

知 5560X-EI Release 终端portal认证上线24小时之后无法上网

Portal认证 宣江明 2021-11-23 发表

组网及说明

一、组网

拓扑：客户端--hub--（G1/0/27） 5560X-EI-（G1/0/14）-防火墙--服务器

问题描述

二、设备：5560X-EI Release 1119P20 故障现象：账户portal认证成功在线一段时间后掉线，无法访问外网业务，但iNode客户端和服务端均显示在线；客户端重新下线再上线后业务恢复。imc侧确认iNode和imc服务侧的心跳通信正常，检查交换机上是否有问题。

过程分析

三、

查看ARP信息，正常应该是认证上线学到的MAC，但是10.10.12.104等终端是动态学习类型的

=====display arp all=====

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP address	MAC address	VLAN/VSI	Interface	Aging	Type
10.10.12.100	fe8c-fe19-00d2	12	GE1/0/27	1190	D
10.10.12.104	fe8c-fe6d-cf85	12	GE1/0/27	1186	D
10.10.12.117	fe8c-fed8-664a	12	GE1/0/27	1182	D
10.10.12.126	fe8c-fe6f-b977	12	GE1/0/27	837	D
10.10.12.103	fe8c-fe5a-8236	12	GE1/0/27	--	R
10.10.12.105	fe8c-fec9-ee3e	12	GE1/0/27	--	R
10.10.12.110	fe8c-feae-0bd3	12	GE1/0/27	--	R
10.10.12.118	fe8c-fea4-c6b7	12	GE1/0/27	--	R
10.10.12.123	fe8c-fefa-e89f	12	GE1/0/27	--	R

[HX_S5560]display portal user all 设备上认证用户里面没有异常用户ip地址

Total portal users: 13

Username: bm4LGx4BOHUsQh9hKFN3fEW/CAQ= liumeixin@portal

Portal server: myportal

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
fe8c-feae-0bd3	10.10.12.110	12	Vlan-interface12

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

Username: OWsJGB0DPSJ7Rx1iK1FyKy8+JPw= zhangqi@portal

Portal server: myportal

State: Online

VPN instance: N/A

MAC	IP	VLAN	Interface
fe8c-fe65-d86a	10.10.12.119	12	Vlan-interface12

Authorization information:

DHCP IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL number: N/A

Inbound CAR: N/A

Outbound CAR: N/A

先初步分析确定现场异常下线终端是否是固定时长掉线，是否所有客户端都会有IMC显示在线，实际访问不了外网。（这点之后得到确认，都是固定24小时客户端被强制下线，所有客户端均会发生同样故障）

之后查看配置发现portal认证中没有配置计费命令（客户现场当时配置认为所有员工均可以通过账号上网不需要配置计费）

#

domain portal

authentication portal radius-scheme allpermit

authorization portal radius-scheme allpermit

accounting portal radius-scheme allpermit ---未配置

<HX_S5560>debugging portal all 开启debugging命令

<HX_S5560>t d

<HX_S5560>t m

---- More ----*Jan 12 04:44:36:245 2013 HX_S5560 PORTAL/7/EVENT: User-SM[10.10.12.119]: Stopped session-timeout timer.

*Jan 12 04:44:36:245 2013 HX_S5560 PORTAL/7/EVENT: User-SM[10.10.12.119]: Session timer timed out and the user will be logged off.

*Jan 12 04:44:36:245 2013 HX_S5560 PORTAL/7/EVENT: User-SM[10.10.12.119]: Notified Auth-SM to log off the user.

*Jan 12 04:44:36:245 2013 HX_S5560 PORTAL/7/FSM: Auth-SM: Started to run.
*Jan 12 04:44:36:245 2013 HX_S5560 PORTAL/7/FSM: Auth-SM [10.10.12.119]: Entered state

解决方法

*Jan 12 04:44:36:249 2013 HX_S5560 PORTAL/7/PACKET:

四、配置命令: `acl 2000 by source-port protocol ip destination ip 10.10.12.119` 该用户下线

进一步检查终端portal认证成功时,交换机底层ACL表中,是否存在放行相关终端IP的规则
问题总结:在进行实验配置时要按照配置手册进行,不能省略主观上认为不需要的命令。另外该问题
[HX_S5560-probe]debug qacl show acl si 1 c 0
在前期咨询时是配置有portal终端的ACL,认证上线后一段时间无法上网的现象,以及故障现象是否具有
规律性?了解这两点更有利于问题定位。

0, Client TTI 0

Acl Hw Resource: Group 0, VTcamId 1, Client TTI 1

Acl Hw Resource: Group 1, VTcamId 4, Client IPCL 0

Pri 4, usedEntries 24, mode Double

=====

acl type	usedEntries[24]
[34]Portal Free	3
[35]Portal User	12 上线用户
[36]Portal Redirect	6
[37]Portal Deny	3

=====

Acl Hw Resource: Group 2, VTcamId 10, Client IPCL 1

Acl Hw Resource: Group 1, VTcamId 4, Client IPCL 2

Pri 0, usedEntries 2, mode Double

通过上面的打印信息,观察发现,故障时,设备底层下发了[36]Portal Redirect重定向和[37]Portal Deny (未认证成功用户,禁止访问)和其它规则。

[HX_S5560-probe]debug qacl show si 1 c 0 v 33 查看底层ACL能看到认证的用户

=====

Acl-Type Portal User, Stage IPCL 0, SinglePort, Installed, Active

Prio Mjr/Sub 0x204/0x5, RuleFormat INGRESS_EXT_NOT_IPV6, Vtcame/Idx 4/47,

Rule Match -----

Port: 27

Source mac: FEFC-FE1B-8208, FFFF-FFFF-FFFF

Outer Vlan: 0xc, 0xffff

Source IP: 10.10.12.121, 255.255.255.255

IP Type: Any IPv4 packet

Actions -----

Permit

Red Permit

Yel Permit

=====

后续进行故障复现,先将10.10.12.119用户认证上线,在IMC平台将默认上线时间24小时修改成60S,此时还未配置accounting portal radius-scheme allpermit计费命令。接着不断进行下述命令查看:

[HX_S5560-isp-portal]dis portal user ip 10.10.12.119 verbose 查看认证用户具体信息

Basic:

Current IP address: 10.10.12.119

Original IP address: 10.10.12.119

Username: ZTALSk8BZn4nHB8weVMpd9L3DCY= zhangqi@portal

User ID: 0x10000089

Access interface: Vlan-interface12

Service-VLAN/Customer-VLAN: 12/-

MAC address: fefc-fe65-d86a

Domain name: portal

VPN instance: N/A

Status: Online

Portal server: myportal

Portal authentication method: Direct

AAA:

Realtime accounting interval: 60s, retry times: 5

Idle cut: N/A

Session duration: **60 sec**, remaining: **17 sec**

Remaining traffic: N/A

Login time: 2013-01-12 05:35:01 UTC

Accounting-start fail action: Online

Accounting-update fail action: Online
Accounting quota-out action: Offline