

# Managed Monitored FIREWALL Protecting YOUR BUSINESS

JT's Managed Firewall Service provides 24/7x365 remote management and monitoring for customers' firewall and security devices. JT secures the Customer's network perimeter, managing industry-leading firewall platforms from Cisco Systems, utilising its comprehensive ISO27001-certified, ITIL-aligned service management framework. The service includes proactive configuration, monitoring, performance and capacity management and access to JT's support capability, technical skills and vendor relationships.

## Supported Devices

Vendor	Model
Cisco	ASA Adaptive Security Appliances
Fortinet	All Appliances and VMs, FortiManager, FortiAnalyzer
Meraki	MX Series Security Appliances
PaloAlto	Appliances, VMs and CloudProtect

## Supported Configurations

Availability	Description
Single Firewall	A standalone Firewall
High Availability (HA) Firewall configuration	Two Firewalls of compatible models in an active/passive configuration, both of them connected at the same time.
Firewall Clustering	Two Firewalls of compatible models in an active/active or active/passive configuration and automatic switch over.

## Managed Service

The offer is available with three service levels:

**Support Services** – Hardware and Software maintenance is undertaken by the JT Engineering team and/or approved JT partners.

**Remote Monitoring Service** - intended to support Customers by detecting, and managing the resolution of service issues, mitigating any impact to critical business operations.

**Proactive Managed Service** – this service is multifaceted – its main purpose is to ensure uninterrupted operation by resolving issues before they arise. It provides intelligence regarding network utilization and traffic visibility via a client access web portal.



### Service Requests

The table below outlines specific tasks that are included as part of the Managed Firewall Service. All requests are known changes with agreed standard operating procedures. All these tasks are performed during business hours.

Task	Description
Management of Zones and Access rules	Creation, change and deletion of Zones and Access Rules configured in the device that allow and deny traffic to/from the Internet, WAN, DMZs, and Internal networks.
Creation and Management of NATs	Creation, change and deletion of NATs rules
Creation and Management of IDS/IPS/APP-FW Features	Creation, change or deletion of Intrusion Detection, Prevention and Application Firewall policies and features (Customer-defined policy)
Management of network interfaces	Creation and changes in the network interfaces parameters (IP addresses, subnets, gateways)
Creation and Management of IDS/IPS/APP-FW Features	Creation, change or deletion of Intrusion Detection, Prevention and Application Firewall policies and features (Customer-defined policy)



Management of Failover	For HA or clustering configurations: Management of failover policy to allow the service to continue working if a device error occurs
Log and SNMP system configuration	Management of the log information resending to a syslog server and SNMP alerts/traps
Management of manufacturer's guarantee	Management of hardware or firmware errors with the manufacturer. Customer needs to contract a valid manufacturer support for this management to be effective and Customer needs to require us to open a support case
Management of disk space	Evaluation and study of actions for freeing and optimizing disk space (if disk is present in the device)
Restore of data	Restore of device configuration from the backup (if any)

To find out more contact us at:

T UK/Int: +44 20 7920 2000

E sales.jtge@jtglobal.com

W www.jtglobalenterprise.co.uk