ADVANCED STATEFUL LAYER 4 REPLAY

OVERVIEW

Traffic replay is an effective way to emulate the real-world network conditions to your device under test (DUT) since all the traffic content, packet sizes, inter-packet gap, packet pattern, and burstiness are from reality.

Xena Advanced Layer 4 Replay (XAR) solution provides stateful Layer 4 replay based on payload data from pcap files, high scalability for performance verification, and preserve correlation information across TCP connections for true emulation. XAR pcap parsing allows multiple TCP connections in one pcap, which greatly increases test efficiency and flexibility. Testing your DUT with real-world traffic generates convincing results for in-depth analysis and is effective in revealing the true behavior of the DUT before deploying into the real network.

To have confidence in your DUT and generate convincing results, you need to continuously test the performance of your system. This requires testing with traffic captured in real world with a right replay solution.

“Xena Advanced Layer 4 Replay provides stateful replay on top of its high-performance TCP stack, high scalability for performance verification and preserve correlation information across sessions for true emulation.”
ADVANCED STATEFUL LAYER 4-7 TRAFFIC REPLAY

Contents

Are You Testing with Realistic Traffic? ................................................................. 3
Why is Testing with Real-World Traffic Important to You? .................................. 3
Test with Your Own Captured Traffic .................................................................... 3
Choose the Right Traffic Replay Solution ............................................................. 4
Xena Advanced Layer 4 Replay ................................................................................. 5
Stateful Layer 4 Replay with TCP Stack ............................................................... 6
Advanced PCAP Parsing ......................................................................................... 8
Connection Correlation Should Be Kept ............................................................... 10
High-Performance Traffic Replay That Can Scale ................................................ 11
Features of Xena Advanced Layer 4 Replay .......................................................... 11
Conclusion .............................................................................................................. 12
ARE YOU TESTING WITH REALISTIC TRAFFIC?

How do you ensure that you have enough confidence in your network or system handling internet traffic, attacks, or failure? Over-provisioning is a common solution for many enterprises, cloud providers, and operators to ensure network Quality-of-Service (QoS) and scalability to tackle the ever-increasing bandwidth demand both on hardware and software. However, over-provisioning is expensive and is not a sustainable solution. Proper planning and testing can prevent spending unnecessary resources on over-provisioning and result in much better efficiency.

Why is Testing with Real-World Traffic Important to You?

There are two Layer 4-7 testing methods to verify your network architecture design or your system implementation: testing with simulation (analytic models) or testing with real-world traffic (traffic replay). A simulated test provides the basic behavior of a network, but may not necessarily obey all the reality being simulated. It can only give you an idea about how a system works. For some tests such as a connection-per-second test, a simulated test solution can be efficient and powerful. However, when testing stateful Layer 4-7 devices, such as next-generation firewalls (NGFW), intrusion prevention/detection systems (IPS/IDS), network packet brokers (NPB), etc., simulated traffic is far from enough to gain true insights into those stateful application-aware devices or content-aware networks. Thus, you need real-world traffic.

Test with Your Own Captured Traffic

Reproducing the real-world traffic using the method of traffic replay onto the device or system under test (DUT/SUT) is one of the most effective and convincing test solutions to produce meaningful results and verify the performance of those computation-intensive devices before and after deployed in the network. The main idea is simple: you record your network traffic into a
standardized format file and replay the TCP connections onto your DUT/SUT to test its performance or functionalities.

However, without a proper test solution and a systematic methodology, it is difficult to effectively reproduce something that makes sense to your network, not to mention producing meaningful results or concluding convincing decisions. You need to choose the right traffic replay platform to reproduce reality again and again to test your DUT/SUT so that you don’t end up with an expensive lesson later in the production phase.

The biggest challenge faced by a variety of test solutions to date is how to replay traffic with highest level of realism. A high-level realistic traffic replay should retain the important correlation information between the mixture of TCP connections seen from a client rather than simply simulating based on superficial assumptions and models. When it comes to having confidence in the test results from your DUT/SUT, you need to provide solid proofs with a systematic test methodology. Tests should generate accurate realistic and stateful end-user traffic otherwise the performance of the DUT/SUT can potentially be misjudged, resulting in a false positive conclusion.

**CHOOSE THE RIGHT TRAFFIC REPLAY SOLUTION**

Traffic replay is an effective way to emulate the real-world network conditions to your DUT/SUT since all the traffic content, packet sizes, inter-packet gap, packet pattern, and burstiness are from reality.

However, a right replay solution should provide Layer 4 replay based on data from pcap files on top of a TCP stack instead of Layer 3 replay that uses stateless technologies to emulate a stateful network behavior. Anything related to network topology changes, congestion control, retransmission, out-of-order segments, and QoS should be handled automatically by the TCP stack itself. The replay solution should always respect the time and sequence information contained in pcap files. Not all TCP connections should be started at the same time because some are in fact triggered by others. The correlation information is vital if you want to verify the
application analysis ability or any intelligent monitoring capability of you DUT/SUT. A right replay solution should provide high performances in terms of number of concurrent TPC connections (CC) and number of TCP connections per second (CPS) in order to stress-test the DUT/SUT for performance verification under various network loads.

**XENA ADVANCED LAYER 4 REPLAY**

Xena Advance Layer 4 Replay (XAR) is built on top of its high-performance TCP stack. This enables you to test with true emulation. XAR reconstructs an overview of all the TCP connections and UDP flows. SYN, ACK, FIN, etc. are filtered out, leaving only TCP payload for replay. Extracting the TCP payload, XAR follows the sequential order and establishes/closes TCP connections on-the-fly. Thus, there is no need to pre-calculate a static RTT.

More, XAR parses and analyzes the pcap file. The powerful parsing feature of XAR not only allows you to use the off-the-shelf application traffic library, XenaAppMix (XAM), to create various scenarios for application emulation, but also provides a platform for bring-your-own-traffic (BYOT). You can recreate the entire application sessions on a client with only one pcap because the advanced parsing of XAR allows more than one TCP connections per IP address in a pcap. BYOT also allows you to create an even more complex application mixes if capturing traffic at the egress of a WAN device.

To truly emulate the traffic captured in a pcap file, the correlation information of different TCP connections is preserved and replayed as is. This generates convincing results and is especially important for stateful Layer 4-7 devices testing.

Performance verification requires a power TCP stack that can support millions of concurrent TCP connections and can push the DUT’s performance to its limit. With XAR, you can scale up your pcap replay to fully load your DUT with various TCP connections to test the capacity, stability and performance.
Stateful Layer 4 Replay with TCP Stack

Some open-source solutions (TRex for instance) claim to be stateful Layer 4 replay, however, they should be considered stateless replay with schedulers rather than true stateful due to lack of TCP stack support. Without a TCP stack, the test is in fact stateless in terms of generating traffic because you have to simulate client-server dialogs, and thus you have to manually pre-calculate a round-trip time (RTT) between the client and the server roles in order to artificially schedule the transmission order of packets to prevent the out-of-sequence problem. If the RTT time is misconfigured when a DUT/SUT is in place, for instance, the server may send a response before it receives a request (RTT too low), or the delay is too high to generate any meaningful results (RTT too high). This significantly limits the flexibility of the test solution. Figure 1 demonstrates this problem. In addition, with no TCP stack support, these replay solutions must artificially replay the TCP handshake and tear-down process, resulting in low operability and flexibility for you.

![Lack of TCP Stack](image)

\[Figure 1. Lack of TCP stack support requires manually pre-calculation of round-trip time (RTT) between the client and the server. Misconfiguration will lead to invalid tests.\]
On the contrary, with a powerful TCP stack, Xena Advanced Layer 4 Replay (XAR) provides an advanced solution. By parsing and analyzing the pcap files in advance to the replay, XAR reconstructs an overview of all the TCP connections and UDP flows. SYN, ACK, FIN, etc. are filtered out, leaving only TCP payload for replay. Extracting the TCP payload, XAR follows the sequential order and establishes/closes TCP connections on-the-fly. Thus, there is no need to pre-calculate a static RTT. The server will not send a response before a request from the client is actually received, which enables the test to adapt to network changes. TCP parameters such as congestion control, flow control, MSS, ACK timeout, maximum retransmission, etc. are fully configurable, providing great flexibility.

Once the lost packet is correctly received, XAR will resume sending the next packet. This ensures...
a successful replay instead of continuing with meaningless traffic. Depending on different bit error rates and packet drop performances, the number of retransmission tries can be greatly different from one DUT/SUT to another. Thus, what is actually replayed onto the DUT/SUT can be different from what is recorded in the pcap due to the fact that network conditions of the real-world network where traffic is captured and the DUT/SUT are different. In case of the same timestamp values found in the pcap due to time resolution, XAR replay the packet as quickly as it can. Advantages of XAR are shown in Table 1.

Table 1. Advantages of Xena Advanced Layer 4 Replay

<table>
<thead>
<tr>
<th>Features</th>
<th>Replay with No TCP Stack</th>
<th>Xena Advanced Layer 4 Replay</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP stack support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Free of pre-calculating RTT</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Retransmission in case of packet loss</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ability to adapt to testbed changes dynamically</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>TCP parameters configuration</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Accurate Layer 4 statistics</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

As shown in the example from Figure 2, XAR parses and analyzes the pcap file and extract the payload for replay. In the pcap file, two TCP connections are found. For a new TCP connection, XAR starts a new TCP three-way handshake and replay the TCP payload when the connection is established. Replay follows in the same sequential packet order recorded in the pcap file. When an HTTP/1.1 200 OK segment is lost, XAR stops progressing to the next packet and starts retransmitting the lost packet from the server side. Until an ACK from the client is received by the server, XAR will not resume to replay the next packet.

**Advanced PCAP Parsing**

Capturing traffic at a client generates a pcap file containing one source IP address and many TCP connections due to different applications running on the client PC. This typical one-client-many-serves scenario is useful when scaling up to multiple clients for a realistic replay.

XAR advanced pcap parser analyzes the file uploaded and is able to discover the one-client-many-server communication pattern. This means, with only one pcap file, you can easily recreate the entire sessions of different applications running on a client as shown in Figure 3. In XAR, the concept of a user refers to multiple TCP connections with one source IP address, which is a typical scenario of a regular PC client.
Comparing to solutions where multiple pcap files have to be loaded in order to recreate a full-fledged client-to-server communication, this vital advantage of using XAR makes it highly efficient for Layer 4 replay.

Figure 3. Multiple TCP connections captured in one pcap file for replay recreates entire applications on a client with XAR.

What more exciting with is that, you can replay a large group of clients with only one pcap file, if you capture the traffic at the egress side of the WAN/NAT as shown in Figure 4. Due to the NAT function in the WAN router, the egress communication is considered as one to other networks. A pcap file captured there will contain not only one client-to-server application sessions, but many of them. With the advanced pcap parsing of XAR, you can replay this more complex traffic composition on top the high-performance TCP stack.

Figure 4. Entire group of clients traffic captured in one pcap file for replay recreates the entire network traffic with XAR.
**Connection Correlation Should Be Kept**

Simply replaying traffic content/payload is not good enough to generate convincing verification results. You should not only consider what are replayed (traffic composition), but also how the traffic is transmitted (traffic sequence). It is extremely important to keep the correlation information between TCP connections and the relative timing information in the pcap file. It is because the TCP connections are not independent from one another or simply interleaved by a mixer, but highly correlated. Failing to provide this valuable information in a test will damage the relevance and credibility of the test results. Thus, a test solution should be able to recreate the traffic complying with the realistic sequences, timings and payload contents/sizes. This can generate results at a much higher convincing level than creating TCP connections at the same time. As shown in Figure 5, the second HTTP session is triggered by the HTML page content so it will not produce legitimate traffic if the two TCP connections are established at the same time.

Ensuring that real network testing is performed and results analyzed becomes the key for providing guaranteed Quality-of-Service (QoS), and high degrees of Quality-of-Experience (QoE). Traffic generated by wrong replay solutions is easy to identify as unreasonable traffic, sabotaging the trustability of the test results.

Test solutions should allow users to replay the traffic captured from real networks with the ability to customize. This means you can configure your tests with true realism. The test solution should automatically adjust its traffic behaviors based on your input and generate traffic that is usually seen on real networks, e.g. negotiate maximum TCP segment size.
High-Performance Traffic Replay That Can Scale

Many enterprises rely on the security and monitoring devices (NGFW, IPS/IDS, NBP) to increase visibility and protect their data from leaking or network from being paralyzed by distributed denial-of-service (DDoS) attacks. Verifying the performance of Layer 4-7 network devices is critical to enterprises because these stateful devices can be the throughput bottleneck by poor policy planning and configuration, degrading the overall QoS and user experience.

Using traffic captured from real networks to verify the performance of stateful DUTs generates convincing results for in-depth analysis. Under many circumstance, the best way to test the performance is to use traffic that matches the actual characteristics of expected traffic.

XAR is capable of scaling up using a snapshot of a network traffic condition to emulate high-volume network load. DUT when put under various network loads can demonstrate different behavior (stability issue). It is vital to stress-test a DUT with not only a few sessions but tens of millions in order to push it to the limit to verify the performance. For enterprises, any new deployment or software/firmware upgrade should always be tested and evaluated before roll-out in order to ensure that the system works properly. The testbed should attempt to replicate the production network as close as possible, which includes the network topology, network traffic that traverses through the device. The DUT/SUT should provide strong performance under all circumstances.

FEATURES OF XENA ADVANCED LAYER 4 REPLAY

XAR provides a powerful and flexible Layer 4 replay test solution to you with many features such as:

- Layer 4 traffic replay on top of a high-performance TCP stack.
No need to pre-calculate RTT. Retransmission in case of packet loss or out-of-order is handled automatically by the TCP stack.

- Sequential replay of packets.
- Pcap parsing and analysis allows more than one TCP connection per IP address.
- Allows you to use the off-the-shelf application traffic library, XenaAppMix (XAM), to create various scenarios for application emulation, but also provides a platform for bring-your-own-traffic (BYOT).
- Ability to process multiple pcap files to create and replay your own application over TCP/UDP.
- Inter-TCP connection correlation is preserved and replayed for realistic emulation.
- Easy to scale up from one user (multiple TCP connections with one source IP address) to millions of users for performance testing.
- Ability to control inter-TCP connection timings of the original capture to test the effect of bandwidth, latency and timing variations.
- TCP/IP parameters can be modified.

**CONCLUSION**

Replay solutions based on schedulers or ignoring the correlations among sessions often fails to suffice the need for convenience and accuracy due to the potential incompatibility between manual configuration and network condition changes. Besides, it is difficult to maintain the credibility of the test results using such a mechanism, not to mention measuring the true performance of the DUT/SUT. It is also risky to rely on inaccurate test results because failures due to lack of valid testing in the production environment will lead to expensive consequences.

To have confidence in your DUT/SUT and generate convincing results, you need to continuously test the performance of your system. This requires testing with traffic captured in real world. Testing your DUT/SUT with real-world traffic generates convincing results for in-depth analysis and is effective in revealing the true behavior of the DUT/SUT before deploying into the real network. Xena Advanced Layer 4 Replay (XAR) provides a true stateful traffic replay on top its high-performance TCP stack and allows multiple TCP connections in one pcap, allowing you to test with maximum flexibility and efficiency. With the high scalability of XAR, you can scale one user traffic (multiple TCP connections per source IP address) up to millions for performance verification. With XAR preserving the correlation information across TCP connections, you are able to recreate the realistic network scenario.