Ш

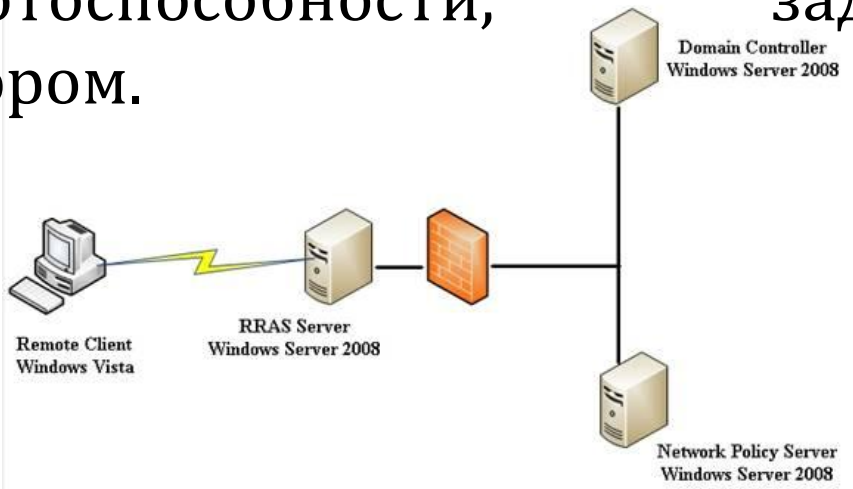
П Д

1 = Д

1 = С

Защита доступа к сети (NAP)

– это новый набор компонентов операционной системы в Windows Server® 2008, предоставляющий платформу, которая помогает обеспечивать соответствие клиентских систем в частной сети требованиям к работоспособности, заданным администратором.



Политики NAP определяют необходимое состояние конфигурации и обновления для операционной системы и критически важного программного обеспечения на клиентских компьютерах.

Например, они могут требовать, чтобы на компьютерах использовалось антивирусное программное обеспечение с новейшими сигнатурами, были установлены необходимые обновления операционной системы и включен индивидуальный брандмауэр.

Для чего нужна защита доступа к сети?

- Защита доступа к сети обеспечивает соблюдение требований к работоспособности, отслеживая и оценивая работоспособность клиентских компьютеров, когда они пытаются подключиться к сети или передать по ней данные.

Для кого предназначена эта возможность

Защита доступа к сети может заинтересовать администраторов сетей и систем, которым необходимо обеспечить соответствие клиентских компьютеров, подключающихся к сети, требованиям к работоспособности.

Возможности

- обеспечивать в локальной сети работоспособность настольных компьютеров, настроенных для использования протокола DHCP, подключающихся к сети через устройства проверки подлинности 802.1X или выполняющих обмен данными в соответствии с политиками NAP IPsec;

- обеспечивать соблюдение требований к работоспособности мобильных компьютеров при их повторном подключении к корпоративной сети;

- определять работоспособность мобильных компьютеров, принадлежащих посетителям и партнерам организации, и ограничивать доступ к ресурсам организации для этих компьютеров.

- проверять соответствие политикам и работоспособность неуправляемых домашних компьютеров, подключающихся к корпоративной сети через сервер виртуальной частной сети со службами маршрутизации и удаленного доступа;

Ключевые процессы защиты доступа к сети

- **Проверка соответствия политике**

Для анализа состояния работоспособности клиентских компьютеров сервер политики сети использует средства проверки работоспособности системы.

- **Применение защиты доступа к сети и ограничение доступа к сети**

Защиту доступа к сети можно настроить так, чтобы клиентские компьютеры, не соответствующие политикам, не могли получить доступ к сети или могли получить только ограниченный доступ.

Используя указанные параметры, можно ограничить доступ, отложить ограничение доступа или разрешить доступ.

- **Разрешить полный доступ к сети**
- **Разрешить полный доступ к сети в ограниченное время**
- **Разрешить ограниченный доступ**

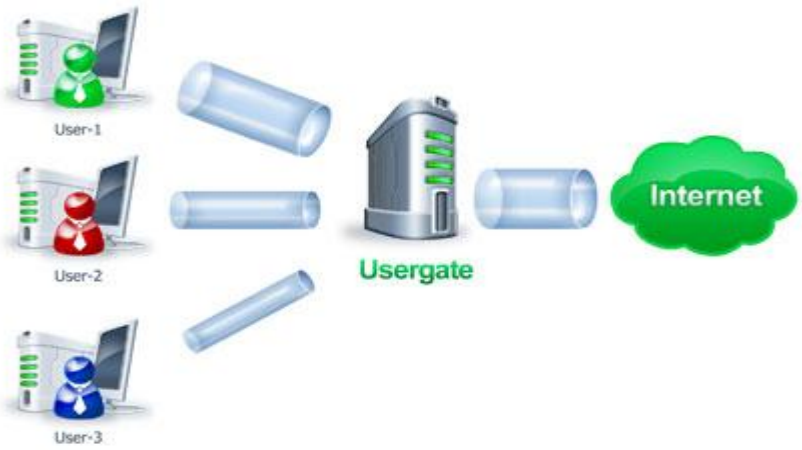
- **Обновление**

Клиентские компьютеры, не соответствующие требованиям и помещенные в сеть с ограниченным доступом, могут пройти процедуру обновления.

Обновлением называется процесс обновления клиентского компьютера для приведения его характеристик в соответствие с текущими требованиям к работоспособности.

Способы применения защиты доступа к сети

- Защита доступа к сети может разрешить полный или ограниченный доступ к сети либо запретить доступ с учетом состояния работоспособности клиентского компьютера. Клиентские компьютеры, не соответствующие политикам работоспособности, могут быть автоматически обновлены для приведения в соответствие им.



Технология защиты доступа к сети применяет политики работоспособности для следующих элементов:

- трафик, защищенный с помощью протокола IPsec;
- управление доступом к проводной и беспроводной сети с использованием портов 802.1X;
- виртуальные частные сети (VPN) с маршрутизацией и удаленным доступом;
- аренда и обновление адресов IPv4 протокола DHCP;

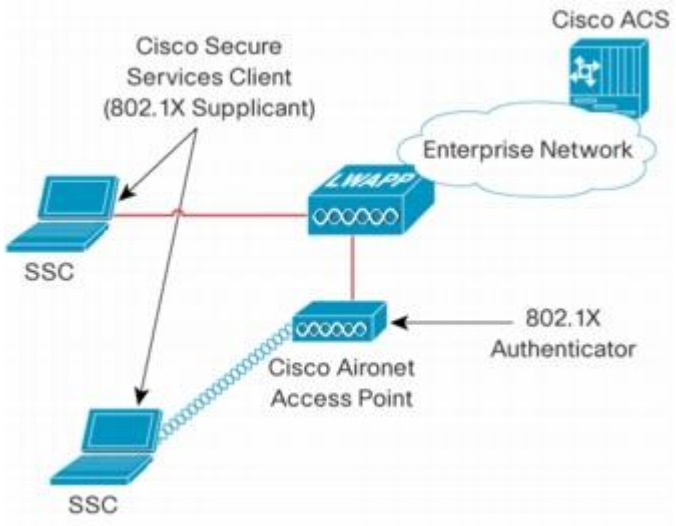
- подключения к серверу шлюза служб терминалов;

Применение защиты доступа к сети для соединений IPsec

Применение защиты доступа к сети для трафика, защищенного с помощью протокола IPsec, обеспечивается с помощью сервера сертификатов работоспособности, сервера центра регистрации работоспособности, сервера политики сети и клиента принудительной защиты доступа к сети с помощью IPsec.

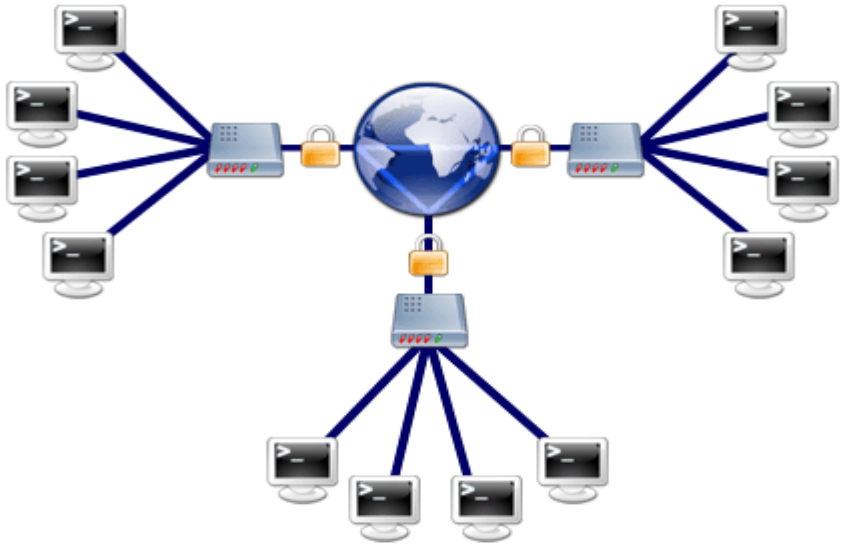
Применение защиты доступа к сети для стандарта безопасности 802.1X

- Применение защиты доступа к сети для управления доступом к сети с использованием портов 802.1X реализуется с помощью сервера политики сети и клиентского компонента принудительной защиты доступа к сети EAPHost.



Применение защиты доступа к сети для виртуальных частных сетей

- Применение защиты доступа к сети для виртуальных частных сетей реализуется с помощью серверного и клиентского компонентов принудительной защиты доступа к сети для виртуальных частных сетей.



Применение защиты доступа к сети для протокола DHCP

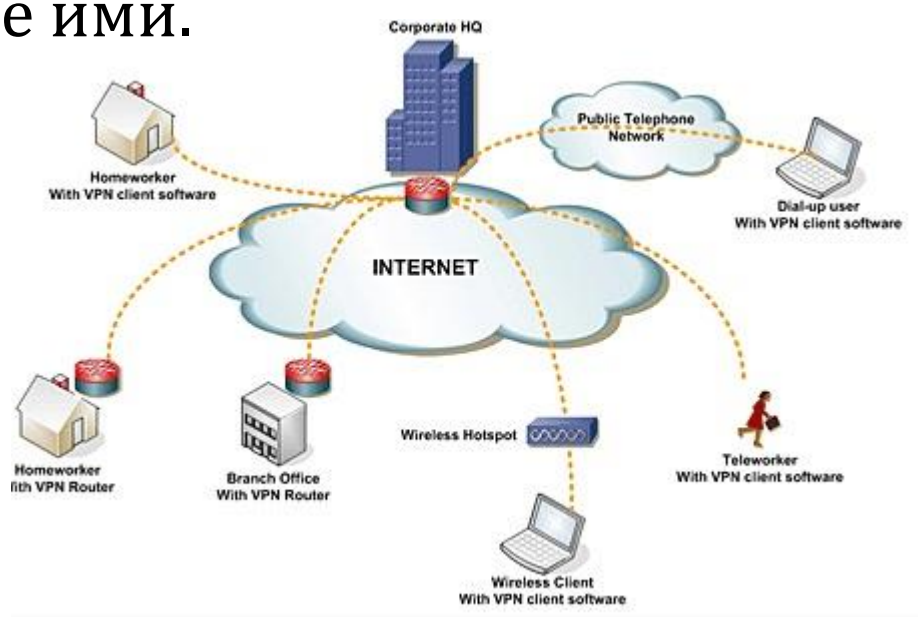
- Применение защиты доступа к сети для протокола DHCP реализуется с помощью серверного и клиентского компонентов принудительной защиты доступа к сети DHCP и сервера политики сети. Система ограничений DHCP позволяет серверу политики сети и DHCP-серверам применять политику работоспособности, когда компьютер предпринимает попытку арендовать или обновить адрес IPv4.

Применение защиты доступа к сети для шлюза служб терминалов

- Применение защиты доступа к сети для шлюза служб терминалов реализуется с помощью серверного и клиентского компонентов принудительной защиты доступа к сети для шлюза служб терминалов.
- Используя защиту доступа к сети для шлюза служб терминалов, сервер шлюза служб терминалов может применять политику работоспособности к клиентским компьютерам, пытающимся подключиться к внутренним корпоративным ресурсам через сервер шлюза служб терминалов.

Комбинированные подходы

- Каждый способ применения защиты доступа к сети имеет свои сильные и слабые стороны. Сочетание разных способов позволяет объединить их преимущества. Однако развертывание нескольких способов применения защиты доступа к сети может затруднить управление ими.



Клиентские компоненты защиты доступа к сети

- **Агент работоспособности системы**
- **Агент защиты доступа к сети**
- **Клиент принудительной защиты доступа к сети**
- **Состояние работоспособности**

Серверные компоненты защиты доступа к сети

- **Сервер политики работоспособности защиты доступа к сети**
- **Сервер администрирования NAP**
- **Средства проверки работоспособности системы**
- **Сервер принудительной защиты доступа к сети**
- **Точка NAP**
- **Сервер состояния работоспособности**
- **Сервер обновлений**
- **Отклик о состоянии работоспособности**

”ОБС”

1 = Н

”ЬЮӨ

3 = Р