
техно 2019 infotecs фест
ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ
12 09 2019
Защита каналов связи и построение VPN - Шлюзы безопасности ViPNet Coordinator HW/KB

ViPNet Coordinator HW 4.3

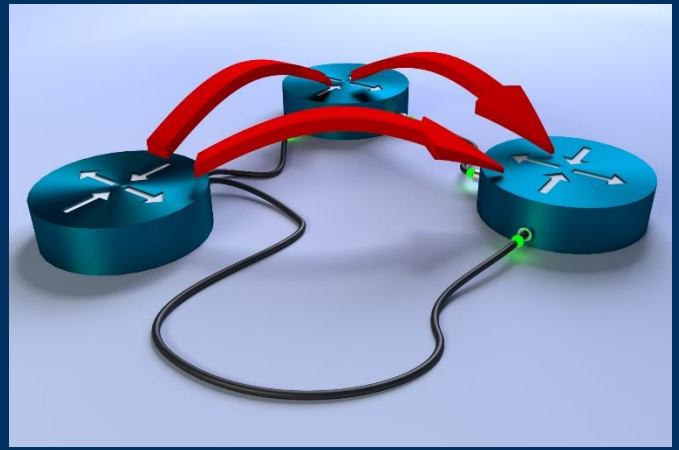
ViPNet Coordinator HW 4.3

- Политики маршрутизации (Policy Routing)
- Проверка состояния шлюзов (Dead Gateway Detection)
- Оптимизированный механизм переключения на альтернативный канал связи с координатором (Dead Peer Detection)

Multi WAN

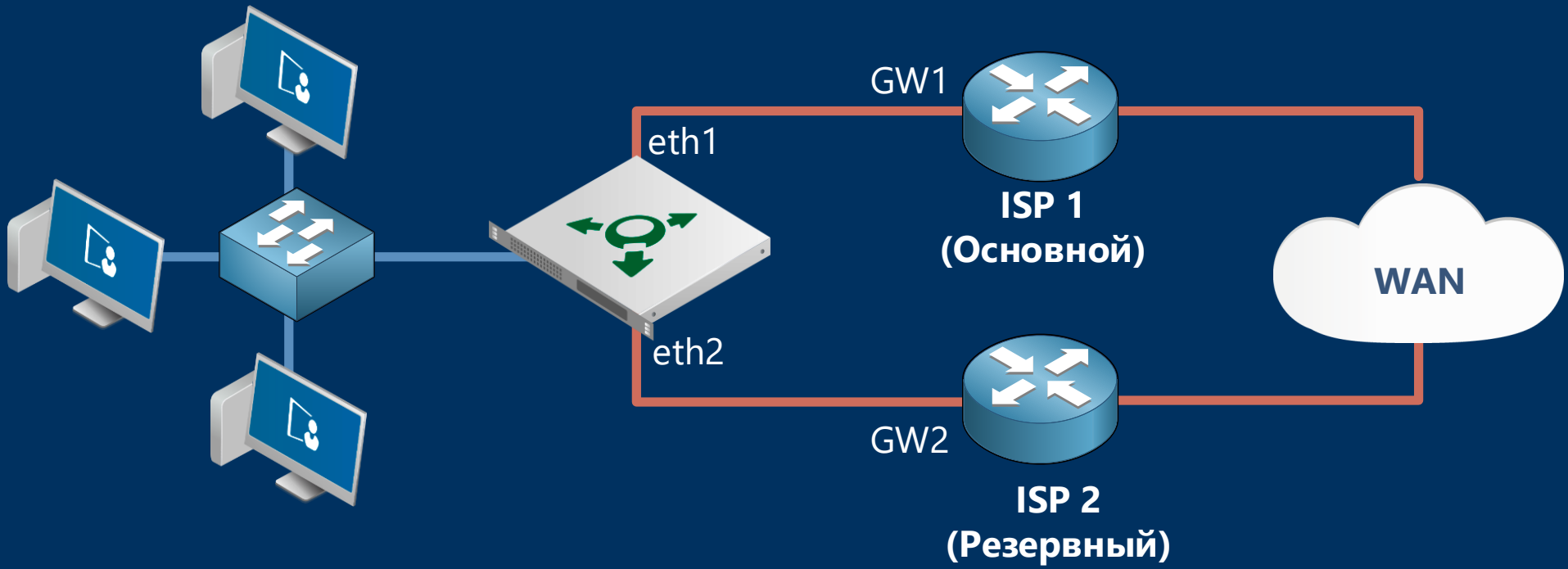
- Расширение возможностей DHCP-сервера и DHCP-Relay
- Отказ от пассивных IP-адресов кластера горячего резервирования
- Повышена производительность

Multi WAN: Работа с несколькими каналами связи

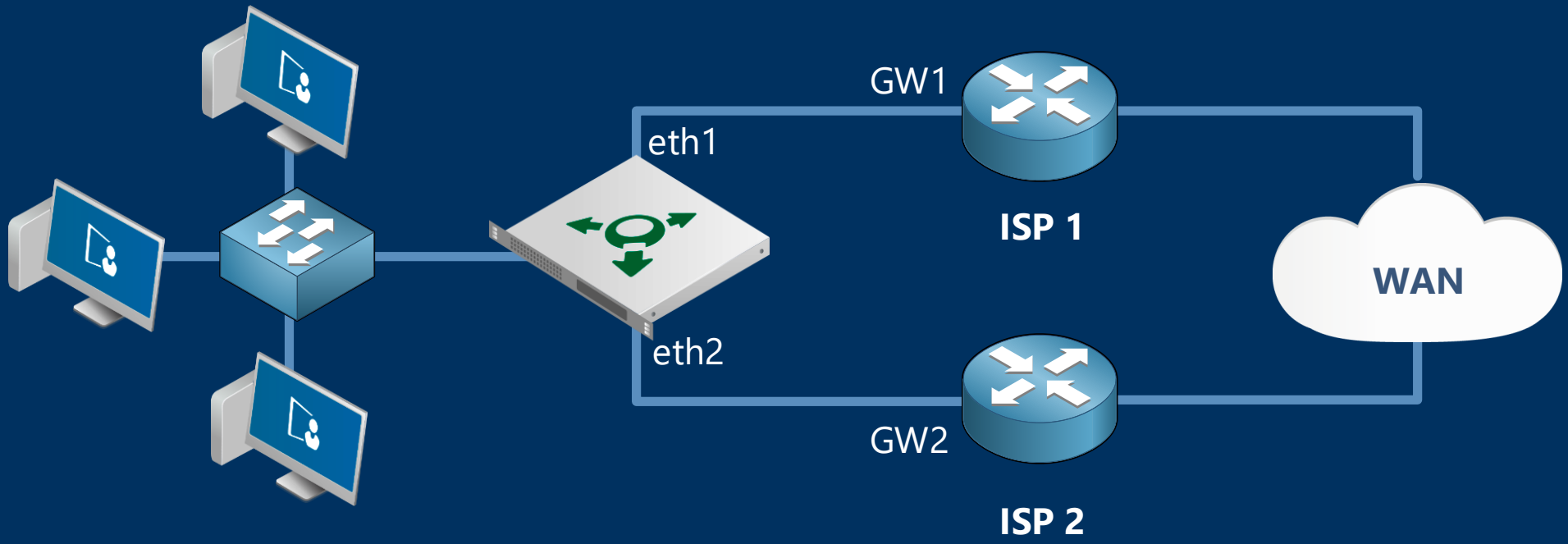


- Пользовательские таблицы маршрутизации
- Политики маршрутизации
- Проверка состояния шлюзов (DGD)

Multi WAN: Резервирование



Multi WAN: Балансировка (открытый трафик)



Пользовательские таблицы маршрутизации


```
va-core# inet show routing static
Table 254 (MAIN)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------

Table 1025 (TEST-TABLE-1)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
0.0.0.0          0.0.0.0          8.8.8.8          10       1

Table 2000 (TEST-TABLE-2)
Destination      Netmask          Next hop         Distance Weight
-----------      -------          --------         -------- ------
0.0.0.0          0.0.0.0          9.9.9.9          10       1
10.1.0.0         255.255.224.0    1.1.1.1          10       1
```

Политики маршрутизации

Признак трафика	Обработка	Приоритет
Политика маршрутизации по умолчанию		
Весь трафик	По таблице маршрутизации по умолчанию	
test-policy-1		
Весь трафик	По таблице маршрутизации по умолчанию	1024
Исходящий от адреса 172.30.255.0/24	По таблице маршрутизации test-table-1	2000
Входящий на адреса 9.9.9.9/32		
Метка DSCP - 0x88		
test-policy-2		
Исходящий интерфейс eth1	Блокировать	1100
Весь трафик	По таблице маршрутизации по умолчанию	1200
Входящий на адреса 1.1.1.1/32	Блокировать	1222
Входящий интерфейс eth3	По таблице маршрутизации test-table-2	1333

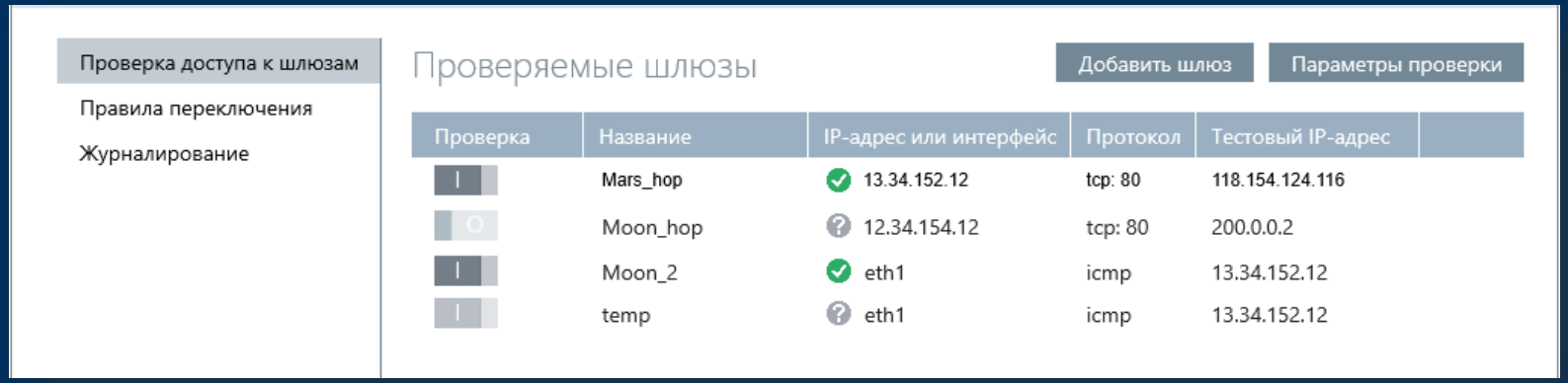
Условия:

- Интерфейс
- Адрес
- Метка DSCP
- Действие:

match / block / reject

- Приоритет

Проверка состояния шлюзов (DGD)

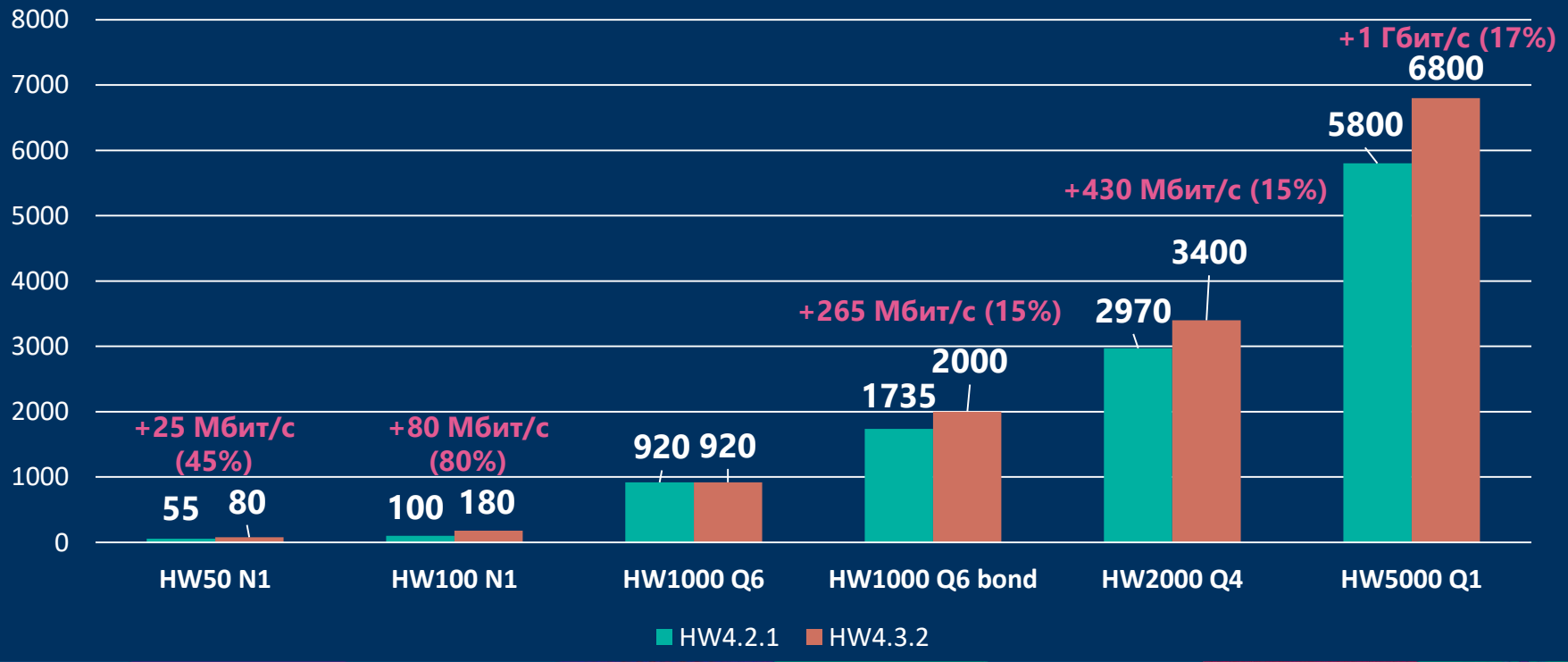


- Метод проверки: ICMP, TCP:80, TCP:443
- Работает для проводных и беспроводных интерфейсов (3G, Wi-Fi)
- Параметры: время ожидания ответа, интервал между проверками, число проверок

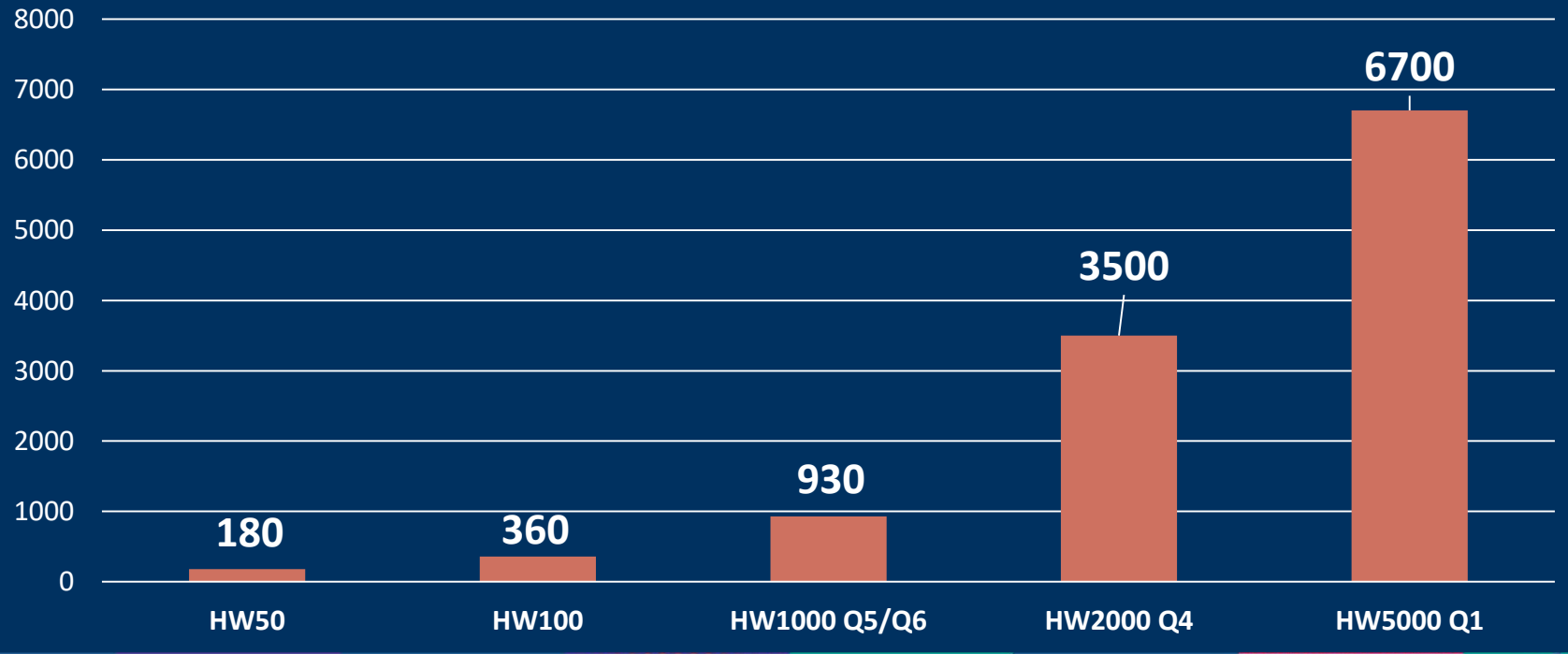
Правила переключения политик

- Время переключения при настройках по умолчанию – 18-20 с
- Минимальное время переключения – 3 с

Производительность VPN (UDP)

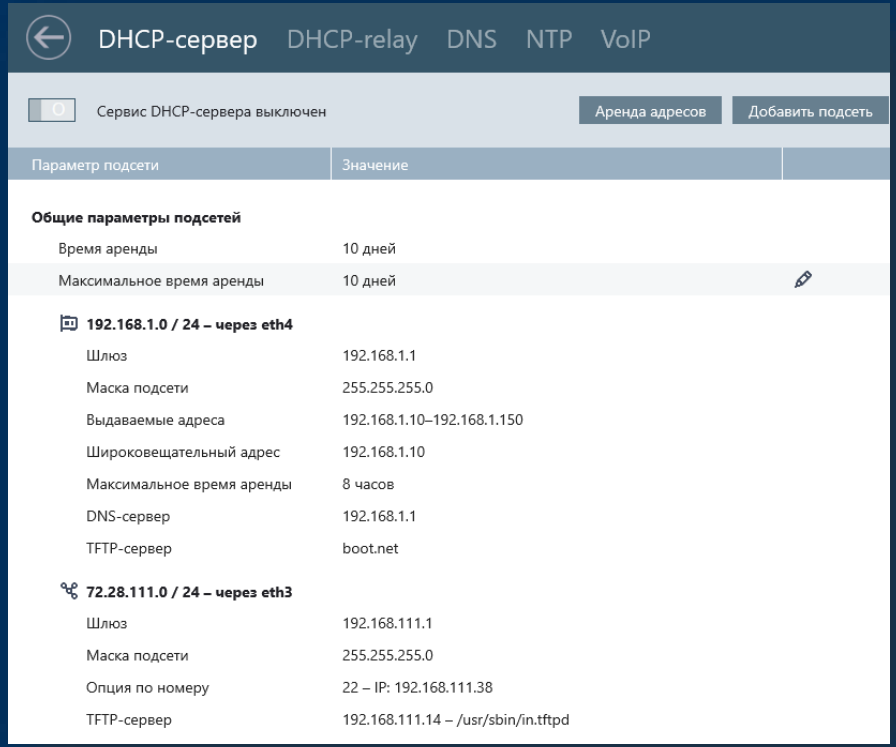


Производительность МЭ (TCP)

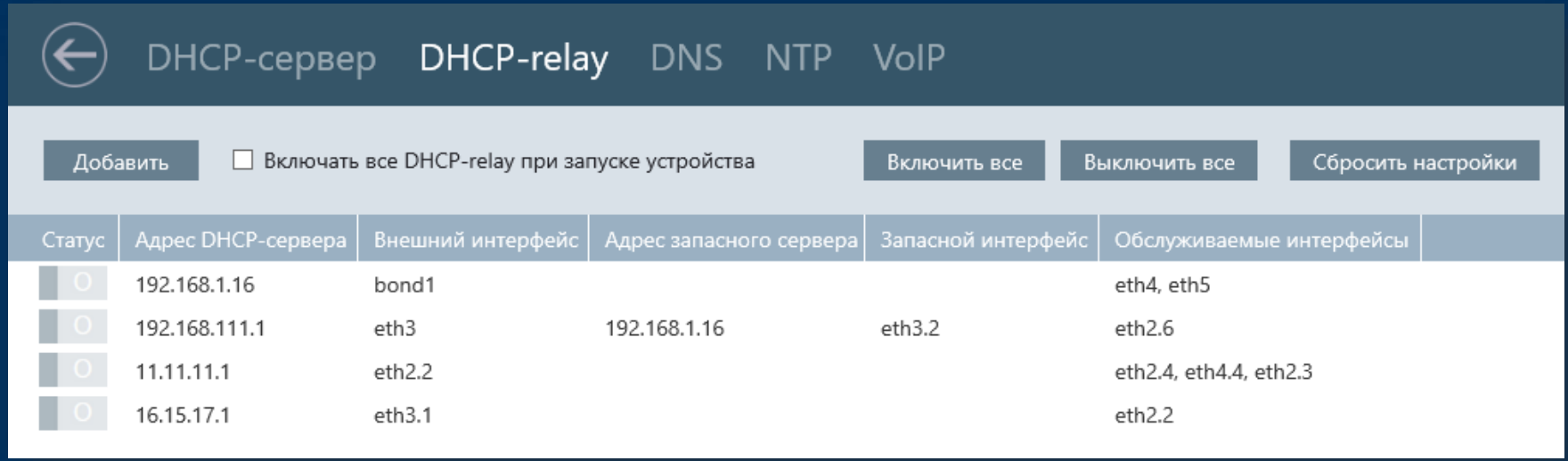


DHCP-сервер

- DHCP-сервер на нескольких интерфейсах
- Работа в кластере
- Резервирование IP-адресов
- Управление DCHP-опциями:
  - IP-адреса DNS- и NTP-сервера
  - IP-адреса TFT-сервера
  - имя домена
  - и другие опции (RFC 2132)



DHCP-relay



- DHCP-Relay для нескольких сетевых интерфейсов
- Возможность указать запасной DHCP-сервер
- Одновременная работа с DHCP-Server и DHCP-Relay (на разных интерфейсах)

HW50 и HW100 без ограничения по туннелям

Отказоустойчивый кластер для HW50 и HW100

- Отдельная лицензия на организацию кластера для HW50 и HW100

ViPNet Coordinator HW 4 : Лицензии расширения	
HC-118-(50-N1/100-N1)-add-LIC-Fail over	Передача права на расширение функционала ViPNet Coordiantor HW50 / HW 100. Лицензия на 1 систему горячего резервирования

- Необходимо дополнительно назначить сетевому узлу роль **Failover100**
- Реализовано в HW 4.2.1 и выше

HA-Cluster (Active-Passive) – HW4.5

- Оптимизация логики обнаружения сбоя и переключения кластера:
  - Мгновенное переключение пассивного узла в активную роль при физическом обрыве соединения
  - Смена роли узлов кластера без перезагрузки (при потере соединения на сетевом интерфейсе)
- Синхронизация таблицы соединений МЭ
- Виртуальный MAC-адрес для кластера
- **Минимальное время переключения кластера сократилось до 1 секунды**

ViPNet Coordinator KB 4

ViPNet Coordinator KB 4

- Соответствие требованиям СКЗИ класса КВ
- Высокая скорость шифрования до 4,5 Гбит/с
- Кластер горячего резервирования
- VPN канального уровня (L2OverIP)
- Поддержка ViPNet Policy Manager
- Поддержка OSPF, vLan, QoS
- 2 новых исполнения

Производительность КВ 4

КВ100

100 Мбит/с

КВ1000

900 Мбит/с

КВ2000

2,3 Гбит/с

КВ5000

4,5 Гбит/с

Модельный ряд КВ 4

	КВ100	КВ1000	КВ2000	КВ5000
Форм-фактор	MiniPC	1U		
L3 VPN	100 Мбит/с	900 Мбит/с	2,3 Гбит/с	4,5 Гбит/с
L2OverIP VPN	100 Мбит/с	840 Мбит/с	2 Гбит/с	3,4 Гбит/с
Максимальное количество туннелей	Не ограничено			
Сетевые интерфейсы (медные)	4x RJ45 1 Гбит/с			
Сетевые интерфейсы (оптические)	1 x SFP 1 Гбит/с	2x SFP 1 Гбит/с	4x SFP+ 10 Гбит/с	
Отказоустойчивый кластер	Нет	Да		

Дополнительные ТС

Устройство аутентификации:

- «Рутокен ЭЦП 2.0» либо «JaCarta ГОСТ»

Трансивер:

- Avago AFBR-5710PZ – KB100 N1/KB1000 Q6
- Avago AFBR-709SMZ – KB2000 Q4/KB5000 Q1

Оптический привод

- Внешний USB DVD привод

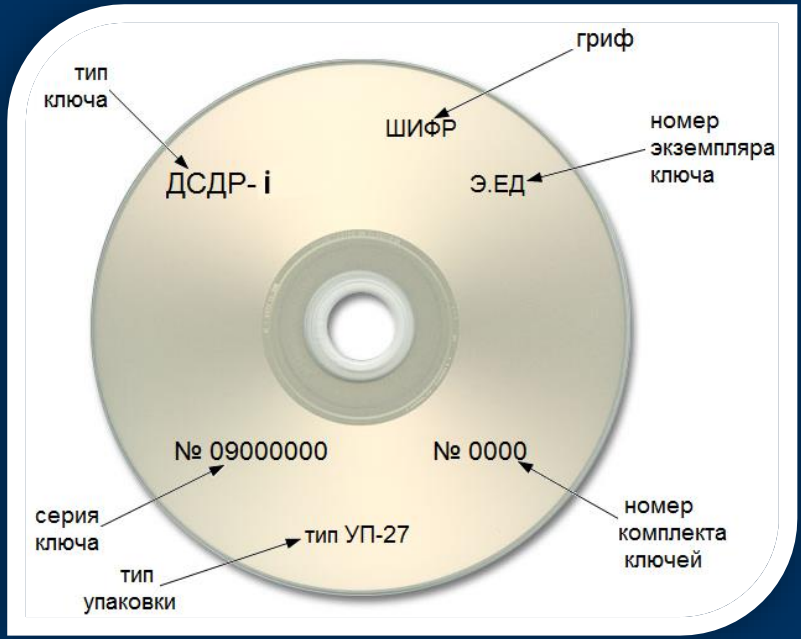
Ключевая система КВ 4

Ключевые блокноты ДСДР, изготавливаемые 8 Центром ФСБ России

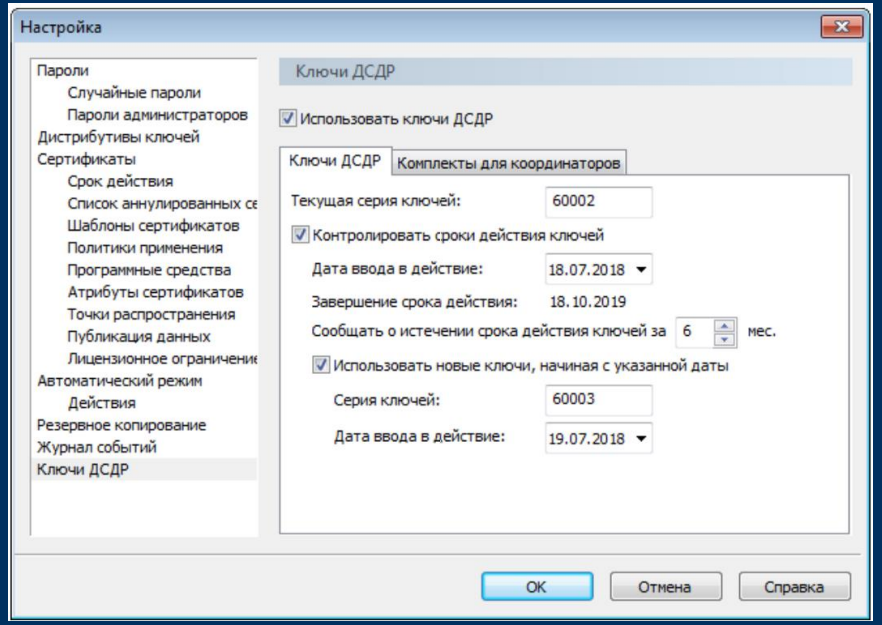
Ключевая информация, формируемая в ViPNet Administrator

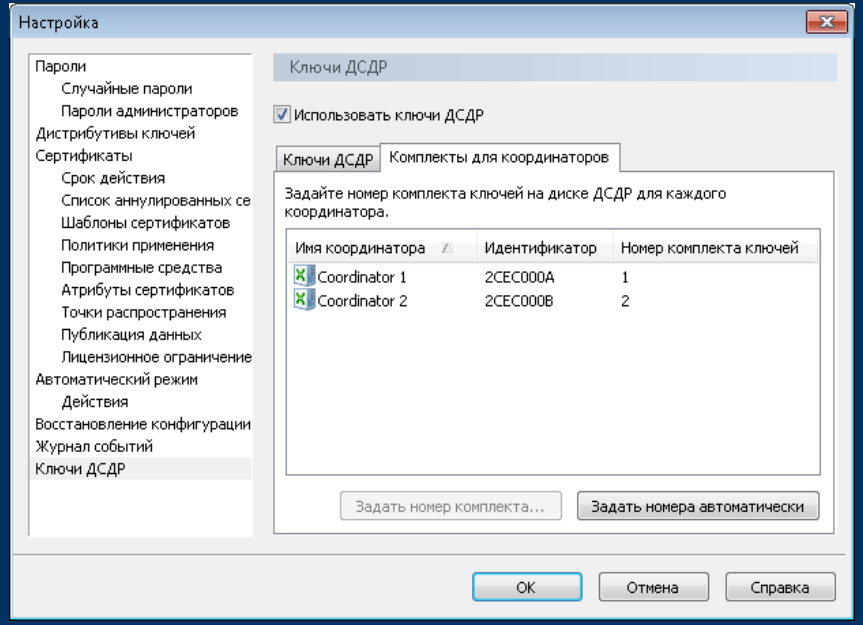
Ключевые блокноты ДСДР

- При заказе ДСДР необходимо заранее запланировать нужное шлюзов КВ в сети
- Размер серии ДСДР не может быть изменен во время действия ключей
- Рекомендуем заказывать комплект ключей с коэффициентом 2,5
- Допустимый срок эксплуатации серии ключей – 1 год и 3 месяца
- Для проведения плановой смены ключей необходимо предварительно заказать и получить новый ключевой блокнот



Регистрация ДСДР в ViPNet Administrator





Генерация и ввод ключей

ТЕХНО 2019 infotecs ФЕСТ

Заказ ключевых блокнотов ДСДР в 8 Центре ФСБ России

Регистрации серии ДСДР в ViPNet Administrator

Формирование DST и Запись ключей на токен

Распаковка DST на КВ4

Ввод ключей ДСДР

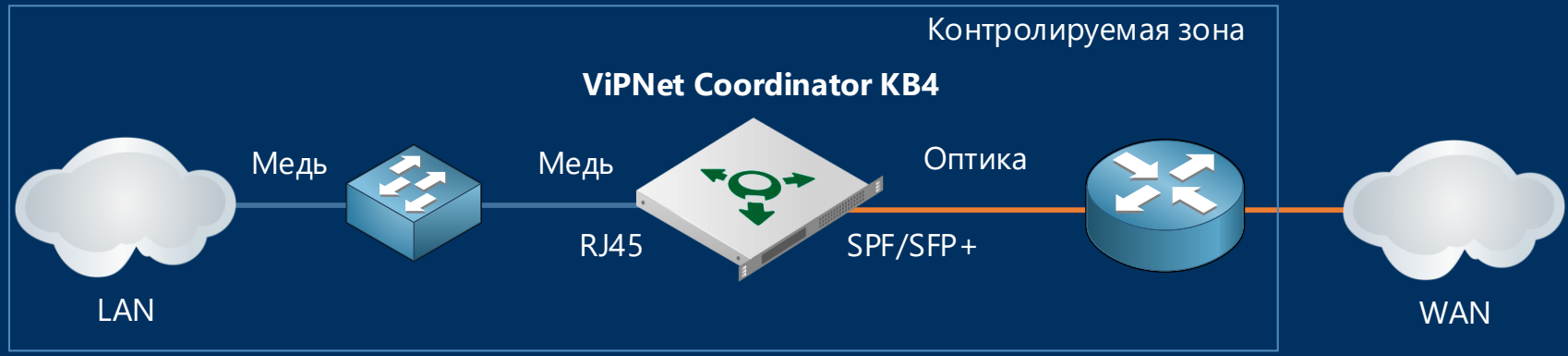
Особенности эксплуатации

- Необходимо использовать службу точного времени NTP и ИБП
- Максимальная разница во времени между узлами КВ:
  - КВ100 – 236 с, КВ1000 – 51 с, КВ2000 – 19 с, КВ5000 – 10 с
- Аутентификация пользователя/администратора по токену
- Локальная работа с ключами ДСДР (обновление/смена)
- При истечении срока действия ключа ДСДР связь между КВ прервется

Функциональные ограничения

- Шлюзовой координатор (межсетевое взаимодействие)
- Подключение к внешней сети через «Координатор»
- Удаленное подключение через SSH или WebUI
- Удаленное обновление ПО
- TCP-туннели
- Поддержка EtherChannel и изменение MTU
- Прокси-сервер и антивирус
- Заблокирован доступ к консольному порту (COM-порт)

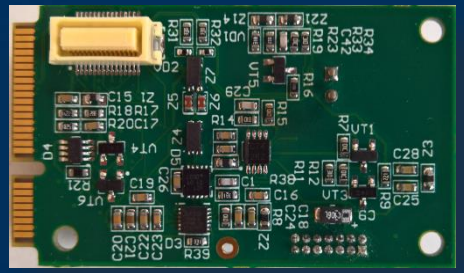
Подключение к внешней сети



- Запрещается проводить **прямое подключение** ViPNet Coordinator KB 4 к каналам связи, выходящим за пределы КЗ
- Подключение ViPNet Coordinator KB 4 к каналу связи, выходящему за пределы КЗ, должно осуществляться **через фрагмент оптоволоконной сети**, содержащей в своём составе коммутационное оборудование

Аппаратный датчик защиты от НСД

- Контроль вскрытия корпуса
- Экстренное уничтожение ключевой информации
- Контроль целостности ПО
- Контроль срока действия ключей ДСДР
- Ведение независимого журнала событий НСД



Совместимость версий ПО

Управляющие компоненты:

- ViPNet Administrator 4
- ViPNet Policy Manager 4
- ViPNet StateWatcher 4

Шлюзы безопасности:

- ViPNet Координатор-КВ2 (есть ограничения)
- ViPNet Coordinator HW 4

VPN-клиенты:

- ViPNet Client 4

Сертификация КВ4

ФСБ России на СКЗИ класса КВ:

- КВ1000 – № СФ/124-3678 действителен до 12.04.2022
- КВ2000 – № СФ/124-3744 действителен до 04.09.2022
- КВ5000 – № СФ/124-3745 действителен до 04.09.2022
- КВ100 – в процессе сертификации

ФСБ России на МЭ 4 класса:

- В процессе сертификации

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3678 от "12" апреля 2019 г.

Действителен до "12" апреля 2022 г.

Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»),
Обществу с ограниченной ответственностью «Линия защиты» (ООО «Линза»).

Настоящий сертификат удостоверяет, что программно-аппаратный комплекс ViPNet Coordinator KB 4 (исполнение ViPNet Coordinator KB1000 на аппаратной платформе KB1000 Q6) в комплектации согласно формуляру ФРКЕ.465614.001ФО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КВ и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных ОАО «ИнфоТеКС»
сертификационных испытаний образца продукции № 781А-001001.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.001ТУ, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.001ФО.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России А.М. Ивашко

Настоящий сертификат внесён в Государственный реестр сертифицированных средств защиты информации 12 апреля 2019 г.

Первый заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России В.Н. Мартынов

Планы развития

- Удалённое управление по SSH
- Графический веб-интерфейс (WebUI)
- Автоматическая смена серии ДСДР
- Переход на новый координатор (HW4.3)
  - Политики маршрутизации и проверка состояния шлюзов
  - Усовершенствованный механизм работы кластера горячего резервирования
  - Расширенная функциональность DHCP-сервера и DHCP-Relay
  - Поддержка EtherChannel и изменение значения MTU
  - и многое другое

ТЕХНО 2019 infotecs Фест

Спасибо
за внимание!