# *Enterprise Wireless Security*

# Agenda

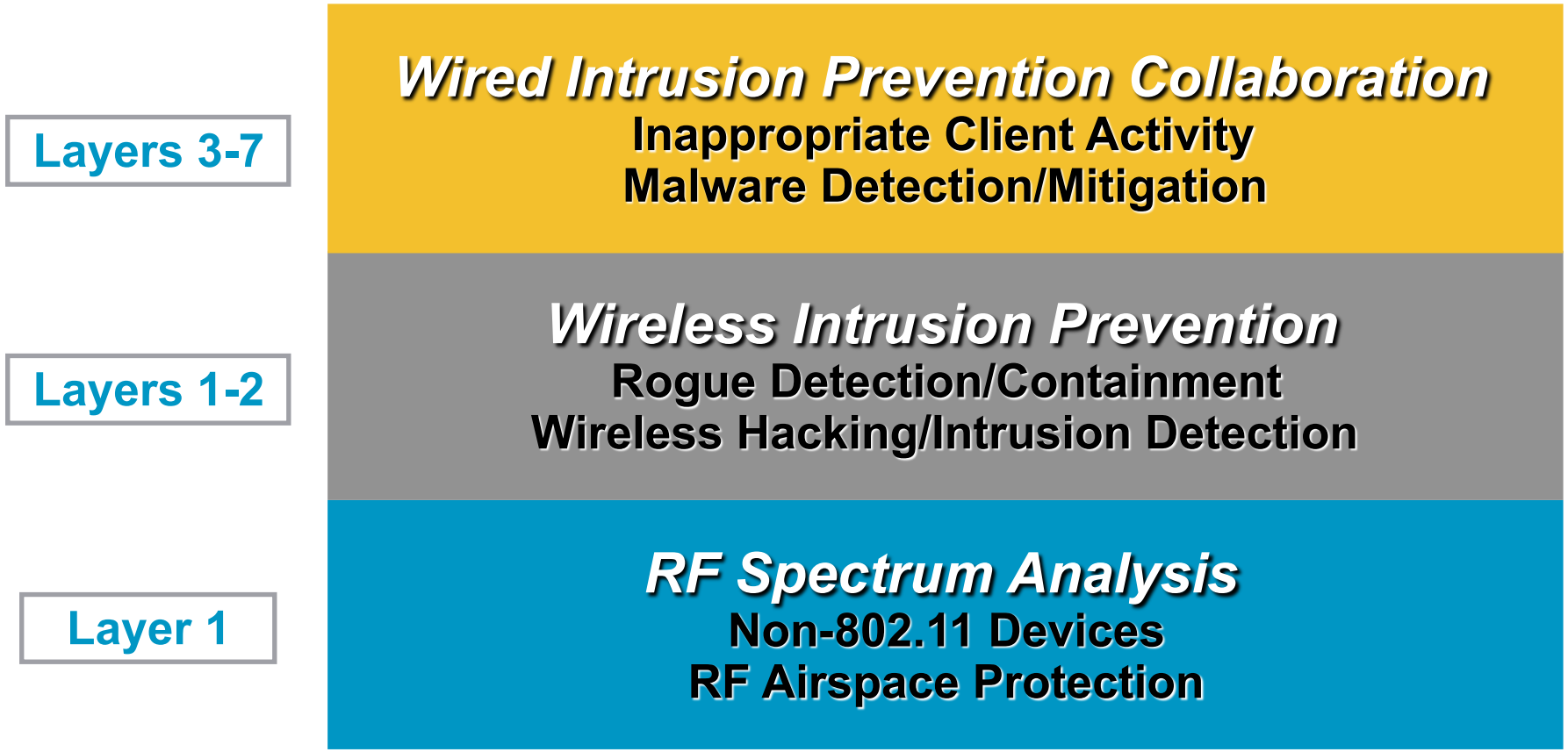
- Corporate Governance and Regulatory
- Wireless Threads and Attack tools
- Enterprise-class WLAN secure network architecture

# Security & Compliance

- Business and security compliance is top-of-mind for executives
- Protecting sensitive business and customer data is the key focus of regulatory compliance requirements

| | |
|---|---|
| Sarbanes-Oxley | Publicly Traded Companies Must:<br>• Maintain an adequate internal control structure and procedures for financial reporting<br>• Assess the effectiveness of internal control structures |
| HIPAA | For Patient Information, Firms Must:<br>• Maintain administrative, technical and physical safeguards to ensure integrity and confidentiality<br>• Protect against threats or hazards; unauthorized uses or disclosures |
| PCI | All Merchants Using Payment Cards, Must:<br>• Build and maintain a secure network<br>• Protect and encrypt cardholder data<br>• Regularly monitor and test networks, including wireless |

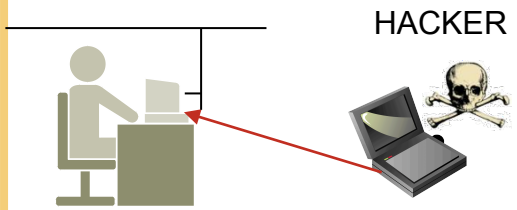
# Wireless Threat Control & Containment – Layer 1-7 Protection



# Wireless Security Threats
## *Top Attacks*

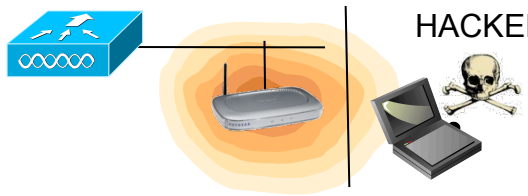
### *On-Wire Attacks*

#### Ad-hoc Wireless Bridge




**Client-to-client backdoor access**

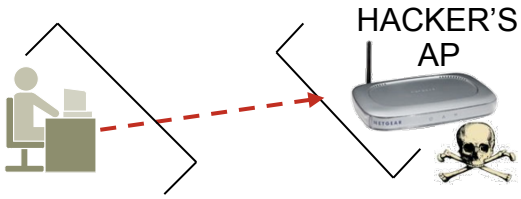
#### Rogue Access Points




**Backdoor network access**

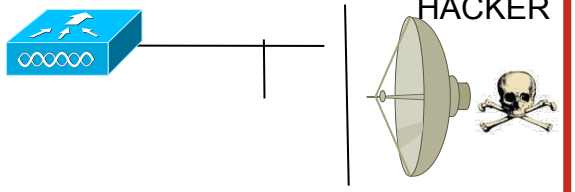
### *Over-the-Air Attacks*

#### Evil Twin/Honeypot AP




**Connection to malicious AP**

#### Reconnaissance

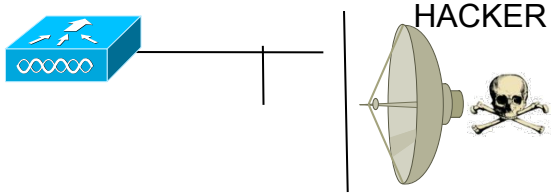



**Seeking network vulnerabilities**

#### Denial of Service


**Service disruption**

#### Cracking Tools




**Sniffing and eavesdropping**

### Non-802.11 Attacks

**Backdoor access**

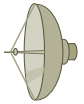
BLUETOOTH AP

**Service disruption**

MICROWAVE

BLUETOOTH

RF-JAMMERS



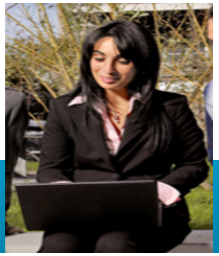
RADAR

# Over-the-Air Attack Techniques and Tools

## *Examples of Attacks Detected*

### Network Profiling and Reconnaissance

- Honeypot AP
- Netstumbler
- Kismet
- Wellenreiter
- Excessive device error
- Excessive multicast/broadcast



### Authentication and Encryption Cracking

- Dictionary attacks
- AirSnarf
- Hotspotter
- WEPCrack
- ASLEAP
- EAP-based attacks
- CoWPAtty
- Chop-Chop
- Airckrack
- Airsnort
- PSPF violation
- WEP Attack
- Illegal frame types
- Excessive association retries
- Excessive auth retries
- LEAPCracker

### Man-in-the-Middle

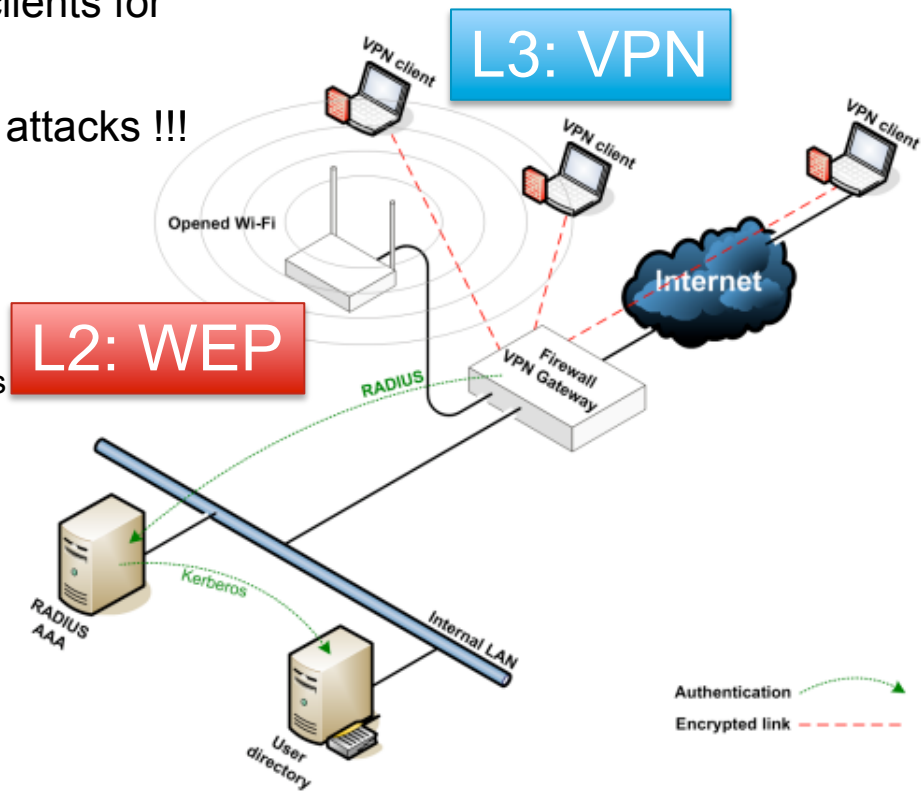
- MAC/IP Spoofing
- Fake AP
- Evil Twin AP
- ARP Request Replay Attack
- Fake DHCP server
- Pre-standard APs (a,b,g,n)

### Denial of Service

- Malformed 802.11 frames
- FATA-Jack, AirJack
- Fragmentation attacks
- Excessive authentication
- De-auth attacks
- Association attacks
- CTS attacks
- RTS attacks
- Excessive device bandwidth
- EAPOL attacks
- Probe-response
- Resource management
- RF Jamming
- Michael
- Queensland
- Virtual carrier
- Big NAV
- Power-save attacks
- Microwave interference
- Bluetooth interference
- Radar interference
- Other non-802.11 interference
- Device error-rate exceeded
- Interfering APs
- Co-channel interference
- VoWLAN-based attacks
- Excessive roaming

# VPN only network security?

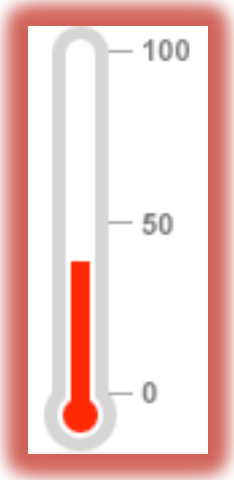
- Allowing the hacker to get onto your open Wi-Fi network and probe your network and Wi-Fi clients for weaknesses !!!
- Prone to many MiM attacks !!!
  - Rogue DHCP
  - ARP poisoning
  - Broadcast Storm
  - Exploit VPN
  - Gateway DoS Attacks



# Was WPA/WPA2 really cracked?

- WPA-PSK (pre-shared key)
  - Vulnerable to Dictionary Attack when using simple words (Happy, Infinitive …)
  - 10-character alpha-numeric random PSK will make it impractical to crack with dictionary attacks. E.g. (3tAy_4WaY_1a)

# Enterprise WLAN Security Index




**Top Security Issues** | View All | Devices

- MFP Client Protection set to Optional for WLAN. (8)
- Client Exclusion disabled for WLAN. (6)
- No WLAN Key Management methods set(Only settable when Authentication Method is WPA+WPA2). (4)
- SSH enabled and timeout set to zero for a Controller. (2)
- WEP 104 bits as one of WLAN Encryption Methods(802.1X or WEP Authentication Method). (2)

**AP Threats/Attacks**

| AP Threats/Attacks | Last Hour | 24 Hours | Total Active |
|---|---|---|---|
| Fake AP Attack | 0 | 2 | 32 |

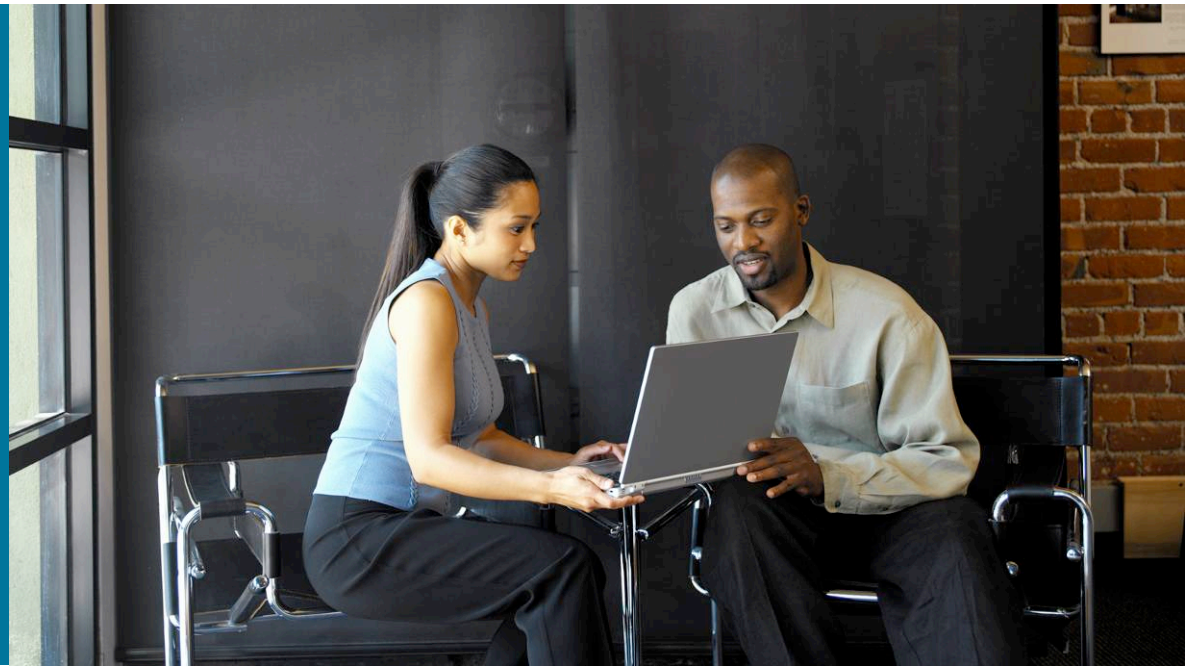
**Attacks Detected**

| wIPS Denial of Service Attacks | Last Hour | 24 Hours | Total Active |
|---|---|---|---|
| Deauth flood | 2 | 3 | 4 |
| EAPOL flood | 0 | 0 | 1 |
| Bcast deauth | 1 | 1 | 1 |

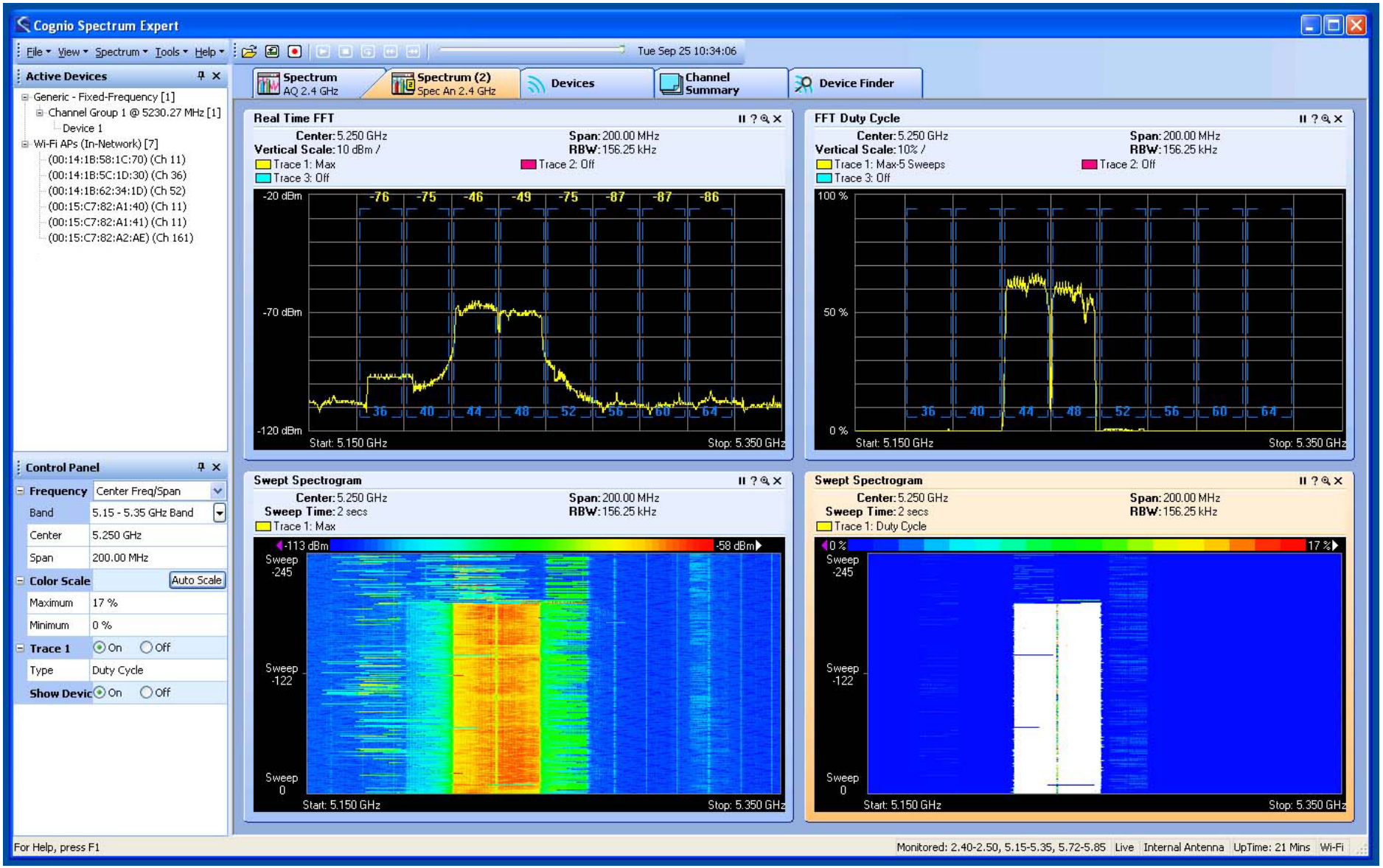
| wIPS Security Penetration Attacks | Last Hour | 24 Hours | Total Active |
|---|---|---|---|
| No Attacks Detected | | | |

| Custom Signature Events | Last Hour | 24 Hours | Total Active |
|---|---|---|---|
| No Attacks Detected | | | |

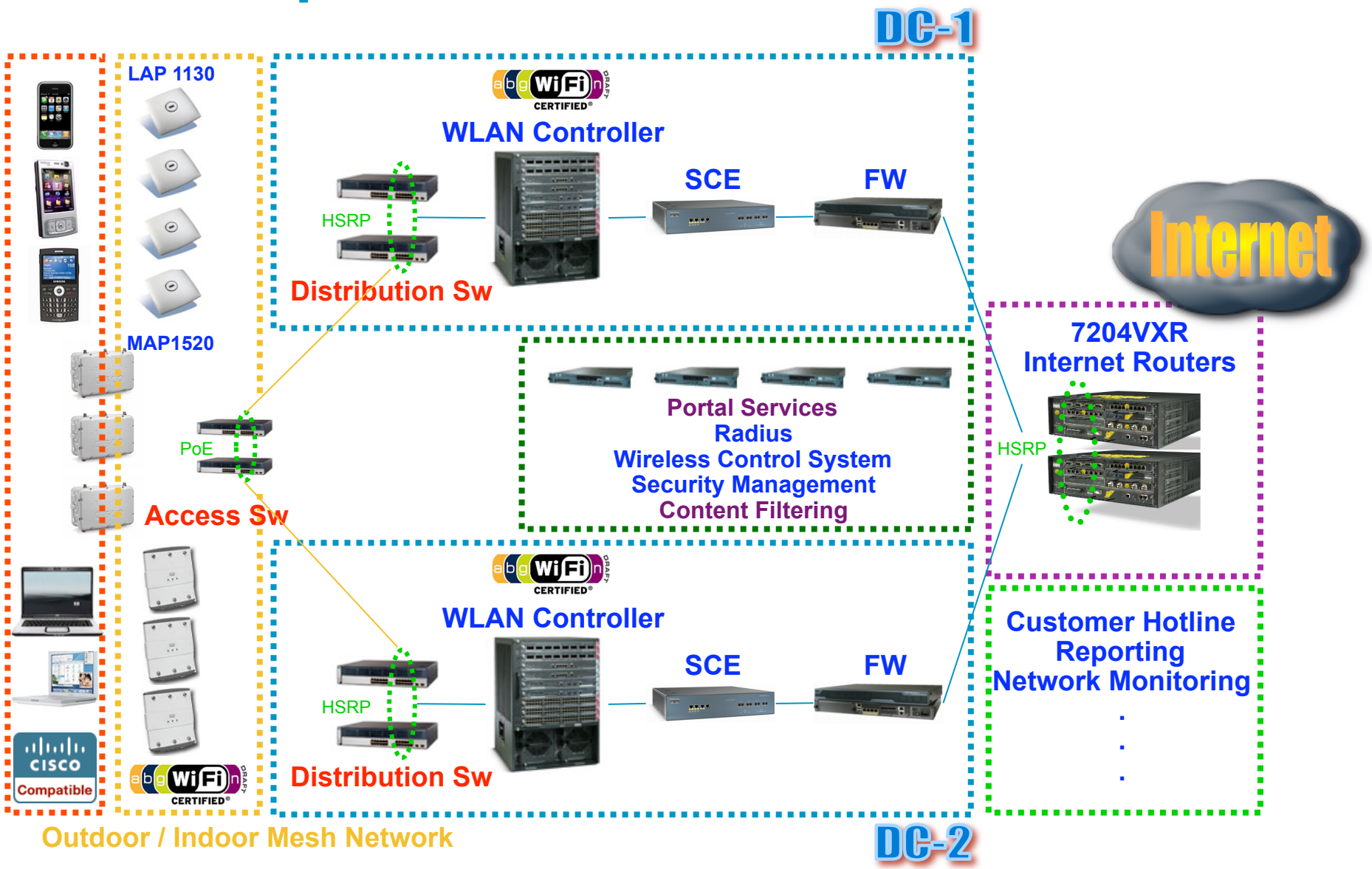
# Enterprise-class WLAN Secure Network Architecture



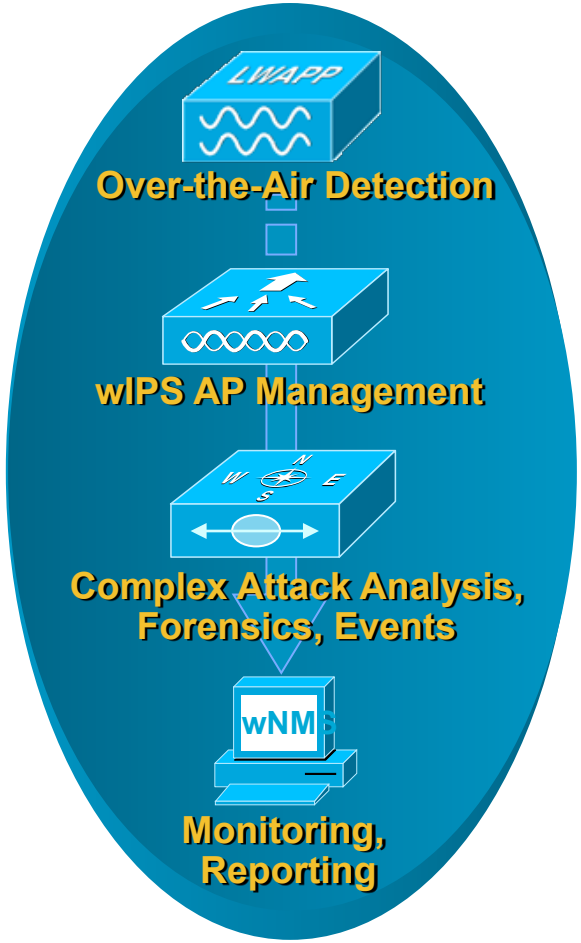
# RF Spectrum Analyzing (L1)



# Enterprise WiFi Services



# wIPS Components (L1-L2)




- wIPS Monitor Mode AP – attack detection
- Controller – manages wIPS APs, forwards wIPS data to wIPS
- wIPS Service – attack archival, correlation and alarm aggregation
- wNMS – centralized configuration and monitoring

# wIPS – AP Detection Logic

00:1F:3B:1A:A2:01

LWAPP

wIPS AP

00:1F:3B:7C:A2:13

00:1F:3B:7C:A2:13

1. Authenticated
2. Associated
3. Passing Data
1. Authentication?
3. Passing Data
2. Association?

802.11 State Machine

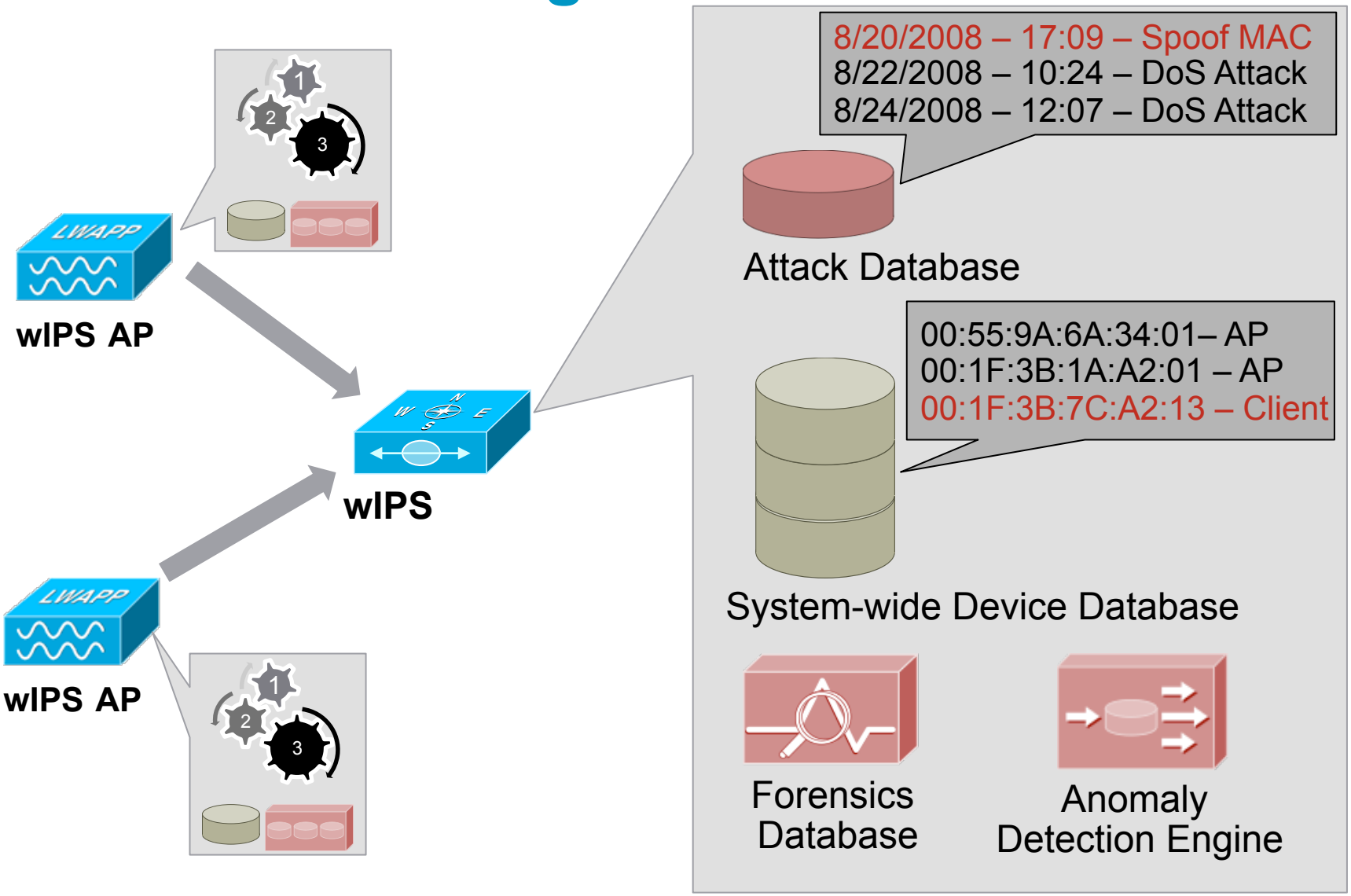
00:1F:3B:1A:A2:01 – AP
00:1F:3B:7C:A2:13 – Client

Device Database

Spoofed MAC

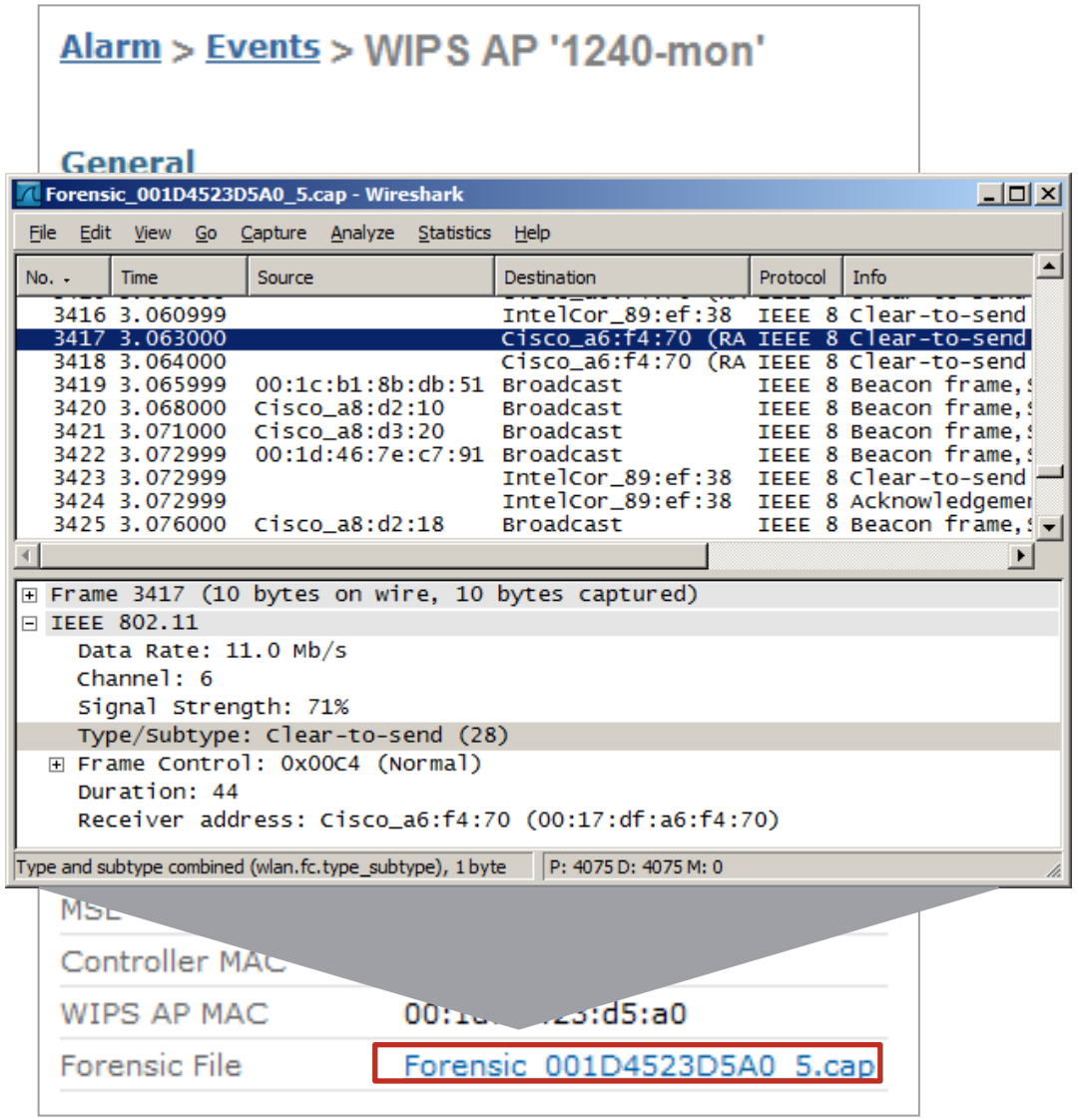
Attack Library

# wIPS Services Engine

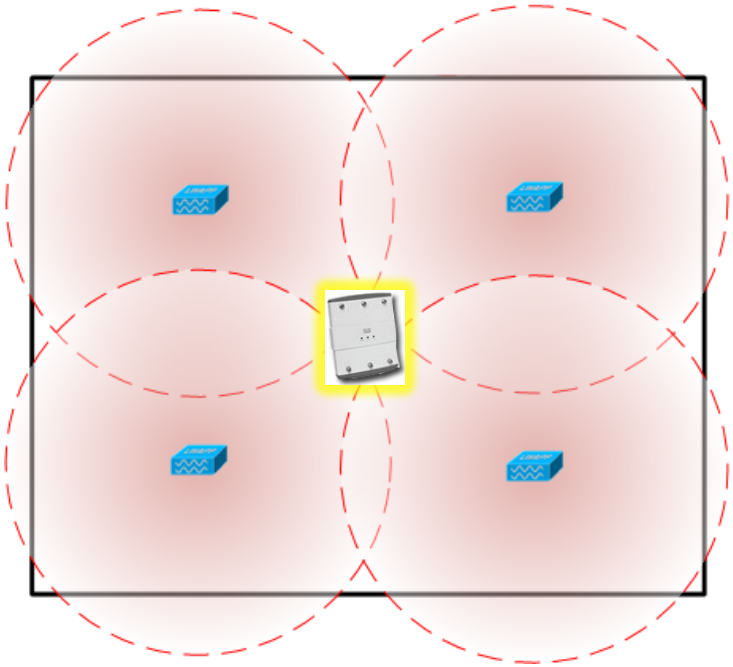


# Forensics

- User configurable per attack
- Captured the first time the attack is detected
- A .cap  capture of packets
  - –Opened by Wireshark, Omnipeek, etc.
- Stored on the wIPS
  - –Can be requested by wNMS on-demand



# Deploy overlay wIPS AP



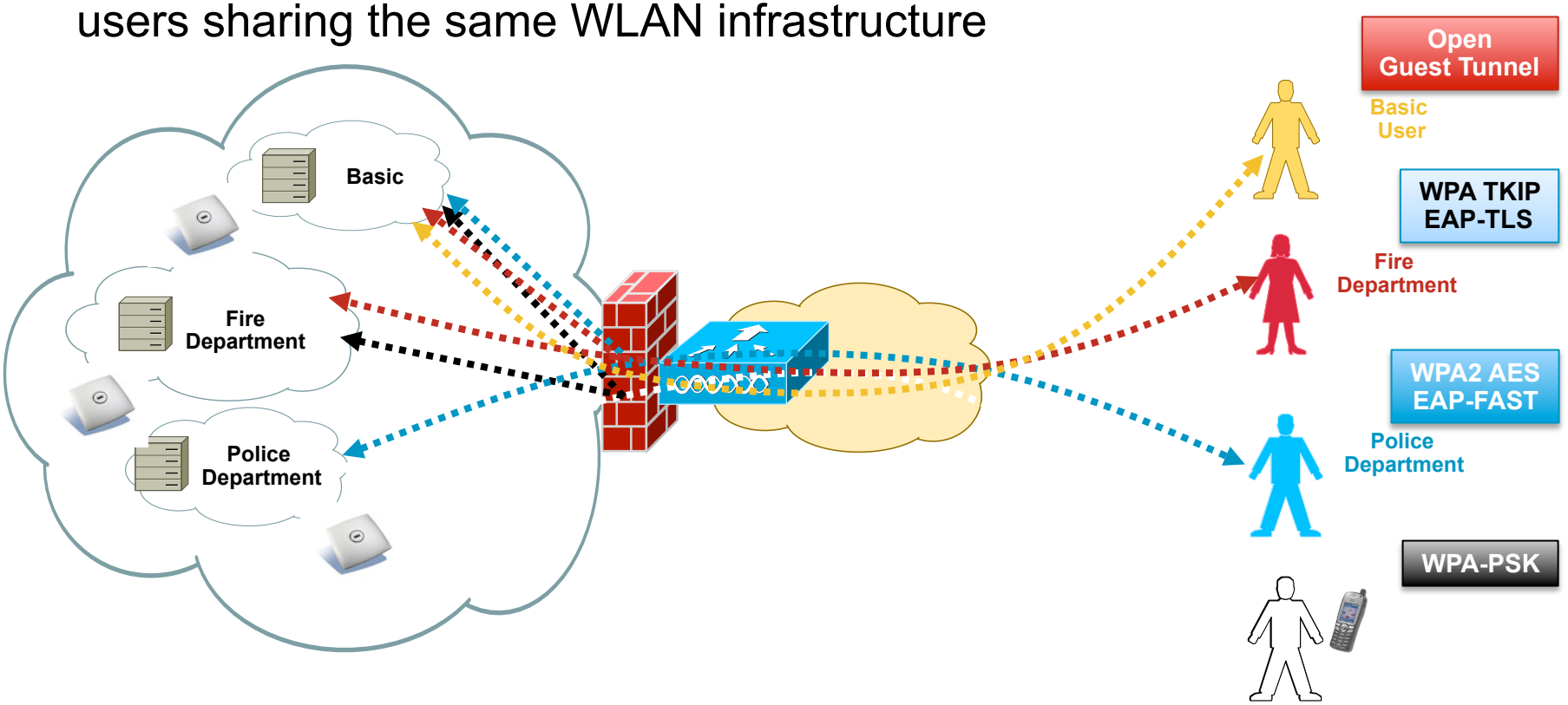
- Environments such as warehouses and manufacturing.
- Deploy 1 wIPS AP every XX,000 sqft.

| Open Indoor Environment | | | |
|---|---|---|---|
| Confidence Level | Deployment Density | 2.4GHz Detection | 5GHz Detection |
| Gold | 30,000 sqft | Exhaustive | Comprehensive |
| Silver | 40,000 sqft | Comprehensive | Adequate |
| Bronze | 50,000 sqft | Adequate | Sparse |

# User Group Access Policy Enforcement

## Firewall Integration on a WLAN Sample Scenario

- To separate users ACL's may suffice, but legal or policy reasons may require a firewall
- Different firewall policies are required for different classes of users sharing the same WLAN infrastructure



# Enterprise-class Wireless Link Layer (L2) Security (per SSID)

General | Security | QoS | Advanced

Layer 2 | Layer 3 | AAA Servers

**WPA+WPA2 Parameters**

WPA — Enabled
- TKIP — Enabled
- AES — Enabled

WPA2 — Enabled
- AES — Enabled
- TKIP — Enabled

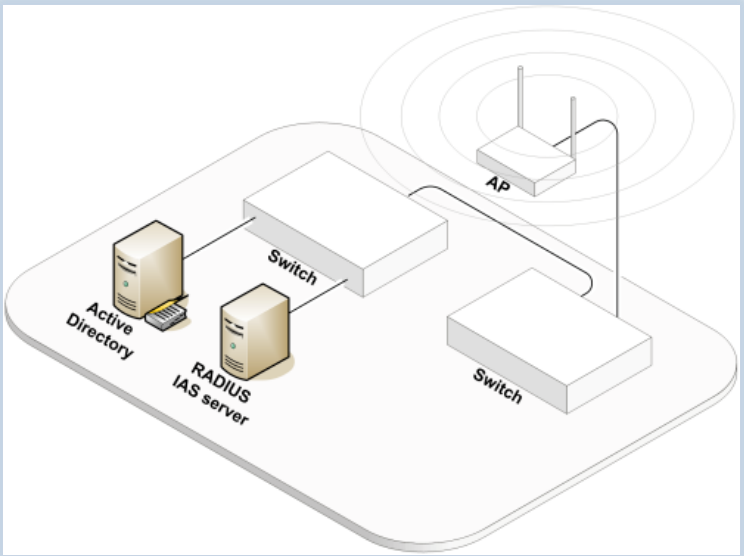
**AuthenticationKeyManagement**

- DOT1X — Enabled
- CCKM — Enabled
- PSK — Enabled

Enable WAP2-AES Encryption

Enable 802.1x Auth

Disable Pre-share Key

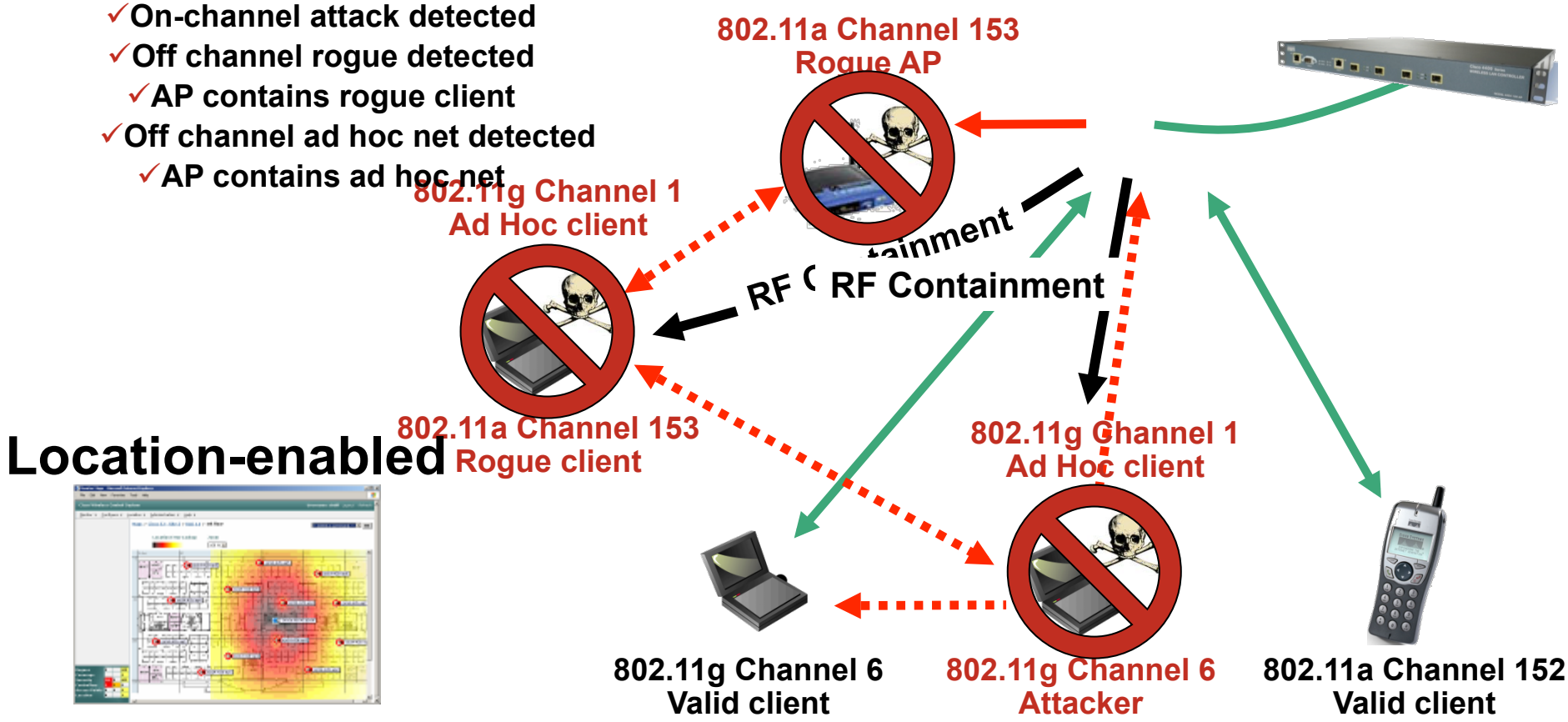


# *Protect the Network*: Rogue Detection and Containment

**ROGUES and AD-HOCs: Detected via intelligent on & off channel scanning**

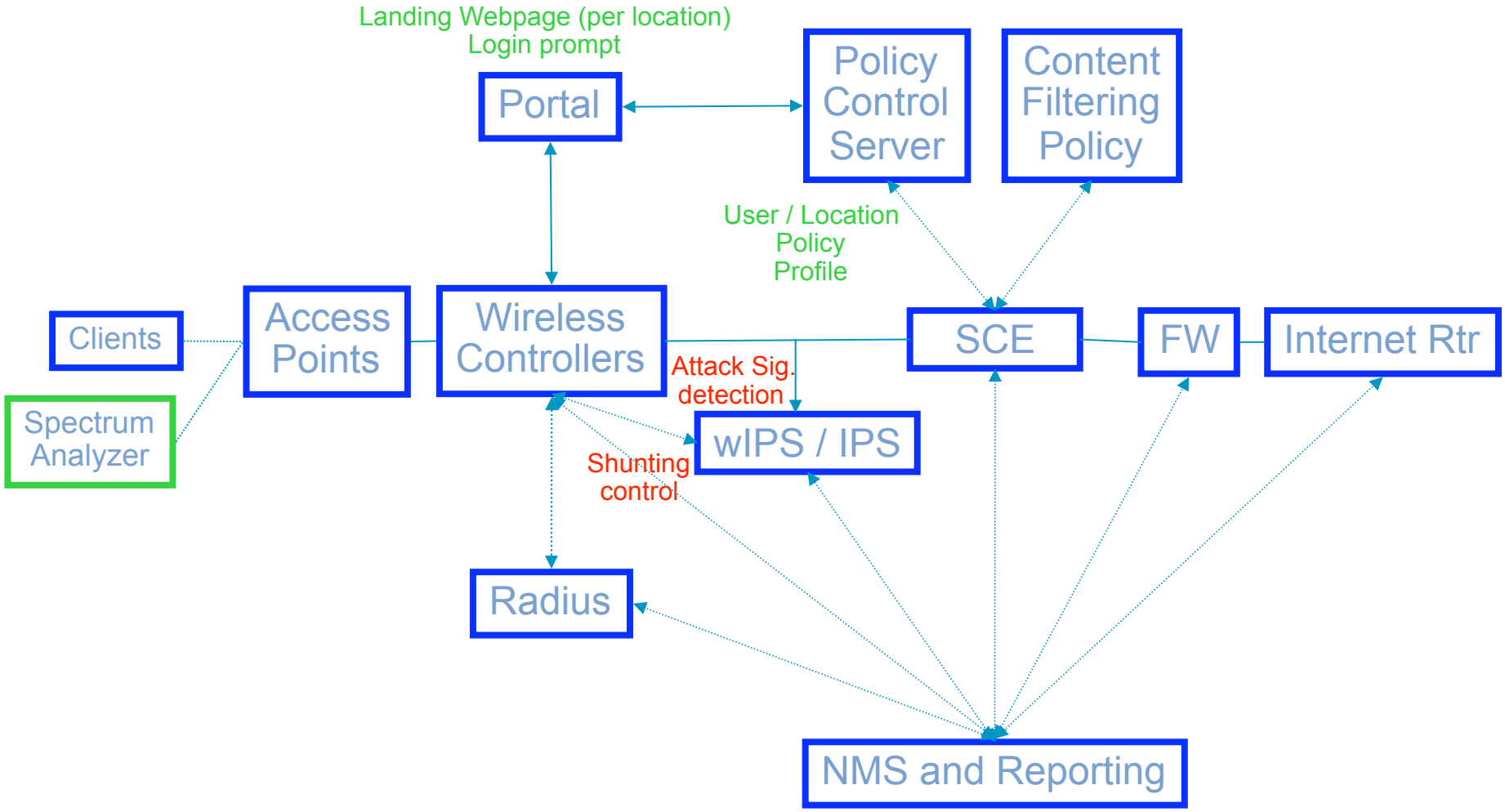
- Integrated 24/7 RF monitoring to identify, locate and contain unauthorized wireless activity
- Proactive threat defense to ensure regulatory compliance

✓On-channel attack detected
✓Off channel rogue detected
✓AP contains rogue client
✓Off channel ad hoc net detected
✓AP contains ad hoc net




**Location-enabled**

# Enterprise Integrated Security (L1-L7)



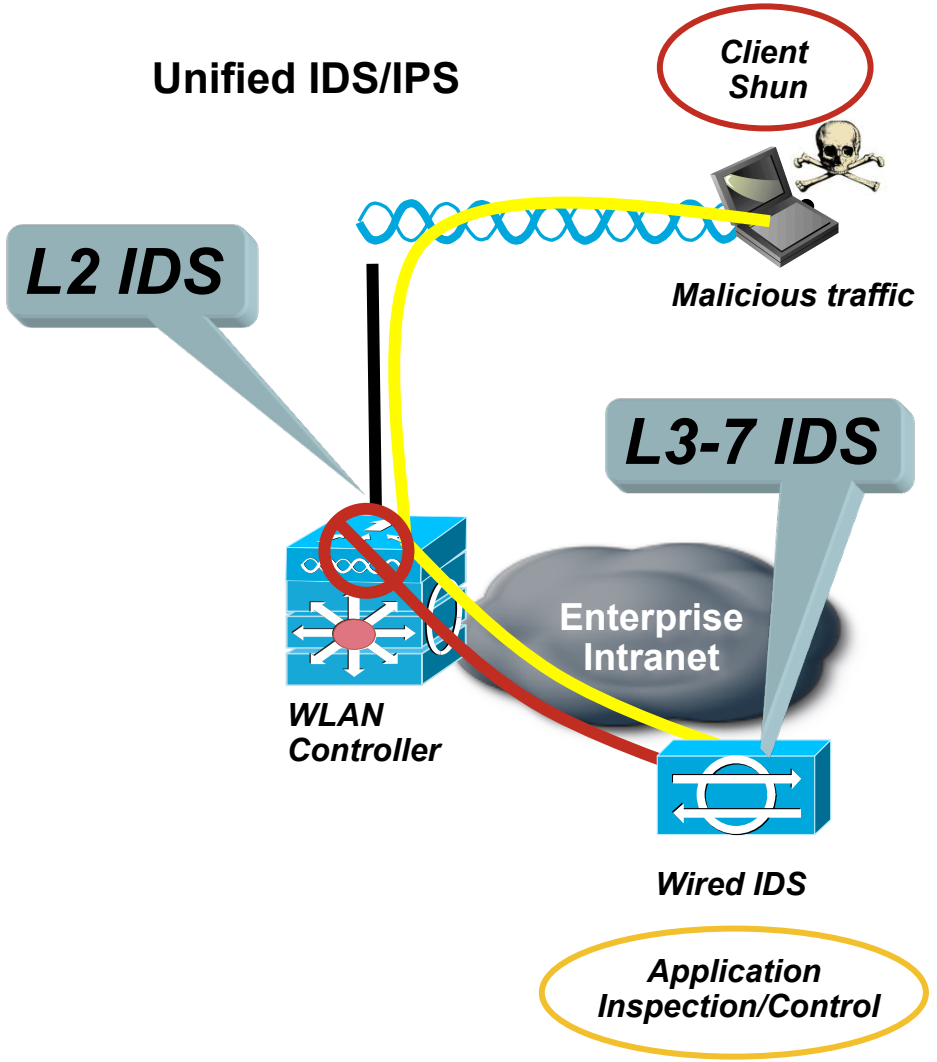
# Unified Wired and Wireless IDS/IPS

**Problem**

- Authorized user's laptop infected with worm or virus

**Solution**

- IDS/IPS sensor monitors traffic with application inspection and control (Layer 7) to identify and triggers shun event
- The network blocks the MAC address of compromised wireless client
- Integration of wired and wireless security



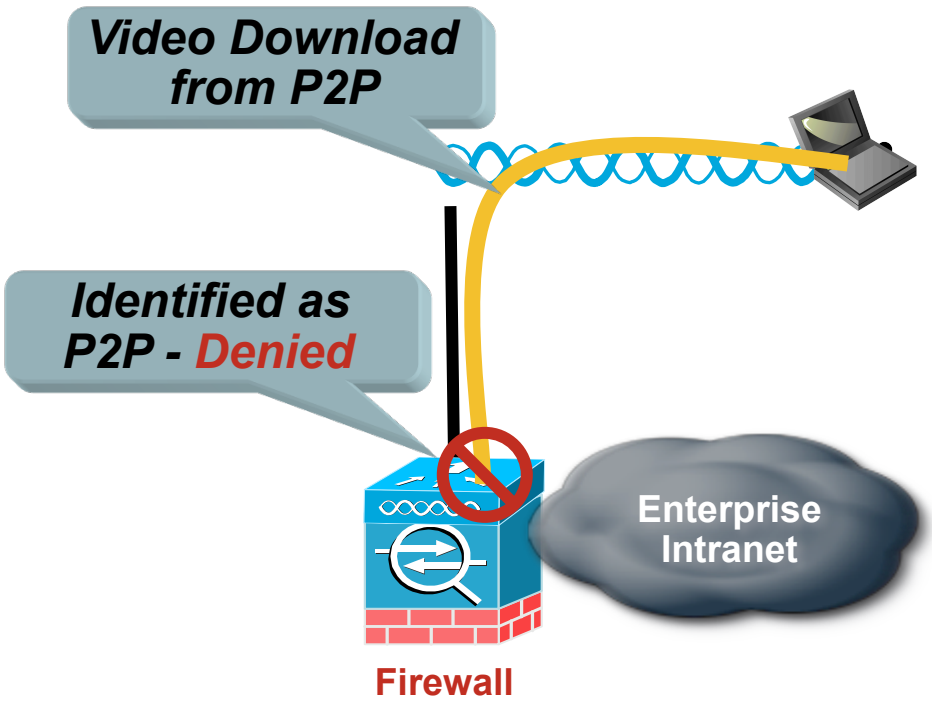
# Wireless Traffic Inspection and Application Control

## Problem

- Application abuse can consume precious bandwidth
- Unauthorized or malicious traffic can traverse legal ports

## Solution

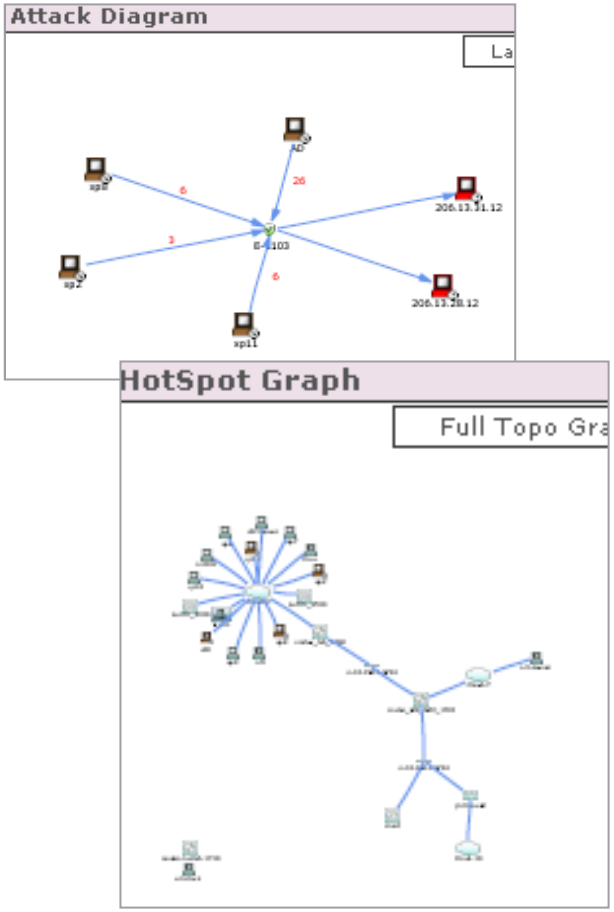
- Inspect traffic with Firewall
- Validate type and protocol compliance of traffic traversing the network
- Block unauthorized application traffic such as peer-to-peer
- Control user commands on applications like IM and FTP



# Network Security Management

**Incident capture and correlation: creates a map of all network traffic and mitigates incidents**

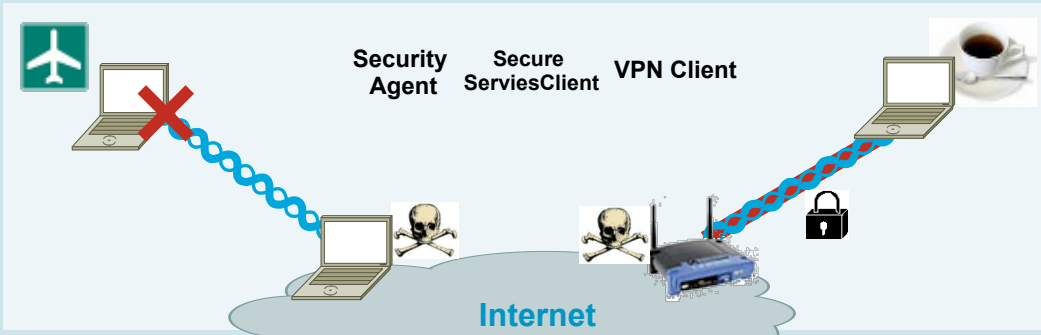
- Vector Analysis
  - –Analyze incidents to determine valid threats
    - •Path analysis
    - •Vulnerability analysis for suspected hosts
    - •Vulnerability scanner correlation
- Correlation
  - –Profile network traffic (NetFlow) and detect anomalies
  - –Correlate events into sessions
  - –Apply correlation rules to sessions to identify incidents



# Summary – Complete Enterprise-class Secure WLAN Network Architecture

Untrusted

Public

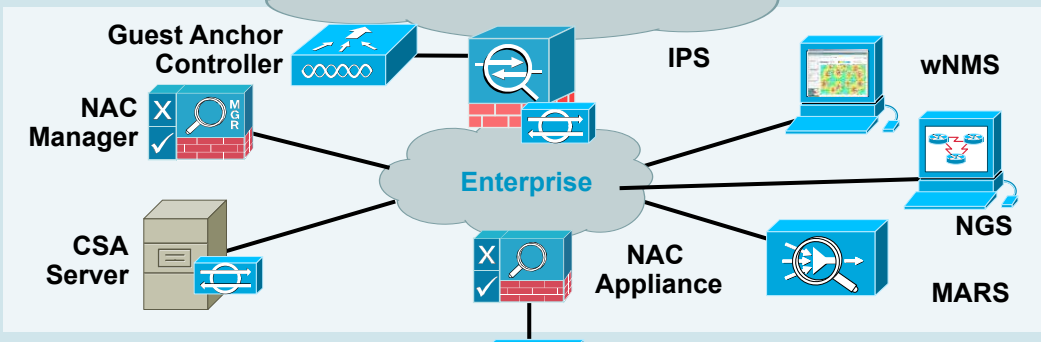



## Endpoint Protection

- Host intrusion prevention
- Endpoint malware mitigation

Trusted

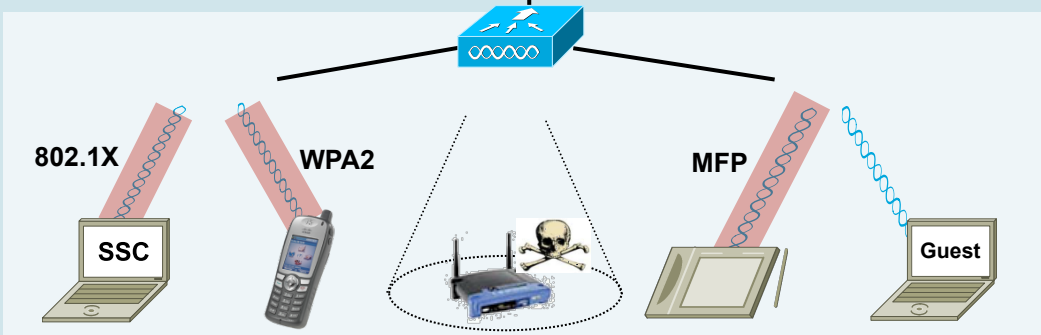
Wired




## Traffic and Access Control

- Device posture assessment
- Dynamic, role-based network access and managed connectivity
- WLAN threat mitigation with IPS/IDS

Wireless




## WLAN Security Fundamentals

- Strong user authentication
- Strong transport encryption
- RF Monitoring
- Secure Guest Access

# Q&A