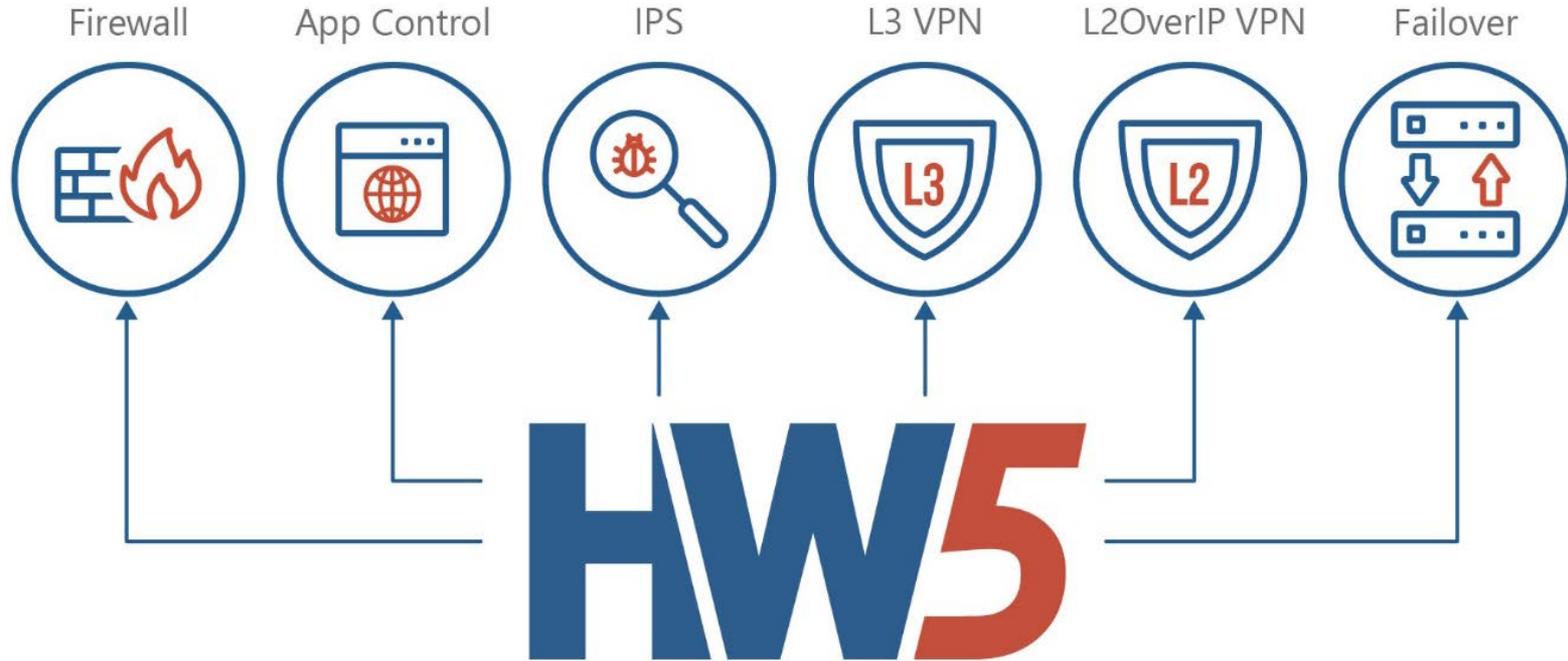




VIPNet Coordinator NW 5 – новое поколение шлюзов безопасности

Виталий Беличко
Ведущий менеджер продуктов

ViPNet Coordinator HW 5



Типовая схема применения HW 5

Центральный офис

Удаленные пользователи



Требования по сертификации

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса

ФСТЭК России

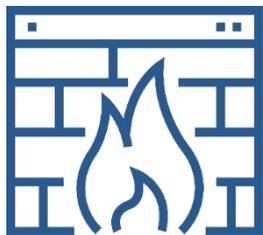
- Межсетевой экран тип «А» и тип «Б» 4 класса
- COB уровня сети 4 класса
- 4-й уровень доверия средств защиты информации
- Многофункциональный межсетевой экран уровня сети **NEW**

Минцифры России

- В реестре российского ПО



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 shows a list of rules. A modal window titled "Заблокировано IPS" (Blocked by IPS) is open, providing details for a specific event.

ViPNet Coordinator VA

Предотвращение вторжений

Поиск правил...

Блокирующие X

- Правило предотвращения
- "ET EXPLOIT Quanta LTE Router UDP I
- "ET EXPLOIT Serialized Java Object G
- "ET EXPLOIT Joomla RCE (JDatabase
- "AM Exploit Disk Sorter Enterprise 9.1
- "AM Exploit Weblogic Remote Code E
- "AM Exploit rConfig v3.9.2 unauthentic
- "AM EXPLOIT Unauthenticated XSS S
- "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	Свойства IP-пакета
Правило: "AM WEB_CLIENT NETGEAR ProSafe Network Management System Arbitrary file download"	Источник: 66.254.33.10 : 59418
Группа: web_client	Назначение: 192.168.1.200 : 80
Класс правила: web-application-attack	Транспортный протокол: 6-TCP
Идентификатор: 1.3001501.12	Сетевой интерфейс: eth2
Результат анализа	Направление: [← Входящий
Пользователь сети: Нет данных	Тип: Открытый
Приложение: unknown	Тип адреса: Одноадресный
Прикладной протокол: HTTP	Трансляция: Нетранслированный
Агрегация пакетов за интервал	Ethernet-протокол: 800h
Начало интервала: 16 Авг 2021, 17:03:16	
Конец интервала: 16 Авг 2021, 17:03:16	
Количество пакетов: 1	
Размер: 366 байт	

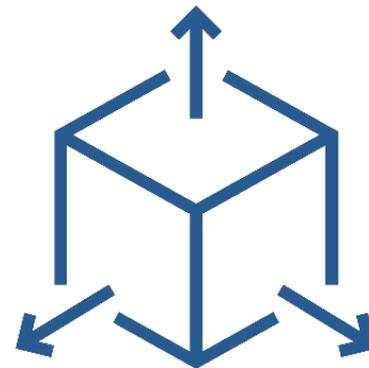
Вкл Блокировать

Заккрыть

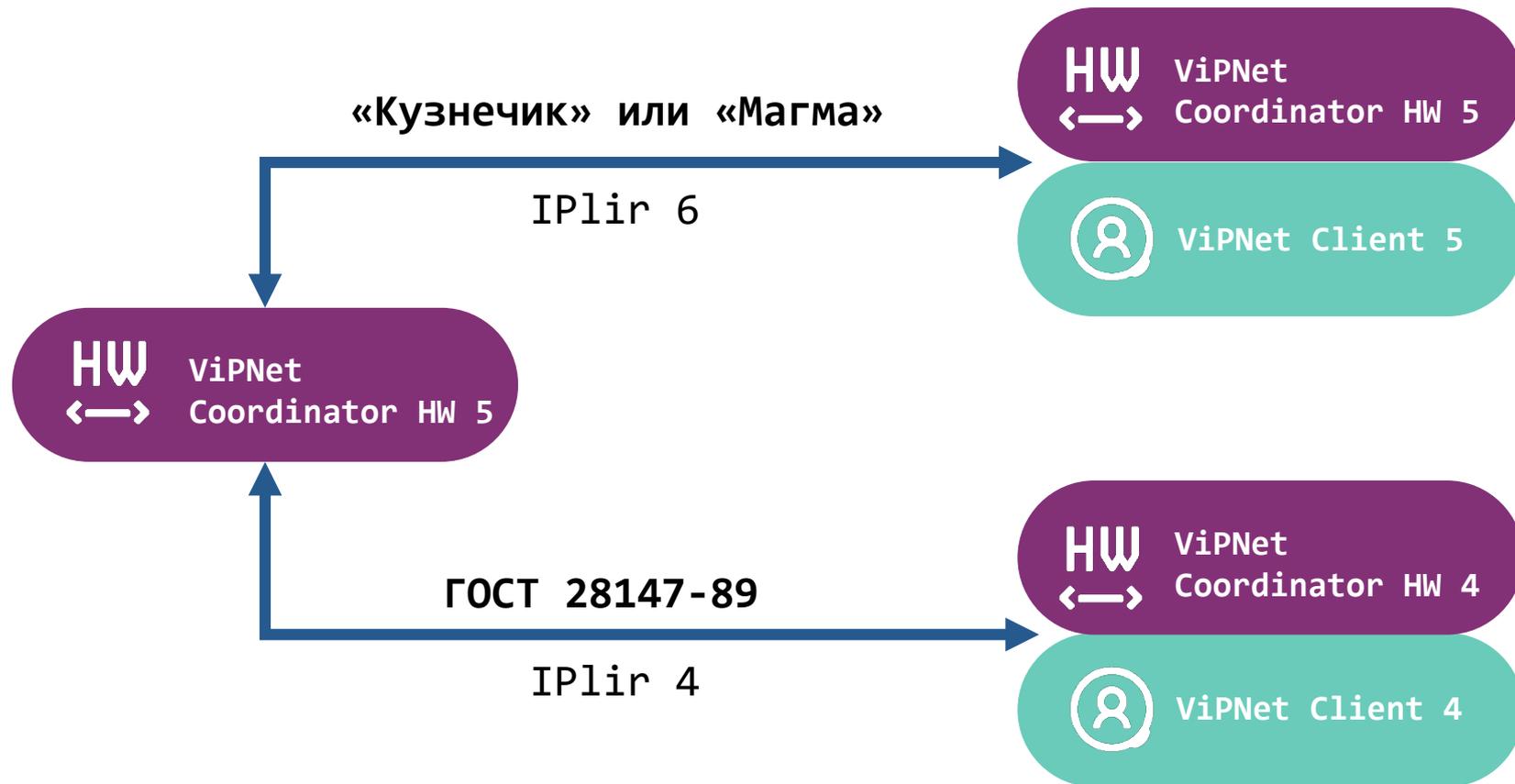
Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- IPsec 6 – протокол безопасности сетевого уровня

TK 26 P 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



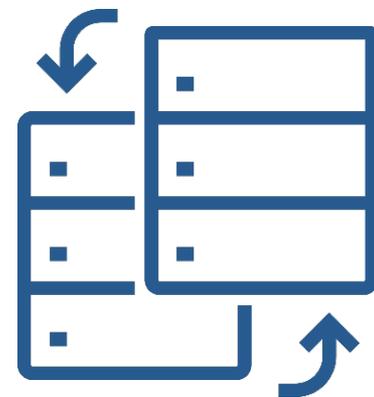
Виртуальный MAC-адрес для кластера



Синхронизация времени пассивного узла кластера



Минимальное время переключения кластера сократилось до 1 секунды



Новая система управления

VIPNet Prime

Ядро

Ролевая модель
Лицензирование
Управление ПО

VPN

Управление
связями,
ключами

PMM

Управление
политиками
безопасности

NVS

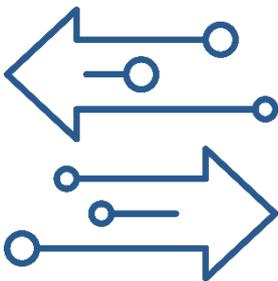
Мониторинг
состояния
узлов

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:

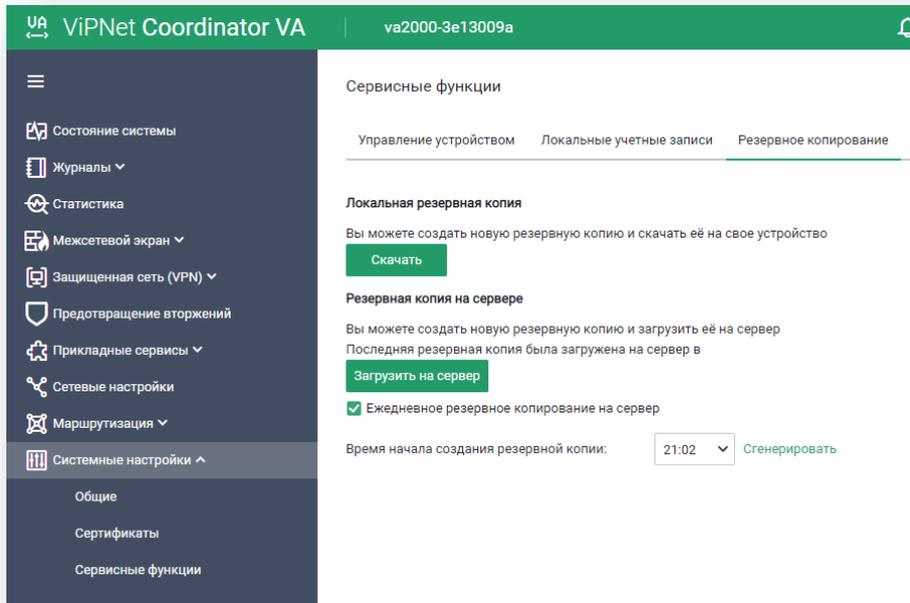
- Администратор
- Пользователь (Аудитор)

+

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

Схема лицензирования

Advanced (NGFW)

Base



VPN

МЭ

Прокси

DPI

IPS

Лицензия может быть как бессрочной, так и срочной – подписка



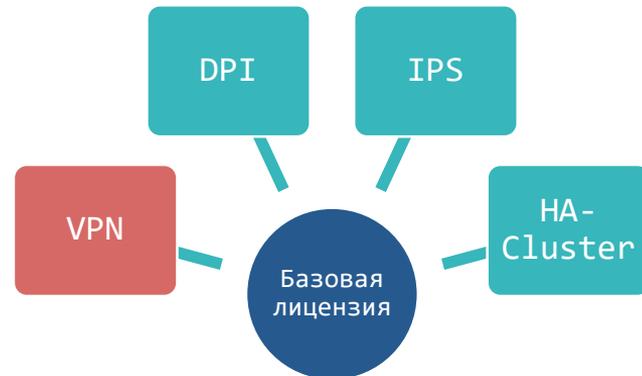
Технологический VPN не лицензируется

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)

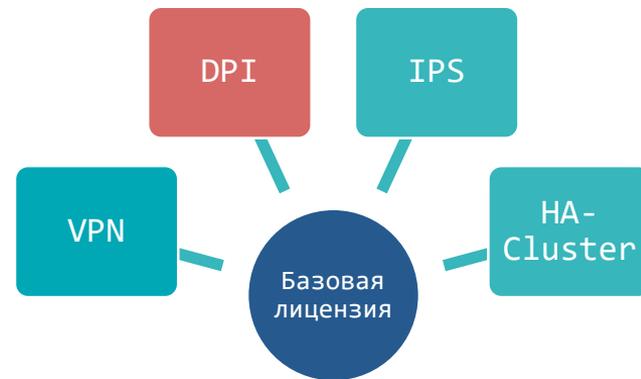


Лицензия на модуль контроля приложений (DPI)

Активация, срок действия



Встроенный прокси-сервер не лицензируем



Предотвращение вторжений (IPS)



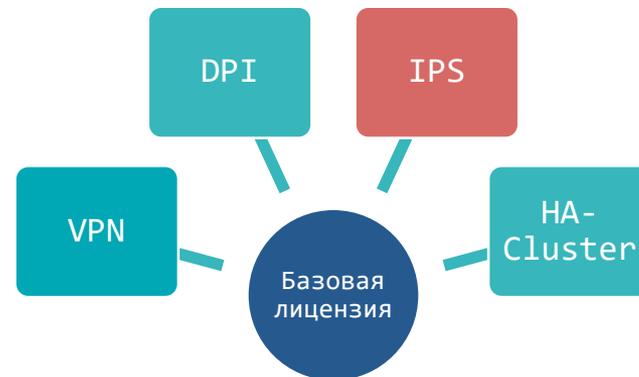
Лицензия на модуль IPS

- Активация
- Срок действия



Подписка на обновления БРП

Срок действия



HA-Cluster, Antivirus, ICAP

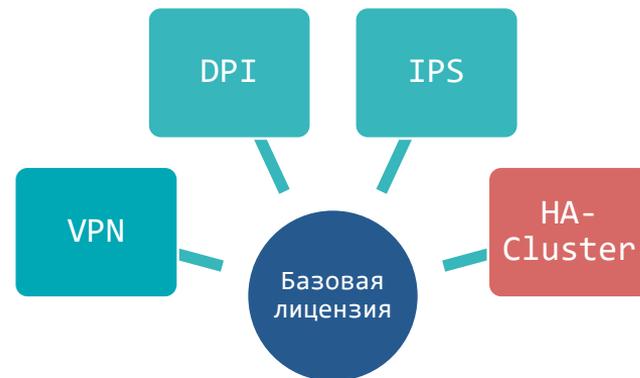


Лицензируем на кластер для всех исполнений (HW и VA)



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



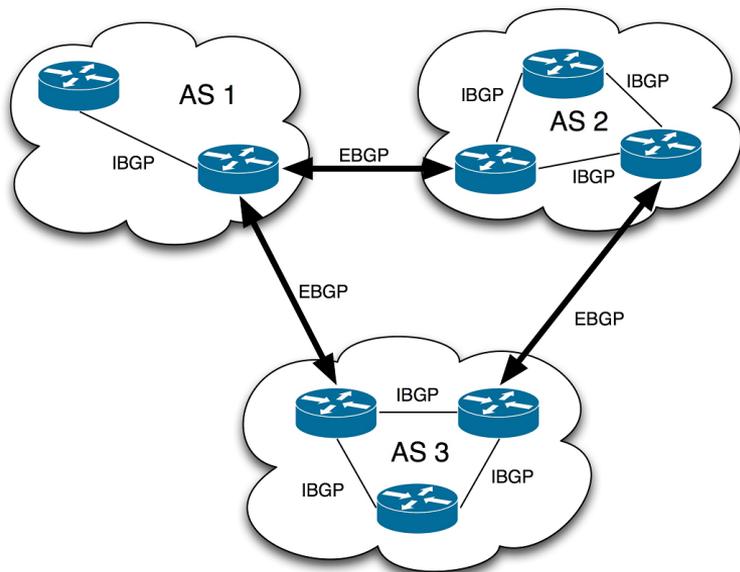
ViPNet Coordinator HW 5.3.1

- Поддержка протокола BGP
- Счетчики срабатывания правил МЭ
- Выборочное логирование правил МЭ
- Серийный номер аппаратной платформы
- Визуализация состояния сетевых интерфейсов
- Расширение возможностей агрегированного интерфейса



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



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



<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						
	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

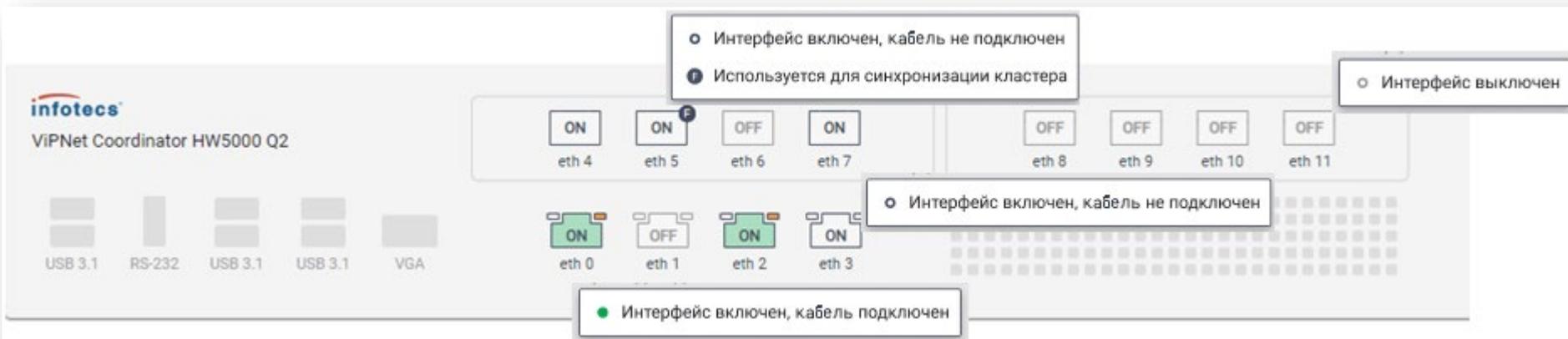
Действие: Блокировать трафик

Пропускать трафик

Отклонять трафик с ответом:

Регистрировать IP-пакеты

Визуализация сетевых интерфейсов



Серийный номер платформы

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

```
kb100-3db7000a# version
Product: ViPNet Coordinator KB
Platform: KB100 N1
Serial number: 123-45678
Software version: 4.3.3-154
DNSD version: 2.0.0, build number: 16
DNSD serial number: 010721001537
```

ViPNet Coordinator KB

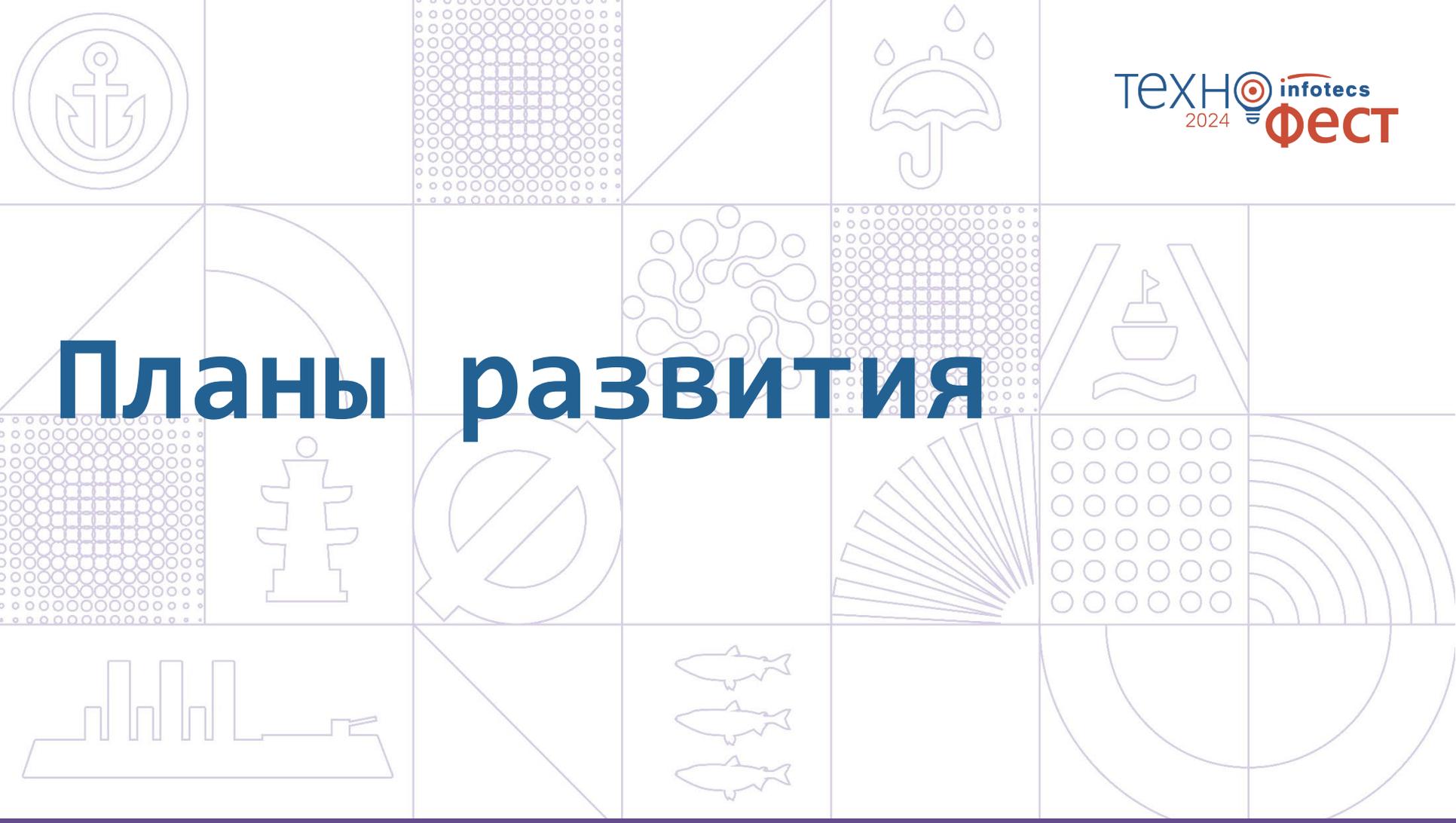
Основное Поддержка

Платформа:	KB100 N1
Продукт:	ViPNet Coordinator KB
Серийный номер:	123-45678
Версия ПО:	4.3.3-55

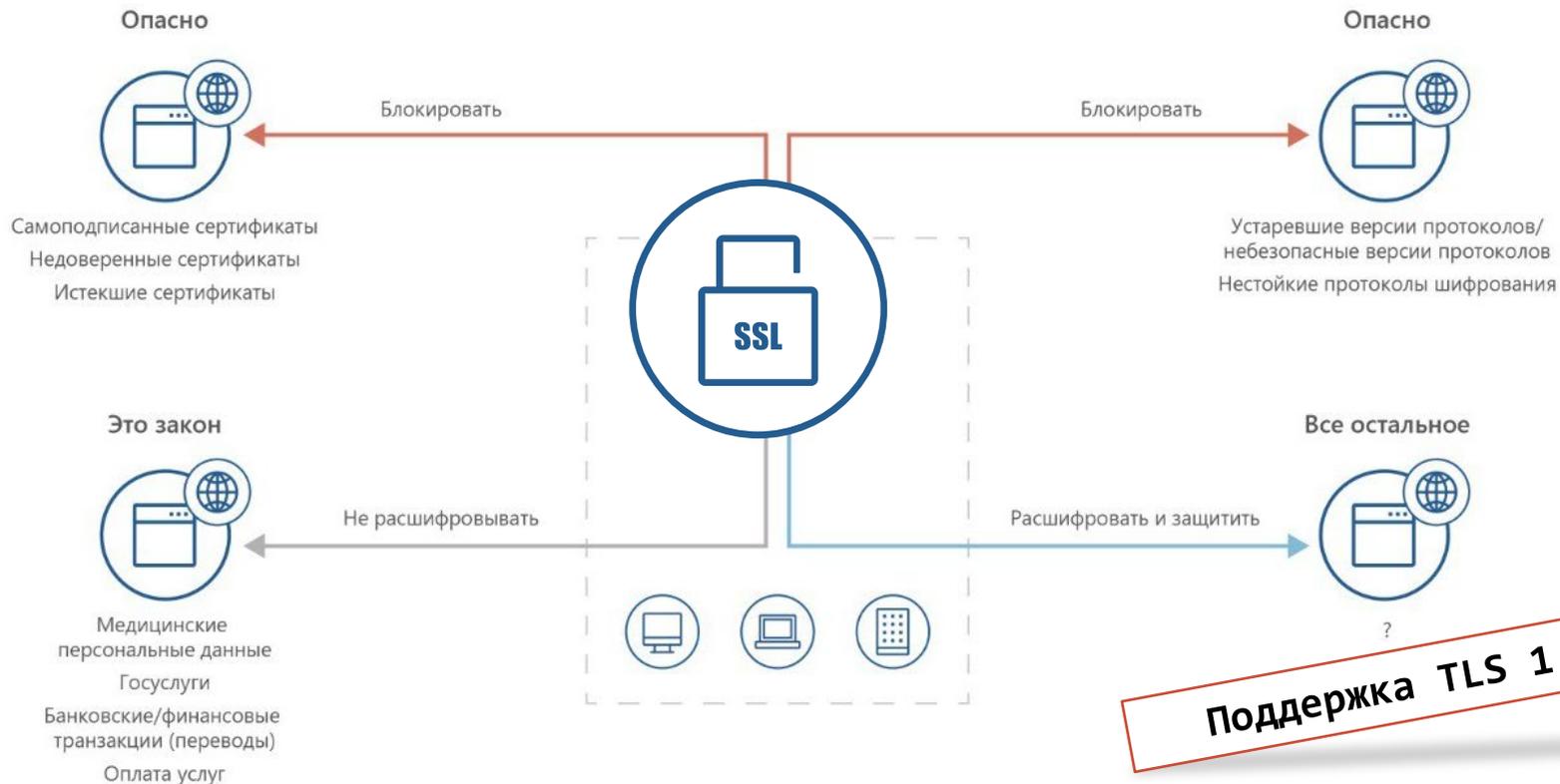
Модуль DNSD

Версия ПО:	2.0.0-16
Серийный номер:	010721001537

Планы развития



SSL/TLS-инспекция



URL-фильтрация

~85 млн веб-ресурсов

80 категорий

+15% ежемесячный
прирост базы



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

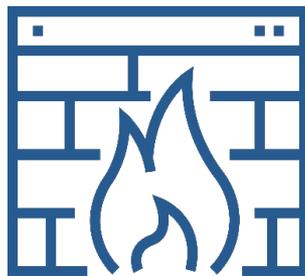
Блокировка по GEO-IP



Фильтрация трафика на основе данных о географической принадлежности отправителей



Использование доверенной базы геолокации IP-адресов на базе «Главного радиочастотного центра» (ФГУП «ГРЧЦ»)



Дружественные страны

Локальные учетные записи

ViPNet _BRAND_NAME_ | xfva-3306000c GeneralAdmin 99+ i

Учётные записи

Локальные учётные записи Активные сеансы

[+](#) Добавить

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

VIPNet Coordinator HW 5.4/5.5



SSL/TLS-инспекция



URL-фильтрация



Блокировка по GEO-IP



Встроенный антивирус



Проверка состояния связи между шлюзами



Локальные учетные записи + новая роль



Интеграция VIPNet SafeBoot

HW



В разработке

А что с ViPNet Coordinator HW 4?

HW100 Q1/Q2



- Аквариус T30 S100DC
- Intel Atom C3338 (2C/2T)
- 8 Gb RAM
- 4 Gb SSD / 240 Gb SSD
- 4x RJ-45
- 2x SFP
- 250 x 44 x 232 ШxВxГ (мм)
- VPN - 400 Мбит/с
- FW - 1400^{BOND} Мбит/с

HW10 F1



- NanoPi R5S
- Rockchip RK3568B2 (ARM)
- 4 GB RAM
- 32 Gb eMMC
- 3x RJ-45
- 95 x 30 x 68 ШxВxГ (мм)
- 260 г

- VPN – 25 Мбит/с
- FW – 100 Мбит/с

HW50 A1



- АТБ-АТОМ-1.3
 - Intel Atom E3845
 - RAM 4 Gb
 - SSD 8 Gb
 - 3x RJ-45
 - Wi-Fi / LTE (опционально)
 - 150 x 150 x 40 ШxВxГ(мм)
-
- VPN - 250 Мбит/с
 - FW - 700 Мбит/с

ТЕХНО infotecs 2024 Фест

Виталий Беличко
Ведущий менеджер продуктов

Подписывайтесь на наши соцсети

