Check Point SecurePlatform with Firewall-1

Quick Hardening

Check Point's SecurePlatform provides a hardened Red Hat Linux with Check Point's own Firewall-1 NG and allows you to install a firewall yourself within a few minutes – without any assistance from system integrators or consultants.

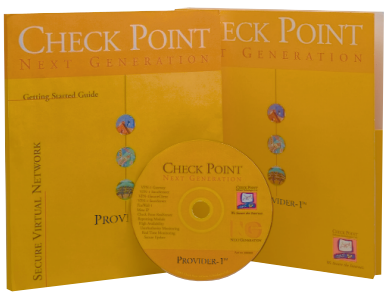
BY JÖRG FRITSCH

Check Point's SecurePlatform [1] provides a combination of the recent Check Point Firewall-1 NG FP3 (Next Generation, Feature Pack 3) with a hardened, minimal Linux distribution on a single CD. The CD is bootable on Intel systems, and installs a customized Red Hat distribution and the Check Point software within a few minutes.

The installation creates an extremely well secured system. An in-depth knowledge of Linux, which the admin user would normally need to harden the system and perform meaningful partitioning, is not required for this product. The admin merely requires basic knowledge of the Firewall-1 structure and licensing to provide the right answers to the questions posed during installation. This makes it easier for end users to set up the Firewall-1 themselves, and avoid integration fees with the exception of licenses (see box "Licensing") and media.

Simply put, Check Point works the market on the basis of the Coca-Cola principle. The soft drinks manufacturer supplies its products to franchising partners who bottle it and sell it to distributors, who in turn sell it to retailers, who finally sell to real customers. The Firewall-1 follows a similar pattern. Check Point sells its products to European distributors, who in turn sell to integrators, who in turn sell the customer both the product and the consulting services the customer may require. The SecurePlatform interrupts this supply chain as it is pre-integrated. Although customers should be pleased, the product has caused a shake up on the European market. Integrators are not prepared to sell licenses off the shelf and act as firefighters if customer installations fail to scale.

SecurePlatform



Manufacturer: Check Point [2]

Content: Minimal and hardened Red Hat Linux, combined with Check Point's Firewall-1, Floodgate-1, Policy Server, User Authority Server and Smartview Monitor. All of these products as NG (Next Generation) version, Feature Pack 3 (FP3).

License: Euro 3,240 for 25 IP addresses, for details see the "Licensing" box. Parts of the Secure Platform are released under the GPL or BSD license.

Hardware: Intel platform, multiple network interface cards. For details see the "Hardware Requirements" box

Installation

The installation of the SecurePlatform is similar to that of a minimal Linux distribution. The system boots a character based installer from CD, asks a few questions (keyboard, 2 tier or 3 tier system) and installs a working Firewall-1 in about 4 minutes. Non-recoverable errors can only occur at two stages: the installer prompts the user to choose between an Enterprise or Small Office system (Figure 1). The second hurdle is the Products Configuration: this detailed configuration option is only available for the Enterprise system.

The selection of a Small Office or Enterprise system affects the choice of products in the subsequent dialog (Figure 2) and on the installed system. Small Office systems are configurable by HTTPS and web server only ("admin_httpd", "cp_httpd"), SSH access is not available. This option is thus suited to small networks with less than 25 clients. Larger networks may experience scalability issues, and this will mean twice the amount of work for the admin user.

The system created when you select the Enterprise option is a completely different matter. This installs 94 RPM archives with a total of 210 Mbytes of software, without a web server, but including OpenSSH. There is no way to influence the choice of packages, the partitioning or the hostname during installation. Table 1 shows how the finished system is partitioned; the Check Point software is stored below the "/opt" directory.

THE AUTHOR

Jörg Fritsch majored in Chemistry at university, has been working with Unix/Linux since 1994, and got into the IT business via programming jobs. He is currently working for Tesion as an Internet service/Hosting system specialist.

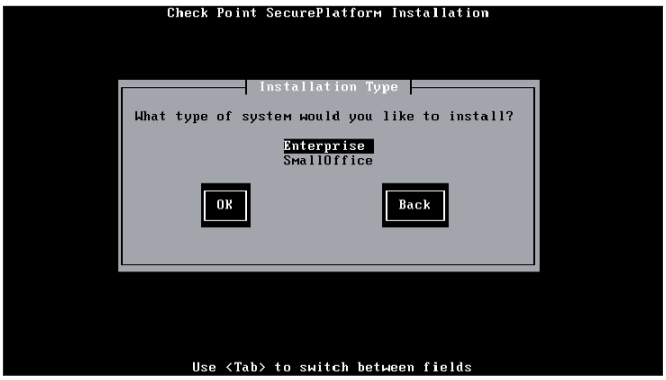


Figure 1: The SecurePlatform installation allows you to choose between an Enterprise Version and a Small Office Version. The latter is fairly inflexible as it only provides a Web-based administration interface

Figure 2: The admin user can install various other Check Point products in addition to Firewall-1. The available options depend on the version being installed – Enterprise or Small Office

Many packages are available under the GPL or BSD license, but the Check Point software itself is proprietary. The package names all end with "cp" (for example, "bash-2.05-8cp"). Check Point is obliged to disclose any changes made to GPL sources. As we were particularly interested in bash, we requested the sources and actually received them within 24 hours. The bash source is identical to the GNU original, despite the "cp" extension. The only difference is the size of the archive, but this is due to compression (Gzip, Bzip2).

Hardening and Operations

The installed system is extremely impressive. After installing the system you will not find any setUID files on the hard disk, and inetd does not launch any services; the system accepts only robust passwords (due to the cracklib installation). Remote access is only available by SSH, direct root logins are not permitted. There are no manpages for the GNU packages or the proprietary software. Manpages for various Unix derivatives (such as Solaris, FreeBSD and Red Hat) have provided a favorite attack path for rootkits in the past. Most of these security problems were caused by the Catman system, which is responsible for caching and displaying formatted texts. Catman is a setGID ("man" group) or even setUID tool (the user "man" even needs a valid login shell). To close regularly occurring security holes, you can let the man viewer rebuild pages when they are requested, instead of serving up prebuilt pages.

The interesting aspects of this distribution are below the surface. Only the root and Admin user entries in "/etc/passwd" (both of which are UID 0) are active users. Only the Admin user is allowed to logon remotely via SSH. The proprietary CP shell (whose sources are not available) is assigned as this user's login shell. The shell is more like Cisco IOS than a traditional Unix shell. You can type a question mark to display a list of available commands.

The CP shell (at least in the Enterprise installation) includes a series of integrated commands, most of which refer to the Check Point software. These commands are all you need to manage the Firewall-1. Configuration commands for the Secure-XL API (Check Point Performance Pack for increased throughput) and Cluster-XL commands are also available.

Expert Included

The "expert" command is one of the built in commands and is available in both installation versions. The command works in a similar way to the "su" command and launches bash as a subshell for the root user (Figure 4). This provides root with several additional GNU system management commands, allowing the root user to create additional directories, mount filesystems (such as CD ROMs) or write shell scripts.

Hardware Requirements

Hardware requirements depend on the throughput the finished firewall (or cluster) will need to handle. The installation procedure allows you to specify various environments for the product – from Small Office and Firewall-1 XL to VSX. VSX is a virtual system mainly used for commercial security service providers.

Simple Hardware is often enough

Simple hardware and a few network interface cards (a trusted and an untrusted interface, for example) are sufficient to provide fairly good throughput, claims the manufacturer. An Intel based computer with a 32 MHz PCI bus and two interfaces attained speeds of 200 Mbps without encryption. Under practical conditions this value will tend to be lower, but these value reflect two factors: You do not need specialist hardware for a 2 Mbit Internet connection and it is unlikely that the CPU will prove to be to slow. Without the Secure XL Performance Pack you would normally expect the system bus to be a bottleneck.

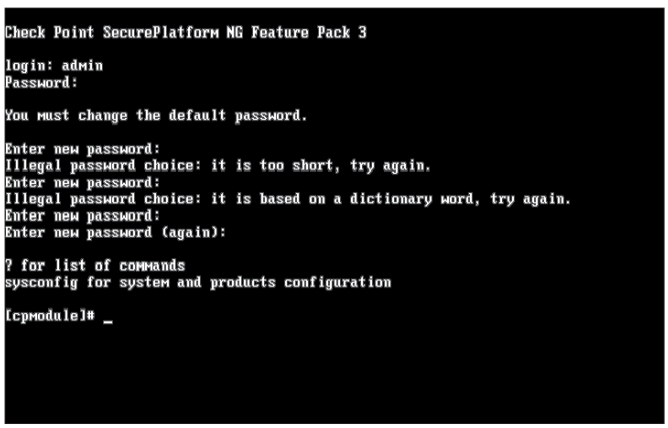


Figure 3: After logging on initially, the CP shell forces the admin user to supply a password. Cracklib prevents passwords that are too short or not sufficiently robust

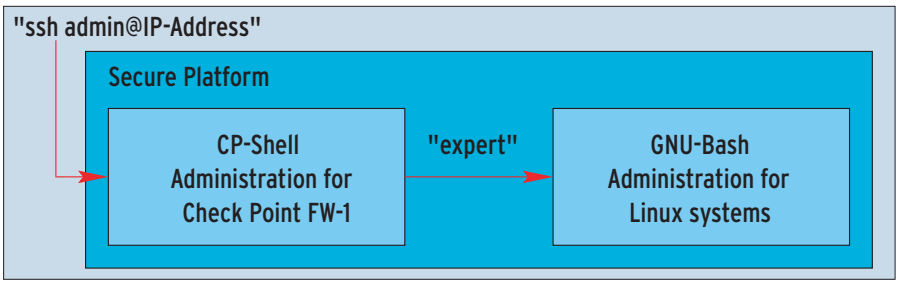


Figure 4: The admin can use SSH to launch the SecurePlatform CP shell. The "expert" command allows bash access, and thus to standard Linux functions

Admin also needs to launch expert mode to install additional packages. The SecurePlatform can also be clustered with Rainwall [3] – this assumes that the GNU C++ library supplied with Rainwall has been installed. Although some manual intervention is required, you do get a cluster without superfluous ballast for your effort.

The platform envisages only the two users we discussed previously, both of which are UID "0" (Root/Expert and Admin). You cannot log on as root either remote or locally. Although the GNU "useradd" and "passwd" commands do exist, we were unable to create a new user. Manual editing of the "/etc/passwd" and "/etc/shadow" files was equally unsuccessful.

The problem is that the "passwd" command seemingly changes the admin user's login password, no matter what user launches the program or what user you need to edit. The sources for this command are unchanged. This behavior may be caused by PAM modules, but we could not find anything unusual there either. And asking the manufacturer, Check Point, did not get us any further.

A Direct Route

The network adapters in the system or VLAN (Virtual LAN) tagging can be configured in the CP shell; the "sysconfig" command takes care of this. Strangely enough there is no submenu to change the speed or operating mode (full duplex FDX, half duplex HDX) of the network adapters. It looks like the admin user is forced to rely on the autosensing function of the network adapters, and that often leads to problems in production environments. A firewall should negotiate as few dynamic parameters as possible.

The sysconfig "Products Configuration" menu item is interesting. You can opt for a simple or distributed (that is 2-tier or 3-tier) installation. A 2-tier installation (Figure 5) involves two machines: the admin workstation with a GUI for configuring a set of rules and the machine running the firewall itself. A 3-tier installation (Figure 6) involves three computers. The firewall is then distributed across a machine that manages the ruleset and receives logfiles, and a machine with the filter and routing function proper (the firewall module). 3-tier installations provide better performance, but licensing is complicated. This installation type is best suited to clusters and for large environments with lots of firewall modules at various positions.

After completing all the items in the sysconfig menu, you should be able to connect to the firewall with the GUI to exchange certificates and set up an initial ruleset (see Figure 7). If this does not

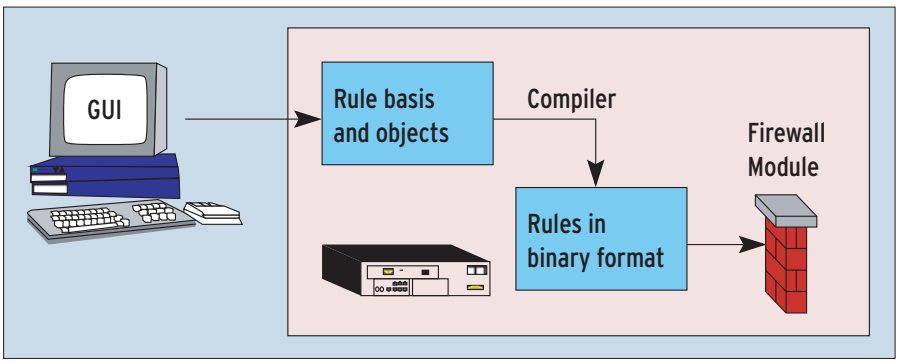


Figure 5: In a 2-tier installation, the GUI stores the ruleset on the firewall machine. A compiler translates the rules that control the firewall modules to binary format

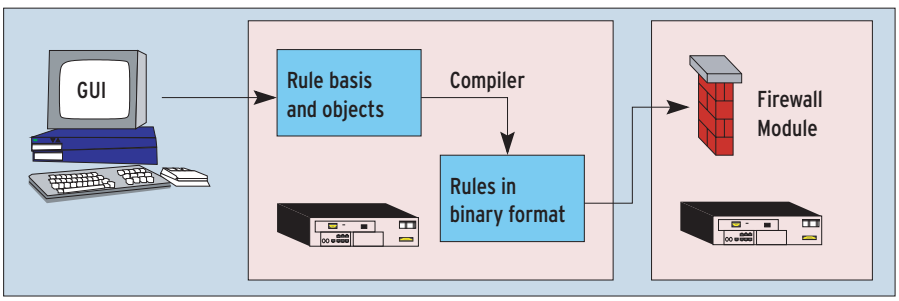


Figure 6: A 3-tier installation uses separate firewall and configuration server machines. This allows a centralized configuration to control multiple firewall modules, a particularly useful architecture for distributed installations

Licensing

In Check Point's case the licensing requirements depend on the number of IP addresses to be protected, and additionally whether you perform a distributed installation (see Figures 5 and 6). The configuration procedure defines one interface (in the simplest case the untrusted interface) as an external interface. The firewall software then counts the IP addresses assigned to all the other interfaces. As the software gets confused by NAT, strictly speaking all the licenses in your LAN should be licensed, whether the firewall actually sees them or not.

Check Point licenses are available in various sizes: for 25, 50, 100, 250, or an unlimited number of IP addresses. In the case of a 2-tier installation (non-distributed) prices range from Euro 3,240 to 20,520. In the case of a distributed (3-tier) installation, the filter module (without management function) are a lot cheaper (Euro 2,160 to 7,560). Encryption will increase the price by approximately Euro 500 to 1,000. Features such as encryption or the Visual Policy Editor (see Figure 7) require additional licensing.

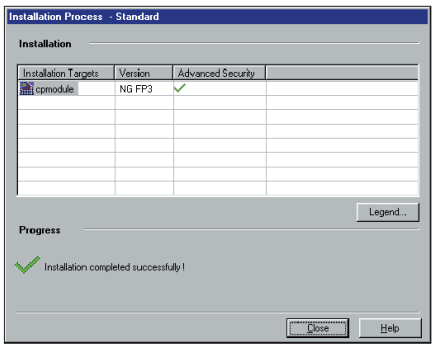


Figure 7: Typical Check Point GUIs allow SecurePlatform administration on a Windows machine

work, because the rules do not allow a GUI workplace, it's back to the console: the "fw unload all.all" command sets the firewall to permissive mode.

The numerous features and APIs that Firewall-1 now provides mean that services will be listening on about 30 TCP ports immediately after installation. With the exception of SSH and the RPC ports 32770 through 32774 all of these open ports belong to Firewall-1 services, for GUI based remote administration, user authentication or logging, for example. To be more precise, not all of these ports are open as the ruleset denies these services by default. An implicit cleanup rule makes sure of this: "any any any deny".

We used a 2-tier installation in our lab environment. After running the CP shell to configure the system, all you need is the Check Point GUI, which is used for creating and managing the ruleset and runs on a Microsoft Windows machine. This was the most time-consuming and confusing item of the whole installation. An experienced Firewall-1 NG user would tend to look for a package called "Management Clients" in the Windows Installer, but unfortunately this was dropped in FP 3. The Management GUIs previously comprised of three applications: Policy Editor, Log Viewer and Status Viewer. In FP 3 all of them have been renamed to SMART Client (SMART Dashboard, SMART Status and SMART View Tracker).

INFO

[1] Check Point SecurePlatform: *http://www.checkpoint.com/products/protect/secureplatform.html*

[2] Check Point: *http://www.checkpoint.com/*

[3] Rainwall: *http://www.rainfinity.com/products/rainwall.html*

Conclusion

Thanks to the CP shell the configuration and administration of the SecurePlatform is more like an appliance than a normal Linux machine with Check Point Software installed. The SecurePlatform offers two advantages over a typical appliance: First, most appliances provide browser based administration, and that means running a web server on them. If you disable the web server, you might find that administration is not particularly convenient. The SecurePlatform offers text based administration via SSH and the CP shell without needing an additional web server. Additionally, there is a bottom-line advantage, as only normal hardware is required provided it complies with the system requirements.

One possible disadvantage is the fact that hardware and software will normally be from different sources in contrast to a genuine appliance. So, if something goes wrong you might expect both parties to disclaim responsibility, although to be fair, this is extremely uncommon in normal circumstances. ■

Table 1: Partitioning layout

Device	Filesystem	Typ	Optionen
/dev/hda2	/	ext3	rw
none	/proc	proc	rw
usbdevfs	/proc/bus/usb	usbdevfs	rw
/dev/hda1	/boot	ext3	rw
none	/dev/pts	devpts	rw,gid=5,mode=620
/dev/hda5	/opt	ext3	rw
none	/dev/shm	tmpfs	rw
/dev/hda3	/sysimg	ext3	rw
/dev/hda7	/var	ext3	rw