

MANAGED FIREWALL



ABOUT US

At Barrier, our mission is to help our customers build cyber resilience and develop strategies to defend against cyber-attacks. We have developed a portfolio of services and solutions that suit customers small and large, in both the private and public sector. Our portfolio encompasses security consultancy, solutions from innovative vendors to mitigate attacks, through to managed services that proactively detect attacks and provide swift incident response measures.

We have built a practice dedicated to providing assurance that systems are resilient to attack. We provide penetration testing services to check the effectiveness of the deployed controls against real-world attacks, and we can implement a vulnerability management system to maintain levels of operational resilience.

Our aim is to build trust and understanding of how our customers' organisation functions. Our work takes us across all sectors, with strong references in the Finance Sector, Data Hosting, Legal, Local Government, MOD, and the wider Public Sector.

Established in 2006, we are a cybersecurity-focused solutions and service provider. Our customers trust Barrier as a strategic part of their cybersecurity team and here's why:

- Our knowledge of the cybersecurity industry helps select the right solutions
- Our experience helps organisations build cohesive cyber resilience strategies
- Our people are empowered to work closely with our customers to forge strong partnerships
- Our services become an intrinsic part of our customer's security operations

The copyright in this work is vested in Barrier Networks Limited and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under direct agreement or with the consent in writing of Barrier Networks Limited.

No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing to any third party, being an individual firm or company, or any employee thereof without the prior consent in writing of Barrier Networks Limited.



SERVICE OVERVIEW

Barrier's Managed Firewall service is based on a cloud-managed platform with hardware appliances deployed at the customer network perimeter to secure traffic flow. Each device is configured to customer-specific security requirements, with continuous monitoring, day-to-day administration, and impact advice for requested changes.

SERVICE FEATURES

- **Multi-Vendor Firewall Platform:** Scalable hardware and software from leading vendors, tailored to organisation size and complexity to secure the network perimeter.
- **Security Policy Development:** Collaborative development of a base security policy to filter traffic based on source, destination, protocol and port.
- **Remote User VPN Access:** Secure IPsec and SSL VPN connectivity with configurable traffic inspection, flexible authentication (LDAP/RADIUS) and optional external two-factor authentication systems.
- **Site-to-Site VPN:** All supplied devices are fully capable of supporting VPNs to firewalls, routers, and other compatible devices as required by the customer organisation.
- **Address Translation:** Configuration of devices to perform address translation (Network Address Translation (NAT) and Port Address Translation (PAT)) in alignment with customer organisation requirements.
- **Monitoring and Event Management:** Cloud-based monitoring managed firewall devices using secure, PCI-DSS compliant channels, tracking performance, health, and traffic metrics, with events assessed and categorised for timely alerting and investigation.
- **SIEM Configuration:** Capability to configure the managed device(s) to log security alerts to a customer's SIEM solution.
- **Dashboard Access:** Provision of highly configurable management and performance dashboards.

Advanced Tier Features (Available on Certain Firewall Models): Intrusion Detection and Intrusion Prevention Services, Malware Threat Analysis, and Web & Application Filtering

SERVICE DELIVERABLES

- **Firewall Audit Review and Report:** Review of existing security architecture and policies. A report will be produced accordingly, detailing recommendations and next steps.
- **Network Security Consultation:** Workshop with a Barrier analyst to understand traffic flows within the organisation.
- **Base Security Policy Documentation:** Development and provision of documentation pertaining to a collaboratively developed security policy, with full ownership of the policy retained by the customer.
- **Security Management and Monitoring:** Operational within the boundaries of the Managed Firewall Service Level Agreements.
- **Break/Fix Maintenance:** Included for all managed service software and hardware components.
- **Service Reporting:** Ongoing performance management reporting inclusive of key service metrics. Barrier will host quarterly service review meetings.

SERVICE OUTCOMES

- **Enhanced Security Posture:** Protect the network perimeter and data flow through the enforcement of security policies tailored to your requirements.
- **Operational Resilience:** Continuous monitoring and administration, reducing the risk of downtime and security incidents.
- **Secure Remote Access:** Enable reliable and flexible VPN connectivity for remote users and site-to-site links while maintaining traffic inspection and authentication controls.
- **Scalable Adaptability:** Flexible hardware and configuration options allow the service to grow and adjust to evolving organisational security and network requirements.
- **Reduced Response Time:** Detect the presence of a successful breach within hours or minutes.
- **Simplified Management:** Centralised dashboards and management streamline oversight, reporting, and change impact assessment for IT teams.

SERVICE LEVELS

Barrier's Managed Firewall service levels are set forth below (based on CPE):

Firewall Size	Deployment	Service Tier	NGFW	Analysis	Dashboard
Small	Standalone	Standard	⊗	Add-on	✓
Small	Highly Available	Standard	⊗	Add-on	✓
Small	Standalone	Advanced	✓	Add-on	✓
Small	Highly Available	Advanced	✓	Add-on	✓
Medium	Standalone	Standard	⊗	Add-on	✓
Medium	Highly Available	Standard	⊗	Add-on	✓
Medium	Standalone	Advanced	✓	Add-on	✓
Medium	Highly Available	Advanced	✓	Add-on	✓
Large	Standalone	Standard	⊗	Add-on	✓
Large	Highly Available	Standard	⊗	Add-on	✓
Large	Standalone	Advanced	✓	Add-on	✓
Large	Highly Available	Advanced	✓	Add-on	✓

Service Level Agreements: Barrier will endeavour to meet the following SLAs:

Priority	Impact	Response SLA	Resolve SLA
P1: Critical	Major impact to business functionality or capability.	30 minutes	1 business day
P2: High	Severe impact to business functionality or capability.	1 hour	1 – 2 business days
P3: Medium	Warnings that could lead to disruption.	24 hours	3 business days
P4: Low	No service impact.	48 hours	5 – 7 business days

NB: For large or complex incidents, varying factors may extend resolution times.

SERVICE CHANGES: Upon a customer's request, Barrier can carry out changes to the service. Customers are allocated a fixed number of change requests per month. These changes can range from standard to complex and will be determined by a Barrier engineer upon receipt of the request. Complex changes may require additional consultancy time at additional cost – this will be discussed and agreed with the customer prior to any change being carried out.

EXCLUSIONS

Services that Barrier will not provide as a part of our Managed Firewall Service are set forth below. Barrier maintains no responsibility for and is not obligated to support:

- 3rd party components to which managed devices are connected (unless under direct management by Barrier)
- Service impacting incidents or errors caused by erroneous information supplied to Barrier.
- Service impacting incidents caused by unauthorised modifications or alternations not carried out by Barrier or the vendor.
- Application performance issues not directly related to managed firewall devices.
- Cases of incompatibility between 3rd party devices and managed firewall devices.
- Issues related to deployment settings not recommended by Barrier or the vendor.
- Issues related to software that is not supported or recommended by Barrier or the vendor.
- Issues with hardware or parts therein which are past their end-of-life (EOL) date.



BARRIER NETWORKS

272 Bath Street
Glasgow, United Kingdom
G2 4JR

✉ info@barriernetworks.com

☎ +44 (0)141 356 0101

