Entry-Level Enterprise Firewall Test

A Broadband-Testing Report
By Steve Broadhead, Founder & Director, BB-T
TABLE OF CONTENTS

TABLE OF CONTENTS ........................................................................................................ 1
BROADBAND-TESTING .................................................................................................. 3
EXECUTIVE SUMMARY ............................................................................................... 4
INTRODUCTION: DEFINING A CURRENT DAY ENTRY-LEVEL ENTERPRISE FIREWALL/UTM ............................................................................................................................. 5
PRODUCT OVERVIEW .................................................................................................. 6
  Cisco ASA 5510 ........................................................................................................ 6
  NetPilot Globemaster 2500B ................................................................................... 7
  SonicWALL TZ 210 .................................................................................................. 8
  WatchGuard XTM 505 .......................................................................................... 9
TEST SECTION .............................................................................................................. 11
  The Test Bed .......................................................................................................... 11
  Performance Testing ............................................................................................ 15
    Basic Firewall Throughput ............................................................................. 15
    IPS Enabled Throughput ............................................................................... 16
    UTM Enabled Throughput .............................................................................. 17
  Threat Blocking - No Background Traffic ...................................................... 18
  Threat Blocking - Maximum Background Traffic ......................................... 19
SUMMARY & CONCLUSIONS .................................................................................... 22

Figure 1 – Cisco ASA 5510 .......................................................................................... 6
Figure 2 – Cisco ASA 5510 ASDM Interface ............................................................. 7
Figure 3 – NetPilot Globemaster R2500 ..................................................................... 8
Figure 4 – SonicWALL TZ 210 .................................................................................. 8
Figure 5 – SonicWALL TZ 210 GUI: IPS Activated ................................................. 9
Figure 6 – WatchGuard XTM 505 .............................................................................. 10
Figure 7 – WatchGuard XTM 505 GUI ..................................................................... 10
Figure 8 – The Test Bed ........................................................................................... 11
Figure 9 – Spirent Studio .......................................................................................... 12
Figure 10 – Basic Firewall Throughput Test ......................................................... 15
Figure 11 – SonicWALL Firewall CPU Pegged ....................................................... 16
Figure 12 – IPS Enabled Throughput Test ............................................................. 16
Figure 13 – WatchGuard Is CPU Pegged During IPS Enabled Throughput Test ... 17
Figure 14 – UTM Enabled Throughput Test.......................................................................................................................... 18

Figure 15 – Threat Blocking Test: No Background Traffic........................................................................................................ 18

Figure 16 – Threat Blocking Test: Published Vulnerabilities........................................................................................................ 19

Figure 17 – Threat Blocking Test: Max Background Traffic........................................................................................................ 19

Figure 18 – Threat Blocking Test: Max Background Traffic - WatchGuard CPU At 100%............................................................... 20

Figure 19 – Threat Blocking Test: Max Background Traffic - SonicWALL System At 100%............................................................... 20

Figure 20 – WatchGuard Performance: Marketing vs Real........................................................................................................... 21

Figure 21 – SonicWALL Performance: Marketing vs Real............................................................................................................ 21
BROADBAND-TESTING

Broadband-Testing is Europe’s foremost independent network testing facility and consultancy organisation for broadband and network infrastructure products.

Based in Andorra, Broadband-Testing provides extensive test demo facilities. From this base, Broadband-Testing provides a range of specialist IT, networking and development services to vendors and end-user organisations throughout Europe, SEAP and the United States.

Broadband-Testing is an associate of the following:

Limbo Creatives (bespoke software development)

Broadband-Testing Laboratories are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

Broadband-Testing Laboratories operates an Approval scheme which enables products to be short-listed for purchase by end-users, based on their successful approval.

Output from the labs, including detailed research reports, articles and white papers on the latest network-related technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

Broadband-Testing Consultancy Services offers a range of network consultancy services including network design, strategy planning, Internet connectivity and product development assistance.

© Broadband-Testing 1995-2012
EXECUTIVE SUMMARY

Using the Spirent Studio product, we put four entry-level Enterprise class security appliances to the test.

The aim here was not to do a straight head-to-head comparison, but rather to look at different solutions at different price-points for the entry-level Enterprise feature set sector and look at relative performance and performance:price ratio.

We first looked at performance (throughput) levels (using Spirent Avalanche as our traffic generator) and what can be sustained, or otherwise, as more and more firewall features are enabled.

We found that, in basic firewall mode, vendors in general were able to get close to their claimed performance figures and that these were perfectly reasonable for the target market.

However, with IDS/IPS functionality enabled, performance fell away markedly in all cases - sometimes to a fraction of what it was in basic firewall mode. While this may not be as significant a problem for a product aimed at supporting say 50-250 people as it is for a larger Enterprise product, it is still of some concern, especially when combined with threat attacks, our second lot of tests in this report.

Using Spirent Studio we used a preset mix of published vulnerability attacks, and tested the security appliances in both low and high traffic conditions to see how well they were able to defend against these attacks both in unstressed and stressed modes.

Again we found differences in the product’s capabilities to prevent threats depending on traffic conditions, though this was not totally consistent, as is often the case when a device is fully utilised (CPU, memory, etc).

All the products tested let significant numbers of attacks through, despite being completely up to date in terms of signature databases, firmware and all aspects of configuration.

The reality is that the devices under test are designed for relatively low levels of use, with according price tags, so there is a level of compromise involved in terms of overall performance, especially when you consider the depth of features now expected to be part of an "entry-level Enterprise-class" firewall (see introduction).
INTRODUCTION: DEFINING A CURRENT DAY ENTRY-LEVEL ENTERPRISE FIREWALL/UTM

Is it really possible to have an entry-level Enterprise firewall - sounds like a contradiction in terms?

Not these days. It is generally recognised in the industry that branch offices of major Enterprises have somewhat different network security requirements from high-end devices, notably the concept of an all-in-one appliance (such as UTM or Unified Threat Management appliance) versus individual, best-of-breed products. At the same time, this size of product is increasingly being loaded with what the vendors describe as "high-end, Enterprise-level functionality".

Gartner describes the multifunction firewall market as being large, fragmented, and highly dynamic, with vendors providing a common set of core security features, differentiating with new added safeguards, ease of installation, and use, and addressing the realities of this level of IT environment.

In this report we look at four vendors approach to providing what they describe as an "entry level Enterprise product" solution to see how this differentiation works out in practise. Differentiation often comes in the form of a variation on a similar theme of multiple security features, flexible licensing options - the products come fully-loaded but not feature-enabled - unique management GUIs and, in some cases, ultra-competitive pricing.

So what can you expect to find in a contemporary firewall/UTM aimed at this market?

In addition to basic firewall functionality, typically you will find some or all of the following features:

- Anti-Virus (AV) engine
- IDS/IPS (Intrusion Detection/Prevention System)
- URL/Website filtering
- Caching engine
- Email security, anti-spam etc
- VoIP/IP telephony
- VPN/SSL VPN
- WLAN

One real commonality is the number of license options - for example, the basic firewall technology comes as part of the base price, but most other features - some of which are
services via a gateway (such as AV) - are based on annual subscriptions. The good news here is that you effectively pay for what you need. The bad news is that the basic acquisition price is often increased significantly (and annually) once you start enabling features and services.

PRODUCT OVERVIEW

For this test we got together four firewall/UTM appliances from vendors that historically play in different market segments, or have a different market focus, but who ultimately overlap in the sense that they are all loaded with what their vendors describe as Enterprise-class features. The four products were:

- Cisco ASA 5505
- NetPilot Globemaster R2500
- Dell SonicWALL TZ 210
- WatchGuard XTM 505

We will now describe each one briefly in turn:

**Cisco ASA 5510**

The ASA 5510 Adaptive Security Appliance is described by Cisco a next-generation, full-featured security appliance for branch office, and Enterprise teleworker environments.

![Figure 1 – Cisco ASA 5510](image)

It features five 10/100 Fast Ethernet ports, and includes VPN services, and optional IPS services through the AIP SSM option pack. Customers can also install a Security Plus license, upgrading two of the Cisco ASA 5510 Adaptive Security Appliance interfaces to Gigabit Ethernet and enabling integration into switched network environments through VLAN support. This upgrade license maximises business continuity by enabling Active/Active and Active/Standby high-availability services.

Using the optional security context capabilities of the Cisco ASA 5510 Adaptive Security Appliance, businesses can deploy up to five virtual firewalls within an appliance to enable compartmentalized control of security policies on a departmental level. Customers can also extend their SSL and IPSec VPN capacity to support a larger number of mobile workers,
remote sites, and business partners. Up to 250 AnyConnect and/or clientless VPN peers can be supported on each Cisco ASA 5510 by installing an Essential or a Premium AnyConnect VPN license; up to 250 IPSec VPN peers are supported on the base platform.

VPN capacity and resiliency can also be increased by taking advantage of the Cisco ASA 5510’s integrated VPN clustering and load-balancing capabilities (available with a Security Plus license). The Cisco ASA 5510 supports up to 10 appliances in a cluster, offering a maximum of 2500 AnyConnect and/or clientless VPN peers or 2500 IPSec VPN peers per cluster.

Performance wise, basic firewall throughput is claimed to be 300Mbps maximum, falling to 150Mbps with firewall + IPS using the basic SSM-10 upgrade, while concurrent sessions using the basic supplied license is 50,000. Management is via CLI/Telnet or using the integrated Cisco ASDM management interface.

NetPilot Globemaster 2500B

The Globemaster R2500 is what NetPilot describes as providing “UTM Premium” security for up to a recommended limit of 500 users.

Physically, it comes in a 1U rack mount enclosure, with three Gigabit Ethernet ports and storage in the form of an 80GB solid state drive (SSD) and is based around a quad-core processor platform. NetPilot makes the point that SSDs are around 10 times more reliable.
than hard disks and consume considerably less power. At the same time SSDs read and write data at up to three times the speed of hard disks, so there is a performance benefit too.

By “Premium”, what NetPilot is defining is a UTM device designed for companies needing the highest levels of security available, regardless of size. NetPilot claims that its Premium pack has the most Checkmark accreditations of any UTM product currently available. Multiple configurable Ethernet ports for LAN, WAN or DMZ are provided - the number depending on the chassis configuration chosen.

It includes AV for email and browsing from Sophos, anti-spam, email policy control, URL filtering, anti-spyware, advanced firewall, IDS/IPS, and access to the software upgrade service. Upgrade options include the VPN Plus SSL technology (see box-out). The device is shipped with a 12 month subscription to all 3rd party services used with the Globemaster.

UTM features include firewall (stateful packet inspection based), anti-virus for email and browsing powered by Sophos, anti-spam, anti-spyware (including proxy malware scanning), email policy controls, Intrusion detection and prevention (IDS/IPS) and URL filtering. Various services can also be software-upgraded, in line with the other products on test here.

Management is GUI-based. VPN functionality is provided (site-to-Site, unit to unit - unlimited VPN clients, up to 200 tunnels) with IPSec as standard, upgradeable to the latest SSL VPN Plus. Other key features include web page caching (http and ftp caching), user and group access controls, time-based connectivity controls and web access controls and filters.

**SonicWALL TZ 210**

The Dell™ SonicWALL TZ 210, integrates Unified Threat Management, Application Intelligence and Control, SSL VPN remote access capabilities with optional 802.11n wireless.

It enables branch offices to use USB ports supporting 3G and analogue failover along with multiple Ethernet WAN failover for greater redundancy and reliability. The TZ 210 Series sums up the current approach by the established entry-level Enterprise firewall players - that
is to claim business-class performance, advanced networking features and configuration flexibility in an affordable desktop appliance that’s easy to set up, operate and manage. Other features include application control, gateway anti-malware, anti-spamware/phishing, intrusion prevention and content filtering.

![Figure 5 – SonicWALL TZ 210 GUI: IPS Activated](image)

The WAN Acceleration Appliance (WXA) Series provides WAN Acceleration to reduce application latency, conserve bandwidth and optimise WAN performance. Management wise, the GUI provides views and control of network traffic broken down by applications, users and content. There is also the ability to prioritise important applications, throttle down unproductive applications and block unwanted application components.

Another feature, SonicWALL Mobile Connect, provides a single unified client app for Apple iOS and Android devices over encrypted SSL VPN connections. Optional is an integrated 802.11n WLAN capability, with support for multiple virtual SSIDs (Virtual Access Points) for secure segmented wireless access. Additionally, the TZ 210 Wireless-N applies all Deep Packet Inspection security services to wireless traffic for extra WLAN protection.

Interface wise, the TZ 210 is supplied with two Gigabit and five 10/100 Ethernet ports, a console interface and two USB ports. Performance is claimed to be 200Mbps of stateful firewall throughput, 110Mbps of IPS throughput, 70Mbps of gateway AV throughput and 50Mbps of UTM throughput, with 30,000 maximum firewall connections and 20,000 maximum UTM connections.

**WatchGuard XTM 505**

The XTM 505 is part of a series of appliances that combine firewall/VPN with powerful security services and a suite of flexible management tools.
It includes - depending on licensing - application control, compliance reporting, VoIP support, IPSec, SSL and PPTP VPN options (with failover and single sign-on) and QoS (eight priority queues, diffserv, modified strict queuing). High availability options include active/passive, active/active with load balancing, port independence, multi-WAN failover, multi-WAN load balancing and transparent/drop-in mode.

The 5 Series appliances feature six Gigabit and one 10/100 Ethernet, plus USB interfaces. Management options are from a centralised console, scriptable CLI, and web UI. Real-time monitoring and reporting are included at no extra cost, as is remote logging capability.

All aspects of the firewall are upgradeable - performance, capacity, and security capabilities. Subscription-based options include application control, reputation enabled defence, WebBlocker, spamBlocker, Gateway AV and IPS (available in the Security Bundle).

Figure 6 – WatchGuard XTM 505

Figure 7 – WatchGuard XTM 505 GUI
In terms of performance, claimed firewall throughput is 1.5Gbps, AV throughput of 520Mbps, IPS throughput of 500Mbps, UTM throughput of 275Mbps and VPN throughput of 320Mbps.

**TEST SECTION**

**The Test Bed**

For our test bed we wanted to combine two elements of Spirent's test solutions - the recently acquired Spirent Studio for our attack traffic, combined with Spirent Avalanche traffic generator, in order to provide continuity with past testing.

![Figure 8 – The Test Bed](image)

Using an HP 6600 Ethernet switch, we combined Gigabit ports (2 + 2) from Spirent Avalanche with Gigabit ports (1 +1 from Spirent Studio) with an "inside-out" type configuration, simulating office-based clients internally and the Internet/cloud externally, from where we delivered both HTTP traffic for throughput testing and attack injections to test blocking capabilities of each security device.

In each case, we set up initially a basic "allow-allow" rule on each firewall, in order to guarantee that a) traffic was passing through the device as planned with no unintended blocking and b) to ensure the highest level of initial performance.

This was our first experience in using Spirent Studio, so we will give an overview of its features. Our focus was on the Security module of the product, rather than the performance module.
Spirent Studio enables you to put security devices to the test by:

- Measuring their ability to detect and prevent thousands of known attacks.
- Testing their resiliency by sending unexpected or malicious traffic.
- Measuring their ability to withstand targeted DDOS attacks.
- Testing their capabilities to inspect traffic for malware, unwanted URLs and spam and take appropriate action.

It provides support for DDOS, known attacks, fuzz testing, malware and spam prevention, and application white or black listing. The software is designed to let you run huge numbers of tests in order to guarantee consistency and repeatability. In addition to pre-set tests, you can also create custom tests for your unique protocols and applications without scripting.

Below is an overview of each key feature:

**Fuzz Testing**

Fuzz testing is the most effective way to run negative tests on your target for unexpected inputs and events. This method efficiently covers the unexpected, negative test cases that often cause catastrophic and costly crashes or failures on the live network.

**DDoS Replication**

Quickly replicate a large variety of actual and potential DDoS attacks to test the resiliency of their applications and services.
Spirent Studio also presents actionable data for DDoS detection, prevention and capacity planning to ensure the organisation can make the changes they need to better prepare their infrastructure to protect against a successful DDoS attack for detection, prevention and capacity planning.

**Known Vulnerabilities**

The Published Vulnerabilities (PV) Module offers a continuously growing list of software vulnerability triggers, which mirrors the latest real-world attacks found in the wild on the Internet. The Published Vulnerabilities module validates any inline signature-based product’s ability to detect and block root causes instead of symptoms.

**Security Capability Verification**

Security features such as malware detection and prevention, URL filtering, white-listing and black-listing of applications can be easily done with Spirent Studio.

**Monitors**

These hook into the target and help isolate and reproduce faults. Monitors include protocol health checks, SNMP monitors, SSH and Telnet based command monitors, remote log monitors and console monitors.

**Remediation Tools**

In addition to finding issues, Spirent Studio helps fix the issues found by providing resilience testers with remediation assets that can be used by engineers. These assets are sent to developers so that issues are replicated and fixed rapidly.

**Automation**

Spirent Studio is designed for automation with a broad set of API interfaces that can be accessed from a TCL, Python, Perl or other similar automation frameworks. The solution can also be set into a mode that enables lights-out testing, automatically restarting targets if they crash during a test run.
SPIRENT STUDIO

Spirent Studio is a purpose-built testing solution designed to ensure that applications and the network infrastructure will perform and scale under real-world conditions and loads.

For example, you can measure the accuracy of DPI-based detection and classification by recreating thousands of the latest applications, validate the effectiveness of policies related to billing and charging, traffic management and quality of experience (QoE) using real application traffic and test the impact of mixed security attacks and real application traffic at scale on the network.

Spirent Studio has a TestCloud feature that provides immediate access to thousands of application test cases from a single unified UI and these are regularly updated. A multi-track feature lets you select multiple classes of applications and run them on separate tracks, measure policies on a per IP or per interface or per application basis using separate tracks, and allows you to mix in security attacks as a separate track along with valid application traffic on other tracks.

Multiple testers can be accessing the solution at the same time and run tests simultaneously. The UI allows for large teams of testers to use the solution at the same time. You can also increase the load of application traffic by increasing the number of scale appliances based on the need. The same UI can control multiple scale appliances enabling a linear increase in performance.
Performance Testing

Basic Firewall Throughput

For our basic firewall throughput test we created a series of HTTP traffic based tests using the Spirent Avalanche to deliver different transaction file sizes ranging from 10KB to 100KB through the firewall. Due to the different port types, allocations and widely varying claimed maximum throughputs of each vendor/firewall combination, we created multiple test runs in order to find the "sweet spot" for each firewall, performance wise, before they started to fail significant numbers of transactions.

Starting with vendor’s claims, WatchGuard claims firewall throughput of 1.5Gbps, Cisco 300Mbps and SonicWALL 200Mbps. NetPilot, in previous testing peaked at 973Mbps through a Gigabit port connection - essentially line rate.

What we found this time around was that the NetPilot fell short of its previous height - it was based on a different Intel motherboard than supplied previously, and here obviously was the bottleneck. Cisco fell just short of NetPilot's 693Mbps with 667Mbps, but this is still over twice the claimed performance (though Cisco is traditionally conservative with its marketing figures). SonicWALL's performance fell short of its 200Mbps claims (delivered via multiple 10/100 ports) by peaking at 130Mbps. WatchGuard, in contrast, came very close to matching its vendor performance claims, reaching 1.43Gbps, just shy of the 1.5Gbps claims.

In terms of system utilisation, WatchGuard was using only 16% CPU and 40% memory. Cisco system utilisation was also relatively modest, as was that of the NetPilot - hence the obvious bottleneck elsewhere - whereas the lower spec'd SonicWALL device was immediately running at 100% CPU capacity.
IPS Enabled Throughput

We then repeated the HTTP testing with IPS enabled. Unfortunately, due to a licensing issue with the Cisco firewall, IPS was not enabled in time for us to test it beyond basic firewall capability before the report deadline, but this will be included in the report update.

With IPS enabled, relative performance between the firewalls changed significantly. The SonicWALL TZ 210, being already CPU pegged in basic firewall mode, did not fall significantly
in performance terms, from 130Mbps to 121Mbps, better than its 110Mbps claims. In contrast despite numerous attempts to achieve WatchGuard’s 500 Mbps claims, with several configuration tweaks, we were not able to replicate this value and observed only 39Mbps throughput.

Figure 13 – WatchGuard Is CPU Pegged During IPS Enabled Throughput Test

CPU utilisation went to 90-100% immediately with IPS enabled and significant traffic levels, suggesting a bottleneck issue relating to the connections per second limits. For this reason, we reran tests with as many different TCP timeout/keep-alive and relative configuration changes as we were able to make, but with no change in results. The NetPilot also took a performance hit with IDS enabled (it has IDS rather than IPS) but still maintained a healthy 267Mbps throughput - far and away the best in this particular test.

**UTM Enabled Throughput**

As a final test we went for an “everything on” mode test - essentially full UTM-enabled configurations for each firewall, but notably with AV Gateways/engines enabled as this can often take the biggest hit on system utilisation.

We then reran the HTTP traffic tests and compared relative performance once again. In this instance we saw all three firewalls again take a performance hit and saw the NetPilot appliance take its first significant utilisation hit. The result was that the NetPilot fell to 77.84Mbps, while the SonicWALL maintained relative performance levels, dropping only to 115.74Mbps. The WatchGuard, meantime, fell again to 33.34Mbps, well short of anticipated performance - based on vendor claims - while the SonicWALL device again exceeded its vendor claims.
We now turned to Spirent Studio to inject threats into each firewall and see what percentage was blocked. We chose to use the Studio’s known vulnerabilities set, which comprises well-documented vulnerabilities from globally used applications. The list is accurately compiled and updated with vendor-specific feeds from Oracle, Microsoft, Novell, IBM, Red Hat and many others.
Figure 16 – Threat Blocking Test: Published Vulnerabilities

Here the WatchGuard was a clear winner, blocking 307 of out 476 threat attack injections, while the SonicWALL and NetPilot devices lagged behind with 90 and 78 blocks respectively, bearing in mind that the latter has only an IDS engine, not IPS.

Threat Blocking - Maximum Background Traffic

Figure 17 – Threat Blocking Test: Max Background Traffic

Under heavy traffic, the WatchGuard took a significant hit in the percentage of threats it was able to block, but still came out easily the best in this test with 251 threats blocked (down from 307) out of 476 - just over 50%. CPU utilisation was at 100% throughout this test.
The NetPilot only blocked 32 threats, while the SonicWALL was unaffected again by the heavy traffic load, blocking 98 threats - actually a marginally better result than the best recorded with no background traffic, despite system utilisation being totally pegged.

So what does it mean if attacks are getting through? Well, it could simply be that there is no corresponding signature in the database of the device under test and this might simply be a timing update issue - though all products tested had up to date signature databases downloaded pre-testing. However, in relation to the "skipped" tests and failed blocks that occurred during our threats with background traffic tests, it can simply be a case of the device being overwhelmed - CPU and memory - by the traffic levels, so that the scanning engine simply fails to operate quickly enough.
In terms of actual versus "marketing" performance, of the three firewalls we were able to fully test, only SonicWALL and WatchGuard publish performance figures. Looking at these two then, we can see that, while the WatchGuard device has all but matched its marketing figures when performing as a simple firewall, once IPS and other features were enabled, we encountered significant problems in achieving even a fraction of those claims.

![WatchGuard Performance: Marketing vs Real (Gbps)](image)

Figure 20 – WatchGuard Performance: Marketing vs Real

In direct contrast, the cheaper, lower-spec'd SonicWALL device failed to meet its published marketing figures for basic firewall throughput, but exceeded the claims when IPS and UTM enabled, significantly in the case of UTM throughput.

![SonicWall Performance: Marketing vs Real (Mbps)](image)

Figure 21 – SonicWALL Performance: Marketing vs Real
SUMMARY & CONCLUSIONS

Here we have a case of four products all designed to provide entry level Enterprise security, but at different price and performance levels, but with a few twists when it comes to actual performance in a real-world scenario.

We found that, in basic firewall mode, vendors in general were able to get close to their claimed performance figures and that these were perfectly reasonable for the target market. However, with IDS/IPS functionality enabled, performance fell away markedly in all cases. Interestingly though, the least expensive and least powerful product in the test, the SonicWALL TZ 210, suffered less of a hit than the more expensive alternatives on test. That product, however, is limited in terms of its ultimate performance capabilities as a basic firewall, and was truly outpointed by the WatchGuard XTM 505 when it came to threat detection.

Using Spirent Studio we used a preset mix of published vulnerability attacks, and found that all devices under test failed to block significant numbers of attacks. Again we found differences in the product’s capabilities to prevent threats depending on traffic conditions, though this was not totally consistent, as is often the case when a device is fully utilised (CPU, memory, etc).

The reality is that the devices under test here are designed for relatively low levels of use, with according price tags, so there is a level of compromise involved in terms of overall performance, especially when you consider the depth of features now expected to be part of this level of firewall. In other words, there is no such thing as a perfect, one-box solution but, realistically, for the target market all the firewalls tested here have some merits, but fall well short of perfection. It’s all about expectation levels...