PEND AUTHORIZATION

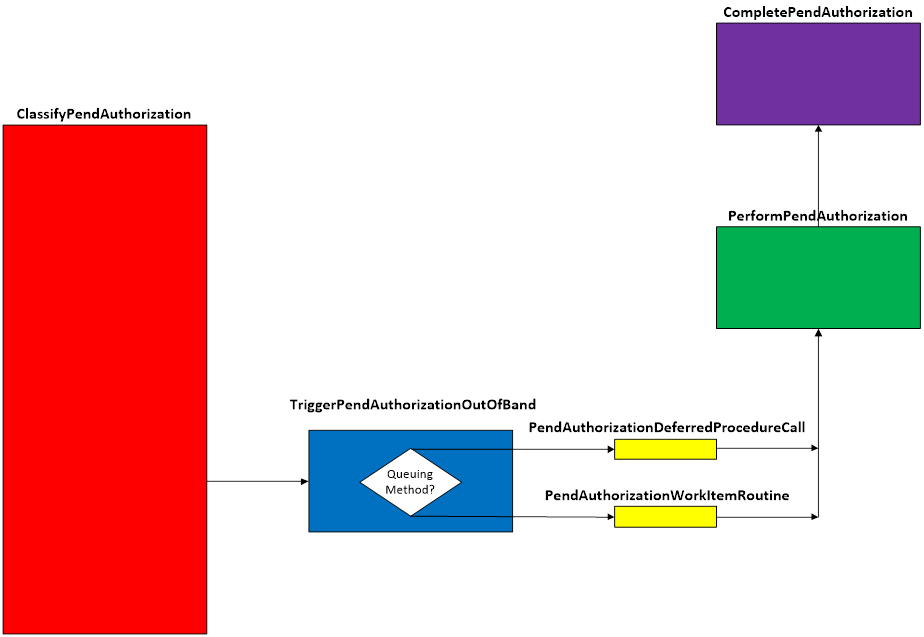
**Overview**

The Pend Authorization scenario will cause the classification to pend for a specified period of time.  In a real world scenario, this time could be used to perform additional process of the packet.  For this scenario though, the thread is just put to sleep for the specified period.

For the layers that contain an NBL, that NBL will be injected back in the final action is to permit the traffic.

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 Pend Authorization Scenario**

When traffic matches a filter at the specified layer, **ClassifyPendAuthorization()** 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.  If the injectionState indicates that we haven’t injected this packet before, then the triggerFn is called.   At this point, the original packet will be blocked.

Because we are essentially telling the classifyFn “Hold on, we need more time”, the injection will always be asynchronous. **TriggerPendAuthorizationOutOfBand()** 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.  The only time a DPC can be used is if there is no delay.  This is due to the fact that the delay introduced is done by using a function only available at PASSIVE\_LEVEL.  Introducing delays at DISPATCH\_LEVEL is rarely a good idea.

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

**PerformPendAuthorization()** will cause the thread to sleep for the duration provided.  When it wakes up, if the layer contains an NBL and the final action is to allow the traffic, then the data offset of the original NBL is retreated to the beginning of the IP Header.  A clone is created, and the offset of the original is advanced back to the original offset.  Once the clone is ready, it is injected back into the TCP/IP stack.

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

Note that with long delays, it is possible to bugcheck the machine by holding on to the inbound NBL for too long.  This normally happens when a machine requests to drop into a power managed state, and processing of the NBL exceeds the allotted time for allowing the state transition to begin.

**Applicable Layers**

❖  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

**Command Line Usage**

|  |  |  |
| --- | --- | --- |
| **Option** | **Argument** | **Meaning** |
| -s | PEND\_AUTHORIZATION | Implement the PEND\_AUTHORIZATION scenario |
| -l | Applicable Layer | Layer at which this filter will apply |
| -pcd | Integer | How long of a pend completion delay to introduce (in ms) |
| -fab |  | Return FWP\_ACTION\_BLOCK after the delay.  If there is an NBL, no injection occurs. [default] |
| -fap |  | Return FWP\_ACTION\_PERMIT after the delay.  If there is an NBL it will be injected. |
| -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 |
| -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 PEND\_AUTHORIZATION -?**“ provides help output

“**WFPSampler.Exe -s PEND\_AUTHORIZATION -l FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4 -v**“  adds a dynamic filter (**-v**) at FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4 (**-l**) which references the appropriate callout.  This filter will have no conditions, meaning it will act on all connections seen at this layer.  The traffic will, by default, be blocked.

“**WFPSampler.Exe -s PEND\_AUTHORIZATION -l FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4 -v -r**“  removes (**-r**) the dynamic filter (**-v**) at FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4 (**-l**) which references the appropriate callout.

“**WFPSampler.Exe -s PEND\_AUTHORIZATION -l FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4 -ipla 1.0.0.1 -ipra 1.0.0.254 -fap**“ adds a persistent filter at FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_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 traffic will be permitted (**-fap**) and the NBL injected.

“**WFPSampler.Exe -s PEND\_AUTHORIZATION -l FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4  -aaid C:\Traffic.exe -ipla 1.0.0.1 -ipra 1.0.0.254 -ipp TCP -fap –pcd 5000**“ adds a persistent filter at FWPM\_LAYER\_ALE\_AUTH\_CONNECT\_V4  (**-l**) which references the appropriate callout.  This filter will have 4 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, and FWPM\_CONDITION\_IP\_PROTOCOL  (**-ipp**) equals TCP.  The decision will be delayed for 5 seconds (**-pcd**) before being permitted (**-fap**).

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.