

Initiate precision packet captures to analyze zero window conditions

Published: 2024-04-01

In TCP metrics, window size specifies the amount of data that a device can receive and process during a flow. When the window size is zero, transmissions are halted until the device signals that it has the space to receive data again.

Zero window conditions that last 1 or 2 seconds are not too unusual, especially during periods of heavy traffic. However, longer-lasting zero window conditions can indicate a more serious problem and cause performance issues.

You can create a dashboard or configure alert notifications to track zero window occurrences, but the cause can be hard to determine. For example, CPU, memory, and NIC usage might be normal, and you don't know if the issue is with the network, the servers, or the application. But you can always find the truth in the packet!


In this walkthrough, you will create a trigger that captures packets with zero window conditions on HTTP transactions. Then, you will download the captures so that you can upload the data to a packet analyzer to help you determine the state of the client and server on a flow when zero window conditions occurred.

Prerequisites

- You must have either unlimited privileges or full write privileges with packet access enabled.
- You must [enable packet capture through the Administration page](#).
- You must have a packet analyzer, such as Wireshark or Microsoft Network Monitor.
- Familiarize yourself with [Triggers](#) concepts and the procedures in [Build a trigger](#).

Write the precision capture trigger

In the following steps, you will write a trigger that initiates a precision packet capture each time a zero window condition occurs on an HTTP transaction.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon  and then click **Triggers**.
3. Click **Create**.
4. Specify the following trigger configuration settings:
 - a) Type `Zero Window PCAP` into the **Name** field.
 - b) In the Assignments field, type `HTTP Servers`, and then select **HTTP Servers**.
 - c) From the Events list, select **FLOW_TICK**.
 - d) Select the **Enable debug log** checkbox.
 - e) Click **Show Advanced Options** and type `128` in the Bytes Per Packet to Capture field.



Tip: The default value is 0. Keep this value to capture all the bytes in each packet.

5. In the right pane, type the following code to initiate the packet capture when a zero window condition occurs:

```
// Check to make sure that this is an HTTP transaction
if ( Flow.l7proto !== 'HTTP' ){
    return;
}
```


```
//The packet capture name, which includes the client and server
//IP addresses and port numbers
var pcapName = 'Zero Windows_'
  + Flow.client.ipaddr + ':' + Flow.client.port
  + '-'
  + Flow.server.ipaddr + ':' + Flow.server.port;

//Initiate packet capture each time a zero window occurs on
//the client or the server
if ( Flow.zeroWnd1 > 0 || Flow.zeroWnd2 > 0 ) {
  var opts = {
    maxPackets: 30,           // Capture up to 30 packets
    maxPacketsLookback: 15 // Capture up to 15 lookback packets
  };
  Flow.captureStart(pcapName, opts);
  //Show capture activity in debug log
  debug('Start Zero PCAP: ' + pcapName);
}
```

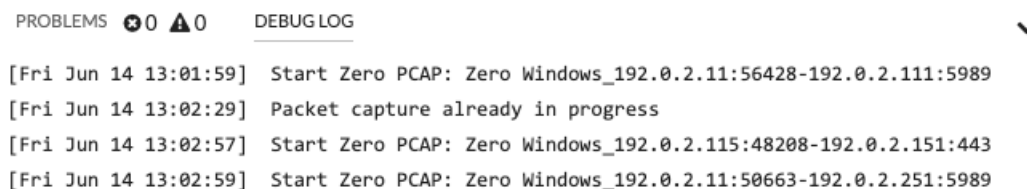
6. Click **Save**.

View debug output in the debug log

In the following steps, you will view the trigger debug output to confirm that the trigger is running and capturing packets. After you assign the trigger to your data sources, the system runs the trigger when HTTP traffic occurs, and if any transactions contain a zero window, the system sends debug results to the debug log.

1. Click the System Settings icon , and then click **Triggers**.
2. Click the **Zero Window PCAP** trigger you just created.
3. Click **Edit Trigger Script**.
4. Click the **Debug Log** tab.

The debug log displays results similar to the following figure:



The screenshot shows a 'DEBUG LOG' tab with a dropdown arrow. Below the tab, there are four log entries:


- [Fri Jun 14 13:01:59] Start Zero PCAP: Zero Windows_192.0.2.11:56428-192.0.2.111:5989
- [Fri Jun 14 13:02:29] Packet capture already in progress
- [Fri Jun 14 13:02:57] Start Zero PCAP: Zero Windows_192.0.2.115:48208-192.0.2.151:443
- [Fri Jun 14 13:02:59] Start Zero PCAP: Zero Windows_192.0.2.11:50663-192.0.2.251:5989

Download and view packet captures


In the following steps, you will download packet captures.



Note: The following steps show how download packets from Reveal(x) Enterprise systems. For information about downloading packets from ExtraHop Performance systems, see [Download packets on ExtraHop Performance systems](#).

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. From the top menu, click **Records**.
3. From the Record Type drop-down list, select **Packet Capture**.
4. After the records associated with your packet capture appear, click the Packets icon , and then click **Download PCAP**.


Download packets on ExtraHop Performance systems

1. Click the System Settings icon , and then click **All Administration**.
2. From the Packet Captures section, click **View and Download Packet Captures**.

The Packet Capture List displays results similar to the following figure:

Packet Capture List

Delete Selected Captures
Download Selected Captures

Name 

- [Zero Windows_192.0.2.246:60849-203.0.113.95:443](#)
 Packets: 562 Bytes: 430286 Duration: 4m53s VLAN: 0 IP Proto: TCP
- [Zero Windows_192.0.2.246:56071-203.0.113.14:443](#)
 Packets: 841 Bytes: 969344 Duration: 35s VLAN: 0 IP Proto: TCP
- [Zero Windows_192.0.2.246:52675-198.51.100.9:443](#)
 Packets: 2603 Bytes: 2990518 Duration: 6s VLAN: 0 IP Proto: TCP

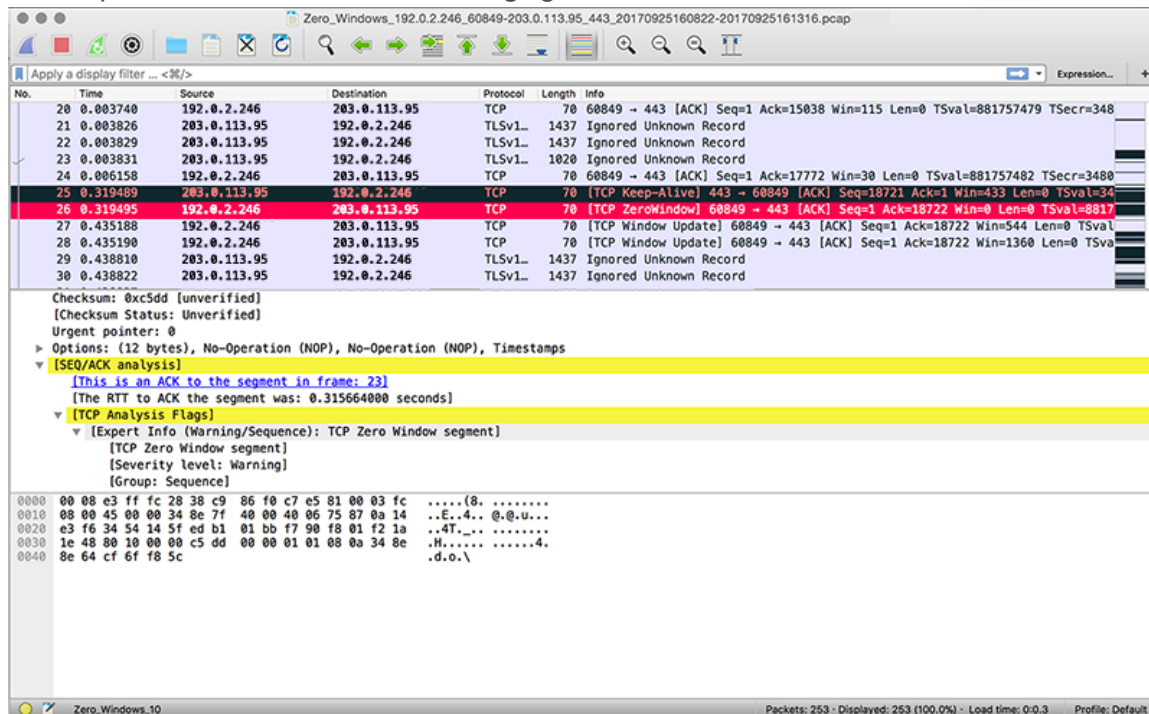
Each packet capture in the list represents a flow of data between devices, and provides information about the devices, ports, and time range to help you narrow down which captures to download.

3. Select any capture named **Zero Windows_** and click **Download Selected Captures**.

The capture is saved to your local machine with the `.pcap` file extension.

4. Open the capture file with a packet analyzer, such as Wireshark.

The output will look similar to the following figure:



No.	Time	Source	Destination	Protocol	Length	Info
20	0.003740	192.0.2.246	203.0.113.95	TCP	70	60849 → 443 [ACK] Seq=1 Ack=15038 Win=115 Len=0 TSval=881757479 TSecr=348
21	0.003826	203.0.113.95	192.0.2.246	TLSv1..	1437	Ignored Unknown Record
22	0.003829	203.0.113.95	192.0.2.246	TLSv1..	1437	Ignored Unknown Record
23	0.003831	203.0.113.95	192.0.2.246	TLSv1..	1020	Ignored Unknown Record
24	0.006158	192.0.2.246	203.0.113.95	TCP	70	60849 → 443 [ACK] Seq=1 Ack=17772 Win=30 Len=0 TSval=881757482 TSecr=3480
25	0.319489	203.0.113.95	192.0.2.246	TCP	70	[TCP Keep-Alive] 443 → 60849 [ACK] Seq=18721 Ack=1 Win=433 Len=0 TSval=34
26	0.319495	192.0.2.246	203.0.113.95	TCP	70	[TCP ZeroWindow] 60849 → 443 [ACK] Seq=1 Ack=18722 Win=0 Len=0 TSval=8817
27	0.435188	192.0.2.246	203.0.113.95	TCP	70	[TCP Window Update] 60849 → 443 [ACK] Seq=1 Ack=18722 Win=544 Len=0 TSval
28	0.435190	192.0.2.246	203.0.113.95	TCP	70	[TCP Window Update] 60849 → 443 [ACK] Seq=1 Ack=18722 Win=1360 Len=0 TSval
29	0.438810	203.0.113.95	192.0.2.246	TLSv1..	1437	Ignored Unknown Record
30	0.438822	203.0.113.95	192.0.2.246	TLSv1..	1437	Ignored Unknown Record

```

Checksum: 0xc5dd [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
  [This is an ACK to the segment in frame: 23]
  [The RTT to ACK the segment was: 0.315664000 seconds]
[TCP Analysis Flags]
  [Expert Info (Warning/Sequence): TCP Zero Window segment]
  [TCP Zero Window segment]
  [Severity level: Warning]
  [Group: Sequence]
0000  08 00 e3 ff fc 28 38 c9 86 f0 c7 e5 01 00 03 fc  ....(8. ....
0010  08 00 45 00 00 34 8e 7f 40 00 40 06 75 87 0a 14  ..E..4.. @.u...
0020  e3 f6 34 54 14 5f ed b1 01 bb f7 90 f8 01 f2 1a  .4T... ..
0030  1e 48 00 10 00 00 c5 dd 00 00 01 01 08 0a 34 8e  .H.....4.
0040  8e 64 cf 6f f8 5c                                .d.o.\
    
```

5. Open packets that indicate a zero window occurrence.

You will see details such as TCP flags, when zero window conditions occurred, the length of each occurrence, and which devices were involved.

Look for patterns in the data and investigate the state of the client and server devices to help you narrow down and resolve the cause.