Contents

Introduction

This document describes the "overrun" error counter and how to investigate performance issues or packet loss problems on the network. An administrator might notice errors reported in the **show interface** command output on the Adaptive Security Appliance (ASA).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problem

The ASA interface error counter "overrun" tracks the number of times that a packet was received on the network interface, but there was no available space in the interface FIFO queue to store the packet. Thus, the packet was dropped. The value of this counter can be seen with the **show interface** command.

Example output that displays the problem:

```
ASA# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 0026.0b31.0c59, MTU 1500
IP address 10.0.0.113, subnet mask 255.255.0.0
580757 packets input, 86470156 bytes, 0 no buffer
Received 3713 broadcasts, 0 runts, 0 giants
2881 input errors, 0 CRC, 0 frame, 2881 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
905828 packets output, 1131702216 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/230)
output queue (blocks free curr/low): hardware (255/202)
```

In the example above, 2881 overruns were observed on the interface since the ASA booted up or since the command **clear interface** was entered in order to clear the counters manually.

Causes of Interface Overruns

Interface overrun errors are usually caused by a combination of these factors:

- Software level - The ASA software does not pull the packets off of the interface FIFO queue fast enough. This causes the FIFO queue to fill up and new packets to be dropped.
- Hardware level - The rate at which packets come into the interface is too fast, which causes the FIFO queue to fill before the ASA software can pull the packets off. Usually, a burst of packets causes the FIFO queue to fill up to maximum capacity in a short amount of time.

Steps to Troubleshoot the Cause of Interface Overruns

The steps to troubleshoot and address this problem are:

1. Determine if the ASA experiences CPU hogs and if they contribute to the problem. Work to mitigate any long or frequent CPU hogs.
2. Understand the interface traffic rates and determine if the ASA is oversubscribed due to the traffic profile.
3. Determine if intermittent traffic bursts cause the problem. If so, implement flow control on the ASA interface and adjacent switchports.

Potential Causes and Solutions

CPU on the ASA is Periodically Too Busy to Process Incoming Packets (CPU Hogs)

The ASA platform processes all packets in software and uses the main CPU cores that handle all system functions (such as syslogs, Adaptive Security Device Manager connectivity, and Application Inspection) in order to process incoming packets. If a software process holds the CPU for longer than it should, the ASA records this as a CPU hog event since the process "hogged" the CPU. The CPU hog threshold is set in milliseconds, and is different for each hardware appliance model. The threshold is based on how long it could take to fill the interface FIFO queue given the CPU power of the hardware platform and the potential traffic rates the device can handle.

CPU hogs sometimes cause interface overrun errors on single-core ASAs, such as the 5505, 5510, 5520, 5540, and 5550. The long hogs, that last for 100 milliseconds or more, can especially cause overruns to occur for relatively low traffic levels and non-bursty traffic rates. The problem does not impact multi-core systems as much, since other cores can pull packets off of a Rx ring if one of the CPU cores is hogged by a process.

A hog that lasts more than the device threshold causes a syslog to be generated with id 711004, as shown here:

```
Feb 06 2013 14:40:42: %ASA-4-711004: Task ran for 60 msec, Process = ssh, PC = 90b0155, Call
stack = Feb 06 2013 14:40:42: %ASA-4-711004: Task ran for 60 msec, Process = ssh, PC = 90b0155,
Call stack = 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b4459 0x090b44d6 0x08c46fcc
0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c 0x0806922c
```

CPU hog events are also recorded by the system. The output of the **show proc cpu-hog** command displays these fields:

- Process - the name of the process that hogged the CPU.
- PROC_PC_TOTAL - the total number of times that this process hogged the CPU.
- MAXHOG - the longest CPU hog time observed for that process, in milliseconds.
- LASTHOG - the amount of time the last hog held the CPU, in milliseconds.
- LASTHOG At - the time the CPU hog last occurred.
- PC - the program counter value of the process when the CPU hog occurred. (Information for the Cisco Technical Assistance Center (TAC))
- Call stack - the call stack of the process when the CPU hog occurred. (Information for the Cisco TAC)

This example shows the **show proc cpu-hog** command output:

```
ASA# show proc cpu-hog

Process:     ssh, PROC_PC_TOTAL: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:          0x08e7b225 (suspend)

Process:     ssh, NUMHOG: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:          0x08e7b225 (suspend)
Call stack: 0x08e7b225 0x08e8a106 0x08e7ebf4 0x08e7efde 0x08e7f4c9 0x08e7f546 0x08a7789c
            0x095a3f60 0x080e7e3d 0x080dcfa2 0x080ddf5c 0x0806897c

CPU hog threshold (msec): 10.240
Last cleared: 12:25:28 EST Jun 6 2012
ASA#
```

The ASA SSH process held the CPU for 119ms on 12:25:33 EST June 6th 2012.

If overrun errors continually increase on an interface, check the output of the **show proc cpu-hog** command in order to see if CPU hog events correlate with an increase in the interface overrun counter. If you find that the CPU hogs contribute to the interface overruns errors, it is best to search for bugs with the Bug Toolkit, or raise a case with the Cisco TAC. The output of the **show tech-support** command also includes the **show proc cpu-hog** command output.

Traffic Profile Processed Periodically Oversubscribes the ASA

Dependent upon on the traffic profile, the traffic that flows through the ASA might be too much for it to handle and overruns might occur.

The traffic profile consists of (among other aspects):

- Packet size
- Inter-packet gap (packet rate)
- Protocol - some packets are subjected to application inspection on the ASA and require more processing than other packets

These ASA features can be used in order to identify the traffic profile on the ASA:

- Netflow - the ASA can be configured to export NetFlow version 9 records to a NetFlow collector. This data can then be analyzed to understand more about the traffic profile.

- SNMP - utilize SNMP monitoring in order to track the ASA interface traffic rates, CPU, connection rates, and translation rates. The information can then be analyzed in order to understand the traffic pattern and how it changes over time. Try to determine if there is a spike in traffic rates that correlates to an increase in the overruns, and the cause of that traffic spike. There have been cases in the TAC where devices on the network misbehave (due to misconfiguration or virus infection) and generate a flood of traffic periodically.

Intermittent Packet Bursts Oversubscribe the ASA Interface FIFO Queue

A burst of packets that arrive on the NIC could cause the FIFO to become filled before the CPU can pull the packets off of it. There usually is not much that can be done in order to solve this problem, but it can be mitigated by the use of QoS in the network to smooth out the traffic bursts, or flow control on the ASA and the adjacent switchports.

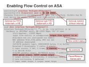
Flow control is a feature that allows the ASA's interface to send a message to the adjacent device (a switchport for example) in order to instruct it to stop sending traffic for a short amount of time. It does this when the FIFO reaches a certain high water mark. Once the FIFO has been freed up some amount, the ASA NIC sends a resume frame, and the switchport continues to send traffic. This approach works well because the adjacent switchports usually have more buffer space and can do a better job buffering packets on transmit than the ASA does in the receive direction.

You can try to enable captures on the ASA to detect the traffic micro-bursts, but usually this is not helpful since the packets are dropped before they can get processed by the ASA and added to the capture in memory. An external sniffer can be used to capture and identify the traffic burst, but sometimes the external sniffer can be overwhelmed by the burst as well.

Enable Flow Control to Mitigate Interface Overruns

The flow control feature was added to the ASA in version 8.2(2) and later for 10GE interfaces, and version 8.2(5) and later for 1GE interfaces. The ability to enable flow control on ASA interfaces that experience overruns proves to be an effective technique to prevent packet drop occurences.

Refer to the flow control feature in the Cisco ASA 5500 Series Command Reference, 8.2 for more information.


Enabling Flow Control on ASA
Optional low FIFO watermark in KB
Optional high FIFO watermark in KB
Optional duration (refresh interval)
Flow control status
No overruns
Pause/Resume frames sent

(Diagram from Andrew Ossipov's Cisco Live Presentation BRKSEC-3021)

Note that "output flow control is on" means that the ASA sends flow control pause frames out the ASA interface towards the adjacent device (the switch). "Input flow control is unsupported" means that the ASA does not support the *reception* of flow control frames from the adjacent device.

Flow Control Sample Configuration:

```
interface GigabitEthernet0/2
 flowcontrol send on
 nameif DMZ interface
 security-level 50
 ip address 10.1.3.2 255.255.255.0
!
```

Related Information

- **ASA 8.3 and Later: Monitor and Troubleshoot Performance Issues**
- **Cisco Live Presentation "Maximizing Firewall Performance" -** This presentation outlines the architecture of the various ASA platforms, and includes information about performance and tuning. For access to this presentation, log in to Ciscolive!365 and search for the presentation number BRKSEC-3021.
- **Cisco TAC Security Podcast Episode #7 "Monitoring Firewall Performance"** - This podcast episode features a discussion of techniques and methods to monitor firewall performance and identify performance problems.
- **Technical Support & Documentation - Cisco Systems**