Good Evening Premium House Light Manager,

I hope you are doing well and had a good weekend. Here is the email report you asked me to look into as quick as possible. We will go over our current network topology map and some recommendations for a more secure network and security culture for our employees.

Figure 1:current network topology

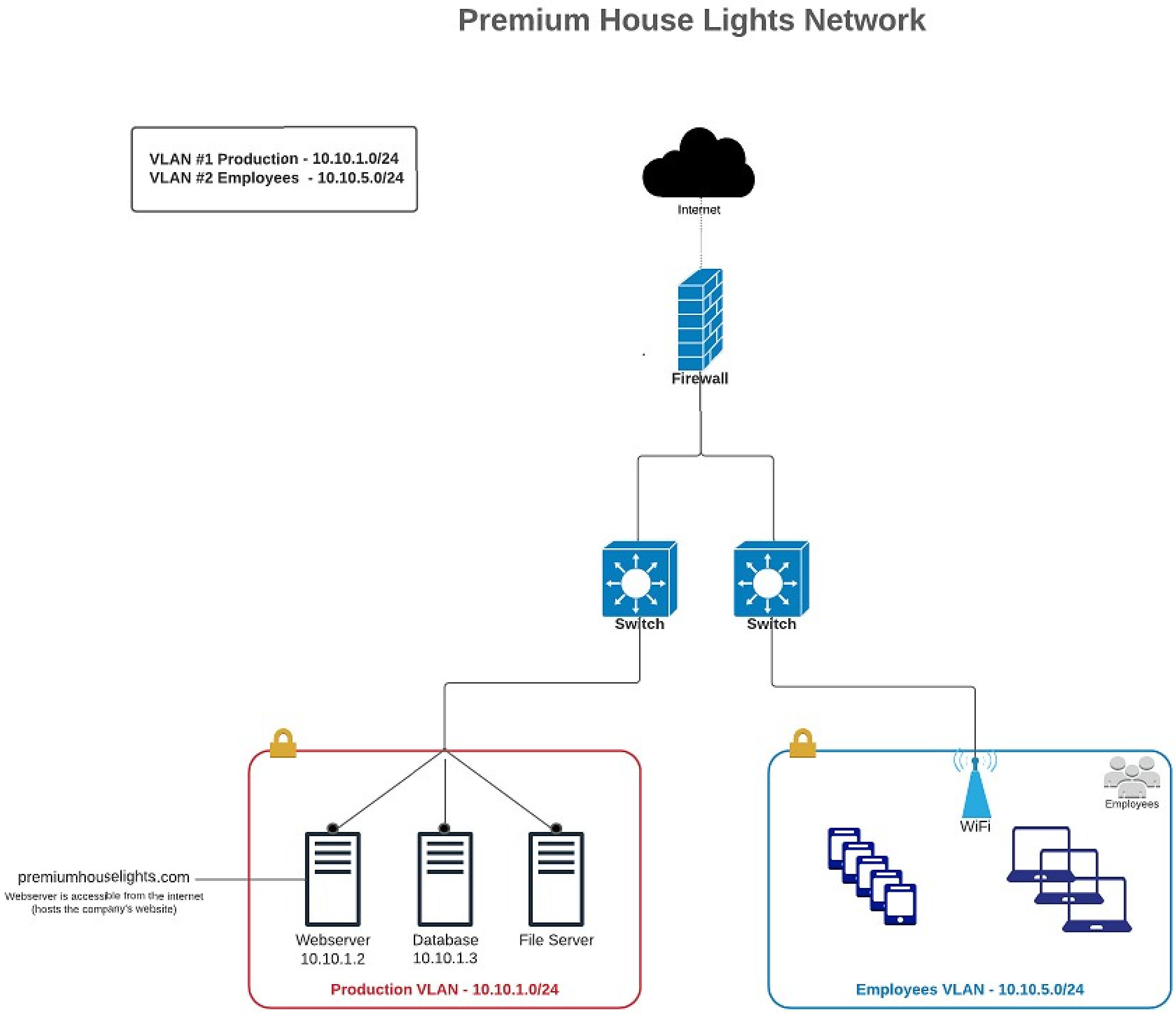
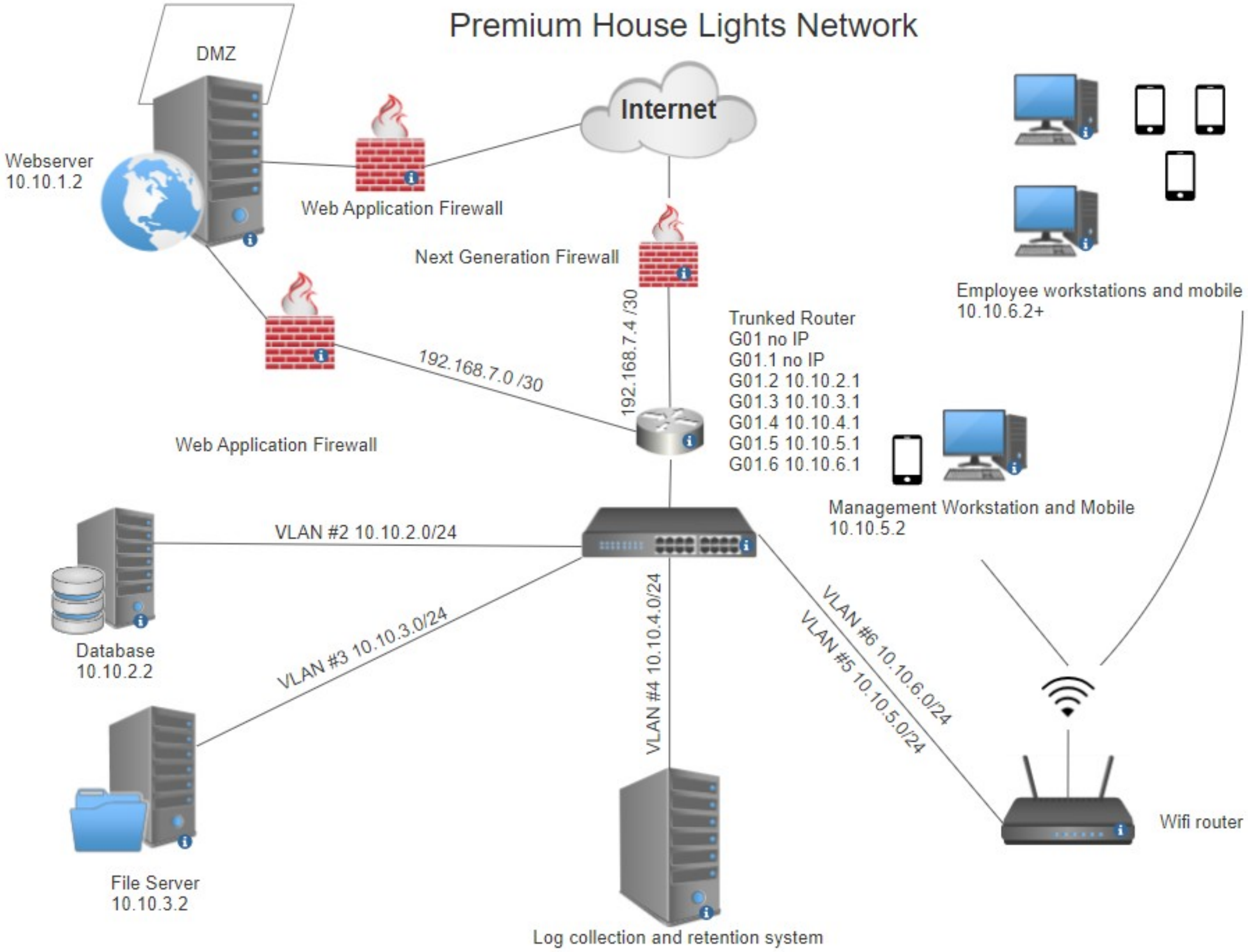

Premium House Lights Network
VLAN #1 Production - 10.10.1.0/24
VLAN #2 Employees - 10.10.5.0/24
Internet
Firewall
Switch
Switch
premiumhouselights.com
Webserver is accessible from the internet
(hosts the company's website)
Webserver
10.10.1.2
Database
10.10.1.3
File Server
Production VLAN - 10.10.1.0/24
WiFi
Employees
Employees VLAN - 10.10.5.0/24

Figure 2: Upgraded network topology



When it comes to our security footprint, it is important to have a detailed network topology map as a visual for where all our security devices are kept and their locations. When connecting our network to the internet, we want the best firewall protection, acting as a front door, lock, and key. A next-generation firewall is like a security guard for your computer network. It not only blocks bad guys from getting in but also keeps an eye on what's happening inside, ensuring everything is safe and sound.

Regarding our web server, it's crucial, per best practices, to separate it completely from our trusted network. We'll then add web application firewalls facing both the internet and our network. A web application firewall is like a protective shield for websites. It blocks harmful content from reaching our website, such as cyber-attacks and bad data, keeping it safe and secure for users. Additionally, implementing IP address changes and Virtual LAN installations can provide further protection. All IP addresses are labeled to keep the new network topology map as up-to-date as possible.

In the cybersecurity industry, professionals don't say "if" something happens, they say "when". Therefore, my recommendation is to invest in a log collection and retention system that connects to the entire network, collecting log reports and backing them up. This ensures that when our system is compromised, we have a way to find out exactly what happened and how to mitigate the damages.

Moving on to employee training and awareness, studies show that 95% of cyber-attacks start with human error. Proper password training and policies are essential. Implementing multi-factor authentication, which sends a code to the employee's work cellular device, adds an extra layer of security. Training employees on how to spot phishing attacks and encouraging them to report suspicious activity fosters a more cyber-secure culture in our workplace. Additionally, implementing the principle of least privilege ensures employees only have access to what's necessary for their job, reducing the risk of accidents or misuse of sensitive information.

For physical protection, securing employee systems is vital. Implementing USB locks on all open USB ports accessible to the public and physically locking our web server, database, and file server prevents unauthorized access.

Lastly, I recommend developing an incident response plan. This plan is akin to a fire drill for computer problems, guiding us step-by-step on what to do in the event of a cyber-attack or data breach. It helps us react quickly and effectively to minimize damage and restore normal operations promptly.

Thank you for your time. If you have any further questions, please contact me via email or phone. I look forward to enhancing our company's security for the future.

Regards, Justin Gale