WHITE PAPER

TUNNELED INTERNET GATEWAY

WI-FI ACCESS FOR MOBILE DEVICES IN HIGH-SECURITY ENVIRONMENTS

aruba NETWORKS

TABLE OF CONTENTS

THE CHALLENGE: WI-FI ACCESS FOR MOBILE DEVICES IN HIGH-SECURITY ENVIRONMENTS

Since the debut of the iPhone in 2007, the private sector has seen a proliferation of personal mobile devices used in the workplace. Government customers, while slower to adopt commercially available mobile devices in the workplace, recognize the cost and productivity advantages and are looking for ways to increase their usage and speed-up adoption.

Many civilian and military organizations have already begun large-scale acquisitions of commercial off-the-shelf (COTS) mobile devices for distribution to relevant personnel. The February 2013 purchase by the U.S. Department of Defense of 630,000 Apple iOS-based mobile devices is just one example. These devices require Internet connectivity to unlock their full functionality and productivity benefits.

Yet in many government facilities, security requirements around network connectivity mean that commercial mobile devices must be air-gapped from restricted networks, necessitating a costly build-out of parallel network infrastructure just to link these devices to an Internet gateway.

ARUBA TUNNELED INTERNET GATEWAY SOLUTION

In situations where a restricted wireless LAN (WLAN) is the only available network within the premises, enabling wireless connectivity for mobile devices requires infrastructure changes in the form of a parallel network with dedicated access points (APs) for guest use or cellular antennas installed within the facility for 3G/4G connectivity to the cellular network. Both options are costly, time-consuming and require ongoing maintenance.

Aruba Networks® offers an alternative known as the Tunneled Internet Gateway. In environments with Aruba controller-based WLANs, mobile device users can connect to the local Aruba AP and securely traverse restricted intermediate networks to access an Internet gateway.

Unsecure Internet traffic is logically and cryptographically separated from restricted network traffic within the AP and across the network. The result is that mobile device users are able to access the Internet without compromising the security of the restricted network.

HOW THE TUNNELED INTERNET GATEWAY WORKS

Summary

The Tunneled Internet Gateway is enabled through software configuration to any new or existing controller-based Aruba WLAN. Mobile users connect their devices to the Internet gateway SSID, creating an encrypted session with an Aruba Mobility Controller deployed in the restricted network.

The controller maintains logical separation between Internet sessions and restricted sessions using a Common Criteria EAL4+ validated firewall, then routes Internet traffic through an additional encrypted data tunnel to a router attached to a commercial Internet service provider. The result is a secure, simple and low-cost network overlay with strong separation between restricted and Internet data.

Technical details

Wireless APs are typically connected to a restricted wired network, which provides IP connectivity between the AP and an Aruba Mobility Controller installed in a network data center or wiring closet.

Policy-compliant wireless devices may access the restricted network directly after authentication. These devices typically implement strong forms of encryption and authentication, and may have numerous locked-down settings.

However, unsecure devices must not have access to the restricted wired network and this requires a strong separation mechanism. Only the Aruba architecture can achieve this using central encryption. With Aruba, wireless traffic is not decrypted or processed in the AP – it is wrapped in an IP tunneling protocol and sent across the wired network to the Aruba Mobility Controller.

When the traffic arrives at the Mobility Controller, is it unwrapped, decrypted and converted into a standard network frame. All other WLAN vendors perform encryption/decryption inside the wireless AP, putting the network at serious risk for compromise.

With the Tunneled Internet Gateway, mobile devices are treated similarly to guest access devices. Authentication is required through the use of a browser-based captive portal. After authentication, traffic from a mobile device is separated within the Mobility Controller based on the authenticated role of the mobile device user.

The integrated EAL4+-validated firewall within the Mobility Controller forces all unsecure mobile device traffic into a second encrypted IP tunnel, destined for an Internet gateway. At the same time, other policy-complaint devices using strong authentication mechanisms are given access to the internal restricted network.

Any attempt by an unsecure mobile device to access resources on the restricted network is blocked, and can optionally trigger the client to be disconnected. Since the Mobility Controller can determine what type of device is authenticating through device fingerprinting capabilities, additional restrictions can be implemented to only allow authorized device types onto the network.

The diagram below shows an example of how separation would occur with the Tunneled Internet Gateway.

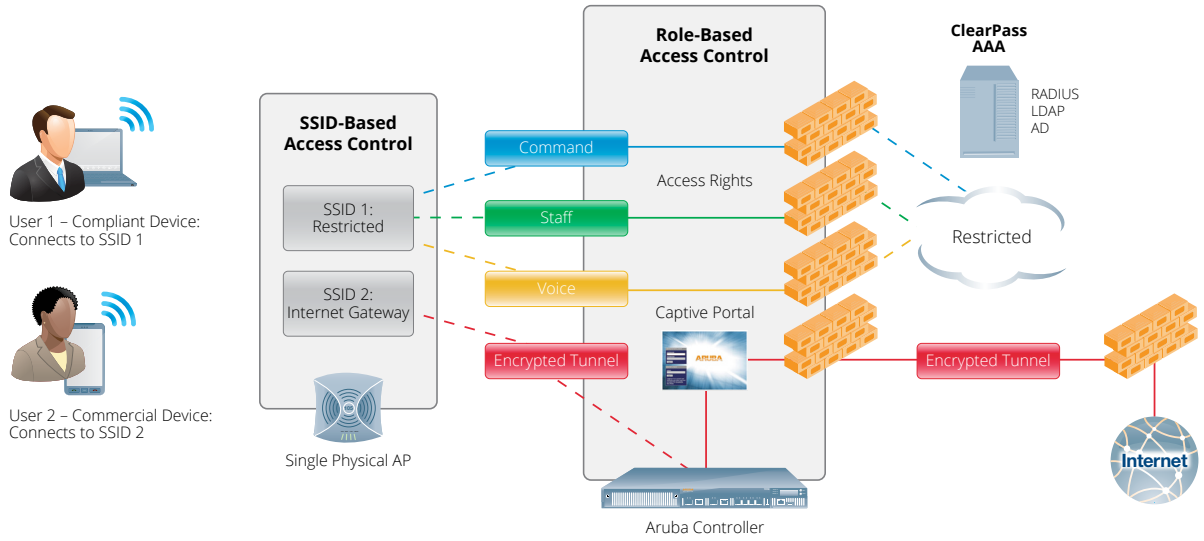

Figure 1: Strong separation in the Tunneled Internet Gateway.

Figure 2: Customizable captive portal registration page.

Authentication

Authentication of Internet-only mobile devices is typically provided by two mechanisms – Wi-Fi using WPA2-PSK or captive portal per-user authentication.

Wi-Fi using WPA2-PSK offers AES-128 encryption with authentication provided by a preshared key. Even though the Internet-only network is untrusted, it is important to provide an encrypted/authenticated network so the general public will be unable to access it. The preshared key is commonly distributed to authorized users by simply printing it out and posting on walls within a facility.

Captive portal per-user authentication is optional. It is used when an organization wishes to establish the identity of an individual Internet user. The captive portal requires a standard web browser and can be customized for look-and-feel with an acceptable-use policy statement inserted for legal purposes.

The Aruba ClearPass Policy Manager serves as the backend authentication database and links to many popular directory services in order to verify authorized user credentials and IT access policies.

Upon connecting to the network and entering a valid username and password, the client device and user are Internet-only authenticated, meaning that the device can be utilized for Internet access only.

Role-based user and device policies can be continuously implemented to prevent access to restricted network data and resources. Internet access using HTTP and HTTPS protocols are allowed when accessing the Internet and other protocols can be defined by the administrator as needed.

Implementing the Mobility Controller using the above configuration provides sufficient data separation from restricted network traffic and, for U.S. DoD customers, provides compliance with Standard Technical Implementation Guides (STIGs) for the DISA Wireless Overview and Internet Gateway Only.[1]

Potential use-cases

Any government or enterprise facility that has a restricted network as the sole available wireless network to access the Internet would be an eligible use-case for the Tunneled Internet Gateway. Examples include, but are not limited to:

- Military facilities
- Military contractors and suppliers
- Embassies/consulates
- Homeland security/national police
- Law enforcement
- Department of Energy laboratories
- Treasury/tax bureaus

STIG compliance

Implementation in U.S. DoD sites requires compliance with the U.S. Defense Information Systems Agency STIGs. The Aruba Tunneled Internet Gateway is compliant with the following STIGs (detail in appendix):

- STIG-ID: WIR0100
- STIG-ID: WIR0105
- STIG-ID: WIR0110
- STIG-ID: WIR0120
- STIG-ID: WIR0121
- STIG-ID: WIR0122
- STIG-ID: WIR0123
- STIG-ID: WIR0124
- STIG-ID: WIR-0130

In addition to compliance with the above STIGs, Aruba mobility solutions have been tested and validated compliant with Common Criteria and FIPS 140-2.

APPENDIX

STIG compliance – details

Rule Version (STIG-ID): WIR0100

- Rule title: The relevant U.S. Forces Command (USFORSCOM) or host nation must approve the use of wireless equipment prior to operation of such equipment outside the United States and its possessions (US&P).
- Vulnerability discussion: When using a wireless system outside of the US&P, host nation wireless spectrum regulations must be followed. Otherwise the system could interfere with or be disrupted by host nation communications systems.

[1] Specific STIGs in Appendix

- Compliance: With Aruba's mobility solution is in operation already at all U.S. Air Force bases. The overall solution has been approved and currently meets the requirements from this STIG rule. Depending on where Aruba controllers are deployed and configured at initial set up time, it should be set for the appropriate country code to comply with the spectrum regulations both within the United States and other host nations. This configuration setting adheres to the regulatory domain regulations for these nations and is automatically set for all APs deployed within the overall solution. Some of the considerations include use of specific frequencies (i.e. 2.4 GHz, 5 GHz, and 4.9 GHz), transmit power, and 802.11 EIRP (Equivalent Isotropically Radiated Power) maximum allowances, based on the host nation, etc. Controllers deployed within the U.S. are based on a specific U.S. version of the controller. In this case, the controller is automatically set for U.S. regulatory domain settings and cannot be changed. Controllers deployed OCONUS (except Alaska, Hawaii and other U.S. territories) would deploy a rest-of-world controller, where the country code of deployment is selected at the initial setup configuration time.

Rule Version (STIG-ID): WIR0105

- Rule title: WLAN SSIDs must be changed from the manufacturer's default to a pseudo random word that does not identify the unit, base, organization.
- Vulnerability discussion: An SSID identifying the unit, site or purpose of the WLAN or is set to the manufacturer default may cause an OPSEC vulnerability.
- Compliance: While the Aruba Mobility Controller ships with default values and profiles, the default SSID is disabled by default. Thus, no SSID can be seen at initial startup time, requiring the configuration of new SSIDs, with various security configurations, to be implemented.

Rule Version (STIG-ID): WIR0110

- Rule title: The WLAN inactive session timeout must be set for 30 minutes or less.
- Vulnerability discussion: A WLAN session that never terminates due to inactivity may allow an opening for an adversary to highjack the session to obtain access to the network.
- Compliance: Upon client authentication to the network, configurable AAA timers exist within the controller to monitor client activity. The idle-timeout AAA timer is set to five minutes of idle time (default). This is the maximum number of minutes after which a client is considered idle if there is no user traffic from the client. The timeout period is reset if there is user traffic. Idle clients are removed from the controller as authenticated client sessions. These clients will require a re-authentication to be able to get back onto the network.

Rule Version (STIG-ID): WIR0120

- Rule title: WLAN signals must not be intercepted outside areas authorized for WLAN access.
- Vulnerability discussion: Most commercially-available WLAN equipment is preconfigured for signal power appropriate to most applications of the WLAN equipment. In some cases, this may permit the signals to be received outside the physical areas for which they are intended. This may occur when the intended area is relatively small, such as a conference room, or when the AP is placed near or window or wall, thereby allowing signals to be received in neighboring areas. In such cases, an adversary may be able to compromise the site's OPSEC posture by measuring the presence of the signal and the quantity of data transmitted to obtain information about when personnel are active and what they are doing. Furthermore, if the signal is not appropriately protected through defense-in-depth mechanisms, the adversary could possibly use the connection to access DoD networks and sensitive information.
- Compliance: There are a number of configurable options within the Aruba Mobility Controller that limit RF and the ability of RF to be intercepted from areas where such interception is undesirable. For example, Aruba Adaptive Radio Management™ (ARM) has options to limit both transmit-power in order to mitigate interference, along with coverage of such APs. Typically, ARM sets transmit powers by default to a value less than max, depending on how APs are deployed. In addition to this, other mechanisms can be deployed. For example, depending on where the APs are deployed (and their surrounding neighboring areas), these APs can be specifically configured to limit transmit power to a maximum. The Max Tx EIRP parameter within the ARM™ profile can be configured to values anywhere from 3 dBm up to the maximum allowed based on the regulatory domain of the host country. In addition to the above, Aruba offers APs that allow for the implementation of directional antennas, as discussed in the "Fix" section of this rule. By utilizing directional antennas, RF coverage is provided towards the direction that the antennas are facing, limiting RF emission from the rear of the antenna.

Rule Version (STIG-ID): WIR0121

- Rule title: WLAN AP must be configured for Wi-Fi Alliance WPA2 security.
- Vulnerability discussion: The Wi-Fi Alliance's WPA2 certification provides assurance that the device has adequate security functionality and can implement the IEEE 802.11i standard for robust security networks. The previous version of the Wi-Fi Alliance certification, WPA, did not require AES encryption, which must be supported for DoD WLAN implementations. Devices without any WPA certification likely do not support required security functionality and could be vulnerable to a wide range of attacks.
- WPA2 Enterprise or WPA2 Personal (WPA2-PSK) is acceptable.
- Compliance: Aruba Mobility Controllers support the use of both WPA2 Enterprise with 802.11i and WPA2-PSK (Personal), or both simultaneously. Both are FIPS validated encryption algorithms that are allowed to be used within the Internet Gateway Only STIG. When configuring an SSID to use WPA2-PSK, the use of a strong passphrase is required and supported.

Rule Version (STIG-ID): WIR0122

- Rule title: The password configured on the WLAN AP for key generation and client access must be set to a 14-character or longer complex password as required by USCYBERCOM CTO 07-15Rev1. Applies to the passphrase for WPA2-PSK.
- Vulnerability discussion: If the organization does not use a strong passcode for client access, then it is significantly more likely that an adversary will be able to obtain it. Once this occurs, the adversary may be able to obtain full network access, obtain DoD sensitive information, and attack other DoD information systems.
- Compliance: Aruba Mobility Controllers support the ability for the WPA2-PSK passphrase to be comprised of at least two of each of the following: upper case letter, lower case letter, number, and special character, as required per the STIG for all APs/controllers that will not use AAA services (RADIUS) for client authentication.

Rule Version (STIG-ID): WIR0123

- Rule title: WLAN APs and supporting authentication servers used for Internet-only connections must reside in a dedicated subnet off of the perimeter firewall.
- Vulnerability discussion: If the AP or its supporting authentication server is placed in front of the perimeter firewall, then it has no firewall protection against an attack. If the AP or its supporting authentication server is placed behind the perimeter firewall (on the internal network), then any breach of these devices could lead to attacks on other DoD information systems.
- Compliance: Aruba Mobility Controllers support the ability to implement non-NIPRNet based VLANs and IP subnets from within the controller. Separation between NIPRNet and non-NIPRNet IP subnets are provided from within the controller. The Aruba Mobility Controller supports an integrated stateful policy enforcement firewall accredited to EAL4+ that allows traffic for Internet Gateway Only traffic to be placed in a VLAN, IP subnet, or tunnel that places it away and off of the perimeter firewall. In essence, the Aruba Mobility Controller acts as a perimeter firewall by separating non-NIPRNet traffic and keeping it outside the firewall towards the DMZ and Internet. The controller supports both user and device role based policies. However, it can also support controller port based policies denying incoming traffic initiated from the outside.

Rule Version (STIG-ID): WIR0124

- Rule title: The perimeter firewall must be configured as required for the dedicated Internet-only WLAN infrastructure subnet.
- Vulnerability discussion: If the perimeter firewall is not configured as required, users connecting to an AP may be able to compromise internal DoD information systems.
- Compliance: Aruba's mobility solution provides compliance to this as described in the compliance information from Rule Version WIR0123 mentioned above.

Rule Version (STIG-ID): WIR0130

- Rule title: WLAN equipment obtained through acquisition programs must be JITC interoperability certified.
- Vulnerability discussion: Interoperability certification assures that warfighters can communicate effectively in joint, combined, coalition, and interagency environments. There is some degree of risk that systems without JITC certification will fail to interoperate. WLAN equipment is also required to be WPA2 certified (verified in another check procedure), which also provides significant interoperability assurance. The Wi-Fi Alliance WPA2 certification is not granted unless the product also has a radio subsystem compliant with the IEEE 802.11a, b, g, or n specifications. Products are tested with many other products to ensure interoperability.
- Compliance: Aruba is consistently active with regard to required validations and certifications for use within DoD environments. Aruba's Mobility Controllers and APs have been submitted to JITC for interoperability testing and WPA2 certification. The mobility solution has achieved a Unified Capabilities-Approved Products List certification from JITC. Information about this certification can be found at https://aplits.disa.mil/processAPList.do.

TOPOLOGY DIAGRAMS

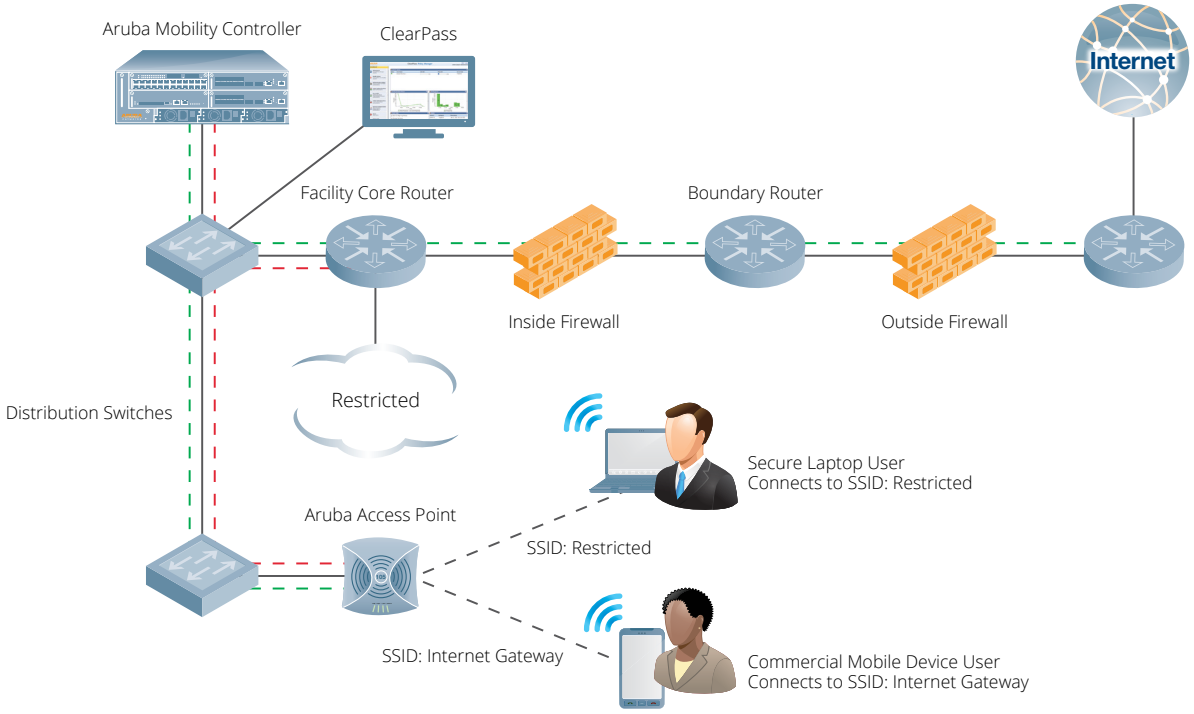

Figure 3: Tunneled Internet Gateway – Network Topology

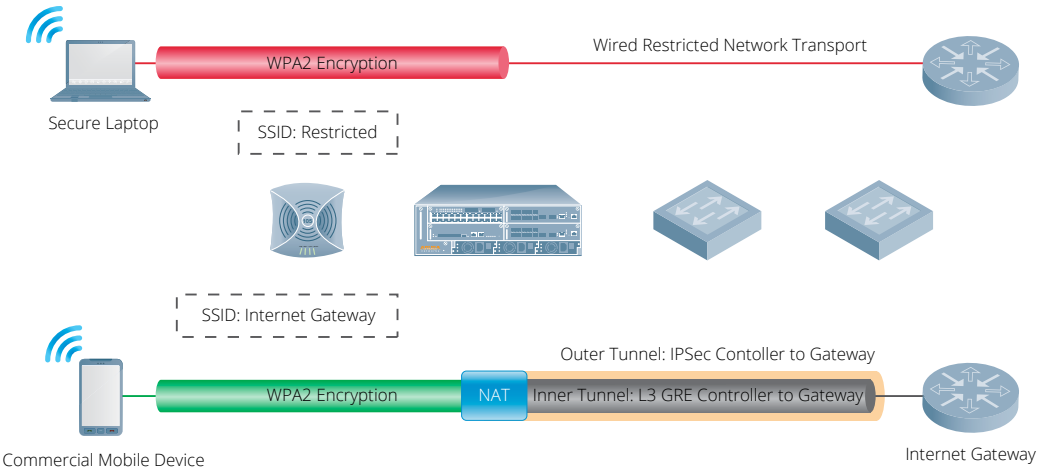

Figure 4: Tunneled Internet Gateway – Logical Topology

ABOUT ARUBA NETWORKS, INC.

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks enables IT organizations and users to securely address the Bring Your Own Device (BYOD) phenomenon, dramatically improving productivity and lowering capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com