РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 667 805**(13) **C1**

(51) МПК
G06F 15/16 (2006.01)
G06F 15/173 (2006.01)
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 29/125 *(2006.01);* ***H04L 29/1282*** *(2006.01);* ***H04L 61/2564*** *(2006.01);* ***H04L 61/6013*** *(2006.01);* ***H04L 63/0281*** *(2006.01);* ***H04L 29/06*** *(2006.01)*

(21)(22) Заявка: **2017143804, 14.12.2017**

(24) Дата начала отсчета срока действия патента:
14.12.2017

Дата регистрации:
24.09.2018

Приоритет(ы):
(22) Дата подачи заявки: **14.12.2017**

(45) Опубликовано: **24.09.2018** Бюл. № **27**

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: **US 7266604 B1, 04.09.2007. US 2003/0120955 A1, 26.06.2003. US 6795870 B1, 21.09.2004. RU 2517411 C1, 27.05.2014.**

(54) Способ работы межсетевого экрана

(57) Реферат:

Изобретение относится к способу работы межсетевого экрана. Техническим результатом является повышение защищенности вычислительной сети. Принимают от отправителя с адресом для получателя с адресом сетевой пакет. Если сетевой пакет имеет номер инкапсулированного протокола транспортного уровня, соответствующий номеру протокола UDP, и содержит данные, то выполняют следующие действия: выполняют пакетную фильтрацию для сетевого пакета; определяют с помощью модуля контроля факт использования в составе данных протокола прикладного уровня из множества. Если факт использования установлен, то выполняют следующие действия: заменяют в сетевом пакете адрес получателя на адрес прокси-модуля в модуле сетевой трансляции адресов; выполняют фильтрацию сетевого потока в прокси-модуле; обрабатывают данные в прокси-модуле.

RU 2667805 C1

RU 2667805 C1

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 667 805**(13) **C1**

(51) Int. Cl.
G06F 15/16 (2006.01)
G06F 15/173 (2006.01)
H04L 29/06 (2006.01)
H04L 29/12 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 29/125 *(2006.01);* ***H04L 29/1282*** *(2006.01);* ***H04L 61/2564*** *(2006.01);* ***H04L 61/6013*** *(2006.01);* ***H04L 63/0281*** *(2006.01);* ***H04L 29/06*** *(2006.01)*

(21)(22) Application: **2017143804, 14.12.2017**

(24) Effective date for property rights:
14.12.2017

Registration date:
24.09.2018

Priority:
(22) Date of filing: **14.12.2017**

(45) Date of publication: **24.09.2018** Bull. № **27**

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)

(54) METHOD OF OPERATING A FIREWALL

(57) Abstract:

FIELD: information technology.

SUBSTANCE: invention relates to a method of operating a firewall. Accept from the sender with the address for the recipient with the address of the network packet. If the network packet has an encapsulated transport layer protocol number corresponding to the UDP protocol number, and contains data, then the following actions are performed: perform packet filtering for the network packet; determine by means of the control module the fact of using in the data of the protocol the application layer from the set. If the fact of use is established, the following actions are performed: replace the address of the recipient in the network packet with the address of the proxy module in the network address translation module; perform filtering of the network stream in the proxy module; process the data in the proxy module.

EFFECT: technical result is to increase the security of the computer network.

1 cl

RU 2667805 C1

RU 2667805 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

Для защиты современных цифровых сетей передачи данных, имеющих выход в сеть Интернет, обычно устанавливают шлюз-компьютер с межсетевым экраном (МЭ), который обеспечивает защиту сети (подсети) путем фильтрации по определенным правилам входящего и исходящего потока данных (трафика). Эффективность защиты зависит от подбора правил и условий их применения.

Так, известен способ защиты вычислительной сети путем применения механизма Proxy Network Address Translation (патент США №7266604, приоритет от 31.03.2000 г.), в котором для защиты вычислительных сетей используют шлюз-компьютер с межсетевым экраном (МЭ), устанавливаемый на каналах связи защищаемой сети с другими сетями, и который содержит прокси-модуль и модуль сетевой трансляции адресов (Network Address Translation, NAT). В модуле NAT производится преобразование адресов назначения в сетевых пакетах, исходящих от клиента и предназначенных для сервера. Модуль NAT перенаправляет пакеты в прокси-модуль. В прокси-модуле выполняется фильтрация сетевого потока данных.

Способ содержит следующие этапы:

- получают сетевой пакет от компьютера в защищаемой сети к серверу во внешней сети;
- заменяют в модуле NAT в пакете адрес назначения на адрес прокси-модуля;
- выполняют в прокси-модуле следующие действия:
  - создают сокет для соединения с клиентом;
  - создают сокет для соединения с сервером, если данный сокет не был создан ранее;
  - создают сокет для виртуального соединения, позволяющего осуществлять взаимодействие между сокетом для соединения с клиентом и сокетом для соединения с сервером;
  - осуществляют фильтрацию сетевого потока данных, передаваемого между клиентом и сервером.

Известный способ принят за прототип.

Известный способ может обеспечить фильтрацию сетевого потока данных, которая, как правило, более функциональная, чем пакетная фильтрация, и при этом не требуется, чтобы специальное программное обеспечение было установлено у клиентов.

Однако, при использовании известного способа не обеспечивается возможность фильтрации потока данных в прокси-модуле только для заданного списка протоколов прикладного уровня и не обеспечивается возможность пакетной фильтрации, что является недостатком и снижает защищенность вычислительной сети.

Раскрытие изобретения

Техническим результатом является повышение защищенности вычислительной сети.

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 протоколов прикладного уровня, для которых необходимо проводить фильтрацию сетевого потока данных, при этом межсетевой экран выполнен с возможностью проводить пакетную фильтрацию и содержит

- операционную систему,
- модуль сетевой трансляции адресов,

• прокси-модуль, имеющий внутренний адрес PR1 и сформированные правила фильтрацию сетевого потока данных для защищаемой сети,

• модуль контроля, выполненное с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня,

• модуль создания сокета TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения, при этом дескриптор указанного пакета при формировании его с помощью операционной системы содержит, по меньшей мере, следующую информацию:

- указатель на данные D пакета;
- флаг, указывающий, что пакет был перенаправлен на прокси-модуль;
- идентификатор протокола прикладного уровня; способ заключается в том, что

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

• если сетевой пакет P1 имеет номер инкапсулированного протокола транспортного уровня, соответствующий номеру протокола UDP, и содержит данные D, то выполняют следующие действия:

- выполняют пакетную фильтрацию для сетевого пакета P1;
- определяют с помощью модуля контроля факт использования в составе данных D протокола прикладного уровня из множества A;
- если факт использования установлен, то выполняют следующие действия:
  - заменяют в сетевом пакете P1 адрес получателя R1 на адрес прокси-модуля PR1 в модуле сетевой трансляции адресов;
  - выполняют фильтрацию сетевого потока в прокси-модуле;
  - обрабатывают данные D в прокси-модуле;
  - если сетевой пакет P1 имеет номер инкапсулированного протокола транспортного уровня, соответствующий номер протокола TCP, и либо установленный флаг SYN, либо установленные флаги SYN и ACK, либо установленный флаг ACK, обозначающий завершение процедуры установления TCP сессии, то выполняют пакетную фильтрацию;

• если сетевой пакет P1 имеет номер инкапсулированного протокола транспортного уровня, соответствующий номер протокола TCP, и содержит данные D, то выполняют следующие действия:

- выполняют для сетевого пакета P1 пакетную фильтрацию;
- определяют с помощью модуля контроля факт использования в составе данных D протокола прикладного уровня из множества A;
- если факт использования установлен, то выполняют следующие действия:
  - станавливают в дескрипторе флаг, указывающий, что сетевой пакет будет перенаправлен на прокси-модуль;
  - заменяют в сетевом пакете P1 адрес получателя R1 на адрес прокси-модуля PR1 в модуле сетевой трансляции адресов;
  - если в дескрипторе установлен флаг, указывающий, что сетевой пакет был перенаправлен на прокси-модуль, то создают сокет TCP соединения для связи отправителя с адресом S1 с прокси-модулем с адресом PR1 в модуле создания сокета TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения;
  - выполняют фильтрацию сетевого потока в прокси-модуле;
  - обрабатывают данные D в прокси-модуле. иначе выполняют пакетную фильтрацию.

Для реализации предложенного способа в состав МЭ должны быть включены модуль контроля, выполненный с возможностью проводить определение используемого в

сетевом соединении протокола прикладного уровня, и прокси-модуль. В общем случае, указанные модули могут быть аппаратными, программно-аппаратными или программными. Для создания указанных модулей должно быть проведено обычное проектирование и изготовлении электронного блока (при выполнении в аппаратном или программно-аппаратном виде) и формирование необходимого программного обеспечения (ПО) с последующим тестированием и установкой в МЭ. Для создания модуля контроля и прокси-модуля в программном виде создается только прикладное ПО, которое затем дополнительно устанавливается в составе прикладного ПО в МЭ. Создание данных модулей может осуществить специалист по проектированию и изготовлению электронной техники и/или специалист по программированию (программист) на основе знания выполняемой средством контроля функции.

Можно отметить, что модуль создания сокета TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения, вполне может быть создан, поскольку создается именно сокет при приеме одного (первого) пакета, а не соединение TCP в целом.

После создания и отладки модуля контроля и прокси-модуля можно приступать непосредственно к реализации предложенного способа.

Для этого с помощью МЭ осуществляют перехват сетевых пакетов для осуществления контроля и фильтрации сетевого трафика в соответствии с заранее заданными правилами, принятыми обычным порядком для защищаемой сети. Для осуществления способа в точке перехвата сетевых пакетов реализуется контроль сетевых пакетов, который включает в себя пакетную фильтрацию и извлечение данных из сетевого пакета и передачу этих данных в модуль контроля, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня. Если установлен факт использования в составе данных Б протокола прикладного уровня из множества А, то принимается решение о перенаправлении сетевого соединения с помощью модуля сетевой трансляции адресов в прокси-модуль. В прокси-модуле осуществляется обработка данных прикладного протокола, включающая в себя фильтрацию сетевого потока данных.

Таким образом, к сетевым пакетам сетевого и транспортного уровня применяется пакетная фильтрация, а к данным, обмен которыми ведется в рамках сетевого соединения по протоколу прикладного уровня из множества А, применяется фильтрация сетевого потока данных.

В результате обеспечивается защита вычислительной сети от несанкционированной передачи информации, так как данный способ позволяет выделить множество А протоколов прикладного уровня, для которых должна быть применена как фильтрация сетевого потока данных, так и пакетная фильтрация на сетевом и транспортном уровнях.

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 контроля в программном виде,

для чего предварительно создается, тестируется и затем инсталлируется в МЭ прикладное ПО в виде программного модуля, выполняющего функции модуля контроля и способного выполнять определение используемого в сетевом соединении протокола прикладного уровня.

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

В качестве прокси-модуля, выполняющего фильтрацию сетевого потока данных, может быть использовано ПО Squid.

В качестве модуля сетевой трансляции адресов может быть использован модуль ядра Linux nf_nat.ko, входящий в состав подсистемы Netfilter ядра Linux.

В качестве модуля создания сокета TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения, может быть использована подсистема ядра syncookies.

В качестве дескриптора сетевого пакета используется структура sk_buff, определенная в ядре Linux.

Анализ сетевых пакетов осуществляется модулем ядра Linux (файл xt_dpi_dnat.ko), который обеспечивает:

• пакетную фильтрацию;

• 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;

• перенаправление сетевого пакета в модуль ядра nf_nat.ko и установку в структуре sk_buff флага, указывающего, что пакет был перенаправлен на прокси-модуль.

Модуль ядра xt_dpi_dnat.ko встраивается в подсистему Netfilter ядра Linux, реализующей функции МЭ, с уровнем приоритета NF_IP_PRI_SELINUX_FIRST, с целью перехвата и анализа транзитных сетевых пакетов.

В пространстве пользователя запускается средство контроля, выполненное 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.

Модуль xt_dpi_dnat.ko осуществляет пакетную фильтрацию и извлекает из сетевого пакета данные прикладного уровня. Извлеченные данные через системный интерфейс netfilter_queue ядра Linux передаются на анализ в средство контроля, которое проводит определение используемого в сетевом соединении протокола прикладного уровня. Полученный результат передается в модуль xt_dpi через системный интерфейс netfilter_queue ядра Linux.

Если установлен факт использования протокола прикладного уровня, к которому должна быть применена фильтрация сетевого потока данных, то модуль xt_dpi_dnat.ko устанавливает в структуре sk_buff специальный флаг, указывающий, что данный пакет перенаправлен на прокси-модуль и перенаправляет сетевой пакет в модуль сетевой трансляции адресов nf_nat.ko.

Модуль сетевой трансляции адресов nf_nat.ko заменяет в обрабатываемом пакете адрес получателя на адрес прокси-модуля.

В случае использования протокола транспортного уровня TCP данный сетевой пакет поступает на обработку в подсистему ядра syncookies, которая при наличии в структуре sk_buff специального флага, указывающего, что данный пакет перенаправлен в прокси-модуль, создает сокет TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения.

В прокси-модуле осуществляется обработка данных соединения, включающая в себя фильтрацию сетевого потока данных.

(57) Формула изобретения

Способ работы межсетевого экрана, причем для межсетевого экрана определено множество A протоколов прикладного уровня, для которых необходимо проводить фильтрацию сетевого потока данных, при этом межсетевой экран выполнен с возможностью проводить пакетную фильтрацию и содержит

операционную систему,

модуль сетевой трансляции адресов,

прокси-модуль, имеющий внутренний адрес PR1 и сформированные правила фильтрации сетевого потока данных для защищаемой сети,

модуль контроля, выполненный с возможностью проводить определение используемого в сетевом соединении протокола прикладного уровня,

модуль создания сокета TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения, при этом дескриптор указанного пакета при формировании его с помощью операционной системы содержит, по меньшей мере, следующую информацию:

указатель на данные D пакета;

флаг, указывающий, что пакет был перенаправлен на прокси-модуль;

идентификатор протокола прикладного уровня; способ заключается в том, что

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

если сетевой пакет P1 имеет номер инкапсулированного протокола транспортного уровня, соответствующий номеру протокола UDP, и содержит данные D, то выполняют следующие действия:

выполняют пакетную фильтрацию для сетевого пакета P1;

определяют с помощью модуля контроля факт использования в составе данных D протокола прикладного уровня из множества A;

если факт использования установлен, то выполняют следующие действия:

заменяют в сетевом пакете P1 адрес получателя R1 на адрес прокси-модуля PR1 в модуле сетевой трансляции адресов;

выполняют фильтрацию сетевого потока данных в прокси-модуле; обрабатывают данные D в прокси-модуле;

если сетевой пакет P1 имеет номер инкапсулированного протокола транспортного уровня, соответствующий номер протокола TCP, и либо установленный флаг SYN, либо установленные флаги SYN и ACK, либо установленный флаг ACK, обозначающий завершение процедуры установления TCP сессии, то выполняют пакетную фильтрацию;

если сетевой пакет P1 имеет номер инкапсулированного протокола транспортного уровня, соответствующий номер протокола TCP, и содержит данные D, то выполняют следующие действия:

выполняют для сетевого пакета P1 пакетную фильтрацию;

определяют с помощью модуля контроля факт использования в составе данных D

протокола прикладного уровня из множества A;

если факт использования установлен, то выполняют следующие действия:

устанавливают в дескрипторе флаг, указывающий, что сетевой пакет будет перенаправлен на прокси-модуль;

заменяют в сетевом пакете P1 адрес получателя R1 на адрес прокси-модуля PR1 в модуле сетевой трансляции адресов;

если в дескрипторе установлен флаг, указывающий, что сетевой пакет был перенаправлен на прокси-модуль, то создают сокет TCP соединения для связи отправителя с адресом S1 с прокси-модулем с адресом PR1 в модуле создания сокета TCP соединения по одному пакету, без проведения процедуры трехэтапного установления TCP соединения;

выполняют фильтрацию сетевого потока данных в прокси-модуле;

обрабатывают данные D в прокси-модуле;

иначе выполняют пакетную фильтрацию.