Global Information Assurance Certification Paper

Cisco Pix: Logging and beyond

Ben Carlsrud

Assignment Version 1.2f

September 26, 2001

It's 12:30 am… Do you know who's breaking into your network?

Introduction

That line or something similar gets used a lot in the security field, but it is very relevant. The first step in any implementation of connecting a local network to the internet is the installation of a firewall to protect the internal network. Once the firewall is in place and configured, how do you know who is knocking at your door? In most installations of a perimeter defense there is usually additional configuration that needs to be done to establish a good logging/monitoring policy. After the implementation of your firewall and security policy, setting up the logging/monitoring of the traffic is the most important step.

The logging/monitoring that is done now will help catch and analyze current traffic plus give the ability to trend and analyze any previous history.

This document will present a "how to" on logging of a Cisco Pix Firewall version 6.1. It will show how to implement logging via a SYSLOG locally and remotely (VPN Solution). It will also discuss some of the logging that can be done with the Cisco Pix Device Manager (PDM) which is a graphical utility that is supported by Cisco Pix Firewall version 6.0(1) and above. For a broader overview of the Cisco Pix Firewall, refer to http://www.sans.org/infosecFAQ/firewall/PIX.htm.

The main reason for writing this paper is to create a clear and concise configuration guide for logging of the Cisco Pix Firewall. This document assumes familiarity with working with the Cisco Pix Firewall. Most importantly before making any changes to the current security configuration, be sure you have authorization to do so.

Pix Logging Methods

The Cisco Pix supports multiple logging/monitoring methods. The real time methods are logging to a SYSLOG server, the console screen (when connected to the console port), the telnet screen, and/or a SNMP manager. The SYSLOG server and SNMP manager are the only methods that are able to save the logs. The PDM allows a user to configure how large of a cache to hold and then be able to display what has already happened in a graphical window.

The Cisco Pix currently is not Open Platform for Secure Enterprise Connectivity (OPSEC) compliant. *OPSEC integration enables products to work together in the most efficient manner to both simplify configuration, monitoring, and tracking, and at the same time provide the highest level of performance and availability. Excerpt from*

http://www.checkpoint.com/opsec/factsheet.html. This means you will not be able to use OPSEC compliant software to integrate with the Cisco Pix Firewall.

SYSLOG

SYSLOG is a method of logging/monitoring that has been around for a long time. When activity happens that is meant to be logged, messages are sent from a client (firewall) to the configured SYSLOG server over UDP port 514 and/or TCP port 1468. The SYSLOGD software running on the SYSLOG server then determines what to do with the logged traffic. Depending on the capabilities of the SYSLOG server software it could just log the information or send an alert via email, pager, and SNMP trap or just simply discard it. For an explanation of a SYSLOG on a UNIX server refer to http://www.sans.org/infosecFAQ/UNIX/syslog.htm and for logging concepts http://www.sans.org/infosecFAQ/securitybasics/logging.htm.

Initial Logging Setup

The first step in configuring the Cisco Pix for logging is to turn logging on, which is accomplished by entering the following command at the config prompt:

Logging on

From here you need to determine how you are going to log your traffic and to what level.

There are seven security levels for logging on the Cisco Pix Firewall.

	KEYWORD	Level	
•	Emergency	0	System Unusable (Not Used - UNIX Only)
•	Alert	1	Immediate Action Needed
•	Critical	2	Critical Condition
•	Error	3	Error Condition
•	Warning	4	Warning Condition
•	Notification	5	Normal but significant condition
•	Informational	6	Informational message only
•	Debug	7	Appears during debugging only

There are actually eight levels displayed but level zero is not used although it is still represented. Many of the logging commands require that you specify a severity level to indicate which SYSLOG message can be sent to SYSLOG server. The lower the severity level number, the more severe the error. The default severity level is 3 (error). The Severity level can be specified as either a number or a keyword. The level specified causes the Cisco PIX Firewall to send messages of that level or lower to the SYSLOG server. If you specify severity level 3, the Pix Firewall sends severity level 1, 2, and 3 messages to the SYSLOG server.

To enable logging at the console, enter the following command the config prompt:

Logging console

To enable logging at a telnet session, enter the following command the config prompt:

Logging Monitor

To be able to view the history of the log at the console monitor or telnet session, enter the following command the config prompt:

Logging Buffered *Severity_Level*

Configuring Local Logging

To enable logging to a SYSLOG server that is internal or connected to a DMZ, enter the following command at the config prompt:

Logging trap severity_level
Logging host [*interface*] *ip_address* [*protocol/port*]

Ex. Logging trap 7
Logging host inside 10.0.0.1

The logging trap command sets the level of severity of the SYSLOG messages. The logging host interface uses the name of the interface given during setup of the firewall. The protocol/port option is in case the SYSLOG server is configured on a different protocol and port versus the default UDP port 514 and TCP port 1468.

Configuring Logging to a remote SYSLOG server with a VPN connection

Many times in a multi-site environment there will be a centralized SYSLOG server that will be receiving messages from remote hosts from across the Internet. If the Cisco Pix Firewall is configured to send to the remote SYSLOG server, there needs to be some additional configuration to be sure the logging/monitoring is secure. SYSLOG messages are not encrypted, they are clear text and anybody with a sniffer could start looking at the packets. If someone did a port sweep they would be able to find the SYSLOG port was open and then trace that back to the SYSLOG server, thus utilizing a possible exploit against the UDP or TCP port. For example http://www.ciac.org/ciac/bulletins/j-023.shtml describes an old exploit against Cisco SYSLOG daemon.

There a two ways to secure traffic with only one of those actually encrypting the traffic. The first being creating access lists to allow only SYSLOG messaging to be setup between specific hosts, the firewall and the SYSLOG server, but this doesn't prevent the packets

from being sniffed. The best solution would be to implement a VPN connection in conjunction with access lists.

The following configuration creates a VPN connection to the firewall utilizing IKE Mode Configuration, Wildcard Pre-Shared Key and the VPN Client 3.0 (This client and VPN solution work for the Windows platform only).

Configure Address Pool (Address scheme not currently implemented on network) for connecting clients:
ip local pool SYSLOG 10.5.0.1-10.5.0.1(restricted to 1 address)

Enable IKE:
isakmp enable outside

Specify the authentication method within the IKE policy:
isakmp policy 20 authentication pre-share

Specify the encryption algorithm (The 3DES is if you purchased the 3DES software upgrade otherwise it would just be des):
isakmp policy 20 encryption 3des

Specify the hash algorithm:
isakmp policy 20 hash md5

Used for VPN Client 3.x:
isakmp policy 20 group 2

Configure a wildcard, pre-shared key:
isakmp key "PresharedSecret" address 0.0.0.0 netmask 0.0.0.0

define the ISAKMP identity the PIX Firewall uses when participating in the IKE protocol:
isakmp identity address

References IP address local pools (created above) to IKE with "SYSLOG" as the pool-name:
isakmp client configuration address-pool local SYSLOG outside

Transform set that defines how the traffic will be protected:
crypto ipsec transform-set SYSLOGSET esp-3des esp-md5-hmac

Create a dynamic crypto map:
crypto dynamic-map dynmap 4 set transform-set SYSLOGSET

Add the dynamic crypto map set into a static crypto map set:
crypto map sys 20 ipsec-isakmp dynamic dynmap

Apply the crypto map to the outside interface:
crypto map sys interface outside

Now Create your VPN Group.

Define Address's for VPN Group:
vpngroup SYSLOGPix address-pool SYSLOG

Enable Split DNS:
vpngroup SYSLOGPix split-tunnel 101

Define Idle Time Out (Make large to maintain connection):
vpngroup SYSLOGPix idle-time 18000

Define VPN Group Password for Client:
vpngroup SYSLOGPix password *"Password"*

Create an access list that defines the PIX Firewall local network(s) requiring IPSec protection:
access-list 101 permit ip 10.1.0.0 255.255.0.0 10.5.0.0 255.255.0.0

Access lists that define what the VPN clients are authorized to use (SYSLOG Ports):
access-list 100 permit TCP 10.5.0.0 255.255.0.0 10.1.0.0 255.255.0.0 eq 1468
access-list 100 permit UDP 10.5.0.0 255.255.0.0 10.1.0.0 255.255.0.0 eq 514

Configure NAT 0 - The Nat 0 command lets you exempt traffic that is matched by the access-list command statements from the NAT services. Adaptive Security remains in effect with the nat 0 access-list command.
nat (inside) 0 access-list 101

Tell PIX Firewall to implicitly permit IPSec traffic:
sysopt connection permit-ipsec

Configure SYSLOG Host:
logging host outside 10.5.0.1

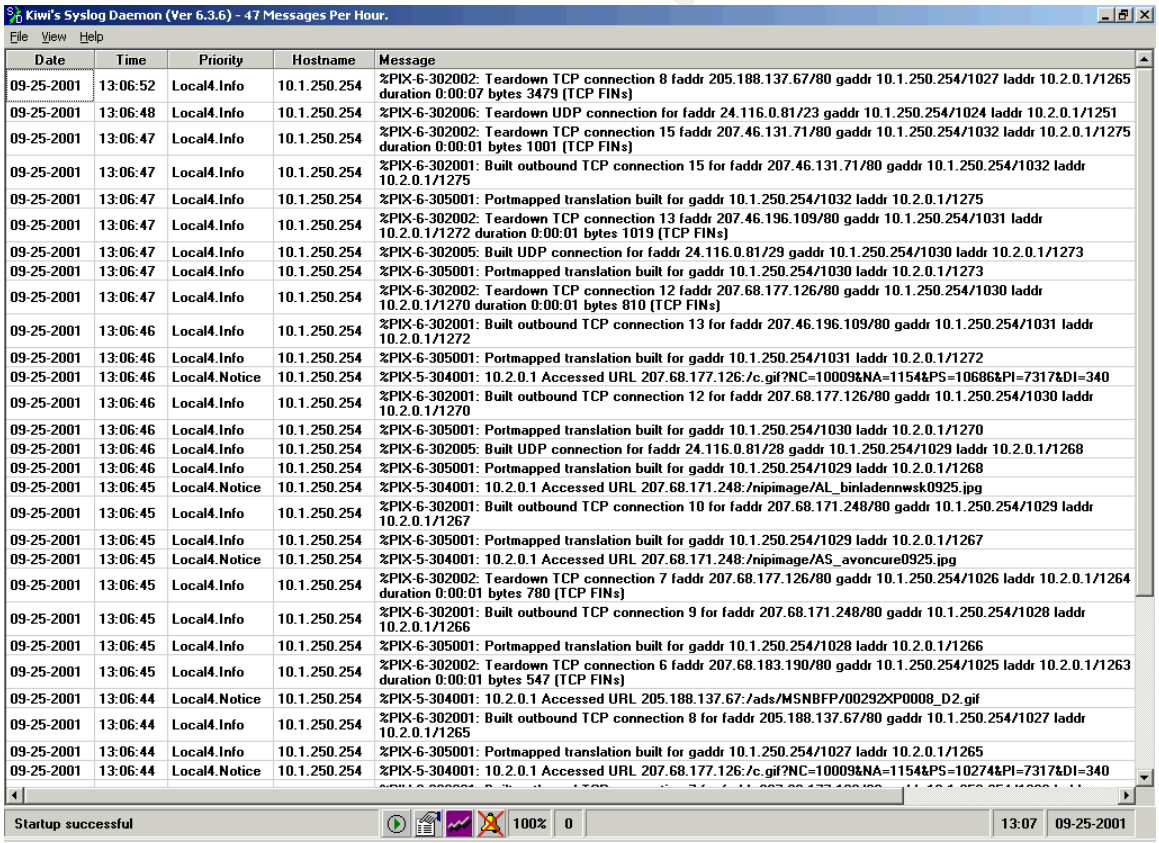
That sets up the Cisco Pix Firewall to accept an incoming VPN connection for SYSLOG monitoring. This only one method of VPN connectivity, for more information on setting the VPN connection refer to http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/basclnt.htm. The next step would be to configure the Cisco VPN Client 3.x for this connection using the corresponding VPN group name and password.

Setting Up and Monitoring SYSLOG

Once the logging has been configured it is now time to setup the SYSLOG server. There are many SYSLOG servers from which to choose. There are SYSLOG daemons for UNIX, LINUX, Windows 95/98, NT4.0, 2000, XP and just about any other operating system on the market. One example would be Kiwi's SYSLOG Daemon for Windows and NT which can be obtained from http://www.kiwi-enterprises.com/software_downloads.htm. Depending on what kind of functionality that is desired in the SYSLOG Daemon will determine what SYSLOG Daemon is used. Evaluate software to find the one that provides the functionality desired.

Most SYSLOG Daemons dump the messages to a log file for archival processes. A 3rd party utility will probably be desired to combine and read the logs. Kiwi also has a utility that reads logs, called Kiwi's CATTOOLS, which can be downloaded from the same location as above.

Below is a screen shot showing how the SYSLOG messages appear in the Kiwi SYSLOG Daemon.



Date	Time	Priority	Hostname	Message
09-25-2001	13:06:52	Local4.Info	10.1.250.254	%PIX-6-302002: Teardown TCP connection 8 faddr 205.188.137.67/80 gaddr 10.1.250.254/1027 laddr 10.2.0.1/1265 duration 0:00:07 bytes 3479 (TCP FINs)
09-25-2001	13:06:48	Local4.Info	10.1.250.254	%PIX-6-302006: Teardown UDP connection for faddr 24.116.0.81/23 gaddr 10.1.250.254/1024 laddr 10.2.0.1/1251
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-302002: Teardown TCP connection 15 faddr 207.46.131.71/80 gaddr 10.1.250.254/1032 laddr 10.2.0.1/1275 duration 0:00:01 bytes 1001 (TCP FINs)
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-302001: Built outbound TCP connection 15 for faddr 207.46.131.71/80 gaddr 10.1.250.254/1032 laddr 10.2.0.1/1275
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1032 laddr 10.2.0.1/1275
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-302002: Teardown TCP connection 13 faddr 207.46.196.109/80 gaddr 10.1.250.254/1031 laddr 10.2.0.1/1272 duration 0:00:01 bytes 1019 (TCP FINs)
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-302005: Built UDP connection for faddr 24.116.0.81/29 gaddr 10.1.250.254/1030 laddr 10.2.0.1/1273
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1030 laddr 10.2.0.1/1273
09-25-2001	13:06:47	Local4.Info	10.1.250.254	%PIX-6-302002: Teardown TCP connection 12 faddr 207.68.177.126/80 gaddr 10.1.250.254/1030 laddr 10.2.0.1/1270 duration 0:00:01 bytes 810 (TCP FINs)
09-25-2001	13:06:46	Local4.Info	10.1.250.254	%PIX-6-302001: Built outbound TCP connection 13 for faddr 207.46.196.109/80 gaddr 10.1.250.254/1031 laddr 10.2.0.1/1272
09-25-2001	13:06:46	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1031 laddr 10.2.0.1/1272
09-25-2001	13:06:46	Local4.Notice	10.1.250.254	%PIX-5-304001: 10.2.0.1 Accessed URL 207.68.177.126:/c.gif?NC=10009&NA=1154&PS=10686&PI=7317&DI=340
09-25-2001	13:06:46	Local4.Info	10.1.250.254	%PIX-6-302001: Built outbound TCP connection 12 for faddr 207.68.177.126/80 gaddr 10.1.250.254/1030 laddr 10.2.0.1/1270
09-25-2001	13:06:46	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1030 laddr 10.2.0.1/1270
09-25-2001	13:06:46	Local4.Info	10.1.250.254	%PIX-6-302005: Built UDP connection for faddr 24.116.0.81/28 gaddr 10.1.250.254/1029 laddr 10.2.0.1/1268
09-25-2001	13:06:46	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1029 laddr 10.2.0.1/1268
09-25-2001	13:06:45	Local4.Notice	10.1.250.254	%PIX-5-304001: 10.2.0.1 Accessed URL 207.68.171.248:/nipimage/AL_binladennwsk0925.jpg
09-25-2001	13:06:45	Local4.Info	10.1.250.254	%PIX-6-302001: Built outbound TCP connection 10 for faddr 207.68.171.248/80 gaddr 10.1.250.254/1029 laddr 10.2.0.1/1267
09-25-2001	13:06:45	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1029 laddr 10.2.0.1/1267
09-25-2001	13:06:45	Local4.Notice	10.1.250.254	%PIX-5-304001: 10.2.0.1 Accessed URL 207.68.171.248:/nipimage/AS_avoncure0925.jpg
09-25-2001	13:06:45	Local4.Info	10.1.250.254	%PIX-6-302002: Teardown TCP connection 7 faddr 207.68.177.126/80 gaddr 10.1.250.254/1026 laddr 10.2.0.1/1264 duration 0:00:01 bytes 780 (TCP FINs)
09-25-2001	13:06:45	Local4.Info	10.1.250.254	%PIX-6-302001: Built outbound TCP connection 9 for faddr 207.68.171.248/80 gaddr 10.1.250.254/1028 laddr 10.2.0.1/1266
09-25-2001	13:06:45	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1028 laddr 10.2.0.1/1266
09-25-2001	13:06:45	Local4.Info	10.1.250.254	%PIX-6-302002: Teardown TCP connection 6 faddr 207.68.183.190/80 gaddr 10.1.250.254/1025 laddr 10.2.0.1/1263 duration 0:00:01 bytes 547 (TCP FINs)
09-25-2001	13:06:44	Local4.Notice	10.1.250.254	%PIX-5-304001: 10.2.0.1 Accessed URL 205.188.137.67:/ads/MSNBFP/00292XP0008_D2.gif
09-25-2001	13:06:44	Local4.Info	10.1.250.254	%PIX-6-302001: Built outbound TCP connection 8 for faddr 205.188.137.67/80 gaddr 10.1.250.254/1027 laddr 10.2.0.1/1265
09-25-2001	13:06:44	Local4.Info	10.1.250.254	%PIX-6-305001: Portmapped translation built for gaddr 10.1.250.254/1027 laddr 10.2.0.1/1265
09-25-2001	13:06:44	Local4.Notice	10.1.250.254	%PIX-5-304001: 10.2.0.1 Accessed URL 207.68.177.126:/c.gif?NC=10009&NA=1154&PS=10274&PI=7317&DI=340

The information above was logged in debug mode so you can see that depending on the security level selected can create quite a huge log so be sure the server has plenty of disk space. How can you monitor all this traffic that you are logging? That is up to the SYSLOG daemon software that is in use. Each message has its own severity level so the

SYSLOG Daemon could be setup to watch for specific messages and then send an alert to a specified user.

Cisco Pix Device Manager Logging

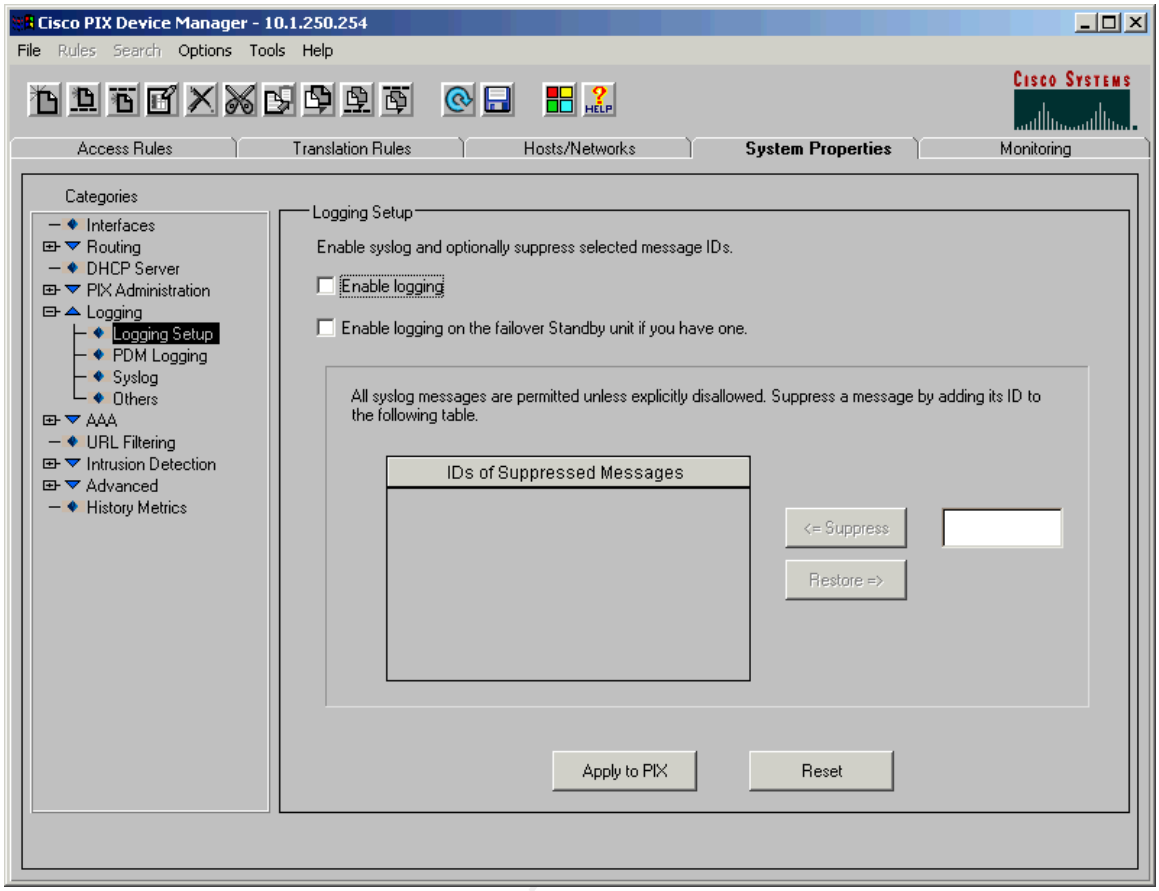
The Cisco Pix Device Manager is a graphical utility that allows you to configure the Cisco Pix Firewall, which is included with all Pix firewalls versions 6.0(1) and above. This utility was created to cut down on mistakes entered at the console, and as can be seen from above that would be very easy. The PDM is fairly limited in the scope of what it can configure. For example, you cannot setup or manage a VPN connection with the PDM so the configuration from above would still need to be entered in at the config prompt.

Within the PDM you can configure all types of logging versus manually entering the commands at the config prompt. The first screen shot below shows the initial setup of logging of the Cisco Pix Firewall through the PDM. To access the PDM be sure that it is enabled and then **https** to the address of the Cisco Pix Firewall.

To turn on the PDM issue the following command at the config prompt:
http ***ipaddress netmask interfacename***

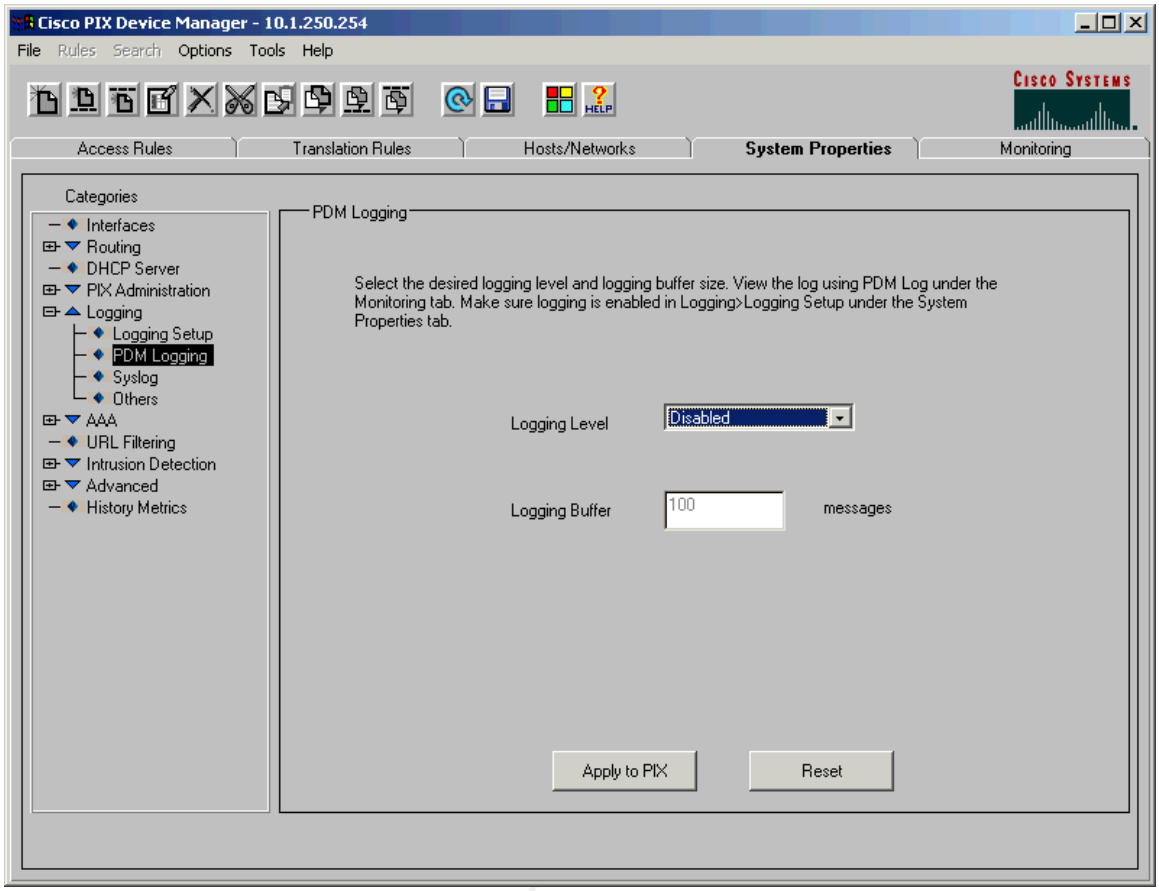
The ip address can be a host/network and depending on which interface the host/network is attached to will be the interface specified. There can be multiple entries for this command.

Ex. http 10.1.0.0 255.255.0.0 inside (Network)
http 201.111.11.1 255.255.255.255 outside (Host)



To enable logging:
Select the System Properties tab across the top
Select Logging from the window on the left
Select Logging Setup from the window on the left
Check the Enable Logging checkbox
Select the Apply to Pix Button (do this before changing screens)

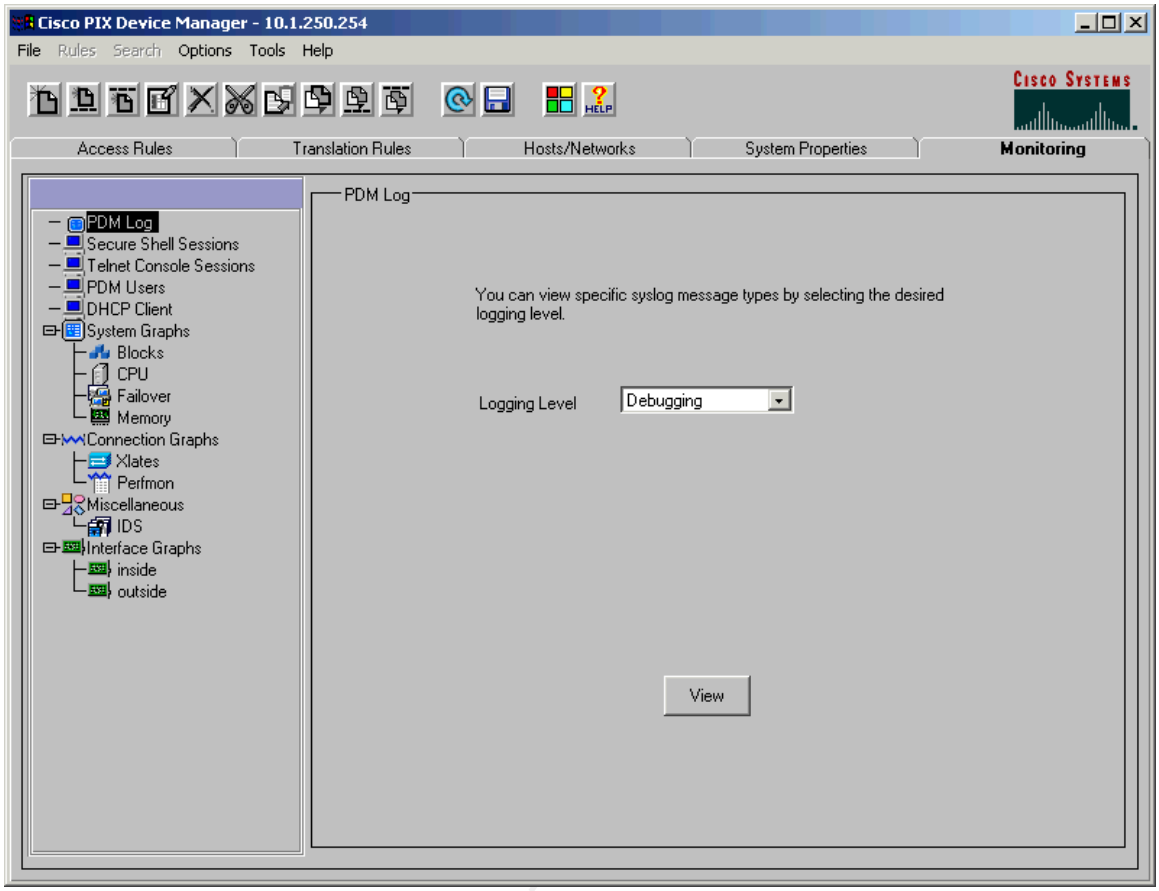
The **Enable logging** must be enabled before any kind of logging can be viewed.

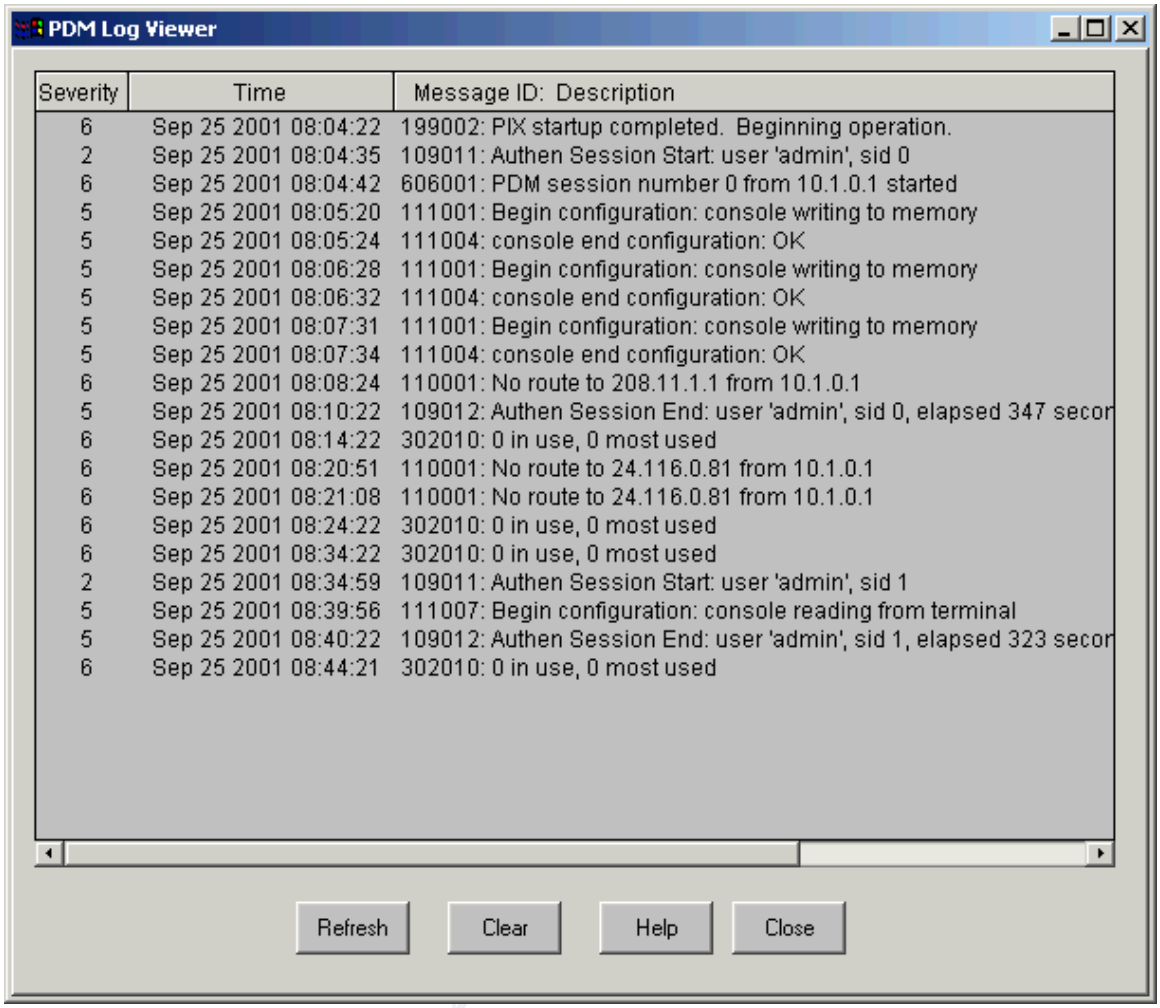


To be able to view the logs from within the PDM:
Select the System Properties tab across the top
Select Logging from the window on the left
Select PDM Logging from the window on the left
Select the logging level desired (this is just for the PDM and not the SYSLOG)
Select the Apply to Pix Button (do this before changing screens)

Once that is done you can then:
Select the Monitoring Tab from the top
Select PDM Log from the window on the left
Select from the drop down list what severity to view *(This is equal to or less than what was selected on the previous page)*
Select View

This will display the following two windows:





Decoding the Logging

After the Cisco Pix Firewall and the SYSLOG Daemon are setup messages will start appearing at the SYSLOG server. The messages can be kind of cryptic so one must learn how to decode what shows up on the screen. The following is an excerpt taken from the Cisco Pix Firewall 6.1 Documentation which can be found at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/syslog/pixemint.htm#xtocid1342911.

System log messages received at a SYSLOG server begin with a percent sign (%) and are structured as follows:

%PIX-Level-Message_number: Message_text

"PIX" identifies the message facility code for messages generated by the PIX

Firewall.Level reflects the severity of the condition described by the message. The lower the number, the more severe the condition. Logging is set to level 3 (error) by default.

Message_number is the numeric code that uniquely identifies the message. The

explanation of the Message Numbers can be found at http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/syslog/pixemapa.htm#25608.

Message_text is a text string describing the condition. This portion of the message sometimes includes IP addresses, port numbers, or usernames. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/syslog/pixemint.htm#41237 lists the variable fields and the type of information in them.

Example Message
%PIX-5-304001: 10.2.0.1 Accessed URL 207.46.226.17:/selfupd.cab

We can see this came from a Pix with severity level 5 (pretty low), message number 304001 which states "This is an FTP/URL message. This message is logged when the specified host successfully accesses the specified URL.", and what URL is being accessed.

Conclusion

Logging of the traffic coming in and out of the firewall is the single most important task that needs to be done after setting up the firewall. As can be seen, this sometimes appears to be an overwhelming task but a very crucial step in securing the network. Continuous monitoring of the SYSLOG Daemon and of the firewall needs to be done to make sure that the logging/monitoring is current and working.

Now that the logging/monitoring is setup when asked the question, "**Its 12:30 am… Do you know who's breaking into your network?**" you can answer… "**Maybe**".

References

"Cisco PIX Firewall System Log"
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/syslog/pixemsgs.htm

"Cisco IOS SYSLOG Denial-of-Service Vulnerability"
http://www.ciac.org/ciac/bulletins/j-023.shtml

"Kiwi Enterprises"
http://www.kiwi-enterprises.com/software_downloads.htm

"Variable Fields in Cisco Syslog Messages"
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/syslog/41237

"Configuring Cisco VPN Remote Access"
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_61/config/basclnt.htm