УДК 621.391

АДАПТИВНОЕ УПРАВЛЕНИЕ МЕЖСЕТЕВЫМ ЭКРАНОМ

М.Н. БОБОВ, Ф.О. МОХАММЕД

ОАО «АГАТ – системы управления»
пр. Независимости, 117, Минск, 220023, Беларусь

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 23 марта 2012

Исследованы процессы проверки трафика в межсетевых экранах (МСЭ), образующих демилитаризованную зону и установлено, что время выполнения функций проверки пакетов зависит как от длины проверяемых пакетов, так и от размеров соответствующих таблиц. Определены наиболее предпочтительные варианты перераспределения функций проверки трафика между МСЭ на границе демилитаризованной зоны за счет организации области адаптации и выбора необходимых точек переключения функций

Ключевые слова: межсетевой экран, информационная телекоммуникационная сеть (ИТС), демилитаризованная зона (ДМЗ), вероятность блокировки.

Введение

Структура современных защищенных ИТС состоит из трех зон безопасности, одна из которых отделяется от остальных двух внешним и внутренним МСЭ и называется демилитаризованной зоной. Анализ различных классов МСЭ показал, что они способны обеспечивать необходимый уровень защищенности ИТС, однако являются транспортно узким местом, что может приводить к блокированию проходящего трафика. Для снижения вероятности блокировки МСЭ из-за перегрузки в работе предлагается адаптировать его управление с учетом структуры защищаемой ИТС. В условиях наличия ДМЗ представляется целесообразным переключать имеющиеся МСЭ на проверку установленных правил в зависимости от сетевой нагрузки. В случае, когда в ИТС трафик не критичный, сетевые экраны осуществляют проверки в соответствии со своим назначением как внешних, так и внутренних барьеров. Когда трафик достигает критического объема, часть функций проверки внешнего МСЭ передается внутреннему МСЭ, снижая тем самим вероятность блокировки из-за перегрузки. Когда угроза атаки ликвидируется и трафик возвращается к нормальному состоянию, МСЭ возвращаются в штатный режим проверки.

Теоретическая часть

Модель МСЭ с традиционным контуром управления представляет собой одноканальную систему массового обслуживания (СМО) с отказами, вероятность отказа (блокировки) которой определяется по формуле:

$$p_{\text{отк}} = \frac{\lambda}{\lambda + \mu}.$$

Параметр μ является неизвестным и зависит от свойств МСЭ. Анализ алгоритма функционирования МСЭ показал, что он анализирует график путем последовательного выполнения функций, включающих в себя контроль целостности, трансляцию адреса, ведение таблицы со-

единений, управление доступом, инспектирование соединения и проверку контента. Поэтому процесс обслуживания МСЭ каждого пакета можно изобразить в виде схемы, приведенной на рис. 1.

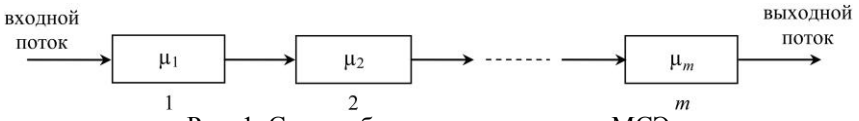

Рис. 1. Схема обслуживания пакетов МСЭ

Функция распределения длительности обслуживания на m последовательно соединенных однолинейных этапах называется распределением Эрланга m-го порядка и для $\mu_1 = \mu_2 = \ldots = \mu$ имеет вид:

$$F(t) = 1 - e^{m\mu t} \sum_{j=0}^{m-1} \frac{(m\mu t)^j}{j!} \qquad (1)$$

Указанная функция распределения представляет собой сумму m независимых случайных величин, каждая из которых распределена по экспоненциальному закону с параметром $m\mu$. Причем длительность обслуживания на каждом этапе имеет экспоненциальное распределение с параметром μ. В нашем случае время обслуживания, а следовательно, и параметр μ на каждом этапе обработки пакета, имеет различные значения, поэтому формулу (1) непосредственно использовать нельзя. Определим посредством $F_j(t)$ и $F_k(t)$ функции распределения времени обслуживания с параметрами μ_j и μ_k, представляющих сумму времен обслуживания пакетов МСЭ на первых j и последних k этапах соответственно.

В этом случае

$$\mu_j = \frac{1}{\sum_{i=1}^{j} t_i},\ j = \overline{m-1,1};\ \mu_k = \frac{1}{\sum_{j=m-(k-1)}^{m} t_i},\ k = \overline{1,m-1},$$

где m – общее количество функций.

Тогда вероятность блокировки пакета с учетом числа включенных в обработку этапов, начиная с первого и последнего, соответственно равны

$$P_{\text{бл}}^{j} = \frac{\lambda}{\mu_j + \lambda};\ P_{\text{бл}}^{k} = \frac{\lambda}{\mu_k + \lambda}.$$

В традиционном контуре управления МСЭ присутствует администратор безопасности, который осуществляет настройку правил проверки пакетов. Если его функции по управлению МСЭ в случае обнаружения аномалий реализовать программными средствами, то устранение возникшей угрозы можно осуществлять автоматически, путем изменения базы правил. С учетом архитектуры защищенной ИТС, в структуре которой присутствует ДМЗ, модель МСЭ с адаптивным контуром управления можно изобразить, как показано на рис. 2.

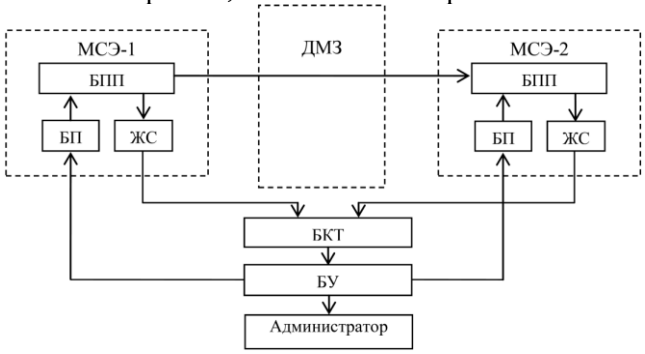

Рис. 2. МСЭ с адаптивным контуром управления, где БКТ – блок контроля трафика

Блокировка в МСЭ с адаптивным контуром управления может наступить в следующих случаях:

- МСЭ-1 заблокирован, МСЭ-2 свободен;
- МСЭ-1 свободен, МСЭ-2 заблокирован.

Тогда вероятность блокировки адаптивного контура МСЭ будет равна

$$P_{бл} = \frac{\lambda\left(\mu_j + \mu_k\right)}{\lambda^2 + \lambda\left(\mu_j + \mu_k\right) + \mu_j\mu_k}.$$

Так как величины μ_j и μ_k являются неизвестными, для их исследования используется полунатурная модель ИТС (см. рис. 3).

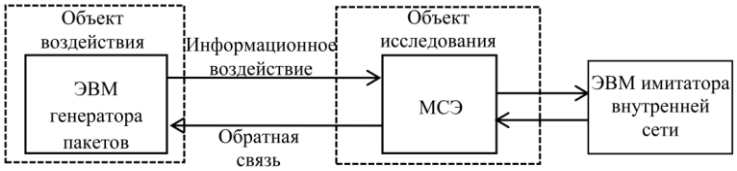

Рис. 3. Схема полунатурной модели ИТС

Полунатурная модель обеспечивает решение следующих задач:

1) определение продолжительности обработки пакетов каждого типа сетевой атаки, поступающей от объекта воздействия в защищаемую сеть;

2) определение продолжительности выполнения каждого вида проверки входящего пакета испытуемым МСЭ.

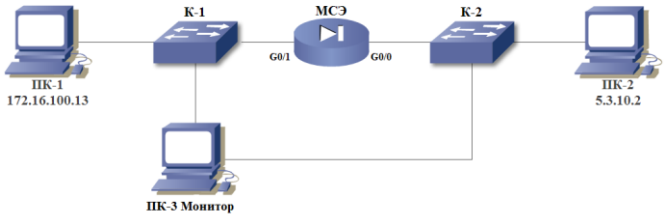

Рис. 4. Рабочая схема полунатурной модели ИТС

Схема полунатурной модели ИТС включает в себя персональный компьютер ПК-1, играющий роль получателя; коммутатор внутренней сети К-1, который соединяет ПК-1 с МСЭ через внутренний интерфейс (G0/1); персональный компьютер ПК-3, играющий роль монитора; межсетевой экран Cisco ASA 5520; коммутатор внешний сети К-2, который соединяет ПК-2 с МСЭ через внешний интерфейс (G0/0) и персональный компьютер ПК-2, играющий роль источника трафика. В ПК-2 установлен программный генератор пакетов Colasoft Packet Builder (CPB), в ПК-1 и ПК-3 установлена программа Wireshark, которая выполняет функцию сниффера, показывает и сохраняет все пакеты и их параметры. В коммутаторах К-1 и К-2 включена функция SPAN, которая обеспечивает копирование всех пакетов, проходящих через определенный интерфейс в указанный интерфейс.

Экспериментальные исследования характеристик МСЭ проводились по следующему сценарию:

1) для каждой из 6 исследуемых функций производилось конфигурирование генератора пакетов таким образом, чтобы в нем формировался трафик определенного протокола, содержащий как правильные, так и ложные пакеты для исследуемой функции контроля;

2) правила МСЭ и его интерфейсы настраивались таким образом, чтобы активизировалась только одна исследуемая функция проверки, а остальные функции были бы заглушены;

3) в течение каждых 30 с генерировались потоки правильных и ложных пакетов с последовательным изменением длин пакетов в диапазоне от 100 до 1500 байт и интенсивностью их поступления в диапазоне от 1000 до 4000 пакет/с;

4) осуществлялась регистрация моментов времени поступления пакетов в МСЭ и моментов их отправки из МСЭ;

5) осуществлялась обработка полученных результатов и расчет среднего времени выполнения выбранной функции контроля пакетов в МСЭ.

Для задания модели потока атак на МСЭ проведен анализ структуры пакетов исследуемых протоколов и содержания полей их заголовков. Установлено, что для задания потока атак для исследования функций контроля целостности, трансляции адреса и управления доступом, необходимо использовать пакеты протокола ICMP, а для исследования функций ведения таблицы соединений и инспектора состояний – пакеты протокола TCP.

Время выполнения функций трансляции адреса, ведения таблицы соединения и управления доступом зависит от числа входов соответствующих таблиц, а время выполнения функций контроля целостности, проверки контента и инспектора состояний зависит от длины проверяемого пакета, т.е.

$$t_j = F_j(k) \text{ и } t_j = F_j(L), \qquad (2)$$

где j – функция проверки, k – количество входов таблицы, L – длина пакета.
Так как вид функций (2) является неизвестным, они также определялись в процессе моделирования.

В результате проведенного моделирования получены значения времени и соответственно интенсивности обслуживания для каждой из функций МСЭ, которые представлены в табл. 1.

Таблица 1. **Время обработки и интенсивность обслуживания функций МСЭ**

№	Наименование функции	t_i (мкс)	μ_i
1	Контроль целостности	1,133	$883 \cdot 10^3$
2	Трансляция адресов	12,5	$80 \cdot 10^3$
3	Ведение таблицы соединения	1,256	$679 \cdot 10^3$
4	Управление доступом	6,00	$167 \cdot 10^3$
5	Инспектор состояния	1,338	$747 \cdot 10^3$
6	Проверка контента	5,42	$190{,}84 \cdot 10^3$

Анализ алгоритмов выполнения функций проверки показал, что между ними существует определенная зависимость. Так, функции ведения таблицы соединения и управления доступом взаимно влияют друг на друга, а функции инспектора состояния и ведения таблицы соединения связаны друг с другом. Таким образом, для осуществления адаптации перегруппирование этих функций нельзя осуществлять в произвольном порядке. Так как функция ведения таблицы соединения связана с функциями управления доступом и инспектора состояния, то при осуществлении адаптации они всегда должны быть вместе. Остальные функции не связаны друг с другом и могут работать автономно. С учетом вышеизложенного в табл. 2 приведены варианты возможного перегруппирования функций между двумя МСЭ.

Таблица 2. **Варианты возможного группирования функций между двумя МСЭ**

№ варианта	Функции МСЭ-1	Функции МСЭ-2
1	1, 2, 3, 4, 5	6
2	2, 3, 4, 5	1, 6
3	1, 3, 4, 5	2, 6
4	3, 4, 5	1, 2, 6
5	3, 4, 5, 6	1, 2
6	1, 2	3, 4, 5, 6

В табл. 3 и 4 предоставлены значения интенсивности обслуживания МСЭ в зависимости от включенных в обработку функций.

Таблица 3. **Интенсивности обслуживания МСЭ в зависимости от *j***

№ варианта	t_j (мкс)	μ_j
1	22,228	44988
2	21,094	47407
3	9,728	102796
4	8,594	116360
5	13,834	72286

Таблица 4. **Интенсивности обслуживания МСЭ в зависимости от *k***

№ варианта	t_k (мкс)	μ_k
1	5,42	19084
2	6,36	15689
3	17,74	5637
4	18,87	5298
5	13,63	7335

Полученные вероятности блокировки МСЭ в конфигурации с ДМЗ предоставлены на рис. 5.

Как следует из полученных графиков, самым худшим вариантом с точки зрения пропускной способности является вариант 1, а самым лучшим – вариант 5. На рис. 6 показаны графики вероятностей блокировки МСЭ с адаптивным управлением и зоной адаптации. Анализ результатов имитационного моделирования процессов защиты от сетевых атак с использованием МСЭ Cisco ASA 5520, образующих демилитаризованную зону, показывает следующее.

При входящей нагрузке λ, сравнимой с интенсивностью обслуживания потока пакетов μ_j и μ_k, вероятность блокировки практически не зависит от перераспределения функций между МСЭ-1 и МСЭ-2. В данном случае это интервал $0 < \lambda < 20 \cdot 10^3$ (зона 1 на рис. 6). Вариант с распределением функций j=5, k=1 является наиболее предпочтительным при нагрузке в переделах от $20 \cdot 10^3 \le \lambda \le 40 \cdot 10^3$ (зона 2 на рис. 6), когда вероятность блокировки обслуживания $P_{бл} \le 0{,}5$.

Приняв вероятность $P_{бл} \le 0{,}5$ в качестве нормы видно, что в интервале $40 \cdot 10^3 < \lambda < 75 \cdot 10^3$ необходимо адаптировать МСЭ, переключая функцию контроля целостности от МСЭ-1 на МСЭ-2. В нашем случае это второй вариант с распределением функций j = 4, k = 2 (зона 3 на рис. 6).

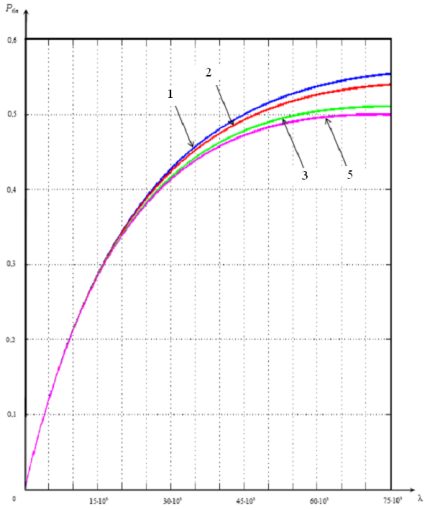

Рис. 5. График вероятностей блокировки сдвоенного МСЭ

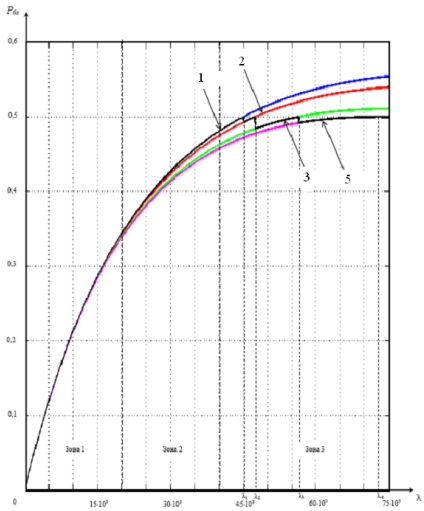

Рис. 6. Графики вероятностей блокировки сдвоенного МСЭ с адаптивным управлением

При продолжении нарастания числа заявок необходимо снова адаптировать МСЭ, переключая функцию трансляции адресов от МСЭ-1 на МСЭ-2, а функцию контроля целостности от МСЭ-2 на МСЭ-1. В нашем случае это третий вариант с распределением функций j = 4, k = 2.

Если число заявок в секунду достигает $\lambda = 60 \cdot 103$, то $P_{бл} \ge 0{,}5$, то МСЭ снова необходимо адаптировать, переключая функцию контроля целостности от МСЭ-1 на МСЭ-2, а функцию проверки контента от МСЭ-2 на МСЭ-1. В нашем случае это четвертый вариант с распределением функций j = 4, k = 2. Ввиду того, что процесс перенастройки МСЭ требует некоторых временных затрат, а значения λ_1 и λ_2 достаточно близкие величины, является целесообразным адаптацию МСЭ производить не в четыре, а в три этапа, как это показано на рис. 7, где область адаптации – диапазон значений нагрузки трафика, в котором осуществляется переключение функции от МСЭ-1 на МСЭ-2. Организация области адаптации поясняется следующими отношениями: $0 < \lambda < \lambda_1 \rightarrow$ вариант №1 (j=5, k=1); $\lambda_1 \le \lambda < \lambda_3 \rightarrow$ вариант №3 (j=4, k=2); $\lambda_3 \le \lambda < \lambda_4 \rightarrow$ вариант №5 (j=4, k=2); $\lambda \ge \lambda_4 \rightarrow$ звуковая сигнализация администратору (варианты конфигурации МСЭ-1 и МСЭ-2 приведены в табл. 2).

Как видно на рис. 7. предложенные правила переключения функций проверки в зоне адаптации, позволяют в 1,7 раза увеличить пропускную способность МСЭ и тем самым уменьшить вероятность блокировки МСЭ из-за перегрузки.

Практическая часть

На основании полученных результатов разработан алгоритм адаптивного управления МСЭ и соответствующее программное средство, работающее в программной среде Windows и инсталлируемое на рабочее место администратора, которое имеет связь с МСЭ.

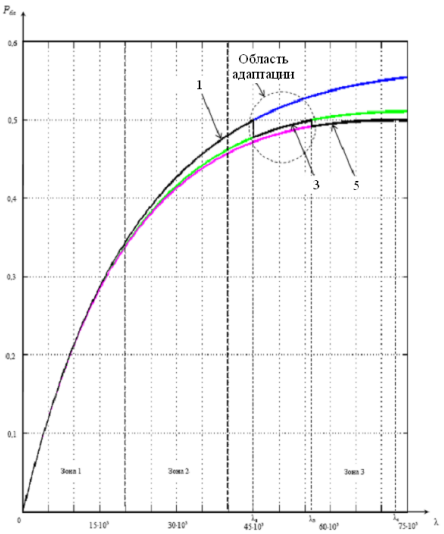

Рис. 7. Графики вероятностей блокировки сдвоенного МСЭ с адаптивным управлением

Адаптация МСЭ выполняется переключением определенных функций между МСЭ-1 и МСЭ-2 в зависимости от расчетной величины вероятности блокировки МСЭ, которая зависит от нагрузки поступающего трафика (число заявок в секунду).

Для использования полученных результатов применительно к любым типам МСЭ в условиях реализации демилитаризованной зоны разработана методика адаптации управления МСЭ, которая в общем виде состоит из следующих основных этапов: анализ функций МСЭ, определение временных значений выполнения функций, выбор вариантов распределения функций, определение границы зоны адаптации.

С целью подтверждения разработанных алгоритма и методики адаптивного управления МСЭ, а также проверки полученных при моделировании значений вероятности блокировки МСЭ в зависимости от нагрузки, были проведены натурные испытания.

Натурные испытания проводились в условиях обработки трех типов трафиков: поток пакетов без сетевых атак; поток пакетов с сетевой атакой на преодоление функции трансляции адресов; поток пакетов с сетевой атакой на преодоление функции ACL, относящейся к классу атак «отказ в обслуживании».

Результаты натурных испытаний приведены на графиках рис. 8, которые иллюстрируют расчетную и практическую вероятности блокировки МСЭ (отдельно выделена зона адаптации). Из представленных графиков видно, что результаты экспериментальных исследований хорошо согласуются с теоретическими расчетами и имеют расхождение от 0,5% до 1%, что свидетельствует о перспективности использования методики адаптивного управления для различных классов МСЭ.

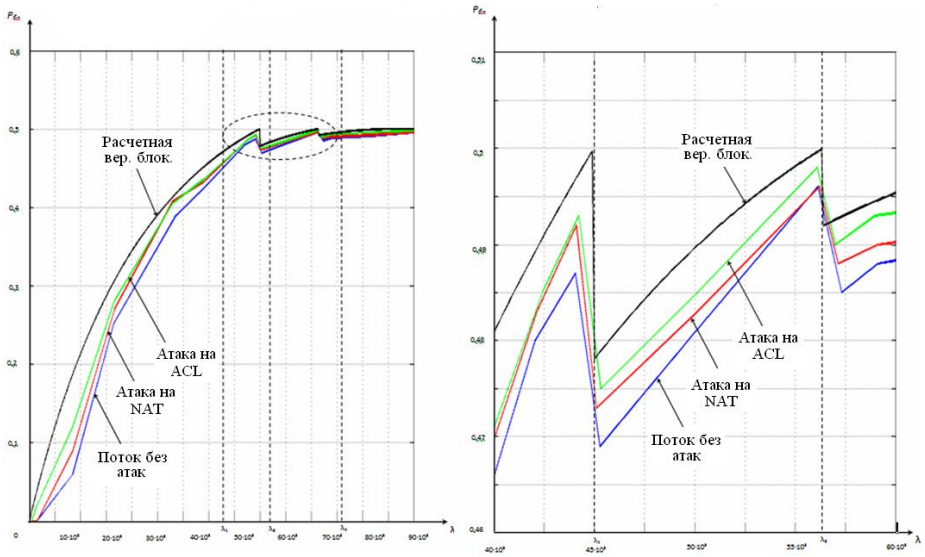

Рис. 8. График расчетной и практической вероятностей блокировки МСЭ

Заключение

Разработана рабочая схема полунатурной модели ИТС и сценарий экспериментальных исследований характеристик МСЭ на полунатурной модели. Сформированы тесты для задания потоков атак на МСЭ, настройки коммутаторов и интерфейсов МСЭ, конфигурирования МСЭ применительно к каждой функции проверки пакетов.

Проведены исследования параметров МСЭ и получены зависимости вероятностей отказов от нагрузки λ для каждой функции проверки. Определен вид функций времени обслуживания в зависимости от объемов таблиц и размера пакетов для каждой функции МСЭ.

Осуществлен поиск наиболее предпочтительных вариантов распределения функций между МСЭ, образующих ДМЗ. Определена область реконфигурирования МСЭ, называемая зоной адаптации, и получены отношения, описывающие правила перераспределения функций проверки между МСЭ.

Показано, что реализация правил переключения функций в зоне адаптации позволяет в 1,7 раза увеличить пропускную способность МСЭ и тем самым уменьшить вероятность блокировки МСЭ из-за перегрузки.

ADAPTIVE CONTROL OF FIREWALL SCREENING

M.N. BOBOF, F.O. MOHAMMED

Abstract

The traffic checking processes in firewall, that forms and configures a demilitarized zone, found that the processing time of initial checking and inspection engine functions depends on the size of packet under check, and the processing time of the xlate lookup (network address translation), connection lookup and access list lookup functions depends on the size of the corresponded table. Identified the most preferred choice to distribute the checking traffic functions between the two firewalls at the border of the demilitarized zone, by calculating the adaptation zone and selecting the required functions of the switching points.

Список литературы

1. *Hucaby D.* Cisco ASA, PIX, and FWSM Firewall Handbook. USA, 2008.
2. *Oppenheimer P.* Top-Down network design. USA, 2009.
3. *Deal A. Richard*. Cisco ASA Configuration. USA, 2009.
4. *Blank A.G.* TCP/IP Foundations USA, 2004.
5. *Palm W.J.* Introduction to MATLAB for engineers. USA, 2011.
6. *Johnson R.K.* The elements of MATLAB style. Cambridge, 2011.