SGX808

IPsec 機能

ヤマハ株式会社

2016 年 1 月　第 2.01 版

更新履歴

更新日付	バージョン	内容
2014.05.29	1.00	初版発行
2015.02.04	2.00	・２つのセッションを張れるようにしました。 ・相手先情報としてホストネームも指定できるようにしました。 ・デフォルト経路として IPsec を設定できるようにしました。
2016.01.15	2.01	・Responder 機能を追加しました。 ・設定例を追加しました。

目次

1 概要 5
2 制約条件 5
3 対応機種とファームウェアリビジョン 5
4 詳細 5
4.1 IPsec の有効と無効 6
4.1.1 Edit IPsec connection settings 6
4.1.2 Default Gateway 6
4.1.3 “Edit”ボタン 6
4.1.4 “Delete”ボタン 7
4.1.5 “Apply”ボタン 7
4.2 接続情報設定 8
4.2.1 Name 8
4.2.2 Pre-Shared-Key 8
4.2.3 Destination 8
4.2.4 Destination ID 9
4.2.5 Destination Local IP Address 9
4.2.6 Destination Local Network 9
4.2.7 Source 9
4.2.8 Source IP Address 9
4.2.9 Source ID 9
4.2.10 Authentication Algorithm 9
4.2.11 Encryption Algorithm 9
4.2.12 Information Mode 10
4.2.13 “Apply”ボタン 10
4.2.14 “Delete”ボタン 10
4.2.15 “Reset”ボタン 10
4.2.16 “Return”ボタン 10
4.3 状態参照 11
5 設定例 12
5.1 Initiator 12
5.1.1 Main mode 12
5.1.2 Aggressive mode 15
5.1.3 Aggressive mode（on PPPoE） 19
5.1.4 NAT Traversal 23
5.2 Responder 28
5.2.1 Main mode 28
5.2.2 Aggressive mode 32

5.2.3 Aggressive mode（on PPPoE） 36
5.3 SGX808 同士の接続 41
5.3.1 Aggressive mode 41
5.3.2 Aggressive mode（on PPPoE） 43
6 補足 45
6.1 Rekey 45
6.2 Keepalive 45

1　概要

本ドキュメントは、SGX808 の IPsec 機能について記述したものです。本機能の有効無効、および IPsec 機能に必要な情報を設定することができます。

機能として同時に 2 つのセッションを張ることができ、それぞれに対して Aggressive mode か Main mode 動作を、Initiator か Responder 動作を設定することができます。

2　制約条件

本機能において、以下の制約条件を設けています。

1. IKE(Internet Key Exchange)は Version 1 のみ対応します。
2. IKE が用いるグループは modp1024 のみ対応します。フェーズ 1 とフェーズ 2 の両方で、modp1024 を提案する形式をとります。
3. トンネルモードのみ対応します。
4. Responder を設定した場合
   - 設定した 1 つの相手先を Initiator として動作します。不特定の相手先を Initiator として動作させることはできません。
   - Responder を設定した IPsec トンネルは、Default Gateway として動作しません。
   - 暗号アルゴリズム及び認証アルゴリズムは Initiator 側に従います。
   - 認証アルゴリズムに sha256 を使用できません。

3　対応機種とファームウェアリビジョン

SGX808 では、以下のファームウェアで IPsec 機能を利用できます。

表 3.1　対応機種とファームウェアリビジョン

機種	ファームウェア	変更点
SGX808	Rev.1.00.03 以降	新規
	Rev.1.00.08 以降	・２つのセッションを張れるようにしました。 ・相手先情報としてホストネームも指定できるようにしました。 ・デフォルト経路として IPsec を設定できるようにしました。
	Rev.1.00.15 以降	・Responder 機能を追加しました。

4　詳細

IPsec 機能は Web 設定画面の[Network]タブ内の[Internet Settings]-[IPsec]のページで設定します。NAT Traversal に対応しており、NAT の有無は自動検出して動作します。NAT の keepalive の送信間隔は 20 秒です。この値は変更できません。

4.1 IPsec の有効と無効

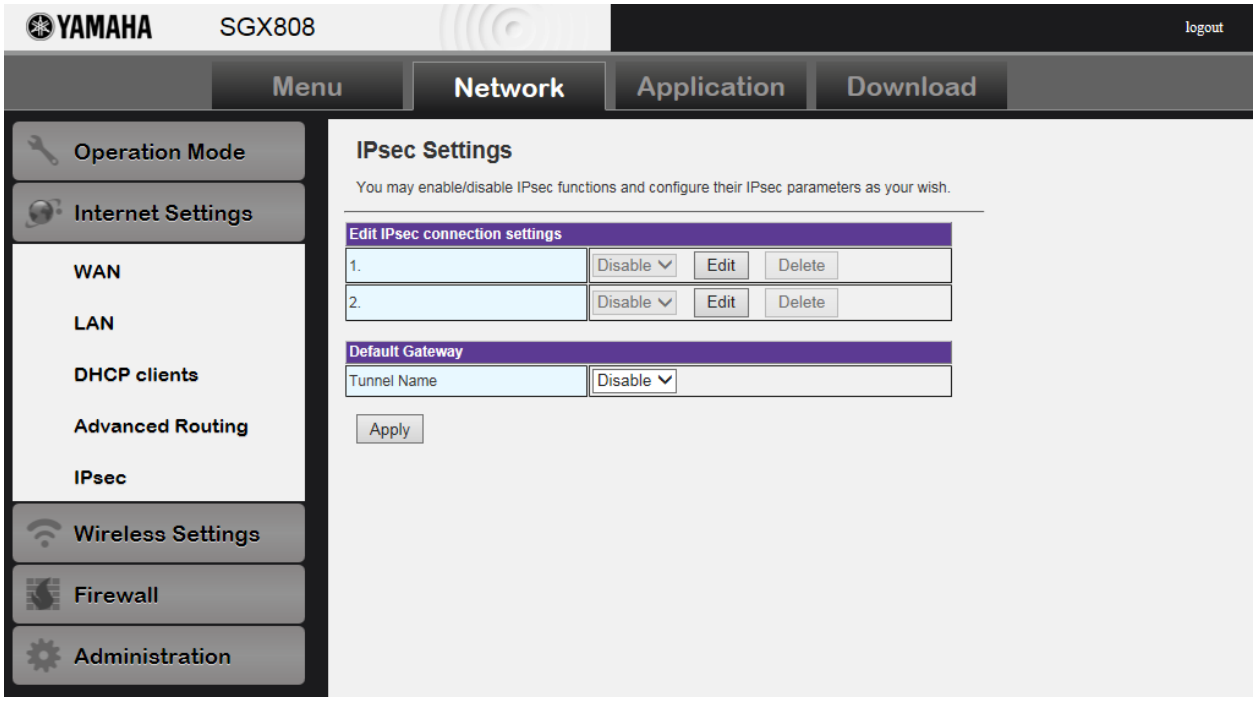


図 4.1 IPsec の有効と無効

4.1.1 Edit IPsec connection settings

個々の接続情報について"Enable"／"Disable"を設定することができます。接続情報が設定されていない場合は選択できません。（デフォルト："Disable"）

4.1.2 Default Gateway

プルダウンメニューからトンネル名を選択することで、デフォルト経路となるトンネルを設定します。（デフォルト："Disable"）

注意すべき点として、この設定を"Disable"以外にすると、WAN 側への送出されるパケットは全て設定されたトンネルへ流れるので、例外とするルーティングは、[Internet Settings]-[Advanced Routing]にて設定しておく必要があります。

また、2 つのトンネルを設定し、片方をデフォルト経路に設定した場合には、それぞれにトンネルが確立した後、全てのパケットは デフォルト経路に設定したトンネルに送出されます。もう片方のトンネルの先にあるネットワークセグメント宛のパケットは、暗黙にルーティング設定されているので、 デフォルト経路には送信されず、もう片方のトンネルに送出されます。

4.1.3 “Edit” ボタン

個々の接続情報設定画面に遷移します。

4.1.4 “Delete” ボタン

個々の接続情報を削除します。接続情報が設定されていない状態の場合は実行できません。

4.1.5 “Apply” ボタン

設定した情報を動作に反映します。2 つのトンネルを設定し、片方が接続状態にあり、もう片方の”Enable/Disable”を変更した場合、接続状態にある側は再接続せず、接続を維持します。デフォルト経路を変更した場合、接続状態であるトンネルを一旦切断し再接続します。

4.2　接続情報設定

2 箇所の接続先に対して、それぞれ以下の情報を設定することができます。

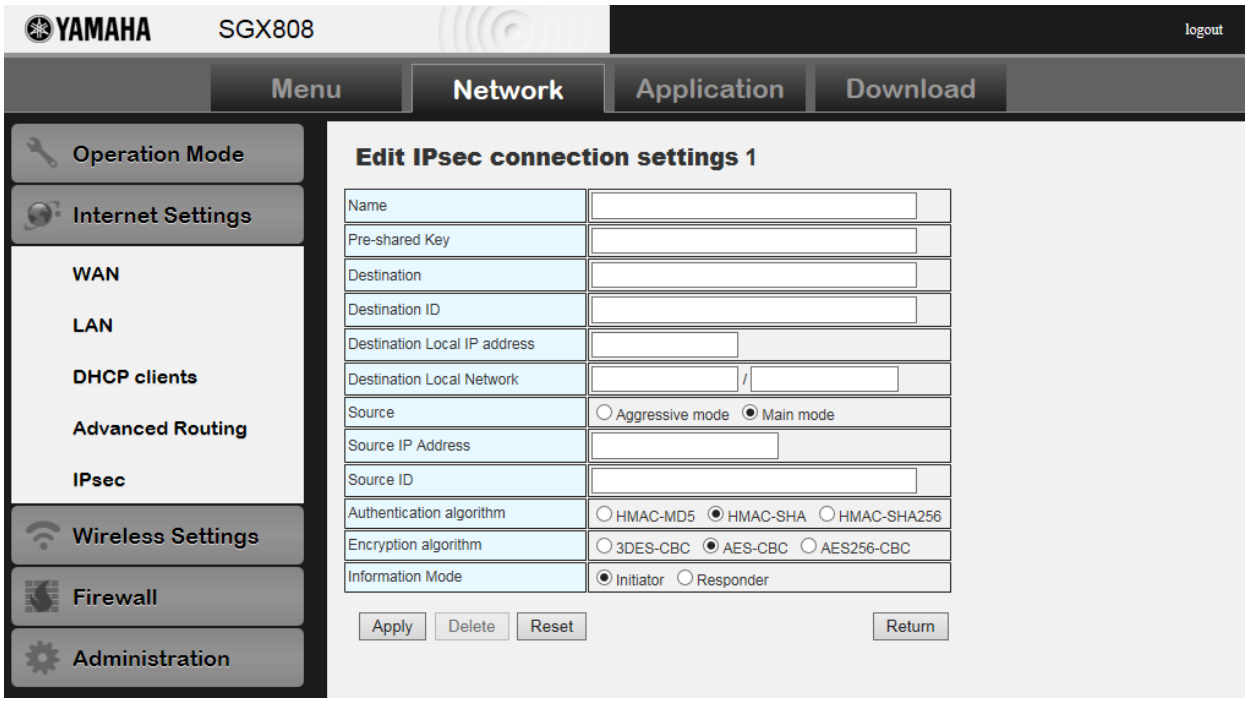


図 4.2　接続状態設定

4.2.1　Name

IPsec セッションの名称を設定します。省略不可です。2 つのセッションに同じ名称を設定することはできません。ASCII 文字 32bytes（デフォルト：なし）。以下の文字は使用禁止です。

""（ダブルクォーテーション）、'='（イコール）、'#'（シャープ）、' '（空白）
';'（セミコロン）、'('、')'（括弧）、'`'（バッククォーテーション）、'\'（バックスラッシュ）
'*'（アスタリスク）、"'"（シングルクォーテーション）、'|'（縦線）、'~'（チルダ）

4.2.2　Pre-Shared-Key

IPsec では、鍵交換プロトコル IKE(Internet Key Exchange)を使用します。省略不可です。必要な鍵は IKE により自動生成されますが、その鍵の種となる事前共有鍵(PSK:Pre-Shared-Key)をここで設定します。ASCII 文字 128bytes（デフォルト：なし）。""(ダブルクォーテーション)は使用禁止です。

4.2.3　Destination

相手先の情報（IP アドレスまたは FQDN）を設定します。省略不可です。ASCII 文字 256bytes（デフォルト：なし）。以下の文字は使用禁止です。

""（ダブルクォーテーション）、'='（イコール）、'#'（シャープ）、' '（空白）

4.2.4 Destination ID

相手先に設定されている ID を設定します。省略不可です。ASCII 文字 256bytes（デフォルト：なし）。以下の文字は使用禁止です。

""（ダブルクォーテーション）、'='（イコール）、'#'（シャープ）、' '（空白）

4.2.5 Destination Local IP Address

相手先に設定されているローカル側の IP アドレスを設定します。省略不可です。（デフォルト：なし）

4.2.6 Destination Local Network

相手先に設定されているローカル側のネットワークアドレスとサブネットマスクアドレスを設定します。省略不可です。（デフォルト：なし）

4.2.7 Source

接続モードを以下の 2 つから選択します。

"Aggressive mode", "Main mode"（デフォルト）

4.2.8 Source IP Address

本機の WAN 側の IP アドレスを設定します。省略不可です。"Aggressive mode"の場合は入力不可となります。

4.2.9 Source ID

IKE のフェーズ 2 で使用する自分側の ID を設定します。省略不可です。"Aggressive mode"の場合は必須の項目となります。ASCII 文字 256bytes（デフォルト：なし）。以下の文字は使用禁止です。

""（ダブルクォーテーション）、'='（イコール）、'#'（シャープ）、' '（空白）

4.2.10 Authentication Algorithm

認証アルゴリズムを以下の 3 つから選択します。

"HMAC-MD5", "HMAC-SHA"（デフォルト）, "HMAC-SHA256"

4.2.11 Encryption Algorithm

暗号アルゴリズムを以下の 3 つから選択します。

"3DES-CBC", "AES-CBC"（デフォルト）, "AES256-CBC"

4.2.12 Information Mode

応答方法を以下の 2 つから選択します。

"Initiator"（デフォルト）, "Responder"

4.2.13 “Apply” ボタン

設定した情報を記憶し、前の画面に戻ります。基本設定(4.1 IPsec の有効と無効)が"Enable"であった場合には設定内容に従い動作を開始します。"Disable"と設定していた場合には、設定内容を記憶しますが、動作を開始しません。

4.2.14 “Delete” ボタン

設定した情報を削除し、前の画面に戻ります。既に実行(接続)状態にあった場合には終了(切断)します。

4.2.15 “Reset” ボタン

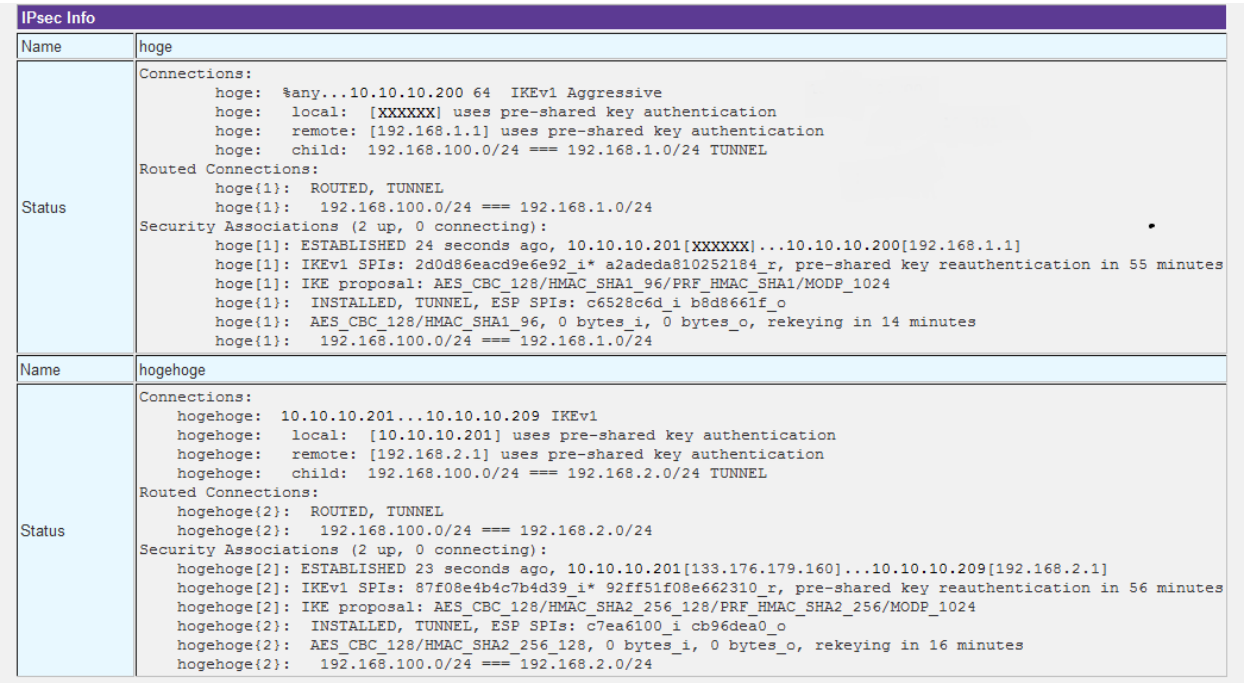
入力途中の設定情報を"確定"ボタンを押す前の状態に戻します。

4.2.16 “Return” ボタン

前の画面に戻ります。入力途中の情報は破棄します。

4.3 状態参照

Web 設定画面の[Administration]-[Status]のページで、接続状態を確認することができます。



IPsec Info

Name	hoge
Status	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
Name	hogehoge
Status	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

図 4.3 状態参照

5　設定例

5.1　Initiator

SGX808 が Initiator、接続する相手先の RTX1200 が Responder として動作する例を説明します。

5.1.1　Main mode

接続モードが Main mode の場合の例を説明します。

- 構成例

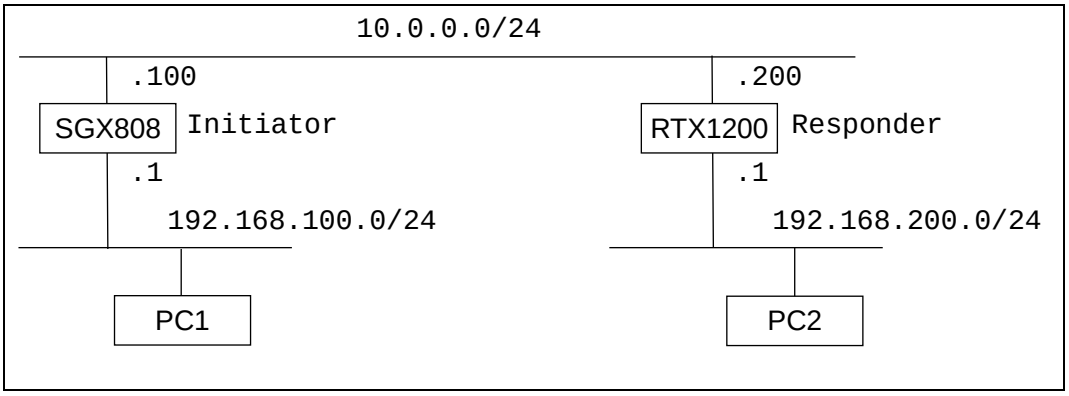


図 5.1.1-1　構成例

SGX808

LAN 側アドレス：192.168.100.1

WAN 側アドレス：10.0.0.100

RTX1200

LAN 側アドレス：192.168.200.1

WAN 側アドレス：10.0.0.200

- RTX1200 の設定例

```
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)
```

```
 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
```

図 5.2.1-2　RTX1200 の設定例

ip route 192.168.100.0/24 gateway tunnel 1

相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

LAN1,LAN2 に固定アドレスを設定します。

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

LAN2 インタフェースに NAT マスカレードを設定します。

ipsec tunnel 1

tunnel enable 1

IPsec 定義の適用と自動鍵交換を行うように設定します。

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

ipsec ike pre-shared-key 1 text test

相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

Pre-Shared-Key は相手側と同じものを設定します。

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

local address と id には LAN1 側のアドレスを設定します。
remote address には相手側の WAN 側のアドレスを設定します。

ipsec ike backward-compatibility 1 2
IKEv1 鍵交換タイプを 2 に設定します。
※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。
※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

ipsec ike send info 1 off
IKE の情報ペイロードを送信しない設定にします。
SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- SGX808 の設定例

表 5.1.1 SGX808 の設定例

項目	内容	設定例
Name	適当な名称を設定します。	example
Pre-Shared-Key	相手先の設定と同じ Pre-Shared-Key を設定します。（RTX1200 の設定例(*1)）	test
Destination	相手先のアドレスを設定します。（RTX1200 の設定例(*2)）	10.0.0.200
Destination ID	相手先の ID を設定します。（RTX1200 の設定例(*3)）	192.168.200.1
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。（RTX1200 の設定例(*4)）	192.168.200.1
Destination Local Network	相手先のローカル側のネットワークアドレスとサブネットマスクアドレスを設定します。	192.168.200.0 / 255.255.255.0
Source	"Main mode"を選択します。	"Main mode"
Source IP Address	WAN 側の IP アドレスを設定します。	10.0.0.100
Source ID	設定の必要はありません。	(空白)
Authentication Algorithm	相手先で設定されたアルゴリズムに従います。（RTX1200 の設定例(*5)）	“HMAC-SHA”
Encryption Algorithm	相手先で設定されたアルゴリズムに従う。（RTX1200 の設定例(*5)）	“AES-CBC”
Information Mode	"Initiator"を選択します。	"Initiator"

5.1.2 Aggressive mode

接続モードが Aggressive mode の場合の例を説明します。

- 構成例

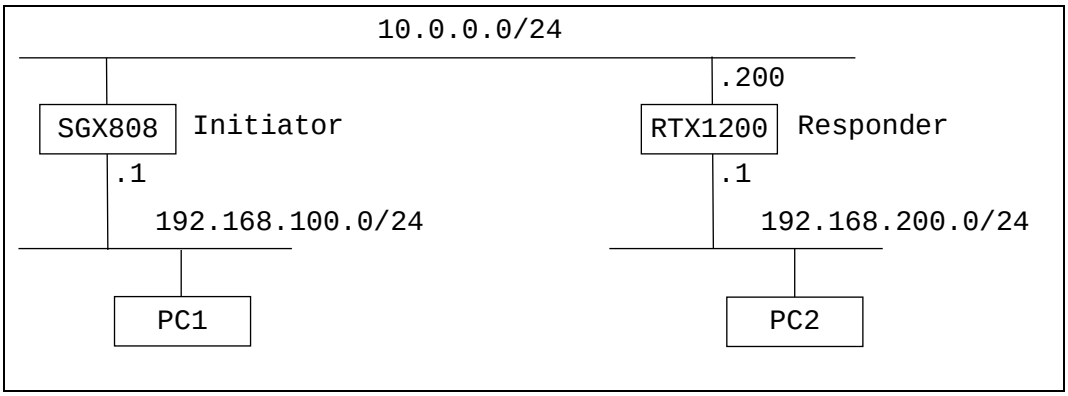


図 5.3.2-1 構成例

SGX808

LAN 側アドレス：192.168.100.1

WAN 側アドレス：不定

RTX1200

LAN 側アドレス：192.168.200.1

WAN 側アドレス：10.0.0.200

- RTX1200 の設定例

```
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
```



```
 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
```

図 5.4.2-2　RTX1200 の設定例

ip route 192.168.100.0/24 gateway tunnel 1

相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

LAN1,LAN2 に固定アドレスを設定します。

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

LAN2 インタフェースに NAT マスカレードを設定します。

ipsec tunnel 1

tunnel enable 1

IPsec 定義の適用と自動鍵交換を行うように設定します。

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

ipsec ike pre-shared-key 1 text test

相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

Pre-Shared-Key は相手側と同じものを設定します。

ipsec ike backward-compatibility 1 2

IKEv1 鍵交換タイプを 2 に設定します。

※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。

※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

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

payload のタイプを 3 に設定します。
remote address には相手側のグローバルアドレスが不定なので any を設定します。
相手側のセキュリティ・ゲートウェイの名前(XXXXXX)を設定します。
これらの設定により、Aggressive mode の responder として動作します。

ipsec ike local address 1 192.168.200.1
ipsec ike local id 1 192.168.200.1

local address と id には LAN1 側のアドレスを設定します。

ipsec ike send info 1 off

IKE の情報ペイロードを送信しないように設定します。
SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- SGX808 の設定例

表 5.1.2 SGX808 の設定例

項目	内容	設定例
Name	適当な名称を設定します。	example
Pre-Shared-Key	相手先の設定と同じ Pre-Shared-Key を設定します。（RTX1200 の設定例(*1)）	test
Destination	相手先のアドレスを設定します。（RTX1200 の設定例(*2)）	10.0.0.200
Destination ID	相手先の ID を設定します。（RTX1200 の設定例(*3)）	192.168.200.1
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。（RTX1200 の設定例(*4)）	192.168.200.1
Destination Local Network	相手先のローカル側のネットワークアドレスとサブネットマスクアドレスを設定します。	192.168.200.0 / 255.255.255.0
Source	"Aggressive mode"を選択します。	"Aggressive mode"
Source IP Address	"Aggressive mode"なので、設定できません。	
Source ID	相手先と同じ key-id を設定します。（RTX1200 の設定例(*6)）	XXXXXX
Authentication Algorithm	相手先で設定されたアルゴリズムに従います。（RTX1200 の設定例(*5)）	“HMAC-SHA”

Encryption Algorithm	相手先で設定されたアルゴリズムに従う。 （RTX1200 の設定例(*5)）	“AES-CBC”
Information Mode	"Initiator"を選択します。	"Initiator"

5.1.3 Aggressive mode（on PPPoE）

PPPoE の設定を必要とした場合の例を説明します。

- 構成例

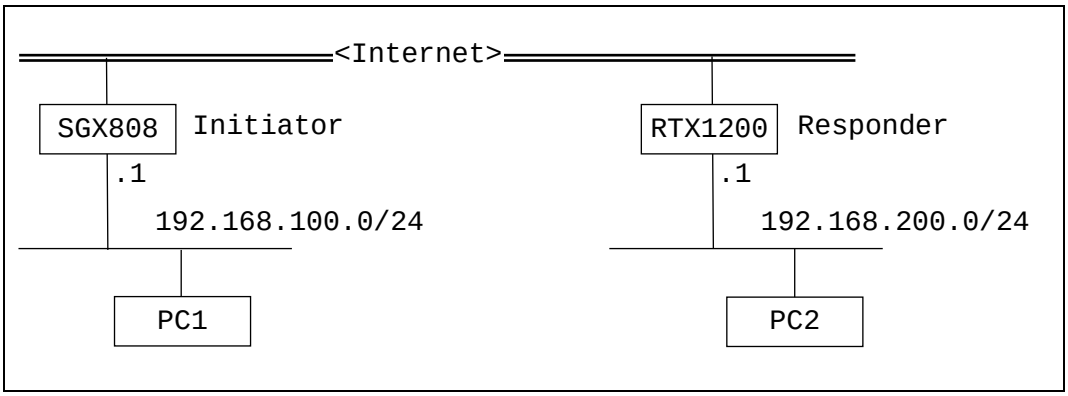


図 5.5.3-1 構成例

SGX808

LAN 側アドレス：192.168.100.1

WAN 側アドレス：不定

RTX1200

LAN 側アドレス：192.168.200.1

WAN 側アドレス：不定

WAN 側ホスト名：xxx.yyy.netvolante.jp

予めネットボランチ DNS サービスで割り当てられた名称

- RTX1200 の設定例

```
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)
```



```
 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
```

図 5.6.3-2　RTX1200 の設定例

ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
　デフォルト経路を pp に設定します。
　相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24
　LAN1 に固定アドレスを設定します。

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

PPPoE を設定します。ホスト名も登録します。

```
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
```

pp インタフェースに NAT マスカレードを設定します。
WAN 側の IP アドレスとして､PPP の接続先から通知される IP アドレスを起用するようにします。

```
ipsec tunnel 1
tunnel enable 1
```

IPsec 定義の適用と自動鍵交換を行うように設定します。

```
ipsec sa policy 1 1 esp aes-cbc sha-hmac
ipsec ike pre-shared-key 1 text test
```

相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。
Pre-Shared-Key は相手側と同じものを設定します。

```
ipsec ike backward-compatibility 1 2
```

IKEv1 鍵交換タイプを 2 に設定します。
※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。
※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

```
ipsec ike payload type 1 3
ipsec ike remote address 1 any
ipsec ike remote name 1 XXXXXX key-id
```

payload のタイプを 3 に設定します。
remote address には相手側のグローバルアドレスが不定なので any を設定します。
相手側のセキュリティ・ゲートウェイの名前(XXXXXX)を設定します。
これらの設定により、Aggressive mode の responder として動作します。

```
ipsec ike local address 1 192.168.200.1
ipsec ike local id 1 192.168.200.1
```

local address と id には LAN1 側のアドレスを設定します。

ipsec ike send info 1 off

IKE の情報ペイロードを送信しないように設定します。

SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- SGX808 の設定例

PPPoE の設定は省略します。IPsec の設定は Aggressive mode の場合の設定とほぼ同じです。相手先として、相手先に割り当てられているホストネームを指定します。

表 5.1.3　SGX808 の設定例

項目	内容	設定例
Name	適当な名称を設定します。	example
Pre-Shared-Key	相手先の設定と同じ Pre-Shared-Key を設定します。（RTX1200 の設定例(*1)）	test
Destination	相手先のアドレスを設定します。（RTX1200 の設定例(*2)）	xxx.yyy.netvolante.jp
Destination ID	相手先の ID を設定します。（RTX1200 の設定例(*3)）	192.168.200.1
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。（RTX1200 の設定例(*4)）	192.168.200.1
Destination Local Network	相手先のローカル側のネットワークアドレスとサブネットマスクアドレスを設定します。	192.168.200.0 / 255.255.255.0
Source	"Aggressive mode"を選択します。	"Aggressive mode"
Source IP Address	"Aggressive mode"なので、設定できません。	
Source ID	相手先と同じ key-id を設定します。（RTX1200 の設定例(*6)）	XXXXXX
Authentication Algorithm	相手先で設定されたアルゴリズムに従います。（RTX1200 の設定例(*5)）	“HMAC-SHA”
Encryption Algorithm	相手先で設定されたアルゴリズムに従う。（RTX1200 の設定例(*5)）	“AES-CBC”
Information Mode	"Initiator"を選択します。	"Initiator"

5.1.4 NAT Traversal

NAT Traversal による２台の SGX808 との IPsec 接続例を示します。相手先には PPPoE サーバーから任意の IP アドレスが WAN 側に付与される場合を想定します。

- 構成例

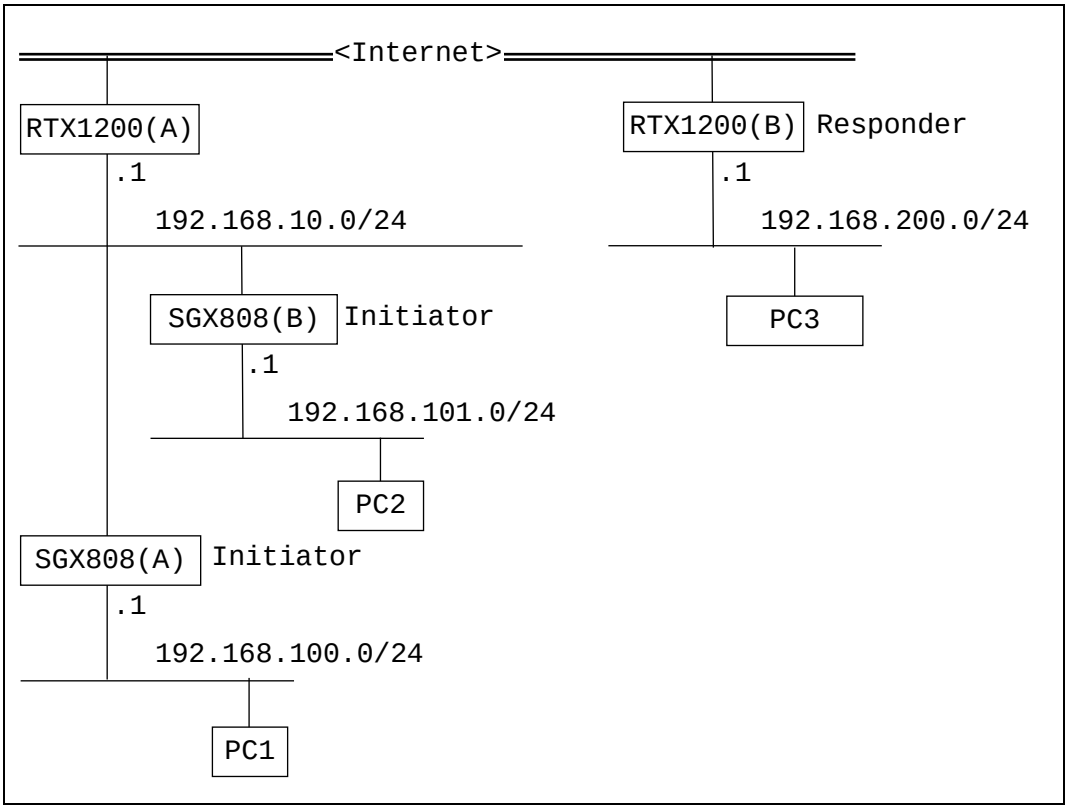


図 5.7.4-1　構成例

SGX808(A)

LAN 側アドレス：192.168.100.1

WAN 側アドレス：不定(DHCP にて RTX1200(A)から付与)

SGX808(B)

LAN 側アドレス：192.168.101.1

WAN 側アドレス：不定(DHCP にて RTX1200(A)から付与)

RTX1200(A)

LAN 側アドレス：192.168.10.1

WAN 側アドレス：不定(PPPoE サーバーから付与)

RTX1200(B)

LAN 側アドレス：192.168.200.1

WAN 側アドレス：不定

WAN 側ホスト名：xxx.yyy.netvolante.jp

予めネットボランチ DNS サービスで割り当てられた名称

- RTX1200 の設定例

「5.1.3 Aggressive mode（on PPPoE）」に対し、NAT Traversal の設定を追加します。

```
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
```

```
 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
```

図 5.8.4-2　RTX1200 の設定例

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

　デフォルト経路を pp に設定します。

　相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24

　LAN1 に固定アドレスを設定します。

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

　PPPoE を設定します。ホスト名も登録します。

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
nat descriptor masquerade static 1 3 192.168.200.1 udp 4500
pp インタフェースに NAT マスカレードを設定します。
外側の IP アドレスとして、PPP の接続先から通知される IP アドレスを起用するようにします。
IPsec の NAT Traversal を有効にするため、4500 の udp ポートを変換しないようにします。

ipsec tunnel 1
tunnel enable 1
ipsec tunnel 2
tunnel enable 2
2 箇所に対する IPsec 定義の適用と自動鍵交換を行うように設定します。

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
相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。
Pre-Shared-Key は相手側と同じものを設定します。

ipsec ike backward-compatibility 1 2
ipsec ike backward-compatibility 2 2
IKEv1 鍵交換タイプを 2 に設定します。
※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。
※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

ipsec ike nat-traversal 1 on
ipsec ike nat-traversal 2 on
IPsec NAT Traversal を利用するために設定します。

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
ipsec ike remote name 2 XXXXXX2 key-id
payload のタイプを 3 に設定します。
remote address には相手側のグローバルアドレスが不定なので any を設定します。
相手側のセキュリティ・ゲートウェイの名前(XXXXXX1,XXXXXX2)を設定します。
これらの設定により、Aggressive mode の responder として動作します。

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
local address と id には LAN1 側のアドレスを設定します。

ipsec ike send info 1 off
ipsec ike send info 2 off
IKE の情報ペイロードを送信しないように設定します。
SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- RTX1200(A)の設定

特別な設定をする必要はありません。インターネットに接続するための PPPoE 設定と NAT の設定、LAN 側に対するネットワーク設定をすればよいです。

- SGX808(A)(B)の設定

NAT Traversal に対して特別な設定は必要ありません。Aggressive mode の接続例と同様に 2 台とも相手先となる RTX1200(B)との接続設定をすればよいです。

5.2 Responder

SGX808 が Responder、接続する相手先の RTX1200 が Initiator として動作する例を説明します。

5.2.1 Main mode

接続モードが Main mode の場合の例を説明します。

- 構成例

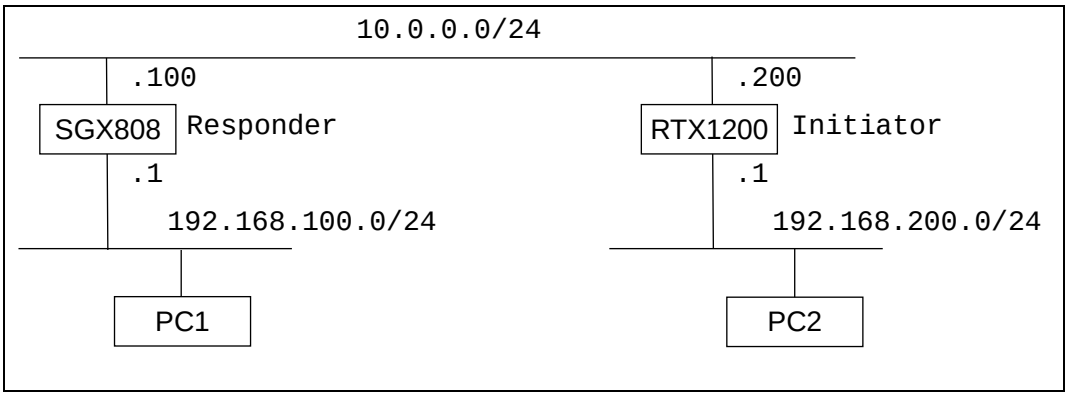


図 5.2.1-1 構成例

SGX808

LAN 側アドレス：192.168.100.1

WAN 側アドレス：10.0.0.100

RTX1200

LAN 側アドレス：192.168.200.1

WAN 側アドレス：10.0.0.200

- RTX1200 の設定例

```
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)
```



```
  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
```

図 5.2.1-2　RTX1200 の設定例

ip route 192.168.100.0/24 gateway tunnel 1

相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24

ip lan2 address 10.0.0.200/24

LAN1,LAN2 に固定アドレスを設定します。

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

LAN2 インタフェースに NAT マスカレードを設定します。

ipsec tunnel 1

tunnel enable 1

IPsec 定義の適用と自動鍵交換を行うように設定します。

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

ipsec ike pre-shared-key 1 text test

相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。

Pre-Shared-Key は相手側と同じものを設定します。

ipsec ike always-on 1 on

ipsec auto refresh on

IKE の鍵交換に失敗したときに鍵交換を休止せずに継続できるようにします。

鍵交換を始動するようにします。(Initiator として動作します)

ipsec ike backward-compatibility 1 2

IKEv1 鍵交換タイプを 2 に設定します。

※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。

※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

ipsec ike local id 1 192.168.200.1/24

local id には LAN1 側のアドレスとサブネットマスクを設定します。

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

payload のタイプを 3 に設定します。

remote address には相手側のグローバルアドレスを設定します。

remote id には相手側の LAN 側のアドレスとサブネットマスクを設定します。

ipsec ike send info 1 off

IKE の情報ペイロードを送信しない設定にします。

SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- SGX808 の設定例

表 5.2.1　SGX808 の設定例

項目	内容	設定例
Name	適当な名称を設定します。	example
Pre-Shared-Key	相手先の設定と同じ Pre-Shared-Key を設定します。（RTX1200 の設定例(*1)）	test
Destination	相手先のアドレスを設定します。（RTX1200 の設定例(*2)）	10.0.0.200
Destination ID	相手先の ID を設定します。（RTX1200 の設定例(*3)）	192.168.200.1
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。（RTX1200 の設定例(*4)）	192.168.200.1
Destination Local	相手先のローカル側のネットワークアドレスとサブネ	192.168.200.0 /

Network	ットマスクアドレスを設定します。	255.255.255.0
Source	"Main mode"を選択します。	"Main mode"
Source IP Address	WAN 側の IP アドレスを設定します。	10.0.0.100
Source ID	相手先の設定と同じになるように本体側の ID を設定します。（RTX1200 の設定例(*6)）	192.168.100.1
Authentication Algorithm	相手先で設定されたアルゴリズムに従います。（RTX1200 の設定例(*5)）	“HMAC-SHA”
Encryption Algorithm	相手先で設定されたアルゴリズムに従う。（RTX1200 の設定例(*5)）	“AES-CBC”
Information Mode	"Initiator"を選択します。	"Responder"

5.2.2 Aggressive mode

接続モードが Aggressive mode の場合の例を説明します。

- 構成例

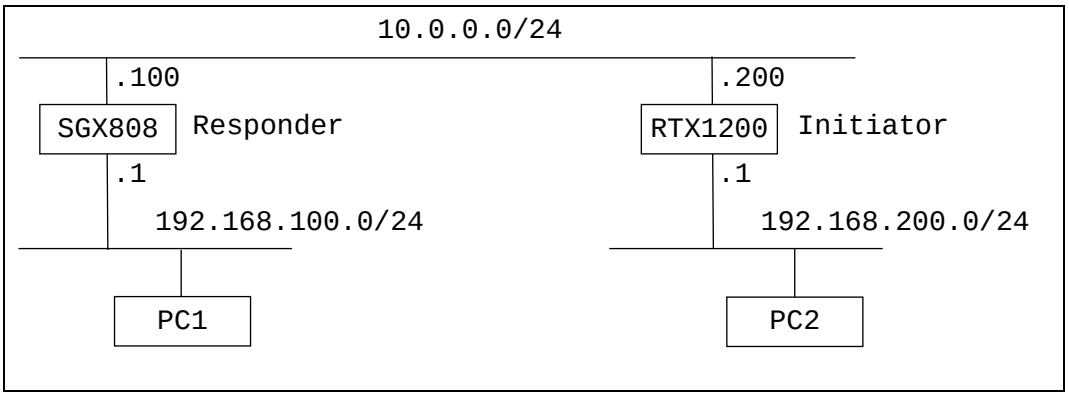


図 5.2.2-1 構成例

SGX808

LAN 側アドレス：192.168.100.1

WAN 側アドレス：10.10.10.100

RTX1200

LAN 側アドレス：192.168.200.1

WAN 側アドレス：10.0.0.200

- RTX1200 の設定例

```
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)
```



```
 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
```

図 5.2.2-2　RTX1200 の設定例

ip route 192.168.100.0/24 gateway tunnel 1

相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24
ip lan2 address 10.0.0.200/24

LAN1,LAN2 に固定アドレスを設定します。

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

LAN2 インタフェースに NAT マスカレードを設定します。

ipsec tunnel 1
tunnel enable 1

IPsec 定義の適用と自動鍵交換を行うように設定します。

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

相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。
このときオプションとして local-id と remote-id も設定します。
Pre-Shared-Key は相手側と同じものを設定します。

ipsec ike backward-compatibility 1 2

IKEv1 鍵交換タイプを 2 に設定します。

※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。
※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

ipsec ike local name 1 bob fqdn
local name には適当な名前を設定します。(設定例：bob）
この設定により Aggressive mode で動作するようになります。

ipsec ike payload type 1 2
ipsec ike remote address 1 10.0.0.100
ipsec ike remote name 1 alice
payload のタイプを 2 に設定します。
remote address には相手側のグローバルアドレスを設定します。
remote name には相手側の名前を設定します。(設定例：alice）

ipsec ike send info 1 off
IKE の情報ペイロードを送信しないように設定します。
SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- SGX808 の設定例

表 5.2.2 SGX808 の設定例

項目	内容	設定例
Name	適当な名称を設定します。	example
Pre-Shared-Key	相手先の設定と同じ Pre-Shared-Key を設定します。（RTX1200 の設定例(*1)）	test
Destination	相手先のアドレスを設定します。（RTX1200 の設定例(*2)）	10.0.0.200
Destination ID	相手先の ID を設定します。（RTX1200 の設定例(*3)）	bob
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。（RTX1200 の設定例(*4)）	192.168.200.1
Destination Local Network	相手先のローカル側のネットワークアドレスとサブネットマスクアドレスを設定します。	192.168.200.0 / 255.255.255.0
Source	"Aggressive mode"を選択します。	"Aggressive mode"
Source IP Address	"Aggressive mode"なので、設定できません。	
Source ID	相手先と同じ key-id を設定します。（RTX1200 の設定例(*6)）	alice

Authentication Algorithm	相手先で設定されたアルゴリズムに従います。 （RTX1200 の設定例(*5)）	“HMAC-SHA”
Encryption Algorithm	相手先で設定されたアルゴリズムに従う。 （RTX1200 の設定例(*5)）	“AES-CBC”
Information Mode	"Responder"を選択します。	"Responder"

5.2.3 Aggressive mode（on PPPoE）

PPPoE の設定を必要とした場合の例を説明します。この場合、SGX808 を Responder として動作させるためには「DDNS クライアント機能」を動作させておく必要があります。SGX808 の PPPoE 設定、DDNS クライアント設定の説明は省略します。

- 構成例

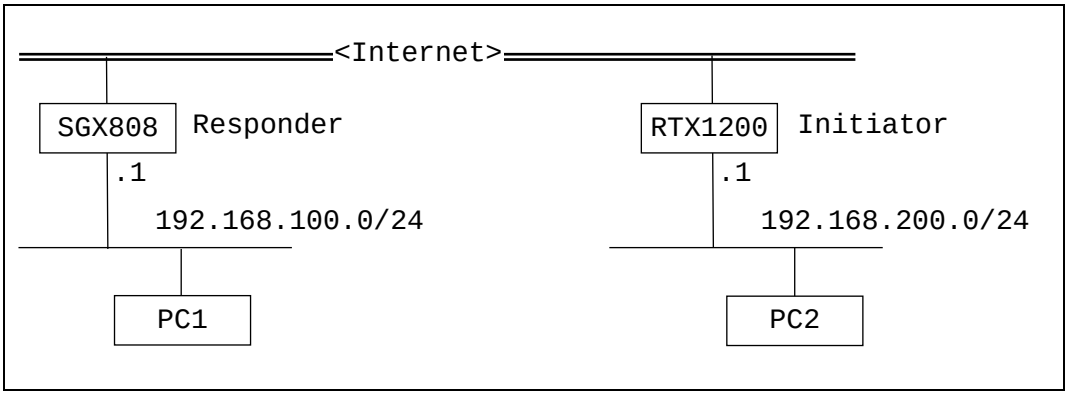


図 5.2.3-1 構成例

SGX808

LAN 側アドレス：192.168.100.1

WAN 側アドレス：sgx808a.xxx.xxx

予め適当な DDNS サービスにて割り当てられた名称

RTX1200

LAN 側アドレス：192.168.200.1

WAN 側アドレス：不定

WAN 側ホスト名：xxx.yyy.netvolante.jp

予めネットボランチ DNS サービスで割り当てられた名称

- RTX1200 の設定例

```
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)
 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
```

図 5.2.3-2　RTX1200 の設定例

ip route default gateway pp 1
ip route 192.168.100.0/24 gateway tunnel 1
　デフォルト経路を pp に設定します。
　相手側 LAN への経路をトンネルに設定します。

ip lan1 address 192.168.200.1/24
　LAN1 に固定アドレスを設定します。

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
PPPoE を設定します。ホスト名も登録します。

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
pp インタフェースに NAT マスカレードを設定します。
WAN 側の IP アドレスとして、PPP の接続先から通知される IP アドレスを起用するようにします。

ipsec tunnel 1
tunnel enable 1
IPsec 定義の適用と自動鍵交換を行うように設定します。

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
相手側のセキュリティ・ゲートウェイに対する SA のポリシーを設定します。
このときオプションとして local-id と remote-id も設定します。
Pre-Shared-Key は相手側と同じものを設定します。

ipsec ike always-on 1 on
ipsec auto refresh on
IKE の鍵交換に失敗したときに鍵交換を休止せずに継続できるようにします。
鍵交換を始動するようにします。(Initiator として動作します)

ipsec ike backward-compatibility 1 2
IKEv1 鍵交換タイプを 2 に設定します。
※認証アルゴリズムに HMAC-SHA256、暗号アルゴリズムに SDES-CBC を設定した場合には、必須となります。
※本コマンドはファームウェアバージョン Rev.10.01.55 以降に追加されています。

ipsec ike local name 1 bob fqdn

local name には適当な名前を設定します。(設定例：bob）
この設定により Aggressive mode で動作するようになります。

ipsec ike payload type 1 2
ipsec ike remote address 1 sgx808a.xxx.xxx
ipsec ike remote name 1 alice
payload のタイプを 2 に設定します。
remote address には相手側のホスト名を設定します。
remote name には相手側の名前を設定します。(設定例：alice）

ipsec ike send info 1 off
IKE の情報ペイロードを送信しないように設定します。
SGX808 は、ISAKMP SA の delete の informational パケットを受信すると IPsec のセッションを切断するように動作してしまうため、この設定をしておく必要があります。

- SGX808 の設定例

PPPoE 及び DDNS クライアントの設定は省略します。IPsec の設定は「5.2.2 Aggressive mode」の場合の設定とほぼ同じです。相手先として、相手先に割り当てられているホストネームを指定します。

表 5.2.3　SGX808 の設定例

項目	内容	設定例
Name	適当な名称を設定します。	example
Pre-Shared-Key	相手先の設定と同じ Pre-Shared-Key を設定します。（RTX1200 の設定例(*1)）	test
Destination	相手先のアドレスを設定します。（RTX1200 の設定例(*2)）	xxx.yyy.netvolante.jp
Destination ID	相手先の ID を設定します。（RTX1200 の設定例(*3)）	bob
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。（RTX1200 の設定例(*4)）	192.168.200.1
Destination Local Network	相手先のローカル側のネットワークアドレスとサブネットマスクアドレスを設定します。	192.168.200.0 / 255.255.255.0
Source	"Aggressive mode"を選択します。	"Aggressive mode"
Source IP Address	"Aggressive mode"なので、設定できません。	
Source ID	相手先と同じ key-id を設定します。（RTX1200 の設定例(*6)）	alice
Authentication	相手先で設定されたアルゴリズムに従います。	“HMAC-SHA”

Algorithm	（RTX1200 の設定例(*5)）	
Encryption Algorithm	相手先で設定されたアルゴリズムに従う。 （RTX1200 の設定例(*5)）	“AES-CBC”
Information Mode	"Responder"を選択します。	"Responder"

5.3 SGX808 同士の接続

SGX808 同士を接続する例を説明します。

5.3.1 Aggressive mode

接続モードが Aggressive mode の場合の例を説明します。

ここでは、Aggressive mode の接続例を説明していますが、Main mode でも同様です。

- 構成例

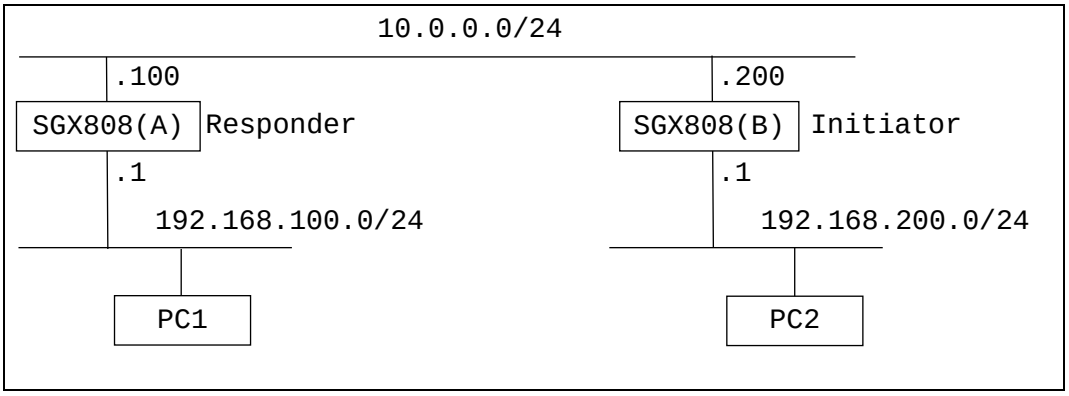


図 5.3.1 構成例

SGX808(A)

LAN 側アドレス：192.168.100.1

WAN 側アドレス：10.10.10.100

SGX808(B)

LAN 側アドレス：192.168.200.1

WAN 側アドレス：10.0.0.200

- SGX808(A)(B)の設定例

表 5.3.1 SGX808 の設定例

項目	内容	設定例	
		(A)	(B)
Name	適当な名称を設定します。	A	B
Pre-Shared-Key	互いに同じ Pre-Shared-Key を設定します。	test	test
Destination	相手先の WAN アドレスを設定します。	10.0.0.200	10.0.0.100
Destination ID	相手先の Source ID を設定します。	bob	alice
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。	192.168.200.1	192.168.100.1
Destination Local	相手先のローカル側のネットワー	192.168.200.0/	192.168.100.0/

Network	クアドレスとサブネットマスクアドレスを設定します。	255.255.255.0	255.255.255.0
Source	"Aggressive mode"を選択します。	"Aggressive mode"	"Aggressive mode"
Source IP Address	"Aggressive mode"なので、設定できません。		
Source ID	適当な ID を設定します。	alice	bob
Authentication Algorithm	互いに同じアルゴリズムを設定します。	“HMAC-SHA”	“HMAC-SHA”
Encryption Algorithm	互いに同じアルゴリズムを設定します。	“AES-CBC”	“AES-CBC”
Information Mode	片方を"Responder"に、他方を”Initiator”に設定します。	"Responder"	"Initiator"

5.3.2 Aggressive mode（on PPPoE）

PPPoE の設定を必要とした場合の例を説明します。この場合、「DDNS クライアント機能」を動作させておく必要があります。PPPoE 設定、DDNS クライアント設定の説明は省略します。

- 構成例

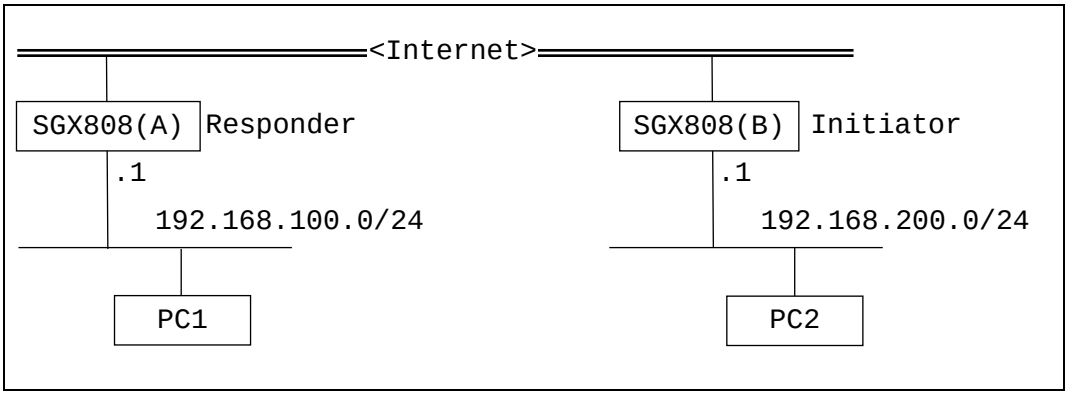


図 5.3.2 構成例

SGX808(A)

LAN 側アドレス：192.168.100.1

WAN 側ホスト名：sgx808a.xxx.xxx

予め適当な DDNS サービスにて割り当てられた名称

SGX808(B)

LAN 側アドレス：192.168.200.1

WAN 側ホスト名：sgx808b.xxx.xxx

予め適当な DDNS サービスにて割り当てられた名称

- SGX808(A)(B)の設定例

表 5.3.2 SGX808 の設定例

項目	内容	設定例	
		(A)	(B)
Name	適当な名称を設定します。	A	B
Pre-Shared-Key	互いに同じ Pre-Shared-Key を設定します。	test	test
Destination	相手先の WAN アドレスを設定します。	sgx808b.xxx.xxx	sgx808a.xxx.xxx
Destination ID	相手先の Source ID を設定します。	bob	alice
Destination Local IP Address	相手先のローカル側の IP アドレスを設定します。	192.168.200.1	192.168.100.1
Destination Local Network	相手先のローカル側のネットワークアドレスとサブネットマスクア	192.168.200.0/ 255.255.255.0	192.168.100.0/ 255.255.255.0

	ドレスを設定します。		
Source	"Aggressive mode"を選択します。	"Aggressive mode"	"Aggressive mode"
Source IP Address	"Aggressive mode"なので、設定できません。		
Source ID	適当な ID を設定します。	alice	bob
Authentication Algorithm	互いに同じアルゴリズムを設定します。	“HMAC-SHA”	“HMAC-SHA”
Encryption Algorithm	互いに同じアルゴリズムを設定します。	“AES-CBC”	“AES-CBC”
Information Mode	片方を"Responder"に、他方を”Initiator”に設定します。	"Responder"	"Initiator"

6　補足

6.1　Rekey

rekey のインターバルは以下の計算式となっています。

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

`rekeytime` : rekey インターバル
`lifetime` : IPsec SA の寿命(20 分)
`margintime` : マージン(3 分)
`rekeyfuzz` : 100%

計算に要する各値は変更不可です。つまり rekey インターバルは 14～17 分となります。

6.2　Keepalive

対向側としてヤマハ製のルーターを使用する場合で、keepalive 機能を設定する場合に使用できる keepalive 方式は ICMP Echo のみです。他の方式を設定した場合には、途中で切断する可能性があるので使用できません。