РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 712 815**(13) **C1**

(51) МПК
H04L 29/06 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 29/00 (2019.08); H04L 29/06 (2019.08)

(21)(22) Заявка: **2018132057, 06.06.2016**

(24) Дата начала отсчета срока действия патента:
06.06.2016

Дата регистрации:
31.01.2020

Приоритет(ы):
(30) Конвенционный приоритет:
08.02.2016 US 62/292,702;
25.02.2016 US 15/053,422

(45) Опубликовано: **31.01.2020** Бюл. № **4**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **10.09.2018**

(86) Заявка PCT:
US 2016/036053 (06.06.2016)

(87) Публикация заявки PCT:
WO 2017/138975 (17.08.2017)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
ГЛЭЙЗМЭЙКЕРС Курт (BE),
АЛЛАНССОН Пер Йохан (SE),
СЕЛЛЕРЬЕ Тома Брюно Эмманюэль (SE),
ВАЛИАНОС Космас (SE),
ВЕБЕР Том Вилью (SE)

(73) Патентообладатель(и):
КРИПТЗОУН НОРТ АМЕРИКА, ИНК. (US)

(56) Список документов, цитированных в отчете о поиске: **US 2015/0293756 A1, 15.10.2015. US 2002/0091859 A1, 11.07.2002. RU 2289886 C2, 27.10.2005. RU 2010142387 A, 27.04.2012.**

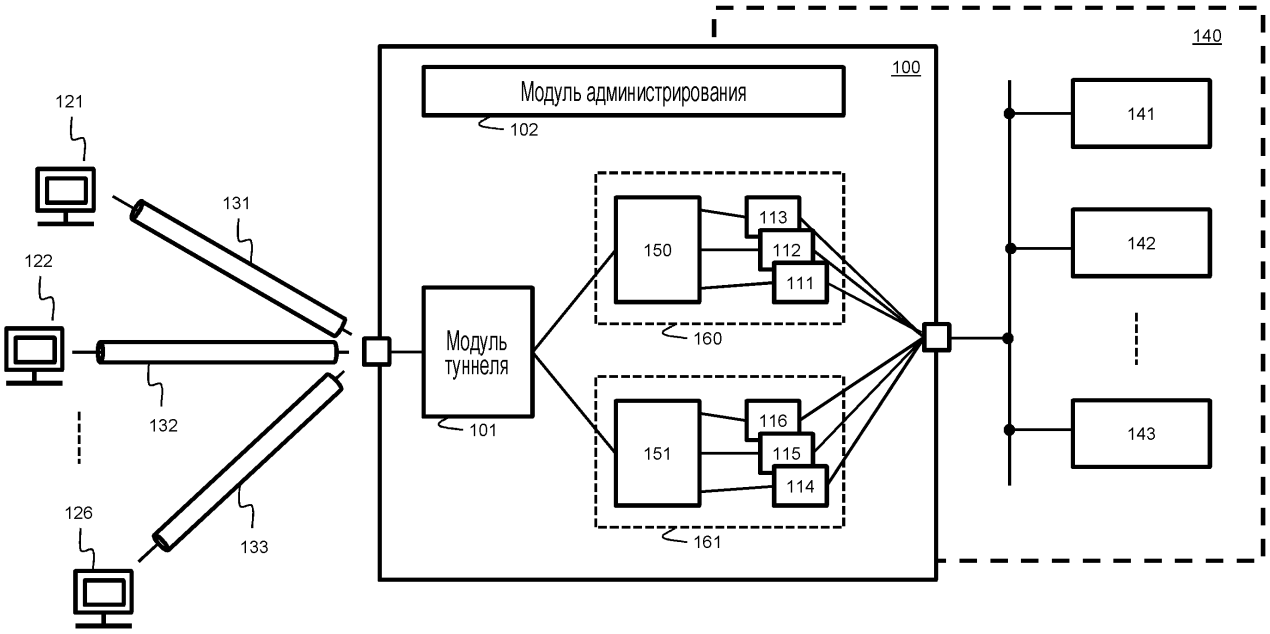
(54) ЗАЩИТА СЕТЕВЫХ УСТРОЙСТВ ПОСРЕДСТВОМ МЕЖСЕТЕВОГО ЭКРАНА

(57) Реферат:

Изобретение относится к области вычислительной техники. Технический результат заключается в обеспечении эффективных масштабируемости и администрировании шлюза. Способ содержит этапы, на которых: создают посредством первой компьютерной системы, реализующей первый шлюз к частной сети, первый сетевой туннель между клиентским устройством и первым шлюзом; принимают список доступа клиента, указывающий те сетевые устройства в частной сети, которым разрешено осуществлять связь с клиентским устройством; и запускают для первого сетевого туннеля отдельную службу межсетевого экрана с отдельным набором правил межсетевого экрана на первой компьютерной системе для выборочной блокировки и разрешения сетевого трафика между клиентским устройством и одним или более сетевыми устройствами в частной сети. 3 н. и 17 з.п. ф-лы, 8 ил.

RU 2712815 C1

RU 2712815 C1



ФИГ. 1

RU 2712815 C1

RU 2712815 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 712 815**(13) **C1**

(51) Int. Cl.
H04L 29/06 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 29/00 (2019.08); H04L 29/06 (2019.08)

(21)(22) Application: **2018132057, 06.06.2016**

(24) Effective date for property rights:
06.06.2016

Registration date:
31.01.2020

Priority:
(30) Convention priority:
08.02.2016 US 62/292,702;
25.02.2016 US 15/053,422

(45) Date of publication: **31.01.2020** Bull. № **4**

(85) Commencement of national phase: **10.09.2018**

(86) PCT application:
US 2016/036053 (06.06.2016)

(87) PCT publication:
WO 2017/138975 (17.08.2017)

Mail address:
129090, Moskva, ul. B.Spasskaya, 25, stroenie 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
GLAZEMAKERS Kurt (BE),
ALLANSSON Per Johan (SE),
CELLERIER Thomas Bruno Emmanuel (SE),
VALIANOS Kosmas (SE),
WEBER Tom Viljo (SE)

(73) Proprietor(s):
CRYPTZONE NORTH AMERICA, INC. (US)

RU 2712815 C1

(54) PROTECTION OF NETWORK DEVICES BY MEANS OF FIREWALL

(57) Abstract:

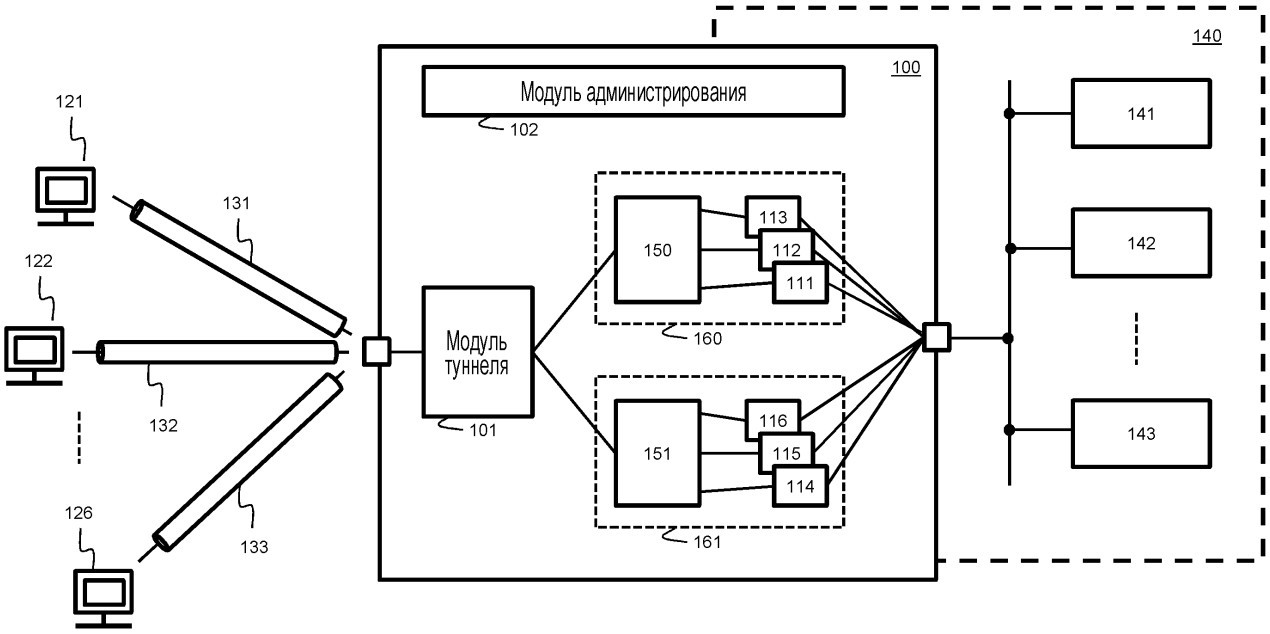
FIELD: calculating; counting.

SUBSTANCE: invention relates to computer engineering. Method comprises steps of: creating, by a first computer system implementing a first gateway to a private network, a first network tunnel between a client device and a first gateway; receiving a client access list indicating those network devices in the private network, which are allowed to communicate with the client device; and starting a separate firewall service for the first network tunnel with a separate set of firewall rules on the first computer system for selectively locking and allowing network traffic between the client device and one or more network devices in the private network.

EFFECT: technical result consists in provision of effective scalability and administration of gateway.

20 cl, 8 dwg

RU 2712815 C1



ФИГ. 1

RU 2712815 C1

RU 2712815 C1

Родственные заявки

[0001] По данной заявке испрашивается преимущество и приоритет Патентной Заявки США Серийный № 15/053,422, поданной 24 марта 2016 г. и Предварительной Заявки США Серийный № 62/292,702, поданной 08 февраля 2016 г., автор Glazemakers и др., которые во всей своей полноте включены в настоящее описание посредством ссылки.

Область техники, к которой относится изобретение

[0002] По меньше мере некоторые варианты осуществления в целом относятся к области защиты сети и, в частности, но не ограничиваются, защите частных сетей посредством шлюза, включающего в себя туннельный сервер, такой как VPN сервер и межсетевой экран (брандмауэр).

Предпосылки создания изобретения

[0003] Для того чтобы защищать частные сети от нежелательного сетевого доступа, межсетевой экран может быть реализован в шлюзе для того, чтобы выборочно фильтровать связь от и к частной сети. Посредством применения правил межсетевого экрана, межсетевой экран тогда разрешает сетевым пакетам проходить, либо блокирует их в одном или обоих направлениях. Правила, обычно, определяются посредством адресов источника и/или назначения у сетевых пакетов, или портов источника и/или назначения у сетевых пакетов.

[0004] Межсетевой экран может дополнительно выполнять инспектирование пакета с учетом состояния, тем самым отслеживая состояние сетевых соединений таких как, например, сетевые соединения TCP или UPD. Таким образом, возможно более детализированное управление, когда правила становятся зависимыми от сетевого соединения и, следовательно, динамическими. Межсетевой экран отслеживает все открытые сетевые соединения посредством ведения таблицы, таблицы состояния или списка состояния, со всеми отложенными соединениями.

[0005] Для того, чтобы иметь более хорошее управление над сетевым трафиком, проходящим через шлюз, межсетевой экран может дополнительно выполнять глубокое инспектирование пакета посредством управления данными полезной нагрузки сетевых пакетов. Таким образом, могут быть реализованы разные типы управления, такие как, например, доступ пользователя или авторизация, соответствие протоколу, фильтрация спама и обнаружение вируса.

[0006] Для того чтобы дополнительно защитить частную сеть, межсетевой экран шлюза может быть объединен с сетевым туннелированием. Доступ к частной сети может тогда создаваться посредством VPN (Виртуальная Частная Сеть), где защищенный сетевой туннель настраивается между клиентским устройством и шлюзом. Настройка такого туннеля разрешается только после успешной аутентификации с шлюзом, который затем функционирует в качестве VPN сервера. Посредством сочетания межсетевого экрана и VPN сервера в шлюзе, доступ к устройствам в частной сети может быть авторизованным на уровне клиента или пользователя посредством VPN сервера и на сетевом уровне посредством межсетевого экрана.

Сущность изобретения

[0007] Ряд проблем может возникнуть с объединенными системами шлюза как описано выше. Во-первых, количество правил межсетевого экрана будет расти с каждым дополнительным пользователем, делая администрирование всех правил сложным для больших систем. Из-за этого, каждый входящий пакет потребуется обрабатывать в отношении всех этих правил.

[0008] Вторая проблема относится к обработке отказа шлюза. В одной схеме обработки отказа, именуемой пассивная обработка отказа, вся информация в шлюзе

(т.е., правила межсетевого экрана, список состояния и активные сетевые туннели) непрерывно синхронизируются со вторым избыточным шлюзом. Если происходит отказ первого шлюза, второй шлюз автоматически берет на себя функции первого шлюза. Благодаря синхронизации, никакие активные сетевые соединения не теряются во время обработки отказа.

[0009] В другой схеме обработки отказа, именуемой активной обработкой отказа, несколько шлюзов также синхронизируются друг с другом, но все являются активными в одно и то же время, так что может осуществляться балансирование нагрузки между шлюзами. Также, в данном случае, благодаря синхронизации, один шлюз может взять на себя все соединения от другого шлюза при отказе без потери сетевых соединений.

[0010] Проблемой двух схем является масштабируемость, так как система не может масштабироваться посредством лишь добавления новых шлюзов. Во-первых, полоса пропускания между шлюзами, требуемая для синхронизации, будет расти экспоненциально с количеством или числом шлюзов. Во-вторых, так как список состояния синхронизируется, размер списка состояния и правил межсетевого экрана для каждого шлюза также будет увеличиваться линейно при масштабировании. Из-за этого, требуемая полоса пропускания, мощность обработки и пространство памяти каждого шлюза будут расти при добавлении нового шлюза.

[0011] В данном документе описываются разнообразные варианты осуществления, которые смягчают вышеизложенные проблемы и предоставляют шлюз, в отношении которого может осуществляться масштабирование и администрирование простым и непосредственным образом. Некоторые варианты осуществления кратко излагаются в данном разделе.

[0012] Варианты осуществления настоящего раскрытия помогают защитить сетевые устройства от неавторизованного доступа. Среди прочих вещей, варианты осуществления раскрытия обеспечивают полный доступ к серверам приложений и другим сетевым устройствам, к которым клиент авторизован осуществлять доступ, при этом предотвращая всякий доступ (или даже знание) сетевых устройств, к которым клиент не авторизован осуществлять доступ.

[0013] Компьютерно-реализуемый способ в соответствии с одним вариантом осуществления настоящего раскрытия включает в себя этапы, на которых: по запросу от клиентского устройства, создают, посредством компьютерной системы, реализующей шлюз к частной сети, сетевой туннель между клиентским устройством и шлюзом; и, по созданию сетевого туннеля, запускают отдельную службу межсетевого экрана с отдельным набором правил межсетевого экрана на компьютерной системе для выборочной блокировки и разрешения сетевого трафика между клиентским устройством и одним или более сетевыми устройствами в частной сети.

[0014] Настоящее раскрытие включает в себя разнообразные способы, устройства (включая компьютерные системы), которые выполняют такие способы, и машиночитаемые носители информации, содержащие инструкции, которые, при их исполнении вычислительными системами, предписывают вычислительным системам выполнять такие способы.

[0015] Другие признаки будут очевидны из сопроводительных чертежей и из подробного описания, которое следует ниже.

Краткое описание чертежей

[0016] Варианты осуществления иллюстрируются в качестве примера, а не ограничения, на фигурах сопроводительных чертежей, на которых подобные ссылки указывают сходные элементы.

[0017] Фиг. 1 является примерной системой для защиты сетевых устройств от нежелательного сетевого доступа в соответствии с разнообразными аспектами настоящего раскрытия.

[0018] Фиг. 2 является примерным процессом для создания сетевого туннеля между клиентским устройством и частной сетью, который может быть исполнен компонентами настоящего раскрытия.

[0019] Фиг. 3 является примерным процессом для распределения служб межсетевого экрана среди разных ядер процессора вычислительной системы, реализующей шлюз в соответствии с одним вариантом осуществления.

[0020] Фиг. 4 является примерной системой для создания сетевого туннеля между клиентским устройством и частной сетью разделенными шлюзом, реализующим службу межсетевого экрана в соответствии с одним вариантом осуществления.

[0021] Фиг. 5 является примерным процессом для синхронизации межсетевого экрана, реализованного в шлюзе, который может быть исполнен компонентами настоящего раскрытия.

[0022] Фиг. 6 является примерной системой, включающей в себя множество шлюзов для защиты сетевых устройств от нежелательного сетевого доступа в соответствии с разнообразными аспектами настоящего раскрытия;

[0023] Фиг. 7 является примерным процессом для гладкого переноса службы межсетевого экрана от одного шлюза к другому шлюзу, исполняемым компонентами настоящего раскрытия.

[0024] Фиг. 8 иллюстрирует примерную вычислительную систему в соответствии с разнообразными аспектами настоящего раскрытия.

Подробное описание

[0025] Предмет изобретения теперь будет описан более полно далее со ссылкой на сопроводительные чертежи, которые формируют его часть, и которые показывают, в качестве иллюстрации, конкретные примерные варианты осуществления. Тем не менее, изобретение может быть воплощено в разнообразие разных форм и, вследствие этого, подразумевается, что охватываемый или заявленный объем изобретения не ограничивается какими-либо примерными вариантами осуществления, изложенными в данном документе; примерные варианты осуществления предоставлены лишь в качестве иллюстративных. Подобным образом, предполагается достаточно широкий объем заявленного или охватываемого изобретения. Среди прочего, например, изобретение может быть воплощено в качестве способов, устройств, компонентов или систем. Соответственно, варианты осуществления могут, например, принимать форму аппаратного обеспечения, программного обеспечения, встроенного программного обеспечения или любого их сочетания (отличного от программного обеспечения как такового). Нижеследующее подробное описание, вследствие этого, не следует понимать в ограничивающем смысле.

[0026] На сопроводительных чертежах некоторые признаки могут быть преувеличены, чтобы показать подробности конкретных компонентов (и любой размер, материал и сходные подробности, показанные на фигурах, подразумеваются в качестве иллюстративных, а не ограничивающих). Вследствие этого, особые структурные и функциональные подробности, раскрываемые в данном документе, не подразумеваются в качестве ограничивающих, а лишь в качестве представительной основы для обучения специалиста в соответствующей области техники, чтобы по-разному использовать раскрываемые варианты осуществления.

[0027] Ссылка в данном техническом описании на «один вариант осуществления»

или «вариант осуществления» означает, что конкретный признак, структура, или характеристика, описанная в связи с вариантом осуществления, включены в, по меньшей мере, один вариант осуществления раскрытия. Появления фразы «в одном варианте осуществления» в разных местах в техническом описании как не обязательно все относятся к одному и тому же варианту осуществления, так и не являются отдельными или альтернативными вариантами осуществления, взаимно исключающими другие варианты осуществления. Более того, описываются разнообразные признаки, которые могут демонстрироваться некоторыми вариантами осуществления, но не другими. Сходным образом, описываются разнообразные требования, которые могут быть требованиями применительно к некоторым вариантам осуществления, но не к другим вариантам осуществления.

[0028] Любое сочетание и/или подмножество элементов способов, изображенных в данном документе, может быть объединено друг с другом, выполняться выборочно или не выполняться на основании разнообразных условий, повторяться любое требуемое число раз, и реализовываться на практике в любой подходящей очередности и в связи с любой подходящей системой, устройством, и/или процессом. Способы, описываемые и изображенные в данном документе, могут быть реализованы любым подходящим образом, таким как посредством программного обеспечения, работающего на одной или более компьютерных системах. Программное обеспечение может содержать машиночитаемые инструкции, хранящиеся на вещественном машиночитаемом носителе информации (таком как память компьютерной системы) и может быть исполнено одним или более процессорами, чтобы выполнять способы разнообразных вариантов осуществления.

[0029] Фиг. 1 иллюстрирует примерную систему для защиты сетевых устройств от нежелательного сетевого доступа в соответствии с разнообразными аспектами настоящего раскрытия. В данном примере, три сетевых устройства (серверы 141, 142 и 143 приложений) являются частью частной сети 140. Доступ к серверам 141-143 получается изнутри частной сети 140 через частный сетевой адрес. В данном контексте, понятие «частный» относится к тому факту, что серверы 141-143 приложений не являются глобально маршрутизируемыми. Другими словами, адресация серверов 141-143 приложений не может быть осуществлена посредством их частных сетевых адресов извне частной сети 140.

[0030] Частная сеть 140 и другие компоненты на Фиг. 1 могут использовать любое число и тип протоколов связи, также именуемых Интернет Протоколом («IP»), или Протоколом Управления Передачей/Интернет Протоколом («TCP/IP»). Например, частная сеть 140 может иметь диапазон адресов, как установлено в RFC 1918 для Интернет Протокола Версии 4 или IPv4 и в RFC 4193 для Интернет Протокола Версии 6 или IPv6.

[0031] Сетевые устройства 141-143 могут соответствовать серверам приложений, которые предоставляют службы по сети 140 другим вычислительным устройствам. Любое число и тип серверов приложений и ассоциированных служб может быть использовано совместно с вариантами осуществления настоящего раскрытия, такие как почтовые серверы, файловые севреры, службы Администрирования Взаимосвязи с Потребителями или CRM, службы Планирования Бизнес-Ресурсов или ERP, и/или службы администрирования документов.

[0032] Соединение для передачи данных затем может быть создано с любым из серверов 141-143 приложений посредством открытия сокета связи с соответствующим сервером приложений по порту (или диапазону портов), ассоциированному со службой.

Серверы 141-143 приложений могут соответствовать физическим устройствам с физическим сетевым интерфейсом, ассоциированным с адресом частной сети. В качестве альтернативы, серверы 141-143 приложений также могут соответствовать экземплярам виртуального сервера, работающего на одном или более физических серверах. Экземпляры виртуального сервера каждый может иметь виртуальный сетевой интерфейс с ассоциированным адресом частной сети. Экземпляры виртуального сервера могут включать в себя, как впрочем и работать совместно с, одним или более экземплярами пространства пользователя (также известными как контейнеры программного обеспечения, виртуальные машины, виртуальные частные серверы, и/или тюрьмы (jail)). Такие экземпляры пространства пользователя могут быть реализованы любым подходящим образом, включая, например, через инструмент программного обеспечения DOCKER.

[0033] В примере, показанном на Фиг. 1, частная сеть 140 отделена от внешней сети шлюзом 100, тем самым обеспечивая прохождение сетевого трафика между внешней сетью и частной сетью 140 управляемым образом. Система Фиг. 1 может идентифицировать клиентов 121-126 в качестве «доверенных клиентов» с правами доступа к одному или более из серверов 141-143 приложений внутри частной сети 140 для того, чтобы использовать функционирующие на них службы. Клиенты 121-126 могут быть, или включать в себя, физическое аппаратное обеспечение и/или виртуальные компоненты. Например, клиент 121-126 может включать в себя виртуальную операционную систему, работающую на физическом устройстве, таком как мобильное устройство. Система также может предоставлять сетевой доступ к выбору серверов 141-143 приложений, к которым клиентам 121-126 обеспечена возможность доступа, и отклонять сетевой доступ к любому серверу приложений, к которому клиентам 121-126 не обеспечена возможность доступа.

[0034] Для того чтобы управлять доступом клиентов 121-126 к серверам 141-143 приложений, сетевые туннели 131-133 создаются между клиентами 121-126 и шлюзом 100. Таким образом, частная сеть 140 расширяется для клиентов 121-126. В некоторых вариантах осуществления, виртуальная частная сеть (или «VPN») создается через туннели 131-133. Таким образом, клиенту 121-126, несмотря на то, что физически он не находится в частной сети 140, предоставляется адрес частной сети в диапазоне частной сети 140, и может, следовательно, потенциально осуществлять доступ к всем серверам 141-143 приложений посредством их соответствующего адреса частной сети (предоставленный доступ является разрешенным, как обсуждается более подробно ниже).

[0035] Все исходные запросы сетевого соединения от клиентов 121-126 обрабатываются посредством модуля 101 туннеля, реализованного в шлюзе 100. В одном варианте осуществления, модуль 101 туннеля смотрит на исходное соединение (например, как правило первый пакет TLS, который прибывает) и затем определяет, осуществлять ли передачу обслуживания соединения модулю 102 администрирования (обсуждается ниже) в случае метаданных, или одной из служб 150, 151 туннеля (обсуждается ниже) в случае фактического трафика туннеля (т.е., данных) от клиентов. Как только осуществлена передача обслуживания соединения (например, это может быть выполнено посредством направления дескриптора файла в модуль 102 администрирования или к одному из модулей службы туннеля), модуль 101 туннеля более не задействован. Затем, соединение проходит непосредственно от клиента к модулю 102 администрирования, или к выбранной службе 150, 151 туннеля.

[0036] Исходный запрос сетевого соединения может быть запросом соединения в отношении создания нового туннеля посредством нового клиентского устройства или

новым запросом сетевого соединения внутри существующего туннеля. Данные, проходящие по соединениям в туннелях 131-133, могут быть дополнительно защищены посредством шифрования, как например в соответствии с Защитой Интернет Протокола (или «протоколом IPsec»), Защитой Транспортного Слоя (или «TLS») и/или Защитой Дейтаграмм Транспортного Слоя (или «DTLS»). В примере, модуль 101 туннеля работает в соответствии с TLS или SSL и настраивает сетевые соединения в качестве сетевых соединений TCP. Для этого, клиенты отправляют запрос на открытие порта или диапазона портов шлюзу 100, предпочтительно стандартного порта 443 для TLS/SSL зашифрованных соединений TCP.

[0037] Шлюз 100 дополнительно реализует службы 111-116 межсетевого экрана. Каждая соответствующая служба межсетевого экрана затем реализует межсетевой экран для выборочной блокировки и разрешения сетевого трафика между соответствующим клиентским устройством и сетевыми устройствами 141-143 в частной сети. Каждая служба межсетевого экрана также содержит набор правил межсетевого экрана, определяющих правила доступа для соответствующего клиентского устройства. Другими словами, шлюз 100 выполняет отдельный межсетевой экран для каждого соединенного клиента 121-126. Преимущество этого состоит в том, что размер правил межсетевого экрана у службы межсетевого экрана не растет с количеством соединенных клиентов. Таким образом, рост соединенных клиентов не приводит к потере производительности из-за роста количества правил межсетевого экрана, администрирование которых должно осуществляться одной службой межсетевого экрана.

[0038] Фиг. 2 показывает примерный процесс, который может быть исполнен компонентами настоящего раскрытия, включая шлюз 100 в соответствии с Фиг. 1. Посредством данного процесса, клиентское устройство 121-126 соединяется с частной сетью 140 через шлюз 100. В качестве примера, процесс будет описан со ссылкой на клиентское устройство 121. На первом этапе 201, модуль 101 туннеля принимает первый запрос соединения от клиентского сетевого устройства 121, чтобы создать первое сетевое соединение со шлюзом 100, например запрос защищенного сетевого соединения TCP, принимаемый по порту 443 шлюза. За этим, сетевое соединение создается на этапе 202, например, посредством трехходового квитирования в случае сетевого соединения TCP. Данное первое сетевое соединение используется, чтобы осуществлять обмен информацией управления между клиентом 121 и шлюзом 100, и, в частности, с модулем 102 администрирования, реализованным в шлюзе 100. Для того, чтобы знать, что соединение служит для целей управления, модуль туннеля может инспектировать первый пакет данных, обмен которым осуществляется через каждое вновь созданное сетевое соединение. Если пакет данных является пакетом данных управления, модуль 101 туннеля идентифицирует сетевое соединение в качестве соединения управления и будет перенаправлять все дальнейшие пакеты, принимаемые через данное соединение, модулю 102 администрирования. Пакте данных управления может, например, быть идентифицирован посредством инспектирования особого поля расширения TSL в заголовке пакета TLS.

[0039] На следующем этапе 203, модуль 102 администрирования принимает информацию туннеля от клиентского устройства 121 через первое сетевое соединение. Данная информация дополнительно именуется списком туннеля клиента. Данный список туннеля клиента включает в себя информацию для того, чтобы создать сетевой туннель 131 со шлюзом, такую как, например, информация аутентификации для аутентификации клиента шлюзом. После успешной аутентификации модулем 102

администрирования, процесс переходит к этапу 204.

[0040] На этапе 204, модуль 102 администрирования принимает список доступа клиента от клиента 121. Список доступа клиента содержит перечень сетевых устройств или приложений в частной сети 140, к которым клиентскому устройству обеспечена возможность доступа. Перечень может, например, содержать сетевой адрес, такой как сетевой адрес IPv4 или IPv6, идентифицирующий соответствующее сетевое устройство в частной сети 140. Также, может быть указан номер порта или диапазон номеров порта для того, чтобы ограничить доступ соответствующего сетевого устройства к одному или более конкретным приложениям. Перечень может также идентифицировать соответствующее сетевое устройство посредством его имени хоста или посредством полностью определенного имени домена (FQDN). Перечень также может идентифицировать соответствующее сетевое устройство опосредованно посредством указания дополнительной службы, откуда одно или более соответствующие сетевые устройства могут быть приняты. Такая служба может, например, быть Web-службами Amazon, которые допускают извлечение списка сетевых устройств с использованием AWS REST API, в соответствии с метаданными, назначенными виртуальным экземплярам в облаке Amazon.

[0041] Клиент 121 может дополнительно извлекать данный список доступа клиента и/или список туннеля из службы аутентификации, которая осуществляет администрирование доступа клиента к частной сети 140. Для того, чтобы избежать ситуации, в которой клиент компрометирует список доступа клиента и/или список туннеля, списки могут быть сделаны неизменяемыми (т.е., защищенными так, что изменение одного или обоих списков может быть обнаружено модулем 102 администрирования).

[0042] Разнообразные способы и системы для аутентификации клиента и предоставления списка клиента и туннеля дополнительно раскрываются в Патенте США № US 9,148,408 B1, который во всей своей полноте включен в настоящее описание посредством ссылки.

[0043] Затем, на этапе 205, модуль 101 туннеля создает второе сетевое соединение с клиентом 121 по запросу клиента 121. Поскольку это новое соединение, модуль 101 туннеля инспектирует первый пакет данных, принимаемый через данное второе соединение. Данное второе соединение используется для фактического сетевого туннеля 131, так как клиент 121 уже имеет созданное первое соединение для обмена информацией управления с шлюзом 100. Вследствие этого инспектируемый пакет данных идентифицируется как первый пакет для еще не созданного сетевого туннеля 131.

[0044] В частности, в одном варианте осуществления, два соединения требуются для каждого туннеля (131, 132, 133) (например, два соединения TCP в случае туннеля TLS). Одно соединение служит для выгрузки жетонов (метаданных), а другое соединение служит для фактического трафика туннеля. Туннель 131 создается только после этапа 207 (см. ниже), и является только разрешающим трафик после этапа 208 (см. ниже), так как межсетевой экран блокируется по умолчанию.

[0045] За этим, на этапе 206, модуль 101 туннеля пропускает второе сетевое соединение (соединение, которое отвечает за туннелирование трафика, исходящего от клиента 121) к службе 150 туннеля. Службы 150 и 151 туннеля обрабатывают траффик туннеля (131, 132, 133). Службы 150, 151 туннеля отвечают за дешифрование/шифрование трафика исходящего и идущего к соответствующему клиента (121, 122, …, 126), реализованного в шлюзе 100. Служба туннеля затем верифицирует с помощью модуля 102 администрирования, может ли быть создан сетевой туннель 131. На следующем этапе

207, служба 150 туннеля создает сетевой туннель 131 посредством запуска службы 111 межсетевого экрана. С этого момента, все данные, обмен которыми осуществляется через второе сетевое соединение и, следовательно, через сетевой туннель 131, проходят через службу 111 межсетевого экрана. Другими словами, данные полезной нагрузки из сетевого туннеля 131 переадресовываются в запущенную службу 111 межсетевого экрана. Данная служба 111 межсетевого экрана реализует межсетевой экран, который блокирует по умолчанию весь трафик между клиентом 121 и частной сетью 140. На следующем этапе 208, служба 111 межсетевого экрана применяет подходящие правила межсетевого экрана к сетевому экрану посредством извлечения правил межсетевого экрана из модуля 102 администрирования. Модуль 102 администрирования в свою очередь получает эти правила межсетевого экрана из списка доступа клиента.

[0046] В частности, в одном варианте осуществления, правила доступа являются в основном описательными правилами межсетевого экрана, и модуль 102 администрирования заполняет некоторые из этих описаний. Некоторые примеры являются следующими:

Разрешить трафик TCP к 1.1.1.1 порт 80 (отметим, что это правило доступа, которое является точным совпадением с правилом межсетевого экрана)

Разрешить трафик TCP к www.google.com порт 80 (отметим, что это правило доступа, которое требует перевода в несколько FW правил, таких как:

Разрешить трафик TCP к 173.194.71.103 порт 80

Разрешить трафик TCP к 173.194.71.105 порт 80

Разрешить трафик TCP к 173.194.71.99 порт 80

…)

Таким образом, одно правило доступа может, например, приводить к нескольким правилам межсетевого экрана. В некоторых случаях, правило доступа может быть вызовом к провайдеру IAAS, подобно web-службам AWS и допускать трафик TCP к, например, следующему: [все экземпляры, которые имеют финансы в их описании].

[0047] Посредством процесса в соответствии с Фиг. 2, сетевой туннель 131 между клиентским устройством 121 и шлюзом 100, таким образом, создается вместе с отдельным межсетевым экраном с отдельным набором правил межсетевого экрана для выборочной блокировки и разрешения сетевого трафика между клиентским устройством 121 и сетевыми устройствами 141-143 в частной сети 140. Данный процесс выполняется для каждого клиента 121-126, который соединяется с частной сетью 140, тем самым получая соответствующие службы 111-116 межсетевого экрана.

[0048] В соответствии с дополнительным вариантом осуществления, шлюз 100 реализуется в компьютерной системе, содержащей несколько ядер процессора. Модуль 102 администрирования, модуль 101 туннеля, служба 150 туннеля и службы 111, 112 и 113 межсетевого экрана тогда могут быть реализованы в компьютерной системе посредством машиноисполняемых инструкций, исполняемых в ядрах процессора. Шлюз 100 тогда включает в себя отдельную службу туннеля, работающую в каждом ядре процессора. Это иллюстрируется посредством примерного варианта осуществления Фиг. 1, где служба 150 туннеля и службы 111, 112 и 113 межсетевого экрана реализуются в первом ядре 160 процессора, а служба 151 туннеля и службы 114, 115 и 116 межсетевого экрана реализуются во втором ядре 161 процессора. Службы 150 и 151 туннеля могут, например, быть реализованы в качестве процессов программного обеспечения, работающих в соответствующих ядрах процессора. Службы межсетевого экрана могут быть реализованы в качестве потоков программного обеспечения, выполняемых соответствующим процессом программного обеспечения (т.е., соответствующими

службами туннеля).

[0049] Преимущество выполнения отдельных служб туннеля в каждом ядре процессора состоит в том, что меж-процессная связь между службами межсетевого экрана и связь между службой межсетевого экрана и службой туннеля ограничивается одним и тем же ядром. В результате, когда шлюз 100 масштабируется посредством добавления еще ядер процессора, будет отсутствовать потеря производительности из-за возросшей меж-процессной связи.

[0050] Фиг. 3 показывает примерный процесс, который может быть исполнен компонентами настоящего раскрытия, включая шлюз 100 в соответствии с Фиг. 1. Посредством процесса, клиентские соединения и, следовательно, сетевые туннели могут быть распределены по разным ядрам 160, 161. Процесс начинается после создания второго соединения на этапе 305, как изложено выше со ссылкой на этап 205 Фиг. 2. Процесс затем переходит к этапу 306, где модуль туннеля выбирает одну из служб 150, 151 туннеля, к которой он будет переадресовывать второе соединение. Это может быть выполнено несколькими путями. Например, модуль туннеля может распределять соединение круговым образом посредством переадресации соединения каждый раз следующему ядру процессора. В качестве альтернативы, он может переадресовывать соединение процессору, который имеет наибольшее число доступных ресурсов таких как, например, мощность обработки, память или любое их сочетание. Когда ядро процессора выбрано, модуль 101 туннеля переадресовывает второе соединение выбранной службе туннеля на этапе 307, как также изложено выше со ссылкой на этап 206 Фиг. 2.

[0051] Фиг. 4 иллюстрирует подробности примерной службы 411 межсетевого экрана, которая может быть реализована в шлюзе 100 в соответствии с настоящим раскрытием, например, в качестве службы с 111 по 116 межсетевого экрана Фиг. 1. Ради примерной иллюстрации, будет предполагаться, что служба 411 межсетевого экрана соответствует службе 111 межсетевого экрана, которая предоставляет сетевой туннель 131 между клиентом 121 и частной сетью 140. Когда служба 411 межсетевого экрана запускается, она содержит компонент 420 межсетевого экрана для выборочной блокировки и разрешения сетевого трафика между соответствующим клиентским устройством 121 и сетевыми устройствами 141-143 в частной сети 140. Правила, используемые межсетевым экраном 420, в соответствии с которыми трафик блокируется или разрешается, хранятся в правилах 421 межсетевого экрана. Эти правила могут, например, храниться в файле или базе данных, которая размещается в памяти вычислительной системы, реализующей шлюз 100.

[0052] Межсетевой экран 420 может быть межсетевым экраном с учетом состояния, выполненным с возможностью выполнения инспектирования пакета с учетом состояния, тем самым отслеживая состояние сетевых соединений, созданных через сетевой туннель 131 между клиентом 121 и сетевыми устройствами 141-143 в частной сети 140. Каждое такое соединение может относиться к сетевым соединениям TCP или UPD. Таким образом, возможно более детализированное управление, когда правила становятся зависимыми от сетевого соединения и, следовательно, являются динамическими. Межсетевой экран продолжает отслеживать все открытые сетевые соединения посредством ведения списка, списка 422 состояния, со всеми отложенными соединениями. Эти состояния, могут, например, быть сохранены в файле или базе данных, которая размещается в памяти вычислительной системы, реализующей шлюз 100.

[0053] Каждая служба 411 межсетевого экрана таким образом ведет отдельный список 422 состояния. Преимущество этого состоит в том, что размер списка состояния

у службы 411 межсетевого экрана не растет с количеством клиентов, соединенных с шлюзом 100. Таким образом, рост соединенных клиентов не приводит к потере производительности из-за увеличения количества состояний, администрирование которых должно осуществляться одной службой межсетевого экрана.

[0054] Служба 411 межсетевого экрана может дополнительно включать в себя компонент 423 шифрования и/или дешифрования для соответственно шифрования и дешифрования данных, переданных к или принятых от клиента 121. Шифрование и дешифрование может дополнительно быть выполнено в соответствии с Защитой Интернет Протокола (или «протоколом IPsec»), Защитой Транспортного Слоя (или «TLS») и/или Защитой Дейтаграмм Транспортного Слоя (или «DTLS»). Шифрование и дешифрование может дополнительно быть аппаратно-ускоренно посредством компонента аппаратного обеспечения в ядре процессора, в котором работает служба 411 межсетевого экрана.

[0055] Фиг. 5 является примерным процессом, который может быть исполнен посредством компонентов настоящего раскрытия, например, посредством службы 411 межсетевого экрана на Фиг. 4. Посредством данного процесса, резервное копирование службы межсетевого экрана выполняется так, что оно может быть использовано во время отказа компьютерной системы, и, следовательно, шлюза, на котором работает служба 411 межсетевого экрана. На этапе 501, межсетевой экран 420 разрешает создание сетевого соединения между клиентом 121 и сетевым устройством или сетевым приложением в частной сети 140. Данное сетевое соединение, таким образом, создается через уже созданный сетевой туннель 131. Для того, чтобы отслеживать трафик через данное новое соединение и, следовательно, разрешать трафику данного соединения через межсетевой экран 420, межсетевой экран регистрирует соединение с помощью списка 422 состояния межсетевого экрана на этапе 501. Затем, на этапе 502, межсетевой экран 420 копирует список 422 состояния и подписывает копию на этапе 503 секретным ключом подписи. Таким образом он может позже верифицировать то, что копия не была изменена неавторизованной стороной. На этапе 504, копия затем передается клиенту 121. Таким образом, список состояния и, следовательно, состояние межсетевого экрана 420 синхронизируется с клиентом 121. Поскольку список состояния подписан на этапе 502, модификации списка состояния могут быть обнаружены посредством проверки подписи.

[0056] Посредством процесса Фиг. 5, отдельное резервное копирование может быть выполнено для каждого межсетевого экрана в шлюзе 100. Это имеет ряд преимуществ. Прежде всего, это может быть выполнено быстро, поскольку только ограниченный набор состояний требуется передавать каждый раз. В результате, когда система масштабируется, время для синхронизации одной службы 411 межсетевого экрана не увеличивается. Во-вторых, это обеспечивает возможность организации обработки отказа, которая является масштабируемой, как будет продемонстрировано ниже.

[0057] Фиг. 6 иллюстрирует систему в соответствии с одним вариантом осуществления для защиты доступа к частной сети 140. Управление доступом осуществляется шлюзами 600, 601 и 602, соответствующими шлюзу 100 посредством также реализации модуля 101 туннеля (не показан), модуля 102 администрирования (не показан), и одной или более служб 150, 151 туннеля (не показаны), причем каждый реализует одну или более службы межсетевого экрана. Для ясности, только две службы 611A и 616A межсетевого экрана показаны в шлюзе 600.

[0058] Фиг. 7 показывает примерный процесс, который может быть исполнен компонентами Фиг. 6 в случае отказа одного из шлюзов 600-602 (в нижеследующем

примере, обсуждается отказ шлюза 600). На этапе 701 процесса, шлюз 600 создает первый сетевой туннель 631 с клиентским устройством 621 для того, чтобы предоставлять клиенту 621 доступ к сетевым устройствам 141-143 в частной сети. Посредством этого, служба 611A межсетевого экрана запускается, тем самым реализуя межсетевой экран с учетом состояния и дополнительно включая правила межсетевого экрана и список состояния. Этап 701 может, например, быть выполнен в соответствии с Фиг. 2.

[0059] После создания сетевого туннеля 631, служба 611A межсетевого экрана непрерывно синхронизирует список состояния с клиентом 621 посредством регулярной отправки копии или обновления 650 списка состояния клиентскому устройству 621. Например, состояние требуется синхронизировать только если меняется фактическое состояние. Таким образом, если клиент не открывает новых соединений с защищенными серверами, не будет происходить синхронизации состояния. Также, данная синхронизация является конфигурируемой и может выполняться, например, непрерывно, или, по меньшей мере, каждые 1-5 секунд, и т.д. При условии, что сетевой туннель существует 631, синхронизация является активной, как иллюстрируется циклом 703-702. Синхронизация списка состояния может дальше выполняться в соответствии с процессом, как иллюстрируется на Фиг. 5.

[0060] В целях примерного обсуждения, рассмотрим, что в некоторый момент времени, сетевой туннель 631 прерывается. В результате данного прерывания, процесс переходит к этапу 704. Прерывание сетевого туннеля 631 может быть вызвано несколькими факторами, такими как, например, отказ сетевого пути между клиентом 621 и шлюзом 600, или посредством отказа самого шлюза 600. Когда клиент обнаруживает отказ сетевого туннеля, он создает новый сетевой туннель 632 со вторым шлюзом 601, который также предоставляет доступ к частной сети 140. Это может, например, быть выполнено посредством процесса, иллюстрируемого Фиг. 2, посредством переадресации информации 653 аутентификации туннеля и списка 652 доступа клиента второму шлюзу 601.

[0061] В частности, в одном варианте осуществления, информация о всех доступных шлюзах (600, 601, 602) является частью списков туннеля, описанных выше. Данная информация может исходить от, например, центрального сервера аутентификации (контроллера), такого как описываемый в Патенте США № US 9,148,408 B1, который был включен в настоящее описание посредством ссылки выше. Данная информация является доступной в первое соединение (т.е., до того как первое соединение может отказать). Центральный сервер аутентификации просто берет другого кандидата из списка туннеля и создает соединение. Единственной исходной информацией, идущей из копии или обновления 650, является фактическое состояние соединения от службы межсетевого экрана, которая будет синхронизироваться, как только создается новый туннель.

[0062] После создания туннеля 632, служба 611B межсетевого экрана запускается в шлюзе 601 с идентичными правилами межсетевого экрана, как используемые в службе 611A межсетевого экрана, поскольку тот же самый список 652 доступа был использован модулем администрирования шлюза 601, чтобы извлечь правила межсетевого экрана.

[0063] После создания второго сетевого туннеля 632, клиент 621 также передает список 651 состояния шлюзу 601 на этапе 705 процесса. В одном варианте осуществления, копия или обновление 650 является источником списка 651 состояния. Соединения проходили в туннель 631 до обработки отказа. В течение активного соединения, состояние непрерывно синхронизировалось с клиентом 621, и также обновлялось, когда состояния обновлялись для службы 611A межсетевого экрана. Когда туннель

сбрасывается, новый туннель создается и последнее принятое состояние 651 синхронизируется со службой 611B межсетевого экрана.

[0064] Список 651 состояния может, например, быть переадресован модулю администрирования. Модуль администрирования проверяет, что список состояния не был изменен клиентом, и затем предоставляет список состояния службе 611B межсетевого экрана, которая использует его в качестве своего списка состояния для того, чтобы восстановить состояние межсетевого экрана на этапе 706. После восстановления состояния межсетевого экрана, клиент возобновляет, на этапе 707, свою связь с частной сетью 140, тем самым достигая непрерывной обработки отказа (т.е., без потери отложенных сетевых соединений, созданных через исходный сетевой туннель 631).

[0065] В качестве альтернативы, список состояния также может быть отправлен через сетевой туннель непосредственно службе 611B межсетевого экрана, при этом данная служба будет проверять то, что список состояния не был изменен. Данная проверка может быть выполнена посредством использования точно того же (совместно используемого) секретного ключа подписи между шлюзами. В одном варианте осуществления, так как состояния межсетевого экрана временно хранятся в памяти у клиента, существует потенциальная опасность неавторизованной фальсификации состояний. Для того чтобы избежать данной опасности, состояния подписываются секретным совместно используемым ключом между шлюзами. Таким образом, если состояния фальсифицированы, подпись нарушена и состояния не будут приняты.

[0066] Процесс Фиг. 7 имеет преимущество в том, что не требуется синхронизации правил межсетевого экрана и состояний между шлюзами 600 и 601. Вследствие этого, система может быть легко масштабирована посредством добавления шлюза (например, шлюза 602) не требуя полосы пропускания между шлюзами (отметим, что не существует требования в отношении использования какой-либо полосы пропускания между шлюзами). Кроме того, после отказа шлюза 600, сетевые туннели могут быть перенесены по шлюзам 601 и 602. Например, служба 616A межсетевого экрана может быть перемещена в шлюз 602 в качестве службы 616B, в то время как межсетевой экран 616A переносится в шлюз 601 в качестве службы 611B.

[0067] Фиг. 8 показывает подходящую примерную вычислительную систему 800 для реализации шлюза в соответствии с упомянутыми ранее вариантами осуществления. Вычислительная система 800 может в целом быть сформирована в качестве подходящего компьютера общего назначения и содержит шину 810, одно или более ядра 802 процессора, локальную память 804, один или боле опциональные интерфейсы 814 ввода, один или более опциональные интерфейсы 815 вывода, один или более интерфейсы 812 связи, интерфейс 806 элемента хранения и один или более элементы 808 хранения. Шина 810 может содержать один или более проводники, которые разрешают связь между компонентами вычислительной системы 800. Ядра 802 процессора могут включать в себя любой тип обычного процессора или микропроцессора, который интерпретирует и исполняет инструкции программирования. Локальная память 804 может включать в себя память с произвольным доступом (RAM) или другой тип динамического запоминающего устройства, которое хранит информацию и инструкции для исполнения ядрами 802 процессора, и/или постоянную память (ROM) или другой тип статического запоминающего устройства, который хранит статическую информацию и инструкции для использования процессором 802. Интерфейс 814 ввода может содержать один или более обычные механизмы, которые разрешают оператору вводить информацию в вычислительное устройство 800, такие как клавиатура 820, мышь 830, перо, механизмы

распознавания голоса и/или биометрические механизмы, и т.д. Интерфейс 816 вывода может содержать один или более обычные механизмы, которые выводят информацию оператору, такие как дисплей 840. Интерфейс 812 связи может содержать любой подобный приемопередатчику механизм, такой как, например, один или более интерфейсы Ethernet, которые позволяют вычислительной системе 800 осуществлять связь с другими устройствами и/или системами 801. Интерфейс 812 связи вычислительной системы 800 может быть соединен с такой другой вычислительной системой посредством локальной сети (LAN) или глобальной сети (WAN), такой как, например, Интернет. Интерфейс 806 элемента хранения может содержать интерфейс хранения, такой как, например, интерфейс Последовательной Усовершенствованной Технологии Прикрепления (SATA) или Интерфейс Малых Вычислительных Систем (SCSI) для соединения шины 810 с одним или более элементами 808 хранения, таким как один или более локальные диски, например, накопители на диске SATA, и управлять чтением и записью данных на и/или с этих элементов 808 хранения. Несмотря на то, что элементы 808 хранения выше описываются в качестве, например, локального диска, в целом, могут быть использованы любые другие подходящие машиночитаемые носители информации, такие как съемный магнитный диск, оптические запоминающие носители информации, такие как CD-ROM или DVD-ROM диски, твердотельные накопители, карты флэш-памяти, и т.д. Система 800 описанная выше может также выполняться в качестве виртуальной машины поверх физического аппаратного обеспечения.

[0068] Этапы, выполняемые в соответствии с вышеизложенными процессами могут быть реализованы в качестве машиноисполняемых инструкций. Эти инструкции затем могут быть исполнены ядрами 802 процессора по выполнению процесса. Таким образом, этапы, исполняемые модулем 101 туннеля, модулем 102 администрирования, службами 150, 151 туннеля и службами 111-116 межсетевого экрана могут, например, быть реализованы в качестве инструкций в вычислительной системе 800, тем самым реализуя шлюз 100. Ядра 802 процессора могут соответствовать ядрам 160, 161 процессора у шлюза 100. Служба 150, 151 туннеля тогда выполняется в каждом ядре 802 процессора. Каждое ядро 802 процессора тогда выполняет отдельные службы межсетевого экрана соответственно запускаемые одной из служб туннеля. Связь для передачи пакетов данных между клиентскими устройствами 121-126 и шлюзом 100 может быть выполнена через сетевой интерфейс 812. Также, обмен пакетами данных, которые сообщаются между шлюзом 100 и частной сетью 140, может быть осуществлен через сетевой интерфейс 812. Машиноисполняемые инструкции могут формировать или быть частью компьютерного программного продукта, который хранится на запоминающем элементе 808 или любом машиночитаемом запоминающем носителе информации.

[0069] Связь между системами, устройствами, и компонентами, работающими в связи с вариантами осуществления настоящего раскрытия, может быть выполнена с использованием любого подходящего способа связи, такой как, например, телефонная сеть, экстрасеть, интрасеть, Интернет, устройство точки взаимодействия (устройство точки продажи, персональный цифровой помощник (например, iPhone®, Palm Pilot®, Blackberry®), сотовый телефон, киоск, и т.д.), онлайновую связь, спутниковую связь, связь автономного режима, беспроводную связь, связь ретранслятора, локальную сеть (LAN), глобальную сеть (WAN), виртуальную частную сеть (VPN), объединенные в сеть или связанные устройства, клавиатура, мышь и/или любая подходящая связь или модальность ввода данных. Системы и устройства настоящего раскрытия могут использовать протоколы связи TCP/IP, как впрочем и IPX, Appletalk, IP-6, NetBIOS, OSI, любой протокол туннелирования (например, IPsec, SSH), или любое число существующих

или будущих протоколов.

[0070] Несмотря на то, что некоторые варианты осуществления могут быть реализованы в полностью функционирующих компьютерах и компьютерных системах, разнообразные варианты осуществления выполнены с возможностью распространения в качестве вычислительного продукта в разнообразии форм и выполнены с возможностью применения независимо от конкретного типа машины или машиночитаемых носителей информации, используемых для фактического результата распространения.

[0071] Машиночитаемый носитель информации может быть использован, чтобы хранить программное обеспечение, и данные, которые при их исполнении системой обработки данных, предписывают системе выполнять разнообразные способы. Исполняемое программное обеспечение и данные могут храниться в разнообразных местах, включая, например, ROM, энергозависимую RAM, энергонезависимую память и/или кэш. Части данного программного обеспечения и/или данных могут храниться в любом из этих запоминающих устройств. Кроме того, данные и инструкции могут быть получены от централизованных серверов или одноранговых сетей. Разные части данных и инструкции могут быть получены от разных централизованных серверов и/или одноранговых сетей в разные времена и в разные сеансы связи или в одном и том же сеансе связи. Данные и инструкции могут быть получены полностью перед исполнением приложений. В качестве альтернативы, части данных и инструкций могут быть получены динамически, как раз во время, когда требуются для исполнения. Таким образом, не требуется, чтобы данные и инструкции были полностью на машиночитаемом носителе информации в конкретный экземпляр времени.

[0072] Примеры машиночитаемых носителей информации включают в себя, но не ограничиваются записываемый и не записываемый тип носителей информации, такие как энергозависимые и энергонезависимые устройства памяти, постоянная память (ROM), память с произвольным доступом (RAM), устройства флэш-памяти, флоппи и другие съемные диски, запоминающие носители информации на магнитном диске, оптические запоминающие носители информации (например, Постоянная Память на Компакт Диске (CD ROM), Цифровые Универсальные Диски (DVD) и т.д.), среди прочего. Машиночитаемые носители информации могут хранить инструкции.

[0073] В разнообразных вариантах осуществления, проводная схема может быть использована с инструкциями программного обеспечения, чтобы реализовывать методики. Таким образом, методики как не ограничены каким-либо конкретным сочетанием схемы аппаратного обеспечения и программного обеспечения, так и не каким-либо конкретным источником для инструкций, исполняемых системой обработки данных.

[0074] Несмотря на то, что некоторые из чертежей иллюстрируют некоторое число операций в конкретной очередности, операции, которые не являются зависимыми от очередности, могут быть переупорядочены и другие операции могут быть объединены или выведены. Несмотря на то, что в частности упомянуты некоторое переупорядочение или другие группирования, другие будут очевидны специалистам в соответствующей области техники и таким образом, не представляют исчерпывающий список альтернатив. Более того, следует признать, что стадии могут быть реализованы в аппаратном обеспечении, встроенном программном обеспечении, программном обеспечении или любом их сочетании.

[0075] Для краткости, обычные организации сетей для передачи данных, разработка приложений и другие функциональные аспекты систем (и компонентов у индивидуальных

рабочих компонентов систем) могут быть не описаны подробно в данном документе. Кроме того, соединяющие линии, показанные на разнообразных фигурах, которые содержатся в данном документе, предназначены для того, чтобы представлять примерные функциональные зависимости и/или физические связывания между разнообразными элементами. Следует отметить, что много альтернативных или дополнительных функциональных зависимостей или физических соединений может присутствовать в практической системе.

[0076] Разнообразные компоненты системы, которые обсуждаются в данном документе, могут включать в себя одно или более из следующего: хост-сервер или другие вычислительные системы, включающие в себя процессор для обработки цифровых данных; память, связанную с процессором, для хранения цифровых данных; цифровой преобразователь ввода, связанный с процессором, для ввода цифровых данных; прикладную программу, хранящуюся в памяти и доступную процессору для направления обработки цифровых данных процессором; устройство отображения, связанное с процессором и памятью, для отображения информации, полученной из цифровых данных, обработанных процессором; и множество баз данных. Разнообразные базы данных, используемые в данном документе, могут включать в себя: данные доставки, данные пакета, и/или данные, используемые при работе системы.

[0077] Разнообразная функциональность может быть выполнена через web-браузер и/или взаимодействие приложений с использованием web-браузера. Такие приложения браузера могут содержать программное обеспечение просмотра Интернет, инсталлированное в вычислительном блоке или системе, чтобы выполнять разнообразные функции. Эти вычислительные блоки или системы могут принимать форму компьютера или набора компьютеров, и может быть использован любой тип вычислительного устройства или систем, включая лэптопы, ноутбуки, планшеты, переносные компьютеры, персональные цифровые помощники, абонентские телевизионные приставки, рабочие станции, компьютерные серверы, компьютеры класса мэйнфрейм, мини компьютеры, PC серверы, сетевые наборы компьютеров, персональные компьютеры и планшетные компьютеры, такие как iPad, iMAC и MacBook, киоски, терминалы, устройства точки продажи (POS) и/или терминалы, телевизоры, или любое другое устройство, выполненное с возможностью приема данных через сеть. Разнообразные варианты осуществления могут использовать Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Apple Safari, Opera, или любой другой из мириады пакетов программного обеспечения, доступных для просмотра Интернет.

[0078] Разнообразные варианты осуществления могут работать в связи с любой подходящей операционной системой (например, Windows NT, 95/98/2000/CE/Mobile/, Windows 7/8, OS2, UNIX, Linux, Solaris, MacOS, PalmOS, и т.д.), как впрочем и разнообразными обычными поддерживающими драйверами или программным обеспечением, как правило, ассоциированными с компьютером. Разнообразные варианты осуществления могут включать в себя любой подходящий персональный компьютер, сетевой компьютер, рабочую станцию, персональный цифровой помощник, сотовый телефон, интеллектуальный телефон, миникомпьютер, мэйнфрейм или подобное. Варианты осуществления могут реализовывать протоколы защиты, такие как Слоя Защищенных Сокетов (SSL), Защиты Транспортного Слоя (TLS), и Безопасной Оболочки (SSH). Варианты осуществления могут реализовывать любой требуемый протокол прикладного слоя, включая http, https, ftp и sftp.

[0079] Разнообразные компоненты системы могут быть независимо, раздельно или сообща подходящим образом связаны с сетью через линии связи для передачи данных,

которые включают в себя, например, соединение с Поставщиком Служб Интернет (ISP) через местную линию связи, как обычно используется в соединении с помощью стандартной модемной связи, кабельного модема, сотовых сетей, ISDN, Цифровой Абонентской Линии (DSL), или разнообразных беспроводных способов связи. Отмечается, что варианты осуществления настоящего раскрытия могут работать совместно с любым подходящим типом сети, такой как сеть интерактивного телевидения (ITV).

[0080] Система может быть частично или полностью реализована используя облачные вычисления. «Облако» или «Облачные вычисления» включают в себя модель для обеспечения удобного, по запросу сетевого доступа к совместно используемому пулу конфигурируемых вычислительных ресурсов (например, сетей, серверов, хранилища, приложений и служб), которые могут быть быстро предоставлены и высвобождены с минимальными усилиями администрирования или взаимодействием с поставщиком службы. Облачные вычисления могут включать в себя независимые от местоположения вычисления, посредством чего совместно используемые серверы предоставляют ресурсы, программное обеспечение, и данные компьютерам и другим устройствам по запросу.

[0081] Разнообразные варианты осуществления могут быть использованы в связи с web-службами, коммунальными вычислениями, повсеместными и индивидуализированными вычислениями, решениями обеспечения безопасности и идентификационных данных, автономными вычислениями, облачными вычислениями, товарными вычислениями, решениями мобильности и беспроводными решениями, с открытыми источниками, биометрией, вычислениями типа «решетка» и/или вычислениями типа «сетка».

[0082] Любые базы данных, обсуждаемые в данном документе могут включать в себя реляционную, иерархическую, графическую, или объектно-ориентированную структуру и/или любые другие конфигурации базы данных. Более того, базы данных могут быть организованы любым подходящим образом, например, в качестве таблиц данных или поисковых таблиц. Каждая запись может быть одним файлом, рядом файлов, сцепленным рядом файлов данных или любой другой структурой данных. Ассоциация некоторых данных может быть осуществлена посредством любой требуемой методики ассоциации данных, такой как те, что известны или используются на практике в области техники. Например, ассоциация может быть осуществлена либо вручную, либо автоматически.

[0083] Любые базы данных, системы, устройства, серверы или другие компоненты системы могут быть расположены в одном местоположении, или в нескольких местоположениях, при этом каждая база данных или система включает в себя любые из разнообразных подходящих признаков защиты, таких как межсетевые экраны, коды доступа, шифрование, дешифрование, упаковка, распаковка, и/или подобное.

[0084] Шифрование может быть выполнено посредством любых методик, доступных в настоящее время в области техники, или которые могут стать доступными - например, Twofish, RSA, El Gamal, Schorr структуры, DSA, PGP, PKI, и симметричных и ассиметричных криптосистем.

[0085] Варианты осуществления могут соединяться с Интернет или интрасетью с использованием стандартного коммутируемого, кабельного, DSL или любого другого Интернет протокола, известного в области техники. Транзакции могут проходить через межсетевой экран для того, чтобы предотвращать неавторизованный доступ от пользователей других сетей.

[0086] Компьютеры, обсуждаемые в данном документе, могут предоставлять

подходящий web-сайт или другой основанный на Интернет графический интерфейс пользователя, который является доступным пользователям. Например, Microsoft Internet Information Server (IIS), Microsoft Transaction Server (MTS), и Microsoft SQL Server, могут быть использованы в связи с операционной системой Microsoft, программным обеспечением web-сервера Microsoft NT, системой базы данных Microsoft SQL Server, и Microsoft Commerce Server. Дополнительно, компоненты, такие как Access или Microsoft SQL Server, Oracle, Sybase, Informix MySQL, Interbase, и т.д., могут быть использованы, чтобы обеспечивать систему администрирования базы данных, совместимую с Объектом Данных ActivX (ADO). В другом примере, web-сервер Apache может быть использован в связи с операционной системой Linux, базой данных MySQL, и языками программирования Perl, PHP, и/или Python.

[0087] Любое из связи, вводов, хранилища, баз данных или отображений, обсуждаемых в данном документе, может обеспечиваться через web-сайт с web-страницами. Понятие «web-страница», используемое в данном документе, не предназначено для ограничения типа документов и приложений, которые возможно используются, чтобы взаимодействовать с пользователем. Например, типичный web-сайт может включать в себя, в дополнение к стандартным документам HTML, разнообразные формы, апплеты Java, JavaScript, активные серверные страницы (ASP), скрипты общего шлюзового интерфейса (CGI), расширяемый язык разметки (XML), динамический HTML, каскадные стилевые таблицы (CSS), AJAX (Асинхронный Javascript И XML), вспомогательные приложения, плагины, и подобное. Сервер может включать в себя web-службу, которая принимает запрос от web-сервера, причем запрос включает URL и IP-адрес. Web-сервер извлекает подходящие web-страницы и отправляет данные или приложения для web-страниц на IP адрес. Web-службы являются приложениями, которые выполнены с возможностью взаимодействия с другими приложениями через средства связи, такие как Интернет.

[0088] Разнообразные варианты осуществления могут использовать любое требуемое число способов для отображения данных внутри основанного на браузере документа. Например, данные могут быть представлены в качестве стандартного текста или внутри фиксированного списка, прокручиваемого списка, выпадающего списка, редактируемого текстового поля, фиксированного текстового поля, всплывающего окна, или подобного. Подобным образом, варианты осуществления могут использовать любое требуемое число способов для модификации данных на web-странице таких как, например, свободный ввод текста используя клавиатуру, выбор пункта меню, кнопки-флажки, кнопки выбора, и подобное.

[0089] Примерные системы и способы, иллюстрируемые в данном документе могут быть описаны исходя из функциональных блочных компонентов, снимков с экрана, опциональных выборов и разнообразных этапов обработки. Следует иметь в виду, что такие функциональные блоки могут быть реализованы посредством любого числа компонентов аппаратного обеспечения и/или программного обеспечения, выполненного с возможностью выполнения указанных функций. Например, система может использовать разнообразные компоненты интегральной микросхемы, например, элементы памяти, элементы обработки, логические элементы, поисковые таблицы, и подобное, которые могут выполнять разнообразные функции под управлением одного или более микропроцессоров или устройств управления. Сходным образом, элементы программного обеспечения системы могут быть реализованы с помощью любого языка программирования или написания сценариев, таких как C, C++, C#, Java, JavaScript, VBScript, Macromedia Cold Fusion, COBOL, Microsoft Active Server Pages, ассемблер, PERL,

PHP, AWK, Python, Visual Basic, SQL Stored Procedures, PL/SQL, любой скрипт оболочки UNIX, и расширяемый язык разметки (XML) с разнообразными алгоритмами, реализованными с помощью любого сочетания структур данных, объектов, процессов, подпрограмм или других элементов программирования. Кроме того, следует отметить, что система может использовать любое число обычных методик для передачи данных, сигнализации, обработки данных, сетевого управления, и подобного. Более того, система может быть использована, чтобы обнаруживать или предотвращать проблемы безопасности с помощью языка написания сценариев клиентской стороны, такого как JavaScript, VBScript или подобный.

[0090] Системы и способы настоящего раскрытия могут быть воплощены в качестве настройки существующей системы, продукта-дополнения, устройства обработки, исполняющего обновленное программное обеспечение, автономной системы, распределенной системы, способа, системы обработки данных, устройства для обработки данных, и/или компьютерного программного продукта. Соответственно, любая часть системы или модуля может принимать форму устройства обработки, исполняющего код, основанного на Интернет варианта осуществления, варианта осуществления полностью в аппаратном обеспечении, или варианта осуществления, объединяющего аспекты Интернета, программного обеспечения и аппаратного обеспечения. Кроме того, система может принимать форму компьютерного программного продукта на машиночитаемом запоминающем носителе информации со средством машиночитаемого кода программы, воплощенным в запоминающем носителе информации. Может быть использован любой подходящий машиночитаемый запоминающий носитель информации, включая жесткие диски, CD-ROM, оптические запоминающие устройства, магнитные запоминающие устройства, и/или подобное.

[0091] Система и способ, описываются в данном документе со ссылкой на снимки с экрана, структурные схемы и иллюстрации блок-схемы способов, устройства (например, систем), и компьютерных программных продуктов в соответствии разнообразными вариантами осуществления. Следует понимать, что каждый функциональны блок структурной схемы и иллюстраций блок-схемы, и сочетания функциональных блоков на структурных схемах и иллюстрациях блок-схемы, соответственно, могут быть реализованы посредством инструкций компьютерной программы.

[0092] Эти инструкции компьютерной программы могут быть загружены в компьютер общего назначения, компьютер специализированного назначения, или другое программируемое устройство обработки данных, чтобы создавать машину, так что инструкции, которые исполняются на компьютере или другом программируемом устройстве обработки данных, создают средство для реализации функций, указанных в блоке или блоках блок-схемы. Эти инструкции компьютерной программы могут также быть сохранены в машиночитаемой памяти, которая может предписывать компьютеру или другому программируемому устройству обработки данных функционировать конкретным образом, так что инструкции, хранящиеся в машиночитаемой памяти, создают изделие, включающее в себя средство инструкции, которое реализует функцию, указанную в блоке или блоках блок-схемы. Инструкции компьютерной программы также могут быть загружены в компьютер или другое программируемое устройство обработки данных, чтобы предписывать выполнение ряда рабочих этапов на компьютере или другом программируемом устройстве, чтобы создавать машинореализуемый процесс так, что инструкции, которые исполняются на компьютере или другом программируемом устройстве, обеспечивают этапы для реализации функций, указанных в блоке или блоках блок-схемы.

[0093] Соответственно, функциональные блоки структурных схем и иллюстраций блок-схемы поддерживают сочетания средств для выполнения указанных функций, сочетания этапов для выполнения указанных функций, и средств инструкции программы для выполнения указанных функций. Также следует понимать, что каждый функциональный блок структурных схем и иллюстраций блок-схемы, и сочетания функциональных блоков в структурных схемах и иллюстрациях блок-схемы, могут быть реализованы либо посредством компьютерных систем основанных на аппаратном обеспечении особого назначения, которые выполняют указанные функции или этапы, либо посредством подходящих сочетаний аппаратного обеспечения особого назначения и компьютерных инструкций. Кроме того, иллюстрации технологических потоков и их описания могут обращаться к окнам пользователя, web-сайтам, web-формам, запросам, и т.д. Специалистам-практикам следует иметь в виду, что иллюстрируемые этапы, описываемые в данном документе, могут содержать любое число конфигураций, включая использование окон, web-страниц, web-форм, вспаивающих окон, запросов и подобное. Также следует иметь в виду, что несколько этапов, как иллюстрируется и описывается, могут быть объединены в единых web-страницах и/или окнах, но были расширены для простоты. В других случаях, этапы, иллюстрируемые и описываемые в качестве единых этапов обработки, могут быть разделены на несколько web-страниц и/или окон, но были объединены для простоты.

[0094] Понятие «долговременный» следует понимать как исключающее только распространяющиеся временные сигналы по существу из объема формулы изобретения, и не отказывающееся от прав на все стандартные машиночитаемые носители информации, которые только не являются по существу распространяющимися временными сигналами. Сформулировав иначе, значение понятия «долговременный машиночитаемый носитель информации» следует толковать как исключающее только те типы временных машиночитаемых носителей информации, которые можно найти в деле In Re Nuijten, как выпадающие за объем патентоспособного изобретения по 35 U.S.C 101.

[0095] Выгода, преимущества, и решения проблем были описаны в данном документе касательно конкретных вариантов осуществления. Тем не менее, выгоду, преимущества, решения проблем, и любые элементы, которые могут вызывать то, что любая выгода, преимущество, или решение происходят или становятся более выраженными, не следует толковать как критические, требуемые, или неотъемлемые признаки или элемент раскрытия.

[0096] Несмотря на то, что раскрытие включает в себя способ, предполагается, что он может быть воплощен в качестве инструкций компьютерной программы на вещественном машиночитаемом носителе, таком как магнитная или оптическая память или магнитный или оптический диск. Все структурные, химические, и функциональные эквиваленты элементов у описанных выше примерных вариантов осуществления, которые известны специалистам в соответствующей области техники, в прямой форме включены в данный документ посредством ссылки и подразумеваются, как охватываемые настоящей формулой изобретения. Более того, необязательно для устройства или способа решать каждую и всякую проблему, которую стремится решить настоящее раскрытие, поскольку оно должно охватываться настоящей формулой изобретения. Кроме того, никакой элемент, компонент, или этап способа в настоящем раскрытии не предназначен для общественности, независимо от того, является ли элемент, компонент, или этап способа явно перечисленным в формуле изобретения. Никакой элемент формулы изобретения в данном документе не должен толковаться в

соответствии с положениями 35 U.S.C. 112, шестого параграфа, при условии, что элемент явно не перечислен используя фразу «средство для». Используемые в данном документе понятия «содержит», «содержащий», или любая другая их вариация, предназначены охватывать не исключительное включение, так что процесс, способ, изделие, или устройство, которое содержит список элементов, не включает в себя только эти элементы, а может включать в себя другие элементы в прямой форме не перечисленные или свойственные такому процессу, способу, изделию, или устройству.

[0097] Там, где используется фраза сходная с «по меньшей мере, одно из A, B, или C», «по меньшей мере, одно из A, B, и C», «одно или более из A, B, или C», или «одно или более из A, B, и C», подразумевается, что такая фраза должна интерпретироваться, как означающая что в варианте осуществления может присутствовать только A, в варианте осуществления может присутствовать только B, в варианте осуществления может присутствовать только C, или что любое сочетание элементов A, B и C может присутствовать в одном варианте осуществления; например, A и B, A и C, B и C, или A и B и C.

[0098] Изменения и модификации могут быть выполнены в отношении раскрываемых вариантов осуществления не отступая от объема настоящего раскрытия. Подразумевается, что эти и другие изменения или модификации должны быть включены в объем настоящего раскрытия, как выражено в нижеследующей формуле изобретения.

(57) Формула изобретения

1. Компьютерно-реализуемый способ обеспечения защиты сети для частных сетей посредством шлюза, включающего в себя туннельный сервер и межсетевой экран, при этом способ содержит этапы, на которых:

в ответ на запрос от клиентского устройства создают посредством первой компьютерной системы, реализующей первый шлюз к частной сети, первый сетевой туннель между клиентским устройством и первым шлюзом, при этом частная сеть содержит одно или более сетевых устройств;

принимают посредством первой компьютерной системы от клиентского устройства список доступа клиента, указывающий те сетевые устройства в частной сети, которым разрешено осуществлять связь с клиентским устройством; и

запускают для первого сетевого туннеля отдельную службу межсетевого экрана с отдельным набором правил межсетевого экрана на первой компьютерной системе для выборочной блокировки и разрешения сетевого трафика между клиентским устройством и одним или более сетевыми устройствами в частной сети, при этом каждое из правил межсетевого экрана извлекается из списка доступа клиента.

2. Способ по п.1, в котором упомянутая отдельная служба межсетевого экрана является межсетевым экраном с учетом состояния, содержащим перечень состояний для отслеживания состояний сетевых соединений между клиентским устройством и сетевыми устройствами в частной сети.

3. Способ по п.2, дополнительно содержащий этап, на котором синхронизируют посредством первой компьютерной системы перечень состояний с клиентским устройством.

4. Способ по п.3, дополнительно содержащий этап, на котором делают посредством первой компьютерной системы перечень состояний неизменяемым посредством клиентского устройства.

5. Способ по п.3, дополнительно содержащий этап, на котором, в ответ на отказ первого сетевого туннеля, реализуют посредством второй компьютерной системы

второй шлюз к частной сети, каковая реализация содержит этапы, на которых:

принимают от клиентского устройства второй запрос на создание второго сетевого туннеля между клиентским устройством и вторым шлюзом;

принимают от клиентского устройства перечень состояний;

создают второй сетевой туннель между клиентским устройством и вторым шлюзом;

после создания второго сетевого туннеля запускают вторую отдельную службу межсетевого экрана с упомянутым отдельным набором правил межсетевого экрана на второй компьютерной системе для выборочной блокировки и разрешения сетевого трафика между клиентским устройством и упомянутыми одним или более сетевыми устройствами в частной сети; и

восстанавливают состояние упомянутой отдельной службы межсетевого экрана внутри второй отдельной службы межсетевого экрана с использованием перечня состояний.

6. Способ по п.5, дополнительно содержащий этапы, на которых:

в ответ на отказ первого сетевого туннеля принимают посредством второй компьютерной системы от клиентского устройства список доступа клиента; и

определяют посредством второй компьютерной системы, из списка доступа клиента, правила межсетевого экрана для второй отдельной службы межсетевого экрана.

7. Способ по п.1, в котором:

первая компьютерная система содержит множество ядер процессора;

первая компьютерная система выполнена с возможностью выполнения процесса на каждом ядре процессора; и

упомянутый запуск отдельной службы межсетевого экрана дополнительно содержит этап, на котором запускают, посредством данного процесса, новый поток обработки для обеспечения упомянутой отдельной службы межсетевого экрана в одном из множества ядер процессора.

8. Способ по п.7, в котором упомянутый запуск отдельной службы межсетевого экрана дополнительно содержит этап, на котором выбирают одно из множества ядер процессора и тем самым процесс для выполнения упомянутой отдельной службы межсетевого экрана, при этом способ дополнительно содержит этап, на котором после запуска этой отдельной службы межсетевого экрана направляют данные полезной нагрузки из первого сетевого туннеля в новый поток обработки.

9. Способ по п.7. дополнительно содержащий этапы, на которых:

шифруют посредством упомянутого нового потока обработки данные полезной нагрузки для клиентского устройства; и

дешифруют данные полезной нагрузки от клиентского устройства.

10. Способ по п.9, в котором множество ядер процессора содержит ускорение аппаратного обеспечения для выполнения по меньшей мере одного из шифрования или дешифрования.

11. Система для обеспечения защиты сети для частных сетей посредством шлюза, включающего в себя туннельный сервер и межсетевой экран, содержащая:

по меньшей мере одно ядро процессора, причем каждое ядро выполнено с возможностью выполнения процесса; и

память, хранящую инструкции, приспособленные для предписания по меньшей мере одному ядру процессора:

в ответ на запрос от клиентского устройства создавать сетевой туннель между клиентским устройством и шлюзом к частной сети, при этом частная сеть содержит одно или более сетевых устройств,

принимать от клиентского устройства список доступа клиента, указывающий те сетевые устройства в частной сети, которым разрешено осуществлять связь с клиентским устройством, и

запускать для первого сетевого туннеля отдельную службу межсетевого экрана с отдельным набором правил межсетевого экрана для выборочной блокировки и разрешения сетевого трафика между клиентским устройством и одним или более сетевыми устройствами в частной сети, при этом каждое из правил межсетевого экрана извлекается из списка доступа клиента.

12. Система по п.11, в которой упомянутый запуск отдельной службы межсетевого экрана дополнительно содержит запуск, посредством первого процесса первого ядра из множества ядер процессора, нового потока обработки для обеспечения упомянутой отдельной службы межсетевого экрана на втором ядре из множества ядер процессора.

13. Система по п.12, в которой второе ядро выполняет упомянутую отдельную службу межсетевого экрана.

14. Система по п.13, в которой инструкции дополнительно приспособлены для предписания по меньшей мере одному ядру процессора, после запуска упомянутой отдельной службы межсетевого экрана, направлять данные полезной нагрузки из сетевого туннеля в упомянутый новый поток обработки.

15. Система по п.11, дополнительно содержащая память, хранящую упомянутый отдельный набор правил межсетевого экрана.

16. Энергонезависимый машиночитаемый носитель информации, хранящий машиночитаемые инструкции для обеспечения защиты сети для частных сетей посредством шлюза, включающего в себя туннельный сервер и межсетевой экран, которые при их исполнении предписывают первой компьютерной системе:

в ответ на запрос от клиентского устройства создавать первый сетевой туннель между клиентским устройством и первым шлюзом;

принимать посредством первой компьютерной системы от клиентского устройства список доступа клиента; и

запускать для первого сетевого туннеля отдельную службу межсетевого экрана с отдельным набором правил межсетевого экрана на первой компьютерной системе для выборочной блокировки и разрешения сетевого трафика между клиентским устройством и одним или более сетевыми устройствами в частной сети, при этом каждое из правил межсетевого экрана извлекается из списка доступа клиента.

17. Носитель информации по п.16, в котором инструкции дополнительно предписывают первой компьютерной системе, в ответ на отказ первого сетевого туннеля, предписывать реализацию, посредством второй компьютерной системы, второго шлюза к частной сети, причем при этой реализации должен создаваться второй сетевой туннель между клиентским устройством и вторым шлюзом, при этом при данной реализации дополнительно должна запускаться вторая отдельная служба межсетевого экрана с упомянутым отдельным набором правил межсетевого экрана.

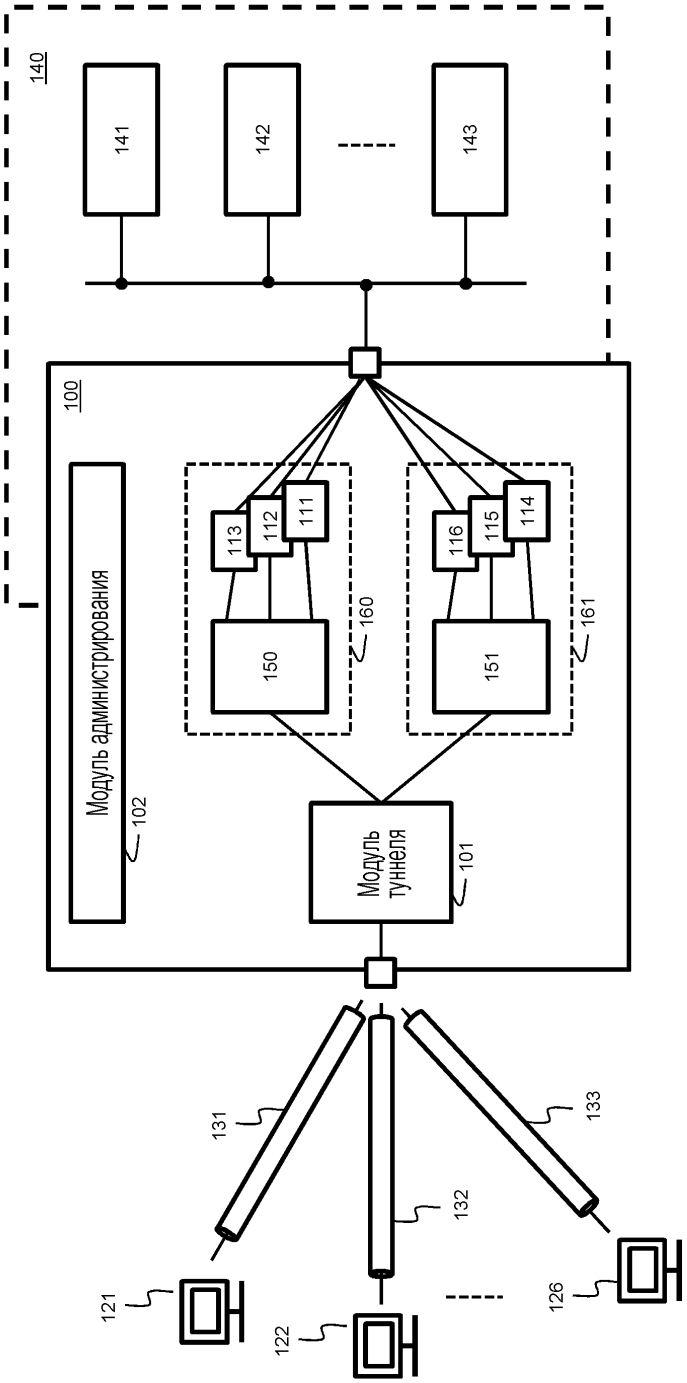
18. Носитель информации по п.17, в котором инструкции дополнительно предписывают первой компьютерной системе:

в ответ на отказ первого сетевого туннеля предписывать предоставление списка доступа клиента второй компьютерной системе.

19. Носитель информации по п.16, при этом упомянутая отдельная служба межсетевого экрана является межсетевым экраном с учетом состояния, содержащим перечень состояний для отслеживания состояний сетевых соединений между клиентским устройством и сетевыми устройствами.

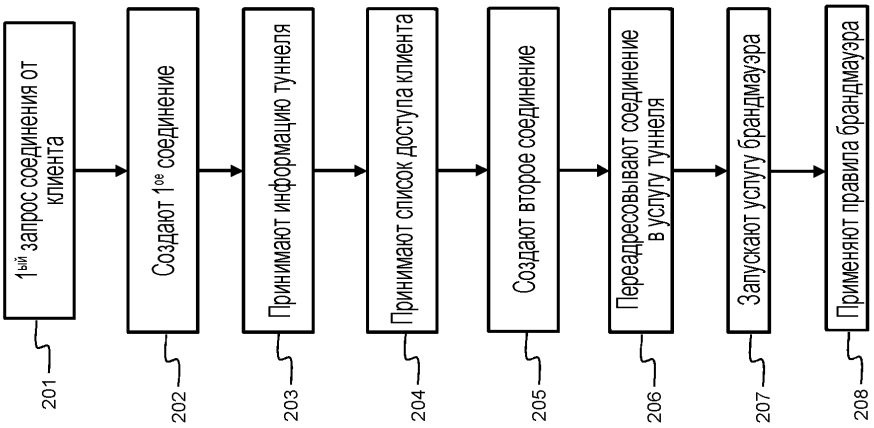
20. Носитель информации по п.16, в котором инструкции дополнительно предписывают первой компьютерной системе шифровать данные полезной нагрузки для клиентского устройства.

1

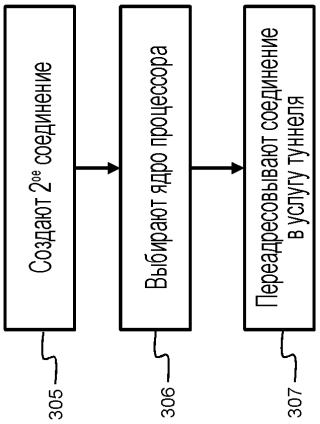

140
141
142
143
100
Модуль администрирования
102
113
112
111
116
115
114
160
161
150
151
Модуль туннеля
101
131
132
133
121
122
126

ФИГ. 1

2

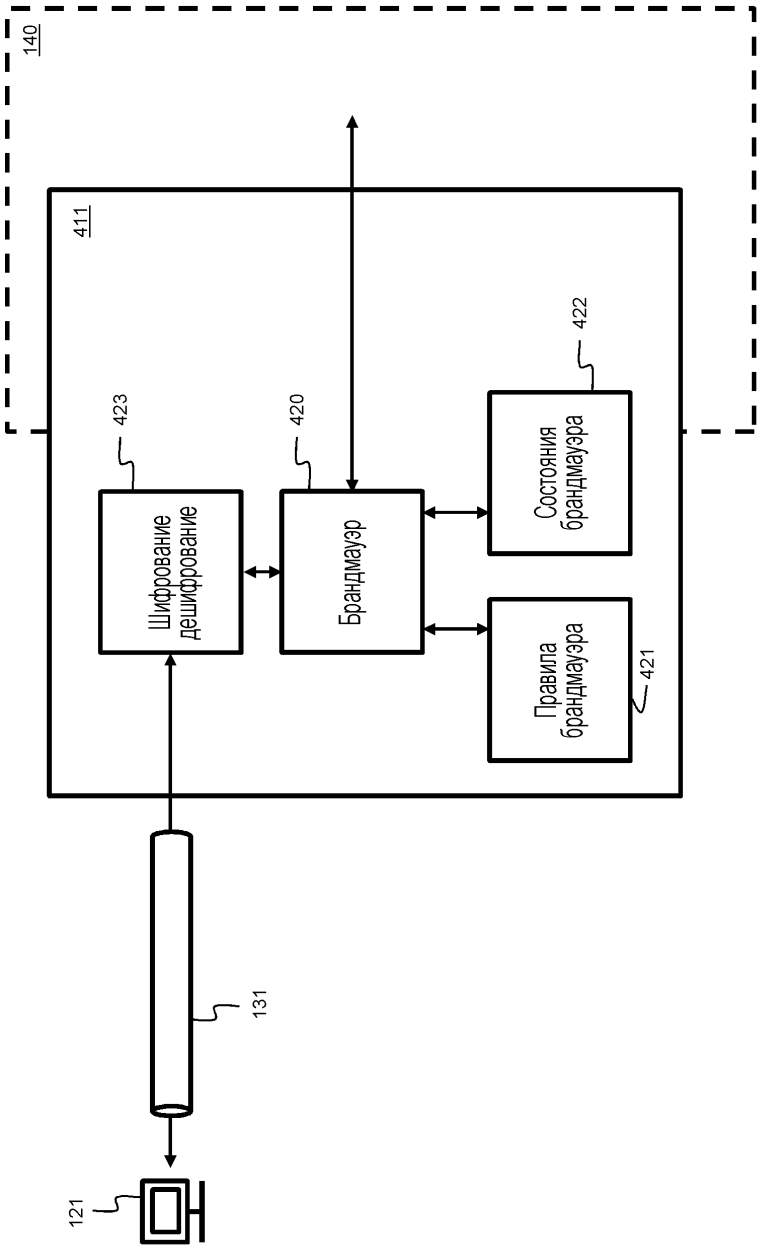

1ый запрос соединения от клиента
Создают 1ое соединение
Принимают информацию туннеля
Принимают список доступа клиента
Создают второе соединение
Переадресовывают соединение в услугу туннеля
Запускают услугу брандмауэра
Применяют правила брандмауэра
201
202
203
204
205
206
207
208

ФИГ. 2


Создают 2ое соединение
Выбирают ядро процессора
Переадресовывают соединение в услугу туннеля
305
306
307

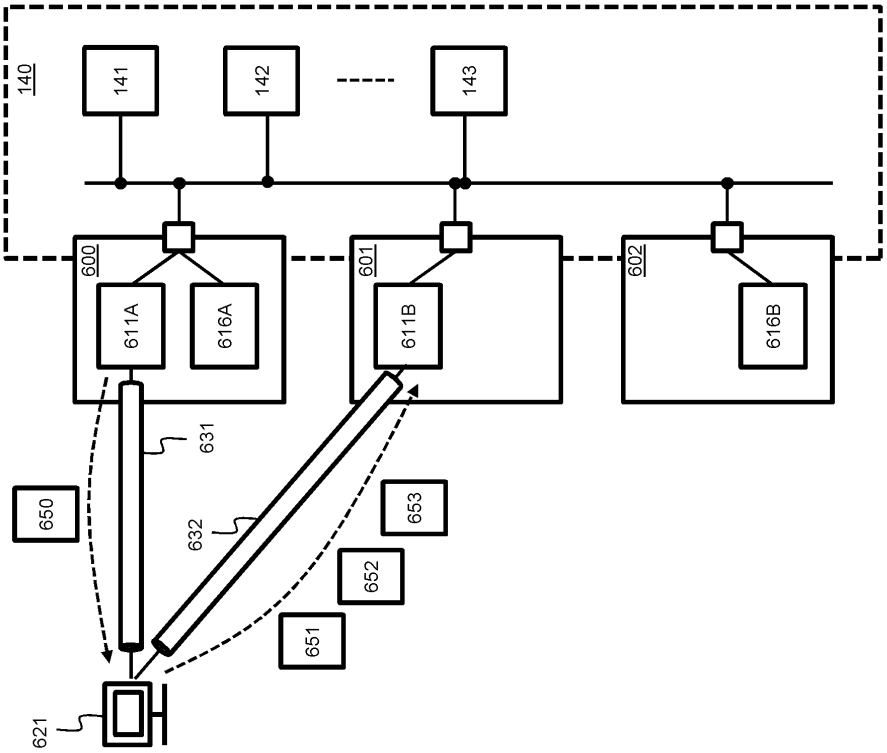
ФИГ. 3

3

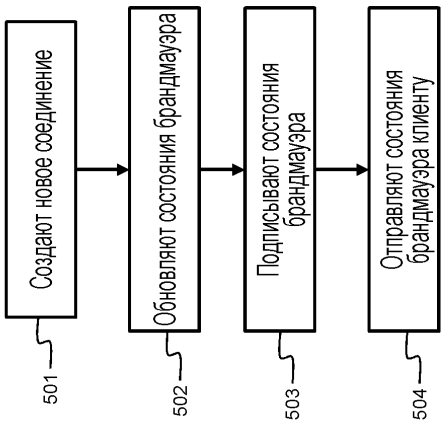

140
411
423
420
422
Шифрование дешифрование
Брандмауэр
Состояния брандмауэра
Правила брандмауэра
421
131
121

ФИГ. 4

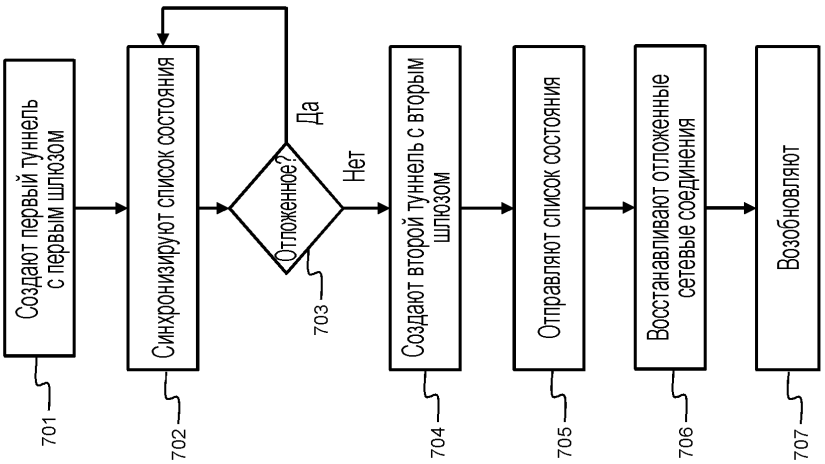
4


140
141
142
143
600
601
602
611A
616A
611B
616B
631
632
650
651
652
653
621

ФИГ. 6

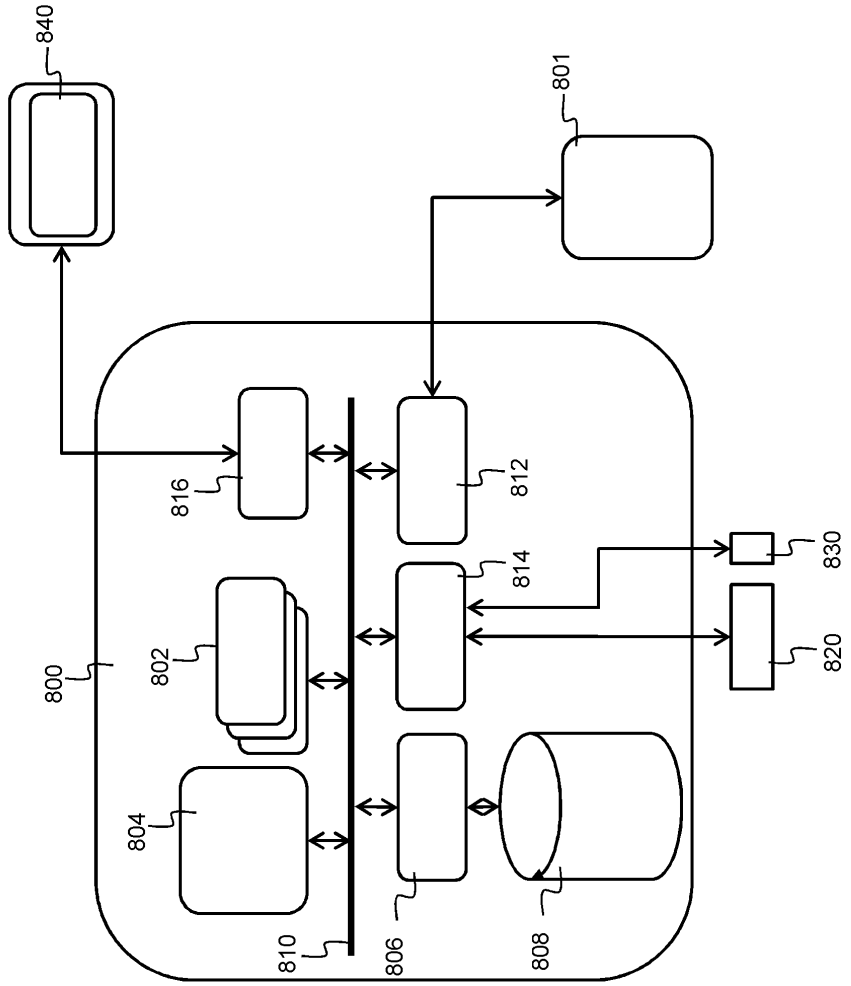

Создают новое соединение
Обновляют состояния брандмауэра
Подписывают состояния брандмауэра
Отправляют состояния брандмауэра клиенту
501
502
503
504

ФИГ. 5


Создают первый туннель с первым шлюзом
Синхронизируют список состояния
Отложенное?
Да
Нет
Создают второй туннель с вторым шлюзом
Отправляют список состояния
Восстанавливают отложенные сетевые соединения
Возобновляют
701
702
703
704
705
706
707

ФИГ. 7

6



ФИГ. 8