

AlphaShield

A Giant Step in Network Security

Product Review

What's the best way to protect a PC from malicious Internet attacks?

Two years ago I attended a network security seminar presented by one of North America's most respected security organizations. Throughout the seminar we learned many techniques used by crackers to circumvent Firewalls, Webservers, E-Mail Servers, and other network related devices. Toward the end of the seminar, the lead instructor took the stage and asked, "After all you've learned, what would you recommend as the safest way to protect a network of PC workstations?"

Although several people came up with brilliant answers, nobody had the answer he was looking for.

Firewalls Aren't Enough

Sure, firewalls are a super layer of protection, but you can't stop there.

Firewalls leave your PC connected through active "IP based components". Whether the device is in use or standby mode, it remains in an active state, and therefore could allow for circumvention.

Hence, the only real answer for full protection is to disconnect the PCs.

In reality, we all know disconnection isn't a practical solution. What if there was a device that would allow us to connect only when needed, and disconnect seconds later?

A new device on the market named AlphaShield does just that, and takes network security one step further.

Out of the Box

Out of the box, Alphashield looks something like a small workgroup hub with 3 ports. One port connects to the WAN, the other to the PC, while a third port acts as a bypass. On the back of the device is a switch that configures the device for Auto mode, 15-minute timeout, or lock mode.

The difference between the modes:

Auto mode allows for a continuous connection with an optional logical disconnect.

Manual mode allows a straight logical disconnect after 15 mins.

Lockout mode allows for a timed connection, with a "physical" disconnect.

In lockout mode, you need to manually re-establish the connection by pressing the "connect" button located on top of the device.

Indicators

The device has three indicators on the front panel:

PC (LAN) Status

Switch Status

WAN Status

Each indicator displays green for connected, and red for disconnected.

Power supply

The device is powered by a small 9 volt DC power supply that plugs into the wall.

Controls

The Alphashield has two main controls located on top of the unit. They are simply “on” / “off” controls that allow the user to logically connect or disconnect the device.

Security Testing

I tested the unit for several vulnerabilities while comparing it to other security devices such as NAT gateways, routers and firewalls. I was impressed to find the Alphashield does ****not**** allow for remote administration or firmware upgrades. Insecure protocols such as SNMP and FTP have also been disabled. This prevents the possibility of remote ***Hacker Exploits*** that would alter the operation of the unit. I ran eight separate security tests against the unit, including several attempts to crash it using oversized UDP packets. The unit stood up to each test, while maintaining complete stability.

Overall, I’m impressed with Alphashield, and will continue to use it as an addition to my firewall.

*Glenn Graham has been working with telecommunications since 1977 when, at age 15, he wrote and passed **The Certificate of Proficiency in Radio** granted by the Government of Canada. He has more than 15 years of experience with Unix-based operating systems. In 1994 he established inTEXT Communications, an international Unix consulting company. Glenn now works full time with his company, providing Unix administrative services worldwide. You can usually find him wide awake at <http://www.intextonline.com>.*