MOJO AirTight WIPS

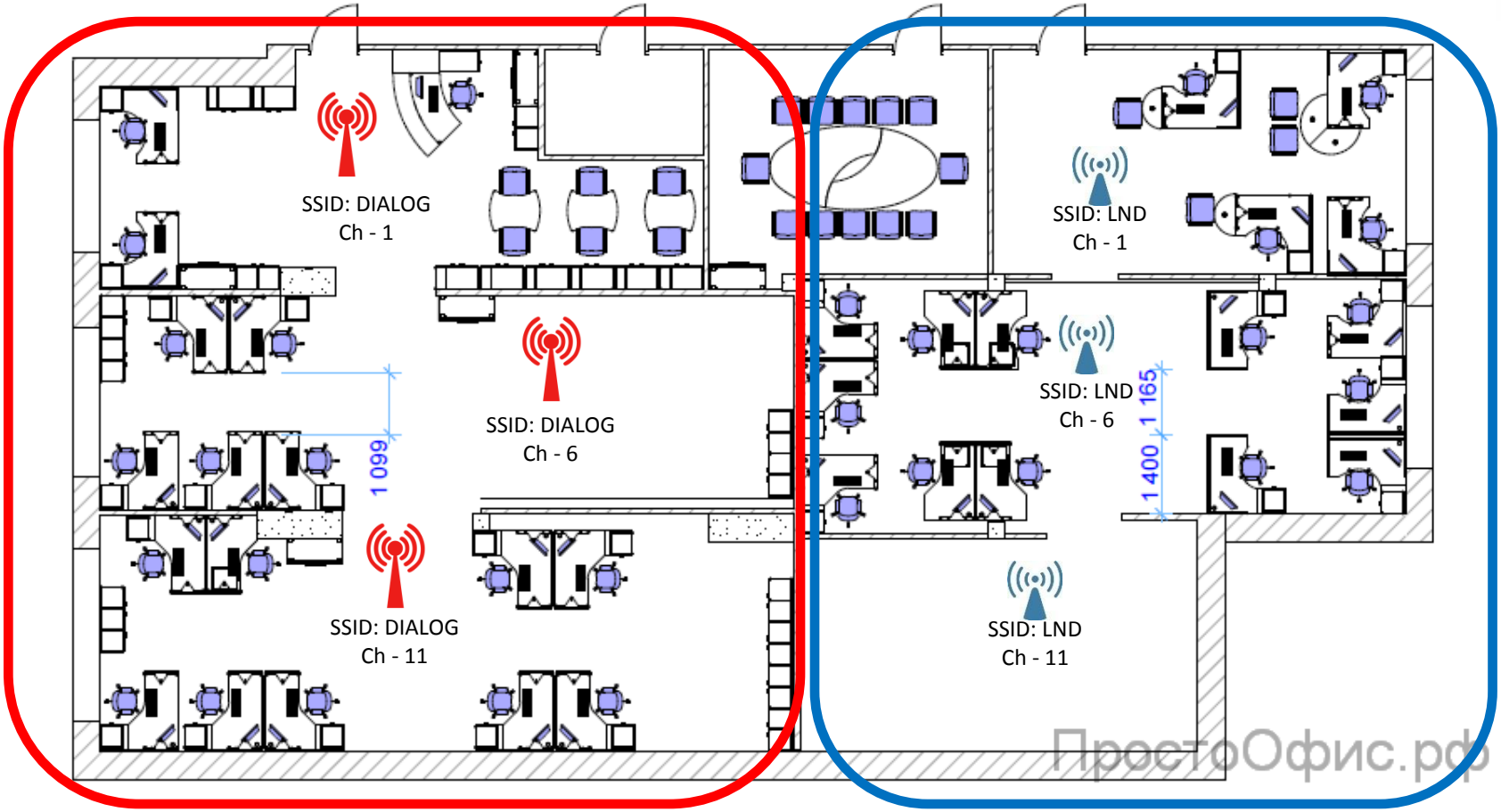
Система Предотвращения Вторжений для беспроводных сетей

План презентации

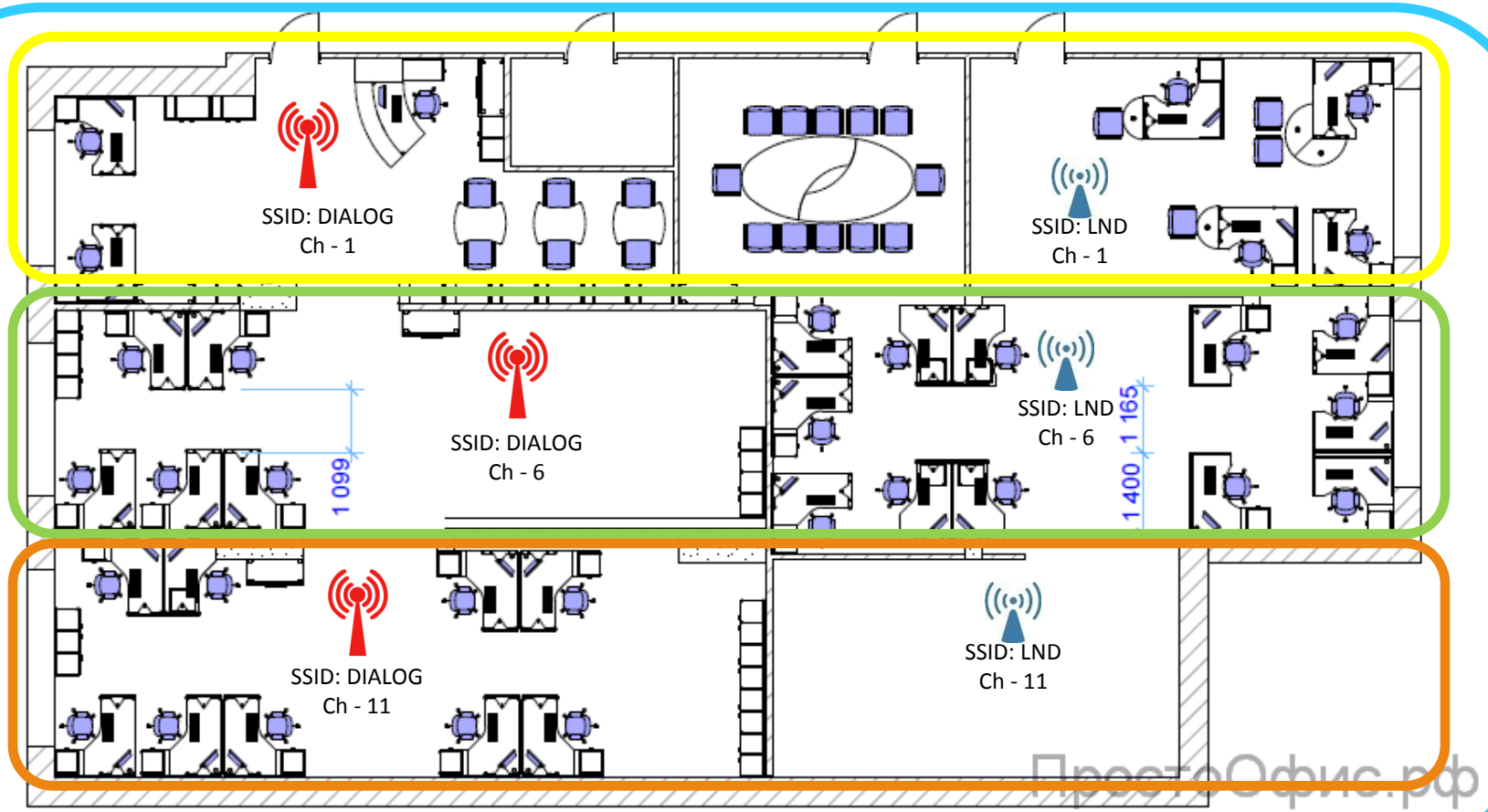
1. Особенности среды передачи беспроводных сетей
2. Типы атак на беспроводные сети
3. Основные задачи выполняемые WIPS
4. Обзор и сравнение различных реализаций WIPS
5. Обзор возможностей WIPS MOJO Networks
6. Виды реализаций WIPS MOJO Networks: on-sight / cloud
7. Обсуждение, вопросы, ответы…

Особенности среды передачи беспроводных сетей

Особенности среды передачи беспроводных сетей



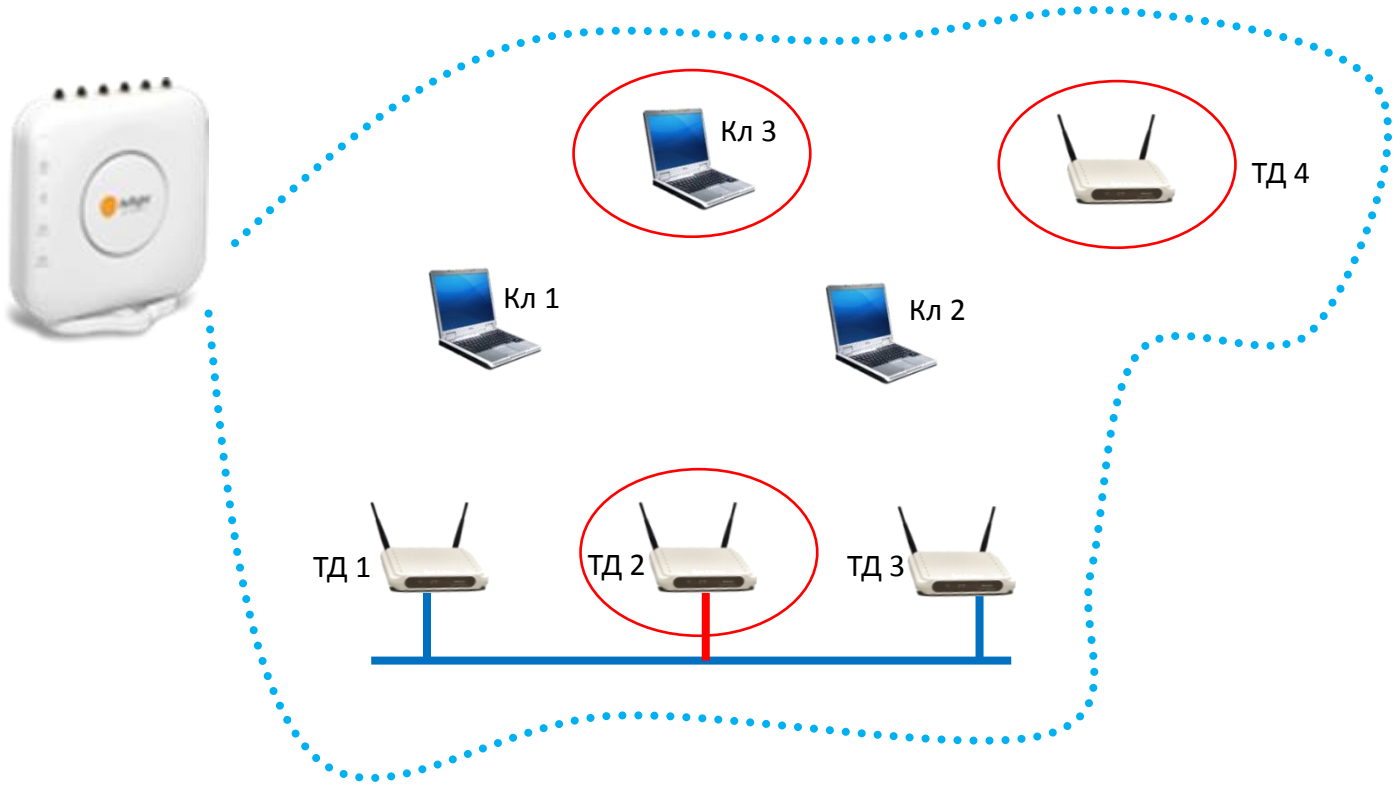
Особенности среды передачи беспроводных сетей



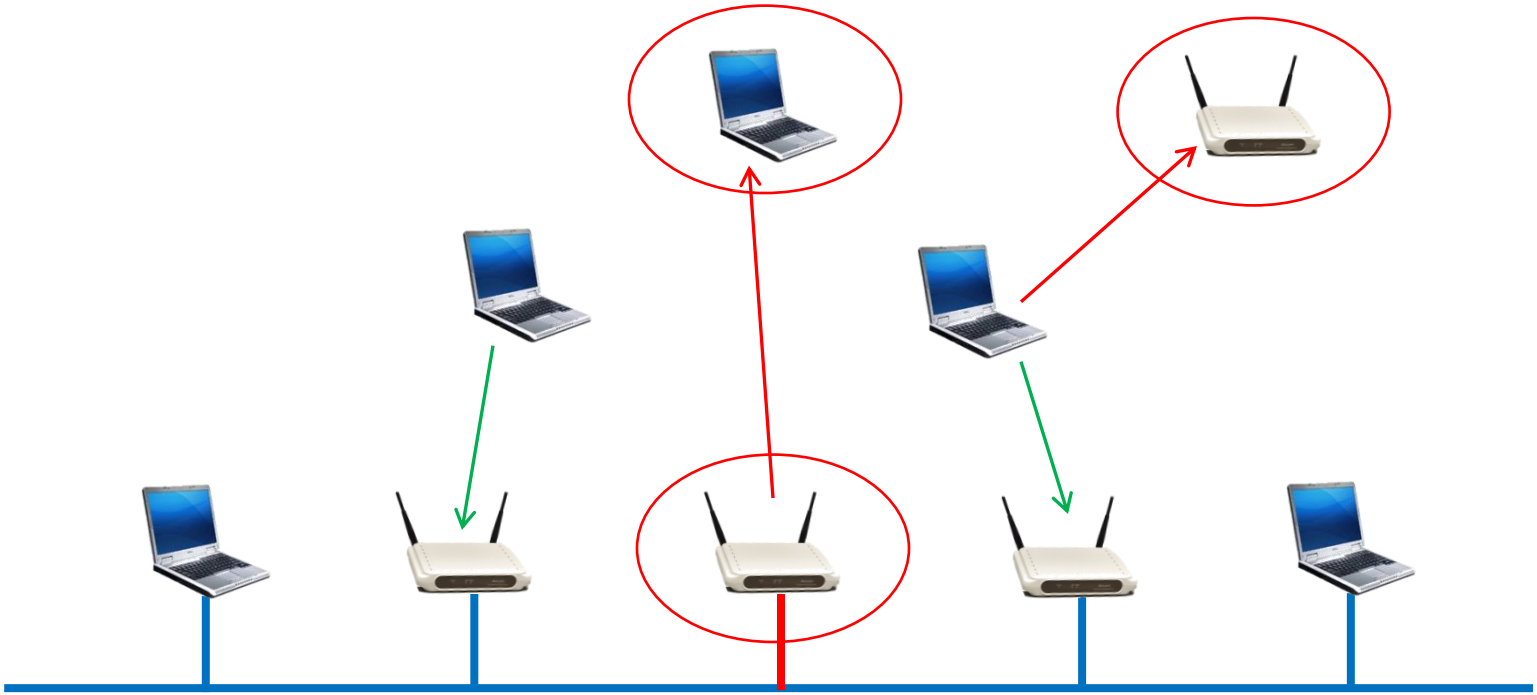
Особенности среды передачи беспроводных сетей

1. Разделяемая среда – доступная всем
   - Любое устройство имеет право получить доступ к среде передачи
   - Все устройства обязаны соблюдать протокол 802.11
   - Все устройства на данном канале должны договариваться об очередности работы в канале
1. Полудуплексный режим передачи – в данный момент времени только одно устройство может вести передачу
   - Один говорит – все слушают

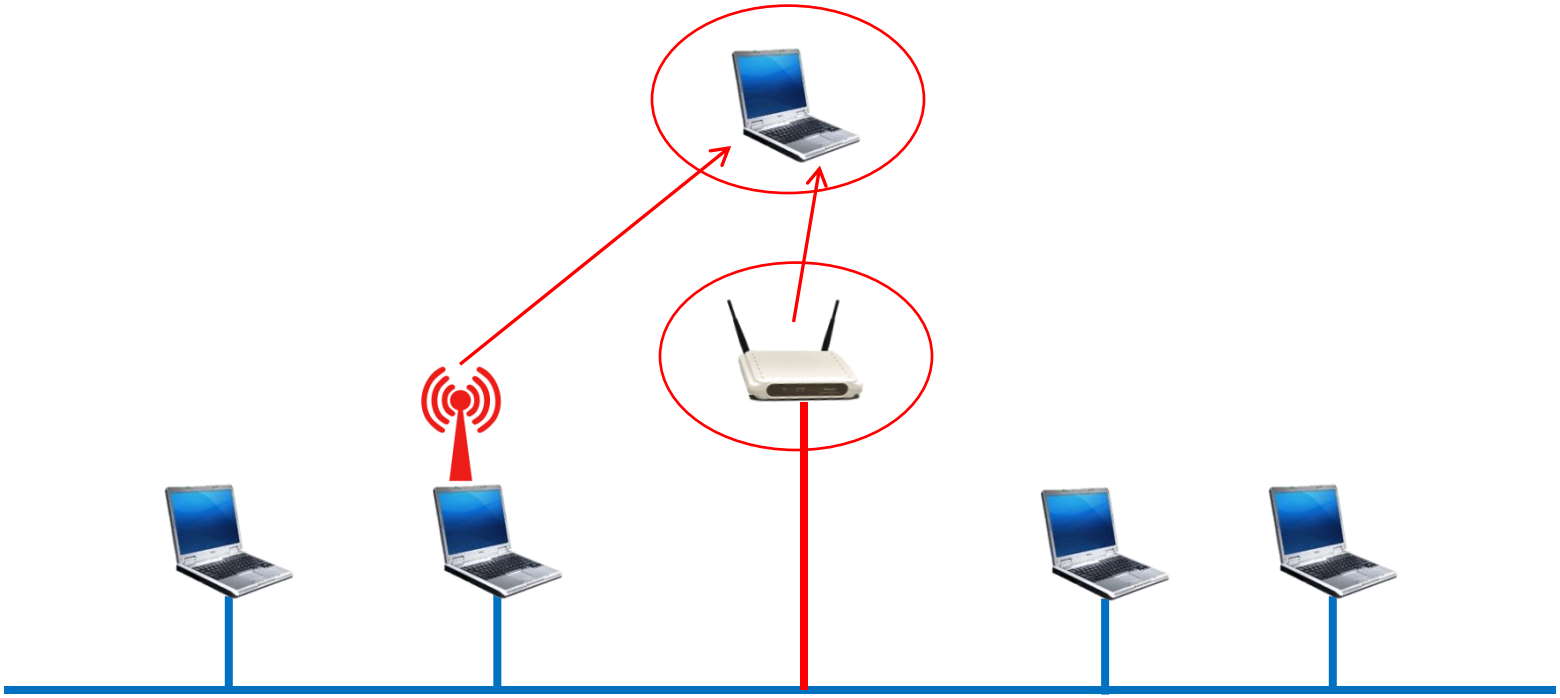
Wi-Fi устройства с точки зрения сенсора



Случай для сетей с разрешенным Wi-Fi



Случай для сетей с запрещенным Wi-Fi

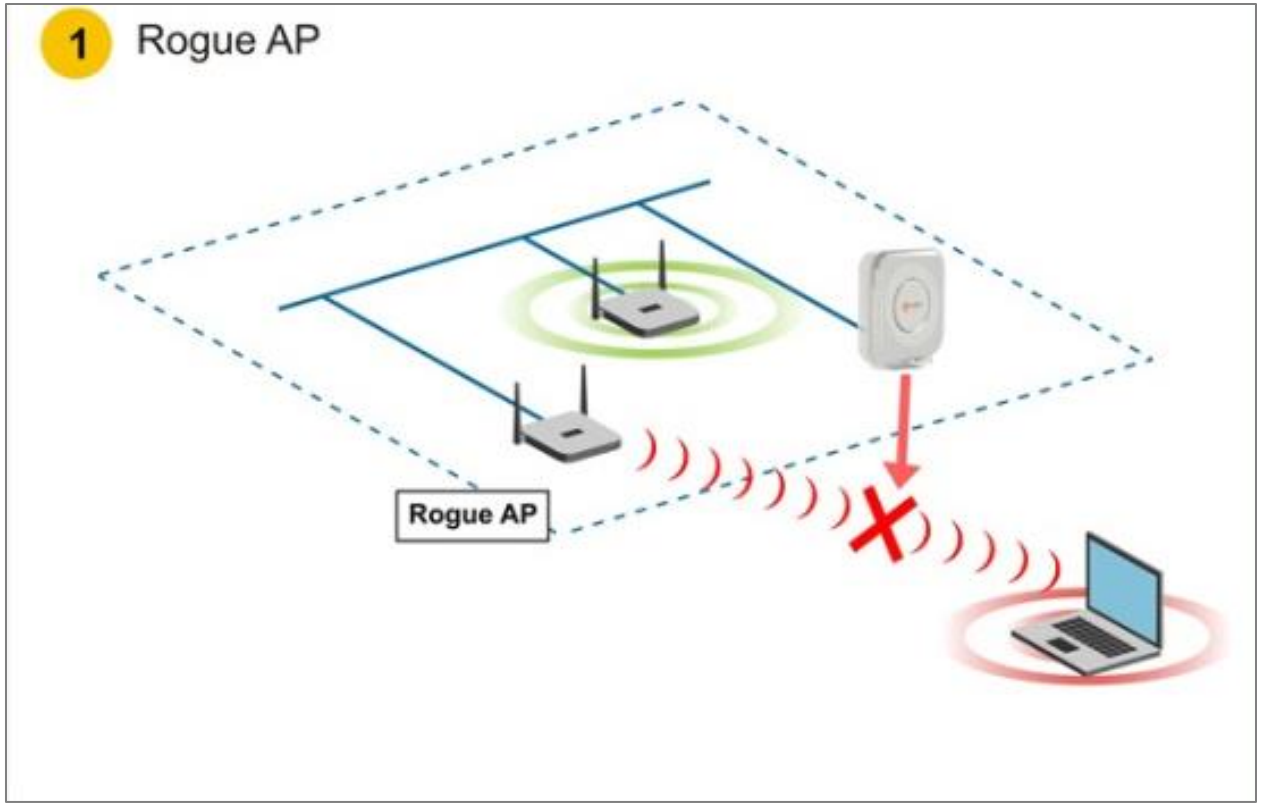


Сегмент с запрещенным Wi-Fi

Типы атак на беспроводные сети

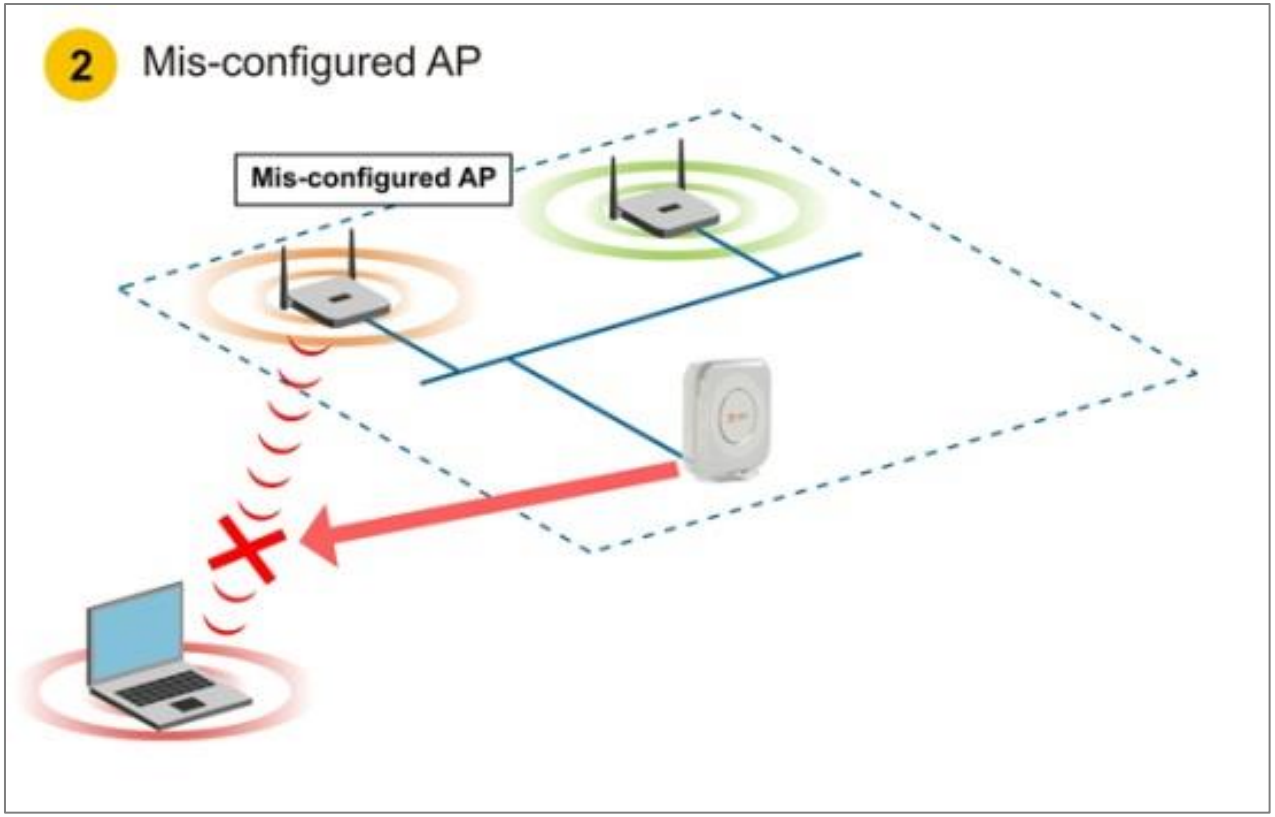
Типы атак на беспроводные сети

- Неавторизованные ТД



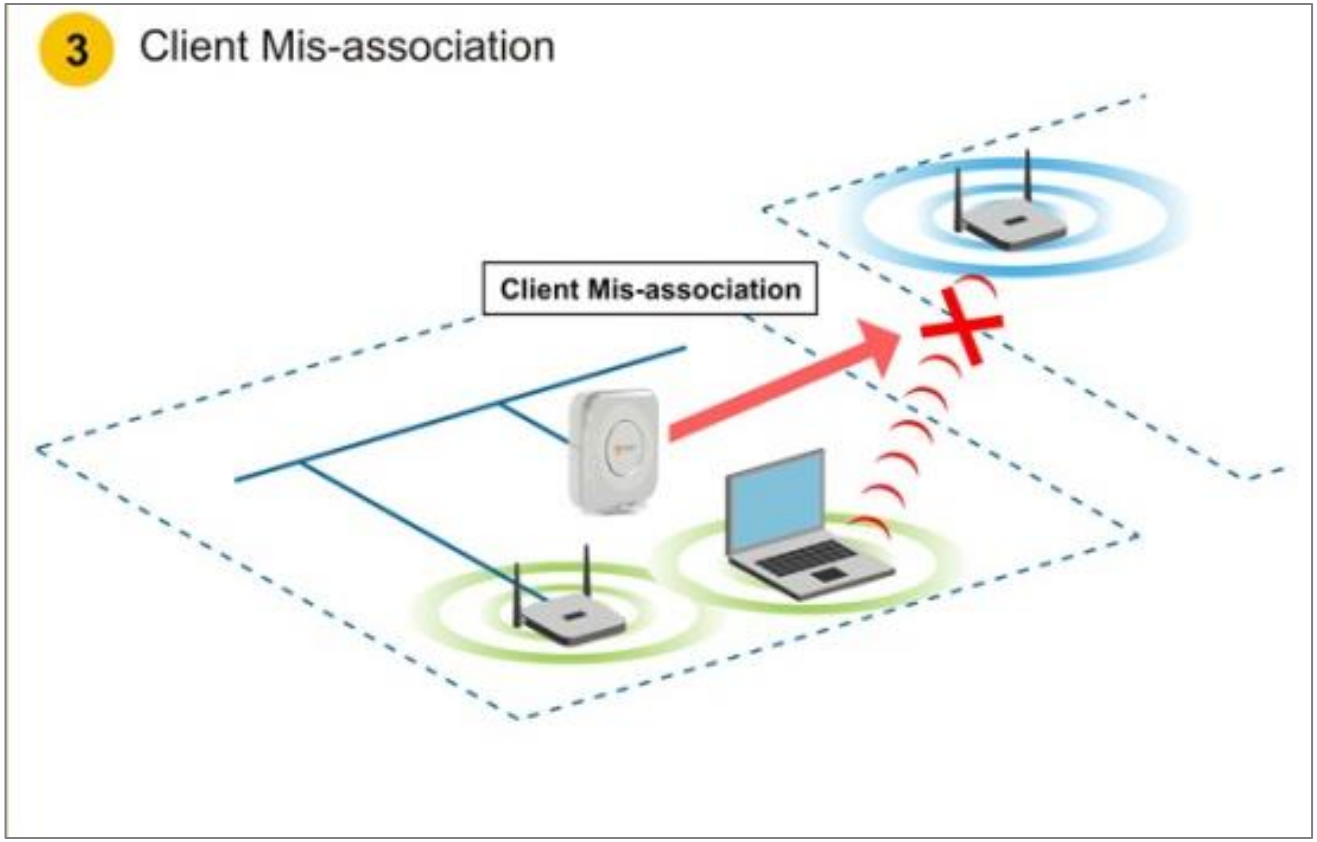
Типы атак на беспроводные сети

- Нарушение настроек ТД



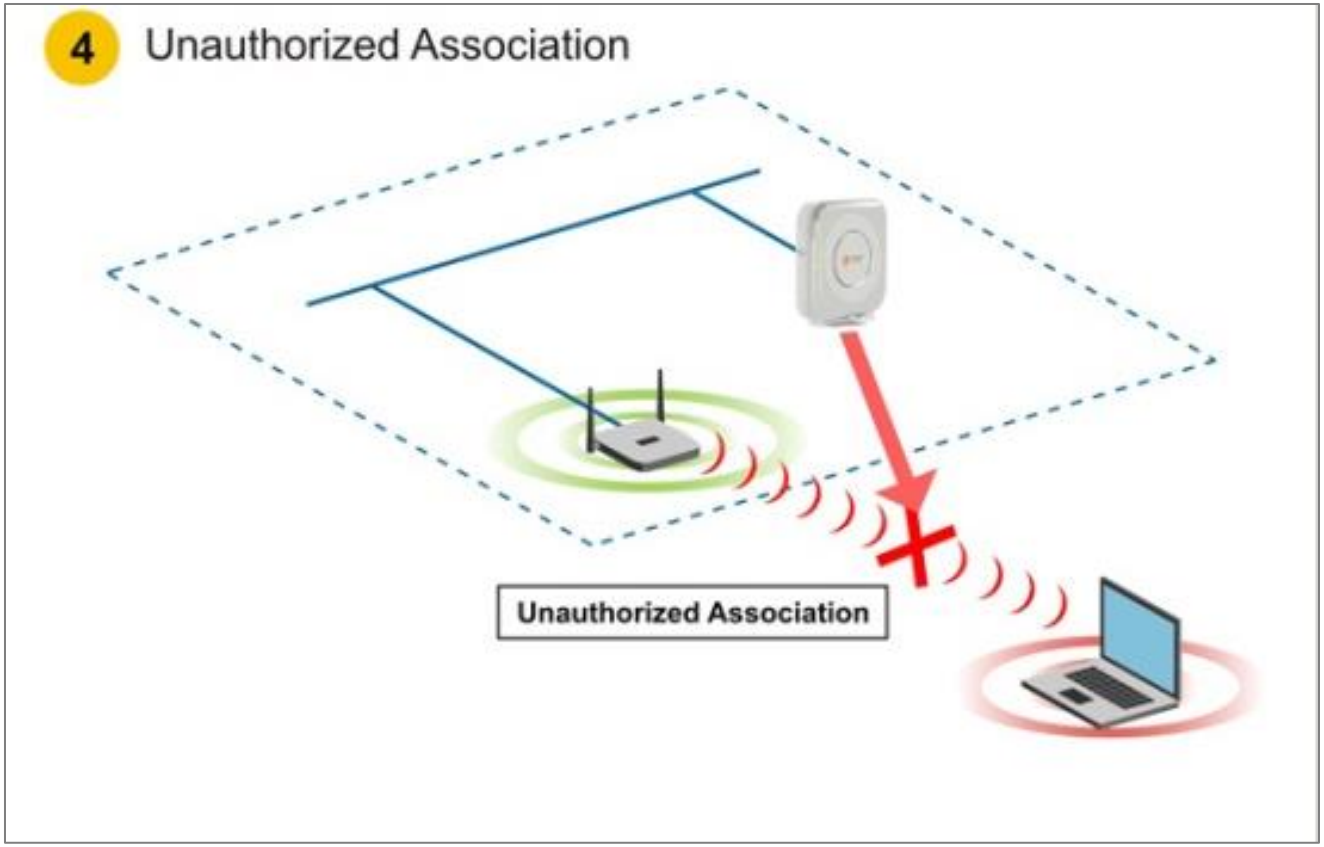
Типы атак на беспроводные сети

- Подключение клиента к неавторизованной ТД



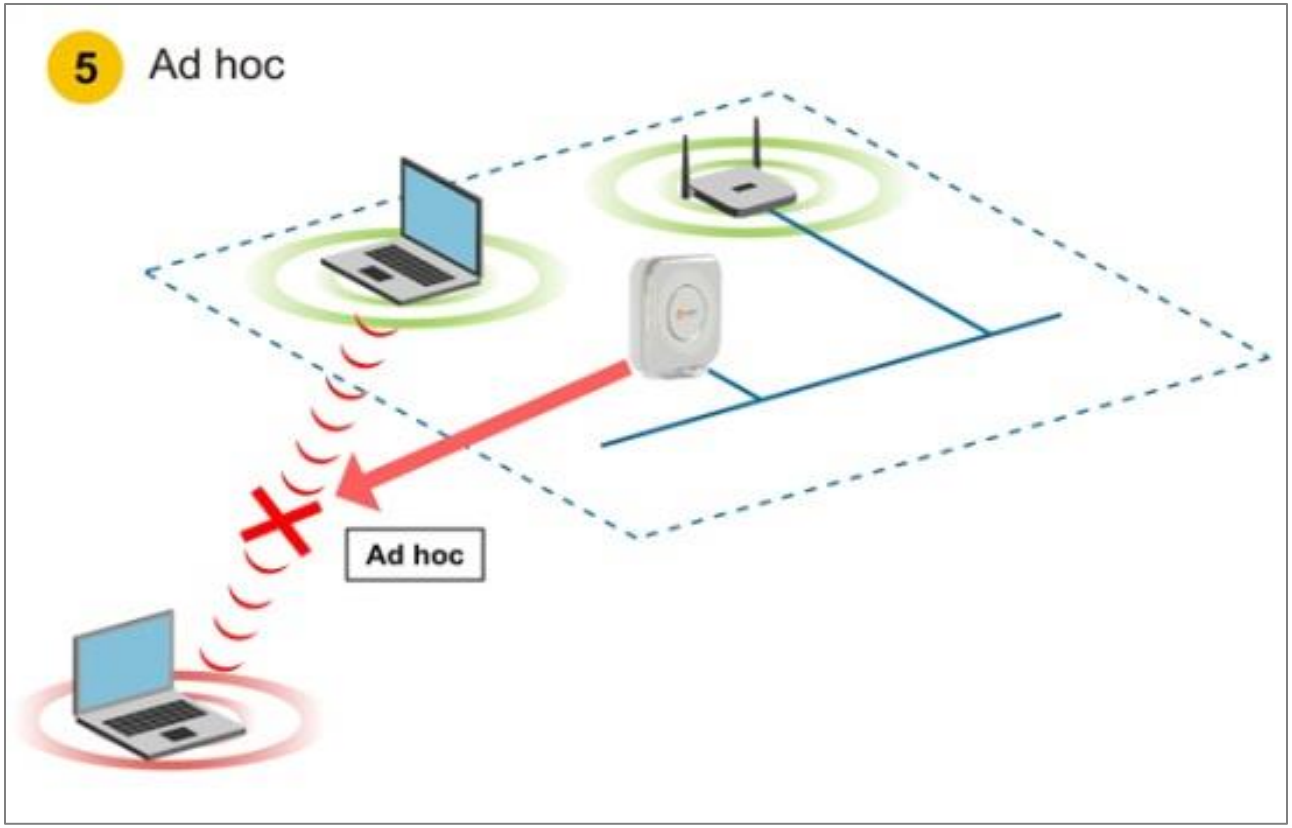
Типы атак на беспроводные сети

- Подключение неавторизованного клиента



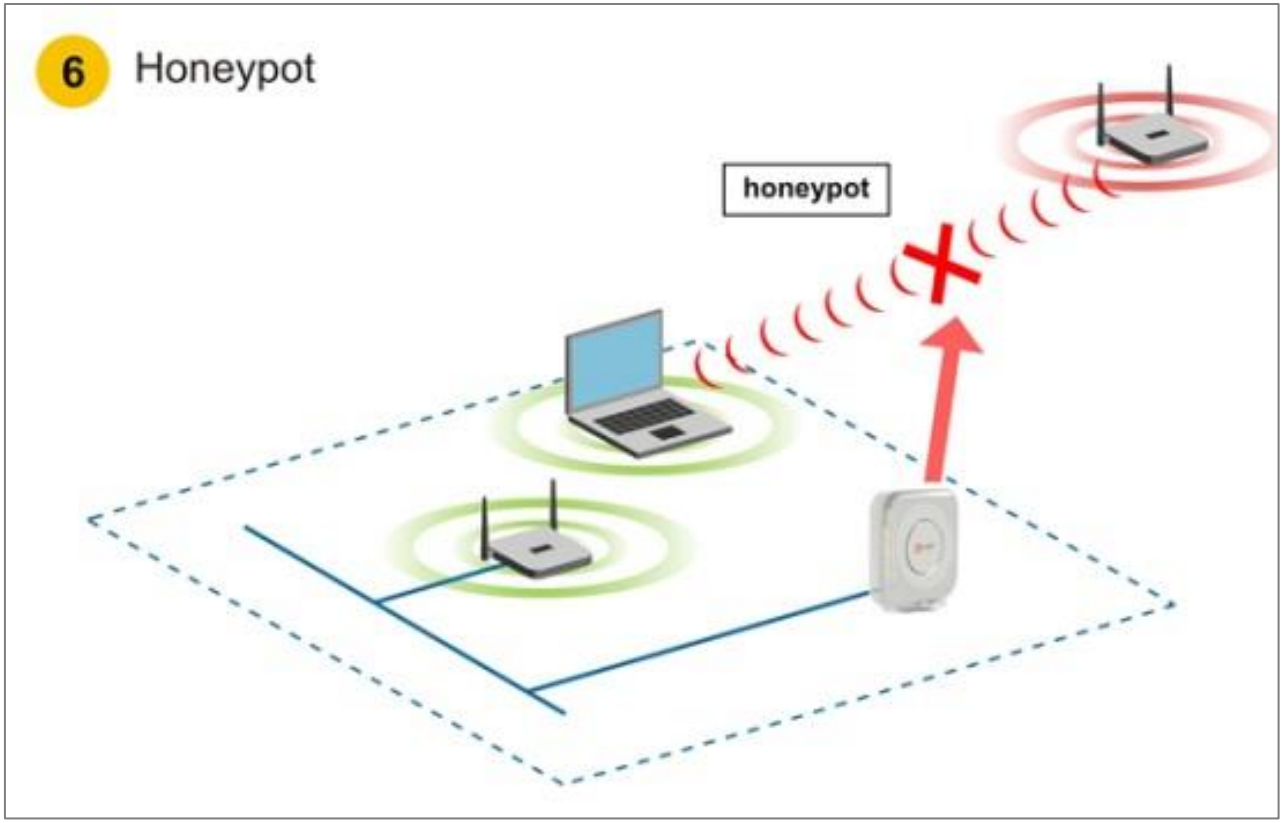
Типы атак на беспроводные сети

- Одноранговые соединения



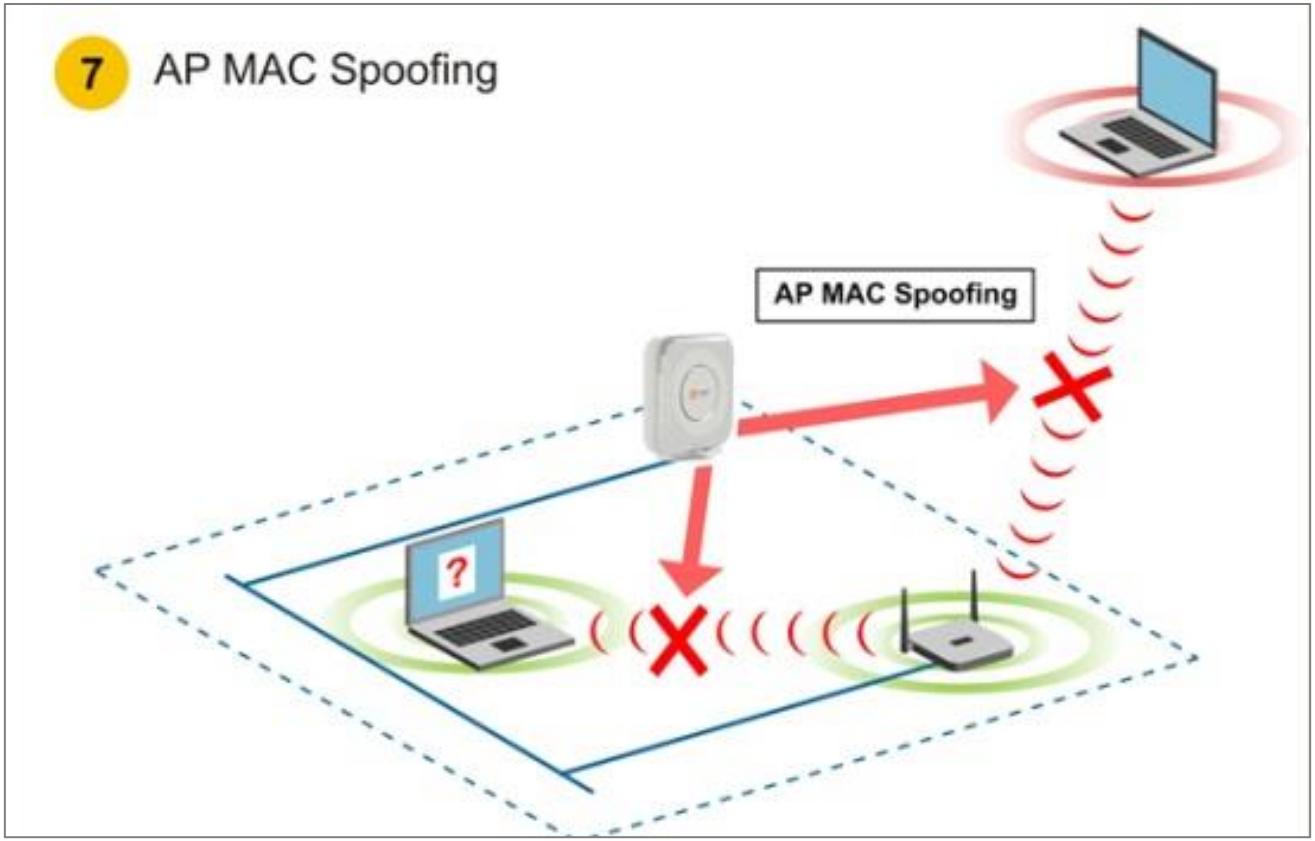
Типы атак на беспроводные сети

- Имитация авторизованных ТД



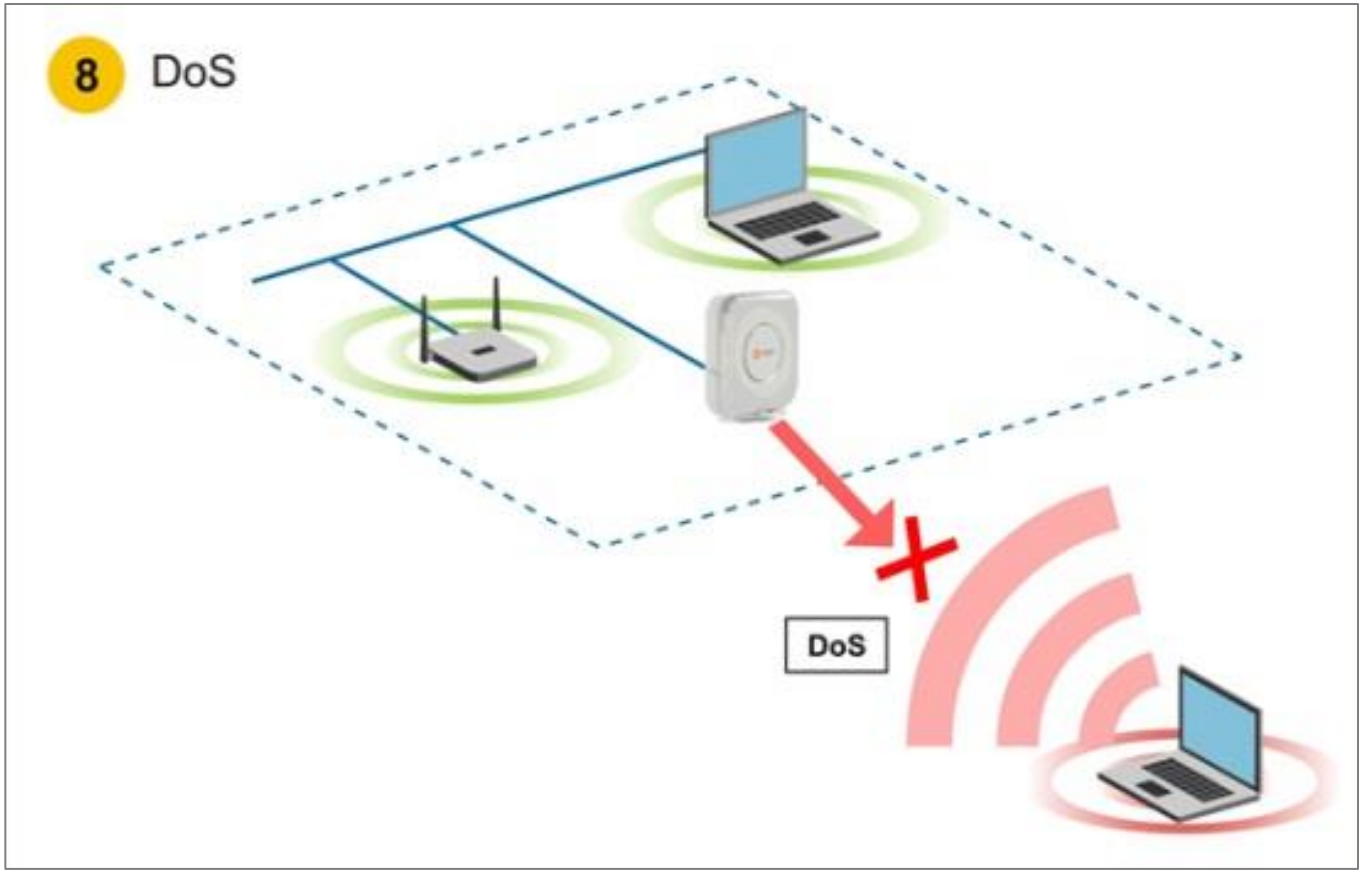
Типы атак на беспроводные сети

- MAC Spoofing



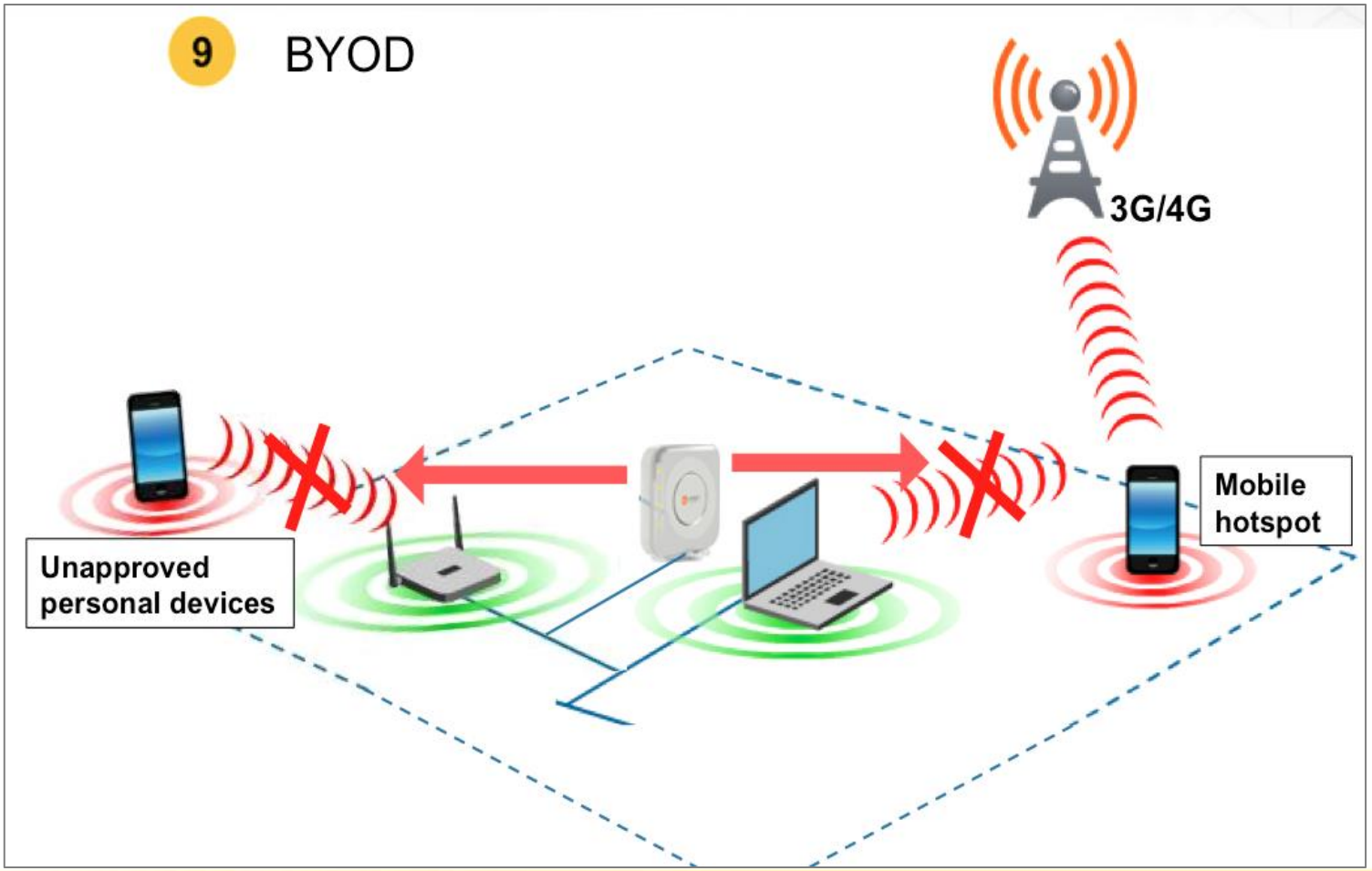
Типы атак на беспроводные сети

- DoS атаки



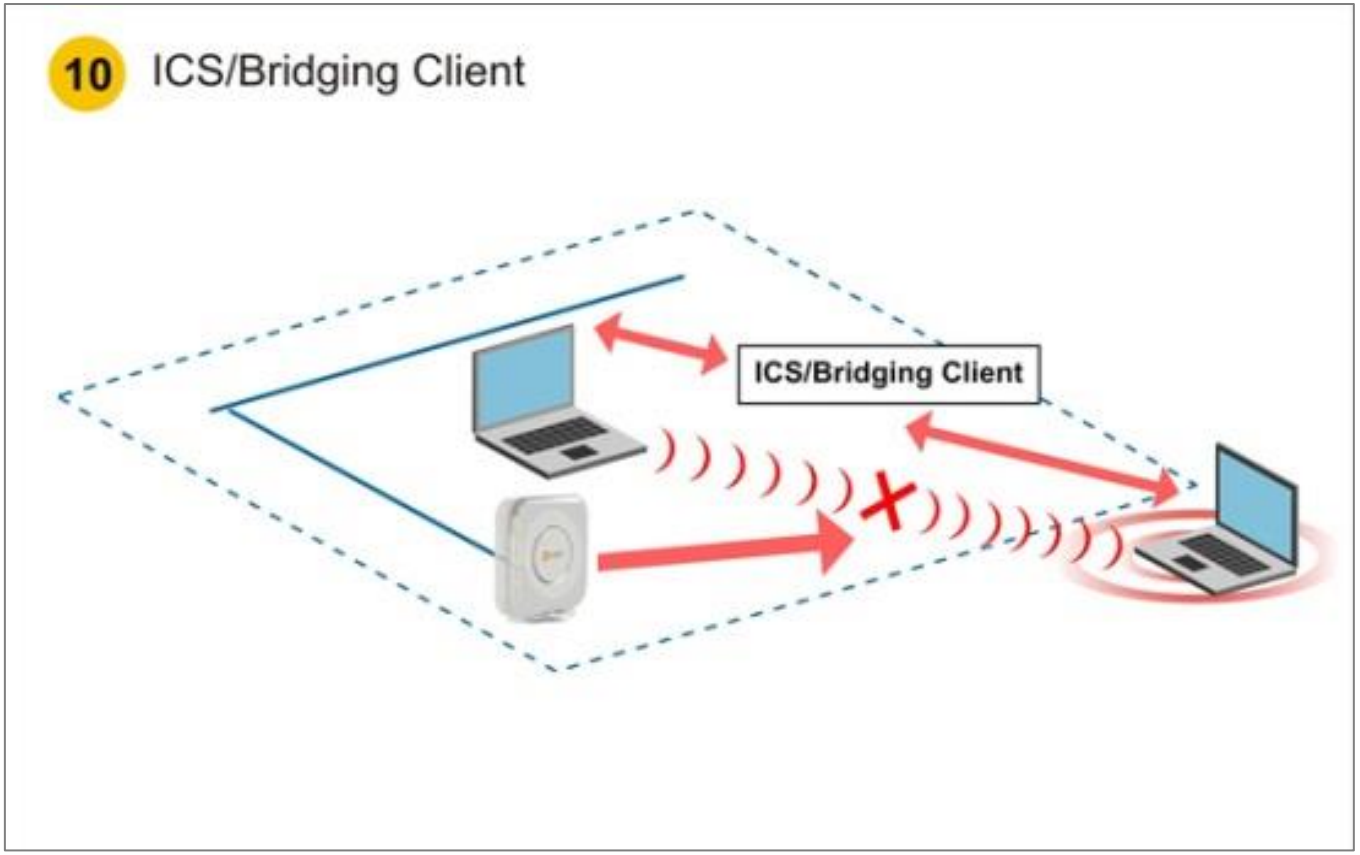
Типы атак на беспроводные сети

- Контроль BYOD устройств



Типы атак на беспроводные сети

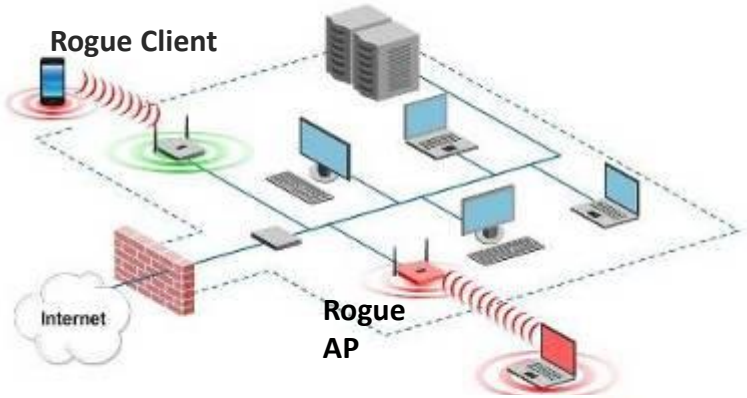
- Организация общего доступа к интернету

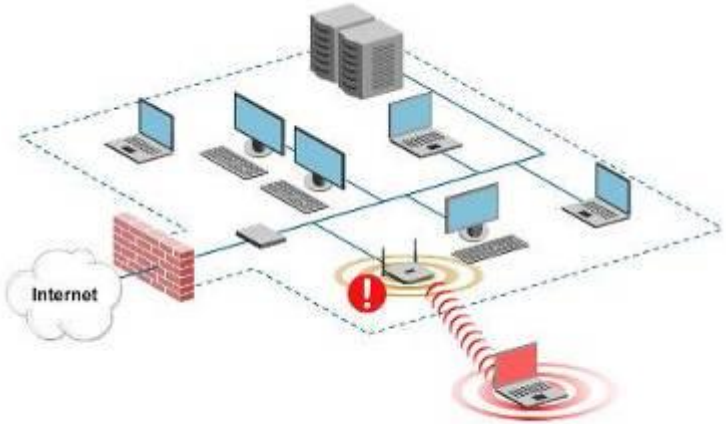


Основные задачи выполняемые Wi-Fi IPS

Наиболее вероятные сценарии вторжения

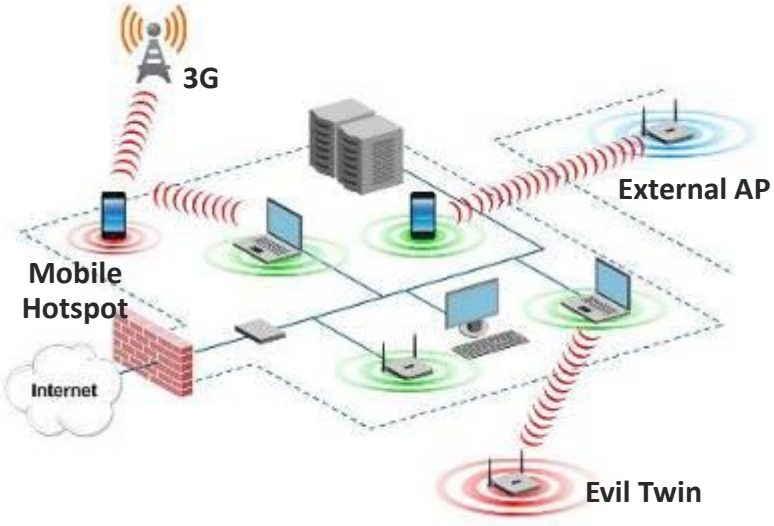
Неавторизованный Wi-Fi в сети



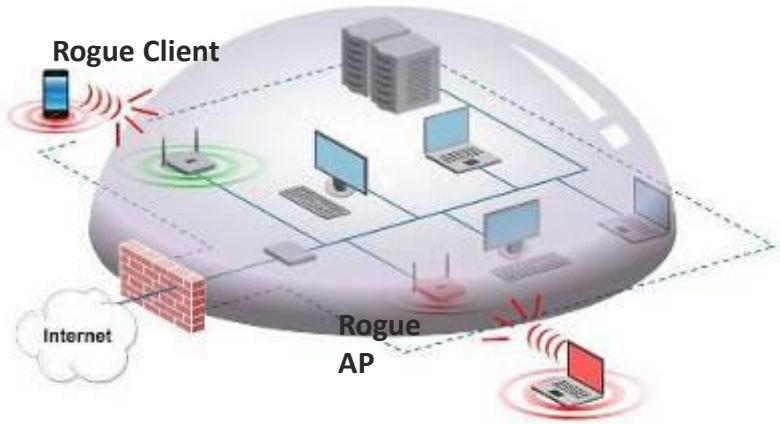


Слабая защита Wi-Fi сети

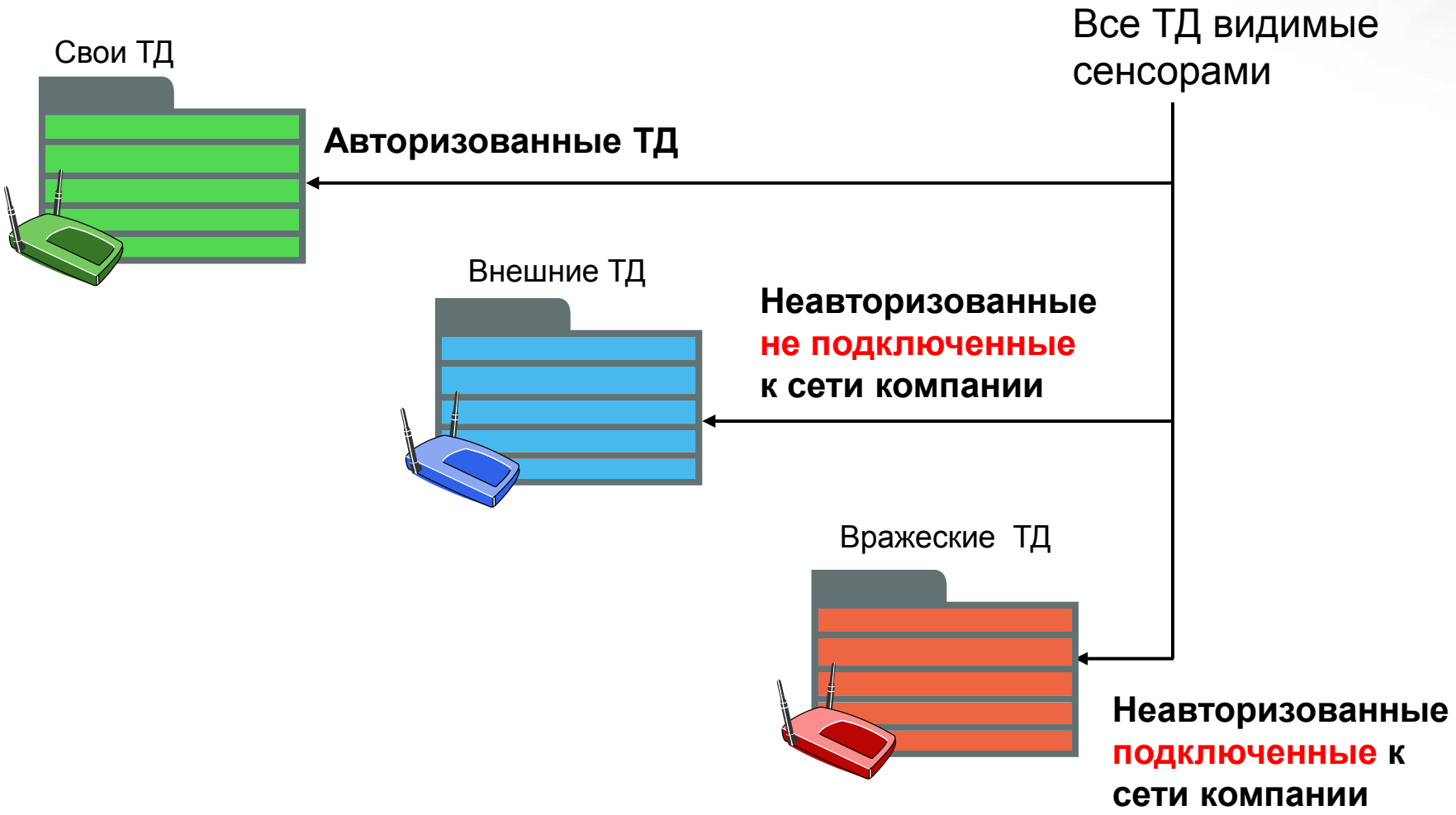
Нарушение политик безопасности клиентами



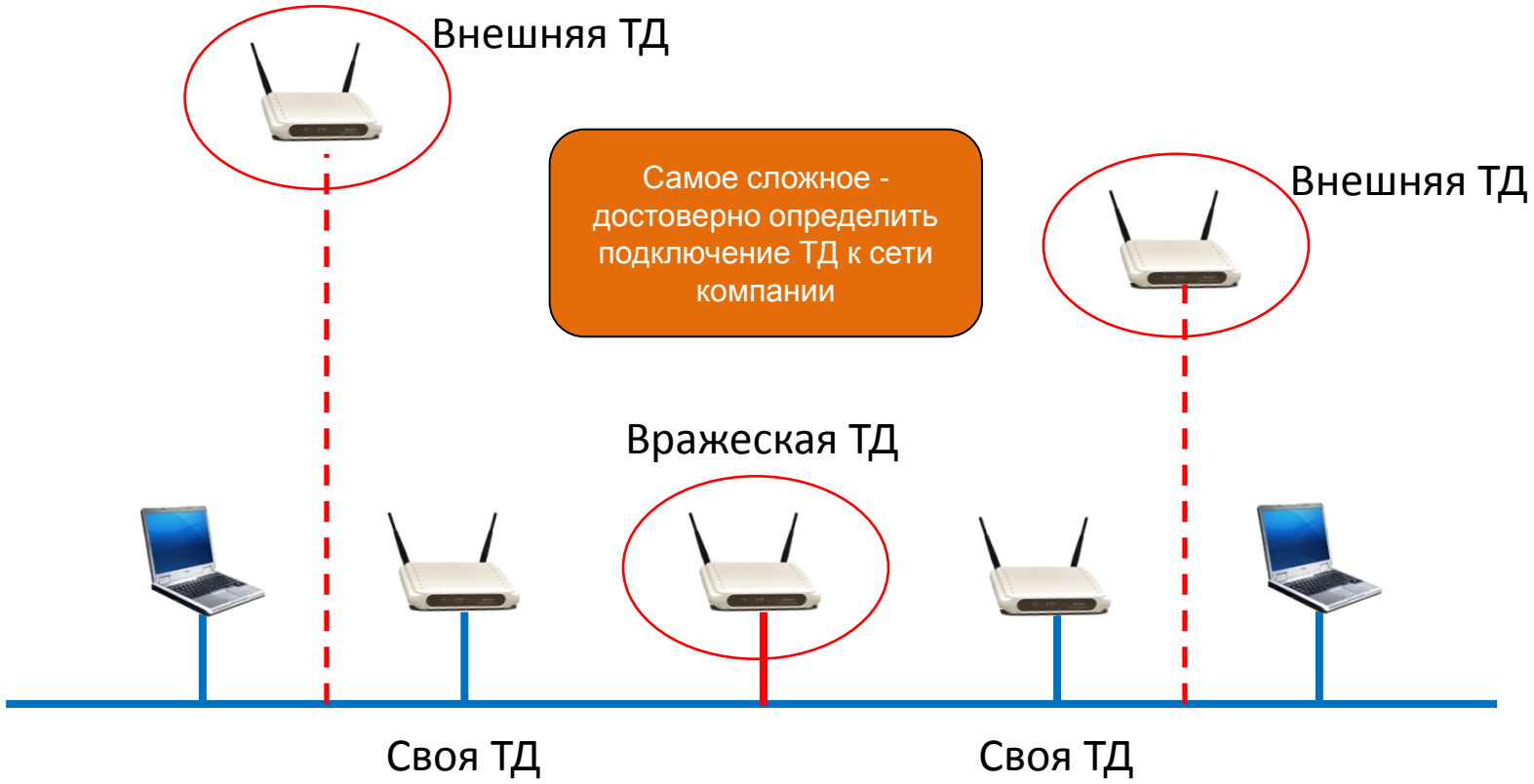
Основные задачи выполняемые WIPS



Классификация устройств



Классификация ТД системами WIPS



Основные задачи выполняемые WIPS

1. Классификация устройств
2. Контроль соблюдения политик безопасности
3. Мониторинг и блокировка атак на беспроводные сети

Обзор различных реализаций WIPS

Методы классификации устройств в различных WIPS

- Метод сигнатур
- Метод корреляции MAC адресов
- Метод маркированных пакетов

Методы классификации в различных WIPS

Метод сигнатур – определяется набор признаков по которым классифицируются ТД

MAC	***Signal Strength***	***Connectivity***
IP Address	***Protocol***	***Association***
Vendor	***Authorization***	***Key Generation***
Channel	***802.X Username***	***Specific EAP Type***
SSID	***Last Seen***	***Encryption***

Минусы

- Достаточно длительная настройка
- Для каждого класса (свои, соседские, гостевые) своя сигнатура
- Постоянное отслеживание изменений признаков
- Легко имитировать на ТД злоумышленника

Методы классификации в различных WIPS

Метод корреляции MAC адресов – за основу берется базовая настройка MAC адресов ТД. Как правило, MAC адреса на проводном и беспроводном интерфейсе ТД отличаются только в последней цифре

1. WIPS определяет MAC адреса видимых беспроводных устройств.
2. WIPS пытается обнаружить подобные им MAC адреса путем опроса таблиц коммутации.
3. В случае обнаружения подобных MAC адресов, соответствующая ТД считается подключенной к сети.

Минусы

- MAC адреса на ТД легко редактируются
- Требуется доступ к коммутаторам (логин/пароль)
- Постоянное отслеживание изменений в настройках коммутаторов
- Невозможно непрерывно опрашивать коммутаторы

Сравнение техник определения подключенных AP

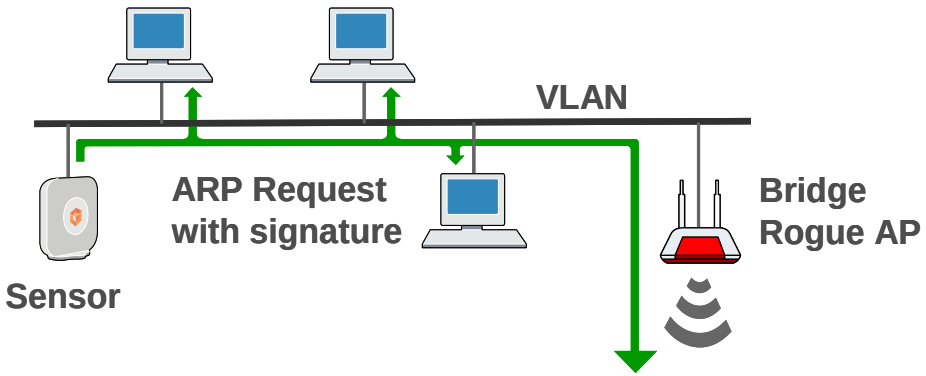
Критерий	Marker Packets	MAC Correlation
1. Ложноотрицательный для AP с NAT	Никогда	Часто
2. Ложноположительный для соседских AP	Никогда	Часто
3. Время определения	До 5 мин	Десятки минут
4. Настройка, обслуживание	Не требуется	Требуется постоянно
5. Масштабируемость	Неограниченно	Плохая
6. Ручное вмешательство в классификацию	Не требуется	Требуется постоянно

Метод Marker Packet™

Точное определение “on-wire / off-wire”

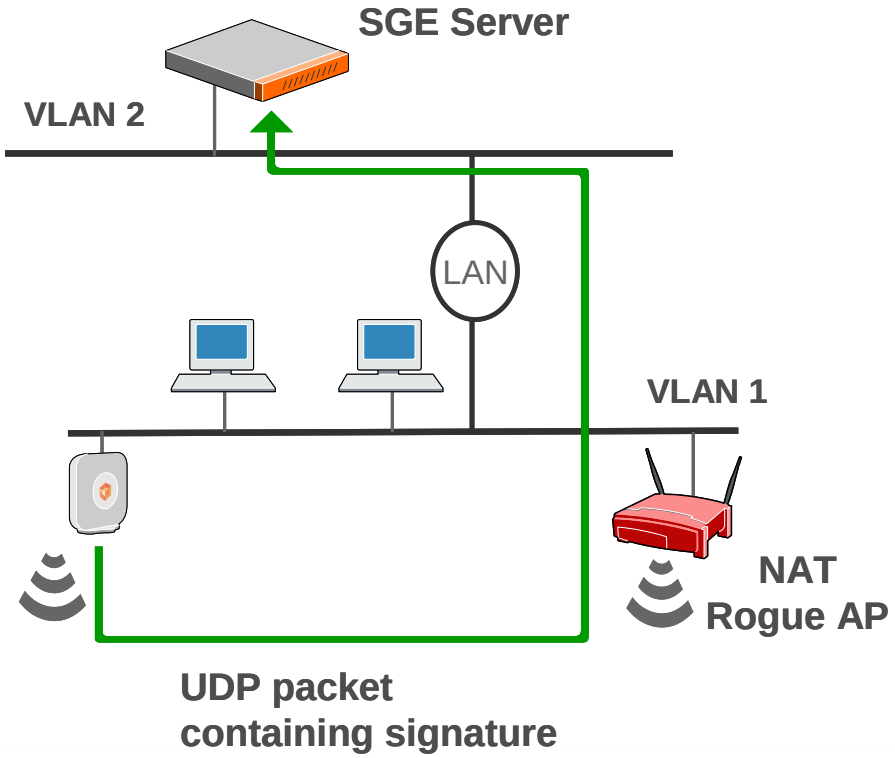
ARP Request Marker Packet

Сенсор делает маркированный ARP запрос «по проводам» и определяет его появление «в воздухе»



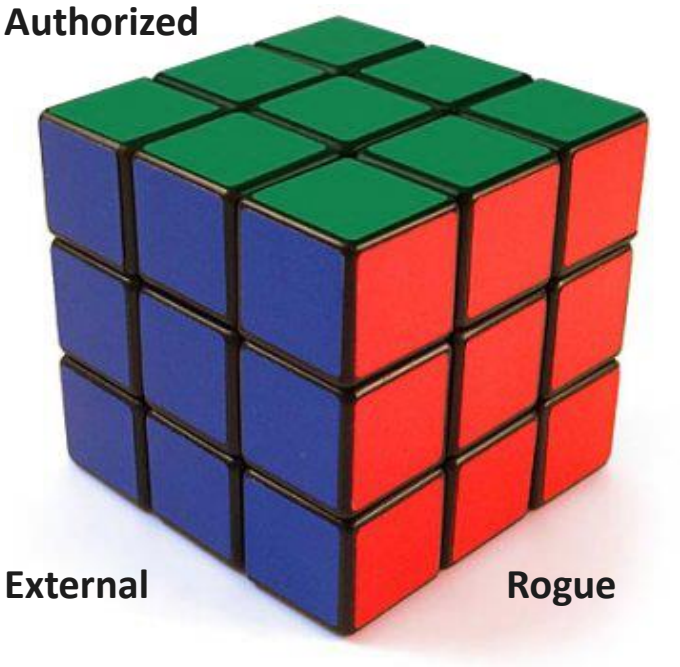
UDP Reverse Marker Packet

Сенсор делает маркированный UDP запрос «по воздуху» и определяет его появление «в проводах»



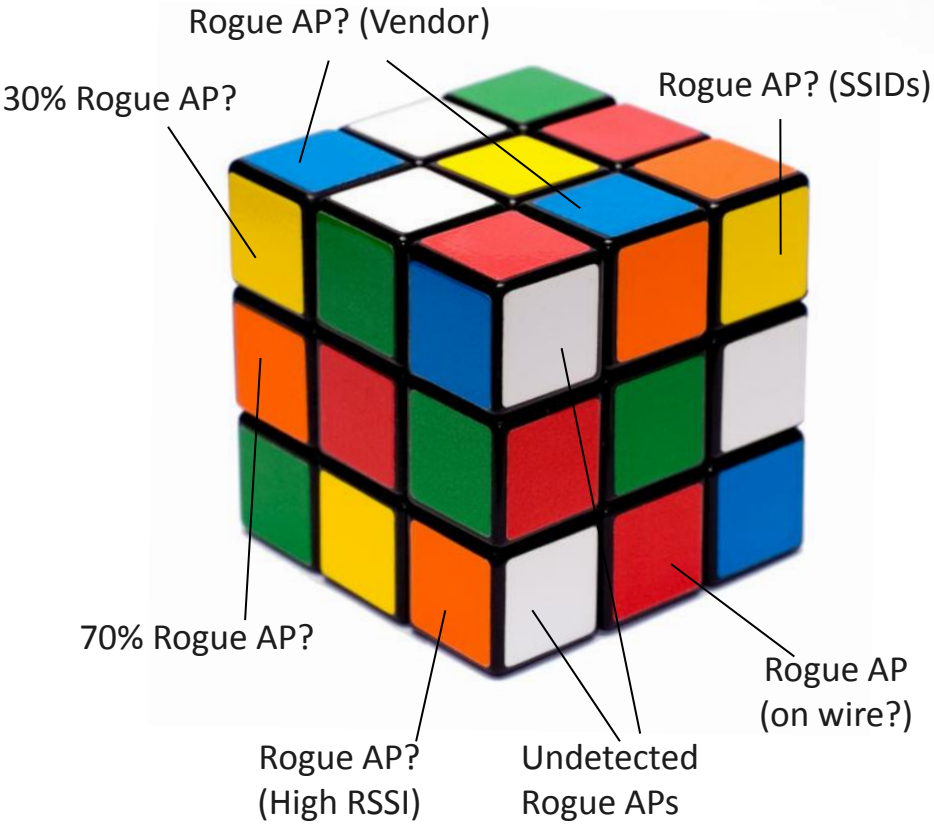
Автоматическая классификация устройств

AirTight WIPS



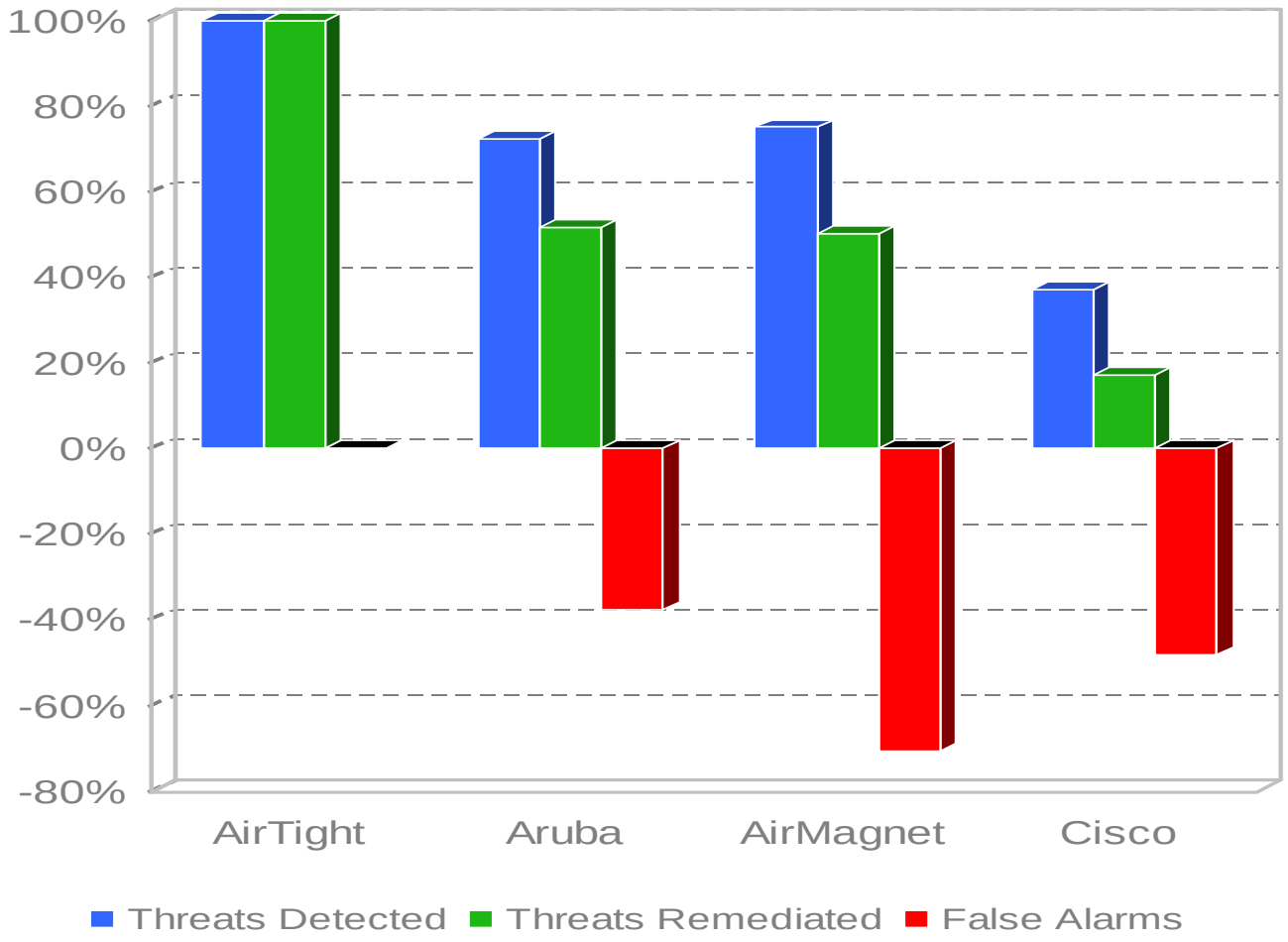
Работает сразу «из коробки»

Прочие WIDS решения



Требует настроек сложных правил и ложные тревоги будут постоянными

Сравнение различных производителей по количеству ложных тревог, обнаружению и нейтрализации угроз



Обзор возможностей WIPS MOJO Networks

AirTight WIPS – единственный истинный WIPS

Автоматическая классификация устройств

Определение всех возможных угроз

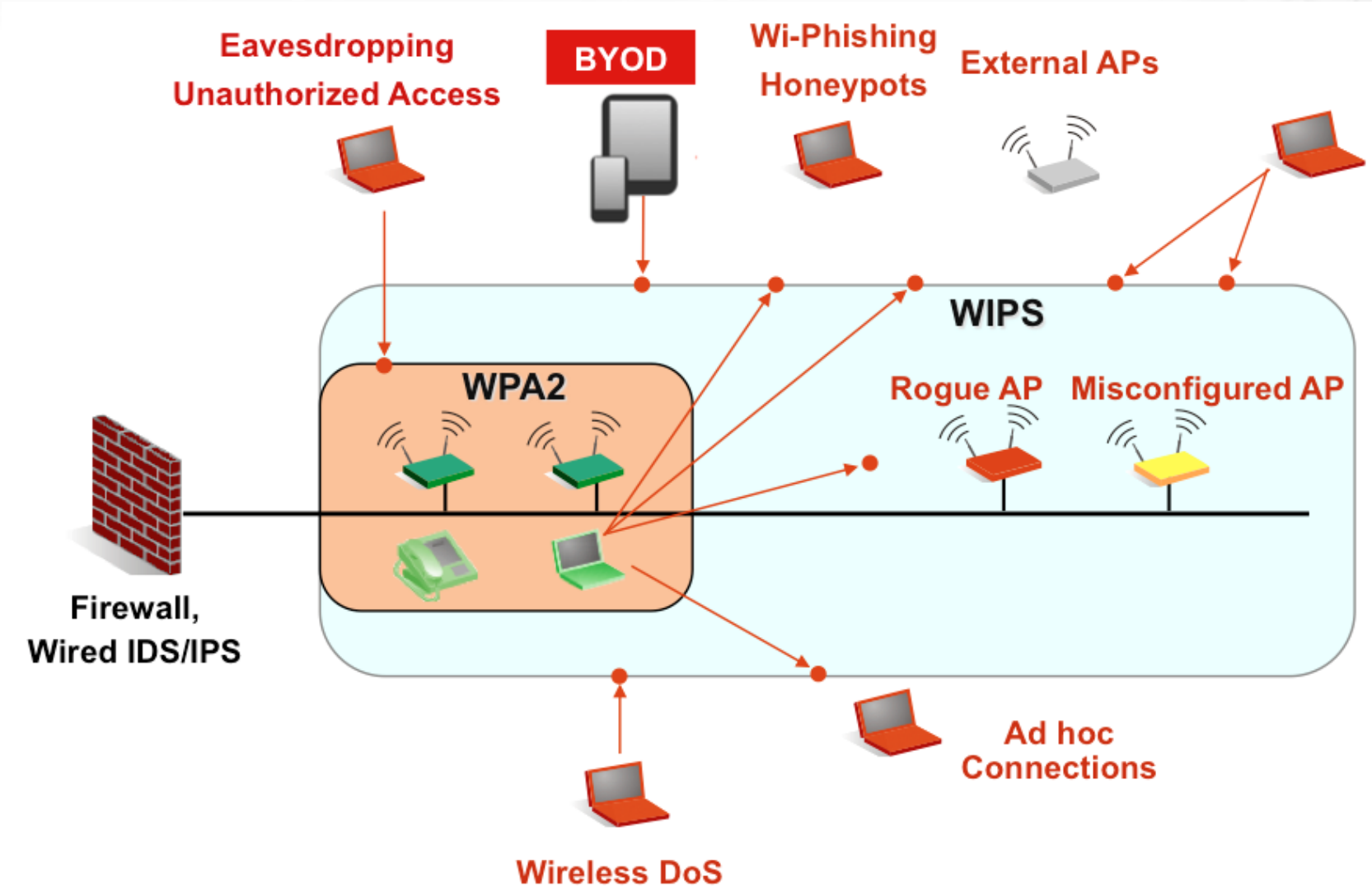
Надежная система противодействия угрозам

Точное определение местонахождения

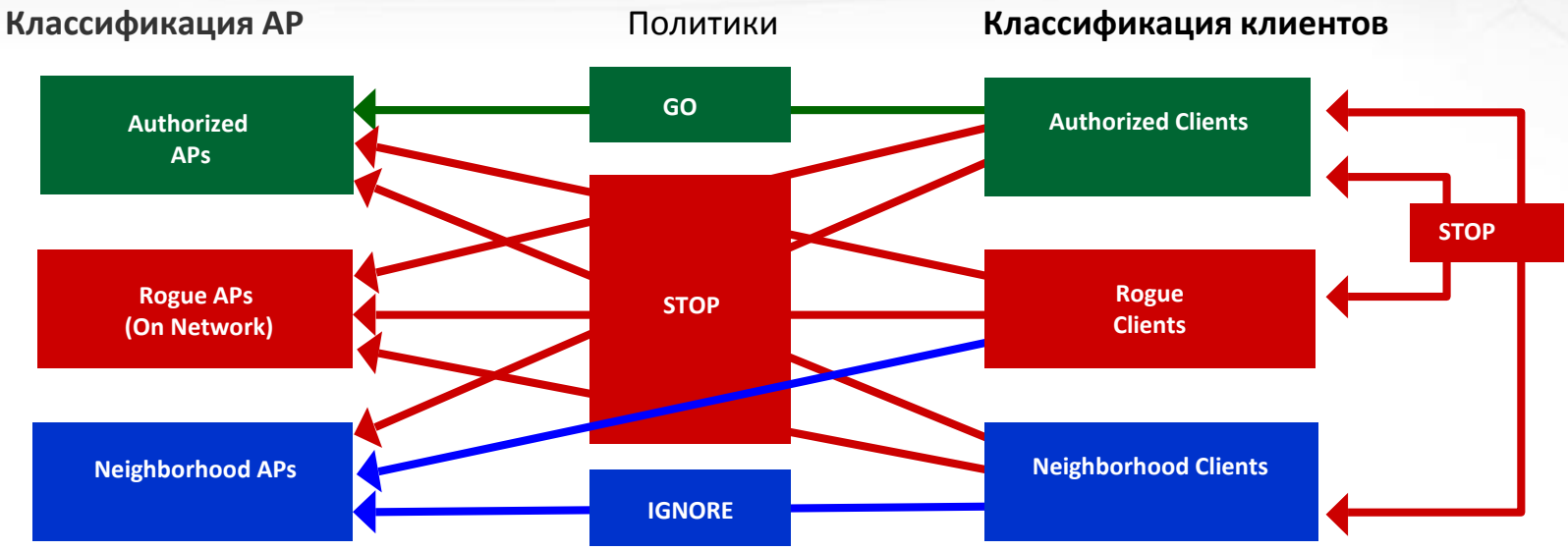
Обеспечение соблюдения политик BYOD

Автоматические отчеты

WPA2 не значит полная безопасность



Как работает MOJO AirTight WIPS 24/7



Такой подход защищает сеть от всех типов беспроводных угроз, уязвимостей и хакерских атак

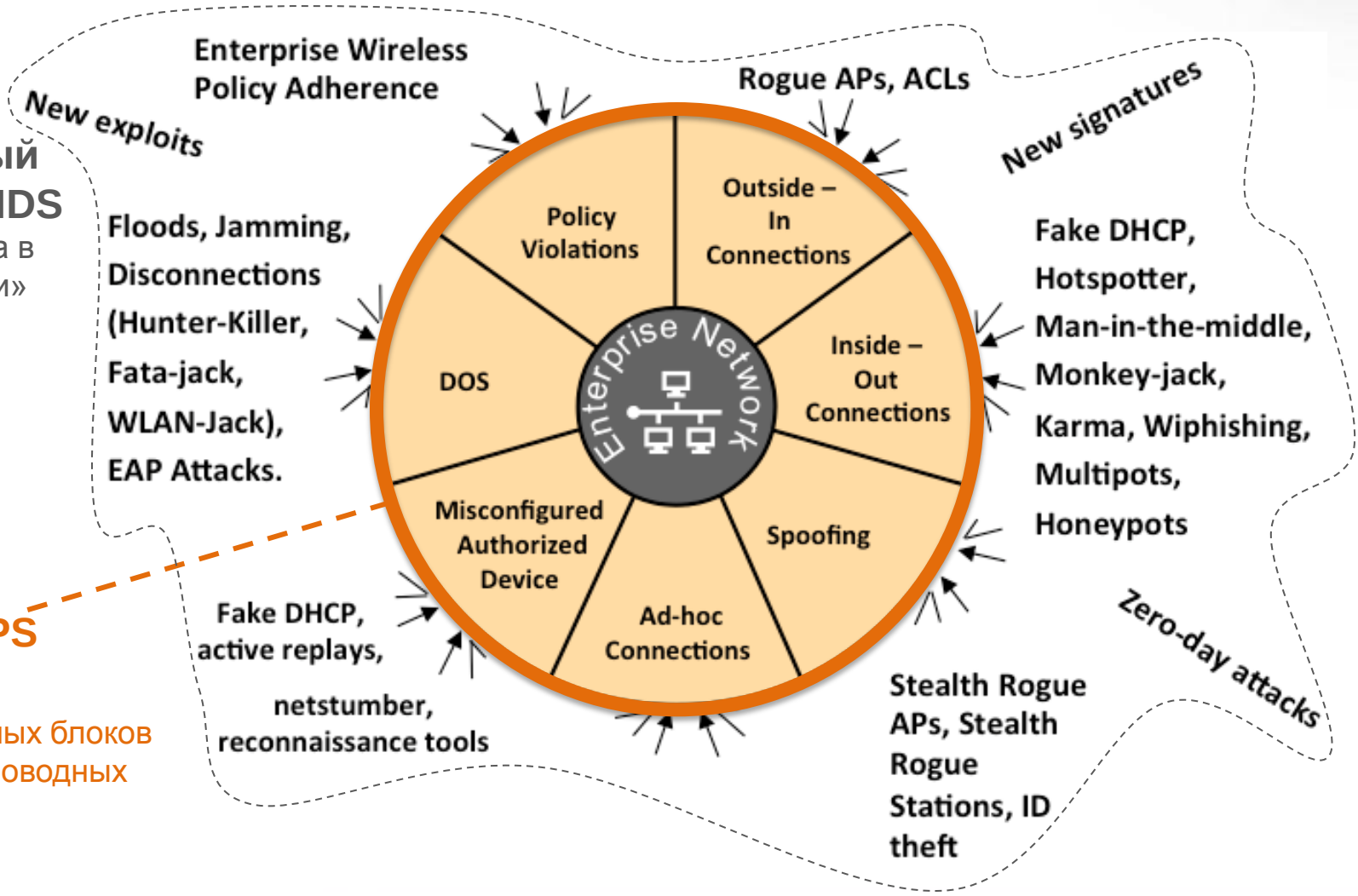
Конкуренты

- Требуется настроить и постоянно обновлять правила классификации
- Определение угроз по сигнатурам и пороговым значениям создает большое количество событий
- «Врожденные» ложные тревоги требуют постоянного вмешательства
- Ненадежны для автоматического функционирования
- Классические проблемы сигнатурного подхода: неполные и меняющиеся сигнатуры
- Минимальная защита от “zero-day attack”

MOJO AirTight применяет принципиально новый подход

Стандартный подход к WIDS

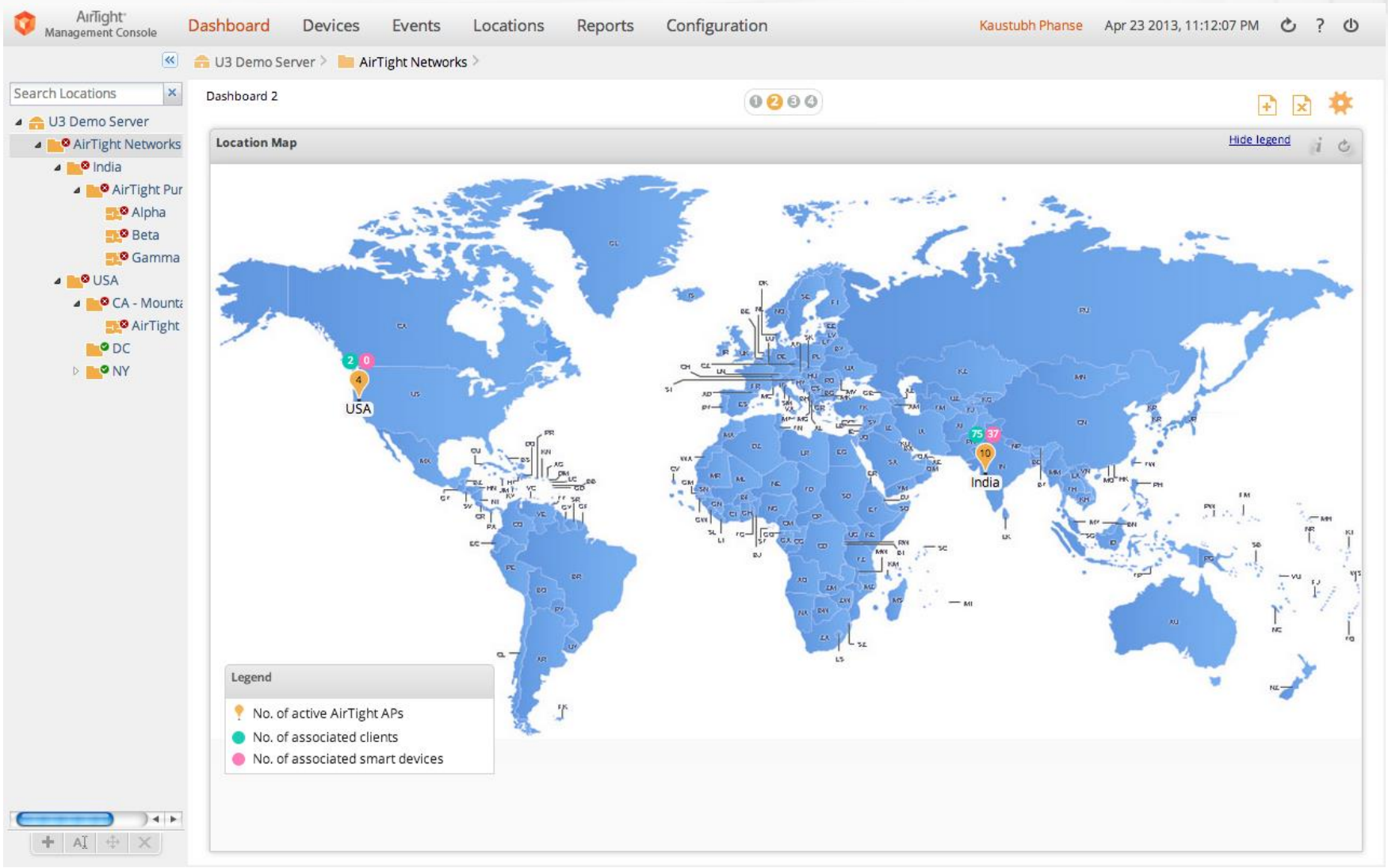
По сути это игра в «кошки – мышки»



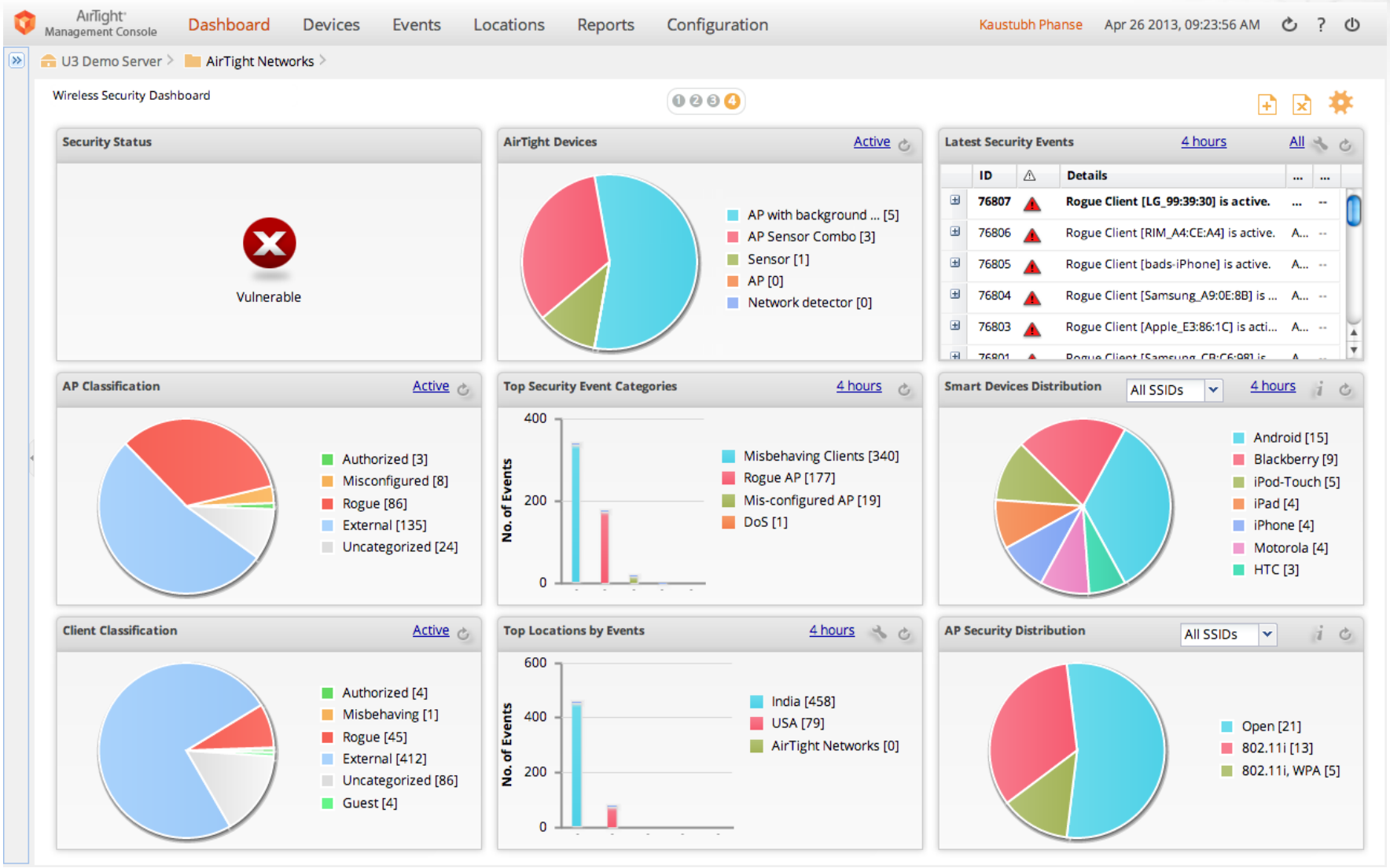
AirTight WIPS

Защищает от фундаментальных блоков угроз для беспроводных сетей

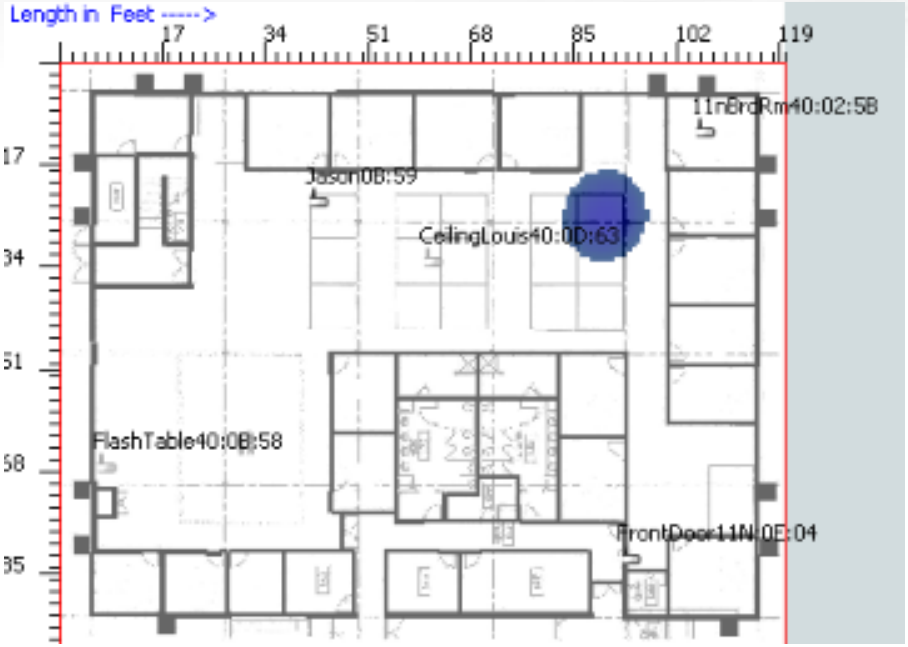
Позиционно зависимое управление



WIPS Dashboard



Обнаружение – триангуляция



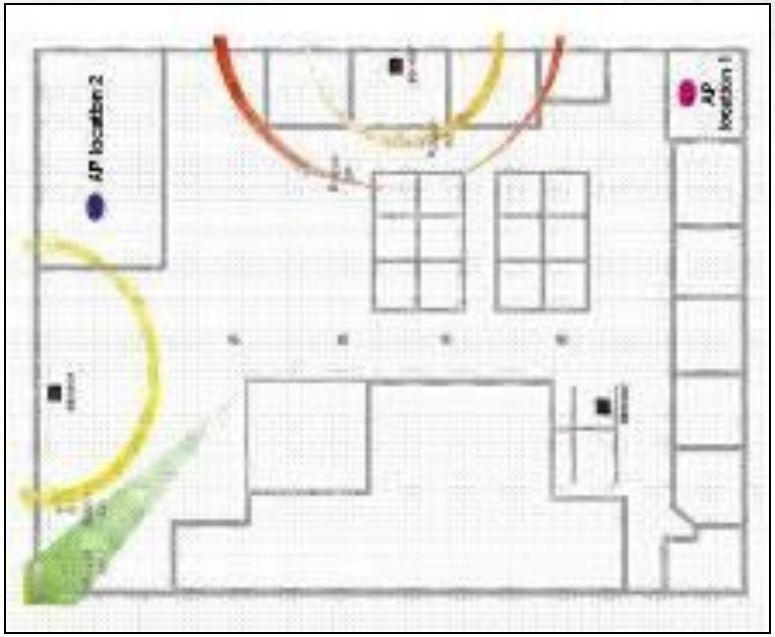
Стохастическая радиочастотная триангуляция

Самокалибрующаяся под изменения сигнала из-за флуктуаций мощности передатчика, ориентации антенн, переотражений

Не требует калибровки на местности

Отображается как карта распределения вероятностей

Конкуренты



Простая триангуляция

Мощность принимаемого сигнала, используемый для оценки расстояния до устройства и расположение оценивается как место пересечения кругов

Чувствительны к изменениям уровня сигнала, результат - неточное местоположение

Требует калибровки на местности

Захват и анализ трафика

- Облачный анализатор MOJO Packets
- Загрузка pcap файлов
- Захват трафика непосредственно с сенсоров
- Возможность работать on-line над одним файлом группе специалистов

https://mojopackets.com/

Безусловный лидер в безопасности WLAN

- AirTight – это 29 собственных патентов компании

Gartner on AirTight

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks				x	
Meraki			x		
Motorola				x	

AirTight WIPS единственная WIPS:

- Единственная получившая рейтинг “Strong Positive” от Gartner – два года подряд!
- На верхних ступенях рейтинга Gartner во всех шести отчетах MarketScope WLAN IPS

US DoD Approved

Common Criteria

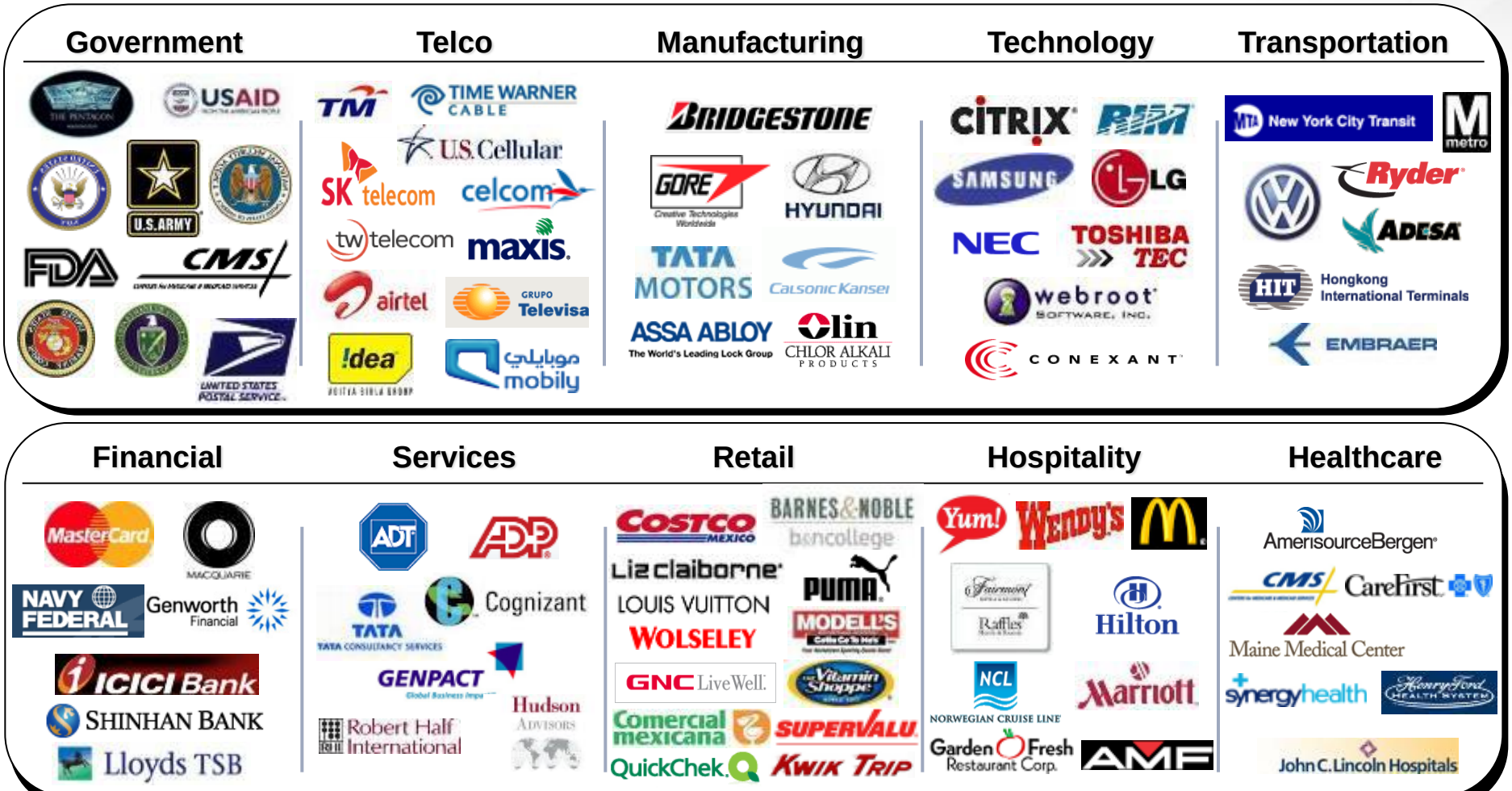
FIPS VALIDATED 140-2

DISA UC APL

AirTight WIPS единственная WIPS:

- Сертифицирован на «Common Criteria EAL2+», FIPS 140-2 и DISA UC APL

Заказчики



Основные особенности MOJO Airtight WIPS

- Более 29 патентов
- Технология Marker Packet (надежное обнаружение и классификация)
- Точная классификация устройств «на проводах»
- Обнаружение, классификация и блокировка точек доступа с NAT, с шифрованием и программных
- Обнаруживает и блокирует несанкционированное поведение клиентов
- Автоматическая блокировка без нарушения коммуникаций соседей
- Интегрируется с WLAN контроллерами Cisco, Aruba и HP
- Одновременная блокировка нескольких вторжений на нескольких каналах одним сенсором
- Блокировка 802.11 DoS атак

Основные особенности MOJO Airtight WIPS

- Разделение Wi-Fi политик по VLAN, SSID, и местонахождению
- Поддержка Multi-VLAN (до 100 VLAN на один сенсор)
- Не зависит от опроса CAM таблиц и SNMP
- Списки мобильных устройств-нарушителей
- Off-line режим сенсоров (всегда активная защита)
- Захват трафика с любого сенсора с любого интерфейса
- Распределенная система управления
- Наиболее точная система локализации устройств
- До 18,000 сенсоров на одной консоли управления
- Масса предустановленных отчетов
- Простота внедрения и использования

Реализация AirTight WIPS

Варианты внедрения AirTight

Платформы


AT-C10


AT-C50


AT-C60


AT-C55

Внедрение


Public Cloud


VMware


Private Cloud


Appliance

Цена

- ✓ Zero Capex
- ✓ Bundled
- ✓ Capex

Нет лицензий за дополнительный функционал!
Нет лицензий за пользователей!

AirTight Server Appliances

SA-250
Standard Appliance

SA-360
Premium Appliance

AirTight APs/Sensors

O-70

Dual band dual radio 3x3
- AP + background scanning
- Dedicated WIPS sensor

C-60

Dual band dual radio 3x3
- AP + background scanning
- Dedicated WIPS sensor
- **Concurrent AP + Dedicated WIPS**

C-50

Dual band single radio 2x3
- AP + background scanning
- Dedicated WIPS sensor

C-55

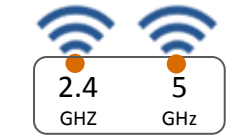
Dual band dual radio 2x2
- AP + background scanning
- Dedicated WIPS sensor

C-10

DoD approved WIPS Sensor
- Common Criteria
- FIPS 140-2
- DISA APL

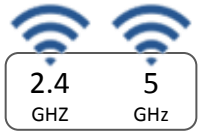
Режимы работы Сенсоров/ТД

- **Интегрированы в AP**
  - AP с фоновым сканированием
  - Полное обнаружение угроз и блокирование Rogue AP «на проводах»
  - Не рекомендуется для чувствительных к времени приложений

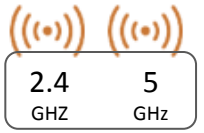


Wi-Fi AP with background scanning

- **Выделенные**
  - Выделенные сенсоры поверх существующей WLAN
  - 24/7 мониторинг и защита

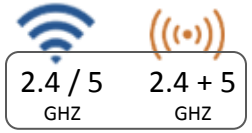


Wi-Fi AP



WIPS Sensor

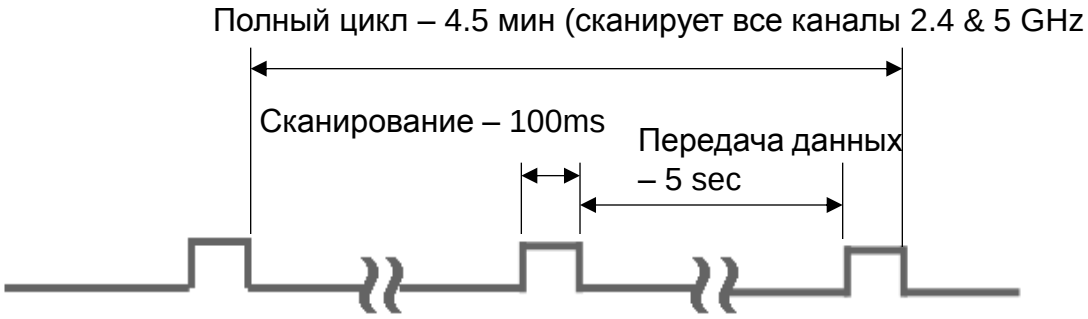
- **Комбинированные**
  - AP работают как выделенный сенсор
  - 24/7 мониторинг и защита
  - Поддерживает все виды приложений, включая VoIP



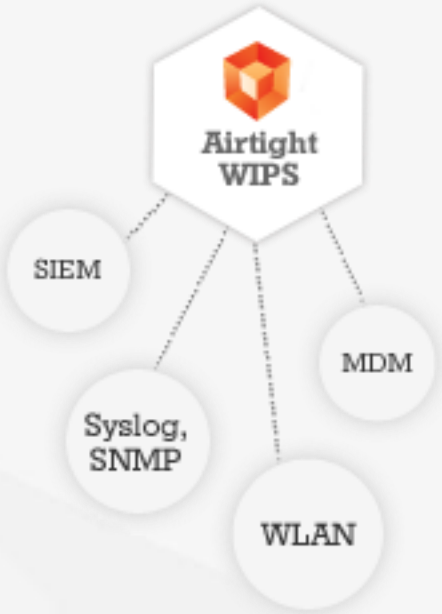
Wi-Fi AP with Concurrent WIPS sensor

Фоновое сканирование WIPS

- Сканирует все каналы диапазонов 2.4 и 5 ГГц
- Мониторинг 8 VLANs на Rogue AP используя Marker Packet™
- Автоматическая защита от неограниченного количества Rogue AP подключенных к проводной сети
- Работает на неуправляемых коммутаторах
- Определяет нарушение беспроводных политик например, ошибочные подключения клиентов, ad-hoc соединения



Интеграция с другими системами



Интеграция с корпоративными системами

SIM/SEM Servers

SysLog

ArcSight

SNMP

AirTight WIPS

CISCO

ARUBA networks

hp

Дистрибьютор в России ЗАО «НТЦ Ландата»

Дмитрий Дундуков
tooltest@landata.ru
Тел. +7 /925/ 6-000-300