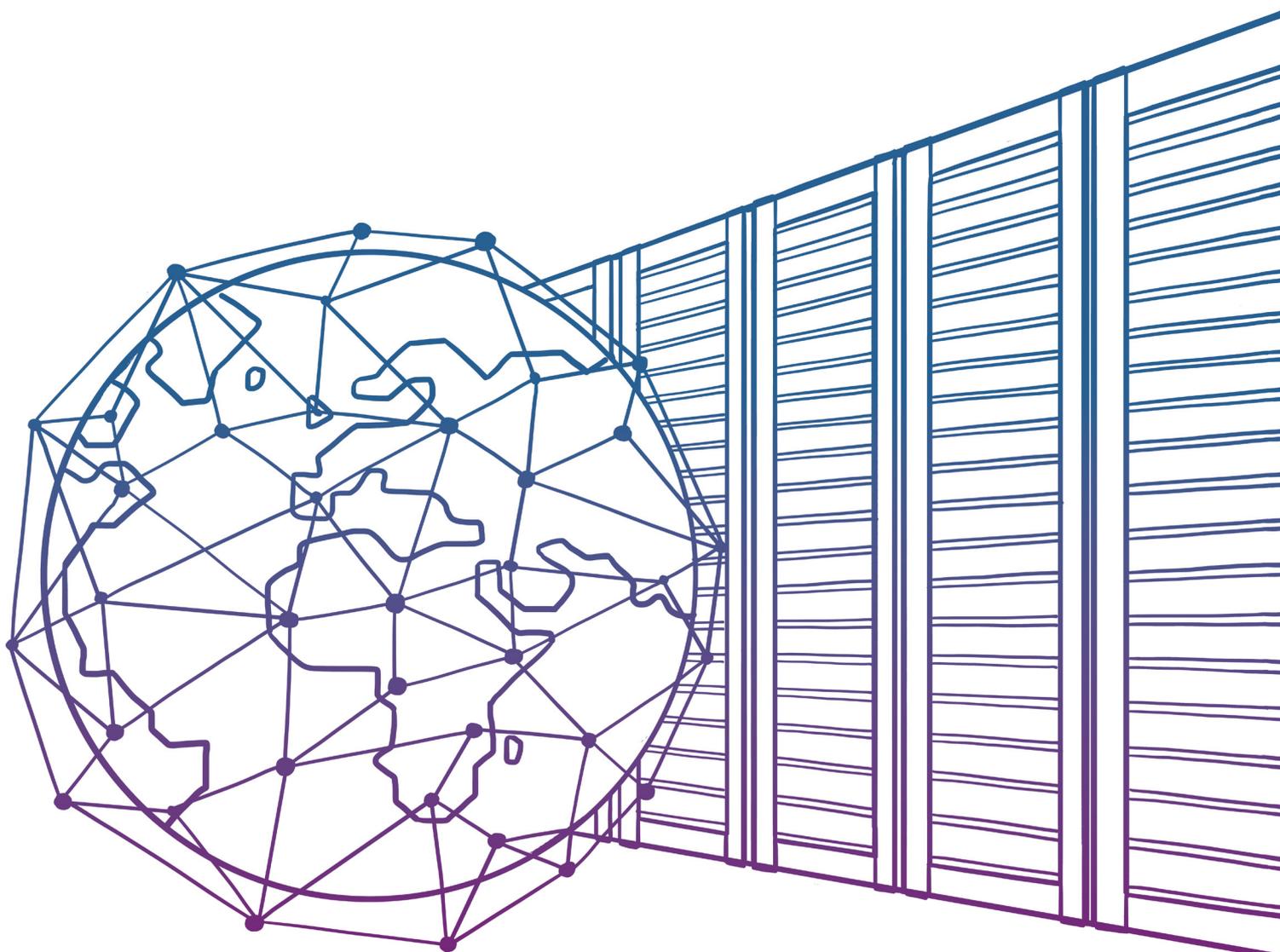


VIPNet Channel Protection

Решения для защиты каналов связи





Решения ViPNet Channel Protection предназначены для создания защищенной доверенной среды передачи информации ограниченного доступа с использованием публичных и выделенных каналов связи методами:

- 1** обеспечения прозрачной криптографической защиты данных, передаваемых по каналам Ethernet («темная оптика», MAN, WAN, выделенный канал)
- 2** организации защищенных каналов связи и предотвращения несанкционированного доступа к объектам промышленных информационных систем
- 3** организации виртуальной частной сети (VPN) с централизованным управлением, а также создания централизованных комплексов управления и мониторинга средств защиты информации в распределенных сетях
- 4** построения защищенных TLS и ГОСТ-каналов

СОСТАВ РЕШЕНИЯ

Шлюзы безопасности – межсетевые экраны нового поколения



ПАК ViPNet Coordinator HW 5
Криптографический шлюз безопасности – межсетевой экран нового поколения



ViPNet Coordinator VA 5
Криптографический шлюз безопасности – межсетевой экран нового поколения в виртуальном исполнении



ViPNet xFirewall
Шлюз безопасности – межсетевой экран нового поколения

Шлюзы безопасности



ПАК ViPNet Coordinator HW 4
Шлюз безопасности для защиты каналов связи



ViPNet Coordinator VA 4
Шлюз безопасности в виртуальном исполнении



ПАК ViPNet Coordinator KB
Шлюз безопасности, соответствующий требованиям к СКЗИ класса KB



ПАК ViPNet Coordinator IG
Шлюз безопасности в промышленном исполнении, МЭ, VPN-сервер



ViPNet TLS Gateway
Шлюз безопасности для организации защищенных соединений по протоколу TLS



ViPNet L2-10G
Шлюз безопасности уровня L2, обеспечивающий криптографическую защиту Ethernet

Системы управления



ViPNet Administrator
Программный комплекс для настройки и управления сетью



ViPNet Policy Manager
Программный комплекс централизованного управления политиками безопасности сетевых экранов



ViPNet Client
Программный комплекс для организации VPN-подключения к защищенным сетям ViPNet

Клиентские компоненты

HW VIPNet Coordinator HW 5

Криптографический шлюз безопасности,
реализующий концепцию NGFW (Next-Generation
Firewall – межсетевой экран нового
поколения)

ViPNet Coordinator HW 5 – решение, реализующее в одном устройстве ряд функций безопасности, действующих совместно:

- > криптографический шлюз, обеспечивающий построение VPN на сетевом (L3) и канальном (L2) уровнях модели OSI
- > межсетевой экран SPI (Stateful Packet Inspection)
- > прокси-сервер
- > межсетевой экран уровня приложений DPI (Deep Packet Inspection)
- > средство обнаружения и предотвращения вторжений (IDS/IPS)
- > кластер высокой доступности (HA-cluster)

ViPNet Coordinator HW 5 реализуется в исполнении программно-аппаратного комплекса на доверенной аппаратной платформе, а также в виде виртуального устройства, которое может функционировать в виртуальной среде (KVM, VMware ESXi, Microsoft Hyper-V, Oracle XenServer).

Реализованные сетевые функции и сервисы безопасности активируются в соответствии с приобретенной лицензией (лицензируются отдельные модули).

ЧТО НОВОГО

01. Поддержка алгоритмов «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
02. Межсетевой экран уровня приложений (DPI)
03. Обнаружение и предотвращение вторжений (IDS/IPS)
04. Многопользовательский ролевой доступ
05. Подсистема идентификации пользователей (LDAP, Active Directory, Captive Portal)
06. Кластер высокой доступности (HA-cluster) с синхронизацией таблицы открытых соединений
07. Централизованное и удаленное резервное копирование конфигурации

СЕРТИФИКАЦИЯ

ФСБ России

В процессе сертификации на соответствие требованиям:

- > СКЗИ класса КСЗ

Свидетельства

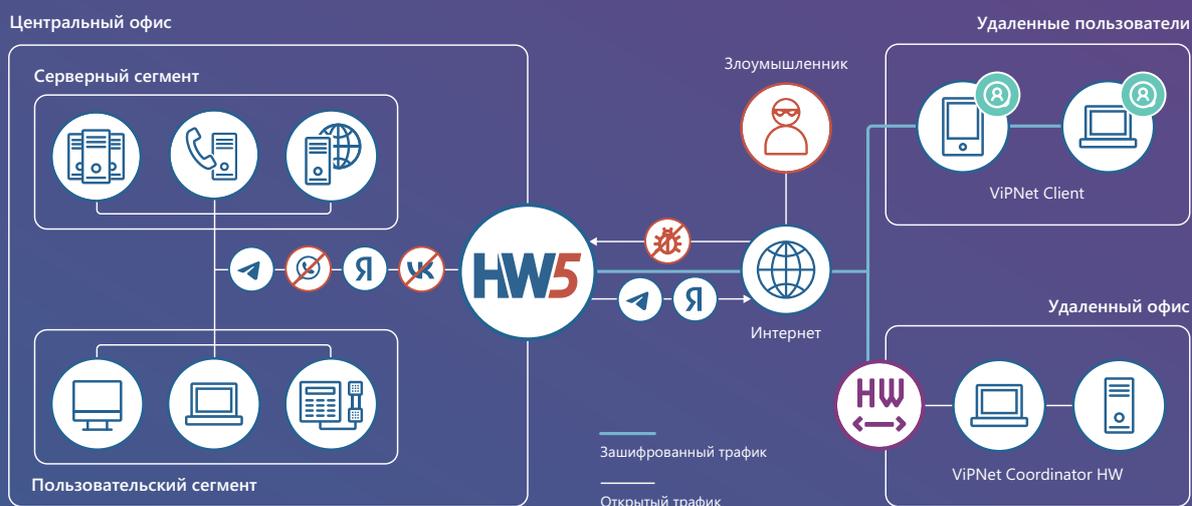
- > Роспатент
- > Интеграл
- > В реестре российского ПО
- > В реестре Минпромторга

ФСТЭК России

В процессе сертификации на соответствие требованиям:

- > МЭ типа А 4 класса (ИТ.МЭ.А4.ПЗ)
- > МЭ типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
- > СОВ уровня сети 4 класса защиты (ИТ.СОВ.С4.ПЗ)
- > 4 уровень доверия средств защиты информации

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ



- > Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
- > Защищенный доступ удаленных пользователей
- > Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
- > Обнаружение и нейтрализация сетевых вторжений
- > Комплексная защита от сетевых угроз
- > Защита магистральных каналов, соединяющих ЦОДы между собой
- > Защита беспроводных сетей связи 3G/LTE и Wi-Fi
- > Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
- > Взаимодействие с сетями ViPNet других организаций

ВОЗМОЖНОСТИ

VPN

- > VPN-шлюз сетевого уровня (L3 VPN)
- > VPN-шлюз канального уровня (L2OverIP VPN)*
- > Поддержка криптографических алгоритмов ГОСТ 34.12-2018 «Магма» и «Кузнечик», ГОСТ 28147-89
- > Сервер IP-адресов и маршрутизатор VPN-пакетов*
- > Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Идентификация пользователей

- > Интеграция с Microsoft Active Directory
- > Captive Portal и интеграция с LDAP-каталогом

Межсетевой экран (SPI)

- > Фильтрация трафика на сетевом и транспортном уровнях модели OSI с контролем состояния сессий
- > Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
- > NAT/PAT
- > Антиспуфинг

Обнаружение и предотвращение вторжений (IPS)

- > Анализ сетевого трафика для защиты от различного вида сетевых атак и вирусов, попыток эксплуатации уязвимостей и получения несанкционированного доступа
- > Работа как в режиме предотвращения вторжений (IPS), так и обнаружения (IDS) с фиксацией событий
- > Сигнатурный и эвристический методы анализа трафика
- > Автоматизированное обновление баз правил с сервера обновлений
- > База правил регулярно обновляется специалистами ГК «ИнфоТеКС» для поддержания в актуальном состоянии

Отказоустойчивость и резервирование

- > Отказоустойчивый кластер высокой доступности по схеме «активный/пассивный» с минимальным временем переключения между элементами кластера (до 1 секунды)
- > Поддержка синхронизации таблицы соединений между элементами кластера
- > Резервирование каналов связи
- > Резервирование сетевых интерфейсов
- > Поддержка ИБП (UPS)

Управление и мониторинг

- > Централизованное управление шлюзом
- > Удаленное управление шлюзом с помощью SSH-консоли и веб-интерфейса (HTTPS)
- > Ролевая модель доступа – разделение полномочий между несколькими администраторами, аудит действий администраторов
- > Централизованное обновление ключевой информации и конфигурации
- > Мониторинг по протоколам SNMP v1, v2c, v3
- > Автоматическое резервное копирование конфигурации шлюза и экспорт в систему централизованного управления
- > Экспорт системного журнала по протоколу Syslog
- > Экспорт журнала IP-пакетов в формате CEF

Межсетевой экран уровня приложений (DPI)

- > Фильтрация трафика на прикладном уровне модели OSI с помощью технологии DPI с целью отслеживания активности приложений и прикладных протоколов
- > Выявление и блокировка более 2000 прикладных протоколов и приложений
- > Выявление приложений, трафик которых шифруется или маскируется
- > Фильтрация трафика для заданного пользователя (AD, LDAP)

Прокси-сервер

- > Поддержка протокола HTTP
- > Работа в «прозрачном» режиме
- > Кэширование данных
- > Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP
- > Проверка трафика внешним антивирусом по протоколу ICAP

Сетевые функции

- > Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
- > Маршрутизация сетевого трафика на основе:
 - статической маршрутизации
 - динамической маршрутизации (OSPFv2)*
 - политик маршрутизации (policy based routing)
- > Поддержка виртуальных локальных сетей (VLAN 802.1Q)
- > Агрегирование сетевых интерфейсов (802.3ad, LACP)
- > Поддержка Jumbo-кадров и технологии Path MTU Discovery
- > Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)
- > Реализация функций клиента и точки доступа Wi-Fi (для платформ HW50 N2 и HW100 N2)

Сервисные функции

- > DHCP-relay
- > DHCP-сервер
- > DNS-сервер
- > NTP-сервер

* Кроме исполнения HW50

МОДЕЛЬНЫЙ РЯД

HW50 N1-N3



МЭ UDP 1518 байт (Мбит/с)	450	Application Control (МЭ+DPI) (Мбит/с)	25	Количество соединений	150 000
МЭ TCP (Мбит/с)	320	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	-	Сетевые интерфейсы	3 x 1G RJ-45 Wi-Fi (только для N2) 3G (только для N3)
VPN, Мбит/с	70				

HW100 N1-N3



МЭ UDP 1518 байт (Мбит/с)	950	Application Control (МЭ+DPI) (Мбит/с)	85	Количество соединений	150 000
МЭ TCP (Мбит/с)	930	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	15	Сетевые интерфейсы	4 x 1G RJ-45 1 x 1G SFP Wi-Fi (только для N2) 3G (только для N3)
VPN, Мбит/с	160				

HW1000 Q7



МЭ UDP 1518 байт (Мбит/с)	1 900	Application Control (МЭ+DPI) (Мбит/с)	350	Количество соединений	1 000 000
МЭ TCP (Мбит/с)	1 800	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	80	Сетевые интерфейсы	6 x 1G RJ-45
VPN, Мбит/с	915				

HW1000 Q8-Q9



МЭ UDP 1518 байт (Мбит/с)	2 800	Application Control (МЭ+DPI) (Мбит/с)	1 000	Количество соединений	3 000 000
МЭ TCP (Мбит/с)	2 800	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	380	Сетевые интерфейсы	Q8 – 8 x 1G RJ-45 Q9 – 8 x 1G RJ-45 4 x 1G SFP
VPN, Мбит/с	2 500				

HW2000 Q5



МЭ UDP 1518 байт (Мбит/с)	19 000	Application Control (МЭ+DPI) (Мбит/с)	2 600	Количество соединений	5 000 000
МЭ TCP (Мбит/с)	9 300	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	880	Сетевые интерфейсы	4 x 1G RJ-45 4 x 1G SFP 4 x 10G SFP+
VPN, Мбит/с	6 600				

HW5000 Q2



МЭ UDP 1518 байт (Мбит/с)	24 000	Application Control (МЭ+DPI) (Мбит/с)	3 300	Количество соединений	9 900 000
МЭ TCP (Мбит/с)	13 000	NGFW Throughput (МЭ + DPI + IPS) (Мбит/с)	1 000	Сетевые интерфейсы	4 x 1G RJ-45 8 x 10G SFP+
VPN, Мбит/с	10 000				



VIPNet

Coordinator

VA 5

Виртуализированный криптографический
шлюз безопасности – межсетевой экран
нового поколения

ViPNet Coordinator VA 5 – шлюз безопасности в виртуальном исполнении, реализующий концепцию NGFW (Next-Generation Firewall – межсетевой экран нового поколения), который объединяет в одном устройстве следующие функции безопасности, работающие совместно:

- | | |
|---|---|
| 01. Криптографический шлюз, обеспечивающий построение VPN на сетевом (L3) и канальном (L2) уровнях модели OSI | 04. Межсетевой экран уровня приложений DPI (Deep Packet Inspection) |
| 02. Межсетевой экран SPI (Stateful Packet Inspection) | 05. Средство обнаружения и предотвращения вторжений (IDS/IPS) |
| 03. Прокси-сервер | 06. Кластер высокой доступности (HA-cluster) |

Реализованные сетевые функции и сервисы безопасности активируются в соответствии с приобретенной лицензией (лицензируются отдельные модули).

Виртуальный шлюз легко интегрируется в существующую сетевую инфраструктуру и отвечает самым высоким требованиям с точки зрения функциональности, удобства для пользователя, надежности и отказоустойчивости.

ViPNet Coordinator VA 5 обеспечивает безопасность передаваемых данных и многоуровневую защиту виртуальной и облачной инфраструктуры как для частных, так и для публичных облаков, не меняя привычного способа доступа пользователей к бизнес-данным.

ViPNet Coordinator VA 5 представляет собой виртуализированное программное обеспечение, предназначенное для развертывания на популярных платформах виртуализации (KVM, VMware ESXi, Microsoft Hyper-V, Oracle VM).

ЧТО НОВОГО

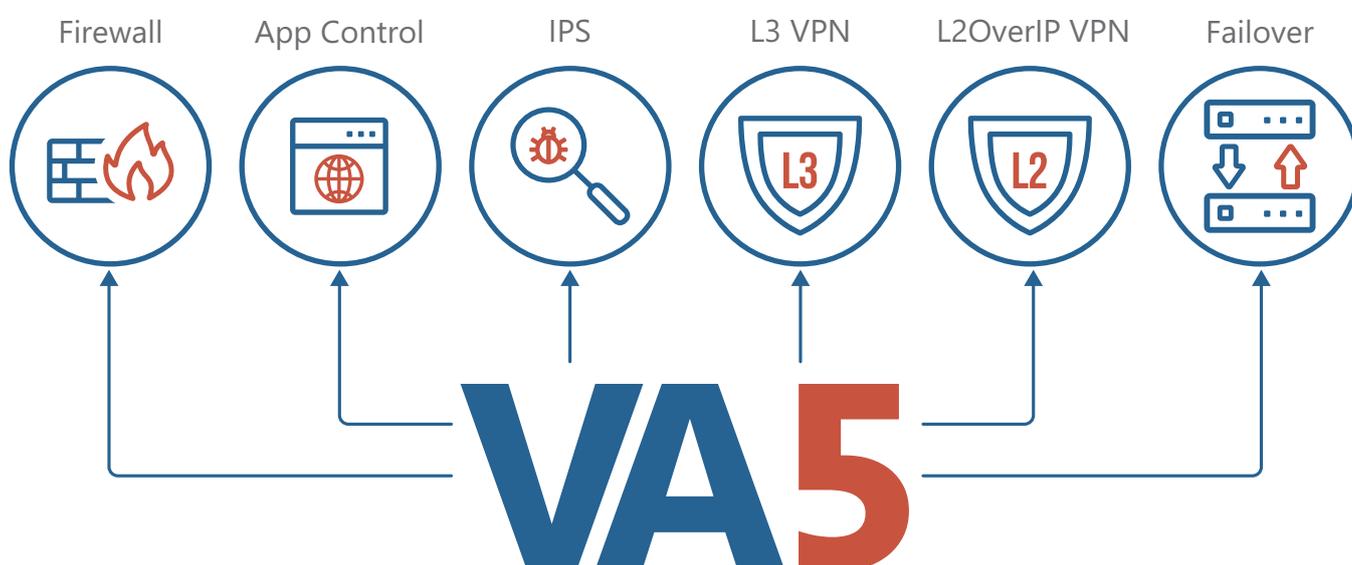
01. Поддержка алгоритмов «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
02. Межсетевой экран уровня приложений (DPI)
03. Многопользовательский ролевой доступ
04. Обнаружение и предотвращение вторжений (IDS/IPS)
05. Подсистема идентификации пользователей (LDAP, Active Directory, Captive Portal)
06. Кластер высокой доступности (HA-cluster) с синхронизацией таблицы открытых соединений
07. Централизованное и удаленное резервное копирование конфигурации

ПРЕИМУЩЕСТВА

- > Удобство управления и скорость развертывания
- > Функциональность, соответствующая аппаратным шлюзам VIPNet Coordinator HW
- > Отсутствие дополнительных затрат на размещение и обслуживание оборудования
- > Поддержка распространенных систем виртуализации
- > Единая система управления для виртуальных и аппаратных шлюзов безопасности
- > Объединение в одном виртуальном устройстве нескольких функций безопасности (FW, DPI, IPS, VPN, Proxy)
- > Гибкая политика лицензирования позволяет приобрести только необходимые функции в зависимости от потребности
- > Централизованное управление шлюзом безопасности с ролевой моделью доступа
- > Гранулированные политики безопасности, которые строятся в терминах «Пользователь» - «Приложение» - «Действие»
- > Обнаружение и нейтрализация сетевых вторжений с использованием встроенной системы предотвращения вторжений (IPS)
- > Обеспечение безопасного использования персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BYOD (Bring Your Own Device)
- > Отказоустойчивый кластер (High-Availability) с синхронизацией сессий позволяет минимизировать время переключения между элементами кластера до 1 секунды
- > Выявление и блокировка более 2000 прикладных протоколов и приложений: игры, социальные сети, torrent и т.д.

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- > Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
- > Защита данных внутри виртуальной и облачной инфраструктуры
- > Защищенный доступ удаленных пользователей
- > Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
- > Обнаружение и нейтрализация сетевых вторжений
- > Комплексная защита от сетевых угроз
- > Защита магистральных каналов, соединяющих ЦОДы между собой
- > Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
- > Взаимодействие с сетями ViPNet других организаций



СЕРТИФИКАЦИЯ

ФСБ России

В процессе сертификации на соответствие требованиям:

- > СКЗИ класса КС1

Свидетельства

В реестре российского ПО

ФСТЭК России

В процессе сертификации на соответствие требованиям:

- > МЭ типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
- > СОВ уровня сети 4 класса защиты (ИТ.СОВ.С4.ПЗ)
- > 4 уровень доверия средств защиты информации

ВОЗМОЖНОСТИ

VPN

- > VPN-шлюз сетевого уровня (L3 VPN)
- > VPN-шлюз канального уровня (L2OverIP VPN)
- > Поддержка криптографических алгоритмов ГОСТ 34.12-2018 «Магма» и «Кузнечик», ГОСТ 28147-89
- > Сервер IP-адресов и маршрутизатор VPN-пакетов
- > Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Межсетевой экран (SPI)

- > Фильтрация трафика на сетевом и транспортном уровнях модели OSI с контролем состояния сессий
- > Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
- > NAT/PAT
- > Антиспуфинг

Межсетевой экран уровня приложений (DPI)

- > Фильтрация трафика на прикладном уровне модели OSI с помощью технологии DPI с целью отслеживания активности приложений и прикладных протоколов
- > Выявление и блокировка более 2000 прикладных протоколов и приложений
- > Выявление приложений, трафик которых шифруется или маскируется
- > Фильтрация трафика для заданного пользователя (AD, LDAP)

Обнаружение и предотвращение вторжений (IPS)

- > Анализ сетевого трафика для защиты от различного вида сетевых атак и вирусов, попыток эксплуатации уязвимостей и получения несанкционированного доступа
- > Работа как в режиме предотвращения вторжений (IPS), так и обнаружения (IDS) с фиксацией событий
- > Сигнатурный и эвристический методы анализа трафика
- > Автоматизированное обновление баз правил с сервера обновлений
- > База правил регулярно обновляется специалистами ГК «ИнфоТеКС» для поддержания в актуальном состоянии

Прокси-сервер

- > Поддержка протокола HTTP
- > Работа в «прозрачном» режиме
- > Кэширование данных
- > Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP
- > Проверка трафика внешним антивирусом по протоколу ICAP

Управление и мониторинг

- > Централизованное управление шлюзом
- > Удаленное управление шлюзом с помощью SSH-консоли и веб-интерфейса (HTTPS)
- > Ролевая модель доступа – разделение полномочий между несколькими администраторами, аудит действий администраторов
- > Централизованное обновление ключевой информации и конфигурации
- > Мониторинг по протоколам SNMP v1, v2c, v3
- > Автоматическое резервное копирование конфигурации шлюза и экспорт в систему централизованного управления
- > Экспорт системного журнала по протоколу Syslog
- > Экспорт журнала IP-пакетов в формате CEF

Сетевые функции

- > Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
- > Маршрутизация сетевого трафика на основе:
 - статической маршрутизации
 - динамической маршрутизации (OSPFv2)
 - политик маршрутизации (policy based routing)
- > Поддержка виртуальных локальных сетей (VLAN 802.1Q)
- > Агрегирование сетевых интерфейсов (802.3ad, LACP)
- > Поддержка Jumbo-кадров и технологии
- > Path MTU Discovery
- > Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

Сервисные функции

- > DHCP-relay
- > DHCP-сервер
- > DNS-сервер
- > NTP-сервер

Идентификация пользователей

- > Интеграция с Microsoft Active Directory
- > Captive Portal и интеграция с LDAP-каталогом

Отказоустойчивость и резервирование

- > Отказоустойчивый кластер высокой доступности по схеме «активный/пассивный» с минимальным временем переключения между элементами кластера (до 1 секунды)
- > Поддержка синхронизации таблицы соединений между элементами кластера
- > Резервирование каналов связи
- > Резервирование сетевых интерфейсов

Тип лицензии	VA100	VA500	VA1000	VA2000	VA5000
Производительность¹					
МЭ UDP 1518 байт, Мбит/с	380	1 500	2 500	5 000	9 500
МЭ UDP 64 байт, пакетов/с	450 000	900 000	1 750 000	2 100 000	3 200 000
МЭ TCP, Мбит/с	360	1 000	2 500	4 500	9 500
Application Control (МЭ+DPI) ² , Мбит/с	300	800	1 800	2 200	2 800
NGFW Throughput (МЭ + DPI + IPS) ³ , Мбит/с	95	250	550	650	925
Количество обслуживаемых соединений	150 000	500 000	2 500 000	5 000 000	10 000 000
L3 VPN, Мбит/с	185	600	1 600	4 000	5 400
L2 VPN, Мбит/с	165	580	1 600	4 000	5 400
Рекомендуемое число связей с ViPNet-узлами	500	2 000	10 000	15 000	16 000
Рекомендуемое число зарегистрированных ViPNet-клиентов	100	500	1000	5000	6 000
Системные требования					
Количество ядер CPU, мин./рек., шт	2 / 4	4 / 4	6 / 8	8 / 12	12 / 16
Оперативная память, мин./рек., Гб	4 / 4	4 / 8	6 / 12	8 / 16	12 / 32
Требования к дисковой подсистеме, Гб	80	80	80	80	80
Сетевые интерфейсы, Гбит/с	1	1	1/10	1/10	1/10
Поддерживаемые среды виртуализации ⁴	<ul style="list-style-type: none"> > KVM, QEMU-KVM и Libvirt > VMware ESXi 6.7/7.0 > VMware Workstation Pro 15.x / 16.x 		<ul style="list-style-type: none"> > Microsoft Hyper-V Server 2016/2019 > Oracle VM Server 3.4 > Oracle VM VirtualBox 6.x 		

¹Условия измерений: VMware ESX 6.7, CPU Xeon E-2278GE, сетевые адаптеры работают в режиме passthrough (DirectPath I/O). Производительность зависит от активированных функций, характеристик обрабатываемого сетевого трафика: протоколов, размера пакетов, количества сессий. Производительность может меняться вследствие изменений, вносимых в новые версии программного обеспечения.

²Результаты получены для трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

³Результаты получены для активированных функций МЭ, DPI, IPS с использованием актуальной на момент теста базы правил IPS при анализе трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

⁴Работа на других платформах виртуализации возможна, но не гарантируется.

HW ViPNet Coordinator HW 4

Криптографический шлюз безопасности для
защиты каналов связи

Благодаря функциям криптографической защиты, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК ViPNet Coordinator HW 4 является оптимальным средством защиты компьютерных сетей организации от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи.

В зависимости от модификации, ПАК ViPNet Coordinator HW 4 позволяет организовать защищенный доступ как в ЦОДы, так и в корпоративную облачную инфраструктуру, может быть использован для защиты филиалов компаний, небольших удаленных офисов, удаленных рабочих мест, а также терминалов и устройств, в том числе обеспечивая безопасное подключение к корпоративной защищенной сети по беспроводным каналам связи.

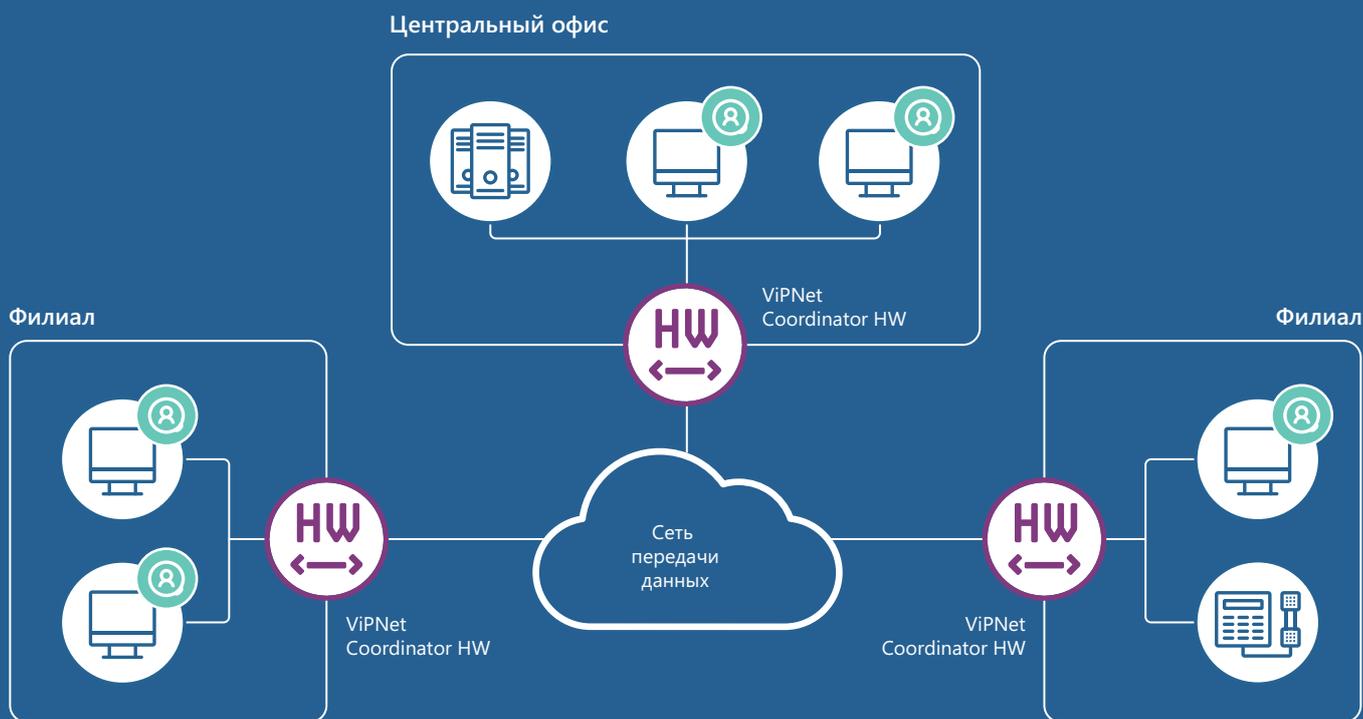
ЧТО НОВОГО

- > Поддержка новых аппаратных платформ HW100 Q1/Q2
- > Работа координаторов через TCP-туннель
- > Управление видимостью узлов ViPNet, расположенных на мобильных устройствах
- > Мониторинг внешних адресов доступа к клиентам сети ViPNet по протоколу SNMP
- > Автоматическое определение провайдера
- > Настройка прямого подключения между клиентами для протоколов SIP и H.323 через веб-интерфейс
- > Настройка маршрутизации транспортных конвертов MFTP между клиентами доверенных сетей
- > Поддержка порта 9443 в прозрачном и непрозрачном режиме работы прокси-сервера на ViPNet Coordinator HW
- > Учет расхода мобильного трафика и настройка SMTP-оповещений

ПРЕИМУЩЕСТВА

01. Организация VPN на сетевом (L3) и канальном уровне (L2)* в одном устройстве
02. Отказоустойчивый кластер (High-Availability cluster) с синхронизацией сессий позволяет минимизировать время переключения между элементами кластера до 1 секунды
03. Работа в необслуживаемом режиме
04. Централизованное и удаленное управление (SSH, WebUI)
05. Поддержка работы в современных мультисервисных сетях связи без ограничений по совместимости:
 - > со службами DHCP, WINS, DNS
 - > с динамическим преобразованием адресов (NAT, PAT)
 - > с использованием мультимедийных протоколов (SIP, H323, SCCP и др.)

*Кроме исполнения HW50



СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

01. Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
02. Защита магистральных каналов
03. Защита беспроводных сетей связи 3G и Wi-Fi
04. Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)
05. Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
06. Защищенный доступ удаленных и мобильных пользователей
07. Взаимодействие с сетями ViPNet других организаций

СЕРТИФИКАЦИЯ

ФСБ России

- > СКЗИ класса КСЗ
- > МЭ 4 класса защищенности

Свидетельства

- > В реестре российского ПО
- > В реестре Минпромторга

ФСТЭК России

- > МЭ типа А 4 класса (ИТ.МЭ.А4.ПЗ)
- > МЭ типа Б 4 класса (ИТ.МЭ.Б4.ПЗ)
- > 4 уровень доверия средств защиты информации

ВОЗМОЖНОСТИ

VPN

- > VPN-шлюз сетевого уровня (L3 VPN)
- > VPN-шлюз канального уровня (L2OverIP VPN)*
- > Сервер IP-адресов*
- > Маршрутизатор VPN-пакетов
- > Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Межсетевой экран

- > Межсетевой экран с контролем состояния сессий
- > Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
- > NAT/PAT
- > Антиспуфинг

Прокси-сервер

- > Поддержка протокола HTTP
- > Работа в «прозрачном» режиме
- > Кэширование данных
- > Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP
- > Проверка трафика сторонним антивирусом по протоколу ICAP

Отказоустойчивость и резервирование

- > Отказоустойчивый кластер высокой доступности по схеме «активный/пассивный» с минимальным временем переключения между элементами кластера (до 1 секунды)
- > Поддержка синхронизации таблицы соединений между элементами кластера
- > Отказоустойчивый кластер горячего резервирования
- > Резервирование каналов связи
- > Резервирование сетевых интерфейсов
- > Поддержка ИБП (UPS)

Сетевые функции

- > Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
- > Маршрутизация сетевого трафика на основе:
 - статической маршрутизации
 - динамической маршрутизации (OSPFv2)*
 - политик маршрутизации (Policy based routing)
- > Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q)
- > Агрегирование сетевых интерфейсов (bonding, EtherChannel, LACP)
- > Поддержка Jumbo-кадров и технологии Path MTU Discovery
- > Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)
- > Реализация функций клиента и точки доступа Wi-Fi (для платформ HW50 N2 и HW100 N2)

Сервисные функции

- > DHCP-сервер
- > DHCP-relay
- > DNS-сервер
- > NTP-сервер

Управление и мониторинг

- > Централизованное управление с помощью ViPNet Administrator и ViPNet Policy Manager
- > Удаленное управление с помощью SSH-консоли и веб-интерфейса (HTTP/HTTPS)
- > Мониторинг по протоколу SNMP v1, v2c, v3
- > Экспорт системного журнала по протоколу Syslog
- > Экспорт журнала IP-пакетов в формате CEF

*Кроме исполнения HW50

МОДЕЛЬНЫЙ РЯД

HW50 N1-N3



VPN, Мбит/с	75	Количество соединений	150 000
МЭ, Мбит/с	320	Сетевые интерфейсы	3 x 1G RJ-45 Wi-Fi (только для N2) 3G (только для N3)

HW100 N1-N3



VPN, Мбит/с	175	Количество соединений	150 000
МЭ, Мбит/с	930	Сетевые интерфейсы	4 x 1G RJ-45 1 x 1G SFP Wi-Fi (только для N2) 3G (только для N3)

HW100 Q1-Q2



VPN, Мбит/с	400	Количество соединений	150 000
МЭ, Мбит/с	1400	Сетевые интерфейсы	4 x 1G RJ-45 2 x 1G SFP

HW1000

Q7-Q9



VPN, Мбит/с	Q7 – 915 Q8 – 2 500 Q9 – 2 500	Количество соединений	1 000 000
МЭ, Мбит/с	Q7 – 2 500 Q8 – 2 800 Q9 – 2 800	Сетевые интерфейсы	Q7 – 6 x 1G RJ-45 Q8 – 8 x 1G RJ-45 Q9 – 8 x 1G RJ-45 4 x 1G SFP

HW2000

Q5



VPN, Мбит/с	L3 – 6 600 L2 – 6 000	Количество соединений	3 000 000
МЭ, Мбит/с	9 200	Сетевые интерфейсы	4 x 1G RJ-45 4 x 1G SFP 4 x 10G SFP+

HW5000

Q2



VPN, Мбит/с	10 000	Количество соединений	6 500 000
МЭ, Мбит/с	13 000	Сетевые интерфейсы	4 x 1G RJ-45 8 x 10G SFP+



VIPNet

Coordinator

VA 4

Виртуализированный криптографический
шлюз безопасности

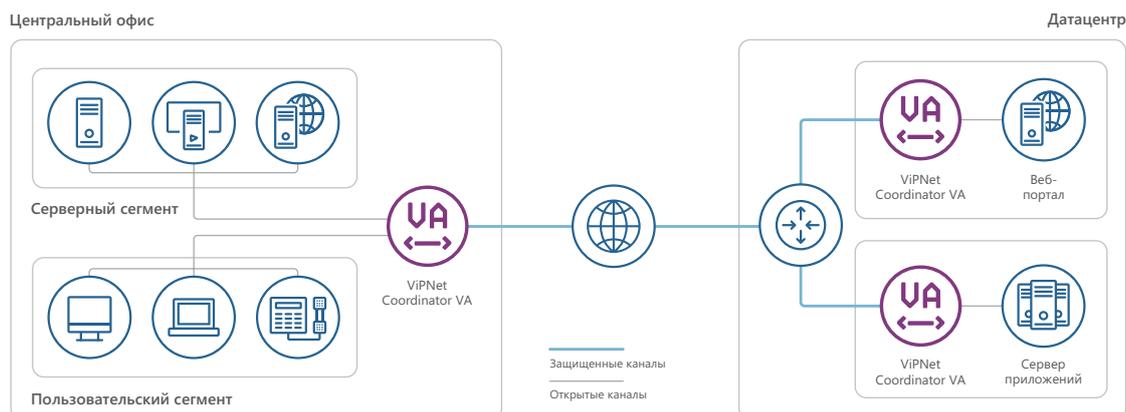
Виртуальный шлюз легко интегрируется в существующую сетевую инфраструктуру и отвечает самым высоким требованиям с точки зрения функциональности, удобства для пользователя, надежности и отказоустойчивости.

ViPNet Coordinator VA обеспечивает безопасность передаваемых данных и многоуровневую защиту виртуальной и облачной инфраструктуры как для частных, так и для публичных облаков, не меняя привычного способа доступа пользователей к бизнес-данным.

ViPNet Coordinator VA представляет собой виртуализированное программное обеспечение, которое предназначено для развертывания на популярных платформах виртуализации (KVM, VMware ESXi, Microsoft Hyper-V, Oracle VM).

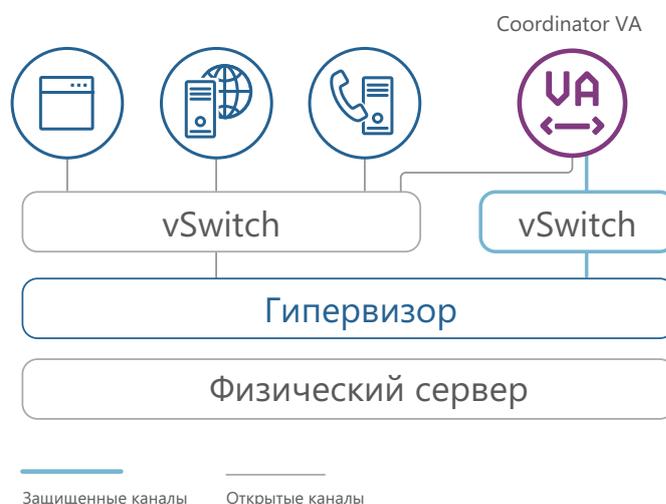
ПРЕИМУЩЕСТВА

- > Удобство управления и скорость развертывания
- > Функциональность, соответствующая аппаратным шлюзам ViPNet Coordinator HW
- > Отсутствие дополнительных затрат на размещение и обслуживание оборудования
- > Единая система управления для виртуальных и аппаратных шлюзов безопасности
- > Отказоустойчивый кластер (High-Availability cluster) с синхронизацией сессий позволяет минимизировать время переключения между элементами кластера до 1 секунды
- > Поддержка распространенных систем виртуализации
- > Гибкое лицензирование и быстрое масштабирование
- > Организация VPN на сетевом (L3) и канальном уровне (L2) в одном виртуальном устройстве



СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

01. Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
02. Защита магистральных каналов связи
03. Разграничение доступа к информации в локальных сетях, сегментирование локальных сетей (например, выделение ДМЗ)
04. Защита данных внутри виртуальной и облачной инфраструктуры
05. Взаимодействие с сетями ViPNet других организаций
06. Защищенный доступ удаленных и мобильных пользователей
07. Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)



ВОЗМОЖНОСТИ

VPN

- > VPN-шлюз сетевого уровня (L3 VPN)
- > VPN-шлюз канального уровня (L2OverIP VPN)
- > Сервер IP-адресов
- > Маршрутизатор VPN-пакетов
- > Маскирование структуры трафика за счет инкапсуляции в UDP, TCP

Сетевые функции

- > Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
- > Маршрутизация сетевого трафика на основе:
 - статической маршрутизации
 - динамической маршрутизации (OSPFv2)
 - политик маршрутизации (Policy based routing)
- > Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q)
- > Агрегирование сетевых интерфейсов (bonding, EtherChannel, LACP)
- > Поддержка Jumbo-кадров и технологии Path MTU Discovery
- > Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

Межсетевой экран

- > Межсетевой экран с контролем состояния сессий
- > Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
- > NAT/PAT
- > Антиспуфинг

Прокси-сервер

- > Поддержка протокола HTTP
- > Работа в «прозрачном» режиме
- > Кэширование данных
- > Проверка и фильтрация трафика по разным типам содержимого, передаваемого в протоколе HTTP
- > Проверка трафика сторонним антивирусом по протоколу ICAP

Сервисные функции

- > DHCP-сервер
- > DHCP-relay
- > DNS-сервер
- > NTP-сервер

Отказоустойчивость и резервирование

- > Отказоустойчивый кластер высокой доступности по схеме «активный/пассивный» с минимальным временем переключения между элементами кластера (до 1 секунды)
- > Поддержка синхронизации таблицы соединений между элементами кластера
- > Резервирование сетевых интерфейсов как на уровне гипервизора, так и на уровне отдельных виртуальных машин
- > Легкое восстановление конфигурации с помощью штатных средств гипервизора – резервных копий и снимков (снапшотов)

Управление и мониторинг

- > Централизованное управление с помощью ViPNet Administrator и ViPNet Policy Manager
- > Удаленное управление с помощью SSH-консоли и веб-интерфейса (HTTP/HTTPS)
- > Мониторинг по протоколу SNMP v1, v2c, v3
- > Экспорт системного журнала по протоколу Syslog
- > Экспорт журнала IP-пакетов в формате CEF

Тип лицензии	VA100	VA500	VA1000	VA2000
--------------	-------	-------	--------	--------

Производительность¹

L3 VPN, Мбит/с	185	600	1 900	4 500
L2 VPN, Мбит/с	180	585	1 900	4 500
МЭ, Мбит/с	360	1 000	3 500	5 500
Количество обслуживаемых соединений	150 000	500 000	1 000 000	3 000 000
Рекомендуемое число зарегистрированных ViPNet-клиентов	100	500	1 000	2 000

Системные требования

Количество ядер CPU, шт.	2	2	4	8
Оперативная память, Гб	2	2	4	8
Требования к дисковой подсистеме, Гб	80	80	80	80
Сетевые интерфейсы, Гбит/с	1	1	1/10	1/10

Поддерживаемые среды виртуализации²

- > VMware ESXi 6.7/7.0
- > VMware Workstation Pro 15.x / 16.x
- > Microsoft Hyper-V Server 2019
- > KVM, например Qemu-KVM или Proxmox
- > Oracle VM VirtualBox 6.x
- > Oracle VM Server 3.4

¹Условия измерений: VMware ESX 6.7, CPU Xeon E-2278GE, сетевые адаптеры работают в режиме passthrough (DirectPath I/O). Производительность зависит от активированных функций, характеристик обрабатываемого сетевого трафика: протоколов, размера пакетов, количества сессий. Производительность может меняться вследствие изменений, вносимых в новые версии программного обеспечения.

²Работа на других платформах виртуализации возможна, но не гарантируется.

СЕРТИФИКАЦИЯ**ФСБ России**

- > СКЗИ класса КС1

ФСТЭК России

- > МЭ типа Б 4 класса защищенности (ИТ.МЭ.Б4.ПЗ)
- > 4 уровень доверия средств защиты информации

Свидетельства

- > В реестре российского ПО

KB **↔** **VIPNet** **Coordinator** **KB**

Шлюз безопасности для защиты каналов
связи по классу KB

Программно-аппаратный комплекс (ПАК) ViPNet Coordinator KB является шлюзом безопасности, предназначенным для организации защищенных каналов связи по классу KB

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- > Построение защищенных каналов связи между объектами организации (Site-to-Site и Multi Site-to-Site)
- > Защита магистральных каналов, соединяющих ЦОДы между собой
- > Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)

ПРЕИМУЩЕСТВА

01. Высокая скорость шифрования (до 7,2 Гбит/с)
02. Шифрование трафика на сетевом (L3) и канальном уровне (L2) модели OSI
03. Построение защищенных каналов связи как Site-to-Site VPN, так и Multi Site-to-Site VPN
04. Возможность создания кластера горячего резервирования
05. Экстренное удаление ключевой информации по нажатию специальной кнопки
06. Встроенный датчик несанкционированного доступа
07. Поддержка работы в современных мультисервисных сетях связи без ограничений по совместимости:
 - > со службами DHCP, WINS, DNS
 - > с динамическим преобразованием адресов (NAT, PAT)
 - > с использованием мультимедийных протоколов (SIP, H323, SCCP и другие)

МОДЕЛЬНЫЙ РЯД

KB100 N1



VPN, Мбит/с	140	Сетевые интерфейсы	4x 1G RJ-45 1x 1G SFP
МЭ, Мбит/с	910	Количество соединений	150 000

KB1000 Q8



VPN, Мбит/с	L3 – 1 600 L2 – 1 400	Сетевые интерфейсы	4x 1G RJ-45 2x 1G SFP
МЭ, Мбит/с	1 800	Количество соединений	4 000 000

KB2000 Q5



VPN, Мбит/с	5 500	Сетевые интерфейсы	4x 1G RJ-45 4x 10G SFP+
МЭ, Мбит/с	9 200	Количество соединений	8 000 000

KB5000 Q2



VPN, Мбит/с	7 200	Сетевые интерфейсы	4x 1G RJ-45 4x 10G SFP+
МЭ, Мбит/с	9 200	Количество соединений	16 000 000

ВОЗМОЖНОСТИ

VPN

- > VPN-шлюз сетевого уровня (L3 VPN)
- > VPN-шлюз канального уровня (L2OverIP VPN)
- > Сервер IP-адресов
- > Маршрутизатор VPN-пакетов
- > Маскирование структуры трафика за счет инкапсуляции в UDP

Межсетевой экран

- > Межсетевой экран с контролем состояния сессий
- > Раздельная настройка фильтрации для открытого и шифруемого IP-трафика
- > NAT/PAT
- > Антиспуфинг

Управление и мониторинг

- > Централизованное управление с помощью ViPNet Administrator и ViPNet Policy Manager
- > Удаленное управление с помощью SSH-консоли и веб-интерфейса
- > Мониторинг по протоколу SNMP
- > Аутентификация с помощью внешних носителей (Рутокен ЭЦП 2.0, Рутокен Lite, JaCarta ГОСТ, JaCarta-2 ГОСТ)

Отказоустойчивость и резервирование

- > Отказоустойчивый кластер горячего резервирования
- > Резервирование каналов связи
- > Резервирование сетевых интерфейсов
- > Поддержка ИБП (UPS)

Сервисные функции

- > DNS-сервер
- > NTP-сервер
- > DHCP-сервер
- > DHCP-relay
- > Поддержка ИБП (UPS)
- > Отказоустойчивый кластер горячего резервирования

Сетевые функции

- > Резервирование и балансировка каналов связи: WAN (балансировка и резервирование), VPN (резервирование)
- > Маршрутизация сетевого трафика на основе:
 - статической маршрутизации
 - динамической маршрутизации
 - политик маршрутизации (Policy based routing)
- > Поддержка виртуальных локальных сетей (VLAN IEEE 802.1Q)
- > Агрегирование сетевых интерфейсов (bonding, EtherChannel, LACP)
- > Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

СЕРТИФИКАЦИЯ

ФСБ России

- > СКЗИ класса KB
- > МЭ 4 класса защищенности

Свидетельства

- > В реестре российского ПО
- > В реестре Минпромторга

VIPNet Coordinator IG

Программно-аппаратный комплекс (ПАК) VIPNet Coordinator IG является российским индустриальным шлюзом безопасности, предназначенным для организации защищенных каналов связи и предотвращения несанкционированного доступа к объектам защиты

ПАК ViPNet Coordinator IG может быть использован:

01. Для защиты информации на всех уровнях значимых и незначимых объектов АСУ КИИ
02. Для защиты информации на всех уровнях АСУ ТП
03. Для защиты данных информационных систем и информационно-телекоммуникационных сетей, в том числе значимых и незначимых объектов КИИ, где необходимо размещение СЗИ при высоких и низких температурах или есть расширенные требования к среде эксплуатации

СЦЕНАРИИ

- > Сегментирование сети и разграничение доступа к ее сегментам
- > Защита проводных и беспроводных каналов связи сети
- > Организация защищенных каналов связи между сегментами сети
- > Организация защищенного удаленного доступа для мобильных пользователей
- > Организация ДМЗ
- > Организация защищенного удаленного мониторинга
- > Организация защищенного удаленного сервисного обслуживания
- > Организация защищенного подключения оборудования по последовательным интерфейсам

ПРЕИМУЩЕСТВА

- > Защита проводных и беспроводных каналов связи
- > Ограничение трафика на уровне разрешения определенных промышленных протоколов
- > Возможность запрета использования сервисных функций для определенных режимов функционирования объекта
- > Сужение векторов атак за счет глубокой фильтрации промышленных протоколов
- > Возможность использования «старых» устройств в системе за счет организации защиты информации при подключении по интерфейсам RS-232 и RS-485
- > Дистанционное конфигурирование и управление политиками безопасности
- > Работа в режиме горячего резервирования и возможность организации резервирования каналов связи
- > Индустриальный дизайн и возможность использования в жестких условиях эксплуатации
- > Возможность построения сквозной безопасности предприятия от ERP-уровня до нижнего уровня АСУ и АСУ ТП на основе единой технологии ViPNet VPN с помощью линейки продуктов ViPNet Channel Protection
- > Защита объекта при подключении к сетям связи общего пользования одним устройством
- > Произведено в России

ВОЗМОЖНОСТИ

VPN

- > ViPNet VPN-шлюз сетевого уровня (L3 VPN)
- > ViPNet VPN-шлюз канального уровня (L2OverIP VPN)
- > Скрытие структуры трафика за счет инкапсуляции в UDP, TCP

Межсетевой экран

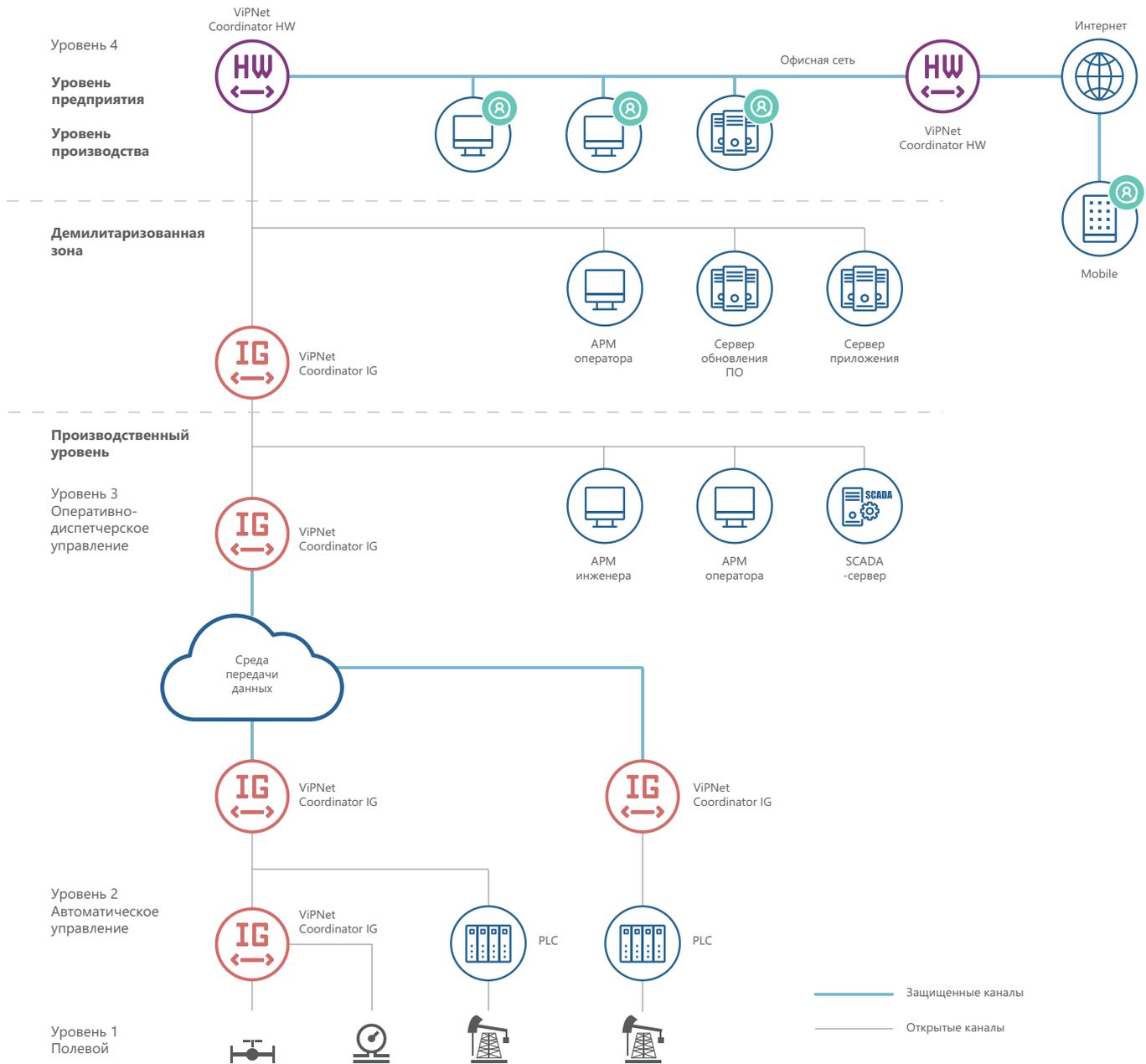
- > Межсетевой экран с контролем состояния сессий
- > Раздельная настройка правил фильтрации для открытого и шифруемого IP-трафика
- > Раздельная настройка правил фильтрации для режимов работы промышленного МЭ: штатный режим, регламентное обслуживание, специальный режим
- > NAT/PAT
- > Фильтрация промышленных протоколов Modbus, Profinet, МЭК 60870-5-104, Ethernet/IP, OPC UA, MMS, DNP3
- > Глубокая фильтрация протокола Modbus, МЭК-60870-5-104
- > Антиспуфинг
- > Прокси-сервер

Сервисные функции

- > DNS-сервер
- > NTP-сервер
- > DHCP-сервер и DHCP-relay
- > Кластер горячего резервирования
- > Dead Gateway Detection (DGD) и MultiWAN
- > Резервирование каналов

Сетевые функции

- > Статическая маршрутизация
- > Динамическая маршрутизация
- > Поддержка VLAN (dot1q)
- > Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)
- > Агрегирование интерфейсов (EtherChannel (LACP))
- > Преобразователь протоколов Modbus TCP/RTU



СЕРТИФИКАЦИЯ

ФСБ России

- > СКЗИ класса КСЗ
- > МЭ 4 класса защищенности

ФСТЭК России

- > МЭ типов А,Б,Д 4 класса защиты
- > 4 уровень доверия средств защиты информации

МИНЦИФРЫ

Включен в реестр Российского ПО

МИНПРОМТОРГ России

Включен в единый реестр РЭП

РОСАККРЕДИТАЦИЯ

Декларация соответствия ТР/ТС 020/2011 на ЭМС по промышленным стандартам

МОДЕЛЬНЫЙ РЯД



IG10 I1, IG100 I1

Порты USB	2 x USB 2.0	RS-232/RS-485	+ (совмещенный)
GPIO	1 x In, 1 x Out	Разъем для SIM-карты	1
Порты Ethernet	WAN: 1 x 10/100Base-T LAN: 2 x 10/100Base-T	Беспроводные интерфейсы	Wi-Fi, 3G, 4G с выносной антенной (опционально)

IG100 I4

Порты USB	2 x USB 2.0	RS-232/ RS-485	+
GPIO	1 x In, 1 x Out	Разъем для SIM-карты	2
Порты Ethernet	WAN: 2 x 10/100/1000Base-T или 2 x 10/100/1000Base-X SFP LAN: 3 x 10/100/1000Base-T	Беспроводные интерфейсы	Wi-Fi, 3G, 4G с выносной антенной (опционально)



IG100 I5

Порты USB	2 x USB 2.0	RS-232/ RS-485	+ (совмещенный)
GPIO	1 x In, 1 x Out	Разъем для SIM-карты	1
Порты Ethernet	WAN: 1 x 10/100BASE-T с возможностью получать питание по стандартам IEEE 802.3af и IEEE 802.3at (PoE) LAN: 2 x 10/100BASE-T с возможностью питать PoE-устройства по стандартам IEEE 802.3af и IEEE 802.3at	Беспроводные интерфейсы	Wi-Fi, 3G, 4G с выносной антенной (опционально)

Аппаратные**характеристики****ViPNet Coordinator IG10****ViPNet Coordinator IG100**

Аппаратная платформа	IG10 I1	IG10 I2	IG100 I1	IG100 I4	IG100 I5
Форм-фактор	Блок с креплением на DIN-рейку				
Размеры (Ш x В x Г), мм	52 x 132 x 120	69 x 157 x 122	52 x 132 x 120	100 x 172 x 120	55 x 169 x 126
Вес, кг	Не более 0,65	Не более 1,5	Не более 0,65	Не более 1,8	Не более 1
Питание	12 - 24 В DC	12 - 24 В DC 2 порта	12 - 24 В DC	12 - 24 В DC 2 порта	Через порт питания – 12 - 24 В DC (при подключении PoE-устройств – 24 В) Через порт WAN по технологии PoE
Потребляемая мощность, Вт	Не более 10	Не более 15	Не более 10	Не более 30	С беспроводными модулями, но без подключенных USB- устройств: > не более 15 – без PoE-устройств > не более 30 – с PoE- устройствами и питанием по PoE (4 класс мощности) > не более 95 – с PoE- устройствами и питанием от блока питания
Питание от PoE	-	-	-	-	+
Рабочая температура	-40° до +60° С ¹	-40° до +60° С ¹	-20° до +60° С ¹	-40° до +60° С ¹	-20° до +60°С ¹
Электромагнитная совместимость (EMI)	ГОСТ Р 51318-22 (CISPR 22), ГОСТ CISPR 24 2013 (CISPR 24)	ГОСТ 30805.22-2013 (CISPR.22:2006), ГОСТ 30804.6.2-2013 (IEC 61000-6-2:2005), ГОСТ CISPR 24 2013 (CISPR 24), ГОСТ Р 51317.6.5-2006 (МЭК 61000-6-5:2001)	ГОСТ Р 51318-22 (CISPR 22), ГОСТ CISPR 24 2013 (CISPR 24)	ГОСТ Р 51318-22 (CISPR 22), ГОСТ CISPR 24 2013 (CISPR 24)	ГОСТ 30804.6.4 – 2013 ГОСТ 30805.22-2013 (CISPR 22:2006) для устройств класса А ГОСТ CISPR 24-2013 ГОСТ 30804.6.2-2013 (IEC 61000-6-2:2005)
Класс защиты IP	IP30				

Межсетевой экран (МЭ)

Производительность МЭ, Мбит/с	10	10	60	160	60
Максимальное количество одновременных сессий	до 1000	до 1000	до 15000	до 100000	до 15000
Межсетевой экран глубокой фильтрации (DPI)	Modbus TCP, МЭК-60870-5-104				

VPN

Пропускная производительность VPN L3 и L2 на проводном канале ² , Мбит/с	10	10	60	160	60
Максимальное количество узлов, туннелируемое координатором	Не ограничено				
Рекомендуемое число зарегистрированных VPN-клиентов ³	Недоступно	Недоступно	до 10 ⁴	до 10 ⁴	до 10 ⁴

¹Исполнение с беспроводными модулями от -20° до +60°С²Указана максимальная пропускная производительность. Реальная производительность зависит от среды передачи данных и технической реализации³Только для узлов со следующими версиями ПО: ViPNet Client for Windows 4.3.2, 4.5.1, ViPNet Client for Linux 4.6.0 и выше, ViPNet Client for Android 2.12, ViPNet Client for iOS 2.16 и выше; ViPNet Client 4U⁴Не поддерживает «Деловую почту» и «Фаловый обмен» для ViPNet Client for Windows, а также ViPNet Connect



VIPNet xFirewall

ПАК VIPNet xFirewall – это шлюз безопасности – межсетевой экран нового поколения (NGFW), сочетающий функции классического меж сетевого экрана: анализ состояния сессии, проксирование, трансляция адресов; с расширенными функциями анализа и фильтрации трафика, такими как: глубокая инспекция протоколов, выявление и предотвращение компьютерных атак, инспекция SSL/TLS-трафика, взаимодействие с антивирусными решениями, DLP и песочницами

ViPNet xFirewall устанавливается на границе сети, предназначен для комплексного решения задач информационной безопасности в корпоративных сетях, позволяет создать гранулированную политику безопасности на основе учетных записей пользователей и списка приложений, обеспечивает обнаружение и нейтрализацию сетевых вторжений.

ПРЕИМУЩЕСТВА

01. Гранулированная политика безопасности, которая строится в терминах «Пользователь» - «Приложение» - разрешить/запретить
02. Обеспечение безопасного использования персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BYOD (Bring Your Own Device)
03. Выявление и блокировка более 5000 прикладных протоколов и приложений: игры, социальные сети, torrent и т.д.
 - > Снижение расходов на потребление интернет-трафика
 - > Минимизация поверхности атак
04. Обнаружение и нейтрализация сетевых вторжений с использованием встроенной системы предотвращения вторжений (IPS)
05. Инспекция SSL/TLS-трафика средствами глубокой инспекции протоколов, системой предотвращения атак, антивирусными решениями и контентной фильтрацией

СЕРТИФИКАЦИЯ

ФСТЭК России

Соответствует:

- > Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) – по 4 уровню доверия
- > Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профилю защиты межсетевых экранов типа А 4 класса защиты. ИТ.МЭ.А4.ПЗ» (ФСТЭК России, 2016)
- > Требованиям к межсетевым экранам» (ФСТЭК России, 2016), «Профилю защиты межсетевых экранов типа Б 4 класса защиты. ИТ.МЭ.Б4.ПЗ» (ФСТЭК России, 2016)
- > Требованиям к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профилю защиты систем обнаружения вторжений уровня сети 4 класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012)

Свидетельства

- > В реестре российского ПО
- > В реестре Минпромторга

ВОЗМОЖНОСТИ

Межсетевой экран

> Межсетевой экран с контролем состояния сессий

> Трансляция адресов NAT/PAT

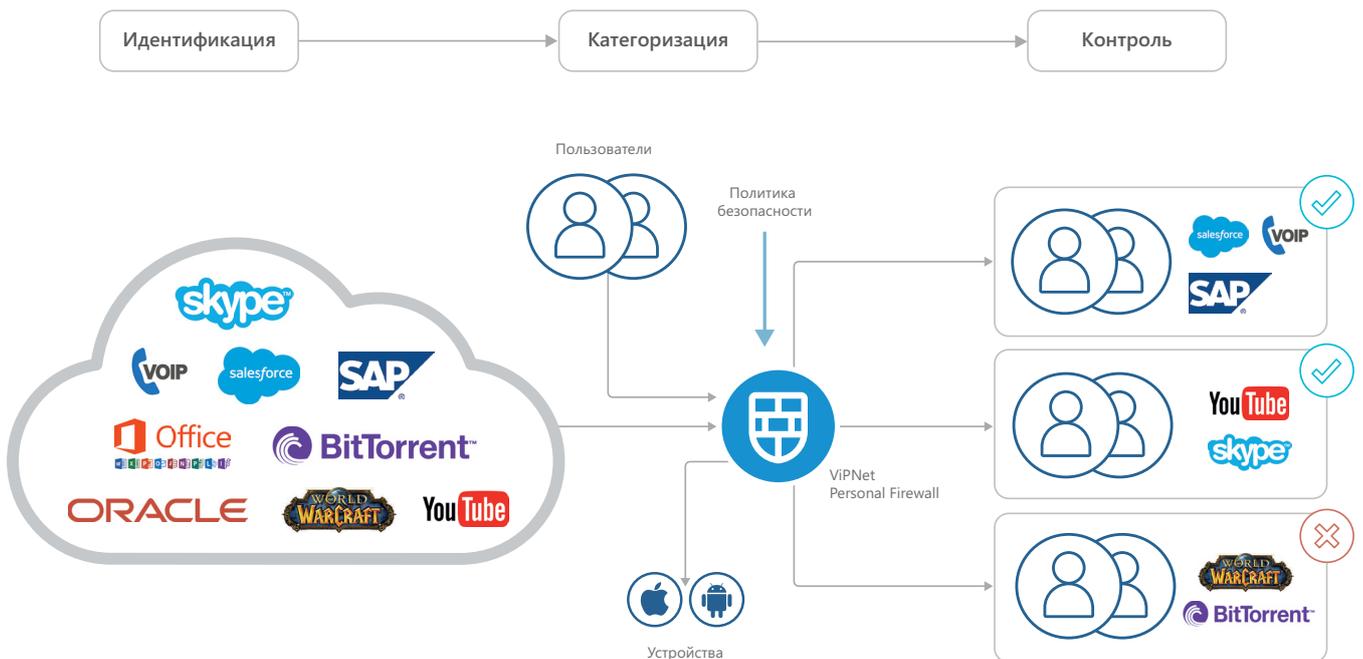
> Защита от атак Antispoofing

Межсетевое экранирование уровня приложений – глубокая инспекция протоколов (DPI – deep packet inspection)

> Выявление и блокировка более 5000 прикладных протоколов и приложений, среди которых:

Игры
Социальные сети
Сервисы мгновенных сообщений
Видеотрансляции

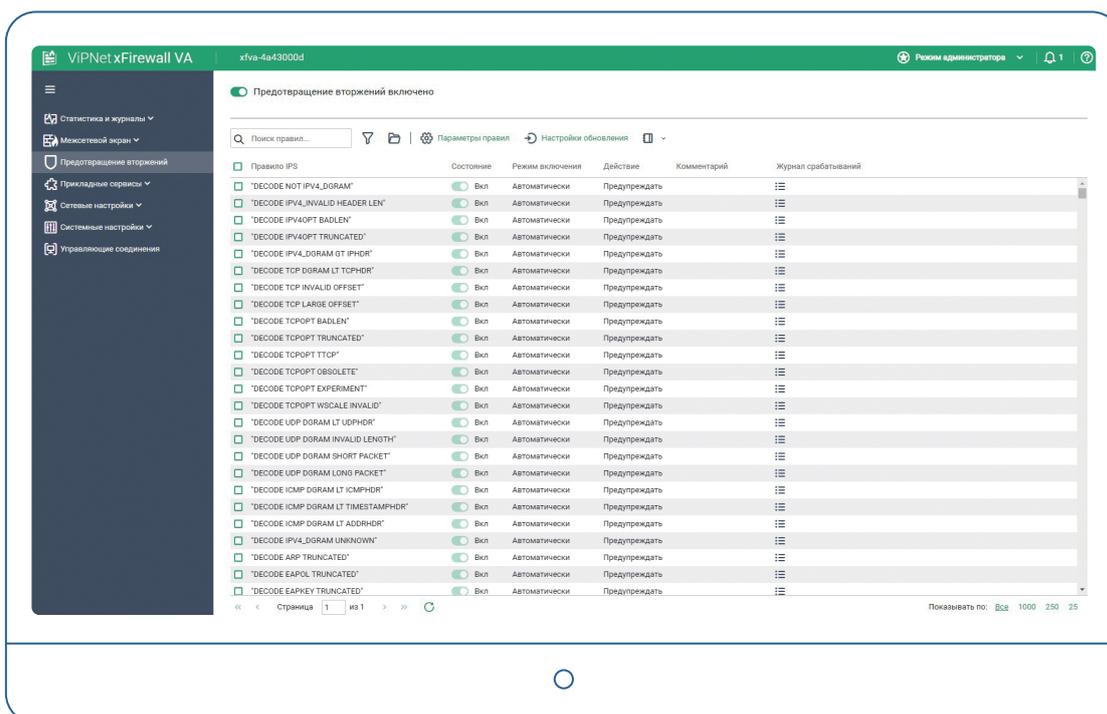
Сервисы P2P, torrent
Хостинг файлов
Туннелирование, VPN
Удаленное управление
Промышленные протоколы



DPI (Deep Packet Inspection) – механизм глубокой инспекции протоколов. DPI использует различные техники идентификации трафика пользовательских приложений: на основе портов и протоколов, сигнатурный метод, эвристический метод. Эти подходы позволяют выявить даже те приложения, трафик которых шифруется или маскируется.

Система предотвращения вторжений (IPS – intrusion prevention system)

- > Сигнатурный метод анализа трафика
- > Эвристический метод анализа трафика
- > База правил, содержащая описания сетевых угроз, регулярно обновляется специалистами ИнфоТеКС для поддержания в актуальном состоянии



При обнаружении характерных признаков вторжения (срабатывании правила IPS) возможны следующие действия с IP-пакетом:

- > IP-пакет пропускается для дальнейшей обработки с предупреждением
- > IP-пакет блокируется межсетевым экраном ViPNet xFirewall

Сетевые функции

- > Развитая статическая маршрутизация
- > Динамическая маршрутизация
- > Поддержка VLAN (dot1q)
- > Агрегирование каналов связи (bonding (LACP), EtherChannel)
- > Поддержка QoS, ToS, DiffServ

Сервисные функции

- > DNS-сервер
- > DHCP-сервер
- > NTP-сервер
- > DHCP-relay

Отказоустойчивость и резервирование

- > Кластер горячего резервирования – failover
- > Поддержка ИБП (UPS)

Инспекция SSL/TLS-трафика

Корневой сертификат MCЭ (Firewall)



Клиент подтверждает корневой сертификат MCЭ



- > Классификация SSL/TLS-трафика, выявление и выборочная фильтрация трафика приложений
- > URL- и контент-фильтрация HTTP(S)-трафика

- > Исследование содержимого SSL/TLS-сессий средствами DPI и IPS
- > Выявление и блокировка вирусов и вредоносного ПО в HTTP(S)-трафике

Инспекция SSL/TLS подразумевает два шага:

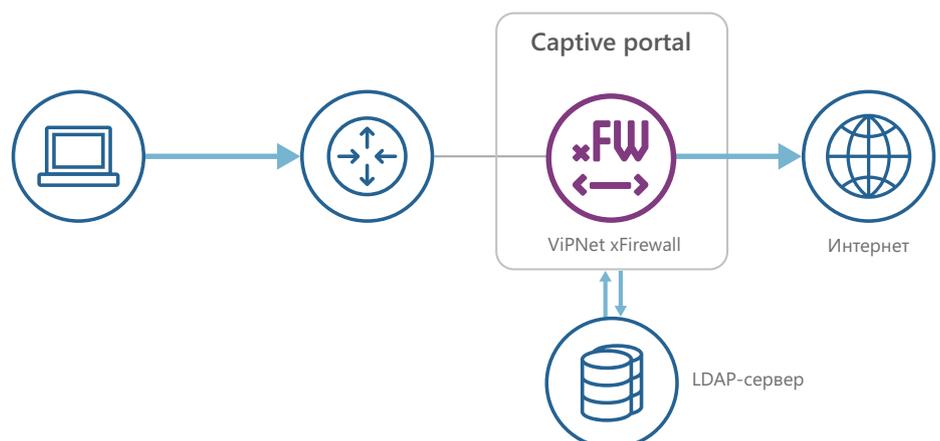
01. SSL decryption – расшифровывание SSL-трафика, проходящего через межсетевой экран

02. Анализ содержимого SSL-трафика

Расшифровывание SSL-трафика в ViPNet xFirewall реализовано по принципу проксирования – forward proxy decryption. Все стадии этого процесса схематично изображены на рисунке выше.

Интеграция с каталогами справочников

- > Microsoft AD
- > Captive Portal с LDAP-каталогом



VIPNet **L2-10G**

ПАК VIPNet L2-10G – шлюз безопасности, обеспечивающий криптографическую защиту данных, передаваемых по каналам Ethernet: темная оптика, MAN, WAN, выделенный канал.

VIPNet L2-10G обеспечивает высокую производительность и сверхнизкие задержки, благодаря чему является идеальным решением для реализации защиты критических сервисов, чувствительных к задержкам и пропускной способности канала связи, а также является эффективным средством защиты каналов связи между ЦОДами

ПАК ViPNet L2-10G представляет собой устройство 1U, корпус которого спроектирован с учетом жестких требований безопасного функционирования: защита от несанкционированного вскрытия, энергонезависимое хранилище ключей шифрования, резервирование электропитания

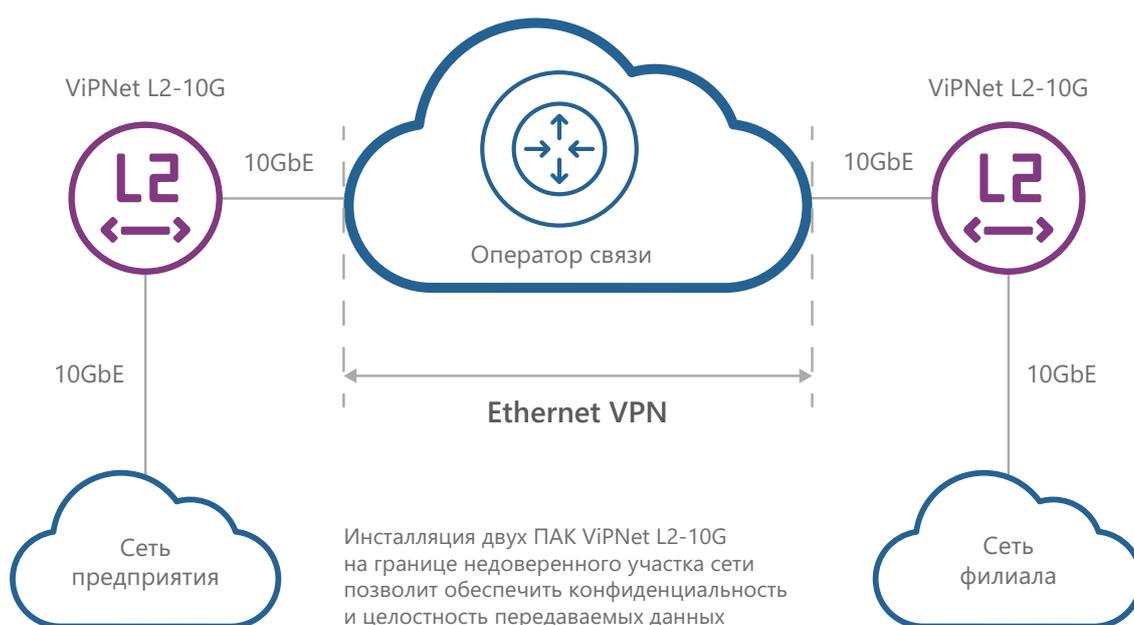
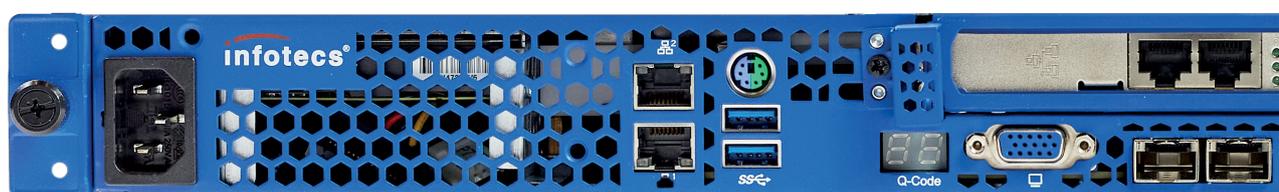


Схема подключения филиала к основной сети предприятия через выделенный Ethernet-канал оператора связи



ВОЗМОЖНОСТИ

ПАК ViPNet L2-10G имеет два порта 10G стандарта SFP+: один внутренний – для подключения в локальную сеть, второй внешний – для подключения в линию оператора связи. Все Ethernet-кадры, пришедшие на внутренний порт, зашифровываются и отправляются во внешний порт, соответственно, Ethernet-кадры, пришедшие на внешний порт, расшифровываются и перенаправляются на внутренний порт.

Для ПАК ViPNet L2-10G разработан специальный протокол шифрования Ethernet-кадров, который обеспечивает надежную криптографическую защиту данных при минимальных накладных расходах:

- > минимальная избыточность – не более 12 байт
- > средняя задержка – менее 3 мкс

ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

Сетевые особенности

- > Топология шифраторов «точка-точка»
- > Поддержка Jumbo frames – до 9000 байт
- > Прозрачен для сетевых протоколов и приложений
- > Unicast-, Multicast-и Broadcast-трафик
- > Автоматическое определение и соединение сопряженных шифраторов
- > Минимальная избыточность протокола защиты

Защита от НСД

- > Энергонезависимое уничтожение ключевой информации при вскрытии корпуса или команде оператора

Алгоритм и сертификация

- > Блочный шифр «Кузнечик» согласно ГОСТ Р 34.12-2015
- > Защита от атак типа «повтор ранее записанных кадров»
- > Сертификат соответствия ФСБ России № СФ/124-4266. Сертификат удостоверяет, что программно-аппаратный комплекс ViPNet L2-10G соответствует требованиям к средствам криптографической защиты информации класса КВ.

Производительность

- > Сверхнизкая задержка – менее 3 мкс
- > Производительность – до 20 Гбит/с (10G Ethernet full-duplex)

Управление

- > Локальный порт управления USB-UART
- > Интерфейс удаленного управления Ethernet 10/100/1000
- > Удаленное управление по протоколу SSH

СЕРТИФИКАЦИЯ

Сертификат соответствия ФСБ России № СФ/124-4266

Сертификат удостоверяет, что программно-аппаратный комплекс ViPNet L2-10G соответствует требованиям к средствам криптографической защиты информации класса КВ.

The icon consists of the letters 'TLS' in a bold, sans-serif font, positioned above a rounded rectangular shape containing three small circles, resembling a network or communication symbol.

VIPNet TLS Gateway

Шлюз безопасности, предназначенный
для организации защищенных
соединений по протоколу TLS
с использованием отечественных
и иностранных криптоалгоритмов

ВОЗМОЖНОСТИ

- > Защищенный доступ к ресурсам по HTTPS
- > Организация TLS-туннеля для защищенного доступа к ресурсам по TCP
- > Интеграция с LDAP (Active Directory)
- > Поддержка режимов односторонней и двусторонней аутентификации с использованием сертификатов, изданных различными удостоверяющими центрами (в т.ч. аккредитованными)
- > Поддержка аутентификации по протоколам NTLM
- > Поддержка политик разграничения доступа по IP-адресам и данным из сертификатов
- > Возможность организации доступа к защищаемым ресурсам с использованием российских и/или иностранных криптоалгоритмов
- > Автоматическое поддержание актуальности списков аннулированных сертификатов (CRL), возможность использования протокола OCSP
- > Возможность организации масштабируемого кластера высокой производительности с балансировкой нагрузки за счет внешнего балансировщика. Управление кластером осуществляется с любого элемента кластера
- > Импорт ключей и сертификатов в формате PFX
- > Поддержка TLS 1.3
- > Поддержка IPv6
- > Мониторинг состояния по протоколу SNMP
- > Удаленное администрирование через веб-интерфейс и по протоколу SSH
- > Лицензирование ViPNet PKI Client

ОБЛАСТЬ ПРИМЕНЕНИЯ

1

Удаленный доступ сотрудников к корпоративным ресурсам

2

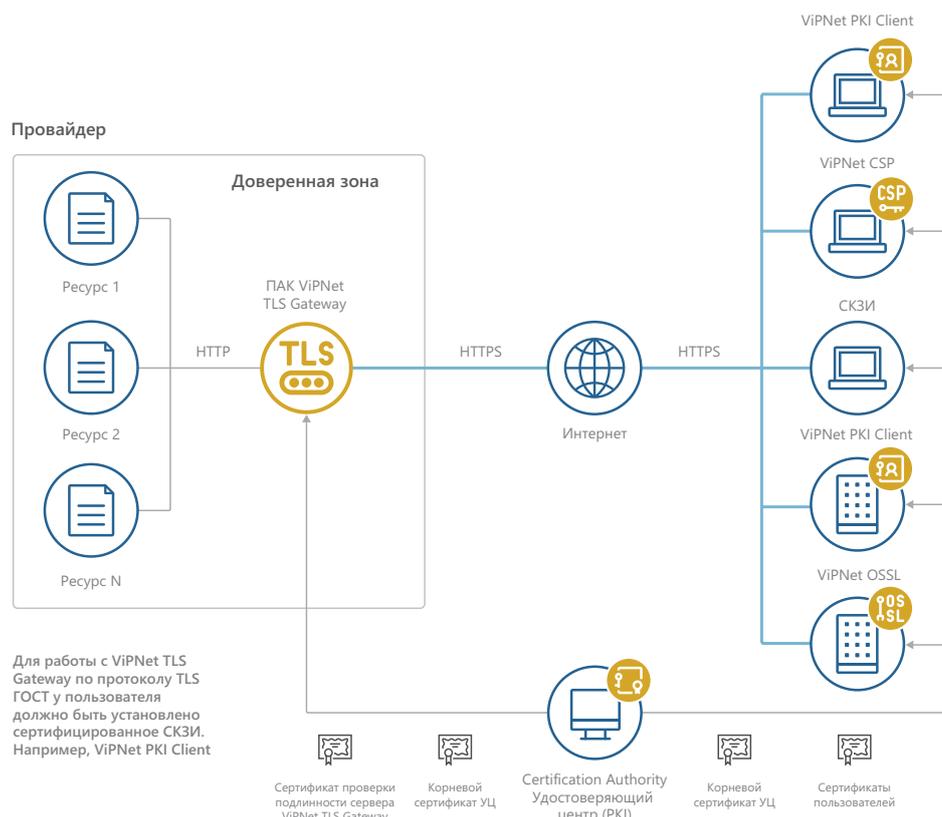
Предоставление электронных услуг по защищенному каналу

Поддерживаемые криптографические стандарты и рекомендации

- > ГОСТ Р 34.10-2012, RSA, ECDSA
- > ГОСТ Р 34.11-2012
- > ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018), AES
- > Рекомендации Технического комитета 026

Поддерживаемые виртуальные среды (для TLS VA)

- > VMware Workstation
- > VMware vSphere ESXi
- > Oracle VM VirtualBox
- > Microsoft Hyper-V
- > Платформы виртуализации, основанные на Kernel Virtual Machine (KVM), в том числе отечественные гипервизоры



**Использование
VIPNet TLS Gateway
для предоставления
пользователям доступа
к веб-сервисам**

Для работы с VIPNet TLS Gateway по протоколу TLS ГОСТ у пользователя должно быть установлено сертифицированное СКЗИ. Например, VIPNet PKI Client

МОДЕЛЬНЫЙ РЯД

Исполнения TLS	TLS VA	TLS 550	TLS 1100	TLS 5500
Аппаратная платформа	виртуальная машина	TLS 500 Q2	TLS 1000 Q3	TLS 5000 Q2
Предельная пропускная способность в режиме обратного HTTPS-прокси, Мбит/с	зависит от характеристик аппаратного обеспечения	до 600	до 1800	до 7600
Максимальное число одновременных соединений в режиме обратного HTTPS-прокси и TCP-туннеля	зависит от характеристик аппаратного обеспечения	до 7000	до 14000	до 65000
Интерфейсы	зависят от характеристик аппаратного обеспечения	6x Ethernet 10/100/1000	8x Ethernet 10/100/1000 4x 1G Ethernet Fiber SFP	4x Ethernet 10/100/1000 8x 10G Ethernet Fiber SFP+

СЕРТИФИКАЦИЯ

ФСБ России

- > СКЗИ класса КС3 для исполнений TLS 500, TLS 1000, TLS 5000, TLS 550, TLS 1100, TLS 5500
- > СКЗИ класса КС1 для исполнения TLS VA

Свидетельства

- > В реестре российского ПО
- > В реестре Минпромторга





VIPNet Administrator

Программный комплекс, предназначенный
для настройки и управления защищенной сетью

ВОЗМОЖНОСТИ

- > Создание и изменение логической структуры защищенной сети, узлов и пользователей, связей между ними
- > Управление лицензиями
- > Конфигурирование параметров узлов и полномочий пользователей
- > Генерация и управление жизненным циклом ключевой информации
- > Централизованное (групповое или точечное) обновление ПО на узлах защищенной сети ViPNet
- > Управление журналами событий и журналами аудита

ПРЕИМУЩЕСТВА

01. Клиент-серверная архитектура, позволяющая нескольким администраторам удаленно управлять защищенной сетью через удобный графический интерфейс
02. Поддержка распределенной установки компонентов программного комплекса позволяет гибко масштабировать систему и обеспечивать требуемую производительность
03. Надежный аудит событий системы и действий администраторов
04. Эффективное управление защищенной сетью с использованием групп узлов и шаблонов политик
05. Настраиваемый автоматический режим работы ключевого центра позволяет автоматизировать работу с приложением

СОСТАВ

- > ViPNet NCC (Network Control Center – Центр управления сетью) – приложение для конфигурирования и управления виртуальной защищенной сетью ViPNet
- > ViPNet KCA (Key and Certification Authority – Удостоверяющий и ключевой центр) – приложение, которое выполняет функции центра формирования ключей шифрования, персональных ключей пользователей и функции удостоверяющего центра

СЕРТИФИКАЦИЯ

ФСБ России
СКЗИ и ЭП класса КС1, КС2, КС3

Свидетельства
В реестре российского ПО



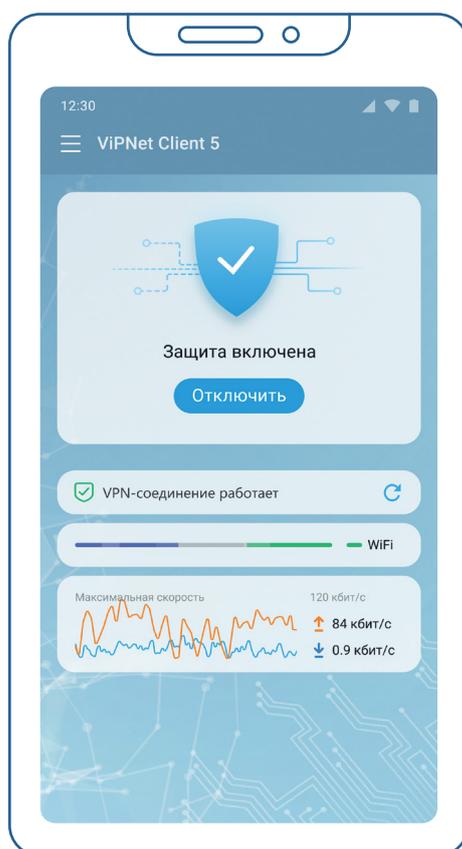
VipNet Client

Программный комплекс для защиты информации при ее передаче по открытым каналам связи с мобильных и стационарных рабочих мест.

Программный комплекс (ПК) VipNet Client защищает устройство от внешних и внутренних сетевых атак и обеспечивает защищенную работу пользователей с корпоративными данными при подключении через интернет

ВОЗМОЖНОСТИ

01. Продукт позволяет обеспечить унифицированный доступ к ресурсам корпоративных информационных систем из любой точки мира с использованием произвольных TCP/IP-сетей.
02. Технология ViPNet, лежащая в основе продукта, позволяет эксплуатировать территориально распределенные ИС из единого центра управления и отправлять ключи шифрования и обновления программного обеспечения по защищенному каналу.
03. Архитектура продукта позволяет обеспечить одновременную работу с ресурсами различных сегментов корпоративной сети.
04. Возможности продукта по шифрованию и фильтрации трафика позволяют в реальном времени осуществлять защиту голосового трафика, видеосвязи, IP-телефонии, почтового обмена и других служб в сетях TCP/IP.

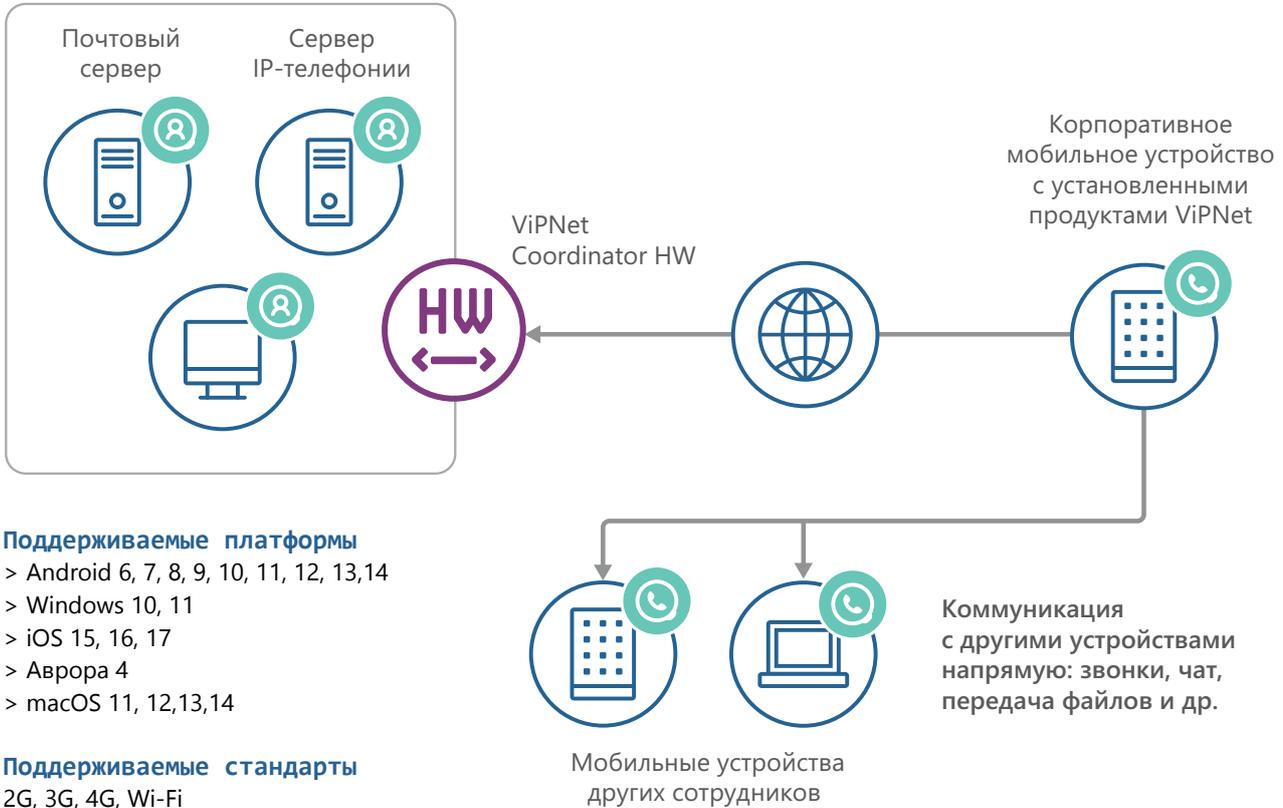


Специальные функции

VPN-клиент – шифрование «точка-точка» и имитозащита IP-пакетов с использованием алгоритмов ГОСТ 28147-89, ГОСТ 34.12-2018 и ГОСТ 34.13-2018 на симметричных ключах 256 бит

Сценарии использования и защиты мобильных и стационарных рабочих мест

Корпоративная сеть

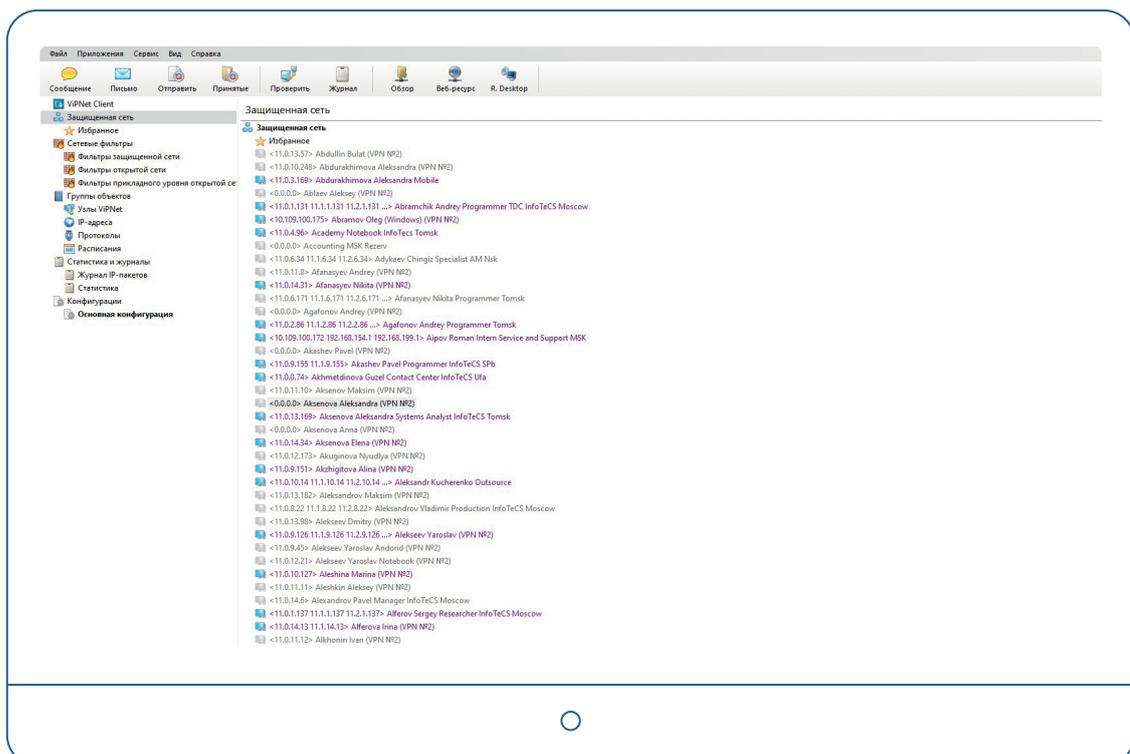


Поддерживаемые платформы

- > Android 6, 7, 8, 9, 10, 11, 12, 13,14
- > Windows 10, 11
- > iOS 15, 16, 17
- > Аврора 4
- > macOS 11, 12,13,14

Поддерживаемые стандарты

2G, 3G, 4G, Wi-Fi



СЦЕНАРИИ

01. Безопасная работа удаленного пользователя с корпоративными ресурсами и сервисами через защищенные каналы как в парадигме Client-to-Site, так и в парадигме Client-to-Client. Работа в парадигме Client-to-Client («точка-точка») позволяет защитить информацию не только при использовании публичных каналов связи, но и при использовании ViPNet Client внутри корпоративной сети, обеспечивая защиту конфиденциальной информации от внутреннего нарушителя.
02. Дополнительно к сценариям защиты есть возможность на базе существующей защищенной сети ViPNet использовать опциональные средства защищенных коммуникаций, таких как защищенная корпоративная почта (продукт «ViPNet Деловая почта») и защищенный корпоративный мессенджер (продукт «ViPNet CSS Connect»).
03. ViPNet Client поддерживает работу на виртуальных машинах, что позволяет использовать средства защиты ViPNet в VDI-средах.
04. ViPNet Client может быть использован и как наложенное средство информационной безопасности для защиты существующих систем почтового обмена, документооборота, IP-телефонии и видеоконференцсвязи. Использование ViPNet Client в таком сценарии не требует изменения и доработок прикладного программного обеспечения.
05. В ViPNet Client можно включить конфигурацию, в которой прямой доступ устройства в интернет блокируется. В этой конфигурации устройство может обращаться в интернет только через корпоративную «зону очистки трафика» (набор средств информационной безопасности, таких как прокси-серверы, DLP-системы, средства контентной фильтрации и т.п.). Такой подход обеспечивает многоуровневую защиту устройства и позволяет применить корпоративные механизмы информационной безопасности к любым устройствам, физически покидающим защищенный периметр.

СЕРТИФИКАЦИЯ

Соответствует требованиям ФСБ России

ViPNet Client для ОС Windows:

- > СКЗИ класса КС1, КС2 и КС3
- МЭ 4 класса

ViPNet Client для ОС Linux:

- > СКЗИ класса КС1, КС2 и КС3

ViPNet Client для ОС Android:

- > СКЗИ класса КС1

ViPNet Client для ОС Аврора:

- > СКЗИ класса КС1 и КС2

Соответствует требованиям ФСТЭК России

ViPNet Client для ОС Windows:

- > МЭ типа В 4 класса



VIPNet Policy Manager

Система централизованного группового
управления политиками безопасности
защищенной сети VIPNet

ПРЕИМУЩЕСТВА

01. Централизованное управление политиками безопасности и возможность объединять узлы защищенной сети по группам
02. Возможность отправки, применения и действия политик безопасности по расписанию
03. Контроль отправки и применения политик безопасности на узлах сети ViPNet
04. Гибкое управление доступом разграничения полномочий по ролям: администраторов безопасности, сетевых администраторов, аудиторов и пр.
05. Регистрация и аудит действий пользователей программы ViPNet Policy Manager
06. Совместная работа с программным комплексом ViPNet Client для управления политиками безопасности через защищенный канал

ВОЗМОЖНОСТИ

- > Возможность назначения политик безопасности как на отдельные узлы, так и на группы устройств
- > Управление политиками безопасности на основе шаблонов
- > Контроль отправки и применения политик безопасности на сетевых узлах ViPNet
- > Разграничение полномочий администраторов системы на основе ролей
- > Аудит действий администраторов



+7 495 737-61-92
8 800 250-0-260 (бесплатный звонок по России)

soft@infotecs.ru
hotline@infotecs.ru

www.infotecs.ru



Содержимое документа носит исключительно информационный характер и не является публичной офертой. Для получения подробной информации об указанных в документе продуктах и услугах вы можете обратиться в АО «ИнфоТекС». Все изображения являются лишь иллюстрациями. Все технические характеристики, внешний вид и комплектность описываемой продукции могут меняться без предварительного уведомления. Символы [™] или [®] в документе не используются, однако, если не указано иного, все товарные знаки в данном документе защищены соответствующим правом, которое принадлежит их владельцам.

CH24_00RU