

V Конференция «IT-Security Conference 2019»



Преимущества решений С-Терра Бел

Сапрыкин А.М.

директор ООО «С-Терра Бел»,

член Оргкомитета международной конференции «Инфофорум»



s•terra®

25-26 марта 2019 г., Ренессанс отель, г. Минск





программно-аппаратный комплекс **«Шлюз безопасности Bel VPN Gate 4.1»** – масштабируемый набор шлюзов, предназначенся для защиты межсетевого обмена данных в территориально распределенных IP-сетях

Поставляется на аппаратных платформах производства РБ, а также Lanner и Cisco



программный комплекс **«Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»** по функциональности аналогичен ПАК, работает в виртуальных средах (VMware, ESXi, Citrix XenServer, Microsoft Hyper-V, KVM)



программно-аппаратное устройство **«Клиент безопасности Bel VPN Client 4.1»** предназначен для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности, функционирует под ОС Windows



программный продукт **«Клиент безопасности Bel VPN Client-P 4.1»** по функциональности аналогичен ПАУ, имеет улучшенные характеристики и работает со всеми версиями ОС Windows

Состав Bel VPN продуктов версии 4.1



программный продукт **«Клиент безопасности мобильный Bel VPN Client-M 4.1»** предназначен для защиты доступа удаленного пользователя к ведомственной сети, защищаемой шлюзом безопасности

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



программный продукт **«Система централизованного управления Bel VPN КР 4.1»** предназначен для централизованного управления и мониторинга продуктами Bel VPN Gate 4.1/Client 4.1/Client-P 4.1/Client-M 4.1 (входит в состав шлюза)

Функционирует под управлением ОС Windows Server




программный модуль **«Bel VPN L2»** предназначен для защиты сетевого трафика на канальном уровне (входит в состав шлюза)

Основные преимущества Bel VPN продуктов

- функционально полный набор средств сетевой криптографической защиты информации:
 - масштабируемые программно-аппаратные шлюзы безопасности **Bel VPN Gate** по производительности и кол-ву туннелей шифрования - от 50 Мб/с до 4 Гб/с и от 10 туннелей шифрования до неограниченного кол-ва
 - наличие виртуальных решений - Bel VPN Gate-V
 - возможность удаленного доступа - Bel VPN Client-P, Bel VPN Client-M
 - наличие системы централизованного управления - Bel VPN KP
 - наличие возможности работы на канальном уровне - Bel VPN L2
- наличие межсетевого экрана **МЭ**
- работа с технологическими сертификатами **ГосСУОК**
- маркировка и приоритезация трафика **QoS**
- событийное протоколирование **Syslog**, мониторинг **SNMP**
- наличие отказоустойчивых (кластерных) решений **VRRP** и балансировка **RRI**
- для управления используется **cisco-like** система команд



 Программно-аппаратный комплекс «Шлюз безопасности **Bel VPN Gate 4.1**» – системообразующий элемент построения территориально распределённых IP-сетей

Применение масштабируемых (по производительности и количеству туннелей) шлюзов в сочетании с удалённым доступом (клиентами) дают **высокий экономический эффект!**

- предлагается перечень масштабируемых шлюзов, различающихся по производительности: 50, 250, 500, 750 Мб/с, 1 Гб/с, 2,8 Гб/с, 3,5 Гб/с и количеству туннелей шифрования: 5, 10, 50, 1000 и неограниченному количеству
- Обеспечивает:
 - защиту транзитного и собственного трафика
 - пакетную и statefull фильтрацию трафика, туннелирование (маскировку топологии)
 - протоколы IPsec ESP/AH, IKE, PKI
 - работу с ТСОК ГосСУОК
 - маркировку и приоритезация трафика (QoS)
 - событийное протоколирование Syslog, мониторинг SNMP
 - горячее резервирование по VRRP, балансировку по RRI и т.д.

Бевалекс
вместе – от идеи к решению





Программный комплекс «Шлюз безопасности виртуальный **Bel VPN Gate-V**» обеспечивает функциональность Bel VPN Gate в виртуальных средах (VMware ESXi, Citrix XenServer, Microsoft Hyper-V). Производительность зависит от аппаратной платформы

○ Преимущества:

- интеграция непосредственно в виртуальную инфраструктуру
- простая и быстрая установка и настройка
- высокая производительность шифрования трафика
- реализация сценариев обеспечения высокой доступности и отказоустойчивости
- оперативная адаптация к меняющимся задачам и требованиям сетевых приложений и инфраструктуры
- легкое сохранение или восстановление резервной копии
- эффективное использование вычислительных ресурсов
- экономия электроэнергии и места в стойке

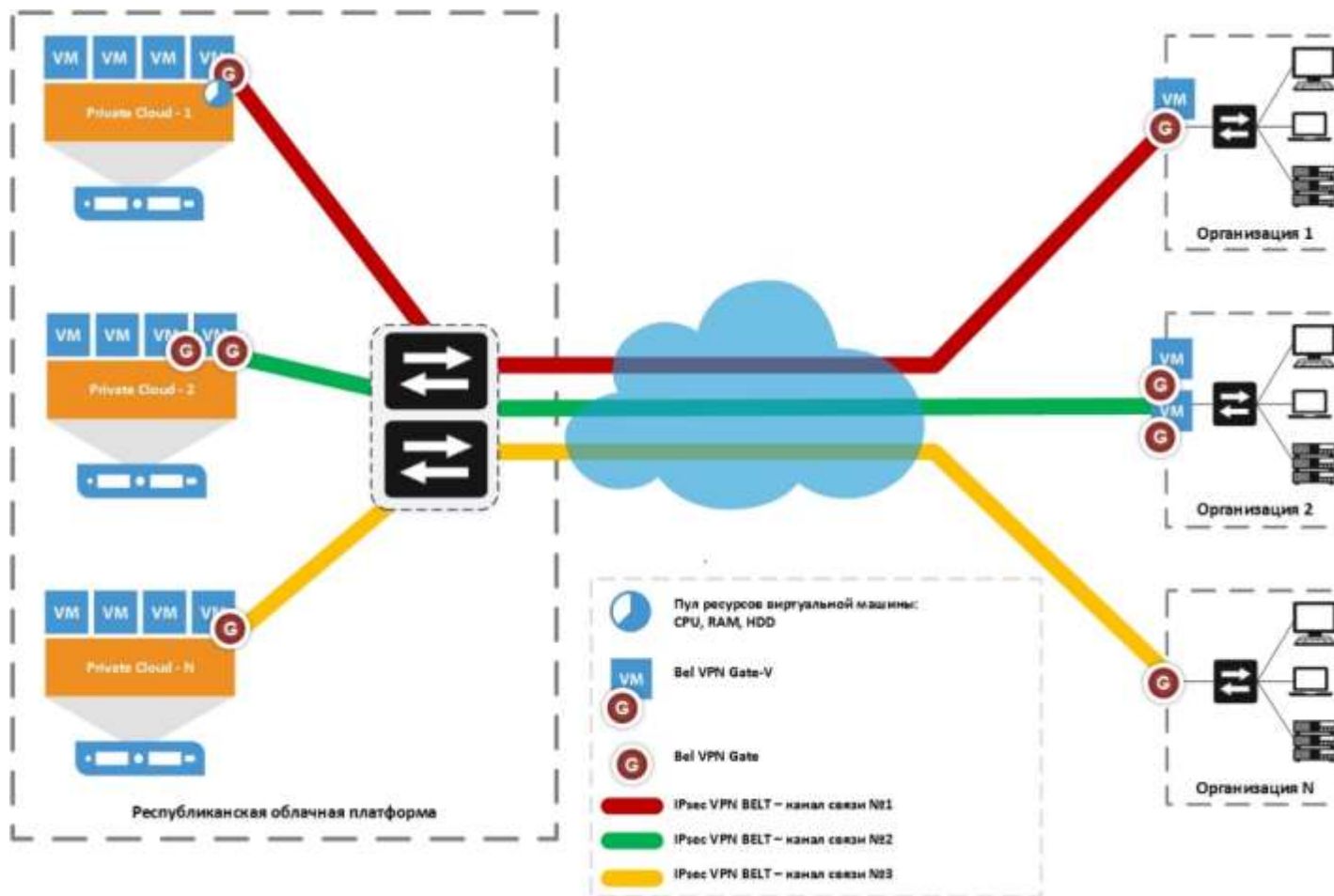
XenServer[®]
Open Source Virtualization

 Microsoft
Hyper-V

 KVM

vmware[®]

Применение Bel VPN Gate-V 4.1 на платформе VeCloud, дата центре Велком



vmware®

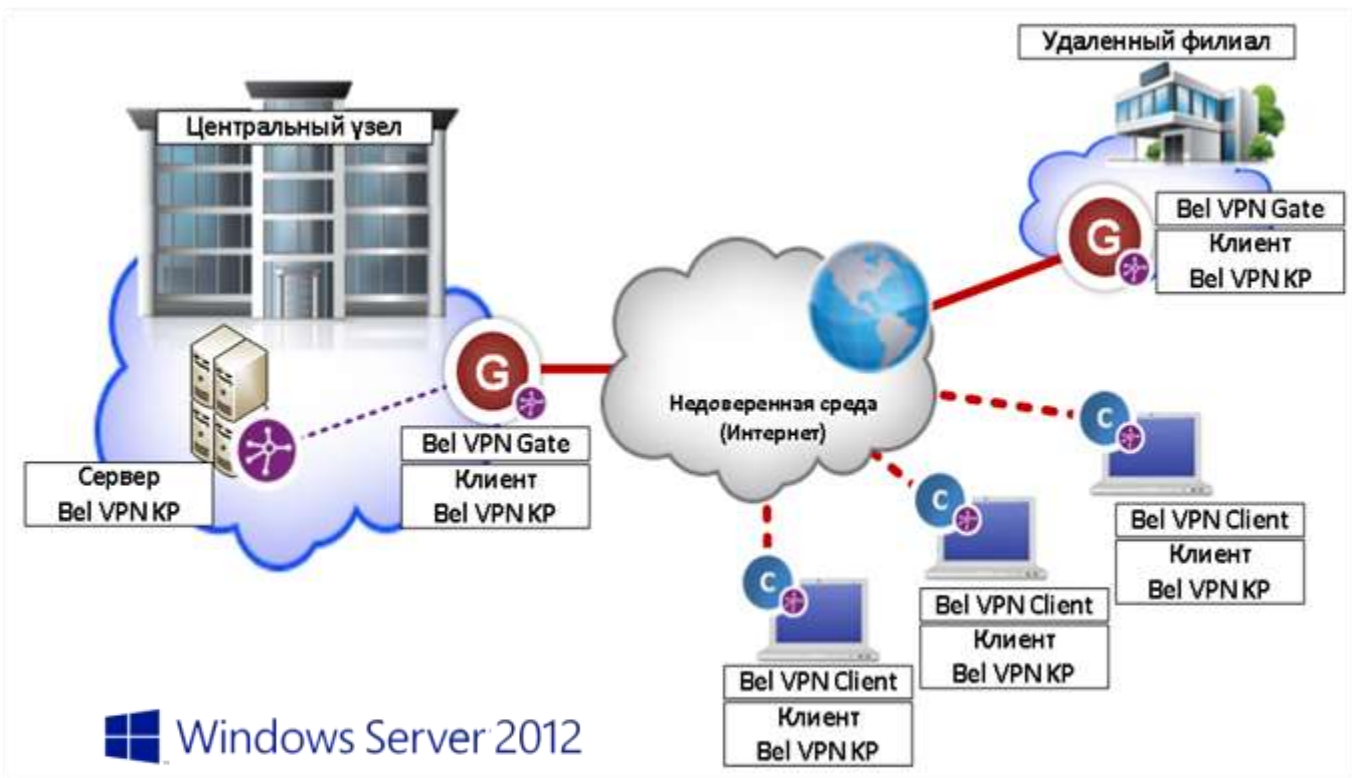


XenServer®
Open Source Virtualization





Система централизованного управления **Bel VPN KP** - для управления и мониторинга Bel VPN продуктов



- позволяет изменять политику безопасности, сертификаты, списки отозванных сертификатов, настройки логирования, формировать ключевую пару непосредственно на VPN-устройстве
- обеспечивает возможность сохранения и быстрого восстановления конфигурационных данных управляемых устройств
- поддерживает дополнительные функции по сбору сообщений из журнала регистрации событий, сбору настроек, обновлению настроек клиентов и др.

Механизмы обеспечения отказоустойчивости VRRP и балансировки RRI

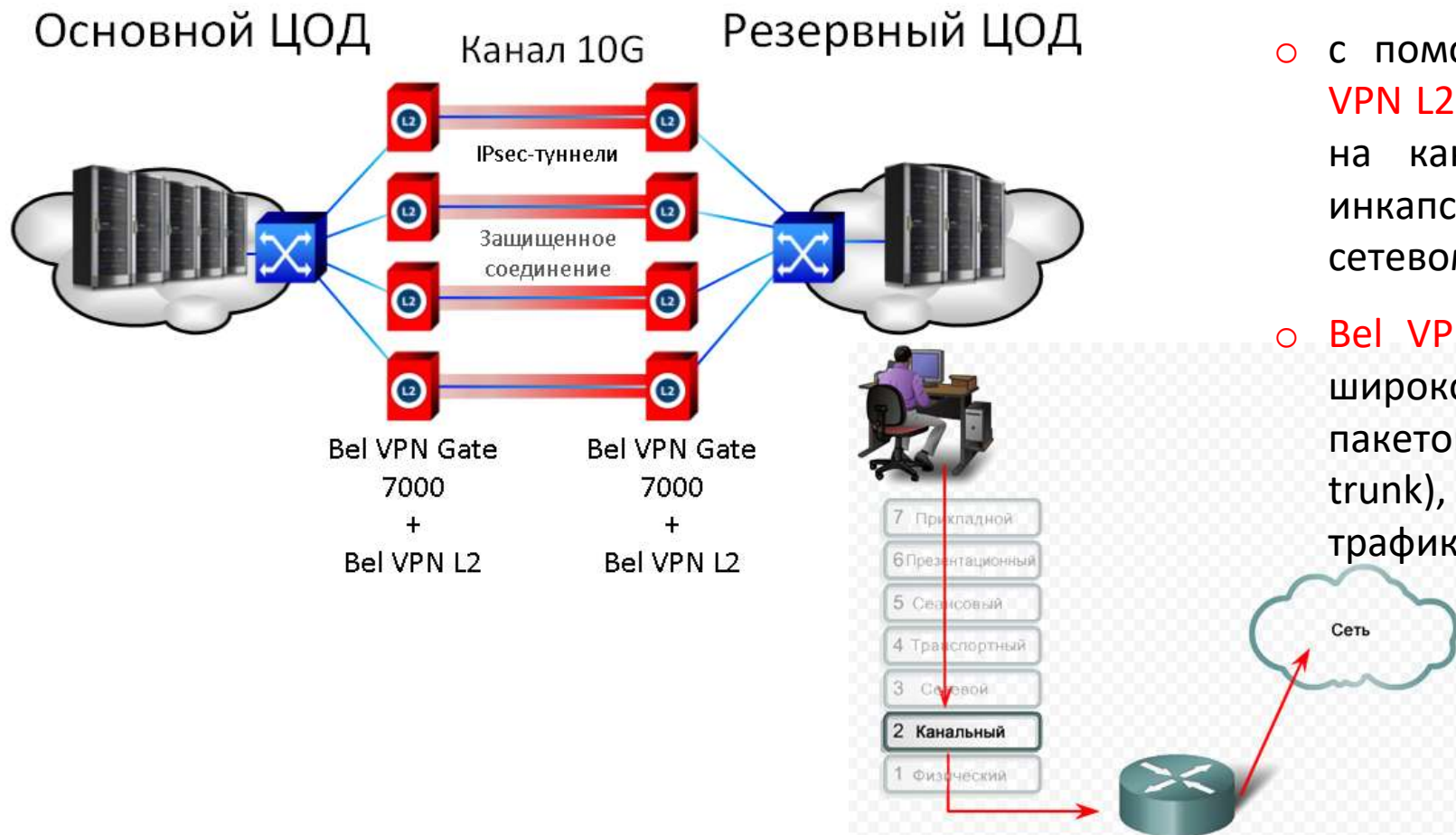
Protocol Virtual Router Redundancy (VRRP)



Protocol Reverse Route Injection (RRI)

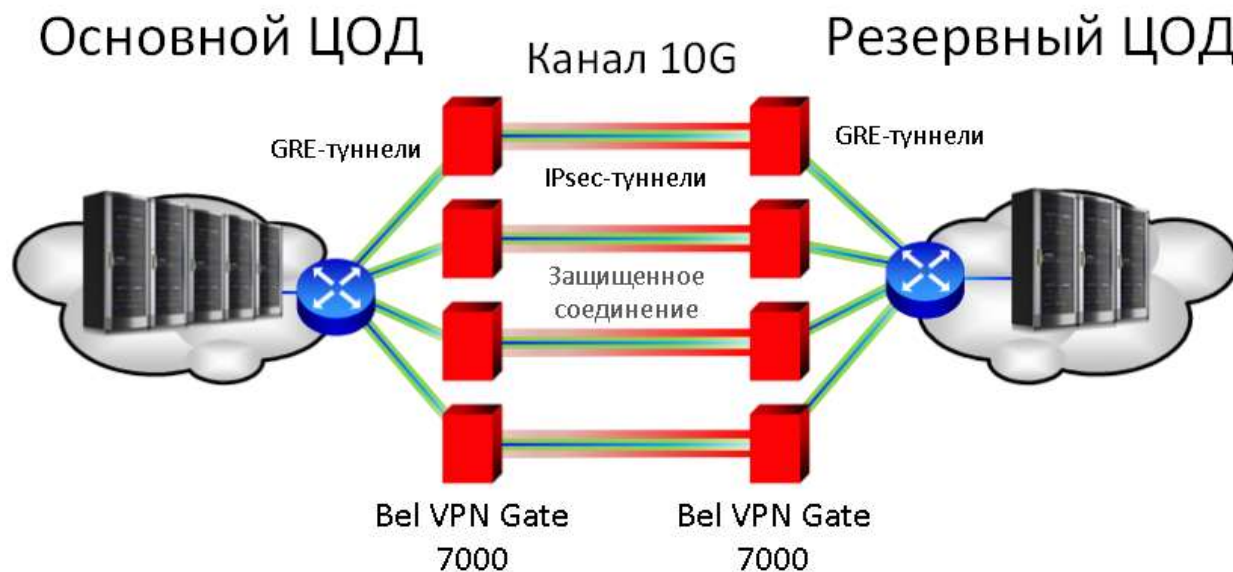


Защита ЦОД и высокопроизводительных каналов с помощью **Bel VPN L2**



- с помощью программного модуля **Bel VPN L2** осуществляется перехват трафика на канальном уровне с дальнейшей инкапсуляцией и шифрованием на сетевом уровне
- **Bel VPN L2** применяется при передаче широковещательных и мультикастовых пакетов, тегированного трафика (VLAN trunk), меток MPLS и других видов трафика

Защита ЦОД и высокопроизводительных каналов L3



- маршрутизаторы создают необходимое количество GRE-туннелей
- данные передаются по параллельным GRE-туннелям, каждый из которых защищается парой шлюзов безопасности
- балансировка и отказоустойчивость достигаются с помощью протокола динамической маршрутизации (OSPF или EIGRP)
- шлюзы безопасности настраиваются в работы в режиме защиты канала связи (site-to-site)
- маршрутизация настроена так, что данные основного и резервного ЦОДов доступны по различным маршрутам с одинаковой метрикой

Основные особенности в Bel VPN продуктах :



- интегрированная функциональность: пакетная фильтрация с контролем состояния соединения
- независимые наборы правил для входящего и исходящего трафика на каждом сетевом интерфейсе, как на входе так и на выходе VPN-туннеля
- управление правилами фильтрации выполняется в привычной для пользователя командной строке ОС маршрутизатора IOS(CLI)

Применение в Bel VPN продуктах технологических сертификатов открытого ключа ГосСУОК дает возможность построения защищенных ИС с **неограниченным количеством взаимодействующих доверенных продуктов!**

- Используется типовая структура сертификатов (X.509 v.3, CRL v.2), которая определена в международных стандартах ITU-T X.509 (ISO/IEC/ITU 9594-8) и RFC 2459 и состоит:
 - «тело» сертификата – формат, версия и серийный номер сертификата, атрибуты владельца (subject) и издателя (issuer) сертификата, значение открытого ключа, расширения сертификата
 - алгоритма ЭП, на котором произведена подпись удостоверяющего центра (certificate authority, CA)
 - ЭП удостоверяющего центра



- Стандартная:
 - дистанционно – телефон/e-mail/портал технической поддержки
 - обработка запросов по схеме 9/5 (с 9 до 18 в рабочие дни). Время реакции:
 - ✓ на запросы с уровнем важности «критичный» и «высокий» - 2 часа
 - ✓ на запросы с уровнем важности «средний» - 1 день
 - ✓ на запросы с уровнем важности «низкий» - 1 день
 - бесплатно первый год
 - предоставление замены на время ремонта неисправного шлюза
 - бесплатное предоставление патчей на обновление ПО
 - скидка на модернизацию СКЗИ при следующей сертифицированной версии
- Расширенная:
 - выезд инженера на площадку Заказчика, в том числе, в регионах
 - время на реакцию и устранение неисправностей - по усмотрению Заказчика
 - совместное оказание ТП с партнерами, оказывающими Заказчику услуги по обслуживанию сетевого оборудования на ежедневной основе (первая линия)

Дорожная карта Bel VPN продуктов (версия 5.0):

- внесение изменений в криптографические функции и МЭ Bel VPN продуктов в соответствии с Положением об СКЗИ
- перевод шлюзов на новую версию Linux
- разработка высокопроизводительной модели шлюза – проект «Шлюз 10 G», в том числе совместно с ЗАО «Авест»
- встраивание виртуальных шлюзов в сетевое оборудование ведущих мировых производителей – Cisco, Huawei, возможно, Check Point и др.
- улучшение функциональности шлюзов, клиентов, системы централизованного управления, в том числе, создание «кнопочного» интерфейса управления для упрощения настройки Bel VPN продуктов
- актуализация клиентов под новые версии Windows, Android (по мере их выпуска), разработка клиента под iOS
- «импортозамещение» - предложение белорусских аппаратных решений во всех сегментах моделей шлюзов по производительности

Спасибо за внимание



БЕЛОРУССКАЯ КРИПТОГРАФИЯ В СЕТЕВЫХ РЕШЕНИЯХ ЛЮБОЙ СЛОЖНОСТИ

220012, г.Минск, ул. Чернышевского, д. 10А

+375 (17) 280 60 00

info@s-terra.by, www.s-terra.by

s•terra[®]