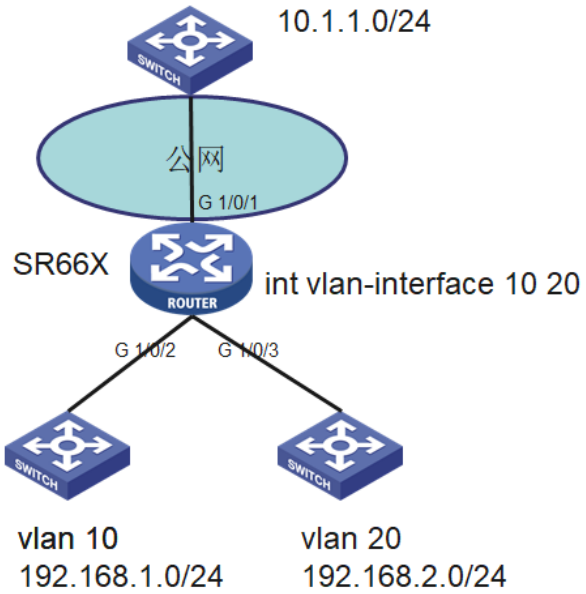
某局点V5 SR66X路由器阻拦443端口不生效故障排查案例

firewall packe packet-filter ACL 吴川云 2021-01-31 发表

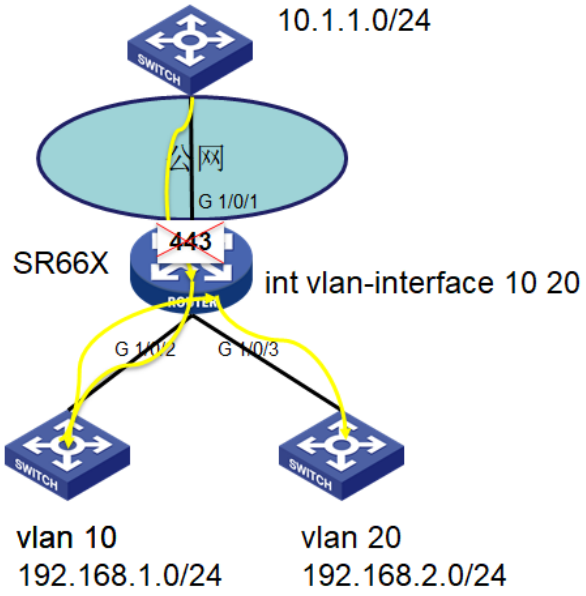
组网及说明



vlan10和vlan20的网关部署在路由器上，1/0/1为公网出口，其余接口为内网接口；
设备版本为Version 5.20.106, Release 3303P21；

问题描述

客户需求：禁止公网的主机访问内网vlan 10 和vlan 20内所有主机的443端口，内网主机可以访问公网和内网其他主机的443端口；



故障现象描述：公网的主机能正常访问到内网主机的443端口，内网主机无法互访443端口，与客户需求不符。

过程分析

首先，针对V5的SR6600-X路由器，需要检查是否配置了firewall enable，使能防火墙功能；若为独立运行非IRF模式，需使能防火墙的全部槽位；若为IRF模式，需使能指定框位或全部框位的防火墙功能；

```
[SR66X]firewall enable ?
  all      Configure all the slot
  chassis  Specify the chassis number
```

在开启上述命令以及现场配置包过滤后，发现外网可访问内网主机的443端口，内网主机均不可访问其余主机的443端口；

查看在V5防火墙上的包过滤配置：

```
#
acl number 3000
 rule 10 deny tcp destination-port eq 443
#
interface GigabitEthernet1/0/1
 port link-mode route
 firewall packet-filter 3000 outbound
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
 firewall packet-filter 3000 inbound
#
interface Vlan-interface20
 ip address 192.168.1.1 255.255.255.0
 firewall packet-filter 3000 inbound
```

按照上述的配置，实现的逻辑如下：任何tcp源端口字段为443的数据包，都会被在外网接口的入方向和内网网关的出方向上进行阻断。

客户需求是外网的主机无法访问固定的443端口，首先我们需要知道流量是从外网的接口的**入方向**进入，且转发的方向为对应网关接口的**出方向**。需在正确的接口对正确的流量方向进行阻拦；上述的配置是将外网接口的出方向的443目的端口，内网官网的入方向的443目的端口进行阻拦。因此外网主机的443端口访问无法被阻拦，而内网主机的443端口访问会被阻拦掉。

解决方法

修改外网接口配置匹配入方向，可以将外网访问的443目的端口的来向流量进行过滤；

```
interface GigabitEthernet1/0/1
 port link-mode route
 firewall packet-filter 3000 inbound
```

修改内网网关配置匹配出方向，可以将去往网关下的443目的端口的去向流量进行过滤，但是同时会将内网互访的443端口的数据进行阻拦，因此需要将内网主机网段的443端口先在ACL中放通，再匹配需要阻拦的443端口。

```
#
acl number 3000
 rule 10 permit tcp source 192.168.0.0 0.0.3.255  destination-port eq 443
 rule 20 deny tcp destination-port eq 443
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
 firewall packet-filter 3000 outbound
#
interface Vlan-interface20
 ip address 192.168.1.1 255.255.255.0
 firewall packet-filter 3000 outbound
```

对于匹配的原理，理解下面两点：

1. 实现对访问内网主机的443端口的阻拦，因为要访问的是主机的443端口，目的端口为固定的443端口，而源端口不固定。因此在设置ACL的规则时，需注意设置的为目的端口；如果数据为双向交互，即被访问的主机会通过固定的端口进行回包，则发回的数据以源端口则是源端口固定，目的端口不固定的方式。以telnet为例，以固定的23目的端口进行访问，回包为固定的23源端口。因此需要针对数据包的特性进行阻拦：

Source	Destination	Protocol	sr-port	ds-port
1.1.1.1	2.2.2.2	TELNET	64525	23
2.2.2.2	1.1.1.1	TCP	23	64525

2. 针对阻断外网访问内网的主机的443端口，而放通内网主机之间的443端口的互访需求，可以通过在ACL的阻断端口的rule前添加放行的rule，以达到内网互访的需求，例：

```
rule 10 permit tcp source 192.168.0.0 0.0.3.255  destination-port eq 443
rule 20 deny tcp destination-port eq 443
```

有多个阻断端口的需求，后面rule禁止了多少个端口，前面的rule就添加相应个数的互访网段permit的端口；