

# Night's Watch Crow

## Deep Packet Inspection

Roadmap: 2026

Night's Watch Crow Deep Packet Inspection (DPI), a Roadmap 2026 feature, provides granular network traffic analysis and application-layer visibility. This resource-intensive service requires substantial hardware capacity that scales with traffic volume and analysis depth. The system delivers detailed traffic insights through:

- Application protocol identification and classification
- Content-based traffic categorization
- User behavior and application usage patterns
- File type identification in network streams
- Protocol compliance monitoring
- Traffic metadata extraction and analysis
- Application-specific security policy enforcement
- Bandwidth usage analysis per application
- Data exfiltration detection capabilities
- SSL/TLS certificate and cipher analysis
- Application command monitoring
- Resource access pattern analysis
- Session reconstruction capabilities
- Performance profiling of application protocols
- Hardware requirements scale with inspection depth and traffic volume

DPI analysis provides essential visibility into network applications and user behaviors, complementing IDS capabilities with detailed protocol and application-layer insights. The service can be tuned to balance inspection depth with performance requirements, allowing focused analysis of critical traffic patterns while managing hardware resource utilization.