

本章ではFirewallを2台使用して、二重化構成を構築するための手順について説明します。

セットアップの概要(→96ページ)	.二重化機能の動作概要について説明しています。
セットアップ(→99ページ)	.二重化構成を構築する場合の設定手順について説 明しています。
運 用(→123ページ)	.二重化構成での運用方法について説明していま す。
二重化構成の再セットアップ(→131ページ)	.再セットアップの手順が単体構成とは異なりま す。再セットアップの際の差分や手順について説 明しています。
注意・制限事項(→137ページ)	.二重化構成で運用する際の注意事項や制限事項に ついて説明しています。



二重化構成について説明します。

動作概要

Firewallを二重化することで1台が障害などにより停止しても、もう1台のFirewall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のプロセスの異常を検出した場合や設定されたIPアドレスとの通 信が途絶した場合にも、待機系に業務を引き継ぐことが可能です。

以下の仕組みでFirewallを二重化します。

● 通常運用時

- 運用系側のFirewall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とイン 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Firewallは互いにサーバの状態を監視をします。



● 運用系サーバ障害時

- 待機系のFirewallが運用系のダウンを検出します。
- 運用系のFirewallが仮想IPアドレスを無効にします。
- 待機系のFirewallが仮想IPアドレスを有効にします。
- インターネット側と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業務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

二重化構成ではFirewall2台のほかに管理用サーバが必要となります。Express5800/ FW300またはFW500をもう1台使用し、管理サーバとして動作させることも可能です。

必要なリソース

二重化を実現するためには、Firewall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IPアドレスを設定してください。

このアドレスはFirewall本体のインタフェースに直接割り当てるアドレスではありません。

● 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IPアドレスを設定してください。

このアドレスはFirewall本体のインタフェースに直接割り当てるアドレスではありません。

● 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IPアドレスを設定してください。

このアドレスはFirewall本体のインタフェースに直接割り当てるアドレスではありません。

● Firewall間通信用アドレス: 1つ

Firewall間の監視に使用するアドレスです。

基本的には、Firewall監視専用アドレスとして、Firewall本体のインタフェースに割り当ててください。

セットアップ

以下のネットワーク構成を例にとって設定を行います。

Firewall1(運用系)

ホスト名: インターネット側実IPアドレス: DMZ側実IPアドレス: イントラネット側実IPアドレス: Firewall間通信用IPアドレス: fws1

202.247.5.1/255.255.255.0 172.16.1.1/255.255.255.0 192.168.1.1/255.255.255.0 192.168.2.1/255.255.255.0

• Firewall2(待機系)

ホスト名: インターネット側実IPアドレス: DMZ側実IPアドレス: イントラネット側実IPアドレス: Firewall間通信用IPアドレス:

fws2 202.247.5.2/255.255.255.0 172.16.1.2/255.255.255.0 192.168.1.2/255.255.255.0 192.168.2.2/255.255.255.0

● 仮想IPアドレス

インターネット側: DMZ側: イントラネット側:

● プロキシARPアドレス

インターネット側:

管理用サーバ

ホスト名: IPアドレス:

● GUIクライアント用PC

IPアドレス:

202.247.5.3

172.16.1.3

202.247.5.4/255.255.255.0

firewall_mgr 192.168.1.4/255.255.255.0

192.168.1.5/255.255.255.0



設定手順の流れ

以下に設定手順の流れを示します。ここでは二重化に関する設定内容を説明します。その他の手順については3章を参照してください。



FireWall-1管理サーバのセットアップ

二重化する2台のサーバを管理するための管理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管理モジュールをインストールしてください。Express5800/ FW300またはFW500をもう1台用意し、管理サーバとして動作させることも可能です。

オペレーティングシステム: Windows 2000 Server(SP1、SP2、SP3、SP4)、 Windows 2000 Advanced Server(SP1、SP2、SP3、 SP4)、 Windows 2003 Server(SP1, SP2)、 Solaris8 / UltraSPARC、 Solaris9 / UltraSPARC、 Solaris10 / UltraSPARC、 RedHat Enterprise Linux 3.0 (kernel version 2.4.21)

Windows

ディスク容量:	300MB以上
メモリ:	256MB以上

Linux

ディスク容量:	300MB以上
メモリ:	256MB以上(推奨512MB以上)

Solaris

ディスク容量:100MB以上メモリ:128MB以上(推奨256MB以上)

* 上記は、2007年3月現在の情報です。今後のパッチリリースにより変更になる可能性があ ります。

FireWall-1管理サーバの設定

Express5800/FW300またはFW500を管理サーバとして動作させる場合の設定例です。以下の手順に従って設定を行ってください。

1. インストール/初期導入設定ディスクによる設定を行う。

3章の「1.インストール/初期導入設定用ディスクによる設定」を参照し、初期設定と管理クライアントの接続を行ってください。

∎ਾ0≣ੂ

「インストール/初期導入設定用ディスクの作成」-「各入力項目の設定」において、「サーバタイ プ」は「管理サーバ」にチェックをしてください。

2. 基本設定ツールによる設定を行う。

⊤0重要

3章の「2.システムのセットアップ」 - 「基本設定ツールによる設定」を参照し、管理サーバとし て 使 用 す る た め の 設 定 を 行 っ て く だ さ い 。 サ ー バ タ イ プ の 設 定 で は 、 「2. ManagementServer」管理サーバになっていることを確認してください。

fwsetup

3. 設定終了後、再起動する。

FireWall-1管理モジュールのコンフィグレーション

管理モジュールを管理サーバヘインストールします。以下の手順でコンフィグレーションを 行ってください。図中の〈略〉の設定する項目については、3章の「2. システムのセットアッ プ」- 「FirewWall-1のコンフィグレーション」を参照してください。

```
# cpconfig
Welcome to Check Point Configuration Program
_____
Please read the following license agreement.
Hit 'ENTER' to continue...
           .
Do you accept all the terms of this license agreement (y/n) ? y .....\textcircled{2}
Please select one of the following options:
Check Point Power - for headquarters and branch offices.
Check Point UTM - for medium-sized businesses.
_____
(1) Check Point Power.
(2) Check Point UTM.
Please specify the Check Point UTM Product type you are about to install:
(1) VPN-1 UTM Gateway.
(2) SmartCenter UTM.
(3) SmartCenter UTM and VPN-1 UTM Gateway.
                                                     Enter your selection (1-3/a-abort) [1]: 2
```

① FireWall-1管理モジュールのコンフィグレーションをする。

- ② 使用許諾に承認した場合は<Y>キーを押す。
- インストールする製品を選択する。
 2の「Check Point UTM」を選択し、インストールします。
- ④ インストールするモジュールを選択する。

「2」を選択し、インストールします。

① 管理モジュールを起動させる。

② 再起動する。

Firewall本体のセットアップ

Firewallのセットアップについて説明します。

マシンの設定

以下の手順に従って設定を行ってください。

1. インストール/初期導入設定用ディスクによる設定を行う。

3章の「1.初期導入設定用ディスクによる設定」を参照し、初期設定と管理クライアントの接続を 行ってください。

2. 基本設定ツールによる設定を行う。

3章の「2.システムのセットアップ」-「基本設定ツールによる設定」を参照し、設定を行ってください。

ਰਾ

上記の設定においては、二重化機能を使用しない設定としてください。二重化機能の設定につきましては、後述の「二重化機能の設定」で行います。

Use cluster system? (y/n) [n]: n

FireWall-1のコンフィグレーション

二重化構成の場合、コンフィグレーション手順が3章とは一部異なります。図中の〈略〉の設定する項目については、3章の「2.システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

① FireWall-1のコンフィグレーションをする。

② 使用許諾に承認した場合は<Y>キーを押す。

# cpconfig	
Welcome to Check Point Configuration Program	
Please read the following license agreement. Hit 'ENTER' to continue :	1
: : Do you accept all the terms of this license agreement (y/n) ? ${\bf y}$	2
Please select one of the following options: Check Point Power - for headquarters and branch offices. Check Point UTM - for medium-sized businesses.	
 Check Point Power. Check Point UTM. 	
Enter your selection (1-2/a-abort) [1]: 2	3
Please specify the Check Point UTM Product type you are about to install:	
(1) VPN-1 UTM Gateway.(2) SmartCenter UTM.(3) SmartCenter UTM and VPN-1 UTM Gateway.	
Enter your selection (1-2/a-abort) [1]: 1	④

③ インストールする製品を選択する。

2の「Check Point UTM」を選択し、インストールします。

④ インストールするモジュールを選択する。

「1」を選択し、インストールします。

Dynamically Assigned IP Address Moduleをインストールするか問い合わせがあるので、<Enter>キーを選択する。

Is this a Dynamically Assigned IP Address gateway installation ? (y/n) [n] ?① Would you like to install a Check Point clustering product (CPHA, CPLS or State Synchronization)? (y/n) [n] ? y② IP forwarding disabled Hardening OS Security: IP forwarding will be disabled during boot. Generating default filter Default Filter installed Hardening OS Security: Default Filter will be applied during boot. This program will guide you through several steps where you will define your Check Point products configuration. At any later time, you can reconfigure these parameters by running cpconfig : (簡)

- ② Check Point clustering productをインストールするか問い合わせがあるので、<Y> キーを押す。
- ① FireWall-1管理サーバとFirewall間での通信に使用するパスワードを設定してください。
- ② 終了後、再起動します。

: (略) : Configuring Secure Internal Communication... -----The Secure Internal Communication is used for authentication between Check Point components Trust State: Uninitialized Enter Activation Key: Retype Activation Key: The Secure Internal Communication was successfully initialized initial_module: Compiled OK. Hardening OS Security: Initial policy will be applied until the first policy is installed In order to complete the installation you must reboot the machine. Do you want to reboot? (y/n) [y] ? **y**

セキュリティポリシーの設定

Firewallオブジェクトの作成

- 1. 2台のFirewallのオブジェクトを作成する。
 - ViewObjectTreeの[CheckPoint]を選択し、右クリックします。
 [New Check Point]→[VPN-1 Power/UTM Gateway]を選択します。
 [Check Point installed Gateway using]ダイアログが表示された場合、[Classic mode]を 選択し、[OK]を押してください。
 - ー オブジェクト : Gateway

内容

- 名前 : fws1、fws2
 - : IP AddressにはFireWall-1管理サーバと同じネットワークの実IPアドレス を設定してください。
- FireWall-1管理サーバからFirewallを管理(セキュリティポリシーの設定やログ表示など)するためには、FireWall-1管理サーバとFirewallとの間で通信を行うための設定が必要です。 Generalページで[Communication...]をクリックし、FireWall-1のコンフィグレーション時に設定したパスワードを入力してください。

CK Point Gateway - Iws1				×
General Properties	Check Point 6	ateway - General Prop	erties	
E Topology				
-NAT	<u>N</u> ame:	fws1		
- Authentication	IP Address:	202.247.5.1	Get address 🔲 Dynamic Address	5
FireWall-1 GX	Comment:	-		
 Logs and Masters Canacity Ontimization 	Color		T	
 Advanced 	CUJUI.			
	C 1.	10		
	Secure Interna			
	Comingnicat			
	Version:	NGX R62	✓ Get Version	
	09-			
	03.	Linux		
	Type:	VPN-1 UTM		
	Check Point F	roducts		
	Firewall			
	□VPN	ar 10 10	Communication	
	Secondary	SmartCenter Server		
	Integrity Server	aver	The Activation Key that	you specify must also be used in the module configuration.
	Canes /			
	A LOC			
		Course 1		
	- Configure	Servers	Activation Key:	*******
			Gonfirm Activation Key:	*****
			Irust state:	Uninitialized
		- OK		
			Initialize	Test SD Status Report

- Topologyページで全インタフェースを設定します。

Topology	r.		
Name eth0 eth1 eth2 cth9	IP Address 192,168,1,1 202,247,5,1 172,16,1,1 1981,189,24	Network Mask 255 255 255 0 255 255 255 0 255 255 255 0 255 255 255 0	IP Addresses behi This Network External This Network This Network
VPN Domain C ALIP Adda C Manually d	esses be lind Gateway afned	based on Topology in	omation.
Srij demain	la Banzo Acceso Ga	enneiy	
	Get Set Name edi0 edi0	Impology Sett. Name IP Address arbit 152 108 1.1 arbit 202 247 5.1 arbit 202 247 24.1 arbit 202 24.1 arbit 202 24.1 arbit 203 24.1 arbit 204 24.1 <td>Topology Gett Name IP Address Network Made, etc. #0 152 (1911.1 252 525 28.0 etc.1 252 247 51.1 252 525 28.0 etc.1 252 247 51.1 252 252 28.0 etc.1 152 101.1 252 252 28.0 etc.1 152 101.1 252 252 28.0 etc.1 152 101.1 252 252 28.0 etc.1 252 252 28.0 192 100.2.1 etc.1 254 253 28.0 192 100.2.1 etc.1 254 253 28.0 192 100.2.1 etc.1 254 253 28.0 192 100.2.1 etc.1 254 272 20.0 100.2.1 etc.1 254 272 20.0 100.2.1 etc.1</td>	Topology Gett Name IP Address Network Made, etc. #0 152 (1911.1 252 525 28.0 etc.1 252 247 51.1 252 525 28.0 etc.1 252 247 51.1 252 252 28.0 etc.1 152 101.1 252 252 28.0 etc.1 152 101.1 252 252 28.0 etc.1 152 101.1 252 252 28.0 etc.1 252 252 28.0 192 100.2.1 etc.1 254 253 28.0 192 100.2.1 etc.1 254 253 28.0 192 100.2.1 etc.1 254 253 28.0 192 100.2.1 etc.1 254 272 20.0 100.2.1 etc.1 254 272 20.0 100.2.1 etc.1

- 2. 以下のクラスタオブジェクトを作成する。
 - ViewObjectTreeの[CheckPoint]を選択し、右クリックします。
 [New Check Point]→[VPN-1 Power/UTM Cluster]を選択します。
 [Check Point installed Gateway using]ダイアログが表示された場合、[Classic mode]を 選択し、[OK] を押してください。
 - ー 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アドレスを指定してください。

General Properties	Gateway Clu	ter Properties - Gen	eral Properties	
 Cluster Members 3rd Party Configuration 	Name:	fws_cluster		
B- Topology NAT	IP Address:	202.247.5.3	Get address	
- SmartDefense	Comment		and the second s	
FireWall-1 GX Logs and Masters	Color:		·	
- Capacity Optimization 3- Advanced	Version:	NGX R62	*	
	OS:	Linux		Get <u>O</u> S
	Туре	VPN-1 UTM		
	Check Point	Products		
	✓Frewall			×
	Cluste XL			
	Anti Virus	1212		
	SmarfView	/ Monitor		-

3. Cluster Membersページで、手順1で作成した2台のFirewallオブジェクト(fws1とfws2)を追加する。

Cennes I Properties Catater Memberal - Grant Party Configuration - NAT - NAT - NAT - Authentication Casacity Optimization - Casacity Optimization - Advanced	Cluster Members Gateway Cluster members List						
	Name Friend free1 Friend free2	IP Address 20224751 20224752					
	AddEot	Bemove					

4. 3rd Party Configurationページで、設定を確認する。

「Use State Synchronization」にチェックが付いていることを確認します。	チェックが付いてい
ない場合は、チェックを付けます。	

「Hide Cluster Members' outgoing traffic behind the Cluster's IP Address」にチェックが付いていないことを確認します。

teway Gluster Properties	- fws_cluster			×
General Properties Cluster Members	3rd Party Configuratio	m		
Topology	Specify Cluster open	ating mode		
Authentication	(High Availability			
Lops and Masters Gapacity Optimization	C Load Sharing			
	3gd Party Solution	Other OPSEG	-	
	🔽 Lipe State Sync	hronization		
	See the OPSEO clus	ter solution's manual for	the correct settings of	these check boxes
	Support non-sti	cky connections. See Hel	p for details.	
	F Hige Cluster Me	mbers' outcoine traffic b	chind the Cluster's IP A	ddress
	Forgerd Oluster	's incoming traffic to Olu	ster Members' IP Addre	1992
				and I
		OK	Cancel	нар

5. Topologyページにてインタフェースの設定をする。

t

[Edit Topology]をクリックします。
IPアドレスには、仮想IPアドレスを設定し、Network Objectiveプルダウンメニューより、「Cluster」を設定します。
同期用ネットワークのIPアドレスは設定せず、プルダウンメニューより、「1st Sync」を設定します。

eneral Properties	Topology								
d Party Configuration									
opology	Line abusta	1 durat	1 for 2	Ataburat. Tom	. 1	- 6			
AT	1721618	1721611	172161	2 Chaster	5	- 2			
Authentication Logs and Masters Gapacity Optimization Advanced	20224753 19216813	202.247.5.1 192.1681.1 192.168.2.1	202.247.5 192.168.1 192.168.2	52 Cluster 12 Cluster 22 1st Sync					
			-						
			Edit Topo	logy					
	I Enable Exte	inded Cluster Ar	nti-Spoofine		2				
	Enable Exte Gupported	ended Cluster Ar from NG with A	nti-Spoofine pplication Intell	igence (RSS) and abov	s)				
	Enable Exte Gupported VPN Domain	inded Cluster Ar from NG with A	nti-Spoofine pplication Intell	igence (PG5) and abov	s)				
	Enable Exte Gupported VPN Domain	Inded Cluster Ar from NG with Ar	nti-Spoofine pplication Intell unter Membera	isence (RS5) and abov based on Topology infi	a) contaction	-			
	C Manually de	nded Cluster A from NG with A coses behind Ok	nti-Spoofine pplication Intell uster Members Idat Topolocy	ieence (RS5) and abov based on Topology Infi	a) symation	-			
	C Enable Extr Supported VPN Domain C All D Addre Darcally de Show VPN	ended Cluster A from NG with A esses behind Ok timed Domain	nti-Spoofine pplication Intell utter Members Edit Topology	istence (PSG) and abov based on Topology infi Network Objective	e) Annation 195 five_cluster	[2] Twat	[E] Fers2	Topology	4
	C Enable Extr Supported VPN Domain C All D Addre Darwally de Show VPN	rided Cluster A from NG with A rises behind Ok fined	nti-Spoofing pplication Intell ster Members (dit Topology	Internor (PSG) and above based on Topology info Metwork Objective	e) rmation (#\ fws_chuter	Typest Get Topology 4%2	[E] Pers2 Get Topology 452	Τοροίοεγ	
	Enable Exit Gisported VPN Domain All IP Addre Manually de Drow VPN Eet, domain	ended Chuster A from NG with A esses behind Ok fined Domain	nti-Spoofine pplication Intell utter Members Litit Tepology	igence (PSS) and abov based on Topology info Nations: Disactive Dayler	a) Implies Imp	(E) twat Get Topology +92	[2] Perg2 Ont Topology +%2 1723412	Topolocy	-
	Enable Extr Susported VPN Doman All IP Addr Manually de Drow VTN Set doman	ended Oluster A from NG with A esses behind Ok elined Domein	nti-Spoofine pplication Intell date: Members List Topolocy Hene IP Adares Het Mask	Internoe (RS5) and above based on Topology Info Nations Objective	e) Frmation (0), fives_cluster + 60,2 (75214513) 1551551950		[10] Two Out Topology Hold 912.41.2 195.195.195.0	Topology Infernal	
	C Enable Extr Supported VPN Doman & All IP Addy C Menually do Drow VPN Est doman	ended Cluster A from NG with A esses behind Ol elined Domein	nti-Spoofine pplication Intell orster: Members Edit Topolocy Wane IP Adars Net Mask Viene	Igence (P55) and above based on Topology Info Metwork Objective Durke	a) rmation (0), five_state (1), five_	(2) fives Get Topology +9:2 172 (43.3 195 20550 +911	[2] 1992 Get Topology end (7223412) 2652612 2652612 2652650 4651	Topolocy	
	Enable Extr Susported VPN Domain All IP Addr Menually de Drow VPN Set domain	ended Chuster A from NG with A cases behind Ok efined Domein 1 for Remote 4	nti-Spoofine pplication Intell uster Membersh Idet Topology Hens Prathusk Henthusk Wens Prathusk	igence (RSS) and above based on Topology info Metwork Objective Objec	2) Primation IPS, fives_cluster + 152 15521552 + 155 - 15521552 - 1552 - 15521552 - 1552 - 15521552 - 1552 - 15521552 - 15521552 - 15521552 - 15521552 - 155215 - 1552 - 155215 -	[22] Twat Get Topology 9%2 175214533 175214533 19525550 9%1 10524731	[B] two2 Get Topology eth2 (722452) (7225252) (7225552) (722552) (7225552) (7225552) (7225552) (722552) (722552	Topolocy	-
	Enable Extension Gupported VPN Domain G All IP Addre C Manually de Draw VIPN Est domain	ended Chuster A from NG with A esses behind Ok efined Domein	nti-Spoofine pplication Intell uster Members Idit Tepolocy Net Mask Teme IP Address Teme IP Address Teme	isence (RSS) and abov based on Topology info Notework Objective Objective	 a) a) b) b) b) c) c	Image: Transmission Transmission	[□] Tws2 0.61 Topology 0.62 0.7214512 0.952451250 48.61 0.0224732 2552551950	Topology Internal Enternal	-
	Enable Exte Gupported VPN Doman A III P A354 Dimenally ob Brow VPN Set domain	ended Oluster A from NG with A reset behind Ol rined <u>Comein</u>	nt-Spoofine pplication Intell aster Members Cdit Topolocy Winne IP Address Net Mask Net Mask Net Mask Net Mask Net Mask Net Mask Net Mask	iemon (1955) and abov based on Topology infi Setewark Objective Durker	a) PFS Two _chester a whit 1925 Two _chester a whit 1922 FKS 3 1922 FKS	[2] Twost Gast Topology #8-2 1952 245 205 00 #81 202 247 81 205 245 205 00 #800	[5] Fws2 Gat Topology e62 (7521512) 9552552550 e661 952255250 20224752 9552552550 202252550 9552552550 202252550 9552552550 e602 95525521550	Topology Infanty Education	
	C Brable Exte Geoported VPN Domain & All Dr Addy C Menually do Brow VPN Set domain	ended Gluster A from NG with A esses behind Ok eined Domein h for Remote 4	nti-Spoofine pplication Intell aster Members Idet Topolecy Net Members Idet Topolecy Idea Idea Idea Idea Idea Idea Idea Idea	Interner (1950) and above based on Topology into Based on Topology into Ourler Durker Durker	 a) (a) <li(a)< li=""> <li(a)< li=""> <li(a)< li=""> (a) <</li(a)<></li(a)<></li(a)<>	(E) rws1 Get Topology 4%3 1721813 185265255 4%3 10224751 1652562550 19527652550 1952765257 19527652550 195276527 1952765 1952765 195776 1957777 195776 1957776 1957777 1957777 195777	[22] Twm2. Dat Topology 4%2 192.24.1.2 295.55.295.0 202.247.5.2 295.55.295.0 1255.255.295.0 4%3 192.142.2 295.35.295.0	Topolocy Internal Enternal	
	Enable Exit Gioportal VPR Doman All IP Astr Disor VPN Est doman	ended Gluster A from NG with A esses behind GN fined Domein 1 for Remote 4	nti-Spoofine oplication Intell aster Members dat Tepabley ¹⁰ Adves ¹⁰ Adv	ligence (REG) and above based on Topology inf Beferenk Discolary Durke Durke Durke	 a) a) a) b) b) b) c) c	[25] Twat Bet Toosloey 993 121613 1265265255.0 991 993 12552555.0 993 1255255.0	[B] tws2 Get Topology 663 (92141.2) 195255195.0 6002478.2) 295255195.0 1602 160.1 162.661.2 295255195.0	Topology Informal Enternal Informal	
	C English Ent Gacottel VPN Domain G All (P A33) C Benally de Drow VPN Set domain	ended Cluster A from NG with A resers behind Ok rined Domen i for Remote 4	nti-Spooline pplication Intell uster Members Idel Tepology Mane Privat	Internet (455) and above based on Topology infi Borter Donter Donter Donter Donter		[20] Ivest Oct Topolety Oct Topolety == 192 147.51 195 255 255 0 === == 02 147.81 102 147.81 195 255 255 0 == == 05 255 255 0 == == 05 255 255 0 == == 05 255 255 0 == == 05 255 255 0 == == ==	[0] Perio 0.4 Topology 4.62 17234732 4.63 17234732 1552551950 4.60 1923432 4.60 1923432 1952551950 4.60 1923432 19525550 4.63 19334 19335 19335 19335 19335 19335 19335 19335 193555 19355 19355 19355 19355 193555 193555 193555 19355 193555 193555 193555 193555 193555 19355	Topolocy Infernal Enfernal Infernal	
	Proble Edd VPR Doman (* All D' Add) (* All D' Add)	ended Cluster A from MO with A esses behind O. rined Domein	nti-Spoofine policiation Intell uster Members Idit Topology Henn Britani Henn Henn Britani Henn Britani Henn Henn Britani Henn Henn Henn Henn Henn Henn Henn He	Internet (1950) and above based on Topology infi Baster Durke Durke Trill geo	a) ministron 10, freq. quester 4, fill 4, fi	22 Twy1 Get Topology mb1 72 Fet13 952 955 951 255 952 955 952 952 <td< td=""><td>[B] Hwm2 Out Topology Heat Topology 1952:55:255:0 Heat 2952:55:255:0 Heat 2001:24:75:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 1952:14:22 Heat</td><td>Topolog y Internal Enternal Internal</td><td></td></td<>	[B] Hwm2 Out Topology Heat Topology 1952:55:255:0 Heat 2952:55:255:0 Heat 2001:24:75:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 2952:55:255:0 Heat 1952:14:22 Heat	Topolog y Internal Enternal Internal	

二重化用ルールの追加

二重化機能を使用するためには、サーバ間の状態監視用通信を通すためのルールを設定する 必要があります。

1. メニューの[Manage]→[Services...]→[New]を選択し、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。)

オブジェク	ト:TCP	TCP Service Properties - clp_tcp
名前 ポート	名前 :clp_tcp ポート :28001	General
		Qomment:
		Color:
		Port [28001 Get
		To specify a port range, add a hyphen between the lowest and the highest port numbers, for example 44-55.
	♥ Keep connections open after Policy has been installed	
オブジェク 々 前	ל:UDP אלי day	UDP Service Properties - clp_udp
名前 :clp_udp ポート :28002	General	
		Qomment

オブジェク	ト:UDP
名前	:clp_udp
ポート	:28002

<u>N</u> ame:	clp_udp
<u>C</u> omment:	
Co <u>l</u> or:	
Port	28002 <u>G</u> et
1010	
To specify lowest and	a port range, add a hyphen between the the highest port numbers, for example 44-55.
To specify lowest and	y a port range, add a hyphen between the d the highest port numbers, for example 44-55.

|**न-**0 **वि**要

上記ポート番号は基本設定ツールにおける既定値のポート番号です。二重化機能の設定でポー 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。

2. 上記の二重化通信用のルールを追加する。

項目	設定値		
Source	:fws1、fws2		
Destination	:fws2、fws1		
Service	:clp_tcp、clp_udp		
Action	:accept		

二重化用設定事項

二重化機能を使用するためには、設定事項として、[Policy] - [Global Properties] - [NAT - Network address translation]ページで[Automatic ARP configuration]のチェックを外す 必要があります。



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 Firewallにインストールされます。

セキュリティポリシーのバックアップ

二重化構成の場合、ポリシー情報はFireWall-1管理サーバに保存されますが、情報のリスト アの際には、管理サーバとFirewall本体の両方のバックアップデータが必要となります。管 理サーバとしてExpress5800/FW300またはFW500を使用している場合には、3章の「4. バックアップ」コマンドによるバックアップを参照してください。FireWall-1モジュールの バックアップ方法と同じです。

その他のサーバを使用している場合には、該当するファイルのバックアップが必要となります。(以下のバックアップファイル取得方法は、Windowsマシンを使用した場合の一例です。)

1. コマンドプロンプトより、FireWall-1を停止させる。

C:¥> cpstop

2. 停止後、以下のコマンドを実行する。

「export.tgz」バックアップファイルが作成されます。

C: ¥> cd C: ¥WINNT¥FW1¥R62¥fw1¥bin¥upgrade tools > upgrade export.exe export

チェック

「C: \pm WINNT \pm FW1 \pm R62 \pm fw1」は、FireWall-1をインストールしたディレクトリになります。 インストールディレクトリによって異なります。

3. バックアップファイルを取得後、FireWall-1を起動します。

C:¥> cpstart



セキュリティポリシーの設定の説明において使用している画像イメージは、FireWall-1の FeaturePackによって異なる場合があります。

二重化機能の設定

二重化機能の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。両Firewallで全 く同じ設定を行ってください。

二重化機能の設定項目およびそれぞれの制限事項は以下のとおりです。

● ハートビート送信間隔

ハートビートの送信間隔(秒)を指定します。

● ハートビートタイムアウト時間

ハートビートが途絶して相手Firewallがダウンしたと認識するまでの時間(秒)を指定します。ハートビート送信間隔より大きい値を指定してください。

• Firewall起動待ち時間

起動時に相手Firewallの起動時間を待ち合わせる時間(秒)を指定します。ハートビートタイムアウト時間より大きい値を指定してください。

● 内部通信用TCPポート番号

2台のFirewall間で通信を行うためのTCPのポート番号を指定します。

● 内部通信用UDPポート番号

2台のFirewall間で通信を行うためのUDPのポート番号を指定します。

Firewall1のサーバ名

ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

Firewall2のサーバ名

ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

● Firewall1のインタコネクトアドレス

相手Firewallを監視するためのアドレスとネットマスクを入力します。

• Firewall2のインタコネクトアドレス

相手Firewallを監視するためのアドレスとネットマスクを入力します。

● 仮想IPアドレス

二重化機能を使用する場合、Firewall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フェースを除く全インタフェースに仮想IPアドレスを設定して ください。

 É
 税対象アドレス

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Firewallにフェイルオーバが行われます。本項目の設定は省略することができます。

• プロキシARPアドレス

StaticNAT機能を使用する場合、外部公開アドレスとして使用するアドレスを指定して ください。

運用系Firewall

運用系のFirewallを指定します。

● 自動フェイルバック

自動フェイルバックを行うかどうか設定します。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。

基本設定ツールでの設定手順を示します。以下の内容は、本章の「セットアップ」で示した ネットワーク構成を例にとって説明します。



- ① 管理クライアントからFirewallの設定ツールであるfwsetupコマンドを起動する。
- ②「use cluster system」の項目までは、<ENTER>キーを押して進み、設定内容を確認する。

START CLUSTERPRO configuration	
CLUSTERPRO Configuration Tool Ver 1.0-4	
cluster configuration	
Input HB interval(0 - 999)[0] :	①
Input HB timeout(1 - 999)[1] :	2
Input WAIT Timeout(1 - 999)[5] :	3
Input API TCP port number[28001] :	. 4
Input HB UDP port number[28002] :	5
Input server1 host name : fws1	. 6
Input server2 host name : fws2	⑦

③ 二重化機能を使用する。<Y>キーを押す。

- ① ハートビート送信間隔(秒)を入力する。
- ② ハートビートタイムアウト時間(秒)を入力する。
- ③ 起動時に相手Firewallの起動を待ち合わせる時間(秒)を入力する。
- ④ 内部通信用のTCPポート番号を入力する。

- ⑤ 内部通信用のUDPポート番号を入力する。
- ⑥ Firewall1のサーバ名(ホスト名)を入力する。

ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

⑦ Firewall2のサーバ名(ホスト名)を入力する。

ホスト名はFQDN形式ではなく、ドメイン名を除いた名前を指定してください。

```
---- server configuration -----
Input fws1 interconnect address
address(1) : 192.168.2.1
netmask(1) : 255.255.255.0
address(2) :
No. address/netmask
 1 192.168.2.1/255.255.255.0
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
Input fws2 interconnect address ......
address(1) : 192.168.2.2
netmask(1) : 255.255.255.0
address(2) :
No. address/netmask
   192.168.2.2/255.255.255.0
 1
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

- ① 運用系FirewallのFirewall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。 インタコネクトアドレスは16個まで設定可能です。 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>+-+ <Enter>+-: インタコネクト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。 指定した番号の設定を削除します。 <D>キー+「削除する一覧の番号」+<Enter>キー: <L>+-+<Enter>+-: 一覧を再表示します。 <Enter> \pm -: 次の項目へスキップします。 待機系FirewallのFirewall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
- (2) 待機系FirewallのFirewall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。

```
---- group configuration ------
No. name
 1 group0
---- group fip configuration -----
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
    202.247.5.3/255.255.255.0
 1
    172.168.1.3/255.255.255.0
 2
    192.168.1.3/255.255.255.0
 3
("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。

仮想IPアドレスは8個まで設定可能です。

設定後に一覧を表示しますので、確認、または、変更して<Enter>キーで進みます。



二重化機能を使用する場合、サーバへのアクセスは、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フェース以外の全インタフェースに仮想IPアドレスを設定してくだ さい。

```
----- group0 ipw configuration ------ ①

Input IPW address ------- ①

address(1) : 202.247.5.xxx |202.247.5.xxx

address(2) :

No. address

1 202.247.5.xxx |202.247.5.xxx

("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ので、確認、または、変更して<Enter>キーで進みます。



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

```
---- group0 proxy arp configuration ----- 
Input proxy address ------ ①
address(1) : 202.247.5.4
address(2) :
No. address
1 202.247.5.4
("a"=add | "m num"=modify | "d num"=delete | "l"=list | Enter=next):
```

① 設定するプロキシアドレスを指定する。

プロキシARPアドレスを入力します。プロキシARPアドレスは256個まで設定可能です。

設定後に一覧を表示しますので、確認、または、変更して<ENTER>キーで進みます。



プロキシARPアドレスでは、運用系サーバにてStaticNATを行う場合の公開用IPアドレスとなります。StaticNATで公開するIPアドレスを全て登録してください。

group0 resource configuration	
Input primary server hostname(fws1, fws2)[fws1] :	
Input failback policy(1:auto, 2:manual) [manual] :	
END CLUSTERPRO configuration	
: 《略》 :	

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。



上記の設定はfws1、fws2で同じ設定にしてください。

上記の設定後は、本体を再起動させる必要があります。以下のコマンドを入力してください。

shutdown -r now

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 としてサーバに設定した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。

【参考】NATのためのルーティングテーブル

Firewallの二重化構成において、DMZ上やローカルネット内のサーバのアドレスを静的に NAT(アドレス変換)し、インターネット上に公開する場合、ルーティングテーブルとプロキ シARPテーブルの設定を別途行う必要があります。

例として、以下のネットワーク構成の場合、公開用WWW/FTPサーバを該当するホストと すると、以下のようなルーティングテーブルとプロキシARPテーブルの設定をFirewallへ行 う必要があります。



destination 202.247.5.127 netmask 255.255.255.255 gateway 172.16.1.2

変換後のアドレスをdestination、実際のアドレスをgatewayに指定してください。 fwsetupのstatic routingの項目で設定することができます。 プロキシARPの設定については、前述の「二重化機能の設定」を参照してください。



二重化構成の運用について説明します。

障害発生時の対応

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。

• ダウンしたときのメッセージ

```
Subject: WARNING: [group0] is downed
  !!WARNING!!
  [group0] is not active on Firewall(fws1.nec.co.jp[202.247.5.1]).
  Urgently check it.
  If you recieved a previous message "NOTICE: [group0] changes
  to the active firewall" from fws1.nec.co.jp[202.247.5.1],
  both groups are downed.
  Urgently check both groups!!
```

• フェイルオーバしたときのメッセージ

```
Subject: NOTICE: [group0] chnges to the active firewall
 !!NOTICE!!
 [group0] chnges to the active
 firewall(fws2.nec.co.jp[202.247.5.2]).
 Urgently check another failed firewall.
```



ダウンした要因がネットワークの通信障害などの場合、ダウンしたときのメッセージがサー バ内に滞留し、障害復旧後に送信されることがあります。メッセージを受信したら必ずその 発信時刻を確認するようにしてください。

メールを受信したらExpress5800/FW300の状態を確認し、システムログからフェイル オーバが発生した要因を確認し、必要な対処を行ってください。メッセージ内容、対処方法 等は「付録C 二重化機能のログメッセージ」を参照してください。

- 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、待機系 Firewallに業務を引き継いだ場合、以後、そのサーバ上での業務の起動が拒否されるよう になります。そのFirewallが業務の起動拒否状態かどうかは、[clpstat -s]の [STARTING]で確認できます。
- 運用系Firewallが起動拒否状態のまま待機系Firewallで業務を遂行している場合、待機系 Firewallで監視対象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ても、待機系Firewallから運用系Firewallへは業務が引き継がれず、引き続き待機系 Firewallで業務が遂行されます。但し、上記の条件においても相互のインターコネクトの 通信が途絶した場合においてはこの限りではなく、起動拒否状態であっても運用系 Firewallで業務が遂行されます。起動拒否状態は、次の手順により解除されます。

[監視対象IPアドレスとの通信途絶が原因の場合]

- 監視対象IPアドレスとの通信復帰
- clpgrpコマンドによって業務を起動
- Firewall再起動

[FireWall-1プロセス消滅が発生した場合]

- clpgrpコマンドによって業務を再開
- Firewall再起動

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。

clpstat -s [-h host_name] -n -i [-h host_name]

状態、設定情報の表示を行います。

〈オプション〉

-sまたは引数なし 各種状態を表示します。

-n.....インタコネクトマップを表示します。

-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。

# clpstat -s	
* server0 : fws1 1.0-1.4 server1 : fws2	
server0 server1	
SERVER STATUS ONLINE ON GROUPO STATUS ONLINE OF POLICY 1st 2: STARTING ALLOW DE	3 GENE GENE M GENE GENE M GENE M GENE GEN
<pre><a> group0-ipw0 ONLINE 00 192.168.1.254</pre>	NLINE
<pre><u> group0-fip0</u></pre>	FFLINE
202.247.5.5	FFLINE
S: /opt/necfws/bin/ckcstat E: /opt/necfws/bin/ckcstat	
<pre><u> group0-exec1 ONLINE 0 W: /opt/necfws/bin/ckfwalive E: /opt/necfws/bin/ckfwalive -k</u></pre>	FFLINE

clpstat -sの各項目について

- ① サーバ名(1台目)
- ② サーバ名(2台目)
- ③ サーバの状態
 ONLINE : ハートビートが受信されている
 OFFLINE : ハートビートが受信されていない
- ④ グループの状態
 ONLINE :正常
 OFFLINE :停止
 ERROR :異常
 - UNKNOWN : 不明
- ⑤ フェイルオーバポリシ
- ⑥ グループ起動の許可/禁止
 - ALLOW :許可 DENY :禁止
 - UNKNOWN : 不明
- ⑦ IPWリソースの起動種別と状態
- <A> :全サーバ起動
くU> :単サーバ起動
ONLINE :正常
 - OFFLINE :停止
 - ERROR : 異常
 - UNKNOWN : 不明

- ⑧ IPWリソース監視アドレス
- ⑨ FIPリソースの状態※ IPWリソースと同様
- 10 FIPリソース設定アドレス/ネットマスク
- PARPリソースの状態
 * IPWリソースと同様
- 12 PARPリソース設定アドレス
- ③ EXECリソースの状態※ IPWリソースと同様
- ④ EXECリソース起動時実行パス S : 監視なし
 - ₩ : 監視あり
- 15 EXECリソース停止時実行パス

# clpstat -i			
CLUS	STER INFORMATION =========		
SERVER : İWSl			
CLUSTER :			
STARTUP : AUTO			\bigcup
WAIT timeout : 5			(2)
HB port : 24002			3
HB interval : 1			4
HB timeout : 5 ······			9
API port : 24001			6
API timeout : 30 ·····			\bigotimes
LOG port : 0 ······			8
ping timeout : 3 ······			9
RECOVER : RESTAN	τ		
RETRY count : 5 ······			U
			(12)
SERVERO : IWSI			13
INTERCONNECTO : 192	2.168.1.1/255.255.255.0		U
INTERCONNECTI : 19.	2.168.2.1/255.255.255.0		
SERVER1 · fws2			(14)
INTERCONNECTO : 192	2.168.1.2/255.255.255.0		(15)
INTERCONNECT1 : 192	2.168.2.2/255.255.255.0		
			<u>(10)</u>
GROUP0 : group0			
START : A	AUTO ·····		
FAILBACK : N	IANUAL ·····		
ENVIRONMENT : A	ACT_NORMAL		W
RECOVER : 1	IGNORE		0
RETRY count : ()/0		20
FAILOVER policy : ():fwsl 1:fws2 ·····		E)
			23
IPW0 : group0-ipw0 ·	2.05		ã
TYPE	: ASR	1	Ã
POLLING address	: 192.168.1.254		26
RECOVER	2 /2		n
REIRI COUIIC	: 2/2		e
FIPO : group0-fip0			28
TYPE	: USR		29
ADDRESS	: 202.247.5.3/255.255.255.0		30
INTERFACE	: eth0:1		31
PING count	: 0		32
ARP count	: 1		33
RECOVER	: RETRY		34)
RETRY count	: 5/5		(35)
	· · · · · · · · · · · · · · · · · · ·		36
TYDE	. IISD		37)
TP ADDRESS	· 202 247 5 5 ·····		38
MAC ADDRESS	: 00:A0:34:1A:4C:D3		39
INTERFACE	: eth0		40
PING count	: 0		(41)
ARP count	: 1		42
RECOVER	: RETRY		43
RETRY count	: 5/5		(44)
<次ページに続<>			

ACT path	: /opt/necfws/bin/ckcstat	
DEACT path	: /opt/necfws/bin/ckcstat	
POLLING	: NO	
PID	: 21623	
RECOVER	: STOP	
RETRY count	: 0/0	
ACT path DEACT path	: /opt/necfws/bin/ckfwalive : /opt/necfws/bin/ckfwalive -k	
DEACT path	: /opt/necfws/bin/ckfwalive -k	
POLLING	: YES	
PID	: 21625	
RECOVER	: FAILOVER	
RETRY count	: 2/2	

clpstat -iの各項目について

\bigcirc	CLUSTERPRO /	AE の起動方法
	YES	:自動起動
	NO	: 手動起動
2	起動待ち合わせ	寺間(秒)
3	ハートビート受信	言用 UDP ポート番号
4	ハートビート送信	言間隔(秒)
(5)	ハートビートタ-	イムアウト(秒)
6	API用 TCP ポー	卜番号
\bigcirc	APIタイムアウト	(秒)
8	ログポート番号	
9	pingコマンドタ-	イムアウト(秒)
\bigcirc	リカバリ方法	
	RESTART	: CLUSTERPRO AE再起動
	STOP	: CLUSTERPRO AE停止
	HALT	: OSシャットダウン
	REBOOT	: OSリブート
	UNKNOWN	:不明
1	リトライ回数	
(12)	サーバ名(1台目)	
(13)	インタコネクトフ	P ドレス
(14)	サーバ名(2台目)	
(15)	インタコネクトフ	P ドレス
(16)	グルーブ名	
1)	グルーブ起動方法	去
	AUTO	
	MANUAL	: 手動
_	UNKNOWN	:不明
(18)	フェイルバックチ	
	AUTO	
	MANUAL	: 寺動
	UNKINOVVIN	:个明

(19)	環境変数		
	ACT_NORMAL		:通常起動
	ACT_FAILOVER	2	:フェイルオーバ
	DEACT_NORM	AL	:通常停止
	DEACT_ILLEGA	AL.	: 異常停止
20	グループリカバ	リ方法	
	IGNORE	: 無視	
	RETRY	:再起	動
	STOP	: 停止	
	FAILOVER	:フェ	イルオーバ
	UNKNOWN	:不明	
21	リトライ回数		
22	運用系サーバ名	待機系·	サーバ名
23	IPWリソース名		
24)	起動タイプ		
	ASR	: 全起	動リソース
	USR	:単起	動リソース
25	IPWリソース監視	見対象ア	^ドレス
26	IPWリソースリス	カバリ方	远
	IGNORE	: 無視	
	RETRY	: 再起	動
	STOP	: 停止	
	FAILOVER	:フェ	イルオーバ
	UNKNOWN	:不明	
27)	リトライ回数		
28	FIPリソース名		
29	起動タイプ		
	※ IPWリソース	と同様	
30	FIPアドレス		
31	FIPインタフェー	-ス	

寥 ping回数

二重化構成について

- ③ arp回数
- ③ FIPリソースリカバリ方法※ IPWリソースと同様
- ③ リトライ回数
- 36 PARPリソース名
- ③ 起動タイプ※ IPWリソースと同様
- 38 PARPアドレス
- 39 MACアドレス
- @ PARPインタフェース
- ④ ping回数
- arp回数
- ④ PARPリソースリカバリ方法※ IPWリソースと同様

- 🚇 リトライ回数
- ④ EXECリソース名
- ④ 起動タイプ※ IPWリソースと同様
- ④ EXECリソース起動時実行パス
- 49 EXECリソース停止時実行パス
- ④ EXECリソース監視設定※ IPWリソースと同様
- ⑤ EXECリソースプロセスID
- ⑤ EXECリソースリカバリ方法 ※IPWリソースと同様
- ¹2 リトライ回数

# clpstat -n				
server1 : fws2	ERCONNECT	INFORMATION	 	(1) (2)
[on server0 : 0 address	NLINE] server0	serverl	 	
192.168.1.1 192.168.2.1	OK OK	OK OK	 	
[on server1 : ON address	LINE] server0	serverl	 	
192.168.1.2 192.168.2.2	OK OK	OK OK		

clpstat -nの各項目について

- ① サーバ名(1台目)
- ② サーバ名(2台目)
- ③ サーバ(1台目)ステータス
- ④ プライマリインタコネクトアドレス/ステータス
- ⑤ セカンダリインタコネクトアドレス/ステータス
- ⑥ サーバ(2台目)ステータス

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。

```
clpgrp -s [-h host_name] [-g group_name]
        -t [-h host_name] [-g group_name]
        -m [-h host_name] [-g group_name]
```

業務の起動/停止関連操作を行います。

〈オプション〉

- -s.....業務の起動を行います。すでに起動されていたり、他のサーバで起動している場合には失敗します。
- -t業務の停止を行います。すでに停止されていたり、他のサーバで起動 されている場合には失敗します。
- -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 操作対象サーバ名です。指定なしの場合、コマンド実行サーバが対象 となります。-m オプション指定時には、業務移動元サーバの意味も持 ちます。
- -g group_name 操作対象グループを指名します。指定なしの場合、全グループが対象 となります。

二重化構成の再セットアップ

二重化構成の場合の再セットアップについて説明します。 次の手順に従って再インストールします。

● 管理サーバ

Express5800/FW300またはFW500を管理サーバにしている場合のFireWall-1管理サーバの再インストールについて説明します。

- 1. 3章の「再セットアップ」-「システムの再インストール」の手順5までを行います。
- 2. 起動後、CD-ROMドライブにCheck Point NGX CD-ROM (CD1)をセットし、FireWall-1のモジュールを以下の手順で適用します。

```
# mount /dev/cdrom
# cd /mnt/cdrom
# ./UnixInstallScript
```

- 3. [Welcome]画面が表示されますので、<N>キーで次に進みます。
- 4. 使用許諾書が表示されますので、お読みいただいた後、使用許諾に承認した場合は<Y>キー を押します。
- 5. 以下のメッセージが表示されます。<2>キーを入力し、<N>キーで次に進みます。

Check Point Power - for headquarters and branch offices Check Point UTM - for medium-sized businesses 1 () Check Point Power 2 (*) Check Point UTM

6. 以下のメッセージが表示されます。<1>キーを入力し、<N>キーで次に進みます。

```
Please select one of the following options
1 (*) New Installation
2 ( ) Installation Using Imported Configuration
```

7. 以下のメッセージが表示されます。<2>キーを入力し、<N>キーで次に進みます。

```
The following products are available in this version
Please select product(s)
1 [] VPN-1 UTM
2 [*] SmartCenter UTM
3 [] Eventia Reporter UTM
4 [] SmartPortal
```

8. インストールするプロダクトが表示されます。<N>キーを入力し、次に進みます。

```
You have selected the following products for installation: * SmartCenter UTM
```

以下のメッセージが表示されます。ここではライセンス入力しないため、<n>キーを入力し、
 <Enter>キーで次に進みます。

```
Configuring Licenses...

Host Expiration Signature Features

Note: The recommended way of managing licenses is using SmartUpdate.

cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [y] ? n
```

以下のメッセージが表示されます。ここでは登録を実施しないため、<n>キーを入力し、
 <Enter>キーを入力します。継続するので、<y>キーを入力し、<Enter>キーを入力します。

11. 以下のメッセージが表示されます。<n>キーを入力し、<Enter>キーで次に進みます。

```
Configuring GUI Clients...

GUI Clients are trusted hosts from which

Administrators are allowed to log on to this SmartCenter Server

using Windows/X-Motif GUI.

No GUI Clients defined

Do you want to add a GUI Client (y/n) [y] ? n
```

Configuring Group Permissions... Please specify group name [<RET> for super-user group]: No group permissions will be granted. Is this ok (y/n) [y] ?

13. 以下のメッセージが表示されます。<n>キーを入力し、<Enter>キーで次に進みます。

14. 再起動をするか確認のメッセージが表示されます。ここでは、<E>キーを入力し、次に進みます。

15. CD-ROMを取り出し、再起動します。

```
# cd
# eject
# shutdown -r now
```

16. 3章の「再セットアップ」-「システムの再インストール」の手順20を行い、管理サーバへパッ クアップをリストアします。

• Firewall本体

Firewall本体の再インストール方法について説明します。

- 1. 3章の「再セットアップ」-「システムの再インストール」の手順5までを行います。
- 記動後、CD-ROMドライブにCheck Point NGX CD-ROM (CD1) をセットし、FireWall-1 のモジュールを以下の手順で適用します。

```
# mount /dev/cdrom
# cd /mnt/cdrom
# ./UnixInstallScript
```

- 3. [Welcome]画面が表示されますので、<N>キーで次に進みます。
- 4. 使用許諾書が表示されますので、お読みいただいた後、使用許諾に承認した場合は<Y>キー を押します。
- 5. 以下のメッセージが表示されます。<2>キーを入力し、<N>キーで次に進みます。

```
Check Point Power - for headquarters and branch offices
Check Point UTM - for medium-sized businesses
1 () Check Point Power
2 (*) Check Point UTM
```

6. 以下のメッセージが表示されます。<1>キーを入力し、<N>キーで次に進みます。

```
Please select one of the following options
1 (*) New Installation
2 ( ) Installation Using Imported Configuration
```

7. 以下のメッセージが表示されます。<1>キーを入力し、<N>キーで次に進む。

```
The following products are available in this version

Please select product(s)

1 [*] VPN-1 UTM

2 [ ] SmartCenter UTM

3 [ ] Eventia Reporter UTM

4 [ ] SmartPortal
```

8. インストールするプロダクトが表示されます。<N>キーを入力し、次に進みます。

You have selected the following products for installation: \star VPN-1 UTM

9. 以下のメッセージが表示されます。<n>キーを入力し、<Enter>キーで次に進みます。

```
Welcome to Check Point Configuration Program

Is this a Dynamically Assigned IP Address gateway installation ? (y/n) [n] ?
```

10. 以下のメッセージが表示されます。<y>キーを入力し、<Enter>キーで次に進みます。

Would you like to install a Check Point clustering product (CPHA, CPLS or State Synchronization)? (y/n) [n] ? ${\bf y}$ IP forwarding disabled

以下のメッセージが表示されます。ここではライセンス入力しないため、<n>キーを入力し、
 <Enter>キーで次に進みます。



12. 以下のメッセージが表示されます。<Enter>キーを2回入力し、次に進みます。

```
Configuring Group Permissions...

Please specify group name [<RET> for super-user group]:

No group permissions will be granted. Is this ok (y/n) [y] ?
```

13. 以下のメッセージが表示されます。FireWall-1管理サーバとFirewall間での通信に使用するパ スワードを設定してください。

```
Configuring Secure Internal Communication...

The Secure Internal Communication is used for authentication between

Check Point components

Trust State: Uninitialized

Enter Activation Key:

Retype Activation Key:
```

14. 再起動をするか確認のメッセージが表示されます。ここでは、<E>キーを入力し、次に進みます。

```
Installation program completed
In order to complete the installation
you must reboot the machine.
Would you like to reboot the machine ?
NOTE: Please remove the CD from
your machine before reboot.
```

15. CD-ROMを取り出し、再起動します。再起動後、必要なLANケーブルを接続してください。

```
# cd
# eject
# shutdown -r now
```

● セキュリティポリシーをインストール

セキュリティポリシーの再インストールについて説明します。

1. SmartDashboardから管理サーバへ接続し、FireWall-1管理サーバとFirewall本体との通信を 行うための設定を行う。

FireWall-1管理サーバとFirewall本体との通信を行うための設定については、本章の「セキュリティポリシーの設定」-「Firewallオブジェクトの作成」を参照してください。

- 2. Firewall本体へセキュリティポリシーをインストールする。
- 3. 運用系Firewall、待機系Firewallの順で再起動する。



- Firewall本体が2台以上必要です。また、ライセンスは同じユーザー数のものをそれぞれの実IPアドレスで申請する必要があります。
- 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。
- フェイルオーバが発生した場合、IKEセッションは失われる可能性があります。
- 自動フェイルバックが設定されている場合、運用系サーバ再起動後、自動的に運用系サーバ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、待機系サーバで業務が起動されたままになり、運用系サーバの方が待機状態になります(運用系、待機系の逆転)。運用系サーバに業務を切り替える場合はコマンド(clpgrp-m)によりサーバの切り替えを実行する必要があります。
- 待機系で監視対象IPアドレスとの通信途絶が発生している場合、運用系でリソース異常 が発生しても待機系サーバに業務は引き継がれません。ただし、この場合でもコマンド (clpgrp-m)により業務実行サーバを切り替えることは可能です。

~Memo~