МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»
Кафедра дискретной математики и информационных технологий

РЕАЛИЗАЦИЯ ДИНАМИЧЕСКОГО DNS–СЕРВЕРА НА ОПЕРАЦИОННОЙ СИСТЕМЕ LINUX ДЛЯ КОРПОРАТИВНОЙ СЕТИ ОРГАНИЗАЦИИ

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 421 группы
направления 09.03.01 — Информатика и вычислительная техника
факультета КНиИТ
Дегтярева Даниила Ильича

Научный руководитель
доцент, к. ф.-м. н. _____ В. А. Поздняков

Заведующий кафедрой
доцент, к. ф.-м. н. _____ Л. Б. Тяпаев

Саратов 2023

ВВЕДЕНИЕ

В современном мире корпоративные сети являются неотъемлемой частью бизнес-процессов организаций. Однако, с ростом числа устройств в сети и их динамической природой, возникает необходимость обеспечения эффективного управления IP-адресами в корпоративной сети. Для этого требуется использование динамического DNS-сервера. Это позволяет автоматизировать процесс обновления DNS-записей и упростить работу сетевых администраторов, что является важным аспектом в современных корпоративных сетях. Кроме того, динамический DNS-сервер обеспечивает безопасность и защиту от кибератак, что является необходимым условием для надежной работы сети.

Данная тема в настоящее время является актуальной по причине ухода многих иностранных разработчиков программного обеспечения, всвязи с чем более востребованным становится открытое программное обеспечение.

Целью данной выпускной квалификационной работы является реализация динамического DNS-сервера на операционной системе Linux для корпоративной сети организации.

Для достижения поставленной цели необходимо выполнить следующие задачи:

— Установить операционную систему CentOS Stream 8 на виртуальные машины и произвести начальную настройку;
— Изучить принцип работы DHCP-сервера;
— Реализовать DHCP-сервер на операционной системе Linux;
— Изучить принцип работы DNS-сервера;
— Реализовать динамический DNS-сервер на операционной системе Linux;
— Проверить работу DHCP- и DNS-серверов.

Теоретическая и/или практическая значимость бакалаврской работы. В данной работе, для реализации динамического DNS-сервера на операционной системе Linux, будет использоваться BIND - один из самых популярных DNS-серверов с открытым исходным кодом. Также будет использоваться DHCP-сервер для автоматического обновления DNS-записей на основе протокола DHCP. Кроме того, для проверки работоспособности динамического DNS-сервера будет использоваться клиентская машина.

Результаты данной работы могут быть использованы организациями

для упрощения процесса настройки и управления корпоративной сетью, а также для повышения безопасности и удобства работы с ней.

Структура и объем работы. Бакалаврская работа состоит из введения, трех глав, заключения, списка использованных источников. Общий объем работы - 39 страниц, из них 37 страниц - основное содержание, включая 48 рисунков, список использованных источников информации - 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первый раздел "Теоретические основы" посвящен основным понятиям и принципам работы DNS, информации касательно динамического DNS, протокола DHCP, основным понятиям об Firewalld, роли динамического DNS в корпоративной сети, операционной системе Linux как платформе для реализации динамического DNS-сервера.

DNS (Domain Name System) - это система, которая преобразует доменные имена в IP-адреса и наоборот. DNS позволяет пользователям использовать удобные для запоминания доменные имена вместо сложных числовых IP-адресов.

DNS-серверы содержат базу данных, которая хранит информацию о доменных именах и соответствующих им IP-адресах. Когда пользователь вводит доменное имя в адресной строке браузера, компьютер отправляет запрос на DNS-сервер, который возвращает соответствующий IP-адрес.

DNS-записи - это записи в базе данных DNS-сервера, которые содержат информацию о доменных именах и соответствующих им IP-адресах. Существуют различные типы DNS-записей, такие как A-записи, которые содержат IPv4-адреса, и AAAA-записи, которые содержат IPv6-адреса.

Далее рассматривался динамический DNS. Динамический DNS (DDNS) является механизмом, который позволяет динамически обновлять записи DNS, когда IP-адрес хоста изменяется. Это особенно полезно в случае использования динамических IP-адресов, которые могут меняться при каждой перезагрузке устройства или при изменении подключения к сети.

DDNS работает путем установления связи между DHCP-сервером, который выдает IP-адрес устройству, и DNS-сервером, который содержит запись DNS для этого устройства. Когда устройство запрашивает IP-адрес, оно также сообщает DNS-серверу свое имя хоста. DHCP-сервер в ответ сообщает DNS-серверу, что IP-адрес устройства был изменен. DNS-сервер обновляет свою запись DNS, чтобы соответствовать новому IP-адресу.

После этого был рассмотрен протокол DHCP. Протокол DHCP (Dynamic Host Configuration Protocol) используется для автоматической настройки IP-адресов, масок подсетей, шлюзов по умолчанию, DNS-серверов и других параметров сетевой конфигурации для компьютеров и других устройств в локальной сети.

Когда компьютер или другое устройство подключается к локальной сети, оно отправляет запрос на получение IP-адреса DHCP-серверу. DHCP-сервер отвечает на запрос, предоставляя IP-адрес и другие параметры сетевой конфигурации. Клиент сохраняет эту информацию и использует ее для подключения к сети.

DHCP также поддерживает функцию обновления IP-адресов, когда устройство меняет свое местоположение в сети или перезагружается. Когда устройство запрашивает новый IP-адрес, DHCP-сервер может предоставить тот же адрес, который был выдан ранее, чтобы сохранить сетевую конфигурацию устройства.

Далее были освещены основные понятия об Firewalld. Firewalld - это программа для управления брандмауэром в Linux. В брандмауэре определяются правила, которые служат фильтром между сетью и хостом, позволяя контролировать прохождение трафика в оба направления. Firewalld обеспечивает более простое и гибкое управление брандмауэром, чем предыдущее решение - iptables. Firewalld использует концепцию зоны безопасности и сервисов, что помогает упростить настройку и облегчить задачу управления брандмауэром.

В Firewalld зоны безопасности - это наборы правил, определяющие доверительность сетей. Каждая сеть ассоциируется с одной зоной. Например, входящие пакеты сети, которые имеются в зоне "домашняя имеют доступ к большему количеству сервисов, чем входящие пакеты сети из зоны "общественная". Управление зонами, доступными в брандмауэре, может осуществляться через интерфейс командной строки или графический интерфейс.

После этого отмечалась роль динамического DNS в корпоративной сети. Динамический DNS (DDNS) является важным инструментом для корпоративных сетей, которые используют динамические IP-адреса. DDNS позволяет автоматически обновлять DNS-записи, когда IP-адрес устройства изменяется, что упрощает управление сетью и повышает ее безопасность.

При использовании DDNS DNS-записи обновляются автоматически при изменении IP-адресов устройств в сети. Это позволяет предотвратить возможные атаки на сеть, связанные с изменением IP-адресов устройств.

Кроме того, DDNS обеспечивает надежную и стабильную работу сети, что позволяет избежать проблем, связанных с недоступностью устройств в

сети. При использовании DDNS устройства всегда будут доступны по имени домена, что упрощает их управление и обслуживание.

Далее рассматривалась операционная система Linux как платформа для реализации динамического DNS-сервера. Linux является свободной и открытой операционной системой, которая используется как на десктопах, так и на серверах. Она предоставляет пользователю полный контроль над системой и позволяет настраивать ее под свои потребности.

В ходе данной работы, для реализации динамического DNS-сервера, использовался дистрибутив CentOS Stream 8 - один из дистрибутивов Linux, который основан на Red Hat Enterprise Linux (RHEL) и предназначен для использования в качестве серверной платформы.

CentOS Stream 8 является отличной платформой для реализации динамического DNS-сервера благодаря своей стабильности, безопасности и производительности.

Второй раздел "Анализ требований к динамическому DNS-серверу для корпоративной сети" посвящен требованиям к динамическому DNS-серверу. Отмечаются функциональные и нефункциональные требования. К функциональным требованиям к динамическому DNS-серверу были отнесены:

1. Автоматическое обновление DNS-записей при изменении IP-адреса отдельных устройств в сети.
2. Возможность настройки прав доступа к DNS-записям для различных пользователей и групп.
3. Поддержка различных типов DNS-записей, таких как A, CNAME и других.
4. Обеспечение безопасности и защиты от кибератак.

В свою очередь, к нефункциональным требованиям отнеслись:

1. Производительность и масштабируемость.
2. Совместимость с другими сервисами и системами.
3. Гибкость настройки и конфигурации.

Третий раздел "Реализация динамического DNS-сервера на операционной системе Linux для корпоративной сети организации" посвящен непосредственно созданию и настройке динамического DNS-сервера, созданию и настройке DHCP-сервера, настройке firewalld и тестированию ра-

ботоспособности DDNS-сервера.

Для создания и настройки динамического DNS-сервера необходимо выполнить следующие задачи:

— Скачать и установить CentOS Stream 8 и VirtualBox;
— Создать необходимое количество виртуальных машин и настроить их;
— Выбрать программные решения для развертывания динамического DNS-сервера на базе CentOS Stream 8;
— Настроить DNS-сервер, DHCP-сервер и клиентскую машину.

Вначале описывается процесс создания и настройки виртуальных машин, а также установка на них операционной системы Linux версии CentOS Stream 8.

Далее следует настройка DNS- и DHCP-сервера на виртуальной машине. Для этого требуется установить следующие пакеты для работы сервреров:

— Bind, который является стандартным днс сервером;
— Dhcp-server для развертывания dhcp сервера;
— Network-scripts, необходимый для работы с сетевыми интерфейсами.

После установки необходимого ПО, настройка начинается с редактирования файла сетевых настроек узла. Требуется зафиксировать ip-адрес и адрес DNS, поскольку адрес будущего DNS-сервера в локальной сети должен оставаться неизменным.

Далее необходимо создать ключ dnssec для цифровой подписи DNS-записей. Это производится для защиты от атак, сервер будет использовать этот ключ для проверки подлинности запрашиваемой пользователем информации.

Для настройки DHCP-сервера необходимо открыть его конфигурационный файл и настроить DHCP зону, указав сеть, которую будет обслуживать данный DHCP-сервер, маску сети, ip-адрес шлюза, который будет использоваться клиентом, маску подсети, адрес DNS сервера, который будет использоваться клиентом и доменное имя.

Следующим шагом требуется настроить DNS сервер. Его настройка состоит из следующих пунктов:

— Настройка основного конфигурационного файла /etc/named.conf;
— Настройка файлов зон поддержки в каталоге /var/named;

— Настройка сетевого экрана.

В целом, в основном конфигурационном файле настраивается список сетей, в нашем случае, локальная и глобальные параметры, такие как расположение файлов ведения статистики днс сервера, и разрешение на получение запросов только из локальной сети.

В файле поддержки описываются общие настройки зоны, имя узла, тип сети, и типы записи. Для начала необходимо создать только статические записи, то есть записи об узлах со статическими адресами. В данной работе используются два узла с именами dserver.hkscorp.com и wserver.hkscorp.com. У dserver.hkscorp.com адрес статический, у wserver.hkscorp.com адрес динамический.

После этого требуется запустить службу DNS-сервера и DHCP-сервера, после чего необходимо снова открыть файл зоны поддержки и добавить в него запись об узле с динамическим адресом, указав ему предполагаемый IP-адрес.

Следующим шагом требуется перезапустить службу DNS-сервера и DHCP-сервера и снова открыть файл зоны поддержки. После открытия файла зоны поддержки, оказалось, что он был обновлен. У узла wserver.hkscorp.com был указан текущий IP-адрес.

Данный факт означает, что DDNS-сервер использует актуальный адрес и функционирует исправно.

Для того чтобы убедиться в работоспособности DDNS, проверим доступность узла с DDNS- и DHCP-серверами с клиентской машины с помощью команды "ping". Было отмечено, что пакеты доставлены успешно, их потерь нет.

Следующим шагом происходит настройка сетевого экрана – firewalld. Она начинается с его запуска и просмотра его текущего статуса. После запуска сетевого экрана, необходимо узнать, какая зона доверия используется по умолчанию. Далее требуется настроить активную зону, удалив ненужные сервисы с помощью команды “–remove-service=название сервиса” и добавив нужные сервисы с помощью команды “–add-service=название сервиса”. После проделанных действий с сетевым экраном, нужно проверить доступность DDNS-сервера и клиентской машины по их IP-адресам и хостовым именам при помощи команды “ping”.

ЗАКЛЮЧЕНИЕ

В ходе данной дипломной работы была рассмотрена тема реализации динамического DNS-сервера на операционной системе Linux версии CentOS Stream 8 для корпоративной сети организации. Основной целью была реализация динамического DNS-сервера на операционной системе Linux для корпоративной сети организации.

В результате выполнения поставленных задач были достигнуты следующие результаты:

— Установлена операционная система CentOS Stream 8 на виртуальные машины и проведена начальная настройка;
— Изучены принципы работы DHCP-сервера;
— Реализован DHCP-сервер на операционной системе Linux;
— Изучены принципы работы DNS-сервера;
— Реализован динамический DNS-сервер на операционной системе Linux;
— Проведена проверка работы DHCP- и DNS-серверов.

Выводы, которые можно сделать из проделанной работы, заключаются в том, что динамический DNS-сервер на операционной системе Linux является удобным и эффективным инструментом для управления IP-адресами в корпоративной сети. Он позволяет автоматизировать процесс обновления DNS-записей и упростить работу сетевых администраторов.

Основные источники информации:

1. Itwo Что такое виртуализация: [Электронный ресурс] URL: https://cloud.yandex (дата обращения: 20.05.2023)
2. Itwo Что такое виртуальная машина: [Электронный ресурс] URL: https://help.r servery-i-dc/vmware-virtualnyy-data-tsentr/sozdaniye-i-nastroyka-virtualnykh-mashin/chto-takoye-virtualnaya-mashina (дата обращения: 20.05.2023)
3. Itwo Обзор CentOS: версии дистрибутива и его преимущества: [Электронный ресурс] URL: https://selectel.ru/blog/centos/ (дата обращения: 20.05.2023)
4. Itwo Таненбаум Э.,Компьютерные сети, 4-е изд.,СПб.: 2002 (дата обращения: 20.05.2023)
5. Itwo Устанавливаем CentOS в VirtualBox: [Электронный ресурс] URL: https://lumpics.ru/installing-centos-on-virtualbox/ (дата обращения: 20.05.2023)
6. Itwo Настройка сети в CentOS и Rocky Linux: [Электронный ресурс]

URL: https://www.dmosk.ru/miniinstruktions.php?mini=centos-network (дата обращения: 20.05.2023)

7. Itwo Стивен Браун.,Виртуальные частные сети,М: Лори, 2001. (дата обращения: 20.05.2023)