CAMS证书认证功能的配置

何颖 2006-09-04 发表

CAMS证书认证功能典型配置

一、组网需求：

CAMS服务器（V2版本），安全联动设备LANSwitch，iNode智能客户端，CA证书服务器。

二、组网图：

iNode智能客户端通过LANSwitch与CAMS服务器相联，iNode智能客户端需可以登陆到CA证书服务器上。实际参数请根据实际组网变化：

1) CAMS 服务器（安装CAMSV200R001B01D010实验局版本）IP : 192.168.0.26。

2) LANSwitch （安全联动设备即NAS）IP :192.168.0.100。实验中以S3526E为例。

3) iNode智能客户端 IP:192.168.0.8。

4) CA证书服务器 IP:192.168.0.109。

三、配置步骤：

1．设备侧配置

1.1 配置IP地址及路由

[S3526E]interface Vlan-interface1

[S3526E-Vlan-interface1]]ip address 192.168.0.100 255.255.255.0

[S3526E]ip route-static 0.0.0.0 0.0.0.0 192.168.0.1 preference 60

上述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三层可达（即可以ping通）的目的。

1.2 配置Radius认证策略

[S3526E] radius scheme test

[S3526E-radius-test]server-type huawei

[S3526E-radius-test]primary authentication 192.168.0.26 1812

[S3526E-radius-test]primary accounting 192.168.0.26 1813

[S3526E-radius-test]key authentication 123

[S3526E-radius-test]key accounting 123

[S3526E-radius-test]user-name-format with-domain

1.3 配置认证域

[S3526E]domain heying

[S3526E-isp-heying] radius-scheme test

1.4 配置802.1x认证

[S3526E]dot1x

[S3526E]dot1x authentication-method eap

[S3526E]dot1x interface Ethernet 0/1 to Ethernet 0/10

2．证书的生成

2.1 根证书的生成

1) 利用Windows自带的证书服务器，在IE地址栏中输入证书服务器的IP地址，如：http://192.168.0.109/certsrv，进入Microsoft 证书服务页面。

2) 下载根证书：首先选择【下载一个CA证书，证书链或CRL】，编码方法：Base 64。点击【安装此CA证书链】，就会把根证书安装到控制台中的受信任的根证书颁发机构。

2.2 服务器身份验证证书的生成

1) 进入Microsoft 证书服务页面，点击【申请一个证书】。

2) 然后选择【高级证书申请】。

3) 接着选择【创建并向此CA提交一个申请】。在“需要的证书类型”中选择“服务器身份验证证书”，并选择“标记密钥可导出”。点击【提交】，弹出一提示框后点击【是】。

4) 点击【安装此证书】，证书就会被安装到控制台中。

5) 导出生成的服务器身份验证证书。

点击【导出】。

6) 点击【下一步】：选择导出私钥。

7) 点击【下一步】，选择“启用加强保护”。

8) 点击【下一步】，输入导出密码。

9）【下一步】：输入服务器证书文件存在的位置。例如：E:\server.pfx。

10）点击【完成】。

2.3 客户端身份验证证书的生成

操作步骤和生成服务器身份验证证书的类似，只是在“高级证书申请”中，选择“客户端身份验证证书”。例如：E:\ client.pfx。

3．CAMS上的配置

3.1 在CAMS配置台“ 服务管理>>证书认证策略配置”页面添加服务器验证证书

1）服务器私钥密码：与服务器证书导出时输入的密码一致。

2）服务器证书文件：即上面导出的server.pfx文件。

3）服务器证书私钥文件：可以与添加服务器证书文件一样。

4）根证书文件：添加的是从CA上下载的根证书文件。

【确定】后，进入系统管理>>系统配置页面，点【立即生效】，使得新添加的证书策略生效。

3.2 配置服务

服务管理>>服务配置>>修改服务：把“启用证书认证”的选项选上，认证类型一定要和客户端的配置一致。

3.3 用户开户

用户管理>>帐号用户>>用户开户：增加用户，帐号名和证书上的CN属性值一致。点击【确定】后即可开户成功。之后就可以进行iNode客户端的认证了。

4．客户端的配置

在客户端选择选择【证书认证】，进行【证书设置】：

1）根证书文件：添加的是从CA上下载的根证书文件。

2）用户证书：即为上面导出的client.pfx文件。

3）用户私钥：可以与添加用户证书文件一样。

4）用户私钥密码：与客户端证书导出时输入的密码一致。

设置完成后【确定】，然后可以开始认证了。认证过程中可以看到“正在进行证书验证…”，表明已经启用了证书认证。

四、配置关键点：

请注意在CAMS中配置的用户名必须和证书中的CN(Common Name) field的值一致，如果不一致就会出现认证不上的问题。

在服务器端配置的根证书是用来签发客户端证书的根证书，而在客户端配置根证书是用来签发服务器证书的，如果服务器证书和客户端证书为同一个根证书签发的，那么服务器和客户端配置的根证书应该是一样的。

服务器中服务配置的启用证书认证的类型(EAP-TLS或者EAP-PEAP)，必须和客户端配置的一致，否则认证也不会通过。

证书的生效的时间不能晚于CAMS服务器当前运行的时间，否则也会出现认证不通过的现象。

如果使用windows自带的1x客户端进行证书认证，直接使用生成的客户端证书。首先查看服务，确保“Wireless Zero Configuration”服务启动，之后才可以进行设置。