WFP 是微软推出来替代 TDI HOOK、NDIS HOOK 等拦截网络通信的方案，WFP 的框架非常庞大，在 RING3 和 RING0 各有一套类似的函数，令人兴奋的是，即使在 R3 使用 WFP，也可以做到全局拦截访问网络。由于 WFP 的范围太广，实在难以一言概括，感兴趣的朋友可以自行到 MSDN 上查看微软对它的官方概述。本文的目的，是给大家理顺 WFP 的框架，并利用 WFP 拦截指定进程访问网络，或拦截对指定 IP 地址/端口的访问。

一个标准的 WFP 程序大体是这样子的：**首先使用 FwpmEngineOpen 开启 WFP 引擎（获得一个 WFP 的使用句柄），然后用 FwpmTransactionBegin 设置对网络通信内容的过滤权限（是只读还是允许修改），然后用 FwpsCalloutRegister、FwpmCalloutAdd、FwpmFilterAdd 选择你要过滤的内容，并添加过滤器对象和回调函数，最后用 FwpmTransactionCommit 确认刚才的内容，让刚才添加的回调函数开始生效。当你不用 WFP 的时候，就要用 FwpmFilterDeleteById、FwpmCalloutDeleteById、FwpsCalloutUnregisterById 把你刚才添加的过滤器对象和回调函数删除掉，然后用 FwpmEngineClose 关闭 WFP 引擎（类似于关闭句柄）。**

一个概述已经是这样子了，实现起来就更加麻烦了。为了方便大家学习，我已经把微软的 WFP 实例进行了最大简化，并把核心的注册回调功能封装成了一个函数。下面一步一步进行分析。在具体分析之前，有一些重要的内容需要先说明，否则后面的内容肯定会让大家一头雾水。一、**WFP 一次性要注册的回调函数不是 1 个，而是 3 个。但只有 1 个是“事前”回调，另外 2 个都是“事后”回调（一般只使用“事前”回调，不使用“事后”回调）。**二、**WFP 能过滤的内容很多，你必须选择一个感兴趣的内容。这个“感兴趣的内容”用官话来说叫做“过滤条件标志”，这货其实是一个常量，由于我们是要过滤进程联网，而且一般都是用 IPV4 协议，所以“过滤条件标志”为 FWPM_LAYER_ALE_AUTH_CONNECT_V4（在这个页面可以查到所有的“过滤条件标志”）。三、你必须为这个“过滤条件标志”指定一个 GUID，当然 GUID 的值随便设置就行，只要在系统范围内不重复。代码中的 GUID 就是随意设定的，它的名称为：GUID_ALE_AUTH_CONNECT_CALLOUT_V4。**

第一步：开启 WFP 引擎、选择过滤权限（监控还是监视）、注册回调（输入感兴趣的内容、回调函数地址*3、返回过滤器和回调函数的“句柄”）、确认所有内容（让回调函数开始生效）。

```
NTSTATUS WallRegisterCallouts()    //启用 WFP 防火墙的主函数
{
    NTSTATUS        status = STATUS_SUCCESS;
    BOOLEAN         bInTransaction = FALSE;
    BOOLEAN         bEngineOpened = FALSE;
    FWPM_SESSION session = {0};
    session.flags = FWPM_SESSION_FLAG_DYNAMIC;
    //开启 WFP 引擎
    status = FwpmEngineOpen( NULL,
                                    RPC_C_AUTHN_WINNT,
                                    NULL,
                                    &session,
                                    &gEngineHandle );
    if( !NT_SUCCESS(status))
        goto exit;
```

```
	bEngineOpened = TRUE;
	//确认过滤权限
	status = FwpmTransactionBegin( gEngineHandle,0 );
	if( !NT_SUCCESS(status))
		goto exit;
	bInTransaction = TRUE;
	//注册回调函数
	status = RegisterCalloutForLayer(
				&FWPM_LAYER_ALE_AUTH_CONNECT_V4,
				&GUID_ALE_AUTH_CONNECT_CALLOUT_V4,
				WallALEConnectClassify,
				WallNotifyFn,
				WallFlowDeleteFn,
				&gAleConnectCalloutId,
				&gAleConnectFilterId);
	if( !NT_SUCCESS(status))
	{
		DbgPrint("RegisterCalloutForLayer-FWPM_LAYER_ALE_AUTH_CONNECT_V4
failed!\n");
		goto exit;
	}
	//确认所有内容并提交，让回调函数正式发挥作用
	status = FwpmTransactionCommit(gEngineHandle );
	if( !NT_SUCCESS(status))
		goto exit;
	bInTransaction = FALSE;
exit:
	if( !NT_SUCCESS(status))
	{
		if( bInTransaction)
		{
			FwpmTransactionAbort( gEngineHandle );
		}
		if( bEngineOpened )
		{
			FwpmEngineClose( gEngineHandle );
			gEngineHandle = 0;
		}
	}
	return status;
}
```

```
NTSTATUS RegisterCalloutForLayer   //注册回调的核心函数
(
	IN const GUID* layerKey,
```

```
    IN const GUID* calloutKey,
    IN FWPS_CALLOUT_CLASSIFY_FN classifyFn,
    IN FWPS_CALLOUT_NOTIFY_FN notifyFn,
    IN FWPS_CALLOUT_FLOW_DELETE_NOTIFY_FN flowDeleteNotifyFn,
    OUT UINT32* calloutId,
    OUT UINT64* filterId
)
{
        NTSTATUS              status = STATUS_SUCCESS;
        FWPS_CALLOUT       sCallout = {0};
        FWPM_FILTER         mFilter = {0};
        FWPM_FILTER_CONDITION mFilter_condition[1] = {0};
        FWPM_CALLOUT       mCallout = {0};
        FWPM_DISPLAY_DATA mDispData = {0};
        BOOLEAN               bCalloutRegistered = FALSE;
        sCallout.calloutKey = *calloutKey;
        sCallout.classifyFn = classifyFn;
        sCallout.flowDeleteFn = flowDeleteNotifyFn;
        sCallout.notifyFn = notifyFn;
        //要使用哪个设备对象注册
        status = FwpsCalloutRegister( gDevObj,&sCallout,calloutId );
        if( !NT_SUCCESS(status))
          goto exit;
        bCalloutRegistered = TRUE;
        mDispData.name = L"WFP TEST";
        mDispData.description = L"TESLA.ANGELA's WFP TEST";
        //你感兴趣的内容
        mCallout.applicableLayer = *layerKey;
        //你感兴趣的内容的 GUID
        mCallout.calloutKey = *calloutKey;
        mCallout.displayData = mDispData;
        //添加回调函数
        status = FwpmCalloutAdd( gEngineHandle,&mCallout,NULL,NULL);
        if( !NT_SUCCESS(status))
          goto exit;
        mFilter.action.calloutKey = *calloutKey;
        //在 callout 里决定
        mFilter.action.type = FWP_ACTION_CALLOUT_TERMINATING;
        mFilter.displayData.name = L"WFP TEST";
        mFilter.displayData.description = L"TESLA.ANGELA's WFP TEST";
        mFilter.layerKey = *layerKey;
        mFilter.numFilterConditions = 0;
        mFilter.filterCondition = mFilter_condition;
        mFilter.subLayerKey = FWPM_SUBLAYER_UNIVERSAL;
```

```
        mFilter.weight.type = FWP_EMPTY;
        //添加过滤器
        status = FwpmFilterAdd( gEngineHandle,&mFilter,NULL,filterId );
        if( !NT_SUCCESS( status))
          goto exit;
exit:
        if( !NT_SUCCESS(status))
        {
          if( bCalloutRegistered )
          {
                FwpsCalloutUnregisterById( *calloutId );
          }
        }
        return status;
}
```

第二步：编写回调函数。WFP 的回调函数里提供了丰富的信息，这是 WFP 最大的优点，不用我们为获得各种相关信息而绞尽脑汁。比如在 **FWPM_LAYER_ALE_AUTH_CONNECT_V4** 的回调函数里，我们能获得进程 ID、进程路径、本地、远程的 IP 地址/端口号以及协议代码。但最爽的是此回调函数的最后一个参数，能让我们指定一个值，决定是放行还是拦截。

```
void NTAPI WallALEConnectClassify
(
      IN const FWPS_INCOMING_VALUES0* inFixedValues,
      IN const FWPS_INCOMING_METADATA_VALUES0* inMetaValues,
      IN OUT void* layerData,
      IN const void* classifyContext,
      IN const FWPS_FILTER* filter,
      IN UINT64 flowContext,
      OUT FWPS_CLASSIFY_OUT* classifyOut
)
{
      char *ProtocolName=NULL;
      DWORD LocalIp,RemoteIP;
      LocalIp=inFixedValues->incomingValue[FWPS_FIELD_ALE_AUTH_CONNECT_V4_IP_LOCAL
_ADDRESS].value.uint32;
      RemoteIP=inFixedValues->incomingValue[FWPS_FIELD_ALE_AUTH_CONNECT_V4_IP_RE
MOTE_ADDRESS].value.uint32;
      ProtocolName=ProtocolIdToName(inFixedValues->incomingValue[FWPS_FIELD_ALE_AUT
H_CONNECT_V4_IP_PROTOCOL].value.uint16);
      DbgPrint("[WFP]IRQL=%d;PID=%ld;Path=%S;Local=%u.%u.%u.%u:%d;Remote=%u.%u.%u.
%u:%d;Protocol=%s\n",
                  (USHORT)KeGetCurrentIrql(),
                  (DWORD)(inMetaValues->processId),
                  (PWCHAR)inMetaValues->processPath->data,
```

```
                (LocalIp>>24)&0xFF,(LocalIp>>16)&0xFF,(LocalIp>>8)&0xFF,LocalIp&0xFF,

inFixedValues->incomingValue[FWPS_FIELD_ALE_AUTH_CONNECT_V4_IP_LOCAL_PORT].value
.uint16,

(RemoteIP>>24)&0xFF,(RemoteIP>>16)&0xFF,(RemoteIP>>8)&0xFF,RemoteIP&0xFF,

inFixedValues->incomingValue[FWPS_FIELD_ALE_AUTH_CONNECT_V4_IP_REMOTE_PORT].val
ue.uint16,
                ProtocolName);
    kfree(ProtocolName);
    classifyOut->actionType = FWP_ACTION_PERMIT; //允许连接
    //禁止 IE 联网（设置“行动类型”为 FWP_ACTION_BLOCK）
    // if(wcsstr((PWCHAR)inMetaValues->processPath->data,L"iexplore.exe"))
    // {
    // classifyOut->actionType = FWP_ACTION_BLOCK;
    // classifyOut->rights &= ~FWPS_RIGHT_ACTION_WRITE;
    // classifyOut->flags |= FWPS_CLASSIFY_OUT_FLAG_ABSORB;
    // }
    return;
}
```

第三步：删除回调函数和过滤器，关闭 WFP 引擎。

```
NTSTATUS WallUnRegisterCallouts()
{
    if( gEngineHandle != 0 )
    {
        //删除 FilterId
        FwpmFilterDeleteById( gEngineHandle,gAleConnectFilterId );
        //删除 CalloutId
        FwpmCalloutDeleteById( gEngineHandle,gAleConnectCalloutId );
        //清空 FilterId
        gAleConnectFilterId = 0;
        //反注册 CalloutId
        FwpsCalloutUnregisterById( gAleConnectCalloutId );
        //清空 CalloutId
        gAleConnectCalloutId = 0;
        //关闭引擎
        FwpmEngineClose( gEngineHandle );
        gEngineHandle = 0;
    }
    return STATUS_SUCCESS;
}
```

代码执行的效果如下（密密麻麻一大片信息）：

#	Time	Debug Print
352	53.18205643	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49408;Remote=163.177.242.54:80;Protocol=TCP
353	53.23688889	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49409;Remote=122.193.23.37:80;Protocol=TCP
354	53.23784637	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49410;Remote=112.90.149.45:80;Protocol=TCP
355	53.23895264	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49411;Remote=122.193.23.165:80;Protocol=TCP
356	53.23957062	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49412;Remote=122.193.23.165:80;Protocol=TCP
357	53.24191666	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49413;Remote=123.125.119.150:80;Protocol=TCP
358	53.61732101	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:59500;Remote=192.168.85.2:53;Protocol=UDP
359	53.61762619	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:54088;Remote=192.168.85.2:53;Protocol=UDP
360	53.69877625	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:57590;Remote=192.168.85.2:53;Protocol=UDP
361	54.14585495	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49414;Remote=163.177.242.54:80;Protocol=TCP
362	54.14604950	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49415;Remote=163.177.242.54:80;Protocol=TCP
363	54.14616776	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49416;Remote=163.177.242.54:80;Protocol=TCP
364	54.14627457	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49417;Remote=163.177.242.54:80;Protocol=TCP
365	54.14637375	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49418;Remote=163.177.242.54:80;Protocol=TCP
366	54.14648819	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49419;Remote=163.177.242.54:80;Protocol=TCP
367	54.34648132	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:52492;Remote=192.168.85.2:53;Protocol=UDP
368	54.36205673	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49420;Remote=42.156.210.3:80;Protocol=TCP
369	54.53512955	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49422;Remote=134.170.50.250:443;Protocol=TCP
370	54.53513336	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49421;Remote=134.170.50.250:443;Protocol=TCP
371	54.53522873	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49423;Remote=134.170.50.250:443;Protocol=TCP
372	54.53531647	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49424;Remote=134.170.50.250:443;Protocol=TCP
373	54.69063950	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49425;Remote=124.160.136.250:80;Protocol=TCP
374	54.69078827	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49426;Remote=124.160.136.250:80;Protocol=TCP
375	54.69090271	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49427;Remote=124.160.136.250:80;Protocol=TCP
376	54.69101715	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49428;Remote=124.160.136.250:80;Protocol=TCP
377	54.69149017	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49429;Remote=112.90.32.50:80;Protocol=TCP
378	54.75631714	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49430;Remote=112.90.149.44:80;Protocol=TCP
379	55.62765884	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:49877;Remote=192.168.85.2:53;Protocol=UDP
380	55.64314270	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49431;Remote=112.90.32.40:80;Protocol=TCP
381	56.52275467	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:58288;Remote=192.168.85.2:53;Protocol=UDP
382	56.55065918	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49432;Remote=123.126.62.212:80;Protocol=TCP
383	57.49368668	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:58222;Remote=192.168.85.2:53;Protocol=UDP
384	57.50413895	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49433;Remote=42.156.210.5:80;Protocol=TCP
385	57.52555847	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:56251;Remote=192.168.85.2:53;Protocol=UDP
386	57.53081131	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49434;Remote=112.90.141.232:80;Protocol=TCP
387	57.57589722	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49435;Remote=112.90.77.179:80;Protocol=TCP
388	57.64109039	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:54905;Remote=192.168.85.2:53;Protocol=UDP
389	57.65683746	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49436;Remote=36.250.0.40:80;Protocol=TCP
390	57.66698456	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49437;Remote=134.170.50.250:443;Protocol=TCP
391	57.69167709	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:52322;Remote=192.168.85.2:53;Protocol=UDP
392	57.69214630	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:55234;Remote=192.168.85.2:53;Protocol=UDP
393	57.69227982	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:49815;Remote=192.168.85.2:53;Protocol=UDP
394	57.69244003	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:50649;Remote=192.168.85.2:53;Protocol=UDP
395	57.69309235	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:52605;Remote=192.168.85.2:53;Protocol=UDP
396	57.69321442	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:50723;Remote=192.168.85.2:53;Protocol=UDP
397	57.69340515	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:57966;Remote=192.168.85.2:53;Protocol=UDP
398	57.69416428	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:51991;Remote=192.168.85.2:53;Protocol=UDP
399	57.70830917	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49438;Remote=134.170.50.250:443;Protocol=TCP
400	57.70956802	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:63445;Remote=192.168.85.2:53;Protocol=UDP
401	57.72072983	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49439;Remote=163.177.68.178:80;Protocol=TCP
402	57.72132111	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49440;Remote=112.64.200.170:80;Protocol=TCP
403	57.72145462	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49441;Remote=27.115.124.172:80;Protocol=TCP
404	57.72333145	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49442;Remote=27.115.124.178:80;Protocol=TCP
405	57.72335052	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49443;Remote=27.115.124.177:80;Protocol=TCP
406	57.72346878	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49444;Remote=27.115.124.177:80;Protocol=TCP
407	57.72533417	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49445;Remote=27.115.124.179:80;Protocol=TCP
408	57.72761917	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49446;Remote=27.115.124.180:80;Protocol=TCP
409	57.74296188	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49447;Remote=112.90.83.46:80;Protocol=TCP
410	57.75927734	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49448;Remote=163.177.83.173:80;Protocol=TCP
411	58.10786819	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49449;Remote=134.170.50.250:443;Protocol=TCP
412	58.11651230	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49450;Remote=112.90.83.46:80;Protocol=TCP
413	60.15168381	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49451;Remote=134.170.50.250:443;Protocol=TCP
414	61.83665848	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49452;Remote=134.170.50.250:443;Protocol=TCP
415	62.92830658	[WFP]IRQL=2;PID=356;Path=\device\harddiskvolume2\windows\system32\svchost.exe;Local=192.168.85.129:51518;Remote=192.168.85.2:53;Protocol=UDP
416	63.36501694	[WFP]IRQL=0;PID=2884;Path=\device\harddiskvolume2\program files\internet explorer\iexplore.exe;Local=192.168.85.129:49453;Remote=134.170.50.250:443;Protocol=TCP

无论怎么看，WFP 都是一个非常完美的模型，不过在这里我想说一下 WFP 一个非常坑爹的地方，就是在 WFP 的回调函数里，IRQL 有时候不等于 0 而是等于 2。这意味着如果你要实现主动防御，就不能使用经典方法（KeWaitForSingleObject + 弹框），而是要设计一套异步处理机制（除非遇到 IRQL 不等于 0 的情况直接放行或者拦截）。实际上，WFP 内就有一套异步处理的模型，但我一直无法使用成功，大家有兴趣可以看看如何实现。

关于 WFP 的使用方法简介就到此结束了，但我想说一个跟我本人有关也跟 WFP 有关的故事。因为 WFP 这个坑爹的地方（回调函数内有时候 IRQL 不为 0），造就了我一段郁闷的经历。2013 年 6 月，我刚从大学毕业，获得了金山公司的 OFFER，踌躇满志地前往珠海，打算在这个所谓的“民族软件公司”混出点名堂。我接到的第一个任务，就是设计一个 WFP 防火墙的模型。因为这个 IRQL 的问题迟迟解决不了，让我的情绪非常不好，因此发生几次顶撞 HR 和直属领导的事情（都是和工作无关的小事情）。这些被我顶撞的中层领导对新员工自然是没啥包容心的，直接让我滚蛋了。离开金山倒不可惜，可惜的是浪费了将近 5000 元的房屋押金和中介费（这 5000 元让我心痛了好几个月）。不过金山这种对新人的恶劣态度也逐渐显露出恶果，之后持续不断出现的蓝屏门和最近的“金山毒霸 XP 防护盾”被黑客秒破就是最好的证明。原因很简单，不是所谓的“报应论”，而是说一般牛人都有牛脾气，金山（或者说金山毒霸部门）连我这种没啥脾气的人都接纳不了，如何接纳那些脾气更加火爆的牛人呢？