Logging in PIX Firewall

Introduction

This article was written based on Cisco PIX 501

Cisco firewalls have seven logging levels:

0. emergencies
1. alerts
2. critical
3. errors
4. warnings
5. notifications
6. informational
7. debugging

Logging in Cisco devices work in the following way:
when you set logging to the fifth level messages from levels 0 to 5 are also logged.
The lower the number is the fewer details there are, but which level we should use depends on our needs and the network environment. In my opinion in ordinary circumstances the best option is to set the level to 4 or 5.
Level seven should be used only while solving problems as it can decrease the performance of the device.
Each log can be presented in two formats: default and EMBLEM
Default format includes:
Time stamp – Device ID – Message ID – Message text

- Time stamp – default none
- Device ID – default None(possible options: hostname, context,ip address or text string)
- Message ID – it consists of %PIX, %ASA or %FWSM string followed by logging level and six-digit message number
- Message text – event description

EMBLEM is used for Syslog Analyzer and it is available only to UDP Syslog servers.

TIMESTAMP

It is a good practice to configure timestamp in logging messages. You can do this by typing logging timestamp
Default behavior is no timestamp.

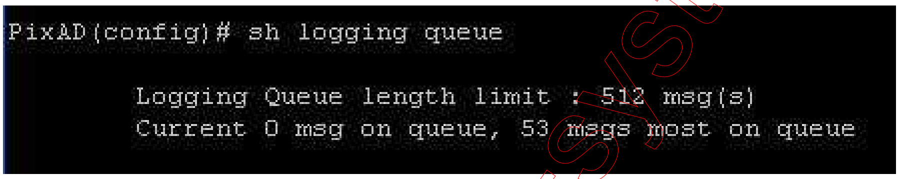
SYSLOG

It is the best option for logging information. Of course we need Syslog server such as the one on UNIX/Linux or Kiwi - free syslog server on Windows .
Normally Cisco devices send events via 514 UDP port.
There is a possibility of changing the port to ,e.g. 514 TCP or others but TCP can decrease the performance, so be carefull.
Before starting logging enable it, because by default logging is disabled

When using pix it can be done by typing logging on.
Set up logging level
logging trap level
If preferable set up identification in syslog messages. It is useful when logging more than one device.
logging device-id X, where X stands for hostname, ip interface or string
Configure syslog server
logging host interface ip_address protocol/port format emblem
,e.g. logging host inside 192.168.2.2 that means all messages are sent to syslog server 192.168.2.2 via udp on 514 port.
Warning!!!
Configuring logging via tcp connection you have to know that in case the connection with syslog server is broken firewall stops forwarding traffic. To enable it you have to manually configure syslog server again even though the former one is online.
Typing show logging you will see that the syslog server is disabled.

QUEUE

Another very important parameter is logging queue. The default value is 512 messages.
If messages are generated faster than they are sent to the syslog server the firewall starts to drop messages
To check how big your queue size is type sh logging queue



```
PixAD(config)# sh logging queue

        Logging Queue length limit : 512 msg(s)
        Current 0 msg on queue, 53 msgs most on queue
```

This picture shows that the average speed generated by the system is 53 and there is no problem with sending them. However, if the value …msgs most on queue is equal or higher than 512 it means that firewalls drops messages.
You can adjust the queue size manually by typing logging queue queue_size
The queue_size can range from 0 to 8192 messages, but when you set 0 it means an unlimited size(up to available memory).

FACILITY

Default facility in PIX is 20 known as a Local4. We can change it by typing:
logging facility facility_number
Facility can range from 0 to 23, e.g.9(cron), 2(mail). In normal environment there is no need to change it.

CONSOLE

This method is not advisable. If applied it should not be used for a prolonged period of time, only for testing rather than analyzing.
When setting up console logging side effects may occur. You can lose control over the devices due to an extensive number of messages.
Enabling logging to console is performed by typing: logging console <level>

SSH, TELNET

This method may encounter similar problems to the ones which may occur utilizing the console method.. We enable it by command:

```
logging monitor <level>
```

To see messages on screen in the current session type: terminal monitor

BUFFER

Instead of briefly using ssh,telnet or console for logging you can use buffer for collecting interesting information. Buffer uses 4096 bytes of memory to store the most recent messages. You enable buffer logging by typing: logging buffered<level>

SNMP

If we want to send logs via snmp traps we have to enable it:

```
snmp-server enable traps
```

Set up snmp-server and interface which will be used to send traps

```
snmp-server host interface_name  ip_address trap
```

Configure level of messages

```
logging history level
```

STANDBY

In active/passive failover environment only active firewall generates messages.
If you wish to collect messages by both firewalls you can do this typing:
logging standby ,
However, you have to be aware that this solution duplicates each information sent by firewall but in case of problems with active firewall all messages are still available for logging because of queuing them in passive firewall.

dzbanek