设置 FortiGate DNS 数据库

说明：

本文档针对所有 FortiGate 设备的 DNS 数据库配置进行说明。DNS 数据库可以让管理员在防火墙上手工设置一些域名对应的 IP 地址，已实现控制访问 某些域名的目的。当防火墙后面的 PC 把 dns 服务器地址设置为内网接口地址后，PC 的 dns 请求先在 DNS 数据库中查找，有则返回数据库中的 IP；如果没 有可以选择丢弃该请求或将它转发到公网 dns 服务器上。

环境介绍：

本文使用 FortiGate310B 做演示。本文支持的系统版本为 FortiOS v4.0 MR1。

步骤一： 配置 DNS 服务器

在系统管理----网络----选项中设置防火墙的 DNS 服务器地址

步骤二：配置接口

在系统管理----网络----接口中编辑内网接口，勾选允许从此端口进行 DNS 查询

Recursive：先在防火墙 DNS 数据库中查找域名，如果没有匹配则将请求发给步骤一中的 DNS 服务器查询。

Non-recursive :在防火墙 DNS 数据库中查找域名 ,如果没有匹配则丢弃请求。

本例选择 Recursive

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

步骤三：配置 DNS 数据库

在系统管理----网络----DNS 数据库中点击新建，下面以 test.com 为例

域名：最好写一级域名例如 test.com

TTL：存储的有效时间

点击 OK，然后点击新建，创建一条 dns 记录

类型：防火墙支持 IPV4（地址 A），IPV6，NS 记录，CNAME 记录，MX 记录，

本例选 IPV4 地址

主机名：该域的详细域名

IP 地址：该主机名解析的 IP

TTL：存储的有效时间，为 0 则使用整个记录的 TTL

下图为写好的三条记录 ,即将 www.test.com 解析为 10.0.0.1 将 mail.test.com

解析为 10.0.0.2；将 news.test.com 解析为 10.0.0.3

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255

下面以 163.com 为例说明将一级域名解析为 IP 地址，创建域名为 163.com 的 dns 区域

在 dns 记录中将主机名设为 163.com，并给出 IP 地址。则只有 163.com 可以被解析，所有 163.com 的二级和二级以下域名都不能被解析。

步骤四：测试

将 PC 的 dns 服务器地址设置为防火墙内网地址，在 windows 的 cmd 中 ping 相应的域名看能不能解析出ＩＰ。

清除 PC dns 缓存的命令（在 cmd 中）：ipconfig /flushdns

北京市海淀区北四环西路 52 号方正国际大厦 12 层 电话: (010)62960376/4006005255