

# FireFly

for VxWorks

## IP-Filtering Firewall

FireFly is a robust, lean, high performance, packet-filtering firewall implementation for VxWorks®. Its core engine permits or denies packets from passing through it based on pre-defined and easily configurable policies.

FireFly's unique, advanced features include hooks for dynamic firewalling and stateful inspection. Its small footprint and robustness have been specifically designed for use in an embedded environment. FireFly's unprecedented flexibility and easy customization make it the firewall of choice in embedded networking applications.

### Filtering Support

FireFly supports a variety of advanced filtering options, including:

- ❖ Source and destination IP addresses and MAC types.
- ❖ Source and destination port numbers.
- ❖ IP/TCP/UDP/ICMP Protocol based filtering.
- ❖ TCP window and flags such as FIN, SYN, RST, PUSH, ACK & URG.
- ❖ All ICMP types.
- ❖ IP options such as strict source route, loose source route, record

### Features

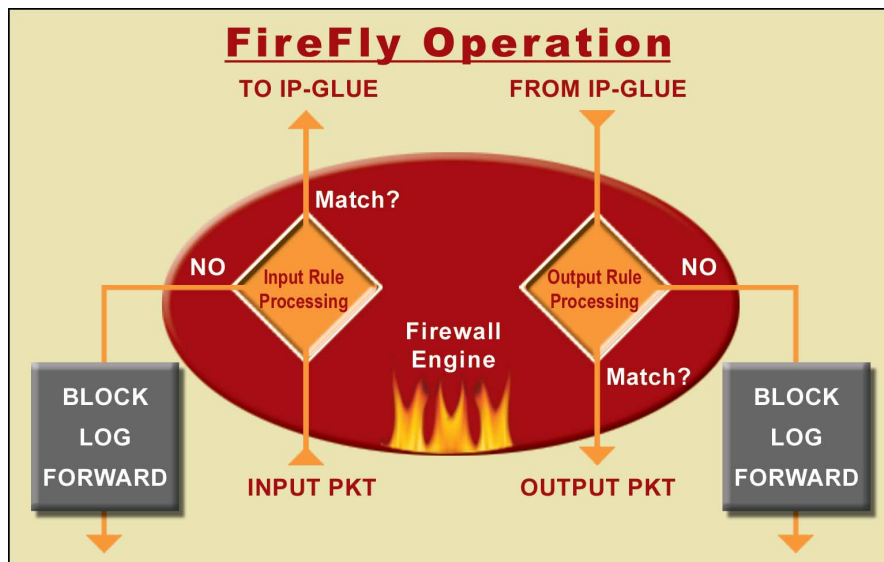
- ❖ Fully configurable anti-spoofing IP packet filtering.
- ❖ Extremely small footprint.
- ❖ Low network latency.
- ❖ Dynamic firewall support in conjunction with NAT.
- ❖ Forwarding and logging hooks.
- ❖ Built-in stateful inspection support for TCP, UDP and ICMP.
- ❖ Easily controlled by webserver through string based CLI.
- ❖ Includes rule numbering support and advanced "or" blocks in rules.
- ❖ Support for rule "sets".
- ❖ Support for CPU types of either endian-ness including PowerPC, MIPS, X86, ARM/XScale.
- ❖ Royalty-free!

route, version, TTL, and time stamp.

- ❖ Fragment flag, service type (TOS), IP ID and IP precedence in the IP header.
- ❖ MAC address, MAC type.

### Stateful Inspection

Stateful inspection provides the ability to track and control the flow of communication passing through the firewall filter. The ability to keep track of state and context information about a session simplifies rules and tries to interpret higher-level protocols. FireFly provides stateful inspection for TCP/UDP/ICMP packets and further enables custom versions of circuit-level filtering and application-level filtering to be easily added with the hooks provided.



### VxWorks Edition Features

- ❖ Designed exclusively for VxWorks and VxWorks based Platforms
- ❖ Requires no special VxWorks source modifications
- ❖ Integrated with VxWorks build & install methodology
- ❖ Project Facility componentization
- ❖ Easy Integration with BSPs
- ❖ Enhanced memory management & partition support
- ❖ Native support for VxWorks 5.3.x, 5.4.x, 5.5.x, 6.0 and AE

## Management Support

**FireFly** supports a customizable management interface that can be programmatically controlled or presented through a string-based command layer, which can be easily controlled through a web-server, with structured data files such as XML or via a command line interface (CLI). Support for rule numbering provides ease of overriding at any level. Advanced "or" blocks can be implemented in the firewall rule-set such as "add 100 allow ip from { x or not y or z } to any". Further, rules can be grouped into "sets" that can be individually disabled and enabled, and allows for atomic ruleset manipulation. Customizable hooks for logging and forwarding enable specific actions to be taken when accepting or rejecting packets.

## Complements Network Security

Securing a connected embedded device requires security in different dimensions. **FireFly**'s system security typically

involves keeping an embedded device protected from external access on specific ports. This perimeter or system security acts as a powerful complement to network security which protects data in transit, when it is used with security solutions such as **TeamF1**'s SSL, SSH and IPsec solutions. For example, a combination of **TeamF1**'s **SSHield** SSH tunneling and **FireFly**'s restricted external access enables sophisticated security policy settings by allowing only a single or few secure points of entrance through the network to the embedded device. Fine grained control over the accessibility of application ports from the public network can be gained while at the same time allowing full access from within the tunneling capabilities of a protocol such as SSL, SSH or IPsec.

## Built for VxWorks

The **VxWorks** edition of **FireFly** is a drop-in component for **VxWorks 5.x, 6.0** and **AE**. It has been extensively validated on a variety of CPU architectures, and this minimizes development and integration efforts.

## Also Available

- ❖ **SSLimSecure**  
*Secure Socket Layer*
- ❖ **ClassHopper**  
*Alternate Queuing Disciplines*
- ❖ **SSHield**  
*Secure Shell*
- ❖ **V-IPSec IPsec & IKE**  
*Network Layer Security*

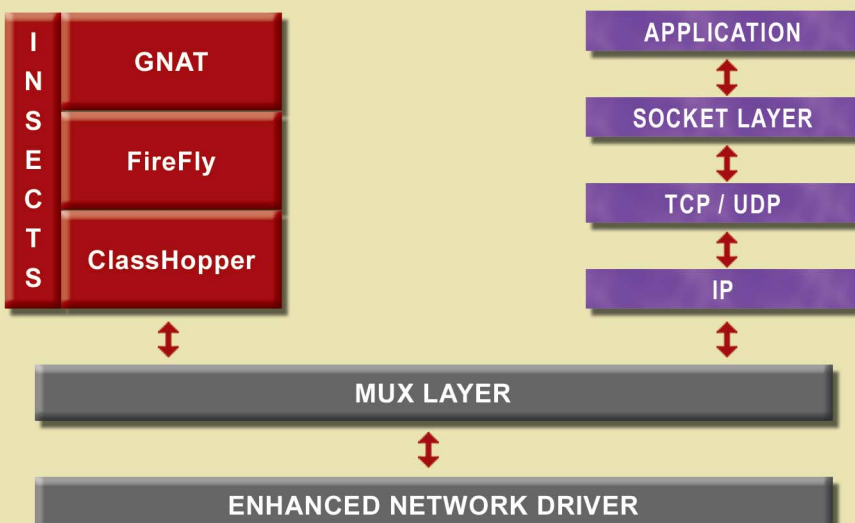
## Custom Solutions

**TeamF1**'s professional services can provide the resources and expertise to build customized implementations of **FireFly** and support for specific provisioning configurations for the firewall rules.

## Customization Flexibility

- ❖ Available in full-source format
- ❖ Interface, port, and direction specific rules
- ❖ Support for adding custom filtering options
- ❖ Customization hooks and callouts
- ❖ Unwanted components can be scaled out

## INSECTS "BUMP-IN-THE-STACK" MODEL



**FireFly** is especially optimized for **VxWorks** and **VxWorks** based Platforms such as PNE, PID and PCD, with support for multi-tasking and memory partitions, and transparently works with the native network stack in **VxWorks** or with **TeamF1**'s **NetF1** high-performance stack as well as other third-party stacks. Like the other members of the **INSECTS** suite, it is built as a network service that binds itself with the MUX layer, thereby guaranteeing compatibility with any **VxWorks** application with minimal to no changes, and without any special network stack source code requirement.

Email: sales@TeamF1.com  
Web: www.TeamF1.com  
Ph: 510-505-9931 ext. 5  
Fax: (510) 505-9941



© 2002-2004 TeamF1, Inc.