CAMS与H3C交换机进行EAD认证的典型配置

冯斯毅　2008-07-04 发表

CAMS和H3C交换机进行802.1X EAD认证的典型配置

CAMS配置

以下配置均需要以系统管理员admin的权限登录CAMS配置台(%CAMSIP%/cams，如http://192.168.4.26/cams/)，缺省密码为Admin。

1.　安全级别：

在安全管理—安全级别可以进行定义，针对每种不同的安全情况，系统都有四种对应的动作（下线，隔离，提醒，监控）来对应，此处可以根据客户的需求来定义各种安全级别。

2.　设置防病毒软件管理

此处可以设置防病毒软件的病毒库，杀毒引擎版本。可根据实际要求设置

3.　软件补丁管理：

EAD补丁检测有两种方式：WSUS自动监测和手工检测。此处以手工检测为例。

此处可以定义EAD解决方案检测的补丁内容。可根据事实际情况进行定制。Windows系统软件补丁名称的定义方法：KB+补丁数字版本号，如：KB896422 （即取补丁文件名“Windows2000-KB896422-x86-CHS.EXE”中间的版本信息）。

4. 配置“可控制软件管理”

此处可定义EAD对客户端软件使用情况的检查。

5. 配置安全策略

安全级别，防病毒软件管理，软件补丁管理，可控软件管理都定义好后，将这些配置引入安全策略中，形成一个安全策略，以后可以被认证用户所申请。同时在安全策略中也可进行其它功能项的设置。

6. 配置“服务”

配置服务，将事前定义好的安全策略引入

7. 账号开户，申请定义好的服务

基本配置至此完毕，可以用eadtest的用户在客户端进行EAD测试了。

交换机配置

此处只是以V3平台H3C交换机S3600-EI作为NAS接入设备做EAD特性相关配置介绍。

配置IP地址及路由

IP、掩码、路由等需要根据实际情况修改配置，达到接入设备与CAMS、自助及管理代理服务器三层可达（即可以ping通）的目的。

配置Radius认证策略及域

配置Radius认证策略：

[H3C] radius scheme cams

[H3C-radius-cams]server-type extended --认证协议（扩展）

[H3C-radius-cams]primary authentication 192.168.4.26 1812 --CAMS认证IP、端口

[H3C-radius-cams]primary accounting 192.168.4.26 1813 --CAMS计费IP、端口

[H3C-radius-cams]key authentication expert --认证密钥

[H3C-radius-cams]key accounting expert --计费密钥(必须与认证密钥相同)

[H3C-radius-cams]user-name-format with-domain –用户名格式（有域名）

配置认证域：

[H3C]domain cams

[H3C-isp-cams] radius-scheme cams --应用上面配置的Radius认证策略

配置缺省域生效：

[H3C]domain default enable cams --配置cams域为缺省认证域

认证和计费密钥、端口如果需要修改，则两个密钥必须相同且与CAMS配置同步

（注意：如果需要给用户申请使用具有不同后缀的多个服务，则需要在我司交换机上配置不同的域，如下：

[H3C]domain huawei-3com

[H3C-isp-huawei-3com] radius-scheme cams --应用Radius认证策略

用户申请了带后缀的服务后，在客户端用该服务认证时必须输入格式如下：用户名@域名，如camsservice@huawei-3com）

配置802.1x认证

[H3C]dot1x --全局启动802.1x认证
[H3C]dot1x port-method macbased --配置基于MAC的认证方式(缺省)
[H3C]dot1x interface Ethernet 0/1 to Ethernet 0/10 --在端口0/1～0/10启动802.1x认证
如果需要可以配置802.1x认证的认证方式，如与LDAP配合需要chap认证方式；而如果需要启用设备无关特性，需要配置为eap透传方式，如下：
[H3C]dot1x authentication-method eap --配置EAP透传模式的认证方式
如果需要限制客户端版本信息，可以使能802.1x认证的版本检测，如下：
[H3C]dot1x --使能802.1x的版本检测功能
如果需要使能客户端防代理功能，需要使能802.1x认证的防代理设置，如下：
[H3C] dot1x supp-proxy-check logoff --使能全局下的防代理功能
[H3C] dot1x supp-proxy-check logoff interface Ethernet 0/1 to Ethernet 0/10
--使能每个端口的防代理功能

配置ACL

EAD方案对认证客户端的安全状态进行检测，然后根据实际认证上网用户PC的状态对其进行访问控制，则需要在设备上配置对应的隔离ACL（对应“隔离区”）和安全上网ACL（对应“Internet”安全区），即安全认证不通过的用户只能被限制在“隔离区”访问，而只有安全认证通过的用户才能正常在安全区进行访问。当用户由于安全问题被隔离时也可被隔离在隔离区域ACL中。

[H3C] acl number 3000 --配置隔离ACL
[H3C-acl-adv-3000]rule 0 permit udp destination-port eq bootps
[H3C-acl-adv-3000]rule 1 permit udp destination-port eq bootpc
[H3C-acl-adv-3000]rule 2 permit ip destination 192.168.4.44 0
[H3C-acl-adv-3000]rule 3 deny ip

[H3C]acl number 3001 --配置安全ACL
[H3C-acl-adv-3001]rule 0 permit ip

说明：EAD方案必须要求客户端在认证上网后无论何时均可以与客户端管理代理服务器进行正常的TCP/IP通讯，所以隔离ACL必须配置可以访问客户端管理代理地址（图1中为192.168.4.44）。隔离ACL 3000中的前两条规则是允许DHCP请求回应报文的可通过性，即如果客户端在认证后要动态获取IP地址则必须配置这两条规则。

注：我司设备的ACL规则匹配原则为“后下发的先匹配”，请在配置时注意。