1- چگونه میتوان یک سرویس را فقط بر روی شبکه داخلی اجرا کرد؟

می‌توان روی interfaceهای مختلف دستگاه پورت هایی را باز کرد. حال اگر این interfaceهمان شبکه wifi باشد پورت برای همه باز می‌شود و اگر روی interface مربوط به loop back داخلی باشد فقط local host خودمان آن پورت خاص را دارد.

2- علاوه بر jwt authentication یکی دیگر از راه های امن کردن سرویس داخلی legacy ، استفاده از روشی به نام TLS termination است. فلسفه این کار را توضیح دهید.

کاری که TLS termination proxyانجام میدهد این است که با کلاینت روبرو می شود و کلاینت و پراکسی توافق می کنند بر روی یک کلید برای ارتباط بین آن ها.

در پروتکل TLS دو کلید خصوصی و عمومی داریم که کلاینت به کمک کلید عمومی و سرور به کمک کلید خصوصی با استفاده از عملیات رمز کردن، کلید Session را تولید و بازیابی میکنند. و اگر کلاینتی بدون این کلید ها درخواست ارسال کند، سرور متوجه میشود که این کلاینت جزو کلاینت های سرویس ما نیست و نباید به آن دسترسی بدهد.

فلسفه این روش این است که فقط کلاینت هایی که مورد تایید باشند (کلید مورد نظر را داشته باشند) به سرور دسترسی داشته باشند و پس همانند jwt authentication روشی است برای کنترل دسترسی کلاینت های معتبر و غیرمعتبر.