

FIREWALL

Packet Filter Package

Internet Security Threats

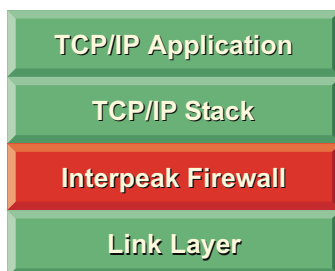
Hacker attacks are an everyday reality in today's Internet, and will be an even bigger threat in the future as more and more computers become permanently connected. The Interpeak Firewall with its packet filtering features is an imperative component when protecting against such attacks.

In the next few years, billions of computers are expected to enter the Internet. As more and more people around the world get access to computers and learn how to use them, Internet traffic will continue to grow. Additionally, the advent of Internet connected mobile phones and PDAs will increase the load on networks and routers even further. When more people and devices are using the Internet, the probability of corrupt, unintended or hacked packets reaching a clean computer system will increase considerably.

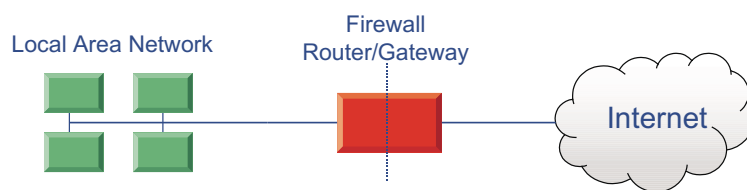
“Always-On” Connections Are Tempting Targets for Attackers

Modern methods to access the Internet such as Cable, DSL and Satellite connections are tempting targets for an attacker. This is because the connection is “always-on”, and that the IP address rarely changes. Many users do also leave their computers connected while they are not using Internet.

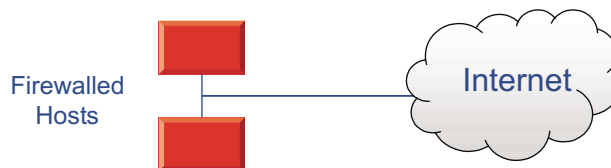
Dial-up connections on the other hand are slow and uses a different IP address each time the modem connects which makes them less appealing for hackers.



Deployment of the Interpeak Firewall as a bump in the stack (BITS).



The Interpeak Firewall is here installed in the gateway between a private LAN and the Internet.



The Firewall may also be installed in all individual hosts needing protection.

Vulnerable Computer Systems Are Connected to the Internet

The intention of the hacker varies. Some attackers just want to make life hard for the user or system by trying to crash it or interrupt its regular service. Others may scan the computer for sensible information. Some hackers may even want to take control over the computer to be able to access other computers or perform hacker attacks without revealing his identity. In summary, as long as vulnerable systems are connected to the Internet, there will be unauthorized people trying to access them.

Different Types of Hacker Attacks Are Frequent

Ping floods, port scans, DoS (Denial

of Service) attacks are examples of hackers attacks that Internet connected computer systems have to face.

Firewall System Setup

There are mainly two different system setups for the Firewall. The first alternative is to run the firewall on the gateway between the LAN and the Internet. This way the hosts on the LAN is protected from unauthorized hosts or hacker attacks without even knowing there is a firewall in place. The other alternative is to run the firewall software on the hosts that require protection. This means that some extra processing is required on each host. There is no straight answer to which solution is best. It has to be decided for each case.

Interpeak Firewall Features

The Interpeak Firewall will protect your protocol stack from hacker attacks. It can be configured to discard unwanted packets that might be part of a hacker attack so that your applications can continue to run smoothly. The Firewall can also log packets for later investigation to examine if they were part of a hacker attack, or originated from a misconfigured host that sends out unintended packets.

Smooth Integration

The Interpeak Firewall can be integrated directly into the TCP/IP stack if stack source code is available. This solution typically generates the optimal solution with respect to performance and handling of fragmented IP packets. If source code for the stack is not available, the Firewall can be integrated as a bump in the stack solution (BITS). Most RTOS and TCP/IP stack vendors supply the necessary function hooks required to examine all incoming and outgoing packets.

Configurable

The necessary rules are assigned to the Firewall through a shell command or through a file specifying the ruleset. Firewall rules may be designed to filter on almost any parameter in the IP, IPv6, UDP and TCP protocols.

Easy to Use

The Firewall rule syntax is compatible with *ipfilter*, the firewall filter package delivered with the NetBSD, FreeBSD and OpenBSD operating systems. This fact makes it possible to use third party graphical tools or rule compilers to generate filter rule files.

The shell command supplied with the Interpeak Firewall is a powerful tool for adding or removing filter rules, disabling or enabling the firewall or examining statistics or logs.

Embeddable

The Interpeak Firewall is the optimal solution for embedded products as it requires little memory and processing power. Performance is further increased by the support of rule groups.

Supports IPv6

The Firewall supports the next generation Internet protocol IPv6. It understands the new protocol header and firewall rules can be specified to filter on IPv6 traffic only. These rules can coexist with IPv4 traditional rules if a dual mode stack is executed on the gateway or host being protected.

Supports Stateful Firewalling

In many situations it is necessary for the firewall to allow incoming traffic on ports and protocols that normally are not open. For example, incoming UDP traffic may not be allowed to enter through the firewall unless there is pending request waiting for a response. This can be the situation when a host queries an external name server for a

domain name. The Interpeak Firewall includes support for the ruleset to specify stateful firewalling.

Firewall Rules

Each firewall rule must specify an action (block or pass) and a direction (in or out) and an address scope (all). In addition the following features are supported:

- Filter on interface.
- Log packet.
- Quick keyword—Fast exit of rule parsing.
- Filter on individual addresses and address ranges.
- Filter on protocol.
- Filter on TCP/UDP ports and port ranges.
- Filter on ICMP type and code.
- Filter on TCP flags.
- Filter on fragments.
- Filter on IP options.
- Supports rule groups for performance optimization.
- Supports stateful firewalling.

- Packet filter type firewall.
- Easy to integrate and use.
- Rule syntax compatible with "ipfilter".
- Embeddable.
- Configure directly with shell command or via firewall rule files.
- Filter on almost any protocol parameter.
- High performance.
- Supports stateful firewalling.
- Keeps logs and statistics.
- Delivered in ANSI compliant "C" source code.
- Complete ready-to-run RTOS integration with examples, makefiles etc.

Interpeak Firewall features.

Interpeak Secure Networking Software

Interpeak provides state-of-the-art networking solutions specifically designed for embedded systems. The company's embedded networking and security software is currently used in thousands of applications across the globe.

Headquartered in Stockholm, Sweden, Interpeak operates through a global network of distribution channels and has its own sales and field application force dispersed in strategic locations worldwide, including the USA, Europe, and Asia. For additional information, please visit our homepage www.interpeak.com.

All Interpeak products are trademarks or registered trademarks of Interpeak AB. Other brand and product names are trademarks or registered trademarks of their respective holders. The information in this document has been carefully reviewed, and is believed to be accurate and reliable. However, Interpeak AB assumes no liabilities for inaccuracies in this document. Furthermore, Interpeak AB reserves the right to change specifications embodied in this document without prior notice.

Version 1.21-r5. Copyright © 2005, Interpeak AB. All rights reserved.