DNSVAULT

Rock-solid & Secure DNS Appliance

CASE STUDY

www.dnsvault.net

UNIVERSITI TEKNOLOGI PETRONAS

ORGANIZATION :
Universiti Teknologi Petronas

DOMAIN :
utp.edu.my

INDUSTRY :
Education

UNIT PURCHASE :
3 Units

RESULT :

- **Secured by DNSSEC**
- **Provides the best availability**
- **More stable and packed , more features.**

PROJECT OVERVIEW

Universiti Teknologi PETRONAS (UTP) is one of Malaysian prestigious private university. UTP places strong emphasis on Research and Development as it strives to achieve the status of an internationally renowned Research University. UTP is the only private university in Malaysia to be ranked in the top 200 for the 2014 QS Asia University Rankings and ranked at 335 for the QS World University Rankings under Engineering and Technology Faculty. As one of the research university in the world the internet and the reliability of the DNS server is very critical. The domain name utp.edu.my and utp-prism.my is used by its students and lecturers to access thousands of online reference and thesis which translated to over 70,000 query each day. While for internal DNS, query per day can reach up to 15 millions. This show how important the DNS to the university. Without a reliable DNS server, DNS service interruption can be a serious issues.

CHALLENGE

Currently, **Universiti Teknologi PETRONAS (UTP)** have IPv6 but the DNS does not support IPv6. **Universiti Teknologi PETRONAS (UTP)** use a BIND base DNS server which comes with the Red Hat Linux. Its a good start for a simple DNS management and low capacity but with the heavy load, untune, and unprotected DNS can be a easy prey for hackers. The first problem that we caught is, UTP is using the old BIND version which have many security vulnerabilities. This is a serious security issues as hacker can use the imperfection in outdated BIND version and gain access to the server. Once they are able to gain access, its a simple path ahead as he control the main DNS server that served all the communities in UTP campus, ranging from simple redirection to malicious website and also phishing for sensitive information like internet banking password. We also found that previous DNS server was not configured properly and the recursive option is open for the whole world to use. This matter can lead to UTP DNS server act as a vector for DNS amplification attacks. Besides, ipv6 configuration for the DNS is very complicated using the old BIND server, so ipv6 is enabled but not configured properly to served the ipv6 networks.

SOLUTION

Universiti Teknologi PETRONAS (UTP) also use DNSSEC for added security. DNSSEC Validation is enabled for recursive queries so all DNSSEC enabled domain will be validated for authenticity. Other than that, the migration to DNSVault has help UTP to do a better job serving DNS query. No more problem with reliability and security, as DNSVault is a DNS appliance that has been tune and hardened to provides the best availability and also security. DNSVault use the latest BIND 9 version, so any security serious security issues has been patch and by using the latest version, it is more stable and packed more features. UTP does not have to worried about DNS DDOS anymore as DNSVault is protected by built in sophisticated IPS firewall. This automatic protection combine with rate limiting features in BIND 9 will surely destroy the hopes of the hackers that tries to DDOS DNSVault. Dual stack DNS Server which is involves running IPv4 and IPv6 at the same time. End nodes and routers/switches run both protocols, and it will be easier to try to run everything in a dual-stack mode.