



ФАКТОРТС



ПАК DIONIS DPS

Решение по защите
финансового сектора на базе
ПАК DIONIS DPS

МОСКВА 2024







О компании

Компания «Фактор-ТС», организованная в 1992 году, специализируется на разработке, производстве, внедрении и сопровождении программных и аппаратных средств защиты информации под торговой маркой DIONIS. Компания предлагает заказчикам решения по организации защищенных информационно-телекоммуникационных систем (ИТС). В частности, ООО «Фактор-ТС» поставляет оборудование и для финансового сектора, так как в современном мире данный сегмент наиболее уязвим и подвержен неправомерным действиям злоумышленников.

Изделия производства компании «Фактор-ТС» (маршрутизаторы, криптомаршрутизаторы, межсетевые экраны, клиентские средства защиты и др.) сертифицированы по требованиям ФСТЭК России и ФСБ России по самым высоким уровням защищенности и используются для организации безопасного информационного обмена. Функционал ПАК DIONIS DPS позволяет решать задачи разной степени сложности: от предоставления безопасного доступа в интернет сотрудникам организации до объединения множества филиалов предприятия в единую защищенную сеть с системой обнаружения и предотвращения вторжений.

Реализованные проекты в финансовом секторе

Ак Барс
Банк



Основные возможности ПАК DIONIS DPS:

- | | |
|--|---|
|  маршрутизация трафика, резервирование каналов связи; |  работа в сложных погодных условиях; |
|  средства защиты информации, сертифицированные ФСБ России для построения VPN; |  защищенный доступ мобильных абонентов; |
|  межсетевое экранирование и безопасный интернет; |  протоколирование событий и система мониторинга; |
|  отказоустойчивый кластер и резервирование; |  система обнаружения и предотвращения вторжений. |

Решения продуктов ПАК DIONIS DPS позволяют организовывать защищенные сети банкоматов и платежных терминалов. Для этого на границе сети финансового учреждения устанавливаются высокопроизводительные криптомаршрутизаторы, поддерживающие защиту передачи данных (при помощи построения защищенных VPN-туннелей), а также систему обнаружения/предотвращения вторжений. Для защиты банкоматов может использоваться компактный криптомаршрутизатор, защищающий каналы связи между основным шлюзом и точкой подключения или клиент удаленного доступа, обеспечивающий конфиденциальность передачи информации и ее защиту, а также надежно защищающий работу с корпоративными данными через Интернет.

Основные преимущества:



- собственное производство и разработка программно-аппаратных комплексов; сертифицированных ФСБ и ФСТЭК России;
- техническая поддержка и сопровождение проектов на всей территории РФ;
- разветвленная партнерская сеть по всей территории РФ;
- опыт реализации и сопровождения проектов федерального масштаба;
- реализация СКЗИ под любой класс защищенности от конфиденциальной информации до ГТ.

Сертификаты и реестры:



Сертификат ФСТЭК
ИТ.МЭ.А4.ПЗ
ИТ.МЭ.Д4.ПЗ
ИТ.СОВ.С4.ПЗ



Сертификат ФСБ
Уровень СКЗИ
КС1, КС3



Реестр
отечественного
программного
обеспечения.



**Минпромторг
России**



ФАКТОР-ТС

+7 (495) 644 31 30 | www.dps.factor-ts.ru

Перечень оборудования ПАК DIONIS DPS и их сравнительная таблица

	DPS-1003S/1003SD	DPS-1004S	DPS-2000	DPS-3000	DPS-4000	DPS-5000	DPS-6000	DPS-7000
max скорость маршрутизации, Мбит/с	2 800	3 800	7 600	13 000	19 600	39 700	109 000	120 000
max скорость шифрования, Мбит/с	100	200	500	1 400	2 300	2 500	4700	8000
max скорость в режиме Firewall, Мбит/с	1200	1 000	4 100	9 400	15 000	25 000	80 000	90 000
max кол-во конкурентных сессий	100 000	500 000	5 000 000	10 000 000	20 000 000	30 000 000	60 000 000	60 000 000
max кол-во интерфейсов	3	4	7	9	9	25	50	50
max кол-во IpSec-туннелей (ГОСТ)	10	5	50	200	300	1000	1500	2000
max кол-во Disec-туннелей (ГОСТ)	10	5	100	300	800	1500	2000	2500
Рекомендуемое max кол-во узлов в ЛВС	20	10	100	200	400	500	1000	2000
Производительность в режиме IPS/IDS, Мбит/с	нет	140	1100	2700	4500	6000	15000	20000
Поддержка отказоустойчивого кластера	да	да	да	да	да	да	да	да
max кол-во дополнительных модулей	нет	нет	нет	нет	нет	3	6	6
Поддержка модуля 8x1000Base-T (4x1000Base-T)	нет	нет	нет	4x1000Base-T	4x1000Base-T	да	да	да
Поддержка модуля 8xSFP1000 (Base-SX/LX)	нет	нет	нет	4xSFP1000	4xSFP1000	да	да	да
Поддержка модуля 2 x SFP+ (10G Base-SR/LR)	нет	нет	нет	нет	да	да	да	да
Поддержка модуля 4 x SFP+ (10G Base-SR/LR)	нет	нет	нет	нет	нет	да	да	да
Поддержка модуля 2 x 40GbE QSFP+	нет	нет	нет	нет	нет	нет	да	да
Подключения монитора (VGA) и клавиатуры	да	нет	да	да	да	да	нет	нет
Конструктив	Десктоп	Десктоп	RM19"1U	RM19"1U	RM19"1U	RM19"1U	RM19"2U	RM19"2U
Охлаждение	Пассивное	Активное	Активное	Активное	Активное	Активное	Активное	Активное
Напряжение питания, В	12	12	220	220	220	220	220	220
Тип блока питания	Внешний	Внешний	Встроен	Встроен	Встроен	2-й встр.	2-й встр.	2-й встр.
Поддержка двойного блока питания	нет	нет	нет	нет	нет	да	да	да
Габариты, мм (ШxВxГ)	106x30x85	165x43x105	484x44x399	484x44x399	484x44x399	438x44x483	438x88x595	438x88x595

Варианты поставки



Наличие сертификата ФСБ

КСЗ

Комплектация FW	нет
Комплектация FWC-КСЗ	да
Комплектация FW-IPS	нет
Комплектация FWC-КСЗ-IPS	да



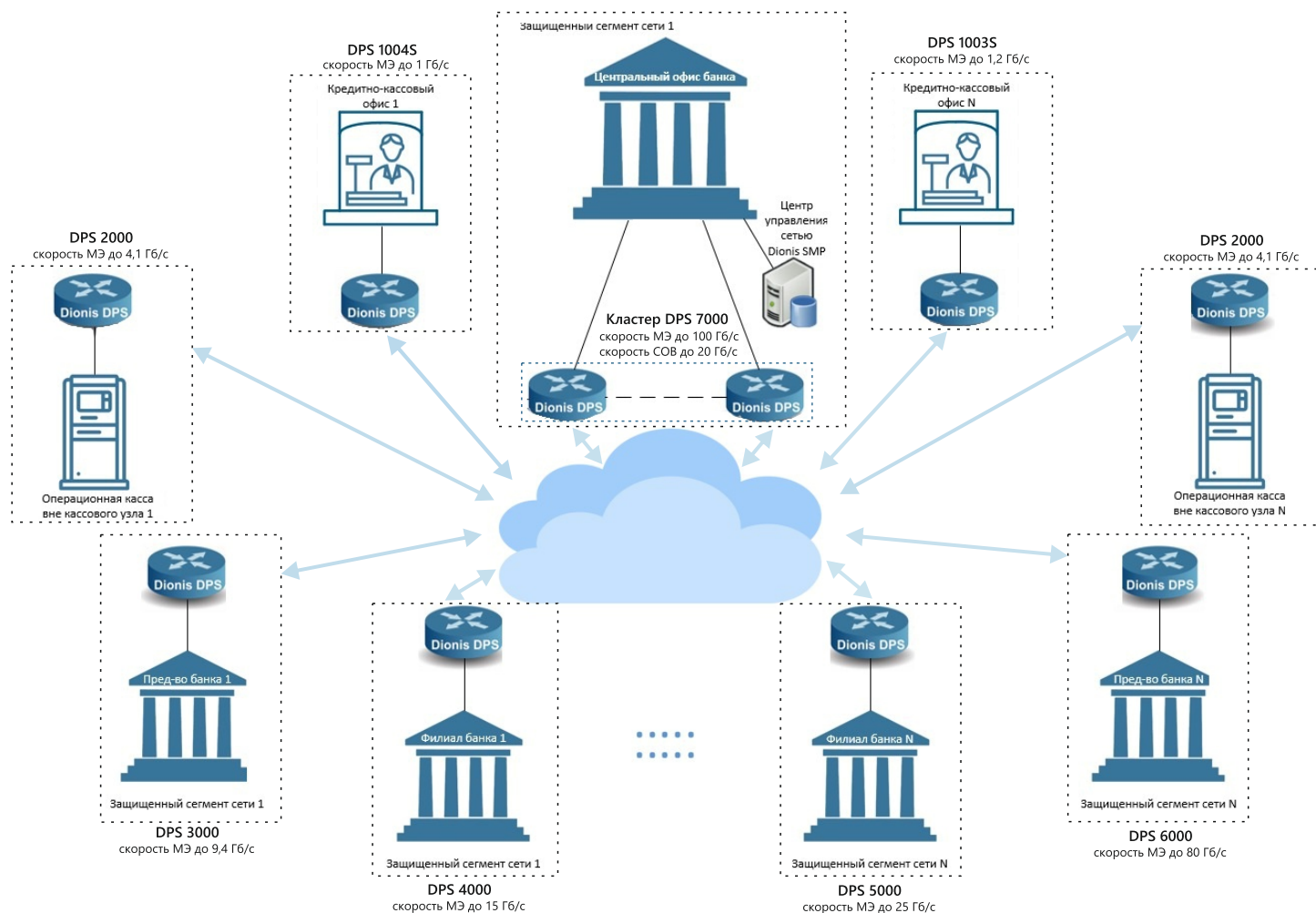
Наличие сертификата ФСТЭК

ИТ.МЭ.А4.ПЗ ИТ.МЭ.Д4.ПЗ ИТ.СОВ.С4.ПЗ

да	да	нет
да	да	нет
да	да	да
да	да	да



Защита периметра сети при помощи высокоскоростных межсетевых экранов



Подразделение банка

Центральный офис банка

Филиалы банка

Кредитно-кассовые офисы и операционная касса вне кассового узла

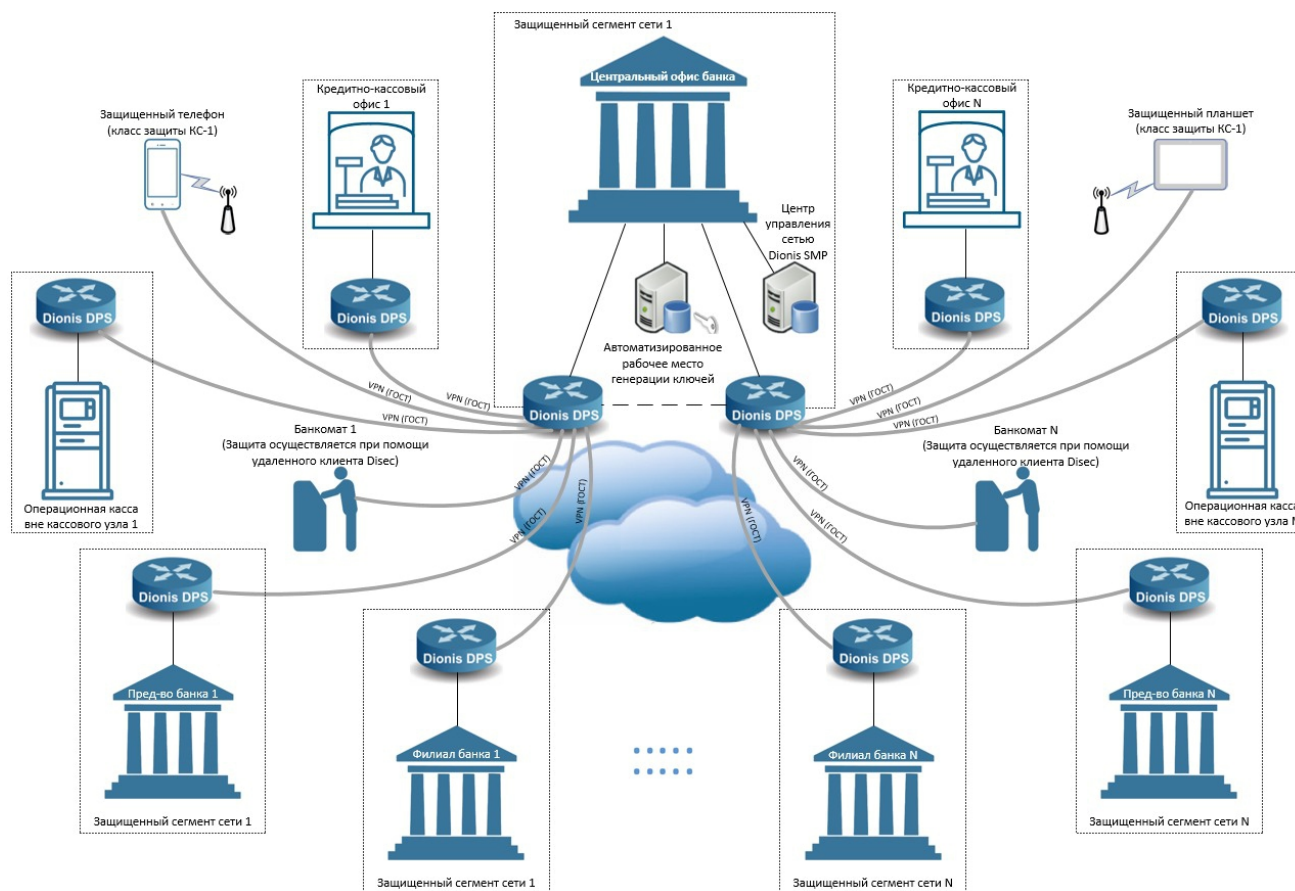
Предлагаемое оборудование ООО «Фактор-ТС»

Межсетевой экран ПАК DIONIS DPS 5000 (кластер)
 Межсетевой экран ПАК DIONIS DPS 6000 (кластер)
 Межсетевой экран ПАК DIONIS DPS 7000 (кластер)

Межсетевой экран ПАК DIONIS DPS 2000-6000

Межсетевой экран ПАК DIONIS DPS 1003S
 Межсетевой экран ПАК DIONIS DPS 1004S
 Межсетевой экран ПАК DIONIS DPS 2000

Построение защищенной криптографической сети (ГОСТ) финансовых организаций



Подразделение банка

Центральный офис банка

Филиалы банка

Кредитно-кассовые офисы и операционная касса вне кассового узла

Банкоматы

Удаленные сотрудники

Предлагаемое оборудование ООО «Фактор-ТС»

Криптомаршрутизатор ПАК DIONIS DPS 4000 (кластер)
Криптомаршрутизатор ПАК DIONIS DPS 5000 (кластер)
Криптомаршрутизатор ПАК DIONIS DPS 6000 (кластер)

Криптомаршрутизатор ПАК DIONIS DPS 2000-6000

Криптомаршрутизатор ПАК DIONIS DPS 1003S
Криптомаршрутизатор ПАК DIONIS DPS 1004S
Криптомаршрутизатор ПАК DIONIS DPS 2000

ПО Disec-W/ Криптомаршрутизатор ПАК DIONIS DPS 1003S, 1004S

ПО Disec LX для Linux



Оборудование ПАК DIONIS DPS, разработанное компанией Фактор-ТС, успешно прошло испытания и используется в проекте с Банком России в качестве транспортного шлюза для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР). Данное оборудование было рекомендовано Банком России для подключения к программе «Цифровой рубль», разрабатываемой Центральным банком Российской Федерации.



Оборудование ПАК DIONIS DPS успешно используется в рамках подключения к ФНС России в проекте «Автоматизированная информационная система ФНС России (АИС «Налог-3»)».

Функциональные возможности ПАК DIONIS DPS

Интерфейсы

Интерфейсы:

- Ethernet с возможностью задания нескольких IP-адресов на одном интерфейсе;
- VLAN с поддержкой QinQ;
- интерфейсы сетевой виртуализации VXLAN;
- туннельные интерфейсы: GRE/GRETAP с контролем состояния туннеля, L2TP с возможностью упаковки в туннель IPsec, PPTP, PPPoE;
- агрегированные интерфейсы Bond с различными алгоритмами балансировки: поочередное циклическое использование (balance-rr), резервирование (active-backup), распределение по хеш-функции (balance-xor), одновременная передача (broadcast) по стандарту IEEE 802.3ad, адаптивная балансировка передачи (balance-tlb), адаптивная балансировка на приеме (balance-alb);
- скомутированные интерфейсы Bridge с поддержкой протокола STP;
- интерфейсы беспроводных адаптеров и модемов 3G/LTE;
- VPN-интерфейсы OpenVPN (клиент/сервер);
- туннельные интерфейсы Ditun/Ditap (L3VPN/L2VPN) с поддержкой криптозащиты трафика по алгоритмам ГОСТ и контролем состояния туннеля.

Маршрутизация

Маршрутизация:

- статическая маршрутизация TCP/IP (v4);
- статическая маршрутизация TCP/IP (v6);
- маршрутизация на основе политик (PBR) IPv4/IPv6 с учетом классификации трафика, с контролем состояния маршрута;
- NHRP, Multipoint GRE ;
- динамическая (протоколы OSPFv2/v3, BGPv4/v6, RIP, RIP-NG) с использованием карт маршрутов (route-map) и протокола быстрого обнаружения недоступности соседа (BFD);
- маршрутизация мультикаст-трафика (статическая, динамическая по протоколам IGMP, DVMRP, PIM);
- MPLS (многопротокольная коммутация по меткам) — с возможностью статической и динамической коммутации по меткам (LDP) и построением L2/L3-туннелей с использованием интерфейсов Ditap/Ditun с криптозащитой и без;
- VRF – технология, позволяющая реализовывать на базе одного физического маршрутизатора несколько виртуальных, каждого со своей независимой таблицей маршрутизации. VRF в связке с технологией MPLS и BGP реализуют (MP-BGP, MPLS-L3VPN).

Функциональные возможности ПАК DIONIS DPS

Сетевые сервисы

Службы:

- DHCP, DHCP6, DHCP-Relay, DHCP-Relay6;
- DNS/EDNS (клиент/сервер); DNS Blackhole, DNSSEC;
- NTP (клиент/сервер);
- FTP-сервер;
- измерительные утилиты NetPerf и IPerf (клиент/сервер);
- SLAgent: агент измерителя качества каналов.

Качество сервиса (QoS)

Качество сервиса (QoS):

- классификация трафика по IP/MAC-адресам, портам и значениям байтов, битам поля CoS фрейма Ethernet и поля TOS/DSCP заголовка IP, наследование значения из заголовка Ethernet в заголовок IP и в заголовок туннеля IPerfIP. Предоставление политик обслуживания, в том числе гарантированной и максимальной полосы пропускания для различных классов трафика;
- управление полосой пропускания и приоритизация могут быть реализованы с помощью различных политик (HTB, Prio и PrioToS) и различных алгоритмов приоритизации (codel/fqcode, RED/GRED и SFQ). В политиках обеспечивается двухуровневая иерархия очередей.

Оптимизация производительности

Оптимизация производительности:

- трансляция ARP (proxy-arp);
- фильтрация ARP только для одного интерфейса (arp-filter);
- управление размером TCP MSS (path-mtu-discovery, adjust-mss);
- равномерное распределение входящих пакетов по очередям обработки (RSS);
- использование аппаратных возможностей сетевого адаптера (offload);
- уведомление о заторах без отброса пакетов (ECN);
- политики для борьбы с перегрузками, очереди, контроль QOS на основе классификаторов трафика;
- управление перегрузками FIFO, PQ, CQ, WFQ, CBWFQ;
- избегание перегрузок WRED/RED.

Функциональные возможности ПАК DIONIS DPS

Средства криптографической защиты информации

Криптографические туннели:

- статические — с использованием симметричных ключей и на ключевых парах Dikey, с шифрованием и имитозащитой IP-трафика по алгоритму ГОСТ 28147-89 (совместимы с хостами Dionis всех версий, в том числе DOS и LX и ПО DiSec);
- динамические — по протоколу IPSec (IKEv1, ESP) с изделиями семейства Dionis и с клиентским ПО семейства Disec, криптографической аутентификацией по алгоритмам ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015 в инфраструктуре открытых ключей (сертификаты X.509), с контролем состояния туннеля.
- Шифратор имеет синхронный режим работы, исключая перемешивание пакетов (out-of-order);
Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26).

Работа через NAT:

- инкапсуляция трафика в протокол UDP;
- поддержка механизма nat-traversal.

Межсетевой экран

Фильтрация пакетов:

- по IP/MAC-адресам, портам, значениям байт в теле пакета;
 - фильтрация, учитывающая состояние соединения (Stateful Packet Inspection);
 - фильтрация по расписанию;
 - фильтрация по мандатным меткам ОС MCBC и ОС Astra Linux;
 - фильтрация пакетов на прикладных уровнях (L7-filter);
 - transparent firewall;
 - защиты от вирусов (с использованием дополнительного ПО);
 - L2 фильтрация bridge, режим работы bridge только L2 (без conntrack), content фильтр;
 - фильтрация по содержимому пакетов (content);
 - фильтрация трафика с использованием регулярных выражений в формате POSIX;
 - фильтрация трафика на основе расширенных регулярных выражений PCRE;
 - фильтрация трафика с использованием PCAP-выражений;
 - использование макросов PCAP-выражений для описания любой структуры специфических протоколов;
 - Описаны макросы PCAP-выражений для следующих промышленных протоколов:
 - MODBUS-TCP;
 - ГОСТ Р МЭК 60870-5-104-2004;
 - IEC 1815-2012 DNP3.
 - Proxy – прозрачный/не прозрачный режим, ssl-bump, аутентификация AD, RADIUS, Kerberos, ICAP;
 - WCF – Веб контент фильтр.
- #### Трансляция пакетов:
- NAT/PAT (трансляция входящего (DNAT) и исходящего (SNAT) трафика;
 - трансляция всех адресов в один адрес (masquerade);
 - трансляция сеть в сеть (netmap);
 - перенаправление трафика (redirect);
 - Ipv6 transition: NAT-PT.

Функциональные возможности ПАК DIONIS DPS

ПАК DIONIS DPS имеет встроенную систему обнаружения и предотвращения сетевых атак (IDS/IPS) на базе Snort. Работа системы возможна в режиме только обнаружения атаки или в режиме обнаружения и предотвращения атаки. Анализ можно применять как для маршрутизируемого трафика, так и для трафика, коммутируемого через сетевой мост. Помимо стандартных широких возможностей системы Snort добавлена поддержка создания собственных правил анализа трафика и возможность записи дампов трафика, распознанного как атака. Управление системой и отображение статистики атак реализовано через портал управления безопасностью Dionis-SMP.

Резервирование

Кластеры:

- отказоустойчивый аппаратный кластер с горячим резервированием (активный/пассивный, с передачей информации о текущих соединениях);
- кластер по протоколу VRRPv2/v3+object tracking.

Общение и связь:

- XMPP — протокол обмена сообщениями;
- Tox — протокол для текстовой, голосовой и видеосвязи.

Управление и мониторинг

Поддерживаются аутентификация и авторизация пользователей через серверы Radius и TACACS+.

Локальное управление (интерфейс командной строки):

- локальная консоль (клавиатура и монитор, возможно подключение монитора по DisplayLink);
- терминал через порт RS-232.

Удаленное управление:

- интерфейс командной строки;
- по протоколам SSH и telnet;
- WEB-интерфейс по протоколу HTTP.

Удобство управления:

- групповые объекты ACL, NAT, PBR;
- архиватор.

Ролевая модель управления:

- возможность задания множества администраторов с назначаемыми правами управления и мониторинга.

Функциональные возможности ПАК DIONIS DPS

Управление и мониторинг

Развитые механизмы обслуживания:

- удаленное обновление программного обеспечения;
- возможность установки нескольких версий на одну аппаратную платформу;
- привязка слотов данных (настроек) к версиям программного обеспечения;
- контроль целостности программного обеспечения;
- резервное архивирование и восстановление, в том числе по сети;
- назначение умалчиваемой, резервной и экспериментальной версий ПО;
- автоматический переход на резервную версию ПО при неуспешном запуске.

Трассировка:

- отслеживание приема, пути и отправки пакета в маршрутизаторе, его трансформаций, попадания в фильтры.

Ведение журналов:

- регистрация в системных журналах различных событий (в том числе протоколирование работы фильтров) и действий администраторов;
- статистика по IP-адресам.

Мониторинг:

- SNMP v2/v3 – с поддержкой аутентификации, NetFlow v1/v5/v9, Syslog, RMON;
- LLDP;
- зеркалирование трафика (mirroring);
- отслеживание сообщений в журналах по заданному шаблону с возможностью отправки на E-mail;
- текущий мониторинг загрузки системы и интерфейсов на консоли.







ФАКТОР·ТС

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

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