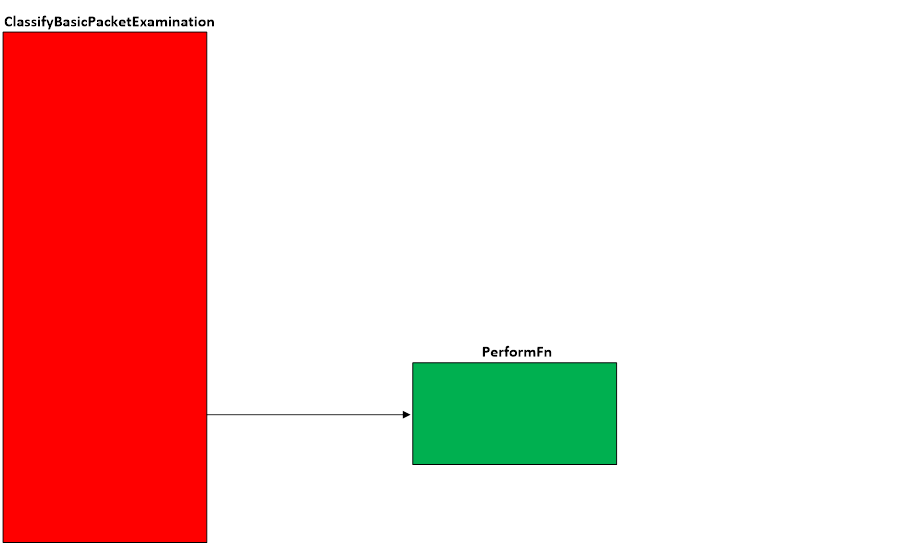
BASIC PACKET EXAMINATION

**Overview**

The Basic Packet Examination scenario will log the packet’s headers at that layer by parsing the NBL and using ETW tracing.  This is performed inline.  For this scenario, no injection occurs.

All filters added sit in FWPM\_SUBLAYER\_INSPECTION.  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 Packet Examination Scenario**

When traffic matches a filter at the specified layer, **ClassifyBasicPacketExamination()** is invoked by the Filtering Engine.  This function creates the CLASSIFY\_DATA and invokes the appropriate performFn.

Each of the performFns are tailored to log the headers for their layer using ETW tracing.  The main need for multiple performFns in this scenario is due to the data offset and information available at each layer.  Within the performFn, the offset of the original NBL is manipulated to get to the appropriate header, after which, the logging function is invoked.  When logging has finished, the data offset is adjusted to the next header.  Before exiting the performFn, the data offset is returned to the original position.

When the performFn is finished, the classifyFn is allowed to continue.  The classifyFn will set the action to FWP\_ACTION\_CONTINUE, and exit.

**Applicable Layers**

❖  FWPM\_LAYER\_INBOUND\_IPPACKET\_V4

❖  FWPM\_LAYER\_INBOUND\_IPPACKET\_V4\_DISCARD

❖  FWPM\_LAYER\_INBOUND\_IPPACKET\_V6

❖  FWPM\_LAYER\_INBOUND\_IPPACKET\_V6\_DISCARD

❖  FWPM\_LAYER\_OUTBOUND\_IPPACKET\_V4

❖  FWPM\_LAYER\_OUTBOUND\_IPPACKET\_V4\_DISCARD

❖  FWPM\_LAYER\_OUTBOUND\_IPPACKET\_V6

❖  FWPM\_LAYER\_OUTBOUND\_IPPACKET\_V6\_DISCARD

❖  FWPM\_LAYER\_IPFORWARD\_V4

❖  FWPM\_LAYER\_IPFORWARD\_V4\_DISCARD

❖  FWPM\_LAYER\_IPFORWARD\_V6

❖  FWPM\_LAYER\_IPFORWARD\_V6\_DISCARD

❖  FWPM\_LAYER\_INBOUND\_TRANSPORT\_V4

❖  FWPM\_LAYER\_INBOUND\_TRANSPORT\_V4\_DISCARD

❖  FWPM\_LAYER\_INBOUND\_TRANSPORT\_V6

❖  FWPM\_LAYER\_INBOUND\_TRANSPORT\_V6\_DISCARD

❖  FWPM\_LAYER\_OUTBOUND\_TRANSPORT\_V4

❖  FWPM\_LAYER\_OUTBOUND\_TRANSPORT\_V4\_DISCARD

❖  FWPM\_LAYER\_OUTBOUND\_TRANSPORT\_V6

❖  FWPM\_LAYER\_OUTBOUND\_TRANSPORT\_V6\_DISCARD

❖  FWPM\_LAYER\_STREAM\_V4

❖  FWPM\_LAYER\_STREAM\_V4\_DISCARD

❖  FWPM\_LAYER\_STREAM\_V6

❖  FWPM\_LAYER\_STREAM\_V6\_DISCARD

❖  FWPM\_LAYER\_DATAGRAM\_DATA\_V4

❖  FWPM\_LAYER\_DATAGRAM\_DATA\_V4\_DISCARD

❖  FWPM\_LAYER\_DATAGRAM\_DATA\_V6

❖  FWPM\_LAYER\_DATAGRAM\_DATA\_V6\_DISCARD

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

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

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

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

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

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

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

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

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

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

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

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

❖  FWPM\_LAYER\_ALE\_AUTH\_LISTEN\_V4

❖  FWPM\_LAYER\_ALE\_AUTH\_LISTEN\_V4\_DISCARD

❖  FWPM\_LAYER\_ALE\_AUTH\_LISTEN\_V6

❖  FWPM\_LAYER\_ALE\_AUTH\_LISTEN\_V6\_DISCARD

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

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

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

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

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

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

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

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

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

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

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

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

❖  FWPM\_LAYER\_ALE\_RESOURCE\_RELEASE\_V4                   (Win7+)

❖  FWPM\_LAYER\_ALE\_RESOURCE\_RELEASE\_V6                   (Win7+)

❖  FWPM\_LAYER\_ALE\_ENDPOINT\_CLOSURE\_V4                  (Win7+)

❖  FWPM\_LAYER\_ALE\_ENDPOINT\_CLOSURE\_V6                  (Win7+)

❖  FWPM\_LAYER\_ALE\_CONNECT\_REDIRECT\_V4                  (Win7+)

❖  FWPM\_LAYER\_ALE\_CONNECT\_REDIRECT\_V6                  (Win7+)

❖  FWPM\_LAYER\_ALE\_BIND\_REDIRECT\_V4                           (Win7+)

❖  FWPM\_LAYER\_ALE\_BIND\_REDIRECT\_V6                           (Win7+)

❖  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\_PACKET\_EXAMINATION | Implement the BASIC\_PACKET\_EXAMINATION scenario |
| -l | Applicable Layer | Layer at which this filter will apply |
| -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 BASIC\_PACKET\_EXAMINATION -?**“ provides help output

“**WFPSampler.Exe -s BASIC\_PACKET\_EXAMINATION -l FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 -v**“  adds a dynamic filter (-v) at FWPM\_LAYER\_INBOUND\_IPPACKET\_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\_PACKET\_EXAMINATION -l FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 –v -r**“  removes (**-r**) the dynamic filter (**-v**) at FWPM\_LAYER\_INBOUND\_IPPACKET\_V4 (**-l**) which references the appropriate callout.

 “**WFPSampler.Exe -s BASIC\_PACKET\_EXAMINATION -l FWPM\_LAYER\_INBOUND\_TRANSPORT\_V4  -ipla 1.0.0.1 –ipra 1.0.0.254 –ipp TCP** “ 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.

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**

**Traces**

In order to get the traces, use a trace utility such as TraceLog.exe and TraceFmt.exe

TraceLog.exe -start wfpsampler -guid #53504657-6d61-6c70-6572-5f496e746572 -f wfpsampler.etl -flags 0xFFFF -level 7

Run the scenario

TraceLog.exe -stop wfpsampler

TraceFmt.exe wfpsampler.etl -pdb <SYMBOLS.PRI\_PATH>\WFPSamplerCalloutDriver\_0x603.pdb  -o \WFPSampler.txt