

This Month's Review

Checking out eye-catching products

Proventia[®] M10 Internet Security Systems[™]

The Proventia M10 is a low-cost, security gateway appliance, packed with a number of functions necessary for protecting corporate, in-house network security. The establishment of this product enables internal network protection against a variety of security threats, particularly external hacking and viruses. In this review, I hope to provide an overview of the characteristics and functions of the Proventia M10, and to clarify its advantages and drawbacks.

By Hiyoshi Ryuu



A low-priced, multifunctional, integrated, security gateway appliance

Positioning of the Proventia M10

Internet Security Systems (ISS) is a vendor dealing exclusively with security, selling security appliances, and vulnerability checks/audit tools. In terms of the company's security appliance lineup, on offer is the "Proventia A" series, an intruder detection system (IDS) appliance, the "Proventia G", an intruder prevention system (IPS) system, and the "Proventia M", an all-in-one security appliance. The Proventia M provides the following functionality:

- ① Firewall functionality
- ② VPN functionality
- ③ IPS functionality
- ④ Antivirus functionality
- ⑤ Web filtering functionality
- ⑥ Anti-spam functionality

The M30 and M50 models were released as products in the same series prior to the release of the "Proventia M10" (referred to below as the M10) in July 2004. However, with the M30 and M50, all functions other than firewall functionality were only available as paid options, meaning that a considerable expenditure was needed to achieve an "all-in-one" configuration. The M10 was released as the lowest model in the M series. However, all of the paid options in the upper models M30 and M50 came as standard options in this model.

The function-enhanced M10 version was shipped in December 2004. With the function-enhanced version, in addition to increasing the number of LAN ports from three to four (external connection port x1, internal connection port x1, user-defined port x2), the design of the auxiliary settings/control tool - the "Proventia Manager" - was redesigned, improving its functionality.

What follows is an outline of the functionality-enhanced version, the M10.

In comparison with the upper models, the M10 hardware specs have been limited. However, the M10 demonstrates ample performance while not exceeding the limitations of its 100-node maximum (Table 1). Furthermore, the price has been kept down for the basic unit to between ¥207,900 (5 nodes) and ¥522,900 (100 nodes), making the M10 an effective alternative for achieving gateway security measures inexpensively.

Note: Prices are applied to purchases with Japan only.

Installation and initial settings

Before dealing with the previously mentioned five functions, let's first discuss its installation and initial settings. Because the M10 is equipped with a hard disk, some care must be taken with exhaust heat. However, the chassis is quite compact (height 4cm x width 25cm x depth 18cm), meaning very few problems with choice of installation location. When setting up an in-house network, the model is often set directly below the existing router. However, the M10 can also be directly connected to PPPoE-compatible broadband lines for compatibility with PPPoE as well, so as to enable use of a full-time connection service. When test-connecting the unit at this writer's home to a B Flets Home Type (VDSL type) line, the connection was both straightforward and stable.

To carry out the initial settings for the M10, the first thing to do is to connect the unit to the PC using the Null cable supplied. For this, a PC with an RS-232C port is necessary. If the M10 is accessed using terminal software on the PC for implementation of the initial network-related settings, the various settings and controls can be made from a Web browser. In principle, Internet Explorer is recommended as the Web browser to use in this case. However, in my experience, both Mozilla and Firefox also work properly.

After completing the initial settings, if you connect to the M10 from the terminal via SSH and execute "uname-a", a message appears as shown in screen 1. As you can tell from this message, the M10 adopts x86 architecture hardware and runs a customized Linux (kernel 2.4 base).

Combining high-speed processing and multi-functionality

With many all-in-one type security appliances, functions developed/sold by other companies are incorporated in the design, as it is difficult for a single vendor to realize all security-related functions.

In contrast, while the M series including the M10 boasts a large array of security-related functions, they are all packaged by ISS. Further, because of the high-degree of integration between functions, the units combine high-speed processing with multi-functionality.

With the M series, all functions are incorporated as a single module, referred to as SDTI (Synchronous Deep Traffic Inspection). Processing common to each function is executed by the same engine inside the module. Optimization of the performance of this module can be more simply and effectively implemented in comparison with the optimization of the multiple modules of typical all-in-one security appliances on offer from other companies.

In view of this, one can see that units in the M series are quite different from appliances that merely aggregate a number of security functions.

Table 1: Hardware specs and performance of the Proventia M10 and high-positioned models

	M10	M30	M50
Monitoring port capable Ethernet standard x number of ports	10/100×4	10/100×6	10/100/1000×8
Build in HD redundancy	—	—	RAID1
Power source redundancy	—	—	○
Chassis design	Tabletop	1U	2U
MTBF (Average period until failure)	3.1 Years	6.4 Years	5.2 Years
Maximum number of nodes	Up to 100 nodes	Up to 500 nodes	Up to 2,500 nodes
Maximum throughput when using full state packet inspection	100Mbps	200Mbps	1,600Mbps
Maximum throughput when using full state packet inspection and IPS	100Mbps	200Mbps	800Mbps

Screen 1: When logging into Proventia M10 via SSH and executing "uname-a"

```

root@proventia:~
login as: root
Sent username "root"
root@192.168.1.1's password:
Last login: Sun Feb 13 23:29:44 2005 from 192.168.1.2
[root@proventia root]# uname -a
Linux proventia.bflets.dyndns.org 2.4.18-1000.ISS.24 #1 Fri Oct 1 15:56:13 EDT 2004 i686 i686 i386 GNU/Linux
[root@proventia root]#

```

Checking out eye-catching products!

Proventia M10,

a low-priced, multifunctional, integrated, security gateway appliance

① Firewall functionality

The M10 is equipped not only with the standard, packet filter type, firewall functionality, but also with full state packet inspection functionality. With general packet filters, a check is made of the sender and receiver IP addresses and port numbers. However, with full state packet inspection, a check is also made of the packet data. In this way, it is possible to prevent passage of unauthorized packets (such as spurious response packets not corresponding to required packets sent from LAN), which are inadvertently passed by packet filters. With the M10, a DMZ (a network in which an Internet server exists, and access is permitted from the outside to that server) can also be constructed, meaning hardly any problems when used for typical applications.

The firewall function settings screen is simple and self-explanatory, and there were no problems with the operations (screen 2). However, there appeared to be no detailed settings^{*1} for the firewall device.

^{*1} With the firewall device, detailed settings can be implemented designating the value of the timeout for each protocol and for policy creation, targeting protocols (ICMP etc.) other than TCP/UDP.

② VPN functionality

Easy setting of VPN functionality is another characteristic function of this unit. A number of settings patterns for connecting to WindowsXP-equipped VPN clients and VPN appliance Netscreen, etc. are already preset, meaning that VPN connections can be implemented with only a few clicks. Also, the equipment shown in Figure 2 comes with a special manual for connecting VPN with the M10. Settings for implementing VPN connection are extremely difficult to make without expert knowledge. Thus, this manual will no doubt come in handy in more than a few cases.

③ IPS functionality

Generally with IPS functionality provided by other companies, the process is based on detecting malicious code with specified patterns, using signatures (data for detecting intrusions). In contrast, the M10 IPS functionality is designed so as to detect behavior related to attacks on vulnerabilities specified by signatures^{*2}. In other words, it becomes possible to detect new malicious code and subspecies with different malicious code targeting the same vulnerability with a single signature. Also, introduction of equipment with IPS functionality almost always involves implementation of highly detailed settings. However, with the M10, IPS settings are completed simply by checking a check box referred to as “X-Force® Protection Responses Enabled” on the IPS settings screen (screen 3). In other words, the settings can easily be done, even by an administrator with no background in security. In the case of the abovementioned setting, the settings are those recommended by X-Force^{*3}, a private sector, maximum-security research agency under ISS. These settings offer a reliable defense based on consideration of risks and characteristics of attacks and similar behavior. For example, when a “Ping Sweep^{*4},” which can hardly be called an attack, is detected, no particular action is taken, but when a “Ping of Death^{*5}” packet, which is certainly an attack, is detected, the packet is automatically destroyed. When the X-Force-recommended settings are not in effect, only IDS equivalent detection procedures are implemented, and all attacks will pass through as is. Thus it is highly advisable that the X-Force-recommended settings be used. Incidentally, ISS has a substantial share of the IDS/IPS-related market. Of these, the Proventia series held the number 2 position in the 2003 global share of the IDS/IPS hardware market. It was cultivated here by the time the share was acquired.

Screen 2: Firewall function access policy settings screen

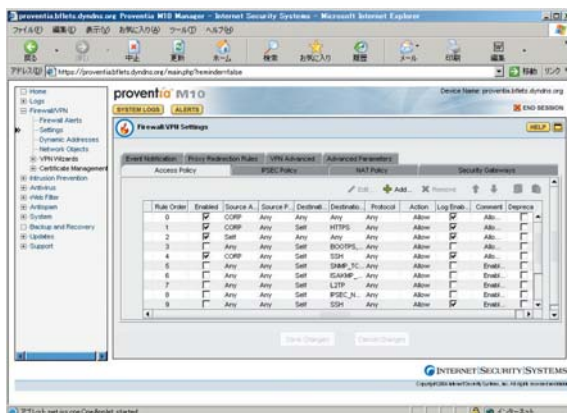


Table 2: Products equipped with manuals for connecting VPN with Proventia M10

Connections between bases

Cisco PIX 515E

Check Point NG FeaturePack 3 system

Proventia M series

NetScreen (version 4.0.0r6)

Symantec 5310

Remote access

SafeNET SoftRemote LT (version 10.0)

Windows 2000/XP

Know-how has been lavishly poured into the M10 IPS functionality. This is to say, the M10 comes with detection capacity basically on par with the RealSecure® series, ISS' trademark product, which boasts the major share of the domestic market.

*2 Detection functionality based on signatures of behavior targeting specific vulnerabilities is referred to as "virtual patch functionality." Its edge is amply demonstrated when protecting the server segment, for which security patch applications cannot easily be implemented during operation.

*3 More than half of high-risk, currently divulged vulnerabilities are discovered by X-Force, and this technological capacity has an established reputation.

*4 A Ping Sweep is a method of inspecting effective IP addresses through transmission of a ping to a range of IP addresses. It is used as a method of searching for target hosts to attack. However, some operational management software implemented by network managers is also designed so as to detect connected hosts using the same method. Thus Ping Sweep cannot always be called an attack.

*5 Ping of Death is an attack that brings a machine down by sending a special ping packet to a host with a specific vulnerability.

④ Antivirus functionality

With antivirus functionality, it is possible to specify HTTP, FTP, SMTP, or POP as the protocol to be monitored. Viruses are detected through packet analysis for the specified protocol. The virus detection capability of this function can be considered formidable, as it responds to virus activity in accordance with 100% WildList*6. At the time of writing, the unit is equipped with a detection engine using a general pattern file. However, by the second quarter of 2005, VPS is scheduled to be added as a detection engine. VPS will be combined with the conventional detection engine, which is expected to further increase the detection capability.

*6 100% WildList is the "Currently active virus list", released monthly by "WildList Organization International", a volunteer organization carrying out data summation regarding viruses.

*7 VPS is an abbreviation of Virus Prevention System, and refers to a detection engine which makes a determination of whether data is a virus based on analysis of program behavior. Since pattern files are basically not necessary, detection of unknown viruses is enabled.

⑤ Web filtering functionality

The Web filter functionality uses proprietary Cobion technology acquired by ISS. Cobion is a company that exclusively developed content analysis software used in Web filters and spam measures. This company has technology to automatically collect Web data and technology to analyze the collected images and text. Based on this technology, it has compiled the world's largest URL database, with more than 1,000 servers. Accordingly, the Web filter functionality could easily be called top notch. However, at present, response to Japanese sites could not be called sufficient*8. Further strengthening of response to Japanese sites is scheduled, and it is hoped that this point will be rectified in subsequent releases. The filter database includes the URLs of sites loaded with spyware*9 and phishing sites*10. In other words, this functionality enables blocking of access to sites, which should indirectly increase the security level of in-house corporate systems.

*8 Image recognition technology operates irrespective of language. However, text analysis technology for the analysis of words extracted from images and Web page text is at present incapable of response except to English.

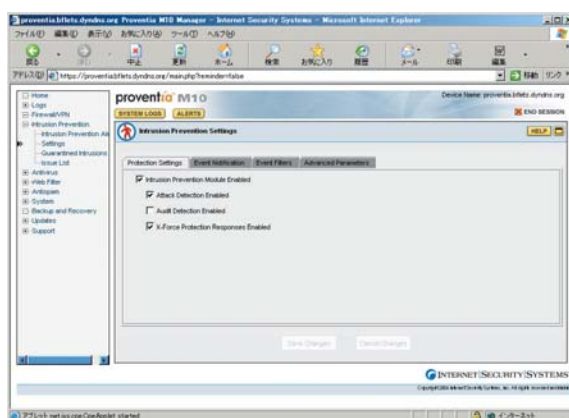
*9 Spyware is a term for programs that misuse a PC accessing the Internet, collecting Website browsing history and user ID/passwords etc. from the PC.

*10 Phishing sites are sites designed to implement scams, in which credit card numbers and pin numbers are fraudulently acquired.

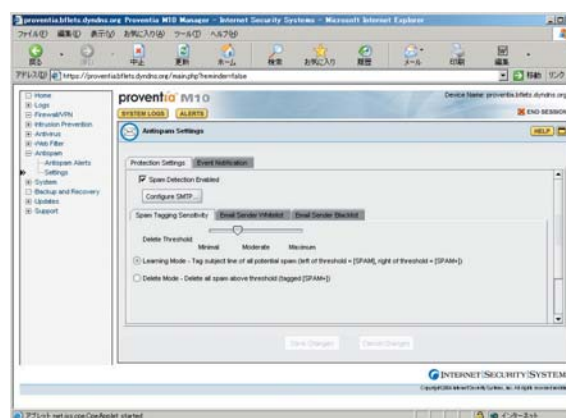
⑥ Anti-spam functionality

The anti-spam functionality detects spam through matching against a database of registered information related to preexisting spam mail (referred to below as spam). Also, is it possible to specify a white list of sender addresses never to be recognized as spam and a black list of sender addresses to always be recognized as spam. Furthermore, you can select whether to delete emails deemed to be spam or to deliver such messages with either [SPAM] or [SPAM+] appended to the subject line (Screen 4).

Screen 3: IPS function settings screen



Screen 4: Anti-spam function settings screen



Checking out eye-catching products!

Proventia M10,

a low-priced, multifunctional, integrated, security gateway appliance

As far as the writer knows, the unit can reliably detect English spam. However, Japanese spam detection is a little weak. The anti-spam functionality basically uses the same technology as the Web filter, functionality that will likely be subsequently strengthened in terms of Japanese spam response.

M10 operational management

“Proventia Manager”, the M10 settings/management tool is easy to use because it offers a Web interface (for which the reader should refer to the screens included in this review) achieving consistency of appearance and operability. Incidentally, if Site Protector™ - an appliance integrated management system offered separately - is used, it is possible to collectively manage multiple M10 units and other ISS products. Settings do not need to be changed often, so normally access is made through the alert screen (screen 5). Operability is good, although it is worrisome that the standby period until screen display increases with the accumulation of alerts. Also, while the M10 syslog can also be accessed by Web browser (screen 6), settings for transferring this log to the system log server were unfortunately missing*11.

If the user is unsure how to appropriately carry out M10 operation management, it is best to consider using the “MPS for SMB*12” monitoring service offered by ISS. (This service is available for around ¥40,000 a month*13.) With this service, ISS implements operational monitoring of the M10 directly, which no doubt achieves/maintains an ever higher security level than one could achieve on one’s own.

*11 If the log management demon (syslogd) settings file “/etc/syslog.conf” is manually rewritten, it is possible to transfer the log file to the syslog server. However, changes to the settings file are implemented at one’s own risk.

*12 MPS for SMB is an operation/monitoring service for the Proventia M series, aimed at small- to medium-sized companies with 500 employees or less.

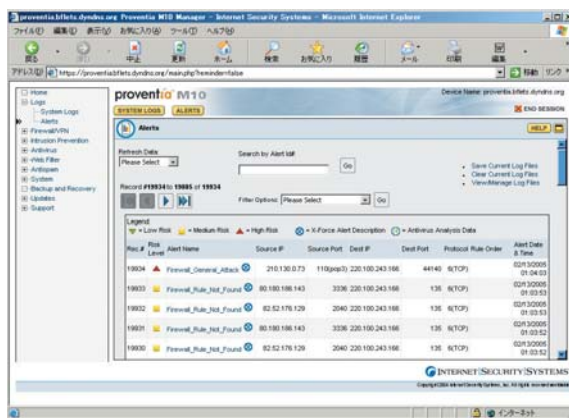
*13 Prices are applied to purchases within Japan only.

Excellent cost-performance ratio

With the introduction of the M10, there are both unit price and maintenance expenses to consider. However, the only costs incurred starting two years after the introduction are maintenance expenses. If no maintenance contract is signed, updates of the signatures and data used by the various functionalities will not be received. Thus, a maintenance contract is really essential.

The M10 unit price and maintenance fees are determined by the number of nodes installed under the M10 (Table 3), but they are set extremely low. Table 4 shows the expenses for the M10 and the higher-positioned M30 model in the case of 100 nodes. In the opinion of this writer, this data highlights the superior cost-performance ratio of the M10 – I wonder whether our readers agree.

Screen 5: Alert Screen



Screen 6: Syslog screen

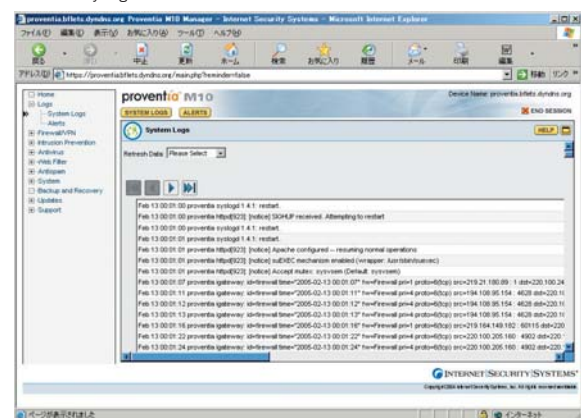


Table 3: Expenses for the Proventia M10

	Up to 5 nodes	Up to 25 nodes	Up to 50 nodes	Up to 100 nodes
Unit cost	¥207,900	¥312,900	¥417,900	¥522,900
Annual maintenance	¥62,370	¥93,870	¥125,370	¥156,870
First year expenses	¥270,270	¥406,770	¥543,270	¥679,770

Note: Prices are applied to purchases within Japan only.

Table 4: Cost comparison of the Proventia M10 and M30 (when using 100 nodes)

	M10	M30
Unit cost	¥522,900 (100 nodes)	¥577,500 (up to 500 nodes)
Annual maintenance	¥156,870	¥86,625
VPN license	With unit	¥65,100 (first year only)
IPS license	Not necessary	¥112,035 (100 nodes/year)
Antivirus license	Not necessary	¥112,035 (100 nodes/year)
Web filter license	Not necessary	¥112,035 (100 nodes/year)
Anti-spam license	Not necessary	¥112,035 (100 nodes/year)
Total (first year)	¥679,770	¥1,334,970
Total (second and subsequent years)	¥156,870	¥692,370

Note: All prices include sales tax and are applied to purchases within Japan only.

Highly Expandable

With appliances, generally, no alterations are needed except for bug fixes. However with the M10, many more functions are scheduled to be added later. Refer to Table 5 for a list of additional functions which are currently scheduled to be added.

Of these, the addition of transparent mode-enabling installation as a bridge without the slightest change to preexisting network configuration – is highly anticipated. This addition will make installation of the M10 a breeze, while ensuring the security of the M10 itself.

Producing maximum results on a limited budget

Problems noted in this test of the M10 were that log handling is a little weak, menus and so on with the Web interface are shown in English, and detailed settings cannot be implemented. However, you will likely not be disappointed in terms of the functionality of this product.

A strategic price has been set while providing the unit with all of these functions, and the cost-performance ratio is quite high. If the M10 is installed at the gateway to small- to medium-scale networks, where antivirus software has already been introduced on the client workstations, a very high security level is easily achieved.

Security measures are already a corporate society responsibility – there is no need to wait for enforcement of the Act for Protection of Computer Processed Personal Data held by Administrative Organs this April. However, as security measures are tied directly to business profits, within small- and medium-sized businesses, obtaining a budget is a difficult prospect. In such a business, it is especially important to reap the maximum results on a limited budget. Certainly the M10 is an effective choice for dealing with this issue.

Table 5: Functions to be added later to the Proventia M10 (scheduled)

Period for scheduled addition	Details of additional functions	Additional information
Second quarter 2005	Addition of VPS (Virus Prevention System) to the antivirus functionality	VPS is a detection engine that makes determination of viruses by analyzing program behavior
	Addition of transparent mode	Transparent mode is a functionality enabling installation as a bridge without the slightest change to preexisting network configuration
Second half 2005	Addition of Bayesian filter to the anti-spam functionality	A Bayesian filter is a filter based on Bayesian theory, in which “the probability of the occurrence of future events can be predicted through analysis of the probability of such events occurring in the past.” By learning which emails were spam, it becomes possible to automatically heighten the unit’s spam detection capability.
	Addition of SPF (Sender Policy Framework) support	SPF is technology using DNS to prevent deception by the sender of emails. Mail certification technology used by major companies such as Microsoft and Sendmail is deemed the standard.
	Addition of email content filter functionality	
Certification during Web filter functionality use is implemented via LDAP and RADIUS		

Proventia M10

OVERALL EVALUATION



Very Good

I would like to stress the fact that this appliance - packed with a great deal of functionality - is being sold at an affordable price by ISS, a renowned vendor in security business.

ITEMIZED EVALUATION

Uniqueness



The IPS and Web filter functionalities are considerably stronger than those found in comparable products from other manufacturers.

Ease of Installation



The settings, in and of themselves, can be implemented intuitively. However, they are not likely to be set properly except by people with an understanding of both corporate in-house networks where the unit is installed and of security issues.

Manageability



A plus is that all functions can be managed using the consistent and simple Web interface. However, operation is slow, probably because it was developed in Java.

Functionality



All conceivably essential security functions are included in the unit. In addition to full security functionality, it has been equipped with an uncompromising level of performance.

Expandability



Handling of up to 100 nodes is possible with a single unit. There are a number of attractive items in the functional additions subsequently scheduled.

SCORE DEFINITION

- ★★★★★.....Excellent
- ★★★★.....Very Good
- ★★★.....Good
- ★★.....Average
- ★.....Not Good