防内网外连典型配置案例

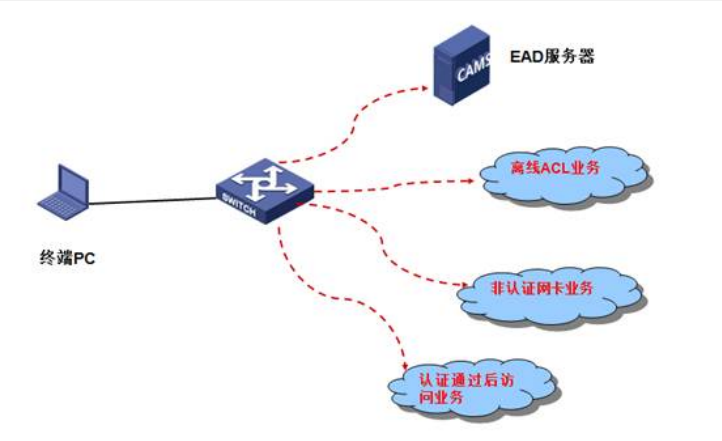
EAD解决方案 舒中华 2012-10-29 发表

防内网外连功能典型配置案例

一、 组网需求：

防内网外连功能主要限制用户对IP网络的访问能力。比如PC终端可能有多个网卡，在接入内网接受EAD控制的同时还接入了其他网络；或者像笔记本电脑这样可以移动的终端，可以随时接入各种网络。对于很多对于网络访问很敏感的场景和用户，都需要一种方法，能够强制PC终端只能接入可信的内网，禁止接入其他网络，客户端防内网外连功能在客户端进行内网接入前，能够将所有IP网络设备置为流出向阻断状态，具体为流出向过滤掉除DHCP报文外的所有IP报文，流入向不做限制。只有当客户端802.1x或Portal认证成功后，才会将认证网卡完全放开，不过滤任何报文。若是多网卡情况（包括但不限于Modem、ADSL、GPRS、CDMA 3G 无线802.11等各种互联网接入），非认证网卡将始终处于阻断状态。这样就从源头上限制了PC对网络的使用，对于信息安全和防病毒木马有重要的作用。起初防内网外联功能控制非常严格，一旦启用该功能，非认证网卡不能访问任何资源，为了控制更灵活，后续版本增加了“非认证网卡ACL”，“离线ACL”，可以通过ACL灵活控制非认证网卡和离线网卡能访问的资源。

二、 组网图：



本例IP地址分配如下：

终端PC:172.16.100.2/24

EAD服务器：172.16.100.122/24

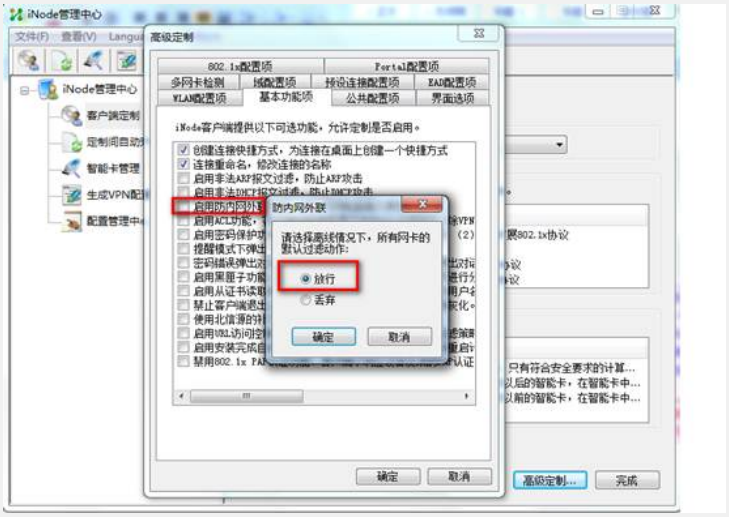
非认证网卡ACL业务：20.20.20.20/24

离线ACL业务：10.10.10.10/24

三、 配置步骤：

1. iMC侧配置

1.1 定制带防内网外连功能的iNode客户端



【图1】

说明：定制iNode客户端，选择网卡的默认过滤动作，“放行”表示安装iNode客户端后，不做任何动作，“丢弃”表示安装iNode客户端后，即使不通过EAD服务器下发策略，也不能访问任何资源，一旦客户端上线，默认策略将不再生效，以EAD服务器下发的策略生效。

1.2 创建EAD安全策略

创建安全策略szhtest

【图2】

1.3 创建客户端ACL，离线ACL业务：只放通EAD服务器IP和10.10.10.10/32主机；在线非认证网卡ACL业务：只放通EAD服务器IP和20.20.20.20/32主机，如图3，图4

【图3】离线ACL

【图4】在线非认证ACL

1.4 创建服务szhstest,并启用防内网外连功能，引用在线非认证网卡ACL和离线ACL

【图5】

1.5 添加接入设备，配置正确的Nas-IP和Key

【图6】

1.6 创建账户szhtest并绑定服务szhtest

【图7】

2. 设备侧关键配置

```
dot1x
radius scheme fan
server-type extended
primary authentication 172.16.100.122
primary accounting 172.16.100.122
key authentication h3c
key accounting h3c
user-name-format without-domain

domain fan
authentication lan-access radius-scheme fan
authorization lan-access radius-scheme fan
accounting lan-access radius-scheme fan
access-limit disable
state active
idle-cut disable
self-service-url disable

int vlan 100
ip address 172.16.100.1 255.255.255.0

int g 1/0/3
dot1x
port access vlan 100

int loopback 1
description onlineunauthenacl
```

ip address 20.20.20.20 255.255.255.255

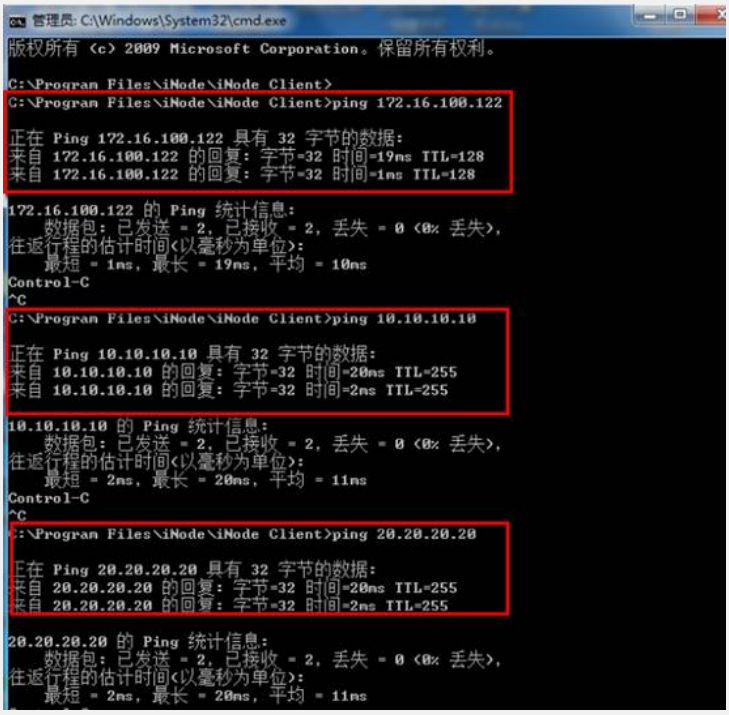
int loopback 2

description offlineacl

ip address 10.10.10.10 255.255.255.255

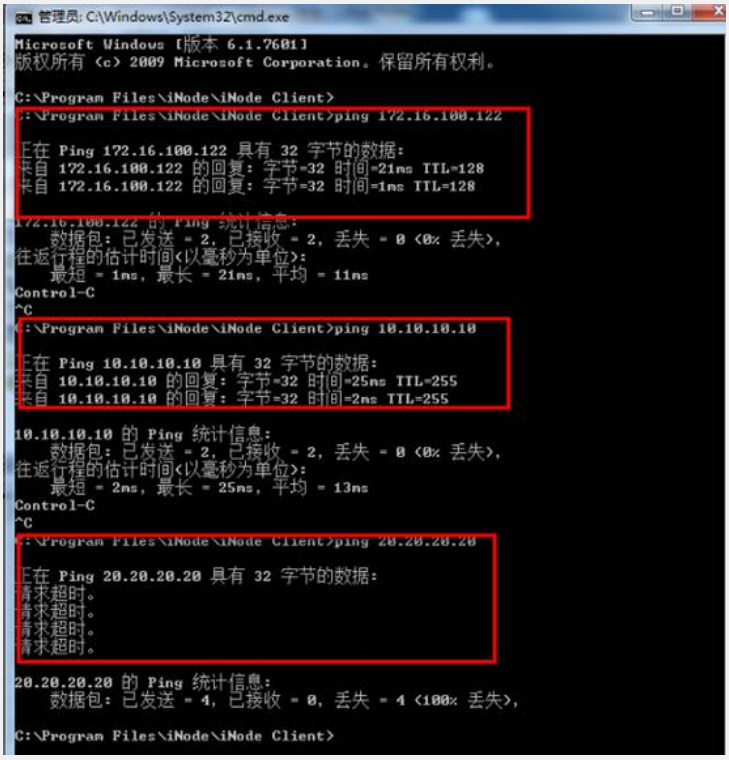
3. 功能测试

3.1 认证通过后连通性测试如下图8，所以业务都能正常连通



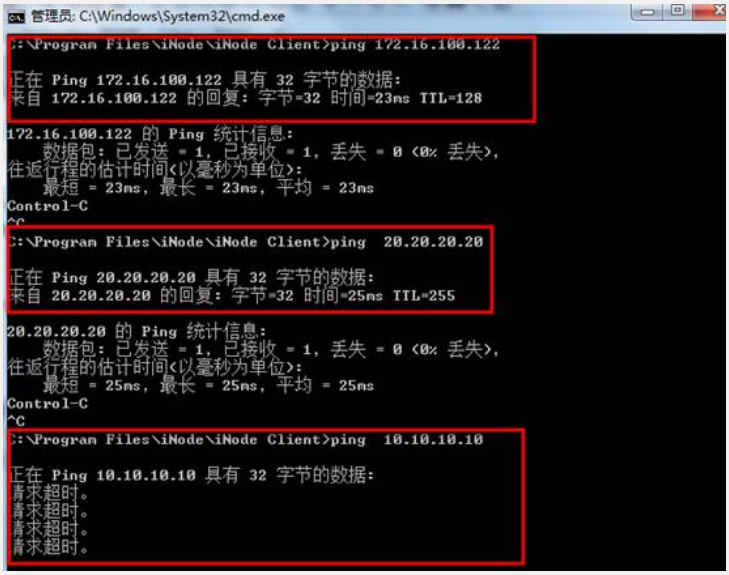
【图8】

3.2 离线后连通性测试如下图9，只有离线ACL放通的业务能连通



【图9】

3.3 非认证网卡连通性测试如下图10，只有非认证网卡业务能连通



【图10】

4. 防内网外连功能不生效问题排查方法

4.1 排查iMC侧的配置是否正确，离线ACL和在线非认证网卡ACL配置是否合理。

4.2 查看EAD调试级别日志和iNode详细级别日志以确认防内网外连策略是否正确下发到iNode客户端，例如本例:

查看EAD的调试级别policyserver.log日志文件的2号报文可以发现服务器已经正确下发了在线非认证ACL（OnlineUnauthACL）和离线ACL(OfflineACL)见红色字体:

2012-08-17 11:05:13 [策略服务器] [信息 (0)] [15] [RequestProcessor::processRequest] szhtest@fan；EAD认证上线回应报文(2)；QHMj1fDh；18:A9:05:DF:D4:0E；172.16.100.2 ;回应报文属性列表:
MsgId: 8415
MsgType: 2
Address: 172.16.100.2
Proxy IP: 172.16.100.122
attr:encrypt: true
attr:compressed: true
WSMConfig: 10.153.43.100;6666;300;5;
licManageIP: 172.16.100.122
iSetACL: true
heartBeatInterval: 7200
heartBeatOutTimes: 3
defaultActionSEC:
OnlineUnauthACL: {
sIP=0.0.0.0;sMk=0.0.0.0;dIP=172.16.100.122;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0;;sIP=0.0.0.0;sMk=0.0.0.0;dIP=20.20.20.20;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0; }
defaultActionOnlineUnauth: 0
OfflineACL: {
sIP=0.0.0.0;sMk=0.0.0.0;dIP=10.10.10.10;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0;;sIP=0.0.0.0;sMk=0.0.0.0;dIP=172.16.100.122;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0; }
defaultActionOffline: 0
defaultACL: 0

查看iNode的detail级别日志iNode Secpkt********.log文件的2号报文发现iNode也正确收到了EAD服务器下发的离线ACL以及在线非认证网卡ACL，见红色字体:
[2012-08-17 11:02:15] [DtlCmn] [e24] sndSecMsg: transfer [2] [8411]
10.153.43.100;6666;300;5;
172.16.100.122
true
7200
3

PluginForbidden
false
unlimit
false
false
false
false
now;cmd
GcPxAW4YhtNz49ySlWKaPQ==
1345172299437

n="OnlineUnauthACL">sIP=0.0.0.0;sMk=0.0.0.0;dIP=172.16.100.122;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0;

sIP=0.0.0.0;sMk=0.0.0.0;dIP=20.20.20.20;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0;
0

n="OfflineACL">sIP=0.0.0.0;sMk=0.0.0.0;dIP=10.10.10.10;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0;

sIP=0.0.0.0;sMk=0.0.0.0;dIP=172.16.100.122;dMk=255.255.255.255;sPt=0;dPt=0;ptl=65535;drt=1;drp=0;
0
0

配置关键点：

1. 在启用防内网外连功能的同时，如果需要下发离线ACL或在线非认证网卡ACL，则iNode需要定制客户端ACL功能，否则认证通过后会提示需要客户端ACL的iNode客户端。

2. 防内网外连功能是EAD的功能，故服务需要绑定EAD策略才能启用防内网外连功能。

3. 功能说明：a.如果离线默认过滤动作为“放行”，也就是认证网卡没有认证或认证不通过处于离线状态下，认证网卡能访问所有网络资源，相当于防内网外联功能不存在。b.如果离线默认过滤动作为“丢弃”，也就是认证网卡没有认证或认证不通过处于离线状态下，认证网卡不能访问任何网络，为了控制更加灵活，引入了离线ACL,即在离线状态下，能访问哪些网络资源。

4. 名词解释：a.在线非认证网卡ACL：是指有多网卡的PC，但是没有通过Dot1x或Portal认证的网卡能访问的网络资源。b.离线ACL:是指认证网卡没有认证或认证不通过处理离线状态时，能访问哪些网络资源。