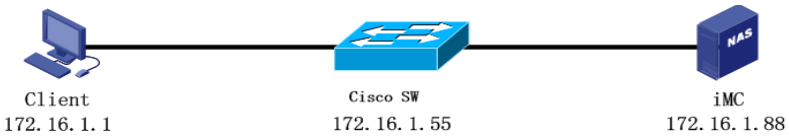
iMC向Cisco交换机下发ACL配置案例

Radius 王晓辉 2015-10-16 发表

在准入环境中，通过向设备下发ACL功能，可以控制用户认证通过后所能获得的访问权限。本案例介绍了在802.1X环境中如何使用我司iMC向Cisco交换机下发ACL。



1.Cisco交换机配置：

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting network default start-stop group radius
aaa nas port extended

aaa server radius dynamic-author
//启用动态授权功能
 client 172.16.1.88 server-key imc
 server-key imc
 port 3799
 auth-type session-key
 ignore session-key

ip device tracking probe use-svi
ip device tracking
dot1x system-auth-control

radius-server attribute 44 include-in-access-req
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 11 default direction in
//开启ACL下发功能
radius-server host 172.16.1.88 auth-port 1812 acct-port 1813 key imc

ip access-list extended test3
//配置下发的ACL必须是name方式，不支持数字
 deny ip any host 192.168.1.1
//目的地192.168.1.1不允许访问
 permit ip any any
//其余都放行

interface FastEthernet0/1
 switchport mode access
 authentication host-mode multi-auth
   authentication port-control auto
 dot1x pae authenticator
   spanning-tree portfast
```

2.iMC UAM配置：

iMC UAM按照正常配置即可，但以下两处需要特别注意：

1）.添加接入设备时要选择“Cisco（General）”和“启用混合组网”；

2）.添加接入策略时下发ACL处不能写数字，只能写acl名字。

3.最终结果：

用户认证通过后，Cisco交换机下使用命令：show authentication interface F0/1即可看到该设备的认证情况，若Filter-ID字段有下发的ACL名字，则证明ACL下发成功。

```
C3560#show authentication sessions interface f0/1
            Interface:  FastEthernet0/1
          MAC Address:  a048.0324.432d
           IP Address:  172.16.1.1
            User-Name:  haha
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
           Filter-Id:  test3
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  A31304370000000E0022F102
      Acct Session ID:  0x00000088
               Handle:  0xEC00000F

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

1. iMC向Cisco交换机下发ACL只支持name方式，不支持数字ID形式；
2. 接入设备处，Cisco交换机必须勾选“启用混合组网”和“Cisco（General）”；
3. Cisco交换机必须开启Radius属性11，以允许ACL下发；
4. ACL的源IP必须是any。