NetworkWorld
20-2001

Benchmark Test for Firewall Appliances: »Astaro Security Linux« and »Cisco PIX 515«

Cisco versus Linux

Bernd Klusmann, Christoph Lange
Translated from German by Daniel Bryant

More and more vendors are betting on Linux as a platform for firewall appliances. The open-source operating system produces outstanding throughput values and is closing in on well-established companies in the field, such as Cisco, becoming a serious competitor.

In the second round of the benchmark test »Firewall appliances« two - once again very distinct - candidates were up against each other: Newcomer Astaro, with its Linux-based system, takes on the challenge against the top dog, Cisco, with its PIX firewall. As before, both vendors delivered two machines to the EANTC test laboratory in Berlin, so that we could test the performance with unencrypted, as well as with encrypted connections (for information about the testing methods, see the introductory article in Network World 19/01, page 71).

The test candidates

The Astaro company was founded in 1999 and was transformed into a corporation in 2000. The vendor describes itself as a specialist for security solutions in the Internet. The target group are small and medium-sized businesses of all sectors, as well as subsidiaries and branches of large companies. With the product »Astaro Security Linux«, Astaro offers a Linux-based firewall appliance.

Pyramid Computer Systems GmbH (ltd.) and Cobalt Networks (the latter has meanwhile been bought by Sun Microsystems) offer this software preinstalled as an appliance solution, . A free version of the software is available on Astaro's web server, for private use.


Test and analysis: »Netcom Smartbits 2000« by Spirent Communications.

The 19-inch, 1U (height-unit) system from Astaro is based on the Linux kernel 2.4. A 750 MHz Intel-Celeron-Processor and 128 Mbyte RAM provides a respectable computing performance. Furthermore, a 20-GByte-harddrive, as well as a CD-ROM drive are part of the standard equipment. The connection to the network is established via, up to six 10/100 base-T-cards. Two of them are situated »on-board«, four of them in PCI slots. At the time of our tests, we were dealing with the version 2.0 of the »Astaro Security Linux« software. Further information about Astaro can be found at http://www.astaro.com. An online demonstration of the management interface is also available on-site. However, the access to this online-demo is limited by the number of users, and is therefore often not available.

Test and Measuring Equipment

For the firewall tests, we use »Netcom Smartbits 2000« with the »Smart Flow« and » Smart TCP« applications by Spirent Communications. Smart Flow generates up to 1000 TCP/IP connections with up to 64,000 packet variations for every interface of the analyzer. This lets you simulate company networks with large amount of users. For every established data stream, the analyzer measures the throughput, packetlosses, packet transmission time and variation of the packet transmission time. Smart TCP allows tests of varying performance parameters regarding the connection parameters, as well as rates for establishing and terminating a large amount of connections.

The Cisco Systems firewall appliance is called »Cisco PIX Firewall«. Apart from add-on variations of the »Cisco IOS« software or intrusion detection systems, the PIX family constitutes the basis/core of Cisco's security products. It covers a very wide spectrum that reaches from the teleworker, all the way to large business customers and service providers. Cisco entered the test with the »PIX 515«, which is designed for small and medium-sized businesses.

Cisco delivered both machines with an acceleration card for the encryption. To be able to compare the test results with the earlier, and possible future test results, we only considered the measurements without hardware support for our evaluation. In some test-scenarios we additionally made measurements with the acceleration card, to be able to find out the differences. These results are shown in brackets in the corresponding tables.

A Pentium-MMX-Processor with 200MHz is at work inside the PIX 515. The machine carried 64 Mbyte of internal memory.

The standard equipment of the firewall is two »fixed« 10/100 Base-T-Interfaces. With a 4-port card, the box can be upgraded to 6 Fast-Ethernet-Connectors. The tests are performed with the PIX Firewall, version 6.1 and the firmware »Phoenix Picobios 4.0, Release 6.0«. For more information about the products, go to http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm.

Handling the Firewalls

Both test candidates were easily and quickly installed. The integration into the network takes place via a terminal program or a web browser. Further settings can be made by the administrator with a standard browser from any location.

		Astaro/Pyramid	**Cisco PIX 515**
Without encryption	Throughput uni-directional	73 MBit/s	92 MBit/s
	Throughput bi-directional	68 MBit/s	48 MBit/s
	Latency uni-directional	160 µs	512 µs
	Latency bi-directional	268 µs	1343 µs
With encryption	Throughput uni-directional	33 MBit/s	11 (50) MBit/s
	Throughput bi-directional	17 MBit/s	5 (25) MBit/s
	Latency uni-directional	1521 µs	14175 (2502) µs
	Latency bi-directional	5429 µs	17212 (3577) µs
All measurements were carried out with 512 Byte packets and 20 parallel active clients (for Cisco, the values in brackets are the values measured when employing the VPN acceleration card). The latency measurements for the tests carried out without encryption, were performed with a load of 40 MBit/s. With encryption, Astaro was measured with a load of 16 MBit/s, Cisco was measured with a load of 4 MBit/s			

Results: IP Performance Measurements

An initial installation for the Astaro Firewall that we received from Pyramid was not necessary, as it was delivered with preinstalled software. The software can also be loaded onto other hardware with the enclosed CD ROM or a creatable boot disk. In this case the installation is divided into two parts. The first steps are carried out with an installation menu, the further steps are carried out with the web-supported configuration tool »WebAdmin«. This offers you a clearly structured and intuitive menu. Detailed settings of the firewall can be carried out in the submenus »System«, »Service and User Definitions«, »Network«, »Packet Filter«, »Proxy«, »VPN« and »Reporting«. However, the Online-Help is only available in English. To make up for this, Astaro offers a lot of interesting documents, such as current handbooks in German and English, or Howtos (configuration instructions for specific subjects) at http://docs.astaro.org/. Another helpful resource is the user bulletin board with references about new software or the exchange of experiences with the Astaro Firewall system (http://www.astaro.org).

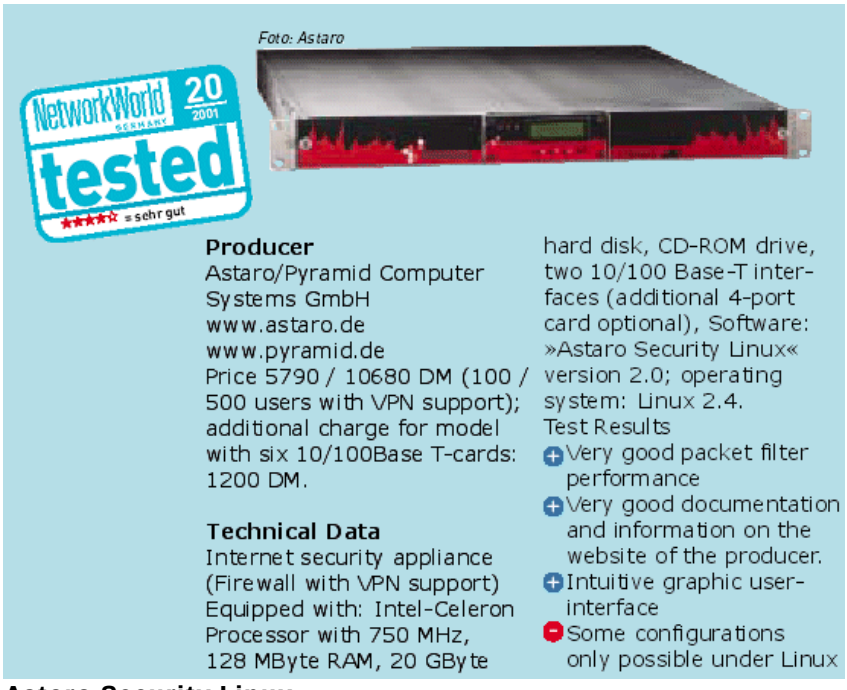
We really liked the reporting function of the system, that presents histograms of the performance data, for example for system hardware, proxy activities and system utilization. Debugging tools based on Linux, such as »snoop« or »tcpdump« were very helpful for error searches regarding the adaptation of the firewall configuration. The telephone support during the tests proved to be highly qualified and helpful. As expected, problems due to varying time zones did not occur with the German producer Astaro.

Function Feature	
Configuration via web browser without additional software	Yes
Backup of the configuration data on the Firewall or PC	Yes
ISDN Interface	No
Ethernet as standard interfaces	Yes
TCP/IP support	Yes
Network Address Translation (NAT)	Yes
Support of Tri-homed firewalls	Yes
Port-forwarding from the Internet into the LAN	Yes
Intrusion Detection Mechanisms	Yes (Port scan detection)
Routing mode	Yes
IPSec-compatible	Yes
Remote administration access via modem/ISDN	No
Reset factory default	Yes
Console port for recovery	Yes
Evaluation standard functions	**4.0**
1 = insufficient, 2 = sufficient, 3 = good, 4 = very good, 5 = excellent	

Standard functions Astaro Security Linux

The Tulip-based 4-port network card showed slight stability problems with the available drivers. That is why we only used the two Onboard-Ethernet-Interfaces while carrying out the tests. Changing the network cards to 100MBit/s in full-duplex-mode was slightly complicated because of some module parameters of Linux had to be modified. It would be better if this setting could also be changed via the web-based interface.

The PIX Firewall 515 by Cisco is also very easy to operate during the first installation. To begin with, we adapted the addresses of the Ethernet ports via a terminal connection. For the configuration we used the known Cisco command-line-mode. After we had created the access from our LAN to the firewall in this way, we used a configuration assistant of the PIX Firewall. The separate steps are very well documented and all parameters that need adjusting are explained in the online help. The entry of rules takes place in self-explaining menus. A graphically presented list of all the current rules offers the administrator a quick overview of the current configuration.



Astaro Security Linux

Results TCP rate test

During the tests we generally did without the browser-supported configuration, as the VPN function can not yet be configured with it. According to a statement by Cisco, this is to be possible by the end of the year. A specific configuration of the complementary hardware was not necessary. Inserting the card was enough to activate it.

IP performance measurements

The results of the IP performance measurements are very good for both producers. As expected, both machines reach the highest throughput values with very large packets (1518 Byte). Both firewall appliances reach a throughput of 100% in uni-directional mode with unencrypted transfer. The first differences become apparent with bi-directional traffic: here Cisco reaches 95% throughput, Astaro only reaches 81%.

The performance limit becomes even clearer with smaller packets. As considerably more packets have to be transferred per time-unit, the demands on the firewall are higher. Cisco displays a very stable behavior. When handling packets with a length of 80 Byte in uni-directional mode, the PIX Firewall reaches a throughput of 22 per cent; in bi-directional mode, it performs at exactly half that value (11%). As the bi-directional mode handles twice as many packets per second as the uni-directional mode, the 11% bi-directional corresponds exactly to the 22% uni-directional.

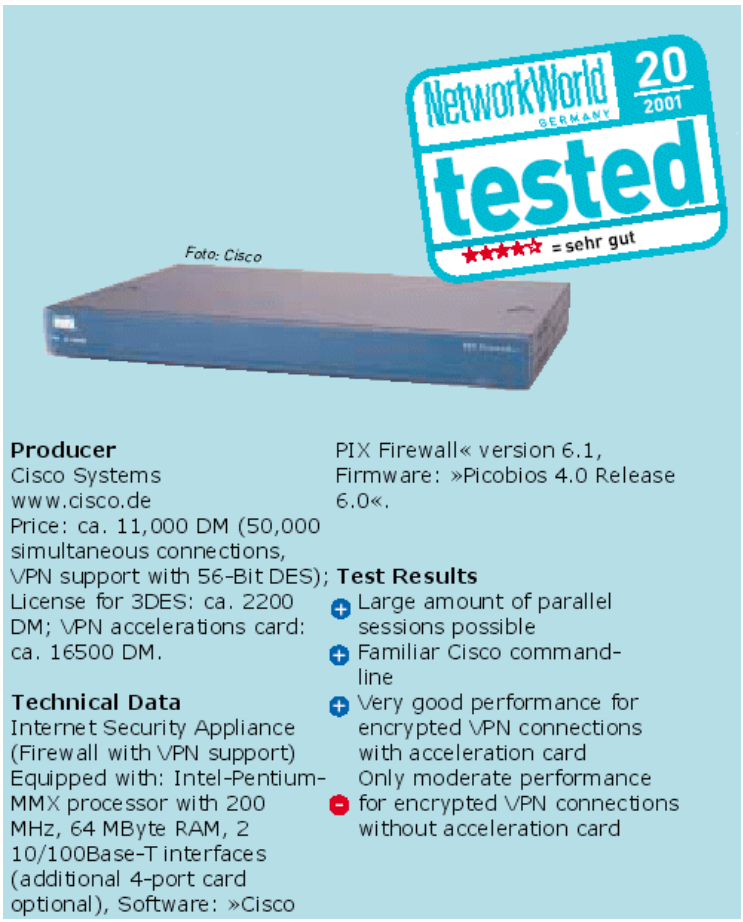
		Astaro Security Linux		Cisco PIX 515	
	Amount of IP clients x connections	No rules	With rules	No rules	With Rules
1000 legal connections	1 IP x 1000	1000 100% 238 µs	1000 100% 236 µs	1000 100% 214 µs	1000 100% 214 µs
	200 IP x 5	1000 100% 230 µs	1000 100% 231 µs	1000 100% 251 µs	1000 99.9% 236 µs
4096 legal connections	1 IP x 4096	1607 39.23% 643 µs	1005 24.54% 1348 µs	4096 100% 213 µs	4096 100% 213 µs
	200 IP x 21	4096 100% 232 µs	4096 100% 232 µs	4096 100% 236 µs	4096 100% 236 µs
6144 legal connections	1 IP x 6144	1421 23.13% 1132 µs	1741 28.32% 794 µs	6144 100% 236 µs	6144 100% 213 µs
	200 IP x 31	6144 100% 233 µs	6144 100% 233 µs	6144 100% 236 µs	6144 100% 236 µs
1000 legal connections at 4000 illegal connections	20 IP x 50	1000 100% 1042 µs	1000 100% 1042 µs	1000 100% 1042 µs	1000 100% 1042 µs
Results for 5000 connections per second (further values online at www.networkworld.de/testcenter)					

The results of Astaro's throughput are not as stable. We performed a total of three identical trials for every measurement value. The fluctuations between the individual trials were as high as 10% with Astaro. These fluctuations that, according to the experience of EANTC, are unusual, could be recreated in Astaro's own laboratory. However, the technicians have not been able to discover the cause of these fluctuations. The values given in the table of results are mean values.

When doing the uni-directional test, we had to carry out static ARP entries (Address Resolution Protocol) on the Astaro Firewalls. The firewall deleted the dynamic entries, which the load generator created with ARP requests at the beginning of every trial, after only ten seconds. Without these ARP entries, a further transfer of the packets was not possible. As an alteration of the corresponding parameters, for example to a period of ten minutes, would be very complicated on the firewall, so we solved the problem with static ARP entries.

Cisco's Firewall did not quite pass the performance tests without problems either. In one case, the system had to be restated by the support, as no packets were being transported anymore. However, this remained a single case.

During the measurements with 3DES encryption, considerable differences between the two producers show up. Without the acceleration card, Cisco is considerably slower (11%) than Astaro (33%) at handling 512 Byte packets in uni-directional mode. In the bi-directional mode, the ratio is similar, with 5% for Cisco and 17% for Astaro.



Cisco PIX 515

However, running Cisco with the acceleration cards is a whole different scenario. Handling 512 Byte-long packets, PIX reaches 51% throughput in the uni-directional mode and 25% in the bi-directional mode. This means that hardware accelerators provide a 5 times performance improvement when handling 512 Byte-long packets. Due to the high processor capacity, the throughput values of Astaro, based purely on software encryption, are very good.

Regarding the latency-values, both machines produce results at the upper end of the performance scale. Although the load values, for which we measured the packet-transfer-times, lay equally close under the throughput values for both candidates, the results slightly show more of a deviation. Astaro shows the slightly better values, for example 0.2 to 0.3 ms without encryption and 1 to 5 ms with encryption. The differences are very large if Cisco's Firewall is used without the acceleration card. In this case the average packet-transfer-time for encrypted packets is at 17 ms. The additional hardware reduces this value to about 4 ms.

TCP-Session-Rate-Tests

The »TCP-Session-Rate-Tests« table shows the results for a measurement of handling 5000 requests in one second. The following values (from top to bottom) are presented in the table:

- Total amount of established connections
- Ratio of established connections to total amount of connections (in per cent)
- Average time needed to establish the connection

In order to test the maximum amount of active parallel connections, the previously employed test scenario had to be expanded, as both firewall appliances were capable of establishing considerably more connections than the machines tested so far. The additional test consisted of 200 simulated clients and connection-establishment rates between 500 and 2500 connections per second. Every client tried to establish 700 connections, which means a maximum of 140,000 possible parallel sessions. Cisco managed 103,000 connections, Astaro 65,000. Both these results lie considerably above the previously established maximum value of 6144 sessions. However, Cisco only managed the high amount of connections in test runs directly after booting the system. Nevertheless, in the following test runs, PIX was still able to hold 66,000 parallel connections.

Product	Performance and Session rate tests	Handling and service	Feature list	Overall result
	40 %	40 %	20 %	
Astaro/Pyramid	★★★★☆ (3,8)	★★★★☆ (4,3)	★★★☆☆(3,0)	★★★★☆ (3,8)
Cisco PIX 515	★★★★☆ (4,3)	★★★★★(4,5)	★★★☆☆(3,3)	★★★★☆ (4,2)

★=insufficient★★=sufficient ★★★=good★★★★=very good★★★★★= excellent

Evaluation of the entire system unit

Further tests regarding the behavior of TCP-performance showed that both firewalls produced better results when dealing with 200 simulated clients than with one simulated client. This effect was also observed with several other firewalls. The reason for this is the differing implementation of the hash algorithms. These make sure that dynamically accumulating data is efficiently sorted into fixed-sized memory areas. In our case these are connection data, i.e. IP address, TCP source and target address. The state of the TCP connection, or the sequence number of the packets. In tests with only one client, one algorithm that calculates this sorting according to, e.g. only the IP address of the client, leads to an inefficiently sorted amount of data, i.e. hash-table. In this case, the table of connection data would only consist of one hash-column. Further accessing of the connection data would require longer searching in the table, reducing the performance data.

In Astaro's case, these effects were clearly visible in test runs with only one simulated client. A fair amount of connections were lost when testing with only medium speed of connection establishment. This effect became especially apparent as the total amount of connections increased. At a total of 6144 connections, and 1000 connections per second, already 28 per cent of the connections failed. At least these values only marginally deteriorated when dealing with a larger amount of rules. Astaro was able to show considerably better performance values in tests with 200 simulated clients. No connections were lost in any of the tests. This also applies to tests with partially illegal connections.

The time required for establishing a connection is almost entirely independent of amount of simulated clients and the amount of rules. The separate test results hardly deviate from one another. Only when the firewall is losing connections, does the time required for establishing a connections increase.

In tests with one simulated client, Cisco nearly showed to no adverse effects related to the aforementioned hash issue. Only at such high connection rates as 10,000 connections per second, does the firewall begin to lose connections. And, as expected: the higher the total amount sessions, the higher the amount of connections lost. The ability of the PIX to perform well with only one simulated client also becomes apparent when you look at the connection times. The values are very stable and, in comparison to Astaro, relatively low. In tests with 200 simulated clients, Cisco was also able to produce very good results. Apart from some small exceptions – twice a loss of 0.1 per cent and once of 0.05 per cent – there were no losses in these test trials.

Cisco's translation table, that contains all the connection data, made a very positive impression on us. In the case of some of the tested firewalls, we were able to delete individual connections from this table with TCP reset packets that contained incorrect sequence numbers. This was not possible with PIX. Cisco thus complicates the so-called »Session Hi-jacking«, i.e. the hi-jacking of legal sessions which then serve as back doors into the protected system.

In this test, we opposed the Linux-based solution of the young German enterprise Astaro to the firewall appliance by Cisco, one of the market-leaders in the Internet working branch. Astaro shows, like the »Defendo« system by Linogate in the last test that appliances based on Linux score very good performance values. Although Astaro doesn't quite reach the performance of the PIX Firewall despite its outstanding stability, the Linux appliances are somewhat cheaper. Astaro's software is even available as a test version, free of charge for private use. Those looking to buy the most performance on a tight budget are on the right track with Astaro's firewall appliance.
In order to also keep up with high-performance Linux solutions when dealing with encrypted transfer via VPN connections, or even to out-perform them, Cisco sent us both its firewalls with acceleration cards for the encryption. The through-put values achieved with these cards are impressive. However, they have their price. For the evaluation of the performance, we used the test values achieved without the accelerations cards as a basis, so as to ensure the comparability of the test candidates.

Comment by Bernd Klusmann

Conclusion

Both machines rank very high in the benchmark test. Cisco is ahead by a nose, because of the performance values. The difference is not so much due to the performance of the packet filter, i.e. in the IP performance measurements, as due to the TCP tests. Here Astaro's lost sessions, when dealing with one simulated client, influence the evaluation negatively. Without these losses, both candidates would score roughly the same values for performance. Regarding the evaluation of the feature list, Astaro also fell slightly behind. This was due to the fact that some of the requested features were not yet available; the failover mode and access limitation on definable URLs, for example are planned for future versions.

Function Feature	
Configuration via web browser without additional software	Yes (Browser-based graphic tool »PIX Device Manager«)
Backup of the configuration data on the Firewall or PC	Yes
ISDN Interface	No
Ethernet as standard interfaces	Yes
TCP/IP support	Yes
Network Address Translation (NAT)	Yes
Support of Tri-homed firewalls	Yes
Port-forwarding from the Internet into the LAN	Yes
Intrusion Detection Mechanisms	Yes (via »Cisco Secure Intrusion Detection System)
Routing mode	Yes
IPSec-compatible	Yes
Remote administration access via modem/ISDN	Yes
Reset factory default	Yes (first the IP address must be set/determined via the console)
Console port for recovery	Yes
Evaluation standard functions	**4.0**
1 = insufficient, 2 = sufficient, 3 = good, 4 = very good, 5 = excellent	

Standard functions Cisco PIX 515

The handling of the machines and the support were very good for Cisco, as well as for Astaro. The discussion server and the extensive documentation on Astaro's website have already been mentioned. The telephone support that we made use of to change the configurations files under Linux, was able to help every time and in every case.

The handling of Cisco's PIX-Firewall was very easy; both in the browser controlled administration tool and in the command-line. Especially the command-line, in combination with fixed/set configuration files tailored for the test scenarios, did not permit any false configuration. The PIX-Firewall was the first test candidate for which we needed no further support after completing the base-installation with the producer. We were able to carry out all test scenarios without having to fall back on further help.

About the author:

Bernd Klusmann
studied Electro Technology at the University of Berlin and is currently a project manager for the EANTC.

Article published in NetWorkWorld 20-01 – 26.10.2001, Germany
(http://www.networkworld.de)

Original article was in German. This is the translated version.