Executive White Paper

Securing your web applications from unintended intrusions has become more important as the Internet has become a critical resource for conducting business in both the B2B and B2C spaces. Web application hackers attempt to disrupt your business in a variety of ways, and if successful, can have a significant impact on your business' image, as well as your bottom line. NetGladiator technology will help you to secure your Internet pipe by simply, cleanly, and affordably preventing web application intrusions. This solution briefing is intended to get you up-to-speed on the NetGladiator technology, what it can do for you, & why you might want to consider it for your environment.

NetGladiators are 1U rack-mountable units,securing Internet pipes up to 250Mbps bi-directionally. See our Data Sheet for detailed specifications.

What is a NetGladiator?

The NetGladiator IPS (www.netgladiator.net) both detects and prevents web application intrusions. NetGladiator IPS is a simple, elegant, turn-key appliance, utilizing our proprietary "gladiator" technology to keep your network secure from hackers and ensuring bandwidth availability for your legitimate network users.

Our greatest advantage relative to other IPS devices is that we do not issue false positives or provide thousands of distracting alerts throughout the day. Nor do we block legitimate requests or break web functionality. We do one thing very well - ***we catch & stop hackers during their information discovery process*** - keeping your web applications secure. NetGladiator is custom-configured for your environment, alerting you on meaningful attempts without false positive alerts.

Our unique, heuristics-based IPS system uses deep packet inspection (DPI) technology to monitor incoming requests, looking for abnormalities in traffic patterns, which represent potential intrusion attempts. When an abnormaity is detected, we secure your network by both blocking the intrusion and notifying your network administrators.

NetGladiator automatically secures your network; no manual intervention is needed to thwart attacks. Our automated response enables your network administrators to focus on further analyzing the intrusion attempt, and fixing any possible entry breach points in your network, without also having to deal with an attack in progress.

Core Capabilities	
Intrusion Detection	Customized configuration to define patterns for your environment. 1) Time-sensitive anomalies 2) Traffic anomalies.
Intrusion Alerting	Notifications are emailed with assigned severity. 1) Level 1 (suspicious) 2) Level 2 (hack)
Intrusion Prevention	Anomalies are logged and blocked, stopping hackers during their information discovery process. 1) Level 1 logs the activity 2) Level 2 logs & blocks the activity
Prevents these types of network breaches	Administrative interface login brute forcing Denial of Service (DoS) attacks Directory Traversal Login brute forcing Reflected HTTP redirects (OWASP Top 10) Reflected cross-site scripting (OWASP Top 10) Persistent cross-site scripting (OWASP Top 10) URL SQL injection (OWASP Top 10)
Logging	Logs all Level 1 and Level 2 activity.
Reporting	1) Blocked IPs 2) Suspicious IPs
Redundancy / Failover	1) Full Redundancy: Install secondary NetGladiator IPS in active:passive mode. Hot swappable via STP. 2) Failover: Install a third-party switch in STP mode (available from APconnections). 3) Failover: Use STP mode on your own switch.
Device Management	Web browser interface
Customized Configuration	NetGladiator IPS is installed between your firewall and your enterprise. Once your patterns are defined through our security assessment process, it is a quick and easy set-up process.

NetGladiator Core Capabilities

The NetGladiator offers these *Core Capabilities* (*see table above*) to secure your network against web application hackers. Two key capabilities are : 1) Intrusion Detection (IDS), which uses heuristics to find anomalies in behavior on your Internet pipe, and 2) Intrusion Prevention (IPS), which both logs and blocks suspicious IPs. We do all this while remaining easy-to-install, cost-effective, and low maintenance.

Copyright © 2012 APconnections, Inc.

All rights reserved

Why should I invest in a NetGladiator?

The NetGladiator is a key device in a layered security approach that should be considered if you are concerned about securing your Internet pipe. The NetGladiator is a stand-alone physical device specifically designed to detect & prevent web application intrusions, ***using a sophisticated parallel processing model to ensure zero latency*** while inspecting traffic - operating unobtrusively on your Internet pipe. We are the only product in our price range able to do this. NetGladiator's behavior-based anomaly detection identifies potential attackers, knowing that a hacker explores and utilizes your website much differently than a normal user. Because we can be confident in their malicious intent, we block their IP address immediately.

We custom-configure the NetGladiator IPS for your environment. Our ethical hackers look for security holes in your web applications and then configure targeted patterns to thwart hackers.

Art Reisman
Co-founder & CTO
AP Connections, Inc.

We also customize your configuration during set-up by having a white knight (ethical hacker) identify possible security holes in your web applications. The security holes are then used to configure the patterns you need to protect against with the NetGladiator IPS. This targeted approach ensures that you are getting meaningful alerts instead of thousands of unnecessary alerts (possibly false positives).

When developing an IT security policy and implementing various security controls, the single most important thing to consider is how the different controls you use will layer your security profile. Because no single piece of equipment or software will be able to thwart 100% of attacks, good layering provides the best chance to stop a hacker from his/her ultimate goal. Here is an example: Say you have four technologies that help secure your environment that are each 75% effective: 1) a web application firewall, 2) a hardware firewall, 3) anti-virus on your server, and 4) hashed passwords in your database. If you only had one of these implemented, an attacker would be successful 25% of the time. But with all of them layered together, each functioning to stop an attack, you lower the chances of an attack to 0.4% (.25x.25x.25x.25).

How does the NetGladiator work?

Every connection into your enterprise is logged. NetGladiator IPS then starts rating the security risk of the connection based on activity. As security risk behaviors are detected, it raises an internal counter of probability on the connection being hostile. At some point, the connection will cross over into the territory of abnormal, and then possibly into high risk.

For example, a normal user does not do any of the following behaviors: scan for passwords, hit 20 web pages in 10 seconds, view web source code, etcetera. If you start seeing these types of behavior together, we can assure you that this is not somebody you want to have access to your website or enterprise. Think of this like a customer in your restaurant disrupting patrons and being rude to waiters. They may be harmless, but they are not good for your business, so you ask them to leave - and it is your right to do so.

After years of analysis and comparing the behavior of a normal user with a hacker, it is very unlikely to get confused between the two. A hacker would not be successful if they were not probing for weaknesses in your enterprise, and by doing so they expose their behavior every time. A normal user just does not do the same things, and there is no crossover. A bank robber pulls a gun and a customer does not. The footprint of a hacker is just as blatant - if you know what to look for.

What if NetGladiator is wrong and blocks a friendly user?

The priority systems of analysis performed by the NetGladiator ensure that it is 99.999% sure that the user is unfriendly when putting a stop on them. When developing the NetGladiator, we had to make sure we did not get any "false positives". A false positive is the case where normal activity might accidentally be flagged as an intruder, and this obviously would be unacceptable. In our test lab we have a series of computers that act like users searching the Internet, the only difference is that we can ramp these robot users up to hyper-speed so that they access millions of pages over a short period of time. We then measured our "false positive" rate from our simulation and ensured that ***our false positive rate on intrusion detection was below 0.001 percent (1/1000th %).***

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 are 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…

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. Please email ips@apconnections.net or call us at **303.997.1300 x123** to discuss.

Copyright © 2012 APconnections, Inc.
rev. 20120521
All rights reserved