4 IP FireWall

Introduction

Alcatel's IP Firewall feature implements a subset of Check Point Software Technologies, Inc.'s Firewall-1™ network security product. Check Point's Firewall-1 software incorporates "stateful inspection" technology to provide comprehensive IP network security. Alcatel offers the IP Firewall feature as an optional feature for users who want to fully secure their IP network-based applications. Installing the IP Firewall feature on your switch eliminates the need for external, dedicated IP firewall servers, which usually run on UNIX- or PC-based platforms, for intercepting, interpreting, and filtering network traffic.

The IP Firewall feature allows your switch to act as a gateway to provide security for all data entering and exiting the switch from (and to) its attached physical ports, as well as *internally* between groups and VLANs defined in the switch. Every IP packet that is *routed* through the switch is inspected on both the input and output sides of the switch's internal router interface, thus allowing datagrams to be filtered between the VLANs in the switch. Only IP routed traffic can be protected by the firewall software; local network traffic is not examined by the firewall, therefore it cannot be filtered.

The following features are available in this release of Alcatel's IP Firewall Feature:

- A complete implementation of Check Point's Software Technologies "stateful inspection" virtual machine for IP data packet filtering.
- Full support of Check Point's event-logging and alert-generation features.
- Provision for secured communications, using Skey authentication, between the switch and the Enterprise Management Console (or EMC, which is described below).

Components of the IP Firewall

Two separate software components work together to provide Alcatel's IP Firewall feature:

- **Enterprise Management Console (EMC)**. Enterprise Management Console is Alcatel's own terminology which we use to refer to a single workstation that is running a licensed copy of Check Point's FireWall-1 software. (The types of workstations that support the EMC are listed inside the CD-ROM sleeve.) At least one EMC must exist in your network, although you may purchase additional licenses to provide redundancy. The EMC is used to create "policies" that are downloaded to the switch by the EMC. These policies contain the rules used by the IP Firewall software running in the switch to provide security.

♦ Terminology Note ♦

Alcatel coined the term "Enterprise Management Console" (EMC) for reasons of simplicity. Check Point's own terminology is much more specific. They use the term "Control Module" which refers to two separate software components: a "GUI Client" application and a "Management Server." Technically, our term EMC is synonymous with their term, "Management Server."

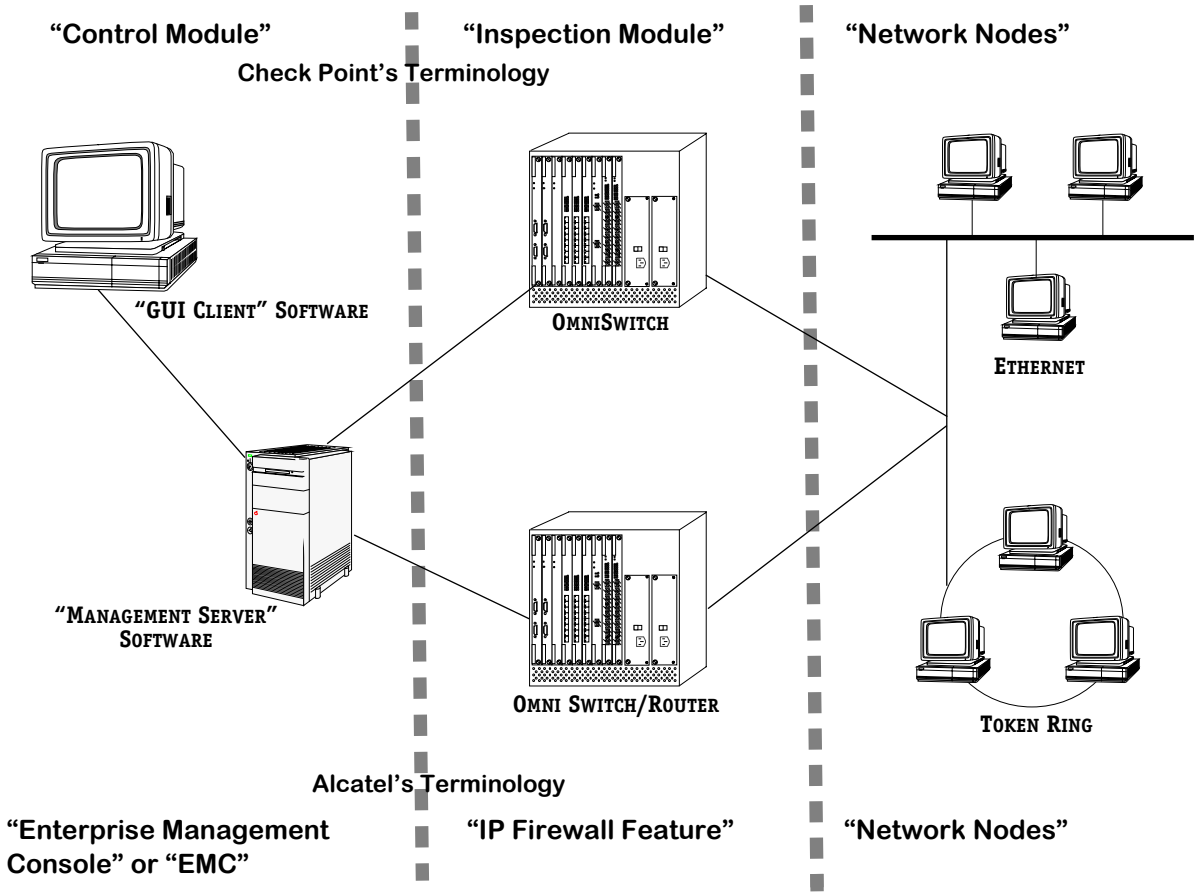
- **Alcatel's IP Firewall Software**. This is the software in the switch's flash memory that does the actual work of filtering network traffic. The switch enforces the rules contained in the policy downloaded by the EMC, logs events and generates alerts as specified by the

policy's rules, then forwards this information to the EMC where they can be displayed by the user. Check Point refers to this component as the "Inspection Module" which does the work of enforcing what they call the "Security Policy."

♦ Terminology Note ♦

A "Security Policy" which is made up of at least one "Rule Base." A Rule Base is a set of instructions that is used by the "Inspection Module" component to filter network traffic.

The following diagram illustrates the two components of the IP Firewall feature as well as showing the terminology used by Check Point and the corresponding Alcatel terminology.



Components of the IP Firewall Feature

Configuration Overview

Setting up the IP Firewall feature requires two major steps: configuring the Enterprise Management Console (EMC) and configuring the IP Firewall software running in the switch. Below is an outline of these two steps.

Step 1 is fully documented in the manuals provided by Check Point with their FireWall-1 product.

1. Set up the Enterprise Management Console. This step involves registering directly with Check Point the certification key on each CD-ROM you received, installing the EMC software on a workstation (see the CD-ROM's sleeve for a list of supported workstations), entering the license keys you obtained from Check Point, defining network objects (including the EMC and the switch which will run the IP Firewall software), creating a Rule Base that defines a "security policy" to control network traffic, and downloading the Rule Base you define to the switch.

   The above procedures are fully documented in the user manuals provided by Check Point with their FireWall-1 product. (There is an electronic version of the manuals on each Check Point CD-ROM; you may order printed manuals for an extra fee.) Although those procedures are *not* duplicated here, see *Troubleshooting Instructions* on page 4-10 for important help with licensing issues and other subjects.

2. Set up the IP Firewall software on the switch (see *Installing the Firewall Software* on page 4-4). After installing the software, configure the IP Firewall via the UI interface to the switch (see *Configuring the Firewall Software* on page 4-5). You *cannot* perform this configuration step using an SNMP client. Access to the firewall software in the switch is supported only through the switch's user interface (UI).

Interaction with Authentication Services

The IP Firewall feature and Authentication Services are two *separate* methods for increasing the security of a network. Authentication may be set up using the RADIUS or LDAP client in the switch, or Check Point's Authentication Management Console (AMC) software.

♦ Note ♦

The firewall and RADIUS or LDAP authentication may be enabled on the same switch at the same time.

The firewall and Check Point's AMC authentication feature *cannot* be enabled at the same time on the same switch, though they can coexist in the same network. The firewall software is actually firewall and AMC authentication software; see *Configuring the Firewall Software* on page 4-5 for details on selecting the desired operating mode. See Chapter 1, "Authentication Services," for more information on using and setting up your switch for AMC authentication.

Also, the EMC and AMC software may *not* reside on the *same* server.

Firewall and the HRE or HRE-X

The IP Firewall inspects all datagrams in software. This means that whenever IP Firewall is installed on the switch and enabled, the Hardware Routing Engine (HRE or HRE-X) is effectively disabled.

Firewall Software

If you order firewall software, you will receive a diskette with a firewall image file for the specific type of switch. Different files are required depending the chassis type.

Type of Switch	Required Image Files(s)
OmniSwitch	fwd.img
OmniStack	fw4.img
OmniS/R	fwx.img fpx.img

For an OmniS/R, two files are required, one for the firewall image (**fwx.img**) and one for the IP fastpath feature (**fpx.img**). The IP fastpath feature described in Chapter 29, "IP Routing," of the *OmniSwitch & OmniS/R User Manual*.

Installing the Firewall Software

Follow these steps to install the IP Firewall software on your switch:

1. First, make certain that you have the *correct* version of the IP Firewall software for the specific *type* of switch you are using. The disk media on which the IP Firewall software is distributed contains more than one version of the firewall image file (the versions are identified by different filenames as indicated in the table above). If you install the wrong version, the IP Firewall feature will not operate.

♦ Note ♦

Version 1.1 of the firewall software is Y2K-compliant.
Earlier versions of the software are not Y2K-compliant.

2. Install the correct version of the firewall image file from the disk media onto your switch (using the standard FTP or ZMODEM procedures) to install the software into the switch's flash memory.

3. If an existing version of firewall was previously installed on the switch, reboot the switch to make the new image active. A reboot is not necessary if this is the first firewall installation on the switch.

4. Proceed to configure the IP Firewall software (as described in the next section).

Configuring the Firewall Software

The software running in the switch that supports the IP Firewall feature is accessed using the **fwconfig** command. This command is also used to configure Check Point Authentication, which is described in Chapter 1, "Authentication Services." Both of these features provide a means of securing your network(s) and switch(es) and both are based on products licensed from Check Point Technologies, Inc. As described earlier in this chapter (see *Components of the IP Firewall* on page 4-1), the Check Point product that is related to the IP Firewall feature is called the "Enterprise Management Console," or EMC.

The switch software accessed by the **fwconfig** command can operate in *either* "Firewall" mode or in "Authentication" mode, but *not* in both modes simultaneously. This restriction means that in order to use both the IP Firewall and the Authenticated Groups software at the same time in a single network you must have at least two switches connected to the network (one switch operating in Firewall mode, the other in Authentication mode).

There are two steps involved in configuring the firewall/authentication software for the first time. Due to the design of the software, these steps are performed sequentially as follows:

1. Display the current configuration of the firewall/authentication software.
2. Enable the firewall by selecting the desired operating mode (in this case, Firewall) and by specifying the required configuration parameters. When configuration is completed, the firewall software will begin operating.

After you have completed the initial configuration, the firewall software may be modified as needed. For example, you may need to reset an Skey password or add a secondary management station. Some modifications, such as changing the IP address of an EMC, may require a reboot; the UI will display a prompt to reboot if one is necessary.

Step 1. Displaying the Firewall's Current Configuration

Follow the steps below to display the current configuration of the firewall software.

a. Enter **fwconfig**. (This command can be abbreviated to **fwc**.)

The following prompt displays:

```
View existing configuration? (y or n) (y) :
```

b. Enter **y** (or just press **<Enter>)** to display the existing firewall configuration.

Because the firewall is disabled at this point, a screen similar to the following displays:

```
Firewall/Authentication is Disabled

Primary manager's IP address = none

Secondary manager's IP address = none

Firewall's IP address = none

Time zone offset to UTC = 0 hours

Default switch interface mode = Open

Modify existing configuration? (y or n) (n) :
```

Because the software in this switch has never been configured before, the display shows that the Firewall is currently disabled (because this is the default mode) and that none of its parameters have been set. These parameters are explained fully in the steps below.

Step 2. Modifying the Firewall Configuration

a. The above prompt asks if you want to modify the existing configuration:

```
Modify existing configuration? (y or n) (n) :
```

Enter **y** to change the configuration.

b. The following prompt displays:

```
Change Firewall/Authentication state to Enable? (y or n) (n) :
```

Enter **y** to enable the software. Keep in mind that the firewall will *not* start operating until you have reached the end of these configuration steps.

c. The following prompt displays:

```
Enable:
  Firewall ------- f
  Authentication - a ? (f) :
```

This prompt asks if you want the software in the switch to operate in the Firewall mode or the Authentication mode. Remember, you can choose only *one* of these two modes at any given time. To switch between these two modes, you must first disable the software, reboot the switch, then re-enable the software in the desired operating mode.

d. The following prompt displays:

```
Change primary management station address? (y or n) (n) :
```

Enter **y** to change the IP address of the workstation to be used as your "primary" EMC. At least one EMC must communicate with this switch. The use of a secondary EMC (which is described below) is optional, and will require that you purchase a second EMC license.

e. The following prompt displays:

```
Enter primary management station IP address :
```

Enter the IP address of an existing EMC already configured for use with this switch (this was done when you configured the switch as one of the EMC's "remote modules"). Until you enter an IP address for an existing EMC, you will not be able to install (i.e., download) the policy (the "Rule Base") that you created on the EMC to the switch.

f. The following prompt displays:

```
Reinitialize primary's skey password? (y or n) (n) :
```

Enter **y** to proceed to enter the Skey password needed to connect to the primary EMC. Because this is your first-time configuration, you must enter **y** at this prompt.

g. The following prompt displays:

```
Enter skey password :
```

Enter the password that was previously specified for use with this switch (you entered a password for this switch when you configured the EMC's "remote modules"). Unless you enter the *exact* password here that the EMC *already* knows about, it will not be able to establish a communications link with the EMC.

Important Notes about Passwords

The password is automatically changed according to Skey algorithms after a selected number of transactions have occurred between the switch and EMC. Therefore, the current password *cannot* be displayed on the switch as it is continually being changed over time according to the Skey rules. The switch and EMC both maintain a copy of the password (in their respective configuration files), which is preserved between reboots. In most cases, you will have to enter the password only one time. However, if you should delete the switch's configuration file (**mpm.cnf**), you will have to re-enter a password on *both* the EMC and the switch.

h. The following prompt displays:

Change secondary management station address? (y or n) (n) :

Enter **y** to change the IP address of the workstation to be used as your "secondary" EMC. You can do so *only* if you have *actually* set up a second EMC. Using a secondary EMC provides redundancy in the event of a failure of the primary EMC. However, the use of a secondary EMC will require that you have at least two separate EMC licenses.

i. The following prompt displays:

Enter secondary management station IP address
(Hit <enter> to delete entry) :

Enter the IP address of an existing EMC (one that already "knows" about this switch).

j. The following prompt displays:

Reinitialize secondary's skey password? (y or n) (n) :

Enter **y** to proceed to enter the Skey password needed to connect to the secondary EMC.

k. The following prompt displays:

Enter skey password (Hit <enter> to delete entry) :

Enter the password that was specified for use with this switch (you "told" the EMC what password to use when you configured the EMC's "remote modules").

l. The next prompt that displays depends on whether or not the primary management station is on the same network as one of the switch router ports.

If the primary management station *is not located* on the same network, the user is prompted to select an address for the IP firewall from a list of IP router interfaces on the switch. For example:

The firewall is not configured with an interface to the primary manager's network.
Please choose the firewall's IP address from the list below:

1. 192.168.10.32
2. 192.202.181.32
3. 104.0.0.32

Enter the number corresponding to the IP address :

If the IP address of the primary management station *is located* on the same network as one of the switch's router ports, the switch assumes that router port's address should be

used in identifying the firewall to the EMC. The user is given an opportunity to configure a different address, but typically the default should be used. For example:

```
Change firewall's IP address 192.202.181.32? (y or n) (n) :
```

m. The following prompt displays:

```
Default switch interface mode is Open, change to Blocked? (y or n) (n):
```

This prompt asks you to specify the default switch interface mode which controls how IP routing operates in the switch during the (usually short) time between booting up and making a connection to the primary EMC. The "open" mode (which is the default) allows routing to operate normally just as if the firewall were not installed. The "blocked" mode disables all IP routing in the switch during the connection phase in order to isolate all VLANs. Routing is then resumed after the connection is made with the primary EMC.

Enter **b** for blocked or **o** for open. (Pressing **<Enter>** accepts the default option of "open.")

n. The following prompt displays:

```
Offset in hours from Universal Time (UTC or GMT; i.e., PST= -8, PDT= -7)
 (Hit <enter> to keep current value) :
```

This prompt asks you to enter a "time zone offset" which specifies the number of hours that must be added to, or subtracted from, *your* local time zone in order to match Universal Time Coordinates (UTC) or Greenwich Mean Time (GMT). The switch uses this parameter to enter the correct the timestamp on events, logs, and alert messages sent to the EMC. The range is plus 14 hours to minus 12 hours. The major time zones in the United States are all "*negative*" values: -8 (Pacific), -7 (Mountain), -6 (Central), and -5 (Eastern). You will only need to set this parameter if you want to normalize message logging on the EMC to UTC.

o. The following prompt displays:

```
Firewall configuration change successful.

fwdSpawn done! fwdTaskId = 0x48BDE620
```

The system prompt will then redisplay, and the IP Firewall feature will immediately become active.

p. To check the firewall configuration parameters you have just made, re-enter **fwconfig**.

A screen similar to the following displays:

```
Firewall is Enabled
    for Firewall only function

Running Xylan Firewall Version 3.2.1.31

Firewall policy installed : policy name is AllOK_fast

Primary manager's IP address = 192.202.181.66
    The state of the connection to this manager is : CONNECTED

Secondary manager's IP address = none

Firewall's IP address = 192.202.181.32

Time zone offset to UTC = -8 hours

Default switch interface mode = Open

Modify existing configuration? (y or n) (n) :
```

This screen display shows that the software is currently enabled in the "Firewall" mode. Also indicated are the version number of the installed software, the name of the policy

that was downloaded from the EMC (in this example it is "AllOK_fast"), the IP addresses of both the primary and secondary EMCs (if they were set), the state of the connection to each existing EMC, the firewall's IP address, the specified time zone offset of this switch from Universal Time Coordinates (UTC) (also known as Greenwich Mean Time), and the default switch-to-EMC interface mode specified for the switch.

Disabling the Firewall

Follow these steps to disable the firewall software in the switch.

1. Enter **fwconfig**.

   The following prompt displays:

   Modify existing configuration? (y or n) (n) :

   Enter **y** to change the configuration.

2. The following prompt displays:

   Change Firewall state to Disable? (y or n) (n) :

   Enter **y** to disable the firewall software.

3. The following prompt displays:

   Once you've disabled the Firewall, to re-enable it will require a reboot of the switch.
   Disable? (y or n) (n) :

   Enter **y** to verify that you want to disable the software.

4. The following message displays:

   Firewall configuration change successful.
   Firewall is now disabled.

   The system prompt reappears.

5. If you decide to re-enable the firewall without rebooting first, you will see this message:

   Firewall started once before, switch must be rebooted to start again.

   You will be allowed to re-enable the software only *after* the switch reboots. The reason for this restriction is that the software in the switch cannot establish a reliable connection to the EMC after it has been disabled. The rebooting of the switch allows the software to reinitialize its connection to the EMC properly.

Troubleshooting Instructions

Below are some instructions intended to aid you during the installation and initial setup phases of the IP Firewall feature. The subjects have been organized under general headings.

EMC Licensing Issues

- A separate license is required for each EMC and one for each switch that will run the firewall software (the firewall image, in Check Point terminology, is the *Firewall Module* or *Inspection Module*). This means that when you purchase IP Firewall software, you will receive at least *two* boxes, each containing a single Check Point FireWall-1 CD-ROM.
- Each CD-ROM contains a unique "Certificate Key" label pasted inside the sleeve that contains the CD-ROM. The certificate key is used to obtain "license strings" from Check Point. You must register each CD-ROM at the Check Point Internet web site (***http://license.checkpoint.com***). And, you must register *each* CD-ROM *separately*. Have *all* your certificate keys available when registering your software with Check Point.
- The Check Point CD-ROMs come packaged in boxes that identify them, but keep track of which CD-ROM is licensed for the EMC (the EMC's key activates unique features that apply only to it.) *On the CD-ROM sleeve next to the Certificate Key label write a note indicating that the CD-ROM corresponds to the EMC.* If you do happen to get the CD-ROMs mixed up, *and* you have failed to identify which one corresponds to the EMC, you will have to contact Check Point for help identifying your certificate keys.
- Install software on your EMC workstation *only* from the CD-ROM that came in the box designated for the EMC.
- Any other CD-ROMs you received (i.e., one for each switch license) must be registered, but you do not have to install software from them on your switch(es). The firewall image that is loaded on the switch is contained in the **fwd.img**, **fw4.img**, or **fwx.img**/**fpx.img** files described in *Installing the Firewall Software* on page 4-4. In Check Point's terminology, the firewall image is the Inspection Module. Registering the certificate key for the switch gives you an Inspection Module license.

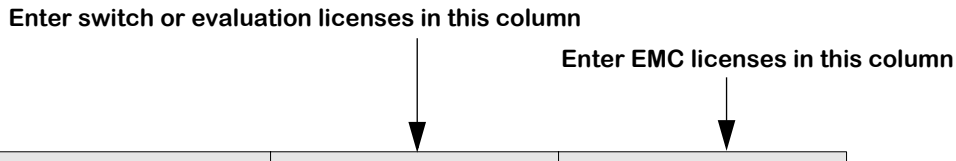
EMC Registration Issues

- First, you should register the CD-ROM for the EMC. You will be asked to provide the certificate key from the label inside the CD-ROM sleeve.
- Use the License Request Form on the Check Point web site (***http://license.checkpoint.com***) to register. The registration process involves filling out information on several screens and then receiving confirmation for the license. The steps are listed here:

  Step 1. Requester Information. The certificate key must be entered on this screen.

  Step 2. User Information. Contact information about the person requesting the license must be entered on this screen.

  Step 3. Host Information. Information about the EMC must be entered on this screen in the appropriate column. Which column you use depends on whether you are registering the EMC or the switch. ***Note that you do not need the IP address of the switch. If you are registering a switch, enter the EMC IP address in the Firewall Module column.*** Also, if you are registering a switch, you may select any value for the Platform and Operating fields. Use the table here as a guideline:



	Firewall Module	*Management Server*
Host ID/IP Address		
Platform		
Operating System		
Firewall Version		
Comments		

Step 4. Confirmation. After you have completed Step 3, a confirmation page displays with some request details.

Step 5. License Generation. After you confirm the information, a page displays that contains a "Features string" and a "License string." Write these two strings down carefully—exactly as they appear on the screen—before exiting the license request form. You will receive a confirmation of these two "license strings" via e-mail some time later, but you should write them down now while you are at the registration site to save time and avoid potential problems.

- You will have to repeat the registration procedures for each of your Check Point licenses (one for each EMC and one for each switch).
- The "Features string" and "License string" for *each license* are required for setting up the EMC software on your server. See the electronic documentation provided on your Check Point CD-ROM for complete details on this procedure.

EMC Setup and Configuration Issues

Following the steps below will help you to avoid having problems establishing a communications link between your switch and the Enterprise Management Console (EMC).

- Both the switch and EMC must be up and running and connected to the network. They can't communicate if the network is down. Also, the switch must have both a VLAN and a port attached to the network that contains the EMC. At this point, the IP Firewall software should be installed on the switch, but it should be set to "*disabled.*"
- The switch must be configured in the EMC's "Network Object" database. The Network Object Type must be set to "Switch".
- For a 4.0 EMC, the EMC's Network Object's configuration ***must*** specify the Version as 3.x, not 4.x. The version of the firewall module on the EMC is different from the version of firewall software on the switch. If the Version is not set correctly on the EMC, the EMC and the switch will not be able to communicate properly.

Configuring the Network Object Database

- When creating a Network Object for your switch(es), you must enter the IP address of the switch or the host name. The IP address of any router interface on the switch may be used. The address should be the same one configured in the firewall software for the Firewall IP address.

  If you are entering a host name, you must click a button to get/add the IP address for the host name you have entered. If this button does not work properly, you must fix the DNS system so that it can properly resolve the switch's name. However, if you are not using DNS (that is, you use a local "Hosts" file on your MS Windows NT machine), make sure that this file contains an entry for the switch. *Be aware that if DNS is enabled on the NT server, the local Hosts file will not be used. In order to use the Hosts file, you will have to disable DNS.*

- When creating a Network Object for your switch(es), you will be prompted for an External Interface and a Type. The External Interface must be specified only if the firewall product on the switch is used as a gateway to the Internet. The Type field indicates the license type and should always be set to Unlimited.

- After creating a Network Object for the switch, you must perform an "SNMP Get" of the switch's network interfaces. You may have to press the "SNMP Get" button twice to reliably get the switch's interface list.

- An Skey password must be established for the switch on the EMC. Refer to Check Point's documentation for complete details on this procedure (in the 3.0 version of their User Guide, this topic is discussed on pages 24-25). *Without a mutual password, the switch and the EMC will not be able to communicate.*

- Install the Network Object database on the EMC *before* you attempt to establish communications with the switch. Use the "Install Database" option under the "Rule Base Editor" window's "Policy" menu to install the database on the EMC.

Creating a Rule Base

- After installing the Network Object database, you must create a "Rule Base" on the EMC to define the policy that will be used on the switch. The Rule Base is created in relation to the switch's Network Object; therefore, make sure you have completed those procedures first.

- After you have created the Rule Base, you must install it on the switch. This step will allow the switch to download the firewall policy defined by the Rule Base when the switch first connects to the EMC. *If you fail to properly "install" the Rule Base, the firewall software in the switch will not be able to function.*

Running the Firewall Software

- After creating the Network Object datase and installing the Rule Base, you are now ready to run the **fwconfig** command on the switch. To enable the firewall, choose "Firewall" mode, enter the IP address of the EMC, and enter the exact Skey password that you entered on the EMC for this switch. The firewall software on the switch should begin operating and automatically establish a communications link with the EMC.

♦ Important Notes ♦

Whenever you create or delete new groups or VLANs on the switch *after* you have created the switch's Network Object on the EMC, you must update the switch's Network Object to reflect those changes. You can accomplish this update on the EMC by doing an "SNMP get" on the switch's Network Object.

Also, remember to install the policy on the switch after making any changes to a Network Object interface. Failure to do so will result in new interfaces running in an unprotected mode.

Unsupported Features of FireWall-1

When using Check Point's GUI Client, you will see certain options which are *not* supported by this release of the IP Firewall feature. These unsupported features are listed under the Rule Base Editor Properties menu and include:

Under the Security Policy tab:

- Apply Gateway Rules to Interface Direction is always "Eitherbound". Enable Decryption on Accept.
- Use FASTPATH is always enabled.

Under the Services tab:

- Intel Phone is not supported.
- Router Access Lists are not supported.
- Authentication is not supported in this release.
- Security Servers are not supported.
- SYNDefender is not supported in this release.

Under the Miscellaneous tab:

- Load Balancing is not supported.
- SKIP Encryption is not supported.

♦ Note ♦

In addition, time restrictions are not supported in the Rule Base.

When creating rules in the Rule Base Editor

Under the "Action" column of the rule:

- Drop and Reject are equivalent and result in the packet being dropped.
- Authenticate is not supported in this release.
- Encrypt is not supported in this release.
- Network Address Translation is not supported in this release.
- The EMC does NOT run on MS Windows '95.