

White Paper |

Government



## **Secure Enterprise Mobility for Government Teleworkers**

Bill Moore

**ARUBA**<sup>®</sup>  
ARUBA  
networks

---

## Introduction

Government Telework initiatives are increasing with many Federal agencies and Congress supporting programs to allow federal employees traveling around the globe or working from home to access their agencies' network. The ability to remotely connect to all resources in a reliable and secure manner is of paramount concern. Regardless of location, teleworkers connection to federal resources must be highly secure and meet policy objectives such as NIST FIPS 140-2 and HSPD-12.

Teleworking requirements are traditionally met through the use of additional software and procedures that exist on top of those that the employee is required to use when physically at the office. Additional passwords and possibly security tokens are needed along with software to protect the connection, and the employee must remember to perform all of the steps in the correct order to avoid failure. The alternative is to use an expensive hardware solution that was never designed for the single home user. This solution includes dedicated VPN devices with an expensive per-user price tag and increased management overhead of configuring full scale routers at employee homes. Phone service is provided by cellular services with the increased cost and additional phone number confusion of having two lines. Any security past the initial logon is provided by the end host, breaking the principals of least access and defense-in-depth.

Adding to this cost is the additional infrastructure that was not built with secure mobility in mind. Additional administrative staff is needed to manage the remote access infrastructure and to deal with user issues as they arise. The complexity level of troubleshooting issues rise as multiple authentication systems now have to be looked at to discover the root of the problem. The devices are typically designed with the expectation that remote access would be limited in both time and speed, and that this connection would not be the users primary connection to the network.

The answer to these remote access issues is to change the remote connectivity paradigm through the use of integrated secure enterprise mobility systems. These systems include Remote Access Points (RAPs) and centralized controllers which provide mobility management and security services. The edge of the network will maintain consistent logon procedures anywhere a user connects and provide integrated QoS, stateful ICSA certified firewall-based security, and FIPS 140-2 certified encryption through a thin Access Point (AP). Users no longer need additional security controls and IT no longer needs multiple layers of infrastructure. Instead, there is a single controller providing a unified point of security with users connecting to their agencies' network with the same rights and security no matter where they are in the world. All that is needed is an Ethernet jack with network access.

## Who are our Federal Government Teleworkers?

The requirement for secure remote access that extends the office anywhere in the world is shared by a diverse group within the Federal Government enterprise.

### *Road Warriors and Day Extenders*

When we think about the typical mobility user we think of the road warrior, the person who rarely sees their agencies office and who is only known by their voice and email. Day extenders are those users who wish to continue working for a few hours in the evening once they've left the office. These users require a reliable and safe data connection to the office. Previously the voice connection was accomplished via cell phone, but soft phones and converged devices will become more common in the near term for these users. Much of their traffic will be back to the agencies office, and will rely on Wi-Fi as the primary connection to the network. To work effectively these users need an integrated RAP that allows them to connect all of their wireless devices with the security of an office environment. They need redundancy with the AP being able to fail over to a secondary mobility controller if the first is unreachable. The IT staff does not want to manage these devices any differently than any other AP, nor do they wish to deploy additional services to support the users. The final factor is cost; a solution

---

must be inexpensive if it is to be ubiquitous in the user base. They need an integrated, secure, cost effective solution with no additional management overhead or new systems to learn.

#### *Government Executives, Full Time Telecommuter, and Disaster Workers*

The Government executive's home office needs to be as connected as their onsite office, and may be the primary office for remote executives. The full time telecommuter is a new class of worker that has grown in number as bandwidth to the home increases and the search for the best talent moves beyond the local work force. Additionally, the need to work through disasters such as hurricanes, pandemics or terror attacks requires a fully connected remote office. These users require data, voice, and print services with full Quality of Service (QoS) integration. The system must be kept up and running with the ability to fail over to a secondary office should the primary be unavailable.

While the working requirements are different, the solution does not need to vary much from what already exists for the home user. High availability for the RAP is paramount as it is the life line for these users to agencies resources. IT staffs aren't going to look to add expense or complexity to their systems when supporting home users. They will look for a single, cost effective solution with central configuration and troubleshooting as an integrated extension of the tools they already have.

#### *Telecommuting Center workers*

Telecommuting Center workers have many of the same needs as the home office user. The lack of onsite or even available IT staff makes site survivability and centralized management critical to operations. The ability to dynamically select channel and power settings for the RAP that best suit the environment allows the IT staff to focus on other projects than adjusting connectivity in the stores.

### **The Productivity Gap with Traditional Remote Access**

As users leave the office, typically productivity drops due to a lack of connectivity to different devices. Devices stop working due to connectivity issues, and this lack of connectivity leads to missed calls, inability to access data resources such as email and files. It also runs into issues with added access controls that must be put in place to secure communications. Mobility can be limited when hardware devices are employed that require users to be physically close to the device instead of working from a telework location.

In contrast users now expect that there is no loss of connectivity to any system. Their laptops and phones require the same connectivity no matter where they are. This challenge must be met by providing seamless connectivity for any device that the user community requires for their job with no more effort than plugging in the RAP to an available open internet connection. They require a seamless connection with no additional requirements for security.

### **Mobile Security Issues**

Mobile Security solutions must meet policy objectives such as end to end FIPS 140-2 compliance. In addition, there must be multiple levels of security including; ensuring the legitimacy of a connection -- including encryption, multi-factor authentication and policy enforcement.

Simply getting connected to a wireless access point can prove hazardous for the user. The advent of software based access points on laptops and Trojan programs setup expressly to fool users into providing login credentials are being seen with increasing frequency wherever teleworkers connect to the network. This can often leave the unsophisticated user at a loss as to which SSID is safe and which are potential hazards. How can they know which connection is the one they should use, and which is a potential hazard?

The quicker a system attaches to a known good, secure AP the less likely potential attackers will have to sniff the systems software. When the typical laptop starts up searching for networks, lots of information about services starts to leak out, allowing unscrupulous users to capture clear text user names and passwords.

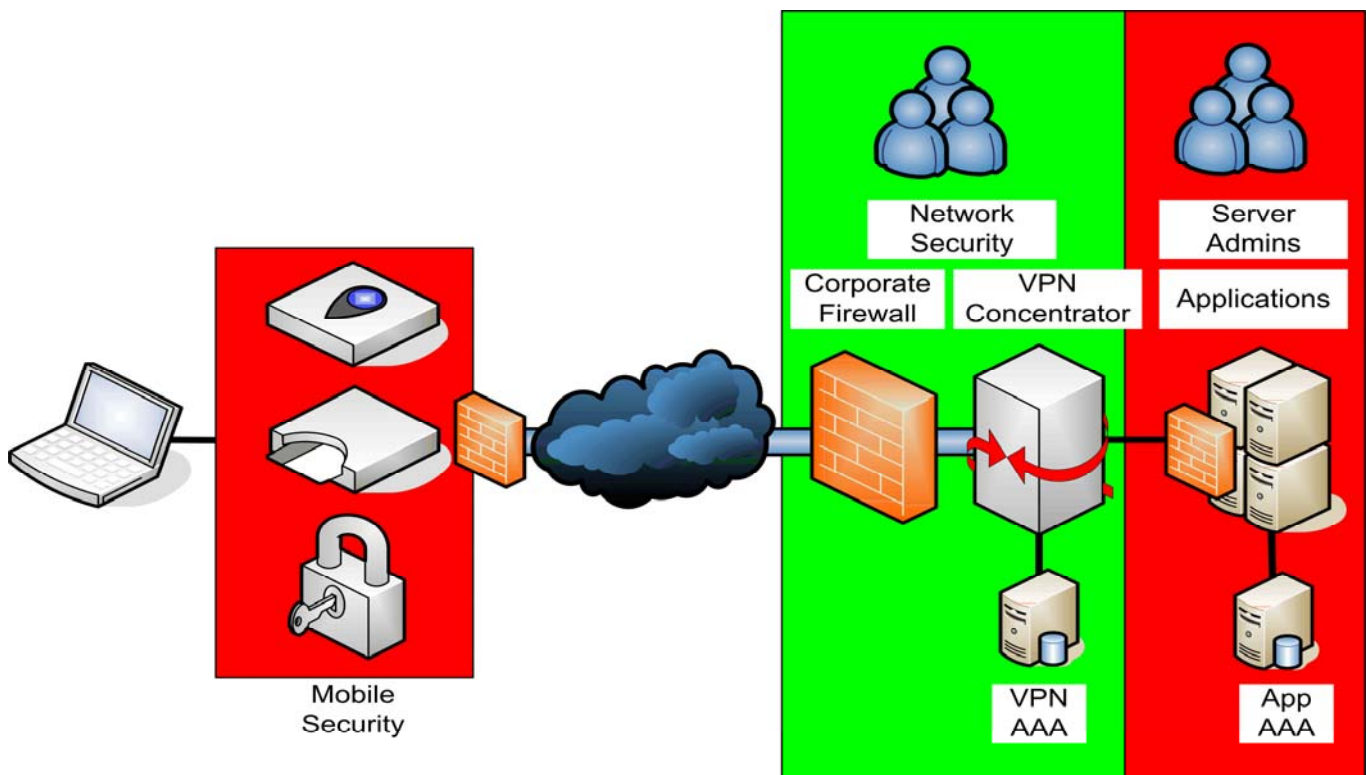
RF issues make the network administrator's life much more challenging. Troubleshooting requires more tools and of a different nature than were required previously. One must be able to 'see the air' to find a problem, and ideally the system will self adjust to handle interference or Denial of Service (DoS) attacks.

Understanding what the security solution does and when it is enabled can often lead to confusion and possible security breaches. The user may do things that violate government policies. They may also inadvertently breach security thinking that they are secured when really they have failed to fully secure the connection or the link has been broken.

When the user is connected to the network, what permissions do they have? Does the network know who the user is and can it control their permission set through the use of roles? Typical remote access solutions leave the user in a generic set of privileges and rely on end point security to limit access instead of applying defense-in-depth security measures and least privilege access at the network edge. This same flaw can also lead to a lack of privilege that the user would experience logged into their agencies network, breaking the user experience when the user is mobile. At each system the user is asked to authenticate to gain privileges, slowing the user's workflow and making remote usage more frustrating.

### A Look at Current Technologies

Typically, teleworkers will use one of two connections to the agencies office, IPSec connections or SSL VPN connections. These are proven technologies, but they suffer from a number of drawbacks including lack of privilege enforcement and the overhead of configuration and maintenance. Additionally, this moves security into the hands of the users and system administrators instead of with the trained network security staff, increasing the possible points of failure.



This additional set of systems requires the IT department to not only configure the user for secure wireless within the building, but they must also outfit all of the user's mobile devices with security packages that conform to standards. Clients must be kept up to date along with the additional infrastructure of the VPN system itself.

The newest breeds of converged devices don't necessarily support the same software that the user uses on their PC systems. This leads to more testing and troubleshooting by the already overworked IT staff. Incompatible systems must run off of the agencies network, or worse will encourage the use of unsafe communication channels. Even hardware VPN devices with their high per-user cost and added complexity can compromise security when the user plugs in a consumer grade wireless AP to enable mobility. Converged devices also present a problem when it comes to prioritization. These solutions were designed with the idea that data is data, and that prioritization for remote users is unnecessary. This is not the case when the connection begins to carry voice and video connections.

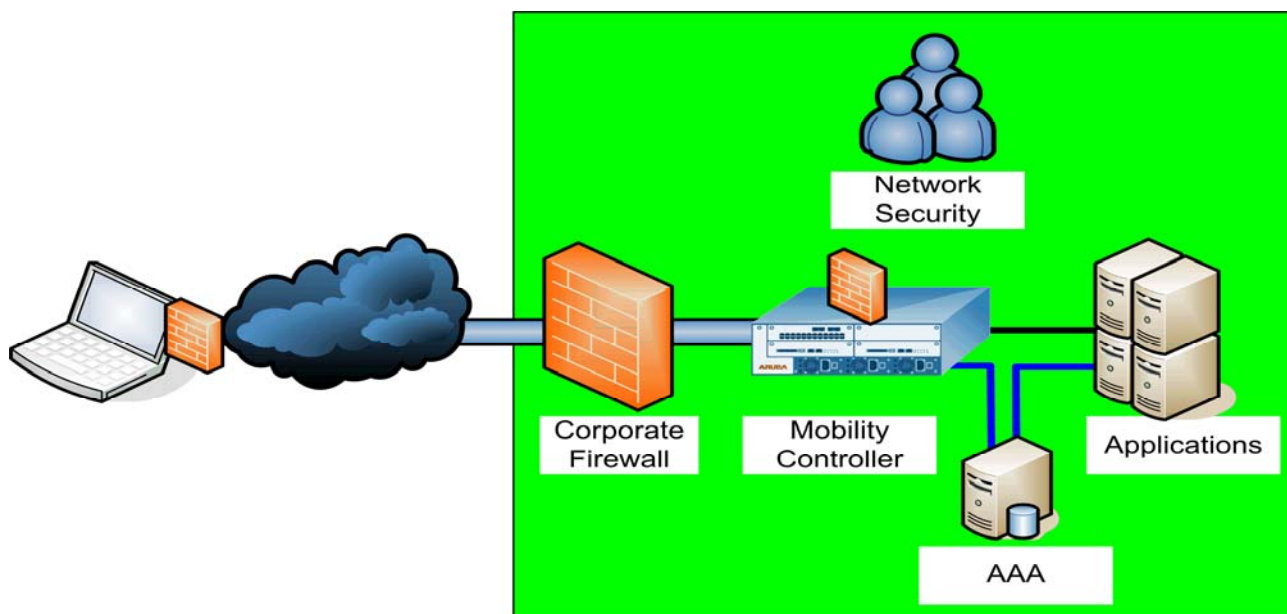
Prioritization of voice over data connections must be done to have a usable voice connection without noticeable drops and delays.

Most systems today are unable to provide any posture and compliance checks when a user logs into the network via the remote connection. Typically this resource is available within the government agencies infrastructure, but few integrated solutions exist for remote users.

In a traditional network security platform, all of this leads to an expensive solution that is not completely integrated. It also fails the user knowledge test, they are keenly aware that they are dealing with security mechanisms. The solutions lack uniformity in privilege and security provided. What is needed instead is a cost effective, integrated solution that doesn't let the user know that they are dealing with a highly secure system. Seamless secure connectivity no matter where the user is.

### The Remote Access Point Solution

Remote Access Point (RAP) solutions involve configuring a standard thin access point to provide certain level of services to the user by tunneling securely back to the government agencies network. The same SSIDs, encryption, and authentication requirements that exist on the agencies network are present on the RAP. The user's laptop will automatically associate with the RAP just as it would in the agencies network, and allows for centralized management of a truly mobile network. Two models of RAP must work to provide the required service to the two classes of user, thin wireless only APs and 'home router' style APs that are configured from a central location.



---

What a RAP is not is a simple home device. It is instead an extension of the agencies network in a similar fashion to a branch office with fewer configuration headaches. To do this effectively requires a secure integrated mobility solution.

The feature integration of the functions into the Mobility Controller and thin AP as a system is critical to having a solution that is both technologically and cost effective. By integrating authentication, encryption, firewall, and QoS features into a single device the network administrator has a single point of troubleshooting and maintenance to deal with. This reduces both initial capital expenditure as well as ongoing maintenance costs. It also provides a solution that does not add any additional burden to the user beyond their regular login credentials. They simply see connectivity to the home office the same as it is when they are in the office.

### *Reducing Complexity through Centralized Management*

Home APs typically have a web interface that allows a number of settings to be configured and few if any troubleshooting capabilities. The average user is likely to use an insecure encryption method or leave security off completely in favor of easy access to the system. When an issue occurs, very few home users have the ability to troubleshoot the problem if the tools are even available.

By centralizing management of RAP systems all management and troubleshooting is handled by a single group on a single platform. When the device boots it will establish a connection to its home controller and download its configuration file over a secure link. Encryption and firewall policy can be configured and enforced from the IT department using profile based systems to insure uniformity. Troubleshooting can be performed on the packets entering the centralized location, and the RAP can be interrogated as to the state of connections and environmental conditions.

The RAP must also enable the network engineers to capture packets from the RAP with the clients still connected. This is extremely critical in home offices where a truck roll is not cost effective. It is also not a workable solution to have the RAP switch into a 'sniffer mode' where clients are no longer allowed to attach, as it completely defeats the purpose in a home environment. The network engineering staff must be able to capture the air as if they were sitting locally to effectively troubleshoot and resolve issues.

### *Projecting Government agencies SSIDs and User Sign On*

Mobility systems typically have a list of acceptable SSIDs with which they will attempt in order to associate with. The agencies SSID is pre-configured on a user's wireless devices and typically configured to be at the top of the list of preferred SSIDs. Authentication with this SSID is typically handled through a login method such as Windows login and leverages 802.1X and RADIUS systems.

The RAP solution is an extension of the agencies network to the user's location no matter where they are in the world. The AP broadcasts the agencies SSID once it has established a connection with its centralized controller. The laptop or converged device will automatically associate with the device and allow the user to login to the system as they normally would, leveraging the authentication protocols that the user would see if they were at the office.

This is a critical difference from the user's perspective. They see no change in logging in with a RAP solution vs. logging in at the office. There is nothing additional to remember and no workflow changes; it is completely transparent security and an identical user experience. This reduces IT costs and help desk calls, along with the centralized troubleshooting previously mentioned brings down the overall maintenance costs of the RAP solution.

---

## *Visualizing the RF Environment and Protecting the Air with WIDS/WIPS*

Traditional wireless networking doesn't make life easier on network administrators. Well understood calculations about wired networks are tossed out the window due to fluctuations in bandwidth and interference from other data devices and non-data devices alike. At the same time security is vital. Wireless is analogous to placing Ethernet jacks to your network on the outside of your building. What are needed are new tools to help manage the environment, recognize potential attacks and take action.

RF management must be able to examine the environment and if appropriate change channel and power settings. What is needed is an Adaptive Radio Management (ARM) system. The RAP system must be able to sample the air on other channels as well as its own, and when appropriate make changes. This sampling is also critical to defend the AP against attack. There is no way to prevent a Layer 1 (L1) attack in a wireless environment. Intentional and even unintentional jamming is easily done and requires either user or system intervention to select another channel.

While scanning the air it is also useful for the AP to recognize common attacks and to take action against the devices. Man-in-the-middle attacks and AP spoofing can often be handled by the combination of the AP and centralized controller. Additional information can be provided to administrators through integration with traditional Intrusion Detection Systems (IDS) that are aware of wireless environments such as the open source tool Snort. Being able to detect and take action are required to defend the network against intrusion, while alerting administrators to the issue for further action.

## *Understanding Centralized and Local Encryption Options*

Strong encryption is becoming much more common on hardware platforms. It is not uncommon for connections to support partial and full implementations of 802.11i security, better known as WPA2. The choice to encrypt then becomes a choice between where the user data will ultimately end up. For many of these users the data is primarily agencies bound allowing encryption to terminate on the centralized wireless controller.

Federal agencies require use of FIPS 140-2 certified solutions such as 802.11i/WPA2 for 802.11 wireless networks through the use of the AES encryption standard. There is no benefit gained from putting this wireless network traffic inside another encrypted tunnel to pass it over the internet connection. By simply wrapping a GRE header around the traffic it can be securely passed back to a centralized controller for decryption. The RAP would only terminate encryption when local resources or split tunneling is required.

For other users who may need to access resources locally, it will make sense to terminate encryption at the RAP instead of at the agencies office, where the traffic would have to make a round trip to the resource. Instead, the RAP will decrypt the wireless data. The RAP will create a secure tunnel for data on the path back to the agencies office and bridge traffic for the local network. Unlike previous Fat AP models, the RAP still takes configuration and control information from a central master controller, making the RAP a mini local controller.

## *Reducing Traffic Backhaul with Local Bridging*

Obviously not all traffic is destined for the agencies network, and backhauling the traffic makes very little sense from both a cost and speed perspective. As such, the RAP must be able to accept and act on basic routing information passed to it in its configuration file. Traffic destined for the agencies office should be placed on a connection to that destination, and local or internet bound traffic should be locally bridged.

---

The AP should also be able to advertise a second SSID for locally bridged traffic. This would include the ability to have guest access at a small office or retail location, or provide wireless access for personal web surfing in a user's home. For security reasons, the AP must still be able to perform encryption on these connections, and must completely segregate the traffic.

### *Defending the Network with Stateful Firewalls and NAT*

Network traffic can be segmented into two zones. The first zone is protected behind the RAP. This includes the authorized local devices which are able to access the agencies network. There must also be an untrusted zone that includes everything on the other side of the RAP, essentially the entire internet. At no time should traffic be able to transverse from the internet onto the agencies link.

This protection requires a stateful firewall to enforce traffic patterns. The firewall must be able to follow traffic statefully and be able to apply different policies based on where the traffic originates, is destined, and what protocol is traversing the network. The RAP must also be able to NAT effectively to allow devices behind the firewall to obtain agencies IP addresses while still communicating with the local internet connection.

### *Ensuring a Usable Connection with Quality of Service*

Quality of Service (QoS) becomes an absolute necessity as Voice over Wireless LAN (VoWLAN) and Fixed Mobile Convergence (FMC) solutions become more common. The access point and mobility controller must be able to prioritize traffic either via traffic aware queuing or more commonly by adopting the Wireless Multi-Media (WMM) standard put forth by the Wi-Fi alliance. This requires an integrated end-to-end solution of prioritizing, tagging, queuing, and enforcing policy on voice traffic.

The access points and centralized controllers must prioritize traffic correctly, placing higher priority voice traffic above that of background data traffic both on the air and on the wire. These packets must be correctly tagged in both upstream and downstream directions irrespective of the medium used. The RAP must also be able to leverage a stateful firewall to insure that voice prioritized traffic is destined for a voice server and is in fact voice traffic. This last piece is critically important with converged devices such as Wi-Fi capable phones and soft phones on laptops. Without this level of integration QoS becomes meaningless as everything becomes "high priority" for the user.

### *Keeping the Lights on with Site Survivability*

The ability to survive a network outage is more critical to the RAP serving local resources. If the WAN link fails all agencies resources are lost no matter which flavor of RAP is in use. Ideally the AP should maintain internet connectivity with access to local resources via wireless so that work can continue until such time as the WAN link can be restored.

### *Simplifying Troubleshooting of Complex Services*

Typical remote access solutions allow for extensive troubleshooting, but often the device is managed by a separate group in the IT organization and requires coordinated troubleshooting by multiple parties to resolve an issue. Troubleshooting with RAP and centralized management is simplified by having a single interface to perform troubleshooting procedures. The system should present statistics on the user as well as allow for remote monitoring of the RF environment and for remote packet captures. The ability to 'capture the air' in a wireless network can be crucial to troubleshooting complex interference problems.

## **Conclusion**

Remote access solutions can no longer be a "connection of convenience" that is nice to have when it works. Teleworkers now utilize internet broadband connections that in many cases are more robust

---

than their agencies network connections. Connectivity requirements for teleworkers, whether traveling or working from home, must be pervasive. The federal employee expects an assured, available connection to their agencies resources from anywhere. This is a new vision of connectivity and mobility with full identity-based access to a converged data and voice network. This connectivity allows users to remain connected and productive no matter where they are in the world with the assurance that their communications are protected.

IT managers benefit from not only reduced capital expenditure costs, but reduced administrative costs as their teams move from limited point solutions to integrated mobility solutions. Centralized troubleshooting, RF management, and security allow a single platform to control access and provide seamless connectivity and security at a reduced cost. IT security moves from something that users see as a burden they must comply with to something transparent that they don't even realize is in operation. The integration of security measures provides uniformity of the user experience, increasing productivity and reducing the chances of user error.

Centralized controllers and the RAP solution integrate the requirements of both network operations and security teams in a simple to deploy and manage package. Administrators get a system they can configure once and deploy. Advanced troubleshooting and reporting tools as well as firewalls and IDS systems are completely integrated. Aruba's user-centric networking architecture extends further, allowing users to seamlessly shift from working at the office to working from a hotel room or home office with no changes to their established workflows. There are no new passwords to remember, no key fobs to carry, no software to launch. As far as the user is concerned the system simply works.

## **About Aruba Networks**

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.

WP\_GVSECMO\_US\_071217



1322 Crossman Ave. Sunnyvale, CA 94089-1113  
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | [info@arubanetworks.com](mailto:info@arubanetworks.com)  
<http://www.arubanetworks.com>