УДК 621.391

ОЦЕНКА ВЛИЯНИЯ ФУНКЦИИ КОНТРОЛЯ СОЕДИНЕНИЯ НА ПРОПУСКНУЮ СПОСОБНОСТЬ МЕЖСЕТЕВОГО ЭКРАНА

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 1 июля 2011

Этот тест используется для измерения времени обработки таблицы соединения в межсетевом экране (МСЭ) Cisco ASA 5520. МСЭ проверяет все пакеты, которые проходят через него, несколькими разными функциями. Для измерения времени обработки таблицы соединения в МСЭ все функции проверки пакетов кроме функции проверки таблицы соединения должны быть выключены. Пропускная способность определяется на основе теории массового обслуживания как вероятность обслуживания заявки.

Ключевые слова: межсетевой экран, таблица соединения, входящее соединение, время обработки, пропускная способность, вероятность блокировки.

Введение

Все пакеты, проходящие через МСЭ, проверяются следующими функциями: контроль целостности, трансляция адреса, контроль соединения, управление доступом и инспектирование состояния. Каждая функция влияет на общую пропускную способность потому, что у каждой функции своя задача и свое время обработки. Для оценки функции контроля соединения в МСЭ все остальные функции проверки пакетов должны быть выключены. Это достигается использованием соответствующих протоколов и настройки МСЭ.

Оценка функции контроля соединения в МСЭ включает две части:

1) экспериментальные исследования для получения данных о временных затратах на выполнение функции контроля соединения,

2) аналитические расчеты на модели для получения значений пропускной способности и вероятности блокировки.

Экспериментальные исследования

Для проведения экспериментальных работ был собран стенд, приведенный на рис. 1. Стенд включает в себя:

1) ПК-1: персональный компьютер, который находится во внутренней сети и играет роль источника (отправителя);

2) К-1: коммутатор внутренней сети, который подключает ПК-1 к МСЭ через внутренний интерфейс (E0/1);

3) ПК-3: персональный компьютер, который играет роль монитора;

4) МСЭ: межсетевой экран Cisco ASA 5520;

5) К-2: коммутатор внешней сети, который подключает ПК-2 к МСЭ через внешний интерфейс (E0/0);

6) ПК-2: персональный компьютер, который находится во внешней сети и играет роль получателя.

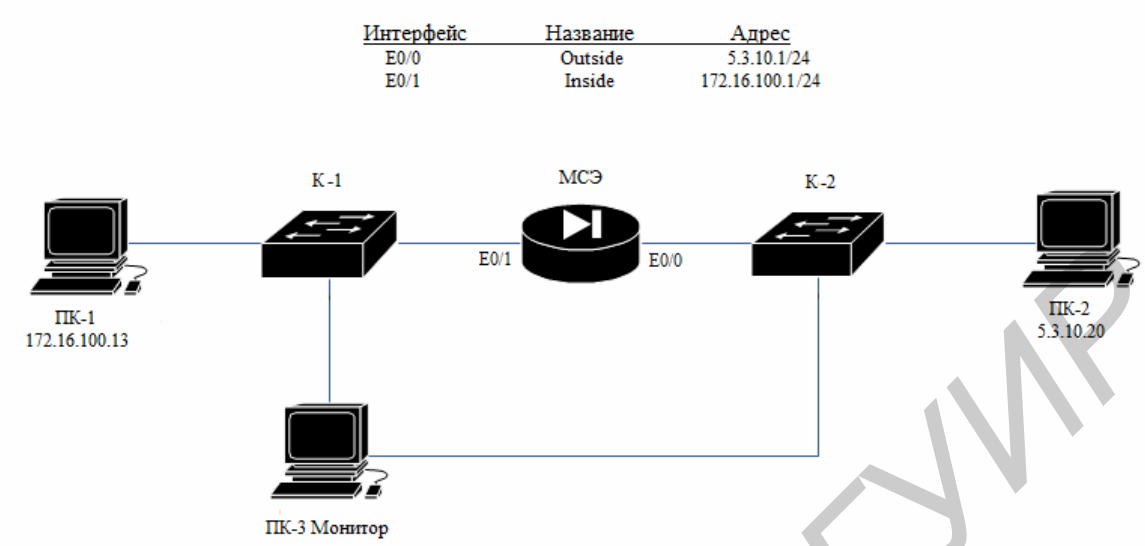

Рис. 1. Схема проведения эксперимента

На ПК-1 установлен генератор пакетов Colasoft packet builder, в ПК-2 и ПК-3 установлена программа Wireshark, которая играет роль сниффера – показывает получаемые пакеты и их параметры. В коммутаторах К-1 и К-2 сконфигурирована функция зеркала (Switch port analyzer (SPAN)), которая копирует все пакеты, проходящие через одни интерфейсы в другие.

Измерения времени работы функции контроля соединения проводились для различных объемов таблицы соединений, начиная от 20000 входов и заканчивая 180000 входами. Обычно входы таблицы соединений не создаются администраторами, они создаются автоматически во время прохождения трафика. Поэтому для создания входов в таблице соединения используется команда ping, которая отправляет ICMP-пакеты. Для ускорения создания входов написана отдельная программа на MATLAB, она создает 180 текстовых файлов, содержащих в себе 1000 ping-команд, разных по адресам назначения. Каждый текстовый файл копируется отдельно в окне командной строки.

В генераторе пакетов формируются две различные группы пакетов. Параметры пакетов первой группы совпадают с последним входом таблицы соединения, поэтому они пропускаются межсетевым экраном. Параметры пакетов второй группы не совпадают ни с каким из входов таблицы соединения, поэтому являются неправильными и блокируются.

Так как все входы таблицы соединения созданы командой ping, они являются входами протокола ICMP. Соответственно, их параметры совпадают с последним входом таблицы соединения МСЭ. Пакеты второй группы формируются с использованием протокола TCP без SYN-флага. Требуемый набор правильных и неправильных пакетов течение 30 с формируется в генераторе пакетов Colasoft packet builder в ПК-1 и отправляется в ПК-2. Неправильные пакеты (пакеты второй группы) блокируются межсетевым экраном, а правильные (пакеты первой группы) пропускаются и принимаются ПК-2. Во время прохождения пакетов коммутаторы К-1 и К-2 с помощью функции SPAN копируют все пакеты, проходящие через них в ПК-3.

В ПК-3 проходящие пакеты К-1 и К-2 регистрируются, обрабатываются программой Wireshark и сохраняются в текстовом файле. С помощью программы MATLAB по данным, находящимися в текстовом файле, рассчитывается среднее время обработки одного пакета и регистрируется в журнале эксперимента.

На рис. 2. представлен график измеренного времени обработки контроля соединения в МСЭ в зависимости от числа входов.

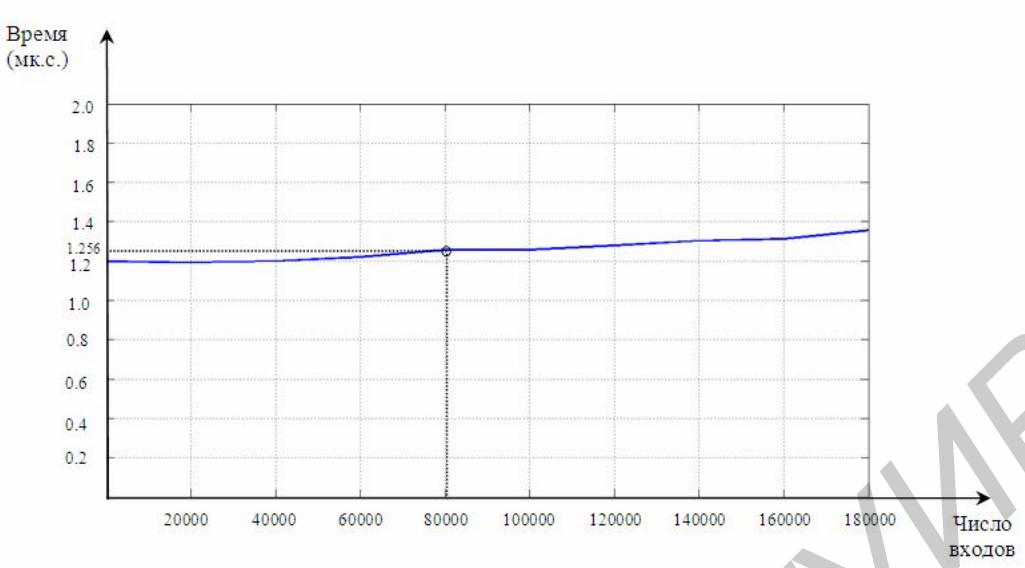

Рис. 2. Время обработки функции контроля соединений в МСЭ в зависимости от числа входов

Анализ графика показывает, что объем таблицы соединения не оказывает существенного влияния на время работы функции контроля соединения. Для проведения аналитических расчетов выбираем среднее значение времени контроля соединения, равное 1,256 мкс.

Аналитические расчеты

МСЭ представляет собой одноканальную систему передачи информации без буфера входящих сообщений. Если на такую систему, занятую проверкой очередного пакета, поступит следующее сообщение, то оно будет отброшено, а система будет считаться заблокированной. Эта модель полностью соответствует модели одноканальной системы массового обслуживания с отказами, используем в задачах теории массового обслуживания.

Данная система массового обслуживания состоит только из одного канала ($n = 1$) и на нее поступает пуассоновский поток заявок с интенсивностью λ, зависящей, в общем случае, от времени:

$\lambda = \lambda(t)$.

Заявка, заставшая канал занятым, получает отказ и покидает систему. Обслуживание заявки продолжается в течение случайного времени $T_{об}$, распределенного по показательному закону с параметром μ:

$f(t) = \mu e^{-\mu t}$ $(t > 0)$.

Из этого следует, что «поток обслуживания» – простейший, с интенсивностью μ.

Рассмотрим единственный канал обслуживания как физическую систему S, которая может находиться в одном из двух состояний: S_0 – свободен, S_1 – занят.

Граф системы перехода (ГСП) показан на рис. 3.

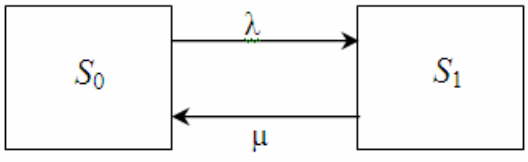

Рис. 3. ГСП для одноканальной СМО с отказами

Из состояния S_0 в S_1 систему, очевидно, переводит поток заявок с интенсивностью λ; из S_1 в S_0 – «поток обслуживания» с интенсивностью μ.

Вероятности состояний: $p_0(t)$ и $p_1(t)$. Очевидно, для любого момента t:

$p_0(t)+p_1(t)=1$. (1)

Для одноканальной СМО с отказами вероятность p_0 есть не что иное, как относительная пропускная способность q. Действительно, p_0 есть вероятность того, что в момент t канал свободен, или вероятность того, что заявка, пришедшая в момент t, будет обслужена. Следовательно, для данного момента времени t среднее отношение числа обслуженных заявок к числу поступивших также равно $p_0(q=p_0)$.

Решение дифференциальных уравнений Колмогорова для вероятности состояний данной СМО в переделе, при $t\to\infty$, когда процесс обслуживания уже установится, дает предельное значение относительной пропускной способности в виде преобразования Лапласа-Стилтьеса (ПЛС):

$$q = \frac{\mu}{\lambda + \mu}. \qquad (2)$$

Зная пропускную способность системы q (вероятность того, что пришедшая в момент t заявка будет обслужена), легко найти вероятность отказа (блокировки)

$$P_{\text{отк}} = 1 - q$$

или среднюю часть необслуженных заявок среди поданных. При $t\to\infty$

$$P_{\text{отк}} = 1 - \frac{\mu}{\lambda + \mu} = \frac{\lambda}{\lambda + \mu} \qquad (3)$$

Параметр μ зависит от свойств МСЭ и может быть вычислен по результатам экспериментальных исследований.

Из результатов эксперимента среднее время обработки МСЭ = 1,256 мкс, поэтому

$$\mu = \frac{1}{1,256^{-6}} = 796178.$$

На рис. 4 предоставлены графики пропускной способности и вероятности блокировки пакетов в МСЭ при выполнении функции контроля соединения в зависимости от нагрузки λ, вычисленные по формулам (2) и (3).

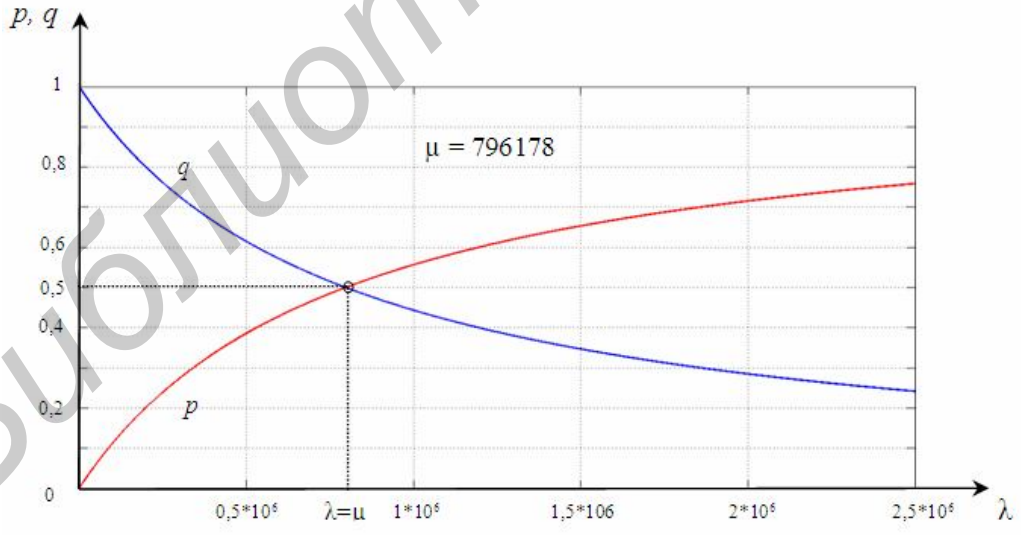

Рис.4. Пропускная способность и вероятность блокировки проверки таблицы соединений в МСЭ

Заключение

МСЭ является эффективным и современным средством, используемым для защиты локальных сетей. Чтобы узнать реальные способности МСЭ, его параметры были определены опытным путем. Функция контроля соединений является одной из самых эффективных функ-

ций, проверяющих трафик в МСЭ, потому что она существенно не увеличивает общее время обработки МСЭ и практически не снижает пропускной способности МСЭ.

EVALUATION THE INFLUENCE OF CONNECTION TABLE FUNCTION IN FIREWALL'S THROUGHPUT

M.N. BOBOF, F.O. MOHAMMED

Abstract

This test is used to measure the processing time for connection table lookup in Cisco ASA 5520 firewall, every packet incoming or outgoing from the protected network checked by many functions working in the firewall, every function has a processing time and it affects on the firewall's throughput. Connection table lookup is one of these working functions, to measure the processing time of this function, all other functions must be deactivated, and then the processing time is measured across the connection entries in the table. Throughput is defined by queuing theory as probability of blocking.

Литература

1. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook // USA, 2008.
2. *Richard A. Deal.* Cisco ASA Configuration // USA, 2009.
3. *Ray Blair, Arvind Durai* // Cisco ASA 5500 Series Configuration Guide using the CLI, Software Version 8.2. USA, 2009.
4. RFC 792 – Internet Control Message Protocol.