The syncache is always checked first because a TFO SYN and a retransmitted fallback non-TFO SYN could be reordered in the network. Also, because middleboxes and bad people.

Cookie generation and validation is performed by computing the 64-bit value SipHash-2-4(key, remote_ip). Cookies returned via SYNJACK are computed using the most recently installed key. Cookies in SYN packets are validated by trying each active key in reverse order of installation.
SYN Processing by non-Listen Socket

- SYN received on a non-listen socket
  - Was fast opened?
    - Yes: In SYN-RCVD?
      - Yes: Drop. Retransmit timer is not affected.
      - No: Standard simultaneous open
    - No: In SYN-SENT?
      - Yes: Send challenge ACK and drop
      - No: Send challenge ACK and drop
Build options:
TCP_RFC7413
TCP_RFC7413_MAX_KEYS

Socket options:
TCP_FASTOPEN
   Allows servicing of TFO connection requests when set on a listen socket. Can be set / cleared at any time during the listen socket's lifetime. If the syscall net.inet.tcp.fastopen.enabled is zero, attempts to set TCP_FASTOPEN will fail.
TCP_FASTOPENED
   This option is read-only and indicates whether fast open was successfully employed in creating the connection.

Per-VNET sysctls:
net.inet.tcp.fastopen.acceptany (RW)
   Disables cookie validation. Any cookie value, including an empty one, will result in a TFO connection.
net.inet.tcp.fastopen.autokey (RW)
   Interval in seconds at which to auto-generate keys. An interval of 0 disables auto key generation. Transition from zero to non-zero will generate one random key if enabled is non-zero and there are no keys.
net.inet.tcp.fastopen.enabled (RW)
   Allow / disallow TCP_FASTOPEN socket option and new TFO connections. Transition from non-zero to zero clears keys. Transition from zero to non-zero generates one random key if autokey is non-zero and there are no keys.
net.inet.tcp.fastopen.keylen (RO)
   Key length in bytes
net.inet.tcp.fastopen.maxkeys (RO)
   Maximum number of keys supported
net.inet.tcp.fastopen.numkeys (RO)
   Current number of keys installed
net.inet.tcp.fastopen.setkey (WO)
   Install a new key by writing keylen bytes