4 二重化構成について

FirewallServerを2台使用した二重化機能の使用方法について説明します。

概　要

二重化構成について説明します。

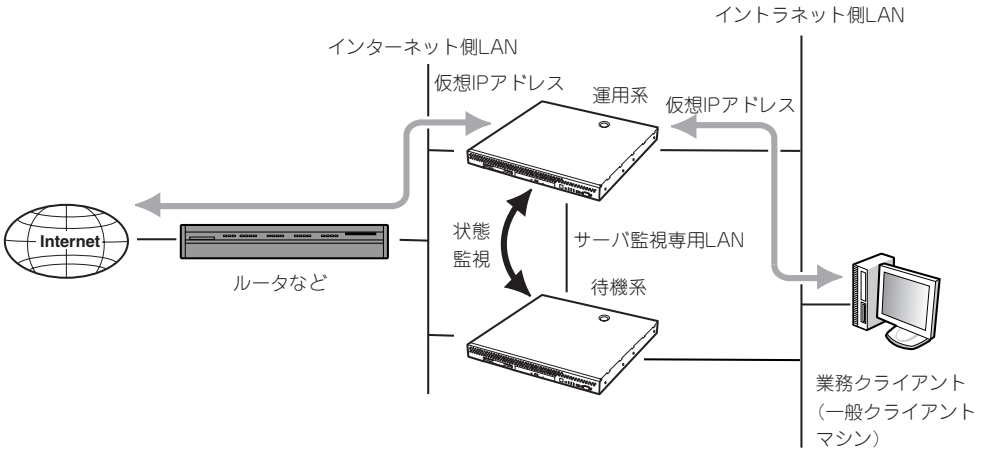
動作概要

FirewallServerを二重化することで一台が障害などにより停止しても、もう一台のサーバへ自動的に引き継ぐことにより、障害時の業務停止時間を最小限に抑えることができます。

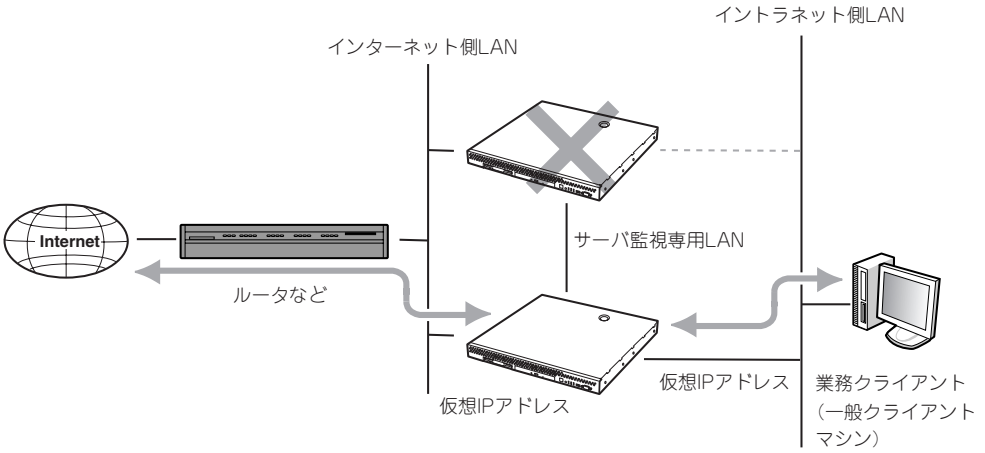
また、運用系で FireWall-1 プロセスの異常を検出した場合、及び、設定された IPアドレスとの通信が途絶した場合にも、待機系に業務を引継ぐことが可能です。

二重化の仕組みを次に示します。

- **通常運用時**
  - 運用系側のFirewallServerで有効にした仮想IPアドレスを使用してインターネット側、イントラネット側の双方からアクセスします。
  - 運用系/待機系のFirewallServerは互いにサーバの状態を監視をします。



- **運用系サーバダウン時**
  - 待機系のFirewallServerが運用系のダウンを検出します。
  - 待機系のFirewallServerが仮想IPアドレスを有効にします。
  - インターネット側、イントラネット側の双方からのアクセスは仮想IPアドレスを使用しているのでサーバの切り替わりを意識することはありません。



DMZを使用する場合もイントラネット、インターネット同様に仮想IPアドレスが引き継がれます。

構　成

FirewallServerでは以下の構成で二重化させることができます。

- **一体型構成**

  FirewallServer2台のみで二重化可能な構成です。それぞれのサーバで管理を行います。FirewallServerには同一ライセンスが2つ必要になります。一体型構成では「UL4005-1x1 Express5800/FirewallServer nライセンス」が使用可能です。

  一体型構成ではVPN通信の二重化はできません。また、障害発生時に接続されていたセッションは切断されます。

- **分散型構成**

  FirewallServer2台のほかに管理用サーバが1台必要な構成です。管理用サーバにFireWall-1管理モジュールをインストールし、2台のFirewallServerを管理します。

  FirewallServerには同一ライセンスが2つ必要になります。分散型構成では下記ライセンスのどちらかが使用可能です。

  ー　UL4005-1x5 Express5800/FirewallServer多重化 nライセンス

  ー　UL4005-1x6 Express5800/FirewallServer多重化（VPN機能付） nライセンス

  管理用サーバには「UL4005-104 Express5800/FirewallServer統合管理ツール」が必要です。

一体型構成と分散型構成では必要なライセンスの種類が異なります。ライセンスを購入する際にはご注意ください。

必要なリソース

二重化を実現するためにFirewallServerを単体で運用するときに比べて新たなリソースが必要です。
セットアップの前にリソースの計画や設定をしてください。

- **仮想IPアドレス(インターネット側): 1つ**

  インターネット側で引き継ぐアドレスです。

  インターネット側のネットワークアドレス内で未使用のホストアドレスをアサインしてください。

  このアドレスはサーバに設定する必要はありません。

- **仮想IPアドレス(イントラネット側): 1つ**

  イントラネット側で引き継ぐアドレスです。

  イントラネット側のネットワークアドレス内で未使用のホストアドレスをアサインしてください。

  このアドレスはサーバに設定する必要はありません。

- **仮想IPアドレス(DMZ側): 1つ**

  DMZで引き継ぐアドレスです。

  DMZを設けない場合には不要です。

  DMZのネットワークアドレス内で未使用のホストアドレスをアサインしてください。

  このアドレスはサーバに設定する必要はありません。

- **サーバ間通信用アドレス: 1つ以上**

  FirewallServer間の監視に使用するアドレスです。

  インターネット側、イントラネット側と共用にしても問題はありませんが、可能であれば、専用のポートを使用してください。

  専用のポートが用意できる場合、サーバ間をクロスケーブルで接続してください。

  それぞれのサーバに最低一つずつ設定してください。

一体型構成での設定手順

以下のネットワーク構成を例にとって設定を行います。

- **運用系サーバ**

ホスト名:	fws1
インターネット側実IPアドレス:	202.247.5.1/255.255.255.0
DMZ側実IPアドレス:	172.16.1.1/255.255.255.0
イントラネット側実IPアドレス:	192.168.1.1/255.255.255.0
サーバ間通信用IPアドレス:	192.168.2.1/255.255.255.0

- **待機系サーバ**

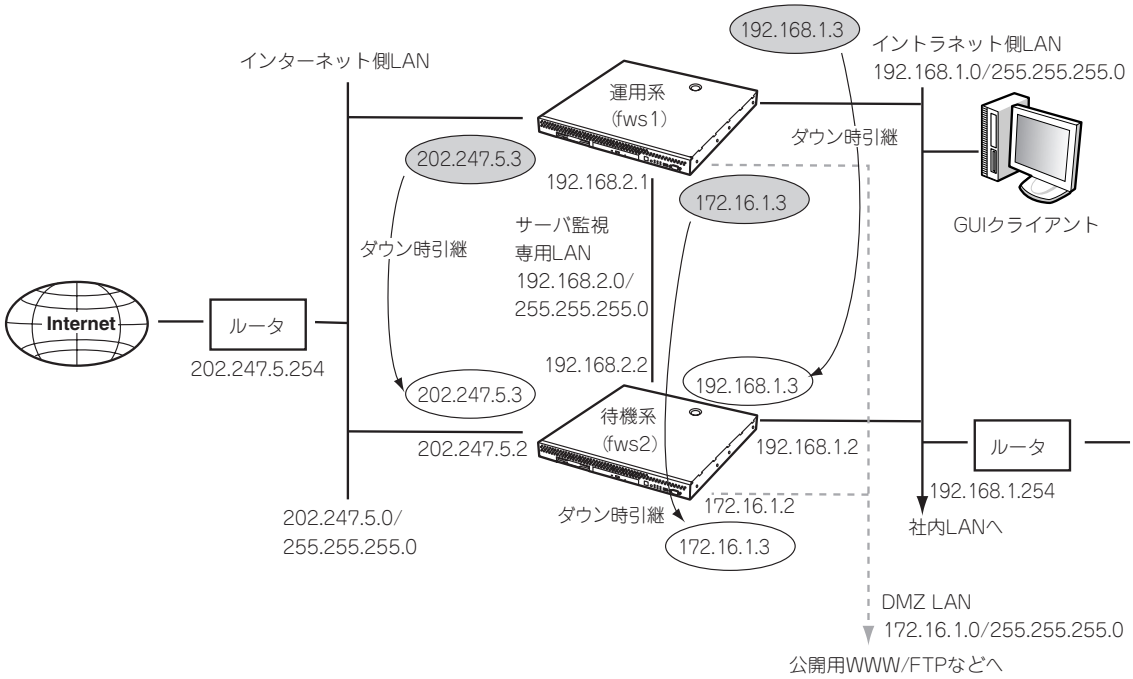
ホスト名:	fws2
インターネット側実IPアドレス:	202.247.5.2/255.255.255.0
DMZ側実IPアドレス:	172.16.1.2/255.255.255.0
イントラネット側実IPアドレス:	192.168.1.2/255.255.255.0
サーバ間通信用IPアドレス:	192.168.2.2/255.255.255.0

- **仮想IPアドレス**

インターネット側:	202.247.5.3
DMZ側:	172.16.1.3
イントラネット側:	192.168.1.3

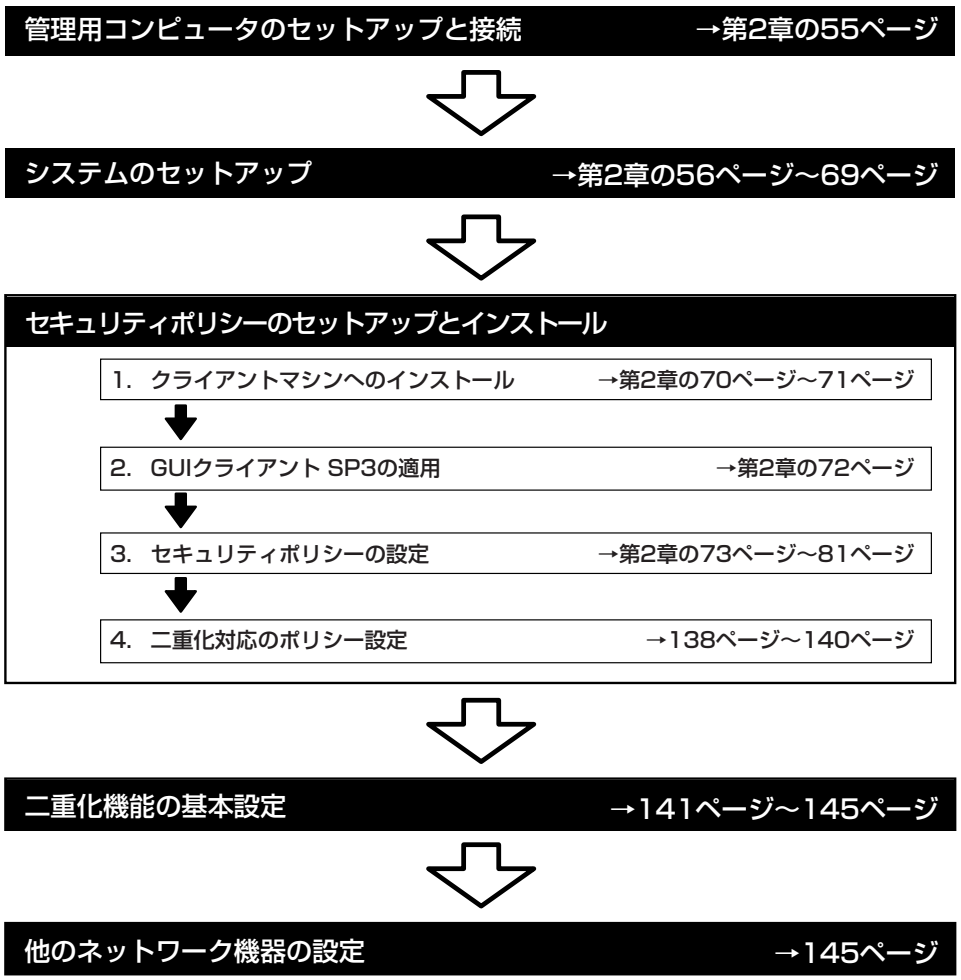
- **監視先IPアドレス**

インターネット側ルータ:	202.247.5.254
イントラネット側ルータ:	192.168.1.254



セットアップの流れ

以下にセットアップの流れを示します。「セキュリティポリシーの設定」までの手順は第2章の「セットアップ」を参照してください。ここでは「二重化対応のポリシー設定」以降の手順を説明します。



二重化対応のポリシー設定

基本的に二重化する2台のFirewallServerには同一のポリシーを設定します。ただし、以下の点に注意してください。

- 自ファイアウォールを定義する際には、実IPアドレスで定義します。
- HideモードのNATを使用する場合、「Hiding IP Address」には仮想IPアドレスを指定します。

また、二重化機能を使用するためには、以下の2つのルールを追加する必要があります。

- FirewallServer間の状態監視用通信を通すためのルール
- FirewallServerと監視対象との間の通信を通すためのルール

fws1側での設定例を示します。fws2側でも同様の設定をしてください。

1. ネットワークオブジェクトとして以下の3オブジェクトを追加する。

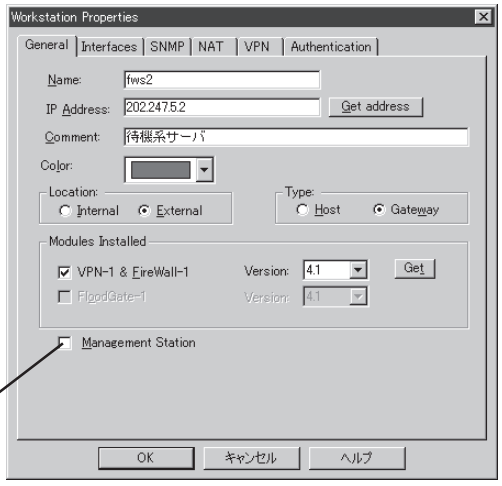
   設定例ではホスト名を名前として設定していますが、必ずしもホスト名にあわせる必要はありません。

   オブジェクト
   Workstation

   名前
   fws2

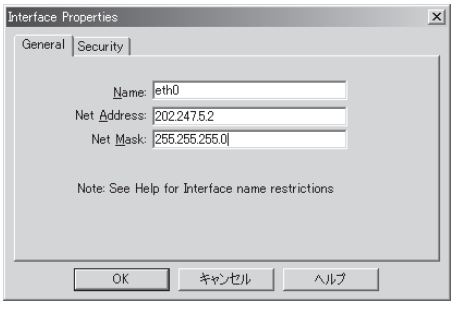
   内容
   対となるもう一方のFirewallServerを定義する。

   「VPN-1&FireWall-1」にチェックして、「Location」はExternal、「Type」はGatewayを選択する。
   「Management Station」にはチェックしないでください。



「Management Station」にはチェックしない

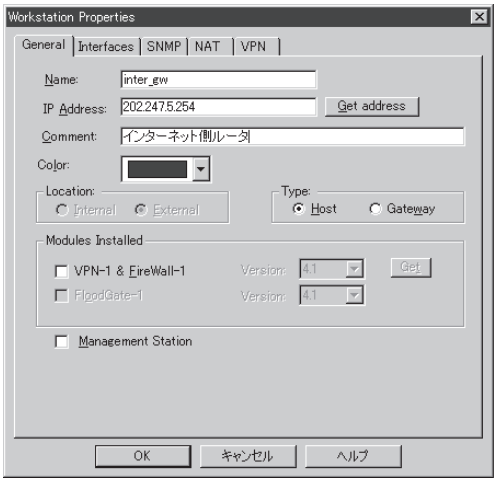
   Interfacesタブで全部のインタフェースを設定してください。他のタブは設定する必要ありません。



オブジェクト
Workstation

名前
inter_gw

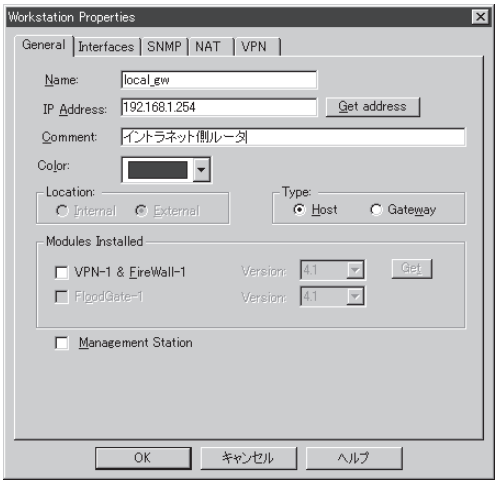
内容
ネットワーク監視に使用するインターネット側のルータ。



オブジェクト
Workstation

名前
local_gw

内容
ネットワーク監視に使用するイントラネット側のルータ



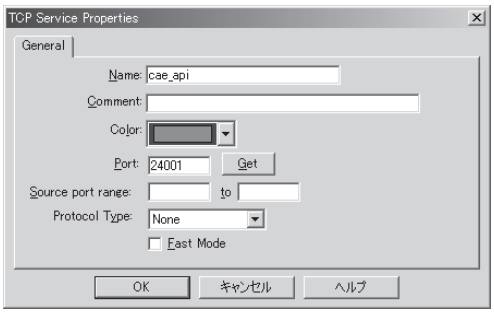
2. 以下のサービスを定義する。

名前は一例です。他の名前でも構いません。

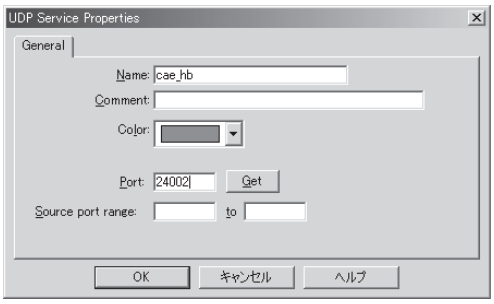
重要

ポート番号はデフォルトのポート番号です。 二重化機能の基本設定でポート番号を変更する場合はその設定に合わせてサービスの定義を行ってください。

オブジェクト: TCP
名前: cae_api
ポート: 24001



オブジェクト: UDP
名前: cae_hb
ポート: 24002



3. 二重化通信用のルールを追加する。

ルールセットの一番上にくるように追加してください。以下のポリシーのルール1、2が追加分です。

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	fws2	fws1	cae_api cae_hb	accept		Gateways	Any	
2	inter_gw local_gw	fws1	icmp-proto	accept		Gateways	Any	
3	Any	fws1	Any	drop	Alert	Gateways	Any	Stealth the Firewall attack prot
4	localnet	mailer	pop-3	accept	Long	Gateways	Any	E-Mail retrieval rule
5	Any	mailer	smtp	accept	Long	Gateways	Any	Allow access to Mail server
6	Any	FtpWebServer	http ftp	accept	Long	Gateways	Any	Ftp and Web Server
7	dmz-net	localnet	Any	reject	Alert	Gateways	Any	Protect localnet from the DMZ
8	localnet	dmz-net	Any	reject	Alert	Gateways	Any	Protect DMZ from the localnet
9	localnet	Any	Any	accept	Long	Gateways	Any	Allow Outgoing traffic
10	Any	Any	SilentServices	drop		Gateways	Any	Silent drop for broadcast pack
11	Any	Any	Any	drop	Alert	Gateways	Any	Last rule

4. セキュリティポリシーをインストールする。

セキュリティポリシーの作成が完了したら、ポリシーをインストールしてください。

二重化機能の基本設定

二重化機能の基本設定方法を説明します。設定は基本設定ツールから行います。
以降の設定はfws1、fws2とも同じ設定にしてください。

```
# /opt/necfws/bin/fwsetup ····· ①
Firewall Server configuration tool Ver.1.3
            <省略します。2章の「セットアップ」を参照してください。>
use cluster system? (y/n)[y]: y ····· ②
---- START CLUSTERPRO AE configuration ---------------
CLUSTERPRO AE Configuration Tool Ver 1.0
---- cluster configuration ----------------------------
Input HB interval(1 - 999)[1] : ····· ③
Input HB timeout(1 - 999)[5] : ····· ④
Input API TCP port number[24001] : ····· ⑤
Input HB UDP port number[24002] : ····· ⑥
Input server1 host name : fws1 ····· ⑦
Input server2 host name : fws2 ····· ⑧
```

① 基本設定ツールを起動する。

② 二重化機能を使用するかどうかの問いに[y]でこたえる。

③ サーバ監視パケット送信間隔(ハートビート送信間隔)(秒)を入力する。

④ サーバダウンと認識するまでの時間(ハートビートタイムアウト時間)(秒)を入力する。

⑤ 内部通信用 TCP ポート番号を入力する。

⑥ 内部通信用 UDP ポート番号を入力する。

⑦ 運用系サーバのホスト名を入力する。

ホスト名は FQDN形式ではなく、ドメイン名部分を除いた名前を指定してください。

⑧ 待機系サーバのホスト名を入力する。

ホスト名は FQDN形式ではなく、ドメイン名部分を除いた名前を指定してください。

```
---- server configuration ----------------------------

Input fws1 interconnect address ·····①
address(1) : 192.168.2.1
netmask(1) : 255.255.255.0
address(2) : 192.168.1.1
netmask(2) : 255.255.255.0
address(3) :
 No.  address/netmask
  1   192.168.2.1/255.255.255.0
  2   192.168.1.1/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):

Input fws2 interconnect address ·····②
address(1) : 192.168.2.2
netmask(1) : 255.255.255.0
address(2) : 192.168.1.2
netmask(2) : 255.255.255.0
address(3) :
 No.  address/netmask
  1   192.168.2.2/255.255.255.0
  2   192.168.1.2/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 運用系サーバのサーバ間監視用アドレス(インタコネクトアドレス)とネットマスクを入力する。

設定後に一覧を表示します。

一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter> キー:	インタコネクトアドレスを追加する。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正する。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除する。
<L>キー+<Enter>キー:	一覧を再表示する。
<Enter>キー:	次の項目へスキップする。

② 待機系サーバのサーバ間監視用アドレス(インタコネクトアドレス)とネットマスクを入力する。

運用系サーバの場合と同様に一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

```
---- fip configuration ------------------------------

Input FIP address ·····①
address(1) : 202.247.5.3
netmask(1) : 255.255.255.0
address(2) : 172.16.1.3
netmask(2) : 255.255.255.0
address(3) : 192.168.1.3
netmask(3) : 255.255.255.0
address(4) :
 No.  address/netmask
  1   202.247.5.3/255.255.255.0
  2   172.16.1.3/255.255.255.0
  3   192.168.1.3/255.255.255.0

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 仮想IPアドレスを入力する。

設定後に一覧を表示します。

一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter> キー:	仮想IP アドレスを追加します。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正します。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除します。
<L>キー+<Enter>キー:	一覧を再表示します。
<Enter>キー:	次の項目へスキップします。

二重化機能を使用する場合、FirewallServerへのアクセスは、原則仮想IPアドレスを使用する必要があります。
サーバ間監視専用インターフェース以外の全インターフェースに仮想IPアドレスを設定してください。

```
---- ipw configuration -------------------------------

Input IPW address address ..... ①
address(1) : 202.247.5.254
address(2) : 192.168.1.254
address(3) :
 No.  address
  1   202.247.5.254
  2   192.168.1.254

("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 監視する IPアドレスを入力する。

「¦」で区切って複数の IPアドレスを入力することができます。その場合は、指定した全IPアドレスとの通信が途絶した場合にリソース異常となります。

監視する IPアドレスは 8個まで設定可能です。ただし、「¦」で区切ったIPアドレスは全体で1つのIPアドレスとしてカウントします。

設定後に一覧を表示します。一覧から設定内容の追加、および修正、削除、一覧の再表示をキー入力から操作できます。

<A>キー + <Enter> キー:	監視するIPアドレスを追加します。
<M>キー+「修正する一覧の番号」+<Enter>キー:	指定した番号の設定を修正します。
<D>キー+「削除する一覧の番号」+<Enter>キー:	指定した番号の設定を削除します。
<L>キー+<Enter>キー:	一覧を再表示します。
<Enter>キー:	次の項目へスキップします。

監視対象として設定された IPアドレスとの通信が途絶した場合、待機系サーバにフェイルオーバが行われます。

<設定例>

- 202.247.5.254と192.168.1.254のどちらかと通信が途絶した場合にフェイルオーバを行いたい場合。

  No. address

  1 202.247.5.254
  2 192.168.1.254

- 202.247.5.254と192.168.1.254の双方と通信が途絶した場合にフェイルオーバを行いたい場合。

  No. address

  1 202.247.5.254 ¦ 192.168.1.254

- 202.247.5.5と202.247.5.254 の双方と通信が途絶した場合か、192.168.1.254と通信が途絶した場合にフェイルオーバを行いたい場合

  No. address

  1 202.247.5.5 ¦ 202.247.5.254
  2 192.168.1.254

```
---- resource configuration --------------------------

Input primary server hostname(fws1, fws2)[fws1] : ..... ①

Input failback policy(1:auto, 2:manual)[manual] : ..... ②

---- END CLUSTERPRO AE configuration ----------------- ..... ③

once again input? (y/n)[n]:

change root password? (y/n)[n]:

Thu May 17 20:21:50 JST 2001
set date and time? (y/n)[n]:


stop unnecessary services? (y/n)[n]:

Please reboot the system.

# shutdown -r now ..... ④
```

① 運用系サーバを入力する。

② 自動フェイルバックを行うかどうか入力する。

自動フェイルバックをautoにした場合、運用系ダウン後、待機系に業務が引き継がれている状態で、運用系が復帰(起動)すると、自動的に運用系に業務を戻します。

③ 二重化機能の設定の終了。

④ 再起動する。

他のネットワーク機器の設定

イントラネットとDMZに存在するネットワーク機器については、デフォルトルートの設定として それぞれのネットワークの仮想IPアドレス(イントラネット側: 192.168.1.3、DMZ側: 172.16.1.3)を指定するようにしてください。

分散型構成での設定手順

以下のネットワーク構成を例にとって設定を行います。

- **運用系サーバ**

  ホスト名: fws1
  インターネット側実IPアドレス: 202.247.5.1/255.255.255.0
  DMZ側実IPアドレス: 172.16.1.1/255.255.255.0
  イントラネット側実IPアドレス: 192.168.1.1/255.255.255.0
  サーバ間通信用IPアドレス: 192.168.2.1/255.255.255.0

- **待機系サーバ**

  ホスト名: fws2
  インターネット側実IPアドレス: 202.247.5.2/255.255.255.0
  DMZ側実IPアドレス: 172.16.1.2/255.255.255.0
  イントラネット側実IPアドレス: 192.168.1.2/255.255.255.0
  サーバ間通信用IPアドレス: 192.168.2.2/255.255.255.0

- **仮想IPアドレス**

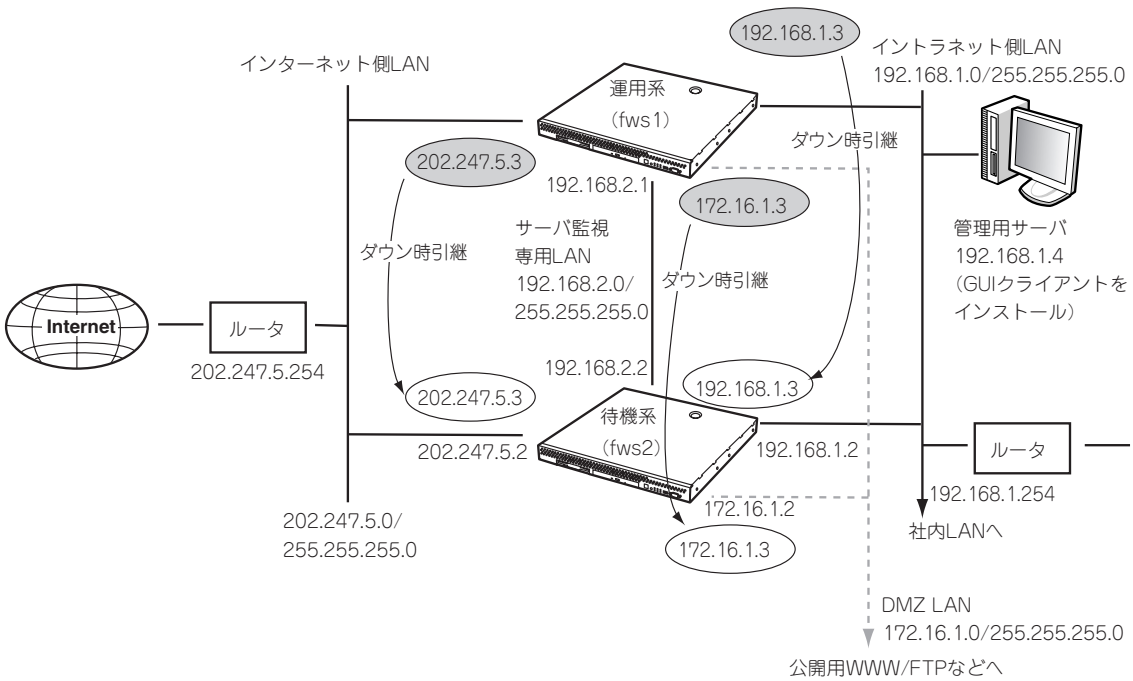
  インターネット側: 202.247.5.3
  DMZ側: 172.16.1.3
  イントラネット側: 192.168.1.3

- **監視先IPアドレス**

  インターネット側ルータ: 202.247.5.254
  イントラネット側ルータ: 192.168.1.254

- **管理用サーバ**

  ホスト名: firewall_manager
  IPアドレス: 192.168.1.4/255.255.255.0



セットアップの流れ

以下にセットアップの流れを示します。ここでは二重化に関する設定内容のみを説明します。その他の手順については第2章の「セットアップ」を参照してください。

管理用コンピュータのセットアップと接続 →第2章の55ページ

⇩

FireWall-1管理サーバのセットアップ →148ページ～152ページ

⇩

FirewallServerのセットアップ

1. 設定ツールによる基本設定 →第2章の58ページ～61ページ
2. FireWall-1モジュールの展開 →第2章の62ページ
3. FireWall-1 SP3の適用 →第2章の62ページ
4. FireWall-1のコンフィグレーション →153ページ～155ページ
5. FireWall-1同期の設定 →156ページ

⇩

セキュリティポリシーのセットアップとインストール

1. クライアントマシンへのインストール →第2章の70ページ～71ページ
2. GUIクライアントSP3の適用 →第2章の72ページ
3. FirewallServerとFireWall-1管理サーバ間の通信設定 →157ページ～159ページ
4. セキュリティポリシーの設定 →160ページ～164ページ

⇩

二重化機能の基本設定 →165ページ

⇩

他のネットワーク機器の設定 →165ページ

FireWall-1管理サーバのセットアップ

分散型構成でインストールされた2台のFirewallServerを管理するための管理用サーバをセットアップします。以下の条件を満たすコンピュータにFireWall-1管理モジュールをインストールしてください。

オペレーティングシステム:	Windows NT 4.0 Server (SP4、SP5、SP6)、Solaris/SPARC 2.6、Solaris/SPARC 7(32bitモードのみ)、RedHat Linux 6.1(SMP kernel)、6.2 (SMP kernel) - kernel version 2.2.x
ディスク空き容量:	40MB以上
メモリ:	64MB以上、推奨128MB以上

以下はWindows NT 4.0 Serverにインストールする場合の例です。

FireWall-1管理モジュールのインストール

1. コンピュータのCD-ROMドライブにCheckPoint2000のCD-ROMをセットする。

   自動的にインストールプログラムが起動し、画面が表示されます。インストールプログラムが起動しない場合は¥wrappers¥windowsフォルダにある「demo32.exe」を実行してください。

2. [Next]ボタンをクリックする。

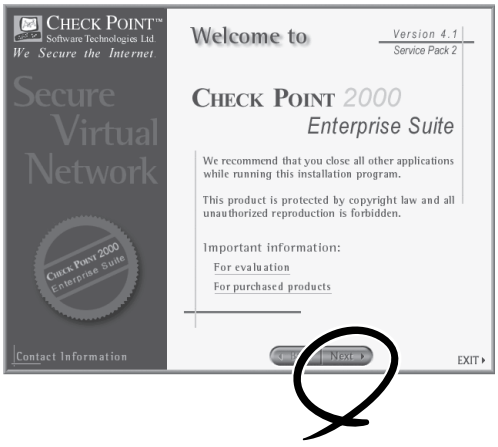
   使用許諾契約書が表示されます。

3. 内容をよく読み、同意する場合は[Yes]ボタンをクリックする。

   同意しない場合は[No]ボタンをクリックして終了します。プロダクトメニューの画面が表示されます。

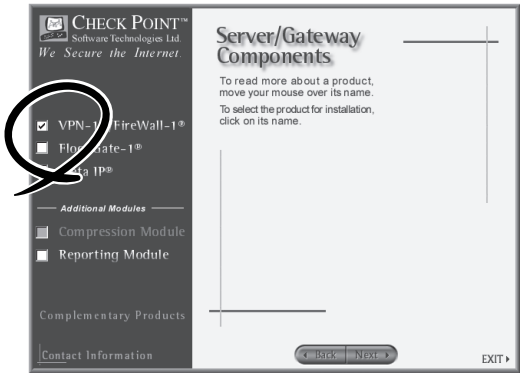
4. 「SERVER/GATEWAY COMPONENTS」を選択し、[Next]ボタンをクリックする。

   プロダクト選択の画面が表示されます。



5. 「VPN-1/FireWall-1」のみをチェックして、[Next]ボタンをクリックする。

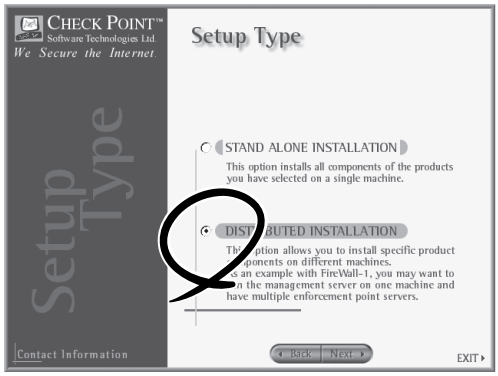
   その他のコンポーネントのチェックは外します。



6. タイプ選択で「DISTRIBUTED INSTALLATION」を選択し、[Next]ボタンをクリックする。

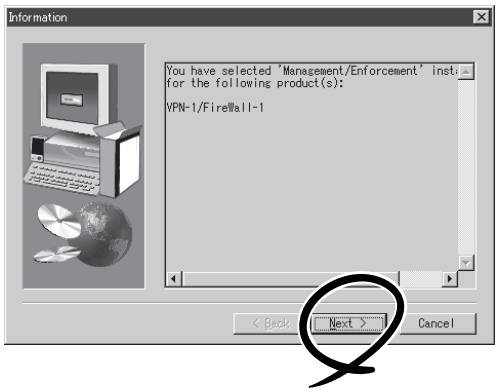
7. コンポーネント選択で「Management Server/EnforcementPoint Software」を選択し、[Next]ボタンをクリックする。

   インストール内容を確認する画面が表示されます。



8. 右図の内容が表示されていることを確認し、[Next]ボタンをクリックする。

   インストールするコンポーネントを選択する画面が表示されます。

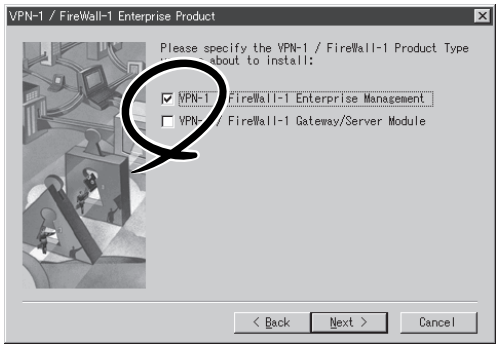


9. 「VPN-1/FireWall-1 Enterprise Management」のみをチェックして、[Next]ボタンをクリックする。

   旧バージョンのVPN-1/FireWall-1モジュールを管理するかを選択する画面が表示されます。

10. 「Install without backward compatibility」をチェックして、[Next]ボタンをクリックする。

    インストール先のフォルダを指定する画面が表示されます。



11. 必要に応じてフォルダを変更し、[Next]ボタンをクリックする。

    インストールが開始され、「CheckPoint VPN-1/FireWall-1 4.1」および「CheckPoint VPN-1/FireWall-1 4.1 SP2」がインストールされます。

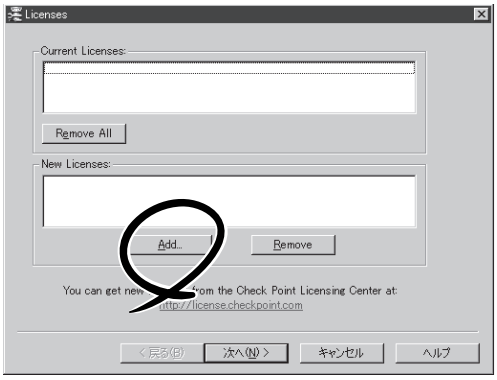
    「Meta IP」製品を統合するか確認メッセージが表示されます。

12. [いいえ]ボタンをクリックする。

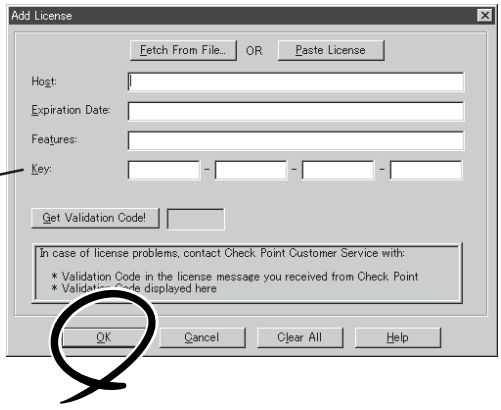
    引き続きFireWall-1のコンフィグレーションを行います。

    最初にライセンスの入力画面が表示されます。

13. [Add]ボタンをクリックする。



14. 取得したライセンスを入力し、[OK]ボタンをクリックする。



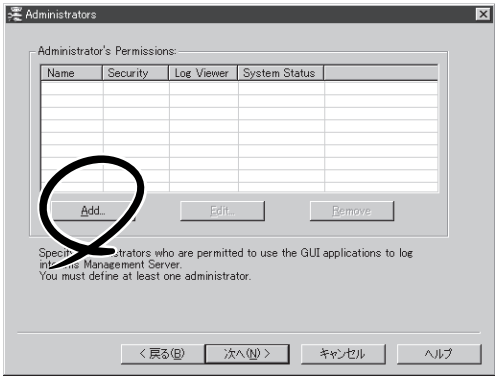
取得したライセンスを入力する

15. [次へ]ボタンをクリックする。

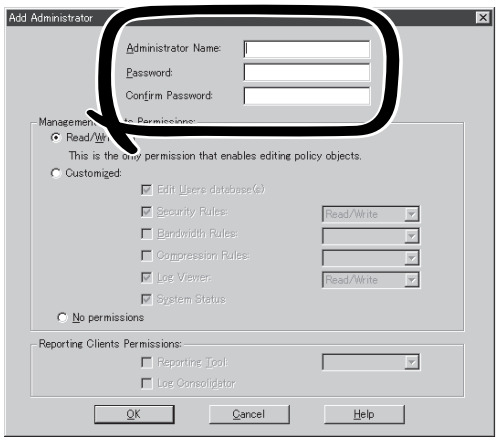
管理者の設定画面が表示されます。

16. [Add]ボタンをクリックする。

管理者の情報を入力する画面が表示されます。



17. FireWall-1の管理者、パスワード、および属性を設定する。



18. [次へ]ボタンをクリックする。

    コンピュータのIPアドレスが表示されます。

19. コンピュータのIPアドレスが表示されない場合、または表示されたIPアドレスが間違っている場合には正しいIPアドレスを入力する。

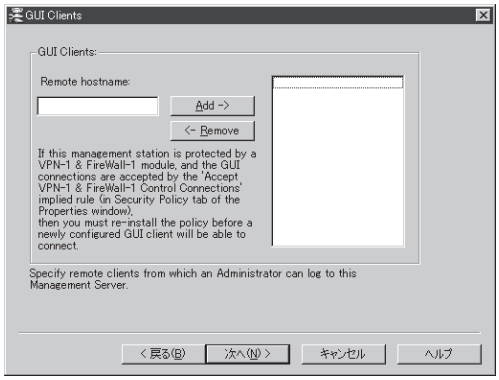
20. [次へ]ボタンをクリックする。

    GUIクライアントの設定画面が表示されます。

21. 本構築例ではGUIクライアントを管理サーバと同一のコンピュータにインストールするので設定必要ありません。GUIクライアントを別コンピュータにインストールする場合には、そのコンピュータのIPアドレスを設定してください。

22. [次へ]ボタンをクリックする。

    管理対象のFirewallServerの設定画面が表示されます。

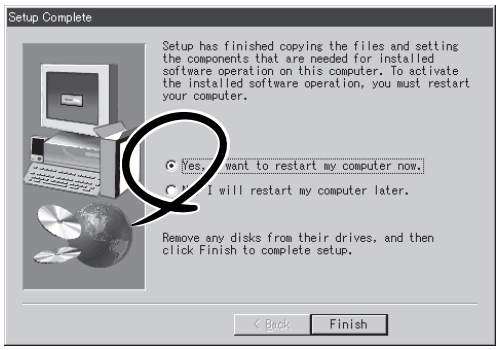


23. 管理対象のFirewallServerは後で設定するのでここでは何も入力せずに「次へ」ボタンをクリックする。

    ランダムキーを入力する画面が表示されます。

24. バーがフルになるまで入力する。

25. 設定が完了したらコンピュータを再起動する。



SP3のインストール

2001年5月末現在の最新サービスパックは、SP3(FW_1_41814_1_WIN32_DES.TGZ)です。
FireWall-1管理モジュールのSPは同梱されているCHECKPOINT製品パッチのCD-ROMから以下の手順でインストールします。

1. FireWall-1管理モジュールがインストールされているコンピュータのCD-ROMドライブにCHECKPOINT製品パッチのCD-ROMをセットする。

2. モジュール「FW_1_41814_1_WIN32_DES.TGZ」をコンピュータの適当なフォルダへコピーする。

   モジュールは、CD-ROMの[FW141]フォルダ→[SP3]フォルダ→[WIN32]フォルダ内にあります。

3. WinZip7.0などのツールを使いモジュールを解凍する。

   モジュールは圧縮されています。解凍されると[Disk_Images]フォルダ→[disk1]フォルダが形成され、[disk1]フォルダの中にモジュールが展開されます。

4. [disk1]フォルダの中にあるSetup.exeをダブルクリックする。

   インストールプログラムが起動し、画面の指示に従い[Next]ボタンをクリックします。
   使用許諾書が表示されます。

5. 問題が無ければ[Yes]ボタンをクリックする。

   [Yes]ボタンをクリックするとSP3のインストールが開始され数十秒で終了します。
   [No]ボタンをクリックした場合は、インストールは中断されます。

FireWall-1のコンフィグレーション

分散型構成の場合、設定項目が2章の「セットアップ」の記載とは一部異なります。以下の手順でコンフィグレーションを行ってください。

```
# cpconfig

Welcome to Check Point Configuration Program
================================================
Checking available options. Please wait.........

Choosing Installation
-------------------------
(1) VPN-1 & FireWall-1 Stand Alone Installation
(2) VPN-1 & FireWall-1 Distributed Installation

Option (1) will install VPN-1 & FireWall-1
Internet GateWay (Management Server and Enforcement Module)
on a single machine.
Option (2) will allow you to install specific
components of the VPN-1 & FireWall-1 Enterprise Products
on different machines.

Enter your selection (1-2/a):2 ..... ①

Installing VPN-1 & FireWall-1 Distributed Installation.

Which Module would you like to install ?
-----------------------------------------
(1) VPN-1 & FireWall-1 Enterprise Management and Gateway/Server Module
(2) VPN-1 & FireWall-1 Gateway/Server Module
(3) VPN-1 & FireWall-1 Enterprise Management

Enter your selection (1-3/a) [1]: 2 ..... ②

Which Module would you like to install ?
-----------------------------------------
(1) VPN-1 & FireWall-1 - Limited hosts (25, 50, 100, 250)
(2) VPN-1 & FireWall-1 - Unlimited hosts
(3) VPN-1 & FireWall-1 - SecureServer

Enter your selection (1-3/a) [2]: 1 ..... ③
```

① FireWall-1インストールタイプを選択する。

2を選択してください。

② インストールするコンポーネントを選択する。

2を選択してください。

③ ノード数が25,50,100,250の製品は1を、無制限の製品は2を選択する。

```
Would you like to install the High Availability product (y/n) [n] ? n

Do you wish to start VPN-1 & FireWall-1 automatically
from /etc/rc.d/rc3.d and /etc/rc.d/rc5.d (y/n) [y] ? y

VPN-1 & FireWall-1 startup code installed in /etc/rc.d/rc3.d and
/etc/rc.d/rc5.d

Configuring Licenses...
=======================
The following licenses are installed on this host:

Do you want to add licenses (y/n) [n] ? y ..... ①
Host:202.247.5.1
Date:
String:
Features:
This is Check Point VPN-1(TM) & FireWall-1(R) Version 4.1 (16May2001
14:42:03)

Host              Expiration Features
202.247.5.1       Never      xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx


Configuring Masters...
======================
Masters are trusted Management Stations which will
control this Check Point Module.

Do you want to add Management Stations (y/n) [y] ? n ..... ②


Configuring External Interface...
=================================
The External Interface is one of the VPN-1 & FireWall-1 host's interfaces
that is connected to an external network. Hosts that are located
on the external side of the Module will not be counted as
protected hosts for the License Enforcement mechanism.

Please enter external interface name:eth0
```

① ライセンス情報を入力する。

② 後で設定するので、ここでは<N>キーを押す。

```
************* Installation completed successfully *************

Starting FireWall-1 and FloodGate-1 ...
FireWall-1: Loading kernel module...
fwstart: Loading fw-1 kernel module
FireWall-1: Starting fwd

FireWall-1: Fetching Security Policy from 192.168.1.4 localhost
Trying to fetch Security Policy from 192.168.1.4:
Fetching Security Policy from 192.168.1.4 failed
Trying to fetch Security Policy from localhost:
Failed to Load Security Policy: No State Saved
Fetching Security Policy from localhost failed
Cannot fetch Security Policy from 192.168.1.4 localhost

FireWall-1 started

Do you wish to start VPN-1 & FireWall-1 now? (y/n) [y] ? n ..... ①

To start VPN-1 & FireWall-1 at any later time, run 'fwstart'

# shutdown -r now ..... ②
```

① 後で再起動するので、ここでは<N>キーを押す。

② 設定を有効にするためにFirewallServerを再起動する。

FireWall-1同期の設定

異なるコンピュータで実行しているVPN-1/FireWall-1モジュールは、互いの状態を同期することができ、これにより情報を共有し、接続の状態が変更されるたびに互いを更新することができます。

同期を行うことにより、運用系FirewallServer(fws1)が停止し、待機系FirewallServer(fws2)が代わりに起動した場合に、fws2は、fws1で接続の更新された状態を保持するため、接続を維持することができます。

以下の手順で同期の設定を行ってください。
fws1、fws2とも「secret key」は同じものを設定してください。

fws1側

1. 下記の1行を含む/etc/fw/conf/sync.confファイルを作成する。

   192.168.2.2

2. fwstopコマンドを実行して、VPN-1/FireWall-1を停止する。

3. fw putkeyコマンドを使用してfws1からfws2への制御パスを確立する。

   ```
   # fw putkey -n 192.168.2.1 192.168.2.2
   Enter secret key:
   Again secret key:
   ```

4. fwstartコマンドを実行して、VPN-1/FireWall-1を開始する。

fws2側

1. 下記の1行を含む/etc/fw/conf/sync.confファイルを作成する。

   192.168.2.1

2. fwstopコマンドを実行して、VPN-1/FireWall-1を停止する。

3. fw putkeyコマンドを使用してfws2からfws1への制御パスを確立する。

   ```
   # fw putkey -n 192.168.2.2 192.168.2.1
   Enter secret key:
   Again secret key:
   ```

4. fwstartコマンドを実行して、VPN-1/FireWall-1を開始する。

FirewallServerとFireWall-1管理サーバ間の通信設定

FireWall-1管理サーバから2台のFirewallServerを管理（セキュリティポリシーの設定やログ表示など）を行うためには、FireWall-1管理サーバとFirewallServerとの間で通信を行うための設定が必要です。以下の手順で設定を行ってください。

fws1側の設定

```
# cpconfig ..... ①


Welcome to Check Point Configuration Program
================================================
This program will let you re-configure
your VPN-1 & FireWall-1 configuration.

Configuration Options:
----------------------
(1)  Licenses
(2)  Masters
(3)  External Interface
(4)  SMTP Server
(5)  SNMP Extension
(6)  Groups
(7)  IP Forwarding
(8)  Default Filter
(9)  Enable High Availability
(10) Exit

Enter your choice (1-10) :2 ..... ②

Configuring Masters...
======================
Masters are trusted Management Stations which will
control this Check Point Module.

Do you want to add Management Stations (y/n) [y] ? y
Please enter the list hosts that will be Management Stations.
Enter hostname or IP address, one per line, terminating with CTRL-D
or your EOF character.
192.168.1.4 ..... ③
Is this correct (y/n) [y] ? y
You will now be prompted to enter a secret key that will be used to
authenticate the communication between this Module and the
Management Stations that you have selected.
Enter secret key: ..... ④
Again secret key:

NOTE:
Do not forget to run 'fw putkey' with the same secret key on each of
the configured masters.
```

① cpconfigコマンドを実行する。

② 2を選択する。

③ FireWall-1管理サーバのIPアドレス（192.168.1.4）を入力する。

④ Secret Keyを入力する。

後で管理サーバ側の設定をする時に同じSecret Keyを入力してください。

```
Configuration Options:
----------------------
(1)  Licenses
(2)  Masters
(3)  External Interface
(4)  SMTP Server
(5)  SNMP Extension
(6)  Groups
(7)  IP Forwarding
(8)  Default Filter
(9)  Enable High Availability
(10) Exit

Enter your choice (1-10) :10 ..... ①

Thank You...

You have changed VPN-1 & FireWall-1 Configuration.
  Would you like to restart
VPN-1 & FireWall-1 now so your changes can take into action? (y/n) [y] ? y ..... ②
Unloading FireWall-1...
FireWall-1: Loading kernel module...
FireWall-1: Starting fwd

FireWall-1: Fetching Security Policy from 192.168.1.4 localhost
Trying to fetch Security Policy from 192.168.1.4:
Authentication for command fetch failed
Fetching Security Policy from 192.168.1.4 failed
Trying to fetch Security Policy from localhost:
Failed to Load Security Policy: No State Saved
Fetching Security Policy from localhost failed
Cannot fetch Security Policy from 192.168.1.4 localhost

FireWall-1 started
#
```

① 10を選択して設定を終了する。

② 設定を有効にするためVPN-1 & FireWall-1モジュールを再起動する。

fws2側の設定

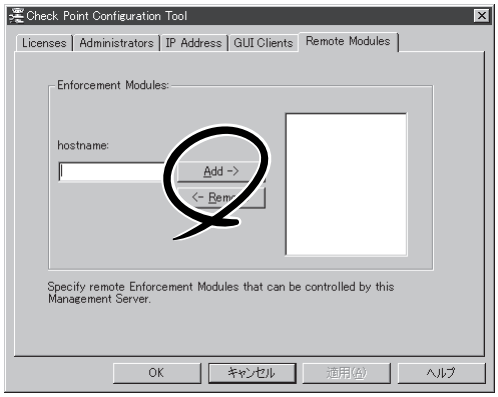
fws1側と同様の設定を行ってください。

FireWall-1管理サーバの設定

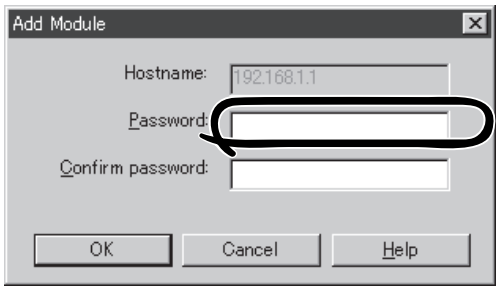
1. 管理サーバマシンの[スタート]メニューからCheck Point Configurationを起動し、Remote Modulesタブを開く。

2. ｈｏｓｔｎａｍｅにｆｗｓ１のＩＰアドレス(192.168.1.1)を入力し、[Add]ボタンをクリックする。

   Password入力画面が表示されます。



3. Passwordには「fws1側の設定」で設定したSecret Keyの値を入力する。

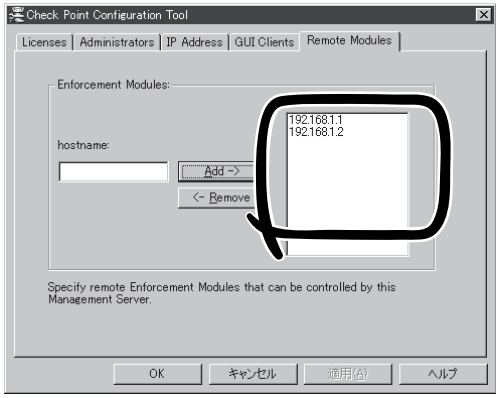


4. fws2のIPアドレス(192.168.1.2)も同様に追加する。

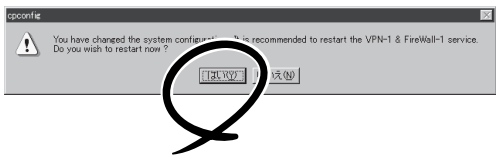
   Passwordには「fws2側の設定」で設定したSecret Keyの値を入力してください。

5. ｆｗｓ１、ｆｗｓ2両方の設定が終了したら[OK]ボタンをクリックする。

   設定を有効にするためＶＰＮ-１　＆FireWall-1 サービスを再起動するか確認する画面が表示されます。



6. [はい]ボタンをクリックしてサービスを再起動する。



セキュリティポリシーの設定

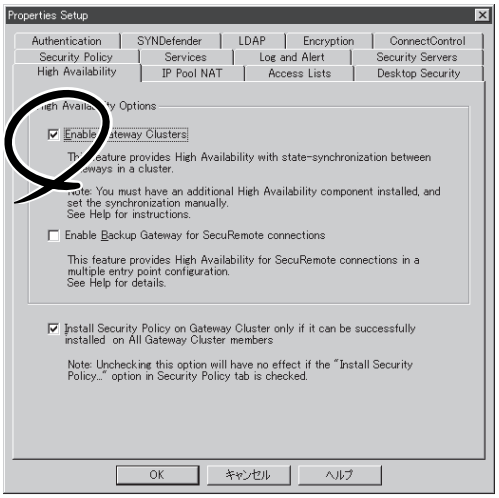
分散型構成ではFireWall-1管理サーバ上にセキュリティポリシーを作成し、管理対象の2台のFirewallServerに一度にインストールします。一体型構成のようにそれぞれのFirewallServerでセキュリティポリシーを作成・インストールする必要はありません。

FireWall Gatewayオブジェクトの作成

分散型構成ではFireWall Gateway(FirewallServer)のオブジェクトの作成方法が異なります。

1. Policy Editorのメニューから[Policy]→[Properties]を選択し、Properties Setupウィンドウを開く。

2. Properties Setup ウインドウのHigh Availability タブでEnable Gateway Clustersにチェックをする。



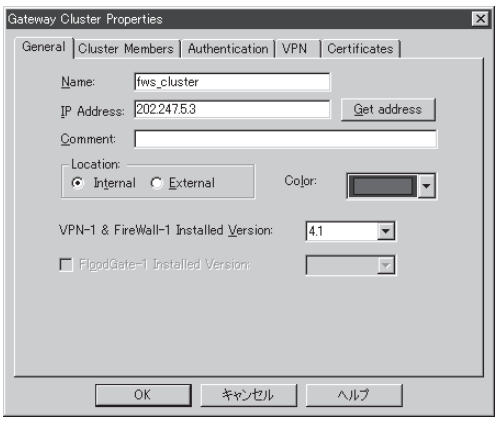
3. ネットワークオブジェクトとして以下のオブジェクトを作成する。

   手順1の設定を行わないとオブジェクトの種類でGateway Clusterは選択できません。

   オブジェクト
   Gateway Cluster

   名前
   fws_cluster

   内容
   IP Address にはインターネット側の仮想IPアドレスを指定する。



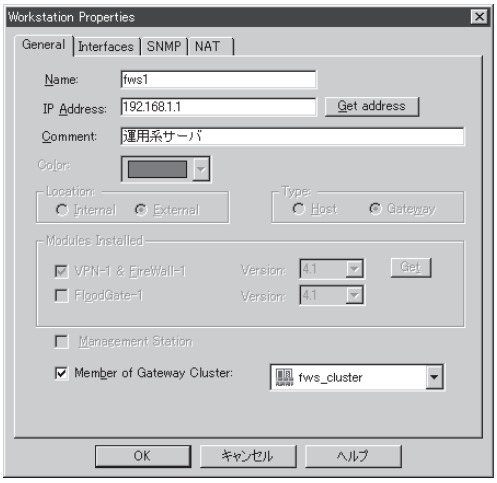
4. 2台のFirewallServerのオブジェクトを作成する。

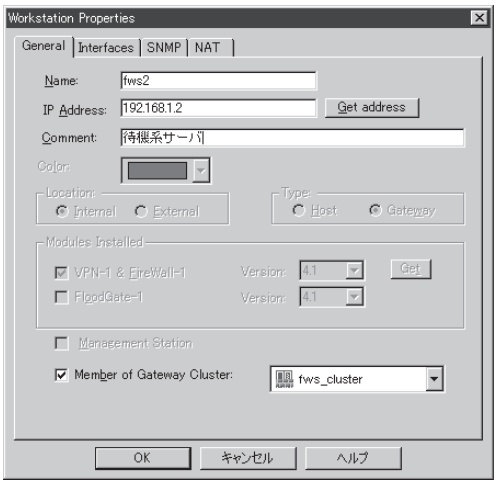
オブジェクト
Workstation

名前
fws1、fws2

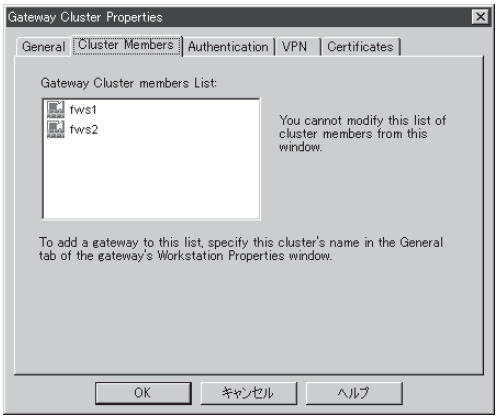
内容
IP Address にはイントラネット側の実IPアドレスを指定する

「Member of Gateway Cluster」にチェックして、ドロップダウンリストから「fws_cluster」を選択する。
Interfaceタブで全インタフェースを設定する。





5. 手順2で作成したfws_clusterオブジェクトを開き、Cluster Membersタブに2台のFirewallServer(fws1、fws2)オブジェクトが登録されていることを確認する。

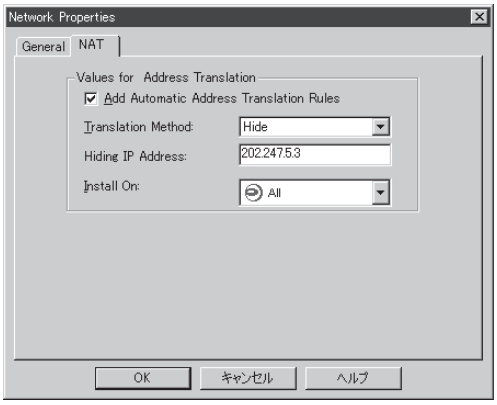


セキュリティポリシーの作成

ネットワーク構成に応じてセキュリティポリシーを作成してください。
ステルスルール(FirewallServer自身へのアクセスを拒否するルール)に関しては、fws1、fws2の両サーバを設定することに注意してください。

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	Any	fws1 fws2	Any	drop	Alert	Gateways	Any	Stealth the Firewall attack protectic
2	localnet	mailer	pop-3	accept	Long	Gateways	Any	E-Mail retrieval rule
3	Any	mailer	smtp	accept	Long	Gateways	Any	Allow access to Mail server
4	Any	FtpWebServer	http ftp	accept	Long	Gateways	Any	Ftp and Web Server
5	dmz-net	localnet	Any	reject	Alert	Gateways	Any	Protect localnet from the DMZ
6	localnet	dmz-net	Any	reject	Alert	Gateways	Any	Protect DMZ from the localnet
7	localnet	Any	Any	accept	Long	Gateways	Any	Allow Outgoing traffic
8	Any	Any	SilentServices	drop		Gateways	Any	Silent drop for broadcast packets
9	Any	Any	Any	drop	Alert	Gateways	Any	Last rule

また、HideモードのNATを使用する場合、「Hiding IP Address」には仮想IPアドレスを指定します。



二重化用ルールの追加

二重化機能を使用するためには、以下の2つのルールを追加する必要があります。

- FirewallServer間の状態監視用通信を通すためのルール
- FirewallServerと監視対象との間の通信を通すためのルール

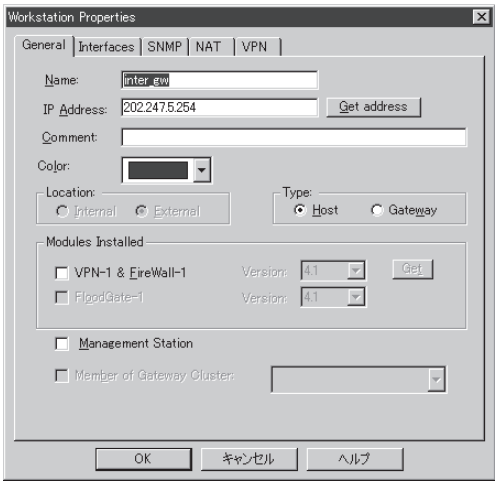
1. ネットワークオブジェクトとして以下の2オブジェクトを設定する。

   設定例ではホスト名を名前として設定していますが、必ずしもホスト名にあわせる必要はありません。

オブジェクト
Workstation

名前
inter_gw

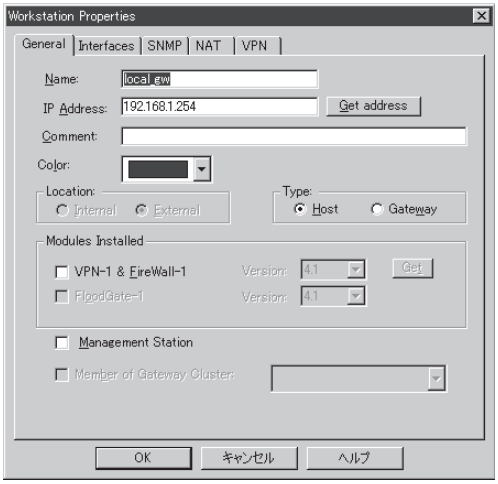
内容
ネットワーク監視に使用するインターネット側のルータ



オブジェクト
Workstation

名前
local_gw

内容
ネットワーク監視に使用するイントラネット側のルータ



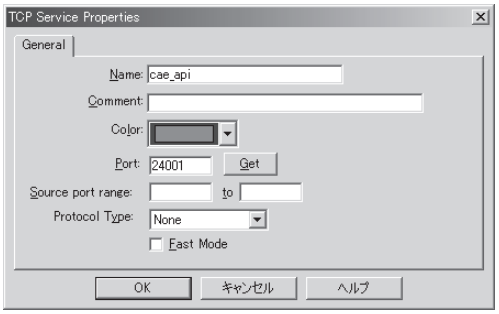
2. 以下のサービスを定義する。

名前は一例です。他の名前でも構いません。

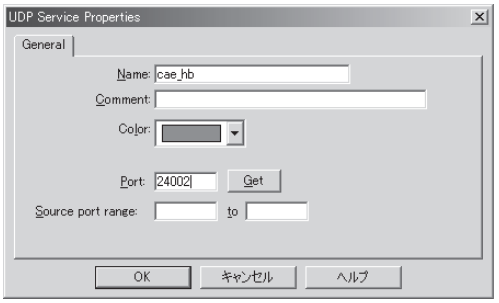
重要

ポート番号はデフォルトのポート番号です。 二重化機能の基本設定でポート番号を変更する場合はその設定に合わせてサービスの定義を行ってください。

オブジェクト: TCP
名前: cae_api
ポート: 24001



オブジェクト: UDP
名前: cae_hb
ポート: 24002



3. 二重化通信用のルールを追加する。

ルールセットの一番上にくるように追加してください。下記ポリシーのルール1、2が追加分です。

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
1	fws1 fws2	fws1 fws2	cae_api cae_hb	accept		Gateways	Any	
2	inter_gw local_gw	fws1 fws2	icmp-proto	accept		Gateways	Any	
3	Any	fws1 fws2	Any	drop	Alert	Gateways	Any	Stealth the Firewall attack prot
4	localnet	mailer	pop-3	accept	Long	Gateways	Any	E-Mail retrieval rule
5	Any	mailer	smtp	accept	Long	Gateways	Any	Allow access to Mail server
6	Any	FtpWebServer	http ftp	accept	Long	Gateways	Any	Ftp and Web Server
7	dmz-net	localnet	Any	reject	Alert	Gateways	Any	Protect localnet from the DMZ
8	localnet	dmz-net	Any	reject	Alert	Gateways	Any	Protect DMZ from the localnet
9	localnet	Any	Any	accept	Long	Gateways	Any	Allow Outgoing traffic
10	Any	Any	SilentServices	drop		Gateways	Any	Silent drop for broadcast pack
11	Any	Any	Any	drop	Alert	Gateways	Any	Last rule

セキュリティポリシーのインストール

セキュリティポリシーの作成が完了したら、ポリシーをインストールしてください。2台のFirewallServerに一度にインストールされます。

二重化機能の基本設定

一体型構成と設定方法は変わりません。一体型構成の説明を参照してください。

他のネットワーク機器の設定

イントラネットとDMZに存在するネットワーク機器については、デフォルトルートの設定として それぞれのネットワークの仮想IPアドレス（イントラネット側: 192.168.1.3、DMZ側: 172.16.1.3）を指定するようにしてください。

運　用

二重化構成の運用について説明します。

障害が発生した場合には

運用系サーバにおいて障害を検出した場合には、フェイルオーバが発生し待機系サーバへ業務が切り替わります。その際に基本設定ツールで指定した管理者のE-mailアドレス宛にメールが送信されます。
メールを受信したらFirewallServerの状態を確認し、フェイルオーバが発生した要因を突き止めてください。
監視先IPアドレスとの通信途絶、あるいはFireWall-1プロセスに異常が発生した場合、/var/log/messages に以下の記録が残ります。

- **監視先IPアドレスとの通信が途絶した場合**

  CLUSTERPRO AE[XXX]: ipwX(group0) error. failover group0.

- **FireWall-1 プロセス に異常が発生した場合**

  CLUSTERPRO AE[XXX]: exec1(group0) error. failover group0.

障害復旧後、運用系サーバを再起動してください。自動フェイルバックが設定されている場合、運用系再起動後、自動的に運用系で業務が開始されます。自動フェイルバックが設定されていない場合は、待機系で業務が起動されたままになり、運用系サーバが待機状態に入ります(運用系、待機系の逆転)。

- **ダウンしたときのメッセージ**

  Subject: WARNING: Firewall is downed

  !!WARNING!!
  Firewall(fws1.nec.co.jp[202.247.5.1]) is not active.
  Urgently check it.

  If you recieved a previous message "NOTICE: Switch over to
  the active firewall" from fws1.nec.co.jp[202.247.5.1],
  both firewalls are downed.
  Urgently check both firewalls!!

- **フェイルオーバしたときのメッセージ**

  Subject: NOTICE: Switch over to the active firewall

  !!NOTICE!!
  Switch over to the active firewall(fws2.nec.co.jp[202.247.5.2]).
  Urgently check another failed firewall.

コマンドリファレンス

状態表示、運用系、待機系の切替等はコマンドを使用して行います。

情報表示

現在の状態、設定内容を確認するには以下のコマンドを実行します。

```
caestat -s [-h host_name]
        -i [-h host_name]
```

状態、設定情報の表示を行うコマンドです。オプションは以下のとおりです。

-sまたは引数なし .... 各種状態を表示します。
-i..... 各種設定を表示します。
-h host_name ..... 操作対象サーバ名。指定なしの場合、コマンド実行サーバが対象となります。

```
# caestat -s

-------------------------------------------------
 CLUSTER STATUS on host1
-------------------------------------------------

 SERVER: host1                ONLINE ..... ①
   GROUP: group0              ONLINE ..... ②
     RESOURCE: fip0           ONLINE ..... ③
     RESOURCE: fip1           ONLINE
     RESOURCE: ipw0           ONLINE
     RESOURCE: ipw1           ONLINE
     RESOURCE: exec0          ONLINE
     RESOURCE: exec1          ONLINE
     RESOURCE: exec2          ONLINE

 SERVER: host2                ONLINE
   GROUP: group0              OFFLINE
     RESOURCE: fip0           OFFLINE
     RESOURCE: fip1           OFFLINE
     RESOURCE: ipw0           OFFLINE
     RESOURCE: ipw1           OFFLINE
     RESOURCE: exec0          OFFLINE
     RESOURCE: exec1          OFFLINE
     RESOURCE: exec2          OFFLINE
```

① サーバの状態

② 業務の状態

③ 各リソースの状態

```
# caestat -i

------------------------------------------------
 CLUSTER INFORMATION on uxg72
------------------------------------------------

 CLUSTER :
  STARTUP             : AUTO ····· ①
  HB interval         : 1 ····· ②
  HB timeout          : 5 ····· ③
  WAIT timeout        : 5
  HB port             : 24002 ····· ④
  API port            : 24001 ····· ⑤
  API timeout         : 30
  ping timeout        : 1
  RECOVER             : RESTART
  RETRY count         : 5

  SERVER0 : host1 ····· ⑥
   INTERCONNECT0      : 192.168.1.1/255.255.255.0 ····· ⑦
   INTERCONNECT1      : 192.168.2.1/255.255.255.0

  SERVER1 : host2
   INTERCONNECT0      : 192.168.1.2/255.255.255.0
   INTERCONNECT1      : 192.168.2.2/255.255.255.0

   GROUP0 : group0
    START             : AUTO
    FAILBACK          : MANUAL ····· ⑧
    ENVIRONMENT       : ACT_NORMAL
    RECOVER           : IGNORE
    RETRY count       : 0
    FAILOVER policy   : host1 host2 ····· ⑨

    FIP0 : fip0
     ADDRESS          : 202.247.5.3/255.255.255.0 ····· ⑩
     INTERFACE        : eth0:0
     PING count       : 0
     ARP count        : 1
     RECOVER          : RETRY
     RETRY count      : 5

    IPW0 : ipw0
     POLLING address  : 202.247.5.3 | 172.16.1.3 ····· ⑪
     RECOVER          : FAILOVER
     RETRY count      : 2
```

① 二重化機能が有効になっているかどうか

② ハートビート送信間隔(秒)

③ ハートビートタイムアウト時間(秒)

④ 内部通信用UDP ポート番号

⑤ 内部通信用TCP ポート番号

⑥ ホスト名

⑦ インタコネクトアドレス

⑧ 自動フェイルバックを行うかどうか

⑨ 運用系サーバ 待機系サーバ

⑩ 仮想IPアドレス

⑪ 監視対象アドレス

運用系／待機系の切り替え・業務の起動／停止

運用系／待機系の切替や、業務の起動／停止を行う場合、以下のコマンドを実行します。

```
caegrp -s   [-h host_name]
       -t   [-h host_name]
       -m   [-h host_nam]
```

業務の起動／停止関連操作を行うコマンドです。オプションは以下のとおりです。

-s ..... 業務の起動を行います。既に起動されていたり、他のサーバで起動している場合、失敗します。
-t ..... 業務の停止を行う。既に停止されていたり、他のサーバで起動されている場合、失敗します。
-m ..... 業務の実行サーバを切り替えます。業務が起動しているサーバ側で実行する必要があります。
-h host_name ..... 操作対象サーバ名。指定なしの場合、コマンド実行サーバが対象。-mオプション指定時には、業務移動元サーバの意味も持つ

分散型構成の再インストール

分散型構成の場合の再インストール方法について説明します。
なお、一体型構成の場合は通常のFirewallServerの再インストール手順と同様です。一体型構成の場合は「システムの再インストール」(87ページ)を参照して再インストールを行ってください。

次の手順に従って再インストールします。

1. 「システムの再インストール」(87ページ)を参照しながら手順11までを行う。
2. 「分散型構成の設定」の以下の作業を行う。
   - 「FireWall-1のコンフィグレーション」(153ページ)
   - 「FireWall-1同期の設定」(156ページ)
   - 「FirewallServerとFireWall-1管理サーバ間の通信設定」(157ページ)
3. GUIクライアントからセキュリティポリシーのインストールを行います。

   分散型構成の場合はポリシー情報がFireWall-1管理サーバの中に保存されているため、FirewallServer本体の再インストールの際にはFireWall-1のポリシー情報のリストアは必要ありません。

注意・制限事項

- FirewallServerは2台購入していただく必要があります。 また、ライセンスは同じノード数のもので、それぞれの実アドレスで、 申請していただく必要があります。
- フェイルオーバ機能（障害時に待機している2台目のFirewallServerに処理を引き継ぐ）のみのサポートです。二台同時に利用できるわけではありません。 負荷分散(ロードバラシング)機能はありません。
- 待機系のFirewallServerにもあらかじめポリシの設定をしておく必要があります。
- 一体型構成ではVPN通信は二重化できません。
- 一体型構成では障害発生時に接続されていたセッションは保持されません。 切り替え時にセッションはいったん切断されます。
- 分散型構成では自動フェイルバック時、接続されていたセッションが切断される場合があります。（一体型構成では必ず切断されます。）
- 高負荷等の要因により、運用系、待機系の双方で業務が起動してしまう場合があります。その場合、運用系、待機系いずれかのサーバを再起動してください。
- 監視対象IPアドレスとの通信途絶、あるいは、FireWall-1 プロセス消滅が発生した際は、フェイルオーバが発生し、待機系のサーバに業務が引き継がれます。このとき、再度運用系で業務を起動するには、運用系の再起動が必要です。

  自動フェイルバックが設定されている場合、運用系再起動後、自動的に運用系で業務が開始されます。自動フェイルバックが設定されていない場合は、待機系で業務が起動されたままになり、運用系の方が待機状態に入ります(運用系、待機系の逆転)。

～Memo～