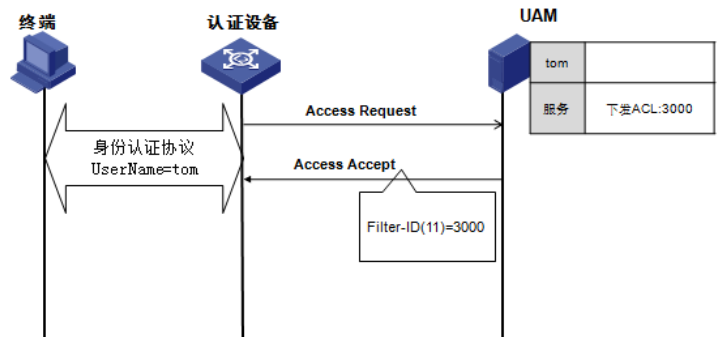


知 UAM或EIA通过下发ACL限制接入用户访问权限的配置方法

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

接入策略名 * abc

业务分组 * 未分组

描述

授权信息

接入时段 无 分配IP地址 *

下行速率(Kbps) 上行速率(Kbps)

优先级 启用RSA认证

证书认证 不启用 EAP证书认证 WAPI证书认证

认证证书类型 EAP-TLS认证

下发VLAN

下发User Profile 下发用户组

下发ACL 列表选择

手工输入 3000

3)、增加服务bcd，调用接入策略abc

用户 > 接入策略管理 > 接入服务管理 > 增加接入服务

基本信息

服务名 * bcd 服务后缀

业务分组 * 未分组 缺省接入策略 * abc

缺省安全策略 * 不使用 缺省内网外连策略 * 不使用

缺省私有属性下发策略 * 不使用 缺省移动办公策略 * 不使用

计费策略 * 不计费

缺省单帐号最大绑定终端数 * 0 缺省单帐号在线数量限制 * 0

服务描述

可申请 Portal无感知认证

4)、接入用户调用服务bcd

用户 > 接入用户 > 增加接入用户

接入用户

接入信息

用户名 *

帐号名 *

预开用户 缺省BYOD用户 MAC地址认证用户 主机名用户 快速认证用户

密码 * 密码确认 *

允许用户修改密码 启用用户密码控制策略 下次登录须修改密码

生效时间 市 失效时间 市

最大闲置时长(分钟) 在线数量限制

帐号类型 预付金额(元) *

接入服务

服务名	服务后跟	缺省安全策略	状态	计费策略	分配IP地址
<input type="checkbox"/> 123		不使用	可申请	不计费	
<input type="checkbox"/> 222		不使用	可申请	不计费	
<input type="checkbox"/> 802.1x		不使用	可申请	jifei	
<input type="checkbox"/> aaa		不使用	可申请	不计费	
<input type="checkbox"/> bangding		不使用	可申请	不计费	
<input checked="" type="checkbox"/> bcd		不使用	可申请	不计费	

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 10.10.10.0

[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

业务 >> 用户接入管理 >> 接入规则管理 >> 增加接入规则

基本信息

接入规则名

* 业务分组

描述

接收信息

接入时段 分配IP地址 否

下行速率 Kbps 上行速率 Kbps

优先级

证书认证 不启用 EAP证书认证 WAP证书认证

认证证书类型 启用RSA认证

下发VLAN

下发User Profile 下发用户组

下发ACL 手工输入 列表选择 插入ACL列表

手工输入

3)、增加服务bcd

业务 >> 用户接入管理 >> 服务配置管理 >> 增加服务配置

基本信息

服务名

服务后跟

* 业务分组

缺省安全策略

缺省私有属性下发策略

计费策略

服务描述

必 可申请 Portal智能终端快速认证

接入策略列表

增加

接入场景	接入规则	安全策略	私有属性下发策略	内网外网配置	优先级	修改

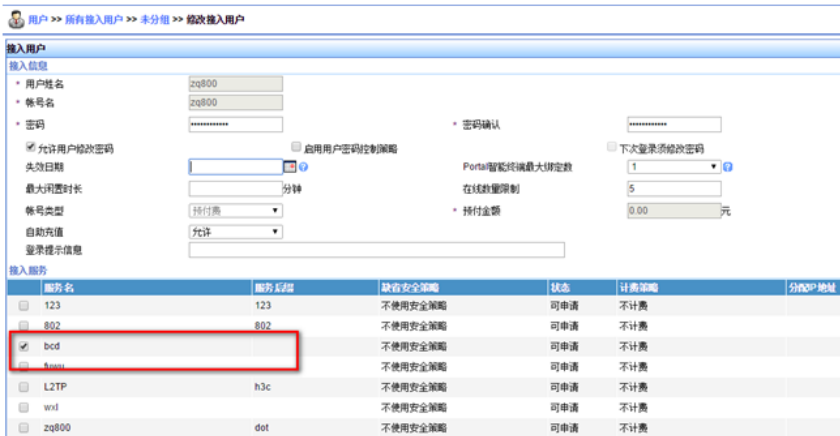
缺省接入规则

缺省内网外网配置

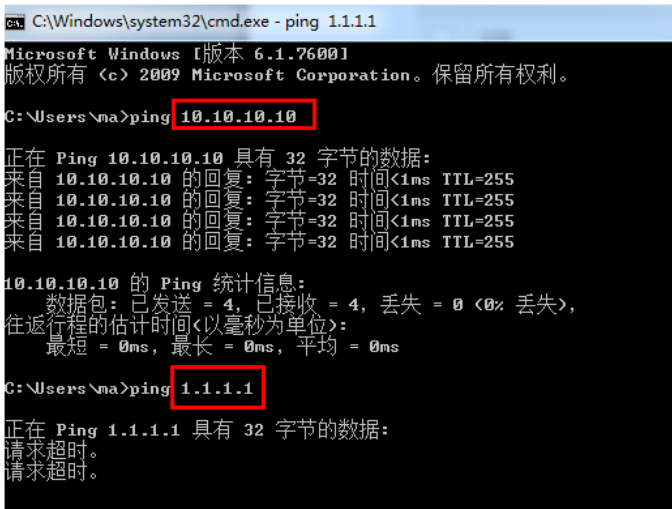
确定 取消

入用户调用服务bcd

4)、接



认证成功，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) =