

知 WX3024 HTTPS方式本地Portal功能的典型配置(Local_Auth)

杨杰 2008-10-24 发表

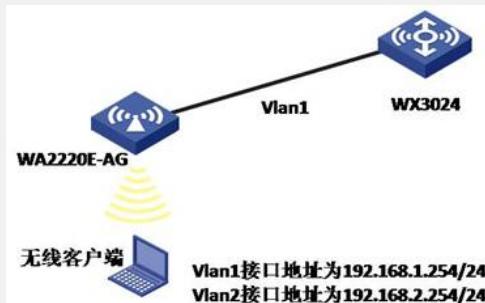
WX3024 HTTPS方式本地Portal功能的典型配置(Local_Auth)

适用WX3024版本：Comware Software, Version 5.20, Release 3106

一、组网需求

WX3024、WA2220E-AG、便携机（安装有11b/g无线网卡）

二、组网图



WX3024上VLAN1、2的IP地址分别为192.168.1.254、192.168.2.254。
WA2220E-AG处在VLAN1。

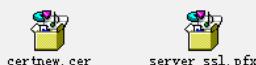
无线客户端处在VLAN2。

本例中WA2220E-AG的序列号为210235A29F0081000109。

SSID的名称为*H3C-local-portal*。

三、WX3024配置步骤

将证书文件拷贝到AC Flash中：



修改ac系统时间：15:00 2008/10/17

将证书文件导入AC Flash中：

[AC]pk1 import-certificate ca domain do der filename certnew.cer

```
[AC]pk1 key local destroy t1
Warning: Confirm to destroy these keys? [Y/N]:y
[AC]pk1 import-certificate ca domain do der filename certnew.cer
The trusted CA's finger print is:
    MD5 Fingerprint: 5710 DB77 4771 641F 6C36 9CF4 35B6 9CAF
    SHA1 Fingerprint: 02AB BAB7 F8C0 8D16 329C 9B4B 5FBD B449 A1FB 24PA
Is the finger print correct? [Y/N]:y
[May 22 15:06:32:437 2008 H3C PKI]4/Verify CA Root Cert:CA root certificate of the domain do is trusted...
[May 22 15:06:42:401 2008 H3C PKI]4/Import CA certificate successfully.
[May 22 15:06:42:401 2008 H3C PKI]4/Update CA Cert:Update CA certificates of the Domain do successfully.
[May 22 15:06:42:501 2008 H3C PKI]4/Import CA Cert:Import CA certificates of the domain do successfully.
```

[AC]pk1 import-certificate local domain do p12 filename server_ssl.pfx

输入密码：123

```
[AC]pk1 import-certificate local domain do p12 filename server_ssl.pfx
Please input challenge password: [REDACTED]
[May 22 15:07:05:625 2008 H3C PKI]4/Verify certificate of the domain do successfully...
[May 22 15:07:05:625 2008 H3C PKI]4/Import local Cert:Import local certificate of the domain do successfully.
Import key pair successfully.
[May 22 15:07:30:702 2008 H3C PKI]4/Import local Cert:Import local certificate of the domain do successfully.
```

配置PKI实体和域

[AC]pk1 entity en

[AC-pki-entity-en]common-name portal

[AC-pki-entity-en]organization portal_server

[AC]pk1 domain do

[AC-pki-domain-do]certificate request entity en

[AC-pki-domain-do]crl check disable

配置SSL服务策略

[AC]ssl server-policy 1

[AC-ssl-server-policy-1]pk1-domain do

[AC-ssl-server-policy-1]handshake timeout 180

[AC-ssl-server-policy-1]close-mode wait

[AC-ssl-server-policy-1]session cachesize 1000

配置本地认证用户名

```
[AC] local-user portal
[AC-luser-portal]service-type portal
[AC-luser-portal]password simple portal
# 配置无线服务模板
[AC] wlan service-template 2 clear
[AC-wlan-st-2]ssid H3C-local-portal
[AC-wlan-st-2]bind WLAN-ESS 2
[AC-wlan-st-2]service-template enable
# 配置无线口, 添加到起Portal的vlan
[AC] interface WLAN-BSS 2
[AC-WLAN-BSS2] port access vlan 2
# 在AC下绑定无线服务模板
[AC-wlan-ap-ap_001]wlan ap ap_001 model WA2220E-AG
[AC-wlan-ap-ap_001]serial-id 210235A22W0073000002
[AC-wlan-ap-ap_001]radio 2
[AC-wlan-ap-ap_001-radio-2]service-template 2
[AC-wlan-ap-ap_001-radio-2]radio enable
# 配置Portal Server和免认证规则
[AC] portal server local ip 192.168.1.254
[AC] portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
[AC] portal local-server https server-policy 1
[AC] interface Vlan-interface 2
[AC-Vlan-interface1]ip address 192.168.2.254 24
[AC-Vlan-interface1]portal server local method direct

四、WX3024交换机的典型配置
#
version 5.20, Release 3106
#
sysname AC
#
domain default enable system
#
telnet server enable
#
port-security enable
#
portal server local ip 192.168.1.254
portal free-rule 0 source interface GigabitEthernet1/0/1 destination any
portal local-server https server-policy 1
#
oap management-ip 192.168.0.101 slot 0
#
vlan 1
#
vlan 2
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
pki entity en
common-name portal
organization portal_server
#
pki domain do
certificate request entity en
crl check disable
#
dhcp server ip-pool vlan1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.254
```

```
#  
dhcp server ip-pool vlan2  
network 192.168.2.0 mask 255.255.255.0  
gateway-list 192.168.2.254  
#  
user-group system  
#  
local-user admin  
password simple admin  
authorization-attribute level 3  
service-type telnet  
local-user portal  
password simple portal  
service-type portal  
#  
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 service-template 2 clear  
ssid H3C-local-portal  
bind WLAN-ESS 2  
service-template enable  
#  
ssl server-policy 1  
pki-domain do  
handshake timeout 7200  
close-mode wait  
session cachesize 1000  
#  
interface NULL0  
#  
interface Vlan-interface1  
ip address 192.168.1.254 255.255.255.0  
#  
interface Vlan-interface2  
ip address 192.168.2.254 255.255.255.0  
portal server local method direct  
#  
interface GigabitEthernet1/0/1  
port link-type trunk  
port trunk permit vlan all  
#  
interface WLAN-ESS2  
port access vlan 2  
#  
wlan ap ap_001 model WA2220E-AG  
serial-id 210235A29F0081000109  
radio 1  
radio 2  
service-template 2  
radio enable  
#  
dhcp enable  
#  
load xml-configuration  
#  
user-interface aux 0  
user-interface vty 0 4  
authentication-mode scheme
```

```
user privilege level 3
```

```
#
```

```
return
```

五、验证结果

1、客户端的相关配置

在STA上打开IE，输入IP地址(在有DNS的情况下可直接输入网址)，弹出警报对话框，选择“继续浏览此网站”。



切换到HTTPS的认证页面，输入帐号，完成认证。

The first screenshot shows the 'Portal Web Authentication' page. It has two input fields: 'User name:' containing 'portal' and 'Password:' containing several asterisks. Below the fields are two buttons: 'Logon' and 'Logoff'.
The second screenshot shows the 'Authentication passed!' confirmation page. It has a single button labeled 'Logoff'.

七、Q&A

WX3024设备上没有时钟芯片，设备重启后造成设置的时间丢失，导致导入的证书无法正常使用，可以使用NTP时钟同步的方式解决，在网络中配置一台能够保存时钟的NTP Server，将该服务器配置为证书能够正确导入的时钟，并将设备上的NTP对等体指向该服务器IP地址192.168.1.100。

NTP服务配置：

```
ntp-service unicast-peer 192.168.1.100 source-interface Vlan-interface1
```