УДК 004.056

РАЗРАБОТКА СЦЕНАРИЕВ ПРИМЕНЕНИЯ МЕТОДОВ РАЗВЁРТЫВАНИЯ СИСТЕМ СЕТЕВОЙ БЕЗОПАСНОСТИ

Волхонская Е.Е.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: lizaveta5.6@mail.ru*
Чупринина А.С.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: anna.chuprinina.02@mail.ru*
Падучих Д.В.[1]
[1]*ФГБОУ ВО «Самарский государственный технический университет», Самара, e-mail: dasha-oleinikova2002@mail.ru*

При разработке технологических процессов и настройки систем их автоматизации требуется учитывать большое количество параметров. Автоматизированные системы состоят из большого количества взаимосвязанных подсистем, каждая из которых выполняют собственную функцию. Функции автоматизированных систем предусматривают большой спектр возможностей, каждая из которых реализуется специфическими программными и техническими комплексами, специализированными на решении определённого рада задач. Сетевая безопасность необходима и обязательна для любых систем. В данной статье будут рассмотрены анализ типичных условий развертывания систем сетевой безопасности, в том числе развертывание нескольких копий активных средств безопасности для обработки трафика в современных высоконагруженных сетях 40G/100G, безопасное развертывание нескольких активных средств безопасности последовательно, поддержка отказоустойчивых сетевых конфигураций и активных систем информационной безопасности.

Ключевые слова: автоматизированные системы, трафик, активные средства, информация

DATA MODELS IN THE DESIGN OF DATABASES OF AUTOMATED SYSTEMS

Volkhinskaya E.E.[1]
[1]*Samara State Technical University, Samara, e-mail: lizaveta5.6@mail.ru*
Chuprinina A.S.[1]
[1]*Samara State Technical University, Samara, e-mail: anna.chuprinina.02@mail.ru*
Paduchikh D.V.[1]
[1]*Samara State Technical University, Samara, e-mail: dasha-oleinikova2002@mail.ru*

When developing technological processes and configuring their automation systems, it is necessary to take into account a large number of parameters. Automated systems consist of a large number of interconnected subsystems, each of which performs its own function. The functions of automated systems provide a wide range of capabilities, each of which is implemented by specific software and technical complexes specialized in solving a certain set of tasks. Network security is necessary and mandatory for all systems. This article will review the analysis of typical conditions for the deployment of network security systems, including the deployment of multiple copies of active security tools for traffic processing in modern high-load 40G/100G networks, the safe deployment of multiple active security tools sequentially, support for fault-tolerant network configurations and active information security systems.

Keywords: automated systems, traffic, active means, information

Анализ типичных условий развёртывания систем сетевой безопасности

Активные инструменты делают больше, чем просто отслеживают трафик, они также могут управлять им. Активные средства вмешиваются в информационный обмен, фильтруя либо блокируя его в части вредоносной составляющей. Внедрение активных инструментов создаёт риски в доступности сети: если такие инструменты теряют питание или выходят из строя, то связь теряется на всём сегменте сети.

В данном разделе будут рассмотрены реальные ситуации и методы применения в них активных средств обеспечения безопасности. [1]

Развёртывание нескольких копий активных средств безопасности для обработки трафика в современных высоконагруженных сетях 40G/100G

В настоящее время широко распространяются стандарты 40G/100G. Производители активных средств безопасности стараются не отставать и предлагают высокопроизводительные инструменты для обеспечения защиты сетей данных стандартов. К сожалению, далеко не все предлагаемые современные инструменты могут обработать трафик высоконагруженных сетей стандартов 40G/100G. А те немногие, которые способны, имеют высокую стоимость и делают это с ограничениями. [2]

Задача: Сеть компании построена по стандарту 40G. Существующая система NGFW имеет интерфейсы 40G, но её производительности хватает только при нагрузке в сети до 30%. При повышении нагрузки в сети установленная NGFW уже не справляется и начинает терять трафик. Необходимо внедрить решение, которое будет обеспечивать работоспособность сети с использованием существующей активной системы NGFW и минимально возможными инвестициями.

На рисунке 1 представлено схематичное изображение поставленной задачи.

Рисунок 1 – Схематичное изображение задачи 1

Решение: Для решения данной задачи необходимы: брокер сетевых пакетов и дополнительная единица NGFW (в некоторых случаях даже менее производительная). Существующую и вновь приобретённую NGFW нужно подключить к брокеру сетевых пакетов, который, в свою очередь, подключить через Bypass к сети компании. Пакетный брокер будет балансировать получаемый из сети трафик на входы NGFW с сохранением целостности сессий и агрегировать трафик с выходов NGFW для дальнейшей передачи. Таким образом, нагрузка будет равномерно распределяться на две системы NGFW, что позволит поддерживать необходимую пропускную способность и быстродействие сети компании. [2]

На рисунке 2 представлено схематичное изображение решения поставленной задачи.

Рисунок 2 – Схематичное изображениерешения задачи 1

Безопасное развёртывание нескольких активных средств безопасности последовательно

Многие компании для достижения более глубокой защиты корпоративной сети последовательно развёртывают несколько активных средств безопасности. Таким образом, прежде чем трафик из интернета попадёт в корпоративную сеть, он должен пройти через системы IPS, Firewall, SWG и др. и получить разрешение на дальнейшее распространение по сети. Для минимизации рисков простоя сети компании нуждаются в эффективном и безопасном способе последовательного развёртывания активных средств ИБ. [3]

Задача: В компании, в сетевой инфраструктуре которой развёрнута система межсетевого экрана, планируется внедрить активные системы IPS и Anti-DDoS. При этом необходимо обеспечить бесперебойность работы сети при выходе из строя средств ИБ.

На рисунке 3 представлено схематичное изображение поставленной задачи.

Рисунок 3 – Схематичное изображение задачи 2

Решение: Для обеспечения бесперебойной работы сети наиболее эффективным вариантом будет подключение активных средств безопасности к сети через Bypass и брокер сетевых пакетов. В таком случае пакетный брокер будет маршрутизировать трафик через каждую последовательно подключённую активную систему, и если какая-либо система выйдет из строя, то брокер исключит её из последовательности. Таким образом, простоя сети не происходит, а инфраструктура по обеспечению информационной безопасности продолжает функционировать. В свою очередь, Bypass, при выходе из строя брокера сетевых пакетов, позволит сохранить целостность сети путём исключения последнего из схемы соединения.

На рисунке 4 представлено схематичное изображение решения поставленной задачи.

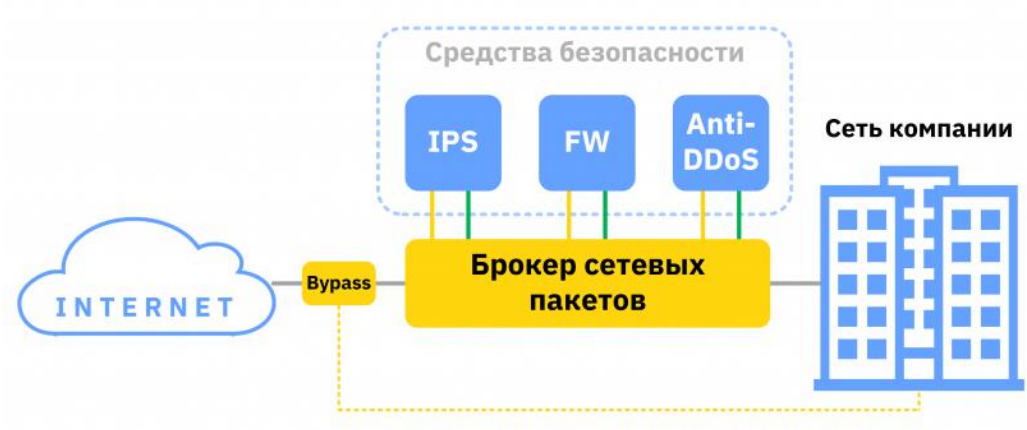

Рисунок 4 – Схематичное изображениерешения задачи 2

Поддержка отказоустойчивых сетевых конфигураций и активных систем информационной безопасности

Компании не могут себе позволить длительные периоды простоя активных систем информационной безопасности в случае их отказа. Поэтому специалисты часто прибегают к использованию отказоустойчивых схем, включающих несколько однотипных групп активных систем ИБ.

Отказоустойчивые сетевые архитектуры требуют избыточных компонентов сетевой инфраструктуры и дополнительных единиц активных средств ИБ. Чтобы избыточность свести к минимуму и в то же время обеспечить максимальную отказоустойчивость, необходимо проектировать сеть с использованием брокера сетевых пакетов и Bypass. [4]

Задача: В компании поставлена задача по организации отказоустойчивой конфигурации сети с активными средствами ИБ. Необходимо обеспечить бесперебойное функционирование системы ИБ в случае отказа группы систем и/или одного из элементов группы. Построенный сегмент активных средств ИБ не должен влиять на работоспособность общей сетевой инфраструктуры компании. Также требуется предусмотреть возможность дальнейшей масштабируемости и повышения производительности активных систем ИБ без изменения общей конфигурации сети.

На рисунке 5 представлено схематичное изображение поставленной задачи.

Рисунок 5 – Схематичное изображение задачи 3

Решение: Все требования поставленной задачи выполняются с помощью использования брокера сетевых пакетов и Bypass для подключения активных средств ИБ. Такое решение позволит уменьшить избыточность компонентов сетевой инфраструктуры, а также обеспечить более высокую отказоустойчивость системы. Брокер сетевых пакетов может эффективно маршрутизировать трафик как через каждый последовательно подключённый активный инструмент, так и через группу активных инструментов с балансировкой нагрузки.

Балансировка нагрузки позволяет равномерно распределять трафик между отдельными инструментами безопасности, тем самым обеспечивая их оптимальную загрузку и повышая отказоустойчивость сети. Если какой-либо инструмент выходит из строя, то брокер сетевых пакетов исключает его из последовательности и балансирует нагрузку на оставшиеся рабочие средства безопасности. Использование Bypass в данном случае аналогично первому кейсу и, при выходе из строя брокера сетевых пакетов, позволит сохранить целостность сети путём исключения последнего из схемы соединения. Подключение активных средств безопасности через брокер сетевых пакетов также позволяет осуществлять дальнейшую масштабируемость и внедрение новых систем ИБ с минимальными затратами и простой реализацией. [5]

На рисунке 6 представлено схематичное изображение решения поставленной задачи.

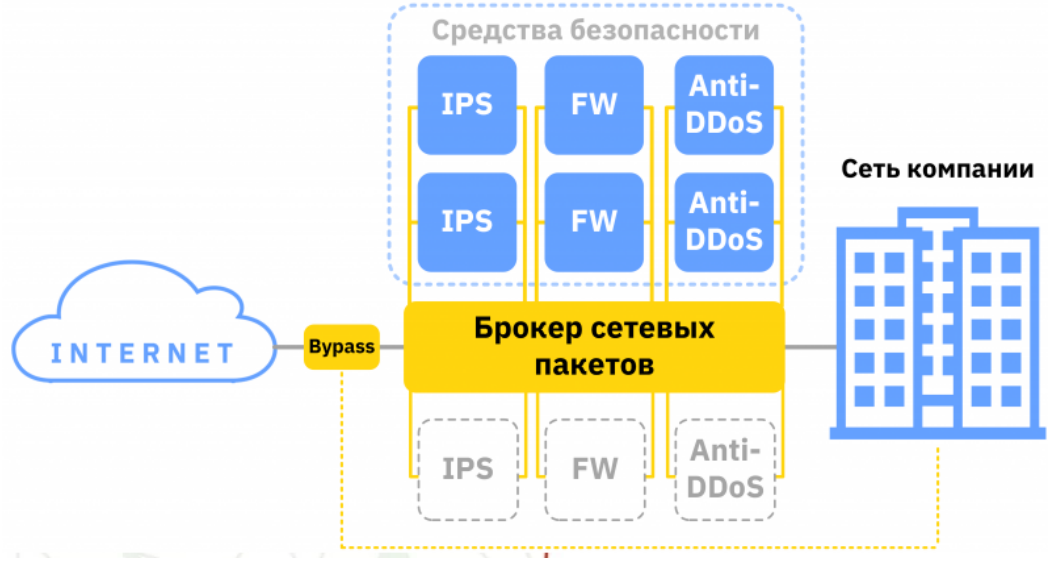

Рисунок 6 – Схематичное изображение решения задачи 3

Список литературы:

1. Пассивные и активные методы и способы защиты каналов утечки информации [Электронный ресурс]//studfile// URL:https://studfile.net/preview/5868802/

2. Активные методы защиты информации от утечки по электромагнитному и акустическому каналам [Электронный ресурс]//Helpiks// URL: https://helpiks.org/8-62604.html

3. Обеспечение сетевой безопасности совместно с брокерами сетевых пакетов. Часть вторая. Активные средства безопасности [Электронный ресурс]// Хабр// URL: https://habr.com/ru/company/dsol/blog/551124/

4. Пассивные и активные средства защиты информации[Электронный ресурс]// Техника для спецслужб // URL:http://www.bnti.ru/showart.asp?aid=547&lvl=04.03.

5. Классификация пассивных и активных способов и средств защиты информации, обрабатываемой техническими средствами. [Электронный ресурс]// Техника для спецслужб // URL:https://cyberpedia.su/5x7b23.html