HP Virus Throttle for Linux©: Installing, Configuring, and Monitoring white paper

Abstract

This paper describes how HP Virus Throttle technology is used to diminish the replication of fast spreading worms and viruses that evade antivirus software. Virus Throttle can detect and slow down the malicious code based on its behavior, giving IT personnel more time to respond to the infection. Representing a different paradigm in the battle against malicious code Virus Throttle mitigates harm to other systems, rather than focusing on the harm already done to an individual server. This technology is now available for HP ProLiant servers running Linux® as part of the very affordable ProLiant Essentials Intelligent Networking Pack – Linux Edition.

Introduction

Many scoff when "Linux" and "virus" are used in the same sentence, yet there are around a hundred Linux viruses in existence today[1]. The Stoag virus was the first Linux virus reported 1996[2]. It has been followed by many others such as the Slapper, Bliss, Lindose, Ramen, and Typot viruses just to name a few. HP Labs tested the HP Virus Throttle technology against the "SQL Slammer" worm as it wreaked havoc on the Internet in February 2003, and found it reduced the virus' spread to a crawl in just two-tenths of a second[3]

Traditional virus scanning solutions - which often rely on existing virus signatures provided by third parties - can be ineffective at protecting against new viruses that often spread in seconds. The HP Virus Throttle technology provides a new approach to worm virus protection and works in concert with current antivirus server solutions to give protection against both known and unknown worm viruses.

The main symptom of a worm virus infection is that an infected server attempts to quickly connect to many other computers, whereas uninfected servers typically make fewer connections more slowly. The HP Virus Throttle technology actively monitors computer communications. When it detects a server attempting to make rapid connections to other servers, it automatically limits the number of connections the infected system makes while simultaneously notifying administrators of the virus-like activity. It buys time for the administrators to investigate the system and bring it offline until the virus can be identified and a remedy established.

HP Virus Throttle technology: stealth defense against malicious code in the Microsoft environments[4] provides an excellent overview of the HP Virus Throttle technology.

How Virus Throttle works

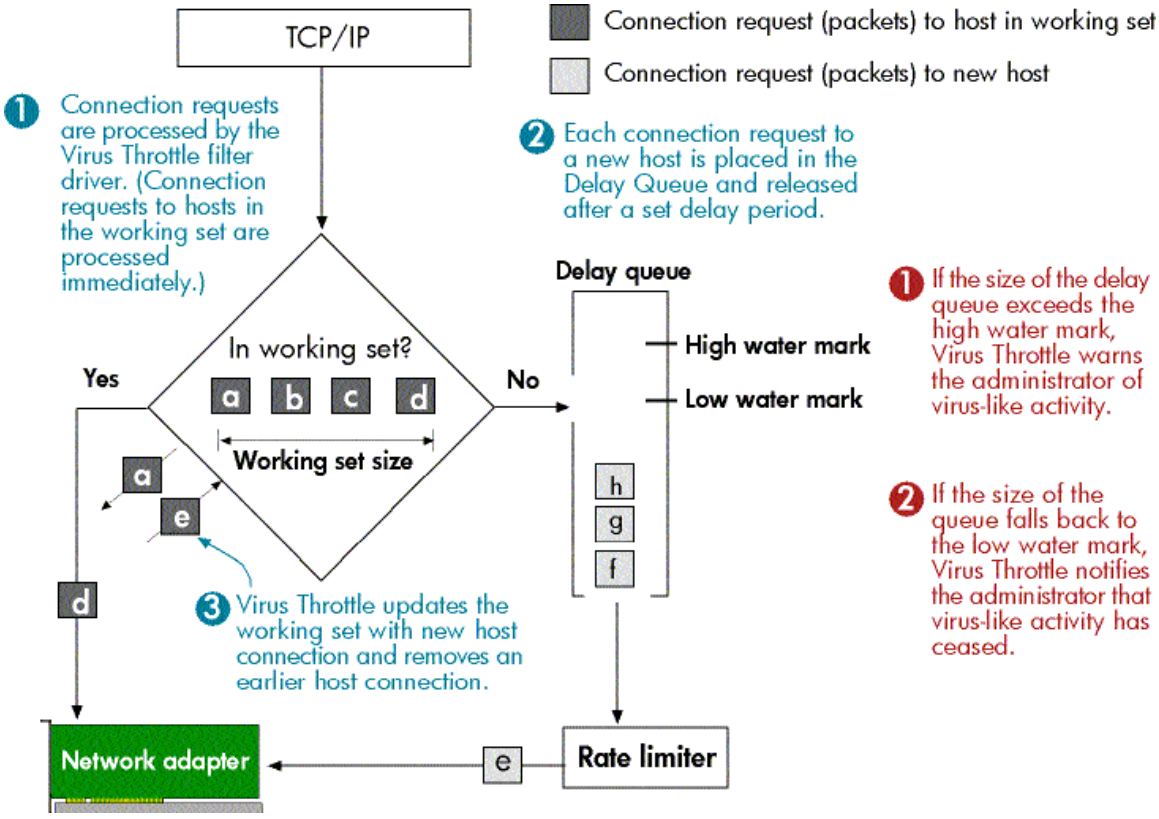
Virus Throttle technology limits the rate of TCP connections to new computers without interfering with the normal operation of the machine. The diagram below depicts when a connection request is made and shows how Virus Throttle compares the destination host for the data packet to a working set of recently contacted hosts. If the destination host is listed in the working set, all packets to that host are processed immediately. If the destination host is not listed in the working set, the packets are sent to a delay queue. The packets in the delay queue are released and processed at regular

[1] *Mainstream means more malicious code for Linux* http://searchsecurity.techtarget.com/qna/0,289202,sid14_gci955041,00.html
[2] Staog: First Linux Virus http://en.wikipedia.org/wiki/Staog
[3] *Immune System for Computers Throttles Viruses* http://www.hpl.hp.com/news/2003/jan_mar/throttling.html
[4] *HP Virus Throttle technology: stealth defense against malicious code in the Microsoft environments* can be found at: http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00369532/c00369532.pdf

intervals as determined by a rate limiter. The rate limiter guarantees that no more than one host address per time interval (set by the administrator) is processed. When a packet is processed to a new destination host, all other packets to the same host are processed.

If the frequency of requests to new hosts is higher than the pre-set frequency of the rate limiter, the size of the delay queue may rise to a pre-set threshold, or high water mark. If this occurs, Virus Throttle logs an event to inform the administrator of virus-like activity. If the HP ProLiant Insight Management NIC Agents are installed on the system, SNMP traps may also be sent. If the size of delay queue drops below the low water mark, Virus Throttle logs and event indicating that virus-like activity has stopped.

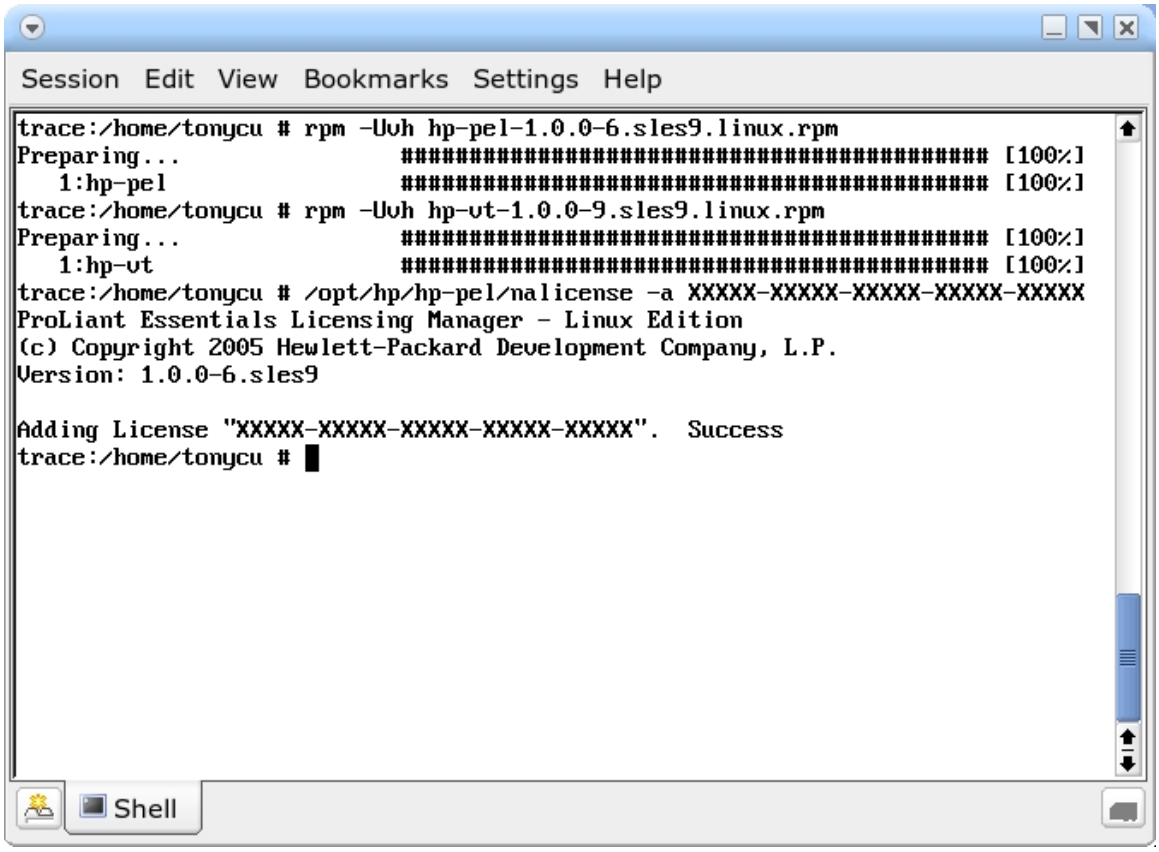
Figure 1: How virus throttling works



Installation

The following screen shot shows the installation process of the Virus Throttle package. The HP Linux ProLiant Essentials License Manager package (`hp-pel`) is a prerequisite to installing the HP Virus Throttle package (`hp-vt`).

Figure 2: Virus Throttle installation



Configurable parameters

The configuration file, hp-vt.conf, is located in the `/etc/opt/hp/hp-vt` directory. The configurable parameters are documented in the configuration file and provided here for reference.

host_working_set_size

The number of known host to which connections are established without delay. When a new connection is made, the oldest member of the working set is replaced with the new host. The default is 5 hosts and the valid range is 1 to 100 inclusive.

delay_queue_delay_seconds

The rate at which the oldest connection request is removed from the delay queue (and all other connection requests to that same host) and passed down the protocol stack. The default is 1 second and the valid range is 1 to 10 seconds inclusive.

delay_queue_size

The maximum number of delayed connection requests in the delay queue. When the queue is full, connection requests are dropped. The default is 200 delayed connection requests and the valid range is 10 to 1000 inclusive.

delay_queue_high_watermark

The number of connection requests in the delay queue at which "virus-like" activity is considered to be occurring for each instance of the filter driver. The default is 160 connection requests and the valid range is 8 to delay_queue_size inclusive.

delay_queue_low_watermark

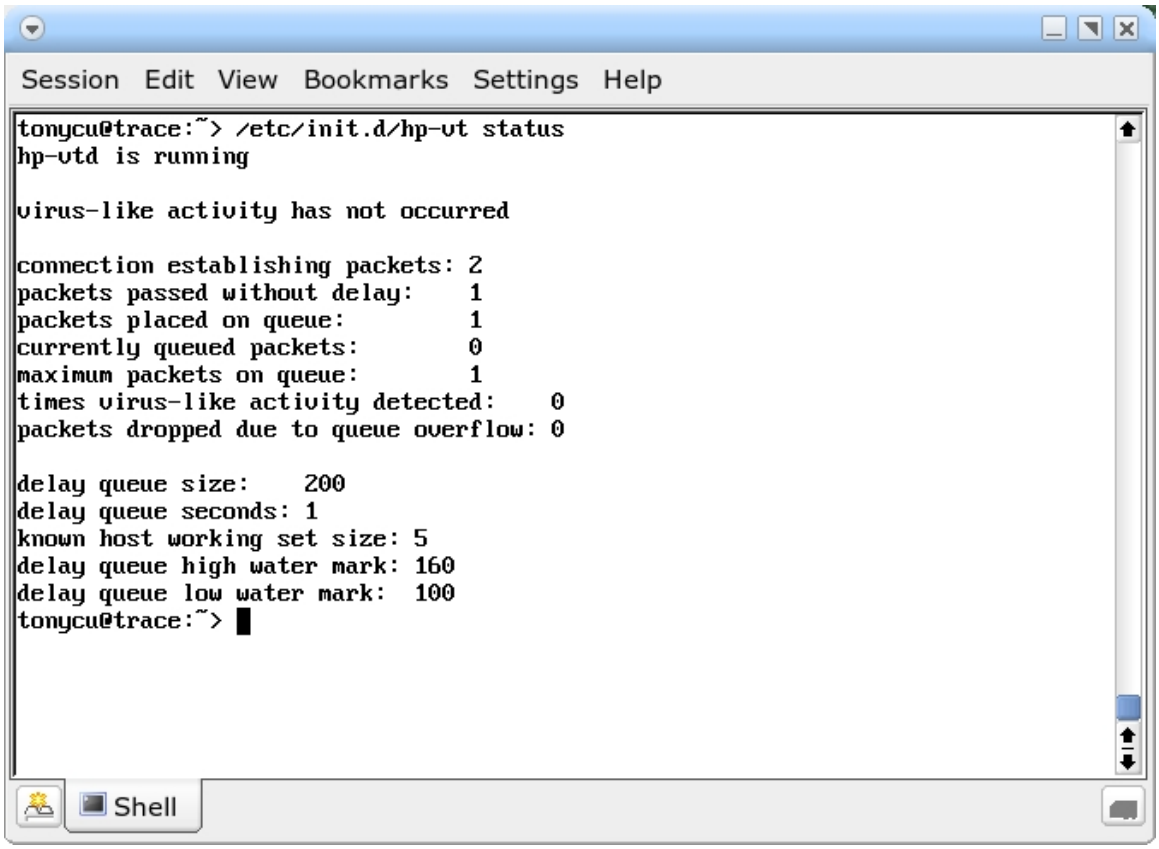
The number of connection requests in the delay queue below which "virus-like" activity is considered to be stopped. The default is 100 connection requests and the valid range is 4 to (*delay_queue_high_watermark* minus 4) inclusive.

Current status and configuration

The current HP Virus Throttle status and configuration can be obtained by running:

/etc/init.d/hp-vt status

Figure 3: Current status and configuration



The following information is reported (in relation to the last time HP VT was started):

The virus-like activity status is reported as:

virus-like activity has not occurred

Meaning no "virus-like" activity is currently detected and none has been detected.

virus-like activity is currently occurring

Meaning "virus-like" activity is currently detected.

virus-like activity has occurred in the past

Meaning no "virus-like" activity is currently detected, but "virus-like" activity has been detected in the past.

The following statistics are reported:

connection establishing packets

The number of connection packets seen.

packets passed without delay

The number of connection packets that were passed without a delay because the target was a known host.

packets placed on queue

The number of connection packets put on the delay queued.

packets removed from queue

The number of connection packets removed from the delay queue.

currently queued packets

The number of connection packets currently on the delay queue.

maximum packets on queue

The maximum number of packets on the delay queue at any point since HP VT was last started.

times virus-like activity detected

The number of times "virus-like" activity was detected.

packets dropped due to queue overflow

The number of packets that were dropped due to the delay queue being full.

Configuring HP Virus Throttle

The following steps outline one method of configuring the HP Virus Throttle.

1. Set the host_working_set_size to the number of hosts the server simultaneously makes connections to under normal circumstances.
2. Set the delay_queue_delay_seconds to the number of seconds you desire between servicing the delay queue.
3. Set delay_queue_size and delay_queue_high_watermark to the maximum value.
4. Set the delay_queue_low_watermark to eighty.

The initial parameters are:

host_working_set_size=4

delay_queue_delay_seconds=3

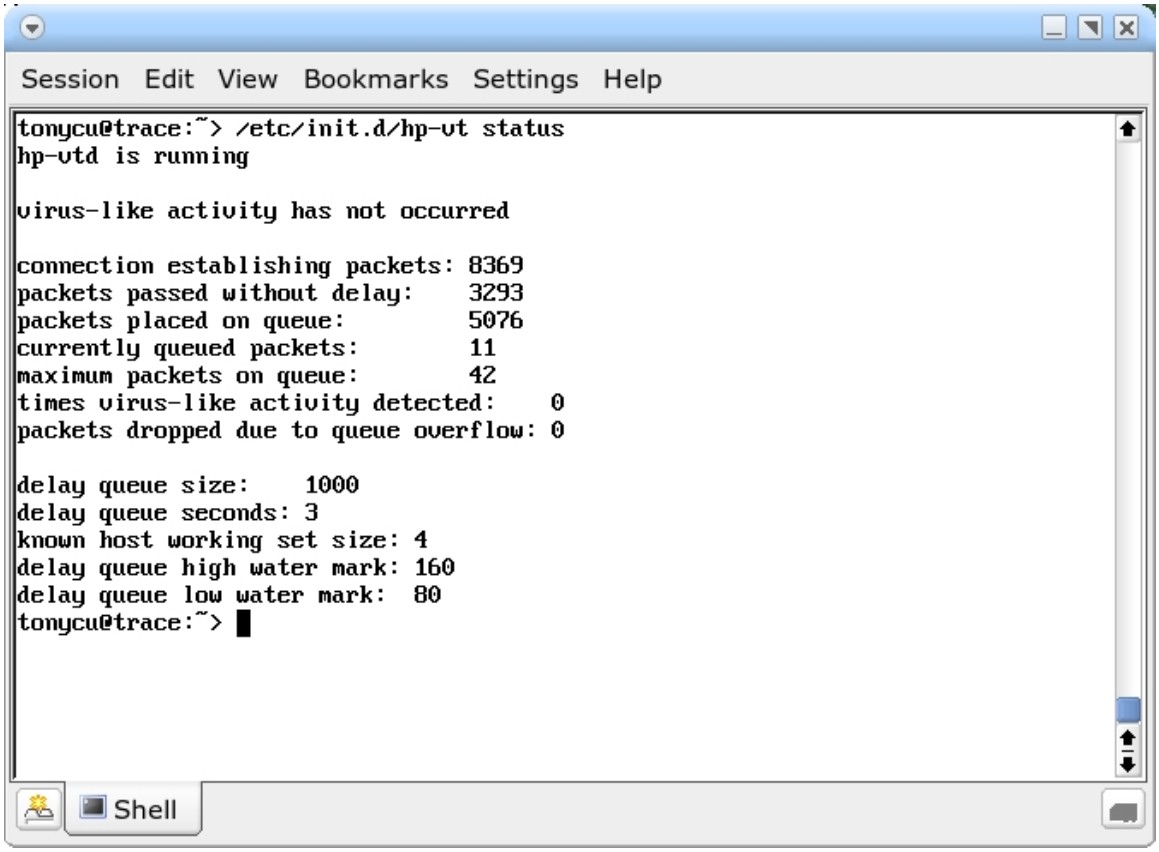
delay_queue_size=1000

delay_queue_high_watermark=160

delay_queue_low_watermark=80

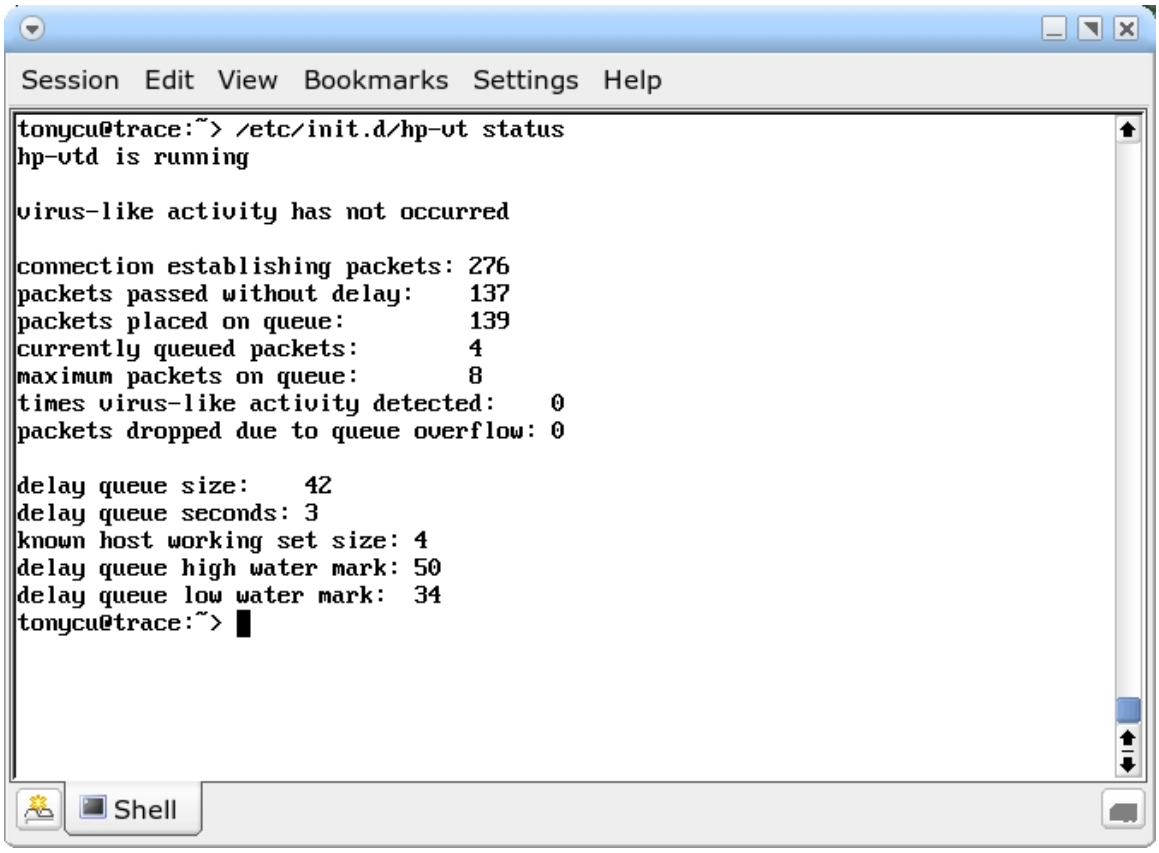
Setting the delay_queue_size to 1000 reduces the possibility of dropping connection requests under normal conditions during the configuration process. Setting the delay_queue_high_watermark to 160 reduces false “virus-like” activity messages. After some time the status reports:

Figure 4: HP Virus Throttle configuration with reduced possibility of dropped connection requests and false virus-like activity messages



The maximum number packets ever concurrently on delay queue is 42. In this case we double the value and assign it to delay_queue_size. The value is increased by twenty percent and assigned to the delay_queue_high_watermark and decreased twenty percent and assigned it to delay_queue_low_watermark. After restarting HP Virus Throttle, the following configuration is reported:

Figure 5: Virus Throttle configuration after altering queue parameters and restarting



The configuration should periodically be checked to ensure proper settings are maintained over time. The following command may be useful for continually monitoring the status during the configuration phase.

watch -d -n 1 /etc/init.d/hp-vt status

Log File Format and Monitoring

HP Virus Throttle messages are logged to `/var/opt/hp/hp-vt/hp-vt.log`.

Log Message Format

Log messages are logged in the following format.

[TAG] SP [DATE] SP TEXT

TAG is one of:

ALERT_VLA_DETECTED

To indicate virus-like activity detected.

ALERT_VLA_STOPPED

To indicate virus-like activity has stopped.

DROPPING_CONNECTIONS

To indicate connections are being dropped. After this event is logged, it will not be logged again until the low water mark is reached.

ERROR

To indicate errors, such as out of range configuration parameters in hp-vt.conf.

WARNING

To indicate warnings, such as not being able to load the ip6_queue module.

INFO

To indicate informative events, such as HP LVT starting and stopping.

SP is one or more spaces.

DATE is the current date stamp in the following format:

Thu Feb 10 12:54:35 CST 2005

TEXT is free form text which may or may not exist in every message.

Lines that do not start with a tag are a continuation of the previous line. A few sample lines are provided below.

```
[INFO]                  [Thu Feb 10 10:34:15 CST 2005] hp-vt started
[ALERT_VLA_DETECTED]    [Thu Feb 10 12:54:35 CST 2005]
[INFO]                  [Thu Feb 10 12:54:36 CST 2005]
  first text line of second info message
  second text line of second info message
[ALERT_VLA_STOPPED]     [Thu Feb 10 12:54:58 CST 2005]
```

Monitoring log messages using SWATCH

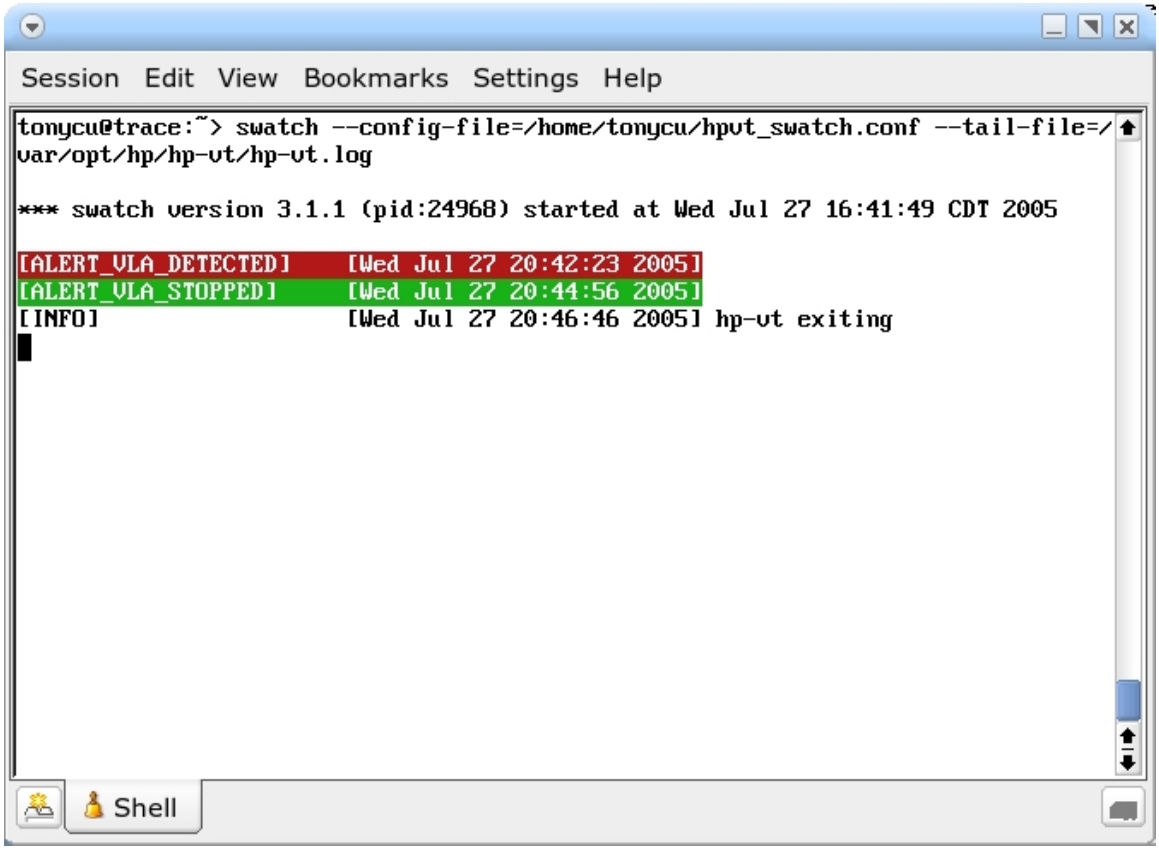
The Simple WATCHer[5] is a utility that monitors log files for particular events and notifies administrators in various ways when those events occur. This sample configuration file should be customized to meet your specific requirements. SWATCH is a useful utility during the Virus Throttle configuration phase.

```
watchfor /^\[INFO\]/
  echo=black
watchfor /^\[WARNING\]/
  bell
  echo yellow
  mail addresses=tonycu\@localhost,subject="hp-vt warning"
  exec "xmessage hp-vt warning"
watchfor /^\[ERROR\]/
  bell
  echo red reverse
  mail addresses=tonycu\@localhost,subject="hp-vt error"
  exec "xmessage hp-vt error"
watchfor /^\[ALERT_VLA_DETECTED\]/
  bell 3
  echo red blink reverse
  mail addresses=tonycu\@localhost,subject="hp-vt VLA DETECTED"
  exec "xmessage hp-vt vla stopped"
watchfor /^\[ALERT_VLA_STOPPED\]/
  bell
  echo green reverse
  mail addresses=tonycu\@localhost,subject="hp-vt VLA STOPPED"
  exec "xmessage hp-vt vla stopped"
watchfor /^\[DROPPING_CONNECTIONS\]/
  bell
  echo blue blink
  mail addresses=tonycu\@localhost,subject="hp-vt dropping connections"
  exec "xmessage hp-vt error"
```

This configuration file sends email notifications for specific events and colors the events for easy visual identification as shown below.

[5] For more information about Simple WATCHer, refer to http://sourceforge.net/projects/swatch/

Figure 6: Sample SWATCH output

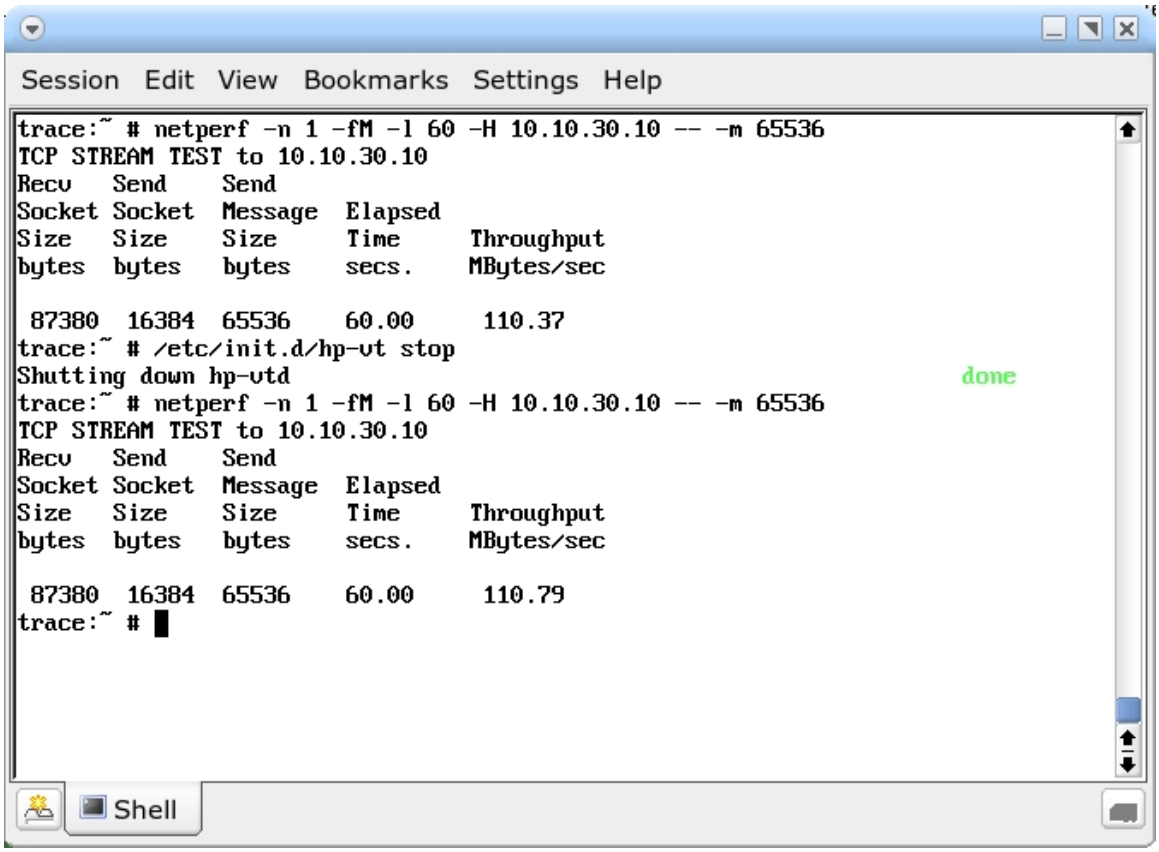


Performance

The performance overhead of HP Virus Throttle was measured using Netperf[6]. The target host was loaded in the `known_hosts` lists by making a connection before the test was started. The Virus Throttle overhead was 0.37% for this particular test.

[6] For information about the Netperf Performance Tool, refer to http://www.netperf.org/

Figure 7: Sample NetPerf performance output



Conclusion

Like it or not, viruses on Linux are becoming more prevalent. Knowing virus like activity is occurring moments after infection is often more useful than knowing what virus has infected the server. This early virus detection is a necessity for large and small organizations alike.

HP Virus Throttle technology is a different paradigm from signature based antivirus approaches by identifying malicious code based on its network behavior. Traditional approaches rely on having to identify the virus itself, often only possible after a new virus has already infected an entire network. As such, Virus Throttle seeks to prevent such programs from leaving the server, instead of preventing them from entering.

Because Virus Throttle is triggered by the behavior of a virus, it can handle unknown threats without waiting for signature updates and patches. Virus Throttle allows the network infrastructure to stay up and running by slowing traffic from servers that exhibit high connection rates. Virus Throttle provides event logging and SNMP traps if the HP ProLiant Insight Manager NIC Agents are utilized. Most significantly, HP Virus Throttle gives system administrators more time to proactively react before the problem escalates to a crisis.

For more information

For more information and other white papers about HP ProLiant network adapters, go to this web page: http://h18004.www1.hp.com/products/servers/networking/whitepapers.html

For information about how to purchase an HP ProLiant Essential Intelligent Networking Pack license, go to the HP website at http://h18004.www1.hp.com/products/servers/proliantessentials/inp/index.html or contact your HP reseller.

For additional information about virus throttling, refer to the following:

- *Virus Throttling* white paper by HP Labs, UK at http://www.hpl.hp.com/techreports/2003/HPL-2003-69.pdf
- *Resilient Infrastructure for Network Security* white paper from HP Labs, UK at http://www.hpl.hp.com/techreports/2002/HPL-2002-273.html
- *Implementing and testing a virus throttle* white paper from HP Labs, UK at http://www.hpl.hp.com/techreports/2003/HPL-2003-103.pdf

© 2003 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Itanium is a trademark or registered trademark of Intel Corporation in the U.S. and other countries and is used under license.

C00432867, 09/2005

invent