AIRHEADS
LAS VEGAS 2012

JOIN: community.arubanetworks.com
FOLLOW: @arubanetworks
DISCUSS: #airheadsconf
DEPLOYING BYOD: ONBOARDING, PROVISIONING, POLICY, REPORTING
The BYOD Challenges

Requirement: Securely Onboard Mobile Devices

Corporate Liable
- Trusted
  - Company-owned
  - Fully managed
  - Fully controlled

Employee Liable
- Tolerated
  - Company or Employee owned
  - Limited visibility
  - Limited control

How do I:
- Maintain visibility & control?
- Deliver secure, differentiated access?
- Simplify device provisioning?
ClearPass Enables Secure Network Access for Mobile Devices

1. Onboard Device
2. Join BYOD Domain
3. Device Access Controls
4. Visibility & Reporting
Join the BYOD Domain

1. Onboard Device
   - Suppliant Config
   - Push Trusted Cert
   - Enable Posture
   - Set Auth type

2. Join BYOD Domain
   - Enrolment workflow
   - Authorize User to provision device
   - Device credential push
   - Link User to Device

3. Device Access Controls
   - Revoke Device Access
   - Device Profiling
   - Role Derivation
   - Corp vs Employee Liable

4. Visibility & Reporting
   - Complete view device & network
   - Command & Control
   - Inventory
   - Diagnostics
BYOD Building Blocks
Foundation Technologies for BYOD

- **Device Profiling**
  - Accurately determine device, force enrollment or deny access

- **Enrollment and Provisioning Workflow**
  - Clean user self managed onboarding process, no IT involvement

- **Context Aware Policy Enforcement**
  - Implement business policy for BYOD access, multi-contextual

- **BYOD lifecycle management**
  - Device inventory, revoke network access, more to come . . .
5-Tier Device Profiling

- Baseline Fingerprinting
- Network Protocol Correlation
- Device Access Heuristics
- Identity & Messaging
- Client Inspection

Model: Galaxy Tab T849
Enrollment & Provisioning Workflow

1. Authorize BYOD enrollment based on AD credentials
2. Register device type & ownership
3. Provision a unique device credential for that user & device
4. Revoke access for devices that are lost or stolen
Context Aware Policy Definition Point

- Employees
- Contractors
- Guests
- Students
- Faculty

- Personal
- Corporate
- Device Type
- Health

- USER
- DEVICE
- LOCATION
- APPLICATION

- WiFi
- Media
- Time of day
- HQ
- Branch
- Home
- Remote
- VPN
- 3G
- Cloud
- Virtual Desktop
- Data Video Voice
Granular Policy Enforcement at the Access Layer

Policy Enforcement Firewall (PEF)

- Identify the Connection
- Classify the Traffic
- Control Access per Packet
- Optimize the Air
- Follow the User

Instant AP
Mobility Access Switch
Mobility Controller
BYOD lifecycle management

- Revoke Device Network Access
- Realtime Dashboard of BYOD Access
- Device Inventory Data
- Enforcement of BYOD Access Policies
BYOD Examples
BYOD Policy Examples

1. Executive BYOD iPad
   - Unique Device Credential 802.1x authentication → BYOD Exec

2. Employee BYOD Windows Laptop
   - Unique Device Credential 802.1x authentication → BYOD LAZ

3. Executive BYOD MacBook
   - Unique Device Credential 802.1x authentication → BYOD Exec

4. Employee BYOD Android Tablet
   - Unique Device Credential 802.1x authentication → BYOD LAZ
Example BYOD Policy Enforcement

Identity Stores

Active Directory

Executives

Employee1 - Employee5

Employees

Employee6 - Employee15

Policy Definition Point (PDP)

Onramps

Enforcement

Aruba Wireless Controller

S-3500 Switch

RAP or VIA

Cisco Switch

Employee Role
- Unrestricted

BYOD-Exec Role
- Unlimited Bandwidth
- Intranet Sites
- Payroll Server

BYOD-LAZ Role
- Bandwidth = 1 Mbps
- Intranet sites

Guest Role
- Internet only

VLAN 681
- Access based on FW
1. Executive BYOD iPad

1. iPad connected to PoC-Employee using cached credentials
2. BYOD device detected & iPad forced to device provisioning page
3. Executive authorizes with domain credentials & unique device credentials & supplicant configuration pushed to the iPad
4. iPad disconnected & re-authenticates with new provisioned credentials

Expected Result: BYOD Exec → Exec Access Zone + unrestricted bandwidth

2. Employee BYOD Windows Laptop

1. Laptop connected to PoC - Employee using cached credentials
2. BYOD device detected & Laptop forced to device provisioning page
3. Employee authorizes with domain credentials & unique device credentials & supplicant configuration pushed to the Laptop
4. Laptop disconnected & re-authenticates with new provisioned credentials

Expected Result: BYOD LAZ → Limited Access Zone + 512K bandwidth

3. Executive BYOD MacBook

1. MacBook connected to PoC-Employee using cached credentials
2. BYOD device detected & MacBook forced to device provisioning page
3. Executive authorizes with domain credentials & unique device credentials & supplicant configuration pushed to the MacBook
4. MacBook disconnected & re-authenticates with new provisioned credentials

Expected Result: BYOD Exec → Exec Access Zone + unrestricted bandwidth

4. Employee BYOD Android Tablet

1. Android connected to PoC-Employee using cached credentials
2. BYOD device detected & Android forced to device provisioning page
3. Android App downloaded. Executive authorizes with domain credentials & unique device credentials & supplicant configuration pushed to the Android
4. Android disconnected & re-authenticates with new provisioned credentials

**Expected Result:** BYOD LAZ → Limited Access Zone + 512K bandwidth

Summary: 5 Tips for BYOD

• Define your BYOD Access Policy
  – Limited Access Zone, Which devices, Bandwidth Contracts

• Device Aware Access Network
  – Device Profiling, ability to force enrollment workflow

• Granular Policy Definition & Enforcement
  – Centralized policy creation, role based enforcement

• User Managed Onboarding Process
  – Avoid Help Desk load, install trusted certs, profile device details

• Method to Revoke Device Access Critical
  – Unique device credential, lost device or employee leaves
Have fun tonight!!