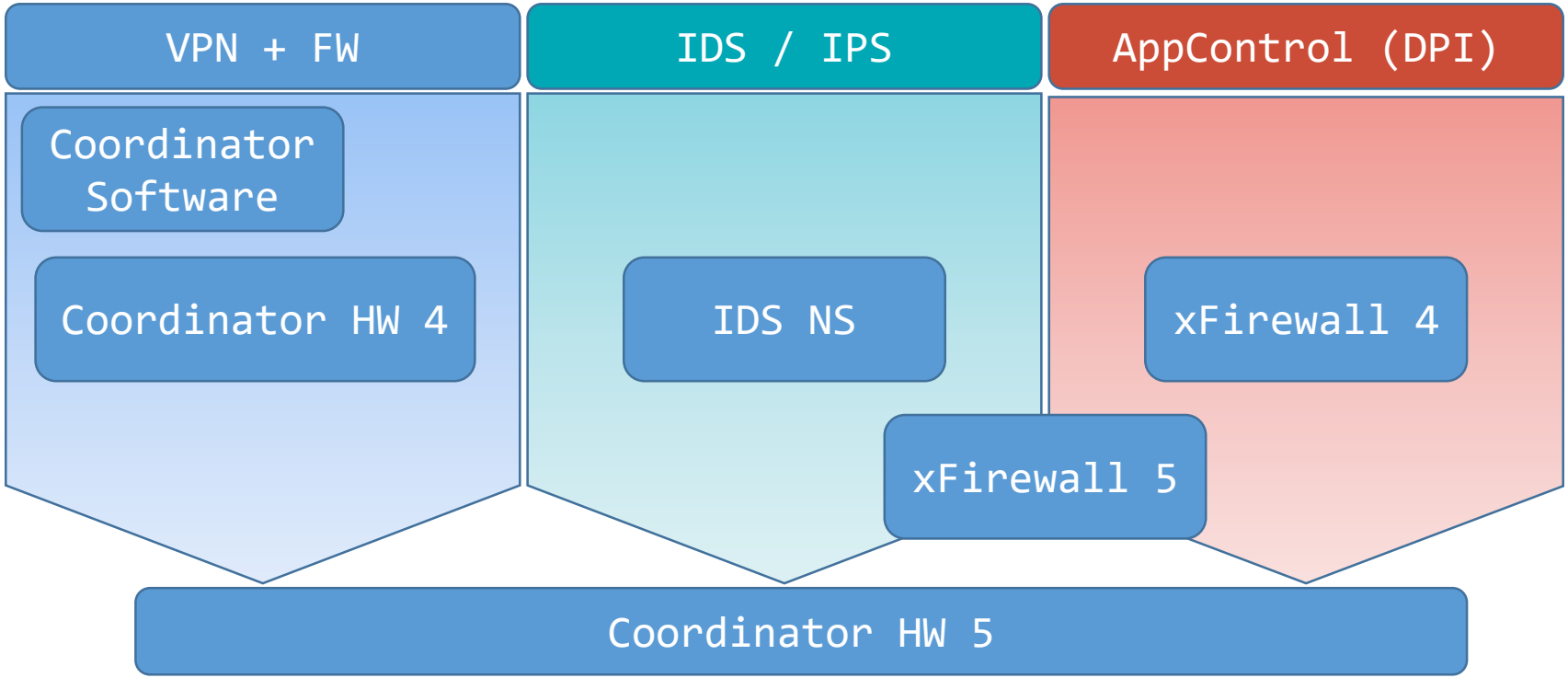
Информационная безопасность 2021..2022

Новое поколение шлюзов безопасности

Шлюзы безопасности ViPNet



ViPNet Coordinator HW 5

infotecs

Firewall
- МЭ с контролем состояния сессий (SPI)
- Контроль приложений (DPI)
- Прокси-сервер
- Идентификация пользователей (AD/LDAP)

VPN
- L3 VPN
- L2OverIP VPN
- Remote Access VPN
- Новые алгоритмы ГОСТ 34.12-2018 ГОСТ 34.13-2018

IPS
- IPS/IDS

Failover
- HA Cluster (active/passive)

Антивирус
- Любой внешний ICAP

Прочее
- Ролевая модель доступа
- Централизованное резервное копирование
- Captive Portal
- Лицензирование отдельных сервисов

HW5

Сертификация

Требования по сертификации

ФСБ России

- СКЗИ класса КС3
- СКЗИ класса КС1 (исполнение VA)
- Межсетевой экран 4 класса
- СОА класса ВП

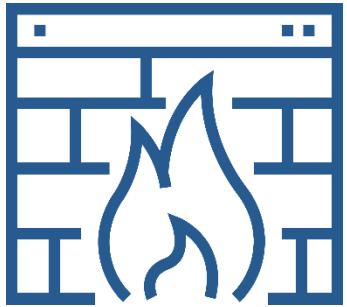
ФСТЭК России

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

Межсетевое экранирование

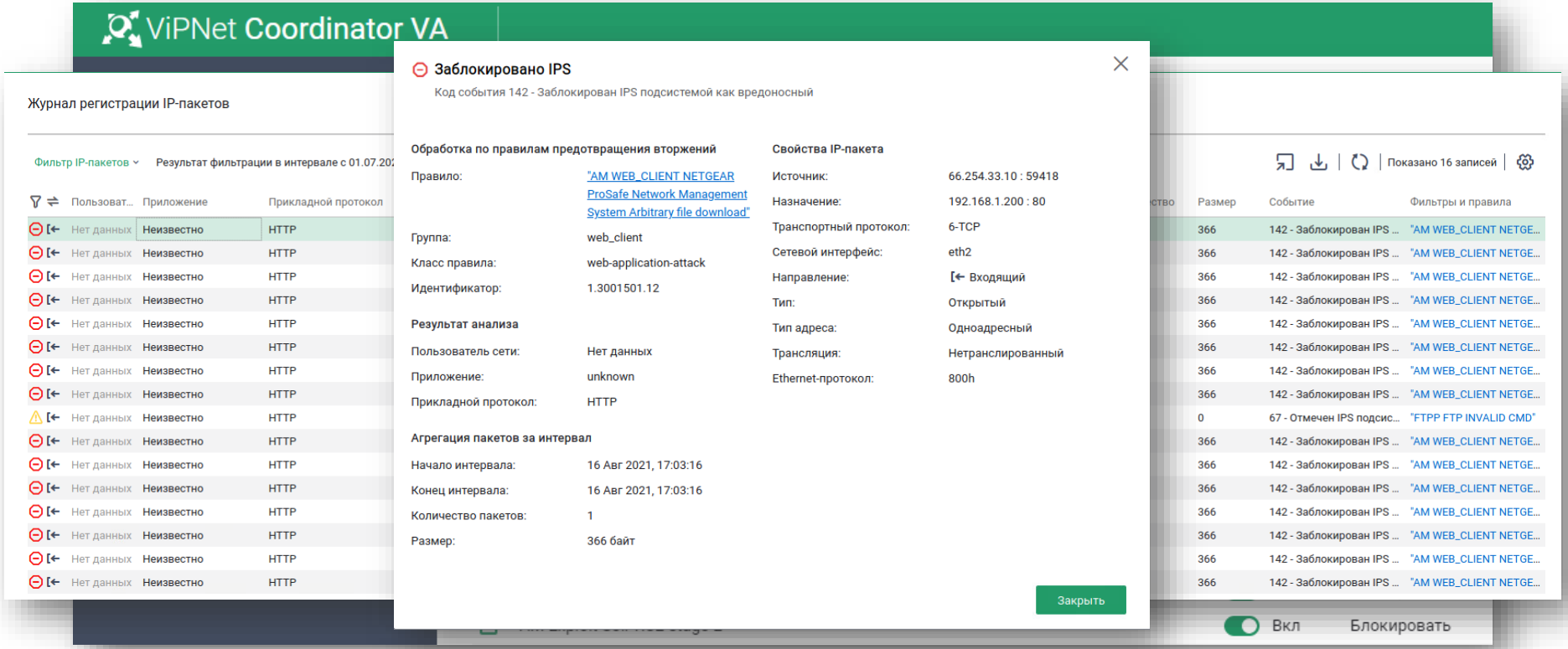
Межсетевое экранирование

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



Предотвращение вторжений (IDS/IPS)

Предотвращение вторжений

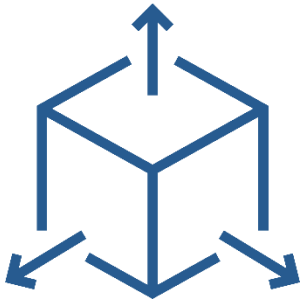


Криптография (VPN)

Криптография (VPN)

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

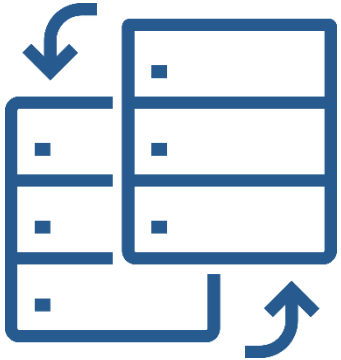
ТК 26 Р 1323565.1.034-2020 «Информационная технология. Криптографическая защита информации. Протокол безопасности сетевого уровня»



Кластер высокой доступности (HA Cluster)

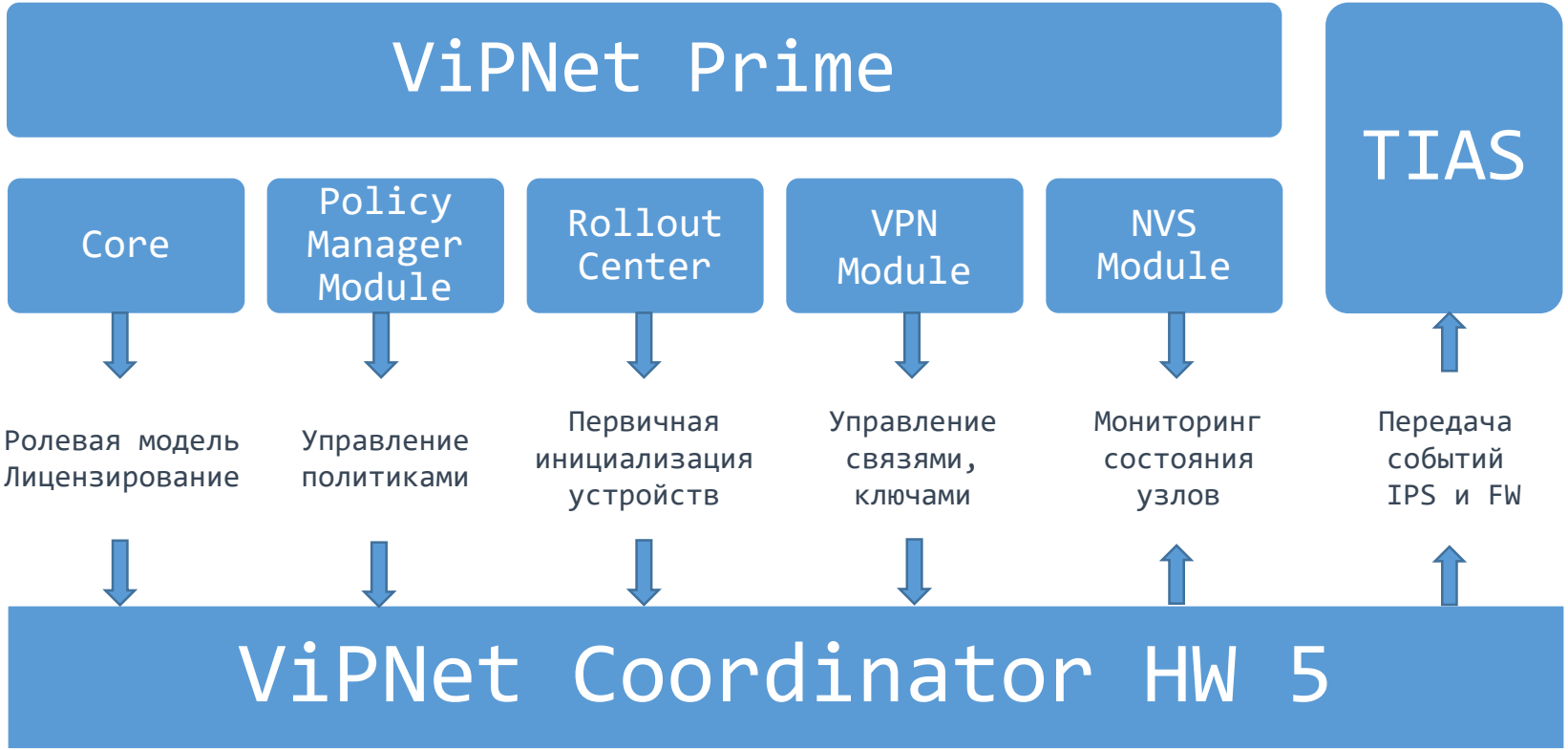
Кластер высокой доступности

- 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

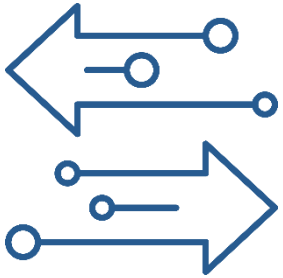
Взаимодействие с внешними системами



Изменение ролевой модели

ViPNet Coordinator HW 4

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



ViPNet Coordinator HW 5

Локальные учетные записи:

- Администратор
- Аудитор

+

Централизованные учетные записи:

- Неограниченное количество
- Администратор/Аудитор
- Single Sign-On (SSO)
- Интеграция с AD через Prime

Развитие ролевой модели

Система

- Системные и сетевые настройки
- Прикладные сервисы

МЭ

- Управление фильтрами
- Задание правил трансляции

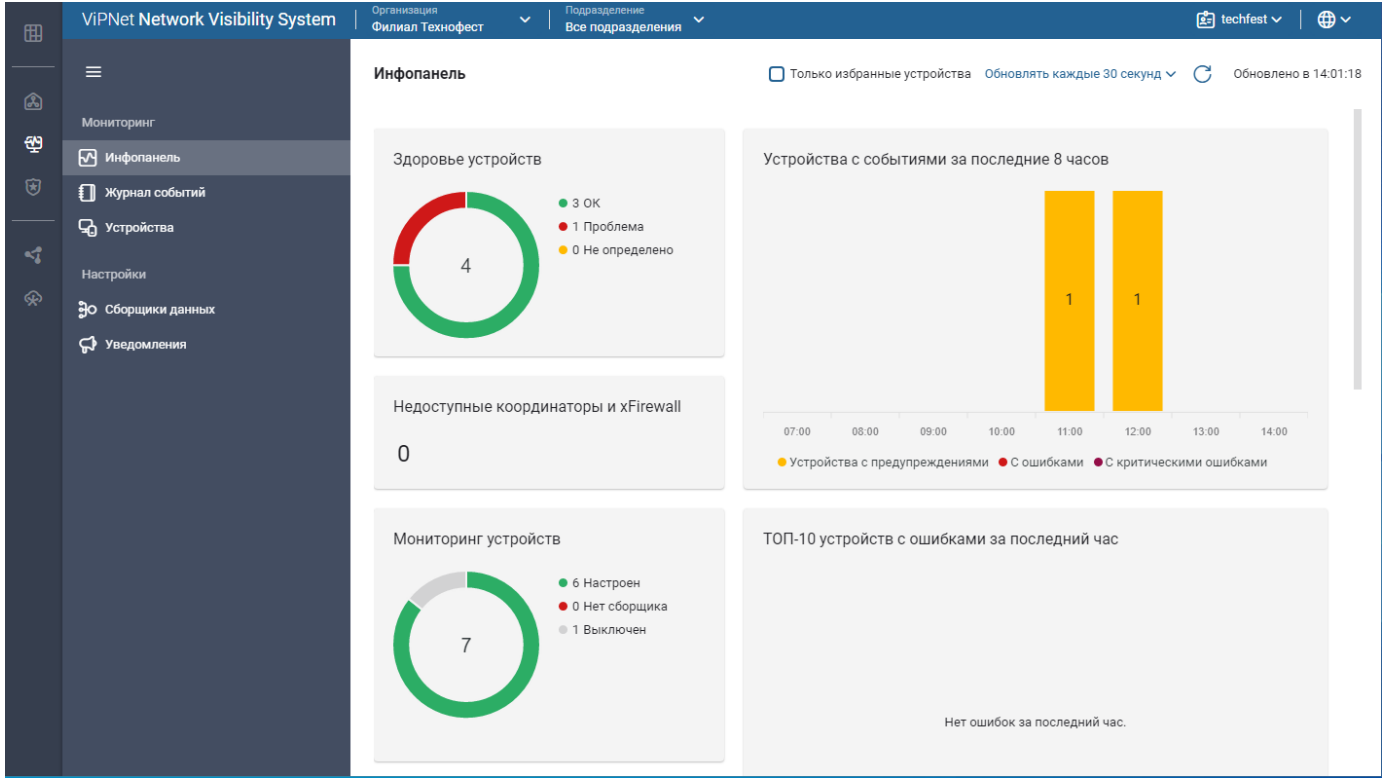
VPN

- Работа с ключевой информацией
- Управление VPN сервисами

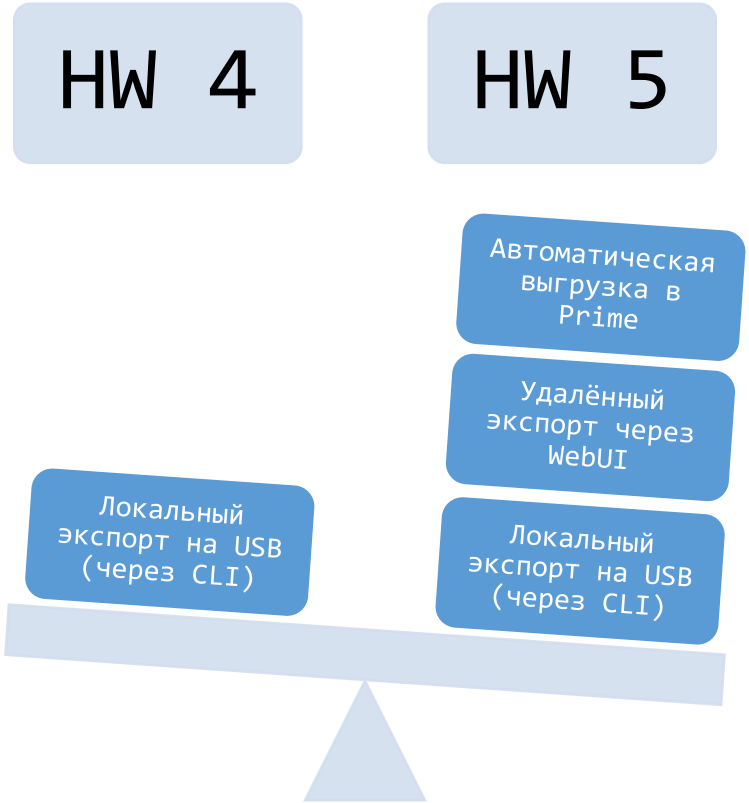
IPS

- Управление БРП
- Работа с событиями

Мониторинг

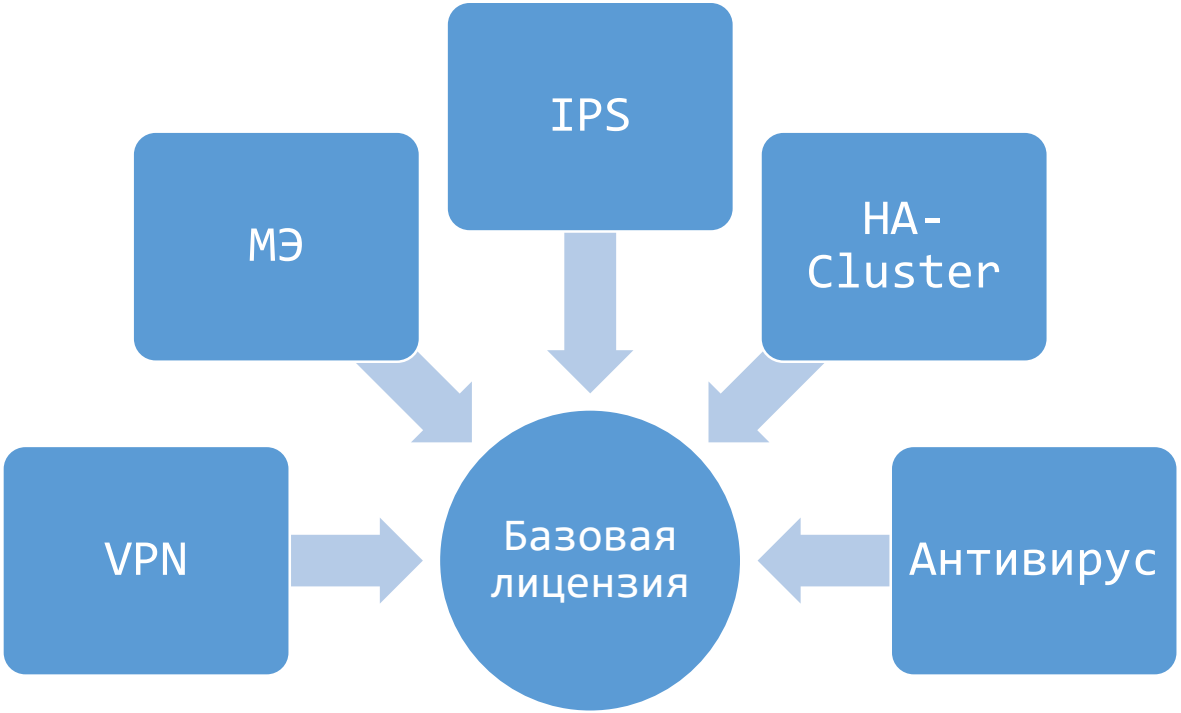

ViPNet Network Visibility System
Организация
Филиал Технофест
Подразделение
Все подразделения
techfest
Мониторинг
Инфопанель
Журнал событий
Устройства
Настройки
Сборщики данных
Уведомления
Инфопанель
Только избранные устройства
Обновлять каждые 30 секунд
Обновлено в 14:01:18
Здоровье устройств
4
3 OK
1 Проблема
0 Не определено
Устройства с событиями за последние 8 часов
1
1
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
Устройства с предупреждениями
С ошибками
С критическими ошибками
Недоступные координаторы и xFirewall
0
Мониторинг устройств
7
6 Настроен
0 Нет сборщика
1 Выключен
ТОП-10 устройств с ошибками за последний час
Нет ошибок за последний час.

Резервное копирование конфигурации



Лицензирование

Новая схема лицензирования

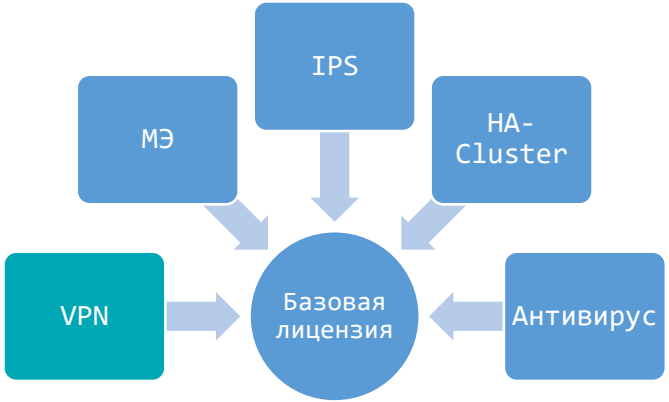


HW50/100/1000/2000/5000

VA100/500/1000/2000

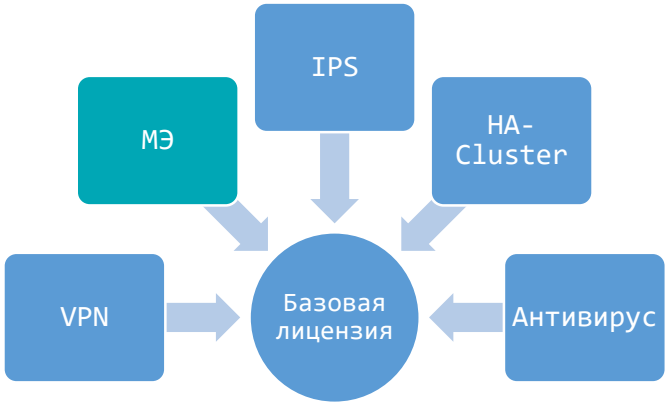
VPN

- **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



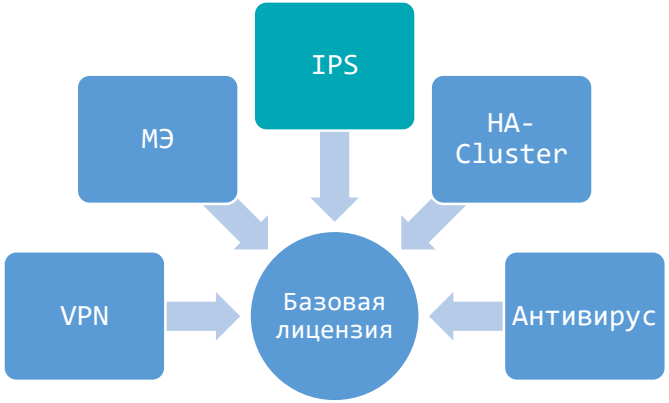
Межсетевой экран

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



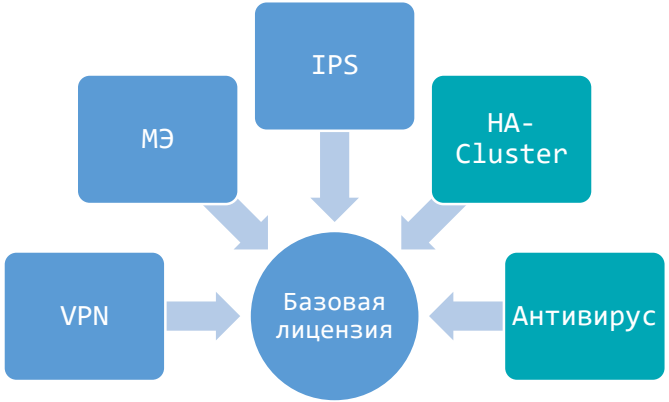
Предотвращение вторжений (IDS/IPS)

- **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

Аппаратные платформы

- ✓ Сделано в России!
- ✓ Замена для 1000-5000-х платформ

- ✓ Одинарный или сдвоенный БП
- ✓ В реестре Минпромторга России

Характеристики платформ

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

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

Поддержка аппаратных платформ

ViPNet Coordinator HW50

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

ViPNet Coordinator HW100

- HW100 N1/N2/N3 ***

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

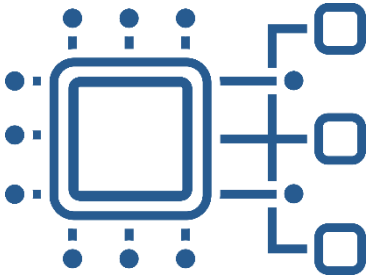
ViPNet Coordinator VA

Среды виртуализации

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

Облачные среды

- Yandex.Cloud
- SberCloud



Спасибо за внимание!

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow