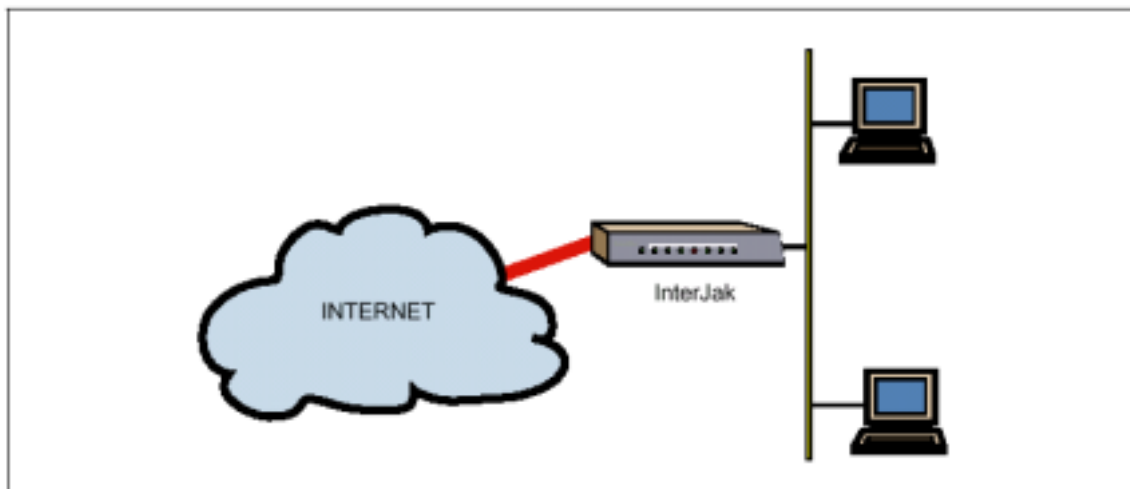


Firewall Application Note

The InterJak, Internet service appliances bring the power and ubiquity of the Internet to small offices, easily & affordably. With the ability to have an “always on” high speed Internet connection using broadband technologies such as DSL and cable, business’ face the threat of exposing their private networks to unauthorized users, data corruption and thefts. This makes an access control service a very attractive offering to this market. Access Control services secures the demarcation between the end user’s private network and the public Internet with the capability to distinguish between friendly and hostile requests trying to gain entry into the private network. The InterJak device’s firewall feature accomplishes this via a safe and effective connection between a Local Area Network (LAN) and Wide Area Network (WAN) link to the Internet. It is user-definable and can be tailored to suit the needs of the individual network. The InterJak device’s firewall feature can also be configured to provide control of traffic between different sections on the LAN.



Positioning InterJak to create firewall protection.

Features of the InterJak Firewall

Packet Inspection and Filtering: The InterJak firewall consists of a series of rules used to inspect all packets trying to travel between the regions. If a packet matches a rule, then a defined action occurs. Although several actions are possible, these can be simplified by stating that packets are either accepted or rejected. The **Advanced Firewall** option allows user-defined rules be added to the InterJak device’s pre configured firewall via the InterJak Management Suite, the remotely managed browser based interface. This enables users to tailor the firewall protection to suit their needs.

Remote Management: The InterJak comes with a preconfigured the firewall feature. The service can be managed or configured with Advance features remotely using the InterJak Management Suite, making it a very attractive value added service offering for Service Providers. The InterJak maintains a systems log which records all events of a security sensitive nature, e.g. access denials on certain vulnerable ports and addresses.

What does the InterJak Firewall Protect You Against?

- Internet Vandalism: Hackers who steal enterprise resources or corrupt systems resources.
- DoS(Denial of Service) attacks: This is an intentional method of disrupting network services under the guise of seemingly normal connections. The perpetrator launches attack from a remote site or distributed attacks from multiple sites resulting in the significant consumption of systems resources and ultimately systems crash or outage to legitimate users. The InterJak firewall configuration protects against DoS attacks such as:
 - **ICMP flooding** This is a denial of service (DoS) attack floods the network with ICMP messages, preventing legitimate users from establishing TCP connections or causing the system to crash.
 - **SYN Flooding**:This is a denial of service (DoS) attack, where the idea is to send as many TCP SYN packets to the system that it either prevents legitimate uses from establishing TCP connections or crashes the system.
 - **Ping of Death**:This is a denial of service (DoS) attack. Oversized ICMP messages (typically echo messages) are sent, resulting in any system receiving the packet to crash, hang or reboot.
 - **Teardrop and Land**: This is a denial of service (DoS) attack that uses specially prepared TCP packets to crash a system or cause it to hang.
 - **IP Spoofing**: IP spoofing exploits the fact that IP packets are routed through the net using only the destination address. By using a false source address (spoofing), attackers can use this to try different types of denial of service attacks.

Understanding and Using InterJak Firewall

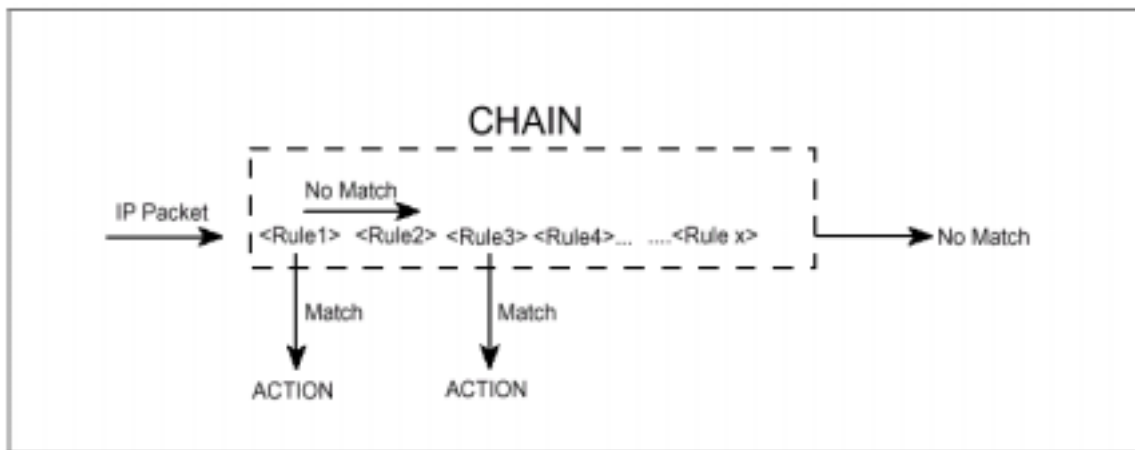
The firewall controls the passage of packets between the outside and inside regions. Access is controlled by inspecting the direction of the packets (using the IP header information), their IP protocol and their TCP port number. If the inspection criteria match one or more of the rules in the firewall rules list, the packets are rejected or permitted to pass depending on the rule.

Firewall Rules

The InterJak inspects the direction of the packets (using the IP header source and destination information), their IP protocols and their TCP port numbers, a set of rules, referred to in the InterJak as a chain. A chain is required for each direction. Packets can travel in three possible directions, so the individual chains are defined as:

- **Input chain**: this contains all the rules for packets traveling into the InterJak.
- **Forward chain**: this contains all the rules for packets traveling through the InterJak.
- **Output Chain**: this contains the rules for packets traveling out of the InterJak.

The rules in these chains are used to "match" the packets. Once a packet is matched, a defined action takes place. Any packets that are not matched by any of the rules are simply dropped. The InterJak supports a maximum of 50 rules or filters in a chain.



The implantation of a chain, its rules and resulting actions

The rules use the following inspection criteria to make a match:

- Source interface specific interface or prefix (for Input and Forward chains only)
- Destination Interface specific interface or prefix (for Input and Forward chains only)
- Destination IP address with mask (0.0.0.0/0 means all packets)
- Source IP address with mask (0.0.0.0/0 means all packets)
- Protocol Type
- Source port (only for TCP and UDP)
- Destination port (only for TCP and UDP)
- Command type (only for ICMP)
- Flags – TCP SYN or non-SYN packets

Any match is met with an ACTION. This can be any one of the following:

- ACCEPT: the packet is allowed
- DENY: the packet is dropped
- REJECT: the packet is dropped and a ICMP reject message is sent to the host
- <chain name>: the current chain is supplemented by another chain, the checking is now in this new chain.
- RETURN: stops the check and returns to the previous chain.
- MASQUERADE (forwarding chain only): accepts match and NAPT's packet before forwarding it.

The InterJak Management Suite interface simplifies the use of these criteria, making firewall creation easy to configure.

The InterJak's Default Firewall Settings

When Firewall protection is enabled in the InterJak, the default configuration enforces:

- Anti-spoofing: packets arriving from the WAN with a local source IP addresses are not permitted entry.
- TCP and UDP connections from the WAN are not permitted.
- ICMP echo-reply is the only type of ICMP packets received.

- HTTP packets arriving from the Internet (WAN) are rejected.
- Access to an Outside DNS name server is rejected.
- PPTP remote access is enabled.
- NATP is enabled.
- E-mail (SMTP) to a local host is rejected.

Firewall Rules for Advanced User

Additional firewall rules can be added to the InterJak **via** the InterJak Management Suite. These advanced rules precede all the rules in the standard chains.

The advanced rules use the following criteria to make a match:

- Source IP address + mask:
 - The definition here uses the source address to control whether the packets entering the InterJak match the rule.
 - 0.0.0.0/0: this covers all traffic.
 - A network address: this covers all traffic from the specified network.
 - Host address: this covers only traffic from the specified host.
- Destination IP address + mask:
 - The definition here uses the destination address to control whether the packets leaving the InterJak match the rule.
 - 0.0.0.0/0: this covers all traffic.
 - A network address: this covers all traffic to the specified network.
 - Host address: this covers only traffic to the specified host.
- Firewall Services:
 - This uses the packets' firewall services (IP protocol and TCP or UDP port number) to define whether they match the firewall rule.
 - There is a list of standard firewall services to choose from, for example, DNS using TCP port number 53 and UDP port number 53.
- Action:
 - The actions resulting from a match in these advanced rules are restricted to the following:
 - Accept
 - Deny
 - Reject