

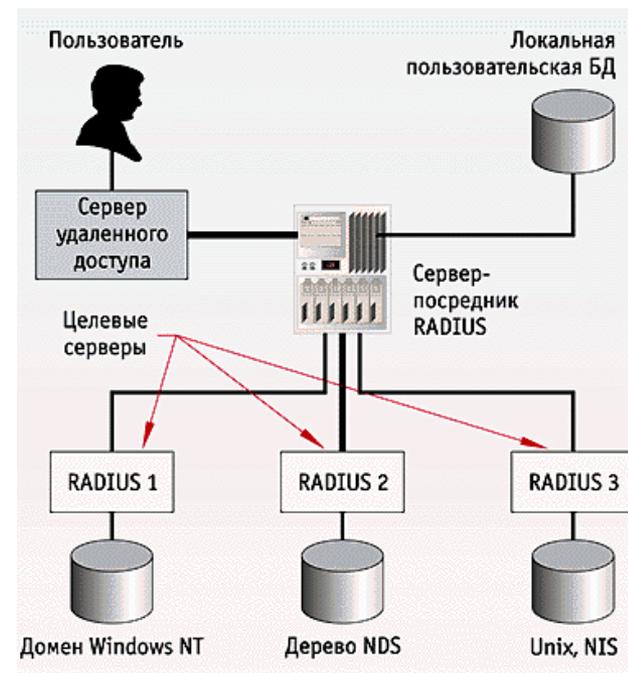
Сервер политики сети



Сервер политики сети позволяет создавать и применять политики доступа к сети на уровне организации для обеспечения работоспособности клиентов, а также выполнения проверки подлинности и авторизации запросов на подключение.



Сервер политики сети МОЖНО использовать в качестве **RADIUS-прокси** для перенаправления запросов на подключение на сервер политики сети или другие **RADIUS-серверы**, настроенные в группах удаленных RADIUS-серверов.

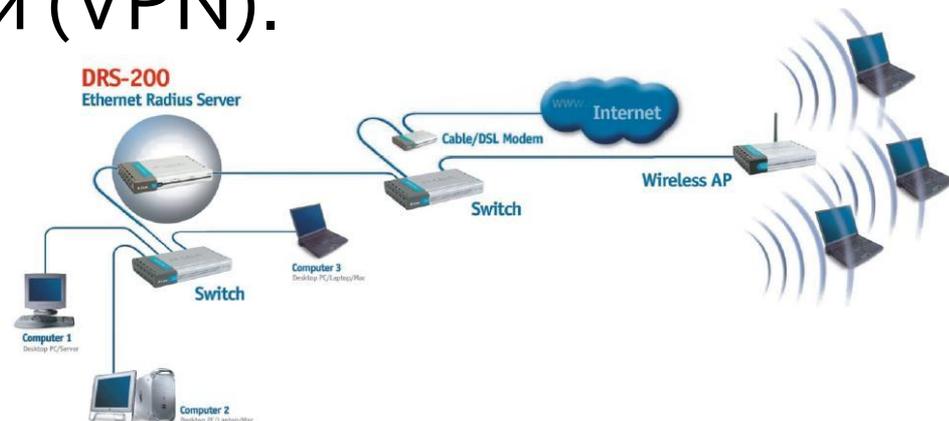


Сервер политики сети позволяет централизованно настраивать политики проверки подлинности, авторизации и работоспособности клиента при предоставлении доступа к сети и управлять этими политиками с помощью трех возможностей:

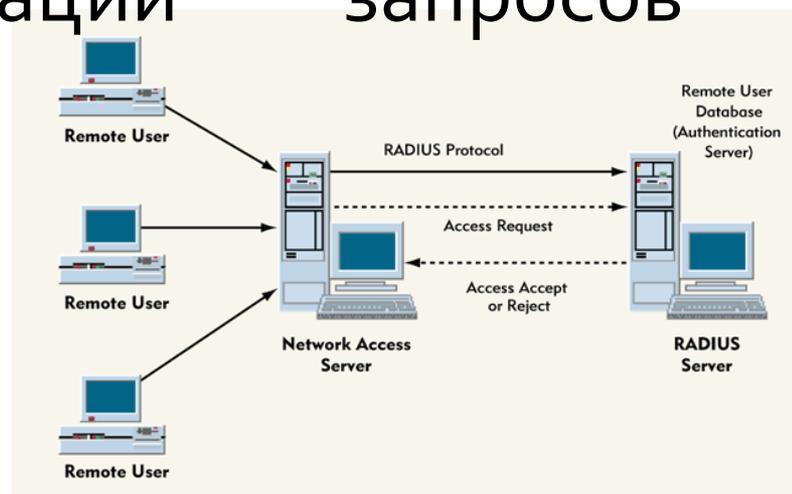
- 1. RADIUS server**
- 2. RADIUS proxy**
- 3. Network Access Protection (NAP) policy server**

RADIUS server

Сервер политики сети централизованно выполняет проверку подлинности, авторизацию и учет для беспроводных подключений, подключений по коммутаторам с проверкой подлинности, подключений удаленного доступа и подключений по виртуальной частной сети (VPN).



При использовании сервера политики сети в **качестве RADIUS-сервера**, серверы доступа к сети, такие как точки беспроводного доступа и VPN-серверы, настраиваются как RADIUS-клиенты на сервере политики сети. Кроме того, настраиваются политики сети, используемые сервером политики сети для авторизации запросов на подключение.



Сервер политики сети позволяет использовать разнородный набор оборудования для беспроводного доступа, удаленного доступа, сетей VPN и коммутирования.

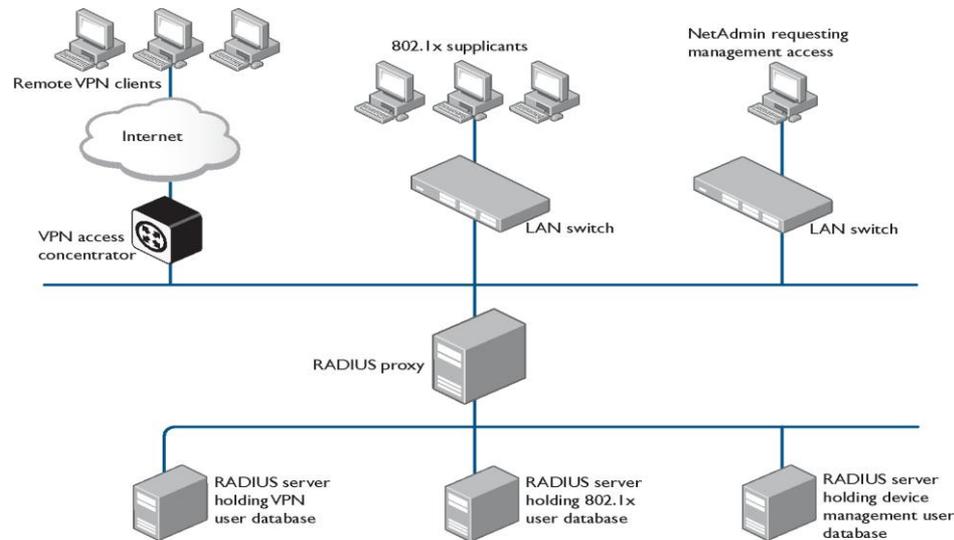
Сервер политики сети можно использовать со службой маршрутизации и удаленного доступа, которая доступна в операционных системах Microsoft Windows



RADIUS proxy

- Если сервер политики сети используется в качестве RADIUS-прокси, необходимо настроить политики запросов на подключение, которые определяют, какие запросы на подключение сервер политики сети будет перенаправлять на другие RADIUS-серверы, а также на какие конкретно RADIUS-серверы будут перенаправляться эти запросы.

С помощью сервера политики сети организации могут передать инфраструктуру удаленного доступа на внешнее управление поставщику услуг, в то же время сохраняя контроль над проверкой подлинности, авторизацией и учетом пользователей.



Конфигурации сервера политики сети могут создаваться для следующих сценариев:

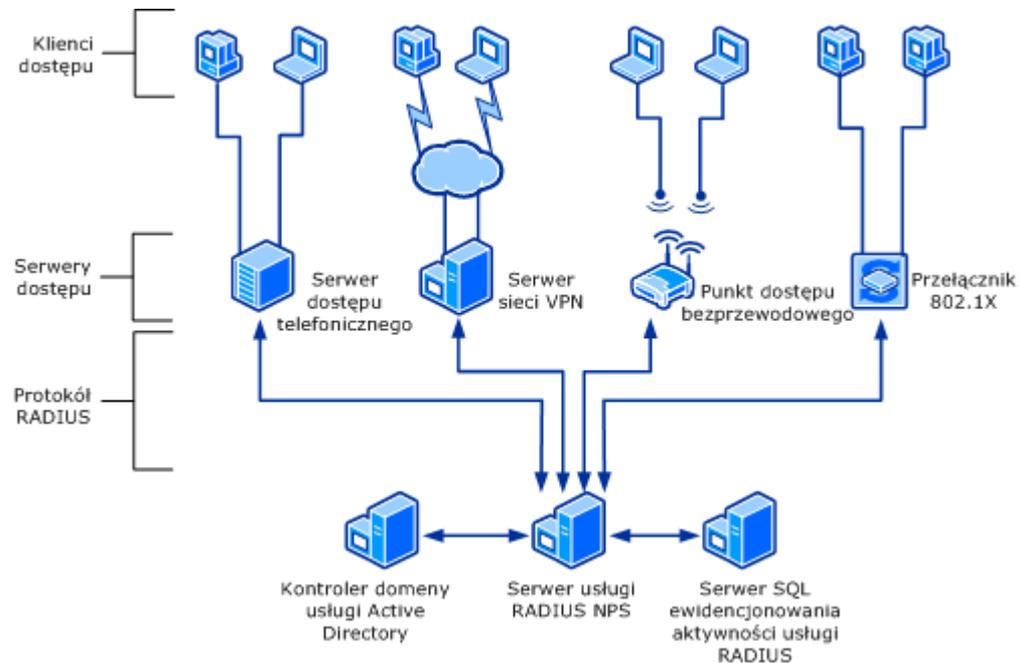
- Беспроводной доступ
- Подключение удаленного доступа или виртуальной частной сети в организации.
- Удаленный доступ или беспроводной доступ, обеспечиваемый внешней организацией
- Доступ к Интернету
- Доступ с проверкой подлинности к ресурсам внешней сети для деловых партнеров

Network Access Protection (NAP) policy server

- Если сервер политики сети настроен в качестве сервера политик защиты доступа к сети, сервер политики сети оценивает состояния работоспособности, направляемые клиентскими компьютерами с поддержкой защиты доступа к сети, которые пытаются подключиться к сети. Сервер сетевых политик, на котором настроена защита доступа к сети, выступает в качестве RADIUS-сервера, выполняя проверку подлинности и авторизацию запросов на подключение.

На сервере политики сети можно настроить политики и параметры защиты доступа к сети, в том числе устройства проверки работоспособности системы, политику работоспособности и группы серверов обновлений, которые обеспечивают обновление конфигурации клиентских компьютеров в соответствии с сетевой политикой организации.

Примеры конфигураций RADIUS-сервера и RADIUS-прокси



NPS as a RADIUS server

Сервер политики сети настроен как RADIUS-сервер, единственной настроенной политикой является установленная по умолчанию политика запросов на подключение, а все запросы на подключение обрабатываются локальным сервером политики сети. Сервер политики сети может выполнять проверку подлинности и авторизацию пользователей, учетные записи которых находятся в домене данного сервера или в доверенных доменах.

NPS as a RADIUS proxy

Сервер политики сети настроен как RADIUS-прокси, который перенаправляет запросы на подключение в группы удаленных RADIUS-серверов в двух разных доменах без доверия. Установленная по умолчанию политика запросов на подключение удаляется, а вместо нее создаются две новые политики запросов на подключение, предусматривающие перенаправление запросов в каждый из двух доменов без доверия. В этом примере сервер политики сети не обрабатывает запросы на подключение на локальном сервере.

NPS as both RADIUS server and RADIUS proxy

В дополнение к установленной по умолчанию политике запросов на подключение, которая предусматривает локальную обработку запросов, создается новая политика запросов на подключение, предусматривающая их перенаправление на сервер политики сети или другой RADIUS-сервер, находящийся в домене без доверия. Вторая политика имеет имя **Прокси**

NPS as a RADIUS server with remote accounting servers.

Локальный сервер политики сети не настроен на ведение учета, а установленная по умолчанию политика запросов на подключение изменена таким образом, чтобы RADIUS-сообщения учета перенаправлялись на сервер политики сети или иной RADIUS-сервер в группе удаленных RADIUS-серверов.

NPS with remote RADIUS to Windows user mapping

Сервер политики сети выступает как в качестве RADIUS-сервера, так и в качестве RADIUS-прокси для каждого отдельного запроса на подключение, перенаправляя запрос на проверку подлинности на удаленный RADIUS-сервер и одновременно выполняя авторизацию с использованием локальной учетной записи пользователя Windows.

Такая конфигурация реализуется путем установки атрибута **Сопоставление удаленного сервера RADIUS пользователю Windows** в качестве условия политики запросов на подключение. (Кроме того, на RADIUS-сервере необходимо создать локальную учетную запись пользователя с тем же именем, что и удаленная учетная запись, по которой будет выполняться проверка подлинности удаленным RADIUS-сервером.)

Сервер политики защиты доступа к сети

Компонент защиты доступа к сети включен в Windows Vista®, Windows® 7, Windows Server® 2008 и Windows Server® 2008 R2. Он помогает обеспечить защиту доступа к частным сетям, гарантируя соответствие параметров клиентских компьютеров действующим в сети организации политикам работоспособности при разрешении этим клиентам доступа к сетевым ресурсам.

Системные администраторы определяют политики работоспособности сети и создают эти политики с использованием компонентов защиты доступа к сети, которые доступны на сервере политики сети или поставляются другими компаниями (в зависимости от реализации защиты доступа к сети).

Политики работоспособности могут иметь такие характеристики, как требования к программному обеспечению, требования к обновлениям системы безопасности и требования к параметрам конфигурации. Защита доступа к сети применяет политики работоспособности, проверяя и оценивая работоспособность клиентских компьютеров.