ISSN 1815-4840
CHEMICAL TECHNOLOGY. CONTROL AND MANAGEMENT
2018, №1-2 (79-80) pp.151-156
International scientific and technical journal
journal homepage: ijctcm.com
Since 2005

УДК 004.056, 004.051

M.M.KARIMOV, SH.R.GULYAMOV, S.M.SAGATOVA

WORK OF FIREWALL IN SPECIAL FILTRATION OF TRAFFIC

Трафикни махсус фильтрлашда тармоқлараро экраннинг ишлаши амалий, транспорт ва тармоқ протоколлари учун тармоқ адреслари трансляциясини таъминлаш, байроқларнинг нотўғри ўрнатилиши билан боғлиқ ҳужумларни блоклаш ва протоколлар бўйича пакетларни алмашиниш жараёнининг назоратини ҳисобга олган ҳолда тармоқ трафиги ҳимояланганлигини оширишга бағишланган. Амалий, транспорт ва тармоқ протоколлари учун тармоқ манзиллари трансляцияси маълумотларни узатишда пакетларни йўқолишини камайтиради, яъни пакетлар йўқолишини камайиши, бузғунчи томонидан ҳужум ва таҳдидларни амалга оширишни пасайиб кетишига имкон яратади.

Таянч сўзлар: *пакетларни фильтрлаш, сессиялар назорати, тармоқ адресларининг трансляцияси, MAC-адрес, ARP-қоидалар жадвали, амалий қоидалар жадвали.*

Проанализировано функционирование межсетевого экрана (МЭ) в специальной фильтрации трафика, позволяющая повысить защищенность сетевого трафика с учетом контроля процесса обмена пакетов по протоколам, блокировки атак, связанных с некорректной установкой флагов и обеспечения трансляции сетевых адресов для прикладных, транспортных и сетевых протоколов. Трансляция сетевых адресов для прикладных, транспортных и сетевых протоколов уменьшает потери пакетов при передаче данных, то – есть при уменьшении потерь пакетов реализация угроз и атак со стороны злоумышленника снижается.

Ключевые слова: *фильтрация пакетов, контроль сессии, трансляция сетевых адресов, MAC-адрес, таблица ARP правил, таблица прикладных правил.*

This article is devoted to the functioning firewall on special traffic filtering, which allows to increase the security of network traffic, taking into account the control over the process of packet exchange by protocols, blocking attacks associated with improperly setting flags, and providing network address translation for application, transport and network protocols. Network address translation for application, transport and network protocols reduces packet loss when data is transmitted, that under decrease packet loss, the implementation of threats and attacks from the attacker is reduced.

Keywords: *packet filtering, control session, network address translation, MAC-address, ARP rule table, application rule table.*

Функционирование межсетевого экрана (МЭ) в специальной фильтрации трафика осуществляется в трёх режимах:

- фильтрация пакетов;
- контроль сессии;
- трансляция сетевых адресов.

Во все этих режимах включена функция зеркалирования трафика.

Фильтрация пакетов. Специальная фильтрация трафика в режиме фильтрации пакетов обрабатывает каждый пакет на канальном, сетевом и транспортном уровнях и каждый пакет проверяется на соответствие правилам фильтрации. На рис.1.1. приведена схема фильтрации пакетов в специальной фильтрации трафика.

Таблица MAC правил. Параметры пакета анализируются в таблице MAC правил по следующим критериям:

- тип полученного Ethernet-кадра;
- MAC-адреса отправителя и получателя;
- инкапсулированный протокол;

▪ поля код организации (OUI);

▪ номер виртуальной локальной сети.

По завершению анализа определяется правило, соответствующее конкретному пакету. Исходя их этого правила, осуществляется дальнейшая обработка пакета по сюжетам:

−если правилом задано удаление пакета – пакет не передается ни на один из фильтрующих интерфейсов;

−если правилом задана передача пакета на выходные интерфейсы – пакет передается на указанные в правиле выходные интерфейсы;

−если правилом задана дальнейшая обработка пакета – пакет передается на следующие уровни обработки в соответствии с типом инкапсулированного протокола:

1. ARP пакет – в таблицу ARP-правил,
2. IP пакет – в таблицу IP-правил,
3. IPX пакет – в таблицу IPX-правил.

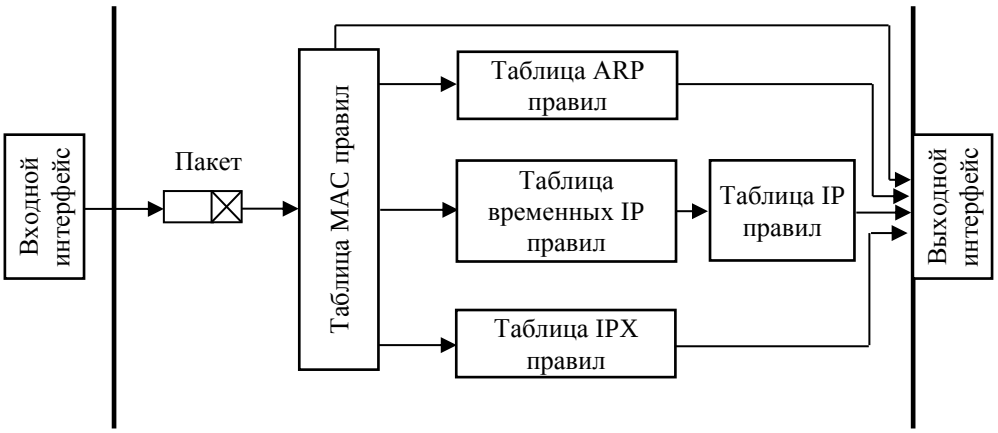

Рис.1.1. ***Схема фильтрации пакетов в специальной фильтрации трафика.***

В ситуации, когда пакеты не содержат протоколы ARP, IP или IPX, пакеты будут переданы на указанные в MAC-правиле выходные интерфейсы без дальнейшей обработки.

Таблица ARP правил. В случае если принятый пакет содержит протокол ARP, происходит обработка пакета в таблице ARP-правил, в которой анализируются следующие параметры пакета:

−MAC-адреса отправителя и получателя заголовка ARP;

−IP-адреса отправителя и получателя заголовка ARP;

−тип запроса;

−номер виртуальной локальной сети, к которой принадлежит данный пакет.

Таблица временных IP правил. Если принятый пакет содержит протокол IP, то, соответственно, обработка пакета будет производиться в таблице временных IP-правил, в которой будут анализироваться следующие параметры пакета:

−протокол транспортного уровня;

−IP-адреса отправителя и получателя;

−порты отправителя и получателя.

В случае, если в результате обработки пакетов в таблице временных IP-правил выявляется правило, соответствующее данному пакету, этот пакет не будет передан ни на один из фильтрующих интерфейсов и на этом обработка данного пакета завершится. Также таблица временных IP-правил может не содержать никаких правил фильтрации, в такой ситуации пакет будет передан на обработку в таблицу IP-правил.

Таблица IP правил. В таблице IP-правил происходит анализ пакета по следующим параметрам:

- анализируется протокол транспортного уровня;
- анализируется IP-адреса отправителя и получателя;
- анализируется поля флагов заголовка IP пакета;
- анализируется поля типа сервиса заголовка IP пакета;
- анализируется поля времени жизни заголовка IP пакета;
- анализируется длина IP пакета;
- анализируется TCP/UDP порты отправителя и получателя;
- анализируется тип и код ICMP-сообщения;
- анализируется номер виртуальной локальной сети, к которой принадлежит пакет.

Таблица IPX правил. В ситуации, когда принятый пакет содержит протокол IPX, осуществляется обработка пакета по следующим критериям:

- адреса сетей и хостов, как отправителя, так и получателя;
- тип пакета;
- сокеты отправителя и получателя;

номер виртуальной локальной сети, к которой принадлежит данный кадр.

Контроль сессии. Контроль сессии – это процесс дополнительной проверки пакета на соответствие текущему состоянию сессии, к которой принадлежит данный пакет.

Таблица IP-правил в контроль сессии. Контроль сессии может быть реализован на базе таблицы IP-правил следующим образом:

- контроль работы виртуального TCP-соединения: каждый пакет будет сверяться на соответствие контексту текущей сессии;
- контроль процесса обмена пакетами по протоколу UDP: пакеты пройдут проверку на соответствие контексту текущей сессии. Важным условием является контроль неизменности параметров UDP-сессии;
- блокировка атак, связанных с некорректной установкой флагов и последовательностей TCP протокола;
- автоматическое открытие клиентских портов, необходимых для текущей сессии.

Таблица вектор состояния. При этом пропускная способность МЭ возрастает, в силу того, что полной проверке по всем правилам фильтрации подвергается только первый пакет сессии, а все последующие пакеты открытой сессии проверяются только на соответствие вектору состояния сессии. На рис.1.2. приведена схема контроля сессии в специальной фильтрации трафика.

Контроль сессии производит поиск на наличие сессии в таблице, соответствующей принятому пакету. Если таковое не обнаружено, пакет будет передан на анализ уже в таблицу IP-правил.

Таблица сессии. В том случае, когда в таблице сессии имеется активная сессия, пакет будет передан на обработку и представляется в следующем порядке:

- MAC адрес, IP-адрес и порты сторон;
- номера родительской и дочерней сессий;
- текущее состояние сессии;
- протокол транспортного и прикладного уровней;
- номера TCP-последовательностей для принятого пакета;
- имя пользователя, которому принадлежит данная сессия;
- идентификатор ICMP протокола, эхо-запрос и эхо-ответ;
- номер порта трансляции при использовании режима NAT.

Таблица прикладных правил. Если все параметры пакета соответствуют контексту сессии, тогда пакет будет отправлен на обработку в таблицу прикладных правил, при условии, что параметр «Использование прикладных правил» включен и в IP-правило, по которой создавалась сессия, задан набор прикладных правил для последующей обработки. Прикладные правила фильтрации расположены в таблице прикладных протоколов (ПП). Таблица ПП-правил по

умолчанию ничего не содержит, глобального правила в таблице ПП-правил нет. Так, что прикладные протоколы фильтруются по следующим условиям:

−не обнаружен список прикладных правил, тогда пакет передается на выходной интерфейс;

−для прикладных протоколов HTTP, HTTPS, SMTP, FTP и распределенных СУБД идентификация прикладного протокола происходит независимо от известного порта сервиса;

−произвольная ASCII-строка длиной до 250 символов;

−произвольная двоичная информация длиной до 16 байт.

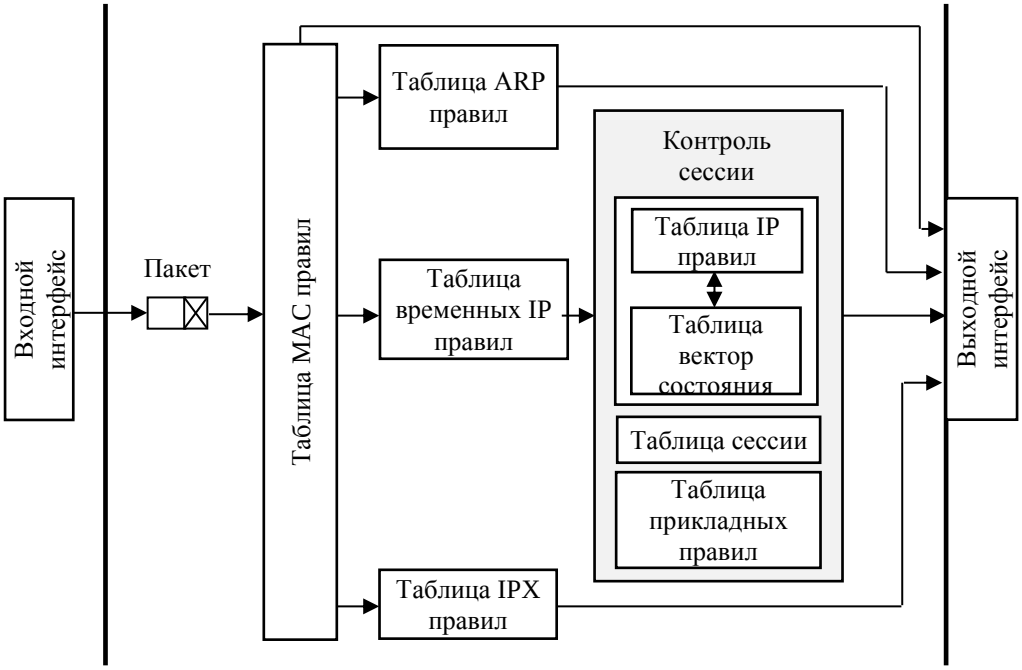

Рис. 1.2. ***Схема контроля сессии в специальной фильтрации трафика.***

Трансляция сетевых адресов. Специальная фильтрация трафика в режиме трансляции сетевых адресов обеспечит:

−сокрытие структуры внутренней сети посредством разграничения доступа из внешней сети. Таким образом, во внутреннюю сеть пропускаются только те пакеты, которые принадлежат к сессиям, уже находящимся в таблице сессий. Пакет из внешней сети без соответствующей сессии будет просто удален;

−экономию пространства IP-адресов: внутренняя сеть с такой реализацией использует лишь один внешний IP – адрес для обращения к ресурсам внешней сети. В отличие от других режимов фильтрации в данном режиме фильтрующие интерфейсы отличаются по своему назначению:

−интерфейс 0-внешний;

−интерфейс 1-внутренний;

−демилитаризованная зона.

Пакеты всех других протоколов не будут переданы из внутренней сети во внешнюю сеть. На рис.1.3. приведена схема трансляции сетевых адресов в специальной фильтрации трафика. Специальная фильтрация трафика обеспечивает трансляцию сетевых адресов для следующих протоколов и процессов:

−TCP протокол;

−UDP протокол;

−ICMP протокол - сообщения типа эхо-запрос и эхо-ответ;

−FTP протокол. Автоматическое открытие портов;

−Антиспуфинг. Предотвращение сетевых атак посредством подмены IP-адреса отправителя на IP-адрес из доверенной сети.

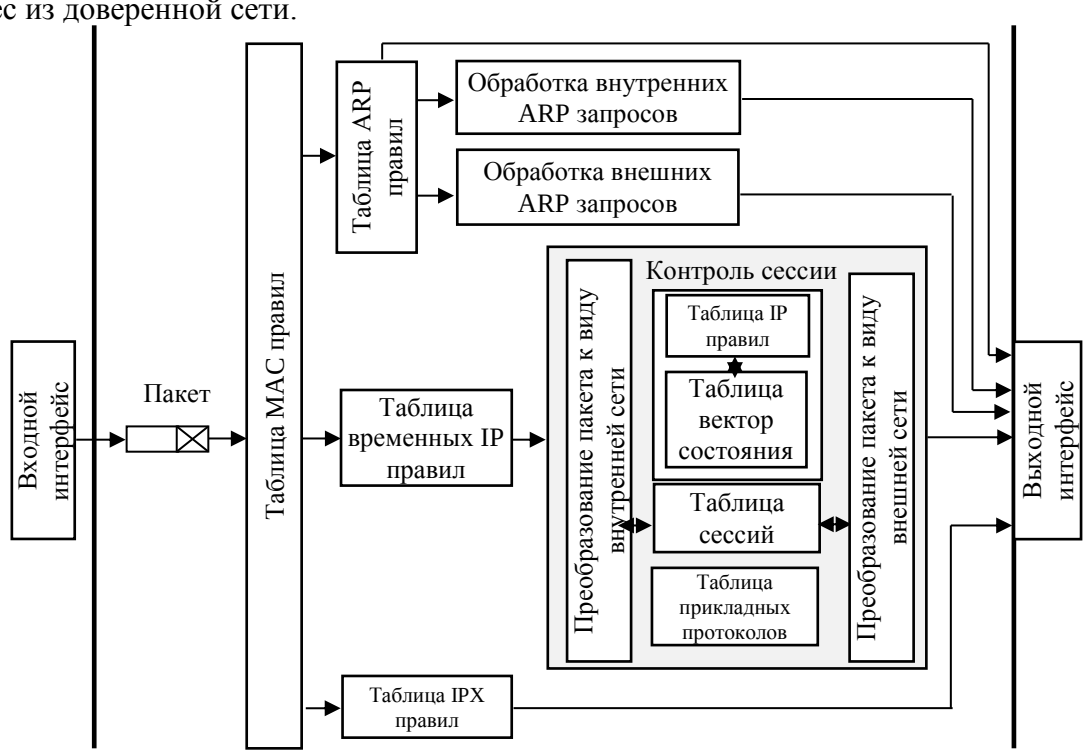

Рис. 1.3. ***Схема трансляции сетевых адресов в специальной фильтрации трафика.***

Обработка внутренних ARP запросов:

−ARP-запрос к IP-адресу внутреннего интерфейса и ARP-ответ от имени IP-адреса внутреннего интерфейса генерируется с указанием MAC-адреса внутреннего интерфейса;

−во всех остальных случаях ARP-пакет удаляется.

Обработка внешних ARP запросов:

−ARP-запрос к IP-адресу внешнего интерфейса и ARP-ответ от имени IP-адреса внешнего интерфейса генерируется с указанием MAC-адреса внешнего интерфейса;

−во всех остальных случаях ARP-пакет передается на заранее заданные выходные интерфейсы, за исключением внутреннего интерфейса.

Механизм контроля сессиями в режиме трансляции сетевых адресов выполняет следующие действия:

1. Определение пакетов, предназначенных для передачи во внутреннюю сеть. К таким пакетам относятся перечисленные далее пакеты, принятые на внешний интерфейс или на интерфейсы демилитаризованной зоны:

−IP-пакеты с адресом получателя, равным IP-адресу внешнего интерфейса;

−IP-пакеты с адресом получателя, равным IP-адресу внешнего интерфейса, на который был получен данный пакет, получивший разрешение.

2. Определение пакетов, предназначенных для передачи во внешнюю сеть или в демилитаризованную зону и для последующего преобразования к виду пакета внешней сети. К такой классификации относятся пакеты, принадлежащие установленной ранее сессии. Пакеты, не установленной ранее сессии, будут удалены. Пакеты отправляются на обработку в блок преобразования пакетов к виду внешней сети. После обработки в данном блоке, пакеты будут переданы на выходные интерфейсы.

Во время преобразования пакета к виду внутренней сети, пакеты преобразуются следующим образом:

−если пакет принадлежит открытой ранее сессии, информация о внутреннем хосте извлекается из информации о данной сессии, хранящейся в таблице сессий;

−если пакет соответствует одному из правил переадресации, информация о IP-адресе и TCP-порте внутреннего хоста извлекается из правила переадресации, информация о MAC-адресе внутреннего хоста извлекается из ARP-таблицы.

После преобразования пакетов к виду внутренней сети, выполняется подмена параметров пакета:

−MAC-адрес отправителя заменяется на MAC-адрес внутреннего интерфейса;

−MAC-адрес получателя заменяется на полученный MAC-адрес внутреннего хоста;

−IP-адрес получателя заменяется на полученный IP-адрес внутреннего хоста;

−порт получателя заменяется на полученный номер порта внутреннего хоста;

−идентификатор для протокола ICMP заменяется на полученное значение идентификатора внутреннего хоста.

В процессе приведения пакета к виду внешней сети, пакеты преобразуются следующим образом:

−из ARP-таблицы извлекается MAC-адрес получателя, соответствующий IP-адресу отправителя;

−в случае, если пакет является первым в сессии, для данной сессии назначается значение идентификатора;

−в случае, если пакет не является первым в сессии, информация о значении идентификатора берется из таблицы сессий.

После преобразования пакетов к виду внешней сети, выполняется подмена параметров пакета:

−MAC-адрес отправителя подменяется на MAC-адрес внешнего интерфейса;

−MAC-адрес получателя подменяется на полученный MAC-адрес;

−IP-адрес отправителя подменяется на IP-адрес внешнего интерфейса;

−порт источника подменяется на полученное значение подставного порта;

−идентификатор для протокола ICMP подменяется на полученное значение подставного идентификатора.

Функционирование МЭ в специальной фильтрации трафика позволяет интегрировать все режимы фильтрации в одной подсистеме. Интеграция режимов фильтрации дает возможность повысить защищенность сетевого трафика и уменьшить потери пакетов при передаче данных, а это приводит к тому, что реализация угроз и атак со стороны злоумышленника снижается.

References:

1. Akram Hakiri, Aniruddha Gokhale, Pascal Berthou, Douglas C. Schmidt, Thierry Gayraud, Software-Defined Networking: International Journal of Pure and Applied Mathematics Special Issue 116 Challenges and research opportunities for Future Internet, Computer Networks 75 (2014), - r.r. 453-471.
2. Gol'dshteyn B. S. Protokoly' seti dostupa. Tom 2. izdanie 3e - SPb.: BHVPeterburg, 2014. - 288s.
3. M.M. Karimov, SH.R. Gulyamov, M.M. Sagatov. Matematicheskaya model' special'noy fil'tracii trafika. Himicheskaya tehnologiya. Kontrol' i upravlenie. Mejdunarodny'y nauchno-tehnicheskiy jurnal №3/2017. Tashkent, - s.74-81.
4. Anna Giannakou, Louis Rilling, Christine Morin, Jean-Louis Pazat. AL-SAFE: A Secure Self-Adaptable Application-Level Firewall for IaaS Clouds. SEC2 2016 - Second workshop on Security in Clouds, Lorient, France. Jul 2016.

Каримов Маджит Маликович – доктор технических наук, профессор, директор Государственного тестового центра Республики Узбекистан. Тел: (998 71) 235-19-14, E-mail: dr.mmkarimov@rambler.ru;
Гулямов Шерзод Ражабоевич – PhD, Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий. Тел: (998 71) 238-65-09, E-mail: sherhisor30@gmail.com;
Сагатова Севара Миразизовна – Ташкентский государственный технический университет имени Ислама Каримова, магистрантка факультета "Электроника ва автоматика". Тел: (998 71) 246-86-22, (998 94) 684-99-35 (м.), E-mail: mssagatova@mail.ru.