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

杨杰 2008-10-20 发表

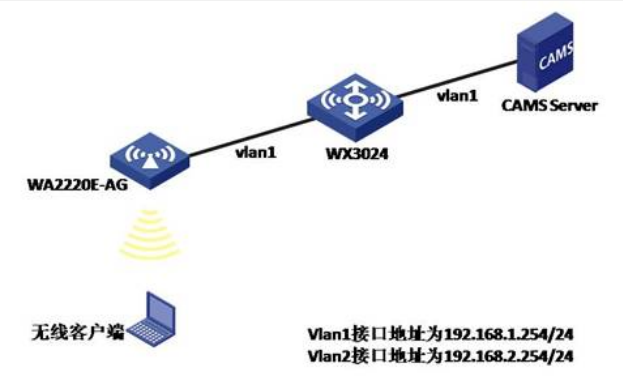
WX3024 HTTPS方式本地Portal功能的典型配置(CAMS_Auth)

适用WX3024版本：Comware Software, Version 5.20, Beta 3105P01

一、组网需求

WX3024、WA2220E-AG、便携机（安装有11b/g无线网卡）、CAMS服务器

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与CAMS服务器同处在VLAN1。

CAMS服务器的IP地址为192.168.1.10。

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***。

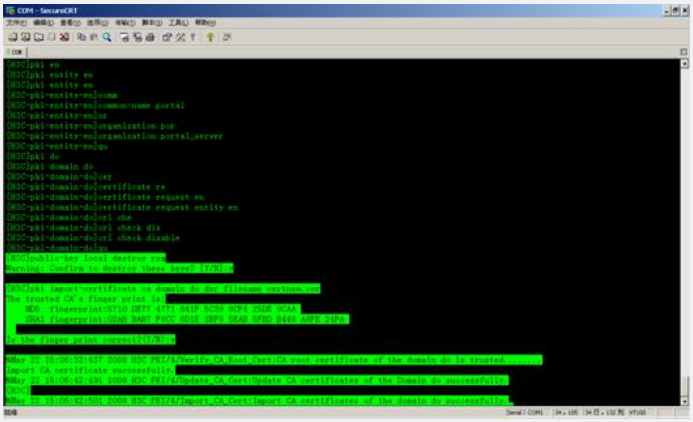
三、WX3024配置步骤

将证书文件拷贝到AC Flash中：

修改ac系统时间：15:00 2008/10/17

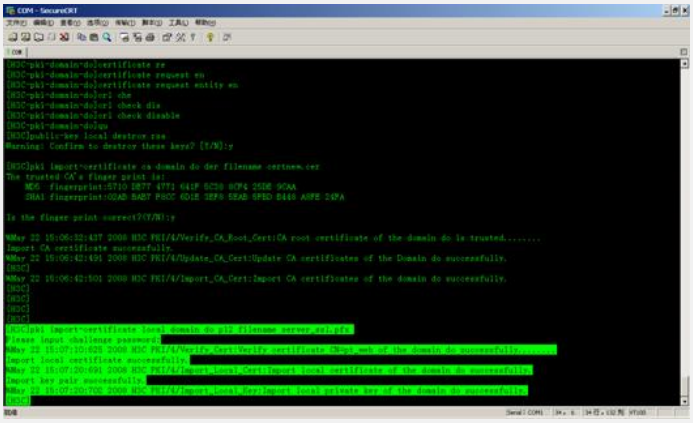
将证书文件导入AC Flash中：

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



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

输入密码：123



配置SSL服务策略
[AC]ssl server-policy 1
[AC-ssl-server-policy-1]pki-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
应用SSL服务策略、开启HTTPS服务
[AC]ip https ssl-server-policy 1
[AC]ip https enable
配置PKI实体和域
[AC]pki entity en
[AC-pki-entity-en]common-name portal
[AC-pki-entity-en]organization portal_server
[AC]pki domain do
[AC-pki-domain-do]certificate request entity en
[AC-pki-domain-do]crl check disable
配置认证策略
[AC]radius scheme cams
[AC-radius-cams]server-type extended
[AC-radius-cams]primary authentication 192.168.1.10
[AC-radius-cams]primary accounting 192.168.1.10
[AC-radius-cams]key authentication h3c
[AC-radius-cams]key accounting h3c
[AC-radius-cams]nas-ip 192.168.1.254
配置认证域
[AC]domain cams
[AC-isp-cams]authentication portal radius-scheme cams
[AC-isp-cams]authorization portal radius-scheme cams
[AC-isp-cams]accounting portal radius-scheme cams
配置无线服务模板
[AC]wlan service-template 2 clear
[AC-wlan-st-2]ssid lopo
[AC-wlan-st-2]bind WLAN-ESS 2
[AC-wlan-st-2]service-template enable
配置无线口，将无线口添加到起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 url https://192.168.1.254/portal
[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, Beta 3105P01
#
 sysname AC
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 portal server local ip 192.168.1.254 url https://192.168.1.254/portal
 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
#
radius scheme cams
 server-type extended
 primary authentication 192.168.1.10
 primary accounting 192.168.1.10
 key authentication h3c
 key accounting h3c
 nas-ip 192.168.1.254
#
domain cams
 authentication portal radius-scheme cams
 authorization portal radius-scheme cams
 accounting portal radius-scheme cams
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
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
#
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
#
 ip https ssl-server-policy 1
 ip https enable
#
 load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

五、CAMS配置：

1、增加服务配置

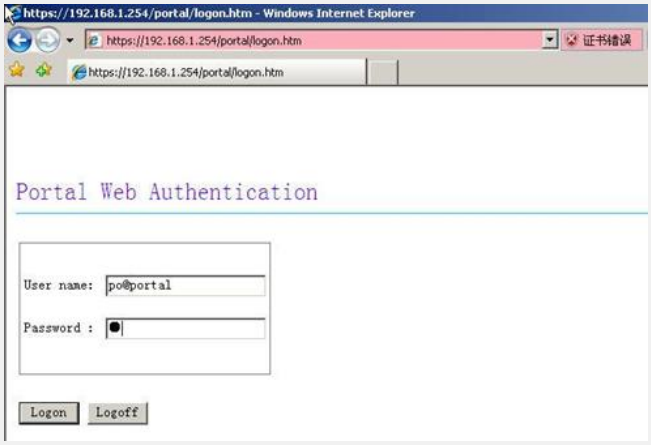
2、增加用户帐号

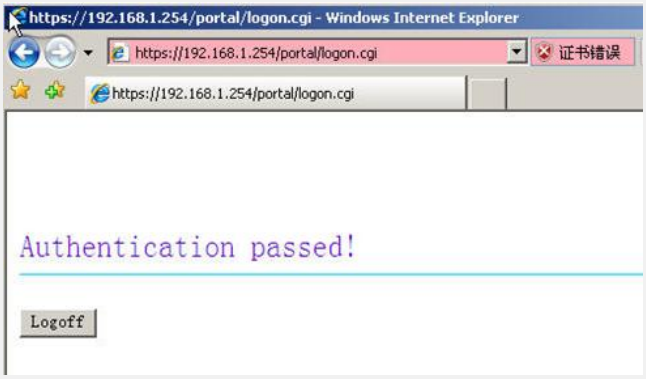
六、验证结果

1、RADIUS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。





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，因此需要重新导入。

重新导入证书的方法：

申请的根证书重命名为certnew.cer使用命令直接导入；

申请的服务器验证证书重命名为server_ssl.pfx，但需要删除原有证书再导入，删除原证书命令：

public-key local destroy rsa

(Y/N)y