

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

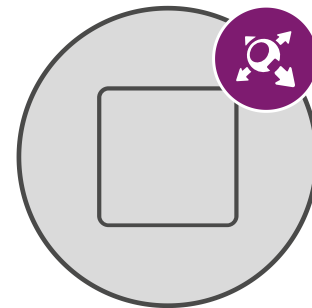


Ограничения:

- 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

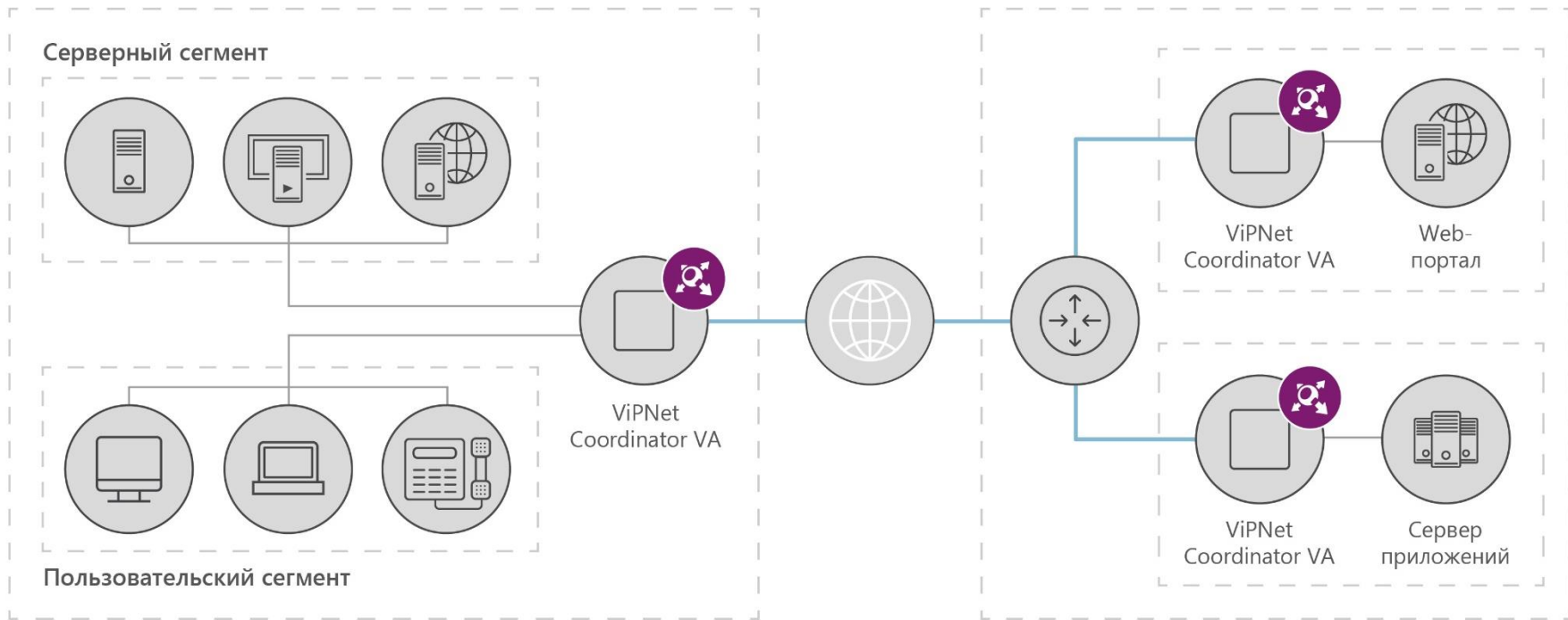


Сценарии использования

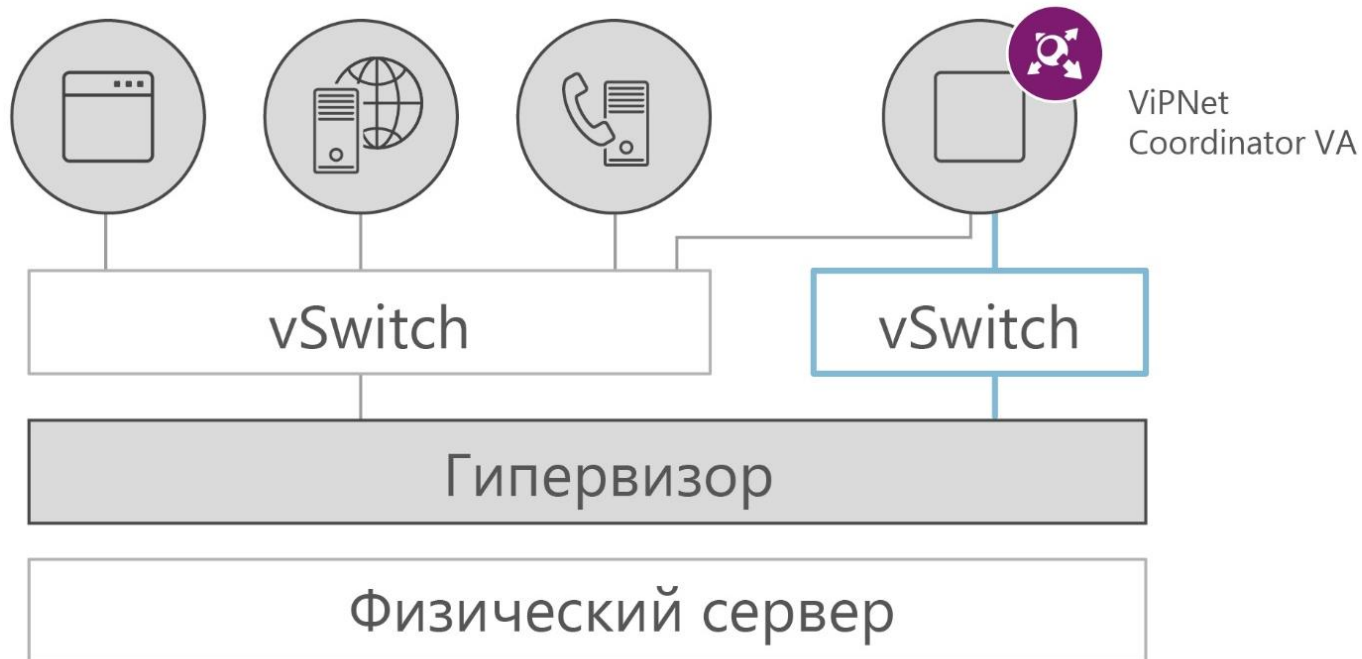
Сегментация сетей и безопасность частного облака

Центральный офис

Датацентр



Сетевая безопасность внутри виртуальной инфраструктуры



Защищенные каналы



Открытые каналы



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

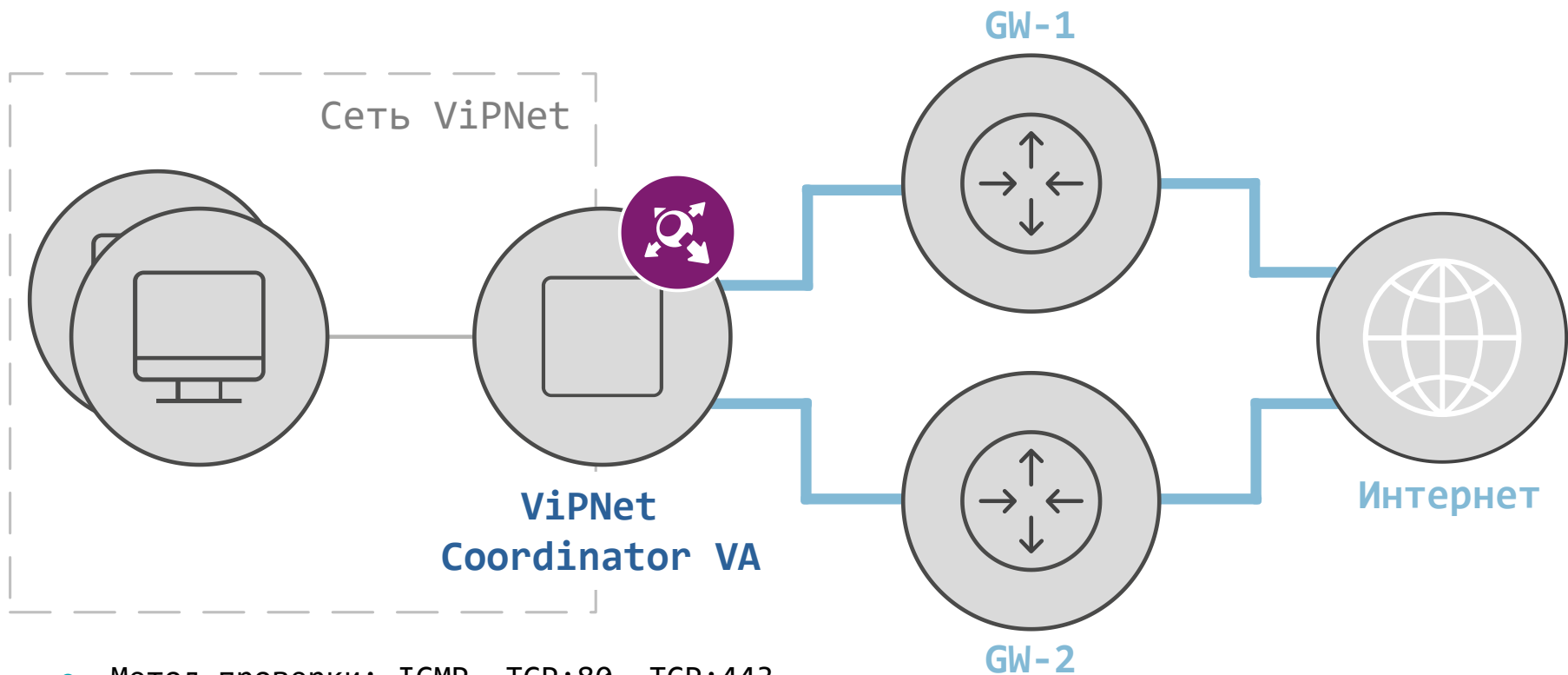
- MultiWAN: Резервирование и балансировка
- Динамическая маршрутизация
- Политики маршрутизации (PBR)
- Поддержка VLAN
- Агрегирование сетевых интерфейсов
- Классификация и приоритизация трафика



СЕРВИСНЫЕ ФУНКЦИИ

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

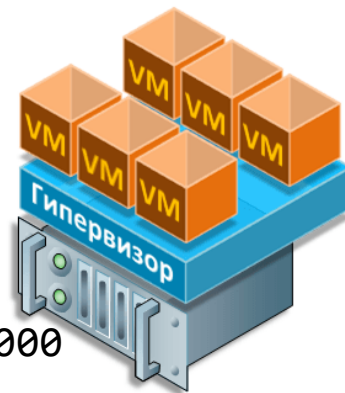
MultiWAN: Резервирование и балансировка



- 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)



ViPNet Coordinator VA Режим пользователя

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...	Расп
Сервисные фильтры						
Block not original udp port	100001	Вкл.	Мой узел	Все	UDP: с 0-204...	Вкл.
Настраиваемые фильтры						
Allow DHCP Service	300001	Вкл.	Все	Все	UDP: с 67 на ...	Вкл.
Allow DHCP Service	300002	Вкл.	Все	Все	UDP: с 68 на ...	Вкл.
Allow DHCP-Relay service	300003	Вкл.	Все	Все	UDP: с 67 на ...	Вкл.
Allow ViPNet base services	300004	Вкл.	Все	Все	UDP: с 2048 ...	Вкл.
					UDP: с 2050 ...	
Allow ViPNet base services	300005	Вкл.	Все	Все	UDP: на 2046	Вкл.
Allow ViPNet StateWatcher	300006	Вкл.	Все	Все	TCP: на 5100	Вкл.
					TCP: на 10092	
Allow ViPNet DBViewer	300007	Вкл.	Все	Все	TCP: на 2047	Вкл.
Allow ViPNet MFTP	300008	Вкл.	Все	Все	TCP: на 5000...	Вкл.

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

SNMP v3

Общие настройки

- Разрешить чтение OID
- Разрешить отправку trap-сообщений

[+ Пользователи](#)

Имя пользоват...	Хэш	Шифрование	Разрешение
defaultuser	MD5	Нет	Read

Добавить сетевой узел

* Адрес сетевого узла

Порт

162 UDP

Тип уведомлений

TRAP

Добавить пользователя

* Имя пользователя

* Пароль Подтверждение пароля Алгоритм хэширования

 MD5

- Разрешить чтение OID
- Разрешить отправку trap-сообщений
- Использовать AES-шифрование

Ключ шифрования Подтверждение ключа

[+ Сетевы...](#)

Адрес сетевого узла	Порт	Тип сообщений
---------------------	------	---------------

Мониторинг пассивного узла кластера

SNMP v3

Общие настройки

Контексты кластера

Контексты узлов кластера

Узел кластера	Контекст узла
10.1.2.1	Node1
10.1.2.2	Node2

SNMP v1/v2c

Чтение

Отправка

Комьюнити кластера

Мониторинг узлов кластера по протоколам SNMP v1/v2c

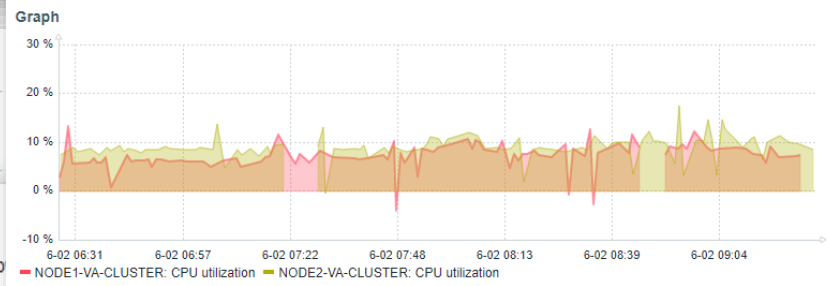
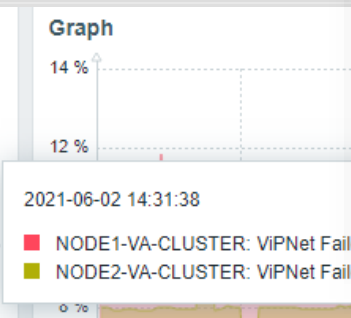
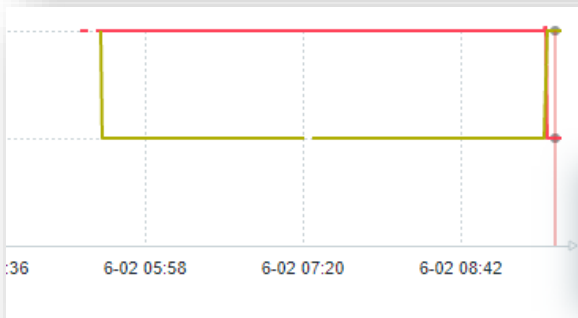
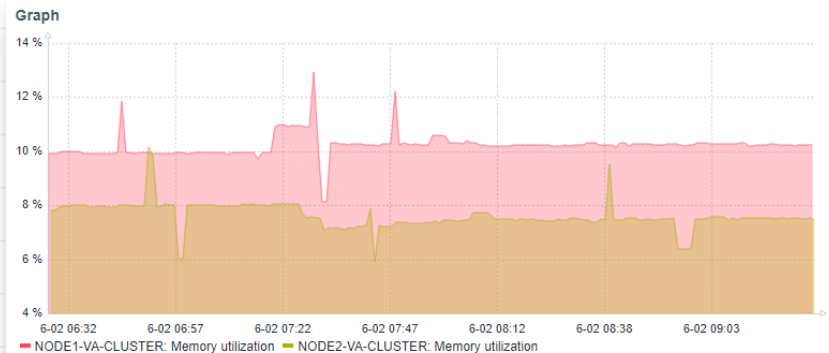
Для включения мониторинга узлов кластера необходимо назначить комьюнити каждому узлу кластера

Комьюнити кластера

Узел кластера	Строка комьюнити
10.1.2.1	—
10.1.2.2	—

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

Передача данных

Сетевой интерфейс:

eth1

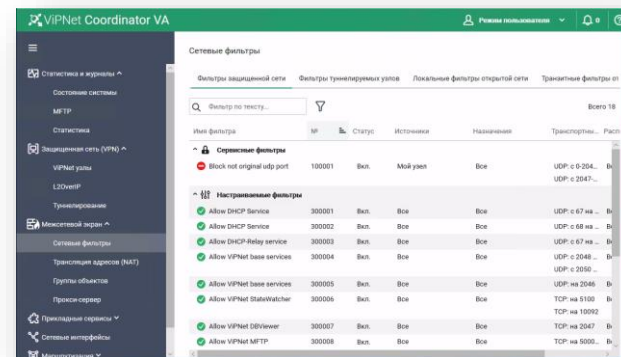
Скорость, Мбит/с



● Входящая скорость: 0 Мбит/с ● Исходящая скорость: 0 Мбит/с

Повышение безопасности

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



Поддержка аутентификации OSPF

Настройки сервиса	⊕ Добавить		
Маршруты	Идентификат...	Аутентифика...	Сети
Области	2	md5	10.0.0.0/16
Интерфейсы	43289742	pswd	5.5.5.0/24
	434254534	off	7.7.7.0/24

- Пароль
- MD5

Настройки сервиса	Сетевой интерфейс	Приоритет	Пароль	Key ID
Маршруты	eth0	1	Установлен	1
Области	eth1	1	Не установлен	Не установлен
Интерфейсы	eth2	1	Не установлен	Не установлен
	eth3	1	Не установлен	Не установлен

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

```
GNU GRUB version 0.97 (629K lower / 1047552K upper memory)
```

```
HW-1000
HW-1000/Text boot
HW-1000/Serial console(38400, 8N1)
HW-1000/Factory reset
HW-1000/Factory reset/Serial console(38400, 8N1)
```

```
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS or 'p' to enter a
password to unlock the next set of features.
```

```
This function deletes all UPN keys and cannot be reverted.
You will need to deploy keys anew after executing this command.
Are you sure you want to execute this command and delete keys? [Delete/No] : Delete
Keys and host links will be deleted in 29 seconds. To cancel, press Ctrl+C
Keys and host links will be deleted in 28 seconds. To cancel, press Ctrl+C
Keys and host links will be deleted in 27 seconds. To cancel, press Ctrl+C
Keys and host links will be deleted in 26 seconds. To cancel, press Ctrl+C
Keys and host links will be deleted in 25 seconds. To cancel, press Ctrl+C
Keys and host links will be deleted in 24 seconds. To cancel, press Ctrl+C
Keys and host links will be deleted in 23 seconds. To cancel, press Ctrl+C
```

Управление отпечатками SSH-ключей

Дата и время | Управление устройством | SNMP | **SSH** | Профили производительности

Ключи локального SSH-сервера | [Перевыпустить ключи](#)

SSH-DSA ▼
SHA256:zSF8k1Arv3ogM4xJyn4KrJRMXYRVFOhN/hqlr85dNps

AAAAB3NzaC1kc3MAAACBAIV3z81fXVGIPtLPGv3SZtndNrZPvhGcESit8xp+NiApz5VWbqTWMR0Kv5xezkr5DWWIMH6C6L9DYWEWysXcBx/vg7yuZJPKYeXkQ0WWMJFwwpinh0798Ej0pOgndj42yhJ0Cch0I8XpsN4Y34EwpTevLnkvnYR7h+j6n0+zWc6DrAAAAFQC+vK6RqH1X23kmX0j/Zjv0/A8BzQAAAIBYzwlUzMi2189hf21g4k71eK9wjFvgxUsGW/xfVACcaR1jWF96GyNcmZT3gDrFP/lf7d3Egudav076mCSWY6mKVzWXC0cX19n4l9zbEppTTf1pYa4ek9o+YS+hzGhAEJKaYItJEHuu7rCwg6aEo6yffqslwStDrRC0xl7wxcivpgAAAIbH24ch8argHcQF95EDksHe0VB001CH3RtRPaFsVWwwRqWJWGUfalOLHBSpfbhNwTN8rtEyOG7Xm5Qpsum7u0EBq81ifHxbDztrcl7dzcKWuCabITcYMsUsszT3CFvPBp2g6s7rPW1dIO0BzcFHK0td1GHoBKJKveYEgwALE0d3g==

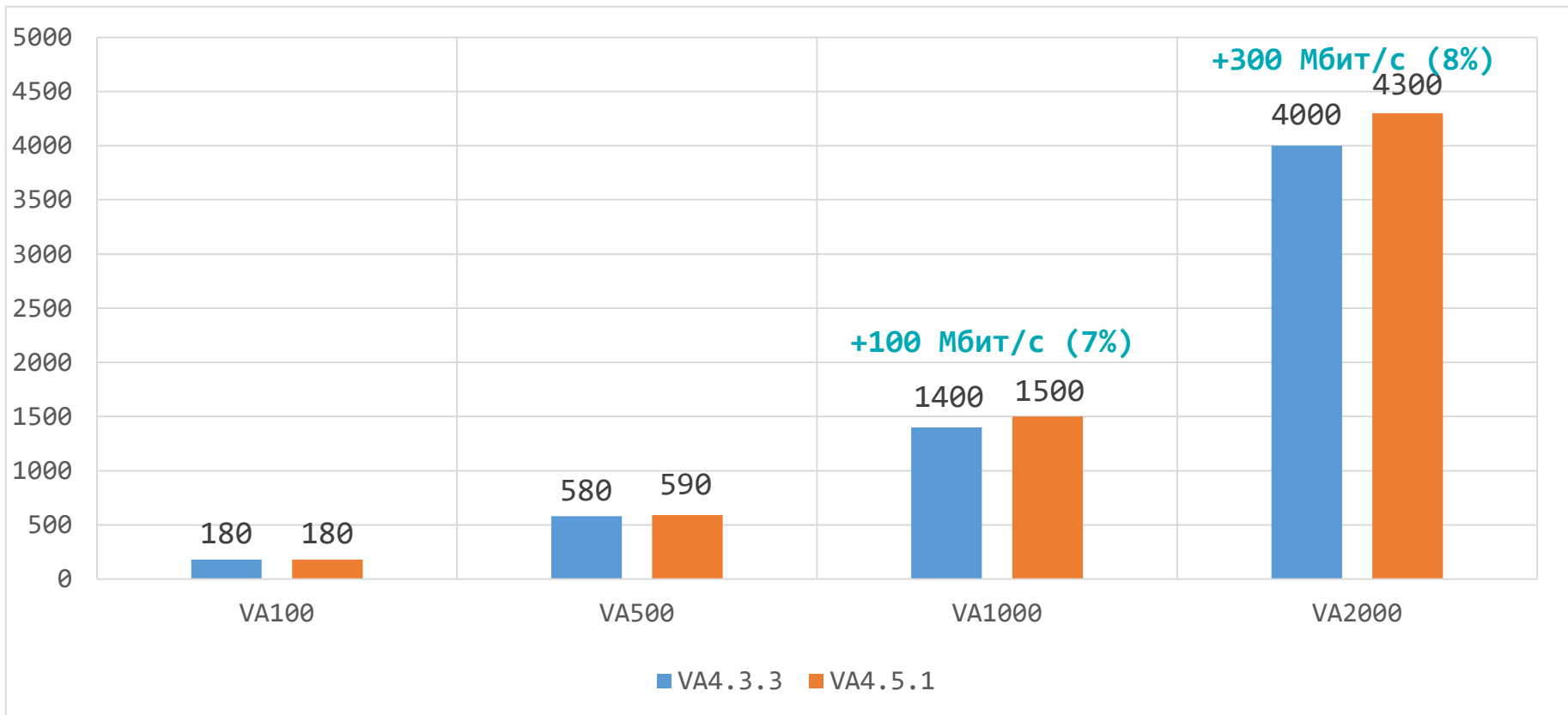
SSH-RSA ▲
SHA256:5z244NklHnmVeE7b07EjBel5zKWbW8yrKIB0dwqy9yA

Внимание! ✕

Ключи локального SSH-сервера будут удалены и созданы заново.

[Продолжить](#) [Отмена](#)

Производительность VPN (UDP)



Производительность FW (ТСР)

