РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 679 227**(13) **C1**

(51) МПК
H04L 12/66 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 12/66 (2018.08); H04L 12/00 (2018.08)

(21)(22) Заявка: **2018112218, 05.04.2018**

(24) Дата начала отсчета срока действия патента:
05.04.2018

Дата регистрации:
06.02.2019

Приоритет(ы):
(22) Дата подачи заявки: **05.04.2018**

(45) Опубликовано: **06.02.2019** Бюл. № **4**

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):
Оладько Алексей Юрьевич (RU)

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

(56) Список документов, цитированных в отчете о поиске: **RU 2012145170 A, 27.04.2014. US 2007/0297333 A1, 27.12.2007. US 2010/0208611 A1, 19.08.2010. US 2004/0153858 A1, 05.08.2004. US 2015/0281125 A1, 01.10.2015.**

(54) **Способ работы межсетевого экрана**

(57) Реферат:

Изобретение относится к области вычислительной техники. Технический результат заключается в повышении защищенности сети в защищаемом сегменте. Способ содержит этапы, на которых: принимают от отправителя с адресом S1 для получателя с адресом R1 сетевой пакет P1; осуществляют поиск с помощью модуля обработки таблицы сетевых соединений дескриптора сетевого соединения, к которому относится сетевой пакет P1, на основе адреса отправителя S1, адреса получателя R1, номера инкапсулированного протокола транспортного уровня, информации о протоколе транспортного уровня; если дескриптор сетевого соединения не найден, то создают и сохраняют в таблице сетевых соединений дескриптор сетевого соединения с помощью модуля обработки таблицы сетевых соединений; производят анализ сетевого пакета в модуле классификации сетевых пакетов; сохраняют в дескрипторе сетевого соединения информацию, полученную в результате анализа сетевого пакета из модуля классификации сетевых пакетов; выполняют фильтрацию сетевого пакета.

RU 2679227 C1

RU 2679227 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 679 227**(13) **C1**

(51) Int. Cl.
H04L 12/66 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 12/66 (2018.08); H04L 12/00 (2018.08)

(21)(22) Application: **2018112218, 05.04.2018**

(24) Effective date for property rights:
05.04.2018

Registration date:
06.02.2019

Priority:
(22) Date of filing: **05.04.2018**

(45) Date of publication: **06.02.2019** Bull. № **4**

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

(72) Inventor(s):
Oladko Aleksej Yurevich (RU)

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

RU 2679227 C1

(54) FIREWALL OPERATING METHOD

(57) Abstract:

FIELD: computer equipment.

SUBSTANCE: method comprises stages, at which: from the sender with the address S1 for the recipient with the address R1 receiving the network packet P1; using the network connections table processing module searching for the network connection descriptor, to which the network packet P1 belongs, based on the sender S1 address, the recipient R1 address, the encapsulated transport layer protocol number, information about the transport layer protocol; if the network connection descriptor is not found, then creating the network connection descriptor, and storing in the network connection table using the network connection table processing module; analyzing the network packet in the network packet classification module; in the network connection descriptor storing the information obtained from the network packet from the network packet classification module analyzing; performing the network packet filtering.

EFFECT: technical result consists in increase in the network in the protected segment security.

1 cl

RU 2679227 C1

Область техники, к которой относится изобретение

Предполагаемое изобретение относится к области защиты сетей передачи данных с коммутацией пакетов и может быть использовано для повышения защищенности сетей.

Уровень техники

Защита современных цифровых сетей передачи данных, имеющих выход в сеть Интернет, обеспечивается различными методами, в том числе с использованием шлюзов-компьютеров с межсетевыми экранами (МЭ), которые обеспечивает защиту сети (подсети) путем фильтрации по определенным правилам входящего и исходящего потока данных (трафика). Для обеспечения эффективной защиты важен выбор правил и условий их применения.

Так, известен способ управления соединениями в межсетевом экране (патент РФ №2517411, приоритет от 24.10.2012 г.), который включает следующие действия:

- получают пакеты из внешней сети;
- формируют таблицу соединений, содержащую следующие сведения:
  - информацию о пакетах, входящих в соединение (исходный пакет, ответный пакет, ошибки ICMP);
  - информацию о преобразованиях пакета в случае трансляции адресов;
  - о типе сетевого протокола;
  - состояние соединения (новое, установленное, закрытое);
  - отметка о времени обработки последнего пакета;
  - информацию о группах соединений в случае прикладных протоколов (FTP, SIP);
- определяют общее количество установленных соединений на данный момент времени;
- определяют уровень загрузки межсетевого экрана путем сравнения количества установленных соединений с определенной пороговой величиной;
- определяют новые и установленные соединения на основе двустороннего обмена пакетами между клиентом и сервером;
- определяют закрытые соединения на основе обработки ICMP-сообщений об ошибках или флагов в TCP-заголовке (только для протокола TCP);
- динамически определяют текущие значения таймаутов для соединений на основании следующих параметров: отип сетевого протокола;
  - состояние соединения;
  - уровень загрузки межсетевого экрана;
- изменяют отметку времени обработки последнего пакета в случае прохождения любого пакета в рамках данного соединения или в рамках группы соединений;
- удаляют соединение, если отметка времени обработки последнего пакета отличается от текущего времени больше, чем таймаут данного соединения.

Недостатками известного способа является невозможность проводить классификацию протокола прикладного уровня, используемого в сетевом соединении, и далее фильтрацию по данному протоколу прикладного уровня.

Также известен способ защиты вычислительной сети путем применения механизма классификации пакетов в сетевом устройстве безопасности (патент США №8009566, приоритет от 26.06.2006 г.), в котором для защиты вычислительных сетей используют шлюз-компьютер с МЭ, устанавливаемый на каналах связи защищаемой сети с другими сетями, и который содержит модуль классификации пакетов.

Способ содержит следующие этапы:

- получают сетевой пакет;
- производят поиск записи в таблице соединений на основе информации из сетевого

и транспортного заголовков сетевого пакета;

• если запись в таблице соединений не найдена, то

○ сетевой пакет ассоциируется с новой сессией, которой присваивается уникальный идентификатор;

○ производят пакетную фильтрацию, например, на основе данных из заголовков сетевого и транспортного уровня;

○ создают новую запись в таблице соединений, если пакет разрешен фильтрами МЭ;

○ передают пакет в модуль классификации пакетов;

○ выполняют фильтрацию сетевого потока на основе результатов классификации, если пакет и соответствующий сетевой поток были классифицированы;

○ сохраняют копию сетевого пакета, если он не был классифицирован;

○ передают сетевой пакет;

• если запись в таблице соединений найдена и соединение было классифицировано в модуле классификации пакетов, то

○ выполняют фильтрацию сетевого потока на основе результатов классификации;

○ передают сетевой пакет;

• если запись в таблице соединений найдена и соединение не было классифицировано в модуле классификации пакетов, то

○ передают пакет в модуль классификации пакетов;

○ выполняют фильтрацию сетевого потока на основе результатов классификации, если пакет и соответствующий сетевой поток были классифицированы;

○ сохраняют копию сетевого пакета, если он не был классифицирован; ○ передают сетевой пакет.

Известный способ может обеспечить фильтрацию потока данных по протоколу прикладного уровня, который был определен модулем классификации пакетов.

Однако, при использовании известного способа первоначальное решение о разрешении или блокировании сетевого потока должно быть принято на основе правил пакетного фильтра, а правила фильтрации потока данных по протоколу прикладного уровня применяются только после получения окончательной классификации модулем классификации сетевых пакетов.

Такая схема действия является недостатком известного способа, так как для окончательной классификации модулем классификации сетевых пакетов может потребоваться более одного сетевого пакета, которые будут пропущены согласно разрешающему правилу пакетного фильтра.

Раскрытие изобретения

Техническим результатом является

1) повышение защищенности сети в защищаемом сегменте,

2) возможность использования правил фильтрации по результату анализа модулем классификации сетевых пакетов совместно с правилами фильтрации пакетного фильтра.

Заявленный результат достигается за счет применения способа работы межсетевого экрана, причем на входе защищаемой вычислительной сети установлен шлюз-компьютер с межсетевым экраном, в котором определено множество А разрешенных для использования протоколов прикладного уровня и множество В запрещенных для использования протоколов прикладного уровня, при этом межсетевой экран выполнен с возможностью проводить пакетную фильтрацию и содержит

• модуль обработки таблицы сетевых соединений, причем элементом таблицы служит дескриптор сетевого соединения, который содержит, по меньшей мере, следующую информацию:

- сетевой адрес источника и назначения;
- статус сетевого соединения, который может принимать следующие значения: "Новый", "Установлено", "Заблокировано";
- номер инкапсулированного протокола транспортного уровня;
- информацию о протоколе транспортного уровня;
- информацию из модуля классификации сетевых пакетов;

• модуль классификации сетевых пакетов, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня;

способ заключается в том, что

• принимают от отправителя с адресом S1 для получателя с адресом R1 сетевой пакет P1;

• осуществляют поиск с помощью модуля обработки таблицы сетевых соединений дескриптора сетевого соединения, к которому относится сетевой пакет P1, на основе адреса отправителя S1, адреса получателя R1, номера инкапсулированного протокола транспортного уровня, информации о протоколе транспортного уровня;

• если дескриптор сетевого соединения не найден, то создают и сохраняют в таблице сетевых соединений дескриптор сетевого соединения с помощью модуля обработки таблицы сетевых соединений, причем статус сетевого соединения принимает значение "Новый";

• производят анализ сетевого пакета в модуле классификации сетевых пакетов, получая, по крайней мере, следующую информацию:

- протокол прикладного уровня Pa, если он был установлен;
- флаг окончательной классификации F, который показывает, что результат классификации сетевого соединения далее не будет изменен;
- множество прикладных протоколов Re, которое содержит список прикладных протоколов, для которых модулем классификации сетевых пакетов определено, что в сетевом соединении не используются протоколы прикладного уровня из множества Re;

• если статус сетевого соединения в дескрипторе сетевого соединения содержит значение "Заблокировано", то блокируют сетевой пакет;

• иначе если информация о пакете из модуля классификации сетевых пакетов совпадает с информацией, сохраненной в дескрипторе сетевого соединения, и статус сетевого соединения содержит значение "Установлено", то пропускают пакет;

• иначе

- сохраняют в дескрипторе сетевого соединения информацию, полученную в результате анализа сетевого пакета из модуля классификации сетевых пакетов;
- выполняют фильтрацию сетевого пакета, причем правила фильтрации по разрешенным или запрещенным протоколам прикладного уровня работают следующим образом:
  - если установленный в результате работы модуля классификации сетевых пакетов прикладной протокол Pa является элементом множества B, то блокируют сетевой пакет и устанавливают для статуса сетевого соединения значение "Заблокировано";
  - если установленный в результате работы модуля классификации сетевых пакетов прикладной протокол Ra является элементом множества A, то пропускают сетевой пакет, и устанавливают для статуса сетевого соединения значение "Установлено";
  - если не установлен флаг окончательной классификации F и разность множеств A и Re образует непустое множество, то пропускают сетевой пакет и устанавливают для статуса сетевого соединения значение "Установлено".

Для реализации предложенного способа в состав МЭ должны быть включены модуль классификации сетевых пакетов, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня, и модуль обработки таблицы сетевых соединений. В общем случае, перечисленные модули могут быть программно-аппаратными или программными. Для создания указанных модулей должно быть проведено обычное проектирование и изготовлении электронного блока (при выполнении в программно-аппаратном виде) и формирование необходимого программного обеспечения (ПО) с последующим тестированием и установкой в МЭ. Для создания модуля контроля и модуля обработки таблицы сетевых соединений в программном виде создается только прикладное либо системное ПО. Создание данных модулей может осуществить специалист по проектированию и изготовлению электронной техники и/или специалист по программированию (программист) на основе знания о выполняемых данными модулями функциях.

После создания и отладки модуля классификации сетевых пакетов и модуля обработки таблицы сетевых соединений можно приступать непосредственно к реализации предложенного способа.

Для осуществления способа МЭ получает сетевые пакеты, принятые на сетевом интерфейсе. Сначала сетевые пакеты проверяются на принадлежность к уже созданным сетевым соединениям. Для этого осуществляется поиск в таблице сетевых соединений. Если подходящего соединения не найдено, то в модуле обработки таблицы сетевых соединений создается запись о новом соединении в виде дескриптора. При создании данного дескриптора, в него заносится информация из заголовка протокола сетевого уровня, включая сетевые адреса источника и назначения, и, при необходимости, информация об используемом протоколе транспортного уровня, включая номера портов источника и назначения. Для созданного дескриптора значение статуса устанавливается как "Новый".

Далее сетевые пакеты передаются в модуль классификации сетевых пакетов, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня. Процесс обработки сетевого пакета в данном модуле может включать в себя сохранение локальной копии пакета для последующего анализа, декодирования протокола на основе контента. Информация о текущем результате процесса классификации передается далее в МЭ. Данная информация может включать в себя как установленный протокол прикладного уровня, так и список прикладных протоколов, которые не используются в сетевом соединении, а так же флаг окончательной классификации, показывающий, что результат классификации далее не будет изменен.

Если значение поля статус в дескрипторе сетевого соединения содержит значение "Заблокировано", то блокируют сетевой пакет. На этом обработка сетевого пакета заканчивается.

Если информация о пакете из модуля классификации сетевых пакетов совпадает с информацией, сохраненной в дескрипторе сетевого соединения, и статус сетевого соединения содержит значение "Установлено", то выполняются все необходимые действия для обработки и дальнейшей передачи сетевого пакета в сеть.

Если информация о пакете из модуля классификации сетевых пакетов не совпадает с информацией, сохраненной в дескрипторе сетевого соединения, или статус сетевого соединения содержит значение "Новый", то осуществляется фильтрация сетевого пакета на соответствие настроенным фильтрам. При этом информация, полученная в результате анализа сетевого пакета из модуля классификации сетевых пакетов, сохраняется в

дескрипторе соединения. Если пакет оказался заблокирован каким-либо из фильтров, то на этом его обработка заканчивается, а в поле статус дескриптора сетевого соединения устанавливается значение "Заблокировано". Если прохождение пакета было разрешено, то поле статус дескриптора сетевого соединения устанавливается значение "Установлено" и выполняются все необходимые действия для обработки и дальнейшей передачи сетевого пакета в сеть.

В результате, в отличие от известного способа обеспечивается возможность совместного применения правил фильтрации по классифицированному протоколу прикладного уровня и по данным из заголовков сетевого и транспортного уровней.

В отличие от известного способа, нет необходимости производить пакетную фильтрацию (например, на основе данных из заголовков сетевого и транспортного уровня) до передачи сетевого пакета на анализ в модуль классификации сетевых пакетов, как и использование фильтрации на основе данных из заголовков сетевого и транспортного уровня. Фильтрация сетевых пакетов может быть осуществлена только по разрешенным или запрещенным протоколам прикладного уровня.

Также, в отличие от известного способа, нет необходимости пропускать все сетевые пакеты из сетевого потока до того момента, когда модуль классификации сетевых пакетов определит используемый в сетевом соединении протокол прикладного уровня. Фильтрация по протоколу прикладного уровня может быть выполнена на основании информации о списке прикладных протоколов, которые не используются в сетевом соединении, еще до получения из модуля классификации сетевых пакетов информации об используемом в сетевом соединении протокола прикладного уровня.

Таким образом, нет необходимости разрешать прохождение сетевых пакетов, которые требуются модулю классификации сетевых пакетов для определения используемого в сетевом соединении протокола прикладного уровня, если уже стало известно, что в данном сетевом соединении не используется протокол прикладного уровня из списка разрешенных.

В результате обеспечивается повышение защищенности вычислительной сети от несанкционированной передачи информации, так как данный способ позволяет заблокировать сетевое соединение, не дожидаясь установления используемого в сетевом соединении протокола прикладного уровня, и нет необходимости пропускать сетевые пакеты до наступления данного события.

Осуществление изобретения

Рассмотрим осуществление предложенного способа в сети с коммутацией пакетов. Это может быть, например, корпоративная сеть, имеющая выход в сеть Интернет через один основной МЭ.

В качестве МЭ может быть использован высокопроизводительный программно-аппаратный комплекс (ПАК) типа HW1000 на базе Intel Core 2 Duo, объемом оперативной памяти 2 Гб, объемом жесткого диска 250 Гб, с установленной ОС Linux (ядро 3.10.92) и специализированным ПО (статья и загружаемая документация по адресу:

http://infotecs.ru/downloads/all/vipnet-coordinator-hw-1000.html?arrFilter_93=408821001&set_filter=Y).

Предпочтительным является выполнение модуля классификации сетевых пакетов в программном виде, для чего предварительно создается, тестируется и затем инсталлируется в МЭ прикладное ПО в виде программного модуля, выполняющего функции модуля классификации сетевых пакетов и способного выполнять определение используемого в сетевом соединении протокола прикладного уровня.

В качестве модуля классификации сетевых пакетов может быть использовано ПО с

возможностью проведения глубокой инспекции пакетов (Deep Packet Inspection). При этом, в результате проведения классификации сетевого пакета должно быть, как минимум, обеспечено получение следующей информации:

• протокол прикладного уровня, используемый в сетевом соединении, если он был установлен;

• флаг окончательной классификации, который показывает, что результат классификации сетевого соединения далее не будет изменен;

• множество прикладных протоколов, которое содержит список прикладных протоколов, для которых модулем классификации сетевых пакетов определено, что в сетевом соединении не используются протоколы прикладного уровня из множества.

В МЭ также определяется множество A разрешенных для использования протоколов прикладного уровня и множество B запрещенных для использования протоколов прикладного уровня. Например, во множество A могут входить следующие протоколы прикладного уровня: Adobe Connect, AFP, AVI, DHCP, DHCP v6, Diameter, Direct Connect, DNS, HTTP, IPsec, Kerberos, Microsoft Dynamics NAV, Modbus, MySQL, NetBIOS, OpenFlow, OpenVPN, Opera Mini, Oracle Database, Poison Ivy, POP, PostgreSQL, SAP, Skype, SSH, SSL, Telnet, VPN-X, WAP-WSP, XBOX, XDCC, XDMCP, XMPP. и др.

В качестве модуля обработки таблицы сетевых соединений может быть использован модуль ядра Linux nf_conntrack.ko, входящая в состав подсистемы Netfilter ядра Linux. Дескриптором сетевого соединения в этом случае выступает структура nf_conn, определенная в ядре Linux.

Анализ сетевых пакетов осуществляется подсистемой Netfilter ядра, которая обеспечивает:

• пакетную фильтрацию;

• анализ информации, содержащейся в структуре nf_conn;

• передачу сетевых пакетов в средство контроля, выполненное с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня, и получение результатов анализа через системный интерфейс netfilter_queue ядра Linux.

Для работы правил фильтрации по разрешенным или запрещенным протоколам прикладного уровня должен быть создан специальный модуль ядра xt_dpi.ko, который регистрируется в подсистеме Netfilter ядра Linux. Модуль xt_dpi.ko осуществляет фильтрацию сетевых пакетов согласно следующей логике:

• если установленный в результате работы модуля классификации сетевых пакетов прикладной протокол является элементом множества B, то блокируют сетевой пакет и устанавливают для статуса сетевого соединения значение "Заблокировано";

• если установленный в результате работы модуля классификации сетевых пакетов прикладной протокол является элементом множества A, то пропускают сетевой пакет, и устанавливают для статуса сетевого соединения значение "Установлено";

• если не установлен флаг окончательной классификации и разность множества A и множества прикладных протоколов, которые не используются в сетевом соединении, согласно результату из модуля классификации сетевых пакетов, образует непустое множество, то пропускают сетевой пакет и устанавливают для статуса сетевого соединения значение "Установлено". Список правил фильтрации в межсетевом экране должен строиться следующим образом:

• первое правило: проверяют значение поля статуса дескриптора сетевого соединения, если значение равно "Заблокировано", то сетевой пакет блокируется, и дальнейшая обработка прекращается;

• второе правило: если информация о пакете из модуля классификации сетевых пакетов совпадает с информацией, сохраненной в дескрипторе сетевого соединения, и статус сетевого соединения содержит значение "Установлено", то пропускают пакет;

• далее следуют правила фильтрации сетевых пакетов, в том числе правила фильтрации по протоколу прикладного уровня.

Например, первое правило может быть записано следующей командой:

iptables -A FORWARD -m -m conntrack --ctstate DROPPED -j DROP

Второе правило может быть записано следующей командой:

iptables -A FORWARD -m conntrack --ctstate ESTABLISHED -m conntrack --dpiresult NOTCHANGED -j ACCEPT

Пример последующих правил фильтрации сетевых пакетов:

iptables -A FORWARD -m dpi --accept-protocol HTTP -j ACCEPT

iptables -A FORWARD -m dpi --drop-protocol FTP -j DROP

iptables -A FORWARD -j DROP

При получении сетевого пакета, модуль ядра nf_conntrack.ko проверяет сетевой пакет на принадлежность к уже установленным соединениям. С этой целью производится поиск в таблице сетевых соединений. Если подходящего соединения не найдено, то модуль ядра Linux nf_conntrack.ko создает запись о новом соединении в виде дескриптора nf_conn и сохраняет его в таблице сетевых соединений. При создании нового дескриптора сетевого соединения, в поле статус устанавливается значение "Новый".

Затем в МЭ запускается модуль классификации сетевых соединений, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня. Сетевые пакеты для анализа данная программа получает через системный интерфейс netfilter_queue ядра Linux.

Далее в подсистеме Netfilter ядра проводится проверка сетевого пакета на соответствие настроенным фильтрам. При этом проверка на соответствие фильтрам по разрешенным или запрещенным протоколам прикладного уровня выполняется в модуле ядра xt_dpi.ko. Также в подсистеме Netfilter ядра производится сохранение в дескрипторе сетевого соединения информацию, полученную в результате анализа сетевого пакета из модуля классификации сетевых пакетов. Если сетевой пакет оказался заблокирован каким-либо из фильтров, то в поле статус дескриптора сетевого соединения устанавливается значение "Заблокировано". Если подсистема фильтрации разрешила прохождение сетевого пакета для дальнейшей обработки, то в поле статус дескриптора сетевого соединения устанавливается значение "Установлено".

В результате, пропускаются сетевые пакеты, которые относятся к сетевым соединениям, работающим по одному из протоколов прикладного уровня из множества A; блокируются сетевые пакеты, которые относятся к сетевым соединениям, работающим по одному из протоколов прикладного уровня из множества B.

(57) Формула изобретения

Способ работы межсетевого экрана, причем для межсетевого экрана определено множество A разрешенных для использования протоколов прикладного уровня и множество B запрещенных для использования протоколов прикладного уровня, при этом межсетевой экран выполнен с возможностью проводить пакетную фильтрацию и содержит

модуль обработки таблицы сетевых соединений, причем элементом таблицы служит дескриптор сетевого соединения, который содержит, по меньшей мере, следующую информацию:

сетевой адрес источника и назначения;

статус сетевого соединения, который может принимать следующие значения: "Новый", "Установлено", "Заблокировано";

номер инкапсулированного протокола транспортного уровня;

информацию о протоколе транспортного уровня;

информацию из модуля классификации сетевых пакетов;

модуль классификации сетевых пакетов, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня;

способ заключается в том, что

принимают от отправителя с адресом S1 для получателя с адресом R1 сетевой пакет P1;

осуществляют поиск с помощью модуля обработки таблицы сетевых соединений дескриптора сетевого соединения, к которому относится сетевой пакет P1, на основе адреса отправителя S1, адреса получателя R1, номера инкапсулированного протокола транспортного уровня, информации о протоколе транспортного уровня;

если дескриптор сетевого соединения не найден, то создают и сохраняют в таблице сетевых соединений дескриптор сетевого соединения с помощью модуля обработки таблицы сетевых соединений, причем статус сетевого соединения принимает значение "Новый";

производят анализ сетевого пакета в модуле классификации сетевых пакетов, получая, по крайней мере, следующую информацию:

протокол прикладного уровня Pa, если он был установлен;

флаг окончательной классификации F, который показывает, что результат классификации сетевого соединения далее не будет изменен;

множество прикладных протоколов Re, которое содержит список прикладных протоколов, для которых модулем классификации сетевых пакетов определено, что в сетевом соединении не используются протоколы прикладного уровня из множества Re;

если статус сетевого соединения в дескрипторе сетевого соединения содержит значение "Заблокировано", то блокируют сетевой пакет; иначе если информация о пакете из модуля классификации сетевых пакетов совпадает с информацией, сохраненной в дескрипторе сетевого соединения, и статус сетевого соединения содержит значение "Установлено", то пропускают пакет;

иначе

сохраняют в дескрипторе сетевого соединения информацию, полученную в результате анализа сетевого пакета из модуля классификации сетевых пакетов;

выполняют фильтрацию сетевого пакета, причем правила фильтрации по разрешенным или запрещенным протоколам прикладного уровня работают следующим образом:

если установленный в результате работы модуля классификации сетевых пакетов прикладной протокол Pa является элементом множества B, то блокируют сетевой пакет и устанавливают для статуса сетевого соединения значение "Заблокировано";

если установленный в результате работы модуля классификации сетевых пакетов прикладной протокол Ra является элементом множества A, то пропускают сетевой пакет, и устанавливают для статуса сетевого соединения значение "Установлено";

если не установлен флаг окончательной классификации F и разность множеств A и Re образует непустое множество, то пропускают сетевой пакет и устанавливают для статуса сетевого соединения значение "Установлено".