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 i MC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W LAN。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 Inf rastructure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A S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

ISC Intelligent Management Center				😫 admin 👩 🚻	助 0 关于
首页 资料	和户 <u>业</u> 务	告誓 系统管理	<b>T</b>	•	Go
业务控制中心 🔺	资源与配置管理				
B 实时攻击告警监控 D 浏览攻击告警 D 小名约利第些管理	型务控制中心				
□ 报表	接入与安全管理				
<b>扶入业务</b> ▲	97 C	-			
<ol> <li>服务配置管理</li> <li>服务配置管理</li> <li>建入区域策略管理</li> <li>建入区域策略管理</li> <li>建入工资箱配置</li> <li>建入工资箱計載</li> <li>中核、工资箱計載</li> <li>中核、工资箱計載</li> <li>中核、工资箱計載</li> <li>中、市場販券</li> <li>電子端升級配置</li> <li>電子端升級配置</li> <li>電子端升級配置</li> </ol>	统入亚分首理 E	200次至管理	<u>米田沢广业分</u>		

2、在接入设备配置页面中选择添加

	首页	资源	R	用户	业务	告警	系統管理		8.	
业务控制中	中心	A	1	业务 >> 技	《入业务 >>	接入设备	en:			
圆 实时	改击告警监持		接.	入设备查询	1					
<ul><li>□ 浏览□</li><li>□ 辿务排</li><li>□ 报表</li></ul>	改击告警 空制策略管理			设备IP地址 设备名称	:		到 接入	设备类型 所有		ġ
19 入小水			接)	设备列表						
<ol> <li>服务配置管理</li> </ol>			共有	增加 (8条记录,	删除 当前第1-8,	第 1/1 页。	改	剧新		每页显示
记 接入日	X规策略管理 + 6.4% 参照管理		T	设备名和	\$r	设计	iP地址	设备型号	接入设备	类型
迎 接入時	时权乘哈官坦		Г	@L0234	5C	10.	53.130.134	ICMP	H3C	
~ 持入山	(名:#2:#1:#100		Г	@10.153	17.42	10.	153.7.42	ICMP	H3C	
in Portal	1277 211 31 10 100 100		Г	GAR28-	80_CE4	10.	153.89.138	Huawei AR28-80	H3C	
山北名参	100.77 IN 211		Г	@AR290	1_106_liuha	0 1.1.	1.1	Huawei AR29-01	H3C	
-8	系统参数配	e I	Г	Cuidw	ay.	10.	153.128.32	Huawei S3026C	H3C	
6	证书配置		Г	@10.153	7.34	10.1	53.7.34	ICMP	H3C	
0	客户端升级]	8	E			10	153 128 36		Hac	

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。

接入配置				
<ul> <li>・ 共享密钥</li> <li>・ 认证端口</li> <li>・ 业务类型</li> </ul>	┃ 1812  LAN接入业务  ▼	<ul> <li>・ 计费端口</li> <li>・ 接入设备类型</li> </ul>	[1813 [H3C	V
设备列表	M.L.			
选择 手工1 中有0条记录。	<b>第70</b> 金融消除。			
	忍久回動計	设备型	룩	国絵

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。

🕗 手工增加接入计	党备 - Microsoft Internet Explorer	
手工增加接入设	<b>A</b>	1813
<ul> <li>・ 起始IP地址 []</li> <li>结束IP地址 []</li> </ul>		H3C
	确定 取消	
副空北	interne	t

	首页 主	EÆ	用户	业务	系统管理					
接入业务	*	1	·务 >> 报	《入业务 >>	接入设备配置					
<ul> <li>2) 服务配置管理</li> <li>2) 接入区域策略管理</li> <li>2) 接入时段策略管理</li> <li>2) 接入时段策略管理</li> </ul>		接入	接入设备查询							
		4	设备IP地址 设备名称	到 接入设备类型	所有					
□ 接入业务拓扑视图 □ 业务参数配置		接入	接入设备列表							
			增加	删除	修改	刷新				
「「「赤坑」	こ 未筑参数配置		1条记录,	当前第1-1,	第 1/1 页。					
10 玄白	端升级配		设备名称	K 设	备IP地址	设备型号	1			
置				10	.153.128.36		H			
《 系统 生效	配置手工									
EAD业务	۸									
第 安全管路	管理									

#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。

族入业务 ▲ 約 服务配置管理			000.0
包 服务配置管理	1 1 业务>> 接入	业务 >> 证书配置	
	证书配置列表		
🖸 接入区域策略管理	配置項名称	描述	动作
接入时段策略管理	EAP证书配置	基于EAP接入方式的证书配置	0
◎ 接入设备配置	WAPI证书配置	基于WAPI接入方式的证书配置	e 💿
★ 人 亚 另 拍 行 代函 ● 並 另 参 数 配置 ○ 案 系 统 参 数 配置 ○ 案 系 统 参 数 配置 ○ 客 户 端 升 级 配置 ○ 客 户 端 升 级 配置 ○ 案 示 就 配置 手 工 4 次 統 配置 手 工			
100	4		
AD业务 A			
	页面中通过浏览	<sup>宽选择一个根证书文件</sup>	(使用附件中的root.cer),,
证书配 1.根证:	书配置 >> 2.CRL配	置 >> 3.服务器证书配置 >>	4.服务器证书私钥密码 >> 5.证
如 中底置1 根证式配要	nn 45.19( 92.		
他近方的直			
* 根址书文件	l		浏览
			15
目前没有WAF	Pl的CA,该页面	可不需要配置, 点击下一	步
目前没有WAF	PI的CA,该页面 书配置 >> 2.CRL 信息预宽	可不需要配置,点击下一 	<b>步</b> 4.服务器证书私钥密码 >> 5.证
目前没有WAF 同 证书配 1.根证 书配 书配面 CRL配置	PI的CA, 该页面 书配置 >> 2.CRL 信息预宽	口不需要配置,点击下一 配置 >> 3.账务器证书配置 >>	-步 - 4. <b>服务器证</b> 书私钥密码 >> 5.证
目前没有WAF <b>董<sup>崔</sup>配</b> 1根证 <b>第配置</b> <b>CRL配置</b> <b>CRL配置</b> <b>CRL配置</b>	PI的CA, 该页面 书配量 >> 2.CRL 信息預覧 更新	可不需要配置,点击下一 配置 >> 3.服务器证书配置 >>	<b>步</b> 4.服务器证书私钥密码 >> 5.证
目前没有WAF <b>送<sup>4</sup>配</b> 1.根证 <b>5</b> <b>6</b> <b>6</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>8</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b> <b>7</b>	PI的CA, 该页面 书配置 >> 2.CRL 信息預覧 更新	口不需要配置,点击下一 配置 >> 3.服务器证书配置 >>	步 4.服务器证书私钥密码 >> 5.ǔ
<ul> <li>目前没有WAF</li> <li> <b>延书配</b> 1.根证 <b>北</b>配置      </li> <li> <b>CRL配置</b> </li> <li> <b>CRL配置</b> </li> <li> <b>反</b>新方式 更新周期(1-30)         </li> </ul>	PI的CA, 该页面 书配量 >> 2.CRL 管急预宽 更新 HTTP D)	□不需要配置,点击下— 【重 >> 3.服务器证书配置 >> ■ ■ 天	步 4.服务器证书私钥密码 >> 5.道
<ul> <li>目前没有WAF</li> <li>運移配 1.根证 移配雪</li> <li>配子</li> <li>1.根证</li> <li>1.根证</li> <li>1.根证</li> <li>5</li> <li>5<td>PI的CA, 该页面 书配置 &gt;&gt; 2.CRL 信息預宽 更新 HTTP D)</td><td>□不需要配置,点击下— <b>已置 &gt;&gt; 3.账务器证书配置 &gt;&gt;</b> ■ ■ 天 时</td><td>步 4.服务器证书私钥密码 &gt;&gt; 5.道</td></li></ul>	PI的CA, 该页面 书配置 >> 2.CRL 信息預宽 更新 HTTP D)	□不需要配置,点击下— <b>已置 &gt;&gt; 3.账务器证书配置 &gt;&gt;</b> ■ ■ 天 时	步 4.服务器证书私钥密码 >> 5.道
<ul> <li>目前没有WAF</li> <li>運移配 1.根证 移配雪</li> <li>配置</li> <li>1.根证</li> <li>1.根证</li> <li>1.根证</li> <li>5</li> <li>5</li> <li>1</li> <li>1<td>PI的CA, 该页面 书配置 &gt;&gt; 2.CRL 電動 更新 IHTTP 3)</td><td>□不需要配置,点击下— <b>已重 &gt;&gt; 3.账务器证书配置 &gt;&gt;</b> ■ ■ 天 时</td><td>步 ▲.服务器证书私钥密码 &gt;&gt; 5.证</td></li></ul>	PI的CA, 该页面 书配置 >> 2.CRL 電動 更新 IHTTP 3)	□不需要配置,点击下— <b>已重 &gt;&gt; 3.账务器证书配置 &gt;&gt;</b> ■ ■ 天 时	步 ▲.服务器证书私钥密码 >> 5.证
. 目前没有WAF <b>证书配 1.根证</b> <b>7.根证</b> <b>7.根证</b> <b>7.根证</b> <b>7.根证</b> <b>7.</b> 意用CRL定时 更新方式 更新闻期(1-30 更新时间(0-23 链接	PI的CA, 该页面 书配置 >> 2.CRL 更新 (HTTP) () () () () () () () () () () () () ()	□不需要配置,点击下— <b>配置 &gt;&gt; 3.服务器证书配置 &gt;&gt;</b> ■ ■ 天 时 ■ 歩 潮试链接 下一步	步 4.服务器证书私钥密码 >> 5.並 取消

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	.CRL配置 >> 3.服务器证书配置 >> 4.服务器证书	私钥密码 >> 5.证
配署服务要证书		
<b>日、日本が始生</b> わ	NL	
L 版为帮证书和私钥任间一人 。 服务器适合合体	+	-
* 旗旁番虹节又件		•
• 服务器证书私钥文件	浏览	
	上一步 下一步 取消	
5、在服务器证书私钥密码 的证书没有私钥密码),力	副置页面中输入私钥密码,如果没有则 点击下一步	不需要输入(附件中
■ <b>证书配</b> 1.根证书配置 >> 2. 考配置信息预定	CRL配置 >> 3.服务器证书配置 >> 4.服务器证书私制	自密码
服务器私钥密码		
服务器私钥密码		
	上一步 下一步 取消	
6、配置完成点击确定	2.CRL配置 >> 3.服务器证书配置 >> 4.服务器证	任书私钥密码
证书配置信息预览		
根证书颁发者	CN=root.cer	
服务展证其主题	Chizroat.cor	
	CN-robicer	
服务器业书有效起始时间	2008-01-05	
服务器证书有效终止时间	2009-01-04	
证书吊销列表更新方式	Import	
	上一步」  确定    取消	
六、结果验证:		
本例中采用西电捷通客户	耑进行验证:	
在西电捷通的无线控制管: 界面,选择"证书鉴别"方: r证书。其他部分和PSK方	里软件的"参数设置"界面修改"网络SSID 弌。然后,在WAPI STA上面,正确安装 式一样。	后,进入"安全配置" 证书asue.cer和root.ce
证书管理		×
序号 序列号 颜	发者(AS)名称 使用者名称 证书	
1 29	root.cer asue.cer 正在他	E.
安装证书	×	
选择安装证书文	+	
安装证书类型:	● X.509 证书 C GBW 证书	
	20 State 1997	

然后,就可以成功接入WAPI无线网络了。

1

用户证书文件: D:\asue.cer

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:

[浏覧(8)...]

**\_\_\_**,

确定(<u>0</u>) 取消(<u>0</u>)

[H3C] display wapi user Total number of users: 1 User information \_\_\_\_\_ MAC address : 00-0b-c0-02-5e-39 VLAN : 1 : WLAN-DBSS2:0 Interface 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 with and the set of t 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 t he 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 th e 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

[H3C]pki import-certificate local domain pki i 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