Securing your Network Perimeter: Check Point FW-1 vs. Cisco PIX

By Robert Sharp and Richard E. Weber

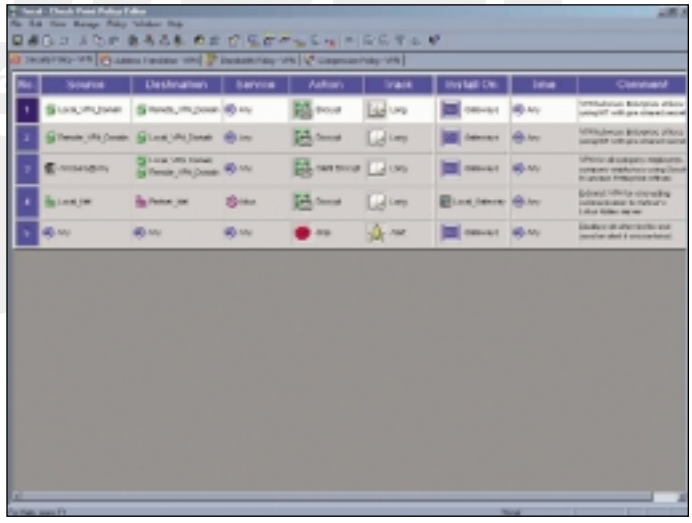
This article evaluates two of the industry's most popular firewall platforms—Check Point NG FireWall-1/VPN-1 (Virtual Private Network) and Cisco PIX (Private Internet Exchange).

WITH over 52,658 break-in attempts reported in 2001[1], security is a very real concern for small businesses and large corporations alike. The need for a firewall is essential for all businesses today, big and small. The problem is that most IT staff are too busy and don't have the time necessary to properly evaluate the large number of firewalls that exist today. Being security consultants, we have had the opportunity to evaluate and implement a large variety of firewalls, so in this article, we are going to review two of the industry's most popular firewall platforms, Check Point NG FireWall-1/VPN-1 (Virtual Private Network) and Cisco PIX (Private Internet Exchange). This article will cover the basic installation and the pros and cons of each platform. We will begin the article by providing some background on what a firewall is and how it works.

INTRODUCTION

Check Point FW-1 and Cisco PIX are based on a Stateful Packet Inspection (SPI). SPI tracks the context of each connection traveling through the firewall and can filter according to your ruleset definitions. The context of a connection consists of TCP/IP sequence numbers, source and destination and the state of the connection (opening, open or closing.) Check Point was the first firewall to market using this technology. Cisco uses a technology called ASA (Adaptive Security Algorithm) to achieve the same result. Stateful packet inspection and ASA differ from other packet filtering firewalls due to their ability to track all TCP (Transmission Control Protocol) connections and UDP (User Datagram Protocol) packets, which are used to decide what is allowed as part of an acceptable TCP/UDP session and what may be forged. This is very important when it comes to allowing only outgoing TCP/UDP requests and blocking incoming requests. Stateful inspection also provides added value, since it brings with it the ability to track all UDP packets and create a virtual session that is transparent to the network application, while still providing the same security offered with stateful connections. This allows users to start HTTP sessions to an outside server and at the same time block incoming requests from the Internet to your protected machines. Today's firewalls should offer more than just this, however. They should also be able to provide a log of usage, user authentication, and in most cases, some sort of encryption over public networks.

FIGURE 1: CHECK POINT GUI: SECURITY POLICY, OVERVIEW OF ACCESS RULES AND POLICIES



VPN COMPARISON

Having a LAN-to-LAN VPN is no longer a luxury or a future add-on; it's an essential feature when determining your needs in a firewall. A VPN can provide a secure connection to your business's other office or to business partners, eliminating the need for costly dedicated lease lines. Both Check Point and Cisco offer LAN-to-LAN IPSec VPN capability depending on the options purchased with the firewall. While

the method differs, both products offer remote user VPN access. Check Point offers a secure remote client as a free download. This allows PC users to connect to your firewall remotely via VPN. For the Secure Remote client, all the settings are stored on the firewall module, and all that is required by the end user is an IP address, user id and password or digital key. Check Point also offers SecureClient as their VPN software. Check Point's Secure Client requires an extra fee. However, it does provide the ability for the administrator to push down security policies to the client, transforming the SecureClient into a personal firewall. This also allows the administrator to secure any holes opened by the remote user. Cisco PIX offers not only their VPN client, but Cisco also supports the Microsoft PPTP client (Microsoft VPN software). The Cisco PIX doesn't offer Check Point's level of control over the remote user, but it does provide an easy encryption solution. For additional VPN solutions, Cisco users should look into the Cisco VPN concentrator product line as they offer extended functionality.

Now let's look at some additional differences between the two products. We can begin by looking at the basic install for each platform. We will begin with Check Point because of its complexity.

FIGURE 2: CHECK POINT GUI: AREA TO DEFINE NETWORK OBJECT: SERVERS, NETWORK BLOCKS, FIREWALL/MANAGEMENT OBJECTS

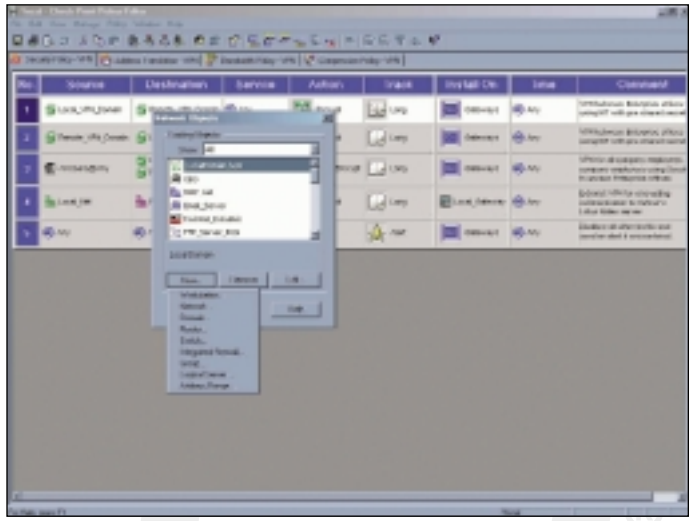


FIGURE 3: PIX DEVICE MANAGER: INCOMING AND OUTGOING RULES FOR NETWORK ACCESS

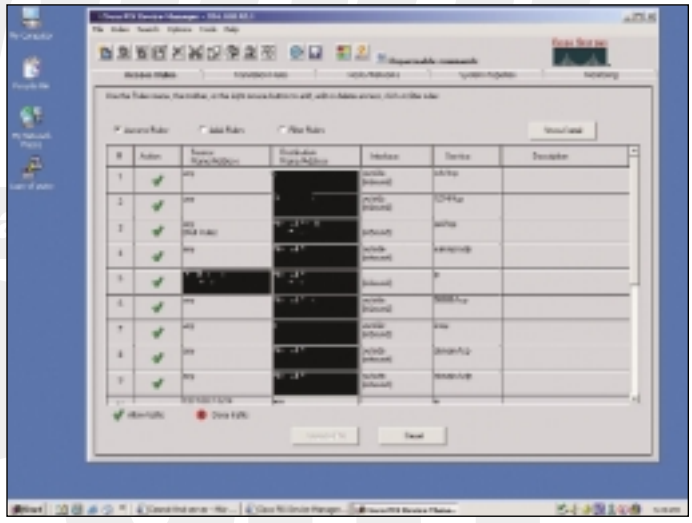
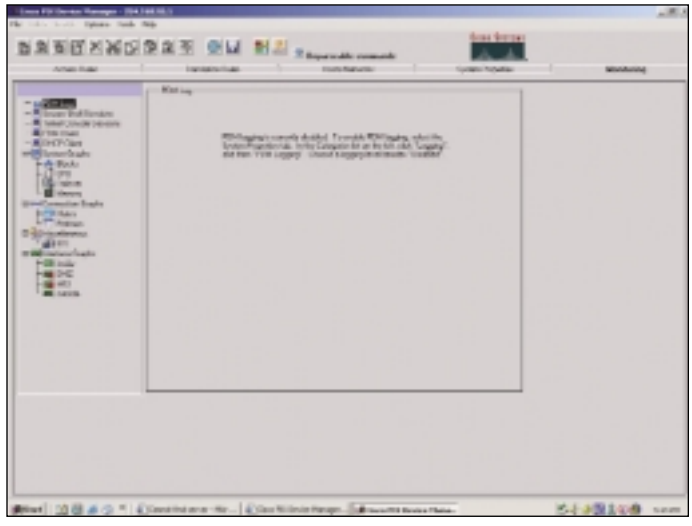


FIGURE 4: PIX DEVICE MANAGER: MONITOR TAB FOR LOGS AND OTHER PERFORMANCE METRICS; NEAR REAL TIME INFORMATION IS PROVIDED



CHECK POINT

Check Point is a software-based firewall. This means the firewall is a software-based application that runs on a standard hardware platform with a variety of operating systems. Some of the more popular operating systems Check Point uses are:

- Windows NT/2000
- Solaris (Sparc, X86)
- Linux
- AIX
- HP UX
- Nokia IPSO

The platform you choose does not matter as far as Check Point is concerned. You should choose the platform that you are most comfortable with. Whichever platform you choose, you should ensure that you strip the operating system down to only what is necessary to run Check Point. There is no reason to run any other services on this box. Doing so just unnecessarily increases your security risk and chance of compromise. There are guides on the Internet that you can use as a basis for stripping down the operating systems (OS). (See http://www.spitzner.net/nt.html for Microsoft and http://www.spitzner.net/linux.html for Solaris). Check Point doesn't really require you to strip down the OS, because you can place a stealth rule on your firewall to deny all traffic destined for the firewall. The stealth rule is a good idea no matter what you decide. While OS hardening is not a Check Point requirement, not doing so is just asking for trouble.

A firewall's primary function is to review and filter all inbound traffic to internal machines and not accept any traffic trying to reach the firewall itself. Your main concern for security on the firewall should be keeping the firewall software itself patched. Most of the remote exploits will be stopped by the stealth rule. We recommend that when using Check Point that you place the management station on a separate machine and not the same machine on which you have the actual firewall applications. The management station machine, like the firewall box, should have no other applications on it, and access to the box needs to be extremely limited.

Nokia has developed an operating system and a box that turns the Check Point firewall from a software-based solution into more of an appliance similar to the Cisco PIX. It uses a pre-installed Check Point combined with a FreeBSD machine. Nokia replaces much of the command line interface, native with FreeBSD, with a Web-based interface, making it more user-friendly. A typical Check Point installation can occur in one of two ways--either a distributed installation or a stand-alone installation. Check Point FW-1 is broken into pieces, a firewall/enforcement module and a management module. This allows you to manage multiple firewalls from one management module and provides a centralized logging point. If you can't afford the additional hardware, Check Point will allow you to place both modules on the same machine. This is called a stand-alone install, and it is not recommended, as it is a potential security issue to have full access to your management station and firewall within a single box.

Once the installation is complete, you're ready to start adding rule sets to the firewall, which is the first step in locking down your network. Check Point FW-1 operates on a security policy that's created by a GUI client. The GUI client is a third piece of software run from the firewall administrator's desktop (See figures 1 and 2). From the GUI client, the administrator can change the properties of your firewall and edit your security policy. Setting up and configuring your firewall rule set can get pretty complicated and varies so widely from network to network that it doesn't make sense to try address it in this article. The GUI client is also used to monitor the firewall's up/down status and view the firewall logs in real time. It's a pretty versatile interface, which configures 90 percent of what the administrator will ever need to do on the firewall. Other tweaking can be done by command line firewall utilities and editing configuration files directly.

Once the Check Point firewall has been configured, we recommend you back up your configuration, since it can be a time-consuming process to re-set up your firewall. At a minimum, listed below are a few of the major items you will need to back up. Please note: You should back up the directories on both the firewall and management stations.

1. $FWDIR/conf/ directory. This contains all your rules, your objects and your users.
2. Static routes. You have to set these up yourself. They can vary by OS, so there is not a standard place to look for these files.
3. Static ARP (Address Resolution Protocol) entries, same as above.

With these three items backed up, you can recreate your firewall by simply reinstalling both the OS and FW-1 and then replacing these files.

Once you have created your security policy, the next step is to save it and "push the policy" to the firewall. After this takes place, the Check Point Management Modules will run a few error checks on your policy, compile it and download it to your firewall module/enforcement point. Next, your firewall modules install the policy and begin operating based on its new set of instructions.

This covers the very basic operation and install of a Check Point firewall.

CISCO PIX

Cisco has created its own version of an SPI firewall and called it PIX. The PIX name is an acronym for Private Internet Exchange, and as its name suggests, its purpose is to regulate and control access between a private network and the Internet. Like most Cisco products, it's an appliance-based unit. PIX runs on x86 type hardware, but it runs a Cisco proprietary OS written for the PIX firewall. This means you don't deal with a separate operating system in addition to the firewall software which, depending on your preferences, can be a plus for you. Since it's an appliance, an actual install is pretty much non-existent. You turn on the device, and using a dumb terminal connected to a console port, you run the command 'setup.' This lets you set up an internal IP address from which you can Telnet or HTTP in. From this point, you can configure your interfaces and start setting up your rules.

The configuration process in a PIX firewall is a bit different from that of Check Point. While Check Point has its command line interface, it's more geared to firewall maintenance and detailed setup only, while Cisco's command line interface can be used for everything. You can

Check Point Reference:

If you do decide on getting a Check Point firewall, we recommend using the Web site www.phoneboy.com and also purchasing the book that the site author published entitled: *Essential Check Point Firewall-1* by Dameon D. Welch-Abernathy (a.k.a. PhoneBoy).

FIGURE 5: PIX DEVICE MANAGER: GENERAL DEVICE-WIDE CONFIGURATION OPTIONS SUCH AS LOGGING, ADMINISTRATIVE ACCESS RULES, ETC.

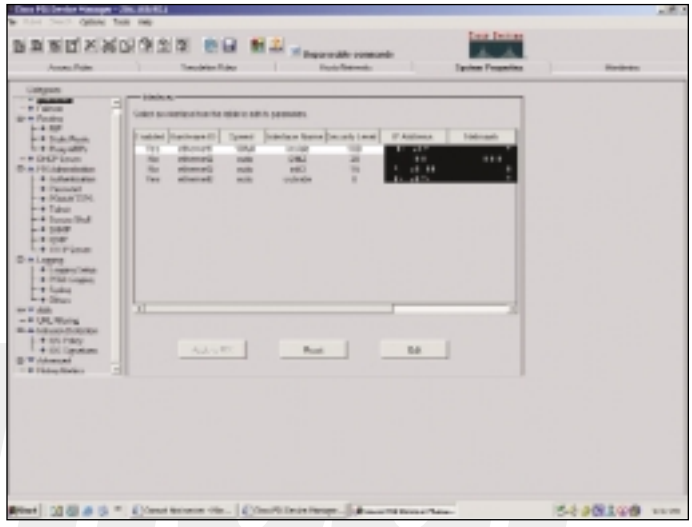
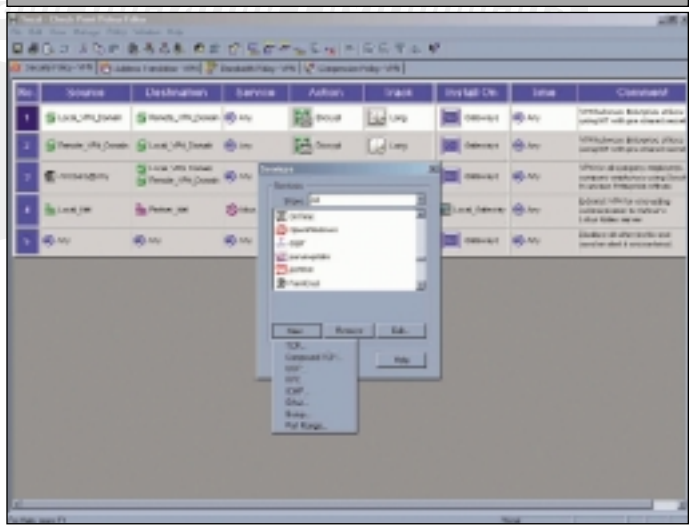


FIGURE 6: DIFFERENT IP PROTOCOLS THAT CAN BE SET UP IN CHECK POINT



operate a Cisco firewall directly from the terminal and still have its full functionality. Cisco, however, in its more recent versions, has been offering the PIX Device Manager (PDM). This is a Web/Java-based interface to the PIX firewall that allows you to get into the PIX configuration and provides you a quick overview (See Figures 3, 4, 5 and 6). Cisco has a few versions of the PDM available. We recommend that you install PDM version 2.2 and PIX OS 6.2. This is the most up-to-date software and offers many new features over the previous versions. This version can handle network/host objects, has improved VPN management/configuration and updated IDS signatures. There is also a third option that we would like to mention, but that won't be discussed in this article. Cisco has an application called Cisco Secure Policy Manager software. This is geared towards high-end clients who may want to manage multiple Cisco firewalls and want the ability to work on all of them from a single interface. Now that we have covered the basic operation and configuration methods, the next step is to point out some issues and concerns that we have about each firewall.

The greatest benefit of owning a PIX, as with any Cisco product, is its top-notch technical support system. If you are having trouble with your PIX, the Cisco Web site has a wealth of information. Pay them a visit at www.cisco.com and see for yourself. You should be able to find an answer to your questions there. However, if you have encountered a problem you can't seem to find an answer for, you should contact the Cisco Technical Assists Center (the TAC) or your Cisco representative. All are excellent resources, and they will find you an answer to your question.

OPERATING CAVEATS

Like everything else in the world of technology, Cisco PIX and Check Point NG FW-1 have their little quirks that aren't documented and are not often discovered until you run across them. These are often things that you wish you knew about before you started down the install path. Hopefully everyone reading this article will learn from our experiences.

First, let's look at Check Point NG and what roadblocks we have encountered. Even if you tell Check Point to control IP forwarding during setup, if you don't tell the Windows NT OS to enable forwarding, you will spend quite a bit of time wondering why your firewall appears to be working but is not. Always enable IP forwarding on your OS, and tell Check Point to control it. This prevents the rare occurrence that something slips through your firewall when it's booting up or loading a new policy. Another big security issue today is content security. Web content filtering, e-mail filtering and scanning are becoming increasingly important. This is where Check Point can really come in handy. Check Point offers a great deal of flexibility when it comes to content security. Check Point integrates with many add-on products and even provides some additional functionality on its own. Check Point NG FW-1 will allow the administrator to create a list of URIs (Uniform Resource Identifiers) that can be restricted or filter out Active X or Java, without any add-on products. It can also scan e-mail and strip out mime attachments; Check Point does require an add-on server for e-mail virus scanning.

Check Point NG FW-1's greatest asset is that 90 percent of all the configuring for your firewall can be done through its management GUI (Graphical User Interface). This is something that can't be done in the Cisco PDM (The PDM is a nice tool, but it has very limited functionality. When using Cisco PIX, you have the option of either using the PDM or the command line interface for doing your configurations. This is nice for those network guys who prefer working with the command line. While Check Point excels in its flexibility, that adds to its complexity, which can make it more difficult during setup and troubleshooting. Check Point also charges for support, software updates and bug fixes, so if you want or need support, you better have deep pockets. Check Point does have a public support knowledge base, but it restricts its full knowledge base to registered users. The PhoneBoy site listed in this article is the best place to go for free help when troubleshooting a Check Point firewall. It would also be a very good idea to attend Check Point training at some point. The advanced training classes offered provide you with a great deal of knowledge, evaluation software and excellent resource manuals. In addition, the classes also provide you with a network of Check Point users that will be in the same position as you during their learning curve as you all get up to speed on the software and its capabilities.

Cisco PIX has a few caveats of its own. One thing we like about Cisco is its ease of setup and management. Cisco PIX is an appliance type of device, which for us means easy setup and easy rollbacks if a change doesn't work quite right. The configuration is in one easy-to-manage and back-up file. If you have any question as to a change that may be causing a problem, you can very quickly and easily roll back to the old configuration. Cisco's PDM provides a nice monitoring feature that lets you monitor CPU (Central Processing Unit), traffic and a whole variety of other metrics in near real time. The PDM has been upgraded in the recent past, and it now provides a fully functional interface to the device.

The Cisco PIX has two Web content filtering vendors it supports—Websense and N2H2. Both platforms support user authentication, although the user authentication isn't tied in with the AAA (Authentication, Authorization and Accounting) model the PIX uses for its authentication, which means two authentication databases may be required (depending on your usage, not always necessary). Both packages provide listings of URLs by category and allow the administrator to tailor access to both users, length of surfing session and times of day. Perhaps the biggest issue to work around with this type of implementation is filtering out the various Internet-enabled applications that use the Web to check for product updates, ect.

SUMMARY OF THE PROS AND CONS OF EACH PLATFORM

Cisco PIX

Pros:

- Easier/faster setup
- Simple self-sufficient appliance
- No OS to worry about
- More compact footprint
- Easier licensing
- Much easier fail over setup
- Updated PDM works well
- Built-in mini IDS
- Supports Cisco AAA

Cons:

- No logging management without a separate server
- Doesn't allow for e-mail filter/scanning
- URL filtering requires a separate server

- Authentication/accounting requires a separate server/system

Check Point NG FW-1

Pros:

- Much more configurable/flexible
- Built-in user authentication, plus many more options for user authentication
- More flexibility with add-on products
- Works on a variety of platforms
- Easier scalability
- CP MAD (Check Point Malicious Activity Detector) good for spotting port scans and dos attacks
- Syn Defender good for protecting servers
- Built-in load-balancing features

Cons:

- Have to maintain an OS below the firewall
- More complicated to set up
- More complicated to identify and troubleshoot issues
- CP Mad (Malicious Activity Detector) difficult to configure and unstable at times

CONCLUSION

Both Cisco PIX and Check Point NG FW-1 will provide you with a top-of-the-line Stateful Packet Inspection firewall, which in today's world is really essential. Each firewall has its advantages and disadvantages as we tried to point out: Check Point is best for outstanding flexibility and functionality, and the Cisco PIX for ease of install, operation and support. PIX still retains most of the basic functionality of Check Point FW-1, but it does leave a few areas to be desired. We hope that this overview will help you to choose a firewall that is right for your organization. Please also keep in mind that a firewall is only one part of a total security solution.

AAA server:

AAA is a Cisco-coined term meaning Authentication, Authorization and Accounting. An AAA server is available from a wide range of sources. It can be provided by TACACS+, which is a Cisco-supported system that provides the ability to authenticate users at a central source, log their usage and authorize activities on your network. It's available in a freeware form with TACACS+ daemon, or Cisco also provides an NT solution that's available for a fee. Another option is a RADIUS server. This is much more popular if you are going to integrate with different equipment vendors or eventually want to add a single sign-on solution to your environment. RADIUS is an open-source protocol that can be purchased in a commercial package or obtained from an open-source author. RADIUS doesn't provide all the functionality that TACACS+ does on Cisco equipment, but it's more interchangeable with other vendors. Both PIX and Check Point support both RADIUS and TACACS+ as an authentication option.

NaSPA member Robert Sharp has been working in the security industry for over three years and is a graduate of the Rochester Institute of Technology. He is currently a network security engineer for a consulting firm in the health-care industry. Robert has several certifications including Systems Security Certified Practitioner, Cisco Certified Network Associate and Check Point Certified Security Administrator. His e-mail address is security@sharpie.org

NaSPA member Richard E. Weber, CISSP, CNE, MCSE, CCNA, CCDA, is technical director at Superior Consultant Company. He can be reached at rweber01@twcny.rr.com.

[1]Cert.org - http://www.cert.org/stats/cert_stats.html