РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 641 233**(13) **C2**

(51) МПК
H04L 29/06 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
H04L 29/06 (2006.01)

(21)(22) Заявка: **2016108977, 10.06.2014**

(24) Дата начала отсчета срока действия патента:
10.06.2014

Дата регистрации:
16.01.2018

Приоритет(ы):
(30) Конвенционный приоритет:
20.08.2013 CN 201310364450.4

(43) Дата публикации заявки: **28.09.2017** Бюл. № **28**

(45) Опубликовано: **16.01.2018** Бюл. № **2**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **21.03.2016**

(86) Заявка PCT:
CN 2014/079625 (10.06.2014)

(87) Публикация заявки PCT:
WO 2014/173365 (30.10.2014)

Адрес для переписки:
191036, Санкт-Петербург, а/я 24, "НЕВИНПАТ"

(72) Автор(ы):
ГАО Йонгганг (CN),
ЛИ Цзюань (CN)

(73) Патентообладатель(и):
ЗетТиИ Корпорейшн (CN)

(56) Список документов, цитированных в отчете о поиске: **US 2010/0161741 A1, 24.06.2010. CN 101834833 A, 15.09.2010. CN 102333080 A, 25.01.2012.**

(54) СПОСОБ, УСТРОЙСТВО И МАШИНОЧИТАЕМЫЙ НОСИТЕЛЬ ДАННЫХ ДЛЯ ЗАВИСЯЩЕЙ ОТ ПРИЛОЖЕНИЯ ФИЛЬТРАЦИИ ПАКЕТОВ ПРОТОКОЛА ПЕРЕДАЧИ ФАЙЛОВ

(57) Реферат:

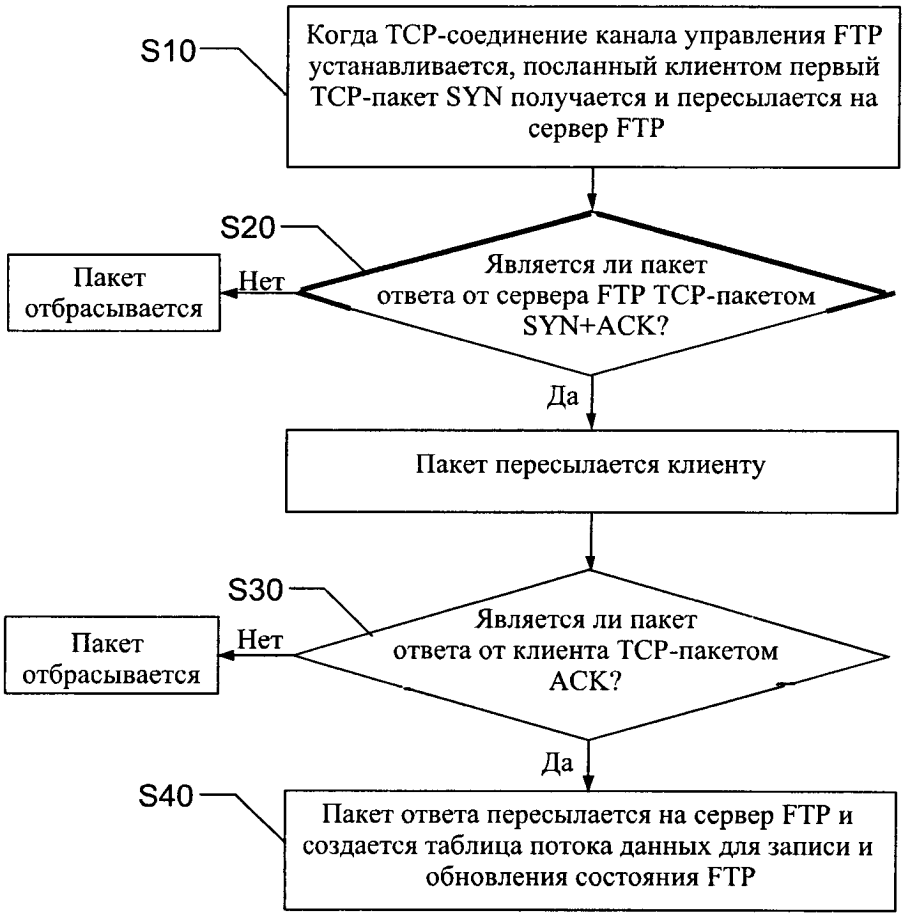
Изобретение относится к технологиям сетевой связи. Технический результат заключается в повышении скорости обработки данных. Способ, включающий: когда устанавливается соединение протокола управления передачей (TCP) канала управления FTP, получение посланного клиентом первого TCP-пакета синхронизации (TCP SYN) и пересылку его на сервер FTP; определение, является ли пакет ответа от сервера FTP TCP-пакетом синхронизации + подтверждения (SYN+ ACK) TCP, и в случае, если пакет ответа от сервера FTP не является TCP-пакетом SYN+ACK, отбрасывание пакета ответа; определение, в случае, если пакет ответа от сервера FTP является TCP-пакетом SYN+ACK, является ли пакет ответа от клиента TCP-пакетом ACK, и в случае, если пакет ответа от клиента не является TCP-пакетом ACK, отбрасывание пакета ответа; и в случае, если пакет ответа от клиента является TCP-пакетом ACK, создание таблицы потока данных для записи и обновления состояния FTP, при этом способ дополнительно включает обнаружение установления связи во время трехэтапного согласования для TCP-пакета канала передачи данных, отслеживание и обнаружение процесса взаимодействия TCP, запись состояния TCP и

RU 2641233 C2

RU 2641233 C2

отказ от передачи пакета данных, не удовлетворяющего протоколу взаимодействия.

3 н. и 6 з.п. ф-лы, 9 ил.



Фиг. 1

RU 2641233 C2

RU 2641233 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 641 233**(13) **C2**

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

(12) ABSTRACT OF INVENTION

(52) CPC
H04L 29/06 (2006.01)

(21)(22) Application: **2016108977, 10.06.2014**

(24) Effective date for property rights:
10.06.2014

Registration date:
16.01.2018

Priority:
(30) Convention priority:
20.08.2013 CN 201310364450.4

(43) Application published: **28.09.2017** Bull. № **28**

(45) Date of publication: **16.01.2018** Bull. № **2**

(85) Commencement of national phase: **21.03.2016**

(86) PCT application:
CN 2014/079625 (10.06.2014)

(87) PCT publication:
WO 2014/173365 (30.10.2014)

Mail address:
191036, Sankt-Peterburg, a/ya 24, "NEVINPAT"

(72) Inventor(s):
GAO Yonggang (CN),
LI Juan (CN)

(73) Proprietor(s):
ZTE Corporation (CN)

RU 2641233 C2

RU 2641233 C2

(54) METHOD, DEVICE, AND COMPUTER-READABLE STORAGE MEDIUM FOR APPLICATION-DEPENDENT FILTERING OF FILE TRANSFER PROTOCOL PACKETS

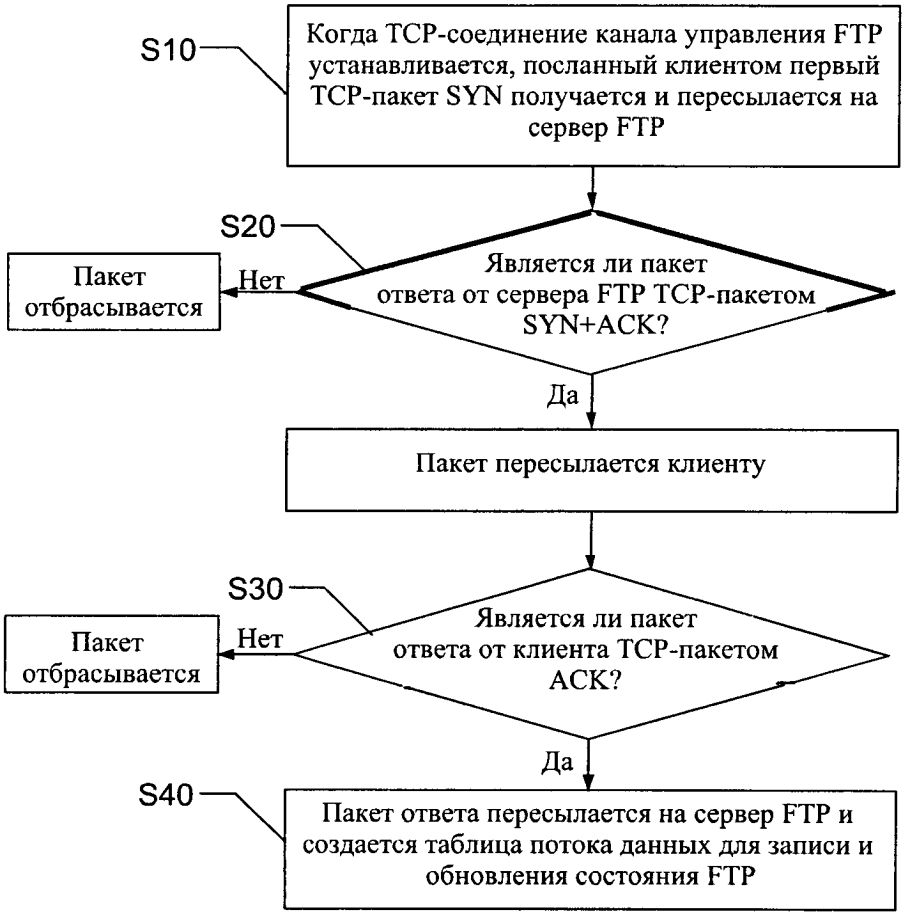
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: method comprising: when a transmission control protocol (TCP) connection of a FTP control channel is established, the receipt of a first TCP sync packet sent by the client (TCP SYN) and sending thereof to the FTP server; determining whether the response packet from the FTP server is a synchronization + acknowledgement (SYN+ACK) TCP/ACK packet (SYN+ACK) TCP, and if the response packet from the FTP server is not a TCP packet SYN+ACK, discarding the response packet; determining if the response packet from the FTP server is a TCP packet SYN+ACK, whether the response packet is from the client by the TCP-ACK packet, and in the case, if the response packet from the client is not a TCP packet ACK, discarding the response packet; and if the response packet from the client is a TCP packet ACK, creating a data stream table for recording and updating the FTP state, wherein the method further comprises detecting a connection establishment during a three-step negotiation for the data transmission channel TCP packet, monitoring and detecting a TCP interaction process, recording a TCP state, and discarding a data packet not satisfying the interaction protocol.

EFFECT: increased data processing rate.

9 cl, 9 dwg



Фиг. 1

RU 2641233 C2

RU 2641233 C2

ОБЛАСТЬ ТЕХНИКИ

Данное изобретение относится к способу для осуществления службы, зависящей от приложения фильтрации пакетов (Application Specific Packet Filter, ASPF) протокола передачи файлов (File Transfer Protocol, FTP) и, в частности, способа, устройства и носителя машиночитаемых данных ASPF на основе FTP.

ПРЕДПОСЫЛКИ СОЗДАНИЯ ИЗОБРЕТЕНИЯ

Протокол передачи файлов (FTP) - один из протоколов в группе протокола управления передачей/протокола Интернет (Transmission Control Protocol / Internet Protocol, TCP/IP). Протокол, который является основой передачи файлов Интернет, состоит из ряда документов спецификации и нацелен на улучшение совместного использования файлов и предоставления возможности носителю данных передавать данные пользователю прозрачно, надежно и эффективно. Проще говоря, протокол FTP осуществляет копирование между двумя компьютерами. Процесс копирования файла с удаленного компьютера на локальный компьютер называется «нисходящей» загрузкой (download) файла, в то время как процесс копирования файла с локального компьютера на удаленный компьютер называется «восходящей» загрузкой (upload) файла. В протоколе TCP/IP стандартный номер порта TCP для передачи команд FTP - 21, а порта для передачи данных в активном режиме - 20. Протокол FTP использует два TCP-соединения для передачи одного файла.

Как правило, соединение управления устанавливается клиентом и сервером. Сервер открывает известный порт (21) для FTP в пассивном режиме и ожидает соединения с клиентом, в то время как клиент открывает TCP-порт 21 в активном режиме, чтобы создать соединение. Соединение управления всегда ожидает связи между клиентом и сервером. Это соединение позволяет передавать команду от клиента на сервер и возвращать ответ от сервера. Так как команда обычно вводится пользователем, особенностью службы IP для соединения управления является "максимальное уменьшение времени задержки". Соединение передачи данных устанавливается каждый раз, когда файл передается между клиентом и сервером. Так как соединение используется для передачи, протокол IP служит для "максимального увеличения пропускной способности" для соединения передачи данных.

С популяризацией компьютерных и сетевых технологий все большее внимание уделяется проблеме сетевой защиты, и получает все большее значение передача файла безопасно и надежно на основе FTP. В качестве механизма защиты для управления передачей файла FTP брандмауэр стал оптимальным вариантом защищенной передачи FTP. Брандмауэр нацелен на установление барьера между надежной сетью и ненадежной сетью, и осуществление соответствующей стратегии защиты. Брандмауэр, применяемый в сети, является чрезвычайно эффективным средством сетевой защиты. Обычно брандмауэр реализуется с помощью технологии фильтрации пакетов.

Ядром технологии фильтрации пакетов является определение правила списка контроля доступа (Access Control List, ACL) для фильтрации пакетов данных. Для пакета данных, который необходимо переслать, брандмауэр с фильтрацией пакетов сначала получает информацию заголовка (включающую номер протокола верхнего уровня, переносимого на уровне IP, и адрес источника, адрес получателя, порт источника и порт получателя пакета данных и так далее) пакета данных, затем сравнивает информацию заголовка с правилом ACL, установленным пользователем, и обрабатывает пакет данных (позволяет пакету данных пройти или отбрасывает пакет данных) согласно результату сравнения.

Преимущества технологии фильтрации пакетов включают то, что фильтрация

происходит только на сетевом уровне, а следовательно, обработка является быстрой. Кроме того, производительность устройства испытывает небольшую нагрузку, особенно в условиях умеренного трафика, а размер сконфигурированного списка ACL является умеренным. Кроме того, технология фильтрации пакетов реализуется прозрачно для приложения верхнего уровня и пользователя, и отсутствует необходимость в установке специального программного обеспечения на хосте пользователя. Хотя технология фильтрации пакетов обладает упомянутыми преимуществами, так как брандмауэр с фильтрацией пакетов проверяет и фильтрует только на сетевом уровне, но не анализирует и не обнаруживает содержимое прикладного уровня пакета, некоторые угрозы от прикладного уровня, такие как атака на учетную запись пользователя в приложении FTP и т.п., не могут быть предотвращены.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

Основной целью данного изобретения является предложить способ, устройство и машиночитаемый носитель данных для фильтрации ASPF FTP, чтобы решить техническую проблему известного уровня техники, заключающуюся в том, что некоторые угрозы прикладного уровня не могут быть предотвращены.

С этой целью форма осуществления данного изобретения предлагает способ для фильтрации ASPF FTP, который включает следующее:

когда TCP-соединение канала управления FTP устанавливается, первый TCP-пакет синхронизации (TCP SYN), посланный клиентом, получается и пересылается на сервер FTP;

определяется, является ли пакет ответа от сервера FTP пакетом синхронизации + подтверждения (SYN+ACK) протокола TCP, и если не является, пакет ответа отбрасывается;

если пакет ответа от сервера FTP является TCP-пакетом SYN+ACK, определяется, является ли пакет ответа от клиента TCP-пакетом ACK, и если не является, пакет ответа отбрасывается; и

если пакет ответа от клиента является TCP-пакетом ACK, создается таблица потока данных, чтобы записывать и обновлять состояние FTP.

Предпочтительно, способ может дополнительно включать следующее:

когда состояние FTP указывает успешное установление TCP-соединения, от клиента требуется передать имя пользователя на сервер FTP;

после получения переданного клиентом имени пользователя блок регистрации состояния FTP уведомляется о необходимости обновить состояние FTP на посланное в команде USER; и от клиента требуется передать пароль на сервер FTP, ожидать пакет подтверждения от сервера и выполнить анализ, успешна ли регистрация;

после успешной регистрации пользователя состояние FTP записывается как успешное установление канала управления, после неудачной регистрации состояние FTP обновляется на успешное установление TCP-соединения и от пользователя требуется выполнение снова верификации имени учетной записи.

Предпочтительно, способ может дополнительно включать следующее:

анализ содержимого пакета команды активного режима (PORT) в канале управления FTP и получение адреса IP и номера порта канала передачи данных;

установление динамического правила пропускания для канала передачи данных согласно адресу IP и номеру порта канала передачи данных, чтобы позволить двум сторонам установить канал передачи данных и передать данные при отказе от пропускания других пакетов, не принадлежащих каналу передачи данных, и после передачи по каналу передачи данных удаление динамического правила пропускания

для канала передачи данных.

Предпочтительно, способ может дополнительно включать следующее:

анализ содержания команды пассивного режима (PASV) и пакета ответа на нее, и получение адреса IP и номера порта канала передачи данных; и

установление согласно адресу IP и номеру порта, полученным из пакета ответа на команду PASV, динамического правила пропускания для канала передачи данных, чтобы позволить передачу данных, используя адрес IP и номер порта.

Предпочтительно, способ может дополнительно включать следующее: обнаружение установления связи во время трехэтапного согласования для TCP-пакета канала передачи данных, отслеживание и обнаружение процесса взаимодействия TCP, запись состояния TCP и отбрасывание передаваемого пакета данных, не удовлетворяющего протоколу взаимодействия.

Форма осуществления данного изобретения далее предлагает устройство для фильтрации ASPF FTP, содержащее блок обнаружения трехэтапного согласования TCP и блок регистрации состояния FTP.

Блок обнаружения трехэтапного согласования TCP сконфигурирован для:

получения, когда устанавливается TCP-соединение канала управления FTP, первого TCP-пакета синхронизации SYN, посланного клиентом, и пересылки его на сервер FTP;

определения, является ли пакет ответа от сервера FTP пакетом SYN+ACK протокола TCP, и если не является, отбрасывания пакета ответа; и

если пакет ответа от сервера FTP является TCP-пакетом SYN+ACK, дополнительного определения, является ли пакет ответа от клиента TCP-пакетом ACK, и если не является, отбрасывания пакета ответа.

Блок регистрации состояния FTP сконфигурирован для создания таблицы потока данных для записи и обновления состояния FTP, если пакет ответа от клиента является TCP-пакетом ACK.

Предпочтительно, устройство может дополнительно содержать:

блок обработки имени пользователя, сконфигурированный так, чтобы, когда состояние FTP указывает успешное установление TCP-соединения, требовать от клиента послать имя пользователя на сервер FTP; и

блок обработки пароля, сконфигурированный так, чтобы уведомлять после получения имени пользователя, посланного клиентом, блок регистрации состояния FTP о необходимости обновить состояние FTP на переданное командой USER; и требовать от клиента передачи пароля на сервер FTP, ожидания пакета подтверждения от сервера и анализа, успешна ли регистрация;

блок регистрации состояния FTP может быть дополнительно сконфигурирован так, чтобы записывать состояние FTP после успешной регистрации пользователя как успешное установление канала управления, после неудачной регистрации обновлять состояние FTP на успешное установление TCP-соединения и требовать от пользователя выполнение снова верификации имени учетной записи.

Предпочтительно, устройство может дополнительно содержать:

блок анализа, сконфигурированный так, чтобы анализировать содержимое пакета команды PORT в канале управления FTP и получать адрес IP и номер порта канала передачи данных;

блок установления правила фильтрации, сконфигурированный так, чтобы устанавливать динамическое правило пропускания канала передачи данных согласно адресу IP и номеру порта канала передачи данных так, чтобы позволять двум сторонам установить канал передачи данных и передать данные при отказе от пропускания

других пакетов, не принадлежащих каналу передачи данных, и после передачи по каналу передачи данных удалять динамическое правило пропускания канала передачи данных.

Предпочтительно, блок синтаксического анализа может быть дополнительно сконфигурирован так, чтобы:

анализировать содержимое команды PASV и пакета ответа на нее и получать адрес IP и номер порта канала передачи данных; и

блок установления правила фильтрации может быть дополнительно сконфигурирован так, чтобы:

устанавливать согласно адресу IP и номеру порта, полученному из пакета ответа на команду PASV, динамическое правило пропускания канала передачи данных, чтобы позволить передачу данных, используя адрес IP и номер порта.

Предпочтительно, устройство может дополнительно содержать блок контроля канала передачи данных, сконфигурированный так, чтобы обнаруживать установление связи во время трехэтапного согласования для TCP-пакета в канале передачи данных, отслеживать и обнаруживать процесс взаимодействия TCP, записывать состояние TCP и отбрасывать пакет данных, не удовлетворяющий протоколу взаимодействия.

Форма осуществления данного изобретения дополнительно предлагает машиночитаемый носитель данных, на котором хранятся выполняемые компьютером команды. Выполняемые компьютером команды используются для выполнения вышеупомянутого способа.

Согласно формам осуществления данного изобретения, TCP-пакет FTP отслеживается и обнаруживается, контролируется, что установление канала управления и канала передачи данных удовлетворяет протоколу TCP с трехэтапным согласованием; и взаимодействие при регистрации между клиентом и сервером в канале управления FTP обнаруживается и контролируется, таким образом отфильтровывается пакет атаки и пакет, не удовлетворяющий протоколу взаимодействия при регистрации; пакет команды PORT, команда PASV и пакет ответа на нее анализируются, чтобы получить адрес IP и номер порта, используемые каналом передачи данных, правило фильтрации канала передачи данных добавляется динамически, и каналу передачи данных, удовлетворяющему правилу, разрешается передать пакет. Посредством вышеупомянутого способа услуга FTP отслеживается, обнаруживается, фильтруется и всесторонне контролируется, таким образом избегая атак на прикладном уровне FTP и гарантируя безопасную и надежную передачу услуги FTP.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Фиг. 1 - блок-схема, показывающая способ для фильтрации ASPF FTP согласно форме осуществления данного изобретения.

Фиг. 2 - блок-схема, показывающая взаимодействие сигнализации в способе для фильтрации ASPF FTP, который показан на фиг. 1.

Фиг. 3 - блок-схема, показывающая способ для фильтрации ASPF FTP согласно другой форме осуществления данного изобретения.

Фиг. 4 - блок-схема, показывающая взаимодействие сигнализации в способе для фильтрации ASPF FTP, который показан на фиг. 3.

Фиг. 5 - блок-схема, показывающая способ для фильтрации ASPF FTP согласно еще одной форме осуществления данного изобретения.

Фиг. 6 - блок-схема, показывающая взаимодействие сигнализации в способе для фильтрации ASPF FTP, который показан на фиг. 5.

Фиг. 7 - структурная схема, иллюстрирующая устройство для фильтрации ASPF FTP

согласно форме осуществления данного изобретения.

Фиг. 8 - структурная схема, иллюстрирующая устройство для фильтрации ASPF FTP согласно другой форме осуществления данного изобретения.

Фиг. 9 - структурная схема, иллюстрирующая устройство для фильтрации ASPF FTP согласно еще одной форме осуществления данного изобретения.

ПОДРОБНОЕ ОПИСАНИЕ

Следует понимать, что описанные здесь конкретные формы осуществления изобретения служат только для объяснения данного изобретения, но не используются для его ограничения.

Данное изобретение предлагает способ для фильтрации ASPF протокола FTP. Как показано на фиг. 1, согласно форме осуществления данного изобретения способ включает следующие шаги:

Шаг 10: когда TCP-соединение канала управления FTP устанавливается, посланный клиентом первый TCP-пакет SYN принимается и пересылается на сервер FTP.

Шаг 20: определяется, является ли пакет ответа от сервера FTP пакетом SYN+ACK протокола TCP, если не является, пакет ответа отбрасывается, если является, пакет ответа пересылается клиенту.

Шаг 30: определяется, является ли пакет ответа от клиента TCP-пакетом ACK, если не является, пакет ответа отбрасывается, если является, пакет ответ пересылается на сервер FTP.

Шаг 40: создается таблица потока данных для записи и обновления состояния FTP.

В частности, как показано на фиг. 2, в форме осуществления данного изобретения, когда клиент 1 посылает первый пакет данных TCP SYN на сервер 2 FTP во время процедуры установления канала управления FTP, устройство 3 фильтрации ASPF FTP создает таблицу потока данных, записывает состояние и пересылает пакет данных TCP SYN на сервер 2 FTP. При обнаружении пакета данных, не являющегося пакетом TCP SYN+ACK, посылаемого в ответ сервером 2 FTP, или пакета данных TCP от другого адреса, устройство 3 фильтрации ASPF FTP отбрасывает такой пакет данных. Если сервер 2 FTP отвечает пакетом данных TCP SYN+ACK, устройство 3 пересылает пакет данных TCP SYN+ACK клиенту 1. Устройство 3 фильтрации ASPF FTP обновляет состояние в таблице потока данных, определяет, является ли пакет ответа от клиента 1 пакетом TCP ACK, и если не является, отбрасывает пакет ответа, а если является, пересылает пакет ответа на сервер 2 FTP. Устройство 3 фильтрации ASPF FTP обновляет состояние в таблице потока данных (например, устройство 3 фильтрации ASPF FTP обновляет состояние в таблице потока данных на TCP_EST, указывающее, что состояние FTP является успешным установлением TCP-соединения).

Как известно, пакет FTP входит в состав TCP-пакета, а TCP-соединение TCP-пакета может быть установлено только трехэтапным согласованием, чтобы использовать соединение для передачи данных. Правильность TCP пакета FTP определяется во время этого трехэтапного согласования согласно протоколу TCP с трехэтапным согласованием во время процедуры установления канала управления FTP в форме осуществления данного изобретения, и состояние соединения FTP TCP во время определения отслеживается и записывается с помощью таблицы потока данных, чтобы фильтровать и удалять те неправильные пакеты, которые не согласованы с взаимодействием по протоколу TCP, таким образом фильтруя неправильные пакеты FTP и реализуя зависящий от приложения фильтр пакетов FTP.

Как показано на фиг. 3, в форме осуществления данного изобретения способ дополнительно включает следующие шаги.

Шаг 50: Когда состояние FTP указывает успешное установление TCP-соединения, от клиента требуется передать имя пользователя на сервер FTP.

Шаг 60: После того, как имя пользователя, переданное клиентом, принимается, блок регистрации состояния FTP уведомляется о необходимости обновить состояние FTP на посланное в команде USER; и от клиента требуется передача пароля на сервер FTP, ожидание пакета подтверждения от сервера и анализ, успешна ли регистрация.

Шаг 70: После успешной регистрации пользователя состояние FTP записывается как успешное установление канала управления, для пользователя с неудачной регистрацией состояние FTP обновляется на успешное установление TCP-соединения и от пользователя требуется снова выполнить верификацию имени учетной записи.

Конкретно, как показано на фиг. 4, в форме осуществления данного изобретения после установления TCP-соединения канала управления FTP состояние FTP соединения записывается как успешное установление TCP-соединения. В данный момент канал управления между клиентом 1 и сервером 2 не был полностью установлен, и сервер 2 FTP должен проверить правильность пользователя. Сервер 2 FTP требует от клиента ввести имя пользователя и пароль для верификации. Состояние соединения канала управления FTP записывается и сохраняется во время выполнения регистрации на сервере 2 FTP клиентом 1. Когда состояние FTP указывает успешное установление TCP-соединения, устройство 3 фильтрации ASPF FTP позволяет клиенту 1 только передать имя пользователя на сервер 2 FTP. После того, как клиент 1 передает имя пользователя, устройство 3 фильтрации ASPF FTP уведомляет блок регистрации состояния FTP о необходимости обновить состояние FTP на посланное в команде USER. В данный момент устройство 3 фильтрации ASPF FTP позволяет клиенту 1 только передать пароль на сервер 2 FTP. После успешной регистрации пользователя устройство 3 фильтрации ASPF FTP записывает состояние FTP как успешное установление канала управления. Для пользователя, который не зарегистрировался успешно, устройство 3 фильтрации ASPF FTP обновляет состояние FTP на успешное установление TCP-соединения и требует от пользователя снова выполнить верификацию имени учетной записи. В форме осуществления данного изобретения все пакеты, не удовлетворяющие взаимодействию протокола FTP во время соединения FTP, отвергаются, таким образом предотвращаются атаки и занятие ресурсов сервера внешним злонамеренным пользователем.

Как показано на фиг. 5, в форме осуществления данного изобретения способ может дополнительно включать следующие шаги.

Шаг 80: Содержимое пакета команды PORT в канале управления FTP анализируется, и получаются адрес IP и номер порта канала передачи данных.

Шаг 90: Динамическое правило пропускания канала передачи данных устанавливается согласно адресу IP и номеру порта канала передачи данных, чтобы позволить двум сторонам установить канал передачи данных и передать данные при отказе от пропускания других пакетов, не принадлежащих каналу передачи данных, и после передачи по каналу передачи данных динамическое правило пропускания канала передачи данных удаляется.

Правило пропускания канала передачи данных является динамическим правилом фильтрации пакетов данных в форме осуществления данного изобретения. В частности, как показано на фиг. 6, канал управления FTP устанавливается формально после того, как клиент 1 посылает пакеты команд USER и PASS на сервер 2 FTP, предоставляет правильное имя пользователя и пароль, и успешно регистрируется на сервере 2 FTP. Устройство 3 фильтрации ASPF FTP обновляет состояние FTP на успешное установление канала управления. После того, как клиент 1 посылает пакет PORT на сервер 2 FTP,

чтобы согласовать канал передачи данных, устройство 3 фильтрации ASPF FTP анализирует информацию в канале передачи данных в пакете PORT, устанавливает динамическое правило пропускания канала передачи данных, позволяет двум сторонам установить канал передачи данных и передать данные при отказе от пропускания других пакетов, не принадлежащих каналу передачи данных, и удаляет динамическое правило пропускания канала передачи данных после передачи данных по каналу передачи данных. В форме осуществления данного изобретения динамическое правило пропускания канала передачи данных может быть в виде списка ACL или других правил фильтрации, чтобы фильтровать недопустимые пакеты данных.

Следует заметить, что вышеприведенная форма осуществления описана в данном изобретении в отношении команды PORT. Данное изобретение применимо также к команде PASV. В форме осуществления данного изобретения способ может дополнительно включать следующие шаги:

содержимое команды PASV и пакета ответа на нее анализируется, и получаются адрес IP и номер порта канала передачи данных; и

динамическое правило пропускания канала передачи данных устанавливается согласно адресу IP и номеру порта, полученному из пакета ответа на команду PASV, чтобы позволить передачу данных, используя адрес IP и номер порта.

В форме осуществления данного изобретения способ может дополнительно включать следующие шаги: установление связи определяется во время трехэтапного согласования для TCP-пакета в канале передачи данных, процесс взаимодействия TCP отслеживается и определяется, состояние TCP записывается, и пакет данных, не удовлетворяющий протоколу взаимодействия, отбрасывается. В форме осуществления данного изобретения процесс, в котором блок 70 контроля канала передачи данных выполняет обнаружение установления связи во время трехэтапного согласования у TCP-пакета в канале передачи данных, является по существу одинаковым с процессом выполнения обнаружения трехэтапного согласования во время процедуры установления канала передачи данных. Форма осуществления данного изобретения определяет также правильность взаимодействия во время трехэтапных согласований TCP для канала передачи данных, таким образом защищая точность и правильность передачи данных и дополнительно осуществляя фильтрацию ASPF FTP.

Кроме того, данное изобретение предлагает устройство для фильтрации ASPF FTP. На фиг. 7 показана структурная схема, иллюстрирующая устройство для фильтрации ASPF FTP в форме осуществления данного изобретения. В данной форме осуществления изобретения устройство 3 фильтрации ASPF FTP содержит: блок 10 обнаружения трехэтапного согласования TCP и блок 20 регистрации состояния FTP. Блок 10 обнаружения трехэтапного согласования TCP сконфигурирован для:

получения, когда TCP-соединение канала управления FTP устанавливается, первого TCP-пакета SYN, посланного клиентом 1, и пересылки его на сервер 2 FTP;

определения, является ли пакет ответа от сервера 2 FTP TCP-пакетом SYN+ACK, и если нет, отбрасывания пакета ответа; и если да, пересылки пакета ответа клиенту 1;

определения, является ли пакет ответа от клиента 1 TCP-пакетом ACK, и если нет, отбрасывания пакета ответа; и если да, пересылки пакета ответа на сервер 2 FTP.

Блок 20 регистрации состояния FTP сконфигурирован так, чтобы создавать таблицу потока данных для записи и обновления состояния FTP.

Конкретно, в форме осуществления данного изобретения, когда клиент 1 посылает первый TCP-пакет данных SYN на сервер 2 FTP во время процедуры установления канала управления FTP, блок 20 регистрации состояния FTP создает таблицу потока

данных, записывает состояние в таблицу потока данных, и блок 10 пересылает TCP-пакет данных SYN на сервер 2 FTP. При обнаружении пакета данных, не являющегося TCP-пакетом данных SYN+ACK, посылаемого в ответ сервером 2 FTP, или пакета данных TCP от другого адреса, блок 10 обнаружения трехэтапного согласования TCP отбрасывает пакет данных, не являющийся TCP-пакетом данных SYN+ACK или являющийся TCP-пакетом данных от другого адреса. Если сервер 2 FTP отвечает TCP-пакетом данных SYN+ACK, блок 10 обнаружения трехэтапного согласования TCP пересылает TCP-пакет данных SYN+ACK клиенту 1. Блок 20 регистрации состояния FTP обновляет состояние в таблице потока данных. Блок 10 обнаружения трехэтапного согласования TCP определяет, является ли пакет ответа от клиента 1 TCP-пакетом ACK, и если нет, отбрасывает пакет ответа, а в ином случае пересылает пакет ответа на сервер 2 FTP. Блок 20 регистрации состояния FTP обновляет состояние в таблице потока данных (например, блок 20 регистрации состояния FTP обновляет состояние в таблице потока данных на TCP_EST, указывающее, что состояние FTP является успешным установлением TCP-соединения).

Как известно, пакет FTP является TCP-пакетом, и TCP-соединение TCP-пакета может быть установлено только трехэтапным согласованием, чтобы использовать соединение для передачи данных. Правильность TCP пакета FTP определяется во время этого трехэтапного согласования согласно протоколу TCP с трехэтапным согласованием во время процедуры установления канала управления FTP в форме осуществления данного изобретения, и состояние TCP-соединения FTP во время определения отслеживается и регистрируются таблицей потока данных, чтобы фильтровать и удалять те недопустимые пакеты, которые не согласуются с взаимодействием по протоколу TCP, таким образом фильтруя недопустимый пакет FTP и осуществляя зависящую от приложения фильтрацию пакетов FTP.

Как показано на фиг. 8, в форме осуществления данного изобретения на основе вышеописанной формы осуществления устройство 3 фильтрации ASPF FTP может дополнительно содержать:

блок 30 обработки имени пользователя, сконфигурированный так, чтобы, когда состояние FTP указывает успешное установление TCP-соединения, требовать от клиента 1 послать имя пользователя на сервер 2 FTP;

блок 40 обработки пароля, сконфигурированный так, чтобы после получения посланного клиентом 1 имени пользователя уведомить блок 20 регистрации состояния FTP о необходимости обновить состояние FTP на посланное в команде USER; и потребовать от клиента 1 послать пароль на сервер 2 FTP, ожидать пакет подтверждения сервера и анализировать, успешна ли регистрация; и

блок 20 регистрации состояния FTP дополнительно сконфигурирован так, чтобы после успешной регистрации пользователя записывать состояние FTP как успешное установление канала управления, для пользователя с неуспешной регистрацией обновлять состояние FTP на успешное установление TCP-соединения, и требовать от пользователя снова выполнить верификацию имени учетной записи.

В форме осуществления данного изобретения после установления TCP-соединения канала управления FTP состояние FTP соединения записывается как успешное установление TCP-соединения. В этот момент канал управления между клиентом 1 и сервером 2 не был полностью установлен, и сервер 2 FTP должен проверить правильность пользователя. Сервер 2 FTP требует от клиента ввести имя пользователя и пароль для верификации. Состояние соединения канала управления FTP записывается и сохраняется во время регистрации на сервере 2 FTP клиентом 1. Когда состояние FTP

указывает успешное установление TCP-соединения, блок 30 обработки имени пользователя позволяет клиенту 1 только послать имя пользователя на сервер 2 FTP. После того, как клиент 1 посылает имя пользователя, блок 40 обработки пароля уведомляет блок регистрации состояния FTP о необходимости обновить состояние FTP на посланное в команде USER. В этот момент блок 40 обработки пароля позволяет клиенту 1 только послать пароль на сервер 2 FTP. После успешной регистрации пользователя блок 20 регистрации состояния FTP записывает состояние FTP как успешное установление канала управления. Для пользователя, который не зарегистрировался успешно, блок 20 регистрации состояния FTP обновляет состояние FTP на успешное установление TCP-соединения и требует от пользователя снова выполнить верификацию имени учетной записи. В форме осуществления данного изобретения все пакеты, не удовлетворяющие взаимодействию протокола FTP в процессе соединения FTP, отвергаются, таким образом предотвращается атака на ресурсы сервера и их захват внешним злонамеренным пользователем.

Как показано на фиг. 9, в форме осуществления данного изобретения на основе вышеописанной формы осуществления устройство 3 фильтрации ASPF FTP может дополнительно содержать:

блок 50 анализа, сконфигурированный так, чтобы анализировать содержимое пакета команды PORT в канале управления FTP и получать адрес IP и номер порта канала передачи данных; и

блок 60 установления правила фильтрации, сконфигурированный так, чтобы устанавливать динамическое правило пропускания канала передачи данных согласно адресу IP и номеру порта канала передачи данных, чтобы позволить двум сторонам установить канал передачи данных и передавать данные при отказе от пропускания других пакетов, не принадлежащих каналу передачи данных, и после передачи по каналу передачи данных удалять динамическое правило пропускания канала передачи данных.

Правило пропускания канала передачи данных в форме осуществления данного изобретения представляет собой динамическое правило фильтрации пакета данных. Канал управления FTP устанавливается формально после того, как клиент 1 посылает пакеты команд USER и PASS на сервер 2 FTP, предоставляет правильное имя пользователя и пароль, и успешно регистрируется на сервере 2 FTP. Блок 20 регистрации состояния FTP обновляет состояние FTP на успешное установление канала управления. После того, как клиент 1 посылает пакет PORT на сервер 2 FTP, чтобы согласовать канал передачи данных, блок 50 анализа анализирует информацию в канале передачи данных в пакете PORT и блок 60 установления правила фильтрации устанавливают динамическое правило пропускания канала передачи данных, позволяет двум сторонам установить канал передачи данных и передать данные при отказе от пропускания других пакетов, не принадлежащих каналу передачи данных, и удаляет динамическое правило пропускания канала передачи данных после передачи по каналу передачи данных. В форме осуществления данного изобретения динамическое правило пропускания канала передачи данных может быть в виде списка ACL или других правил фильтрации для фильтрации недопустимых пакетов данных.

Далее, в форме осуществления данного изобретения устройство 3 фильтрации ASPF FTP может дополнительно содержать: блок 70 контроля канала передачи данных, сконфигурированный так, чтобы выполнять обнаружение установления связи во время трехэтапного согласования для TCP-пакета в канале передачи данных, отслеживать и определять процесс взаимодействия TCP, записывать состояние TCP и отбрасывать

пакеты данных, не удовлетворяющие протоколу взаимодействия. В форме осуществления данного изобретения процесс, в котором блок 70 контроля канала передачи данных выполняет обнаружение установления связи во время трехэтапного согласования в пакете TCP в канале передачи данных, по существу одинаков с процессом выполнения обнаружения установления связи во время трехэтапного согласования во время процедуры установления канала передачи данных. Форма осуществления данного изобретения определяет также правильность взаимодействия трехэтапных согласований TCP для канала передачи данных, таким образом защищает точность и правильность передачи данных и дополнительно реализует фильтрацию ASPF FTP.

Следует заметить, что вышеупомянутая форма осуществления описана в данном изобретение относительно команды PORT. Данное изобретение применимо также к команде PASV. В форме осуществления данного изобретения блок 50 анализа дополнительно сконфигурирован так, чтобы: анализировать содержимое команды PASV и пакета ответа на нее и получать адрес IP и номер порта канала передачи данных; и

блок 60 установления правила фильтрации дополнительно сконфигурирован так, чтобы: устанавливать согласно адресу IP и номеру порта, полученным из пакета ответа на команду PASV, динамического правила пропускания для канала передачи данных, чтобы позволить передачу данных, используя адрес IP и номер порта.

Форма осуществления данного изобретения дополнительно предлагает машиночитаемый носитель данных, на котором хранятся выполняемые компьютером команды. Выполняемые компьютером команды используются для выполнения способов вышеупомянутых форм осуществления.

Описанные выше блоки могут быть реализованы центральным процессором (Central Processing Unit, CPU), цифровым процессором сигналов (Digital Signal Processor, DSP) или программируемой пользователем вентильной матрицей (Field-Programmable Gate Array, FPGA) в электронном устройстве.

Специалистам в данной области техники будет понятно, что формы осуществления данного изобретения могут предоставляться как способы, системы или программные изделия для компьютера. Таким образом, данное изобретение может осуществляться в виде аппаратных средств, программного обеспечения или их комбинации. Кроме того, данное изобретение может применяться в виде программного изделия для компьютера, выполняемого на одном или нескольких пригодных для компьютера носителях данных (включая, в частности, запоминающее устройство на магнитных дисках, запоминающее устройство на оптических дисках и т.п.), содержащих выполняемые компьютером коды программы.

Данное изобретение описано со ссылкой на схемы последовательности операций и/или блок-схемы способов, устройства (системы) и программные изделия для компьютера согласно формам осуществления данного изобретения. Следует понимать, что каждая процедура и/или блок на схемах последовательности операций и/или блок-схемах, и комбинации процедур и/или блоков на схемах последовательности операций и/или блок-схемах, могут быть реализованы командами компьютерной программы. Эти команды компьютерной программы могут подаваться на процессор универсального компьютера, специализированного компьютера, встроенного процессора или других программируемых устройств обработки данных для получения такой машины, чтобы команды, выполняемые с помощью процессора компьютера или других программируемых устройств обработки данных, создавали устройство для реализации функций, определенных в одной или нескольких процедурах схем последовательности

операций или одном или нескольких блоках блок-схем.

Эти команды компьютерной программы могут также храниться в машиночитаемом запоминающем устройстве, которое может заставлять компьютер или другие программируемые устройства обработки данных функционировать определенным способом, чтобы команды, хранящиеся в машиночитаемом запоминающем устройстве, производили промышленное изделие, включающее командное устройство, которое осуществляет функции, определенные в одной или нескольких процедурах схем последовательности операций или в одном или нескольких блоках блок-схем.

Эти команды компьютерной программы также могут загружаться на компьютер или другие программируемые устройства обработки данных, чтобы заставлять выполнять ряд рабочих шагов на компьютере или других программируемых устройствах для выполнения обработки, реализуемый компьютером так, чтобы команды, выполняемые на компьютере или других программируемых устройствах, обеспечивали шаги для осуществления функций, определенных в одной или нескольких процедурах схем последовательности операций или в одном или нескольких блоках блок-схем.

Вышеописанное является только предпочтительными формами осуществления данного изобретения, но не предназначено для ограничения объема данного изобретения. Все эквивалентные структуры или эквивалентные изменения потока данных, сделанные согласно описанию и содержанию прилагаемых чертежей данного изобретения, или любые эквивалентные структуры или эквивалентные изменения процедур, применяемые в других уместных областях техники прямо или косвенно, аналогично включены в объем охраны данного изобретения.

(57) Формула изобретения

1. Способ для зависящей от приложения фильтрации пакетов (ASPF) протокола передачи файлов (FTP), включающий: когда устанавливается соединение протокола управления передачей (TCP) канала управления FTP, получение посланного клиентом первого TCP-пакета синхронизации (TCP SYN) и пересылку его на сервер FTP; определение, является ли пакет ответа от сервера FTP TCP-пакетом синхронизации + подтверждения (SYN+ACK) TCP, и в случае, если пакет ответа от сервера FTP не является TCP-пакетом SYN+ACK, отбрасывание пакета ответа; определение, в случае, если пакет ответа от сервера FTP является TCP-пакетом SYN+ACK, является ли пакет ответа от клиента TCP-пакетом ACK, и в случае, если пакет ответа от клиента не является TCP-пакетом ACK, отбрасывание пакета ответа; и в случае, если пакет ответа от клиента является TCP-пакетом ACK, создание таблицы потока данных для записи и обновления состояния FTP, при этом способ дополнительно включает обнаружение установления связи во время трехэтапного согласования для TCP-пакета канала передачи данных, отслеживание и обнаружение процесса взаимодействия TCP, запись состояния TCP и отказ от передачи пакета данных, не удовлетворяющего протоколу взаимодействия.

2. Способ по п. 1, дополнительно включающий: когда состояние FTP указывает успешное установление TCP-соединения, требование от клиента передать имя пользователя на сервер FTP; после получения переданного клиентом имени пользователя, уведомление блока регистрации состояния FTP о необходимости обновить состояние FTP на переданное командой USER; и требование от клиента передать пароль на сервер FTP, ожидать пакет подтверждения от сервера и выполнить анализ, успешна ли регистрация; и после успешной регистрации пользователя, запись состояния FTP как успешное установление канала управления, обновление состояния FTP как успешное установление TCP-соединения при неудачной регистрации и требование от пользователя

повторно выполнить верификацию имени учетной записи.

3. Способ по п. 2, дополнительно включающий: анализ содержимого пакета управления команды активного режима (PORT) в канале управления FTP и получение адреса протокола Интернет (IP) и номера порта канала передачи данных; и установление динамического правила пропускания для канала передачи данных согласно адресу IP и номеру порта канала передачи данных, так, чтобы позволить двум сторонам установить канал передачи данных и передать данные, отказывая в пропускании других пакетов, не принадлежащих каналу передачи данных, и удаление динамического правила пропускания для канала передачи данных после передачи по каналу передачи данных.

4. Способ по п. 3, дополнительно включающий: анализ содержания команды пассивного режима (PASV) и пакета ответа на нее, и получение адреса IP и номера порта канала передачи данных; и установление согласно адресу IP и номеру порта, полученным из пакета ответа на команду PASV, динамического правила пропускания для канала передачи данных для разрешения передачи данных с использованием упомянутых адреса IP и номера порта.

5. Устройство для зависящей от приложения фильтрации пакетов (ASPF) протокола передачи файлов (FTP), включающее блок обнаружения трехэтапного согласования протокола управления передачей (TCP) и блок регистрации состояния FTP, в котором блок обнаружения трехэтапного согласования TCP сконфигурирован для: когда устанавливается TCP-соединение канала управления FTP, получения первого TCP-пакета синхронизации (TCP SYN), посланного клиентом, и пересылки его на сервер FTP; определения, является ли пакет ответа от сервера FTP TCP-пакетом синхронизации + подтверждения (SYN+ACK), и в случае, если пакет ответа от сервера FTP не является TCP-пакетом SYN+ACK, отбрасывания пакета ответа; и в случае, если пакет ответа от сервера FTP является TCP-пакетом SYN+ACK, определения, является ли пакет ответа от клиента TCP-пакетом ACK, и в случае, если пакет ответа от клиента не является TCP-пакетом ACK, отбрасывания пакета ответа; и блок регистрации состояния FTP сконфигурирован для создания таблицы потока данных для записи и обновления состояния FTP, если пакет ответа от клиента является TCP-пакетом ACK, при этом устройство также содержит блок контроля канала передачи данных, сконфигурированный для обнаружения установления связи во время трехэтапного согласования для TCP-пакета в канале передачи данных, отслеживания и обнаружения процесса взаимодействия TCP, записи состояния TCP и отбрасывания пакетов данных, не удовлетворяющих протоколу взаимодействия.

6. Устройство по п. 5, которое дополнительно содержит: блок обработки имени пользователя, сконфигурированный для требования от клиента послать имя пользователя на сервер FTP, когда состояние FTP указывает успешное установление TCP-соединения; блок обработки пароля, сконфигурированный для уведомления после получения имени пользователя, посланного клиентом, блока регистрации состояния FTP о необходимости обновить состояние FTP на переданное командой USER; и требования от клиента передать пароль на сервер FTP, ожидания пакета подтверждения от сервера и анализа, успешна ли регистрация; и блок регистрации состояния FTP, дополнительно сконфигурированный для записи состояния FTP после успешной регистрации пользователя как успешное установление канала управления, после неудачной регистрации обновления состояния FTP на успешное установление TCP-соединения и требования от пользователя повторно выполнить верификацию имени учетной записи.

7. Устройство по п. 6, которое дополнительно содержит: блок анализа,

сконфигурированный для анализа содержимого пакета команды активного режима (PORT) в канале управления FTP, и получения адреса протокола Интернет (IP) и номера порта канала передачи данных; блок установления правила фильтрации, сконфигурированный для установления динамического правила пропускания канала передачи данных согласно адресу IP и номеру порта канала передачи данных так, чтобы позволять двум сторонам установить канал передачи данных и передать данные, отказывая в пропускании других пакетов, не принадлежащих каналу передачи данных, и удаления динамического правила пропускания канала передачи данных после передачи по каналу передачи данных.

8. Устройство по п. 7, в котором блок анализа дополнительно сконфигурирован для: анализа содержания команды пассивного режима (PASV) и пакета ответа на нее, и получения адреса IP и номера порта канала передачи данных; и блок установления правила фильтрации дополнительно сконфигурирован для: установления согласно адресу IP и номеру порта, полученным из пакета ответа на команду PASV, динамического правила пропускания для канала передачи данных, чтобы позволить передачу данных с использованием упомянутых адреса IP и номера порта.

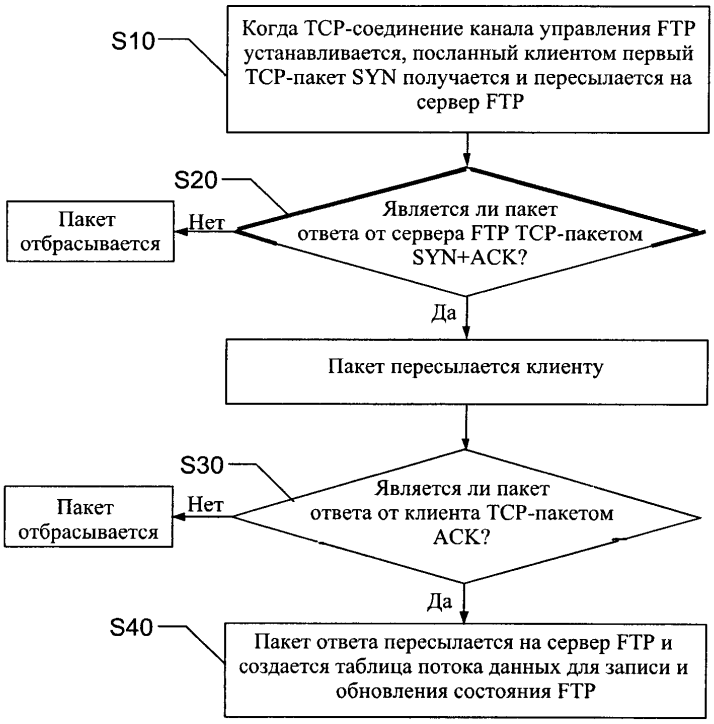
9. Машиночитаемый носитель, на котором хранятся выполняемые компьютером команды, сконфигурированные так, чтобы выполнять способ по какому-либо из пп. 1-4.

1

Способ, устройство и машиночитаемый носитель данных для зависящей от приложения фильтрации пакетов протокола передачи файлов

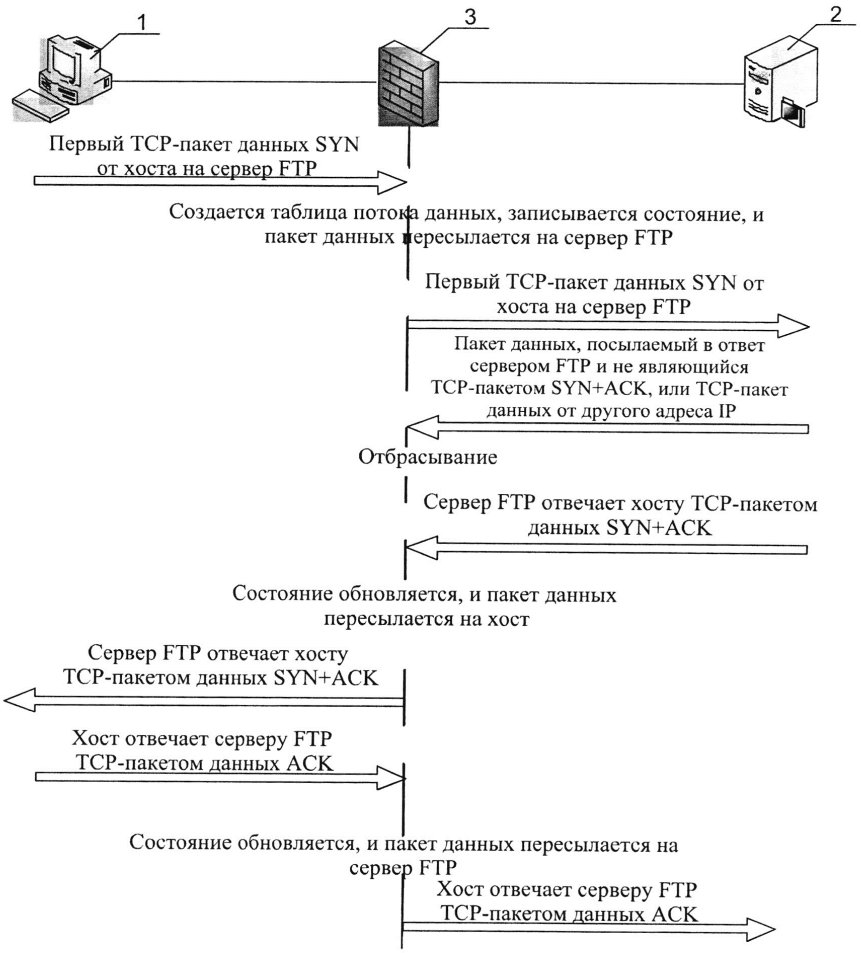
1

Фиг. 1

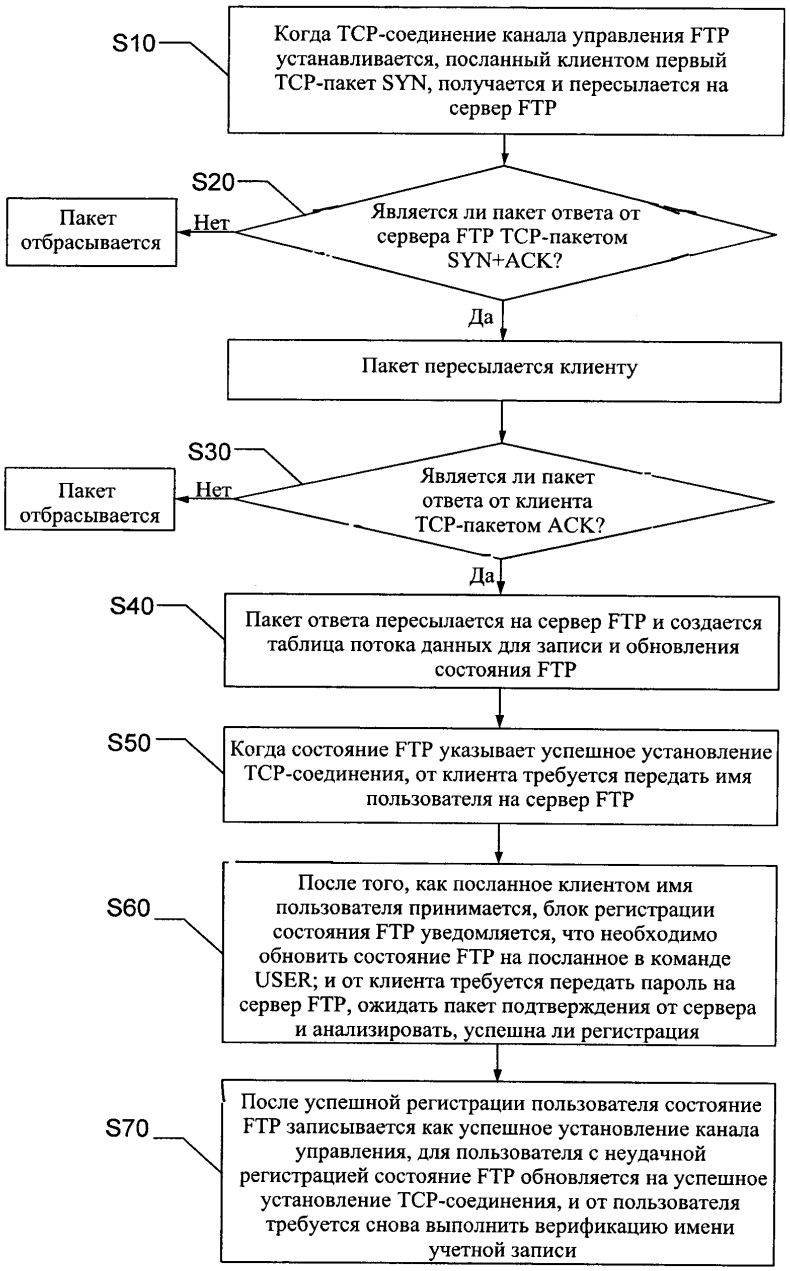


2

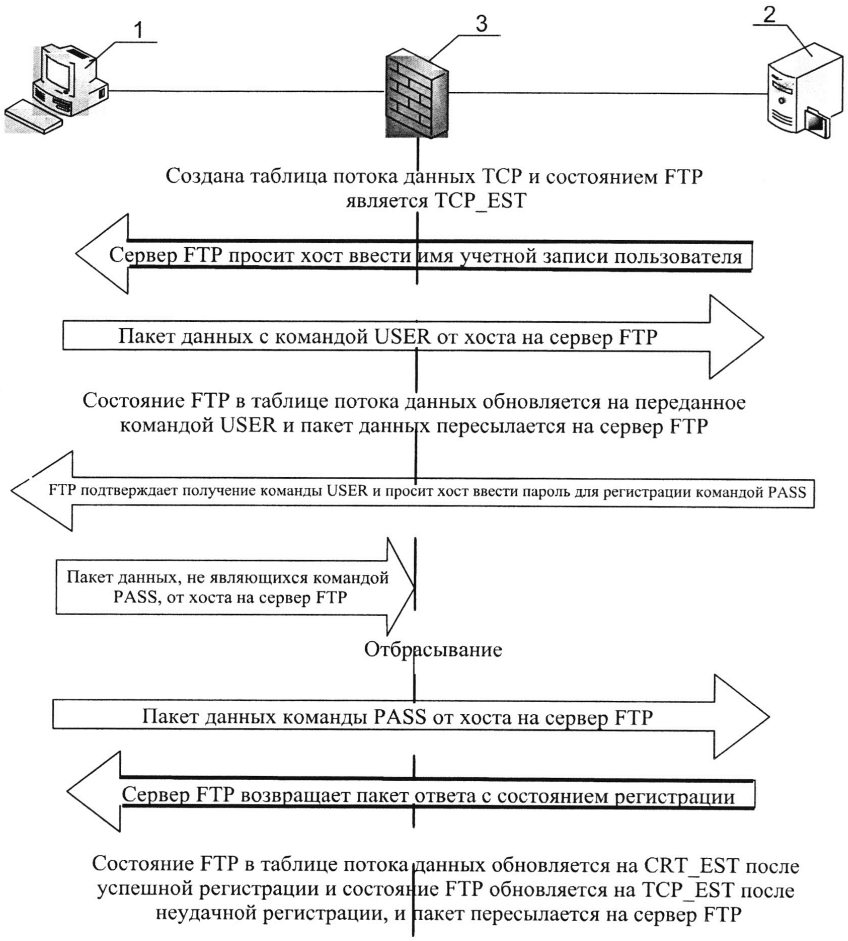
Фиг.2


1
3
2
Первый TCP-пакет данных SYN от хоста на сервер FTP
Создается таблица потока данных, записывается состояние, и пакет данных пересылается на сервер FTP
Первый TCP-пакет данных SYN от хоста на сервер FTP
Пакет данных, посылаемый в ответ сервером FTP и не являющийся TCP-пакетом SYN+ACK, или TCP-пакет данных от другого адреса IP
Отбрасывание
Сервер FTP отвечает хосту TCP-пакетом данных SYN+ACK
Состояние обновляется, и пакет данных пересылается на хост
Сервер FTP отвечает хосту TCP-пакетом данных SYN+ACK
Хост отвечает серверу FTP TCP-пакетом данных ACK
Состояние обновляется, и пакет данных пересылается на сервер FTP
Хост отвечает серверу FTP TCP-пакетом данных ACK

Фиг. 3


S10
Когда TCP-соединение канала управления FTP устанавливается, посланный клиентом первый TCP-пакет SYN, получается и пересылается на сервер FTP
S20
Является ли пакет ответа от сервера FTP TCP-пакетом SYN+ACK?
Нет
Пакет отбрасывается
Да
Пакет пересылается клиенту
S30
Является ли пакет ответа от клиента TCP-пакетом ACK?
Нет
Пакет отбрасывается
Да
S40
Пакет ответа пересылается на сервер FTP и создается таблица потока данных для записи и обновления состояния FTP
S50
Когда состояние FTP указывает успешное установление TCP-соединения, от клиента требуется передать имя пользователя на сервер FTP
S60
После того, как посланное клиентом имя пользователя принимается, блок регистрации состояния FTP уведомляется, что необходимо обновить состояние FTP на посланное в команде USER; и от клиента требуется передать пароль на сервер FTP, ожидать пакет подтверждения от сервера и анализировать, успешна ли регистрация
S70
После успешной регистрации пользователя состояние FTP записывается как успешное установление канала управления, для пользователя с неудачной регистрацией состояние FTP обновляется на успешное установление TCP-соединения, и от пользователя требуется снова выполнить верификацию имени учетной записи

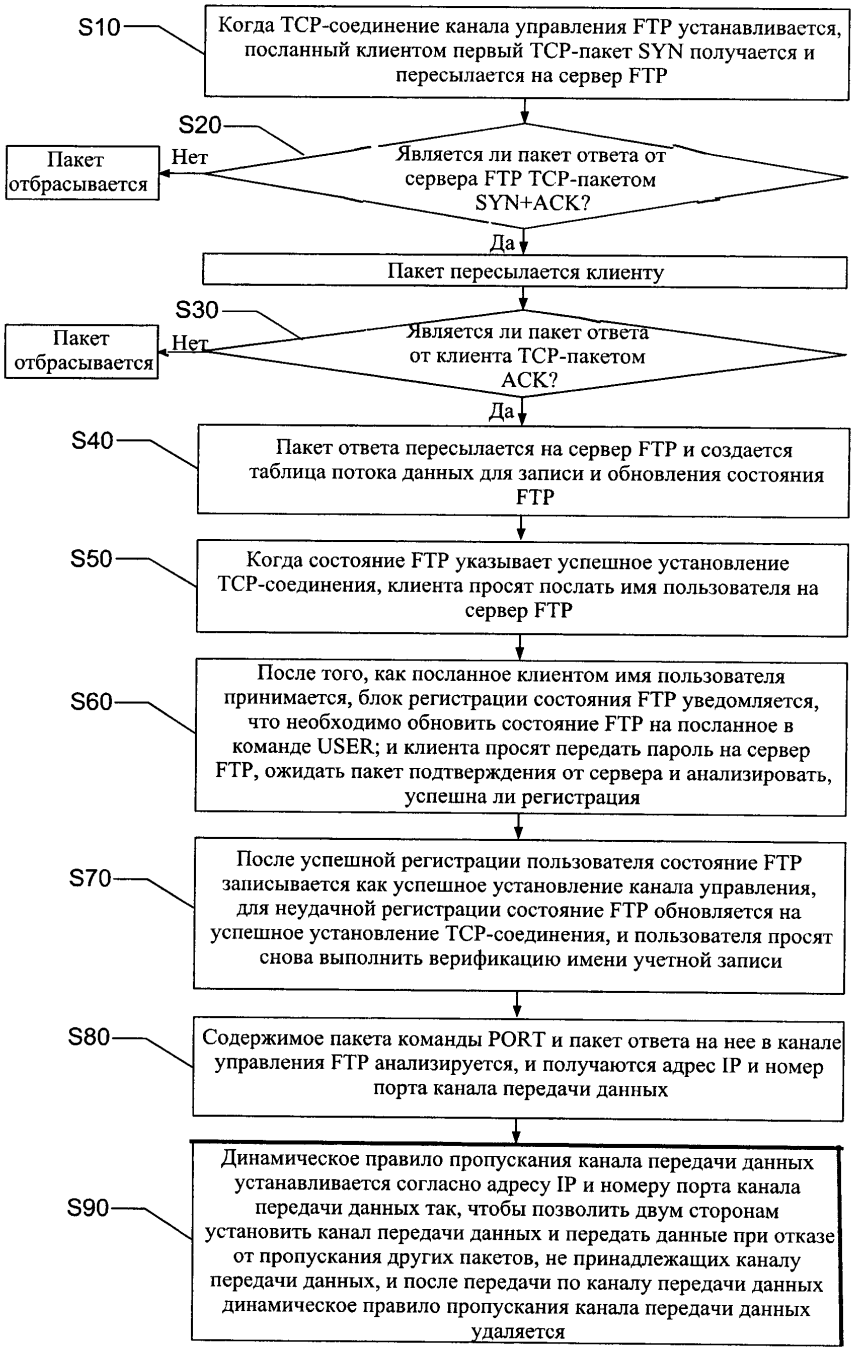
Фиг. 4


1
3
2
Создана таблица потока данных TCP и состоянием FTP является TCP_EST
Сервер FTP просит хост ввести имя учетной записи пользователя
Пакет данных с командой USER от хоста на сервер FTP
Состояние FTP в таблице потока данных обновляется на переданное командой USER и пакет данных пересылается на сервер FTP
FTP подтверждает получение команды USER и просит хост ввести пароль для регистрации командой PASS
Пакет данных, не являющихся командой PASS, от хоста на сервер FTP
Отбрасывание
Пакет данных команды PASS от хоста на сервер FTP
Сервер FTP возвращает пакет ответа с состоянием регистрации
Состояние FTP в таблице потока данных обновляется на CRT_EST после успешной регистрации и состояние FTP обновляется на TCP_EST после неудачной регистрации, и пакет пересылается на сервер FTP

Способ, устройство и машиночитаемый носитель данных для зависящей от приложения фильтрации пакетов протокола передачи файлов

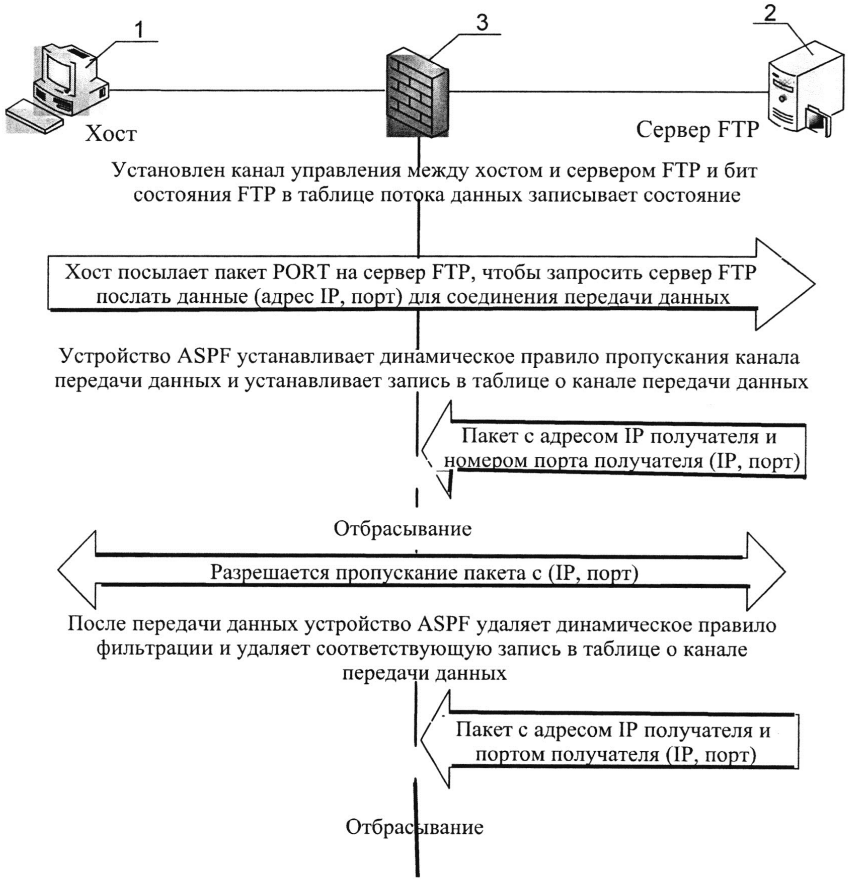
5

Фиг.5

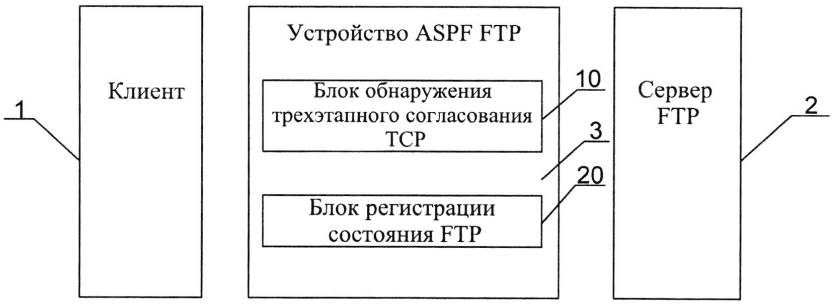


6

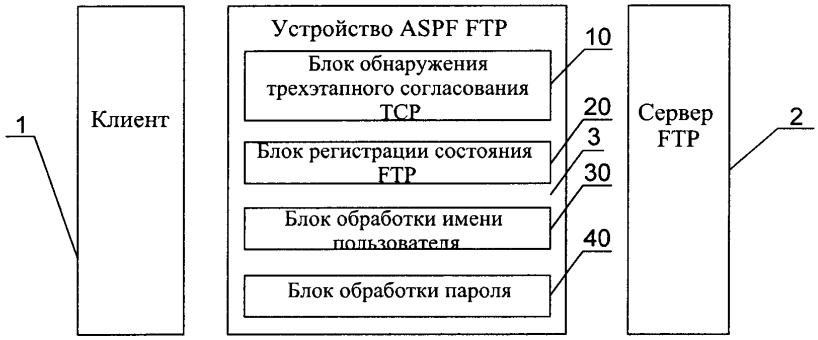
Фиг. 6


1
3
2
Хост
Сервер FTP
Установлен канал управления между хостом и сервером FTP и бит состояния FTP в таблице потока данных записывает состояние
Хост посылает пакет PORT на сервер FTP, чтобы запросить сервер FTP послать данные (адрес IP, порт) для соединения передачи данных
Устройство ASPF устанавливает динамическое правило пропускания канала передачи данных и устанавливает запись в таблице о канале передачи данных
Пакет с адресом IP получателя и номером порта получателя (IP, порт)
Отбрасывание
Разрешается пропускание пакета с (IP, порт)
После передачи данных устройство ASPF удаляет динамическое правило фильтрации и удаляет соответствующую запись в таблице о канале передачи данных
Пакет с адресом IP получателя и портом получателя (IP, порт)
Отбрасывание

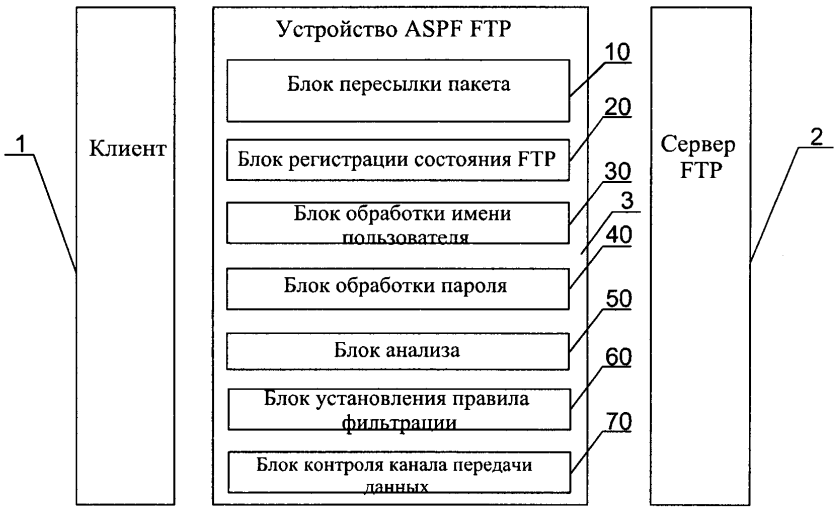
Фиг. 7


1
Клиент
Устройство ASPF FTP
Блок обнаружения трехэтапного согласования TCP
Блок регистрации состояния FTP
10
3
20
Сервер FTP
2

Фиг. 8


1
Клиент
Устройство ASPF FTP
Блок обнаружения трехэтапного согласования TCP
Блок регистрации состояния FTP
Блок обработки имени пользователя
Блок обработки пароля
10
20
3
30
40
Сервер FTP
2

Фиг. 9


1
Клиент
Устройство ASPF FTP
Блок пересылки пакета
Блок регистрации состояния FTP
Блок обработки имени пользователя
Блок обработки пароля
Блок анализа
Блок установления правила фильтрации
Блок контроля канала передачи данных
10
20
30
3
40
50
60
70
Сервер FTP
2