Managing Who's on Your Network

Max Buxton

max@callandy.com

Network Security

- Designing a secure but usable system
- 802.1x authentication standards
- Certificates
- 802.1x for your wifi network
- 802.1x for your wired network

Call Andy!
MACINTOSH CONSULTING

Gauge Your Network

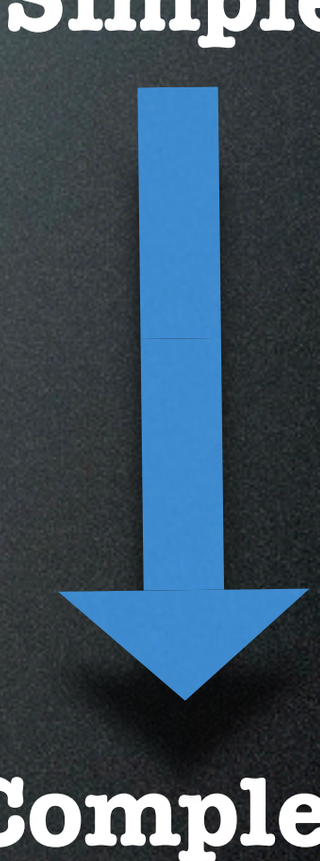
- Size
- Data
- Threats
- Requirements

Call Andy!
MACINTOSH CONSULTING

Size: Campus or Coffee Shop; Laptops vs. iOS
Data: How much data and what types of data?
Threats: Isolated location? City? High value target?
Requirements: HIPPA regulations? Financial? Dept. Of Ed?

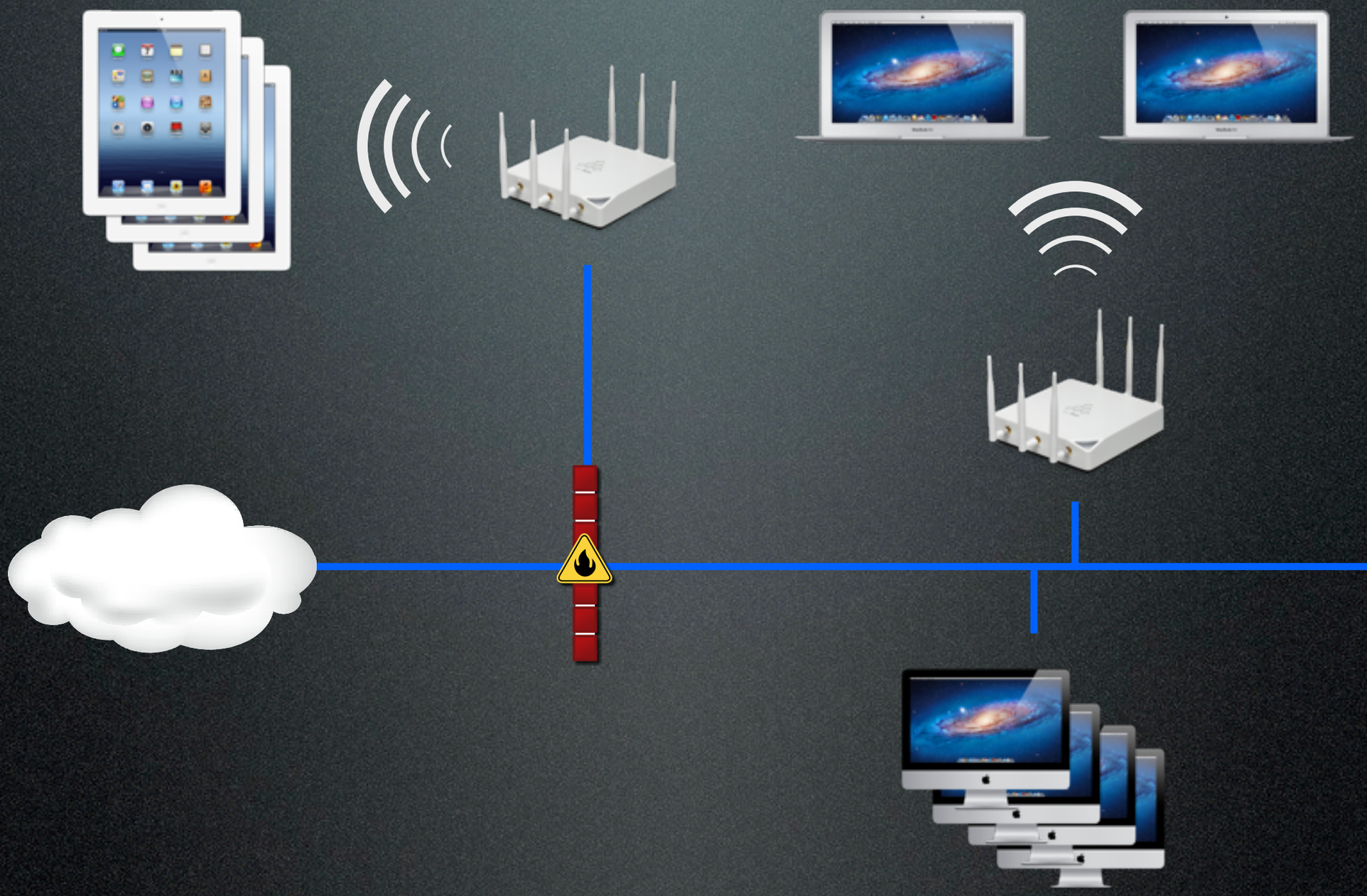
How Much Do You Want to Manage?

- Public
- Private only
- Public and Private
- Segregated
- Nailed shut
- Wireless vs Wired



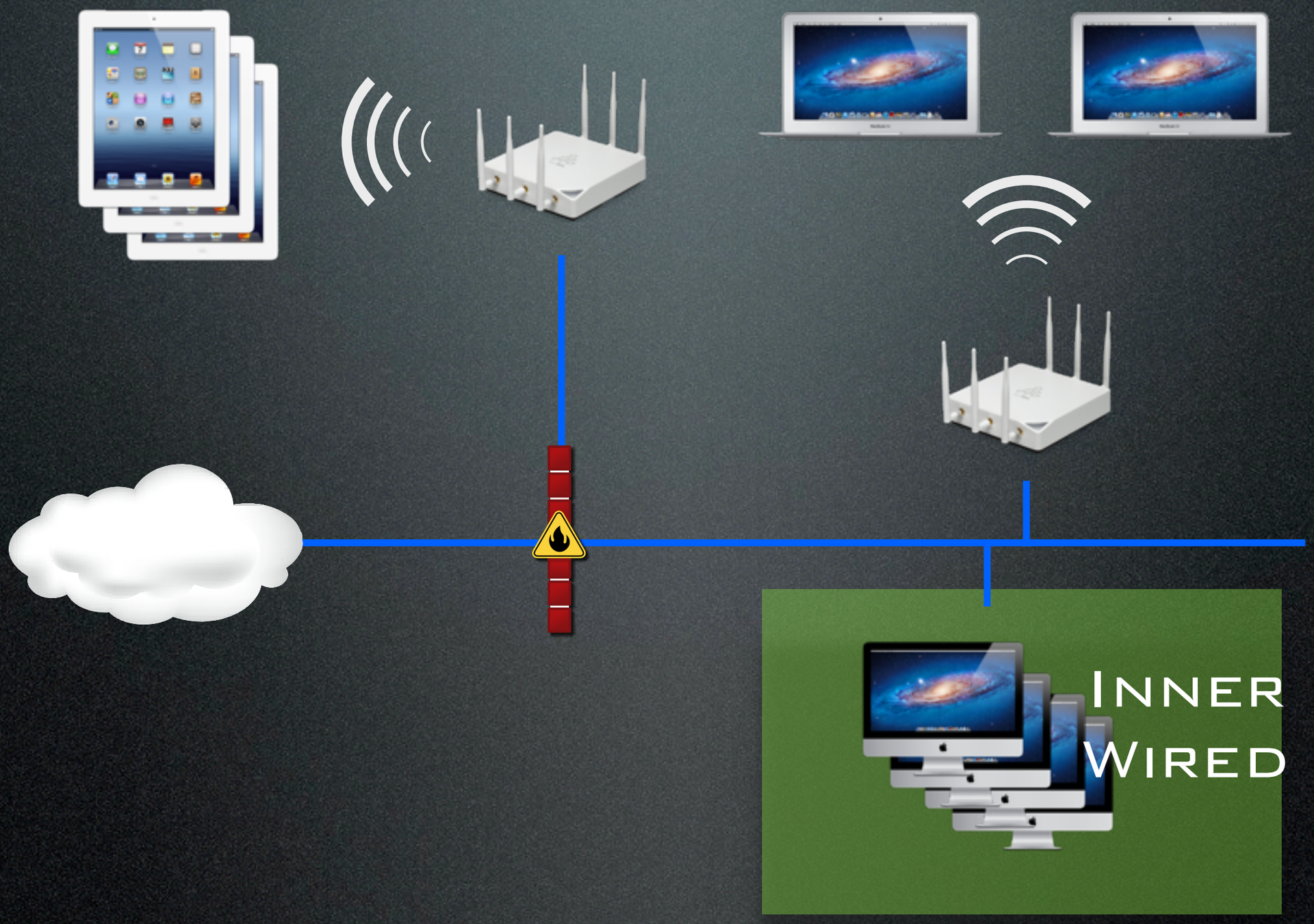
Call Andy!
MACINTOSH CONSULTING

What are the Zones?



Call Andy!
MACINTOSH CONSULTING

What are the Zones?



Call Andy!
MACINTOSH CONSULTING

Inner Wired

- Physical Security

- Don’t be stupid

- Beware of visitors

- 802.1X

Call Andy!
MACINTOSH CONSULTING

What are the Zones?

Call Andy!
MACINTOSH CONSULTING

Inner Wireless

WPA2

WPA2-Personal

EAP

RADIUS

RADIUS

WPA2-PSK

TLS

WPA

802.1X

WPA2-Enterprise

TKIP

LEAP

PEAP

EAP-FAST

TLS

Call Andy!
MACINTOSH CONSULTING

Hidden SSID

- Worthless
- Worse than worthless

Call Andy!
MACINTOSH CONSULTING

Sunday, September 30, 2012

Hiding your ssid is detrimental to those trying to join your network legitmately

Does not help mutual interference by others with APs...

Inner Wireless: Simple

- Small, low risk
- WPA2-PSK
  - Single, fixed password
- Security compromises mean more work

Call Andy!
MACINTOSH CONSULTING

PSK:Pre-Shared Key

Inner Wireless: Complex

- Large, high risk
- WPA2-Enterprise
- 802.1X
- Per-user or per-Device authentication
- Security compromises mitigated

Call Andy!
MACINTOSH CONSULTING

Sunday, September 30, 2012

"WPA Enterprise" is Apple's implementation of RADIUS

RADIUS: Remote Authentication Dial In User Service
Lion in Server Admin
Mountain Lion in Server.app

802.1X Details

- Authentication of network devices
- Prior to Allowing network access
- EAP - Extensible Authentication Protocol
  - Collection of protocols
- Relies on Certificates or RADIUS server for actual authentication

Call Andy!
MACINTOSH CONSULTING

Sunday, September 30, 2012

Authentication: Wired or wireless
Prior to Access: Supplicant – Authenticator – Authentication Server
EAP: Generic authentication framework, many methods
Protocols: Kerberos, public-key encryption, one-time PW
RADIUS: Uses directory services (OD, AD) to validate user account

802.1X Details

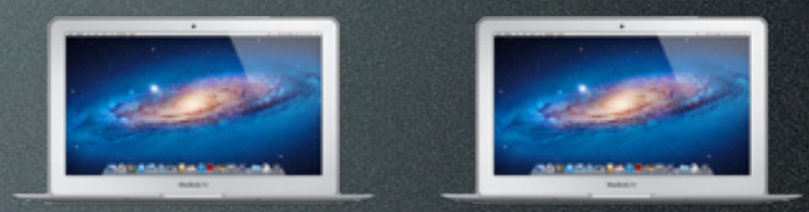
- Configurable only via profiles
- 3 Modes
  - User
  - Device
  - Login Window

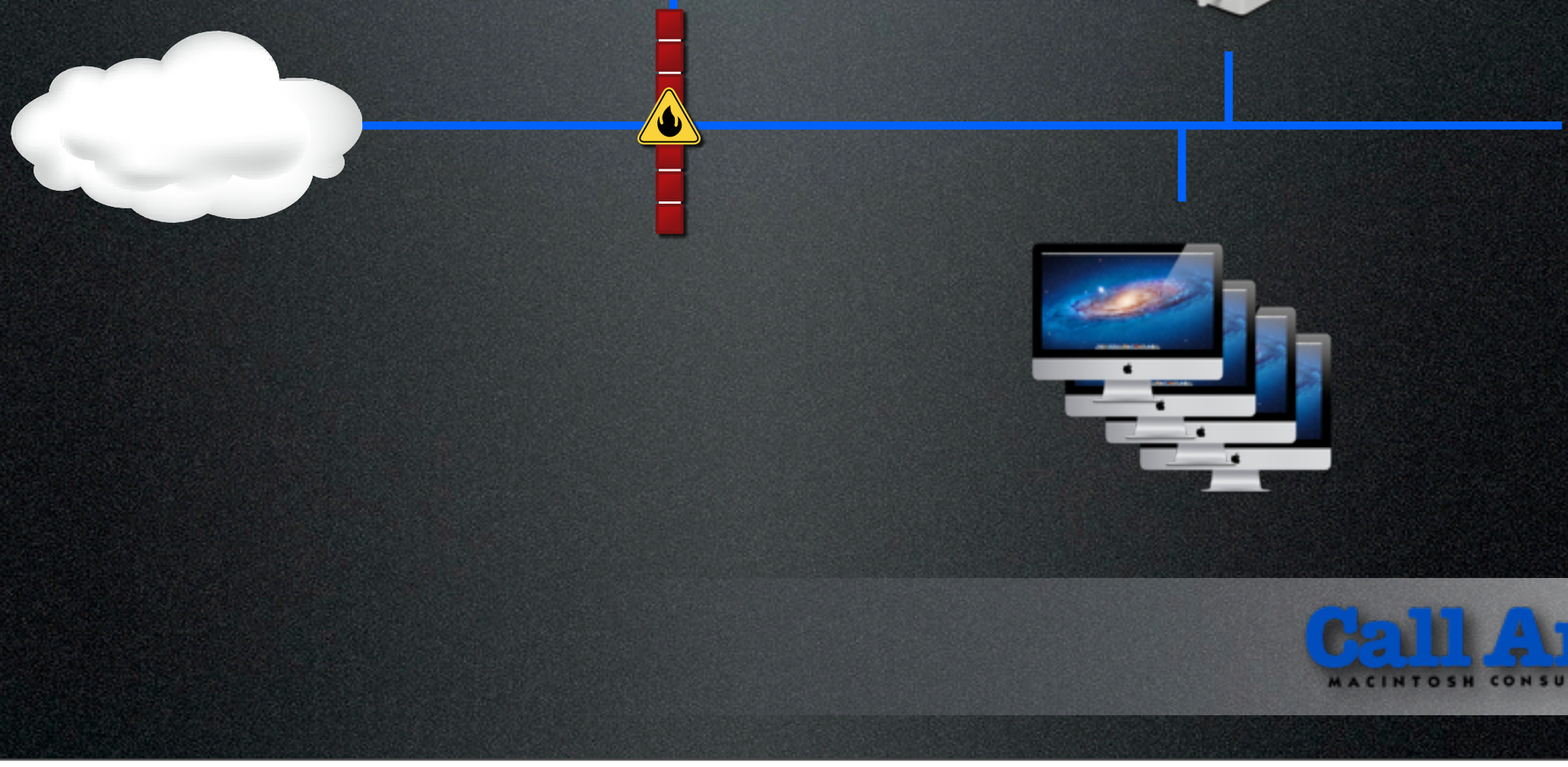
Call Andy! MACINTOSH CONSULTING

Sunday, September 30, 2012

User Mode: most basic; user joins network, authenticates
Device Mode: aka System Mode; computer authentication, even without user logged in
Login Window Mode: 1st make 802.1x connection, 2nd authenticates to directory

What are the Zones?





Call Andy!
MACINTOSH CONSULTING

Outer Wireless

- Different SSID
- Public access
- Untrusted
- Captive portal
- Acceptable use policy
- Bandwidth management

Captive Portal

Call Andy!
MACINTOSH CONSULTING

Bandwidth Management

- Limit usage by any one device
- Monitor and cut off commonly abused protocols — see IDS/IPS
- Wi-Fi is shared bandwidth
- even with different SSID's
- A bandwidth hog on the outer wireless will affect the inner wireless directly

Call Andy!
MACINTOSH CONSULTING

Abused Protocols: Tor, Torrent, Other sharing, Backups (4242), SMTP

IDS/IPS

- Intrusion Detection System
  - Passive, detection only
- Intrusion Prevention System
  - Active, filters connections
- Unified Threat Management

Call Andy!
MACINTOSH CONSULTING

Sunday, September 30, 2012

IDS: produces reports to a Management Station

IPS: Reactive IDS
resetting the connection or by reprogramming the firewall to block network traffic from the suspected malicious source
Different from Firewall: FW looks outside
IPS is another form of an application layer firewall

Unified Threat Management

- Evolution of the Firewall
- Services Include:
  - Gateway AV
  - Anti-spam
  - VPN
  - Content Filtering
  - Load Balancing

Call Andy!
MACINTOSH CONSULTING

Sunday, September 30, 2012

UTM: evolution of the traditional firewall into an all-inclusive security product
Includes: gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing
E.G.: Barracuda, Cisco, Sonicwall, WatchGuard

Unified Threat Management

Call Andy!
MACINTOSH CONSULTING

Sunday, September 30, 2012

UTM: evolution of the traditional firewall into an all-inclusive security product
Includes: gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing

Q & A

Max Buxton

max@callandy.com

Demo
802.1X Profile Creation

Call Andy!
MACINTOSH CONSULTING