Netfilter Conntrack Sysfs variables

/proc/sys/net/netfilter/nf_conntrack_* Variables:

nf_conntrack_acct - BOOLEAN

- 0 - disabled (default)
- not 0 - enabled

Enable connection tracking flow accounting. 64-bit byte and packet counters per flow are added.

nf_conntrack_buckets - INTEGER

Size of hash table. If not specified as parameter during module loading, the default size is calculated by dividing total memory by 16384 to determine the number of buckets. The hash table will never have fewer than 1024 and never more than 262144 buckets. This sysctl is only writeable in the initial net namespace.

nf_conntrack_checksum - BOOLEAN

- 0 - disabled
- not 0 - enabled (default)

Verify checksum of incoming packets. Packets with bad checksums are in INVALID state. If this is enabled, such packets will not be considered for connection tracking.

nf_conntrack_count - INTEGER (read-only)

Number of currently allocated flow entries.

nf_conntrack_events - BOOLEAN

- 0 - disabled
- not 0 - enabled (default)

If this option is enabled, the connection tracking code will provide userspace with connection tracking events via ctnetlink.

nf_conntrack_expect_max - INTEGER

Maximum size of expectation table. Default value is nf_conntrack_buckets / 256. Minimum is 1.

nf_conntrack_frag6_high_thresh - INTEGER

default 262144

Maximum memory used to reassemble IPv6 fragments. When nf_conntrack_frag6_high_thresh bytes of memory is allocated for this purpose, the fragment handler will toss packets until nf_conntrack_frag6_low_thresh is reached.

nf_conntrack_frag6_low_thresh - INTEGER

default 196608

See nf_conntrack_frag6_low_thresh

nf_conntrack_frag6_timeout - INTEGER (seconds)

default 60

Time to keep an IPv6 fragment in memory.

nf_conntrack_generic_timeout - INTEGER (seconds)

default 600

Default for generic timeout. This refers to layer 4 unknown/unsupported protocols.

nf_conntrack_helper - BOOLEAN

- 0 - disabled (default)
- not 0 - enabled

Enable automatic conntrack helper assignment. If disabled it is required to set up iptables rules to assign helpers to connections. See the CT target description in the iptables-extensions(8) man page for further information.

nf_conntrack_icmp_timeout - INTEGER (seconds)

default 30

Default for ICMP timeout.

nf_conntrack_icmpv6_timeout - INTEGER (seconds)

default 30

Default for ICMP6 timeout.

nf_conntrack_log_invalid - INTEGER

- 0 - disable (default)
- 1 - log ICMP packets
- 6 - log TCP packets
- 17 - log UDP packets
- 33 - log DCCP packets
- 41 - log ICMPv6 packets
- 136 - log UDPLITE packets
- 255 - log packets of any protocol

Log invalid packets of a type specified by value.

nf_conntrack_max - INTEGER

Maximum number of allowed connection tracking entries. This value is set to nf_conntrack_buckets by default. Note that connection tracking entries are added to the table twice -- once for the original direction and once for the reply direction (i.e., with the reversed address). This means that with default settings a maxed-out table will have a average hash chain length of 2, not 1.

nf_conntrack_tcp_be_liberal - BOOLEAN

- 0 - disabled (default)
- not 0 - enabled

Be conservative in what you do, be liberal in what you accept from others. If it's non-zero, we mark only out of window RST segments as INVALID.

nf_conntrack_tcp_ignore_invalid_rst - BOOLEAN

- 0 - disabled (default)
- 1 - enabled

If it's 1, we don't mark out of window RST segments as INVALID.

nf_conntrack_tcp_loose - BOOLEAN

- 0 - disabled
- not 0 - enabled (default)

If it is set to zero, we disable picking up already established connections.

nf_conntrack_tcp_max_retrans - INTEGER

default 3

Maximum number of packets that can be retransmitted without received an (acceptable) ACK from the destination. If this number is reached, a shorter timer will be started.

nf_conntrack_tcp_timeout_close - INTEGER (seconds)

default 10

nf_conntrack_tcp_timeout_close_wait - INTEGER (seconds)

default 60

nf_conntrack_tcp_timeout_established - INTEGER (seconds)

default 432000 (5 days)

nf_conntrack_tcp_timeout_fin_wait - INTEGER (seconds)

default 120

nf_conntrack_tcp_timeout_last_ack - INTEGER (seconds)

default 30

nf_conntrack_tcp_timeout_max_retrans - INTEGER (seconds)

default 300

nf_conntrack_tcp_timeout_syn_recv - INTEGER (seconds)

default 60

nf_conntrack_tcp_timeout_syn_sent - INTEGER (seconds)

default 120

nf_conntrack_tcp_timeout_time_wait - INTEGER (seconds)

default 120

nf_conntrack_tcp_timeout_unacknowledged - INTEGER (seconds)

default 300

nf_conntrack_timestamp - BOOLEAN

- 0 - disabled (default)
- not 0 - enabled

Enable connection tracking flow timestamping.

nf_conntrack_udp_timeout - INTEGER (seconds)

default 30

nf_conntrack_udp_timeout_stream - INTEGER (seconds)

default 120

This extended timeout will be used in case there is an UDP stream detected.

nf_conntrack_gre_timeout - INTEGER (seconds)

default 30

nf_conntrack_gre_timeout_stream - INTEGER (seconds)

default 180

This extended timeout will be used in case there is an GRE stream detected.

nf_hooks_lwtunnel - BOOLEAN

- 0 - disabled (default)
- not 0 - enabled

If this option is enabled, the lightweight tunnel netfilter hooks are enabled. This option cannot be disabled once it is enabled.

nf_flowtable_tcp_timeout - INTEGER (seconds)

default 30

Control offload timeout for tcp connections. TCP connections may be offloaded from nf conntrack to nf flow table. Once aged, the connection is returned to nf conntrack with tcp pickup timeout.

nf_flowtable_udp_timeout - INTEGER (seconds)

default 30

Control offload timeout for udp connections. UDP connections may be offloaded from nf conntrack to nf flow table. Once aged, the connection is returned to nf conntrack with udp pickup timeout.