

Icon Labs'

Floodgate™ Packet Filter

Embedded Firewall for Networked Devices

"As cybercriminals are now targeting non-conventional electronic appliances such as battery chargers, mobile phones, smart meters and digital photo frames, companies need to pay even more attention to their security practices."

Kevin Kwang,
ZDNet

Overview

Floodgate™ Packet Filter is a complete embedded firewall providing a critical layer of security for networked devices. Floodgate's unique design provides three types of filtering to protect against Internet-based threats:

- Static/rules-based filtering blocks packets based on configurable rules.
- Dynamic filtering/stateful packet inspection (SPI) blocks packets based on connection state.
- Threshold-based filtering blocks packets based on threshold crossings to protect against denial of service (DoS) attacks, broadcast storms and other packet flood conditions.

Embedded Devices Targeted by Internet-Based Attacks

Internet-based attacks are on the rise and an increasing number of these attacks target embedded devices. Despite this, many embedded devices are built without a firewall leaving them vulnerable to attack.

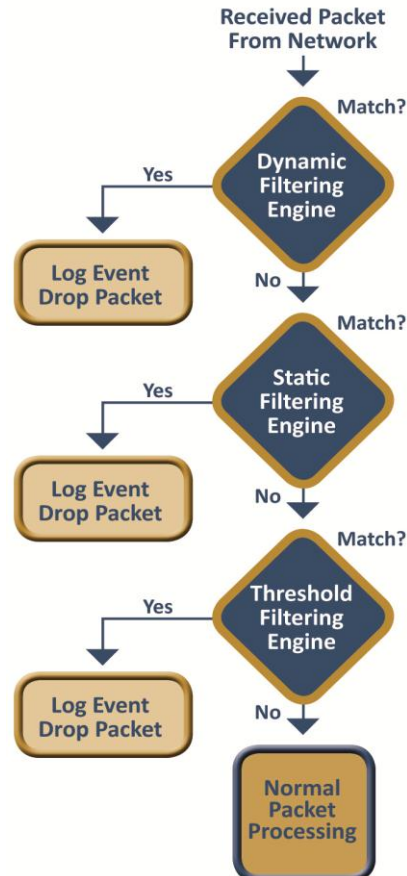
Reported attacks against embedded devices include:

- Electronic road sign reprogrammed by hackers to display false information.
- Electronic billboard reprogrammed to display adult content.
- Sewage spill caused by a compromised control system.
- Remote monitoring system that failed due to a packet flood DoS attack.

Features

- Easily configured filtering rules.
- Ethernet, IP/UDP/TCP/ICMP filtering.
- Layer-based callbacks allow easy integration at any layer in the IP stack.
- Extremely low latency, tests show improved network throughput under load by blocking packets earlier.
- Small footprint and efficient design for embedded systems.
- Portable source code for use with any embedded OS.

Floodgate Operation



Threshold-based Filtering

Floodgate's threshold filtering engine performs filtering based on network traffic patterns. Configurable thresholds are used to determine the level at which network traffic will be blocked. Floodgate does not require any knowledge of the network configuration or make any assumptions about what network traffic should be allowed or blocked. Floodgate analyzes traffic patterns in real-time and only blocks packets when traffic patterns exceed the configured thresholds.

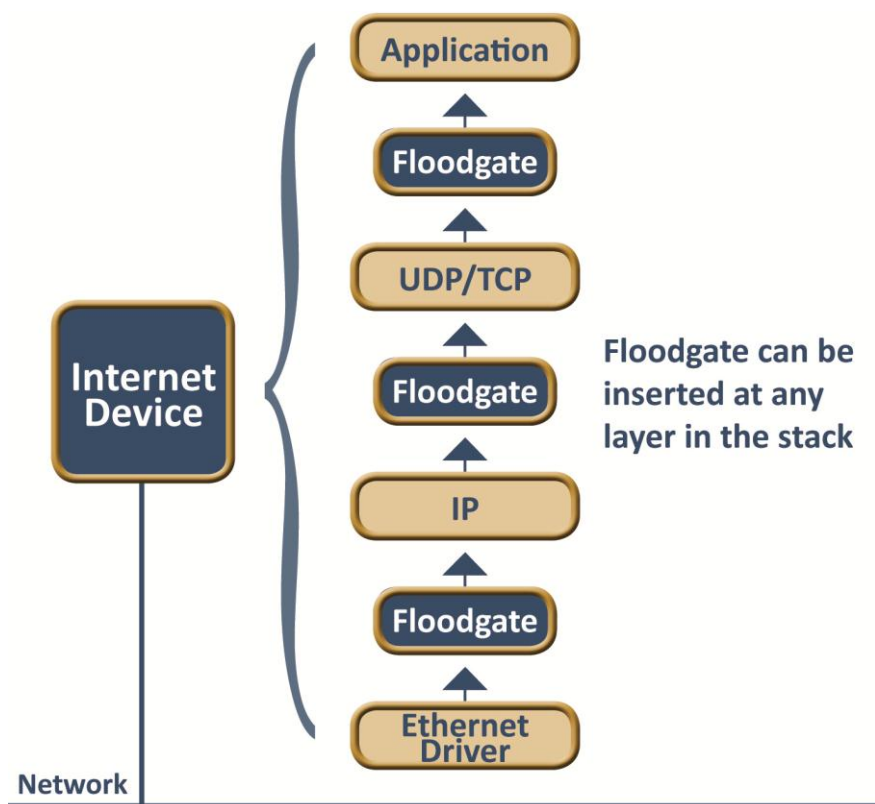
The threshold filtering engine is configurable. The user can configure:

- Filtering criteria (IP address, port, protocol, etc.)
- Thresholds
- Interval length
- Filtering type (deterministic vs. non-deterministic)
- Permeability

Event Logging

An API is provided for logging threshold crossings and other events to a file or to another interface.

Floodgate Usage:



Configurable Filtering Rules

Floodgate uses configured filtering rules to control the filtering engine. The user has complete control over the type of filtering performed and the specific criteria used to filter packets. The user can configure:

- Static filtering rules for Ethernet, IP and protocol (TCP/UDP/ICMP) layers.
- Static filtering by IP address, MAC address, port number and protocol number.
- Blacklist and whitelist filtering.
- Threshold-based filtering criteria.
- Stateful Packet Inspection (SPI) filtering rules.
- Independently enable and disable static filtering, dynamic filtering and threshold-based filtering.

Stateful Packet Inspection

Stateful Packet Inspection performs filtering based on the state of a connection, allowing faster performance and simplifying the filtering rules. Floodgate's SPI filtering engine supports:

- Configuration of SPI filtering rules
- IP header options
- TCP flags
- Configurable TTL

Lockdown Mode

Floodgate supports a Lockdown Mode for security critical applications. In lockdown mode all communication must originate from the embedded device; any communication originating from the Internet is blocked. Support is provided for a trusted devices list that can initiate communication.

- Provides the highest levels of protection.
- Protects against IP Spoofing.
- Used in combination with rules-based filtering to further control the packets processed by the device.

Layer based callback

Floodgate provides layer-based callbacks for integration with the protocol stack on the embedded device. Floodgate's callback routines can be inserted at the Ethernet, IP or protocol (TCP/UDP/ICMP) layer. This provides engineers maximum flexibility in the design of their embedded product.

Other Products from Icon Labs

Icon Labs provides portable embedded software for military/aerospace, medical devices, telecom/datacom, industrial control and other embedded devices.

- **Device Protection** with Floodgate Packet Filter and Floodgate SNMP
- **Secure Remote Access** with Iconfidant SSH & SSL
- **Network Management** with Envoy SNMP

www.iconlabs.com



3636 Westown Parkway
Suite 203
West Des Moines, IA 50266
Ph: 515-226-3443
Fax: 877-379-0504
Email: info@iconlabs.com