

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。

系统参数	
打开Web网管配置	
协议	HTTP
* 端口号	80
默认轮询时间	
* 默认状态轮询时间(1-500分钟)	1
* 默认配置轮询时间(60-1500分钟)	120
周期通知间隔	
* 周期通知间隔(60-86400秒)	60
CPE访问参数	
连接请求用户名	cpe
连接请求密码	***
CPE增加策略	
自动增加CPE	允许
增加CPE时同步系统名称	启用
通用密码参数	
通用密码状态	启用
* 通用密码	****
ACS运行日志	
ACS日志级别	信息
输出ACS报文	禁用
输出CPE报文	禁用

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。

CPE认证用户列表			
增加		刷新	
共有2条记录，当前第1-2，第 1/1 页。		每页显示：8 15 [50] 100 200	
用户名	描述	修改	删除
bims	默认的CPE认证用户。		
acs			

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。

业务 >> 分支网点管理 >> Option工具

Option工具

转换类型: URL转换为Option 43

DHCP服务器类型: H3C设备

* ACS URL: http://172.16.100.122:9090 acs acs

DHCP Option 43: option 43 hex 01226874 74703A2F 2F313732 2E31362E 3130302E 3132323A 39303930 20616373 20616373

转换

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。

CPE列表

删除 同步 IP Ping测试 远程重启 恢复出厂设置 同步系统名称

共有1条记录，当前第1-1，第 1/1 页。 每页显示：8 15 [50] 100 200

状态	CPE名称	NAT CPE	序列号	类型	厂商	IP地址	上次同步时间	同步结果	操作
<input type="checkbox"/>	重要 CPE	否	210235a19gb096000174	MSR30-20	H3C	192.168.10.1	2013-04-13 15:02:26	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。

IPsec安全提议列表

增加 删除

共有3条记录，当前第1-3，第 1/1 页。 每页显示：8 15 [50] 100 200

提议名称	报文封装形式	安全协议	AH验证算法	ESP验证算法	ESP加密算法	修改
<input type="checkbox"/> Default1	隧道模式	ESP	无验证算法	MD5	无加密算法	
<input type="checkbox"/> Default2	传输模式	ESP	无验证算法	MD5	无加密算法	
<input type="checkbox"/> test	隧道模式	ESP	无验证算法	MD5	DES	

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。

IKE安全提议列表

增加 删除

共有3条记录，当前第1-3，第 1/1 页。 每页显示：8 15 [50] 100 200

提议名称	验证方法	加密算法	验证算法	Diff-Hellman组标识	ISAKMP SA生存周期	修改
<input type="checkbox"/> Default1	预共享密钥	DES	SHA1	DH组1	86400	
<input type="checkbox"/> Default2	CA认证	DES	SHA1	DH组1	86400	
<input type="checkbox"/> test	预共享密钥	DES	SHA1	DH组1	86400	

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。

业务 >> IPsec VPN管理 >> IVM参数配置

BIMS服务参数配置 | BIMS设备参数 | 监视参数设置

启用BIMS服务

BIMS服务器地址

用户名

密码

确定

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。

设备列表

选择设备 | 选择BIMS设备 | 删除

共有2条记录，当前第1-2，第 1/1 页。 每页显示：8 15 [50] 100 200

设备标签	子网掩码	设备类型	设备型号
<input type="checkbox"/> 172.16.0.201(172.16.0.201)	255.255.255.0	路由器	H3C MSR30-20
<input type="checkbox"/> CPE(192.168.10.1)		BIMS设备	H3C MSR30-20

确定 | 取消

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。

配置基本信息

基本信息

网络域名称

网络域描述

网络域类型 IPsec VPN GRE over IPsec DvPN

部署设备回滚策略

配置IPsec和IKE信息

采用默认的IPsec和IKE配置

IKE协商模式 主模式 野蛮模式

NAT穿越 是 否

IKE验证方法 预共享密钥 CA认证

身份验证字

ID Type IP 名字

IPsec报文封装形式 隧道模式 传输模式

使用策略模板 是 否

使用PFS特性

配置安全联盟生存周期 是 否

完成 | 下一步 | 取消

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。

配置安全提议

IPsec安全提议

增加 | 删除

共有1条记录。

提议名称	报文封装形式	安全协议	AH验证算法	ESP验证算法	ESP加密算法	修改
<input type="checkbox"/> test	隧道模式	ESP	不验证	MD5	DES	

IKE安全提议

增加 | 删除

共有1条记录。

提议序号	IKE验证方法	加密算法	验证算法	DH组标识	ISAKMP SA生命周期	修改
<input type="checkbox"/> 1	预共享密钥	DES	SHA1	DH组1	86400	

上一步 | 完成 | 取消

网络域列表							
增加		删除					
共有1条记录, 当前第1-1, 第 1/1 页。				每页显示: 8 15 [50] 100 200			
<input type="checkbox"/>	网络域名称	网络域类型	网络域描述	隧道数目	接收速率(bits/s)	发送速率(bits/s)	操作
<input type="checkbox"/>	bims	IPsec VPN	bims配合IVM 下发IPsec VPN配置。	0	-	-	

第四步：创建IPsec VPN并对其进行配置。

- 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。

Hub设备信息			
Hub设备:	172.16.0.201(172.16.0.201)		

隧道列表			
<input type="button" value="选择Hub设备"/>	<input type="button" value="选择Spoke设备"/>	<input type="button" value="选择BIMS Spoke设备"/>	<input type="button" value="增加虚拟Spoke设备"/>
<input type="button" value="从文件导入隧道"/>	<input type="button" value="删除"/>		
<input type="checkbox"/>	Hub设备接口	网关地址	Spoke设备名称
<input type="checkbox"/>			

- 更改HUB设备和Spoke设备启用IPsec Policy的接口。

隧道列表					
<input type="button" value="选择Hub设备"/>	<input type="button" value="选择Spoke设备"/>	<input type="button" value="选择BIMS Spoke设备"/>	<input type="button" value="增加虚拟Spoke设备"/>	<input type="button" value="从文件导入隧道"/>	
<input type="button" value="删除"/>					
<input type="checkbox"/>	Hub设备接口	网关地址	Spoke设备名称	Spoke设备接口	网关地址
<input type="checkbox"/>	GigabitEthernet0/1	192.168.9.3	CPE	GigabitEthernet0/1	192.168.10.1

- 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。

配置基本信息	配置设备参数	配置安全提议	Spoke设备附加配置
IKE协商模式	<input type="radio"/> 主模式	<input checked="" type="radio"/> 野蛮模式	
NAT穿越	<input checked="" type="radio"/> 是	<input type="radio"/> 否	
IKE验证方法	<input checked="" type="radio"/> 预共享密钥	<input type="radio"/> CA认证	
身份验证字	<input type="text" value="iMC"/>		
ID Type	<input type="radio"/> IP	<input checked="" type="radio"/> 名字	
Hub IKE网关名称	<input type="text" value="HUB"/>		
Spoke IKE网关名称	<input type="text" value="SPOKE"/>		
IPsec报文封装形式	<input checked="" type="radio"/> 隧道模式	<input type="radio"/> 传输模式	
使用策略模板	<input type="radio"/> 是	<input checked="" type="radio"/> 否	
使用PFS特性	<input type="checkbox"/>		
配置安全联盟生存周期	<input type="radio"/> 是	<input checked="" type="radio"/> 否	
是否在Hub设备上生成静态路由	<input type="radio"/> 不生成	<input checked="" type="radio"/> 生成	<input type="radio"/> 反向路由注入
是否在Spoke设备上生成静态路由	<input type="radio"/> 不生成	<input checked="" type="radio"/> 生成	

- 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。

保护流配置					
*172.16.0.201 - CPE*保护流列表					
增加		删除			
共有1条记录, 当前第1-1, 第 1/1 页。				每页显示: 8 15 [50] 100 200	
<input type="checkbox"/>	协议类型	Hub侧保护流IP地址/掩码	操作符	端口号	Spoke侧保护流IP地址/掩码
<input type="checkbox"/>	IP	10.2.0.1/255.255.255.255	-	-	10.1.0.1/255.255.255.255

- 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。

Hub设备	Hub设备接口(网关地址)	Spoke设备	Spoke设备接口(网关地址)	部署状态	监视参数	配置	操作
<input type="checkbox"/>	172.16.0.201(172.16...	GigabitEthernet...	CPE(192.168.10.1)	GigabitEthernet...	未部署	已配置	

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。

配置基本信息	配置设备参数	配置安全提议	Spoke设备附加配置	Hub设备高级配置	Spoke设备高级配置
* IPsec策略名称		hub			
* IKE Peer名称		hub			
		<input type="button" value="确定"/> <input type="button" value="返回"/>			

点击“Spoke设备高级配置”，可做截图中所示配置。

<div style="text-align: center;"> 修改隧道“172.16.0.201(172.16.0.201) - CPE(192.168.10.1)”Spoke设备高级配置成功。 </div>					
配置基本信息	配置设备参数	配置安全提议	Spoke设备附加配置	Hub设备高级配置	Spoke设备高级配置
* IPsec策略名称		spoke			
* IKE Peer名称		spoke			
		<input type="button" value="确定"/> <input type="button" value="返回"/>			

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。

Hub设备	Hub设备接口(网关地址)	Spoke设备	Spoke设备接口(网关地址)	部署状态	监视参数	配置	操作
<input checked="" type="checkbox"/>	172.16.0.201(172.16...	GigabitEthernet...	CPE(192.168.10.1)	GigabitEthernet...	未部署	已配置	

隧道名称	失败设备	错误命令	是否回滚	回滚结果	操作结果	操作失败原因
172.16.0.201 (172.16.0.201...					Hub配置已下发，Spoke配置已下发到BIMS。	

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。

拆除列表						
 拆除完成。共拆除1条隧道，其中：拆除成功1条，拆除失败0条。						
隧道名称	失败设备	错误命令	是否回滚	回滚结果	操作结果	操作失败原因
172.16.0.201 (172.16.0.201...					Hub配置已下发，Spoke配置已下发到BIMS。	

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每个选项的定义，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。