S3500-EA系列交换机SSL-HTTPS功能的配置

岳斌 2008-09-03 发表

S3500-EA系列交换机SSL-HTTPS功能的配置

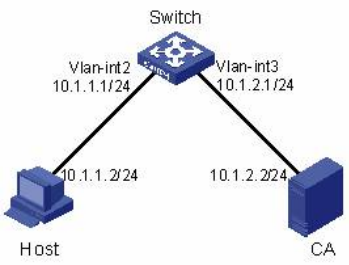
一、 组网需求：

（1）Switch作为HTTPS服务器；

（2）Host作为HTTPS客户端，通过基于SSL的HTTP协议访问HTTPS服务器；

（3）CA（Certification Authority，认证机构）为Switch颁发证书。

二、 组网图：



三、 配置步骤：

（1）为Switch申请证书

配置PKI实体。

<Sysname> system-view

[Sysname] pki entity en

[Sysname-pki-entity-en] common-name http-server1

[Sysname-pki-entity-en] fqdn ssl.security.com

[Sysname-pki-entity-en] quit

配置PKI域。

[Sysname] pki domain 1

[Sysname-pki-domain-1] ca identifier ca1

[Sysname-pki-domain-1] certificate request url

http://10.1.2.2/certsrv/mscep/mscep.dll

[Sysname-pki-domain-1] certificate request from ra

[Sysname-pki-domain-1] certificate request entity en

[Sysname-pki-domain-1] quit

用RSA算法生成本地的密钥对。

[Sysname] public-key local create rsa

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It will take a few minutes.

Press CTRL+C to abort.

Input the bits of the modulus[default = 1024]:

Generating Keys...

.....++++++

.....++++++

.....++++++++

....++++++++

.....

从CA获取服务器证书。

[Sysname] pki retrieval-certificate ca domain 1

本地证书申请。

[Sysname] pki request-certificate domain 1

（2）配置HTTPS服务使用的SSL服务器端策略

创建一个名为myssl的SSL服务器端策略。

[Sysname] ssl server-policy myssl

配置SSL服务器端策略使用的PKI域名为1。

[Sysname-ssl-server-policy-myssl] pki-domain 1

配置服务器端需要认证客户端。

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

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

（3）配置HTTPS服务与SSL服务器端策略关联，并使能HTTPS服务

配置HTTPS服务使用的SSL策略为myssl。
[Sysname] ip https ssl-server-policy myssl
使能HTTPS服务。
[Sysname] ip https enable
（4）验证配置结果
在Host上打开IE浏览器，输入网址https://10.1.1.1，可以登录Switch，并实现对Switch的控制。
四、 配置关键点：
（1）在进行SSL服务器端策略配置之前，需要先配置PKI（Public Key Infrastructure，公钥基础设施）域。
（2）如果服务器端需要对客户端进行基于证书的身份验证，即配置了client-verify enable命令，而SSL客户端的证书不存在或不能被信任，则必须先为SSL客户端申请并安装证书。
（3）如果服务器端证书不能被信任，请在SSL客户端安装为SSL服务器颁发证书的CA服务器根证书，或服务器向SSL客户端信任的CA服务器重新申请证书。
（4）使用display ssl server-policy命令查看SSL服务器端策略支持的加密套件。如果SSL服务器端和客户端支持的加密套件不匹配，请用ciphersuite命令修改SSL服务器支持的加密套件。
（5）关闭HTTPS服务后，将自动取消HTTPS服务与SSL服务器端策略的关联。再次使能HTTPS服务之前，需要重新配置HTTPS服务与SSL服务器端策略关联。
（6）使能HTTPS服务，会触发SSL的握手协商过程。在SSL握手协商过程中，如果设备的本地证书已经存在，则SSL协商可以成功，HTTPS服务可以正常启动；如果设备的本地证书不存在，则SSL协商过程会触发证书申请流程。由于证书申请需要较长的时间，会导致SSL协商不成功，从而无法正常启动HTTPS服务。因此，在这种情况下，需要多次执行ip https enable命令，这样HTTPS服务才能正常启动。