intact
правильный интегратор

Контроль доступа к сети

Олег Абанкин

Генеральный директор компании intact

- 13 лет в ИТ и ИБ
- МГУ им. М.В. Ломоносова, математика и механика
- MBA, стратегический менеджмент

intact | Предпосылки — угрозы

Несанкционированный доступ к сети

Подключение неавторизованных пользователей или устройств к сети (например, гость или злоумышленник)

Подключение заражённых или уязвимых устройств

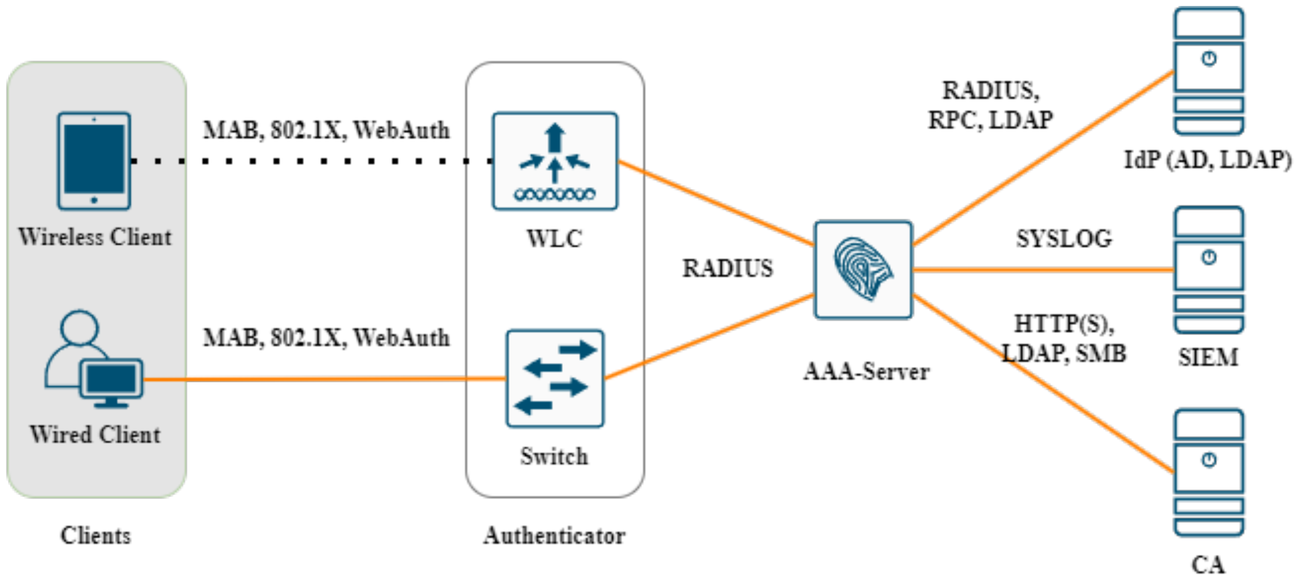
Заражённый ноутбук сотрудника или устаревшее ПО могут стать источником распространения вредоносного ПО

Вредительство от увольняемых сотрудников

Уволенный сотрудник может попытаться получить доступ к сети, особенно через ранее подключённые устройства

Сетевые атаки с внутренней стороны

Сотрудник или злоумышленник с доступом к сети может сканировать её, выполнять MITM-атаки и т.д.



Компоненты решения

- AAA-сервер
- Каталог учетных записей (IdP, Identity Provider)
- Центр сертификации CA
- Внешние системы: SIEM, SYSLOG-сервер

Несанкционированный доступ к сети

Подключение неавторизованных пользователей или устройств к сети (например, гость или злоумышленник)

Аутентификация пользователей и устройств перед допуском в сеть (802.1X, Captive Portal, сертификаты и др.)

Подключение заражённых или уязвимых устройств

Заражённый ноутбук сотрудника или устаревшее ПО могут стать источником распространения вредоносного ПО

Проверка состояния устройств перед подключением (антивирус, обновления, политики); возможность блокировки или помещения в карантин

Вредительство от увольняемых сотрудников

Уволенный сотрудник может попытаться получить доступ к сети, особенно через ранее подключённые устройства

Централизованный контроль и возможность мгновенно отключить доступ

Сетевые атаки с внутренней стороны

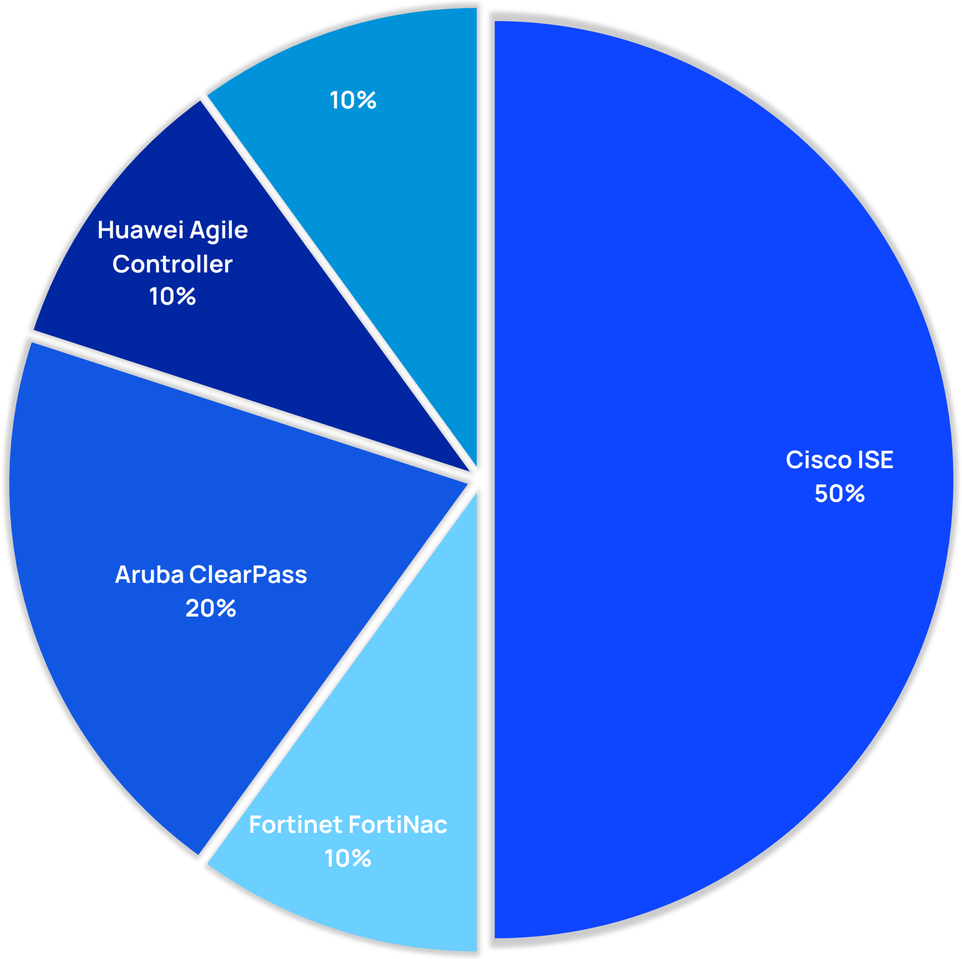
Сотрудник или злоумышленник с доступом к сети может сканировать её, выполнять MITM-атаки и т.д.

Сегментация сети и предоставление доступа только к необходимым ресурсам (принцип наименьших привилегий)

intact

Рынок решений класса NAC

intact | Решения до 2022 года



Ключевые функции

- Мультивендорный RADIUS
- TACACS+
- Гостевая аутентификация
- Поддержка IdP (AD, LDAP, API и прочее)
- Профилирование
- Posture Assessment - проверка состояния устройств (антивирус, патчи и т.д.)
- BOYD-сценарии
- Отказоустойчивость и кластеризация

intact | Отечественные аналоги Cisco ISE

WNAM

Ключевые функции

- Мультивендорный RADIUS
- TACACS+
- Гостевая аутентификация
- Поддержка IdP (AD, LDAP, API и прочее)
- Профилирование
- Posture Assessment - проверка состояния устройств (антивирус, патчи и т.д.)
- **BOYD-сценарии**
- Отказоустойчивость и кластеризация

DECKAUTH

Ключевые функции

- Мультивендорный RADIUS
- TACACS+
- Гостевая аутентификация
- Поддержка IdP (AD, LDAP, API и прочее)
- Профилирование
- Posture Assessment - проверка состояния устройств (антивирус, патчи и т.д.)
- **BOYD-сценарии**
- Отказоустойчивость и кластеризация

intact

Опыт внедрения WNAM как замены Cisco ISE

intact | Исходные вводные и задачи

Инфраструктура заказчика

- Сетевое оборудования: Aruba, Cisco
- Беспроводная сеть: Aruba
- VPN решение: UserGate
- Около 700 устройств в сети
- Отсутствует PKI (CA)
- Внедрена Active Directory

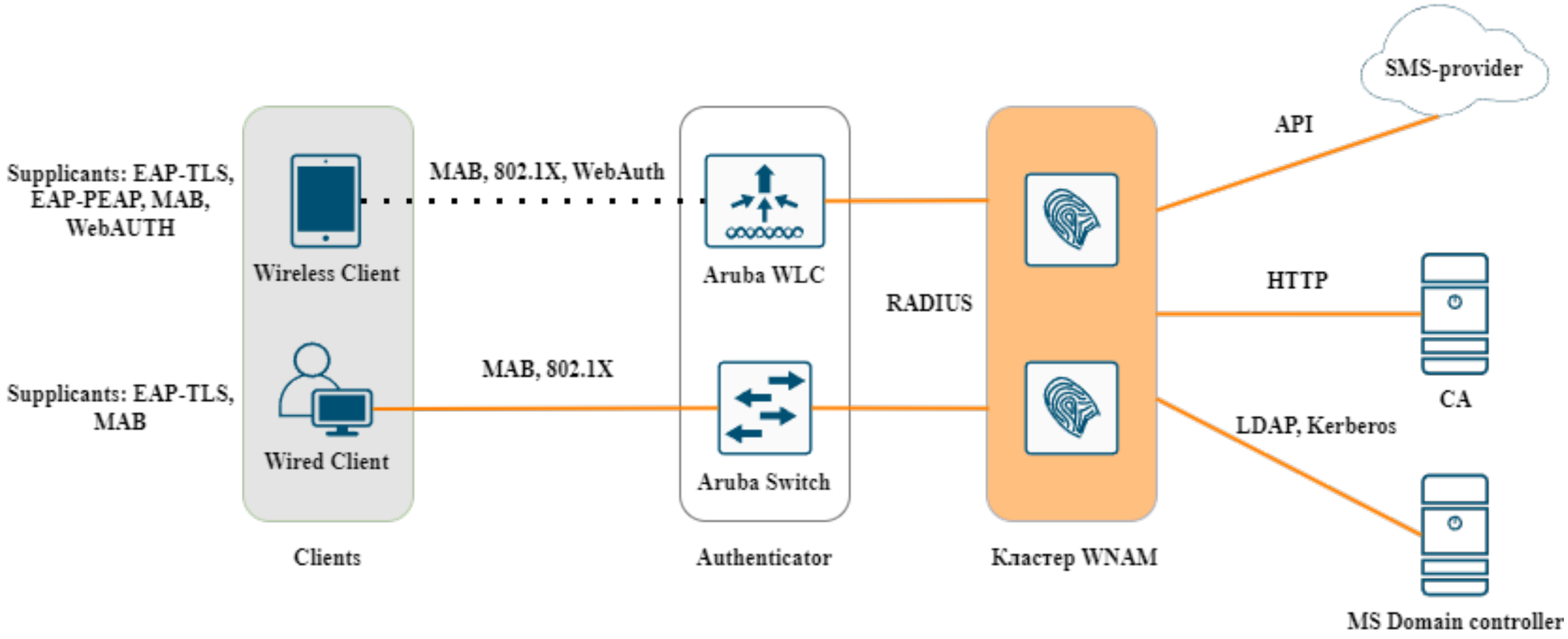
Этап 1

- Обеспечить контроль периметра сети и беспроводного оборудования
- Отказоустойчивость системы
- Использование встроенного supplicant
- Бесшовная для пользователя аутентификации

Этап 2

- Обеспечить posture (проверка антивируса и т.д.)
- Расширить периметр до VPN решения
- Внедрить профилирование для мультимедиа устройств

intact | Схема внедрения



Сложность № 1 — PKI

Причины

- Изменение процесса для установки и обновления сертификатов
- Требуется отслеживание срока действия сертификатов
- Требуются компетенции в Microsoft CA

Основной вывод

- Внедрение dot1x требует зрелого и рабочего PKI
- Внедрение PKI – отдельный проект

Сложность № 2 — особенности Aruba

Причины

- Реализация dot1x существенно отличается у производителей
- Российские вендора тестируют только для части решений
- Сложности могут нарастать при появлении новых сценариев CoA

Основной вывод

- До продуктивного внедрения требуется пилотное тестирование системы

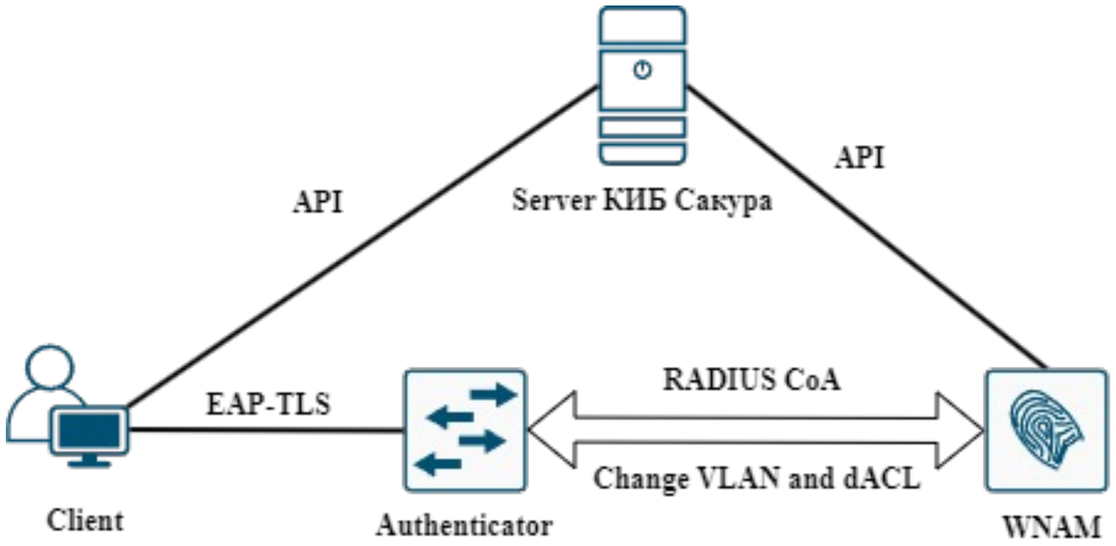
Сложность № 3 — организационные ограничения

Причины

- Система NAC влияет на все сетевые устройства
- Любое изменение в NAC, например, обновление – риски простоя всей сети

Основной вывод

- Требуется полная откладка системы до перевода в продуктив
- Изменение системы «на живую» крайне затруднено



Трудности интеграции

- Интеграция по API (задержки, а также потеря состояний)
- Vendor-Specific CoA

Инженерные системы

Сети передачи данных

Объединенные коммуникации

Мультимедийные системы

Вычислительные системы

ИТ-сервисы

Информационная безопасность

Импортозамещение

Услуги компании

- Аудит
- Проектирование
- Поставка оборудования и ПО
- Монтажные и пусконаладочные работы
- Техническая поддержка

15+
лет на рынке

1500+
реализованных проектов

100+
сотрудников

intact
правильный интегратор

Сделайте правильный выбор

121609, г. Москва, Осенний бульвар, д.23
+7 495 989 40 49 I info@intact.ru I intact.ru