HOW TO MAKE SURE YOU HAVE ROCK SOLID DNS

Checklist

MUST DO:

Be global and local

Use a DNS service with a strong global footprint and a good spread of sites in the regions most important to your business. Make sure the Service Level Agreement (SLA) ensures high availability and a sufficient minimum number of available sites at all times.

Don't rely on a single solution

Using just one type of DNS solution exposes you to a high risk of failure. Use multiple solutions to guarantee 100% uptime.

Use DNSSEC to protect your domains

The DNSSEC (DNS Security Extensions) protocol has been around for more than a decade. It uses digital signatures to enable DNS records to be authenticated and is the industry standard for protecting against DNS hijacking and man-in-the-middle (MITM) attacks. Making sure your domains are protected by DNSSEC is a vital part of your network security.

HIGHLY RECOMMENDED:

Choose an organisation with long experience and high competence

DNS is business critical. When choosing a provider, look for an organisation that has a high level of DNS expertise, a proven track record of running a highly available global service, and the competence to help tailor a DNS solution to meet your specific network needs.

Ensure relevant statistics and measurements are provided

When looking for a provider, make sure they provide the relevant statistics in a way that is simple to use. For daily operations and troubleshooting, you need access to data from all sites preferably via an API that can be integrated into your system.

Use DNS anycast to protect your online presence

Using DNS anycast is one of the best things you can do to protect your online presence against Distributed Denial of Service (DDoS) attack and other possible outages. Anycast enables multiple instances of a name server to be distributed across the world. If one instance is unavailable, the system automatically reroutes queries to the best available location.

Follow security best practice

There are a range of tools that help keep domains secure. Using registration features like Registry Lock can protect domain names from being changed, while using classic access control lists helps protect applications, Internet traffic and monitoring tools.