



Service Catalogue

Your secure data centric guardians

Units 1-3 Trinity Court, Brunel Rd, Totton, Hampshire SO40 3WX

www.amicusits.co.uk

+44 2380 429429

Network & Firewall Administration

1 Introduction

Amicus ITS are secure data centric guardians. We follow the tough regulatory procedures of ISO 20000, ISO27001 and ISO 9001, along with the process frameworks of PRINCE2 and ITIL_v3 methodologies. As a leading provider of managed IT and cloud services, we specialise in delivering holistic solutions tailored for our customers in healthcare, public sectors, regulated markets and to blue chip corporates. Amongst our capabilities, we are specialists in design and build and maintaining services to align with boardroom strategies.

2 Objectives and Benefits

Amicus ITS offers a comprehensive solution where we manage the complex network and next generation security for our customers. This removes the resource-intensive operations from their inhouse support team, which could include considerable configuration changes on a daily basis.

We proactively monitor the customer's IT infrastructure from our central location, affording greater co-ordination and peace of mind, with no geographical boundaries for their infrastructure.

Amicus ITS has many years of managed service experience and brings extensive knowledge on network design, firewall design, network administration and Disaster Recovery. Our Network Administrators explore and solve problems logically and consistently, including analysing and critical thinking of the issues.

Amicus ITS provides security and risk consulting, through its inhouse Security & Compliance Team. They provide an array of services to address information security, plus risk and compliance needs for our customers.

We help customers identify vulnerabilities and assess real business risk, assist with meeting security compliance requirements efficiently and effectively, devise security and governance programmes that are the right fit for the customer's environment - and help them recover and prepare for cybersecurity breaches/threats.

3 Service Scope

Our Network and Firewall Administration Service includes all network and security equipment (routers, switches, firewalls, load balancers etc.). Amongst these service activities we provide the following:

- Monitoring
- Administration
- Review of alarms
- Filtering for false alarms
- Escalation of issues
- Customising monitoring thresholds
- Configure notification and escalation policies to ensure all monitored systems are available, healthy and performing

Our tools are capable of monitoring all aspects and dynamics of the network and firewall infrastructure, which provides us with a wealth of information that we use for troubleshooting and problem detection.

Network & Firewall Administration / Contd.....

NETWORK AND FIREWALL ADMINISTRATION	Basic	Enhanced	Advanced
Real-time 24x365 agentless monitoring through software / hardware probes for availability, health and performance via SNMP and CLI protocols	✓	✓	✓
Securing network systems by establishing and enforcing policies, and defining and monitoring access	✓	✓	✓
Up to 4 hr tailored SLAs - multi-level thresholds and instant notification	✓	✓	✓
Remediation of alarms based on an agreed-upon set of tasks and run lists	✓	✓	✓
Troubleshooting network problems and outages - undertaking data network fault investigations in local and wide area environments, using information from multiple sources - remote troubleshooting and fault-finding if issues occur	Optional	✓	✓
Basic configuration of firewalls	Optional	✓	✓
Basic configuration of routing and switching equipment	Optional	✓	✓
Remote assistance to onsite engineers and end users / customers	Optional	✓	✓
Capacity management and audit of IP addresses and hosted devices within data centres	Optional	Optional	✓
Automating configuration tasks - automate all repetitive, time-consuming configuration management tasks. Apply configuration changes in bulk	Optional	Optional	✓
Compliance auditing - define standard practices and policies and automatically check device configurations for compliance	Optional	Optional	✓
Real-time change tracking - monitor configuration changes, get instant notifications and prevent unauthorised changes	Optional	Optional	✓
User activity tracking - get complete record of who, what and when detail of configuration changes. Record actions, archive and playback	Optional	Optional	✓
Firewall used rules monitoring	Optional	Optional	✓
Advanced configuration of firewalls	Optional	Optional	✓
Advanced configuration of routing and switching equipment	Optional	Optional	✓

Network & Firewall Administration / Contd.....

Bandwidth monitoring and traffic analysis - collect, analyse flows from major devices like Cisco, 3COM, Juniper, Foundry Networks, Hewlett-Packard, extreme and other leading vendors	Optional	Optional	✓
Network forensics and security analysis	Optional	Optional	Optional
Switch port & IP address management	Optional	Optional	Optional
Establishing a networking environment by designing system configuration, directing system installation, defining, documenting and enforcing system standards	Optional	Optional	Optional
Design and implementation of new solutions and improving resilience of the current environment	Optional	Optional	Optional
Upgrading data network equipment to the latest stable firmware releases - firmware upgrade and OS images transfer	Optional	Optional	Optional
Detect rogue devices - identify the rogue device intrusions and block their access	Optional	Optional	Optional
Firewall security analysis	Optional	Optional	Optional
Firewall compliance report with security audit and configuration analysis	Optional	Optional	Optional
Virus, attack, security and spam reports from firewall logs	Optional	Optional	Optional

4 How We Provide This Service

- We have a team of trained and Original Equipment Manufacturer (OEM)-certified Network Administrators, with required experience, exposure and skillset. This service is primarily provided by the NOC Team with optional services from the Service Desk, Change and Configuration Management team, and Service Delivery Managers.
- The NOC Team maintains the interaction with the customer throughout the service lifecycle unless the customer has availed Service Desk services / SDM Services.
- We have a 24x365 monitoring team, monitoring the network infrastructure for our customers. The network administration team works as a point of technical escalation.

Network & Firewall Administration / Contd.....

5 Service Reporting

The standard Network Administration Reports include:

- Network Availability Report
- Network Health Report
- Network Performance Report

Other reports can be included based on the subscribed optional services.

6 Service Pricing

The Service pricing is based on a per device basis. Where optional services are projects, these will be priced separately.