EAD配置了URL访问控制策略时，客户端上线后马上下线问题分析

张明磊 2017-11-20 发表

iMC的EAD安全管理组件在对接入用户进行身份认证的基础上要求接入用户进行安全认证，实现对其安全状态的准入控制，融合了安全策略管理、网络资源控制、网络拓扑监测等功能，为操作员提供全面、高效的网络安全管理平台。

某局点客户在使用EAD功能时反馈，在安全策略中添加了URL访问控制策略时，客户端在上线后会马上下线；不使用URL访问控制策略，则没有该问题

遇到此类问题，首先要收集iNode、UAM和EAD的调试日志，然后根据日志进行分析。

查看iNodeSecPkt日志，发现iNode正常发送了EAD 1号报文，但iMC在回复的EAD 2号报文中报错提示“服务器要求客户端启用URL访问控制功能”，

[2017-04-01 16:31:52] [DtlCmn] [2980] SecPkt secPushInner: out-pkt [1]

<data>

inside

70:5A:0F:D5:92:F8

10102

CH V7.20-0408

CH iNode PC 7.2 (E0408)

1

Sj5+a6kyr2moV0aPoE2GYA==

2NDOXkXvVt8=

true

true

true

true

true

true

PC

192.168.100.177

nfw2588DC

H3C

true

H3C

48F97BB25235E04598163905B81C58C1

false

false

false

false

true

true

Windows 7 Enterprise

2016-08-17 11:00:51

true

1

true

57363242453950342020202020202020202020202020

3543473631383144444320202020202020202020

false

Hewlett-Packard

HP EliteBook 820 G2

</data>

[2017-04-01 16:31:52] [DtlCmn] [2980] SecPkt secPushInner: the state send before is 3

[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secRcvThrd: [192.168.100.100 : 9019] sent me 562 bytes

.

[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secDataProc: The head id is ad878

[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secDataProc: The type is 2

[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secDataProc: The id is 5732

[2017-04-01 16:31:52] [DtlCmn] [2708] SecPkt sndSecMsg: transfer [2] [5732]

<data>

autoAdapt

false
false
false
false
unlimit
false
false
false
false
false
false
false
false
false
3232261220
9029
720
3

服务器要求客户端启用URL访问控制功能
The server requires iNode to support URL access control
false
false
afterCheck
Critical,monitor;Important,monitor;Moderate,monitor;Low,monitor
false
false
NM6hKAf3
iMCV700R003B04D016
</data>

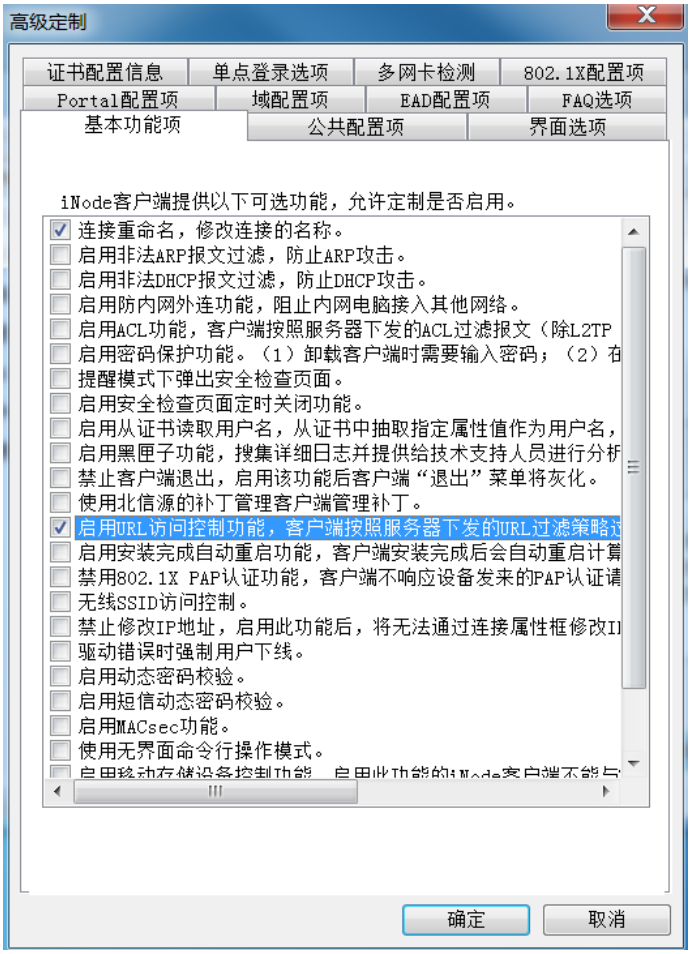
随即iNode发送了EAD 19号报文，即EAD认证下线报文，使用MsgID也可以在EAD的debug日志中看到整个EAD报文的交互过程。

[2017-04-01 16:31:52] [DtlCmn] [1564] SecPkt secPushInner: out-pkt [19]
<data>
inside
70:5A:0F:D5:92:F8
NM6hKAf3
</data>
[2017-04-01 16:31:52] [DtlCmn] [1564] SecPkt secPushInner: the state send before is 1
[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secDataProc: The head id is ad877
[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secDataProc: The type is 14
[2017-04-01 16:31:52] [Dbg] [2708] SecPkt secDataProc: The id is 5733
[2017-04-01 16:31:52] [Warn] [2708] SecPkt secDataProc: matching offline-respnd pckt FAILED.

分析此问题，可以发现iMC在回应的EAD报文中提示服务器要求客户端启用URL访问控制功能。由此可以发现，客户在使用URL访问控制策略时，没有注意到客户端需要定制此功能才可以使用，因此导致EAD报文交互时报错，用户下线。

在iNode客户端发送的1号报文中也可以得到验证，false，表示此iNode不支持URL功能。

在定制iNode客户端时，需要在“高级定制”的“基本功能项”中，勾选“启用URL访问控制功能”，



1、查看EAD报文交互时，可以在iNode客户端的debug日志（iNodeSecPkt）中查看，也可以查看EAD的debug日志，两者可以通过MsgID进行对应

2、使用EAD的某些功能时，一定要注意是否需要iNode客户端进行特殊的定制