某局点使用域间策略阻断某域名访问不成功案例

域间策略/安全域 卢鹏 2018-11-17 发表

组网及说明

无

问题描述

某局点客户配置基于域名的地址对象组，然后在域间策略里阻断该地址的访问，测试未能成功。

过程分析

测试发现终端访问该域名解析得到的地址和防火墙上解析该域名得到的ip地址不一样，防火墙上如果配置了域名的安全策略，防火墙就向DNS服务器发起一个DNS请求，获取域名对应的IP地址，保存起来，然后域间策略会把基于域名的策略转换成基于IP地址的策略，后续就是普通的基于IP的域间策略匹配。也就是说通过放通或阻断这个IP地址来达到访问控制的目的。当防火墙上DNS表项老化时，防火墙重新发起DNS查询，重新保存DNS表项，重新刷新安全策略。

因为终端访问该域名解析得到的地址和防火墙上解析该域名得到的ip地址不一样，所以防火墙未对该域名访问进行阻断。

如果配置了基于域名的对象组，防火墙上马上就出现了dns host表项，这是防火墙自身向DNS服务器发请求得到的地址，老化时间根据DNS服务器返回的DNS应答携带的老化时间决定（TTL）。

```
[H3C]display dns host
Type:
  D: Dynamic    S: Static

Total number: 1
No.  Host name            Type  TTL      Query type  IP addresses
1    www.sina.com.cn       D    44       A           115.238.190.238
```

比如配置安全策略禁止访问www.sina.com.cn ，用户在访问www.sina.com.cn 首先向DNS服务器发送DNS请求，然后能得到DNS解析的地址（如115.238.190.238），之后访问地址115.238.190.238的时候被防火墙阻断。

解决方法

建议内网pc和防火墙配置同一个dns服务器地址，否则同一个域名可能解析出来不同的地址，影响到策略匹配，或者内网pc把DNS指向防火墙，防火墙做DNS代理。