ФАКТОР-ТС

DIONIS DPS

UTM–РЕШЕНИЯ, СЕРТИФИЦИРОВАННЫЕ ФСБ И ФСТЭК РОССИИ

МОСКВА 2023

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.

Dionis DPS - UTM-решение, сертифицированное ФСБ и ФСТЭК России

Dionis DPS — это современное UTM-решение для российского рынка IT. Dionis DPS выполняет функции маршрутизатора и межсетевого экрана, а также имеет в своем составе средства криптографической защиты информации (СКЗИ). Данный функционал 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.

Прикладное программное обеспечение производства компании «Фактор-ТС» в сочетании с маршрутизатором Dionis DPS позволяет внедрять комплексные решения для всей IT-инфраструктуры заказчика.

Dionis DPS включает в себя:

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

Области применения Dionis DPS

Dionis DPS защищает:

- передачу данных через незащищенные сети общего пользования;
- автоматизированные системы управления технологическими процессами;
- системы видеонаблюдения, системы организации безопасности дорожного движения, системы «умный город»;
- видеоконференции и телефонию;
- периметр корпоративной сети.

Dionis DPS позволяет организовать:

- географически распределенные защищенные VPN-сети;
- защищенный центр обработки данных (ЦОД);
- высокоскоростной и отказоустойчивый канал шифрования (ГОСТ) до 10 Гб/с.

Основные возможности Dionis DPS

- Скорость маршрутизации до 100 Гб/с на одном устройстве позволяет строить ЦОДы с минимальным количеством пограничных маршрутизаторов.
- Все 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+),G.703 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.

Dionis DPS - доступное решение!

Особенности Dionis DPS, снижающие затраты

- Младшие модели поддерживают почти весь функционал старших моделей. Модели отличаются только производительностью и количеством сетевых портов.
  Нет необходимости приобретать более дорогую версию ради дополнительных функций.
- Dionis DPS не требует ежегодной покупки лицензии.
- Подробное техническое руководство на русском языке и техническая поддержка сокращают затраты на обучение персонала.
- Повышенная скорость защищенных межфилиальных соединений позволяет оптимально использовать арендуемые каналы связи.

Перечень оборудования 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, Мб/с	2 800	3 800	7 600	13 000	19 600	39 700	109 000	120 000
max скорость шифрования , Мб/с	100	200	500	1 400	2 300	2 500	4700	8000
max скорость в режиме Firewall, Мб/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, Мб/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 (ШхВхГ)	106x30x85	165x43x105	484x44x399	484x44x399	484x44x399	438x44x483	438x88x595	438x88x595

Варианты поставки

Наличие сертификата ФСБ

Наличие сертификата ФСТЭК

	КС3	ИТ.МЭ.А4.ПЗ	ИТ.МЭ.Д4.ПЗ	ИТ.СОВ.С4.ПЗ
Комплектация FW	нет	да	да	нет
Комплектация FWC-КС3	да	да	да	нет
Комплектация FW-IPS	нет	да	да	да
Комплектация FWC-КС3-IPS	да	да	да	да

Функциональные возможности Dionis DPS

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 Wi-Fi и модемов 3G/LTE;

— E1 (HDLC);

— VPN-интерфейсы OpenVPN (клиент/сервер);

— туннельные интерфейсы Ditun/Ditap (L3VPN/L2VPN) с поддержкой криптозащиты трафика по алгоритмам ГОСТ и контролем состояния туннеля.

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 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)

— 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

— 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 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 281470-89, 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 Dionis DPS

Dionis DPScодержит 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 для маршрутизируемого трафика 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 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.

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

dps.factor-ts.ru

sales@factor-ts.ru

+7 (495) 644 31 30