Securing TP-Link Routers Against Open DNS Server Operation

Introduction

Many ISPs, including Cerberus Networks have experienced and at the time of writing are still experiencing some level of Distributed Denial of Service (DDoS) attack on their DNS servers due to a widespread worm virus that has infected many computers on the Internet. DNS is used to resolve Internet names (e.g. www.google.com) into a IP address that your computer can then use to contact the server. A full explanation of the issue, as well as how you can protect your systems against the attack, can be found here:

http://www.us-cert.gov/ncas/alerts/TA13-088A

Some TP-Link routers which Cerberus has supplied with is ADSL2+ services, when configured in No-NAT mode, are vulnerable to attack. The simple fix below will prevent these routers from operating as an open DNS server.

Solution

You should configure a filter rule to block inbound access on port 53 as below:

The source IP filter is not effective so leave it set to all 0.0.0.0/0.0.0.0. Please note the “**direction**” has to be “**Incoming**” only or the outgoing DNS requests service will be blocked.

The Firewall and the ACL features can still stay disabled and we do not recommend enabling them.