S3500-EA系列交换机证书属性的访问控制策略功能的配置

岳斌 2008-09-03 发表

S3500-EA系列交换机证书属性的访问控制策略功能的配置

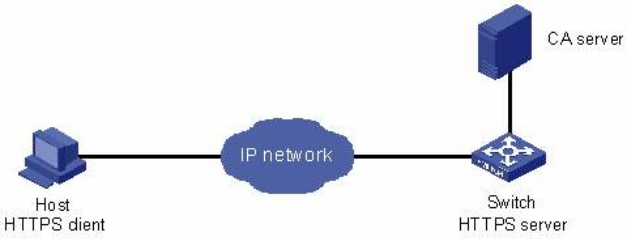
一、 组网需求：

（1）客户端通过HTTPS（HTTP Security，HTTP安全）协议远程访问设备（HTTPS服务器）。

（2）通过SSL协议保证合法客户端安全登录HTTPS服务器。

（3）为HTTPS服务器制定证书属性的访问控制策略，对客户端的访问权限进行控制。

二、 组网图：



三、 配置步骤：

（1）配置PKI域参数

创建并进入PKI域torsa。

[Switch] pki domain torsa

配置可信任的CA名称为myca。

[Switch-pki-domain-torsa] ca identifier myca

配置注册服务器URL，格式为http://host:port/Issuing Jurisdiction ID。其中的Issuing Jurisdiction ID为CA服务器上生成的16进制字符串。

[Switch-pki-domain-torsa] certificate request url http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337

配置证书申请的注册受理机构为CA。

[Switch-pki-domain-torsa] certificate request from ca

指定实体名称为aaa。

[Switch-pki-domain-torsa] certificate request entity aaa

配置CRL发布点位置。

[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl

[Switch-pki-domain-torsa] quit

（2）配置HTTPS服务器

配置HTTPS服务器使用的SSL策略。

<Switch> system-view

[Switch] ssl server-policy myssl

[Switch-ssl-server-policy-myssl] pki-domain torsa

[Switch-ssl-server-policy-myssl] client-verify enable

[Switch-ssl-server-policy-myssl] quit

（3）配置证书属性组

配置证书属性组mygroup1，并创建两个属性规则。规则1定义证书主题名的DN包含字符串aabbcc；规则2定义证书颁发者名中的IP地址等于10.0.0.1。

[Switch] pki certificate attribute-group mygroup1

[Switch-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc

[Switch-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1

[Switch-pki-cert-attribute-group-mygroup1] quit

配置证书属性组mygroup2，并创建两个属性规则。规则1定义证书备用主题名中的FQDN不包含字符串apple；规则2定义证书颁发者名的DN包含字符串aabbcc。

[Switch] pki certificate attribute-group mygroup2

[Switch-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple

[Switch-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc

[Switch-pki-cert-attribute-group-mygroup2] quit

（4）配置证书访问控制策略

配置访问控制策略myacp，并建立两个控制规则。

[Switch] pki certificate access-control-policy myacp

[Switch-pki-cert-acp-myacp] rule 1 deny mygroup1
[Switch-pki-cert-acp-myacp] rule 2 permit mygroup2
[Switch-pki-cert-acp-myacp] quit
（5）配置HTTPS服务器与相关策略进行关联，并启动HTTPS服务器
配置指定HTTPS服务器的SSL策略为myssl。
[Switch] ip https ssl-server-policy myssl
配置指定HTTPS服务器的证书访问控制策略为myacp。
[Switch] ip https certificate access-control-policy myacp
启动HTTPS服务器。
[Switch] ip https enable
四、 配置关键点：
配置证书属性控制规则时，group-name必须是已存在的证书属性组的名称。