

gateProtect GPA 400

The alarming number of network security breaches occurring isn't just down to increasingly devious hackers, as all too often they're simply exploiting a gaping hole left by a misconfigured device. This is not surprising as some products have management interfaces that are so badly designed they make a slip up during configuration almost inevitable.

German company GateProtect aims to change all that, as its GPA UTM appliances introduce the concept of ergonomic operability - its words, not ours. It grandly claims to be the only company in the world whose software fully complies with Part 110 of the ISO 9241 standard.

This defines the ergonomics of human system interaction with computers and describes seven dialogue principles such as clarity of descriptiveness and tolerance of user errors.

The GPA 400 on review is designed to handle up to 250 users, although there's no actual user limit. It's endowed with a 2GHz dual-core Pentium E2180 teamed up with 1GB of RAM while storage is handled by a 160GB SATA hard disk. The motherboard's five expansion slots are put to good use, as all are occupied by Gigabit network cards and, along with the embedded port, can all provide either LAN, WAN or DMZ duties. Use two for WAN links and failover is a possibility as well.

The 400 is certainly not short on features as its SPI firewall is partnered by an SSO solution, IPsec and SSL VPNs, IDS and traffic shaping. To these you can add the optional Commtouch anti-spam, Kaspersky anti-virus and Cobion web content filtering. A one-year subscription to all three services costs £1,048.

All management is via the eGUI management console, which kicks off by automatically discovering the GPA appliance and providing a quick-start wizard where you pick your initial LAN and WAN ports, set up basic internet access and lock down administrative access. It then switches to its main interface, which opens with a smart desktop graphic that is quite unique.

The desktop view shows each network port accompanied by link lines and connection points that show clearly how they are connected. At the top, you have the port designated for internet access, with all others below this. To set up a policy between two ports just requires the relevant connection point to be selected.

This pops up a dialogue box, which opens with a range of services in the left pane and a graphic alongside that shows the current rule in force, the action and whether it's active. Arrows are used to show which traffic direction the rule applies to and simply clicking on it changes the direction.

If you want to block all traffic, just keep clicking until a red no-entry icon appears - it's as simple as that. A dialogue box below also provides an explanation for each rule that describes clearly what it's doing. The left pane next to the desktop shows all available services and selecting one changes the link lines in the graphic to show which connections it applies to.

The appliance uses the Squid HTTP proxy, which can run in transparent or intransparent modes. The former requires no client configuration, while the latter allows you to apply proxy authentication to users and you can employ the appliance's internal database, LDAP, AD or an external Radius server. The https proxy operates as a 'man in the middle', allowing it to scan encrypted content before passing it on.

Anti-spam policies are applied to all traffic and are a cinch to set up: you select this option from the security drop-down menu and use a slider bar to choose one of three detection settings. The Commtouch service is extremely good as it generates a hash value for each email which it compares with its own remote servers. Commtouch works with a number of ISPs, allowing it to store hashes of known spam, making the identification process very simple.



It certainly worked well during testing as we set up the anti-spam service to tag all known spam and let it through. We used an Outlook client to download live email from a number of accounts and created a rule to pass tagged mail to a separate folder. After eight days, we saw a spam success rate of 100 per cent, with only three false positives.

The Cobion web category database can be used remotely or locally. Policies are applied to connections and appear in the same dialogue box as traffic rules where you choose the categories you want to block. We found performance was very good: with the games and gambling categories activated, we were blocked from all but one of 50 online bingo sites visited.

For anti-virus scanning, you pick the protocols you want Kaspersky to check and for each one you decide which files to scan and what actions to take. Intrusion detection is based on the well-respected Snort and GateProtect provides an extensive attack database that is updated regularly. Even IPsec and SSL VPNs get the GateProtect touch as wizards are provided for both server-to-server and client-to-server connections and they appear in the desktop, so you can see exactly which ports they apply to.

GateProtect's approach to UTM appliance management is refreshing and has clear advantages when configuring complex firewall rules. The GPA 400 delivers an impressive range of security features and we found the eGUI management client really made it easy to configure most of them without making any errors.

Dave Mitchell

PRODUCT INFORMATION

Vendor
gateProtect

Product
GateProtect GPA 400
www.gateprotect.com

Price
From £2,812 (exc VAT)

PRODUCT RATING

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★☆
Documentation	★★★★☆
Support	★★★★☆
Value for Money	★★★★☆
Overall Rating	★★★★☆

For
The eGUI is a pleasure to work with, excellent web filtering and anti-spam performance, a complete range of security measures that can be easily customised, good overall value

Against
No UK resellers yet

Verdict
With an impressive range of features, GateProtect offers security appliance management that will avoid the pitfalls of misconfiguration

