

# Network Security



Many small business owners know how dependent they've become on their computer systems.

Files stored on your network are shared by various people in your office. Your email may be stored on your network server. Your accounting information for invoicing, accounts payable and payroll may also be stored on your network.

What if you couldn't get to this information?

For a day?

For a few days?

Maybe for a week?

What affect would that have on your business?

What if your systems were compromised and added to some hacker's botnet? (a botnet is a network of remotely controlled "robot" systems usually used for illegal purposes)

Network security is just as critically important as email and web security.

How does The BOX protect your network?

There are four main areas:

- Deep packet inspection firewall
- Logging and monitoring
- Intrusion detection/prevention
- Hardened rules
- Regularly scheduled vulnerability scans

Let me explain each one.

## **DEEP PACKET INSPECTION FIREWALL**

A little lesson first.

Typical firewalls use source and destination to determine what goes out of your network and what comes in.

Every time someone in your office connects to a web site, two-way communication occurs. They request a web page and the web server responds with the page.

The source of this requested communication is your network. The destination is the web server. When the web server responds, it becomes the source and your network becomes the destination.

When you send an email, your network, or your email server specifically, is the source and the recipient's email server is the destination. When they reply, their email server is the source and your email server is the destination.

If your email server and your web server are one and the same, how does it know when to receive email and when to respond with a web page?

Welcome to ports. In addition to source and destination address, Internet communication also uses ports. When you request a web page, you're the source address and the web server is the destination address and port. Web servers "listen" on port 80 for any requests for web pages. Email servers "listen" on port 25 for any email sent.

Why is this important for you to know?

Because in your firewall most traffic is blocked or allowed by port number. If you want to block email from exiting your network you would block destination port 25.

Other Internet communication uses different ports.

For instance, it's widely known that hackers typically use Internet Relay Chat (IRC) for controlling their botnets. IRC by default uses destination port 6667. Many firewalls are confident that blocking destination port 6667 negates the ability of the hacker to communicate with their bots via IRC.

However, hackers are smarter than that. They know everyone wants to "surf" the Internet so port 80 must be open. They program their IRC bots to go out of your network via port 80. Their destination server is configured to listen for IRC traffic on port 80.

They can control their bots inside your firewall without any problem. The real problem is that you think you're safe!

The BOX goes deeper. The BOX looks at the traffic deep inside and determines whether or not it should be allowed or denied. The BOX positively identifies the traffic as legitimate or illegitimate.

This takes extra processing power and extra configuration – but we feel it's worth it. And we think you'll agree.

Even if one of your PCs is part of a botnet, it doesn't matter. We'll catch the outgoing traffic, block it and display a screen on the infected system that alerts the user to the infection – and we get a notice as well. We'll know about the same time you do.

One of our technicians then works with you, or someone you designate, over the phone to try and clean your system.

But you don't have to worry about one of your systems being controlled by people with malicious intent.

The BOX also only allows email out of your network that originates from your email server – your email server must be the source. If one of your systems is compromised, it cannot be used to send SPAM! Only email with the source address of your email server is allowed out. Everything else is blocked, logged and reported to us. We'll then work with you to clean that system.

Our philosophy is "Block everything other than that which is absolutely necessary."

## **Logging and monitoring**

The BOX logs everything. Everything coming in and going out of your network gets logged.

Who monitors those logs?

We do.

One of the biggest problems with firewalls and network security in general is “who has the time, let alone the knowledge, to read and analyze all the logs”.

We’re constantly watching for alerts in your traffic. We’ll know when an attack is occurring or when one of your systems has been compromised before you do.

As new attacks are detected on one BOX, if necessary we’ll make modifications to the rules to assist in blocking it. We then “push” that change out to all the other BOXes.

This makes your BOX part of a huge network of “sensor” stations.

## **Intrusion detection/prevention**

Intrusion detection systems (IDS) have been quite popular on the security sites in the past few years. They are typically used only in larger organizations because of the amount of information they spew. This requires someone to monitor them full time, analyze the output, determine what is a false positive and what is legitimate then decide the correct course of action.

An intrusion prevention system (IPS) is an IDS taken one step further. IPS rules state that if a positively identified attack is detected, the rules are automatically modified to take a specific action to prevent the attack from being successful.

The logs on IDS/IPS are constantly monitored. The rules are updated frequently to block new threats.

The BOX uses IDS/IPS for outgoing as well as incoming traffic. This enables us to determine if one of your systems has been compromised – immediately.

## **Hardened rules**

Our motto is “You’re either hardened, or you’re hacked?”

The BOX has hardened rules throughout every section. As stated earlier, The BOX only lets out and only lets in what is absolutely necessary. Everything else is logged, blocked and reported.

## **Regularly scheduled vulnerability scans**

Your BOX is delivered to you with a very powerful vulnerability scanner built in. We schedule monthly scans of your systems with updated rules to verify everything is safe.

We carefully select the tests to perform that meet your specific environment. No need to test for Oracle vulnerabilities if you don’t use any Oracle applications.

Each month you can view the results of these scans on your Web Reporter. You’ll see what was tested and the results. Obviously if we find anything, we’ll alert you right away so we can discuss steps necessary to close up the opening. All of this is covered in the normal maintenance.

The BOX – designed specifically for small business owners.

Visit: <http://www.ebasedsecurity.com> to learn more. Or call, 1-866-838-6108