DDoS 云高防服务

操作手册

Radware

目 录

1 配置目标.....3
2. Portal 配置检查.....3
2.1 登陆高防管理 Portal 账号.....3
3 GRE tunnel 的连通性.....4
3.1 回源通道 GRE.....4
4 代播网段配置.....4
4.1 配置说明.....4
4.2 配置步骤.....4

1 配置目标

检查 Cloud DDOS 按需服务的配置，与设计预期一致，有下面几个检查项

1. Portal 配置和静态路由
2. Tunnel 状态
3. 网段代播情况

回源方式:

节点 GRE 隧道，4 条（2 个数据中心各有 2 台出口路由器，主备 2 条线路）

（Radware 准备了东京节点，作为 XX 节点的地理容灾）

2. Portal 配置检查

2.1 登陆高防管理 Portal 账号

a) 查看 Asset 配置状况

每个网段是一个 asset，检查:

代播网段 IP 和数量和配置 asset 一致，Asset 的状态是 off-cloud

b) 查看 site 配置情况

清洗中心 Location 是 HKG （TKO 是东京，预留为地理容灾使用）

Connections： GRE 的 IP 和数量

清洗流量回源：机房 1：有 2 条 tunnels，主备 HA

清洗流量回源：机房 2：有 2 条 tunnels，主备 HA

3 GRE tunnel 的连通性

3.1 回源通道 GRE

在 RadwareXX 清洗中心与客户 2 个机房：机房 1 和机房 1，分别建立 2 个 GRE 隧道，共 4 个 GRE tunnels

下图是 tunnel 的示意图，除了 tunnel 的公网地址，要关注私有地址情况

Radware 和 客户 互 ping ： 对方公网 IP / 对方私有 IP / MTU 1470

Radware 侧已完成：静态路由正确设置，即不同网段送入不同机房的隧道

4 代播网段配置

4.1 配置说明

这个配置是模拟攻击发生时操作，牵引过程涉及互联网路由收敛，这个过程对生产业务可能会有影响，建议如下

a) 在维护窗口进行

b) 选择业务量小的网段 并有 IP 可供 ping 配置

4.2 配置步骤

配置前准备，信息收集：

1. 选择配置网段：x.x.x.x
2. 登陆互联网 looking Glass 查看互联网上的路由情况 show ip bgp
3. 选择配置网段一个 IP

4. 登陆互联网进行 ping 配置，验证配置 IP 连通性和时延
5. 收集上述配置数据

Cloud DDoS 高防服务，按需牵引到 Radware 配置：

1. 登陆 Radware portal，把具体/24 网段对应 asset 进行激活对外代播，点击 Activity 按键
2. Radware 对外代播成功转为 on-cloud 状态 ，互联网上 BGP 收敛时间 3 分钟不等。
3. 客户出口路由器上停止该/24 网段对 ISP 的广播
4. 登陆互联网 looking Glass 查看互联网上的路由情况 show ip bgp
5. 登陆互联网进行 ping 配置，验证配置 IP 连通性和时延
6. 收集上述配置数据.

Cloud DDoS 高防服务，按需牵引回客户机房的配置：

1. 客户出口路由器上恢复对该/24 网段对 ISP 的广播
2. 登陆 Radware portal，把具体/24 网段对应 asset 进行“去激活”停止对外代播，点击 Deactivity 按键
3. Radware 对外代播成功转为 off-cloud 状态 ，互联网上 BGP 收敛时间 3 分钟不等。
4. 登陆互联网 looking Grass 查看互联网上的路由情况 show ip bgp
5. 登陆互联网进行 ping 配置，验证配置 IP 连通性和时延
6. 收集上述配置数据.

<本文结束>