s•terra

ЗАЩИТА УДАЛЕННОГО ДОСТУПА С МОБИЛЬНЫХ УСТРОЙСТВ

Задача

Мобильные устройства прочно вошли в нашу жизнь. Сотрудники большинства компаний не могут представить свою работу без планшетов и смартфонов с возможностью получения удаленного доступа к внутренним рабочим ресурсам. Корпоративная почта, чат, файловые хранилища, системы учета проектов, базы знаний и много другое необходимы не только в офисе, но и в командировке, на деловой встрече, а иногда и во время отпуска.

Несомненно, оперативный доступ к информации является одной из важнейших потребностей успешной модели бизнеса. Но эта потребность ставит перед организацией задачу защиты информации при удаленном доступе с мобильных устройств.

Существует два базовых подхода при решении этой задачи: предоставление корпоративных устройств или использование сотрудниками собственных.

В первом случае, для подключения к внутренним сервисам компания выделяет работникам мобильные устройства с заранее настроенной политикой безопасности. Преимуществом данного подхода является удобство администрирования типовых устройств, недостатками – расходы на приобретение и необходимость сотрудникам использовать несколько устройств (корпоративные и личные).

Второй случай – использование для работы личных устройств – отражает современную концепцию BYOD (Bring Your Own Device – "принеси свое собственное устройство"). Преимуществом данного подхода является удобство использования сотрудником привычного ему телефона или планшета, недостатком – необходимость контроля его защищенности и отсутствие на устройствах механизма разделения и изоляции данных на пользовательские и корпоративные.

Общие требования для обоих вариантов решения – не допустить снижения уровня защищенности информационной системы (ИС) компании и обеспечить максимально прозрачную защиту канала связи между мобильным устройством и корпоративной сетью.

Кроме того, следует учитывать, что если на мобильном устройстве обрабатывается информация, подлежащая обязательной защите в соответствии с требованиями российского законодательства (например, персональные данные или информация, обрабатываемая в государственных информационных системах), то необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки соответствия регуляторами.

С-Терра Клиент-М для ОС Android

Программный комплекс С-Терра Клиент-М предназначен для защиты удаленного доступа с устройств на платформе Android. С помощью технологии виртуальных частных сетей (VPN) на основе шифрования по ГОСТ 28147-89 обеспечиваются конфиденциальность и целостность. Таким образом, продукт позволяет защитить трафик мобильного устройства при его передаче по недоверенным каналам связи, независимо от того, устройство личное, или корпоративное.

Перед подключением к корпоративной сети происходит аутентификация как пользователя (с помощью пароля), так и устройства – на основе цифрового сертификата открытого ключа, закрытый ключ которого может храниться на токене. В качестве точки подключения мобильных пользователей к ИС может использоваться шлюз безопасности в виде виртуальной машины (С-

Терра Виртуальный Шлюз) или программно-аппаратный комплекс С-Терра Шлюз из линейки 100/1000/3000/7000/MCM. Трафик до корпоративных ресурсов передается внутри IPsec VPN туннеля и шифруется отечественными криптоалгоритмами в соответствии с ГОСТ 28147-89.

Если пользователю необходим доступ к публичным ресурсам, расположенными в сети Интернет, то существуют два варианта решения этой задачи:

1) Инкапсулировать данный трафик в IPSec туннель и шифровать (аналогично трафику до корпоративных ресурсов). Доступ в Интернет в этом варианте осуществляется из центральной точки через корпоративный прокси-сервер.

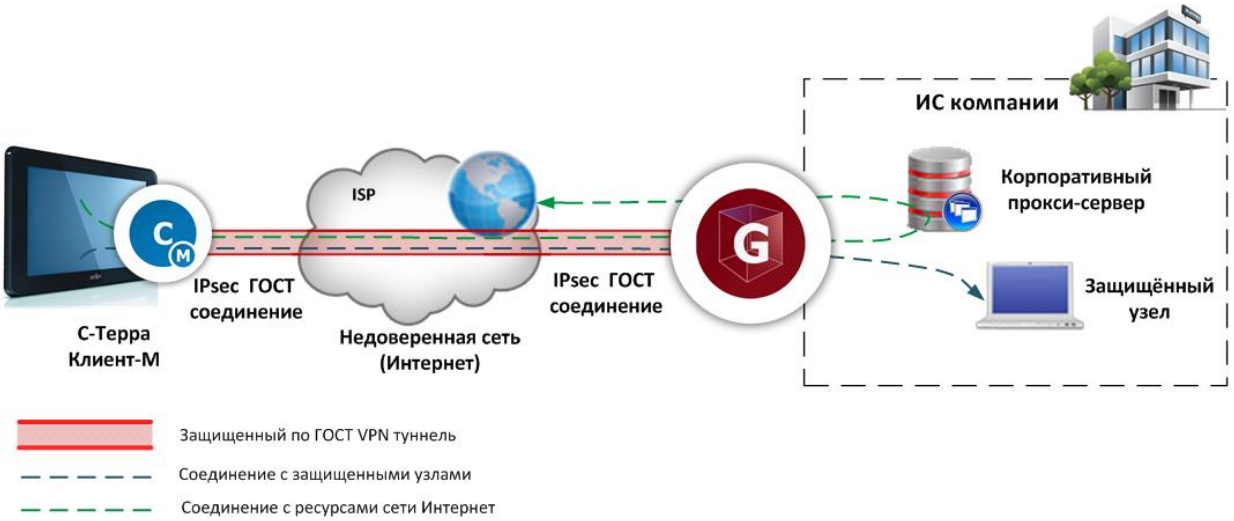

Рисунок 1. Защита удаленного доступа с использованием корпоративного proxy

2) Устанавливать прямое соединение мобильного устройства с Интернет (без шифрования), т.н. split tunneling.

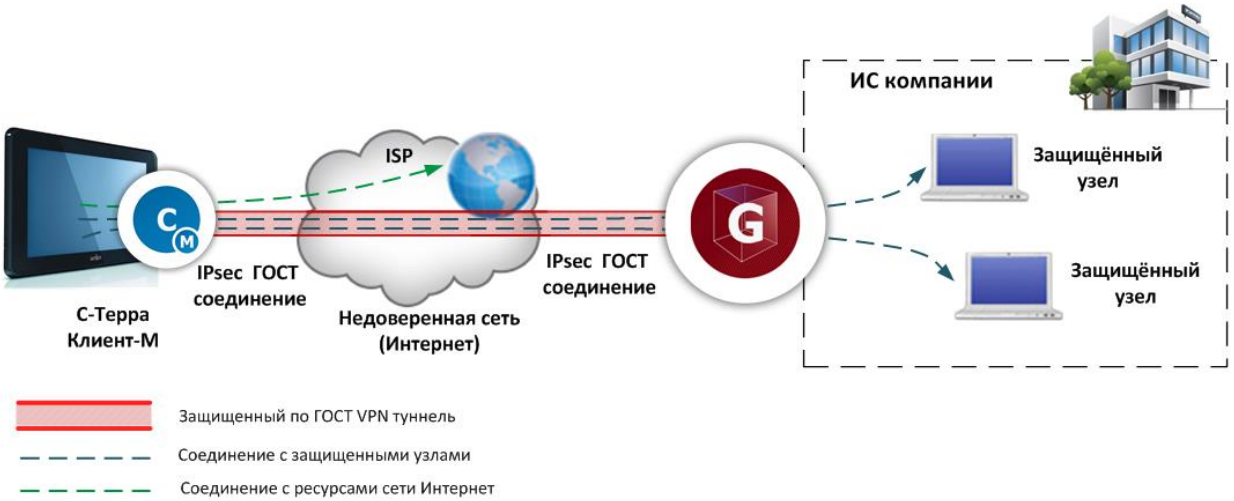

Рисунок 2. Защита удаленного доступа без ограничения доступа к Интернету (split tunneling)

Преимущества и характеристики

Программный комплекс С-Терра Клиент-М обладает следующими преимуществами:

- выполнение требования российского законодательства;
- обеспечение конфиденциальности и целостности трафика;
- установка штатными средствами (без взлома устройства);
- возможность применения двухфакторной аутентификации;
- различные варианты доступа в интернет (split tunneling или proxy);
- поддержка различных сетей доступа (3G/4G/wi-fi и т.д.);
- интеграция с корпоративными системами управления мобильными устройствами (MDM).

Таблица 1. Характеристики С-Терра Клиент-М

Возможности	**Описание**
ОС	Android 4.0.4 и выше
Установка	Стандартными средствами (административных прав не требуется)
Протоколы IKE/IPsec	Стандарты RFC 2401 - 2412
Алгоритм шифрования	ГОСТ 28147-89
Алгоритмы электронной подписи	ГОСТ Р 34.10-2012
Алгоритмы вычисления хэш-сумм	ГОСТ Р 34.11-2012
Криптопровайдер	Криптография «С-Терра СиЭсПи»
Сертификация	ФСБ России СКЗИ КС1
Событийное протоколирование	Syslog
Формат сертификатов публичных ключей	X.509 v.3 (ГОСТ)
Способы получения сертификатов	Протоколы IKE, LDAP v.3 Импорт из файла (bin и base64, PKCS#7 bin и base64, PKCS#12 bin и base64)
Способ получения ключевой пары	Генерация внешним PKI сервисом с доставкой на токене или локально
Интеграция с MDM-системами	Citrix XenMobile SafePhone
Поддерживаемые токены	JaCarta MicroSD, Рутокен ЭЦП (USB), Рутокен ЭЦП Bluetooth
Примеры совместимых мобильных устройств	Samsung Galaxy S5/S5 mini Samsung Galaxy Tab 10.1 Samsung Galaxy Note4 YotaPhone 1/2
Криптографические средства защиты для центральной точки	С-Терра Шлюз линейки 100/1000/3000/7000 С-Терра Виртуальный Шлюз Модуль МСМ 950

Выбор оборудования и приобретение комплекса

Для выбора конкретных моделей оборудования необходимо учитывать объем и тип передаваемого трафика, требования к резервированию, отказоустойчивости и т.д. Рекомендации по выбору представлены в таблице ниже:

Таблица 2. Расчет примерного состава решения по защите мобильных устройств пользователей для доступа к информационной системе компании

	До 10 устройств	**До 100 устройств**	**До 500 устройств**
Клиентская часть	10xC-Терра Клиент-М	100xC-Терра Клиент-М	500xC-Терра Клиент-М
Серверная часть	1xC-Терра Виртуальный Шлюз (лицензия на 1 ядро) *или* 1xC-Терра Шлюз 100	1xC-Терра Виртуальный Шлюз (лицензия на 4 ядра) *или* 1xC-Терра Шлюз 3000LE	2xC-Терра Виртуальный Шлюз (лицензия на 4 ядра) *или* 2xC-Терра Шлюз 3000 *или* 1xC-Терра Шлюз 7000

Приведенные в таблице 2 данные носят ориентировочный характер, поскольку трафик целевых приложений может отличаться в различных прикладных задачах. Данные в таблицах приведены для одновременной работы пользователей. Если сеансы пользователей статистически распределены во времени, требуемая мощность шлюза серверной части может быть снижена.

Получить помощь в выборе продуктов и оборудования, а также расчет стоимости решения для вашей организации Вы можете, обратившись к нашим менеджерам:
– по телефону: +7 499 940-90-61
– или по электронной почте: sales@s-terra.com
Вам обязательно помогут!

Citrix Ready

Для повышения уровня защищенности системы удаленного доступа необходим контроль за мобильными устройствами пользователей. Он осуществляется с помощью так называемых Mobile Device Management (MDM) систем. Они представляют собой комплексное решение для управления и аудита мобильными устройствами, приложениями и данными пользователя. Использование данного подхода позволяет набором приложений пользователя, его привилегиями, при необходимости ограничивать эксплуатацию взломанных или украденных.

Управление устройствами с помощью MDM происходит удаленно и централизованно. Трафику управления, как и трафику пользователя, необходима защита, которая реализуется VPN-клиентом.

Компании С-Терра и Citrix провели совместное тестирование своих продуктов – Citrix MDM и С-Терра Клиент-М. Тестирование подтвердило стабильную совместную работу продуктов, по его результатам продукту С-Терра Клиент-М присвоен статус Citrix Ready (citrixready.citrix.com/s-terra-csp/s-terra-client-m.html).

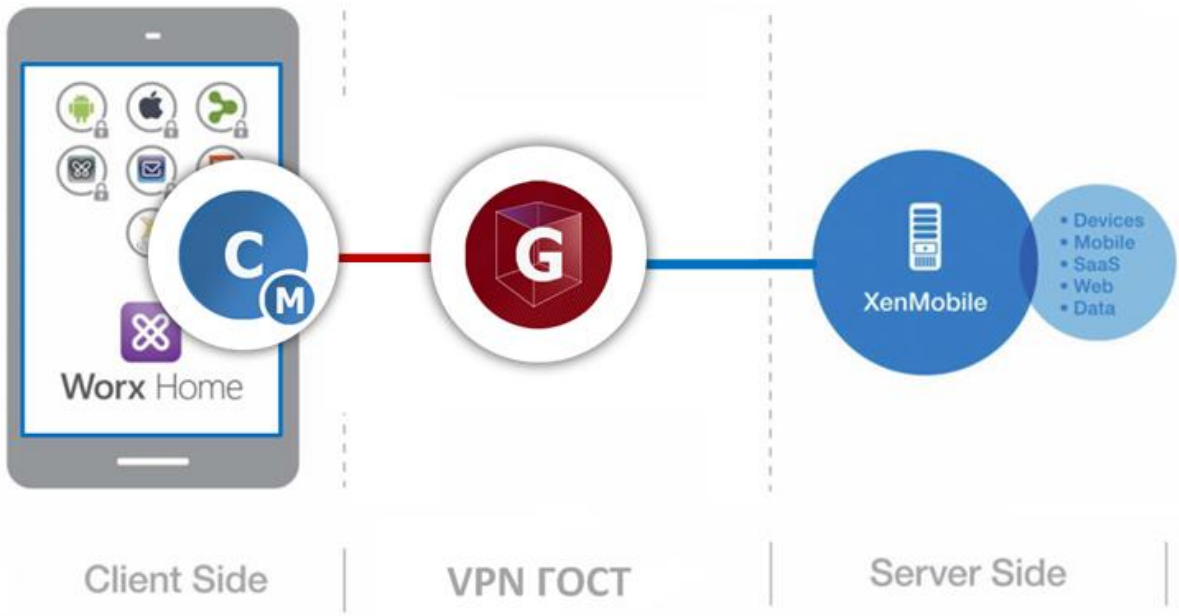

Рисунок 3. Пример защиты удаленного доступа с мобильных устройств сотрудников в сочетании с MDM-системой Citrix XenMobile

Сведения о производителе

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.

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/