INTECHNOLOGY

MANAGED FIREWALL SERVICE DEFINITION

SD007 v3.0
Issue Date 19th July 2013

inTechnology
MANAGED SERVICES

SECTION 1: OVERVIEW

SERVICE OVERVIEW

InTechnology's Managed Firewall Service provides Customers with a hardware firewall that controls traffic between devices on different networks. The firewall is configured to a Customer's specific requirements. The service is designed to offer passive defense, providing restrictions on the source and destination IP addresses and service ports that are allowed to pass through the firewall.

The function of any firewall service is to filter traffic coming into a network (also called border protection) based upon pre-determined criteria. No firewall can protect against all protocol or application weaknesses, and new software vulnerabilities are discovered regularly. All devices protected by a firewall should be administered with the same level of diligence as if the firewall were not present.

SUMMARY

- InTechnology offers market leading firewall appliances.
- Single device or High Availability Firewall Pairs are available.
- Support for site-to-site Virtual Private Networks (VPN)
- Support for remote client VPNs for home workers.
- Utilises Network Address Translation to hide Customer network addresses from the Internet.
- Fully configurable rule-base managed by InTechnology's trained professionals.
- Customers receive advice and guidance on the effectiveness of the implemented rule-base, and any proposed changes.

LIMIT OF LIABILITY

Security vulnerabilities can arise through many causes and no firewall can offer protection against all protocol vulnerabilities.

InTechnology recommends that Customers make regular use of security scanning services and applications to monitor network and application security. It is essential that InTechnology is notified in writing of the intent to perform such scans in good time.

InTechnology does not offer intrusion detection services (IDS) and intrusion prevention services (IPS) as part of the Managed Firewall Service. InTechnology recommends that Customers deploy network and host IDS/IPS as part of their overall security policy.

SECTION 2: SERVICE DEFINITION

CUSTOMER SECURITY POLICY

InTechnology provides, configures and maintains the managed firewall hardware, and configures the firewall(s) with bespoke rules configured to meet the Customer's operational requirements. It is recommended that prior to implementing any firewall solution the Customer undertakes a full security review. One component of this security review should be the creation of a network security policy. The security policy can form the basis of the firewall rule-base that will be implemented on the firewall(s).

FIREWALL HARDWARE MODELS

Cisco Systems ASA devices are most commonly deployed as part of InTechnology's Managed Firewall Service. Cisco produce a number of chassis to meet the needs of Customers looking to deploy firewall devices at SOHO sites through to very large corporate head offices. The devices are E3 approved enterprise firewall appliances from one of the world's leaders in networking solutions.

InTechnology does not currently offer hardware options for VPN acceleration, IDS/IPS etc.

SOFTWARE LICENSES

All licensing costs required to deliver the service are included in the monthly service charge.

INSTALLATION/CONFIGURATION CONSULTANCY

The service includes basic security policy development by one of InTechnology's technical specialists. The objective is to document network objects and applications, and to determine the required network traffic restrictions and controls.

The standard consultancy time allocated to this work is half a day.

If the implementation has special requirements, such as proprietary equipment needing access through the firewall, additional consultancy may be required and will be charged accordingly.

DEFAULT SECURITY POLICY

The default firewall rule-base assumes that all outbound traffic is to be permitted and all inbound traffic is to be denied. This can of course be overridden during the initial deployment or modified at any point in time using the Firewall Change Request form (please see the appropriate section below).

VIRTUAL PRIVATE NETWORKS

InTechnology supports IP-Security (IP-sec) VPN connections to Cisco firewalls and routers, and other devices where compatibility exists. In such cases, the following applies:

IP-sec authentication based upon shared secret passwords

IP-sec encryption using 56-bit Data Encryption Standard (DES)

3DES may be available subject to conditions being met.

InTechnology cannot guarantee the compatibility of the VPN service unless InTechnology manages the firewalls at each end.

InTechnology does not currently offer Secure Socket Layer (SSL) based remote access.

NAT and PAT

The firewalls are configured to translate addresses as part of the standard security implementation. Depending upon the number of addresses available and the required functionality, Network Address Translation (NAT), Port Address Translation (PAT), or a combination of the two may be deployed. It is not always necessary or desirable to translate the addresses of traffic on VPN tunnels.

LOGGING AND ANALYSIS

Basic logging information is captured and stored for one month on InTechnology's servers. This information is available on request and can be analysed by Customers and used to constantly improve security stance as part of their security policy. InTechnology does not perform analysis of alarm logs although this can be arranged through a third-party partner if required.

MANAGEMENT

InTechnology manages all firewall solutions via a dedicated interface or sub-interface on the firewall. Within an InTechnology Data Centre, the management VLAN connects directly to the firewall. When a firewall is installed on a Customer site, it is a pre-requisite that the site is connected to the InTechnology network using the LANnet Service, which hosts the management link for the firewall.

SERVICE DELIVERY

InTechnology's service delivery staff will review the proposed rule-base with the Customer and provide feedback and/or recommendations as required. Firewalls can be located on a Customer site or within an InTechnology Data Centre.

If the firewall is to be deployed within an InTechnology Data Centre it would usually be installed within a rack set aside for 'Managed Devices'. If the Customer has subscribed to InTechnology Co-location Service, the firewall(s) can be located in the Customer's environment to simplify connectivity to multiple Demilitarised Zone (DMZ) devices if required.

If the firewall is to be deployed on a customer site, an InTechnology engineer will visit site and undertake installation, configuration and basic testing.

MONITORING / ALARMS

InTechnology polls Managed firewalls regularly to check for availability and critical events (these include hardware failures, environmental alarms etc. where available). Service tickets are automatically generated on the InTechnology system when faults are detected. The tickets are managed by skilled engineering professionals in InTechnology's Operations Centre.

IMPLEMENTATION OF CHANGE REQUESTS

During the implementation phase, the Customer will be provided with a Firewall Change Request form. This should be used to submit change requests during a contract term.

The validation and consequential implementation or rejection of change requests will be performed Monday to Friday between 8 am and 6 pm, with a target completion time of 48 hours for routine changes. Emergency changes are prioritized accordingly, and performance targets are detailed in InTechnology's Customer Service Plan.

In accordance with the InTechnology change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If InTechnology's security engineer cannot validate the change requester against the authorised list, then InTechnology will place the change request on hold and attempt to contact one of the alternative authorised contacts. InTechnology must wait for the request to be ratified by a known authorised contact before proceeding with any firewall change. It is therefore essential that Customers provide accurate and current contact information for their designated and authorised staff.

It is extremely easy to weaken network security by submitting a seemingly innocuous change request. InTechnology staff review change requests based only on the information they have available therefore InTechnology cannot take responsibility for network weakness resulting from rule-base changes. If InTechnology support staff believe that a rule-base change request compromises the security of the Customer's network, InTechnology may ask the Customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered. In extreme cases, staff reserve the right to reject the change outright; for example if the weakness could affect other InTechnology customers.

SECTION 3: CHARGING POLICY

CHARGES

Charging for the Managed Firewall service consists of a one-off Installation Charge and a Recurring Charge which is payable monthly in advance.

Installation Charges specific to Managed Firewalls include the components listed below:

- Pre-sales consultation
- Security design consultancy (4 hours)
- Firewall configuration & implementation
- Project management
- Installation of the Firewall on the Customer site or within the InTechnology Data Centre
- Service testing and internal documentation

This work will under-taken during normal office hours (9:00 – 17:00 Monday to Friday excluding Bank Holidays).

Any Customer requests for work to be completed outside of these hours will be accommodated where possible and such work will be subject to additional charge.

All other components will carry additional charges, including, but not limited to, the following items:

- Additional consultancy time required for complex routing, rule-base or VPN requirements
- Any work required to make sites 'ready' for new service (e.g. Cabling or configuration of existing devices)
- Any documentation produced for the benefit of the Customer detailing the implemented solution

The Monthly Recurring Charge for the service incorporates:

- Depreciation of the hardware
- Power & Space if located in a Managed Services Rack within an InTechnology Data Centre.
- Change Control
- Software and hardware support

Minor Configuration Changes

InTechnology undertakes 'change' projects on a 'fair use' basis (please see InTechnology's Customer Service Plan [CSP] for details); this meets the requirements of the vast majority of Customers. If InTechnology feels that a disproportionate amount of resource is required to undertake change work for a particular Customer, InTechnology will notify the Customer and subsequent work may be chargeable.

Changes are scheduled to be completed by InTechnology's engineers using a priority system with 'Emergency' changes undertaken first. 'Non-emergency' changes will usually be scheduled to be completed during office hours. If non-emergency changes are required outside of office hours, the request will be accommodated where possible and may be subject to additional charge.

SUPPORT

InTechnology supports products and services to meet the Service Level Agreement which forms part of the contract. Any support requests beyond this will be considered, and may be chargeable if implemented. For example, any major reconfiguration work required on a Customer's systems/network to provide a work-round fix for a Customer 'disaster'.

LOGGING AND ANALYSIS

Basic logging information is provided (on request) as part of the service, any requests for non standard logging is chargeable.

ADDITIONAL CHARGING

If additional charging is necessary:

- Where possible, InTechnology will issue an estimate for any chargeable work in advance.
- The figure will be calculated based on the 'standard' or 'out-of-hours' rate for the type of work and consultancy/engineering skills required

- Travel and/or other expenses will be detailed separately when applicable

As an illustration, please refer to the pricing below:

STANDARD RATES	
ENGINEER day	£750
ENGINEER hour (from)	£100
CONSULTANT day	£1000
CONSULTANT hour (from)	£120

Day rates apply to work carried out 9am – 5pm on weekdays, including 30 mins lunch break. Rates inclusive of 2 hours' travel time.

OUT-OF-HOURS RATES	
ENGINEER 'day'	£900
ENGINEER hour (from)	£115
CONSULTANT 'day'	£1200
CONSULTANT hour (from)	£140

'Day' rates apply to work carried out on bank holidays & weekends, or between 5pm and 9am on weekdays. Rate shown is per 8 hour project including 30 mins break.

Project specific quotes are available on request. Discounts may be available when 'multi-day' service bundles are purchased.

SECTION 4: SERVICE LEVEL AGREEMENT

This Service Level Agreement (SLA) defines the terms and scope of InTechnology's commitment to provide Customers Managed Services. The Service Level Agreement for the Managed Firewall service is based on the Percentage of time that the service is available for use.

SERVICE AVAIILABILITY

In calculating firewall availability and time needed to restore service, the following circumstances are excluded:

- Service unavailability as a result of contractual service suspension
- Service unavailability due to faults on the Customer's side of the Managed Firewall service including power or network failure
- Faults that do not affect delivery of the Managed Firewall service
- Service unavailability due to planned maintenance controlled outages
- Reboots required to implement policy changes

Customers are provided with a committed average availability, as listed below:

Availability	**Service Component**	**Equivalent Downtime per month**
99.5%	Single Managed Firewall hosted at an InTechnology Data Centre	3 hours 39 minutes
99.0%	Single Managed Firewall hosted at a Customer site	7 hours 18 minutes
100%	Dual Firewall in failover mode hosted at an InTechnology Data Centre	0 minutes
100%	Dual Firewall in failover mode hosted at a Customer site	0 minutes

In the dual firewall deployments configured for failover, should one of the firewalls fail, InTechnology will repair or replace the failed one as soon as possible. The failure of one firewall that does not affect the overall service will not constitute a service failure.

Faulty units hosted in an InTechnology Data Centre will usually be replaced within 4 hours. InTechnology aims to replace faulty units on customer sites the next working day.

For purposes of measuring the service's availability performance against the SLA, service availability is calculated each month. Service Credits are available where the service availability at a site falls below the committed average availability for that month (as outlined below).
For sites with a high availability failover solution, the service is deemed unavailable during the period when a qualifying fault exists simultaneously on both primary and failover devices that comprise the overall solution.
Each period of service unavailability is the time taken to restore (TTR) a qualifying fault. The TTR each qualifying fault is classed as the time from either 1)

the Customer report a fault or 2) InTechnology identifying a fault to the time the fault is rectified and the service is restored. At all other times the service is deemed to be available.

SERVICE CREDITS

If the availability of the service, as measured over one month, is lower than the committed figure, a proportionate amount of the monthly charge will be refunded by way of a service credit. The proportion will be the committed availability percentage minus the achieved availability percentage. For example, if the committed availability is 99.5% and the achieved availability is 99.2%, the service credit is 0.3% of the monthly charge.

Note: for the purposes of this calculation 1 month = 1/12th of 365 days. 'Month periods' will be measured from the first day the contract commences.

PLANNED MAINTENANCE

Planned Maintenance can involve a temporary suspension of part or all services, in order to enable us to undertake vital remedial/maintenance or upgrade work. Controlled outages will always be notified to Customers at least 7 days in advance and be planned in such a way as to have minimum impact on Customer operations. Controlled outages will not be classified as qualifying faults.

InTechnology reserves the right to carry out emergency works to maintain the integrity of the network and prevent the occurrence of a more prolonged failure. This may result in a shorter notification period.

InTechnology Head Office
Central House
Beckwith Knowle
Harrogate
HG3 1UG
Tel: +44 (0)1423 850 000
Fax: +44 (0)1423 850 001

challenge@intechnology.com
www.intechnology.com

InTechnology Reading
Commensus House
3-5 Worton Drive
Reading
RG2 0TG
Tel: +44 (0)870 777 7778
Fax: +44 (0)870 777 7779

challenge@intechnology.com
www.intechnology.com

InTechnology London
17 St. Helen's Place
Bishopsgate
London
EC3A 6DG
Tel: +44 (0)20 30 40 50 00
Fax: +44 (0)20 30 40 50 01

challenge@intechnology.com
www.intechnology.com

inTechnology