Choosing an IPS White Paper NETGLADIATOR

The APconnections technical staff put together this list of seven (7) things to look for when choosing an intrusion detection & prevention system (IPS). This is intended to be product-agnostic, and so is a good primer when you are starting your research on the IPS space. Whether you decide to look at our product or not, we believe this list will be valuable to you. In February 2012 we released NetGladiator, an IPS appliance that automatically detects and prevents a network hacker from breaking into your web applications.

#1 - Don't degrade your network speed

Make sure your IPS system is not going to slow down your network. If you have a T1 or smaller sized network, chances are just about any tool you choose will not slow down your connection; however with links approaching 10 megabits and higher, it is worth investing in a tool whose throughput speeds can be quantified. Higher network speeds generally will require a tool specifically designed and tested as an IPS device and rated for your link speed. Problems can arise if you buy a software add-on module for your web server.

A stand-alone physical device specifically designed to prevent intrusion is likely your best option. A good IPS system is very CPU intensive, and lower-end routers, switches, and heavily utilized web servers generally do not have the extra CPU cycles to support an IPS system. For example, IT managers are aware that large web server sites must use multiple servers to handle large volumes of HTTPS pages, which are also CPU intensive. The same metrics will apply to an IPS system on a smaller scale, so make sure you are not underpowered.

#2 - Watch out for high license fees

Try to get a tool with a one-time cost and a small licensing fee. Many vendors sell their equipment below cost with the hopes of getting a monthly fee on per seat license. Yes, you should expect to pay a yearly support fee, but it should be a small fraction of the tool's original cost.

#3 - More features is not necessarily better when it comes stopping intrusion from hackers

You may not realize that large, robust "all-in-one" IPS solutions can be rendered useless by alerting you thousands of times a day, as you will ignore their alerts at that volume. They can also block legitimate requests ("false positives"), and can break web functionality.

You should consider solutions that are not as fully-featured but are targeted to your security concerns, so that you receive meaningful alerts on real potential intrusion attempts. More features can just introduce clutter, where you are not able to sift through your alerts to find what you really care about. Also, doing everything can dilute the mission of the toolset, so instead of doing one thing well, it does everything poorly.

Remember, the biggest threat to your enterprise is a person that breaks into your internal systems and attains access to your customer data. A typical PC virus or Denial of Service (DoS) attack does not pose this type of threat. Although it may be counter-intuitive to your experience, *it is a good idea to make sure you have a solid intrusion detection system before investing in things like virus prevention, web-filters and reporting*. Yes, viruses are a pain and can bring down systems, but the damage will likely not compare in real cost to a hacker that steals your customer records.

Intrusion Prevention System (IPS) Selection

Key Points

1) *Don't degrade your network speed.*
2) *Watch out for high license fees.*
3) *More features is not necessarily better when it comes to stopping intrusions from hackers.*
4) *Block first, ask questions later.*
5) *Don't rely on manpower for detection.*
6) *Use a white knight.*
7) *Use a combination of techniques.*

#4 - Block first ask questions later

An intruder usually behaves oddly when compared to a normal visitor. Your intrusion detection device should block first and ask questions later. *It is better to accidentally block a small number of friendlies than to let one hacker into your network*. You will get feedback if legitimate visitors are locked out from your website, and it won't take long to hear from them if your intrusion device is accidentally blocking a friendly visitor.

#5 - Don't rely on manpower for detection

Let your intrusion detection device do the work. If you are relying on a reporting system and a human to make a final decision on what to block, you will get hacked. Your device must be automated and on the job 24/7. There is nothing wrong with an analyst doing the follow-up.

#6 - Use a white knight

Hire a white knight to expose your security risks. There was an article in the Wall Street Journal (January 23rd, 2012) on how anybody can hire a professional hacker. What they failed to mention is that you can also hire a white knight to test your armor and let you know if you have any weaknesses. Most weaknesses are common back doors in web servers that can easily be remedied once exposed by a white knight.

#7 - Use a combination of techniques

The only way to 100 percent secure your enterprise is to block all outside access, and with the silo mentality of a some security zealots you could end up with this solution if you are not careful. Given the reality that you must have a public portal for your customers, the next best thing to locking them out is a combination of white knight testing, plugging holes in web servers and entry points, and a permanent watch dog intrusion prevention system – this should keep you safe from a hacker.

Conclusion

We share our findings here based on what we have gleaned from our research in the IPS space. Hopefully, these points to consider will help you on your journey researching intrusion prevention systems (IPS).

Some good intrusion prevention links:

Checkpoint
Lanner
NetGladiator
Radware
SOURCEFire

About APconnections, Inc.

APconnections is an innovation-driven technology company that delivers best-in-class network traffic management solutions to give our customers better networks, with zero maintenance, at the best prices. We specialize in turn-key bandwidth shaping and intrusion prevention system (IPS) appliances.

Since 2003, APconnections' mission has been to provide simple turn-key network optimization appliances to any network topology. Our products are simple to install, easy to use, require little maintenance, and offered at the best prices.

APconnections is based in Lafayette, Colorado, USA. We released our first commercial offering in July 2003, and since then thousands of customers all over the world have put our products into service. Today, our flexible and scalable solutions can be found in many types of public and private organizations of all sizes across the globe, including: Fortune 500 companies, major universities, K-12 schools, and Internet Providers on six (6) continents.

To Learn More…

If you would like to learn more about our intrustion prevention solution, NetGladiator, give us a call at **303.997.1300 x123** or email us at ips@apconnections.net.

We would be a happy to provide a detailed walkthrough of the NetGladiator technology, to help you determine if this is the right solution for you.