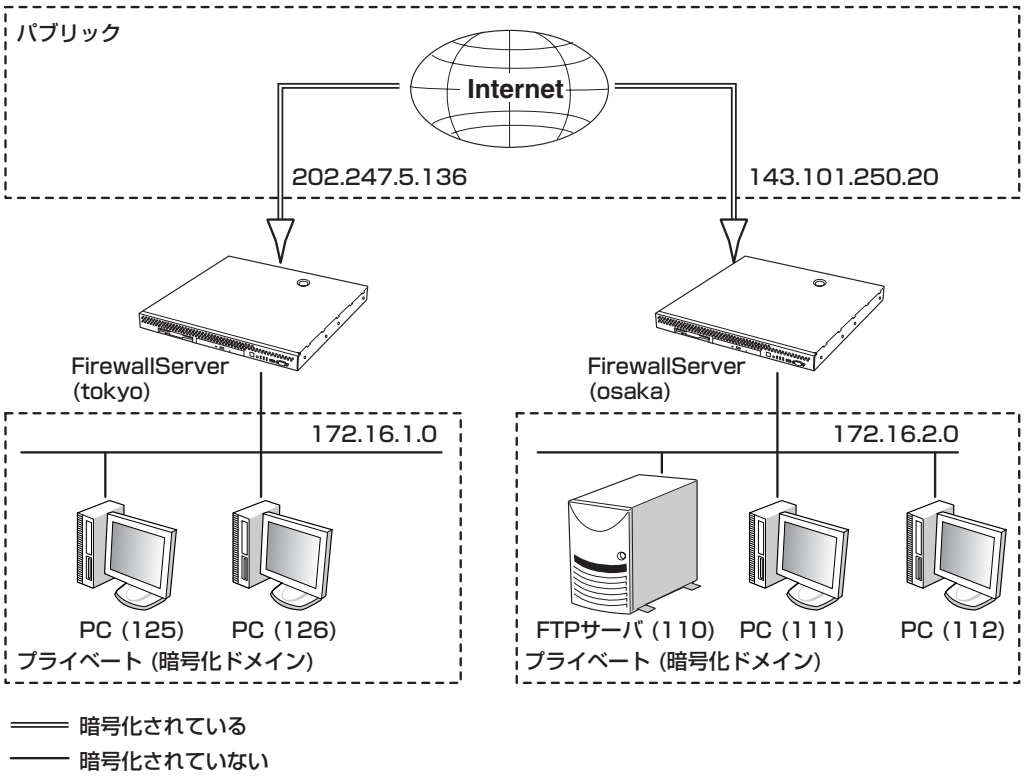
3 Virtual Private Network(VPN)

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。

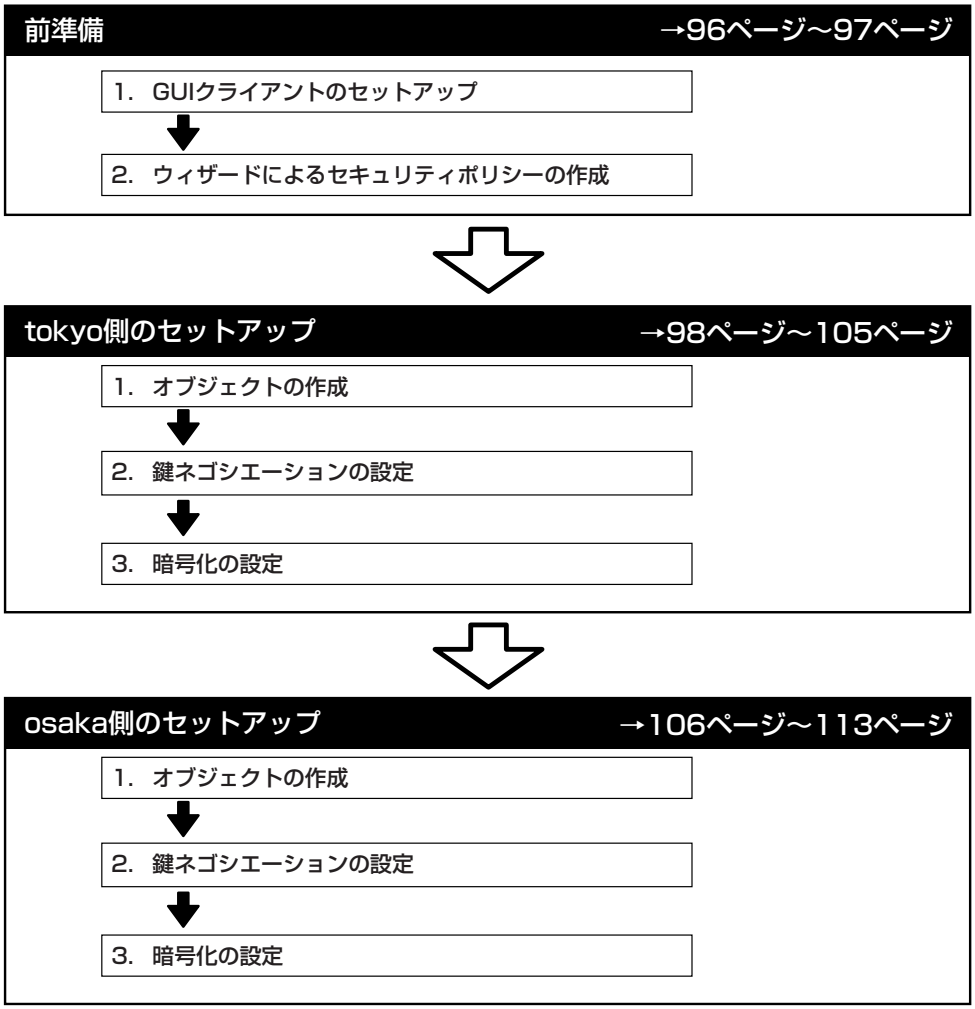
エクストラネットVPNの設定

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バーチャル・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**
  - ー 選択したRulebase Name: Starter Network
  - ー firewallのオブジェクト名: tokyo
    - □ IPアドレス: eth0(外側) 202.247.5.136
eth1(内側) 172.16.1.0
  - ー 内部のネットワークオブジェクト名: tokyo_local_network
    - □ ネットワークアドレス: 172.16.1.0
    - □ ネットマスク: 255.255.255.0
  - ー 許可するサービス: 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	Any	Any	SilentServices	drop		Gateways	Any
4	Any	Any	Any	drop	Alert	Gateways	Any

- **osaka側の設定**
  - ー 選択したRulebase Name: Publisher Network
  - ー firewallのオブジェクト名: osaka
    - □ IPアドレス: eth0(外側) 143.101.250.20
eth1(内側) 172.16.2.20
  - ー 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
  - ー 許可するサービス: ftp
  - ー 公開サーバオブジェクト名: FtpServer
    - □ IPアドレス: 172.16.2.110

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	osaka	Any	drop	Alert	Gateways	Any
2	osaka_local_network	Any	InternetServices	accept	Long	Gateways	Any
3	Any	FtpServer	ftp	accept	Long	Gateways	Any
4	Any	Any	SilentServices	drop		Gateways	Any
5	Any	Any	Any	drop	Alert	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。

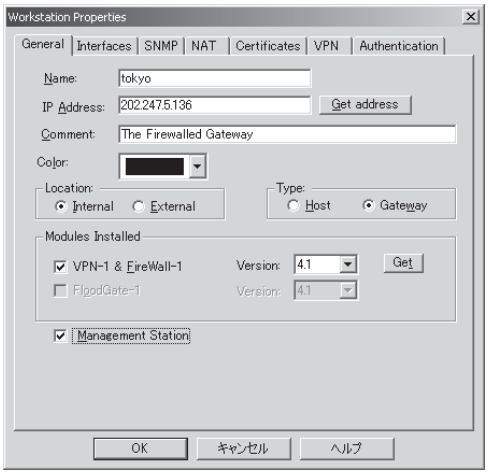
ゲートウェイのワークステーション・オブジェクトの作成

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tokyoに接続します。接続されたら をクリックして、Network Objectsウィンドウを開きます。

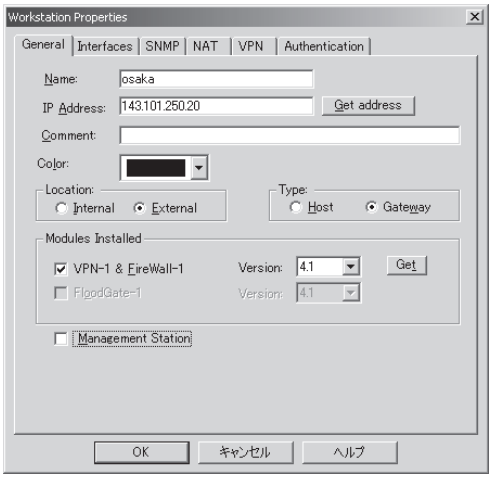
次に[New]ボタンをクリックし、ドロップダウンリストからWorkstationを選択して、Workstation Propetesを開きFirewallServer(osaka)のワークステーション・オブジェクトを作成します(ここではオブジェクト名をosakaにしています)。

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。



tokyoのWorkstation Propeties



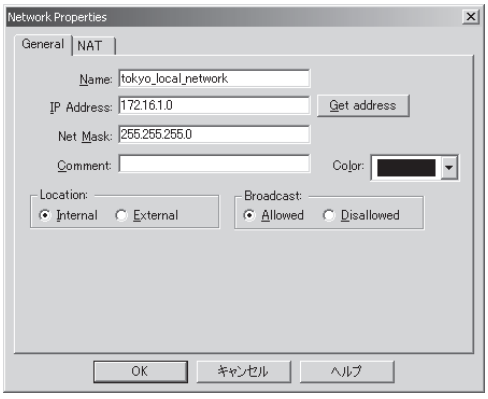
osakaのWorkstation Propeties

ネットワーク・オブジェクトの作成

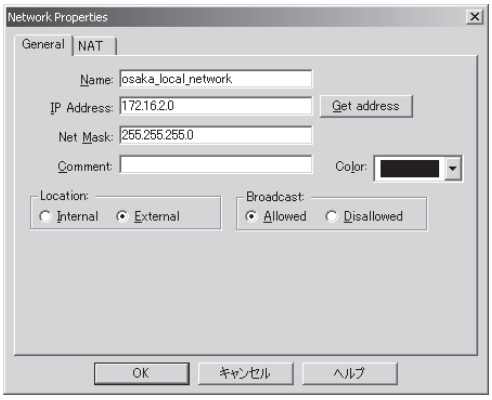
次に保護すべきtokyo側のローカルネットワークとosaka側のローカルネットワークのネットワーク・オブジェクトを作成します。tokyo側のネットワーク・オブジェクトはすでに作成されています(ウィザードにより作成される)ので、osaka側のネットワーク・オブジェクトを作成します。
もし、tokyo側のネットワーク・オブジェクトが作成されていない場合は、ここで作成してください(ここでは、tokyo_local_networkという名前でネットワーク・オブジェクトを作成して、説明しいます)。

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

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。



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。

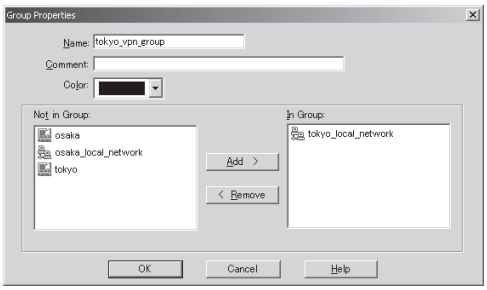
暗号化ドメインの作成とネットワーク・オブジェクトの登録

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。

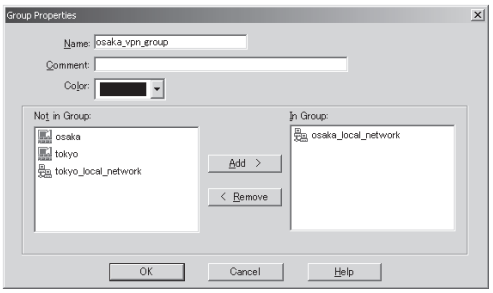
をクリックして、Network Objectsウィンドウを開きます。
次に[New]ボタンをクリックし、ドロップダウンリストからGroupを選択して、Group Propetesを開き、tokyo側の暗号化ドメインを作成します(ここでは、暗号化ドメインをtokyo_vpn_groupとして作成しています)。

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。



tokyoの暗号化ドメイン



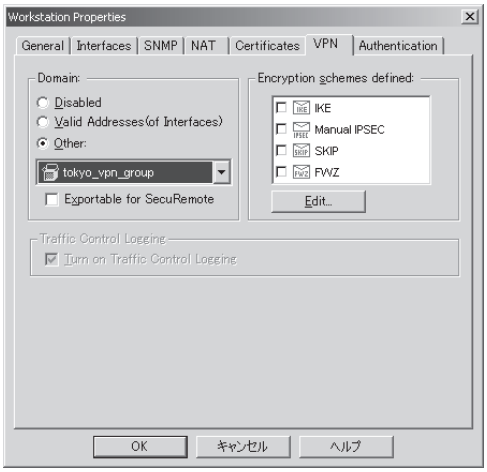
osakaの暗号化ドメイン

暗号化ドメインの登録

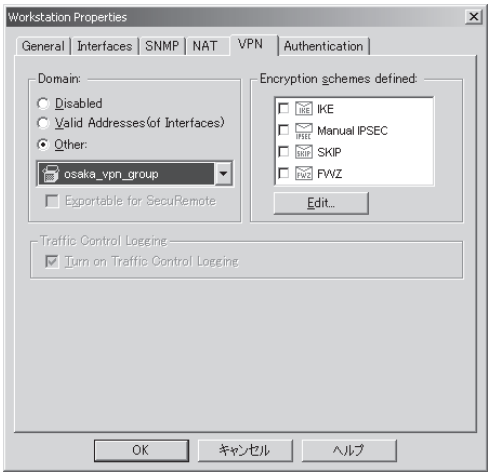
作成した暗号化ドメインを前述の「オブジェクトの作成」で作成したゲートウェイに登録する方法を説明します。この登録により、FirewallServerに暗号化対象のネットワークおよびホストを認識させます。

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

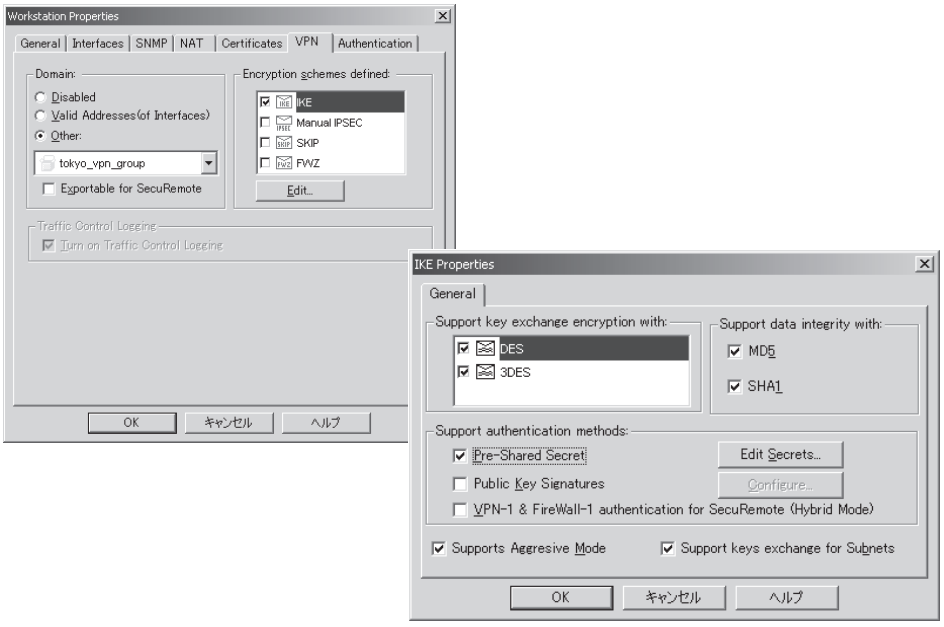
認証方式の設定

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。

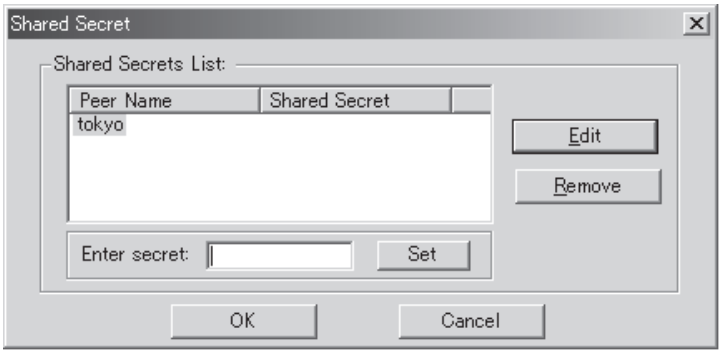


ワークステーション・オブジェクトosakaも同様にWorkstation Propertiesウィンドウから VPNタブを開きます。

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。



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

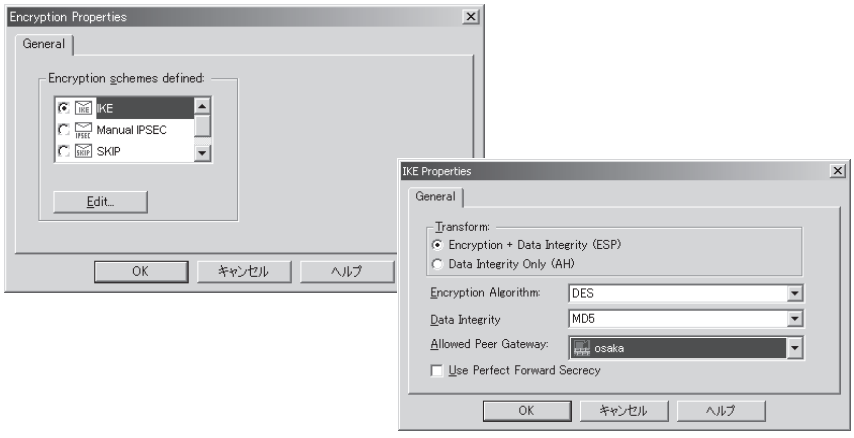
ここでは、データを暗号化するルールの追加と暗号化方式の設定を説明します。
ルール1の下に新しいルールを追加します。このルールのSourceカラムにtokyo側のネットワークオブジェクト、Destinationカラムにosaka側のネットワークオブジェクトを設定します。Serviceカラムはftpサービス、ActionカラムにEncryptを設定して、tokyo側のネットワークから、osaka側のネットワークへの通信を暗号化するルールを作成します（下図参照）。

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	tokyo	Any	drop	Alert	Gateways	Any
2	tokyo_local_network	osaka_local_network	ftp	Encrypt	Long	Gateways	Any
3	tokyo_local_network	Any	InternetServices	accept	Long	Gateways	Any
4	Any	Any	SilentServices	drop		Gateways	Any
5	Any	Any	Any	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。



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

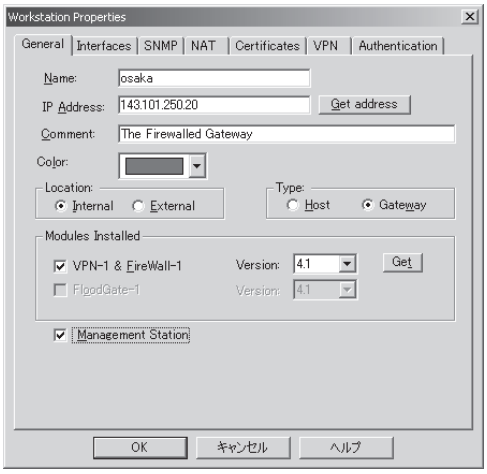
オブジェクトを作成します。

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

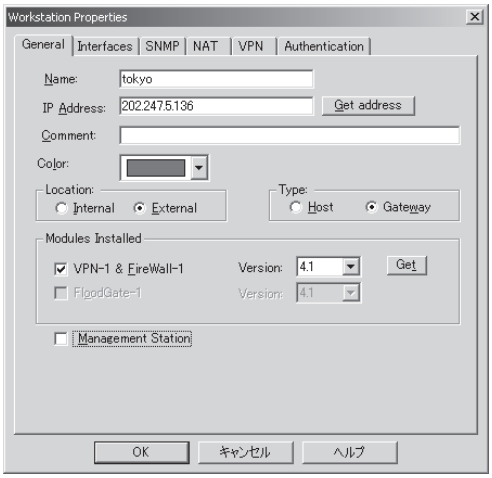
ここでは、鍵ネゴシエーションや暗号化に必要なオブジェクトを作成する方法を説明します。
最初に、GUIクライアントを管理ステーションであるosakaに接続します。接続されたら  をクリックして、Network Objectsウィンドウを開きます。

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)。



osakaのWorkstation Propeties



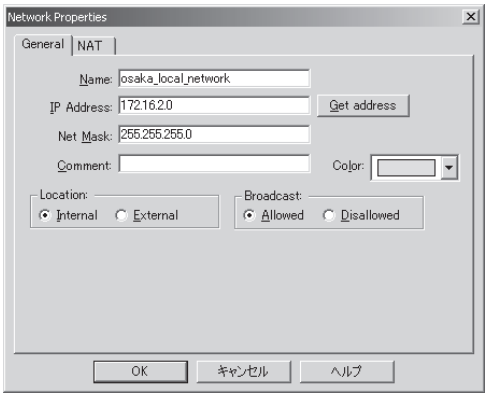
tokyoのWorkstation Propeties

ネットワーク・オブジェクトの作成

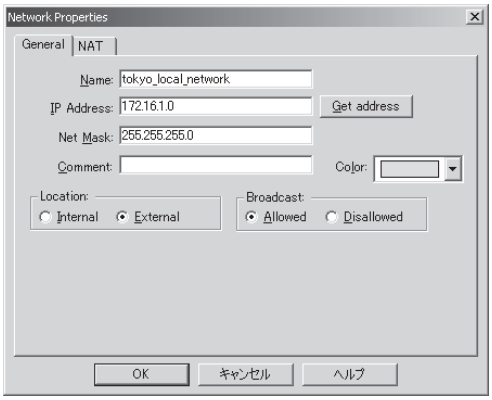
次に保護すべきosaka側のローカルネットワークとtokyo側のローカルネットワークのネットワーク・オブジェクトを作成します。osaka側のネットワーク・オブジェクトはすでに作成されています(ウィザードにより作成される)ので、tokyo側のネットワーク・オブジェクトを作成します。

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、  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)。



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

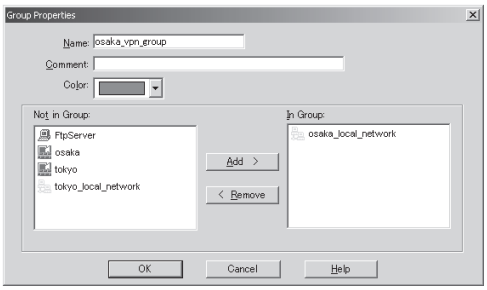
鍵ネゴシエーションを設定します。

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

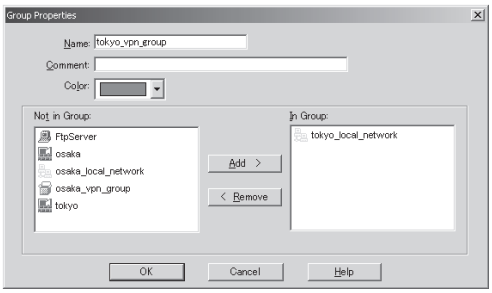
ここでは暗号化対象のネットワークあるいはホストを登録する暗号化ドメイン(グループ)の作成手順について説明します。

まず をクリックして、Network 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。



osakaの暗号化ドメイン



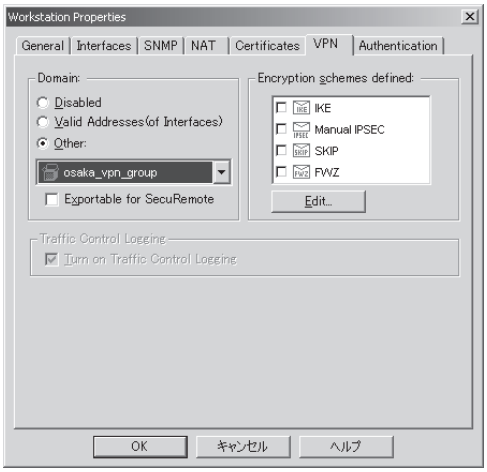
tokyoの暗号化ドメイン

暗号化ドメインの登録

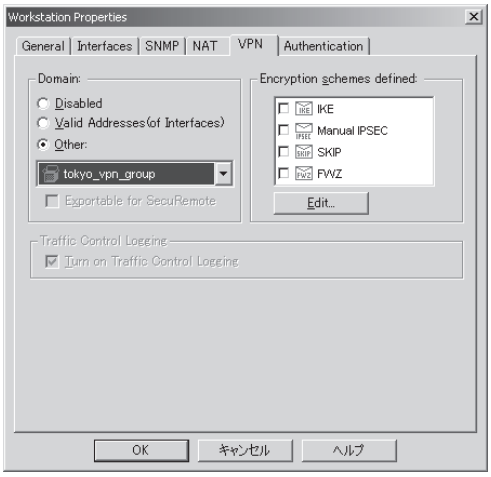
ここでは、作成した暗号化ドメインを前述の「オブジェクトの作成」で作成したゲートウェイに登録する方法を説明します。この登録により、FirewallServerに暗号化対象のネットワークおよびホストを認識させます。

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



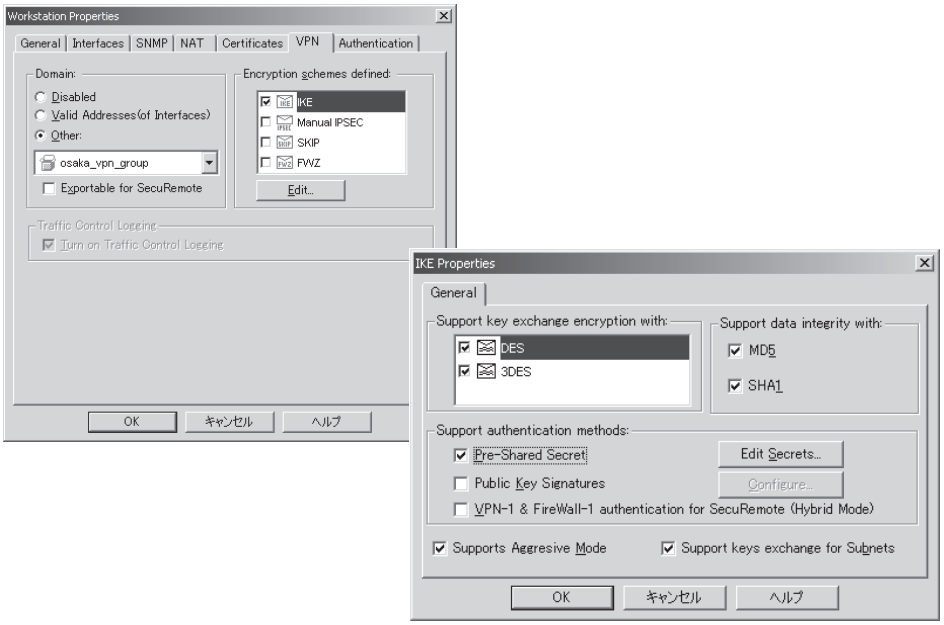
tokyoの暗号化ドメインの登録

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。

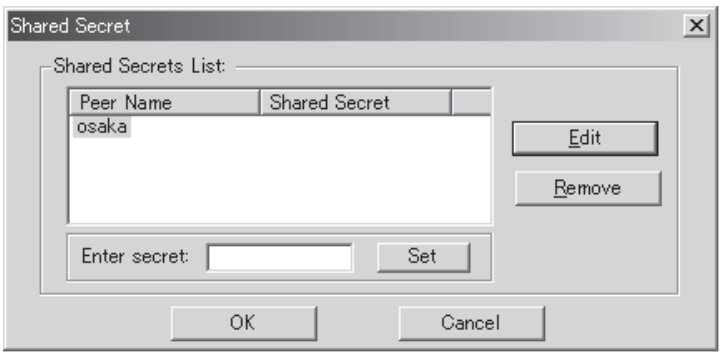


ワークステーション・オブジェクトtokyoも同様にWorkstation Propertiesウィンドウから VPNタブを開きます。

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。



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。

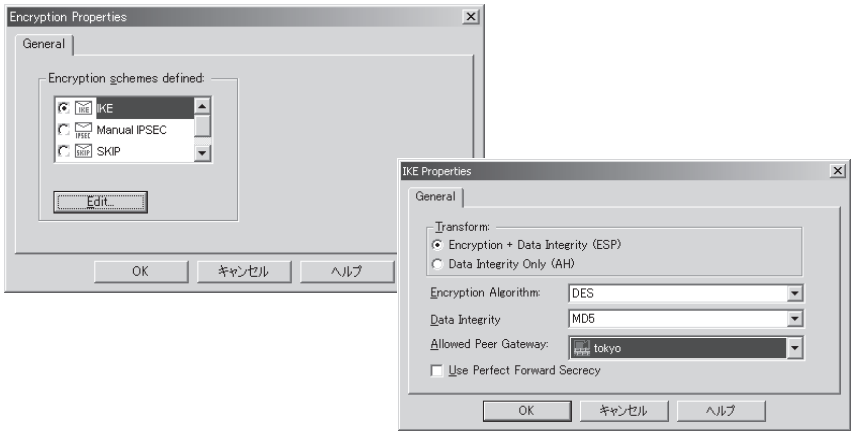
すでにウイザードにより作成してあった内部FTPサーバの接続を許可したルール3を変更して、tokyo側のネットワークからosaka側のネットワークへの通信を暗号化するルールを作成します。

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	osaka	Any	drop	Alert	Gateways	Any
2	osaka_local_network	Any	InternetServices	accept	Long	Gateways	Any
3	tokyo_local_network tokyo	osaka_local_network	ftp	Encrypt	Long	Gateways	Any
4	Any	Any	SilentServices	drop		Gateways	Any
5	Any	Any	Any	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。

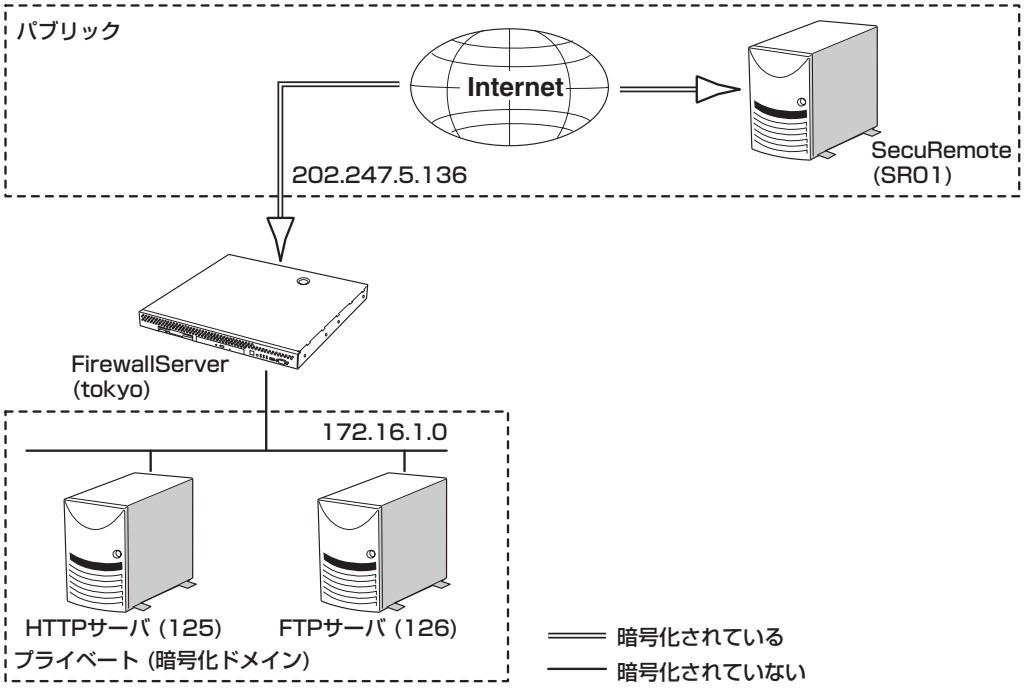


セキュリティポリシーのインストール

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。

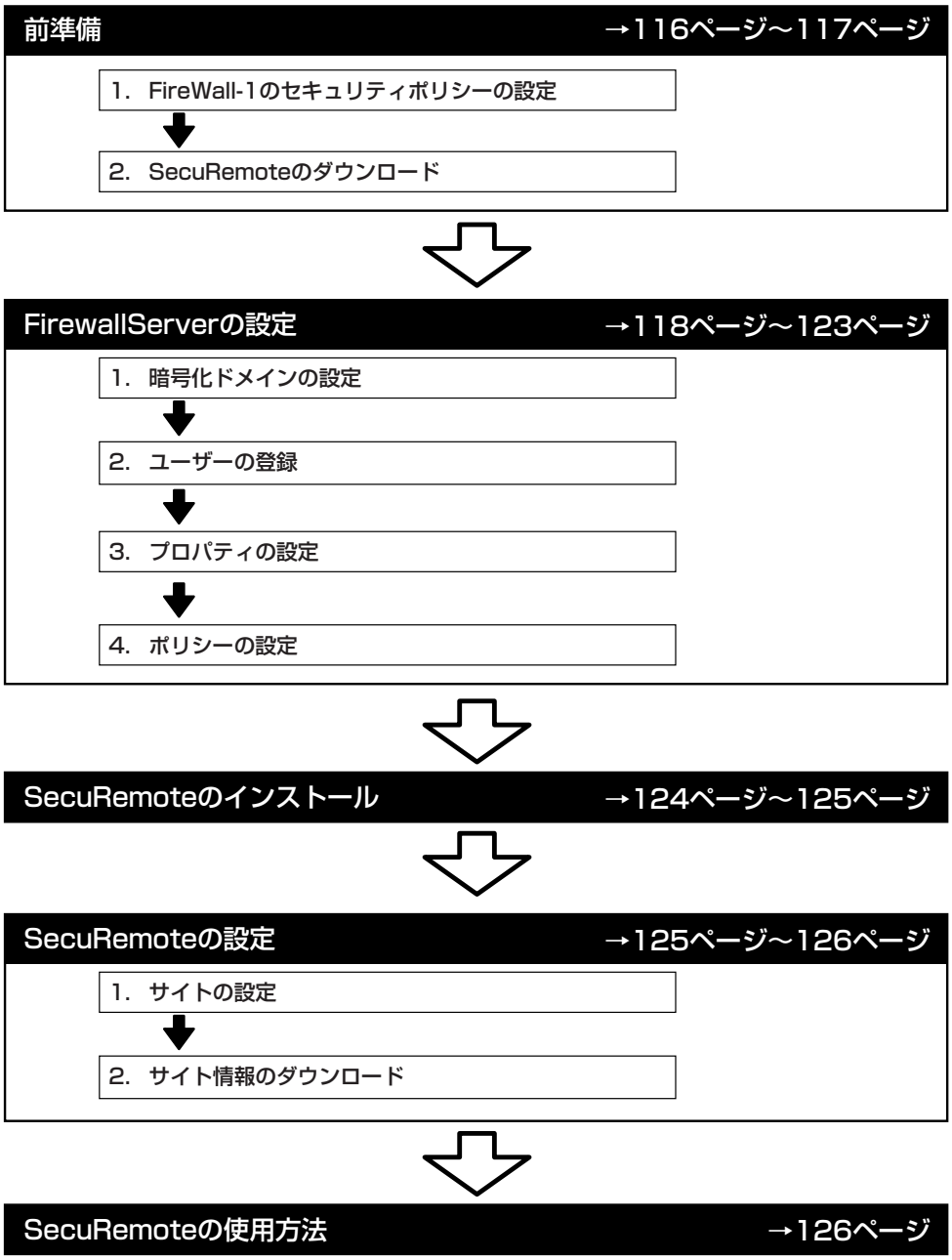
リモートアクセスVPNの設定

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: tokyo
  - IPアドレス: eth0(外側) 202.247.5.136
eth1(内側) 172.16.1.0
- 内部のネットワークオブジェクト名: tokyo_local_network
  - ネットワークアドレス: 172.16.1.0
  - ネットマスク: 255.255.255.0
- 許可するサービス: 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	Any	Any	SilentServices	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

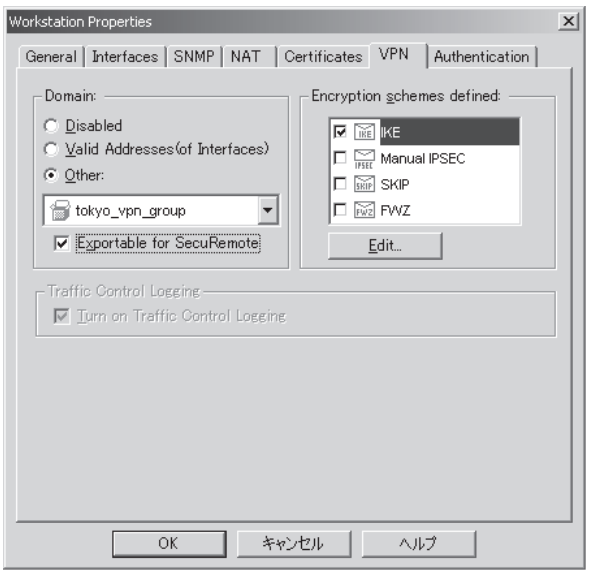
最初に管理ステーションであるFirewallServer(tokyo)で、暗号化通信に使用する鍵をネゴシエーションする方式とデータを暗号化する方式、およびユーザーをあらかじめ設定しておく必要があります。設定を行うにはGUIクライアントを管理ステーションであるtokyoに接続します。

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。

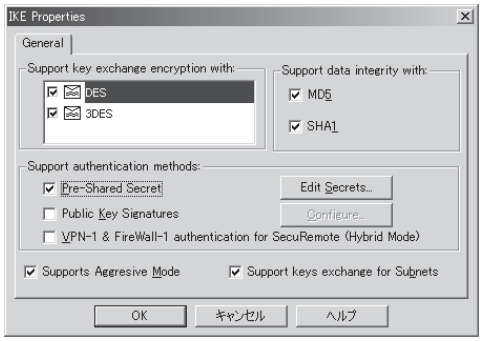
暗号化ドメインの登録

GUIクライアントをtokyoに接続したら 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。



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。

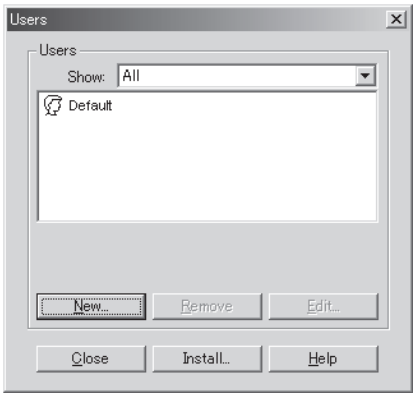


ユーザーの定義

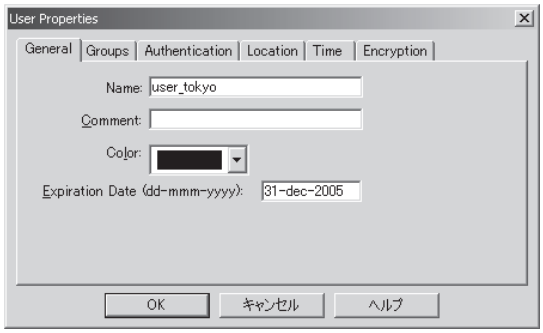
ユーザーの設定をします。

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)。

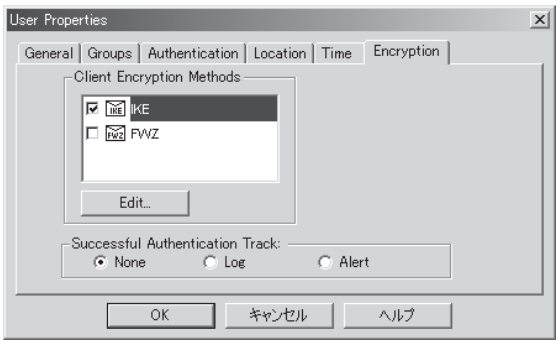


NameにSecuRemoteを使用するユーザー名(user_tokyo)を入力してください。Expiration Dateにはこのユーザの有効期限を設定します。デフォルトでは、31-dec-2000となっていますので、必ず正しい有効期限を設定してください。



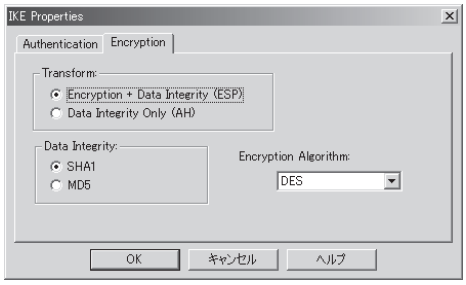
ユーザの暗号化方式の決定

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。



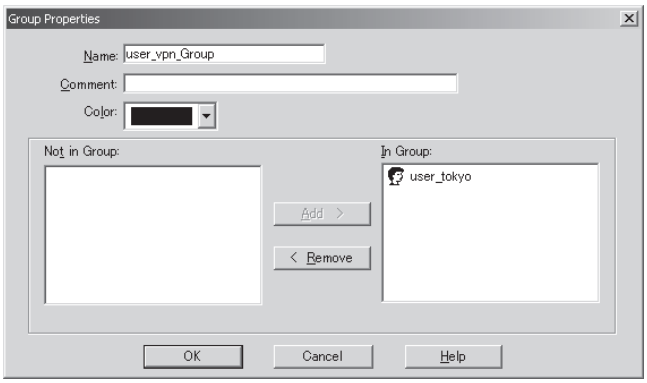
ユーザーの認証方式・暗号方式の決定

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。

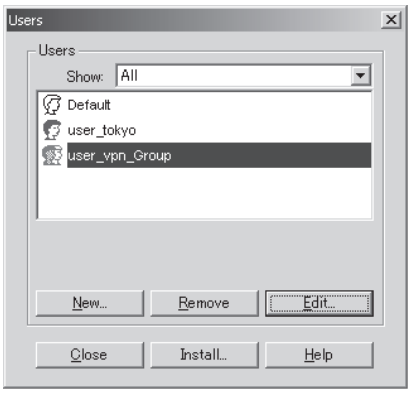


ユーザーグループの作成とユーザーの登録

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、

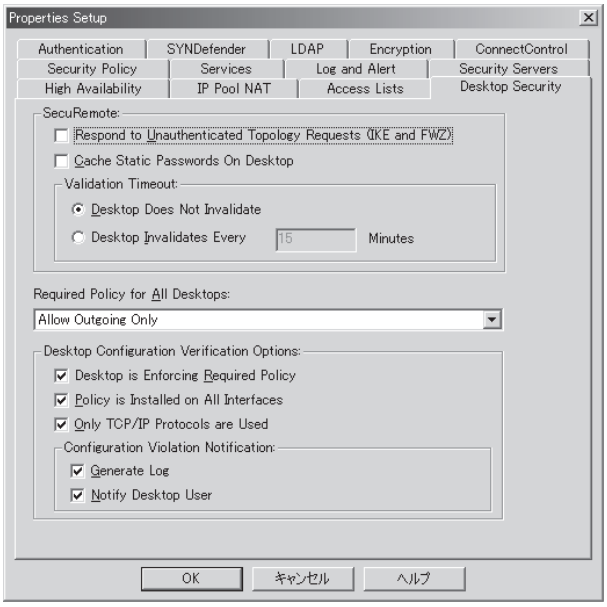


Group Propertiesウィンドウを閉じます。
Usersウィンドウで、[Install]ボタンをクリックし、作成したユーザー・ユーザーグループを有効にします。



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。



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	Alert	Gateways	Any
2	user_vpn_Group@Any	tokyo_local_network	ftp	Client Encrypt	Long	Gateways	Any
3	tokyo_local_network	Any	InternetServices	accept	Long	Gateways	Any
4	Any	Any	SilentServices	drop		Gateways	Any
5	Any	Any	Any	drop	Alert	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。

2. Welcome画面が表示されたら[Next]ボタンをクリックする。

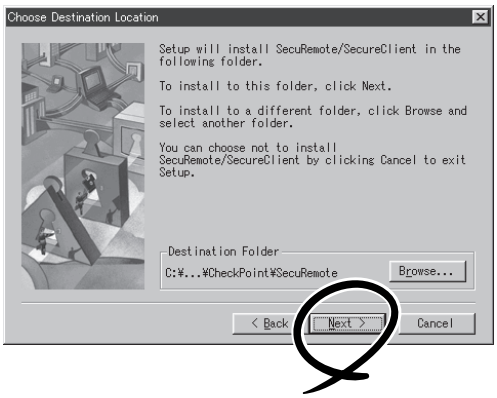
   使用許諾契約書が表示されます。

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。

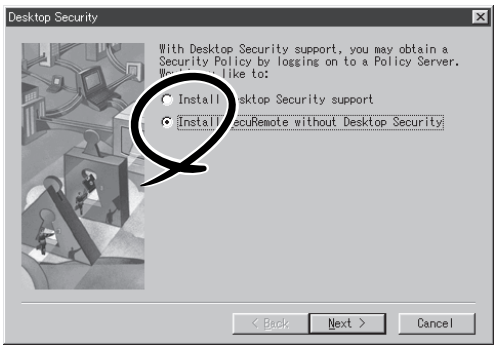
4. インストール先のフォルダを確認したら[Next]ボタンをクリックする。

   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。



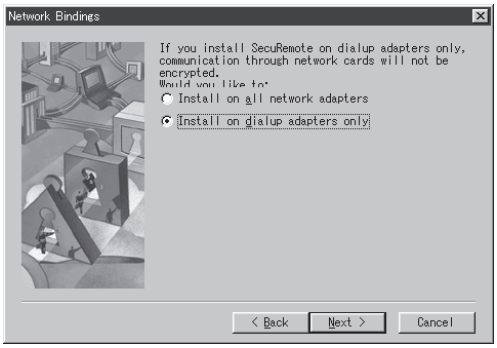
5. 「Install SecuRemote without Desktop Security」を選択し、[Next]ボタンをクリックする。

   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。



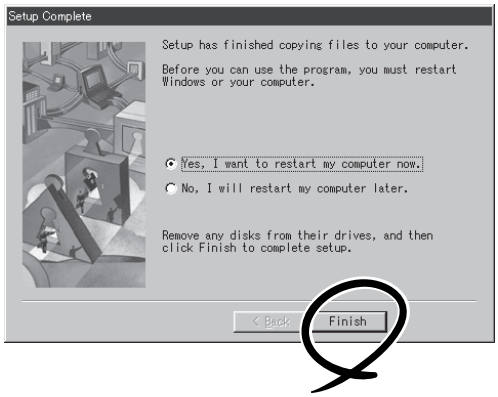
6. どのアダプタにSecuRemoteをインストールするかを指定する。

   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。

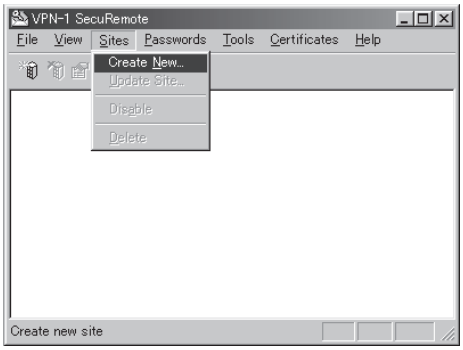


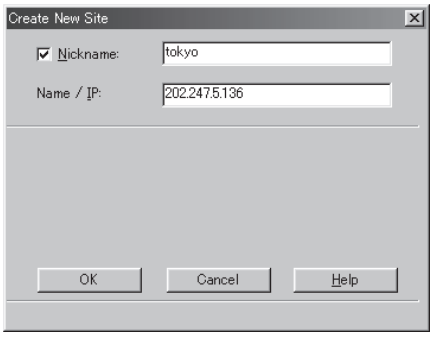
SecuRemoteの設定

インストールしたSecuRemoteの設定をします。

サイトの設定

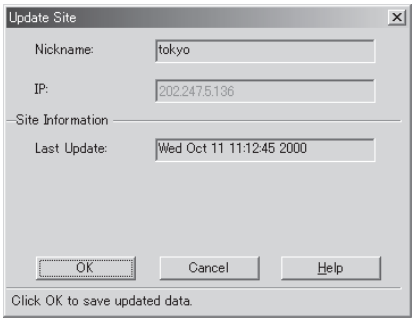
SecuRemoteを使用して通信する前に、通信相手のサイト(tokyo)を定義する必要があります。
サイトの定義をするには、SecuRemoteがインストールされているPCがネットワークに接続されている必要があります。まずはネットワークに接続されているか確認してください。
次に下図のようなSecuRemoteのウィンドウからSitesメニューを開いて、Create Newを選択するか、をクリックしてCreate Net Siteウィンドウを開きます。
このウィンドウのNicknameにサイト名(tokyo)を入力し、Name/IPに解決可能なホスト名またはIPアドレスを入力します。サイトの情報を入力したら、[OK]ボタンをクリックします。

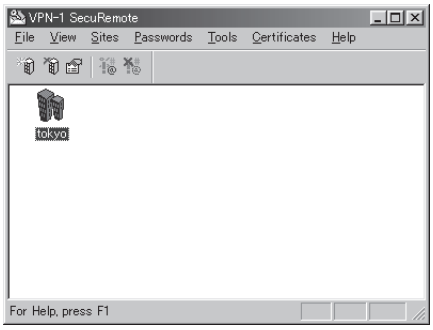




サイト情報のダウンロード

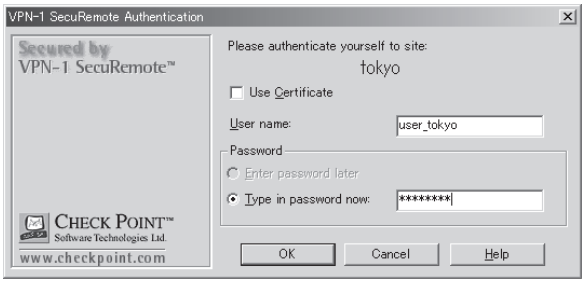
サイトの設定に間違いがなく、サイト側(tokyo)の設定が適切にされると、下図(左)のようにサイト情報がダウンロードされ、[OK]ボタンをクリックすると定義したサイトのアイコンが作成されます(下図(右))。以上でSecuRemote(SR01)側の設定は終了です。





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。



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

ー 修正1(以下の箇所に1行追加)

```
:options (
           :default_key_scheme (isakmp)
           :active_resolver (true)
           :slan_enabled (false)
           :use_cert (false)
           :force_udp_encapsulation (true)
```

この1行を追加する

ー 修正2 (以下の箇所をグローバルアドレスに変更)

ここに記載されているアドレスを控える

```
:gws (
           : (202.247.5.136.fws
                 :obj (
                       : (192.168.1.1)
                 )
```

ここを変更する(上記例だと、202.247.5.136)

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～