Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Using The Cisco Pix Device Manager

The complexity of the many services and features offered by the Cisco PIX firewall appliance can make configuration from the console a daunting task even for someone who is familiar with the Cisco IOS. Because a firewall is only as good as its configuration, security may suffer if the PIX is configured poorly due to a lack of skill with the command-line interface. Fortunately, Cisco has provided a GUI tool called the PIX Device Manager (PDM) that allows secure configuration, management, and monitoring from a browser. D...

Copyright SANS Institute
Author Retains Full Rights

AD

USING THE CISCO PIX DEVICE MANAGER

Jason Holcomb
GSEC Practical Version 1.4b

ABSTRACT

The complexity of the many services and features offered by the Cisco PIX firewall appliance can make configuration from the console a daunting task even for someone who is familiar with the Cisco IOS. Because a firewall is only as good as its configuration, security may suffer if the PIX is configured poorly due to a lack of skill with the command-line interface. Fortunately, Cisco has provided a GUI tool called the PIX Device Manager (PDM) that allows secure configuration, management, and monitoring from a browser. Despite the bad reputation of many vendors' past attempts to port command-line interfaces to graphical interfaces, Cisco PDM version 2.02 integrates most commands supported on the PIX very robustly. In addition to providing an effective tool to configure, manage, and monitor a PIX firewall, the Cisco PDM can improve security by making these tasks more understandable for the firewall administrator. This paper examines the PDM starting with an overview of the PIX, requirements of the PDM software, initial configuration guide, and finally a walk-through of the software.

PIX OVERVIEW

The Cisco PIX (Private Internet eXchange) firewall uses stateful inspection to filter traffic. This method, which balances performance and security, evaluates traffic based on more than just the header information that is used by other methods like packet filtering. Instead, stateful inspection evaluates additional information about the packet such as its relationship to other packets as well as application-level information. To determine which networks are protected the PIX uses a numeric value from 0-100 to label each interface. The least secure interface, generally the Internet connection, is assigned a value of 0 and by default is the Ethernet-0 interface. The most secure interface is given the value of 100 and by default is the Ethernet-1 interface. The numbers themselves do not mean anything – what matters is their relationship to each other. Traffic originating from a lower-numbered interface to a higher-numbered interface is not allowed unless specific access has been configured.

There are just enough differences in the way things are done in the IOS versus the Cisco PIX operating system that configuration can be frustrating for those who are used to working with Cisco routers. One notable difference is that interfaces are named and referenced by that name. This is unlike the Cisco IOS where the interface name (FastEthernet0/0, for example) is static and represents its physical location on the router. Although it can be changed, the interface that connects to the unprotected network is generally named "outside", while the interface connected to the trusted network is known as the "inside" interface. By default, these two names will be given to Ethernet0 and Ethernet1, respectively.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

PDM REQUIREMENTS

According to Cisco, most PIX firewall appliances that are running the latest version of the Cisco PIX software (currently version 6.2) have the ability to run version 2.02 of the PDM. This includes PIX platforms 501, 506/506E, 515/515E, 520, 525, and 535. Those units that are not running the Cisco PIX software version 6.2 may be able to upgrade but in some cases will require a hardware purchase as well. The most common place older PIX firewall units will be lacking in hardware is the flash memory card. As a general rule, the PDM requires at least 8 MB of flash memory and 32 MB of system memory. The added functionality of the PDM may be worth the investment in hardware to make an older PIX suitable for the new software. ("System Requirements", 1-2)

INITIAL CONFIGURATION

Although nearly every function available at the CLI is also available with the PDM, for the initial configuration, the CLI must be used. To begin configuration of a new PIX firewall, a console cable and terminal emulation program must be used to gain access to the CLI. The initial setup will ask some basic questions about how the PIX will be set up. Once an IP address has been assigned to the "inside" interface, configuration can be completed with the PDM. Here is an example of the initial configuration prompts:

PIX prompts are in italics
User responses are in bold
Author's comments start with an asterisk (*)

* This series of initial configuration questions will get the PIX to a point where configuration can be completed using the PDM. Saying yes to go through these prompts is the easiest way to get started.

Pre-configure PIX Firewall now through interactive prompts [yes]? <enter>

* The PIX does not have any password requirements. It is up to the administrator to choose a secure password. There are many articles about strong passwords available on the Internet.

Enable password [<use current password>]: 297FR**tKak3s!

*Accurate system time is essential for monitoring, problem diagnosis, and forensics. Setting up Network Time Protocol (NTP) on the PIX will be referenced later in this paper.

Clock (UTC):
Year [2002]: <enter>
Month [Sep]: <enter>

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Day [29]: <enter>
Time [17:14:37]: <enter>

* As referenced before, the “Inside” IP address will be the interface that resides on the protected network. Enter that address and mask here. Generally, this is a private address that is translated when traversing the PIX to the outside network.

Inside IP address: 192.168.0.1
Inside network mask: 255.255.255.0
Host name: pix1
Domain name: mydomain.com

* The address that is entered here will be the only host that can access the PDM until additional addresses are specified. Under most circumstances, it is recommended that only addresses on the internal network be allowed access to the PDM. The PIX, however, will allow hosts or networks from any interface to access the PDM if it is configured to do so.

IP address of host running PIX Device Manager: 192.168.0.2

* The PIX CLI gives a summary of the information that has been entered and gives the user the option to use the summarized configuration and save it to flash memory. If the configuration appears to be correct, it is safe to let the PIX write it to flash.

The following configuration will be used:
*Enable password: 297FR**tKak3s!*
Clock (UTC): 17:14:37 Sep 29 2002
Inside IP address: 192.168.0.1
Inside network mask: 255.255.255.0
Host name: pix1
Domain name: mydomain.com
IP address of host running PIX Device Manager: 192.168.0.2

Use this configuration and write to flash? y

* This is the user mode prompt that appears. To activate privileged mode, type the enable command and then enter the enable password that was set in the CLI initial configuration:

pix1>
pix1> enable
Password: *****

* When the PIX is in privileged mode, the prompt appears as below (pixname#)
pix1#

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Some newer PIX firewalls ship with the PDM already installed. To verify information about the software loaded on a PIX, use the "show version" command in the CLI. (Make sure the PIX is in privileged mode) The results of this command will show the version of the Cisco PIX software and, if it exists, the version of the PDM. Most often, the PIX firewall will not have the latest operating system and PDM versions out of the box. Fortunately, upgrading each of these is a very simple process using trivial file transfer protocol (TFTP). Updated software files can typically be downloaded from Cisco's website.

Figure 1 shows how to upgrade a PIX to a different version of the operating system and PDM. The example assumes that the 'bin' files of the operating system and PDM versions that are to be installed have been copied to the TFTP server. There are many free TFTP servers available for download, including one from Cisco. Consult the TFTP server documentation for setting the local directory and determining where to copy the PIX 'bin' files.

Figure 1

For this example the following command will upgrade the PIX operating system with the bin file that is named pix_update_file.bin:

```
copy tftp://192.168.0.2/pix_update_file.bin flash:image
```

Next, this command will upgrade the PDM with the bin file named pdm_update file.bin:

```
copy tftp://192.168.0.2/pdm_update_file.bin flash:pdm
```

Again, to verify software versions, use the "show version" command at the CLI. ("Upgrading Software for the Cisco Secure PIX Firewall", 9)

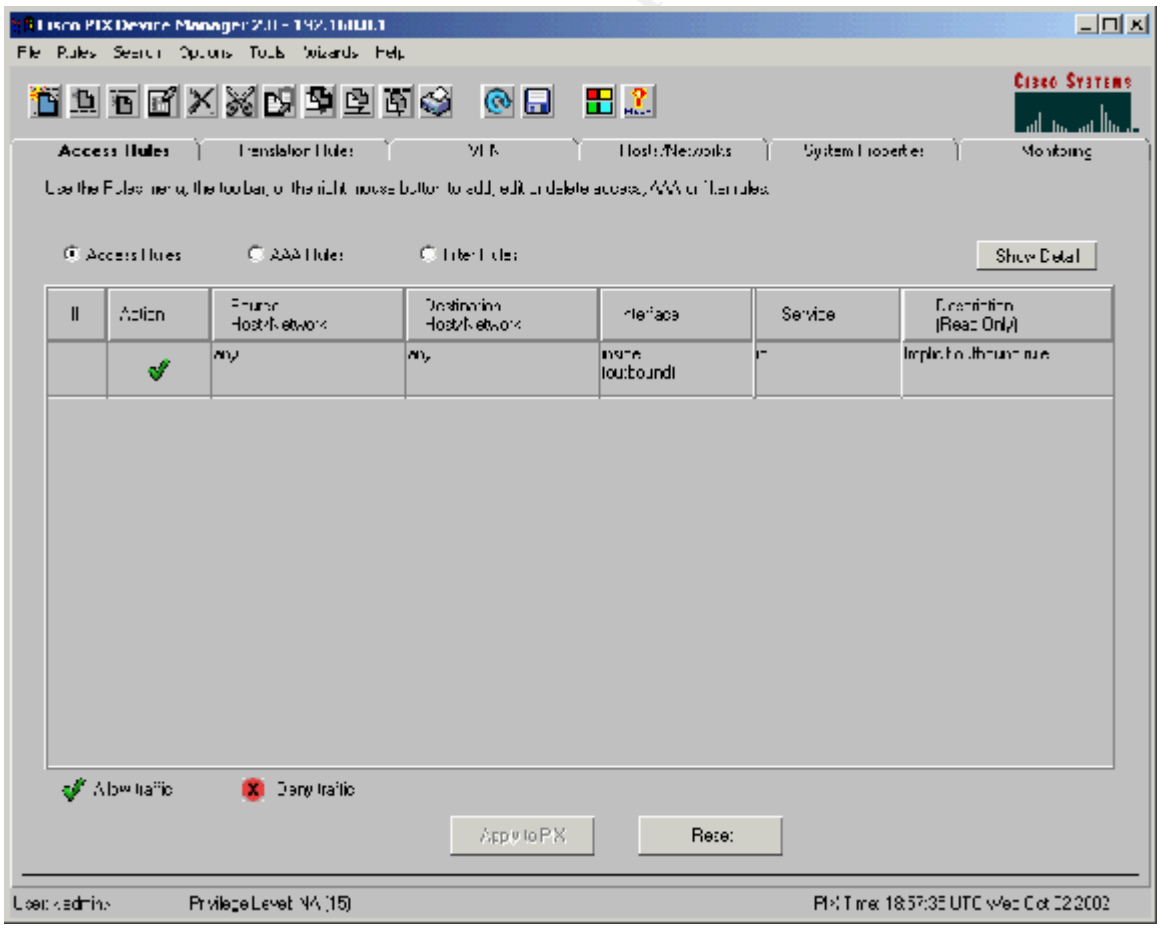
USING THE PDM

The PIX only communicates using SSL, so to access a PIX with an "inside" IP address of 192.168.0.1 using a browser, the URL will be https://192.168.0.1. Browser access is limited to the IP address that was

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

specified in the initial configuration. After connecting, the browser will take several seconds to load the necessary software and will display a security warning. Once this is completed, a prompt will be given for a login name and password. Assuming no user accounts have been created (this will be covered later in the paper), access can be obtained by leaving the username field blank and entering the "enable mode" password that was set up during the initial CLI configuration. Once the applet is loaded and a user is logged in, configuration can begin. The PDM has the look and feel of a standard Widows application. Across the top, drop-down menu items can be found, and within the window there are six tabs. The drop-down menus are File, Rules, Search, Options, Tools, Wizards, and Help. The tabs are Access Rules, Translation Rules, VPN, Host/Networks, System Properties, and Monitoring. Each one of these menus and tabs will be examined briefly with the intent of providing an overview of what is available using the PDM. To completely understand what is happening with specific PDM options, it may prove beneficial to research the underlying CLI commands and consult other documentation. Figure 2 shows the general appearance of the PDM applet.

Figure 2



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

File Menu

There are several options under the file menu. They are as follows:

"Refresh PDM with the Running Configuration on the PIX"

Occasionally when configuring the PIX, it makes sense to use both the PDM and the CLI. This command will do as it implies and read into the PDM latest changes made from the CLI.

"Reset PIX to the Factory Default Configuration"

This option does as it says but also gives the options to re-configure the inside interface so the initial configuration can be avoided.

"Show Running Configuration in New Window"

This opens a browser window and gives the equivalent of a show running-config CLI command.

"Save Running Configuration to Flash"

This is the equivalent to the "write memory" command.

"Save Running Configuration to TFTP Server"

This is a way to back up the PIX configuration file.

"Save Running Configuration to Standby Unit"

This option only applies if the PIX fail-over unit is used.

Rules Menu

This menu that allows insertion of rules will only work on the first three tabs. Generally, the same options are available by right clicking within the window. The options available include the standard copy, cut, and paste operations but also include others. The other operations, "insert before", "insert after", "paste before", and "paste after". This is important to note as access lists are built and expanded upon over time. As with most access lists, the PIX operating system will traverse the list sequentially until a match is found. In addition, the last, implied line is always equivalent to "deny everything". If rules are not exhibiting the intended behavior, the "paste before" and "paste after" options can be particularly useful for troubleshooting.

Search Menu

This menu item provides a tool for searching through access rules. Searches may be performed on the fields within the rules including the host and network addresses. It is not always obvious in rules display area what a rule does and finding a rule in question can be difficult if there is an extensive list. The search feature alleviates this problem. Once the rule in question has been found, double-clicking on it will provide a window that should clarify the properties of the rule.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Options Menu
Under “Options-Preferences”, there is a checkbox to enable the preview of commands before they are sent to the PIX. This is very helpful in learning the commands behind the PDM actions that are executed.

Tools Menu
Under this menu, there is a command line interface window that can be useful when the command that is needed is not available in the PDM. The windows will show the results of the command and has the ability to perform subcommands and multiple-line commands. Ping is an invaluable tool from any network device to help determine the status of connectivity to hosts and networks. Fortunately, under “Tools-Ping”, the PDM gives this option. Those experienced with the PIX CLI will remember that previously the syntax “ping interface-name ip-address” had to be used. In the ping window option, the PIX determine for the user the interface to use for the ping. It does still give the option of selecting an interface using a drop-down menu. Finally, there is a “Service Groups” option in the tools menu that allows grouping of particular types of network traffic access. “Service Groups” can be defined to reduce the number of access lists that are necessary. Consider a scenario where a host needs access to ports 25, 80, and 443. Without a service group, this would have to be defined with three separate access rules. With a service group defined for the three ports, however, it can be done with one access rule and service groups can usually be put together in such a way that allows reuse as the firewall configuration and rules evolve.

Wizards Menu
The VPN wizard greatly simplifies VPN setup and configuration. Configuring VPN connectivity from the CLI requires use of obscure commands that many administrators will not understand. The VPN wizard fixes this by making clear what is happening with VPN setup. The Startup Wizard is a good place to start configuring the PIX. It goes through a dialog that helps set up rules for the networks and hosts that connect to the firewall.

Help Menu
The PDM help menu is a good resource for general PIX configuration information. It also has an option “About Cisco PIX Firewall” that is equivalent to the show version CLI command.

Access Rules Tab
This tab defines access lists that allow or deny different types of traffic based on the information that is given to the PIX. Three kinds of rules can be managed here: access rules, AAA rules, and filter rules. Access rules are the basic rules that allow or deny access to particular hosts or networks. Criteria that can be used are protocols, origin ports, and destination ports. “Service Groups” can be defined to reduce the number of access lists necessary. Authentication, Authorization and Accounting (AAA) rules can also be defined in the access rules tab. Using TACACS+ or RADIUS, the PIX can be configured to require

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

authentication for various services based on hosts or networks. Finally, filter rules can be added to allow or deny traffic based on information further up the protocol stack including ActiveX, Java, and specific URLs.

Translation Rules Tab
This tab allows configuration of network address translation (NAT) and port address translation (PAT). In most cases, dynamic translation occurs from private addressing on an internal network to public addressing on the Internet or static translation occurs from the Internet to a protected resource such as a web server.

VPN Tab
Anyone who has configured a PIX-to-PIX or client-to-PIX VPN will appreciate the VPN feature of the PDM that greatly simplifies configuration and literally enables VPN setup in minutes.

Hosts/Networks Tab
This tab allows the definition and naming of hosts and networks as well as the creation of groups. This can make configuration of access rules much easier than would otherwise be possible.

System Properties Tab
This tab is packed full of functionality that allows configuration of PIX services such as routing, DHCP, NTP, user administration and intrusion detection. All other system properties can be adjusted here as well such as host name, domain name, interface speeds, interface IP addresses, etc… Although detailed description of each option available in the system properties tab is outside the scope of this paper, exploring the options available there is quite informative. In addition to the basic interface information required to make the PIX work on the network, some features that are highly recommended for security are:

- Turn on as much logging as possible. Even if a sophisticated logging product is not available, there are free syslog servers available that will gather logs from the PIX. The logs, combined with the graphs available from the PDM monitoring tools that will be examined later, should provide an accurate picture of what is happening with the PIX firewall.
- Decide how to limit remote access to the PIX. Secure Shell access can be configured here and in most cases is the only recommended means of remote access beyond the PDM. Telnet, by its nature, will pass unencrypted information, including usernames and passwords over the network.
- Create user accounts with the appropriate level of access. Accounts created here grant access to the PIX through telnet, Secure Shell, and the PDM, assuming that these services have been configured on the PIX. Some administrators may need view-only access, which limits PDM access to the monitoring tab. To turn on this type of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

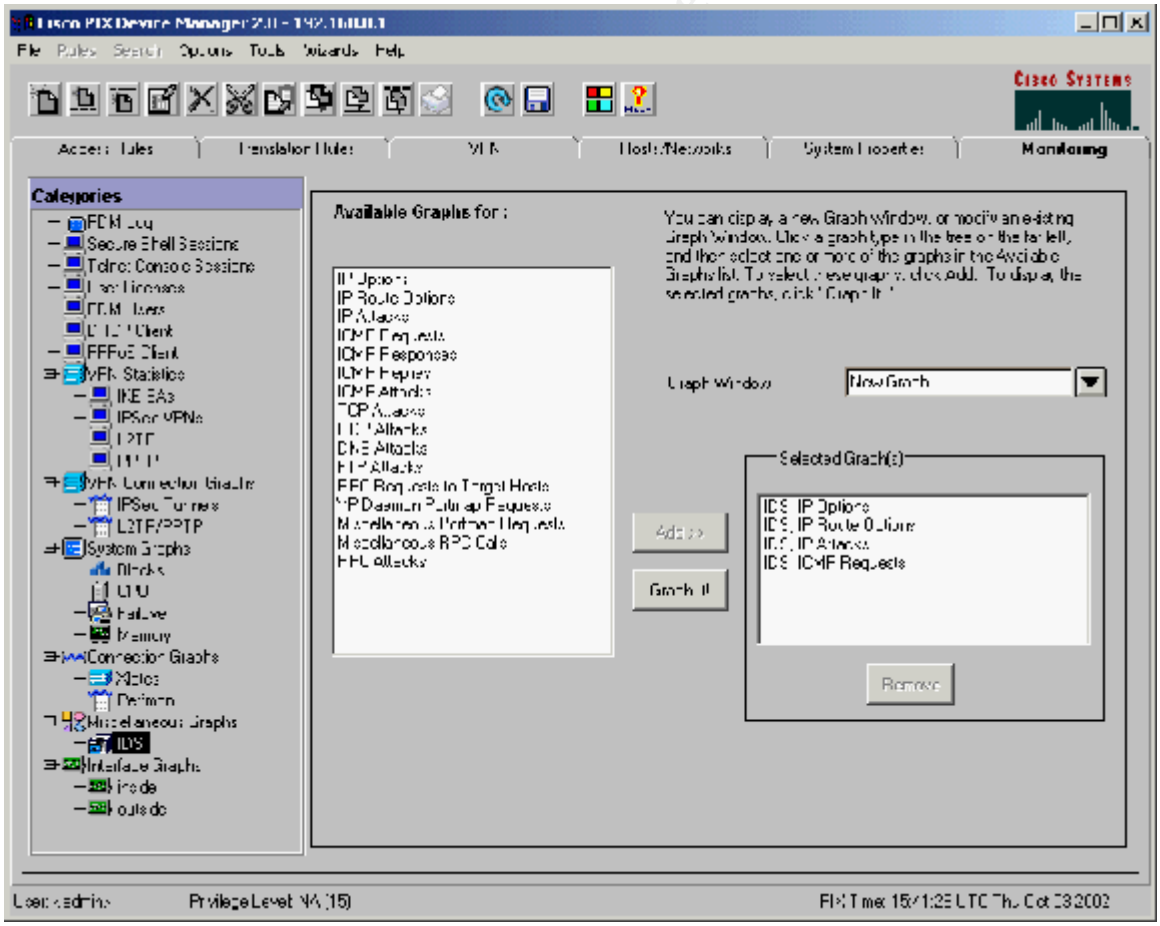
authorization, the “Enable Authorization” checkbox must be checked in the “Authentication/Authorization” window within the system properties tab.

– The level of IDS level may be overwhelming depending upon characteristics of the network traffic encountered by the PIX. Once an understanding of the regular traffic patterns on the network has been developed, scaling the level of IDS signatures may be advisable.

Monitoring

The monitoring tab offers a wealth of information to help understand what is happening on the PIX. Available information includes the PDM log, secure shell sessions, telnet console sessions, user licensing, DHCP clients, PPoE clients, and VPN statistics. Graphs are available for system information, connections, IDS, and interface information. Figure 3 shows what options are available.

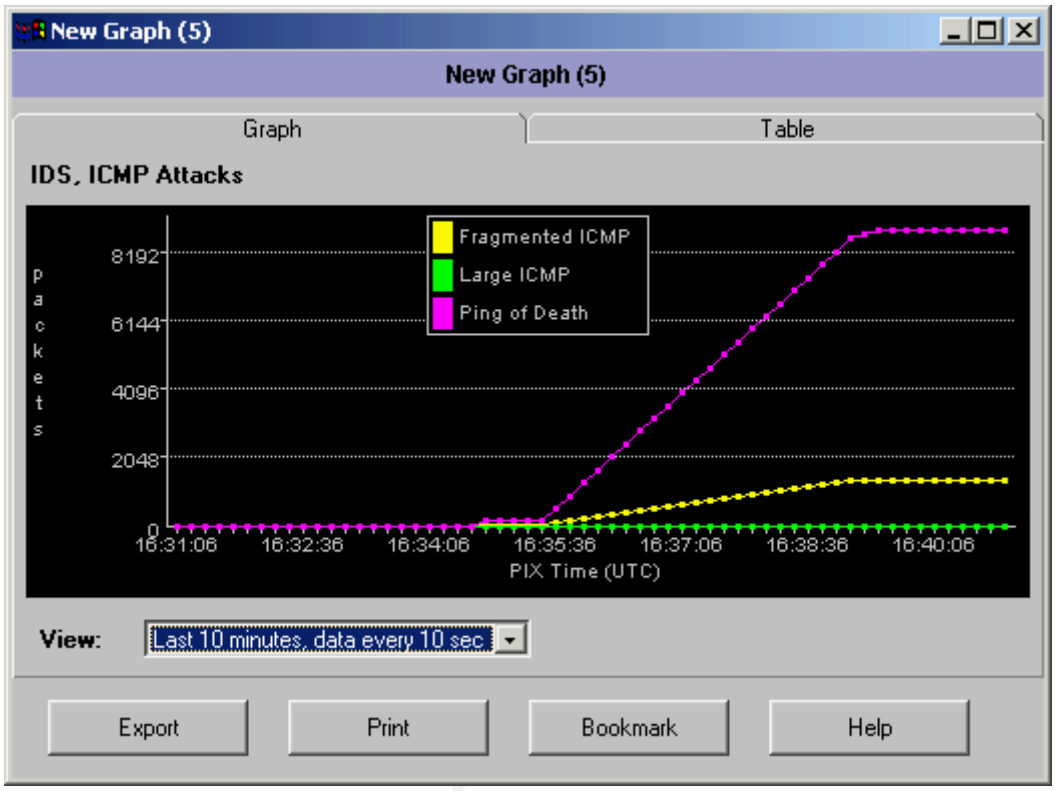
Figure 3



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Up to four graphs can be displayed at once. To do so, select the desired graphs, click the “Add” button, and then click the “Graph It!” button. Figure 4 shows an example of the ICMP attacks IDS graph.

Figure 4



CONCLUSION

Hopefully this overview and walkthrough of the Cisco PDM will prove to be beneficial information and ease the fear of using a GUI configuration tool for a device that has traditionally used only a CLI. As configuration options become easier to understand and implement for the masses, security is improved. Because of this, the Cisco PDM can help make a network more secure while providing an effective tool to configure, manage and monitor Cisco PIX firewalls.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

RESOURCES

"Cisco PIX Device Manager Data Sheet". 2001. URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pixdm_ds.pdf

"Cisco Announces Next Generation Graphical Interface for Security and Virtual Private Network (VPN) Products". 10 April 2001. http://newsroom.cisco.com/dlls/prod_041001.html

"System Requirements". Cisco PIX Device Manager Installation Guide, Version 2.0. URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/pdm_ig/pdm_star.pdf

"Installing PDM on a PIX Firewall". Cisco PIX Device Manager Installation Guide, Version 2.0. URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_62/pdm_ig/pdm_inst.pdf

"Troubleshooting PIX Device Manager". 21 May 20002. URL: http://www.cisco.com/warp/public/110/pdm_http404.pdf

"Upgrading Software for the Cisco Secure PIX Firewall". 27 November 2002. URL: http://www.cisco.com/warp/public/110/upgrade.pdf

Barkley, John. "Introduction to Firewalls". Security in Open Systems. 1994. URL: http://csrc.nist.gov/publications/nistpubs/800-7/node155.html

"Design the firewall system". 1 July 1999. URL: http://www.cert.org/security-improvement/practices/p053.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**