ФАКТОР·ТС

DISEC-W

КЛИЕНТ ЗАЩИЩЕННОГО ДОСТУПА ДЛЯ УСТРОЙСТВ НА БАЗЕ ОС WINDOWS

МОСКВА 2023

DiSec-W
клиент криптографического сервера доступа

DiSec-W – решение для эффективной защиты передаваемого трафика от рабочих станций и мобильных устройств под управлением ОС Windows в корпоративную сеть. DiSec-W обеспечивает конфиденциальность передачи информации и ее защиту на вашем персональном устройстве, а также надежно защищает работу с корпоративными данными через Интернет.

Сертификат ФСБ:
КС1, КС2, КС3

Преимущества:

- максимально быстрое соединение и стабильная работа приложения на каналах связи любого качества;
- автоматическое восстановление VPN защищенного соединения при временных разрывах связи;
- автоматическое переключение на резервный VPN канал;
- использование централизованных корпоративных сервисов для контроля трафика в целях защиты устройства;
- защита от вмешательств в удаленное соединение и MITM-атак.

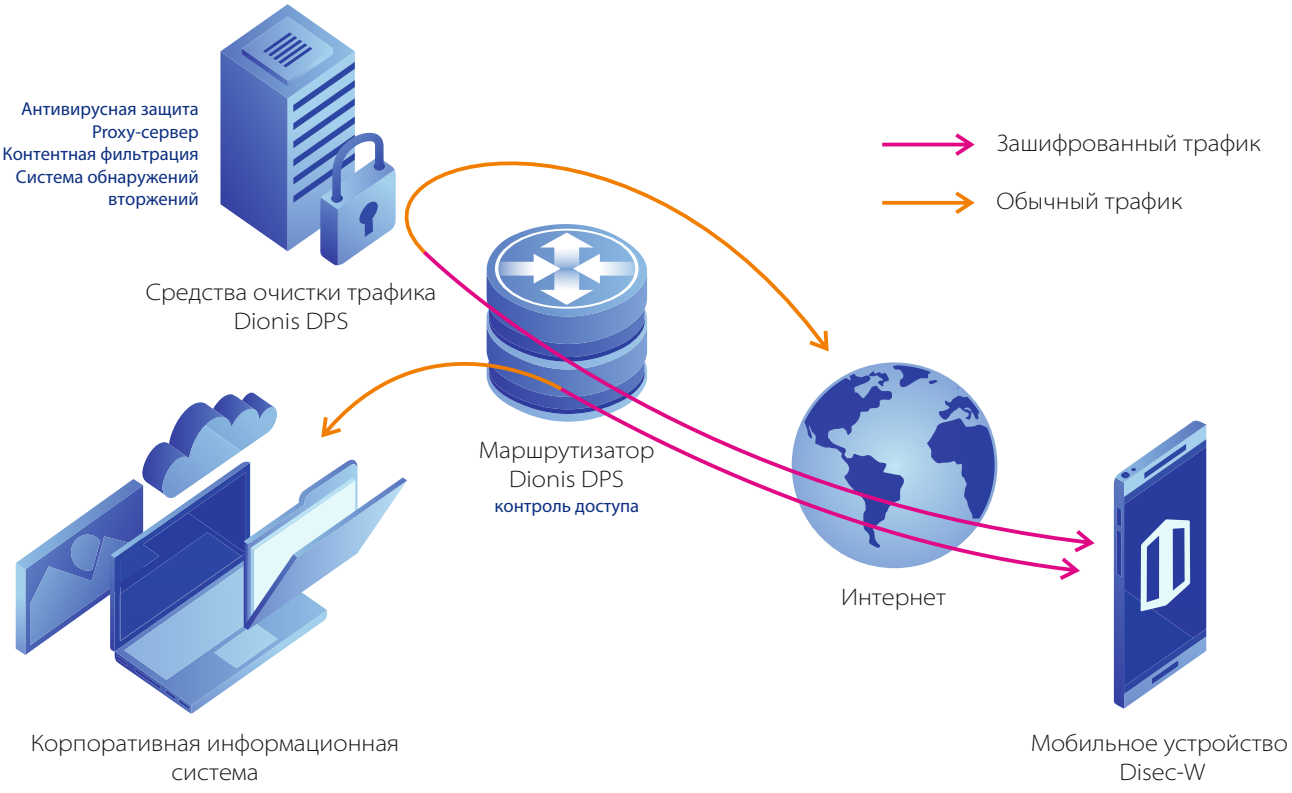

Рис. 1. Сценарий использования DiSec-W

Основные характеристики	
Категория программы	VPN-клиент, реализующий набор протоколов IPSEC (IPSecurity)
Назначение программы	Создание виртуального канала между компьютером пользователя и VPN-сервером для доступа к ресурсам защищенной сети.
Тип виртуального канала	IPSec с шифрованием и контролем целостности передаваемого трафика
Тип VPN-сервера	программно-аппаратный комплекс Dionis-NX
Операционная платформа (ОС Windows)	Десктоп-компьютеры Серверы Ноутбуки Планшеты
Сетевые конфигурации	Совместимость с любыми сетевыми интерфейсами, в том числе с Wi-Fi (статический и динамический IP-адрес), мобильные широкополосные модемы GSM
Количество одновременных подключений	не более 10
Типы подключений (по способу организации)	Статический с настройками правил отбора и выбором типа инкапсуляции Динамический (IKE v1)
Количество туннелей в подключении (каждый туннель предоставляет доступ к одному целевому объекту из списка в настройках подключения или соответствует одному правилу отбора)	Не ограничено на стороне DiSec
Режимы взаимной аутентификации клиента и сервера	Динамический: инфраструктура PKI (асимметричные ключи шифрования). Статический: симметричные ключи шифрования
Лицензирование	Защита ключом регистрации - разрешена установка на одном компьютере. Возможно использование Лицензии на ограниченный срок действия

Программная операционная среда	
Поддерживаемые операционные системы: Microsoft Windows (x64)	Microsoft Windows 10 Microsoft Windows Server 2016
Совместимость со средствами защиты	- Функционирует при наличии установленного антивирусного ПО - требуется тестирование при наличии средств VPN
Совместимость со средствами мониторинга сети (анализаторы трафика)	да
Тип VPN-сервера	программно-аппаратный комплекс Dionis-NX
Вход в домен Windows по защищенному каналу (установление виртуального канала ДО входа пользователя в систему)	Автоматическая установка туннеля в режиме службы Windows (служба DiSecSRV)
Возможность авто-подключения при входе пользователя в систему	1) Несколько подключений одновременно 2) Несколько подключений последовательно, переход на следующий при разрыве соединения.
Сетевые конфигурации	
Поддерживаемые сетевые интерфейсы	Ethernet Wi-Fi Модем телефонной линии Mobile Broadband modem
Стек TCP\IP	Ipv4 Ipv6 - поддерживается для статических туннелей
Поддержка нескольких сетевых интерфейсов	- Автоматическое определение сетевого интерфейса для туннеля и маршрутизация трафика - возможность блокирования "открытого" трафика при наличии\отсутствии туннеля
Работа через NAT (NAT Traversal)	Динамический: NAT Traversal Статический: UDP-инкапсуляция - настраиваемые порты
Изменение сетевой конфигурации компьютера	Отслеживает отключение и подключение сетевых адаптеров - автоматически отключает туннель.

Особенности реализации	
Шифрование и контроль целостности передаваемого трафика	Динамический: Протоколы IPsec ESP (RFC2401-2412), с использованием (только) российских криптографических алгоритмов. Статический: Протоколы IPsec: "IP Encapsulation within IP" (RFC 2003), с использованием (только) российских криптографических алгоритмов.
Аутентификация взаимодействующих сторон	Динамический: по протоколу IKE (RFC 2407-2409 и RFC 4303) с использованием сертификатов X509 (RFC 5280). Статический: Использование симметричных ключей.
Режимы туннелирования	Динамический: - транспортный и туннельный режимы ESP-инкапсуляции. Статический: - туннельный режим "IP-in-IP" - UDP-инкапсуляция пакет (поверх IP-in-IP)
Режимы инкапсуляции	Динамический: -ESP_GOST-4M-IMIT, -ESP_GOST-1K-IMIT - UDP\ESP-инкапсуляция (NAT-Traversal) Статический: UDP-инкапсуляция пакет (поверх IP-in-IP). Настройка портов по согласованию с оппонентом (Сервером VPN)
Информационные обмены протокола ISAKMP\IKE	Динамический: IKEv1 - Main mode - Quick mode - Informational Exchanges - Transaction Exchanges (MODECFG) IKEv2 - не реализован Статический: отсутствуют
Алгоритмы выработки сессионных ключей	Динамический: - VKO ГОСТ Р 34.10-2012 - VKO_GOSTR3410_2012_256, - VKO_GOSTR3410_2012_512 Статический: ГОСТ28147-89
Алгоритмы шифрования	- ГОСТ28147-89
Алгоритмы контроля целостности сетевых пакетов	Динамический: - ГОСТ Р 34.11-2012 - ESP_GOST-4M-IMIT, - ESP_GOST-1K-IMIT Статический: ГОСТ Р 34.11-94
Алгоритмы электронной цифровой подписи (ЭЦП)	Динамический: - ГОСТ Р 34.10-2012

Журналирование и протоколирование	
Журнал действий пользователя	- начало\окончание сеанса пользователя с указанием имени пользователя - основные этапы установки подключения, возникшие ошибки - смена пользователя Windows
Протоколирование сетевого трафика	Опционально при включении данной опции администратором.
Системный журнал (Event Log, System Log)	Фиксируются ошибки функционирования виртуального канала драйвером (источник данных DISEC). Для приложения и службы - фиксируются события безопасности (положительные и отрицательные). Источник данных DISECAPP.
Сбор статистики сети в целом, а также по интерфейсам	Начиная от загрузки ОС: - количество пакетов принятого и переданного трафика; - количество сброшенных пакетов с разбивкой по причинам (блокировка, ошибки); - количество ошибочных пакетов с разбивкой по типу ошибок (крипто, нехватка памяти, искаженные IP\TCP-пакеты)
Статистика Туннелей	Динамический: - число пакетов с искаженной контр. суммой (Integrity Fail); - статистика нарушения нумерации пакетов (Replay атаки). Статический: статистика нарушения нумерации пакетов (Replay атаки).
Криптография	
Криптографические библиотеки	Встроенные библиотеки разработки ООО "Фактор-ТС"
Поддерживаемые ключевые носители	- флэш-память USB - Токены производства компании Aladdin: eToken PRO32k – при наличии драйверов производителя - Токены производства компании Актив: Рутокен, Рутокен S - при наличии драйверов производителя
Формат ключевого контейнера	Динамический: - PKCS#15 - объекты PKCS#11 с контейнером ключа PKCS#15 Статический: контейнер
Формат сертификатов публичных ключей	X.509 v.3 (ГОСТ)
Поддержка списка отозванных сертификатов	Обновление и обработка Certificate Revocation List (CRL). Поддерживается CRL v.2. Способ получения CRL – протокол LDAP v.3, FTP, HTTP
Контроль валидности сертификатов по протоколу OCSP.	Опционально.

Москва, 1-й Магистральный пр-д,
дом 11, строение 1

dps.factor-ts.ru
sales@factor-ts.ru
+7 (495) 644 31 30