目 录

1 Group Domain VPN ····· 1-1
1.1 Group Domain VPN简介 ····· 1-1
1.1.1 Group Domain VPN的组网结构 ····· 1-1
1.1.2 Group Domain VPN的工作机制 ····· 1-2
1.1.3 协议规范 ····· 1-4
1.2 Group Domain VPN配置限制和指导 ····· 1-5
1.3 配置GDOI GM ····· 1-5
1.3.1 GDOI GM配置任务简介 ····· 1-5
1.3.2 配置GDOI GM组 ····· 1-5
1.3.3 配置IPsec GDOI安全策略 ····· 1-7
1.3.4 在接口上应用IPsec GDOI安全策略 ····· 1-8
1.3.5 GDOI GM显示和维护 ····· 1-8
1.4 Group Domain VPN典型配置举例 ····· 1-9
1.4.1 Group Domain VPN典型配置举例 ····· 1-9

1 Group Domain VPN

说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

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 IPsec 安全策略集中管理的点到多点无隧道连接 VPN 解决方案，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，属于同一个组的所有成员共享相同的安全策略及密钥。

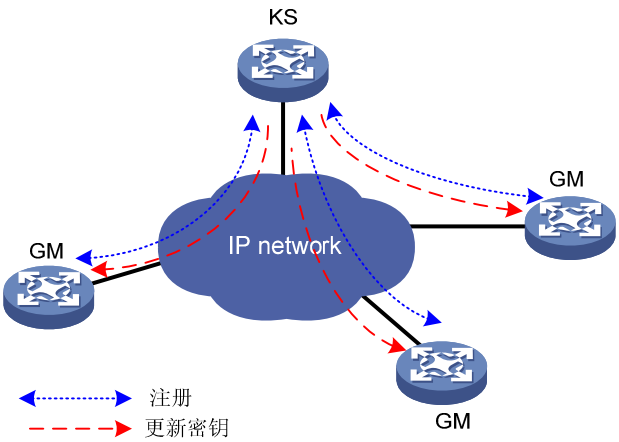
相比较传统的 IPsec VPN，Group Domain VPN 具有如下优点：

- 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，管理复杂度高，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，如果封装了新的 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。
- 可提供点到多点的连通性。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由KS（Key Server，密钥服务器）和GM（Group Member，组成员）组成，它的典型组网结构如 图 1-1 所示。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。

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 消息。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（traffic encryption 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 消息。

可以通过配置，使多个 KS 之间进行冗余备份，以提供高可靠性和提供注册服务的负载分担。

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。它们在 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

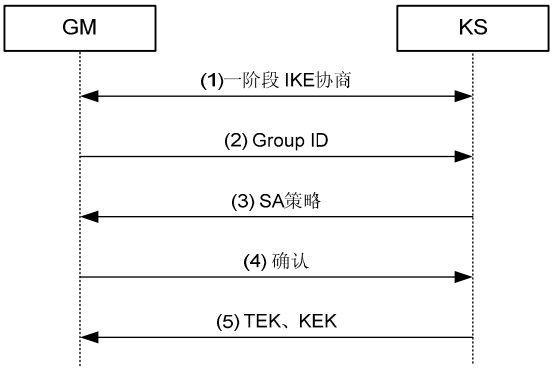
在 GM 的某接口上应用了 Group Domain VPN 的相关 IPsec 安全策略后，GM 会向 KS 发起注册，这个注册过程包括两个阶段的协商：IKE 协商和 GDOI（Group Domain of Interpretation，组解释域）协商，具体内容如下：

(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，生成用于保护第二阶段 GDOI 协商的 IKE SA。

(2) 第二阶段的 GDOI 协商：这是一个 GM 从 KS 上“拉”IPsec 安全策略的过程，其具体的协议过程由 GDOI 协议定义，可参见 RFC3547 中关于 GROUPKEY-PULL 交换的描述。

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 IPsec 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 IPsec 安全策略进行验证，如果该策略是可接受的（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 IPsec 安全策略和密钥获取到了本地。此后，就可以利用获取的 IPsec 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。

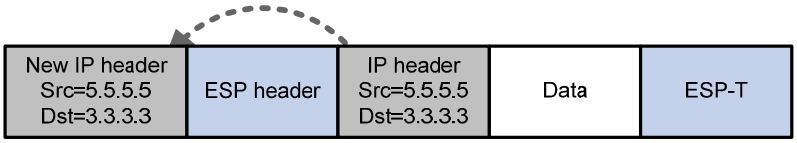
2. 数据保护

GM 完成注册之后，将使用获取到的 IPsec SA 对符合 IPsec 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 VPN 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。有关 Rekey 消息的详细描述，请参见 RFC 3547 中关于 GROUPKEY-PUSH 消息的描述。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 IPsec 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，缺省情况下 KS 采用组播发送方式。
- 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
- RFC 6407：The Group Domain of Interpretation(GDOI)

1.2 Group Domain VPN配置限制和指导

说明

当前设备仅支持作为 GM，不支持作为 KS。

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。

1.3 配置GDOI GM

1.3.1 GDOI GM配置任务简介

GDOI GM 需要 IKE 的相关配置进行配合，IKE 的配置主要包括用来与 GDOI KS 进行一阶段 IKE 协商的 IKE 提议和 IKE profile。IKE 的具体配置步骤请参见“安全配置指导”中的“IKE”。

表1-1 GDOI GM 配置任务简介

配置任务	说明	详细配置
配置GDOI GM组	必选	1.3.2
配置IPsec GDOI安全策略	必选	1.3.3
接口上应用IPsec GDOI安全策略	必选	1.3.4

1.3.2 配置GDOI GM组

在 GM 上可以同时存在多个 GDOI GM 组。一个 GDOI GM 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 GM 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 GM 组在 Group Domain VPN 中的一个标识。KS 通过 GM 提交的组 ID 来区分 GM 要向哪个 KS 注册，GM 提交的组 ID 必须与它要加入的 KS 的组 ID 一致。一个 GDOI GM 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 GM 组中最多允许同时配置 16 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 GM 组以 KS 地址为目的地址的路由的出接口作为注册接口向 KS 注册。配置的注册接口可以跟 GDOI GM 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。
- 支持的 KEK 加密算法：GM 注册过程中，当 KS 下发的 KEK 算法不符合 GM 支持的 KEK 算法时，GM 终止与 KS 的协商且注册失败；Rekey 过程中，当 KS 下发的 KEK 算法不符合 GM 支持的 KEK 算法时，GM 丢弃收到的 rekey 报文。

- 支持的 IPsec 安全提议：GM 注册过程中，当 KS 下发的 IPsec 安全提议不在本地支持的范围之内，则 GM 终止与 KS 的协商且注册失败；Rekey 过程中，当 KS 下发的 IPsec 安全提议不在本地支持的范围之内，则 GM 丢弃收到的 rekey 报文。

配置限制和指导：

- 一个 GDOI GM 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 GM 组中指定的 KS 地址和组 ID 这两项信息不允许都相同。

表1-2 配置 GDOI GM 组

配置任务	命令	说明
进入系统视图	**system-view**	-
创建一个GDOI GM组，并进入GDOI GM组视图	**gdoi gm group** [**ipv6**] *group-name*	缺省情况下，不存在GDOI GM组
配置GDOI GM组的组ID	**identity** { **address** *ip-address* | **number** *number* }	缺省情况下，未定义GDOI GM组的组ID 一个GDOI GM组只能有一种类型的标识，IP地址或者组号
指定KS地址	**server address** *host* [**vrf** *vrf-name*]	缺省情况下，未指定KS的地址
（可选）指定GM的注册接口	**client registration interface** *interface-type interface-number*	缺省情况下，GM使用到达KS地址的路由的出接口作为注册接口向KS注册
（可选）指定GM支持的KEK加密算法	非FIPS模式下： **client rekey encryption** { **des-cbc** | **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** } * FIPS模式下： **client rekey encryption** { **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** } *	非FIPS模式下： 缺省情况下，GM支持DES-CBC、3DES-CBC、AES-CBC-128、AES-CBC-192、AES-CBC-256加密算法 FIPS模式下： 缺省情况下，GM支持AES-CBC-128、AES-CBC-192、AES-CBC-256加密算法
（可选）指定GM支持的IPsec安全提议	**client transform-sets** *transform-set-name*&<1-6>	缺省情况下，GM支持如下的安全提议： • 安全协议：ESP • 封装模式：隧道模式和传输模式 • 加密算法：DES-CBC、3DES-CBC、AES-CBC-128、AES-CBC-192、AES-CBC-256 • 验证算法：MD5、SHA1
（可选）配置GDOI GM组的抗重放时间窗口	**client anti-replay window** { **sec** *seconds* | **msec** *milliseconds* }	缺省情况下，未配置GDOI GM组的抗重放时间窗口

1.3.3 配置IPsec GDOI安全策略

一个 IPsec GDOI 安全策略是若干具有相同名字、不同顺序号的 IPsec GDOI 安全策略表项的集合。在同一个 IPsec GDOI 安全策略中，顺序号越小的 IPsec GDOI 安全策略表项优先级越高。IPsec GDOI 安全策略视图下，目前包括且仅包括以下两个配置：

- 指定引用的 GDOI GM 组。IPsec GDOI 安全策略通过引用的 GDOI GM 组查找到注册的 KS 地址，以及注册的组 ID。只有引用了已存在且相同 IP 协议类型的 GDOI GM 组，且引用的 GDOI GM 组配置完整（配置了组 ID 和 KS 地址）的 IPsec GDOI 安全策略才能生效。
- 引用本地访问控制列表。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。当报文匹配上本地访问控制列表的 deny 规则时，会被明文转发；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。

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/解密，哪些报文需要转发。

- 对于 GM 要发送的报文，若匹配上下载的访问控制列表的 permit 规则，则会被加密后转发；若匹配上下载的访问控制列表的 deny 规则，则会被以明文形式转发。
- 对于 GM 接收到的密文，若匹配上下载的访问控制列表的 permit 规则，则会被解密；若匹配上下载的访问控制列表的 deny 规则，则会被以密文形式转发。
- 对于 GM 接收到的明文，若匹配上下载的访问控制列表的 permit 规则，则会被丢弃；若匹配上下载的访问控制列表的 deny 规则，则会被以明文形式转发。
- 如果报文没有匹配任何下载的访问控制列表，默认的处理方式是转发。

如果 IPsec GDOI 安全策略中引用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，具体处理机制如下：

- 在加密处理时，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。
- 在解密处理时，密文优先匹配下载的访问控制列表，若报文没有匹配到下载访问控制列表的任何规则，则会接着匹配本地访问控制列表；明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 GDOI安全策略视图	**ipsec** { **ipv6-policy** | **policy** } *policy-name seq-number* **gdoi**	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 GM组	**group** *group-name*	缺省情况下，IPsec GDOI安全策略没有引用任何GDOI GM组 一条IPsec GDOI安全策略下只能够引用一个GDOI GM组

配置任务	命令	说明
（可选）引用本地访问控制列表	**security acl** [**ipv6**] *acl-number*	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，则配置本地访问控制列表 本命令的详细介绍请参见“安全命令参考”中的“IPsec”

1.3.4 在接口上应用IPsec GDOI安全策略

当 IPsec GDOI 安全策略应用到接口上，且该策略引用的 GDOI GM 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

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	**ipsec apply** { **ipv6-policy** | **policy** } *policy-name*	缺省情况下，接口下未应用任何IPsec安全策略 本命令的详细介绍请参见“安全命令参考”中的“IPsec”

1.3.5 GDOI GM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 GDOI GM 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 GM组信息	**display gdoi gm** [**group** *group-name*]
显示GDOI GM组的抗重放时间戳类型和时间窗口大小	**display gdoi gm anti-replay** [**group** *group-name*]
显示GM获取的IPsec SA信息	**display gdoi gm ipsec sa** [**group** *group-name*]
显示GM的简要信息	**display gdoi gm members** [**group** *group-name*]
显示GM的ACL信息	**display gdoi gm acl** [**download** | **local**] [**group** *group-name*]
显示GM的Rekey信息	**display gdoi gm rekey** [**verbose**] [**group** *group-name*]
显示GM接收到的公钥信息	**display gdoi gm pubkey** [**group** *group-name*]

操作	命令
显示IPsec GDOI安全策略相关信息	**display ipsec policy** [*policy-name* [*seq-number*]]
清除GM的GDOI信息，并发起注册	**reset gdoi gm** [**group** *group-name*]

说明

display ipsec policy 命令的详细介绍，请见“安全命令”中的“IPsec”。

1.4 Group Domain VPN典型配置举例

1.4.1 Group Domain VPN典型配置举例

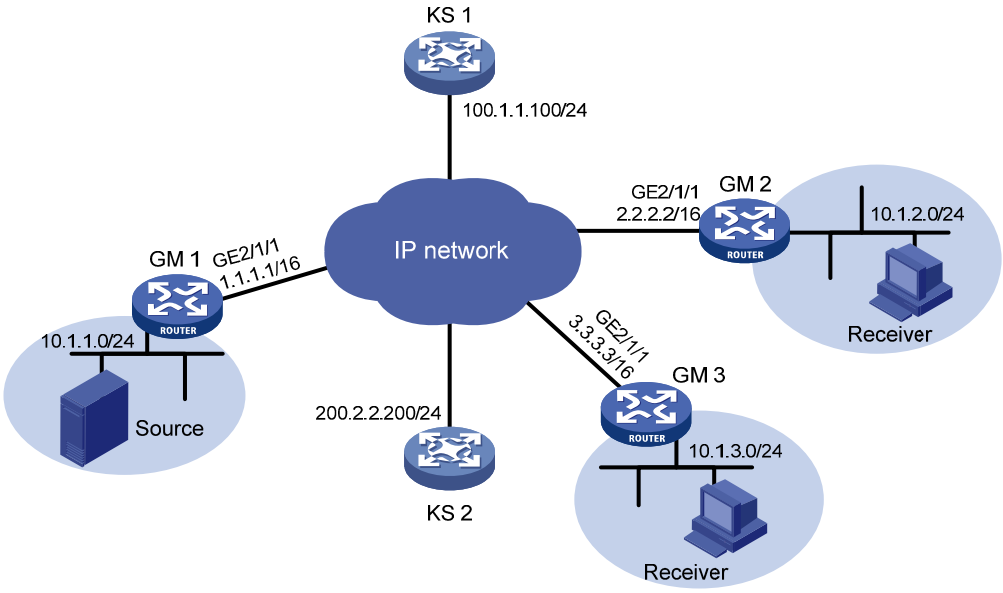
1. 组网需求

在如 图 1-4 所示的组网环境中，需要组建一个Group Domain VPN，对指定子网之间的数据流进行安全保护，具体要求如下：

- 子网 10.1.1.0/24 与子网 10.1.2.0/24 之间的业务流量，以及子网 10.1.1.0/24 与子网 10.1.3.0/24 之间的业务流量受 IPsec 保护。
- GM 1、GM 2 和 GM 3 加入相同的 GDOI 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。
- KS 采用组播方式向 GM 发送 Rekey 消息。
- KS 1 与 KS 2 做冗余备份。KS 1 与 KS 2 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 1、KS 2 之间路由可达。
- 请确保 KS 1 与 KS 2 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，以及 KS 和 GM 之间的组播报文可正常转发。
- 本例中，若 KS 需要采用单播方式发送 Rekey 消息，需要使用 **rekey transport unicast** 命令修改发送 Rekey 消息的模式即可。
- 本例中的 KS 1 和 KS 2 为 Comware V5 版本的设备。

(1) 配置 KS 1

配置各接口的 IP 地址，此处略。

创建 IKE 提议 1。

```
<KS1> system-view
[KS1] ike proposal 1
```

指定 IKE 提议使用的加密算法为 AES-CBC 128。

```
[KS1-ike-proposal-1] encryption-algorithm aes-cbc 128
```

指定 IKE 提议使用的认证算法为 SHA1。

```
[KS1-ike-proposal-1] authentication-algorithm sha
```

指定 IKE 提议使用 DH group 2。

```
[KS1-ike-proposal-1] dh group2
```

```
[KS1-ike-proposal-1] quit
```
创建 IKE 对等体 toks2，用于与 KS 2 之间的 IKE 协商。
```
[KS1] ike peer toks2
```
指定 IKE 对等体 toks2 引用 IKE 提议 1。
```
[KS1-ike-peer-toks2] 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。
```
[KS1-ike-peer-toks2] pre-shared-key simple tempkey1
```
指定对端安全网关的 IP 地址为 200.2.2.200。
```
[KS1-ike-peer-toks2] remote-address 200.2.2.200
[KS1-ike-peer-toks2] quit
```
创建 IKE 对等体 togm，用于与 GM 之间的 IKE 协商。
```
[KS1] ike peer togm
```
指定 IKE 对等体 togm 引用 IKE 提议 1。
```
[KS1-ike-peer-togm] 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。
```
[KS1-ike-peer-togm] pre-shared-key simple tempkey1
[KS1-ike-peer-togm] quit
```
创建 IPsec 安全提议 fortek。
```
[KS1] ipsec transform-set fortek
```
配置 IPsec 安全提议 fortek 使用 ESP 协议。
```
[KS1-ipsec-transform-set-fortek] transform esp
```
配置 IPsec 安全提议 fortek 使用 AES-CBC 128 加密算法。
```
[KS1-ipsec-transform-set-fortek] esp encryption-algorithm aes-cbc-128
```
配置 IPsec 安全提议 fortek 使用 SHA1 认证算法。
```
[KS1-ipsec-transform-set-fortek] esp authentication-algorithm sha1
[KS1-ipsec-transform-set-fortek] quit
```
创建 IPsec 安全框架 fortek。
```
[KS1] ipsec profile fortek
```
配置 IPsec 安全框架 fortek 引用 IPsec 安全提议 fortek
```
[KS1-ipsec-profile-fortek] transform-set fortek
[KS1-ipsec-profile-fortek] quit
```
创建名称为 fortek 的 ACL。
```
[KS1] acl number 3000 name fortek
```
配置 ACL 规则，定义 TEK 保护的流量范围。因为这里业务流量为单播，所以规则要配置为对称的。
```
[KS1-acl-adv-3000-fortek] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination
 10.1.2.0 0.0.0.255
[KS1-acl-adv-3000-fortek] rule 1 permit ip source 10.1.2.0 0.0.0.255 destination
 10.1.1.0 0.0.0.255
[KS1-acl-adv-3000-fortek] rule 2 permit ip source 10.1.1.0 0.0.0.255 destination
 10.1.3.0 0.0.0.255
[KS1-acl-adv-3000-fortek] rule 3 permit ip source 10.1.3.0 0.0.0.255 destination
 10.1.1.0 0.0.0.255
[KS1-acl-adv-3000-fortek] quit
```

创建访问控制列表 forrekey。

```
[KS1] acl number 3001 name forrekey
```

配置 Rekey 的目的地址（组播地址）。

```
[KS1-acl-adv-3001-forrekey] rule 0 permit ip destination 225.0.0.1 0
[KS1-acl-adv-3001-forrekey] quit
```

创建本地 RSA 密钥对，名称为 rsa1。

```
[KS1] public-key local create rsa name rsa1
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
++++++++++++++++
+++++++
+++++++++
+++
```

导出名称为 rsa1 的本地密钥对，导出时使用的加密算法为 3DES CBC，加密口令为 12345678。该导出的密钥对信息被复制后，将用于导入到 KS 2 上。

```
[KS1] public-key local export rsa name rsa1 pem 3des-cbc-128 12345678
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC6Ne4EtnoKqBCL2YZvSjrG+8He
sae5FWtyj9D25PEkXagpLqb3i9Gm/Qbb6cqLLPUIgDS8eK7Wt/dXLeFUCDc0lY8V
gujJPvarFL4+Jn+VuL9znNbboA9IxPH2fMvew8lkPCwkXoP+52J+1LRpYkh+rIpE
Kj7FG/3/wzGsXu8WJQIDAQAB
-----END PUBLIC KEY-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7F8FAB15399DF87C

MGaftNqe4esjetm7bRJHSpsbwZ9YUpvA9iWh8R406NGq8e+1A/ZiK23+t1XqRwaU
1FXnwbqHgW1pZ7JxQdgBuC9uXc4VQyP/xe6xCyUepdMC71fmeOaiwUFrj6LAzzBg
o3SfhX1NHyHBnr7c6SnIeUTG2g/qRdj40TD4HcRjgPaLaTGguZ553GyS6ODWAwL7
ZBTjv+vow9kfewZ74ocoBje2gLcWlbmiEKCJGV06zW4gv2AH6I8TAhv4GovIN/v1
lCsD2PscXnPOloLTE/8EDLRHNE8RpIYDWqI/YI8Yg6wlx29mf29+cj/9r4gPrDPy
c/TQ0a0g95Khdy+yl4eDKaFiQQ+Kqn4zdzDTDNq7LRtqr7lGQzVw6srfrr71ib7J
yJFdi2RXETEgOS/jE+xGtNqd38F/YzIRPax7NNMK+hAJC2MzdbN/BEoLWOqG7Plm
hvCE3LFxelExLJU+0XfAX77TI2+5LEHBi1UiGLeH08fd1XUQCefARlIxGoRJdtTu
gHP4+NF4PC9B1/GZoAYUp+171p1QwPk0vyU3TXijueqVUpQBUHGxSE0UW+SS1iwL
8vsSLHIwK4aZ77Z1o+Uw1QBoqw9jpubG4gUkX8RII8E8b13I6/QTH78E4/FgAmIQ
HTYnE2RDHXkhPGR5FGJsZnd21XLvd2BEkGGmhTk80nDeiI2XH3D48E6UahQwcam/
q/txd/KsLnp0rpJkc/WhOTprioeLQQEBayixKRWzNLsZt3L6lqYbA01Z1THho+EV
0Ng0EZKQyiRV1j7gsBYFRinbSAsIpeYlr7gDAnBCRJdSfPNBKG+ewg==
-----END RSA PRIVATE KEY-----
```

创建 GDOI KS 组 ks1。

```
[KS1] gdoi ks group ks1
```

配置 GDOI KS 组的 ID 为编号 12345。

```
[KS1-gdoi-ks-group-ks1] identity number 12345
```
引用密钥对 rsa1。
```
[KS1-gdoi-ks-group-ks1] rekey authentication public-key rsa rsa1
```
引用名称为 forrekey 的 Rekey ACL。
```
[KS1-gdoi-ks-group-ks1] rekey acl name forrekey
```
创建一个 GDOI KS 组的 IPsec 策略，序号为 10。
```
[KS1-gdoi-ks-group-ks1] ipsec 10
```
引用 IPsec 安全框架 fortek。
```
[KS1-gdoi-ks-group-ks1-ipsec-10] profile fortek
```
引用名称为 fortek 的 ACL。
```
[KS1-gdoi-ks-group-ks1-ipsec-10] security acl name fortek
[KS1-gdoi-ks-group-ks1-ipsec-10] quit
```
配置对端 KS 的 IP 地址为 200.2.2.200。
```
[KS1-gdoi-ks-group-ks1] peer address 200.2.2.200
```
配置 KS 发送报文的源地址为 100.1.1.100。
```
[KS1-gdoi-ks-group-ks1] source address 100.1.1.100
```
配置本端优先级为 10000。
```
[KS1-gdoi-ks-group-ks1] local priority 10000
```
开启冗余备份功能。
```
[KS1-gdoi-ks-group-ks1] redundancy enable
[KS1-gdoi-ks-group-ks1] quit
```
以上配置的具体步骤请参考 KS 的相关配置指导。

(2) 配置 KS 2

配置各接口的 IP 地址，此处略。

创建 IKE 提议 1。
```
<KS2> system-view
[KS2] ike proposal 1
```
指定 IKE 提议使用的加密算法为 AES-CBC 128。
```
[KS2-ike-proposal-1] encryption-algorithm aes-cbc 128
```
指定 IKE 提议使用的认证算法为 SHA1。
```
[KS2-ike-proposal-1] authentication-algorithm sha
```
指定 IKE 提议使用 DH group 2。
```
[KS2-ike-proposal-1] dh group2
[KS2-ike-proposal-1] quit
```
创建 IKE 对等体 toks1，用于与 KS1 之间的 IKE 协商。
```
[KS2] ike peer toks1
```
指定 IKE 对等体 toks1 引用 IKE 提议 1。
```
[KS2-ike-peer-toks1] 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。
```
[KS2-ike-peer-toks1] pre-shared-key simple tempkey1
```
指定对端安全网关的 IP 地址为 100.1.1.100。
```
[KS2-ike-peer-toks1] remote-address 100.1.1.100
[KS2-ike-peer-toks1] quit
```

创建 IKE 对等体 togm，用于与 GM 之间的 IKE 协商。

```
[KS2] ike peer togm
```

指定 IKE 对等体 togm 引用 IKE 提议 1。

```
[KS2-ike-peer-togm] 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。

```
[KS2-ike-peer-togm] pre-shared-key simple tempkey1
[KS2-ike-peer-togm] quit
```

创建 IPsec 安全提议 fortek。

```
[KS2] ipsec transform-set fortek
```

配置 IPsec 安全提议 fortek 使用 ESP 协议。

```
[KS2-ipsec-transform-set-fortek] transform esp
```

配置 IPsec 安全提议 fortek 使用 AES-CBC 128 加密算法。

```
[KS2-ipsec-transform-set-fortek] esp encryption-algorithm aes-cbc-128
```

配置 IPsec 安全提议 fortek 使用 SHA1 认证算法。

```
[KS2-ipsec-transform-set-fortek] esp authentication-algorithm sha1
[KS2-ipsec-transform-set-fortek] quit
```

创建 IPsec 安全框架 fortek。

```
[KS2] ipsec profile fortek
```

配置 IPsec 安全框架 fortek 引用 IPsec 安全提议 fortek。

```
[KS2-ipsec-profile-fortek] transform-set fortek
[KS2-ipsec-profile-fortek] quit
```

创建名称为 fortek 的 ACL。

```
[KS2] acl number 3000 name fortek
```

配置 ACL 规则，定义 TEK 保护的流量范围。

```
[KS2-acl-adv-3000-fortek] rule 0 permit ip source 10.1.1.0 0.0.0.255 destination
 10.1.2.0 0.0.0.255
[KS1-acl-adv-3000-fortek] rule 1 permit ip source 10.1.2.0 0.0.0.255 destination
 10.1.1.0 0.0.0.255
[KS2-acl-adv-3000-fortek] rule 2 permit ip source 10.1.1.0 0.0.0.255 destination
 10.1.3.0 0.0.0.255
[KS1-acl-adv-3000-fortek] rule 3 permit ip source 10.1.3.0 0.0.0.255 destination
 10.1.1.0 0.0.0.255
[KS2-acl-adv-3000-fortek] quit
```

创建访问控制列表 forrekey。

```
[KS2] acl number 3001 name forrekey
```

配置 Rekey 的目的地址（组播地址）。

```
[KS2-acl-adv-3001-forrekey] rule 0 permit ip destination 225.0.0.1 0
[KS2-acl-adv-3001-forrekey] quit
```

将从 KS1 导出的 RSA 密钥以 PEM 格式导入到 KS2，并命名为 rsa1。此导入过程中，需要将从 KS 1 上复制的密钥信息粘贴到本端界面上。

```
[KS2] public-key local import rsa name rsa1 pem
Enter PEM-formatted certificate.
End with a Ctrl+C on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
```

```
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,7F8FAB15399DF87C

MGaftNqe4esjetm7bRJHSpsbwZ9YUpvA9iWh8R406NGq8e+1A/ZiK23+t1XqRwaU
1FXnwbqHgW1pZ7JxQdgBuC9uXc4VQyP/xe6xCyUepdMC71fmeOaiwUFrj6LAzzBg
o3SfhX1NHyHBnr7c6SnIeUTG2g/qRdj40TD4HcRjgPaLaTGguZ553GyS6ODWAwL7
ZBTjv+vow9kfewZ74ocoBje2gLcWlbmiEKCJGV06zW4gv2AH6I8TAhv4GovIN/v1
lCsD2PscXnPOloLTE/8EDLRHNE8RpIYDWqI/YI8Yg6wlx29mf29+cj/9r4gPrDPy
c/TQ0a0g95Khdy+yl4eDKaFiQQ+Kqn4zdzDTDNq7LRtqr7lGQzVw6srfrr71ib7J
yJFdi2RXETEgOS/jE+xGtNqd38F/YzIRPax7NNMK+hAJC2MzdbN/BEoLWOqG7Plm
hvCE3LFxelExLJU+0XfAX77TI2+5LEHBi1UiGLeH08fd1XUQCefARlIxGoRJdtTu
gHP4+NF4PC9B1/GZoAYUp+171p1QwPk0vyU3TXijueqVUpQBUHGxSE0UW+SS1iwL
8vsSLHIwK4aZ77Z1o+Uw1QBoqw9jpubG4gUkX8RII8E8b13I6/QTH78E4/FgAmIQ
HTYnE2RDHXkhPGR5FGJsZnd21XLvd2BEkGGmhTk80nDeiI2XH3D48E6UahQwcam/
q/txd/KsLnp0rpJkc/WhOTprioeLQQEBayixKRWzNLsZt3L6lqYbA01Z1THho+EV
0Ng0EZKQyiRV1j7gsBYFRinbSAsIpeYlr7gDAnBCRJdSfPNBKG+ewg==
-----END RSA PRIVATE KEY-----
^C
Please input the password:
```

创建 GDOI KS 组 ks2。

```
[KS2] gdoi ks group ks2
```

配置 GDOI KS 组的 ID 为编号 12345。

```
[KS2-gdoi-ks-group-ks2] identity number 12345
```

引用密钥对 rsa1。

```
[KS2-gdoi-ks-group-ks2] rekey authentication public-key rsa rsa1
```

引用名称为 forrekey 的 Rekey ACL。

```
[KS2-gdoi-ks-group-ks2] rekey acl name forrekey
```

创建一个 GDOI KS 组的 IPsec 策略，序号为 10。

```
[KS2-gdoi-ks-group-ks2] ipsec 10
```

引用 IPsec 安全框架 fortek。

```
[KS2-gdoi-ks-group-ks2-ipsec-10] profile fortek
```

引用名称为 fortek 的 ACL。

```
[KS2-gdoi-ks-group-ks2-ipsec-10] security acl name fortek
[KS2-gdoi-ks-group-ks2-ipsec-10] quit
```

配置对端 KS 的 IP 地址为 100.1.1.100。

```
[KS2-gdoi-ks-group-ks2] peer address 100.1.1.100
```

配置 KS 发送报文的源地址为 200.2.2.200。

```
[KS2-gdoi-ks-group-ks2]source address 200.2.2.200
```

配置本端优先级为 100。

```
[KS2-gdoi-ks-group-ks2] local priority 100
```

开启冗余备份功能。

```
[KS2-gdoi-ks-group-ks2] redundancy enable
```

(3)　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 提议使用的认证算法为 SHA1。
```
[GM1-ike-proposal-1] authentication-algorithm sha
```
指定 IKE 提议使用 DH group 2。
```
[GM1-ike-proposal-1] dh group2
[GM1-ike-proposal-1] quit
```
创建 IKE keychain，名称为 keychain1。
```
[GM1] ike keychain keychain1
```
配置与 IP 地址为 100.1.1.100 的对端使用的预共享密钥为明文 tempkey1。
```
[GM1-ike-keychain-keychain1] pre-shared-key address 100.1.1.100 255.255.255.0 key simple
tempkey1
[GM1-ike-keychain-keychain1] quit
```
创建 IKE keychain，名称为 keychain2。
```
[GM1] ike keychain keychain2
```
配置与 IP 地址为 200.2.2.200 的对端使用的预共享密钥为明文 tempkey1。
```
[GM1-ike-keychain-keychain2] pre-shared-key address 200.2.2.200 255.255.255.0 key simple
tempkey1
[GM1-ike-keychain-keychain2] quit
```
创建并配置 IKE profile，名称为 profile1。
```
[GM1] ike profile profile1
[GM1-ike-profile-profile1] proposal 1
[GM1-ike-profile-profile1] keychain keychain1
[GM1-ike-profile-profile1] keychain keychain2
[GM1-ike-profile-profile1] match remote identity address 100.1.1.100 255.255.255.0
[GM1-ike-profile-profile1] match remote identity address 200.2.2.200 255.255.255.0
[GM1-ike-profile-profile1] quit
```
创建 GDOI GM 组 1。
```
[GM1] gdoi gm group 1
```
配置 GDOI GM 组的 ID 为编号 12345。
```
[GM1-gdoi-gm-group-1] identity number 12345
```
指定 GDOI GM 组的 KS 地址为 100.1.1.100 和 200.2.2.200。
```
[GM1-gdoi-gm-group-1] server address 100.1.1.100
[GM1-gdoi-gm-group-1] server address 200.2.2.200
[GM1-gdoi-gm-group-1] quit
```
创建 GDOI 类型的 IPsec 安全策略 1。
```
[GM1] ipsec policy map 1 gdoi
```
引用 GDOI GM 组 1。
```
[GM1-ipsec-policy-gdoi-map-1] group 1
[GM1-ipsec-policy-gdoi-map-1] quit
```
在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map。
```
[GM1] interface gigabitethernet 2/1/1
[GM1-GigabitEthernet2/1/1] ipsec apply policy map
```

```
[GM1-GigabitEthernet2/1/1] quit
```

(4) 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 DH group 2。

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

创建 IKE keychain，名称为 keychain1。

```
[GM2] ike keychain keychain1
```

配置与 IP 地址为 100.1.1.100 的对端使用的预共享密钥为明文 tempkey1。

```
[GM2-ike-keychain-keychain1] pre-shared-key address 100.1.1.100 255.255.255.0 key simple
tempkey1
[GM2-ike-keychain-keychain1] quit
```

创建 IKE keychain，名称为 keychain2。

```
[GM2] ike keychain keychain2
```

配置与 IP 地址为 200.2.2.200 的对端使用的预共享密钥为明文 tempkey1。

```
[GM2-ike-keychain-keychain2] pre-shared-key address 200.2.2.200 255.255.255.0 key simple
tempkey1
[GM2-ike-keychain-keychain2] quit
```

创建并配置 IKE profile，名称为 profile1。

```
[GM2] ike profile profile1
[GM2-ike-profile-profile1] proposal 1
[GM2-ike-profile-profile1] keychain keychain1
[GM2-ike-profile-profile1] keychain keychain2
[GM2-ike-profile-profile1] match remote identity address 100.1.1.100 255.255.255.0
[GM2-ike-profile-profile1] match remote identity address 200.2.2.200 255.255.255.0
[GM2-ike-profile-profile1] quit
```

创建 GDOI GM 组 1。

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

配置 GDOI GM 组的 ID 为编号 12345。

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

指定 GDOI GM 组的 KS 地址为 100.1.1.100 和 200.2.2.200。

```
[GM2-gdoi-gm-group-1] server address 100.1.1.100
[GM2-gdoi-gm-group-1] server address 200.2.2.200
[GM2-gdoi-group-1] quit
```

创建 GDOI 类型 IPsec 安全策略 1。

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

引用 GDOI GM 组 1。

```
[GM2-ipsec-policy-gdoi-map-1] group 1
[GM2-ipsec-policy-gdoi-map-1] quit
```
在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map。
```
[GM2] interface gigabitethernet 2/1/1
[GM2-GigabitEthernet2/1/1] ipsec apply policy map
[GM2-GigabitEthernet2/1/1] quit
```
(5) 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 提议使用的认证算法为 SHA1。
```
[GM3-ike-proposal-1] authentication-algorithm sha
```
指定 IKE 提议使用 DH group 2。
```
[GM3-ike-proposal-1] dh group2
[GM3-ike-proposal-1] quit
```
创建 IKE keychain，名称为 keychain1。
```
[GM3] ike keychain keychain1
```
配置与 IP 地址为 100.1.1.100 的对端使用的预共享密钥为明文 tempkey1。
```
[GM3-ike-keychain-keychain1] pre-shared-key address 100.1.1.100 255.255.255.0 key simple
tempkey1
[GM3-ike-keychain-keychain1] quit
```
创建 IKE keychain，名称为 keychain2。
```
[GM3] ike keychain keychain2
```
配置与 IP 地址为 200.2.2.200 的对端使用的预共享密钥为明文 tempkey1。
```
[GM3-ike-keychain-keychain2] pre-shared-key address 200.2.2.200 255.255.255.0 key simple
tempkey1
[GM3-ike-keychain-keychain2] quit
```
创建并配置 IKE profile，名称为 profile1。
```
[GM3] ike profile profile1
[GM3-ike-profile-profile1] proposal 1
[GM3-ike-profile-profile1] keychain keychain1
[GM3-ike-profile-profile1] keychain keychain2
[GM3-ike-profile-profile1] match remote identity address 100.1.1.100 255.255.255.0
[GM3-ike-profile-profile1] match remote identity address 200.2.2.200 255.255.255.0
[GM3-ike-profile-profile1] quit
```
创建 GDOI GM 组 1。
```
[GM3] gdoi gm group 1
```
配置 GDOI GM 组的 ID 为编号 12345。
```
[GM3-gdoi-gm-group-1] identity number 12345
```
指定 GDOI GM 组的 KS 地址为 100.1.1.100 和 200.2.2.200。
```
[GM3-gdoi-gm-group-1] server address 100.1.1.100
[GM3-gdoi-gm-group-1] server address 200.2.2.200
```

```
[GM3-gdoi-gm-group-1] quit
```

创建 GDOI 类型 IPsec 安全策略 1。

```
[GM3] ipsec policy map 1 gdoi
```

引用 GDOI GM 组 1。

```
[GM3-ipsec-policy-gdoi-map-1] group 1
[GM3-ipsec-policy-gdoi-map-1] quit
```

在接口 GigabitEthernet2/1/1 上应用 IPsec 安全策略 map。

```
[GM3] interface gigabitethernet 2/1/1
[GM3-GigabitEthernet2/1/1] ipsec apply policy map
[GM3-GigabitEthernet2/1/1] 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 1 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 1 的 SA 为 IKE SA；connection-id 为 2 的 SA 为 Rekey SA。

```
[GM1] display ike sa
    Connection-ID  Remote           Flag        DOI
  -------------------------------------------------------------
      1            100.1.1.100      RD          Group
      2            100.1.1.100      RD|RK       Group
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

IKE 协商成功后，GM 1 获取到 IPsec SA。可通过如下显示信息查看到有四组 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: GigabitEthernet2/1/1
------------------------------

  ----------------------------
  IPsec policy: map
  Sequence number: 1
  Mode: GDOI
  ----------------------------
    Encapsulation mode: tunnel
    Path MTU: 1443
    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: 801701189 (0x2fc8fd45)

    [Inbound ESP SAs]
      SPI: 801701189 (0x2fc8fd45)
      Connection ID: 5
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 0/900
```

```
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 20
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active

  [Outbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 6
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 21
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active

------------------------------
IPsec policy: map
Sequence number: 1
Mode: GDOI
------------------------------
  Encapsulation mode: tunnel
  Path MTU: 1443
  Flow:
      sour addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 10.1.3.0/255.255.255.0  port: 0  protocol: ip

  Current outbound SPI: 801701189 (0x2fc8fd45)

  [Inbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 7
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 22
```

```
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active

  [Outbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 8
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 23
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active

------------------------------
IPsec policy: map
Sequence number: 1
Mode: GDOI
------------------------------
  Encapsulation mode: tunnel
  Path MTU: 1443
  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: 801701189 (0x2fc8fd45)

  [Inbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 45
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 46
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active
```

```
  [Outbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 43
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 44
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active

-----------------------------
IPsec policy: map
Sequence number: 1
Mode: GDOI
-----------------------------
  Encapsulation mode: tunnel
  Path MTU: 1443
  Flow:
      sour addr: 10.1.3.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 10.1.1.0/255.255.255.0  port: 0  protocol: ip

  Current outbound SPI: 801701189 (0x2fc8fd45)

  [Inbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 24
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 25
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active

  [Outbound ESP SAs]
    SPI: 801701189 (0x2fc8fd45)
    Connection ID: 12
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
```

```
    SA remaining duration (kilobytes/sec): 0/63
    Status: Active

    SPI: 1611821838 (0x6012730e)
    Connection ID: 13
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 0/900
    SA remaining duration (kilobytes/sec): 0/850
    Status: Active
```

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 gm
Group name: 1

  Group identity             : 12345
  Address family             : IPv4
  Rekeys received            : 1

  Group server               : 100.1.1.100
  Group server               : 200.2.2.200

  Group member               : 1.1.1.1
    Registration status      : Registered
    Registered with          : 100.1.1.100
    Re-register in           : 3226 sec
    Succeeded registrations  : 1
    Attempted registrations  : 1
    Last rekey from          : 100.1.1.100
    Last rekey seq num       : 1
    Multicast rekeys received: 1

  Allowable rekey cipher     : Any
  Allowable rekey hash       : Any
  Allowable transform        : Any

  Rekeys cumulative:
    Total received                  : 1
    Rekeys after latest registration: 1
    Last rekey received for         : 00hr 04min 41sec

  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
    rule 2 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
    rule 3 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255

  KEK:
    Rekey transport type        : Multicast
```

```
    Remaining key lifetime      : 86119 sec
    Encryption algorithm        : 3DES-CBC
    Signature algorithm         : RSA
    Signature hash algorithm    : SHA1
    Signature key length        : 1024 bits

  TEK:
    SPI                         : 0x2FC8FD45(801701189)
    Transform                   : ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    Remaining key lifetime      : 900 sec

    SPI                         : 0x6012730E(1611821838)
    Transform                   : ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    Remaining key lifetime      : 3319 sec
```

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。

在 KS 1 上可以看到 GM 的注册信息。

```
<KS1> display gdoi ks members
Group Name: ks1
  Group member ID      : 1.1.1.1
  Group member version : 1.0
  Group ID             : 12345
  Rekeys sent          : 0
  Rekey retries        : 0
  Rekey ACKs received  : 0
  Rekey ACKs missed    : 0

  Group member ID      : 2.2.2.2
  Group member version : 1.0
  Group ID             : 12345
  Rekeys sent          : 0
  Rekey retries        : 0
  Rekey ACKs received  : 0
  Rekey ACKs missed    : 0

  Group member ID      : 3.3.3.3
  Group member version : 1.0
  Group ID             : 12345
  Rekeys sent          : 0
  Rekey retries        : 0
  Rekey ACKs received  : 0
  Rekey ACKs missed    : 0
```

类似地，在 KS 2 上也可以看到所有 GM 的注册信息。

在 KS 1 上可以看到与 KS 2 之间的冗余备份相关信息。

```
<KS1> display gdoi ks redundancy
Group Name :ks1
```

```
  Local address   : 100.1.1.100
  Local version   : 1.0
  Local priority  : 10000
  Local role      : Primary
  Primary address : 100.1.1.100

  Sessions:
      Peer address  : 200.2.2.200
      Peer version  : 1.0
      Peer priority : 100
      Peer role     : Secondary
      Peer status   : Ready
```

在 KS 2 上可以看到与 KS 1 之间的冗余备份相关信息。

```
<KS2> display gdoi ks redundancy
Group Name :ks2
  Local address   : 200.2.2.200
  Local version   : 1.0
  Local priority  : 100
  Local role      : Secondary
  Primary address : 100.1.1.100

  Sessions:
      Peer address  : 100.1.1.100
      Peer version  : 1.0
      Peer priority : 10000
      Peer role     : Primary
      Peer status   : Ready
```