سوال ۱:

اگر منظور سوال بالا آوردن سرویس بدون هیچ ارتباطی با شبکه خارجی باشد، کافی است که سرویس را روی اینترفیس localhost بالا بیاوریم و تنظیمات آدرس‌دهی مودم شبکه داخلی را تغییر دهیم تا از شبکه خارجی قابل دسترس نباشد.(در صورت داشتن IP static)

اگر در سوال ارتباط غیر مستقیم و امن با با شبکه‌ی خارجی ایراد نداشته باشد، می‌توان به کمک Reverse Proxy ها این کار را انجام داد. عملکرد Reverse Proxy ها دقیقاً عکس عمل Forward Proxy Server ها می‌باشد زیرا Forward Proxy Server ها درخواست‌ها را از شبکه داخلی از کلاینت‌ها دریافت می‌کند و به سرور های موجود در اینترنت ارسال می‌کند اما Reverse Proxy ها درخواست‌های کلاینت‌ها را از محیط اینترنت دریافت و به سرورهای مورد نظر در شبکه داخلی هدایت می‌کند. به Reverse Proxy گاهاً Inbound Proxy نیز گفته می‌شود و به Proxy، Outbound Proxy گفته می‌شود. دلیل آن هم کاملاً واضح است چون Reverse Proxy یا همان Inbound Proxy درخواست‌ها را از سمت بیرون شبکه داخلی دریافت می‌کند اما Forward Proxy یا همان Outbound Proxy درخواست‌ها را از سمت داخل شبکه به بیرون شبکه یا اینترنت ارسال می‌کند.
Reverse Proxy Server پشت فایروال قرار می‌گیرد و درخواست‌ها را از شبکه اینترنت دریافت کرده و آن‌ها را به سرورهای موجود در شبکه داخلی ارسال می‌کند. بدیهی است که سرورهای موجود در شبکه داخلی به صورت مستقیم از شبکه خارجی اینترنت قابل دسترسی نمی‌باشند. Reverse Proxy باعث می‌شود که کاربران درخواست کننده سرویس از سمت اینترنت از طرف Reverse Proxy سرور احراز هویت شوند.[1]

سوال ۲:

TLS termination فرآیندی است که توسط آن ترافیک داده‌ی رمزگذاری شده با TLS رمزگشایی (یا بارگیری) می شود. سرورهایی با اتصال SSL می توانند به طور هم‌زمان بسیاری از اتصالات یا جلسات را مدیریت کنند. یک اتصال TLS با استفاده از یک گواهی برای احراز هویت، داده‌های رمزگذاری شده را بین رایانه کاربر نهایی و وب سرور ارسال می‌کند. خاتمه TLS به سرعت فرآیند رمزگشایی کمک می‌کند و بار پردازش را بر روی سرورهای باطن کاهش می‌دهد.
TLS termination ترافیک https رمزگذاری شده را هنگامی که سرور، داده‌ها را از SSL در یک جلسه SSL دریافت می‌کند، رهگیری می‌کند. TLS termination داده ها را به جای سرور برنامه، روی بار متعادل کننده رمزگشایی و تأیید می‌کند. سرور بدون نیاز به سازماندهی اتصالات ورودی، می تواند کارهای دیگری مانند بارگذاری صفحات وب را اولویت بندی کند. این به افزایش سرعت سرور کمک می‌کند. TLS termination نشان دهنده پایان - یا نقطه پایان - یک اتصال SSL است.

سوال ۳:

از Reverse Proxy آماده[2]استفاده شده، که بعد از ایجاد تغییرات روی آن به پروژه‌ی خواسته شده در دستور کار[3]متصل شده است.
پروژه‌ی httbin را بر روی docker از پورت ۶۰۰۰ به ۸۰ بالا آورده و سپس Reverse Proxy را روی پورت ۳۰۰۰ بالا می‌آوریم. حال با ابزار curl یا postman به Reverse Proxy رکوئست POST را با body نام کاربری و رمز عبور می‌زنیم که در صورت درست بودن هویت، در ریسپانس JSON Web Tokens را دریافت می‌کنیم. سپس آن توکن را در هدر با کلید Authentication رکوئست GET وارد کرده و رکوئست را ارسال می‌کنیم و در صورت درست بودن توکن به صفحه‌ی اصلی httbin متصل می‌شویم.

---

[1] https://tosinso.com/ajj
[2] https://github.com/maisonm/jwt_auth_example
[3] GitHub - postmanlabs/httpbin: HTTP Request & Response Service, written in Python + Flask.