



NetProbe

AI-based Network Intrusion Prevention



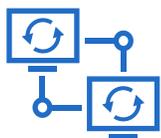
Gorilla Technology Group
www.gorilla-technology.com

NetProbe

AI-based Network Intrusion Prevention

Detect and block various types of external attacks at the edge of all network connection points

From malicious IP connections to DDoS or other targeted attacks, the AI-based detection engine in NetProbe automatically detects and blocks without human intervention which greatly reduces manual processes & alert fatigue on staff which allows your team to focus on key security actions.



Precise & Up-to-Date

NetProbe can identify and learn localized cyber attack patterns. Moreover, it can automatically sync & update threat intelligence with the Security Convergence Intelligence Center.



Intelligent Defense

AI-based technology automatically detects and blocks malicious connections without the need for IT staff intervention. Supports inline deployment methods and provides a bypass network interface so when equipment fails, packet transmission is unaffected and overall network operations go uninterrupted.



DoS/DDoS Protection

Use machine learning algorithms which learn network traffic characteristics and automatically execute Layer3 & Layer4 DoS/DDoS detection and blocking.



Specific Alerts & Notifications

The network administrator will receive attack detection notifications which include time, source/destination IP, triggering rules, and other key data. These notifications will be added to and sent with an automated daily email report.





Powered by Gorilla Technology

Specifications are subject to change. Gorilla products are sold with a limited warranty. Gorilla Technology Group.

All rights reserved. Gorilla Technology, the Gorilla Technology logo are trademarks or registered trademarks of Gorilla Technology Group in the United States and other countries. All other trademarks are the property of their respective owners.