Night's Watch Crow

Traffic Flow Metrics

Roadmap: MVP

Night's Watch Crow Traffic Flow Metrics, a Minimum Viable Product feature, provides extensive traffic monitoring and logging capabilities through its counter, quota, and logging subsystems. Traffic metrics can be collected at multiple levels: Statistics Features:

- Packet and byte counters per rule
- Connection tracking statistics
- Per-rule quota enforcement with customizable thresholds
- Real-time flow monitoring with packet sampling
- Interface-specific metrics collection
- Protocol-specific counters (TCP, UDP, ICMP)

Logging Framework (in order of increasing verbosity):

- emerg - System is unusable (default: logged)
- alert - Action must be taken immediately (default: logged)
- crit - Critical conditions (default: logged)
- err - Error conditions (default: logged)
- warning - Warning conditions (default: logged)
- notice - Normal but significant conditions (default: not logged)
- info - Informational messages (default: not logged)
- debug - Debug-level messages (default: not logged)

The default logging level is set to warning. Additional logging levels can be enabled for troubleshooting purposes. Log data can be directed to syslog, netlink queues, or custom targets, supporting integration with external monitoring and analysis tools. The device includes rate limiting capabilities to prevent log flooding during high-traffic events.