OPNSense Perf tweaking

Sunday, 21 March 2021 6:54 PM

The biggest impact was from the Flow Control (FC) setting. FC is a level 1 layer adding pause frames before the data is transmitted. My assumption is Netmap has issues with FC which causes the dropped connections. Recommendations from many sources, including Cisco, suggest disabling FC altogether and let the higher levels handle the flow. There are exceptions, but these usually involve ESXi, VMware and other special applications.

I have done all my testing using an Intel i350T4 and i340T4, common NICs used for firewalls, in 4 different systems and, by the way, neither NIC had any performance advantage. I have tested these system for 5 days without any down links experienced after the changes were made. Without these changes every system was plagued with down WAN links and poor performance using the default settings.

Do not use this file if you are not using an igb driver. igb combined with other drivers is ok as long as you have at least one igb NIC, and I recommend you use the igb for all WAN interfaces.

Add the file below in the '/boot' folder and call it 'loader.conf.local' right besides 'loader.conf'. I use WinSCP, in a Windows environment, as a file manager to get easy access to the folders. Don't forget to Enable Secure Shell. I have tried using the 'System Tunables' in the WebGUI to add these settings. Some worked and some didn't using that method. Not sure why. Better to just add this file. If you're a Linux guru, I am not, then use your own methods to add this file.

The two most **IMPORTANT** things to insure is that power management be disabled in the OPNsense settings and also in the BIOS settings of the system (thanks wefinet). And the second is to disable flow control (IEEE 802.3x) on all ports. It is advisable to not connect an IPS interface to any device which has flow control on. Flow control should be turned off to allow the congestion to be managed higher up in the stack

Please test all tunables in a test environment before you apply to a production system.

```
# File starts below this line, use Copy/Paste ######################
# Check for interface specific settings and add accordingly.
# These ae tunables to improve network performance on Intel igb driver NICs

# Flow Control (FC) 0=Disabled 1=Rx Pause 2=Tx Pause 3=Full FC
# This tunable must be set according to your configuration. VERY IMPORTANT!
# Set FC to 0 (<x>) on all interfaces
hw.igb.<x>.fc=0 #Also put this in System Tunables hw.igb.<x>.fc: value=0

# Set number of queues to number of cores divided by number of ports. 0 lets FreeBSD decide
hw.igb.num_queues=0

# Increase packet descriptors (set as 1024,2048, or 4096) ONLY!
# Allows a larger number of packets to be processed.
# Use "netstat -ihw 1" in the shell and make sure the idrops are zero
# If the NIC has constant disconnects, lower this value
# if not zero then lower this value.
hw.igb.rxd="2048" # For i340/i350 use 2048
hw.igb.txd="2048" # For i340/i350 use 2048
net.link.ifqmaxlen="4096" # value here equal sum of above values. For i340/i350 use 4096

# Increase Network efficiency
```

hw.igb.enable_aim=1

# Increase interuppt rate
hw.igb.max_interrupt_rate="64000"

# Network memory buffers
# run "netstat -m" in the shell and if the 'mbufs denied' and 'mbufs delayed' are 0/0/0 then this is not needed
# if not zero then keep adding 400000 until mbufs are zero
kern.ipc.nmbclusters="1000000"

# Fast interrupt handling
# Normally set by default. Use these settings to insure it is on.
# Allows NIC to process packets as fast as they are received
hw.igb.enable_msix=1
hw.pci.enable_msix=1

# Unlimited packet processing
# Use this only if you are sure that the NICs have dedicated IRQs
# View the IRQ assignments by executing this in the shell "vmstat -i"
# A value of "-1" means unlimited packet processing
hw.igb.rx_process_limit="-1"
hw.igb.tx_process_limit="-1"
##
File ends above this line

##UPDATE 12/12/2017##
After testing I have realized that some of these settings are NOT applied via loader.conf.local and must be added via the WebGUI in System>Settings>Tunables. I have moved these from the file above to this list.
Add to Tunables

Disable Energy Efficiency - set for each igb port in your system
This setting can cause Link flap errors if not disabled
Set for **every** igb interface in the system as per these examples
dev.igb.0.eee_disabled: value=1
dev.igb.1.eee_disabled: value=1
dev.igb.2.eee_disabled: value=1
dev.igb.3.eee_disabled: value=1

IPv4 Fragments - 0=Do not accept fragments
This is mainly need for security. Fragmentation can be used to evade packet inspection
net.inet.ip.maxfragpackets: value=0
net.inet.ip.maxfragsperpacket: value=0

Set to 0 (<x>) for every port used by IPS
dev.igb.<x>.fc: value=0

##UPDATE 1/16/2018##
Although the tuning in this thread so far just deals with the tunables, there are other settings that can impact IPS performance. Here are a few...

In the Intrusion Detection Settings Tab.

Promiscuous mode- To be used only when multiple interfaces or VLAN's are selected in the Interfaces setting.
This is used so that IPS will capture data on all the selected interfaces. Do not enable if you have just

one interface selected. It will help with performance.

Pattern matcher: This setting can select the best algorithm to use when pattern matching. This setting is best set by testing. Hyperscan seems to work well with Intel NIC's. Try different ones and test the bandwidth with an internet speed test.

Home networks (under advanced menu.
Make sure the interfaces fall within the actual local networks. You may want to change the generic 192.168.0.0/16 to your actual local network ie 192.168.1.1/24

##
USEFUL SHELL COMMANDS
sysctl net.inet.tcp.hostcache.list # View the current host cache stats
vmstat -i # Query total interrupts per queue
top -H -S # Watch CPU usage
dmesg | grep -i msi # Verify MSI-X is being used by the NIC
netstat -ihw 1 # Look for idrops to determine hw.igb.txd and rxd
grep <interface> /var/run/dmesg.boot # Shows useful info like netmap queue/slots
sysctl -A # Shows system variables
##
« *Last Edit: February 02, 2018, 05:38:29 pm by dcol* »

From <https://forum.opnsense.org/index.php?topic=6590.0>