Неуправляемые устройства в сети
Чем грозят и что делать

Андрей Москвитин

Специалист по решениям ИБ

amoskvit@cisco.com

@anmosk

«Глупые» устройства в корпоративной сети

- IP-телефония
- Принтеры, факсы, МФУ ...
- АТС
- Камеры наблюдения
- Плазменные панели
- Кассы и терминалы
- Личные ноутбуки

На самом деле не очень «глупые»

И иногда странные

В чём опасность?

- Проприетарные или устаревшие ОС
  - Патчей нет в природе или они не устанавливаются
- Пароли cisco или P@$$w0rd
- Не поддерживают механизмы безопасности
  - Антивирус
  - Доменные политики, в т.ч. парольные
  - Аутентификация по сертификатам или 802.1x
- Требуют для себя исключений из общих правил
  - Чем пользуются злоумышленники

Как идентифицировать устройство?

ИЛИ

ИЛИ

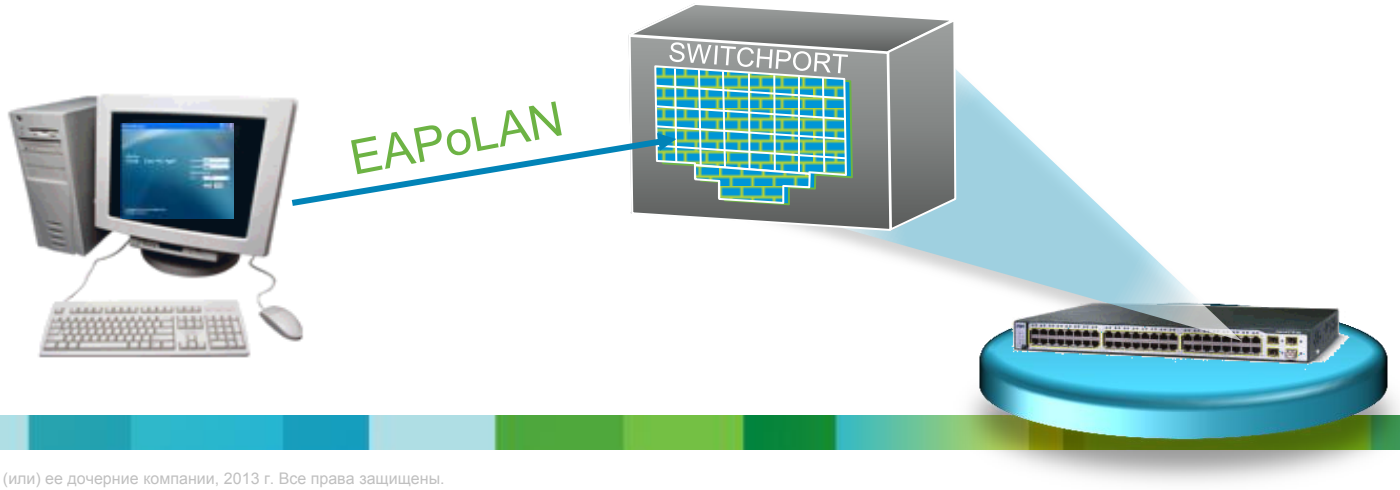
- MAC-адрес ненадёжен
- Активное сканирование ненадёжно
- Характер трафика
- Профилирование (TTL, etc)

С чего начать строить оборону?

- Инвентаризация существующих устройств
- Принцип минимальных полномочий
- Оборудование корпоративного класса
- Изолировать «глупые» сегменты
  + списки контроля доступа или TrustSec и аналоги

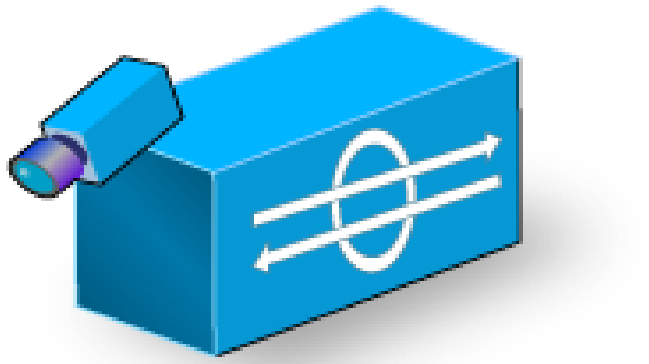
Network Admission Control

- Контроль «здоровья» на этапе подключения
- Инвентаризация
- Профилирование трафика
- Обнаружение аномалий
- Блокирование как до, так и после подключения
- Обучение пользователей, стоимость



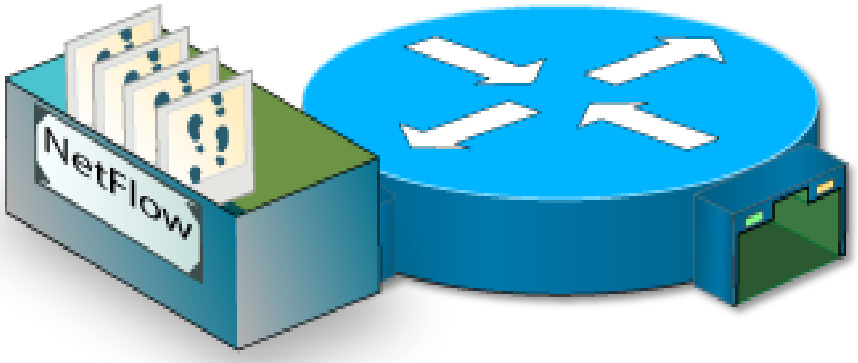
IDS/IPS

- Обнаружение аномалий и атак
- Инвентаризация
- Пассивное профилирование трафика и хостов
- Мгновенное блокирование
- Стоимость, видимость сети только в точках установки



Обнаружение аномалий через NetFlow

- Инвентаризация
- Профилирование трафика
- Обнаружение аномалий и атак
- Блокирование
- Видимость во ВСЕХ точках сети, низкая стоимость



Спасибо!

security-request@cisco.com