s•terra

РЕШЕНИЯ для ТЕЛЕКОММУНИКАЦИОННОЙ ОТРАСЛИ

Информационная безопасность в телекоммуникационной отрасли условно делится на два направления – обеспечение защиты собственной инфраструктуры оператора и оказание услуг по предоставлению защищенных каналов связи и удаленного доступа клиентам. Решения, используемые для собственных нужд, обычно ложатся в основу предложений для клиентов.

При этом важно обеспечить конфиденциальность и целостность информации при передаче по недоверенным каналам связи. Если в информационной системе обрабатывается информация, подлежащая обязательной защите в соответствии с российским законодательством (например, персональные данные – ПДн), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки регуляторами – ФСБ России и ФСТЭК России.

Российская компания «С-Терра СиЭсПи» предлагает высокопроизводительные, надежные и оптимальные по стоимости решения для защиты сетевого взаимодействия для операторов связи, облачных провайдеров и иных компаний, предоставляющих услуги связи.

Преимущества решений С-Терра

1. **Легкая интеграция** в существующую сетевую инфраструктуру, благодаря использованию единых компонентов:

- система централизованного управления и мониторинга оборудования С-Терра КП;
- любой удостоверяющий центр, выпускающий ГОСТ-сертификаты (например, Microsoft CA или УЦ КриптоПро);
- Cisco-like интерфейс локального управления.

Таким образом, нет необходимости обучать или нанимать новых специалистов для поддержания работоспособности безопасности сетевой инфраструктуры.

2. **Использование мировых стандартов IKE/IPsec** (RFC2401-2412) обеспечивает отсутствие ошибок, связанных с дизайном протокола защиты. Архитектура IPsec проверена многократным техническим анализом и тестированием специалистами многих стран, и внедряется по всему миру, в том числе и в России.

3. **Отсутствие зависимости от поставщика оборудования.** Технология IPsec является унифицированным мировым стандартом. Поэтому, если в Вашей организации уже используется иностранное оборудование для защиты сетей, Вы сможете плавно и без лишних усилий перейти на соответствующие отечественным стандартам продукты С-Терра.

Более того, можно использовать уже имеющиеся в организации аппаратные платформы, установив на них ПО С-Терра VPN.

4. **Легитимность**. Продукты компании «С-Терра СиЭсПи» сертифицированы ФСБ России до классов КС3 и МЭ4 включительно, а также ФСТЭК России по уровням МЭ 3, НСД 3, ОУД 4+, НДВ 3, АС 1В, ГИС до 1кл вкл., ПДн 1-4 ур. Указанные уровни сертификации обеспечивают выполнение требований Российского законодательства по защите персональных данных: Федеральный закон №152 «О персональных данных» и Федеральный закон №149 «Об информации, информационных технологиях и о защите информации».

5. **Высокая экономическая эффективность продуктов**. Оптимальный функциональный состав решений С-Терра, а также использование международных технологических стандартов позволяет не только оптимизировать Ваши первоначальные затраты на приобретение, но и

снизить стоимость обслуживания (ТСО). Стоимость лицензий зафиксирована в рублях и не зависит от курса доллара.

6. **Качественная, оперативная служба технической поддержки.** Выбрав решения С-Терра для решения задач информационной безопасности (ИБ), Вы не останетесь с ними «один на один»: наши специалисты всегда готовы Вас проконсультировать. Время реакции нашей службы технической поддержки - от 2 часов. В техническую поддержку можете обратиться как Вы, так и интегратор, установивший у Вас наши продукты. На все аппаратные платформы С-Терра предоставляется гарантия производителя не менее 3-х лет. Некоторые аппаратные платформы поставляются на условиях безусловной оперативной замены в случае выявления неисправности (в течение срока гарантии).

Решения С-Терра для различных задач отрасли

Таблица 1. Сводная таблица решений С-Терра для телеком-сектора

Решения С-Терра	Продукты С-Терра	Описание
Задача:	***Защита взаимодействия между офисами***	
Защита корпоративной сети	• С-Терра Шлюз • С-Терра Виртуальный Шлюз • Криптомаршрутизатор ESR-ST	Защита любого сетевого трафика при передаче по недоверенным каналам связи. Широкая линейка продуктов в различных форм-факторах, масштабирование производительности.
Задача:	***Удаленный доступ сотрудников, работающих вне офиса***	
Защита удаленного доступа	• С-Терра Клиент • С-Терра Клиент-М	Удаленный доступ сотрудников через интернет с помощью программного клиента для различных ОС.
Задача:	***Оказание услуг по предоставлению защищенных каналов связи***	
С-Терра VPN-как-сервис	• С-Терра Виртуальный Шлюз • С-Терра Клиент • С-Терра Клиент-М	Предоставление оператору связи продуктов С-Терра для оказания услуг защиты каналов связи и удаленного доступа клиентам. Поквартальная оплата.
Задача:	***Защита взаимодействия с ЦОД или между ЦОД***	
Защита канала 10Гб	• С-Терра Шлюз • С-Терра Шлюз 10G	Защита канала 10G с помощью одной пары шлюзов. Использование кластера мощных шлюзов.

Защита взаимодействия между офисами

Защита взаимодействий территориально-распределенных подразделений и офисов – типовая задача для продуктов С-Терра, многократно проверенная нашими заказчиками.

В каждом таком подразделении или офисе устанавливается криптошлюз, реализующий IPsec VPN ГОСТ и межсетевое экранирование. Благодаря широкой линейке продуктов С-Терра, можно подобрать подходящее устройство для решения любой задачи, с любой требуемой скоростью передачи данных. В том числе, имеется возможность встраивания в маршрутизаторы Cisco серий 2900, 3900.

Поддержка кластеризации в продуктах С-Терра позволяет обеспечить отказоустойчивость канала связи с критически важными объектами.

Удаленный доступ сотрудников

Темпы развития современного бизнеса требуют оперативной реакции на запросы. Для этого сотрудникам необходим доступ к корпоративным ресурсам, где бы они ни находились – дома, в командировке или в отпуске. При этом, они осуществляют доступ к корпоративным ресурсам через Интернет, который является недоверенной сетью.

Для того, чтобы снизить риски и обеспечить конфиденциальность и целостность передаваемых данных, непосредственно на устройство пользователя устанавливается VPN-клиент С-Терра:

a) С-Терра Клиент – для ОС Windows;
b) С-Терра Клиент-М – для ОС Android.

В точке подключения клиентов к корпоративной сети (например, в головном офисе) устанавливается С-Терра Шлюз.

С-Терра VPN-как-сервис

Решение С-Терра VPN-как-сервис открывает для операторов связи новую возможность – предложить потребителям услугу «безопасность как сервис» путем добавления в свою инфраструктуру сертифицированных VPN-компонентов производства С-Терра.

В основе решения – использование сертифицированных программных комплексов С-Терра Виртуальный Шлюз, С-Терра Клиент и С-Терра Клиент-М. Получая от оператора преднастроенные продукты С-Терра, абонент обеспечивает легитимную защиту передаваемых данных и снижает капитальные затраты.

Одно из важных преимуществ предлагаемого решения С-Терра VPN-как-сервис в том, что оператору не требуется устанавливать у себя десятки аппаратных криптошлюзов. Вместо этого – он просто "разворачивает" виртуальную машину из имеющегося шаблона.

Данное решение обладает рядом уникальных преимуществ:

1. Быстрый запуск новой услуги – VPN-как-сервис.
2. Отсутствие необходимости в установке специального оборудования.
3. Защита каналов связи сертифицированными VPN-продуктами, использующими российские ГОСТ-криптоалгоритмы и технологию IPsec VPN.

4. Возможность, по желанию сервис-провайдера и/или его абонента, установки дополнительных аппаратных криптошлюзов.
5. Легкое масштабирование.

Защита взаимодействия с ЦОД

Одним из современных трендов в бизнесе является централизация ИТ-ресурсов. При этом, появляется задача защиты высокоскоростных каналов связи между офисом и центром обработки данных (ЦОД), а также между основным и резервным ЦОДами.

Распространенные заблуждения о том, что оптические каналы связи не требуют защиты, и что отсутствуют отечественные средства криптографической защиты для обеспечения скорости шифрования 10Гб/с и выше, очень легко опровергнуть.

Во-первых, устройства съема информации с оптических каналов значительно снизились в цене и могут быть свободно приобретены за 100-300$, что существенно расширяет возможности злоумышленников и свидетельствует о том, что оптические каналы связи нужно защищать точно так же, как и любые другие.

Во-вторых, производительность шифрования С-Терра Шлюз 10G достигает 10Гб/с на **смешанном** трафике. При этом, шифрование осуществляется в соответствии с ГОСТ28147-89 и ГОСТ Р 34.12-2015.

Данный продукт является уникальной разработкой компанией «С-Терра СиЭсПи» и базируется на высокопроизводительной аппаратной платформе и ПО С-Терра Шлюз, специально оптимизированном для решения именно такой задачи.

Как результат, решение С-Терра, используя всего **одну пару** устройств С-Терра Шлюз 10G, обеспечивает защиту канала связи с пропускной способностью 10Гб/с с IMIX трафиком.

Для защиты более высокоскоростных каналов решение масштабируется до скорости 40G.

Наши клиенты

Пользователями решений С-Терра являются крупнейшие федеральные телекоммуникационные компании.

Как один из примеров, оборудование С-Терра использовалось при реализации проекта, называемого «Отмена мобильного рабства». Другой пример: установка шлюзов безопасности С-Терра в ПАО «Ростелеком» для осуществления защиты подключения к СМЭВ.

Приобретение решений

По всем вопросам, касающимся конфигурации системы ИБ и подбора продуктов для решения Ваших задач информационной безопасности обращайтесь к нашим менеджерам:

- по телефону +7 499 940-90-61
- или по почте sales@s-terra.ru