УДК 004.042

С.В. Морковин, сотрудник, Академия ФСО России (Орел, Россия) (e-mail: msw-c@ya.ru)

В.С. Панищев, канд. техн. наук, доцент, ФГБОУ ВО «Юго-Западный государственный университет» (Курск., Россия) (e-mail:gskunk@yandex.ru)

ОПТИМИЗАЦИЯ АЛГОРИТМА ПАРАЛЛЕЛЬНОЙ ОБРАБОТКИ ДАННЫХ ЯДРОМ SNORT

В статье рассматриваются вопросы оптимизации алгоритма программно-аппаратного средства обнаружения и предупреждения компьютерных атак на автоматизированное рабочее место доступа к сети интернет и сетевое оборудование. Главная задача исследования заключалась в увеличении пропускной системы и снижении ресурсов на обработку данных.

Указана необходимость модификации существующих программных продуктов, разработанных под архитектуры однопоточного выполнения программы. В частности, рассматривается проект обнаружения компьютерных атак Snort, изначально ориентированный на работу на одном ядре процессора в однопоточном режиме.

Принцип распараллеливания вычислений ядром Snort основан на делении входного трафика на более низкоскоростные атомарные каналы, распределяемые на несколько отдельно запущенных ядер Snort в виде отдельных процессов, которые имеют связь друг с другом и могут обмениваться информацией.

Предложена оптимизация разработанного алгоритма, заключающаяся в использовании быстрой разделяемой памяти для обмена данным между процессами.

Рассмотрен один из ключевых элементов в алгоритме распараллеливания обработки данных, а именно, алгоритм балансировки. На основе предложенного алгоритма оптимизирована работа блока балансировки входного трафика, что повысило скорость работы системы в целом.

Для решения задачи моделирования и оптимизации построенной распределенной системы обнаружения компьютерных атак предложен испытательный стенд. Описана структура стенда, методика тестирования, а также численные данные проведенного эксперимента. В качестве объекта испытаний на вход системы подавался типовой трафик из магистрального канала связи. По результатам исследования представлена зависимость скорости обработки трафика от количества ядер в системе.

Ключевые слова: *компьютерная атака, система отражения атак, балансировка трафика, сетевой сенсор.*

DOI: 10.21869/2223-1560-2017-21-1-30-35

Ссылка для цитирования: Морковин С.В., Панищев В.С. Оптимизация алгоритма параллельной обработки данных ядром SNORT // Известия Юго-Западного государственного университета. 2017. Т. 21, № 1(70). С. 30–35.

***

Особенности развития современных аппаратных серверных платформ заключаются в том, что предельные частоты работы процессоров достигнуты и для повышения производительности разработчики процессоров идут по пути расширения количества ядер в системе. В силу такого развития аппаратной архитектуры возникают задачи модификации существующих «старых» программных продуктов, разработанных под архитектуры однопоточного выполнения программы.

Популярный проект обнаружения компьютерных атак Snort, написанный на языке Си, спроектирован для работы на одном ядре процессора в однопоточном режиме [1-4]. Следовательно, производительность системы ограничивается тактовой частой процессора. Конечно, помимо тактовой частоты, большое значение в скорости выполнения программы играет количество уровней и объемы внутренней быстрой памяти процессора, а также набор поддерживаемых инструкций. Но, в данном случае с проектом Snort проблема заключается в том, что, например, серверный процессор имеет 12 ядер с технологией Hyper-threading, следовательно, способен параллельно выполнять 24 задачи (процесса), а приложение Snort способно захватить под свои ресурсы только половину ядра, что означает загрузить процессор не более чем на 5%. В

такой конфигурации система обнаружения атак способна обрабатывать типовой трафик со скоростью не более 0.7 Гбит/с на одном из самых производительных серверных процессоров Intel.

Одной из целей работы являлось достижение высокой пропускной способности системы обработки трафика с последующим его глубоким анализом.

Решение задачи преодоления предела пропускной способности одного сенсора осуществлялось путем распараллеливания процесса обработки с последующей оптимизацией узких мест системы [5-6].

Разработанный алгоритм параллельной обработки данных ядром Snort показал существенный прирост производительности в системе обнаружения компьютерных атак, что позволило на первых этапах исследования обрабатывать входной трафик со скоростями до 5 Гбит/с. Особенности распараллеливания вычислений ядром Snort заключаются в физическом делении входного трафика на более низкоскоростные атомарные каналы, которые распределяются на несколько отдельно запущенных ядер Snort в виде отдельных процессов, которые имеют связь друг с другом и могут обмениваться информацией. В процессе оптимизации разработанного алгоритма было принято решение использовать быструю разделяемую память для обмена данным между процессами. Также была оптимизирована работа блока балансировки входного трафика, что упростило алгоритм балансировки и повысило скорость работы системы в целом [7-10].

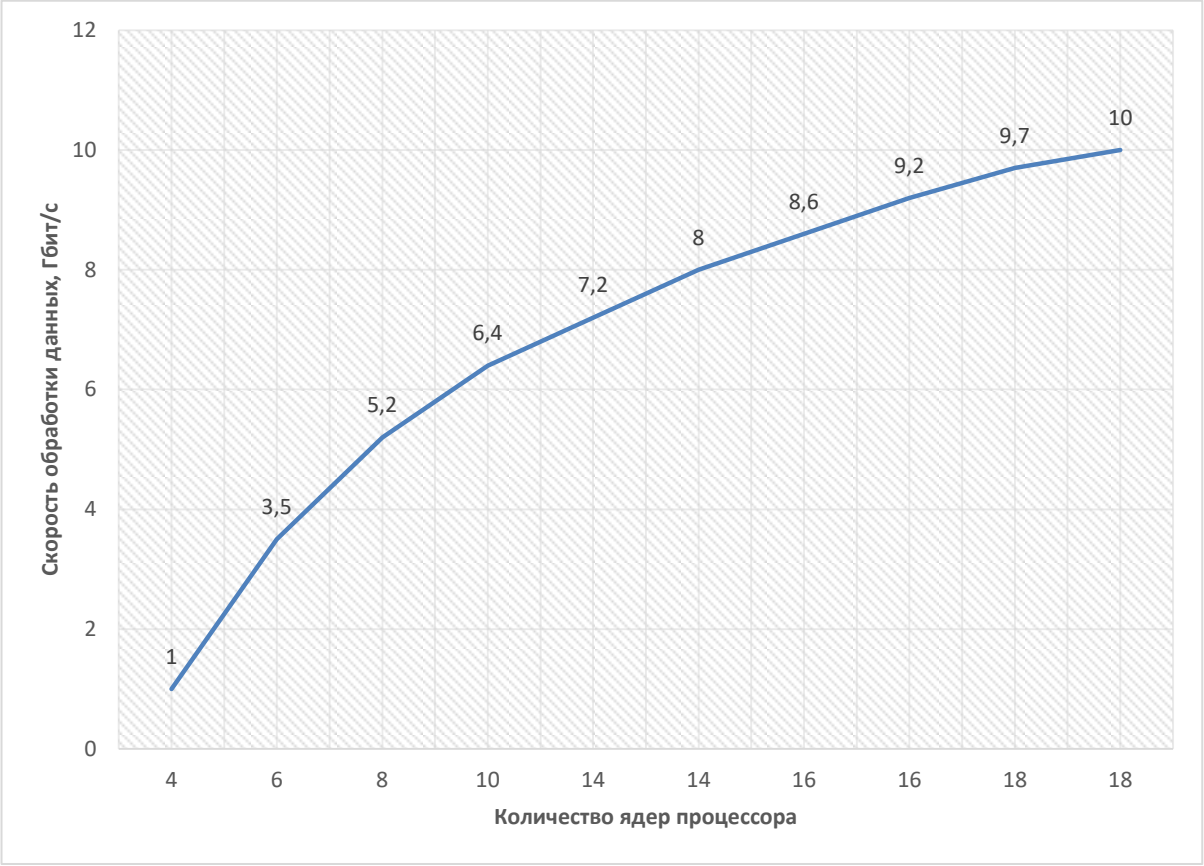

Рис. 1. Зависимость пропускной способности системы от количества процессорных ядер

Простота системы заключается в гибкости масштабирования. Для обработки определенной скорости потока данных необходима определенная вычислительная мощность сервера. При недостаточных ресурсах одного сервера предостав-

ляется возможность расширения системы на несколько серверов.

Алгоритм балансировки является одним из ключевых элементов в алгоритме распараллеливания обработки данных. Перед началом работы системе балансировки задается количество выходных потоков, на которое необходимо делить входной поток. На вход системы балансировки поступают IP-пакеты. Над каждым пакетом производится операция битового сложения по модулю два адреса источника и адреса получателя. Вычисляется остаток от деления результата сложения адресов на количество выходных потоков. Значением остатка от деления является индекс выходного потока, в который отправляется данный пакет.

Основные физические компоненты от которых зависит пропускная способность системы: тактовая частота процессора, количество ядер в процессоре, пропускная способность оперативной памяти.

Другими факторами, от которых зависит пропускная способность системы, являются: обрабатываемый трафик и конфигурация сенсоров; глубина и полнота анализа данных; количество подключенных предпроцессоров и правил.

Для решения задачи оптимизации построенной распределенной системы обнаружения компьютерных атак в рамках проводимого исследования был разработан испытательный стенд на базе процессора Intel Xeon E7-8890. В процессе испытаний на вход системы подавался типовой трафик из магистрального канала связи. По результатам исследования был выявлен закон зависимости скорости обработки трафика от количества ядер в системе.

Для построения испытательного стенда на терминале мониторинга трафика устанавливается специальное программного обеспечение «Сенсор», задача которого состоит в анализе и обработке входящего траффика, и в случае обнаружения вредоносных данных генерации и отправке соответствующего отчета координационному центру. Координационный центр представляет из себя связующее звено системы, контролирующее функционирование всех модулей. На сервере координационного центра помимо специального программного обеспечения, принимающего данные от сенсоров, также располагается база данных, в которую поступают события с информацией об обнаруженных атаках.

К координационному центру для управления системой удаленно подключается консоль администратора, которая позволяет отслеживать состояние сенсоров в режиме реального времени, а также производить операции по включению, отключению сенсоров, загрузки новых правил обработки, модулей и препроцессоров.

Основой подсистемы стенда системы обнаружения атак являются детектирующие сенсоры, которые позволяют анализировать входящий трафик с большой скоростью и своевременно оповещать координационный центр о возможных угрозах.

Архитектурно ядро сенсора состоит из трёх подсистем: декодера пакетов, подсистемы обнаружения и подсистемы регистрации и реагирования.

Декодер пакетов выполняет две основные функции – осуществляет перехват пакетов и представляет всю необходимую информацию о перехваченных пакетах в специально предназначенном для последующего анализа формате.

Сенсор поддерживает три вида подключаемых модулей: детектирующие,

препроцессоры и модули вывода информации.

Тестирование системы было начато с небольших скоростей – 2 Гбит/с. На данной скорости было запущено 4 сенсора, и общая загрузка процессора сервера составляла 15%.

На протяжении всего времени тестирования производились замеры скорости входных данных, загрузки процессора, количества ошибок, количества обнаруженных атак.

На вход сетевого адаптера поступал реальный поток интернет-трафика. Скорость потока варьировалась от 2 до 7 Гбит/с в зависимости от времени суток.

Для процессора, выбранного для тестирования, выявлен предел скорости на одно ядро сенсора - 700 Мб/с.

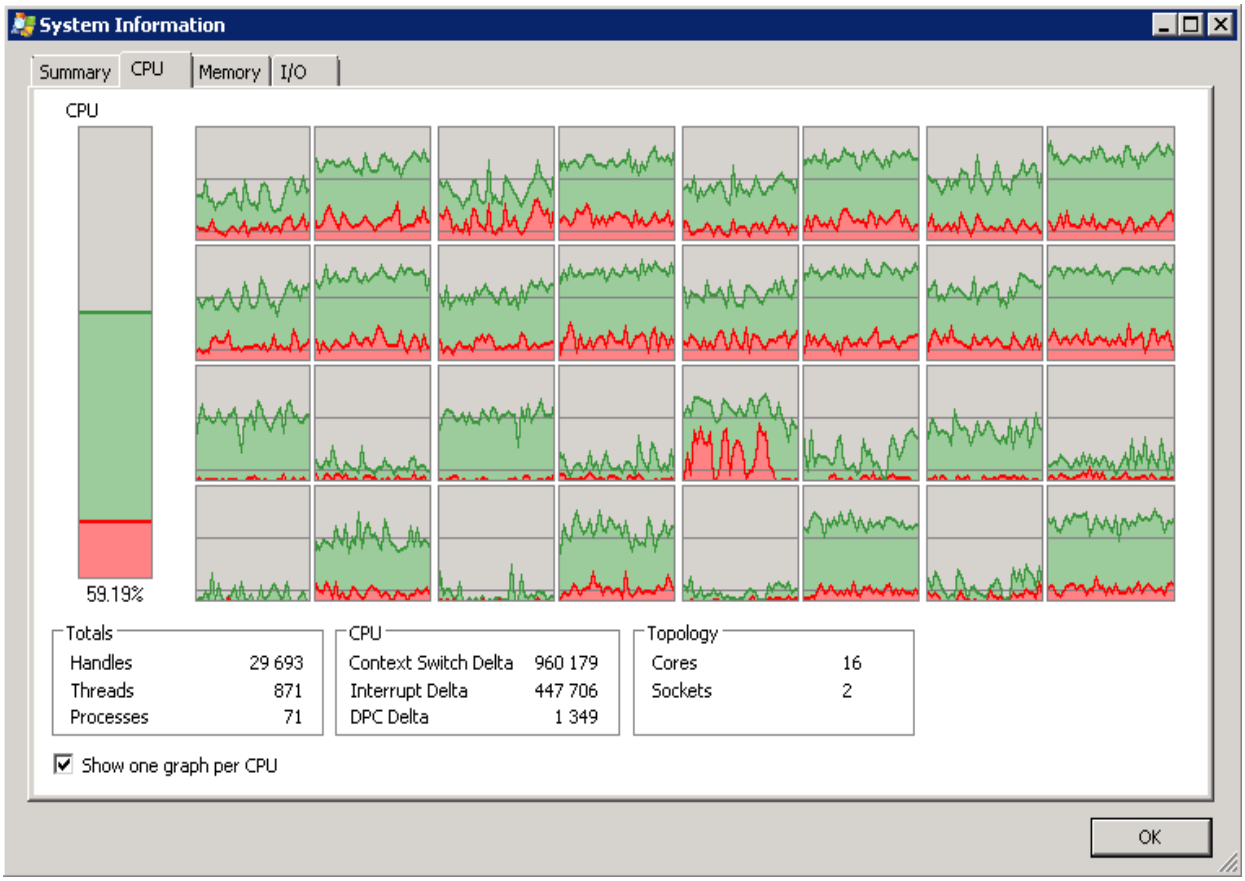

Рис. 2. Загрузка процессоров при скорости 7 Гбит/с

За время тестирования максимально наблюдаемая скорость в канале составляла 7 Гб/с. Для обработки данных с такой скоростью на тестовом стенде необходима работа 12 сенсоров. Загрузка процессоров составляла 60%. Имеется запас производительности для более высоких скоростей.

Отказоустойчивость оценивалась путем непрерывной работы всей системы на протяжении 7 суток, после чего система была остановлена для перезапуска, чтобы осуществить обновление ее компонентов. За данное время работы не выявлено ни одного отказа.

Техническое решение в виде макета обнаружения и предупреждения компьютерных атак позволяет производить масштабные тесты разработанной системы обнаружения и отражения атак. Предо-

ставляется возможность исследования зависимости загрузки системы от количества физических процессоров, задействованных под комплекс от скорости входных данных и соотношения вредоносных данных с полезным трафиком на скорости до 10 Гбит/с.

Список литературы

1. Andrew R. Baker. Snort IDS and IPS Toolkit // Syngress. – 2008. – Pp. 79-139.

2. SNORT Users Manual. – URL: https: // www.snort.org/

3. Jay Beale and oth. Snort Intrusion Detection 2.0 // Syngress. – 2010. – 550p.

4. Jay Beale and oth. Snort Intrusion Detection and Prevention Toolkit // Syngress. – 2010. – 768 p.

5. Нетес В. А. Качество обслуживания на сетях связи. Обзор рекомендаций МСЭ-Т // Сети и системы связи. – 1999. – №. 3. – С. 66-71.

6. Кузнецов С. Н., Огнев И. В., Поляков С. Ю. Методика тестирования каналов связи Ethernet // Технологии и средства связи. – 2005. – №. 2. – С. 46-48.

7. Воеводин В. В. Параллельные вычисления // БХВ-Петербург. – 2002. – С. 32-78.

8. Ватутин Э.И., Титов В.С. Особенности реализации технологии hyper-threading в процессорах Intel Pentium 4 на примере выполнения кода различного типа // Известия Юго-Западного государственного университета. – 2008. – № 2 (23). – С. 62-65.

9. Ватутин Э.И., Титов В.С. Оценка реальной производительности современных процессоров в задаче умножения матриц для однопоточной программной реализации с использованием расширения SSE (часть 1) // Известия Юго-Западного государственного университета. – 2015. – № 4 (61). – С. 26-35.

10. Alan G. Konheim. Computer Security and Cryptography // Wiley. – 2016. – Pp. 46-182.

Поступила в редакцию 12.01.17

UDC 004.042

S.V. Morkovin, Academy FSO (Orel, Russia) (e-mail: msw-c@ya.ru)

V.S. Panishchev, Candidate of Engineering Sciences, Associate Professor**,** Southwest State University (Kursk, Russia) (e-mail:gskunk@yandex.ru)

AN OPTINIZED ALGORITHM OF PARALELL DATA PROCESSING BY SNORT CORE

The paper addresses the problem of optimizing the firmware algorithm of detecting and preventing computer attacks on the Internet access workstations and networking equipment. The main objective was to boost the device capacity and save data processing resources.

It has been proved that existing soft products that have been developed for single thread execution architectures need to be modified. In particular the paper discusses Snort network intrusion and prevention system that initially has been made to operate on the processor single core in single thread mode.

Snort core paralleling principle is based on dividing the inbound traffic into lower-speed atomic channels that are distributed over several individually runnable Snort cores as individual processes that are interconnected and can exchange information.

The authors suggest the algorithm optimization way that consists in utilizing the fast shared memory to facilitate information exchange between the processes.

The paper focuses on a key element in the data processing paralleling algorithm which is the balance algorithm. The proposed algorithm has been used to optimize the performance of the inbound traffic balancing unit, which increased the operation speed of the total system.

A test facility has been developed to simulate and refine the constructed intrusion detection distributed system. The paper presents the testing facility structure, testing method and test numerical results.

The test item was a standard traffic routed to the system input from backbone link. The research results were used to determine the dependency of the traffic processing speed on the number of cores in the system.

Key words: *computer attack, intrusion prevention system, traffic balancing, netted sensor*

DOI: 10.21869/2223-1560-2017-21-1-30-35

For citation: Morkovin S.V., Panishchev V.S. An Optinized Algorithm of Paralell Data Processing by SNORT Core, Proceeding of Southwest State University, 2017, vol. 21, no. 1(70), pp. 30-35 (in Russ.).

***

Reference

1. Andrew R. Baker. Snort IDS and IPS Toolkit // Syngress. – 2008. – Pp. 79-139.

2. SNORT Users Manual. – URL: https: // www.snort.org/

3. Jay Beale and oth. Snort Intrusion Detection 2.0 // Syngress. – 2010. – 550p.

4. Jay Beale and oth. Snort Intrusion Detection and Prevention Toolkit // Syngress. – 2010. – 768 p.

5. Netes V. A. Kachestvo obsluzhivanija na setjah svjazi. Obzor rekomendacij MSJe-T // Seti i sistemy svjazi, 1999. – no. 3, – Pp. 66-71.

6. Kuznecov S. N., Ognev I. V., Poljakov S. Ju. Metodika testirovanija kanalov svjazi Ethernet // Tehnologii i sredstva svjazi, 2005. no. 2, pp. 46-48.

7. Voevodin V. V. Parallel'nye vychislenija // BHV-Peterburg, 2002, pp. 32-78.

8. Vatutin Je.I., Titov V.S. Osobennosti realizacii tehnologii hyper-threading v processorah Intel Pentium 4 na primere vypolnenija koda razlichnogo tipa // Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta, 2008, no. 2 (23), pp. 62-65 (in Russ.).

9. Vatutin Je.I., Titov V.S. Ocenka real'noj proizvoditel'nosti sovremennyh processorov v zadache umnozhenija matric dlja odnopotochnoj programmnoj realizacii s ispol'zovaniem rasshirenija SSE (chast' 1) // Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta, 2015, no. 4 (61). pp. 26-35.

10. Alan G. Konheim. Computer Security and Cryptography // Wiley. – 2016. – Pp. 46-182.