

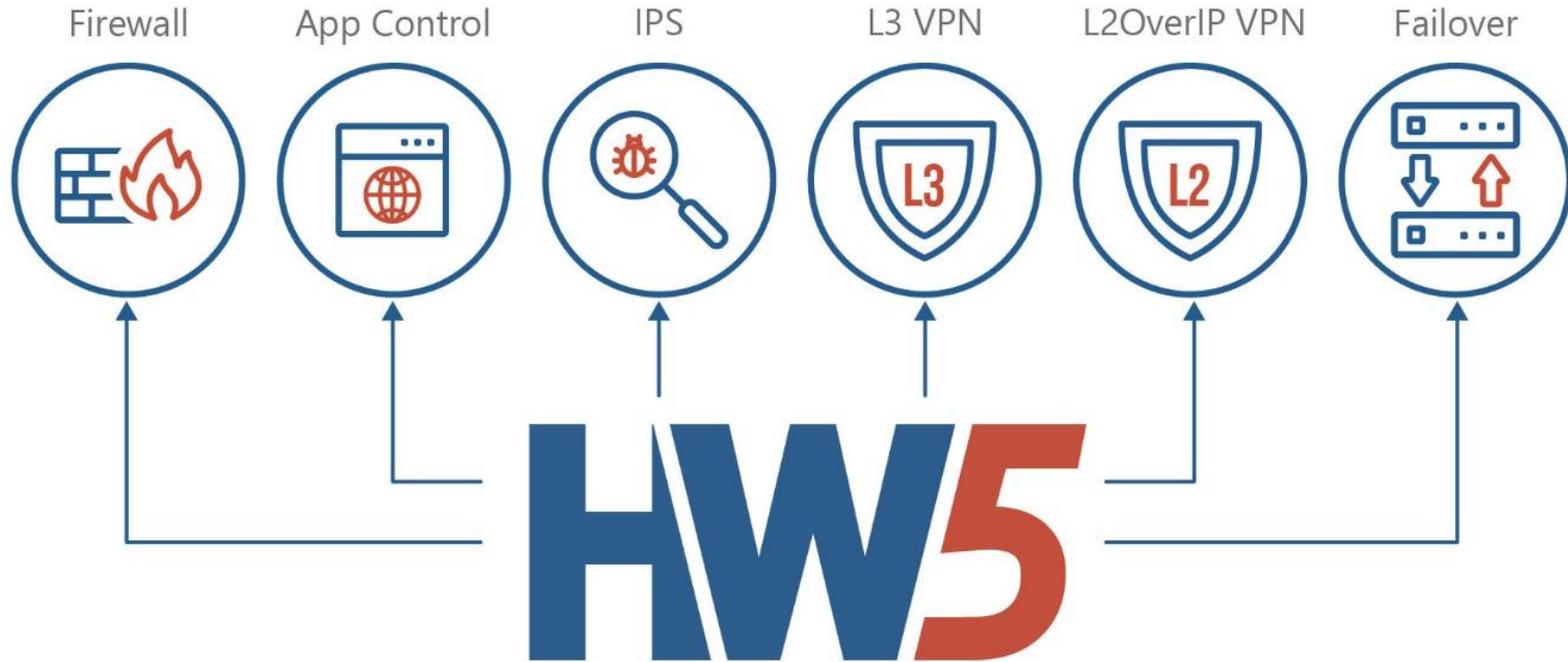
VIPNet Coordinator HW 5

– новое поколение
шлюзов безопасности



Виталий Беличко

VIPNet Coordinator HW 5



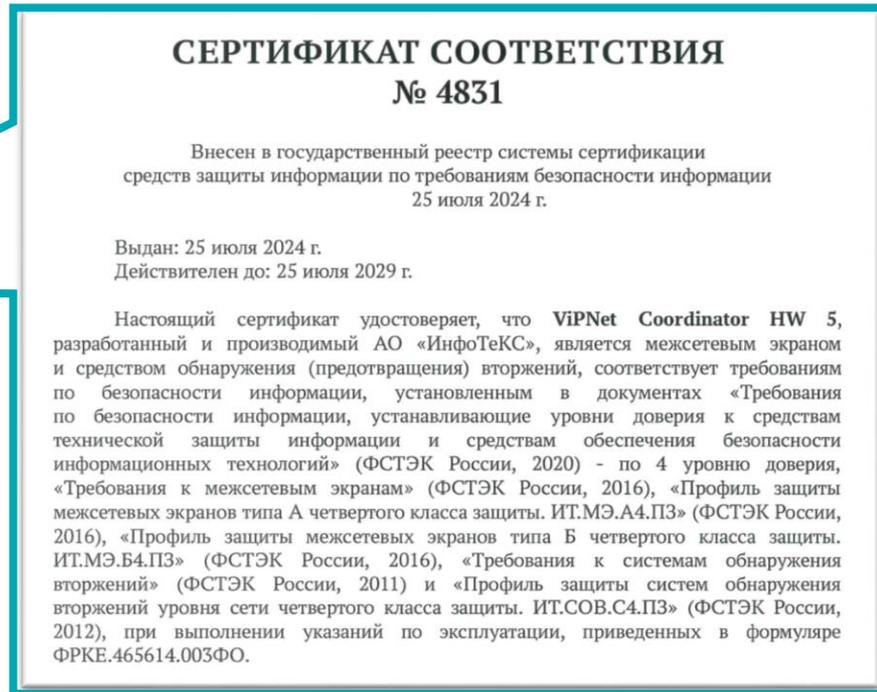
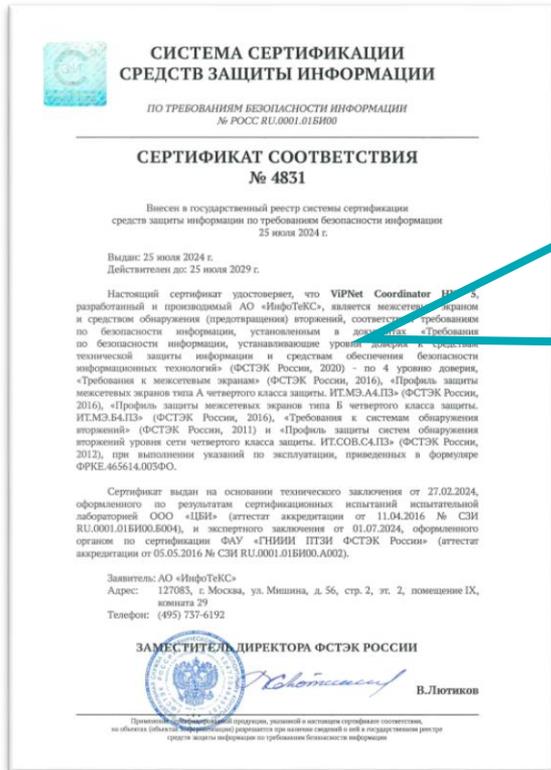
Типовая схема применения HW 5

Центральный офис

Удаленные пользователи



Сертификат ФСТЭК России МЭ и СОВ



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



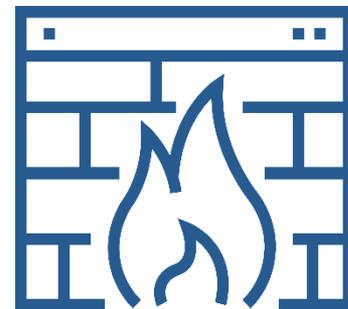
Минцифры
России



МИНПРОМТОРГ
РОССИИ

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



Предотвращение вторжений

The screenshot displays the ViPNet Coordinator VA interface. The main window is titled "Предотвращение вторжений" (Intrusion Prevention) and contains a search bar for rules, a filter icon, and a list of rules. A modal window titled "Заблокировано IPS" (Blocked by IPS) is open, showing details for event code 142. The modal is divided into two columns: "Обработка по правилам предотвращения вторжений" (Processing by intrusion prevention rules) and "Свойства IP-пакета" (IP packet properties).

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

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

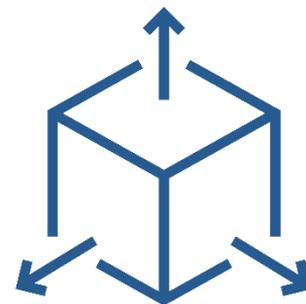
Агрегация пакетов за интервал

Начало интервала:	16 Авг 2021, 17:03:16
Конец интервала:	16 Авг 2021, 17:03:16
Количество пакетов:	1
Размер:	366 байт

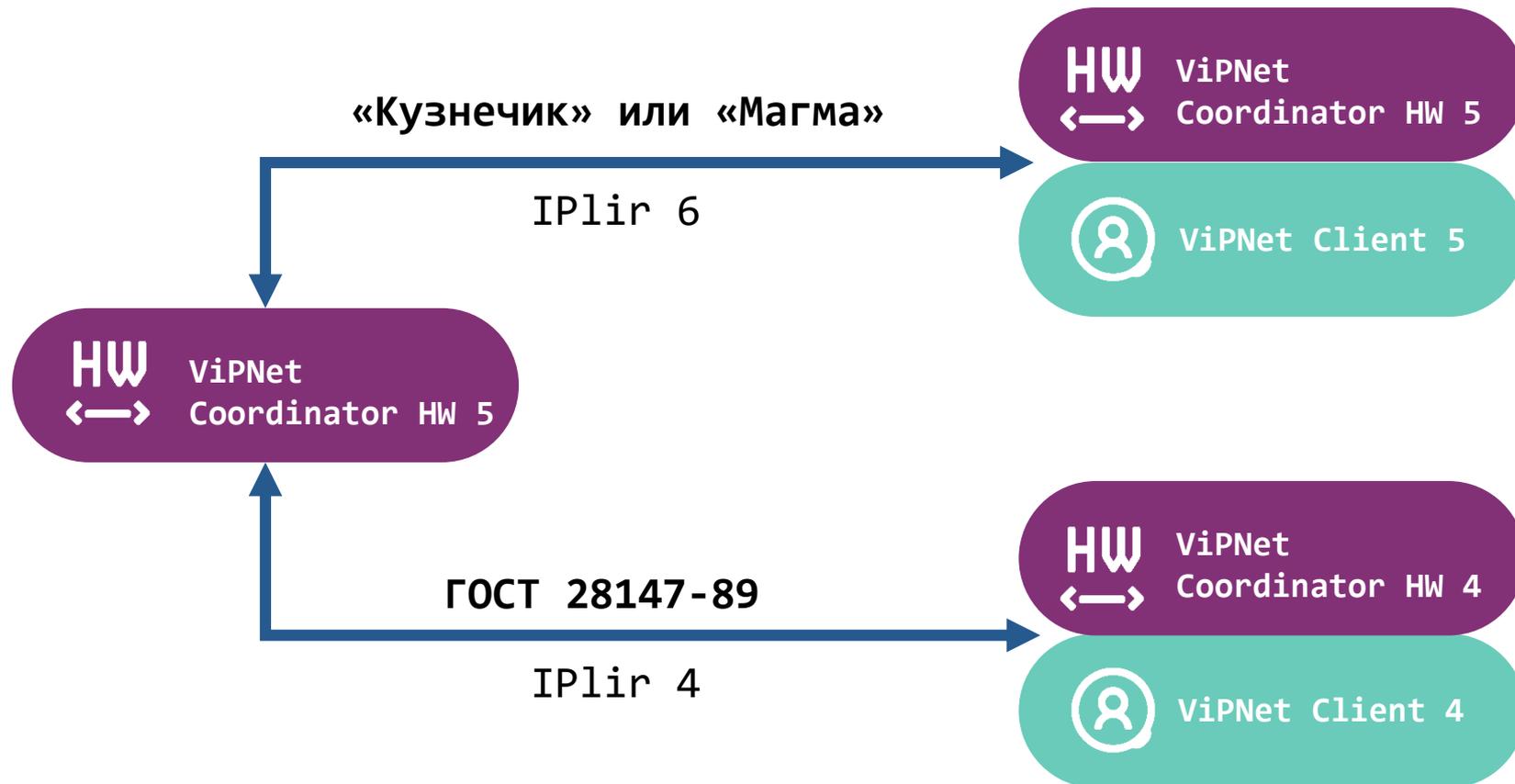
Buttons: Вкл, Блокировать, Закрыть

Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPsec 6 – протокол безопасности сетевого уровня
ТК 26 Р 1323565.1.034-2020 «Информационная технология.
Криптографическая защита информации. Протокол безопасности
сетевого уровня»

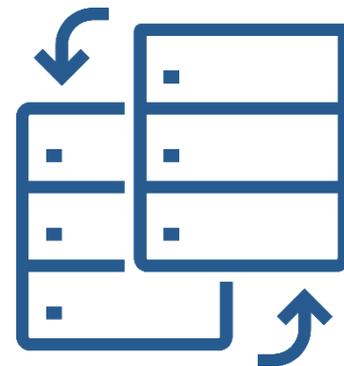


Обратная совместимость



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**



Новая система управления

VIPNet Prime

Ядро

VPN

PMM

NVS

Ролевая модель
Лицензирование
Управление ПО

Управление
связями,
ключами

Управление
политиками
безопасности

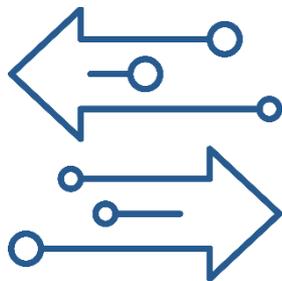
Мониторинг
состояния
узлов

VIPNet Coordinator HW 5

Изменение ролевой модели

ViPNet Coordinator HW 4

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



ViPNet Coordinator HW 5

Локальные учетные записи:

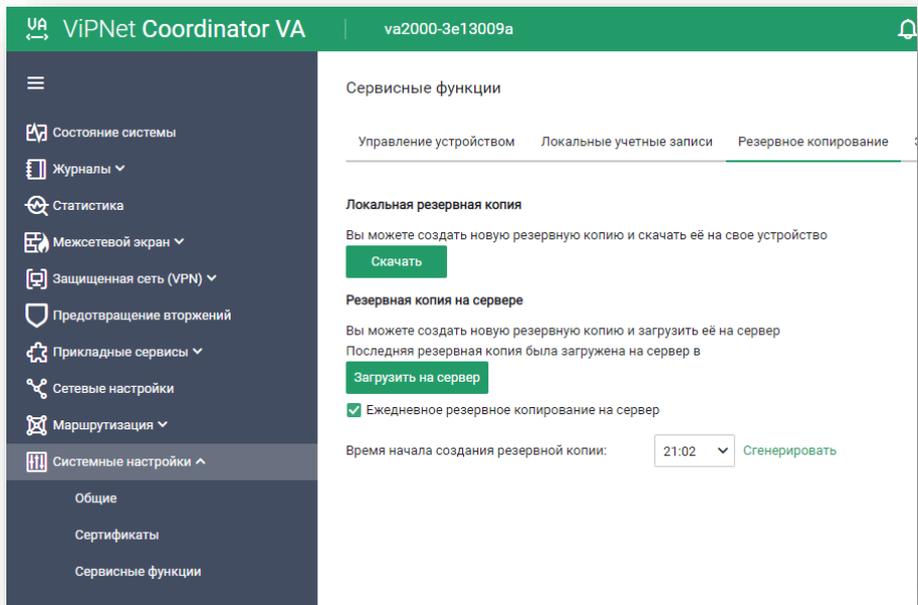
- Администратор
- Пользователь (Аудитор)

+

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

Next-Generation Firewall

Based

Advanced

VPN

МЭ

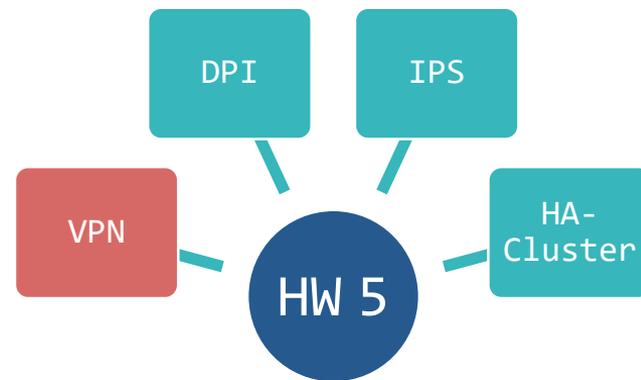
Прокси

IPS

DPI

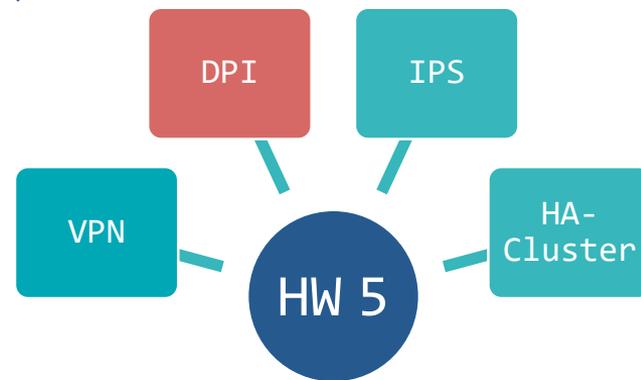
Лицензия может быть как бессрочной, так и срочной – подписка

- Технологический VPN не лицензируется
 - Связь с системой управления всегда активна
- Лицензия на VPN (активация, срок действия)
 - Туннелирование (L3/L2)
 - Кол-во туннелей не ограничиваем
 - Регистрация ViPNet клиентов



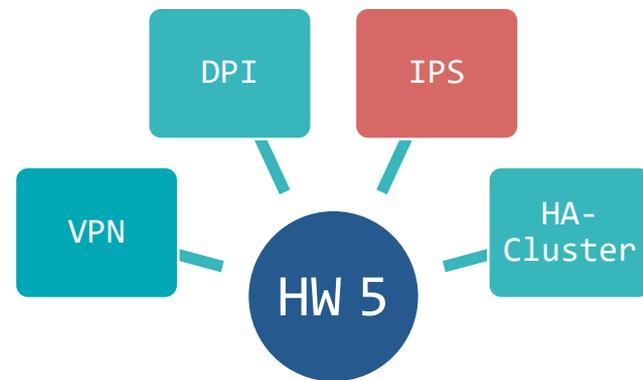
Межсетевой экран

- Межсетевой экран (SPI) не лицензируется (всегда активирован)
- Лицензия на модуль контроля приложений (DPI)
 - Активация, срок действия
- Встроенный прокси-сервер не лицензируем



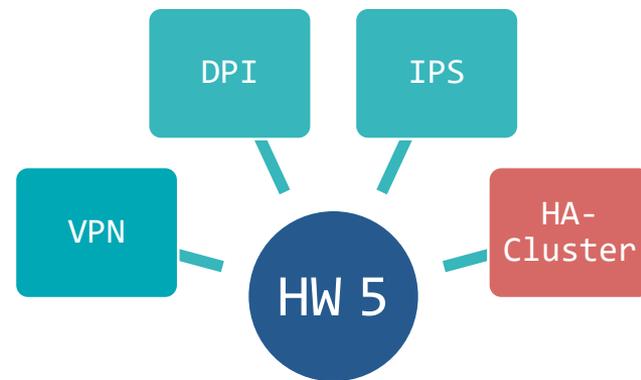
Предотвращение вторжений (IPS)

- Лицензия на модуль IPS
 - Активация
 - Срок действия
- Подписка на обновления БРП
 - Срок действия



HA-Cluster и ICAP-сервер

- Лицензируем на кластер для всех исполнений (HW и VA)
- Внешние подключения по ICAP не лицензируются:
 - Антивирусы
 - Песочницы
 - DLP



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

VIPNet Coordinator VA 5

Поддерживаемые гипервизоры:

- KVM, QEMU-KVM и Libvirt
- VMware ESXi 6.7, 7.0
- VMware Workstation 15.x, 16.x
- Microsoft Hyper-V Server 2016/2019
- Oracle VM Server 3.4
- Oracle VM VirtualBox 6.1.3



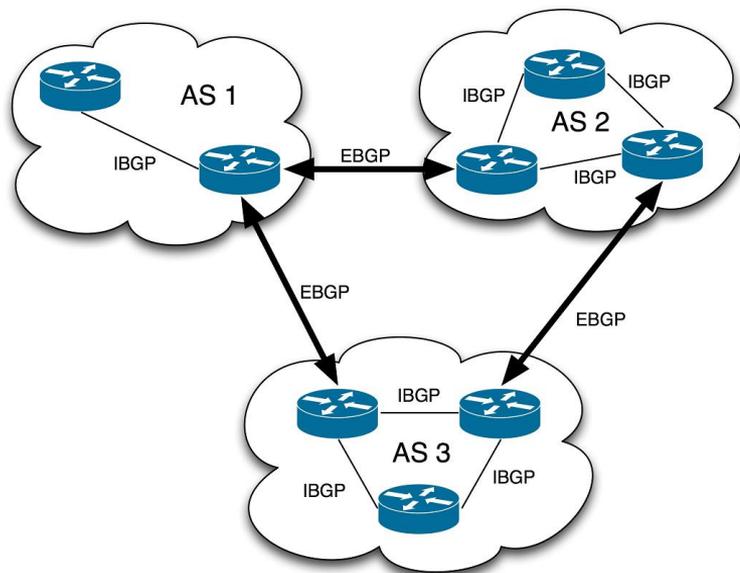
ViPNet Coordinator HW 5.3.2

- Поддержка протокола BGP
- Счетчики срабатывания правил МЭ
- Выборочное логирование правил МЭ
- Серийный номер аппаратной платформы
- Визуализация состояния сетевых интерфейсов
- Расширение возможностей агрегированного интерфейса
- Трансляция адреса источника в адрес из другой сети



Актуальный релиз

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)

Счетчики срабатывания правил МЭ

ViPNet Coordinator VA

va1000-3f7a0518

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 ?

<input type="checkbox"/>	№	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
<input type="checkbox"/>	⚙️ Настраиваемые фильтры						
⋮	<input type="checkbox"/>	<input checked="" type="checkbox"/>	✗ ICMP redirect in	4000035	0	Вкл.	Все
⋮	<input type="checkbox"/>	<input checked="" type="checkbox"/>	✗ ICMP redirect out	4000036	0	Вкл.	Мой узел ViPNet
⋮	<input type="checkbox"/>	<input checked="" type="checkbox"/>	✓ Allow ICMP Ping in	4000037	5	Выкл.	Все
⋮	<input type="checkbox"/>	<input checked="" type="checkbox"/>	✓ Allow ICMP Ping out	4000038	0	Выкл.	Мой узел ViPNet

Выборочное логирование правил МЭ

Параметры сетевого фильтра ✕

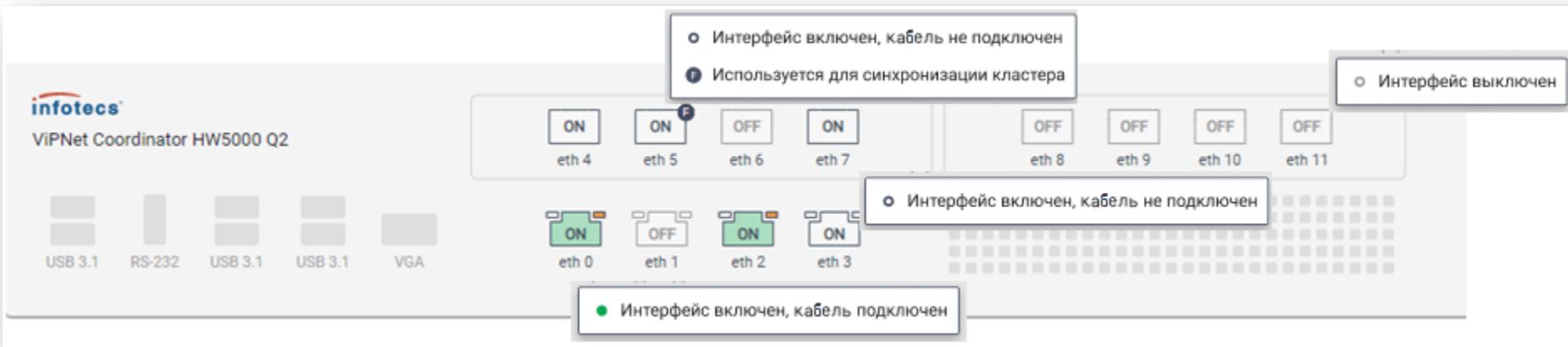
Название:

Состояние: Включено

Действие:

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

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

Планы развития

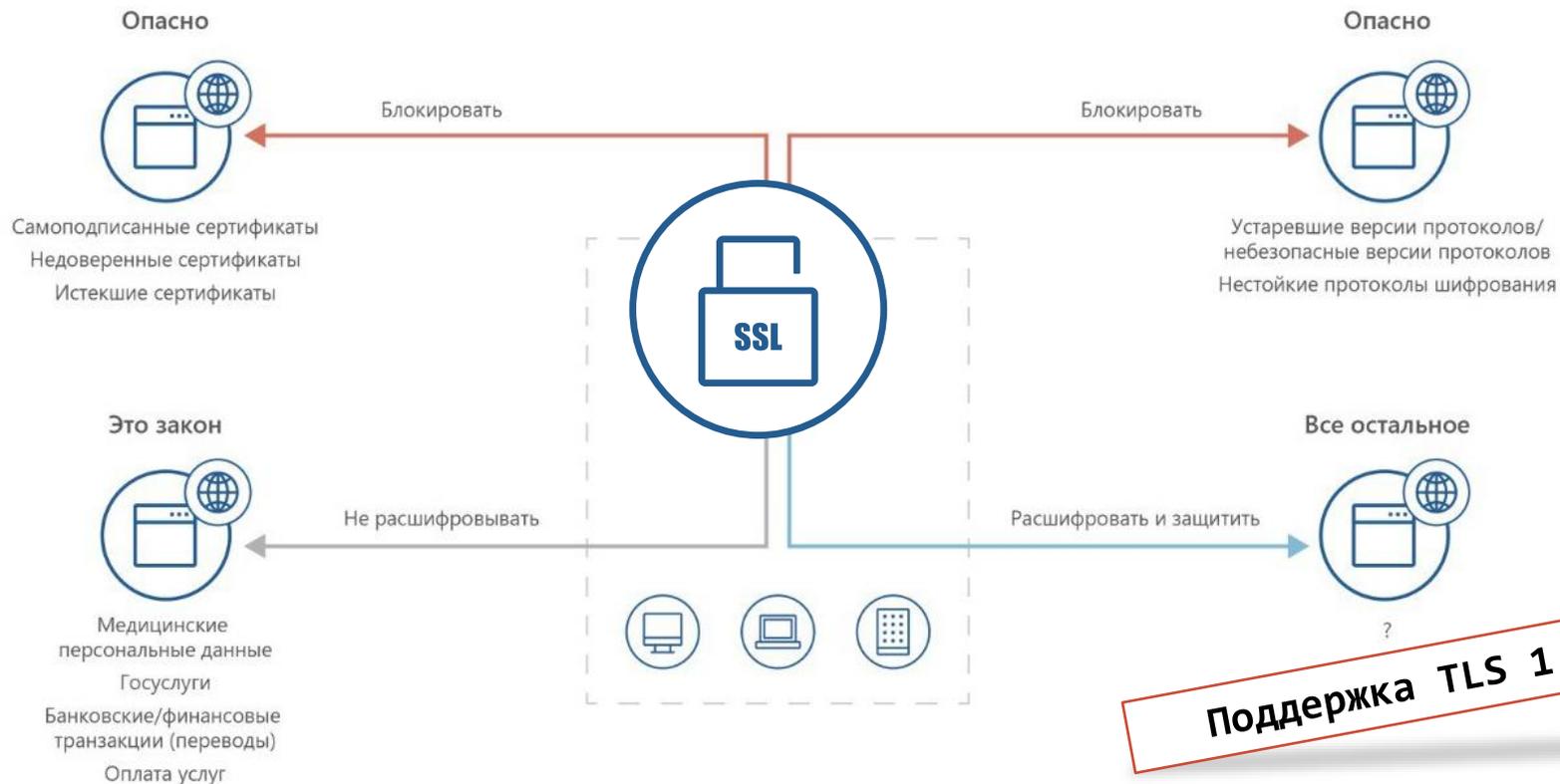
VIPNet Coordinator HW 5.4/5.5

- 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

SSL/TLS-инспекция



Поддержка TLS 1.3

URL-фильтрация

~85 млн. веб-ресурсов

80 категорий

+15% ежемесячный
прирост базы



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

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

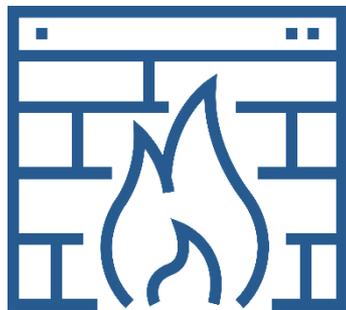
Импортировать

Всего: 33

<input type="checkbox"/> Имя URL-категории	Состав	Описание
<input type="checkbox"/> 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
Плагии и рефераты	1233 веб-ресурса	Архивы рефератов, ответов на вопросы ЕГЭ и
Заякорившие сайты	8916 веб-ресурсов	Панковки

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»)



Блокировка по GEO-IP



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](#)

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-Auth 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)

Обнаружение вредоносного ПО



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

Локальные учетные записи

+ новая роль «Сетевой администратор»

ViPNet Coordinator HW | GeneralAdmin 99+

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 ...	[] []
● Kononov.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			[] []

Настройки сессий

Мониторинг сессий пользователей

ViPNet Coordinator HW

GeneralAdmin | 99+ | i

Настройки сессий

Учётные записи

Локальные учётные записи Сессии

Поиск



<input type="checkbox"/>	Подключение	Дата и время авторизации	Длительность сессии	
<input type="checkbox"/>	Superadmin – Суперадминистратор (Вы) Завершить все сессии, кроме текущей			
<input type="checkbox"/>	tty1 (CLI)	11.06.2020 16:41:42	● 00:12:55	×
<input type="checkbox"/>	192.168.1.81 (Web)	11.06.2020 16:41:42	● 00:12:55	×
<input type="checkbox"/>	Admin – Администратор Завершить все сессии			
<input type="checkbox"/>	ssh: 192.168.1.12 (CLI)	11.06.2020 16:41:42	● 00:12:55	×
<input type="checkbox"/>	192.168.1.86 (Web)	11.06.2020 16:41:42	● 00:12:55	×
<input type="checkbox"/>	Auditor – Аудитор Завершить все сессии			
<input type="checkbox"/>	ssh: 192.168.1.32 (CLI)	11.06.2020 16:41:42	● 00:12:55	×
<input type="checkbox"/>	192.168.1.81 (Web)	11.06.2020 16:41:42	● 00:12:55	×

А что с ViPNet Coordinator HW 4?

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



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

- VPN - 250 Мбит/с
- FW - 700 Мбит/с

HW10 F1



- 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

техно infotecs
2024 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363