электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

**УДК 004.514.6**

# Разработка административного интерфейса межсетевого экрана типа «пакетный фильтр»

***Карондеев АМ.***, *студент*
*кафедра «Информационная безопасность»*
*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана*

***Терещенко В.А.***, *студент*
*кафедра «Информационная безопасность»*
*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана*

*Научный руководитель: Старчак С.Л., д.т.н., доцент, профессор*
*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана*

*Научный консультант: Морозов Ю.В., к.т.н., начальник отдела*
*НИИЦ (г. Москва) «ЦНИИ ВВКО» МО РФ*
*starchak@bmstu.ru*

## Введение

Развитие сетей, в том числе и сети Интернет, выявило и обострило проблемы, возникающие при безопасном подключении корпоративной сети к внешним недоверенным сетям. Связано это, в первую очередь, с тем, что в качестве недоверенной чаще всего выступает сеть интернет, которая разрабатывалась как открытая, предназначенная для всех, система. Поэтому вопросам безопасности при проектировании стека протоколов TCP/IP, являющихся основой практически всех сетей, уделялось довольно мало внимания.

Для устранения проблем, связанных с безопасностью, было разработано много различных решений, самым известным и распространенным из которых является применение межсетевых экранов (МСЭ) или брандмауэров. Развитие технологий и приложений приводит к открытию все новых лазеек для злоумышленников, а практическая реализация системы безопасности усложняется. В связи с этим функциональность современных МСЭ значительно расширилась и теперь к ним предъявляются больше требований. Одним из требований к современным МСЭ является обеспечение безопасной работы приложений с помощью удобных графических интерфейсов, позволяющих сформировать унифицированную

политику безопасности.

В настоящей работе рассмотрены классификации МСЭ, предложена собственная классификация по типу интерфейса управления МСЭ, изучены требования к современным МСЭ, а также проделана работа по созданию вебинтерфейса доступа к МСЭ в ОС Эльбрус на основе встроенного МСЭ типа пакетный фильтр.

**Классификация МСЭ**

До сих пор не существует единой и общепризнанной классификации межсетевых экранов. Каждый производитель выбирает удобную для себя классификацию и приводит ее в соответствие с разработанным этим производителем МСЭ. Однако, можно выделить следующие их классы, учитывающие уровни OSI или стека TCP/IP (также данная классификация отражает область применения МСЭ):

- коммутаторы, функционирующие на канальном уровне;
- сетевые или пакетные фильтры, которые, как видно из названия, функционируют на сетевом уровне;
- шлюзы сеансового уровня (*circuit-level proxy*);
- посредники (агенты) прикладного уровня (*application proxy или application gateway*);
- инспекторы состояния (*stateful inspection*).

Как правило, современный МСЭ совмещает в себе функции двух, трех и более типов. Технология инспектор состояния (*Stateful Inspection*) или иначе динамическая фильтрация пакетов (*Dynamic Packet Filtering*) – технология построения межсетевых экранов, объединяющая в себе положительные свойства большинства вышеназванных типов, существует и развивается в настоящее время наиболее активно. МСЭ в этом случае является, по сути, шлюзом сеансового уровня с расширенными возможностями. Инспекторы состояния оперируют на сеансовом уровне, но «понимают» протоколы прикладного и сетевого уровней. В отличие от шлюза прикладного уровня, открывающего два виртуальных канала TCP (один — для клиента, другой — для сервера) для каждого соединения, инспектор состояния не препятствует организации прямого соединения между клиентом и сервером. В настоящий момент практически все коммерческие МСЭ анонсируются, как относящиеся к этой категории.

Если организация располагает исходными текстами МСЭ и в состоянии их модифицировать должным образом, перед ней открываются широкие возможности по настройке МСЭ с учетом собственных нужд. В связи с этим утверждением, а так же необходимостью удобного управления МСЭ ниже описана разработка интерфейса управления МСЭ типа пакетный фильтр.

МСЭ можно также разделять на классы по расположению:

*Персональный брандмауэр* – программа, которая устанавливается на каждую автоматизированную рабочую станцию в сети и контролирует соединения, которые пытается установить то или иное приложение.

*Распределённый межсетевой экран,* как правило, устанавливается в «разрыв» между внутренней и внешней сетью, проверяет весь трафик, который проходит через него. При наличии достаточно большой сети имеет смысл установка нескольких межсетевых экранов: для каждого отдела или рабочей группы – в качестве средства защиты от атак внутри сети компании.

МСЭ, как и любое другое сетевое устройство, должен каким-либо образом управляться. Различные функции и возможности упрощают и совершенствуют эксплуатацию, мониторинг и оптимизацию управления сетью в целом. Управление может происходить как локально, так и удаленно. Как правило, для этих целей используют один и тот же интерфейс управления. Иногда, в зависимости от навыков оператора, а так же конкретики поставленной задачи или скорости ее выполнения используются различные интерфейсы управления (терминальный доступ или доступ с помощью вебинтерфейса). Предлагается классификация МСЭ по типу интерфейса управления:

1) *Командный интерфейс.* Может быть реализован в виде пакетной технологии (когда команды компьютеру передаются в виде пакетов данных) или технологии командной строки (символьный интерфейс).

2) *WIMP–интерфейс* (Window – окно, Image – образ, Menu – меню, Pointer – указатель). Характерной особенностью этого вида интерфейса является то, что диалог с пользователем ведется не с помощью команд, а с помощью графических образов – меню, окон, других элементов. Хотя и в этом интерфейсе подаются команды машине, но это делается опосредственно, через графические образы. Этот вид интерфейса реализован на двух уровнях технологий:

- простой графический интерфейс;
- «истинно-графический» *WIMP* – интерфейс (графические элементы управления представляют собой двумерные либо трехмерные объекты).

3) *Речевой интерфейс управления* – наиболее удобный для человека вид управления, но он имеет достаточно низкую распространенность ввиду своей ресурсозатратности, сложности разработки и неточности распознавания голоса (для произвольного оператора). Интерес к разработкам в данной области демонстрируют крупные зарубежные корпорации (Google, Apple). Их продукты часто снабжены речевым интерфейсом управления.

На сегодняшний день второй тип интерфейса управления является преобладающим, что обусловлено удобством в использовании и простотой разработки.

**Требования к современным МСЭ**

Хотя традиционные межсетевые экраны остаются фундаментальным средством обеспечения безопасности, они неэффективны при защите от сложных сетевых атак. Развитие технологий и приложений приводит к открытию все новых лазеек для злоумышленников, а практическая реализация системы безопасности усложняется. Чтобы противостоять меняющимся угрозам, производителям приходится активизировать разработку новых методов выявления и предотвращения атак и блокирования нежелательного сетевого трафика. Например, не для кого не секрет, что традиционные МСЭ, как правило, идентифицируют приложение по используемому TCP-порту, FTP-клиент работает через порт TCP/21, MySQL - TCP/3306 и т.д. Пользователи идентифицируются исходя из IP-адреса источника. Однако современные приложения уже давно не используют одни и те же статические порты, более того, некоторые приложения меняют номера портов во время коммуникационной сессии. За пользователем сегодня вовсе не обязательно закреплен один и тот же IP-адрес. Понимая данную специфику, в основу современных МСЭ производители закладывают идентификацию приложений, пользователей и угроз. Основная часть таких МСЭ - политики безопасности создаются на основе пользователей и приложений. Стоит отметить, что многие производители применяют, так называемых, помощников МСЭ, таких как IPS, URL-фильтрация и т.д. Несмотря на то, что весь функционал находится в одной коробке, его настройки находятся на различных вкладках, политиках, что затрудняет процесс написания политик ИБ, помимо этого трафик проходит через все эти “помощники”

поочередно, что увеличивает задержки. В современном МСЭ должны быть реализованы:

- Идентификация пользователей, а не только IP-адресов - использование информации о пользователях и группах из корпоративных каталогах для мониторинга, создания политик, формирования отчетов и расследование инцидентов в сфере ИБ независимо от местоположения пользователя.
- Анализ контента в режиме реального времени - защита сети от попыток использования эксплойтов для известных уязвимостей и распространения вредоносных программ в трафике уровня приложений независимо от источника.
- Упрощенное управление политиками - обеспечение безопасной работы приложений с помощью удобных графических интерфейсов, которые позволяют сформировать унифицированную политику безопасности.
- Формирование логического периметра - защита всех пользователей, включая сотрудников, находящихся в командировке, и удаленных работников, с помощью согласованных механизмов обеспечения безопасности, формирующих не физический, а логический периметр сети.
- Обеспечение мультигигабитной пропускной способности - сочетание специализированного оборудования и программного обеспечения для достижения мультигигабитной производительности с низкими задержками при всех включенных службах.

Стоит отметить, что существуют угрозы, которым МСЭ не может противостоять. Кроме того, применение МСЭ создает определенные трудности. Наиболее очевидным недостатком МСЭ является большая вероятность того, что он может *заблокировать* некоторые необходимые пользователю службы, такие как Telnet, FTP, XWindow, NFS и т.д. Однако, эти недостатки присущи не только МСЭ, доступ к сети может быть ограничен также и на уровне отдельных СВТ, в зависимости от методики обеспечения безопасности сети. Некоторые объекты могут обладать топологией, не предназначенной для использования МСЭ, или использовать службы (сервисы) таким образом, что его использование потребовало бы полной реорганизации локальной сети. Далее, МСЭ не защищают системы локальной сети от проникновения через "*люки*" (*backdoors*). Например, если на систему, защищенную МСЭ, все же разрешается неограниченный модемный доступ, злоумышленник может с успехом обойти МСЭ. Связь через протоколы PPP (Point-to-Point) и SLIP (Serial Line

IP) в рамках защищенной подсети является, по существу, еще одним сетевым соединением и потенциальным каналом нападения. МСЭ, как правило, не обеспечивает защиту от внутренних угроз. С одной стороны, МСЭ можно разработать так, чтобы предотвратить получение конфиденциальной информации злоумышленниками из внешней сети, однако, МСЭ не запрещает пользователям внутренней сети копировать информацию на носители или выводить ее на печатающее устройство. Таким образом, было бы ошибкой полагать, что наличие МСЭ обеспечивает защиту от внутренних атак или вообще атак, для которых не требуется использование МСЭ. Кроме того, есть недостаток МСЭ, связанный с низкой пропускной способностью - МСЭ представляют собой потенциально узкое место, поскольку все соединения с сетью Интернет должны осуществляться через него и еще подвергаться фильтрации. Существует также и возможность "*общего риска*" - в МСЭ все средства безопасности сосредоточены в одном месте, а не распределены между системами сети. Компрометация МСЭ ведет к нарушению безопасности для других, менее защищенных систем.

**Реализация интерфейса управления**

Для реализации интерфейса МСЭ был выбран клиент-ориентированный вебинтерфейс. В качестве программного средства был выбран веб-сервер apache, язык программирования perl, язык разметки html, каскадные таблицы стилей CSS.

При разработке управляющего интерфейса для него учитывались требования к МСЭ по 2 классу защищенности [5]. Из них применительно к интерфейсу были соблюдены следующие:

1. Администрирование: идентификация и аутентификация
   1) МСЭ должен обеспечивать идентификацию и аутентификацию администратора МСЭ при его запросах на доступ.
   2) МСЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору и паролю временного действия.
   3) МСЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.
   4) При удаленных запросах на доступ администратора МСЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и

активному перехвату информации.

Для реализации вышеуказанных требований использована встроенная аутентификация пользователей в ОС Эльбрус на основе подключаемых модулей аутентификации (PAM). Для того, чтобы произвести аутентификацию с помощью PAM-модуля, операционная система вызывает его посредством системной библиотеки (рис. 1). В нашем случае PAM-модуль используется вебсервером для аутентификации пользователей по идентификатору и паролю (рис. 2). Для обеспечения устойчивости против перехвата регистрационных данных пользователя используется защищенное соединение между клиентом (браузером клиента) и сервером на основе SSL сертификата. При условии, что администратор находится в локальной сети с МСЭ, данный прием обеспечивает приемлемый уровень защиты от перехвата передаваемых по сети аутентификационных данных. Дополнительно при передаче идентификатора и пароля администратора они хешируются с помощью алгоритма MD5.

Рис. 1. Взаимодействие между ОС Эльбрус, модулем аутентификации, вебсервером и браузером клиента

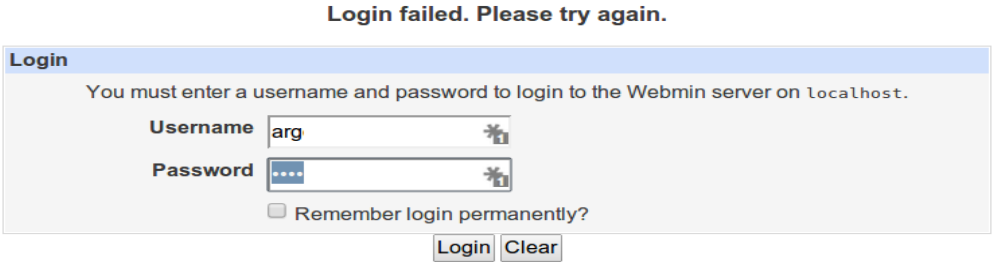


Рис. 2. Авторизация пользователя в административном интерфейсе.

2. Администрирование: регистрация

- МСЭ должен обеспечивать регистрацию входа (выхода) администратора МСЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МСЭ;
- В параметрах регистрации указываются:

- дата, время и код регистрируемого события;
- результат попытки регистрирации события - успешная или неуспешная;
- идентификатор администратора МСЭ, предъявленный при попытке осуществления регистрируемого события.
- МСЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).
- МСЭ должен обеспечивать регистрацию действия администратора МСЭ по изменению правил фильтрации.

Роль системы аудита выполняет системный журнал ОС Эльбрус. Регистрацию запуска программ и процессов обеспечивает системный журнал ОС Эльбрус, некоторые службы и программы ведут свои собственные журналы (рис. 3). Регистрацию действий администратора выполняет модуль регистрации событий аутентификации в составе PAM-модуля.

3. Администрирование: простота использования

- Многокомпонентный МСЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

Графический интерфейс является дружелюбным для пользователей (рис. 4). Администраторы могут устранять неисправности в сети, не мешая работе пользователей. Сеть администрируется в оперативном режиме. Программы и сервисы МСЭ можно запускать удаленно, с любого рабочего места сети. Веб-интерфейс, доступный по сети, обеспечивает дистанционное управление МСЭ, а также возможность конфигурирования сервисов, проверки взаимной согласованности всех фильтров, и просмотра журналов событий.

Настройка модуля

Системный журнал

Добавить

| Куда записывается журнал | Ведется? | Выбранные сообщения | |
|---|---|---|---|
| Файл /var/log/auth.log | Да | auth,authpriv.* | Просмотреть.. |
| Файл /var/log/syslog | Да | *.* ; auth,authpriv.none | Просмотреть.. |
| Файл /var/log/cron.log | Нет | cron.* | |
| Файл /var/log/daemon.log | Нет | daemon.* | |
| Файл /var/log/kern.log | Да | kern.* | Просмотреть.. |
| Файл /var/log/lpr.log | Нет | lpr.* | |
| Файл /var/log/mail.log | Да | mail.* | Просмотреть.. |
| Файл /var/log/user.log | Нет | user.* | |
| Файл /var/log/mail.info | Нет | mail.info | |
| Файл /var/log/mail.warn | Нет | mail.warn | |
| Файл /var/log/mail.err | Да | mail.err | Просмотреть.. |
| Файл /var/log/news/news.crit | Да | news.crit | Просмотреть.. |
| Файл /var/log/news/news.err | Да | news.err | Просмотреть.. |
| Файл /var/log/news/news.notice | Да | news.notice | Просмотреть.. |
| Файл /var/log/debug | Нет | news.none ; mail.none | |
| Файл /var/log/messages | Нет | mail,news.none | |
| Сообщение пользователям :omusrmsg:* | Да | *.emerg | |
| Файл /dev/tty8 | Нет | *.=notice ; *.=warn | |
| Именованный канал /dev/xconsole | Да | *.=notice ; *.=warn | |
| Файл /var/webmin/miniserv.error | Да | Лог ошибок Webmin | Просмотреть.. |
| Output from dmesg | Да | Сообщения ядра | Просмотреть.. |

Добавить

Рис. 3. Различные журналы, доступные для просмотра через вебинтерфейс.

Настройка модуля

Настройка

Управление доступом по IP
Порт и адрес
Журнал
Прокси-сервер
Внешний вид
Модули
Операционная система и переменные окружения
Язык
Главное меню
Обновление
Аутентификация
Two-Factor Authentication
Категории модулей
Список категорий
Названия модулей
Темы Webmin
Проверка ссылок
Анонимный доступ
Блокировка файлов
Настройки мобильных устройств
Заблокированные хосты и пользователи
Сбор информации о состоянии системы в фоновом режиме
Дополнительные опции
Лог-файл отладки (Debugging Log File)
Web Server Options
Webmin Scheduled Functions
Sending Email
Шифрование SSL
Авторизация по сертификатам

Рис. 4. Главное меню административного интерфейса

**Заключение**

МСЭ - традиционные средства защиты сети, они были построены на основе моделей, разработанных в то время, когда сети еще не получили широкого распространения и способы

атак на эти сети не были так развиты, как сейчас. Чтобы на должном уровне противодействовать этим атакам, необходимо применение новых концепций и технологий. Например, система обнаружения вторжений, которая стала активно развиваться за рубежом, уже активно разрабатывается и в России. Эта технология позволяет эффективно дополнять существующие МСЭ, обеспечивая более высокий уровень защищенности сети. Межсетевые экраны не обеспечивают достаточного уровня защищенности корпоративных сетей. Однако от них не следует отказываться. Они могут обеспечить необходимый (но недостаточный) уровень защиты ресурсов предприятия.

В качестве продолжения работы рассматривается доработка интерфейса взаимодействия с администратором до соответствия всем требованиям к интерфейсу для МСЭ 2 класса защищенности, а также адаптация интерфейса для работы с дополнительными программными пакетами ОС Эльбрус и повышение защищенности вебприложений, обеспечивающих взаимодействие с администратором, расширение возможностей интерфейса.

## Список литературы


1. Получение максимальной отдачи от межсетевого экрана нового поколения. Режим доступа: http://www.cisco.com/web/RU/campaigns/borderless/security/pdf/wp_next_gen_firewall_ru.pdf (дата обращения 03.03.2014).
2. Норберт Польман, Тим Кразерс. Архитектура брандмауэров для сетей предприятия М.: Вильямс, 2003. 432 с.
3. Лукацкий А.В. Firewall - не панацея. Режим доступа: http://citforum.ru/internet/securities/fw_pan.shtml (дата обращения 03.03.2014).
4. Лукацкий А.В. Способы обхода межсетевых экранов. Режим доступа: http://citforum.ru/security/internet/passthrough/ (дата обращения 03.03.2014).
5. Руководящий документ. Средства вычислительной техники. Межсетевые экраныЗащита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997г. Режим доступа: http://fstec.ru/component/attachments/download/295 (дата

обращения 03.03.2014).

6. Орлов С. Межсетевые экраны: новое поколение. Режим доступа: http://www.osp.ru/lan/2013/02/13034063/ (дата обращения 03.03.2014).