ViPNet Coordinator VA

Виртуализированный шлюз безопасности

Беличко Виталий

ViPNet Coordinator HW-VA

Поддерживаемые платформы виртуализации:

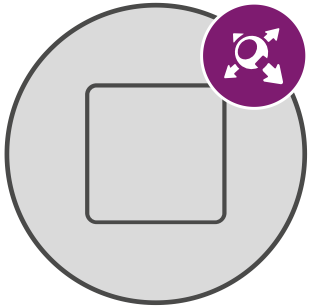
- VMware ESXi 6.7
- VMware Workstation 12.x
- Microsoft Hyper-V 10.0
- Oracle VM VirtualBox 5.x

Ограничения:

- Для шифрования трафика можно использовать не более 2-х CPU
- Число туннелей задается в ЦУС (лицензируется)
- Не сертифицировано

ViPNet Coordinator VA

- Защита данных внутри виртуальной и облачной инфраструктуры
- Функциональность, соответствующая аппаратным шлюзам
- Удобство управления и скорость развертывания
- Отсутствие дополнительных затрат на размещение и обслуживание оборудования
- Поддержка распространённых систем виртуализации
- Гибкое лицензирование и быстрое масштабирование



ViPNet Coordinator VA

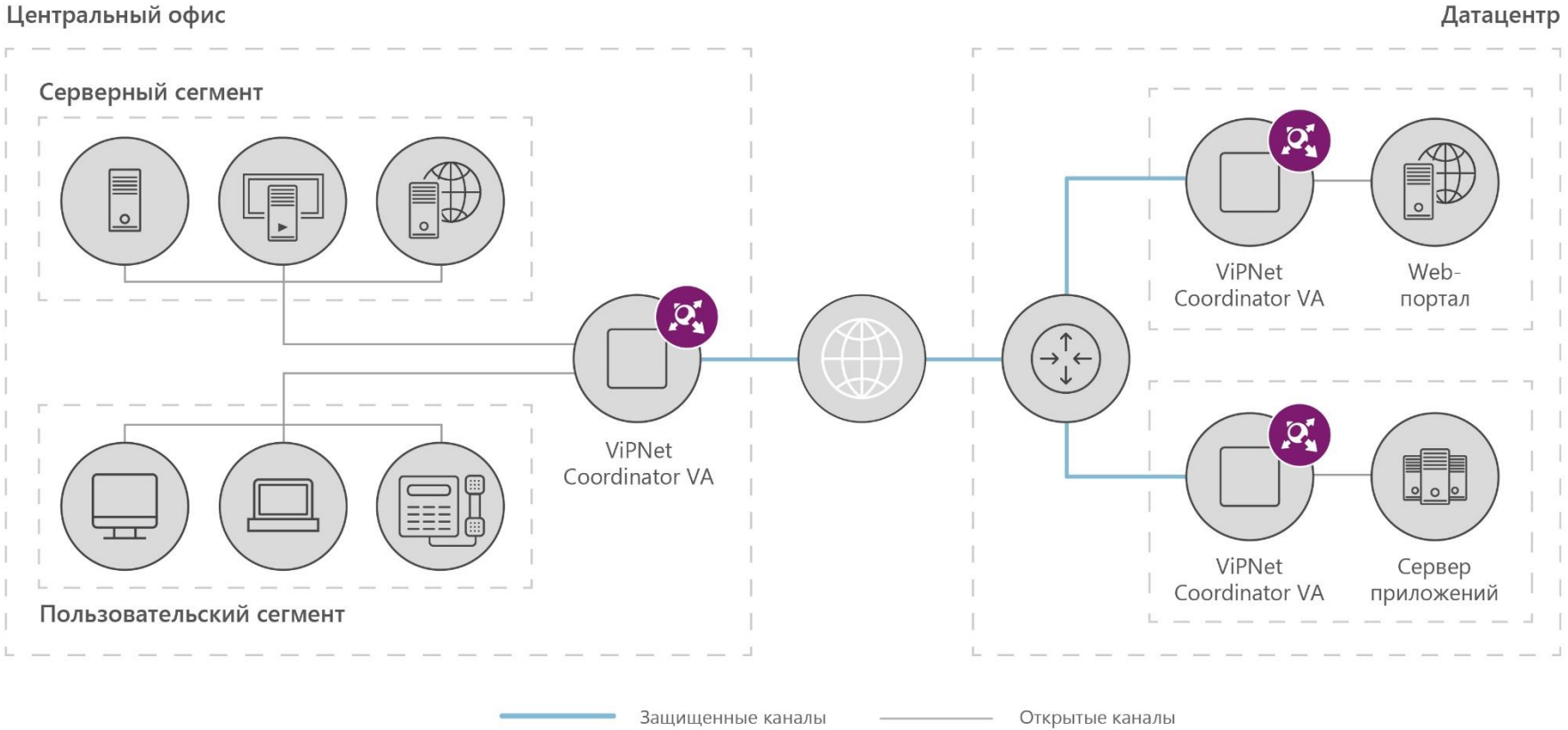
Сертификация

- ViPNet Coordinator VA - исполнение ViPNet Coordinator HW 4
- **ФСБ России** – подписано положительное заключение ФСБ России*
  - СКЗИ класса КС1
- **ФСТЭК России** – материалы проходят экспертизу ИЛ*
  - Межсетевой экран тип «Б» 4 класса
  - 4-й уровень доверия средств защиты информации
- **Минцифры России** – в Реестре российского ПО

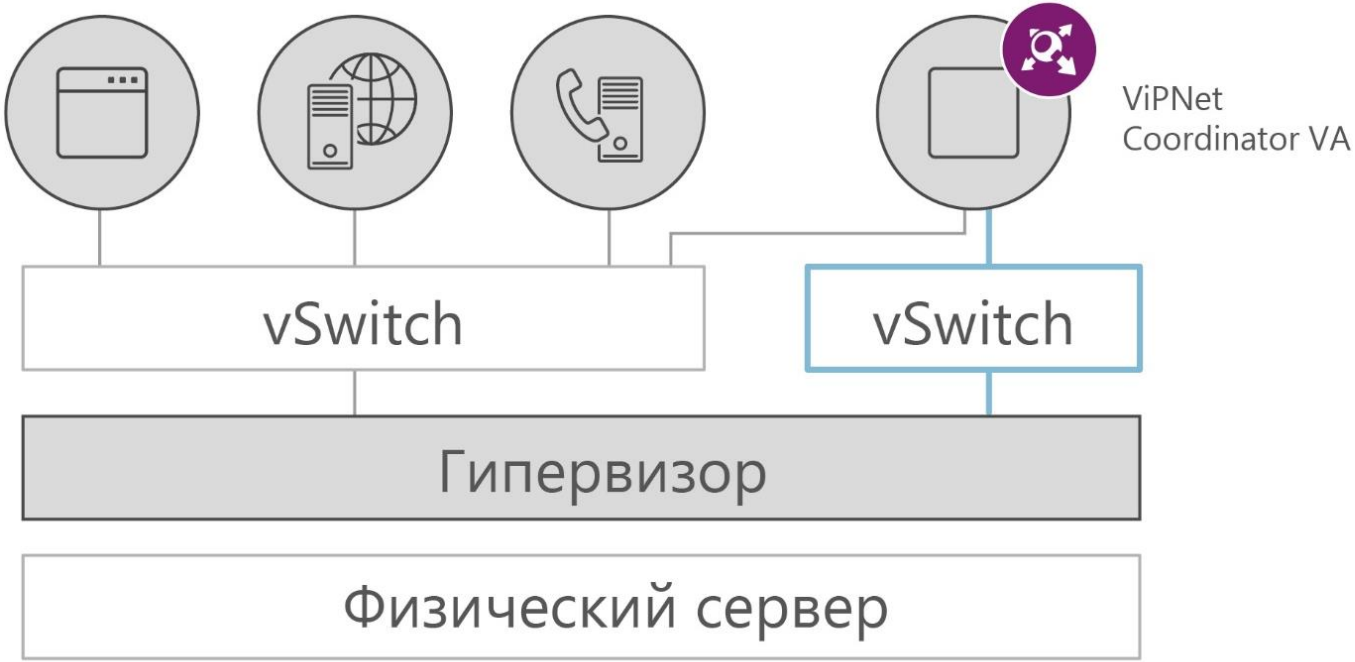
* Статус сертификации на 22.09.2021

Сценарии использования

Сегментация сетей и безопасность частного облака



Сетевая безопасность внутри виртуальной инфраструктуры



Функциональные возможности

Функциональные возможности

VPN

- VPN-шлюз сетевого уровня (L3 VPN)
- VPN-шлюз канального уровня (L2OverIP VPN)
- Сервер IP-адресов
- Маскирование структуры трафика в UDP, TCP

МЕЖСЕТЕВОЙ ЭКРАН

- Межсетевой экран с контролем состояния сессий
- Раздельная фильтрация открытого и шифруемого IP-трафика
- NAT/PAT
- Прокси-сервер с ICAP

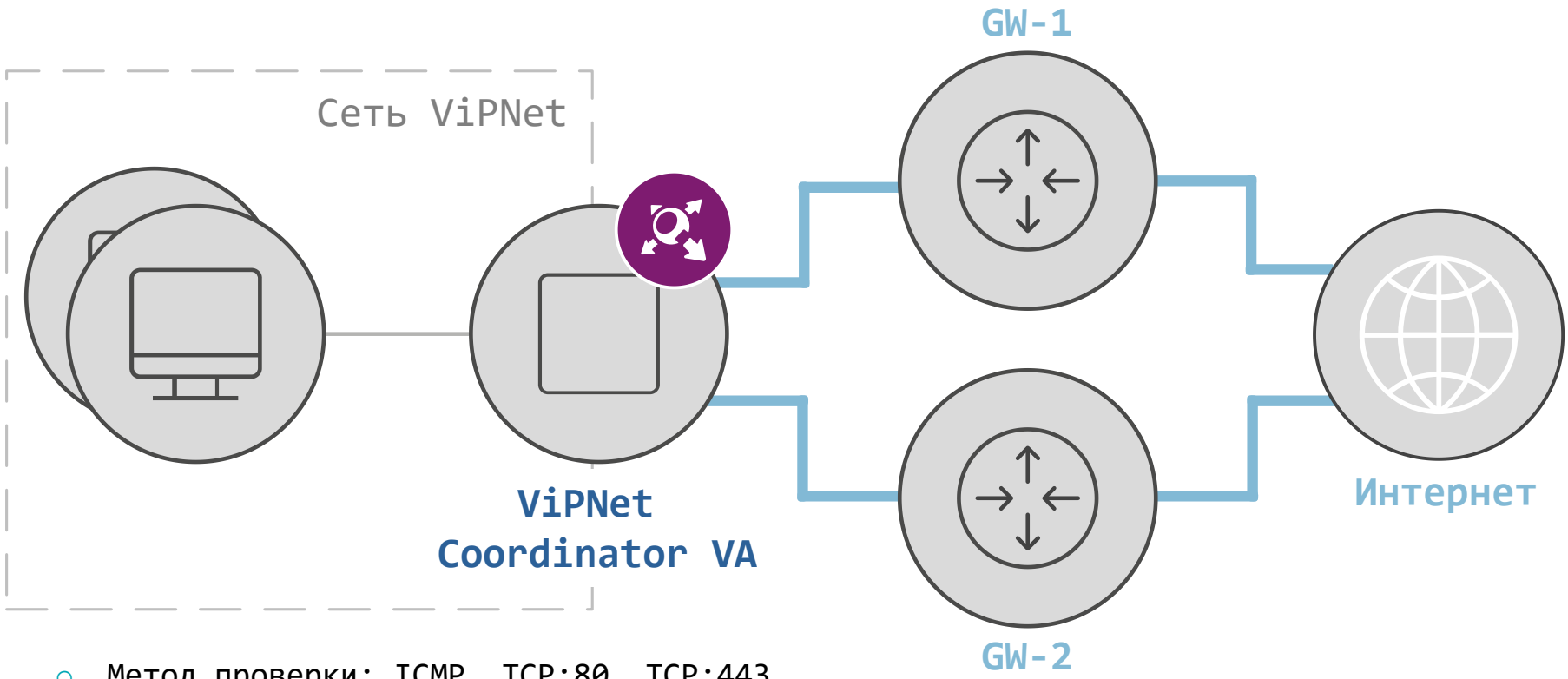
СЕТЕВЫЕ ФУНКЦИИ

- MultiWAN: Резервирование и балансировка
- Динамическая маршрутизация
- Политики маршрутизации (PBR)
- Поддержка VLAN
- Агрегирование сетевых интерфейсов
- Классификация и приоритизация трафика

СЕРВИСНЫЕ ФУНКЦИИ

- DNS-, DHCP-, NTP-сервер и DHCP-Relay
- Мониторинг по протоколу SNMP
- Экспорт событий по протоколу CEF
- Кластер горячего резервирования

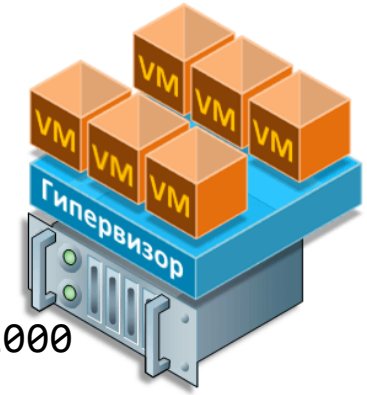
MultiWAN: Резервирование и балансировка



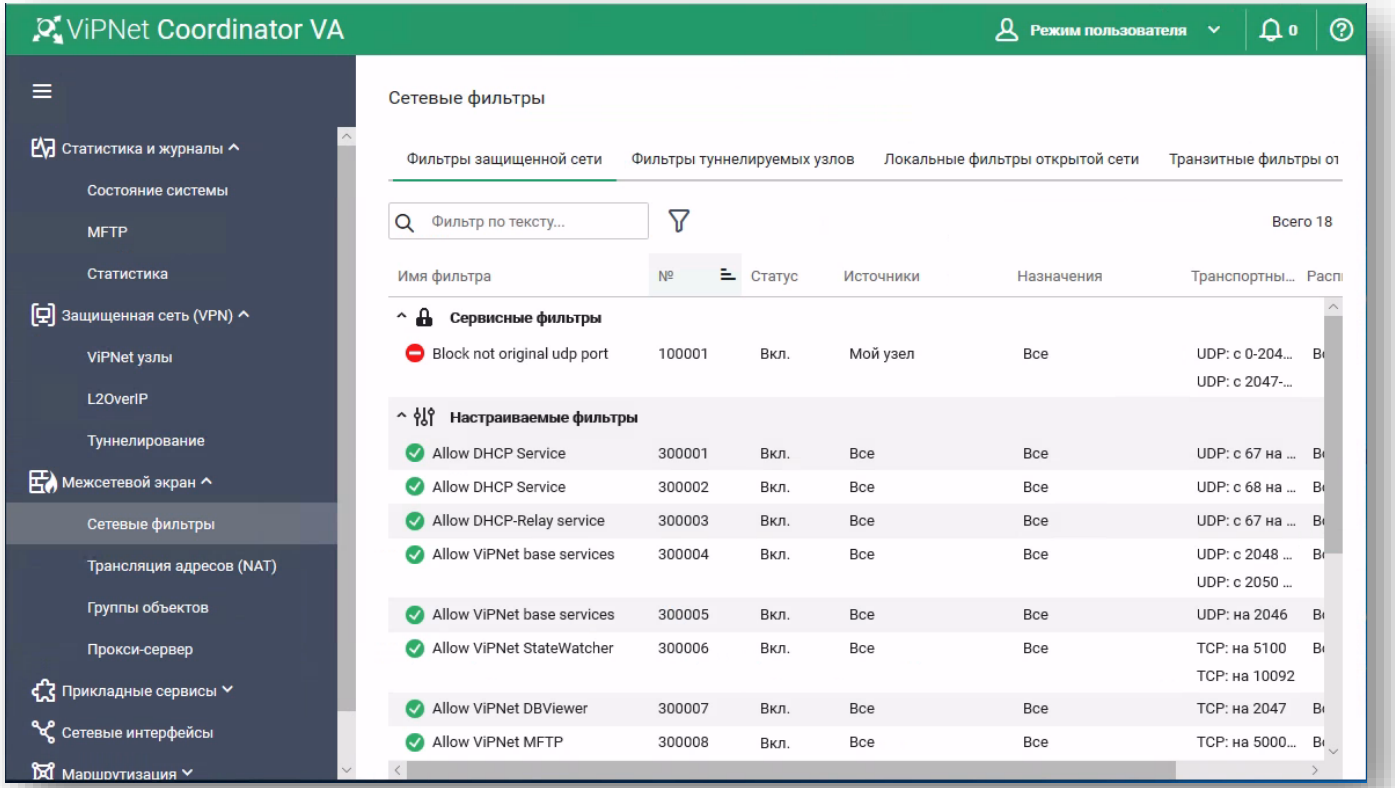
- Метод проверки: ICMP, TCP:80, TCP:443
- Минимальное время переключения – 3 сек.

Новые функции релиза VA 4.3.3

- Функциональность релиза HW4.3.2
- Изменение в лицензировании:
  - VA100, VA500, VA1000, VA2000
  - Failover100, Failover500, Failover1000, Failover2000
- Добавлена поддержка Kernel-based Virtual Machine (KVM)
- Экспорт журнала регистрации IP-пакетов по сети в формате CEF
- Новый дизайн веб-интерфейса
- Локализация на английском языке (документация и WebUI)



Новый WebUI


ViPNet Coordinator VA
Режим пользователя
0
Статистика и журналы
Состояние системы
MFTP
Статистика
Защищенная сеть (VPN)
ViPNet узлы
L2OverIP
Туннелирование
Межсетевой экран
Сетевые фильтры
Трансляция адресов (NAT)
Группы объектов
Прокси-сервер
Прикладные сервисы
Сетевые интерфейсы
Маршрутизация
Сетевые фильтры
Фильтры защищенной сети
Фильтры туннелируемых узлов
Локальные фильтры открытой сети
Транзитные фильтры от
Фильтр по тексту...
Всего 18
Имя фильтра
№
Статус
Источники
Назначения
Транспортны...
Сервисные фильтры
Block not original udp port 100001 Вкл. Мой узел Все UDP: с 0-204... UDP: с 2047-...
Настраиваемые фильтры
Allow DHCP Service 300001 Вкл. Все Все UDP: с 67 на ...
Allow DHCP Service 300002 Вкл. Все Все UDP: с 68 на ...
Allow DHCP-Relay service 300003 Вкл. Все Все UDP: с 67 на ...
Allow ViPNet base services 300004 Вкл. Все Все UDP: с 2048 ... UDP: с 2050 ...
Allow ViPNet base services 300005 Вкл. Все Все UDP: на 2046
Allow ViPNet StateWatcher 300006 Вкл. Все Все TCP: на 5100 TCP: на 10092
Allow ViPNet DBViewer 300007 Вкл. Все Все TCP: на 2047
Allow ViPNet MFTP 300008 Вкл. Все Все TCP: на 5000...

ViPNet Coordinator VA

Среды виртуализации

- KVM, QEMU-KVM и Libvirt
- VMware ESXi 6.7
- VMware Workstation 12.x, 14.x, 15.x
- Microsoft Hyper-V Server 2019
- Oracle VM Server 3.4
- Oracle VM VirtualBox 6.x

Облачные среды

- Yandex.Cloud
- SharxBase

Лицензирование

Роль узла	Роль кластера	Макс. CPU	Кол-во туннелей
Coordinator VA100	Failover100	2	unlim
Coordinator VA500	Failover500	2	unlim
Coordinator VA1000	Failover1000	4	unlim
Coordinator VA2000	Failover2000	7	unlim

- Единый дистрибутив ПО для всех типов лицензий
- Возможность обновления лицензии VA100 → VA500 → VA1000 → VA2000
- Лицензии поддерживаются ПК ViPNet Administrator 4.6.4

Производительность

- Зависит от конфигурации хостовой машины и гипервизора

Тип лицензии	VA100	VA500	VA1000	VA2000
VPN, Мбит/с	180	580	1 400	4 000
МЭ, Мбит/с	330	940	3 500	5 500
Макс. количество сессий МЭ	150 000	500 000	1 000 000	3 000 000
Рекомендуемое число VPN-клиентов	100	500	1 000	2 000

*Условия измерений: VMware ESX 6.7, CPU Xeon E-2278GE

Комплект поставки

- Файл с образом виртуальной машины:
  - va_vipnet_**vhd**.tar.gz (для развертывания в среде Microsoft Hyper-V)
  - va_vipnet_**raw**.tar.gz
  - va_vipnet_**qcow2**.tar.gz

  } (для развертывания в среде KVM)
  - va_vipnet_.**ova** (для в ESXi и остальных сред виртуализации)
- Файл обновления в формате LZH
- Документация в формате PDF
- Формуляр (в печатном виде)

Планы развития

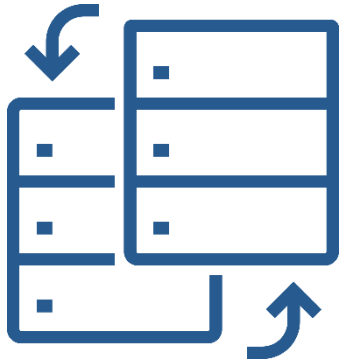
ViPNet Coordinator VA 4.5.1

VA4.5.1 – релиз вышел в сентябре 2021

- Кластер высокой доступности
- Новые возможности мониторинга
- Повышение безопасности сетевых протоколов
- Новые сервисные функции
- Повышение производительности

Кластер высокой доступности

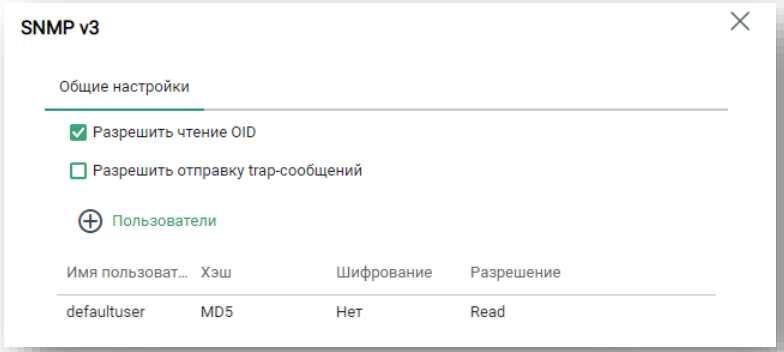
- Быстрое переключение кластера по потере связи и питания
- Синхронизация сессий МЭ в кластере
- Виртуальный MAC-адрес для кластера
- Синхронизация времени пассивного узла кластера
- **Минимальное время переключения кластера сократилось до 1 секунды**

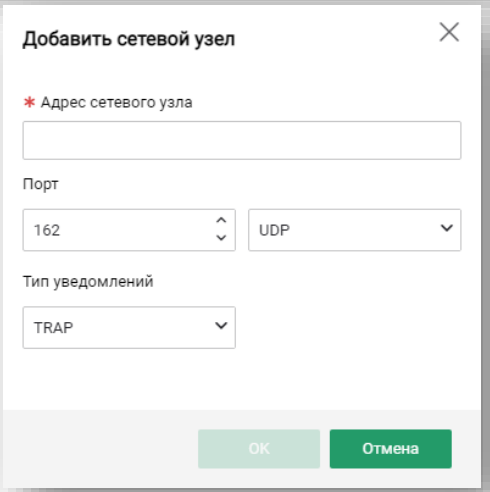


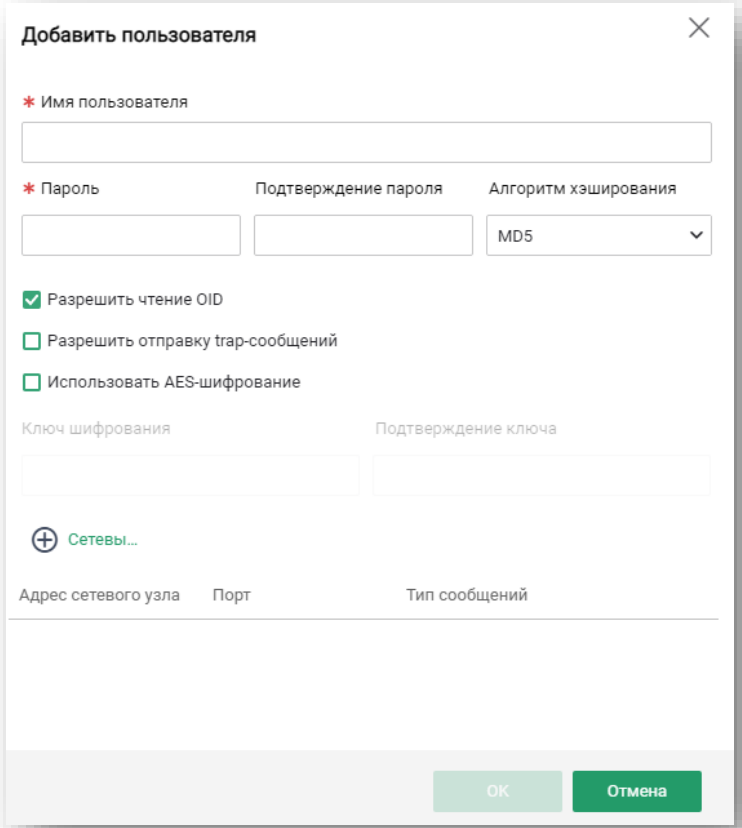
Новые возможности мониторинга

- Поддержка протокола SNMPv3 (+INFORM)
- Мониторинг пассивного узла кластера через SNMP
- Интеграция базы SNMP MIB в WebUI
- Утилизация сетевых интерфейсов в WebUI

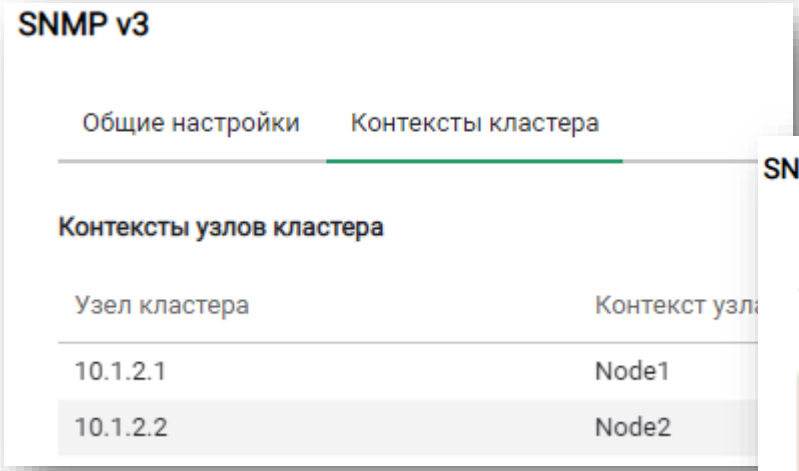
Поддержка протокола SNMPv3

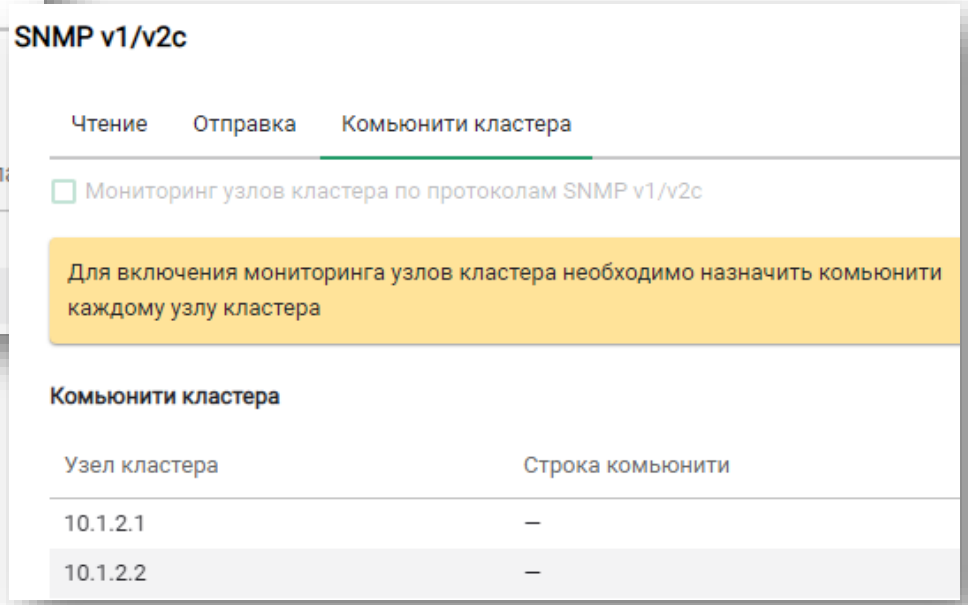






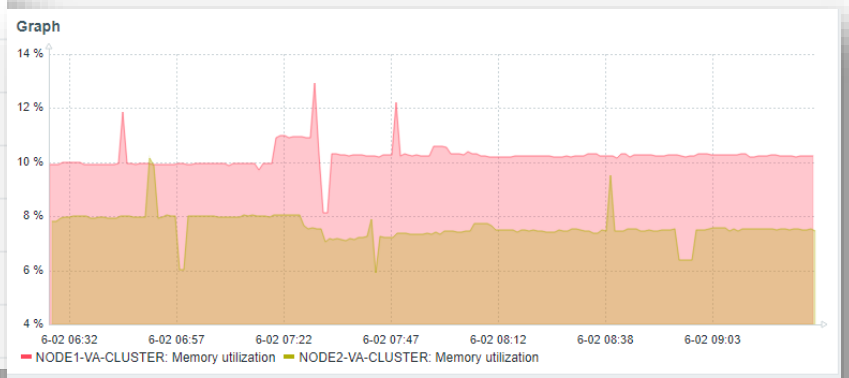
Мониторинг пассивного узла кластера

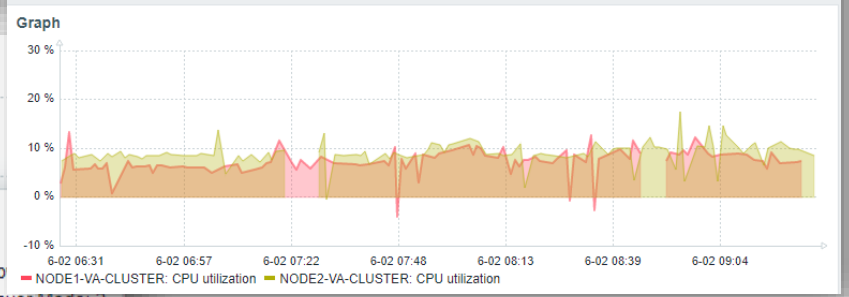


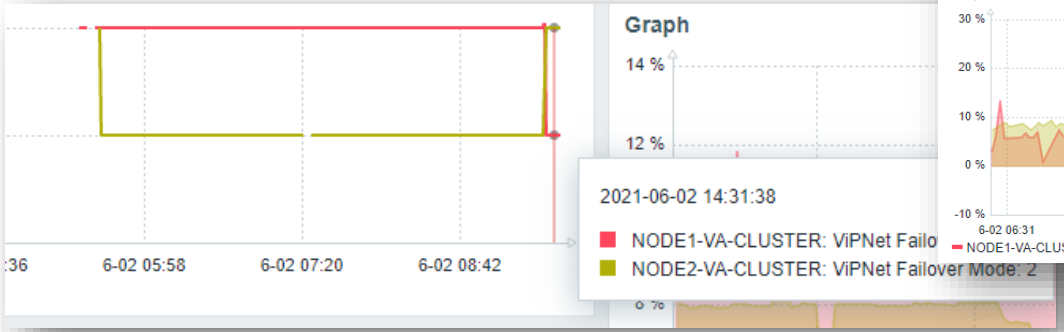


Мониторинг пассивного узла кластера

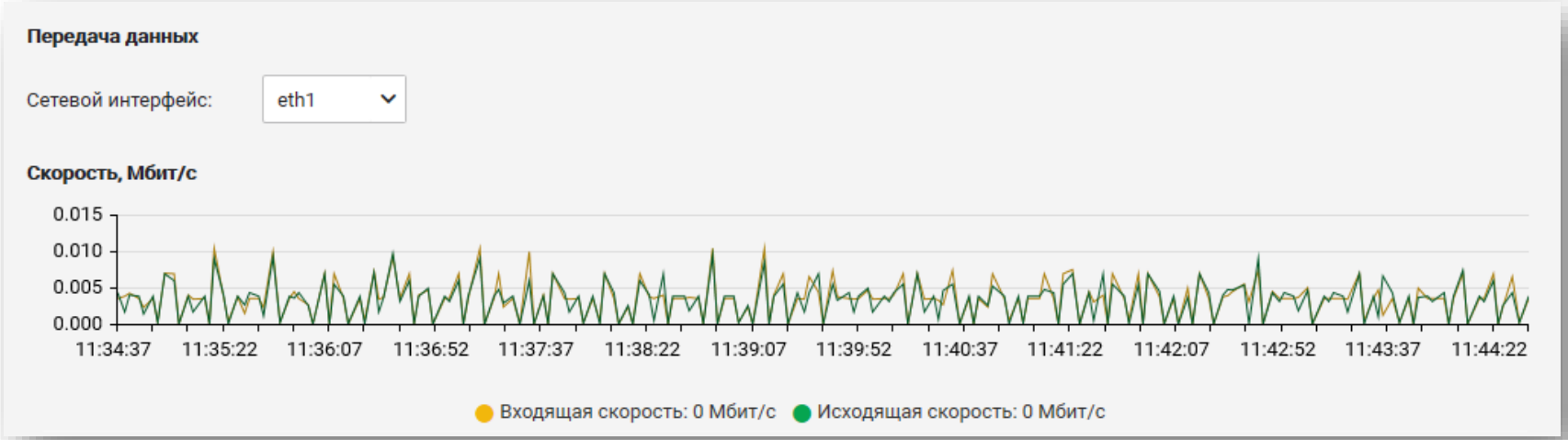
ViPNet FailoverIp	10.1.2.1	10.1.2.2
ViPNet Failover Mode	ClusterActive (2)	ClusterPassive (1)
ViPNet Failover Node Visibility Status	Reachable (1)	Reachable (1)
ViPNet Failover Other Cluster Node Ip	10.1.2.2	10.1.2.1
ViPNet FailoverSendconfig Interface Name	eth2	eth2
ViPNet Failover Sync Connections count	2 conn	2 conn
ViPNet Last Failover Event DateTime	Wed Jun 2 05:31:58 ...	Wed Jun 2 07:24:18 ...





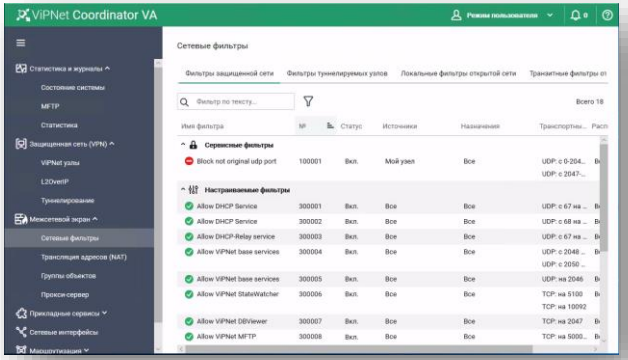


Утилизация сетевых интерфейсов

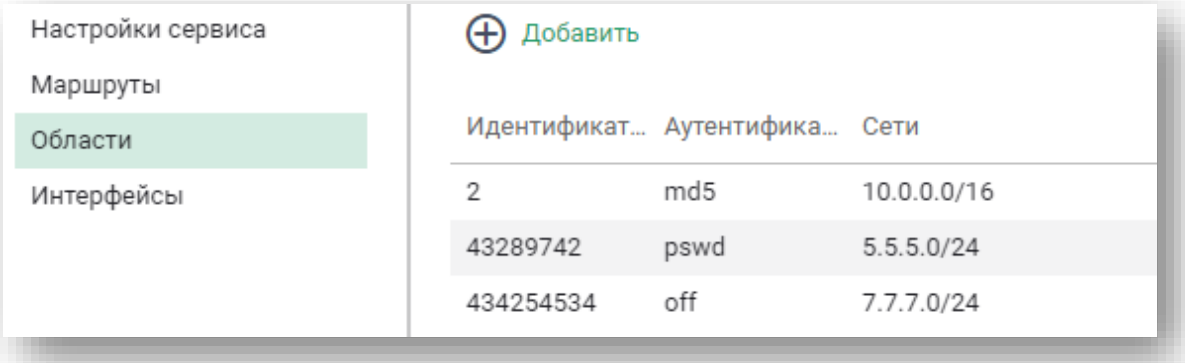


Повышение безопасности

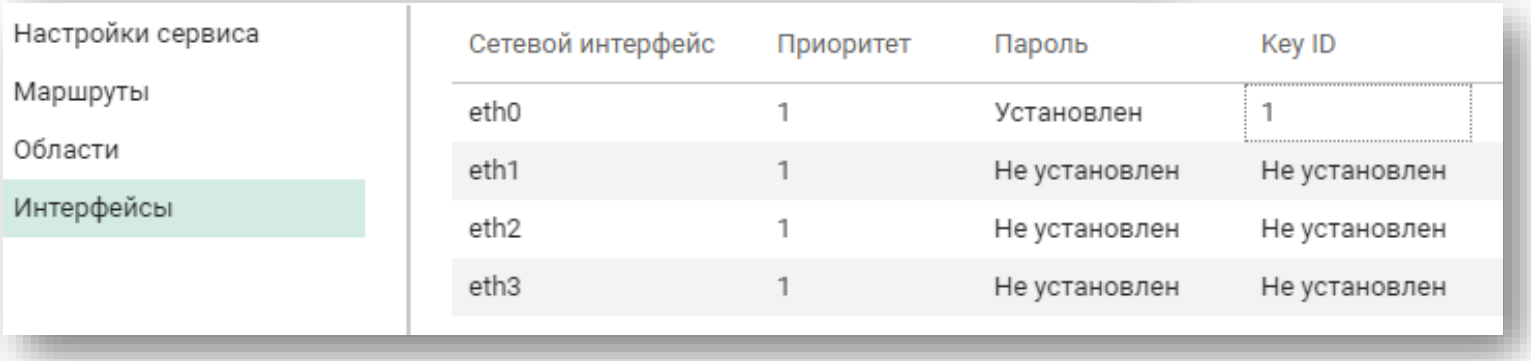
- Поддержка протокола SNMPv3
- Работа веб-интерфейса по HTTPS (AES)
- Поддержка аутентификации OSPF



Поддержка аутентификации OSPF



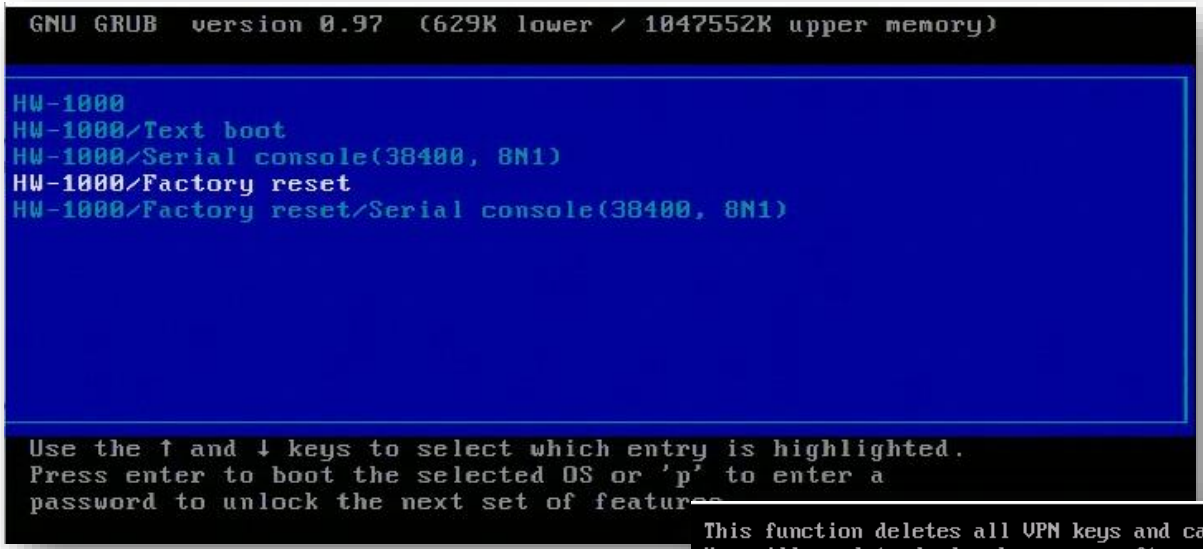
- Пароль
- MD5

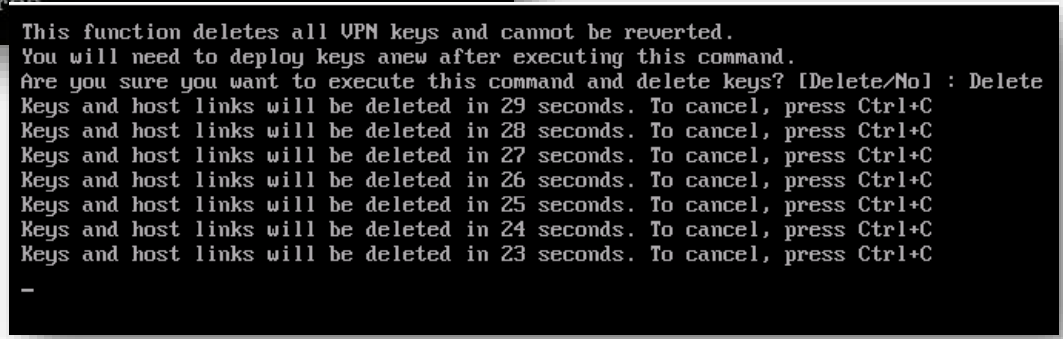


Сервисные функции

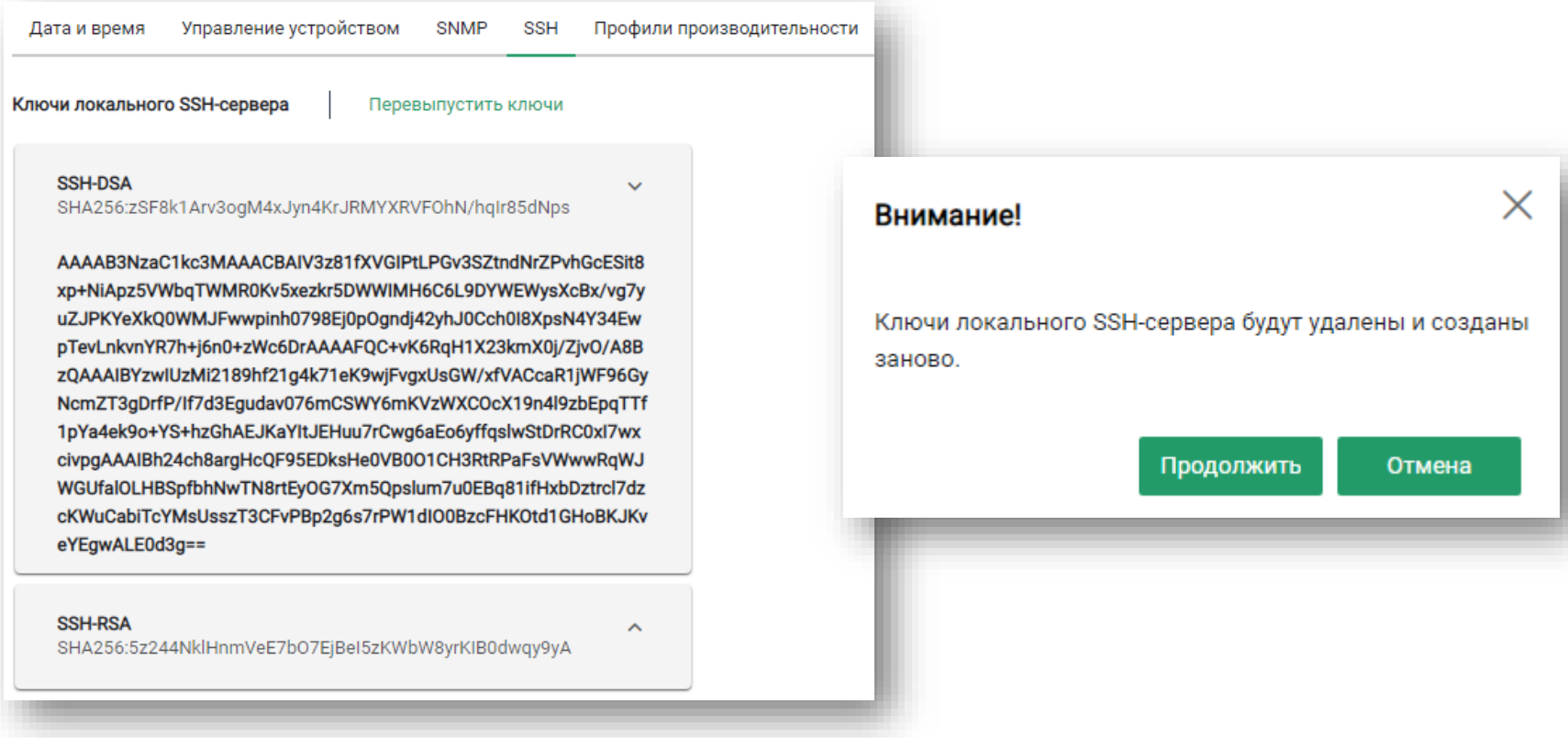
- Возврат к заводским настройкам
- Управление отпечатками SSH-ключей
- Локальное обновление справочников и ключей
- Управление перезагрузкой и службами ALG в WebUI

Возврат к заводским настройкам

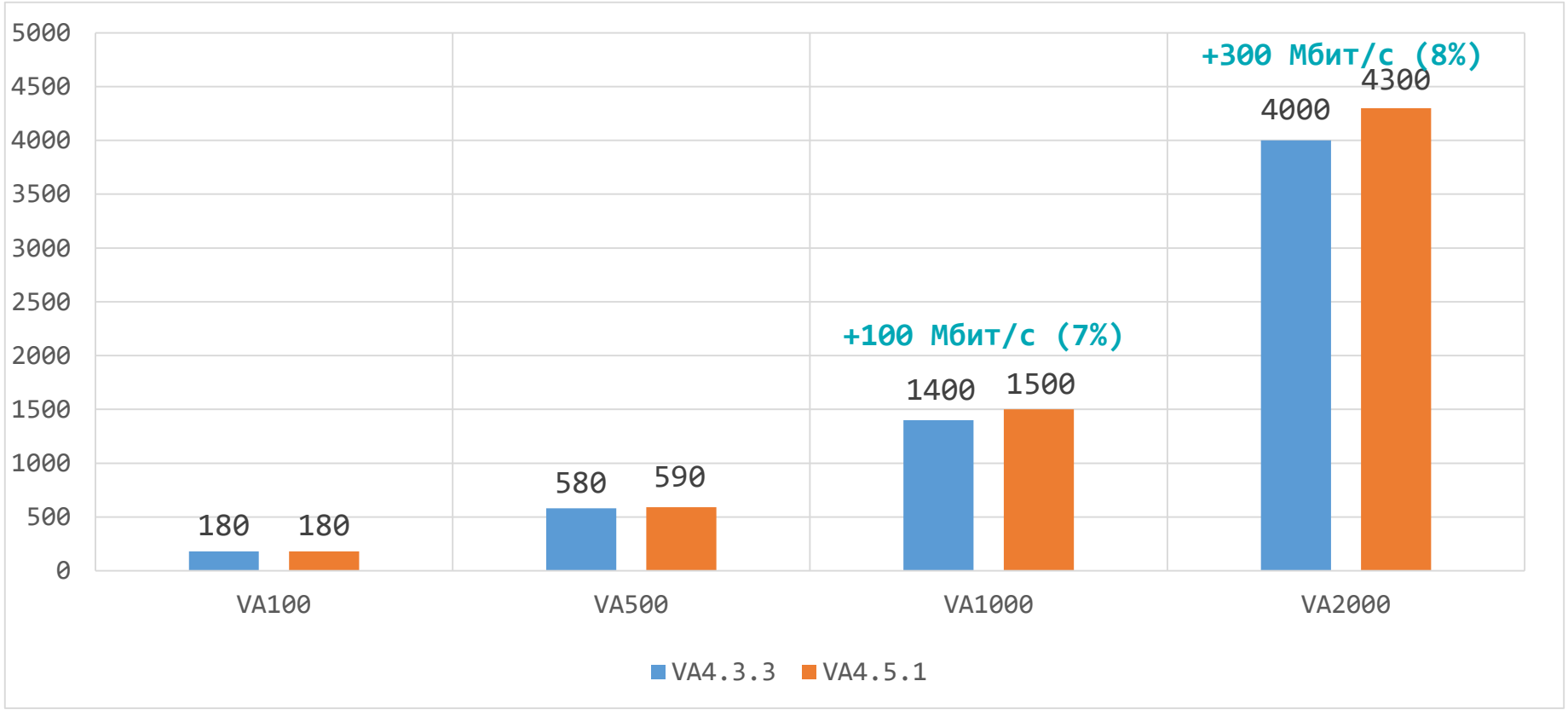




Управление отпечатками SSH-ключей



Производительность VPN (UDP)



Производительность FW (TCP)