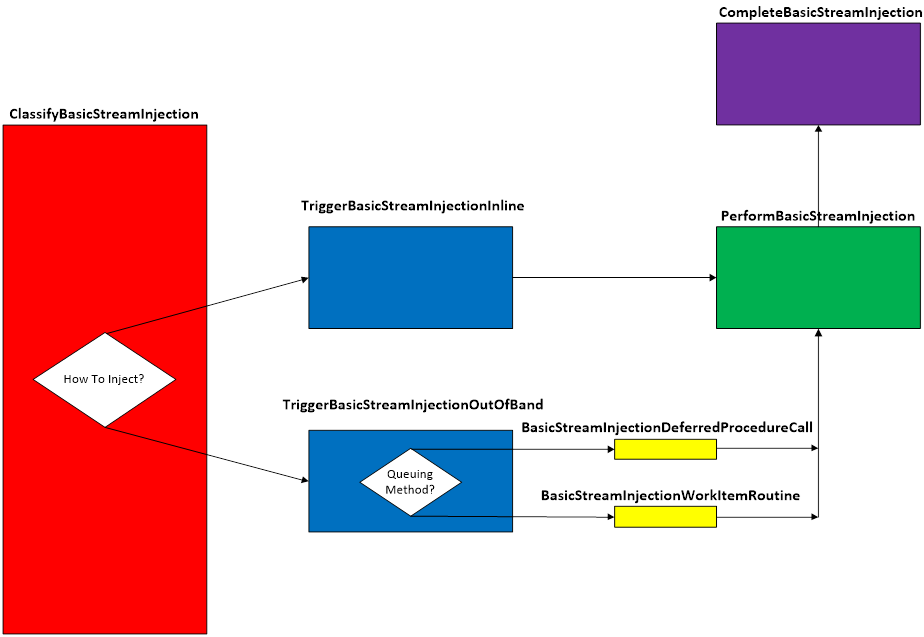
BASIC STREAM INJECTION

**Overview**

The Basic Stream Injection scenario will clone the data and inject it back to the stream.  No modification is performed on the data.

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.

The following diagram shows how the code flows for this callout:

  
**Figure A. Code flow for Basic Stream Injection Scenario**

When traffic matches a filter at the specified layer, **ClassifyBasicStreamInjection()** is invoked by the Filtering Engine.  This function validates that we can perform the injection by looking at the pClassifyOut rights.  It will then create the INJECTION\_DATA which consists of the injectionHandle and the injectionState.  The injection method is determined (default is Asynchronous), and the appropriate triggerFn is called.   At this point, the original data will be blocked.

If the injection method is synchronous (inline), **TriggerBasicStreamInjectionInline()** is invoked.  This function creates the CLASSIFY\_DATA, which consists of the data that was passed into the classifyFn.  The performFn is then called.

If the injection method is asynchronous (out of band), **TriggerBasicStreamInjectionOutOfBand()** is invoked.  This function creates the CLASSIFY\_DATA which consists of copies and references of the data that was passed into the classifyFn.  Based on the queuing method, the appropriate queueFn is invoked.

Regardless of which queueFn is used, each will call **PerformBasicStreamInjection()**.

The **PerformBasicStreamInjection()** will gather the required injection information.  The data is cloned, and then injected back.

Upon successful injection, **CompleteBasicStreamInjection()** will be called by the TCPIP stack.  This function will show the status of the injected data.  Additionally, any memory that was allocated from the functions above, will be freed and any references released.

**Applicable Layers**

❖  FWPM\_LAYER\_STREAM\_V4

❖  FWPM\_LAYER\_STREAM\_V6

**Command Line Usage**

|  |  |  |
| --- | --- | --- |
| **Option** | **Argument** | **Meaning** |
| -s | BASIC\_STREAM\_INJECTION | Implement the BASIC\_STREAM\_INJECTION scenario |
| -l | Applicable Layer | Layer at which this filter will apply |
| -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 |
| -in |  | Perform the injection synchronously (inline) |
| -tdpc |  | Use threaded DPCs for asynchronous (out of band) queuing method |
| -wi |  | Use work items for asynchronous (out of band) queuing method |
| -r |  | Remove objects associated with this scenario instance |
| -? |  | Display help |

“**WFPSampler.Exe -s BASIC\_STREAM\_INJECTION -?**“ provides help output

“**WFPSampler.Exe -s BASIC\_STREAM\_INJECTION -l FWPM\_LAYER\_STREAM\_V4 -v**“ adds a dynamic filter (**-v**) at FWPM\_LAYER\_STREAM\_V4 (**-l**) which references the appropriate callout.  This filter will have no conditions, meaning it will act on all traffic seen at this layer.

“**WFPSampler.Exe -s BASIC\_STREAM\_INJECTION -l FWPM\_LAYER\_STREAM\_V4 –v -r**“ removes (**-r**) the dynamic filter (**-v**) at FWPM\_LAYER\_STREAM\_V4 (**-l**) which references the appropriate callout.

“**WFPSampler.Exe -s BASIC\_STREAM\_INJECTION -l FWPM\_LAYER\_STREAM\_V4 -ipla 1.0.0.1 –ipra 1.0.0.254**“ adds a persistent filter at FWPM\_LAYER\_STREAM\_V4 (**-l**) which references the appropriate callout.  This filter will have 2 conditions; FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS (**-ipla**) equals 1.0.0.1, and FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS (**-ipra**) equals 1.0.0.254.

“**WFPSampler.Exe -s BASIC\_STREAM\_INJECTION -l FWPM\_LAYER\_STREAM\_V4 -ipla 1.0.0.1 –ipra 1.0.0.254 -in**“ adds a persistent filter at FWPM\_LAYER\_STREAM\_V4  (**-l**) which references the appropriate callout.  This filter will have 2 conditions; FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS (**-ipla**) equals 1.0.0.1, and FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS (**-ipra**) equals 1.0.0.254.  The injection will be performed synchronously (**-in**).

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.