СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В КОРПОРАТИВНУЮ СЕТЬ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мурашко Е.А, Прокофьев С.В, Марычев Д.В.

Вишняков В.А., д.т.н., профессор

Системы предотвращения сетевых вторжений и выявления признаков атак на информационные системы уже достаточно длительное время используются как одно из необходимых средств защиты информационных систем. На сегодня системы предотвращения вторжений и атак обычно представляют собой программные или аппаратно-программные комплексы, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, а также анализируют эти события в поисках уязвимостей. Использование технологий виртуализации для построения системы предотвращения вторжений позволяет обеспечить как более рациональное распределение и использование физических ресурсов, так и упрощает администрирование всех компонентов системы защиты. В качестве средства обнаружения и предотвращения вторжений используется IDS/IPS Snort.

Система предотвращения вторжений (СПВ) (англ. Intrusion Protection System (IPS)) – программное или аппаратное средство, предназначенное для предотвращения попыток получения несанкционированного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть. В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, IPS служат механизмами мониторинга и наблюдения подозрительной активности. Типовая структура IPS включает:

8) Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
9) Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
10) Хранилище, в котором накапливаются первичные события и результаты анализа;
11) Консоль управления, позволяющая конфигурировать IPS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

Пример реализации СПВ с использованием технологий виртуализации представлен на рисунке 1:

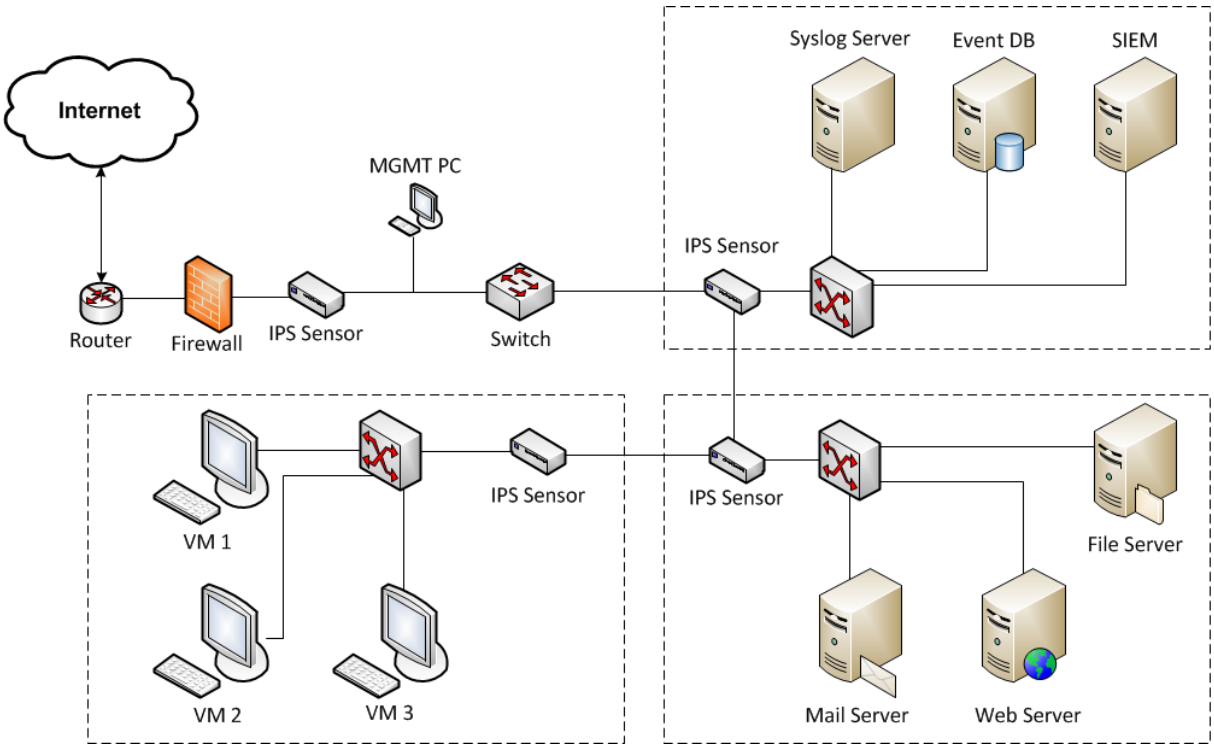

Рисунок 4 - Структура сети с применением различных типов СПВ

Штриховыми областями на схеме обозначены сервера виртуализации, на которых развёрнуты сенсоры сети, виртуальные коммутаторы, различные сервера и виртуальные рабочие станции.

Созданная виртуальная инфраструктура обладает следующими особенностями:

а) события с IPS-сенсоров сети собираются в базу данных на выделенном виртуальном сервере;

б) файлы журналов с сенсоров дублируются на Syslog-сервере;

в) для упрощения работы и анализа событий, принятых от сенсоров сети, развёрнута виртуальная система сбора и обработки данных о событиях информационной безопасности (SIEM).

Основные преимущества использования виртуальной инфраструктуры:

- уменьшение количества используемого физического оборудования;
- возможность быстрой миграции виртуальных машин и создания резервных копий;
- возможность перераспределения используемых виртуальными машинами ресурсов;
- возможность организации защиты как отдельных виртуальных машин, так и гипервизора в целом;
- упрощение администрирования и реконфигурации сети.

Основные недостатки применения виртуализации:

- высокая стоимость качественных серверов и корпоративных лицензий для использования виртуальных гипервизоров;
- риск потери данных и увеличение времени простоя виртуальных серверов или рабочих станций при выходе из строй одного из серверов виртуализации;
- необходимость повышения квалификации сотрудников для работы с виртуальной инфраструктурой;
- необходимость сокрытия факта использования виртуальных средств от обнаружения злоумышленником.

Неизбежный рост количества всевозможных угроз сетевой безопасности ставит всё новые задачи для специалистов по информационной безопасности и сетевых администраторов для предотвращения утечки важной информации и поддержания жизнеспособности критических активов в корпоративной сети. Внедрение технологий виртуализации является залогом успешного развития корпоративных сетей и улучшением их средств защиты.

Список использованных источников:

1. Кёртис, А. Real-time Intrusion Detection Systems. / А. К. Кёртис, Дж. Хамфрис. – Техас : Department Of Computer Science, 2008 – 20 с.

2. Вишняков, В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения / В. А. Вишняков. – Минск : Белорусская государственная академия связи, 2016. – 276 с.

3. Национальный открытый университет [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/.

4. Dave Mishchenko. VMware ESXi: Planning, Implementation, and Security.

5. Бэйкер, Э. Р. Snort IDS and IPS Toolkit. / Э. Р. Бэйкер, Дж. Эслер. – Берлингтон : Syngress, 2007. – 766 с.

6. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства. / В.Ф. Шаньгин. – Москва : ДМК Пресс, 2010. – 544 с.

7. BYTE/Россия. Системы обнаружения вторжений [Электронный ресурс]. – Режим доступа : https://www.bytemag.ru/.