iMC 802.1X zhiliao_4Dtat 2018-08-25 发表

组网及说明 本案例适用无线802.1X EAP-TLS的认证方式。 本案例中EIA和接入设备使用的版本如下: EIA版本为iMC EIA 7.3(E0511) 接入设备为H3C WX3540H Comware Software, Version 7.1.064, Release 5215P01 iNode客户端版本为iNode 7.3(E0522) 配置步骤 1、设备802.1X认证关键配置 # 配置主认证/计费RADIUS服务器的IP地址为192.168.127.110,认证、计费RADIUS服务器的共享密 钥为明文字符串admin,配置设备发送RADIUS报文使用的源IP地址为192.168.127.33。 radius scheme 1x primary authentication 192.168.127.110 primary accounting 192.168.127.110 key authentication simple admin key accounting simple admin nas-ip 192.168.127.33 # 配置802.1X用户使用RADIUS方案1x进行认证、授权、计费。 domain 1x authentication lan-access radius-scheme 1x authorization lan-access radius-scheme 1x accounting lan-access radius-scheme 1x # 使能RADIUS session control功能。 radius session-control enable # 配置802.1X系统的认证方法为EAP。 dot1x authentication-method eap # 创建并配置无线服务模板1x。 wlan service-template 1x ssid 1x vlan 10 akm mode dot1x cipher-suite ccmp security-ie rsn client-security authentication-mode dot1x dot1x domain 1x service-template enable # 将无线服务模板1x绑定到radio 1和radio 2,并开启射频。 wlan ap I2-software model WA2620i-AGN serial-id 210235AXXXXXX000007 radio 1 radio enable service-template 1x radio 2 radio enable service-template 1x 2、iMC服务器的配置 (1) 由于采用EAP-TLS证书认证, iMC服务器侧需要导入根证书和服务器证书, 客户端需要导入客户 端证书,如果客户端验证服务器证书,客户端还需要安装根证书,本案例中客户端不验证服务器证书 用户>接入策略管理>业务参数配置>证书配置,分别导入根证书和服务器证书。

SD C	29 用户> 接入策略管理> 业务参数配置> 证书配置 ⑦ 帮					
	证书文件校验 已导入证书校验 导入预置证书					
	 ●提示 同一种类型的服务器证书只能上传一个。 					
	根证书配置服务器证书配置					
	导入EAP根证书 导入WAPI根证书					
	優发者 \$	主題 ≎	类型 \$	动作		
	CN=WIN-OIR9LETTM24-CA	CN=WIN-0IR9LETTM24-CA	EAP根证书			

(2) 用户>接入策略管理>接入设备管理>接入设备配置,增加认证接入设备192.168.127.33。

「入配置						
认证端口 *	1812		计删	高口 * 1	.813	
业务类型	不限	*	强制	下线方式	所开用户连接	•
接入设备类型	H3C (General)	-	业务	3组 3	未分组 •	•
共享密钥 *			确认	+享密钥*		
摘入位置分组	无	-				
洛列表 选择 手工増加 :	全部清除					
设备名称	设备P地址		设备型号	音注		削除
	192.168.127	33			ť	Ì

注意:增加的接入设备IP需要和认证设备radius scheme下的nas-ip一致,共享密钥需要和radius sche me下的认证、计费radius服务器的密钥一致。

(3) 用户>接入策略管理>接入策略管理,增加接入策略tls,首选EAP类型选择EAP-TLS,其他参数 保持缺省即可。

● 用户> 接入策略管理> 接)	↓用户 > 抽入策略管理 > 描入策略管理 > 描加接入策略					
基本信息					-	
接入策略名 * 业务分组 * 描述	tls 未分组	•				
授权信息					-	
接入时段 下行連案(Kbps) 优先级	π.	-	分配P地址 * 上行速率(Kbps) 下发用户组	KI	•	
首选EAP类型 FAP白协商	EAP-TLS 白田	•	单次最十五线时长(分钟)		0	
	A47.0		TO BE CLEARED NUMBER		U	

(4) 用户>接入策略管理>接入服务管理,增加接入服务tls,服务后缀配置为空,缺省接入策略选择tls

92 用户> 接入策略管理> 接入服务管理	▌> 増加接入服务				?帮助
基本信息					-
服务名 *	tls		服务后缀		
业务分组 *	未分组 🔻		缺省接入策略*	tis	
缺省安全策略 *	不使用 👻		缺省内网外连策略 *	不使用	
缺省私有属性下发策略 *	不使用	0			
缺省单帐号最大绑定终端数*	0	?	缺省单帐号在线数重限制*	0	?
单日累计在线最长时间(分钟) *	0	?			
服务描述					
✔ 可申请 ?			🖌 无感知认证 ②		

(5) 用户>接入用户,增加并配置接入用户whjuser2,接入服务分配tls。

用户姓名 *	wanghong 选择	増加用户			
帐号名 *	whjuser2				
预开户用户	缺省BYOD用户	MAC地址认证用户	主机名用户	快速认证用户	
密码 *		密码确认 *			
✔ 允许用户修改密码	启用用户	密码控制策略	下次登录需修改	密码	
生效时间		失效时间			
最大闲置时长(分钟)		在线数量限制			
登录提示信息					
接入服务					-
服务名		服务后缀	缺省安全策略	状态	分配IP地址
1x		1x	不使用	可申请	
V tls		1х	不使用	可申请	

3、客户端的配置

(1) 使用iOS手机终端拨号测试

连接SSID为1x的信号, 输入用户名001@1x和密码, 点击信任证书, 终端上线。

18:31 -	1	.111 4G 🔳
	输入"1x"的密码	
取消	输入密码	加入
用户名	001@1x	
密码	•••	
模式		自动 >
18.32 4		
10.52 7		111 40 E
取消	证书	信任
	imc.h3c.com 签发者: GeoTrust SSL CA - G3	
	不可信	
过期日!	8 2019/7/14 07:59:59	
更多详细	信息	>

(1) 使用Windows 7电脑终端拨号测试

双击客户端证书文件开始导入客户端证书,打开Internet选项>内容>证书,可以查看客户端证书whjuse r2已安装导入成功。



管理无线网络下手动添加SSID 1x的无线网络连接:

	控制面板 🕨 网络和 Internet 🕨	管理无线网络	-
管理使用(Windows 将	🚱 🔐 手动连接到无线网络		1
添加 适配器属	输入您要添加的无线	网络的信息	
您可以查看、修改	网络名(E):	1x	支持项
2	安全类型(S):	WPA2 - 企业/	
, jn	加密类型(R):	AES 🔹	支持项
mayuan mayuan	安全密钥(C):	□ 隐藏字符(H)	支持项
	自动启动此连接(T)		支持项
iPhone×	即使网络未进行广播 警告:如果选择此选项	也连接(C) 页,则计算机的隐私信息可能存在风险。	支持项
iPhone6			支持项
<			7 特. 印

手动添加无线网络连接后,右键设置属性:

1x 无线网络属性		1001	×
连接 安全			
安全类型(E):	WPA2 - 企业		-
加密类型(N):	AES		•
选择网络身份验证方	方法 (0):		
Microsoft: 智能卡	≂或其他证书		5)
☑ 每次登录时记住	此连接的凭据(B	0	
		确定	取消

网络身份验证方法选择智能卡或其他证书,点击设置,这里客户端不验证服务器证书,去勾选"验证服务器证书":



设置无线网络连接属性后,连接信号1x,弹出的网络身份验证中选择证书whjuser2,点击确定进行认证:

选择证书	
证书上的用户名()):
whjuser2	•
友好名称:	
颁发者:	WIN-OIR9LETTM24-CA
截止日期:	2019/6/18 14:54:24
	确定 取消 查看证书(V)

终端连接SSID 1x成功之后,用户>在线用户,可以查看到whjuser2的在线信息:

🗓 用户 > 在线用户									步 加入收	藤 ⑦ 帮
本地在线用户	漫游在线用户	□ 设备在线	用户							
本地在线用户查询									高	级查询
帐号名	1				用户姓名					
用户IP地址从					至					
用户分组				ů ^ů â					查询	重置
消息下发 强制	下线 清除花	:线信息 重认	证 定制	界面 批量导出						
帐号名 ≎	登录名≎	用户姓名 \$	服务名	接入时间 \$	接入时长 \$	设备IP地址 ≎	用户IP地址 ≎	安全状态 \$	容户端定制时间 \$	操作
whjuser2	whjuser2	wanghong	tls	2018-07-23 19:58:13	0秒	192.168.127.33	192.168.127.42	无需安全认证		

(2) Windows 7电脑使用iNode客户端拨号

打开iNode客户端,右上角无线图标选择使用iNode客户端管理无线网络,然后选择无线网络SSID信号 1x:

	rn ♥ - ★ Node智能客户端
Ÿ≓1x	• C
用户名	
密码	
域	•
☑ 保存	明户名 🗸 保存密码
	连接 ▼

点击连接旁边的下拉选项选择属性进行设置:

<mark>%</mark> 1x 属性	-X-
连接 安全	
安全类型	WPA2
加密类型	AES 🔹
密钥索引	1 -
	□ 自动连接
	🗐 断线后自动重连
	自动重连次数 3 🔻
	802.1X 属性
	确定 取消

点击802.1X属性进行设置,认证类型选择EAP-TLS,本案例中客户端不验证服务器证书,去勾选验证 服务器证书:

2 802.1X 属性	X
网络设置 连接设置	
 普通连接 	
◎ 单点登录连接	
认证类型	
EAP-TLS	选择客户端证书
◎ PEAP 子类型	自动 🔻
◎ EAP-TTLS 子类型	
🔲 验证服务器证书	
□ 从证书中读取用户名	
	确定 取消

选择客户端证书中选择客户端证书whjuser2:

	↓ 选择证书			
	颁发给	颁发者	预期目的	截止时
		issueca	客户端验证,安全电	2022-12-15
	whjuser2	WIN-0IR9LETTM2	客户端验证	2019-06-18

输入用户名whjuser2, 点击连接开始认证:

	™ Er Node智能客户端	• • - ×
¶∎l1x		• C
用户名	whjuser2	
域		-
✓ 保存	· 序用户名	
	连接	•

认证成功:



配置关键点

1、EAP-TLS认证iMC服务器侧必须导入服务器证书和客户端证书对应的根证书。

客户端侧必须导入客户端证书,如果客户端验证服务器证书,客户端还需要导入服务器证书对应的根 证书。

2、在iMC服务器勾选"检查帐号名与证书中的属性"的情况下,客户端证书名必须和iMC服务器接入用户 名一致,否则会认证失败,提示"E63500:证书标识与用户名不匹配。"

如果不勾选"检查帐号名与证书中的属性",客户端输入的用户名可以和客户端证书名不一样,但是必须 保证在iMC服务器上已经创建好此接入用户并分配了EAP-TLS认证对应的接入服务。

其中是否检查帐号名与证书中的属性可以在用户>接入策略管理>业务参数配置>系统配置>系统参数配置页面进行配置,缺省为勾选。

客户端保护密码			确认密码		
用户认证仿真模式	禁用 ▼	?	接入明细零点切换	禁用 ▼	?
动态密码长度 *	4	?	短信认证图形验证码有效期(分钟) *	5	?
哑终端激活后再上线	禁用 ▼	?	客户端IP地址冲突检测	禁用	?
用户名后缀处理方式	是 🔻	?			
认证出现数据库错误时报文处理方式	回应认证拒绝报文		• ?		
下发Session Timeout属性	都下发		• (?)		
检查帐号名与证书中的属性					