

**VPN  
Server**  
Suite

## Check Point® VPN-I™ Gateway to NetMAX VPN Server

Date: 11/8/00

**Version tested:** Check Point VPN-I Gateway running software version 4.1 Service Pack 2 (current release at the time of this writing)

### ***Conventions Used in This Document:***

Throughout this document, several conventions will be used in order to simplify the explanation and understanding of the procedure described herein.

Items that are to be input by the user are signified by using the Helvetica font. (e.g. localgateway)  
Such items often vary from installation to installation, and need to be replaced by the appropriate value when following this procedure unless otherwise specified.

Items that are presented by the Check Point FW-I software to the operator, such as menu items, and form field names, are signified in bold text. (e.g. Name:)  
These items have preset values and will appear in the Check Point FW-I software exactly as specified.

Some items appear in the Check Point FW-I software, but require user input, such as check boxes and lists. These items are signified by using both bold text and the Helvetica font. (e.g. 3DES).

## 1. Create Network Objects

---

### Step 1.1: Create Local Network Object

Open the Policy Editor

Manage -> Network Objects

New -> Network

Enter the following data in the General Tab:

*Name: localnet*

*IP Address: 192.168.1.0*

*Net Mask: 255.255.255.0*

*Location: Internal*

You may allow or disallow Broadcast here as well.

Click OK.

The screenshot shows the 'Network Properties' dialog box with the 'General' tab selected. The fields are filled with the following values: Name: localnet, IP Address: 192.168.1.0, Net Mask: 255.255.255.0, and Location: Internal. The Broadcast option is set to Disallowed. The dialog has OK, Cancel, and Help buttons at the bottom.

### Step 1.2: Create Local Gateway Object

New -> Workstation

Enter the following data in the General Tab:

*Name: localgateway*

*IP Address: 206.16.48.129*

*Location: Internal*

*Type: Gateway*

*Modules Installed: VPN-1 & Firewall-1: checked*

The screenshot shows the 'Workstation Properties' dialog box with the 'General' tab selected. The fields are filled with the following values: Name: localgateway, IP Address: 206.16.48.129, Location: Internal, and Type: Gateway. Under 'Modules Installed', 'VPN-1 & Firewall-1' is checked and 'FloodGate-1' is unchecked. The dialog has OK, Cancel, and Help buttons at the bottom.

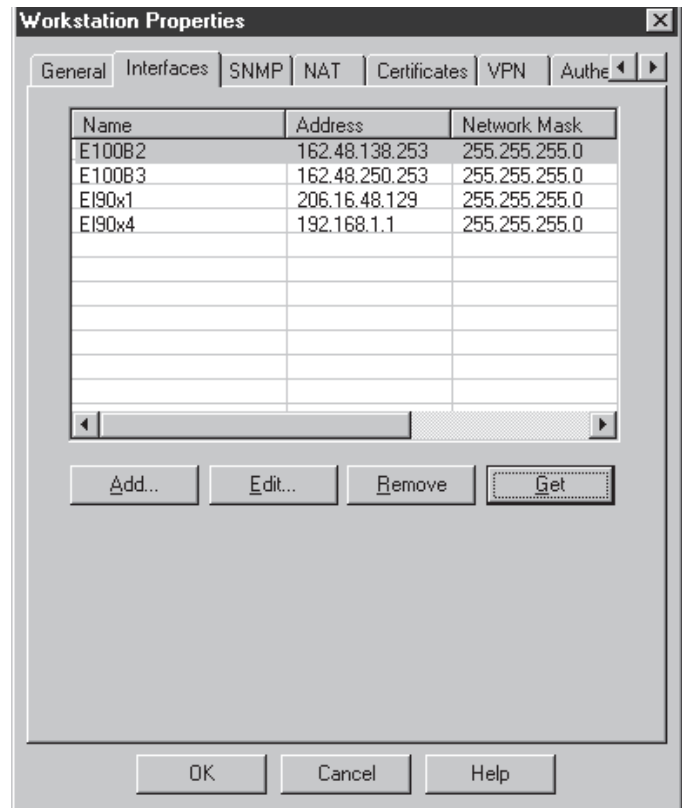
### Step I.3: Configure Interfaces for local gateway

Click the Interfaces Tab

Click Get.

If this does not detect your interfaces, manually add them using the Add button.

Click OK.



### Step I.4: Create Local Group Object

(Encryption Domain for Check Point side.)

New -> Group

Name: localgroup

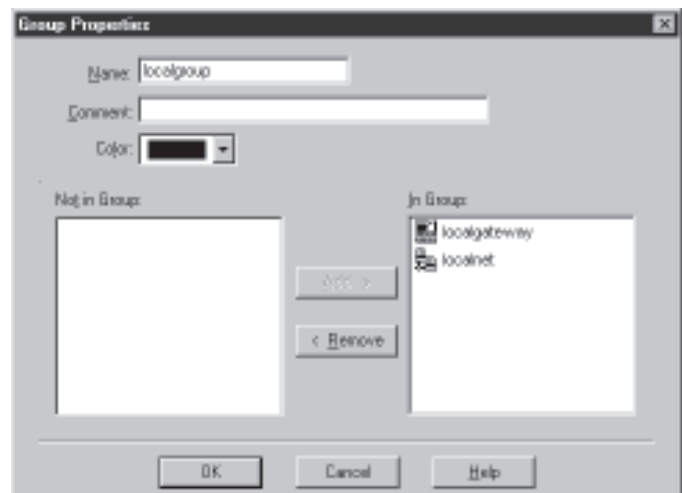
Select localgateway under Not in Group:

Click Add.

Select localnet under Not in Group:

Click Add.

Click OK.



### Step 1.5: Create Remote Network Object

New -> Network

Enter the following data in the General Tab:

*Name: remotenet*

*IP Address: 192.168.2.0*

*Net Mask: 255.255.255.0*

*Location: External*

You may allow or disallow Broadcast here as well.  
(OPTIONAL)

Click OK.

The screenshot shows the 'Network Properties' dialog box with the 'General' tab selected. The fields are filled with the following information:

- Name: remotenet
- IP Address: 192.168.2.0 (with a 'Get address' button)
- Net Mask: 255.255.255.0
- Comment: (empty)
- Color: (black)
- Location:  Internal  External
- Broadcast:  Allowed  Disallowed

Buttons at the bottom: OK, Cancel, Help.

### Step 1.6: Create Remote Gateway Object

New -> Workstation

Enter the following data in the General Tab:

*Name: remotegateway*

*IP Address: 206.16.48.1*

*Type: Gateway*

Click OK.

The screenshot shows the 'Workstation Properties' dialog box with the 'General' tab selected. The fields are filled with the following information:

- Name: remotegateway
- IP Address: 206.16.48.1 (with a 'Get address' button)
- Comment: (empty)
- Color: (black)
- Location:  Internal  External
- Type:  Host  Gateway
- Modules Installed:
  - VPN-1 & FireWall-1 (Version: 4.1) (with a 'Get' button)
  - FloodGate-1 (Version: 4.1)
  - Management Station

Buttons at the bottom: OK, Cancel, Help.

### Step 1.7: Create Remote Group Object

(Encryption Domain for NetMAX side.)

New -> Group

Name: remotegroup

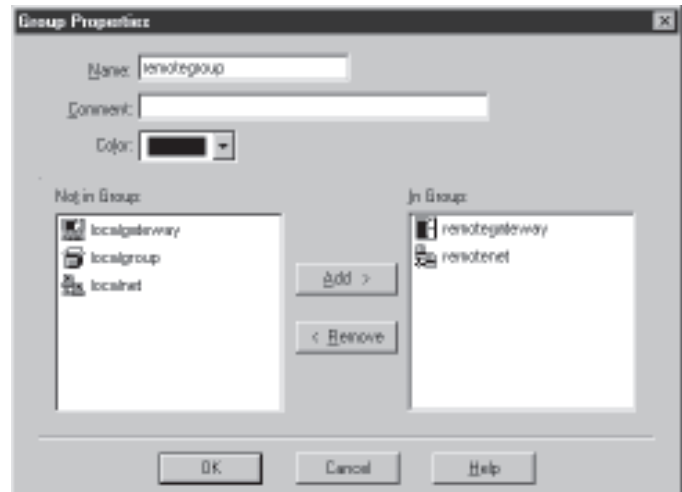
Select localgateway under Not in Group:

Click Add.

Select localnet under Not in Group:

Click Add.

Click OK.



## 2. Configure VPN Settings for Check Point

### Step 2.1: Modify Local Gateway properties

Double-click localgateway to return to Local Gateway Properties.

Click the VPN Tab.

Select Other: under

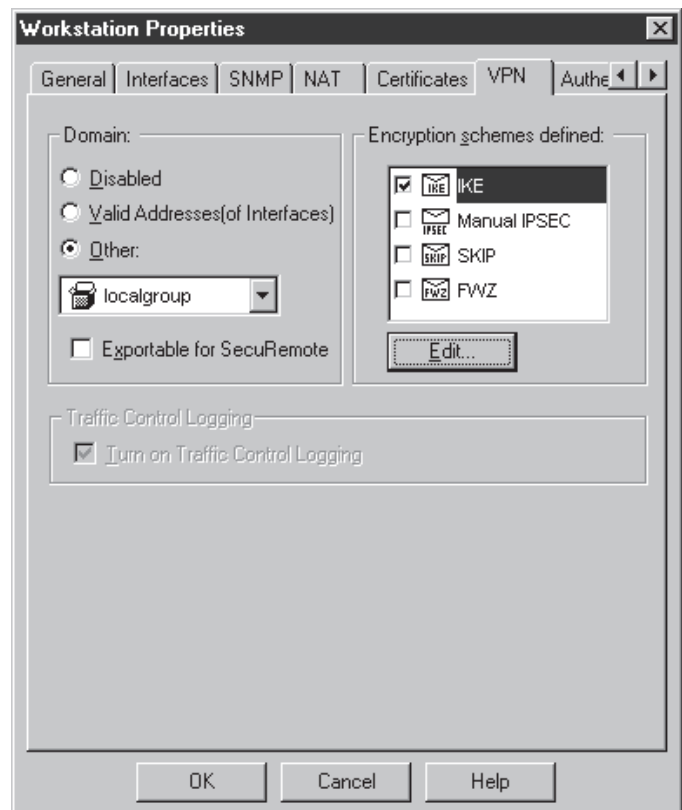
Domain:.

Select localgroup in the pulldown under

Other:.

Ensure that only IKE is checked under

Encryption schemes defined:



### Step 2.2: Configure IKE for Check Point

Click Edit.

Ensure that only 3DES is checked under

Support key exchange encryption with:

Ensure that only SHA1 is checked under

Support data integrity with:

Ensure that only Pre-Shared Secret is checked under

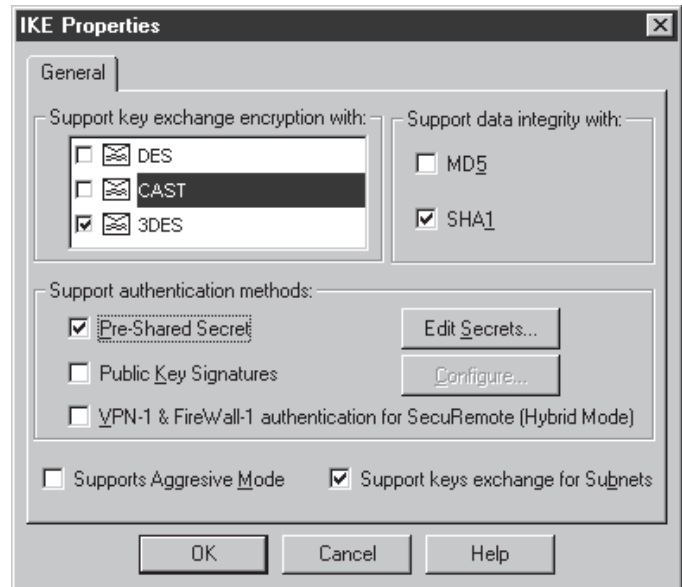
Support authentication methods:

You may check Support Aggressive Mode if the

Check Point will be using aggressive mode.

Ensure that Support keys exchange for Subnets is checked

to allow communication between subnets.



Click OK. (to close IKE dialog).

Click OK. (to close Workstation Properties dialog).

### Step 2.3: Configure VPN for NetMAX side

Double-click remotegateway to return to RemoteGateway properties.

Click the VPN Tab.

Select Other: under

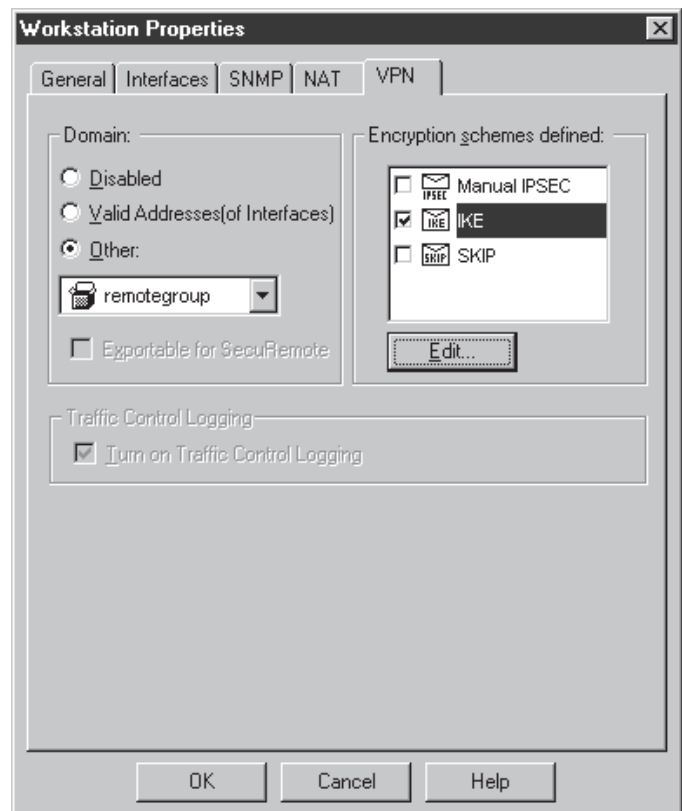
Domain:

Select remotegroup from the pulldown under

Other:

Ensure that only IKE is checked under

Encryption schemes defined:



### Step 2.4: Set up IKE for NetMAX side

Click Edit button.

Ensure that only 3DES is checked under

Support key exchange encryption with:

Ensure that only SHA1 is checked under

Support data integrity with:

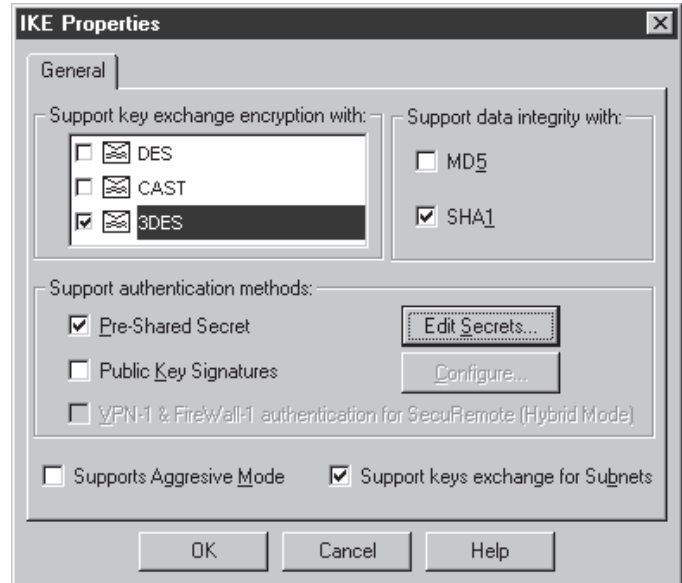
Ensure that only Pre-Shared Secret is checked under

Support authentication methods:

You may check Support Aggressive Mode if the NetMAX will be using aggressive mode.

Ensure that Support keys exchange for Subnets is checked

to allow communication between subnets.



### Step 2.5: Enter pre-shared secret for NetMAX

Click Edit Secrets button.

Select localgateway under Peer Name

Click Edit button.

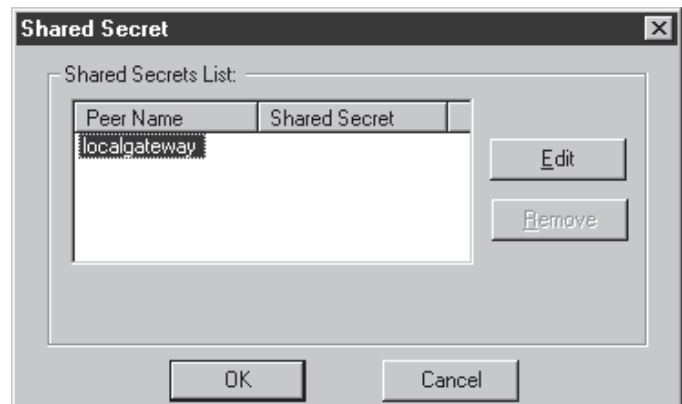
Enter the pre-shared secret.

Click Set button.

Click OK. (to close Shared Secret dialog)

Click OK. (to close IKE Properties dialog).

Click OK. (to close Workstation Properties dialog).



### 3. Configure Firewall and VPN Rules For Checkpoint

---

#### Step 3.1: Add rule to allow VPN between gateways.

Choose Edit -> Add Rule -> Top  
 if no rules are already defined, else Edit -> Add Rule  
 -> After  
 For Source add remotegateway and localgateway.  
 For Destination add localgateway and remotegateway.  
 For Service choose ISAKMP.  
 For Action choose accept.  
 For Track choose logging option (Long).  
 For Install On choose Gateways.  
 For Time choose Any.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	remotegateway localgateway	localgateway remotegateway	ISAKMP	accept	Long	Gateways	Any

#### Step 3.2: Add rule to allow VPN between subnets.

Edit -> Add Rule -> After  
 For Source add localgroup and remotegroup.  
 For Destination add remotegroup and localgroup.  
 For Service choose Any.  
 For Action choose Encrypt.  
 For Track choose logging option (Long).  
 For Install On choose Gateways  
 For Time choose Any.

No.	Source	Destination	Service	Action	Track	Install On	Time
1	remotegateway localgateway	localgateway remotegateway	ISAKMP	accept	Long	Gateways	Any
2	localgroup remotegroup	remotegroup localgroup	Any	Encrypt	Long	Gateways	Any

### Step 3.3: Set up options for Encryption Action.

Right-click the Encrypt Action icon.

Choose Properties.

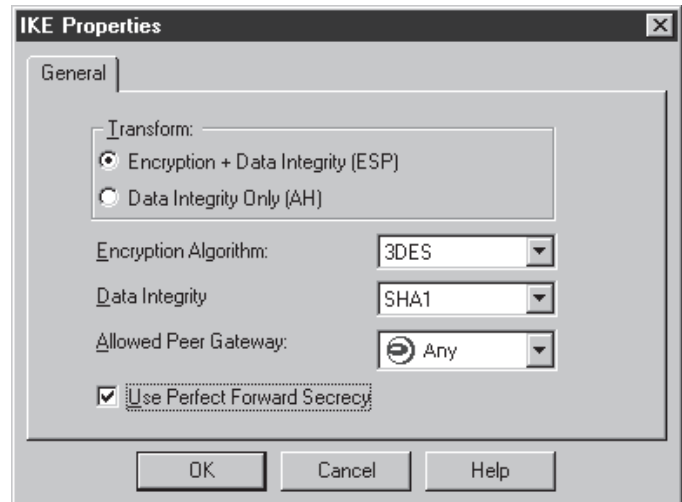
For Transform: select Encryption + Data Integrity(ESP).

For Encryption Algorithm: select 3DES.

For Allowed Peer Gateway: select Any.

Ensure that there is a check in Use Perfect Forward Secrecy.

Click OK.



### Step 3.4: Set up a rule to deny all services not specifically allowed by defined rules (OPTIONAL).



---

### Step 3.5: Setup IKE rekeying Intervals for Checkpoint.

Policy > Properties

Click Encryption tab.

Renegotiate IKE Security Associations every 5 minutes

Renegotiate IPSEC Security Associations every 120 minutes.

PLEASE NOTE: The values for renegotiation are specific.

Choosing a value other than those presented in this document

may result in your VPN not creating and maintaining connections

as expected, not working at all.

Do not check SKIP.

Click OK.

The screenshot shows the 'Properties Setup' dialog box with the 'Encryption' tab selected. The 'SKIP' section has the 'Enable Exportable SKIP' checkbox unchecked. The 'Change SKIP Session Key' section has 'Every' set to 120 seconds and 'Every or Every' set to 10485760 bytes. The 'Manual IPSEC' section has 'SPI allocation range (hex)' with 'From' set to 100 and 'To' set to ffff. The 'IKE' section has 'Renegotiate IKE Security Associations every' set to 5 minutes and 'Renegotiate IPSEC Security Associations every' set to 120 seconds. The dialog box has 'OK', 'Cancel', and 'Help' buttons at the bottom.