

The APconnections NetGladiator IPS appliance both detects and prevents web application network intrusions.

NetGladiator IPS is a simple, elegant solution, utilizing algorithms to assess risk to your network through our proprietary "gladiator" technology, detecting traffic and time-sensitive anomalies. We keep your network secure from web application hackers, ensuring bandwidth availability for your legitimate network users.

Based on APconnections' years of experience creating network solutions that are simple to set-up and use, at great price points, the NetGladiator IPS continues our commitment to helping our customers achieve "Secure Networks, with Zero Maintenance, at the Best Prices". If you would like an IPS appliance that stops intruders without thousands of misleading alerts, and does not require a lot of maintenance, this is the IPS for you.



NetGladiator keeps your network secure from web application hackers. It is a rack-mountable unit that acts as a transparent bridge on Internet links up to 250Mbps.

APconnections NetGladiator IPS Key Features

- **Targeted solution to stop hackers during their Information Discovery Process.** We do one thing very well - we catch & stop hackers while they are probing to learn more about your environment (*their Information Discovery Process*), thereby keeping your web applications secure. 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.
- **Protects your web applications** from malicious hacker activities. Fights the three (3) traffic-based risks identified in the [OWASP Top 10 Application Security Risks](#): 1) A1-Injection, 2) A2-Cross Site Scripting (XSS), and 3) A10-Unvalidated Redirects and Forwards (OWASP = Open Web Application Security Project).
- **Upfront Baseline Security Assessment & Custom Configuration** Our white knights (ethical hackers) work with you to identify possible security holes in your web applications, which are used to configure patterns to protect against. Our targeted approach ensures that you are getting meaningful alerts.
- **Intrusion Detection** Our traffic-based detection algorithms incorporate the following methods in our gladiator technology to stop hackers in their tracks:
 - **Time-sensitive anomaly detection:** The network is assessed for per-IP address deviations from accepted *time pattern* activity baselines. Focus here is on the time aspect of the behavior: repetition, interval, etc. (*also known as statistical anomaly*)
 - **Traffic anomaly detection:** The network is assessed for deviations from accepted definitions of "benign" *usage pattern* activity baselines. Focus here is on the types of activities being performed. (*also known as stateful protocol analysis*)
- **Intrusion Alerts** Alerts are created based on time-sensitive and traffic anomalies, classified simply as either Level 1 (suspicious) or Level 2 (hack).
- **Intrusion Prevention** Default action is to log a warning with the IP address of the intruder at both Level 1 and Level 2. Access is blocked immediately for a Level 2.
- **No false positives** This is a low-maintenance solution. You are not weeding through thousands of false alerts. If a pattern is hit, we know the intent was malicious. You do not need a team of IT people to sift through alerts, read reports, and make adjustments.
- **P2P Blocking** We offer an add-on module to block and monitor the world's top 10 peer-to-peer (P2P) protocols, which account for 99 percent of P2P traffic today.
- **Attractive pricing** We offer great pricing for the performance delivered. Available factory-direct with in-house engineering support.
- Rack-mountable unit that acts as a transparent bridge on Internet links up to 250 megabits.
- Hardware warranties (GHW) available from 1 year to 3 years, to protect your hardware investment.
- Reasonably-priced, yearly software upgrade and support contracts (GSS) available in 1 year to 3 year increments.

Features

Summary	Description
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 (<i>OWASP Top 10</i>) Reflected cross-site scripting (<i>OWASP Top 10</i>) Persistent cross-site scripting (<i>OWASP Top 10</i>) URL SQL injection (<i>OWASP Top 10</i>)
P2P Blocking	Optional add-on module blocks and monitors the world's top 10 P2P protocols.
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.

Specifications

Summary	NG-3000	NG-4000
Capacity		
Number of Connections / Flows per Minute	2,000,000	3,000,000
Maximum Number of IPS Rules	32	48
Throughput (full duplex)	up to 100Mbps	up to 250Mbps
Latency	< 1 millisecond (ms)	< 1 millisecond (ms)
Interfaces		
Network Interfaces (in/out) (internal/external)	2 - copper 10/100/1000 3rd optional Fiber optional	2 - copper 10/100/1000/10000 3rd optional Fiber optional
Out of Band Management	yes	yes
Console Port	RS-232 (AT-compatible) with male DB-9 connectors	RS-232 (AT-compatible) with male DB-9 connectors
Dimensions		
	1U	1U
Rack Mountable	yes	yes
Height	1.7 in (4.3 cm)	1.7 in (4.3 cm)
Width	16.8 in (42.6 cm)	16.8 in (42.6 cm)
Depth (length)	14.0 in (35.6 cm)	14.0 in (35.6 cm)
Weight	11.1 lbs (5.05 kg)	11.1 lbs (5.05 kg)
Power		
Power Rating	152W	180W
Heat Dissipation	521.51 BTU/hr	617.58 BTU/hr
Power Supply	260W AC with PFC 100-240 VAC, 50-60Hz, 4 Amp max	260W AC with PFC 100-240 VAC, 50-60Hz, 4 Amp max
Safety and Certifications		
Safety, Emission, & Power Supply	USA - UL listed, FCC Canada - CUL listed Germany - TUV certified Europe/CE Mark EN 60950/IEC 60950-Compliant CCC certified	USA - UL listed, FCC Canada - CUL listed Germany - TUV certified Europe/CE Mark EN 60950/IEC 60950-Compliant CCC certified

To Learn More...

We would be a happy to provide a detailed walkthrough of the NetGladiator IPS 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 schedule a technical discussion.

About APconnections

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.