Doorman – Service definition

Contents

Contents 2
Doorman – Service Definition 3
1. Service overview 3
2. Service scope and delivery models 4
3. Key features and benefits 5
4. System requirements and constraints 6
5. Security and compliance 7
6. Onboarding and offboarding 8
7. Support and service management 9
8. Availability and resilience 10
9. Data handling and exit 11
10. Pricing assumptions 12
11. Document control 13

Doorman – Service Definition

1. Service overview

Doorman is a network traffic filtering, enforcement, and monitoring service designed to protect and assure the security of IPsec VPN deployments. It operates as an independent control in front of existing VPN gateways, helping organisations detect misconfiguration, prevent insecure protocol usage, and maintain alignment with NCSC guidance over time.

The service is deployed within the customer’s network or cloud environment and does not rely on supplier-operated datacentres. Doorman can be delivered as customer-managed infrastructure software with supplier assistance, or as a fully managed service operated by the supplier.

2. Service scope and delivery models

Doorman is available in the following delivery models:

Customer-managed deployment (iSaaS)

- Deployed by the customer on physical, virtual, or cloud infrastructure
- Supplier provides setup assistance, guidance, and optional support
- Customer retains operational control of the environment

Supplier-managed service (SaaS)

- Deployed and operated by the supplier within the customer's environment
- Supplier manages configuration, updates, and operational health
- Customer consumes the service outputs, telemetry, and reports

Doorman augments existing VPN services and does not replace VPN gateways or provide VPN termination.

3. Key features and benefits

Key features

- Independent enforcement layer for IPsec VPN traffic
- Real-time inspection of IPsec and IKE control-plane traffic
- Enforcement of approved cryptographic profiles
- Blocking of deprecated or insecure protocols
- Prevention of plaintext traffic leakage
- Detailed logging, telemetry, and event generation
- Integration with customer SIEM and monitoring platforms

Key benefits

- Reduced risk from VPN misconfiguration
- Improved visibility of VPN security posture
- Ongoing assurance against cryptographic drift
- Defence-in-depth without replacing existing infrastructure
- Faster detection and investigation of security issues

4. System requirements and constraints

System requirements

- Existing IPsec-compliant VPN gateway or managed VPN service
- Network capability to deploy the service inline with VPN traffic
- Supported physical, virtual, or cloud hosting environment
- Adequate compute capacity for expected traffic volumes
- Connectivity to customer logging or SIEM platforms (optional)

Constraints

- Supports IPsec and IKE protocols only
- Does not provide VPN tunnel termination or client services
- Availability depends on deployment architecture
- Advanced detection features may require additional integrations

5. Security and compliance

The supplier aligns its security practices with NCSC Cyber Essentials and Cyber Essentials Plus requirements.
Security controls include:

- Secure configuration and access control
- Least-privilege administration
- Patch and vulnerability management
- Incident identification and response processes

Doorman operates within customer environments and does not store customer data in supplier-operated datacentres.

6. Onboarding and offboarding

Onboarding

- Supplier-led setup and configuration
- Deployment validation and testing
- Assistance with SIEM and telemetry integration
- Guided troubleshooting during initial deployment
- Provision of onboarding documentation

Offboarding

- Controlled service withdrawal and decommissioning
- Termination of telemetry and integrations
- Provision of offboarding documentation
- Support during the agreed exit period

7. Support and service management

Support is available as a paid option and may include:

- Email and online ticketing support
- Support during agreed business hours
- Prioritised response options by agreement
- Access to a cloud support engineer or technical account manager (premium tiers)

Incident handling includes acknowledgement, investigation, and reporting appropriate to incident severity.

8. Availability and resilience

Doorman is designed to support resilient deployments through:

- Multiple service instances
- Cloud-native high availability and failover mechanisms
- Physical appliance redundancy using link aggregation or load balancing

The supplier does not operate datacentres for this service.
Resilience is provided by the customer's hosting environment and chosen architecture.
Availability SLAs are agreed contractually where applicable.

9. Data handling and exit

- Telemetry, logs, and packet captures are exported in standard formats
- Data is forwarded to customer-owned systems during operation
- No proprietary data formats are used
- Customers retain ownership of all service-generated data

At contract end, data extraction is supported and the service is securely decommissioned.

10. Pricing assumptions

The base service includes deployment and core functionality as agreed.
Additional costs may apply for:

- Enhanced or premium support levels
- Extended onboarding or offboarding assistance
- Bespoke configuration or integration work

11. Document control

- Document version: 1.0
- Review cycle: As required following service changes