Cisco 6.3 Log Sizing

Tips for Sizing:

1. Locate the pix log and Perl script in the same directory.
   1a. When prompted to enter a file name type the name of the file only without a path.

Script: pixcount.pl
Description: This script provides a number of different counts.
a. Total Count of Events
b. Total Count by Pix Severity (Severity 1-7)
c. Total Count for Security Related Events
Usage: perl pixcount.pl
Usage Notes: The script will prompt for a file name. Provide a file name and wait for script to finish. If the pix log is large, please be patient. For example, a 100Mb pix log will take approximate 1 Min 30 Seconds on an IBM T41. The security events were chosen out of all events based on their relevance to a security analyst. The script can be modified to include or exclude events from the security report table.

Output:

Cisco Pix 6.3 Report

All Events	
Description	**Quantity**
Deny protocol reverse path check from source_address to dest_address on interface interface_name :	49119
Dropping echo request from IP_address to PAT address IP_address:	2
Deny IP spoof from IP_address to IP_address on interface interface_name:	46
Deny IP teardrop fragment size = number, offset = number from IP_address to IP_address:	2
Authen Session Start user user , sid number :	176
Deny inbound No xlate string:	83
Outbound static identity portmap regular translation creation failed for protocol src interface_name source_address source_port dst interface_name dest_address dest_port:	8
Deny protocol src interface_name source_address source_port dst interface_name dest_address dest_port type string , code code by access_group acl_ID:	3132748
decaps rec d IPSEC packet has invalid spi for destaddr=dest_address, prot=protocol, spi=number:	323
identity doesn t match negotiated identity ip dest_address= dest_address, src_addr= source_address, prot= protocol, ident local=inside_address, remote=remote_address, local_proxy=IP_address IP_address port port, remote_proxy=IP_address IP_address port port :	9923
Rec d packet not an IPSEC packet ip dest_address= dest_address, src_addr= source_address, prot= protocol :	113
PPP virtual interface interface_name, user user missing MPPE key from aaa server:	2
Received ARP request response collision from IP_address mac_address on interface	9

interface_name, page 2-62:	
FTP port command low port IP_address port to IP_address on interface interface_name:	5
FTP port command different address IP_addressIP_address to IP_address on interface interface_name:	2
UDP DNS packet dropped due to domainname length check of 255 bytes actual length n bytes, page 2-70 :	3003
Invalid transport field for protocol=protocol, from source_address source_port to dest_address dest_port :	536

Totals by Severity	
Severity 1 Alert Events:	49119
Severity 2 Critical Events:	226
Severity 3 Error Events:	91
Severity 4 Warning Events:	3146664
Total Events:	**3196100**

Security Related Totals	
Description	**Quantity**
Deny protocol reverse path check from source_address to dest_address on interface interface_name	49119
Dropping echo request from IP_address to PAT address IP_address	2
Deny IP spoof from IP_address to IP_address on interface	46
Deny IP teardrop fragment (ize = number, offset = number from IP_address to IP_address	2
Deny inbound No xlate string	83
Total Security Events:	**49252**