Portmaster Firewall Decision Flow

For a connection to be allowed it must be accepted in all applicable flows.

To domain: Before resolving DNS and gathering Intel

To domain: After resolving DNS and gathering Intel

Any: With first packet

Flags Internet and LAN not set → Yes → BLOCK

Domain label blacklisted? → Yes → BLOCK

Check remote IP according to Internet, LAN and Localhost Flags

Check domain list for requested domain

ACCEPT

Filter DNS replies according to Internet and LAN Flags

No → Permitted? → No → BLOCK*

In list? → Yes → Permitted? → Yes → ACCEPT

Flag PeerToPeer set? ← Direct (no DNS) ← Connection Type

No → BLOCK*

Profile mode → Whitelist → BLOCK*

Permitted? → No → BLOCK*

Any replies left? → No → BLOCK*

Flag PeerToPeer set? → Yes

To domain

Blacklist

Prompt

Check port list for destination port

Flag Service set? → Yes

Connection Type → Incoming

Flag Service set? → No → BLOCK*

"Link"

ACCEPT

Flag Related set? → Yes → Process related to domain? → Yes → ACCEPT

In list? → Yes

Flag Related set? → No

Process related to domain? → No

In list? → No → Profile mode → Whitelist

Profile mode → Prompt

Profile mode → Blacklist → ACCEPT

Ask user about domain/port and save answer into list → No answer → DROP

permitted? → No → BLOCK*

permitted? → Yes → ACCEPT
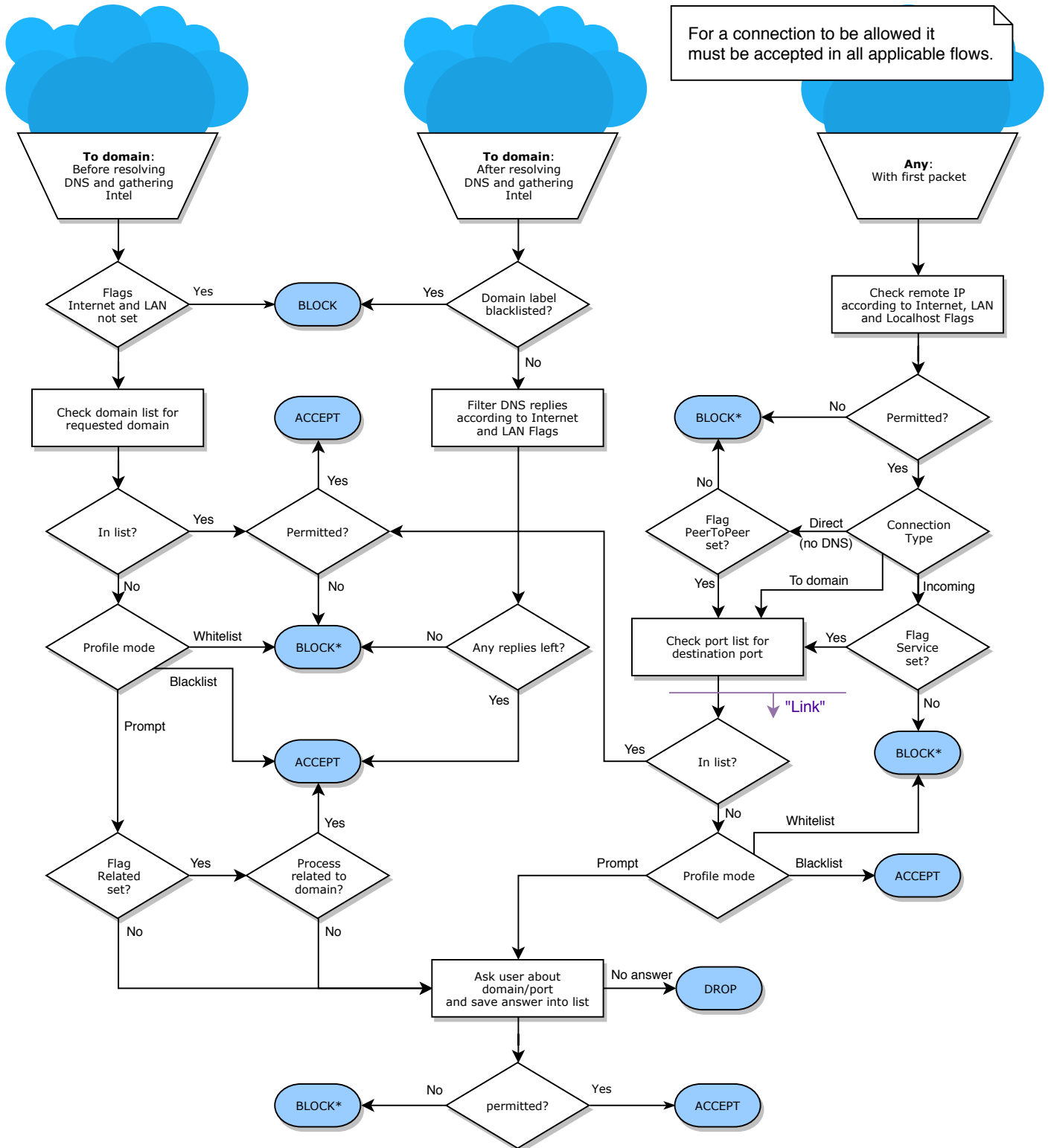
- Connections by the Portmaster itself are always allowed.
- Connections are re-evaluated on the next new Link when a Profile has changed, Links are never re-evaluated.
- Links may be inspected by additional modules, which can then block/drop previously accepted Links, but not accept previously blocked/dropped ones.

*Incoming connections/links are always dropped, not blocked.