Wireless Network Security

Integrated Security for Wireless Guest Access
Session Topics

• Wireless User Classification
• Security Mechanisms for Internal/Employee Wireless Networks
• Secure Wireless Guest Access – Balancing Security and Access for Guests
• Expanded Security Solutions using Sponsored Guest Access
• Integrating Guest Access Security with Perimeter Firewalls
Wireless User Classification

• Internal User Classifications vary by Organization & Market Segment
  • For the most part, easy to identify and differentiate, based on roles within organization, security other internally defined classifications
    • Employee Classifications – Management, Finance, Employee
    • University/School Classifications – Students, Professors, Administrators, etc.
  • Varying levels of system access primarily differentiates internal user classifications
    • Access Restrictions based on destinations and applications with no time component
    • Guest User Classifications are much more varied within each market segment
Guest User Classification

• What is a Guest?
  • Temporary Visitor
  • Contractor/Auditor
    • Temporary, Semi-Permanent, Periodic Visitor
  • Hospital Patient/Visitor
  • Hotel Guest/Conference Attendee
  • Corporate Client
Guest User Classification

- Guest Users require both access and time restrictions.
- Minimized Authentication Requirements so as to reduce barriers to join the network.
  - Often customers implement guest networks with no security so that client visitors can get access without any “complications”.
  - Law of Unintended Consequences – wireless access provided to all with minimal to no restriction on who can access Internet resources.
  - Often little to no restrictions on external access
Internal User Security Mechanisms
Internal User Security Mechanisms

• Corporate Security Policy typically defines user classifications and levels of access restrictions to be implemented for each user classification.

• Internal User Security Mechanisms typically incorporate both authentication and encryption for wireless access.
  • WPA2/Personal utilizing a pre-shared key/passphrase.
  • WPA2/Enterprise utilizing 802.1x
    • Machine and/or User Authentication via centralized directory service (AD/LDAP)
    • Encryption using AES256 mechanisms with certificates to validate and pass encryption keys.
  • WEP is rapidly being removed from any/all internal security implementations.
Internal User Security Mechanisms

• Multi-tiered network designs provide opportunity to implement network security at various tiers of the network.
  • Threat/Vulnerability Detection can be implemented between users and data centers using transparent firewall/traffic monitoring/out-of-band mirroring solutions.
  • Integrated Netflow/Sflow can also provide monitoring, although these often become more sampling-based as network speeds increase.

• Active Directory Group Policy provides opportunity to implement user or group-based security.

• Perimeter firewalls/security platforms can augment security with threat/vulnerability detection, URL filtering, anti-virus and spyware monitoring, etc.
Guest Wireless Security Mechanisms
Guest Wireless Security Mechanisms

- Simplified mechanisms available in many personal and enterprise wireless access points.
  - Network Address Translation
    - Guest DHCP services provided by the wireless access points.
    - All Guest packets are source-translated and appear to be sourced from the access point’s IP address on the corporate network.
    - Authentication and Encryption can be added for enhanced security.
    - Easy-to-implement guest solution that provides only minimal security and can impede attempts to implement security policy for guests using external devices.
  - Captive Portal requiring acknowledgement of Acceptable Use Policy and/or Authentication.
    - Often implemented with common username for all guests.
Guest Wireless Security Mechanisms

- Captive Portal
  - Several different methods to implement.
    - DNS Poisoning – all DNS requests resolve to IP address of captive portal server.
    - Destination NAT – all attempts to access websites are redirected via DNAT to the captive portal server.
  - Internal Captive Portal (onboard controller or access point) services are typically simplified with only minimal customization and few enhancements.
  - External Captive Portal has significant customization options and enhancements but requires external servers, increasing cost and complexity.
Guest Wireless Security Mechanisms

- Once authenticated via either captive portal, MAC address, passphrase, etc., users are generally connected to a separate layer-2 VLAN with a firewall interface configured as the default gateway.

- This is somewhat problematic in large, multi-tiered networks, requiring L2 VLAN extension through multiple tiers of the network design.
  
  - Other options such as policy-based routing, multiple VRF implementations, can be used but not always easy to implement with differing network components at various tiers of the network.
Guest Wireless Overlay on Network Infrastructure

Focus on Security

John Sayer (jsayer@asktech.com)

November 2, 2016
Guest Wireless Security Mechanisms

• However, this only provides one aspect of security needed to truly provide secure guest wireless access in today’s environment.
  • Does not address potential for guests to monopolize wireless access points, impacting internal user wireless access.
  • Does not address potential impacts of guest unethical or criminal behavior while using largely open wireless network.
  • Does not inherently put any time constraints on guest user’s access to the network.
    • In the case of a pre-shared key, likely that the passphrase will be known by many in addition to known guests and unlikely that it will be changed often enough to provide secure access.
Growth Expectations for Wireless Overall

Devices

Apps

Traffic

4X

10X

100X

Focus on Security

John Sayer (jsayer@asktech.com)

November 2, 2016
Wireless Networks Bandwidth Growth

**CY 2013/2014: Draft 802.11ac**

- Max data rate 1.3Gbps - 4x performance compared to 2x2 802.11n
- 5GHz only
- Up to 3 spatial streams, up to 80MHz wide channels – reduced number of overall channels in 5GHz
- Client devices start shipping mid-2013; Mass adoption early-2014

**CY 2014/2015: IEEE ratified 802.11ac**

- Max data rate of 6.93Gbps - 50% better range compared to 2x2 802.11n
- Up to 8 spatial streams, up to 160MHz wide channels – even fewer 5GHz channels
- **Multi-User MIMO** - Increased Capacity with simultaneous transmit to multiple receivers
- Mass adoption mid-2015
Guest Access Issues & Concerns

- Guest Wireless Users are not typically controlled in any way.
- Internal Users may bypass corporate security by connecting to “open access” guest network.
- Guest Wireless networks typically utilize the same network infrastructure as internal/employee wired and wireless users.
- Increase in available bandwidth for wireless users can cause bandwidth usage issues on both the wireless and wired networks.
- Open guest networks can lead to unintended guests watching Italian League soccer all afternoon using critical corporate resources.
Guest Access Security Policy Components

- Per-User Bandwidth Restrictions
- Time-Limited Network Access
- Usage Monitoring
- Threat Detection
- Guest Device Posture Assessment
- URL Filtering
Enhancements to Guest Security

• Self-Registration
• Sponsored Self-Registration
• Differentiated Classes of Guest Users
• Bandwidth Controls per-User or per-Class of Guest User
• Application Identification and Policy
• Integration with Firewall to provide differentiated Access

Focus on Security

John Sayer (jsayer@asktech.com)

November 2, 2016
Enhancements to Wireless Guest Security

Focus on Security

John Sayer (jsayer@asktech.com)

November 2, 2016
Sponsored Guest Self-Registration

1. Collect visitor information
2. Sponsor prompted to confirm that guest is valid
3. Account enabled, visitor notified via screen, SMS, or email
Integration of Services in Aruba ClearPass

Focus on Security

John Sayer (jsayer@asktech.com)
Integrating Guest Wireless with Perimeter Firewalls

- Guest Wireless VLAN is typically connected directly to a separate firewall interface to keep traffic completely off of internal IP network.
- Newer firewalls can then implement URL Filtering, Anti-Spyware and Anti-Virus checking, and Threat Prevention.
- Further inclusion of wireless guest user names, provided via API into Palo Alto firewalls, allows for monitoring, isolation of individual users, and identification in the event of unethical or criminal activity.
Guest Wireless Firewall Integration

• Utilizing Network Address Translation, a unique public IP address should be used for guest wireless users, distinct from internal users.

• Implement separate security policies for wireless guest users, which may include time-of-day and/or QoS/bandwidth restrictions.

• Monitor firewall bandwidth and application usage for guest wireless users.

• Implement URL filtering at firewall with separate policies for each type of guest wireless user.
Conclusions
Guest Wireless Security Conclusions

• Differentiated Classes of Guest Users may require unique user roles or even unique SSID’s within corporate wireless infrastructure.

• Traditional Open-Access Guest Wireless leaves organizations open to many types of concerns, including reduced usability for internal users, both wired and wireless.

• Integration with external services that can provide additional, enhanced visibility and control of guest wireless access can greatly reduce the exposure.

• Many of these steps can be implemented with existing corporate-grade wireless access points and controllers.
Questions?