

知 某局点S5130S-28S-LI IP Source Guard 不生效问题处理经验案例

IP Source Guard zhiliao_wm055 2018-09-28 发表

组网及说明

无

问题描述

某局点采用S5130S-28S-LI 做IP Source Guard 绑定，发现配置绑定之后，并没有生效，无论是配置在全局还是接口下，都不生效，查看设备的关键配置，绑定都配置正常，但是唯一在vlan 虚接口下配置了包过滤。

```
ip source binding ip-address 188.8.8.200 mac-address 0001-0000-0001
interface Vlan-interface1
ip address 188.8.8.253 255.255.255.0
packet-filter 3000 inbound
interface GigabitEthernet1/0/21
ip verify source ip-address mac-address
ip source binding ip-address 188.8.8.200 mac-address 0001-0000-0001
```

过程分析

因为IP source guard 和包过滤都是基于acl 实现的，初步怀疑是vlan 虚接口下的包过滤先生效导致的，在设备上查看协议的生效顺序

```
[H3C-probe]debug qacl show acl-prioinfo slot 1
```

```
-----Qacl Type Priority Info-----
```

Type	Acl Type Name	Reserved	Major	Sub
0	MQC Vlan	FALSE	6	4
1	MQC Global	FALSE	6	3
2	MQC Port	FALSE	6	5
3	MQC COPP	FALSE	9	1
4	NAT_HIGH	FALSE	9	3
5	NAT_LOW	FALSE	9	2
6	MQC_PORT Low	FALSE	6	1
7	RX IPv4 Super High	TRUE	11	26
8	RX IPv4 High	TRUE	11	24
9	RX IPv4 Middle High	TRUE	11	20
10	RX IPv4 Middle	TRUE	11	18
11	RX IPv6 Sup/High	TRUE	11	15
12	RX IPv6 Sup/High Shadow	TRUE	11	16
13	RX IPv6 High	TRUE	11	12
14	RX IPv6 Middle_High	TRUE	11	9
15	RX IPv6 Middle	TRUE	11	8
16	RX IPv4 Sup/High Shadow	TRUE	11	27
17	RX IPv4 High Shadow	TRUE	11	25
18	RX IPv4 Mid/High Shadow	TRUE	11	21
19	RX IPv4 Middle Shadow	TRUE	11	19
20	RX IPv6 High Shadow	TRUE	11	13
21	RX IPv6 Middle/High Shadow	TRUE	11	11
22	RX IPv6 Middle Shadow	TRUE	11	10
23	RX Low	TRUE	0	38
24	RX Low Shadow	TRUE	0	39
25	Super_RX Low	TRUE	0	34
26	Super_Rx Low Shadow	TRUE	0	35
27	Voice-Vlan	FALSE	4	17
28	PortBind Default	FALSE	4	5
29	PortBind Bind	FALSE	4	7
30	PortBindV6 Default	FALSE	5	15
31	PortBindV6	FALSE	5	17
32	Portal Free	FALSE	4	12
33	Portal User	FALSE	4	11
34	Portal Redirect	FALSE	4	9
35	Portal Deny	FALSE	4	8
36	Proxy IPv6	TRUE	0	20
37	Proxy IPv4-Cap	TRUE	0	19

38	Proxy IPv4-GRECap	TRUE	0	18
39	Proxy L3	TRUE	0	26
40	Proxy L2-Miss	TRUE	0	17
41	Proxy L2-DLF	TRUE	0	16
42	Proxy All	TRUE	0	15
43	Proxy Redirect-to-SA-CPU	TRUE	0	29
44	Storm Control	FALSE	5	9
45	Equipment	TRUE	11	29
46	UDP-Helper	TRUE	0	30
47	OAM-High	TRUE	11	31
48	OAM-High-Shadow	TRUE	11	32
49	OAM-Low	TRUE	11	30
50	IPv4-Cap-Redirect	TRUE	0	33
51	Fabric-Relay	TRUE	0	13
52	OUI-MAC	TRUE	0	10
53	MPLS-LSP-Ping-Decap	TRUE	0	9
54	Mirror Remote-Dest-Redirect	TRUE	12	2
55	EAD Free-IP	FALSE	4	16
56	EAD Middle	FALSE	4	15
57	EAD AAA-Rule	FALSE	4	14
58	EAD Auth-Rule	FALSE	4	13
59	MAC-Based-Vlan	FALSE	9	7
60	Zero-Mac-Deny	TRUE	0	32
61	CPU-CAR	TRUE	11	14
62	MCBC-SMod-Deny	TRUE	0	8
63	DMod-Redirect	TRUE	0	11
64	L2-Miss-Operation	TRUE	0	31
65	Permit-KnownMC	TRUE	0	25
66	EgressMask-KnownMC-High	TRUE	0	24
67	EgressMask-KnownMC-Low	TRUE	0	14
68	Portal User ACL	FALSE	4	10
69	DMod-IntfsMAC-No-Redirect	TRUE	0	12
70	RX Middle Low	TRUE	11	6
71	RX Middle Low Shadow	TRUE	11	7
72	RRPP Transmit Source Mac	TRUE	11	17
73	RRPP Deny Illegal	TRUE	0	40
74	Cos Shapping	FALSE	6	2
75	Cos Shapping Back	TRUE	0	7
76	DMod/Port redirect-to DMod/Port	TRUE	0	5
77	Port Mirror Proxy	FALSE	3	1
78	ACFP Type HIGH	TRUE	11	33
79	ACFP Type MIDDLE	FALSE	3	4
80	ACFP Type LOW	FALSE	3	3
81	MFF Type HIGH	TRUE	11	28
82	MFF Type MIDDLE	TRUE	0	37
83	MFF Type LOW	TRUE	0	36
84	NAT	TRUE	0	28
85	RX PRIO LLOW	TRUE	0	6
86	NETSTREAM FILTER	FALSE	4	18
87	STMVLAN_PERMIT	TRUE	11	37
88	STM_DENYALL	TRUE	11	36
89	BYTEACCOUNT	TRUE	11	5
90	PKTACCOUNT	TRUE	11	4
91	PDT_IRF	TRUE	11	38
92	DATAPROTECT	TRUE	0	23
93	UntrustPriority	TRUE	0	3
94	PktFilter Eth_Mac on PORT	FALSE	8	28
95	PktFilter IP on PORT	FALSE	8	27
96	PktFilter IP on VRF	FALSE	8	6
97	PktFilter Eth_Mac on VRF	FALSE	8	7
98	PktFilter IP on VSIPORT	FALSE	8	39
99	PktFilter Eth_Mac on VSIPORT	FALSE	8	40
100	PktFilter VSI DEFAULT MAC	FALSE	8	35
101	PktFilter VRF DEFAULT MAC	FALSE	8	1

102	PktFilter PORT DEFAULT MAC	FALSE	8	22
103	Pdt VFP FirstNh2Classid	TRUE	10	1
104	Statistics based PktPattern	TRUE	0	1
105	PDT Stack src modid block	TRUE	11	34
106	VFP LOW	TRUE	5	6
107	VFP HIGH	TRUE	5	7
108	IFP LOW	TRUE	0	4
109	IFP MIDDLE	FALSE	5	8
110	IFP HIGH	TRUE	11	3
111	Policy Based Routing V4	FALSE	7	1
112	Policy Based Routing V6	FALSE	7	2
113	ARP SMac Deny	TRUE	11	35
114	PDT HIGH	FALSE	9	6
115	PDT MIDDLE	FALSE	9	5
116	PDT LOW	FALSE	9	4
117	MQC L3 Port	FALSE	6	6
118	PktFilter IPV4 on RPORT	FALSE	8	20
119	PktFilter Eth_Mac on RPORT	FALSE	8	21
120	MPLS Vpn High	TRUE	0	41
121	MPLS Vpn Middle	TRUE	0	27
122	MPLS Vpn Low	TRUE	0	21
123	FCOE TO CPU Shadow	TRUE	4	4
124	FCOE TO CPU	TRUE	4	3
125	FCOE ROUTE	TRUE	4	2
126	FCOE ZONE	TRUE	5	3
127	FCOE FIPS DENY	TRUE	5	5
128	FIP SYS	TRUE	11	22
129	FIP SHADOW	TRUE	11	23
130	FCOE CLASSSCIFY SYS	TRUE	4	1
131	Dhcp RateLimit	TRUE	12	1
132	PortBind Special	FALSE	2	1
133	GlobalBind_V4	FALSE	4	6
134	GlobalBind_V6	FALSE	5	16
135	PktFilter IPV6 on PORT	FALSE	8	26
136	PktFilter IPV6 on VRF	FALSE	8	5
137	PktFilter IPV6 on RPORT	FALSE	8	19
138	FCOE NPVMAP	TRUE	5	4
139	MQC Vsi	FALSE	6	9
140	MQC UserProfile	FALSE	6	10
141	PDT HIGH INITIAL	TRUE	11	39
142	PDT LOW INITIAL	TRUE	0	42
143	PktFilter IPV6 on VSIPOINT	FALSE	8	38
144	PktFilter RPORT DEFAULT MAC	FALSE	8	15
145	FIPS NORMAL	TRUE	5	2
146	FIPS LOW	TRUE	5	1
147	MQC Schannel	FALSE	6	8
148	PktFilter IP on SChannel	FALSE	8	33
149	PktFilter IPV6 on SChannel	FALSE	8	32
150	PktFilter Eth_Mac on SChannel	FALSE	8	34
151	PktFilter SChannel DEFAULT MAC	FALSE	8	29
152	FCOE ROUTE SHADOW	FALSE	202	202
153	IPv6 Portal Free	FALSE	5	14
154	IPv6 Portal User	FALSE	5	13
155	IPv6 Portal User ACL	FALSE	5	12
156	IPv6 Portal Redirect	FALSE	5	11
157	IPv6 Portal Deny	FALSE	5	10
158	OPEN FLOW	FALSE	10	3
159	OPEN FLOW DEFALUT	FALSE	10	2
160	OPEN FLOW PORT	FALSE	10	11
161	OPEN FLOW DEV	FALSE	10	10
162	OPEN FLOW MACIP DEFAULT	FALSE	10	4
163	OPEN FLOW MACIP	FALSE	10	5
164	PktFilter VSI DEFAULT IP	FALSE	8	37
165	PktFilter VSI DEFAULT IPV6	FALSE	8	36

166	PktFilter VRF DEFAULT IP	FALSE	8	3
167	PktFilter VRF DEFAULT IPV6	FALSE	8	2
168	PktFilter PORT DEFAULT IP	FALSE	8	24
169	PktFilter PORT DEFAULT IPV6	FALSE	8	23
170	PktFilter RPORT DEFAULT IP	FALSE	8	17
171	PktFilter RPORT DEFAULT IPV6	FALSE	8	16
172	PktFilter SChannel DEFAULT IP	FALSE	8	31
173	PktFilter SChannel DEFAULT IPV6	FALSE	8	30
174	PktFilter RPORT DEFAULT MAC SUB	FALSE	8	8
175	PktFilter RPORT DEFAULT IP SUB	FALSE	8	10
176	PktFilter RPORT DEFAULT IPV6 SUB	FALSE	8	9
177	PktFilter Eth_Mac on RPORT SUB	FALSE	8	14
178	PktFilter IPV6 on RPORT SUB	FALSE	8	12
179	PktFilter IPV4 on RPORT SUB	FALSE	8	13
180	UDF PROTOCOL	TRUE	11	1
181	UDF PROTOCOL SHADOW	TRUE	11	2
182	PROXY PINNING	TRUE	0	2
183	PEX TO CPU	FALSE	202	202
184	ECN REMARK	FALSE	202	202
185	VXLAN TAG DROP	FALSE	3	2
186	TRILL_BOUNCE_FILTER	FALSE	202	202
187	TRILL_UC_INIT	FALSE	202	202
188	SYS FILTER	TRUE	12	4
189	OPEN FLOW GLOBAL	FALSE	10	7
190	OPEN FLOW GLOBAL DEFALUT	FALSE	10	6
191	PEX PERMIT	TRUE	12	3
192	PktFilter UDF on PORT	FALSE	8	25
193	PktFilter UDF on VRF	FALSE	8	4
194	PktFilter UDF on RPORT	FALSE	8	18
195	PktFilter UDF on RPORT sub	FALSE	8	11
196	OPEN FLOW GLOBAL MACIP DEFAULT	FALSE	10	8
197	OPEN FLOW GLOBAL MACIP FLOW	FALSE	10	9
198	PortBindV6 Unknown to cpu	FALSE	202	202
199	MPLS Vpn Low Tag Num	TRUE	0	22
200	BFD FROM VXLAN TO CPU	FALSE	13	1
201	MQC L3Sub Port	FALSE	6	7

解决方法

在vlan 虚接口下取消包过滤之后，IP Source Guard 就正常生效了。通过查看协议生效顺序，发现包过滤的优先级是8，IP source guard优先级是4，包过滤是比绑定优先的，所以两个同时配置，导致IP Source Guard 不生效。

28	PortBind Default	FALSE	4	5
29	PortBind Bind	FALSE	4	7
192	PktFilter UDF on PORT	FALSE	8	25
193	PktFilter UDF on VRF	FALSE	8	4
194	PktFilter UDF on RPORT	FALSE	8	18
195	PktFilter UDF on RPORT sub	FALSE	8	11
196	OPEN FLOW GLOBAL MACIP DEFAULT	FALSE	10	8