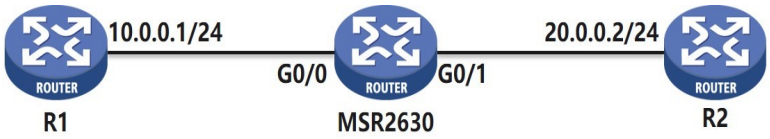
MSR2630上网行为管理功能不生效问题经验案例

特征库　攻击防范及检测　郭昊　2019-03-27 发表

组网及说明



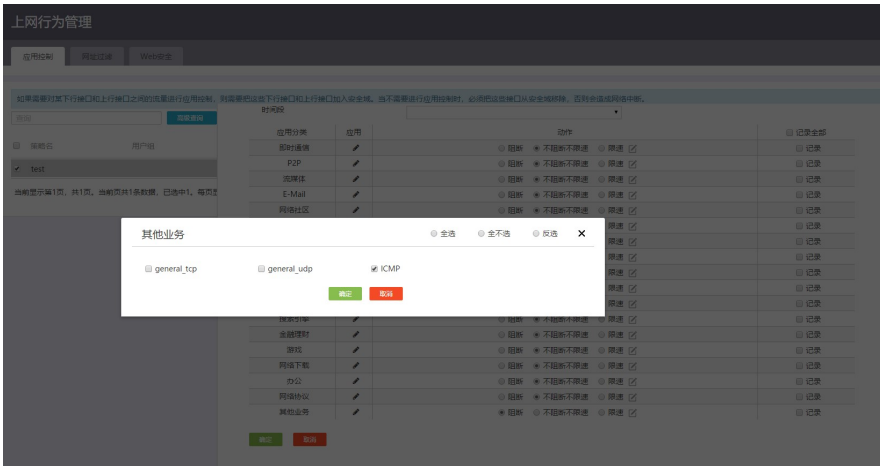
客户使用MSR2630设备作为网关，启用上网行为管理功能，对内网用户访问外网的流量进行监控和管理。

问题描述

以上图组网为例，MSR2630启用上网行为管理禁止R1 ping R2后，ping的流量还可以通，上网行为管理功能没有生效。

过程分析

先检查配置。对于此类应用场景，客户配置上网行为管理大多是通过WEB来配置的（命令行配置相对比较复杂），因此先检查WEB的配置。配置很简单，除了ICMP，其他所有应用均放通。



上网行为管理实际上是通过域间策略来实现的，因此需要看下接口是否在正确的安全域中。查看域防火墙部分的配置，内网口G0/0、外网口G0/1分别在安全域Trust、Untrust中，没有问题。

这里有一个需要注意的地方，就是设备上配置了Trust和Untrust域之间的全放通策略。按照一般情况理解，域防火墙和上网行为管理好像是两个功能，应该有类似于“与”的关系，即流量既要被域防火墙放通，也要被上网行为管理放通，这样才能通。但实际上这里是有问题的。我们来看一下对应命令行的配置，就可以理解这个问题的原因了。

上述WEB配置，对应下发到设备命令行的配置如下。可以看到上网行为管理过滤icmp的app group是调用在Any-Any这个object policy里面，最后下发在Any到Any的域间策略中。而域防火墙对应的域间策略则是下发在Trust和Untrust这两个明细的域之间。

当前MSR G2域间策略的实现是，对域间流量先检查是否有明细的策略，即Trust到Untrust，或者Untrust到Trust之间的策略，如果没有明细策略，则检查是否匹配了Any到Any的域间策略。

对于现网这例配置，流量会直接按照Trust到Untrust的策略rull 0 pass直接放通，不会再检查是否匹配上网行为管理，导致icmp过滤不生效。

```
#
object-policy ip Any-Any
 rule 0 drop app-group test_142
 rule 1 inspect test
 rule 65534 pass
#
object-policy ip Trust-Untrust
 rule 0 pass
#
object-policy ip Untrust-Trust
 rule 0 pass
#
security-zone name Trust
 import interface GigabitEthernet0/0
#
security-zone name Untrust
 import interface GigabitEthernet0/1
#
zone-pair security source Any destination Any
 object-policy apply ip Any-Any
#
zone-pair security source Trust destination Untrust
 object-policy apply ip Trust-Untrust
#
zone-pair security source Untrust destination Trust
 object-policy apply ip Untrust-Trust
#
app-group test_142
 description "User-defined application group"
 include application ICMP
#
url-filter policy test
 default-action permit
#
```

同样的道理，如果域防火墙配置的阻断，无论上网行为管理是否放通，流量都会被域防火墙过滤掉。

如果上图中域防火墙配置部分，写了Trust到Untrust的明细策略，但是没有勾选启用（没有生效），这种情况也会有问题。因为实际生成的配置如下，相当于设备上有Trust到Untrust的策略，但策略没有将流量放通，无论上网行为管理如何配置，此处流量都会被过滤。

```
#
object-policy ip Trust-Untrust
 rule 0 pass disable
#
object-policy ip Untrust-Trust
 rule 0 pass disable
#
```

解决方法

将域防火墙的Trust到Untrust等明细的域间策略删除，流量才可以正常匹配到Any to Any域间策略中的上网行为管理。