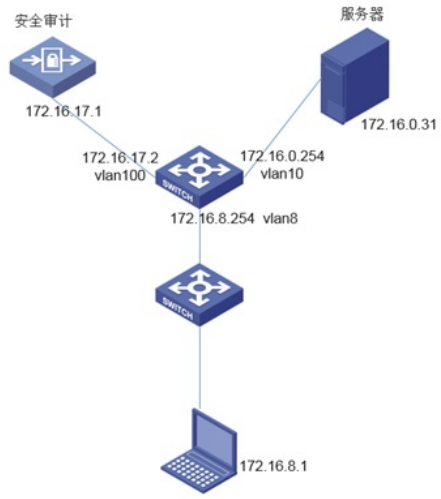
S7500E交换机策略路由转发不通经验案例

策略路由 孙兆强 2019-10-30 发表

组网及说明



用户、安全审计设备和服务器的网关都在网关交换机上。

问题描述

PC访问服务器的流量要到安全审计设备上绕行一圈，网关上配置策略路由将来回流量都引到安全审计设备上。但是配置策略路由后无法访问服务器。

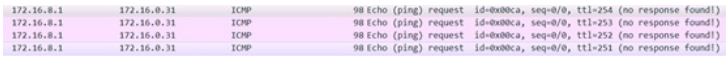
```
policy-based-route back permit node 6
 if-match acl 2001
 apply next-hop 172.16.17.1
#
policy-based-route in permit node 5
 if-match acl 2000
 apply next-hop 172.16.17.1
#
acl basic 2000
 rule 0 permit source 172.16.8.0 0.0.0.255
#
acl basic 2001
 rule 0 permit source 172.16.0.0 0.0.0.255
#
interface Vlan-interface8
 ip address 172.16.8.254 255.255.255.0
 ip policy-based-route in
#
interface Vlan-interface10
 ip address 172.16.0.254 255.255.255.0
 ip policy-based-route back
```

过程分析

在pc上tracert服务器地址发现流量一直在安全设备和网关之间来回。

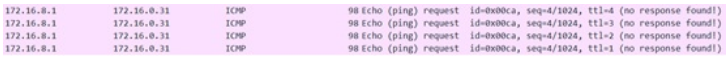
```
<pc>tracert 172.16.0.31
traceroute to 172.16.0.31 (172.16.0.31), 30 hops at most, 40 bytes each packet, press CTRL_C to br
eak
 1  172.16.8.254 (172.16.8.254)  1.000 ms  2.000 ms  0.000 ms
 2  172.16.17.1 (172.16.17.1)  1.000 ms  1.000 ms  1.000 ms
 3  172.16.17.2 (172.16.17.2)  1.000 ms  1.000 ms  1.000 ms
 4  172.16.17.1 (172.16.17.1)  1.000 ms  1.000 ms  2.000 ms
 5  172.16.17.2 (172.16.17.2)  2.000 ms  4.000 ms  2.000 ms
 6  172.16.17.1 (172.16.17.1)  1.000 ms  1.000 ms  2.000 ms
 7  172.16.17.2 (172.16.17.2)  1.000 ms  1.000 ms *
 8  172.16.17.1 (172.16.17.1)  3.000 ms  3.000 ms  1.000 ms
 9  * 172.16.17.2 (172.16.17.2)  3.000 ms  3.000 ms
10  172.16.17.1 (172.16.17.1)  3.000 ms  2.000 ms  3.000 ms
```

在连接安全审计设备的接口抓包现象和tracert结果一致



.

.



流量到达核心交换机后为何会重新发回安全审计设备呢？应该是匹配了某个表项。查看快速转发表后发现，流量到达交换机后快速转发表

<hexin>display ip fast-forwarding cache

Total number of fast-forwarding entries: 4

SIP	SPort	DIP	DPort	Pro	Input_If	Output_If	Flg
172.16.8.1	**203**	**172.16.0.31**	**2048**	**1**	**Vlan8**	**Vlan100**	**1**
172.16.17.2	0	172.16.8.1	2816	1	InLoop0	Vlan8	1
172.16.0.31	203	172.16.8.1	0	1	Vlan100	Vlan8	3
172.16.8.1	0	172.16.17.2	0	1	Vlan8	N/A	1

默认情况下，快速转发表不关心流量的入接口，按照流量的五元组信息来匹配流量进行转发。

解决方法

关闭快速转发负载分担功能undo ip fast-forwarding load-sharing

关闭快速转发负载分担功能后，将会根据入接口的不同对五元组标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。

开启快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据五元组标识一条数据流。缺省情况下，快速转发负载分担功能处于开启状态。