






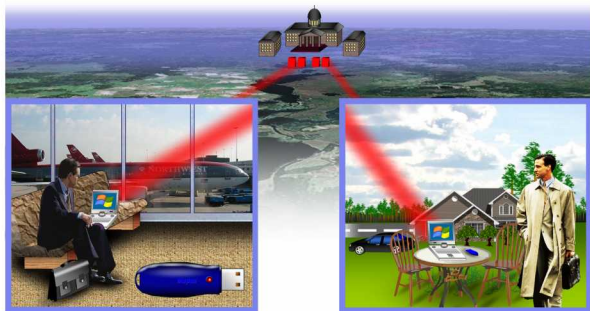
СРЕДА ПОСТРОЕНИЯ ДОВЕРЕННОГО СЕАНСА

Задача организации удаленного доступа пользователей весьма актуальна для государственных и коммерческих организаций, причем потребность в защите доступа растет год от года.

В системах удаленного доступа риски информационной безопасности, как правило, выше, чем в локальных сетях:

-  Без административного контроля пользователь может отступать от регламента безопасности, в частности - пытаться отключить предписанные механизмы защиты.
-  Окружение пользователя может быть более агрессивным, злоумышленник может вести скрытое наблюдение за ним или применять попытки атак social engineering.
-  Оборудование без присмотра пользователя может быть компрометировано или похищено.
-  Вычислительная среда рабочего места удаленного пользователя может быть заражена опасным кодом, содержать программные закладки.
-  Сетевая среда пользователя может быть незамкнута, с рабочего места пользователя могут быть установлены опасные посторонние соединения.

Администратор безопасности не может с достоверностью контролировать все перечисленные риски и поэтому удаленный доступ для него всегда представляется не до конца решенной проблемой безопасности.



Перечисленные риски могут быть существенно снижены в случае применения среды построения доверенного сеанса (СПДС), обеспечивающей:

- Целостность программной среды терминала удаленного доступа.
- Изоляцию вычислительного процесса клиента удаленного доступа при использовании «грязной» (недоверенной) среды.
- Строгую аутентификацию пользователя, криптографически стойкий контроль доступа, изоляцию сетевой среды удаленных пользователей, целостность передаваемых данных, защиту потока пакетов от внедрения посторонних данных, включая повтор ранее переданных пакетов.
- Масштабируемость сети удаленного доступа до сотен тысяч пользователей. Высокую экономическую эффективность решения в целом.
- Применение сертифицированных средств криптографической защиты информации.
- Настройку функциональности среды на доступ к информационным сервисам. Доступ осуществляется в защищенном режиме к веб- и терминальным сервисам, покрывая полный спектр потребностей Заказчика.

Структура, принцип работы

Среда построения доверенного сеанса включает следующие средства защиты информации:

- Специальный загрузочный носитель (СЗН) «Марш!» емкостью 4 ГБ. Конструкция СЗН «Марш!» гарантирует целостность размещенных на специальном носителе данных и программного обеспечения.
- Модуль доверенной загрузки, обеспечивающий аутентификацию пользователя и загрузку среды функционирования ПО.



- Среда функционирования (СФ) прикладного программного обеспечения на основе специально подготовленной ОС Linux (CentOS 5). В составе СФ работают средства криптографической защиты информации «КриптоПро 3.6» и продукт CSP VPN Gate в исполнении «Марш!-USB».
- Прикладное программное обеспечение – веб-браузер или клиент терминального доступа на основе протокола RDP.

Для работы с продуктом пользователь должен настроить свое рабочее место на загрузку с USB носителя и произвести загрузку операционной системы со специального загрузочного носителя. После этого на рабочее место будет произведена загрузка эталона СФ, для которого гарантирована целостность и в которой пользователю предоставля-

ется доступ только к целевому приложению. Доступа к операционной системе пользователь в ходе сеанса не получает. Среда выгружается сразу после выхода пользователя из целевого приложения, причем никаких следов работы пользователя в системе (cash-, swap-, временные файлы) не остается.

Изоляция сетевой среды

Весь трафик рабочего места пользователя защищается на основе технологий IPsec VPN, которые, в отличие от технологий SSL или TLS, обеспечивают перехват и обработку

каждого сетевого пакета. В сеть может войти только владелец секретного ключа, открытый трафик отсутствует. Нарушение целостности пакетов и потока пакетов исключены, защищенный канал не примет даже ранее переданный легитимный пакет. Таким образом достигается полная изоляция сетевой среды в рамках доверенного сеанса.

Защита от хищения

Модуль загрузки СПДС обеспечивает доступ к среде функционирования только при вводе оператором PIN-кода. Число попыток ограничено тремя операциями ввода, после чего продукт закрывается для пользователя и поступает к администратору безопасности для расследования события потенциального несанкционированного доступа. Таким образом обеспечивается надежный контроль доступа к доверенному сеансу.

Стандартные приложения

СПДС «Марш!» выпускается в двух стандартных исполнениях: «W» (веб) и «Т» (терминал). Для ввода в эксплуатацию стандартных исполнений достаточно установить перед серверами целевых приложений веб-шлюз и настроить удаленный доступ пользователей в соответствии со сценариями построения VPN удаленного доступа. Однако в ряде случаев Заказчик выдвигает дополнительные требования.

Специфические решения

Дополнительные требования, как правило, возникают в трех областях:

- Применение нестандартных (мобильных) сред доступа. Например, расширенные СФ СПДС могут работать в сетях 3G (CDMA) и 4G (WiMAX).
- Организация файлового обмена с внешними (недоверенными или условно доверенными) системами.
- Применение в целевых приложениях криптографических функций, например, ЭЦП веб-документов.

Построение решений, удовлетворяющих таким специфическим требованиям, требует специальной настройки среды функционирования и выполняется в режиме пилотного проекта.

Сертификация

СПДС в исполнении «Марш!-USB» сертифицирована как СКЗИ класса КС2. На СПДС распространяются все сертификаты продукта CSP VPN Gate. Продукт применим в АС класса 1Г и ИСПДн класса К1.

Поставки СПДС

Продукты в стандартных исполнениях доступны для закупок (крупные серии изделий требуют предварительного заказа). Для реализации дополнительных требований Заказчика организуется пилотный проект и доработка среды функционирования. При этом базовая цена продуктов СПДС не увеличивается. Для заказа продуктов, организации пилотного проекта или получения дополнительной информации необходимо отправить запрос по адресу sales@s-terra.com.