



техно infotecs
2021 Фест

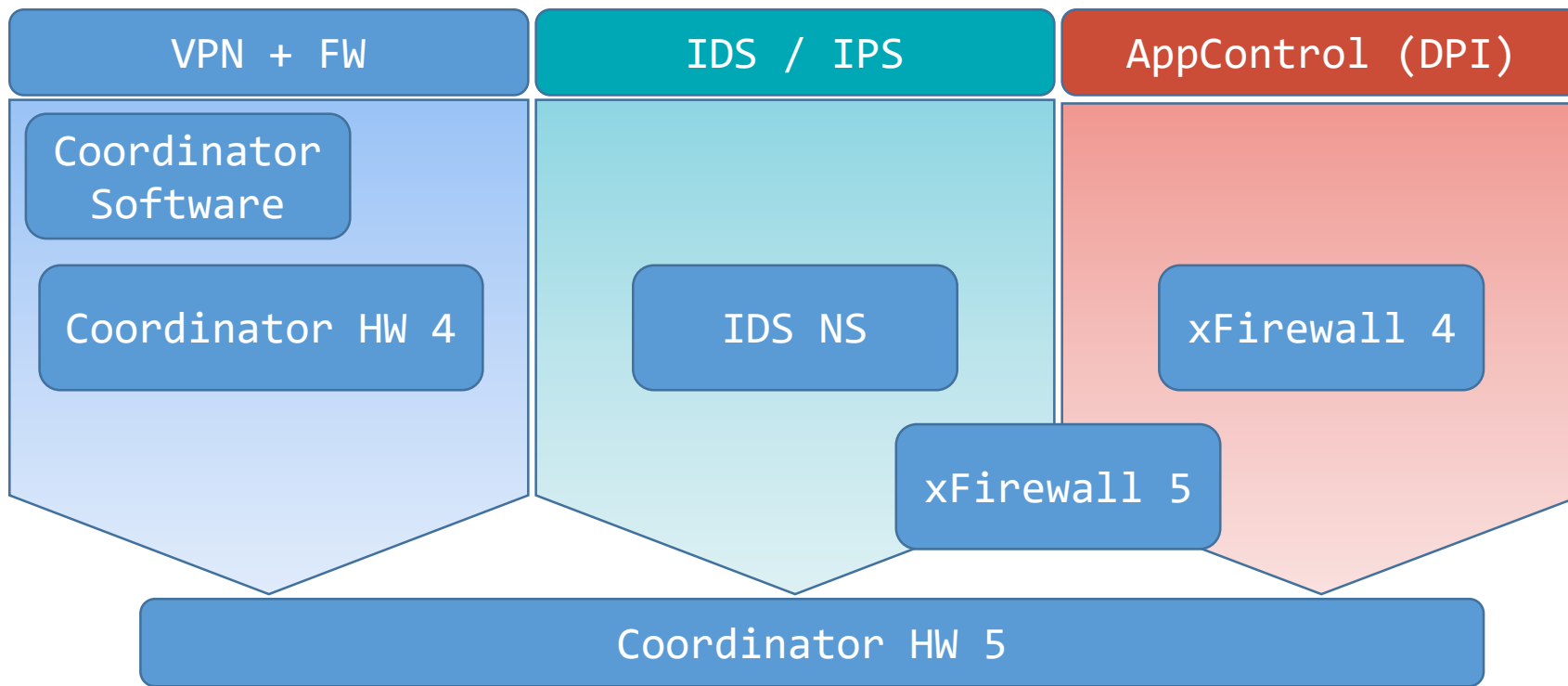
ТЕХНИЧЕСКИЙ
ФЕСТИВАЛЬ

VIPNet Coordinator HW 5

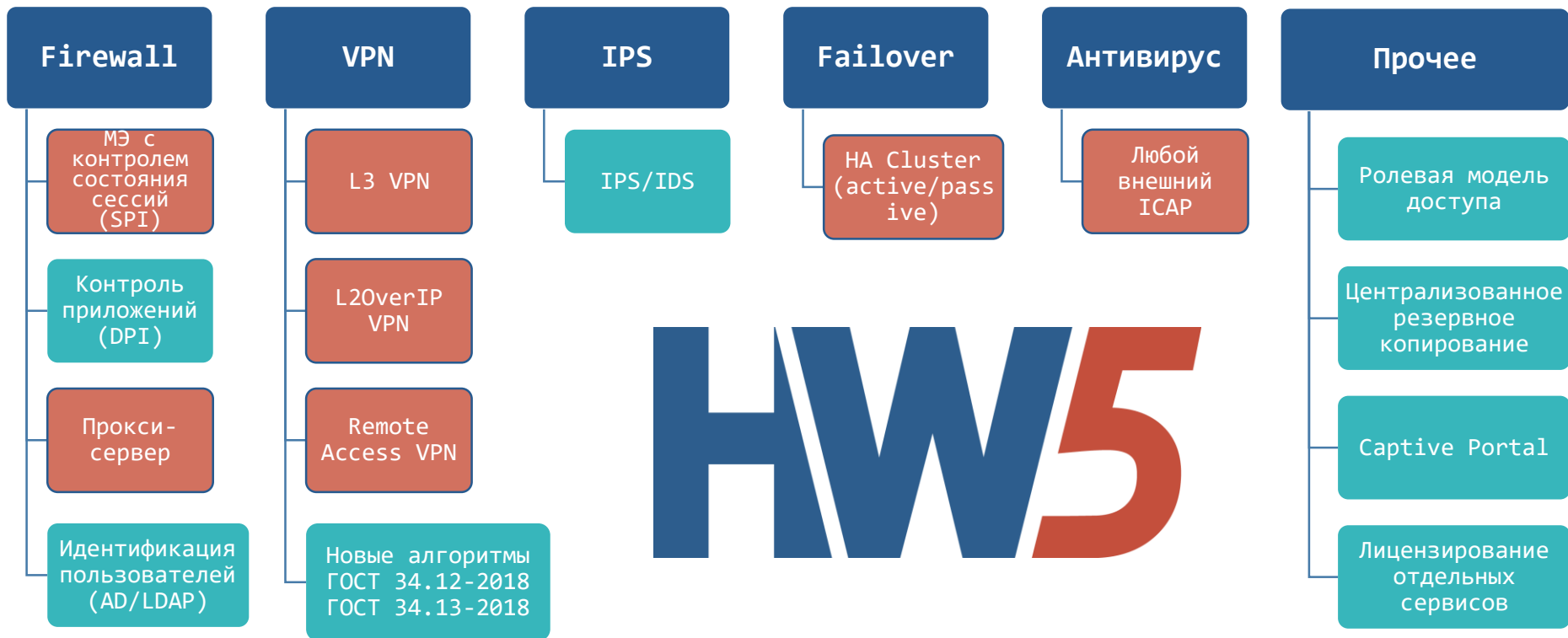
Новое поколение шлюзов
безопасности

Виталий Беличко

Шлюзы безопасности ViPNet



ViPNet Coordinator HW 5



Сертификация

Требования по сертификации

ФСБ России

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

ФСТЭК России

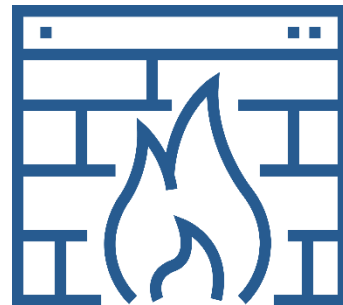
- Межсетевой экран тип «А» 4 класса
- Межсетевой экран тип «Б» 4 класса
- COB уровня сети 4 класса
- 4-й уровень доверия средств защиты информации



Межсетевое экранирование

Межсетевое экранирование

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



Предотвращение вторжений (IDS/IPS)

Предотвращение вторжений

 VIPNet Coordinator VA

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: unknown
Прикладной протокол: HTTP

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


















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

Закрыть

Журнал регистрации IP-пакетов

Фильтр IP-пакетов ▼ Результат фильтрации в интервале с 01.07.2021

	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

   | Показано 16 записей | 

Ство	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...
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...



Вкл

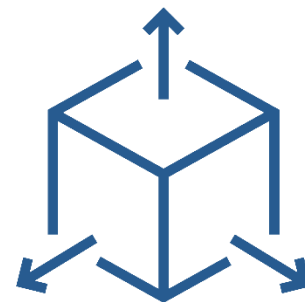
Блокировать

Криптография (VPN)

Криптография (VPN)

- «Кузнечик» и «Магма» (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- ГОСТ 28147-89 для обратной совместимости
- Iprir 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)

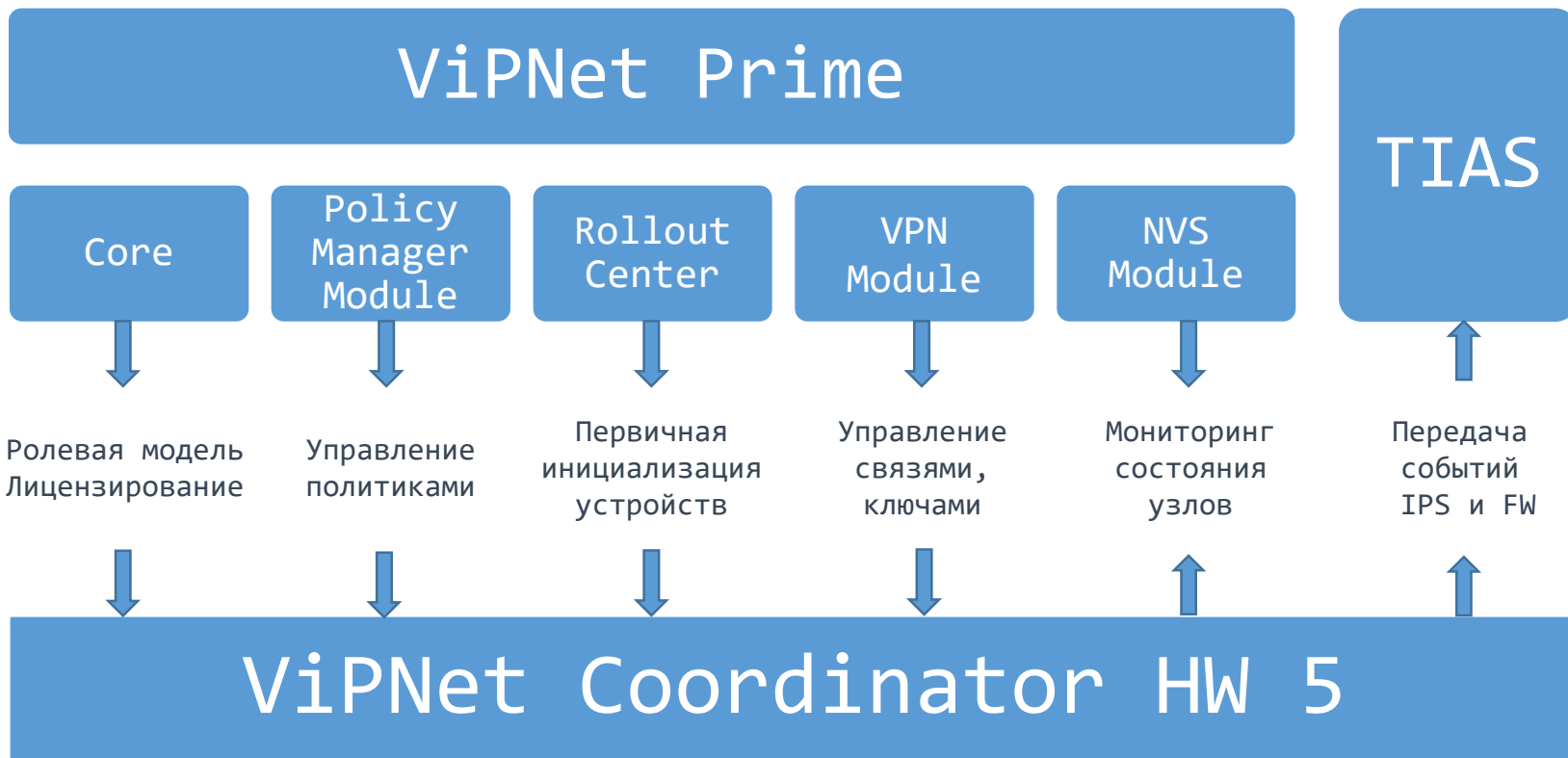
Кластер высокой доступности

- 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

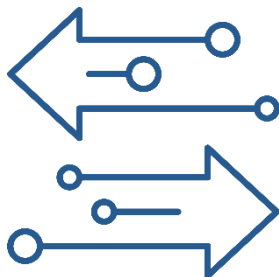
Взаимодействие с внешними системами



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

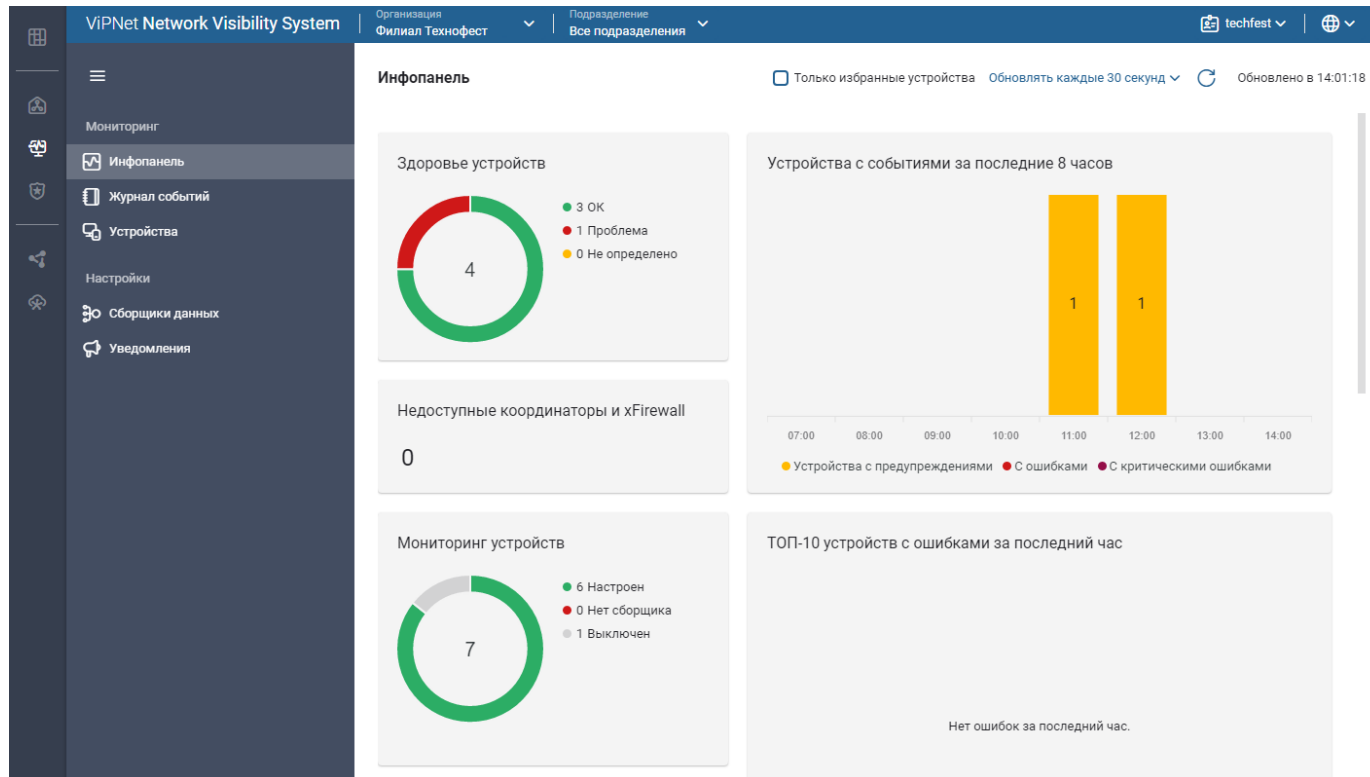
VPN

- Работа с ключевой информацией
- Управление VPN сервисами

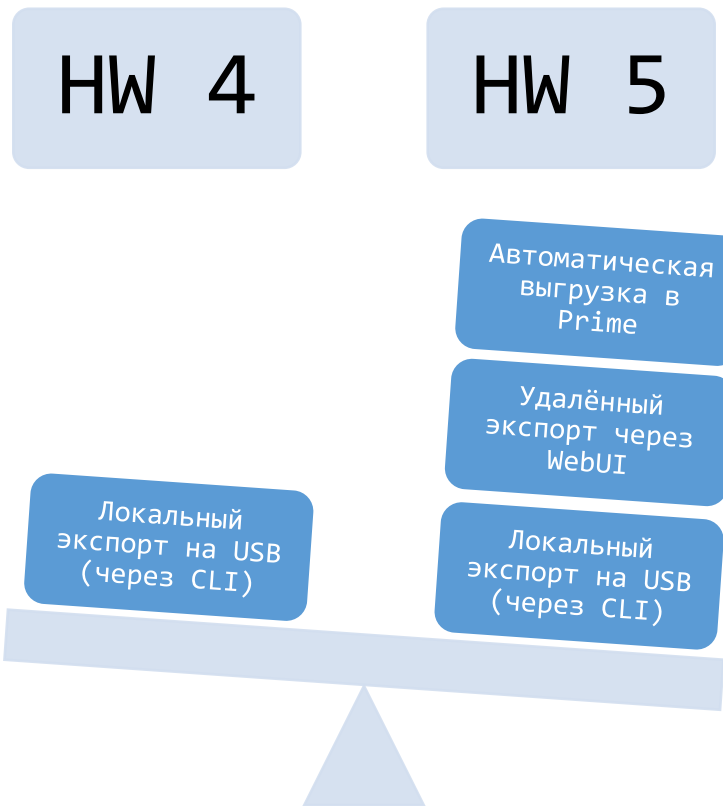
IPS

- Управление БРП
- Работа с событиями

Мониторинг

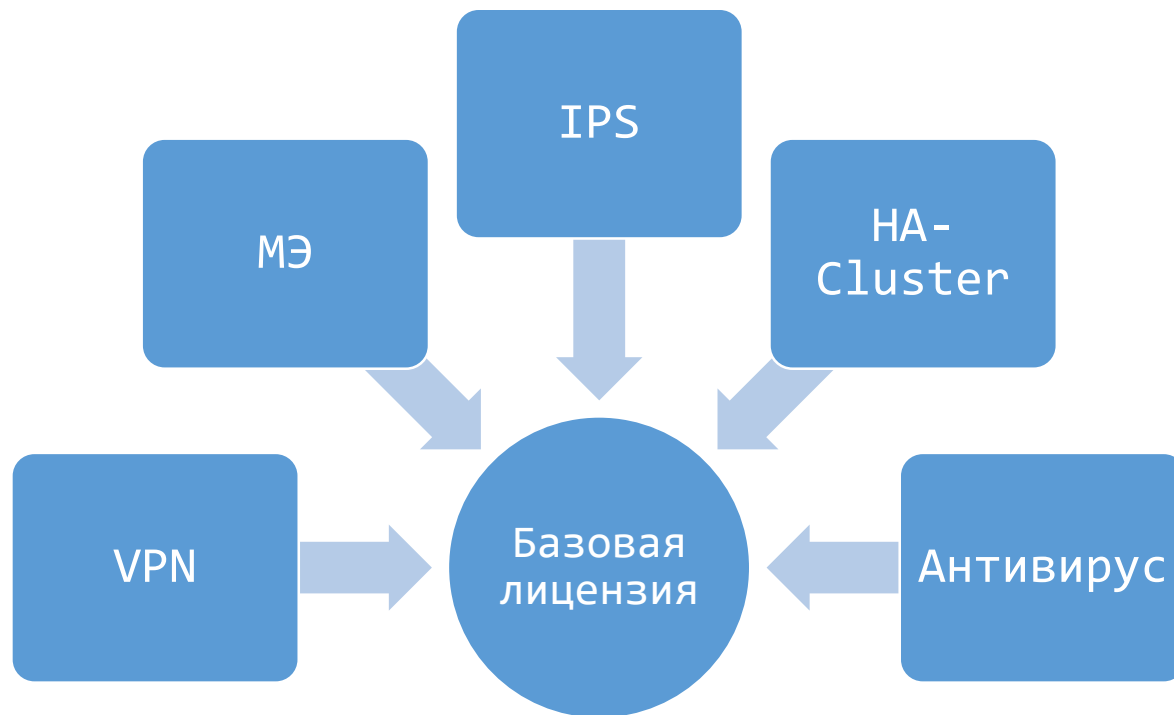


Резервное копирование конфигурации



Лицензирование

Новая схема лицензирования



HW50/100/1000/2000/5000

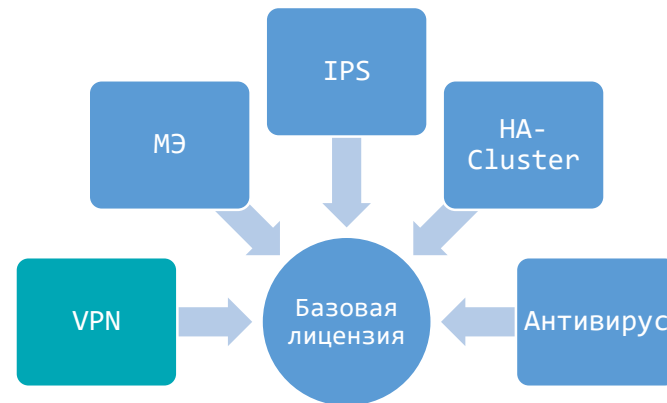
VA100/500/1000/2000

○ Технологический VPN не лицензируется

- Связь с системой управления всегда активна

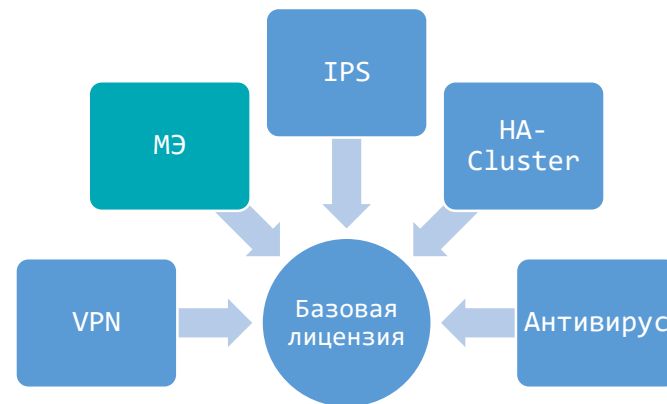
○ Лицензия на VPN (активация, срок действия)

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



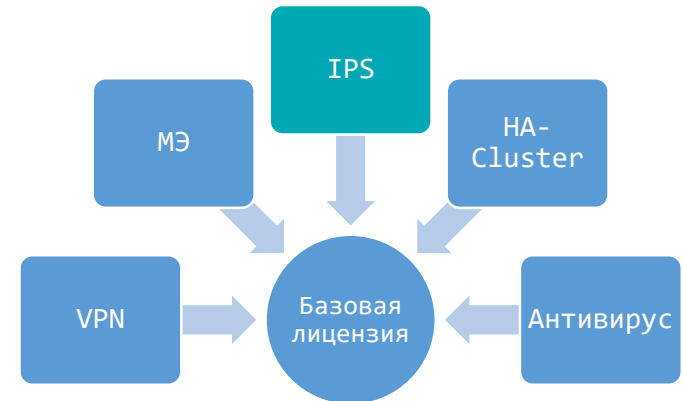
Межсетевой экран

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



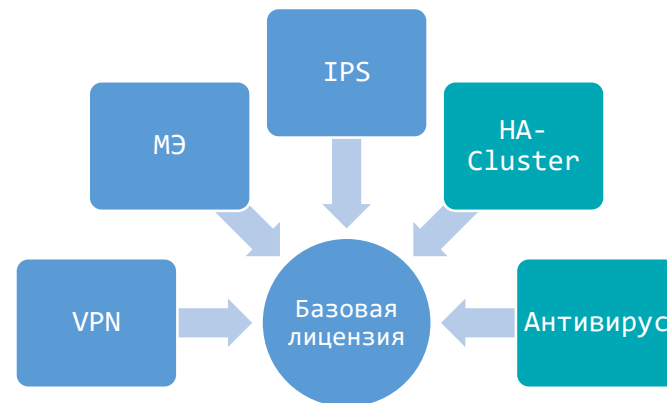
Предотвращение вторжений (IDS/IPS)

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



HA-Cluster и Антивирус

- Лицензируем на кластер для всех исполнений (НМ 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 двойной 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



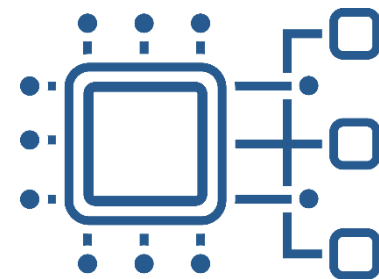
VIPNet Coordinator VA

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



ТЕХНО infotecs
2021 Фест

Спасибо
за внимание!

Подписывайтесь на наши соцсети



@infotecs.ru



@vpninfotecs



@InfoTeCS_Moscow