

知 iMC EAD安全检查通过后终端无法拿到安全VLAN的IP地址

iMC

贾海韵

2022-09-29 发表

组网及说明

无

问题描述

客户配置了这样的EAD安全策略：终端未通过安全检查时，下发vlan 35；通过安全检查后，下发安全vlan24。客户测试时发现，即使客户端通过安全检查后仍然会获得vlan35。

过程分析

收集iMC侧抓包和uam DEBUG级别日志，分析如下。

1. 从uam日志和抓包中看到，安全检查通过后，iMC服务器有发送session control报文给设备，下发vlan24:

%% 2022-07-25 12:44:40.280 ; [LDBG] ; [262464] ; sendVlantoNas ; Try to send VLAN: 24 for [imcuser03,F8:75:A4:A9:33:86,000000004202207250444140000002732100245,0] to 10.15.10.12(25506).

No.	Time	Source	Destination	Protocol	Length	Info
340	2022-07-25 12:44:14.048592000	10.7.1.251	10.15.10.12	RADIUS	116	Accounting-Response(5) (Id=183, l=24)
402	2022-07-25 12:44:14.370199000	10.15.10.12	10.7.1.251	RADIUS	474	Accounting-Request(4) (Id=184, l=432)
403	2022-07-25 12:44:14.370924000	10.7.1.251	10.15.10.12	RADIUS	62	Accounting-Response(5) (Id=184, l=20)
405	2022-07-25 12:44:14.403580000	10.15.10.12	10.7.1.251	Syslog	275	LOCAL7.INFO: Jul 25 12:44:13 2022 015-2F-A-531305 %N
612	2022-07-25 12:44:18.578484000	10.15.10.2	10.7.1.251	RADIUS	517	Accounting-Request(4) (Id=29, l=475)
613	2022-07-25 12:44:18.579251000	10.7.1.251	10.15.10.2	RADIUS	68	Accounting-Response(5) (Id=29, l=26)
965	2022-07-25 12:44:21.578525000	10.15.10.2	10.7.1.251	RADIUS	514	Accounting-Request(4) (Id=30, l=472)
966	2022-07-25 12:44:21.579391000	10.7.1.251	10.15.10.2	RADIUS	65	Accounting-Response(5) (Id=30, l=20)
2284	2022-07-25 12:44:28.578828000	10.15.10.2	10.7.1.251	RADIUS	511	Accounting-Request(4) (Id=31, l=469)
2285	2022-07-25 12:44:28.579364000	10.7.1.251	10.15.10.2	RADIUS	68	Accounting-Response(5) (Id=31, l=20)
3981	2022-07-25 12:44:40.281041000	10.7.1.251	10.15.10.12	UDP	156	Source port: 54055 Destination port: radius
4497	2022-07-25 12:44:45.578933000	10.15.10.2	10.7.1.251	RADIUS	511	Accounting-Request(4) (Id=32, l=469)
4498	2022-07-25 12:44:45.579397000	10.7.1.251	10.15.10.2	RADIUS	68	Accounting-Response(5) (Id=32, l=26)

Frame 3981: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits) on interface 0
Ethernet II, Src: VMware_a5:6c:88 (00:50:56:a5:6c:88), Dst: 38:ad:8e:6f:1a:01 (38:ad:8e:6f:1a:01)
Internet Protocol Version 4, Src: 10.7.1.251 (10.7.1.251), Dst: 10.15.10.12 (10.15.10.12)
User Datagram Protocol, Src Port: 54055 (54055), Dst Port: radius (1812)
Data (114 bytes)
[Length: 114]

0000 38 ad 8e 6f 1a 01 00 50 56 a5 6c 88 08 00 45 00 8...P V...E.
0010 00 8e 5a 75 00 00 80 11 00 00 0a 07 01 fb 0a 0f ..ZU...
0020 0a 0c d3 27 07 14 00 7a 20 a5 6c 88 08 00 45 00Z
0030 71 e2 58 f8 0a 3a bc 03 12 62 46 12 1a 66 2c 28 0xK2...bf...
0040 30 30 30 30 30 30 30 12 30 30 32 37 33 32 00000004 0020732
0050 30 34 34 34 31 34 30 30 30 30 30 32 37 33 32 04441400 00002732
0060 31 36 00 00 00 00 00 00 00 00 0d 41 06 00 00 1002458.A...
0070 00 00 00 00 00 00 00 00 00 00 00 43 a2 18 06C.....
0080 00 00 00 00 00 00 00 00 63 a2 18 06 00 00 00 01C.....
0090 1a 06 00 00 e3 a2 14 06 00 00 00 00C.....

综上，inode认证时，安全检查通过后，iMC服务器正常下发安全vlan24给设备。

2. 检查设备配置，发现设备上未开启session-control功能，导致收到报文后未响应。

解决方法

设备上开启session-control功能。

3. 配置步骤

- (1) 进入系统视图。

system-view

- (2) 开启 RADIUS session control 功能。

radius session-control enable

缺省情况下，RADIUS session control 功能处于关闭状态。

- (3) 指定 session control 客户端。

radius session-control client (**ip** *ipv4-address* | **ipv6** *ipv6-address*) [**key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name*] *

缺省情况下，未指定 session control 客户端。

