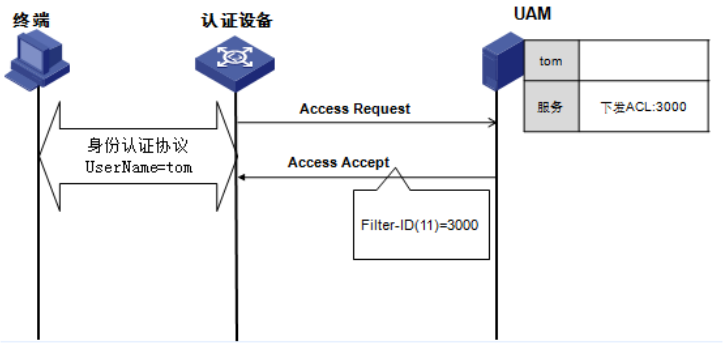
UAM或EIA通过下发ACL限制接入用户访问权限的配置方法

802.1X Portal Radius 马光彬 2015-10-13 发表

终端用户认证时，UAM/EIA通过radius 2号报文下发ACL号给接入设备（该ACL需要提前在设备上配置好），由接入设备动态将该ACL作用于终端用户，从而对接入用户访问权限进行限制。下发ACL需要设备同时支持该特性，目前只有H3C设备支持，具体支持的设备型号可以查询设备的版本说明书。还有一种“接入ACL列表”的方式，该特性仅对HP设备有效，国内不使用。



1、802.1x或portal认证（略）。

2、V7 EIA场景

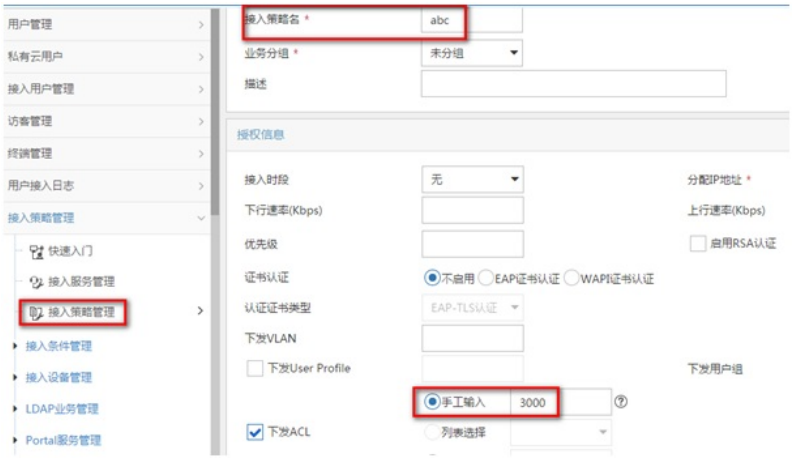
1)、设备上配置ACL 3000

[H3C]acl number 3000

[H3C-acl-adv-3000] rule 1 permit ip destination 10.10.10.10 0

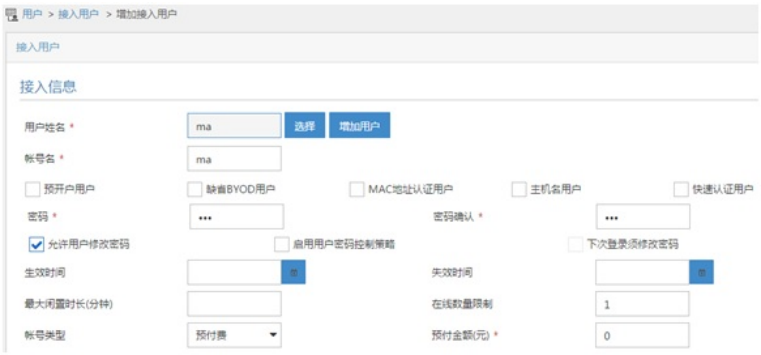
[H3C-acl-adv-3000] rule 2 deny ip

2)、iMC侧定制策略abc，下发ACL3000



3)、增加服务bcd，调用接入策略abc

4)、接入用户调用服务bcd



3、V5 UAM场景

1)、设备上配置ACL3000

[H3C]acl number 3000

[H3C-acl-adv-3000] rule 1 permit ip destination 10.10.10.10 0

[H3C-acl-adv-3000] rule 2 deny ip

创建两个loopback地址用于测试

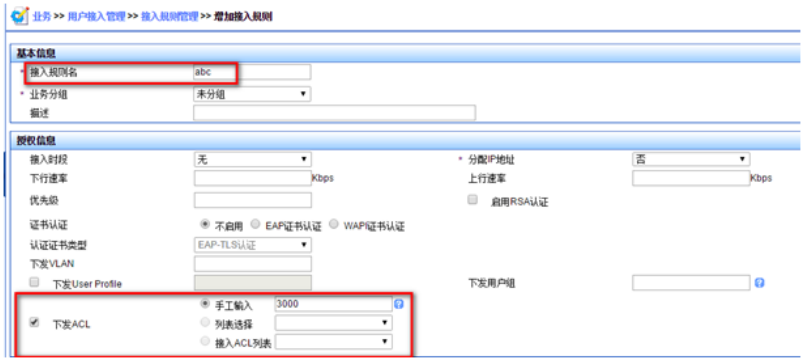
[H3C]int loopback 1

[H3C-LoopBack1]ip address 1.1.1.1 255.255.255.255

[H3C]int loopback 10

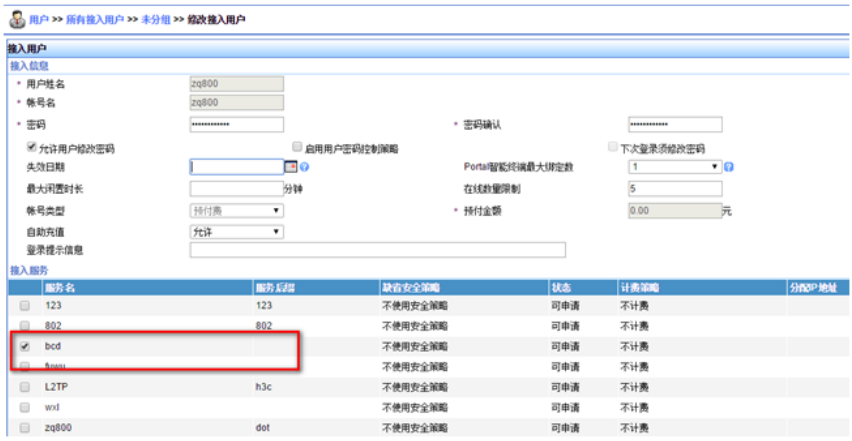
[H3C-LoopBack10]ip address 10.10.10.10 255.255.255.255

2)、iMC侧定制策略abc，下发ACL3000

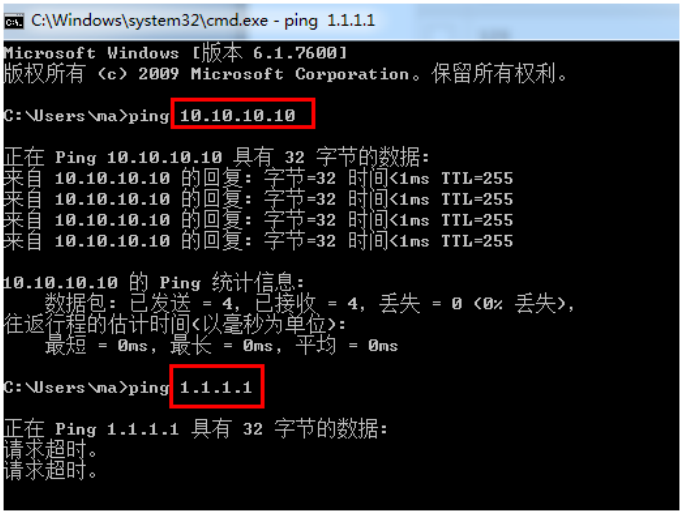


3)、增加服务bcd

4)、接入用户调用服务bcd



认证成功后，分别ping设备上两个loopback地址1.1.1.1和10.10.10.10，发现可以ping通10.10.10.10，1.1.1.1则不通，与ACL设置的规则匹配。



查看UAM日志，ACL3000已通过radius 2号报文下发。

% 2015-01-

05 22:55:16.095 ; [L_DEBUG (4)] ; [15644] ; LAN ; ma@portal ; 2 ; a785845407b34bfb95b138e3656a9a

3c ; uCAcHqqD ; Send message attribut list:

Code = 2

ID = 243

ATTRIBUTES:

User-Name(1) = ..O2MNHBkHNiB5Tx1iJFV6KVygzUk= ma@portal

Service_Type(6) = 2

State(24) = uCAcHqqD

Termination-Action(29) = 0

Filter_Id(11) = 3000

Session-Timeout(27) = 86401

Acct-Interim-Interval(85) = 600

hw-Connect-Id(26) = 441

hw_User_Notify(61) =