Network Availability Incident Review

Example report

Kit Baroness | Security analysis example

Executive assessment

The supplied incident analysis describes an Internet Control Message Protocol (ICMP) flood that prevented normal access to internal network services for approximately two hours. It attributes the disruption to a firewall configuration that allowed excessive incoming traffic. The recorded response restricted incoming ICMP traffic, took non-critical services offline, and prioritized restoration of critical services.

The immediate business concern is service availability. The record does not establish data theft, financial loss, or the identity of the attacker. This review develops the supplied analysis into a response and improvement plan; packet captures, firewall exports, and recovery test results were not supplied for independent verification.

Evidence and reasoning

The following references identify sections of the supplied analysis, rather than separately collected system artifacts.

Reference	Observation in the record	Assessment
INC-S1: incident summary	Network resources were unavailable during excessive ICMP traffic.	Consistent with a network availability incident; the two-hour duration is reported, not independently timed.
INC-S2: cause analysis	The firewall did not limit or filter the incoming traffic.	A configuration weakness is the recorded contributing condition; confirm it against the effective rules and traffic path.
INC-S3: response account	Traffic restrictions and service prioritization supported restoration.	Response actions are described; their effectiveness and side effects require retained validation evidence.

The relationship between traffic volume, firewall behavior, and service disruption supports the proposed mitigation. It does not establish that every ICMP message should be blocked: required network diagnostics and control messages must be considered when defining the permitted traffic policy.

Actions and completion criteria

Owners below are proposed accountable roles; assignment and implementation are pending.

Work item	Proposed owner	Evidence required to complete
Review the effective firewall policy and define appropriate traffic limits.	Network lead	Reviewed rule export; approved permitted-traffic profile; controlled tests showing the restriction works and essential communication remains available.
Establish traffic baselines and alerts for abnormal volume.	Security operations lead	Recorded baseline, alert condition, and an authorized test that produces the expected alert.

Work item	Proposed owner	Evidence required to complete
Validate recovery of priority services and dependencies.	Service owner	Service checks, restoration sequence, monitoring results, and a record of remaining issues.
Record lessons, configuration ownership, and review triggers.	Operations lead	Named control owners, updated response procedures, and scheduled follow-up.

Decision and closure

Approve the scoped configuration review and validation work before describing the incident as fully resolved. Preserve the relevant source records and document event times with explicit time zones when they become available.

The incident record can close when priority services meet their agreed acceptance criteria, the traffic controls are tested, and unresolved evidence gaps and remaining exposure have an accountable owner. Until those checks are recorded, the improvement plan remains proposed and recovery assurance remains unverified.

Reference method

The structure follows the incident analysis, response, recovery, and improvement approach in NIST SP 800-61 Rev. 3, which uses Cybersecurity Framework 2.0.

https://doi.org/10.6028/NIST.SP.800-61r3