С-Терра Бел: Сертифицированные решения по защите виртуализации

Сапрыкин А.М.
директор ООО «С-Терра Бел»
представитель НП «Инфофорум» в Республике Беларусь

Постановка проблемы

Эксплуатируемые в настоящее время в банках информационные системы, включая платежные, не имеют аттестата соответствия белорусскому законодательству по защите информации

Таким образом:

- де-факто не исполняется законодательство РБ по защите персональных данных
- государство, являясь гарантом сохранности вкладов белорусских граждан и надежности платежных систем, на практике, не имеет возможности оценить реальную безопасность банковских ИС. Поскольку иного варианта, кроме аттестации банковских ИС в национальной системе соответствия, не существует

Вывод: в банковских ИС необходимо применение сертифицированных средств защиты, соответствующих Положению об СКЗИ, утвержденному приказом ОАЦ № 62

Сертифицированные Bel VPN продукты версии 4.1

s•terra

Соответствуют Положению об СКЗИ, утвержденному приказом ОАЦ № 62, сертификаты соответствия со сроком действия по 26.06.2021г.

- Надежная защита передаваемого трафика:
  - технология IPsec VPN
  - национальные криптоалгоритмы (СТБ 34.101.31/45/66)
  - PKI-инфраструктура – поддержка сертификатов УЦ ГосСУОК
- Легкая интеграция в существующую инфраструктуру
- Масштабируемость, технологичность, универсальность

Bel VPN 4.1 – продукты для защиты сетей

s•terra

Bel VPN Gate 4.1 – масштабируемый набор программно-аппаратных комплексов Шлюз безопасности для защиты межсетевого обмена данных в распределенных IP-сетях

Поставляется на аппаратных платформах производства РБ, Lanner, Cisco, HP

Bel VPN Gate-V 4.1 – программный комплекс Шлюз безопасности виртуальный функционирует в виртуальных средах (Vmware, ESXi, Citrix XenServer, Microsoft Hyper-V, KVM)

Bel VPN L2 – программный модуль, расширяющий функциональные возможности шлюза безопасности. Предназначен для защиты сетевого трафика на канальном уровне (входит в состав шлюза)

Bel VPN 4.1 – продукты для защиты рабочих мест

s•terra

Bel VPN Client 4.1 – программно-аппаратное устройство, предназначенное для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности

Функционирует на вычислительных устройствах с ОС Windows

Bel VPN Client-M 4.1 – программный продукт для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности

Функционирует на мобильных устройствах (планшетах, смартфонах) с ОС Android

Bel VPN KP 4.1 – программный комплекс для централизованного управления и мониторинга продуктов Bel VPN 4.1

Функционирует под управлением ОС Windows Server

Преимущества виртуального шлюза Bel VPN Gate-V 4.1

s•terra

- функционирует в виртуальной машине, созданной в наиболее популярных гипервизорах, и обеспечивает полную функциональность Bel VPN Gate 4.1
- интеграция непосредственно в виртуальную инфраструктуру
- простая и быстрая установка и настройка
- масштабирование производительности шифрования трафика в зависимости от процессорных ядер: 1, 4, 12
- реализация сценариев обеспечения высокой доступности и отказоустойчивости
- гибкая адаптация к меняющимся задачам, сетевой инфраструктуре и приложениям
- эффективное использование вычислительных ресурсов
- экономия электроэнергии и места в стойке

vmware

XenServer® Open Source Virtualization

Microsoft Hyper-V

KVM

Масштабируемость Bel VPN Gate-V 4.1

s•terra

Производительность и возможности (масштабируемость) виртуального шлюза определяются лицензией, которой при необходимости можно сделать upgrade:

- VG-100-C1-D-AV – до 10 туннелей с ограничением на 1 ядро
- VG-1000-C4-D-AV – до 50 туннелей с ограничением до 4-х ядер
- VG-3000-C12-D-AV – до 1000 туннелей с ограничением до 12-х ядер

Минимально необходимые ресурсы для старта Bel VPN Gate-V 4.1:

- Количество процессорных ядер – от 1
- Оперативная память - от 1 GB
- Жесткий диск – от 4 GB
- Образ виртуальной машины Gate-V OVF/OVA

KVM

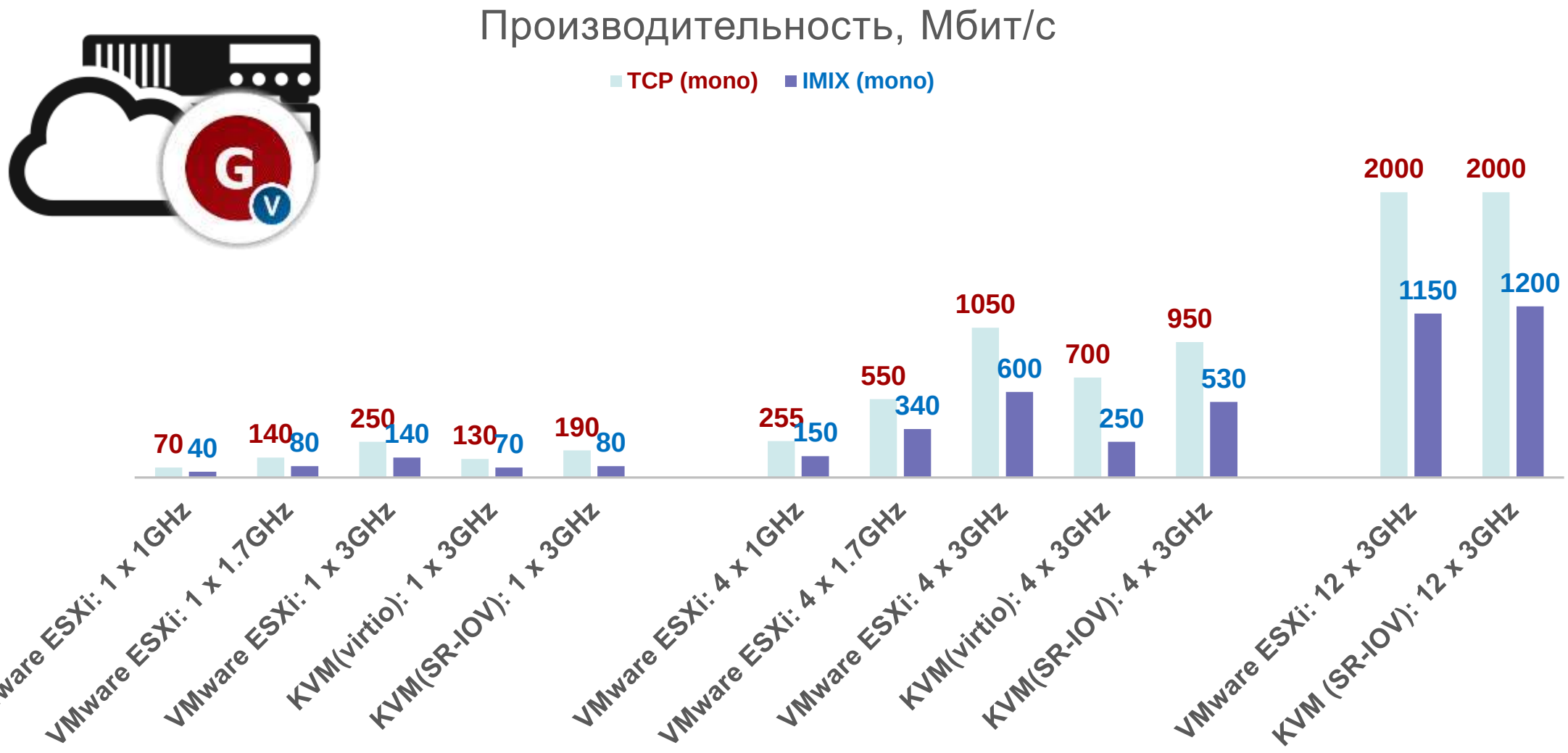
vmware

XenServer® Open Source Virtualization

Microsoft Hyper-V

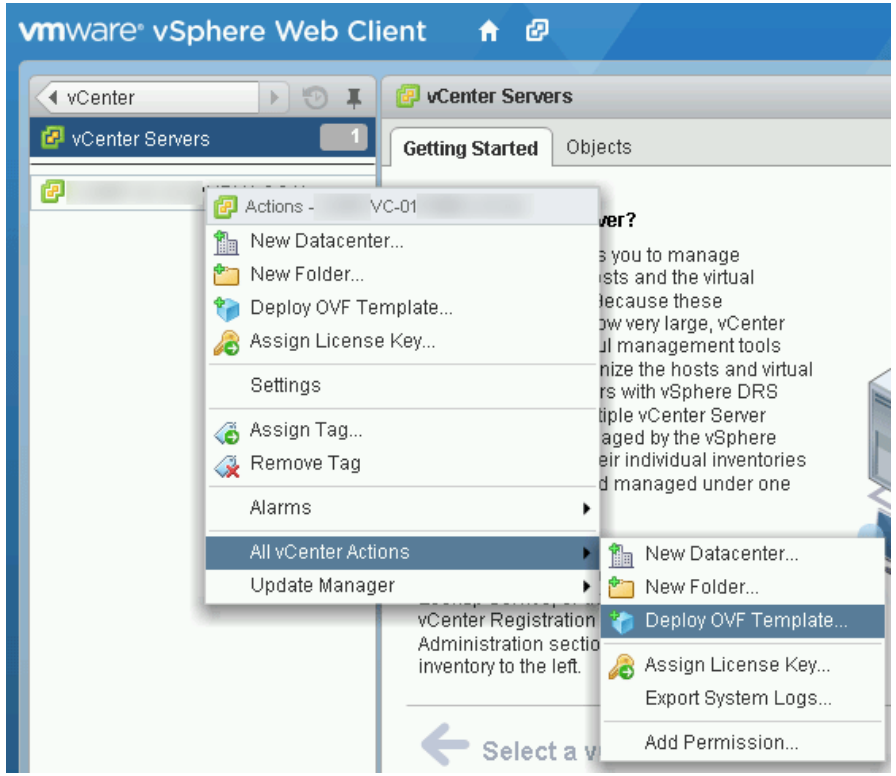
Производительность Bel VPN Gate-V 4.1

s•terra

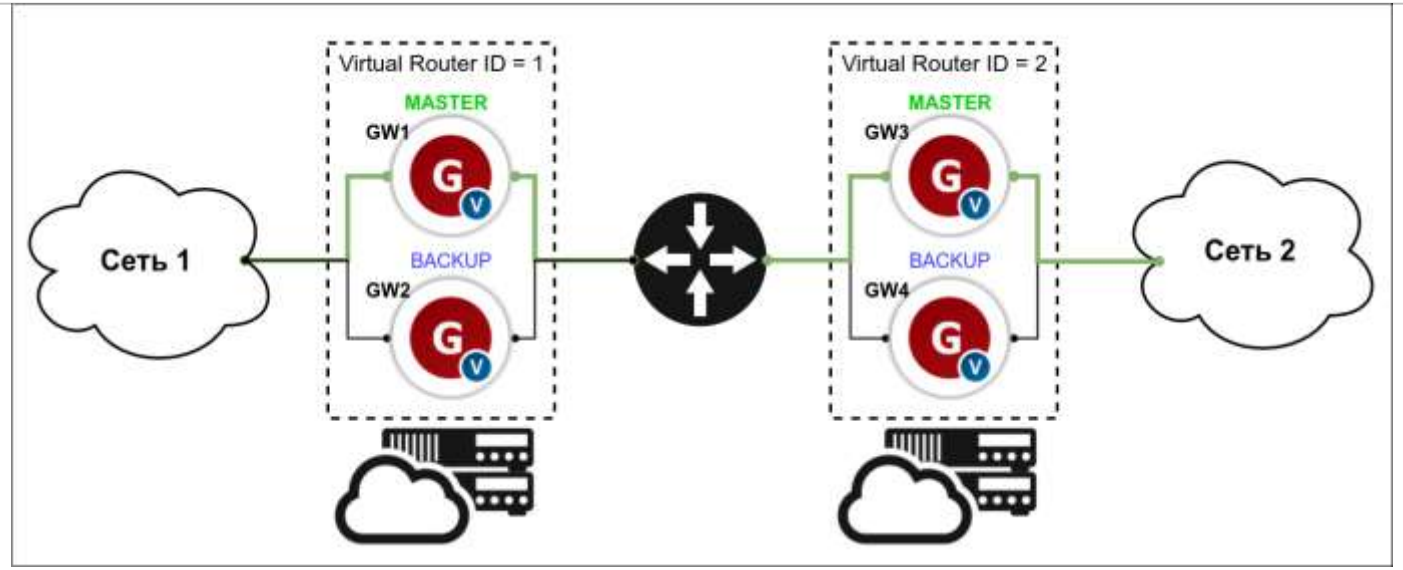


Отказоустойчивость

- Быстрая доставка и установка
- Возможность использования “snapshot”
- Методы обеспечения отказоустойчивости средствами среды виртуализации (HA, fault tolerance)
- Кластер VRRP – защита от:
  - отключения питания
  - выхода из строя аппаратной платформы
  - отказа сетевого интерфейса
  - отказа порта на коммутационном оборудовании
  - отказа подсистемы шифрования трафика

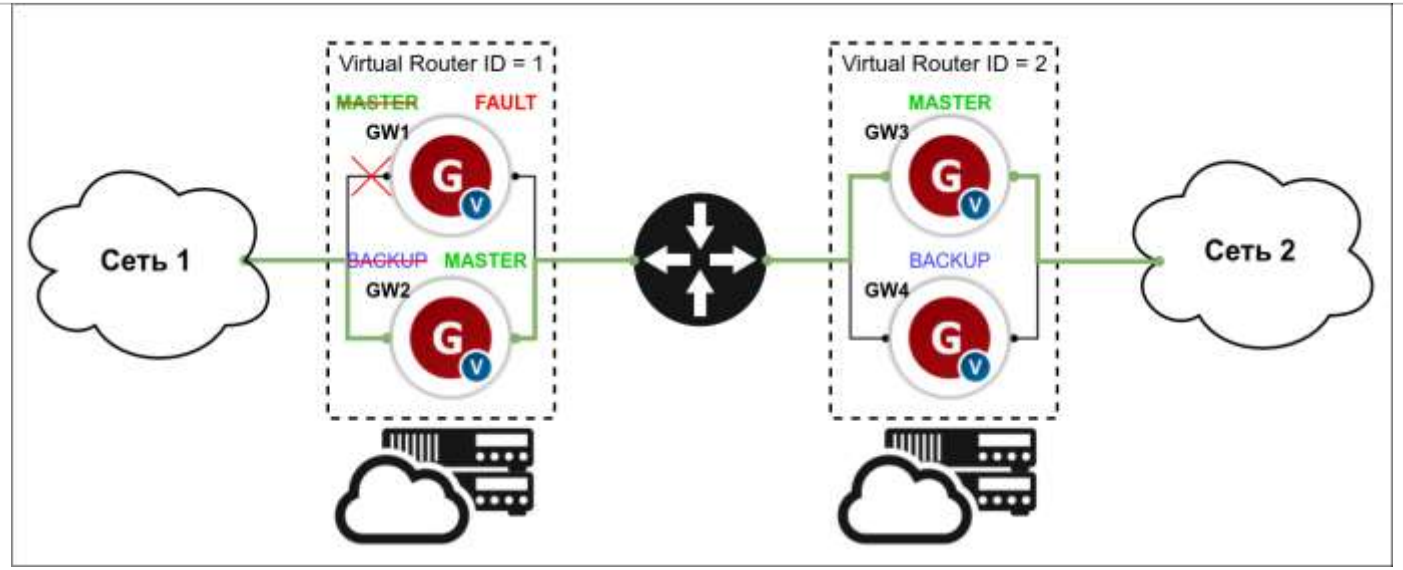


Сценарий применения на базе VRRP



- Шлюзы GW1 и GW2 объединены в виртуальный маршрутизатор (Virtual Router) с идентификатором 1, GW3 и GW4 – в виртуальный маршрутизатор с идентификатором 2
- При использовании протокола VRRP шлюзы каждого кластера имеют разделяемый виртуальный адрес во внутреннем сегменте (защищаемом) сети и внешнем (публичном)
- Один из шлюзов является главным – **MASTER**
- Второй является второстепенным – **BACKUP**
- В каждый момент времени виртуальный адрес может быть только на шлюзе, который находится в состоянии **MASTER**

Сценарий применения на базе VRRP



- Трафик, идущий на виртуальный адрес, обрабатывает **MASTER**
- В случае выхода из строя главного шлюза, его состояние меняется с **MASTER** на **FAULT**, состояние второстепенного шлюза меняется с **BACKUP** на **MASTER**
- Второстепенный шлюз продолжает заниматься обработкой трафика
- Обнаружение недоступности шлюза, находящегося в состоянии **MASTER** происходит благодаря обмену служебными пакетами протокола **VRRP**
- При возвращении в строй главного шлюза, трафик снова будет обрабатываться на нем

Bel VPN Client 4.1 – удаленный доступ и не только

s•terra

- Криптозащита сетевого трафика по протоколам IKE/IPsec
- Пакетная и statefull фильтрация трафика
- Протоколирование Syslog и мониторинг SNMP
- Интеграция с Radius сервером
- Получение сетевых настроек по IKECFG (виртуальный адрес)
- Инструментарий для массового развертывания
- Централизованное управление: локальная политика безопасности, ключевые контейнеры и сертификаты

Microsoft Windows xp Windows 7 Windows 8 Windows 10 Windows Server 2012

Практика применения Bel VPN 4.1 в банках

s•terra

Bel VPN продукты применяются на практике для защиты:

- межбанковского взаимодействия
- центров обработки данных (ЦОД)
- корпоративного (ведомственного) межсетевого взаимодействия

между офисами банков, в том числе, с помощью виртуальных шлюзов

- удаленного доступа с устройств, работающих под ОС Windows и Андроид

Проводится тестирование для защиты каналов связи с устройствами самообслуживания (банкоматами, инфокиосками, терминалами)

Microsoft Windows xp Windows 7 Windows 8 Windows 10 Windows Server 2012

Техническая поддержка

s•terra

РАСШИРЕННАЯ

- Скидка на обновление до следующей сертифицированной версии
- Выезд инженера на площадку Заказчика

СТАНДАРТНАЯ

- Дистанционно – телефон/ e-mail/ портал технической поддержки
- Бесплатно первый год

Спасибо за внимание

s·terra®

220012, г.Минск
ул.Чернышевского, 10А, пом.611

(+375 17) 280 6000

info@s-terra.by

www.s-terra.by