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

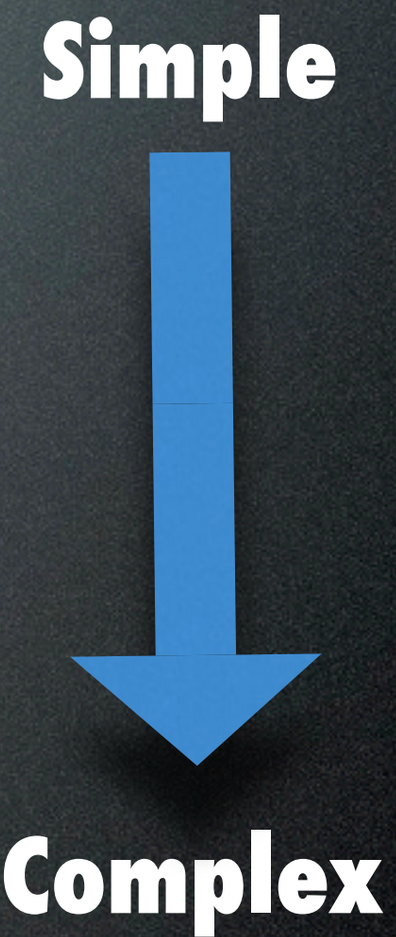
FAVARGER CONSULTING

Gauge Your Network

- Size
- Data
- Threats
- Requirements

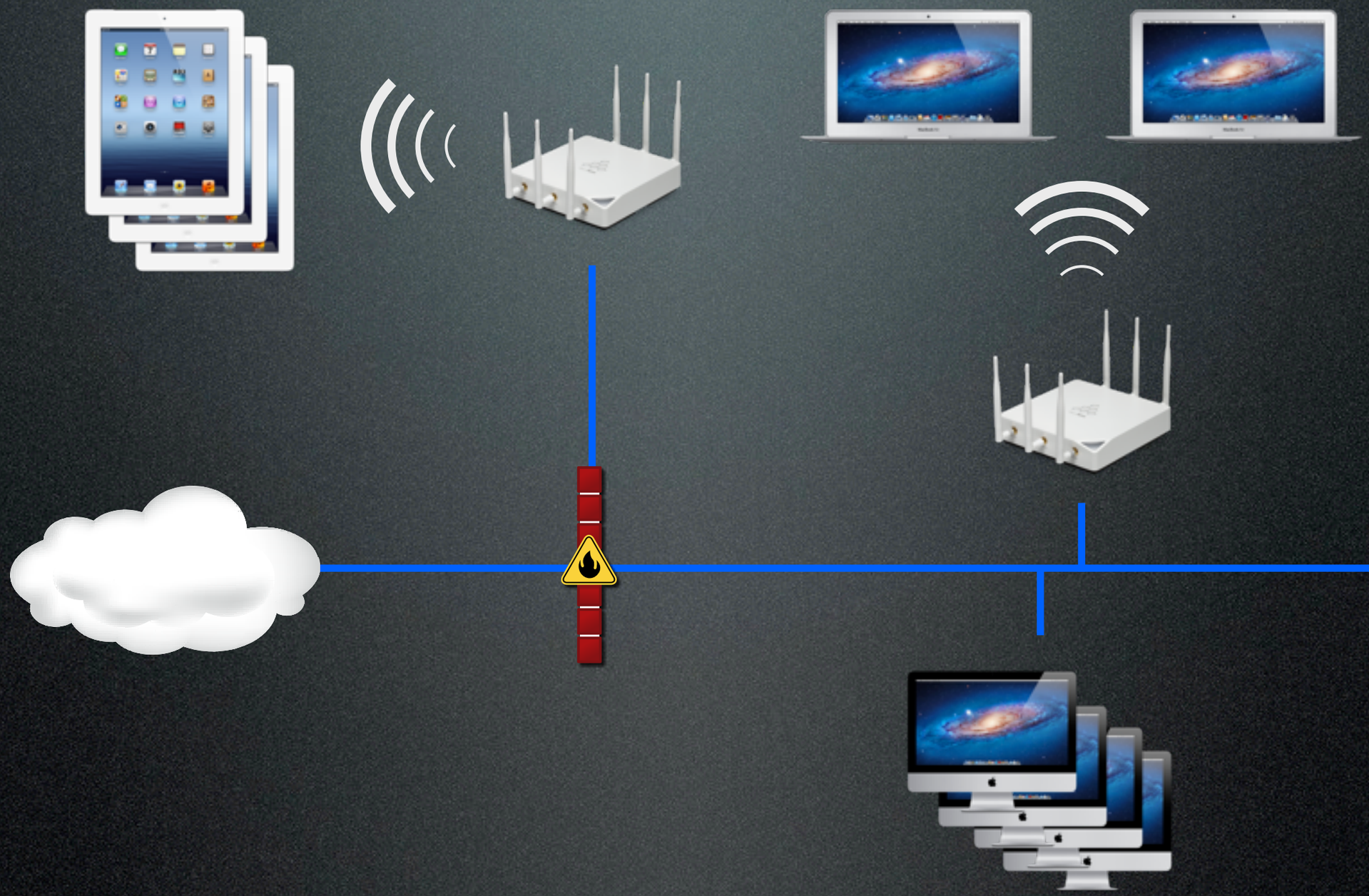
How Much Do You Want to Manage?

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



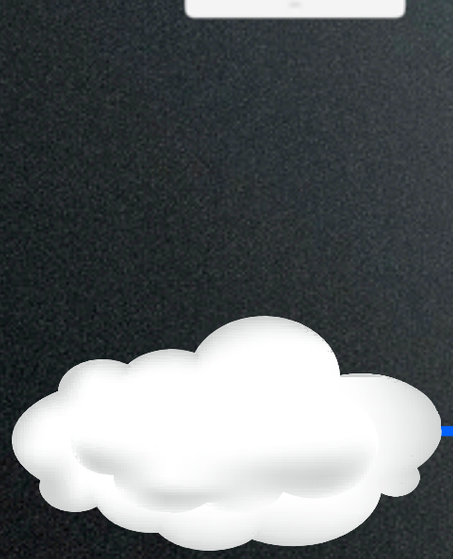
FAVARGER CONSULTING

What are the Zones?



FAVARGER CONSULTING

What are the Zones?

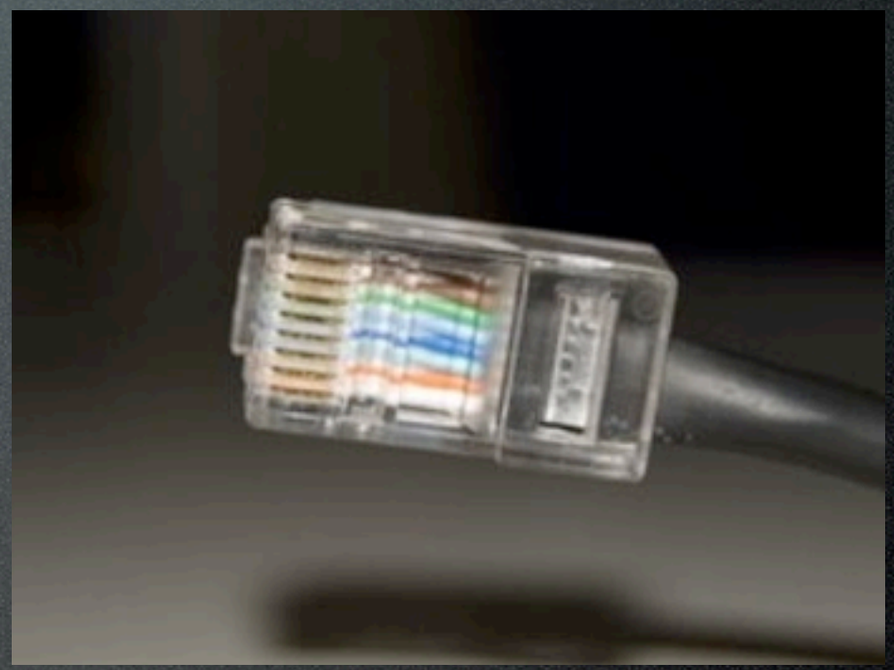


Inner Wired

FAVARGER CONSULTING

Inner Wired

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



What are the Zones?

FAVARGER CONSULTING

Inner Wireless

RADIUS

WPA2

WPA2-Personal

EAP

WPA2-Enterprise

RADIUS

WPA

TTLS

WPA2-PSK

802.1X

TKIP

EAP-FAST

PEAP

TLS

LEAP

Hidden SSID

- Worthless
- Worse than worthless

Inner Wireless: Simple

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

FAVARGER CONSULTING

Inner Wireless: Complex

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

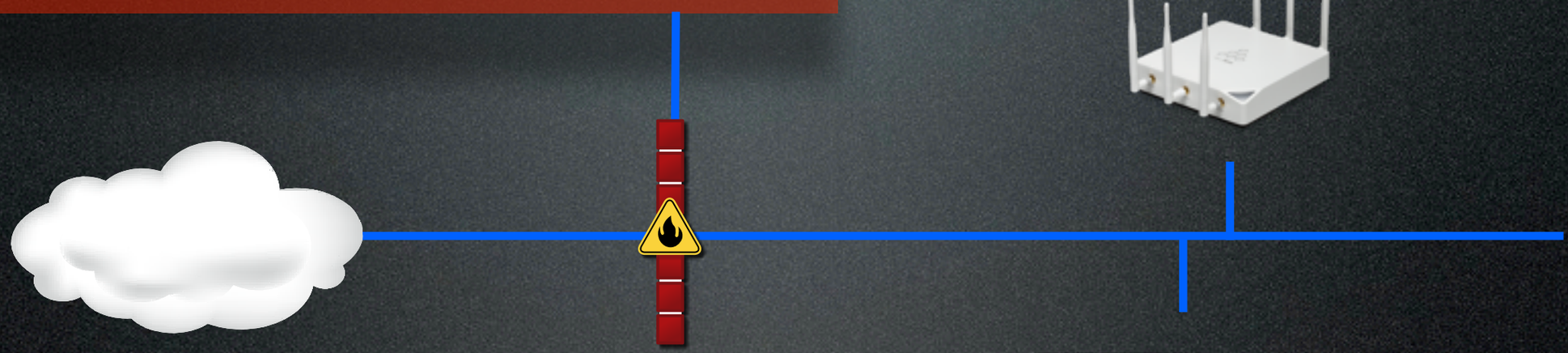
802.1X Details

- 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

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

FAVARGER CONSULTING

Unified Threat Management

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

Unified Threat Management

Unified Threat Management

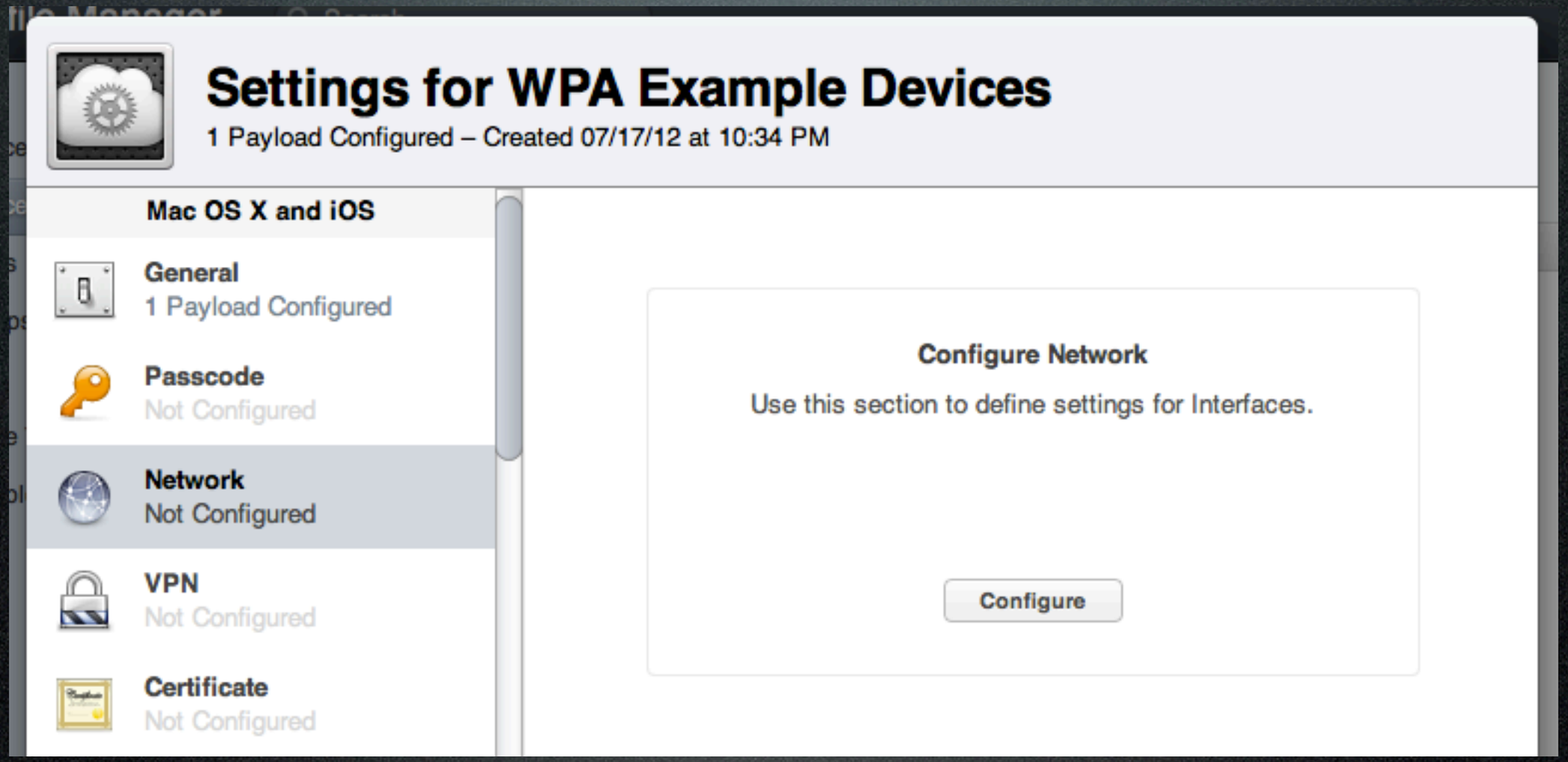
Q & A

Mark Jeffries
mark@favarger.net

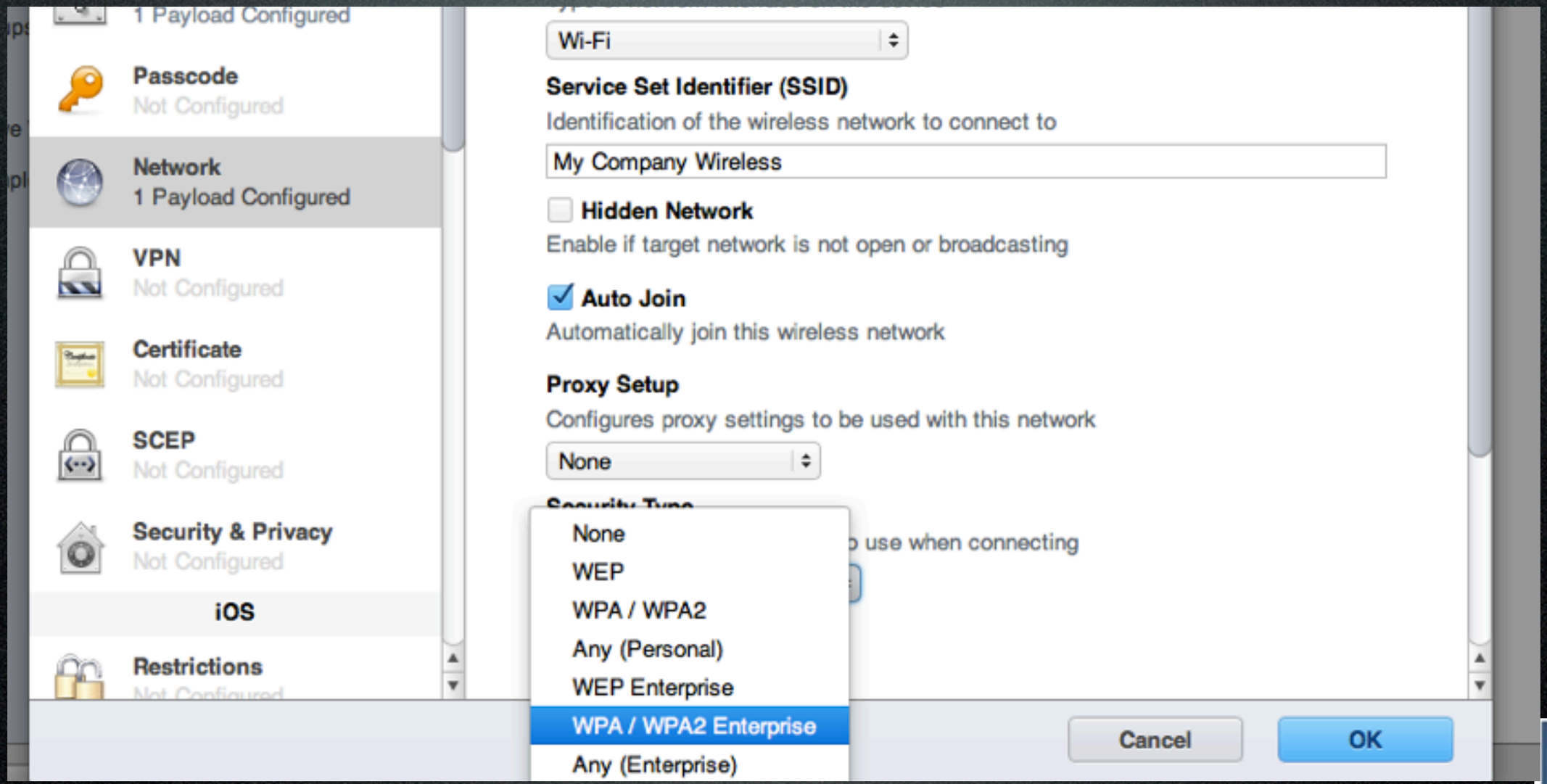
Demo

802.1X Profile Creation

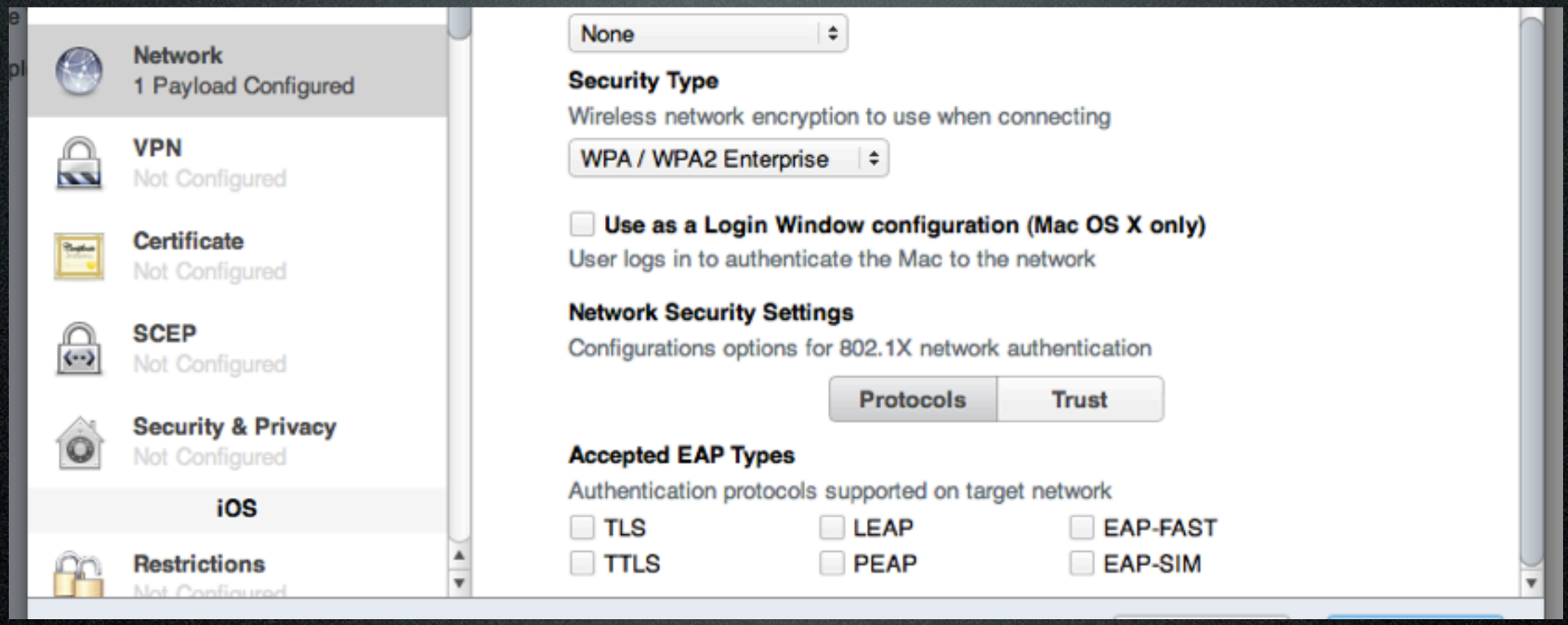
802.1X Profile Creation



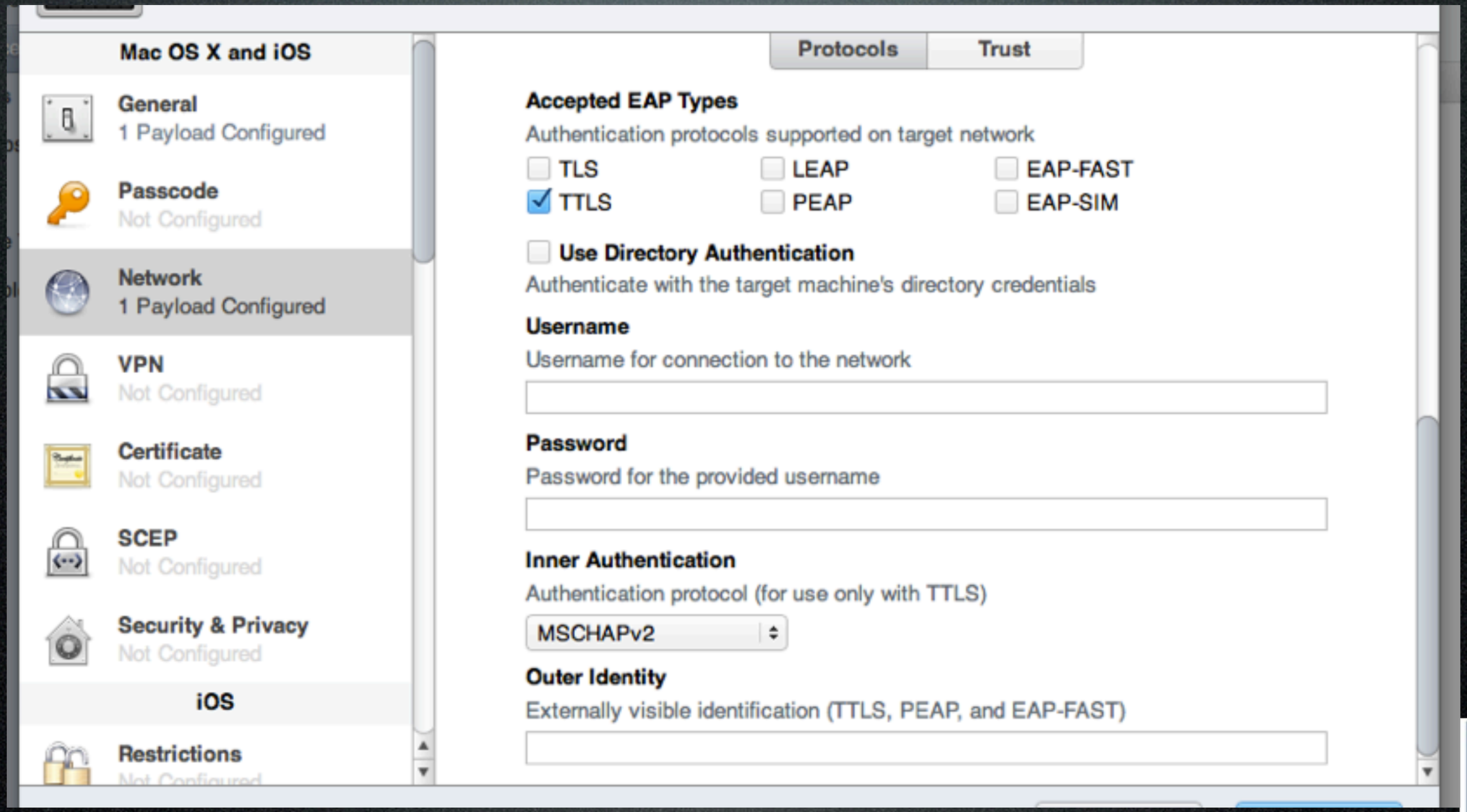
802.1X Profile Creation



802.1X Profile Creation



802.1X Profile Creation



802.1X Profile Creation