Принципы маршрутизации и преобразования IP-трафика в VPN-сети, созданной с использованием технологии ViPNet

Оглавление

1. Введение

В настоящей статье рассматриваются основные принципы маршрутизации и преобразования трафика, реализованные в виртуальной сети ViPNet, обеспечивающие взаимодействие узлов ViPNet при любых способах их подключения к телекоммуникационным сетям.

Принципы управления сетью ViPNet, ее ключевая структура, принципы служебного взаимодействия узлов ViPNet, технология фильтрации трафика, прикладные системы и почтовый транспорт технологии ViPNet, технология создания инфраструктуры электронной цифровой подписи не являются предметом рассмотрения настоящей статьи.

Современные классические VPN-системы предназначены главным образом для безопасного соединения локальных сетей через Интернет и организации удаленного доступа к их ресурсам. Однако далеко не все VPN-системы могут быть использованы для создания защищенной среды в разнородной сетевой инфраструктуре с непрозрачной IP-адресацией путем организации соединений непосредственно между источником и получателем информации (схема Peer to Peer). Другим принципиальным отличием технологии ViPNet от классических VPN-систем является отсутствие необходимости каких-либо процедур предварительной синхронизации между узлами ViPNet для начала обмена между ними информацией в зашифрованном виде.

Это свойство значительно повышает помехозащищенность системы и обеспечивает высокую надежность работы различных сетевых служб.

Задачей VPN-сети, развернутой с помощью технологии ViPNet, помимо типовой задачи VPN-сетей – защиты трафика в глобальных сетях, является задача обеспечить защиту трафика различных сетевых устройств в процессе информационного обмена между ними на всем пути от узла-источника к узлу-получателю независимо от расположения этих узлов. На этом пути может находиться разнородная сетевая инфраструктура, включающая Интернет, корпоративные, локальные сети и их сегменты.

Виртуальная сеть строится как с использованием программных компонентов ViPNet, путем установки на компьютеры ПО ViPNet Client, ПО ViPNet Coordinator, ПО ViPNet Coordinator Linux, а также программно-аппаратных комплексов ViPNet серии HW100/1000/2000/VPNM. В виртуальную сеть могут включаться также мобильные устройства на платформах IOS, Android с установленным специальным ПО ViPNet Client под эти платформы.

Компьютеры и мобильные платформы с ПО ViPNet Client в дальнейшем именуются Клиентами.
Компьютер с ПО ViPNet Coordinator, ПО ViPNet Coordinator Linux, а также программно-аппаратные комплексы ViPNet серии HW100/1000/2000/VPNM в дальнейшем именуется Координаторами. Клиенты и Координаторы являются узлами виртуальной сети ViPNet или просто узлами ViPNet. Клиенты обеспечивают сетевую защиту и включение в VPN отдельных компьютеров и устройств.

Координаторы обеспечивают сетевую защиту туннелируемых ими сетевых ресурсов, включение в VPN защищенных компьютеров независимо от места их расположения и оповещение Клиентов и координаторов о способах доступа к другим сетевых узлам, связанных с ними.

Координаторы, как правило, устанавливаются на границе сетей, и выполняют функции:

- Сервера IP-адресов — функция, которая в автоматическом режиме с помощью специального защищенного протокола динамической маршрутизации VPN-трафика обеспечивает обмен между узлами ViPNet актуальной информацией о топологии сети как внутри данной виртуальной сети, так и при взаимодействии с узлами других виртуальных сетей ViPNet. Результатом работы данного протокола является возможность маршрутизации VPN-трафика между узлами сети ViPNet тем методом, который наиболее оптимален для используемого способа и места подключения узла к сети.

- Маршрутизатора VPN-пакетов — функция, обеспечивающая маршрутизацию транзитного VPN-трафика, проходящего через координатор на другие VPN-узлы. Маршрутизация осуществляется на основании идентификаторов защищенных узлов, находящихся в открытой части VPN-пакетов, которая защищена от подделки имитовставкой, и на основании данных, полученных в результате работы протокола динамической маршрутизации VPN-трафика. Одновременно выполняется функция трансляции адресов для VPN-трафика, и все пакеты, поступающие на координатор, отправляются на другие узлы с использованием IP-адреса координатора.

- VPN-шлюза — стандартная для классических VPN функция, реализующая создание защищенных каналов (туннелей) между локальными открытыми и удаленными защищенными или туннелируемыми узлами. Координатор такой канал может создавать через каскад других координаторов, выполняющих функцию маршрутизации VPN-пакетов.

- Сервера соединений — функциональность координатора, обеспечивающая соединение клиентов и других координаторов друг с другом кратчайшим путем. Для каждого клиента можно выбрать свой сервер соединений. По умолчанию сервером соединений для клиента назначен сервер IP-адресов. Для координаторов также при необходимости может быть выбран сервер соединений.

- Транспортного Сервера — функция, которая обеспечивает доставку обновлений ключевой, справочной информации, политик и ПО из программ управления сетью ViPNet на защищенные узлы.

- Межсетевого экрана — функция фильтрации открытых, защищенных и туннелируемых транзитных и локальных сетевых соединений, трансляции адресов для открытых и туннелируемых соединений.

2. Общие принципы взаимодействия узлов ViPNet в виртуальной сети

Узлы сети ViPNet могут располагаться в сетях любого типа, поддерживающих IP-протокол. Способ подключения к сети может быть любой: сеть Ethernet, PPPoE через XDSL-подключение, PPP через подключение Dial-up или ISDN, сеть сотовой связи GPRS или UMTS, устройства Wi-Fi, сети MPLS или VLAN. ПО ViPNet поддерживает разнообразные протоколы канального уровня.

Для создания защищенных соединений между сетевыми узлами используются IP-протоколы трех типов (IP/241, UDP и TCP), в которые упаковываются пакеты любых других IP-протоколов.

При появлении любого трафика в адрес других узлов он немедленно, без каких-либо протоколов предварительного установления соединений с узлом-получателем инкапсулируется в ViPNet-пакеты и передается через VPN-сеть на узел-получатель.

Основным условием успешного соединения клиента с любым конечным узлом является наличие при включении доступа к своему Координатору, который выполняет для него функцию Сервера IP-адресов и передает ему всю необходимую информацию о способе доступа к узлам, с которыми связан.

Координаторы взаимодействуют между собой напрямую или через другие координаторы.

Указанное взаимодействие клиентов и координаторов обеспечивается с помощью протокола динамической маршрутизации VPN-трафика, работающего на прикладном уровне системы через те же VPN-соединения, и заключающегося в следующем:

- Каждый узел при включении в сеть или изменении параметров подключения:
  - Сообщает на свой Сервер IP-адресов или другие Координаторы (если узел сам является Координатором), необходимую информацию о своих адресах и способах доступа к ним,
  - Координаторы передают эту информацию на другие координаторы, в том числе координаторы других VPN-сетей с учетом заданных связей между узлами ViPNet,
  - Каждый узел при включении в сеть, а также в процессе работы, получает от своего Сервера IP-адресов или других Координаторов (если узел сам является Координатором), необходимую информацию об адресах других узлов, связанных с ним, и способах доступа к этим адресам.

- Для инкапсуляции в ViPNet-пакеты любых других IP-протоколов используются три типа IP-протокола:
- IP/UDP с портом 55777 по умолчанию или любым другим портом, который автоматически регистрируется на других узлах,
- IP/241
- TCP с портом 443 по умолчанию или любым другим портом, который автоматически регистрируется на других узлах

В локальной сети при доступности узлов по широковещательному адресу, система автоматически использует более экономичный протокол IP/241 (не имеющий дополнительных UDP-заголовков).

В других случаях, при взаимодействии узлов, которые могут быть недоступны друг другу напрямую по реальному адресу узла (т.е. между ними могут быть устройства, выполняющие NAT, или координаторы), система автоматически использует протокол UDP, для которого легко организовать прохождение IP-пакетов через любые типы Firewall и другие устройства с NAT.

Бывают случаи, когда взаимодействие защищенных узлов по UDP-протоколу невозможно, передача UDP-пакетов провайдером услуг запрещена. Например, при удаленном подключении к сети ViPNet из гостиниц или других общественных мест. В таком случае весь IP-трафик клиентов может передаваться через TCP-туннель, настроенный на координаторе, выполняющем для них роль сервера соединений, являющегося инициатором соединения. При настройке TCP-туннеля на сервере соединений может быть указан произвольный порт. По умолчанию используется порт 443.

Клиентские узлы в сети ViPNet автоматически выполняют соединения с другими узлами по кратчайшим доступным маршрутам. Для установки соединений они используют серверы (координаторы) соединений. Информацию о других узлах, параметрах доступа и их активности в данный момент клиенты получают от своего сервера IP-адресов. По умолчанию сервер IP-адресов является сервером соединений для клиента, но при необходимости сервером соединений может быть назначен другой координатор.

В зависимости от точки подключения координатора ViPNet к сети есть несколько режимов, в которые может быть установлен координатор:

- Режим – «Без использования межсетевого экрана»;
- Межсетевой экран - «За координатором»;
- Межсетевой экран – устройство «Со статической трансляцией адресов», на котором возможна настройка статических правил для входящих соединений;
- Межсетевой экран - устройство «С динамической трансляцией адресов», которое в большинстве случаев автоматически позволяет создавать исходящие соединения.

Если координатор имеет IP-адрес в Интернете, то к нему можно построить маршрут из любого места и на узле можно использовать режим «Без использования межсетевого экрана».

Если координатор расположен на границе сегмента локальной сети, которая в свою очередь защищена другим внешним координатором, то такой координатор обычно устанавливают в режим «За Координатором», выбрав в качестве координатора этот внешний координатор. Такая установка координаторов в цепочку друг за другом (каскадирование) позволяет защитить трафик внутренних сегментов локальной сети, как в самой локальной сети, так при выходе трафика за ее пределы. Количество координаторов в цепочке не ограничивается. За один координатор можно установить несколько координаторов и, тем самым обеспечить надежную защиту друг от друга и от общей локальной сети нескольких ее сегментов. В любом месте этой локальной сети могут находиться клиенты для защиты конкретных рабочих станций.

Если на границе локальной сети уже установлен межсетевой экран другого типа с возможностью настройки статических правил трансляции, то за ним можно установить координатор с внутренними адресами в режим межсетевого экрана «Со статической трансляцией адресов». Каждый из сетевых интерфейсов координатора может находиться за своим межсетевым экраном со статическими правилами трансляции. Через этот координатор будет обеспечено взаимодействие других узлов ViPNet и открытых узлов в локальной сети с узлами за ее пределами. Координатор в данном режиме успешно работает и при отсутствии внешнего межсетевого экрана. Поэтому такой режим устанавливается на координаторах по умолчанию.

Если координатор устанавливается на выходе небольшой локальной сети, которая подключается к внешним сетям через NAT-устройства с динамической трансляцией адресов, то используется режим межсетевого экрана «С динамической трансляцией адресов». В этом случае для этого координатора выбирается в качестве сервера соединений один из координаторов, имеющий постоянный доступ из внешней сети. Сервер соединений обеспечивает такому координатору возможность инициативного соединения с защищаемыми им ресурсами со стороны любых других связанных с ним узлов.

По умолчанию Координаторы устанавливаются в режим работы через межсетевой экран «Со статической трансляцией адресов», который может быть изменен в центре управления сетью.

Для того, чтобы узлы могли начать взаимодействовать с другими узлами сети ViPNet без каких-либо дополнительных настроек со стороны пользователей достаточно в центре управления сетью задать IP-адреса доступа к координаторам или их DNS-имена, а для взаимодействия с узлами других сетей ViPNet обменяться некоторой информацией экспорта/импорта между центрами управления этими сетями. Всю остальную информацию, необходимую для взаимодействия приложений, узлы получат с помощью протокола динамической маршрутизации VPN-трафика.

3. Работа клиентов в сети ViPNet

3.1. Соединение двух клиентских узлов, подключившиеся к сети Интернет через устройства с динамическим NAT

Рассмотрим организацию соединений между двумя клиентскими узлами, подключившиеся к сети Интернет через устройства с динамическим NAT. Например один из них (Клиент 1) находится в гостинице в Лондоне, а другой в гостинице в Санкт Петербурге (Клиент 2):

- При включении компьютера каждый из клиентов определяет канал доступа к своему серверу соединений (сервер соединений может быть и общий). Если клиент определил, что работает через устройство NAT, то он продолжает поддерживать канал путем периодической отправки на сервер IP-пакетов, тем самым открывая доступ к себе для инициативных соединений с других узлов через свой сервер соединений. Интервал отправки IP-пакетов на сервер соединений по умолчанию равен 25 секундам. Этого, как правило, достаточно для работы через большинство устройств NAT. При необходимости интервал (тайм-аут) может быть изменен.

- Если от некоторого приложения на Клиенте 1 появляется трафик в сторону Клиента 2 (например Voice IP), то он начинает передавать первые пакеты через свой сервер соединений. Сервер соединений в свою очередь пересылает эти пакеты на сервер соединений Клиента 2, а тот уже – Клиенту 2. Обратный трафик идет аналогичным маршрутом. Одновременно с этим Клиент 1, а при получении первого любого пакета и Клиент 2 делают попытку установить более прямое соединение с удаленным узлом путем передачи тестовых IP-пакетов напрямую на адрес доступа к Клиенту и адрес доступа к серверу соединений Клиента. Информацию о прямых адресах и портах доступа к этим узлам клиент получил от своего сервера IP-адресов

- Если тестовые прямые IP-пакеты сумели пройти через NAT хотя бы одного из клиентов, то этот клиент регистрирует у себя прямое соединение с другим клиентом и начинает передавать ему свой Voice IP трафик напрямую через открывшееся соединение. Другой клиент при получении первого прямого пакета от удаленного узла весь свой трафик также начинает передавать ему напрямую.

- Если тестовые IP-пакеты дошли только до сервера соединений удаленного узла, то сервер соединений регистрирует это соединение и отправляет напрямую клиенту ответные IP-пакеты удаленного узла.

- Если клиенту не удается соединиться со своим сервером соединений (провайдер не пропускает UDP трафик), то клиент пытается установить соединение со своим сервером соединений по TCP (порт 443 по умолчанию, можно установить порт 80 и любой другой). Если ему это удается, то весь зашифрованный трафик с другими защищенными узлами автоматически передается через это TCP-соединение на сервер соединений, а уже оттуда на другие узлы в виде инкапсулированных UDP-пакетов. Если этот трафик предназначен другому клиенту, находящемуся в аналогичных условиях, то UDP-трафик, дойдя до его сервера соединений, пойдет к этому клиенту через установленное с ним TCP-соединение.

- Если клиента необходимо расположить за устройством со статической трансляцией адресов, то в его настройках следует зафиксировать нужный порт инкапсуляции UDP-пакетов.

То есть с удаленным узлом устанавливается либо прямое соединение или соединение через один из серверов соединений. Если тестовые IP-пакеты никуда не дошли, то клиенты по-прежнему продолжают обмен между собой через свои серверы соединений.

Существует 4 типа динамического NAT: Cone NAT, Address-Restricted cone NAT или Restricted cone NAT. Port-Restricted cone NAT, Symmetric NAT. Для установки прямого соединения в полной мере не поддерживается только Symmetric NAT. Но если хотя бы у одной стороны другой тип, то прямое соединение установится.

Таким образом, если существует возможность, узлы устанавливают взаимодействие друг с другом по кратчайшим маршрутам без участия координаторов, за счет чего повышается скорость обмена шифрованным IP-трафиком и снижается нагрузка на координаторы.

3.2. Работа клиента в локальной сети и другие особенности работы клиентских узлов

Если клиентский узел находится в маршрутизируемой по отношению к другим узлам сети, то клиент автоматически определяет эту ситуацию и соединение с другими узлами производится в соответствии с заданными маршрутами, а не через координаторы.

Если удаленный узел, с которым устанавливается соединение, не расположен за устройством NAT, то информация о возможности прямого доступа к нему сохраняется и при следующих соединениях с этим узлом, если не изменилось его местоположение, IP-трафик сразу начинает передаваться по прямому маршруту в соответствии с таблицей маршрутизации.

Сам пользователь или администратор может выбрать для клиента в качестве сервера соединений любой координатор. Это дает возможность пользователям с мобильными компьютерами или устройствами подключиться к VPN-сети в чужой локальной сети, где есть Координатор и с ним связан данный узел. В этом случае мобильный узел получает доступ ко всем ресурсам, как будто находится в его собственной локальной сети. Возможность смены Координатора полезна также в случае выхода из строя оборудования или каналов связи.

4. Работа координаторов в сети ViPNet

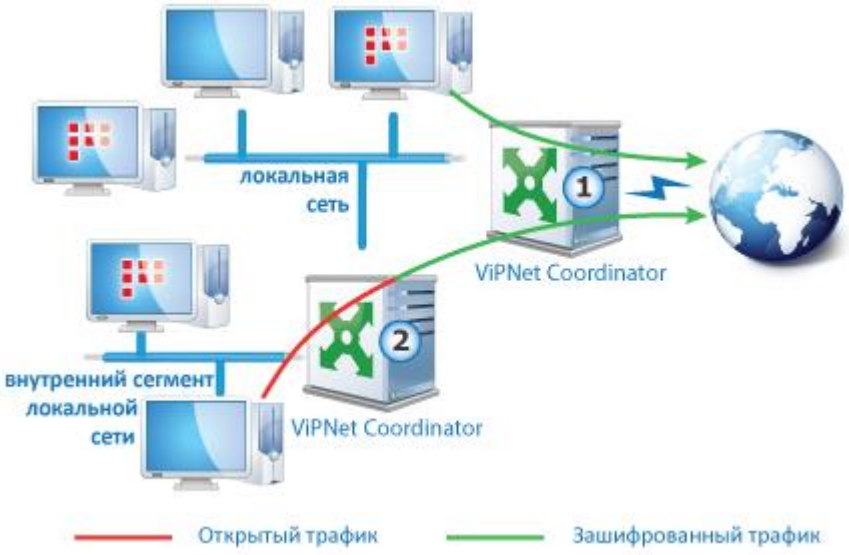
4.1. Режим без использования межсетевого экрана

Как было сказано выше, этот режим главным образом используется на координаторах, которым выделен адрес в сети Интернет. Через этот координатор открытые узлы и узлы ViPNet локальной сети взаимодействуют с внешними ресурсами.

4.2. Режим межсетевого экрана «За координатором»

Установка координаторов внутри локальной сети в этот режим за координатор, стоящий на ее границе, приводит к следующим свойствам:

- Координаторы ViPNet, защищающие сегменты локальной сети, автоматически отправляют зашифрованный ими туннелируемый трафик, предназначенный внешним защищенным ресурсам, на координатор на границе сети, который отправляет его дальше в соответствии с имеющейся у него информацией о внешних узлах.
- Удаленные узлы ViPNet отправляют трафик, предназначенный ресурсам, защищаемым внутренним координатором, на внешний координатор, который перенаправляет его дальше.



Такое включение Координаторов называется «каскадным». Каскадное включение координаторов позволят защитить трафик с внутренним сегментом локальной сети, как в самой локальной сети, так и во внешней сети. Количество координаторов в каскаде не ограничивается.

Каскадирование координаторов позволяет также пропустить VPN-трафик по нужному маршруту в глобальной сети, что часто используется для его контроля в различных схемах администрирования.

4.3. Режим межсетевого экрана "Со статической трансляцией адресов".

В ряде случаев на границе локальной сети уже установлен межсетевой экран, выполняющий функции трансляции адресов с возможностью настройки статических правил трансляции адресов.

Координатор с частным IP-адресом может использовать этот межсетевой экран для взаимодействия с узлами ViPNet во внешних сетях. Для этого на координаторе выбирается режим межсетевого экрана «Со статической трансляцией адресов" и задается порт, для взаимодействия с внешними узлами.

Если в локальной сети устанавливается несколько клиентов ViPNet, то в такой сети целесообразно установить Координатор в режиме межсетевого экрана "Со статической трансляцией адресов". В этом

случае на межсетевом экране потребуется сделать настройки только для координатора. Другие узлы ViPNet будут работать с внешними узлами через координатор и межсетевой экран без дополнительных настроек на межсетевом экране

Для обеспечения прохождения трафика через внешний межсетевой экран, на нем должны быть настроены статические правила трансляции адресов, обеспечивающие:

- Перенаправление входящих пакетов на адрес координатора в соответствии с заданным на координаторе портом доступа.
- Пропуск во внешнюю сеть UDP-пакетов с адресом и портом координатора.

4.4. Режим межсетевого экрана "С динамической трансляцией адресов"

Как сказано выше, координатор в этот режим следует устанавливать, если локальная сеть к внешней сети подключается через устройства с динамическим NAT. Внутри локальной сети могут находиться и клиенты и туннелируемые ресурсы. Работа с такой сетью с других узлов также возможна в полном объеме с использованием внешнего сервера соединений, доступного для других узлов. Работа координатора в этом режиме аналогична описанной выше работе клиента

5. Туннелирование открытых ресурсов

Для включения в виртуальную сеть ViPNet устройств или узлов локальной сети, трафик которых не требуется защищать в локальной сети, координатор выполняет функцию туннелирующего сервера (или Крипто шлюза).

Координатор обеспечивает туннелируемые устройства сведениями об IP-адресах узлов сети ViPNet, выступает шлюзом для передачи трафика в сеть ViPNet, осуществляет инкапсуляцию в UDP-протокол и шифрование трафика от открытых устройств, осуществляет прием и передачу туннелированного трафика в сети ViPNet от своего имени.

Таким образом, для обеспечения соединения любого удаленного узла ViPNet (или любого другого туннелируемого устройства удаленной локальной сети) с открытыми ресурсами, туннелируемыми Координатором, доступны все вышеописанные схемы подключения, что позволяет использовать все преимущества виртуальной сети ViPNet в распределенных информационных сетях со сложной топологией.

6. Маршрутизация трафика координатором с несколькими сетевыми интерфейсами

Координатор может иметь произвольное количество физических или виртуальных адаптеров, подключенных к разным подсетям. Со стороны каждого адаптера могут находиться туннелируемые открытые ресурсы, клиенты и другие координаторы. Для соединения с удаленными ресурсами, расположенными за другими координаторами, может использоваться несколько отдельно маршрутизируемых альтернативных каналов связи.

Для того, чтобы координатор успешно обслуживал трафик со стороны всех своих адаптеров, требуется только настроить стандартные для маршрутизаторов маршруты для адресов доступа к удаленным и локальным ресурсам. Для удаленных ресурсов, расположенных за другими координаторами, достаточно настроить маршрут только до адресов доступа к ближайшему координатору.

То есть достаточно иметь шлюз по умолчанию, шлюзы в подсетях интерфейсов для адресов доступа к другим удаленным ViPNet-узлам, шлюзы для доступа в локальные подсети, доступные через подсети интерфейсов. Такой минимум настроек маршрутных таблиц стал возможным в современных версиях ViPNet. Ранее требовалось производить настройки не только к адресам доступа к соответствующим подсетям, но и к самим подсетям, где располагались защищаемые ресурсы.

7. Виртуальные адреса системы ViPNet

Технология ViPNet предоставляет возможность обеспечить взаимодействие между защищаемыми ресурсами, которые имеют частные IP-адреса. При этом не надо заботиться о распределении подсетей частных IP-адресов. На удаленных сторонах могут использоваться одинаковые частные IP-адреса и подсети защищаемых ресурсов.

Для обеспечения такой возможности на каждом узле ViPNet для всех узлов ViPNet, автоматически формируются непересекающиеся виртуальные адреса в соответствии с количеством адресов на удаленном узле. Для каждого туннелируемого адреса или диапазона адресов удаленных координаторов, с которым может взаимодействовать данный узел или его туннелируемые ресурсы, формируются непересекающиеся виртуальные адреса и диапазоны.

Виртуальные адреса для узлов не зависят от собственных адресов узлов и привязаны к уникальным идентификаторам этих узлов, присвоенным им в ЦУСа.

На каждом узле для других узлов и туннелируемых ими устройств формируется свой набор виртуальных адресов.

Драйвер ViPNet при отправке и получении пакетов производит подмену адресов источника и назначения пакетов, тем самым информируя приложения на данном компьютере или туннелируемом ресурсе об адресе, по которому ему надо работать с приложениями на других узлах.

Кроме того, информирование приложения о виртуальном адрес происходит через службы DNS, WINS для любых приложений, протоколы SCCP, SIP, H323 и другие для приложений мультимедиа. Драйвер ViPNet в теле пакетов этих протоколов также производит подстановку нужных адресов видимости узлов и туннелируемых ресурсов.

В результате таких преобразований приложения на данном узле ViPNet или туннелируемых им устройствах обращаются к соответствующим приложениям на других узлах или туннелируемых ими ресурсах по уникальному на данном компьютере виртуальному адресу, исключающим конфликты.

Узлы ViPNet по умолчанию используют виртуальные адреса при взаимодействии с компьютерами, которые узел ViPNet, определил, как недоступные по прямому адресу узла, то есть находящиеся в других подсетях.

При изменении IP-адреса узла ViPNet (что характерно для мобильных компьютеров и компьютеров с настроенной службой DHCP-client), его виртуальный адрес, единожды зарегистрированный на другом узле, не изменится. Это свойство можно использовать в приложениях для надежной аутентификации узла по его виртуальному адресу.

Для виртуальных адресов на узлах ViPNet нет необходимости задавать какие-либо маршруты. Драйвер ViPNet выполняет автоматическую маршрутизацию трафика с виртуальными адресами на нужные реальные адреса доступа.

8. Заключение

Рассмотренные в настоящей статье методы и способы использования технологических решений ViPNet для организации безопасного соединения компьютеров в IP-сетях с непрозрачной адресацией, решают все возникающие на сегодня практические потребности в этой области.

За счет работы протокола динамической маршрутизации VPN-трафика настройки на узлах ViPNet со стороны пользователей и администраторов даже в самых сложных конфигурациях сетей максимально минимизируются или не требуются вовсе.

Вице-президент
ОАО Инфотекс по развитию продукта
Владимир Игнатов,
Тел. (495) 737-61-92,
E-mail: science@infotecs.ru