Mitigating UDP Abuses

Collins Khuu, Tucker Baron
Advisors: Jorge Crichigno, Jose Gomez

Department of Integrated Information Technology
University of South Carolina

Tuesday, December 2nd, 2021
Agenda

• Purpose.

• Introduction.

• Problem description.

• Proposed solution and implementation.

• Conclusion.
Purpose

• Understand UDP’s lack of flow control.

• Understand QoS Policy rules.

• Understand UDP abuse attacks.

• Understand how to mitigate UDP abuse attack using a next generation Palo Alto firewall.
Introduction

• UDP (User Datagram Protocol) does not implement any congestion control mechanisms.
  • UDP can be unreliable since it does not enforce that all the packets are delivered correctly.
  • Often used in audio / video streaming and online games.

• In contrast, TCP (Transmission Control Protocol) can handle congestion over networks.
  • TCP is more reliable than UDP and ensures that all the packets are delivered correctly.
Background Information

- Palo Alto Next-generation Firewalls.
- QoS (Quality of Service) is used to achieve outcomes such as:
  - Allocating bandwidth.
  - Prioritizing network / application traffic.

Figure 1. QoS Traffic Flow
Source: PAN-OS® Administrator's Guide
Problem Description

• Without congestion control, application using UDP generates traffic at a high rate.
  • Overflows at routers, switches, and other network devices.
  • Unfair bandwidth allocations and starvation within a network.
• Network devices are prone to UDP abuse attacks.

Figure 2. Network Topology
Proposed Solution and Implementation

- UDP abuse attacks can be mitigated through NGFWs.
  - Configure default QoS profile class egress and priority.
  - Create QoS policy.
  - Apply QoS profile to the relevant interface.

<table>
<thead>
<tr>
<th>Name</th>
<th>Guaranteed Egress (Mbps)</th>
<th>Maximum Egress (Mbps)</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>0.000</td>
<td>0.000</td>
<td>real-time</td>
</tr>
<tr>
<td>class1</td>
<td>0.000</td>
<td>0.000</td>
<td>high</td>
</tr>
<tr>
<td>class2</td>
<td>0.000</td>
<td>0.000</td>
<td>high</td>
</tr>
<tr>
<td>class3</td>
<td>0.000</td>
<td>0.000</td>
<td>medium</td>
</tr>
<tr>
<td>class4</td>
<td>0.000</td>
<td>0.000</td>
<td>medium</td>
</tr>
<tr>
<td>class5</td>
<td>0.000</td>
<td>0.000</td>
<td>low</td>
</tr>
<tr>
<td>class6</td>
<td>0.000</td>
<td>0.000</td>
<td>low</td>
</tr>
<tr>
<td>class7</td>
<td>0.000</td>
<td>0.000</td>
<td>low</td>
</tr>
<tr>
<td>class8</td>
<td>0.000</td>
<td>200.000</td>
<td>low</td>
</tr>
</tbody>
</table>

*Figure 3. Adjusted QoS Default Profile*
Proposed Solution and Implementation

- UDP abuse attacks can be mitigated through NGFWs.
  - Configure default QoS profile class egress and priority.
  - Create QoS policy.
  - Apply QoS profile to the relevant interface.

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Source Zone</th>
<th>Source Address</th>
<th>Source User</th>
<th>Destination Zone</th>
<th>Destination Address</th>
<th>Application</th>
<th>Service</th>
<th>DSCP/Tos</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>my_QoS_Policy</td>
<td>none</td>
<td>Outside</td>
<td>any</td>
<td>any</td>
<td>inside</td>
<td>any</td>
<td>any</td>
<td>ipports_UDP</td>
<td>any</td>
<td>8</td>
</tr>
</tbody>
</table>

**Figure 4. QoS Policy**

<table>
<thead>
<tr>
<th>Name</th>
<th>Guaranteed Egress (Mbps)</th>
<th>Maximum Egress (Mbps)</th>
<th>Profile</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet1/1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunneld Traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clear Text Traffic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5. QoS Profile for ethernet1/1**
Results

• The resulting bitrates of UDP.

Figure 6. Result after two minute iperf3 test
Conclusion

• A next-generation firewall is an effective measure in mitigation of a UDP abuse attack.
• This QoS Policy can be applied to many different network topologies, and the rate of UDP flow can be set according to the available bandwidth of the network.