POWERDNS

CASE STUDY

Providing a Southeast Asian operator with a state-of-the-art DNS solution, implemented under special circumstances

The challenge

At the beginning of 2020, a leading communication service provider (CSP) from Southeast Asia decided to replace its legacy DNS system to a modern and future proof setup. The CSP is the second largest broadband provider in its home market, with around 500,000 fixed broadband subscribers, including many Fiber-to-the-Home (FTTH) users, as well as business customers. It decided that the new platform needed to be highly scalable, and ready for the traffic and load challenges of the future. Additionally, the new solution should provide enhanced security to its network. As a result, the CSP required it to be capable of handling security threats to both its telecom infrastructure, as well as to end-users on the network.

The operator had previously been running a legacy platform with a DPI-based system for traffic analysis, but with the growth of traffic volumes and the uptake of encrypted traffic, it envisioned a more modern and manageable DNS solution that would also provide DNS-based malware protection. In addition, the CSP wanted to move towards more privacy for its subscribers and offer encrypted DNS with DNS over HTTPS (DoH) and DNS over TLS (DoT) for its customers, whilst increasing DNS integrity using DNSSEC signing. By choosing PowerDNS, the CSP can now enable malware protection via RPZ as a security layer that it offers to its high-end subscribers.

About the CSP

The Southeast Asian network operator is a telecommunications provider specializing in domestic and international connectivity. It offers Retail, Enterprise, and Wholesale market solutions. In addition to its domestic market, where the CSP delivers the fastest fiber broadband service (speeds of up to 2Gbps), it provides fiber optic network services in various other Southeast Asian countries.

The CSP was looking for a replacement for its mix of open source software DNS platform and commercial security solution. Its mission for providing latest technology, innovative product offerings and transparency to subscribers led to it identifying PowerDNS as a potential partner. As a result, PowerDNS was invited to participate in a detailed evaluation.

Deploying PowerDNS Recursor, DNSdist and Authoritative Server remotely during Covid-19 lockdowns & across several time zones

The solution

During 2020, the CSP performed a rigorous evaluation of various solutions. PowerDNS convinced them in an on-site proof of concept (PoC), where the team demonstrated the solution's capabilities to meet all requirements.

Together with a regional integrator, PowerDNS equipped the CSP with a state-of-the-art DNS installation. Specifically, DNSdist offered both Distributed Denial of Service (DDoS) protection, as well as providing an entry point for encrypted DNS.

Apart from technical benefits, the Southeast Asian operator also appreciated PowerDNS' commercial business model. PowerDNS understands that a predictable cost structure helps to guarantee the longer-term viability of any solution, specifically since the CSP's traffic is seeing significant growth year-on-year. In addition, the PowerDNS business model allows expansion to a third datacenter location, including mitigation of DDoS attacks or adding additional service locations for its DNS platform.

The project

After going through a technical on-site PoC, the implementation of the service took place in 2021. In a time when Covid-19 posed practical challenges to many people as well as companies, PowerDNS worked closely with a regional integrator and the CSP to deploy the solution remotely, often working across several time zones.

The project involved the initial deployment of PowerDNS recursive services, PowerDNS Recursor and DNSdist, across two geographically separated sites, in addition to PowerDNS Authoritative Server.

To offer additional security for high-end customers, network-based malware protection was implemented using Spamhaus threat intelligence feeds, which are distributed using RPZ. Advanced privacy was also enabled by making the platform DoH capable, accommodating users and applications that were ready to move to using DoH.

The future

The CSP has seen a steady increase in DNS traffic and subscriptions. This growth leads to new challenges for its DNS installation, in terms of capacity and geographical DNS server locations. As its PowerDNS solution is ready to scale up and out, the CSP is looking forward to extending its DNS capacity to accommodate the current growth in traffic for the coming years.

In addition, the operator is evaluating the extension of its PowerDNS solution with value added services using PowerDNS Protect. And, for the future, the CSP is also looking at moving to a cloud-native deployment model with PowerDNS Cloud Control.

Please contact us if you want to learn more about this project or PowerDNS.

Contact PowerDNS
for more information

Stay up to date
by signing up for
PowerDNS Updates