Night's Watch Crow

Night's Watch Crow Traffic Filtering, a Minimum Viable Product feature, provides stateful packet filtering through a flexible, dynamic ruleset framework. It offers comprehensive packet classification and filtering based on protocol fields across network layers 2-4, including:

- Layer 2: MAC addresses, ethertype, bridge port
- Layer 3: IP addresses, IP protocol, IP options, fragmentation
- Layer 4: TCP/UDP ports, TCP flags and connection states, ICMP types/codes
- Prefix List like collections of similar addresses contained in a managable form

The filtering engine supports advanced matching criteria through stateful connection tracking, rate limiting, and set-based operations for efficient handling of large IP/port ranges. Rules can be organized into type-specific chains (filter, route, nat) and tables, with customizable priorities and hooks into the netfilter packet processing pipeline.

Flow control actions include accept, drop, reject (with configurable ICMP responses), queue (to userspace), and jump/goto for rule organization. The framework supports atomic ruleset updates and uses a just-in-time (JIT) compiler to optimize packet processing performance.