SGX808

IPsec 功能

雅马哈株式会社

2016 年 1 月　第 2.01 版

Copyright© 2014-2016 Yamaha Corporation

更新记录

更新日期	版本	说明
2014.05.29	1.00	初版发行
2015.02.04	2.00	• 可以执行 2 个对话。 • 可以指定主机名称作为目的地信息。 • 可以设置 IPsec 作为默认路由。
2016.01.15	2.01	• 追加了 Responder 功能。 • 追加了设置示例。

Copyright© 2014-2016 Yamaha Corporation

目录

Copyright© 2014-2016 Yamaha Corporation

Copyright© 2014-2016 Yamaha Corporation

1 概要

本文档中记述了 SGX808 的 IPsec 功能。可以设置本功能的有效或无效，以及 IPsec 功能的必要信息。

功能上，可以执行 2 个对话，可分别对每个对话的 Aggressive mode 或 Main mode，设置 Initiator 或 Responder 运行。

2 限制条件

本功能设置了下述限制条件。

1. IKE(Internet Key Exchange)仅支持 Version 1。
2. IKE 使用的群仅支持 modp1024。在阶段 1 和阶段 2 中，都要求使用 modp1024。
3. 仅支持隧道模式。
4. 设置了 Responder 时
   - 把设置的 1 个目的地作为 Initiator 使用。无法把非指定目的地作为 Initiator 使用。
   - 设置了 Responder 的 IPsec 隧道，不能作为 Default Gateway 使用。
   - 加密算法及认证算法遵从 Initiator 端的设置。
   - 认证算法中不能使用 sha256。

3 支持的机型和固件版本

SGX808 通过下述固件使用 IPsec 功能。

表 3.1 支持的机型和固件版本

机型	固件	修订内容
SGX808	Rev.1.00.03 及更高版本	新版
	Rev.1.00.08 及更高版本	• 可以执行 2 个对话。 • 可以指定主机名称作为目的地信息。 • 可以设置 IPsec 作为默认路由。
	Rev.1.00.15 及更高版本	• 追加了 Responder 功能。

4 详细

在 Web 设置画面的[Network]选项卡内的[**网络设置**]-[IPsec]页面上，设置 IPsec 功能。支持 NAT Traversal，运行时自动检测是否有 NAT。NAT 的 keepalive 的发送间隔为 20 秒。该值不能更改。

Copyright© 2014-2016 Yamaha Corporation

4.1 IPsec 的有效和无效

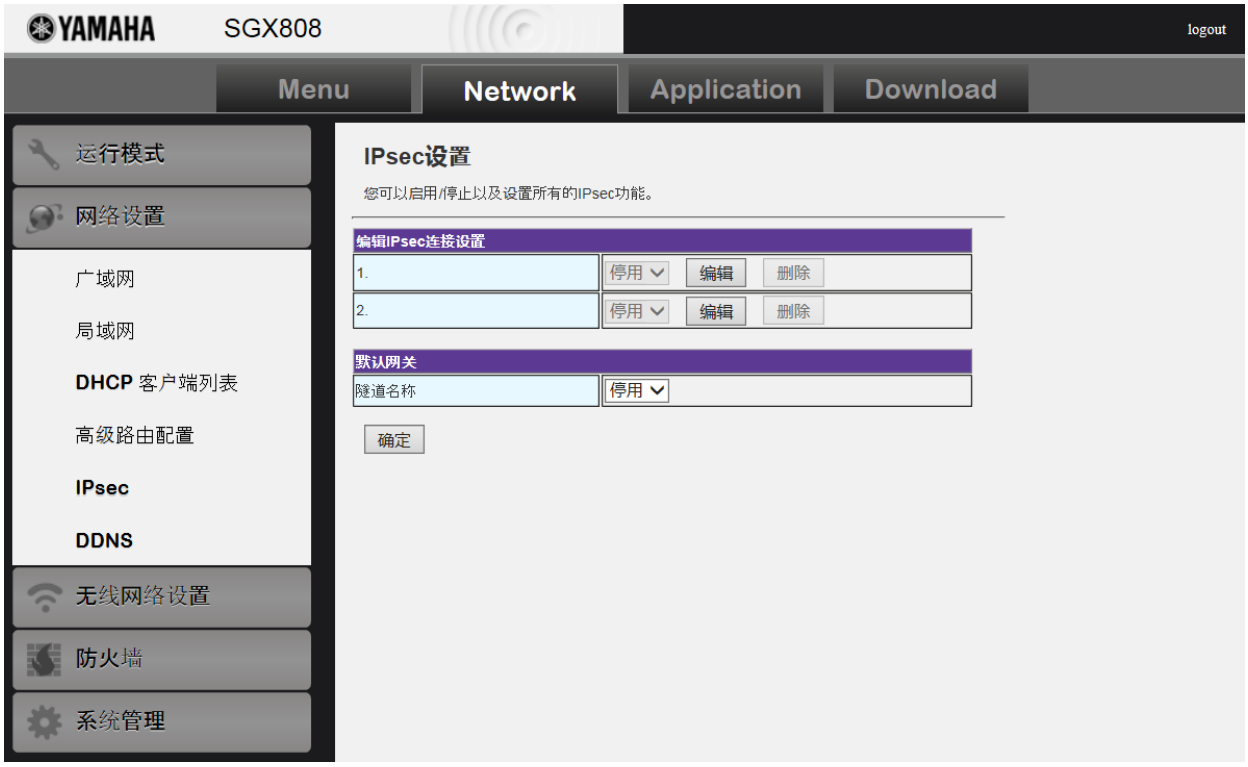

图 4.1 IPsec 的有效和无效

4.1.1 编辑 IPsec 连接设置

可以对每个连接信息分别设置"**启用**" / "**停用**"。没有设置连接信息时无法选择该项。（默认："**停用**"）

4.1.2 默认网关

从下拉菜单上选择隧道名称，设置作为默认路由的隧道。（默认："**停用**"）

需要注意的是，如果把该设置设为"**停用**"以外的其他内容，向 WAN 端发送的信息包将全部进入设置的隧道中，所以需要在［**网络设置**］-［**高级路由配置**］中事先设置不受该项限制的路由。

此外，设置了 2 个隧道，其中一个设为默认路由时，2 个隧道分别确立之后，所有的信息包将发送到设为默认路由的隧道中。对于发送目的为位于另一个隧道前方的网络段的信息包，由于已经默认设置了路由，所以不会向默认路由发送，而是发送给另一个隧道。

Copyright© 2014-2016 Yamaha Corporation

4.1.3 "编辑"按钮

进入个别连接信息设置画面。

4.1.4 "删除"按钮

删除个别连接信息。没有设置连接信息的状态下，无法执行该项。

4.1.5 "确定"按钮

把设置的信息应用到运行中。设置 2 个隧道后，其中一个隧道为连接状态，更改了另一个隧道的“Enable/Disable”时，处于连接状态的隧道将保持该状态，无需重新连接。更改了默认路由时，将断开处于连接状态的隧道，然后重新连接。

Copyright© 2014-2016 Yamaha Corporation

4.2 设置连接信息

可以对 2 处连接目标，分别设置下述信息。

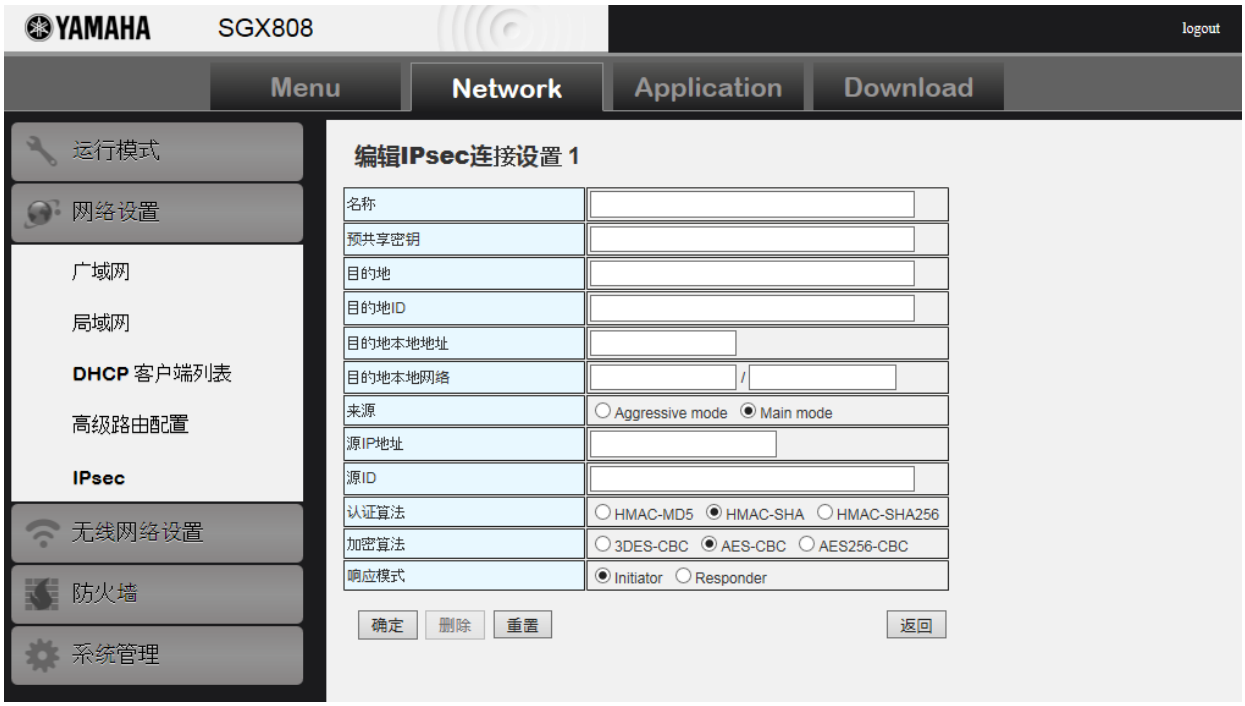

图 4.2 设置连接状态

4.2.1 名称

设置 IPsec 对话的名称。不可省略。不能把 2 个对话设为相同名称。ASCII 字符 32bytes（默认：无）。禁止使用下述字符。

""（双引号）、'='（等号）、'#'（井号）、' '（空白）
';'（分号）、'(',')'（括号）、'`'（反引号）、'\'（反斜线）
'*'（星号）、"'（单引号）、'|'（竖线）、'~'（波浪号）

4.2.2 预共享密钥

IPsec 使用密钥转换协议 IKE(Internet Key Exchange)。不可省略。所需密钥由 IKE 自动生成，但需要在此处设置作为该密钥种类的预共享密钥(PSK:Pre-Shared-Key)。ASCII 字符 128bytes（默认：无）。禁止使用""(双引号)。

4.2.3 目的地

设置目的地信息（IP 地址或 FQDN）。不可省略。ASCII 字符 256bytes（默认：无）。禁止使用下述字符。

""（双引号）、'='（等号）、'#'（井号）、' '（空白）

Copyright© 2014-2016 Yamaha Corporation

4.2.4 目的地 ID

设置目的地的 ID。不可省略。ASCII 字符 256bytes（默认：无）。禁止使用下述字符。

""（双引号）、'='（等号）、'#'（井号）、' '（空白）

4.2.5 目的地本地地址

设置目的地中设置的本地 IP 地址。不可省略。（默认：无）

4.2.6 目的地本地网络

设置目的地中设置的本地网络地址和子网掩码地址。不可省略。（默认：无）

4.2.7 来源

从下述 2 个选项中选择连接模式。

"Aggressive mode"、"Main mode"（默认）

4.2.8 源 IP 地址

设置本机 WAN 端的 IP 地址。不可省略。选择"Aggressive mode"时，该项不可输入。

4.2.9 源 ID

设置 IKE 的阶段 2 中使用的自己一方的 ID。不可省略。选择"Aggressive mode"时，该项为必填项目。ASCII 字符 256bytes（默认：无）。禁止使用下述字符。

""（双引号）、'='（等号）、'#'（井号）、' '（空白）

4.2.10 认证算法

从下述 3 项中选择认证算法。

"HMAC-MD5"、"HMAC-SHA"（默认）、"HMAC-SHA256"

4.2.11 加密算法

从下述 3 项中选择加密算法。

"3DES-CBC"、"AES-CBC"（默认）、"AES256-CBC"

Copyright© 2014-2016 Yamaha Corporation

4.2.12 响应模式

从下述 2 个选项中选择响应方法。

"Initiator"（默认）、"Responder"

4.2.13 "确定"按钮

存储设置的信息，返回之前的画面。基本设置(4.1 IPsec 的有效和无效)为"Enable"时，根据设置内容开始运行。设为"启用"时，虽然存储设置内容，但不会开始运行。

4.2.14 "删除"按钮

删除设置的信息，返回之前的画面。已经处于执行（连接）状态时，将退出（切断）操作。

4.2.15 "重置"按钮

把输入中途的设置信息，返回到按下“确定”按钮之前的状态。

4.2.16 "返回"按钮

返回之前的画面。废弃输入中途的信息。

Copyright© 2014-2016 Yamaha Corporation

4.3 状态参照

可以在 Web 设置画面的［**系统管理**］-［**状态**］页面上，确认连接状态。

IPsec信息

名称	hoge
状态	Connections: hoge: %any...10.10.10.200 64 IKEv1 Aggressive hoge: local: [XXXXXX] uses pre-shared key authentication hoge: remote: [192.168.1.1] uses pre-shared key authentication hoge: child: 192.168.100.0/24 === 192.168.1.0/24 TUNNEL Routed Connections: hoge{1}: ROUTED, TUNNEL hoge{1}: 192.168.100.0/24 === 192.168.1.0/24 Security Associations (2 up, 0 connecting): hoge[1]: ESTABLISHED 24 seconds ago, 10.10.10.201[XXXXXX]...10.10.10.200[192.168.1.1] hoge[1]: IKEv1 SPIs: 2d0d86eacd9e6e92_i* a2adeda810252184_r, pre-shared key reauthentication in 55 minutes hoge[1]: IKE proposal: AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024 hoge{1}: INSTALLED, TUNNEL, ESP SPIs: c6528c6d_i b8d8661f_o hoge{1}: AES_CBC_128/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 14 minutes hoge{1}: 192.168.100.0/24 === 192.168.1.0/24
名称	hogehoge
状态	Connections: hogehoge: 10.10.10.201...10.10.10.209 IKEv1 hogehoge: local: [10.10.10.201] uses pre-shared key authentication hogehoge: remote: [192.168.2.1] uses pre-shared key authentication hogehoge: child: 192.168.100.0/24 === 192.168.2.0/24 TUNNEL Routed Connections: hogehoge{2}: ROUTED, TUNNEL hogehoge{2}: 192.168.100.0/24 === 192.168.2.0/24 Security Associations (2 up, 0 connecting): hogehoge[2]: ESTABLISHED 23 seconds ago, 10.10.10.201[133.176.179.160]...10.10.10.209[192.168.2.1] hogehoge[2]: IKEv1 SPIs: 87f08e4b4c7b4d39_i* 92ff51f08e662310_r, pre-shared key reauthentication in 56 minutes hogehoge[2]: IKE proposal: AES_CBC_128/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_1024 hogehoge{2}: INSTALLED, TUNNEL, ESP SPIs: c7ea6100_i cb96dea0_o hogehoge{2}: AES_CBC_128/HMAC_SHA2_256_128, 0 bytes_i, 0 bytes_o, rekeying in 16 minutes hogehoge{2}: 192.168.100.0/24 === 192.168.2.0/24

图 4.3 状态参照

Copyright© 2014-2016 Yamaha Corporation

5 设置示例

5.1 Initiator

以 SGX808 为 Initiator、连接目的地的 RTX1200 为 Responder 作为运行示例进行说明。

5.1.1 Main mode

以连接模式为 Main mode 作为示例进行说明。

- 结构示例

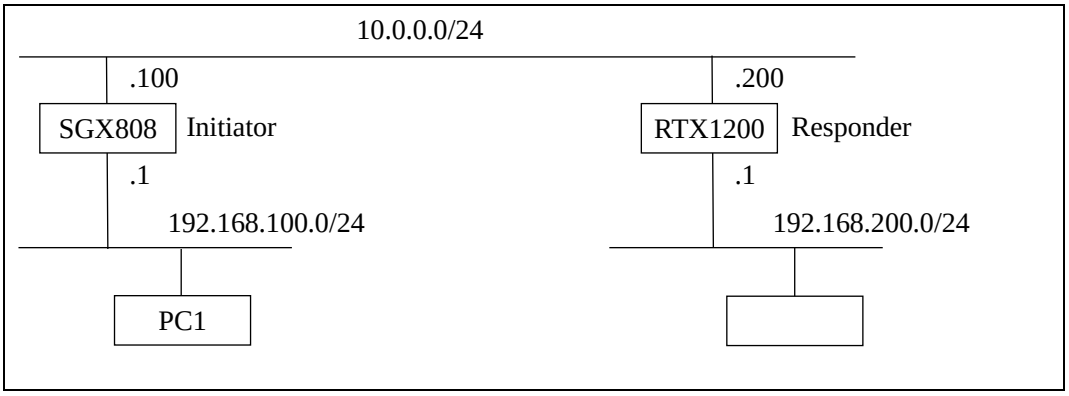

图 5.1.1-1 结构示例

SGX808

LAN 端地址：192.168.100.1

WAN 端地址：10.0.0.100

RTX1200

LAN 端地址：192.168.200.1

WAN 端地址：10.0.0.200

- RTX1200 的设置示例

```
ip route 192.168.100.0/24 gateway tunnel 1
ip lan1 address 192.168.200.1/24                ...(*4)
ip lan2 address 10.0.0.200/24                   ...(*2)
ip lan2 nat descriptor 1

tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac      ...(*5)
  ipsec ike local address 1 192.168.200.1
  ipsec ike local id 1 192.168.200.1            ...(*3)
  ipsec ike backward-compatibility 1 2
  ipsec ike pre-shared-key 1 text test          ...(*1)
```

Copyright© 2014-2016 Yamaha Corporation

```
  ipsec ike remote address 1 10.0.0.100
  ipsec ike send info 1 off
 tunnel enable 1

nat descriptor type 1 masquerade
nat descriptor address outer 1 primary
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
```

图 5.1.1-2　RTX1200 的设置示例

ip route 192.168.100.0/24 gateway tunnel 1

把到达目的地 LAN 的路由设为隧道。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

对 LAN1 和 LAN2 设置固定地址。

ip lan2 nat descriptor 1

nat descriptor type 1 masquerade

nat descriptor address outer 1 primary

nat descriptor address inner 1 auto

nat descriptor masquerade static 1 1 192.168.200.1 udp 500

nat descriptor masquerade static 1 2 192.168.200.1 esp

对 LAN2 接口设置 NAT 地址伪装。

ipsec tunnel 1

tunnel enable 1

设置应用 IPsec 定义和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac

ipsec ike pre-shared-key 1 text test

设置针对目的地安全网关的 SA 策略。

Pre-Shared-Key 设为与目的地相同。

ipsec ike local address 1 192.168.200.1

ipsec ike local id 1 192.168.200.1

ipsec ike remote address 1 10.0.0.100

Copyright© 2014-2016 Yamaha Corporation

在 local address 和 id 中设置 LAN1 端的地址。

在 remote address 中设置目的地 WAN 端的地址。

ipsec ike backward-compatibility 1 2

把 IKEv1 密钥转换类型设为 2。

※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。

※本命令追加与固件版本 Rev.10.01.55 及更高版本中。

ipsec ike send info 1 off

设置不发送 IKE 的信息有效载荷。

SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- SGX808 的设置示例

表 5.1.1 SGX808 的设置示例

项目	说明	设置示例
名称	设置适当的名称。	example
预共享密钥	设置与目的地设置相同的 Pre-Shared-Key。 （RTX1200 的设置示例(*1)）	test
目的地	设置目的地地址。 （RTX1200 的设置示例(*2)）	10.0.0.200
目的地 ID	设置目的地 ID。 （RTX1200 的设置示例(*3)）	192.168.200.1
目的地本地地址	设置目的地的本地 IP 地址。 （RTX1200 的设置示例(*4)）	192.168.200.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0 / 255.255.255.0
来源	选择"Main mode"。	"Main mode"
源 IP 地址	设置 WAN 端的 IP 地址。	10.0.0.100
源 ID	无需设置。	(空白)
认证算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“HMAC-SHA”
加密算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“AES-CBC”
响应模式	选择"Initiator"。	"Initiator"

Copyright© 2014-2016 Yamaha Corporation

5.1.2 Aggressive mode

以连接模式为 Aggressive mode 作为示例进行说明。

- 结构示例

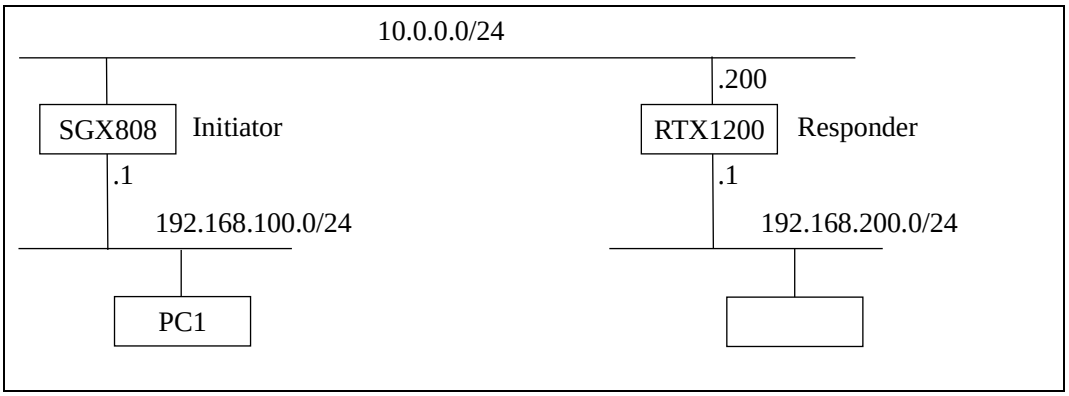

图 5.1.2-1 结构示例

SGX808

LAN 端地址：192.168.100.1

WAN 端地址：不固定

RTX1200

LAN 端地址：192.168.200.1

WAN 端地址：10.0.0.200

- RTX1200 的设置示例

```
ip route 192.168.100.0/24 gateway tunnel 1
ip lan1 address 192.168.200.1/24                ...(*4)
ip lan2 address 10.0.0.200/24                   ...(*2)
ip lan2 nat descriptor 1

tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac      ...(*5)
  ipsec ike local address 1 192.168.200.1
  ipsec ike local id 1 192.168.200.1            ...(*3)
  ipsec ike backward-compatibility 1 2
  ipsec ike payload type 1 3
  ipsec ike pre-shared-key 1 text test          ...(*1)
  ipsec ike remote address 1 any
  ipsec ike remote name 1 XXXXXX key-id         ...(*6)
  ipsec ike send info 1 off
```

Copyright© 2014-2016 Yamaha Corporation

```
 tunnel enable 1


nat descriptor type 1 masquerade
nat descriptor address outer 1 primary
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
```

图 5.1.2-2　RTX1200 的设置示例

ip route 192.168.100.0/24 gateway tunnel 1

把到达目的地 LAN 的路由设为隧道。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

对 LAN1 和 LAN2 设置固定地址。

ip lan2 nat descriptor 1

nat descriptor type 1 masquerade

nat descriptor address outer 1 primary

nat descriptor address inner 1 auto

nat descriptor masquerade static 1 1 192.168.200.1 udp 500

nat descriptor masquerade static 1 2 192.168.200.1 esp

对 LAN2 接口设置 NAT 地址伪装。

ipsec tunnel 1

tunnel enable 1

设置应用 IPsec 定义和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac

ipsec ike pre-shared-key 1 text test

设置针对目的地安全网关的 SA 策略。

Pre-Shared-Key 设为与目的地相同。

ipsec ike backward-compatibility 1 2

把 IKEv1 密钥转换类型设为 2。

※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。

※本命令追加于固件版本 Rev.10.01.55 及更高版本中。

Copyright© 2014-2016 Yamaha Corporation

ipsec ike payload type 1 3

ipsec ike remote address 1 any

ipsec ike remote name 1 XXXXXX key-id

把 payload 的类型设为 3。

由于目的地的全局地址不固定，所以在 remote address 设置 any。

设置目的地安全网关的名称(XXXXXX)。

执行这些设置后，将作为 Aggressive mode 的 responder 运行。

ipsec ike local address 1 192.168.200.1

ipsec ike local id 1 192.168.200.1

在 local address 和 id 中设置 LAN1 端的地址。

ipsec ike send info 1 off

设置不发送 IKE 的信息有效载荷。

SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- SGX808 的设置示例

表 5.1.2 SGX808 的设置示例

项目	说明	设置示例
名称	设置适当的名称。	example
预共享密钥	设置与目的地设置相同的 Pre-Shared-Key。 （RTX1200 的设置示例(*1)）	test
目的地	设置目的地地址。 （RTX1200 的设置示例(*2)）	10.0.0.200
目的地 ID	设置目的地 ID。 （RTX1200 的设置示例(*3)）	192.168.200.1
目的地本地地址	设置目的地的本地 IP 地址。 （RTX1200 的设置示例(*4)）	192.168.200.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0 / 255.255.255.0
来源	选择"Aggressive mode"。	"Aggressive mode"
源 IP 地址	已选择"Aggressive mode"，所以无法设置。	
源 ID	设置与目的地相同的 key-id。 （RTX1200 的设置示例(*6)）	XXXXXX
认证算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“HMAC-SHA”

Copyright© 2014-2016 Yamaha Corporation

加密算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“AES-CBC”
响应模式	选择"Initiator"。	"Initiator"

Copyright© 2014-2016 Yamaha Corporation

5.1.3 Aggressive mode（on PPPoE）

以需要设置 PPPoE 作为示例进行说明。

- 结构示例

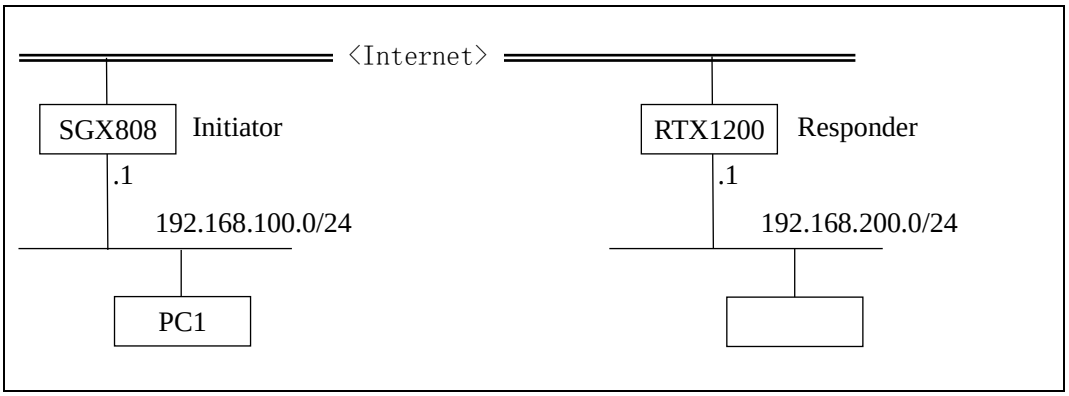

图 5.1.3-1　结构示例

SGX808

LAN 端地址：192.168.100.1

WAN 端地址：不固定

RTX1200

LAN 端地址：192.168.200.1

WAN 端地址：不固定

WAN 端主机名：xxx.yyy.netvolante.jp

事先由 Netvolante DNS 服务等分配的名称

- RTX1200 的设置示例

```
ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
ip lan1 address 192.168.200.1/24                    ...(*4)

pp select 1
 pppoe use lan2
 pp auth accept pap chap
 pp auth myname [userID] [PASS]
 ppp lcp mru on 1454
 ppp ipcp ipaddress on
 ppp ipcp msext on
 ppp ccp type none
 ip pp nat descriptor 1
 netvolante-dns hostname host pp 1 xxx.yyy.netvolante.jp   ...(*2)
```

Copyright© 2014-2016 Yamaha Corporation

```
 pp enable 1

tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac                ...(*5)
  ipsec ike local address 1 192.168.200.1
  ipsec ike local id 1 192.168.200.1                      ...(*3)
  ipsec ike backward-compatibility 1 2
  ipsec ike payload type 1 3
  ipsec ike pre-shared-key 1 text test                    ...(*1)
  ipsec ike remote address 1 any
  ipsec ike remote name 1 XXXXXX key-id                   ...(*6)
  ipsec ike send info 1 off
 tunnel enable 1

nat descriptor type 1 masquerade
nat descriptor address outer 1 ipcp
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
```

图 5.1.3-2　RTX1200 的设置示例

ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1

把默认路由设为 pp。
把到达目的地 LAN 的路由设为隧道。

ip lan1 address 192.168.200.1/24

对 LAN1 设置固定地址。

pp select 1
pppoe use lan2
pp auth accept pap chap
pp auth myname [userID] [PASS]
ppp lcp mru on 1454
ppp ipcp ipaddress on ppp ipcp msext on
ppp ccp type none
netvolante-dns hostname host pp 1 xxx.yyy.netvolante.jp pp enable 1

Copyright© 2014-2016 Yamaha Corporation

设置 PPPoE。同时注册主机名。

ip pp nat descriptor 1
nat descriptor type 1 masquerade
nat descriptor address outer 1 ipcp
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
对 pp 接口设置 NAT 地址伪装。
WAN 的 IP 地址使用 PPP 的连接目标通知的 IP 地址。

ipsec tunnel 1
tunnel enable 1
设置应用 IPsec 定义和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac
ipsec ike pre-shared-key 1 text test
设置针对目的地安全网关的 SA 策略。
Pre-Shared-Key 设为与目的地相同。

ipsec ike backward-compatibility 1 2
把 IKEv1 密钥转换类型设为 2。
※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。
※本命令追加于固件版本 Rev.10.01.55 及更高版本中。

ipsec ike payload type 1 3
ipsec ike remote address 1 any
ipsec ike remote name 1 XXXXXX key-id
把 payload 的类型设为 3。
由于目的地的全局地址不固定，所以在 remote address 设置 any。
设置目的地安全网关的名称(XXXXXX)。
执行这些设置后，将作为 Aggressive mode 的 responder 运行。

ipsec ike local address 1 192.168.200.1
ipsec ike local id 1 192.168.200.1
在 local address 和 id 中设置 LAN1 端的地址。

Copyright© 2014-2016 Yamaha Corporation

ipsec ike send info 1 off

设置不发送 IKE 的信息有效载荷。

SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- SGX808 的设置示例

省略 PPPoE 的设置。IPsec 的设置与 Aggressive mode 的设置基本相同。应指定目的地中分配的主机名称。

表 5.1.3 SGX808 的设置示例

项目	说明	设置示例
名称	设置适当的名称。	example
预共享密钥	设置与目的地设置相同的 Pre-Shared-Key。 （RTX1200 的设置示例(*1)）	test
目的地	设置目的地地址。 （RTX1200 的设置示例(*2)）	xxx.yyy.netvolante.jp
目的地 ID	设置目的地 ID。 （RTX1200 的设置示例(*3)）	192.168.200.1
目的地本地地址	设置目的地的本地 IP 地址。 （RTX1200 的设置示例(*4)）	192.168.200.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0 / 255.255.255.0
来源	选择"Aggressive mode"。	"Aggressive mode"
源 IP 地址	已选择"Aggressive mode"，所以无法设置。	
源 ID	设置与目的地相同的 key-id。 （RTX1200 的设置示例(*6)）	XXXXXX
认证算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“HMAC-SHA”
加密算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“AES-CBC”
响应模式	选择"Initiator"。	"Initiator"

Copyright© 2014-2016 Yamaha Corporation

5.1.4 NAT Traversal

下述是通过 NAT Traversal，连接 2 台 SGX808 的 IPsec 连接示例。假设在目的地中，从 PPPoE 服务器向 WAN 端分配了任意的 IP 地址。

- 结构示例

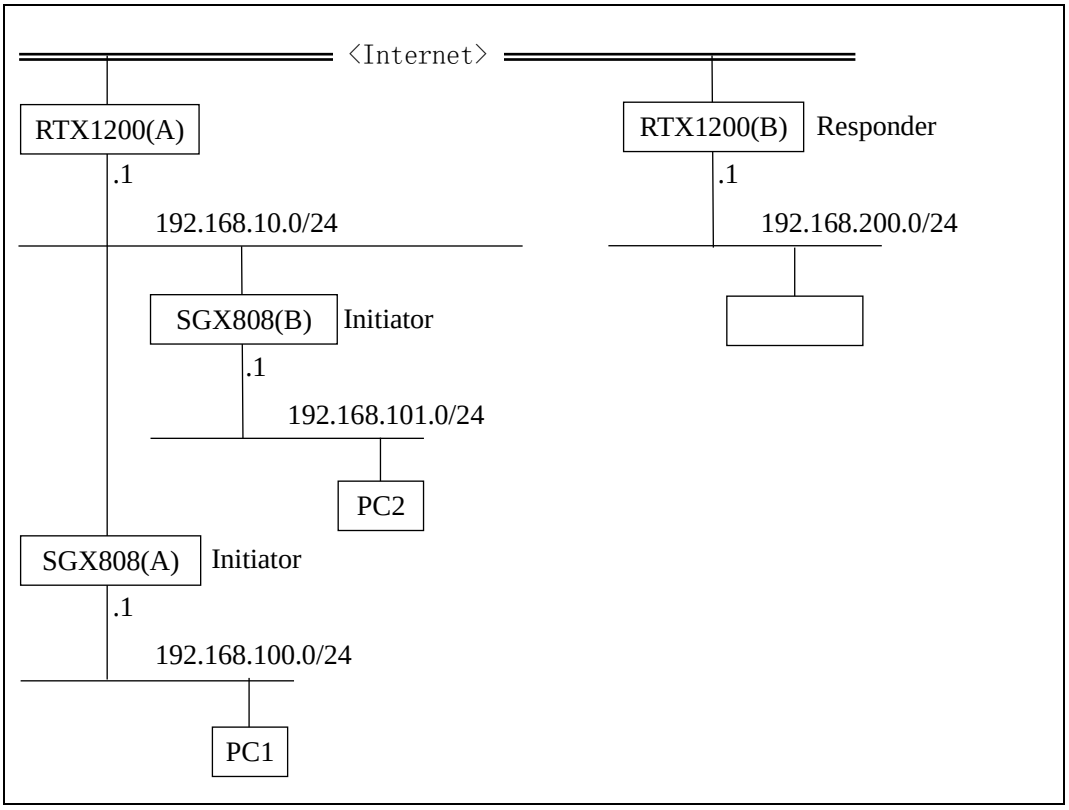

图 5.1.4-1 结构示例

SGX808(A)

LAN 端地址：192.168.100.1

WAN 端地址：不固定(通过 DHCP 从 RTX1200(A)分配)

SGX808(B)

LAN 端地址：192.168.101.1

WAN 端地址：不固定(通过 DHCP 从 RTX1200(A)分配)

RTX1200(A)

LAN 端地址：192.168.10.1

WAN 端地址：不固定(PPPoE 服务器分配)

RTX1200(B)

LAN 端地址：192.168.200.1

WAN 端地址：不固定

WAN 端主机名：xxx.yyy.netvolante.jp

事先由 Netvolante DNS 服务等分配的名称

Copyright© 2014-2016 Yamaha Corporation

- RTX1200 的设置示例

  针对“5.1.3 Aggressive mode（on PPPoE）”，追加 NAT Traversal 设置。

```
ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
ip route 192.168.101.0/24 gateway tunnel 2
ip lan1 address 192.168.1.1/24

pp select 1
 pppoe use lan2
 pp auth accept pap chap
 pp auth myname [userID] [PASS]
 ppp lcp mru on 1454
 ppp ipcp ipaddress on
 ppp ipcp msext on
 ppp ccp type none
 ip pp nat descriptor 1
 netvolante-dns hostname host pp 1 xxx.yyy.netvolante.jp
 pp enable 1

tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac
  ipsec ike local address 1 192.168.200.1
  ipsec ike local id 1 192.168.200.1
  ipsec ike backward-compatibility 1 2
  ipsec ike nat-traversal 1 on
  ipsec ike payload type 1 3
  ipsec ike pre-shared-key 1 text test
  ipsec ike remote address 1 any
  ipsec ike remote name 1 XXXXXX1 key-id
  ipsec ike send info 1 off
 tunnel enable 1

tunnel select 2
 ipsec tunnel 2
  ipsec sa policy 2 2 esp aes-cbc sha-hmac
  ipsec ike local address 2 192.168.200.1
```

Copyright© 2014-2016 Yamaha Corporation

```
   ipsec ike local id 2 192.168.200.1
   ipsec ike backward-compatibility 2 2
   ipsec ike nat-traversal 2 on
   ipsec ike payload type 2 3
   ipsec ike pre-shared-key 2 text test2
   ipsec ike remote address 2 any
   ipsec ike remote name 2 XXXXXX2 key-id
   ipsec ike send info 2 off
 tunnel enable 2

nat descriptor type 1 masquerade
nat descriptor address outer 1 ipcp
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
nat descriptor masquerade static 1 3 192.168.200.1 udp 4500
```

图 5.1.4-2　RTX1200 的设置示例

```
ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
ip route 192.168.101.0/24 gateway tunnel 2
```

把默认路由设为 pp。

把到达目的地 LAN 的路由设为隧道。

```
ip lan1 address 192.168.200.1/24
```

对 LAN1 设置固定地址。

```
pp select 1
pppoe use lan2
pp auth accept pap chap
pp auth myname [userID] [PASS]
ppp lcp mru on 1454
ppp ipcp ipaddress on
ppp ipcp msext on
ppp ccp type none
netvolante-dns hostname host pp 1 xxx.yyy.netvolante.jp pp enable 1
```

设置 PPPoE。同时注册主机名。

```
ip pp nat descriptor 1
```

Copyright© 2014-2016 Yamaha Corporation

nat descriptor type 1 masquerade
nat descriptor address outer 1 ipcp
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
nat descriptor masquerade static 1 3 192.168.200.1 udp 4500
对 pp 接口设置 NAT 地址伪装。
外部 IP 地址使用 PPP 的连接目标通知的 IP 地址。
如需把 IPsec 的 NAT Traversal 设为有效，应设置不转换 4500 的 udp 端口。

ipsec tunnel 1
tunnel enable 1
ipsec tunnel 2
tunnel enable 2
设置执行针对 2 处的 IPsec 定义的应用和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac
ipsec ike pre-shared-key 1 text test
ipsec sa policy 2 2 esp aes-cbc sha-hmac
ipsec ike pre-shared-key 2 text test
设置针对目的地安全网关的 SA 策略。
Pre-Shared-Key 设为与目的地相同。

ipsec ike backward-compatibility 1 2
ipsec ike backward-compatibility 2 2
把 IKEv1 密钥转换类型设为 2。
※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。
※本命令追加于固件版本 Rev.10.01.55 及更高版本中。

ipsec ike nat-traversal 1 on
ipsec ike nat-traversal 2 on
设置该项，使用 IPsec NAT Traversal。

ipsec ike payload type 1 3
ipsec ike remote address 1 any
ipsec ike remote name 1 XXXXXX1 key-id
ipsec ike payload type 2 3
ipsec ike remote address 2 any

Copyright© 2014-2016 Yamaha Corporation

ipsec ike remote name 2 XXXXXX2 key-id

把 payload 的类型设为 3。

由于目的地的全局地址不固定，所以在 remote address 设置 any。

设置目的地安全网关的名称(XXXXXX1,XXXXXX2)。

执行这些设置后，将作为 Aggressive mode 的 responder 运行。

ipsec ike local address 1 192.168.200.1

ipsec ike local id 1 192.168.200.1

ipsec ike local address 2 192.168.200.1

ipsec ike local id 2 192.168.200.1

在 local address 和 id 中设置 LAN1 端的地址。

ipsec ike send info 1 off

ipsec ike send info 2 off

设置不发送 IKE 的信息有效载荷。

SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- RTX1200(A)的设置

无需特别设置。执行连接网络时的 PPPoE 设置和 NAT 设置，以及 LAN 端的网络设置等即可。

- SGX808(A)(B)的设置

无需对 NAT Traversal 进行特别设置。与 Aggressive mode 的连接示例相同，设置 2 台设备都与目的地 RTX1200(B)连接即可。

Copyright© 2014-2016 Yamaha Corporation

5.2 Responder

以 SGX808 为 Responder、连接目的地的 RTX1200 为 Initiator 作为运行示例进行说明。

5.2.1 Main mode

以连接模式为 Main mode 作为示例进行说明。

- 结构示例

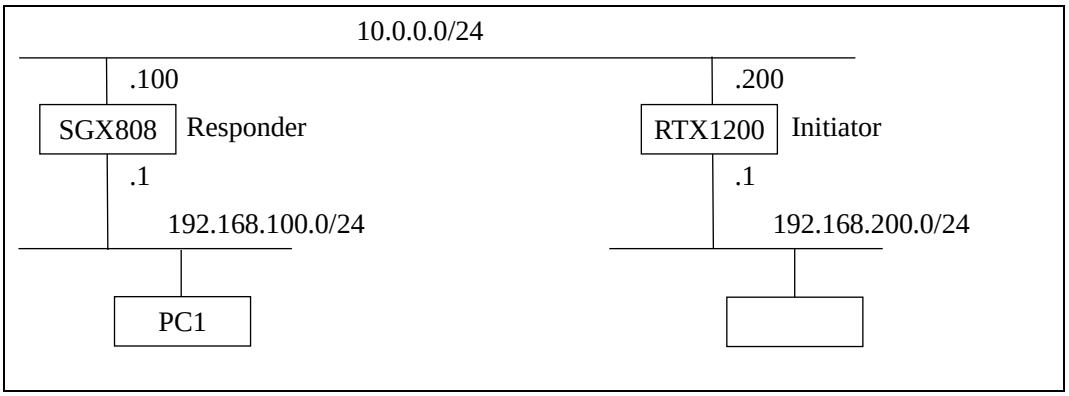

图 5.2.1-1 结构示例

SGX808

LAN 端地址：192.168.100.1

WAN 端地址：10.0.0.100

RTX1200

LAN 端地址：192.168.200.1

WAN 端地址：10.0.0.200

- RTX1200 的设置示例

```
ip route 192.168.100.0/24 gateway tunnel 1
ip lan1 address 192.168.200.1/24                ...(*4)
ip lan2 address 10.0.0.200/24                   ...(*2)
ip lan2 nat descriptor 1

tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac      ...(*5)
  ipsec ike always-on 1 on
  ipsec ike local id 1 192.168.200.1/24         ...(*3)
  ipsec ike payload type 1 3
  ipsec ike backward-compatibility 1 2
  ipsec ike pre-shared-key 1 text test          ...(*1)
```

Copyright© 2014-2016 Yamaha Corporation

```
   ipsec ike remote address 1 10.0.0.100
   ipsec ike remote id 1 192.168.100.1/24                    ...(*6)
   ipsec ike send info 1 off
  tunnel enable 1
ipsec auto refresh on

nat descriptor type 1 masquerade
nat descriptor address outer 1 primary
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
```

图 5.2.1-2　RTX1200 的设置示例

ip route 192.168.100.0/24 gateway tunnel 1

把到达目的地 LAN 的路由设为隧道。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

对 LAN1 和 LAN2 设置固定地址。

ip lan2 nat descriptor 1

nat descriptor type 1 masquerade

nat descriptor address outer 1 primary

nat descriptor address inner 1 auto

nat descriptor masquerade static 1 1 192.168.200.1 udp 500

nat descriptor masquerade static 1 2 192.168.200.1 esp

对 LAN2 接口设置 NAT 地址伪装。

ipsec tunnel 1

tunnel enable 1

设置应用 IPsec 定义和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac

ipsec ike pre-shared-key 1 text test

设置针对目的地安全网关的 SA 策略。

Pre-Shared-Key 设为与目的地相同。

ipsec ike always-on 1 on

Copyright© 2014-2016 Yamaha Corporation

ipsec auto refresh on

IKE 密钥转换失败时，可继续运行，无需停止密钥转换。

启动密钥转换。(作为 Initiator 运行)

ipsec ike backward-compatibility 1 2

把 IKEv1 密钥转换类型设为 2。

※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。

※本命令追加于固件版本 Rev.10.01.55 及更高版本中。

ipsec ike local id 1 192.168.200.1/24

在 local id 中设置 LAN1 端的地址和子网掩码。

ipsec ike payload type 1 3

ipsec ike remote address 1 10.0.0.100

ipsec ike remote id 1 192.168.100.1/24

把 payload 的类型设为 3。

在 remote address 中设置目的地全局地址。

在 remote id 中设置目的地 LAN 端的地址和子网掩码。

ipsec ike send info 1 off

设置不发送 IKE 的信息有效载荷。

SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- SGX808 的设置示例

表 5.2.1 SGX808 的设置示例

项目	说明	设置示例
名称	设置适当的名称。	example
预共享密钥	设置与目的地设置相同的 Pre-Shared-Key。 （RTX1200 的设置示例(*1)）	test
目的地	设置目的地地址。 （RTX1200 的设置示例(*2)）	10.0.0.200
目的地 ID	设置目的地 ID。 （RTX1200 的设置示例(*3)）	192.168.200.1
目的地本地地址	设置目的地的本地 IP 地址。 （RTX1200 的设置示例(*4)）	192.168.200.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0 / 255.255.255.0

Copyright© 2014-2016 Yamaha Corporation

来源	选择"Main mode"。	"Main mode"
源 IP 地址	设置 WAN 端的 IP 地址。	10.0.0.100
源 ID	设置主机的 ID，与目的地的设置相同。 （RTX1200 的设置示例(*6)）	192.168.100.1
认证算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“HMAC-SHA”
加密算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“AES-CBC”
响应模式	选择"Initiator"。	"Responder"

Copyright© 2014-2016 Yamaha Corporation

5.2.2 Aggressive mode

以连接模式为 Aggressive mode 作为示例进行说明。

- 结构示例

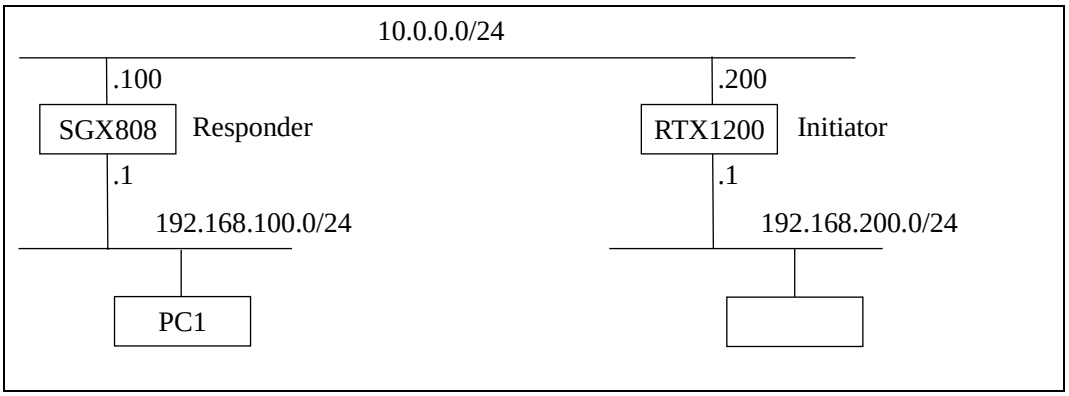

图 5.2.2-1 结构示例

SGX808

LAN 端地址：192.168.100.1

WAN 端地址：10.10.10.100

RTX1200

LAN 端地址：192.168.200.1

WAN 端地址：10.0.0.200

- RTX1200 的设置示例

```
ip route 192.168.100.0/24 gateway tunnel 1
ip lan1 address 192.168.200.1/24                          ...(*4)
ip lan2 address 10.0.0.200/24                             ...(*2)
ip lan2 nat descriptor 1

tunnel select 1
  ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac local-id=192.168.200.1/24
remote-id=192.168.100.1/24                                ...(*5)
    ipsec ike always-on 1 on
    ipsec ike local name 1 bob fqdn                       ...(*3)
    ipsec ike payload type 1 2
    ipsec ike backward-compatibility 1 2
    ipsec ike pre-shared-key 1 text test                  ...(*1)
    ipsec ike remote address 1 10.0.0.100
    ipsec ike remote name 1 alice fqdn                    ...(*6)
```

Copyright© 2014-2016 Yamaha Corporation

```
  ipsec ike send info 1 off
 tunnel enable 1
ipsec auto refresh on

nat descriptor type 1 masquerade
nat descriptor address outer 1 primary
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
```

图 5.2.2-2　RTX1200 的设置示例

ip route 192.168.100.0/24 gateway tunnel 1

把到达目的地 LAN 的路由设为隧道。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

对 LAN1 和 LAN2 设置固定地址。

ip lan2 nat descriptor 1

nat descriptor type 1 masquerade

nat descriptor address outer 1 primary

nat descriptor address inner 1 auto

nat descriptor masquerade static 1 1 192.168.200.1 udp 500

nat descriptor masquerade static 1 2 192.168.200.1 esp

对 LAN2 接口设置 NAT 地址伪装。

ipsec tunnel 1

tunnel enable 1

设置应用 IPsec 定义和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac local-id=192.168.200.1/24 remote-id=192.168.100.1/24

ipsec ike pre-shared-key 1 text test

设置针对目的地安全网关的 SA 策略。

同时也设置 local-id 和 remote-id 作为选项。

Pre-Shared-Key 设为与目的地相同。

ipsec ike backward-compatibility 1 2

把 IKEv1 密钥转换类型设为 2。

Copyright© 2014-2016 Yamaha Corporation

※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。
※本命令追加于固件版本 Rev.10.01.55 及更高版本中。

ipsec ike local name 1 bob fqdn

在 local name 中设置适当的名称。(设置示例：bob）
设置后，可在 Aggressive mode 中运行。

ipsec ike payload type 1 2
ipsec ike remote address 1 10.0.0.100
ipsec ike remote name 1 alice

把 payload 的类型设为 2。
在 remote address 中设置目的地全局地址。
在 remote name 中设置目的地的名称。(设置示例：alice）

ipsec ike send info 1 off

设置不发送 IKE 的信息有效载荷。
SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- SGX808 的设置示例

表 5.2.2 SGX808 的设置示例

项目	说明	设置示例
名称	设置适当的名称。	example
预共享密钥	设置与目的地设置相同的 Pre-Shared-Key。 （RTX1200 的设置示例(*1)）	test
目的地	设置目的地地址。 （RTX1200 的设置示例(*2)）	10.0.0.200
目的地 ID	设置目的地 ID。 （RTX1200 的设置示例(*3)）	bob
目的地本地地址	设置目的地的本地 IP 地址。 （RTX1200 的设置示例(*4)）	192.168.200.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0 / 255.255.255.0
来源	选择"Aggressive mode"。	"Aggressive mode"
源 IP 地址	已选择"Aggressive mode"，所以无法设置。	
源 ID	设置与目的地相同的 key-id。 （RTX1200 的设置示例(*6)）	alice

Copyright© 2014-2016 Yamaha Corporation

认证算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“HMAC-SHA”
加密算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“AES-CBC”
响应模式	选择"Responder"。	"Responder"

Copyright© 2014-2016 Yamaha Corporation

5.2.3 Aggressive mode（on PPPoE）

以需要设置 PPPoE 作为示例进行说明。这种情况下，为了使 SGX808 能够作为 Responder 运行，必须先运行“DDNS 客户端功能”。在此省略 SGX808 的 PPPoE 设置、DDNS 客户端设置的说明。

- 结构示例

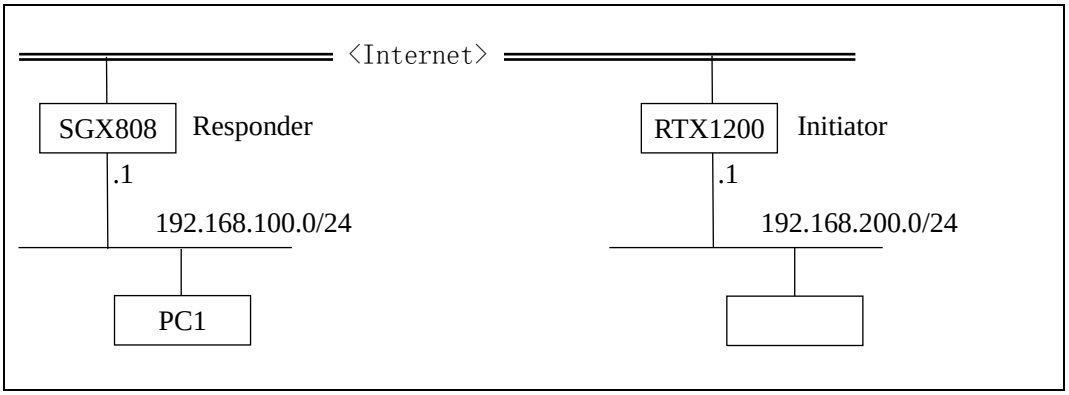

图 5.2.3-1 结构示例

SGX808

LAN 端地址：192.168.100.1

WAN 端地址：sgx808a.xxx.xxx

事先由适当的 DDNS 服务分配的名称

RTX1200

LAN 端地址：192.168.200.1

WAN 端地址：不固定

WAN 端主机名：xxx.yyy.netvolante.jp

事先由 Netvolante DNS 服务等分配的名称

- RTX1200 的设置示例

```
ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
ip lan1 address 192.168.200.1/24                    ...(*4)

pp select 1
 pppoe use lan2
 pp auth accept pap chap
 pp auth myname [userID] [PASS]
 ppp lcp mru on 1454
 ppp ipcp ipaddress on
 ppp ipcp msext on
 ppp ccp type none
```

Copyright© 2014-2016 Yamaha Corporation

```
 ip pp nat descriptor 1
 netvolante-dns hostname host pp 1 xxx.yyy.netvolante.jp   ...(*2)
 pp enable 1

tunnel select 1
 ipsec tunnel 1
  ipsec sa policy 1 1 esp aes-cbc sha-hmac local-id=192.168.200.1/24
remote-id=192.168.100.1/24                                 ...(*5)
  ipsec ike always-on 1 on
  ipsec ike local name 1 bob fqdn                          ...(*3)
  ipsec ike payload type 1 2
  ipsec ike backward-compatibility 1 2
  ipsec ike pre-shared-key 1 text test                     ...(*1)
  ipsec ike remote address 1 sgx808a.xxx.xxx
  ipsec ike remote name 1 alice fqdn                       ...(*6)
  ipsec ike send info 1 off
 tunnel enable 1
ipsec auto refresh on

nat descriptor type 1 masquerade
nat descriptor address outer 1 ipcp
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
```

图 5.2.3-2　RTX1200 的设置示例

ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
　把默认路由设为 pp。
　把到达目的地 LAN 的路由设为隧道。

ip lan1 address 192.168.200.1/24
　对 LAN1 设置固定地址。

pp select 1
pppoe use lan2
pp auth accept pap chap
pp auth myname [userID] [PASS]

Copyright© 2014-2016 Yamaha Corporation

ppp lcp mru on 1454
ppp ipcp ipaddress on ppp ipcp msext on
ppp ccp type none
netvolante-dns hostname host pp 1 xxx.yyy.netvolante.jp pp enable 1
设置 PPPoE。同时注册主机名。

ip pp nat descriptor 1
nat descriptor type 1 masquerade
nat descriptor address outer 1 ipcp
nat descriptor address inner 1 auto
nat descriptor masquerade static 1 1 192.168.200.1 udp 500
nat descriptor masquerade static 1 2 192.168.200.1 esp
对 pp 接口设置 NAT 地址伪装。
WAN 的 IP 地址使用 PPP 的连接目标通知的 IP 地址。

ipsec tunnel 1
tunnel enable 1
设置应用 IPsec 定义和自动密钥转换。

ipsec sa policy 1 1 esp aes-cbc sha-hmac local-id=192.168.200.1/24 remote-id=192.168.100.1/24
ipsec ike pre-shared-key 1 text test
设置针对目的地安全网关的 SA 策略。
同时也设置 local-id 和 remote-id 作为选项。
Pre-Shared-Key 设为与目的地相同。

ipsec ike always-on 1 on
ipsec auto refresh on
IKE 密钥转换失败时，可继续运行，无需停止密钥转换。
启动密钥转换。(作为 Initiator 运行)

ipsec ike backward-compatibility 1 2
把 IKEv1 密钥转换类型设为 2。
※把认证算法设为 HMAC-SHA256、加密算法设为 SDES-CBC 时，该项为必须设置项目。
※本命令追加于固件版本 Rev.10.01.55 及更高版本中。

Copyright© 2014-2016 Yamaha Corporation

ipsec ike local name 1 bob fqdn

在 local name 中设置适当的名称。(设置示例：bob）

设置后，可在 Aggressive mode 中运行。

ipsec ike payload type 1 2

ipsec ike remote address 1 sgx808a.xxx.xxx

ipsec ike remote name 1 alice

把 payload 的类型设为 2。

在 remote address 中设置目的地的主机名。

在 remote name 中设置目的地的名称。(设置示例：alice）

ipsec ike send info 1 off

设置不发送 IKE 的信息有效载荷。

SGX808 在接收到 ISAKMP SA 的 delete 的 informational 信息包后，会自动切断 IPsec 的对话，所以应事先执行该项设置。

- SGX808 的设置示例

在此省略 PPPoE 及 DDNS 客户端的设置。IPsec 的设置与“5.2.2 Aggressive mode”的设置基本相同。应指定目的地中分配的主机名称。

表 5.2.3 SGX808 的设置示例

项目	说明	设置示例
名称	设置适当的名称。	example
预共享密钥	设置与目的地设置相同的 Pre-Shared-Key。 （RTX1200 的设置示例(*1)）	test
目的地	设置目的地地址。 （RTX1200 的设置示例(*2)）	xxx.yyy.netvolante.jp
目的地 ID	设置目的地 ID。 （RTX1200 的设置示例(*3)）	bob
目的地本地地址	设置目的地的本地 IP 地址。 （RTX1200 的设置示例(*4)）	192.168.200.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0 / 255.255.255.0
来源	选择"Aggressive mode"。	"Aggressive mode"
源 IP 地址	已选择"Aggressive mode"，所以无法设置。	
源 ID	设置与目的地相同的 key-id。 （RTX1200 的设置示例(*6)）	alice

Copyright© 2014-2016 Yamaha Corporation

认证算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“HMAC-SHA”
加密算法	遵从目的地中设置的算法。 （RTX1200 的设置示例(*5)）	“AES-CBC”
响应模式	选择"Responder"。	"Responder"

Copyright© 2014-2016 Yamaha Corporation

5.3 SGX808 之间的连接

本部分说明 SGX808 和 SGX808 的连接示例。

5.3.1 Aggressive mode

以连接模式为 Aggressive mode 作为示例进行说明。

在此说明 Aggressive mode 的连接示例，Main mode 也同样连接。

- 结构示例

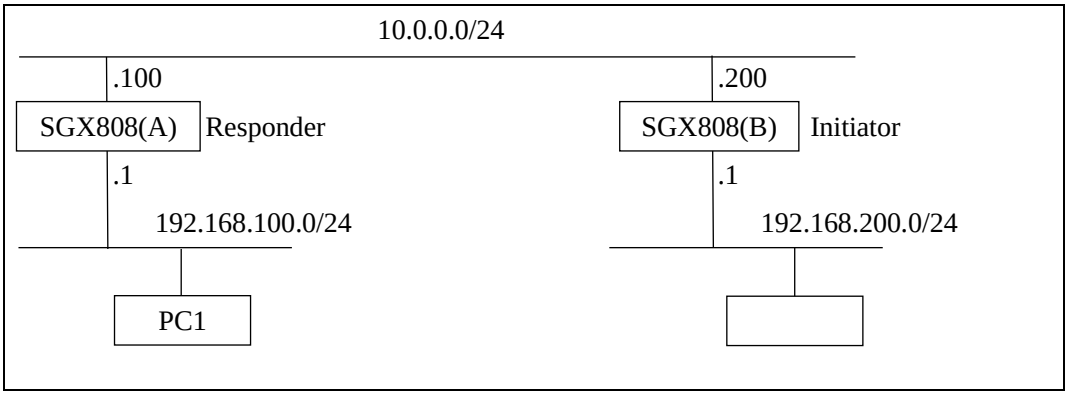

图 5.3.1 结构示例

SGX808(A)

LAN 端地址：192.168.100.1

WAN 端地址：10.10.10.100

SGX808(B)

LAN 端地址：192.168.200.1

WAN 端地址：10.0.0.200

- SGX808(A)(B)的设置示例

表 5.3.1 SGX808 的设置示例

项目	说明	设置示例	
		(A)	(B)
名称	设置适当的名称。	A	B
预共享密钥	相互设置相同的 Pre-Shared-Key。	test	test
目的地	设置目的地 WAN 地址。	10.0.0.200	10.0.0.100
目的地 ID	设置目的地的 Source ID。	bob	alice
目的地本地地址	设置目的地的本地 IP 地址。	192.168.200.1	192.168.100.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0/ 255.255.255.0	192.168.100.0/ 255.255.255.0
来源	选择"Aggressive mode"。	"Aggressive mode"	"Aggressive mode"

Copyright© 2014-2016 Yamaha Corporation

源 IP 地址	已选择"Aggressive mode"，所以无法设置。		
源 ID	设置适当的 ID。	alice	bob
认证算法	相互设置相同算法。	“HMAC-SHA”	"HMAC-SHA"
加密算法	相互设置相同算法。	“AES-CBC”	"AES-CBC"
响应模式	一个设为"Responder"，另一个设为"Initiator"。	"Responder"	"Initiator"

Copyright© 2014-2016 Yamaha Corporation

5.3.2 Aggressive mode（on PPPoE）

以需要设置 PPPoE 作为示例进行说明。此时，需要事先运行“DDNS 客户端功能”。在此省略 PPPoE 设置、DDNS 客户端设置的说明。

- 结构示例

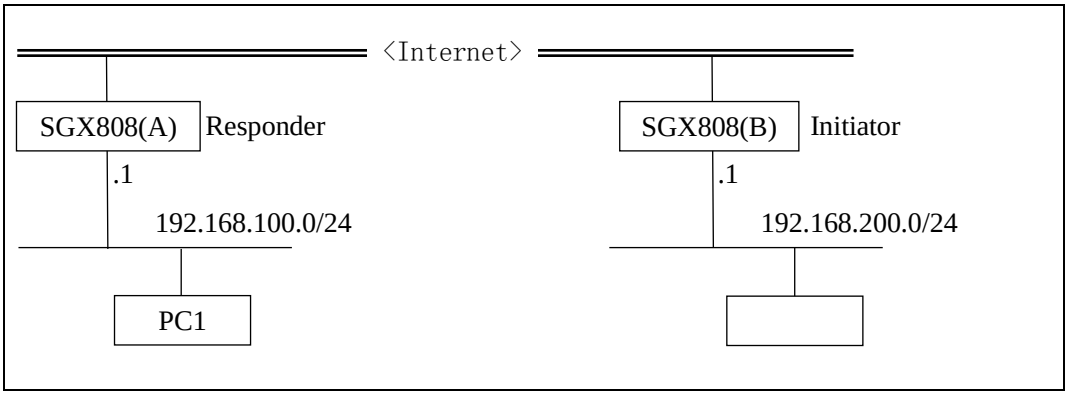

图 5.3.2 结构示例

SGX808(A)

LAN 端地址：192.168.100.1

WAN 端主机名：sgx808a.xxx.xxx

事先由适当的 DDNS 服务分配的名称

SGX808(B)

LAN 端地址：192.168.200.1

WAN 端主机名：sgx808b.xxx.xxx

事先由适当的 DDNS 服务分配的名称

- SGX808(A)(B)的设置示例

表 5.3.2 SGX808 的设置示例

项目	说明	设置示例	
		(A)	(B)
名称	设置适当的名称。	A	B
预共享密钥	相互设置相同的 Pre-Shared-Key。	test	test
目的地	设置目的地 WAN 地址。	sgx808b.xxx.xxx	sgx808a.xxx.xxx
目的地 ID	设置目的地的 Source ID。	bob	alice
目的地本地地址	设置目的地的本地 IP 地址。	192.168.200.1	192.168.100.1
目的地本地网络	设置目的地的本地网络地址和子网掩码地址。	192.168.200.0/ 255.255.255.0	192.168.100.0/ 255.255.255.0
来源	选择"Aggressive mode"。	"Aggressive mode"	"Aggressive mode"
源 IP 地址	已选择"Aggressive mode"，所以无法设置。		

Copyright© 2014-2016 Yamaha Corporation

源 ID	设置适当的 ID。	alice	bob
认证算法	相互设置相同算法。	“HMAC-SHA”	“HMAC-SHA”
加密算法	相互设置相同算法。	“AES-CBC”	“AES-CBC”
响应模式	一个设为"Responder"，另一个设为“Initiator"。	"Responder"	"Initiator"

Copyright© 2014-2016 Yamaha Corporation

6 补充

6.1 Rekey

rekey 间隔使用下述计算公式。

rekeytime = lifetime - (margintime + random(0, margintime * rekeyfuzz))

rekeytime : rekey 间隔
lifetime : IPsec SA 的寿命(20 分钟)
margintime : 范围(3 分钟)
rekeyfuzz : 100%

不可更改计算时使用的各个值。这样，rekey 间隔为 14～17 分钟。

6.2 Keepalive

如果使用了雅马哈公司生产的路由器作为级联对象，那么设置 keepalive 功能时可使用的 keepalive 方式只有 ICMP Echo。设置其他方式，可能导致中途断开，所以不能使用。

Copyright© 2014-2016 Yamaha Corporation