# FortiGate-v5.0-GTSM 通用 TTL 安全保护机制

| | |
|---|---|
| 版本 | 1.0 |
| 时间 | 2015 年 1 月 |
| 支持的版本 | FortiOS v5.0.x 以后版本 |
| 作者 | 黄豪赫 |
| 状态 | 已审核 |
| 反馈 | support_cn@fortinet.com |

# 目　录

# 简介

当今网络世界中，网络攻击行为变得十分常见，每天在公网都有大量的基于IP 的网络扫描，因此网络设备安全变得尤为重要。RFC5082 介绍了一种基于 IP TTL 字段的安全机制，目的是为了保护网络设备安全。FortiOS v5.0 以上版本支持 GTSM 安全保护机制，基于端口接收或拒绝指定的 TTL 范围的数据包，从而防止不受信任的数据包抵达设备。

本文主要简述 RFC5082 的实现机制和 FortiGate 上的相关配置和相关测试。

# 通用 TTL 安全保护机制介绍

RFC 5082 定义了通用 TTL 安全保护机制 Generalized TTL Security Mechanism (GTSM)，目的是保护网络设备控制平台 CPU 利用率，防止基于 IP 网络的 DDOS 攻击造成设备 CPU 利用率过载及系统崩溃。

在 IP 报文包头中，TTL(Time To Live)字段用于指定 IP 包被路由器丢弃之前允许通过的最大网段数量。而网络设备中，协议相关的数据包大部分和网络邻接设备交互。通用 TTL 安全保护机制(GTSM)通过指定 TTL(Time To Live)值的范围允许进入网络设备的数据包，防止 IP 欺骗，保护设备资源。

FortiGate 在 5.0 以上版本支持，通用 TTL 安全保护机制目的在于保护网络设备 CPU，仅对设备的控制平面起作用，意味着对穿越防火墙的业务流量不起效果。

# 相关组件

FortiGate 防火墙。

# 参考文档

《RFC 5082 The Generalized TTL Security Mechanism (GTSM)》

《FortiOS Handbook What’s New for FortiOS 5.0》

# FortiGate 相关命令介绍

配置步骤：

- 需要定义 ttl-policy 策略
- 需要定义源接口、地址组、服务和调用的时间表
- 定义 ttl 的取值范围
- 定义策略动作

配置案例：

```
config firewall ttl-policy
    edit 1
        set action accept
        set srcintf "port2"
        set srcaddr "ddos"
        set service "ALL"
        set schedule "always"
        set ttl 100-200
    next
end
```

# 测试拓扑图

# 测试内容

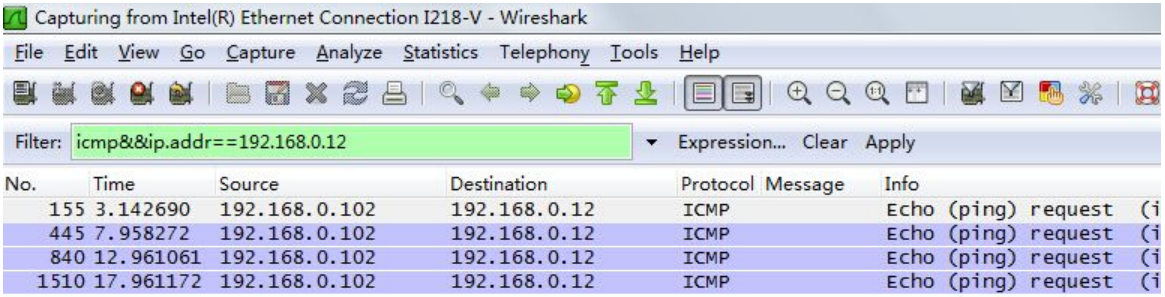
1. FortiGate 上 Port1 拒绝从 PC1 IP 地址为 192.168.0.102 ttl=64 的 icmp request 数据包。

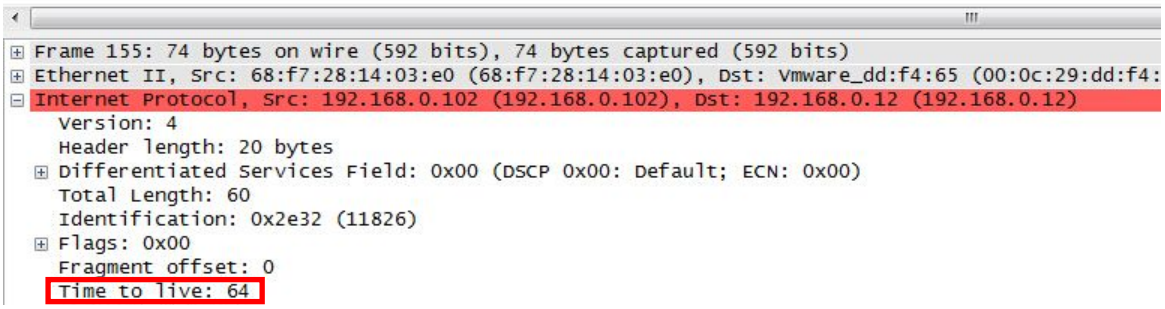
   FortGate 配置如下：

```
config firewall ttl-policy            //进入 ttl-policy 配置//
    edit 1                            //定义名规则 1 的策略//
        set srcintf "port1"           //定义策略使用的源端口//
        set srcaddr "all"             //定义地址本//
        set service "PING"            //定义服务内容//
        set schedule "always" //定义策略调用时间表//
        set ttl 64                    //定义 ttl 的取值范围//
    next
end
```

   **注:缺省的动作为 deny**

2. 从 PC1 上抓包，PC 发送 ttl=64 echo request 的 icmp 请求包，防火墙收到数据包后，配置到 ttl-policy 策略，将其丢弃。




防火墙打开 debug 后，检测到 ttl-policy 策略，将其丢弃：

```
id=0 trace_id=908 msg="vd-root received a packet(proto=1,
192.168.0.102:1->192.168.0.12:8) from port1. code=8, type=0, id=1, seq=4476."
id=0 trace_id=908 msg="allocate a new session-0003116a"
id=0 trace_id=908 msg="iprope_in_check() check failed on policy 0, drop"
```