

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:

Access Management
Quick Start
Interface Setup
Advanced Setup
Access Management
Maintenance
Status
Help

ACL
Filter
SNMP
UPnP
DDNS
CWMP

Filter

Filter Type

Filter Type Selection : IP / MAC Filter

IP / MAC Filter Set Editing

IP / MAC Filter Set Index : 1

Interface : PVC0

Direction : Incoming

IP / MAC Filter Rule Editing

IP / MAC Filter Rule Index : 1

Rule Type : IP

Active : Yes No

Source IP Address : 0.0.0.0 (0.0.0.0 means Don't care)

Subnet Mask : 0.0.0.0

Port Number : 0 (0 means Don't care)

Destination IP Address : 0.0.0.0 (0.0.0.0 means Don't care)

Subnet Mask : 0.0.0.0

Port Number : 53 (0 means Don't care)

Protocol : UDP

Rule Unmatched : Next

IP / MAC Filter Listing

		IP / MAC Filter Set Index	Interface	PVC0	Direction		Incoming
#	Active	Src Address/Mask	Dest IP/Mask	Src Port	Dest Port	Protocol	Unmatched
1	Yes	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	0	53	UDP	Next
2	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-

SAVE
DELETE
CANCEL

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.