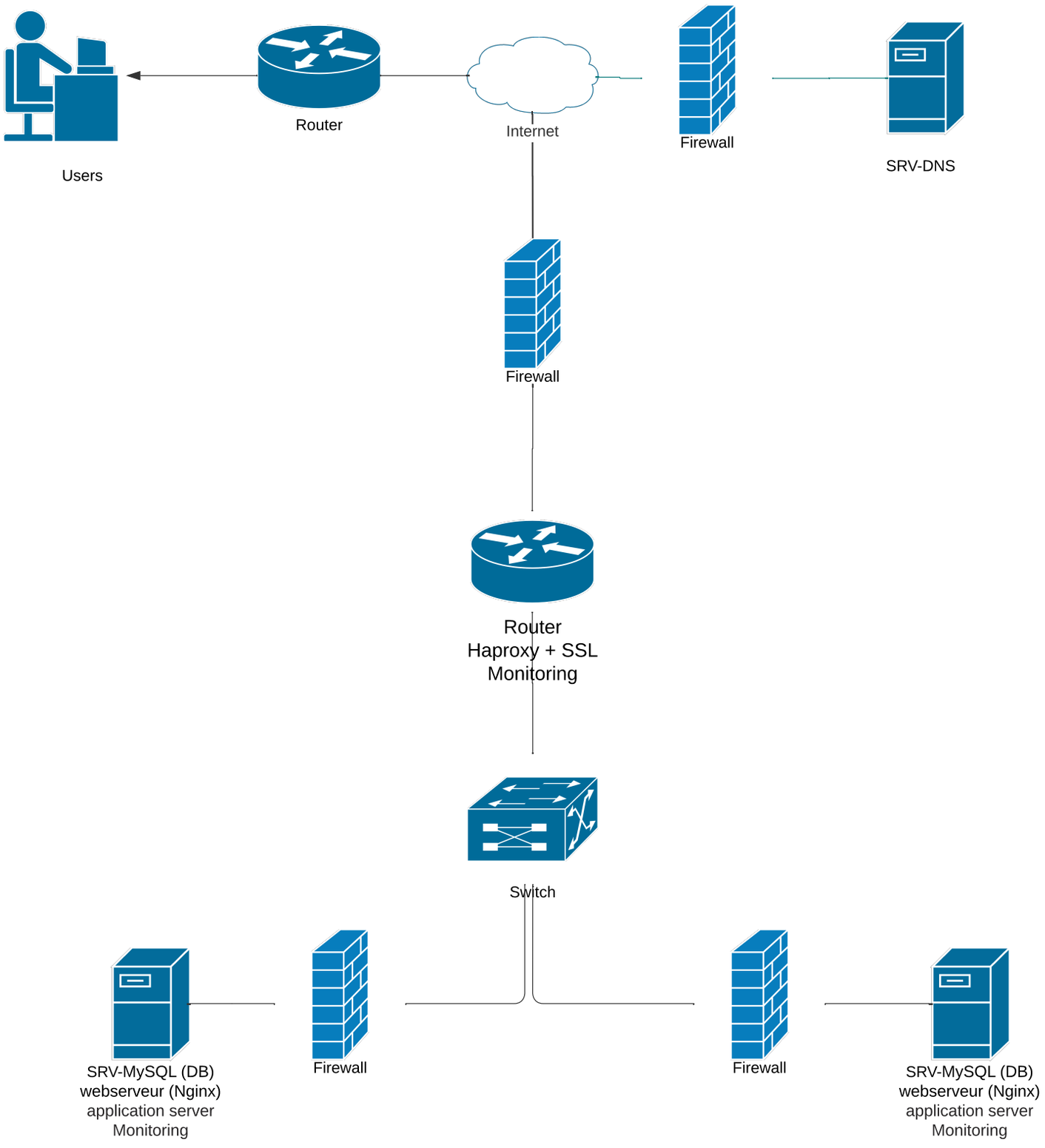
2-secured_and_monitored_web_infrastructure_FR

Verschueren Samuel | September 11, 2024



En savoir plus sur ce modèle

1. L'utilisateur tape www.foobar.com dans son navigateur.
2. Le navigateur envoie une requête au serveur DNS pour résoudre le nom de domaine www.foobar.com.
3. Le serveur DNS répond avec l'adresse IP du load balancer.
4. Le navigateur de l'utilisateur envoie une requête HTTPS à l'adresse IP du load balancer.
5. La requête atteint le premier pare-feu, qui filtre le trafic entrant.
6. Le load balancer (HAproxy) reçoit la requête HTTPS, décrypte le trafic avec le certificat SSL, et la distribue à l'un des serveurs disponibles selon l'algorithme de distribution configuré.
7. La requête passe par le deuxième pare-feu avant d'atteindre le serveur choisi.
8. Le client de monitoring sur le serveur commence à collecter des données sur cette requête.
9. La requête arrive au serveur web Nginx sur le serveur choisi.
10. Nginx, agissant comme un reverse proxy, transmet la requête au serveur d'application sur le même serveur.
11. Le serveur d'application exécute le code de l'application (par exemple, PHP, Python, etc.).
12. Si nécessaire, l'application envoie des requêtes à la base de données MySQL, passant par le troisième pare-feu.
13. La base de données MySQL traite la requête et renvoie les résultats au serveur d'application.
14. Le serveur d'application génère la réponse HTML finale.
15. La réponse est renvoyée à Nginx, qui la transmet au load balancer.
16. Le load balancer chiffre la réponse avec le certificat SSL et la renvoie au navigateur de l'utilisateur.
17. Le navigateur de l'utilisateur déchiffre et affiche la page web demandée.
18. Tout au long du processus, les clients de monitoring sur chaque serveur et le load balancer collectent des données sur les performances, la sécurité et l'utilisation des ressources. Ces données sont prêtes à être envoyées à un service de monitoring externe (comme Sumologic, mentionné dans l'énoncé) pour analyse.

Information complementaire: