

Давайте рассмотрим, как может выглядеть обеспечение безопасности сети с технической точки зрения

Клиент в браузере делает запрос на нашем сайте. Что может происходить по порядку:

1. DNS Защита

- **Инструмент:** DNS Firewall или DNS Security Extensions (DNSSEC)
- **Нужен для:** Фильтрации запросов на уровне доменных имен, для предотвращения DNS-спуфинга и перенаправления на вредоносные сайты.
- **Реализация:** Когда пользователь пытается получить доступ к вашему сайту, DNS Firewall сначала проверяет запрос. Если домен находится в "черном списке" или запрос кажется подозрительным, доступ будет заблокирован.

2. CDN Защита

- **Инструмент:** Content Delivery Network (CDN) с встроенными мерами безопасности.
- **Нужен для:** Ускорения загрузки ресурсов сайта и защиты от DDoS-атак.
- **Реализация:** Запрос сначала направляется на ближайший сервер CDN. Сервер может фильтровать трафик и снижать нагрузку на основной веб-сервер, обрабатывая статические ресурсы и отсеивая атаки DDoS.

3. Фаерволл WAF

- **Инструмент:** Web Application Firewall (WAF)
- **Нужен для:** Защиты веб-приложения от различных угроз на уровне приложения, таких как SQL-инъекции, XSS-атаки и другие.
- **Реализация:** После прохождения CDN, запрос направляется через WAF. WAF анализирует запрос на наличие подозрительного или вредоносного кода и, при обнаружении, блокирует его.

4. Балансировщик нагрузки

- **Инструмент:** Load Balancer

- **Нужен для:** Распределения входящего интернет-трафика по нескольким серверам.
- **Реализация:** После прохождения WAF, запрос направляется на балансировщик нагрузки, который распределяет его на один из фронтенд-серверов в зависимости от текущей нагрузки на каждый из них.

5. Фронтенд с HTTPS

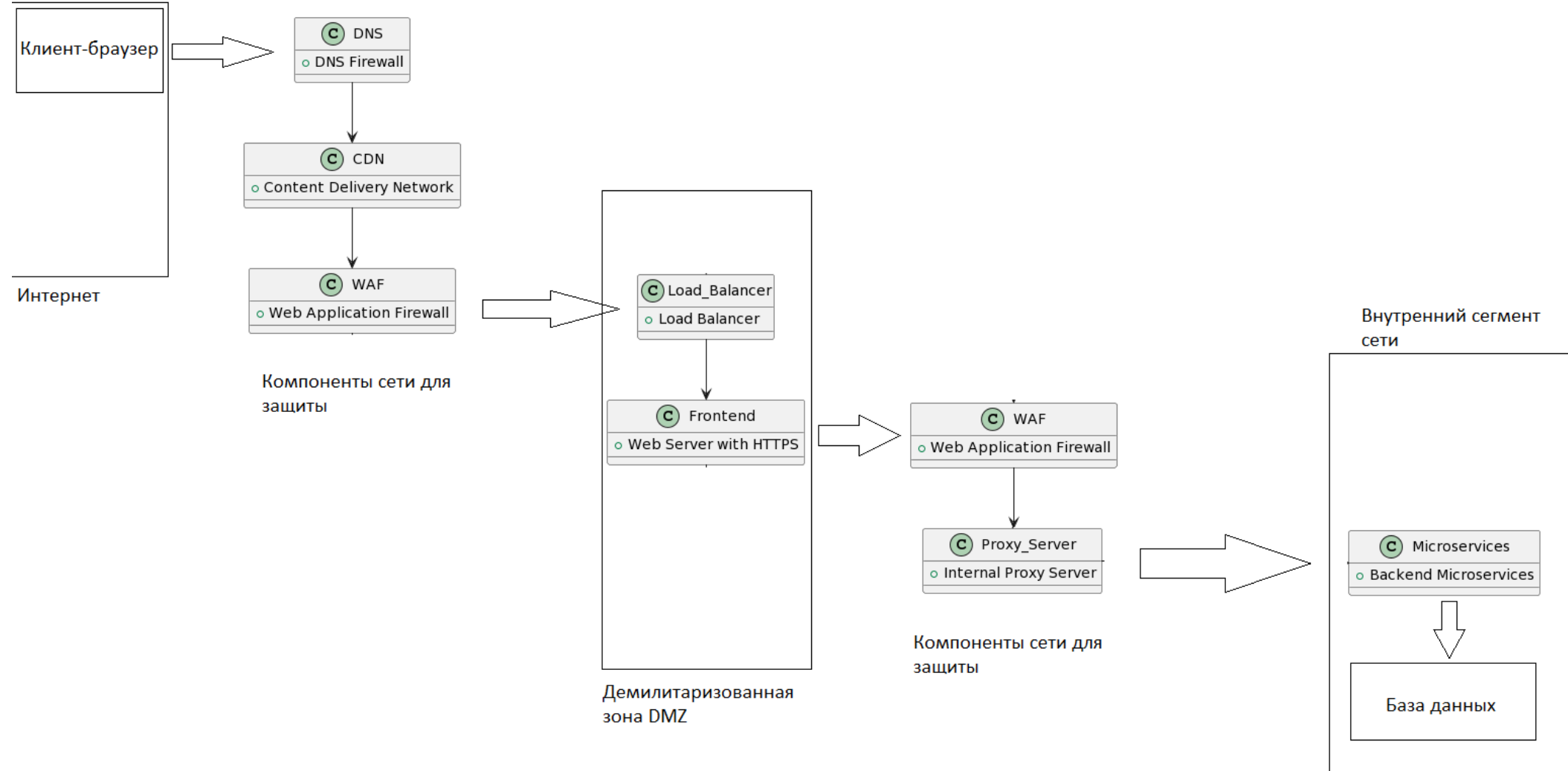
- **Инструмент:** Web Server с HTTPS
- **Нужен для:** Шифрования данных между клиентом и сервером. Отображается фронтенд в браузере клиента.
- **Реализация:** Балансировщик направляет запрос на фронтенд-сервер. Весь трафик шифруется с использованием HTTPS для защиты данных пользователя. Отображается фронтенд в браузере клиента.

6. Прокси-сервер для внутренней сети

- **Инструмент:** Внутренний прокси-сервер
- **Нужен для:** Фильтрации и проксирования запросов из фронтенда на бэкенд.
- **Реализация:** Фронтенд-сервер, получив запрос, направляет его через прокси-сервер. Прокси может проводить дополнительную фильтрацию и направлять запрос на соответствующий микросервис во внутренней сети.

7. Сегментация сети и микросервисы

- **Инструмент:** Внутренние микросервисы и сегментация сети
- **Нужен для:** Изоляции различных частей приложения для улучшения безопасности и производительности.
- **Реализация:** Прокси-сервер направляет запрос на соответствующий микросервис в сегментированной сети. Сегментация помогает изолировать потенциальные угрозы и облегчает масштабирование.



Это общая схема со всеми компонентами которые помогают защитить нас на уровне сети.

В разных компаниях в зависимости от уровня зрелости может быть меньше компонентов, либо больше (несколько Фаерволл WAF, пограничные маршрутизаторы и так далее).

Как вы поняли, дело не столько в сетевых устройствах, которые помогают защитить нас от атак, но и в главном механизме - **сегментации сети**.

Сегментация сети является важным механизмом обеспечения безопасности в современных IT-инфраструктурах. Она предполагает разделение физической или виртуальной сети на различные сегменты (или "зоны безопасности") с определенными правилами доступа и коммуникации между этими сегментами. Ниже приведены причины, по которым сегментация сети считается полезной:

Изоляция и минимизация рисков

- **Снижение уровня угроз:** Если злоумышленник получит доступ к одному сегменту сети, он не сможет легко перемещаться по другим сегментам.
- **Минимизация внутренних угроз:** Сегментация может предотвратить несанкционированный доступ к критическим системам со стороны собственных сотрудников или других внутренних систем.

Лучший контроль и гибкость

- **Контроль доступа:** Через маршрутизацию и правила фаервола можно точно определить, какие виды трафика разрешены между различными сегментами.
- **Упрощение управления безопасностью:** Сегменты с похожими требованиями к безопасности можно группировать, что упрощает управление политиками безопасности.

Производительность и оптимизация ресурсов

- **Оптимизация трафика:** Сегментация позволяет локализовать трафик внутри определенных зон, уменьшая нагрузку на сетевое оборудование.

Зоны и DMZ

- **Зоны (Зоны безопасности):** Это выделенные сегменты, которые часто группируются по функциональности. Например, одна зона может содержать только базы данных, в то время как другая зона может быть предназначена для веб-серверов.
- **DMZ (Demilitarized Zone):** Это сегмент сети, который выступает в роли "буфера" между вашей внутренней сетью и внешним миром (например, интернетом). Серверы в DMZ могут взаимодействовать с внешними системами, но у них ограниченный доступ к внутренней сети, что уменьшает риски безопасности.

Использование сегментации сети, зон безопасности и DMZ позволяет создать многоуровневую модель безопасности, которая обеспечивает глубину защиты и уменьшает вероятность успешных атак.