# WX系列AC无线安全WAPI-标准证书功能的配置

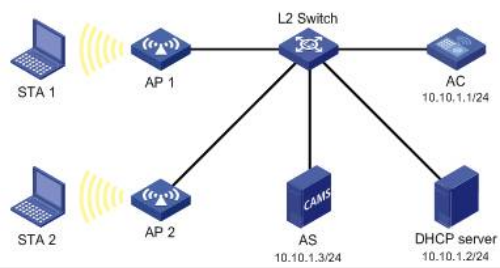
wlan接入 wlan安全 宋斌 2011-08-30 发表

## WX系列AC无线安全WAPI-标准证书功能的配置

**一、 组网需求：**

WX系列AC、FIT AP、便携机（安装有WAPI无线网卡）、AS服务器（本例中使用H3C iMC服务器作为AS服务器）、DHCP Server

**二、 组网图：**




AP 1和AP 2通过二层交换机与AC建立连接，STA 1和STA 2分别通过AP 1和AP 2接入WLAN。STA 1、STA 2、AP 1和AP 2都从DHCP服务器获取IP地址。WAPI系统采用证书鉴别方式中的标准鉴别模式，AP、CA和AS各自所使用的证书ap.cer、ca.cer和as.cer均已保存至AC；单播密钥和组播密钥的更新时间均为20000秒，关闭BK更新功能。

**三、 特性介绍：**

WAPI是无线局域网鉴别和保密基础结构的英文术语WLAN Authentication and Privacy Infrastructure的首字母缩写。这是中国具有自主知识产权的802.11无线局域网络的用户身份认证和数据报文加解密的标准。

本特性提供了标准鉴别模式：即基于WAPI标准协议的UDP模式。在该模式下，AP与AS之间的WAI协议报文将通过UDP方式进行传输，最终完成证书鉴别。该模式不支持对用户的计费功能。WAPI既可以应用到小型无线网络，也应用于大规模部署的无线网络。标准证书的认证方式，提供一种结合认证服务器实现的更高级别安全要求的认证机制。

**四、 配置信息：**

```
#
 version 5.20, release 2115P20
#
 sysname H3C
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
vlan 1
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
pki domain pki1
  crl check disable
  signature-algorithm ecdsa
  peer-entity as1 import
#
user-group system
#
```

```
local-user admin
 password simple admin
 authorization-attribute level 3
 service-type telnet
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan radio-policy 1
 undo wmm enable
#
wlan service-template 1 wapi
 ssid wapi-cer
 bind WLAN-ESS 1
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 10.10.1.1 255.255.255.0
#
interface M-GigabitEthernet2/0/0
#
interface Ten-GigabitEthernet2/0/1
#
interface WLAN-ESS1
 wapi authentication-server ip 10.10.1.3
 undo wapi bk rekey enable
 wapi certificate domain pki1 authentication-server as1
 wapi msk-rekey method time-based 20000
 wapi usk lifetime 20000
 port-security port-mode wapi
#
wlan ap ap1_002 model WA2210-AG
 serial-id 210235A29D0083000778
 radio 1
  radio-policy 1
  service-template 1
  radio enable
#
 dhcp enable
#
 load xml-configuration
#
user-interface con 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

**五、 主要配置步骤：**

# 创建PKI域pki1，在该域中禁止CRL检查（对导入的证书不进行有效期的检查，即默认此方式下用户证书有效），指定证书采用ECDSA签名算法，并配置外部实体as1采用手工导入证书方式。

```
[AC] pki domain pki1
[AC-pki-domain-pki1] crl check disable
[AC-pki-domain-pki1] signature-algorithm ecdsa
[AC-pki-domain-pki1] peer-entity as1 import
```

[AC-pki-domain-pki1] quit

# 分别导入证书文件ap.cer、ca.cer和as.cer。

[AC] pki import-certificate local domain pki1 pem filename ap.cer （ae.cer）
[AC] pki import-certificate ca domain pki1 pem filename ca.cer (root.cer)
[AC] pki import-certificate peer-entity as1 domain pki1 pem filename as.cer (root.cer)

# 使能端口安全功能，并配置接口WLAN-ESS1的端口安全模式为WAPI模式。

[AC] port-security enable
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port-security port-mode wapi

# 在接口WLAN-ESS1上配置WAPI采用证书鉴别方式中的标准鉴别模式；指定AS的IP地址为10.10.1.3，并指定证书所属的PKI域为pki1、AS为as1。

[AC-WLAN-ESS1] wapi authentication method certificate
[AC-WLAN-ESS1] wapi authentication mode standard
[AC-WLAN-ESS1] wapi authentication-server ip 10.10.1.3
[AC-WLAN-ESS1] wapi certificate domain pki1 authentication-server as1

# 在接口WLAN-ESS1上关闭BK更新功能，并配置单播密钥和组播密钥的更新时间均为20000秒。

[AC-WLAN-ESS1] undo wapi bk rekey enable
[AC-WLAN-ESS1] wapi usk lifetime 20000
[AC-WLAN-ESS1] wapi msk-rekey method time-based 20000
[AC-WLAN-ESS1] quit

# 创建射频策略radio1。

[AC] wlan radio-policy 1
[AC-wlan-rp-radio1] undo wmm enable

# 创建类型为WAPI的服务模板1，配置其SSID为wapi1，绑定接口WLAN-ESS1，并使能该服务模板。

[AC] wlan service-template 1 wapi
[AC-wlan-st-1] ssid wapi1
[AC-wlan-st-1] bind wlan-ess 1
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit

（1）配置AP 1相关功能

# 创建型号为wa2200的AP管理模板ap1_002。

[AC] wlan ap ap1 model wa2210-AG
[AC-wlan-ap-ap1] serial-id 210235A29D0083000778

# 创建类型为11b的射频1，配置其与服务模板1关联，射频策略为radio1，并使能该射频。

[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio-policy 1
[AC-wlan-ap-ap1-radio-1] radio enable

# 配置iMC标准证书

# 接入设备配置

1、在iMC配置台的业务标签中的接入业务中选择接入设备配置


2、在接入设备配置页面中选择添加


3、在增加接入设备页面中填入共享密钥，对于标准方式该密钥可以随便配置一个，但是对于radius扩展方式共享密钥必须与设备侧配置的一致，认证计费端口使用默认的即可，接入设备类型使用“H3C”的。配置完成选择手工增加。


4、在弹出页面中的起始IP地址中输入接入设备的IP地址，结束IP地址可以不输入，配置完成点击确定。


5、完成上述配置，需要在业务参数配置中点击系统配置手工生效


# 证书配置

1、在接入业务的业务参数配置中选中证书配置，在证书配置列表中选择WAPI证书配置，点击动作。


2、在根证书配置页面中通过浏览选择一个根证书文件（使用附件中的root.cer）,点击下一步。


3、目前没有WAPI的CA，该页面不需要配置，点击下一步


4、在服务器证书配置页面中配置服务器证书和私钥文件（使用附件中的root.cer和root.key），点击下一步


5、在服务器证书私钥密码配置页面中输入私钥密码，如果没有则不需要输入（附件中的证书没有私钥密码），点击下一步


6、配置完成点击确定


**六、 结果验证：**

本例中采用西电捷通客户端进行验证：

在西电捷通的无线控制管理软件的“参数设置”界面修改“网络SSID”后，进入“安全配置”界面， 选择“证书鉴别”方式。然后，在WAPI STA上面，正确安装证书asue.cer和root.cer证书。其他部分和PSK方式一样。


然后，就可以成功接入WAPI无线网络了。

WAPI用户接入后，检查设备上面WAPI用户接入情况，可以看到如下信息：

```
[H3C] display wapi user
Total number of users: 1
                User information
------------------------------------------------------------
MAC address             : 00-0b-c0-02-5e-39
VLAN                    : 1
Interface               : WLAN-DBSS2:0
Authentication method   : Certificate
Current state           : Online
  Authentication state  : Authenticate success
  USK handshake  state  : Establish
  MSK handshake  state  : Establish
  AAA handshake  state  : Idle
Online time (hh:mm:ss)  : 00:02:26
------------------------------------------------------------
```

**七、 注意事项：**

证书导入过程示例：

配置PKI域并且导入相应证书，这需要先把需要的证书上传到设备上面。这里以


，和证书组为例。这些证书是文件对象，可以拆下来，作为试验使用。假设设备需要导入的证书root.cer和ae.cer已经上传到设备上。

```
dir
Directory of flash:/

  0    -rw-     9270  Mar 14 2008 10:23:40   config.cfg
  1    -rw-  9718892  Apr 15 2008 10:00:15   wx6103.bin
  10   -rw-      615  Apr 18 2008 09:58:24   root.cer
  11   -rw-      805  Apr 18 2008 09:59:37   ae.cer


31750 KB total (22248 KB free)
```

# 配置PKI域。

```
[H3C]pki domain pki1
[H3C-pki-domain-pki1]crl check disable
[H3C-pki-domain-pki1]signature-algorithm ecdsa
Note: Change signature algorithm will impact the use of existing certificates, please d
elete all certificates of the domain.
[H3C-pki-domain-pki1]peer-entity as1 import
[H3C-pki-domain-pki1]quit
```

# 配置PKI域，按照下面顺序导入证书。注意，如果导入证书时顺序不正确，将会导入失败。

```
[H3C]pki import-certificate peer-entity as1 domain pki1 pem filename root.cer
Importing certificates. Please wait a while......
%Apr 18 10:54:12:327 2008 H3C PKI/4/Verify_Cert:Verify certificate CN=root.cer of t
he domain pki1 successfully.....
Import peer entity certificate successfully.
%Apr 18 10:54:17:215 2008 H3C PKI/4/Import_Peer_Entity_Cert:Import peer entity c
ertificate of the domain pki1 successfully.
[H3C]pki import-certificate ca domain pki1 pem filename root.cer
Importing certificates. Please wait a while......
The trusted CA's finger print is:
   MD5  fingerprint:F02E 4528 8269 791A 6A70 0D41 C7D0 5516
   SHA1 fingerprint:2FAF 6D42 BC52 A8FA CB77 49B7 3972 2069 3728 E302

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

%Apr 18 10:54:40:258 2008 H3C PKI/4/Verify_CA_Root_Cert:CA root certificate of t
he domain pki1 is trusted.....
Import CA certificate successfully.
```

%Apr 18 10:54:45:155 2008 H3C PKI/4/Update_CA_Cert:Update CA certificates of the Domain pki1 successfully.
[H3C]
%Apr 18 10:54:45:165 2008 H3C PKI/4/Import_CA_Cert:Import CA certificates of the domain pki1 successfully.
[H3C]pki import-certificate local domain pki1 pem filename ae.cer
Importing certificates. Please wait a while.....
%Apr 18 10:55:48:267 2008 H3C PKI/4/Verify_Cert:Verify certificate CN=ae.cer of the domain pki1 successfully...
Import local certificate successfully.
%Apr 18 10:55:50:715 2008 H3C PKI/4/Import_Local_Cert:Import local certificate of the domain pki1 successfully...
Import key pair successfully.
%Apr 18 10:55:53:185 2008 H3C PKI/4/Import_Local_Key:Import local private key of the domain pki1 successfully.
[H3C]

# 正确导入这些证书后，将会在设备的文件系统中，看到重新生成的证书。

[H3C]return
dir
Directory of flash:/

| | | | | |
|---|---|---|---|---|
| 0 | -rw- | 9270 | Mar 14 2008 10:23:40 | config.cfg |
| 1 | -rw- | 9718892 | Apr 15 2008 10:00:15 | main.bin |
| 10 | -rw- | 615 | Apr 18 2008 09:58:24 | root.cer |
| 11 | -rw- | 805 | Apr 18 2008 09:59:37 | ae.cer |
| 12 | -rw- | 615 | Apr 18 2008 10:54:14 | pki1_peerentity_as1.cer |
| 13 | -rw- | 615 | Apr 18 2008 10:54:42 | pki1_ca.cer |
| 14 | -rw- | 611 | Apr 18 2008 10:55:48 | pki1_local.cer |

31750 KB total (22229 KB free)

如果按照上面顺序，重新导入证书时，有如下提示信息：

[H3C]pki import-certificate local domain pki1 pem filename ae.cer
Both local device and import file has a key, please choose one of them.
[H3C]

则需要把原来已经导入的密钥删除，然后按照上面顺序，重新导入证书。

[H3C]public-key local destroy ecdsa
Warning: Confirm to destroy these keys? [Y/N]: y
.....