/proc/sys/net/ipv4/vs/* Variables:

am_droprate - INTEGER
        default 10

        It sets the always mode drop rate, which is used in the mode 3
        of the drop_rate defense.

amemthresh - INTEGER
        default 1024

        It sets the available memory threshold (in pages), which is
        used in the automatic modes of defense. When there is no
        enough available memory, the respective strategy will be
        enabled and the variable is automatically set to 2, otherwise
        the strategy is disabled and the variable is set to 1.

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

        If it is enabled, forward packets to the original destination
        directly when no cache server is available and destination
        address is not local (iph->daddr is RTN_UNICAST). It is mostly
        used in transparent web cache cluster.

debug_level - INTEGER
        0   - transmission error messages (default)
        1   - non-fatal error messages
        2   - configuration
        3   - destination trash
        4   - drop entry
        5   - service lookup
        6   - scheduling
        7   - connection new/expire, lookup and synchronization
        8   - state transition
        9   - binding destination, template checks and applications
        10   - IPVS packet transmission
        11   - IPVS packet handling (ip_vs_in/ip_vs_out)
        12 or more - packet traversal

        Only available when IPVS is compiled with the CONFIG_IPVS_DEBUG

        Higher debugging levels include the messages for lower debugging
        levels, so setting debug level 2, includes level 0, 1 and 2
        messages. Thus, logging becomes more and more verbose the higher
        the level.

drop_entry - INTEGER
        0 - disabled (default)

        The drop_entry defense is to randomly drop entries in the
        connection hash table, just in order to collect back some
        memory for new connections. In the current code, the
        drop_entry procedure can be activated every second, then it
        randomly scans 1/32 of the whole and drops entries that are in

the SYN-RECV/SYNACK state, which should be effective against syn-flooding attack.

The valid values of drop_entry are from 0 to 3, where 0 means that this strategy is always disabled, 1 and 2 mean automatic modes (when there is no enough available memory, the strategy is enabled and the variable is automatically set to 2, otherwise the strategy is disabled and the variable is set to 1), and 3 means that that the strategy is always enabled.

drop_packet - INTEGER
0 - disabled (default)

The drop_packet defense is designed to drop 1/rate packets before forwarding them to real servers. If the rate is 1, then drop all the incoming packets.

The value definition is the same as that of the drop_entry. In the automatic mode, the rate is determined by the follow formula: rate = amemthresh / (amemthresh - available_memory) when available memory is less than the available memory threshold. When the mode 3 is set, the always mode drop rate is controlled by the /proc/sys/net/ipv4/vs/am_droprate.

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

The default value is 0, the load balancer will silently drop packets when its destination server is not available. It may be useful, when user-space monitoring program deletes the destination server (because of server overload or wrong detection) and add back the server later, and the connections to the server can continue.

If this feature is enabled, the load balancer will expire the connection immediately when a packet arrives and its destination server is not available, then the client program will be notified that the connection is closed. This is equivalent to the feature some people requires to flush connections when its destination is not available.

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

When set to a non-zero value, the load balancer will expire persistent templates when the destination server is quiescent. This may be useful, when a user makes a destination server quiescent by setting its weight to 0 and it is desired that subsequent otherwise persistent connections are sent to a different destination server. By default new persistent connections are allowed to quiescent destination servers.

If this feature is enabled, the load balancer will expire the persistence template if it is to be used to schedule a new

connection and the destination server is quiescent.

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

It controls sending icmp error messages (ICMP_DEST_UNREACH) for VS/NAT when the load balancer receives packets from real servers but the connection entries don't exist.

secure_tcp - INTEGER
0 - disabled (default)

The secure_tcp defense is to use a more complicated state transition table and some possible short timeouts of each state. In the VS/NAT, it delays the entering the ESTABLISHED until the real server starts to send data and ACK packet (after 3-way handshake).

The value definition is the same as that of drop_entry or drop_packet.

sync_threshold - INTEGER
default 3

It sets synchronization threshold, which is the minimum number of incoming packets that a connection needs to receive before the connection will be synchronized. A connection will be synchronized, every time the number of its incoming packets modulus 50 equals the threshold. The range of the threshold is from 0 to 49.