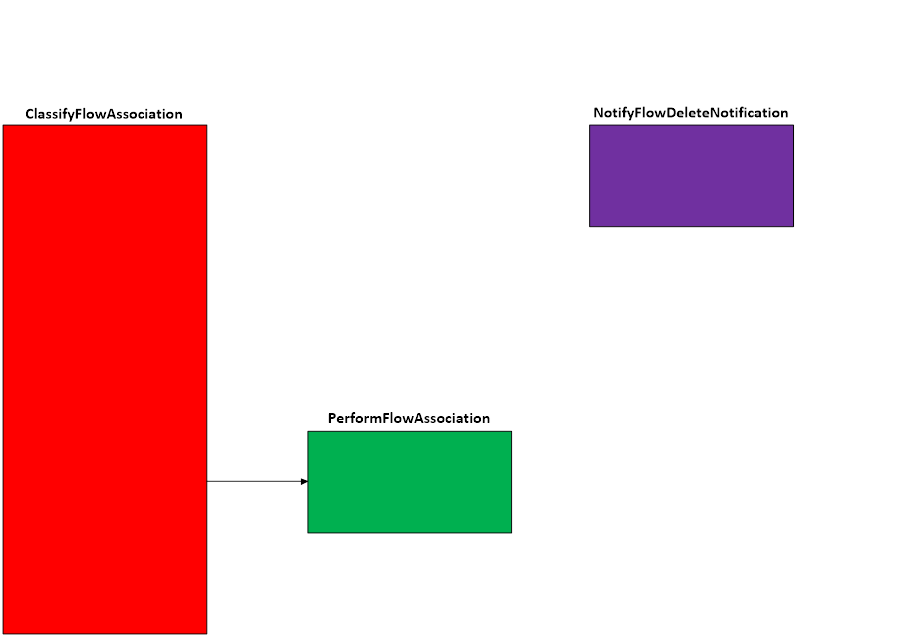
FLOW ASSOCIATION

**Overview**

The Flow Association scenario will cause the classification to associate context to the flow at the specified layers.  This context will then be available as the flowContext parameter of those classifyFns.

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 Flow Association Scenario**

When traffic matches a filter at the specified layer, **ClassifyFlowAssociation()** is invoked by the Filtering Engine.  This function verify we have write access, and invoke **PerformFlowAssociation()**.

**PerformFlowAssociation()** will create the FLOW\_CONTEXT and call FwpsFlowAssociateContext() for the layer(s) that were indicatedfor the context to be associated with (**-awl**).

This context will be valid until the flow is terminated or until FwpsFlowRemoveContext() is called, after which  **NotifyFlowDeleteNotification()** will be invoked and will clean up the FLOW\_CONTEXT.

**Applicable Layers**

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

❖  FWPM\_LAYER\_ALE\_ FLOW\_ESTABLISHED\_V6

**Command Line Usage**

|  |  |  |
| --- | --- | --- |
| **Option** | **Argument** | **Meaning** |
| -s | FLOW\_ASSOCIATION | Implement the FLOW\_ASSOCIATION scenario |
| -l | Applicable Layer | Layer at which this filter will apply |
| -aws | Scenario | Applicable scenario |
| -awl | Applicable Layer … | Layer(s) at which to associate Flow |
| -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 |

“**WFPSampler.Exe -s FLOW\_ASSOCIATION -?**“ provides help output

“**WFPSampler.Exe -s FLOW\_ASSOCIATION -l FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4 -aws BASIC\_STREAM\_INJECTION -awl FWPM\_LAYER\_STREAM\_V4 -v**“  adds a dynamic filter (**-v**) at FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4 (**-l**) which references the appropriate callout.  This filter will have no conditions, meaning it will act on all flows seen at this layer.  The context will then be visible to all classifies at FWPM\_LAYER\_STREAM\_V4 (**-awl**) using the BASIC\_STREAM\_INJECTION callout (**-aws**).  Note that the scenario for BASIC\_STREAM\_INJECTION must already have been configured before implementing this scenario.

“**WFPSampler.Exe -s FLOW\_ASSOCIATION -l FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4  -aws BASIC\_STREAM\_INJECTION -awl FWPM\_LAYER\_STREAM\_V4 -v -r**“  removes (**-r**) the dynamic filter (**-v**) at FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4 (**-l**) which references the appropriate callout.

“**WFPSampler.Exe -s FLOW\_ASSOCIATION -l FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4 -ipla 1.0.0.1 -ipra 1.0.0.254 –aws BASIC\_STREAM\_INJECTION –awl FWPM\_LAYER\_STREAM\_V4**“ adds a persistent filter at FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_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 context will then be visible to all classifies at FWPM\_LAYER\_STREAM\_V4 (**-awl**) using the BASIC\_STREAM\_INJECTION callout (**-aws**).  Note that the scenario for BASIC\_STREAM\_INJECTION must already have been configured before implementing this scenario.

“**WFPSampler.Exe -s FLOW\_ASSOCIATION -l FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4  -aaid C:\Traffic.exe -ipla 1.0.0.1 -ipra 1.0.0.254 -ipp TCP –iprp 6000 –aws BASIC\_STREAM\_INJECTION –awl FWPM\_LAYER\_STEAM\_V4 FWPM\_LAYER\_ALE\_ENDPOINT\_CLOSURE\_V4**“ adds a persistent filter at FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4  (**-l**) which references the appropriate callout.  This filter will have 5 conditions; FWPM\_CONDITION\_ALE\_APP\_ID (**-aaid**) equals C:\Traffic.exe, FWPM\_CONDITION\_IP\_LOCAL\_ADDRESS (**-ipla**) equals 1.0.0.1, FWPM\_CONDITION\_IP\_REMOTE\_ADDRESS (**-ipra**) equals 1.0.0.254, FWPM\_CONDITION\_IP\_PROTOCOL  (**-ipp**) equals TCP, and FWPM\_CONDITION\_IP\_REMOTE\_PORT equals 6000.    The context will then be visible to all classifies at FWPM\_LAYER\_STREAM\_V4 and FWPM\_LAYER\_ALE\_ENDPOINT\_CLOSURE\_V4 (**-awl**) using the BASIC\_STREAM\_INJECTION (and PEND\_ENDPOINT\_CLOSURE) callout (**-aws**).  Note that the scenario for BASIC\_STREAM\_INJECTION and PEND\_ENDPOINT\_CLOSURE must already have been configured before implementing this scenario.

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.

**Notes**

**FlowDelete**

The FlowDeleteNotificationFn is only invoked when the flow terminates or FwpsFlowRemoveContext is called.

**Mixing Scenarios**

FLOW\_ASSOCIATION is only useful when mixed with other scenarios.  For example:

                WFPSampler.exe -s BASIC\_STREAM\_INJECTION -l FWPM\_LAYER\_STREAM\_V4 -ipra 1.0.0.254 -iprp 6000 -v

                WFPSampler.exe -s PEND\_ENDPOINT\_CLOSURE -l FWPM\_LAYER\_ALE\_ENDPOINT\_CLOSURE\_V4 -aaid C:\Traffic.exe -ipra 1.0.0.254 -ipp TCP -iprp 6000 -pcd 5000 -v

                WFPSampler.exe -s FLOW\_ASSOCIATION -l FWPM\_LAYER\_ALE\_FLOW\_ESTABLISHED\_V4 -aaid C:\Traffic.exe -ipra 1.0.0.254 -ippTCP -iprp 6000 -aws BASIC\_STREAM\_INJECTION -awl FWPM\_LAYER\_STREAM\_V4 FWPM\_LAYER\_ALE\_ENDPOINT\_CLOSURE\_V4 -v

This will associate flows with both the BASIC\_STREAM\_INJECTION and PEND\_ENDPOINT\_CLOSURE scenarios. The endpoint associated with the specified flow will remain open for the duration of the injection being performed at STREAM.  Once everything has been injected, the endpoint is allowed to close, and the flow contexts are cleaned up.