РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 604 328**(13) **C1**

(51) МПК
G06F 15/16 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2015126544/08, 03.07.2015**

(24) Дата начала отсчета срока действия патента:
03.07.2015

Приоритет(ы):
(22) Дата подачи заявки: **03.07.2015**

(45) Опубликовано: **10.12.2016** Бюл. № **34**

(56) Список документов, цитированных в отчете о поиске: **US 2013/0246640 A1, 19.09.2013. US 8499095 B1, 30.07.2013. RU 2292648 C2, 27.01.2007. WO 00/39987, 06.07.2000. US 2008/0137859 A, 12.06.2008. RU 2132597 C1, 27.06.1999.**

Адрес для переписки:
127287, Москва, Старый Петровско-Разумовский пр-д, 1/23, стр. 1, Открытое акционерное общество "Информационные технологии и коммуникационные системы"

(72) Автор(ы):
Тычина Леонид Анатольевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Информационные технологии и коммуникационные системы" (RU)

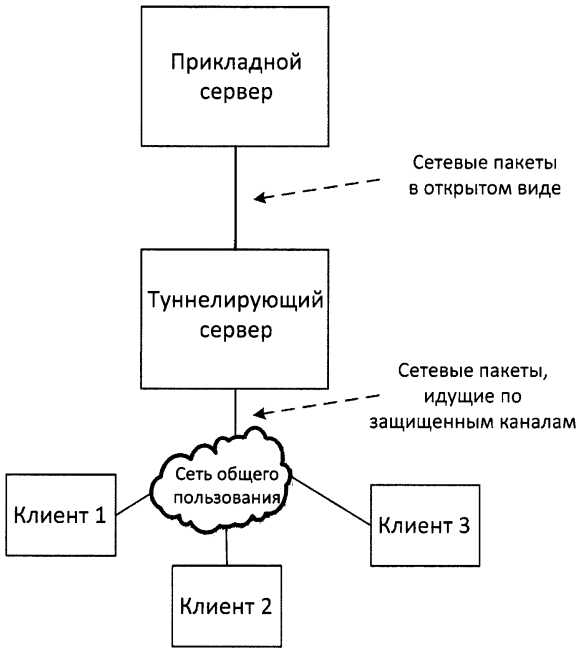
RU 2604328 C1

(54) СПОСОБ ФОРМИРОВАНИЯ ЗАЩИЩЕННОГО СОЕДИНЕНИЯ В СЕТЕВОЙ КОМПЬЮТЕРНОЙ СИСТЕМЕ

(57) Реферат:

Изобретение относится к способам обеспечения безопасности в сетях передачи данных. Технический результат заключается в повышении защищенности соединения между компьютерами-клиентами. Указанный результат достигается за счет применения способа формирования защищенного соединения в сетевой компьютерной системе. Система включает прикладной сервер, осуществляющий прием и обработку запросов по прикладному протоколу от компьютеров-клиентов по сети через туннелирующий сервер. Компьютеры-клиенты выполнены с возможностью осуществлять взаимодействие между собой и с прикладным сервером по прикладному протоколу. Посылают запрос из первого компьютера-клиента в прикладной сервер для осуществления взаимодействия со вторым компьютером-клиентом; анализируют в туннелирующем сервере ответ из прикладного сервера первому компьютеру-клиенту; если в ответе присутствует сетевой адрес второго компьютера-клиента, то передают из туннелирующего сервера первому компьютеру-клиенту вместе с сообщением прикладного протокола информацию, необходимую для установки защищенного соединения со вторым компьютером-клиентом; формируют защищенное соединение между первым компьютером-клиентом и вторым компьютером-клиентом. 2 ил.

RU 2604328 C1



Фиг. 1

RU 2604328 C1

RU 2604328 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 604 328** (13) **C1**

(51) Int. Cl.
G06F 15/16 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2015126544/08, 03.07.2015**

(24) Effective date for property rights:
03.07.2015

Priority:
(22) Date of filing: **03.07.2015**

(45) Date of publication: **10.12.2016** Bull. № **34**

Mail address:
127287, Moskva, Staryj Petrovsko-Razumovskij pr-d, 1/23, str. 1, Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy"

(72) Inventor(s):
Tychina Leonid Anatolevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Informatsionnye tekhnologii i kommunikatsionnye sistemy" (RU)

(54) METHOD OF SECURED CONNECTION FORMING IN NETWORK COMPUTER SYSTEM

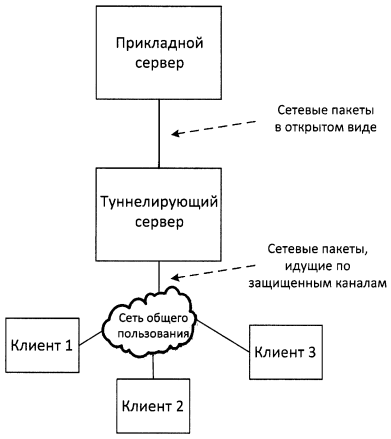
(57) Abstract:

FIELD: safety.

SUBSTANCE: invention relates to methods of ensuring safety in data networks. Said result is achieved by using method of protected connection establishing in network computer system. System includes application server, performing reception and processing of requests via application protocol from client computers over network through tunnelling server. Client computers are made with possibility of interaction between themselves and with application server via application protocol. Sending request from first client computer to application server for interaction with second client computer; analyzing response from application server to first client computer in tunnelling server; if response contains network address of second client computer, then sending from tunnelling server to first client computer together with application protocol message information, required for establishing secured connection with second client computer; generating secured connection between first client computer and second client computer.

EFFECT: technical result is improved security of connection between client computers.

1 cl, 2 dwg



Фиг. 1

RU 2604328 C1

RU 2604328 C1

Область техники, к которой относится изобретение

Предлагаемое изобретение относится к способам обеспечения безопасности в сетях передачи данных и, в частности, к способам организации защищенного канала передачи по требованию.

Уровень техники

Развитие сетей передачи данных привело к созданию многочисленных прикладных приложений, использующих сеть для взаимодействия. Актуальной задачей является обеспечение безопасности такого сетевого взаимодействия. Для обеспечения безопасности в практике используются различные решения.

Разработаны отдельные протоколы, обеспечивающие безопасность, например, архитектура безопасности IPsec [1, 2] обеспечивающие криптографическую защиту IP протокола.

В архитектуре IPsec предусмотрен способ организации защищенного канала передачи по требованию. Способ включает в себя предварительное определение диапазонов IP-адресов, взаимодействие по которым должно происходить по защищенному каналу. При начале взаимодействия по адресу из диапазона происходит организация защищенного канала. Защищенный канал при отсутствии активности удаляется.

Недостатком способа является необходимость заранее знать диапазоны IP-адресов, которые подлежат защите. Это часто невозможно, особенно в больших сетях.

Известен также способ маршрутизации пакетов [3], реализуемый в сетевой компьютерной системе.

Сетевая компьютерная система включает связанные через сеть центральный концентратор и компьютеры-клиенты, причем компьютеры-клиенты, в общем случае, могут входить в состав других подсетей, имеющих локальные концентраторы.

Способ включает следующие действия:

- получают пакет в центральном концентраторе, причем пакет, полученный от 1-го компьютера-клиента, предназначен для передачи 2-му компьютеру-клиенту;

- в ответ на получение пакета в центральном концентраторе направляют запрос 2-му компьютеру-клиенту, чтобы передать в центральный концентратор информацию о множестве сетей, с которыми связан 2-ой компьютер-клиент;

- на основе информации, переданной 2-ым компьютером-клиентом о множестве сетей, с которыми связан 2-ой компьютер-клиент, находят путь для пакета, причем этот путь определяет предпочтительный маршрут, который проходит через центральный концентратор от 1-го компьютера-клиента ко 2-му компьютеру-клиенту;

- отправляют перенаправленное сообщение к 1-му компьютеру-клиенту, причем перенаправленное сообщение отправляет пакет по найденному пути;

причем нахождение пути включает:

- нахождение множества маршрутов, проходящих от 1-го компьютера-клиента ко 2-му компьютеру-клиенту;

- выбор предпочтительного маршрута из множества маршрутов, причем предпочтительный маршрут является оптимальным путем от 1-го компьютера-клиента ко 2-му компьютеру-клиенту и определяется из информации, сохраняемой в центральном концентраторе, а информация связана с 1-ым компьютером-клиентом и 2-ым компьютером-клиентом;

причем отправка перенаправленного сообщения включает:

- определение соединения, через которое центральный концентратор получил пакет от 1-го компьютера-клиента;

- определение адреса источника, связанного с пакетом;

- передача в адрес источника, через определенное соединение, перенаправленного сообщения,

- перенаправление пакета по предпочтительному маршруту.

Способ также может включать создание для найденного пути туннеля, который обеспечивается в составе центрального концентратора.

В известном способе не требуется, чтобы в концентратор каждой подсети передавались сведения обо всех маршрутах (диапазоны IP-адресов, подлежащие защите), но необходимо, чтобы концентраторы всех подсетей использовали центральный концентратор в качестве маршрута по умолчанию.

Необходимость использования центрального концентратора в качестве маршрута по умолчанию является недостатком известного способа. Это создает повышенную избыточную нагрузку на центральный концентратор и на сеть в целом, особенно при шифровании канала между концентраторами.

Описанный способ принимается за прототип.

Известный способ относится к большим сетям, в общем случае, включающим множество подсетей. Вместе с тем, довольно часто встречается более простая схема работы сетевого узла, оказывающего различные услуги пользователям и использующего прикладные приложения.

Обычно в такой схеме используется центральный сервер, на котором установлено прикладное приложение (прикладной сервер), а компьютеры-клиенты взаимодействуют с прикладным сервером, посылая запросы и получая ответы, с использованием определенного прикладного протокола, причем типичной потребностью является формирование защищенных соединений непосредственно между компьютерами-клиентами, без использования прикладного сервера.

В качестве характерного примера можно привести работу прикладного сервера, обеспечивающего телефонную цифровую связь между абонентами, подключенными к сети передачи данных, например, внутри одной компании. Обеспечение соединения здесь возможно между абонентами через центральный сервер, но более предпочтительно устанавливать соединение непосредственно между абонентами.

Предлагаемый способ предназначен для использования именно в такой, более простой схеме. При этом, в отличие от прототипа, оптимизировать путь между компьютерами-клиентами, в общем случае, нет необходимости.

Раскрытие изобретения

Техническим результатом является снижение нагрузки сети в целом, прикладного и туннелирующего серверов.

Основная идея заключается в том, чтобы при начале сетевого обмена через прикладной протокол формировать защищенный канал связи.

Для этого предлагается способ формирования защищенного соединения в сетевой компьютерной системе,

причем система включает

- прикладной сервер, осуществляющий прием и обработку запросов по прикладному протоколу от компьютеров-клиентов по сети через туннелирующий сервер,

- туннелирующий сервер, обеспечивающий защищенное соединение для компьютеров-клиентов с прикладным сервером,

- компьютеры-клиенты, выполненные с возможностью осуществлять взаимодействие между собой и с прикладным сервером по прикладному протоколу,

способ заключается в том, что

- посылают запрос из 1-го компьютера-клиента в прикладной сервер для

осуществления взаимодействия со 2-м компьютером-клиентом;

- получают запрос от 1-го компьютера-клиента в прикладном сервере;

- посылают ответ на запрос из прикладного сервера 1-му компьютеру-клиенту, в котором содержится сетевой адрес 2-го компьютера-клиента;

- анализируют в туннелирующем сервере ответ из прикладного сервера 1-му компьютеру-клиенту;

- если в ответе присутствует сетевой адрес 2-го компьютера-клиента, то передают из туннелирующего сервера 1-му компьютеру-клиенту вместе с сообщением прикладного протокола информацию, необходимую для установки защищенного соединения со 2-м компьютером-клиентом;

- получают в 1-м компьютере-клиенте ответ на запрос из туннелирующего сервера, включающий сообщение прикладного протокола и информацию для установки защищенного соединения со 2-м компьютером-клиентом;

- формируют защищенное соединение между 1-м компьютером-клиентом и 2-м компьютером-клиентом.

Способ предполагает наличие прикладного сервера, например это может быть служба имен, сервер IP-телефонии или сервер видеоконференций.

Доступ к прикладному серверу осуществляется через туннелирующий сервер. Туннелирующий сервер осуществляет пересылку сетевых пакетов между прикладным сервером и компьютерами-клиентами в защищенном виде.

Компьютер-клиент - это потребитель услуг прикладного сервера. Компьютер-клиент подключается к прикладному серверу через туннелирующий сервер, причем сетевой обмен между компьютером-клиентом и прикладным сервером на участке от клиента до туннелирующего сервера осуществляется в защищенном формате, прозрачно для прикладного протокола (фиг. 1).

Защищенный канал между клиентом и туннелирующим сервером, например, можно построить с помощью IPsec.

Способ позволяет инициировать защищенный канал между клиентами в момент, когда инициируется прямое взаимодействие по прикладному протоколу. Примерами могут служить IP-телефония или видеоконференции: в момент совершения звонка они взаимодействуют с сервером прикладного протокола, далее взаимодействие идет напрямую между клиентами.

При инициировании соединения и посылке запроса из 1-го компьютера-клиента в прикладной сервер, для последующего осуществления взаимодействия со 2-м компьютером-клиентом, в состав запроса 1-й компьютер-клиента включаются сведения о 2-м компьютере-клиенте, сетевой адрес которого предполагается получить. В качестве таких сведений, в зависимости от вида прикладных услуг, может быть использован, например, номер телефона, идентификатор (имя) абонента и др.

При получении запроса из 1-го компьютера-клиента прикладной сервер на основе сведений запроса и имеющейся у него информации обо всех компьютерах-клиентах определяет сетевой адрес 2-го компьютера-клиента и высылает ответ, содержащий сетевой адрес 2-го компьютера-клиента.

Далее, в отличие от прототипа, нет необходимости маршрутизировать весь трафик на туннелирующий сервер, достаточно, чтобы трафик до прикладного сервера всегда шел через туннелирующий сервер.

Краткое описание чертежей

На фиг. 1 показана общая схема сетевой компьютерной системы для реализации предложенного способа.

На фиг. 2 показана схема взаимодействия в сетевой компьютерной системе для реализации предложенного способа.

Осуществление изобретения

Рассмотрим пример реализации предложенного способа в сетевой компьютерной системе.

Наиболее общий случай предусматривает, что прикладной и туннелирующий серверы территориально расположены в одном месте, компьютеры-клиенты - в разных местах, а в качестве сети используется сеть Интернет.

Прикладной сервер, осуществляющий прием и обработку запросов по прикладному протоколу от компьютеров-клиентов по сети через туннелирующий сервер, представляет собой компьютер, на котором установлено общесистемное, серверное и прикладное программное обеспечение (ПО) и который связан через сетевой интерфейс с туннелирующим сервером. Прикладное ПО позволяет принимать и обрабатывать запросы от компьютеров-клиентов и, таким образом, оказывать услуги, например, видеоконференцсвязи.

Обычными предварительными условиями работы прикладного сервера является формирование внутренней базы данных, в которой после стандартной процедуры регистрации клиентов находится минимально необходимая информация о клиентах (как правило, это имя абонента, пароль доступа к услуге, данные об оплате услуги, актуальный сетевой адрес компьютера-клиента в момент входа в систему, тип протокола, факт соединений в текущий момент и пр.).

В качестве туннелирующего сервера также используется компьютер, на котором установлено общесистемное, серверное и прикладное ПО и который связан через сетевой интерфейс с прикладным сервером и сетью Интернет. Прикладное ПО туннелирующего сервера позволяет принимать и обрабатывать запросы от прикладного сервера и компьютеров-клиентов и обеспечивать защищенное соединение (туннель) между заданными адресами в сети.

Каждый компьютер-клиент представляет собой компьютер, на котором установлено общесистемное и прикладное ПО и который связан через сетевой интерфейс с сетью Интернет. Прикладное ПО компьютера-клиента позволяет посылать запросы прикладному серверу и принимать от него ответы, а также обеспечивать реализацию прикладных услуг пользователям и устанавливать защищенные соединения с другими компьютерами-клиентами.

При реализации предложенного способа, из 1-го компьютера-клиента, заранее зарегистрированного в прикладном сервере, начавшего активную сессию и предполагающего установить защищенное соединение со 2-м компьютером-клиентом, посылают запрос в прикладной сервер для осуществления взаимодействия со 2-м компьютером-клиентом, причем запрос содержит сведения о 2-м компьютере-клиенте (например, имя абонента, использующего 2-й компьютер-клиент в системе).

В прикладном сервере получают запрос от 1-го компьютера-клиента, выделяют в запросе имя абонента, определяют, что искомое имя зарегистрировано в базе данных прикладного сервера, причем в данный момент компьютер-клиент с таким именем также начал активную сессию и имеет определенный сетевой адрес, и посылают 1-му компьютеру-клиенту ответ на запрос из прикладного сервера, в котором содержится актуальный в данный момент сетевой адрес 2-го компьютера-клиента.

Ответ на запрос из прикладного сервера проходит через туннелирующий сервер, в котором анализируется ответ из прикладного сервера 1-му компьютеру-клиенту. Анализ состоит в определении факта ответа на запрос 1-му компьютеру-клиенту и наличии

сетевого адреса 2-го компьютера-клиента.

Если в ответе присутствует сетевой адрес 2-го компьютера-клиента, то передают из туннелирующего сервера 1-му компьютеру-клиенту вместе с сообщением прикладного протокола информацию, необходимую для установки защищенного соединения со 2-м компьютером-клиентом.

Затем получают в 1-м компьютере-клиенте ответ на запрос из туннелирующего сервера, включающий сообщение прикладного протокола и информацию, необходимую для установки защищенного соединения со 2-м компьютером-клиентом.

После этого формируют защищенное соединение между 1-м компьютером-клиентом и 2-м компьютером-клиентом с помощью прикладного ПО двух компьютеров-клиентов.

Далее весь трафик защищенного соединения между двумя компьютерами-клиентами идет напрямую между двумя сетевыми адресами, и ресурсы прикладного и туннелирующего сервера не используются, что снижает нагрузку на сеть в целом, на прикладной и туннелирующий серверы.

Все действия способа выполняются в автоматическом режиме с помощью соответствующего прикладного ПО, которое на основе знания содержания выполняемых действий и особенностей известных прикладных протоколов может быть разработано специалистом по программированию (программистом) и установлено на компьютерах системы.

Источники информации

1. RFC 4302 - Идентификационный заголовок IP, 2005, материал по адресу http://rfc2.ru/4302.rfc

2. RFC 4303 - Инкапсуляция защищенных данных IP (ESP), материал по адресу http://rfc2.ru/4303.rfc

3. Патент США №8499095, приоритет от 25.05.2006 г.

Формула изобретения

Способ формирования защищенного соединения в сетевой компьютерной системе, причем система включает

прикладной сервер, осуществляющий прием и обработку запросов по прикладному протоколу от компьютеров-клиентов по сети через туннелирующий сервер,

туннелирующий сервер, обеспечивающий защищенное соединение для компьютеров-клиентов с прикладным сервером,

компьютеры-клиенты, выполненные с возможностью осуществлять взаимодействие между собой и с прикладным сервером по прикладному протоколу,

способ, заключающийся в том, что:

посылают запрос из первого компьютера-клиента в прикладной сервер для осуществления взаимодействия со вторым компьютером-клиентом;

получают запрос от первого компьютера-клиента в прикладном сервере;

посылают ответ на запрос из прикладного сервера первому компьютеру-клиенту, в котором содержится сетевой адрес второго компьютера-клиента;

анализируют в туннелирующем сервере ответ из прикладного сервера первому компьютеру-клиенту;

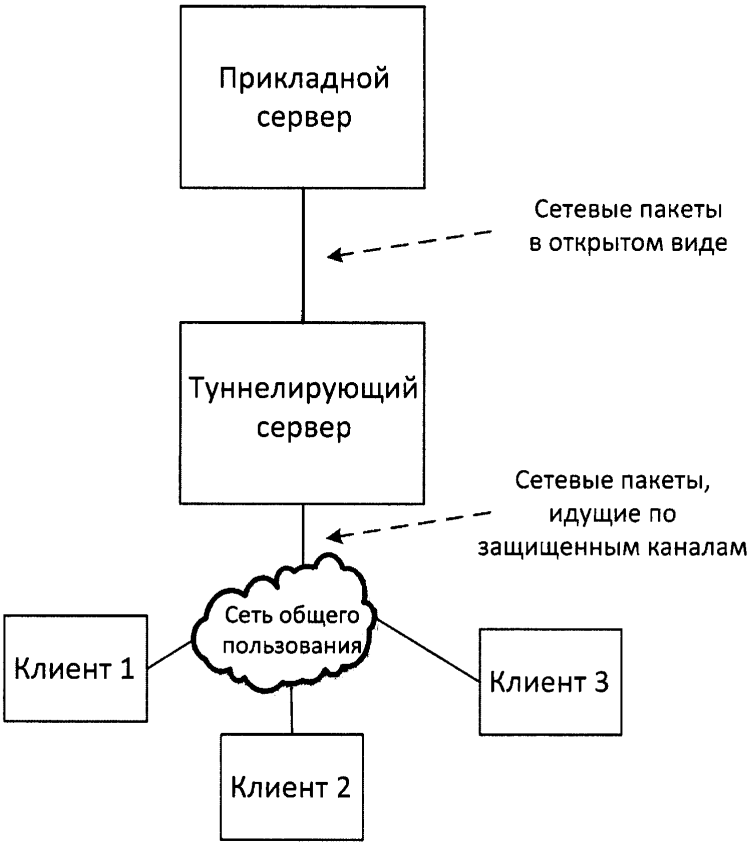
если в ответе присутствует сетевой адрес второго компьютера-клиента, то передают из туннелирующего сервера первому компьютеру-клиенту вместе с сообщением прикладного протокола информацию, необходимую для установки защищенного соединения со вторым компьютером-клиентом;

получают в первом компьютере-клиенте ответ на запрос из туннелирующего сервера,

включающий сообщение прикладного протокола и информацию, необходимую для установки защищенного соединения со вторым компьютером-клиентом;

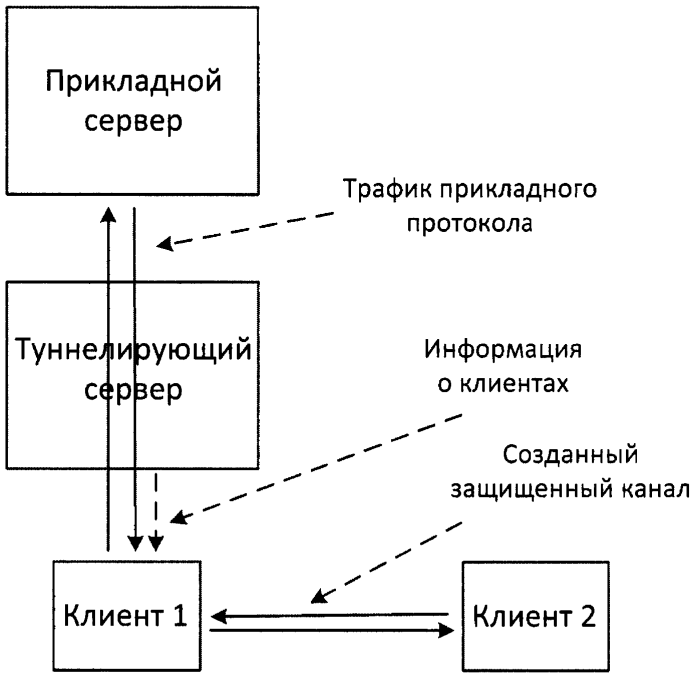
формируют защищенное соединение между первым компьютером-клиентом и вторым компьютером-клиентом.

Способ формирования защищенного соединения в сетевой компьютерной системе



Фиг. 1

Способ формирования защищенного соединения в сетевой компьютерной системе



Фиг. 2