ФАКТОР-ТС

АЛЬБОМ РЕШЕНИЙ ПРИКЛАДНЫХ ЗАДАЧ ПРИ ПОСТРОЕНИИ ЗАЩИЩЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА БАЗЕ

DIONIS DPS

МОСКВА 2023

ОГЛАВЛЕНИЕ

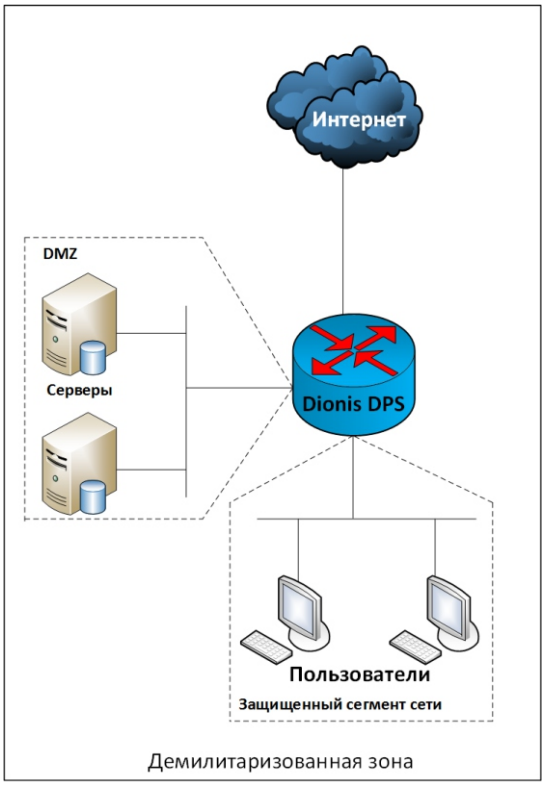
1 БЕЗОПАСНЫЙ ИНТЕРНЕТ

1.1.1 Демилитаризованная зона

ДМЗ — сегмент сети, содержащий общедоступные сервисы, которые отделены от частных сегментов сети.

В качестве общедоступного сервиса может выступать, например, веб сервис (обеспечивающий его сервер), который физически размещен в локальной сети (Интранет).
Сервер должен отвечать на любые запросы из внешней сети (Интернет), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа.

Цель ДМЗ — добавить дополнительный уровень безопасности, который позволит минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в ДМЗ.



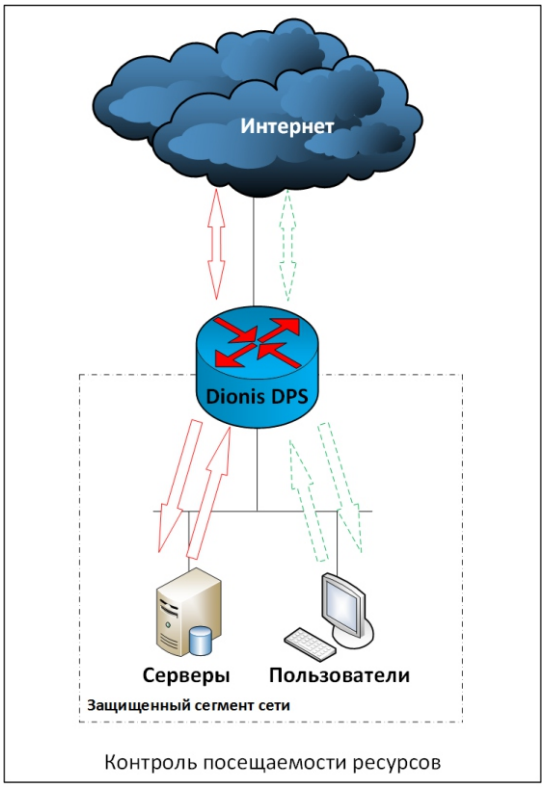
Демилитаризованная зона

1.1.2 Контроль посещаемости ресурсов

Для реализации данной задачи используется служба Proxy server — служба, позволяющая клиентам выполнять косвенные запросы к другим сетевым службам.

Сначала клиент подключается к прокси серверу и запрашивает какой либо ресурс (например, http://factor-ts.ru), расположенный на другом сервере. Затем прокси сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях если прокси имеет свой кеш).

Прокси сервер позволяет вести записи обо всех запросах, проходящих через него, а также может работать в прозрачном режиме, что обеспечивает анонимность контроля.

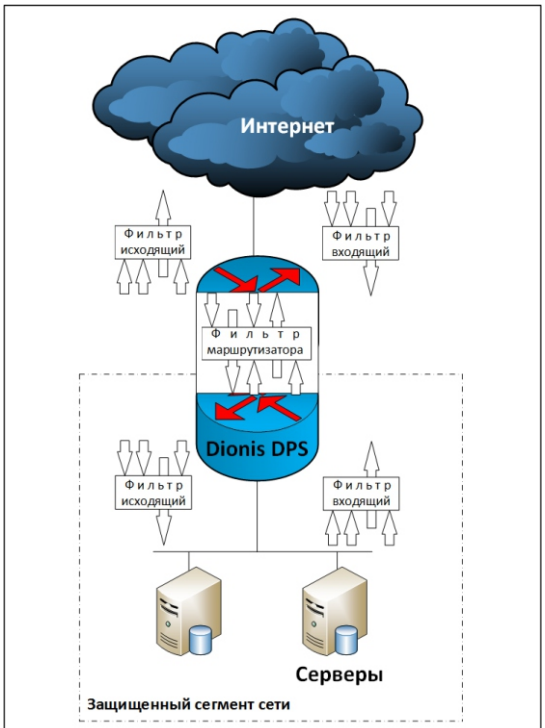


Контроль посещаемости ресурсов

1.1.3 Межсетевое экранирование

ПАК Dionis DPS обеспечивает безопасность сети и позволяет управлять прохождением трафика через интерфейсы маршрутизатора, обеспечивая фильтрацию принимаемых и передаваемых пакетов по различным критериям (адресам отправителя и получателя, протоколам, номерам портов, содержимому пакета).

Правила фильтрации объединяются в IP-списки контроля доступа (ip access-list). Списки контроля доступа могут быть применены к конкретным интерфейсам с учетом направления трафика.

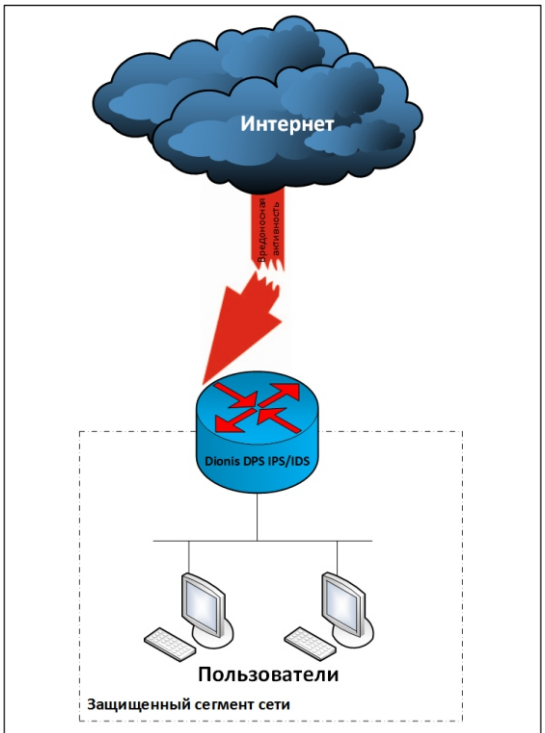


Межсетевое экранирование

1.1.4 Система обнаружения и предотвращения атак

Система обнаружения и предотвращения вторжений (IDS/IPS) входит в состав изделий Dionis DPS, но лицензируется отдельно. Это система сетевой безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Системы IPS можно рассматривать как расширение систем обнаружения вторжений (IDS), так как задача отслеживания атак остается одинаковой. Однако они отличаются тем, что IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак.
Возможные реакции со стороны IPS: блокировка потоков трафика в сети, сброс соединений, выдача сигналов оператору. Также IPS могут выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами.



Система обнаружения и предотвращения атак

1.1.5 Сокрытие адресного пространства корпоративной сети

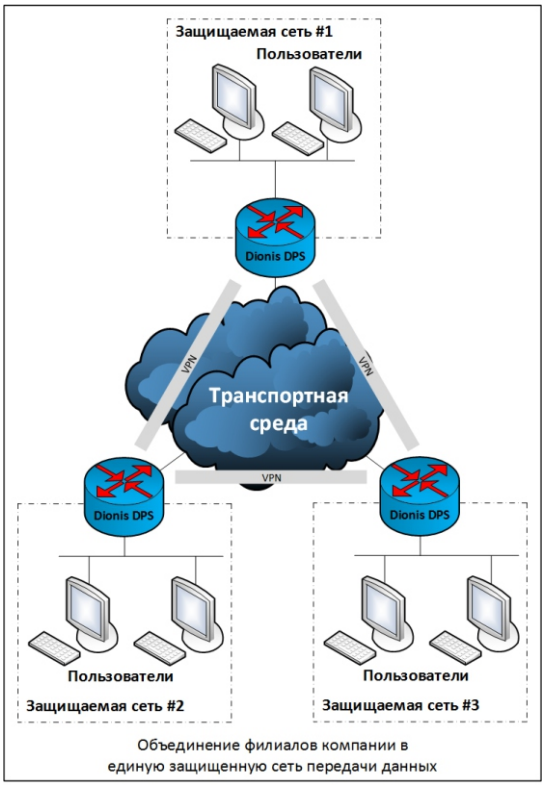
Поддержка технологии NAT/PAT позволяет скрывать внутреннюю структуру защищаемых сегментов сети при передаче открытого и закрытого трафика.

Сокрытие внутренней структуры защищаемой сети осуществляется путем преобразования IP-адресов внутренней сети (фиктивных адресов) в адрес (-а) внешней сети (реальные адреса) — для исходящих датаграмм (транзитных пакетов).

Сокрытие адресного пространства корпоративной сети

2 ОБЪЕДИНЕНИЕ ФИЛИАЛОВ КОМПАНИИ В ЕДИНУЮ ЗАЩИЩЕННУЮ СЕТЬ ПЕРЕДАЧИ ДАННЫХ

Для объединения филиалов компании в единую защищенную сеть применяются VPN-туннели (ГОСТ). Для построения географически распределенной сети организации может использоваться как асимметричная ключевая схема с возможностью интеграции в существующую сеть (IpSec), так и асимметричная ключевая схема (DiSec)..



Объединение филиалов компании в единую защищенную сеть передачи данных

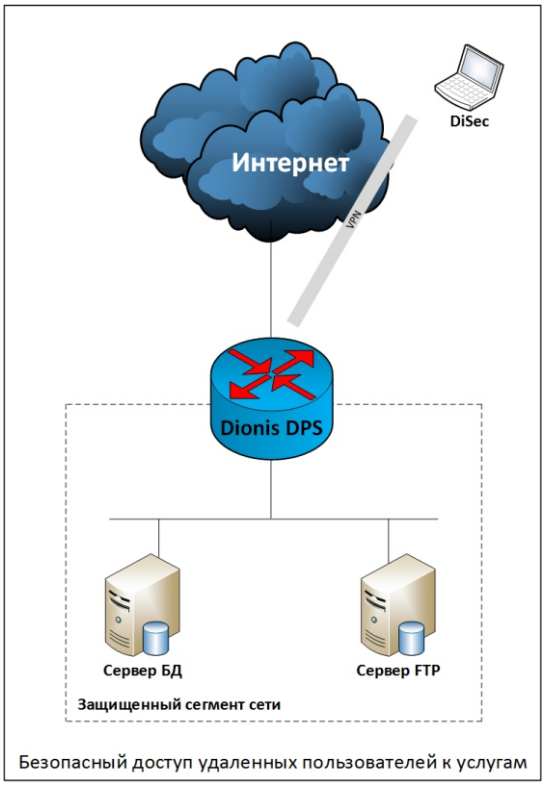
3 БЕЗОПАСНЫЙ ДОСТУП УДАЛЕННЫХ ПОЛЬЗОВАТЕЛЕЙ К УСЛУГАМ

Обеспечение безопасного доступа удаленных пользователей реализовано по протоколам DiSec, IpSec, OpenVPN.

Специальное программное обеспечение DiSec, работающее на платформах Windows 7, 8, 8.1, предназначено для обеспечения криптографической защиты данных, передаваемых по открытым каналам связи с использованием стека протоколов TCP/IP, а также для обеспечения доступа удаленных пользователей к ресурсам сети, защищенным Dionis DPS.

В ПО DiSec реализованы два протокола защиты данных, что обеспечивает гибкий подход к реализации защиты.

Поддерживаемые протоколы: протокол IKE версии 1 (RFC2407-2409) и ESP (RFC4303), с использованием российских криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.

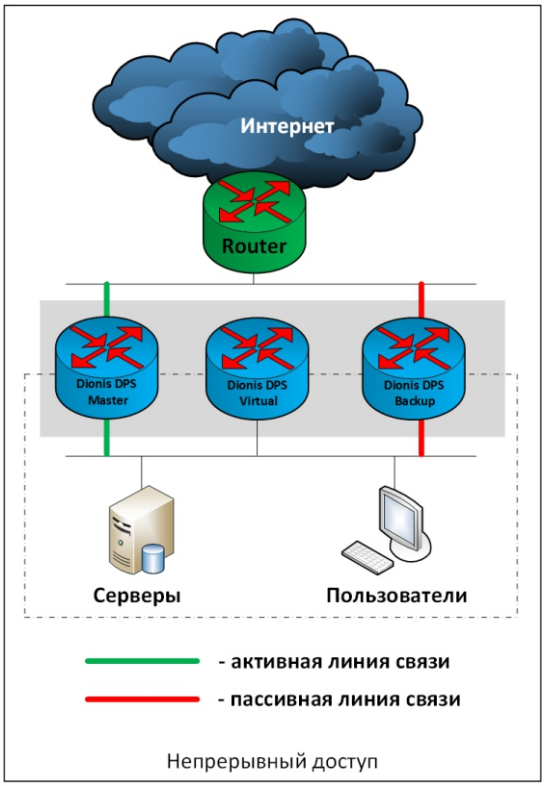


Безопасный доступ удаленных пользователей к услугам

4 ПОВЫШЕНИЕ НАДЕЖНОСТИ ДОСТУПА К УСЛУГАМ

4.1 Непрерывный доступ

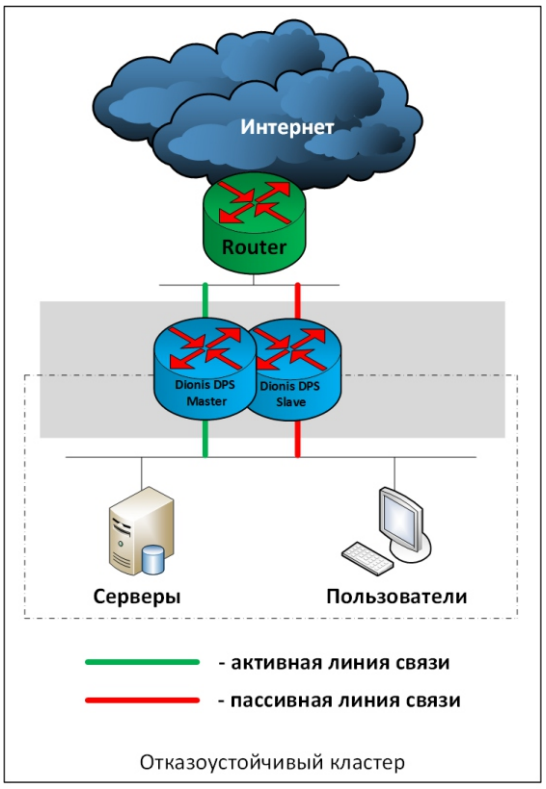
Для обеспечения надежности в данной реализации применяется сетевой протокол VRRP, предназначенный для увеличения доступности/надежности маршрутизаторов, выполняющих роль шлюза по умолчанию. Это достигается путем объединения группы маршрутизаторов в один виртуальный маршрутизатор и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для всех компьютеров в сети.



Непрерывный доступ

4.2 Отказоустойчивый кластер

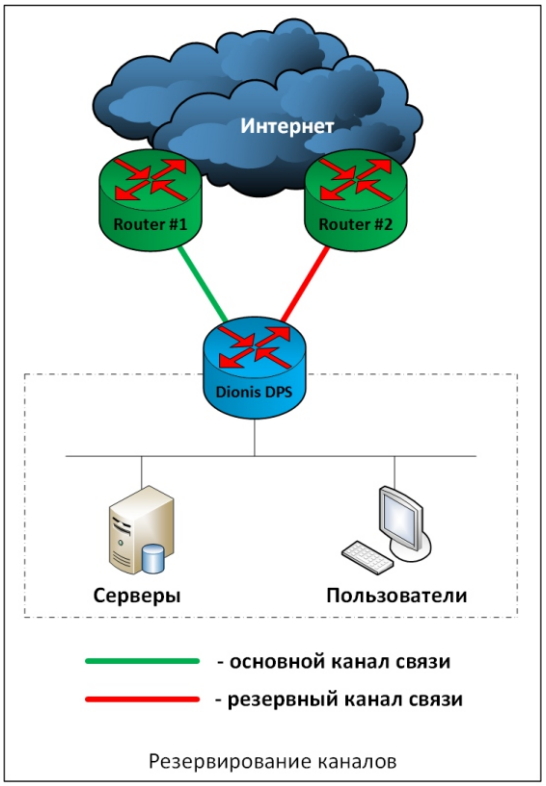
Кластер — отказоустойчивое решение для постоянного доступа к услугам. Для решения данной задачи используются два одинаковых маршрутизатора Dionis DPS. В каждый момент времени активен только один из них (master). Второй находится в резерве (slave). В случае выхода из строя основного маршрутизатора (master) все функции основного маршрутизатора возьмет на себя slave. Как только master возобновит работу, slave перейдет в режим ожидания. Также маршрутизаторы Dionis DPS поддерживают протокол VRRP.



Отказоустойчивый кластер

4.3 Резервирование каналов

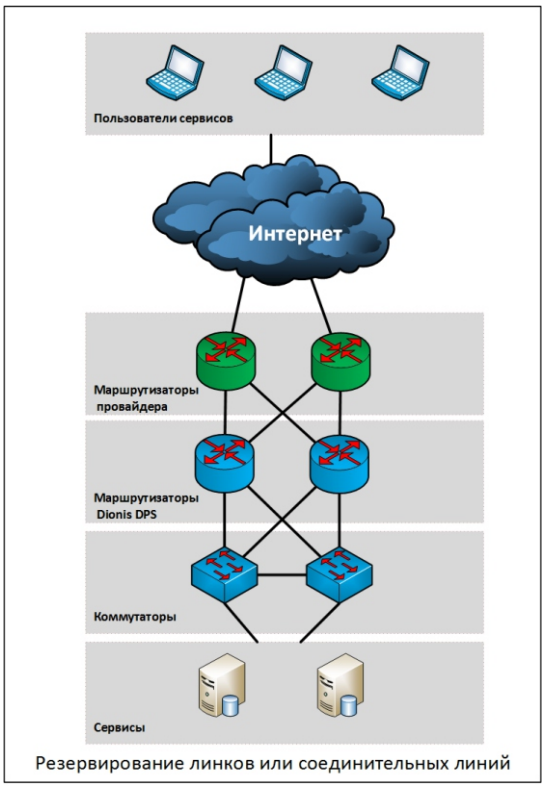
Резервирование каналов связи — это добавление дополнительных (избыточных) линий связи с целью избавления от узких мест, то есть единственных каналов передачи данных, от работоспособности которых зависит функционирование сети. В Dionis DPS реализовано несколько вариантов резервирования каналов: при помощи протоколов динамической маршрутизации (RIP, OSPF, BGP) или при помощи маршрутизации на основе политик (PBR) с контролем состояния маршрута.



Резервирование каналов

4.4 Резервирование линков или соединительных линий

Комплексное решение. Достигается путем каскадирования и дублирования каждого уровня сети с построением физических и логических дублирующих связей, требующих скоординированной настройки маршрутизаторов Dionis DPS, управляемых коммутаторов и маршрутизаторов провайдера.

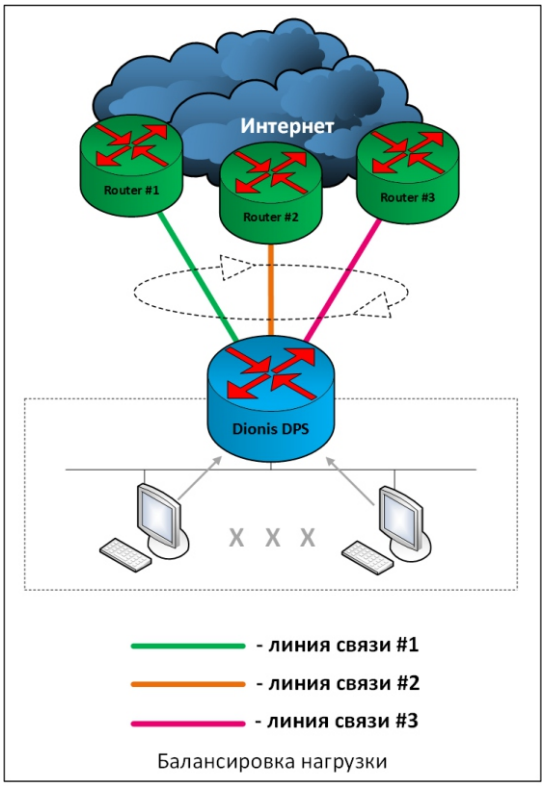


Резервирование линков или соединительных линий

ПРЕДОСТАВЛЕНИЕ УСЛУГ С ГАРАНТИРОВАННЫМ КАЧЕСТВОМ

5.1 Балансировка нагрузки

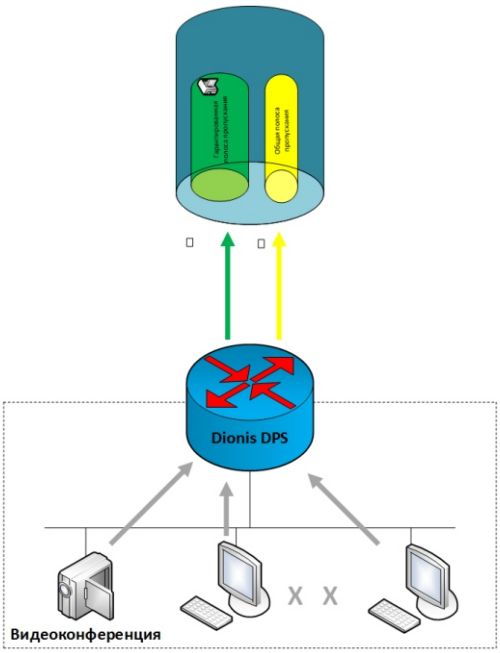
Метод распределения трафика между несколькими сетевыми устройствами (например, провайдерами) с целью оптимизации использования ресурсов, сокращения времени обслуживания запросов, горизонтального масштабирования кластера (динамическое добавление/удаление устройств), а также обеспечения отказоустойчивости (резервирования).



Балансировка нагрузки

5.2 Выделение полосы пропускания пользователю

Данная задача возникает при необходимости обеспечения компьютеру или сервису в локальной сети гарантированной скорости работы в Интернете. Решить такую задачу помогает технология управления полосой пропускания, позволяющая распределять ресурсы канала на основе нескольких параметров, в том числе IP-адреса вашего компьютера. Механизм дает возможность зарезервировать гарантированную полосу пропускания для каждого компьютера и сервиса в локальной сети.

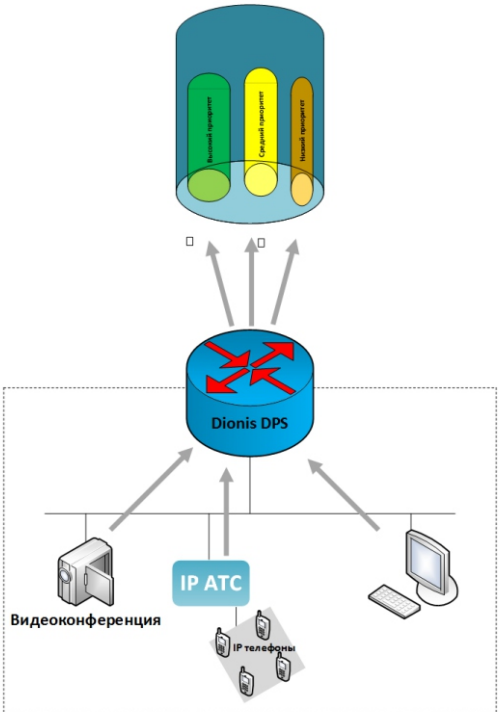


Выделение полосы пропускания пользователю

5.3 Приоритизация

Реализованный в Dionis DPS механизм приоритизации трафика позволяет обеспечить качество обслуживания на основе распределения ресурсов в ядре сети и определенных классификаторов, а также ограничений на границе сети, комбинируемых с целью предоставления требуемого качества услуг.

В этой модели вводится разделение трафика по классам, для каждого из которых определяется свой уровень QoS. QoS состоит из управления формированием трафика (классификация пакетов) и управления политикой (распределение ресурсов, маркировка, управление интенсивностью). Данный механизм является наиболее подходящим примером «умного» управления приоритетом трафика.

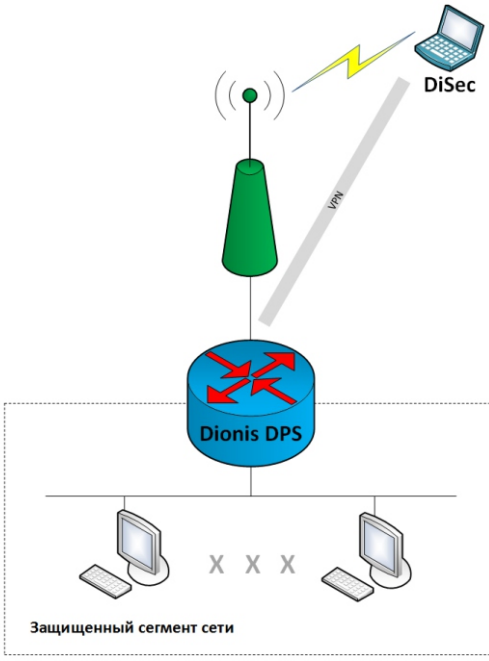


Приоритизация

6 ЗАЩИТА БЕСПРОВОДНЫХ СЕТЕЙ

6.1 VPN-туннели через WiFi и 3G

С помощью программы DiSec возможно защищенное подключение клиентов беспроводной сети (Wi-Fi, 3G) к выделенным сегментам защищаемой сети (подключение к Dionis DPS) с возможностью разграничения прав доступа.

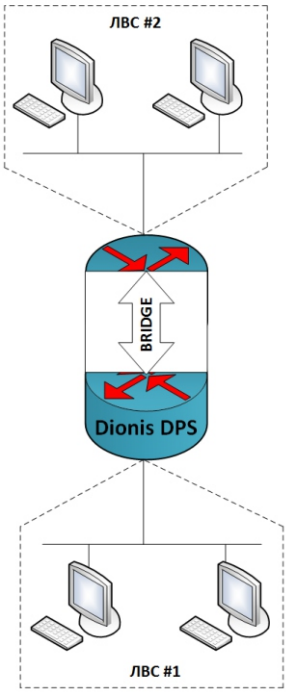


Защита беспроводных сетей

7 РАНЖИРОВАНИЕ СЕТЕЙ

7.1 Разграничение сетей на канальном уровне без изменения пространства

Существует возможность объединения на канальном уровне сегментов локальных сетей в единую сеть, как в рамках локального офиса, так и для удаленных офисов и абонентов.

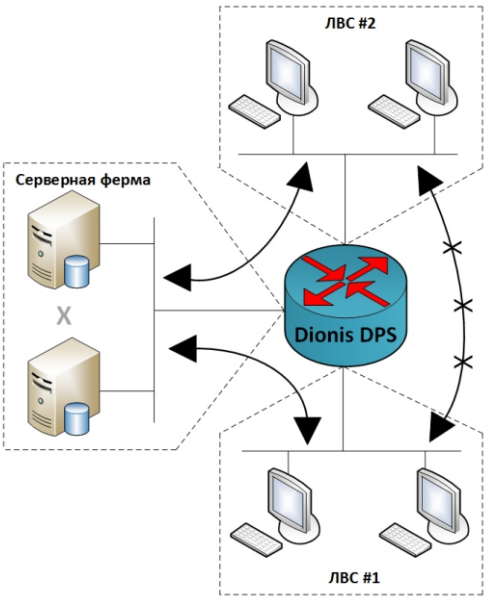


Объединение сетей на канальном уровне без изменения адресного пространства

7.2 Разделение сетей на физическом уровне с ограничением

Разделение сетей на физическом уровне (например, подсистемами различных подразделений предприятия).

Dionis DPS позволяет разделять сети разных подразделений на уровне сетевых интерфейсов, что дает возможность дифференцированного управления правилами безопасности для каждого сегмента сети.

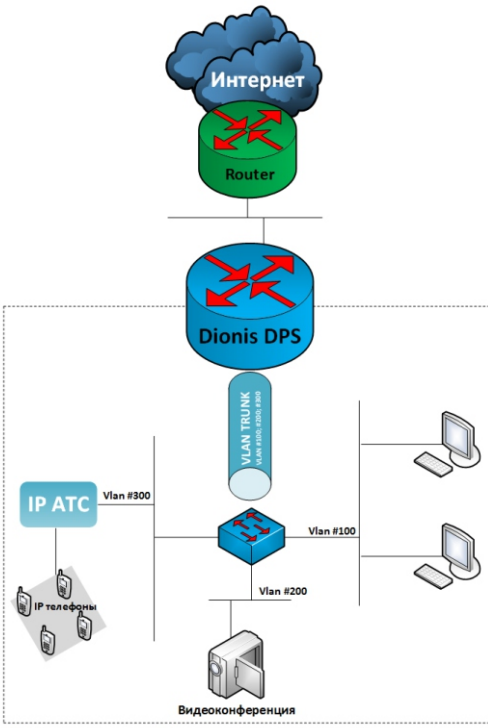


Разделение сетей на физическом уровне с ограничением

7.3 Разделение сетей в зависимости от принадлежности

Разделение доступа между информационными подсистемами в рамках одного сегмента сети.

Dionis DPS обеспечивает независимое управление всеми информационными подсистемами на межсетевом уровне.

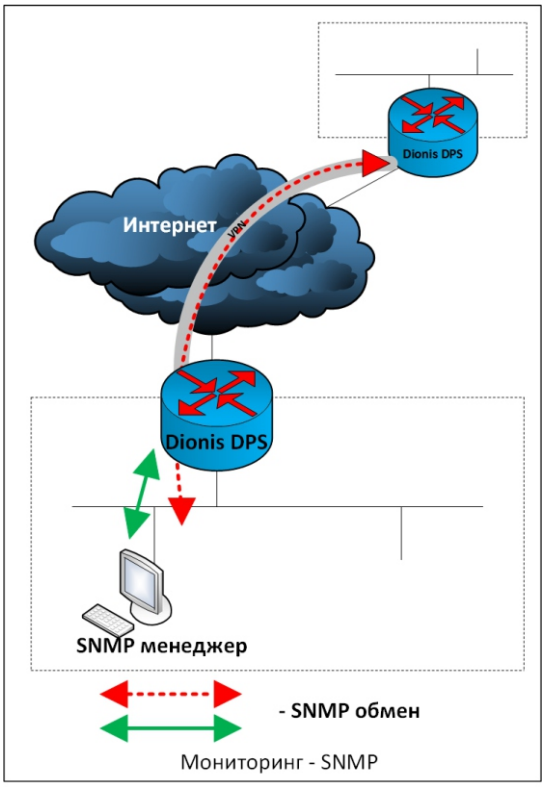


Разделение сетей в зависимости от принадлежности

8 БЫСТРОЕ ОБНАРУЖЕНИЕ СБОЕВ СЕТИ

8.1 Мониторинг-SNMP

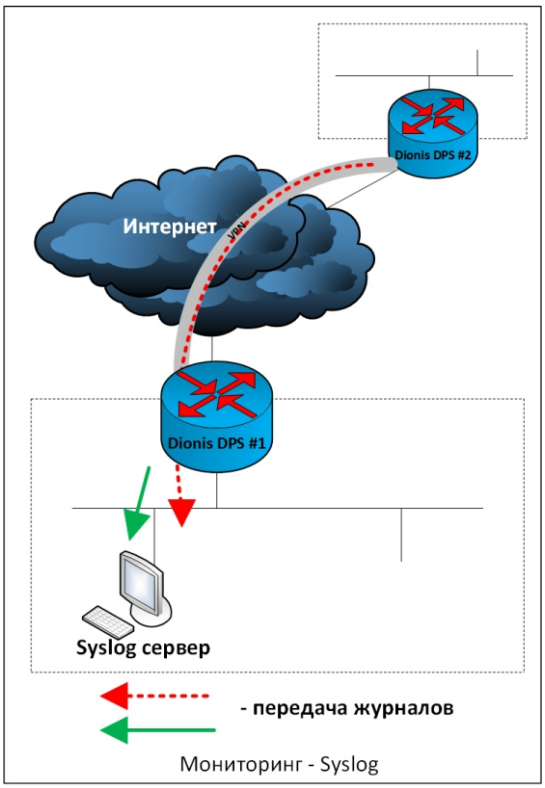
При использовании протокола SNMP менеджера на административном компьютере выполняется отслеживание или управление группой хостов или устройств в компьютерной сети. На Dionis DPS есть постоянно запущенная программа, называемая «агентом», которая через SNMP передает информацию менеджеру. На основании этой информации можно отслеживать работоспособность всей системы.



Мониторинг - SNMP

8.2 Мониторинг-Syslog

Syslog — служба для передачи всех системных событий об управлении и работе Dionis DPS.

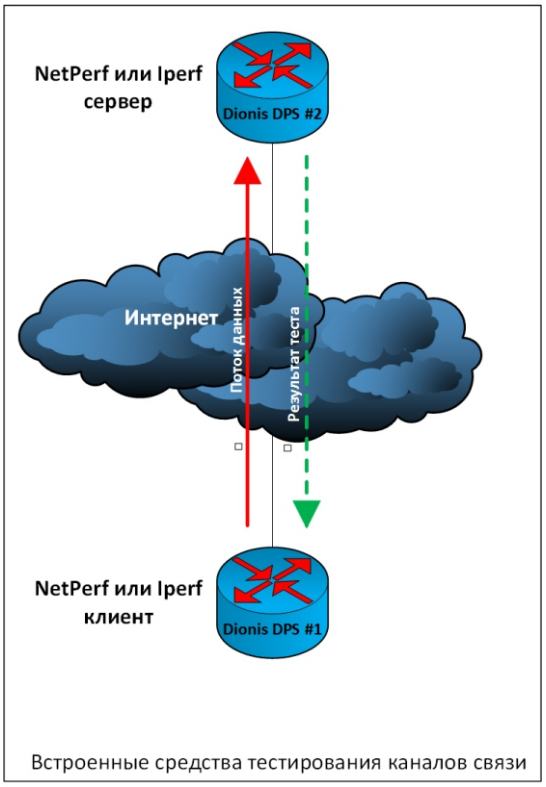


Мониторинг - Syslog

9 АНАЛИЗ И КОНТРОЛЬ

9.1 Встроенные средства тестирования каналов связи

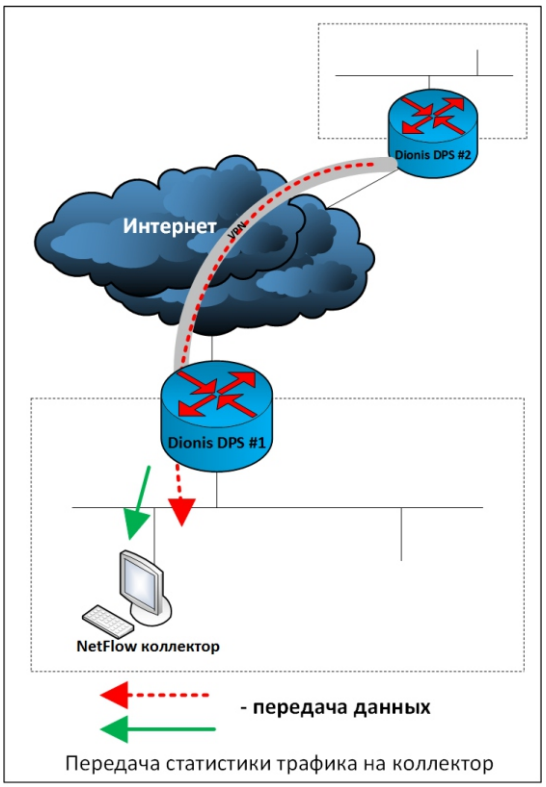
Службы NetPerf и Iperf в системе Dionis DPS позволяют получить мгновенную информацию о пропускной способности сети.



Встроенные средства тестирования каналов связи

9.2 Передача статистики трафика на коллектор

Протокол Netflow, поддерживаемый Dionis DPS, предназначен для учета и последующего анализа сетевого трафика на уровне сеансов, он делает запись о каждой транзакции TCP/IP.



Передача статистики трафика на коллектор

Москва, 1-й Магистральный пр-д,
дом 11, строение 1

dps.factor-ts.ru
sales@factor-ts.ru
+7 (495) 644 31 30