Содержание:

ВВЕДЕНИЕ

Интенсивное развитие глобальных компьютерных сетей, появление новых технологий поиска информации привлекают все больше внимания к сети Internet со стороны частных лиц и различных организаций. Многие организации принимают решение об интеграции своих локальных и корпоративных сетей в глобальную сеть. Использование глобальных сетей в коммерческих целях, а также при передаче информации, содержащей сведения конфиденциального характера, влечет за собой необходимость построения эффективной системы защиты информации. В настоящее время в России глобальные сети применяются для передачи коммерческой информации различного уровня конфиденциальности, например для связи с удаленными офисами из головной штаб-квартиры организации или создания Web-страницы организации с размещенной на ней рекламой и деловыми предложениями.

Вряд ли нужно перечислять все преимущества, которые получает современное предприятие, имея доступ к глобальной сети Internet. Но, как и многие другие новые технологии, использование Internet имеет и негативные последствия. Развитие глобальных сетей привело к многократному увеличению количества пользователей и увеличению количества атак на компьютеры, подключенные к сети Internet. Ежегодные потери, обусловленные недостаточным уровнем защищенности компьютеров, оцениваются десятками миллионов долларов. При подключении к Internet локальной или корпоративной сети необходимо позаботиться об обеспечении информационной безопасности этой сети. Глобальная сеть Internet создавалась как открытая система, предназначенная для свободного обмена информацией. В силу открытости своей идеологии Internet предоставляет для злоумышленников значительно большие возможности по сравнению с традиционными информационными системами. Поэтому вопрос о проблеме защиты сетей и её компонентов становиться достаточно важным и актуальным и это время, время прогресса и компьютерных технологий. Многие страны наконец-то поняли важность этой проблемы. Происходит увеличение затрат и усилий, направленных на производство и улучшение различных средств защиты. Основной целью реферата является рассмотрение, и изучение функционирования одного из таких средств сетевой защиты как брандмауэр или межсетевой экран. Который в

настоящее время является наиболее надежным в плане защиты из предлагаемых средств.

ГЛАВА 1. БРАНДМАУЭР

1.1. Понятие брандмауэр.

Брандмауэр, или межсетевой экран — это «полупроницаемая мембрана», которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети Internet и контролирует все информационные потоки во внутренний сегмент и из него. Контроль трафика состоит в его фильтрации, то есть в выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске отказано. Фильтрация осуществляется на основании набора условий, предварительно загруженных в брандмауэр и отражающих концепцию информационной безопасности корпорации. Брандмауэры могут быть выполнены в виде как аппаратного, так и программного комплекса, записанного в коммутирующее устройство или сервер доступа (сервер -шлюз, просто сервер, хост-компьютер и т.д.), встроенного в операционную систему или представлять собой работающую под ее управлением программу.

1.1.1. Функции брандмауэра.

Работа брандмауэра заключается в анализе структуры и содержимого информационных пакетов, поступающих из внешней сети, и в зависимости от результатов анализа пропуске пакетов во внутреннюю сеть (сегмент сети) или полном их отфильтровывании. Эффективность работы межсетевого экрана, работающего под управлением Windows, обусловлена тем, что он полностью замещает реализуемый стек протоколов TCP\IP, и поэтому нарушать его работу с помощью искажения протоколов внешней сети (что часто делается хакерами) невозможно.

Межсетевые экраны обычно выполняют следующие функции:

физическое отделение рабочих станций и серверов внутреннего сегмента сети (внутренней подсети) от внешних каналов связи;

многоэтапную идентификацию запросов, поступающих в сеть (идентификация серверов, узлов связи о прочих компонентов внешней сети);

проверку полномочий и прав доступа пользователя к внутренним ресурсам сети;

регистрацию всех запросов к компонентам внутренней подсети извне;

контроль целостности программного обеспечения и данных;

экономию адресного пространства сети (во внутренней подсети может использоваться локальная система адресации серверов);

сокрытие IP адресов внутренних серверов с целью защиты от хакеров.

Брандмауэры могут работать на разных уровнях протоколов модели OSI.

На сетевом уровне выполняется фильтрация поступающих пакетов, основанная на IP адресах (например, не пропускать пакеты из Интернета, направленные на те серверы, доступ к которым снаружи запрещен; не пропускать пакеты с фальшивыми обратными адресами или IP адресами, занесенными в «черный список», и т.д.). На транспортном уровне фильтрация допустима еще и по номерам портов TCP и флагов, содержащихся в пакетах (например, запросов на установление соединения). На прикладном уровне может выполняться анализ прикладных протоколов (FTP, HTTP, SMTP и т.д.) и контроль за содержанием потоков данных (запрет внутренним абонентам на получение каких-либо типов файлов: рекламной информации или исполняемых программных модулей, например).

Можно в брандмауэре создавать и экспертную систему, которая, анализируя трафик, диагностирует события, могущие представлять угрозу безопасности внутренней сети, и извещает об этом администратора. Экспертная система способна также в случае опасности (спам, например) автоматически ужесточать условия фильтрации и т.д.

1.1.2. Виды брандмауэров

Брандмауэры бывают аппаратными или программными.

Аппаратный брандмауэр представляет собой устройство, физически подключаемое к сети. Это устройство отслеживает все аспекты входящего и исходящего обмена данными, а также проверяет адреса источника и назначения каждого обрабатываемого сообщения. Это обеспечивает безопасность, помогая предотвратить нежелательные проникновения в сеть или на компьютер. Программный брандмауэр выполняет те же функции, используя не внешнее устройство, а установленную на компьютере программу.

На одном и том же компьютере могут использоваться как аппаратные, так и программные брандмауэры.

1.1.3. Преимущества использования брандмауэра

Брандмауэр представляет собой защитную границу между компьютером (или компьютерной сетью) и внешней средой, пользователи или программы которой могут пытаться получить несанкционированный доступ к компьютеру. Обычно взломщики используют специальные программы для поиска в Интернете незащищенных подключений. Такая программа отправляет на компьютер очень маленькое сообщение. При отсутствии брандмауэра компьютер автоматически отвечает на сообщение, обнаруживая свою незащищенность. Установленный брандмауэр получает такие сообщения, но не отвечает на них; таким образом, взломщики даже не подозревают о существовании данного компьютера.

1.1.4. Уровень опасности

Существует несколько путей свести на нет либо подвергнуть риску брандмауэрную защиту. И хотя они все плохи, о некоторых можно с уверенностью говорить как о самых неприятных. Исходя из того, что основной целью установки большинства брандмауэров является блокирование доступа, очевидно, что обнаружение кем-либо лазейки, позволяющей проникнуть в систему, ведет к полному краху всей защиты данной системы. Если же несанкционированному пользователю удалось проникнуть в брандмауэр и переконфигурировать его, ситуация может принять еще более угрожающий характер. В целях разграничения терминологии примем, что в первом случае мы имеем дело со взломомбрандмауэрной защиты, а во втором -- с полным ее разрушением. Степень ущерба, который может повлечь за собой разрушение брандмауэрной защиты, определить невероятно сложно. Наиболее

полные сведения о надежности такой защиты может дать только информация о предпринятой попытке взлома, собранная этим брандмауэром. Самое плохое происходит с системой защиты именно тогда, когда при полном разрушении брандмауэра не остается ни малейших следов, указывающих на то, как это происходило. В лучшем же случае брандмауэр сам выявляет попытку взлома и вежливо информирует об этом администратора. Попытка при этом обречена на провал.

Один из способов определить результат попытки взлома брандмауэрной защиты -- проверить состояние вещей в так называемых зонах риска. Если сеть подсоединена к Internet без брандмауэра, объектом нападения станет вся сеть. Такая ситуация сама по себе не предполагает, что сеть становится уязвимой для каждой попытки взлома. Однако если она подсоединяется к общей небезопаснойсети, администратору придется обеспечивать безопасность каждого узла отдельно. В случае образования бреши в брандмауэре зона риска расширяется и охватывает всю защищенную сеть. Взломщик, получивший доступ к входу в брандмауэр, может прибегнуть к методу "захвата островов" и, пользуясь брандмауэром как базой, охватить всю локальную сеть. Подобная ситуация все же даст слабую надежду, ибо нарушитель может оставить следы в брандмауэре, и его можно будет разоблачить. Если же брандмауэр полностью выведен из строя, локальная сеть становится открытой для нападения из любой внешней системы, и определение характера этого нападения становится практически невозможным.

В общем, вполне возможно рассматривать брандмауэр как средство сужения зоны риска до одной точки повреждения. В определенном смысле это может показаться совсем не такой уж удачной идеей, ведь такой подход напоминает складывание яиц в одну корзину. Однако практикой подтверждено, что любая довольно крупная сеть включает, по меньшей мере, несколько узлов, уязвимых при попытке взлома даже не очень сведущим нарушителем, если у него достаточного для этого времени. Многие крупные компании имеют на вооружении организационную политику обеспечения безопасности узлов, разработанную с учетом этих недостатков. Однако было бы не слишком разумным целиком полагаться исключительно на правила. Именно с помощью брандмауэра можно повысить надежность узлов, направляя нарушителя в такой узкий тоннель, что появляется реальный шанс выявить и выследить его, до того, как он наделает бед. Подобно тому, как средневековые замки обносили несколькими стенами, в нашем случае создается взаимоблокирующая защита.

1.2. Межсетевой экран как средство от вторжения из Internet

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать межсетевые экраны, В отечественной литературе до последнего времени использовались вместо этого термина другие термины иностранного происхождения: брандмауэр и firewall. Вне компьютерной сферы брандмауэром (или firewall) называют стену, сделанную из негорючих материалов и препятствующую распространению пожара. В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от фигурального пожара - попыток злоумышленников вторгнуться во внутреннюю сеть для того, чтобы скопировать, изменить или стереть информацию либо воспользоваться памятью или вычислительной мощностью работающих в этой сети компьютеров. Межсетевой экран призван обеспечить безопасный доступ к внешней сети и ограничить доступ внешних пользователей к внутренней сети.

Межсетевой экран (МЭ) — это система межсетевой защиты. позволяющая разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между корпоративной (локальной) сетью предприятия и глобальной сетью Internet, хотя ее можно провести и внутри корпоративной сети предприятия. МЭ пропускает через себя весь трафик, принимая для каждого проходящего пакета решение - пропускать его или отбросить. Для того чтобы МЭ мог осуществить это ему необходимо определить набор правил фильтрации.

Обычно межсетевые экраны защищают внутреннюю сеть предприятия от "вторжений" из глобальной сети Internet, однако они могут использоваться и для защиты от "нападений" из корпоративной интрасети, к которой подключена локальная сеть предприятия. Ни один межсетевой экран не может гарантировать полной защиты внутренней сети при всех возможных обстоятельствах. Однако для большинства коммерческих организаций установка межсетевого экрана является необходимым условием обеспечения безопасности внутренней сети. Главный довод в пользу применения межсетевого экрана состоит в том, что без него системы внутренней сети подвергаются опасности со стороны слабо защищенных служб сети Internet, а также зондированию и атакам с каких-либо других хост - компьютеров внешней сети.

Проблемы недостаточной информационной безопасности являются "врожденными" практически для всех протоколов и служб Internet. Большая часть этих проблем связана с исторической зависимостью Internet от операционной системы UNIX. Известно, что сеть Arpanet (прародитель Internet) строилась как сеть, связывающая исследовательские центры, научные, военные и правительственные учреждения, крупные университеты США. Эти структуры использовали операционную систему UNIX в качестве платформы для коммуникаций и решения собственных задач. Поэтому особенности методологии программирования в среде UNIX и ее архитектуры наложили отпечаток на реализацию протоколов обмена и политики безопасности в сети. Из-за открытости и распространенности система UNIX стала любимой добычей хакеров. Поэтому совсем не удивительно, что набор протоколов TCP/IP, который обеспечивает коммуникации в глобальной сети Internet и в получающих все большую популярность интрасетях, имеет "врожденные" недостатки защиты. То же самое можно сказать и о ряде служб Internet.

Набор протоколов управления передачей сообщений в Internet (Transmission Control Protocol/Internet Protocol - TCP/IP) используется для организации коммуникаций в неоднородной сетевой среде, обеспечивая совместимость между компьютерами разных типов. Совместимость - одно из основных преимуществ TCP/IP, поэтому большинство локальных компьютерных сетей поддерживает эти протоколы. Кроме того, протоколы TCP/IP предоставляют доступ к ресурсам глобальной сети Internet. Поскольку TCP/IP поддерживает маршрутизацию пакетов, он обычно используется в качестве межсетевого протокола. Благодаря своей популярности TCP/IP стал стандартом де фактора для межсетевого взаимодействия.

В заголовках пакетов TCP/IP указывается информация, которая может подвергнуться нападениям хакеров. В частности, хакер может подменить адрес отправителя в своих "вредоносных" пакетах, после чего они будут выглядеть, как пакеты, передаваемые авторизированным клиентом.

1.2.1. Функциональные требования и компоненты межсетевых экранов

Функциональные требования к межсетевым экранам включают:

требования к фильтрации на сетевом уровне;

требования к фильтрации на прикладном уровне;

требования по настройке правил фильтрации и администрированию;

требования к средствам сетевой аутентификации;

требования по внедрению журналов и учету.

Большинство компонентов межсетевых экранов можно отнести к одной из трех категорий:

фильтрующие маршрутизаторы;

шлюзы сетевого уровня;

шлюзы прикладного уровня.

Эти категории можно рассматривать как базовые компоненты реальных межсетевых экранов. Лишь немногие межсетевые экраны включают только одну из перечисленных категорий. Тем не менее, эти категории отражают ключевые возможности, отличающие межсетевые экраны друг от друга.

1.3. Фильтрующие маршрутизаторы

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящее и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP- заголовках пакетов.

Фильтрующие маршрутизаторы обычно может фильтровать IP-пакет на основе группы следующих полей заголовка пакета:

IP- адрес отправителя (адрес системы, которая послала пакет);

IP-адрес получателя (адрес системы, которая принимает пакет);

порт отправителя (порт соединения в системе отправителя);

порт получателя (порт соединения в системе получателя);

Порт — это программное понятие, которое используется клиентом или сервером для посылки или приема сообщений; порт идентифицируется 16 - битовым числом.

В настоящее время не все фильтрующие маршрутизаторы фильтруют пакеты по TCP/UDP - порт отправителя, однако многие производители маршрутизаторов начали обеспечивать такую возможность. Некоторые маршрутизаторы проверяют, с какого сетевого интерфейса маршрутизатора пришел пакет, и затем используют эту информацию как дополнительный критерий фильтрации.

Фильтрация может быть реализована различным образом для блокирования соединений с определенными хост - компьютерами или портами. Например, можно блокировать соединения, идущие от конкретных адресов тех хост-компьютеров и сетей. которые считаются враждебными или ненадежными.

Добавление фильтрации по портам TCP и UDP к фильтрации по IP-адресам обеспечивает большую гибкость. Известно, что такие серверы, как домен TELNET, обычно связаны с конкретными портами (например, порт 23 протокола TELNET). Если межсетевой экран может блокировать соединения TCP или UDP с определенными портами или от них, то можно реализовать политику безопасности, при которой некоторые виды соединений устанавливаются только с конкретными хост - компьютерами.

К положительным качествам фильтрующих маршрутизаторов следует отнести:

сравнительно невысокую стоимость;

гибкость в определении правил фильтрации;

небольшую задержку при прохождении пакетов.

Недостатками фильтрующих маршрутизаторов являются:

внутренняя сеть видна (маршрутизируется) из сети Internet правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;

при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;

аутентификацию с использованием IP-адреса можно обмануть путем подмены IP-адреса (атакующая система выдает себя за другую, используя ее IP-адрес);

отсутствует аутентификация на пользовательском уровне.

1.4. Шлюзы сетевого уровня

Шлюз сетевого уровня иногда называют системой трансляции сетевых адресов или шлюзом сеансового уровня модели OSI. Такой шлюз исключает, прямое взаимодействие между авторизированным клиентом и внешним хост-компьютером. Шлюз сетевого уровня принимает запрос доверенного клиента на конкретные услуги, и после проверки допустимости запрошенного сеанса устанавливает соединение с внешним хост - компьютером. После этого шлюз копирует пакеты в обоих направлениях, не осуществляя их фильтрации.

Шлюз следит за подтверждением (квитированием) связи между авторизированным клиентом и внешним хост - компьютером, определяя, является ли запрашиваемый сеанс связи допустимым.

Фактически большинство шлюзов сетевого уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня. Примерами таких шлюзов являются Gauntlet Internet Firewall компании Trusted Information Systems, Alta Vista Firewall компании DEC и ANS Interlock компании ANS. Например, Alta Vista Firewall использует канальные посредники прикладного уровня для каждой из шести служб TCP/IP, к которым относятся, в частности, FTP, HTTP (Hyper Text Transport Protocol) и Telnet. Кроме того, межсетевой экран компании DEC обеспечивает шлюз сетевого уровня, поддерживающий другие общедоступные службы TCP/IP, такие как Gopher и SMTP, для которых межсетевой экран не предоставляет посредников прикладного уровня.

Шлюз сетевого уровня выполняет еще одну важную функцию защиты: он используется в качестве сервера-посредника. Этот сервер-посредник выполняет процедуру трансляции адресов, при которой происходит преобразование внутренних IP-адресов в один "надежный" IP-адрес. Этот адрес ассоциируется с межсетевым экраном, из которого передаются все исходящие пакеты. В результате в сети со шлюзом сетевого уровня все исходящие пакеты оказываются отправленными из этого шлюза, что исключает прямой контакт между внутренней (авторизированной) сетью и потенциально опасной внешней сетью. IP-адрес шлюза сетевого уровня становится единственно активным IP-адресом, который попадает во внешнюю сеть. Таким образом, шлюз сетевого уровня и другие серверы-посредники защищают внутренние сети от нападений типа подмены адресов.

1.5. Шлюзы прикладного уровня

Для устранения ряда недостатков, присущих фильтрующим маршрутизаторам, межсетевые экраны должны использовать дополнительные программные средства для фильтрации сообщений сервисов типа TELNET и FTP. Такие программные средства называются полномочными серверами (серверами-посредниками), а хост-компьютер, на котором они выполняются, - шлюзом прикладного уровня.

Шлюз прикладного уровня исключает прямое взаимодействие между авторизированным клиентом и внешним хост - компьютером. Шлюз фильтрует все входящие и исходящие пакеты на прикладном уровне. Связанные с приложением серверы - посредники перенаправляют через шлюз информацию, генерируемую конкретными серверами.

Для достижения более высокого уровня безопасности и гибкости шлюзы прикладного уровня и фильтрующие маршрутизаторы могут быть объединены в одном межсетевом экране. В качестве примера рассмотрю сеть, в которой с помощью фильтрующего маршрутизатора блокируются входящие соединения TELNET и FTP. Этот маршрутизатор допускает прохождение пакетов TELNET или FTP только к одному хост - компьютеру - шлюзу прикладного уровня TELNET/FTP. Внешний пользователь, который хочет соединиться с некоторой системой в сети, должен сначала соединиться со шлюзом прикладного уровня, а затем уже с нужным внутренним хост- компьютером.

В дополнение к фильтрации пакетов многие шлюзы прикладного уровня регистрируют все выполняемые сервером действия и, что особенно важно, предупреждают сетевого администратора о возможных нарушениях защиты. Например, при попытках проникновения в сеть извне BorderWare Firewall Server компании Secure Computing позволяет фиксировать адреса отправителя и получателя пакетов, время, в которое эти попытки были предприняты, и используемый протокол. Межсетевой экран Black Hole компании Milkyway Networks регистрирует все действия сервера и предупреждает администратора о возможных нарушениях, посылая ему сообщение по электронной почте или на пейджер. Аналогичные функции выполняют и ряд других шлюзов прикладного уровня.

Шлюзы прикладного уровня позволяют обеспечить наиболее высокий уровень защиты, поскольку взаимодействие с внешним миром реализуется через

небольшое число прикладных полномочных программ-посредников, полностью контролирующих весь входящий и выходящий трафик.

Шлюзы прикладного уровня имеют ряд преимуществ по сравнению с обычным режимом, при котором прикладной трафик пропускается непосредственно к внутренним хост - компьютерам. Перечислю эти преимущества.

Невидимость структуры защищаемой сети из глобальной сети Internet. Имена внутренних систем можно не сообщать внешним системам через DNS, поскольку шлюз прикладного уровня может быть единственным хост - компьютером, имя которого должно быть известно внешним системам.

Надежная аутентификация и регистрация. Прикладной трафик может быть аутентифицирован, прежде чем он достигнет внутренних хост-компьютеров, и может быть зарегистрирован более эффективно, чем с помощью стандартной регистрации.

Оптимальное соотношение между ценой и эффективностью. Дополнительные или аппаратные средства для аутентификации или регистрации нужно устанавливать только на шлюзе прикладного уровня.

Простые правила фильтрации. Правила на фильтрующем маршрутизаторе оказываются менее сложными, чем они были бы, если бы маршрутизатор сам фильтровал прикладной трафик и отправлял его большому числу внутренних систем. Маршрутизатор должен пропускать прикладной трафик, предназначенный только для шлюза прикладного уровня, и блокировать весь остальной трафик.

Возможность организации большого числа проверок. Защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, что снижает вероятность взлома с использованием "дыр" в программном обеспечении.

К недостаткам шлюзов прикладного уровня относятся:

более низкая производительность по сравнению с фильтрующими маршрутизаторами; в частности, при использовании клиент-серверных протоколов, таких как TELNET, требуется двухшаговая процедура для входных и выходных соединений;

более высокая стоимость по сравнению с фильтрующим маршрутизатором.

Помимо TELNET и FTP шлюзы прикладного уровня обычно используются для электронной почты, Windows и некоторых других служб.

1.6. Усиленная аутентификация

Одним из важных компонентов концепции межсетевых экранов является аутентификация (проверка подлинности пользователя). Прежде чем пользователю будет предоставлено право воспользоваться, тем или иным сервисом, необходимо убедиться, что он действительно тот, за кого себя выдает.

Одним из способов аутентификации является использование стандартных UNIX-паролей. Однако эта схема наиболее уязвимо с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Многие инциденты в сети Internet произошли отчасти из-за уязвимости традиционных паролей. Злоумышленники могут наблюдать за каналами в сети Internet и перехватывать передающиеся в них открытым текстом пароли, поэтому схему аутентификации с традиционными паролями следует признать устаревшей.

Для преодоления этого недостатка разработан ряд средств усиленной аутентификации: смарт-карты, персональные жетоны, биометрические механизмы и т.п. Хотя в них задействованы разные механизмы аутентификации, общим для них является то, что пароли, генерируемые этими устройствами, не могут быть повторно использованы нарушителем, наблюдающим за установлением связи. Поскольку проблема с паролями в сети Internet является постоянной, межсетевой экран для соединения с Internet, не располагающий средствами усиленной аутентификации или не использующий их, теряет всякий смысл.

Ряд наиболее популярных средств усиленной аутентификации, применяемых в настоящее время, называются системами с одноразовыми паролями. Например, смарт-карты или жетоны аутентификации генерируют информацию, которую хост-компьютер использует вместо традиционного пароля. Результатом является одноразовый пароль, который, даже если он будет перехвачен, не может быть использован злоумышленником под видом пользователя для установления сеанса с хост - компьютером.

Так как межсетевые экраны могут централизовать управление доступом в сети, они являются подходящим местом для установки программ или устройств усиленной аутентификации. Хотя средства усиленной аутентификации могут

использоваться на каждом хост - компьютере, более практично их размещение на межсетевом экране. На рис. показано, что в сети без межсетевого экрана, использующего меры усиленной аутентификации, неаутентифицированный трафик таких приложений, как TELNET или FTP, может напрямую проходить к системам в сети. Если хост - компьютеры не применяют мер усиленной аутентификации, злоумышленник может попытаться взломать пароли или перехватить сетевой трафик с целью найти в нем сеансы, в ходе которых передаются пароли.

В этом случае сеансы TELNET или FTP, устанавливаемые со стороны сети Internet с системами сети, должны проходить проверку с помощью средств усиленной аутентификации, прежде чем они будут разрешены, Системы сети могут запрашивать для разрешения доступа и статические пароли, но эти пароли, даже если они будут перехвачены злоумышленником, нельзя будет использовать, так как средства усиленной аутентификации и другие компоненты межсетевого экрана предотвращают проникновение злоумышленника или обход ими межсетевого экрана.

1.6.1. Основные схемы сетевой защиты на базе межсетевых экранов

При подключении корпоративной или локальной сети к глобальным сетям администратор сетевой безопасности должен решать следующие задачи:

защита корпоративной или локальной сети от несанкционированного доступа со стороны глобальной сети;

скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети,

разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Необходимость работы с удаленными пользователями требует установки жестких ограничений доступа к информационным ресурсам защищаемой сети. При этом часто возникает потребность в организации в составе корпорационной сети нескольких сегментов с разными уровнями защищенности:

свободно доступные сегменты (например, рекламный WWW-сервер),

сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов),

закрытые сегменты (например, локальная финансовая сеть организации).

Для защиты корпоративной или локальной сети применяются следующие основные схемы организации межсетевых экранов:

межсетевой экран - фильтрующий маршрутизатор;

межсетевой экран на основе двупортового шлюза;

межсетевой экран на основе экранированного шлюза;

межсетевой экран - экранированная подсеть.

1.6.2. Межсетевой экран – фильтрующий маршрутизатор

Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации. Он состоит из фильтрующего маршрутизатора, расположенного между защищаемой сетью и сетью Internet. Фильтрующий маршрутизатор сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов. Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в сеть Internet, в то время как большая часть доступа к ним из Internet блокируется. Часто блокируются такие опасные службы, как X Windows, NIS и NFS.

1.6.3. Межсетевой экран на базе двупортового шлюза

Межсетевой экран на базе двупортового прикладного шлюза включает двудомный хост-компьютер с двумя сетевыми интерфейсами. При передаче информации между этими интерфейсами и осуществляется основная фильтрация. Для обеспечения дополнительной защиты между прикладным шлюзом и сетью Internet обычно размещают фильтрующий маршрутизатор. В результате между прикладным шлюзом и маршрутизатором образуется внутренняя экранированная

подсеть. Эту подсеть можно использовать для размещения доступных извне информационных серверов.

1.6.4. Межсетевой экран на основе экранированного шлюза

Межсетевой экран на основе экранированного шлюза объединяет фильтрующий маршрутизатор и прикладной шлюз, разрешаемый со стороны внутренней сети. Прикладной шлюз реализуется на хост - компьютере и имеет только один сетевой интерфейс.

1.6.5. Межсетевой экран - экранированная подсеть

Межсетевой экран, состоящий из экранированной подсети, представляет собой развитие схемы межсетевого экрана на основе экранированного шлюза. Для создания экранированной подсети используются два экранирующих маршрутизатора. Внешний маршрутизатор располагается между сетью Internet и экранируемой подсетью, а внутренний - между экранируемой подсетью и защищаемой внутренней сетью. Экранируемая подсеть содержит прикладной шлюз, а также может включать информационные серверы и другие системы, требующие контролируемого доступа. Эта схема межсетевого экрана обеспечивает хорошую безопасность благодаря организации экранированной подсети, которая еще лучше изолирует внутреннюю защищаемую сеть от Internet.

1.7. Возможности брандмауэра Windows

Он может:	Он не может:

Блокировать компьютерным вирусам и «червям» доступ на компьютер.	Обнаружить или обезвредить компьютерных вирусов и «червей», если они уже попали на компьютер. По этой причине необходимо также установить антивирусное программное обеспечение и своевременно обновлять его, чтобы предотвратить повреждение компьютера вирусами, «червями» и другими опасными объектами, а также не допустить использования данного компьютера для распространения вирусов на другие компьютеры.
Запросить пользователя о выбореблокировки или разрешения для определенных запросов на подключение.	Запретить пользователю открывать сообщения электронной почты с опасными вложениями. Не открывайте вложения в сообщениях электронной почты от незнакомых отправителей. Следует проявлять осторожность, даже если источник сообщения электронной почты известен и заслуживает доверия. При получении от знакомого пользователя электронного письма с вложением внимательно прочтите тему сообщения перед тем, как открыть его. Если тема сообщения представляет собой беспорядочный набор знаков или не имеет смысла, не открывайте письмо, пока не свяжетесь с отправителем для получения подтверждения.
Вести учет (журнал безопасности) -- по желанию пользователя -- записывая разрешенные и заблокированные попытки подключения к компьютеру. Этот журнал может оказаться полезным для диагностики неполадок.	Блокировать спам или несанкционированные почтовые рассылки, чтобы они не поступали в папку входящих сообщений. Однако некоторые программы электронной почты способны делать это. Ознакомьтесь с документацией своей почтовой программы, чтобы выяснить ее возможности.

ГЛАВА 2. СПОСОБЫ ФИЛЬТРАЦИИ ПРИ ПОМОЩИ IPTABLES

2.1. Netfilter/iptables

Ограничить весь входящий трафик, кроме трафика IMAP и HTTPS. Исходящий трафик может быть любой.

Фильтр по запросам. Разрешить трафик HTTP и блокировать пакеты по определенным словам.

Запретить пользователю доступ к сайтам vk.com и facebook.com

Для начального понимания архитектуры Netfilter/iptables отлично подойдет иллюстрация из википедии, которую я несколько модифицировал для большей прозрачности и понимания материала:

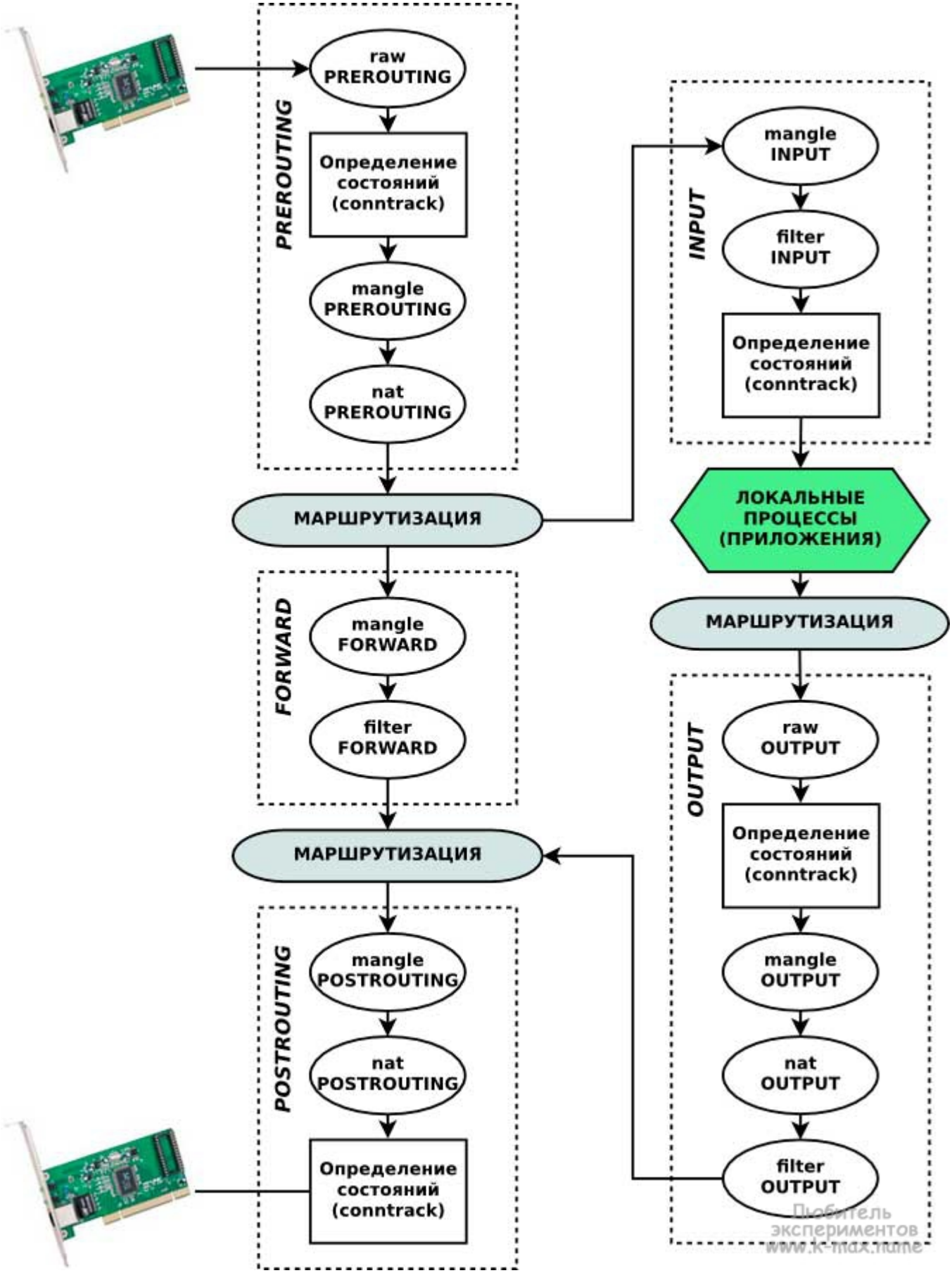

Рис.1 Архитектура netfiler/iptables в схеме

Сетевые пакеты поступают в сетевой интерфейс, настроенный на стек TCP/IP и после некоторых простых проверок ядром (например, контрольная сумма) проходят последовательность цепочек (chain) (обозначены пунктиром). Пакет обязательно проходит первоначальную цепочку PREROUTING. После цепочки PREROUTING, в соответствии с таблицей маршрутизации, проверяется кому принадлежит пакет и, в зависимости от назначения пакета, определяется куда он дальше попадет (в какую цепочку). Если пакет НЕ адресован (в TCP пакете поле адрес получателя - НЕ локальная система) локальной системе, то он направляется в цепочку FORWARD, если пакет адресован локальной системе, то направляется в цепочку INPUT и после прохождения INPUT отдается локальным демонам/процессам. После обработки локальной программой, при необходимости формируется ответ. Ответный пакет, отправляемый локальной системой в соответствии с правилами маршрутизации, направляется на соответствующий маршрут (хост из локальной сети или адрес маршрутизатора) и направляется в цепочку OUTPUT. После цепочки OUTPUT (или FORWARD, если пакет был проходящий) пакет снова сверяется с правилами маршрутизации и отправляется в цепочку POSTROUTING. Может возникнуть резонный вопрос: почему несколько раз пакет проходит через таблицу маршрутизации? (об этом - ниже).

Каждая цепочка, которую проходит пакет состоит из набора таблиц (table) (обозначены овалами). Таблицы в разных цепочках имеют одинаковое наименование, но тем не менее никак между собой не связаны. Например, таблица nat в цепочке PREROUTING никак не связана с таблицей nat в цепочке POSTROUTING. Каждая таблица состоит из упорядоченного набора (списка) правил. Каждое правило содержит условие, которому должен соответствовать проходящий пакет и действия к пакету, подходящему данному условию.

Проходя через серию цепочек пакет последовательно проходит каждую таблицу (в указанном на иллюстрации порядке) и в каждой таблице последовательно сверяется с каждым правилом (точнее сказать - с каждым набором условий/критериев в правиле), и если пакет соответствует какому-либо критерию, то выполняется заданное действие над пакетом. При этом, в каждой таблице (кроме пользовательских) существует заданная по умолчанию политика. Данная политика определяет действие над пакетом в случае, если пакет не соответствует ни одному из правил в таблице. Чаще всего — это действие ACCEPT, чтобы принять пакет и передать в следующую таблицу или DROP - чтобы отбросить пакет. В случае, если пакет не был отброшен, он завершает свое путешествие по ядру

системы и отправляется в сетевую карту сетевой интерфейс, которая подходит по правилам маршрутизации

Цепочки netfilter:

PREROUTING — для изначальной обработки входящих пакетов

INPUT — для входящих пакетов, адресованных непосредственно локальному компьютеру

FORWARD — для проходящих (маршрутизируемых) пакетов

OUTPUT — для пакетов, создаваемых локальным компьютером (исходящих)

POSTROUTING— для окончательной обработки исходящих пакетов

Также можно создавать и уничтожать собственные цепочки при помощи утилиты iptables.

Цепочки организованны в 4 таблицы:

raw — пакет проходит данную таблицу до передачи системе определения состояний. Используется редко, например, для маркировки пакетов, которые НЕ должны обрабатываться системой определения состояний. Для этого в правиле указывается действие NOTRACK. Содержится в цепочках PREROUTING и OUTPUT.

mangle — содержит правила модификации (обычно полей заголовка) IP-пакетов. Среди прочего, поддерживает действия TTL, TOS, и MARK (для изменения полей TTL и TOS, и для изменения маркеров пакета). Редко необходима и может быть опасна. Содержится во всех пяти стандартных цепочках.

nat — предназначена для подмены адреса отправителя или получателя. Данную таблицу проходят только первый пакет из потока, трансляция адресов или маскировка (подмена адреса отправителя или получателя) применяются ко всем последующим пакетам в потоке автоматически. Поддерживает действия DNAT, SNAT, MASQUERADE, REDIRECT. Содержится в цепочках PREROUTING, OUTPUT, и POSTROUTING.

filter — основная таблица, используется по умолчанию если название таблицы не указано. Используется для фильтрации пакетов. Содержится в цепочках INPUT, FORWARD, и OUTPUT.

Непосредственно для фильтрации пакетов используются таблицы filter. Поэтому в рамках данной темы важно понимать, что для пакетов, предназначенных данному узлу, необходимо модифицировать таблицу filter цепочки INPUT, для проходящих пакетов — цепочки FORWARD, для пакетов, созданных данным узлом — OUTPUT.

Ход работы:

Компьютер, на котором установлена операционная система Ubuntu 14.04 будет использоваться в качестве сервера для локальной подсети.

Таким образом будет задействовано 2 сетевых адаптера: проводной с помощью которого будет подключена операционная система и беспроводной – с помощью которого будет обеспечен выход в интернет.

Схема подключения:

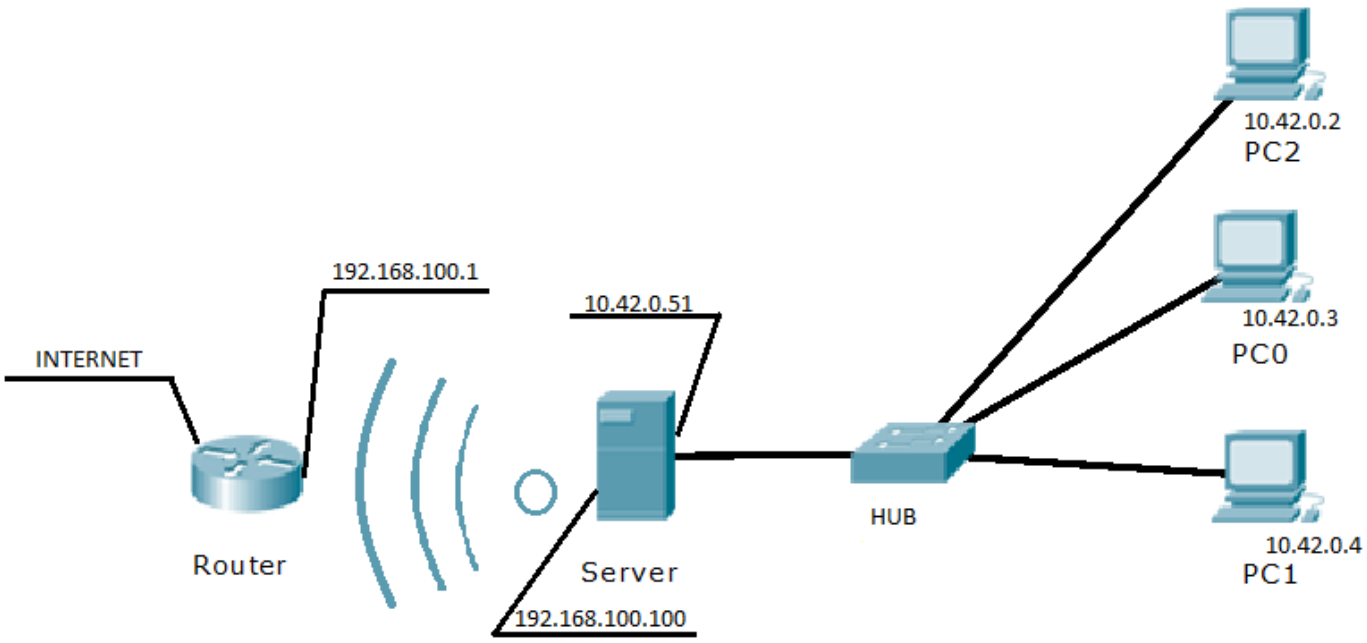

Рис.2 Схема подключения Пользователей к серверу.

2.2. Ubuntu.

На Ubuntu вся работа ведется в терминале (командная строка).

Открываем командную строку и командой

sudo apt-get install iptables
устанавливаем iptables.

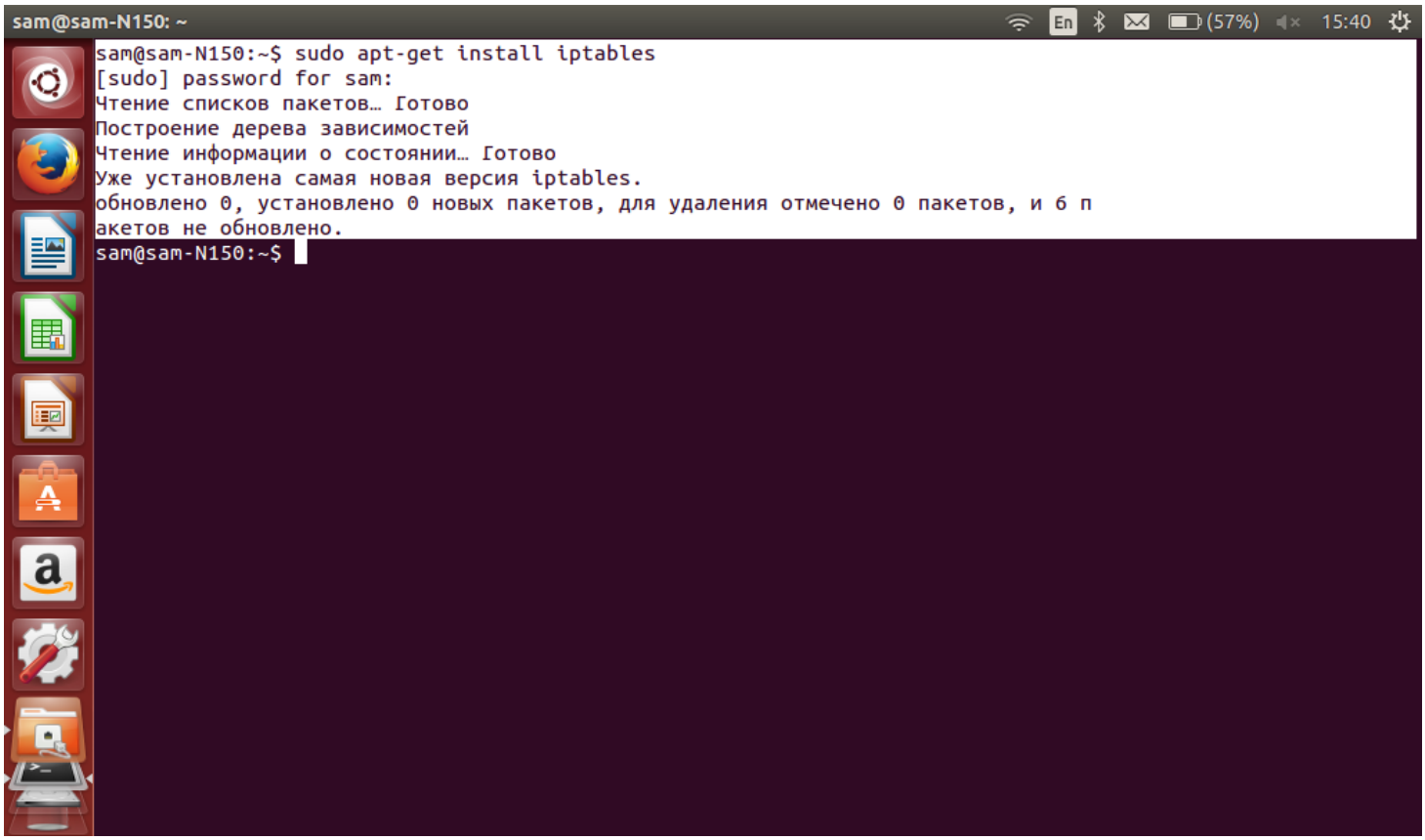

Рис.3.Установка iptables

Как видно на рисунке - iptables уже установлен и в обновлении не нуждается.

Для избежание ошибок очистим правила всех цепочек следующим набором команд:

sudo iptables -F INPUT
sudo iptables -F OUTPUT
sudo iptables -F FORWARD

Что бы увидеть какие правила назначены нужно выполнить команду
sudo iptables –L

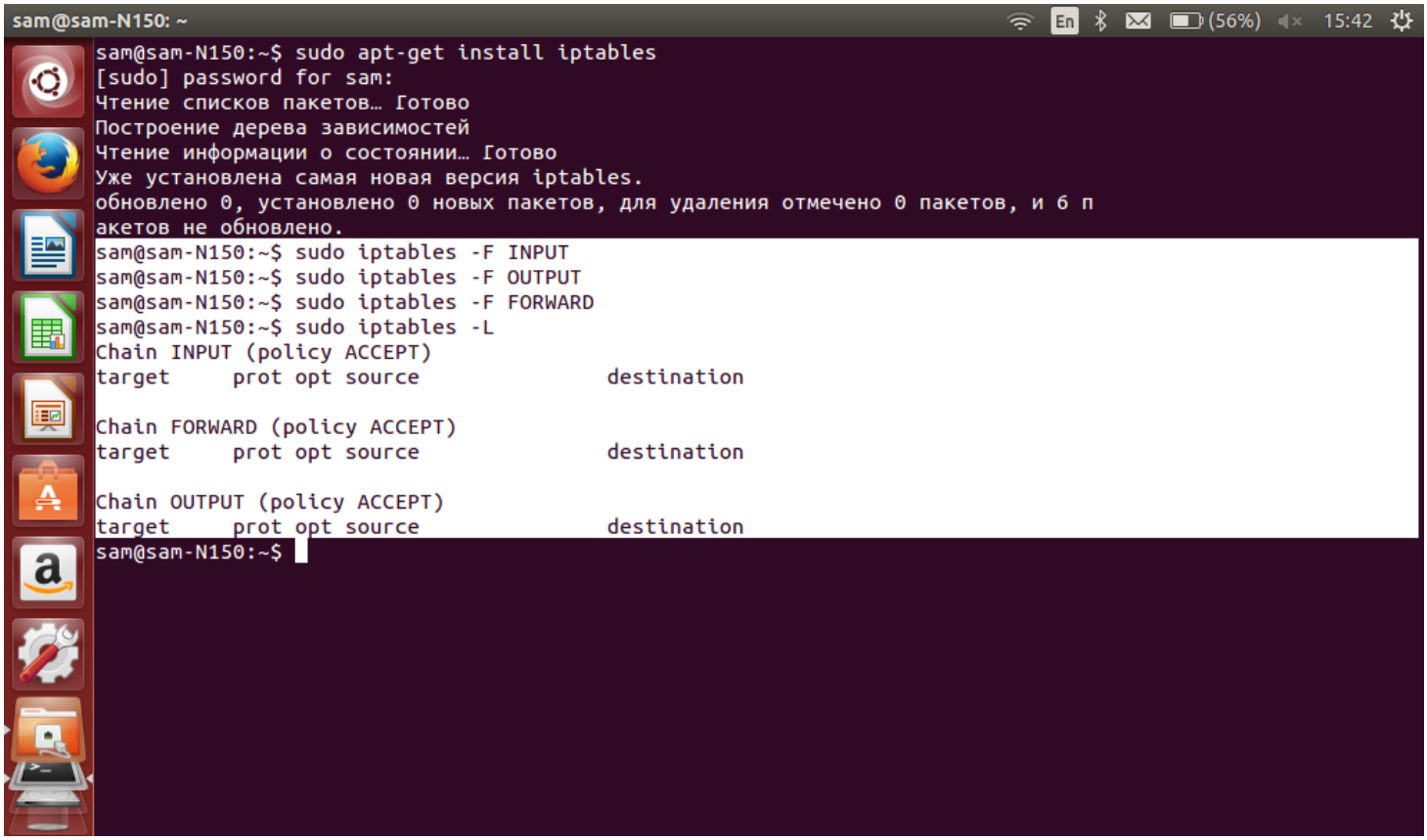

Рис.4 Правила iptables

По рисунку можно заметить, что никаких правил не назначено.

Поскольку весь трафик, который идет по протоколу https будет адресован не локальной сети 10.40.0.0/24 он пойдет по ветке FORWARD.

sudo iptables -A FORWARD -p tcp -s 10.42.0.0/24 -j ACCEPT
данная команда разрешает отправлять пакеты по протоколам tcp из подсети 10.42.0.0/24 в любую подсеть по любому порту

sudo iptables -A FORWARD -p tcp -d 10.42.0.0/24 --sport 53 -j ACCEPT
данная команда разрешает пакеты по протоколам tcp в подсеть 10.42.0.0/24 из любой подсети по 53 порту (данная команда разрешает локальным компьютерам принимать пакеты по протоколу DNS)

sudo iptables -A FORWARD -p tcp -d 10.42.0.0/24 --sport 443 -j ACCEPT
данная команда разрешает пакеты по протоколам tcp в подсеть 10.42.0.0/24 из любой подсети по 443 порту (данная команда разрешает локальным компьютерам принимать пакеты по протоколу HTTPS)

sudo iptables -A FORWARD -p tcp -d 10.42.0.0/24 --sport 143 -j ACCEPT
данная команда разрешает пакеты по протоколам tcp в подсеть 10.42.0.0/24 из любой подсети по 143 порту (данная команда разрешает локальным компьютерам принимать пакеты по протоколу IMAP)

sudo iptables -A FORWARD -j DROP
Данная команда сбрасывает все пакеты.

Все эти команды должны назначаться именно в этом порядке поскольку политика iptables заключается в построчной проверке правил. Если пакет подошел под данное правило, то на соответствие другим правилам он проверяться не будет. Если же пакет не подошел под данное правило, то он проверяется следующей строчкой, а именно следующим правилом. Таким образом: ели пакет ни подошёл ни под одно вышеописанное правило то его уничтожит последнее правило, которое сбрасывает все пакеты, попавшие на него.

Следующими правилами разрешим все пакеты на INPUT и OUTPUT.

sudo iptables –A INPUT –j ACCEPT

sudo iptables – A OUTPUT –j ACCEPT

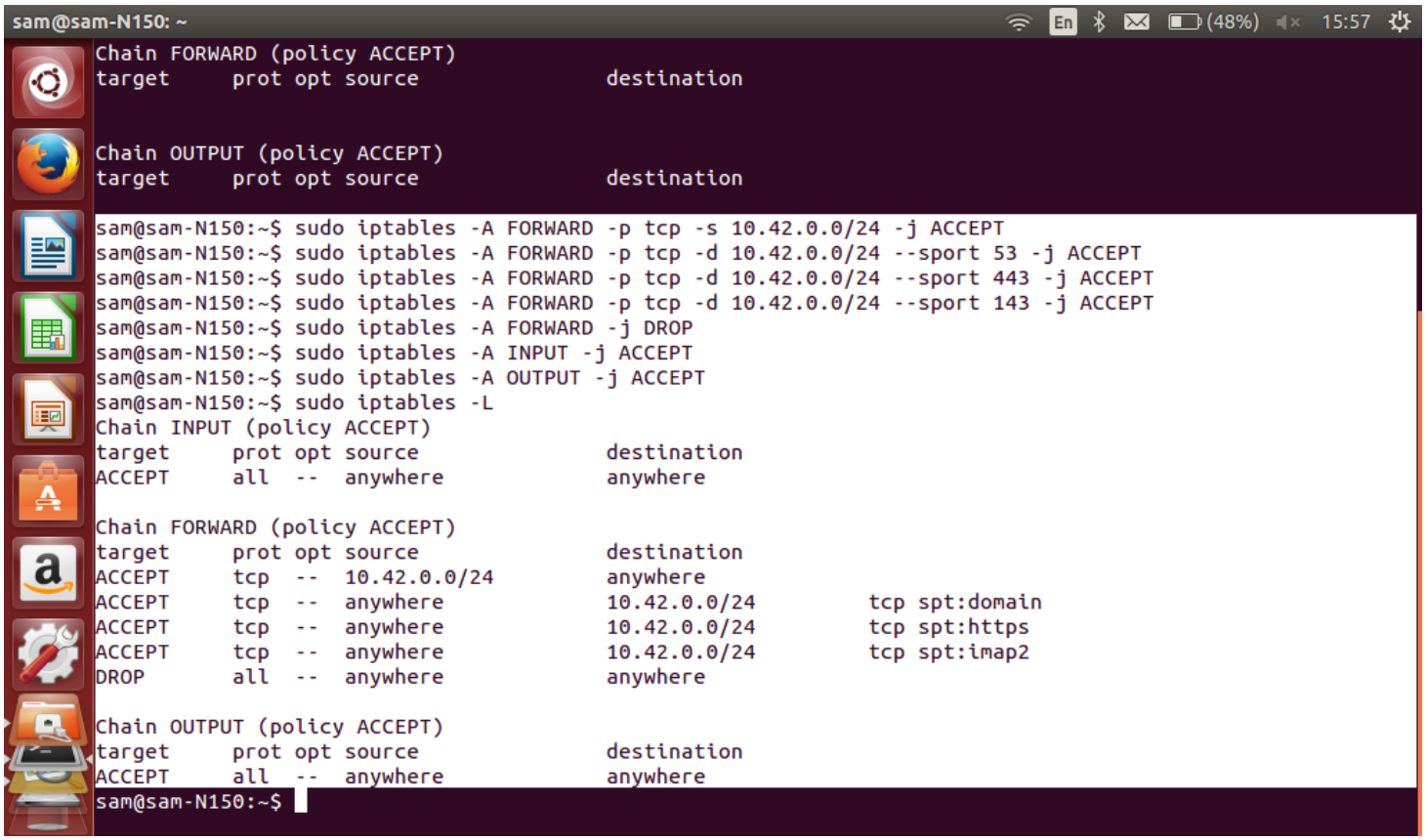

Рис.5 Таблица правил

Данные правила можно не выставлять поскольку iptables разрешает все пакеты по умолчанию, но только в том случае ели политика цепочки INPUT и OUTPUT находится в режиме ACCEPT. Для приведения политики в данное состояние можно использовать вышеописанные команды, а можно вместо них использовать команды, которые назначают именно состояние(режим):

sudo iptables –P INPUT ACCEPT
sudo iptables –P OUTPUT ACCEPT

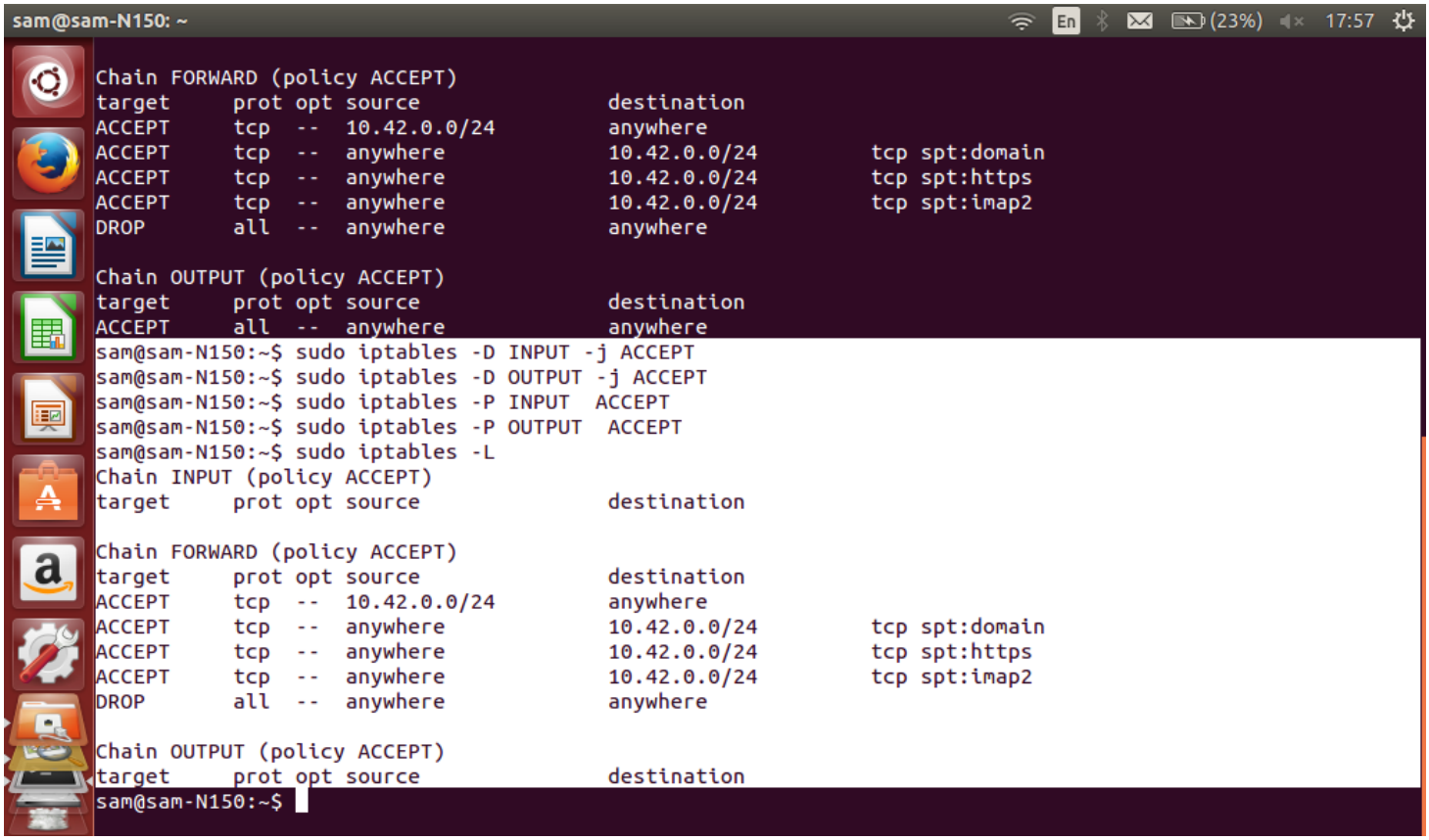

Рис.6 Таблица правил с изменениями

Эти команды можно так же не использовать поскольку по умолчанию режим INPUT и OUTPUT находится в режиме ACCEPT.

Связь проводного интерфейса и беспроводного интерфейса в Ubuntu происходит автоматически. Администратор только указывает правила, для пакетов, которые проходят между этими интерфейсами.

2.3. Фильтр по запросам

Суть фильтра по запросам заключается в том, что отправляемый пакет распаковывается проверяющим средством и проверяется на наличие запрещенных слов или словосочетаний.

Реализуется командой:

sudo iptables -A FORWARD -p tcp --dport 80 -m string --string "слово" --algo kmp -j DROP

Ограничиваем https запросы по слову «drugs»:

sudo iptables -I FORWARD 5 -p tcp -d 10.42.0.0/24 --dport 80 -m string --string " drugs" --algo kmp -j DROP
данная команда запрещает(сбрасывает) пакеты по протоколам tcp в подсеть 10.42.0.0/24 из любой подсети по 80 порту, с входящим в состав пакета словом «наркотики».

Затем нужно разрешить http трафик. Поскольку ранее исходящий трафик был разрешен любой, нужно разрешить прием трафика http.

sudo iptables -I FORWARD 6 -p tcp -d 10.42.0.0/24 --sport 80 -j ACCEPT
данная команда разрешает пакеты по протоколам tcp в подсеть 10.42.0.0/24 из любой подсети по 80 порту (данная команда разрешает локальным компьютерам принимать пакеты по протоколу HTTP)

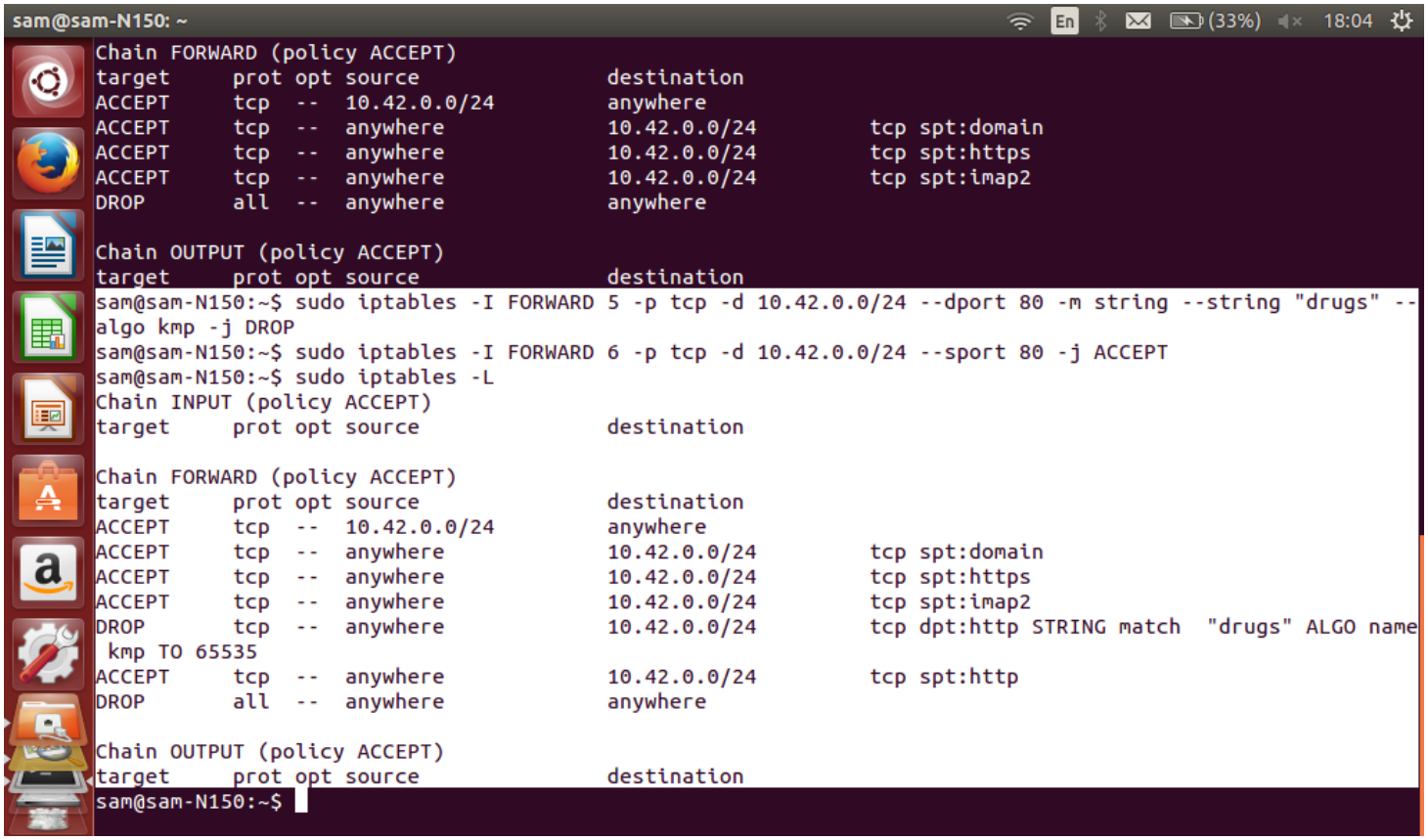

Рис.7 Фильтр по запросу «drugs»

Для того что бы заблокировать доступ к сайтам vk.com и facebook.com есть несколько способов реализации:

Вариант 1.

Обратиться к официальному сайту http://www.he.net/ который предоставляет информацию о всех префиксах по ipv4 для искомого сайта. Следовательно, как вариант для блокировки сайта можно прописать следующий набор команд:

sudo iptables -A FORWARD -s 87.240.128.0/18 -j DROP

sudo iptables -A FORWARD -s 93.186.224.0/21 -j DROP

sudo iptables -A FORWARD -s 93.186.232.0/21 -j DROP

sudo iptables -A FORWARD -s 95.142.192.0/21 -j DROP

sudo iptables -A FORWARD -s 87.240.184.0/24 -j DROP

sudo iptables -A FORWARD -s 95.142.206.0/24 -j DROP

sudo iptables -A FORWARD -s 95.213.0.0/18 -j DROP

sudo iptables -A FORWARD -s 185.32.248.0/22 -j DROP

sudo iptables -A FORWARD -s 95.142.200.0/21 -j DROP

После выполнения данного набора команд доступ к сайту vk.com будет заблокирован, но это сильно нагрузит процессор поскольку каждый пакет нужно будет проверять по каждому из этих правил.

Поэтому данный способ можно признать не актуальным, что бы сохранить вычислительную мощность сервера

Для сайта facebook.com адресов гораздо больше.

А в совокупности запрет к данным сайтам будет занимать большие вычислительные мощности центрального процессора.

Вариант 2.

Одним из вариантов является блокировка данных по запросу. Такой вариант исполняется набором команд

Для vk.com:

sudo iptables -A FORWARD -m string --string "vk.com" --algo kmp -j DROP

sudo iptables -A FORWARD -m string --string "m.vk.com" --algo kmp -j DROP

sudo iptables -A FORWARD -m string --string "lg.vk.com" --algo kmp -j DROP

Для facebook.com:

sudo iptables -A FORWARD -m string --string "facebook.com" --algo kmp -j DROP

sudo iptables -A FORWARD -m string --string "m.facebook.com" --algo kmp -j DROP

Данный вариант реализации использует меньшее количество команд, но системе придется открывать каждый пакет и полностью его просматривать, что так же снизит скорость обработки пакетов. Поэтому данный вариант возможен при больших вычислительных мощностях, но также является неактуальным.

Вариант 3.

Ещё одной реализацией ограничения доступа может являться сбрасывание пакетов по параметру правила -destination. Для реализации данного варианта понадобится команда

для vk.com:

sudo iptables -I FORWARD 1 -p tcp -d vk.com -j DROP

для дополнительного ограничения можно добавить команды

sudo iptables -I FORWARD 1 -p tcp -d m.vk.com -j DROP

sudo iptables -I FORWARD 1 -p tcp -d lg.vk.com -j DROP

для facebook.com:

sudo iptables -I FORWARD 1 -p tcp -d facebook.com -j DROP

sudo iptables -I FORWARD 1 -p tcp -d m.facebook.com -j DROP

Данный вариант является более приемлемым по количеству команд. Распаковка пакета при проверке идет не настолько глубокая по сравнению с вариантом 2, что так же сохраняет вычислительные мощности. Но перекрывает только один IP данного домена, а именно тот, который на данный момент отрезольвился приоритетным.

Сравнивая все три варианта исполнения ограничения доступа к выбранным сайтам можно сделать следующие выводы:

Вариант 1 перекрывает доступ к сайту полностью, но использует больше количество правил, что задействует большие вычислительные мощности процессора.

Вариант 2 задействует меньше вычислительной мощности по сравнению с вариантом 1, но блокирует сайты только по запросам и подходит в случае полной некомпетентности пользователей локальной сети в сфере сетей передачи данных.

Вариант 3 блокирует доступ не полностью, но задействует меньше вычислительной мощности по сравнению с вариантом 2 и перекрывает больший диапазон пакетов.

Если есть большие мощности, то для блокировки лучше использовать вариант 1, если пользователи некомпетентны, то лучше использовать вариант 2, если

мощности мало, то можно ограничиться вариантом 3.

Самым наилучшим решением будет использовать все три варианта в совокупности, но при условии, что имеется большие мощности процессора на сервере

Применимо к используемому маломощному серверу выбираем вариант 3.

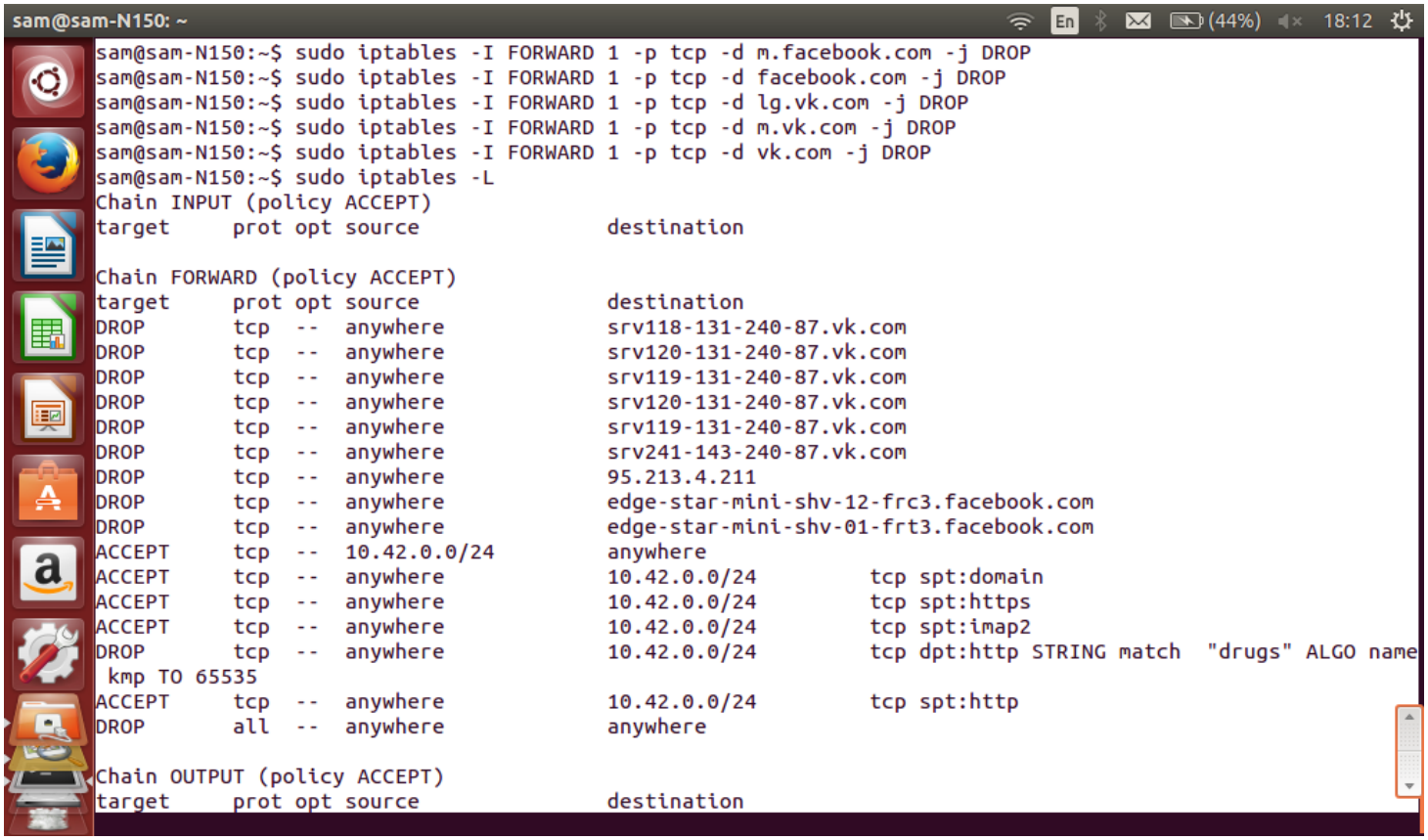

Рис.8 Ограничение доступа к заданным сайтам по параметру –destination

2.4. Итог.

Итоговый набор правил iptables для локальной подсети 10.42.0.0/24 который указывается именно в данном порядке:

sudo apt-get install iptables
sudo iptables -F INPUT
sudo iptables -F OUTPUT
sudo iptables -F FORWARD
sudo iptables -A FORWARD -p tcp -s 10.42.0.0/24 -j ACCEPT
sudo iptables -A FORWARD -p tcp -d 10.42.0.0/24 --sport 53 -j ACCEPT

sudo iptables -A FORWARD -p tcp -d 10.42.0.0/24 --sport 443 -j ACCEPT
sudo iptables -A FORWARD -p tcp -d 10.42.0.0/24 --sport 143 -j ACCEPT
sudo iptables -A FORWARD -j DROP
sudo iptables -I FORWARD 5 -p tcp -d 10.42.0.0/24 --dport 80 -m string --string "
наркотики" --algo kmp -j DROP
sudo iptables -I FORWARD 6 -p tcp -d 10.42.0.0/24 --sport 80 -j ACCEPT
sudo iptables -I FORWARD 1 -p tcp -d m.facebook.com -j DROP
sudo iptables -I FORWARD 1 -p tcp -d facebook.com -j DROP
sudo iptables -I FORWARD 1 -p tcp -d lg.vk.com -j DROP
sudo iptables -I FORWARD 1 -p tcp -d m.vk.com -j DROP
sudo iptables -I FORWARD 1 -p tcp -d vk.com -j DROP

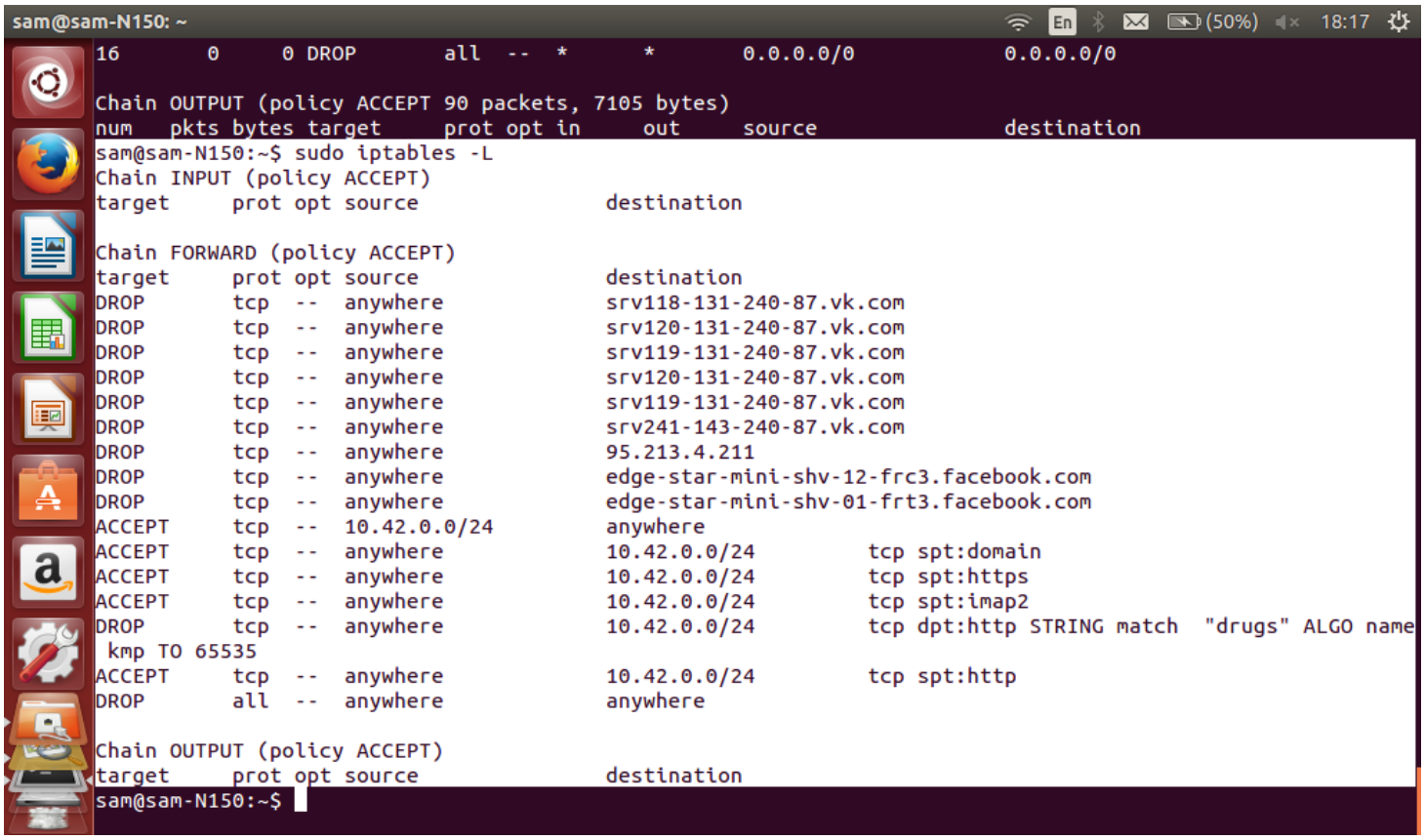

Рис.9 Итоговая таблица правил iptables для локальной подсети 10.42.0.0/24

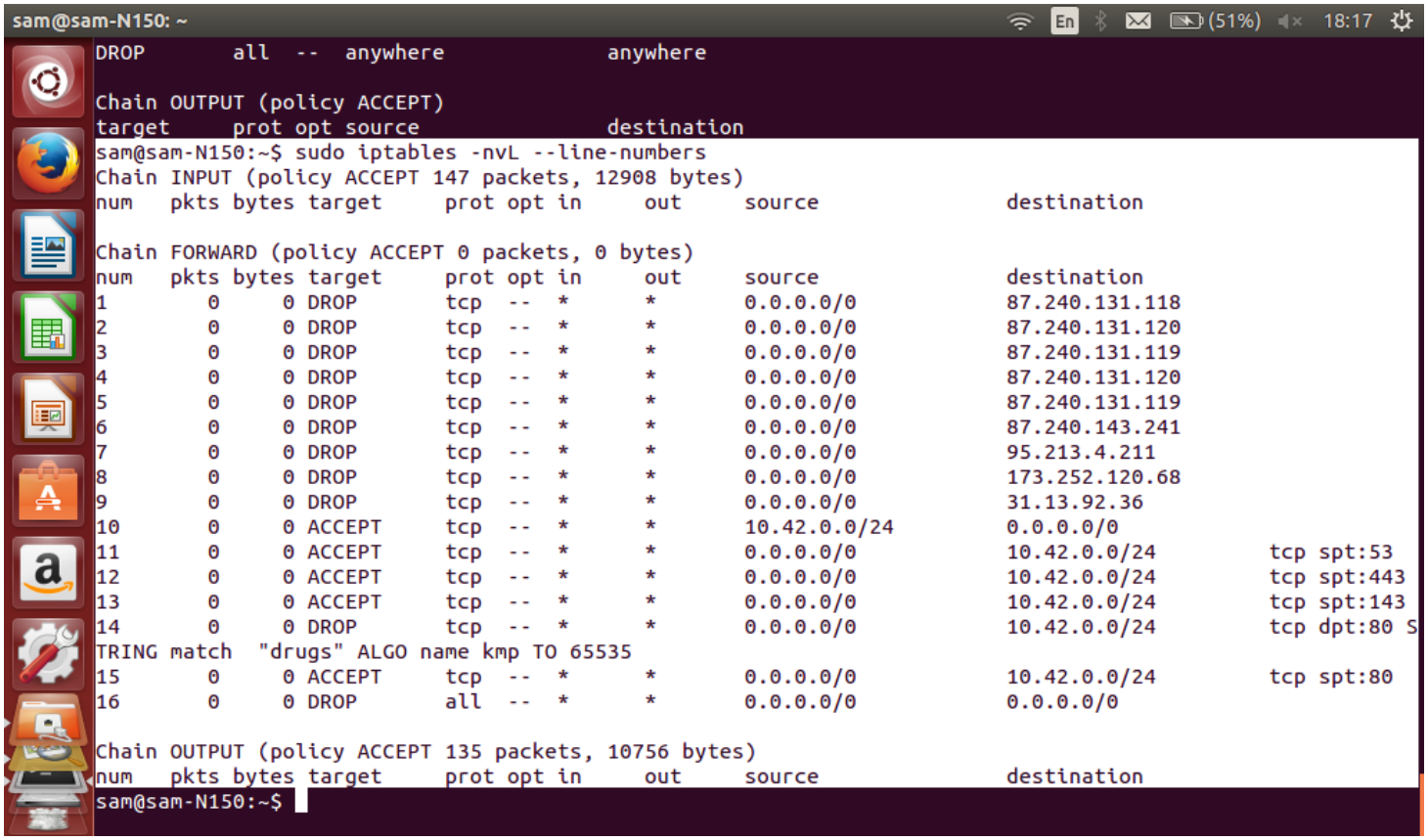

Рис.10 Итоговая таблица правил iptables для локальной подсети 10.42.0.0/24 с номерами строк и ip адресами

Описанный способ применим только для фильтрации пакетов локальной подсети, которая отличается от подсети сервера. При данном исполнении фильтрация пакетов происходит между двумя интерфейсами сервера с iptables. С точки зрения безопасности выбранной подсети 10.42.0.0/24 данная совокупность правил отвечает заявленным требованиям, но сервер сам сервер остается абсолютно беззащитным для атак.

Одним из вариантов защиты данного сервера является запрещение всего входящего трафика кроме удалённого подключения SSH. Так же ограничим количество параллельных соединений по SSH до 1. Все другие пакеты будем запрещать

sudo iptables -A INPUT -p tcp --dport 22 -m connlimit --connlimit-above 1 -j ACCEPT
sudo iptables –A INPUT –j DROP
sudo iptables -A OUTPUT -p tcp --sport 22 -m connlimit --connlimit-above 1 -j ACCEPT
sudo iptables –A OUTPUT –j DROP

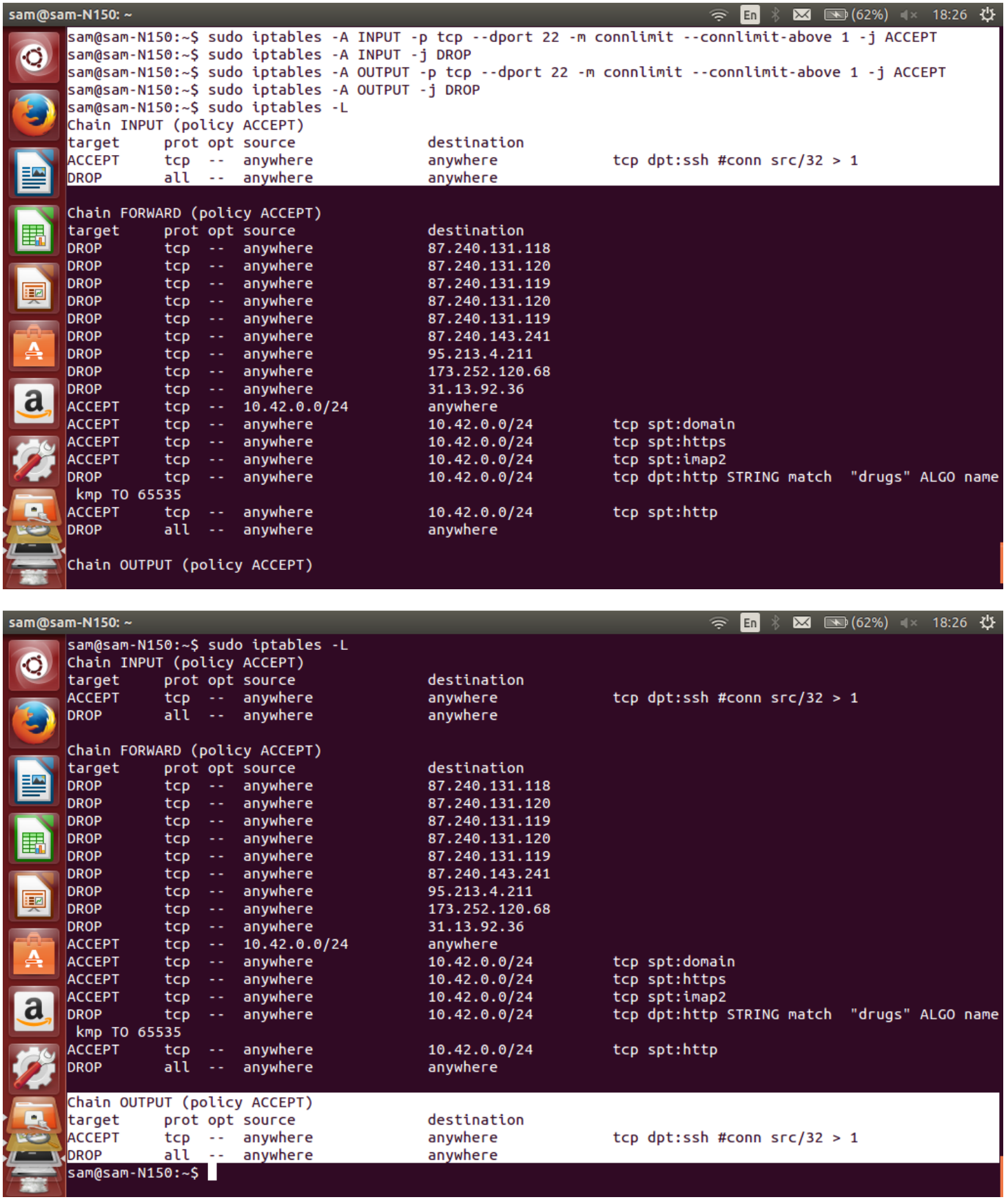

Рис.11 Защита сервера с открытым SSH для iptables

Если данное подключение не требуется и iptables будет настраиваться непосредственно на самой машине, то и трафик SSH можно не допускать.

sudo iptables –A INPUT –j DROP
sudo iptables –A OUTPUT –j DROP

либо

sudo iptables –P INPUT –j DROP
sudo iptables –P OUTPUT –j DROP

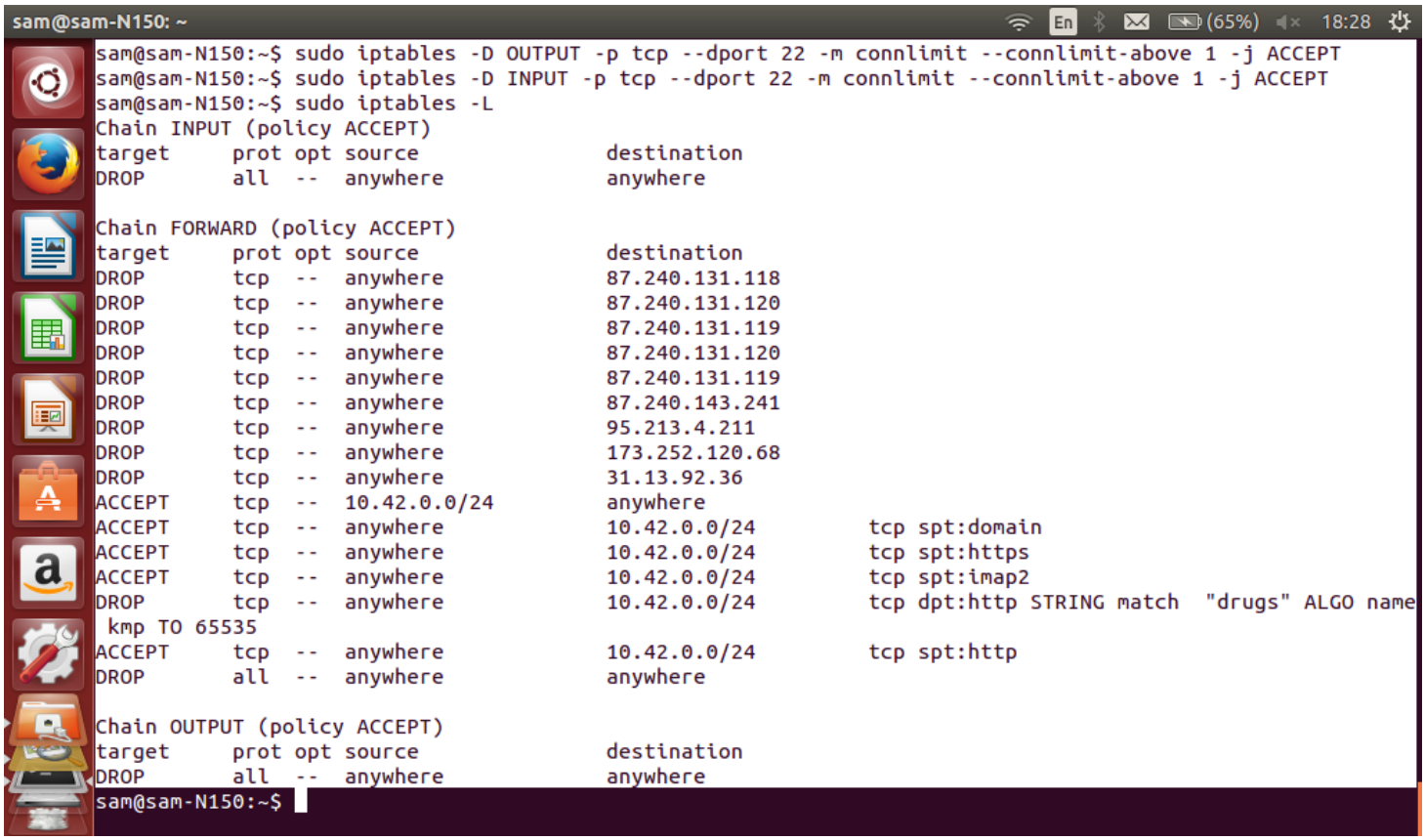

Рис.12 Защита сервера с iptables

Заключение

После всего изложенного материала можно заключить следующее.

На сегодняшний день лучшей защитой от компьютерных преступников является брандмауэр, правильно установленный и подобранный для каждой сети. И хотя он не гарантирует стопроцентную защиту от профессиональных взломщиков, но зато

усложняет им доступ к сетевой информации, что касается любителей, то для них доступ теперь считается закрытым. Также в будущем межсетевые экраны должны будут стать лучшими защитниками для банков, предприятий, правительств, и других спецслужб. Также есть надежда, что когда-нибудь будет создан межсетевой экран, который никому не удастся обойти. На данном этапе программирования можно также заключить, что разработки по брандмауэрам на сегодняшний день сулят в недалёком будущем весьма неплохие результаты.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Балдин Константин, Уткин Владимир «Информатика», Москва, 2003г.

2.Дьяконов Владимир, Абраменкова Ирина, Пеньков Александр «Новые информационные технологии», Москва, 2006г.

3.Фридланд А. «Основные ресурсы информатики», Москва, 2007г.

4. Чернышов М.К., Чернышова Е.В. Особенности установки и настройки операционных систем MAC OS X НА PC // Актуальные направления научных исследований XXI века: теория и практика. – 2015. – Т. 3. – № 5–2. – С. 206–214.

Интернет-ресурсы:

1. Аверченков, В.И. Аудит информационной безопасности: учебное пособие для вузов / В.И. Аверченков. – 2-е изд., стер. – М.: Флинта, 2011. – 269 с. – ISBN 978-5-9765-1256-6; То же [Электронный ресурс].
– https://biblioclub.ru/index.php?page=book&id=93245: (15.03.2017).

2. Порт 22. Безопасное соединение. [Электронный ресурс]. –http://www.port-22.ru/ (15.03.2017).

3. ФСТЭК России. [Электронный ресурс]. – http://www.fstec.ru/(15.03.2017).

4. АПКИТ [Электронный ресурс]. – http://apkit.ru/ (15.03.2017).

5. ASPE [Электронный ресурс].
– http://aspe.hhs.gov/admnsimp/pl104191.htm (15.03.2017).

6. Центр аудита информационной безопасности [Электронный ресурс].
– http://bezpeka.ladimir.kiev.ua/index.php (15.03.2017).

7. BEST of security [Электронный ресурс]. – http://bos.dn.ua/(15.03.2017).

8. Академик [Электронный ресурс]. – http://dic.academic.ru/ (15.03.2017).

9. Сентр.ру [Электронный ресурс].
– http://edocs.al.ru/secure/content.html(15.03.2017).

10. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ИНТЕРНЕТ БУДУЩЕГО[Электронный ресурс]. – http://internet-future.narod.ru/ (15.03.2017).

11. Professional [Электронный ресурс]. – http://it-professional.ru/(15.03.2017).

12. Служба безопасности [Электронный ресурс].
– http://sb.adverman.com/(15.03.2017).

13. Информационные войны и информационная безопасность. [Электронный ресурс]. – http://ww-4.narod.ru/warfare/warfare.htm(15.03.2017).

14. Abbyy [Электронный ресурс]. – http://www.abbyy.ru/ (15.03.2017).