Защита ЦОД и высокопроизводительных каналов связи: решения ООО «С-Терра Бел»

Сапрыкин А.М., директор ООО «С-Терра Бел»
представитель НП «Инфофорум»

2-я конференция «IT-Security Conference 2016»

29-30 марта 2016 года
Академия управления при Президенте Республики Беларусь, г. Минск

Bel VPN продукты версии 4.1

- в Bel VPN 4.1:
  - полномасштабное соответствие требованиям приказа ОАЦ «О некоторых вопросах технической и криптографической защиты информации» от 30 августа 2013 г. №62 (с изменениями и дополнениями согласно приказу от 15 января 2015г. №3), в частности:
    - шифрование и контроль целостности – СТБ 34.101.31-2011, ГОСТ 28147-89, СТБ П 34.101.50-2012
    - хэширование – СТБ 34.101.31-2011, СТБ 1176.1-99
    - электронная цифровая подпись – СТБ 1176.2-99, СТБ 34.101.45-2013 генерация случайных данных – СТБ 34.101.47-2012
    - управление ключами – СТБ 34.101.66-2014 (приложение А), управление криптографическими ключами, рекомендованное ОАЦ
    - поддержка сертификатов ГосСУОК, формат сертификатов и списков отозванных сертификатов – СТБ 34.101.19-2012
    - требования безопасности – СТБ 34.101.27-2011 (кл. 1), СТБ П 34.101.43-2009
    - межсетевой экран – СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014

Bel VPN продукты версии 4.1

- Продукты Bel VPN 4.1 включают следующий набор средств защиты сетевого уровня:

  - Bel VPN Gate 4.1 – масштабируемый набор программно-аппаратных шлюзов безопасности для защиты межсетевого обмена данных в распределенных корпоративных (ведомственных) сетях
  - Bel VPN Gate-V 4.1 – программный виртуальный шлюз безопасности, функционирующий в виртуальной среде (VMware ESXi, Citrix XenServer, Microsoft Hyper-V). Предназначен как для защиты периметра облачной инфраструктуры, так и взаимодействия между отдельными виртуальными машинами
  - Bel VPN Client 4.1 – программно-аппаратное устройство для защиты индивидуального (удаленного) пользователя
  - Bel VPN Client-M 4.1 – программный продукт для защиты мобильных устройств
  - Bel VPN KP 4.1 – программный модуль для централизованного управления Bel VPN продуктами (входит в состав шлюза как функциональная опция)
  - Bel VPN L2 – программный модуль для защиты на канальном уровне (входит в состав шлюза как функциональная опция)

Шлюз безопасности Bel VPN Gate 4.1

Bel VPN Gate 4.1 – системообразующий программно-аппаратный комплекс шлюз безопасности на базе серверных платформ HP, Cisco, Huawei, Kraftway, Tonk, Depo, а также белорусских производителей - Bevalex, TradeixBel, Belsoft, функционирующий под управлением ОС *Debian*

- Предлагается перечень масштабируемых шлюзов, различающихся по производительности – от 50 Мб/с до 5 Гб/с и количеству туннелей шифрования – от 10 туннелей до неограниченного количества
- Обеспечивает:
  - ✓ защиту транзитного и собственного трафика;
  - ✓ пакетную и statefull фильтрацию трафика, туннелирование (маскировку топологии)
  - ✓ протоколы IPsec ESP/AH, IKE, PKI
  - ✓ маркировку и приоритезация трафика (QoS)
  - ✓ событийное протоколирование Syslog, мониторинг SNMP
  - ✓ горячее резервирование по VRRP, балансировку по RRI и т.д.

Виртуальный шлюз безопасности Bel VPN Gate-V 4.1

Bel VPN Gate-V 4.1 – программный комплекс «Виртуальный шлюз безопасности Bel VPN Gate-V» обеспечивает полную функциональность Bel VPN Gate и функционирует в виртуальной среде (VMware ESXi, Citrix XenServer, Microsoft Hyper-V). Предназначен как для защиты периметра облачной инфраструктуры, так и взаимодействия между отдельными виртуальными машинами. Производительность зависит от аппаратной платформы

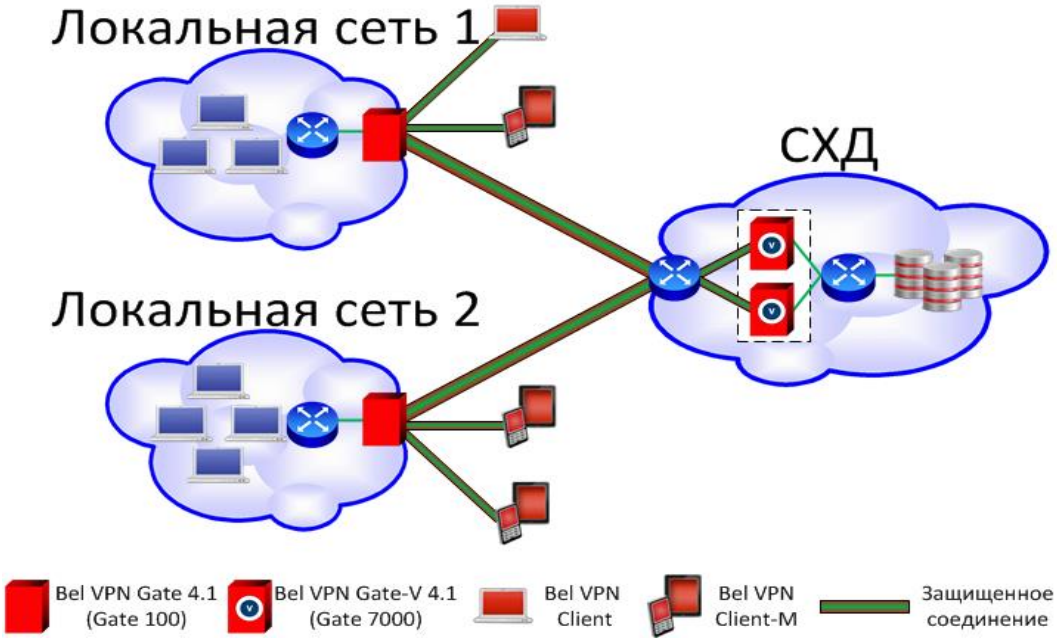
- Преимущества:
  - ✓ интеграция непосредственно в виртуальную инфраструктуру
  - ✓ простая и быстрая установка и настройка
  - ✓ высокая производительность шифрования трафика
  - ✓ реализация сценариев обеспечения высокой доступности и отказоустойчивости
  - ✓ оперативная адаптация к меняющимся задачам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

Модуль канального шифрования Bel VPN L2

Программный продукт Bel VPN L2 (в составе шлюза) обеспечивает защищенное взаимодействие сегментов сети на канальном уровне.

- Обеспечивает:
  - ✓ объединение территориально-распределенных сетей в один широковещательный домен
  - ✓ передачу широковещательных (broadcast) и multicast пакетов, тестированного трафика (VLAN trunk), меток IPV4 и др.
  - ✓ обработку приоритетного трафика
  - ✓ минимальные настройки маршрутизации
- Применяется:
  - ✓ организация защищенного канала между ЦОД
  - ✓ реализация миграции сетевой инфраструктуры
  - ✓ защита IP-телефонии и видеоконференцсвязи
  - ✓ построение высокопроизводительного, отказоустойчивого решения с балансировкой нагрузки

Удаленный доступ к ЦОД (СХД)



- Для защиты ЦОД применяются шлюзы на наиболее производительных аппаратных платформах с балансирующим устройством
- В сетях с JumboFrames один Bel VPN Gate способен защищать поток данных до 4,5 Гбит/с
- При шифровании IMIX трафика – около 1,5 Гбит/с в обе стороны (1+1)
- Высокопроизводительная защита может быть обеспечена с помощью Bel VPN L2 и на канальном уровне
- И на сетевом, и на канальном уровне решения отказоустойчивы и масштабируются при возрастании трафика
- Механизм QoS позволяет обеспечить высокое качество сервиса для приоритетного трафика (например, IP-телефонии) даже в состоянии перегрузки

Высокопроизводительные аппаратные платформы

- KW Express ISP ES29 (ES221)
- KW Express Lite EL19
- HP Proliant DL20 Gen9
- Сервер «Белсофт»
- Сервер «Бевалекс»
- Cisco UCS C220 M4
- Huawei RH1288 V3

Пример высокой производительности шлюзов

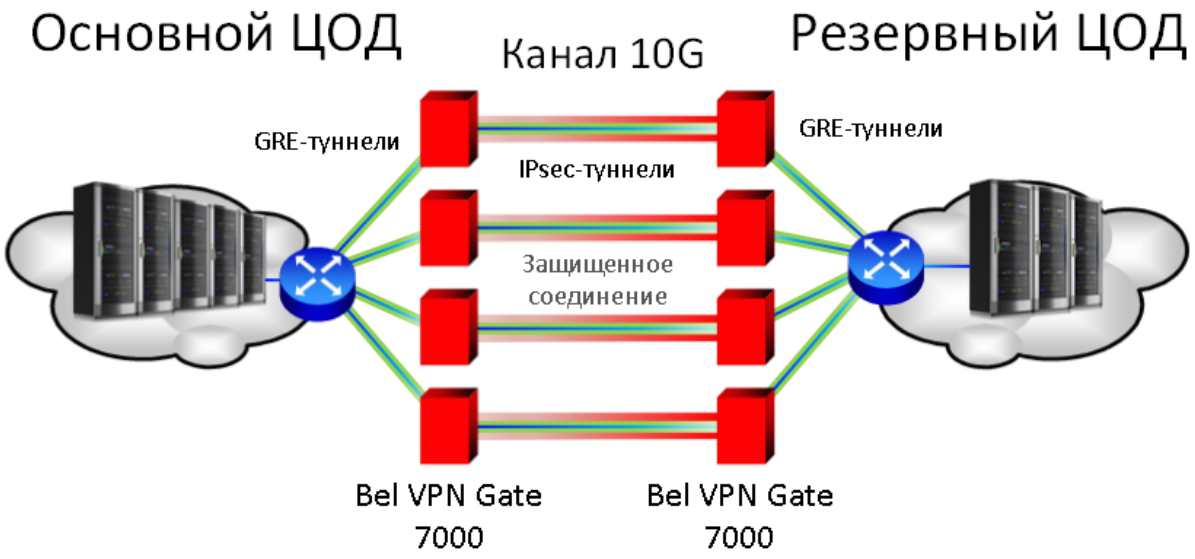
- Увеличение количества шифрующих шлюзов вызывает пропорциональный рост общей производительности решения.
- Выбор необходимого количества шлюзов зависит от объема и типа трафика.
- Производительность программного модуля Bel VPN L2 должна выбираться по аналогии с платформой L3 с дополнительным запасом 15-20%.

Аппаратная платформа (процессор)	TCP, Мбит/с	UDP 1380, Мбит/с	IMIX, Мбит/с
Kraftway ISP ES 29 (2x Xeon E5-2643v2)	3530	3635	1508
Kraftway Express Lite EL19 (Xeon E3-1280v3)	2135	2541	1138

Производительность шифрования зависит от многих факторов и, в первую очередь, от размера пакетов. Наибольшая производительность достигается на пакетах больших размеров (Jumbo Frames).

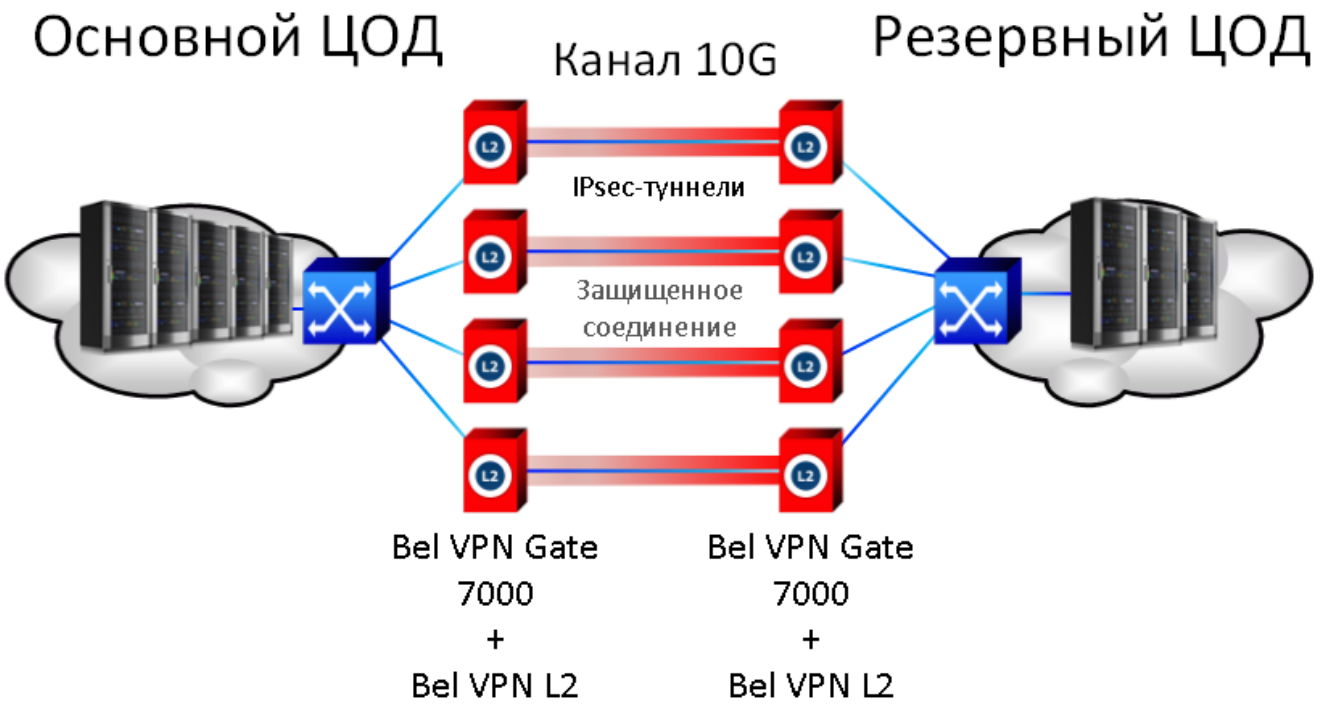
Аппаратная платформа (процессор)	TCP, Гбит/с	UDP 8800, Гбит/с
Kraftway ISP ES 29 (2x Xeon E5-2643v2)	4,5	4,7
Kraftway Express Lite EL19 (Xeon E3-1280v3)	2,7	2,9

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

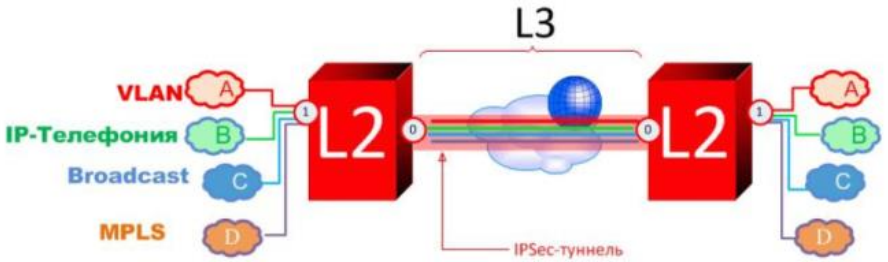
Защита ЦОД и высокопроизводительных каналов L2



- **Bel VPN L2** – это дополнительный программный модуль, встраиваемый в Шлюз безопасности, для перехвата трафика на канальном уровне с дальнейшей инкапсуляцией и шифрованием на сетевом уровне
- Позволяет передавать широковещательные и мультикастовые пакеты, тегированный трафик (VLAN trunk), метки MPLS и другие виды трафика

Технология шифрования на канальном уровне (L2)

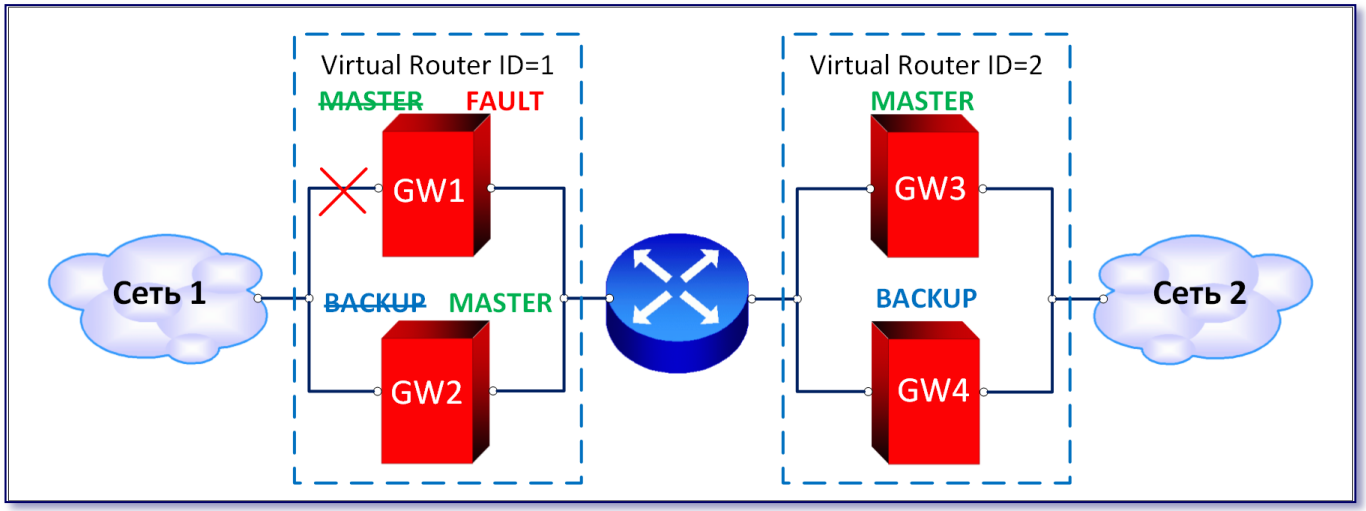
- Интерфейс Eth1 шлюза установлен в promisc режим. Весь трафик, поступающий на данный интерфейс, перехватывается специализированным модулем и передается на сетевой уровень интерфейса Eth0.
- Перехваченный пакет шифруется (инкапсулируется в ESP), IP-адрес источника становится адрес интерфейса Eth0, адресом назначения – IP-адрес шлюза на другом конце. После этого пакет отправляется в канал связи.
- На другой стороне обработка пакетов осуществляется в обратном порядке. Таким образом, происходит туннелирование L2 в L3.



Балансировка на канальном уровне (L2)

- Для балансировки трафика между шлюзами используются технология Etherchannel (протоколы LACP или PAgP).
- Балансировка осуществляется посессионно. В качестве параметров можно использовать IP-адреса источника и/или назначения, MAC-адреса источника и/или назначения, комбинацию IP или MAC адресов источника и назначения.
- Распределение трафика зависит от количества интерфейсов, объединенных в агрегированный канал, а также от количества источников/получателей трафика. Равномерное распределение нагрузки осуществляется при использовании 2, 4, 8 или 16 интерфейсов.

Отказоустойчивое решение 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
- Сценарий отрабатывает следующие типы **отказов**:

  - отключение питания;
  - выход из строя аппаратной платформы;
  - отказ сетевого интерфейса;
  - отказ порта на коммутационном оборудовании;
  - отказ демона отвечающего за шифрование трафика

КОНТАКТЫ

- Адрес:
  220012, г.Минск
  ул.Чернышевского,
  10А, пом.702
  (+375 17) 280 6000
  (+375 17) 280 7867
- Факс:
  (+375 17) 280 7867
- Электронная почта:
  info@s-terra.by

s•terra
BEL

Спасибо!

Обращайтесь к нам!