

Our Services

Managed Firewalls

The crucial first line of defence in protecting your company.



Why use a firewall?

Firewalls form the crucial first line of defence in protecting your company against unwanted malicious threats. But the challenge of maintaining perimeter security against these ever-evolving threats has become a headache for many organisations, which is why TelecitGroup offers a Managed Firewall service based on industry-leading security platforms and backed by skilled 24x7 live support.

What technology should I choose?

Our consultants work with you to analyse your performance, security and availability requirements to ensure that you get the right security platform. All of our solutions are tailored to your specific requirements using the latest market-leading technology, from vendors including Cisco and Check Point. Once we have implemented the hardware, we develop a security policy based on best practices in line with your requirements, and maintain it 24x7 to ensure that you receive the highest levels of security around the clock.

All of our firewall products support virtual private networks (VPN), either client-to-site for end-user applications (SSL or IPsec), or site-to-site, whether between two TelecitGroup managed devices or to an IPsec compliant customer endpoint. We support both single or two-factor authentication.

What configuration is suitable for my requirements?

We offer four standard configurations to best match your needs:

Single firewall

Cost-effective solution for single servers or pre-production sites.

Dual redundant firewalls

Resilient solution offering no single point of failure, suitable for business-critical infrastructure and high revenue websites.

Multi-site firewall pairs

If you need even higher levels of redundancy, we are able to run the firewall pair in different data centres, providing geographical redundancy.

Multi-tiered firewalls

Our most secure solution designed using different vendor equipment to reduce the likelihood of a single exploit compromising the entire infrastructure.

Related products

Our IP Multihome service provides fully-resilient Internet access and for improved connectivity, we can also provision LAN extension links between multiple sites. In addition, we can defend you against distributed denial of service (DDoS) attacks, which aim to render your website unavailable to legitimate users. If you are a target of large-scale DDoS attacks, we recommend our DDoS mitigation service that uses technology from Arbor Networks to ensure you are protected.

Why TelecitGroup?

TelecitGroup recognise that every customer's security requirements are different. That's why we offer a variety of technology options, backed by independent design expertise to make sure we can tailor the right solution to your requirements.

Our Managed Firewall service offers you the best match between cost and security:

- Wide range of different technologies at price points to suit you
- Expertise in managing perimeter security
- Consultants that help design your security policy and support your compliance efforts
- 24x7 onsite support from our Managed Services team
- Professionally run network managed to ISO27001 and ISO9001 standards

Key benefits

Available

Active monitoring and full hardware support 24x7 ensures maximum uptime and availability.

Optimised

Policy reviews and recommendations to optimise availability, performance and security of the firewall at all times.

Comprehensive

Remote firewall management provides support for remote or regional businesses with limited technical resources.

Up-to-date

Full maintenance including regular vendor updates and periodic upgrades provides effective protection against new vulnerabilities.

Capacity planning

We monitor your firewall platform to ensure that the technology scales with your business. This includes identifying projected traffic requirements, for example, to allow for seasonal peaks that place the solution under greater load.

Secure access

Integration of VPN access with the managed firewall service provides a secure tunnel between a user and the solution, allowing seamless encrypted connectivity to hosted infrastructure.

Multi-layered

Selected firewall platforms include the ability to deploy application-level security and intrusion prevention technology to further enhance the secure environment.

Deployment			
Type	Description	Applications	Architecture
Single firewall	A cost-effective, non-resilient security solution that provides one or more networks with filtering and routing based on a defined policy.	<ul style="list-style-type: none"> • Entry-level security platforms • Proof of concept projects 	
High-availability firewall pair	TelecitGroup will configure two firewalls in a highly available clustered pair via diversely connected internet handoffs. This solution provides a resilient network architecture with no single points of failure and minimal unplanned downtime. In addition, we are able to split the firewall pair over different data centres.	<ul style="list-style-type: none"> • Business critical infrastructure • High revenue websites • Split-site option for higher levels of redundancy 	
Multi-tiered firewalls	Provides increased security and performance by segregating the network over two or more physical firewalling layers. For maximum security, these layers can utilise multiple vendors thus reducing the likelihood of a single exploit transgressing the entire infrastructure.	<ul style="list-style-type: none"> • Websites with highly sensitive information • Enhanced level of security 	

Technical details

- High specification unified threat management (UTM) platform from Check Point offering anti-malware, URL filtering, spam filtering, quality of service and intrusion prevention with daily definition updates
- Affordable and proven hardware-based firewalling from Cisco. Integrated FastEthernet switch on low-end models appropriate for smaller solutions
- Deep inspection firewall services for HTTP, FTP, Extended Simple Mail Transport Protocol (ESMTP), and more
- Other available features include: routing (static or dynamic), network address translation (NAT), IKE v2, 802.1q, basic layer-4 load balancing

Management

Our support team optimises the performance of your firewall device to ensure it continues to operate effectively. This service includes:

- Preventative maintenance including patches, upgrades, error log review and traffic analysis
- Firewall configuration reviews and recommendations to assess availability, performance and security considerations
- 24x7 support of the firewall platform to ensure prompt response to performance or hardware issues



**Outstanding data centres.
Expertise you can trust.**

Europe's leading provider of premium network-independent data centres.

www.telecitygroup.com

VPN Deployment Options

Type	Description
Client-to-site	TelecityGroup supports the deployment of client-based VPNs via Check Point SecuRemote software and Cisco VPN Client software with security provided by either SSL or IPsec. We can also provide two-factor authentication for client-to-site VPNs using SSL or token based devices. These solutions are priced per client.
Site-to-site	When a secure encrypted tunnel is required, TelecityGroup can setup a VPN between firewalls at each site. Unmanaged customer VPN endpoints must be IKE/IPsec compliant. This connectivity solution is priced per setup of each VPN Tunnel.

Service response time

Service	Response Time
Notification of monitoring alerts	15 minutes
Response to customer requests	15 minutes
Hardware failure fix	Within 4 hours
Firewall rule changes	Completed within 4 business hours
Software upgrades and patches	Quarterly

Contact TelecityGroup

10th Floor
6 Harbour Exchange Square
London E14 9GE

+44 (0)20 7001 0101
info@telecity.com