

VIPNet Coordinator

HW 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

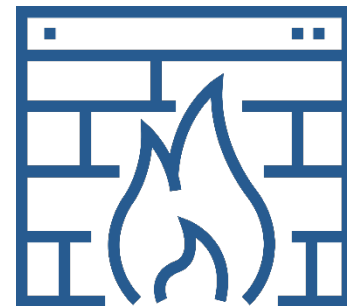


Минцифры России

- 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

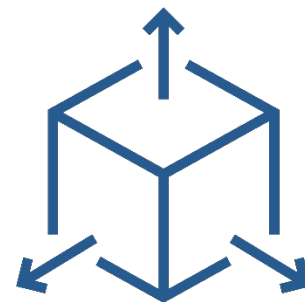
Обработка по правилам предотвращения вторжений	Свойства IP-пакета
Правило: "AM WEB_CLIENT NETGEAR ProSafe Network Management System Arbitrary file download"	Источник: 66.254.33.10 : 59418
Группа: web_client	Назначение: 192.168.1.200 : 80
Класс правила: web-application-attack	Транспортный протокол: 6-TCP
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

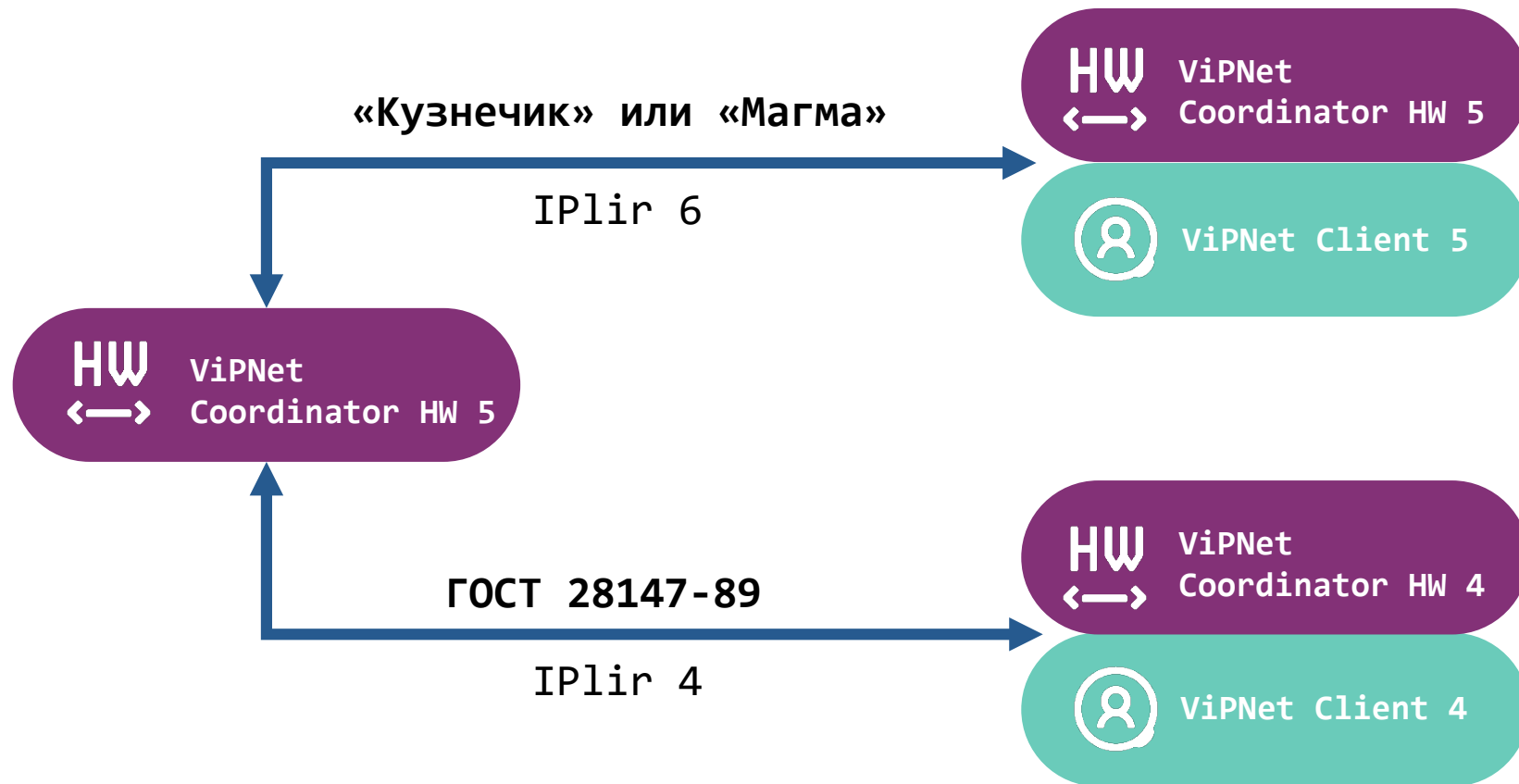
Заккрыть

Криптография (VPN)

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

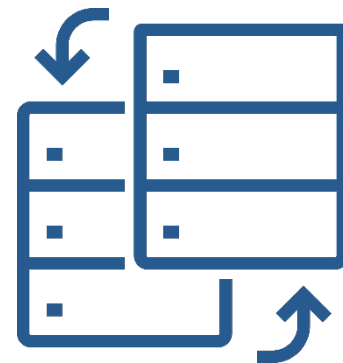


Обратная совместимость



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

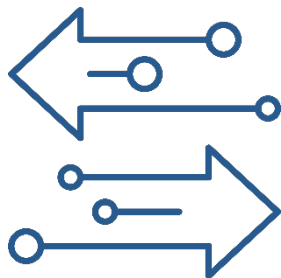
Мониторинг
состояния
узлов

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:

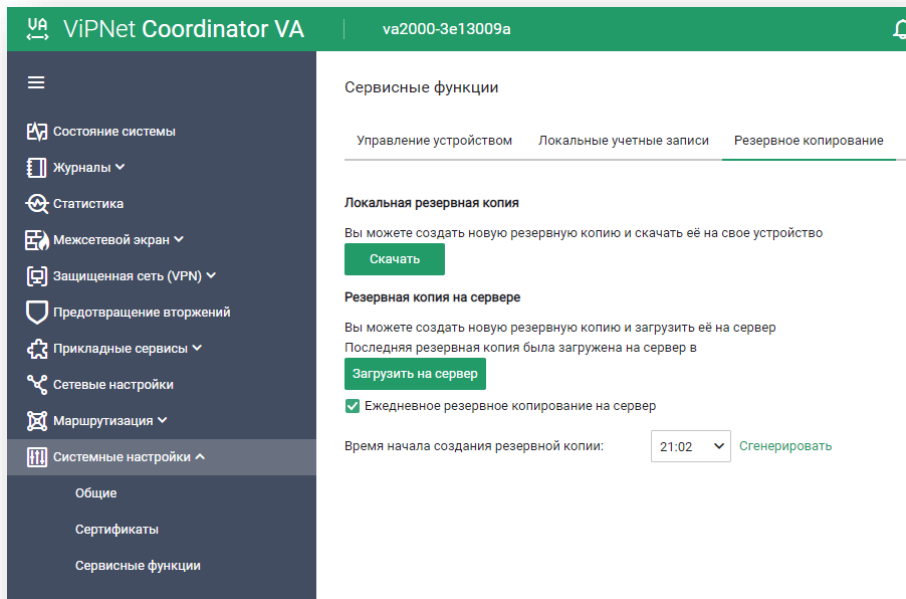
- Администратор
- Пользователь (Аудитор)

+

Централизованные учетные записи:

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

Резервное копирование



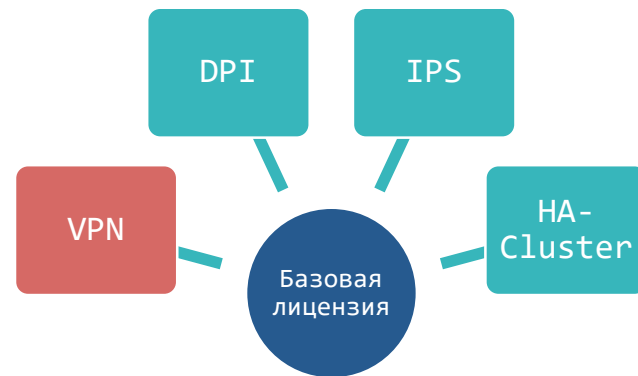
- Локальный экспорт на USB
- Удаленный экспорт через WebUI
- Выгрузка на сервер Prime

Новая схема лицензирования



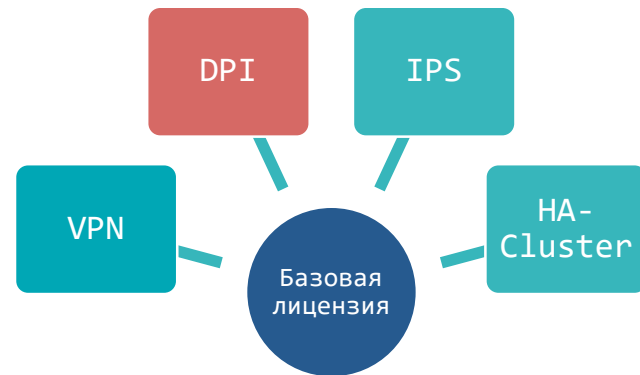
HW50/100/1000/2000/5000
VA100/500/1000/2000/5000

- 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



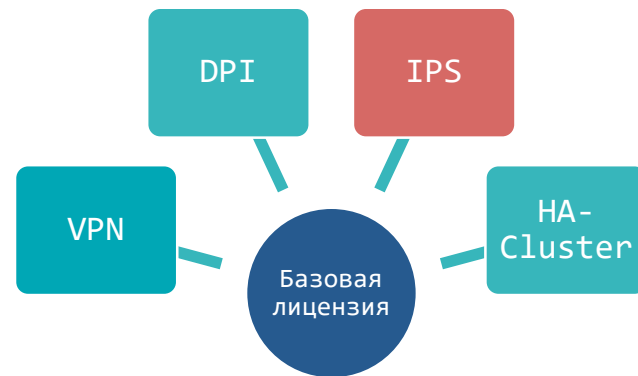
Межсетевой экран

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



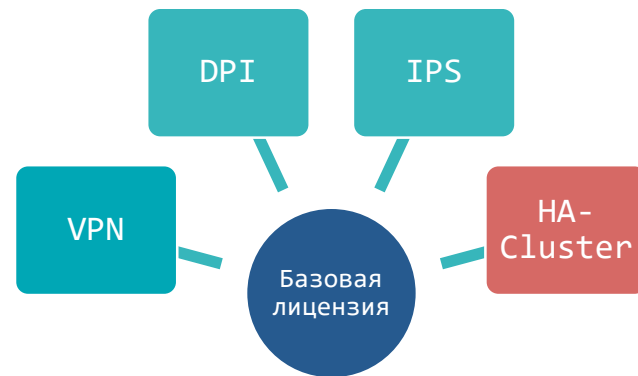
Предотвращение вторжений (IPS)

- 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/N6 *
- HW50 A1 NEW

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 VPN 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 5.3.0

- 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

Планы на 2024

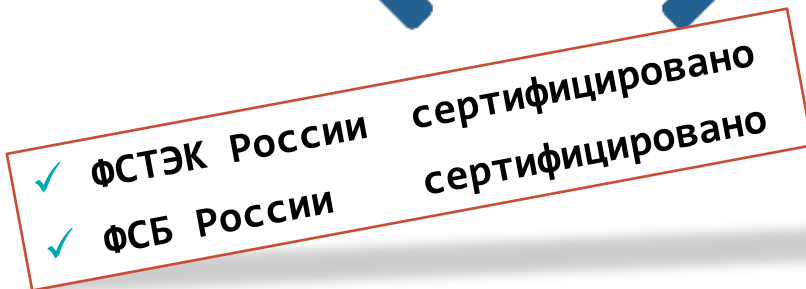
- Самостоятельная маркировка трафика (QoS)
- Поддержка Netflow
- Поддержка SSL-инспекции
- Переход на новый журнал пакетов
- Мониторинг открытых сессий МЭ
- Сопряжение с КПК и реализация ProtoQa



А что с ViPNet Coordinator HW 4?

VIPNet Coordinator HW 4.5.4

- Кластер высокой доступности
- Новые возможности мониторинга
- Повышение безопасности сетевых протоколов
- Новые сервисные функции
- Улучшения веб-интерфейса
- Поддержка новых платформ



HW100 Q1/Q2



- Аквариус Т30 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 eMCC
- 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

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363