ViPNet Terminal

Категория: **Сетевые экраны / Виртуальные частные сети**
Исполнение: **Программно-аппаратный комплекс**
Тип операционной системы: **Linux**

Общее описание

Основной проблемой при решении задачи обеспечения защиты конфиденциальной информации в любой организации в настоящее время является проблема внутреннего нарушителя, часто называемая проблемой «инсайдера». Действительно, ни один даже самый надежный криптошлюз или межсетевой экран не могут обеспечить защиту от кражи важной информации недобросовестным сотрудником со своего рабочего компьютера в локальной сети организации. Попытки реализовать защиту от такого нарушителя путем установки на компьютер разнообразных средств защиты от несанкционированного доступа, таких как электронные замки и программного обеспечения DLP (data leak prevention) предотвращения утечек данных, приводят к необходимости осуществления сложных настроек, разрешению разнообразных конфликтов на уровне операционной системы и прикладного ПО и, как следствие, большим затратам на обслуживание подобных решений.

Альтернативой этим решениям является концепция «тонкого клиента» - терминала, через который пользователь получает доступ к терминальному серверу и определенному набору приложений, перечень которых может быть жестко зафиксирован в зависимости от выполняемых пользователем функций. При этом, возможность сохранять данные на отчуждаемые носители (флэшки, подключаемые жесткие диски) через терминал полностью определяется централизованными настройками и никак не зависит от действий пользователя. Такая особенность терминального решения позволяет гарантировать 100% защиту от утечек важной

ViPNet Terminal - это миниатюрный компьютер - терминальный клиент с адаптированной ОС Linux и ПО ViPNet, размером 202x30x133 мм и весом 450 грамм,
информации из корпоративной сети.

который может быть установлен на любой современный VESA-совместимый монитор. К ViPNet Terminal необходимо лишь подключить стандартную USB-клавиатуру и мышь, и включить

ViPNet Terminal в компьютерную сеть. **ViPNet Terminal** предназначен для организации полноценного защищенного рабочего места пользователя, путем установления зашифрованной сессии с терминальными серверами Microsoft Windows Server 2003/2008 по протоколу RDP и Citrix по протоколам ICA/HTTP(s), а так же в качестве тонкого защищенного HTTP(s) клиента, при доступе к WEB ресурсам. ViPNet Terminal поддерживает работу с DHCP, обеспечивает прозрачную авторизацию по учетным записям пользователей в Active Directory с использованием логина и пароля или электронных ключей - USB-токенов. ViPNet Terminal при работе с прикладным программным обеспечением позволяет пользователю использовать ключи ЭЦП, хранящиеся на USB-токене, в том числе для подписи электронных документов. ViPNet Terminal поддерживает работу с сетевыми или локально подключенными принтерами.

Технические характеристики

Аппаратная платформа	Компактный компьютер, представляет собой вычислительную платформу на базе процессора Intel Atom с частотой 1,6 ГГц.
Условия эксплуатации	t - 0..+40 °C
1 Размеры	202x30x133 мм (ШхВхГ)
Масса	450 г (без адаптера переменного тока)
Потребляемая мощность	22 Вт (средняя)
Операционная система	Специализированная ОС Linux
Число сетевых интерфейсов	1 x RJ45 Ethernet 10/100/1000 Карта Wi-Fi 802.11 b/g
Поддержка периферийных устройств	3G модемы Beeline/MTS/MegaFon WiMax модем Yota Электронные ключи Aladdin eToken Pro, eToken Pro (JAVA) Локальные принтеры Xerox, HP (список устройств запрашивайте в ОАО ИнфоТеКс).
Программная совместимость	С любыми VPN-продуктами из решения ViPNet CUSTOM 2.8 и 3.x (ViPNet Coordinator, ViPNet Coordinator Failover, ViPNet Coordinator HW, ViPNet NME-RVPN)
Протоколы **1** туннелирования	По технологии ViPNet (инкапсуляция любого IP-трафика приложений в IP#241 и UDP)
Шифрование/ Аутентификация	Шифрование по ГОСТ 28147-89 (256 бит), Аутентификация для каждого зашифрованного IP-пакета на основе технологии симметричного распределения ключей ViPNet и уникального идентификатора
Поддерживаемые протоколы удаленных сессий	Протокол RDP с версии 5.2 до версии 6.1 включительно (Windows Server 2003/2008); Протоколы ICA, HTTP(s) (Citrix MetaFrame, XenApp 5/6).
Инфраструктура ключей	Парные симметричные ключи шифрования, обеспечивающие гарантированно высокую стойкость шифрования. Симметричная ключевая структура не требует дополнительных открытых процедур синхронизации для формирования ключей, что повышает помехозащищенность системы, исключает задержки в обработке любых сетевых протоколов, обеспечивает мгновенную (по первому поступившему IP-пакету) организацию защищенных сетевых подключений. Автоматическое распределение симметричной ключевой информации при появлении в сети новых пользователей, задании в Центре управления сетью новых связей или удалении существующих связей, компрометации ключей или штатных процедурах смены ключевой информации
Маршрутизация	Статическая маршрутизация; Прозрачность для NAT-устройств; Поддержка DHCP; Автоматическая регулировка параметров MSS в TCP-сессиях для исключения излишней фрагментации трафика, которая может возникать при передаче длинных пакетов; Возможность работы при изменении собственных IP-адресов, IP-адресов NAT - устройств, возможность работы за устройствами с динамическими правилами NAT; Технология назначения виртуальных IP-адресов для любых удаленных узлов.

Фильтрация	Пакетная фильтрация по IP-адресу (диапазон IP) источника и назначения, номерам портов и типу протокола, типу и коду сообщений ICMP, направлению пакетов, клиент или сервер в TCP-соединении, Контроль фрагментированных пакетов, предотвращение DoS-атак; Антиспуфинг
Настройка и управление	Удаленная/локальная настройка через специализированную консоль ViPNet; Удаленная настройка базовых параметров через ViPNet Administrator;
	Удаленный запрос журнала IP-пакетов (через Windows-продукты ViPNet Coordinator и Client).
Обновление ПО модуля	Централизованное удаленное обновление ПО ViPNet Terminal в модуле через ViPNet Administrator с контролем прохождения обновления

Преимущества ViPNet Terminal

ViPNet Terminal создан на аппаратной платформе, хорошо защищенной от механических повреждений (отсутствуют вентилятор и жесткий диск), обладает малыми размерами и весом, отличается низким потреблением электроэнергии (22 Вт) и устойчив к сбоям электропитания.

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-флэшки, если это не разрешено политиками информационной безопасности. ViPNet Terminal не производит хранение и обработку данных, а лишь осуществляет их отображение на экране монитора в терминальной сессии.

ViPNet Terminal поддерживает работу с сетевым и локально подключенным принтером, что позволяет пользователю распечатывать документы, если это не запрещено политиками информационной безопасности.

ViPNet Terminal, 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.

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

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

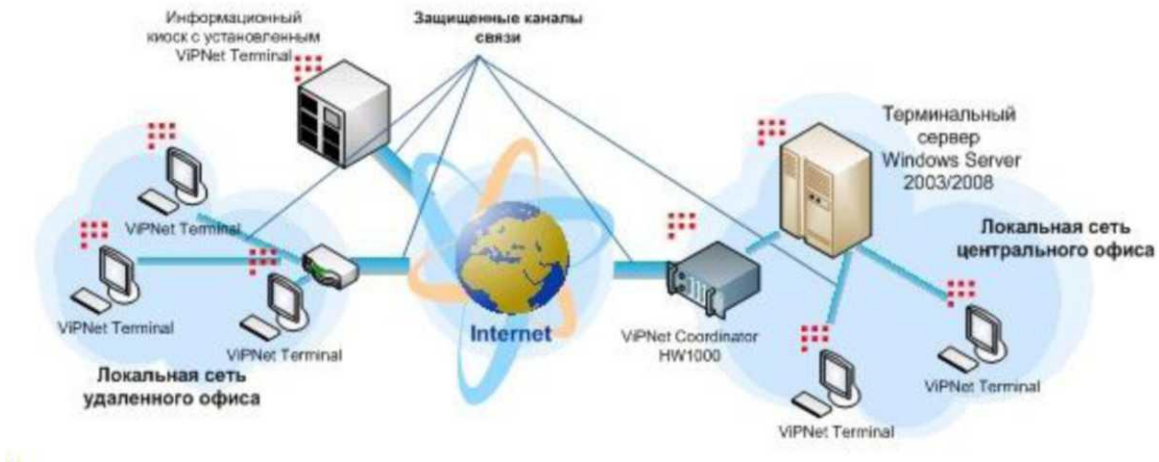
ViPNet Terminal поддерживает работу различных мультимедийных приложений, что позволяет использовать его в системах IP-телефонии и видеоконференцсвязи.

Сценарии применения

Для организации зашифрованных терминальных сессий ViPNet Terminal 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 защищенных точечных подключений к инфраструктуре компании без значительных капиталовложений;
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.



Сертификация

ФСБ РФ

«Программно-аппаратный комплекс ViPNet Terminal» соответствуют требованиям ФСБ России к устройствам типа межсетевые экраны по 4 классу защищенности и может использоваться для защиты информации от несанкционированного доступа в информационно-телекоммуникационных системах органов государственной власти Российской Федерации.

ПАК ViPNet Terminal соответствует требованиям ФСБ РФ, предъявляемым к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, по классам КС1, КС2 и КС3.

ФСТЭК РФ

Программный комплекс защиты информации "ViPNet Terminal 3.0"
является программным средством защиты информации от несанкционированного доступа

к информации и соответствует требованиям руководящих документов "Средства вычислительной техники. Межсетевые экраны. защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации (Гостехкомиссия России, 1997) - по 3 классу защищенности, "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей" (Гостехкомиссия России, 1999) - по 3 уровню контроля.

Гарантийное обслуживание

На ViPNet Terminal предоставляется гарантия 1 год.

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.