

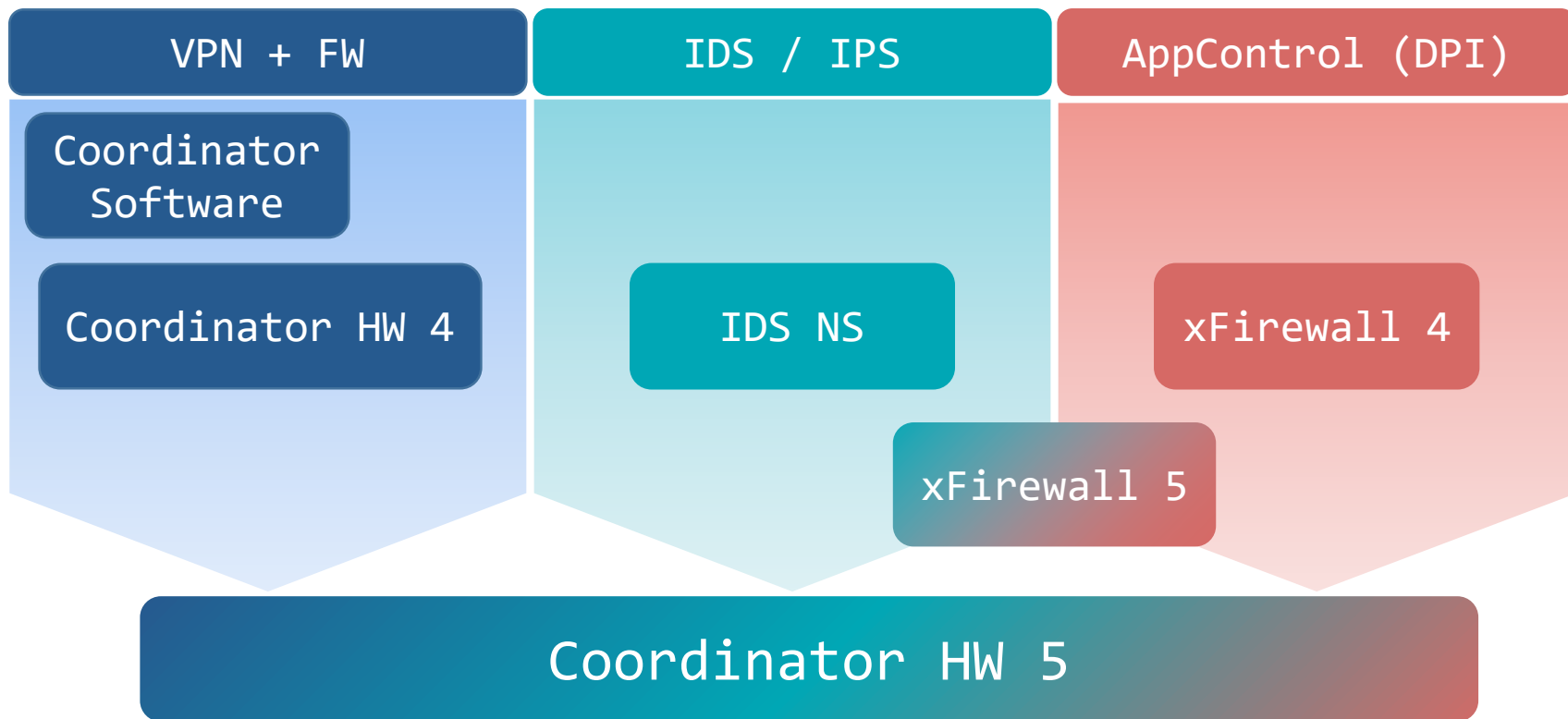
VIPNet Coordinator HW 5

Виталий Беличко

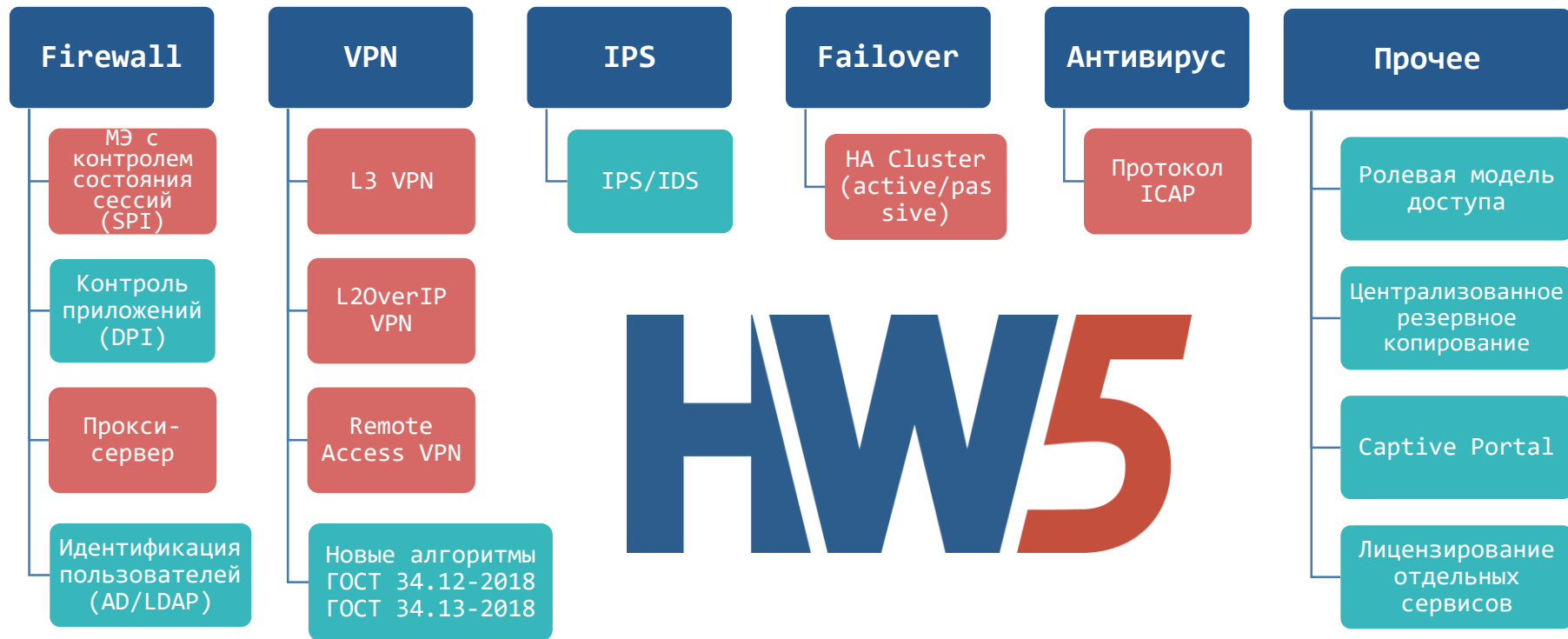
техно infotecs
2022 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Шлюзы безопасности ViPNet



ViPNet Coordinator HW 5



Сертификация

Требования по сертификации

ФСБ России

- СКЗИ класса КС1-КС3
- Межсетевой экран 4 класса
- СОА класса ВП

ФСТЭК России

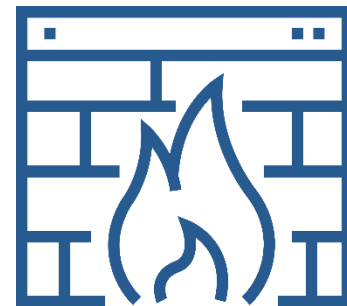
- Межсетевой экран тип «А» и тип «Б» 4 класса
- COB уровня сети 4 класса
- 4-й уровень доверия средств защиты информации



Межсетевое экранирование

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



Идентификация правил МЭ

| Событие | Фильтры и правила |
|------------------------------------|----------------------------------|
| 60 - Пропущен открытый локальны... | Allow Web Access |
| 60 - Пропущен открытый локальны... | Allow Web Access |
| 60 - Пропущен открытый локальны... | Allow Web Access |
| 60 - Пропущен открытый локальны... | Allow Web Access |

Параметры сетевого фильтра

Название:

Состояние: Включено

Действие: Блокировать трафик
 Пропускать трафик

✓ **Пропущено МЭ**
Код события 60 - Пропущен открытый локальный IP-пакет

Обработано фильтром межсетевого экрана

Имя фильтра: [Allow Web Access](#)

Тип фильтра: local

Агрегация пакетов за интервал

Начало интервала: 01 Июнь 2022, 16:13:17

Конец интервала: 01 Июнь 2022, 16:14:02

Количество пакетов: 2

Размер: 104 байт

Свойства IP-пакета

Источник: 192.168.25.166 : 8080

Назначение: 192.168.19.208 : 63163

Транспортный протокол: 6-TCP

Сетевой интерфейс: eth0

Направление: [→ Исходящий

Тип: Открытый

Тип адреса: Одноадресный

Трансляция: Нетранслированный

Ethernet-протокол: 800h

Закреть

Порт назначения недоступен

Добавить

Протоколы

Источники

Назначения

Расписания

Сохранить **Отмена**

Предотвращение вторжений (IDS/IPS)

Предотвращение вторжений

ViPNet Coordinator VA

Журнал регистрации IP-пакетов

Фильтр IP-пакетов ▼ Результат фильтрации в интервале с 01.07.20...

| Пользоват... | Приложение | Прикладной протокол |
|------------------|------------|---------------------|
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |
| ⊘ [← Нет данных] | Неизвестно | HTTP |

⊘ 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: unknowн

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

Закрыть

Показано 16 записей

| Размер | Событие | Фильтры и правила |
|--------|----------------------------|-------------------------|
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 0 | 67 - Отмечен IPS подис... | "FTPP FTP INVALID CMD" |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |
| 366 | 142 - Заблокирован IPS ... | "AM WEB_CLIENT NETGE... |

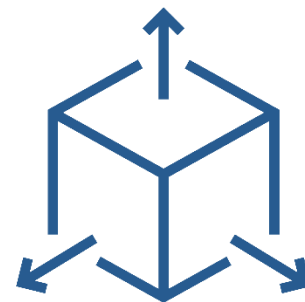
Вкл Блокировать

Криптография (VPN)

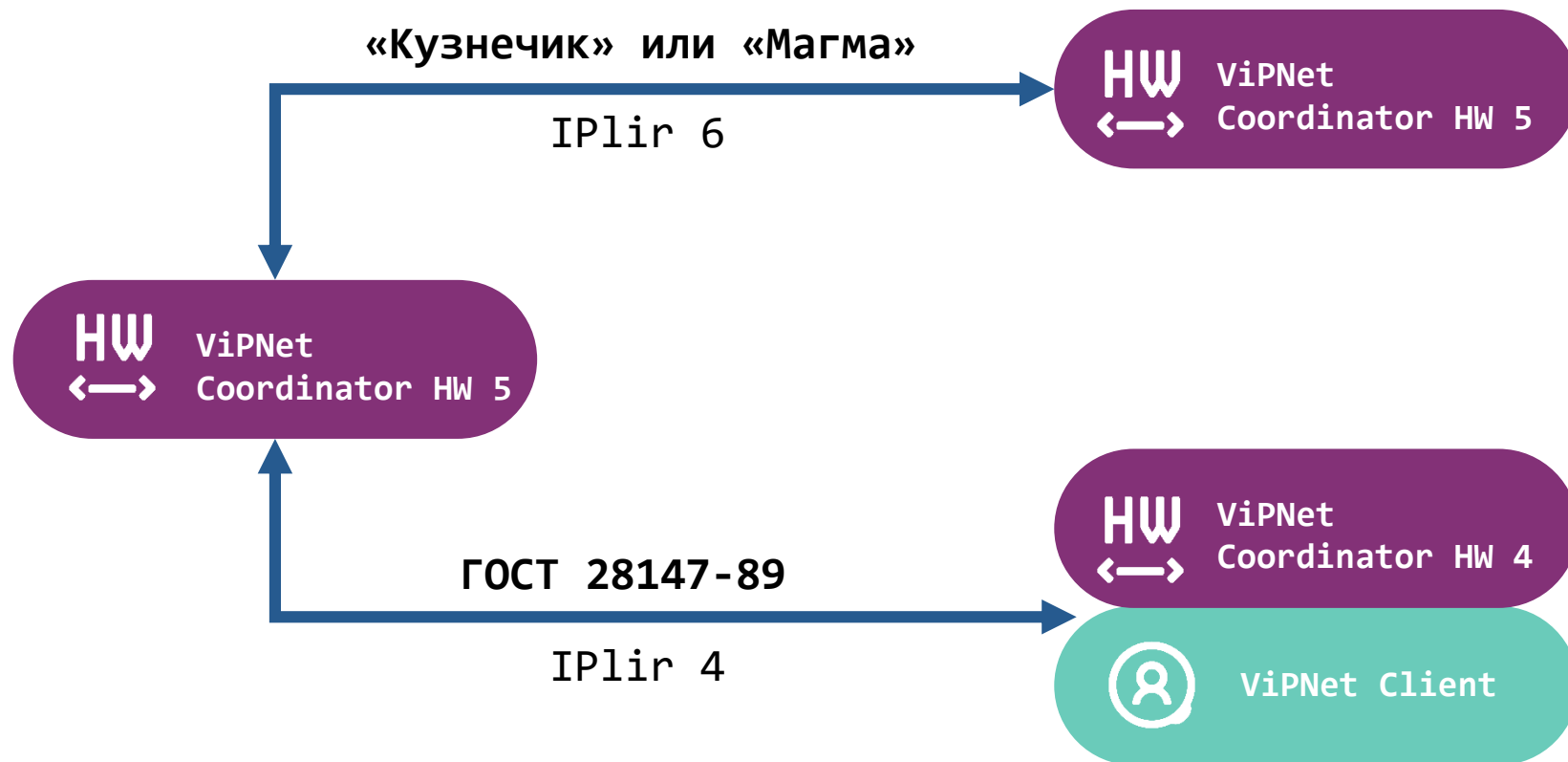
Криптография (VPN)

- «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»



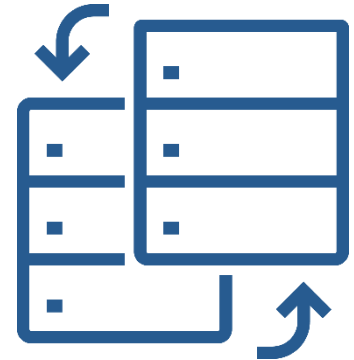
Обратная совместимость



Кластер высокой доступности (HA Cluster)

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**



Управление и мониторинг

Модули ViPNet Prime

ViPNet Prime

Ядро

Ролевая модель
Лицензирование
Управление ПО

VPN

Управление
связями,
ключами

PMM

Управление
политиками
безопасности

NVS

Мониторинг
состояния
узлов

Rollout
Center

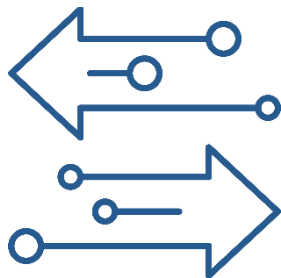
Первичная
инициализация
устройств

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)
- Интеграция с AD через Prime

Планы развития ролевой модели

Система

- Системные и сетевые настройки
- Прикладные сервисы

МЭ

- Управление фильтрами
- Задание правил трансляции

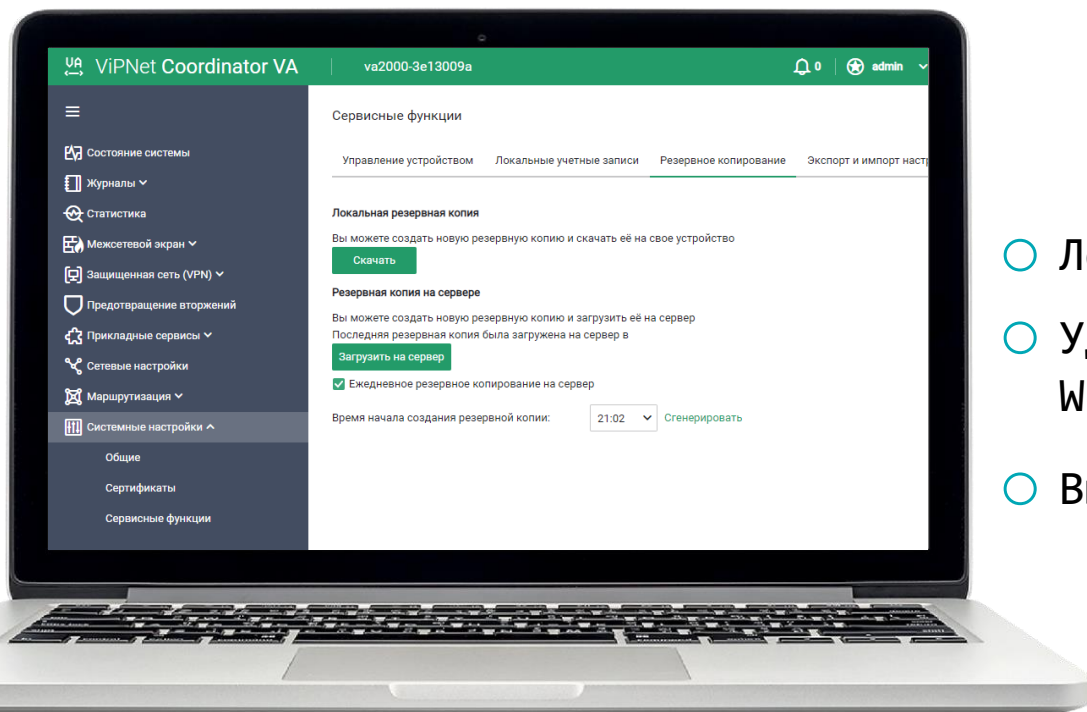
VPN

- Работа с ключевой информацией
- Управление VPN-сервисами

IPS

- Управление БРП
- Работа с событиями

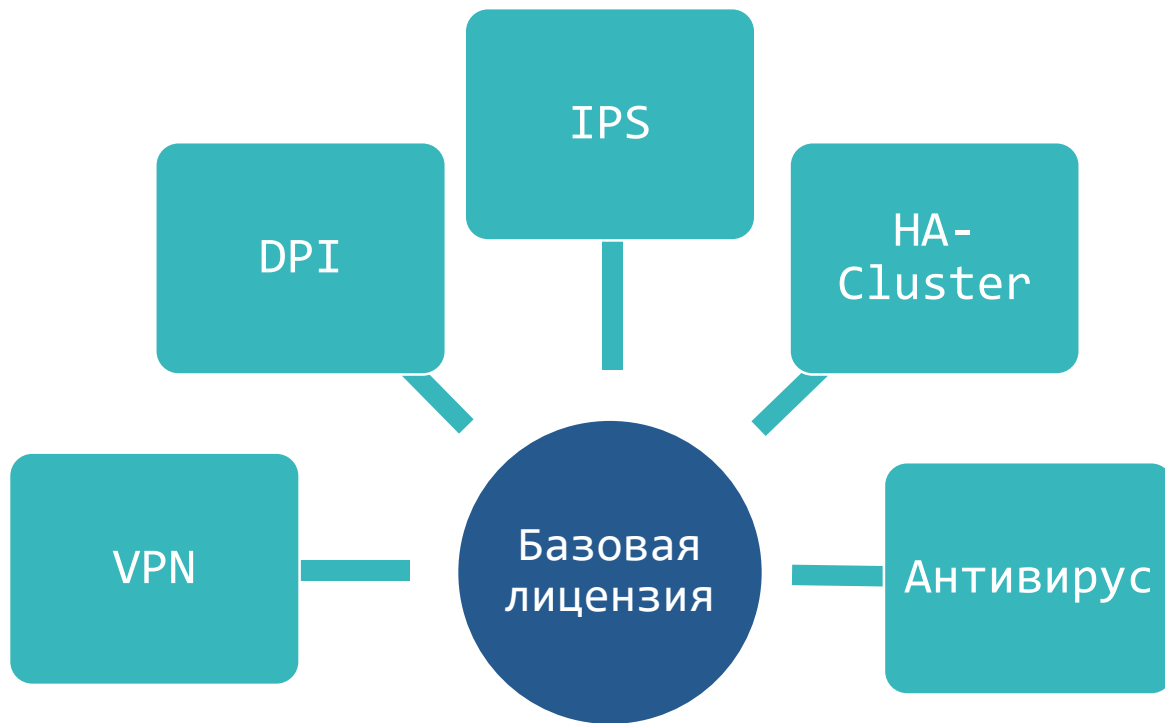
Резервное копирование



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

Лицензирование

Новая схема лицензирования



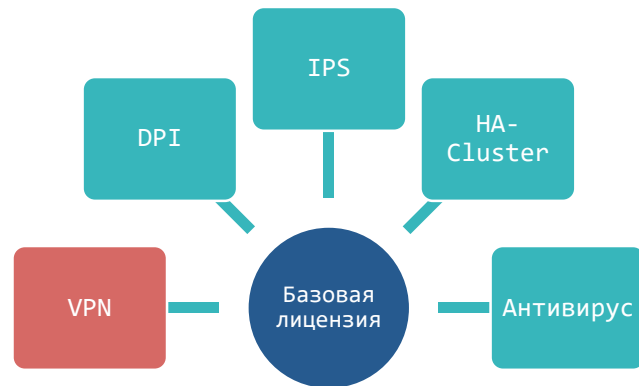
HW50/100/1000/2000/5000
VA100/500/1000/2000

○ Технологический VPN не лицензируется

- Связь с системой управления всегда активна

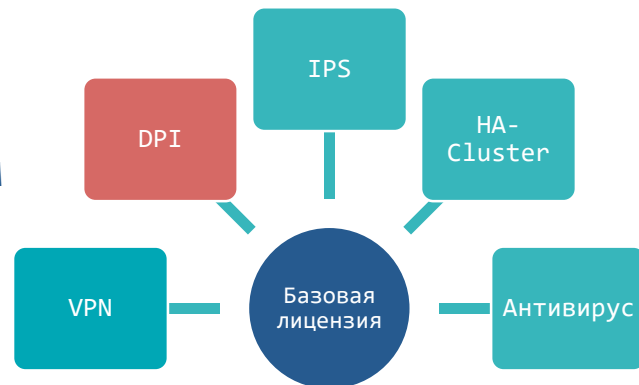
○ Лицензия на VPN (активация, срок действия)

- Туннелирование (L3/L2)
- Кол-во туннелей не ограничиваем
- Регистрация ViPNet клиентов



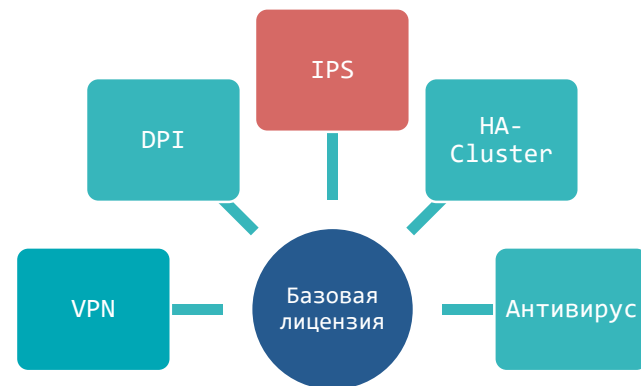
Межсетевой экран

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



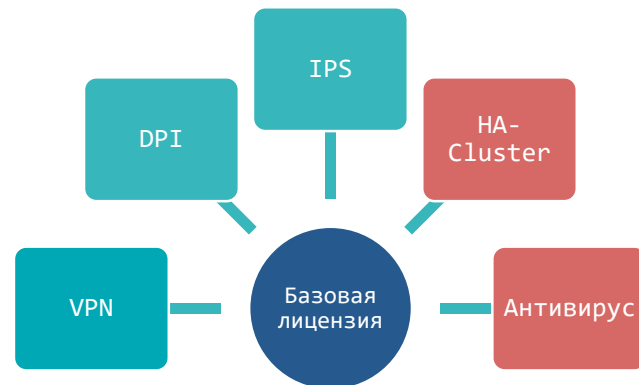
Предотвращение вторжений (IPS)

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



HA-Cluster и антивирус

- Лицензируем на кластер для всех исполнений (HW и VA)
- Подключение внешнего антивируса (ICAP) не лицензируется
- Встроенный антивирус*:
 - Заказчик самостоятельно приобретает лицензию на активацию и обновление



Исполнения

Характеристики старших платформ

| Исполнение | Платформа | Интерфейсы (медь) | Интерфейсы (оптика) | Блок питания |
|------------|-----------|-------------------|---------------------|--------------|
| HW1000 | HW1000 Q7 | 6x RJ45 | - | 1x 250 W |
| HW1000 C | HW1000 Q8 | 8x RJ45 | - | 1x 250 W |
| HW1000 D | HW1000 Q9 | 8x RJ45 | 4x SFP | 2x 300 W |
| HW2000 | HW2000 Q5 | 4x RJ45 | 4x SFP 4x SFP+ | 2x 300 W |
| HW5000 | HW5000 Q2 | 4x RJ45 | 8x SFP+ | 2x 300 W |

- Более производительные CPU
- Увеличен объем RAM (4/16/32/64 Gb)
- Увеличен объем SSD (4 Gb) и HDD (1/2 Tb)



Поддержка аппаратных платформ

ViPNet Coordinator HW50

- HW50 N1/N2/N3/N4/N6 ***
- HW50 A1 NEW

ViPNet Coordinator HW100

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

ViPNet Coordinator HW2000

- HW2000 Q4
- HW2000 Q5 NEW

ViPNet Coordinator HW1000

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

ViPNet Coordinator HW5000

- HW5000 Q1
- HW5000 Q2 NEW

*** - режим VPN only



VIPNet Coordinator VA

- KVM, QEMU-KVM и Libvirt
- VMware ESXi
- VMware Workstation
- Microsoft Hyper-V Server
- Oracle VM Server
- Oracle VM VirtualBox



Миграция

HW 4 -> HW 5

Миграция HW 4 -> HW 5

ViPNet Prime (чистая установка)

Создаем узел HW 5, настраиваем связи,
лицензии, формируем DS5

Снимаем VBE-файл от HW 4 (*если меняется
аппаратная платформа*)*

Локально обновляем ПО HW 4.5.2 до HW 5 с
удалением VPN конфигурации

Инициализируем DS5 (+VBE). Готово!

Импорт настроек из VBE файла

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](#) [Просмотр](#)

Сетевые настройки [Просмотр](#)

Таблицы и политики статической маршрутизации [Заменить](#) [Просмотр](#)

[Назад](#) [Далее](#) [Отмена](#)

```
Firewall rules
-----
Service Vpn Rules:
-----
Num  Name                               Option Schedule
Act  Protocol                            Source      -> 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
     to 2046                          @any
     @any
-----
2    Allow ViPNet base               Generated
pass services in                      @any      -> @local
     udp:
```

[Закрыть](#)

ТЕХНО infotecs
2022 ФЕСТ

Спасибо за внимание!

Беличко Виталий
Ведущий менеджер продукта
e-mail: Vitaly.Belichko@infotecs.ru

Информационный
партнер



Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363