SOLUTION BRIEF

NEXT-GENERATION GUEST NETWORK ACCESS FOR #GENMOBILE

Best practices that safeguard visitors and internal assets

Users today expect to connect from anywhere and giving them high-performance guest access is absolutely essential. Weak security on your guest network can expose your business to external threats and create serious liability issues.

If your guest network purely uses a shared key or an open SSID, you can forget about security. Anyone can connect when they want, and you have no record or way to enforce restrictions.

Fortunately, there are new, better ways to secure your guest network that involves very little IT intervention.

PRESHARED KEYS ARE OBSOLETE

Ever been to an office with combination locks on the restroom doors? It's usually an inconvenience as guests need to acquire the code. The physical security is a misconception. Similarly, securing your guest network using a preshared key (PSK) isn't very secure and can be just as frustrating for guests.

The use of a guest portal in tandem with an open SSID and other network controls can provide the appropriate balance of security and usability, without the hassle of managing PSKs. This also provides flexibility to streamline workflow processes for external guest connectivity.

- Portals can be customized with your organization's look and feel and configured to ask for specific information about your guest.
- When pairing a portal with sponsor-based approval, companies benefit by gaining governance around their guest access process.
- Login credentials are only issued to authorized guests.
- Guest traffic can be properly segmented and differentiated from other traffic utilizing role-based enforcement.
- In many retail and public venues, guest access is wide open, with a click-and-accept approach. Alternate lightweight logon mechanisms, such as Facebook, Google and other social media logins, can provide user identity and more information on the customer.

As a result, no access privileges are granted without an approved identity. Session data associated with a visitor's credentials are accurately captured for troubleshooting, law enforcement or compliance retention requirements.

GET RID OF VULNERABILITIES

One of the biggest security threats to open SSID guest networks is a man-in-the-middle attack. Wi-Fi is a shared medium and open wireless networks do not encrypt traffic or ensure the integrity of traffic.

Consequently, it's easy for an attacker to broadcast your SSID and intercept your guest's traffic. These honeypots open your network and guests to endpoint attacks, data leakage and denial-of-service attacks.

To prevent this, pick a unique SSID name and confirm that your WLAN has an intrusion detection system (IDS) that scans for SSIDs that impersonate your own. Be sure that the IDS is properly configured and that you have procedures in place to respond to alerts.

Once detected, it is essential to identify, locate and eliminate those threats. Some enterprise WLANs have the built-in intelligence to automatically locate and disable hostile wireless access points (APs).

Another vulnerability often overlooked is having the guest portal's domain name mismatch the SSL certificate associated with the webpage. As a result users may receive certificate error warnings that may heighten their suspicion and does not confirm with security best practices.

THE ENEMY IS CLOSER THAN YOU THINK

It's important to have reasonable safeguards on your guest network to protect others in physical or logical proximity to the user. Consider implementing these procedures to fortify your guest security posture:

- Deploy content filtering to prevent access to inappropriate or offensive web sites in the workplace.
- Integrate your network access management system with next-generation application-aware firewalls from companies like Palo Alto Networks. This provides additional protection against non-http traffic.
- Enforce bandwidth contracts on guest sessions to maintain service-level agreements and quality of service for all.
- Be sure your WLAN prohibits peer-to-peer communication among guest devices to prevent malicious actors from attacking others on the same guest network.

USERS DO UNPREDICTABLE THINGS

Corporate data leakage is a big concern for the enterprise and particularly for BYOD. So make sure your enterprise mobility management (EMM) system keeps IT-managed mobile devices on the corporate network and not the guest network.

Utilizing network access management systems that tightly integrate with EMM for complete device management is important. This enables you to keep IT-managed or personally-owned devices from monopolizing your guest network.

MANAGING LONG-TERM CONTRACTORS AND VISITORS

802.1X authentication paired with WPA2 security is the gold standard for securing enterprise wireless traffic. 802.1X networks ensure that packets are protected from outside threats and close security gaps that open-networks exposed.

Segment your guest demographic and strike a balance between security and the user experience. Contractors and other long-term visitors should use 802.1X-based WPA2 for secure WLAN access. New onboarding technologies make it simple and automate the provisioning of identity certificates and network settings for wireless endpoints.

With a minimal amount of setup, long-term visitors can easily onboard their own devices and get a secure Wi-Fi connection without logging in every day. And in the process, you have stronger security by reducing the guest network's attack surface.

SUMMARY

Take control of guest access before employees, students or visitors do it themselves. Leverage next-generation guest access technology to classify, segregate and log visitor traffic. With the right tools and design, a guest experience can be both secure and easy to use.

So put your organization's best foot forward without taxing your IT resources. And while you're at it, make your #GenMobile guest experience a memorable one.

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