infotecs

ViPNet Terminal 4

Защищенное терминальное решение

ПАК ViPNet Terminal 4 представляет собой линейку устройств с интегрированным программным обеспечением производства ОАО «ИнфоТеКС»

ViPNet Terminal 4 является универсальным средством для организации защищенного рабочего места пользователя, совмещающего в себе функциональность АРМ (автоматизированного рабочего места) и СЗИ (средства защиты информации)

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

Для организации зашифрованных терминальных сессий ViPNet Terminal 4 использует не встроенные механизмы ОС Windows или Linux, а VPN-технологию ViPNet.

По этой причине перед терминальным сервером Windows должен быть установлен любой из программно-аппаратных криптошлюзов ViPNet Coordinator HW либо непосредственно на терминальный сервер должно быть установлено ПО ViPNet Coordinator. При этом может быть реализовано множество сценариев организации защищенного рабочего места пользователя:

- создание защищенных удаленных офисов, филиалов с использованием инфраструктуры центрального офиса
- организация удаленного защищенного доступа к корпоративным ресурсам (ЦОДам и облакам) из публичных точек, используя недоверенный ПК (ноутбук)
- организация защищенных публичных точек доступа (инфоматов) к ресурсам учреждений для сдачи отчетности, работы с ПДн
- организация рабочих мест банковских служащих, сотрудников кадровых служб и бухгалтерии, работающих с конфиденциальной информацией и ПДн

ВОЗМОЖНОСТИ

ViPNet Terminal 4 – это тонкий клиент, который позволяет в любой телекоммуникационной инфраструктуре, включая сети связи общего пользования, организовать защищенный доступ к удаленному или виртуальному рабочему столу пользователя, размещенному на терминальном сервере.

Функции безопасности

- **VPN-клиент** – стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) посредством шифрования трафика и передачи этого трафика на защищаемые VPN-шлюзами открытые ресурсы или другие защищенные клиенты.
- **Межсетевой экран** – функция, благодаря которой ViPNet Terminal 4 выполняет фильтрацию открытых и зашифрованных сетевых соединений по IP-адресам, протоколам, портам, направлениям соединений и другим параметрам на основании заданных правил.
- **Аутентификация (двухфакторная)** – процесс идентификации пользователя на основании его учетной записи (однофакторная) либо на основании учетной записи и внешнего устройства (двухфакторная).
- **Электронная подпись (ЭП)** – при работе с прикладным программным обеспечением ViPNet Terminal 4 позволяет пользователю использовать ключи ЭП, хранящиеся на USB-токене, в том числе для подписи электронных документов.
- **Контроль над выводом информации** – ViPNet Terminal 4 предоставляет возможность печати документов на локальных и сетевых принтерах и возможность сохранять данные на отчуждаемых носителях (USB носители, подключаемые жесткие диски), обрабатываемых на терминальном сервере. С целью защиты от утечки информации данные возможности полностью определяются политиками безопасности и никак не зависят от действий пользователя.

Функции терминального клиента

- Доступ к удаленному рабочему столу на терминальном сервере Windows Server по протоколу RDP.
- Доступ к удаленному рабочему столу и опубликованным приложениям на сервере Citrix (по протоколам ICA, HTTP/HTTPS).
- Доступ к виртуальным рабочим столам, реализованным по технологии VMware Horizon View (по протоколам PCoIP, Blast и RDP).
- Доступ к виртуальным рабочим столам, реализованным по технологии IBS Parallels VDI.
- Доступ к виртуальным рабочим столам, реализованным по технологии Fusion Access (по протоколу HDP – Huawei Desktop Protocol).
- Доступ к видеоконференциям TrueConf и Vinteo.
- Доступ к службам, реализованным по технологии Web Access (по протоколам HTTP и HTTPS).

ПРЕИМУЩЕСТВА

1. ViPNet Terminal 4 создан на аппаратной платформе, без механических элементов (отсутствуют вентилятор и жесткий диск), обладает малыми размерами и весом, отличается низким потреблением электроэнергии и устойчив к сбоям электропитания.

2. Перечень прикладного программного обеспечения, доступного пользователю для работы, контролируется администратором терминального сервера. Пользователь не может самостоятельно устанавливать и удалять какое-либо программное обеспечение, сохранять данные на USB носителе, если это не разрешено политиками информационной безопасности.

3. ViPNet Terminal 4 не производит хранение и обработку данных, а лишь осуществляет их отображение на экране монитора в терминальной сессии.

4. Поддержка работы с сетевым и локально подключенным принтером, что позволяет пользователю распечатывать документы, если это не запрещено политиками информационной безопасности.

5. Возможность сохранения данных на отчуждаемые носители (USB носители), подключаемые жесткие диски обрабатываемые на терминальном сервере, если это не запрещено политиками информационной безопасности, что обеспечивает удобство при работе с документами.

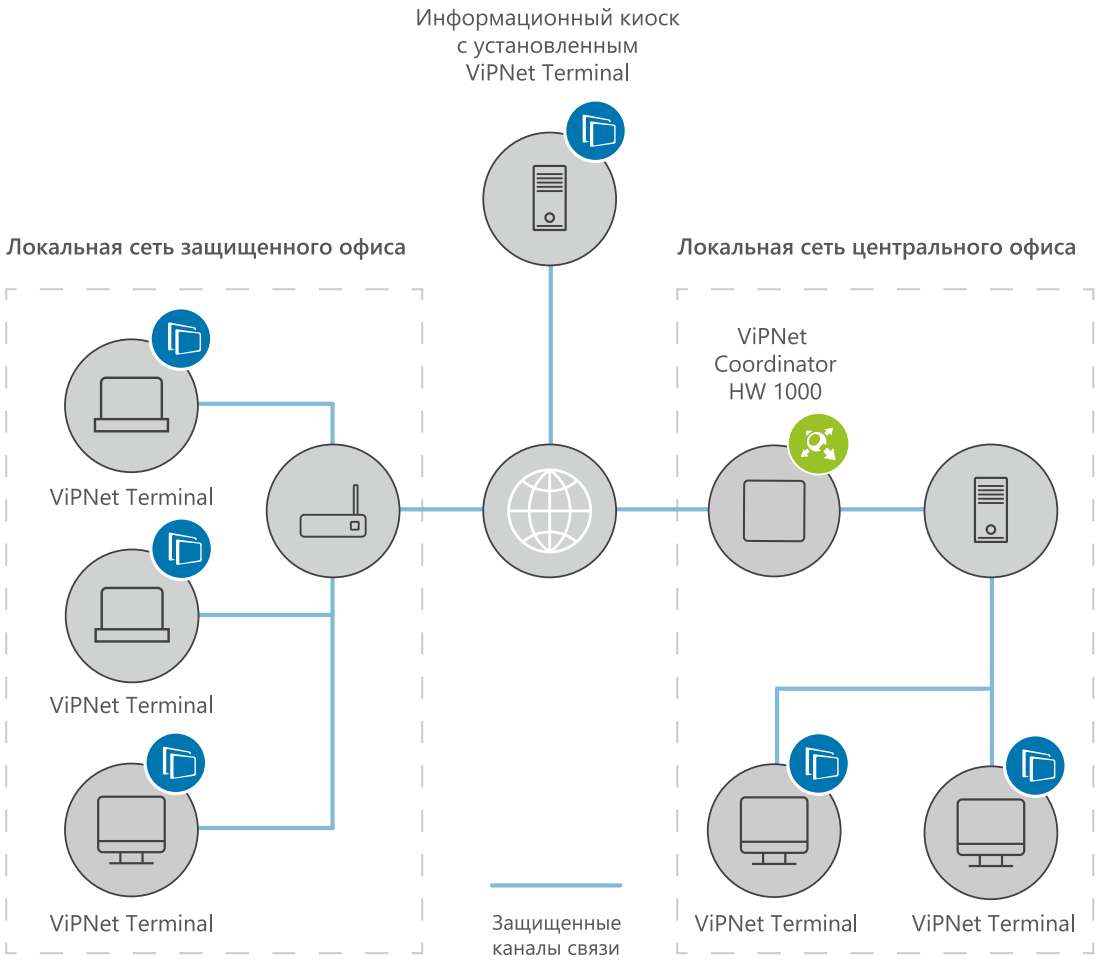
6. ViPNet Terminal 4, как и ViPNet Client, является персональным сетевым экраном и шифратором IP-трафика по ГОСТ 28147-89, поэтому он защищен от сетевых атак и вмешательства в терминальную сессию пользователя с целью перехвата логина и пароля пользователя или навязывания ложных терминальных серверов. Обновление ключей шифрования может осуществляться локально или удаленно через ПО ViPNet Adminstrator.

7. ViPNet Terminal 4 позволяет использовать все преимущества VPN-технологии ViPNet по организации удаленного защищенного доступа к терминальным серверам через любые доступные каналы связи.

8. Производительность аппаратной платформы ViPNet Terminal 4 никак не влияет на возможность запуска тех или иных приложений – все определяется лишь производительностью терминального сервера, поэтому эффективное время эксплуатации ViPNet Terminal 4 без необходимости апгрейда рабочего места пользователя может составлять 5–7 лет, а не 2–3 года, как в случае с обычной рабочей станцией.

9. Поддержка работы различных мультимедийных приложений, позволяющая использовать его в системах IP-телефонии и видеоконференцсвязи.

10. В результате указанные выше преимущества позволяют организовать защищенную инфраструктуру компании без значительных капиталовложений и снизить затраты на обслуживание.


Информационный киоск
с установленным
ViPNet Terminal
Локальная сеть защищенного офиса
Локальная сеть центрального офиса
ViPNet
Coordinator
HW 1000
ViPNet Terminal
ViPNet Terminal
ViPNet Terminal
ViPNet Terminal
ViPNet Terminal
Защищенные
каналы связи

VPN

Шифрование по ГОСТ 28147-89 (256 бит)	Технология ViPNet без потери качества соединения обеспечивает постоянство тех свойств защищенного соединения, которые существенно влияют на безопасность. А именно: постоянное шифрование всего IP-пакета вместе с исходными IP-адресами и протоколами, постоянное обеспечение имитозащиты пакета (защиты от навязывания ложных пакетов), шифрование всего трафика (а не только части трафика) в направлении заданного защищенного узла
Аутентификация и контроль целостности для каждого зашифрованного IP-пакета	Для обеспечения целостности защищенных данных в технологии ViPNet используется имитозащитная вставка, по которой при расшифровании данных можно проверить, соответствует ли входящий пакет данных исходящему. Вероятность получения искаженного пакета менее 10^{-18}
Автоматическое распределение ключевой информации при модификации VPN сети	В технологии ViPNet для организации защищенного соединения используется схема с автоматически распределенными на этапе установки ПО симметричными ключами шифрования и автоматической процедурой их синхронного обновления
Прозрачность для NAT-устройств	Протокол UDP, используемый в рамках технологии ViPNet, обеспечивает защищенную передачу данных по любым каналам связи, через любые устройства NAT/PAT – даже в том случае, когда интернет-провайдер препятствует установлению соединения путем запрета VoIP или авторизующих соединений IPsec.
Бесшовная работа при смене адреса доступа	В технологии ViPNet применяются пиринговые соединения, которые обеспечивают автоматическое оповещение связанных узлов о параметрах доступа друг к другу. Это позволяет реализовать не только классические для IPsec схемы site-to site и client-to-site, но также схему client-to-client в автоматическом режиме и с возможностью объединения неограниченного количества компьютеров, независимо от точки их подключения к сети, принадлежности определенной VPN-сети, без централизованной раздачи IP-адресов.
Поддержка технологии виртуальных ip-адресов	При объединении нескольких LAN в единую VPN-сеть или организации прямого взаимодействия компьютеров (в том числе мобильных) возникает проблема пересечения диапазонов IP-адресов. В технологии ViPNet при взаимодействии компьютеров используются виртуальные IP-адреса, уникальные для каждого сетевого узла сети ViPNet или для туннелируемых узлов в пределах локальной сети. Таким образом, пересечение диапазонов IP-адресов устраняется автоматически, без вмешательства технического персонала и изменения адресной структуры существующих сетей.
Реализация VPN для мультимедиа трафика (VoIP, videoconference)	Каждый пакет, который отправляется в сеть, автоматически шифруется с использованием уникального производного ключа, без каких-либо процедур установления соединения (handshaking). Это позволяет организовывать защищенную передачу данных по ненадежным каналам, по каналам, которые характеризуются большими потерями трафика (спутниковые каналы, модемное соединение и так далее), а также обеспечивать бесперебойную работу локальной сети, для которой недопустимы задержки в установлении соединений.

Межсетевой экран

Фильтрация трафика с учетом состояния сессии (stateful packet inspection)	С помощью правил фильтрации можно контролировать протокол, адрес и порт отправителя, адрес и порт получателя, направление установления соединения. Применение фильтрации пакетов по направлению установления соединения позволяет ограничить прохождение пакетов рамками установленных соединений: пропускать только запросы, инициализирующие соединения в заданном направлении, а также ответы на них, и запрещать запросы, инициализирующие соединения в обратном направлении.
Инспекция прикладных протоколов	Функция обработки прикладных протоколов обеспечивает: • подмену виртуального IP-адреса в теле пакета на реальный IP-адрес в случае использования технологии виртуальных IP-адресов • подмену IP-адреса защищаемого узла в прикладном протоколе на транслируемый адрес в случае использования технологии трансляции адресов • активацию разрешающего сетевого фильтра для дополнительного соединения на случайно выбранный порт, открываемый прикладным протоколом

Контроль фрагментированных пакетов, предотвращение DOS-атак

Антиспуфинг	Основная задача антиспуфинга – это защита от так называемого спуфинга, одного из видов сетевых атак, основанного на подделке IP-адреса.
Поддержка раздельной фильтрации для открытого IP-трафика (функция межсетевого экрана) и VPN-трафика	Фильтрации подвергается весь трафик, который проходит через сетевой узел: • открытый (нешифрованный) трафик • защищенный (зашифрованный) трафик (перед его шифрованием и после расшифровки) • туннелируемый трафик (перед его шифрованием и после расшифровки)

Сетевые возможности

- √ **Поддержка протокола DHCP-client**
- √ **Поддержка NTP-client**
- √ **Статическая маршрутизация**
- √ **Java-апплет мониторинга текущего состояния**

Модификации

ViPNet Terminal 4 TONK

Миниатюрный компьютер, который может быть установлен на любой современный VESA-совместимый монитор. Необходимо лишь подключить стандартную USB-клавиатуру и мышь и включить ViPNet Terminal 4 TONK в компьютерную сеть

Характеристики

Процессор
INTEL Baytrail-D J1900
Quad-Core 2.42GHz
Память 4GbSSD 16Gb

Интерфейсы

4xUSB2.0 + 1xUSB2.0 (расположены на задней части)
1xUSB3.0 (расположен на передней части)
Аналоговые звуковые разъемы
Display Port+DVI + переходник на VGA
Lan 1Gb, Wi-Fi (опционально)

ViPNet Terminal 4 LiveUSB

USB-носитель, который может быть подключен к любому ПК или ноутбуку, поддерживающему загрузку ОС с внешних USB носителей.

Мгновенно превращает любой подходящий компьютер (десктоп, ноутбук) в защищенное рабочее место, позволяя получить доступ к информационным ресурсам компании в любое время и в любом месте.

ОБСЛУЖИВАНИЕ

ГАРАНТИЙНОЕ ОБСЛУЖИВАНИЕ

На ViPNet Terminal 4 предоставляется гарантия 1 год с возможностью продления.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения услуг технического сопровождения необходимо заключать отдельный договор.

Договор заключается сроком на 1 год. После окончания срока по необходимости следует продлить договор. Для приобретения продукта и технической поддержки обращайтесь к официальным партнерам ОАО «ИнфоТеКС».

Пожалуйста, используйте ресурс **http://infotecs.ru/partners/,** чтобы найти ближайшего к вам партнера компании ОАО «ИнфоТеКС».

СЕРТИФИКАЦИЯ

Программно-аппаратный комплекс ViPNet Terminal 4 (Live-USB) сертифицирован в ФСБ России по требованиям к СКЗИ уровня КС1/КС3 и по требованиям к МЭ 4 класса.

infotecs

ОАО «ИнфоТеКС», 127287, Москва,
Старый Петровско-Разумовский проезд, 1/23, стр. 1

+7 495 737-6192, 8 800 250-0-260 (бесплатный звонок по России)

+7 495 737-7278

soft@infotecs.ru, hotline@infotecs.ru

www.infotecs.ru

ViPNet Virtual Private Network

infotecs.ru/f24

Ваше впечатление от листовки: