# Protecting DNS Servers from Denial of Service Threats

Typically, DNS servers only provide DNS services to machines within a trusted domain. Restricting recursion and disabling the ability to send additional delegation information can help prevent DNS-based DoS attacks and cache poisoning. It can also improve performance on your network by reducing the vulnerability of your DNS servers to use as a reflector in such an attack. The following US-CERT recommendations provide guidance on mitigating this threat.

Included in this ZIP file are:
- Intro Page.pdf
- Terms and Conditions.pdf
- The Continuing Denial of Service Threat Posed by DNS Recursion.pdf