УДК 004.056.53

А.Т. Рахманов, Ш.К. Камалов, К.Ф. Керимов

МЕХАНИЗМ ТРЕХСЛОЙНОЙ ЗАЩИТЫ НА ОСНОВЕ ВЕБ-СЕРВЕРОВ ПРОТИВ РАСПРЕДЕЛЕННОГО ОТКАЗА ОТ ОБСЛУЖИВАНИЯ

Ключевые слова: распределенные DOS-атаки, выявление угроз, трехслойный механизм, математическая модель, незаконный трафик, TTL, веб-серверы.

Введение

Признано, что атаки с распределенным отказом в обслуживании (DDoS) могут нарушить веб-сервис и привести к большим потерям доходов, таким как Yahoo, CNN, Amazon и E * Trade в начале 2000 года. Атаки DDoS ограничивают и блокируют законных пользователей для доступа к веб-серверам путем исчерпания ресурсов жертвы или для насыщения сетей доступа к сети с доступом к Интернету. Поскольку используются системные утечки и скрытая проблема безопасности, данная атака обладает характеристиками естественного поведения и ее сложно заблокировать. Исследование механизма безопасности защиты DDoS-атак стало «горячей точкой» в области сетевой безопасности.

Из анализа связанных работ следует, что предлагаемый механизм [1], который вероятностно оценивает пакеты с помощью маршрутизаторов, позволяет собирать маркированные пакеты и восстанавливать путь атаки, а также предлагается расширенная схема вероятностной маркировки пакетов [2], чтобы уменьшить ложную положительную скорость для восстановления пути атаки. Предложена еще одна усовершенствованная схема вероятностной маркировки пакетов для уменьшения вычислительных накладных расходов [3].

Предоставляется схема трассировки ICMP [4], которая похожа на вероятностную схему маркировки пакетов. В этой схеме маршрутизаторы генерируют ICMP-пакеты, которые с малой вероятностью отправляются в необходимое место. Для значительного потока трафика пункт назначения может постепенно восстанавливать маршрут, который был создан пакетами в потоке. Позднее эта схема была расширена Wuetal, Махаджан предоставляют схему [5], в которой маршрутизаторы изучают сигнатуру перегрузки, чтобы определить «хороший» трафик и отличить его от плохого. Согласно этой сигнатуре маршрутизатор может фильтровать плохой трафик. Кроме того, предоставляется схема pushback, позволяющая маршрутизатору запрашивать соседние маршрутизаторы для фильтрации плохого трафика на более раннем этапе [7].

В настоящее время большая часть исследований DDoS направлена на отслеживание истоков нападавших [8]. Если установить истинную личность атакующего через трассировку, его можно заблокировать. В общем это медленный процесс, который может занять несколько часов или даже дней. В течение этого

периода веб-серверы ничего не могут сделать для восстановления своих услуг для законных клиентов. Поэтому, хотя трассировка IP-адресов полезна для идентификации злоумышленника, она не может смягчить эффект атаки. В настоящее время нет эффективных механизмов защиты от DDoS, которые могут решить проблему полностью.

Анализ предлагаемого решения. Защита веб-сервисов имеет первостепенное значение, поскольку Интернет — основная технология электронной коммерции и основная цель DDoS-атак [1]. В настоящей работе описан новый механизм безопасности DDoS, который представляет собой трехслойную защиту, основанную на веб-серверах.

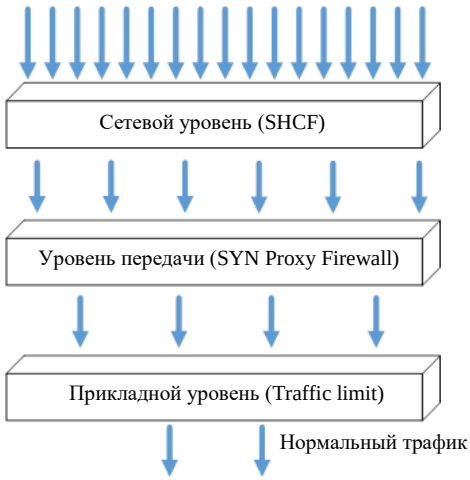

Рис. 1

Сочетая характеристику трафика веб-серверов и нацеленность на опорную модель TCP/IP, используются средства статистической фильтрации и ограничения трафика в сетевом уровне, транспортном и прикладном уровнях для фильтрации незаконного трафика и обеспечения прохода нормального трафика.

Основная идея предлагаемой системы — изоляция и защита «правильного» трафика от огромных объемов трафика DDoS, когда происходит атака. Первый шаг — отличать пакеты, содержащие IP-адреса подлинного источника, от тех, которые содержат поддельные адреса. Это осуществляется защитой первого уровня на основе сетевого уровня и защиты второго уровня на основе транспортного уровня. Алгоритм упрощенной фильтрации графов (SHCF) используется в качестве защиты на основе сетевого уровня. Алгоритм SYNProxyFirewall используется в качестве защиты на основе уровня передачи. Поэтому можно отличить незаконный трафик от обычного трафика. Однако злоумышленники также могут использовать свои подлинные IP-адреса для отправки большого объема трафика жертве. Второй шаг — не допустить потребления слишком многих ресурсов системы. Это достигается защитой третьего уровня на основе уровня приложения. Стратегия состоит в том, чтобы обеспечить справедливое распределение полосы пропускания среди всех клиентов и злоумышленников, которые используют законные IP-адреса. Но даже при справедливом распределении пропускной способности злоумышленники могут по-прежнему превосходить число законных клиентов и присваивают большую часть пропускной способности системы. Во избежание этого применяется закон обеспечения квоты, по которой может совершить отправление каждый клиент. Если клиент превысил эту квоту, его подозре-

вают как возможного злоумышленника, и ему будет предоставлена лишь часть его справедливой доли. Таким образом, есть гарантия, что в конечном итоге большая часть системного ресурса будет предоставлена законным клиентам.

Благодаря совместной защите трехслойного механизма при атаках DDoS [9] поддержку доступности веб-сервисов можно обеспечить. Наконец, защитный механизм реализован и протестирован внутри ядра Linux.

Проектирование предлагаемой системы

С учетом характеристики трафика веб-серверов и нацеленности на опорную модель TCP/IP используются средства статистической фильтрации и ограничение трафика в сетевом уровне, транспортном и прикладном уровнях для доступа к нормальному трафику. Нелегитимный трафик в основном фильтруется алгоритмом SHCF (упрощенная фильтрация количества хопов) на сетевом уровне, остальная часть — по алгоритму SYN ProxyFirewall на уровне передачи, IP-адреса — на уровне приложений. При атаках DDoS поддержка совместной защиты трехслойного механизма доступности веб-сервисов может быть обеспечена.

Защита на основе сетевого уровня. На сетевом уровне алгоритм SHCF используется для отсеивания большого объема поддельных IP-пакетов, которые идентифицируют законного клиента путем извлечения первого 24-битового префикса IP-адреса источника и значения TTL из заголовка IP. Обоснованием SHCF является то, что большинство поддельных IP-пакетов, их получает жертва атаки, не имеет значений подсчета переходов, которые согласуются с подделками IP-адресов. SHCF строит точную таблицу при использовании умеренного объема хранилища путем кластеризации первых 24 бит адресных префиксов на основе количества переходов.

Для каждого веб-сервера создается таблица SHCF, группируя его IP-адреса в соответствии с первыми 24 битами. Авторы используют минимальный подсчет переходов всех IP-адресов в 24-битовым сетевом адресе как счетчик переходов в сети. После построения таблицы каждый IP-адрес преобразуется в 24-битовый адресный префикс, а фактическое количество переходов IP-адреса сравнивается с тем, которое хранится в сводной таблице SHCF. Поскольку 24-разрядная агрегация не сохраняет правильные подсчеты шагов для всех IP-адресов, пакеты, чьи подсчеты переходов отличаются больше чем на два, отбрасываются.

Вычисление Hop-Count. Поскольку информация о подсчете хопа непосредственно не хранится в заголовке IP, нужно вычислить подсчет хопов на основе поля TTL, которое является 8-битовым полем в заголовке IP, изначально введенным для указания максимального времени жизни каждого пакета в Интернете. Каждый промежуточный маршрутизатор уменьшает значение TTL для транзитного IP-пакета на единицу перед пересылкой его на следующий хоп. Конечное значение TTL, когда пакет достигает своего адресата, поэтому начальный TTL вычитается из числа промежуточных переходов.

Большинство модемных ОС используют только несколько выбранных начальных значений TTL, 30, 32, 60, 64, 128 и 255, как показано в [7]. Этот набор TTL охватывает большинство популярных ОС, таких как MicrosoftWindows, Linux, варианты BSD и многие коммерческие Unix-системы. Поскольку интернет-трассы показали, что несколько интернет-хостов разделены более чем на 30 переходов, можно определить начальное значение TTL для пакета, выбрав наименьшее начальное значение в наборе, которое больше его окончательного TTL. Если T_i обозначает начальное значение TTL, T_r обозначает конечное значение TTL, а H_e — количество прыжков, то $T_i = \min \{> T_r \}$, $H_e = T_i - T_r$.

Например, если конечное значение TTL $T_r = 112$, начальное значение TTL $T_i = 128$, меньшее из двух возможных начальных значений: 128 и 255. Для устранения двусмысленности в случаях {30, 32}, {60, 64 } и {32, 60} вычисляем значение количества прыжков для каждого из возможных начальных значений TTL и принимаем пакет, если есть совпадение с одним из возможных значений перескока [2].

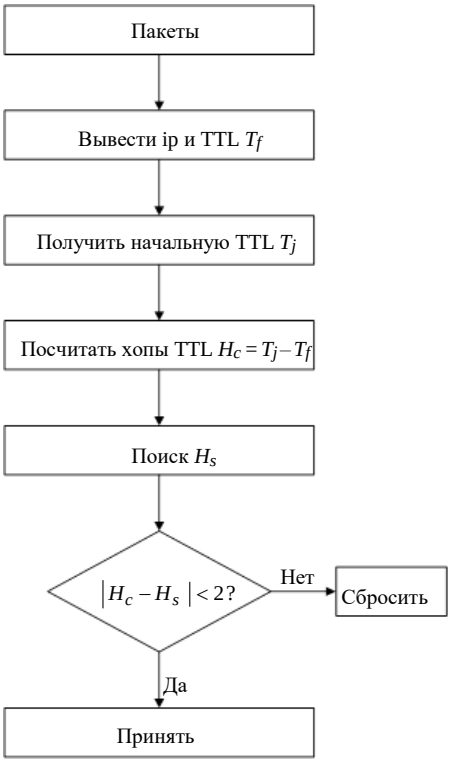

Рис. 2

Проверка Hop-Count. Алгоритм проверки извлекает исходный IP-адрес и конечное значение TTL из каждого IP-пакета. Алгоритм отображает начальное значение TTL и вычитает из него окончательное значение TTL, чтобы получить счетчик переходов. Исходный IP-адрес служит индексом в таблице для получения правильного количества переходов для этого IP-адреса. Если вычисленное количество ходов отличается более чем на два, пакет, скорее всего, подделан. Если H обозначает количество переходов IP-адреса источника в таблице, то алгоритм проверки выглядит следующим образом.

Если $IH_e - H_S$ 1 <= 2, пакеты принимаются. В противном случае отбрасываются.

Поддельный IP-адрес может иметь одно и то же количество хопов, что и компьютеры-зомби. В этом случае HCF не сможет идентифицировать поддельный пакет. Однако его можно «отгонять» защитой второго уровня.

Защита на основе транспортного уровня. В транспортном уровне алгоритм SYNProxyFirewall используется для отсеивания остальных поддельных IP-пакетов.

SYNProxy — подход защиты на основе брандмауэра. Он основан на идее, что каждый пакет, предназначенный для хоста внутри брандмауэра, сначала должен рассматриваться брандмауэром, и затем решения могут быть приняты на его подлинности, и могут быть предприняты действия защиты внутренних узлов (рис. 3).

В схеме SYN Proxy при получении запроса TCP-соединения брандмауэр отвечает от имени сервера. Только после успешного завершения трехстороннего рукопожатия брандмауэр связывается с хостом и устанавливает второе соединение.

В случае атаки брандмауэр отвечает на SYN, отправленный злоумышленником. Поскольку последний Acknowledgment Number (ACK) никогда не прибывает, брандмауэр завершает соединение, и хост никогда не получает датаграмму. В случае законного соединения после получения последним ACK брандмауэра он создает новое соединение с внутренним хостом от имени первоначального клиента. Как только соединение установлено, брандмауэр должен продолжать действовать как прокси-сервер, чтобы перевести порядковые номера в пакетах, между клиентом и сервером.

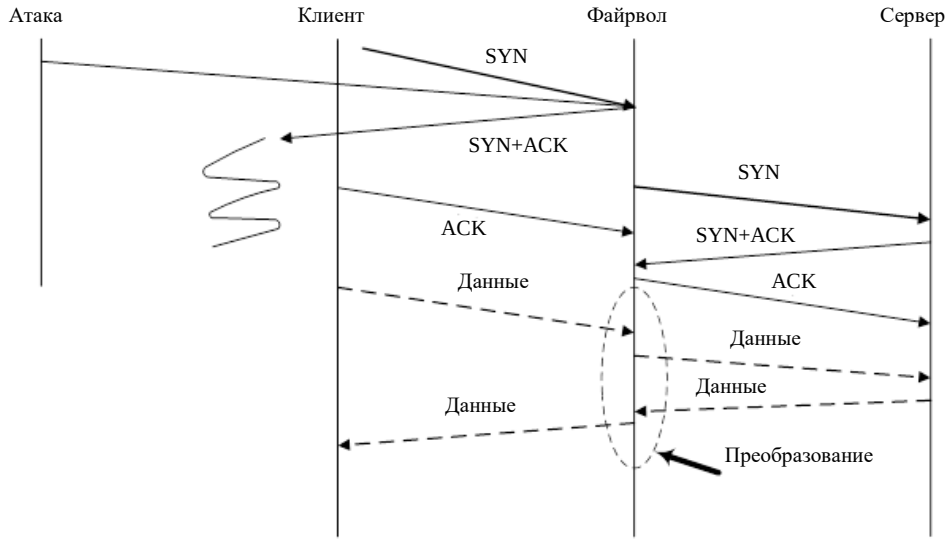

Рис. 3

Защита на основе прикладного уровня. Атакующие могут также представлять законных клиентов и отправлять законные HTTP-запросы, чтобы использовать пропускную способность предлагаемой системы. На прикладном уровне алгоритм ограничения трафика используется для защиты атак с использованием подлинных IP-адресов.

Для решения этой проблемы брандмауэр должен выполнять справедливое распределение полосы пропускания среди всех клиентов и злоумышленников, использующих подлинные IP-адреса. Система может установить квоту Q такую, что вероятность для законной транзакции отправлять больше Q-пакетов очень мала. После того как с IP-адреса отправлено больше Q пакетов, ему будет предоставлено только 1/10 его справедливой доли. Это эффективно ограничивает количество злоумышленников, использующих пропускную способность. Эта квота Q должна быть установлена в соответствии с обычным поведением транзакций, профилированным на защищенном веб-сайте.

Реализация и испытание

Обсудим вопросы, связанные с реализацией и тестированием предлагаемой системы. Для улучшения транзакции пакетов и эффективности предлагаемой системы внедряем модуль внутри ядра Linux, защита сетевого уровня реализована внутри драйвера netcardLinux, защита транспортного уровня и защиты прикладного уровня — внутри фильтра netfilter. Блок-схема изображена на рис. 4.

Для проверки эффективности атаки DDoS создаем тестовую сцену (рис. 5). Хосты 1, 2 действуют как законные клиенты; хосты 3, 4 — как атакующие; веб-сервер и защитная система настроены следующим образом: CPU P4 2.4G, память 512M, ядро 4 Fedora, веб-сервер Apache. Другие настроены следующим образом: процессор Celeron 2.4G, память 256M, ОС Windows XP sp2.

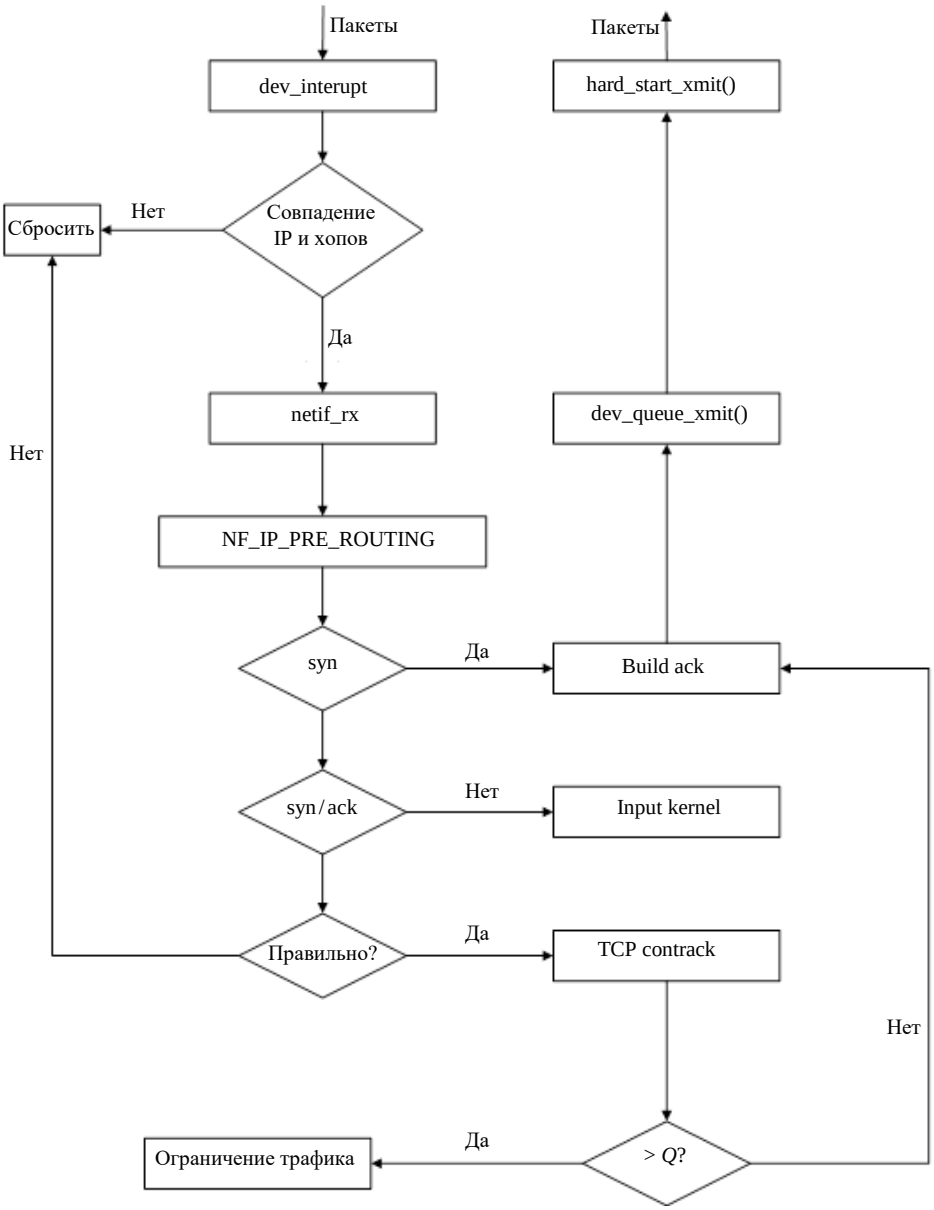

Рис. 4

1. Без защиты системы. Если хосты 3 и 4 не запускают атаки DDoS, хосты 1 и 2 могут посещать веб-сервер. Если хосты 3 и 4 запускают DDoS-атаки одновременно, хосты 1 и 2 не могут посещать веб-сервер.

2. С защитной системой. Если хосты 3 и 4 запускают DDoS-атаки, в то же время хосты 1 и 2 соединяют веб-сервер, веб-сервер можно без промедления посещать.

Таким образом, трехслойный защитный механизм, основанный на веб-серверах, может обеспечить поддержание доступности веб-сервисов при атаках DDoS.

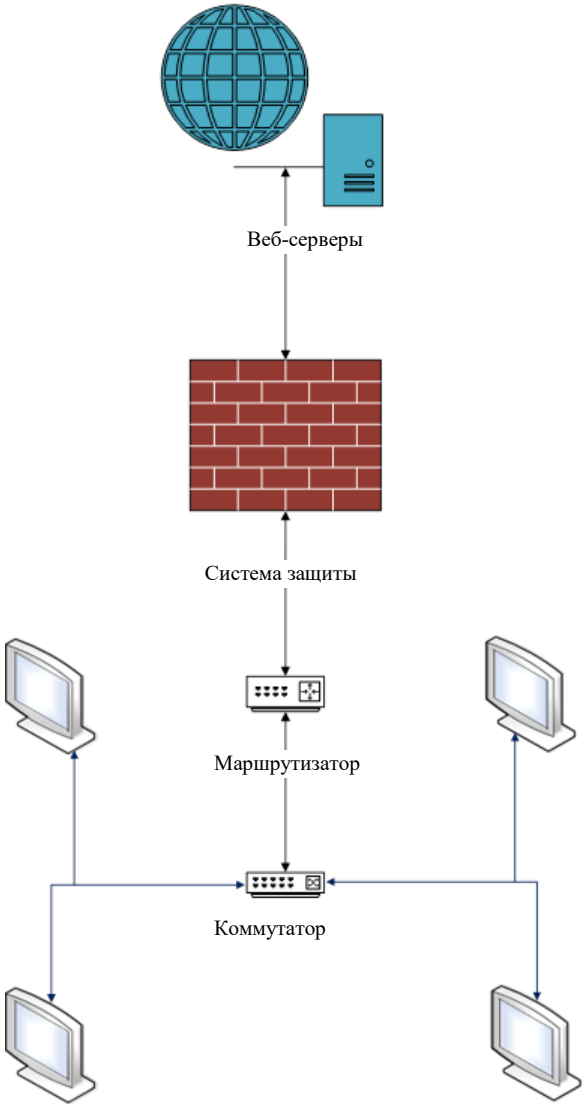

Рис. 5

Заключение

Настоящая публикация посвящена разработке механизма безопасности DDoS, который представляет собой трехслойный защитный механизм, основанный на веб-серверах. Сочетая характеристику трафика веб-серверов и нацеленность на опорную модель TCP / IP, он использует средства статистической фильтрации и ограничения трафика в сетевом, транспортном и прикладном уровнях для фильтрации незаконного трафика, обеспечивая проход законного трафика.

Упрощен алгоритм фильтрации графа хопа и используется SHCF для защиты первого слоя.

Реализована предлагаемая система защиты внутри ядра Linux. Результат показывает, что механизм защиты трех уровней, основанный на веб-серверах, может эффективно защищать от атаки DDoS.

ISSN 0572-2691

А.Т. Рахманов, Ш.К. Камалов, К.Ф. Керимов

МЕХАНІЗМ ТРИШАРОВОГО ЗАХИСТУ НА ОСНОВІ WEB-СЕРВЕРІВ ВІД РОЗПОДІЛЕНОЇ ВІДМОВИ ВІД ОБСЛУГОВУВАННЯ

Визнано, що атаки з розподіленою відмовою від обслуговування (DDoS) можуть порушити веб-сервіс і призвести до великих втрат доходів. Атаки DDoS обмежують і блокують законних користувачів для доступу до веб-серверів шляхом вичерпання ресурсів жертви. Оскільки використовуються системні витоки і прихована проблема безпеки, дана атака має характеристики природної поведінки і її складно заблокувати. Захист веб-сервісів має першорядне значення, оскільки Інтернет є базовою технологією, яка лежить в основі електронної комерції — це і є основною метою DDoS-атак. Запропоновано ізолювати і захистити правильний трафік від великих обсягів трафіку DDoS, коли відбувається атака. Розроблено новий механізм безпеки DDoS — тришаровий захисний механізм, заснований на веб-серверах. Поєднуючи характеристику трафіка веб-серверів і націленість на опорну модель TCP/IP, використовуються кошти статистичної фільтрації та обмеження трафіку в мережевому, транспортному і прикладному рівнях для фільтрації незаконного трафіку для забезпечення проходу нормального трафіку. Більшість нелегітимного трафіку фільтрується за алгоритмом SHCF (спрощена фільтрація кількості хопів) на мережевому рівні. Інша частина незаконного трафіку фільтрується за алгоритмом SYNProxyFirewall на рівні передачі. Обмеження трафіку використовується на рівні додатку для DDoS-атак з використанням законної IP-адреси. Завдяки спільному захисту тришарового механізму підтримка доступності веб-сервісів може забезпечуватися при атаках DDoS. Механізм захисту реалізований і протестований всередині ядра Linux. Результат показує, що тришаровий захисний механізм може ефективно захищати від атаки DDoS.

Ключові слова: розподілені DOS-атаки, виявлення загроз, тришаровий механізм, математичний аналіз, незаконний трафік, TTL, веб-сервери.

A.T. Rakhmanov, Sh.K. Kamalov, K.F. Kerimov

A THREE-LAYER DEFENSE MECHANISM BASED ON WEB SERVERS AGAINST DISTRIBUTED DENIAL OF SERVICE ATTACKS

It is widely recognized that distributed denial of service (DDoS) attacks can disrupt web services and lead to large revenue losses. DDoS attacks restrict and block legitimate users accessing web servers by exhaustion of victim's resources. Due to system leaks and a hidden security problem are used, this attack has the characteristics of natural behavior and it is difficult to be blocked. Protection of web services is of paramount importance, since the Internet is the main technology underlying e-commerce — this is the main purpose of DDoS attacks. The article proposed to isolate and protect the correct traffic from the huge volumes of DDoS traffic when an attack occurs. A new DDoS security mechanism has been developed, which is a three-layer protection mechanism based on web servers. Combining the characteristics of web server traffic and aiming at TCP / IP reference model, it uses statistical filtering and traffic restriction in the network layer, transport layer and application layer to filter out illegal traffic to ensure normal traffic passage. Most of the illegitimate traffic is filtered by SHCF (Simplified Filtering of Hopes) algorithm at the network lev-

el. The rest of the illegal traffic is filtered according to the SYNProxyFirewall algorithm at the transmission level. Traffic restriction is used at the application level while DDoS attacks using a legitimate IP address. Thanks to the joint protection of the three-layer mechanism, support for the availability of web services can be provided during DDoS attacks. The protection mechanism is implemented and tested inside the Linux kernel. The result shows that a three-layer protection mechanism can effectively protect against DDoS attacks.

Keywords: DDOS attacks, threat identification, three-layer mechanism, mathematical model, illegal traffic, TTL, web-servers.

1. Керимов К.Ф. Модель выявления угроз информационной безопасности в электронных ресурсах. *Перспективы развития техники и технологии и достижения горно-металлургической отрасли за годы независимости Республики Узбекистан: Тез. докл. Респ. науч. конф*. 12–14 мая 2011. Навои, 2011. С. 339–340.
2. Козлов Д.Д., Петухов А.А. Методы обнаружения уязвимостей в web-приложениях. *Программные системы и инструменты*. 2006. № 7. С. 156–166.
3. Керимов К.Ф., Мухсинов Ш.Ш. Исматуллаев С.О. Брандмауэр баз данных, основанный на обнаружении аномалий. *Проблемы информатики и энергетики*. 2015. № 3–4.
4. Низамутдинов М.К. Тактика защиты и нападения на ИТ- приложения. Санкт-Петербург: БХВ-Петербург, 2005. С. 10–30.
5. Пазизин С.В. Основы защиты информации в компьютерных системах. М. : ТВП-ОпиПМ, 2003. 73 с.
6. Петренко С. А., Петренко А. А. Аудит безопасности Intranet. М. : ДМК Пресс, 2002. 416 с.
7. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем. Волгоград: ВолГУ, 2002. 122 с.
8. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. М. : Гелиос, 2006. 62 с.
9. Opanasenko V.N., Kryvyi S.L. Synthesis of adaptive logical networks on the basis of Zhegalkin polynomials. *Cybernetics and Systems Analysis.* 2015. **51**, N 6. P. 969–977. DOI: 10.1007/s-10559-015-9790-1.

Получено 01.04.2019
После доработки 24.05.2019