Министерство образования Республики Беларусь

Учреждение образования

Белорусский государственный университет

информатики и радиоэлектроники

УДК 004.7

Хайнацкий

Максим Александрович

Разработка адаптивного метода и программы мониторинга корпоративной сети

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-45 80 02 «Телекоммуникационные системы и компьютерные сети»

_____

Научный руководитель

Давыдова Надежда Сергеевна

Кандидат технических наук, доцент

_____

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

Для современного уровня формирования информационного общества характерно интенсивное развитие технологий сетей post - NGN и концепции Интернета Вещей (ИВ). Происходит интенсивное развитие самоорганизующихся сетей связи, в которых абонентами являются не только люди, но и разнообразные автоматические устройства, которые осуществляют информационное взаимодействие друг с другом без прямого участия человека в рамках межмашинной коммуникации (M2M).

Для обслуживания и поддержания небольших локальных сетей требуются минимальные технические и программные средства. В представленной работе рассматриваются крупные сети операторов связи, состоящие из оборудования разных производителей, которые обслуживаются целым штатом инженеров и географически разнесены по разным городам и странам (MAN, WAN). Такие сети требуют методов комплексного управления инфраструктурой с целью понимания происходящих в них процессах.

Автором проведен анализ основных проблем, с которыми сталкиваются технические специалисты при обслуживании сети передачи данных, на примере сети провайдера ЮНЕТ. В результате чего были выделены основные характеристики сети, которые необходимо учитывать при разработке эффективных систем мониторинга и управления корпоративной сетью. К ним можно отнести:

1. Информационная сложность системы безопасности и сети.
2. Недостаточная эффективность средств обнаружения, определения приоритетов и выработки ответных действий в отношении атак и сбоев.
3. Повышенная сложность, скорость распространения и стоимость ликвидации последствий сетевых атак.
4. Необходимость соблюдения норм соответствия и требований по отчетности.
5. Квалификация разного уровня у отделов технической поддержки сети
6. Разнообразие оборудования различных производителей
7. Незнание топологии сети специалистами не технических отделов
8. Разные технологии подключения пользователей (Ethernet, LTE)

Таким образом, актуальным является разработка адаптивного метода, который сможет решить задачи оперативного сбора информации и эффективного контроля за текущим состоянием сети в интерактивном виде, что позволит ускорить выработку ответных действий при сетевых отказах для пользователей. Не менее актуальной является разработка проактивного алгоритма мониторинга корпоративной сети для устранения некоторых

инцидентов в сети до их наступления. Это позволит нивелировать эффект человеческого фактора, увеличит надежность, понизит информационную сложность.

Цель работы

Целью диссертационной работы является разработка и внедрение адаптивного метода и программы мониторинга корпоративной сети

Задачи работы

Для решения поставленной цели были выделены следующие задачи:

1. Обзор существующих систем и методов мониторинга сети.
2. Выявление основных критических изменений сети, реагирование на которые возможно осуществлять с помощью адаптивных средств систем мониторинга.
3. Разработка алгоритма на основе протокола snmp, который позволит оперативно выявлять участки сети, в которых возникла повышенная нагрузка и оперативно устранять при помощи адаптивных средств самой программы, либо при помощи уведомления ответственного персонала
4. Разработка эффективного метода мониторинга инфокоммуникационной сети, способного адаптироваться к любым условиям и изменениям сети.
5. Разработка метода реагирования на атаки типа “Отказ в обслуживании”
6. Разработка программных средств мониторинга и анализа телекоммуникационных сетей
7. Апробация предложенного метода и программных средств на базе корпоративной сети ООО «Объединенные сети»

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Он заключается в практическом определении технических характеристик и проблем систем мониторинга корпоративных сетей. Автором предложен алгоритм работы программ, входящих в комплекс проактивной системы мониторинга, для автоматического реагирования системой на сетевые инциденты. Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились совместно с научным руководителем Н.С. Давыдовой. В апреле 2018 года магистрант был

награжден почетной грамотой министерства связи и информатизации, за вклад в развитие связи в Республике Беларусь.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В начале работы осуществляется анализ существующих программ, приводятся теоретические основы построения сетевой инфраструктуры, основных протоколов, использующихся для мониторинга сетей.

Рассмотренные в главе системы мониторинга и управления компьютерными сетями включают как бесплатные решения, так и предложения от крупных производителей ПО и оборудования, конечную стоимость которых определить не представляется возможным. Можно сделать вывод, что система Cisco MARS позволяет в наиболее полном объеме решать задачи, с которыми сталкиваются администраторы крупных сетей за счет следующих решений:

1. Интеграция в сеть интеллектуальных функций для повышения эффективности механизма корреляции сетевых аномалий и событий безопасности.
2. Визуализация подтвержденных нарушений безопасности и автоматизация их расследования.
3. Отражение атак за счет использования всех преимуществ существующей инфраструктуры сети и безопасности.
4. Мониторинг конечных узлов, сети и операций службы безопасности для обеспечения соответствия нормативным документам.

Наиболее привлекательными решениями из распространяемых по лицензии свободного ПО являются системы Nagios и Zabbix. В них реализованы основные необходимые модуля, отвечающие требованиям модели FCAPS, такие как мониторинг состояния хостов (загрузка процессора, использование диска, системные журнал), отправка оповещений в случае возникновения проблем со службой или хостом, возможность определять иерархии хостов. Однако в данных системах нет возможности отображения на карте местности расположения оборудования, за исключением нескольких версий свободно распространяемых дополнений, написанных скорее обычными пользователями, которым не хватало данного функционала. Пример – система Zabbix Imap, которая в полной мере не отвечает требованиям FCAPS и не поддерживается разработчиком с 2015 года. Кроме того, уже существующие встроенные модули, рисующие топологию сети, достаточно громоздки и трудны в восприятии и не делают этого с привязкой к реальной карте местности, из-за чего понижается их информативность.

В главе 2 рассматриваются вопросы структурного состояния объекта исследования. Описывается оборудование сети провайдера, иерархическая модель сети. Так же рассматриваются основные сервисы, которые функционируют в сети и перечислено оборудование, при помощи которого они функционируют. Представлена схема организации сети провайдера UNET.

Глава 3 полностью посвящена разработке адаптивного метода мониторинга корпоративной сети. Выделяются основные компоненты разрабатываемой системы. В разделе 3.1 описывается общая структура системы мониторинга корпоративной сети и основные компоненты, такие как база данных, модуль сбора данных с устройств, модуль отображения статуса хостов сети, модуль балансировки внешних каналов интернет, модуль защиты от распределенных атак типа «отказ в обслуживании», модуль отображения карты сети. Подраздел 3.2.1 содержит описание работы протокола SNMP и основных запросов, использующихся в протоколе для получения данных. Подраздел 3.2.2 содержит информацию о базах управляющей информации MIB. В разделе 3.3 приводится описание баз данных, СУБД MariaDB, система хранения InnoDB. В подразделе 3.3.1 описан этап логического проектирования БД, реляционные отношения сущностей, а также их атрибуты. Приведено описания 4-х таблиц реляционных отношений. В подразделе 3.2.2 представлен код создания таблиц на языке DDL. Раздел 3.4 содержит описание модуля отображения состояния хостов сети. Приведено описание веб интерфейса, а также mrtg графики используемых ресурсов на примере одного из устройств. В разделе 3.5 описан алгоритм балансировки внешних каналов провайдера, основываясь на механизмах протокола BGP и данных, полученных с устройств при помощи snmp и формулы по расчету коэффициента использования сети. Раздел 3.6 содержит описание модуля по блокированию распределенных атак “отказ в обслуживании”, который основан на механизме community протокола bgp и контроле количества пакетов в секунду для каждого из пользователей. Раздел 3.7 содержит описание принципа работы модуля карты сети, протокола LLDP, описание на примере оборудования “D-Link” настройки LLDP на коммутаторах, для сбора данных, необходимых для построения связей на карте между устройствами.

Глава 4 описывает результаты опробации метода и внедрения разработанных модулей в сеть провайдера. Раздел 4.1 описывает внедрение модуля защиты от распределенных атак «отказ в обслуживании» в сеть провайдера. Рассматриваются этапы внедрения, представлен пример смоделированной атаки на один из адресов провайдера. Так же рассматривается возможность ручного блокирования, атакуемого ip созданными в рамках работы инструментами. Раздел 4.2 содержит примеры внедрения модуля балансировки внешних каналов интернет. Модуль 4.3

содержит данные, по внедрению карты сети с отображением оборудования на основе gps координат. Рассматривается функционал данного модуля.

ЗАКЛЮЧЕНИЕ

Результаты выполненной диссертационной работы:

– Выполнен анализ существующих систем мониторинга сетевой инфраструктуры

– Проанализированы возможные инструменты для создания адаптивного метода и программы мониторинга сетевой инфраструктуры;

– Разработан алгоритм модулей программы, для автоматизации реагирования на некоторые сетевые инциденты;

– Осуществлена реализация базы данных сущностей экосистемы мониторинга;

– Внедрены в сеть провайдера UNET модули по защите от распределенных атак “отказ в обслуживании”, модуль отображения карты сети, модуль балансировки внешних каналов интернет, модуль сбора данных с устройств.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Хайнацкий, М. А. Разработка адаптивного метода и программы мониторинга корпоративной сети / М. А. Хайнацкий // Инфокоммуникации: материалы 54-й научной конференции аспирантов, магистрантов и студентов, Минск, 23–27 апреля 2018 г. – Минск: БГУИР, 2018. – С. 68.