CASE STUDY

ORGANIZATION :
Bank Simpanan Nasional

DOMAIN :
mybsn.com.my

INDUSTRY :
Banking

UNIT PURCHASE :
6 Units

RESULT :

- **Better response time and highest reliability for the DNS services.**

- **Advance DNS protection.**

- **Provide the best reliability and client does not experience any timeout issues**.

PROJECT OVERVIEW

Bank Simpanan Nasional (BSN) is a government owned bank in Malaysia, which has more than 5,100 employees, 382 branches and 621 automatic teller machine (ATM) nationwide. More than 7 million customers spread throughout the country and with savings account worth more than RM 8 billion.

CHALLENGE

The availability of transaction and banking services is the crucial part in maintaining the best user experience to the customer. Online banking is one of the most important services that every bank does not tolerate downtime. Even a simple DNS malfunction can cause a lot of customer dissatisfaction. Previous DNS server use by BSN is based on Microsoft DNS and the reliability of server does not meet the quality they wanted. With more than 7 million customers and multiple e-banking services, this translated to almost 70,000 query everyday. With the high volume of query everyday, standard Microsoft DNS server would not stand a chance, causing the server need to be rebooted once a week to refresh the DNS service.

Besides the unreliability of the DNS service, Microsoft DNS is plagued with many security problems and malware attack. Without the comprehensive protection and advance security hardening Microsoft DNS is waiting to be attacked by hackers and the likes. A simple DNS attack can cause a serious effect to the reliability of other online services which depend to the DNS.

Same issues also happen to the internal DNS server for BSN. To complicate the matters, the internal DNS server is also the Active Directory server, which handle more service and the reliability of the server is already critical. As we all know, Microsoft DNS does not have any protection or High Availability for its DNS server. If one of the DNS server is down, the client will take some time to change the DNS lookup to the secondary DNS server. The timeout waiting for the resolving process to resolve to the secondary DNS server will definitely slow down a lot of the work done by the BSN staff.

SOLUTION

Within two months of PoC (Proof of Concept), all problems that have plagued Microsoft DNS server is alleviated. The system admin also reported better response time and performance, furthermore he does not have to restart any DNS service anymore. DNSVault itself is already tune and harden to provide the best performance and highest reliability for the DNS services so 10,000,000 queries per day is normal. Plus with the advance DNS protection any hacker that tries to attack DNSVault server will be automatically block for certain duration of time.

With the rate limiting technology DNSVault will normalize response to the single IP that trying to attack the server indirectly give more reliability when the server is under attack and also break the attempt of an attack. Extra feature like DNS query graph and live DNS query is an added bonus for the server administrator, where with this data, system admin is able to analyze the DNS traffic and further improved the their e-banking facility.

For internal DNS, DNSVault has taken over the burden for the Active Directory server as a DNS server and specially with BSN DNSVault was able to reroute Active Directory (AD) request back to the AD server. For internal DNS, DNSVault is configured in High Availability mode. If something bad happens to one of the server, the other server will automatically take over the IP of the server that have a problem. This provide the best reliability and client does not experience any timeout issues. For added security, DNSSEC Validation is enabled as recursive queries so all DNSSEC enabled domain will be validated for authenticity. BSN is also planning to enable DNSSEC to all its domain within the year 2015. By enabling DNSSEC, all BSN domains will benefit with the added security to the domain.