Chapter 20 Overview

- Mobile Device Management
- Guest WLAN access
- Network access control (NAC)
Mobile Device Management

- Tablets and smartphones provided the true mobility that employees and businesses desire
- The number of mobile devices connecting to corporate WLANs surpassed the number of laptop connections
- A BYOD policy is needed to define how employees’ personal devices may access the corporate WLAN

Mobile Device Management

- An MDM solution can manage devices across multiple mobile operating systems and across multiple mobile service providers.
- Some of the major vendors selling overlay MDM solutions:
  - Airwatch—www.air-watch.com
  - Fiberlink—www.maas360.com
  - JAMF Software—www.jamfsoftware.com
  - Mobile Iron—www.mobileiron.com
Company-Issued Devices vs. Personal Devices

- Management strategy for company mobile devices usually entails more in-depth security because very often the CIDs have company documents and information stored on them.
- Personal mobile devices are much more difficult to manage unless a proper MDM solution has been deployed.
- Every company should have its own unique BYOD containment strategy while still allowing access to the corporate WLAN.

Device restrictions
MDM Architecture

Four main components:
- Mobile Device
- AP/WLAN Controller
- MDM Server
- Push Notification Servers

MDM Enrollment

Step 1: Mobile device connects with the access point.
Step 2: AP checks if the device is enrolled
Step 3: MDM server queries LDAP
MDM Enrollment

• Step 4: Device is redirected to the MDM server

![MDM Enrollment Step 4]

MDM Enrollment

• Step 5: Devices installs certificate and MDM profile

![MDM Enrollment Step 5]
MDM Enrollment

- Step 6: MDM server releases mobile device
- Step 7: Mobile device exits the walled garden

MDM Profiles

- Can include device restrictions, email settings, VPN settings, LDAP directory service settings, and Wi-Fi settings
MDM Agent Software

- Operating systems of some mobile devices require MDM agent application software
- Employee downloads the MDM agent from a public website or company website and installs it on their Android device.
- The MDM agent contacts the MDM server over the WLAN and is typically required to authenticate to the server.

Over-the-Air Management

- MDM server can monitor device information including device name, serial number, capacity, battery life, and the applications that are installed on the device.
- Information that cannot be seen includes SMS messages, personal emails, calendars, and browser history.
Remote actions

- Make changes to the configuration
- Make changes to the device restrictions
- Deliver a message to the device
- Lock the device
- Wipe the device
- Make application management changes
Application Management

• Once an MDM profile is installed, all of the applications installed on the device can be viewed from the MDM server.

Integration with public application stores
Wi-Fi Client Onboarding solutions

• Main purpose is to give the customer an inexpensive and simple way to provision mobile devices onto the secure corporate SSID
• Over-the-air provisioning is used to install Wi-Fi client profiles configured with the corporate SSID security settings

Guest WLAN Access

• Purpose is simply to provide a wireless gateway to the Internet for company visitors and/or customers
• Segmentation approaches:
  – Guest SSID
  – Guest VLAN
  – Guest Firewall Policy
GRE tunneling guest traffic to a DMZ

Guest firewall policy
Application firewall policy

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: YOUTUBE</td>
<td>Deny</td>
</tr>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: PANDORA AUDIO</td>
<td>Deny</td>
</tr>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: PANDORA TV</td>
<td>Deny</td>
</tr>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: GOOGLE VIDEO</td>
<td>Deny</td>
</tr>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: HULU</td>
<td>Deny</td>
</tr>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: ITUNES</td>
<td>Deny</td>
</tr>
<tr>
<td>[any]</td>
<td>[any]</td>
<td>Application Service: NETFLIX VIDEO STREAM</td>
<td>Deny</td>
</tr>
</tbody>
</table>

Captive web portal—DNS redirect

DNS lookup = whois www.sybex.com

Please Login

USER: PASS:

DNS response = www.sybex.com = 1.1.1.1
Captive web portal logon pages

Client Isolation, Rate Limiting, and Web Content Filtering

- Client Isolation - blocks wireless clients from communicating directly with other wireless clients on the same wireless VLAN
- Rate Limiting - can be used to curb traffic at either the SSID level or user level.
- Web Content Filtering - blocks employees from viewing websites based on content categories
Guest Management

Guest credential delivery methods
Guest Self-Registration

- Self-registration logon page runs on an iPad or Android tablet that functions as the kiosk

Employee Sponsorship
Encrypted Guest Access

- Recent trend is to provide encryption and better authentication security for WLAN guest users
- One simple way to provide encryption on a guest SSID is to use a static PSK
- Some WLAN vendors offer cloud-based servers to distribute secure guest credentials in the form of unique dynamic PSKs
- Hotspot 2.0 is a Wi-Fi Alliance technical specification that is supported by the Passpoint certification program
Network Access Control (NAC)

- Provides what is known as posture assessment
- Posture check is performed via
  - persistent agent
  - dissolvable agent
- If a computer is considered unhealthy, the ideal scenario would be for the posture agent to automatically fix or remediate the problem
- NAC uses various monitoring and fingerprinting techniques to identify different devices so that access can be controlled.

OS Fingerprinting

- An use DHCP snooping
- The parameters within DHCP option 55 create a fingerprint that can be used to identify the operating system of the client.
AAA

Authorization is used to process information such as the following:
• User type (admin, help desk, staff)
• Location, connection type (wireless, wired, VPN)
• Time of day
• Device type (smartphone, tablet, computer)
• Operating system
• Posture

RADIUS Change of Authorization

• RADIUS CoA can dynamically change the permissions that the users has on the network.
• Defined by RFC3576 and later updated in RFC5176.
Chapter 20 Summary

- Mobile Device Management
- Guest WLAN access
- Network access control (NAC)