ICON LABS

Floodgate Defender

Bump-in-the-wire Firewall Appliance for industrial automation and embedded devices

"Embedded devices have failed to maintain pace with the increasing number of attacks targeting them, making them easy targets for industrial espionage, hacktivists or even terrorist groups. These devices need the same level of security as used to protect enterprise networks."

Jared Weiner - Analyst, M2M Embedded Software & Tools, VDC Research

Overview

Floodgate Defender™ is a compact firewall appliance providing drop in protection for networked industrial devices. Installation and configuration is done in minutes, providing instant protection against cyberattacks from hackers, denial of services attacks, cyber-sabotage, automated hacking bots and other Internet-based threats.

A secure web interface allows configuration of customized communication policies. Floodgate Defender enforces these policies, dropping unwanted packets before they are passed to the protected device, blocking attacks before a connection is even established.

Protection for Legacy Devices

Many industrial devices are 10 and even 20 years old, predating concerns over Internet-based threats. These devices were manufactured with inadequate security and likely have insufficient resources to run security software.

Updating to newer systems to improve security may be difficult or impossible. The cost of replacing existing equipment with new, more secure devices is often prohibitive and, in some cases, more secure devices may not even be available.

The Floodgate Defender helps **maintain the investment in existing systems** by transparently filtering IP traffic. No modification to the existing industrial device or network is required. Simply install the Floodgate Defender appliance, configure the filtering rules and your existing equipment will be protected from cyberattacks.

Features

- Secured with McAfee Application Control to ensure the device itself remains secure
- Rules-based filtering and Stateful Packet Inspection
- SSL tunneling support
- Secure web configuration interface
- Logging and alerting of security events
- Supports user-defined or default policies
- Protocols supported: Ethernet: TCP/IP, UDP/IP, & ICMP
- Filtering modes: whitelist or blacklist
- Filtering criteria: Ethernet MAC address, Ethernet frame type, IP address, IP protocol, TCP port number, UDP port number
- Integration with the McAfee ePolicy Orchestrator

Hardware specifications

- Size: 4" x 4.5" x 1"
- Weight: 13 oz
- Operating temperature: 0–70 C
- Power input: 12 VDC (external power brick provided)
- Power usage: 8W full load, 1W standby, 6W low load
- 2 x 1000 BaseT Ethernet connections

ICON LABS

McAfee® COMPATIBLE

Drop-in protection

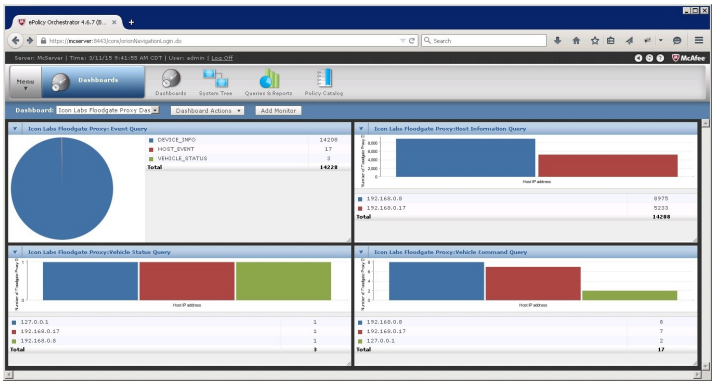
Floodgate Defender can be used to protect any device attached to the Internet or any other TCP/IP network. It is installed between the device and the network and operates transparently; no modifications are required to either the network or to the device being protected.

Floodgate Defender provides bidirectional firewall capabilities, allowing complete control of communication both to and from the protected device. A secure web interface allows configuration of customized communication policies. Floodgate Defender enforces these policies, dropping unwanted packets before they are passed to the target device, blocking attacks before a connection is even established.

NERC-CIP Electronic Security Perimeter

NERC-CIP mandates protection of assets using routable protocols. Floodgate Defender can help in achieving NERC CIP compliance by creating an Electronic Security Perimeter around assets that are otherwise unprotected, such as an RTU that utilizes a routable protocol to prevent unauthorized access. The Floodgate Defender meets the Electronic Security Perimeter requirements of NERC CIP by providing:

- Access Control
- Electronic logging and alerting
- Strong authentication (using SSL tunneling mode)
- Ports and Services protection by blocking all unused ports and protocols
- Small secure enclaves of one to several devices within the perimeter for additional required protection



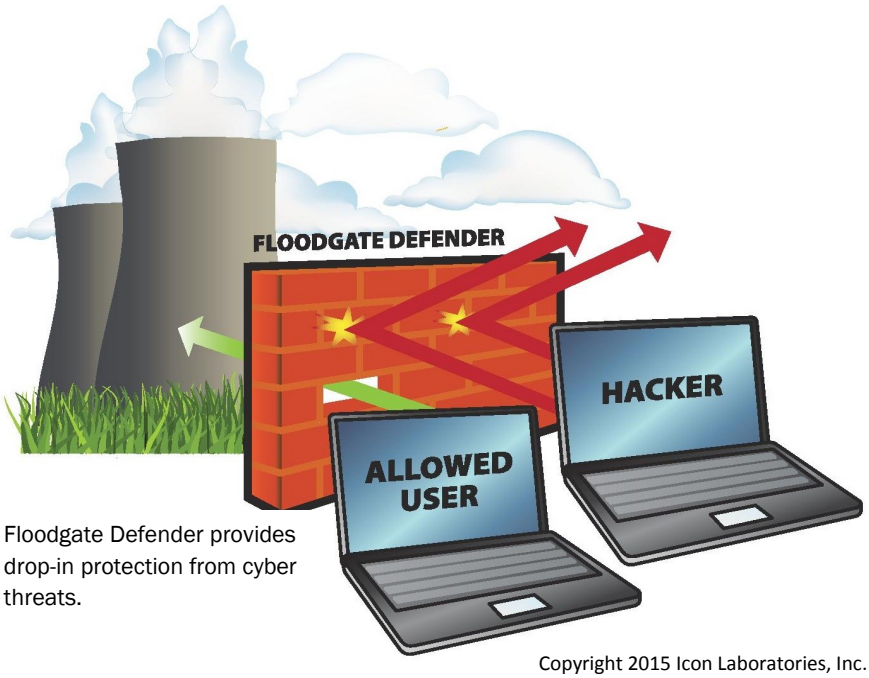
Integration with McAfee ePO and SIEM

The Floodgate Defender appliance is integrated with the McAfee ePolicy Orchestator, enabling centralized management of Floodgate Defender appliances. Using the McAfee ePO provides:

- Centralized management of security policies
- Situational Awareness and device status monitoring
- Event management. All security events detected by the Floodgate Defender are reported to the ePO which provides reporting and event notification

Logging and Alerting

Floodgate Defender generates alerts when alarm conditions are detected. It also maintains a log of all events and policy violations. These logs can be used for forensic investigation to determine the source of an attack. Floodgate Defender can send logs and alerts to the McAfee ePO, Icon Labs' Floodgate Management system or to other Security Information and Event Management (SIEM) systems.



Floodgate Defender provides drop-in protection from cyber threats.

In UK supplied by
www.Phaedsys.com

PhaedruS SystemS

Phaedrus Systems
96 Brambling
Tamworth B77 5PG
Ph: 0808 1800 358

Email: info@phaedsys.com