????? ????? ??????? ? ????????

Напомню, как выглядит наша схема.

basic-infra-schema-principals.png

Если рассматривать сетевой путь от клиента до конечного сервиса, здесь есть 3 основных узла: WAN-proxy, сам маршрутизатор (A660) и LAN-proxy.

В случае с **маршрутизатором** - здесь все просто:

1. Входим в ПУ вашего маршрутизатора
2. Идем в "Приложение" -> "Переадресация порта"
3. Настраиваем переадресацию на хост-балансировщик, находящийся в вашей домашней сети. Например, для адреса 192.168.1.102 и диапазона портов 50001-50032, настройка будет примерно такой:

image.png

На места этого IP-адреса может быть любой из вашей сети, единственный критерий - к нему должен быть доступ от маршрутизатора. Проверить это можно в "Администрирование" -> "Диагностика Ping".

А вот дальше уже сложнее...

Многие задаются вопросом: а зачем вообще открывать диапазоны портов и потом как-то сложно их маппить? Можно же просто открыть, например, 443 порт, и хостить балансировку сразу за ним.

Да, можно, но только не на F660 - эта рокетка уже использует 443 порт в LAN и, открывая его и в WAN, происходит ситуация, которая решается только физическим сбросом маршрутизатора. ПУ перестает открываться, а перенаправление не работает. Как? Не спрашивайте, потому что на нормальном железе (например, на Keenetic или TPlink) такой ситуации не происходит: они видят разницу между LAN и WAN подключениями.

Помимо этого, вы не сможете скрыть своей реальный IP-адрес, тем самым вам придется столкнуться с 2 нюансами:

1. Вам придется реализовать блокировку доступа к ПУ не на уровне маршрутизатора, а на уровне Nginx на самой ноде PVE (или прокси). Казалось, бы, это не проблема? Я напоминаю - сам хост стоит в LAN, за маршрутизатором, и заголовок Source-EA у

всех пакетов, которые будут к нему приходить, всегда будут содержать только 1 IP-адрес - вашего маршрутизатора. При таком подходе и на этом железе вы не сможете "отсеять" нежелательные подключения к ПУ, как следствие - она будет торчать в интернет as-is.
2. При попытке положить вам хост, вы рискуете лишиться не только его самого, но и всего интернета - маршрутизатор уйдет в перезагрузку, а вместе с ним и весь ваш канал.

Балансировщик решает эту проблему и дает возможность тонкой настройки единой точки входа:

- Хотите общий WAF для всех приложений? Настраивайте его на балансировщике, ведь именно через него проходит весь трафик от пользователя до приложения;
- Хотите запретить доступ сразу ко всем пользователям? Просто погасите балансировщик, и хуй кто из пользователей воспользуется вашей инфраструктурой (моментами, может сыграть против вас);
- Такая архитектура - один из моментов, когда мы применяем наш костыльный "SOLI", а именно - Single Responsibility. Функционал сервисов - на самих сервисах, а функционал доступа к ним - на отдельных хостах.

Чтобы настроить балансировку со стороны WAN

Revision #3
Created 2025-12-01 14:43:36 UTC by root
Updated 2025-12-02 16:29:47 UTC by root