D Simple Firewall Syntax

When creating an firewall rule, keywords must be written in the following order. Some keywords are mandatory while other keywords are optional. The words shown in uppercase represent a variable and the words shown in lowercase must precede the variable that follows it. The # symbol is used to mark the start of a comment and may appear at the end of a rule or on its own line. Blank lines are ignored. The overall format is:

```
RULE_NUMBER ACTION log LOG_AMOUNT PROTO from SRC SRC_PORT to DST DST_PORT OPTIONS
```

Unless otherwise specified, a *minimal* set of instructions can be used which follow the format of:

```
RULE_NUMBER ACTION PROTO from SRC SRC_PORT to DST DST_PORT
```

For example:

```
100 allow UDP from any to 8.8.8.8 53
```

```
200 allow TCP from 146.231.123.120/21 5127,3119 to 9.9.9.0/24 8127,672
```

This section provides an overview of these keywords and their options. It is not an exhaustive list of every possible option. Refer to ipfw(8) for a complete description of the rule syntax that can be used when creating IPFW rules.

RULE_NUMBER Each rule is associated with a number from 1 to 65534. The number is used to indicate the order of rule processing. Multiple rules can have the same number, in which case they are applied according to the order in which they have been added. Otherwise rules are processed top to bottom in numerical order. The packet exits (stops being processed) on the **first** match.

ACTION A rule can be associated with one of the following actions. The specified action will be executed when the packet matches the selection criterion of the rule.

- *allow|accept|pass|permit:* these keywords are equivalent and allow packets that match the rule.
- *check-state:* checks the packet against the dynamic state table. If a match is found, execute the action associated with the rule which generated this dynamic rule, otherwise move to the next rule. A check-state rule does not have selection criterion. If no check-state rule is present in the ruleset, the dynamic rules table is checked at the first keep-state or limit rule.
- *count:* updates counters for all packets that match the rule. The search continues with the next rule.
- *deny|drop:* either word silently discards packets that match this rule.

LOG_AMOUNT When a packet matches a rule with the **log** keyword, a message will be logged. Logging only occurs if the number of packets logged for that particular rule does not exceed a specified LOG_AMOUNT. If no LOG_AMOUNT is specified, the limit is taken from the default value.

PROTO This optional value can be used to specify any protocol name or number found in /etc/protocols. Commonly used are TCP, UDP, ICMP, but could include others such as GRE (47), ESP (50), AH (51) see List of IP protocol Numbers for details.

SRC The from keyword must be followed by the source address or a keyword that represents the source address. An address can be represented by any, me (any address configured on an interface on this system), When specifying an IP address, it can be optionally followed by its CIDR mask or subnet mask. For example, 1.2.3.4/25 or 1.2.3.4**:**255.255.255.128.

SRC_PORT An optional source port can be specified using the port number or name from /etc/services.

DST The to keyword must be followed by the destination address or a keyword that represents the destination address. The same keywords and addresses described in the SRC section can be used to describe the destination.

DST_PORT An optional destination port can be specified using the port number or name from /etc/services.

OPTIONS Several keywords can follow the source and destination. As the name suggests, OPTIONS are optional. Commonly used options include in or out, which specify the direction of packet flow, icmptypes followed by the type of ICMP message, and keep-state.