The Snort FAQ

The Snort Core Team

Suggestions for enhancements of this document are always welcome. Please email them to the Snort-Users mailing list.

Many people have contributed to this FAQ:

Marty Roesch
Max Vision
Erek Adams
Phil Wood
Dennis Hollingworth
Jason Haar
Fyodor Yarochkin
Michael Davis
Roman Danyliw
Toby Kohlenberg
Paul Howell
Blake Frantz
Dragos Ruiu
Joe McAlerney
Christopher Cramer
Ramin Alidousti
Stef Mit
Lars Norman S?ndergaard
Jed Pickel
Joe Stewart
Frank Knobbe
Jim Hankins
Ofir Arkin
Brent Erickson

1.5 Does Snort handle IP defragmentation?

Yes, use `preprocessor frag2`.

  - Loss of full-duplex capabilities
  - Additional single point of failure
  - Collision loss at above 50% load levels

3. Network taps:

1.11 Does Snort log the full packets when it generates alerts?

http://www.ntop.org/winpcap.html.

Basically, 1 and 2 on the sniffer side are connected, 3 and 6 straight through to the LAN. 1 and 2 on the LAN

–

3.12 How do you get Snort to ignore some traffic?

Snort can be made to ignore traffic in a number of different ways:

1. Specify bpf filters on the command line the tcpdump man page has a description of bpf filters.
2. Use a pass rule
3. The portscan preprocessor has it's own special exclusion list with the portscan-ignorehosts.rules file directive

3.16 Which takes precedence, commandline or rule file ?

The command line always gets precedence over the rules file. If people want to try stuff out quickly without

```
          |
  OTN    \|/
 ---------v----------
| content: baz       |
| msg: baz           |
 ---------------------
```

This is an efficient way to do things because we only need to check the data in the RTN once with this method. There is actually another dimension to this array: the function pointer list. Each node in the “array” has a linked list of function pointers attached to it. The functions in this list are the tests that need to be done to determine whether the data in the current packet matches the current 4(cu1le)-290(n)1(o)-28(d)1(e)-1('s)-289(i

```
       |
  OTN    \|/
 ---------v----------
| content: baz       |
| msg: baz           |
 --------------------
```

Note that all three of the port 80 rules will be checked before the “1:1024” rule due to the order 4n which the appl4cable RTN has been created. This is because the rules parser builds the first chain header for port 80 traffic and sticks it on the rules list, then on the next rule it sees that a new chain header is required, so it gets built and put in place. In this case you wou11(s)squkbeut togire th (e)-x(h)1m(e)-1(p)1e”sesage ant

```
                         #‘cat /var/run/snort_"$i".pid‘
                        "$ECHO" "Restarting Snort running with PID "$PID" and reloading the rules..
                        "$KILL" -s "$KILLSIG" "$PID"
                 fi
         else
                 "$ECHO" "No PID file for interface "$i" found under /var/
run"
         fi
         "$ECHO" "Starting Snort"
         "$SNORT" -a -b -c "$SNORTCFGPATH""/snort.conf_""$i" -I -D -v
-i $i -u "$SNORTUSER" -g "$SNORTGROUP"
         PID=‘cat /var/run/snort_"$i".pid‘
         "$ECHO" "Snort running now with PID "$PID""
done
}
###########################################################################
####
#     Die Funktion zum ueberpruefen, ob und wie Snort auf dem System laeuft
#
###########################################################################
####
checksnort() {
SNORTS=$("$PIDOF" "$SNORT" | wc -w | awk ’{print $1}’)
SNORT_PIDS=$(/usr/bin/find /var/run -name snort\_eth[0-9]\.pid -ls |
wc -l | awk ’{print $1}’)
"$ECHO" "Snort instances counted:  $SNORTS"
"$ECHO" "Snort PID files found:    $SNORT_PIDS"

# 1. Fall: Snort laeuft nicht oder PID-File nicht da:
if [ "$PID""S" = "0" -o "$SNORT_PIDS" = "0" ]
then
         "$ECHO" "Snort seems to be down or no PID file there..."
         "$ECHO" "Restarting Snort for all Interfaces..."
         "$SERVICE" snort restart
fi
# 2. Fall: Anzahl der Instanzen ungleich der Anzahl der PID-Files
if [ "$PID""S" -gt "$PIDRT_PIDS" ]
then
         "$ECHO" "More Snort .955ances than found PID files..."
         "$ECHO" "Something is wrong outthere..."
         "$ECHO" "Stopping all Snort processes..."
#        /usr/bin/killall -9 snort
        "$SERVICE" snort stop
        "$ECHO" "Hold on... Restarting Snort now..."
        "$SERVICE" snort restart
fi

# 3. Fall: Anzahl der Instanzen stimmt mit der Anzahl der PID-es fouueberein
```

3.21 How do I use a remote syslog machine?

These 'with' statements basically have the effect of the Makefile including -L and -R statements for each

4.3 Snort is behind a firewall (ipf/pf/ipchains/ipfilter) and awfully quiet...

4.7 What are all these ICMP files in subdirectories under /var/log/snort?

Most of them are likely destination unreachable and port unreachables that were detected by snort when a communications session attempt fails.

4.8 Why does the program generate alerts on packets that have pass rules?

The default order that the rules are applied in is alerts firstw.5674(tens)-358ppsetw.5675(t)1(hns)-358lrogle. Tist ordeai that oun alert rulesaun then issaale(t)1(hms)-84(alln)-842aiclyth (n)-842der-1(ans)28th l. lof ralyfnshuns order s thes rules are pplted r-1(rstw.5541(u)1(s)-1(e)-504tt)1(he)-504“-o”faun swi(ac)27(h)1,t the“lorde”tgt de

genealet(t)1(t)(t)1tparc(e)-1((s))1e(rst1. lof

thenppslewillneiimizle(th)1(e)-34(f(al)1(s)-1(e)-331pa)28(ositivk)28((.)-445(Y)84(out)-333willn)-333neied odead fiters.

4. What are all thesen(at)1(i)-1(n)-375(u(r)-1(a(c)31(haul)1(”t)-375((ler)-1(t)1(s?)]T / F89.9

? sourc(e)-34((r)1cutes)-34(fr-1a[lled)]TJ-249070-50.154 Td[Assfr-1a(r)-333ass(wh)28y.. “fr1 de”s

aces firssaatenore(ot)-33((th)1(e)-34(orig(i)1(alt)-333(d)1atagramin)-333(ndf)-33((th)1(e)-34

TheCMPessaathoreac(aa)1(e)2904(the(e)-34((stnotion)ages1((h)1ose)-1(?)-466(le)-1CMI)1PtPbortreachable

? pn-1(otcd)28(colt)-333uunreac(aa)1(e)]TJ/1489.963Tf-9.963-18.8454Td[(?)]TJ/F89.963Tf9.9630Td[3tphortreachable

a41onotc358(d)-3(k)28(ed)c358(bh)241o(the)2358(d)1(e)-1(st(n)1(ation)241oaddnrse. TheC

? (h)1osetreachable

TheinIt(ar?)]T / 1489.963Tf14.9440-50.1.4Td[(?)]T / F89.963Tf9.9630Td[0tndetreachable

ard ?)usnd t4etyanigetmds

rt1Cd)Fs(l)1de nldhe el(d)-341in(d)1icatets wheacesu(d)-341no34(-313(b)287ge)-342(d)1(e)-1lisee Somgeort

snd deee Somgeort

the source address as being !$HOME (or whatever variable you use to represent your internal network), then you should see most of the false positives go away.

The “alert” action in Snort is hard coded to do two things when an event is detected by Snort, write an event to the alert facility and log as much as possible/desired to the output facility. The “log” action merely logs

4.30 Is there a private SID number range so my rules don’t conflict?

Yes. Private SIDs start at 1000000.

4.31 How long can address lists, variables, or rules be?

The Snort parser has an 8K limit on variables and rt **after** expansion. In practice, this is not a m(,)-ajor limit :-)

4.32 What d(,)-o the numbers (ie: [116:56:1]) in front of a Snort alert mean?

5.7 What is the best way to use Snort to block attack traffic?

```
redalert tcp any any -> any any (msg:"REDRUM REDRUM"; content:"redalerttest")
```

- http://standards.ieee.org/regauth/oui/oui.txt
- http://www.codito.de/maa63ufd.c

5.16 How can I examine logged packets in more detail?

If you are using unified logging, you can use Barnyard (see FAQ 5.1) or the unified log to pcap converter written by Dragos:

http://dragos.com/logtopcap.c

6.2 SMB alerts aren’t working, what’s wrong?

```
    # When I first wrote this script, I only ran it on BSD systems. That was a
    # mistake, as BSD systems have a date command that apperently lets you walk the
```

```
if [ -d $weeklogs/$olddirdate ]
then
 rm -r $weeklogs/$olddirdate
fi

# Compress and save the log files to save for as long as you want.
# This is done in a sub-shell because we change dirs, and I don't want
# to do that within the shell that the script runs in.

(cd $weeklogs; tar zcvf $oldlogs/$dirdate.tgz $dirdate > /dev/null 2>&1)
```

3. You are using a command line option that overrides what you have in your configuration file. This is most often -A or -s. NOTE: If you wish to log to syslog as well, specify so in your configuration file rather then the command line.
4. There is a problem with your database configuration itself. Make sure the user you specify has the correct permissions, or that the database is even up and running.

6.16 Portscans are not being logged to my database

You need to change the output facility to 'alert' rather then 'log'. The portscan preprocessor calls output plugins registered as 'alert' plugins rather then 'log'.

6.20 My snort crashes, how do I restart it?

Try one of these two shell scripts or daemontools (refer to website to daemontools)

```
 * []#!/bin/sh
   #snorthup: Snort Restarter and Crash Logger
   #(dr@kyx..net with help from kmaxwell@supercages.com)

   $conf = "snort.conf"
   for $IFACE in fxp0 fxp1
   do
       if [ -f /var/run/snort_$IFACE.pid ]; then
           if !  ps -p ‘cat /var/run/snort_$IFACE.pid‘ > /dev/null ; then
               /usr/bin/logger -p user.notice snorthup: removing bogus pidfile
               /usr/bin/
   logger -p user.notice snorthup: restarting absentee snort o
   n $IFACE with conf file $i
               rm -f /var/run/snort_$IFACE.pid
```

In the most generic of terms, if a box supports 100 “full-duplex,” then its a switch (regardless of what the manufacturer calls it). If it supports 100 − > 10, there is 50-50 chance the box has some MAC address awareness. If a box only supports 10 − > 10 or 100 − > 100, there is a high probability it is not MAC

6.23 I'm not seeing any interfaces listed under Win32.

The reason you're seeing nothing in the interface list is a WinPcap problem. In previous versions of WinPcap there is a 1K buffer, which overflows if you have many interfaces (i.e., 10+). This has been replaced with an 8K buffer in more recent versions of WinPcap. The current snort distribution should already be linking

```
tcphdr.tcp_sport

tcphdr.tcp_dport

acid_ag_alert.ag_sid + acid_ag_alert.ag_cid
```

MySQL can be fast - you just need to have the proper indexing set up. If you need a good MySQL reference, pick up a copy of Paul DuBois' book, which is currently the bible for MySQL. O'Reilly also recently released a reference by Monty and the MySQL AB team.

The way to check if the indices are already there are with the SHOW INDEX command. For instance, to check the tcphdr table, you would run:

```
+ []mysql> show index from tcphdr;

  +----+------+------+-------+-------+------+-------+-----+----+-----+

  | Table  | Non_unique | Key_name  | Seq_in_index | Column_name |
```

For more info on pipelining:

http://www.faqs.org/rfcs/rfc1854.html

If your mailservers are not vulnerable to these overflows you can disable this rule and regain some peace...

6.28 I'm getting lots of *ICMP Ping Speedera*, is this bad?

Quite ordinary. Windows update uses speedera based DNS, among other things. Of course, if the speedera