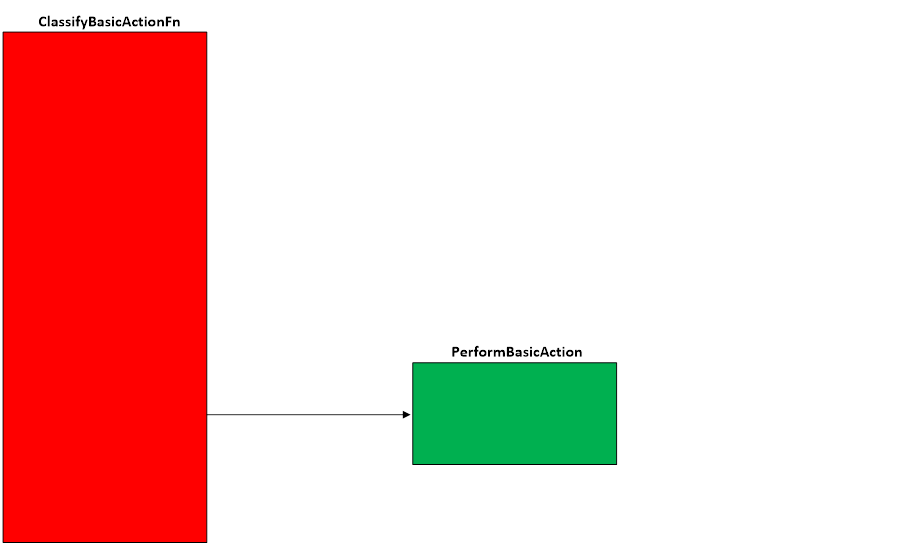
BASIC ACTION

**Overview**

The Basic Action scenarios are designed to return simple actions.  No injection takes place, and by default, they utilize static filters.

All filters added sit in WFPSampler’s sublayer (which is weighted just below IPsec’s sublayer), unless otherwise specified using the –sl <SUBLAYER> command line option.  All filters are associated with WFPSampler’s provider.

When a callout is used, the following diagram shows how the code flows:

  
**Figure A. Code flow for Basic Action Scenario**

When traffic matches a filter at the specified layer, and the filter uses a callout, then the ClassifyBasicActionFn is invoked by the Filtering Engine.  These functions make sure it can update the action and dictates which action to return via **PerformBasicAction()**.

The **ClassifyBasicActionBlock()** function will always return FWP\_ACTION\_BLOCK, causing the traffic to be dropped.

The **ClassifyBasicActionContinue()** function will always return FWP\_ACTION\_CONTINUE, causing the traffic to be allowed unless another filter in a different sublayer returns FWP\_ACTION\_BLOCK.

The **ClassifyBasicActionPermit()** function will always return FWP\_ACTION\_PERMIT, causing the traffic to be allowed unless another filter in a different sublayer returns FWP\_ACTION\_BLOCK.

The **ClassifyBasicActionRandom()** function (which always uses a callout) will randomly return an action of FWP\_ACTION\_BLOCK, FWP\_ACTION\_CONTINUE, or FWP\_ACTION\_PERMIT.  This callout is meant to be for testing purposes only, and would never dictate real world behavior of a callout.  The chance of each action return can be controlled by command-line parameters.

**Applicable Layers**

❖  FWPM\_LAYER\_INBOUND\_IPPACKET\_V4

❖  FWPM\_LAYER\_INBOUND\_IPPACKET\_V6

❖  FWPM\_LAYER\_OUTBOUND\_IPPACKET\_V4

❖  FWPM\_LAYER\_OUTBOUND\_IPPACKET\_V6

❖  FWPM\_LAYER\_IPFORWARD\_V4

❖  FWPM\_LAYER\_IPFORWARD\_V6

❖  FWPM\_LAYER\_INBOUND\_TRANSPORT\_V4

❖  FWPM\_LAYER\_INBOUND\_TRANSPORT\_V6

❖  FWPM\_LAYER\_OUTBOUND\_TRANSPORT\_V4

❖  FWPM\_LAYER\_OUTBOUND\_TRANSPORT\_V6

❖  FWPM\_LAYER\_STREAM\_V4

❖  FWPM\_LAYER\_STREAM\_V6

❖  FWPM\_LAYER\_DATAGRAM\_DATA\_V4

❖  FWPM\_LAYER\_DATAGRAM\_DATA\_V6

❖  FWPM\_LAYER\_INBOUND\_ICMP\_ERROR\_V4

❖  FWPM\_LAYER\_INBOUND\_ICMP\_ERROR\_V6

❖  FWPM\_LAYER\_OUTBOUND\_ICMP\_ERROR\_V4

❖  FWPM\_LAYER\_OUTBOUND\_ICMP\_ERROR\_V6

❖  FWPM\_LAYER\_ALE\_RESOURCE\_ASSIGNMENT \_V4

❖  FWPM\_LAYER\_ALE\_RESOURCE\_ASSIGNMENT\_V6

❖  FWPM\_LAYER\_ALE\_AUTH\_LISTEN\_V4

❖  FWPM\_LAYER\_ALE\_AUTH\_LISTEN\_V6

❖  FWPM\_LAYER\_ALE\_AUTH\_RECV\_ACCEPT\_V4

❖  FWPM\_LAYER\_ALE\_AUTH\_RECV\_ACCEPT\_V6

❖  FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4

❖  FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V6

❖  FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4

❖  FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V6

❖  FWPM\_LAYER\_STREAM\_PACKET\_V4                                     (Win7+)

❖  FWPM\_LAYER\_STREAM\_PACKET\_V6                                     (Win7+)

❖  FWPM\_LAYER\_INBOUND\_MAC\_FRAME\_ETHERNET       (Win8+)

❖  FWPM\_LAYER\_OUTBOUND\_MAC\_FRAME\_ETHERNET   (Win8+)

❖  FWPM\_LAYER\_INBOUND\_MAC\_FRAME\_NATIVE                            (Win8+)

❖  FWPM\_LAYER\_OUTBOUND\_MAC\_FRAME\_NATIVE        (Win8+)

❖  FWPM\_LAYER\_INGRESS\_VSWITCH\_ETHERNET                  (Win8+)

❖  FWPM\_LAYER\_EGRESS\_VSWITCH\_ETHERNET                    (Win8+)

❖  FWPM\_LAYER\_INGRESS\_VSWITCH\_TRANSPORT\_V4      (Win8+)

❖  FWPM\_LAYER\_INGRESS\_VSWITCH\_TRANSPORT\_V6      (Win8+)

❖  FWPM\_LAYER\_EGRESS\_VSWITCH\_TRANSPORT\_V4        (Win8+)

❖  FWPM\_LAYER\_EGRESS\_VSWITCH\_TRANSPORT\_V6        (Win8+)

**Command Line Usage**

|  |  |  |
| --- | --- | --- |
| **Option** | **Argument** | **Meaning** |
| -s | BASIC\_ACTION\_XXXX | Implement the BASIC\_PACKET\_INJECTION scenario |
| -l | Applicable layer | Layer at which this filter will apply |
| -rab | Integer (0-100) | Determines chance of returning FWP\_ACTION\_BLOCK for BASIC\_ACTION\_RANDOM. [default is 50]\* |
| -rac | Integer (0-100) | Determines chance of returning FWP\_ACTION\_CONTINUE for BASIC\_ACTION\_RANDOM. [default is 25]\* |
| -rap | Integer (0-100) | Determines chance of returning FWP\_ACTION\_PERMIT for BASIC\_ACTION\_RANDOM. [default is 25]\* |
| -c |  | Causes the action to be returned via a callout, rather than the filter’s action. |
| -sl | Applicable subLayer | SubLayer to associate with the filter.  [default is WFPSAMPLER\_SUBLAYER]. |
| -v |  | Make the objects associated with this scenario’s instance dynamic |
| -b |  | Make the objects associated with this scenario’s instance available during boot-time |
| -r |  | Remove objects associated with this scenario instance |
| -? |  | Display help |

\*   -rab, -rac, and -rap should total 100. If this is not the case then the code will try to balance the values out (i.e. if you specify only -rab, then -rac, and -rap are calculated as best as possible).

“**WFPSampler.Exe -s BASIC\_ACTION\_BLOCK -?**“ provides help output

“**WFPSampler.Exe -s BASIC\_ACTION\_BLOCK -l FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 -v**“ adds a dynamic filter (**-v**) at FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 (**-l**) This filter will have no conditions, meaning it will block all traffic seen at this layer.

“**WFPSampler.Exe -s BASIC\_ACTION\_PERMIT  -l FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 -v -c**“ adds a dynamic filter (**-v**) at FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 (**-l**) which invokes a callout (**-c**) This filter will have no conditions, meaning it will allow all traffic seen at this layer (unless another filter at a different sublayer blocks it).

“**WFPSampler.Exe -s BASIC\_ACTION\_PERMIT -l FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 -v -c -r**“ removes (**-r**) the dynamic filter (**-v**) at FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 (**-l**) which references the appropriate callout (**-c**).

 “**WFPSampler.Exe -s BASIC\_ACTION\_CONTINUE -l FWPM\_LAYER\_INBOUND\_TRANSPORT\_V4  -ipla 1.0.0.1 -ipra 1.0.0.254 -ipp TCP -c**“ adds a persistent filter at FWPM\_LAYER\_INBOUND\_IPPACKET\_V4  (**-l**) which references the appropriate callout (**-c**).  This filter will have 3 conditions; FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS (**-ipla**) equals 1.0.0.1, FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS (**-ipra**) equals 1.0.0.254, and FWPM\_CONDITION\_IP\_PROTOCOL (**-ipp**) equals TCP.

“**WFPSampler.Exe -s BASIC\_ACTION\_RANDOM -l FWPM\_LAYER\_INBOUND\_TRANSPORT\_V4  -ipla 1.0.0.1 -ipra 1.0.0.254 -ipp TCP -rab 50 -rac 25 -rap 25**“ adds a persistent filter at FWPM\_LAYER\_INBOUND\_IPPACKET\_V4  (**-l**) which references the appropriate callout.  This filter will have 3 conditions; FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS (**-ipla**) equals 1.0.0.1, FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS (**-ipra**) equals 1.0.0.254, and FWPM\_CONDITION\_IP\_PROTOCOL (**-ipp**) equals TCP.  The callout will return FWP\_ACTION\_BLOCK 50% of the time (**-rab**), FWP\_ACTION\_CONTINUE 25% of the time (**-rac**), and FWP\_ACTION\_PERMIT 25% of the time (**-rap**).  In theory, the traffic should be allowed 50% of the time, and blocked the 50% of the time.  Notice that we do not have to specify “-c” for this scenario, as it can only be implemented via a callout.

For a list of conditions applicable to each layer, refer to Filtering Conditions Available at Each Filtering Layer.

For a list of command line parameters for configuring each condition, refer to Conditions for Command Line.