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

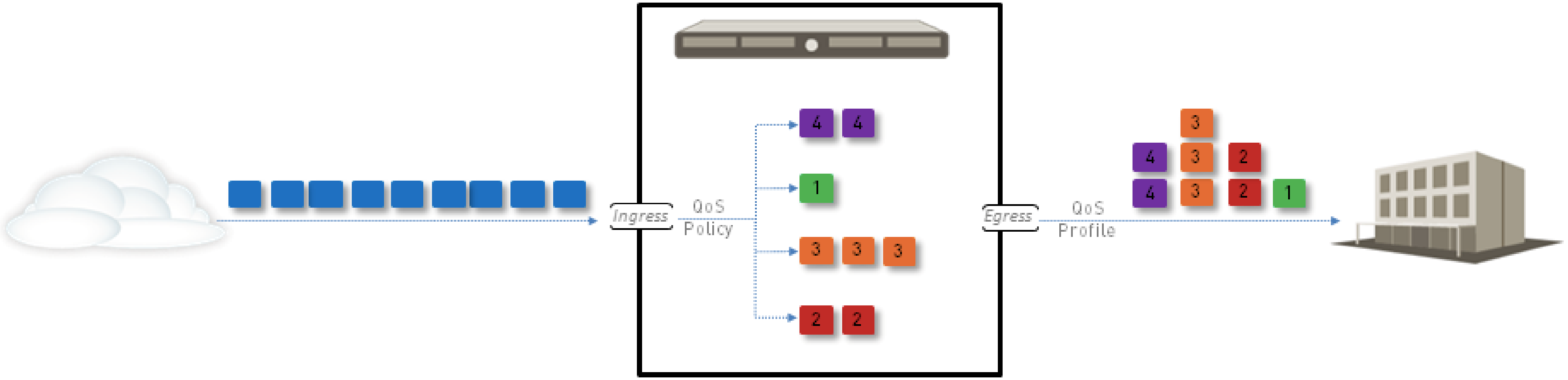
- Understand UDP’s lack of flow control.
- Understand QoS Policy rules.
- Understand UDP abuse attacks.
- Understand how to mitigate UDP abuse attack using a next generation Palo Alto firewall.

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.



Unclassified traffic enters the firewall.

The QoS policy identifies traffic and associates it with a QoS class.

At the egress interface, the QoS profile prioritizes and limits traffic according to its QoS class.

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.

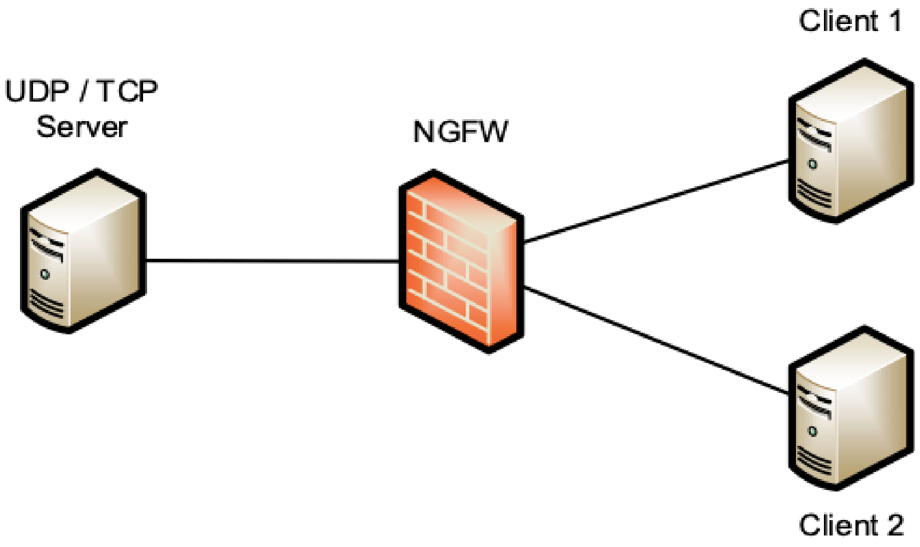
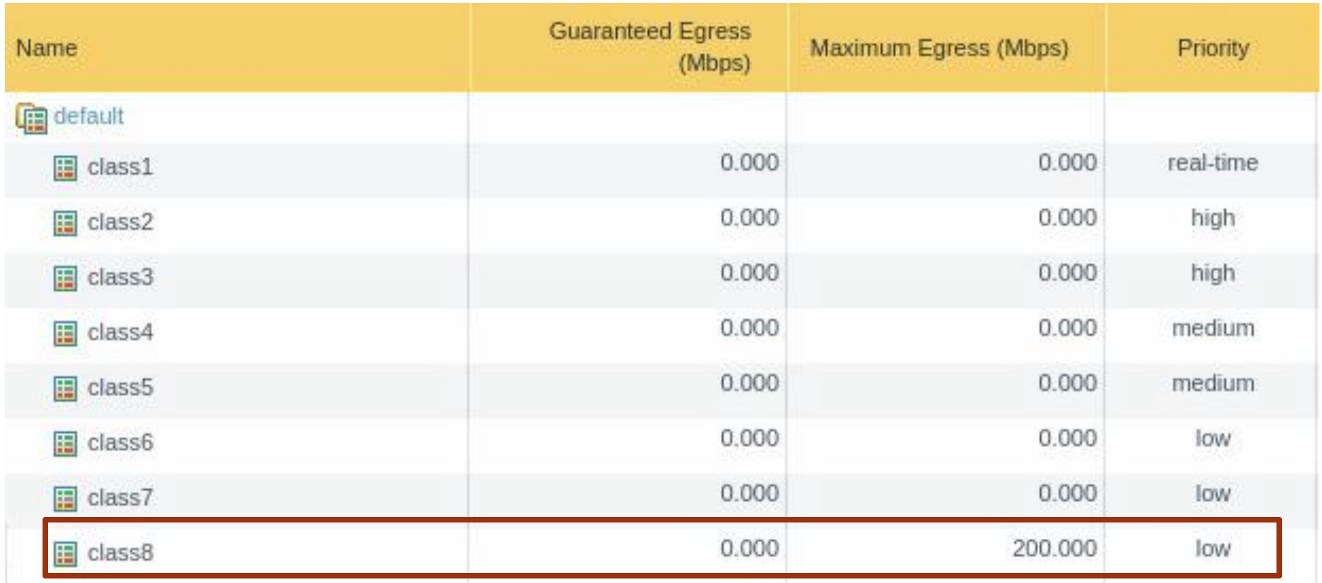


Figure 2. Network Topology

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.

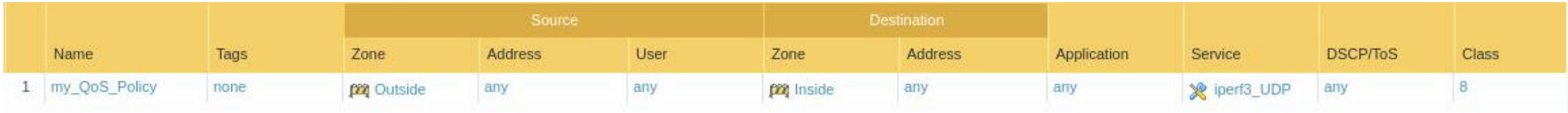


Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Priority
default			
class1	0.000	0.000	real-time
class2	0.000	0.000	high
class3	0.000	0.000	high
class4	0.000	0.000	medium
class5	0.000	0.000	medium
class6	0.000	0.000	low
class7	0.000	0.000	low
class8	0.000	200.000	low

Figure 3. Adjusted QoS Default Profile

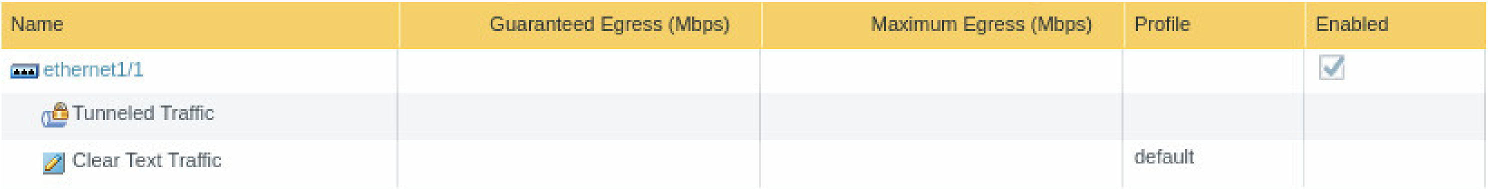
Proposed Solution and Implementation

- 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.



			Source			Destination					
	Name	Tags	Zone	Address	User	Zone	Address	Application	Service	DSCP/ToS	Class
1	my_QoS_Policy	none	Outside	any	any	Inside	any	any	iperf3_UDP	any	8

Figure 4. QoS Policy

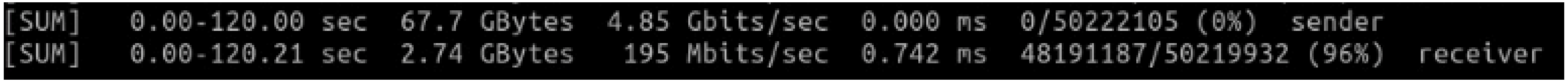


Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Profile	Enabled
ethernet1/1				☑
Tunneled Traffic				
Clear Text Traffic			default	

Figure 5. QoS Profile for ethernet1/1

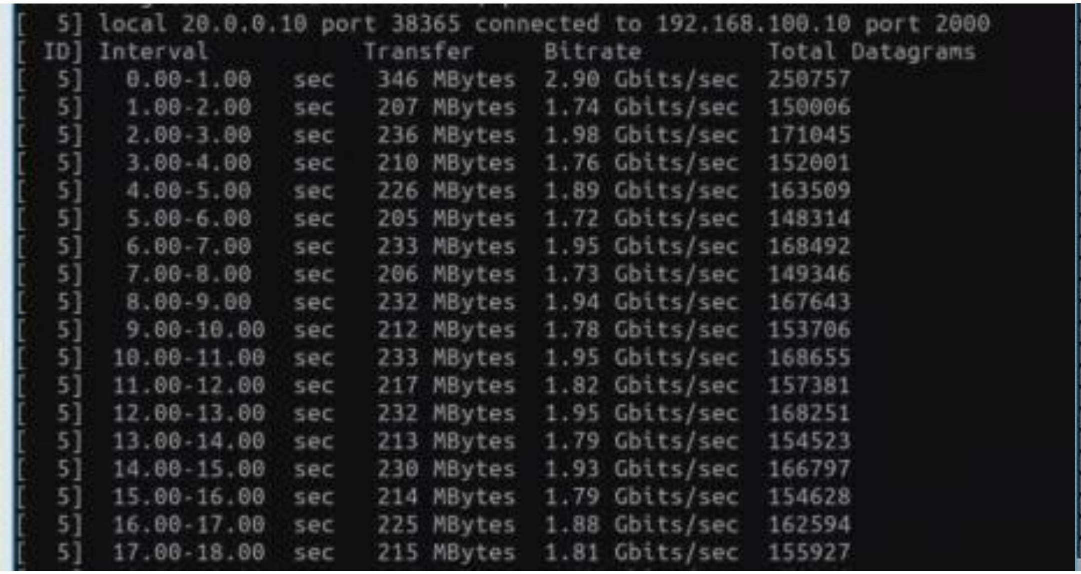
Results

- The resulting bitrates of UDP.

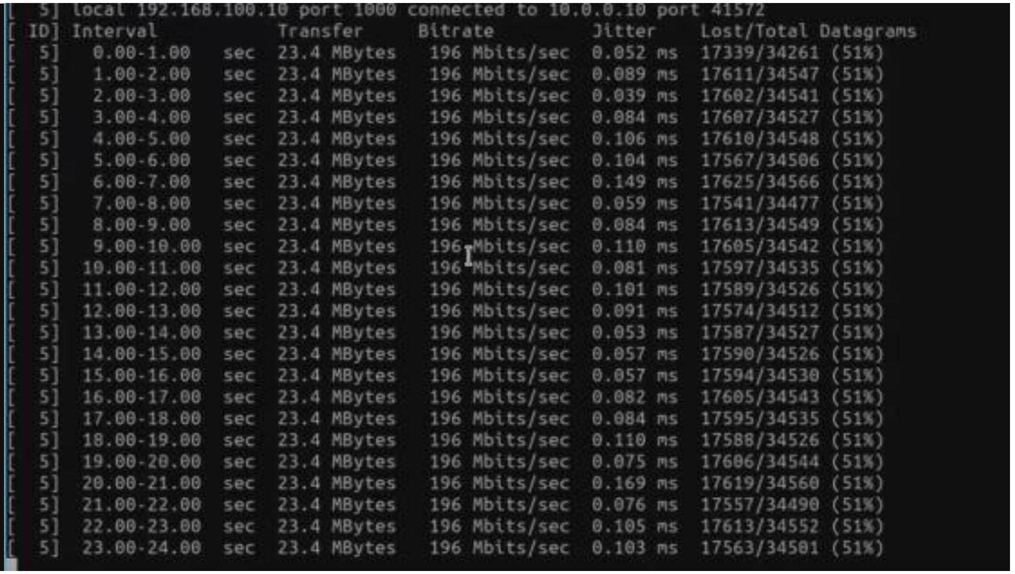


```
[SUM]   0.00-120.00 sec  67.7 GBytes  4.85 Gbits/sec  0.000 ms  0/50222105 (0%)  sender
[SUM]   0.00-120.21 sec  2.74 GBytes   195 Mbits/sec  0.742 ms  48191187/50219932 (96%)  receiver
```

Figure 6. Result after two minute iperf3 test



```
[  5] local 20.0.0.10 port 38365 connected to 192.168.100.10 port 2000
[ ID] Interval           Transfer     Bitrate         Total Datagrams
[  5]   0.00-1.00   sec   346 MBytes  2.90 Gbits/sec  250757
[  5]   1.00-2.00   sec   207 MBytes  1.74 Gbits/sec  150006
[  5]   2.00-3.00   sec   236 MBytes  1.98 Gbits/sec  171045
[  5]   3.00-4.00   sec   210 MBytes  1.76 Gbits/sec  152001
[  5]   4.00-5.00   sec   226 MBytes  1.89 Gbits/sec  163509
[  5]   5.00-6.00   sec   205 MBytes  1.72 Gbits/sec  148314
[  5]   6.00-7.00   sec   233 MBytes  1.95 Gbits/sec  168492
[  5]   7.00-8.00   sec   206 MBytes  1.73 Gbits/sec  149346
[  5]   8.00-9.00   sec   232 MBytes  1.94 Gbits/sec  167643
[  5]   9.00-10.00  sec   212 MBytes  1.78 Gbits/sec  153706
[  5]  10.00-11.00  sec   233 MBytes  1.95 Gbits/sec  168655
[  5]  11.00-12.00  sec   217 MBytes  1.82 Gbits/sec  157381
[  5]  12.00-13.00  sec   232 MBytes  1.95 Gbits/sec  168251
[  5]  13.00-14.00  sec   213 MBytes  1.79 Gbits/sec  154523
[  5]  14.00-15.00  sec   230 MBytes  1.93 Gbits/sec  166797
[  5]  15.00-16.00  sec   214 MBytes  1.79 Gbits/sec  154628
[  5]  16.00-17.00  sec   225 MBytes  1.88 Gbits/sec  162594
[  5]  17.00-18.00  sec   215 MBytes  1.81 Gbits/sec  155927
```



```
[  5] local 192.168.100.10 port 1000 connected to 10.0.0.10 port 41572
[ ID] Interval           Transfer     Bitrate         Jitter    Lost/Total Datagrams
[  5]   0.00-1.00   sec  23.4 MBytes   196 Mbits/sec  0.052 ms  17339/34261 (51%)
[  5]   1.00-2.00   sec  23.4 MBytes   196 Mbits/sec  0.089 ms  17611/34547 (51%)
[  5]   2.00-3.00   sec  23.4 MBytes   196 Mbits/sec  0.039 ms  17602/34541 (51%)
[  5]   3.00-4.00   sec  23.4 MBytes   196 Mbits/sec  0.084 ms  17607/34527 (51%)
[  5]   4.00-5.00   sec  23.4 MBytes   196 Mbits/sec  0.106 ms  17610/34548 (51%)
[  5]   5.00-6.00   sec  23.4 MBytes   196 Mbits/sec  0.104 ms  17567/34506 (51%)
[  5]   6.00-7.00   sec  23.4 MBytes   196 Mbits/sec  0.149 ms  17625/34566 (51%)
[  5]   7.00-8.00   sec  23.4 MBytes   196 Mbits/sec  0.059 ms  17541/34477 (51%)
[  5]   8.00-9.00   sec  23.4 MBytes   196 Mbits/sec  0.084 ms  17613/34549 (51%)
[  5]   9.00-10.00  sec  23.4 MBytes   196 Mbits/sec  0.110 ms  17605/34542 (51%)
[  5]  10.00-11.00  sec  23.4 MBytes   196 Mbits/sec  0.081 ms  17597/34535 (51%)
[  5]  11.00-12.00  sec  23.4 MBytes   196 Mbits/sec  0.101 ms  17589/34526 (51%)
[  5]  12.00-13.00  sec  23.4 MBytes   196 Mbits/sec  0.091 ms  17574/34512 (51%)
[  5]  13.00-14.00  sec  23.4 MBytes   196 Mbits/sec  0.053 ms  17587/34527 (51%)
[  5]  14.00-15.00  sec  23.4 MBytes   196 Mbits/sec  0.057 ms  17590/34526 (51%)
[  5]  15.00-16.00  sec  23.4 MBytes   196 Mbits/sec  0.057 ms  17594/34530 (51%)
[  5]  16.00-17.00  sec  23.4 MBytes   196 Mbits/sec  0.082 ms  17605/34543 (51%)
[  5]  17.00-18.00  sec  23.4 MBytes   196 Mbits/sec  0.084 ms  17595/34535 (51%)
[  5]  18.00-19.00  sec  23.4 MBytes   196 Mbits/sec  0.110 ms  17588/34526 (51%)
[  5]  19.00-20.00  sec  23.4 MBytes   196 Mbits/sec  0.075 ms  17606/34544 (51%)
[  5]  20.00-21.00  sec  23.4 MBytes   196 Mbits/sec  0.169 ms  17619/34560 (51%)
[  5]  21.00-22.00  sec  23.4 MBytes   196 Mbits/sec  0.076 ms  17557/34490 (51%)
[  5]  22.00-23.00  sec  23.4 MBytes   196 Mbits/sec  0.105 ms  17613/34552 (51%)
[  5]  23.00-24.00  sec  23.4 MBytes   196 Mbits/sec  0.103 ms  17563/34501 (51%)
```

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.