SecPath防火墙IPSecVPN野蛮模式验证方法为预共享密钥典型配置

刘军 2006-09-08 发表

SecPath防火墙IPSec 野蛮模式验证为预共享密钥
典型配置指南

一、 组网需求

防火墙建立IPSEC VPN有两种验证方法，一种是预共享密钥，一种是证书认证，下面讲述IKE为野蛮模式，验证方法为预共享密钥的配置。

二、 组网图

如图所示，SecPath1000F要与SecPath500F-B建立基于野蛮模式验证方法为预共享密钥的VPN，中间的SecPath500F只起数据转发的作用。

软件版本如下：

SecPath1000F： VRP 3.40 ESS 1604;

SecPath500F： VRP 3.40 ESS 1604;

SecPath500F-B： VRP 3.40 ESS 1604。

三、 典型配置

1、SecPath500-B的配置

```
<500F-B>dis cu
#
 sysname 500F-B
#
 ike local-name 500f
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
pki entity 2000
  common-name 2000
  organization-unit tc
  organization huawei-3com
  locality beijing
  country CN
#
pki domain 1
  ca identifier ts-sec
  certificate request url http://5.5.5.1
  certificate request from ra
  certificate request entity 2000
  crl check disable
#
radius scheme system
#
domain system
#

#
ike peer 1000f                  //定义IKE PEER
 exchange-mode aggressive       //IKE交换模式为野蛮模式
```

```
 pre-shared-key 123456              //预共享密钥 为 123456
 id-type name                      //ID的类型为名字
 remote-name 1000f                 //对端名字为1000f
 nat traversal                     //支持NAT穿越

#
ike peer 100f
#
ipsec proposal p1                  //定义安全提议，安全提议采用默认设置，加
//密算法 为DES，验证算法为MD5
#
ipsec policy test 1 isakmp         //定义安全策略
 security acl 3000                 //定义触发IPsec的数据流
 ike-peer 1000f                    //定义使用的IKE PEER
 proposal p1                       //定义使用的安全提议
#
acl number 3000
 rule 0 permit ip source 2.2.2.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 loopback
 ip address 2.2.2.1 255.255.255.0
#
interface GigabitEthernet0/1
#
interface GigabitEthernet1/0
 ip address 1.1.1.1 255.255.255.0
 ipsec policy test
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
```

```
 ip route-static 3.3.3.0 255.255.255.0 1.1.1.2 preference 60
 ip route-static 4.4.4.0 255.255.255.0 1.1.1.2 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
<500f>
```

2、 SecPath1000F的配置

```
 <1000f>dis cu
#
 sysname 1000f
#
 ike local-name 1000f
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
 qos carl 1 dscp 16
 qos carl 2 dscp 16
 qos carl 3 mac 0000-1111-2222
 qos carl 4 precedence 0
 qos carl 5 precedence 2
#
 firewall blacklist enable
 firewall blacklist 10.1.1.123
#
pki entity 3000
  common-name 3000
  organization-unit tc
  organization huawei-3com
  locality beijing
  country cn
#
pki domain 1
  ca identifier ts-sec
  certificate request url http://5.5.5.5
  certificate request from ra
  certificate request entity 3000
  crl check disable
#
radius scheme system
#
domain system
#
local-user aaa
 password simple aaaaaa
 service-type telnet
 level 3
local-user ftp
 password simple ftp
 service-type ftp
#

#
ike peer 500f                          //定义IKE PEER
 exchange-mode aggressive              //IKE交换模式为野蛮模式
pre-share-key 123456                   //预共享密钥为123456
```

```
 id-type name                        //ID的类型为名字
 remote-name 500f                    //对端名字为500f
 remote-address 1.1.1.1              //对端地址
 nat traversal                      //支持NAT穿越

#
ike peer test
#
ipsec proposal p1                   //定义安全提议，安全提议采用默认设置，加
//密算法 为DES，验证算法为MD5


ipsec policy test 1 isakmp          //定义安全策略
 security acl 3000                  //定义触发IPsec的数据流                              ike-peer 500f
          //定义使用的IKEE PEER
 proposal p1                        //定义使用的安全提议
#
acl number 3000
 rule 0 permit ip source 3.3.3.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 3.3.3.1 255.255.255.0
 qos gts acl 3000 cir 150000 cbs 75000 ebs 0 queue-length 50
#
interface GigabitEthernet0/1
 ip address 4.4.4.2 255.255.255.0
 ipsec policy test
#
interface GigabitEthernet1/0
 shutdown
 ip address 55.1.1.1 255.255.255.0
 qos gts any cir 50000000 cbs 75000000 ebs 0 queue-length 50
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 add interface GigabitEthernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
```

```
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
 FTP server enable
#
 ip route-static 1.1.1.0 255.255.255.0 4.4.4.1 preference 60
 ip route-static 2.2.2.0 255.255.255.0 4.4.4.1 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0
 undo shell
user-interface vty 1 4
#
return
<1000f>
<1000f>
```

3、SecPath500F的配置

```
<mid-500>dis cu
#
 sysname mid-500
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 firewall statistic system enable
#
radius scheme system
#
domain system
#
acl number 2000
 rule 0 permit source 4.4.4.0 0.0.0.255
#
interface Aux0
 async mode flow
#
interface GigabitEthernet0/0
 ip address 1.1.1.2 255.255.255.0
#
interface GigabitEthernet0/1
#
interface GigabitEthernet1/0
 ip address 4.4.4.1 255.255.255.0
#
interface GigabitEthernet1/1
#
interface Encrypt2/0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet1/0
 set priority 85
#
firewall zone untrust
 set priority 5
```

```
#
firewall zone DMZ
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
#
return
```

四、配置关键点和关键命令

```
exchange-mode aggressive            //IKE交换模式为野蛮模式
pre-share-key 123456                //预共享密钥为123456
id-type name                        //定义ID的类型
```