MSR系列路由器内存高问题处理参考

内存 刘昳 2024-08-15 发表

问题描述

当MSR存在攻击扫描导致内存升高时，可以通过配置防御攻击控制设备内存

解决方法

```
#
interface GigabitEthernet0/1
port link-mode route
ip address 20.x.x.10 255.255.0.0
attack-defense apply policy test1
#
```

配置1：

```
#
attack-defense policy test1
scan detect level low action drop logging
#
 [H3C-attack-defense-policy-test1]dis ip fa c
Total number of fast-forwarding entries: 504543
 [H3C-attack-defense-policy-test1]dis ip fa c
Total number of fast-forwarding entries: 588978
```

配置2：

```
#
attack-defense policy test1
scan detect level high action drop
#

[H3C-attack-defense-policy-test1]dis ip fa c
Total number of fast-forwarding entries: 24400
```

附录命令行说明：

scan detect命令用来配置开启指定级别的扫描攻击防范。

undo scan detect命令用来关闭指定级别的扫描攻击防范。

【命令】

scan detect level { { **high** | **low** | **medium** } | **user-defined** { **port-scan-threshold** *threshold-value* | **ip-sweep-threshold** *threshold-value* } * [**period** *period-value*] } **action** { { **block-source** [**timeout** *minutes*] | **drop** } | **logging** } *

undo scan detect

【缺省情况】

扫描攻击防范处于关闭状态。

【视图】

攻击防范策略视图

【缺省用户角色】

network-admin

mdc-admin

vsys-admin

【参数】

level：指定攻击防范的检测级别。

high：表示高防范级别，该级别能检测出大部分的扫描攻击，但对活跃主机误报率较高，即将可提供服务的主机的报文错误判断为攻击报文的概率比较高。该级别的扫描攻击检测周期为10秒，针对端口扫描的防范阈值为5000 packets，针对地址扫描的防范阈值为5000 packets。

low：表示低防范级别，该级别提供基本的扫描攻击检测，有很低的误报率，但对于一些扫描攻击类型不能检出。该级别的扫描攻击检测周期为10秒，针对端口扫描的防范阈值为100000 packets，针对地址扫描的防范阈值为100000 packets。

medium：表示中防范级别，该级别有适中的攻击检出率与误报率，通常能够检测出Filtered Scan等攻击。该级别的扫描攻击检测周期为10秒，针对端口扫描的防范阈值为40000 packets，针对地址扫描的防范阈值为40000 packets。

user-defined：表示用户自定义防范规则，用户可根据网络实际情况和需求指定端口扫描、地址扫描的

防范阈值和检测周期。

port-scan-threshold *threshold-value*：指定端口扫描攻击防范的触发阈值。其中，*threshold-value*为源IP地址每个检测周期内发送的目的端口不同的报文数目，取值范围为1～1000000000。

ip-sweep-threshold *threshold-value*：指定地址扫描攻击防范的触发阈值。其中，*threshold-value*为源IP地址每个检测周期内发往不同目的IP地址的报文数目，取值范围为1～1000000000。

period *period-value*：表示检测周期，*period-value*的取值范围为1～1000000000，单位为秒，缺省值为10。

action：设置对扫描攻击的处理行为。

block-source：表示阻断并丢弃来自该IP地址的后续报文。具体实现是，当设备检测到攻击发生后，会自动将发起攻击的源IP地址添加到IP黑名单动态表项中，当接口或安全域上的黑名单过滤功能处于开启状态时，来自该IP地址的报文将被丢弃。

timeout *minutes*：动态添加的黑名单表项的老化时间。其中，*minutes*表示老化时间，取值范围为1～10080，单位为分钟，缺省值为10。

drop：表示丢弃攻击报文，即设备检测到攻击发生后，由该攻击者发送的报文都将被丢弃。

logging：表示输出告警日志，即设备检测到攻击发生时，生成记录告警信息，生成的告警信息将被发送到日志系统。

【使用指导】

要使扫描攻击防范添加的IP黑名单动态表项生效，必须保证接口或安全域上的黑名单过滤功能处于开启状态。

对于扫描攻击防范动态添加的黑名单，需要配置其老化时间大于扫描攻击的统计周期。

输出告警日志功能开启后，设备生成的告警日志信息不会输出到控制台和监视终端，可通过执行**display logbuffer**命令进行查看。有关**display logbuffer**命令的详细介绍，请参见“网络管理和监控命令参考”中的“信息中心”。

【举例】

在攻击防范策略atk-policy-1中配置扫描攻击的检测级别为低级别，处理行为是丢弃后续报文。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action drop
```

在攻击防范策略atk-policy-1中配置扫描攻击的检测级别为低级别，处理行为是发日志，阻断并丢弃来自该IP地址的后续报文，并设置添加的IP黑名单表项的老化时间为10分钟。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level low action logging block-source timeout 10
```

在攻击防范策略atk-policy-1中配置扫描攻击的检测级别为用户自定义，端口扫描防范阈值是6000 packets，地址扫描防范阈值是80000 packets，检测周期是30秒，处理行为是发日志，阻断并丢弃来自该IP地址的后续报文，并设置添加的IP黑名单表项的老化时间为10分钟。

```
<Sysname> system-view
[Sysname] attack-defense policy atk-policy-1
[Sysname-attack-defense-policy-atk-policy-1] scan detect level user-defined port-scan-threshold 6000 ip-sweep-threshold 80000 period 30 action logging block-source timeout 10
```

【相关命令】

- **blacklist enable**
- **blacklist global enable**