SERVICE DEFINITION DOCUMENT
FIREWALL / SEGMENTATION REVIEW

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

About JUMPSEC

JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- to reduce the risk of significant security incidents
- to speed up the detection and containment of threats, and
- to demonstrate robust governance to stakeholders such as boards, auditors, and insurers

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

Example use cases

Central government department — Any-any rules across shared services

During our department-scale review, JUMPSEC uncovered legacy any-any allowances that remained from earlier migrations. Our teams identified unused objects, duplicate address groups, and broad service sets that obscured the intent behind rules. We saw that flat inter-VLAN flows permitted users to traverse from their subnets into shared services, which elevated the risk of lateral movement and complicated audit processes.

JUMPSEC led a remediation programme to clean up the environment: we removed unused objects, collapsed duplicates, and replaced broad service allowances with explicit port definitions. We tightened administrative pathways, enforced logging on privileged flows, and applied expiry and review cycles to every exception. Our verification exercises demonstrated that we had reduced exposure, clarified the intent behind rules, and left fewer opportunities for unauthorised traversal.

NHS Trust — Segmentation drift between clinical and corporate zones

We found that trust environments contained inconsistent inter-zone rules, which allowed clinical endpoints to initiate access to corporate services. JUMPSEC identified overly permissive DNS/SMB rules, incomplete logging, and legacy allowances in backup and imaging networks that bypassed modern controls.

We restated trust boundaries, enforced one-way flows where feasible, and narrowed DNS/SMB exposure. JUMPSEC introduced change governance with exception lifecycles and validation checks. During our follow-up assessments, we evidenced cleaner dependencies and stronger control of privileged pathways.

Charity — Branch firewalls with object sprawl

Decentralised changes across branches led to object sprawl, shadowed rules, and conflicting address groups. Over the years, organisations inherited policies that no longer matched active services, which increased audit findings and slowed troubleshooting.

JUMPSEC and our teams consolidated and deduplicated objects, standardised naming conventions, and removed stale entries. We helped organisations adopt a core branch template that aligned with head-office policy and enabled rule-usage monitoring to retire dormant entries. During verification, we demonstrated that our approach resulted in simpler policies, faster change cycles, and fewer audit exceptions.

Transport operator (CNI) — Privileged paths to control systems

JUMPSEC sampled transport estates and uncovered unmanaged admin routes leading from IT into OT-adjacent jump hosts. We observed that broad maintenance windows left high-risk services open for longer than necessary, and noticed how temporary exceptions drifted into permanent pathways.

We remediated the environment by isolating admin networks, restricting protocols to approved windows, and implementing just-in-time access for maintenance activities. JUMPSEC strengthened exception management by adding mandatory expiry and post-change attestation. During subsequent verification, we confirmed that administrative routes were tighter and that OT exposure from IT networks had been materially reduced.

Service Overview

JUMPSEC conduct an independent review of firewall policies and network segmentation to reduce lateral movement and blast radius. The engagement analyses rule hygiene, object usage, inter-zone flows, and exception handling. Validation sampling confirms intent against real traffic paths without disrupting production. Outputs prioritise safe clean-up, segmentation improvements, and measurable governance changes.

Objectives

- Validate segmentation against trust boundaries and asset criticality
- Identify and remove risky services, unused objects, and redundant rules
- Strengthen exception management and change governance
- Produce a staged clean-up and segmentation roadmap

Approach

Evidence-led analysis of configurations, rulebases, and representative flows. Work uses exports and read-only access, with targeted non-disruptive checks in agreed windows. Stakeholders typically include Network, Security, and Operations teams, plus relevant suppliers.

Method

- **Plan** — confirm zones, critical flows, artefacts, windows, and evidence handling
- **Analyse** — review rules, hit counts, objects, services, NAT, and logging
- **Validate** — sample key flows against intended policy and zone design
- **Debrief** — classify issues, document precise changes, and sequence actions
- **Improve** — optional verification to confirm policy and flow outcomes

Deliverables

- Executive summary highlighting highest-value changes and risk reduction
- Segmentation & Policy Assurance Report covering:
    - Zone model and trust boundaries with rationale
    - Rule hygiene (shadowed, redundant, unused, risky any-any) and service exposure
    - Object and address-group hygiene (duplicates, stale entries, sprawl)
    - Intra/inter-VLAN flows and privileged pathways (admin/jump/backup)
    - Exception and change governance, with expiry and review mechanics
    - Sampled flow validation results and before/after intent diagrams
- Issue register (CSV/XLSX) with severity, owners, due dates, acceptance criteria
- Staged 30/60/90-day clean-up and segmentation roadmap with rollback points
- Optional verification letter after change windows
- Standards and alignment embedded in reporting: CIS control references for segmentation and firewall management; MITRE ATT&CK lateral-movement techniques used as rationale for hardening; governance mapped to NIST CSF/NCSC CAF where helpful (no SOC engineering required)

Outcomes and benefits

- Smaller blast radius and clearer, auditable policy
- Fewer risky services and legacy protocols across trust boundaries
- Tighter exception control and faster, safer policy changes
- Improved confidence in inter-zone flows supporting critical services

Pricing model

Fixed price per scoped policy set or time-and-materials aligned to SFIA. Price factors: device/vendor mix, rulebase size, site count, artefact availability, and optional verification.

Timelines

- Planning and artefact collection: up to 1 week
- Analysis and validation: 1–2 weeks (scope dependent)
- Report issue: 5–10 working days after testing completion

- Optional verification review based on findings and recommendations

Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

Team and roles

- **Engagement Lead** — scope, governance, quality management, stakeholder alignment
- **Network Security Consultant(s)** — rule/flow analysis and validation sampling
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead
- Provide rule exports, diagrams, and change window approvals
- Arrange supplier participation where managed devices or services are in scope

JUMPSEC responsibilities

- Operate within agreed rules of engagement and change control
- Conduct a non-disruptive review and minimise operational impact
- Secure handling and time-boxed retention of data and artefacts

Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

Constraints and assumptions

- Non-destructive activities performed in approved windows
- Third-party participation requires prior written approval
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Network Architecture / Asset Discovery
- Internal Network Penetration Testing
- Detection Engineering and Use Case Tuning

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com