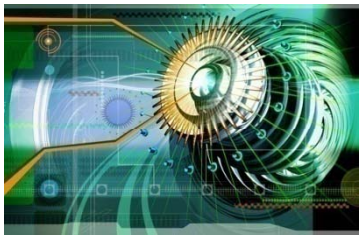

# Защита информации с помощью ViPNet KZ

Вячеслав Казанцев
ТОО «Ak Kamal Security»

Астана, 2012 г.

# Модернизация технологий приносит новые возможности и также новые риски!



- Взрывной рост объемов обрабатываемой информации
  - ✓ Данные в процессе движения / обработки
  - ✓ Данные на хранении
  - ✓ Данные во время доставки в конечную точку / перемещения в архив
- Новые технологии, новые опасности
  - ✓ Электронные сервисы / новыеуслуги / «Облака»
  - ✓ Business-to-Business взаимодействие
- Законодательство, требования Регуляторов и другие подзаконные акты дополнительно увеличивают нагрузку
  - ✓ Официальные Законы и другие подзаконные Акты
  - ✓ Сертификация по требованиям PCI-DSS (актуально для коммерческих банков)
  - ✓ Внутренние регламентирующие документы организаций

***Всеми из которых необходимо управлять …***

# Криптографическая защита

- Шифрование информации, передаваемой по информационно-телекоммуникационным сетям
  - ✓ абонентское шифрование;
  - ✓ канальное шифрование;
  - ✓ центр управления и мониторинга.
- Шифрование хранимой информации
- Использование электронной цифровой подписи

# Решение по защите информации

- Использование казахстанского решения ViPNet KZ, построенного на российских технологий защиты информации ViPNet компании ИнфоТеКС
- Сертификация СКЗИ «Домен-КС2», входящего в состав ViPNet KZ, на 3 уровень по СТ РК 1073-2007
- Производство и техническая поддержка программно-аппаратных комплексов в Казахстане
- Подтверждения соответствия каждого ПАК общим и специальным требованиям безопасности, а также требованиям СТ РК 1073-2007

Ak Kamal Security

infotecs®

# Продукты ViPNet как СКЗИ

**Базовые функции**
- Шифрование
- Имитозащита
- ЭЦП

**Объекты защиты**
- Файлы и области памяти
- IP-трафик

**Среда функционирования**
- В рамках ОС
- В рамках прикладного ПО

**Способ применения**
- в контролируемом сетевом окружении
- с подключением к сетям общего пользования (Интернет)

**Уровень требований**
- КС1/КС2/КС3
- КВ1/КВ2

ViPNet®
Virtual Private Network

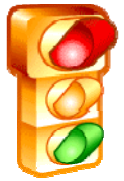
VPN

PKI

# Технология ViPNet: шифрование IP-трафика

- ✓ Шифрование IP-пакета с полной инкапсуляцией в UDP-пакеты: аналог режима ESP+AH+NAT-T в IPSec
- ✓ Прозрачность для приложений пользователя и системных служб
- ✓ Высокая скорость шифрования на алгоритмах ГОСТ(256 бит) – до 320 Мбит/с на Intel Xeon
- ✓ Одновременная работа с открытым и шифруемым трафиком
- ✓ Трансляция адресов для зашифрованного трафика
- ✓ Абонентское шифрование и работа в качестве криптошлюза

# Технология ViPNet: фильтрация IP-трафика



- ✓ Функционирование на сетевом уровне стека TCP/IP
- ✓ Фильтрация по всем полям IP-заголовка и по расписанию
- ✓ Раздельные фильтры для открытых и зашифрованных пакетов
- ✓ Режим инициативных соединений (режим «бумеранг»)
- ✓ Антиспуфинг и встроенная IPS для блокировки опасных атак
- ✓ Запуск фильтрации трафика до старта прикладных систем
- ✓ Отдельный список правил фильтрации для каждого сетевого интерфейса
- ✓ Фильтрация по паре адресов (обработка транзитного трафика)
- ✓ Трансляция адресов для открытых пакетов (NAT)

# Технология ViPNet: виртуализация IP-адресов

Любой сетевой узел, включенный в VPN может «видеть» другие сетевые узлы VPN под реальными или виртуальными IP-адресами

Виртуальный адрес привязывается к уникальному идентификатору узла, используется исключительно для сети ViPNet, позволяет всем компьютерам виртуально работать в одной *локальной сети, даже если физически компьютеры расположены на разных континентах.*

**Преимущества:**

- ✓ Возможность развертывания VPN в сетях с пересекающейся IP-адресацией
- ✓ Неограниченное число виртуальных адресов
- ✓ Независимость от способа подключения к сети; из дома, по Wi-Fi, по 3G, из корпоративной сети – Вы всегда обращаетесь к защищенному ресурсу по единому виртуальному адресу

# Технология ViPNet: управление и мониторинг

- ✓ Раздельное управление структурой VPN и ключевой системой
- ✓ Централизованное:
  - управление структурой сети / управление ключевой системой
  - управление сетевыми настройками узлов VPN
  - управление полномочиями пользователей
  - обновление ПО, управление лицензиями
  - выполнение процедур компрометации и смены ключей
  - мониторинг состояния узлов VPN, журналирование
- ✓ Взаимодействие с другими VPN-сетями на базе продуктов ViPNet

# Технология ViPNet: масштабируемость

- ✓ Реальная «емкость» одной защищенной сети до 16 000 узлов
- ✓ Один VPN-сервер может эффективно поддерживать до 1000 абонентских пунктов
- ✓ Технология межсетевого взаимодействия
- ✓ Отсутствие точек сосредоточения трафика

**ViPNet – дает возможность наращивать VPN без ущерба функционированию уже работающих узлов сети**

**ViPNet – работает в ИС реального времени критичных к времени простоя**

# Продуктовая линейка ViPNet KZ

## Компоненты администрирования

Программные и программно-аппаратные комплексы для управления и мониторинга защищенной сети

## Серверные компоненты

Программно-аппаратные комплексы (ПАК) - межсетевые экраны и криптошлюзы

## Клиентские компоненты

Программное обеспечение для установки на рабочие станции, ноутбуки, мобильные устройства, терминалы

# Компоненты администрирования ViPNet KZ

- ViPNet Центр Управления (Administrator) - базовый программный либо программно-аппаратный комплекс для настройки и управления сетью
- ViPNet Пункт Регистрации - программный либо программно-аппаратный комплекс для регистрации пользователей
- ViPNet Publication Service - сервис публикации сертификатов ЭЦП
- ViPNet StateWatcher - система централизованного мониторинга

# Серверные компоненты ViPNet KZ

- ViPNet Координатор KZ-1000 – сервер защищенной сети

- ViPNet Координатор KZ-100 – сервер защищенной сети для небольших компаний или удаленных офисов

**В разработке:**

- Специализированные криптошлюзы защищенной сети для банкоматов, платежных терминалов, одиночных сетевых узлов

# Клиентские компоненты ViPNet KZ

- ViPNet Клиент – программный VPN-клиент, персональный экран, клиент защищенной почтовой системы

- ViPNet Клиент iOS/Android - приложение для Apple iOS и Android OS, функция защиты мобильных устройств от сетевых атак и VPN-клиент

- ПАК ViPNet Терминал – терминальный «тонкий» Клиент для организации полноценного защищенного рабочего места пользователя

# ViPNet Центр Управления (Administrator)

## Центр управления сетью (ЦУС)

- Формирование и управление структурой защищенной сети (определение объектов, назначение связей)
- Межсетевое взаимодействие
- Управление полномочиями пользователей
- Рассылка обновлений (настройки, ключи шифрования и ЭЦП, ПО ViPNet)
- Управление лицензиями

## Удостоверяющий и ключевой центр (УКЦ)

- Выработка ключей шифрования и защиты, паролей пользователей и администраторов
- Управление жизненным циклом ключей шифрования
- Выработка, сертификация, отзыв ключей ЭЦП
- Кроссертификация со сторонними УЦ
- Журналирование операций, ведение базы сертификатов ЭЦП, списков отозванных сертификатов
- Работа с электронными ключами (токенами)

ГОСТ 28147-89 ГОСТ Р 34.10-2001

# ViPNet Центр Управления (Administrator)

- Варианты поставки :
  - ✓ ПО или ПАК (сервер или моноблок с полностью предустановленным ПО)
  - ✓ комплектуется USB-токенами для хранения ключей (раздельное хранение ключей доступа к управлению сетью и к управлению ключевой информацией)
- Возможность подбора аппаратной платформы с учетом специфики защищаемой сети
- Защита комплекса ViPNet Клиентом

# ViPNet Пункт Регистрации (Registration Point)

- ✓ Регистрация пользователей ViPNet и внешних пользователей (держателей ЭЦП)
- ✓ Формирование и отправка в УКЦ запроса на подключение к сети ViPNet, прием ключей, запись на токен
- ✓ Формирование и отправка в УКЦ запроса на сертификат, прием и ввод в действие, запись на токен
- ✓ Ведение справочника запросов и изданных сертификатов
- ✓ Управление связями узлов
- ✓ Формирование запросов на отзыв, приостановление и возобновление сертификатов
- ✓ Журналирование событий, списков изданных сертификатов и действий Уполномоченного лица
- ✓ Интеграция с LDAP Active Directory

# ViPNet Пункт Регистрации (Registration Point)

- Варианты поставки :
  - ✓ ПО или ПАК (сервер или моноблок с полностью предустановленным ПО)
  - ✓ комплектуется USB-токеном для хранения ключевой информации
- Возможность подбора аппаратной платформы с учетом специфики защищаемой сети
- Защита комплекса ViPNet Клиентом

# ViPNet Publication Service

- ✓ Публикация списков отозванных сертификатов
- ✓ Публикация списков изданных сертификатов пользователей и Уполномоченных лиц
- ✓ Интеграция с внешними УЦ и хранилищами через LDAP и FTP
- ✓ Формирование отчетов о публикации сертификатов Уполномоченных лиц для УЦ с целью включения этой информации в сертификаты пользователей
- ✓ Работает совместно с ViPNet Administrator : УКЦ

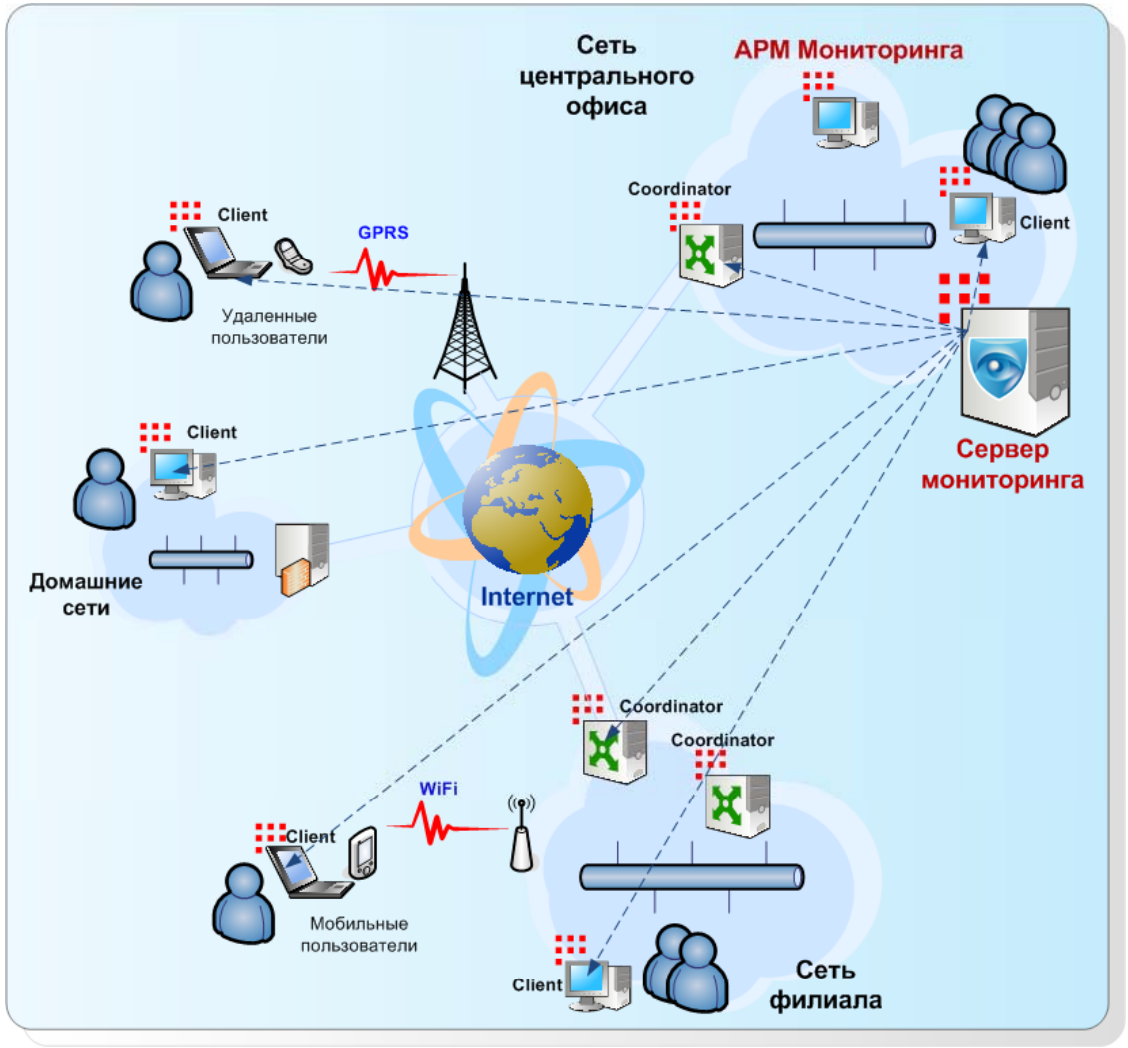
# ViPNet StateWatcher

NEW

- ✓ Мониторинг  локальных и распределенных сетей ViPNet
- ✓ Определение текущего состояния ViPNet-узлов
- ✓ Определение текущего состояния компонентов ViPNet на узлах
- ✓ Слежение как за состоянием отдельных узлов, так и выбранных групп узлов
- ✓ Определение сбоев и других критических событий в работе ViPNet-узлов и отдельных компонентах ПО ViPNet
- ✓ Оперативное уведомление о событиях системы мониторинга
- ✓ Накопление и анализ информации мониторинга

# ViPNet StateWatcher

NEW

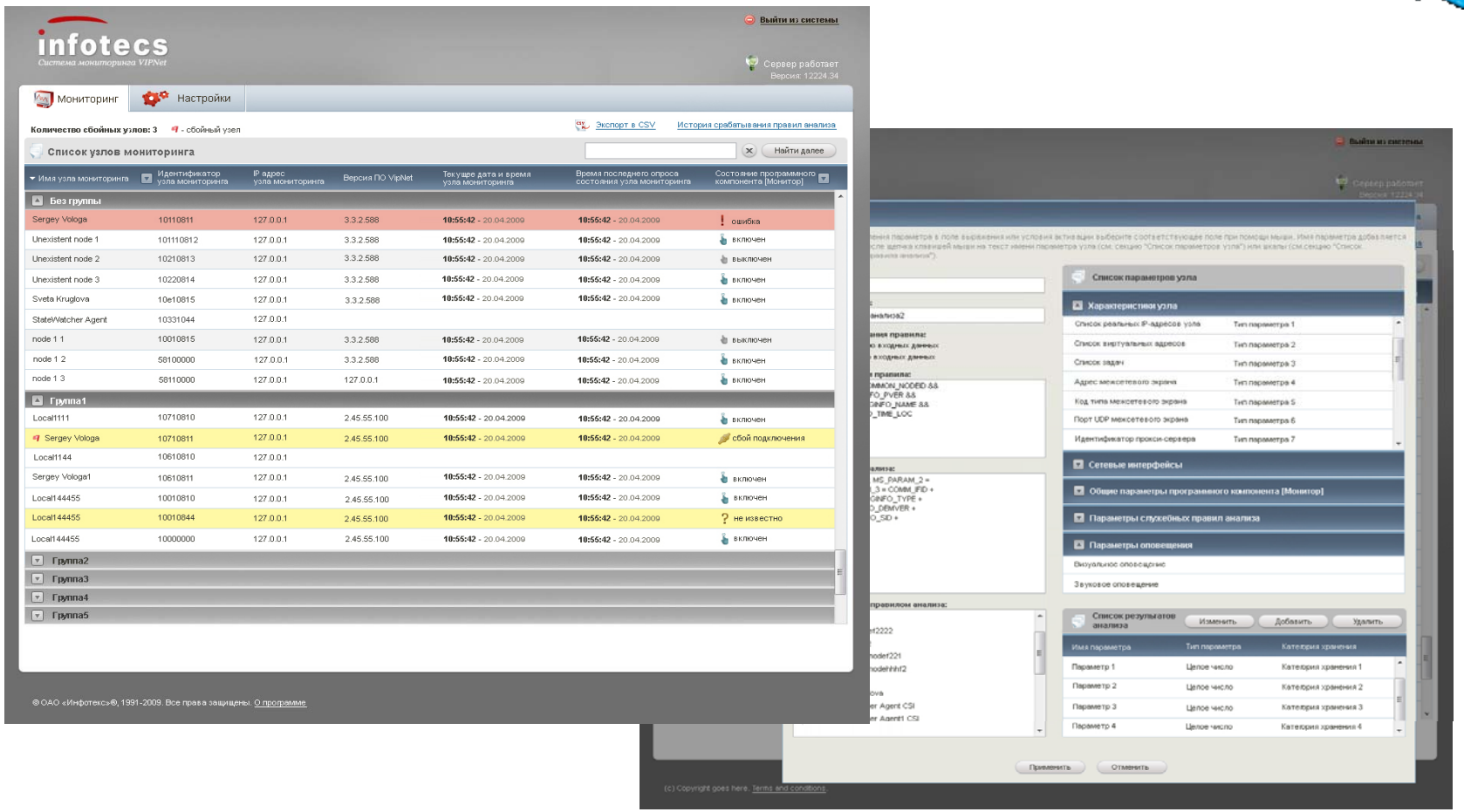



- ✓ Мониторинг состояния узлов локальной сети, удаленных узлов, мобильных узлов и домашних пользователей, независимо от способа подключения

# ViPNet StateWatcher

NEW

## Удобный WEB-доступ к консоли сервера мониторинга



# ViPNet StateWatcher

NEW

- Варианты поставки :
  - ✓ ПО или ПАК (сервер с полностью предустановленным ПО)
  - ✓ комплектуется USB-токеном для хранения ключевой информации
- Возможность подбора аппаратной платформы с учетом специфики защищаемой сети
- Защита комплекса ViPNet Клиентом

# ViPNet Координаторы KZ: функциональность

Межсетевой экран | Криптошлюз | VPN-сервер | Защищенный почтовый сервер

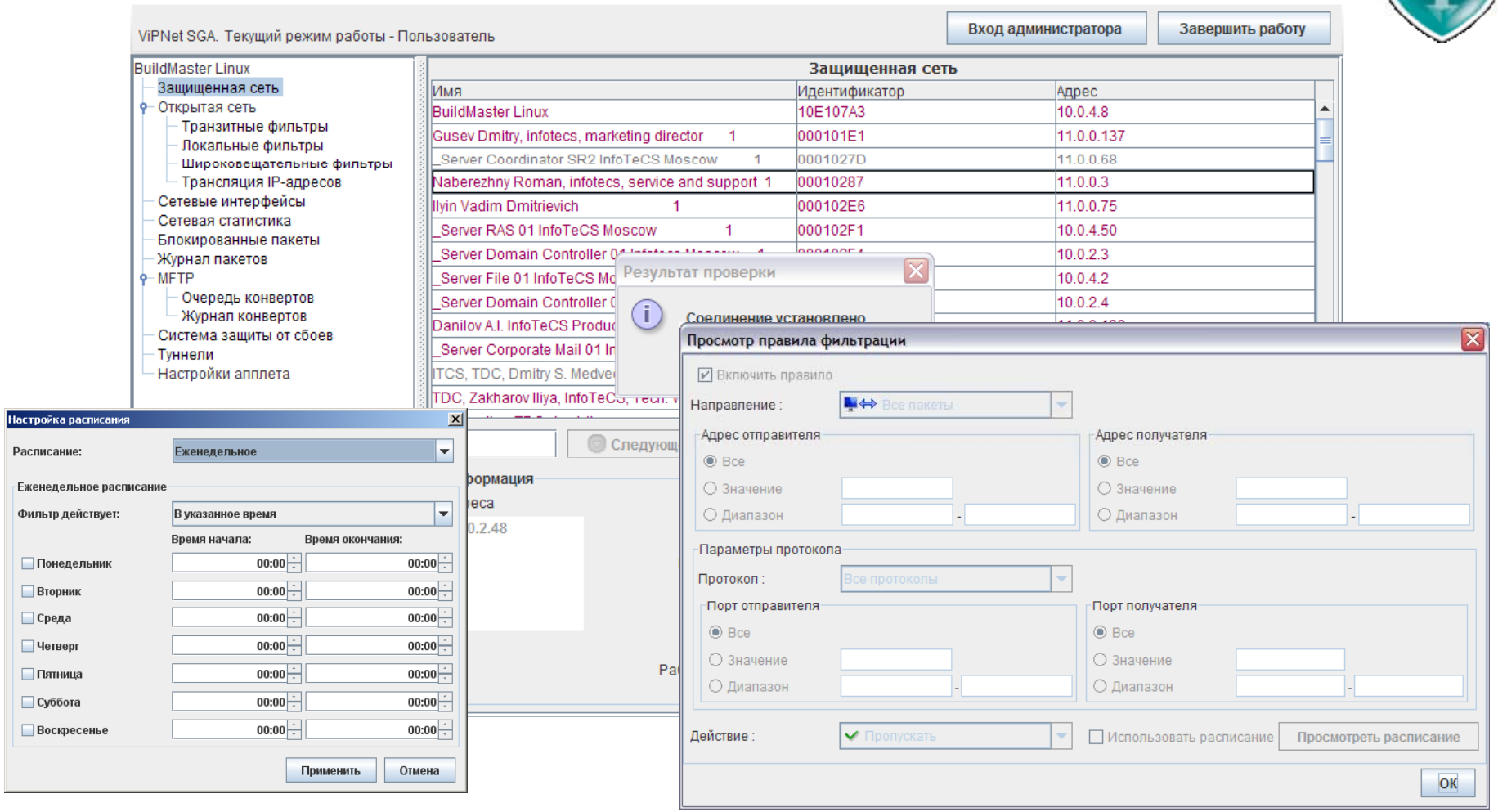
- ✓ Шифрование IP-трафика (алгоритм ГОСТ 28147-89)
- ✓ Фильтрация IP-трафика, защита от сетевых атак, антиспуфинг
- ✓ Работа в качестве криптошлюза для удаленных и мобильных пользователей
- ✓ Функции сервера-маршрутизатора для защищенных сетей ViPNet
- ✓ Функции транспортного (почтового) сервера*
- ✓ Совместимость с сетевым оборудованием преобразования адресов (NAT и PAT), реализация NAT для открытого трафика
- ✓ Сетевые сервисы для локальной сети (DHCP, DNS, NTP)
- ✓ Горячее резервирование*
- ✓ Поддержка многоядерных систем

** - не для всех моделей*

# ViPNet Координатор KZ: особенности

- ✓ ПАКи ViPNet Координатор KZ поставляются готовыми к работе, необходимо только выполнить процедуру развертывания ключей из стандартного DST-файла
- ✓ Развертывание ключей возможно по протоколу TFTP или с USB-flash
- ✓ Локальное и удаленное управление через консоль, SSH и WEB-интерфейс
- ✓ Возможность ведения системного журнала на удаленном компьютере
- ✓ В качестве ОС используется собственный дистрибутив Linux, оптимизированный под целевые функции ПАК и аппаратную платформу
- ✓ Доступ в ОС ограничен, все операции осуществляются через собственный командный интерпретатор ViPNetKZ Shell
- ✓ Контроль версии СКЗИ осуществляется при производстве, сертификации, работе
- ✓ Восстановление заводской прошивки ПАК с USB-flash

# ViPNet Координатор KZ : WEB-интерфейс



# Модели ПАК ViPNet Координатор KZ

## ViPNet Координатор KZ-1000

- ✓ Высокопроизводительная серверная платформа SuperMicro
- ✓ 4-х ядерный 3,4 GHz Intel Xeon процессор
- ✓ 4 GB DDR-3 оперативной памяти
- ✓ 4 гигабитных сетевых интерфейса

## ViPNet Координатор KZ-100

- ✓ Компактный мини-компьютер с низким уровнем тепловыделения и энергопотребления
- ✓ Процессор Intel Atom 1,6 GHz
- ✓ 1 GB DDR-2 оперативной памяти
- ✓ 4 гигабитных сетевых интерфейса

# ViPNet Координатор KZ-1000

**Универсальный криптошлюз и межсетевой экран для защиты трафика в любых сценариях защиты информации**

## Особенности

- ✓ Промышленный сервер для установки в стандартную стойку
- ✓ Поддержка режима failover (горячее резервирование)
- ✓ Высокая надежность в режиме 24/7/365
- ✓ Производительность по шифрованию – до 320 Мбит/с (TCP)

## Области применения

- ✓ Шифрование каналов связи между локальными сетями
- ✓ Защита локальных сетей от сетевых атак, фильтрация трафика, NAT
- ✓ Организация защищенного удаленного доступа к корпоративным ресурсам (серверам, порталам, базам данных, IP-телефонии и т.п.)
- ✓ Защита мультисервисных сетей связи (поддержка прозрачного шифрования приоритезированного трафика)

# ViPNet Координатор KZ-1000

- **Варианты поставки** – один, максимальный. Нет ограничений на число туннелируемых адресов и защищенных соединений

- **Сертификация** – сертифицирован по 3-му уровню безопасности в соответствии с СТ РК 1073-2007

- **Техническая поддержка:**
  - ✓ в стоимость включена годовая поддержка
  - ✓ возможность приобретения расширенной тех.поддержки
  - ✓ гарантийные обязательства по аппаратной части ПАК обеспечиваются сервисным центром компании ТОО «Ak Kamal Security»

# ViPNet Координатор KZ-100

**Компактный криптошлюз и межсетевой экран для защиты трафика удаленных сетевых устройств или небольших локальных сетей**

- **Особенности**
  - ✓ Малые размеры и вес, высокая механическая прочность
  - ✓ Безвентиляторное исполнение
  - ✓ Возможность бездискового варианта исполнения
  - ✓ 4 сетевых интерфейса Ethernet 10/100/1000
  - ✓ Производительность по шифрованию – до 20 Мбит/с (TCP)
- **Области применения**
  - ✓ Включение в единую VPN разветвленной сети небольших офисов компании
  - ✓ Защита IP-трафика и оборудования промышленных систем управления и сбора данных
  - ✓ Защита банкоматов и различных платежных устройств

# ViPNet Координатор KZ-100

- **Ограничения**
  - ✓ Не поддерживается режим failover (горячее резервирование)
  - ✓ До 10  одновременно туннелируемых устройств

- **Сертификация** – сертифицирован по 3-му уровню безопасности в соответствии с СТ РК 1073-2007

- **Техническая поддержка:**
  - ✓ в стоимость включена годовая поддержка
  - ✓ возможность приобретения расширенной тех.поддержки
  - ✓ гарантийные обязательства по аппаратной части ПАК обеспечиваются сервисным центром компании ТОО «Ak Kamal Security»

# ViPNet Client KZ: возможности

- ✓ VPN-клиент для работы в сети ViPNet
  - шифрование трафика любых приложений
  - поддержание актуальных параметров доступа к узлам VPN
  - работа в схемах:
    - клиент - клиент
    - клиент - сервер
    - клиент - туннелируемый ресурс
  - поддержка виртуальных IP-адресов
- ✓ Персональный сетевой экран (раздельная фильтрация открытого и шифрованного трафика)
- ✓ Мониторинг сетевой активности приложений и компонентов ОС
- ✓ Клиент защищенной почтовой службы ViPNet Деловая Почта
- ✓ Защищенные службы ViPNet: чат, конференция, обмен файлами
- ✓ Криптопровайдер для ОС Windows и прикладного ПО
- ✓ Работа с любыми типами подключений – Ethernet/GPRS/3G/xDLS/Wi-Fi/Wi-Max/Dial-Up
- ✓ Комплектуется USB-токеном для хранения ключевой информации

# ViPNet Клиент KZ: работа ViPNet-драйвера

ViPNet-драйвер перехватывает и контролирует весь трафик, поступающий и исходящий из всех реальных и виртуальных сетевых адаптерах компьютера.

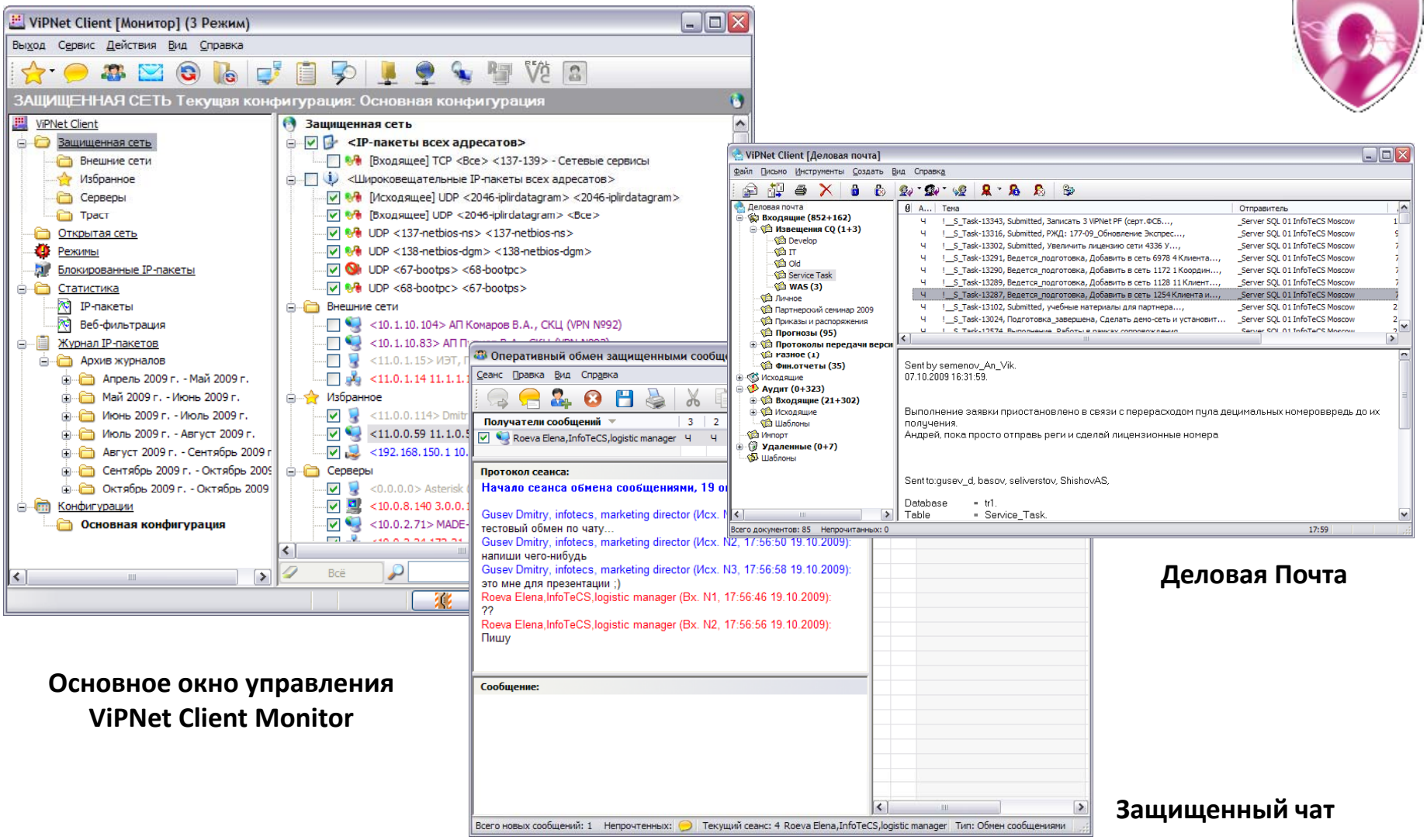
***Режимы безопасности:***

- ✓ Первый– блокирует весь открытый (незашифрованный) трафик (работа только внутри сети ViPNet)
- ✓ Второй– разрешает работу с открытым трафиком согласно фильтрам Открытой Сети
- ✓ Третий– режим инициативных соединений (бумеранг) открытого трафика, «Что не запрещено, то разрешено».
- ✓ Четвертый– выключает работу сетевого экрана ViPNet, но оставляет работать систему шифрования
- ✓ Пятый–отключение драйвера защиты

# ViPNet Клиент KZ: Деловая Почта

- ✓ Отправка и получение писем с прикрепленными к ним вложениями
- ✓ Отправка файлов (в виде вложений) из Windows Explorer адресатам ViPNet
- ✓ Получение подтверждений (квитанций) о доставке и прочтении
- ✓ Шифрование писем и вложений к ним
- ✓ Электронная подпись писем и вложений к ним
- ✓ Ведение регистрационной нумерации документов, архивов
- ✓ Сортировка и автоматическая обработка корреспонденции, в соответствии с различными правилами, задаваемыми пользователем (автопроцессинг)

# ViPNet Клиент KZ: интерфейс




**Основное окно управления ViPNet Client Monitor**

**Деловая Почта**

**Защищенный чат**

# ViPNet Клиент iOS

ViPNet Клиент iOS - приложение, работающее под управлением ОС Apple iOS, предназначенное для обеспечения защиты iPad и iPhone от сетевых атак и позволяющее осуществить доступ посредством защищенного технологиями ViPNet VPN туннеля, к ресурсам корпоративной сети


- Аутентификация пользователя (по паролю)
- Функции персонального сетевого экрана
- Шифрование сетевого трафика iPad и iPhone

Поддерживаются сетевые соединения через GPRS, EDGE, 3G и WiFi.

# ViPNet Клиент Android

ViPNet Клиент Android –программный комплекс, предназначенный для эксплуатации на устройствах поддерживающих ОС Android и реализующий функции VPN-клиента для защищенных сетей ViPNet и функции персонального сетевого экрана


- Аутентификация пользователя (по паролю)
- Функции персонального сетевого экрана
- Шифрование сетевого трафика мобильного устройства

Поддерживаются сетевые соединения через GPRS, EDGE, 3G, 4G и WiFi.

# ViPNet Terminal – защищенный «тонкий» клиент

NEW

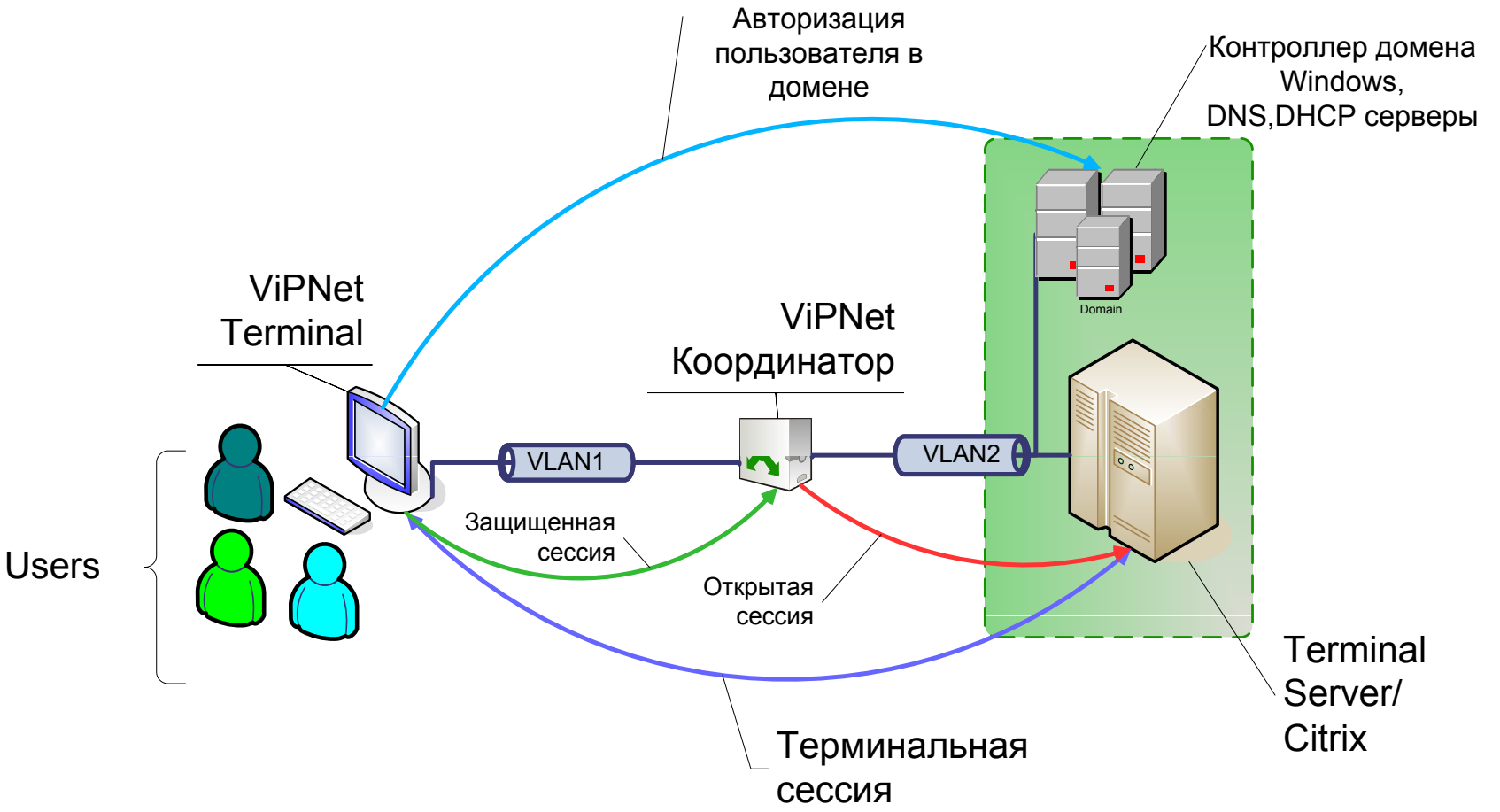
ViPNet Terminal
Защищенное терминальное решение

- ✓ Полный контроль над системным окружением пользователя и обрабатываемой информацией
- ✓ Решение проблемы внутреннего нарушителя
- ✓ Надежная защита канала связи и терминального сервера
- ✓ Поддержка протоколов RDP, ICA, HTTP/HTTPS
- ✓ Эксплуатационный цикл не зависит от системных требований прикладного ПО
- ✓ Интеграция в доменную инфраструктуру Windows

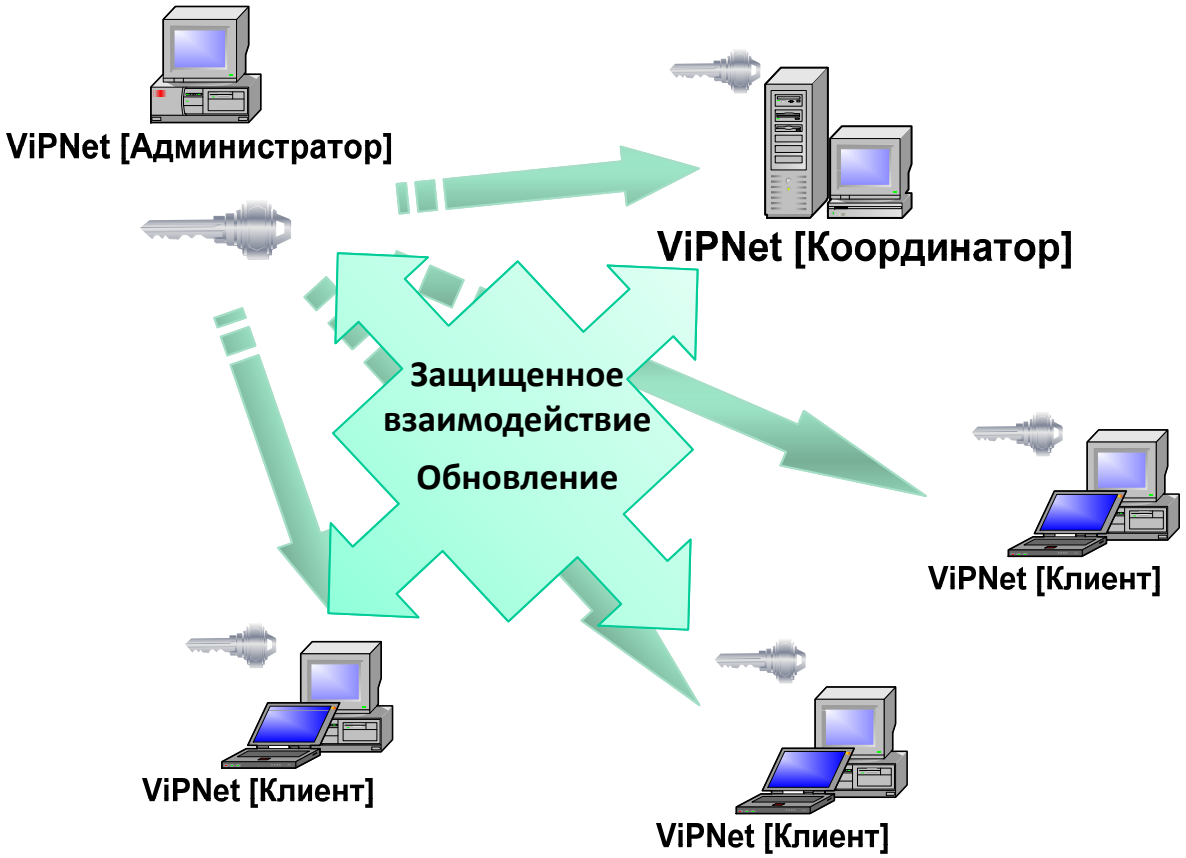
# ViPNet Terminal – защищенный «тонкий» клиент

NEW

ViPNet Terminal
Защищенное терминальное решение



# Как строится и работает VPN в технологии ViPNet




1. Формирование связей и ключей шифрования. Распределение ключей по серверам и рабочим местам.

2. Работа в рамках созданной VPN: связи Клиент-Клиент, Клиент-Координатор, Координатор-Координатор

3. Модификация структуры VPN (добавление новых пользователей, изменение связей и т.д.). Обновление ПО ViPNet.

# ViPNet и другие решения VPN

**ViPNet** vs **IPSEC**, **OpenVPN**, **L2TP**, **PPTP**

Сравнение проведем по следующим основным направлениям:

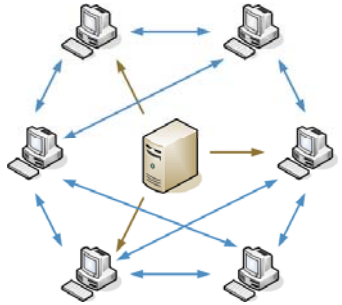
- Обеспечиваемый уровень безопасности
- Возможные сценарии использования
- Эксплуатационные характеристики

# Ключевая структура

**Основное отличие ViPNet от других VPN-решений – использование симметричной ключевой структуры**

- В правительственных и военных системах используют лишь симметричные алгоритмы, т. к. нет строгого математического обоснования стойкости систем с открытыми ключами
- Ассиметричные системы требуют периодических сеансов аутентификации и процедур выработки ключей, что может негативно сказаться при работе большой сети
- ViPNet имеет систему управления симметричной ключевой структурой, что делает ее использование удобным и незаметным для пользователя
- В PKI, если закончился срок действия сертификата, секретного ключа, COC - связь прерывается. Если это происходит на шлюзе – остановится работа всей VPN-сети

# Peer to Peer архитектура



- ViPNet ориентирован на Peer to Peer схемы, основанные на авторегистрации информации, нужной для автоматического установления защищенных соединений с другими узлами VPN по текущему актуальному адресу
- Peer to Peer позволяет использовать ViPNet в таких случаях, где пасуют другие технологии VPN
- Отсутствует необходимость в проведении каких-либо настроек на своем узле для других узлов для соединения с ними
- Неограниченные возможности по каскадированию через цепочки Координаторов. Координаторы выполняют роль транзитных NAT-устройств и образуют сквозные каналы между любыми участками сетей

# Криптографическая фильтрация трафика

- IPSec предусматривает фильтрацию VPN-трафика, только на некотором внешнем Firewall, где информация об отправителе, кроме IP-адреса, потеряна
- ViPNet производит криптографическую фильтрацию трафика до того, как пакет потеряет связь с источником информации. IP-адрес пакета не имеет значения (важен только ID-пользователя)
- Для любого узла ViPNet можно задать любые правила для разграничения доступа к ресурсам внутри VPN-сети
- Использование виртуальных адресов ViPNet, дает возможность связки сетевого уровня безопасности с уровнем приложений для ИС где в качестве критерия разграничения помимо логина и пароля используется IP-адрес пользователя

# Работа с открытыми ресурсами Интернет

- В OpenVPN, L2TP, PPTP, IPSEC работа с VPN происходит через виртуальные адаптеры. Работа с открытыми ресурсами Интернет происходит путем направления всего трафика через VPN-туннель на VPN-шлюз и Firewall офиса. Возможно локально изменить маршрутную таблицу в ОС и отправить трафик Интернет через местного провайдера либо вообще отменить шифрование трафика, предназначенного для туннеля

- ViPNet также имеет такой сценарий работы с Интернет, но при этом не создается никаких виртуальных адаптеров и маршрутов в ОС. ViPNet-драйвер обеспечивает шифрование трафика в соответствии с заданными адресами, блокирует любой трафик с местным провайдером, исключает влияние ОС на работу в режиме VPN

# Поддержка приоритетов обработки трафика

1. Какое влияние оказывает ViPNet на обработку таких пакетов различным оборудованием при их прохождении по сети?
2. Поддерживает ли ViPNet обработку приоритетов при прохождении пакетов через Координаторы?

Драйвер ViPNet без каких-либо модификаций переносит из заголовка исходного IP-пакета в заголовок ViPNet-пакета поле Type of Service (TOS), в котором и задается приоритет обработки

**Ответ на 1-й вопрос** - ViPNet не оказывает влияние на работу другого оборудования при обработке заголовков TOS

**Ответ на 2-й вопрос** – сам ViPNet не поддерживает, но если включена служба QoS, расположенная по архитектуре выше драйвера ViPNet, то пакеты проходя через эту службу, могут подвергаться регулировке очередности их прохождения

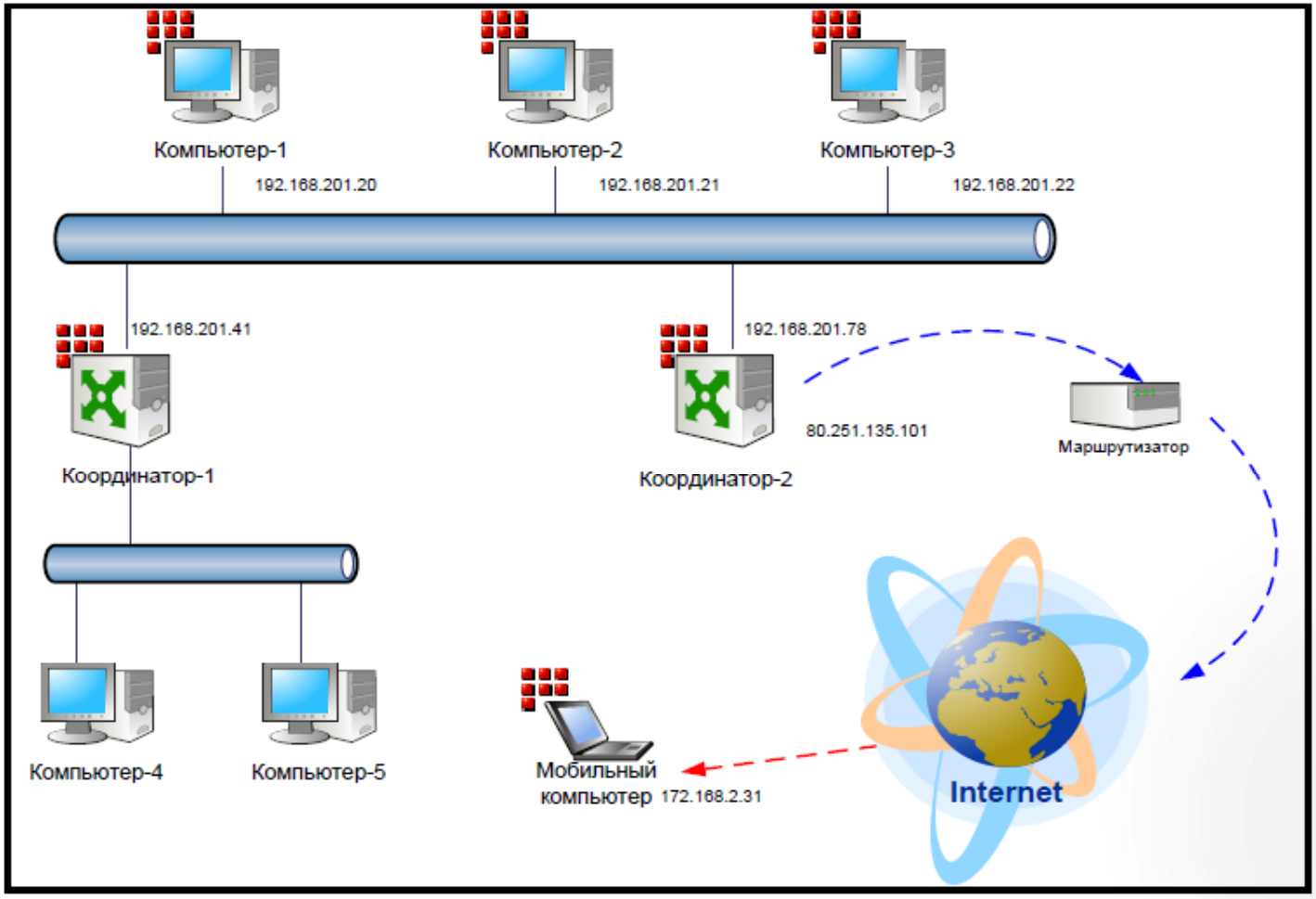
# Работа Координаторов/Клиентов с Интернет

**Различные режимы работы Координатора/Клиента с публичными сетями (Интернет):**

- ✓ Прямой доступ в Интернет
- ✓ Работа через другой ViPNet Координатор
- ✓ Работа через межсетевой экран, внешний IP-адрес которого известен и не меняется в процессе работы («Со статической трансляцией адресов»)
- ✓ Работа через межсетевой экран, внешний IP-адрес и порт доступа которого заранее неизвестны и (или) могут меняться в процессе работы («С динамической трансляцией адресов»)

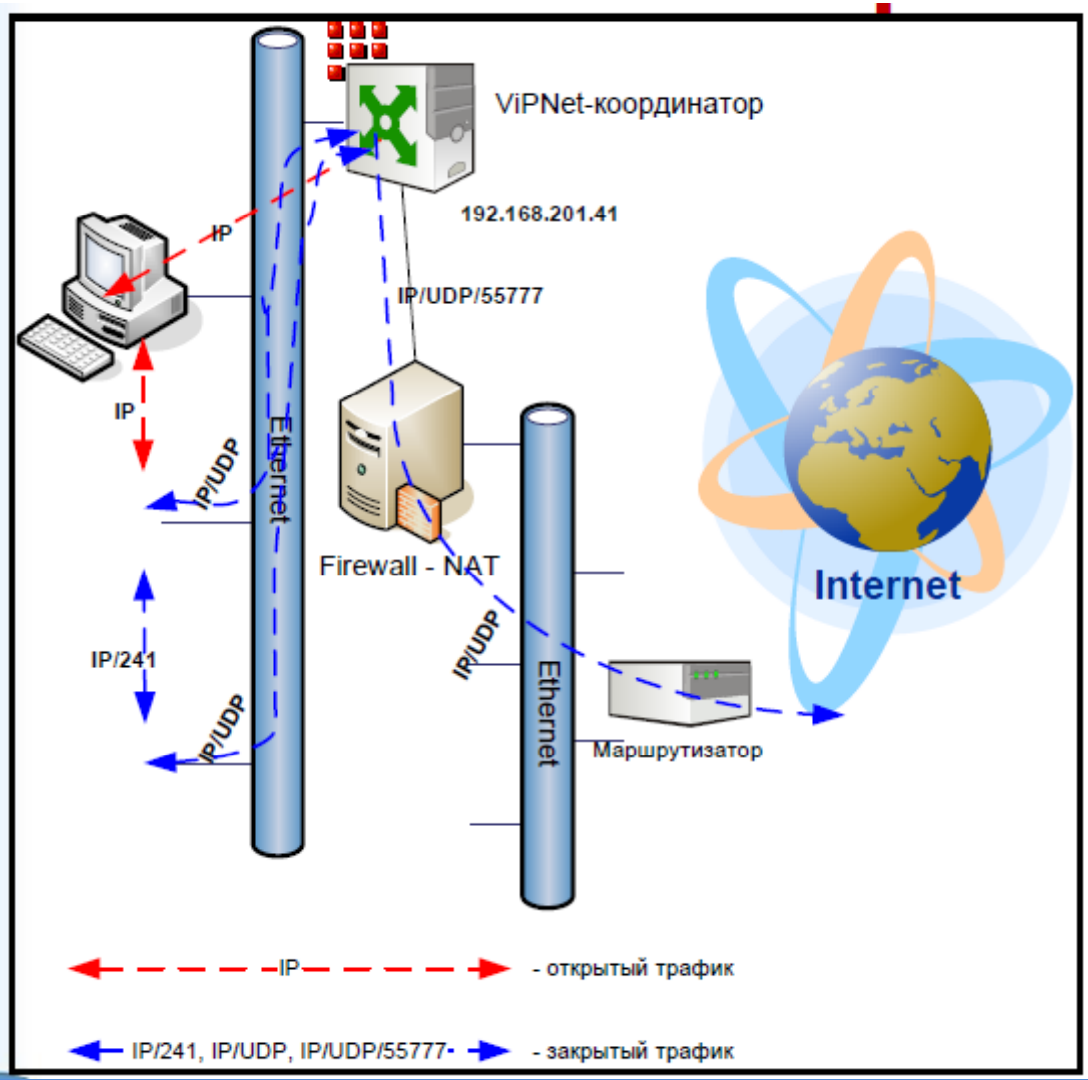
# Работа Координаторов /Клиентов с Интернет

✓ Работа через другой ViPNet Координатор



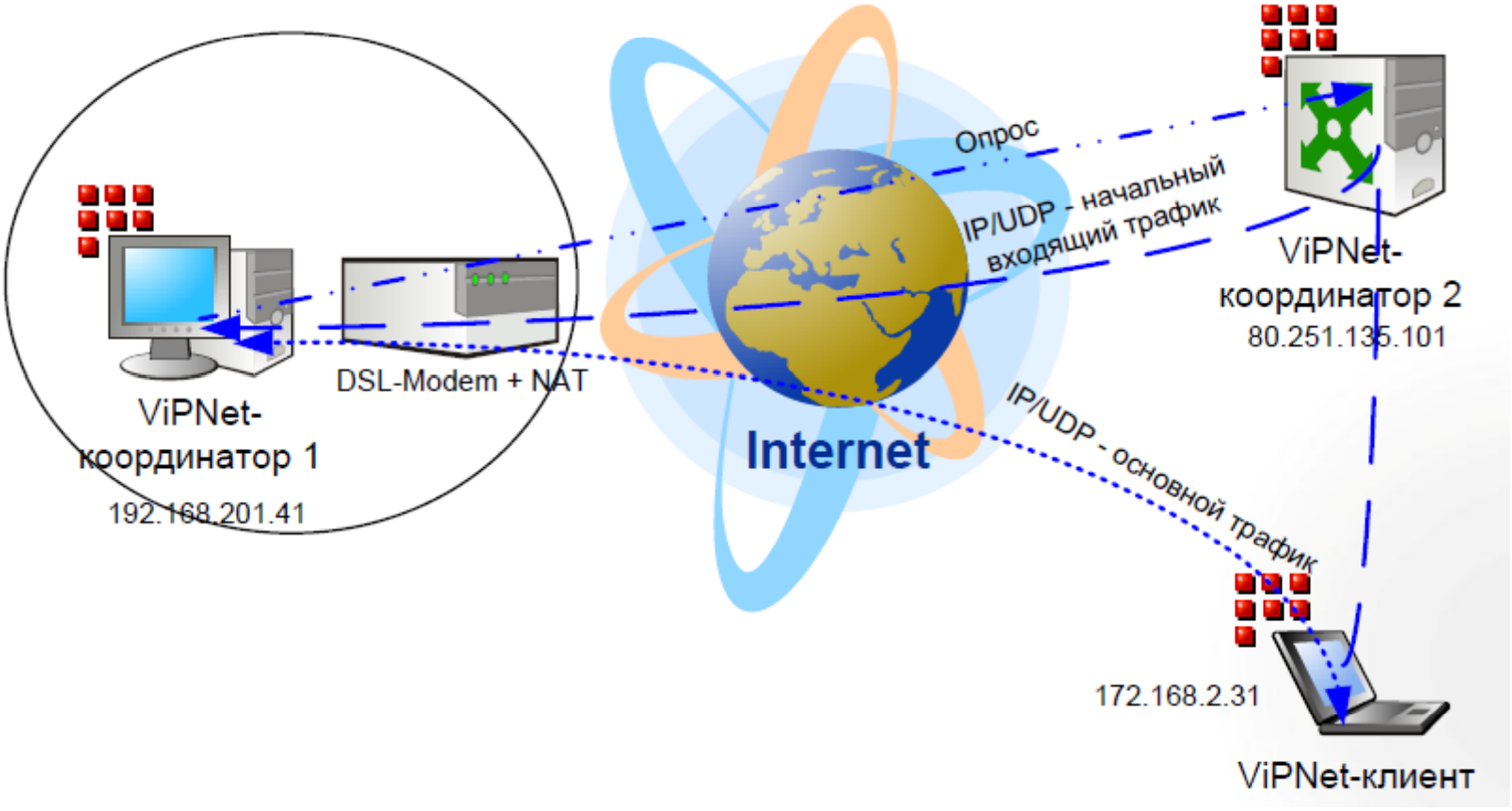
# Работа Координаторов /Клиентов с Интернет

- ✓ Работа через межсетевой экран со статической трансляцией адресов



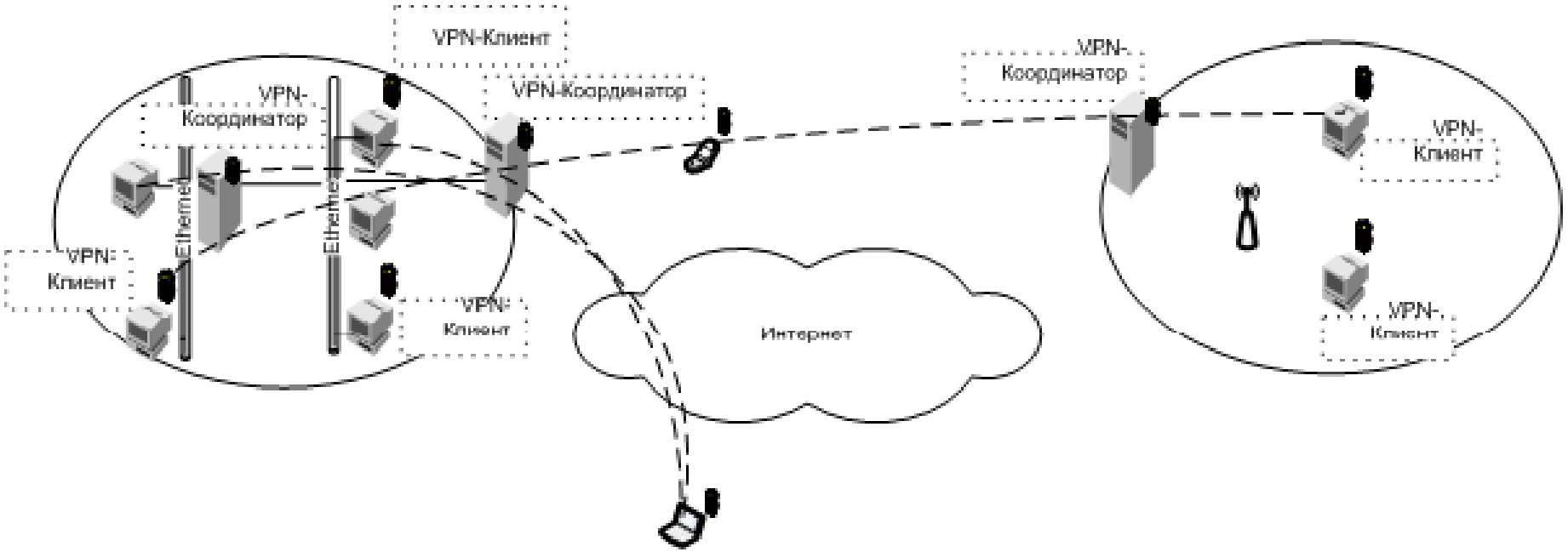
# Работа Координаторов /Клиентов с Интернет

- ✓ Работа через межсетевой экран с динамической трансляцией адресов



# Маршрутизация VPN-пакетов

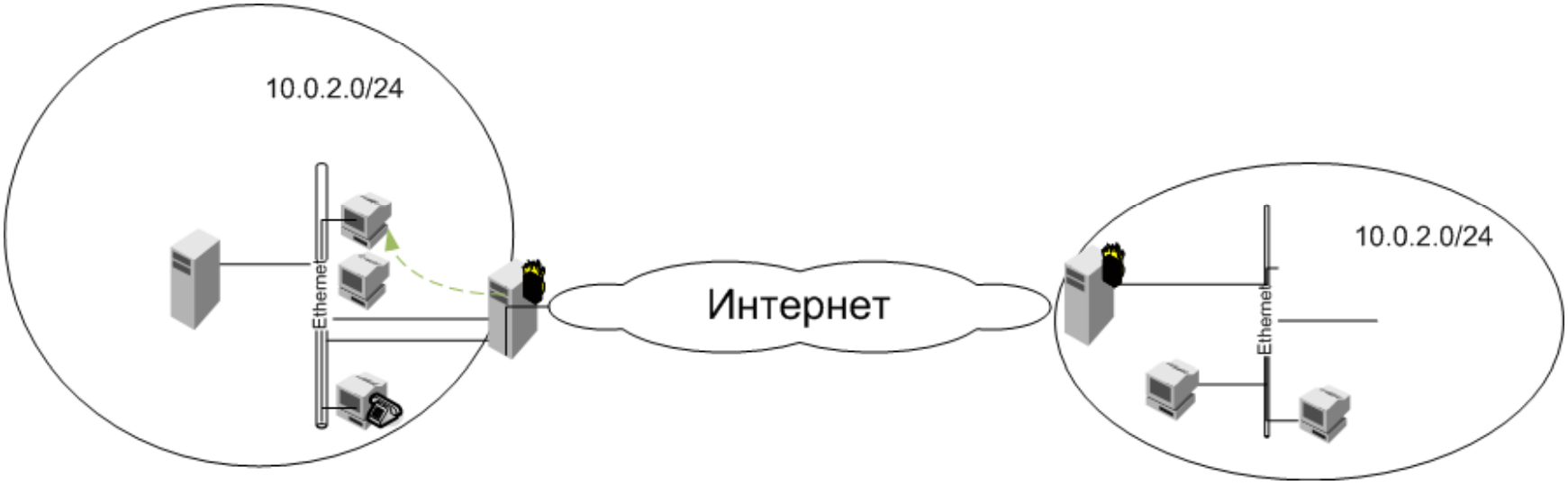
- **Удаленный конфиденциальный доступ к ресурсам или узлам, находящимся в локальной сети. Локальная сеть защищена ViPNet Координатором.**




ViPNet Координатор умеет маршрутизировать VPN-пакеты. Ни один другой VPN-шлюз делать этого не умеет, а соответственно, не может реализовать такую схему.

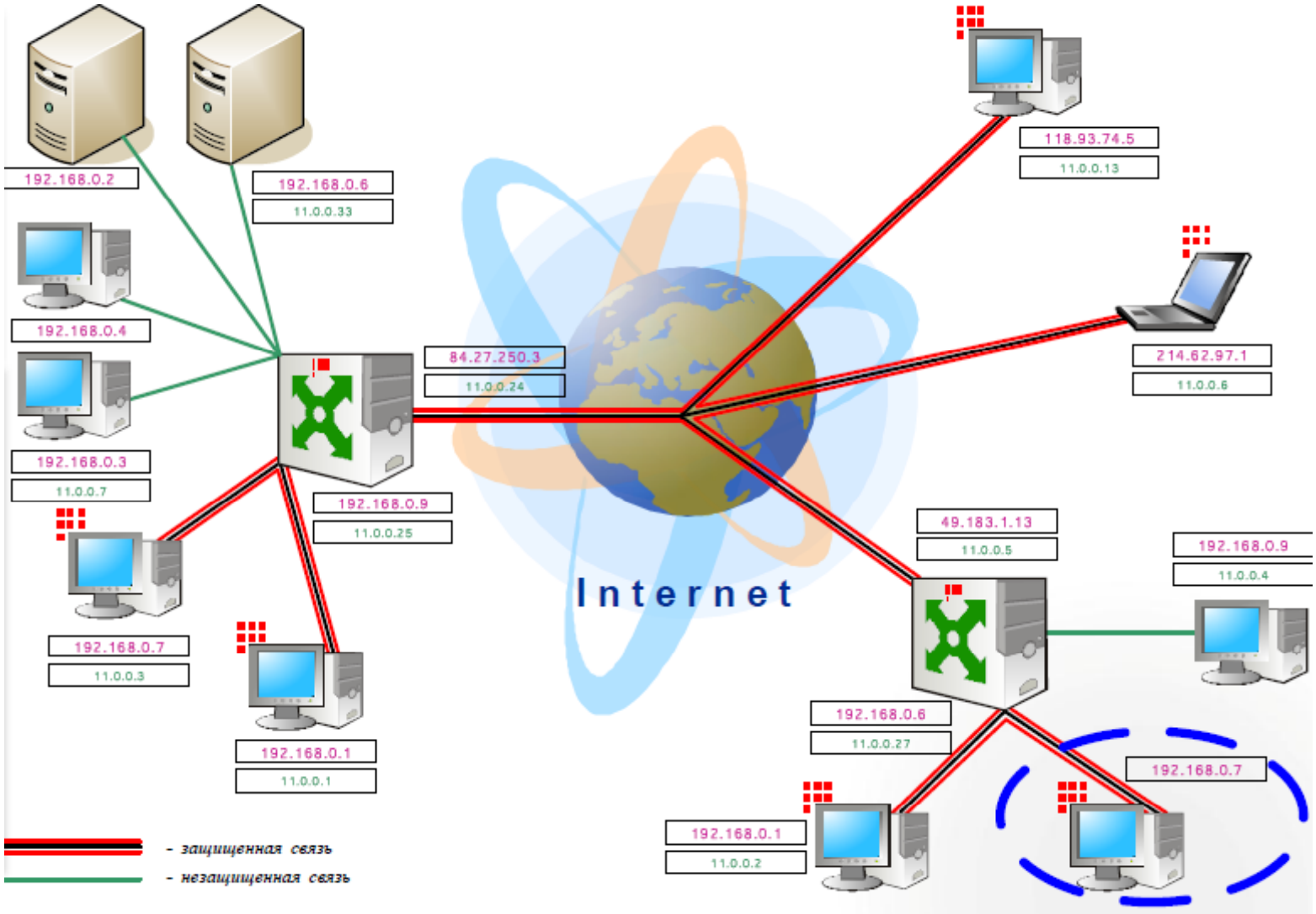
# Работа в сетях с пересекающимися IP-адресами

- **Установление взаимодействия с сетью партнера, имеющей такие же частные IP-адреса.** И согласовать адреса невозможно.



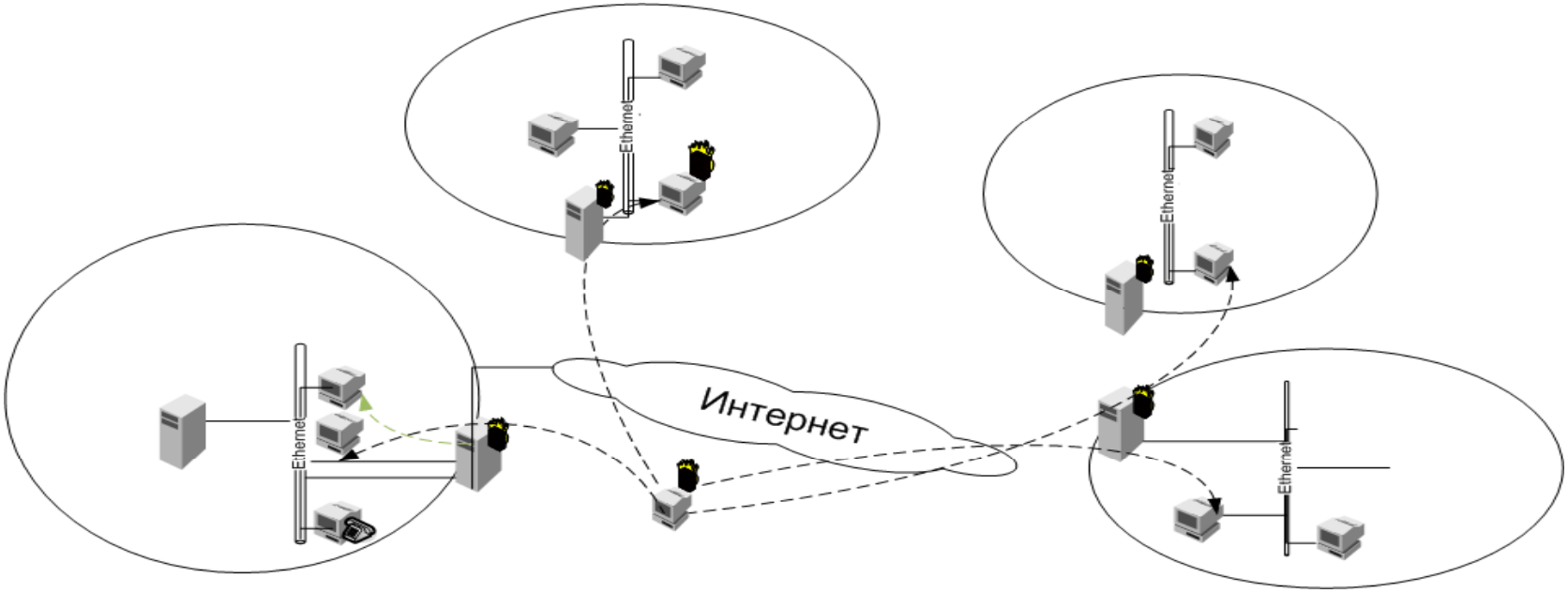

Благодаря специальной технологии виртуальных адресов, ViPNet без проблем обеспечивает взаимодействие таких сетей. Согласование IP-адресации не требуется. Для других технологий потребуется такое согласование.

# Работа в сетях с пересекающимися IP-адресами



# Множественное взаимодействие

- **Взаимодействие с множеством VPN-шлюзов и/или VPN-клиентов**



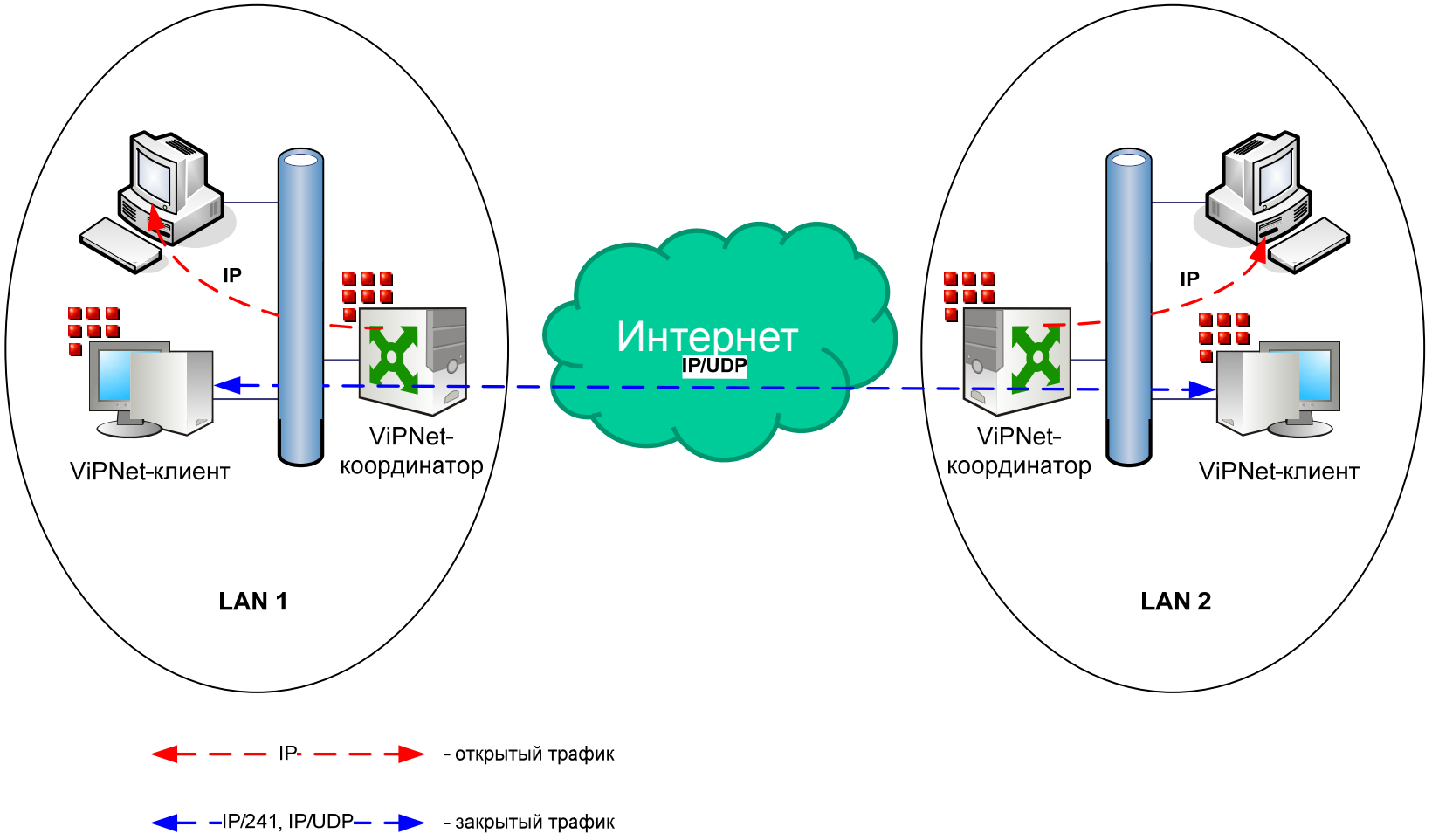

В других системах VPN потребуется настройка множества VPN-соединений для каждого VPN-шлюза. В технологии ViPNet никаких дополнительных сетевых настроек делать не надо. Пакеты маршрутизируются автоматически, если в ЦУСе заданы соответствующие связи.

# Сравнение ViPNet с другими VPN: Выводы

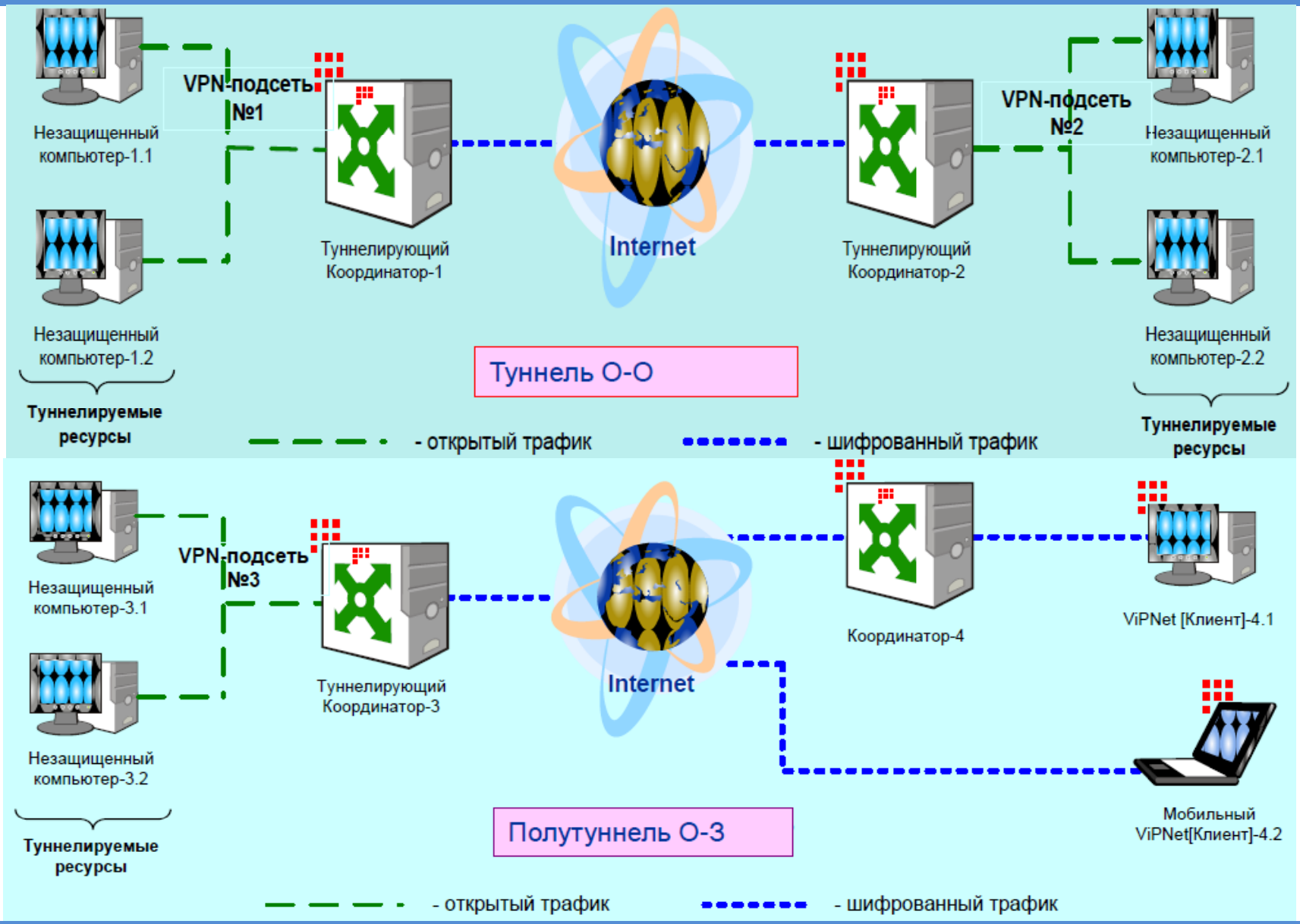
Решения ViPNet на основе симметричной криптографии и P2P-технологий позволяют быстро построить VPN-сеть любой масштабности, не обращая внимания на адресную структуру, размещать VPN-модули, как на компьютерах внутри локальных сетей, защищенных NAT-устройствами, так и на VPN-шлюзах на границе локальных сетей для защиты локальной сети в целом или ее фрагментов.

# Сценарии использования

## Защита канала связи между офисами

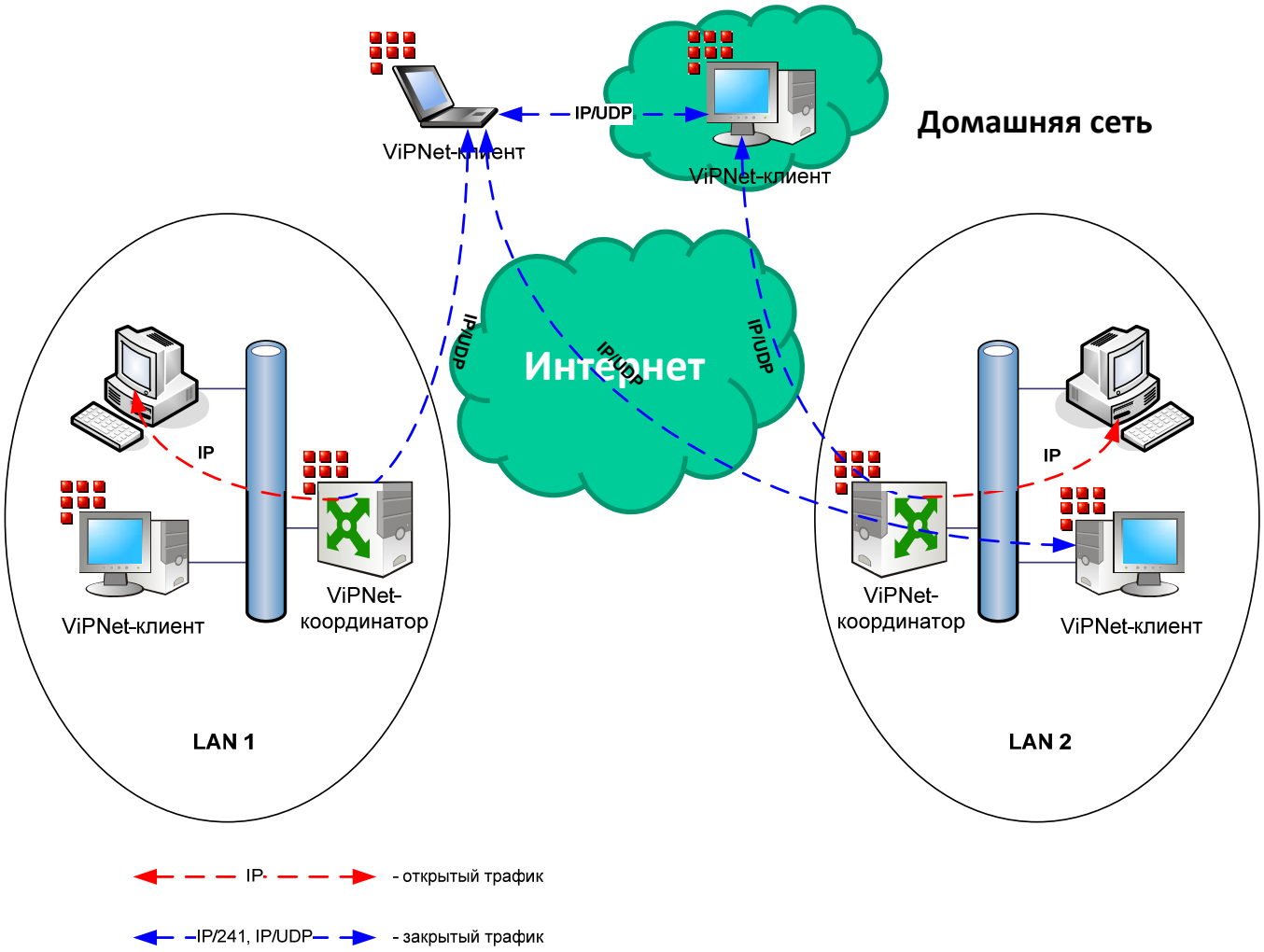


# Сценарии использования



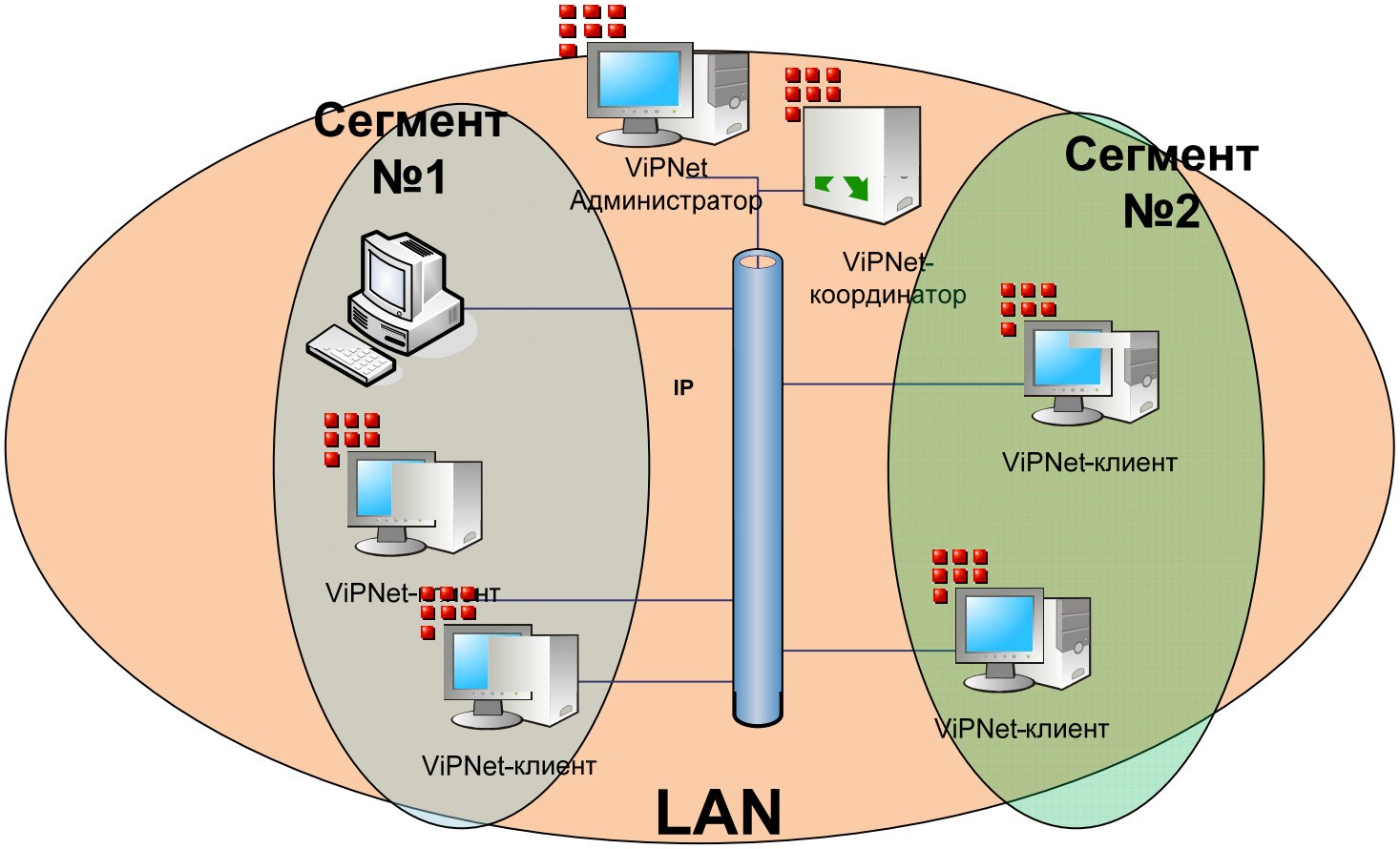
# Сценарии использования

## ❑ Защищенный удаленный доступ



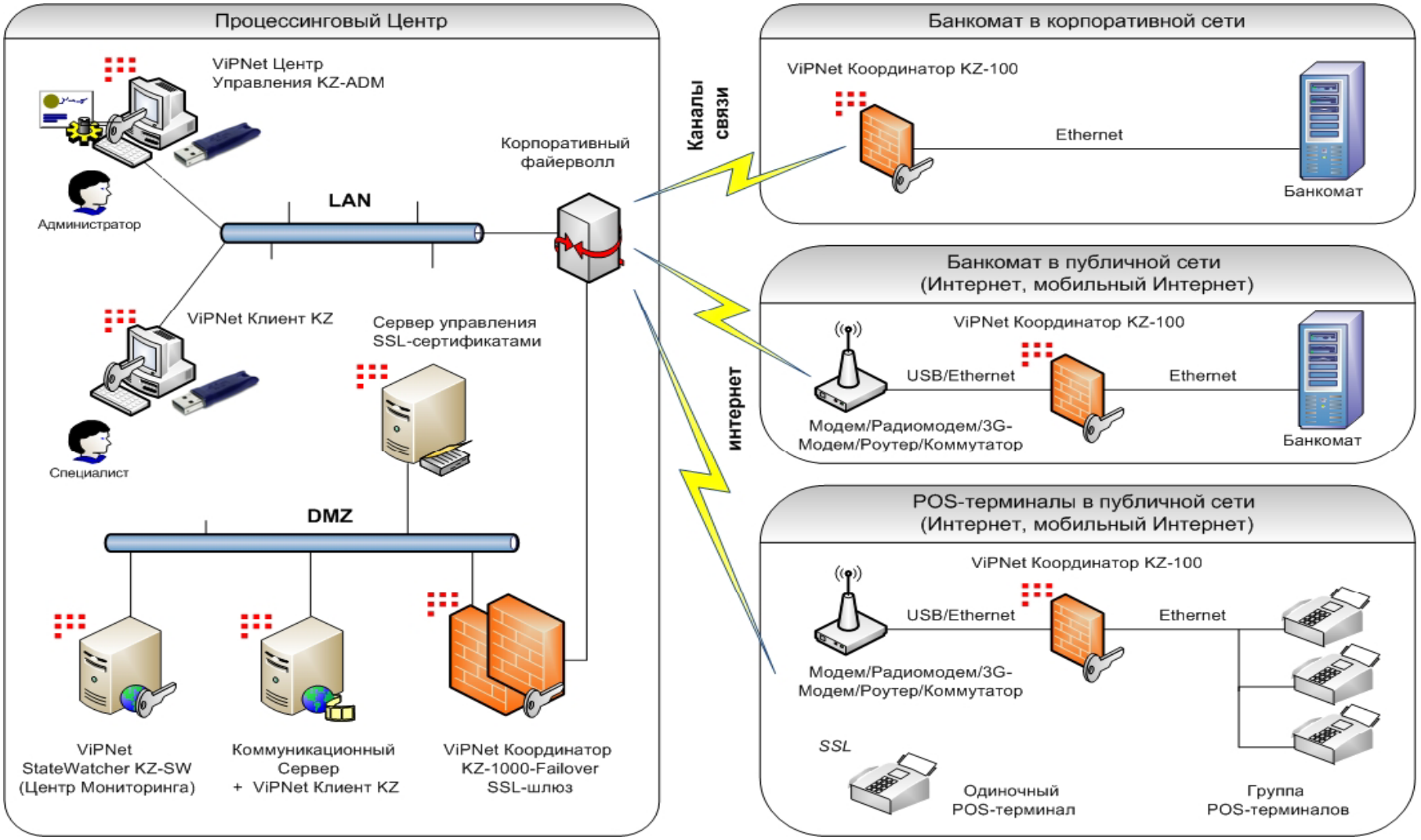
# Сценарии использования

## Разграничение доступа внутри локальной сети



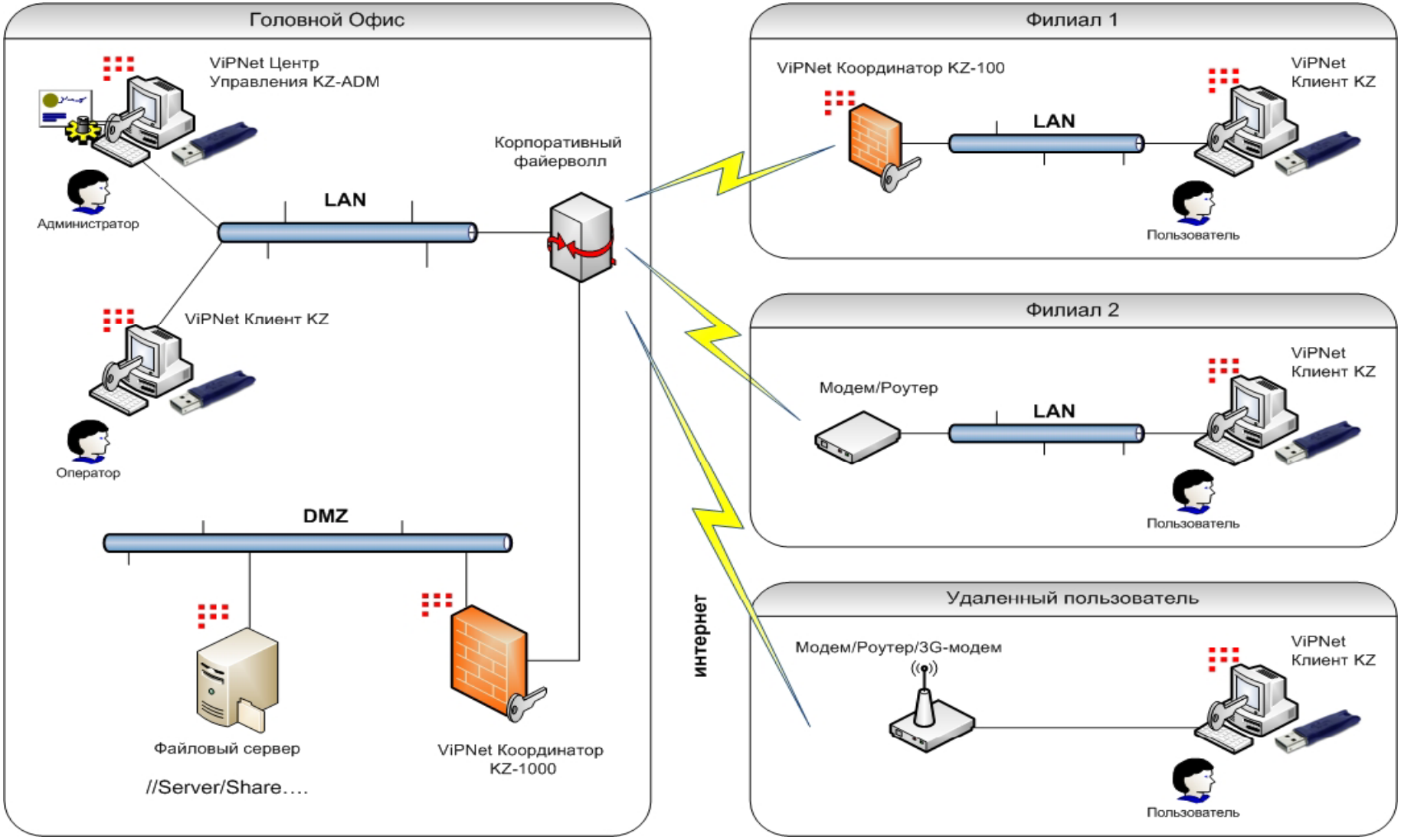
# Сценарии использования

## ❑ Защита каналов передачи данных банкоматов и POS-терминалов



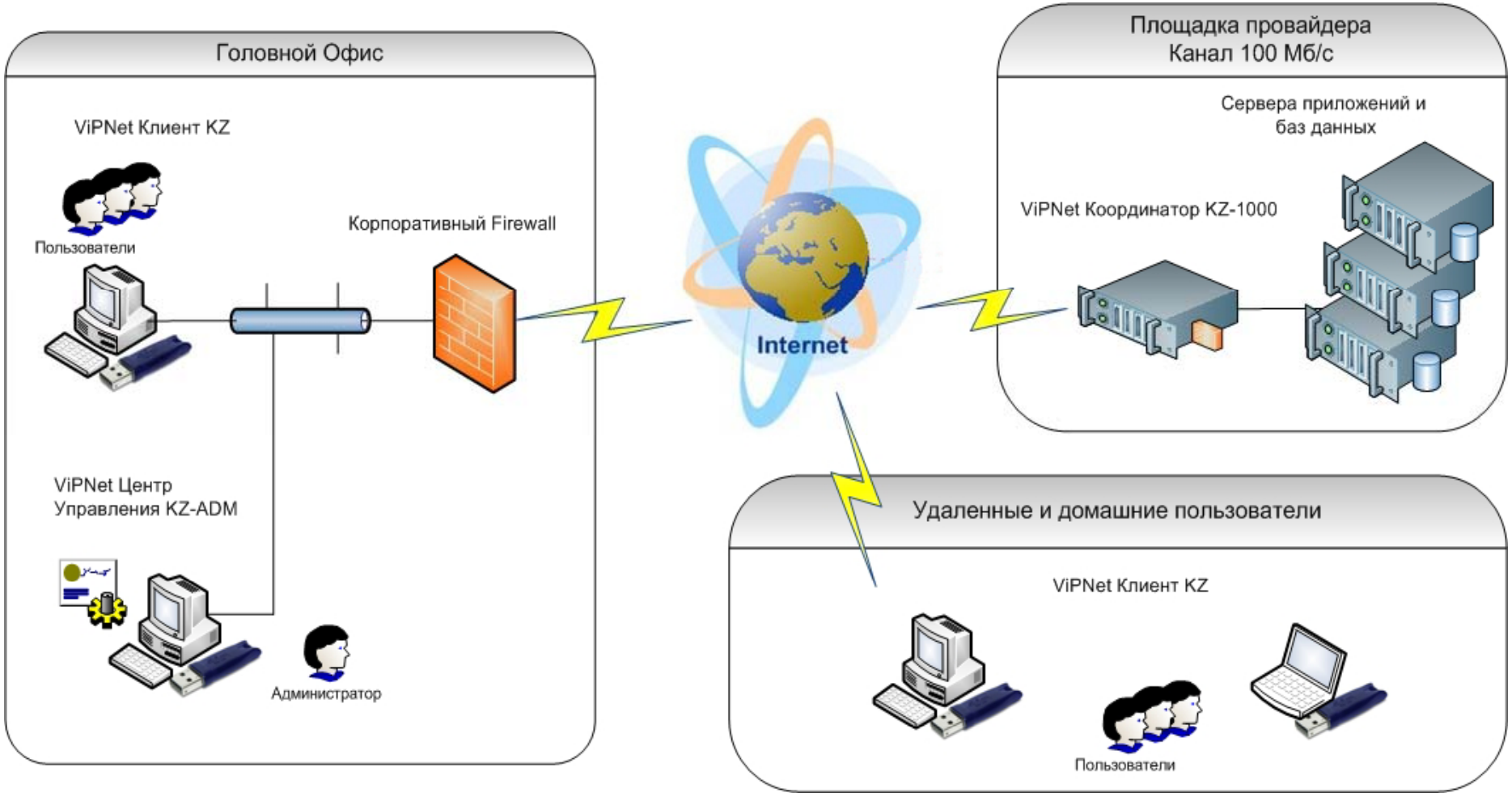
# Сценарии использования

## ❑ Автоматизированный защищенный документооборот



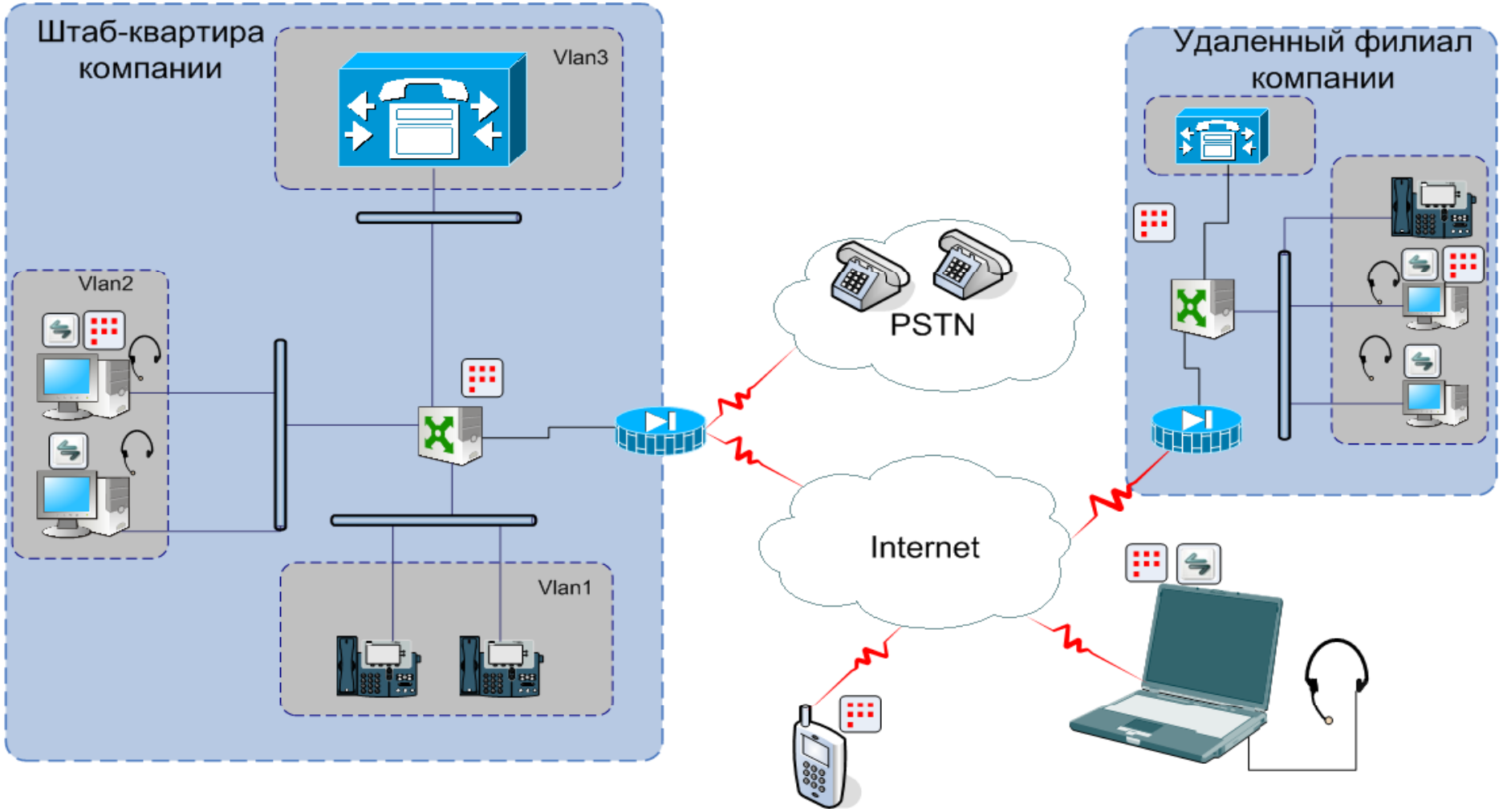
# Сценарии использования

- **Защищенный доступ к серверам приложений и базам данных**



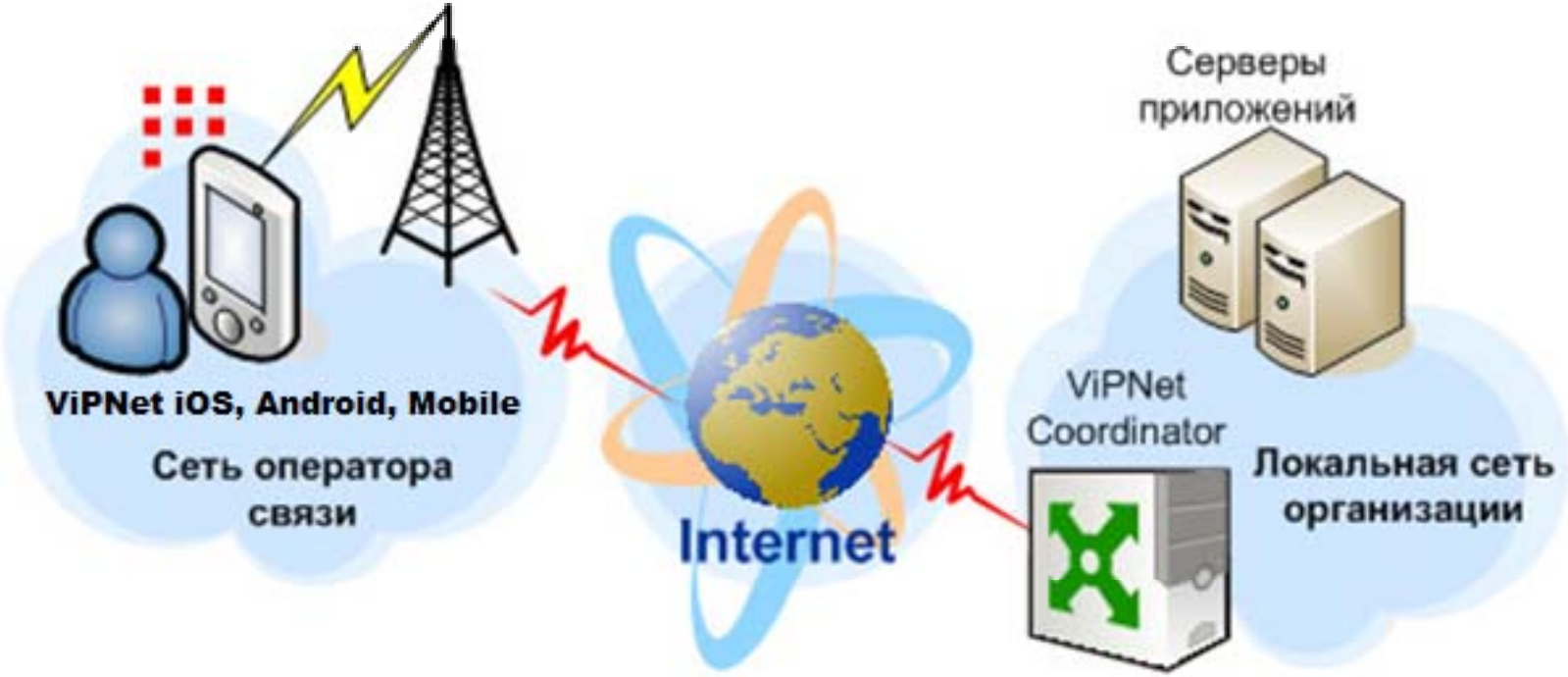
# Сценарии использования

- **Защита IP-телефонии**



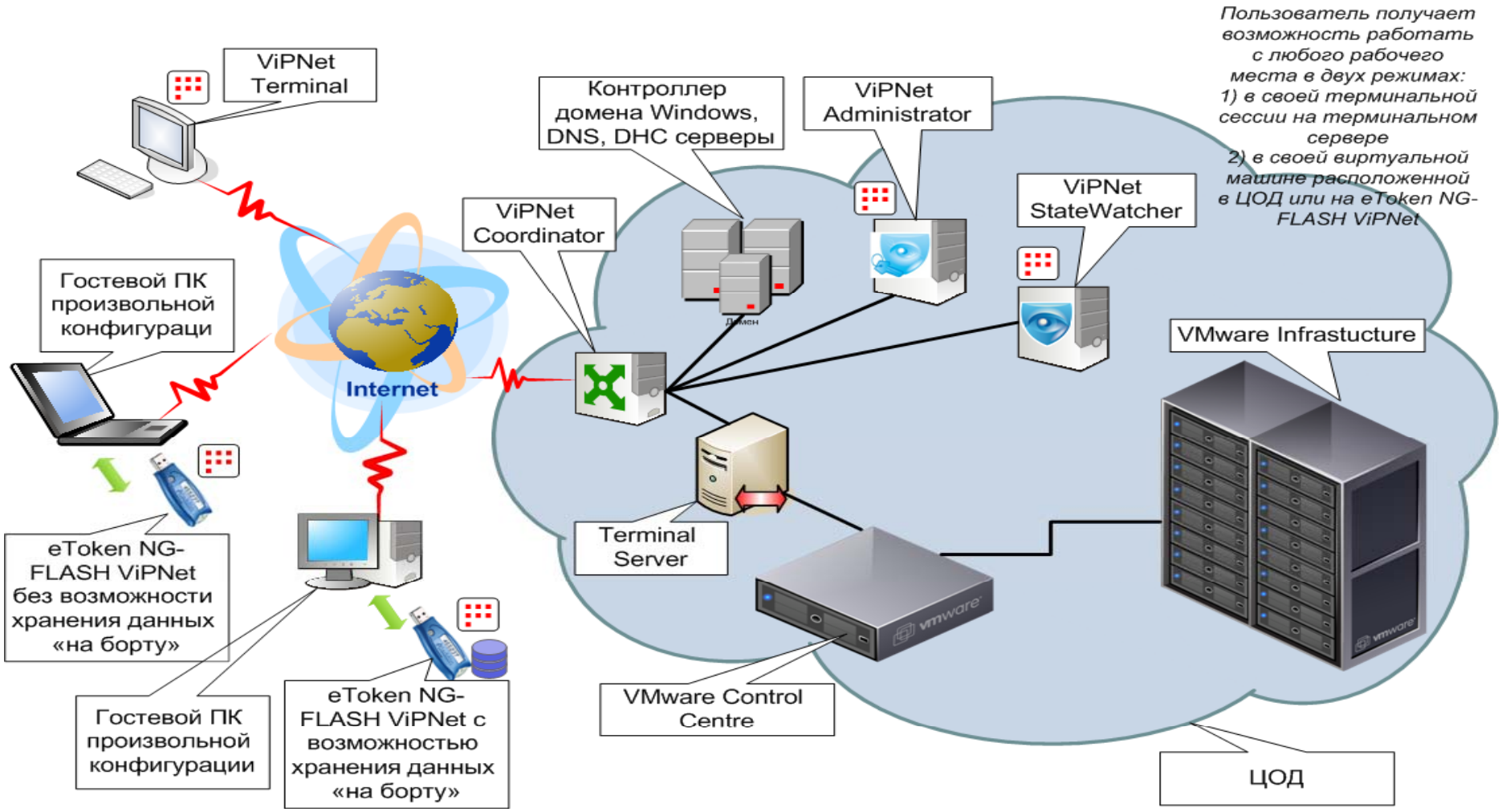
# Сценарии использования

- **Защищенный мобильный доступ**



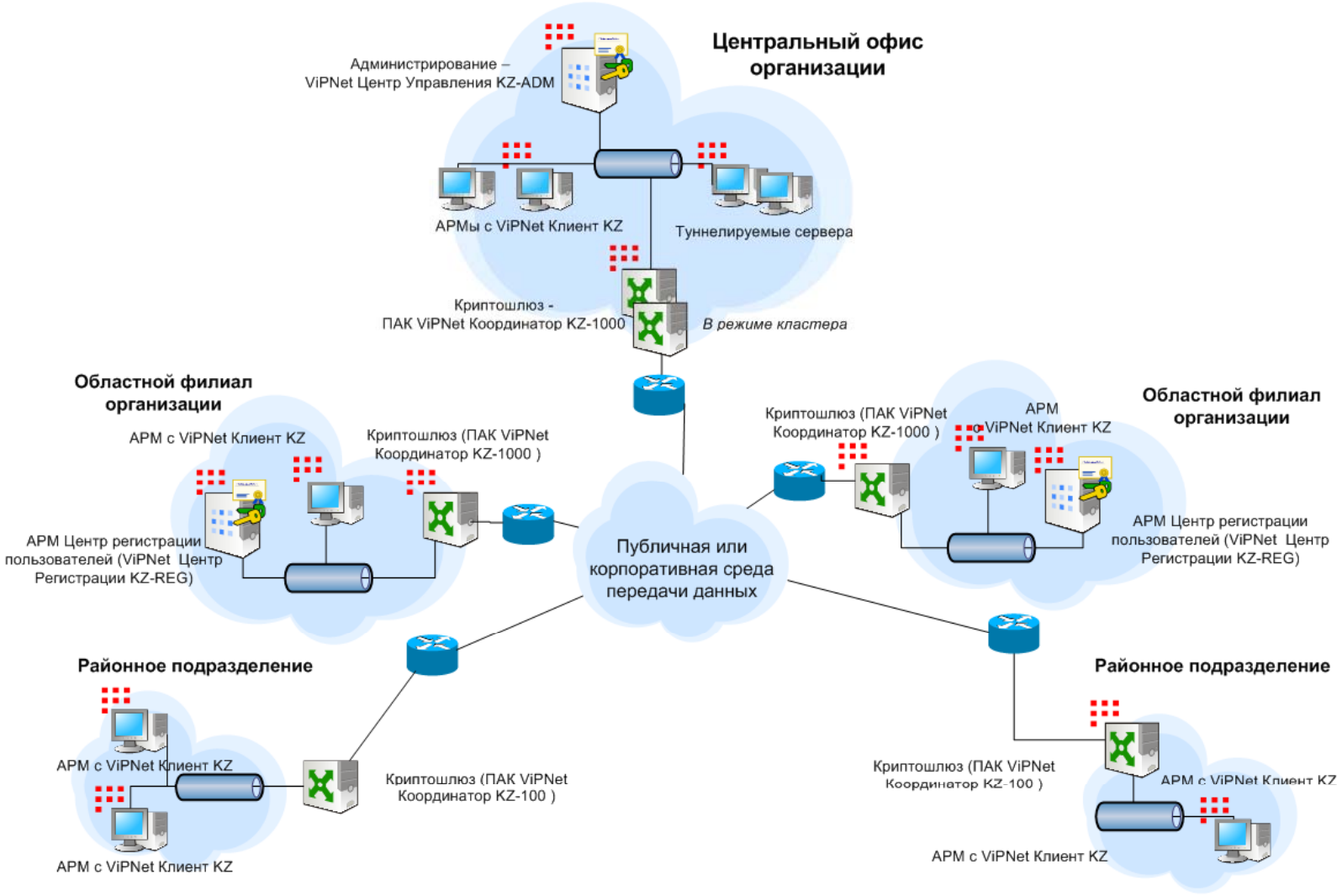
# Сценарии использования

## Защищенный терминальный доступ



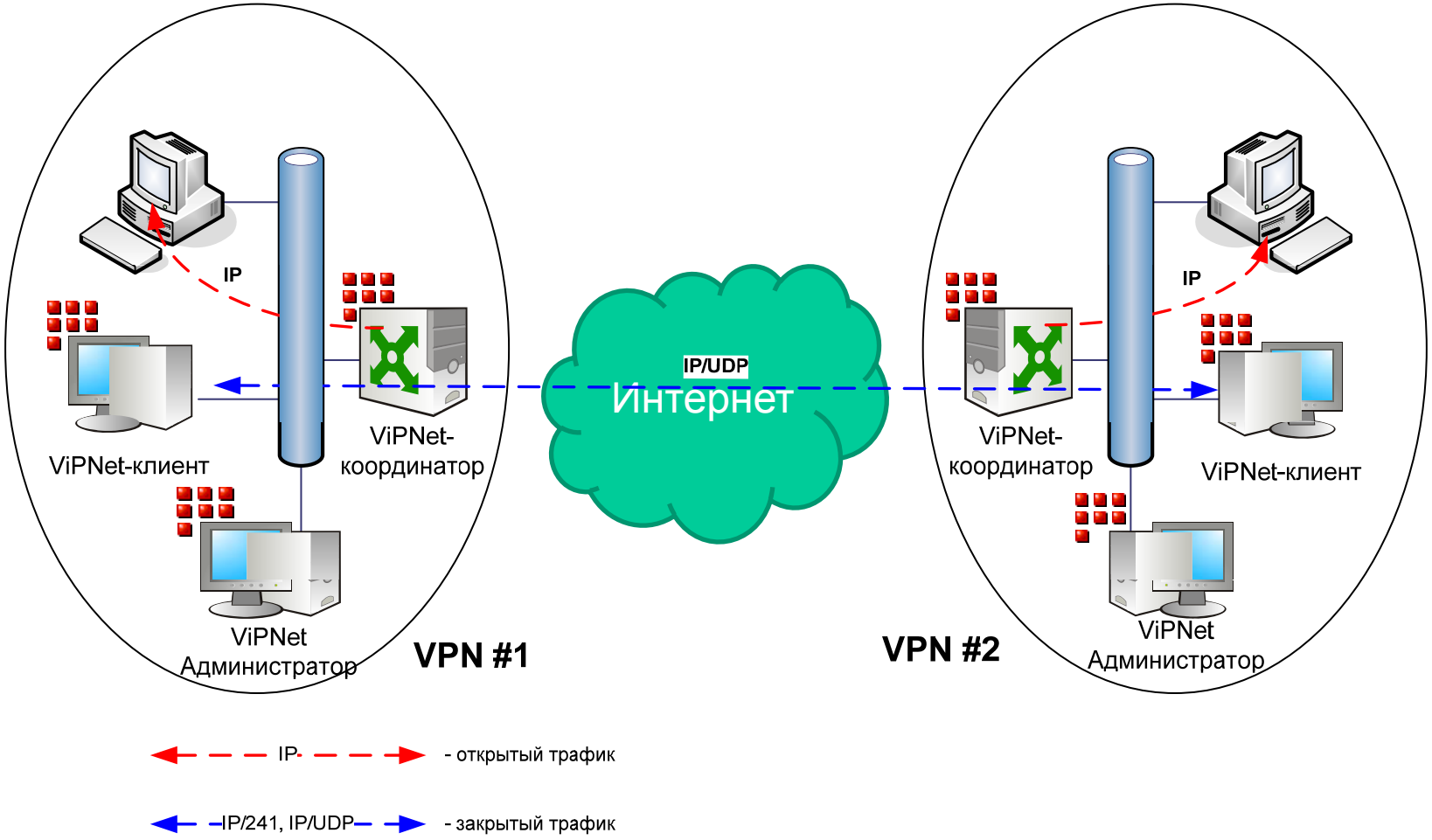
# Сценарии использования

## Территориально-распределенная защищенная сеть



# Сценарии использования

- **Межсетевое взаимодействие двух и более ViPNet-сетей**



# Преимущества нашего решения

- Лучшие и проверенные технологии, отлично показавшие себя в больших проектах
- Высокий уровень доверия к решению
- Высокие технические характеристики
- Возможность реализации различных сценариев защиты информации
- Многофункциональность
- Гибкая и удобная система управления

Спасибо за внимание.

Вопросы?