How to implement WLAN Security Technologies in Enterprise and SME

ARUBA networks

Wireless LAN Risk

Uncontrolled Wireless Devices不受IT監管的無線用品

- Rogue APs非法接入点
- Laptops acting as bridge筆記本作為網橋
- Misconfigured laptops設置錯誤的筆記本
- Ad-Hoc networks隨建即連網路

Attacks against WLAN infrastructure 駭客對無線綱的攻擊

- Denial of Service/flooding分散式阻絕服務程式
- Forged deauthenticate/disassociate偽裝下線包
- Man-in-the-Middle 中間人攻擊
- WEP cracking 破解WEP碼
- WPA-PSK cracking 破解WEP-PSK

Introduction To PCI Compliance

Goal: Prevent Cardholder Data Theft

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 1.2
October 2008

ARUBA networks

PCI Compliance & Wireless付款卡安全性標準與無線網的關係

PCI Security Standards Council

Wireless Is Considered
A Public Network

THE WALL STREET JOURNAL.

FRIDAY, MAY 4, 2007 *Copyright © 2007, Dow Jones & Company, Inc.*

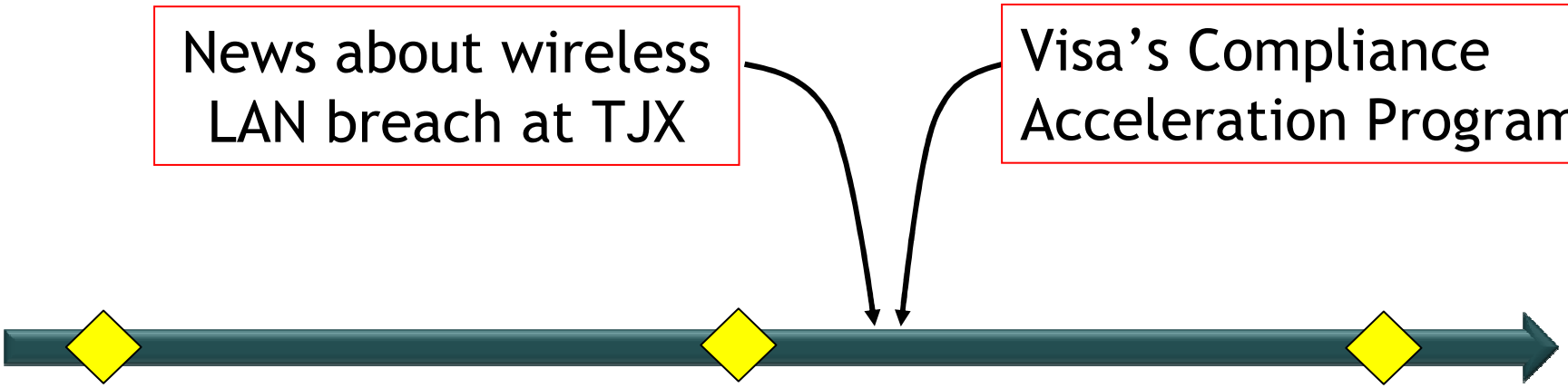
Breaking The Code

How Credit-Card Data Went Out Wireless Door

In Biggest Known Theft, Retailer's Weak Security Lost Millions of Numbers

ARUBA networks

The New PCI DSS Version 1.2



Jan 1, 2005: PCI v1.0

-12 Major requirements
-Defined process
-Enforced by card brands

Jan 1, 2007: PCI v1.1

-Updates and clarifications
-Added requirements for wireless LAN security

Jan 1, 2009: PCI v1.2

-Process clarifications
-Strict requirements for wireless LAN security

Mandatory For All Merchants Worldwide對全球商户一致執行

PCI on Wireless LANs

沒有用WiFi	在用WiFi	用WiFi POS
		
Category 1	**Category 2**	**Category 3**

PCI v1.2 Requirements & Wireless LANs

Wireless LAN Is Considered
A Public Network

7.2: Role-based Access
10: Monitor Access

1.1.2: Inventory WLAN
1.2.3: Firewall WLAN
2.1.1: Don't Use Defaults
2.2: Standard Config
4.1.1: Better Than WEP
6.1: Get latest patches
9.1.3: Physical Security

1.1.2: Inventory WLAN
1.2.3: Firewall WLAN
2.1.1: Don't Use Defaults
2.2: Standard Config
4.1.1: Better Than WEP
6.1: Get latest patches
9.1.3: Physical Security

11.1: Wireless IDS/IPS

11.1: Wireless IDS/IPS

11.1: Wireless IDS/IPS

Category 1

沒有用 WLAN

Category 2

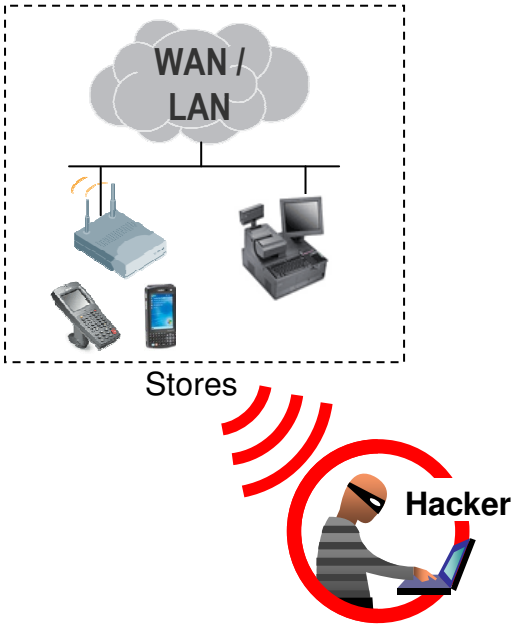
沒有卡用户資料傳送

Category 3

卡用户資料以
WLAN 傳送

Wireless Threat #1: War-Driving

- Wireless attacks are opportunistic
  - Wardriving to identify vulnerable, interesting targets
- Passive monitoring reveal sensitive information
  - Usernames, passwords, SNMP community strings, default SSID's
- WEP & WPA-PSK have been compromised
- Hence Requirement 1.1, 1.2.3, 2.1 & 4.1.1



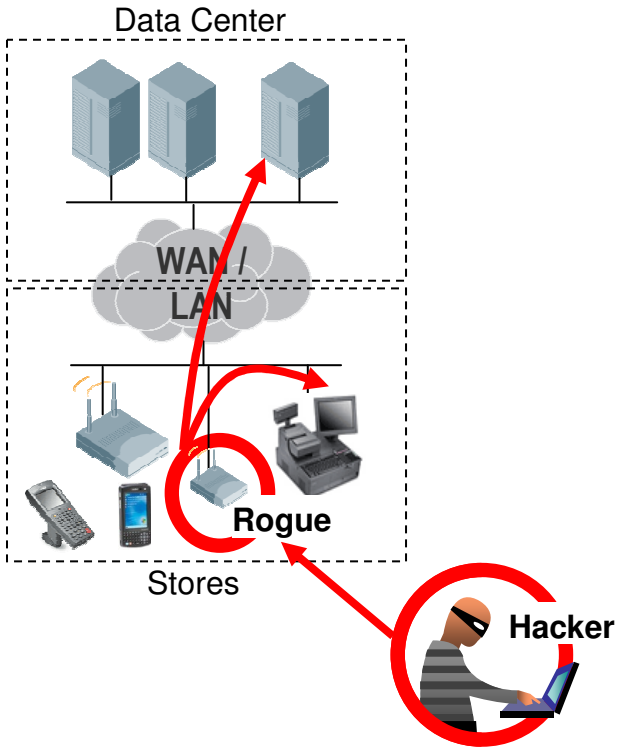
OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, and DSW were also the victims of crime rings that used unprotected wireless networks as their points of entry.

http://www.darkreading.com/document.asp?doc_id=160888

ARUBA networks

Wireless Threat #2: Accidental Wireless LAN

- Employees may introduce rogue AP's to your wired LAN
  - SOHO devices
  - Extends your network to your parking lot
- Rogue devices can be malicious
- PCI Requirement 11 For “Monitoring”

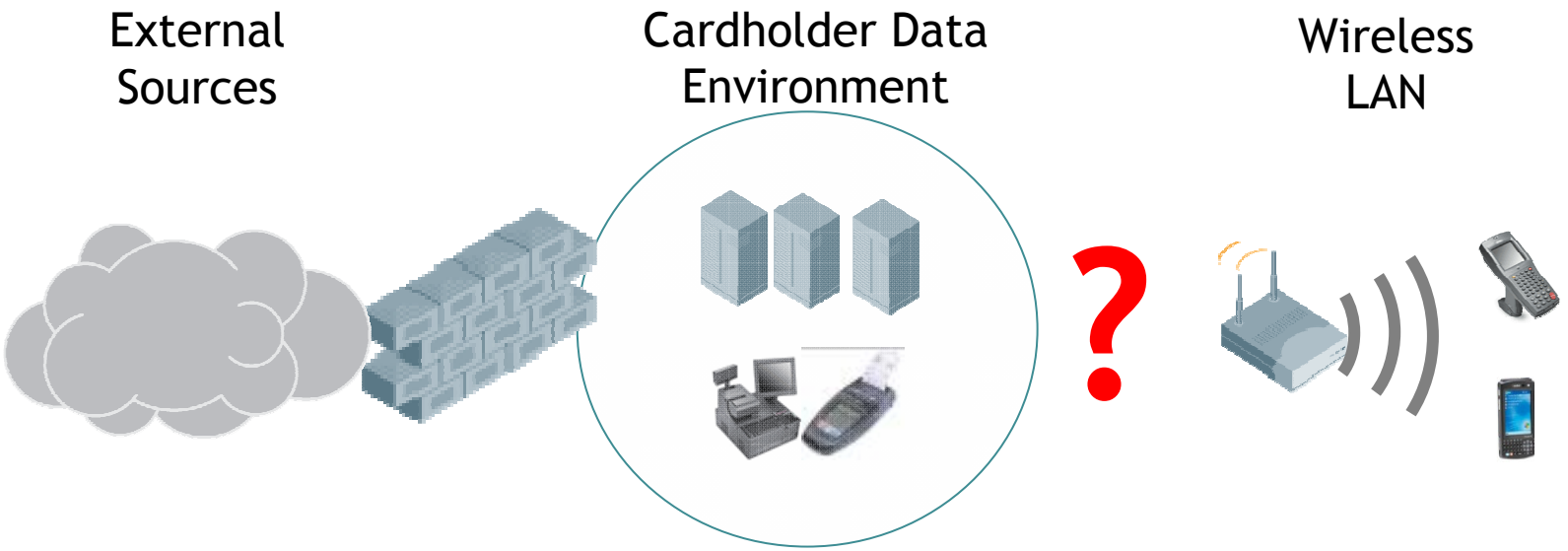


"We recently suffered an intrusion attempt on our internal network. We traced the source back to an unauthorized wireless router plugged into a live but unused network jack in a barely-accessible location. We have suspicion, but not actual certainty, that the router was placed by the same intruder as executed the network attacks."

http://www.securityfocus.com/archive/75/374672

ARUBA networks

Requirement 1.2.3: Firewall For WLAN



- Wireless LAN is considered a public network
- Wireless LAN must be segmented with a Firewall
- Firewall must do “stateful” inspection
- Firewall must deny all traffic from wireless LAN
  - Unless required for business purposes

Requirement 4.1.1: Encrypt Wireless

- Applies to all wireless networks **whether or not** they transmit cardholder data
- Starting Mar'09 for new networks
- Starting Jun'10 for existing networks

Option 1

Replace all legacy hardware in use

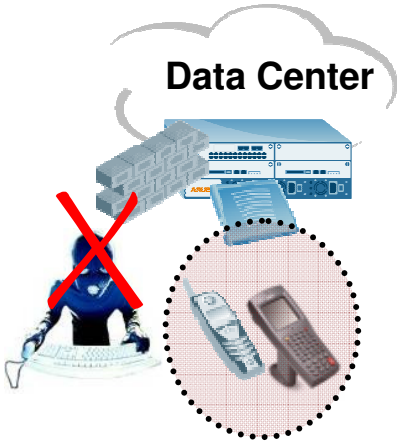
Upgrade new hardware in use

Replace Every WEP Device

Option 2

Per-User-Firewall sits between WEP devices & data center

Firewall Blacklists Unauthorized Users & Intruders

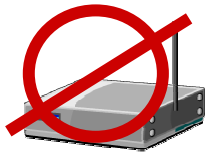


Make Every WEP Device Out-of-Scope

ARUBA networks

Requirement 11.1: Monitor All Wireless Devices

Goal: Detect& Locate:



Rogue Devices

Accidental Connections

Policy Violations

Two Options

Manual

Handheld Analyzer

Walk-around every site, once a quarter

Automatic

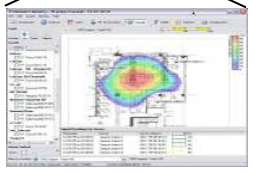
Wireless IDS

Sensor

At every site

Server

In Data Center



ARUBA networks

PCI v1.2 & Wireless Summary

Get The Facts

- Wireless LAN security is needed even if no wireless LANs are in use
- PCI compliance doesn't require rip & replace existing networks
- PCI is a NOT-IF-BUT-HOW problem

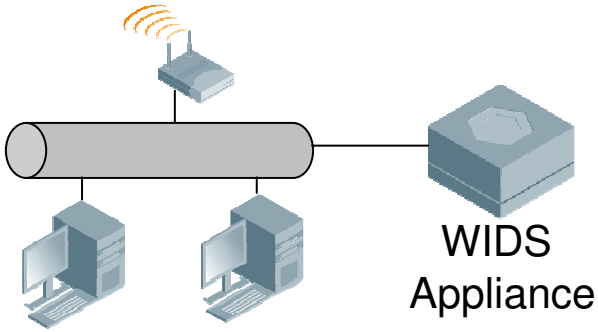
PCI Doesn't Have To Break The Bank

- Look for overlay security solutions to fill gaps & protect investments
- Look for new all-in-one solutions that can replace legacy networks
- Quantify positive side-effects of upgrading

ARUBA networks

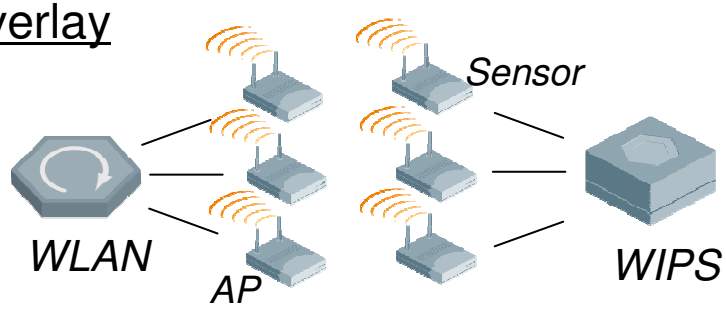
Categories of WIP Systems

Wired



- No wireless sensors
- Scanning performed from wired network
- Good for rogue AP detection
- Does not detect wireless attacks

Overlay

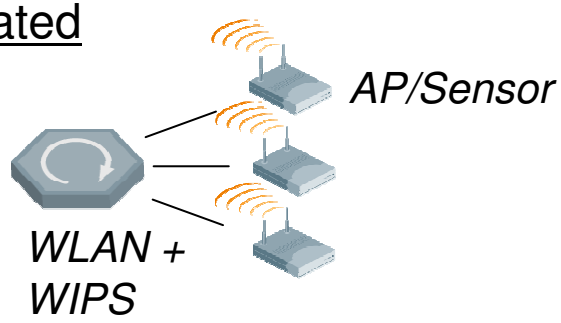


- Infrastructure-independent
- Dedicated sensors
- No visibility into encrypted traffic
- Dedicated WIP console

On-Demand

- Portable
- Conduct scans as-needed
- No installation required
- Does not provide continuous monitoring

Integrated



- WIP is a feature of the WLAN infrastructure
- Sensors/APs can be interchangable
- Single management console for all wireless
- Visibility into encrypted traffic

ARUBA networks

Dedicated/Hybrid Sensors

Use dedicated sensors? You decide.

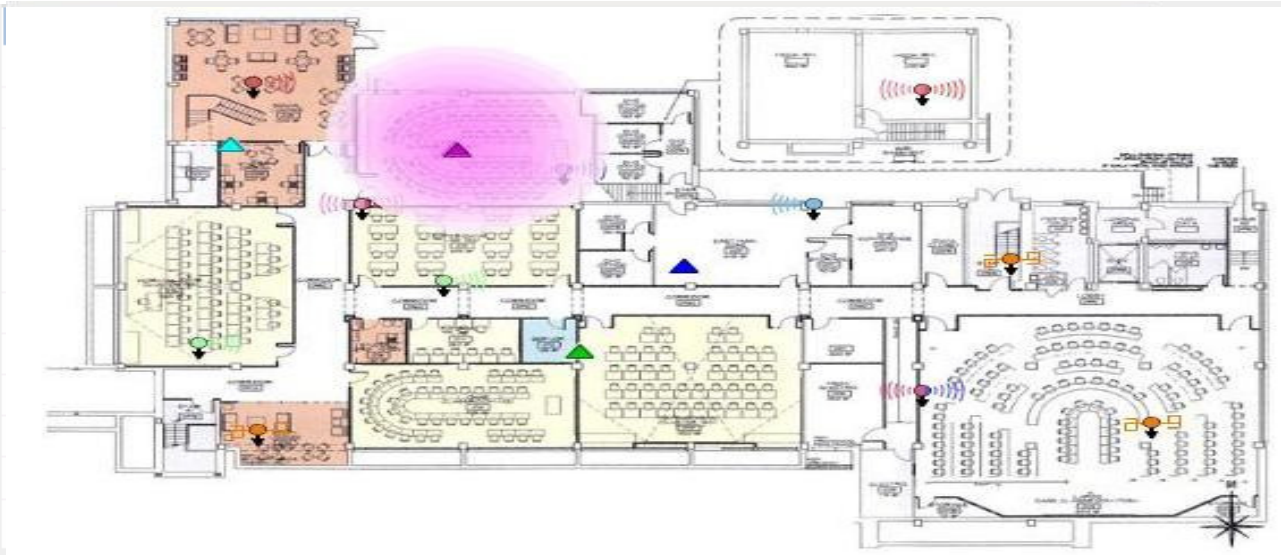
Dedicated Sensors

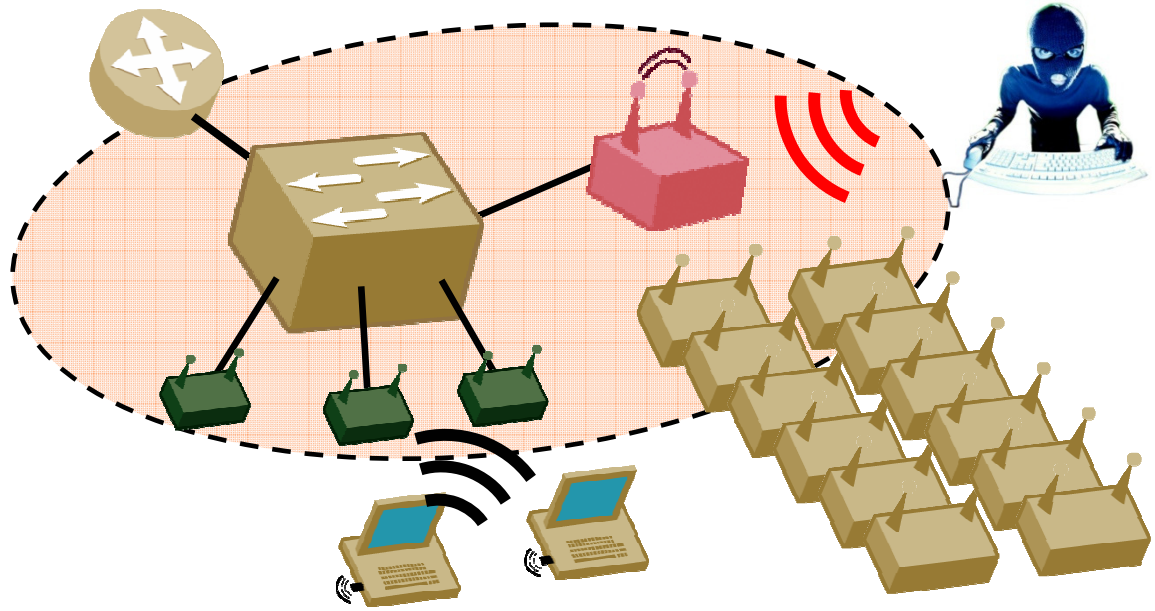
- Sensors are single-purpose devices – only scan
- No performance impact on WLAN traffic
- More reliable containment
- Use when high visibility is required

Hybrid AP/Sensor

- Dual-purpose: WLAN access and WIP scanning
- Tradeoff between WLAN performance and WIP visibility
- Containment is second priority to WLAN service
- Use when cost is an issue

Auto Rogue AP Management

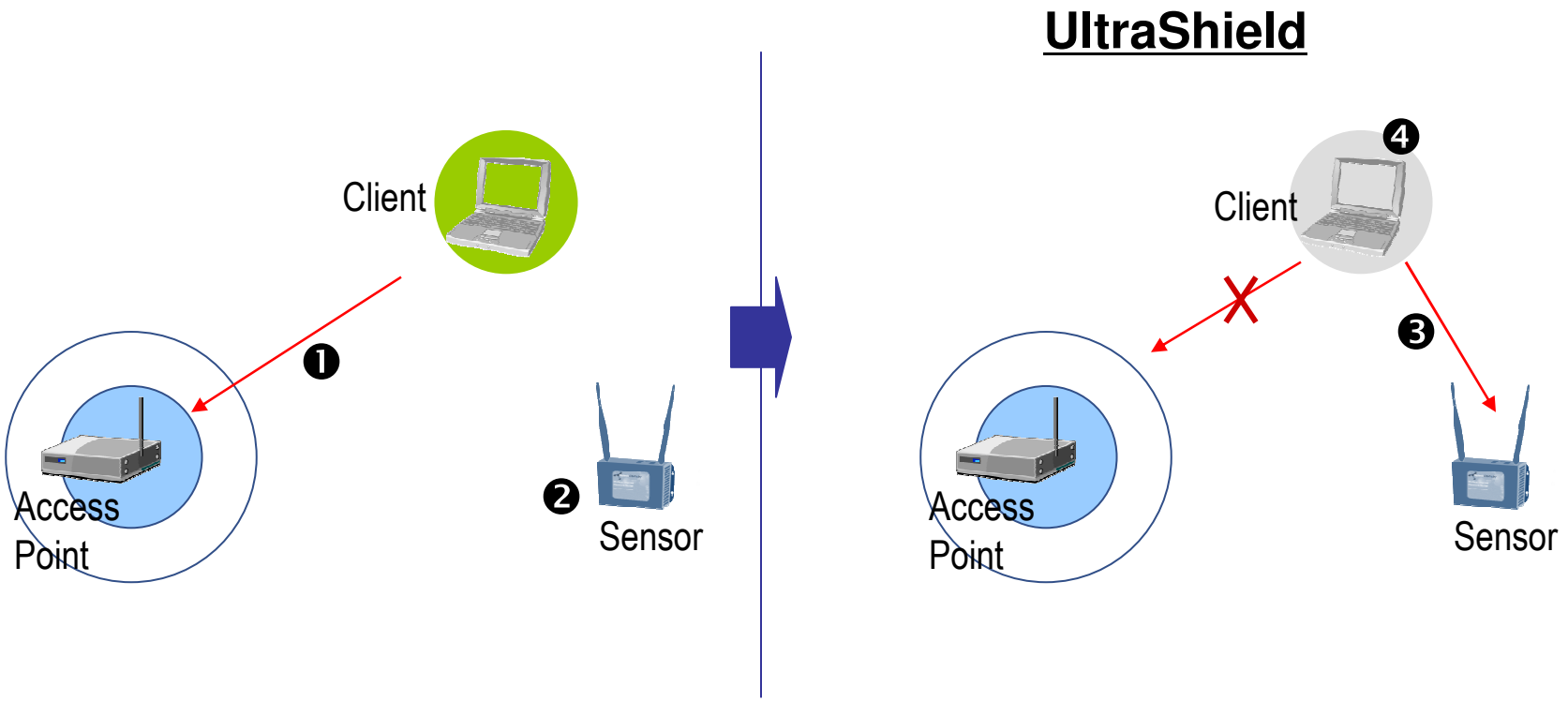




1. **AP detection**
   - See all APs
2. **AP classification**
   - Are they neighbors?
   - Or are they a threat?
3. **Rogue containment**
   - Stop users from accessing rogue APs over the wire & over wireless
   - Leave neighbors alone
4. **Locate Rogue**
   - Find where it is and disconnect

ARUBA networks

Client Tarpit



❶ Client is trying to associate to AP (rogue or authorized)

❷ Sensor creates tarpit and steers client to tarpit instead of AP

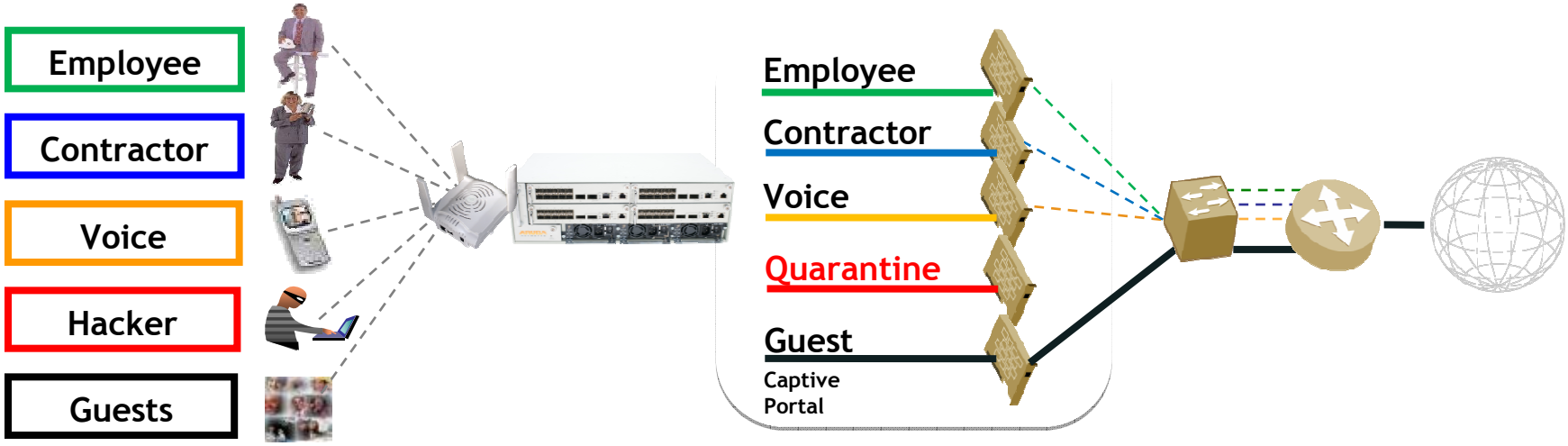
❸ Client associates to Sensor tarpit in preference to AP

❹ Once client thinks it is associated to AP it stops association attempts

Shield *multiple* rogues on *multiple* channels simultaneously

Identity-Based Security

- Network access rights by user identity, *not* by port
- Integrated ICSA stateful firewall
- Seamless NAC integration
- Integrated Wireless Intrusion Detection Services



Prevent security breaches and meet compliance needs

ARUBA networks

Workplace Situation

Applications are Centralizing

Data • Voice • Video

Users & Devices are Distributing

Branch • Telework
Continuity • Partners

What is the best network solution?

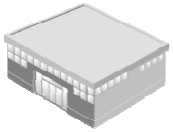
ARUBA networks

Client VPN Solves The Mobile Worker

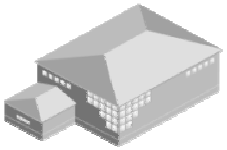
Mobile Worker

Occasional Telecommuter

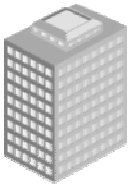
Work At home



"Micro" Branch



Small Branch



Medium Branch

VPN

- ✓ Centralized
- ✓ Per-user control
- ✓ Strong security
- ✓ "Transport independent"
- ✓ Low-cost & easy to deploy

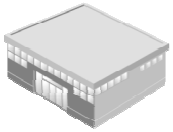
ARUBA networks

What About Branch Office Needs?

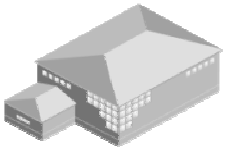
Mobile Worker

Occasional Telecommuter

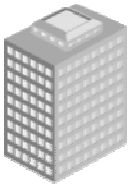
Work At home



"Micro" Branch



Small Branch



Medium Branch

VPN

"Outside" network experience

- Single user
- Data-only access
- Device-dependent
- User-initiated sessions
- Software

"Inside" network experience

- Multiple users
- Data+Voice+Video
- Multiple devices
- "Always On"
- Infrastructure

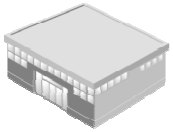
ARUBA networks

The Traditional Branch Solution

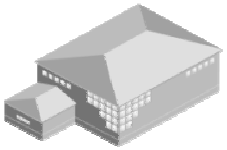
Mobile Worker

Occasional Telecommuter

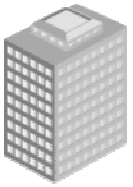
Work At home



"Micro" Branch



Small Branch



Medium Branch

Router/VPN Firewalls

IT must trade off **cost and complexity** against **functionality and security**

- Complex features
- Subnet/port policy model
- Static configurations
- 1st-generation wireless
- Piecemeal management

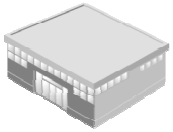
ARUBA networks

Solution: Virtual BRANCH Networks

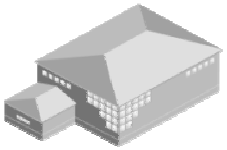
Mobile Worker

Occasional Telecommuter

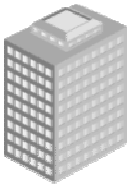
Work At home



"Micro" Branch



Small Branch



Medium Branch

VPN

VBN

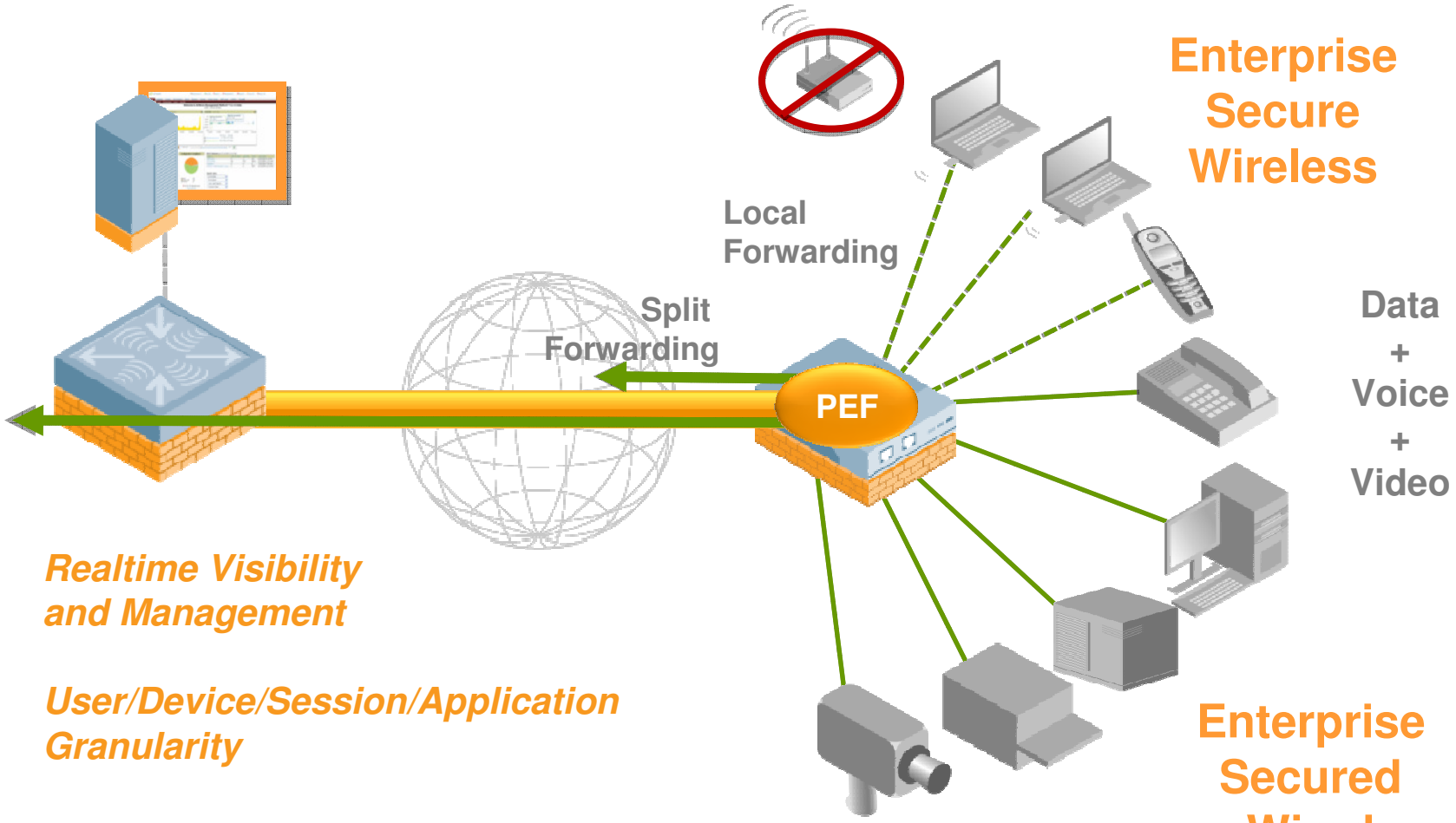
- ✓ Centralized
- ✓ Per-user control
- ✓ Strong security
- ✓ "Transport independent"
- ✓ Low Cost & easy to deploy

*VPN "**Plus**" for the Branch*

ARUBA networks

No Compromise Functionality

Centralized/Virtualized + Policy Enforcement + Site Connectivity

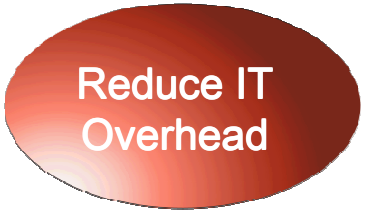


ARUBA networks

Why Companies Choose Aruba?

- No additional security products: Integrated Firewall + WIP
- Secures legacy devices & wired networks

- Overlay architecture preserves existing investments
- Eliminate wiring with Secure Enterprise Mesh



- Delivers over-the-air Service Level Agreements
- One console to manage stores, DC & corporate offices
- Comprehensive reporting & help-desk capabilities

- Voice, video & RFID applications on the same network
- Security & QoS segmentation

ARUBA networks

www.arubanetworks.com
dennylo@arubanetworks.com

ARUBA networks