目 录

1 Group Domain VPN

1.1 Group Domain VPN简介

Group Domain VPN（Group Domain Virtual Private Network，组域虚拟专用网络）是一种实现密钥和安全策略集中管理的 VPN 解决方案。传统的 IPsec VPN 是一种点到点的隧道连接，而 Group Domain VPN 是一种点到多点的无隧道连接。Group Domain VPN 主要用于保护组播流量，例如音频、视频广播和组播文件的安全传输。

Group Domain VPN 提供了一种基于组的 IPsec 安全模型。组是一个安全策略的集合，属于同一个组的所有成员共享相同的安全策略及密钥。Group Domain VPN 由 KS（Key Server，密钥服务器）和 GM（Group Member，组成员）组成。其中，KS 通过划分不同的组来管理不同的安全策略和密钥；GM 通过加入相应的组，从 KS 获取安全策略及密钥，并负责对数据流量加密和解密。

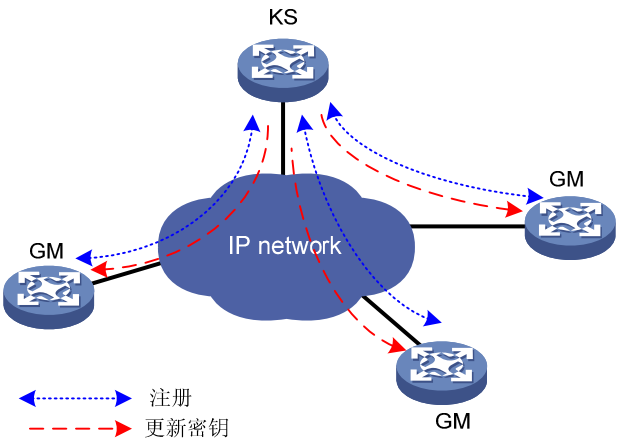
相比较传统的 IPsec VPN，Group Domain VPN 具有如下优点：

- 网络扩展性强。传统的 IPsec VPN 中，每对通信对等体之间都需要建立 IKE SA 和 IPsec SA，管理复杂度为 N^2，而 Group Domain VPN 中所有组成员之间共用一对 IPsec SA，管理复杂度低，可扩展性更好。
- 无需改变原有路由部署。传统的 IPsec VPN 是基于隧道的 VPN 连接，由于封装了新的 IP 头，需要重新部署路由。Group Domain VPN 不需修改报文 IP 头，报文外层封装的新的 IP 头与内层的原 IP 头完全相同，因此，不需要改变原有部署的路由。
- 更好的 QoS 处理。传统的 IPsec VPN 由于在原有 IP 报文外封装了新的 IP 头，报文在网络中传输时，需要重新配置 QoS 策略。Group Domain VPN 保留了原有的 IP 头，网络传输时可以更好地实现 QoS 处理。
- 组播效率更高。由于传统的 IPsec VPN 是点到点的隧道连接，当需要对组播报文进行 IPsec 保护时，本端需要向组播组里的每个对端均发送一份加密报文，因此组播效率低。Group Domain VPN 是无隧道的连接，只需对组播报文进行一次加密即可，本端无需单独向每个对端发送加密报文，组播效率高。
- 可提供 any-to-any 的连通性。所有组成员共用一对 IPsec SA，同一个组中的任意两个组成员之间都可以实现报文的加密和解密，真正实现了所有节点之间的互联。

1.1.1 Group Domain VPN的组网结构

Group Domain VPN的典型组网结构如图 1-1所示，其中包括两大组成元素，KS和GM。

图1-1 Group Domain VPN 组网结构示意图



1. KS（Key Server，密钥服务器）

KS 是一个为组维护安全策略、创建和维护密钥信息的网络设备。它有两个责任：响应 GM 的注册请求，以及发送 Rekey 报文。当一个 GM 向 KS 进行注册时，KS 会将安全策略和密钥下发给这个 GM。这些密钥将被周期性的更新，在密钥生存周期超时前，KS 会通过 Rekey 消息通知所有 GM 更新密钥。

KS 下发的密钥包括两种类型：

- TEK（tranfic encrytion key，加密流量的密钥）：由组内的所有 GM 共享，用于加密 GM 之间的流量。
- KEK（key encrytion key，加密密钥的密钥）：由组内的所有 GM 共享，用于加密 KS 向 GM 发送的 Rekey 报文。

2. GM（Group Member，组成员）

GM 是一组共享相同安全策略且有安全通信需求的网络设备。它在 KS 上注册，并利用从 KS 上获取的安全策略与属于同一个组的其它 GM 通信。GM 在 KS 上注册时提供一个组 ID，KS 根据这个组 ID 将对应组的安全策略和密钥下发给该 GM。

1.1.2 Group Domain VPN的工作机制

Group Domain VPN 的工作过程可分为 GM 向 KS 注册、GM 保护数据以及密钥更新三大部分。

1. GM向KS注册

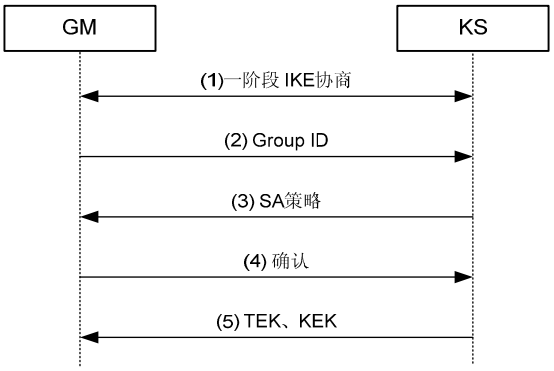
在 GM 的某接口上应用了 Group Domain VPN 的相关 IPsec 策略后，GM 会向 KS 发起注册，这个注册过程包括两个阶段的协商：IKE 协商和 GDOI（Group Domain of Interpretation，组解释域）协商，具体内容如下：

(1) 第一阶段的 IKE 协商：GM 与 KS 进行协商，进行双方的身份认证，身份认证通过后，生成用于保护二阶段 GDOI 协商的 IKE SA。

(2) 第二阶段的 GDOI 协商：这是一个 GM 从 KS 上“拉”安全策略的过程，其具体的协议过程由 GDOI 协议定义。

具体的注册过程包括图 1-2所示的五个步骤：

图1-2 注册过程流程图



(1) GM 与 KS 进行一阶段 IKE 协商；

(2) GM 向 KS 发送所在组的 ID；

(3) KS 根据 GM 提供的组 ID 向 GM 发送相应组的安全策略（保护的数据流信息、加密算法、认证算法、封装模式等）；

(4) GM 对收到的安全策略进行验证，如果这些策略是可接受的（例如安全协议和加密算法是可支持的），则向 KS 发送确认消息；

(5) KS 收到 GM 的确认消息后，向 GM 发送密钥信息（KEK、TEK）。

通过这个过程，GM 把 KS 上的安全策略和密钥“拉”到了本地。此后，就可以利用获取的安全策略和密钥在 GM 之间加密、解密传输的数据了。

说明

在 GM 向 KS 发起注册时，GM 会开启一个 GDOI 注册定时器。若该定时器超时时 GM 还未注册成功，则表示当前的注册过程失败，GM 会重新发起注册。该定时器的时间不可配，且在注册成功之后会根据下发的 Rekey SA 和 IPsec SA 的生命周期来更新超时时间。

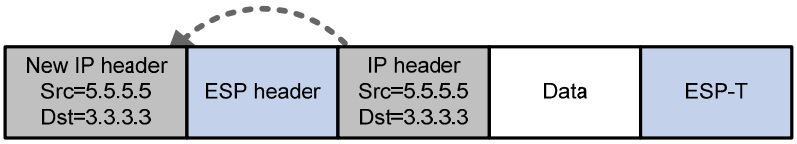
2. 数据保护

GM 完成注册之后，将使用获取到的 IPsec SA 对符合安全策略的报文进行保护。保护的数据可包括单播数据和组播数据两种类型。

与传统的 IPsec 类似，Group Domain VPN 也支持隧道和传输两种封装模式，该模式由 KS 决定并下发给 GM。

- 隧道模式：首先在原有的IP报文外部封装安全协议头（AH头或ESP头，目前Group Domain VPN不支持AH协议），然后在最外层封装一个与原有报文IP头的源和目的地址完全相同的IP头。图 1-3表示了一个进行ESP封装后的IP报文。

图1-3 隧道模式 Group Domain VPN 数据封装示意图



- 传输模式：在原有的 IP 报文头与报文数据之间封装安全协议头，不对原始的 IP 报文头做任何修改。

与传统 IPsec VPN 相同，Group Domain VPN 也支持对 MPLS L3VPN 的数据进行保护。MPLS L3VPN 的相关介绍，请参见“MPLS 配置指导”中的“MPLS L3VPN”。

3. 密钥更新（Rekey）

GM 向 KS 注册后，如果 KS 上配置了 Rekey 的相关参数（具体配置请参见 KS 的相关配置指导），则 KS 会向 GM 发送密钥更新 SA（Rekey SA）。在 KS 本端维护的 IPsec SA 或 Rekey SA 老化时间到达之前，KS 将通过密钥更新消息（也称为 Rekey 消息）定期向 GM 以单播或组播的方式发送新的 IPsec SA 或 Rekey SA，该 Rekey 消息使用当前的 Rekey SA 进行加密，GM 会通过 KS 下发的公钥对该消息进行认证。所有 GM 会周期性地收到来自 KS 的密钥更新消息。如果 GM 在 IPsec SA 或 Rekey SA 生命周期超时前一直没有收到任何 Rekey 消息，将会重新向 KS 发起一次注册，把安全策略和密钥“拉”过来。

说明

- 由 KS 来决定采用单播或组播的方式向 GM 发送 Rekey 消息。
- KS 在 GM 注册的过程中，会将本端的公钥信息下发给 GM。

1.1.3 协议规范

与 Group Domain VPN 相关的协议规范有：

- RFC 2408：Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 3547：The Group Domain of Interpretation(GDOI)
- RFC 3740：The Multicast Group Security Architecture
- RFC 5374：Multicast Extensions to the Security Architecture for the Internet Protocol

1.2 Group Domain VPN配置任务简介

Group Domain VPN 的配置思路如下：

(1) 配置 KS，具体请参见相关 KS 的配置指导。目前，设备仅支持作为 GM，不支持作为 KS。

(2) 配置 GM，包括以下两个部分：

- 配置 IKE：包括用来与 KS 进行一阶段 IKE 协商的 IKE 提议和 IKE 对等体。具体配置步骤请参见“安全配置指导”中的“IKE”。
- 配置GDOI：具体配置步骤请见表 1-1。

表1-1 GDOI 配置任务简介

配置任务	说明	详细配置
配置GDOI组	必选	1.3
配置IPsec GDOI安全策略	必选	1.4
接口上应用IPsec GDOI安全策略	必选	1.5

说明

- KS 与 GM 上的 IKE 配置必须匹配，否则会导致一阶段 IKE 协商失败。
- IKE 对等体的对端安全网关地址为 KS 的 IP 地址。

1.3 配置GDOI组

在 GM 上可以同时存在多个 GDOI 组。一个 GDOI 组中包含了 GM 向 KS 注册时需要提交的关键信息，包括组 ID、KS 地址和注册接口等。各项配置信息的具体介绍如下：

- 组名：GDOI 组在设备上的一个配置标识，仅用于本地配置管理和引用。
- 组 ID：GDOI 组在 Group Domain VPN 中的一个标识。KS 通过 GM 提交的组 ID 来区分 GM 要加入的 GDOI 组。一个 GDOI 组只能使用组号或者 IP 地址作为组 ID，且只能配置一个组 ID。
- KS 地址：GM 要注册的 KS 的 IP 地址。一个 GDOI 组中最多允许同时配置 8 个 KS 地址，其使用的优先级按照配置先后顺序依次降低。GM 首先向配置的第一个 KS 地址发起注册，如果无法成功注册，则在 GDOI 注册定时器超时后，会依次向后续配置的 KS 地址发起注册，直到注册成功为止；如果 GM 向所有的 KS 地址发起的注册都失败，则会继续从第一个 KS 地址开始重复以上过程。
- 注册接口：GM 通过注册接口向 KS 发起注册。缺省情况下，GDOI 组以 IPsec GDOI 安全策略应用的接口作为注册接口向 KS 注册。配置的注册接口可以跟 GDOI 组所在的 IPsec 安全策略应用接口相同，也可以不同。当用户希望注册报文和 IPsec 报文通过不同的接口处理时，可指定设备上的其它接口（物理接口或逻辑接口）作为注册接口。

表1-2 配置 GDOI 组

配置任务	命令	说明
进入系统视图	**system-view**	-
创建一个GDOI组，并进入GDOI组视图	**gdoi group** *group-name*	必选 缺省情况下，不存在GDOI组
配置GDOI组的组ID	**identity** { **address** *ip-address* | **number** *number* }	必选 缺省情况下，未定义GDOI组的组ID 一个GDOI组只能有一种类型的标识，IP地址或者组号
配置GDOI组的KS地址	**server address** *ip-address*	必选 缺省情况下，未指定KS的IP地址
配置GDOI组的注册接口	**client registration interface** *interface-type interface-number*	可选 缺省情况下， GDOI组以IPsec GDOI安全策略应用的接口为注册接口向KS注册

说明

- 一个 GDOI 组只能配置一个组 ID，后配置的组 ID 会覆盖前面配置的组 ID。
- 不同 GDOI 组中指定的 KS 地址和组 ID 这两项信息不允许都相同。

1.4 配置IPsec GDOI安全策略

一条 IPsec GDOI 安全策略由“名字”和“顺序号”共同唯一确定，顺序号小的优先级高。IPsec GDOI 安全策略视图下指定了引用的 GDOI 组，以及本地访问控制列表。IPsec GDOI 安全策略试图下，目前包括且仅包括以下两个配置：

- IPsec GDOI 安全策略通过引用的 GDOI 组查找到注册的 KS 地址，以及注册的组 ID；
- IPsec GDOI 安全策略可以通过引用一个本地配置的访问控制列表（称为本地访问控制列表）决定哪些报文需要丢弃，哪些报文需要明文转发。当匹配本地访问控制列表的结果为 **permit** 时，报文会被丢弃；当匹配本地访问控制列表的结果为 **deny** 时，报文会被明文转发。

GM 向 KS 注册后，会从 KS 上获取安全策略，其中包含了 KS 上配置的访问控制列表（称为下载的访问控制列表）。KS 上配置的访问控制列表用来控制 GM 的行为，即决定 GM 上的哪些报文需要加密，哪些报文需要明文转发。对于 GM 收到的报文，匹配下载的访问控制列表的结果为 **permit** 时，会被加密；匹配下载的访问控制列表的结果为 **deny** 时，会以明文形式转发。如果报文没有匹配任何下载的访问控制列表，默认的处理方式是明文转发。

如果 IPsec GDOI 安全策略中配置了本地访问控制列表，则 GM 向 KS 注册后，两种类型的访问控制列表将在 GM 上共存，且报文优先匹配本地访问控制列表。若报文没有匹配到本地访问控制列表的任何规则，则会接着匹配下载的访问控制列表，两者都匹配不上时，则默认进行明文转发。

表1-3 配置 IPsec GDOI 安全策略

配置任务	命令	说明
进入系统视图	**system-view**	-
创建一条IPsec GDOI安全策略，并进入IPsec 安全策略视图	**ipsec policy** *policy-name seq-number* **gdoi**	必选 缺省情况下，没有IPsec GDOI安全策略存在 本命令的详细介绍请参见“安全命令参考”中的“IPsec”
指定IPsec GDOI安全策略引用的GDOI组	**group** *group-name*	必选 缺省情况下，IPsec GDOI安全策略没有引用任何GDOI组 一条IPsec GDOI安全策略下只能够引用一个GDOI组

配置任务	命令	说明
引用本地访问控制列表	**security acl** *acl-number*	可选 缺省情况下，没有配置本地访问控制列表 一般情况下，无需配置本地访问控制列表。如果需要本地对数据流进行管理时，则配置 本命令的详细介绍请参见“安全命令参考”中的“IPsec”

说明

- 对于 IPsec GDOI 安全策略，只有引用了已存在的 GDOI 组，且引用的 GDOI 组配置完整时（配置了组 ID 和 KS 地址），该策略才能生效。
- 一条 IPsec 安全策略只能引用一条本地访问控制列表，当报文匹配上本地访问控制列表的 **permit** 规则时，会被丢弃，因此请慎重配置本地访问控制列表的 **permit** 规则。
- GDOI 协议报文与非首片报文不进行 IPsec GDOI 安全策略的匹配。
- 目的地址为本机的待解封装的 IPsec 报文不与 IPsec GDOI 安全策略中的本地访问控制列表进行匹配，仅与下载的访问控制列表进行匹配。

1.5 在接口上应用IPsec GDOI安全策略组

IPsec 安全策略组是所有具有相同名字、不同顺序号的 IPsec 安全策略的集合。在同一个 IPsec 安全策略组中，顺序号越小的 IPsec 安全策略，优先级越高。IPsec 安全策略的详细介绍，请参见“安全配置指导”中的“IPsec”。

当 IPsec 安全策略组应用到接口上时，如果该策略组中存在一条 IPsec GDOI 安全策略，且该策略引用的 GDOI 组配置了组 ID 和 KS 地址，则设备会向 KS 发起注册。当数据报文经过该接口时，如果报文匹配了该接口的本地访问控制列表，则丢弃；如果报文匹配了下载的访问控制列表，则该按照 IPsec GDOI 策略处理。

表1-4 在接口上应用 IPsec GDOI 安全策略组

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
应用IPsec 安全策略组	**ipsec policy** *policy-name*	必选 缺省情况下，接口下未应用任何IPsec安全策略组 本命令的详细介绍请参见“安全命令参考”中的“IPsec”

说明

一个接口只能应用一个 IPsec 安全策略组。通过 GDOI 方式创建的 IPsec 安全策略可以应用到多个接口上。

1.6 Group Domain VPN显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 Group Domain VPN 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 GM 的 GDOI 信息，并发起注册。

表1-5 Group Domain VPN 显示和维护

操作	命令
显示GDOI组信息	**display gdoi** [**group** *group-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示GM获取的IPsec SA信息	**display gdoi** [**group** *group-name*] **ipsec sa** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示GM的简要信息	**display gdoi** [**group** *group-name*] **gm** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示GM的ACL信息	**display gdoi** [**group** *group-name*] **gm acl** [**download** | **local**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示GM的Rekey信息	**display gdoi** [**group** *group-name*] **gm rekey** [**verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示GM接收到的公钥信息	**display gdoi** [**group** *group-name*] **gm pubkey** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IKE SA相关信息	**display ike sa** [**active** | **standby** | **verbose** [**connection-id** *connection-id* | **remote-address** [**ipv6**] *remote-address*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec SA相关信息	**display ipsec sa** [**active** | **brief** | **duration** | **policy** *policy-name* [*seq-number*] | **remote** [**ipv6**] *ip-address* | **standby**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示IPsec GDOI安全策略相关信息	**display ipsec policy** [**brief** | **name** *policy-name* [*seq-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除GM的GDOI信息，并发起注册	**reset gdoi** [**group** *group-name*]

说明

display ike sa、**display ipsec sa** 以及 **display ipsec policy** 命令的详细介绍，请见“安全配置指导”中的“IPsec”。

1.7 Group Domain VPN典型配置举例

1.7.1 Group Domain VPN典型配置举例

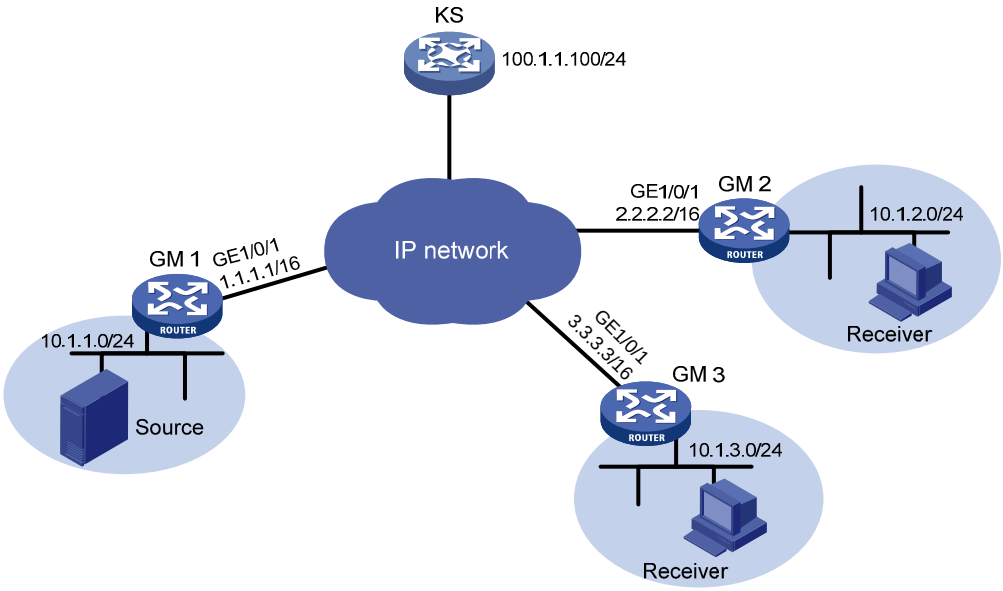
1. 组网需求

在如图 1-4所示的组网环境中，需要组建一个Group Domain VPN，对组播源与各子网之间，以及各子网之间的数据流进行安全保护，具体要求如下：

- GM 1、GM 2 和 GM 3 加入相同的组（组 ID 为 12345），并向维护、管理该组的 KS 进行注册。
- 对各 GM 之间的数据进行 IPsec 保护时，采用的安全协议为 ESP，加密算法为 AES-CBC 128，认证算法为 SHA1。
- GM 与 KS 之间进行 IKE 协商时，使用预共享密钥的认证方法。

2. 组网图

图1-4 Group Domain VPN 典型配置组网图



3. 配置步骤

说明

- 请确保 GM 1、GM 2、GM 3 分别与 KS 之间路由可达。
- 请确保 GM 1、GM 2、GM 3 之间的组播报文可正常转发。

(1) 配置 KS

- 配置访问控制列表，定义要保护的数据流的范围为组播源到各子网的数据流，以及各子网之间的数据流。
- 配置 IPsec 安全策略，使用的 IPsec 封装协议为 ESP，加密算法为 AES-CBC 128，认证算法为 SHA1。

以上配置的具体步骤请参考 KS 的相关配置指导。

(2) 配置 GM 1

配置各接口的 IP 地址，此处略。

创建 IKE 提议 1。

```
<GM1> system-view
[GM1] ike proposal 1
```

指定 IKE 提议使用的加密算法为 AES-CBC 128。

```
[GM1-ike-proposal-1] encryption-algorithm aes-cbc 128
```

指定 IKE 提议使用的认证为 SHA1。

```
[GM1-ike-proposal-1] authentication-algorithm sha
```

指定 IKE 提议使用的 DH 组为 group 2。

```
[GM1-ike-proposal-1] dh group2
[GM1-ike-proposal-1] quit
```

创建 IKE 对等体 1。

```
[GM1] ike peer 1
```

指定 IKE 对等体 1 引用 IKE 提议 1。

```
[GM1-ike-peer-1] proposal 1
```

配置采用预共享密钥认证时，使用的预共享密钥为明文 tempkey1。

```
[GM1-ike-peer-1] pre-shared-key simple tempkey1
```

指定对端安全网关的 IP 地址为 100.1.1.100。

```
[GM1-ike-peer-1] remote-address 100.1.1.100
[GM1-ike-peer-1] quit
```

创建 GDOI 组 1。

```
[GM1] gdoi group 1
```

配置 GDOI 组的 ID 为编号 123456。

```
[GM1-gdoi-group-1] identity number 12345
```

指定 GDOI 组的 KS 地址为 100.1.1.100。

```
[GM1-gdoi-group-1] server address 100.1.1.100
[GM1-gdoi-group-1] quit
```

创建 GDOI 类型的 IPsec 安全策略。

```
[GM1] ipsec policy map 1 gdoi
```

引用 GDOI 组 1。

```
[GM1-ipsec-policy-gdoi-map-1] group 1
[GM1-ipsec-policy-gdoi-map-1] quit
```

在接口 GigabitEthernet1/0/1 上应用安全策略组。

```
[GM1] interface gigabitethernet 1/0/1
[GM1-GigabitEthernet1/0/1] ipsec policy map
[GM1-GigabitEthernet1/0/1] quit
```

(3) 配置 GM 2

配置各接口的 IP 地址，此处略。

创建 IKE 提议 1。

```
<GM2> system-view
[GM2] ike proposal 1
```

指定 IKE 提议使用的加密算法为 AES-CBC 128。

```
[GM2-ike-proposal-1] encryption-algorithm aes-cbc 128
```

指定 IKE 提议使用的认证为 SHA1。

```
[GM2-ike-proposal-1] authentication-algorithm sha
```

指定 IKE 提议使用的 DH 组为 group 2。

```
[GM2-ike-proposal-1] dh group2
[GM2-ike-proposal-1] quit
```

创建 IKE 对等体 1。

```
[GM2] ike peer 1
```

指定 IKE 对等体 1 引用 IKE 提议 1。

```
[GM2-ike-peer-1] proposal 1
```

配置采用预共享密钥认证时，使用的预共享密钥为明文 tempkey1。

```
[GM2-ike-peer-1] pre-shared-key simple tempkey1
```

配置对端安全网关的 IP 地址为 100.1.1.100。

```
[GM2-ike-peer-1] remote-address 100.1.1.100
[GM2-ike-peer-1] quit
```

创建 GDOI 组 1。

```
[GM2] gdoi group 1
```

配置 GDOI 组的 ID 为编号 123456。

```
[GM2-gdoi-group-1] identity number 12345
```

指定 GDOI 组的 KS 地址为 100.1.1.100。

```
[GM2-gdoi-group-1] server address 100.1.1.100
[GM2-gdoi-group-1] quit
```

创建 GDOI 类型 IPsec 安全策略。

```
[GM2] ipsec policy map 1 gdoi
```

引用 GDOI 组 1。

```
[GM2-ipsec-policy-gdoi-map-1] group 1
[GM2-ipsec-policy-gdoi-map-1] quit
```

在接口 GigabitEthernet10//1 上应用 IPsec 安全策略组。

```
[GM2] interface gigabitethernet 1/0/1
[GM2-GigabitEthernet1/0/1] ipsec policy map
[GM2-GigabitEthernet1/0/1] quit
```

(4)　配置 GM 3

配置各接口的 IP 地址，此处略。

创建 IKE 提议 1。

```
<GM3> system-view
[GM3] ike proposal 1
```

指定 IKE 提议使用的加密算法为 AES-CBC 128。

```
[GM3-ike-proposal-1] encryption-algorithm aes-cbc 128
```

指定 IKE 提议使用的认证为 SHA1。

```
[GM3-ike-proposal-1] authentication-algorithm sha
```

指定 IKE 提议使用的 DH 组为 group 2。

```
[GM3-ike-proposal-1] dh group2
```

```
[GM3-ike-proposal-1] quit
```
创建 IKE 对等体 1。
```
[GM3] ike peer 1
```
指定 IKE 对等体 1 引用 IKE 提议 1。
```
[GM3-ike-peer-1] proposal 1
```
配置采用预共享密钥认证时，使用的预共享密钥为明文 tempkey1。
```
[GM3-ike-peer-1] pre-shared-key simple tempkey1
```
配置对端安全网关的 IP 地址为 100.1.1.100。
```
[GM3-ike-peer-1] remote-address 100.1.1.100
[GM3-ike-peer-1] quit
```
创建 GDOI 组 1。
```
[GM3] gdoi group 1
```
配置 GDOI 组的 ID 为编号 123456。
```
[GM3-gdoi-group-1] identity number 12345
```
指定 GDOI 组的 KS 地址为 100.1.1.100。
```
[GM3-gdoi-group-1] server address 100.1.1.100
[GM3-gdoi-group-1] quit
```
创建 GDOI 类型 IPsec 安全策略。
```
[GM3] ipsec policy map 1 gdoi
```
引用 GDOI 组 1。
```
[GM3-ipsec-policy-gdoi-map-1] group 1
[GM3-ipsec-policy-gdoi-map-1] quit
```
在接口 GigabitEthernet1/0/1 上应用 IPsec 安全策略组。
```
[GM3] interface gigabitethernet 1/0/1
[GM3-GigabitEthernet1/0/1] ipsec policy map
[GM3-GigabitEthernet1/0/1] quit
```

4. 验证配置结果

以上配置完成后，GM 1、GM 2 和 GM 3 分别向 KS 注册，可通过如下显示信息查看到 GM 1 在 IKE 协商成功后生成的 IKE SA 和 Rekey SA。其中，connection-id 为 658 的 SA 为 IKE SA；connection-id 为 659 的 SA 为 Rekey SA。

```
[GM1] display ike sa
    total phase-1 SAs:  2
    connection-id  peer                    flag        phase   doi      status
  -------------------------------------------------------------------------------
     658           100.1.1.100             RD|ST       1       GROUP    --
     659           100.1.1.100             RD|RK       1       GROUP    --

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
```

IKE 协商成功后生成的 IPsec SA，可通过如下显示信息查看到有两组 IPsec SA 分别用于与不同的组成员之间进行安全通信。

```
[GM1] display ipsec sa
==============================
Interface: GigabitEthernet1/0/1
```

```
    path MTU: 1500
================================

  ----------------------------
  IPsec policy name: "map"
  sequence number: 1
  mode: gdoi
  ----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.1.1.1
        remote address: 0.0.0.0
    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

    current outbound spi: 0xDB865076(3683012726)

    [inbound ESP SAs]
      spi: 0xDB865076(3683012726)
      transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
      in use setting: Transport
      connection id: 317
      sa duration (kilobytes/sec): 0/900
      sa remaining duration (kilobytes/sec): 0/63
      anti-replay detection: Disabled

      spi: 0x640321A(104870426)
      transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
      in use setting: Transport
      connection id: 325
      sa duration (kilobytes/sec): 0/900
      sa remaining duration (kilobytes/sec): 0/853
      anti-replay detection: Disabled

    [outbound ESP SAs]
      spi: 0xDB865076(3683012726)
      transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
      in use setting: Transport
      connection id: 318
      sa duration (kilobytes/sec): 0/900
      sa remaining duration (kilobytes/sec): 0/63
      anti-replay detection: Disabled

      spi: 0x640321A(104870426)
      transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
      in use setting: Transport
      connection id: 326
```

```
    sa duration (kilobytes/sec): 0/900
    sa remaining duration (kilobytes/sec): 0/853
    anti-replay detection: Disabled


----------------------------
IPsec policy name: "map"
sequence number: 1
mode: gdoi
----------------------------
  PFS: N, DH group: none
  tunnel:
      local  address: 1.1.1.1
      remote address: 0.0.0.0
  flow:
      sour addr: 10.1.2.0/255.255.255.0  port: 0  protocol: IP
      dest addr: 10.1.1.0/255.255.255.0  port: 0  protocol: IP

  current outbound spi: 0xDB865076(3683012726)

  [inbound ESP SAs]
    spi: 0xDB865076(3683012726)
    transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
    in use setting: Transport
    connection id: 321
    sa duration (kilobytes/sec): 0/340
    sa remaining duration (kilobytes/sec): 0/61
    anti-replay detection: Disabled

    spi: 0x640321A(104870426)
    transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
    in use setting: Transport
    connection id: 329
    sa duration (kilobytes/sec): 0/900
    sa remaining duration (kilobytes/sec): 0/851
    anti-replay detection: Disabled

  [outbound ESP SAs]
    spi: 0xDB865076(3683012726)
    transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
    in use setting: Transport
    connection id: 322
    sa duration (kilobytes/sec): 0/340
    sa remaining duration (kilobytes/sec): 0/61
    anti-replay detection: Disabled

    spi: 0x640321A(104870426)
    transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
```

```
      in use setting: Transport
      connection id: 330
      sa duration (kilobytes/sec): 0/900
      sa remaining duration (kilobytes/sec): 0/851
      anti-replay detection: Disabled
```

GM 1 向 KS 注册成功后，可通过如下显示信息查看到 GM 1 的注册信息。

```
[GM1] display gdoi
Group Name: 1

  Group Identity             : 12345
  Rekeys Received            : 129
  IPsec SA Direction         : Both

  Group Server List          : 100.1.1.100

  Group Member               : 1.1.1.1
    Registration status      : Registered
    Registered with          : 100.1.1.100
    Re-register in           : 81 sec
    Succeeded registrations  : 1
    Attempted registrations  : 1
    Last rekey from          : 100.1.1.100
    Last rekey seq num       : 1
    Multicast rekeys received: 0
    Allowable rekey cipher   : Any
    Allowable rekey hash     : Any
    Allowable transform      : Any

  Rekeys Cumulative
    Total received           : 129
    After latest registration: 129
    Rekey received (hh:mm:ss): 00:00:57

  ACL Downloaded From KS 100.1.1.100:
    rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
    rule 1 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255

  KEK Policy:
    Rekey transport type     : Multicast
    Lifetime (sec)           : 243
    Encrypt algorithm        : AES
    Key size                 : 128
    Sig hash algorithm       : SHA1
    Sig key length (bit)     : 2048

  TEK Policy:
    Interface GigabitEthernet1/0/1:
      IPsec SA:
```

```
SPI: 0x640321A(104870426)
Transform: ESP-ENCRYPT-AES-128 ESP-AUTH-SHA1
SA timing:
  remaining key lifetime (sec): 123
Anti-replay detection: Disabled
```

以上配置完成后，如果子网 10.1.1.0/24 与子网 10.1.2.0/24 之间有报文传输，将分别由 GM 1 和 GM 2 进行加密/解密处理。

1.8 常见错误配置举例

1.8.1 IKE SA协商失败

1. 故障现象

一阶段 IKE 协商失败。

2. 故障分析

GM 和 KS 的 IKE 配置不匹配，或者 GM 与 KS 之间路由不可达。

可以通过以下显示信息看到，没有 IKE SA 生成：

```
<Router> display ike sa
    total phase-1 SAs:  0
    connection-id  peer                    flag        phase   doi      status
  -------------------------------------------------------------------------------
```

3. 处理过程

检查 GM 上配置的 IKE 提议和 IKE 对等体是否与 KS 上配置的相匹配，并检查 GM 到 KS 是否路由可达。

1.8.2 GM无法注册成功

1. 故障现象

GM 无法向 KS 注册成功。

2. 故障分析

可以通过以下显示信息看到，只有一阶段 IKE 协商成功，生成了一个 IKE SA，没有生成 Rekey SA 和 IPsec SA：

```
<Router> display ike sa
    total phase-1 SAs:  1
    connection-id  peer                    flag        phase   doi      status
  -------------------------------------------------------------------------------
     18            90.1.1.1                RD|ST       1       GROUP    --
```

3. 处理过程

检查 GM 和 KS 配置的组 ID 是否一致。