NETWORK BOX

REAL TIME
NETWORK SECURITY

PUSH
PUSH TECHNOLOGY
WHY WAIT?

FIREWALL | IDP | VPN | ANTI-SPAM | CONTENT FILTERING | ANTI-VIRUS | ANTI-HACKER

ANTI-WORM | ANTI-TROJAN | ANTI-SPYWARE | ANTI-PHISHING | ADOBE PDF REPORT SYSTEM | LIVE WATCH MONITOR | REAL TIME UPDATES

STATE-OF-THE-ART INTERNET PROTECTION

World class technology is vital. Everyone connected to the Internet is in an "arms race" with hackers, viruses, worms and spyware, whether they realise it or not. Staying one step ahead, can be the difference between being safe, or being compromised. But technology is only half the story. Even the best technology available needs to be expertly installed, configured, managed and updated to remain effective. One configuration mistake, one missing security feature or one missed update, can result in disaster. You can end up losing money, time, privacy, access, data integrity and ultimately even your credibility.

Network Box security specialists sit down with each customer to determine their exact requirements and priorities. Then, they install and configure that customer's Network Box system to suit their customised requirements. Each client will have different needs. Existing networks need to be taken into account. Organisational policies, business continuity and detailed personal preferences all need to be carefully considered.

The global system of Network Box "Security Operation Centres" monitors and manages every Network Box 24x7 year round (including environment, hardware, operating system, security modules and performance measures). Updated threat protection signatures and software packages are installed as soon as they are available, using Network Box proprietary PUSH technology. 3DES encryption and 2048bit RSA authentication keys protect the management and monitoring communication channels.

All Network Box **Security Operation Centres** *and* **Service Centres** *offer help desk support, with a range of SLA options (including "Self Managed", "Remote Managed 8x5" and "Remote Managed 24x7") to meet customer requirements. SLAs may vary in each country.*

Australia • Austria • Belgium • China • France • Germany • Gibraltar • Hong Kong • Indonesia • Ireland • Japan • Korea • Liechtenstein • Luxembourg • Malaysia • Middle East • Netherlands • New Zealand • Philippines • Russia • Singapore • Switzerland • Taiwan • Thailand • UK • USA

Security Operation Centres | Service Centres | Content Filtering Labs | Anti-Virus Labs

The Network Box Worldwide Network of Research, Data and Service Centres

WWW.NETWORK-BOX.COM

Network Box S-80

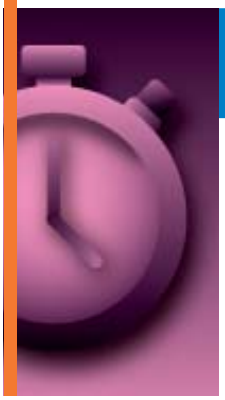
Network Box M-250

WORLD CLASS SIGNATURE DATABASE

Each Network Box includes a world class signature database, covering well over a million viruses, worms, spyware, Trojans and SPAM e-mail threats, as well as over 500 active IDP signatures, 2,500 passive IDS signatures and over 3 billion web pages (in 70 languages) for content filtering. And this database is being updated in real time, all of the time. These signatures are used in conjunction with multiple heuristic engines, to offer highly effective perimeter security, against both known and unknown, malware and Internet threats.

ANTI-SPYWARE

Spyware is rapidly becoming the number one headache, not to mention security risk, for computer users worldwide. Yet very few network security systems are able to block this relatively new type of threat. Network Box can effectively use multiple scanning engines and signature sets to block malicious Spyware downloads over HTTP and other protocols. In addition, SurfControl categorisations in the URL filtering web proxy can be used to apply company policies to control this menace effectively. All forms of spyware, adware and pornware are covered.

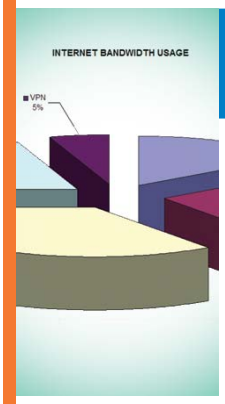


PUSH UPDATES

At the heart of the Network Box system is a global web of Network Box Security Operation Centres. These centres work around the clock, twenty-four hours a day, three hundred and sixty five days a year, PUSHING updates out in real time. Once a new anti-virus, anti-SPAM or IDP signature is available, it is immediately PUSHED out to every Network Box. The average time required to update a system is currently under 45 seconds, across all the systems Network Box manages around the globe.

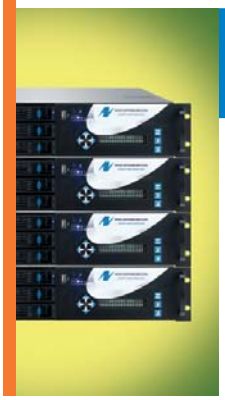
INTERNET ACCELERATION

Installing a traditional network security system can result in slower downloads. Installing a Network Box, on the other hand, can actually speed things up. Each Network Box system includes a built-in high speed Internet cache as standard. By caching previously downloaded Internet data, not only can local Internet access speed be greatly increased, but the usage of valuable bandwidth can also be optimised. Upstream HTTP proxies are fully configurable, including support for the ICP, HTCP, CARP, WCCP and Cache Digest protocols.



QUALITY OF SERVICE CONTROL

No matter how much communications bandwidth an organisation has at its disposal, it is impossible to guarantee that it will always be enough. Built into every Network Box system is the next best thing: the ability to allocate bandwidth and to shape communications traffic. By controlling bandwidth usage intelligently - e.g. by allocating 30% to e-mail, 30% to FTP and the remaining 40% to web access - it is possible to ensure that vital communication channels are always kept open.



HIGH AVAILABILITY & LOAD BALANCING

Network Box systems are built using only the highest quality components, but no matter how good the hardware is, sooner or later it will fail and will need servicing. Many businesses are 24/7 operations that cannot afford downtime. To maximise business continuity, it is possible to configure two (or more) Network Box units in high availability mode, providing total failover redundancy. This feature is available on all Network Box models. The industry standard VRRP protocol is fully supported, so the Network Box can co-exist and inter-operate with extant high availability equipment.

GUI Main Screen

Network Load Statistics

Firewall – Live Watch

IDP – Live Watch

Web Based Graphical Administrative Interface

Network Box M-380

Network Box E-1000

MULTIPLE INTERNET LINKS

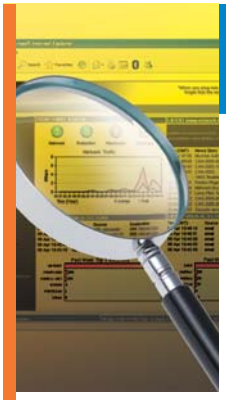
All Network Boxes include support for multiple Internet connectivity as standard. This means that it is possible to connect simultaneously to two or more Internet Service Providers. When all connections are functioning normally, their combined bandwidth is available for use. Should one of the connections become temporarily unavailable, Internet connectivity is still available over the remaining connections.

FAULT TOLERANCE

Each Network Box system from the S-50 up is built to last, using only high quality components. From time to time, however, hardware faults can still occur. Many of the Network Box models include either dual redundant power supplies, and/or RAID 1 mirrored hard disk drives, to minimise the impact of either a hard disk or power supply failure. Should a primary component fail, the back-up takes over almost instantly, without interruption of service or network protection.

HEURISTIC PROTECTION

The Network Box includes sophisticated heuristic threat detection engines as part of its comprehensive anti-virus, anti-SPAM and IDP modules. The heuristic engines combine cryptanalysis, statistical analysis, anomaly detection and protocol enforcement to detect and block new and emerging threats - providing protection against the latest macro and polymorphic viruses. Tests show that 92% of viruses can be detected and blocked by the Network Box, using heuristic technology alone, without using any of the anti-virus signatures installed.

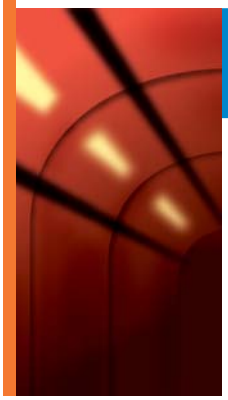


ANTI-HOAXES & ANTI-PHISHING

Social engineering and false information, aimed at tricking end users, is an increasingly common vector of attack. Indeed, these attacks are starting to make international news headlines. An extensive combination of heuristics, signatures, and blacklists is used by Network Box mail scanners to detect and block both hoaxes and phishing e-mails at the gateway to your network. Company policy can be applied either to filter these as SPAM, or to block and alert as a malicious threat.

ALERTS & REPORTS

The Network Box automatically generates comprehensive weekly and real time alert reports. Every attack on your computer system is recorded in detail, including the attacking IP addresses, number of hack attacks blocked, viruses, Trojans, spyware and worms blocked, intrusion attempts blocked, normal SPAM marked, as well as malicious SPAM blocked. Comprehensive web content filtering reporting is also available, which allows accurate tracking of Internet usage. Reports are produced in Adobe PDF format, for easy viewing, printing and filing.



SSL VPN

SSL VPN is perhaps the most convenient way for users to securely connect back to the office. Implementing OSI layer 2 or 3 secure connectivity, using the industry standard SSL / TLS protocol, flexible client authentication is well catered for. Both user, and group specific access control policies can be set, allowing access control policies to be applied directly to the virtual VPN interface. The Network Box SSL VPN implementation uses state-of-the-art authentication, certification and encryption technologies, to ensure your private data remains private, as it traverses the notoriously insecure Internet.

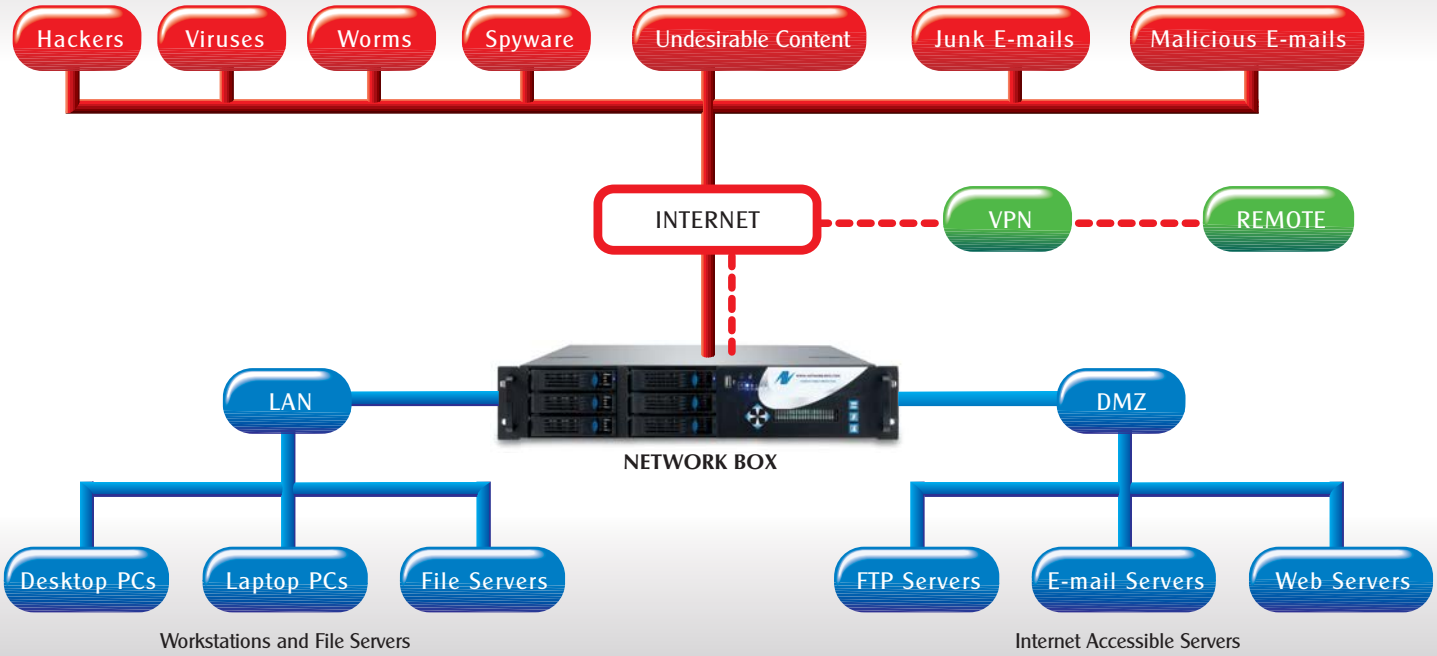
VPN Status Overview

Anti-Virus Status Overview

Anti-SPAM Status Overview

Web Proxy Analysis Overview

https://my.network-box.com



Firewall

Keep hackers out and your private data in.

At the core of every Network Box is a state-of-the-art hybrid firewall, including all three firewall technologies (packet filtering, connection tracking and proxy). The firewall supports both TCP/IP routing and NAT (Network Address Translation), and can operate in proxy-ARP transparent mode. For added protection, the Network Box firewall protects servers and workstations from a host of network-level attacks, including protocol anomalies, connection flooding, Denial of Service, SYN flooding, as well as packet fragmentation evasion techniques. Black hole, fingerprint obfuscation and decoy technologies further shield protected networks from malicious probes.

IDP (Intrusion Detection and Prevention)

Separate your friends from your enemies.

Integrated with the firewall, the Network Box IDP (Intrusion Detection and Prevention) module scans network traffic at the application level, and seamlessly blocks malicious behaviour with zero latency. A comprehensive database of IDP signatures precisely matches and actively blocks known exploits. Protection against newly emerging threats is provided by a database of vulnerability class based signatures and heuristic (expert system) anomaly-based behavioural analysis. The Network Box IDP system is updated in real time, using high speed PUSH technology, from the global system of Network Box Security Operation Centres.

VPN (Virtual Private Networking)

Sending an e-mail is like mailing a postcard.

The Network Box VPN supports PPTP, L2TP, GRE and IPSEC protocols; in client, server and "road warrior" configurations. Modular configuration permits multiple encapsulation layers, such as L2TP within IPSEC. PSK, RSA PKI and X.509 certificates are available for IPSEC authentication, with all secure encryption standards (including 3DES, AES, Blowfish and CAST) fully supported. 128/256 bit encryption keys are available, and 4,096 bit certificates and keys are supported for authentication. Most major VPN servers (such as Microsoft, Cisco, Checkpoint and Symantec) can be connected to the Network Box. Full SSL VPN functionality is also included, allowing convenient secure access for users on the move.

Anti-Virus Gateway

You have (virus) mail.

The Network Box anti-virus gateway, in partnership with Kaspersky Labs, provides a multi-layered, multi-engine approach to block both known and unknown viruses effectively. A signature database, updated in real time using high speed PUSH technology, provides comprehensive recognition of more than 275,000 known viruses, worms, spyware, Trojans and general malware threats. More than 900 different compression and encoding formats are supported. For new and emerging threats, the state-of-the-art heuristic analyser uses both cryptanalysis and statistical analysis techniques to block even previously unknown viruses and worms.

Anti-SPAM E-mail Gateway

Up to 90% of your e-mail is junk.

The Network Box anti-SPAM e-mail gateway achieves an industry record 95% average detection rate, with almost zero false-positives. Combining comprehensive header analysis, with full textual analysis of the message body, as well as all attachments, the system constantly tunes itself to improve the SPAM "hit rate." Multiple techniques are simultaneously utilised, including distributed mail signature databases, DNS look-ups, real time black lists and URL categorisation against the SurfControl database of more than 17 million URLs. Bayesian filtering and heuristic tests are also supported, and used alongside auto-white listing to increase accuracy further. State-of-the-art image SPAM handling, including Optical Character Recognition technology, is included as standard.

Content Filtering

Keep their minds on the job.

The SurfControl content filtering engine, from the world's #1 web and e-mail filtering company, is based on a categorisation database covering 3 billion web pages, in 70 languages spread across 192 countries and is included with every Network Box. The system is fully customisable by the administrator through a web browser interface. Policies can be set per authenticated user or IP address, and can also be restricted by time, date, protocol, method or URL category. Authentication options include Windows domain controllers, LDAP directory servers and locally defined users. Powerful and flexible reporting is available.

KASPERSKY lab | NETWORK BOX | SurfControl®

	TECHNICAL SPECIFICATIONS	S-50 / S-80	M-250	M-380	E-1000/ E-2000	
						
NETWORK BOX	Processor	VIA C3	Intel Celeron M	Intel Pentium 4	AMD Opteron 250	2 x AMD Opteron 250
	System Architecture	32bit	32bit	32bit	64bit	64bit
	Independent network connections	4 x 10/100 baseT	4 x 10/100/1000 baseT	4 X 10/100/ 1000 baseT Upgradeable: 8 ports	1 X 10/100 baseT / 2 x 10/100/1000 baseT Upgradeable: Fibre LX / Fibre SX / Additional TX ports	
	Solid State Storage	1GB (ICF)	1GB (ICF)	1GB (ICF)	1GB (SS HDD)	1GB (SS HDD)
	System RAM	1GB	1GB	1GB	2GB ECC	2GB ECC
	Hard Disk Drive(s)	None / 80GB PATA	80 GB PATA	80GB SATA	RAID-1 72GB SCSI	RAID-1 72GB SCSI
	Threat types protected against	Viruses, e-mail, hacking, Denial of Service, software vulnerabilities, SPAM, company policy violations				
	IP address requirements	Requires 1 public IP address (static or dynamic IPv4) for upstream connection, additional required for high availability				
	Front panel display	None	LCD (Liquid Crystal Display) with built-in 4-key keypad for easy operator control		VFD (Vacuum Fluorescent Display) with built-in 7-key keypad for easy operator control	
	Licensing	5 User / 10 User / Per-Box	Per Box		Per Box	
	Power supply	110volt-60Hz / 240volt-50Hz [Single Power Supply]			110volt-60Hz / 240volt-50Hz [Dual Redundant Power Supplies	
	Weight	3.5 kg	8 kg	14 kg	24 kg	
	Dimensions (H x D x W)	5cm x 17cm x 34cm	1U (4.5cm x 27.5cm x 43cm)	1U (4.5cm x 50cm x 43cm)	2U (9cm x 66cm x 43cm)	
FIREWALL	Packet filtering firewall	Yes - filtering by protocol, source, destination (address and/or port) and interface				
	Stateful packet inspection	Yes - connection tracking and filtering by invalid, established, new, and related states				
	Application proxies	Yes - security-hardened ARP, DHCP, NTP, HTTP, HTTPS, FTP, GOPHER, SMTP, POP3 and IMAP4				
	Application level filtering	Yes - filters configurable on data stream				
	Network Address Translation (NAT)	Yes - both source (connection sharing) and destination (call/port forwarding)				
	Load balancing/multiple gateway support	Yes - both incoming (via call forwarding/routing) and outgoing (multiple gateways)				
	Available routing protocols	Static (recommended), RIP, HELLO, OSPF, IS-IS, EGP, BGP				
	Unauthorised action response	Blackhole (silently drop), reject (with correct protocol response), or blacklist (drop further traffic)				
	Address spoofing protection	Both inbound and outbound protection against network address spoofing				
	Basic Routed Protocols support	ARP, ICMP, IPv4, IPv6				
	Maximum network nodes	Unlimited				
	Suggested maximum network connections	65,536	131,072	262,144	524,288	524,288
	Absolute maximum network connections	262,144	524,288	1,048,576	1,048,576	1,572,864
	Maximum throughput	387 Mbps	820 Mbps	2,100 Mbps	2,800 Mbps	2,800 Mbps
IDS/IDP	Intrusion detection engine	Zero latency, hybrid, multi-level, tightly integrated with firewall				
	Action	Active (blocks network traffic) and/or passive (logs intrusion attempts)				
	Reporting	Real time (on demand), and periodic (summary) by SMTP e-mail				
	Types of intrusion detected	ICMP/IP, Denial of Service (DoS), portscans, protocol level, application level				
	Signatures	Depends on configuration, but normally in excess of 2,500 (IDS) / 350 (IDP)				
VPN	VPN types	IPSEC, L2TP, PPTP, GRE, SSL				
	IPSEC encryption algorithms	DES, 3DES, AES, CAST, Blowfish, Serpent, Twofish				
	IPSEC digest algorithms	MD5, SHA1, SHA2				
	IPSEC key sizes supported	168 / 192bit DES, 128 / 256bit AES, 256 / 512bit SHA2, 2048+bit RSA				
	IPSEC VPN	92 Mbps (AES 256bit)	75 Mbps (AES 256bit)	200 Mbps (AES 256bit)	394 Mbps (AES 256bit)	394 Mbps (AES 256bit)
	SSL VPN	74 Mbps (AES 256bit)	72 Mbps (AES 256bit)	110 Mbps (AES 256bit)	222 Mbps (AES 256bit)	308 Mbps (AES 256bit)
	Simultaneous VPNs tested	200 tested	1,000 tested	10,000 tested	10,000 tested	10,000 tested
	Configuration options	Site-to-Site, Site-to-Remote, Site-to-Roadwarrior				
	Hardware Acceleration	VIA Padlock (AES for SSL & IPSEC VPN)	Not Required			
ANTI-VIRUS/ ANTI-SPYWARE	Protocols for scanning/detection	SMTP, POP3, IMAP4, FTP, HTTP				
	Anti-relay protection	Protects LAN segment(s) and DMZ segment(s)				
	Basic encoding methods supported	MIME, uuencode, Base64, text				
	Anti-virus engines	Heuristic and signature-based engines, including Kaspersky Laboratories and optionally CLAM (Over 275,000 signatures)				
	E-mail anti-virus scanning throughput	16,600 – 32,000 messages per hour (AV+)	26,000 – 51,000 messages per hour (AV+)	66,500 – 130,500 messages per hour (AV+)	73,000 – 129,500 messages per hour (AV+)	74,700 – 219,400 messages per hour (AV+)
ANTI-SPAM / ANTI-PHISHING	Protocols for scanning/detection	SMTP, POP3, IMAP4				
	Maximum message size	Configurable, but at least 100Mbytes				
	Basic encoding methods supported	MIME, uuencode, Base64, text				
	Actions on SPAM detection	Scoring, Header-Insertion, Subject-Marking, Forwarding, Drop[1], Redirect[1] and Quarantine[1]				
	Anti-SPAM engines	Heuristic, signature, RBL and Bayesian state-of-the-art SPAM engines (Over 750,000 signatures)				
	E-mail anti-SPAM scanning throughput	6,300 – 17,200 messages per hour (AV+)	8,100 – 26,000 messages per hour (AV+)	22,000 - 70,000 messages per hour (AV+)	27,500 – 73,500 messages per hour (AV+)	27,500 – 125,000 messages per hour (AV+)
	Optical Character Recognition Technology	Yes	Yes	Yes	Yes	Yes
CONTENT FILTERING	Protocols supported	HTTP, HTTPS, FTP, GOPHER, WAIS				
	Source user filtering	Authenticated user/source IP address				
	Filtering rules	Source user, Method, Category, Schedule				
	Scheduling flexibility	Multiple schedules by time of day/day of week across different users/groups of users				
	Categorisation database	Over 17 million sites, covering 3 billion web pages, categorised into 54 categories, collected from 192 countries, in 70 different languages				
	Black lists/White lists	Both, selectable for individual users/groups				
	Web Proxy scanning throughput (UTM+)	41 - 49 requests per second	64 - 77 requests per second	78 - 79 requests per second	169 - 172 requests per second	169 - 172 requests per second
	Reporting	Flexible, drill-down, "slice and dice" by IP, user, site, category, date, time, cache status				
SERVICE	Installation/configuration	Network Box is fully and individually configured according to the customer's requirements				
	Configuration verification	Periodic verification of system integrity and configuration				
	24 x 7 monitoring	Active and passive monitoring of environment, hardware, O/S, key subsystems, configuration and performance				
	24 x 7 updates	Delivered on an as-available basis, pushed to Network Box systems from a worldwide network of NOCs				
	Just-in-time updates	Just-in-time release of latest threat signatures for protection from blended threats				
	Help desk	8x5 or 24x7 access to help desk as per Service Level Agreement (SLA)				
	Reporting	Real time (on demand), and periodic PDF (summary) via SMTP e-mail				
	Hardware maintenance	Included with managed service				
	Configuration back-up	Full configuration back-up maintained at managing Network Box NOC(s)				
	Live Watch Monitoring System	Built into Network Box Graphical User Interface Version 3, using AJAX technology				

[1] Anti-Spam actions Drop, Redirect and Quarantine are not supported for POP3 and IMAP4 protocols.


6th IT Exellence Awards
Product Gold Award


Network Box "SME-250"
Overall Rating: ★★★★★
Security Appliance Review:
6th April 2006


Finalist in US and European
Secure Computing Magazine
Awards 2006


PC3 Magazine Awards
Editors' Choice


Technology & Business
2004 Editors' Choice


Linuxpilot Editors'
Choice 2006
Winner of UTM Solution


APICTA 2004 Hong Kong
Winner of Security


Innovationspreis
2005 Award


Technology Committee Expo
Technology Innovations of
the Year Award 2005


2005
C3 Expo
Best of Show in
Enterprise Services 2005


Silicon Valley Communications
Info Security
"Hot Company" 2006


Network Box SME-250, 13th February 2006

Network Box Corporation Limited
E-mail: info@network-box.com Website: http://www.network-box.com