Literature Review Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Source | Type | Summary | Relevance to Project |
| BSI TR-03148 Secure Broadband Router | National Security Standard | Outlines minimum security requirements for broadband routers, including secure boot, update mechanisms, and secure configuration defaults. | Reinforces our security scoring categories like firmware updates, encryption protocols, and remote access configuration. |
| CL-GL-GDS-BCP-V01-211007: Gateway Device Security Best Practices | Industry Best Practice Guide | Defines a broad set of security requirements for consumer broadband devices, secure software updates, and data protection. | Used to select practical, measurable security criteria for evaluation. Criteria not selected were excluded due to verification or access limitations. |
| NIST IR 8425A – Recommended Cybersecurity Requirements for Consumer-Grade Router Products | Government Technical Report | Cybersecurity requirements specifically for home/consumer routers. Covers secure setup, software update mechanisms, interface access control, logging, and data protection. | Directly informed our security rating grid. Used to select quantifiable, testable categories like secure default credentials, auto-updates, encryption standards, and configuration hardening. |
| TR-124: Functional Requirements for Broadband Residential Gateway Devices | Industry Functional Specification | Defines baseline and advanced functional requirements for residential gateway devices, including LAN/WAN connectivity, IPv6 support, remote management, firewall features, and QoS. | Informs the router performance and usability categories, especially around features like remote admin, IPv6, firewall behavior, and how gateways interact with ISP management tools (e.g., TR-069). |
| NIST SP 800-128 – Security-Focused Configuration Management | Government Framework | Provides guidance on managing configuration settings for security. | Supports methodology for evaluating router configuration defaults (e.g., firewall, remote access settings). |
| CVSS (Common Vulnerability Scoring System) | Industry Scoring Model | Framework for assigning severity scores to known security vulnerabilities. | Informs scoring model for counting and weighing CVEs per router. |
| RFC 2544 – Benchmarking Methodology for Network Interconnect Devices | IETF Standard | Defines procedures for measuring throughput, latency, and packet loss. | Basis for evaluating performance metrics from third-party benchmarks. |
| System Usability Scale (SUS) | Assessment Tool | 10-question survey giving a usability score from user experience. | Provides scoring reference for subjective usability feedback from reviews. |
| SmallNetBuilder.com Reviews | Third-Party Benchmarks | Wi-Fi speed, range, and latency tests on common consumer routers. | Used to assign performance ratings when physical testing isn’t possible. |
| Ookla Speedtest Reports | Crowdsourced Data | Aggregated download/upload latency stats by ISP and router model. | Used for estimating expected router performance across ISPs. |
| Heuristic Evaluation (Nielsen) | Usability Framework | 10 heuristics for identifying interface design problems. | Supports usability evaluation framework where physical testing is limited. |