某局点 S6813 6615P07版本 PBR在三层聚合口下发失败问题

策略路由 **许家豪** 2022-09-16 发表

问题描述

型号及版本：S6813 6615P07

问题描述：PBR在三层聚合口应用失败，将PBR中调用的ACL内的规则条目（匹配VPN实例）删除后就能应用上

过程分析

过程分析：PBR中调用的ACL若不存在匹配VPN的rule则可以下发，说明与匹配VPN实例有关。

经研发确认，系Marvell系列的产品都不支持acl里带vpn，如果带了就会下发失败，包括pbr，mqc，packet-filter等应用。

查看6813命令行手册可以看到，并没有vpn参数。

1.1.19 rule (IPv4 advanced ACL view)

rule命令用来为IPv4高级ACL创建一条规则。

undo rule命令用来为IPv4高级ACL删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

查看6520X-EI手册中可以看到，有vpn-instance参数说明了，但是有额外的标注，需要参考各业务模块。

1.1.18 rule (IPv4 advanced ACL view)

rule命令用来为IPv4高级ACL创建一条规则。

undo rule命令用来为IPv4高级ACL删除一条规则或删除规则中的部分内容。

1.1.18 rule (IPv4 advanced ACL view)

rule命令用来为IPv4高级ACL创建一条规则。

undo rule命令用来为IPv4高级ACL删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | [**flow-logging** | **logging**] | **source** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * | **fragment** | **icmp-type** | [**flow-logging** | **logging**] | **source** | **source-port** | **time-range** | **vpn-instance**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | [**flow-logging** | **logging**] | **source** { **microsegment** *microsegment-id* [**mask-length** *mask-length*] | *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 应用ACL进行报文过滤，ACL规则中未指定VPN实例时，表示该规则对非VPN报文和VPN报文均有效 其他特性引用ACL，ACL规则中未指定VPN实例时，不同业务模块的处理方式有所不同，请参见业务模块中的相关说明

解决方法

解决方法：acl中去除掉匹配vpn的rule即可。

策略路由业务模块的命令手册能明确看到，不支持调用的acl中存在VPN

1.1.12 if-match acl

if-match acl命令用来设置ACL匹配规则。

undo if-match acl命令用来恢复缺省情况。

【参数】

acl-number：访问控制列表号，取值范围为2000～3999。其中：

- 基本ACL，*acl-number*取值范围为2000～2999；
- 高级ACL，*acl-number*取值范围为3000～3999。

name *acl-name*：指定ACL的名称。*acl-name*表示ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。为避免混淆，ACL的名称不允许使用英文单词all。只有指定基本ACL或高级ACL的*acl-name*才生效。

【使用指导】

引用ACL时，需要注意的是：

- 若引用的ACL不存在，或者引用的ACL中没有配置规则，则表示所有的报文都满足该ACL匹配规则。
- 策略路由引用ACL时，若某条rule规则中指定了**vpn-instance**，则该ACL不生效。不指定**vpn-instance**参数，表示该条规则对公网和私网报文都有效。