

# 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. You probably have all of your customer contact information stored on your server too.

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:

- Firewall
- Logging and monitoring
- Intrusion detection/prevention
- Hardened rules
- Regularly scheduled vulnerability scans

## **FIREWALL**

A firewall is something you most definitely already have at your business.

However, when was the last time you or somebody else reviewed the logs? If you're like most, small businesses, they've never been reviewed. Or maybe they were when it was first installed.

Another problem with your current firewall is that it probably only logs blocked traffic. If that's the situation, how do you know when something malicious has passed through?

You don't.

When was the last time the rules were modified?

Do you think the protection your firewall was originally configured for is still current? Many of our clients firewall rules are modified every week, that's how often new attacks are uncovered.

The BOX looks deep inside the data being transferred into and out of your network. By doing this we're able to positively identify malicious traffic.

A typical scenario when a new client connects their BOX to their network is that we're notified of pre-existing malicious traffic. This is a clear indication that one of their systems is infected and has been sending malicious traffic through their existing security "defense".

Our staff will work with you or with someone you designate, to clean the system. We then scan the network again to determine a safe level of security.

Clients are quite surprised that the malicious traffic was never identified by their previous firewall. However, we know, most firewalls don't look deep enough inside the data to positively identify it as malicious. The technology used for this deep inspection is more complicated and would require constant monitoring. We know small businesses can't dedicate the resources necessary to constantly monitor security logs, which is why we do that for you.

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 in the security industry in the past few years. They are typically used only in larger organizations because of the amount of information they record. This requires someone to monitor them full time, analyze the output, determine what's 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.

If someone comes into your business with laptop and they connect to your network, how do you know their system isn't infected?

You don't.

We'll know. As soon as they connect their system will be blocked if they're infected. Then we'll get a notification alert and we'll contact you to let you know. More than likely the person with the laptop doesn't even know they're infected.

## **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 all the recent vulnerabilities to verify everything is safe.

We carefully select only 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. We'll take care of your system security so you can get back to running your business.

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