ФАКТОР·ТС

Высокопроизводительное оборудование для ЦОД.
Производительность в режиме шифрования до 100 Гб/с (ГОСТ)
и скорость маршрутизации до 120 Гб/с.

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).

Технические решения компании позволяют замещать импортные аналоги в критически важных для безопасности страны сегментах национальной информационной структуры.

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 в министерствах и ведомствах силового блока России, а также в Государственной думе, Банке России, Министерстве экономического развития РФ (Росреестре), Министерстве труда и социальной защиты РФ, Федеральной таможенной службе, региональных подразделениях Федерального казначейства, администрациях целого ряда субъектов Российской Федерации, Сбербанке России и в других государственных организациях.

Высокоскоростные маршрутизаторы ПАК Dionis DPS 6000 и 7000 Series. Маршрутизация до 120 Гб/с и шифрование до 8 Гб/с.

ПАК Dionis DPS 6000 и 7000 — это модульные решения уровня ядра с производительностью маршрутизатора до 120 Гб/с и скорости шифрования до 8 Гб/с. Данные платформы позволяют реализовать в одном устройстве высокопроизводительный маршрутизатор с поддержкой VPN (ГОСТ) и систему обнаружения и предотвращения вторжений IPS/IDS. Гибкая модульная система способна значительно упростить интеграцию решения в существующую сетевую инфраструктуру. Резервирование источника питания в сочетании с отказоустойчивым кластером позволяет обеспечить высокий уровень надежности ядра сети организации. Для DPS 6000 и 7000 Series модули приобретаются отдельно и могут самостоятельно устанавливаться заказчиком по мере расширения сети.

ПАК Dionis DPS включает в себя:

- Высокопроизводительный маршрутизатор
- Криптошлюз для защиты передачи данных ФСБ КС1,КС3
- Сертифицированный межсетевой экран ФСТЭК ИТ.МЭ.А4.П3 ФСТЭК ИТ.МЭ.Д4.П3
- PROXY, DHCP, NTP-сервер, балансировщик нагрузки с поддержкой QoS
- Систему обнаружения вторжений IDS/IPS ФСТЭК ИТ.СОВ.С4.П3
- Сервер удаленного защищенного доступа мобильных абонентов

Основные возможности ПАК Dionis DPS:

- Скорость маршрутизации до 120 Гб/с на одном устройстве позволяет строить ЦОДы с минимальным количеством пограничных маршрутизаторов
- Модели поддерживают отказоустойчивый кластер, что дает возможность организовать безотказный доступ к корпоративной сети
- Запись всех событий в сети и оповещение администратора позволяет оперативно реагировать на события в сети
- Поддержка интерфейсов 1Ge, SFP, 10Ge (SFP+), 40GbE QSFP+ для интеграции в сети с разнообразными физическими каналами связи
- Поддержка протоколов динамической маршрутизации (RIP, BGP, OSPF) и маршрутизация multicast на младших моделях позволяют строить полноценную сеть без существенных затрат
- Возможность использования двух схем распределения ключей шифрования: -симметричная(Disec-туннели), -несимметричная(IpSec-туннели)
- Программно неограниченное количество VPN - туннелей (до 4000). Масштабирование сети без покупки дополнительных лицензий
- Единый центр анализа и управления системой обнаружения и предотвращения сетевых вторжений

Сравнительная таблица моделей ПАК Dionis DPS 6000 и 7000

	ПАК Dionis DPS-6000 Series	ПАК Dionis DPS-7000 Series

Характеристики

max скорость маршрутизации, Мб/с	109 000	120 000
max скорость шифрования , Мб/с	4 700	8 000
max скорость в режиме Firewall, Мб/с	80 000	90 000
max кол-во конкурентных сессий	60 000 000	60 000 000
max кол-во интерфейсов	50	50
max кол-во IpSec-туннелей (ГОСТ)	1 500	2 000
max кол-во Disec-туннелей (ГОСТ)	2 000	2 500
Рекомендуемое max кол-во узлов в ЛВС	1 000	2 000
Производительность в режиме IPS/IDS, Мб/с	15 000	20 000
Поддержка отказоустойчивого кластера	да	да
max кол-во дополнительных модулей	6	6
Подключения монитора (VGA) и клавиатуры	да	да
Консольный порт	да	да
Разъем HDMI	нет	нет
Разъем DVI	нет	нет
Конструктив	RM19"2U	RM19"2U
Охлаждение	Активное	Активное
Напряжение питания, В	220-240	220-240
Тип блока питания	2-й встр.	2-й встр.
Поддержка двойного блока питания	да	да
Габариты, мм (ШхВхГ)	438x88x595	438x88x595

Сертификаты

Сертификат ФСБ
СКЗИ КС1,КС3

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

Реестр отечественного программного обеспечения

Поддерживаемые модули (max 6 модулей)

	Кол-во интерфейсов
Модуль 8x1Ge	8
Модуль 8xSFP 1Ge	8
Модуль 4xSFP+ 10Ge	4
Модуль 2x40GbE QSFP+	2

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);

— скоммутированные интерфейсы Bridge с поддержкой протокола STP;

— интерфейсы беспроводных адаптеров и модемов 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 IPoverIP. 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/fqcodel, 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;

— избежание 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, исключающий 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 МСВС 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 использование 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

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.

Высокопроизводительный «Канальный шифратор Dionis-CE». Скорость шифрования до 100 Гб/с.

ПАК «Канальный шифратор Dionis-CE» предназначен для криптографической защиты информации, передаваемой по высокоскоростным каналам связи на скорости 100 Гб/с. ПАК «Канальный шифратор Dionis-CE» содержит плату на базе программируемых логических интегральных схем (ПЛИС), в которой на аппаратном уровне реализованы криптографические алгоритмы ГОСТ, что обеспечивает высокую производительность и минимальную задержку. Плата ПЛИС имеет сетевые порты, обеспечивающие подключение трансиверов по стандарту QSFP28 для приема/передачи кадров Ethernet. Защита информации реализована путем шифрования и имитозащиты данных, содержащихся в кадрах Ethernet. Для защиты канала связи требуется два изделия.

Криптографическая защита информации

- Реализованы алгоритмы ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015.
- Применяются ключи шифрования парно-выборочной связи, изготавливаемые с использованием сертифицированного СКЗИ «Автоматизированное рабочее место генерации ключей «АРМ ГК-4».
- Сертификат ФСБ РФ на соответствие требованиям к средствам криптографической защиты информации класса КС3 (№ СФ/124-4682 от 15.12.2023 г. действителен до 20.12.2025 г.).
- Ввод ключевой информации со сменных носителей, подключаемых к порту USB. Хранение ключевой информации в памяти устройства.

Обеспечение качества сервиса

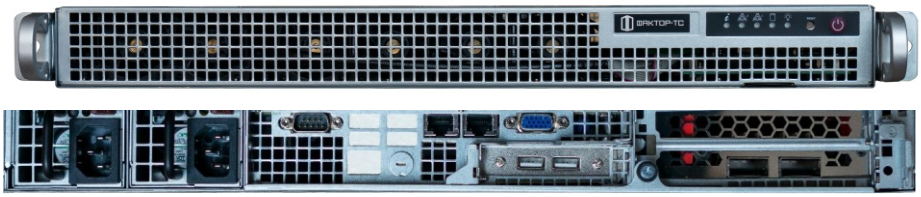
- Сохранение тега IEEE 802.1q, включая значения идентификатора VLAN и приоритета (CoS), из заголовка исходного кадра Ethernet.
- Удаление тега IEEE 802.1q из исходного кадра Ethernet.
- Установка/замена тега IEEE 802.1q, включая значения идентификатора VLAN и приоритета (CoS) в заголовке исходного кадра Ethernet.
- Прозрачное (без зашифрования) пропускание кадров указанного типа (EtherType), например, кадров протоколов диагностики канального подключенияIEEE 802.3ag (CFM).

Система управления и мониторинга

- Управление и мониторинг с помощью интерфейса командной строки. Доступ к интерфейсу командной строки по протоколам SSH и Telnet.
- Ролевая модель аутентификации пользователей с поддержкой ролей привилегированного пользователя (администратора), в рамках которой могут выполняться функции управления (настройка, конфигурирование и т.д.) и непривилегированного пользователя, в рамках которой выполняется контроль функционирования СКЗИ.
- Мониторинг в реальном времени состояния интерфейсов шифратора, загрузки системы и статистики трафика.
- Поддержка внешнего мониторинга работы шифратора по протоколу SNMP.
- Регистрация событий, связанных с настройкой и функционированием шифратора в журналы и экспорт журналов на внешний носитель, подключаемый к порту USB.
- Поддержка отправки журналов по протоколу Syslog.

Программно-аппаратный комплекс «Канальный шифратор Dionis-CE»

Сертификат ФСБ
СКЗИ КС3



Спецификация

Количество встроенных интерфейсов	4
max скорость шифрования (UDP 1500), Гб/с	до 98
max количество Disec-туннелей (ГОСТ)	1
max количество интерфейсов	4

Параметры

Конструктив	1U 19"
USB-порты	2
Разъем VGA	да
Консольный порт	да
Тип ключевого носителя	USB
Охлаждение	активное
Напряжение питания, В	220
Блок питания	встроенный, двойной
Мощность, Вт	400
Размеры ШхВхГ, мм	438x44x435
Диапазон рабочих t, С °	10...35
Масса, кг	7

Конфигурации аппаратной платформы

	1000 Base-T	SFP (1000 Base-SX/LX)	QSFP28 (100GBASE-SR4)	Всего интерфейсов:
Dionis-CE	2	нет	2	4

Технические характеристики

— Поддержка тегированных кадров Ethernet IEEE 802.1q;

— Поддержка кадров длиной до 10000 байт (Jumbo frame);

— Поддержка кадров по стандарту Ethernet IEEE 802.3ba (100-гигабитный Ethernet);

— Максимальная задержка обработки кадра на двух шифраторах в двух направлениях (Round-Trip Time) не превышает 0,1 мс;

— Максимальная задержка обработки кадра на одном шифраторе в одном направлении не превышает 0,024 мс.

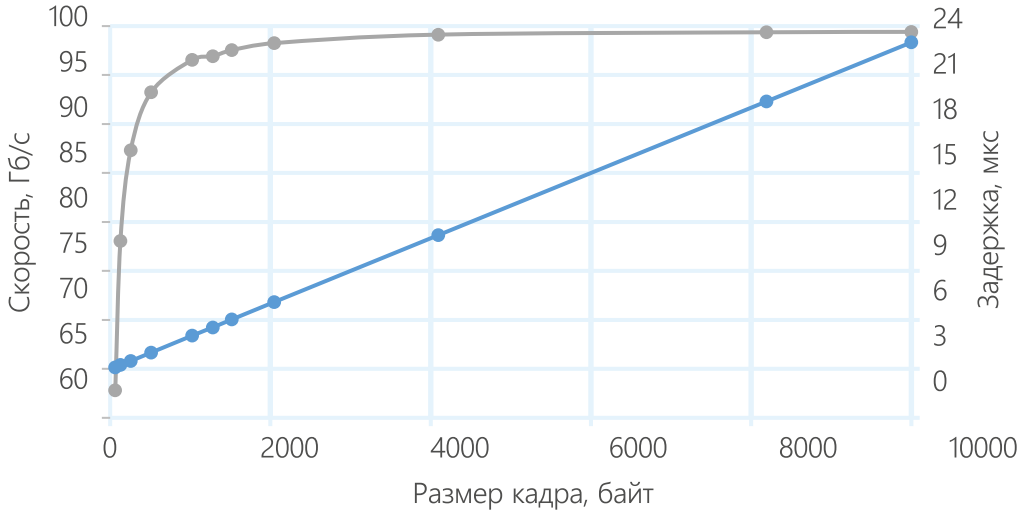
Дополнительные возможности:

— Контроль целостности ПО;
— Контроль функционирования шифратора;
— Средства обновления ПО.

Результаты лабораторных испытаний пропускной способности и задержки по методике RFC 2544

Размер кадра (байт)	64	128	256	512	1 024	1 280	1 518	2 048	4 096	8 192	10 000
Суммарные показатели для прямого и обратного направления трафика (режим duplex)											
Процент утилизации канала	82,44%	90,24%	94,15%	96,88%	98,44%	98,44%	98,83%	99,22%	99,61%	99,61%	99,61%
Скорость на уровне L2 (Гб/с)	125,62	156,1	174,65	186,47	193,11	193,85	195,09	196,52	198,25	198,73	198,82
Скорость (кадр/с)	245 355 514	152 439 426	85 277 612	45 525 434	23 572 572	18 930 588	16 064 580	11 994 624	6 050 154	3 032 444	2 485 272
Потери кадров	0	0	0	0	0	0	0	0	0	0	0
Детализация показателей в одном направлении											
Скорость на уровне L2 (Гб/с)	62,81	78,05	87,32	93,24	96,55	96,92	97,54	98,26	99,13	99,37	99,41
Скорость (кадр/с)	122 677 757	76 219 713	42 638 806	22 762 717	11 786 286	9 465 294	8 032 290	5 997 312	3 025 077	1 516 222	1 242 636
Средняя задержка (мкс)	3,088	3,244	3,481	3,998	5,035	5,54	6,024	7,094	11,192	19,384	23,003
Min задержка (мкс)	3,056	3,208	3,449	3,962	5,004	5,51	5,991	7,057	11,131	19,325	22,958
Max задержка (мкс)	3,136	3,289	3,529	4,05	5,077	5,582	6,071	7,129	11,227	19,438	23,054
Джиттер (мкс)	0,003	0,004	0,003	0,004	0,005	0,005	0,006	0,005	0,007	0,013	0,005
Размер кадра (байт)	64	128	256	512	1024	1280	1518	2048	4096	8192	10 000
Детализация показателей в обратном направлении											
Скорость на уровне L2 (Гб/с)	62,81	78,05	87,32	93,24	96,55	96,92	97,54	98,26	99,13	99,37	99,41
Скорость (кадр/с)	122 677 757	76 219 713	42 638 806	22 762 717	11 786 286	9 465 294	8 032 290	5 997 312	3 025 077	1 516 222	1 242 636
Средняя задержка (мкс)	3,1	3,249	3,485	4,019	5,032	5,549	6,032	7,098	11,192	19,379	23,016
Min задержка (мкс)	3,064	3,208	3,449	3,986	4,996	5,518	5,991	7,065	11,131	19,325	22,974
Max задержка (мкс)	3,144	3,297	3,537	4,058	5,069	5,598	6,079	7,137	11,227	19,43	23,07
Джиттер (мкс)	0,002	0,004	0,003	0,004	0,005	0,005	0,006	0,005	0,007	0,013	0,005

График производительности и задержки по результатам испытаний



Криптографическая защита высокоскоростных каналов связи. Шифрование до 10 Гб/с, класс защищенности КВ, КА.

Решение по защите высокоскоростных каналов связи с пропускной способностью до 10 Гбит/с.

Криптомаршрутизатор М-479Р2К (далее — изделие) является аппаратно-программным шифровальным средством, отвечающим требованиям ФСБ России к СКЗИ до класса КА включительно. В изделии используется аппаратное шифрование, которое позволяет значительно увеличить скорость криптографической обработки (до 19 000 Мб/с в дуплексном режиме) по сравнению с программным шифрованием, использующим центральный процессор. Аппаратное шифрование потока данных реализуется с помощью специальной платы без привлечения к процедуре шифрования центрального процессора.

Применение данного решения эффективно в случаях, когда для хранения и обработки больших объемов конфиденциальной информации используются распределенные центры обработки данных (ЦОД). С появлением такого решения проще и дешевле защищать информацию, передаваемую между ЦОД, а также между защищаемыми сегментами ЛВС.

Применение предлагаемого решения эффективно для защиты трафика, циркулирующего через сети общего пользования между ЦОД (и между сегментами ЛВС), как на уровне L3, так и на уровне L2 эталонной модели взаимосвязи открытых систем (модели OSI).

Последнее особенно важно в связи с использованием специализированных протоколов при обмене Ethernet-кадрами на уровне L2 модели OSI (трафик между ЦОД). Применение предлагаемых изделий не вносит ограничений в работу этих протоколов обмена между ЦОД (в отличие от криптомаршрутизаторов, обеспечивающих обмен только на уровне L3): для двух ЦОД пара изделий КМ-МПМР2К протоколами обмена на уровне L2 воспринимается как отрезок Ethernet-кабеля, по которому осуществляется высокоскоростной прозрачный для Ethernet-кадров обмен между двумя сегментами ЛВС. Отметим, что такое высокопроизводительноше ифрованиеп отока данных может применяться в «облачных» технологиях при переносе физической IT-инфраструктуры в виртуальную среду, особенно если речь идет о корпорациях либо о ведомственных и государственных структурах. Одним из достоинств представленного решения является его эффективная масштабируемость, что позволяет увеличивать количество используемых криптомаршрутизаторов по мере увеличения числа каналов связи для передачи возрастающего объёма передаваемых данных. Используя комбинацию маршрутизатора Dionis DPS серии 5000, выполняющего балансировку трафика между криптомаршрутизаторами, с несколькими М-479Р2К, можно обеспечить шифрование потока данных с суммарной пропускной способностью свыше 10 Гбит/с при неизменно высоком уровне сервиса. Также возможно резервирование криптомаршрутизаторов М-479Р2К для обеспечения повышенной надежности работы защищаемого тракта передачи данных.

Криптомаршрутизатор М-479Р2К

Сертификат ФСБ СКЗИ до КА включительно

Характеристики

Количество интерфейсов	12
Максимальная скорость криптографической обработки, Мбит/с	до 18 500
Максимальная производительность кадров в секунду	2 000 000
Конструктив	4Ux19" со встроенной консолью управления
Габариты моноблока изделия, мм	431x456x177
Электропитание от однофазной сети с переменного тока (частота 50-60 Гц), В	110-240
Габариты моноблока с крепежными кронштейнами, мм	483x494x177
Группа по ГОСТ РВ 20.39.304-98 (с ограничением)	1.1 (исполнение УХЛ)
Средняя наработка на отказ	не менее 25 000 ч
Коэффициент готовности	не менее 0,995
Среднее время восстановления работоспособности	не более 0,5 ч
Потребляемая мощность	не более 150 Вт
Масса изделия	не более 15 кг
Средний срок службы изделия	не менее 10 лет
Количество L3 VPN туннелей (криптотуннелей)	до 256
Количество L2 VPN туннелей (криптотуннелей)	до 256
Количество изделий в сети	не ограничено (до 10 000 устройств в одной ключевой зоне)
Наличие перешифрования	да
Локальный ввод ключевой информации	CD / DVD / SD / USB FLASH
Обеспечение качества обслуживания (QoS)	есть
Поддержка IP Multicast	есть
Удаленное управление	встроенный Центр удаленного администрирования, SNMP-менеджер
Механизмы контроля состояния доступности узлов сети	есть
Поддерживаемые протоколы	TCP, IP, ARP, UDP, ICMP, SNTP, SNMP, DNS, RIP, LLDP, SYSLOG, TELNET, GRE, 802.1Q, IGMP
Удалённая смена ключевой документации	есть
Работа Криптомаршрутизатора за NAT	да
Агрегирование интерфейсов: резервирование и балансировка	есть
Поддержка jumbo frame	да (до 2К)

Поддерживаемые модули

Ethernet 100 / 1000 TX / SFP

Ethernet 10 000 SFP+

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