



## Managed Firewall Service

**Our Managed Firewall Service provides full management of devices that ensure we increase the integrity of a customer's security solution.**

### **The service delivers:**

#### **Traceability**

The service ensures there is complete visibility so tracking incidents or breaches can be easily achieved with confidence. All events can be monitored and tracked and the Networks First team of security specialists check and validate all changes being made against known vulnerabilities.

#### **Increased Stability**

All manufacturer-recommended upgrades, patches and fixes are applied so you are always up to date on all known vulnerabilities. To ensure we manage the risks effectively and increase the resilience of your solution these are applied following testing in Networks First Lab environment.

#### **Traceability**

Managing security is as much about having the time and skills as it is the hardware. Our team of security specialists ensure you stay abreast of the latest firewall developments including IPS/IDS, URL Filtering, Anti-Spam/Anti-Malware, and manage the devices accordingly so that maintaining high levels of security doesn't consume your budget.

### **Managed Firewall Service features:**

- ▶ Available on a range of Cisco ASA and Check Point devices
- ▶ Patch Management
- ▶ Firewall change verification process
- ▶ Security Information and Event Monitoring (SIEM)
- ▶ Compliance Reporting
- ▶ Vulnerability Scanning

## Oversight not hackers is the key concern

It may be less dramatic than the threat of hackers but it is true to say that most security issues are in fact as a result of an accidental oversight, a human error. Common examples of how this occurs include a firewall administrator may temporarily permit the application developer to test their new application, or where the change board may be more focused on the processes than technically underwriting the change.

Our Managed Firewall Service is designed to back our view that the blame doesn't fall on the person whose request caused the vulnerability, it falls on the people or processes who allowed this to happen.

## Unified Threat Management rather than single device management

It used to be easy to define the network perimeter however; wireless LAN, smartphones and self-service portals have all made this less rigid. Security management has moved from single device management to unified threat management. The firewall has ceased to become a single 'gate-keeping' device and more of an intersection point to all entry points to today's network.

## The Full Service Includes:

- ▶ Review of policy changes with all known vulnerabilities and checks against your internal company changes
- ▶ Our dual management station replicates the management platform so changes can be made if the primary platform fails
- ▶ Complete visibility of the rule base ensures total transparency
- ▶ Ongoing security information and event monitoring and vulnerability scanning
- ▶ Firewall change verification process
- ▶ Firewall topology and configuration review ensuring adherence to industry best practices
- ▶ PCI and CoCo log monitoring compliance
- ▶ Quarterly advisory reports on product developments that impact on the firewall
- ▶ Quarterly review meetings
- ▶ Reports on hot fixes and patch upgrades on any emerging end of life equipment
- ▶ Regular security bulletins on relevant security issues
- ▶ End of Life Support



## Our commitment

At Networks First our commitment is to **Do More.** We achieve this through our multi-vendor engineering skills, our guaranteed SLA and 'fix' time and employee dedication to go that extra mile. All of this ensures we can **guarantee** your communication infrastructure.

For more information on Networks First's **Guarantees, Accreditations and Services Portfolio,**

visit [www.networksfirst.com](http://www.networksfirst.com)