联想网御防火墙和SecPath 100F实现IPsec互通

陶鹏 2006-05-09 发表

联想网御防火墙和SecPath 100F实现IPsec互通

某项目测试中，遇到联想网御300防火墙和我司SECPATH 100F，进行IPSEC对接测试，测试中碰到一点问题，拿出来和大家分享。

组网：

组网说明：

PC机A的地址是192.168.1.100 网关地址192.168.1.254。PC机B的地址192.168.0.100，网关地址192.168.0.254。

SECPATH100F防火墙模拟中心节点设备，联想网御防火墙模拟分支节点设备。使用IPSEC野蛮模式进行互连。

故障现象：

两端配置一样， IKE SA始终无法建立。

我司SECPATH配置情况：

IKE PROPOSA是3DES加密，MD5认证，使用野蛮模式：

```
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group5
 authentication-algorithm md5
 sa duration 28800
ike peer lx
 exchange-mode aggressive
 pre-shared-key 12345678
 id-type name
 remote-name lx
```

IPSEC PROPOSA都是 3DES加密，MD5认证：

```
ipsec proposal 1
 esp encryption-algorithm 3des
```

查看IKE SA：

```
[huawei-ike-proposal-1]dis ike sa
   connection-id  peer           flag       phase   doi
  --------------------------------------------------------------
       7        <unnamed>       NONE         1     IPSEC
```

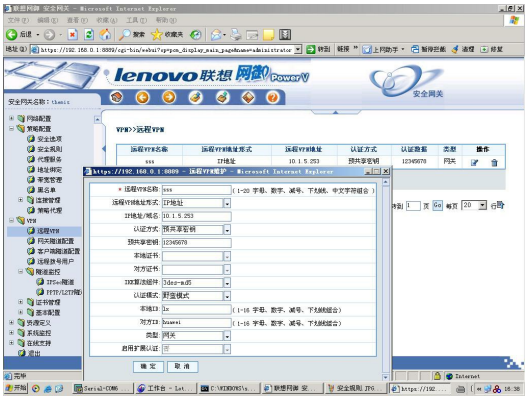
IKE SA没有建立

提示错误信息

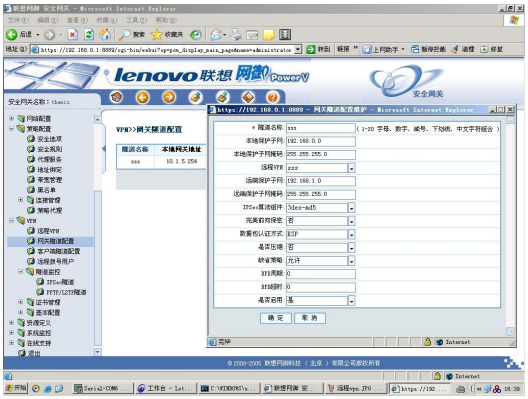
```
#Nov 12 10:15:22:992 2006 huawei IKEMONIT/5/No SA Failure:
 No SA Failure

%Nov 12 10:15:22:992 2006 huawei IKE/4/DROP:
IKE packet dropped: (src addr: 10.1.5.253, dst addr: 10.1.5.254) with I_COOKIE f5c9ae3bef83aa8a a
nd R_COOKIE 0000000000000000, because of ' No proposal is chosen ' from payload PROPOSAL.
```

联想WEB配置

联想“远程VPN”，对应我司的IKE PROPOSA：



联想“网关隧道配置”，对应我司IPSEC PROPOSA：



原理和解决方法：

打开debugging ike message查看IKE协商信息，发现如下提示：

*0.16938973 huawei IKE/8/DEBUG: Transform 0's attributes

*0.16938973 huawei IKE/8/DEBUG: Attribute LIFE_TYPE : SECONDS

*0.16938973 huawei IKE/8/DEBUG: Attribute LIFE_DURATION : 28800

*0.16938973 huawei IKE/8/DEBUG: Attribute ENCRYPTION_ALGORITHM : 3DES_CBC

*0.16938973 huawei IKE/8/DEBUG: Attribute HASH_ALGORITHM : SHA

*0.16938973 huawei IKE/8/DEBUG: Attribute AUTHENTICATION_METHOD : PRE_SHARED

*0.16938974 huawei IKE/8/DEBUG: Attribute GROUP_DESCRIPTION : MODP_1024

*0.16938974 huawei IKE/8/DEBUG:validate payload KEY_EXCH of message 844c6d64

*0.16938974 huawei IKE/8/DEBUG:validate payload ID of message 844c6d64

由上面信息可以看到联想实际发送过来的IKE PROPOSA验证算法是SHA，由此可以肯定联想设备的WEB设置和后台实际运行配置不一致，造成了和SECPATH 的IKE SA无法建立。

修改SECPATH 100F IKE PROPOSA 1 的验证算法为SHA。

联想默认发送过来的DH组是dh group2即10248-bit的Diffie-Hellman组，而SECPATH 100F上面配置的是dh group5（默认是dh group1），修改SECPATH 100F为dh group2。

查看IKE SA

```
[huawei]dis ike sa
  connection-id  peer           flag       phase   doi
 --------------------------------------------------------------
    198          10.1.5.254      RD           1     IPSEC
 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT
```

可以看到IKE SA 已经建立。

备注：

查看IKE SA VERBOSE信息如下：

```
[huawei]dis ike sa verbose
  ----------------------------------------------
  connection id: 198
  transmitting entity: responder
  ----------------------------------------------
  local ip: 10.1.5.253
  local id type: FQDN
  local id: huawei

  remote ip: 10.1.5.254
```

```
    remote id type: FQDN
    remote id: lx

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: 3DES-CBC

    life duration(sec): 28800
    remaining key duration(sec): 28193
    exchange-mode: AGGRESSIVE
    diffie-hellman group: GROUP2
nat traversal: NO
```

查看IPSEC 信息，已经全部建立起来：

```
[huawei]dis ipsec sa
================================
Interface: Ethernet1/1
    path MTU: 1500
================================
   -----------------------------
    IPsec policy name: "1"
    sequence number: 1
    mode: isakmp
    -----------------------------
    Created by: "Host"
    connection id: 4
    encapsulation mode: tunnel
    perfect forward secrecy: None
    tunnel:
        local  address: 10.1.5.253
        remote address: 10.1.5.254
    flow:    (5 times matched)
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP
        dest addr: 192.168.0.0/255.255.255.0  port: 0  protocol: IP
    [inbound ESP SAs]
      spi: 3613558760 (0xd76287e8)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887436580/3574
      max received sequence-number: 5
      udp encapsulation used for nat traversal: N
    [outbound ESP SAs]
      spi: 903478232 (0x35d9fbd8)
      proposal: ESP-ENCRYPT-3DES ESP-AUTH-MD5
      sa remaining key duration (bytes/sec): 1887436800/3574
      max sent sequence-number: 1
      udp encapsulation used for nat traversal: N

[huawei]dis ipsec tunnel
    -------------------------------------------------
    Connection ID : 4
    Perfect forward secrecy: None
    SA's SPI :
        Inbound :  3613558760 (0xd76287e8) [ESP]
        Outbound : 903478232 (0x35d9fbd8) [ESP]
    Tunnel :
        Local Address:  10.1.5.253  Remote Address : 10.1.5.254
    Flow :     (8 times matched)
        Sour Addr : 192.168.1.0/255.255.255.0  Port: 0  Protocol : IP
        Dest Addr : 192.168.0.0/255.255.255.0  Port: 0  Protocol : IP
```