iMC BIMS配合IVM组件建立IPsec VPN的配置方法

Bims 刘思 2013-04-25 发表

iMC BIMS配合IVM组件建立IPsec VPN的配置方法

一、组网需求：

某客户处组网为HUB-SPOKE方式，分部IP地址为运营商自动分配且出口做了NAT地址转换。为了实现对所有在网设备进行集中配置管理和数据的安全传输需求，可通过iMC 平台、BIMS、IVM组件来进行设备管理以及相关VPN配置的下发。

二、组网图：

三、配置步骤：

基础组网部分相关配置：

第一步：配置设备IP地址，并确保路由的可达。

CPE的IP地址配置如下：

GE0/1 192.168.10.1

Loop0 10.1.0.1

其中GE0/1的地址为自动获取，Loop0用来模拟分支机构的上网设备。

运营商的IP地址配置如下：

GE0/0 192.168.10.2

GE0/1 192.168.9.2

HUB的IP地址配置如下：

GE0/0 172.16.0.201

GE0/1 192.168.9.3

Loop0 10.2.0.1

Loop0用来模拟总部机构的上网设备，GE0/0用来与iMC（172.16.100.122）实现IP三层互连。

第二步：CPE GE0/1上启用NAT，模拟现实组网环境。

#

acl number 3001

rule 0 deny ip source 10.1.0.1 0 destination 10.2.0.1 0

rule 5 permit ip source 10.1.0.1 0

interface GigabitEthernet0/1

port link-mode route

nat outbound 3001

ip address dhcp-alloc

#

BIMS部分相关配置：

第一步：iMC上BIMS相关参数的配置。

1、 依次点击【业务】--【分支网点管理】--【系统配置】--【系统参数】。其中打开“Web网管配置”为iMC打开CPE Web网管的方式和对应的端口。支持HTTP方式和HTTPS方式。“默认轮询时间”表示网管系统轮询设备状态和配置的默认时间间隔。“周期通知间隔”表示每隔该时间间隔，设备通过Inform方法周期向ACS发送CPE设备信息，该值也可在设备上通过命令行来配置。“CPE访问参数”表示网管系统访问设备时携带的用户名以及密码信息。通过“CPE增加策略”可配置网管系统是否可自动增加CPE设备。

2、 依次点击【业务】--【分支网点管理】--【系统配置】--【CPE认证用户】。该处可创建、修改以及删除CPE认证用户，需要注意的是只有管理员才能增加、修改CPE用户信息，查看员和维护员只能修改用户密码且CPE用户一旦注册就不可修改用户名。

第二步：CPE侧CWMP（TR-069）协议的配置，主要支持命令行配置、DHCP Option43属性下发以及短信配置下发等方式。本文以命令行配置以及DHCP Option43属性为例说明。

1、 命令行配置方式，如下配置为实验室配置，具体参数请根据现场环境而定。

[CPE]cwmp

[CPE-cwmp]cwmp enable

[CPE-cwmp]cwmp cpe username cpe

[CPE-cwmp]cwmp cpe password cpe

[CPE-cwmp]cwmp acs username acs

[CPE-cwmp]cwmp acs password acs

[CPE-cwmp]cwmp acs url http://172.16.100.122:9090

[CPE-cwmp]cwmp cpe inform interval 20

[CPE-cwmp]cwmp cpe connect interface GigabitEthernet 0/1

[CPE-cwmp]cwmp cpe connect retry 10

[CPE-cwmp]cwmp cpe wait timeout 60

2、 通过DHCP Option43方式。DHCP Option43可携带厂商私有扩展属性，当设备IP地址为自动获取时，利用该属性可将BIMS（ACS）URL以及用户名密码信息。

iMC BIMS组件自带Option工具，可将URL转换为Option43。依次点击【业务】--【分支网点管理】--【系统配置】--【Option工具】，得如下截图。

将转换后的Option 43结果导入到DHCP服务器配置中后，CPE在自动获取IP地址时可自动获取ACS的URL、用户和密码信息。DHCP服务器的位置请结合用户实际组网情况而定。

#

dhcp server ip-pool 1

network 192.168.10.0 mask 255.255.255.0

gateway-list 192.168.10.2

option 43 hex 01226874 74703A2F 2F313732 2E31362E 3130302E 3132323A 3930 3930 20616373 20616373

#

第三步：iMC BIMS资源管理中查看CPE设备。

依次点击【业务】--【分支网点管理】--【资源管理】--【所有CPE】，即可查看CPE设备已自动添加成功。

IVM部分相关配置：

第一步：创建IPsec和IKE的安全模板。

1、 依次点击【业务】--【IPsec VPN管理】--【模板管理】--【IPsec安全提议】，该处可增加和修改相关IPsec安全提议，本文中将对模板test进行调用。

2、 依次点击【业务】--【IPsec VPN管理】--【模板管理】--【IKE安全提议】，该处可增加和修改相关IKE安全提议，本文中将对模板test进行调用。

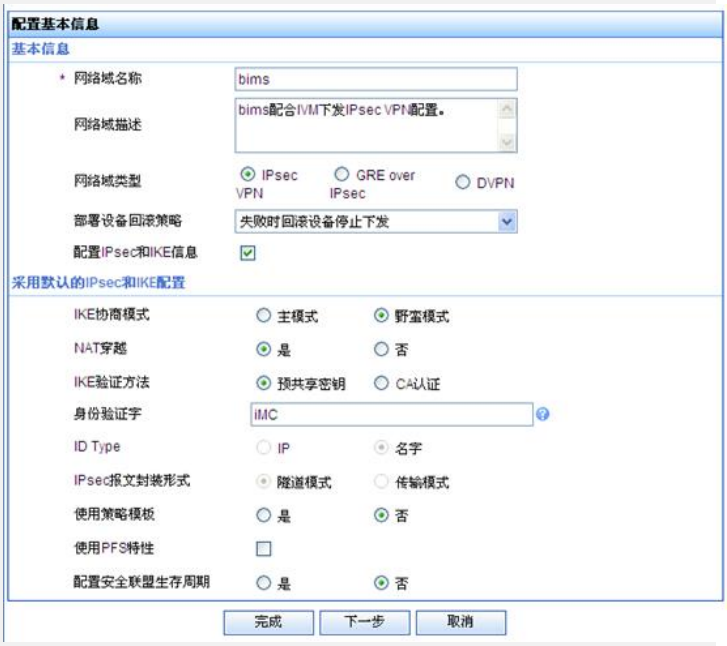
第二步：增加IPsec设备。

1、 依次点击【业务】--【IPsec VPN管理】--【IVM参数配置】，该处可填写访问BIMS服务的参数，BIMS服务器地址须与之前BIMS设置中“打开web网管配置”先匹配。

2、 增加HUB设备，依次点击【业务】--【IPsec VPN管理】--【IPsec资源管理】--【设备管理】--【导入设备】，选择设备可导入HUB，选择BIMS设备可导入CPE。需要注意的是在点击【选择设备】时相关设备须配置telnet或者ssh参数。

第三步：创建网络管理域。

依次点击【业务】--【IPsec VPN管理】--【IPsec资源管理】--【设备管理】--【网络域管理】--【增加】。“使用策略模板”选是，则HUB侧通过策略模板来建立VPN，选否则通过ACL方式来建立VPN。



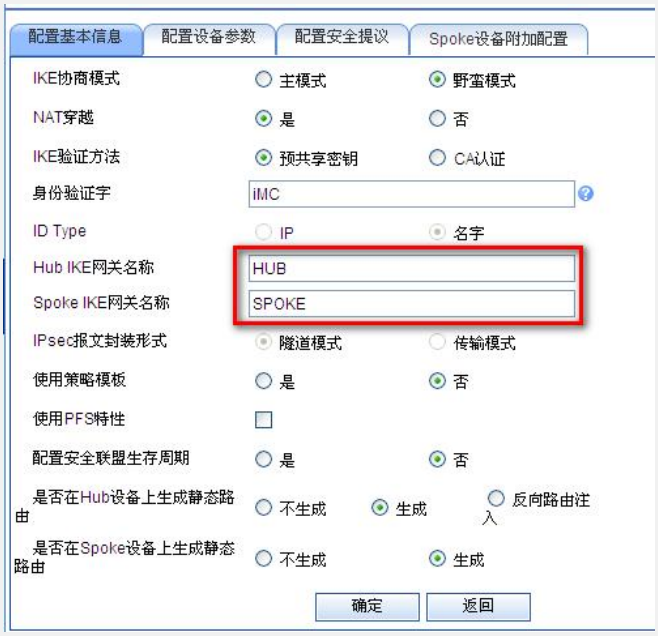
点击下一步，该处可配置IPsec和IKE的安全提议，二者皆调用之前配置的test模板。IKE安全提议必须为数字。

第四步：创建IPsec VPN并对其进行配置。

1、 依次点击网络域【bims】--【增加】--【选择HUB设备】，系统会自动将符合条件的HUB设备筛选。之后点击【选择BIMS Spoke设备】，可将Spoke设备添加。

2、 更改HUB设备和Spoke设备启用IPsec Policy的接口。

3、 对IPsec 隧道进行配置，点击上图中的 功能按钮，进去基本信息配置页面。该处可配置HUB设SPOKE设备IKE网管名称，其他部分保持不变。



4、 点击上图中【配置设备参数】，该处可增加感兴趣的流，用于确定ACL中的相关源和目的网段。增加完成之后点击返回。

5、 点击【SPOKE设备附加配置】，不做任何配置，点击确定之后点击返回。

6、 此时即可对IPsec VPN隧道进行部署，但配置下发到对应设备之后安全提议等名称为iMC自定义，继续点击配置功能按钮进行配置。

点击“HUB设备高级配置”，可做截图中所示配置。

点击“Spoke设备高级配置”，可做截图中所示配置。

配置完成之后点击返回，即可返回隧道列表页面。

第五步：进行隧道的配置下发以及验证。

1、 在隧道列表页面，选定隧道并点击【部署】按钮，即可对隧道进行部署。

2、 由于做了NAT穿越，由SPOKE侧发起ping来建立VPN隧道。

reset ipsec sa

reset ike sa

ping -c 2 -a 10.1.0.1 10.2.0.1

PING 10.2.0.1: 56 data bytes, press CTRL_C to break

Request time out //该ping包用以触发VPN隧道的建立。

Reply from 10.2.0.1: bytes=56 Sequence=2 ttl=255 time=2 ms

--- 10.2.0.1 ping statistics ---

2 packet(s) transmitted

1 packet(s) received

50.00% packet loss

round-trip min/avg/max = 2/2/2 ms

3、 VPN隧道的拆除，在VPN隧道列表中选择隧道，点击拆除即可拆除VPN隧道。

dis ipse sa

dis ike sa

total phase-1 SAs: 0

connection-id peer flag phase doi

----------、

四、配置关键点：

1、请正确配置ACS访问参数，相关参数数值请根据现场环境而定。

2、在IVM视图中配置基本信息和配置设备参数时请仔细了解没个选项的定义，如是否生成策略模板以及静态路由的注入，以免在配置下发之后造成网络的中断。

3、下发配置前，请先从BIMS同步设备配置，然后再次从IVM同步设备配置。