МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

ЗАЩИТА СЕТЕЙ С ПРИМЕНЕНИЕМ МЕЖСЕТЕВЫХ ЭКРАНОВ

Методические указания по выполнению практических работ по дисциплине «Проектирование защищенных телекоммуникационных систем» для студентов специальности 10.05.02

Курск 2017

УДК 004.056.55

Составители: А.Л. Марухленко

Рецензент
Кандидат технических наук, доцент А.Г. Спеваков

Защита сетей с применением межсетевых экранов: методические указания к выполнению практических работ / Юго-Зап. гос. ун-т; сост.: А. Л. Марухленко Курск, 2017. - 14с.

Указываются необходимые теоретические сведения, порядок выполнения практической работы, содержание отчета.

Методические указания по выполнению практических работ по дисциплине «Проектирование защищенных телекоммуникационных систем» соответствуют требованиям программы, утвержденной учебно-методическим объединением и предназначены для студентов направления подготовки 10.05.02.

Текст печатается в авторской редакции

Подписано в печать 01.11.2017. Формат 60x84 1/16.
Усл.печ. л. 0,8. Уч.-изд.л. 0,7. Тираж 30 экз. Заказ _____. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Овладеть навыками работы с сетевой программой ATGuard

2. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Межсетевой экран (firewall или брандмауэр) является программно-аппаратным средством осуществления сетевой политики безопасности в выделенном сегменте IP-сети.

В сфере компьютерных сетей межсетевой экран представляет собой барьер, защищающий от вторжения злоумышленников во внутреннюю локальную 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.

Название «брандмауэр», может относиться к одному устройству или одной программе. Термин «межсетевой экран» был принят для обозначения совокупности компонентов, которые находятся между вашей сетью и внешним миром и образуют защитный барьер.

Брандмауэр не может защитить от:

– вирусов. Хотя некоторые брандмауэры и способны распознавать вирусы в проходящем через них трафике, существует множество способов спрятать вирусы в программе. Если даже в описании вашего брандмауэра заявлена функция антивирусной проверки, не выключайте проверку вирусов на отдельных компьютерах в сети;

– «троянских коней». Как и в случае с вирусами, блокировать проникновение в сеть «троянских коней» (Trojan horses) достаточно сложно. Пользователь нередко поддается искушению загрузить программу из Internet или открыть прикрепленный к сообщению электронной почты файл, проложив тем самым путь в систему вредоносной программе;

– «социальной инженерии». Термин «social engineering» возник недавно и применяется для описания методов получения хакерами информации от доверчивых пользователей. Часто люди готовы сообщить свой пароль любому, кто позвонил по телефону и отрекомендовался представителем службы безопасности, что-нибудь «проверяющим». Межсетевой экран не в состоянии остановить невоздержного на язык сотрудника

– некомпетентности. Плохо подготовленные сотрудники или небрежное руководство приводят к ошибкам в настройках локальной сети и межсетевого экрана. Если сотрудники не понимают, как работает брандмауэр и как правильно его настраивать, не исключено, что это будет способствовать возникновению проблем;

– атаки изнутри. Межсетевой экран не может предотвратить злонамеренные действия внутри вашей сети. Это одна из причин, по которой безопасность компьютеров в сети остается важной проблемой и после установки брандмауэра.

3. ПОРЯДОК ВЫПОЛНЕНИЕ ПРАКТИЧЕСКОЙ РАБОТЫ

1) Установка и описание программы AtGuard

После инсталляции программы и перезагрузки компьютера Вы обнаружите в системном трее (system tray) иконку запущенного AtGuard’a , а вверху экрана его же панель (dashboard). Это означает, что инсталляция и первый запуск прошли успешно. Двойной щелчок на иконке открывает окно настроек.

Установка флажка Enable web filters включает блокирование, опции секретности и активные установки фильтров, определенные в диалоговом окне Web (HTTP) Filters. Уберите этот флажок, если Вы хотите выключить все web-фильтры.

Enable web filters действует как главный переключатель, который позволяет вам отменять индивидуальные установки фильтра в диалоговом

окне Web (HTTP) Filters и отключать всю фильтрацию веб-трафика. Когда Вы отключаете web-фильтры, программное обеспечение прекратит фильтровать любые HTTP данные, входящие или исходящие от рабочей станции. Если Вы устанавливаете или снимаете флажок Enable web filters, то эти изменения начинают действовать сразу.

Опции в этом диалоговом окне позволяют Вам включать или выключать индивидуальные web-фильтры, cookie и Java/ActiveX мониторы. Вы можете также модифицировать список портов, которые AtGuard контролирует для HTTP связи, когда web-фильтры включены. Установите флажки Ad Blocking, Privacy, Active Content и Cookie Assistant в этом диалоговом окне - этого будет достаточно. Флажок Java/ActiveX Assistant можете не устанавливать, иначе AtGuard будет каждый раз задавать ненужные вопросы.

HTTP Port List - сетевые сервисы (типа HTTP или FTP) используют специфические порты на вашем компьютере. Например, HTTP-связь обычно проводится через порт 80. Web-фильтры AtGuard’a контролируют весь HTTP-трафик, посланный и полученный через порты, которые указаны в Port List, применяя блокирование, секретность и другие опции, которые Вы определили. Ваша рабочая станция может соединяться с Интернетом посредством proxy-сервера, при этом весь HTTP-трафик проходит через порт, используемый этим proxy-сервером. Или Вы можете использовать приложение, которое инициирует HTTP-связь через нестандартный порт. Если HTTP-трафик идет через нестандартный порт, вы должны добавить номер этого порта в Port List. Изменения в настройках фильтров вступают в действие сразу после нажатия кнопки "Применить".

Add Site - нажмите эту кнопку, чтобы открыть диалоговое окно New Site/Domain, которое используется для добавления нового сайта или домена к иерархическому списку сайтов в левом окне. Напечатайте имя web-сайта или имя домена и нажмите OK. После добавления сайта Вы можете выбрать его в списке. Используйте установки Ad Blocking, Privacy, Active Content, чтобы

определить правила и набор блокировок, которые AtGuard использует только когда Вы посещаете конкретный web-сайт.

Ad Blocking - эти установки позволяют поддерживать блокирующий список по умолчанию и специфические для конкретных сайтов блокирующие списки, которые используются, чтобы указать, чего не нужно отображать на веб-страницах. Когда блокирующий фильтр включен, все HTML-страницы просматриваются на предмет наличия HTML-строк, специфичных для конкретного сайта, указанного в списке для блокирования, плюс значения по умолчанию, определенные для всех сайтов. Любой HTML-код, который содержит разрешенную к блокированию строку, будет удален из web-страницы AtGuard'ом прежде, чем эта страница будет интерпретирована и показана браузером.

Privacy - установки секретности позволяют определять правила, управляющие тем, как Ваш браузер обрабатывает запросы о различных типах информации, сделанных сайтами, которые Вы посещаете.

Cookies - это информация, которую web-серверы сохраняют на вашем компьютере для более позднего использования. Web-серверы могут читать cookies, чтобы следить, сколько раз вы их посетили, когда и какую информацию вы просматривали. Они могут даже использовать cookies, чтобы передать эту информацию другим web-серверам, типа серверов рекламы. Положительная сторона cookies в том, что они могут использоваться, чтобы сохранить вашу собственную конфигурацию web-сайта, запоминать, что вы поместили в вашу "покупательскую корзину" в интерактивном магазине или сохранять имя пользователя и пароль для сайтов подписки. Чтобы обеспечить максимальную секретность, разрешите использование cookies только проверенным сайтам, которым вы доверяете.

Referer - позволяет вам определить, узнают ли третьи сайты о том, из какого места поступил запрос данных с этих серверов.

Refer field - эти поля используются, чтобы обеспечить "третьи" сайты информацией относительно сайта, с которого поступил запрос данных из их

сервера. Refer поля позволяют веб-серверам знать, где вы только что были. Вполне возможно, что вы не захотите, чтобы эта информация становилась известной. Иногда это опасно. Например, некоторые онлайновые почтовые службы подставляют пароль просто в сетевой путь, который отображается в браузере. Если вам пришло письмо, содержащее ссылку на какой-нибудь сайт, и вы последовали по ссылке прямо из web-mail, то в статистике сайта на, который вы пришли, будет зафиксирован адрес страницы, содержавшей ссылку на него - refferer. А этот самый refferer может содержать ваш логин и пароль к вашему почтовому ящику. Некоторые сайты не позволяют заходить на них с включенным Block refer fields.

Browser (User-agent) - позволяет определить, обеспечиваются ли сайты информацией, какой браузер вы используете.

E-mail (From) - позволяет определить, получат ли сайты адрес электронной почты, который использует ваш браузер, чтобы идентифицировать вас как отправителя почты.

Active Content - эти установки позволяют Вам предотвращать выполнение следующих типов программ: JavaScript, Java applets, ActiveX controls. Кроме того, можно установить, чтобы анимационные изображения проигрывались только один раз. Когда блокирование активного содержимого включено, все HTML страницы просматриваются, и любой HTML-код, который активизирует нежелательное содержание, будет удален из страницы AtGuard'ом прежде, чем страница интерпретируется и отобразится веб-браузером.

Установки файрвола определяют, должен ли AtGuard запретить или разрешить приложениям на вашем компьютере посылать или получать информацию по TCP/IP. Для этого имеется список правил, которые описывают, какие типы сетевой активности разрешаются, и через какие сервисы приложения могут связываться. Вы можете добавлять, изменять, или удалять правила.

Включите опции Enable firewall, Enable RuleAssistant (interactive learning mode)

Для временного отключения какого-либо правила уберите флажок напротив соответствующей строки в списке правил.

Если правило "Блокировать" (Block) или "Разрешить" (Permit) указано, все оставшиеся правила игнорируются. Другими словами если вы, например, закрыли порт номер N, а ниже прописано правило, разрешающее использование этого порта, то оно будет проигнорирована и соединение по этому порту будет закрыто.

Если правило "Игнорировать" (Ignore) указано, тип связи, которая была предпринята, регистрируется в лог-файле firewall'a и затем обработка продолжается, пока не произойдет какого-либо другого соответствия. Если не найдется никакого правила, связь или блокируется (по умолчанию) или вызывается RuleAssistant. Чтобы перемещать правило по списку, выделите соответствующую строку и затем используйте кнопки "стрелка вверх" или "стрелка вниз" для помещения правила в соответствующую позицию.

Любое TCP/IP соединение, для которого нет firewall правила, блокируется по умолчанию. Если Вы хотите выборочно блокировать или разрешать соединение, для которого нет правила, установите флажок Enable RuleAssistant (интерактивный режим изучения).

Если флажок RuleAssistant включен, вам будет автоматически задан вопрос запретить (Block) или разрешить (Permit) соединение всякий раз, когда приложение на вашей рабочей станции или какое-то приложение извне делает попытку установить связь, для которой не описано никаких правил в firewall. В результате вашего решения AtGuard разрешает или блокирует сетевую связь и может создавать правило firewall, которое применяется в дальнейшем для данного типа сетевого соединения.

Direction. Inbound связь включает пакеты, посланные вашему компьютеру. Outbound связь включает пакеты, посланные вашим компьютером. Either - связь в любом направлении.

Protocol. Определяет, к какому протоколу связи применяется правило: TCP, UDP, или TCP и UDP, ICMP...

TCP - стандартный протокол Интернета транспортного уровня, обеспечивает надежную полнодуплексную связь. Программное обеспечение, реализующее протокол TCP, обычно постоянно находится в операционной системе и использует IP протокол, чтобы передать информацию. Примеры TCP приложений и сервисов - FTP, web-браузер, email и IRC.

UDP - транспортый уровень в TCP/IP сетях. UDP - низкоуровневый протокол, который использует IP, чтобы доставить пакеты. Примеры сервисов и приложений, которые используют UDP - DNS, NetBIOS.

ICMP - протокол межсетевых управляющих сообщений.

Application. Эта опция позволяет определять, применяется ли правило к конкретному приложению или к любому приложению, которое делает попытку сетевой связи, определенной правилом.

Service. Позволяет определять, применяется ли правило к локальным или удаленным сервисам и применяется ли это к одиночному определенному сервису или к любому сервису, который делает попытку сетевой связи, определенной правилом.

Time Active. Используйте эти установки, чтобы определить время когда, правило будет действовать.

Logging. Определяет, что событие регистрируется в лог-файле, когда устанавливается описанное правилом соединение.

Show taskbar icon - при запущенном AtGuard показывать его иконку в панели задач.

Show dashboard window - при запущенном AtGuard показывать dashboard.

Enable password protection - если выбрано, то как только вы попытаетесь открыть диалоговое окно AtGuard Settings, окно Dashboard Properties, Event Log, или окно статистики, вы будете должны ввести пароль.

StartUp Options / Run at network startup. Когда эта опция выбрана, AtGuard запускается автоматически, если вы открываете сетевое соединение, и останавливается также автоматически, когда вы закрываете ваше сетевое соединение.

Сразу после инсталляции, зайдите в настройки Firewall. Снимите флажки Default Inbound ICMP, Default Inbound DNS, Default Inbound Bootp, Default Inbound NetBIOS

Для дальнейшей настройки Inbound DNS необходимо узнать DNS адрес вашего провайдера. Затем Settings -> Firewall -> Add. В поле "Name" впишите DNS, поля "Action" и "Directon" изменять не нужно. Поле "Protocol" установите "TCP or UDP 3". Здесь же нажмите закладку "Service" и установите "Remote service" в "Single service", в появившееся поле впишите 53 (номер порта домена). Теперь выберите закладку "Address" и поставьте "Remote address" = "Host address" и в появившееся поле впишите адрес DNS вашего провайдера, нажмите OK. Теперь повторите эту же операцию только измените "Directon" на "Inbound". Повторите то же самое и для остальных адресов DNS, если они есть. Все, настройка DNS закончена.

Как можно защититься от рекламных баннеров. Правой кнопкой мыши нажимаем по баннеру. В всплывающем меню выбираем "Копировать ярлык". Вызываем AtGuard Settings -> Web. Выбираем в списке (Defaults), Ad Blocking -> Add. В появившемся окошке нажимаем правой кнопкой мыши, выбираем «вставить». Например, для linkexchange будет такая строка http://www.linkexchange.ru/users/091164/goto.map Ее нужно отредактировать, чтобы получилось linkexchange.ru/users/ ибо удаленная часть может изменяться от сайта к сайту. Всё. Еще пример. http://www.reklama.ru/cgi-bin/href/myclub?3353573 После правки: reklama.ru/cgi-bin/ .

Есть еще один более простой способ. Если у вас запущен Dashboard, то в правом углу будет Trashcan ("Мусорная корзина") AtGuard'a. Чтобы переместить рекламу в мусорку при использовании MSIE 4.0, выберите рисунок и мышкой перетащите его в Trashcan. При использовании Netscape

или MSIE 3.0, щелкните правой кнопкой мыши на баннере. Чтобы заблокировать все подобные ссылки, выберите пункт Copy link location (если картинка грузится с того же сервера, что и страница). Если баннер грузится с сервера рекламодателя (например, это могут быть баннеры сетей reklama.ru, linkexchange), то выберите пункт Copy image location. Затем щелкните правой кнопкой мыши на иконке Trashcan и выберите пункт Paste (Вставка) из всплывающем меню.

Как говорилось выше, нашу задачу сильно облегчает то, что вся реклама объединяется или уже объединена в рекламные (баннерные) сети. Поэтому закрыв для себя AtGuard'ом один рекламный сайт, вы избавитесь от сотен и сотен рекламных баннеров. Это сохранит вам деньги, нервы и высокую скорость соединения.

Обязательно установите все флажки в окне AtGuard Settings -> Web -> Active Content.

В окне AtGuard Settings -> Firewall включите Enable Rule-Assistant для интерактивного обучения вашего стража. Если в процессе вам встретится непонятное на первый взгляд сообщение о каком-либо соединении, запретите его, потом всегда можно посмотреть в лог-файлах.

2) Защита от атак WinNuke

Чтобы защититься от атаки WinNuke, нужно поставить соответствующий фильтр. Атака WinNuke заключается в посылке OOB-данных на 139 порт. Таким образом, достаточно будет заблокировать TCP-соединения с 139 портом. Однако 139 порт используется для NetBIOS и потому при работе в локальной сети его перекрывать не следует. Но если вы заходите в Сеть с домашнего компьютера, то блокируйте смело.

В настройке Firewall добавляем новое правило – “Add”. Назовем “WinNuke”, действие – “Block”, направление только входящие – “Inbound”, протокол “TCP”. Далее на закладках: Any Application. Service: remote - "Any", local – single service 139 порт. Остальные настройки можно оставить по

умолчанию. Включите протоколирование, чтобы можно было видеть, что вы подверглись атаке. По аналогии можно настроить и другие фильтры.

3) Задание на практическую работу

– Изучить функции программы, пользуясь описанием программы.

– Установить 2 виртуальные машины. Настроить локальную сеть между двумя виртуальными машинами, если требуется.

– Установить обе виртуальные машины AtGuard.

– Осуществить обмен пакетами запрещенного типа при включенном и при выключенном AtGuard с другим компьютером сети.

– Создать правило запрещающее получение доступа к компьютеру с удаленного компьютера (с конкретного IP-адреса или с определенного имени компьютера), попытаться обратиться с запрещенного компьютера и отследить реакцию AtGuard.

– Составить отчет о проделанной работе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Шувалов В.П., Величко В.В., Субботин Е.А., Ярославцев А.Ф. Телекоммуникационные системы и сети. Том 3. Мультисервисные сети (2005)

2) Петраков А.В. Основы практической защиты информации. 2-е изд. Учебн. пособие. – М.: Радио и связь. 2000. – 368 с.

3) Цифровые и аналоговые системы передачи: Учебник для вузов/ В.И.Иванов, В.Н.Гордиенко, Г.Н.Попов и др.; Под ред. В.И.Иванова. – 2-е изд. – М.: Горячая линия – Телеком, 2003. – 232 с.

4) Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для ВУЗов. - СПб.: БХВ-Петербург, 2010. - 400 с.

5) Башарин Г.П. Лекции по математической теории телетрафика: Учеб. пособие. Изд. 3-е, испр. и доп. - М.: РУДН, 2009. - 342 с.

6) Буч Г. Объектно-ориентированный анализ и проектирование. – М.: Вильямс, 2008.

7) Леоненков А.В. Самоучитель языка UML. – СПб.: БХВ-Петербург, 2004.

8) Розенберг Д., Скотт К. Применение объектного моделирования с использованием UML и анализ прецедентов. – М.: ДМК Пресс, 2002.

9) А.В. Росляков. Виртуальные частные сети. Основы построения и применения. - М.: Эко-Трендз, 2006. - 242 с.