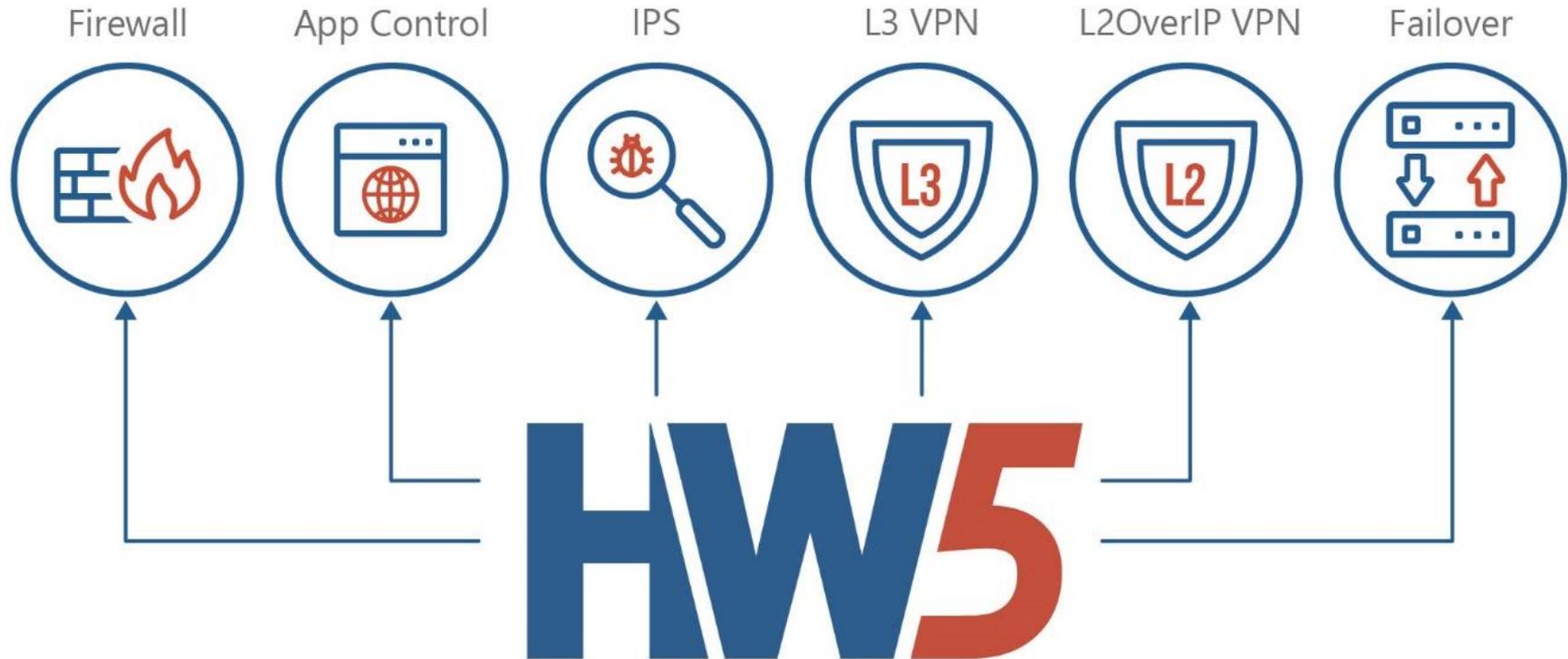


VIPNet Coordinator HW 5 новое поколение шлюзов безопасности

Виталий Беличко
Ведущий менеджер продуктов



VIPNet Coordinator HW 5



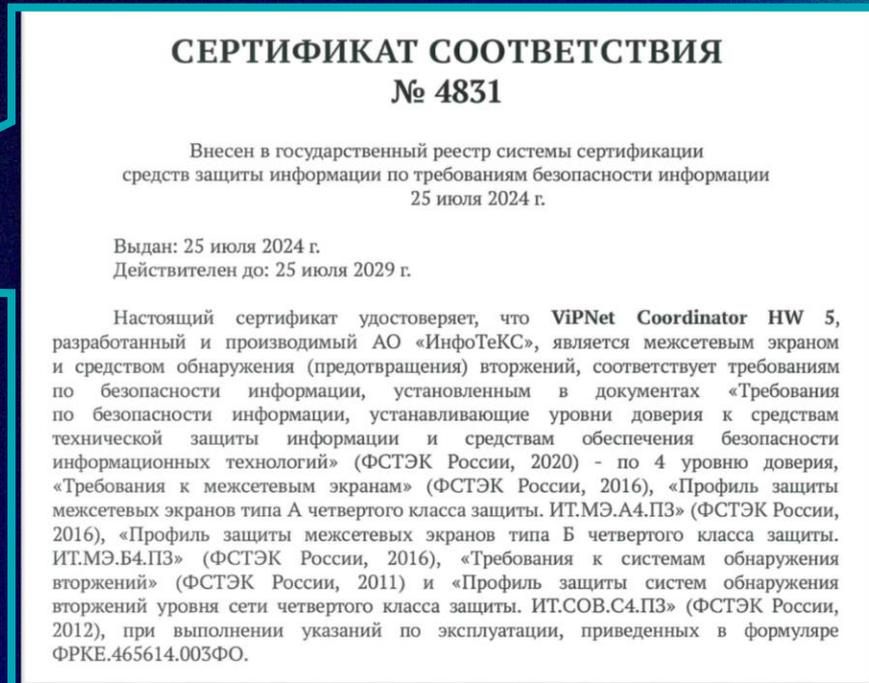
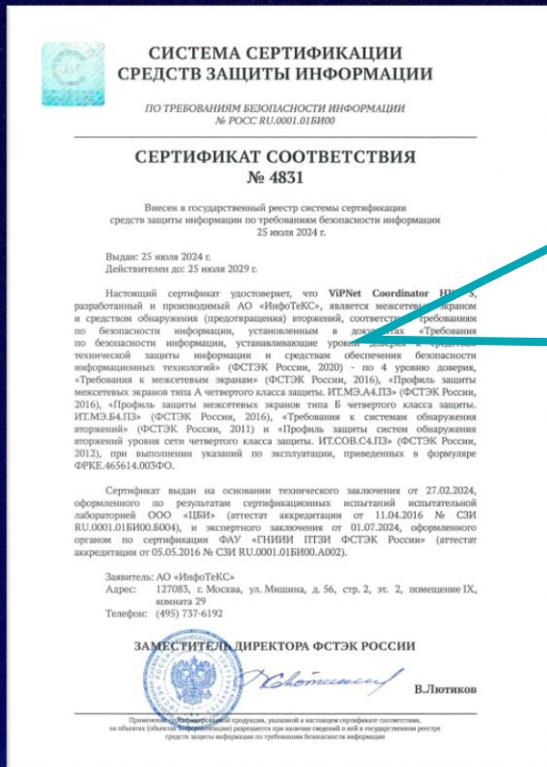
Типовая схема применения НВ 5

Центральный офис

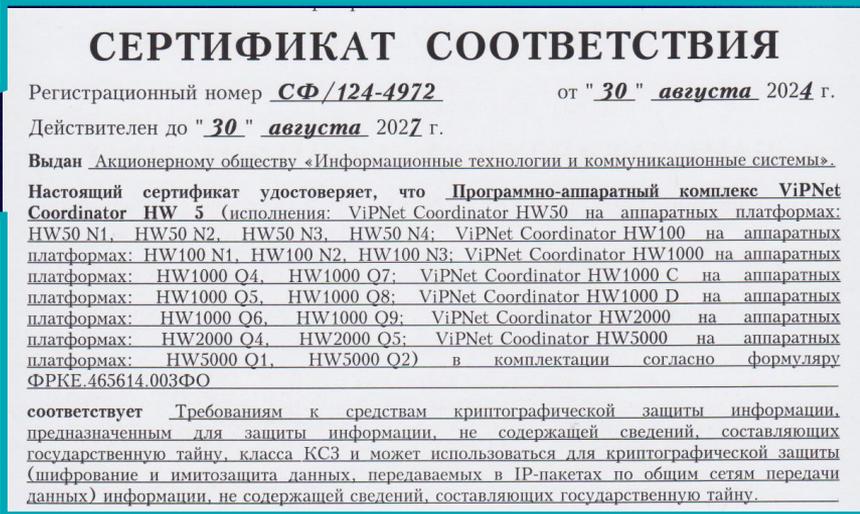
Удаленные пользователи



Сертификат ФСТЭК России (МЭ и СОВ)



Сертификат ФСБ России (СКЗИ КСЗ)



Требования по сертификации

ФСБ России

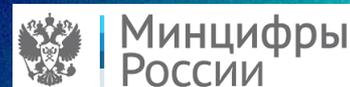
- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

- Межсетевой экран тип «А» и тип «Б» 4 класса
- COB уровня сети 4 класса
- 4-й уровень доверия средств защиты информации
- Многофункциональный межсетевой экран уровня сети **NEW**

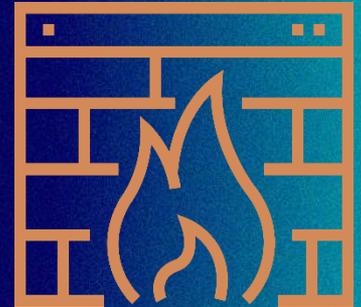
Минцифры России и Минпромторг России

- В реестре российского ПО и реестре РЭП



Межсетевое экранирование

- Внедрение технологии DPI (контроль приложений)
- Идентификация пользователей с использованием:
 - Microsoft Active Directory
 - Captive Portal с LDAP каталогом
- Повышение производительности МЭ
- Идентификация правил МЭ
- Счетчики срабатывания правил МЭ



Счетчики срабатывания правил МЭ

- Состояние системы
- Журналы
- Статистика
- Межсетевой экран
- Сетевые фильтры
- Трансляция адресов (NAT)
- Обработка прикладных прот...
- Группы объектов
- Прокси-сервер
- Пользователи сети
- Защищенная сеть (VPN)
- Предотвращение вторжений
- Прикладные сервисы

Сетевые фильтры

Фильтры защищенной сети Фильтры туннелируемых узлов Локальные фильтры открытой сети Транзитные фильтры открытой сети

Фильтр по тексту... Добавить Обновить счетчики срабатываний Временный подсчет

№	Статус	Имя фильтра	ID	Срабатывания	Регистрация	Источники
4	Вкл.	✓ Allow RES subsystem	100006	0	Выкл.	Все
5	Вкл.	✓ Allow ViPNet MFTP in	100007	0	Выкл.	Все
6	Вкл.	✓ Allow ViPNet MFTP out	100008	0	Выкл.	Мой узел ViPNet
7	Вкл.	✓ Allow ViPNet Control services out	100009	2K	Выкл.	Мой узел ViPNet
8	Вкл.	✓ Allow ViPNet Control services in	100010	1K	Выкл.	Control Center
Настраиваемые фильтры						
1	Вкл.	✗ ICMP redirect in	4000035	0	Вкл.	Все
2	Вкл.	✗ ICMP redirect out	4000036	0	Вкл.	Мой узел ViPNet
3	Вкл.	✓ Allow ICMP Ping in	4000037	5	Выкл.	Все
4	Вкл.	✓ Allow ICMP Ping out	4000038	0	Выкл.	Мой узел ViPNet

Выборочное логирование правил МЭ

Параметры сетевого фильтра ✕

Название:

Состояние: Включено

Действие:

- Блокировать трафик
- Пропускать трафик
- Отклонять трафик с ответом:
- Регистрировать IP-пакеты

Предотвращение вторжений (IPS)

ViPNet Coordinator VA



Статистика и журналы

Межсетевой экран

Защищенная сеть (VPN)

Предотвращение вторжений

Прикладные сервисы

Сетевые настройки

Маршрутизация

Системные настройки

Предотвращение вторжений включено

Поиск правил...

Блокирующие

- Правило предотвращения
- "ET EXPLOIT Quanta LTE Router UDP Backdoor Activati
- "ET EXPLOIT Serialized Java Object Generated by yso
- "ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli)"
- "AM Exploit Disk Sorter Enterprise 9.1.12 Buffer Overflo
- "AM Exploit Weblogic Remote Code Execution"
- "AM Exploit rConfig v3.9.2 unauthenticated Remote Co
- "AM EXPLOIT Unauthenticated XSS SugarCRM Enterpri
- "AM Exploit Hootoo HT-05 - RCE"
- "AM Exploit Solr RCE stage 2"

Заблокировано IPS

Код события 142 - Заблокирован IPS подсистемой как вредоносный

Обработка по правилам предотвращения вторжений

Правило: ["AM_WEB_CLIENT_NETGEAR ProSafe Network Management System Arbitrary file download"](#)

Группа: web_client

Класс правила: web-application-attack

Идентификатор: 1.3001501.12

Результат анализа

Пользователь сети: Нет данных

Приложение: unknown

Прикладной протокол: HTTP

Агрегация пакетов за интервал

Начало интервала: 16 Авг 2021, 17:03:16

Конец интервала: 16 Авг 2021, 17:03:16

Количество пакетов: 1

Размер: 366 байт

Свойства IP-пакета

Источник: 66.254.33.10 : 59418

Назначение: 192.168.1.200 : 80

Транспортный протокол: 6-TCP

Сетевой интерфейс: eth2

Направление: [← Входящий

Тип: Открытый

Тип адреса: Одноадресный

Трансляция: Нетранслированный

Ethernet-протокол: 800h

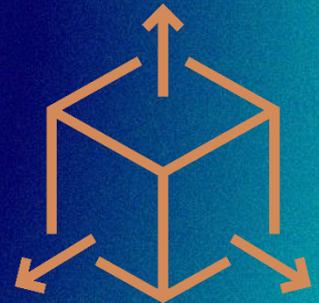
Закрыть

Вкл Блокировать

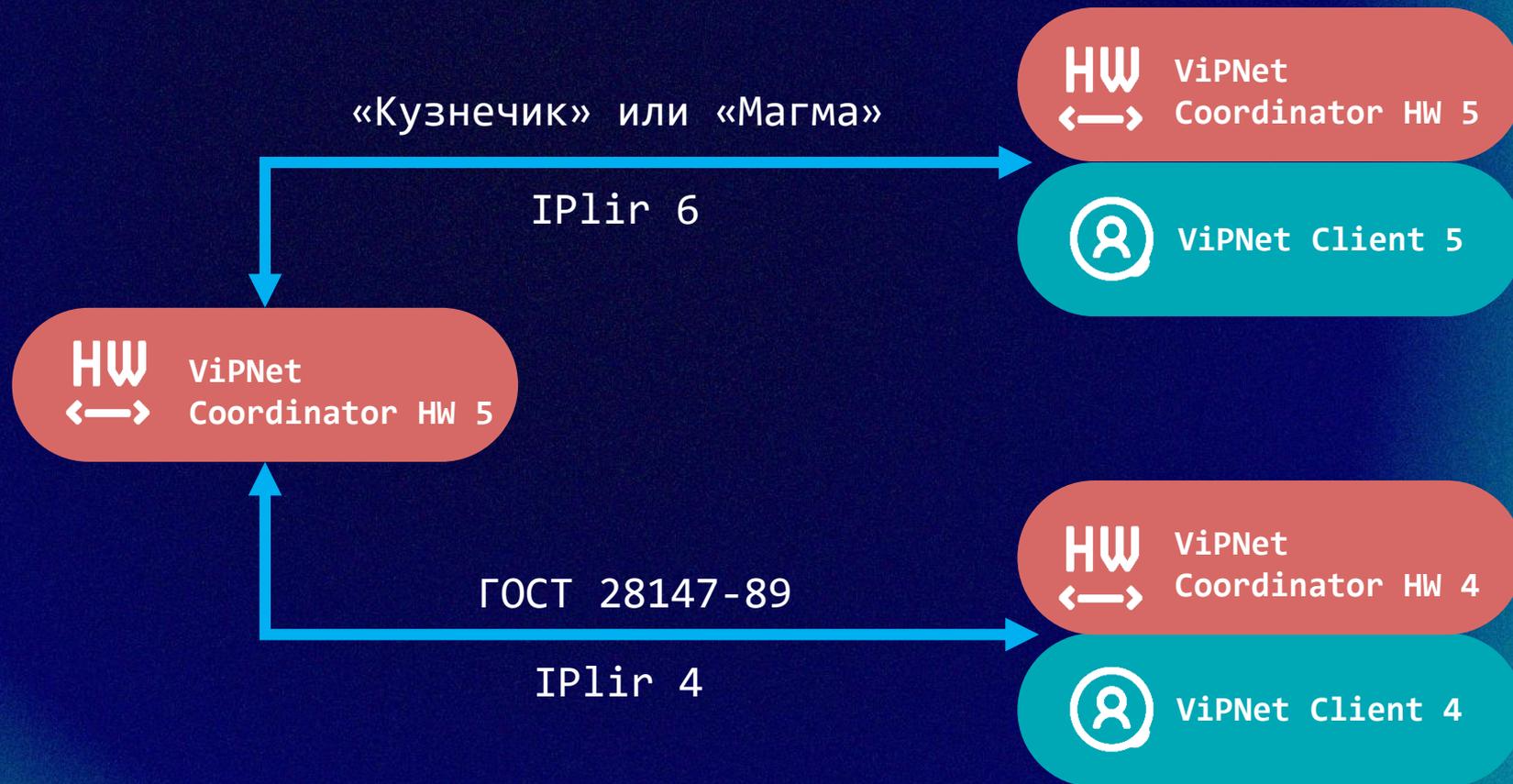
Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPsec – протокол безопасности сетевого уровня

ТК 26 Р 1323565.1.034-2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня»

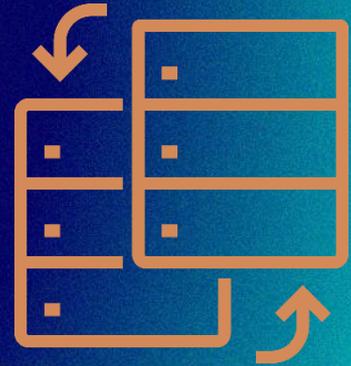


Обратная совместимость



Кластер высокой доступности

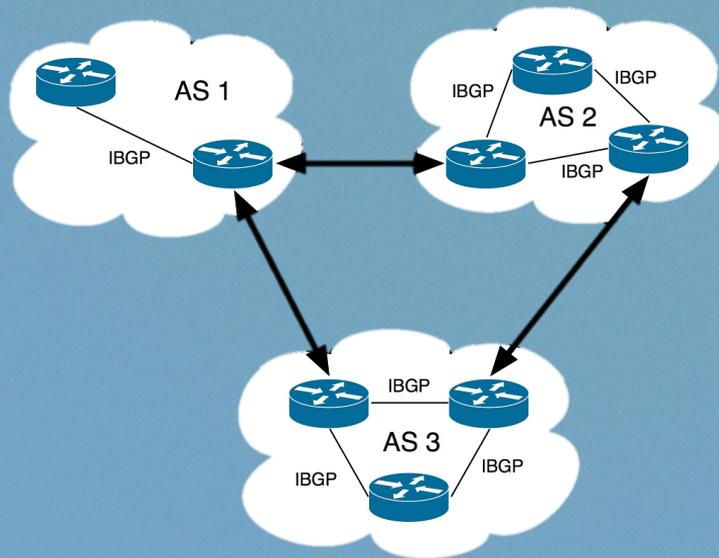
- Быстрое переключение кластера по потере связи и питания
- Синхронизация сессий МЭ в кластере
- Виртуальный MAC-адрес для кластера
- Синхронизация времени пассивного узла кластера
- Минимальное время переключения кластера сократилось до 1 секунды



Сетевые функции

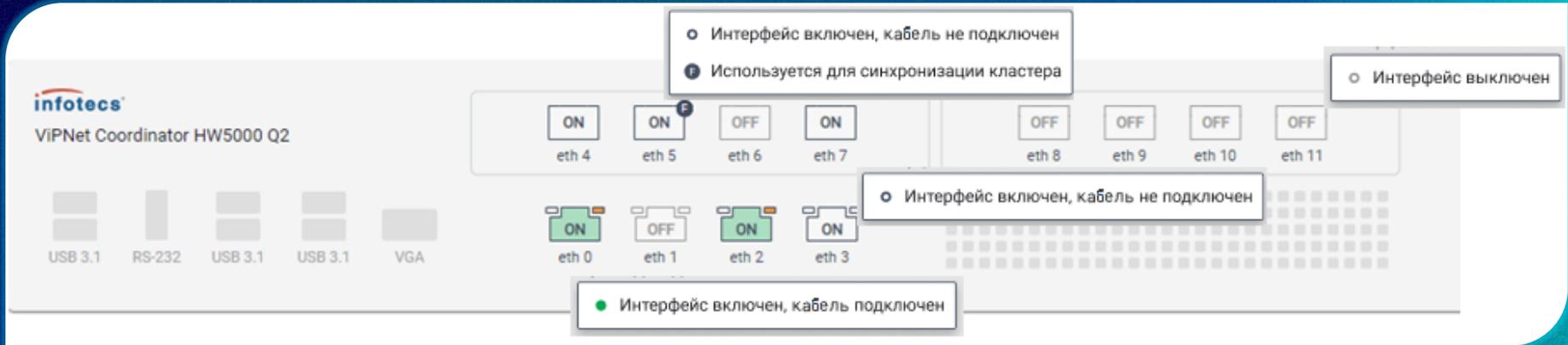
- Расширенная статическая маршрутизация (Policy based routing)
- Динамическая маршрутизации (OSPF, BGP)
- Поддержка VLAN
- Агрегирование сетевых интерфейсов (802.3ad, LACP)
- Поддержка Jumbo-кадров и Path MTU Discovery
- Приоритизация трафика (QoS, ToS, DiffServ)
- Встроенный DHCP-, DNS-, NTP-сервер
- SNMP, Syslog, Syslog (CEF), SSH, HTTPS

Поддержка протокола BGP



- Создание BGP-окружения или встраивание узла в существующее
- Получение и использование маршрутов по протоколу BGP
- Анонсирование и перераспределение маршрутов
- Балансировка трафика (ECMP, UCMP)

Визуализация сетевых интерфейсов



Серийный номер платформы

- Добавление серийного номера при производстве и пользователем самостоятельно
- Отображение в CLI, WebUI
- Передача данных по SNMP

```
HW1000Q9-node-1# version
Product: ViPNet Coordinator HW
Platform: HW1000 Q9
Serial number: 1234567-890
License: HW1000 D
Software version: 5.3.2-8878
```

Основное	Лицензия
ViPNet Coordinator HW1000 5.3.2-8878	
© 2024, АО «ИнфоТеКС»	
Веб-сайт:	www.infotecs.ru
E-mail:	soft@infotecs.ru
Телефон для регионов России:	8 800 250-0-260
Телефон для Москвы:	+7 495 737-61-92
<hr/>	
Платформа:	HW1000 Q9
Версия ПО:	5.3.2-8878
Серийный номер:	1234567-890

Новая система управления

VIPNet Prime

Ядро

Ролевая модель
Лицензирование
Управление ПО

VPN

Управление
связями,
ключами

РММ

Управление
политиками
безопасности

NVS

Мониторинг
состояния
узлов

VIPNet Coordinator HW 5

Схема лицензирования

Next-Generation Firewall

Based

Advanced

VPN

МЭ

Прокси

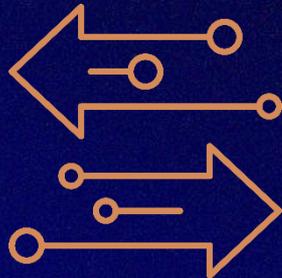
IPS

DPI

Изменение ролевой модели

VipNet Coordinator HW 4

- Пользователь
- Администратор узла
- Администратор группы узлов
- Администратор сети



VipNet Coordinator HW 5

Локальные учетные записи:

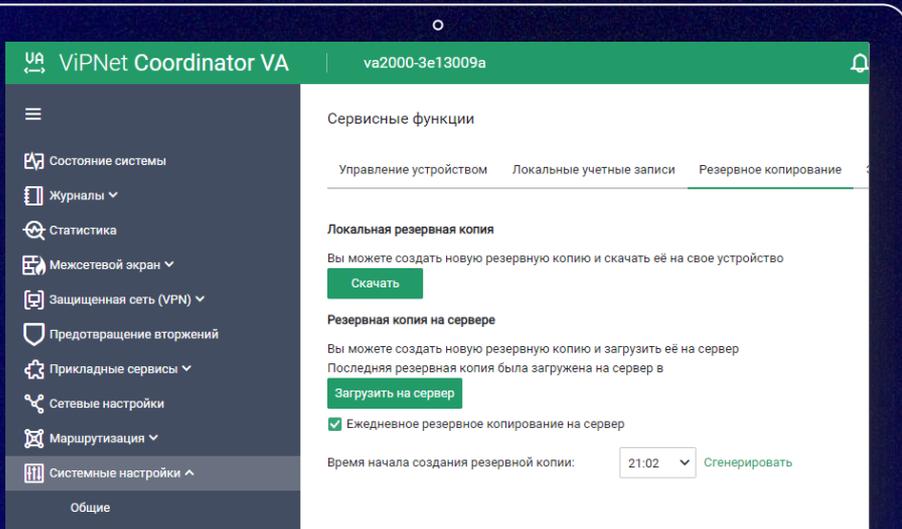
- Администратор
- Пользователь (Аудитор)

+

Централизованные учетные записи:

- Неограниченное количество
- Администратор/Аудитор
- Single Sign-On (SSO)

Резервное копирование



- Локальный экспорт на USB
- Удаленный экспорт через WebUI
- Выгрузка на сервер Prime

Перенос настроек с любой платформы

Импорт настроек

Ввод пароля

Дата создания файла: 09.12.2021

Продукт: HW-VA

Платформа: VA

Версия ПО: 4.5.1

Комментарий: —

Введите пароль защиты файла конфигурации:

От 8 до 31 символа.

Назад

Далее

Импорт настроек

Выбор настроек для восстановления

Укажите настройки, которые вы хотите импортировать на устройство.

Настройки МЭ

Заменить ▾

Просмотреть

Сетевые настройки

Просмотреть

Таблицы и политики статической маршрутизации

Заменить ▾

Просмотреть

Назад

Далее

Отмена

Firewall rules

Service Vpn Rules:

Num	Name	Source	Option	Schedule
Act	Protocol		-> Destination	
	DpiProtocol	[G]DpiGroup, DpiApp	DomainUser	
1	Block not original udp		Generated	
drop	port	@local	-> @any	
	udp:			
	from 0-2045			
	to 2046,			
	udp:			
	from 2047-65535		@any	
	to 2046	@any		
	@any			
2	Allow ViPNet base		Generated	
pass	services in	@any	-> @local	
	udp:			

Закреть

Аппаратные платформы

HW50



HW100



Малые офисы и филиалы

HW1000

HW1000 C

HW1000 D



Предприятия среднего
бизнеса

HW2000



HW5000



Крупные предприятия,
ЦОД

Поддержка аппаратных платформ

ViPNet Coordinator HW50

- HW50 N1*/N2*/N3*/N4*
- HW50 A1 DEV

ViPNet Coordinator HW100

- HW100 N1/N2/N3
- HW100 Q1/Q2 NEW

ViPNet Coordinator HW2000

- HW2000 Q4
- HW2000 Q5

ViPNet Coordinator HW1000

- HW1000 Q4*/Q5/Q6
- HW1000 Q7/Q8/Q9

ViPNet Coordinator HW5000

- HW5000 Q1
- HW5000 Q2

* - режим BASE only



HW100 Q1/Q2



- 4x 1G RJ-45 / 2x 1G SFP
- 2x USB, Console, VGA
- Внешний БП
- 250 x 44 x 227 ШxВxГ (мм)
- 1,9 кг
- VPN – 400 Мбит/с
- FW – 1400^{BOND} Мбит/с

HW50 A1 DEV



- 3x 1G RJ-45
- 2x USB, Console, HDMI
- Внешний БП
- 150 x 150 x 40 ШxВxГ(мм)
- 400 г

- VPN – 250 Мбит/с
- FW – 700 Мбит/с

HW10 F1 DEV

- 3x 1G RJ-45
 - 2x USB, HDMI
 - Внешний БП, Type-C
 - 95 x 30 x 68 ШxВxГ (мм)
 - 260 г
-
- VPN – 35 Мбит/с
 - FW – 200 Мбит/с



VIPNet Coordinator VA 5

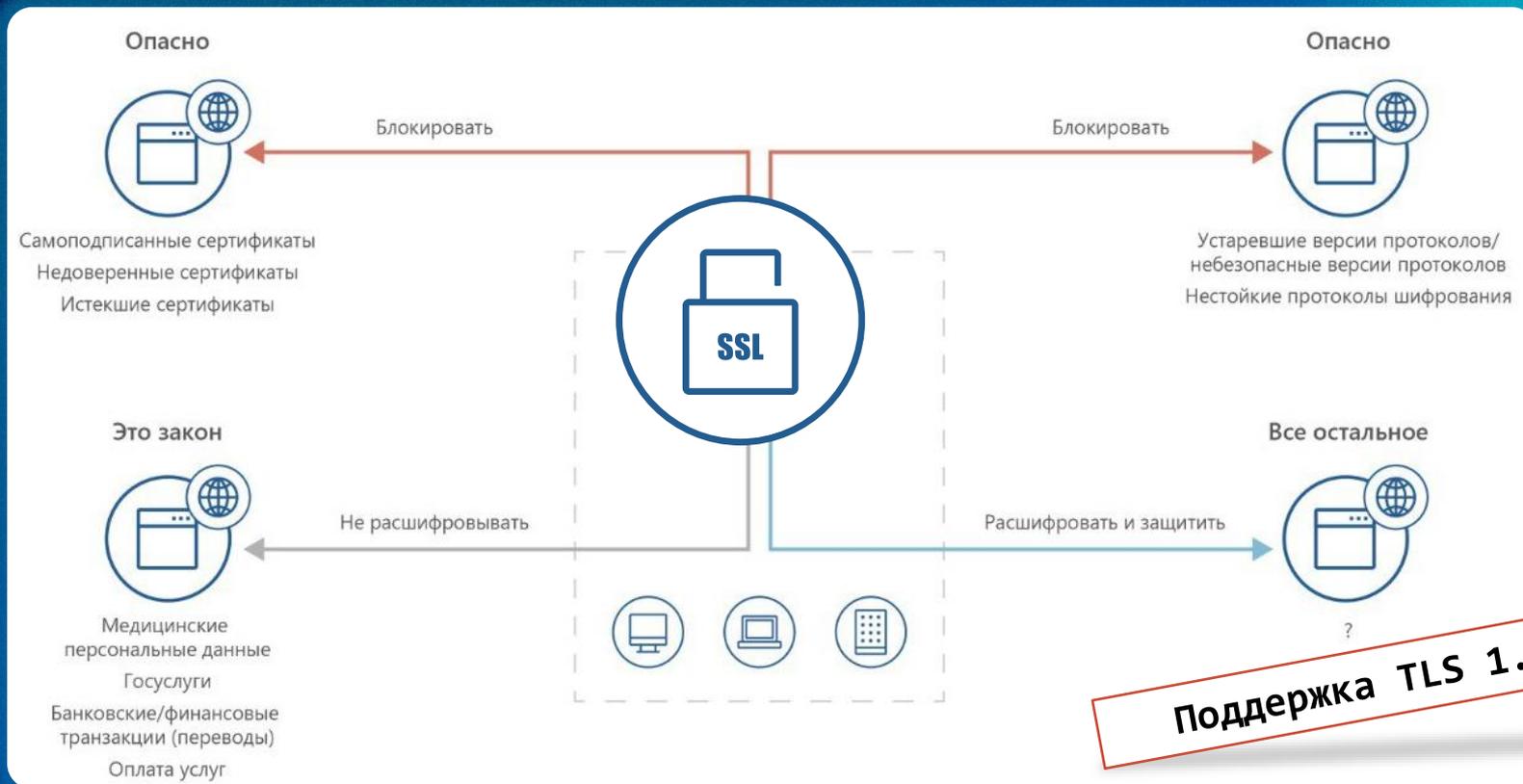
Поддерживаемые гипервизоры:

- KVM, QEMU-KVM и Proxmox VE
- Астра Брест, zVirt, SharxBase
- VMware ESXi
- VMware Workstation
- Microsoft Hyper-V Server
- Oracle VM Server
- Oracle VM VirtualBox



Планы развития

SSL/TLS-инспекция



Поддержка TLS 1.3

URL-фильтрация

- Межсетевой экран ^
- Сетевые фильтры
- Трансляция адресов (NAT)
- Группы объектов
- ICAP-сервер
- Пользователи сети
- Расшифровка SSL/TLS
- Прикладные службы v
- Сетевые настройки v
- Системные настройки v
- Управляющие соединения

База URL-категорий Обновить v Настройки обновления с сервера

Поиск... + [Добавить](#) [Импортировать](#) Всего: 33

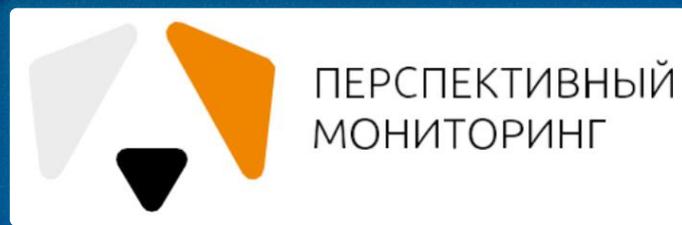
<input type="checkbox"/> Имя URL-категории	Состав	Описание
<input type="checkbox"/> v Настраиваемые (2)		
<input type="checkbox"/> Категория 1	activation.sls.microsoft.com messenger.live.com lr.live.net account.live.com update.microsoft.com	Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ✎ ↻ 🗑
<input type="checkbox"/> Категория 1	account.live.com	✎ ↻ 🗑
<input type="checkbox"/> Из базы URL-категорий (27)		
Malware	3581 веб-ресурс	Сайты, распространяющие вирусы и
Phishing & Typosquatting	4984 веб-ресурсов	Фишинг и регистрация доменных имён,
Botnets & C2C	8916 веб-ресурсов	Ботнеты и командные центры для их
Реклама и баннеры	1233 веб-ресурса	Сайты рекламных и баннерных сетей или
Наркотики	3219 веб-ресурсов	Сайты, рекламирующие или продающие
Грубость, матерщина, непристойность	3219 веб-ресурсов	Сайты, содержащие избыточное количество

Источник баз URL-категорий

~85 млн веб-ресурсов

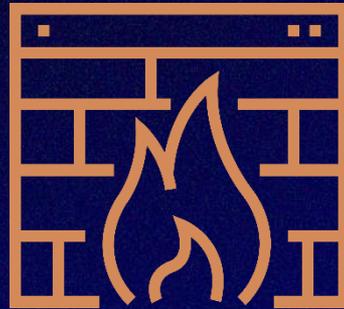
80 категорий

+15% ежемесячный
прирост базы



Блокировка по GEO-IP

- Фильтрация трафика на основе данных о географической принадлежности отправителей
- Использование доверенной базы геолокации IP-адресов на базе «Главного радиочастотного центра» (ФГУП «ГРЧЦ»)



Дружественные страны

Блокировка по GEO-IP

- Состояние системы
- Журналы
- Статистика
- Межсетевой экран
 - Сетевые фильтры
 - Трансляция адресов (NAT)
 - Обработка прикладных протоколов
 - Группы объектов
 - Прокси-сервер
 - Пользователи сети
- Защищённая сеть (VPN)
- Предотвращение вторжений
- Прикладные службы
- Сетевые настройки
- Маршрутизация

Группы объектов

Узлы ViPNet IP-адреса Интерфейсы Протоколы Расписания Страны

Поиск Обновить из файла Последнее

Страна	Код
 Афганистан	AF
 Албания	AL
 Алжир	DZ
 Американское Самоа	AS
 Андорра	AD
 Ангола	AO
 Ангилья	AI
 Антарктида	AQ
 Антигуа и Барбуда	AG
 Аргентина	AR
 Армения	AM
 Аруба	AW

Антигуа и Барбуда

Список применений группового объекта

Объект не используется

Общая информация

Страна:  Антигуа и Барбуда

Код: AG

[Список подсетей](#)

Обнаружение вредоносного ПО

ViPNet Coordinator HW

Admin | 99+ | i



Состояние системы

Журналы

Статистика

Межсетевой экран

Защищённая сеть (VPN)

Предотвращение вторжений

Прикладные службы

Сетевые настройки

Маршрутизация

Системные настройки

Предотвращение вторжений включено

Правила IPS | Методы анализа

База правил IPS

Обновить базу

Настройки обновления с сервера

Дата выпуска базы: от 27 мая 2021, 15:00

Сервер обновления:

updateids.infotecs.ru

Действует до: 13 мая 2022, 03:00

Автоматическое обновление базы:

Ежедневно в 23:59

Обнаружение вредоносного ПО

Обновить базу

Настройки обновления с сервера

Дата выпуска базы: от 27 мая 2021, 15:00

Сервер обновления:

updatemd.infotecs.ru

Действует до: 13 мая 2022, 03:00

Автоматическое обновление базы:

Ежедневно в 23:59

Журнал сетевых сессий



Состояние системы

Журналы ▾

Журнал аудита

Журнал IP-пакетов

Журнал сессий

Журнал СКЗИ

Журнал MFTP

Журнал DNS-запросов

Системный журнал

Статистика

Межсетевой экран ▾

Защищённая сеть (VPN) ▾

Предотвращение вторжений

Прикладные службы ▾

Сетевые настройки

Маршрутизация ▾

Системные настройки ▾

Журнал сессий

Поиск



Результат фильтрации за последний час, с 20.06.2024 13:39:41



Показано: 37



Дата и время	Завершение	Состояние	Источник	Назначение	Пользователь сети	Протокол	URL
2020.06.11 16:45:31	17:55:31	● Завершена	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com https://example.com/blog https://example.com/blog https://example.com/blog
2020.06.11 16:45:31	2020.06.12 13:23:54	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog
2020.06.11 16:45:31	—	● Активна	Isaenko ivan ufa Россия	192.168.15.44:8080 Германия	user@domain	TCP	https://example.com/blog

Расширение возможностей ICAP

- Состояние системы
- Журналы
- Статистика
- Межсетевой экран
 - Сетевые фильтры
 - Трансляция адресов (NAT)
 - Обработка прикладных протоколов
 - Группы объектов
 - Прокси-сервер
 - ICAP-серверы
- Защищённая сеть (VPN)
- Предотвращение вторжений
- Прикладные службы
- Сетевые настройки
- Маршрутизация

ICAP-серверы

Поиск [+ Добавить ICAP-сервер](#)

Статус	Имя сервера	Режим и тип	Адрес и порт	Путь к ICAP-серверу	Передаваемые параметры
<input checked="" type="checkbox"/>	Dr.Web-ICAP Удалённый антивирус Dr.Web	Инспекция трафика Антивирус (av)	● 192.168.15.22:1344	Входящего: /incoming-traffic Исходящего: /outgoing-traffic	Имя пользователя с заголовком: X-Aut IP-адрес с заголовком: X-Client-Ip MAC-адрес с заголовком: X-Client-Mac
<input checked="" type="checkbox"/>	ATHENA Песочница ATHENA	Инспекция трафика Песочница (sandbox)	● 192.168.15.92:1344	Входящего: /incoming-traffic	IP-адрес с заголовком: X-Client-Ip MAC-адрес с заголовком: X-Client-Mac
<input checked="" type="checkbox"/>	Solar Dozor DLP-система Solar	Инспекция трафика Система предотвращения	● 192.168.1.15:1344	Исходящего: /outgoing-traffic	Выкл.
<input type="checkbox"/>	ICAP-сервер	Зеркалирование трафика	● 192.168.15.22:1344	Входящего: /incoming-traffic	Выкл.

- Инспекция:
- SSL/TLS-инспекция
 - Предотвращение вторжений (IPS)
 - Обнаружение вредоносного ПО
 - Антивирус (av)
 - Песочница (sandbox)
 - Предотвращение утечки данных (dlp)

Локальные учетные записи

- новая роль «Сетевой администратор»

ViPNet Coordinator HW

GeneralAdmin 99+

Настройки сессий

Учётные записи

Локальные учётные записи Сессии

Поиск Добавить

Имя учетной записи	Роль	Полное имя	Описание	
Superadmin (Вы)	Суперадминистратор		Встроенная учётная запись	
Admin	Администратор			
Ivanov.Sergej	Администратор	Иванов Сергей Егорович	Инженер по технической ...	
Konovalov.Roman	Администратор	Коновалов Роман Тимофеевич	Инженер по технической ...	
Pavlov.Mikhail	Администратор	Павлов Михаил Николаевич	Инженер по технической ...	
Auditor	Аудитор			
Smirnov.Nikita	Аудитор	Смирнов Никита Михайлович	Инженер по технической ...	
User	Аудитор			

VIPNet Coordinator HW 5.4

- SSL/TLS-инспекция
- URL-фильтрация
- Блокировка по GEO-IP
- Обнаружение вредоносного ПО
- Расширение возможностей ICAP
- Журнал сетевых сессий
- Локальные учетные записи + новая роль
- Интеграция VIPNet SafeBoot



В разработке

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

