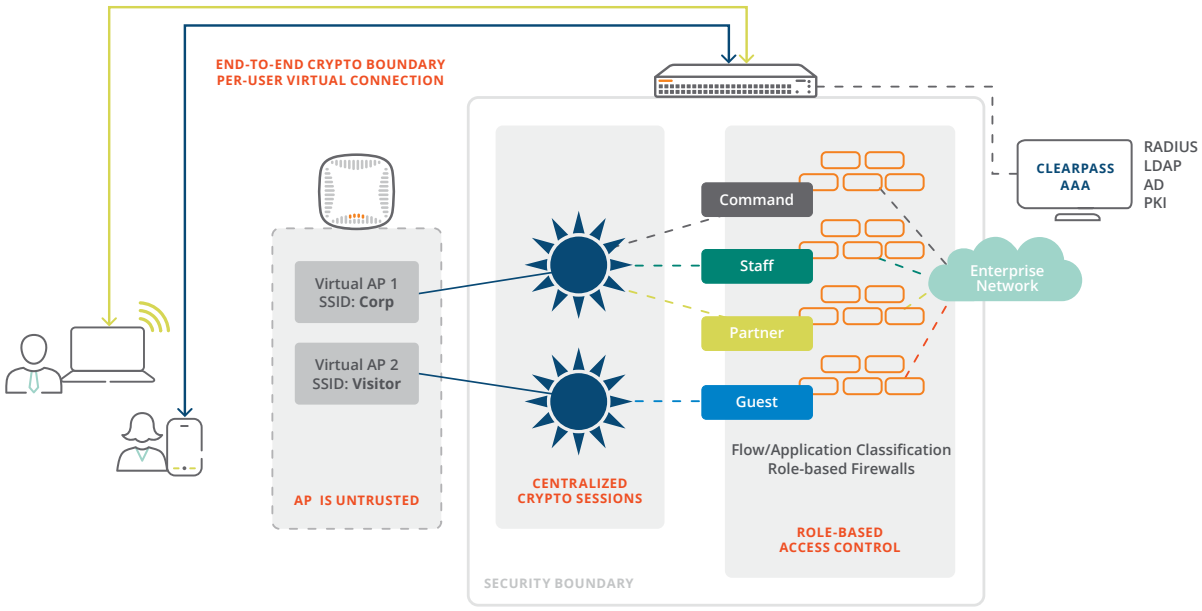

Figure 1: Aruba's Centralized Architecture

Aruba's MultiZone AP feature is the key to providing the additional separation that is required in the above examples. With Aruba MultiZone AP, all current APs authenticate against a defined "Primary Zone" controller to start. Additional "zones" are defined and configured on the Primary Zone controller. Once authenticated, these APs receive a configuration from the Primary Zone controller, which direct the AP to authenticate to additional "Data Zone" controllers to receive another AP configuration for that particular zone. Up to 4 Data Zone controllers may be defined from the Primary Zone controller.

The AP establishes a per SSID GRE tunnel against multiple controllers. This provides several advantages. Among them are:

- Each "zone" controller may be configured and managed by separate entities, providing more control for each separate entity.
- Partitioned "zone" traffic is directed away from a single centralized controller and is forwarded to a separate zone controller for processing.
- Individual role-based access and policy enforcement rules can be implemented on each zone controller, tailored to the security requirements of that zone.
- A single RF infrastructure of APs can be utilized, even though there are different WLAN controllers implemented for each zone.

Let's take some use case examples from above to demonstrate the advantages of Aruba's overall architecture and how including MultiZone can provide ease of deployment.

COMMERCIAL SOLUTIONS FOR CLASSIFIED – CAMPUS WLAN CAPABILITY PACKAGE 2.

The NSA's CSfC program provides a way to implement secure solutions that protect classified information. By following the guidelines within their Capability Packages, these solutions may be implemented using Commercial Off The Shelf products that meet all the requirements within the capability package. If we take a look at the Campus WLAN Capability Package, page 14, Figure 2, it depicts the following:

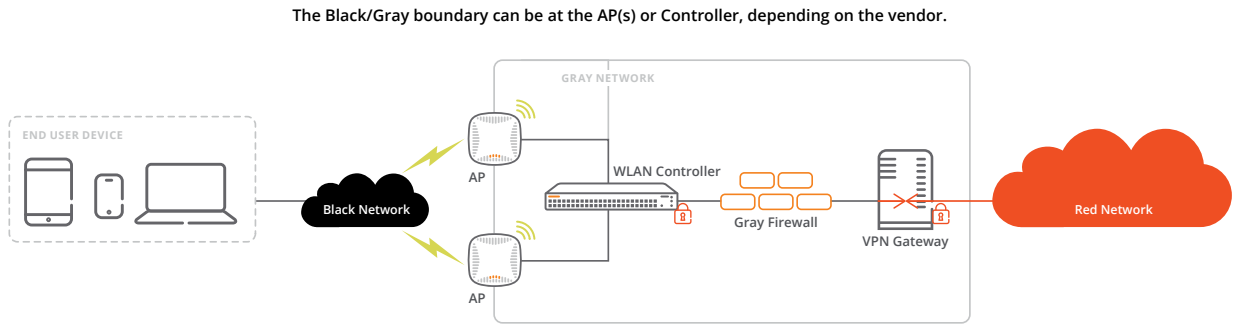

Figure 2: CSfC Campus WLAN Security Boundary

With any non-Aruba solution, the AP is the "black/gray" security boundary because it is performing crypto functions.

With an Aruba solution, the security "black/gray" boundary is at the controller, not at the AP. Since Aruba APs do not perform crypto functions on user traffic, they are considered to be part of the "black" network, thus not part of the security boundary. We will see that this is significant when considering the ability to do multiple data classifications, which is introduced in version 2.0 of the Capability Package.

Figure 3 below shows this (as in the Campus WLAN Capability Package on page 10). This figure shows that while multiple classifications are allowed, it also shows that a VPN solution needs to be implemented for the unclassified (NIPR) portion of the overall solution. This is because with this figure, unclassified traffic potentially traverses the "gray" network. That "gray" network requires one tunnel of encrypted data. Taking this a step further, the amount of design and implementation effort to provide VPN capabilities to potentially thousands of unclassified EUDs can be a huge undertaking.

Because the security boundary on an Aruba CSfC solution is at the controller (not the AP), we can offer an alternative to implementing VPN capabilities on the unclassified data classification. This alternative is called MultiZone AP.

With the Aruba MultiZone AP feature, additional "zones" can be implemented (for example, an unclassified network) where a VPN solution will NOT be required. The reason is that unclassified traffic will be directed away from the CSfC controller towards a "Data Zone" unclassified controller. This is a key advantage versus competitor solutions. Figure 4 depicts this scenario. As an added value, the non-classified networks don't require a CSfC registration package and follow already well-established federal and DoD wireless access requirements.

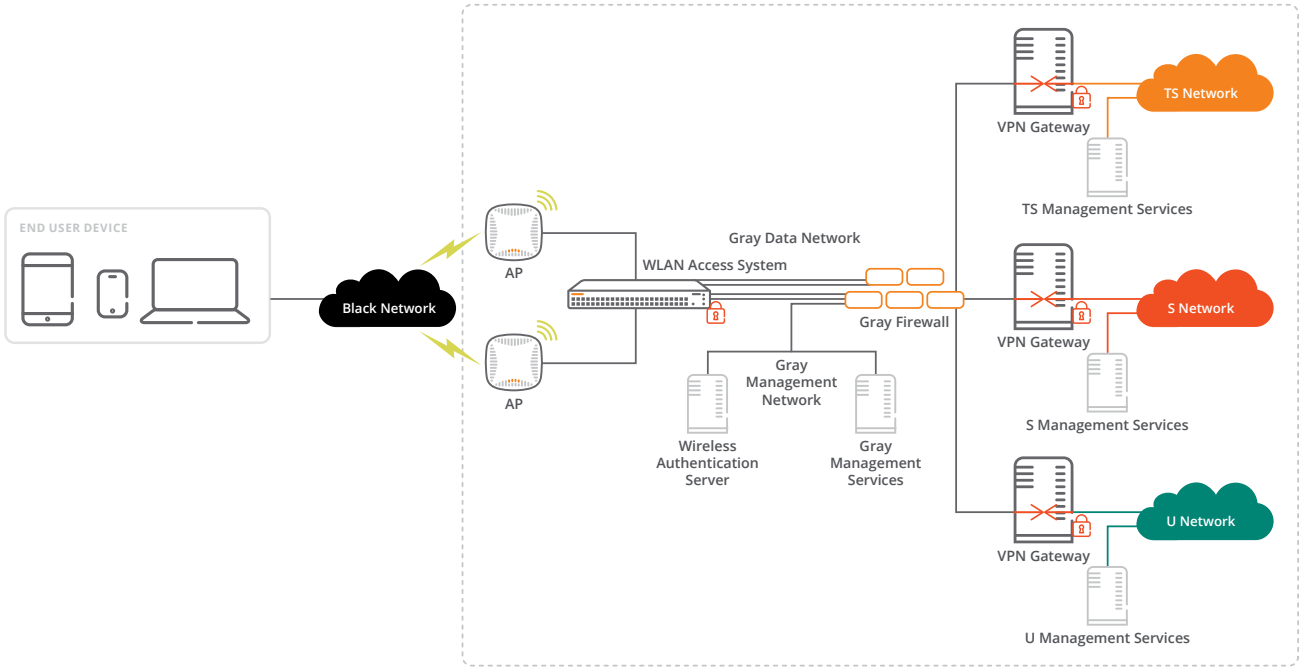

Figure 3: Overview of Campus WLAN CP

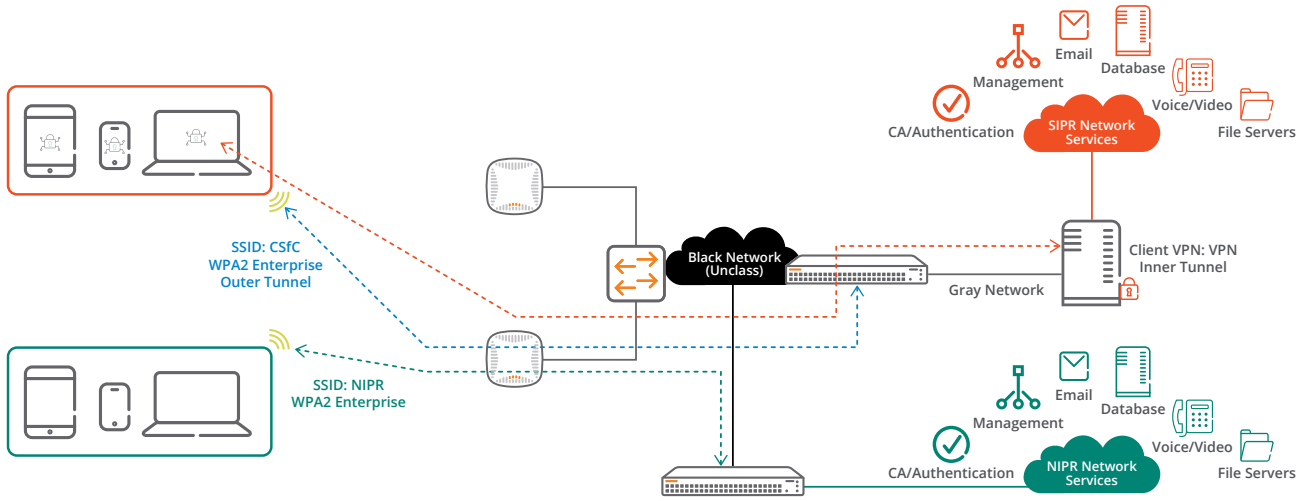

Figure 4: Aruba MultiZone AP to separate data classifications

SEPARATE GOVERNMENT NETWORKS

In this use case, we'll consider two different government networks that operate at the same government building or facility. An example of this is two different MAJCOMs operating at the same facility. Each MAJCOM uses a different network, from authentication and access to operation and management. Configuring the MultiZone capability, one controller is configured as the primary zone controller. This Primary Zone controller will manage the APs and RF for the environment. A configuration is implemented on the primary zone controller to provide EUDs the ability to authenticate using CAC certificates with EAP-TLS and WPA2 Enterprise (AES-CCM) as the data payload encryption algorithm. Also, the Primary Zone controller has a configuration telling the APs to authenticate to a Data Zone controller. The APs are whitelisted to the Data Zone controller just like on the Primary Zone controller.

The Data Zone controller has a different configuration in place that supports the same authentication/access capabilities, but the controller connects to a completely separate network. A different network operations/management team provides its services to its own network and controller that is connected to that network.

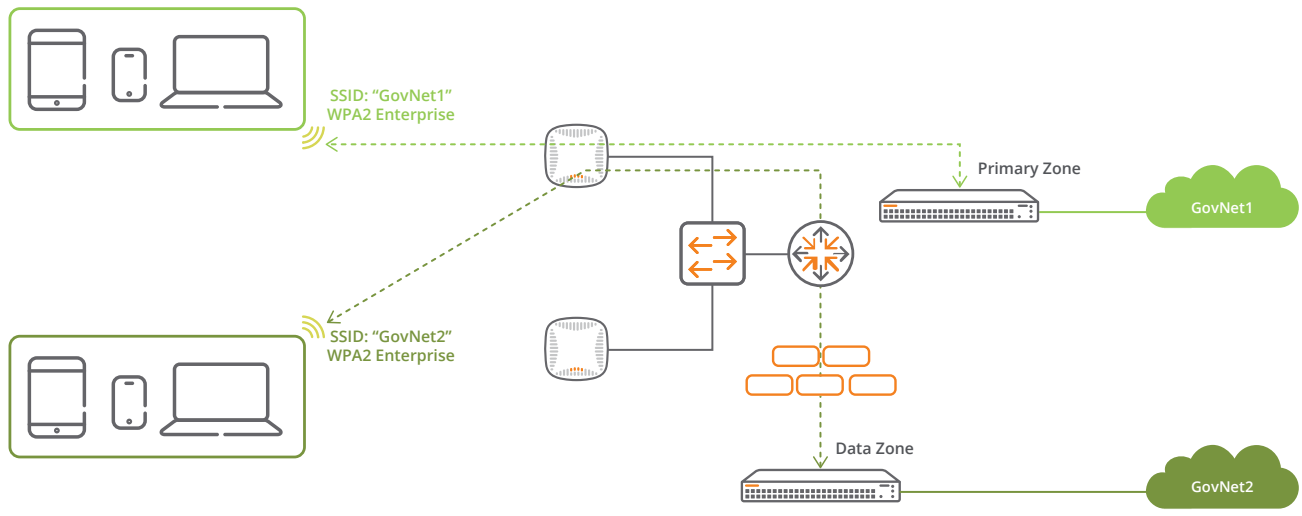

Figure 5: Aruba MultiZone AP to separate two different Government networks

GUEST/VISITOR ACCESS

Aruba had an initial Guest access capability which was called "Tunneled Internet Gateway". The solution covering this use case was accomplished by placing guest access users/devices into its own dedicated VLAN after captive portal based authentication. Guest traffic was tunneled (using IPsec encryption and GRE tunnel) to another network device (i.e. typically an Internet gateway that resided in a DMZ) and provided Internet-only access. At the time, we had the appropriate DISA approvals because the solution met the definition of "logical" separation. The following figures show an example of a Tunneled Internet Gateway network topology and logical topology.

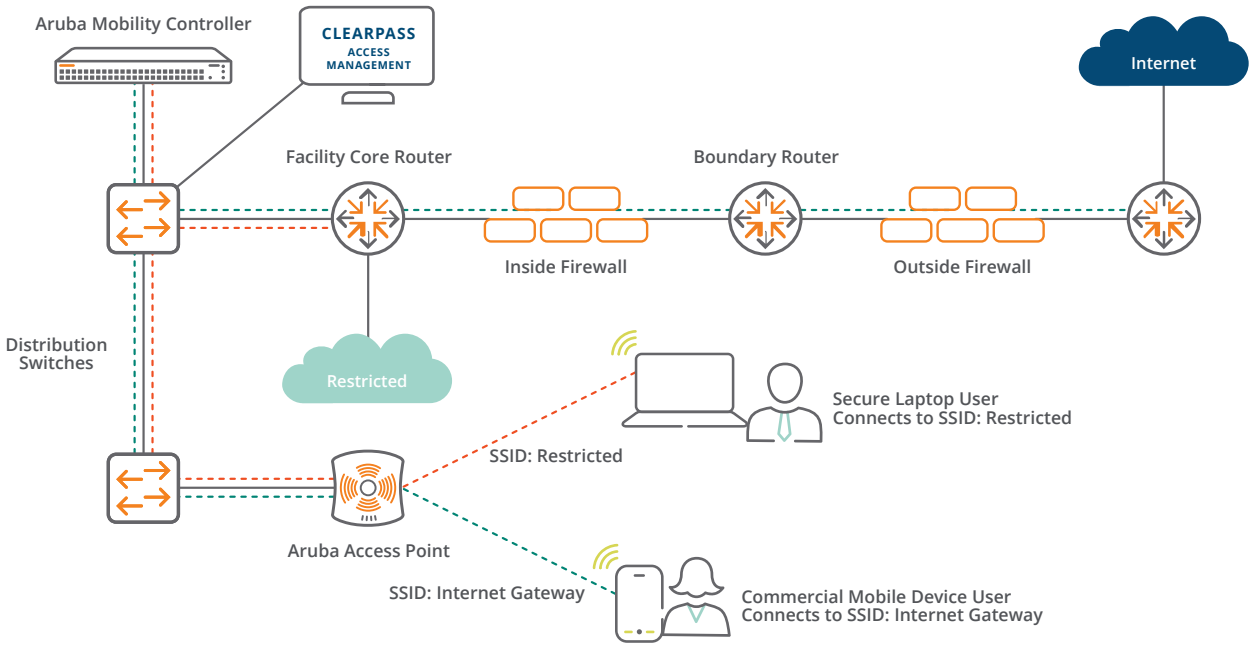

Figure 6: Tunneled Internet Gateway – Network Topology

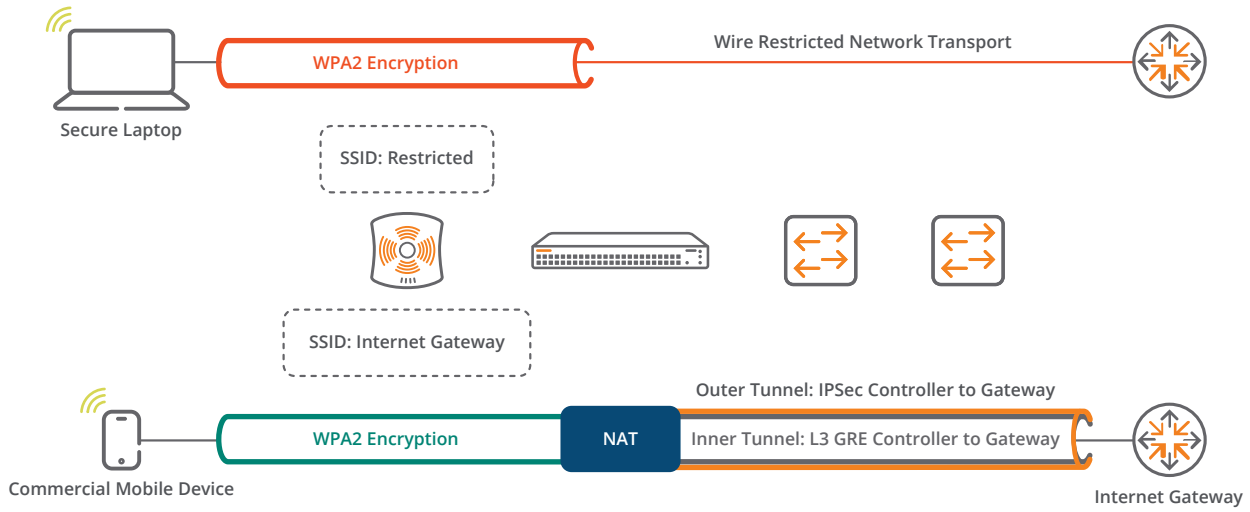

Figure 7: Tunneled Internet Gateway – Logical Topology

MultiZone AP changes the design from the tunneled Internet Gateway solution by configuring a Data Zone controller to have the APs forward authenticated guest traffic to a dedicated guest controller (still typically residing in a DMZ). This guest traffic will no longer be terminated at a single controller that resides in the core of the production network. Also, the establishment of an IPsec tunnel over a Layer 3 GRE tunnel between the production controller and Internet Gateway is no longer a requirement since the guest traffic will not touch the production Primary Zone controller. The network topology of Guest Access using MultiZone is shown below.

MULTI-TENANCY

With this use case, we will consider the scenario where the Government, contractors, and vendors require Wi-Fi access to their respective network resources. This can be provided in the way of a small enclave on the backside of their respective controllers or simply providing Internet access to establish VPN connectivity to their home base.

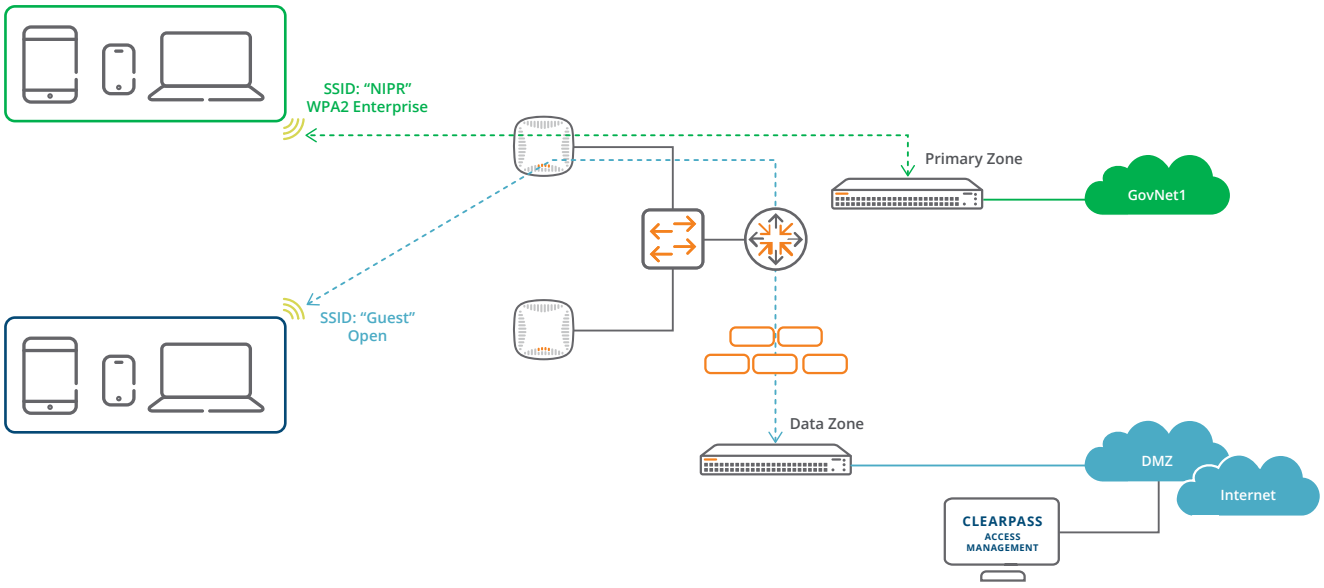

Figure 8: Guest Access – MultiZone Network Topology

In the example listed in Figure 9, the Primary Zone controller is implemented to allow the Government facility to provide Data Zone controllers, along with having management control of the APs and RF. The tenants would purchase their own Data Zone controller to be implemented (perhaps a DMZ). The contractor and vendor will have configuration control of their respective Data Zone controller.

Note that the Primary Zone controller shows an example of a three-node controller cluster for expansion and redundancy, along with the use of a Mobility Master virtual machine to configure the cluster.

IN SUMMARY

When discussing WLAN designs with prospective and existing customers, it's key to stress the importance of their selection of an overall Wi-Fi architecture design upfront. They should consider not only their current Wi-Fi requirements, but also future requirements that may need additional separation for security reasons. This is why Aruba's architecture is superior from both a security and ease of deployment perspective. Aruba's solution, which includes MultiZone AP, provides a way to easily expand the overall Wi-Fi solution to provide data separation where it makes sense and is required. When it comes to security separation, this cannot be done with any competitor solution.

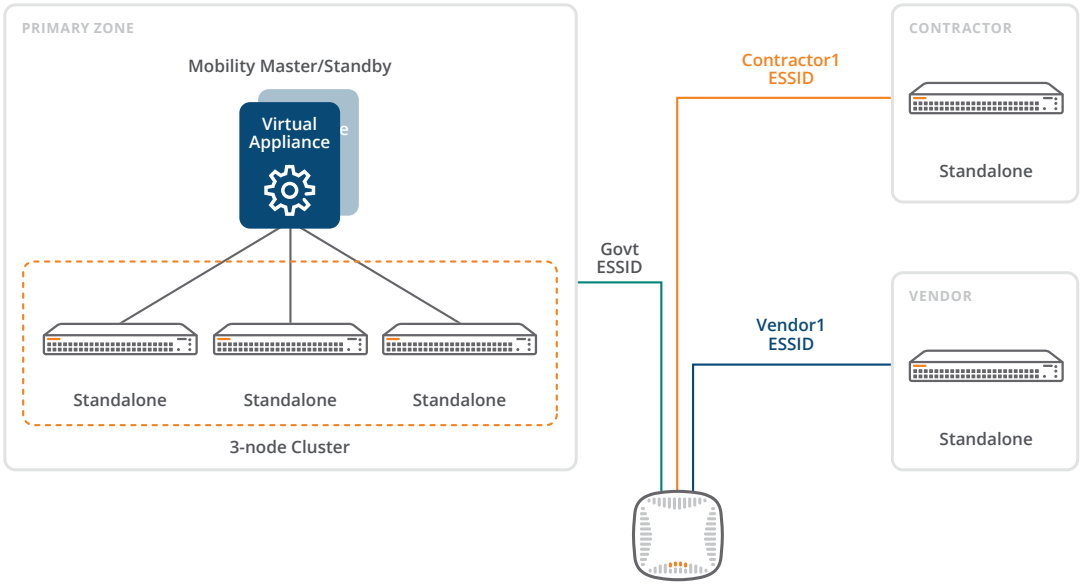

Figure 9: Multi-Tenancy Example MultiZone AP Configuration

a Hewlett Packard Enterprise company

www.arubanetworks.com

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM