Технологии контроля доступа к сети
Опыт внедрения

Случанко Кирилл
Ведущий инженер
KSluchanko@polikom.ru

ПОЛИКОМ ПРО

Поставка ПО и оборудования
ИТ-инфраструктура
Бизнес-приложения
ЦОД, сети, инженерная инфраструктура

Проблема

Наибольшая угроза – узлы, подключенные к внутренней сети:

- вирусы – широкие возможности для распространения
- шпионское ПО – прямой доступ к внутренней информации и учётным данным пользователей
- подключения гостей и подрядчиков – узлы, не подчиняющиеся установленным политикам безопасности
- ошибки или небрежность при физически подключениях – потенциальные бреши в безопасности или нарушение нормального функционирования систем

Идея

Проверка на соответствие конечных узлов установленным политикам безопасности:

- аутентификация конечных узлов и пользователей
- наличие антивируса, включая версию ПО и баз данных
- проверка версии ОС и установленных обновлений
- проверка конфигурации ОС (параметры реестра, версии и содержимое файлов)
- проверка состояния ОС (запущенные службы и процессы)

Доступ к сети предоставляется только после прохождения проверки и регулируется результатами такой проверки.

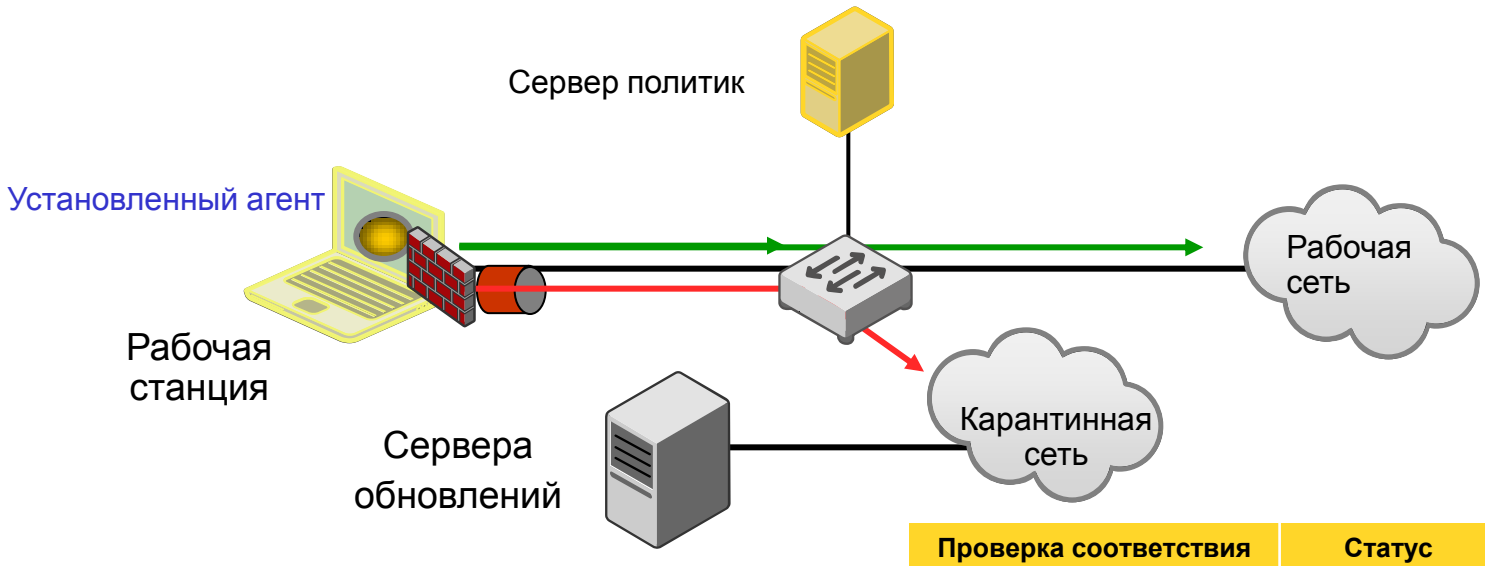
Как это работает?

Общие сведения

1. Локальное применение политик на конечной точке
2. Управление выдачей IP-адресов по протоколу DHCP – подсеть для конечной точки выбирается на основании результатов проверки
3. Шлюз в разрыве физического канала передачи данных – допустимые для конечного узла точки назначения и протоколы определяются по результатам проверки
4. Управление устройствами доступа (коммутаторами или точками беспроводного доступа) по протоколам IEEE 802.1x и RADIUS или SNMP

Как это работает?

Метод 1: Локальное применение политик



Клиент подключается к сети и проверяется на соответствие политикам

Установленный агент выполняет проверку компьютера

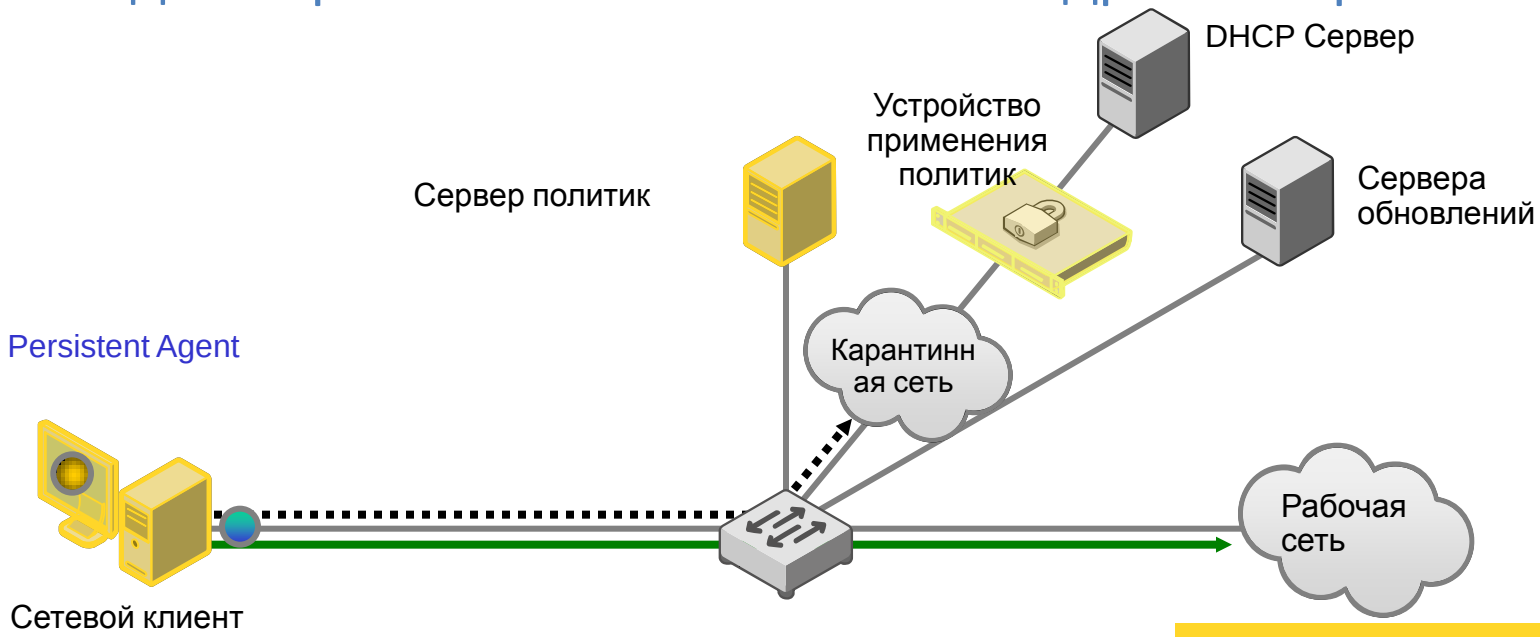
Проверка пройдена, компьютер допущен в «Рабочую сеть»

Проверка не прошла, компьютер перенаправлен в карантин

Проверка соответствия	Статус
Антивирус включён	✓
Антивирус обновлён	✓
Firewall включён	✓
ServicePack установлен	✓
Patch Updated	✓
Патчи не установлены	✘

Как это работает?

Метод 2: Управление назначением IP-адресов через DHCP



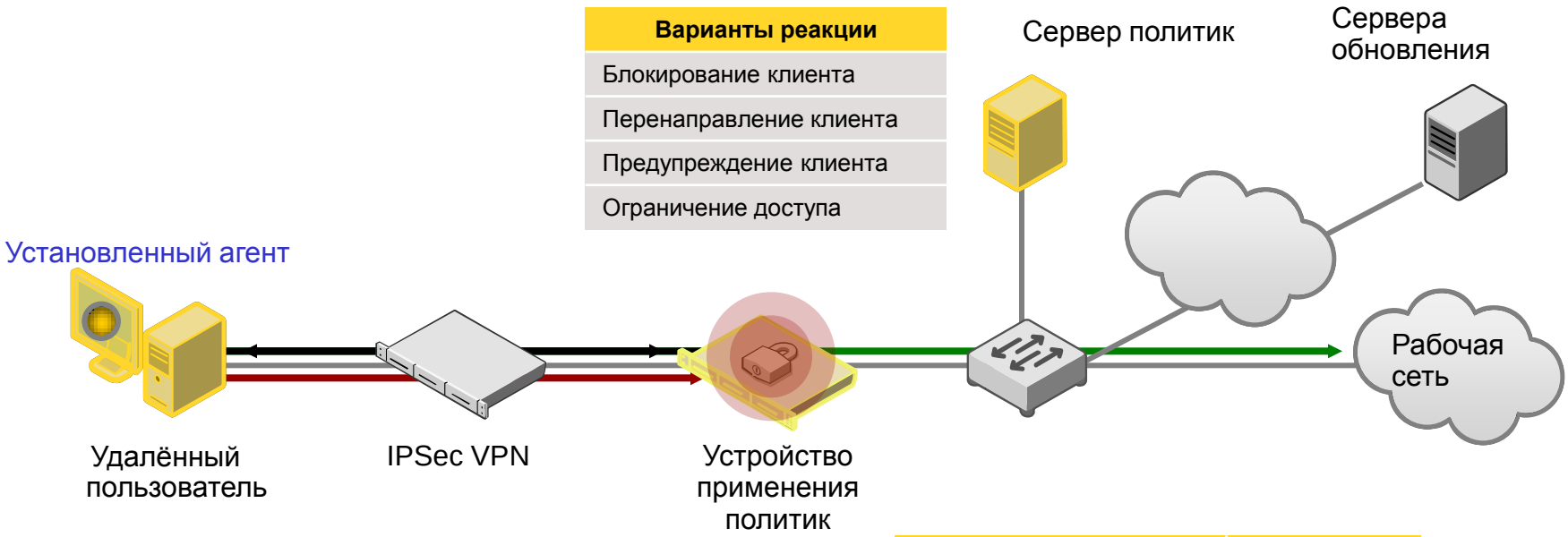
Проверка соответствия	Статус
Антивирус включён	✓
Антивирус обновлён	✓
Firewall включён	✓
ServicePack установлен	✓
Патчи установлены	✓

Клиент посылает DHCP request → УПП выдаёт «карантинный» IP; запрашивает состояние клиента и политику → УПП сравнивает политику и полученные от клиента данные → УПП выполняет DHCP release & renew на слиенте → Клиент получает адрес из рабочей сети

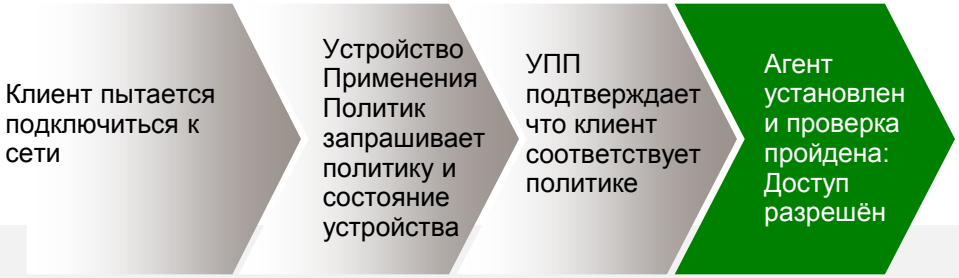
Как это работает?

Метод 3: Шлюз в разрыве физического канала

Варианты реакции
Блокирование клиента
Перенаправление клиента
Предупреждение клиента
Ограничение доступа

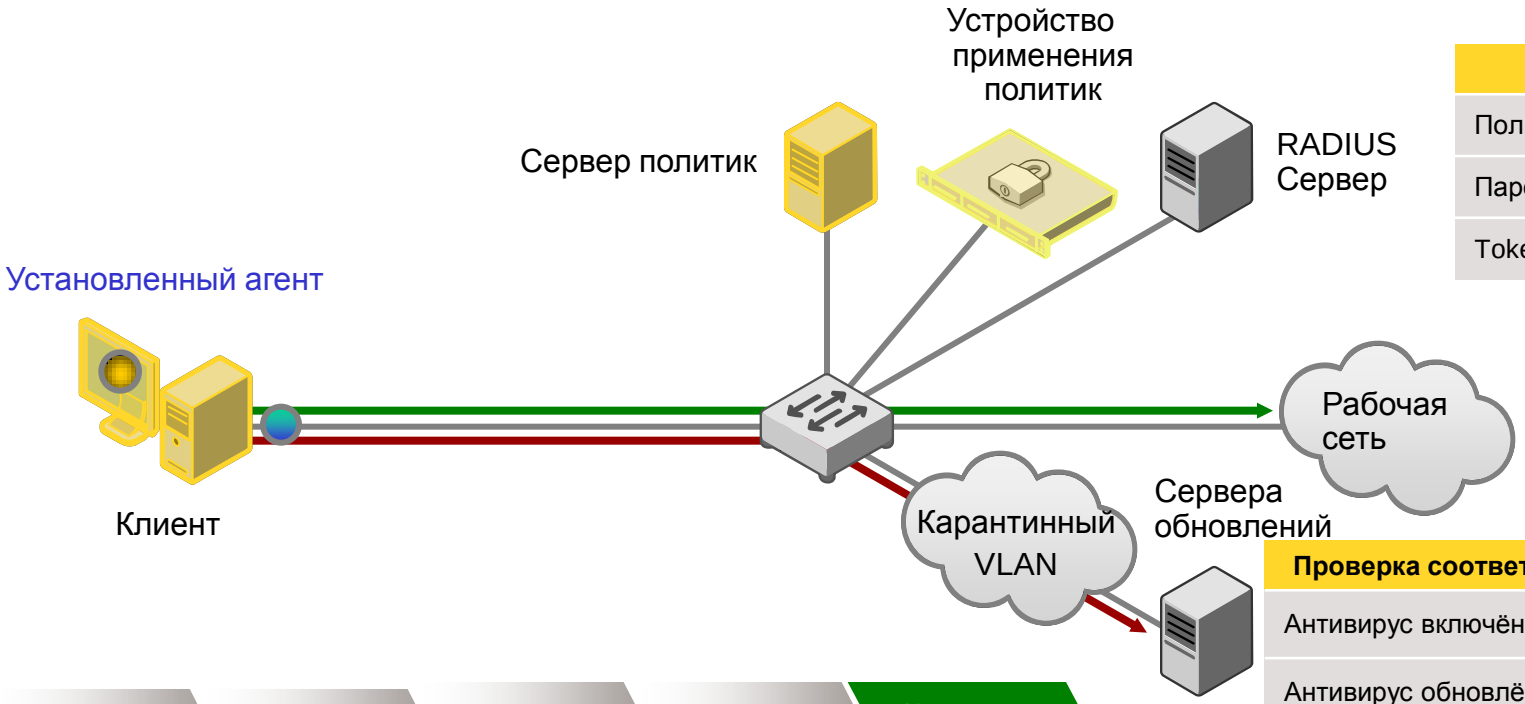


Проверка соответствия	Статус
Антивирус включён	✓
Антивирус обновлён	✓
Firewall включён	✓
ServicePack установлен	✓
Патчи установлены	✓



Как это работает?

Метод 4: Управление устройствами доступа



EAP	Status
Пользователь	✓
Пароль	✓
Token	✓

Проверка соответствия	Статус
Антивирус включён	✓
Антивирус обновлён	✓
Firewall включён	✓
ServicePack установлен	✓
Patch Updated	✓
Патчи не установлены	✘

1. Клиент подключается и посылает данные авторизации и состояние клиента через EAP
2. Коммутатор пересылает данные на УПП
3. УПП проверяет логин и пароль пользователя на RADIUS сервере
4. LAN Enforcer проверяет соответствует ли клиент политикам
   - Клиент соответствует политикам
   - Клиент не соответствует политикам

Системы контроля доступа к сети

Что мы можем предложить?

- Microsoft NAP
- Symantec NAC
- Cisco NAC

Существуют и другие решения (например, от Juniper Networks) – но их распространённость и доступность несколько ниже.

Системы контроля доступа к сети

Microsoft NAP

Плюсы:

- наиболее доступное решение – клиентская часть входит в комплект поставки Windows XP SP3 и выше, серверная часть (Network Policy Server) – в комплект поставки Windows Server 2003 R2 и выше
- использует открытые стандарты и протоколы
- относительная простота развёртывания и настройки

Минусы:

- поддержка только ОС Microsoft
- ограниченный список проверок
- ограниченный набор возможных реакций

Системы контроля доступа к сети

Symantec NAC

Плюсы:

- построено на открытых стандартах и протоколах
- широкий спектр проверок
- широкий набор реакций, допускающий добавление собственных вариантов реакций заказчиком
- наличие загружаемого агента
- поддержка различных ОС (часть - в процессе реализации)
- интеграция с Symantec Endpoint Protection

Минусы:

- необходимость дополнительного оборудования
- в некоторых сценариях неприменим

Системы контроля доступа к сети

Cisco NAC

Плюсы:

- тесная интеграция с активным сетевым оборудованием Cisco
- широкий спектр проверок
- широкий набор реакций, допускающий добавление собственных вариантов реакций заказчиком
- наличие загружаемого агента
- поддержка различных ОС

Минусы:

- необходимость дополнительного оборудования
- работает ТОЛЬКО с оборудованием Cisco (использует проприетарные расширения протокола SNMP)

Практические примеры

Подключения к «плоской сети»

1. Минимизация расходов: применение политик локально на конечных точках – **Symantec NAC, Microsoft NAP, Cisco NAC**
2. Минимизация затрат: управление выдачей IP-адресов по протоколу DHCP - **Microsoft NAP**
3. Стандартизация используемых систем: управление устройствами доступа - **Microsoft NAP, Symantec NAC, Cisco NAC**
4. Стандартизация используемых систем: управление устройствами доступа и/или применение политик на шлюзах - **Symantec NAC, Cisco NAC** (использование Microsoft NAP возможно – но только в комбинации с MS RRAS и продуктами на его основе, либо требует ручной доводки)

Практические примеры

Подключения удалённого доступа

1. Работа в разрыве физического канала связи – **Symantec NAC, Cisco NAC**
2. Управление устройствами доступа – Microsoft NAP (с оговорками)

Практические примеры

Управление устройствами доступа

1. Использование активного сетевого оборудования различных производителей – **Symantec NAC, Microsoft NAP**
2. Использование активного сетевого оборудования компании Cisco - **Cisco NAC, Symantec NAC, Microsoft NAP**
3. Использование IP-телефонии с подключением конечных устройств через IP-телефоны - **Cisco NAC**

Практические примеры

Обход аутентификации по MAC-адресу

Используется для подключения сетевых принтеров, сканеров и других устройств, для которых невозможна установка агента.

1. Использование общей группы для всех неуправляемых устройств - **Symantec NAC, Microsoft NAP, Cisco NAC**
2. Распределение устройств по группам – **Symantec NAC, Microsoft NAP, Cisco NAC (с оговорками)**

Заключение

Проблема выбора – что учитывать?

1. Основное – требуемая функциональность и состав используемого оборудования
2. Перспективы развития сетевой инфраструктуры
3. Цена – наименее важный фактор

При использовании только ОС Microsoft достаточно легко развернуть систему контроля доступа к сети на основе Microsoft NAP для оценки её функциональности и полезности в общем.

Благодарю за внимание!

Случанко Кирилл
Ведущий инженер
KSluchanko@polikom.ru

ПОЛИКОМ ПРО

Москва
тел. (495) 660 32 91
факс (495) 660 32 93

Санкт-Петербург
тел. (812) 325 84 00
факс (812) 320 56 86

www.polikom.ru