EAD认证过程解析

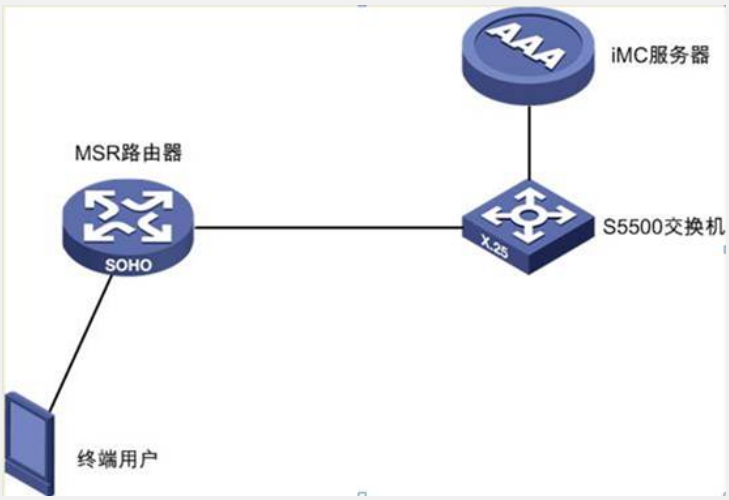
2013-04-24 发表

EAD认证过程解析

一、 组网需求：

EAD即终端准入控制（End User Admission Domination），从最终用户的安全控制入手，对接入网络的终端实施企业安全准入策略，最头痛的事是在实施或者定位EAD相关问题，在碰到该种问题我们常用的杀手锏就是：1.排查设备侧和iMC服务器侧配置是否正确。2.如果配置正确，只能在服务器和客户端抓包，收集客户端和服务器侧UAM/EAD调试日志，配置倒是难不倒大部分业软大拿，但是如果需要抓包和日志来定位时，一线朋友都会主动将收集的信息发给二线定位，主要原因是对整个认证过程报文交互不熟悉，如果掌握了整个报文交互流程，您也可以自己看懂这些神奇的代码，本文通过举例来详细介绍认证过程，希望对大家有所帮助。

二、 组网图



【图1】

说明：
终端用户的IP：192.168.133.2 /24
EAD代理服务器IP：172.16.100.122

三、配置步骤

3.1 iMC服务器配置

本文以802.1X+EAD并下发隔离，安全ACL为例说明。

1）创建端口组QQdeny:

【图2】

2）创建EAD策略windstr:

【图3】

3）创建服务wind

【图4】

4）添加接入设备MSR:

【图5】

5）创建接入账号并绑定服务windstr:

【图6】

3.2设备侧配置

1）设备版本

[MSR]dis ver

H3C Comware Platform Software

Comware Software, Version 5.20, Release 2105P31

Copyright (c) 2004-2011 Hangzhou H3C Tech. Co., Ltd. All rights reserved.

H3C MSR30-11F uptime is 0 week, 0 day, 22 hours, 59 minutes

2）设备配置

802.1X

acl number 3000//隔离ACL，控制终端只能访问IMC服务器172.16.100.122

rule 1 permit IP destination 172.16.100.122 0

rule 2 deny IP

acl number 3001 //安全ACL，控制不允许访问192.168.122.2主机

rule 2 deny IP destination 192.168.122.2 0

rule 3 permit IP

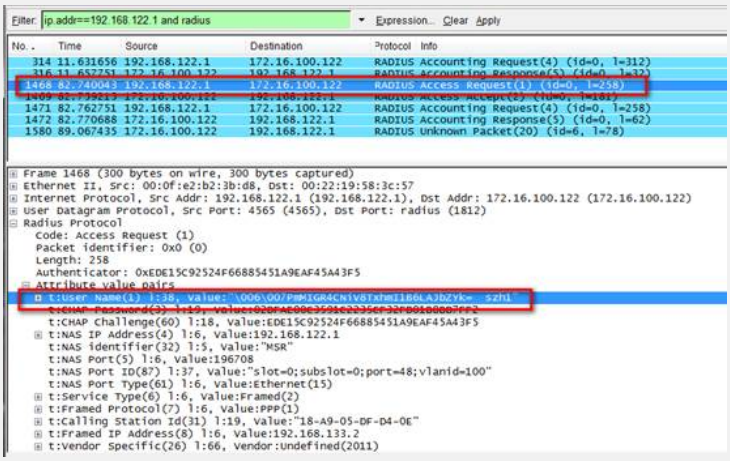
Radius scheme iMC

server-type extended

primary authentication 172.16.100.122
primary accounting 172.16.100.122
key authentication iMC
key accounting iMC
user-name-format without-domain
nas-IP 192.168.122.1
domain iMC
authentication lan-access Radius-scheme iMC
authorization lan-access Radius-scheme iMC
accounting lan-access Radius-scheme iMC
access-limit disable
state active
idle-cut disable
self-service-url disable
interface Vlan-interface100
IP address 192.168.133.1 255.255.255.0
interface Vlan-interface122
IP address 192.168.122.1 255.255.255.0
interface Ethernet0/48 //终端接入接口
port link-mode bridge
port access vlan 100
802.1X
3.3认证过程详解
1）客户端第一次认证未被隔离场景分析

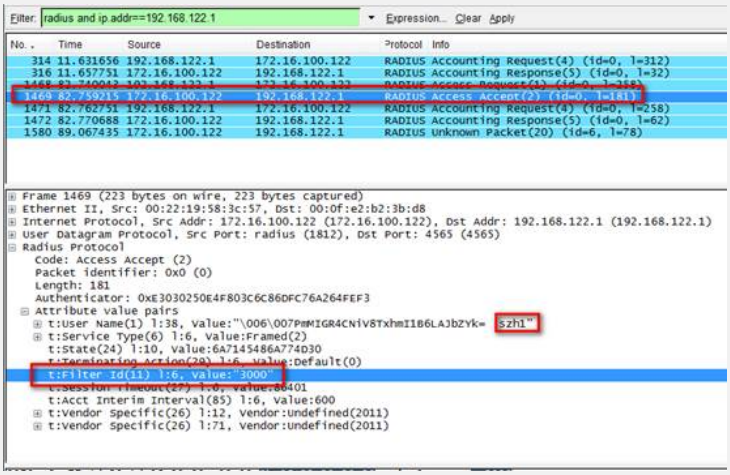
【图7】

2） 服务器Radius抓包分析
常见的Radius报文即code=1（认证请求报文），code=2（认证回应报文），code=3（认证拒绝报文），code=4（计费请求报文），code=5（计费回应报文），1号报文由设备发起，AAA服务器收到设备的认证请求报文后，检查接入用户的合法性，然后回应2号报文，EAD方案里，隔离ACL通过2号报文属性下发，设备收到AAA服务器的回应报文后，发送计费开始报文，AAA服务器收到4号报文后，回应5号报文，当然如果存在安全ACL，则服务器通过20号报文下发到BAS设备侧。
a．Radius认证请求报文（code=1）



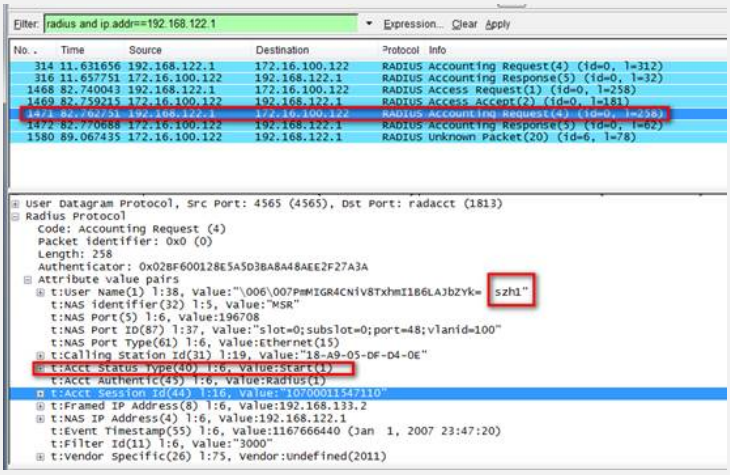
【图8】

b.Radius 认证回应报文（code=2）
说明：注意隔离ACL是Radius 2号报文属性下发的。



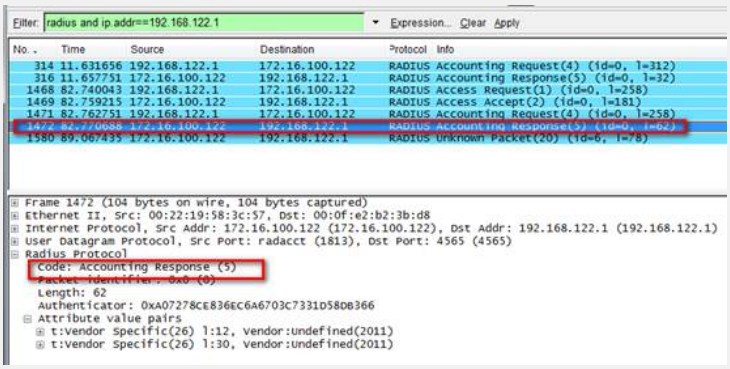
【图9】

C. Radius 计费开始报文（code=4）



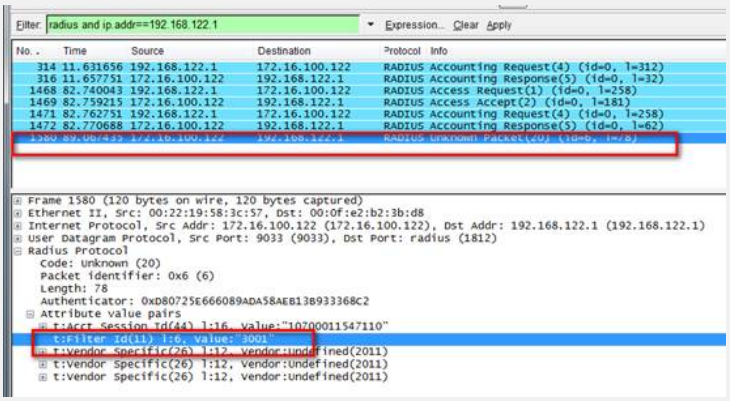
【图10】

d. Radius 计费回应报文（code=5）



【图11】

e．Radius 安全ACL下发报文（code=20）



【图12】

3) 服务器UAM认证日志分析

在网上认证失败问题处理过程中，大多需要收集IMC UAM（IMC/UAM/LOG）的调试级别日志以协助定位，因为调试级别日志记录了服务器和BAS设备Radius的详细交互过程和属性值,如下所示：

```
CODE = 1.ATTRIBUTES:
User-Name(1) = "..MzJVSk1fZyhxHkU1cA0rIUzCeMA=  szh1".
CHAP-Password(3) = "..}..Uf..DUV.UU.L".
CHAP-Challenge(60) = ".?.">...dh.x.,!.".
NAS-IP-Address(4) = 3232266753.
NAS-Identifier(32) = "MSR".
NAS-Port(5) = 196708.
NAS-Port-Id(87) = "slot=0;subslot=0;port=48;vlanid=100".
NAS-Port-Type(61) = 15.
Service-Type(6) = 2.
Framed-Protocol(7) = 1.
Calling-Station-Id(31) = "18-A9-05-DF-D4-0E".
Framed-IP-Address(8) = 3232269570.
hw_Connect_ID(26) = 16.
hw_Product_ID(255) = "H3C MSR30-11F".
hw_IP_Host_Addr(60) = "192.168.133.2 18:a9:05:df:d4:0e".
hw_Nas_Startup_Timetamp(59) = 1167609632.
Code = 2
ID = 0
ATTRIBUTES:
User-Name(1) = ..MzJVSk1fZyhxHkU1cA0rIUzCeMA=  szh1
Service_Type(6) = 2
State(24) = NLZIdD3d
Termination-Action(29) = 0
Filter_Id(11) = 3000
Session-Timeout(27) = 86401
Acct-Interim-Interval(85) = 600
hw-Connect-Id(26) = 16
hw_User_Notify(61) =
IF_PROXY = 0
IF_DOUBLE_NETCARD = 0
IF_IE_PROXY = 0
FRAMED_IP_SET_MODE = 0
IF_CHECK_MODIFY_MAC = 0
IF_CHECK_SAME_MAC = 0
CAMS_DETAIL_VERSION = R003B01D003SP14
EAD_EVENT_SEQ_ID = NLZIdD3d
CODE = 4.
ID   = 0.
ATTRIBUTES:
User-Name(1) = "..MzJVSk1fZyhxHkU1cA0rIUzCeMA=  szh1".
NAS-Identifier(32) = "MSR".
NAS-Port(5) = 196708.
NAS-Port-Id(87) = "slot=0;subslot=0;port=48;vlanid=100".
NAS-Port-Type(61) = 15.
Calling-Station-Id(31) = "18-A9-05-DF-D4-0E".
Acct-Status-Type(40) = 1.
Acct-Authentic(45) = 1.
Acct-Session-Id(44) = "10700011543100".
Framed-IP-Address(8) = 3232269570.
NAS-IP-Address(4) = 3232266753.
Event-Timestamp(55) = 1167666186.
Filter-Id(11) = "3000".
hw_Connect_ID(26) = 16.
hw_Input_Peak_Rate(1) = 0.
hw_Input_Average_Rate(2) = 0.
hw_Output_Peak_Rate(4) = 0.
hw_Output_Average_Rate(5) = 0.
```

hw_Priority(22) = 0.
hw_IP_Host_Addr(60) = "192.168.133.2 18:a9:05:df:d4:0e".
Code = 5
ID = 0
ATTRIBUTES:
hw-Connect-Id(26) = 16
hw_User_Notify(61) =
EAD_EVENT_SEQ_ID = NLZIdD3d
EAD_PROXY_IP = 2886755450 //在做EAD方案中，安全检查报文由iNode客户端发起，而客户端必须知道策略服务器的IP，如果是eap方式，可以通过抓包看到，会在第一个11号报文的challenge中最后六个字节携带，格式为 xx xx xx xx（IP） xx xx （PORT）如果不是eap，在计费开始的回应报文的HW扩展属性中携带。
EAD_PROXY_PORT = 9019

4）策略服务器认证日志分析
EAD Client与EAD Server Proxy之间的报文交互主要用于安全认证， 以下是EAD Client与EAD Server Proxy之间的交互报文种类的汇总：
SEC_START = 0x01, /*EAD认证上线报文*/
SEC_CHECK_LIST = 0x02, /*EAD认证上线回应报文*/
SEC_CHECK_RESULT = 0x03, /*安全认证检查结果上报报文*/
SEC_CHCK_SUCCESS = 0x04, /*安全认证成功报文*/
SEC_CHECK_FAIL = 0x06, /*安全认证失败报文*/
SEC_MONITOR_REPORT = 0x07, /*安全认证实时监控结果上报报文*/
SEC_MONITOR_RESPOnD= 0x08, /*安全认证实时监控结果无异常回应报*/
SEC_REQUEST_ISOLATION = 0x09, /*not used currently*/
SEC_ MONITOR_RESULT = 0x0A, /*安全认证实时监控结果下发报文*/
SEC_ERR_NOTICE = 0x10, /*安全认证错误通知报文*/
SEC_HEARTBEAT = 0x11, /*EAD认证心跳报文*/
SEC_HEARTBEAT_RESPOnD= 0x12, /*EAD认证心跳回应报文*/
SEC_OFFLINE = 0x13, /*EAD认证下线报文*/
SEC_OFFLINE_RESPOnD= 0x14, /*EAD认证下线回应报文*/
SEC_CHANGE_PASSWORD = 0x31, /*EAD认证密码修改报文*/
SEC_CHGPASSWD_RESULT = 0x32, /*EAD认证密码修改回应报文*/
SEC_PWD_WINLOGON_REPORT = 0x41, /*EAD认证弱密码检查结果上报报文*/
SEC_PWD_WINLOGON_RESPOnD= 0x42, /*EAD认证弱密码检查结果上报回应报文*/
SEC_TELNET_REQUEST = 0x44, /*EAD远程桌面登录请求报文*/
SEC_TELNET_RESPOnD= 0x45, /*EAD远程桌面登录回应报文*/
SEC_NET_SCAN_REPORT = 0x51, /* EAD认证网络流量监控上报报文*/
SEC_NET_SCAN_RESPOnD= 0x52, /* EAD认证网络流量监控回应报文*/
SEC_ACL_REQUEST = 0x61, /* EAD认证ACL请求报文*/
SEC_ACL_RESPOnD= 0x62, /* EAD认证ACL规则集下发报文*/
SEC_INFORM_NEED_RR = 0xA0, /*消息下发报文，要求客户端回应*/
SEC_INFORM_RR = 0xA1, /*0xA0的回执*/
SEC_INFORM = 0xA2, /*消息下发报文*/
SEC_DMA_REQUEST = 0xA4, /*EAD Server的DMA请求报文*/
SEC_DMA_RESPOnD= 0xA5 /*EAD Client的DMA回应报文*/
说明：奇数号报文为客户端发给EAD Proxy的报文，偶数号报文为EAD Proxy发给客户端的报文。代理服务器与客户端使用UDP协议进行通讯，代理服务器使用固定（缺省为9019）端口监听客户端消息；具体的客户端也从固定监听端口（从10102开始递增的第一个空闲端口）发送和接受报文,报文交互过程分析：

a. EAD认证上线请求报文
2012-02-10 08:57:38 [策略服务器] [信息 (0)] [24] [ProxyRequestHandler::run] szh1@iMC ; EAD认证上线请求报文(1) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ; 文解析成功
userName: szh1@iMC
hwAddr: 18:A9:05:DF:D4:0E
eventSeqID: kNIXeLUQ /*序列ID，八字节定长字符串（由大小写字母和数字符号组成），唯一标识本次连接。在线重认证时，必须携带概述性；非在线重认证时，客户端在发起本报文之前如果能够获取到本次连接的序列ID，则携带该属性；*/
clientPort: 10102 /*客户端监听的UDP端口号，S erver主动给客户端下发报文时需要使用该端口号；*/
clientVersion: CH V5.00-0101 /*客户端版本号，Server据此判断是否要升级客户端版

本；clientDisVersion: CH iNode PC 5.0 (E0101)*/
isIndependent: 0 /*是否为设备无关特性，1：是，0：不是.*/
patchStamp: 2NDOXkXvVt8= /*保存在本地的补丁检查时间戳，需要上传给iMC策略服务器*/
SupSoftRunCheckType: true /*服务器依据此特性判断是否下发新的进程检查方式，取值固定为true。*/
supBlackWhiteGroup: true /*服务器依据此属性判断是否支持可控软件、进程、服务组，取值固定为true。*/
supPureWhiteGroup: true /*服务器依此属性判断客户端是否支持纯白软件组。新版本客户端只能上报true，表示支持；不上报时（客户端是旧版本），表示不支持*/
supProcessCheckMD5: true /*是否支持进程检查。*/
supBWGroupWithDtl: true
iSupCmp: true /*服务器依据此属性判定是否支持压缩特性，取值固定为true。*/
ClientType: PC
IPAddr: 192.168.133.2 /*客户端IP地址*/
hostname: sfw0445 /*客户端主机名*/
BindToDomain: H3C /*绑定域*/
IsDomainUser: true /*服务器依据此特性判断是否下发登陆密码检查策略。*/
LogonDomain: H3C /*登陆域*/
DamClientId: 3DD5A8868633E94A894C92FF3E355ACA /*桌面资产管理客户端进行配合，上报操作系统编号ID。*/
iSupWanControl: false /*服务器依据此属性判定当前连接是否支持放内网外连特性，客户端从定制好的配置文件中来读取属性，并且会看底层协议，如果是底层协议是1x或者Portal,并且定制了这个特性，就确认是支持内网外联特性，否则就认为不支持，即使客户端定制了，但是底层协议不是1x或者Portal,也会上报该属性的值为false,确认是否支持内网外联特性，服务器依据此属性判断是否支持内网外联特性，取值为true或者false，如果当前支持防内网外联特性，但是驱动出现了问题，那么客户端将上报属性值为DrvErr。*/
iSupACL: false /*服务器依据此属性判定客户端当前的连接是否支持ACL特性，客户端从定制好的配置文件中来读取属性，并且会看底层协议，如果是底层协议是1x并且定制了这个特性，就确认是支持ACL下发，否则就认为不支持，即使客户端定制了，但是底层协议不是1x,也会上报该属性的值为false,服务器依据此属性判断是否支持ACL下发，取值为true或者false，如果当前支持ACL下发，但是驱动出现了问题，那么客户端将上报属性值为DrvErr；*/
iSupRegHighOS: true
iSupAlias: true
OSInfo: Windows 7 Ultimate
iSupOnlyWAV: true
iSupShareCheck: 1
Proxy IP: 172.16.100.122/*ead代理服务器*/
Address: 192.168.133.2 /*客户端IP
Port: 10102 /*客户端通信原端口*/
MsgId: 11245
MsgType: 1
b. EAD认证上线回应报文
2012-02-10 08:57:38 [策略服务器] [信息 (0)] [15] [RequestProcessor::processRequest] szh1@iMC ; EAD认证上线回应报文(2) ; kNIXeLUQ ;18:A9:05:DF:D4:0E ; 192.168.133.2 ; 回应报文属性列表：
MsgId: 11245
MsgType: 2
Address: 192.168.133.2 /*客户端IP*/
Proxy IP: 172.16.100.122 /*ead代理服务器IP*/
heartBeatInterval: 720 /*心跳间隔时长（秒），整数；*/
heartBeatOutTimes: 3 /*心跳超时间隔次数（次），整数；*/
eventSeqID: kNIXeLUQ
说明1：心跳在二次认证初期收到x02报文后启动；且只有在退出二次认证时才停止。heartBeatInterval属性规定了客户端两条EAD心跳报文的发送时间间隔，heartBeatOutTimes属性规定了连续多少个心跳报文异常就认为心跳已经中断。
checkList: /*检查项*/
blackProcessGroup: qqdeny;QQ.exe;simple;/* 该属性规定一种黑名单进程（禁止运行的进程），其取值格式为：“组名;进程名;检查类型”，该属性的下发与否取决于1号上传的属性supBlackWhiteGroup。其中：进程运行检查取值格式：组名;进程名;检查类型。组名，即服务器配置的组的名称。进程名，对应软件的进程名。进程检查方式。取值为“simple”或者“complex”，分别表示“简单检查”和“复杂的防止伪进程检查”。进

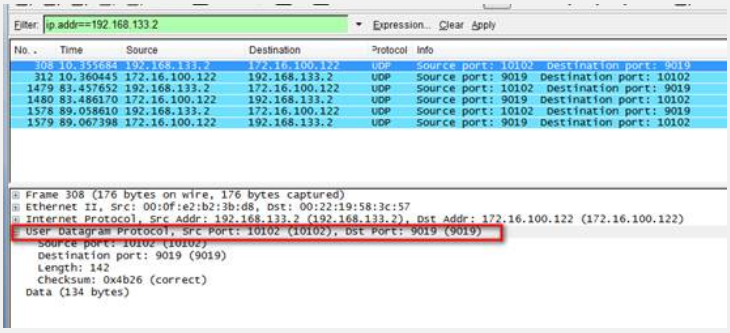
程检查方式紧跟在运行进程名称的后面，与名称之间用;隔开。注意：要界定N个黑名单进程需要在x02报文的数据段中携带N个blackProcessGroup属性。如果多个进程同在一个组内，须携带多个blackProcessGroup属性，而且组名相同。*/
patchLevel:Critical,repair;Important,repair;Moderate,repair;Low,repairserverVersion: iMCV500R003B01D003SP14 /*服务器版本*/
strategyMode: autoAdapt /* strategyMode，安全认证模式，其取值只能为 “autoAdapt”，表示混合模式，当不携带本属性时表示不进行安全认证；*/
userBalance: 您的帐号余额是：0.00 元。/*下发用户余额或欠费信息；*/
systemMessage: hello world! /*服务器系统信息*/
userMessage: /*用户组信息*/
antiAgent: false /*是否防上网代理程序，取值为true/false；*/
antIProxy: false /*是否防IE Proxy设置，取值为true/false；*/
antiDualNetcard: false /*是否防多网卡，取值为true/false；
IPSetMode，是否限制客户端认证网卡IP地址获取方式，取值为unlimit/static/dynamic，分别表示不限、静态设置和动态获取；
IPSetMode: unlimit /*是否限制客户端认证网卡IP地址获取方式，取值为unlimit/static/dynamic，分别表示不限、静态设置和动态获取；*/
macCheck: false /*是否限制客户端认证网卡MAC地址修改*/
sameMacCheck: false /*相同MAC地址检查*/

c.EAD检查结果请求报文
2012-02-10 08:57:44 [策略服务器] [调试 (0)] [24] [ProxyRequestHandler::run] szh1@iMC ; 检查结果请求报文(3) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ; 报文解析成功
userName: szh1@iMC
hwAddr: 18:A9:05:DF:D4:0E
dictionaryDigest: /* A. 格式如下：词典文件的BASe64(MD5)摘要。B. 说明：服务器再收到该摘要的时候，判断该摘要和数据库表中记录的摘要是否相同，如果相同，4号或者6号报文不下发关于弱密码的信息，客户端则会继续使用原来的策略。如果不相同，或者为空，服务器则在4号或者6号报文中重新下发url。C. URL的格式固定为：http://IP:端口号/selfservice/passwordFile?fileName=passwordDic.txt。URL举例：http://10.153.128.82:8080/ selfservice/passwordFile?fileName=passwordDic.txt
eventSeqID: kNIXeLUQ
supNetScan: true /* supNetScan，服务器依据此属性判断是否支持新的网络流量协议，取值固定为true。
AScheckResult:
APcheckResult:
FWcheckResult:
HDcheckResult:
blackSofts: /*上报禁止安装但已经安装的软件列表，取值格式为：“组1:软件名1,软件名2,软件名3;组2:软件名;”，其中软件名列表为每组查到的违规软件，之间用“,”隔开。*/
whiteSofts: /*上报要求安装但没有安装的软件列表，取值格式为：“组1;组2;”blackProcess: /*上报禁止运行但已经运行的进程列表，取值格式为：“组1:进程名1,进程名2,进程名3;组2:进程名;”，其中进程名为每组查到的违规进程，之间用“,”隔开。*/
whiteProcess: /*上报要求运行但没有运行的软件列表，取值格式为：“组1;组2;”*/blackServices: /*上报禁止运行但已经运行的服务列表，取值格式为：“组1:服务名1,服务名2,服务名3;组2:服务名;”，其中服务名为每组查到的违规服务，之间用“,”隔开。*/
whiteServices: /*上报要求运行但没有运行的服务列表，取值格式为：“组1;组2;”；*/
NoValidFileGroup:
blackFiles:
whiteFiles:
Proxy IP: 172.16.100.122
Address: 192.168.133.2
Port: 10102
MsgId: 11246
MsgType: 3

d.EAD安全认证成功报文
即安全认证成功报文。客户端收到该报文就说明通过了安全认证。
2012-02-10 08:57:44 [策略服务器] [调试 (0)] [16] [RequestProcessor::processRequest] szh1@iMC ; 安全认证成功报文(4) ; kNIXeLUQ ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ;回应报文属性列表：
MsgId: 11246

MsgType: 4
Address: 192.168.133.2
Proxy IP: 172.16.100.122
isRealtimeMonitor: true /*指示客户端是否启动实时监控功能，取值为“false”、“true”之一，分别表示不启动实时监控和启动实时监控；如果不携带该属性也表示要启动实时监控（说明：x06号报文固定不携带该属性，且不启动实时监控）；*/
monitorInterval: 60 /*实时监控间隔时长（秒），整数；
说明：monitorInterval用于设置实时监控功能的检查周期。如果x04报文中没有携带该属性，但又要求进行实时监控，检查周期的值则取x02报文下发的heartBeatInterval属性的值。
realtimeMonitorAll: true /*实时监控所有*/
realtimeMonitorItems: ;software;;/* “;”分隔的监控项。取值包括“virus”（发现不能清除的病毒），“avexcept”（防病毒客户端异常），“software”（检查软件使用），“register”（检查注册表使用）。
netScanPolicy: /*分隔的网络流量监控策略。取值为“samplingInterver= ”（采样间隔，单位是秒），“IPPktPeak1= ”（IP流量域值1，单位是M），“IPPktPeak2= ”（IP流量域值2，单位是M），“NUcastPktsPeak1= ”（二层广播报文数域值1，单位是个），“NUcastPktsPeak2= ”（二层广播报文数域值2，单位是个），“PktsPeak1= ”（经过认证网卡的报文数域值1，单位是个），“PktsPeak2= ”（经过认证网卡的报文数域值2，单位是个），“IPConnPeak1= ”（TCPIP连接数域值1，单位是个），“IPConnPeak2= ”（TCPIP连接数域值2，单位是个）*/
netMonItem: /*用“;”隔开的网络流量监控条目，其值为“IPPkt”，“NUcastPkt”“Pkts”，“IPConn”。服务器如果判断是新版本，将不再下发（27）属性“isNetScanMonitor”,而是下发该属性。客户端在接收到这样的属性之后，知道了应该进行网络流量监控并且监控哪个也知道了。
okMessage: /*成功通过安全认证的提示信息*/

5） 策略服务器端抓包之EAD安全认证过程分析
Radius报文是BAS设备和AAA服务器直接交互，而EAD安全检查时，iNode和EAD proxy服务器直接使用UDP报文交互，交互过程的具体类容建议查看EAD策略服务器的调试日志，日志记录了交互的具体属性，在服务器端抓包，主要用于确定客户端是否和服务器正确交互安全检查报文，如果服务器端没有抓到客户端发送的安全检查报文，则需要确定客户端是否发出了安全检查请求报文，具体可以在客户端抓包或者查看iNode的detail日志文件：secpkt.txt,如果客户端发起了，服务器侧没收到，则需排查网络环境，比如：是否有防火墙阻塞了UDP端口等等。



【图13】

客户端detail日志secpkt文件：
[2012-02-10 10:42:26] [DtlCmn] [674] secPushInner: out-pkt [1] //安全认证请求报文
szh1@iMC
<in="hwAddr">18:A9:05:DF:D4:0E
JOvPBgcC
10102
CH V5.00-0101
CH iNode PC 5.0 (E0101)
0
2NDOXkXvVt8=
true
true
true
true
true

true
PC
192.168.133.2
sfw0445
H3C
true
H3C
3DD5A8868633E94A894C92FF3E355ACA
false
false
true
true
Windows 7 Ultimate
true
1

[2012-02-10 10:42:27] [DtlCmn] [1ba0] sndSecMsg: transfer [2] [11260] //安全认证回应报文

<data>
720
3

qqdeny;QQ.exe;simple;;
<n="patchLevel">Critical,repair;Important,repair;Moderate,repair;Low,repair/i>
JOvPBgcC
iMCV500R003B01D003SP14
autoAdapt
您的帐号余额是：0.00 元。
hello world!

false
false
false
unlimit
false
false
</data>

[2012-02-10 10:42:33] [DtlCmn] [1cdc] secPushInner: out-pkt [3] //检查结果上报请求报文

szh1@iMC
18:A9:05:DF:D4:0E

JOvPBgcC
true

<in="blackFiles">

[2012-02-10 10:42:33] [DtlCmn] [1ba0] sndSecMsg: transfer [4] [11261] //安全检查成功报文

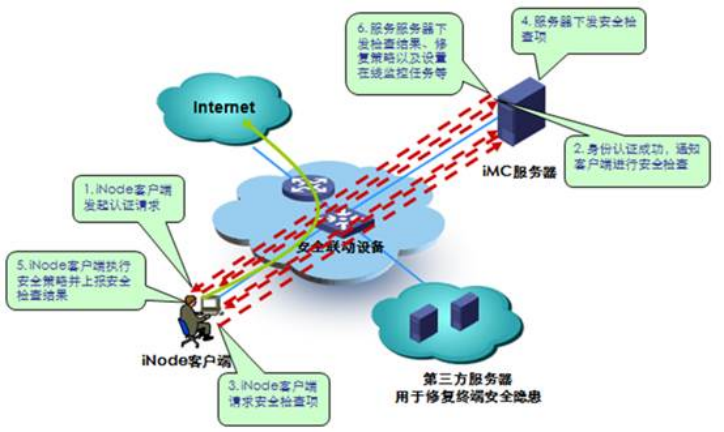
<data>
true
60
true

;software;;

6)客户端第二次认证被隔离场景分析
a.服务器Radius抓包分析
被隔离场景时服务器侧的抓包和未被隔离场景报文交互一致，唯一不同的就是没有下发安全ACL，code 20报文。
b.服务器UAM认证日志分析
被隔离场景时服务器侧的抓包和未被隔离场景报文交互一致，在此省略。
c.策略服务器认证日志分析
(1). EAD认证上线请求报文
2012-02-10 09:06:31 [策略服务器] [信息 (0)] [24] [ProxyRequestHandler::run] szh1@iMC ; EAD认证上线请求报文(1) ; DraKiUwU ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ; 文解析成功
userName: szh1@iMC
hwAddr: 18:A9:05:DF:D4:0E
eventSeqID: DraKiUwU
clientPort: 10102
clientVersion: CH V5.00-0101
clientDisVersion: CH iNode PC 5.0 (E0101)
isIndependent: 0
patchStamp: 2NDOXkXvVt8=
SupSoftRunCheckType: true
supBlackWhiteGroup: true
supPureWhiteGroup: true
supProcessCheckMD5: true
supBWGroupWithDtl: true
iSupCmp: true
ClientType: PC
IPAddr: 192.168.133.2
hostname: sfw0445
BindToDomain: H3C
IsDomainUser: true
LogonDomain: H3C
DamClientId: 3DD5A8868633E94A894C92FF3E355ACA
iSupWanControl: false
iSupACL: false
iSupRegHighOS: true
iSupAlias: true
OSInfo: Windows 7 Ultimate
iSupOnlyWAV: true
iSupShareCheck: 1
Proxy IP: 172.16.100.122
Address: 192.168.133.2
Port: 10102
MsgId: 11251
MsgType: 1
(2) EAD认证上线回应报文
2012-02-10 09:06:31 [策略服务器] [信息 (0)] [16] [RequestProcessor::processRequest] szh1@iMC ; EAD认证上线回应报文(2) ; DraKiUwU ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ; 回应报文属性列表:
MsgId: 11251
MsgType: 2
Address: 192.168.133.2
Proxy IP: 172.16.100.122
heartBeatInterval: 720
heartBeatOutTimes: 3
checkList:
blackProcesGroup: qqdeny;QQ.exe;simple;;
patchLevel Critical,repair;Important,repair;Moderate,repair;Low,reair
eventSeqID: DraKiUwU
serverVersion: iMCV500R003B01D003SP14

strategyMode: autoAdapt
userBalance: 您的帐号余额是：0.00 元。
systemMessage: hello world!
userMessage:
antiAgent: false
antIProxy: false
antiDualNetcard: false
IPSetMode: unlimit
macCheck: false
sameMacCheck: false
(3) 检查结果请求报文
2012-02-10 09:06:37 [策略服务器] [调试 (0)] [24] [ProxyRequestHandler::run] szh1@iMC ; 检查结果请求报文(3) ; DraKiUwU ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ; 报文解析成功
userName: szh1@iMC
hwAddr: 18:A9:05:DF:D4:0E
dictionaryDigest:
eventSeqID: DraKiUwU
supNetScan: true
AScheckResult:
APcheckResult:
FWcheckResult:
HDcheckResult:
blackSofts:
whiteSofts:
blackProcess: qqdeny:QQ.exe;
whiteProcess:
blackServices:
whiteServices:
NoValidFileGroup:
blackFiles:
whiteFiles:
Proxy IP: 172.16.100.122
Address: 192.168.133.2
Port: 10102
MsgId: 11252
MsgType: 3

(4)安全认证失败报文
2012-02-10 09:06:37 [策略服务器] [调试 (0)] [17] [RequestProcessor::processRequest] szh1@iMC ; 安全认证失败报文(6) ;DraKiUwU ; 18:A9:05:DF:D4:0E ; 192.168.133.2 ; 回应报文属性列表：
MsgId: 11252
MsgType: 6
Address: 192.168.133.2
Proxy IP: 172.16.100.122
action: repair /取值只能为“remind”，表示通过安全认证但存在安全隐患，不携带该属性表示成功通过安全认证且不存在安全隐患（说明：x06号报文中的action属性为必带属性，取值为“repair”、“offline”之一，分别表示隔离用户和让用户下线）；
netScanPolicy:
netMonItem:
blackProcess: qqdeny|repair
softFailMessage:
softRepairUrl:
d.策略服务器端抓包分析
被隔离场景时服务器侧的抓包和未被隔离场景报文交互一致，在此省略。
4.配置关键点



【图14】

EAD方案中，终端用户首先发起身份认证（常见的认证方式802.1x，Portal），并通过Radius2号报文下发隔离ACL（下方给设备或者iNode客户端）构造隔离区，将接入用户放到隔离区限制只能访问有限资源，身份认证通过后，客户端发起安全检查请求报文，对终端进行安全检查，客户端根据服务器下发的策略检查相关选项，最终由EAD策略的安全级别来执行相关的动作：隔离，下线，提醒，监控，如果通过安全检查，则下发安全ACL最终到达终端准入控制的最佳效果。

根据身份认证，安全认证报文交互的流程，可以为定位问题提供思路，比如：比较常见的，身份认证通过后，安全认证失败，我们就可以确定Radius交互过程已经结束，问题出现安全认证阶段，此时就可以将时间和精力用在排查客户端和安全代理服务器为什么通信不正常上，是不是中间有防火墙阻断了UDP 9019/10102,也可以在客户端抓包确定客户端是否发起了安全检查请求报文，如果客户端发出了，那就一步步定位，看报文在哪里被丢弃了，客户端和服务器通信问题解决了，剩下的问题就是配置了，很容易解决了。

说明：本案例只是以802.1X认证方式举例，不同的认证方式，不同的安全策略场景下，策略服务器交互的报文可能有差异，只是为大家提供一个问题定位的思路。