使用AD CAMPUS进行普通 vlan 8021x认证的典型配置

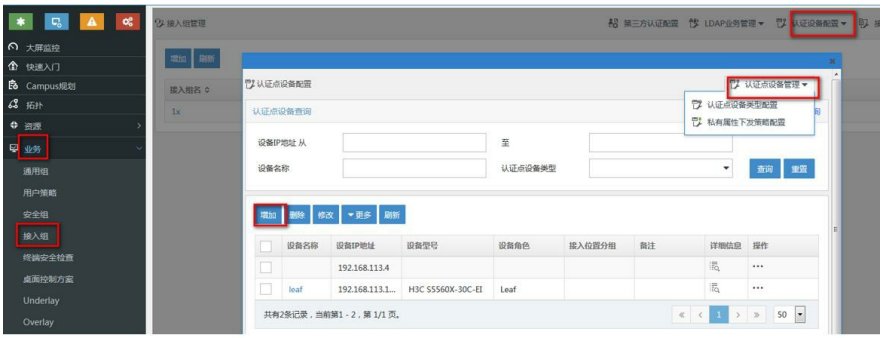
寻尚岩　2018-01-27 发表

AD CAMPUS进行8021x认证时一般都会结合leaf设备，leaf设备启用vxlan和evpn，同时启用1x认证。但是有的局点仅仅使用CAMPUS进行普通的8021x认证，所谓普通的8021x认证是指中间无需经过xlan隧道传输认证报文和数据报文。本案例描述使用CAMPUS进行普通8021x接入的通用配置。

如上图，终端通过G1/0/5口接入网络，在二层接入交换机开启3A认证和802.1x认证，认证服务器指向CAMPUS。

1. iMC侧增加接入设备

如下图所示，点击业务-接入组-认证设备配置-认证点设备配置，弹出增加接入设备的界面，点击增加按钮增加接入设备，具体输入内容同iMC普通8021x配置，不再赘述，如下图192.168.113.4就是本例增加的接入设备。

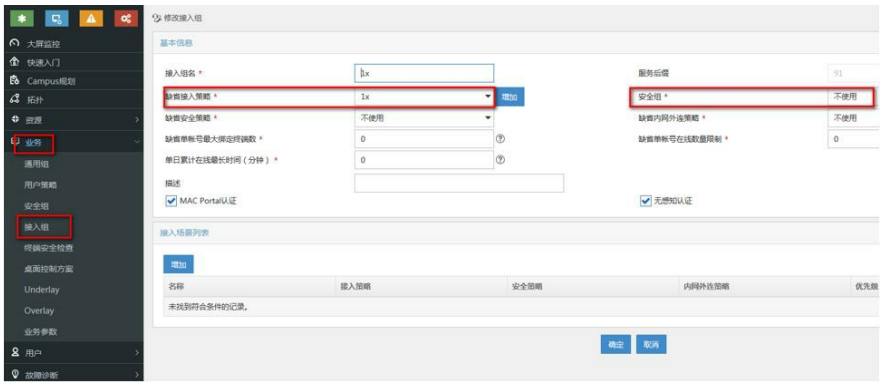


2. iMC侧增加接入策略

如下图所示，点击业务-接入组-接入策略弹出增加接入策略的界面，点击增加按钮，勾选相关策略后确定。此处配置和普通8021x认证配置类似，此处不再赘述。如下图1x就是本例增加的接入策略。

3. iMC侧增加接入服务

如下图，依次点击业务-接入组，点击增加接入组按钮，此处的接入组概念就是传统iMC里面服务的概念，其中缺省接入策略选择上一步创建的1x，需要注意的是安全组选择不使用，点击确定。



4. iMC侧增加接入用户

如下图所示，依次点击用户-接入用户-增加按钮，弹出增加接入用户的界面，页面输入项和普通8021x类似，此处不再赘述，注意勾选上一步创建的1x接入组，本案例增加的账号名为1x。iMC侧配置完毕。

5. 设备侧3A配置

增加radius方案配置，认证服务器指向CAMPUS

[sw1]radius scheme 91-1x

[sw1-radius-91-1x]dis this

#

radius scheme 91-1x

primary authentication 192.168.113.91

primary accounting 192.168.113.91

key authentication cipher c3$kgMWgWKWr+xHQMZFINeC2lsHDWVshA==

key accounting cipher c3$FtJKjV1vKKftxrtxaYC0ybmxJyTG/Q==

#

return

[sw1-radius-91-1x]

增加3A配置，注意域名需要和接入组后缀一致。

[sw1-isp-91]dis this

#

domain 91

authentication lan-access radius-scheme 91-1x

authorization lan-access radius-scheme 91-1x

accounting lan-access radius-scheme 91-1x

access-limit disable

state active

idle-cut disable

self-service-url disable

#

return

[sw1-isp-91]

增加802.1x配置，开启全局802.1x配置

[sw1]dot1x

802.1X is already enabled globally.

开启g1/0/5接口802.1x配置。

[sw1]

[sw1]dot1x interface g1/0/5

802.1X is enabled on port GigabitEthernet1/0/5 already.

6. iNode侧认证上线

如下图所示在8021x连接里面输入用户名密码，点击上线，此时账号可以上线成功。

iMC侧存在在线用户

1：接入组里面不要勾选安全组；

2：接入组后缀需要与域名保持一致；