s•terra

ЗАЩИТА ВЗАИМОДЕЙСТВИЯ ЦОД-ЦОД

Москва, 2018г.

Центры обработки данных (ЦОД) стали логичным ответом на растущие требования к скорости обработки и доступности информации, а также эффективному использованию ИТ-ресурсов. Консолидация ИТ-сервисов в ЦОД имеет множество преимуществ: эффективное использование вычислительных ресурсов, высокая доступность критичных сервисов, гибкость и масштабируемость ИТ-инфраструктуры. Однако, ЦОДы также стали и чрезвычайно привлекательной мишенью для злоумышленников. Особенно перспективной точкой взлома выглядят магистральные волоконно-оптические каналы связи, соединяющие ЦОДы, ведь через них передается колоссальное количество данных. Одна часть этих данных является ценностью сама по себе (например, персональные или коммерческие данные), другая часть позволяет узнать больше о внутренней структуре ЦОД, используемых версиях операционных систем и программного обеспечения и прочей ценной служебной информации. При этом устройства съема данных с волоконно-оптических каналов без разрыва волокна стоят всего лишь несколько сотен долларов. С их помощью злоумышленники могут в режиме реального времени получать доступ к передаваемым данным, а также собирать информацию для будущих атак.

Становится очевидно, что каналы, соединяющие ЦОД между собой, необходимо защищать как от пассивного вмешательства (т.е. прослушивания данных), так и от активных действий злоумышленников (т.е. попыток изменить передаваемую информацию или не допустить её передачи).

Одним из вариантов такой защиты может служить физическая защита канала передачи данных. Она может хорошо работать в том случае, если канал проходит в пределах одного здания или, по крайней мере, по закрытой частной территории. В тех же случаях, когда ЦОДы географически удалены друг от друга, физическая защита становится очень дорогой, а зачастую совсем невозможной. В такой ситуации приходится использовать недоверенные каналы связи и применять криптографическую защиту передаваемых данных.

Важно также учесть, что если в информационной системе компании обрабатывается информация, подлежащая обязательной защите в соответствии с российским законодательством (например, персональные данные), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки регуляторами – ФСБ России и ФСТЭК России.

Компания «С-Терра СиЭсПи» предлагает применять комплексное сертифицированное решение на базе продуктов С-Терра Шлюз и коммутаторов, обеспечивающих балансировку трафика. Решение позволяет организовать высокопроизводительный защищенный канал между центрами обработки данных на скоростях от 10 Гбит/с и выше.

Помимо высокой производительности, решение обладает следующими преимуществами:

- **Надежная защита в соответствии с российским законодательством.** Используется набор протоколов IKE/ IPsec с алгоритмами шифрования по ГОСТ 28147-89, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94. Продукт сертифицирован ФСБ России.
- **Отказоустойчивость.** При обрыве одного из туннелей (по причине отказа шлюза, канала или промежуточного оборудования) коммутатор автоматически перераспределит нагрузку по рабочим шифрованным туннелям. Таким образом обеспечивается отказоустойчивость самих шлюзов безопасности, провайдеров и

промежуточного оборудования. Также возможно использование стека коммутаторов.

- **Масштабируемость.** В случае, если возрастает потребность в увеличении количества шифруемого трафика, решение легко масштабируется до более производительного добавлением дополнительных шлюзов безопасности.

В состав решения входят комплект шлюзов безопасности С-Терра Шлюз 10G, настроенных для оптимальной реализации этой задачи, специальная документация по интеграции и настройке оборудования в данном решении, комплект стандартной документации для продуктов С-Терра Шлюз. Для применения данного решения необходимо наличие коммутаторов, соответствующих следующим требованиям:

– поддержка протокола LACP или PAgP;

– наличие необходимого количества 10Gbps интерфейсов.

Минимальный комплект состоит из четырех шлюзов безопасности и набора документации. Для его применения требуется наличие двух коммутаторов. Шлюзы используются для построения защищенного туннеля связи на канальном уровне. Такой туннель позволяет обеспечить конфиденциальность и целостность передаваемых данных даже в том случае, если промежуточное оборудование на канале было взломано злоумышленником. Коммутаторы выступают в роли балансировщиков трафика, обеспечивая масштабируемость и отказоустойчивость решения. Для балансировки трафика коммутаторы используют агрегированный канал (LACP или PAgP).

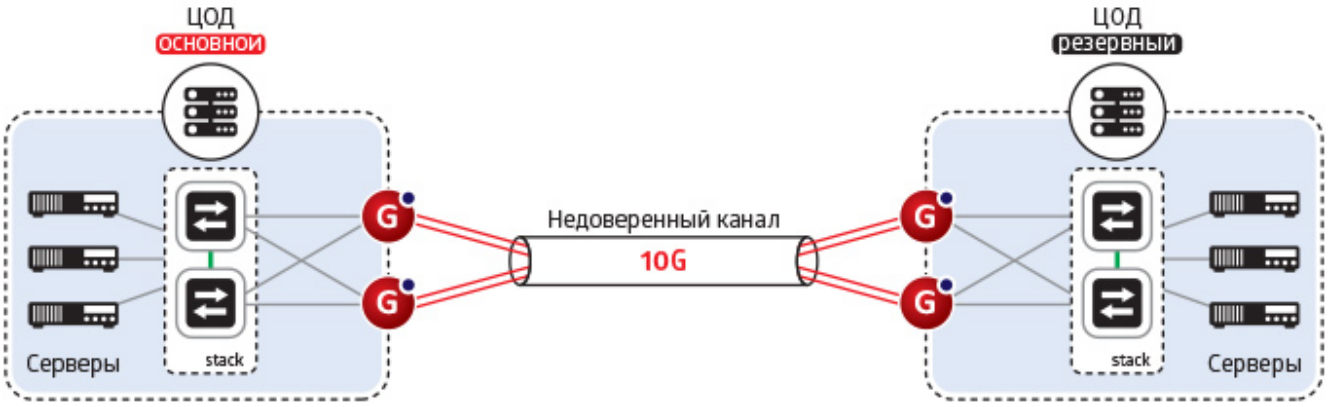
Пример защиты связи ЦОД-ЦОД для канала 10 Гбит/с

Исходные данные: требуется защитить канал, связывающий два ЦОД на канальном уровне L2. Ширина канала – 10 Гбит/с. Передаваемый трафик – преимущественно TCP, IP-телефония отсутствует. Решение должно быть отказоустойчивым, с временем отработки отказа менее 3 секунд.

Предлагаемое решение:

Предлагается использовать 2 пары шлюзов С-Терра Шлюз 10G и два стека коммутаторов.

Схема решения представлена на рисунке.



Сведения о продуктах и производителе

Подробную информацию о компонентах данного решения вы можете получить на сайте производителя www.s-terra.com.

Компания «С-Терра СиЭсПи»

ООО «С-Терра СиЭсПи» основано в 2003 году и является ведущим российским разработчиком и производителем средств сетевой информационной безопасности.

Компания «С-Терра СиЭсПи» предлагает органично входящие в сетевую инфраструктуру решения, которые используют протокол IPsec и российские сертифицированные криптографические алгоритмы. Решения характеризуются отличной масштабируемостью, надежностью и рекордной производительностью, что обеспечивает высокую экономическую эффективность.

Продукты и решения С-Терра обеспечивают защиту каналов связи любой производительности (как на сетевом, так и на канальном уровне), безопасный удаленный доступ, в том числе с мобильных платформ, а также предоставляет эффективное управление VPN-инфраструктурой С-Терра.

Продукты С-Терра сертифицированы ФСТЭК России и ФСБ России, в том числе как средства криптографической защиты информации (СКЗИ) по классу КС1, КС2, КС3.

Компания является первым российским технологическим партнером Cisco (Cisco Solution Technology Integrator), Серебряным партнером Samsung и Авторизованным партнером Huawei.

Подробную инструкцию по настройке компонентов решения Вы можете получить здесь.

Получить помощь в выборе оборудования и расчет стоимости решения для вашего ЦОД Вы можете, обратившись к нашим менеджерам:

– по телефону **+7 499 940-90-61**

– или по электронной почте: sales@s-terra.ru