s•terra

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ

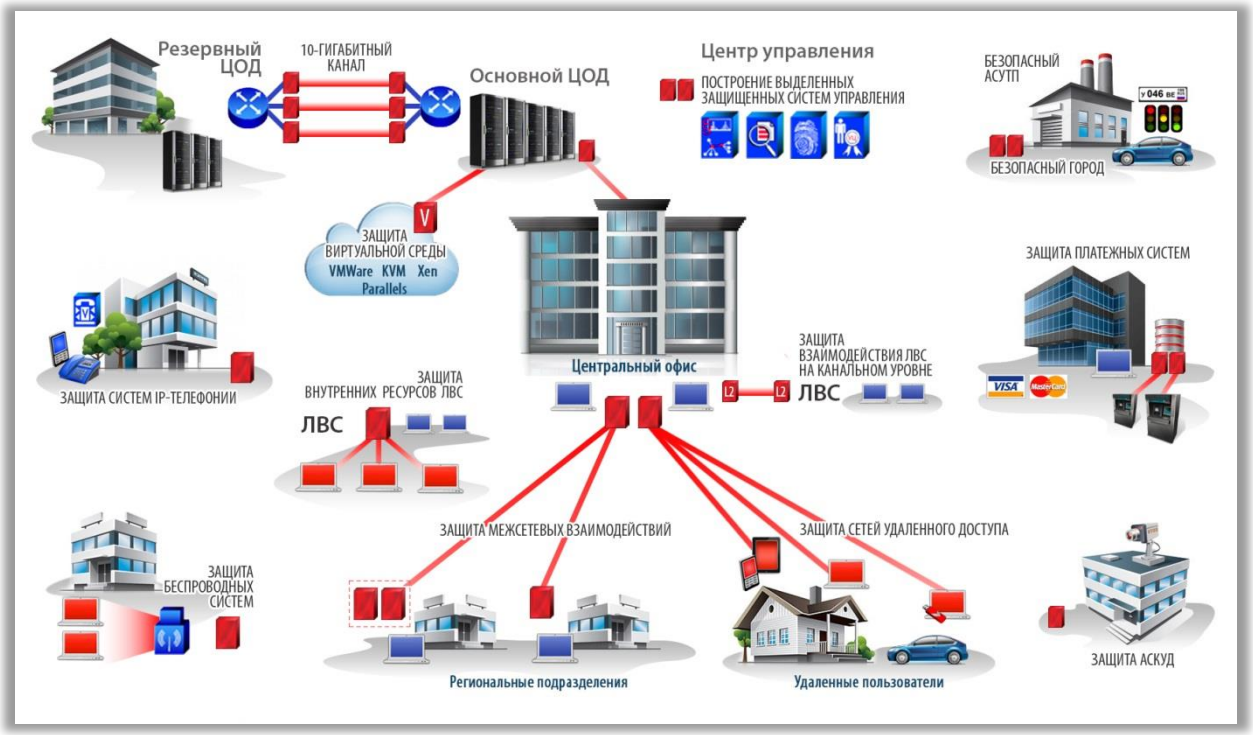
Задача

Любая организация заботится о сохранении своей информации, т.к. ее разглашение может нанести ущерб, как самой организации, так и другим лицам. Такую информацию называют конфиденциальной. С этимологической точки зрения, слово «конфиденциальный» происходит от латинского confidentia — доверие. В современном русском языке это слово означает «доверительный, не подлежащий огласке, секретный».

С развитием информационных технологий задача обеспечения информационной безопасности, и в частности конфиденциальности, приобретает все большую значимость. Она крайне важна для любой организации, а для некоторых областей регламентируется на государственном уровне. 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.

Типовые задачи защиты корпоративной сети

- Защита филиальной сети различного масштаба;
- Защищенный доступ удаленных сотрудников;
- Специальные решение (высокопроизводительные каналы связи, АСУ ТП, видеонаблюдение).



Защита территориально распределенных сегментов

Современный бизнес не ведётся в пределах офисных стен, компоненты инфраструктуры большинства компаний географически распределены. При этом им необходимо единое информационное пространство, для создания которого используются в том числе недоверенные каналы связи. Для обеспечения конфиденциальности и целостности информации, передаваемой по таким каналам, необходимы VPN-продукты.

Компания С-Терра СиЭсПи является ведущим разработчиком и производителем VPN-продуктов и предлагает широкую линейку шлюзов безопасности – С-Терра Шлюз, как в аппаратном исполнении, так и в виде виртуальной машины, которые обеспечивают защиту трафика при его передаче, а также межсетевое экранирование. В центральной точке шлюзы могут работать в отказоустойчивой конфигурации для обеспечения беспрерывного сервиса.

Линейка шлюзов безопасности масштабируется от миниатюрных устройств, размером чуть больше спичечного коробка, до полноценных серверов, предназначенных для защиты десятков гигабит трафика. Это позволяет найти оптимальное по производительности решение для любой задачи будь то защита взаимодействия офисов, IP-телефонии, видеоконференцсвязи и т.д.

Управление шлюзами осуществляется как через командно-строчный интерфейс, аналогичный Cisco IOS, так и с помощью централизованной системы управления – С-Терра КП.

Одна из важнейших составляющих безопасности – постоянный мониторинг и реагирование на инциденты. Все продукты С-Терра поддерживают запись основных событий безопасности по протоколу Syslog и мониторинг по протоколу SNMP. Обнаружение сетевых атак обеспечивается отдельным продуктом – С-Терра СОВ.

Решения на основе продуктов С-Терра обеспечивают надежную защиту трафика при передаче между территориально распределенными сегментами так в Российской Федерации, так и за её пределами – с помощью экспортного варианта шлюза.

Защита удаленного доступа

Темпы ведения современного бизнеса буквально заставляют людей постоянно находиться на связи, быть готовыми отреагировать в сжатые сроки на любые виды запросов. Многие компании привлекают сотрудников из других городов, регионов, даже стран. Удаленно работающие сотрудники – это тоже сегмент корпоративной сети и ему нужна защита.

Для решения этой задачи на удаленное рабочее место устанавливается программное обеспечение – С-Терра Клиент (для всех современных ОС Windows) или С-Терра Клиент-М (для ОС Android). Продукты обеспечивают защиту трафика как внутри сети, так при передаче по внешним каналам связи.

Специальные решения

Тенденция централизации ресурсов привела к широкомасштабному распространению ЦОДов. Высокопроизводительным каналам связи между головным офисов и ЦОД или между основным и резервным ЦОДами также необходима защита.

Для защиты таких каналов используется несколько устройств С-Терра Шлюз с балансировкой нагрузки между ними. Таким образом обеспечивается защита репликации данных, миграции виртуальных машин и т.п.

Резюме

Казалось бы, каждая из трех описанных задач имеет отдельное решение. Но в современном мире важным критерием является универсальность, а именно решение одним продуктом нескольких задач.

Продукты С-Терра позволяют одновременно решить все три задачи и предоставляют дополнительные преимущества:

- Проверенный российский производитель
- Использование стандартных протоколов
- Поддержка ГОСТ алгоритмов шифрования
- Интеграция в существующую инфраструктуру (в том числе в виртуальную)
- Сертификация ФСБ и ФСТЭК России
- Высокая экономическая эффективность

Пример

- *Условия:* Организация состоит из головного офиса и 20 филиалов. Связь филиалов с головным офисом осуществляется через недоверенную сеть - интернет. В головном офисе развернута база данных, содержащая ПДн, доступ к которой необходим удаленным и сотрудникам в филиалах. Канал в головном офисе 100 Мбит/с, в филиалах – по 10 Мбит/с. Удаленные сотрудники (20 человек) используют ноутбуки на ОС Windows.
- *Требуется:* защитить ПДн при их передаче через недоверенную сеть в соответствии с законодательством. В головном офисе требуется резервирование оборудования. Класс защиты по линии ФСБ России – КС1.
- *Решение:*

  В центре рекомендуется использовать:

  - Кластер из шлюзов безопасности С-Терра Шлюз 1000: *2x G-1000M-D-4120-4-ST-KC1*
  - Систему управления С-Терра КП на 100 лицензий: *1x KP-100-D*

  В филиалах рекомендуется установить:

  - Шлюзы безопасности С-Терра Шлюз 100: *20x G-100-D-4107-2-ST-KC1*

  Удаленным пользователям рекомендуется установить:

  - Клиент безопасности С-Терра Клиент: *20x C-X-WIN-D-ST-KC1*

  Актуальные цены доступны в прайс-листе, размещенном на сайте компании.

О компании «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. Уникальным преимуществом продукции компании является широкий спектр совместимого оборудования различных производителей – как зарубежных, так и отечественных.

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.

Партнерская сеть компании "С-Терра СиЭсПи" состоит из более чем 300 компаний, включая всех крупнейших российских системных интеграторов. Имеется представительство компании в Республике Беларусь.

Более подробную информацию о компании можно получить на сайте: http://www.s-terra.com/about/