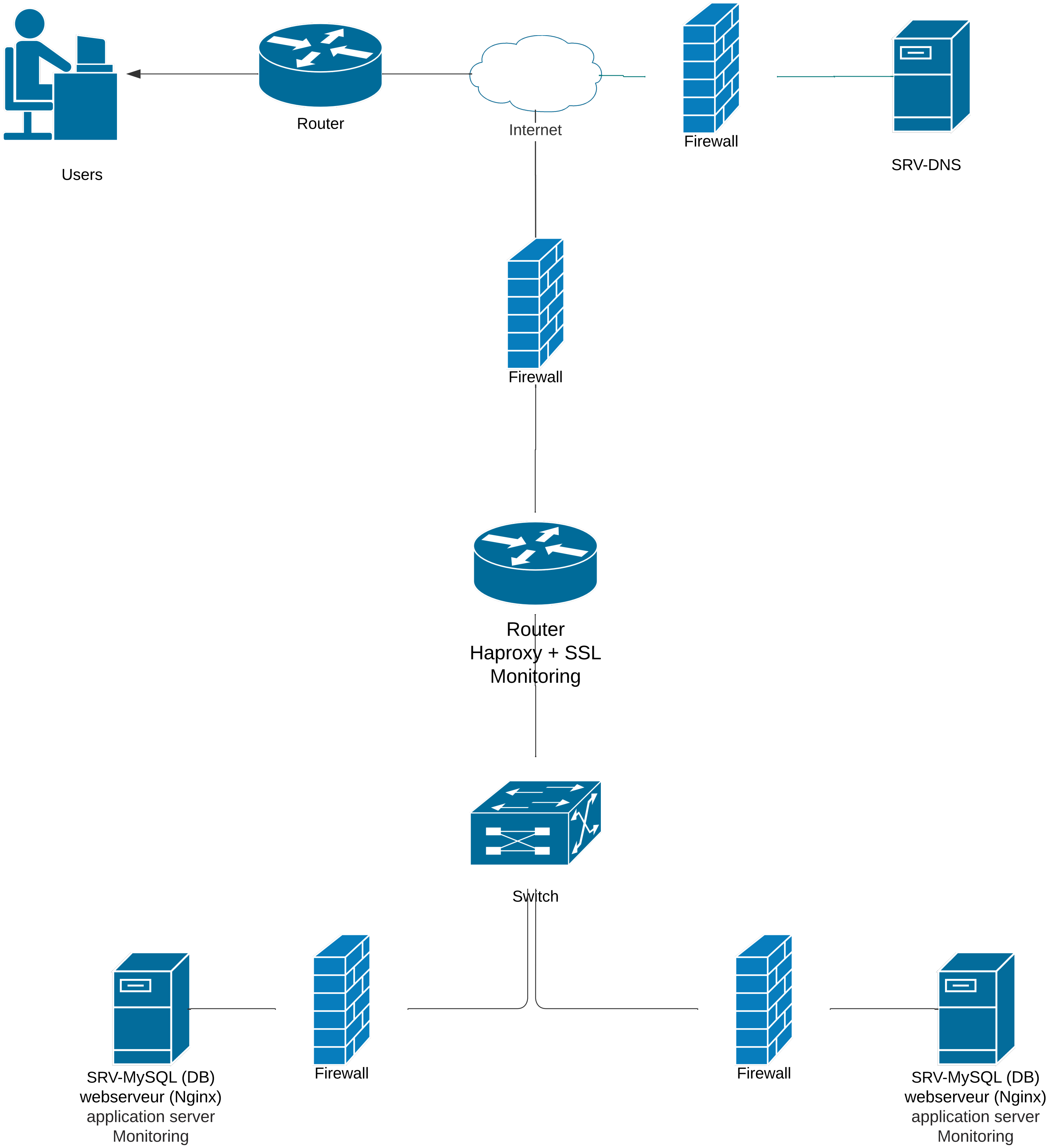
2-secured_and_monitored_web_infrastructure_FR

Verschueren Samuel | September 11, 2024



En savoir plus sur ce modèle

1. The user types www.foobar.com into their browser.
2. The browser sends a request to the DNS server to resolve the domain name www.foobar.com.
3. The DNS server responds with the IP address of the load balancer.
4. The user’s browser sends an HTTPS request to the load balancer’s IP address.
5. The request reaches the first firewall, which filters incoming traffic.
6. The load balancer (HAproxy) receives the HTTPS request, decrypts the traffic with the SSL certificate, and distributes it to one of the available servers according to the configured distribution algorithm.
7. The request passes through the second firewall before reaching the chosen server.
8. The monitoring client on the server starts collecting data on this request.
9. The request reaches the Nginx web server on the chosen server.
10. Nginx, acting as a reverse proxy, forwards the request to the application server on the same server.
11. The application server executes the application code (e.g., PHP, Python, etc.).
12. If necessary, the application sends queries to the MySQL database, passing through the third firewall.
13. The MySQL database processes the query and returns the results to the application server.
14. The application server generates the final HTML response.
15. The response is sent back to Nginx, which forwards it to the load balancer.
16. The load balancer encrypts the response with the SSL certificate and sends it back to the user’s browser.
17. The user’s browser decrypts and displays the requested web page.
18. Throughout the process, monitoring clients on each server and the load balancer collect data on performance, security, and resource usage. This data is ready to be sent to an external monitoring service (like Sumologic, mentioned in the statement) for analysis.

Information complementaire: