Briefing

Why they want to do this

It's completely unacceptable to have a website server accessible directly by the public. That is a huge security risk as it opens up more attack vectors and thus increases the attack surface.

And so, we want to implement a proxy that we can hide our website server behind as this will now become the **only** attack surface point. The proxy can also be used to aid in providing scalability. We always want to think about the future when implementing technologies and we have decided on this proxy technology.

I'll explain the scalability portion with an example.

Scalability Example

Say that our website is getting millions and millions of visits per day. A single web server machine will be struggling to handle this and so we need to add more web servers to handle the requests. Let's say 10 for this example.

With the old model, we would need to give people the IP addresses of the 10 different webservers. This is a nightmare logistically as you would need to find a way to balance out the distribution of these IPs so one server doesn't get overloaded (DoS). From a security standpoint, if we have 10 web servers that are publicly accessible, this would mean that there are 10 different machines that malicious parties can attack; which is a colossal security risk. This isn't acceptable/ feasible. This is where a proxy helps us.

With the newer model, all the website servers are hidden behind the proxy in a **server farm**. The proxy has the capability of performing load balancing. This is simply just trying to efficiently distribute incoming network traffic across a group of servers. Forwarding requests is not an expensive operation because it's not doing any intensive processing. And so, the clients will still send their requests to the proxy IP and then the proxy will choose 1 machine for 1 request, another machine for another request, etc etc. In this way, the client has no idea we added more machines and their experience is uninterrupted. From a security perspective, the attack surface only involves this one proxy machine and so reducing the number of machines from 10 to 1 is a significant decrease in the risk.

Resources Provided

You've been provided a sample from the old administrators on a technology they've heard of; Nginx.

Basic Sample (/etc/nginx/nginx.conf):

```
events {}

http {
    server {
        listen 80;
        server_name my_server.com
        location / {
            proxy_pass http://my_server/;
        }
    }
}
```

The admins didn't provide any helpful comments unfortunately.

YOU MUST USE THE DOMAIN NAME teamX.umlcyber.club . Replace X with your team number!