

# INTRUSION PREVENTION SERVICE

## MANAGED INTRUSION PREVENTION

### Manage and monitor your network traffic to prevent and detect unusual traffic

Atlantic.Net's Managed Intrusion Prevention Service (IPS) consists of our NIPS (network intrusion prevention system) and alerting services working in harmony to monitor internet traffic communicating with your systems. While a NIDS (network intrusion detection system) is limited to detecting and reporting on unusual activity inside the perimeter, an IPS is also able to shield a network from hacking attempts by dropping bad traffic before it reaches your servers. Working in conjunction with our Managed Firewall, our Managed IPS helps protect your critical information.



## INTRUSION PREVENTION SERVICE FEATURES

- ✓ Any detected activity or violation is collected centrally using a security information and event management (SIEM) system and reported on a regular basis to the customer.
- ✓ Evaluates all traffic going to and from the Internet. If a suspected intrusion or anomaly takes place, the traffic is either alerted or dropped, depending on customizable rule sets.
- ✓ Rule sets updated daily from reputable organizations like Cisco Talos, Emerging Threats, and Spamhaus.



### Intrusion Detection and Blocking

24/7 network monitoring to prevent abnormal and compromised traffic from infiltrating your sensitive data



### Packet Logging and Reporting

Any traffic generating alerts is logged and viewable. Weekly reports provide a concise summary of events



### Real-Time Traffic Analysis

Quickly detect and patch system vulnerabilities by continuous traffic analysis and breach prevention



### Protocol Analysis

Access to forensic tools to determine system vulnerabilities that led to a compromise



### Flexible Configurations

Choose from a variety of custom configurations to match your unique system needs



### Content Searching & Matching

Identifies suspicious network behavior or an anomaly that could lead to a harmful exploit using customizable rule sets

# INTRUSION PREVENTION SERVICE



## WHY CHOOSE ATLANTIC.NET MANAGED INTRUSION PREVENTION SERVICE

To keep your network safe from attackers, Atlantic.Net's Managed Intrusion Prevention Service utilizes a cutting-edge NIPS. We believe in NIPS because of the active development and transparency it brings with it. Using rule sets from Cisco Talos, Emerging Threats, Spamhaus, and more, our IPS is capable of performing realtime traffic analysis against a wide breadth of attacks.

Our flexible rulesets are built to block known blacklisted and compromised sources while protecting against emerging malware threats and a wide range of vulnerabilities on the host and application level, including Operating Systems, Web, SQL, and File services.



### Find Out More

Atlantic.Net stands ready to help you attain fast compliance with a range of certifications, such as SOC 2 and SOC 3, HIPAA, and HITECH, all with 24x7x365 support, monitoring, and world-class data center infrastructure. For faster application deployment, free IT architecture design, and assessment, visit us at [www.atlantic.net](http://www.atlantic.net), call **+1-408-335-0825**, or email us at [sales@atlantic.net](mailto:sales@atlantic.net).