ПРОЕКТИРОВАНИЕ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СЕТИ КОМПАНИИ

О.Ф. Ковалёв, Т.Ф. Шмигирёв

БГУ, Минск, Беларусь
E-mail: OKovaliov@gmail.com

Компаниям, имеющим несколько филиалов, требуется организовать корпоративную информационную сеть для общей работы с базами данных и документами, позволяющую сотрудникам общаться и обмениваться данными, а также обеспечить безопасную передачу этих данных и защиту от проникновения извне. В статье представлено эффективное проектирование и тестирование корпоративной сети предприятия с учётом требований к безопасности, скорости сходимости и масштабируемости.

Ключевые слова: корпоративная информационная сеть; маршрутизатор; динамическая маршрутизация; OSPF; BDP; межцеховой экран; ContainerLab.

ВВЕДЕНИЕ

Когда компания небольшая и имеет только один офис, есть возможность проложить физически единую сеть. Однако в случае наличия нескольких офисов даже в пределах одного города, не говоря уже о разных городах и странах, корпоративная информационная сеть (КИС) становится бизнес-инструментом решения для организации и оптимизации трёх бизнес-процессов:

1. Совместная работа с информационными ресурсами. Филиалы, их отделы и сотрудники имеют доступ к единой базе данных, предоставляется возможность единого документооборота и доступа к нему сотрудников.

2. Передача информации. Так как в КИС передаются конфиденциальные данные компании, обеспечение защиты информации важный аспект проектирования КИС. Защита корпоративных сетей обеспечивается как аппаратно, так и программно: межсетевые экраны, виртуальные частные сети, антивирусное программное обеспечение, авторизация и аутентификация, системы обнаружения вторжений (*IDS*) и предотвращения вторжений (*IPS*).

3. Деловое общение. В рамках КИС сотрудники, используя специальные программы, могут общаться в чатах, обмениваться файлами и папками, проводить видеоконференции.

Основными свойствами КИС являются:

1. Топология – тип и структура связей между узлами сети.

2. Пропускная способность – возможности сети передавать данные с заданной скоростью.

3. Масштабируемость – создание нового отдела или филиала, например – подключение новых компьютеров должно происходить без значительных изменений в инфраструктуре [1].

Учёт современных требований к безопасности, скорости сходимости и масштабируемости стал важнейшим моментом при проектировании и тестировании корпоративной информационной сети.

ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ

Топология сети – это , по сути, конфигурация графа, в котором вершинами являются узлы сети (маршрутизатор/компьютер), а рёбрами – связи между вершинами. Зачастую рассматривается не физическая топология компьютеров или других устройств, а логическая, при которой определены пути данных между устройствами в сети. Пути могут задаваться административно – статические маршруты, или – определяться при помощи протоколов маршрутизации – динамическая маршрутизация [2].

Статическая маршрутизация имеет целый рад недостатков, среди которых основным является плохая масштабируемость: добавление (N+1)-ой сети потребует добавления 2·(N+1) новых записей о маршрутах.

При динамической маршрутизации таблица маршрутизации заполняется и редактируется программно (в *UNIX*-системах подобные программы называются демонами маршрутизации).

МОДЕЛИРОВАНИЕ СИСТЕМЫ И ЕЁ ТЕСТИРОВАНИЕ

На виртуальном клиенте Linux была развернута лаборатория с помощью утилиты Containerlab, в нее были загружены виртуальные образы ПО межсетевых экранов, маршрутизаторов, серверов и пользовательских станций. Количество межсетевых экранов, соответствовало количеству филиалов, включая центр обработки данных (ЦОД). Отличие от реальной системы лишь в том, что применяется виртуальные оборудование, моделирование при помощи которого эффективнее и дешевле использования реального оборудования: отсутствие затрат на доставку, наладку и поддержку, не требуется место для хранения на сервере, а также лёгкость резервирования.

На границе каждого филиала был настроен Network Address Translation (межсетевые экраны переведены в режим NAT), – механизм, позволяющий преобразовывать IP-адреса транзитных пакетов для удобства и разграничения.

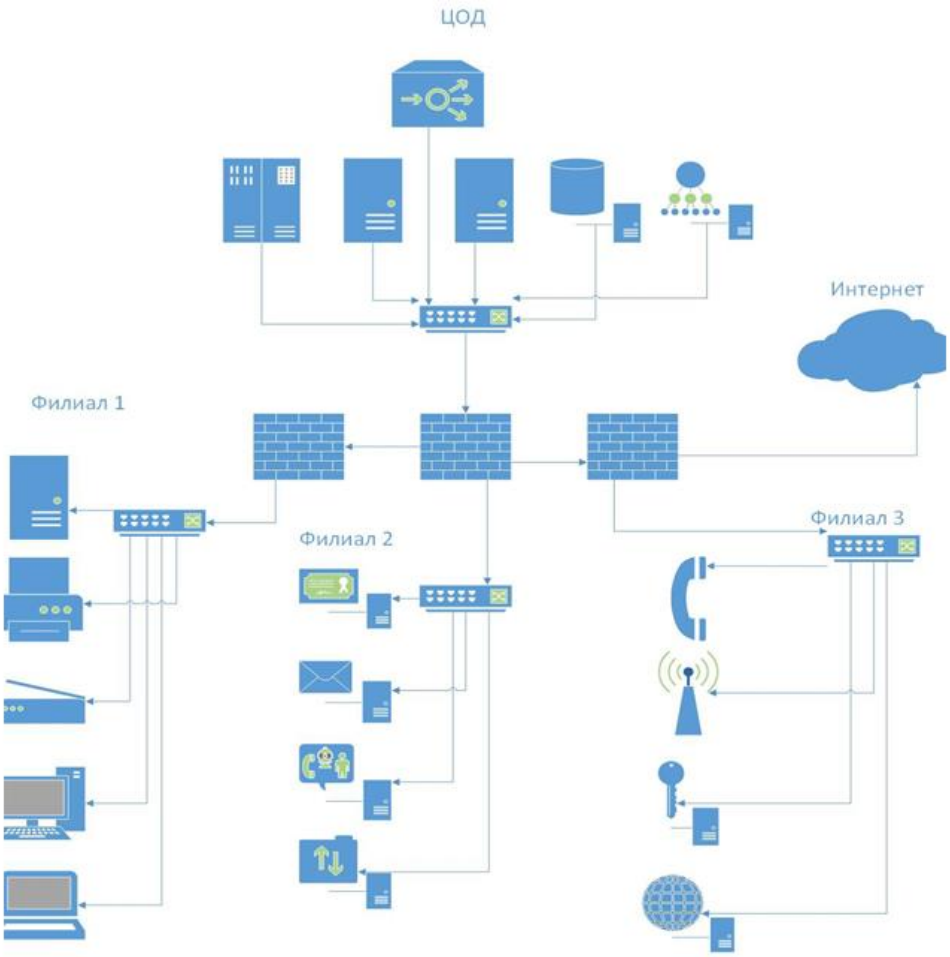

Схема смодлеированной корпоративной информационной сети

Маршрутизаторы были настроены так, чтобы внутренняя сеть предприятия функционировала по протоколу внутренней динамической маршрутизации OSPF (Open Shortest Path First – протокол, который составляет карту соседей и прокладывает самый короткий путь из одной точки в другую), а внешняя – по протоколу внешней динамической маршрутизации BGP (Border Gateway Protocol – протокол, обеспечивающий маршрутизацию между автономными системами).

В настоящее время наиболее популярный подход это создание OSPF-зон, между которыми настраиваются статические маршруты [3]. Наша модель включает использование BGP-протокола для организации динамической маршрутизации между OSPF-зонами, а фактически, между несколькими локальными сетями в рамках одной корпоративной информационной сети, что повышает масштабируемость и уменьшает вероятность выхода из строя сети.

В рамках протокола BGP имеется механизм BGP Community, представляющий 32-битовое значение, прикрепляемое к одному или нескольким маршрутам. Такая маркировка помогает при управление трафиком (возможно указать какой трафик должен быть направлен через конкретные маршруты), группировке маршрутов (создаются группы маршрутов с одинаковыми характеристиками, что упрощает управление).

В каждом филиале трафик перенаправлялся в межсетевой экран, который работал в прозрачном режиме и защищал внутреннюю сеть от вредоносных файлов. На межсетевых экранах были настроены политики для контроля потока трафика, логирование для выявления возможных проблем, внутренние анализаторы для составления статистики и визуализации контроля трафика и обновлена антивирусная база данных, а также настроена маршрутизация для нормального функционирования в системе. Был настроен DNS сервер 8.8.8.8 (Google). Для автоматизации назначения *IP*-адресов в локальной сети используется *Dynamic Host Client Protocol* с внутренним пулом адресов для автоматической их выдачи соответствующим MAC адресам. На сервере была настроена служба каталогов Active Directory, было создано несколько учётных записей при помощи протокола доступа к каталогам LDAP (*Lightweight Directory Access Protocol*), а также настроен вход по токенам (ключам/тикетам/билетам) через систему аутентификации Kerberos.

ВЫВОДЫ

Таким образом, моделирование корпоративной информационной системы включает проверку редистрибьюции двух протоколов динамической маршрутизации (OSPF и BGP) в системе, приближенной к реальной. Используя Eicar-файл, была протестирована безопасность системы, запись отобразилась в логах, файл заблокирован по всем протоколам (FTP, HTTP). По протоколам ICMP (ping) была проверена доступность и сходимость между конечными станциями. Также с помощью трассировки пути было проверено перенаправление трафика на межсетевой экран. С помощью инструментария Containerlab был создан сценарий высоконагруженности системы, сетевого шторма и DOS атаки.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Бройдо В.Л., Ильина О.П.* Архитектура ЭВМ и систем: учебник для вузов // 2 изд. Питер, 2021. С. 720.
2. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы // Питер, 2013. С. 944.
3. *Дибров М.* Сети и телекоммуникации. Маршрутизации в IP-сетях: учебник и практикум для академического бакалавриата // Москва: издательство Юрайт, 2024. С. 423.