Initiate precision packet captures to analyze zero window conditions

Published: 2024-04-02

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 system and access administration 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);
}
```
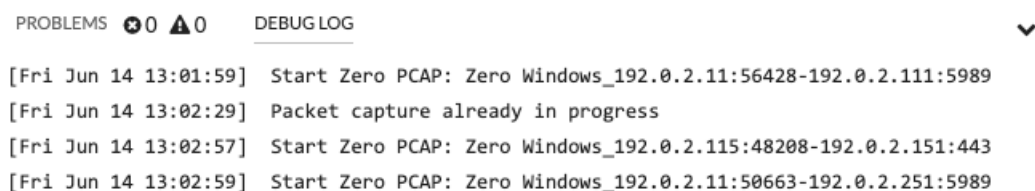
6. Click **Save**.

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:

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. Click **View Records**.
4. From the Record Type drop-down list, select **Packet Capture**.
5. 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**.

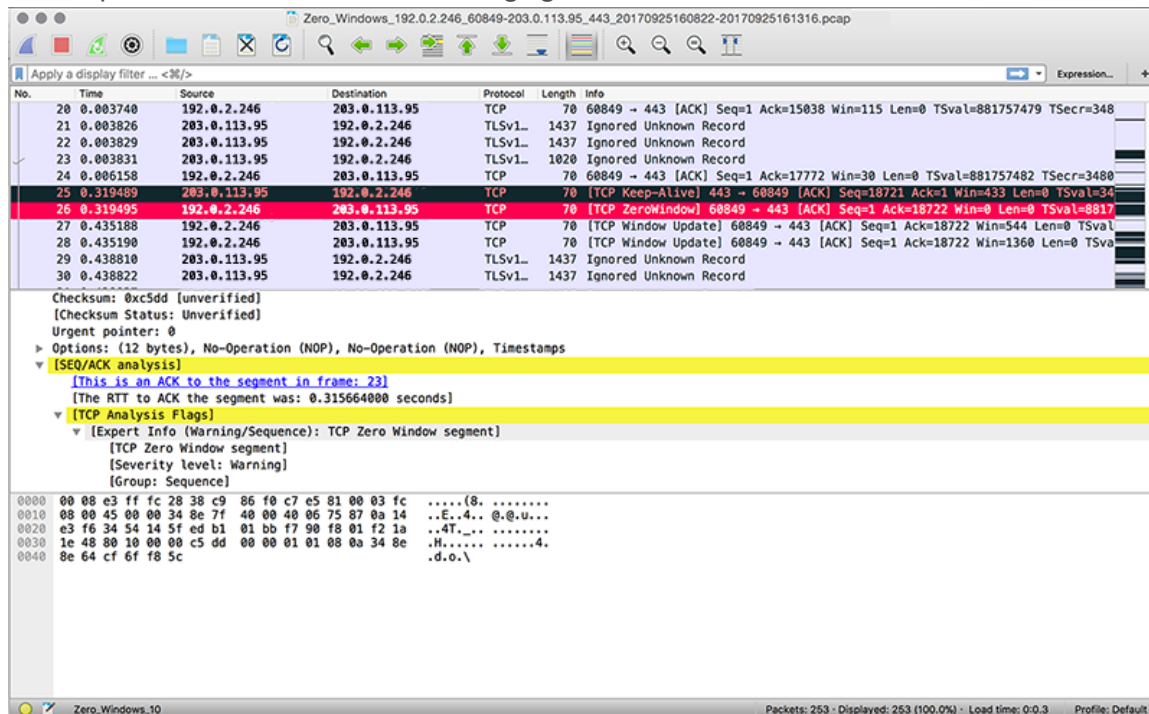   The Packet Capture List displays results similar to the following figure:

   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:

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.