СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

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

Мурашко Е.А, Марычев Д.В, Петкевич Д.А.

Вишняков В.А., д.т.н., профессор

Системы обнаружения сетевых вторжений и выявления признаков атак на информационные системы уже достаточно длительное время используются как одно из необходимых средств защиты информационных систем.Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие сети за последние годы значительно увеличилось, системы обнаружения атак (СОА) стали необходимым компонентом инфраструктуры большинства организаций. Использование виртуальной инфраструктуры для построения системы обнаружения 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/IPSSnort.

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть. СОВ всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности.В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, СОВ служат механизмами мониторинга и наблюдения подозрительной активности.Архитектура СОВ включает:

1) Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
2) Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
3) Хранилище, в котором накапливаются первичные события и результаты анализа;
4) Консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты.

Пример реализации СОВ с использованием виртуальной инфраструктуры представлен на рисунке 1:

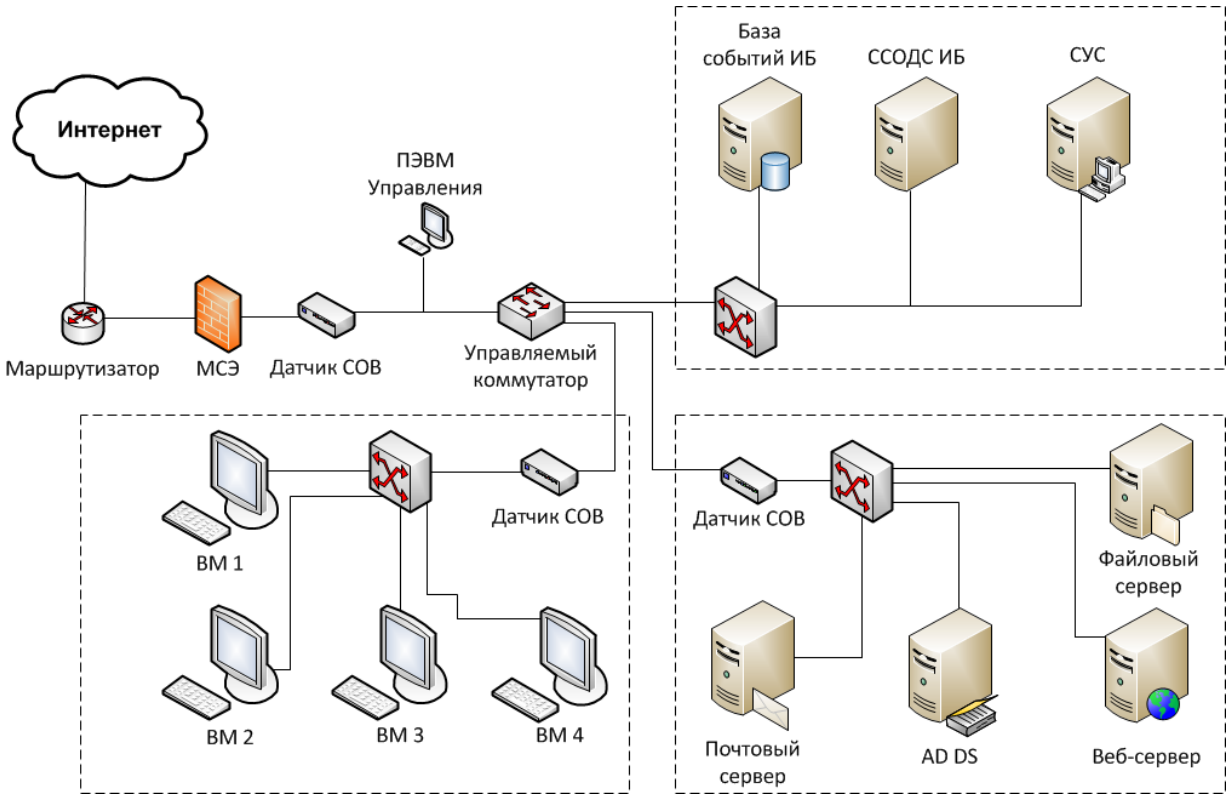

Рисунок 1 – Упрощённая структура сети с виртуальными и физическими СОВ

Штриховыми областями на схеме обозначены сервера виртуализации, на которых развёрнуты

датчики сети, виртуальные коммутаторы, различные сервера и виртуальные рабочие станции.

Созданная виртуальная инфраструктура обладает следующими особенностями:

а) события с датчиков СОВ собираются в базу данных на выделенном виртуальном сервере;

б) для упрощения работы и анализа событий, принятых от датчиков сети, развёрнута виртуальная система сбора и обработки данных о событиях информационной безопасности (ССОДС ИБ).

Основные преимущества использования виртуальной инфраструктуры:

- возможность быстрой миграции виртуальных машин и создания резервных копий;
- возможность перераспределения используемых виртуальными машинами ресурсов;
- уменьшение количества используемого физического оборудования;
- упрощение администрирования и реконфигурации сети;
- упрощение добавления новых рабочих мест и серверов.

Основные недостатки применения виртуализации:

- высокая стоимость серверов и корпоративных лицензий для использования виртуальных гипервизоров;
- необходимость повышения квалификации администраторов и пользователей для работы с виртуальной инфраструктурой;
- риск потери данных и увеличение времени простоя виртуальных серверов или рабочих станций при выходе из строй одного из серверов виртуализации.

Эволюция технологий виртуализации открывает новые возможности для обеспечения оптимальной и максимально удобной организации любых современных локальных сетей. Неизбежный рост сетевой инфраструктуры способствует всё большей популяризации использования средств виртуализации как для простых объектов, как-то рабочие места сотрудников предприятий, так и более сложных и комплексных информационных систем. Переход от исключительно физической инфраструктуры сети к комбинированной с виртуальной является залогом успешного развития локальных и глобальных сетей.

Список использованных источников:

1. 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.

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

3. Таненбаум, Э. Компьютерные сети. Пятое издание. / Э. Таненбаум, Д. Уэзеролл – Санкт-Петербург. : Питер, 2012. – 960 с.

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

5. David Chisnall, The definitive guide to the Xen hypervisor. ISBN-13: 978-0-13-234971-0.

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