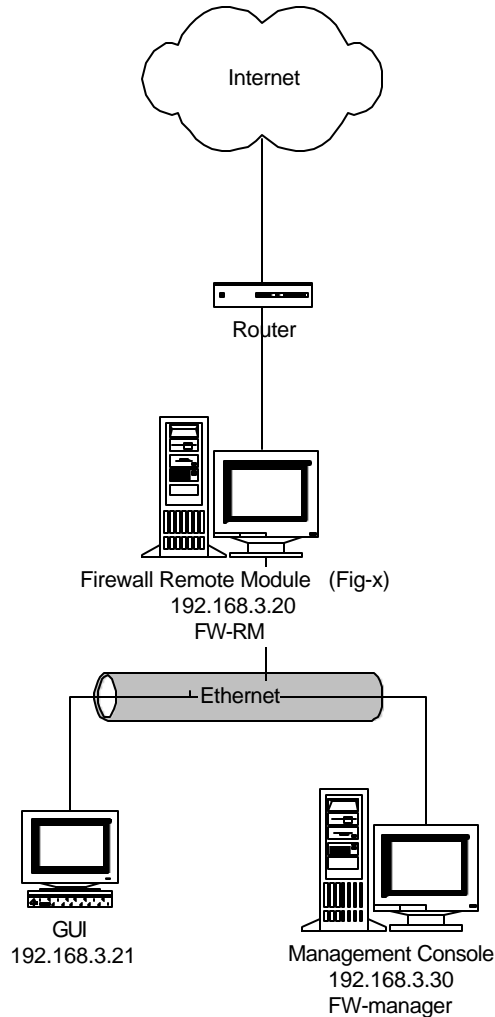


Check Point Software Technologies LTD.ä

*How to download a Security Policy to a FIG-x
from an existing Mgt. Station.
A Quick Reference*

**Area Technical Consultant for NJ
CheckPoint Software Technologies LTD. 
Date Published: January 21, 1999**

Downloading a Security Policy to a FIG-x from an existing Mgt. Station.



Environment:

Firewall Remote Module (FIG-x): Single Gateway Installation version 4.0 sp1

Management Console: Enterprise Center version 4.0 sp1

To install a Security Policy to a Single Gateway Firewall (FIG-x) from an existing Management Station, follow these steps;

- 1) Create / Modify the \$FWDIR/conf/masters file
- 2) Run "fwconfig" from the Management Station to "add a remote firewall module"
- 3) Create an object for the 'new' Remote Firewall Module on the Management Station
- 4) Stop the Firewall process on the Firewall Module and Management Station
- 5) Perform "fw putkey" on both the Remote Module and the Management Station
- 6) Start the Firewall process on the FireWall Module and the Management Station

These steps are explained in more detail in the remainder of this document.

On the Firewall Module manually create the following file;

Solaris

\$FWDIR/conf/masters

Windows NT

WINNT\fw\conf\masters

Note:

This file, \$FWDIR/conf/masters, contains the IP address (or resolvable name), of the FireWall-1 modules Management Station (or Master). FireWall-1 directs logging to the machine designated as Master, even if the Master is not itself a FireWalled gateway. To see a sample “masters” file, see the Trouble Shooting tips at the end of this document.

In our example this would be either 192.3.68.30 or “FW-manager”. If you are using the resolvable name it is best to make “FW-manager” an entry in the Remote Modules *hosts* file. Make sure that you can ping the host “FW-manager” from the Firewall Remote Module. To see a sample hosts file, see the Trouble Shooting tips at the end of this document.

- 1) From your existing FireWall-1 Management Console perform the following tasks;

NOTE:

If you do not have an Enterprise Management Console you will need to purchase one from your Check Point re-seller.

Solaris

Via the “fwconfig” menu

/etc/fw/bin/fwconfig

Select *Remote Modules* from the text menu

Answer “yes” to the question,

‘Do you want to configure Remote Modules (y/n) [n] ?’

Enter either a hostname or an IP address,

‘Please enter the list hosts that will be Remote Modules.

Enter hostname or IP address, one per line, terminating with CTRL-D or your EOF character.’

192.168.3.20

<CTRL>-D

Answer “yes” to the question,

‘Is this correct (y/n) [y] ?’

Next enter a secret key,

‘You will be prompted to use a secret key that will be used to authenticate the communication between this Management Station and the Remote Modules that you have selected.

*Enter secret key: ******

*Again secret key: *****’*

Note:

It is required that the ‘secret key’ you enter be identical on both the Management Console and Remote Module,

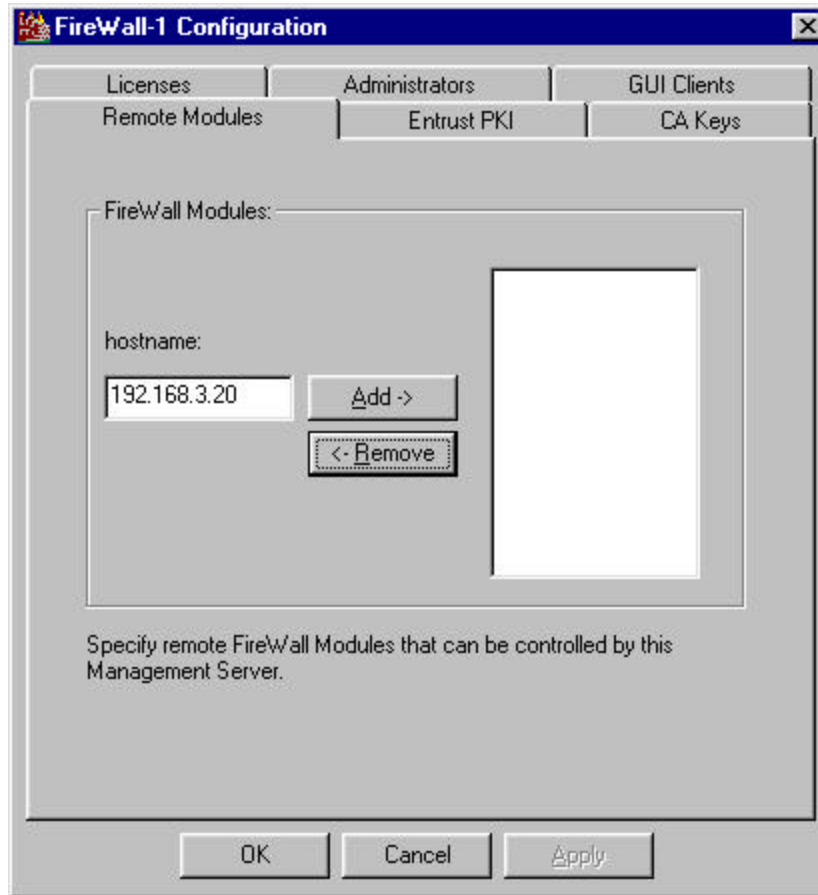
‘NOTE:

Do not forget to run ‘fw putkey’ with the same secret key on each of the configured clients.’

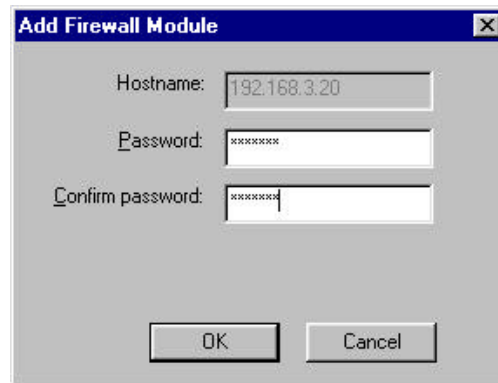
Windows NT

Via the FireWall-1 Configuration Menu

Select the Remote Modules TAB



In the 'hostname' field, enter the IP Address of the firewall module and click on 'Add->'
When prompted, enter a password for the Firewall Module.



Note:
The Password entered here MUST be the same as the 'Secret Key' entered on the Remote Module.

The FireWall will next ask you if it is OK to restart the FireWall service. Click on 'OK'.

- 2) On the Management Console (FW-Manager), create a new *Network Object* in the object database for the 'new' Remote Firewall Module.

Define the new Workstation Object as it was defined within the original FIG Management Console:

IP Address 192.168.3.20
Internal
Gateway
FireWall-1 Installed
Version 4.0

Your configuration may vary slightly.

- 3) At the command-line of the Remote Module, type the following string;

Solaris

```
$FWDIR/bin/fwstop  
$FWDIR/fw putkey <hostname> where hostname is 'FW-manager'  
Enter secret key: *****  
Again secret key: *****'
```

Note:

The 'secret key' entered here has to match the 'secret key' entered in step 2 for Solaris

FWDIR/bin/fwstart

Note:

When the firewall module starts, the following message should be displayed on screen:

```
Firewall-1: Starting fwd  
Firewall-1: Starting fwm (Remote Management Server)  
fwm: Firewall-1 Management Server is running  
  
Firewall-1: Fetching Security Policy from FW-manager localhost  
Trying to fetch Security Policy from FW-manager:  
  
Installing Security Policy Standard on all.all@FW-RM  
Fetching Security Policy from FW-manager succeeded  
Firewall-1 Started
```

Windows NT

```
WINNT\fw\bin\fwstop  
WINNT\fw putkey <hostname> where hostname is 'FW-manager'  
Enter secret key: *****  
Again secret key: *****'
```

Note:

The 'secret key' entered here has to match the password entered in step 2 for Windows NT

Re-boot the NT Server

- 4) At this point you will be able to install a Security Policy from the Management Console to the Remote Module.

Trouble Shooting Tips

1) Sample 'masters' file

Solaris

```
$FWDIR/conf/masters  
192.168.3.30
```

Windows NT

```
WINNT\fw\conf\masters  
FW-manager
```

2) Sample 'hosts' file

Solaris

```
/etc/hosts  
127.0.0.1          localhost  
192.168.3.30      loghost FW-manager  
192.168.3.20      FW-RM
```

Windows NT

```
WINNT\system32\drivers\etc\hosts  
127.0.0.1          localhost  
192.168.3.30      loghost FW-manager  
192.168.3.20      FW-RM
```

- 3) The "control.map" file on both the FireWall Module and Management Station defines access privileges and authentication measures for the control link between the FireWall Module and the Management Console. If you are having problems with access privileges or authenticating to the FireWall Module, you may want to see "control.map" in the FireWall-1 Architecture and Administration User Guide.