

本章ではFirewallServerを使用してVPN(Virtual Private Network)環境を構築するための手順を説明します。

ここで示しているのは一例です。実環境ではネットワーク構成 · セキュリティポリシー等により作成手順 は異なります。

FireWall-1,VPN の設定方法およびGUIクライアントの使用方法の詳細に関してはCheck Point 2000 パッケージ添付の日本語ユーザ・ガイドCD-ROM内にあるマニュアル(¥Jdocs¥UserGuide¥FireWall-1¥下のPDFファイル)を参照してください。

エクストラネットVPNの設定(→94ページ) ......2台のFirewallServer間でVPN環境を構築する場合の設定方法について説明します。

リモートアクセスVPNの設定(→114ページ) .....リモートユーザーが企業ネットワークへ安全にア クセスするための設定方法について説明します。

# エクストラネットVPNの設定

ここでは下図のネットワーク環境のように、2台のFirewallServer間(tokyo-osaka)でVPN環境を構築する際の手順を簡単に説明します。

暗号化方式はIKEを使用した例です。その他の暗号化方式を使用する場合や詳細な設定方法に関しては Check Point 2000パッケージ添付の日本語ユーザ・ガイドCD-ROM内の「Check Pointパーチャル・プ ライベート・ネットワーク」(¥Jdocs¥UserGuide¥FireWall-1¥VPNJ.pdf)を参照してください。



## 設定手順の流れ

VPN構築手順は、下図に従って説明します。



## 前準備 ~FireWall-1のセキュリティポリシーの設定~

次の順序に従ってセットアップの前準備をします。

### GUIクライアントのセットアップ

GUIクライアントのセットアップについては、2章を参照してください。

### ウィザードによるセキュリティポリシーの作成

ウイザードによるセキュリティポリシーの作成は、2章の「セキュリティポリシーの設定」を 参照してください。

ここでは、以下の条件で設定されていることを前提に説明します。 以下の条件下でウイザードにより作成されたセキュリティポリシーも併せて示します。

- tokyo側の設定
  - 選択したRulebase Name: S
  - firewallのオブジェクト名:

□ IPアドレス:

- 内部のネットワークオブジェクト名:
  - □ ネットワークアドレス:
  - 🔲 ネットマスク:
- 許可するサービス:

Starter Network

tokyo

eth0(外側) 202.247.5.136 eth1(内側) 172.16.1.0

tokyo\_local\_network

172.16.1.0 255.255.255.0

ftp

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	tokyo	Any	drop	Alert	Gateways	🔊 Any
2	tokyo_local_network	Any	InternetServices	accept	Long	Gateways	Any
3	<ul> <li>Any</li> </ul>	Any	SilentServices	DROP drop		Gateways	Any
4	) Any	) Any	Any	drop	Alert	GW Gateways	) Any

#### osaka側の設定

- 選択したRulebase Name: Publisher Network
- − firewallのオブジェクト名: osaka
   □ IPアドレス: eth0(外側) 143.101.250.20
- 内部のネットワークオブジェクト名: osaka\_local\_network
   □ ネットワークアドレス: 172.16.2.0
   □ ネットマスク: 255.255.255.0
- 許可するサービス:
- − 公開サーバオブジェクト名:
   □ IPアドレス:
- ftp
- FtpServer
- 172.16.2.110

eth1(内側) 172.16.2.20

No.	Source	Destination	Service	Action	Track	Install On	Time
1	🔊 Any	osaka	Any	(DROP) drop	Alert	Gateways	🗩 Any
2	esaka_local_network	Any	InternetServices	accept	Long	GW Gateways	Any
3	🔊 Any	FtpServer	19 ftp	accept	Long	GW Gateways	Any
4	🔊 Any	Any	👕 SilentServices	(DROP) drop		GW Gateways	Any
5	🗩 Any	🗩 Any	Any	drop	Alert	GW Gateways	🖲 Any

## tokyo側の設定

最初に各管理ステーションであるFirewallServer「tokyo」と「osaka」でお互いの鍵をネゴシ エーションする方式とデータを暗号化する方式をあらかじめ設定しておく必要があります。 ここでは、tokyo側の設定手順を説明します。osaka側の設定手順についてはこの後の項を 参照してください。

### オブジェクトの作成

オブジェクトを作成します。

#### ゲートウェイのワークステーション・オブジェクトの作成

次に[New]ボタンをクリックし、ドロップダウンリストからWorkstationを選択して、 Workstation Propetesを開きFirewallServer(osaka)のワークステーション・オブジェクト を作成します(ここではオブジェクト名をosakaにしています)。

osakaの設定内容は、すでにポリシーウィザードにより作成されているFirewallServer (tokyo)のワークステーション・オブジェクト「tokyo」と同様に、マシン名、IPアドレスを入 力して、TypeにはGatewayをチェックし、Modules InstalledのVPN-1 & FireWall-1に チェックしてください。

また管理ステーションであるtokyoでは、Management Stationにチェック、Locationの設 定でInternalにチェックしてありますが、osakaではManagement Stationにチェックせず Locationの設定でExternalにチェックしてください。

Workstation Properties	Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authentication	General Interfaces   SNMP   NAT   VPN   Authentication
Name: tokyo	Name: osaka
IP Address: 202.247.5.136 Get address	IP Address: 143.101.250.20 Get address
Comment: The Firewalled Gateway	Comment
Color:	Color:
CLocation: © Internal © External Type: C Host © Gateway	Location:
Modules Installed	Modules Installed
VPN-1 & FireWall-1 Version: 4.1 Version: Get	✓ VPN-1 & FireWall-1 Version: 4.1 ▼ Get
FloodGate=1 Version: 4.1	FlgodGate=1 Version: 4.1 ▼
☑ [ <u>Management Station</u> ]	☐ [ <u>Management Station</u> ]
OK キャンセル ヘルプ	OK キャンセル ヘルナ

tokyoのWorkstation Propeties

osakaのWorkstation Propeties

#### ネットワーク・オブジェクトの作成

次に保護すべきtokyo側のローカルネットワークとosaka側のローカルネットワークのネットワーク・オブジェクトを作成します。tokyo側のネットワーク・オブジェクトはすでに作 成されています(ウィザードにより作成される)ので、osaka側のネットワーク・オブジェク トを作成します。

もし、tokyo側のネットワーク・オブジェクトが作成されていない場合は、ここで作成して ください(ここでは、tokyo\_local\_networkという名前でネットワーク・オブジェクトを作成 して、説明しいます)。

ネットワーク・オブジェクトの作成には、 <u><u></u> の を りックして、Network Objectsウィンド ウを開きます。</u>

次に[New]をクリックし、ドロップダウンリストからNetwrokを選択して、Network Propetesを開き、osaka側のプライベートネットワークのネットワーク・オブジェクトを作 成します(ここではオブジェクト名をosaka\_local\_networkにしています)。また、location はExternalにチェックしてください。

Network Properties	Network Properties
General NAT	General NAT
Name: tokyo_local_network	Name: losaka_local_network
IP Address:  172.16.1.0	IP Address: 172.16.2.0 Get address
Net <u>M</u> ask: 255.255.255.0	Net Mask: 255.255.255.0
Color: Color:	Color:
Location: Broadcast: © Internal © External © Allowed © Disallowed	Location:Broadcast C Internal ⓒ External ⓒ Allowed ○ Disallowed
	OK +++>tell ^/l/

tokyoのプライベートネットワーク

osakaのプライベートネットワーク

### 鍵ネゴシエーションの設定

鍵ネゴシエーションを設定します。

#### 暗号化ドメインの作成とネットワーク・オブジェクトの登録

ここでは暗号化対象のネットワークあるいはホストを登録する暗号化ドメイン(グループ)の 作成手順について説明します。

らったいので、Network Objectsウィンドウを開きます。

次に[New]ボタンをクリックし、ドロップダウンリストからGroupを選択して、Group Propetesを開き、tokyo側の暗号化ドメインを作成します(ここでは、暗号化ドメインを tokyo\_vpn\_groupとして作成しています)。

作成した暗号化ドメインに前述の「オブジェクトの作成」で作成したネットワーク・オブジェ クトtokyo\_local\_networkを選択し[Add]ボタンをクリックして、Not in GroupからIn Groupへ移動させてください。

同様にosaka側の暗号化ドメインを作成し(ここでは、osaka\_vpn\_groupとして作成しています)、前述の「オブジェクトの作成」で作成したosaka側のネットワーク・オブジェクト osaka\_local\_networkを登録します。

Group Properties	Group Properties
Name: tokyo_vpn.group	Name:  osaka_vpn_group
Comment	Comment
Cojor	Color:
Not in Group: In Group:	Not in Group: [n Group:
saka 🛱 tokyo_local_network	🔛 osaka 🖳 🖳 osaka_local_network
	La tokyo 是 tokyo_local_network Add >
<u> </u>	< <u>Remove</u>
OK Cancel Help	OK Cancel Help

tokyoの暗号化ドメイン

osakaの暗号化ドメイン

#### 暗号化ドメインの登録

作成した暗号化ドメインを前述の「オブジェクトの作成」で作成したゲートウェイに登録する 方法を説明します。この登録により、FirewallServerに暗号化対象のネットワークおよびホ ストを認識させます。

前述の「オブジェクトの作成」で作成したゲートウェイtokyoのWorkstation PropertiesウィンドウからVPNタブを開きます。

次にDomainでOtherを選択し、「暗号化ドメインの作成とネットワーク・オブジェクトの登録」で作成した暗号化ドメインtokyo\_vpn\_groupを選択します。

osaka側のワークステーション・オブジェクトも同様に暗号化ドメインosaka\_vpn\_group を選択します。



tokyoの暗号化ドメインの登録

osakaの暗号化ドメインの登録

#### 認証方式の設定

ここでは、tokyoとosakaで行う認証方式の設定を説明します(ここでは、IKEの場合を説明します)。

まずワークステーション・オブジェクトtokyoのWorkstation Propertiesウィンドウから VPNタブを開きます。

次にEncryption schemes definedでIKEをチェックし、[Edit]ボタンをクリックし、IKE Propertiesウィンドウを開きます。

IKE Propertiesウィンドウでは、認証で使用される暗号方式やアルゴリズムを設定しますが、通常はSupport authentication methods以外はデフォルトのままにしておいてください。

Support authentication methodsは、Pre-Shared Secretにチェックしてください。 最後に[OK]ボタンをクリックし、IKE Propertiesウィンドウを閉じます。

Workstation Properties	×	
General   Interfaces   SNMP   NAT   Certificates VPN   Authentication		
Domain: Disabled Valid Addresses (of Interfaces) Other: tokyo_vpn_group Exportable for SecuRemote Traffic Control Logging-		
Ium on Traffic Control Logging	IKE Properties	x
	General	
	Support key exchange encryption with:	
OK ++>>セル ^>1/7	Support authentication methods:	
	✓ Pre-Shared Secreti       Edit Secrets         ✓ Public Key Signatures       Oprificure         ✓ VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	
	▼ Supports Aggresive Mode ▼ Support keys exchange for Subnets	

次にEncryption schemes definedでIKEをチェックし、IKE Propertiesウィンドウを開きま す。IKE Propertiesウィンドウもtokyo同様に、通常はSupport authentication methods 以外はデフォルトのままにし、Support authentication methodsは、Pre-Shared Secret にチェックしてください。

osakaでは、続けて[Edit Secrets]ボタンをクリックして、Shared Secretウィンドウ(下図) を開きます。Shared Secrets Listにtokyoのワークステーションが表示されていますので、 ワークステーションを選択し、[Edit]ボタンをクリックします。次にShared Secretを入力 するテキスト・ボックスが表示されますので、入力して[Set]ボタンをクリックします。そ の後、Shared Secretウィンドウを終了させます。

ここで入力する文字列は6文字以上、英数字で4つ以上異なる文字を入力してください。 なお、入力する文字列にFireWall-1/VPN-1で使用する予約語は使用できません。予約語については付録Bを参照してください。

Shared Se	cret	×
Share	ed Secrets List:	
Pe	eer Name Shared Secret	
tol	kyo <u>E</u> dit	
	Remove	
	<u>Temore</u>	
Er	nter secret: Set	
	OK Cancel	

以上で鍵ネゴシエーションの設定は終了です。続いてデータの暗号化方式について説明しま す。

## 暗号化の設定

暗号化の設定をします。

#### セキュリティポリシーの作成

ここでは、データを暗号化するルールの追加と暗号化方式の設定を説明します。 ルール1の下に新しいルールを追加します。このルールのSourceカラムにtokyo側のネット ワークオブジェクト、Destinationカラムにosaka側のネットワークオブジェクトを設定しま す。Serviceカラムはftpサービス、ActionカラムにEncryptを設定して、tokyo側のネット ワークから、osaka側のネットワークへの通信を暗号化するルールを作成します(下図参 照)。

No	. Source	Destination	Service	Action	Track	Install On	Time
1	) Any	tokyo	Any	drop	Alert	Gw Gateways	Any
2	tokyo_local_network	e osaka_local_network	19 ftp	Encrypt	Long	Gateways	🔊 Any
3	tokyo_local_network	Any	InternetServices	accept	Long	Gateways	Any
4	) Any	Any	SilentServices	GROPI drop		Gw Gateways	Any
5	) Any	Any	le Any	(DROP) drop	Alert	Gateways	Any

#### 暗号化の設定

ルールのActionカラムのEncryptを選択して、ダブルクリックします。

Encryption PropertiesウィンドウのGeneralタブからIKEを選択して、[Edit]ボタンをクリッ クするとIKE Propertiesウィンドウが開きます。このウィンドウでは、ルールが適用される 接続を暗号化するのに使用するIPSec方式を定義します。

通常の場合、Allowed Peer Gateway以外は、デフォルトのままで問題ありません。

Allowed Peer Gatewayでは通信先のFirewallServerであるosakaワークステーションを選択 してください。

Encryption Properties	x
General	1
Encryption schemes defined:	
	IKE Properties
Edit	General
	Transform:
	Encryption + Data Integrity (ESP)     Data Integrity Only (AH)
	Encryption Algorithm: DES
	Data Integrity
	Allowed Peer Gateway:
	□ Use Perfect Forward Secrecy

### セキュリティポリシーのインストール

最後に作成したルールを有効にする必要があります。 ♥ をクリックして、作成したルール を有効にしてください。 以上でtokyo側の設定は終了です。

## osaka側の設定

ここではosaka側で鍵のネゴシエーションする方式とデータを暗号化する方式について説明 します。

### オブジェクトの作成

オブジェクトを作成します。

#### ゲートウェイのワークステーション・オブジェクトの作成

ここでは、鍵ネゴシエーションや暗号化に必要なオブジェクトを作成する方法を説明しま す。

最初に、GUIクライアントを管理ステーションであるosakaに接続します。接続されたら ら をクリックして、Network Objectsウィンドウを開きます。

次に[New]ボタンをクリックし、ドロップダウンリストからWorkstationを選択して、 Workstation Propetesを開き、FirewallServer(tokyo)のワークステーション・オブジェク トを作成します(ここではオブジェクト名をtokyoにしています)。

tokyoの設定内容は、すでにポリシーウィザードにより作成されているFirewallServer (osaka)のワークステーション・オブジェクトosakaと同様に、マシン名、IPアドレスを入 力して、TypeにはGatewayをチェックし、Modules InstalledのVPN-1 & FireWall-1に チェックしてください。

また管理ステーションであるosakaでは、Management Stationにチェック、Locationの設 定でInternalにチェックしてありますが、tokyoではManagement Stationにチェックせず Locationの設定でExternalにチェックしてください(下図参照)。

Workstation Properties	Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authentication	General Interfaces   SNMP   NAT   VPN   Authentication
Name: osaka	Name: tokyo
IP Address: 143.101.250.20 Get address	IP Address: 202.247.5.136 Get address
Comment: The Firewalled Gateway	Comment:
Color:	Color:
Location: Type: Type: C Host © Gateway	Location:
Modules Installed	Modules Installed
VPN-1 & EireWall-1 Version: 4.1  Get	✓ VPN-1 & EireWall-1 Version: 4.1 ▼ Get
FlgodGate=1 Version: 4.1	FloodGate=1 Version: 4.1
✓   <u>Management Station</u>	☐ [ <u>Management Station</u> ]
	OK ##57671

osakaのWorkstation Propeties

tokyoのWorkstation Propeties

#### ネットワーク・オブジェクトの作成

次に保護すべきosaka側のローカルネットワークとtokyo側のローカルネットワークのネットワーク・オブジェクトを作成します。osaka側のネットワーク・オブジェクトはすでに作 成されています(ウィザードにより作成される)ので、tokyo側のネットワーク・オブジェク トを作成します。

もし、osaka側のネットワーク・オブジェクトが作成されていない場合は、ここで作成して ください(ここでは、osaka\_local\_networkという名前でネットワーク・オブジェクトを作成 して、説明してあります)。

ネットワーク・オブジェクトの作成には、 <sup>9</sup>をクリックして、Network Objectsウィンド ウを開きます。

次に[New]ボタンをクリックし、ドロップダウンリストからNetwrokを選択して、Network Propetesを開き、tokyo側のプライベートネットワークのネットワーク・オブジェクトを作 成します(ここではオブジェクト名をtokyo\_local\_networkにしています)。またlocationは、 Externalにチェックしてください(下図参照)。

Network Properties	Network Properties
General NAT	General NAT
Name: [osaka_local_network] IP Address 172162.0 Net Mask: 255255255.0 Comment Color:	Name:         tokyo_local_network           IP Address:         172.16.1.0         Qet address           Net Mask:         255.255.255.0         Color:
Location: © Internal © External © Allowed © Disallowed	Location: Broadcast C Disallowed
OK キャンセル ヘルプ	OK キャンセル ヘルプ

osakaのプライベートネットワーク

tokyoのプライベートネットワーク

### 鍵ネゴシエーションの設定

鍵ネゴシエーションを設定します。

#### 暗号化ドメインの作成とネットワーク・オブジェクトの登録

ここでは暗号化対象のネットワークあるいはホストを登録する暗号化ドメイン(グループ)の 作成手順について説明します。

まず Mark Objects ウィンドウを開いてください。

次に[New]ボタンをクリックし、ドロップダウンリストからGroupを選択して、Group Propetesを開きosaka側の暗号化ドメインを作成します(ここでは、暗号化ドメインを osaka\_vpn\_groupとして作成しています)。

作成した暗号化ドメインに前述の「オブジェクトの作成」で作成したネットワーク・オブジェクトosaka\_local\_networkを選択し[Add]ボタンをクリックして、Not in GroupからIn Groupへ移動させてください(下図参照)。

同様にtokyo側の暗号化ドメインを作成し(ここでは、tokyo\_vpn\_groupとして作成しています)、前述の「オブジェクトの作成」で作成したtokyo側のネットワーク・オブジェクト tokyo\_local\_networkを登録します。

Group Properties	×	Group Properties	x
Name: osaka_vpn.group		Name: tokyo_vpn_group	
Comment		Qomment:	
Color:		Color:	
Not in Group:     In Group:       In Group: </td <td></td> <td>Not in Group: PDServer Social Costia Costi</td> <td>In Group: Add &gt; &lt; Bemove</td>		Not in Group: PDServer Social Costia Costi	In Group: Add > < Bemove
OK Cancel Help		ОК	Cancel <u>H</u> elp

osakaの暗号化ドメイン

tokyoの暗号化ドメイン

#### 暗号化ドメインの登録

ここでは、作成した暗号化ドメインを前述の「オブジェクトの作成」で作成したゲートウェイ に登録する方法を説明します。この登録により、FirewallServerに暗号化対象のネットワー クおよびホストを認識させます。

まず、前述の「オブジェクトの作成」で作成したゲートウェイosakaのWorkstation PropertiesウィンドウからVPNタブを開きます(下図参照)。

次にDomainでOtherを選択し、「暗号化ドメインの作成とネットワーク・オブジェクトの登録」で作成した暗号化ドメインosaka\_vpn\_groupを選択します。

tokyo側のワークステーション・オブジェクトも同様に暗号化ドメインtokyo\_vpn\_groupを 選択します。



osakaの暗号化ドメインの登録

tokyoの暗号化ドメインの登録

#### 認証方式の設定

ここでは、osakaとtokyoで行う認証方式の設定を説明します。(ここでは、IKEの場合を説 明します)

まずワークステーション・オブジェクトosakaのWorkstation Propertiesウィンドウから VPNタブを開きます。

次にEncryption schemes definedでIKEをチェックし、[Edit]ボタンをクリックし、IKE Propertiesウィンドウを開きます。

IKE Propertiesウィンドウでは、認証で使用される暗号方式やアルゴリズムを設定しますが、通常はSupport authentication methods以外はデフォルトのままにしておいてください(下図参照)。

Support authentication methodsは、Pre-Shared Secretにチェックしてください。 最後に[OK]ボタンをクリックし、IKE Propertiesウィンドウを閉じます。

Workstation Properties	x	
Workstein Properties         General Interfaces SNMP NAT Certificates VPN Authentication         Domain:       Encryption gchemes defined:         Disabled       Valid Addresses (of Interfaces)         © Qther:       Image: Supportable for SecuRemote         Egopatable for SecuRemote       Edit.         - Traffic Control Lorenne       Edit.		
Ium on Traffic Control Logging		
		×
	Support key exchange encryption with:	
OK キャンセル ヘルプ		
	✓       Pre-Shared Secret       Edit Secrets         ○       Public Key Signatures       Oonfigure         ○       VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)         ✓       Supports Aggresive Mode       ✓	

ワークステーション・オブジェクトtokyoも同様にWorkstation Propertiesウィンドウから VPNタブを開きます。

次にEncryption schemes definedでIKEをチェックし、IKE Propertiesウィンドウを開きま す。IKE Propertiesウィンドウもtokyoと同様に、通常はSupport authentication methods 以外はデフォルトのままにし、Support authentication methodsは、Pre-Shared Secret にチェックしてください。

tokyoでは、続けて[Edit Secrets]ボタンをクリックして、Shared Secretウィンドウ(下図) を開きます。Shared Secrets Listにosakaのワークステーションが表示されていますので、 ワークステーションを選択し、[Edit]ボタンをクリックします。次にShared Secretを入力 するテキスト・ボックスが表示されますので、入力して[Set]ボタンをクリックします。そ の後、Shared Secretウィンドウを終了させます。

ここで入力する文字列は6文字以上、英数字で4つ以上異なる文字を入力してください。 なお、入力する文字列にFireWall-1/VPN-1で使用する予約語は使用できません。予約語については付録Bを参照してください。

Share	d Secret		x
5 ا	Shared Secrets List: —		
	Peer Name	Shared Secret	
	osaka		<u>E</u> dit
			<u>R</u> emove
	Enter secret:	Set	
	Ok	Cance	el

以上で鍵ネゴシエーションの設定は終了です。続いてデータの暗号化方式について説明しま す。

暗号化の設定

暗号化の設定をします。

#### セキュリティポリシーの作成

ここでは、データを暗号化するルールの追加と暗号化方式の設定を説明します。

すでにウイザードにより作成してあった内部FTPサーバの接続を許可したルール3を変更して、tokyo側のネットワークからosaka側のネットワークへの通信を暗号化するルールを作成します。

ルール3のSourceカラムをtokyo側のネットワークオブジェクトとtokyoのワークステー ションオブジェクトへ、Destinationカラムをosaka側のネットワークオブジェクトへ変更し ます。Serviceカラムをftpサービスとし(例では変更なし)、ActionカラムをEncryptへ変更 します。

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	saka osaka	Any	(DROP) drop	Alert	Gateways	Any
2	network	) Any	InternetServices	accept	Long	Gw Gateways	Any
3	e tokyo_local_network	Be osaka_local_network	19 ftp	Encrypt	Long	Gateways	🔊 Any
4	Any	) Any	🔐 SilentServices	(DROP) drop		GW Gateways	🔊 Any
5	) Any	🕑 Any	) Any	(DROP) drop	Alert	Gateways	🕘 Any

#### 暗号化の設定

ルールのActionカラムのEncryptを選択して、ダブルクリックします。

Encryption PropertiesウィンドウのGeneralタブからIKEを選択して、[Edit]ボタンをクリッ クするとIKE Propertiesウィンドウが開きます。このウィンドウでは、ルールが適用される 接続を暗号化するのに使用するIPSec方式を定義します。

通常の場合、Allowed Peer Gateway以外は、デフォルトのままで問題ありません。 Allowed Peer Gatewayでは通信先のFirewallServerであるtokyoワークステーションを選択 してください。

Encryption Properties General Encryption schemes defined:  KE Manual IPSEC	×
	IXE Properties X General General Generation Generative
	Encryption Algorithm: DES エ Data Integrity MD5 エ Allowed Peer Gateway: 瞬 tokyo 「Use Perfect Forward Secrecy OK キャンセル ヘルプ

### セキュリティポリシーのインストール

最後に変更したルール有効にするため、 ₩ をクリックしてください。 以上で、osaka側の設定は終了です。

# リモートアクセスVPNの設定

SecuRemoteを使用することで、モバイルおよびリモートユーザーがインターネットに接続された企業 ネットワークへ安全にアクセスすることが可能になります。ここでは、下図のようにSecuRemoteと FirewallServer間(SR01-tokyo)で、VPN環境を構築する際の手順を簡単に説明します。このときの暗号化 方式はIKEを使用します。



## 設定手順の流れ

VPN構築手順は、以下の図に従って説明します。



## 前準備

次の順序に従ってセットアップの前準備をします。

### FireWall-1のセキュリティポリシーの設定

後述の「FirewallServerの設定」では、すでにFireWall-1の設定ができている環境に、VPNの 設定を追加する手順を示します。

#### GUIクライアントのセットアップ

GUIクライアントのセットアップについては、2章を参照してください。

#### ウィザードによるセキュリティポリシーの作成

ウイザードによるセキュリティポリシーの作成は、2章の「セキュリティポリシーの設定」を 参照してください。 ここでは、以下の条件で設定されていることを前提に話を進めます。

以下の条件下でウイザードにより作成されたセキュリティポリシーも併せて示します。

#### 設定内容

- 選択したRulebase Name: Starter Network
- firewallのオブジェクト名:
  - IPアドレス:
- 内部のネットワークオブジェクト名:
  - ネットワークアドレス:
  - ネットマスク:

) 許可するサービス:

tokyo

eth0(外側) 202.247.5.136 eth1(内側) 172.16.1.0

tokyo\_local\_network

172.16.1.0 255.255.255.0

ftp

No.	Source	Destination	Service	Action	Track	Install On	Time
1	🔊 Any	🔛 tokyo	Any	drop	Alert	Gateways	Any
2	tokyo_local_network	Any	InternetServices	accept	Long	Gateways	Any
3	le Any	Any	SilentServices	(DROP) drop		Gateways	Any
4	Any	🗩 Any	Any	drop	Alert	Gateways	Any

## SecuRemoteのダウンロード

リモートユーザーが暗号化通信を行うにはクライアントPCにSecuRemoteが必要です。 SecuRemoteはCheck Point 2000 CD-ROMにも収録されていますが、最新版をwebから ダウンロードして使用されることをお勧めします。 最新版のSecuRemoteは下記URLからダウンロードしてください。

#### http://www.checkpoint.com/techsupport/freedownloads.html

SecuRemote対応プラットフォームは以下のとおりです。

- Windows 95
- Windows 98
- Windows NT 4.0(SP4、SP5、SP6)
- Windows 2000

## FirewallServerの設定

最初に管理ステーションであるFirewallServer(tokyo)で、暗号化通信に使用する鍵をネゴシ エーションする方式とデータを暗号化する方式、およびユーザーをあらかじめ設定しておく 必要があります。設定を行うにはGUIクライアントを管理ステーションであるtokyoに接続 します。

### 暗号化方式の設定

暗号化通信に使用する鍵をネゴシエーションする方式とデータを暗号化する方式を設定します。

#### 暗号化ドメインの登録

GUIクライアントをtokyoに接続したら らをクリックして、Network Objectsウィンドウを開きます。

tokyo(ウィザードで作成済みのfirewallオブジェクト)を選択し、Workstation Properties ウィンドウを開きます。

DomainでOtherにチェックし、tokyo\_local\_network(ウィザードで作成済みの内部ネット ワークオブジェクト)をプルダウンメニューから選択します。tokyo\_local\_network宛の通信 が暗号化されます。

SecuRemoteからの接続を許可するには、Exportable for SecuRemoteをチェックします。 次にEncryption schemes definedでIKEをチェックし、[Edit]ボタンをクリックし、IKE Propertiesウィンドウを開きます。

Workstation Properties General Interfaces SNMP NAT C	Certificates VPN Authentication
Domain: © Disabled © Valid Addresses(of Interfaces) © Other: Tokyo_ypn_group	Encryption schemes defined:
Traffic Control Logging	
OK \$**	

#### 認証方式の選択

IKE Propertiesウィンドウの設定では、Support key exchange encryption with:と Support data integrity with:の設定はデフォルトのままで設定を変更する必要はありません。

Support authentication methods:では Pre-Shared Secretを選択します。[OK]ボタンを クリックし、IKE Propertiesウィンドウを閉じます。

IKE Properties	×
General	
Support key exchange encryption with: Support data integrity with: Support data integrity with: MD5 Support data integrity with: Support data integrity	
Support authentication methods:	
Pre-Shared Secret     Edit Secrets	
Public Key Signatures     Onfigure	
□ VPN-1 & FireWall-1 authentication for SecuRemote (Hybrid Mode)	
☑ Supports Aggresive Mode ☑ Support keys exchange for Subnets	
OK キャンセル ヘルプ	

### ユーザーの定義

ユーザーの設定をします。

#### ユーザーの作成

GUIクライアントで をクリックしUsersウィンドウを開いて、SecuRemoteを使用する ユーザーを登録します。

[NEW]ボタンをクリックしてDefaultを選択し、User propertiesウィンドウを開きます(下 図参照)。

Jsers			×
Users			
Show: All		-	
📿 Default			
1			
<u>N</u> ew	<u>R</u> emove	<u>E</u> dit	
			J
<u>C</u> lose	Install	<u>H</u> elp	

NameにSecuRemoteを使用するユーザー名(user\_tokyo)を入力してください。Expiration Dateにはこのユーザの有効期限を設定します。デフォルトでは、31-dec-2000となっていますので、必ず正しい有効期限を設定してください。

User Properties	x
General Groups Authentication Location Time Encryption	
Name: user_tokyo	
Comment	
Cojor:	
Expiration Date (dd-mmm-yyyy): 31-dec-2005	
OK 445270 1005	

#### ユーザの暗号化方式の決定

User propertiesのEncryptionタブを開き暗号化方式を選択します。ここではClient Encryption Methodsの中にあるIKEにチェックし、[Edit]ボタンをクリックし、IKE Propertiesウィンドウを開きます。

User Properties	×
General Groups Authentication Location Time Encryption	
Edit	
Successful Authentication Track:	
OK キャンセル ヘルプ	

#### ユーザーの認証方式・暗号方式の決定

まず、Authenticationタブで認証方式の設定を行います。

Select authentication schemes used: でPasswordにチェックしてパスワードを入力します。ここで入力する文字列は6文字以上、英数字で4つ以上異なる文字を入力してください。なお、入力する文字列にFireWall-1/VPN-1で使用する予約語は使用できません。予約語については付録Bを参照してください。

ここで入力したパスワード(プリシェアード・キー)を使用して、SecuRemoteユーザーを認 証します。

次にEncrptionタブをクリックし、暗号方式の設定をおこなってください。通常はデフォルトのままで変更する必要はありません。

設定が終わったら、[OK]ボタンをクリックして、IKE Propertiesウィンドウ、Users Propertiesウィンドウを閉じてください。

IKE Properties	IKE Properties
Authentication Encryption Select authentication schemes used	Authentication Encryption
I⊄ Password I	C Encryption + Data Integrity (ESP) C Data Integrity Only (AH) Data Integrity. C SHA1 C MD5 Encryption Algorithm: DES
 OK キャンセル ヘルプ	

#### ユーザーグループの作成とユーザーの登録

Usersウィンドウの[NEW]ボタンをクリックしGroupを選択してGroup Propertiesウィンドウを開きます。NameタブにSecuRemoteを使用するユーザーグループ名 (user\_vpn\_Group)を入力してください。

この項での説明で事前に作成したユーザー(user\_tokyo)がNot in Groupに表示されていますので、表示されているユーザーを選択し[Add]ボタンをクリックします。

選択したユーザーがIn Groupへ移動したことを確認したら、[OK]ボタンをクリックして、

Group Properties	×
<u>N</u> ame: user_vpr <u>C</u> omment Color:	LGroup
Not in Group:	In Group: Add > C Bemove
	OK Cancel <u>H</u> elp

Group Propertiesウィンドウを閉じます。

Usersウィンドウで、[Install]ボタンをクリックし、作成したユーザー・ユーザーグループを 有効にします。

Use	ers	×I
ſ	Users	
	Show: All	
	🕼 Default	
	😨 user_tokyo	
	🕵 user_vpn_Group	
	New <u>R</u> emove <u>Edit</u>	
	<u>C</u> lose Install <u>H</u> elp	

## プロパティの設定

GUIクライアントで 「をクリックしProperties Setupウィンドウを開き、Desktop Securityタブの設定を行います。SecuRemote:でRespond to Unauthenticated Topology Requests(IKE and FWZ)のチェックをはずします。

このオプションがチェックされている場合、SecuRemoteがサイト情報のダウンロードに失敗することがあります。

perties Setup		>
Authentication SYNDefender LDAP Encryption Security Policy Services Log and Alert S	ConnectControl Security Servers	
High Availability IP Pool NAT Access Lists D	esktop Security	
-SecuRemote:		
Respond to Unauthenticated Topology Requests (IKE and FWZ)		
Cache Static Passwords On Desktop		
Validation Timeout		
Desktop Does Not Invalidate		
O Desktop Invalidates Every 15 Minutes		
,,,,,,,		
Required Policy for All Decktops:		
Allow Outgoing Only	<b>*</b>	
- Desktop Configuration Verification Options:		
Desktop is Enforcing Required Policy		
Policy is Installed on All Interfaces		
Colv TCP/IP Protocols are Lised		
Configuration Violation Notification		
Notify Desktop Licer		
It Tous courte con		
OK キャンヤル ヘルプ		

### ポリシーの設定

ポリシーの設定をします。

#### セキュリティポリシーの作成

既存のセキュリティポリシーのルール1の下に暗号化ルールを追加します。 ルールのSourceカラムに事前にで作成したユーザーグループを追加し、Actionカラムで Client Encryptを選択します(下図のルール2)。

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	tokyo	Any	(DROP) drop	Alert	Gw Gateways	Any
2	🕵 user_vpn_Group@Any	network	19 ftp	Client Encrypt	Long	Gateways	🔊 Any
3	tokyo_local_network	Any	InternetServices	accept	Long	GW Gateways	Any
4	Any	🕑 Any	SilentServices	(DROP) drop		Gateways	Any
5	Any	Any	Any	(DROP) drop	Alert	GW Gateways	Any

#### セキュリティポリシーのインストール

最後に 〒をクリックして、作成したルールを有効にしてください。 以上でFirewallServer(tokyo)側の設定は終了です。

## SecuRemoteのインストール

クライアントPCにSecuRemoteをインストールする手順について説明します。

- 1. 「前準備」でダウンロードしたzipファイルを一時ディレクトリに展開し、展開されたディレクト リにあるsetup.exeを実行する。
- Welcome画面が表示されたら[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。必要に応じてフォルダを変更してく ださい。

4. インストール先のフォルダを確認したら [Next]ボタンをクリックする。

ファイルのコピーが開始されます。 デスクトップ・セキュリティ機能をイン ストールするか指定する選択画面が表示 されます。



 「Install SecuRemote without Desktop Security」を選択し、[Next]ボタンをク リックする。

SecuRemoteではデスクトップ・セキュ リティ機能はサポートしていませんので インストールしても使用できません。



6. どのアダプタにSecuRemoteをインス トールするかを指定する。

どちらを選択するかはシステム管理者に ご確認ください(この設定はインストール 後に変更可能です)。



7. 右のメッセージが表示されたら、 [Finish]ボタンをクリックして再起動す る。

新しい構成は、PCを再起動した後に有効 になります。



Setup has finished copying files to your computer. Before you can use the program, you must restart Windows or your computer.

Mes, I want to restart my computer now.
 C No, I will restart my computer later.

Remove any disks from their drives, and then click Finish to complete setup.

## SecuRemoteの設定

インストールしたSecuRemoteの設定をします。

## サイトの設定

SecuRemoteを使用して通信する前に、通信相手のサイト(tokyo)を定義する必要があります。

サイトの定義をするには、SecuRemoteがインストールされているPCがネットワークに接続されている必要があります。まずはネットワークに接続されているか確認してください。 次に下図のようなSecuRemoteのウィンドウからSitesメニューを開いて、Create Newを選 択するか、 愛をクリックしてCreate Net Siteウィンドウを開きます。

このウィンドウのNicknameにサイト名(tokyo)を入力し、Name/IPに解決可能なホスト名またはIPアドレスを入力します。サイトの情報を入力したら、[OK]ボタンをクリックします。

<u>کی</u> ۱	/PN-1 Se	cuRemo	ite				- 🗆 🗵	Create New Site		
Eile	⊻iew	<u>S</u> ites	Passwords	<u>T</u> ools	<u>C</u> ertificates	<u>H</u> elp		Vickname:	tokvo	_
Ê	10 6	Crea	te <u>N</u> ew					j∙ <u>n</u> ickname.	Juive	
								Name / IP:	202.247.5.136	
		Dele	te							
								OK	Cancel <u>H</u> elp	
Crea	te new s	ite								

## サイト情報のダウンロード

サイトの設定に間違いがなく、サイト側(tokyo)の設定が適切にされると、下図(左)のよう にサイト情報がダウンロードされ、[OK]ボタンをクリックすると定義したサイトのアイコン が作成されます(下図(右))。以上でSecuRemote(SR01)側の設定は終了です。

Update Site		x
Nickname:	tokyo	
IP:	202.247.5.136	
—Site Information ———		
Last Update:	Wed Oct 11 11:12:45 2000	
OK	Cancel <u>H</u> elp	
Click OK to save update	ed data.	

Ele View Sites Passwords Iools Certificates Help	å vi	PN-1 Se	cuRemo	ote				_ 🗆 🗙
	<u>F</u> ile	⊻iew	<u>S</u> ites	<u>P</u> asswords	<u>T</u> ools	<u>C</u> ertificates	<u>H</u> elp	
TC(SYO)	÷ô	<b>``</b> 6		<b>1</b> 5				
tosyo		1						
		tokyo						
For Help press F1	 For H	leln nres	s F1				_	

## SecuRemoteの使用方法

SecuRemoteを使用して暗号化通信を行うには、特別な手順は必要ありません。通常のアプリケーションの起動方法と同じです。

ただし、SecuRemoteクライアントが最初にサイトへの接続する場合(あるいはパスワードの有効期限が切れた場合)には認証が行われ、ユーザー名とパスワードを入力するダイアロ グボックスが表示されます。

ユーザーは自ユーザー名とパスワード(「ユーザーの定義」で設定したパスワード)を入力しま す。認証に成功すると以降の接続時にはダイアログボックスは表示されません。

VPN-1 SecuRemote Authentication		x
Secured by VPN-1 SecuRemote™	Please authenticate yourself tok	tosite: YO
	🔲 Use <u>C</u> ertificate	
	<u>U</u> ser name:	user_tokyo
	Password	
	C Enter password later	
	● Type in password now:	*okokokokokok
CHECK POINT"		
www.checkpoint.com	OK Ca	ancel <u>H</u> elp

# アドレス変換機器を介したVPN構築のための設定

VPN構成では、暗号化されたデータをIPプロトコル(プロトコル番号50番)のパケットにカプセル化して通信します。IPプロトコルであるため、IPアドレスのみが送信元を識別する識別子になります。このため VPNの各ノード(FirewallServerとSecuRemote)間にアドレス変換機器(ダイアルアップルータや、他の ファイアウォール)が入るケースではVPN通信が正しく行えない場合があります。

これは、送信元のアドレスが、1つのアドレスに変換されるため、戻りパケットの返送先をアドレスだけでは識別できないからです。通常、アドレス変換機機器はTCPやUDPのポート番号とIPアドレスと組み合わせて、送信元の識別に利用します。

したがって、このようなネットワーク構成でVPNを構築するには、IPプロトコルではなく、TCP、UDPを 使用する必要があります。これに対応するため、FireWall-1/VPN-1には暗号化されたデータをUDPのパ ケットにカプセル化して通信を行う方法があります。

以下に、その設定を方法を説明します。

## FirewallServer側の設定

/etc/fw/conf/objects.Cに以下の内容を追加してください。

```
:isakmp.udpencapsulation (
    :resource (
        :type (refobj)
        :refname ("#_CP_IPSec_transport_encapsulation")
    )
    :active (true)
)
```

修正が完了したら、マシンをリブートするか、fwデーモンの再起動をしてください。fwデー モンは以下のコマンドで、停止・起動ができます。

● 停止

# fwstop

起動

# fwstart

## SecuRemote側の設定

SecuRemote側では、FirewallServerからダウンロードするトポロジ(userc.C)ファイルを編集する必要があります。トポロジのダウンロードからその編集方法までを示します。

#### 1. トポロジのダウンロード

- ① メニューバーから[Sites]-[Create New]を選択
- ② Nicknameにチェックせず、Name/IP:にFirewall-1/VPN-1のサーバのIPアドレス(グローバルアドレス)を入力
- ③ [OK]ボタンをクリック

#### 2. SecuRemoteの終了

メニューバーの[File]-[Kill]でSecuRemoteを終了させる。

#### 3. トポロジの編集

- ① userc.C (通常はC:¥Program Files¥CheckPoint¥SecuRemote¥database¥にある)を編集
  - 修正1(以下の箇所に1行追加)



② Saveして編集終了

#### 4. SecuRemote の再立ち上げ

スタートメニューから、SecuRemoteを選択して立ち上げる。

上記作業は、最初にトポロジのダウンロードをしたとき(userc.Cが変更されたとき)のみに 必要な作業です。再度トポロジのダウンロードをしなければ、今後上記の作業を行う必要は ありません。

言い換えると、トポロジのダウンロードをするたびにトポロジの編集作業が必要になります。

~Memo~