ПОЛИКОМ ПРО
информационные технологии

Контроль доступа к сети: вчера, сегодня, завтра

Идея NAC

Первоначальная:
Возможность предоставить или ограничить доступ к сети, в зависимости от «здоровья» клиента.

Современная:
Соответствие политикам как критерий для принятия решений и совершения действий.

Зачем контролировать?

Идентификация подключающихся

- Кто? Где? Каким способом?

Организация доступа к ресурсам по ролям

- Допуск только к тому, что необходимо

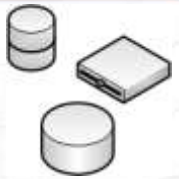
Контроль исполнения корпоративных политик

- Принудительное, а не рекомендательное соответствие

Как контролировать?

На уровне ресурсов

- Отдельный «список контроля доступа» для каждого типа ресурсов
- Сложности при добавлении новых ресурсов

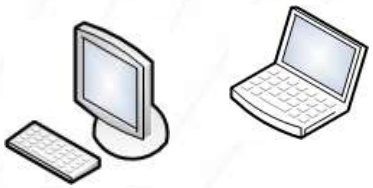


На уровне доступа к сети

- Контроль «на уровне порта»
- Возможность централизованного управления доступом
- Сложности проверки соответствия клиентов политикам

На уровне рабочей станции

- Полный контроль конфигурации и соответствия
- Уязвимость перед локальными администраторами



Вчера

- Рождение 802.1x
  - Очень высокая трудоемкость внедрения
  - Сложность реализации в масштабных сетях
  - Сложность поддержки

- Соответствие – что это?
  - Контроль через не приспособленные механизмы
  - Отсутствие
  - Отсутствие «обратной связи» и отчетности

- Карантин VPN?
  - Спорные механизмы у различных вендоров
  - Сложность конфигурации доступа клиентов

Сегодня

- Два подхода вендоров:
  - Вендор предоставляет «конструктор», вся поддержка сторонних компонентов (как ПО, так и оборудования) – от партнеров
  - Вендор самостоятельно предоставляет поддержку сторонних компонентов

- Варианты решений NAC
  - **NAC Framework** – почти 100% привязка к вендору
  - **NAC Appliance** – аппаратное «решение из коробки» (к сожалению, не всегда работает так как надо)
  - **Совместно** Soft & Appliance – собраны лучшие черты обоих вариантов

- Гибкие настройки, централизованное управление
  - Требования задаются **свободно** – в форме сценариев
  - Частичная интеграция с различными «инфраструктурными» средствами – домены, обновления, антивирусы, PKI
  - Достаточно развитые механизмы отчетности и оповещения, реакции на инциденты

Завтра

- Полная интеграция с различными решениями, свободная работа в гетерогенной среде
  - Системы управления инфраструктурой
  - Автоматическое определение типа клиентов
  - Системы проактивного мониторинга
  - IDS/IPS, DLP
- Универсальный, динамический гостевой доступ
  - Управление временным доступом
  - Отслеживание действий
  - Биллинг
- Решения NAC «из коробки»
  - Минимальные затраты на обновление и внедрение

Полученные преимущества

- Обеспечение полного соответствия политикам
  - Можно задать **<u>любые</u>** требования!
- Полная, актуальная информация
  - Получение информации о соответствии в реальном времени
  - Автоматическое реагирование на события
- Автоматическое исправление
  - Возможно исправление незаметно для пользователей!
  - Сокращение затрат на исправление за счет автоматизации

информационные технологии

Москва

ул. Сущевский вал, 16,
строение 3, офис 12

тел. | 495 | 660 32 91
тел. | 495 | 660 32 93
тел.факс | 495 | 660 32 93

Санкт - Петербург

наб. реки Мойки, 86

тел. | 812 | 325 84 00
факс | 812 | 110 64 31