Занятие 8. Веб-серверы. Nginx. Действия межсетевого экрана

Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, обслуживающего HTTP-запросы клиентов, так и непосредственно сам сервер, на котором располагается программное обеспечение.

С точки зрения аппаратного обеспечения («железа»), веб-сервер - это сам сервер, который хранит файлы сайта и отправляет их по запросу клиенту, он подключен либо к сети Интернет и имеет глобальный IP-адрес и доменное имя, либо к локальной сети клиента. С точки зрения программного обеспечения, веб-сервер включает в себя несколько компонентов, которые отвечают за доступ клиентов к ресурсам, расположенным на сервере, по протоколу HTTP. Сайты и документы, которые отдает веб-сервер, могут быть как статическими (веб-сервер отдает html-, css-, js- и т.п. файлы, находящиеся в файловой системе, без каких-либо преобразований), так и динамическими (для получения содержимого ответа веб-сервер либо обращается к бэкенду, либо преобразует файлы, находящиеся в файловой системе, в соответствии с запросом клиента).

Кроме задач доставки содержимого документов в ответ на HTTP-запросы клиентов, веб-серверы выполняют различные дополнительные функции, например, аутентификация/авторизация пользователей, поддержка SSL/TLS-шифрования, журналирование действий пользователей, преобразование данных и заголовков ответов, пересылка запросов на бекенд-сервера. Одними из самых популярных и распространенных веб-серверов являются: HTTPD (Apache), IIS, Nginx, LigHTTPd.

NGINX

Nginx [engine x] - это HTTP-сервер и обратный прокси-сервер, почтовый прокси-сервер, а также TCP/UDP прокси-сервер общего назначения. Согласно статистике Netcraft nginx обслуживал или проксировал 23.20% самых нагруженных сайтов в январе 2021 года.

У nginx есть один главный и несколько рабочих процессов. Основная задача главного процесса - чтение и проверка конфигурации и управление рабочими процессами. Рабочие процессы выполняют фактическую обработку запросов и работают под непривилегированным пользователем. Nginx состоит из модулей, которые настраиваются директивами, указанными в конфигурационном файле. Одна из важных задач конфигурации nginx - раздача файлов, таких как изображения или статические HTML-страницы. Часто nginx применяется в качестве прокси-сервера, то есть сервера, который принимает запросы, перенаправляет их на проксируемые сервера, получает ответы от них и отправляет их клиенту.

Основными и часто используемыми возможностями сервера nginx являются:

- Обслуживание статических запросов, поиск индексных файлов, создания списков файлов в каталоге, возможность настройки ответов в зависимости от типов файлов
- Распределение нагрузки и отказоустойчивость, проксирование запросов

- Модульность, фильтры, в том числе сжатие, докачка, chunked ответы, xslt-преобразование, SSI, преобразование изображений, параллельная обработка подзапросов
- Поддержка SSL/TLS, поддержка HTTP/2
- Поддержка виртуальных серверов, определяемых по имени или IP-адресу
- Широкая функциональность настройки и работы с логами
- Модуль rewrite для изменения URI при помощи регулярных выражений
- Определение территориальной принадлежности клиента при помощи GeoIP
- Ограничение доступа по адресу клиента, результату подзапроса, прохождению аутентификации
- Поддержка DAV
- Стриминг FLV, MP4
- Ограничения на частоту и количество запросов от клиентов, одновременных соединений или запросов по определенным параметрам
- Встроенные механизмы реализации A/B-тестирования и зеркалирования запросов
- Функциональность почтового прокси-сервера с поддержкой SSL/TLS, аутентификации клиентов
- Проксирование потоков данных по протоколам TCP/UDP
- Поддержка сценарного языка njs для гибкой работы с заголовками, создания асинхронных обработчиков и фильтров, управления доступом

Подробнее об nginx и работе с ним:

- https://nginx.org/ru/docs/
- https://nginx.org/ru/docs/beginners_guide.html

МЕЖСЕТЕВОЙ ЭКРАН И НЕКОТОРЫЕ ЕГО ДЕЙСТВИЯ

Межсетевой экран (брандмауэр, firewall) - это программный или программно-аппаратный комплекс, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика. Основными задачами межсетевых экранов являются защита отдельных хостов или сегментов сети от несанкционированного доступа, преобразование или ограничение трафика (шейпинг), а так же организация взаимодействия между различными сетями. Обычно межсетевые экраны располагаются на границе периметра сети или на стыке различных сетей. Чаще всего межсетевые экраны работают на 2-4 уровнях модели OSI, иногда встречаются реализации, работающие на более высоких уровнях.

В семействе ОС Linux в ядре, начиная с версии 2.4 встроен межсетевой экран netfilter, управление его правилами обработки трафика происходит при помощи различных утилит,

например, iptables. Трафик «внутри» межсетевого экрана проходит через цепочки правил, правила могут содержать критерии, действие или переход. Критериев может быть очень много и задействуют практически все параметры трафика, например, адреса и порты источника и назначения, протокол транспортного уровня, состояние пакета и т.п. Действия зависят от цепочки, которую проходит трафик, удовлетворяющий критериям.

Существует 5 стандартных типов цепочек (помимо них существует возможность создания собственных цепочек):

- PREROUTING — для изначальной обработки входящих пакетов
- INPUT — для входящих пакетов адресованных непосредственно локальному процессу (клиенту или серверу)
- FORWARD — для входящих пакетов перенаправленных между разными сетевыми интерфейсами (все перенаправляемые пакеты проходят сначала цепочку PREROUTING, затем FORWARD и POSTROUTING)
- OUTPUT — для пакетов генерируемых локальными процессами
- POSTROUTING — для окончательной обработки исходящих пакетов

Цепочки организованы в 4 таблицы:

- raw - используется редко, в основном для маркировки пакетов, содержит цепочки PREROUTING и OUTPUT
- mangle - используется для модификации IP-пакетов, в основном их заголовков (например, изменение TTL), содержит все пять стандартных типов цепочек
- nat - используется для перенаправления пакетов, создающих новое соединение, содержит цепочки PREROUTING, OUTPUT, POSTROUTING
- filter - основная таблица, используется для разрешения или ограничения пакетов/ трафика по критериям, содержит цепочки INPUT, FORWARD, OUTPUT

Часто используемые действия во всех цепочках - ACCEPT (принять), DROP (сбросить), LOG (журналировать пакет или событие). Притом сброс пакета происходит без какого-либо обратного уведомления клиента о действии. Для цепочки filter так же часто используется действие REJECT, в отличие от DROP клиенту сообщается причина отказа обслуживания пакета/трафика. Для цепочки nat используются следующие действия: DNAT (destination network address translation) - преобразование адреса и порта назначения, SNAT (source network address translation) - преобразование адреса источника, MASQUERADE - в основе то же самое, что и SNAT, только преобразование адреса источника происходит автоматически в соответствии с параметрами сетевых интерфейсов, REDIRECT - перенаправление пакетов на другой порт текущего хоста.

Действие DNAT обычно используется для «проброса портов», действие MASQUERADE обычно используется для организации шлюза и предоставлении доступа клиентов локальной сети в глобальную или в другую сеть, действие REDIRECT используется в случае, когда необходимо реализовать возможность доступа по разным портам к одному и тому же сервису без открытия этих портов и обслуживания дублирующих конфигураций.

Подробнее базовую информацию о прохождении трафика через межсетевой экран можно почитать в руководстве: https://www.opennet.ru/docs/RUS/iptables/