s•terra

ЗАЩИТА
УДАЛЕННОГО ДОСТУПА

Задача

Одним из инструментов развития современного бизнеса является повсеместное использование информационных технологий. Сотрудникам компаний необходим доступ к корпоративной информации из любой точки мира, поэтому от информационных систем требуется гибкость и способность быстро подстраиваться под новые условия. Перед службами безопасности компаний стоит непростая задача: предоставить пользователям удобное решение, обеспечивающее удаленный доступ к сервисам компании, сохранив высокий уровень защищенности, включая:

- организацию индивидуального защищенного удаленного доступа к виртуальным рабочим столам, сервисам или приложениям;
- контроль и разграничение доступа пользователей к сервисам и ресурсам компании;
- соблюдение требований законодательства.

VPN-продукты С-Терра уже более 15 лет успешно используются для реализации такой задачи.

Состав решения

На каждое конечное устройство пользователя, работающего вне контролируемой зоны, устанавливается программный VPN-клиент – С-Терра Клиент, обеспечивающий криптографическую защиту передаваемого трафика, а также контроль сессий и пакетную фильтрацию. Перед тем, как пользователю предоставляется доступ к сервисам компании, он проходит процедуру аутентификации путем ввода пароля и цифрового сертификата открытого ключа, закрытый ключ которого может храниться на токене.

На площадке компании устанавливается С-Терра Шлюз в одной из модификаций:

- С-Терра Шлюз в виде программно-аппаратного комплекса,
- С-Терра Виртуальный Шлюз,
- Криптомаршрутизатор ESR-ST,
- С-Терра CSCO-STVM.

Для централизованного управления необходима система управления – С-Терра КП.

Преимущества решения

При запуске С-Терра Клиент на рабочей станции пользователя, между ней и точкой доступа в корпоративную сеть устанавливается защищенное VPN-соединение на основе набора протоколов IKE/IPsec с применением отечественных криптоалгоритмов ГОСТ 28147-89, ГОСТ Р 34.10/34.11-2012 и ГОСТ Р 34.12/34.13-2015.

При этом имеется возможность:

- Запретить прямой доступ с рабочей станции к незащищенным ресурсам. Организовать доступ через корпоративный прокси-сервер, обеспечив полную изоляцию сетевой среды.
- Выдавать подключившимся устройствам IP-адреса из предопределенного пула, на основе данных адресов возможно дальнейшее разграничение доступа внутри корпоративной сети. Также имеется возможность задания адреса DNS сервера.

- Реализовать дополнительную аутентификацию на RADIUS сервере (в том числе XAUTH).
- Использовать инкапсуляцию IPsec трафика в протокол HTTP. Это позволяет строить защищенные соединения, даже если у провайдеров разрешен только HTTP (например, в публичных местах).
- В качестве дополнительного фактора аутентификации использовать токены eToken Pro 72k (Java), JaCarta PKI, JaCarta PKI/ГОСТ, Рутокен Lite, Рутокен ЭЦП.
- Удаленно обновлять политику безопасности С-Терра Клиент при помощи С-Терра КП.

Соответствие требованиям регуляторов

Решение позволяет выполнить требования российского законодательства, так как входящие в его состав продукты обладают сертификатами соответствия:

- ФСБ России СКЗИ по классам КС1 и КС2,
- ФСТЭК России межсетевой экран уровня хоста (тип «В») 4 класса,

и внесены в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Рекомендации по выбору продуктов

Для выбора конкретных продуктов, кроме требуемого класса защиты, необходимо учитывать тип передаваемого трафика, количество пользователей, требования к резервированию и отказоустойчивости. Рекомендации по выбору оборудования представлены в таблицах 1 и 2.

Таблица 1. Расчет примерного состава решения по защите доступа на базе С-Терра Клиент. СКЗИ класса КС1 на стороне периметра.

Количество устройств	**До 10 устройств**	**До 100 устройств**	**500 и более устройств**
Пропускная способность серверной части	20 Мбит/с	250 Мбит/с	1 Гбит/с
Управление	1хС-Терра КП (лицензия на 10 устройств)	1хС-Терра КП (лицензия на 100 устройств)	1х С-Терра КП (лицензия на 500 и более устройств)
Серверная часть	1хС-Терра Виртуальный Шлюз (лицензия на 1 ядро) или 1хС-Терра Шлюз 100	1хС-Терра Виртуальный Шлюз (лицензия на 4 ядра) или 1хС-Терра Шлюз 3000	2хС-Терра Виртуальный Шлюз (лицензия на 12 ядер) или 2хС-Терра Шлюз 7000 *В режиме горячего резервирования*
Клиентская часть	10хС-Терра Клиент	100хС-Терра Клиент	500хС-Терра Клиент

Таблица 2. Расчет примерного состава решения по защите доступа на базе С-Терра Клиент. СКЗИ класса КС2 на стороне периметра.

Количество устройств	**До 10 устройств**	**До 100 устройств**	**500 и более устройств**
Пропускная способность серверной части	20 Мбит/с	250 Мбит/с	1 Гбит/с
Управление	1хС-Терра КП (лицензия на 10 устройств)	1хС-Терра КП (лицензия на 100 устройств)	1х С-Терра КП (лицензия на 500 и более устройств)
Серверная часть	1хС-Терра Шлюз 100	1хС-Терра Шлюз 3000	2хС-Терра Шлюз 7000 *В режиме горячего резервирования*
Клиентская часть	10хС-Терра Клиент*	100хС-Терра Клиент*	500хС-Терра Клиент*

* для класса защиты КС2 на рабочих станциях требуется АПМДЗ, сертифицированный ФСБ России, из перечня совместимых: Соболь, Аккорд-АМДЗ, КРИПТОН-ЗАМОК и МАКСИМ-М1.

Приведенные в таблицах 1 и 2 данные носят ориентировочный характер, поскольку трафик целевых приложений может отличаться в различных прикладных задачах. Кроме того, при оценке производительности шлюза безопасности следует учитывать статистику сеансов доступа. Данные в таблицах приведены для одновременной работы пользователей. Если сеансы пользователей статистически распределены во времени, требуемая мощность шлюза серверной части может быть снижена.

О компании «С-Терра СиЭсПи»

Компания «С-Терра СиЭсПи» с 2003 года является ведущим российским разработчиком и производителем средств сетевой защиты на основе технологии IPsec VPN.

Продукты С-Терра, сертифицированные ФСТЭК России и ФСБ России, используют современные российские криптографические алгоритмы ГОСТ и включены в Единый реестр российских программ для электронных вычислительных машин и баз данных (Реестр российского ПО).

Решения С-Терра обеспечивают защиту каналов связи любой производительности:

- на сетевом и на канальном уровне,
- в виртуальной инфраструктуре,
- при удаленном доступе, в том числе с мобильных платформ,
- при доступе к VDI и с использованием технологии построения доверенного сеанса.

Специальные решения С-Терра применяются для защиты:

- каналов связи банкоматов,
- подключения к СМЭВ,
- взаимодействия между ЦОД.

Широкое применение

- в госструктурах различных уровней,
- в крупнейших финансовых организациях,
- в коммерческих фирмах,
- на производственных предприятиях

обусловлено высокой производительностью, масштабируемостью, надежностью и сетевой функциональностью решений.

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