v7 802.1x本地认证加密

802.1X 陆启隆 2019-08-22 发表

组网及说明

v7的ac集中转发架构下，AP和Client通过DHCP server获取IP地址，并且开启了802.1x本地认证。希望对1x认证进行加密，需要导入证书（必须），而且AC必须使用D029版本，电脑终端结合inode客户端使用，手机终端可直接使用。

配置步骤

通过ftp或者tftp方式将附件cert_BPS.rar中的CA证书cacert.crt和本地证书local.pfx 导入设备。

(1) 配置pki domain，并导入证书。

#创建一个名称为eap-gtc的PKI域，导入CA证书cacert.crt和本地证书local.pfx。

[Device] pki domain eap-gtc

[Device] pki import domain eap-gtc pem ca filename cacert.crt

The trusted CA's finger print is:

MD5 fingerprint:CEA3 E3EF C7B6 6BFD 8D9E 8174 606C 8D8E

SHA1 fingerprint:4D25 EA37 4885 5E94 3B0E 1B83 7AA7 290D 23A6 4EC3

Is the finger print correct?(Y/N):y

[Device] pki import domain eap-gtc p12 local filename local.pfx

Please input the password: 123456

(2) 配置ssl server-policy

#创建一个名称为ssl-eap 的SSL服务器端策略，配置SSL服务器策略所使用的PKI域为eap-gtc。

<Device>system-view

[Device] server-policy ssl-eap

[Device-ssl-server-policy-ssl-eap] pki-domain eap-gtc

(3) 配置eap-profile模板

#创建一个名称为eap-srv 的EAP认证方案，配置的认证方法为PEAP-GTC、引用SSL服务器端策略为ssl-eap。

[Device] eap-profile eap-srv

[Device-eap-profile-eap-srv] method peap-gtc

[Device-eap-profile-eap-srv] ssl-server-policy ssl-eap

(4) 配置全局dot1x认证

#启用EAP中继方式，支持客户端与RADIUS服务器之间所有类型的EAP认证方法。

[Device] dot1x authentication-method eap

(5) 配置ISP模板

创建一个名称为eap-gtc的ISP域，使用local认证、none授权和none计费方法。

[Device] domain eap-gtc

[Device-isp-local] authentication lan-access local

[Device-isp-local] authorization lan-access local

[Device-isp-local] accounting lan-access local

[Device-isp-local] quit

(6)创建本地用户

[Device] local-user localuser class network

[Device] password simple 123456

[Device] service-type lan-access

(7) 配置WLAN 服务模板

创建一个名称为10的服务模板，配置ssid、vlan、认证方式、加密套件、ISP域和eap-profile模板。

[Device] wlan service-template 10

[Device-wlan-st-10] ssid bendi1x

[Device-wlan-st-10] vlan 300

[Device-wlan-st-10] akm mode dot1x

[Device-wlan-st-10] cipher-suite ccmp

[Device-wlan-st-10] security-ie rsn

[Device-wlan-st-10] client-security authentication-mode dot1x

[Device-wlan-st-10] dot1x domain eap-gtc

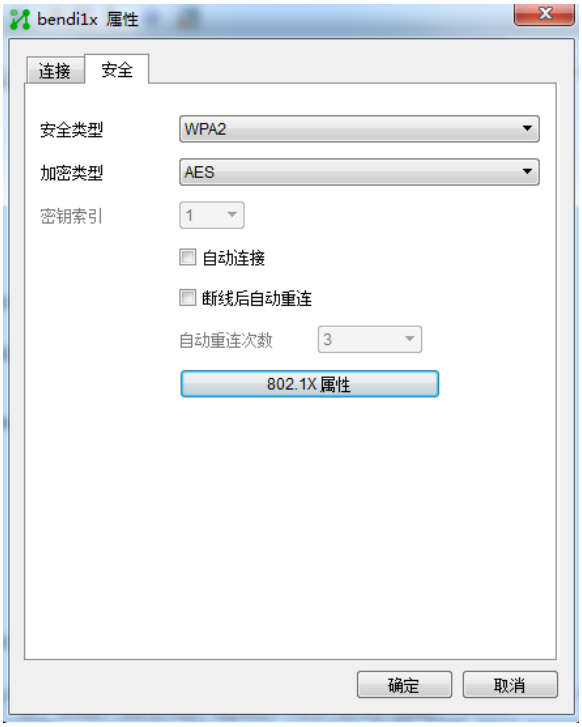
[Device-wlan-st-10] dot1x eap-termination eap-profile eap-srv

[Device-wlan-st-10] service-template enable

(8) 电脑端inode的配置

1.点击无线连接设置属性

2.选择wpa2和aes



3.在1x属性中做如下选择

4.设置完成后点击连接即可。

（9） 手机端的配置

1. 选择不验证证书


20:09
bendi1x
PEAP
阶段2身份验证
无
CA证书
不验证
未指定任何证书。您的网络连接将不是私密连接。
身份
localuser
匿名身份
密码
显示密码
取消
连接

2.点击连接即可

配置关键点

1. 需要使用eap的方式
2. 电脑终端需要使用inode客户端，手机终端需要选择不校验证书
3. 需要给ac上传证书

附件下载：cert_BPS.rar