

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 выполнения функций криптоимитозащиты при передаче информации между клиентами OTN-сетей по магистральным волоконно-оптическим линиям связи
- 2 обеспечения прозрачной криптографической защиты данных, передаваемых по каналам Ethernet («темная оптика», MAN, WAN, выделенный канал)
- 3 организации виртуальной частной сети (VPN) с централизованным управлением, а также создания централизованных комплексов управления, аудита и мониторинга средств защиты информации в распределенных сетях
- 4 построением защищенных TLS и ГОСТ-каналов

[СОСТАВ РЕШЕНИЯ]

ШЛЮЗЫ БЕЗОПАСНОСТИ



ПАК ViPNet Coordinator HW
Шлюз безопасности, МЭ, VPN-сервер



ViPNet Coordinator VA
Шлюз безопасности в виртуальном исполнении



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



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



ViPNet xFirewall
Шлюз безопасности – межсетевой экран нового поколения



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

КЛИЕНТСКИЕ КОМПОНЕНТЫ



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

ViPNet Coordinator HW 4

Шлюз безопасности для защиты
каналов связи



Программно-аппаратные комплексы (ПАК)
ViPNet Coordinator HW 4 – модельный ряд шлюзов
безопасности, предназначенных для построения
виртуальной сети ViPNet и обеспечения безопасной
передачи данных между ее защищенными сегментами,
а также фильтрации IP-трафика

Благодаря функциям криптографической защиты, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК ViPNet Coordinator HW 4 является оптимальным средством защиты компьютерных сетей организаций 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]

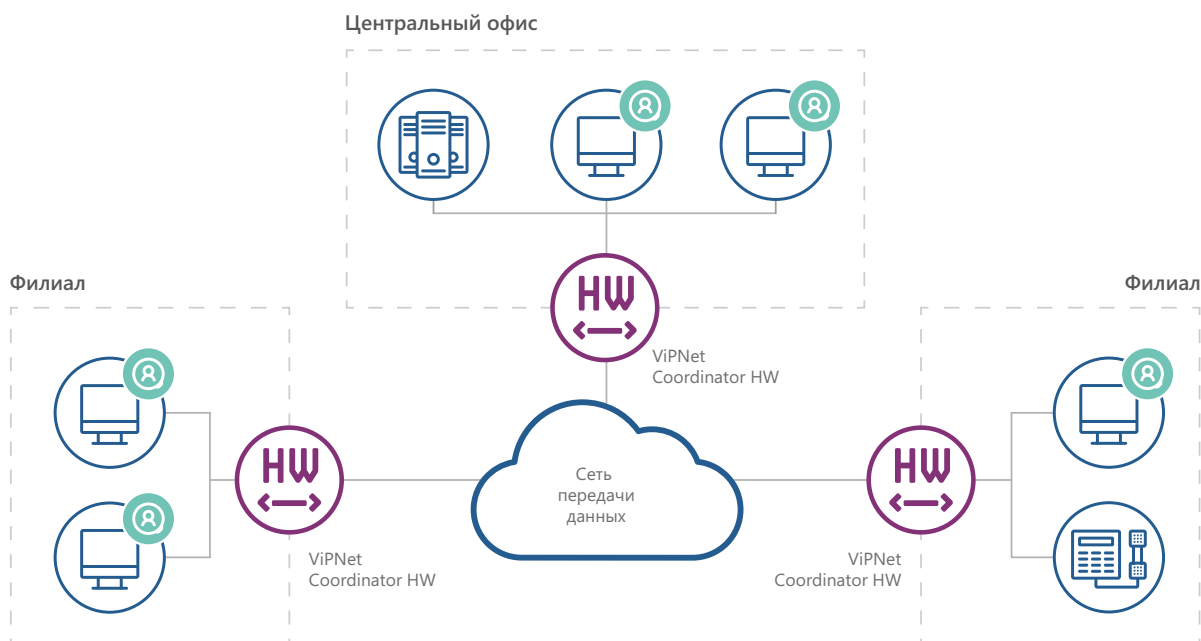
- | | | | |
|---|--|---|--|
| 1 | Поддержка новых аппаратных платформ (HW1000 Q7/Q8/Q9, HW2000 Q5 и HW5000 Q2) | 5 | Расширенная функциональность DHCP-сервера и службы DHCP-Relay |
| 2 | Поддержка режима Multi-WAN | 6 | Усовершенствованный механизм работы кластера горячего резервирования |
| 3 | Поддержка Jumbo-кадров | 7 | Повышение производительности и стабильности работы |
| 4 | Проверка трафика сторонним антивирусом по протоколу ICAP | | |



[ПРЕИМУЩЕСТВА]

- Организация VPN на сетевом (L3) и канальном уровне (L2)* в одном устройстве
- Кластер горячего резервирования
- Работа в необслуживаемом режиме
- Централизованное и удаленное управление (SSH, WebUI)
- 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)

* Кроме исполнения HW50



[СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ]

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

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

СКЗИ класса КСЗ

МЭ 4 класса защищенности

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

РЕЕСТРЫ И СЕРТИФИКАТЫ

Включен в Единый реестр российского ПО

Включен в Единый реестр российской радиоэлектронной продукции (ТОРП)

Сертификат соответствия требованиям «Правил применения оборудования коммутации и маршрутизации пакетов информации» Минкомсвязи

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]



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

Фильтрация содержимого трафика

Проверка трафика сторонним антивирусом по протоколу ICAP



СЕРВИСНЫЕ ФУНКЦИИ

DHCP-сервер

DHCP-relay

DNS-сервер

NTP-сервер



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 Jumbo-кадров

Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

Реализация функций клиента и точки доступа Wi-Fi (для платформ HW50 N2 и HW100 N2)



ОТКАЗОУСТОЙЧИВОСТЬ И РЕЗЕРВИРОВАНИЕ

Отказоустойчивый кластер горячего резервирования

Резервирование каналов связи

Резервирование сетевых интерфейсов

Поддержка ИБП (UPS)



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

Экспорт системного журнала по протоколу Syslog

* Кроме исполнения HW50

[МОДЕЛЬНЫЙ РЯД]



Исполнение	HW50 A	HW100 C
Область применения	Рабочие места и сетевые устройства	Малые офисы и филиалы

Производительность¹

Пропускная способность L3 VPN, Мбит/с	до 75	до 175
Пропускная способность L2 VPN, Мбит/с	Недоступно	до 175
Пропускная способность МЭ, Мбит/с	до 170	до 360
Максимальное количество сессий МЭ	150 000	150 000
Рекомендуемое число VPN-клиентов ²	Недоступно	до 10

Аппаратная платформа	HW50 N1	HW50 N2	HW50 N3	HW100 N1	HW100 N2	HW100 N3
Форм-фактор	Десктоп					
Размеры (Ш x В x Г), мм	124,3 x 19,4 x 120			170 x 41 x 138		
Масса, кг	0,5 (без БП)					
Источник питания	Внешний БП, 12 В, 3 А			Внешний БП, 24 В, 2,5 А		

Сетевые возможности

Интерфейсы RJ-45	3x 1 Гбит/с			4x 1 Гбит/с		
Интерфейсы SFP/SFP+	нет			1x SFP 1 Гбит/с		
Беспроводные интерфейсы	нет	Wi-Fi	3G	нет	Wi-Fi	3G

Доступность и надежность

Кластер горячего резервирования	есть (с доп. лицензией)					
Работа в необслуживаемом режиме 24 x 7	есть					
Управление электропитанием с помощью ИБП	есть					
Среднее время наработки на отказ (MTBF)	30 000 часов					

¹Приведены максимальные достигнутые результаты производительности, полученные на оптимальном профиле трафика. Реальные показатели на различных типах трафика, могут отличаться от приведенных в меньшую сторону.

²Клиенты сети ViPNet, для которых координатор выполняет роль транспортного сервера (передает служебную информацию о работе в защищенной сети). Если на координаторе зарегистрировано число клиентов выше оптимального, показатели производительности могут снизиться.



HW1000	HW1000 C	HW1000 D	HW2000	HW5000
Предприятия малого и среднего бизнеса			Крупные предприятия и корпорации	ЦОД
до 915	до 2 300³		до 5 800	10 000³
до 890	до 2 300³		до 5 800	10 000³
до 930	до 2 700³		до 9 200	13 000³
1 000 000			3 000 000	6 500 000
до 500	до 1000		до 5000	до 6000
HW1000 Q7	HW1000 Q8	HW1000 Q9	HW2000 Q5	HW5000 Q2
1U				
430 x 44 x 435			430 x 44 x 435	
7			8	
1x 250 Вт		2x 300 Вт с «горячей» заменой	2x 300 Вт с «горячей» заменой	2x 300 Вт с «горячей» заменой
6x 1 Гбит/с	8x 1 Гбит/с		4x 1 Гбит/с	
нет		4x SFP 1 Гбит/с	4x SFP 1 Гбит/с 4x SFP+ 10 Гбит/с	8x SFP+ 10 Гбит/с
нет				
есть				
есть				
есть				
50 000 часов				

³Приведена производительность при объединении двух и более физических сетевых интерфейсов.

ViPNet Coordinator HW 5

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

ViPNet COORDINATOR HW 5 – РЕАЛИЗУЕТ В ОДНОМ УСТРОЙСТВЕ СЛЕДУЮЩИЕ ФУНКЦИИ БЕЗОПАСНОСТИ, ФУНКЦИОНИРУЮЩИЕ 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)

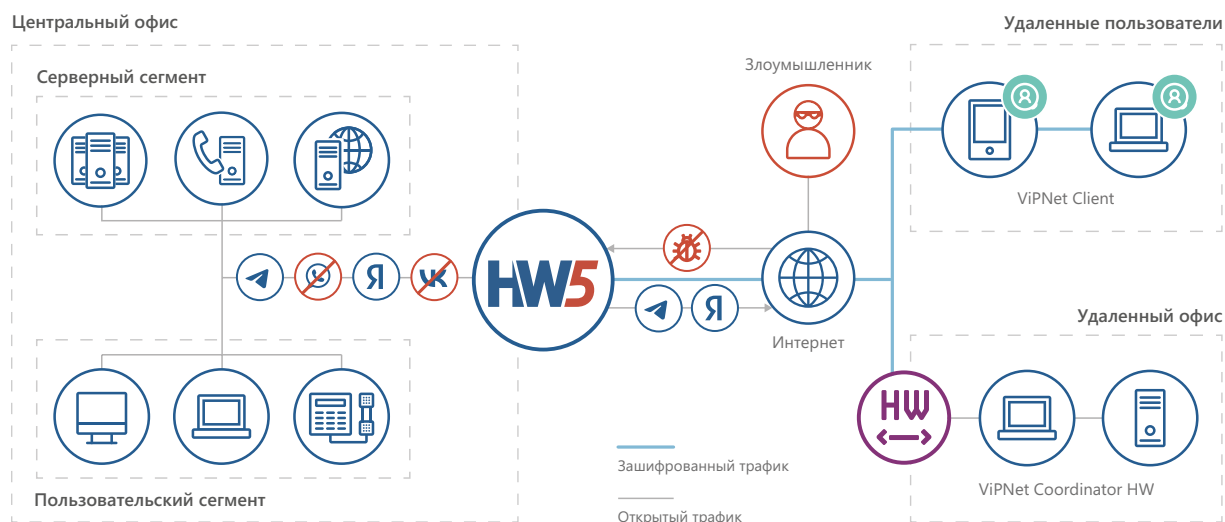
ViPNet Coordinator HW 5 реализуется в исполнении программно-аппаратного комплекса на доверенной аппаратной платформе, а также в виде виртуального устройства, которое может функционировать в виртуальной среде (KVM, VMware ESXi, Microsoft Hyper-V, Oracle XenServer).

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

[ЧТО НОВОГО]

- 1 Поддержка алгоритмов «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- 2 Межсетевой экран уровня приложений (DPI)
- 3 Обнаружение и предотвращение вторжений (IDS/IPS)
- 4 Многопользовательский ролевой доступ
- 5 Подсистема идентификации пользователей (LDAP, Active Directory, Captive Portal)
- 6 Кластер высокой доступности (HA-cluster) с синхронизацией таблицы открытых соединений
- 7 Централизованное и удаленное резервное копирование конфигурации

[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

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]



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 вторжений (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)



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)



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



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



СЕРВИСНЫЕ ФУНКЦИИ

DHCP-Relay

DHCP-сервер

DNS-сервер

NTP-сервер



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)

* Кроме исполнения HW50

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

В процессе сертификации на соответствие требованиям:

СКЗИ класса КСЗ

Межсетевой экран 4 класса

Средство обнаружения компьютерных атак класса ВП

СВИДЕТЕЛЬСТВА

Роспатент

Интеграл

ФСТЭК РОССИИ

В процессе сертификации на соответствие требованиям:

МЭ типа А четвертого класса (ИТ.МЭ.А4.ПЗ)

МЭ типа Б четвертого класса (ИТ.МЭ.А4.ПЗ)

СОВ уровня сети четвертого класса защиты (ИТ.СОВ.С4.ПЗ)

4 уровень доверия средств защиты информации

[МОДЕЛЬНЫЙ РЯД]



Исполнение	HW50 A	HW100 C
Область применения	Рабочие места и сетевые устройства	Малые офисы и филиалы

Производительность¹

МЭ UDP 1518 Б, Мбит/с	450	950
МЭ UDP 64 Б (пакетов/с)	40 000	85 000
МЭ TCP, Мбит/с	320	930
Application Control (МЭ+DPI) ³ (Мбит/с)	25	85
NGFW Throughput ⁴ (МЭ + DPI + IPS) (Мбит/с)	-	15
Соединений в секунду TCP	8 600	18 400
Количество обслуживаемых соединений	150 000	150 000
L3 VPN, Мбит/с	70	160
L2 VPN, Мбит/с	Недоступно	160
Рекомендуемое число связей с ViPNet-узлами	500	1 000
Рекомендуемое число зарегистрированных ViPNet-клиентов	-	10

Аппаратная платформа	HW50 N1	HW50 N2	HW50 N3	HW100 N1	HW100 N2	HW100 N3
Форм-фактор	Мини-компьютер					
Сетевые интерфейсы	3 x 1G RJ-45			4 x 1G RJ-45 1 x 1G SFP		
Беспроводные интерфейсы	-	Wi-Fi	3G	-	Wi-Fi	3G
Интерфейсы ввода/вывода	2 x USB Console (RJ-45) HDMI			2 x USB Console (RJ-45) VGA		
Внутреннее хранилище	2 Gb SSD -			2 Gb SSD 500 Gb HDD		
Размеры (ШxВxГ), мм	125 x 20 x 120			174 x 44 x 138		
Масса, кг	0,5 (без БП)					
Источник питания	Внешний БП, 12 В, 3 А			Внешний БП, 24 В, 2,5 А		
Потребляемая мощность (макс.), Вт	9			11		
Условия эксплуатации	0° - 40° C			0° - 50° C		
Средняя наработка на отказ (MTBF)	30 000 часов					

¹Производительность исполнения зависит от активированных функций, характеристик обрабатываемого сетевого трафика: протоколов, размера пакетов, количества сессий. Производительность может меняться вследствие изменений, вносимых в новые версии программного обеспечения.

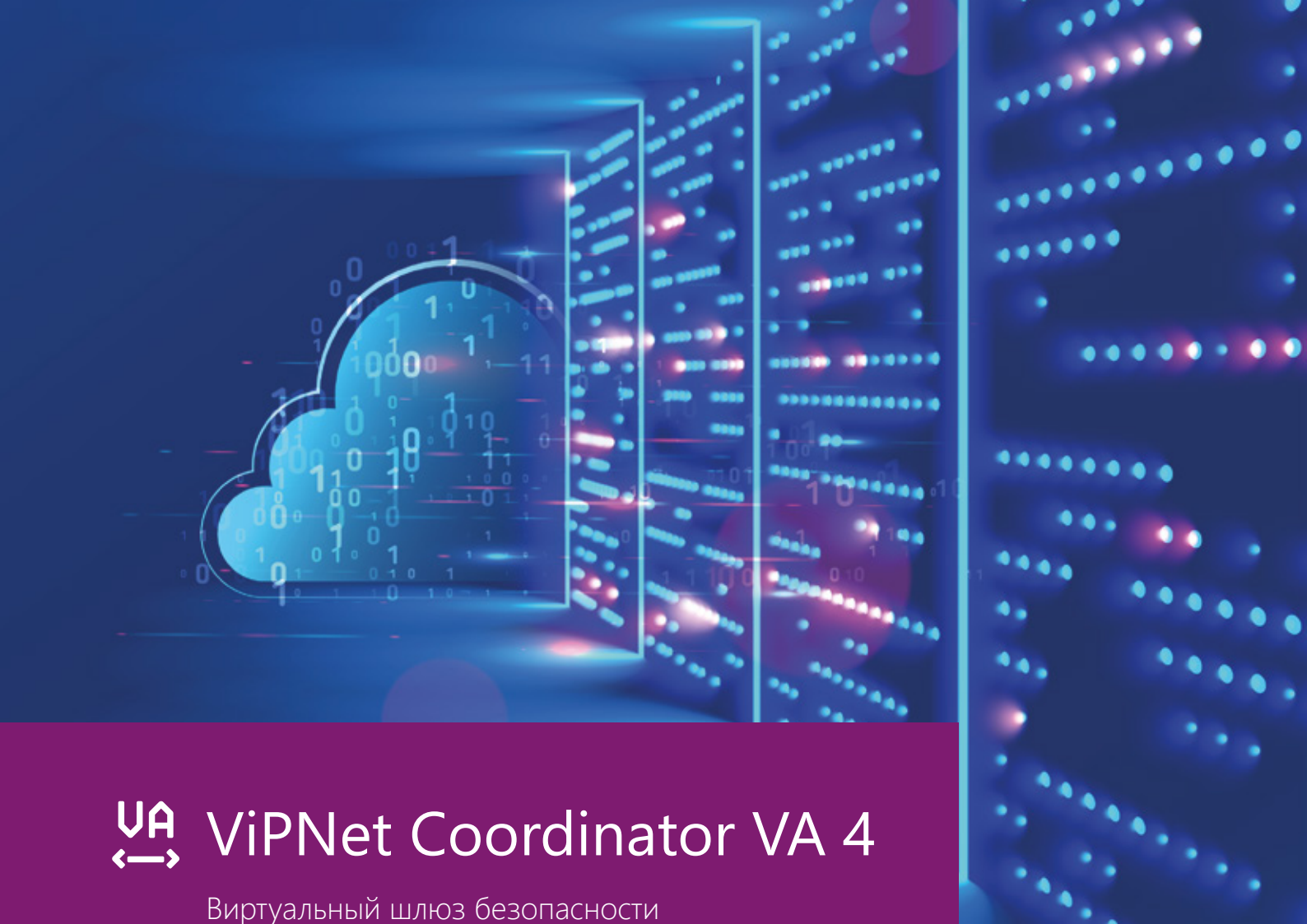
²Приведена производительность при объединении двух и более физических сетевых интерфейсов.



HW1000	HW1000 C	HW1000 D	HW2000	HW5000
Предприятия малого и среднего бизнеса			Крупные предприятия и корпорации	ЦОД
1 900 ²	2 800 ²		19 000 ²	24 000 ²
545 000	1 600 000		2 900 000	4 800 000
1 800 ²	2 800 ²		9 300	13 000 ²
350	1 000 ²		2 600	3 300
80	380		880	1 000
115 300	275 000		500 000	570 000
1 000 000	3 000 000		5 000 000	9 900 000
915	2 500		6 600	10 000 ²
915	2 500 ²		6 000	10 000 ²
5 000	10 000		15 000	15 000
500	1 000		5 000	6 000
HW1000 Q7	HW1000 Q8	HW1000 Q9	HW2000 Q5	HW5000 Q2
1U				
6 x 1G RJ-45	8 x 1G RJ-45	8 x 1G RJ-45 4 x 1G SFP	4 x 1G RJ-45 4 x 1G SFP 4 x 10G SFP+	4 x 1G RJ-45 8 x 10G SFP+
-	-	-	-	-
6 x USB Console (RS-232) VGA		6 x USB Console (RS-232) VGA		
4 Gb SSD 1 Tb HDD		4 Gb SSD 1 Tb HDD		4 Gb SSD 2 Tb HDD
430 x 44 x 453		430 x 44 x 476		
7		8		
1x 250 Вт		2x 300 Вт с «горячей» заменой		
215	230	230	274	283
5° - 35° C				
50 000 часов				

³Результаты получены для трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

⁴Результаты 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.



ViPNet Coordinator VA 4

Виртуальный шлюз безопасности
для защиты каналов связи

Программный комплекс ViPNet Coordinator VA 4 – шлюз безопасности в виртуальном исполнении, предназначенный для обеспечения безопасной передачи данных между защищенными сегментами виртуальной сети ViPNet, а также фильтрации IP-трафика

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

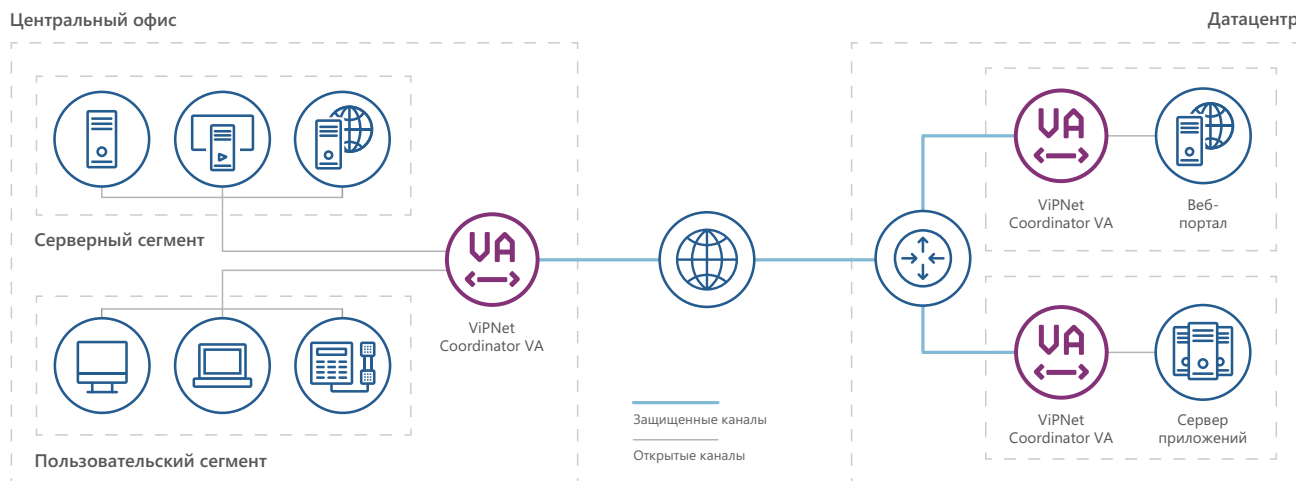
ViPNet Coordinator VA 4 обеспечивает безопасность передаваемых данных и многоуровневую защиту виртуальной и облачной инфраструктуры

как для частных, так и для публичных облаков, не меняя привычного способа доступа пользователей к бизнес-данным.

ViPNet Coordinator VA 4 представляет собой виртуализированное программное обеспечение, предназначенное для развертывания на популярных платформах виртуализации (KVM, VMware ESXi, Microsoft Hyper-V, Oracle VM).

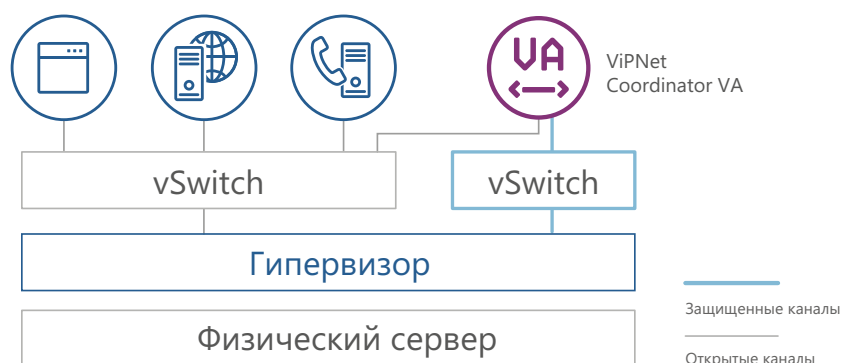
[ПРЕИМУЩЕСТВА]

- Удобство управления и скорость развертывания
- Гибкое лицензирование и быстрое масштабирование
- Поддержка распространенных систем виртуализации
- Отсутствие дополнительных затрат на размещение и обслуживание оборудования
- Функциональность, соответствующая аппаратным шлюзам ViPNet Coordinator HW
- Единая система управления для виртуальных и аппаратных шлюзов безопасности
- Организация VPN на сетевом (L3) и канальном уровне (L2) в одном виртуальном устройстве



[СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ]

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



[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]



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



ПРОКСИ-СЕРВЕР

Поддержка протокола HTTP

Работа в «прозрачном» режиме

Кэширование данных

Фильтрация содержимого трафика

Проверка трафика сторонним антивирусом по протоколу ICAP



СЕРВИСНЫЕ ФУНКЦИИ

DHCP-сервер

DHCP-relay

DNS-сервер

NTP-сервер



ОТКАЗОУСТОЙЧИВОСТЬ И РЕЗЕРВИРОВАНИЕ

Отказоустойчивый кластер горячего резервирования из двух виртуальных машин

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)



МЕЖСЕТЕВОЙ ЭКРАН

Межсетевой экран с контролем состояния сессий

Раздельная настройка фильтрации для открытого и шифруемого IP-трафика

NAT/PAT

Антиспуфинг



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 Jumbo-кадров

Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)



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

Экспорт системного журнала по протоколу Syslog

Экспорт журнала IP-пакетов в формате CEF

Тип лицензии	VA100	VA500	VA1000	VA2000
Производительность¹				
Пропускная способность L3 VPN, Мбит/с	180	580	1 400	4 000
Пропускная способность МЭ, Мбит/с	330	940	3 500	5 500
Максимальное количество сессий МЭ	150 000	500 000	1 000 000	3 000 000
Рекомендуемое число VPN-клиентов ²	100	500	1 000	2 000
Кластер горячего резервирования	да (с доп. лицензией)			

Минимальные системные требования

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

Поддерживаемые среды виртуализации³

VMware ESXi 6.5, 6.7 VMware Workstation 12.x, 14.x, 15.x	да
Microsoft Hyper-V Server 2019	да
KVM, QEMU-KVM и Libvirt	да
Oracle VM VirtualBox 6.x Oracle VM Server 3.4	да

¹Условия измерений: VMware ESX 6.7, CPU Xeon E-2278GE

²Клиенты сети ViPNet, для которых координатор выполняет роль транспортного сервера (передает служебную информацию о работе в защищенной сети). Если на координаторе зарегистрировано число клиентов выше оптимального, показатели производительности могут снизиться

³Работа на других платформах виртуализации возможна, но не гарантирована

[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

Включен в Единый реестр
российского ПО

Свидетельство
о государственной регистрации
ViPNet Coordinator HW 4



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 реализует в одном устройстве следующие функции безопасности, функционирующие совместно:

- | | | | |
|---|---|---|---|
| 1 | криптографический шлюз, обеспечивающий построение VPN на сетевом (L3) и канальном (L2) уровнях модели OSI | 4 | межсетевой экран уровня приложений DPI (Deep Packet Inspection) |
| 2 | межсетевой экран SPI (Stateful Packet Inspection) | 5 | средство обнаружения и предотвращения вторжений (IDS/IPS) |
| 3 | прокси-сервер | 6 | 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]

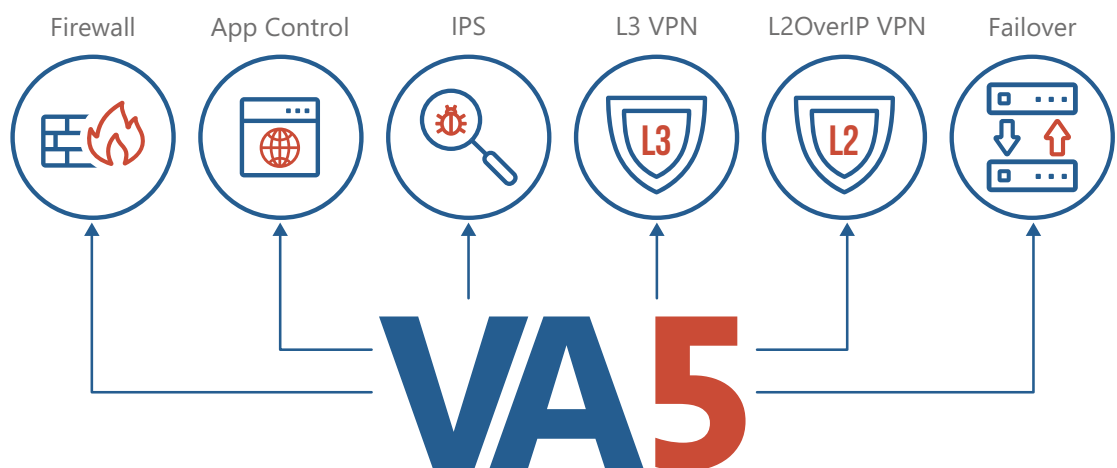
- Поддержка алгоритмов «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Межсетевой экран уровня приложений (DPI)
- Многопользовательский ролевой доступ
- Обнаружение и предотвращение вторжений (IDS/IPS)
- Подсистема идентификации пользователей (LDAP, Active Directory, Captive Portal)
- Кластер высокой доступности (HA-cluster) с синхронизацией таблицы открытых соединений
- 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

Роспатент

Интеграл

ФСТЭК РОССИИ

В процессе сертификации
на соответствие требованиям:

МЭ типа Б четвертого класса (ИТ.МЭ.А4.ПЗ)

СОВ уровня сети четвертого класса защиты
(ИТ.СОВ.С4.ПЗ)

4 уровень доверия средств защиты
информации

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]



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)



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



СЕРВИСНЫЕ ФУНКЦИИ

DHCP-Relay

DHCP-сервер

DNS-сервер

NTP-сервер



ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Интеграция с Microsoft Active Directory

Captive Portal и интеграция с LDAP каталогом



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



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



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



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



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)

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	1 Гбит/с	1 Гбит/с	1/10 Гбит/с	1/10 Гбит/с	1/10 Гбит/с
Поддерживаемые среды виртуализации ⁴	• KVM, QEMU-KVM и Libvirt • VMware ESXi 6.7/7.0 • VMware Workstation Pro 15.x / 16.x • 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.

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
- Защищенный доступ удаленных и мобильных пользователей
- Защита мультисервисных сетей (включая IP-телефонию и видеоконференцсвязь)

[ПРЕИМУЩЕСТВА]

- 1 Высокая скорость шифрования (до 5,8 Гбит/с)
- 2 Шифрование трафика на сетевом (L3) и канальном уровне (L2) модели OSI
- 3 Построение защищенных каналов связи как Site-to-Site VPN, так и Multi Site-to-Site VPN
- 4 Возможность создания кластера горячего резервирования
- 5 Экстренное удаление ключевой информации по нажатию специальной кнопки
- 6 Встроенный датчик несанкционированного доступа
- 7 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]

Аппаратные характеристики



Модификация	KB100	KB1000	KB2000	KB5000
Область применения	Удаленные офисы и филиалы	Предприятия	Корпоративные сети	ЦОД

Производительность

Пропускная способность VPN, Мбит/с	до 140	до 910	до 2 700	до 5 800
Пропускная способность L2 VPN, Мбит/с	до 140	до 890	до 2 700	до 5 300
Пропускная способность МЭ, Мбит/с	до 360	до 930	до 4 400	до 6 100
Максимальное количество узлов, туннелируемых координатором	Не ограничено			

Аппаратная платформа

платформа	KB100 N1	KB1000 Q8	KB2000 Q4	KB5000 Q1
Форм-фактор	Декстоп	1U	1U	1U
Размеры (Ш x В x Г), мм	170 x 43,7 x 138,5	430 x 44 x 477,2	444 x 44 x 381	
Масса, кг	0,5 (без БП)	8	8	
Источник питания	Внешний БП, 24 В, 2,5 А	2 x 300 Вт с «горячей» заменой	Встроенный БП, 500 Вт	
Датчик вскрытия корпуса	есть			
Кнопка экстренного стирания ключевой информации	есть			

Сетевые возможности

Сетевые интерфейсы (медные)	4x RJ45 1 Гбит/с			
Сетевые интерфейсы (оптические)	1x SFP 1 Гбит/с	2x SFP 1 Гбит/с	4x SFP+ 10 Гбит/с	
Трансивер в комплекте	1 x Avago AFBR-5710PZ		2 x Avago AFBR-709SMZ	

Доступность и надежность

Кластер горячего резервирования	есть (с доп. лицензией)	есть	есть	есть
Работа в необслуживаемом режиме 24 x 7	есть			
Управление электропитанием с помощью ИБП	есть			
Среднее время наработки на отказ (MTBF)	30 000 часов	50 000 часов	50 000 часов	50 000 часов

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]



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



СЕРВИСНЫЕ ФУНКЦИИ

DNS-сервер

NTP-сервер

DHCP-сервер

DHCP-Relay

Поддержка ИБП (UPS)

Отказоустойчивый кластер горячего резервирования



МЕЖСЕТЕВОЙ ЭКРАН

Межсетевой экран с контролем состояния сессий

Раздельная настройка фильтрации для открытого и шифруемого IP-трафика

NAT/PAT

Антиспуфинг



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)



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)



ОТКАЗОУСТОЙЧИВОСТЬ И РЕЗЕРВИРОВАНИЕ

Отказоустойчивый кластер горячего резервирования

Резервирование каналов связи

Резервирование сетевых интерфейсов

Поддержка ИБП (UPS)

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

СКЗИ класса KB

МЭ 4 класса защищенности



ViPNet Coordinator IG

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

ПАК ViPNet
COORDINATOR IG МОЖЕТ
БЫТЬ ИСПОЛЬЗОВАН:

- для защиты информации на всех уровнях значимых и незначимых объектов АСУ КИИ
- для защиты информации на всех уровнях АСУ ТП
- 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
- Работа в режиме горячего резервирования и возможность организации резервирования каналов связи
- Индустриальный дизайн и возможность использования в жестких условиях эксплуатации
- Дистанционное конфигурирование и управление политиками безопасности
- 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

[ФУНКЦИОНАЛЬНЫЕ ОСОБЕННОСТИ]



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

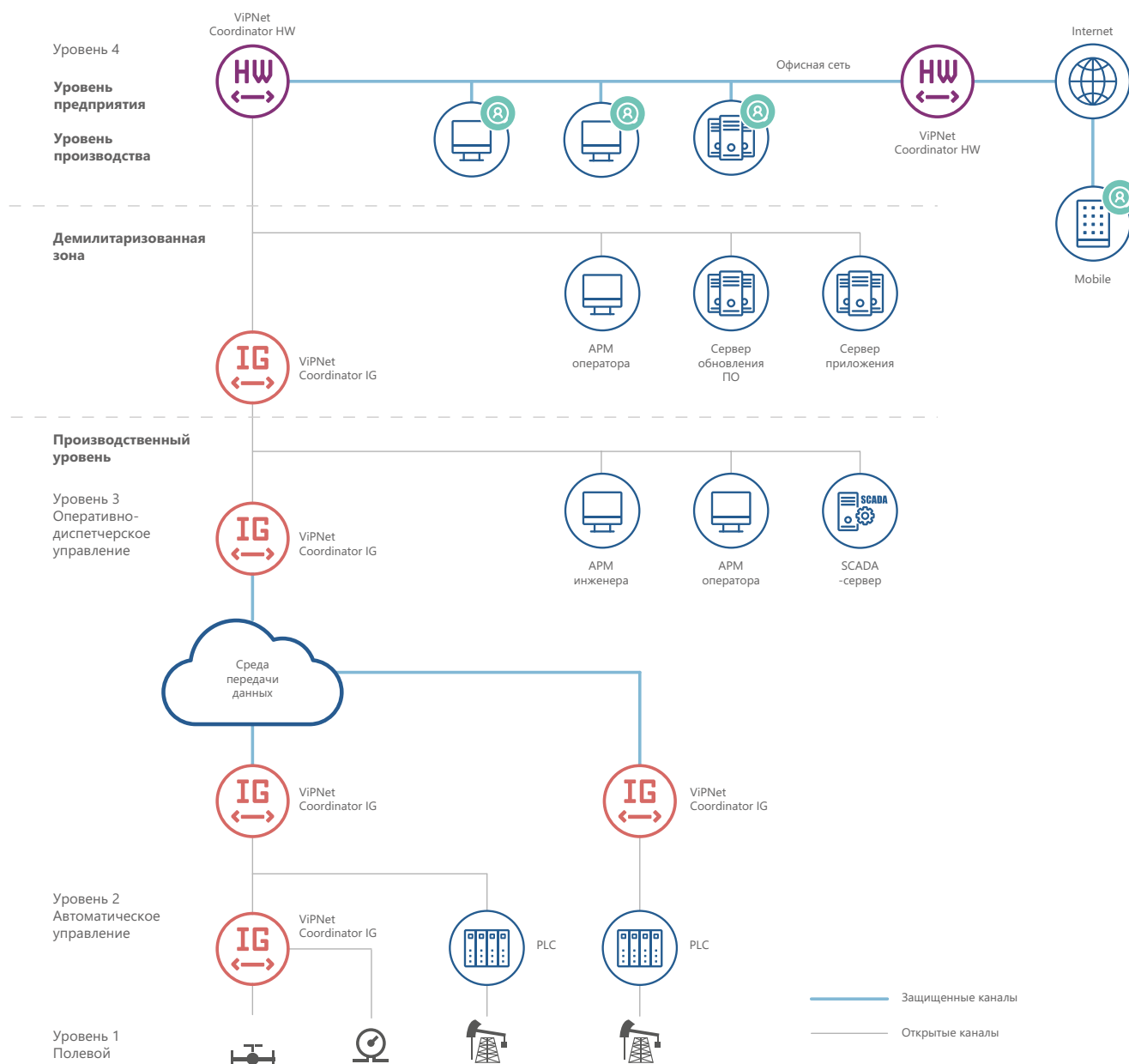
Динамическая маршрутизация

Поддержка VLAN (dot1q)

Поддержка классификации и приоритизации трафика (QoS, ToS, DiffServ)

Агрегирование сетевых интерфейсов (bonding, EtherChannel, LACP)

Преобразователь протоколов Modbus TCP/RTU



[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

СКЗИ класса КСЗ

МЭ 4 класса защищенности

ФСТЭК РОССИИ

МЭ 4 класса типа А (ИТ.МЭ.А4.ПЗ)

МЭ 4 класса типа Д (ИТ.МЭ.Д4.ПЗ)

4 уровень доверия средств
защиты информации

МИНЦИФРЫ

Оборудование коммутации и маршрутизации
и оборудование радиодоступа 802.11b/g

Абонентские терминалы стандарта
UMTS и LTE

Включен в реестр Российского ПО

МИНПРОМТОРГ РОССИИ

Включен в реестр ТОРП и единый реестр РЭП

РОСАККРЕДИТАЦИЯ

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

[МОДЕЛЬНЫЙ РЯД]



Аппаратные характеристики

ViPNet Coordinator IG10

ViPNet Coordinator IG100

Аппаратная платформа	IG10 I1	IG10 I2	IG100 I1	IG100 I4
Форм-фактор	Блок с крепление на DIN-рейку			
Размеры (Ш × В × Г), мм	52 x 132 x 120	69 x157x122	52 x 132 x 120	100 x 172 x 120
Вес, кг	Не более 0,65	Не более 1,5	Не более 0,65	Не более 1,8
Питание	12 - 24 В DC	12 - 24 В DC 2 порта	12 - 24 В DC	12 - 24 В DC 2 порта
Потребляемая мощность, Вт	Не более 10	Не более 15	Не более 10	Не более 30
Питание от PoE	-	-	-	-
Рабочая температура	-40° до +60° C ¹	-40° до +60° C ¹	-20° до +60° C ¹	-40° до +60° C ¹
Электромагнитная совместимость (EMI)	ГОСТ P51318-22 (СИСПР 22), ГОСТ CИСПР 24 2013 (СИСПР 24)	ГОСТ 30805.22-2013 (СИСПР.22:2006), ГОСТ 30804.6.2-2013 (IEC 61000-6-2:2005), ГОСТ CИСПР 24 2013 (СИСПР 24), ГОСТ P 51317.6.5-2006 (МЭК 61000-6-5:2001)	ГОСТ P51318-22 (СИСПР 22), ГОСТ CИСПР 24 2013 (СИСПР 24)	ГОСТ P51318-22 (СИСПР 22), ГОСТ CИСПР 24 2013 (СИСПР 24)
Класс защиты IP	IP30			

Межсетевой экран (МЭ)

Производительность МЭ, Мбит/с	10	10	60	До 100
Максимальное количество одновременных сессий	до 1000	до 1000	до 15000	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	До 10	60	До 100
Максимальное количество узлов, туннелируемое координатором	Не ограничено			
Рекомендуемое число зарегистрированных VPN-клиентов ³	Недоступно	Недоступно	до 10 ⁴	до 10 ⁴



Порты ввода-вывода

ViPNet Coordinator IG10

ViPNet Coordinator IG100

Аппаратная платформа	IG10 I1	IG10 I2	IG100 I1	IG100 I4
Порты Ethernet	WAN 1xRJ-45 100 Мбит/с LAN 1xRJ-45 100 Мбит/с	WAN 2xRJ-45 100 Мбит/с LAN 3xRJ-45 100 Мбит/с	WAN 1xRJ-45 100 Мбит/с LAN 2xRJ-45 100 Мбит/с	WAN 2xRJ-45 1 Гбит/с или 2xSFP 1 Гбит/с LAN 3xRJ-45 1 Гбит/с
Порты USB	2 x USB 2.0			
GSM интерфейсы	4G с выносной антенной (опционально)			
Разъем для Sim-карты	1	2	1	2
Wi-Fi в режиме клиента/ Wi-Fi в режиме точки доступа	Wi-Fi-модуль стандарта IEEE 802.11 b/g/n 2,4 ГГц с выносной антенной (опционально)			
RS-232/ RS-485	+ (совмещенный)	+	+ (совмещенный)	+
GPIO	1 x In, 1 x Out			

Интегрированные сервисы

DNS, NTP, DHCP-сервер	+
DHCP-relay	+
MiltiWan	+
Прокси-сервер	+
Шлюз Modbus TCP/RTU и Modbus RTU/TCP	+

Управление

Локальное управление	Консоль RS-232 (RJ45), веб-интерфейс
Удаленное управление	ViPNet Administrator , веб-интерфейс, системная консоль
Удаленное обновление	ViPNet Administrator
Управление политиками безопасности	ViPNet PolicyManager

Доступность и надежность

Кластер горячего резервирования	+
Работа в необслуживаемом режиме 24x7	+
Время наработки на отказ (MTBF)	350 000 часов

¹Исполнение с беспроводными модулями от -20° до +60°

²Указана максимальная пропускная производительность. Реальная производительность зависит от среды передачи данных и технической реализации.

³Только 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 4U

⁴Не поддерживает «Деловую почту» и «Фаловый обмен» для ViPNet Client for Windows, а также ViPNet CSS Connect



ViPNet xFirewall

ПАК ViPNet xFirewall – это шлюз безопасности – межсетевой экран нового поколения, сочетающий функции классического межсетевого 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]



Гранулированная политика безопасности, которая строится в терминах «Пользователь» - «Приложение» - разрешить/запретить



Обеспечение безопасного использования персональных устройств в рабочих целях с полным соблюдением политик безопасности компании – BYOD (Bring Your Own Device)



Выявление и блокировка более 2000 прикладных протоколов и приложений: игры, социальные сети, torrent и т.д.

- Снижение расходов на потребление интернет-трафика
- Минимизация поверхности атак



Обнаружение и нейтрализация сетевых вторжений с использованием встроенной системы предотвращения вторжений (IPS)



Инспекция SSL/TLS-трафика средствами глубокой инспекции протоколов, системой предотвращения атак, антивирусными решениями и контентной фильтрацией

[ВОЗМОЖНОСТИ]

МЕЖСЕТЕВОЙ ЭКРАН

Межсетевой экран
с контролем
состояния сессий

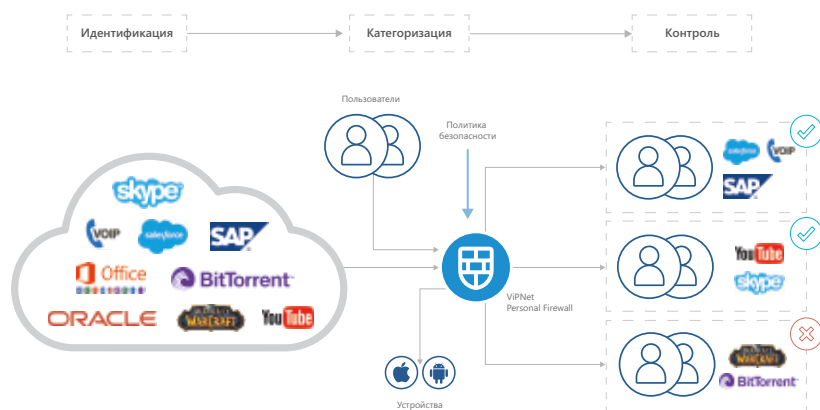
Трансляция
адресов NAT/PAT

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



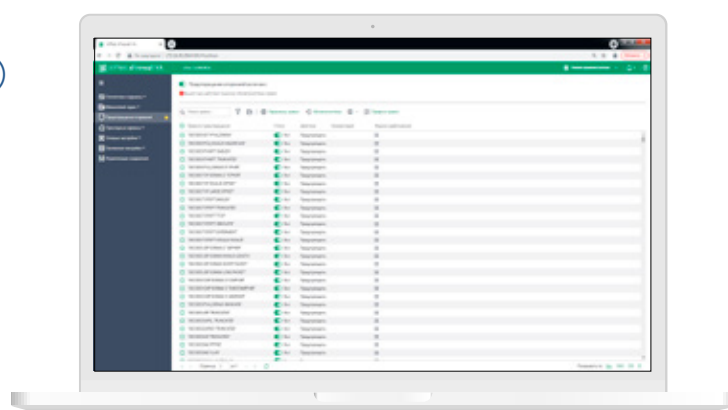
DPI (deep packet inspection) – механизм глубокой инспекции протоколов. DPI использует различные техники идентификации трафика пользовательских приложений: на основе портов и протоколов, сигнатурный метод, эвристический метод. Эти подходы позволяют выявить даже те приложения, трафик которых шифруется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

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ (IPS – INTRUSION PREVENTION SYSTEM)

Сигнатурный метод анализа трафика

Эвристический метод анализа трафика

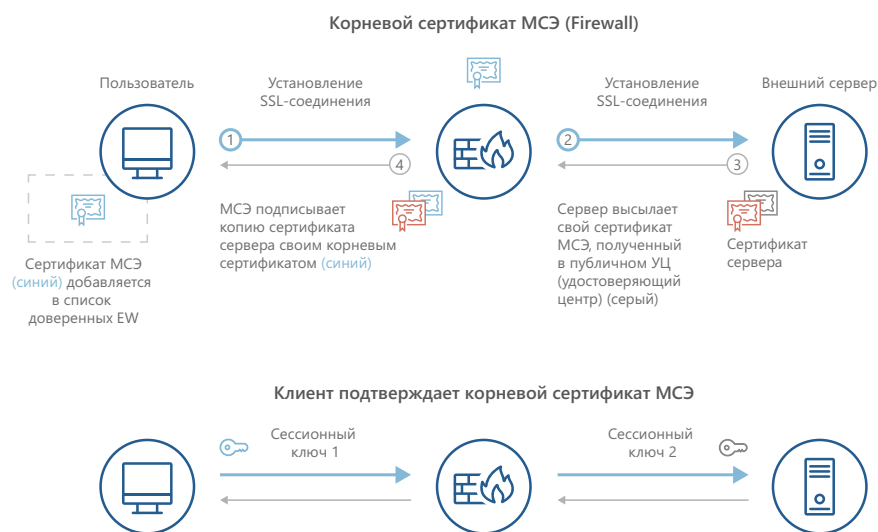
База правил, содержащая описания сетевых угроз, регулярно обновляется специалистами ИнфоТеКС для поддержания в актуальном состоянии



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

ИНСПЕКЦИЯ SSL/TLS-ТРАФИКА



Классификация SSL/TLS-трафика, выявление и выборочная фильтрация трафика приложений

Исследование содержимого SSL/TLS-сессий средствами DPI и IPS

URL- и контент-фильтрация HTTP(S)-трафика

Выявление и блокировка вирусов и вредоносного ПО в HTTP(S)-трафике

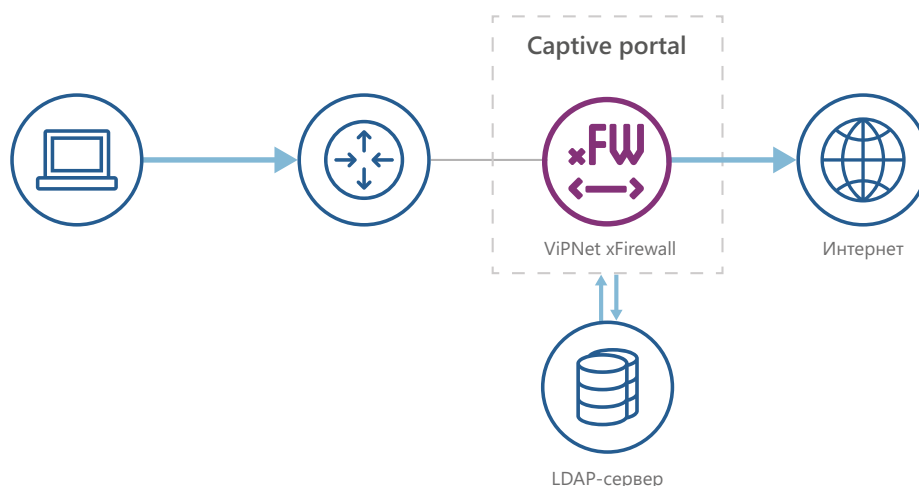
Инспекция SSL/TLS подразумевает два шага:

- 1) SSL decryption – расшифровывание SSL-трафика, проходящего через межсетевой экран
- 2) 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



СЕТЕВЫЕ ФУНКЦИИ

- Развитая статическая маршрутизация
- Динамическая маршрутизация
- Поддержка VLAN (dot1q)

- Агрегирование каналов связи (bonding (LACP), EtherChannel)
- Поддержка QoS, ToS, DiffServ

СЕРВИСНЫЕ ФУНКЦИИ

- DNS-сервер
- NTP-сервер
- DHCP-сервер
- DHCP-Relay

ОТКАЗОУСТОЙЧИВОСТЬ И РЕЗЕРВИРОВАНИЕ

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

[ПРОИЗВОДИТЕЛЬНОСТЬ]¹

Исполнение	xF100	xF1000 C/D	xF5000
			
МЭ, 1518 байт UDP (Мбит/сек) ²	800	2 700	19 000
МЭ (пакетов/сек)	90 000	1 300 000	4 000 000
МЭ, TCP (Мбит/сек)	720	2 700	9300
Application Control (МЭ+DPI) ³ (Мбит/сек)	190	1 500	3 400
NGFW Throughput ⁴ (Мбит/с)	9,5	249	669
NGFW+SSL Inspection ⁵ (Мбит/с)		260	615
Соединений в секунду	2 500	20 000	50 000
Кол-во одновременно обслуживаемых соединений	148 500	990 000	9 900 000

¹Производительность зависит от активированных функций, характеристик обрабатываемого сетевого трафика: протоколов, размера пакетов. Производительность может меняться вследствие изменений, вносимых в новые версии программного обеспечения.

²Результаты получены на основании методики АО «ИнфоТекС»

³Результаты получены для трафика EMIX, который представляет собой смесь трафиков различных прикладных протоколов: BitTorrent, HTTP, HTTPS, Oracle DB, SMTP, SSH и др.

⁴Результаты получены для активированных 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.

⁵Результаты получены для активированных МЭ, DPI, IPS с использованием актуальной на момент теста базы правил IPS, контентной и антивирусной инспекции SSL-трафика при анализе HTTPS-трафика.

[АППАРАТНЫЕ ХАРАКТЕРИСТИКИ]

Наименование аппаратной платформы	xF100 N1	xF1000 Q7, Q8	xF5000 Q2
			
Форм-фактор	ПАК (MiniPC)	ПАК (19" Rack 1U)	ПАК (19" Rack 1U)
Размеры (Ш × В × Г), мм	170 x 41,5 x 138	430 x 43,4 x 380	444 x 44 x 383
Масса, кг	1	7,2	7.9
Источник питания	DC 24В; 2,5А	xF1000 Q7 – встроенный БП, 110-240 В, 300 Вт xF1000 Q8 – два встроенных БП с функцией «горячей» замены, 110-240 В, 300 Вт	Два встроенных БП с функцией «горячей» замены, 110-240 В, 300 Вт
Порты ввода/вывода	1x VGA 2x USB	1x VGA 1x COM DB9 6x USB	1x VGA 1x COM DB9 6x USB
Сетевые порты	• 4 x RJ45 1 Гбит/с • 1 x SFP 1 Гбит/с	xF1000 Q7: • 8 x RJ45 10/100/1000 Мбит/с xF1000 Q8: • 4 x RJ45 10/100/1000 Мбит/с • 4 x SFP 10/100/1000 Мбит/с	• 4 x RJ45 1 Гбит/с • 8 x SFP+ 10 Гбит/с

[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)

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.

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



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

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]

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	• Поддерживает 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»	• Ведутся работы по сертификации на соответствия требованиям ФСБ России к СКЗИ 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	



ViPNet TLS Gateway

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

Использование протокола TLS обеспечивает аутентификацию пользователей и организацию защищенных соединений при работе с порталными решениями

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]

- 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 политик разграничения доступа
- Возможность организации доступа к защищаемым ресурсам с использованием российских и/или иностранных криптоалгоритмов
- Автоматическое поддержание актуальности списков аннулированных сертификатов (CRL)
- 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 протоколов IPv6 и OCSP
- Мониторинг состояния по протоколу SNMP
- Работа в режиме кластера

[ОБЛАСТЬ ПРИМЕНЕНИЯ]

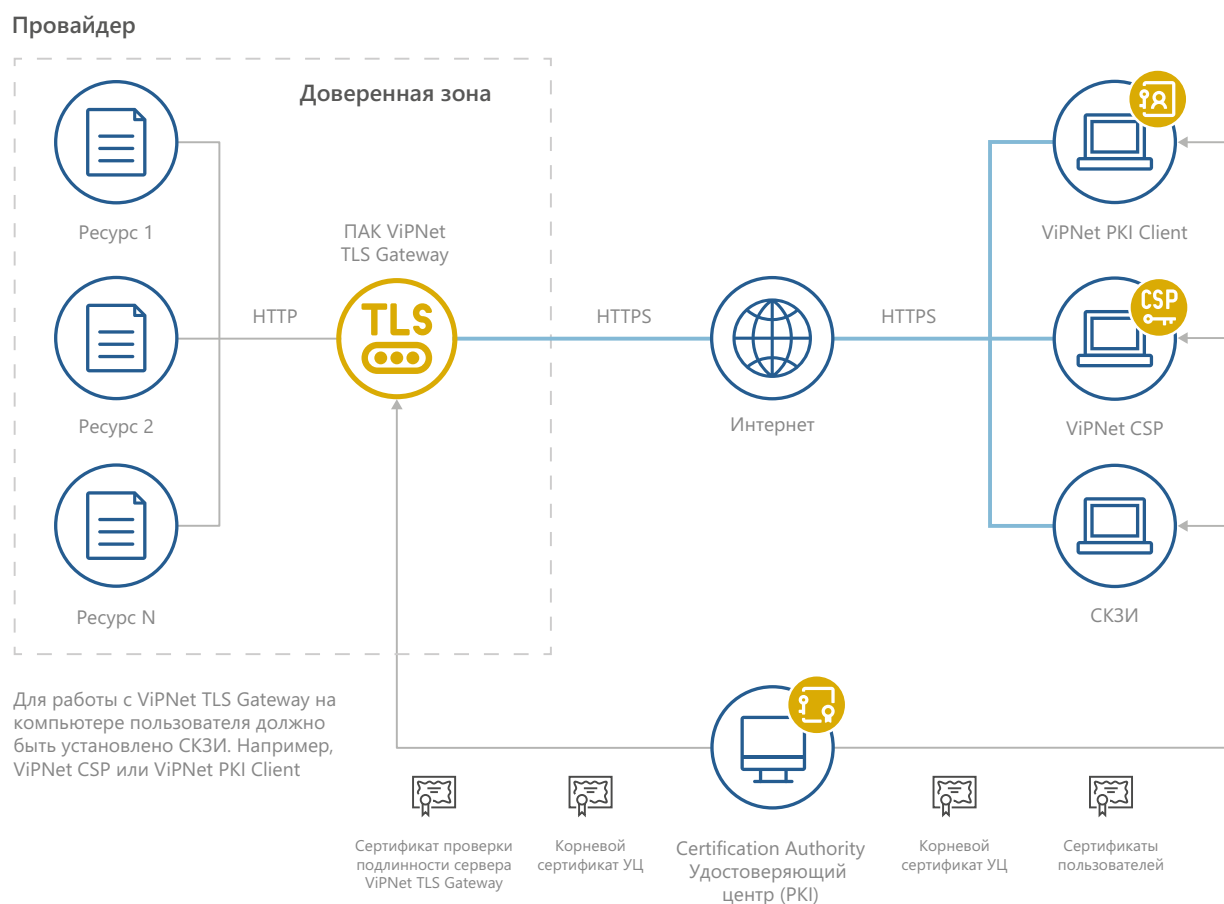


Удаленный доступ сотрудников к корпоративным ресурсам



Предоставление электронных услуг по защищенному каналу

Использование ViPNet TLS Gateway для предоставления доступа пользователей к веб-сервисам



ПОДДЕРЖИВАЕМЫЕ КРИПТОГРАФИЧЕСКИЕ СТАНДАРТЫ И РЕКОМЕНДАЦИИ

- ГОСТ Р 34.10-2001/2012, RSA, ECDSA
- ГОСТ Р 34.11-94/2012
- ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ Р 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ Р 34.13-2018), AES
- Рекомендации Технического комитета 026

ПОДДЕРЖИВАЕМЫЕ ВИРТУАЛЬНЫЕ СРЕДЫ (ДЛЯ TLS VA)

- VMware Workstation
- VMware vSphere ESXi
- Oracle VM VirtualBox
- Платформы виртуализации, основанные на Kernel Virtual Machine (KVM)

[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 КСЗ для исполнений
TLS 500, TLS 1000, TLS 5000, TLS 550,
TLS 1100, TLS 5500



ViPNet Administrator

Программный комплекс, предназначенный
для настройки и управления защищенной сетью

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]

- 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]

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

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

СКЗИ и ЭП класса КС1, КС2, КС3

[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

The background of the slide is a high-angle photograph of a business meeting. Several people are seated around a table, working on laptops and tablets. Overlaid on this image is a complex network diagram consisting of white dots (nodes) and thin white lines (edges) that connect the nodes in a web-like pattern. Some nodes are larger than others. Scattered around the diagram are various sequences of numbers, some separated by dots, such as '0 0 5 . 2 3', '3 2 . 2 4 5', '3 4 0', '6 6 2 . 3 5 7', '4 5 . 1 3 3', '0 9 . 8 2 7', and '8 6 . 5 2'.

Ⓜ 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]

- Продукт позволяет обеспечить унифицированный доступ к ресурсам корпоративных информационных систем из любой точки мира с использованием произвольных TCP/IP-сетей
- Технологии ViPNet, лежащая в основе продукта, позволяет эксплуатировать территориально распределенные ИС из единого центра управления и обновлять ключи шифрования и программное обеспечение по защищенным каналам
- 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
- Архитектура продукта позволяет обеспечить одновременную работу с ресурсами различных сегментов корпоративной сети

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
- Персональный сетевой экран

[СЕРТИФИКАЦИЯ]

ФСБ РОССИИ

ViPNet Client for Windows соответствует требованиям: СКЗИ класса КС1, КС2 и КС3 МЭ 4 класса

ViPNet Client for Linux: СКЗИ класса КС1, КС2 и КС3

ViPNet Client for Android СКЗИ класса КС1

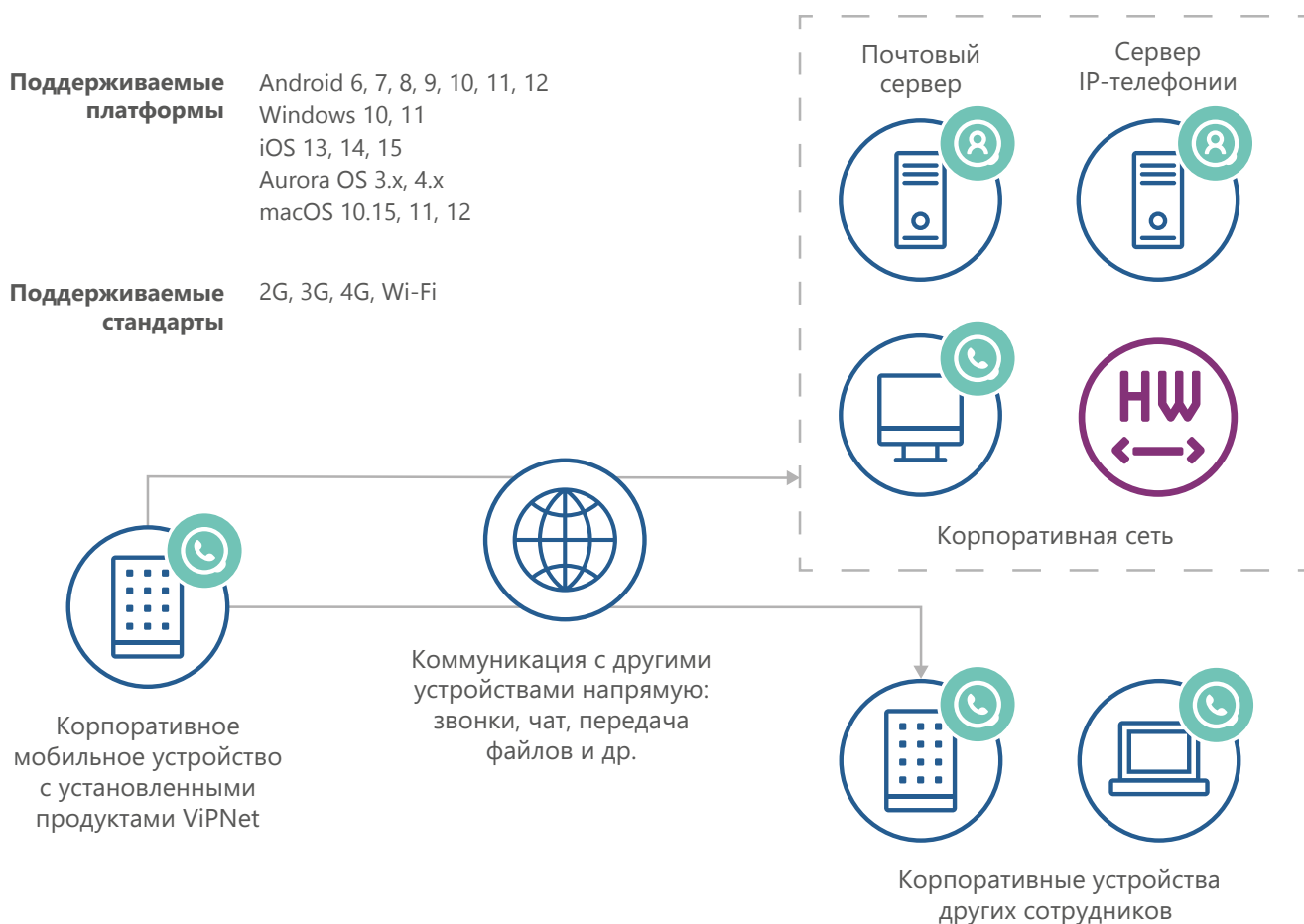
ViPNet Client for iOS СКЗИ класса КС1

ViPNet Client for Aurora СКЗИ класса КС1 и КС2

ФСТЭК РОССИИ

ViPNet Client for Windows соответствует требованиям: МЭ типа В 4 класса

Сценарии использования и защиты мобильных и стационарных рабочих мест



[СЦЕНАРИИ]

1. 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, что позволяет обеспечить защиту конфиденциальной информации, в том числе и от внутреннего нарушителя.
2. 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»).
3. ViPNet Client поддерживает работу на виртуальных машинах, что позволяет использовать средства защиты ViPNet в VDI-средах.

- 4 ViPNet Client может быть использован 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.
- 5 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 применять корпоративные механизмы информационной безопасности к любым устройствам, физически покидающим защищенный периметр.



ViPNet Policy Manager

Система централизованного
группового управления политиками
безопасности защищенной сети ViPNet

[ПРЕИМУЩЕСТВА]

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

[СПЕЦИАЛЬНЫЕ ФУНКЦИИ]

- 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.