ISSN 1814-1196
Научный вестник НГТУ
том 56, № 3, 2014, с. 108–114

http://journals.nstu.ru/vestnik
Scientific Bulletin of NSTU
Vol. 56, No. 3, 2014, pp. 108–114

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

MODERN INFORMATION TECHNOLOGIES

УДК 006.72

Разработка системы обнаружения аномалий сетевого трафика*

Д.К. ЛЕВОНЕВСКИЙ[1], Р.Р. ФАТКИЕВА[2]

[1] 199178, РФ, г. Санкт-Петербург, 14-я линия В.О., 39, Санкт-Петербургский институт информатики и автоматизации РАН, младший научный сотрудник, e-mail: DLewonewski.8781@gmail.com
[2] 199178, РФ, г. Санкт-Петербург, 14-я линия В.О., 39, Санкт-Петербургский институт информатики и автоматизации РАН, к. т. н., старший научный сотрудник, e-mail: rikki2@yandex.ru

Масштабное развитие сетевых сервисов ставит перед их администраторами задачу обеспечить управляемость и подотчётность этих систем, их штатное функционирование и максимально исключить факты нештатного функционирования – сетевые аномалии, для чего используются системы мониторинга. Рассмотрены существующие системы мониторинга сети. Предложен способ построения системы обнаружения сетевых аномалий на принципах гибкости, модульности и расширяемости. Система использует клиент-серверную архитектуру, что способствует независимости компонентов и созданию распределённой системы. К компонентам системы относятся сетевой сенсор, анализатор, база конфигурации и сетевой статистики, модуль реагирования и веб-интерфейс. Предлагается способ повышения эффективности и быстродействия системы с использованием методов прогноза сетевого трафика. Для реализации прогнозирования в состав системы может включаться дополнительный модуль. Описан процесс обработки данных о сетевой активности в системе. К основным этапам процесса относятся обнаружение фактов, подсчёт фактов, агрегация фактов, фильтрация данных, проверка критериев сетевых аномалий и получение результата. Среди дальнейших направлений исследования – анализ методов построения профилей сетевой активности и прогнозирования легитимного сетевого трафика с учётом этих профилей. Отклонение прогноза от реального трафика предполагается анализировать на предмет изменения состояния системы.

Ключевые слова: информационная безопасность, сетевой трафик, сетевые аномалии, *Distributed Denial of Service*, *DDoS*, отказ в обслуживании, мониторинг сети, архитектура приложений, обработка данных

ВВЕДЕНИЕ

Одним из проявлений процесса информатизации общества является масштабное развитие сетевых сервисов. Перед администраторами информационно-вычислительных систем, предоставляющих сервисы, стоит задача обеспечить управляемость и подотчётность этих систем, целостность, доступность и конфиденциальность данных, т. е. обеспечить штатное функционирование системы и максимально исключить факты нештатного функционирования – сетевые аномалии.

Сетевые аномалии имеют различные причины и могут быть связаны с деятельностью хакеров, некомпетентных пользователей, неисправностью аппаратуры и дефектами программного обеспечения. Существуют видимые аномалии, проявляющиеся непосредственно в некорректной работе информационно-вычислительной системы. Аномалии могут и не иметь видимых признаков, но привести к сбоям через длительное время. Классификация аномалий [1] показана на рис. 1.

Обнаружение сетевых аномалий возможно с помощью использования систем мониторинга – комплекса мер, направленных на получения сведений о состоянии системы для приня-

* *Статья получена 20 марта 2014 г.*

тия решений о реакции на события. Эффективность системы мониторинга напрямую зависит от входящих в ее состав компонент, каждый из которых выполняет свою функцию. При этом при проектировании подобных систем необходимо учитывать целевую аудиторию, параметры отслеживаемой подсистемы, условия переходов от одного состояния в другое, частоту обновления и способ хранения данных. Отдельно можно выделить формат представления данных пользователю.

Рис. 1. Классификация сетевых аномалий

Из представленных и наиболее популярных в настоящее время систем мониторинга можно выделить:

1) Cacti (*www.cacti.net*) – веб-приложение с открытым кодом. Позволяет производить сбор статистических данных за определенный промежуток времени с отображением их в виде графиков. Статистика отображается по таким параметрам, как процессор, оперативная память, количество запущенных процессов, входящий и исходящий трафик сети;

2) Zabbix – (*www.zabbix.com*) – система мониторинга серверов, компьютерных сетей, сетевого оборудования, распространяемая на бесплатной основе. В качестве хранилища данных используется PostgreSQL, SQLite, MySQL, Oracle. Поддерживает несколько видов мониторинга: ZABBIXagent, Simplechecks, externalcheck;

3) Nagios – (*www.nagios.org*) – программа с открытым кодом. Осуществляет следующие операции: мониторинг сетевых служб, наблюдение за состоянием хостов, удаленный мониторинг с помощью шифрованных туннелей SSLи SSH;

4) Ganglia (*ganglia.sourceforge.net*) – система, предназначенная для мониторинга кластеров параллельных вычислений, а также облачных систем с иерархической структурой. Позволяет наблюдать за каждой машиной в режиме реального времени;

5) PRTG (*www.paessler.com/prtg*) – условно-бесплатная программа за наблюдением сети. Работает в операционных системах семейства Windows. Осуществляет сбор данных о протоколах, с возможностью сохранения их в базе данных и просмотром в виде таблиц и графиков;

6) Snort [2] – свободная сетевая система предотвращения и обнаружения вторжений с открытым исходным кодом, выполняющая регистрацию пакетов по определённым признакам и в реальном времени осуществляющая анализ трафика в IP сетях.

Однако анализ и использование описанных систем мониторинга затрудняется по следующим причинам:

1) общая задача обнаружения аномалий требует возможности тонкой настройки системы и управления процессом разбора заголовков и содержимого пакетов, тогда как в рассмотренных системах эти возможности ограничены;

2) ряд продуктов являются закрытыми, что не позволяет изучить алгоритмы, лежащие в их основе.

По этой причине предлагается способ построения наиболее гибкой модели обнаружения сетевых аномалий на принципах модульности и расширяемости.

1. ОПИСАНИЕ СИСТЕМЫ МОНИТОРИНГА

Первоначальной задачей в разработке системы мониторинга было определение архитектуры системы, её компонентов и схемы взаимодействия между ними. Используется клиент-серверная архитектура, что способствует независимости компонентов и созданию распределённой системы. Схема представлена на рис. 2, реализация в виде сети – на рис. 3.

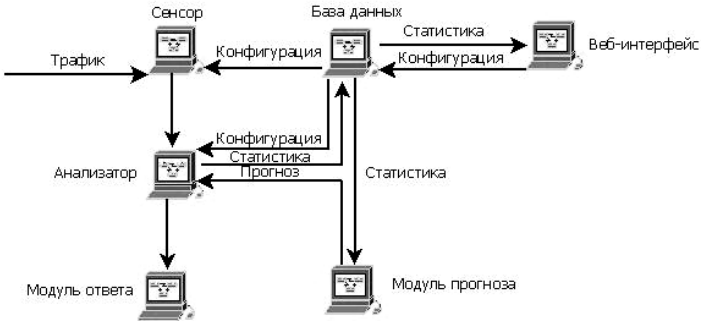

Рис. 2. Схема взаимодействия компонентов

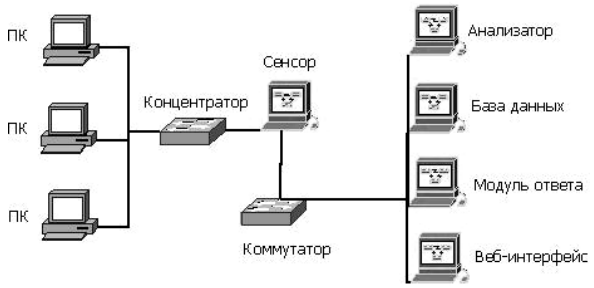

Рис. 3. Схема сети

Архитектура системы включает в себя следующие компоненты.

Сетевой сенсор перехватывает входящий трафик и подвергает его сортировке по протоколам с подсчётом количества пакетов, их длин, флагов и других параметров. Сенсор связан с сегментом локальной сети для перехвата трафика, базой данных для чтения правил разбора пакетов и анализатором для передачи статистики.

Модуль-анализатор получает данные о сетевом трафике от сенсора и рассчитывает метрики – показатели интенсивности аномалии. Далее анализатор проверяет критерии наличия аномалии и при необходимости вызывает модуль ответа для реакции.

База данных является реляционной. Для разработки базы данных использовалась СУБД MySQL. База данных разбита на 3 части, которые могут быть реализованы на отдельных серверах:

1) описательная часть хранит информацию о протоколах, измеряемых признаках, метриках, критериях аномалий;

2) статистические данные по измеряемым величинам – таблицы с данными по протоколам, метрикам, событиям об угрозах;

3) административная часть хранит информацию о пользователях системы.

Модуль прогноза является опциональным и использует модели построения профиля сетевой активности и прогнозирования временных рядов.

Модуль ответа предназначен для реакции на наличие аномалии. Реакция основывается на данных, поступающих от анализатора.

Веб-интерфейс разработан для визуализации и администрирования системы мониторинга, с помощью него возможно просмотреть все события по угрозам, весь входящий трафик за

определенный период, по определенным протоколам в режиме реального времени (рис. 4). Для администратора существует настройка базы данных, отображаемых протоколов, событий, связанных с угрозами.

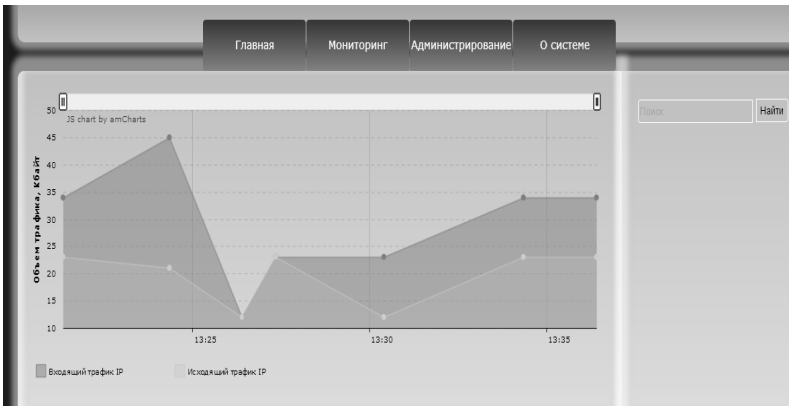

Рис.4. Интерфейс программы мониторинга

2. ОБРАБОТКА ДАННЫХ

Обработка данных в системе происходит в ряд этапов (рис. 5).
Ошибка!

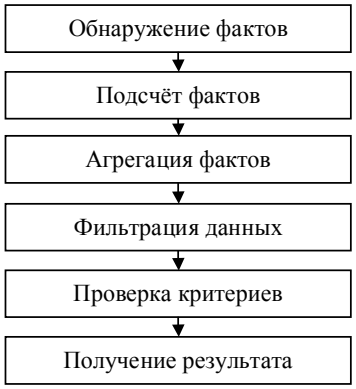

Рис. 5. Этапы обработки данных

Обнаружение фактов представляет собой выделение из сетевого трафика пакетов, обладающих значимыми для целей обнаружения признаками (например, пакеты, соответствующие определённому протоколу; пакеты с некоторым значением поля или флага в заголовке).

Подсчёт фактов представляет собой вычисление количества и/или объёма пакетов для каждого признака, учитываемого на предыдущем этапе обработки данных.

Агрегация фактов – определение количества и/или объёма пакетов для каждого признака за период времени.

Фильтрация данных заключается в применении статистических методов для ослабления влияния случайных вариаций во временных рядах. Применяются методы выделения тренда, например метод скользящего среднего.

Проверка критериев заключается в построении списка критериев сетевых аномалий, выполняющихся в данный момент. Критерии определяются пороговыми значениями измеряемых величин [3].

Получение результата представляет собой определение типов аномалии исходя из полученной на предыдущем этапе комбинации атак.

2. ВЕДЕНИЕ УЧЁТА УГРОЗ

На странице администрирования представлены графики по входящим угрозам. На рис. 6 и 7 показан отчет по трафику протокола TCP. На графике задано среднее пороговое значение, при пересечении графика в течение от 30 секунд и более регистрируется сообщение об угрозе.

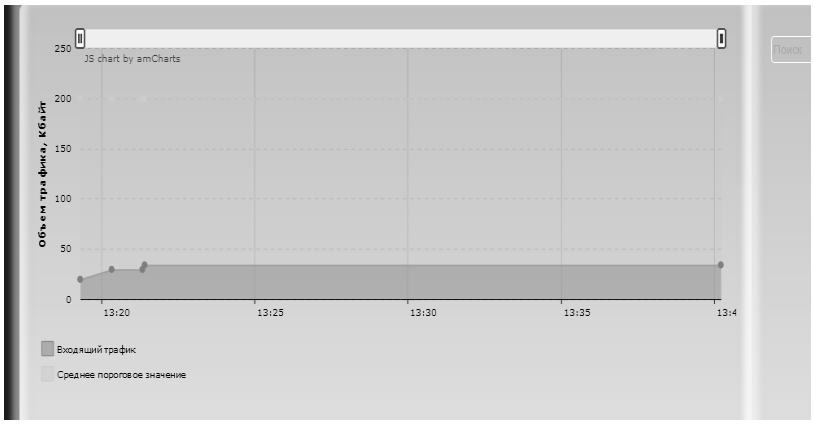

Рис. 6. Отсутствие атаки TCP-флуд

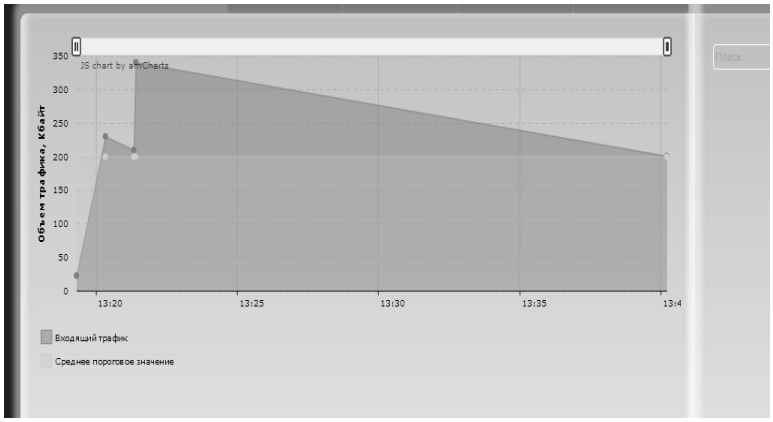

Рис. 7. Обнаружение атаки TCP flood

Для анализа и обнаружения той или иной атаки рассчитываются метрики, позволяющие обнаружить аномальную активность. Расчёт этих метрик связан с типом сетевых аномалий, большое число таких метрик для DDoS рассмотрено в статьях [4–8]. Если в течение заданного временного промежутка среднее значение метрики превышает пороговое значение, то регистрируется отклонение. Соответствующая информация записывается в базу данных. События может просматривать администратор сети.

ЗАКЛЮЧЕНИЕ

В результате проведённых исследований предложены архитектура системы и структура данных, предназначенные для использования в средствах обнаружения аномального сетевого трафика. В качестве приоритетов разработки выбраны гибкость и расширяемость.

Результаты применены для разработки программного обеспечения, предназначенного для администраторов компьютерных сетей.

Эффективность борьбы с вредоносной сетевой активностью и скорость реакции системы повышается с помощью использования методов прогноза сетевого трафика [9, 10]. Среди

дальнейших направлений исследования – анализ методов построения профилей сетевой активности и прогнозирования сетевого трафика.

СПИСОК ЛИТЕРАТУРЫ

1. *Афонцев Э.* Сетевые аномалии: статья [Электронный ресурс]. – URL: http://nag.ru/go/text/15588/.

2. *Бабенко Г.В., Белов С.В.* Анализ трафика TCP/IP наоснове методики допустимого порога и отклонения как инструмент определения инцидентов информационной безопасности [Электронный ресурс] // Технологии техносферной безопасности: интернет-журнал. 2011. – Вып. № 5 (39). – URL: http://agps-2006.narod.ru/ttb/2011-5/08-05-11.ttb.pdf

3. Traffic Anomaly Detection with Snort / M. Szmit, R. Wężyk, M. Skowroński, A. Szmit // Information Systems Architecture and Technology. Information Systems and Computer Communication Networks. – Wrocław: Wydawnictwo Politechniki Wrocławskiej, 2007. – P. 181–187. – ISBN 978-83-7493-348-3.

4. *Lu W., Traore I.* An unsupervised approach for detecting DDoS attacks based on traffic-based metrics // IEEE Pacific Rim Conference on Communications, Computers and signal Processing, PACRIM 2005, 24–26 Aug. 2005. – P. 462–465.

5. *Levonevskiy D.K., Fatkieva R.R.* DDoS attack detection method based on the statistical research of the traffic metrics // 6th International Conference on European Science and Technology. – URL: http://www.rusnauka.com/15_NPN_2013/Informatica/4_138702.doc.htm

6. *Levonevskiy D.K., Fatkieva R.R.* Statistical research of traffic-based metrics for the purpose of DDos attack detection // European Science and Technology: materials of the IV international research and practice conference, Munich, April 10th–11th, 2013. – Munich, Germany: Publishing office Vela Verlag Waldkraiburg, 2013. – Vol. 1. – P. 259–268.

7. *Фаткиева Р.Р.* Разработка метрик для обнаружения атак на основе анализа сетевого трафика // Вестник Бурятского государственного университета. Математика, информатика. – 2013. – Вып. 9. – С. 81–86.

8. Detecting distributed denial of service (DDoS) attacks through inductive learning // Lecture Notes in Computer Science. – Berlin; Heidelberg: Springer, 2003. – Vol. 2690. – P. 286–295.

9. *Szmit M., Szmit A.* Use of Holt-Winters method in the analysis of network traffic: Case study // Communications in Computer and Information Science. – 2011. Vol. 160. – P. 224–231.

10. Usage of Holt-Winters Model and Multilayer Perceptron in Network Traffic Modelling and Anomaly Detection / M. Szmit, A. Szmit, S. Adamus, S. Bugala // Informatica (Slovenia). – 2012. – Vol. 36 (4). – P. 359–368.

Левоневский Дмитрий Константинович, младший научный сотрудник лаборатории информационно-вычислительных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Основное направление научных исследований – исследование DDoS-атак, статистический анализ и моделирование трафика локальных сетей. Имеет 5 научных публикаций. E-mail: DLewonewski.8781@gmail.com.

Фаткиева Роза Равильевна, кандидат технических наук, старший научный сотрудник лаборатории информационно-вычислительных систем Федерального государственного бюджетного учреждения науки Санкт-Петербургский институт информатики и автоматизации РАН (СПИИРАН). Основное направление научных исследований – моделирование информационных систем. Имеет 37 научных публикаций. E-mail: rikki2@yandex.ru.

Development of network anomaly detection system architecture[*]

D.K. LEVONEVSKIY[1], R.R. FATKIEVA[2]

[1] St. Petersburg institute for informatics and automation of RAS, 39, 14th line O., St. Petersburg, 199178, Russian Federation, junior research fellow, e-mail: DLewonewski.8781@gmail.com

[2] St. Petersburg institute for informatics and automation of RAS, 39, 14th line O., St. Petersburg, 199178, Russian Federation, C. St, senior researcher, e-mail: rikki2@yandex.ru

An active process of network service development obliges their administrators to ensure the accountability and controllability of these systems, their regular operation mode and to exclude the facts of irregular functioning, network anomalies, as much as possible. Monitoring systems are used for this purpose. This paper overviews existing network monitoring systems and proposes a method of building a network anomaly detection system on basis of flexibility, expansibility and modularity. The system is based on the client-server architecture that is useful for building a distributed system from nearly independent modules. System components include network sensor, network analyzer, configurational and statistical database, response module and web interface. There is proposed a method of efficiency and operating speed improvement by means of traffic forecasting models. An additional module can be included for that. Also the paper describes the network activity data processing technique. Basic stages of this process are: fact discovery, fact counting, fact aggregation, data filtering, checking network anomaly criteria and drawing the conclusions. Among the

[*] *Received 20 March 2014.*

following research directions there are: analysis of methods of building network activity profiles and research of possibilities of regular network traffic forecasting using these methods. The difference between the forecast and the measured traffic may be inspected for the purpose of system state alterations.

Keywords: information security, network traffic, network anomalies, Distributed Denial of Service, DDoS, denial of service. network monitoring, application architecture, data processing

REFERENCES

1. Afontsev E. Setevye anomalii (Network anomalies). Available at: http://nag.ru/go/text/15588 (accessed 01.06.2014).

2. Babenko G.V., Belov S.V. [Analysis of TCP/IP traffic based on the methodology of specified threshold and the deviation as a tool of detecting information security accidents]. *Tekhnologii tekhnosfernoi bezopasnosti,* 2011, iss. no. 5 (39). (In. Russ.) Available at: http://agps-2006.narod.ru/ttb/2011-5/08-05-11.ttb.pdf (accessed 04.09.2014)

3. Szmit M., Wężyk R., Skowroński M., Szmit A. Traffic Anomaly Detection with Snort. Information Systems Architecture and Technology. Information Systems and Computer Communication Networks. Wrocław, Wydawnictwo Politechniki Wrocławskiej, 2007, pp. 181-187. ISBN 978-83-7493-348-3.

4. Lu W., Traore I. An unsupervised approach for detecting DDoS attacks based on traffic-based metrics. IEEE Pacific Rim Conference on Communications, Computers and signal Processing, PACRIM 2005, 24–26 Aug. 2005, pp. 462–465.

5. Levonevskiy D.K., Fatkieva R.R., DDoS attack detection method based on the statistical research of the traffic metrics. 6th International Conference on European Science and Technology. Available at: http://www.rusnauka.com/15_NPN_2013/Informatica/4_138702.doc.htm (accessed 04.09.2014)

6. Levonevskiy D.K., Fatkieva R.R. Statistical research of traffic-based metrics for the purpose of DDos attack detection. European Science and Technology. Materials of the IV international research and practice conference, Munich, April 10th–11th, 2013. Munich, Germany, Publishing office Vela Verlag Waldkraiburg, 2013, vol. 1. pp. 259-268.

7. Fatkieva R.R. Razrabotka metrik dlya obnaruzheniya atak na osnove analiza setevogo trafika [Development of Metrics for Attack Detection on the Basis of Network]. *Vestnik Buryatskogo gosudarstvennogo universiteta. Matematika, informatika – Bulletin of Buryat State University. Mathematics, informatics*, 2013, iss. 9, pp. 81-86.

8. Noh S., Lee C., Choi K., Jung G. Detecting distributed denial of service (DDoS) attacks through inductive learning. Lecture Notes in Computer Science. Berlin/Heidelberg, Springer, 2003, vol. 2690, pp. 286-295.

9. Szmit M., Szmit A. Use of Holt-Winters method in the analysis of network traffic: Case study. Communications in Computer and Information Science, 2011, vol. 160, pp. 224-231.

10. Szmit M., Szmit A., Adamus S., Bugala S. Usage of Holt-Winters Model and Multilayer Perceptron in Network Traffic Modelling and Anomaly Detection. Informatica (Slovenia), 2012, vol. 36 (4), pp. 359-368.