

# Характеристики Dionis DPS

## 1. Маршрутизация трафика

- 1.1. Статическая маршрутизация.
- 1.2. Динамическая маршрутизация по протоколам RIP, OSPF, BGP.
- 1.3. Маршрутизация на основе политик с контролем состояния (keepalive) маршрутов
- 1.4. Статическая маршрутизация мультикаст-трафика.
- 1.5. Маршрутизация мультикаст-трафика по протоколам PIM, DVMRP, IGMP.
- 1.6. Объединение нескольких интерфейсов в коммутированный Bridge-интерфейс.
- 1.7. Объединение нескольких интерфейсов в агрегированный интерфейс повышенной пропускной способности.
- 1.8. VLAN-интерфейсы с возможностью работы с транковыми (тегированными) портами коммутатора.
- 1.9. Дублирование (зеркалирование) трафика на отдельный интерфейс.
- 1.10. Туннельные интерфейсы с поддержкой шифрования и имитозащиты IP-трафика.

## 2. Средства организации VPN

- 2.1. VPN-туннели с изделиями семейства «Dionis» шифрованием и имитозащитой IP-трафика по алгоритмам ГОСТ 28147-89 на симметричных ключах, с контролем состояния (keepalive) туннеля.
- 3.2. VPN-туннели с изделиями семейства «Dionis» с шифрованием и имитозащитой передаваемых IP-пакетов и двусторонней криптографической аутентификацией по алгоритмам ГОСТ 281470-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, в инфраструктуре открытых ключей (сертификаты X.509), с контролем состояния (keepalive) туннеля.
- 3.3. Поддержка технологии «NAT Traversal» для VPN-туннелей с изделиями семейства «Dionis» и клиентским ПО семейства «Disec».
- 3.4. VPN-туннели по протоколу GRE/GRETAG с контролем состояния (keepalive) туннеля.
- 3.5. VPN-туннели по протоколу PPTP/L2TP с контролем состояния (keepalive) туннеля.
- 3.6. VPN-туннели по протоколу OpenVPN с контролем состояния (keepalive) туннеля.

## 4. Межсетевой экран

- 4.1. Фильтрация трафика по MAC-адресам, IP-адресам, TCP/UDP-портам, TCP-флагам, полю «ToS/DSCP» IP-заголовка, содержимому любого поля IP-пакета.
- 4.2. Фильтрация трафика по расписанию.
- 4.3. Фильтрация трафика с контролем состояния соединений (Statefull Firewall).
- 4.4. Ограничение числа соединений с одного IP-адреса.
- 4.5. Соккрытие внутренней структуры ЛВС: трансляция пакетов (SNAT, DNAT, PAT, Masquerade).
- 4.6. Создание статических ARP-записей.
- 4.7. Проxy-сервер для протоколов HTTP/FTP с «прозрачным» режимом работы.
- 4.8. Система обнаружения и предотвращения вторжений (IDS/IPS).

## **5. Отказоустойчивость**

- 5.1. Поддержка работы в режиме отказоустойчивого аппаратного кластера (активный/пассивный) с сохранением состояния сессий при переходе на резерв.
- 5.2. Агрегирование сетевых интерфейсов в отказоустойчивом режиме (активный/пассивный).
- 5.3. Поддержка работы в отказоустойчивом режиме по протоколу VRRP.

## **6. Качество сервиса**

- 6.1. Классификация трафика по MAC-адресам, IP-адресам, TCP/UDP-портам, полю «ToS/DSCP» IP-заголовка, полю «CoS» Ethernet-заголовка.
- 6.2. Маркировка трафика в поле «ToS/DSCP» IP-заголовка и в поле «CoS» Ethernet-заголовка.
- 6.3. Установка приоритета обработки для трафика разных классов.
- 6.4. Предоставление гарантированной полосы пропускания для трафика разных классов.
- 6.5. Режим шифрования VPN-туннелей, исключающий нарушение порядка следования пакетов.
- 6.6. Поддержка механизма уведомления о заторах без отброса пакетов (ECN).
- 6.7. Поддержка механизма управления размером TCP MSS (Path MTU Discovery).

## **7. Мониторинг и диагностика**

- 7.1. Выдача информации о состоянии устройства и сетевых интерфейсах по протоколу SNMP.
- 7.2. Выдача информации о трафике по протоколу NetFlow.
- 7.3. Выдача журналов работы устройства по протоколу Syslog.
- 7.4. Поддержка протокола обнаружения оборудования LLDP.
- 7.5. Регистрация и учёт событий, срабатываний фильтров, с поддержкой механизма «тревоги» и уведомлением по электронной почте.
- 7.6. Средства сетевой диагностики (ping, traceroute, whois).
- 7.7. Средства отладки с контролем прохождения IP-пакетов через маршрутизатор и сохранением дампов пакетов.
- 7.8. Средства тестирования канала связи (netperf, lperf).
- 7.9. Средства мониторинга в реальном времени состояния интерфейсов и загрузки системы.
- 7.10. Отражатель UDP-пакетов для поддержки работы средств контроля за соблюдением уровня сервиса (SLA).

## **8. Средства управления**

- 8.1. Управление по протоколам Telnet, SSH через интерфейс командной строки.
- 8.2. Встроенный Telnet и SSH клиент.
- 8.3. Управление по протоколу HTTP через Web-интерфейс управления.
- 8.4. Ролевая модель управления.
- 8.5. Задание времени действия учетных записей в ролевой модели.

## **9. Дополнительные возможности**

- 9.1. DHCP сервер и клиент.
- 9.2. DNS-сервер.
- 9.3. NTP сервер и клиент.
- 9.4. Контроль целостности ПО.
- 9.5. Средства обновления ПО и резервного копирования.
- 9.6. Поддержка множества версий ПО и конфигураций на одном устройстве.
- 9.7. Пробная (экспериментальная) загрузка с возможностью автоматического отката на резервную копию.