# SecPath防火墙综合组网中BIMS的应用案例

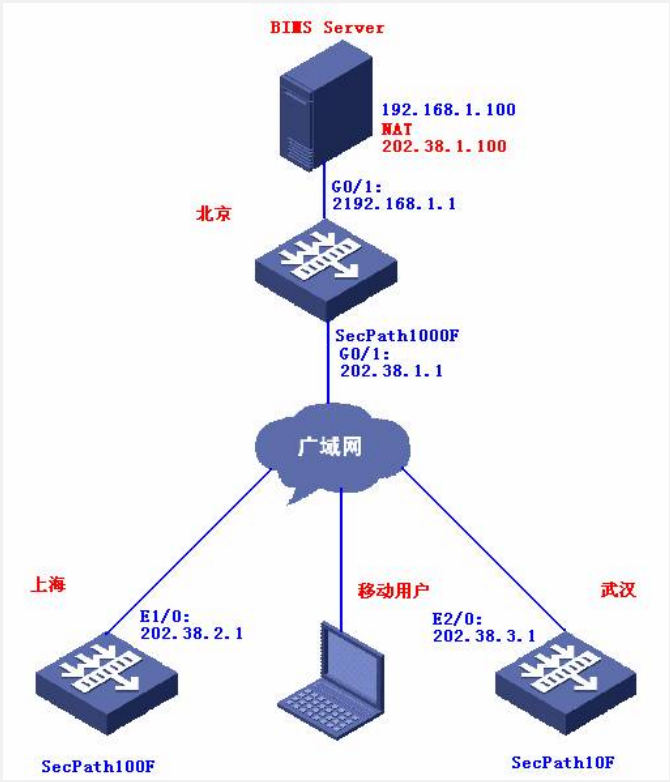
赵彪 2006-11-14 发表

**SecPath防火墙综合组网中BIMS的应用案例**

**一、 组网需求：**

在一个互联的VPN网络里，通过BIMS网管软件对全网设备进行管理。

**二、 组网图**




SecPath1000F：Version 3.40, ESS 1605；

SecPath100F：Version 3.40, R1210；

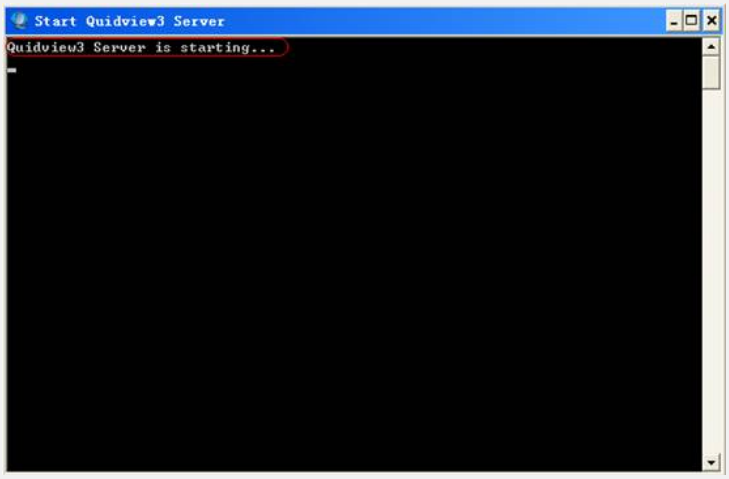
SecPath10F：Version 3.40, ESS 1605；

BIMS Server：Windows XP，安装有BIMS网管软件。

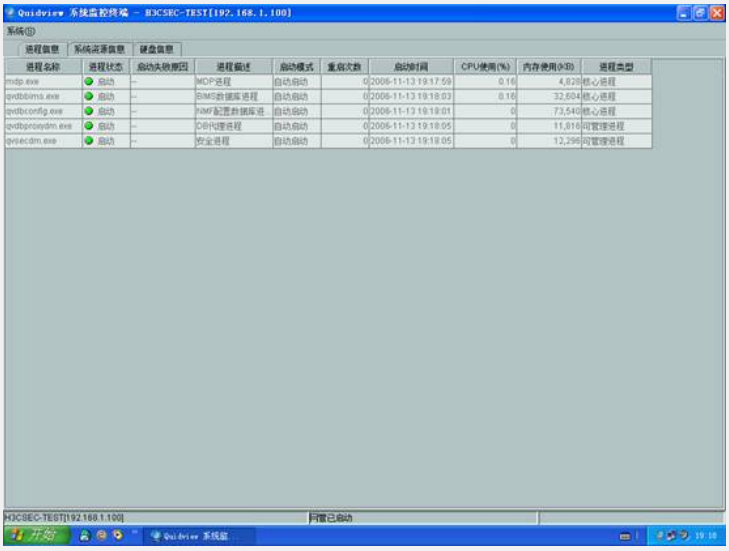
**三、 配置信息**

**1、BIMS Server的主要配置**

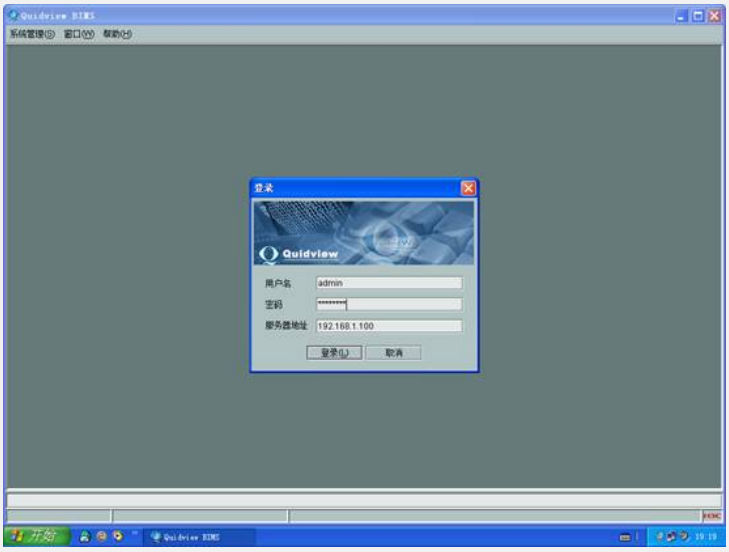
安装完BIMS后，启动BIMS后台服务：



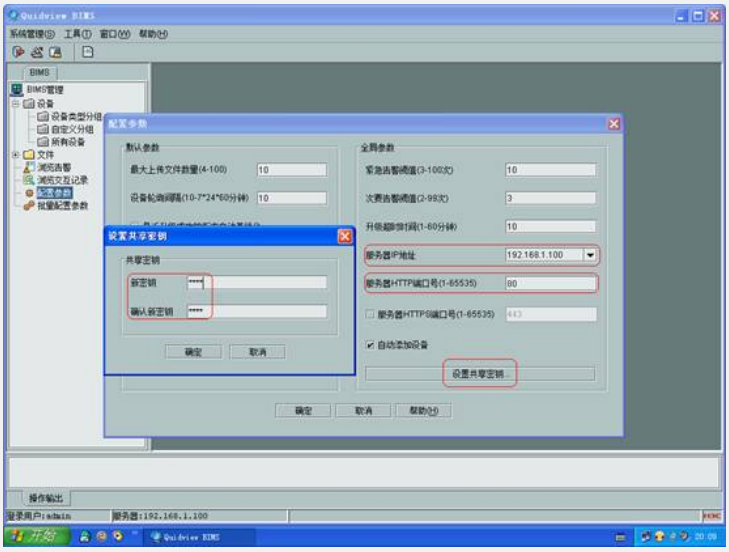

后台启动成功，显示下面的界面：



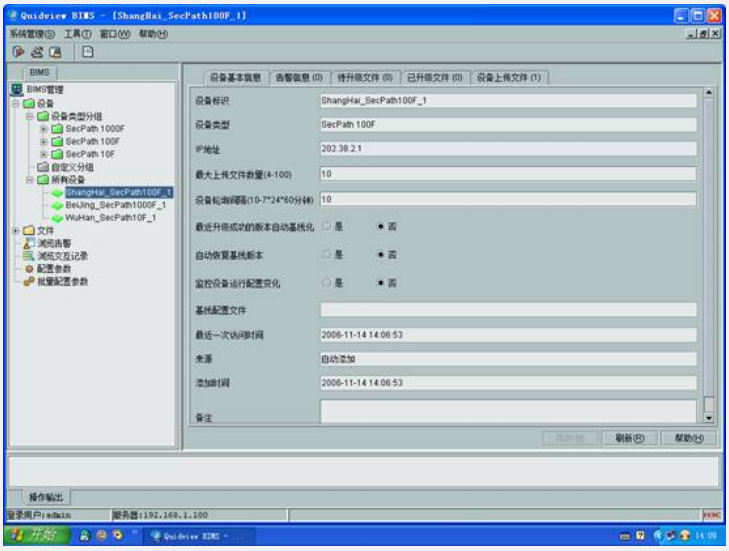
启动BIMS客户端：



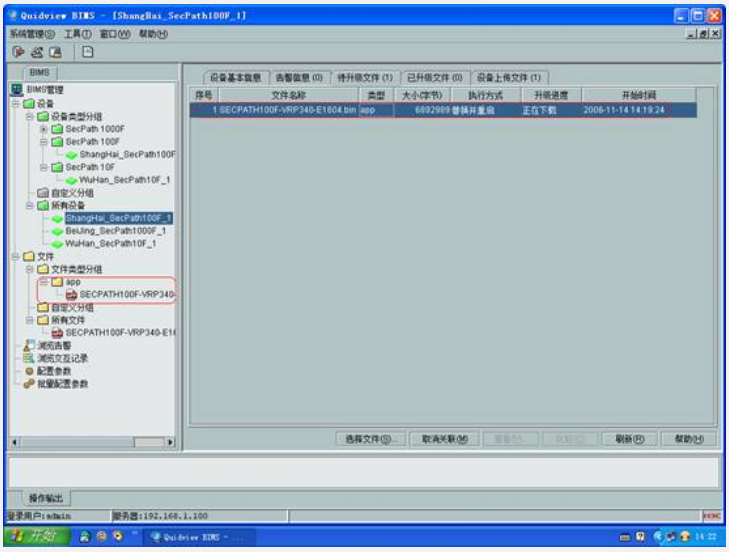
配置BIMS网管：



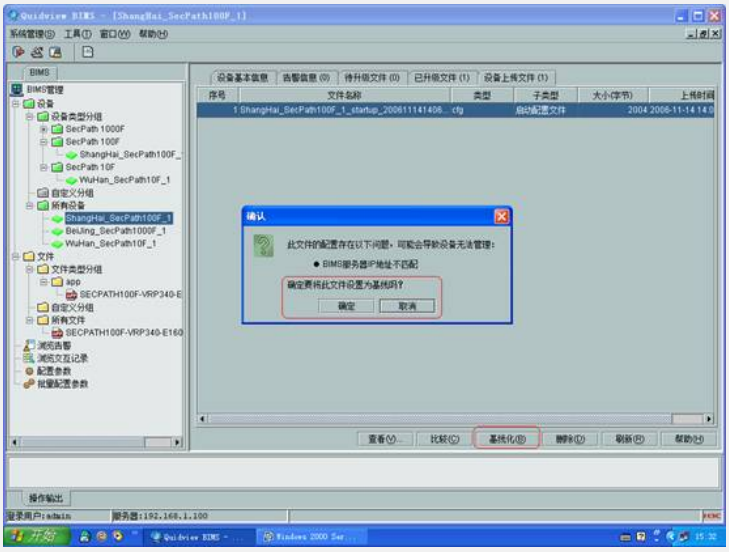
设备成功添加到BIMS网管上：



通过BIMS对SecPath100F进行升级:



在BIMS上设置基线:



**2、SecPath1000F的主要配置**

#

sysname BeiJing

#

l2tp enable　　//启用L2TP

#

ike local-name Beijing　　//配置IKE本地名称

#

firewall packet-filter enable

```
 firewall packet-filter default permit
#
 bims enable                                    //启用BIMS
 bims device-id BeiJing_SecPath1000F_1          //配置BIMS设备标识符
 bims ip address 192.168.1.100 port 80          //配置BIMS服务器的IP地址
 bims interval 10                               //配置BIMS请求间隔时间
 bims sharekey cipher =W6JJ`N_LBKQ=^Q`MAF4<1!!  //配置BIMS共享密钥
#
domain system                                   //配置L2TP地址池
 ip pool 1 10.0.0.2 10.0.0.100
#
local-user admin                                //配置管理员帐号
 password cipher .]@USE=B,53Q=^Q`MAF4<1!!
 service-type telnet
 level 3
local-user zhaobiao                             //配置L2TP账号
 password cipher 7-CZB#/YX]KQ=^Q`MAF4<1!!
 service-type ppp
#
ike dpd 1                                       //配置DPD
#
ike peer lac                                    //配置IKE PEER
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name lac
 nat traversal
#
ike peer shanghai                               //配置IKE PEER
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name shanghai
 nat traversal
 dpd 1
#
ike peer wuhan                                  //配置IKE PEER
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name wuhan
 nat traversal
 dpd 1
#
ipsec proposal lac                              //配置IPSEC安全提议
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec proposal shanghai                         //配置IPSEC安全提议
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec proposal wuhan                            //配置IPSEC安全提议
 esp authentication-algorithm sha1
 estion-algorithm 3des
#
ipsec policy-template lac 1                     //创建IPSEC模板
 ike-peer lac
 proposal lac
#
ipsec policy-template shanghai 1                //创建IPSEC模板

 ike-peer shanghai
 proposal shanghai
```

```
#
ipsec policy-template wuhan 1              //创建IPSEC模板

 ike-peer wuhan
 proposal wuhan
#
ipsec policy pol1 1 isakmp template wuhan      //利用模板创建IPEC策略
#
ipsec policy pol1 2 isakmp template shanghai  //利用模板创建IPEC策略
#
ipsec policy pol1 3 isakmp template lac       //利用模板创建IPEC策略
#
acl number 3000                               //定义NAT转换的ACL
 rule 0 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 1 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
 rule 2 permit ip source 192.168.1.0 0.0.0.255
 rule 3 deny ip
#
interface Virtual-Template1                   //创建虚模板
 ppp authentication-mode chap
 ip address 10.0.0.1 255.255.255.0
 remote address pool 1
#
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/1
 ip address 202.38.1.1 255.255.255.0
 nat outbound 3000
 nat server protocol tcp global 202.38.1.100 www inside 192.168.1.100 www
 nat server protocol icmp global 202.38.1.100 inside 192.168.1.100
 ipsec policy pol1                            //启用IPSEC Policy
#
firewall zone trust
 add interface GigabitEthernet0/0
 set priority 85
#
firewall zone untrust
 add interface GigabitEthernet0/1
 add interface Virtual-Template1
 set priority 5
#
l2tp-group 1                                  //配置L2TP组
 allow l2tp virtual-template 1
 tunnel password cipher =W6JJ`N_LBKQ=^Q`MAF4<1!!
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.1.2      //配置默认路由
#
user-interface vty 0 4
 authentication-mode scheme
 protocol inbound telnet
#
```

**3、SecPath100F的主要配置**

```
#
 sysname ShangHai
#
 ike local-name shanghai                      //配置IKE本地名称
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 insulate
#
 bims enable                                  //启用BIMS
```

```
 bims device-id ShangHai_SecPath100F_1          //配置BIMS设备标识符
 bims ip address 202.38.1.100 port 80          //配置BIMS服务器的IP地址
 bims interval 10                              //配置BIMS请求间隔时间
 bims boot request                             //配置系统启动发送BIMS请求
 bims sharekey cipher =W6JJ`N_LBKQ=^Q`MAF4<1!!  //配置BIMS共享密钥
#
ike dpd 1                                      //配置DPD
#
ike peer beijing                               //配置IKE PEER
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name beijing
 remote-address 202.38.1.1
 nat traversal
 dpd 1
#
ipsec proposal beijing                         //配置IPSEC安全提议
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy pol1 1 isakmp                     //配置IPSEC Policy
 security acl 3001
 ike-peer beijing
 proposal beijing
#
acl number 3000                                //定义NAT转换的ACL
 rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 1 permit ip source 192.168.2.0 0.0.0.255
 rule 2 deny ip
acl number 3001                                //配置保护数据流
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 1 deny ip
#
interface Ethernet0/0
 ip address 192.168.2.1 255.255.255.0
interface Ethernet1/0
 tcp mss 1024
 ip address 202.38.2.1 255.255.255.0
 nat outbound 3000
 ipsec policy pol1                             //启用IPSEC Policy
#
firewall zone trust
 add interface Ethernet0/0
 set priority 85
#
firewall zone untrust
 add interface Ethernet1/0
 set priority 5
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.2.2     //配置默认路由
#
```

**4、SecPath10F的主要配置**

```
#
 sysname WuHan
#
 ike local-name wuhan                          //配置IKE本地名称
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 bims enable                                   //启用BIMS
 bims device-id WuHan_SecPath10F_1             //配置BIMS设备标识符
 bims ip address 202.38.1.100 port 80          //配置BIMS服务器的IP地址
```

```
 bims interval 10                          //配置BIMS请求间隔时间
 bims sharekey cipher =W6JJ`N_LBKQ=^Q`MAF4<1!! //配置BIMS共享密钥
#
ike dpd 1                                  //配置DPD
#
ike peer beijing                           //配置IKE PEER
 exchange-mode aggressive
 pre-shared-key 123456
 id-type name
 remote-name beijing
 remote-address 202.38.1.1
 nat traversal
 dpd 1
#
ipsec proposal beijing                     //配置IPSEC安全提议
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy pol1 1 isakmp                 //创建IPSEC Policy
 security acl 3001
 ike-peer beijing
 proposal beijing
#
acl number 3000                            //定义NAT转换的ACL
 rule 0 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 1 permit ip source 192.168.3.0 0.0.0.255
 rule 2 deny ip
acl number 3001                            //配置保护数据流
 rule 0 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
 rule 1 deny ip
#
interface Ethernet1/0
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet2/0
 speed 10
 duplex half
 tcp mss 1024
 ip address 202.38.3.1 255.255.255.0
 nat outbound 3000
ipsec policy pol1                          //启用IPSEC Policy
#
firewall zone trust
 add interface Ethernet1/0
 set priority 85
#
firewall zone untrust
 add interface Ethernet2/0
 set priority 5
#
 ip route-static 0.0.0.0 0.0.0.0 202.38.3.2      //配置默认路由
#
```

**四、 配置关键点**

1. BIMS使用HTTP协议，必须保证80端口没有被占用；
2. BIMS客户端默认帐户和口令为：admin/quidview；
3. BIMS服务端和客户端可以分开安装;
4. SecPath防火墙Version 3.40 - ESS 1605以后的版本默认启用“bims boot request ”。