



## Aruba's Guest Access Solution

Guest access is often the first application implemented by organizations deploying a WLAN. Guest access provides visible interaction with partners and visitors and makes a positive impression about the organization. A good guest access system will, first and foremost, provide reliable and high-performance access to the Internet without requiring the guest to negotiate countless hurdles reconfiguring his PC in order to connect. Aruba's follow-me connectivity and application continuity services ensure that guests experience optimum performance.

A guest access network must separate and segregate internal and guest traffic to provide iron-clad security for the organization's LAN and servers. Since guest access is provisioned on the same WLAN and LAN infrastructure carrying internal traffic, this is a significant challenge, and one that is directly addressed by Aruba's follow-me security.

## Using Guest Access

There are numerous productivity gains to be realized from providing guests, contractors and temporary workers with instant access to timely business information. Offering secure Internet access enables these users to VPN back to their corporate or home network to utilize email and other resources not stored on their laptop or mobile device.

### **PROTECTION OF THE INTRANET:**

A secure guest access solution must ensure that guests are connected directly to the Internet, but can never access internal network resources despite the fact that guest traffic runs on the organization's LAN and WLAN infrastructure alongside corporate computing traffic. Older architectures use a dedicated VLAN to provide this protection. However, VLAN administration is cumbersome, and the slightest configuration error can result in security holes, potentially allowing an intruder to use the guest access network to attack the organization's servers and resources.

Aruba implements identity-based security to identify, categorize and contain a guest's traffic no matter where they roam on the WLAN, and it does so without requiring any VLAN configuration.

Captive portals are now well-established as a means to access the Internet, whether in hotels, conference centers or Wi-Fi hotspots. When the guest first brings up a web browser, the stream is intercepted and the guest is presented with an authentication page. This captive portal, which can be customized with the organization's look and feel, can prompt for an email address, password and/or a click-through terms of use agreement.

### **FLEXIBLE, EFFORTLESS CREDENTIAL ASSIGNMENT:**

Some organizations are content to provide open Internet access to anyone in range. However, this is becoming increasingly unusual due to the risk of organizations being held responsible for misuse of its network. For instance, if

## Benefits:

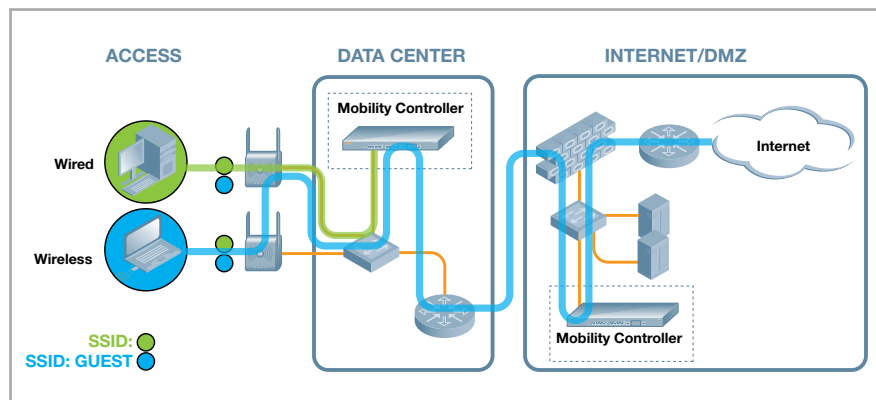
- **Separation of traffic:** ICSA-certified stateful firewall ensures guests cannot access the organization's Intranet
- **Built-in feature:** Guest access can be added to any Aruba User-centric network
- **Flexible control:** From open access for all to unique individual passwords
- **Hospitality-ready:** Integrates with third-party systems for credit card verification

an attack on a target across the Internet originates from a company's network, and they have not taken proper steps to protect their network, they could be held liable. Guest access is best controlled by issuing individual, limited-time passwords, but this can become cumbersome if support systems are not available. The best practice is to issue each guest with a pre-printed or printed-to-order card showing their unique password at the time they check in at the reception desk. This minimizes inconvenience while maximizing security.

**MINIMAL ADMINISTRATION COSTS:**

IT applications should operate without the need for frequent support and with minimal help-desk calls from users. For guest access, this means that the receptionist must be able to easily add guest accounts and quickly issue credentials. The guest should be able to gain access with minimal PC reconfiguration and the Internet service should be smooth and fast.

**USAGE AND AUDIT DATA:** Even guest access services must provide historical data accounting for who used the network, when they used it and how it was used.

**How Aruba Enables Guest Access**

The Aruba guest access solution consists of three key components – thin access points (APs), central Mobility Controllers, and security software modules for the Mobility Controller. There is also an optionally available Mobility Management System (MMS) for larger networks. APs provide secure wireless connectivity to devices and connect over existing LAN/WAN systems to carry all wireless LAN traffic through a GRE tunnel or IPsec tunnel to a Mobility Controller installed in the data center. The Mobility Controller is the central point of configuration, management, application continuity services and security. Guest access is an inherent feature of all Aruba user-centric networks.

**GUEST ACCESS ON AN EXISTING WLAN:** An Aruba user-centric network deployed for corporate use will have access points placed to provide Wi-Fi

coverage. When adding guest access, it may be desirable to cover new areas of the building with additional APs. In larger installations a Mobility Controller may be added at the DMZ of the organization's firewall. All guest traffic is carried encrypted from the APs through GRE tunnels to a Mobility Controller, and then via another encrypted tunnel to the DMZ, where it is safely connected to the firewall and the Internet. Aruba's Mobility Controllers provide an ICSA-certified stateful firewall, enabling them to perform this demanding function.

**CAPTIVE PORTAL:** Client devices connected to the network are blocked from all access until a web browser is opened and authentication credentials are entered. The exchange of authentication credentials is secured using industry-standard SSL. The system can require a valid name and password, or it can be configured to collect only non-validated

email addresses. The captive portal pages may be customized with company logos, backgrounds, acceptable use policies and other text. Provisioning of credit card access and billing systems is enabled through integration of third-party applications.

**SEPARATION OF GUEST TRAFFIC:**

Guest traffic can be separated from all corporate traffic by way of a software module on the Mobility Controller. Contractors can have a different security policy applied to them without giving them full corporate network privileges. This is a benefit of Aruba's unique

identity-based security. The policy enforcement firewall enables fine-grained user control, applying policies to individuals or groups of users.

**ROLE-BASED PROVISIONING:** Guest access is provisioned via a web page, so a receptionist can easily and quickly add a visitor's individual guest account and issue the guest a unique, trackable password. Alternatively, accounts can be pre-provisioned and matched to guests at registration. Yet another option is a common 'guest password' can be published for all guest users.

## Benefits of Aruba's Guest Access Solution

- Permits only authorized guests to use the network
- Prevents guest users from accessing the internal network: controls Internet access by time of day, location, bandwidth contract, and more.
- Provides a simple system for provisioning guest access credentials that can be used by employees and receptionists without involving IT staff
- Maintains accountability and auditing of who is using the network, when it is being used and how it is being used
- Controls guest access over both wired and wireless networks
- Provides guest access without major reconfiguration of guest computers, and without the need to call IT support staff for help
- Fully integrated with Aruba's Mobility Controller



[WWW.ARUBANETWORKS.COM](http://WWW.ARUBANETWORKS.COM)

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550