This Linux on a stick protects Windows computers

LITTLE SHIELD

This Linux computer on a USB stick acts as a tiny mobile firewall.

BY JÖRG FRITSCH

A hardware-based firewall solution offers several advantages over a simple personal firewall application. In theory, a hardware firewall can prevent dangerous packets from even reaching the system it is protecting, keeping threats safely at arm's length. An outside firewall device also assumes the performance cost of protecting the system, using its own CPU cycles for packet filtering so the user system is free for user tasks.

Hardware-based firewalls are extremely common on corporate networks, but when a user takes to the road with a laptop, the situation is not so clear. Hotels and coffee house hotspots often have their own firewalls, but the user typically has no knowledge or control of the security configuration. In the past, the only option for a uniform security configuration was a personal firewall. Now, a company called Yoggie Security Systems [1] is trying to change that. Yoggie packs a complete Linux-based firewall appliance – complete with a 520MHz CPU, 128MB RAM, and 135MB Flash memory – on a compact USB stick (Figure 1). This firewall on a stick, which is known as the Yoggie Gatekeeper Pico, is available in Personal and Pro Editions for corporate use, as well as in a basic Firestick Pico version for home users. Prices range from US$ 120 to 200.

The Gatekeeper Pico is designed as a Unified Threat Management (UTM) device, which means that it integrates several security tools. According to the product description, the tool comes with 13 security applications. The open source components [2] include iptables/Netfilter as a stateful firewall, the http antivirus proxy HAVP, an SMTP proxy, and a number of others. On top of these open source tools are a number of commercial applications: Snort with Sourcefire VRT rules as an IDS/IPS; the Kaspersky engine, which checks for viruses and spyware; Mailshell, which identifies and tags spam and phishing; and the SurfControl web content filter.

Although the Pico family [3] runs on Linux, the firesticks are designed to protect Windows XP and Vista systems, with the emphasis on notebooks. We

Table 1: Yoggie Gatekeeper Pico

Device type:	USB stick with embedded PC as a firewall appliance
Vendor:	Yoggie Security Systems
Tested Version:	Yoggie Gatekeeper Pico, Software 1.3.9
Yoggie operating system:	Linux with kernel 2.6.16.16, P3Scan 2.3.2, Open Swan 2.4.6rc5, Ifplugd 0.28 and Netfilter 1.3.5, modified Snort 2.4.4, and HAVP 0.86 [2]. Also includes commercial modules such as Kaspersky AV, Mailshell, and SurfControl
Host operating system:	Pico Gatekeeper only works with Windows XP and Vista because it requires proprietary drivers

Figure 1: The Yoggie Gatekeeper Pico is a complete firewall appliance on a USB stick.

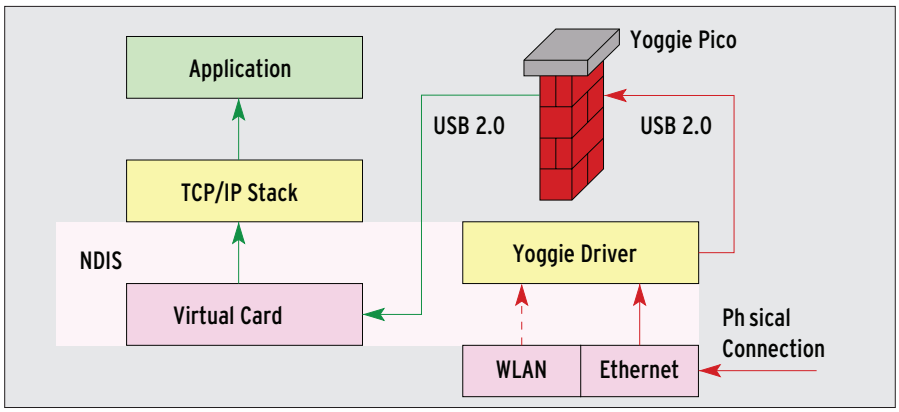

Figure 2: The network adapter in the PC has an the external IP address 172.16.1.3. The driver uses USB to forward data to the stick. Yoggie works as a NAT gateway and uses the PC's internal address, 192.168.10.200, to talk to the PC.

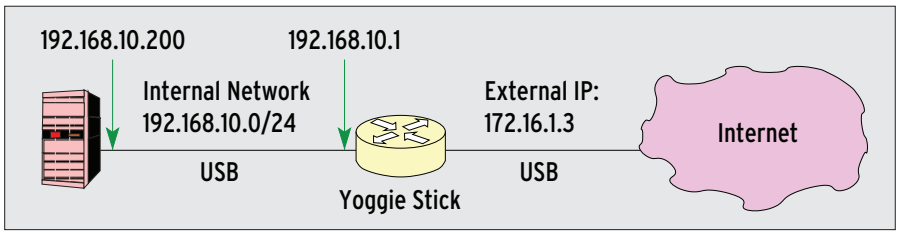

Figure 3: The topology of a micro-network. The network adapter in the PC has an the external IP address 172.16.1.3. The driver uses USB to forward data to the stick. Yoggie works as a NAT gateway and uses the PC's internal address, 192.168.10.200, to talk to the PC.

had three Gatekeeper Picos to experiment with, so we decided to see how well this gatekeeper kept watch.

How It Works

A Pico device does not have a separate network adapter. A driver running on the host system intercepts incoming network packets and sends them to the Gatekeeper stick. The Yoggie driver inhabits the NDIS (Network Driver Interface Specification) layer [4] between Windows' TCP/IP protocol stack and the local network adapter (Figure 2). Yoggie offers drivers for XP and Vista systems.

The Gatekeeper device filters the incoming data, and only packets that pass the filtering rules are forwarded back to Windows. The big advantage of this approach is that the Gatekeeper device is independent of the network architecture. If the necessary driver is up and running, the Gatekeeper Pico can handle traffic from any kind of network connection: Ethernet, WLAN, or even infrared.

A virtual network adapter is assigned to the host system with a separate IP address and subnet mask to receive data forwarded from the Gatekeeper system. The firestick thus acts like a real router, forwarding authorized packets to the virtual adapter address for processing by the host. In addition to its security tasks, the Yoggie appliance also attends to other routing-related tasks such as NAT (Network Address Translation). The path from Windows to the network is again via the Gatekeeper device. The virtual interface sends outgoing data to the USB stick, which filters the network traffic and sends it through the Windows driver to the physical network adapter (Figure 3).

After installation, a Yoggie icon in the task bar confirms that the system is ready for use. Because Yoggie is a separate computer, it has to boot. This happens when you plug the device into the USB port and takes about 30 seconds. Three LEDs show when the stick is done booting. It then updates its software, engines, and patterns (antivirus, antispam) with an SSL tunnel to the Yoggie update server.

Although Yoggie fulfills its obligations as a packet filter, the user interface, which is accessible in a browser (Figure 4), hides the underlying iptables filter rules from the user. This filtering information might be confusing to non-experts, and it makes sense to hide it by default, but the rules should be accessible to experts who need to make sure the firewall implements their policies correctly.

Locked Out

Despite all restrictions that the configuration interface puts in place, the tester succeeded in deliberately misconfiguring the device so badly that it refused any access. One stick had failed before, so I only had one fully functional device left to experiment with. The incorrect configuration was caused by a tester entering an address of 195.169.118.0 with a netmask of 255.255.255.0 as the internal Yoggie network. Unfortunately, this is not a private address block, and the Yoggie GUI automatically corrected the setting to 192.168.118.0/24. The stick booted in the normal way and worked fine for the most part, but I was unable to access the administration GUI.

The web filter in the gatekeeper appliance is based on SurfControl. The software implements an enterprise web policy. If a user inadvertently or deliberately attempts to access prohibited web con-

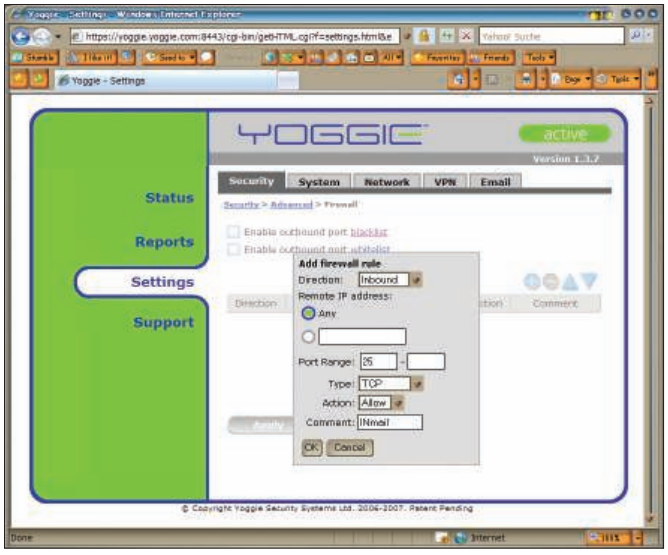

Figure 4: The firewall settings are easily completed in the Yoggie stick's web interface. Unfortunately, the stick does not tell you anything about the underlying iptables commands.

tent, the filter displays a warning instead of the web page. The current version does not let you change the error message. It might make more sense for companies to be able to modify this to display a message with the mail addresses and phone numbers of the IT department before distributing Yoggie sticks to their field staff. After all, if the web filter denies access to a legitimate site, the user is definitely going to need help.

The SurfControl mobile filter can compete with the Websense remote client, which is more established in the enterprise market. Unfortunately, Websense acquired SurfControl in January 2008 and immediately discontinued the SurfControl web filter but promises to maintain the URL database until December 2011 for existing customers [5].

Gatekeeper does not protect against malware entering through an encrypted connection (i.e., https). Interestingly, Yoggie supplies a one-year license of the Kaspersky antivirus scanner with each Gatekeeper. This scanner runs directly on the laptop, thus providing a second line of defense against viruses entering via https.

Figure 5: Hidden away in a logfile was the only indication why email traffic failed to reach a legitimate mail server that used port 2525.

Advertising with the Pentagon

Yoggie's marketing people advertise a "layer 8 engine" designed to protect customers against previously unknown zero-day attacks. The company claims to have a patent pending on the technology, but the name is confusing because the OSI reference model only has seven layers. The Yoggie box promises "Pentagon-level protection in the palm of your hand." When asked, the company, based in Israel, admitted that it had nothing to do with the Pentagon and that the sen-

Hole in the Firewall

In our lab, author Jörg Fritsch discovered a major vulnerability in the Yoggie Gatekeeper Pico, Version 1.3.8, that allows attackers to work around the firewall and to directly attack the target system. This attack requires that the attacker be on the same subnet as the target system's physical interface. This is the case not only on an enterprise LAN, for example, but also on an Ethernet network at a hotel or with a WLAN hotspot at the airport. Of course, these are exactly the kind of hostile environments for which Yoggie is designed to protect users. The proof-of-concept attack involves four steps:

Step 1: A Nessus scan of the Yoggie-protected system would seem to indicate that the IP address belonging to the physical interface is perfectly protected – the system does not react to any kind of packets sent to it. Surprisingly, a UDP traceroute reveals the internal IP address belonging to the Yoggie stick; that is, the address the stick uses to communicate with the host system.

Step 2: Initially it is impossible to scan the internal address because its subnet is unknown and not routed. Our test team chose a suitable group 16 subnet mask that would work in any case and set up a route to the subnet on the attacking machine. The physical interface of the protected system was used as the gateway address.

Step 3: An Nmap scan of the new routed group 16 subnet revealed two addresses: the Yoggie firewall appliance's internal address and that of the new virtual host adapter.

Step 4: A final Nessus scan of both IP addresses revealed the vulnerability: The host state is visible to Nessus as if Yoggie was not in place. Nothing is there to stop an attacker from exploiting vulnerabilities on the host system.

The author immediately disclosed the vulnerability to Yoggie (on the night of March 16/17, 2008), and the manufacturer developed an update to version 1.3.9 within 36 hours to remove the security hole. The response time was fast, but the vendor's information policy not exemplary. The company responded negatively to various inquiries as to when Yoggie would be releasing an advisory on the vulnerability, stating that Yoggie automatically installs updates and this was far more than a classical advisory could ever hope to achieve. The only reference to the security disaster is in a history file on the firmware [8]:

```
1.3.9 (18 March 2008)
---------------------
Fixed:
------
Issue #1008: Critical security
update; device hardening
including network interfaces
and improved Firewall
stealth mode
```

This is not a convincing argument. If a stick does not have an online connection, the system is still vulnerable; and even if a connection exists, there is still a race condition that leaves the host vulnerable. Because the attacker has to be on the LAN, situations in which the system would be vulnerable to attacks while the gatekeeper was installing an update are conceivable. Corporate mode also allows the administrator to say which updates are installed on sticks. The terse comment quoted above makes it impossible for users to realize the full potential of the threat. Yoggie still had not revealed the bug two months after the event.

At first, Yoggie failed to give a full explanation of the vulnerability, but then they confirmed our suspicions. Basically, the gatekeeper acts as a NAT router, like any normal Linux firewall, the only exception being the connection to the Windows system. This means that all precautions that apply to the firewall configuration apply here, too. The Yoggie stick created netfilter rules, but without specifying interfaces: the *-i* and *-o* parameters thus only applied to the IP addresses.

The proof-of-concept attack sent packets directly targeted at the internal address to the external interface. The Linux kernel's internal routing algorithms correctly forwarded the packets without a firewall rule intervening.

Real world system administration training

LISA'08

22ND LARGE INSTALLATION SYSTEM ADMINISTRATION CONFERENCE

San Diego
CALIFORNIA

November 9–14, 2008

6 DAYS OF TRAINING BY INDUSTRY EXPERTS, INCLUDING:

- Mark Burgess on Integrating Cfengine into Organizational Service Management
- Tom Christiansen on Advanced Perl
- David N. Blank-Edelman on Over the Edge System Administration
- Rik Farrow on Working with SELinux
- Tobias Oetiker on RRDtool by Example

NEW! TRAINING TRACKS ON SOLARIS AND VIRTUALIZATION

This 2-track, 6-day series includes classes such as:

- Peter Baer Galvin on Solaris 10 Administration
- Jim Mauro on Solaris Dynamic Tracing (DTrace)
- Æleen Frisch and Kyrre Begnum on Virtualization: VMs! What Are They Good For?
- Richard McDougall on VMware ESX Performance and Tuning

3-DAY TECHNICAL PROGRAM

- 2 tracks of invited talks including: Keynote on Intellipedia by Don Burke and Sean Dennehy, *U.S. Central Intelligence Agency,* and Plenaries by Bruce Schneier and David Wagner
- Workshops, refereed papers, Guru Is In sessions, Birds-of-a-Feather sessions, Work-in-Progress reports, and more!
- Vendor Exhibition: A showcase of the latest commercial innovations

Can't make it to San Diego?
View the invited talks streamed live, powered by *Linux Pro Magazine*.
Find out more at http://www.linuxpromagazine.com/lisa08

SPONSORED BY
USENIX & [sage]

Register by October 17 and save! www.usenix.org/lisa08/lpa

tence was simply intended to emphasize the product's revolutionary nature.

Before a product is deployed in the Pentagon, it has to pass various tests and achieve various certifications (i.e., Common Criteria, EAL, FIPS). The Yoggie Gatekeeper Pico does not have these certifications. Also, the Pentagon requires that certain IT security products be produced in the USA, whereas Yoggie is made in China. The ambitious Pentagon statement is misleading, but beyond the PR bravado, Yoggie does at least provide solid security technology and good spam and phishing detection. By default, the Gatekeeper marks the subject line in unsolicited, incoming mail with *[SPAM]*, *[POSSIBLY SPAM]*, or *[PHISHING]* tags. Yoggie relies on the Mailshell engine [6] and the open source SMTP proxy, ProxSMTP, for filtering mail.

Spam and Phishing

The anti-phishing function returned useful results in our lab. To investigate the antispam function, testers set up a number of email accounts and mirrored them to a [*spamcop.net*] mailbox. Yoggie's results were better than those provided by the Spamcop service, with a spam detection rate of just below 100 percent. However, Yoggie returned one to two percent false positives (i.e., legitimate email incorrectly identified as spam) when mailing lists were used. The spam filter is fine for corporate use in small- to medium-sized enterprises, but it is not a genuine alternative in the enterprise sector. To compare, Cisco Ironport [7] only returned one false positive in 109 million messages in an extensive test.

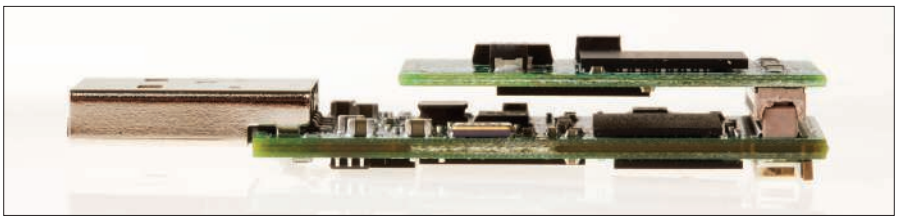

Figure 6: The interior of the Yoggie Gatekeeper Pico comprises two small PCBs that together form a complete mini PC.

IDS and IPS

Yoggie's intrusion detection (and prevention) system is Snort with Sourcefire rules. This combo forms a top-notch team from a technology point of view, but as with the web filter, administrators have no way of modifying the software to reflect their requirements. In our lab, with a default setting of *Medium Security*, we could not send mail via the server over TCP port 2525, and we got no message telling us that Yoggie IPS had blocked the outgoing connection. Other personal firewalls at least pop up a window to warn you of such actions.

After searching, the testers found a message in the Yoggie logfiles: *Suspicious 220 Banner on Local Port Detection of a nonstandard protocol or event* (Figure 5). All they could do was disable the IPS for all mail traffic. It was impossible to disable just one signature because it triggered a false positive response.

Configurability of security systems is a matter of opinion. Yoggie seems to be targeted at inexperienced users. Asking this target group to take care of complex details would be too much, and the artificial restrictions are justifiable in this light. However, some users, such as field staff or home workers, could benefit from the enhanced security of a compact appliance compared with a software-only solution. Yoggie cultivates this market with a VPN function and corporate mode that lets a company preconfigure and manage hundreds or thousands of Yoggie Pico Pro Gatekeepers via the Yoggie Management Server (YMS), which was not ready in time for this test.

Amazing Device

The Yoggie Gatekeeper Pico surprised the test team in two respects: In a positive sense, we were impressed with its design and the quality of the tiny hardware package. In a negative sense, we were surprised that we could open such a large hole in the system. No software is perfect, but being able to work around the firewall in a security product raises some serious questions about the device.

Apart from its deficiencies, the mini-appliance left a generally positive impression. UTM appliances tend to be bulky – rack mountable at best. The market is currently moving toward integration. Standalone security solutions are being acquired, dissected, and integrated with larger product series. Contrary to this trend, Yoggie has now introduced a new standalone security solution that provides better protection than a legacy personal firewall, but users do need to carry additional hardware around with them on the road, and hardware can be lost or broken. Potential customers will have to decide whether to trust the product despite the vulnerabilities, which have since been fixed. ■

Yoggie Autopsy

That one of the three test devices gave up the ghost just 20 minutes after we plugged it in for the first time, might be a coincidence, but it at least gave us a good excuse to dissect the device in our lab. Opening the Gatekeeper Pico revealed two dual-sided PCBs (still connected in Figure 6) with a 520MHz CPU by Intel (XScale PXA270), 128MB SDRAM, and 135MB Flash memory (128MB NAND plus 8MB NOR).This is the CPU that is used in some Blackberry models. It has been on the market for about three years now, but it is still state-of-art.

The Gatekeeper Pico's hardware and architecture are convincing, and you can't say the price is overly expensive. It is surprising, in fact, that Yoggie has managed to offer the hardware at such a low price. Of course, the product would be more interesting as an open Linux appliance that users could install and configure to suit their own needs. A more open design would give users the ability to, say, integrate a mini–web server, groupware system, or CVS server that would run off any host computer.

INFO

[1] Yoggie: *http://www.yoggie.com*

[2] Open Source components in Yoggie: *http://www.yoggie.com/opensource*

[3] Yoggie product line: *http://www.yoggie.com/comparison.shtml*

[4] NDIS Developer's Reference: *http://www.ndis.com*

[5] SurfControl: *http://www.websense.com/acquisition/surfcontrolCustomers.html*

[6] Mailshell: *http://www.mailshell.com*

[7] Ironport: *http://www.ironport.com*

[8] Firmware history: *http://www.yoggie.com/PDF/Firmware-Version-History.txt*