Securing Wireless Communications

A Layered Approach

Jeremy Bennett
Security Architect
jbennett@arubanetworks.com

Agenda

Layer 0	• Why?
Layer 1	• Environment
Layer 2	• Data
Layer 3	• Network
Layer 4	• Management
Layer 5	• Audit and Report

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 0 – Why Security Matters

Security ICU

- Integrity
- Confidentiality
- Utility

Risks

- Rogue APs
- Data loss
- Brand exposure

Rewards

- Flexibility
- Cost Savings
- Enabler

Regulation

- PCI
- Financial
- Government

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

A Word About PCI DSS

Who is PCI

- A worldwide consortium
- Started by major card brands
- Includes card issuers and banks
- Includes merchants
- Includes technology providers

What is PCI

- A digital security standard
- Covers all aspects of IT from systems to storage to networks
- Designed to protect debit and credit card data
- **Mandatory for all merchants worldwide**

Why Comply?

- Protect the brand
- Avoid $160/card breach penalty under safe harbor
- Prevent $10,000 - $100,000 a month out-of-compliance fine
- Lower per transaction rates, only available with PCI compliance

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

PCI DSS Wireless Guidelines

- Authored by the Wireless Special Interest Group
  - A group of PCI members interested in wireless
  - Many wireless experts
- NOT a new set of requirements
- Provides concrete guidance on how PCI DSS requirements impact wireless networks
  - Whether you have wireless or not
  - Whether you use wireless for cardholder data or not
- Reviewed and approved by the PCI council

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 1 – Environment

- Physical and RF space
- Threats
  - Man in the Middle – device inserted between AP and port
  - Rogue – device inserted into unused port
  - Jamming & Interference
  - Tampering with or stealing APs
- Regulation
  - PCI DSS 11.1 – Wireless scanning
  - PCI DSS 9.1, 9.2 – Secure ports and APs

Layer 1 - Secure the Environment

Physically secure devices

- Restrict access to network ports
- Lock down connected devices or ensure they contain no sensitive data
- Prevent tampering with devices
- Ensure wireless network is resistant to jamming and noise

Allow only authorized devices

- Know what’s on your network: Wired or Wireless
- Wireless devices extend the network in an uncontrolled manner
- Multiple techniques and multiple vectors ensures better discovery and better classification
- PCI requires at least quarterly scans for wireless devices

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 1 – Using Aruba

Physically Secure Devices

- Centralized architecture means no sensitive data is exposed if an AP is lost
- Integrated TPMs mean APs cannot be spoofed our swapped out with altered devices
- Wired & wireless authentication
- Centralized management means alerts can be generated if an AP is lost or disconnected
- Spectrum monitoring and Adaptive Radio Management (ARM) ensure consistent operation

Allow Only Authorized Devices

- Aruba AirMonitors scan the RF space and correlate wireless and wired traffic to accurately categorize rogues
- AirWave RAPIDS proactively scans the wired network through switches, routers, and direct probes to find all suspicious devices.
- Multiple techniques and multiple vectors ensures better discovery and better classification
- Wired & wireless containment reduces the threat of rogues

Layer 2 – Data

- Not just bytes but also the ability to trust them
- Threats
  - Eavesdropping
  - Data forging
  - Floods & DoS
  - 802.11 protocol attacks
- Regulation
  - PCI DSS 7.1, 7.1.2 – Access on need to know
  - PCI DSS 7.2, 8.1 – Individual user accounts
  - PCI DSS 4.1, 4.1.1 – Use strong encryption

Layer 2 - Protect the Data

Secure the protocol

- Avoid floods and DoS attacks
- Use wireless IDS to monitor all network traffic

Authenticate

- Know your wireless clients
- Prevent bogus clients from getting online
- Devices should be unusable for business without a valid user
- Use 802.1x where possible

Encrypt

- WPA2 WLANs are securely authenticated and encrypted.
- Open wireless + VPN = Window of client exposure
- Make sure the link between the AP and controller is secure

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 2 – Aruba Secures 802.11

- Every frame received by the AP is processed by the IDS
  - Dedicated AMs receive a few frames on every channel
  - In AP mode all valid traffic is processed by the IDS, nothing is lost.
- All devices are tracked
  - Client and AP associations are tracked and stored.
  - All ad hoc networks are also tracked and stored
- Each frame is checked for known attacks
  - Checked for syntactic correctness – is the frame OK?
  - Checked for semantic correctness – does the frame make sense in context?
- Any problems are sent to the controller for correlation and disposition
  - Repeat alerts are suppressed as per policy
  - Traps and logs are generated for external systems like AirWave

© 2010 All Rights Reserved.

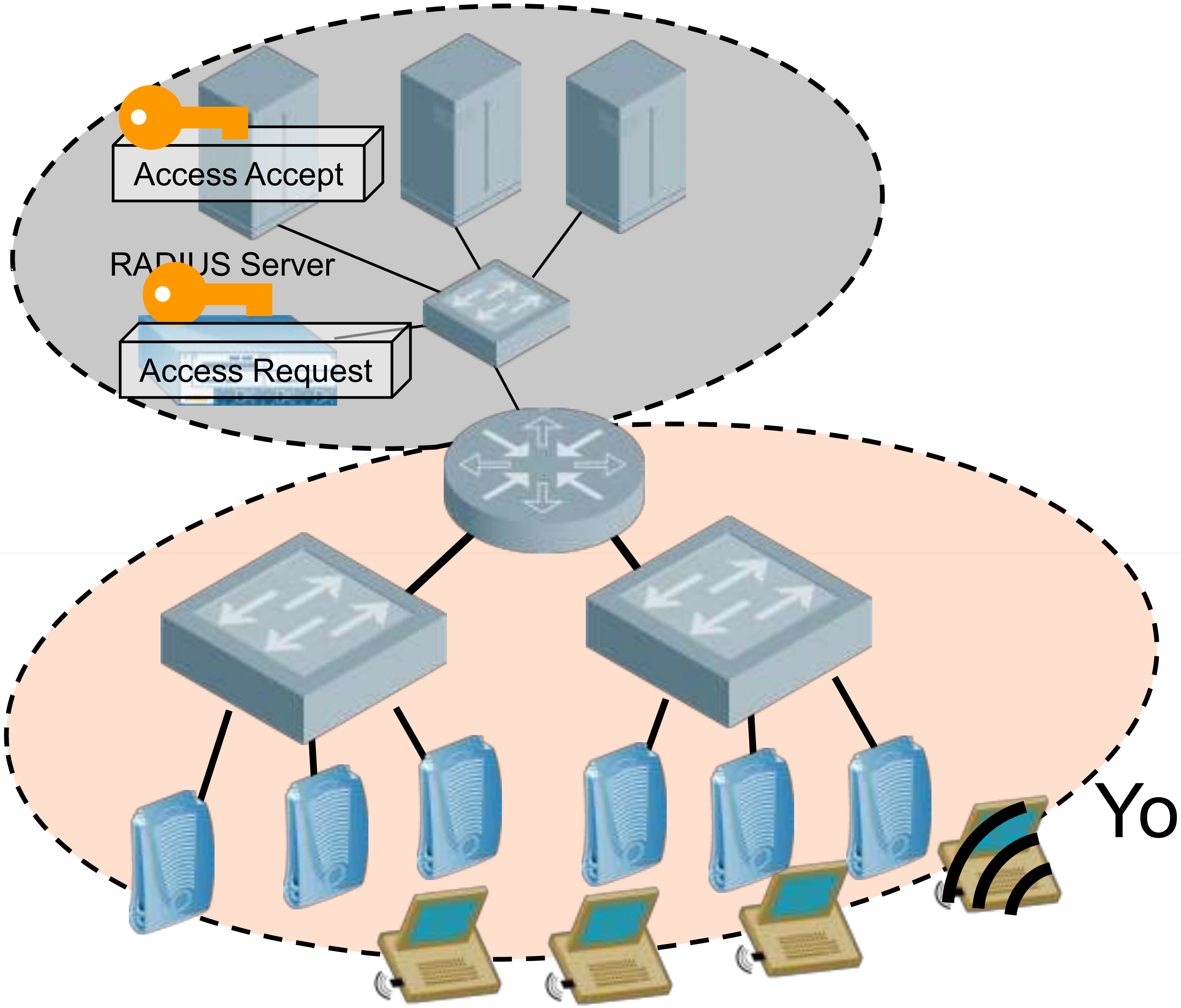
Layer 2 - Authenticate

- Authenticate devices
  - Aruba enforces machine authentication before user authentication
  - Prevent non-corporate devices from accessing the network
  - Use a dynamic firewall like Aruba PEF to put authenticated devices outside the CDE until a user logs in
- Authenticate users
  - Recommend using a centralized directory for accounts
  - PCI DSS requires processes for disabling and terminating access.

Layer 2 – Encrypt

- ALL wireless traffic
  - Use WPA2 Enterprise with AES where possible
  - If Enterprise is not feasible use PSK
- Across unsecured wired links
  - Centralized encryption allows APs to be deployed in insecure areas
  - Remote AP automatically creates IPSec tunnels back to controller even over the Internet

Layer 2 - Centralized Encryption



- Client finishes authentication and the AP sends the wireless packet to the controller
- The controller sends an access request to the RADIUS server
- The RADIUS server sends the accept and encrypted keys to the controller
- All encryption is processed centrally

NO keys are distributed to APs

Your Keys Never Leave Data Center

Layer 3 – Network

- Classic TCP/IP network (OSI 5-7)
- Threats
  - Misbehaving users
  - Unauthorized applications
  - Bandwidth hogs
  - Guests & Partners
- Regulation
  - PCI DSS section 1 – use firewalls
  - PCI DSS 4.1 requires strong network encryption
  - PCI DSS section 7 – use strong access control

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 3 – Secure the Network

- Segment the network
  - Use physical or virtual techniques to break the network into manageable pieces
  - Segment based on business need. Example PCI DSS allows the ‘cardholder data environment’ to be contained in a segment thus simplifying compliance
- Segment and control applications
  - Use roles to grant access to secure applications
  - Use QoS rules to enable streaming and prevent saturation
  - Allow guests and partners minimal access or external-only access

Layer 3 - Physical Segmentation

No shared wires – **VLANs are not sufficient**

- VLAN tagging does not prevent a tap from capturing data
- VLAN tags can be spoofed
- If CDE traffic must cross untrusted segments make it strongly encrypted

No shared switches or routers

- Unless they have a built-in firewall
- Overloaded switches can be fooled into mishandling traffic
- Routing protocols can be spoofed

No shared APs

- Unless they have a built-in firewall
- Make sure CDE SSID and non-CDE SSID traffic remains separated physically or by a firewall at all times

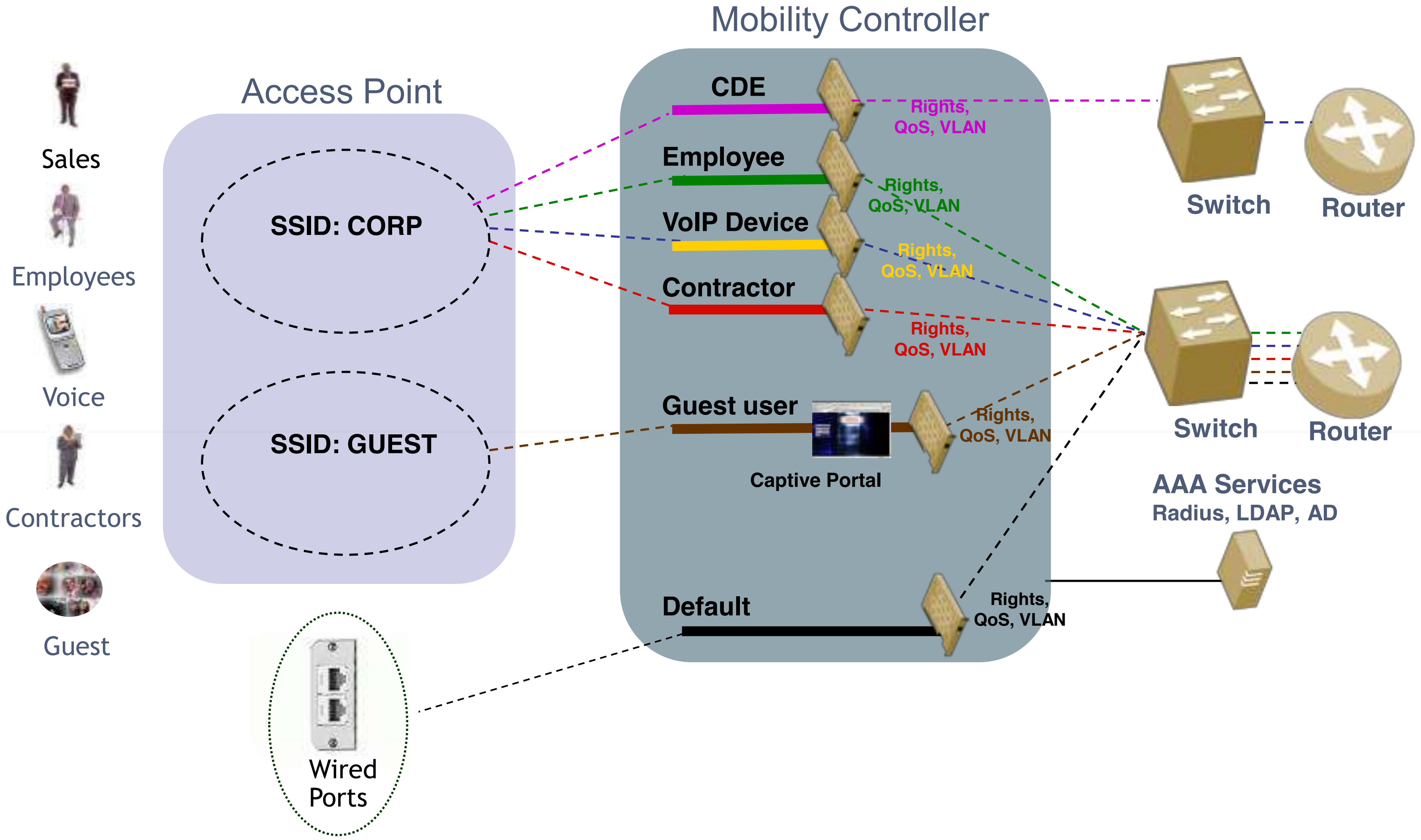
Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Policy Enforcement Firewall (PEF)

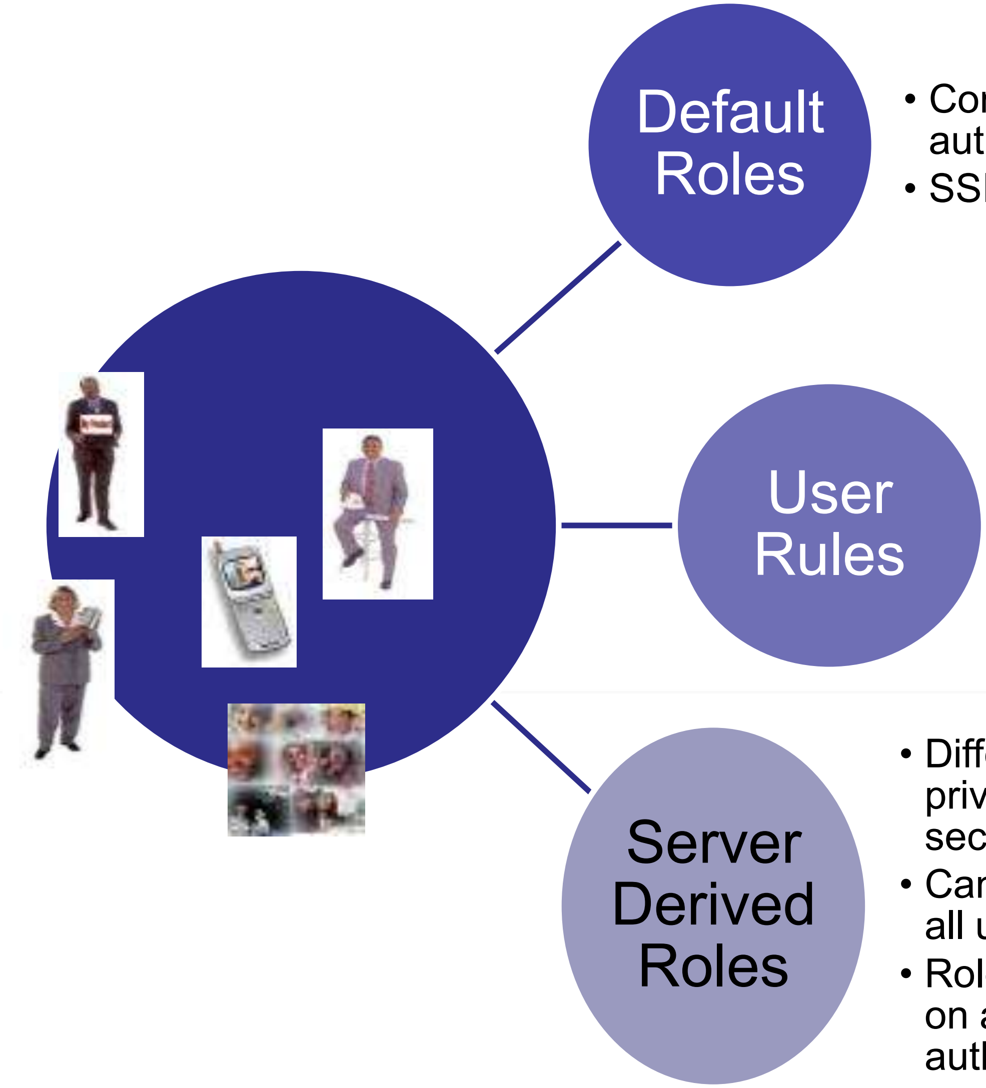
- Corner stone of Aruba Security Architecture
- Role-based
  - Derived from client or server attributes or upon successful authentication
  - Integrated architecture ensures no spoofing
  - Every untrusted IP or MAC is assigned a role
  - Layered: Layer 3 role overrides Layer 2 role
- Session ACLs define policy
  - Applied to all IP traffic (i.e. TCP and UDP)
  - From untrusted and to untrusted users
  - Rules allow, deny, or limit bandwidth
- Application Level Gateways allow complex protocols through simple rules
  - FTP active and passive
  - VoIP – SIP, RTP, etc

Role-Based Separation

Multiple Classes of Users on Same Infrastructure are Kept Separate



Role Derivation



Default Roles

- Configurable by authentication method
- SSID

User Rules

- Device-specific attributes
- Encryption type
- AP used (by name or BSSID)

Server Derived Roles

- Different access privileges based on security policy
- Can use single SSID for all users/devices
- Role assignment based on attributes from authentication server

Firewall Processing

- Session processing
  - Identity-based firewall policies
  - Traffic management
- Protocol processing
- Traffic cleanup
  - Detects SYN, ping, ports scan attacks
  - Can prevent continued attacks (black list station)
  - Enforces TCP handshakes, prevents replay attacks
- Station blacklisting
  - Authentication failure
  - Firewall rule violation
  - TCP attacks

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 4 – Management

- People and process for controlling configuration and operation of the network
- Threats
  - Ignored rogues
  - Accidental configuration errors
  - Disgruntled ex-employees
  - Stolen laptops
- Regulation
  - PCI DSS section 10 requires network and security monitoring
  - PCI DSS section 12 requires documenting and following security processes

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 4 – Management

Monitor and Repair

- Mitigate rogues using automated methods
- Physically remove rogues
- Repair configuration problems
- Remove user access on termination
- Remove device access when devices are lost/stolen
- Review firewall hits and address problems

Maintain Compliance

- Regularly check configuration of all equipment
- Regularly review firewall configurations
- Regularly confirm authorized users and devices

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Layer 4 – Secure Management

Monitor and Repair

- Wired and wireless containment minimizes the threat of rogue APs
- AirWave reports, location, switch, and port of discovered rogues
- Send alerts for configuration problems

Maintain Compliance

- Automatic configuration can repair mistakes
- Full log of all configuration changes is kept to prove continuous compliance.
- Alerts can be sent if compliance conditions are violated

AIRHEADS

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

ARUBA networks

Multiple Rogue Containment Methods

- Deauth
  - Less impact on the client device
  - Best for steering authorized clients away from problem APs
- Tarpit*
  - Less RF traffic than deauth and more effective
  - Best for preventing any access to rogue APs
  - May confuse client users and client software
- Wired Containment
  - Poison ARP from AP
  - Shutdown Wired Port with AirWave RAPIDs module

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

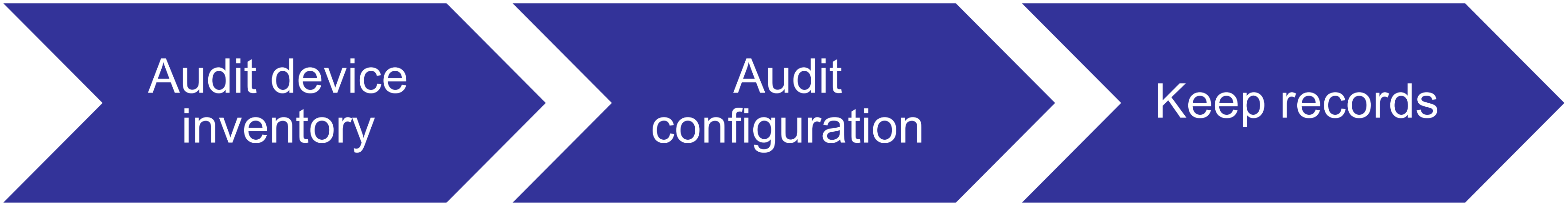
Compliance Maintenance Plan

Review Period	Item
Every 90 days (A)	Remove unused accounts (8.5.5)
	Change passwords (8.5.9)
	Wireless scan (11.1)
	Vulnerability scan (internal and external) (11.2)
Every 6 months (B)	All in A
	Firewall and router configs (1.1.6)
Every year (C)	All in A + B
	Pen test (11.3)
	Security policy (12.1.3)
	Test Incident Response Plan
	Rotate crypto keys (3.6.4) (or as recommended by vendor)

Layer 5 – Audit and Report

- Regular reviews of activity, process, and people
- Threats
  - Miscommunication
  - Disgruntled administrator
  - Business and regulation changes
- Regulation
  - PCI DSS requirements for process also require its review (e.g. 12.1.3)
  - PCI DSS is updated every two years

Layer 5 - Audit and Report



Audit device inventory

- AirWave automatically tracks all devices
- Device classification can be based on a combination of rules
- Authorized devices are managed to ensure compliance

Audit configuration

- AirWave’s interactive PCI report highlights potential problems
- Report can be scheduled or run on demand

Keep records

- AirWave can keep records for more than a year
- Many PCI reports can be kept for comparison
- All changes and administrator actions are logged and audited.

Aruba Networks CONFIDENTIAL. © 2010 All Rights Reserved.

Demo Flow

- Rogues
  - Classification
  - Discovery and resolution workflow
- Alerting
  - Configuration
  - Alert resolution workflow
- Reporting
  - Creating reports
  - Scheduling reports
  - Key security reports