PRODUCT REVIEW: NORMAN NETWORK PROTECTION APPLIANCE – JULY 2009

This product review marks something of a departure for *VB*, as we take a break from our usual diet of desktop anti-virus products and security suites to take a look at one of the growing field of hardware-based security solutions. The security appliance market seems to have become a boom area of late, with just about every security firm worth its salt introducing an appliance solution to provide its services in a single package. Dedicated firewalls, spam filters and web filters, as well as integrated blends offering a selection of these features, all jostle for position in the marketplace, all looking for the unique selling point which will set them apart from the crowd. In this month's review we will be looking at a dedicated anti-malware solution: *Norman's Network Protection Appliance*.

PRODUCT AND VENDOR

Norman has been around since pretty much the dawn of time as far as computer security and anti-malware goes. Founded in 1984 (as the company's website points out, some two years before the first PC virus and four years before the first virus was discovered in the company's native Norway), the company quickly went global and over the next decade or so developed a variety of security solutions and services, before merging with the brains behind the classic *ThunderByte* anti-virus product. *Norman*'s *Virus Control* product line has been a stalwart in VB100 testing since its inception over ten years ago – one of an elite few to achieve a pass in the first ever certification (see *VB*, January 1998, p.10) and maintaining a splendid reliability ever since.

Alongside its venerable flagship product line, the company has continued to innovate in a number of areas, with pioneering work at corporate server and gateway level in the early days, followed up by early entry into the spheres of personal firewalls and anti-spam. The *Sandbox* solution – which evolved from internal emulation in the *Norman* scanner into a standalone, automated malware analysis system – was a revolution when it first appeared and remains cutting edge (as anyone who has joined a crowd of entranced onlookers at a demonstration of its abilities can attest). The inclusion of the advanced *Sandbox* technology in the company's anti-malware scanner, and the resulting high levels of signature-less detection of new malware, have made the engine a favourite for inclusion in OEM and multi-engine products, many of which are now also regulars in *VB* testing.

The company's online presence at www.norman.com has undergone a fairly drastic overhaul of late, and provides a wealth of information in a slick and accessible format. The *Network Protection* solution is fairly new to market and is currently being heavily promoted, with a prominent advertisement in the form of an animation showing a machine sliding rapidly into place – apparently a metaphor for the system's easy implementation. A selection of related information is provided on the website, including registration for a trial version, detailed product overview sheets and a full manual. A link provides details of a recent accolade for the product: a 'Best in Antimalware Solution' prize from *Network Products Guide*.

The appliance is available either pre-installed, with a choice of fairly standard set-ups of either *Dell* or *HP* hardware, or as a software version, provided complete with operating system as a CD or iso image download. For those opting to use their own hardware, the minimal specifications are fairly exacting, thanks to the rather specific demands of the networking and RAID design and the need for reliability. Thus the software version is unlikely to suit anyone trying to save pennies by recycling an old system, but the self-install option is provided for those organizations with fixed policies on hardware sourcing; in addition to the *HP* and *Dell* specs also available directly from *Norman*, an acceptable design of *IBM* hardware is approved.

The version provided for this review was the full hardware set-up, installed on a *Dell* box, so we didn't get to try the complete installation process, but as a pre-configured system it seemed likely to be fairly straightforward; the guidance in the manual mainly covers correct implementation of network cards, with the bulk of the set-up on a fixed, option-free path.

The shipped machine came with a clear and straightforward quick-install guide, which looked ample to steer us through, but we also took along a copy of the manual in case of need. The manual is provided both as a complete guide and as a tailored version for purchasers of the full hardware appliance, leaving out all the unnecessary information on initial installation. With plenty of support on hand, we took the box into the test lab and prepared to fire it up.

INSTALLATION AND SET-UP

Following the instructions in the admin guide, a network layout was planned but nothing plugged in until the initial stages of IP address configuration were completed. During the initial stages of our anti-spam testing regime we spent many hours setting up a selection of appliance products, and experienced a wide variety of initial set-up processes required to get a machine activated and integrated into a network. It was interesting to see just how many different ways there are of getting a piece of hardware configured out of the box – some require full direct access with a keyboard and monitor, others demand access via a pre-configured IP address, while a few are even accessed via a good old-fashioned null-modem cable. At least one appliance on the market is capable of picking up an address from DHCP and displaying it on an LED front panel, allowing the administrator to access it with no special tweaks to his network. In *Norman*'s case, the initial stage required console access with a keyboard and monitor, which should present little difficulty to the average corporate admin with a KVM switch handy.

The boot-up showed the system to be based on *Debian Linux*, with a slick and attractive splashscreen identifying it as a *Norman* product. With the initial stages of booting complete, a simple text-based process led us through the low-level configuration: the keymap used, a password for the root user, hostname and IP address for the management interface, speed configuration of the additional interfaces, and time zone. With this complete and details confirmed, the machine was rebooted before being ready for remote control via the management link. The manual urges readers not to boot up the machine before connecting it to the network, but being dedicated troublemakers we ignored this advice and tried various configurations of switching on and off and plugging network cables in and out, without upsetting the system at all. Of course, such behaviour is not recommended and we would urge readers always to pay attention to instructions from their solution providers.

Once up and running again, and connected to the chosen management network, a web interface is accessed via a browser, which is fairly standard for appliances. This one seemed smooth and stable, with none of the awkward load time or wobbly, error-prone controls we have observed in some of the appliances run as part of our anti-spam testing. On initial access, the appliance runs through a second stage of configuration, this time focusing on the protection side of things, starting with the selection of a password and configuration of access controls for the configuration interface itself, restricting access to specific IP addresses or subnets.

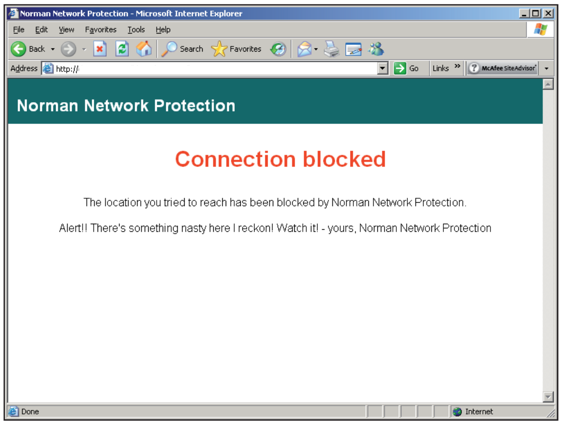
A licence key is required for activation, and then a selection of settings screens are run through, including a separate setting for each of the protocols covered by the system. The protocols covered include HTTP, FTP, TFTP, SMTP, POP3, SMB/CIFS, RPC and IRC, and each can be scanned at a different level, with traditional signature scanning, the sandbox, and looking inside archives all available. Other options include how long to keep known bad URLs blocked, and a configurable message to display to users trying to access a blocked site. This can take the form of either a customized message on a standard web page or a bespoke web page at the location of your choice. Some control of logging and email alert messaging is also provided, and updating can be set to a range of periods or left entirely manual. All in all, barring the time spent getting hold of a licence key to activate – which would normally be provided along with the shipped product – and despite some time spent messing around with settings and trying unsuccessfully to confuse the system, the whole set-up from initial boot to fully operational status took less than half an hour, much of which was spent waiting for reboots and rummaging for network cables of the right length.

MALWARE PROTECTION AND CONTROL

With the machine set up more or less to our liking, it was time to see how it went about protecting networks. The design of the product is brilliantly simple; apparently inspired by a demanding commission from a food manufacturer (requiring protection from malware in a sealed and certified environment where changes to either software or network configuration were highly undesirable), the *Norman* appliance sits invisibly between two network nodes, its two interfaces simply passing all data through and keeping an eye on the stream as it goes by, blocking the transfer of anything identified as a danger. So we simply slid the machine in between the hubs of two subnets, moved the cable connecting them to one interface on the appliance, inserted another in the second interface to complete the link, and sat back to watch.

After an invisible judder as the network adjusted itself to the new layout, connection between the two subnets seemed entirely unaffected and data transfer between them continued virtually uninterrupted. Checking the management GUI showed that traffic was being watched and throughput levels recorded, and attempts to pass malware samples from the outer zone to the protected subnet were immediately blocked. It all seemed very easy and painless.

We tried a variety of transfers via various protocols, and all seemed to function along much the same lines, with

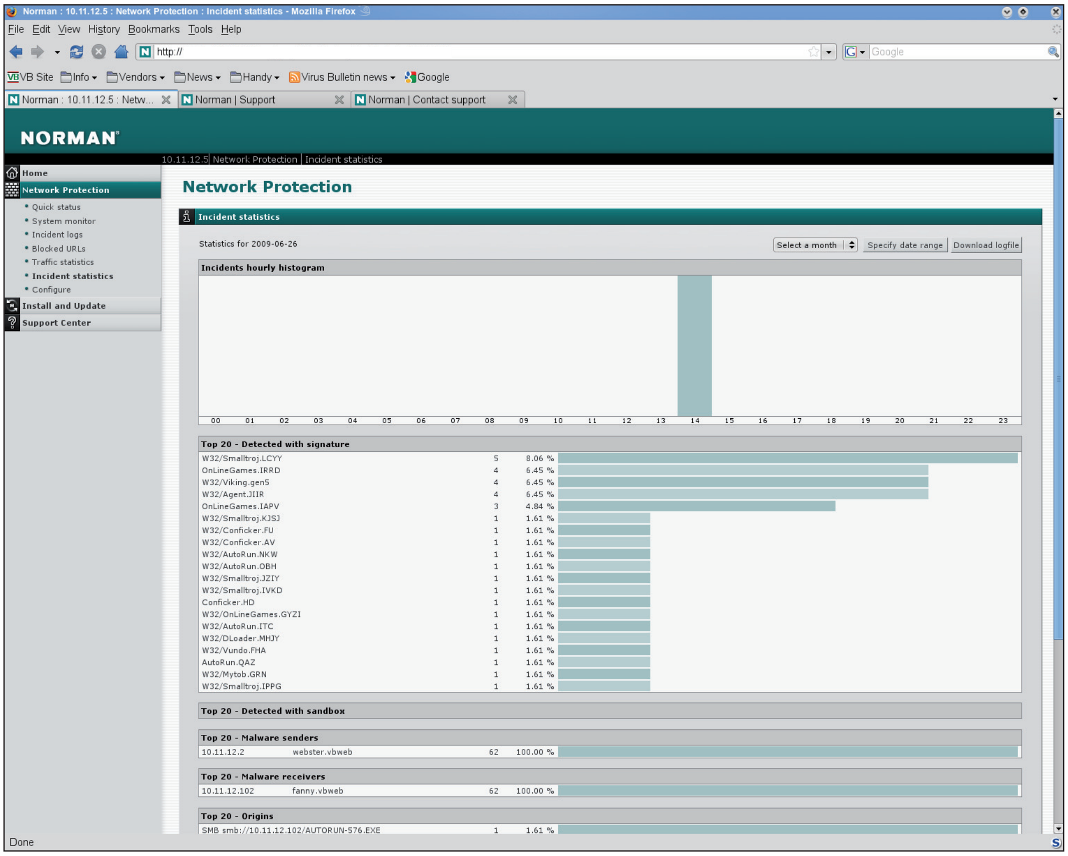

Norman Network Protection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://
Go Links McAfee SiteAdvisor
Done
Internet

Norman Network Protection

Connection blocked

The location you tried to reach has been blocked by Norman Network Protection.

Alert!! There's something nasty here I reckon! Watch it! - yours, Norman Network Protection



Statistics for 2009-06-26

Top 20 - Detected with signature

W32/Smalltroj.LCYY	5	8.06 %
OnLineGames.IRRD	4	6.45 %
W32/Viking.gen5	4	6.45 %
W32/Agent.JIIR	4	6.45 %
OnLineGames.IAPV	3	4.84 %
W32/Smalltroj.KJSJ	1	1.61 %
W32/Conficker.FU	1	1.61 %
W32/Conficker.AV	1	1.61 %
W32/AutoRun.NKW	1	1.61 %
W32/AutoRun.OBH	1	1.61 %
W32/Smalltroj.JZIY	1	1.61 %
W32/Smalltroj.IVKD	1	1.61 %
Conficker.HD	1	1.61 %
W32/OnLineGames.GYZI	1	1.61 %
W32/AutoRun.ITC	1	1.61 %
W32/DLoader.MHJY	1	1.61 %
W32/Vundo.FHA	1	1.61 %
AutoRun.QAZ	1	1.61 %
W32/Mytob.GRN	1	1.61 %
W32/Smalltroj.IPPG	1	1.61 %

Top 20 - Detected with sandbox

Top 20 - Malware senders

10.11.12.2	webster.vbweb	62	100.00 %

Top 20 - Malware receivers

10.11.12.102	fanny.vbweb	62	100.00 %

Top 20 - Origins

SMB smb://10.11.12.102/AUTORUN-576.EXE	1	1.61 %

network latency barely noticeable as traffic flowed smoothly through the system. Even with large files and the most thorough settings, little slowdown was observed, and malicious items tucked into archives were noticed as the final few packets made their way across the network. Compared to more proxy-oriented appliances, which may require full download to the appliance before scanning, then transfer to the target system once files have been approved, this invisible bridging set-up provides much smoother and quicker connectivity. The system automatically blocks access to web domains found to contain malware, showing a warning message instead, while other protocols simply present a 'not found' or 'access denied', again keeping the specific path blocked for a configurable period. If desired, the URL blocked message shown for the HTTP protocol could even be configured to display a standard 404 message, thus erasing all evidence from the user's point of view that the appliance is monitoring traffic to their network.

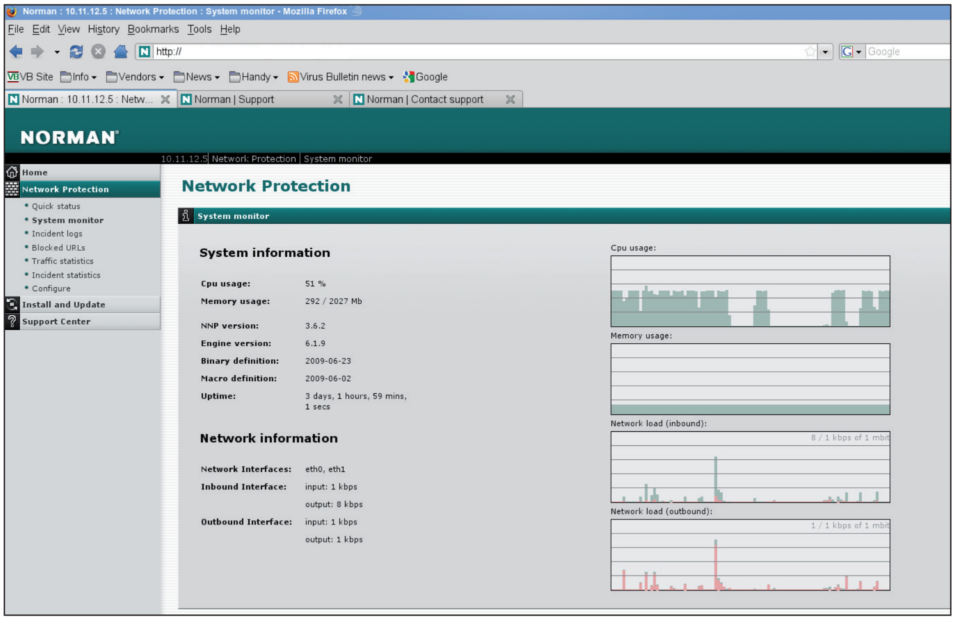
Going back into the configuration system to tweak settings provided the same set of controls run through in the initial set-up, with the main area being the level of scanning imposed on each supported protocol, with the option to ignore all traffic over a given protocol if so desired. The most significant option here is whether or not to use the *Sandbox* facility. We found this gave a significantly better level of detection, particularly for the newest samples, without excessive increase to the connection overhead. There is also a simple way to exclude certain systems or network segments from filtering, and a set of options that allow scanning to be disabled, passing all traffic through unhindered, or to completely block all traffic – the so-called 'panic button'.

The remainder of the controls provided in the interface covered the logging and reporting of traffic and incident data. One area that seemed to be missing was the option to adjust the low-level settings of the appliance operating system itself, but little needs doing here in most situations. Rather oddly, when we went back in via the console and hacked some changes to the IP address to connect to a different network for management, we found that the web GUI did not register the change but continued reporting the old address (perhaps because we hadn't restarted the system), but no ill effects were observed and everything continued to operate smoothly.

REPORTING FEATURES

The main function of the GUI, once the basic settings have been adjusted as required, is to provide information on traffic and incidents, and it provides a useful selection of tables and graphs which present all the necessary information clearly and logically.

The 'Quick status' page provides an overview of the system set-up and settings, details of the product and update versions, a summary of the network interfaces and how they are running, the number of files processed and those found to be malicious, and the settings of the scanner on a per-protocol basis. The 'System monitor' gives more detailed information on CPU and memory usage, uptime, product and update versions, and network load, accompanied by



System information

Cpu usage: 51 %
Memory usage: 292 / 2027 Mb

NNP version: 3.6.2
Engine version: 6.1.9
Binary definition: 2009-06-23
Macro definition: 2009-06-02
Uptime: 3 days, 1 hours, 59 mins, 1 secs

Network information

Network Interfaces: eth0, eth1
Inbound Interface: input: 1 kbps
output: 8 kbps
Outbound Interface: input: 1 kbps
output: 1 kbps

some nice graphs which chart changes in load over time. The other sections show statistics on traffic passing through the system, and on threats spotted and blocked, with detailed logs of all detected threats and malicious URLs, and full data on systems hosting and targeted by malware. All of this information can be configured to cover specific periods and levels of verbosity, and exported to plain logs.

One of the most interesting features here is the *Sandbox* log area. Where a malicious item has been run through the *Sandbox* system, detailed information is logged on the behaviours spotted when executed in the emulator. This data, including information on how a file has been packed or encrypted, what changes it makes to the filesystem, what network activity it attempts and more besides, is also made available to the administrator. These reports always make for fascinating reading, and are of great value in identifying malicious items and tracking down any activities they may have perpetrated before being caught. With automated log retrieval and parsing, the data can be used to keep other parts of the network secure by updating firewall rules and other security systems.

Email and SNMP options allow alerts to be sent to administrators without keeping an eye on the interface, again with fairly in-depth configuration of what level of data is recorded, where it is sent and how. With the logs saved on the local system, administrators can of course also automate transfer of logs as required, using the underlying fully functional *Linux* system. This would allow a fairly detailed record of all activity passing between the appliance's bridged interfaces, including what kind of malware was coming in, from where, and where it was headed when intercepted – all useful data for the alert security admin.

CONCLUSIONS

Having looked at a number of similar appliances in recent months, there were a few things that we expected to find in *Norman*'s solution but which were lacking. Many products targeting the same sort of market offer online reputation databases to block known malicious URLs, detailed content inspection and control of user activity, for corporations to keep a tight rein on their employees' web-browsing habits, configurable monitoring of specific applications and versions, and much else besides. *Norman*'s selling point is all about simplicity though. Its raison d'être is to block malware passing through the core protocols, and it does that with remarkably little effort on the administrator's part. The plug-and-play ease of implementation also makes it very flexible, happy to be installed in any part of the network rather than being limited to the gateway.

Being practically undetectable to the network it is protecting, up until the moment it blocks the transfer of a malicious item, makes it not only extremely easy to integrate into just about any network layout, but it also keeps the overheads to a minimum, barely impacting traffic flow until it is needed. The integration of the *Sandbox* detection alongside the traditional signature scanning adds an extra layer of defence against new and unknown threats. Providing such simple and unproblematic malware protection, along with an excellent, again very straightforward control system, makes this an extremely user-friendly weapon in the fight against malware problems in business networks, as well as a powerful one. We look forward to investigating a wider range of appliances to see how they match up to this impressive effort from *Norman*.

NORMAN®

Norman ASA, P.O. Box 43, N-1324 Lysaker, Norway
Tel: +47-67-10-97-00, Fax: +47-67-58-99-40
Email: norman@norman.no
Web: http://www.norman.com/nnp