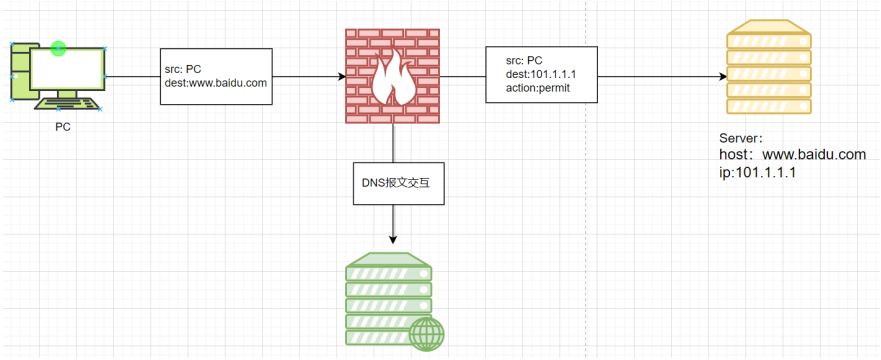
防火墙配置基于域名的安全策略原理详解

ACL　域间策略/安全域　孔凡安　2024-01-03 发表

组网及说明

简化组网如下



配置步骤

防火墙配置基于域名的安全策略：

方案一：直接在设备上配置域名对象组，并在安全策略中调用该对象组。设备检测到基于host name的对象组配置之后，会主动向dns server解析请求该域名对应的IP地址。表项老化后再次解析。

示例如下：

```
#
object-group ip address baidu
 0 network host name www.baidu.com
#
 dns server 10.158.2.10       ----dns server必须配置，否则设备无法解析到地址对象组中域名对应的IP
#
```

该方案配置简单，由于设备上本质还是基于IP做安全策略检查，因此需要确保终端和设备本身关于域名的解析结果一致。可以使用如下命令查看解析结果：

```
RBM_P<F5080D_1>disp dns host
Type:
  D: Dynamic    S: Static

Total number: 1
No.  Host name          Interface    Type  TTL     QType  IP addresses
1    www.baidu.com      -            D     3146    A      101.1.1.1            ----确保设备上解析结果和终端解析结果一致

RBM_P<F5080D_1>disp object-group ip host object-group-name baidu
Object group       : baidu
  Object ID        : 0
    Host name      : www.baidu.com
    VPN instance   : -
    Updated at     : 2024-01-03 15:43:04
    IP addresses   :
      101.1.1.1
```

需要注意的是，如果设备不做DNS代理，即终端的DNS指向单独的DNS服务器而非设备，是无法针对于模糊域名（例如*.baidu.com）做安全策略限制的。由此引出方案二。

方案二：设备做DNS代理，终端的DNS指向FW设备。FW设备需要增加配置如下：

```
#
 dns proxy enable       ---开启dns代理功能
```

```
#
```

现网实际使用中，以上方案可能遇到如下问题：
1. 域名老化的太快。终端的访问是持续的，其域名对应的IP没有变化。但是设备上重新解析得到的IP是新的，两边不匹配。
解决方案：可以尝试配置*dns cache ttl*命令调整域名表项老化时间。
2. 终端和设备关于某个域名的解析结果不一致，导致策略无法通过。
解决方案：该问题和DNS服务器行为有关，针对终端和FW设备的DNS请求返回不同的解析结果。可以尝试设备上配置DNS代理解决。

配置关键点

FW本质是基于IP匹配安全策略，需要保证终端DNS的解析结果和FW设备一致。
如果按照以上调整仍不能解决现网问题，可以尝试配置dns snooping功能（老版本不支持）。
机制实现参考案例：配置dns snooping功能实现防火墙基于域名的安全策略原理分析