НОВЫЙ ПОДХОД К ЗАЩИТЕ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ.

Антонов Н. А., Авдеев А. С., Борисов И. С., Борисов С.П., Гонтарь К. Т., Залеский С. Б.
МИРЭА – Российский технологический университет (РТУ МИРЭА)
+7 (916) 341-11-34, bsp345@gmail.com

Статья посвящена новому подходу к защите локальных компьютерных сетей, с использованием разнесения защиты на несколько эшелонов. Предложенный способ позволяет сократить время прохождения трафика через устройства, реализующие защиту по периметру сети.

Ключевые слова: эшелонированная защита, список доступа (access list).

Antonov N. A., Avdeev A. S., Borisov I. S., Borisov S.P., Gontar K. T., Zalessky S. B., MIREA – Russian Technological University (RTU MIREA)

The article is devoted to a new approach to the protection of local computer networks, using the separation of protection into several echelons. The proposed method makes it possible to reduce the time of traffic passing through devices that implement protection along the perimeter of the network.

Keywords: layered protection, defense in depth, access list.

Введение

Угроза безопасности данных – это действие, произведенное над системой, в результате которого она может поменять свои функциональные характеристики. Такого рода действия возникают в связи с нарушениями защищенности данных, которые хранятся в системе или в ней обрабатываются. Если во время функционирования компьютерной системы возникает такая ситуация, при которой хранимая в системе информация оказывается под угрозой, то есть появляется возможность несанкционированного доступа к ней, то говорят, что возникла уязвимость информации.

Постановка проблемы

Чтобы воспользоваться этой информацией, соответственно, требуется в систему проникнуть. Для этого злоумышленник устраивает атаку на нужную ему компьютерную систему. Чтобы атака была успешна, атакующему требуется заранее получить информацию об уязвимостях, проанализировать их и использовать в своих недобрых целях. То есть атака на компьютерную систему являет собой итоговую реализацию имеющихся брешей в системе защиты компьютерной системы.

Чтобы успешно противодействовать большинству угроз и атак на сеть можно использовать эшелонированную систему защиты. Название Defense in depth можно перевести с английского языка как защита в глубину. По сути, такой перевод и характеризует этот тип защиты.

В сети должны присутствовать, безотказно работать и корректно быть настроены такие элементы как антивирусы, фаерволы, программы, отслеживающие и анализирующие трафик и другие. Вместе с тем нельзя забывать о своевременных обновлениях приложений, ведь они могут закрывать имеющиеся дырки в обороне. Также стоит помнить о том, что защитить сеть внутри будет легче, если ограничить количество участников в ней до минимально необходимого. То есть в ней не должно оставаться больше мест, чем устройств, которые к ней должны быть обязательно подключены. Есть еще методики, направленные на борьбу с атаками извне. К таким методикам можно отнести ведение журналов со списками черных, белых и серых MAC и IP адресов, использование статических ARP таблиц, корректное использование межсетевых экранов.

Для защиты системы чаще всего применяют два подхода к настройке сетевых устройств, обеспечивающих безопасность периметра сегмента сети:

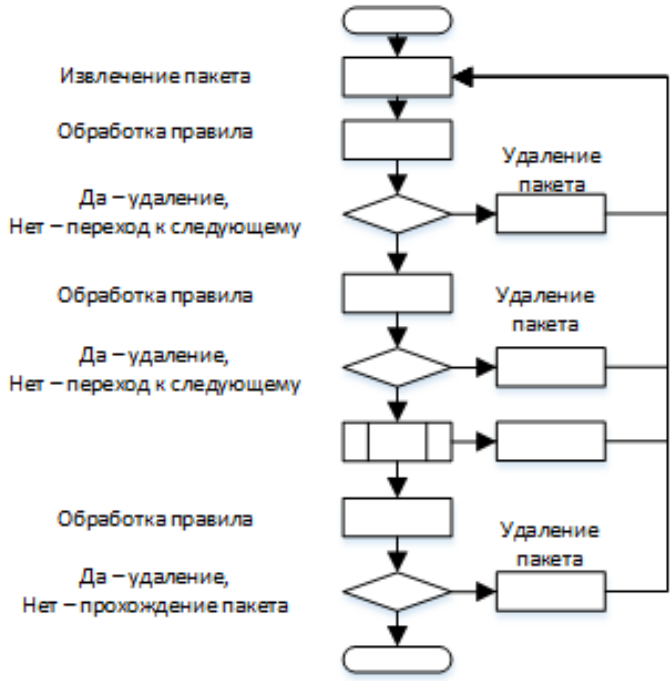
1.«Все разрешено, кроме..», т.е. когда надо описывать все запрещающие правила.

2.«Все запрещено, кроме..», т.е. когда надо описывать только разрешающие правила.

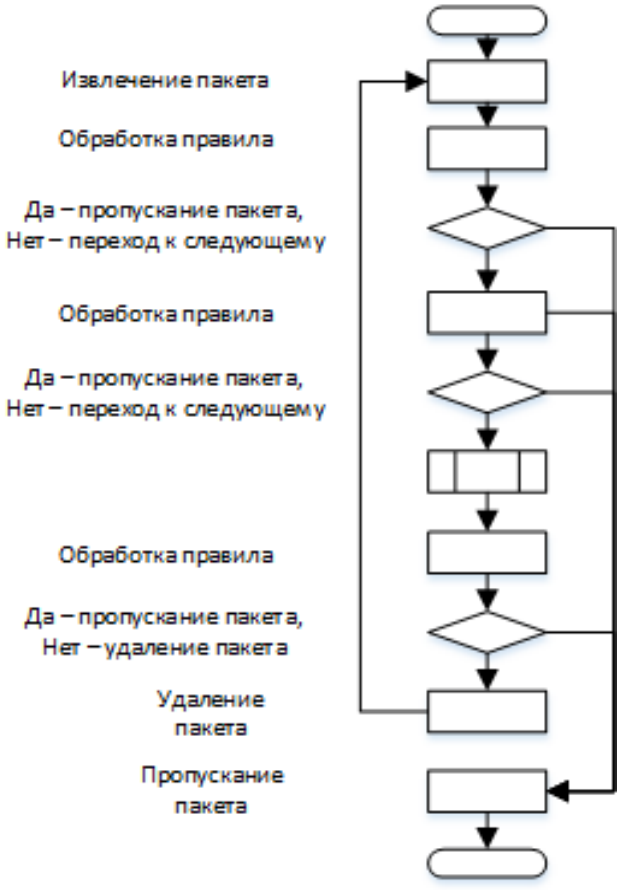
Первый подход очень трудоемок и очень зависим от квалификации сетевого администратора. Второй подход безопасен, и обеспечивает прозрачность, когда через «фильтрующее» звено проходит только разрешенный трафик.

Второй подход наиболее надежен, но устройство, на котором сосредоточены все запрещающие правила, будет вызывать наибольшие задержки.

С программной точки зрения это будет «цикл в цикле» с принудительным выходом из вложенного цикла. С точки зрения быстродействия при реализации первого подхода самой оптимистичной будет ситуация, когда каждый пакет будет отбрасываться на первом правиле.



а) Программная реализация первого подхода



б) Программная реализация второго подхода

Рисунок 1. Программная реализация работы алгоритмов защиты

И, самой пессимистичной, когда правило будет последним. Т.е. в очереди N пакетов, и существует M правил, и время обработки правилом одного пакет составляет t, то в лучшем случае это будет: время на удаление пакетов из очереди.

$T_{min} = N*t;$
$T_{max} = M*N*t;$
или
$T_{пакета} = m*N*t$, где m – номер правила.

Принцип – «первое встреченное правило удаляет пакет». На рис.1 а) показан алгоритм программной реализации, это будет «цикл в цикле» с принудительным выходом из вложенного цикла. Очевидно, что не все пакеты будут проходит через правила максимальное, время, потому что m всегда меньше M, кроме случая прохождения всех правил. Это и есть задержка на сетевом устройстве.

При реализации второго метода, который называется список доступа (access lists) очевидно, что каждый пакет будет «искать» правило, которое ему позволит пройти через фильтр. И для того, чтобы гарантировано быть удаленным, он должен пройти через все «разрешающие» правила (см. рис.1, б)).

С точки зрения быстродействия самой оптимистичной будет ситуация, когда каждый пакет будет пропускаться на первом правиле. И самой пессимистичной, когда пакет на найдет правил для прохождения через это устройство. Т.е. в очереди N пакетов, и существует M правил, и время обработки правилом одного пакет составляет t, то в лучшем случае это будет: время на удаление пакетов из очереди.

$T_{min} = N*t$ – пакет пропускается;
$T_{max} = M*N*t$ – пакет удаляется;
или
$T_{пакета} = m*N*t$, где m – номер правила.

Принцип – «пакет удаляется, если нет правил для его пропускания». И самая большая задержка на устройстве будет в ситуации, когда трафик содержит большое количество «запрещенных» пакетов.

Из приведенных выше рассуждений можно сделать вывод, что, если используется второй подход, который наиболее надежен, устройство на котором сосредоточены все запрещающие правила, будет вызывать наибольшие задержки.

Поэтому была выдвинута гипотеза, что для снижения времени задержки необходимо разнести эти правила на два устройства или эшелона. Для проверки гипотезы была написана программа на языке C++, которая моделирует эти ситуации. Было реализовано разделение по принципу: первое устройство содержит 20% от общего количества правил, и задерживает 80% запрещенных пакетов, второе устройство содержит остальные 80% правил и обрабатывает оставшиеся 20% трафика.

Основные результаты экспериментов показаны в табл.1.

Таблица 1. Результаты экспериментов

	Количество запрещенных пакетов	Количество разрешенных пакетов	Сложность правил	Политика	Время работы 1 устройства	Количество пропущенных пакетов	Время работы 2 устройства	Количество пропущенных пакетов	Время работы 3 устройства	Количество пропущенных пакетов
1	10000	0	0	1	0,005	1969	0,002	0	0,008	0
2	10000	0	0	1	0,006	2032	0,001	0	0,008	0
3	10000	0	0	2	0,061	1990	0,011	0	0,329	0
4	10000	0	0	2	0,059	1984	0,012	0	0,326	0
5	100000	0	0	1	0,059	19908	0,028	0	0,078	0
6	100000	0	0	1	0,066	20145	0,021	0	0,078	0
7	100000	0	0	2	0,555	20061	0,116	0	3,333	0
8	100000	0	0	2	0,546	19871	0,126	0	3,305	0

Эксперименты показали, второй метод настройки устройств требует эшелонирования, так как устройства с полным набором правил вызывают большую задержку, чем два устройства с разным набором правил.

Так же по результатам экспериментов с уверенностью можно сделать вывод, что большее количество простых правил может выполнятся быстрее чем, на порядок меньшее количество сложных правил.

Результаты математических экспериментов были также подтверждены и результатами экспериментов в «Cisco Packet Tracer» – программном пакете для моделирования и создания сетей передачи данных.

Было реализовано 5 эшелонов с различным набором списков доступа (access lists) по тому же принципу: на каждом последующем устройстве обрабатывается меньшее количество трафика, приблизительное соотношение: 70%,15%,10%, 3%, 2%.

Реализованная в эксперименте топология сети и настройки сетевого оборудования показаны на рис.2.

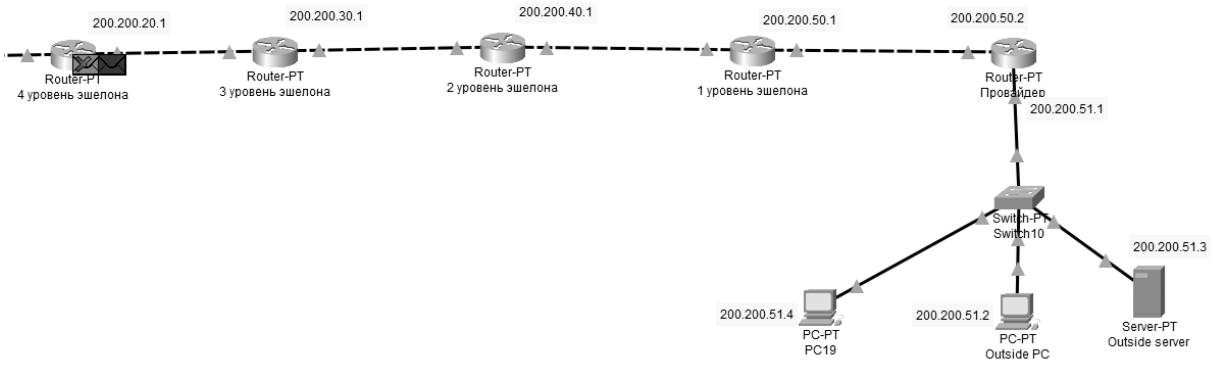


Рисунок 2. Топология, реализованная в Cisco Packet Tracer

Чтобы продемонстрировать то, что защита действительно работает, будет отправлен пакет ICMP с не доверительного компьютера из внешней сети на компьютер, находящийся внутри сети. Исходя из составленной обороны, пакеты должны быть заблокированы на последних эшелонах защиты.

Таблица 2. – Результаты измерений скорости работы

	5 эшелонов, правильная настройка	5 эшелонов, неправильная настройка	1 эшелон	Без защиты
Минимум (мс)	0	0	0	0
Максимум (мс)	6	12	12	1
Среднее (мс)	1	3	5	0

Заключение.

Результаты научной работы показывали, что использование эшелонированной защиты значительно увеличивают производительность защиты периметра сети с большим размером списков доступа (access list). Полученные результаты по новому подходу к эшелонированной защите распределенной корпоративной сети, при правильной топологии сети, правильно выбранном оборудовании доказана работоспособность и эффективность такой защиты. Доказано, что надежно защищенная распределенная корпоративная сеть с 5 эшелонами, которая работает быстрее, чем сеть с 1 эшелоном при той же защите, что говорит об эффективности нового подхода к эшелонированной защите периметра корпоративной локальной сети.

Литература

1. Борисов С.П. Компьютерные сети. Анализ и диагностика. Часть 1. [Электронный ресурс]: учебное пособие / Борисов С.П. — М.: МИРЭА – Российский технологический университет, 2021. — 1 электрон. опт. диск (CD-ROM).
2. Борисов С.П. Компьютерные сети. Анализ и диагностика. Часть 2. [Электронный ресурс]: учебное пособие / Борисов С.П. — М.: МИРЭА – Российский технологический университет, 2021. — 1 электрон. опт. диск (CD-ROM).
3. Кузьменко Н.Г. Компьютерные сети и сетевые технологии. Сетевые протоколы, сетевое оборудование, сетевая инфраструктура, сетевые сервисы. —СПб.: Наука и Техника, 2013. —368 с.
4. Стивенс У.Р. Протоколы TCP/IP. Практическое руководство. —Спб.: Невский Диалект –БХВ-Петербург, 2003. —672 с..
5. Э.Таненбаум, Д.Уэзеролл. Компьютерные сети. —СПб.: Питер, 2012. —960 с.
6. Брейман А.Д., Баканов В.М. Сети ЭВМ и телекоммуникации: учебное пособие (конспект лекций). Часть 1. Общие принципы построения сетей. Локальные сети. – М.: МГУПИ, 2012. – 79 с.
7. Дж.Скотт Хогдал. Анализ и диагностика компьютерных сетей. —М.: Лори, 2015. —352 с.