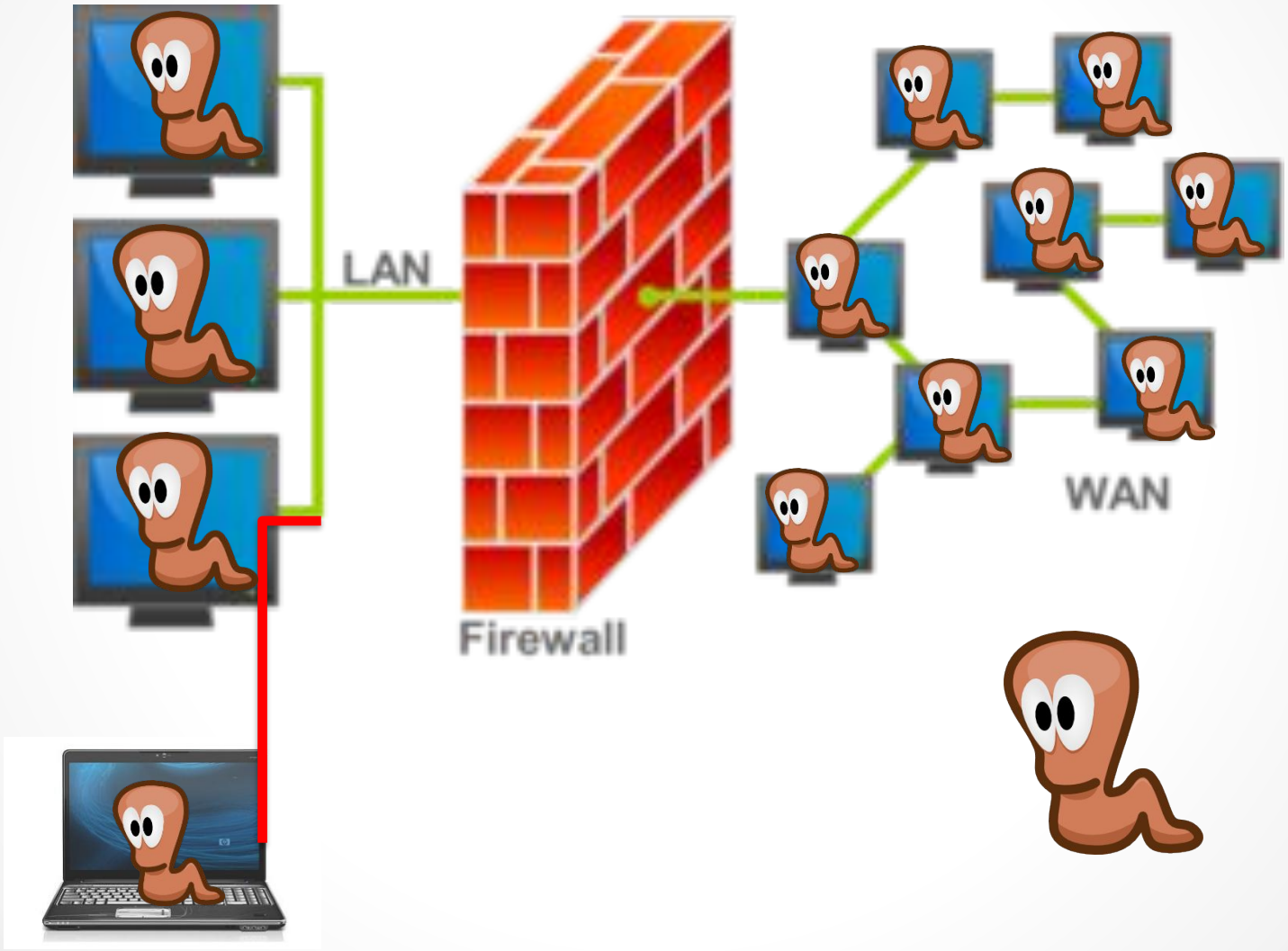
Основы Network Access Protection


LAN
Firewall
WAN

Что такое Network Access Protection и откуда он появился?

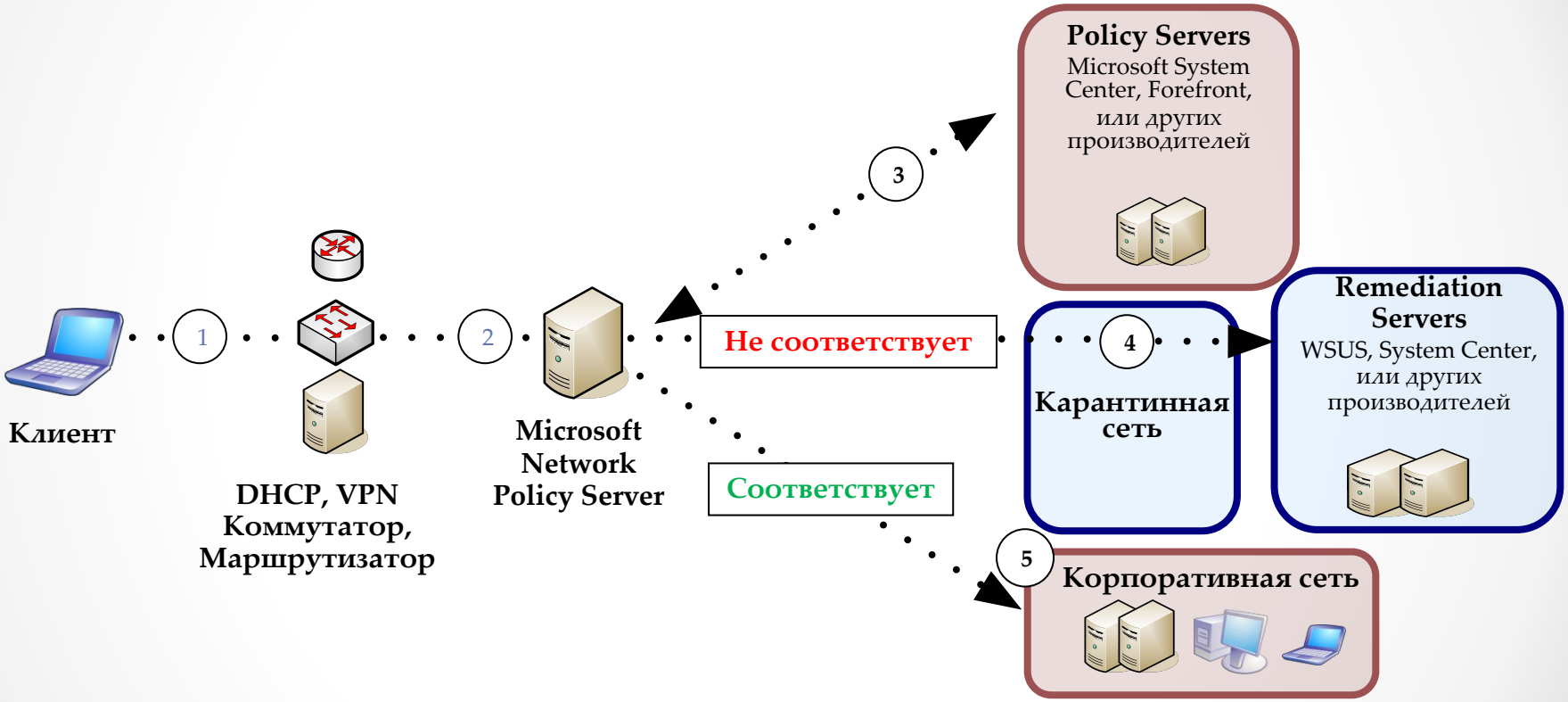
Как работает NAP и какие методы защиты использует?

Как правильно внедрить NAP?

Network Access Protection

- **Системные требования**:
  - NAP сервер – Windows Server 2008
  - NAP клиенты: Vista, XP SP3, RHEL
- **Контроль с помощью роли NPS** (Network Policy Server) **Windows Server 2008**
- **Network Access Protection выpос из VPN quarantine**
- **Поддерживает все типы сетевых клиентов, а не только VPN**
- **Управление с помощью политик, которые должны удовлетворять клиенты сети:**
  - Обновления системы, обновления антивируса, наличие межсетевого экрана

Схема функционирования NAP



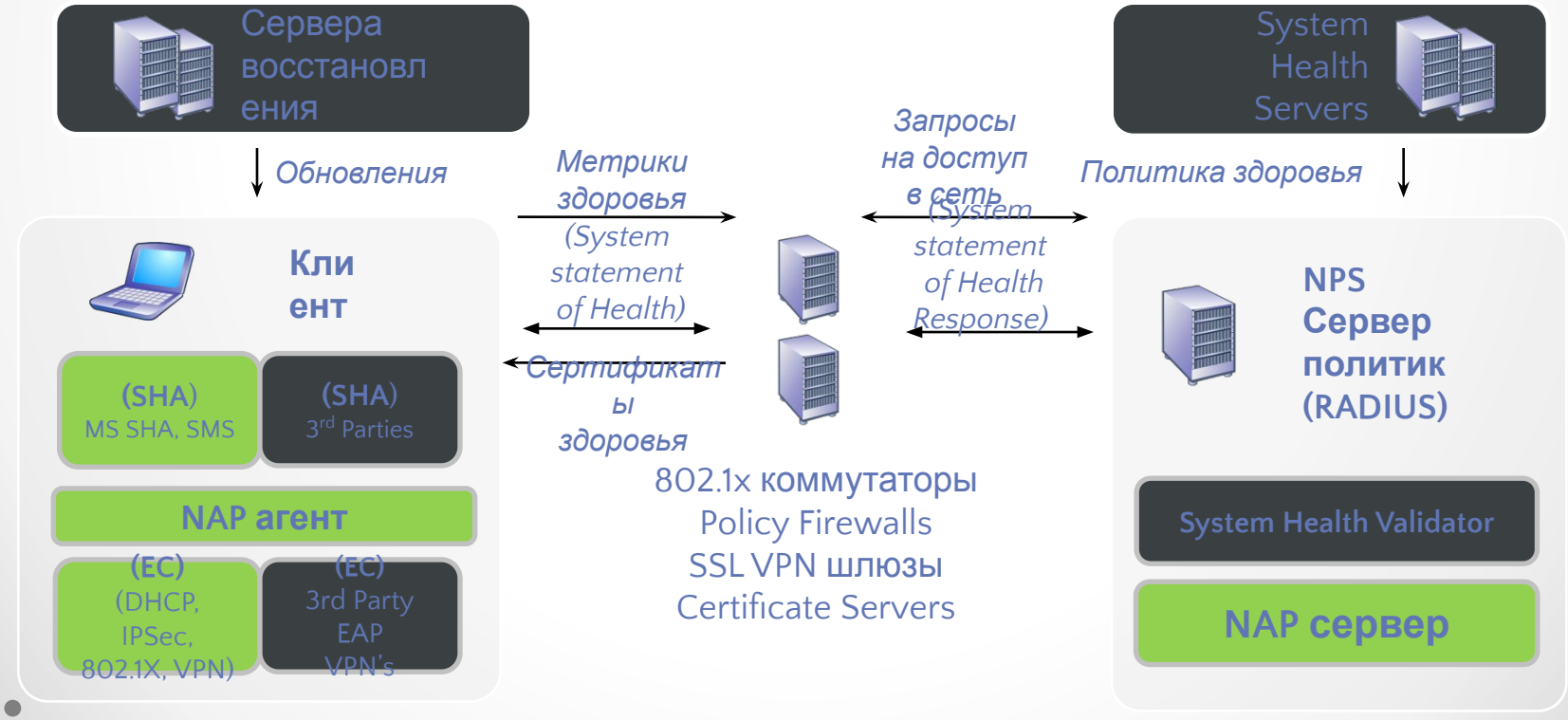
Методы принудительной защиты NAP

- **802.1x проводная и беспроводная сеть**
  - Список контроля доступа (Access Control List, ACL)
  - Виртуальная локальная сеть
- **IPSec**
  - Health Certificate Server выдает X.509 сертификаты только «правильным» клиентам
- **VPN (с помощью Routing and Remote Access)**
- **Управляет соединениями к Terminal Services Gateway**
- **DHCP выдает адреса из карантинной подсети**
  - DHCP можно обойти с помощью статической адресации – будьте осторожны!

NAP {Архитектура}

- **Клиент**
  - SHA – Агенты здоровья проверяют метрики
  - QA – Агент каратина координирует работу SHA/EC
  - EC – Определяет метод принуждения
- **Сервер восстановления (Remediation)**
- Распространяет обновления, сигнатуры антивируса, и. т.д.

- **Network Policy Server**
  - NAP Server – проверяет метрики здоровья клиентов
  - SHV –проверяет ответы SHA
- **System Health Server**
- предоставляет SHV



Этапы внедрения NAP

- **Наблюдение и отчеты (Reporting Mode)**
- **Отложенное принуждение (Deferred Enforcement)**
- **Полное принуждение (Full Enforcement)**

Ресурсы:

- ✔ http://technet.microsoft.com/en-us/network/bb545879.aspx
- ✔ http://msdn.microsoft.com/en-us/library/aa369712(VS.85).aspx