УДК 004.054.53
DOI: 10.33764/2618-981X-2019-9-61-65

ПРИМЕНЕНИЕ SIEM РЕШЕНИЙ НА МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

Глеб Владимирович Попков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доцент кафедры информационной безопасности; Сибирский государственный университет телекоммуникаций и информатики, 630009, Россия, г. Новосибирск, ул. Гурьевская, 9, доцент кафедры безопасности и управления в телекоммуникациях, тел. (383)343-91-11, e-mail: glebpopov@inbox.ru

В статье рассмотрены решения в области систем управления инцидентами безопасности SIEM (Security information and event management) и работа систем обнаружения / предупреждения сетевых вторжения класса IDS/IPS. Приводятся общие функциональные характеристики данных программных продуктов, предлагаются типовые решения по включению IDS/IPS в сеть передачи данных, на втором и третьем, четвёртом уровне модели OSI. Даётся краткое описание и некоторые практические примеры по применению IDS/IPS компании Sourcefire, продукта SNORT.

Ключевые слова: защита информации, SIEM, СОВ, IDS/IPS, SNORT.

APPLICATION OF SIEM SOLUTIONS ON MULTI-SERVICE COMMUNICATIONS NETWORKS

Gleb V. Popkov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Department of Information Security; Siberian State University of Telecommunications and Informatics, 9, Gurievskaya St., Novosibirsk, Russia, 630009, Associate Professor, Department of Security and Management in Telecommunications, phone: (383)343-91-11, e-mail: glebpopov@inbox.ru

The article discusses solutions in the field of SIEM (Security information and event management systems) and the operation of IDS / IPS class network intrusion detection / prevention systems. The general functional characteristics of these software products are presented, typical solutions for the inclusion of IDS / IPS in data transmission network are offered, at the second, third and fourth levels of the OSI model. A brief description and some practical examples of using IDS / IPS from Sourcefire, the SNORT product, are given.

Key words: information security, IDS/IPS, SNORT.

Традиционное применение межсетевых экранов для фильтрации трафика сетей передачи данных зачастую недостаточно для обнаружения сетевых атак на канальном, сетевом и транспортном уровнях модели OSI.

Широко распространенные системы обнаружения и предотвращения вторжений IDS/IPS (анг. Intrusion detection system/Intrusion prevention system) и их дальнейшее развитие системы класса NGIPS обеспечивают приемлемые решения для мониторинга и локализации сетевых аномалий. Данные решения входят в более обширный класс систем предупреждения инцидентов безопасности SIEM.

К основному функционалу SIEM систем относится:

- сбор, обработка, анализ инцидентов безопасности;
- анализ рисков безопасности;
- принятие эффективных методов по защите информации;
- обнаружение аномалий сетевого трафика, возможных вторжений;
- прогнозирование и поиск возможных уязвимостей;
- выявление возможного источника атаки;
- формирование онтологий событий сетевых вторжений;
- формирование принципов администрирования сетевого оборудования.

В отличие от сетевых экранов указанные системы могут просматривать содержимое пакетов, что повышает возможности системы обнаруживать «аномальные» пакеты. Принятие решения о пропуске или блокировке пакета ложится, в данном случае, на подсистему SIEM IDS/IPS. В таких системах очень важно задание правил сканирования входящего трафика. В случае большого количества ограничений на сканируемые пакеты, возможен рост ложных срабатываний, на предмет получения «аномальных» пакетов данных, что приводит к большому количеству формируемых алармистских сообщений администраторам сети, это ведёт к непроизводительной работе системы.

Очевидно, что формирование правил облегчающих или упрощающих прохождение нежелательных пакетов приводит к повышению вероятности проведения успешной атаки нарушителем. Как правило, операторы пакетных сетей передачи данных используют систему IDS/IPS в двух основных режимах работы. Первый режим характеризуется постоянным сканированием в реальном режиме времени поступающего трафика на сетевое оборудование, второй режим является инцидентным, в зависимости от поведения поступающего трафика формируются решения от системы IDS/IPS по изменению политики пропуска поступающего трафика в защищаемую сеть.

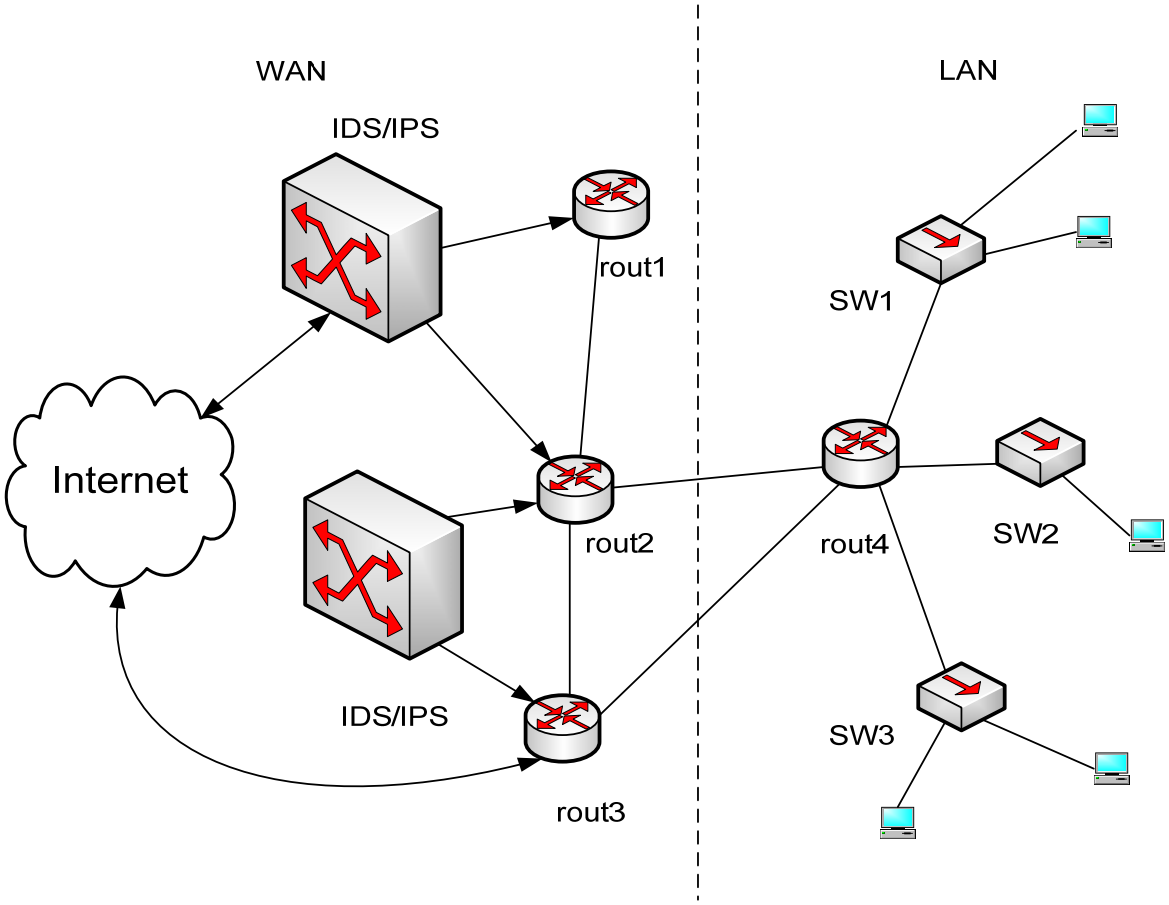
Возможны, два типа подключения IDS/IPS к действующему сетевому оборудованию, модули IDS/IPS ставятся между внешними сетями и защищаемой сетью, второй вариант – модули работают параллельно портам сетевого оборудования обслуживающего поступающий трафик в защищаемую сеть.

Дальнейшее развитие этих программных сенсоров получили системы NGIPS (англ. Next generation intrusion prevention system), преимуществом этой генерации платформ является, эффективная работа онлайн, наименьшим образом влияющая на скорость обработки данных. Использование единой платформы и децентрализованного управления позволяют выполнять контроль критически важных приложений и их мониторинг. NGIPS эффективно анализирует содержимое файлов, имеют возможность использовать внешние источники по базам уязвимостей (base vulnerability), а также использовать данные геолокации. В сетевой инфраструктуре IPS модули новой генерации могут использоваться в режиме IDS, например, анализируя поступающий трафик со SPAN портов маршрутизаторов, или используя технологию Network Tap.

Системы NGIPS имеют возможность поддержки протокола STP, способны маршрутизировать трафик по протоколам RIP, OSPF. NGIPS имеют возмож-

ность строить карту сети используя информацию со SPAN-портов, а также производят активное сканирование оборудования.

Приведём пример типового включения оборудования IDS/IPS в сети передачи данных, рисунок.



Пример типового включения IDS\IPS

Одним из самых популярных программных решений IDS/IPS является ПО Snort, это GNU/GPL программное обеспечение с открытым исходным кодом поддерживается компанией Sourcefire (входит в состав Cisco inc.).

Основные возможности Snort IDS/IPS:

– анализ трафика согласно правилам, установленным администратором защищаемой сети;

– использование эксплойтов (Shellcode);

– сканирование портов активного сетевого оборудования, операционных систем, пользователей сети;

– возможность определения атаки на WEB- сервисы;

– блокирование DoS/DDoS атак;

– возможность выявления атак на базы данных SQL, Oracle и. т. д;

– возможность WEB-фильтрации;

– блокирование атак по протоколам SNMP, NetBios, SMTP, ICMP и т.д.

В различных режимах работы Snort может блокировать трафик, анализировать трафик согласно правилам, вести журналирование, скрывать IP- адреса, выдавать ALERT -сообщения согласно ранее прописанным правилам администратора защищаемой сети. Возможности расширенных версий Snort позволяют создавать такие пользовательские конфигурации, которые полностью контролируют весь трафик, циркулирующий в сети передачи данных.

Например, в режиме анализа пакетов Snort просто читает пакеты, приходящие из сети, и выводит их на экран монитора администратора. Если ставится задача вывести на экран заголовки пакетов TCP/IP, необходимо прописать команду snort –v. Эта команда выводит заголовки IP и TCP, UDP, ICMP пакетов. Если есть потребность, кроме того, увидеть данные, содержащиеся в пакетах, используется команда: snort -vd. Для еще более подробного вывода, включающего заголовки кадров канального уровня, используется команда snort -vde.

Пример выводимой информация представлен ниже.

```
01/18-15:06:17.807867 0:E0:81:2F:FE:2C ->0:0:C:7:AC:2 type:0x800
len:0x5EA
66.179.164.20:22 ->24.136.161.188:62456 TCP TTL:64 TOS:0x10 ID:27401
IpLen:20 DgmLen:1500 DF
***A**** Seq: 0x50692152 Ack: 0xDD1E2B42 Win: 0x2180 TcpLen: 20
AA A8 5A 92 A7 BF DF 32 7D BF F7 7B 1B 5C 35 47
..Z....2}..{.\5G...mhA.S+....1B E0 C9 87 A8 71 91 EA D0 F4 1C 6C B4…
```

Система Snort анализирует трафик до тех пор, пока не поступит комбинация клавиш завершения захвата пакетов Ctrl-C. После нажатия Ctrl-C выводится отчёт о захваченных пакетах. Пример отчёта показан далее.

```
Snort received 74260 packets
Analyzed: 5923(7.976%)
Dropped: 68337(92.024%)
Breakdown by protocol:
TCP: 1602 (2.157%)
UDP: 4142 (5.578%)
ICMP: 0 (0.000%)
ARP: 6 (0.008%)
EAPOL: 0 (0.000%)
IPv6: 0 (0.000%)
IPX: 0 (0.000%)
ALERTS: 0
LOGGED: 0
PASSED: 0
Snort exiting
```

В версии Snort 2.3.0 RC1 интегрирована новая возможность, предупреждения вторжений (Intrusion Prevention System, IPS) snort_inline. Snort_inline получает пакеты не от libpcap, а от iptables, и с помощью новых типов правил помогает определить, что нужно сделать с пакетом – пропустить или уничтожить. Этот режим Snort называется встраиваемым.

Теоретически количество правил, задаваемых для систем подобных Snort, может быть неограниченное количество, определяемое администрацией сети связи. На практике количество правил ограничивается готовыми шаблонами известных атак, прописанных в онтологиях баз данных систем IDC/IPS.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Бирюков А. А. Информационная безопасность: защита и нападение. – 2-е изд. – М. : ДМК Пресс, 2017. – 434 с. – ISBN 978-5-97060-435-9. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/93278.

2. Шаньгин В. Ф. Защита компьютерной информации : учеб. пособие. – М. : ДМК Пресс, 2010. – 544 с. – ISBN 978-5-94074-518-1. – Текст : электронный // Электронно-библиотечная система «Лань» : [сайт]. – URL: https://e.lanbook.com/book/1122.

3. Snort [Электронный ресурс] / отдел «Documents». – Электрон. дан. – ЛА., 2019. – Режим доступа: https://www.snort.org/documents. – Загл. с экрана.