举例：总部与分支机构之间建立IPSec VPN（IKE安全策略）

在实际的应用中，经常需要使用HUB-Spoke类型的组网，即一个总部到多个分支机构的组网，分支节点建立到总部的IPSec隧道，各个分支机构之间的通信由总部节点转发和控制。实现HUB-Spoke组网的配置有2种配置方式，安全策略方式与策略模版方式。本配置任务中，两个分支机构及总公司都采用安全策略方式建立IPSec隧道。安全策略方式可以由双方主动发起IPSec连接，适用于分支机构IP固定的情况。

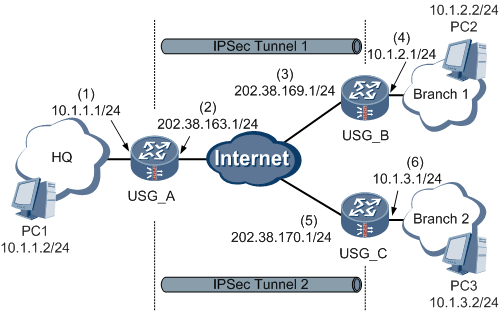
组网需求

如[图1](http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/cfg_vpn/sec_vsp_cfg_ipsec_0046.html?ft=0&fe=10&hib=9.3.10.2.4.6&id=sec_vsp_cfg_ipsec_0046&text=%25E4%25B8%25BE%25E4%25BE%258B%25EF%25BC%259A%25E6%2580%25BB%25E9%2583%25A8%25E4%25B8%258E%25E5%2588%2586%25E6%2594%25AF%25E6%259C%25BA%25E6%259E%2584%25E4%25B9%258B%25E9%2597%25B4%25E5%25BB%25BA%25E7%25AB%258BIPSec%2520VPN%25EF%25BC%2588IKE%25E5%25AE%2589%25E5%2585%25A8%25E7%25AD%2596%25E7%2595%25A5%25EF%25BC%2589&docid=EDOC1000086423" \l "sec_vsp_cfg_ipsec_0046__fig1)所示，某企业分为(HQ)和两个分支机构（Branch 1和Branch 2）。组网如下：

* 公司总部和两个分支机构分别通过USG\_A、USG\_B和USG\_C连接到Internet。
* USG\_A和USG\_B、USG\_C路由可达。
* USG\_A与USG\_B、USG\_C的公网IP地址均固定。

要求实现如下需求：

主机PC1与PC2、PC3之间可以安全的通信，PC2、PC3通过USG\_A进行安全通信，USG\_A与USG\_B 、USG\_C之间使用IKE自动协商建立安全通道，分支机构1、分支机构2之间可以通过IPSec隧道进行通信。

**图1** 总部与分支机构之间建立IPSec VPN（IKE安全策略）组网图   


| **项目** | **USG\_A** | **USG\_B** | **USG\_C** |
| --- | --- | --- | --- |

| **项目** | | **USG\_A** | **USG\_B** | **USG\_C** |
| --- | --- | --- | --- | --- |
| 外网接口 | | （2）  接口号：GigabitEthernet 0/0/2  IP地址：202.38.163.1/24 | （3）  接口号：GigabitEthernet 0/0/2  IP地址：202.38.169.1/24 | （5）  接口号：GigabitEthernet 0/0/2  IP地址：202.38.170.1/24 |
| 内网接口 | | （1）  接口号：GigabitEthernet 0/0/1  IP地址：10.1.1.1/24 | （4）  接口号：GigabitEthernet 0/0/1  IP地址：10.1.2.1/24 | （6）  接口号：GigabitEthernet 0/0/1  IP地址：10.1.3.1/24 |
| IPSec策略建立方式 | | 安全策略 | 安全策略 | 安全策略 |
| IPSec安全提议 | 封装模式 | 隧道模式 | 隧道模式 | 隧道模式 |
| 安全协议 | ESP | ESP | ESP |
| ESP协议认证算法 | SHA1 | SHA1 | SHA1 |
| ESP协议加密算法 | AES | AES | AES |
| IKE安全提议 | 验证方法 | 预共享密钥 | 预共享密钥 | 预共享密钥 |
| 认证算法 | SHA1 | SHA1 | SHA1 |
| IKE对等体 | 协商模式 | peer b：主模式  peer c：主模式 | 主模式 | 主模式 |
| 预共享密钥 | peer b：abcde  peer c：abcde | abcde | abcde |
| 身份类型 | peer b：IP  peer c：IP | IP | IP |
| 对端IP地址 | peer b：202.38.169.1  peer c：202.38.170.1 | 202.38.163.1 | 202.38.163.1 |
| 版本 | peer b：V1 and V2  peer c：V1 and V2 | V1 and V2 | V1 and V2 |

配置思路

对于USG\_A、USG\_B和USG\_C，配置思路相同。配置步骤和配置思路如下：

1. 基本配置，包括配置接口IP地址，将接口加入相应的安全区域。
2. 配置域间包过滤。
3. 配置公网路由，一般情况下，USG上配置静态路由。
4. 通过配置ACL规则组来定义需要保护的数据流。
5. 配置IPSec安全提议。
6. 配置IKE安全提议。
7. 配置IKE Peer。
8. 配置IPSec安全策略。
9. 应用IPSec安全策略。

操作步骤

* 配置USG\_A。
  1. 基本配置。
     1. 配置接口IP地址。
     2. <USG\_A> **system-view**
     3. [USG\_A] **interface GigabitEthernet 0/0/1**
     4. [USG\_A-GigabitEthernet0/0/1] **ip address 10.1.1.1 24**

[USG\_A-GigabitEthernet0/0/1] **quit**

[USG\_A] **interface GigabitEthernet 0/0/2**

[USG\_A-GigabitEthernet0/0/2] **ip address 202.38.163.1 24**

[USG\_A-GigabitEthernet0/0/2] **quit**

* + 1. 配置接口加入相应安全区域。
    2. [USG\_A] **firewall zone trust**
    3. [USG\_A-zone-trust] **add interface GigabitEthernet 0/0/1**

[USG\_A-zone-trust] **quit**

[USG\_A] **firewall zone untrust**

[USG\_A-zone-untrust] **add interface GigabitEthernet 0/0/2**

[USG\_A-zone-untrust] **quit**

* + 1. 配置域间包过滤规则。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

既可以打开Trust域和Untrust域的域间包过滤规则,也可以配置域间策略。

配置Local域和Untrust域的域间包过滤规则的目的为允许IPSec隧道两端设备通信，使其能够进行隧道协商。

配置Trust域与Untrust域的域间包过滤规则。

[USG\_A] **policy interzone trust untrust inbound**

[USG\_A-policy-interzone-trust-untrust-inbound] **policy 1**

[USG\_A-policy-interzone-trust-untrust-inbound-1] **policy source 10.1.2.0 0.0.0.255**

[USG\_A-policy-interzone-trust-untrust-inbound-1] **policy source 10.1.3.0 0.0.0.255**

[USG\_A-policy-interzone-trust-untrust-inbound-1] **policy destination 10.1.1.0 0.0.0.255**

[USG\_A-policy-interzone-trust-untrust-inbound-1] **action permit**

[USG\_A-policy-interzone-trust-untrust-inbound-1] **quit**

[USG\_A-policy-interzone-trust-untrust-inbound] **quit**

[USG\_A] **policy interzone trust untrust outbound**

[USG\_A-policy-interzone-trust-untrust-outbound] **policy 1**

[USG\_A-policy-interzone-trust-untrust-outbound-1] **policy source 10.1.1.0 0.0.0.0.255**

[USG\_A-policy-interzone-trust-untrust-outbound-1] **policy destination 10.1.2.0 0.0.0.255**

[USG\_A-policy-interzone-trust-untrust-outbound-1] **policy destination 10.1.3.0 0.0.0.255**

[USG\_A-policy-interzone-trust-untrust-outbound-1] **action permit**

[USG\_A-policy-interzone-trust-untrust-outbound-1] **quit**

[USG\_A-policy-interzone-trust-untrust-outbound] **quit**

配置Untrust域与Local域的域间包过滤规则。

[USG\_A] **policy interzone local untrust inbound**

[USG\_A-policy-interzone-local-untrust-inbound] **policy 1**

[USG\_A-policy-interzone-local-untrust-inbound-1] **policy source 202.38.169.0 0.0.0.255**

[USG\_A-policy-interzone-local-untrust-inbound-1] **policy source 202.38.170.0 0.0.0.255**

[USG\_A-policy-interzone-local-untrust-inbound-1] **policy destination 202.38.163.0 0.0.0.255**

[USG\_A-policy-interzone-local-untrust-inbound-1] **action permit**

[USG\_A-policy-interzone-local-untrust-inbound-1] **quit**

[USG\_A-policy-interzone-local-untrust-inbound] **quit**

[USG\_A] **policy interzone local untrust outbound**

[USG\_A-policy-interzone-local-untrust-outbound] **policy 1**

[USG\_A-policy-interzone-local-untrust-outbound-1] **policy source 202.38.163.0 0.0.0.255**

[USG\_A-policy-interzone-local-untrust-outbound-1] **policy destination 202.38.169.0 0.0.0.255**

[USG\_A-policy-interzone-local-untrust-outbound-1] **policy destination 202.38.170.0 0.0.0.255**

[USG\_A-policy-interzone-local-untrust-outbound-1] **action permit**

[USG\_A-policy-interzone-local-untrust-outbound-1] **quit**

[USG\_A-policy-interzone-local-untrust-outbound] **quit**

* 1. 配置到达分支机构的静态路由，此处假设下一跳地址为202.38.163.2。
  2. [USG\_A] **ip route-static 10.1.2.0 255.255.255.0 202.38.163.2**

[USG\_A] **ip route-static 10.1.3.0 255.255.255.0 202.38.163.2**

* 1. 定义被保护的数据流。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

为了实现各分支机构之间的互通，高级ACL的源地址（Source）定义为包括总部和分支的所有网段，目的地址（Destination）定义为各个分支机构的精确网段。

* + 1. 配置高级ACL 3000，定义总部到分支机构1的数据流。
    2. [USG\_A] **acl 3000**
    3. [USG\_A-acl-adv-3000] **rule permit ip source 10.1.0.0 0.0.255.255 destination 10.1.2.0 0.0.0.255**

[USG\_A-acl-adv-3000] **quit**

* + 1. 配置高级ACL 3001，定义总部到分支机构2的数据流。
    2. [USG\_A] **acl 3001**
    3. [USG\_A-acl-adv-3001] **rule permit ip source 10.1.0.0 0.0.255.255 destination 10.1.3.0 0.0.0.255**

[USG\_A-acl-adv-3001] **quit**

* 1. 配置名称为tran1的IPSec安全提议。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

其中，ESP为缺省安全协议，Tunnel为缺省封装模式，可以不配置。SHA1为ESP缺省认证算法，AES为ESP缺省加密算法，可以不配置。

[USG\_A] **ipsec proposal tran1**

[USG\_A-ipsec-proposal-tran1] **encapsulation-mode tunnel**

[USG\_A-ipsec-proposal-tran1] **transform esp**

[USG\_A-ipsec-proposal-tran1] **esp authentication-algorithm sha1**

[USG\_A-ipsec-proposal-tran1] **esp encryption-algorithm aes-128**

[USG\_A-ipsec-proposal-tran1] **quit**

* 1. 配置序号为10的IKE安全提议。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

pre-share验证方法为IKE缺省验证方法，SHA1为默认认证算法，可以不配置。

[USG\_A] **ike proposal 10**

[USG\_A-ike-proposal-10] **authentication-method pre-share**

[USG\_A-ike-proposal-10] **authentication-algorithm sha1**

[USG\_A-ike-proposal-10] **quit**

* 1. 配置IKE Peer。
     1. 配置名称为b的IKE Peer。
     2. [USG\_A] **ike peer b**
     3. [USG\_A-ike-peer-b] **ike-proposal 10**
     4. [USG\_A-ike-peer-b] **remote-address 202.38.169.1**
     5. [USG\_A-ike-peer-b] **pre-shared-key abcde**

[USG\_A-ike-peer-b] **quit**

* + 1. 配置名称为c的IKE Peer。
    2. [USG\_A] **ike peer c**
    3. [USG\_A-ike-peer-c] **ike-proposal 10**
    4. [USG\_A-ike-peer-c] **remote-address 202.38.170.1**
    5. [USG\_A-ike-peer-c] **pre-shared-key abcde**

[USG\_A-ike-peer-c] **quit**

* 1. http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**
  2. USG同时开启IKEv1和IKEv2，缺省情况下采用IKEv2进行协商，若对端不支持IKEv2，请禁用IKEv2，采用IKEv1进行协商。请在IKE Peer视图下执行命令**[undo version 2](http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/cli/version_ikepeer_view.html)**进行配置。
  3. 隧道对端IP地址分别为USG\_B、USG\_C与Internet相连的接口的IP地址。
  4. 验证字的配置需要与对端设备相同。
  5. 配置IPSec安全策略组map1。
     1. 配置序号为10的安全策略。
     2. [USG\_A] **ipsec policy map1 10 isakmp**
     3. [USG\_A-ipsec-policy-isakmp-map1-10] **security acl 3000**
     4. [USG\_A-ipsec-policy-isakmp-map1-10] **proposal tran1**
     5. [USG\_A-ipsec-policy-isakmp-map1-10] **ike-peer b**

[USG\_A-ipsec-policy-isakmp-map1-10] **quit**

* + 1. 配置序号为20的安全策略。
    2. [USG\_A] **ipsec policy map1 20 isakmp**
    3. [USG\_A-ipsec-policy-isakmp-map1-20] **security acl 3001**
    4. [USG\_A-ipsec-policy-isakmp-map1-20] **proposal tran1**
    5. [USG\_A-ipsec-policy-isakmp-map1-20] **ike-peer c**

[USG\_A-ipsec-policy-isakmp-map1-20] **quit**

* 1. 在接口GigabitEthernet 0/0/2上应用安全策略组map1。
  2. [USG\_A] **interface GigabitEthernet 0/0/2**
  3. [USG\_A-GigabitEthernet0/0/2] **ipsec policy map1**

[USG\_A-GigabitEthernet0/0/2] **quit**

* 配置USG\_B。
  1. 基础配置。

请根据[图1](http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/cfg_vpn/sec_vsp_cfg_ipsec_0046.html?ft=0&fe=10&hib=9.3.10.2.4.6&id=sec_vsp_cfg_ipsec_0046&text=%25E4%25B8%25BE%25E4%25BE%258B%25EF%25BC%259A%25E6%2580%25BB%25E9%2583%25A8%25E4%25B8%258E%25E5%2588%2586%25E6%2594%25AF%25E6%259C%25BA%25E6%259E%2584%25E4%25B9%258B%25E9%2597%25B4%25E5%25BB%25BA%25E7%25AB%258BIPSec%2520VPN%25EF%25BC%2588IKE%25E5%25AE%2589%25E5%2585%25A8%25E7%25AD%2596%25E7%2595%25A5%25EF%25BC%2589&docid=EDOC1000086423" \l "sec_vsp_cfg_ipsec_0046__fig1)的数据配置接口IP地址。将接口GigabitEthernet 0/0/1加入Trust区域，接口GigabitEthernet 0/0/2加入Untrust区域，并配置域间包过滤规则。详细步骤可参见USG\_A的配置。

* 1. 配置到达总部和其他私网的静态路由，此处假设下一跳地址为202.38.169.2。

[USG\_B] **ip route-static 0.0.0.0 0.0.0.0 202.38.169.2**

* 1. 定义被保护的数据流。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

为了实现和总部及分支机构2之间的通信，Source定义为分支机构1的精确网段，Destination定义为包含总部和分支机构2的所有网段。

[USG\_B] **acl 3000**

[USG\_B-acl-adv-3000] **rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.255.255**

[USG\_B-acl-adv-3000] **quit**

* 1. 配置名称为tran1的IPSec安全提议。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

其中，ESP为缺省安全协议，Tunnel为缺省封装模式，可以不配置。SHA1为ESP缺省认证算法，AES为ESP缺省加密算法，可以不配置。

[USG\_B] **ipsec proposal tran1**

[USG\_B-ipsec-proposal-tran1] **encapsulation-mode tunnel**

[USG\_B-ipsec-proposal-tran1] **transform esp**

[USG\_B-ipsec-proposal-tran1] **esp authentication-algorithm sha1**

[USG\_B-ipsec-proposal-tran1] **esp encryption-algorithm aes-128**

[USG\_B-ipsec-proposal-tran1] **quit**

* 1. 配置序号为10的IKE安全提议。

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

pre-share验证方法为IKE缺省验证方法，SHA1为默认认证算法，可以不配置。

[USG\_B] **ike proposal 10**

[USG\_B-ike-proposal-10] **authentication-method pre-share**

[USG\_B-ike-proposal-10] **authentication-algorithm sha1**

[USG\_B-ike-proposal-10] **quit**

* 1. 配置名称为a的IKE peer。
  2. [USG\_B] **ike peer a**
  3. [USG\_B-ike-peer-a] **ike-proposal 10**
  4. [USG\_B-ike-peer-a] **remote-address 202.38.163.1**
  5. [USG\_B-ike-peer-a] **pre-shared-key abcde**

[USG\_B-ike-peer-a] **quit**

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

USG同时开启IKEv1和IKEv2，缺省情况下采用IKEv2进行协商，若对端不支持IKEv2，请禁用IKEv2，采用IKEv1进行协商。

验证字的配置需要与对端设备相同。

* 1. 配置名称为map1序号为10的安全策略。
  2. [USG\_B] **ipsec policy map1 10 isakmp**
  3. [USG\_B-ipsec-policy-isakmp-map1-10] **security acl 3000**
  4. [USG\_B-ipsec-policy-isakmp-map1-10] **proposal tran1**
  5. [USG\_B-ipsec-policy-isakmp-map1-10] **ike-peer a**

[USG\_B-ipsec-policy-isakmp-map1-10] **quit**

* 1. 在接口GigabitEthernet 0/0/2上应用安全策略map1。
  2. [USG\_B] **interface GigabitEthernet 0/0/2**
  3. [USG\_B-GigabitEthernet0/0/2] **ipsec policy map1**

[USG\_B-GigabitEthernet0/0/2] **quit**

* 配置USG\_C。

USG\_C的配置请参考USG\_B的配置。需要注意的是，在保护的数据流中，源地址与USG\_B不同，应为10.1.3.0/24网段。配置如下：

[USG\_C] **acl 3000**

[USG\_C-acl-adv-3000] **rule permit ip source 10.1.3.0 0.0.0.255 destination 10.1.0.0 0.0.255.255**

[USG\_C-acl-adv-3000] **quit**

http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/public_sys-resources/icon-note.gif**说明：**

为了实现和总部及分支机构1之间的通信，Source定义为分支机构2的精确网段，Destination定义为包含总部和分支机构1的所有网段。

结果验证

1. 配置成功后，分支机构1与总部之间、分支机构2与总部之间分别可以相互ping通。分别在USG\_A、USG\_B和USG\_C上执行**display** **ike** **sa**、**display** **ipsec** **sa**会显示安全联盟的建立情况。以USG\_B为例，出现以下显示说明IKE安全联盟、IPSec安全联盟建立成功。
2. <USG\_B> **display** **ike** **sa**
3. current ike sa number: 2
4. ---------------------------------------------------------------------
5. conn-id peer flag phase vpn
6. ---------------------------------------------------------------------
7. 101 202.38.163.1 RD v2:2 public
8. 100 202.38.163.1 RD v2:1 public
9. flag meaning
10. RD--READY ST--STAYALIVE RL--REPLACED FD--FADING
11. TO--TIMEOUT TD--DELETING NEG--NEGOTIATING D--DPD
12. <USG\_B> **display** **ipsec** **sa**
13. -----------------------------
14. IPsec policy name: "map1"
15. sequence number: 10
16. mode: isakmp
17. vpn: public
18. -----------------------------
19. connection id: 4
20. rule number: 0
21. encapsulation mode: tunnel
22. tunnel local : 202.38.169.1 tunnel remote: 202.38.163.1
23. flow source: 10.1.2.0-10.1.2.255 0-65535 0
24. flow destination: 10.1.1.0-10.1.1.255 0-65535 0
25. [inbound ESP SAs]
26. spi: 7519344 (0x72bc70)
27. vpn: public said: 8 cpuid: 0x0000
28. proposal: ESP-ENCRYPT-AES ESP-AUTH-SHA1
29. sa remaining key duration (bytes/sec): 1887436044/3572
30. max received sequence-number: 9
31. udp encapsulation used for nat traversal: N
32. [outbound ESP SAs]
33. spi: 5365969 (0x51e0d1)
34. vpn: public said: 9 cpuid: 0x0000
35. proposal: ESP-ENCRYPT-AES ESP-AUTH-SHA1
36. sa remaining key duration (bytes/sec): 1887435576/3572
37. max sent sequence-number: 10
38. udp encapsulation used for nat traversal: N
39. 执行命令**display** **ipsec** **statistics**可以查看被加密的数据包的变化，即它们之间的数据传输已被加密。以USG\_B为例。
40. <USG\_B>**display** **ipsec** **statistics**
41. the security packet statistics:
42. input/output security packets: 4/4
43. input/output security bytes: **400**/**400**
44. input/output dropped security packets: 0/0
45. the encrypt packet statistics
46. send sae:0, recv sae:0, send err:0
47. local cpu:0, other cpu:0, recv other cpu:0
48. intact packet:0, first slice:0, after slice:0
49. the decrypt packet statistics
50. send sae:0, recv sae:0, send err:0
51. local cpu:0, other cpu:0, recv other cpu:0
52. reass first slice:0, after slice:0, len err:0
53. dropped security packet detail:
54. no enough memory: 0, too long: 0
55. can't find SA: 0, wrong SA: 0
56. authentication: 0, replay: 0
57. front recheck: 0, after recheck: 0
58. exceed byte limit: 0, exceed packet limit: 0
59. change cpu enc: 0, dec change cpu: 0
60. change datachan: 0, fib search: 0
61. rcv enc(dec) form sae said err: 0, 0
62. send port: 0, output l3: 0, l2tp input: 0
63. negotiate about packet statistics:
64. IP packet ok:0, err:0, drop:0
65. IP rcv other cpu to ike:0, drop:0
66. IKE packet inbound ok:0, err:0
67. IKE packet outbound ok:0, err:0
68. SoftExpr:0, HardExpr:0, DPDOper:0, SwapSa:0

ModpCnt: 0, SaeSucc: 0, SoftwareSucc: 0

配置脚本

* USG\_A的配置脚本
* #
* acl number 3000
* rule 5 permit ip source 10.1.0.0 0.0.255.255 destination 10.1.2.0 0.0.0.255
* #
* acl number 3001
* rule 5 permit ip source 10.1.0.0 0.0.255.255 destination 10.1.3.0 0.0.0.255
* #
* ike proposal 10
* encryption-algorithm aes-cbc
* dh group2
* #
* ike peer b
* pre-shared-key %$%$U\zWG^\*\_4zY'uAgs\e:j'{r%$%$
* ike-proposal 10
* remote-address 202.38.169.1
* #
* ike peer c
* pre-shared-key %$%$U\zWG^\*\_4zY'uAgs\e:j'{r%$%$
* ike-proposal 10
* remote-address 202.38.170.1
* #
* ipsec proposal tran1
* esp authentication-algorithm sha1
* esp encryption-algorithm aes-128
* #
* ipsec policy map1 10 isakmp
* security acl 3000
* ike-peer b
* proposal tran1
* #
* ipsec policy map1 20 isakmp
* security acl 3001
* ike-peer c
* proposal tran1
* #
* interface GigabitEthernet0/0/1
* ip address 10.1.1.1 255.255.255.0
* #
* interface GigabitEthernet0/0/2
* ip address 202.38.163.1 255.255.255.0
* ipsec policy map1
* #
* firewall zone trust
* set priority 85
* add interface GigabitEthernet0/0/1
* #
* firewall zone untrust
* set priority 5
* add interface GigabitEthernet0/0/2
* #
* ip route-static 10.1.2.0 255.255.255.0 202.38.163.2
* ip route-static 10.1.3.0 255.255.255.0 202.38.163.2
* #
* policy interzone local untrust inbound
* policy 1
* action permit
* policy source 202.38.169.0 0.0.0.255
* policy source 202.38.170.0 0.0.0.255
* policy destination 202.38.163.0 0.0.0.255
* #
* policy interzone local untrust outbound
* policy 1
* action permit
* policy source 202.38.163.0 0.0.0.255
* policy destination 202.38.169.0 0.0.0.255
* policy destination 202.38.170.0 0.0.0.255
* #
* policy interzone trust untrust inbound
* policy 1
* action permit
* policy source 10.1.2.0 0.0.0.255
* policy source 10.1.3.0 0.0.0.255
* policy destination 10.1.1.0 0.0.0.255
* #
* policy interzone trust untrust outbound
* policy 1
* action permit
* policy source 10.1.1.0 0.0.0.0.255
* policy destination 10.1.2.0 0.0.0.255
* policy destination 10.1.3.0 0.0.0.255
* USG\_B的配置脚本
* #
* acl number 3000
* rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
* #
* ike proposal 10
* encryption-algorithm aes-cbc
* dh group2
* #
* ike peer a
* pre-shared-key %$%$U\zWG^\*\_4zY'uAgs\e:j'{r%$%$
* ike-proposal 10
* remote-address 202.38.163.1
* #
* ipsec proposal tran1
* esp authentication-algorithm sha1
* esp encryption-algorithm aes-128
* #
* ipsec policy map1 10 isakmp
* security acl 3000
* ike-peer a
* proposal tran1
* #
* interface GigabitEthernet0/0/1
* ip address 10.1.2.1 255.255.255.0
* #
* interface GigabitEthernet0/0/2
* ip address 202.38.169.1 255.255.255.0
* ipsec policy map1
* #
* firewall zone trust
* set priority 85
* add interface GigabitEthernet0/0/1
* #
* firewall zone untrust
* set priority 5
* add interface GigabitEthernet0/0/2
* #
* ip route-static 0.0.0.0 0.0.0.0 202.38.169.2
* #
* policy interzone local untrust inbound
* policy 1
* action permit
* policy source 202.38.163.0 0.0.0.255
* policy destination 202.38.169.0 0.0.0.255
* #
* policy interzone local untrust outbound
* policy 1
* action permit
* policy source 202.38.169.0 0.0.0.255
* policy destination 202.38.163.0 0.0.0.255
* #
* policy interzone trust untrust inbound
* policy 1
* action permit
* policy source 10.1.1.0 0.0.0.255
* policy destination 10.1.2.0 0.0.0.255
* #
* policy interzone trust untrust outbound
* policy 1
* action permit
* policy source 10.1.2.0 0.0.0.255
* policy destination 10.1.1.0 0.0.0.0.255
* USG\_C的配置脚本
* #
* acl number 3000
* rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.0.0 0.0.255.255
* #
* ike proposal 10
* encryption-algorithm aes-cbc
* dh group2
* #
* ike peer a
* pre-shared-key %$%$U\zWG^\*\_4zY'uAgs\e:j'{r%$%$
* ike-proposal 10
* remote-address 202.38.163.1
* #
* ipsec proposal tran1
* esp authentication-algorithm sha1
* esp encryption-algorithm aes-128
* #
* ipsec policy map1 10 isakmp
* security acl 3000
* ike-peer a
* proposal tran1
* #
* interface GigabitEthernet0/0/1
* ip address 10.1.3.1 255.255.255.0
* #
* interface GigabitEthernet0/0/2
* ip address 202.38.170.1 255.255.255.0
* ipsec policy map1
* #
* firewall zone trust
* set priority 85
* add interface GigabitEthernet0/0/1
* #
* firewall zone untrust
* set priority 5
* add interface GigabitEthernet0/0/2
* #
* ip route-static 0.0.0.0 0.0.0.0 202.38.170.2
* #
* policy interzone local untrust inbound
* policy 1
* action permit
* policy source 202.38.163.0 0.0.0.255
* policy destination 202.38.170.0 0.0.0.255
* #
* policy interzone local untrust outbound
* policy 1
* action permit
* policy source 202.38.170.0 0.0.0.255
* policy destination 202.38.163.0 0.0.0.255
* #
* policy interzone trust untrust inbound
* policy 1
* action permit
* policy source 10.1.1.0 0.0.0.255
* policy destination 10.1.3.0 0.0.0.255
* #
* policy interzone trust untrust outbound
* policy 1
* action permit
* policy source 10.1.3.0 0.0.0.255
* policy destination 10.1.1.0 0.0.0.0.255

父主题： [配置举例-局域网通过VPN互通](http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/cfg_vpn/sec_vsp_cfg_ipsec_0071.html)

华为专有和保密信息 版权所有 © 华为技术有限公司

华为专有和保密信息  
版权所有 © 华为技术有限公司

[< 上一节](http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/cfg_vpn/sec_vsp_cfg_ipsec_0056.html)[下一节 >](http://support.huawei.com/hedex/pages/EDOC1000086423SZD0528J/15/EDOC1000086423SZD0528J/15/resources/cfg_vpn/sec_vsp_cfg_ipsec_0034.html)

http://support.huawei.com/hedex/images/feedback.png我要反馈