The firewall rules is setup in the incoming direction. There is no firewall rule in the outgoing direction, so packets are free to go outside from the device. (The “device” here means IP Surveillance itself)

**IP Filter**

This function is setup by [IP\_FILTER\_STATE](http://172.16.5.24/svn/repos/FWDesignSpec/DFI/URLDesignSpec/System/IPFilterState.htm), [IP\_FILTER\_TYPE](http://172.16.5.24/svn/repos/FWDesignSpec/DFI/URLDesignSpec/System/IPFilterType.htm) and [IP\_FILTER\_RULE](http://172.16.5.24/svn/repos/FWDesignSpec/DFI/URLDesignSpec/System/IPFilterRule.htm), packets that matches the rule specified in IP\_FILTER\_RULE will follow the action (DENY or ALLOW) in IP\_FILTER\_TYPE.

The ALLOW packets then will go filtered by **Default Firewall Rules.**

**Default Firewall Rules**

1. Default rule filters out (drop) multicast packet (224.0.0.0/4).
2. Default rule filters out the following abnormal TCP packets.
   1. port scanning packets (NMAP FIN/URG/PSH)
   2. Xmas Tree packet
   3. Null Scan (TCP flag field with all bits off)
   4. SYN/RST
   5. SYN/FIN (Scan possibly)
3. Stateful firewall allows the packet belong to established connections to pass through firewall.
4. Port-Limit:

Allows HTTP(80), HTTPS(443), ACTI-TCP2.0(6001,6002), FTP(20,21), SSH(22) and RTSP(7070) ports to connect-in (listening on device) with Rate-Limit.

Allows SNMP(161,162) UDP packets.

1. Rate-Limit:

Only allows at most 35 new TCP connection requests (SYN) in every second.

1. Default rule drops all the rest packets which not matched the above rule.