H3C 防火墙与华为防火墙 IPsec 对接操作指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W100-20230627

前 言

《H3C 防火墙与华为防火墙 IPsec 对接操作指导》将会详细地介绍 H3C 防火墙与华为防火墙的 IPsec 对接操作。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... }*	表示从多个选项中至少选取一个。
[x | y | ...]*	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格　式	意　义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 H3C 防火墙与华为防火墙 IPsec 对接操作指导

1.1 简介

本章介绍 H3C 防火墙与华为防火墙 IPsec 对接的常用典型配置举例。

IPsec（IP Security，IP 安全）是 IETF 制定的三层隧道加密协议，它为互联网上传输的数据提供了高质量的、基于密码学的安全保证，是一种传统的实现三层 VPN（Virtual Private Network，虚拟专用网络）的安全技术。IPsec 通过在特定通信方之间（例如两个安全网关之间）建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

1.2 网关与网关之间采用IKE方式建立保护IPv4报文的IPsec隧道配置举例（预共享密钥认证方式）

1.2.1 适用产品和版本

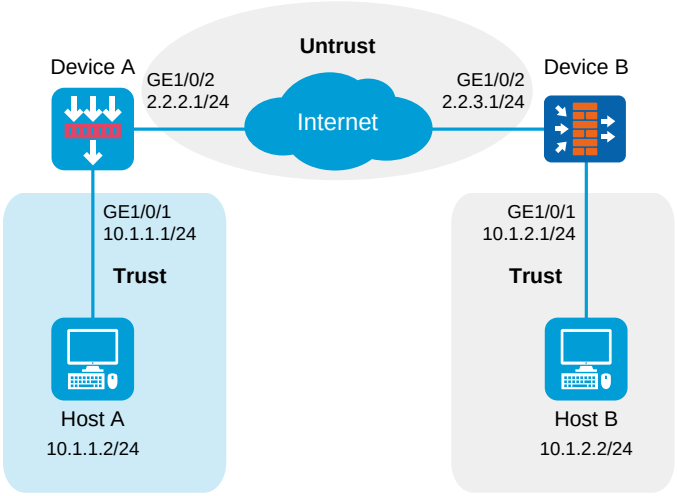
本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

1.2.2 组网需求

在 Device A 和 Device B 之间建立一条 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。具体要求如下：

- Device B 是华为设备。
- 封装形式为隧道模式。
- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- IKE 协商方式建立 IPsec SA。
- IKE 协商采用预共享密钥认证方式，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。

图1-1 保护 IPv4 报文的 IPsec 配置组网图



1.2.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ip route-static 10.1.2.0 24 2.2.2.2
[DeviceA] ip route-static 2.2.3.1 24 2.2.2.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy ip
[DeviceA-security-policy-ip] rule name ipseclocalout
[DeviceA-security-policy-ip-1-ipseclocalout] source-zone local
[DeviceA-security-policy-ip-1-ipseclocalout] destination-zone untrust
[DeviceA-security-policy-ip-1-ipseclocalout] source-ip-host 2.2.2.1
[DeviceA-security-policy-ip-1-ipseclocalout] destination-ip-host 2.2.3.1
[DeviceA-security-policy-ip-1-ipseclocalout] action pass
[DeviceA-security-policy-ip-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalin
[DeviceA-security-policy-ip-2-ipseclocalin] source-zone untrust
[DeviceA-security-policy-ip-2-ipseclocalin] destination-zone local
[DeviceA-security-policy-ip-2-ipseclocalin] source-ip-host 2.2.3.1
[DeviceA-security-policy-ip-2-ipseclocalin] destination-ip-host 2.2.2.1
[DeviceA-security-policy-ip-2-ipseclocalin] action pass
[DeviceA-security-policy-ip-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host A 与 Host B 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name trust-untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-zone trust
[DeviceA-security-policy-ip-3-trust-untrust] destination-zone untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-ip-subnet 10.1.1.0 24
[DeviceA-security-policy-ip-3-trust-untrust] destination-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-3-trust-untrust] action pass
[DeviceA-security-policy-ip-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name untrust-trust
[DeviceA-security-policy-ip-4-untrust-trust] source-zone untrust
[DeviceA-security-policy-ip-4-untrust-trust] destination-zone trust
[DeviceA-security-policy-ip-4-untrust-trust] source-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-4-untrust-trust] destination-ip-subnet 10.1.1.0 24
```

```
[DeviceA-security-policy-ip-4-untrust-trust] action pass
[DeviceA-security-policy-ip-4-untrust-trust] quit
[DeviceA-security-policy-ip] quit
```

(5) 定义需要保护的数据流

配置一个 IPv4 高级 ACL，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
[DeviceA] acl advanced 3101
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
[DeviceA-ipsec-transform-set-tran1] protocol esp
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-256
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha256
[DeviceA-ipsec-transform-set-tran1] quit
```

(7) 配置 IKE 安全提议

指定加密算法、认证算法、DH、认证方法，取值要与华为防火墙的配置值严格一致。

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method pre-share
[DeviceA-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceA-ike-proposal-1] dh group14
[DeviceA-ike-proposal-1] authentication-algorithm sha256
[DeviceA-ike-proposal-1] quit
```

(8) 配置 IKE keychain，约定通信双方使用的密钥信息

创建并配置 IKE keychain，协商双方配置的预共享密钥必须完全相同，具体配置步骤如下。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 2.2.3.1 255.255.255.0 key simple 123456TESTplat&!
[DeviceA-ike-keychain-keychain1] quit
```

(9) 配置 IKE profile，约定建立 IKE SA 所需的安全参数

```
[DeviceA] ike profile profile1
[DeviceA-ike-profile-profile1] keychain keychain1
[DeviceA-ike-profile-profile1] proposal 1
[DeviceA-ike-profile-profile1] match remote identity address 2.2.3.1 255.255.255.0
[DeviceA-ike-profile-profile1] quit
```

(10) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，指定本端和对端的 IP 地址，引用 IKE profile，具体配置步骤如下。

```
[DeviceA] ipsec policy map1 10 isakmp
[DeviceA-ipsec-policy-isakmp-map1-10] security acl 3101
[DeviceA-ipsec-policy-isakmp-map1-10] transform-set tran1
[DeviceA-ipsec-policy-isakmp-map1-10] local-address 2.2.2.1
[DeviceA-ipsec-policy-isakmp-map1-10] remote-address 2.2.3.1
[DeviceA-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-map1-10] quit
```

(11) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

在接口 GigabitEthernet1/0/2 上应用安全策略，具体配置步骤如下。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ipsec apply policy map1
[DeviceA-GigabitEthernet1/0/2] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.3.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ip route-static 10.1.1.0 24 2.2.3.2
[DeviceB] ip route-static 2.2.2.1 24 2.2.3.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface gigabitethernet 1/0/1
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface gigabitethernet 1/0/2
[DeviceB-zone-untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ipseclocalout
[DeviceB-policy-security-rule-ipseclocalout] source-zone local
[DeviceB-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceB-policy-security-rule-ipseclocalout] source-address 2.2.3.1 32
[DeviceB-policy-security-rule-ipseclocalout] destination-address 2.2.2.1 32
[DeviceB-policy-security-rule-ipseclocalout] action permit
[DeviceB-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-policy-security] rule name ipseclocalin
[DeviceB-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceB-policy-security-rule-ipseclocalin] destination-zone local
[DeviceB-policy-security-rule-ipseclocalin] source-address 2.2.2.1 32
[DeviceB-policy-security-rule-ipseclocalin] destination-address 2.2.3.1 32
[DeviceB-policy-security-rule-ipseclocalin] action permit
[DeviceB-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name trust-untrust
[DeviceB-policy-security-rule-trust-untrust] source-zone trust
[DeviceB-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceB-policy-security-rule-trust-untrust] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-trust-untrust] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-trust-untrust] action permit
[DeviceB-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name untrust-trust
[DeviceB-policy-security-rule-untrust-trust] source-zone untrust
[DeviceB-policy-security-rule-untrust-trust] destination-zone trust
[DeviceB-policy-security-rule-untrust-trust] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-untrust-trust] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-untrust-trust] action permit
```

```
[DeviceB-policy-security-rule-untrust-trust] quit
```

(5) 定义数据流需要保护的数据流

配置一个 IPv4 高级 ACL，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。

```
[DeviceB] acl 3101
[DeviceB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceB-ipsec-proposal-tran1] transform esp
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256
[DeviceB-ipsec-proposal-tran1] quit
```

(7) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] encryption-algorithm aes-256
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] authentication-algorithm sha2-256
[DeviceB-ike-proposal-1] quit
```

(8) 配置 IKE 对等体，指定协商模式、IKE 版本、预共享密钥，对端 IP 地址。

```
[DeviceB] ike peer h3c
[DeviceB-ike-peer-h3c] exchange-mode main
[DeviceB-ike-peer-h3c] undo version 2
[DeviceB-ike-peer-h3c] ike-proposal 1
[DeviceB-ike-peer-h3c] pre-shared-key 123456TESTplat&!
[DeviceB-ike-peer-h3c] remote-address 2.2.2.1
[DeviceB-ike-peer-h3c] quit
```

(9) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，引用 IKE 对等体，具体配置步骤如下。

```
[DeviceB] ipsec policy use1 10 isakmp
[DeviceB-ipsec-policy-isakmp-use1-1] ike-peer h3c
[DeviceB-ipsec-policy-isakmp-use1-1] proposal tran1
```

```
[DeviceB-ipsec-policy-isakmp-use1-1] security acl 3101
[DeviceB-ipsec-policy-isakmp-use1-1] quit
```

(10) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

在接口 GigabitEthernet1/0/2 上应用 IPsec 安全策略，具体配置步骤如下。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ipsec policy use1
[DeviceB-GigabitEthernet1/0/2] quit
```

1.2.4 验证配置

以上配置完成后，Device A 和 Device B 之间如果有子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的报文通过，将触发 IKE 进行 IPsec SA 的协商。IKE 成功协商出 IPsec SA 后，子网 10.1.1.0/24 与子网 10.1.2.0/24 之间数据流的传输将受到 IPsec SA 的保护。可通过以下显示查看到协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
------------------------------
Interface: GigabitEthernet1/0/2
------------------------------
  ------------------------------
  IPsec policy: map1
  Sequence number: 10
  Alisa: map1-10
  Mode: ISAKMP
  ------------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Initiator
    Path MTU: 1443
    Tunnel:
        local  address/port: 2.2.3.1/500
        remote address/port: 2.2.2.1/500
    Flow:
        sour addr: 2.2.3.1/0.0.0.0  port: 0  protocol: ip
        dest addr: 2.2.2.1/0.0.0.0  port: 0  protocol: ip
    [Inbound ESP SAs]
```

```
      SPI: 3769702703 (0xe0b1192f)
      Connection ID: 90194313219
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 3000/28800
      SA remaining duration (kilobytes/sec): 2300/797
      Max received sequence-number: 1
      Anti-replay check enable: N
      Anti-replay window size:
      UDP encapsulation used for NAT traversal: N
      Status: Active
    [Outbound ESP SAs]
      SPI: 3840956402 (0xe4f057f2)
      Connection ID: 64424509441
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 3000/28800
      SA remaining duration (kilobytes/sec): 2312/797
      Max sent sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

Device B 上也会产生相应的 IPsec SA 来保护 IPv4 报文，查看方式与 Device A 同，此处略。

1.2.5 配置文件

1. Device A

```
#
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy map1
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
#
 ip route-static 2.2.3.0 24 2.2.2.2
```

```
 ip route-static 10.1.2.0 24 2.2.2.2
#
acl advanced 3101
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3101
 local-address 2.2.2.1
 remote-address 2.2.3.1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 match remote identity address 2.2.3.1 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain keychain1
 pre-shared-key address 2.2.3.1 255.255.255.0 key simple 123456TESTplat&!
#
security-policy ip
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 2.2.2.1
  destination-ip-host 2.2.3.1
 rule 2 name ipseclocalin
  action pass
```

```
  source-zone untrust
  destination-zone local
  source-ip-host 2.2.3.1
  destination-ip-host 2.2.2.1
 rule 3 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
  destination-ip-subnet 10.1.2.0 255.255.255.0
 rule 4 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 10.1.2.0 255.255.255.0
  destination-ip-subnet 10.1.1.0 255.255.255.0
#
```

2. Device B

```
#
acl number 3101
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
#
ike peer h3c
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
 undo version 2
 remote-address 2.2.2.1
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ipsec policy use1 10 isakmp
```

```
 security acl 3101
 ike-peer h3c
 proposal tran1
#
interface GigabitEthernet1/0/1
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 2.2.3.1 255.255.255.0
 ipsec policy use1
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/2
#
 ip route-static 2.2.2.0 255.255.255.0 2.2.3.2
 ip route-static 10.1.1.0 255.255.255.0 2.2.3.2
#
security-policy
 rule name ipseclocalout
  source-zone local
  destination-zone untrust
  source-address 2.2.3.1 mask 255.255.255.255
  destination-address 2.2.2.1 mask 255.255.255.255
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 2.2.2.1 mask 255.255.255.255
  destination-address 2.2.3.1 mask 255.255.255.255
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
```

```
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
#
return
```

1.3 网关与网关之间采用IKE方式建立保护IPv6报文的IPsec隧道配置举例

1.3.1 适用产品和版本

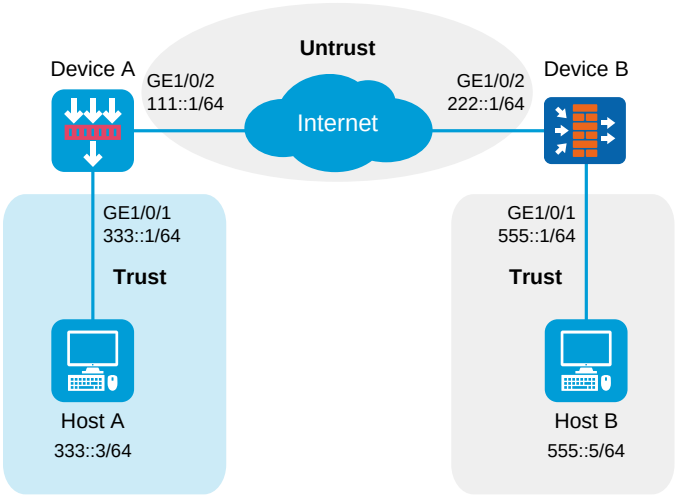
本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

1.3.2 组网需求

在 Device A 和 Device B 之间建立一条 IPsec 隧道，对 Host A 所在的子网（333::/64）与 Host B 所在的子网（555::/64）之间的数据流进行安全保护。具体要求如下：

- Device B 是华为设备。
- 封装形式为隧道模式。
- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- IKE 协商方式建立 IPsec SA。
- IKE 协商采用预共享密钥认证方式，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。

图1-2 保护 IPv6 报文的 IPsec 配置组网图



1.3.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipv6 address 333::1/64
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 111::2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ipv6 route-static 555::0 64 111::2
[DeviceA] ipv6 route-static 222::0 64 111::2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy ipv6
[DeviceA-security-policy-ipv6] rule name ipseclocalout
[DeviceA-security-policy-ipv6-1-ipseclocalout] source-zone local
[DeviceA-security-policy-ipv6-1-ipseclocalout] destination-zone untrust
[DeviceA-security-policy-ipv6-1-ipseclocalout] source-ip-host 111::1
[DeviceA-security-policy-ipv6-1-ipseclocalout] destination-ip-host 222::1
[DeviceA-security-policy-ipv6-1-ipseclocalout] action pass
```

```
[DeviceA-security-policy-ipv6-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ipv6] rule name ipseclocalin
[DeviceA-security-policy-ipv6-2-ipseclocalin] source-zone untrust
[DeviceA-security-policy-ipv6-2-ipseclocalin] destination-zone local
[DeviceA-security-policy-ipv6-2-ipseclocalin] source-ip-host 222::1
[DeviceA-security-policy-ipv6-2-ipseclocalin] destination-ip-host 111::1
[DeviceA-security-policy-ipv6-2-ipseclocalin] action pass
[DeviceA-security-policy-ipv6-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host A 与 Host B 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ipv6] rule name trust-untrust
[DeviceA-security-policy-ipv6-3-trust-untrust] source-zone trust
[DeviceA-security-policy-ipv6-3-trust-untrust] destination-zone untrust
[DeviceA-security-policy-ipv6-3-trust-untrust] source-ip-subnet 333::1 64
[DeviceA-security-policy-ipv6-3-trust-untrust] destination-ip-subnet 555::1 64
[DeviceA-security-policy-ipv6-3-trust-untrust] action pass
[DeviceA-security-policy-ipv6-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ipv6] rule name untrust-trust
[DeviceA-security-policy-ipv6-4-untrust-trust] source-zone untrust
[DeviceA-security-policy-ipv6-4-untrust-trust] destination-zone trust
[DeviceA-security-policy-ipv6-4-untrust-trust] source-ip-subnet 555::1 64
[DeviceA-security-policy-ipv6-4-untrust-trust] destination-ip-subnet 333::1 64
[DeviceA-security-policy-ipv6-4-untrust-trust] action pass
[DeviceA-security-policy-ipv6-4-untrust-trust] quit
[DeviceA-security-policy-ipv6] quit
```

(5) 定义需要保护的数据流

配置一个 IPv6 高级 ACL，定义要保护由子网 333::/64 去往子网 555::/64 的数据流。

```
[DeviceA] acl ipv6 advanced 3101
[DeviceA-acl-ipv6-adv-3101] rule permit ipv6 source 333::0 64 destination 555::0 64
[DeviceA-acl-ipv6-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceA] ipsec transform-set tran1
```

```
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
[DeviceA-ipsec-transform-set-tran1] protocol esp
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-256
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha256
[DeviceA-ipsec-transform-set-tran1] quit
```

(7) 配置 IKE keychain，约定通信双方使用的密钥信息

创建并配置 IKE keychain，协商双方配置的预共享密钥必须完全相同，具体配置步骤如下。

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address ipv6 222::1 64 key simple 123456TESTplat&!
[DeviceA-ike-keychain-keychain1] quit
```

(8) 配置 IKE 安全提议

指定加密算法、认证算法、DH、认证方法，取值要与华为防火墙的配置值严格一致。

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method pre-share
[DeviceA-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceA-ike-proposal-1] dh group14
[DeviceA-ike-proposal-1] authentication-algorithm sha256
[DeviceA-ike-proposal-1] quit
```

(9) 配置 IKE profile，约定建立 IKE SA 所需的安全参数

```
[DeviceA] ike profile profile1
[DeviceA-ike-profile-profile1] keychain keychain1
[DeviceA-ike-profile-profile1] proposal 1
[DeviceA-ike-profile-profile1] match remote identity address ipv6 222::1 64
[DeviceA-ike-profile-profile1] quit
```

(10) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，指定本端和对端的 IP 地址，引用 IKE profile，具体配置步骤如下。

```
[DeviceA] ipsec ipv6-policy map1 10 isakmp
[DeviceA-ipsec-ipv6-policy-isakmp-map1-10] security acl ipv6 3101
[DeviceA-ipsec-ipv6-policy-isakmp-map1-10] transform-set tran1
[DeviceA-ipsec-ipv6-policy-isakmp-map1-10] local-address ipv6 111::1
[DeviceA-ipsec-ipv6-policy-isakmp-map1-10] remote-address ipv6 222::1
[DeviceA-ipsec-ipv6-policy-isakmp-map1-10] ike-profile profile1
[DeviceA-ipsec-ipv6-policy-isakmp-map1-10] quit
```

(11) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

在接口 GigabitEthernet1/0/2 上应用 IPsec 安全策略，具体配置步骤如下。

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ipsec apply ipv6-policy map1
[DeviceA-GigabitEthernet1/0/2] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

开启全局 IPv6 功能，根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
[DeviceB] ipv6
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipv6 enable
[DeviceB-GigabitEthernet1/0/1] ipv6 address 555::1/64
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 222::2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ipv6 route-static 333::0 64 222::2
[DeviceB] ipv6 route-static 111::0 64 222::2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface gigabitethernet 1/0/1
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface gigabitethernet 1/0/2
[DeviceB-zone-untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ipseclocalout
[DeviceB-policy-security-rule-ipseclocalout] source-zone local
[DeviceB-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceB-policy-security-rule-ipseclocalout] source-address 222::1 64
[DeviceB-policy-security-rule-ipseclocalout] destination-address 111::1 64
```

```
[DeviceB-policy-security-rule-ipseclocalout] action permit
[DeviceB-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-policy-security] rule name ipseclocalin
[DeviceB-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceB-policy-security-rule-ipseclocalin] destination-zone local
[DeviceB-policy-security-rule-ipseclocalin] source-address 111::1 64
[DeviceB-policy-security-rule-ipseclocalin] destination-address 222::1 64
[DeviceB-policy-security-rule-ipseclocalin] action permit
[DeviceB-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name trust-untrust
[DeviceB-policy-security-rule-trust-untrust] source-zone trust
[DeviceB-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceB-policy-security-rule-trust-untrust] source-address 555::1 64
[DeviceB-policy-security-rule-trust-untrust] destination-address 333::1 64
[DeviceB-policy-security-rule-trust-untrust] action permit
[DeviceB-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name untrust-trust
[DeviceB-policy-security-rule-untrust-trust] source-zone untrust
[DeviceB-policy-security-rule-untrust-trust] destination-zone trust
[DeviceB-policy-security-rule-untrust-trust] source-address 333::1 64
[DeviceB-policy-security-rule-untrust-trust] destination-address 555::1 64
[DeviceB-policy-security-rule-untrust-trust] action permit
[DeviceB-policy-security-rule-untrust-trust] quit
[DeviceB-policy-security] quit
```

(5) 定义需要保护的数据流

配置一个 IPv6 高级 ACL，定义要保护由子网 555::/64 去往子网 333::/64 的数据流。

```
[DeviceB] acl ipv6 3101
[DeviceB-acl-ipv6-adv-3101] rule permit ipv6 source 555::/64 destination 333::/64
[DeviceB-acl-ipv6-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceB] ipsec proposal transform1
[DeviceB-ipsec-proposal-transform1] encapsulation-mode tunnel
[DeviceB-ipsec-proposal-transform1] transform esp
[DeviceB-ipsec-proposal-transform1] esp encryption-algorithm aes-256
[DeviceB-ipsec-proposal-transform1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-transform1] quit
```

(7) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] encryption-algorithm aes-256
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] authentication-algorithm sha2-256
[DeviceB-ike-proposal-1] quit
```

(8) 配置 IKE 对等体，指定协商模式、IKE 版本、预共享密钥，对端 IP 地址。

```
[DeviceB] ike peer h3c
[DeviceB-ike-peer-h3c] exchange-mode main
[DeviceB-ike-peer-h3c] undo version 2
[DeviceB-ike-peer-h3c] ike-proposal 1
[DeviceB-ike-peer-h3c] pre-shared-key 123456TESTplat&!
[DeviceB-ike-peer-h3c] remote-address 111::1
[DeviceB-ike-peer-h3c] quit
```

(9) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，引用 IKE 对等体，具体配置步骤如下。

```
[DeviceB] ipsec policy use1 10 isakmp
[DeviceB-ipsec-policy-isakmp-use1-10] ike-peer h3c
[DeviceB-ipsec-policy-isakmp-use1-10] proposal transform1
[DeviceB-ipsec-policy-isakmp-use1-10] security acl ipv6 3101
[DeviceB-ipsec-policy-isakmp-use1-10] quit
```

(10) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

在接口 GigabitEthernet1/0/2 上应用 IPsec 安全策略，具体配置步骤如下。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ipsec policy use1
[DeviceB-GigabitEthernet1/0/2] quit
```

1.3.4 验证配置

以上配置完成后，当 Device A 和 Device B 之间有子网 333::/64 与子网 555::/64 之间的报文通过时，将触发 IKE 进行 IPsec SA 的协商。IKE 成功协商出 IPsec SA 后，子网 333::/64 与子网 555::/64 之间数据流的传输将受到 IPsec SA 的保护。可通过以下显示查看到协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
------------------------------
Interface: GigabitEthernet1/0/2
------------------------------
  ----------------------------
  IPsec policy: map1
  Sequence number: 10
  Alisa: map1-10
  Mode: ISAKMP
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Initiator
    Path MTU: 1423
    Tunnel:
        local  address/port: 111::1/500
        remote address/port: 222::1/500
    Flow:
    sour addr: 333::1/0      port: 0  protocol: ipv6
    dest addr: 555::1/0      port: 0  protocol: ipv6
    [Inbound ESP SAs]
      SPI: 3769702703 (0xe0b1192f)
      Connection ID: 1
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 3000/28800
      SA remaining duration (kilobytes/sec): 2300/797
      Max received sequence-number: 1
      Anti-replay check enable: N
      Anti-replay window size:
      UDP encapsulation used for NAT traversal: N
```

```
      Status: Active
    [Outbound ESP SAs]
      SPI: 3840956402 (0xe4f057f2)
      Connection ID: 2
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 3000/28800
      SA remaining duration (kilobytes/sec): 2312/797
      Max sent sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

Device B 上也会产生相应的 IPsec SA 来保护 IPv6 报文，查看方式与 Device A 同，此处略。

1.3.5 配置文件

1. Device A

```
#
interface GigabitEthernet1/0/1
 ipv6 address 333::1/64
#
interface GigabitEthernet1/0/2
 ipv6 address 111::1/64
 ipsec apply ipv6-policy map1
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
#
 ipv6 route-static 222:: 64 111::2
 ipv6 route-static 555:: 64 111::2
#
acl ipv6 advanced 3101
 rule 0 permit ipv6 source 333::/64 destination 555::/64
#
ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
```

```
ipsec ipv6-policy map1 10 isakmp
 transform-set tran1
 security acl ipv6 3101
 local-address ipv6 111::1
 remote-address ipv6 222::1
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 match remote identity address ipv6 222::1 64
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain keychain1
 pre-shared-key address ipv6 222::1 64 key simple 123456TESTplat&!
#
security-policy ipv6
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 111::1
  destination-ip-host 222::1
 rule 2 name ipseclocalin
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 222::1
  destination-ip-host 111::1
 rule 3 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 333::/64
```

```
  destination-ip-subnet 555::/64
 rule 4 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 555::/64
  destination-ip-subnet 333::/64
#
```

2. Device B

```
#
ipv6
#
acl ipv6 number 3101
 rule 5 permit ipv6 source 555::/64 destination 333::/64
#
ipsec proposal transform1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
#
ike peer h3c
 undo version 2
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
 remote-address 111::1
#
ipsec policy use1 10 isakmp
 security acl ipv6 3101
 ike-peer h3c
 proposal transform1
#
interface GigabitEthernet1/0/1
 ipv6 enable
 ipv6 address 555::1/64
```

```
#
interface GigabitEthernet1/0/2
 ipv6 enable
 ipv6 address 222::1/64
 ipsec policy use1
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/2
#
ipv6 route-static 111:: 64 222::2
ipv6 route-static 333:: 64 222::2
#
security-policy
 rule name ipseclocalout
  source-zone local
  destination-zone untrust
  source-address 222::1 64
  destination-address 111::1 64
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 111::1 64
  destination-address 222::1 64
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 555::1 64
  destination-address 333::1 64
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 333::1 64
```

```
  destination-address 555::1 64
  action permit
#
```

1.4 网关与网关之间存在NAT设备时采用IKE方式建立保护IPv4报文的IPsec隧道配置举例

1.4.1 适用产品和版本

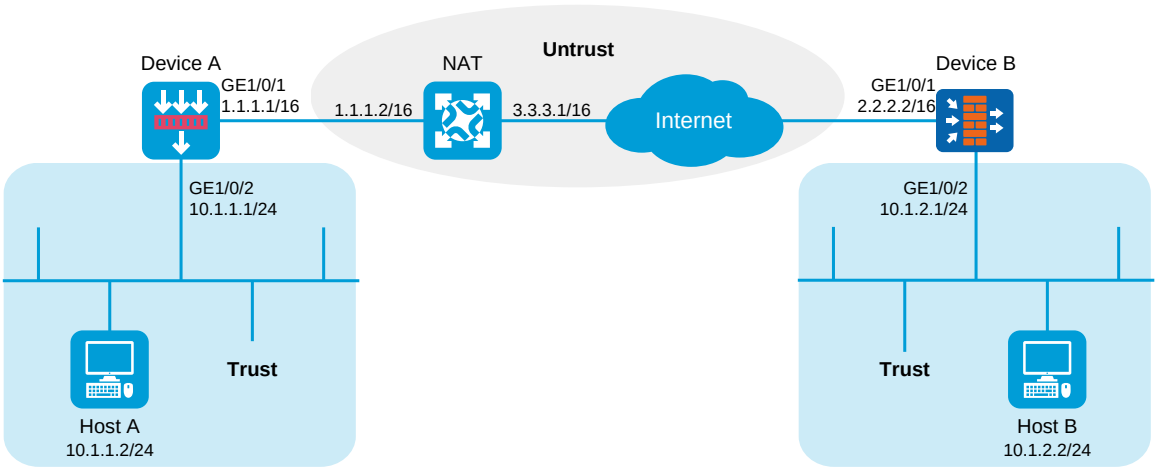
本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

1.4.2 组网需求

Device A 在 NAT 安全网关内网侧，所连接的内网侧用户使用 NAT 地址 3.3.3.1 访问外网。要求在 Device A 和 Device B 之间建立一个 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。具体需要求如下：

- Device B 是华为设备。
- 封装形式为隧道模式。
- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- IKE 协商方式建立 IPsec SA。
- IKE 协商采用预共享密钥认证方式，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- Device B 开启 NAT 穿越功能。

图1-3 NAT 穿越配置组网图



1.4.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 255.255.0.0
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 1.1.1.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ip route-static 10.1.2.0 24 1.1.1.2
[DeviceA] ip route-static 2.2.2.2 16 1.1.1.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy ip
[DeviceA-security-policy-ip] rule name ipseclocalout
[DeviceA-security-policy-ip-1-ipseclocalout] source-zone local
[DeviceA-security-policy-ip-1-ipseclocalout] destination-zone untrust
[DeviceA-security-policy-ip-1-ipseclocalout] source-ip-host 1.1.1.1
[DeviceA-security-policy-ip-1-ipseclocalout] destination-ip-host 2.2.2.2
[DeviceA-security-policy-ip-1-ipseclocalout] action pass
[DeviceA-security-policy-ip-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalin
[DeviceA-security-policy-ip-2-ipseclocalin] source-zone untrust
[DeviceA-security-policy-ip-2-ipseclocalin] destination-zone local
[DeviceA-security-policy-ip-2-ipseclocalin] source-ip-host 2.2.2.2
[DeviceA-security-policy-ip-2-ipseclocalin] destination-ip-host 1.1.1.1
[DeviceA-security-policy-ip-2-ipseclocalin] action pass
[DeviceA-security-policy-ip-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host A 与 Host B 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name trust-untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-zone trust
[DeviceA-security-policy-ip-3-trust-untrust] destination-zone untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-ip-subnet 10.1.1.0 24
[DeviceA-security-policy-ip-3-trust-untrust] destination-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-3-trust-untrust] action pass
[DeviceA-security-policy-ip-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name untrust-trust
[DeviceA-security-policy-ip-4-untrust-trust] source-zone untrust
[DeviceA-security-policy-ip-4-untrust-trust] destination-zone trust
[DeviceA-security-policy-ip-4-untrust-trust] source-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-4-untrust-trust] destination-ip-subnet 10.1.1.0 24
[DeviceA-security-policy-ip-4-untrust-trust] action pass
[DeviceA-security-policy-ip-4-untrust-trust] quit
[DeviceA-security-policy-ip] quit
```

(5) 定义需要保护的数据流

配置 IPv4 高级 ACL 3000，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

```
[DeviceA] ipsec transform-set transform1
[DeviceA-ipsec-transform-set-transform1] protocol esp
[DeviceA-ipsec-transform-set-transform1] esp encryption-algorithm aes-cbc-256
```

```
[DeviceA-ipsec-transform-set-transform1] esp authentication-algorithm sha256
[DeviceA-ipsec-transform-set-transform1] quit
```

(7) 配置 IKE keychain，约定通信双方使用的密钥信息

```
[DeviceA] ike keychain keychain1
[DeviceA-ike-keychain-keychain1] pre-shared-key address 2.2.2.2 255.255.0.0 key simple 123456TESTplat&!
[DeviceA-ike-keychain-keychain1] quit
```

(8) 配置 IKE 安全提议

指定加密算法、认证算法、DH、认证方法，取值要与华为防火墙的配置值严格一致。

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method pre-share
[DeviceA-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceA-ike-proposal-1] dh group14
[DeviceA-ike-proposal-1] authentication-algorithm sha256
[DeviceA-ike-proposal-1] quit
```

(9) 配置 IKE profile，约定建立 IKE SA 所需的安全参数

```
[DeviceA] ike profile profile1
[DeviceA-ike-profile-profile1] keychain keychain1
[DeviceA-ike-profile-profile1] proposal 1
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.0.0
[DeviceA-ike-profile-profile1] quit
```

(10) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条手工方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，指定对端的 IP 地址，具体配置步骤如下。

```
[DeviceA] ipsec policy policy1 1 isakmp
[DeviceA-ipsec-policy-isakmp-policy1-1] remote-address 2.2.2.2
[DeviceA-ipsec-policy-isakmp-policy1-1] transform-set transform1
[DeviceA-ipsec-policy-isakmp-policy1-1] security acl 3000
[DeviceA-ipsec-policy-isakmp-policy1-1] ike-profile profile1
[DeviceA-ipsec-policy-isakmp-policy1-1] quit
```

(11) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy policy1
[DeviceA-GigabitEthernet1/0/1] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 2.2.2.2 255.255.0.0
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.2.1，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ip route-static 10.1.1.0 24 2.2.2.1
[DeviceB] ip route-static 3.3.3.3 16 2.2.2.1
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface gigabitethernet 1/0/2
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface gigabitethernet 1/0/1
[DeviceB-zone-untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ipseclocalout
[DeviceB-policy-security-rule-ipseclocalout] source-zone local
[DeviceB-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceB-policy-security-rule-ipseclocalout] source-address 2.2.2.2 32
[DeviceB-policy-security-rule-ipseclocalout] destination-address 3.3.3.1 32
[DeviceB-policy-security-rule-ipseclocalout] action permit
[DeviceB-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-policy-security] rule name ipseclocalin
[DeviceB-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceB-policy-security-rule-ipseclocalin] destination-zone local
[DeviceB-policy-security-rule-ipseclocalin] source-address 3.3.3.1 32
[DeviceB-policy-security-rule-ipseclocalin] destination-address 2.2.2.2 32
```

```
[DeviceB-policy-security-rule-ipseclocalin] action permit
[DeviceB-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name trust-untrust
[DeviceB-policy-security-rule-trust-untrust] source-zone trust
[DeviceB-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceB-policy-security-rule-trust-untrust] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-trust-untrust] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-trust-untrust] action permit
[DeviceB-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name untrust-trust
[DeviceB-policy-security-rule-untrust-trust] source-zone untrust
[DeviceB-policy-security-rule-untrust-trust] destination-zone trust
[DeviceB-policy-security-rule-untrust-trust] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-untrust-trust] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-untrust-trust] action permit
[DeviceB-policy-security-rule-untrust-trust] quit
[DeviceB-policy-security] quit
```

(5) 定义数据流需要保护的数据流

配置一个 IPv4 高级 ACL，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。

```
[DeviceB] acl 3101
[DeviceB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
[DeviceB-acl-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceB] ipsec proposal transform1
[DeviceB-ipsec-proposal-transform1] encapsulation-mode tunnel
[DeviceB-ipsec-proposal-transform1] transform esp
[DeviceB-ipsec-proposal-transform1] esp encryption-algorithm aes-256
[DeviceB-ipsec-proposal-transform1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-transform1] quit
```

(7) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] encryption-algorithm aes-256
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] authentication-algorithm sha2-256
[DeviceB-ike-proposal-1] quit
```

(8) 配置 IKE 对等体，指定协商模式、IKE 版本、预共享密钥，对端 IP 地址。

```
[DeviceB] ike peer h3c
[DeviceB-ike-peer-h3c] exchange-mode main
[DeviceB-ike-peer-h3c] undo version 2
[DeviceB-ike-peer-h3c] ike-proposal 1
[DeviceB-ike-peer-h3c] pre-shared-key 123456TESTplat&!
[DeviceB-ike-peer-h3c] remote-address 3.3.3.1
[DeviceB-ike-peer-h3c] remote-address authentication-address 1.1.1.1
[DeviceB-ike-peer-h3c] nat traversal
[DeviceB-ike-peer-h3c] quit
```

(9) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，引用 IKE 对等体，具体配置步骤如下。

```
[DeviceB] ipsec policy use1 10 isakmp
[DeviceB-ipsec-policy-isakmp-use1-10] ike-peer h3c
[DeviceB-ipsec-policy-isakmp-use1-10] proposal transform1
[DeviceB-ipsec-policy-isakmp-use1-10] security acl 3101
[DeviceB-ipsec-policy-isakmp-use1-10] quit
```

(10) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec policy use1
[DeviceB-GigabitEthernet1/0/1] quit
```

1.4.4 验证配置

以上配置完成后，子网 10.1.1.0/24 若向子网 10.1.2.0/24 发送报文，将触发 IKE 协商。可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。

```
[DeviceA] display ike sa
    Connection-ID   Remote                Flag         DOI
-----------------------------------------------------------------
    13              2.2.2.2/500           RD           IPsec
```

```
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
[DeviceA] display ike sa verbose
   -----------------------------------------------
   Connection ID: 13
   Outside VPN:
   Inside VPN:
   Profile: profile1
   Transmitting entity: Initiator
   -----------------------------------------------
   Local IP/port: 1.1.1.1/500
   Local ID type: FQDN
   Local ID: www.devicea.com
   Remote IP/port: 2.2.2.2/500
   Remote ID type: IPV4_ADDR
   Remote ID: 2.2.2.2
   Authentication-method: PRE-SHARED-KEY
   Authentication-algorithm: SHA256
   Encryption-algorithm: AES-CBC-256
   Life duration(sec): 86400
   Remaining key duration(sec): 84565
   Exchange-mode: Aggressive
   Diffie-Hellman group: Group 1
   NAT traversal: Detected
   Extend authentication: Disabled
   Assigned IP address:
```

可通过如下显示信息查看到 IKE 第二阶段协商生成的 IPsec SA。

```
[DeviceA] display ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/1
-------------------------------
  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
```

```
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Initiator
    Path MTU: 1435
    Tunnel:
        local  address/port: 1.1.1.1/500
        remote address/port: 2.2.2.2/500
    Flow:
        sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 10.1.2.0/255.255.255.0  port: 0  protocol: ip
    [Inbound ESP SAs]
      SPI: 830667426 (0x3182faa2)
      Connection ID: 90194313219
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/2313
      Max received sequence-number:
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: Y
      Status: Active
    [Outbound ESP SAs]
      SPI: 3516214669 (0xd1952d8d)
      Connection ID: 64424509441
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/2313
      Max sent sequence-number:
      UDP encapsulation used for NAT traversal: Y
      Status: Active
```

Device B 上也会产生相应的 IPsec SA 来保护 IPv4 报文，查看方式与 Device A 同，此处略。

1.4.5 配置文件

1. Device A

```
#
interface GigabitEthernet1/0/1
```

```
 ip address 1.1.1.1 255.255.0.0
 ipsec apply policy policy1
#
interface GigabitEthernet1/0/2
 ip address 10.1.1.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1
#
 ip route-static 2.2.0.0 16 1.1.1.2
 ip route-static 10.1.2.0 24 1.1.1.2
#
acl advanced 3000
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec transform-set transform1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
ipsec policy policy1 1 isakmp
 transform-set transform1
 security acl 3000
 remote-address 2.2.2.2
 ike-profile profile1
#
ike profile profile1
 keychain keychain1
 match remote identity address 2.2.2.2 255.255.0.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
```

```
ike keychain keychain1
 pre-shared-key address 2.2.2.2 255.255.0.0 key simple 123456TESTplat&!
#
security-policy ip
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 1.1.1.1
  destination-ip-host 2.2.2.2
 rule 2 name ipseclocalin
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 2.2.2.2
  destination-ip-host 1.1.1.1
 rule 3 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
  destination-ip-subnet 10.1.2.0 255.255.255.0
 rule 4 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 10.1.2.0 255.255.255.0
  destination-ip-subnet 10.1.1.0 255.255.255.0
#
```

2. Device B

```
#
acl number 3101
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal transform1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
```

```
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer h3c
 undo version 2
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
 remote-address 3.3.3.1
 remote-address authentication-address 1.1.1.1
#
ipsec policy use1 10 isakmp
 security acl 3101
 ike-peer h3c
 proposal transform1
#
interface GigabitEthernet1/0/1
 ip address 2.2.2.2 255.255.0.0
 ipsec policy use1
#
interface GigabitEthernet1/0/2
 ip address 10.1.2.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/2
#
firewall zone untrust
 add interface GigabitEthernet1/0/1
#
ip route-static 3.3.0.0 255.255.0.0 2.2.2.1
ip route-static 10.1.1.0 255.255.255.0 2.2.2.1
#
security-policy
 rule name ipseclocalout
```

```
  source-zone local
  destination-zone untrust
  source-address 2.2.2.2 mask 255.255.255.255
  destination-address 3.3.3.1 mask 255.255.255.255
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 3.3.3.1 mask 255.255.255.255
  destination-address 2.2.2.2 mask 255.255.255.255
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
#
return
```

1.5 基于IPsec隧道接口建立保护IPv4报文的IPsec隧道配置举例

1.5.1 适用产品和版本

本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

1.5.2 组网需求

某企业分支和总部均使用固定的 IP 地址接入 Internet。现有如下组网要求：

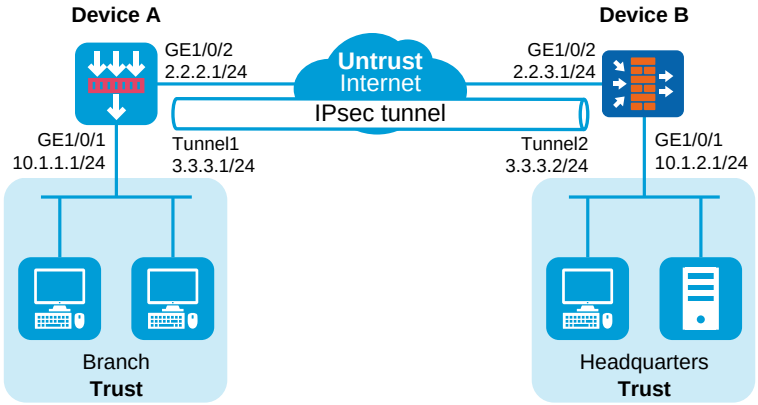
- Device B 是华为设备。
- 企业分支与企业总部之间的所有流量通过 IPsec 安全隧道进行传送。
- 当企业分支的私网 IP 地址段调整时，不需要改变企业总部网关的 IPsec 配置。

- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- IKE 协商方式建立 IPsec SA。
- IKE 协商采用预共享密钥认证方式，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。

为实现如上组网需求，可采用如下配置思路实现：

- 在 Device A 和 Device B 之间使用 IPsec 隧道接口建立 IPsec 连接，将发送给对端私网的数据流路由到 IPsec 虚拟隧道接口上，由 IPsec 虚拟隧道接口上动态协商建立的 IPsec 安全隧道对分支子网（10.1.1.0/24）与总部子网（10.1.2.0/24）之间的所有数据流进行安全保护。

图1-4 基于 IPsec 隧道建立保护 IPv4 报文的 IPsec 隧道配置组网图



1.5.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置 IPsec 隧道接口

```
[DeviceA] interface tunnel 1 mode ipsec
[DeviceA-Tunnel1] ip address 3.3.3.1 255.255.255.0
[DeviceA-Tunnel1] source 2.2.2.1
[DeviceA-Tunnel1] destination 2.2.3.1
[DeviceA-Tunnel1] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ip route-static 2.2.3.1 24 2.2.2.2
```

请根据组网图中规划的信息，配置静态路由，将需要保护的流量引入 IPsec 隧道接口，本举例的 IPsec 隧道接口为 Tunnel1，具体配置步骤如下。

```
[DeviceA] ip route-static 10.1.2.0 255.255.255.0 tunnel 1
```

(4) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Untrust] import interface tunnel 1
[DeviceA-security-zone-Untrust] quit
```

(5) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy ip
[DeviceA-security-policy-ip] rule name ipseclocalout
[DeviceA-security-policy-ip-1-ipseclocalout] source-zone local
[DeviceA-security-policy-ip-1-ipseclocalout] destination-zone untrust
[DeviceA-security-policy-ip-1-ipseclocalout] source-ip-host 2.2.2.1
[DeviceA-security-policy-ip-1-ipseclocalout] destination-ip-host 2.2.3.1
[DeviceA-security-policy-ip-1-ipseclocalout] action pass
[DeviceA-security-policy-ip-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalin
[DeviceA-security-policy-ip-2-ipseclocalin] source-zone untrust
[DeviceA-security-policy-ip-2-ipseclocalin] destination-zone local
[DeviceA-security-policy-ip-2-ipseclocalin] source-ip-host 2.2.3.1
[DeviceA-security-policy-ip-2-ipseclocalin] destination-ip-host 2.2.2.1
[DeviceA-security-policy-ip-2-ipseclocalin] action pass
[DeviceA-security-policy-ip-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host A 与 Host B 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name trust-untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-zone trust
[DeviceA-security-policy-ip-3-trust-untrust] destination-zone untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-ip-subnet 10.1.1.0 24
[DeviceA-security-policy-ip-3-trust-untrust] destination-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-3-trust-untrust] action pass
[DeviceA-security-policy-ip-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name untrust-trust
[DeviceA-security-policy-ip-4-untrust-trust] source-zone untrust
[DeviceA-security-policy-ip-4-untrust-trust] destination-zone trust
[DeviceA-security-policy-ip-4-untrust-trust] source-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-4-untrust-trust] destination-ip-subnet 10.1.1.0 24
[DeviceA-security-policy-ip-4-untrust-trust] action pass
[DeviceA-security-policy-ip-4-untrust-trust] quit
[DeviceA-security-policy-ip] quit
```

(6) 配置 IPsec 安全框架，建立 IPsec 隧道，保护需要防护的数据流

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method pre-share
[DeviceA-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceA-ike-proposal-1] dh group14
[DeviceA-ike-proposal-1] authentication-algorithm sha256
[DeviceA-ike-proposal-1] quit
[DeviceA] ike keychain abc
[DeviceA-ike-keychain-abc] pre-shared-key address 2.2.3.1 255.255.255.0 key simple
123456TESTplat&!
[DeviceA-ike-keychain-abc] quit
[DeviceA] ike profile abc
[DeviceA-ike-profile-abc] keychain abc
[DeviceA-ike-profile-abc] proposal 1
[DeviceA-ike-profile-abc] local-identity address 2.2.2.1
[DeviceA-ike-profile-abc] match remote identity address 2.2.3.1 24
[DeviceA-ike-profile-abc] exchange-mode aggressive
[DeviceA-ike-profile-abc] quit
```

```
[DeviceA] ipsec transform-set abc
[DeviceA-ipsec-transform-set-abc] esp encryption-algorithm aes-cbc-256
[DeviceA-ipsec-transform-set-abc] esp authentication-algorithm sha256
[DeviceA-ipsec-transform-set-abc] quit
[DeviceA] ipsec profile abc isakmp
[DeviceA-ipsec-profile-isakmp-abc] transform-set abc
[DeviceA-ipsec-profile-isakmp-abc] ike-profile abc
[DeviceA-ipsec-profile-isakmp-abc] quit
```

(7) 配置 IPsec 隧道接口，用于对需要保护的流量进行 IPsec 封装

```
[DeviceA] interface tunnel 1
[DeviceA-Tunnel1] tunnel protection ipsec profile abc
[DeviceA-Tunnel1] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 创建 IPsec 隧道接口

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] ip address 3.3.3.2 255.255.255.0
[DeviceB-Tunnel1] tunnel-protocol ipsec
[DeviceB-Tunnel1] source 2.2.3.1
[DeviceB-Tunnel1] destination 2.2.2.1
[DeviceB-Tunnel1] quit
```

(3) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.3.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ip route-static 2.2.2.1 24 2.2.3.2
```

请根据组网图中规划的信息，配置静态路由，将需要保护的流量引入 IPsec 隧道接口，本举例的 IPsec 隧道接口为 Tunnel1，具体配置步骤如下。

```
[DeviceA] ip route-static 10.1.1.0 255.255.255.0 tunnel 1
```

(4) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface GigabitEthernet 1/0/1
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface GigabitEthernet 1/0/2
[DeviceB-zone-untrust] add interface Tunnel 1
[DeviceB-zone-untrust] quit
```

(5) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ipseclocalout
[DeviceB-policy-security-rule-ipseclocalout] source-zone local
[DeviceB-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceB-policy-security-rule-ipseclocalout] source-address 2.2.3.1 24
[DeviceB-policy-security-rule-ipseclocalout] destination-address 2.2.2.1 24
[DeviceB-policy-security-rule-ipseclocalout] action permit
[DeviceB-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-policy-security] rule name ipseclocalin
[DeviceB-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceB-policy-security-rule-ipseclocalin] destination-zone local
[DeviceB-policy-security-rule-ipseclocalin] source-address 2.2.2.1 24
[DeviceB-policy-security-rule-ipseclocalin] destination-address 2.2.3.1 24
[DeviceB-policy-security-rule-ipseclocalin] action permit
[DeviceB-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name trust-untrust
[DeviceB-policy-security-rule-trust-untrust] source-zone trust
[DeviceB-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceB-policy-security-rule-trust-untrust] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-trust-untrust] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-trust-untrust] action permit
[DeviceB-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name untrust-trust
[DeviceB-policy-security-rule-untrust-trust] source-zone untrust
[DeviceB-policy-security-rule-untrust-trust] destination-zone trust
[DeviceB-policy-security-rule-untrust-trust] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-untrust-trust] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-untrust-trust] action permit
[DeviceB-policy-security-rule-untrust-trust] quit
[DeviceB-policy-security] quit
```

(6) 配置 IPsec 安全框架，建立 IPsec 隧道，保护需要防护的数据流

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] encryption-algorithm aes-256
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] authentication-algorithm sha2-256
[DeviceB-ike-proposal-1] quit
[DeviceB] ike peer abc
[DeviceB-ike-peer-abc] undo version 2
[DeviceB-ike-peer-abc] exchange-mode aggressive
[DeviceB-ike-peer-abc] pre-shared-key 123456TESTplat&!
[DeviceB-ike-peer-abc] ike-proposal 1
[DeviceB-ike-peer-abc] remote-address 2.2.2.1
[DeviceB-ike-peer-abc] quit
[DeviceB] ipsec proposal abc
[DeviceB-ipsec-proposal-abc] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-abc] esp encryption-algorithm aes-256
[DeviceB-ipsec-proposal-abc] quit
[DeviceB] ipsec profile abc
[DeviceB-ipsec-profile-abc] proposal abc
[DeviceB-ipsec-profile-abc] ike-peer abc
[DeviceB-ipsec-profile-abc] quit
```

(7) 配置 IPsec 隧道接口，用于对需要保护的流量进行 IPsec 封装

```
[DeviceB] interface Tunnel 1
[DeviceB-Tunnel1] ipsec profile abc
[DeviceB-Tunnel1] quit
```

1.5.4 验证配置

以上配置完成后，Device A 会自动与 Device B 进行 IKE 协商。当 IKE 协商完成后，Device A 和 Device B 上的 IPsec 虚拟隧道接口都将 up，即可以满足上述组网需求，对总部和分支的数据流进行安全保护。

通过 display ip interface brief 命令可查看接口状态如下：

```
<DeviceA> display ip interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface           Physical Protocol IP address/Mask    VPN instance Description
GE1/0/1             up       up       10.1.1.1/24        --           --
GE1/0/2             up       up       2.2.2.1/24         --           --
Tun1                up       up       3.3.3.1/24         --           --
```

通过 display interface tunnel 命令可查看隧道状态如下：

```
<DeviceA> display interface Tunnel 1
Tunnel1
Current state: UP
Line protocol state: UP
Description: Tunnel1 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1444
Internet address: 3.3.3.1/24 (primary)
Tunnel source 2.2.2.1, destination 2.2.3.1
Tunnel TTL 255
Tunnel protocol/transport IPsec/IP
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

通过 display ipsec sa 命令查看协商生成的 IPsec SA：

```
<DeviceA> display ipsec sa
-------------------------------
Interface: Tunnel1
-------------------------------
  -----------------------------
```

```
  IPsec profile: abc
  Alias: profile-abc
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Transmitting entity: Initiator
    Path MTU: 1388
    Tunnel:
        local  address/port: 2.2.2.1/500
        remote address/port: 2.2.3.1/500
    Flow:
        sour addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
        dest addr: 0.0.0.0/0.0.0.0  port: 0  protocol: ip
    [Inbound ESP SAs]
      SPI: 2701952073 (0xa10c8449)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3180
      Max received sequence-number: 0
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active
    [Outbound ESP SAs]
      SPI: 3607077598 (0xd6ffa2de)
      Connection ID: 12884901889
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/3180
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

在 Device A 上用私网地址可以 Ping 通 Device B 连接的私网地址：

```
<DeviceA> ping -a 10.1.1.1 10.1.2.1
Ping 10.1.2.1 (10.1.2.1) from 10.1.1.1: 56 data bytes, press CTRL_C to break
```

```
56 bytes from 10.1.2.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.2.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.2.1: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 10.1.2.1: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.2.1: icmp_seq=4 ttl=255 time=0.000 ms
--- Ping statistics for 10.1.2.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/1.000/0.490 ms
```

1.5.5 配置文件

1. Device A

```
#
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 2.2.2.1 255.255.255.0
#
interface Tunnel1 mode ipsec
 ip address 3.3.3.1 255.255.255.0
 source 2.2.2.1
 destination 2.2.3.1
 tunnel protection ipsec profile abc
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
 import interface Tunnel1
#
 ip route-static 2.2.3.0 24 2.2.2.2
 ip route-static 10.1.2.0 24 Tunnel1
#
ipsec transform-set abc
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
```

```
ipsec profile abc isakmp
 transform-set abc
 ike-profile abc
#
ike profile abc
 keychain abc
 exchange-mode aggressive
 local-identity address 2.2.2.1
 match remote identity address 2.2.3.1 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain abc
 pre-shared-key address 2.2.3.1 255.255.255.0 key simple 123456TESTplat&!
#
security-policy ip
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 2.2.2.1
  destination-ip-host 2.2.3.1
 rule 2 name ipseclocalin
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 2.2.3.1
  destination-ip-host 2.2.2.1
 rule 3 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
  destination-ip-subnet 10.1.2.0 255.255.255.0
```

```
 rule 4 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 10.1.2.0 255.255.255.0
  destination-ip-subnet 10.1.1.0 255.255.255.0
#
```

2. Device B

```
#
ipsec proposal abc
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
#
ike peer abc
 undo version 2
 exchange-mode aggressive
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
 remote-address 2.2.2.1
#
ipsec profile abc
 ike-peer abc
 proposal abc
#
interface GigabitEthernet1/0/1
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 2.2.3.1 255.255.255.0
#
interface Tunnel1
 ip address 3.3.3.2 255.255.255.0
```

```
 tunnel-protocol ipsec
 source 2.2.3.1
 destination 2.2.2.1
 ipsec profile abc
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/2
 add interface Tunnel1
#
ip route-static 2.2.2.0 255.255.255.0 2.2.3.2
ip route-static 10.1.1.0 255.255.255.0 Tunnel1
#
security-policy
 rule name ipseclocalout
  source-zone local
  destination-zone untrust
  source-address 2.2.3.0 mask 255.255.255.0
  destination-address 2.2.2.0 mask 255.255.255.0
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 2.2.2.0 mask 255.255.255.0
  destination-address 2.2.3.0 mask 255.255.255.0
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
```

```
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
#
```

1.6 总部采用IPsec安全策略模板方式与分支建立保护IPv4报文的IPsec隧道配置举例（分支为华为设备）

1.6.1 适用产品和版本

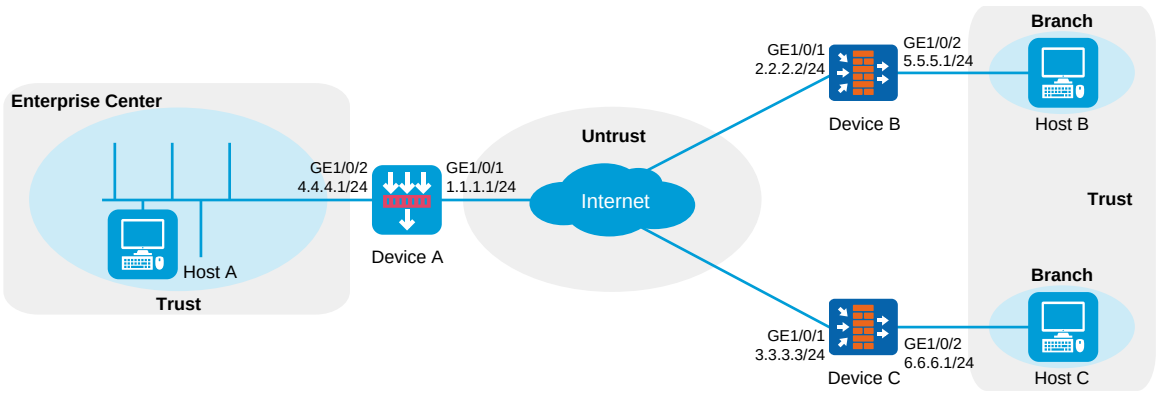
本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

1.6.2 组网需求

企业分支通过 IPsec VPN 接入企业总部，有如下具体需求：

- Device B、Device C 是华为设备。
- 总部网关 Device A 和各分支网关 Device B、Device C 之间建立 IPsec 隧道，对总部网络 4.4.4.0/24 分别与分支网络 5.5.5.0/24 和 6.6.6.0/24 之间的数据进行安全保护。
- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- IKE 协商方式建立 IPsec SA。
- IKE 协商采用预共享密钥认证方式，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- 总部网关 Device A 采用 IPsec 安全策略模板方式，分支网关 Device B 和 DeviceC 采用 IPsec 安全策略方式。

图1-5 IPsec 安全策略模板方式配置组网图



1.6.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达对端网关设备和分支网络的下一跳 IP 地址为 1.1.1.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ip route-static 2.2.2.0 24 1.1.1.2
[DeviceA] ip route-static 3.3.3.0 24 1.1.1.2
[DeviceA] ip route-static 5.5.5.0 24 1.1.1.2
[DeviceA] ip route-static 6.6.6.0 24 1.1.1.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout1 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy ip
[DeviceA-security-policy-ip] rule name ipseclocalout1
[DeviceA-security-policy-ip-0-ipseclocalout] source-zone local
[DeviceA-security-policy-ip-0-ipseclocalout] destination-zone untrust
[DeviceA-security-policy-ip-0-ipseclocalout] source-ip-host 1.1.1.1
[DeviceA-security-policy-ip-0-ipseclocalout] destination-ip-host 2.2.2.2
[DeviceA-security-policy-ip-0-ipseclocalout] action pass
[DeviceA-security-policy-ip-0-ipseclocalout] quit
```

配置名称为 ipseclocalin1 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalin1
```

```
[DeviceA-security-policy-ip-1-ipseclocalin1] source-zone untrust
[DeviceA-security-policy-ip-1-ipseclocalin1] destination-zone local
[DeviceA-security-policy-ip-1-ipseclocalin1] source-ip-host 2.2.2.2
[DeviceA-security-policy-ip-1-ipseclocalin1] destination-ip-host 1.1.1.1
[DeviceA-security-policy-ip-1-ipseclocalin1] action pass
[DeviceA-security-policy-ip-1-ipseclocalin1] quit
```

配置名称为 ipseclocalout2 的安全策规则，使 Device A 可以向 Device C 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalout2
[DeviceA-security-policy-ip-2-ipseclocalout2] source-zone local
[DeviceA-security-policy-ip-2-ipseclocalout2] destination-zone untrust
[DeviceA-security-policy-ip-2-ipseclocalout2] source-ip-host 1.1.1.1
[DeviceA-security-policy-ip-2-ipseclocalout2] destination-ip-host 3.3.3.3
[DeviceA-security-policy-ip-2-ipseclocalout2] action pass
[DeviceA-security-policy-ip-2-ipseclocalout2] quit
```

配置名称为 ipseclocalin2 的安全策略规则，使 Device A 可以接收和处理来自 Device C 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalin2
[DeviceA-security-policy-ip-3-ipseclocalin2] source-zone untrust
[DeviceA-security-policy-ip-3-ipseclocalin2] destination-zone local
[DeviceA-security-policy-ip-3-ipseclocalin2] source-ip-host 3.3.3.3
[DeviceA-security-policy-ip-3-ipseclocalin2] destination-ip-host 1.1.1.1
[DeviceA-security-policy-ip-3-ipseclocalin2] action pass
[DeviceA-security-policy-ip-3-ipseclocalin2] quit
```

b. 配置安全策略放行 Host A 与 Host B、Host C 之间的流量

配置名称为 trust-untrust1 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name trust-untrust1
[DeviceA-security-policy-ip-4-trust-untrust1] source-zone trust
[DeviceA-security-policy-ip-4-trust-untrust1] destination-zone untrust
[DeviceA-security-policy-ip-4-trust-untrust1] source-ip-subnet 4.4.4.0 24
[DeviceA-security-policy-ip-4-trust-untrust1] destination-ip-subnet 5.5.5.0 24
[DeviceA-security-policy-ip-4-trust-untrust1] action pass
[DeviceA-security-policy-ip-4-trust-untrust1] quit
```

配置名称为 untrust-trust1 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name untrust-trust1
[DeviceA-security-policy-ip-5-untrust-trust1] source-zone untrust
[DeviceA-security-policy-ip-5-untrust-trust1] destination-zone trust
```

```
[DeviceA-security-policy-ip-5-untrust-trust1] source-ip-subnet 5.5.5.0 24
[DeviceA-security-policy-ip-5-untrust-trust1] destination-ip-subnet 4.4.4.0 24
[DeviceA-security-policy-ip-5-untrust-trust1] action pass
[DeviceA-security-policy-ip-5-untrust-trust1] quit
```

配置名称为 trust-untrust2 的安全策略规则，使 Host A 访问 Host C 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name trust-untrust2
[DeviceA-security-policy-ip-6-trust-untrust2] source-zone trust
[DeviceA-security-policy-ip-6-trust-untrust2] destination-zone untrust
[DeviceA-security-policy-ip-6-trust-untrust2] source-ip-subnet 4.4.4.0 24
[DeviceA-security-policy-ip-6-trust-untrust2] destination-ip-subnet 6.6.6.0 24
[DeviceA-security-policy-ip-6-trust-untrust2] action pass
[DeviceA-security-policy-ip-6-trust-untrust2] quit
```

配置名称为 untrust-trust2 的安全策略规则，使 Host C 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name untrust-trust2
[DeviceA-security-policy-ip-7-untrust-trust2] source-zone untrust
[DeviceA-security-policy-ip-7-untrust-trust2] destination-zone trust
[DeviceA-security-policy-ip-7-untrust-trust2] source-ip-subnet 6.6.6.0 24
[DeviceA-security-policy-ip-7-untrust-trust2] destination-ip-subnet 4.4.4.0 24
[DeviceA-security-policy-ip-7-untrust-trust2] action pass
[DeviceA-security-policy-ip-7-untrust-trust2] quit
[DeviceA-security-policy-ip] quit
```

(5) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceA] ipsec transform-set transform1
[DeviceA-ipsec-transform-set-transform1] encapsulation-mode tunnel
[DeviceA-ipsec-transform-set-transform1] protocol esp
[DeviceA-ipsec-transform-set-transform1] esp encryption-algorithm aes-cbc-256
[DeviceA-ipsec-transform-set-transform1] esp authentication-algorithm sha256
[DeviceA-ipsec-transform-set-transform1] quit
```

(6) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method pre-share
[DeviceA-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceA-ike-proposal-1] dh group14
```

```
[DeviceA-ike-proposal-1] authentication-algorithm sha256
[DeviceA-ike-proposal-1] quit
```

(7) 配置 IKE keychain，约定通信双方使用的密钥信息

创建并配置名为 key1 的 IKE keychain，指定与地址为 2.2.2.2 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[DeviceA] ike keychain key1
[DeviceA-ike-keychain-key1] pre-shared-key address 2.2.2.2 255.255.255.0 key simple 123456TESTplat&!
[DeviceA-ike-keychain-key1] quit
```

创建并配置名为 key2 的 IKE keychain，指定与地址为 3.3.3.3 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[DeviceA] ike keychain key2
[DeviceA-ike-keychain-key2] pre-shared-key address 3.3.3.3 255.255.255.0 key simple 123456TESTplat&!
[DeviceA-ike-keychain-key2] quit
```

(8) 配置 IKE profile，约定建立 IKE SA 所需的安全参数。

```
[DeviceA] ike profile profile1
[DeviceA-ike-profile-profile1] keychain key1
[DeviceA-ike-profile-profile1] keychain key2
[DeviceA-ike-profile-profile1] proposal 1
[DeviceA-ike-profile-profile1] match remote identity address 2.2.2.2 255.255.255.0
[DeviceA-ike-profile-profile1] match remote identity address 3.3.3.3 255.255.255.0
[DeviceA-ike-profile-profile1] quit
```

(9) 配置 IPsec 安全策略模板，用于创建 IPsec 安全策略

创建并配置名为 temp1 的 IPsec 安全策略模板，引用安全提议 transform1

```
[DeviceA] ipsec policy-template temp1 10
[DeviceA-ipsec-policy-template-temp1-10] transform-set transform1
[DeviceA-ipsec-policy-template-temp1-10] ike-profile profile1
[DeviceA-ipsec-policy-template-temp1-10] quit
```

(10) 引用安全策略模板 temp1 创建一条 IKE 协商方式的安全策略 **map1**，建立 IPsec 隧道，保护需要防护的数据流

```
[DeviceA] ipsec policy map1 1 isakmp template temp1
```

(11) 在接口下引用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec apply policy map1
[DeviceA-GigabitEthernet1/0/1] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 2.2.2.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达对端网关设备和总部网络的下一跳 IP 地址为 2.2.2.3，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ip route-static 4.4.4.0 24 2.2.2.3
[DeviceB] ip route-static 1.1.1.1 24 2.2.2.3
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface gigabitethernet 1/0/1
[DeviceB-zone-untrust] quit
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface gigabitethernet 1/0/2
[DeviceB-zone-trust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ipseclocalout
[DeviceB-policy-security-rule-ipseclocalout] source-zone local
[DeviceB-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceB-policy-security-rule-ipseclocalout] source-address 2.2.2.2 24
[DeviceB-policy-security-rule-ipseclocalout] destination-address 1.1.1.1 24
[DeviceB-policy-security-rule-ipseclocalout] action permit
[DeviceB-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-policy-security] rule name ipseclocalin
[DeviceB-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceB-policy-security-rule-ipseclocalin] destination-zone local
```

```
[DeviceB-policy-security-rule-ipseclocalin] source-address 1.1.1.1 24
[DeviceB-policy-security-rule-ipseclocalin] destination-address 2.2.2.2 24
[DeviceB-policy-security-rule-ipseclocalin] action permit
[DeviceB-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name trust-untrust
[DeviceB-policy-security-rule-trust-untrust] source-zone trust
[DeviceB-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceB-policy-security-rule-trust-untrust] source-address 5.5.5.0 24
[DeviceB-policy-security-rule-trust-untrust] destination-address 4.4.4.0 24
[DeviceB-policy-security-rule-trust-untrust] action permit
[DeviceB-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name untrust-trust
[DeviceB-policy-security-rule-untrust-trust] source-zone untrust
[DeviceB-policy-security-rule-untrust-trust] destination-zone trust
[DeviceB-policy-security-rule-untrust-trust] source-address 4.4.4.0 24
[DeviceB-policy-security-rule-untrust-trust] destination-address 5.5.5.0 24
[DeviceB-policy-security-rule-untrust-trust] action permit
[DeviceB-policy-security-rule-untrust-trust] quit
[DeviceB-policy-security] quit
```

(5) 配置 ACL，定义需要保护的数据流

配置 IPv4 高级 ACL 3000，定义要保护由子网 5.5.5.0/24 去往子网 4.4.4.0/24 的数据流。

```
[DeviceB] acl 3000
[DeviceB-acl-adv-3000] rule permit ip source 5.5.5.0 0.0.0.255 destination 4.4.4.0
0.0.0.255
[DeviceB-acl-adv-3000] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceB-ipsec-proposal-tran1] transform esp
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256
[DeviceB-ipsec-proposal-tran1] quit
```

(7) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] encryption-algorithm aes-256
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] authentication-algorithm sha2-256
[DeviceB-ike-proposal-1] quit
```

(8) 配置 IKE 对等体，指定协商模式、IKE 版本、预共享密钥，对端 IP 地址。

```
[DeviceB] ike peer h3c
[DeviceB-ike-peer-h3c] exchange-mode main
[DeviceB-ike-peer-h3c] undo version 2
[DeviceB-ike-peer-h3c] ike-proposal 1
[DeviceB-ike-peer-h3c] pre-shared-key 123456TESTplat&!
[DeviceB-ike-peer-h3c] remote-address 1.1.1.1
[DeviceB-ike-peer-h3c] quit
```

(9) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，引用 IKE 对等体，具体配置步骤如下。

```
[DeviceB] ipsec policy use1 10 isakmp
[DeviceB-ipsec-policy-isakmp-use1-1] ike-peer h3c
[DeviceB-ipsec-policy-isakmp-use1-1] proposal tran1
[DeviceB-ipsec-policy-isakmp-use1-1] security acl 3000
[DeviceB-ipsec-policy-isakmp-use1-1] quit
```

(10) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec policy use1
[DeviceB-GigabitEthernet1/0/1] quit
```

3. 配置 Device C

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 3.3.3.3 255.255.255.0
[DeviceC-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达对端网关设备和总部网络的下一跳 IP 地址为 3.3.3.4，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceC] ip route-static 4.4.4.0 24 3.3.3.4
[DeviceC] ip route-static 1.1.1.1 24 3.3.3.4
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceC] firewall zone untrust
[DeviceC-zone-untrust] add interface gigabitethernet 1/0/1
[DeviceC-zone-untrust] quit
[DeviceC] firewall zone trust
[DeviceC-zone-trust] add interface gigabitethernet 1/0/2
[DeviceC-zone-trust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device C 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceC] security-policy
[DeviceC-policy-security] rule name ipseclocalout
[DeviceC-policy-security-rule-ipseclocalout] source-zone local
[DeviceC-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceC-policy-security-rule-ipseclocalout] source-address 3.3.3.3 24
[DeviceC-policy-security-rule-ipseclocalout] destination-address 1.1.1.1 24
[DeviceC-policy-security-rule-ipseclocalout] action permit
[DeviceC-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device C 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceC-policy-security] rule name ipseclocalin
[DeviceC-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceC-policy-security-rule-ipseclocalin] destination-zone local
[DeviceC-policy-security-rule-ipseclocalin] source-address 1.1.1.1 24
[DeviceC-policy-security-rule-ipseclocalin] destination-address 3.3.3.3 24
[DeviceC-policy-security-rule-ipseclocalin] action permit
[DeviceC-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host C 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host C 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceC-policy-security] rule name trust-untrust
[DeviceC-policy-security-rule-trust-untrust] source-zone trust
[DeviceC-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceC-policy-security-rule-trust-untrust] source-address 6.6.6.0 24
[DeviceC-policy-security-rule-trust-untrust] destination-address 4.4.4.0 24
[DeviceC-policy-security-rule-trust-untrust] action permit
[DeviceC-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host C 的报文可通，具体配置步骤如下。

```
[DeviceC-policy-security] rule name untrust-trust
[DeviceC-policy-security-rule-untrust-trust] source-zone untrust
[DeviceC-policy-security-rule-untrust-trust] destination-zone trust
[DeviceC-policy-security-rule-untrust-trust] source-address 4.4.4.0 24
[DeviceC-policy-security-rule-untrust-trust] destination-address 6.6.6.0 24
[DeviceC-policy-security-rule-untrust-trust] action permit
[DeviceC-policy-security-rule-untrust-trust] quit
[DeviceC-policy-security] quit
```

(5) 配置 ACL，定义需要保护的数据流

配置 IPv4 高级 ACL 3000，定义要保护由子网 6.6.6.0/24 去往子网 4.4.4.0/24 的数据流。

```
[DeviceC] acl 3000
[DeviceC-acl-adv-3000] rule permit ip source 6.6.6.0 0.0.0.255 destination 4.4.4.0
0.0.0.255
[DeviceC-acl-adv-3000] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceC] ipsec proposal tran1
[DeviceC-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceC-ipsec-proposal-tran1] transform esp
[DeviceC-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceC-ipsec-proposal-tran1] esp encryption-algorithm aes-256
[DeviceC-ipsec-proposal-tran1] quit
```

(7) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceC] ike proposal 1
[DeviceC-ike-proposal-1] authentication-method pre-share
[DeviceC-ike-proposal-1] encryption-algorithm aes-256
[DeviceC-ike-proposal-1] dh group14
```

```
[DeviceC-ike-proposal-1] authentication-algorithm sha2-256
[DeviceC-ike-proposal-1] quit
```

(8) 配置 IKE 对等体，指定协商模式、IKE 版本、预共享密钥，对端 IP 地址。

```
[DeviceC] ike peer h3c
[DeviceC-ike-peer-h3c] exchange-mode main
[DeviceC-ike-peer-h3c] undo version 2
[DeviceC-ike-peer-h3c] ike-proposal 1
[DeviceC-ike-peer-h3c] pre-shared-key 123456TESTplat&!
[DeviceC-ike-peer-h3c] remote-address 1.1.1.1
[DeviceC-ike-peer-h3c] quit
```

(9) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条 IKE 协商方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，引用 IKE 对等体，具体配置步骤如下。

```
[DeviceC] ipsec policy use1 10 isakmp
[DeviceC-ipsec-policy-isakmp-use1-1] ike-peer h3c
[DeviceC-ipsec-policy-isakmp-use1-1] proposal tran1
[DeviceC-ipsec-policy-isakmp-use1-1] security acl 3000
[DeviceC-ipsec-policy-isakmp-use1-1] quit
```

(10) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ipsec policy use1
[DeviceC-GigabitEthernet1/0/1] quit
```

1.6.4 验证配置

以上配置完成后，当分支子网 5.5.5.0/24 向总部网络 4.4.4.0/24 发起数据连接时，将触发 Device B 和 Device A 之间进行 IKE 协商。IKE 成功协商出 IPsec SA 后，企业总部与分支子网之间的数据流传输将受到 IPsec SA 的保护。

可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。

```
[DeviceA]display ike sa


IKE SA information :
 Conn-ID    Peer                                VPN           Flag(s)             Phase
RemoteType  RemoteID
-------------------------------------------------------------------------------------
-----------------------------------------
 2         2.2.2.2:500                                          RD|A                v1:2
IP          2.2.2.2
 1         2.2.2.2:500                                          RD|A                v1:1
IP          2.2.2.2
```

```
  Number of IKE SA : 2
-------------------------------------------------------------------------------
-----------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

可通过如下显示信息查看到 Device A 上协商生成的 IPsec SA。

```
[DeviceA]display ipsec sa

ipsec sa information:

===============================
Interface: GigabitEthernet1/0/1
===============================

  -----------------------------
  IPSec policy name: "map1"
  Sequence number  : 1
  Acl group        : 0
  Acl rule         : 0
  Mode             : Template
  -----------------------------
    Connection ID     : 2
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 17m 2s
    Tunnel local      : 1.1.1.1:500
    Tunnel remote     : 2.2.2.2:500
    Flow source       : 4.4.4.0/255.255.255.0 0/0-65535
    Flow destination  : 5.5.5.0/255.255.255.0 0/0-65535

    [Outbound ESP SAs]
      SPI: 200509728 (0xbf38920)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 10485760/2578
      Max sent sequence-number: 5
```

```
      UDP encapsulation used for NAT traversal: N
      SA encrypted packets (number/bytes): 4/336

    [Inbound ESP SAs]
      SPI: 191596935 (0xb6b8987)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 10485760/2578
      Max received sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      SA decrypted packets (number/bytes): 4/336
      Anti-replay : Enable
      Anti-replay window size: 1024
```

1.6.5 配置文件

1. Device A

```
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec apply policy map1
#
interface GigabitEthernet1/0/2
 ip address 4.4.4.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1
#
 ip route-static 2.2.2.0 24 1.1.1.2
 ip route-static 3.3.3.0 24 1.1.1.2
 ip route-static 5.5.5.0 24 1.1.1.2
 ip route-static 6.6.6.0 24 1.1.1.2
#
ipsec transform-set transform1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
```

```
ipsec policy-template temp1 10
 transform-set transform1
 ike-profile profile1
#
ipsec policy map1 1 isakmp template temp1
#
ike profile profile1
 keychain key1
 keychain key2
 match remote identity address 2.2.2.2 255.255.255.0
 match remote identity address 3.3.3.3 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain key1
 pre-shared-key address 2.2.2.2 255.255.255.0 key simple 123456TESTplat&!
#
ike keychain key2
 pre-shared-key address 3.3.3.3 255.255.255.0 key simple 123456TESTplat&!
#
security-policy ip
 rule 0 name ipseclocalout1
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 1.1.1.1
  destination-ip-host 2.2.2.2
 rule 1 name ipseclocalin1
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 2.2.2.2
  destination-ip-host 1.1.1.1
 rule 2 name ipseclocalout2
```

```
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 1.1.1.1
  destination-ip-host 3.3.3.3
 rule 3 name ipseclocalin2
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 3.3.3.3
  destination-ip-host 1.1.1.1
 rule 4 name trust-untrust1
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 4.4.4.0 255.255.255.0
  destination-ip-subnet 5.5.5.0 255.255.255.0
 rule 5 name untrust-trust1
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 5.5.5.0 255.255.255.0
  destination-ip-subnet 4.4.4.0 255.255.255.0
 rule 6 name trust-untrust2
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 4.4.4.0 255.255.255.0
  destination-ip-subnet 6.6.6.0 255.255.255.0
 rule 7 name untrust-trust2
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 6.6.6.0 255.255.255.0
  destination-ip-subnet 4.4.4.0 255.255.255.0
#
```

2. Device B

```
#
```

```
acl number 3000
 rule 5 permit ip source 5.5.5.0 0.0.0.255 destination 4.4.4.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer h3c
 undo version 2
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
 remote-address 1.1.1.1
#
ipsec policy use1 10 isakmp
 security acl 3000
 ike-peer h3c
 proposal tran1
#
interface GigabitEthernet1/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec policy use1
#
interface GigabitEthernet1/0/2
 ip address 5.5.5.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/2
#
firewall zone untrust
 add interface GigabitEthernet1/0/1
```

```
#
ip route-static 1.1.1.0 255.255.255.0 2.2.2.3
ip route-static 4.4.4.0 255.255.255.0 2.2.2.3
#
security-policy
 rule name ipseclocalout
  source-zone local
  destination-zone untrust
  source-address 2.2.2.0 mask 255.255.255.0
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 2.2.2.0 mask 255.255.255.0
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 5.5.5.0 mask 255.255.255.0
  destination-address 4.4.4.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 4.4.4.0 mask 255.255.255.0
  destination-address 5.5.5.0 mask 255.255.255.0
  action permit
#
return
```

3. Device C

```
#
acl number 3000
 rule 5 permit ip source 6.6.6.0 0.0.0.255 destination 4.4.4.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
```

```
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 authentication-method pre-share
 integrity-algorithm hmac-sha2-256
 prf hmac-sha2-256
#
ike peer h3c
 undo version 2
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
 remote-address 1.1.1.1
#
ipsec policy use1 10 isakmp
 security acl 3000
 ike-peer h3c
 proposal tran1
#
interface GigabitEthernet1/0/1
 ip address 3.3.3.3 255.255.255.0
 ipsec policy use1
#
interface GigabitEthernet1/0/2
 ip address 6.6.6.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/2
#
firewall zone untrust
 add interface GigabitEthernet1/0/1
#
ip route-static 1.1.1.0 255.255.255.0 3.3.3.4
ip route-static 4.4.4.0 255.255.255.0 3.3.3.4
#
security-policy
```

```
 rule name ipseclocalout
  source-zone local
  destination-zone untrust
  source-address 3.3.3.0 mask 255.255.255.0
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 3.3.3.0 mask 255.255.255.0
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 6.6.6.0 mask 255.255.255.0
  destination-address 4.4.4.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 4.4.4.0 mask 255.255.255.0
  destination-address 6.6.6.0 mask 255.255.255.0
  action permit
#
return
```

1.7 总部采用IPsec安全策略模板方式与分支建立保护IPv4报文的IPsec隧道配置举例（总部为华为设备）

1.7.1 适用产品和版本

本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

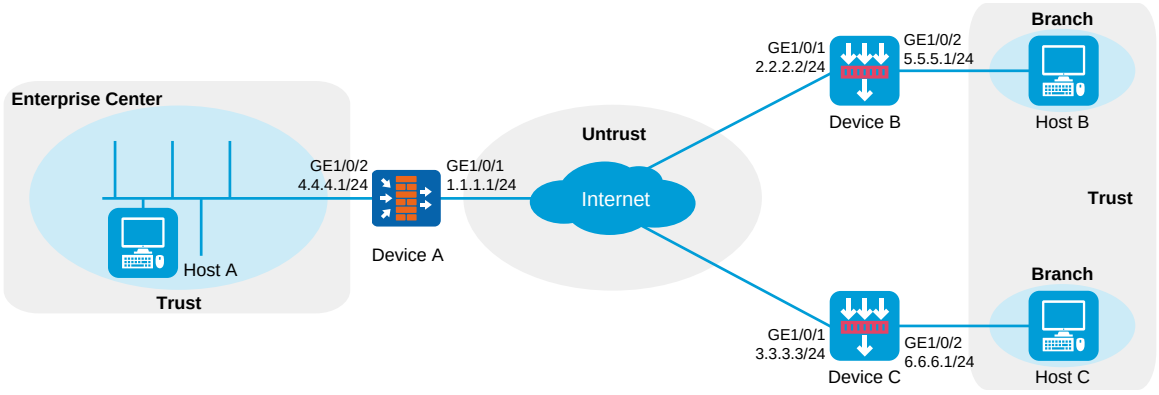
1.7.2 组网需求

企业分支通过 IPsec VPN 接入企业总部，有如下具体需求：

- Device A 是华为设备。

- 总部网关 Device A 和各分支网关 Device B、Device C 之间建立 IPsec 隧道，对总部网络 4.4.4.0/24 分别与分支网络 5.5.5.0/24 和 6.6.6.0/24 之间的数据进行安全保护。
- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- IKE 协商方式建立 IPsec SA。
- IKE 协商采用预共享密钥认证方式，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- 总部网关 Device A 采用 IPsec 安全策略模板方式，分支网关 Device B 和 DeviceC 采用 IPsec 安全策略方式。

图1-6 IPsec 安全策略模板方式配置组网图



1.7.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 1.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达对端网关设备和分支网络的下一跳 IP 地址为 1.1.1.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ip route-static 2.2.2.0 24 1.1.1.2
[DeviceA] ip route-static 3.3.3.0 24 1.1.1.2
[DeviceA] ip route-static 5.5.5.0 24 1.1.1.2
```

```
[DeviceA] ip route-static 6.6.6.0 24 1.1.1.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] firewall zone trust
[DeviceA-zone-trust] add interface gigabitethernet 1/0/2
[DeviceA-zone-trust] quit
[DeviceA] firewall zone untrust
[DeviceA-zone-untrust] add interface gigabitethernet 1/0/1
[DeviceA-zone-untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout1 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy
[DeviceA-policy-security] rule name ipseclocalout1
[DeviceA-policy-security-rule-ipseclocalout1] source-zone local
[DeviceA-policy-security-rule-ipseclocalout1] destination-zone untrust
[DeviceA-policy-security-rule-ipseclocalout1] source-address 1.1.1.1 24
[DeviceA-policy-security-rule-ipseclocalout1] destination-address 2.2.2.2 24
[DeviceA-policy-security-rule-ipseclocalout1] action permit
[DeviceA-policy-security-rule-ipseclocalout1] quit
```

配置名称为 ipseclocalin1 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-policy-security] rule name ipseclocalin1
[DeviceA-policy-security-rule-ipseclocalin1] source-zone untrust
[DeviceA-policy-security-rule-ipseclocalin1] destination-zone local
[DeviceA-policy-security-rule-ipseclocalin1] source-address 2.2.2.2 24
[DeviceA-policy-security-rule-ipseclocalin1] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-ipseclocalin1] action permit
[DeviceA-policy-security-rule-ipseclocalin1] quit
```

配置名称为 ipseclocalout2 的安全策规则，使 Device A 可以向 Device C 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-policy-security] rule name ipseclocalout2
[DeviceA-policy-security-rule-ipseclocalout2] source-zone local
[DeviceA-policy-security-rule-ipseclocalout2] destination-zone untrust
[DeviceA-policy-security-rule-ipseclocalout2] source-address 1.1.1.1 24
[DeviceA-policy-security-rule-ipseclocalout2] destination-address 3.3.3.3 24
[DeviceA-policy-security-rule-ipseclocalout2] action permit
```

```
[DeviceA-policy-security-rule-ipseclocalout2] quit
```

配置名称为 ipseclocalin2 的安全策略规则，使 Device A 可以接收和处理来自 Device C 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-policy-security] rule name ipseclocalin2
[DeviceA-policy-security-rule-ipseclocalin2] source-zone untrust
[DeviceA-policy-security-rule-ipseclocalin2] destination-zone local
[DeviceA-policy-security-rule-ipseclocalin2] source-address 3.3.3.3 24
[DeviceA-policy-security-rule-ipseclocalin2] destination-address 1.1.1.1 24
[DeviceA-policy-security-rule-ipseclocalin2] action permit
[DeviceA-policy-security-rule-ipseclocalin2] quit
```

b. 配置安全策略放行 Host A 与 Host B、Host C 之间的流量

配置名称为 trust-untrust1 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-policy-security] rule name trust-untrust1
[DeviceA-policy-security-rule-trust-untrust1] source-zone trust
[DeviceA-policy-security-rule-trust-untrust1] destination-zone untrust
[DeviceA-policy-security-rule-trust-untrust1] source-address 4.4.4.0 24
[DeviceA-policy-security-rule-trust-untrust1] destination-address 5.5.5.0 24
[DeviceA-policy-security-rule-trust-untrust1] action permit
[DeviceA-policy-security-rule-trust-untrust1] quit
```

配置名称为 untrust-trust1 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-policy-security] rule name untrust-trust1
[DeviceA-policy-security-rule-untrust-trust1] source-zone untrust
[DeviceA-policy-security-rule-untrust-trust1] destination-zone trust
[DeviceA-policy-security-rule-untrust-trust1] source-address 5.5.5.0 24
[DeviceA-policy-security-rule-untrust-trust1] destination-address 4.4.4.0 24
[DeviceA-policy-security-rule-untrust-trust1] action permit
[DeviceA-policy-security-rule-untrust-trust1] quit
```

配置名称为 trust-untrust2 的安全策略规则，使 Host A 访问 Host C 的报文可通，具体配置步骤如下。

```
[DeviceA-policy-security] rule name trust-untrust2
[DeviceA-policy-security-rule-trust-untrust2] source-zone trust
[DeviceA-policy-security-rule-trust-untrust2] destination-zone untrust
[DeviceA-policy-security-rule-trust-untrust2] source-address 4.4.4.0 24
[DeviceA-policy-security-rule-trust-untrust2] destination-address 6.6.6.0 24
[DeviceA-policy-security-rule-trust-untrust2] action permit
[DeviceA-policy-security-rule-trust-untrust2] quit
```

配置名称为 untrust-trust2 的安全策略规则，使 Host C 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-policy-security] rule name untrust-trust2
[DeviceA-policy-security-rule-untrust-trust2] source-zone untrust
[DeviceA-policy-security-rule-untrust-trust2] destination-zone trust
[DeviceA-policy-security-rule-untrust-trust2] source-address 6.6.6.0 24
[DeviceA-policy-security-rule-untrust-trust2] destination-address 4.4.4.0 24
[DeviceA-policy-security-rule-untrust-trust2] action permit
[DeviceA-policy-security-rule-untrust-trust2] quit
[DeviceA-policy-security] quit
```

(5) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceA ipsec proposal transform1
[DeviceA-ipsec-proposal-transform1] encapsulation-mode tunnel
[DeviceA-ipsec-proposal-transform1] transform esp
[DeviceA-ipsec-proposal-transform1] esp encryption-algorithm aes-256
[DeviceA-ipsec-proposal-transform1] esp authentication-algorithm sha2-256
[DeviceA-ipsec-proposal-transform1] quit
```

(6) 配置 IKE 安全提议，指定加密算法、认证算法、DH

创建并配置 IKE 安全提议，双方必须至少有一条匹配的 IKE 安全提议才能协商成功，具体配置步骤如下。

```
[DeviceA] ike proposal 1
[DeviceA-ike-proposal-1] authentication-method pre-share
[DeviceA-ike-proposal-1] encryption-algorithm aes-256
[DeviceA-ike-proposal-1] dh group14
[DeviceA-ike-proposal-1] authentication-algorithm sha2-256
[DeviceA-ike-proposal-1] quit
```

(7) 配置 IKE 对等体，指定协商模式、IKE 版本、预共享密钥，对端 IP 地址。

```
[DeviceA] ike peer h3c
[DeviceA-ike-peer-h3c] exchange-mode main
[DeviceA-ike-peer-h3c] undo version 2
[DeviceA-ike-peer-h3c] ike-proposal 1
[DeviceA-ike-peer-h3c] pre-shared-key 123456TESTplat&!
[DeviceA-ike-peer-h3c] quit
```

(8) 配置 IPsec 安全策略模板，用于创建 IPsec 安全策略

创建并配置名为 temp1 的 IPsec 安全策略模板，引用安全提议 transform1

```
[DeviceA] ipsec policy-template temp1 10
[DeviceA-ipsec-policy-templet-temp1-1] proposal transform1
```

```
[DeviceA-ipsec-policy-templet-temp1-1] ike-peer h3c
[DeviceA-ipsec-policy-templet-temp1-1] quit
```

(9) 引用安全策略模板 temp1 创建一条 IKE 协商方式的安全策略 **map1**，建立 IPsec 隧道，保护需要防护的数据流

```
[DeviceA] ipsec policy map1 1 isakmp template temp1
```

(10) 在接口下引用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ipsec policy map1
[DeviceA-GigabitEthernet1/0/1] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 2.2.2.2 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达对端网关设备和总部网络的下一跳 IP 地址为 2.2.2.3，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ip route-static 4.4.4.0 24 2.2.2.3
[DeviceB] ip route-static 1.1.1.1 24 2.2.2.3
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] security-zone name untrust
[DeviceB-security-zone-Untrust] import interface gigabitethernet 1/0/1
[DeviceB-security-zone-Untrust] quit
[DeviceB] security-zone name trust
[DeviceB-security-zone-Trust] import interface gigabitethernet 1/0/2
[DeviceB-security-zone-Trust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy ip
```

```
[DeviceB-security-policy-ip] rule name ipseclocalout
[DeviceB-security-policy-ip-1-ipseclocalout] source-zone local
[DeviceB-security-policy-ip-1-ipseclocalout] destination-zone untrust
[DeviceB-security-policy-ip-1-ipseclocalout] source-ip-host 2.2.2.2
[DeviceB-security-policy-ip-1-ipseclocalout] destination-ip-host 1.1.1.1
[DeviceB-security-policy-ip-1-ipseclocalout] action pass
[DeviceB-security-policy-ip-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-security-policy-ip] rule name ipseclocalin
[DeviceB-security-policy-ip-2-ipseclocalin] source-zone untrust
[DeviceB-security-policy-ip-2-ipseclocalin] destination-zone local
[DeviceB-security-policy-ip-2-ipseclocalin] source-ip-host 1.1.1.1
[DeviceB-security-policy-ip-2-ipseclocalin] destination-ip-host 2.2.2.2
[DeviceB-security-policy-ip-2-ipseclocalin] action pass
[DeviceB-security-policy-ip-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-security-policy-ip] rule name trust-untrust
[DeviceB-security-policy-ip-3-trust-untrust] source-zone trust
[DeviceB-security-policy-ip-3-trust-untrust] destination-zone untrust
[DeviceB-security-policy-ip-3-trust-untrust] source-ip-subnet 5.5.5.0 24
[DeviceB-security-policy-ip-3-trust-untrust] destination-ip-subnet 4.4.4.0 24
[DeviceB-security-policy-ip-3-trust-untrust] action pass
[DeviceB-security-policy-ip-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-security-policy-ip] rule name untrust-trust
[DeviceB-security-policy-ip-4-untrust-trust] source-zone untrust
[DeviceB-security-policy-ip-4-untrust-trust] destination-zone trust
[DeviceB-security-policy-ip-4-untrust-trust] source-ip-subnet 4.4.4.0 24
[DeviceB-security-policy-ip-4-untrust-trust] destination-ip-subnet 5.5.5.0 24
[DeviceB-security-policy-ip-4-untrust-trust] action pass
[DeviceB-security-policy-ip-4-untrust-trust] quit
[DeviceB-security-policy-ip] quit
```

(5) 配置 ACL，定义需要保护的数据流

配置 IPv4 高级 ACL 3000，定义要保护由子网 5.5.5.0/24 去往子网 4.4.4.0/24 的数据流。

```
[DeviceB] acl advanced 3000
[DeviceB-acl-ipv4-adv-3000] rule permit ip source 5.5.5.0 0.0.0.255 destination 4.4.4.0
0.0.0.255
[DeviceB-acl-ipv4-adv-3000] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceB] ipsec transform-set tran1
[DeviceB-ipsec-transform-set-tran1] encapsulation-mode tunnel
[DeviceB-ipsec-transform-set-tran1] protocol esp
[DeviceB-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-256
[DeviceB-ipsec-transform-set-tran1] esp authentication-algorithm sha256
[DeviceB-ipsec-transform-set-tran1] quit
```

(7) 配置 IKE keychain，约定通信双方使用的密钥信息

创建并配置名为 key1 的 IKE keychain，指定与地址为 1.1.1.1 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[DeviceB] ike keychain key1
[DeviceB-ike-keychain-key1] pre-shared-key address 1.1.1.1 key simple 123456TESTplat&!
[DeviceB-ike-keychain-key1] quit
```

(8) 配置 IKE 提议，定义双方进行 IKE 协商所需的安全参数

创建并配置 IKE 提议 1，指定预共享密钥认证方式、加密算法、认证算法。

```
[DeviceB] ike proposal 1
[DeviceB-ike-proposal-1] authentication-method pre-share
[DeviceB-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceB-ike-proposal-1] dh group14
[DeviceB-ike-proposal-1] authentication-algorithm sha256
[DeviceB-ike-proposal-1] quit
```

(9) 配置 IKE profile，约定建立 IKE SA 所需的安全参数

```
[DeviceB] ike profile profile1
[DeviceB-ike-profile-profile1] keychain key1
[DeviceB-ike-profile-profile1] proposal 1
[DeviceB-ike-profile-profile1] match remote identity address 1.1.1.1 255.255.255.0
[DeviceB-ike-profile-profile1] quit
```

(10) 配置 ISAKMP 方式的安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建并配置名为 map1 的 IPsec 安全策略，引用安全提议 tran1，引用 ACL 3000，并指定 IPsec 隧道的对端地址为 1.1.1.1。

```
[DeviceB] ipsec policy map1 10 isakmp
[DeviceB-ipsec-policy-isakmp-map1-10] transform-set tran1
[DeviceB-ipsec-policy-isakmp-map1-10] security acl 3000
```

```
[DeviceB-ipsec-policy-isakmp-map1-10] local-address 2.2.2.2
[DeviceB-ipsec-policy-isakmp-map1-10] remote-address 1.1.1.1
[DeviceB-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceB-ipsec-policy-isakmp-map1-10] quit
```

(11) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ipsec apply policy map1
[DeviceB-GigabitEthernet1/0/1] quit
```

3. 配置 Device C

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceC> system-view
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ip address 3.3.3.3 255.255.255.0
[DeviceC-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设到达对端网关设备和总部网络的下一跳 IP 地址为 3.3.3.4，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceC] ip route-static 4.4.4.0 24 3.3.3.4
[DeviceC] ip route-static 1.1.1.1 24 3.3.3.4
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceC] security-zone name untrust
[DeviceC-security-zone-Untrust] import interface gigabitethernet 1/0/1
[DeviceC-security-zone-Untrust] quit
[DeviceC] security-zone name trust
[DeviceC-security-zone-Trust] import interface gigabitethernet 1/0/2
[DeviceC-security-zone-Trust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device C 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceC] security-policy ip
[DeviceC-security-policy-ip] rule name ipseclocalout
```

```
[DeviceC-security-policy-ip-1-ipseclocalout] source-zone local
[DeviceC-security-policy-ip-1-ipseclocalout] destination-zone untrust
[DeviceC-security-policy-ip-1-ipseclocalout] source-ip-host 3.3.3.3
[DeviceC-security-policy-ip-1-ipseclocalout] destination-ip-host 1.1.1.1
[DeviceC-security-policy-ip-1-ipseclocalout] action pass
[DeviceC-security-policy-ip-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device C 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceC-security-policy-ip] rule name ipseclocalin
[DeviceC-security-policy-ip-2-ipseclocalin] source-zone untrust
[DeviceC-security-policy-ip-2-ipseclocalin] destination-zone local
[DeviceC-security-policy-ip-2-ipseclocalin] source-ip-host 1.1.1.1
[DeviceC-security-policy-ip-2-ipseclocalin] destination-ip-host 3.3.3.3
[DeviceC-security-policy-ip-2-ipseclocalin] action pass
[DeviceC-security-policy-ip-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host C 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host C 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceC-security-policy-ip] rule name trust-untrust
[DeviceC-security-policy-ip-3-trust-untrust] source-zone trust
[DeviceC-security-policy-ip-3-trust-untrust] destination-zone untrust
[DeviceC-security-policy-ip-3-trust-untrust] source-ip-subnet 6.6.6.0 24
[DeviceC-security-policy-ip-3-trust-untrust] destination-ip-subnet 4.4.4.0 24
[DeviceC-security-policy-ip-3-trust-untrust] action pass
[DeviceC-security-policy-ip-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host C 的报文可通，具体配置步骤如下。

```
[DeviceC-security-policy-ip] rule name untrust-trust
[DeviceC-security-policy-ip-4-untrust-trust] source-zone untrust
[DeviceC-security-policy-ip-4-untrust-trust] destination-zone trust
[DeviceC-security-policy-ip-4-untrust-trust] source-ip-subnet 4.4.4.0 24
[DeviceC-security-policy-ip-4-untrust-trust] destination-ip-subnet 6.6.6.0 24
[DeviceC-security-policy-ip-4-untrust-trust] action pass
[DeviceC-security-policy-ip-4-untrust-trust] quit
[DeviceC-security-policy-ip] quit
```

(5) 配置 ACL，定义需要保护的数据流

配置 IPv4 高级 ACL 3000，定义要保护由子网 6.6.6.0/24 去往子网 4.4.4.0/24 的数据流。

```
[DeviceC] acl advanced 3000
```

```
[DeviceC-acl-ipv4-adv-3000] rule permit ip source 6.6.6.0 0.0.0.255 destination 4.4.4.0
0.0.0.255
[DeviceC-acl-ipv4-adv-3000] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceC] ipsec transform-set tran1
[DeviceC-ipsec-transform-set-tran1] encapsulation-mode tunnel
[DeviceC-ipsec-transform-set-tran1] protocol esp
[DeviceC-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-256
[DeviceC-ipsec-transform-set-tran1] esp authentication-algorithm sha256
[DeviceC-ipsec-transform-set-tran1] quit
```

(7) 配置 IKE keychain，约定通信双方使用的密钥信息

创建并配置名为 key1 的 IKE keychain，指定与地址为 1.1.1.1 的对端使用的预共享密钥为明文 123456TESTplat&!。

```
[DeviceC] ike keychain key1
[DeviceC-ike-keychain-key1] pre-shared-key address 1.1.1.1 key simple 123456TESTplat&!
[DeviceC-ike-keychain-key1] quit
```

(8) 配置 IKE 提议，定义双方进行 IKE 协商所需的安全参数

创建并配置 IKE 提议 1，指定预共享密钥认证方式、加密算法、认证算法。

```
[DeviceC] ike proposal 1
[DeviceC-ike-proposal-1] authentication-method pre-share
[DeviceC-ike-proposal-1] encryption-algorithm aes-cbc-256
[DeviceC-ike-proposal-1] dh group14
[DeviceC-ike-proposal-1] authentication-algorithm sha256
[DeviceC-ike-proposal-1] quit
```

(9) 配置 IKE profile，约定建立 IKE SA 所需的安全参数

```
[DeviceC] ike profile profile1
[DeviceC-ike-profile-profile1] keychain key1
[DeviceC-ike-profile-profile1] proposal 1
[DeviceC-ike-profile-profile1] match remote identity address 1.1.1.1 255.255.255.0
[DeviceC-ike-profile-profile1] quit
```

(10) 配置 ISAKMP 方式的安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建并配置名为 map1 的 IPsec 安全策略，引用安全提议 tran1，引用 ACL 3000，并指定 IPsec 隧道的对端地址为 1.1.1.1。

```
[DeviceC] ipsec policy map1 10 isakmp
[DeviceC-ipsec-policy-isakmp-map1-10] transform-set tran1
[DeviceC-ipsec-policy-isakmp-map1-10] security acl 3000
[DeviceC-ipsec-policy-isakmp-map1-10] local-address 3.3.3.3
```

```
[DeviceC-ipsec-policy-isakmp-map1-10] remote-address 1.1.1.1
[DeviceC-ipsec-policy-isakmp-map1-10] ike-profile profile1
[DeviceC-ipsec-policy-isakmp-map1-10] quit
```

(11) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] ipsec apply policy map1
[DeviceC-GigabitEthernet1/0/1] quit
```

1.7.4 验证配置

以上配置完成后，当分支子网 5.5.5.0/24 向总部网络 4.4.4.0/24 发起数据连接时，将触发 Device B 和 Device A 之间进行 IKE 协商。IKE 成功协商出 IPsec SA 后，企业总部与分支子网之间的数据流传输将受到 IPsec SA 的保护。

可通过如下显示信息查看到 Device A 上 IKE 第一阶段协商成功后生成的 IKE SA。

```
[DeviceA]display ike sa

IKE SA information :
 Conn-ID   Peer                                VPN           Flag(s)            Phase
RemoteType  RemoteID
-------------------------------------------------------------------------------------
-----------------------------------------
 2        2.2.2.2:500                                        RD|A               v1:2
IP          2.2.2.2
 1        2.2.2.2:500                                        RD|A               v1:1
IP          2.2.2.2

  Number of IKE SA : 2
-------------------------------------------------------------------------------------
-----------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

可通过如下显示信息查看到 Device A 上协商生成的 IPsec SA。

```
[DeviceA]display ipsec sa

ipsec sa information:

==============================
```

```
Interface: GigabitEthernet1/0/1
================================


  ----------------------------
  IPSec policy name: "map1"
  Sequence number  : 1
  Acl group        : 0
  Acl rule         : 0
  Mode             : Template
  ----------------------------
    Connection ID     : 2
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 17m 2s
    Tunnel local      : 1.1.1.1:500
    Tunnel remote     : 2.2.2.2:500
    Flow source       : 4.4.4.0/255.255.255.0 0/0-65535
    Flow destination  : 5.5.5.0/255.255.255.0 0/0-65535

    [Outbound ESP SAs]
      SPI: 200509728 (0xbf38920)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 10485760/2578
      Max sent sequence-number: 5
      UDP encapsulation used for NAT traversal: N
      SA encrypted packets (number/bytes): 4/336

    [Inbound ESP SAs]
      SPI: 191596935 (0xb6b8987)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
      SA remaining key duration (kilobytes/sec): 10485760/2578
      Max received sequence-number: 1
      UDP encapsulation used for NAT traversal: N
      SA decrypted packets (number/bytes): 4/336
      Anti-replay : Enable
      Anti-replay window size: 1024
```

1.7.5 配置文件

1. Device A

```
#
ipsec proposal transform1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
#
ike peer h3c
 undo version 2
 pre-shared-key 123456TESTplat&!
 ike-proposal 1
#
ipsec policy-template temp1 10
 ike-peer h3c
 proposal transform1
#
ipsec policy map1 1 isakmp template temp1
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
interface GigabitEthernet1/0/2
 ip address 4.4.4.1 255.255.255.0
#
firewall zone trust
 add interface GigabitEthernet1/0/2
#
firewall zone untrust
 add interface GigabitEthernet1/0/1
#
ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
```

```
ip route-static 3.3.3.0 255.255.255.0 1.1.1.2
ip route-static 5.5.5.0 255.255.255.0 1.1.1.2
ip route-static 6.6.6.0 255.255.255.0 1.1.1.2
#
security-policy
 rule name ipseclocalout1
  source-zone local
  destination-zone untrust
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 2.2.2.0 mask 255.255.255.0
  action permit
 rule name ipseclocalin1
  source-zone untrust
  destination-zone local
  source-address 2.2.2.0 mask 255.255.255.0
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name ipseclocalout2
  source-zone local
  destination-zone untrust
  source-address 1.1.1.0 mask 255.255.255.0
  destination-address 3.3.3.0 mask 255.255.255.0
  action permit
 rule name ipseclocalin2
  source-zone untrust
  destination-zone local
  source-address 3.3.3.0 mask 255.255.255.0
  destination-address 1.1.1.0 mask 255.255.255.0
  action permit
 rule name trust-untrust1
  source-zone trust
  destination-zone untrust
  source-address 4.4.4.0 mask 255.255.255.0
  destination-address 5.5.5.0 mask 255.255.255.0
  action permit
 rule name untrust-trust1
  source-zone untrust
  destination-zone trust
```

```
  source-address 5.5.5.0 mask 255.255.255.0
  destination-address 4.4.4.0 mask 255.255.255.0
  action permit
 rule name trust-untrust2
  source-zone trust
  destination-zone untrust
  source-address 4.4.4.0 mask 255.255.255.0
  destination-address 6.6.6.0 mask 255.255.255.0
  action permit
 rule name untrust-trust2
  source-zone untrust
  destination-zone trust
  source-address 6.6.6.0 mask 255.255.255.0
  destination-address 4.4.4.0 mask 255.255.255.0
  action permit
#
```

2. Device B

```
#
interface GigabitEthernet1/0/1
 ip address 2.2.2.2 255.255.255.0
 ipsec apply policy map1
#
interface GigabitEthernet1/0/2
 ip address 5.5.5.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1
#
 ip route-static 1.1.1.0 24 2.2.2.3
 ip route-static 4.4.4.0 24 2.2.2.3
#
acl advanced 3000
 rule 0 permit ip source 5.5.5.0 0.0.0.255 destination 4.4.4.0 0.0.0.255
#
ipsec transform-set tran1
```

```
 encapsulation-mode tunnel
 protocol esp
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3000
 local-address 2.2.2.2
 remote-address 1.1.1.1
 ike-profile profile1
#
ike profile profile1
 keychain key1
 match remote identity address 1.1.1.1 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain key1
 pre-shared-key address 1.1.1.1 255.255.255.255 key simple 123456TESTplat&!
#
security-policy ip
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 2.2.2.2
  destination-ip-host 1.1.1.1
 rule 2 name ipseclocalin
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 1.1.1.1
  destination-ip-host 2.2.2.2
```

```
 rule 3 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 5.5.5.0 255.255.255.0
  destination-ip-subnet 4.4.4.0 255.255.255.0
 rule 4 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 4.4.4.0 255.255.255.0
  destination-ip-subnet 5.5.5.0 255.255.255.0
#
```

3. Device C

```
#
interface GigabitEthernet1/0/1
 ip address 3.3.3.3 255.255.255.0
 ipsec apply policy map1
#
interface GigabitEthernet1/0/2
 ip address 6.6.6.1 255.255.255.0
#
security-zone name Trust
 import interface GigabitEthernet1/0/2
#
security-zone name Untrust
 import interface GigabitEthernet1/0/1
#
 ip route-static 1.1.1.0 24 3.3.3.4
 ip route-static 4.4.4.0 24 3.3.3.4
#
acl advanced 3000
 rule 0 permit ip source 6.6.6.0 0.0.0.255 destination 4.4.4.0 0.0.0.255
#
ipsec transform-set tran1
 encapsulation-mode tunnel
 protocol esp
 esp encryption-algorithm aes-cbc-256
```

```
 esp authentication-algorithm sha256
#
ipsec policy map1 10 isakmp
 transform-set tran1
 security acl 3000
 local-address 3.3.3.3
 remote-address 1.1.1.1
 ike-profile profile1
#
ike profile profile1
 keychain key1
 match remote identity address 1.1.1.1 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group14
 authentication-algorithm sha256
#
ike keychain key1
 pre-shared-key address 1.1.1.1 255.255.255.255 key simple 123456TESTplat&!
#
security-policy ip
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 3.3.3.3
  destination-ip-host 1.1.1.1
 rule 2 name ipseclocalin
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 1.1.1.1
  destination-ip-host 3.3.3.3
 rule 3 name trust-untrust
  action pass
  source-zone trust
```

```
 destination-zone untrust
 source-ip-subnet 6.6.6.0 255.255.255.0
 destination-ip-subnet 4.4.4.0 255.255.255.0
rule 4 name untrust-trust
 action pass
 source-zone untrust
 destination-zone trust
 source-ip-subnet 4.4.4.0 255.255.255.0
 destination-ip-subnet 6.6.6.0 255.255.255.0
#
```

1.8 网关与网关之间采用手工方式建立保护IPv4报文的IPsec隧道配置举例

1.8.1 适用产品和版本

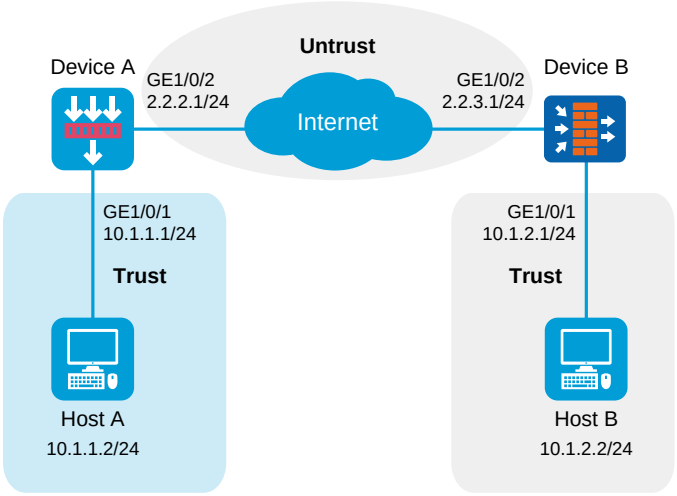
本举例是在 H3C 防火墙 F5000-AI160 的 E8371 版本，华为防火墙 USG6600E 的 V600R007C20SPC500 版本上进行配置和验证的。

1.8.2 组网需求

在 Device A 和 Device B 之间建立一条 IPsec 隧道，对 Host A 所在的子网（10.1.1.0/24）与 Host B 所在的子网（10.1.2.0/24）之间的数据流进行安全保护。具体要求如下：

- Device B 是华为设备。
- 封装形式为隧道模式。
- 安全协议采用 ESP 协议，加密算法采用 256 比特 CBC 模式的 AES 算法，认证算法采用 256 比特的 HMAC-SHA-256 算法。
- 手工方式建立 IPsec SA。

图1-7 保护 IPv4 报文的 IPsec 配置组网图



1.8.3 配置步骤

1. 配置 Device A

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 255.255.255.0
[DeviceA-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.2.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceA] ip route-static 10.1.2.0 24 2.2.2.2
[DeviceA] ip route-static 2.2.3.1 24 2.2.2.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceA] security-zone name trust
[DeviceA-security-zone-Trust] import interface gigabitethernet 1/0/1
[DeviceA-security-zone-Trust] quit
[DeviceA] security-zone name untrust
[DeviceA-security-zone-Untrust] import interface gigabitethernet 1/0/2
[DeviceA-security-zone-Untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device A 可以向 Device B 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA] security-policy ip
[DeviceA-security-policy-ip] rule name ipseclocalout
[DeviceA-security-policy-ip-1-ipseclocalout] source-zone local
[DeviceA-security-policy-ip-1-ipseclocalout] destination-zone untrust
[DeviceA-security-policy-ip-1-ipseclocalout] source-ip-host 2.2.2.1
[DeviceA-security-policy-ip-1-ipseclocalout] destination-ip-host 2.2.3.1
[DeviceA-security-policy-ip-1-ipseclocalout] action pass
[DeviceA-security-policy-ip-1-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device A 可以接收和处理来自 Device B 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name ipseclocalin
[DeviceA-security-policy-ip-2-ipseclocalin] source-zone untrust
[DeviceA-security-policy-ip-2-ipseclocalin] destination-zone local
[DeviceA-security-policy-ip-2-ipseclocalin] source-ip-host 2.2.3.1
[DeviceA-security-policy-ip-2-ipseclocalin] destination-ip-host 2.2.2.1
[DeviceA-security-policy-ip-2-ipseclocalin] action pass
[DeviceA-security-policy-ip-2-ipseclocalin] quit
```

b. 配置安全策略放行 Host A 与 Host B 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name trust-untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-zone trust
[DeviceA-security-policy-ip-3-trust-untrust] destination-zone untrust
[DeviceA-security-policy-ip-3-trust-untrust] source-ip-subnet 10.1.1.0 24
[DeviceA-security-policy-ip-3-trust-untrust] destination-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-3-trust-untrust] action pass
[DeviceA-security-policy-ip-3-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceA-security-policy-ip] rule name untrust-trust
[DeviceA-security-policy-ip-4-untrust-trust] source-zone untrust
[DeviceA-security-policy-ip-4-untrust-trust] destination-zone trust
[DeviceA-security-policy-ip-4-untrust-trust] source-ip-subnet 10.1.2.0 24
[DeviceA-security-policy-ip-4-untrust-trust] destination-ip-subnet 10.1.1.0 24
```

```
[DeviceA-security-policy-ip-4-untrust-trust] action pass
[DeviceA-security-policy-ip-4-untrust-trust] quit
[DeviceA-security-policy-ip] quit
```

(5) 定义需要保护的数据流

配置一个 IPv4 高级 ACL，定义要保护由子网 10.1.1.0/24 去往子网 10.1.2.0/24 的数据流。

```
[DeviceA] acl advanced 3101
[DeviceA-acl-ipv4-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[DeviceA-acl-ipv4-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceA] ipsec transform-set tran1
[DeviceA-ipsec-transform-set-tran1] encapsulation-mode tunnel
[DeviceA-ipsec-transform-set-tran1] protocol esp
[DeviceA-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-256
[DeviceA-ipsec-transform-set-tran1] esp authentication-algorithm sha256
[DeviceA-ipsec-transform-set-tran1] quit
```

(7) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条手工方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，指定对端的 IP 地址，具体配置步骤如下。

```
[DeviceA] ipsec policy map1 10 manual
[DeviceA-ipsec-policy-manual-map1-10] security acl 3101
[DeviceA-ipsec-policy-manual-map1-10] transform-set tran1
[DeviceA-ipsec-policy-manual-map1-10] remote-address 2.2.3.1
[DeviceA-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[DeviceA-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
[DeviceA-ipsec-policy-manual-map1-10] sa string-key outbound esp simple abcdefg
[DeviceA-ipsec-policy-manual-map1-10] sa string-key inbound esp simple gfedcba
[DeviceA-ipsec-policy-manual-map1-10] quit
```

(8) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

在接口 GigabitEthernet1/0/2 上应用 IPsec 安全策略，具体配置步骤如下。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] ipsec apply policy map1
[DeviceA-GigabitEthernet1/0/2] quit
```

2. 配置 Device B

(1) 配置接口 IP 地址

根据组网图中规划的信息，配置各接口的 IP 地址，具体配置步骤如下。

```
<DeviceB> system-view
```

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.2.1 255.255.255.0
[DeviceB-GigabitEthernet1/0/1] quit
```

请参考以上步骤配置其他接口的 IP 地址，具体配置步骤略。

(2) 配置静态路由

本举例仅以静态路由方式配置路由信息。实际组网中，请根据具体情况选择相应的路由配置方式。

请根据组网图中规划的信息，配置静态路由，本举例假设下一跳 IP 地址为 2.2.3.2，实际使用中请以具体组网情况为准，具体配置步骤如下。

```
[DeviceB] ip route-static 10.1.1.0 24 2.2.3.2
[DeviceB] ip route-static 2.2.2.1 24 2.2.3.2
```

(3) 配置接口加入安全域。

请根据组网图中规划的信息，将接口加入对应的安全域，具体配置步骤如下。

```
[DeviceB] firewall zone trust
[DeviceB-zone-trust] add interface gigabitethernet 1/0/1
[DeviceB-zone-trust] quit
[DeviceB] firewall zone untrust
[DeviceB-zone-untrust] add interface gigabitethernet 1/0/2
[DeviceB-zone-untrust] quit
```

(4) 配置安全策略

a. 配置安全策略放行 Untrust 与 Local 安全域之间的流量，用于设备之间可以建立 IPsec 隧道。

配置名称为 ipseclocalout 的安全策规则，使 Device B 可以向 Device A 发送 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB] security-policy
[DeviceB-policy-security] rule name ipseclocalout
[DeviceB-policy-security-rule-ipseclocalout] source-zone local
[DeviceB-policy-security-rule-ipseclocalout] destination-zone untrust
[DeviceB-policy-security-rule-ipseclocalout] source-address 2.2.3.1 32
[DeviceB-policy-security-rule-ipseclocalout] destination-address 2.2.2.1 32
[DeviceB-policy-security-rule-ipseclocalout] action permit
[DeviceB-policy-security-rule-ipseclocalout] quit
```

配置名称为 ipseclocalin 的安全策略规则，使 Device B 可以接收和处理来自 Device A 的 IPsec 隧道协商报文，具体配置步骤如下。

```
[DeviceB-policy-security] rule name ipseclocalin
[DeviceB-policy-security-rule-ipseclocalin] source-zone untrust
[DeviceB-policy-security-rule-ipseclocalin] destination-zone local
[DeviceB-policy-security-rule-ipseclocalin] source-address 2.2.2.1 32
[DeviceB-policy-security-rule-ipseclocalin] destination-address 2.2.3.1 32
```

```
[DeviceB-policy-security-rule-ipseclocalin] action permit
[DeviceB-policy-security-rule-ipseclocalin] quit
```

b. 配置安全策略放行 Host B 与 Host A 之间的流量

配置名称为 trust-untrust 的安全策略规则，使 Host B 访问 Host A 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name trust-untrust
[DeviceB-policy-security-rule-trust-untrust] source-zone trust
[DeviceB-policy-security-rule-trust-untrust] destination-zone untrust
[DeviceB-policy-security-rule-trust-untrust] source-address 10.1.2.0 24
[DeviceB-policy-security-rule-trust-untrust] destination-address 10.1.1.0 24
[DeviceB-policy-security-rule-trust-untrust] action permit
[DeviceB-policy-security-rule-trust-untrust] quit
```

配置名称为 untrust-trust 的安全策略规则，使 Host A 访问 Host B 的报文可通，具体配置步骤如下。

```
[DeviceB-policy-security] rule name untrust-trust
[DeviceB-policy-security-rule-untrust-trust] source-zone untrust
[DeviceB-policy-security-rule-untrust-trust] destination-zone trust
[DeviceB-policy-security-rule-untrust-trust] source-address 10.1.1.0 24
[DeviceB-policy-security-rule-untrust-trust] destination-address 10.1.2.0 24
[DeviceB-policy-security-rule-untrust-trust] action permit
[DeviceB-policy-security-rule-untrust-trust] quit
[DeviceB-policy-security] quit
```

(5) 定义需要保护的数据流

配置一个 IPv4 高级 ACL，定义要保护由子网 10.1.2.0/24 去往子网 10.1.1.0/24 的数据流。

```
[DeviceB] acl 3101
[DeviceB-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0
0.0.0.255
[DeviceB-acl-adv-3101] quit
```

(6) 配置 IPsec 安全提议，协商封装报文使用的各种安全协议

创建 IPsec 安全提议，两端配置的安全提议参数需要完全相同，具体配置步骤如下。

```
[DeviceB] ipsec proposal tran1
[DeviceB-ipsec-proposal-tran1] encapsulation-mode tunnel
[DeviceB-ipsec-proposal-tran1] transform esp
[DeviceB-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[DeviceB-ipsec-proposal-tran1] esp encryption-algorithm aes-256
[DeviceB-ipsec-proposal-tran1] quit
```

(7) 配置 IPsec 安全策略，建立 IPsec 隧道，保护需要防护的数据流

创建一条手工方式的 IPsec 安全策略，引用需要保护数据流的 ACL 和所需的 IPsec 安全提议，指定本端和对端的 IP 地址，具体配置步骤如下。

```
[DeviceB] ipsec policy use1 10 manual
[DeviceB-ipsec-policy-manual-use1-10] security acl 3101
[DeviceB-ipsec-policy-manual-use1-10] proposal tran1
[DeviceB-ipsec-policy-manual-use1-10] tunnel remote 2.2.2.1
[DeviceB-ipsec-policy-manual-use1-10] tunnel local 2.2.3.1
[DeviceB-ipsec-policy-manual-use1-10] sa spi inbound esp 12345
[DeviceB-ipsec-policy-manual-use1-10] sa spi outbound esp 54321
[DeviceB-ipsec-policy-manual-use1-10] sa string-key inbound esp abcdefg
[DeviceB-ipsec-policy-manual-use1-10] sa string-key outbound esp gfedcba
[DeviceB-ipsec-policy-manual-use1-10] quit
```

(8) 在接口上应用 IPsec 安全策略，对接口上的流量进行保护

在接口 GigabitEthernet1/0/2 上应用 IPsec 安全策略，具体配置步骤如下。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ipsec policy use1
[DeviceB-GigabitEthernet1/0/2] quit
```

1.8.4 验证配置

以上配置完成后，Device A 和 Device B 之间的 IPsec 隧道就建立好了，子网 10.1.1.0/24 与子网 10.1.2.0/24 之间数据流的传输将受到生成的 IPsec SA 的保护。可通过以下显示查看 Device A 上手工创建的 IPsec SA。

```
[DeviceA] display ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/2
-------------------------------
  -----------------------------
  IPsec policy: map1
  Sequence number: 10
  Alisa: map1-10
  Mode: Manual
  -----------------------------
    Tunnel id: 549
    Encapsulation mode: tunnel
    Path MTU: 1443
    Tunnel:
        local  address/port: 2.2.2.1/0
        remote address/port: 2.2.3.1/0
```

```
    Flow:
        as defined in ACL 3101
    [Inbound ESP SA]
      SPI: 54321 (0x0000d431)
      Connection ID: 1
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      No duration limit for this SA
    [Outbound ESP SA]
      SPI: 12345 (0x00003039)
      Connection ID: 2
      Transform set: ESP-ENCRYPT-AES-CBC-256 ESP-AUTH-SHA256
      No duration limit for this SA
```

Device B 上也会产生相应的 IPsec SA 来保护 IPv4 报文，查看方式与 Device A 同，此处略。

1.8.5 配置文件

1. Device A

```
#
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 2.2.2.1 255.255.255.0
 ipsec apply policy map1
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
#
security-zone name Untrust
 import interface GigabitEthernet1/0/2
#
 ip route-static 2.2.3.0 24 2.2.2.2
 ip route-static 10.1.2.0 24 2.2.2.2
#
acl advanced 3101
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec transform-set tran1
 encapsulation-mode tunnel
```

```
 protocol esp
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha256
#
ipsec policy map1 10 manual
 transform-set tran1
 security acl 3101
 remote-address 2.2.3.1
 sa spi inbound esp 54321
 sa string-key inbound esp simple gfedcba
 sa spi outbound esp 12345
 sa string-key outbound esp simple abcdefg
#
security-policy ip
 rule 1 name ipseclocalout
  action pass
  source-zone local
  destination-zone untrust
  source-ip-host 2.2.2.1
  destination-ip-host 2.2.3.1
 rule 2 name ipseclocalin
  action pass
  source-zone untrust
  destination-zone local
  source-ip-host 2.2.3.1
  destination-ip-host 2.2.2.1
 rule 3 name trust-untrust
  action pass
  source-zone trust
  destination-zone untrust
  source-ip-subnet 10.1.1.0 255.255.255.0
  destination-ip-subnet 10.1.2.0 255.255.255.0
 rule 4 name untrust-trust
  action pass
  source-zone untrust
  destination-zone trust
  source-ip-subnet 10.1.2.0 255.255.255.0
  destination-ip-subnet 10.1.1.0 255.255.255.0
```

```
#
```

2. Device B

```
#
acl number 3101
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ipsec policy use1 10 manual
 security acl 3101
 proposal tran1
 tunnel local 2.2.3.1
 tunnel remote 2.2.2.1
 sa spi inbound esp 12345
 sa string-key inbound esp abcdefg
 sa spi outbound esp 54321
 sa string-key outbound esp gfedcba
#
interface GigabitEthernet1/0/1
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 2.2.3.1 255.255.255.0
 ipsec policy use1
#
firewall zone trust
 add interface GigabitEthernet1/0/1
#
firewall zone untrust
 add interface GigabitEthernet1/0/2
#
ip route-static 10.1.1.0 255.255.255.0 2.2.3.2
ip route-static 2.2.2.0 255.255.255.0 2.2.3.2
#
security-policy
 rule name ipseclocalout
```

```
  source-zone local
  destination-zone untrust
  source-address 2.2.3.1 mask 255.255.255.255
  destination-address 2.2.2.1 mask 255.255.255.255
  action permit
 rule name ipseclocalin
  source-zone untrust
  destination-zone local
  source-address 2.2.2.1 mask 255.255.255.255
  destination-address 2.2.3.1 mask 255.255.255.255
  action permit
 rule name trust-untrust
  source-zone trust
  destination-zone untrust
  source-address 10.1.2.0 mask 255.255.255.0
  destination-address 10.1.1.0 mask 255.255.255.0
  action permit
 rule name untrust-trust
  source-zone untrust
  destination-zone trust
  source-address 10.1.1.0 mask 255.255.255.0
  destination-address 10.1.2.0 mask 255.255.255.0
  action permit
#
return
```