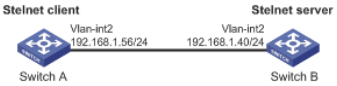
设备支持Stelnet Suite B配置举例（128-bit）

SSH 郑标 2020-09-28 发表

组网及说明



配置Switch A作为Stelnet Suite B客户端，用户能够通过Switch A安全地登录到Switch B上；
SwitchB设备配置为suite-b服务器模式；
用户可以通过Switch A上运行的Stelnet Suite B客户端软件（SSH2版本）安全地登录到Switch B上，并被授予用户角色network-admin进行配置管理；
Switch B采用publickey认证方式对Stelnet Suite B客户端进行认证。

配置步骤

(1) Suite B客户端
客户端和服务器证书生成后，需要将保存的证书文件ssh-server-ecdsa256.p12和ssh-client-ecdsa256.p12通过FTP/TFTP方式上传到客户端设备，具体过程略。
配置验证服务器证书的PKI域。
<SwitchA> system-view
[SwitchA] pki domain server256
关闭CRL检查。
[SwitchA-pki-domain-server256] undo crl check enable
[SwitchA-pki-domain-server256] quit
导入CA证书。
[SwitchA] pki import domain server256 p12 local filename ssh-server-ecdsa256.p12
The system is going to save the key pair. You must specify a key pair name, which is a case-insensitive string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: server256]:
显示导入CA证书信息。
[SwitchA] display pki certificate domain server256 local
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 3 (0x3)
  Signature Algorithm: ecdsa-with-SHA256
    Issuer: C=CN, ST=Beijing, L=Beijing, O=H3C, OU=Software, CN=SuiteB CA
    Validity
      Not Before: Aug 21 08:39:51 2015 GMT
      Not After : Aug 20 08:39:51 2016 GMT
    Subject: C=CN, ST=Beijing, O=H3C, OU=Software, CN=SSH Server secp256
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
        Public-Key: (256 bit)
        pub:
          04:a2:b4:b4:66:1e:3b:d5:50:50:0e:55:19:8d:52:
          6d:47:8c:3d:3d:96:75:88:2f:9a:ba:a2:a7:f9:ef:
          0a:a9:20:b7:b6:6a:90:0e:f8:c6:de:15:a2:23:81:
          3c:9e:a2:b7:83:87:b9:ad:28:c8:2a:5e:58:11:8e:
          c7:61:4a:52:51
        ASN1 OID: prime256v1
        NIST CURVE: P-256
    X509v3 extensions:
      X509v3 Basic Constraints:
        CA:FALSE
      Netscape Comment:
        OpenSSL Generated Certificate
      X509v3 Subject Key Identifier:
        08:C1:F1:AA:97:45:19:6A:DA:4A:F2:87:A1:1A:E8:30:BD:31:30:D7
      X509v3 Authority Key Identifier:
        keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22

```
    Signature Algorithm: ecdsa-with-SHA256
        30:65:02:31:00:a9:16:e9:c1:76:f0:32:fc:4b:f9:8f:b6:7f:
        31:a0:9f:de:a7:cc:33:29:27:2c:71:2e:f9:0d:74:cb:25:c9:
        00:d2:52:18:7f:58:3f:cc:7e:8b:d3:42:65:00:cb:63:f8:02:
        30:01:a2:f6:a1:51:04:1c:61:78:f6:6b:7e:f9:f9:42:8d:7c:
        a7:bb:47:7c:2a:85:67:0d:81:12:0b:02:98:bc:06:1f:c1:3c:
        9b:c2:1b:4c:44:38:5a:14:b2:48:63:02:2b
# 配置客户端向服务器发送证书所在的PKI域。
[SwitchA] pki domain client256
# 关闭CRL检查。
[SwitchA-pki-domain-client256] undo crl check enable
[SwitchA-pki-domain-client256] quit
# 导入CA证书。
[SwitchA] pki import domain client256 p12 local filename ssh-client-ecdsa256.p12
The system is going to save the key pair. You must specify a key pair name, which is a case-insensiti
ve string of 1 to 64 characters. Valid characters include a to z, A to Z, 0 to 9, and hyphens (-).
Please enter the key pair name[default name: client256]:
# 显示导入CA证书信息。
[SwitchA] display pki certificate domain client256 local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=CN, ST=Beijing, L=Beijing, O=H3C, OU=Software, CN=SuiteB CA
        Validity
            Not Before: Aug 21 08:41:09 2015 GMT
            Not After : Aug 20 08:41:09 2016 GMT
        Subject: C=CN, ST=Beijing, O=H3C, OU=Software, CN=SSH Client secp256
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:da:e2:26:45:87:7a:63:20:e7:ca:7f:82:19:f5:
                    96:88:3e:25:46:f8:2f:9a:4c:70:61:35:db:e4:39:
                    b8:38:c4:60:4a:65:28:49:14:32:3c:cc:6d:cd:34:
                    29:83:84:74:a7:2d:0e:75:1c:c2:52:58:1e:22:16:
                    12:d0:b4:8a:92
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                1A:61:60:4D:76:40:B8:BA:5D:A1:3C:60:BC:57:98:35:20:79:80:FC
            X509v3 Authority Key Identifier:
                keyid:5A:BE:85:49:16:E5:EB:33:80:25:EB:D8:91:50:B4:E6:3E:4F:B8:22
    Signature Algorithm: ecdsa-with-SHA256
        30:66:02:31:00:9a:6d:fd:7d:ab:ae:54:9a:81:71:e6:bb:ad:
        5a:2e:dc:1d:b3:8a:bf:ce:ee:71:4e:8f:d9:93:7f:a3:48:a1:
        5c:17:cb:22:fa:8f:b3:e5:76:89:06:9f:96:47:dc:34:87:02:
        31:00:e3:af:2a:8f:d6:8d:1f:3a:2b:ae:2f:97:b3:52:63:b6:
        18:67:70:2c:93:2a:41:c0:e7:fa:93:20:09:4d:f4:bf:d0:11:
        66:0f:48:56:01:1e:c3:be:37:4e:49:19:cf:c6
# 配置VLAN接口2的IP地址。
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit
(2)配置Stelnet Suite B服务器
# 服务器上配置证书的PKI域与客户端相同，具体过程略。
# 配置服务器suite-b算法集。
```

<SwitchB> system-view
[SwitchB] ssh2 algorithm key-exchange ecdh-sha2-nistp256
[SwitchB] ssh2 algorithm cipher aes128-gcm
[SwitchB] ssh2 algorithm public-key x509v3-ecdsa-sha2-nistp256 x509v3-ecdsa-sha2-nistp384
配置服务器证书所在的PKI域。
[SwitchB] ssh server pki-domain server256
开启Stelnet服务器功能。
[SwitchB] ssh server enable
配置VLAN接口2的IP地址，客户端将通过该地址连接Stelnet服务器。
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[SwitchB-Vlan-interface2] quit
设置Stelnet客户端登录用户线的认证方式为AAA认证。
[SwitchB] line vty 0 15
[SwitchB-line-vty0-15] authentication-mode scheme
[SwitchB-line-vty0-15] quit
创建设备管理类本地用户client001，服务类型为SSH，用户角色为network-admin。
[SwitchB] local-user client001 class manage
[SwitchB-luser-manage-client001] service-type ssh
[SwitchB-luser-manage-client001] authorization-attribute user-role network-admin
[SwitchB-luser-manage-client001] quit
设置SSH用户client001的认证方式为publickey，并指定认证证书所在PKI域为client256。
[Switch] ssh user client001 service-type stelnet authentication-type publickey assign pki-domain client256
(3)Stelnet Suite B客户端建立与Stelnet suite-b服务器的连接
建立到服务器192.168.1.40的SSH连接。
<SwitchA> ssh2 192.168.1.40 suite-b 128-bit pki-domain client256 server-pki-domain server256
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
Enter a character ~ and a dot to abort.

<SwitchB>

配置关键点

1、在服务器的配置过程中需要指定服务器和客户端的证书信息，因此需要首先完成证书的配置，再进行Suite B相关的服务器配置。
2、客户端软件支持Suite B的较少，OpenSSH的pkix版本通过修改可以实现。本文中仅以我司设备客户端为例，说明Stelnet Suite B客户端的配置方法。