

Managing Who's on Your Network

Mark Jeffries
mark@favarger.net



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

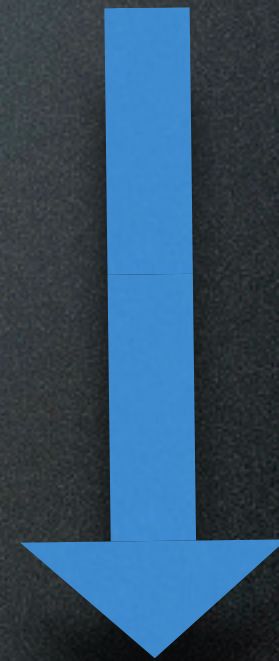
Gauge Your Network

- Size
- Data
- Threats
- Requirements

How Much Do You Want to Manage?

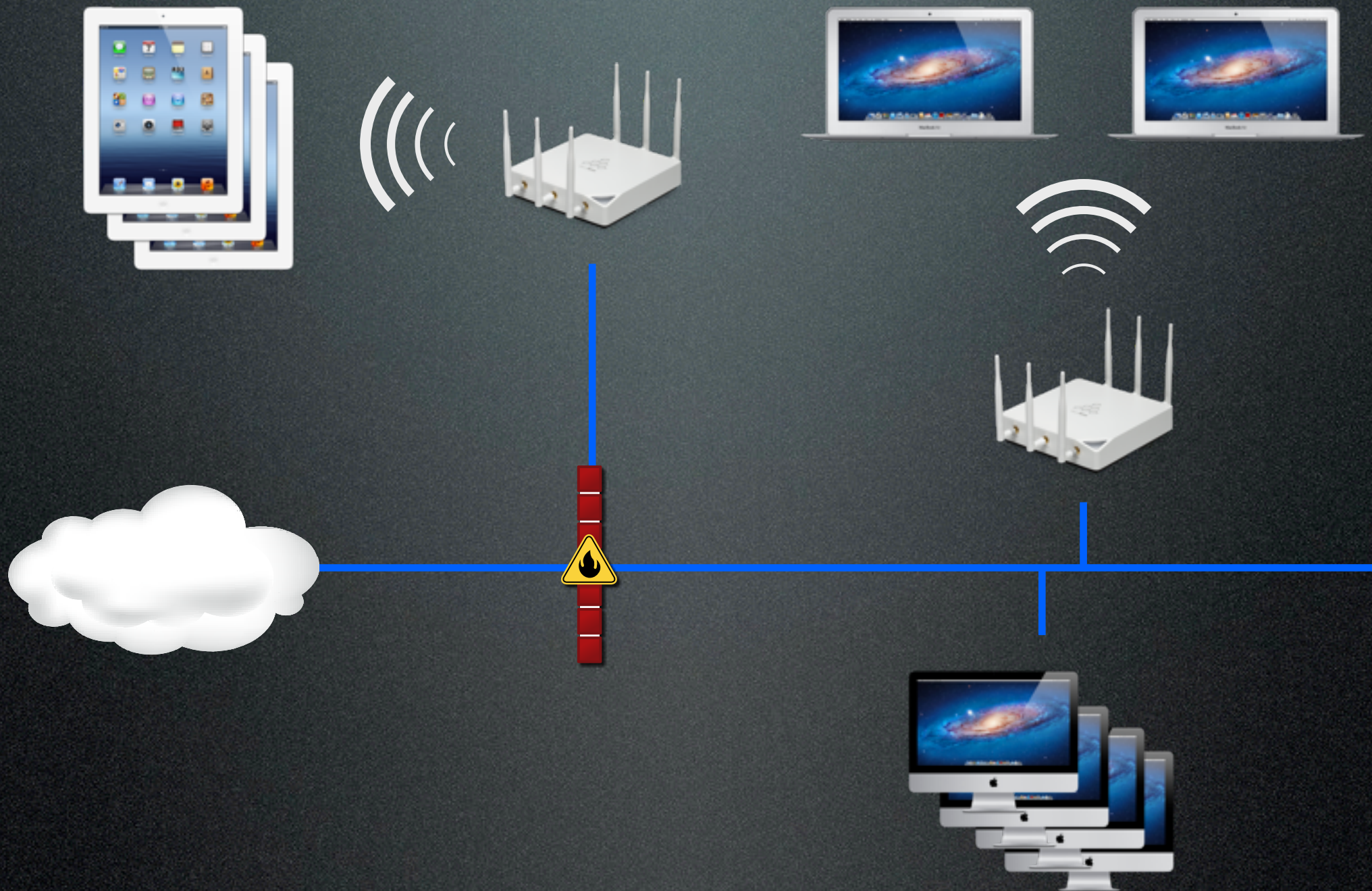
- Public
- Private only
- Public and Private
- Segregated
- Nailed shut
- Wireless vs Wired

Simple

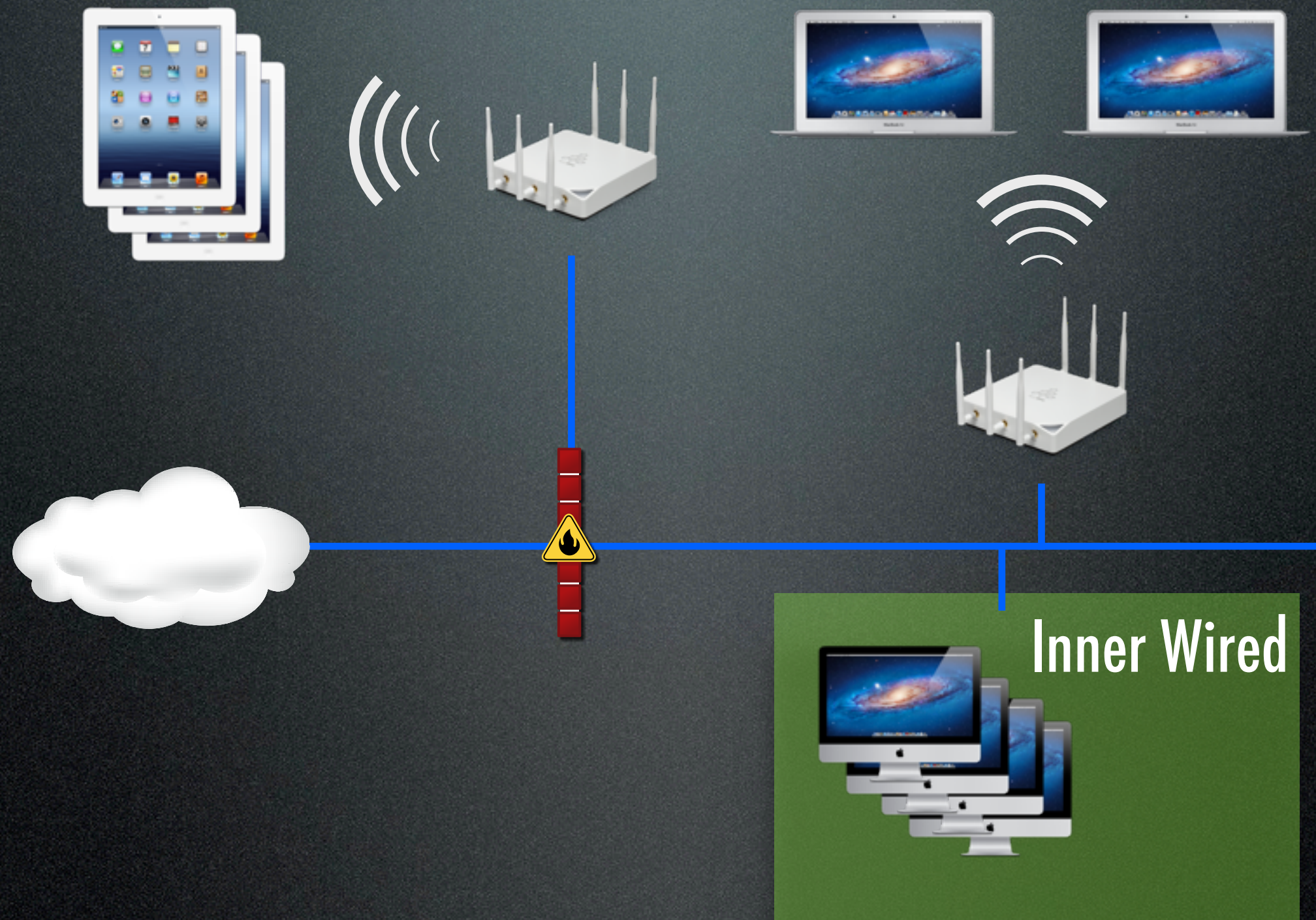


Complex

What are the Zones?

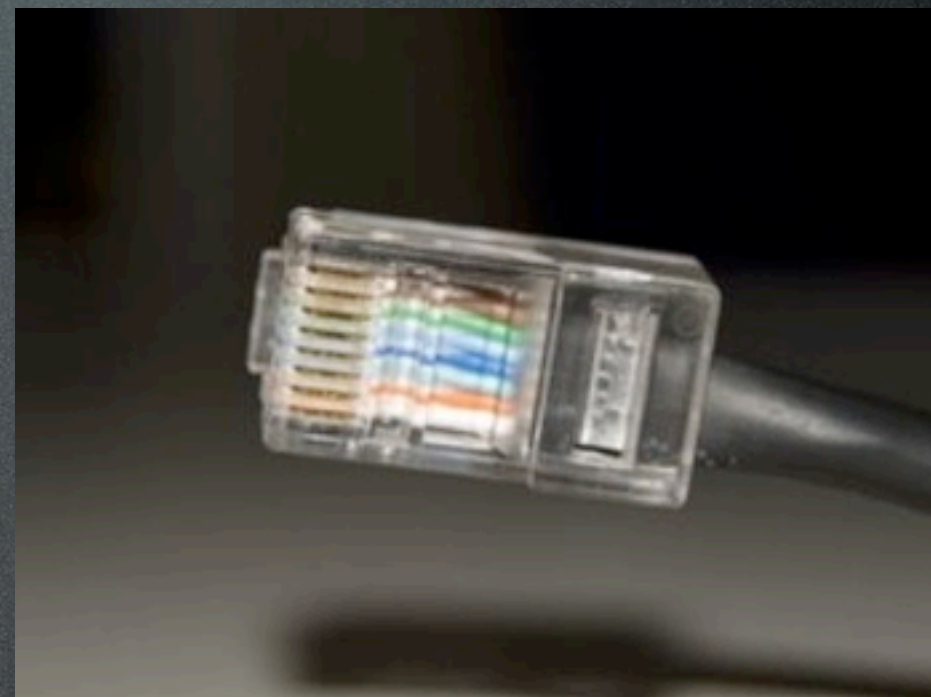


What are the Zones?

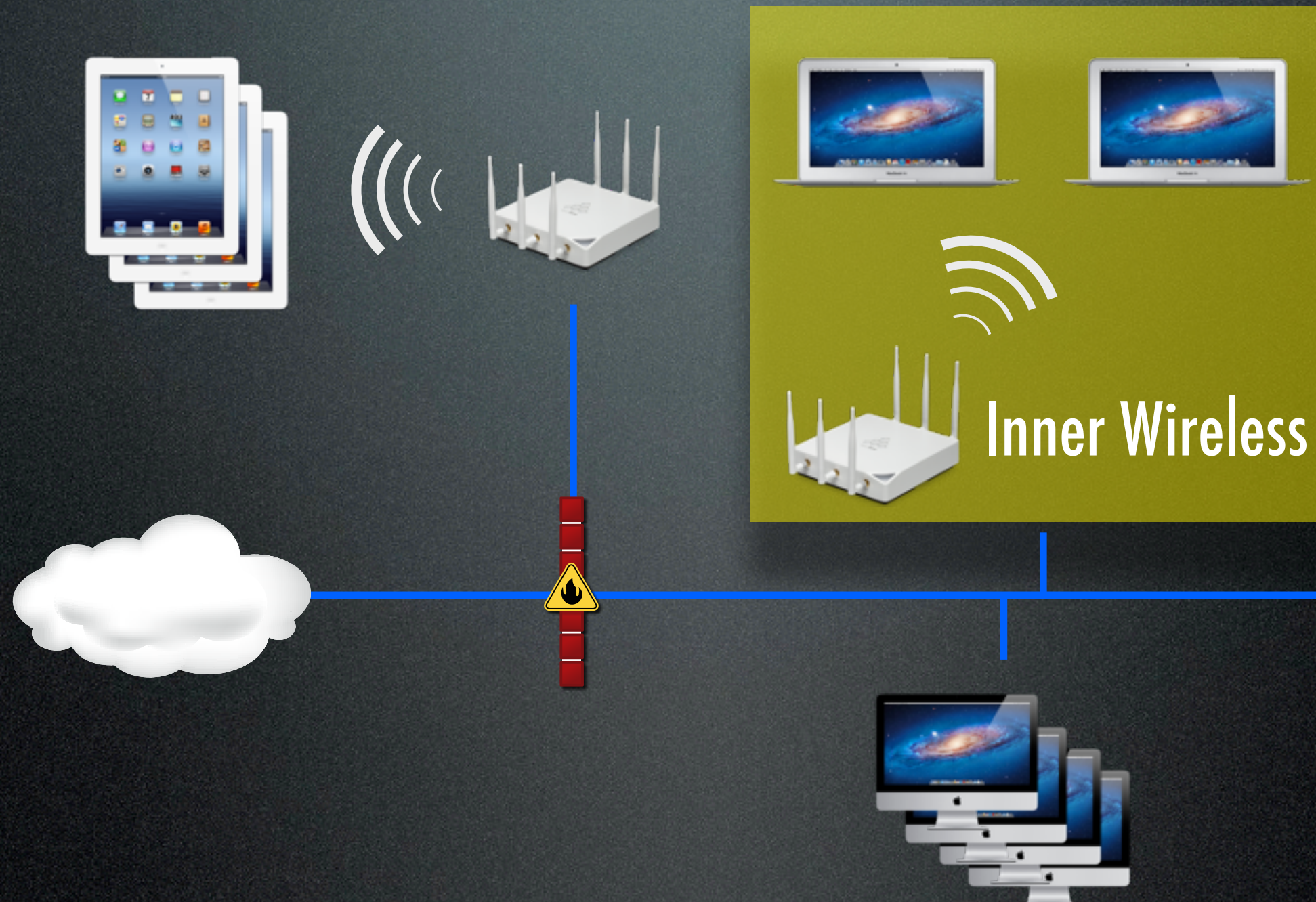


Inner Wired

- Physical Security
- Don't be stupid
- Beware of visitors
- 802.1X



What are the Zones?



Inner Wireless

WPA2
WPA2-Personal
WPA2-PSK
802.1X
WPA2-Enterprise
TKIP
LEAP
RADIUS
EAP
WPA
RADIUS
EAP
PEAP
TLS
EAP-FAST
TTLS

Hidden SSID

- Worthless
- Worse than worthless

Inner Wireless: Simple

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

Inner Wireless: Complex

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

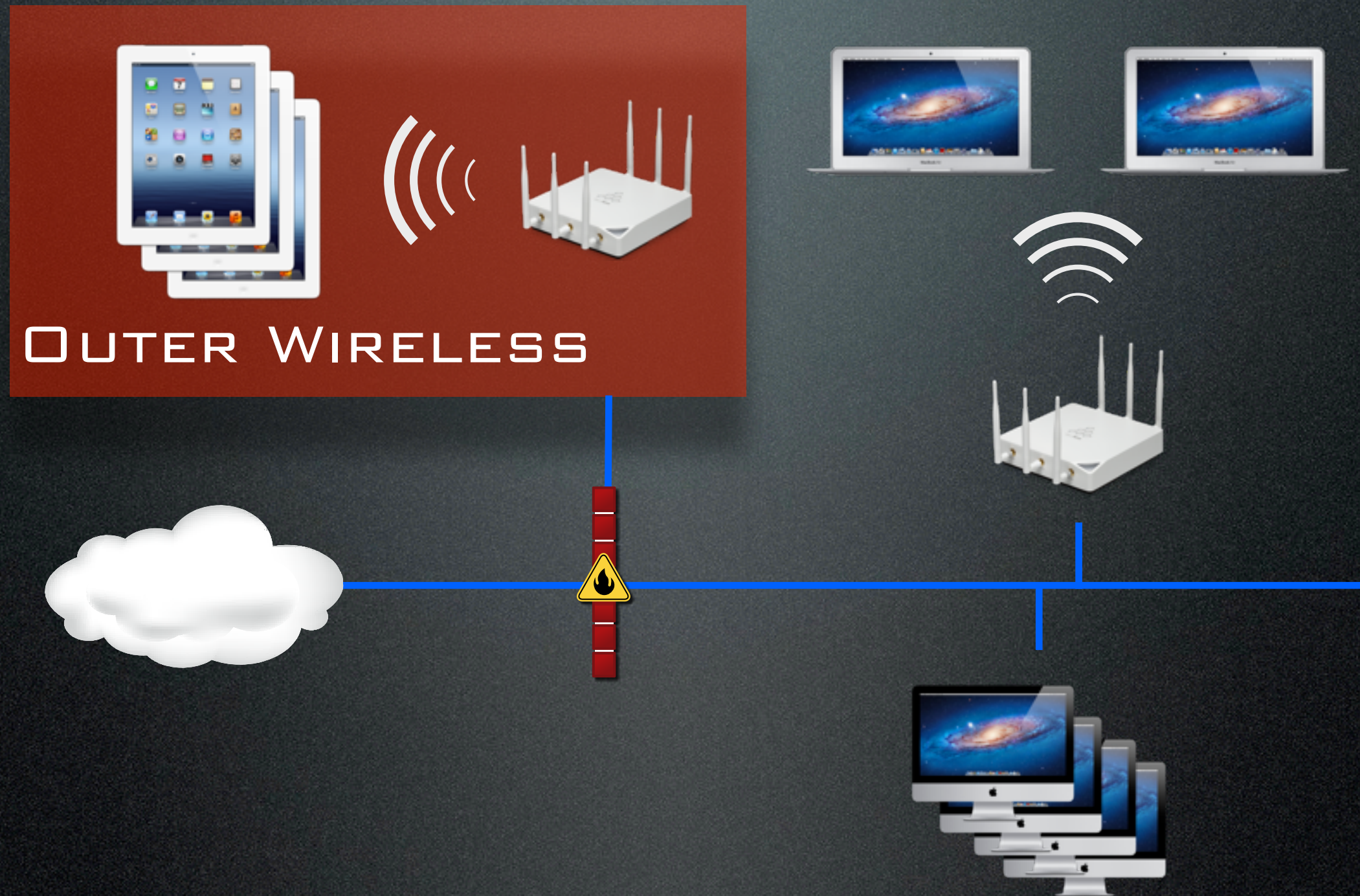
802.1X Details

- 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

802.1X Details

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

What are the Zones?



Outer Wireless

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

Captive Portal

AT&T 3G 9:51 PM 44%

http://ezxcess.antlabs.com

Log In Cancel

Travelodge

Authentication: Complimentary access

Complimentary Code:

Your Name:

Room #:

Your Email:

Connect Now >

INTERNET USE POLICY / Acceptable Use Policy (AUP)

The wireless access service PROVIDER is referred to as PROVIDER and the client using the services is referred to as the END USER. Overall Principles:

1. The END USER agrees to use the network for lawful activities. The use of the network support provided by Redwood Systems Group.

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

IDS/IPS

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

Unified Threat Management

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

Unified Threat Management



Unified Threat Management



Q & A

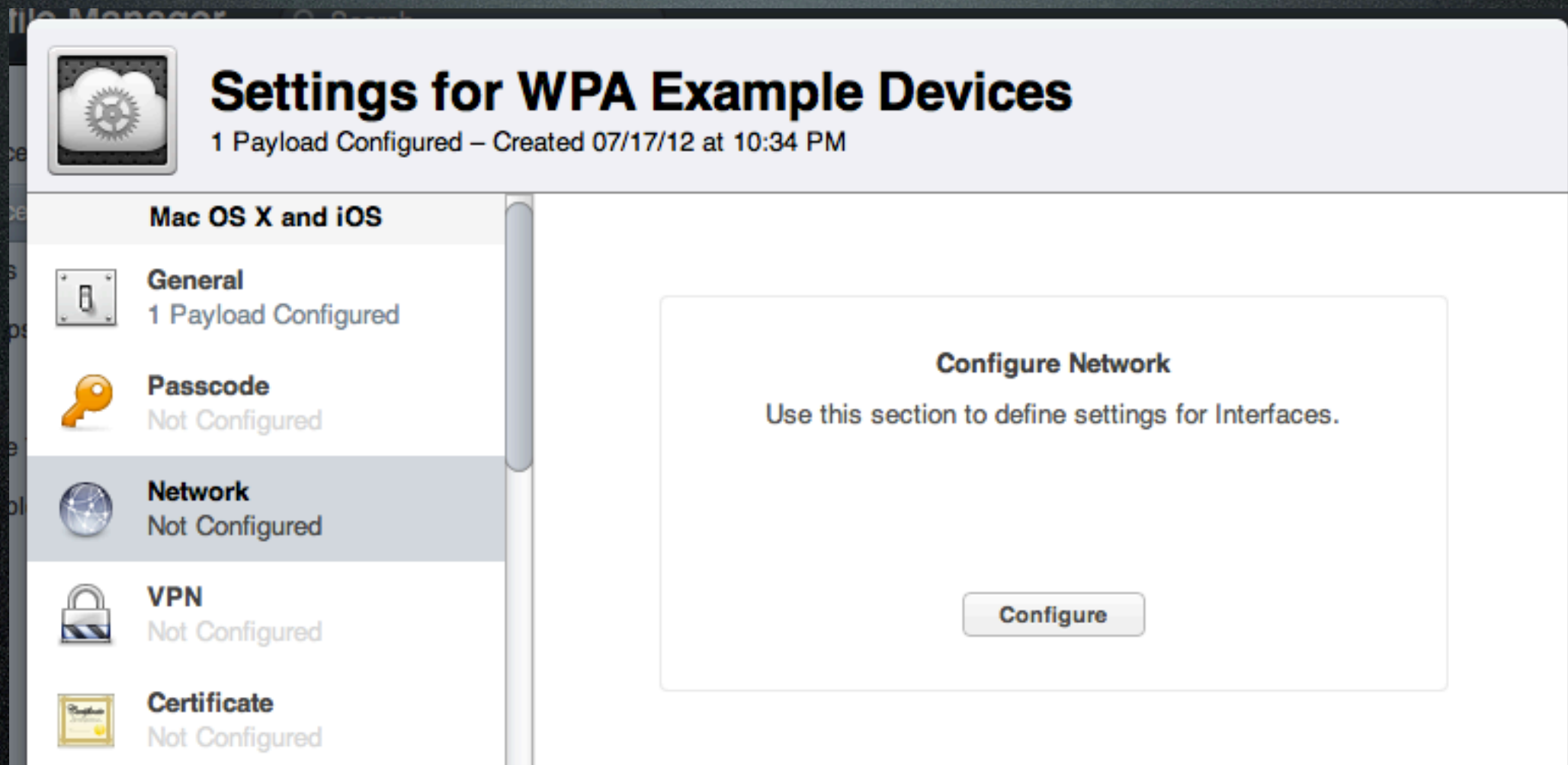
Mark Jeffries
mark@favarger.net



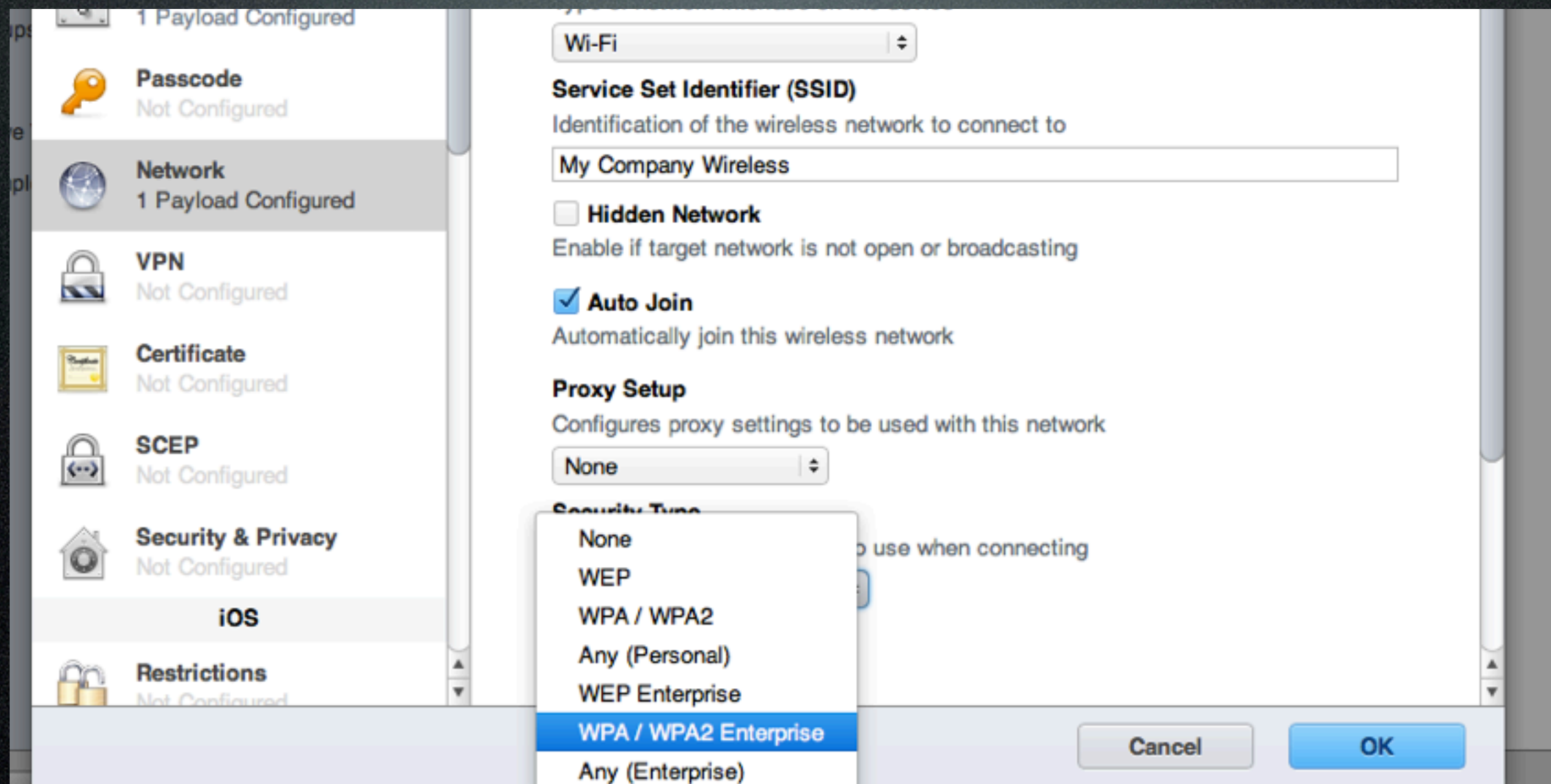
Demo

802.1X Profile Creation

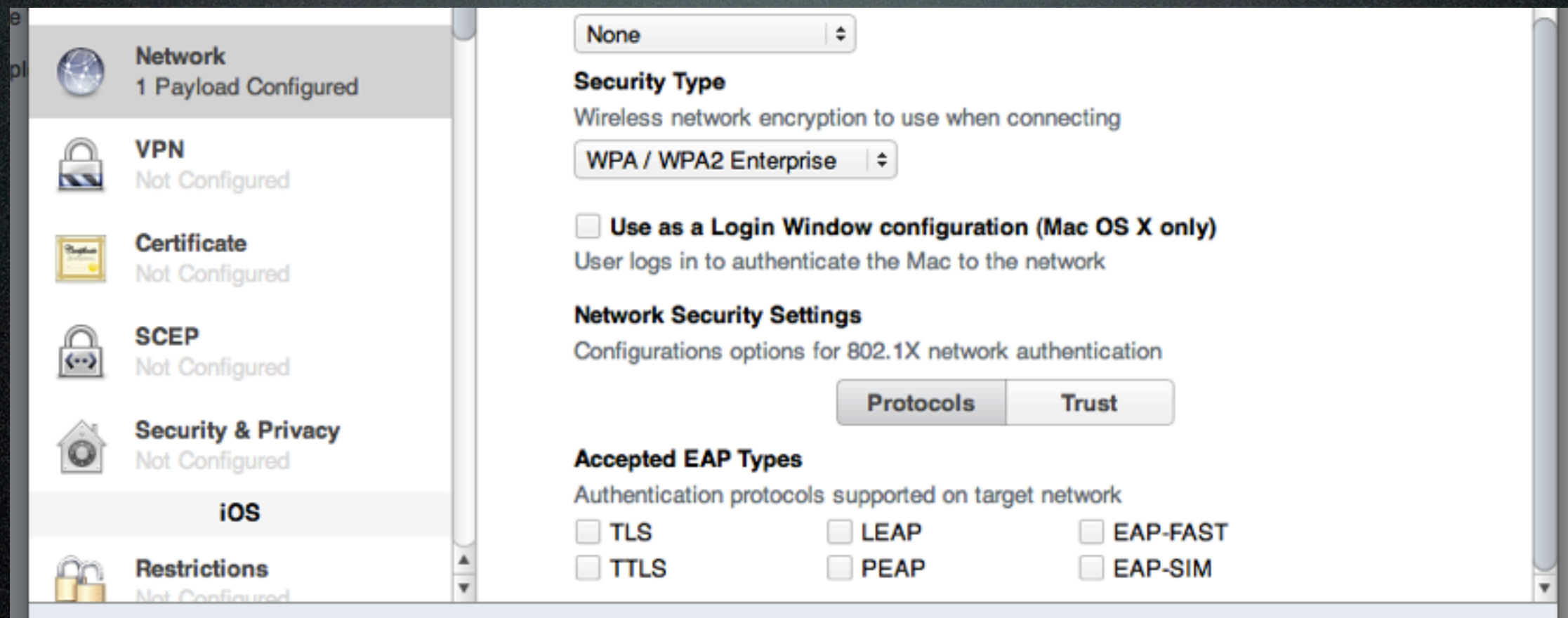
802.1X Profile Creation



802.1X Profile Creation



802.1X Profile Creation



802.1X Profile Creation

The screenshot shows the 'Network' settings window for a Mac OS X system. The left sidebar lists various settings: General (1 Payload Configured), Passcode (Not Configured), Network (1 Payload Configured), VPN (Not Configured), Certificate (Not Configured), SCEP (Not Configured), Security & Privacy (Not Configured), iOS, and Restrictions (Not Configured). The 'Network' section is selected, and the 'Protocols' tab is active. The 'Accepted EAP Types' section shows 'TTLS' selected with a blue checkmark, while 'TLS', 'LEAP', 'EAP-FAST', 'PEAP', and 'EAP-SIM' are unselected. Below this, the 'Use Directory Authentication' checkbox is also unselected. The 'Username' field is empty, and the 'Password' field is also empty. The 'Inner Authentication' dropdown menu is set to 'MSCHAPv2'. The 'Outer Identity' field is empty.

Mac OS X and iOS

General
1 Payload Configured

Passcode
Not Configured

Network
1 Payload Configured

VPN
Not Configured

Certificate
Not Configured

SCEP
Not Configured

Security & Privacy
Not Configured

iOS

Restrictions
Not Configured

Protocols **Trust**

Accepted EAP Types
Authentication protocols supported on target network

☐ TLS ☐ LEAP ☐ EAP-FAST
☒ TTLS ☐ PEAP ☐ EAP-SIM

☐ **Use Directory Authentication**
Authenticate with the target machine's directory credentials

Username
Username for connection to the network

Password
Password for the provided username

Inner Authentication
Authentication protocol (for use only with TTLS)
MSCHAPv2

Outer Identity
Externally visible identification (TTLS, PEAP, and EAP-FAST)

802.1X Profile Creation

