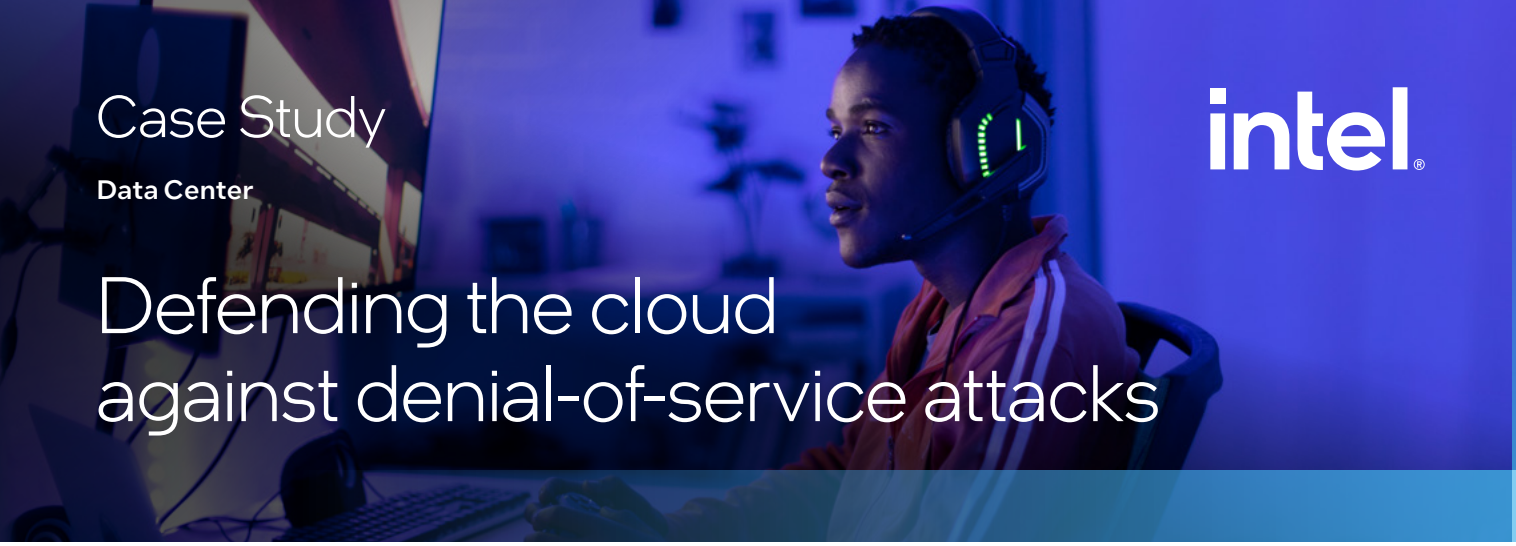

Case Study

Data Center

Defending the cloud against denial-of-service attacks

Cloud service provider Gcore worked with Intel to develop a traffic filtering solution. It aims to defend customers against TCP SYN flood attacks and attacks that mimic UDP game traffic.

At a glance:

- Gcore developed its own distributed denial-of-service (DDoS) filtering solution, based on 3rd Generation Intel® Xeon® Scalable processors and 100GbE Intel® Ethernet Network Adapter E810. Intel® Hyperscan enabled high-performance pattern matching across data streams.
- Intel provided expert insight, including on the Express Data Path (XDP) technology that was used for packet filtering.
- Using the new software on the latest 3rd Generation Intel® Xeon® Scalable processors has increased the filtering capacity from 100 Gbps to up to 400 Gbps per alliance[1].

To protect its customers against DDoS attacks, Gcore needed robust protection. However, the intensity of attacks was doubling each year and it was not sustainable to keep doubling the license fee payments. The company developed its own solution, working with its customers Wargaming and Intel. 3rd Generation Intel® Xeon® Scalable processors and 100GbE Intel® Ethernet Network Adapter E810 cards deliver the performance required.

Challenge

- Gcore needed to double its DDoS protection capacity each year to keep pace with the rising threat but could not afford to double the license fees for its commercial solution each year.

Solution

- Gcore built its own DDoS filtering solution, which can be hosted on its content delivery network (CDN).
- 3rd Generation Intel® Xeon® Scalable processors and 100GbE Intel® Ethernet Network Adapter E810 cards were used for high-performance packet filtering.
- The Intel team brought expertise on Intel® technologies, the Express Data Path (XDP) packet filtering technology and performance optimization.

Results

- The new in-house solution was as performant as the previous commercial solution, and in some respects achieved higher performance.
- The new solution can be hosted across Gcore's 1,000 node content delivery network (CDN), providing scalability to keep pace with the DDoS threat.
- Gcore will make substantial savings in license fees by migrating away from its previous commercial solution.

Defending the cloud against targeted attacks

In a distributed denial-of-service (DDoS) attack, someone attempts to bring down a web service by overwhelming it with traffic. Cloud service providers, such as Gcore, must build defenses to protect their clients.

Gcore originally used software appliances based on the Data Plane Development Kit (DPDK) to filter out illegitimate traffic. The solution used industry-standard servers, but those servers could not be used for other software at the same time.

The software appliances had significant limitations. "All the traffic for customers had to pass through the protection system," said Ivan Koveshnikov, Lead Software Engineer at Gcore. "We had to build our network to the design set out by the DDoS protection creators, and we had to maintain a lot of connections to achieve high performance."

Gcore had seen the ferocity of attacks increase significantly. "Two years ago, we suffered from 300 to 400 Gbps attacks," said Andrew Slastenov, Product Manager, Security, Gcore. "Now, we're seeing attacks of 700 Gbps and the biggest attack we've seen was 1.4 TB per second. To keep up with the increasing power of DDoS attacks, we need to at least double our DDoS protection each year. The software license for our DDoS solution costs a lot, and it's not sustainable to double our license fees each year."

One of Gcore's customers is Wargaming, a company that provides immersive, graphically rich combat simulators including World of Tanks, World of Warships, and World of Warplanes. Wargaming relies on Gcore's content delivery network of 1,000 servers worldwide to provide a fast and responsive service to players.

"We constantly face the threat of DDoS attacks," said Dmitry Kuryanovich, Head of Maintenance, Wargaming. "Part of the puzzle is that vendors do not all have the same quality of protection around the globe. Some have good coverage in the US and Europe, but not a strong presence in the Middle East. In the US, our previous vendor had a significant lag because we were hosted a long way from their data center. That affected the user experience even if we survived the attack. The ping time is important for gaming companies, especially during battles."

In 2020, Wargaming experienced a sustained attack of 200 Gbps to 440 Gbps over a period of a month. "It was a planned and well-designed attack against us," said Kuryanovich. "It resulted in downtime several times, which is frustrating for our customers. We had to increase our protection in stages. First, we had to protect the service so it would not go down. Then, we had to ensure we were not dropping any players. Finally, we achieved full protection."

Wargaming's gaming traffic is particularly hard to filter because it is encrypted and uses the User Datagram Protocol (UDP). "The attacks mimicked our gaming traffic," said Kuryanovich. "There's no easy way to understand what is legitimate traffic and what is fake."

As well as the attacks on its gaming servers, Wargaming needed protection for the servers that host its websites. These servers use the Transmission Control Protocol (TCP). One common type of attack is a TCP SYN flood attack, in which the attacking server initiates a series of connections to the server under attack but does not acknowledge the response (see Figure 1). This results in the server under attack allocating resources to half-open connections. When there are enough of these half-open connections, they consume so many resources that the server cannot connect to legitimate clients.

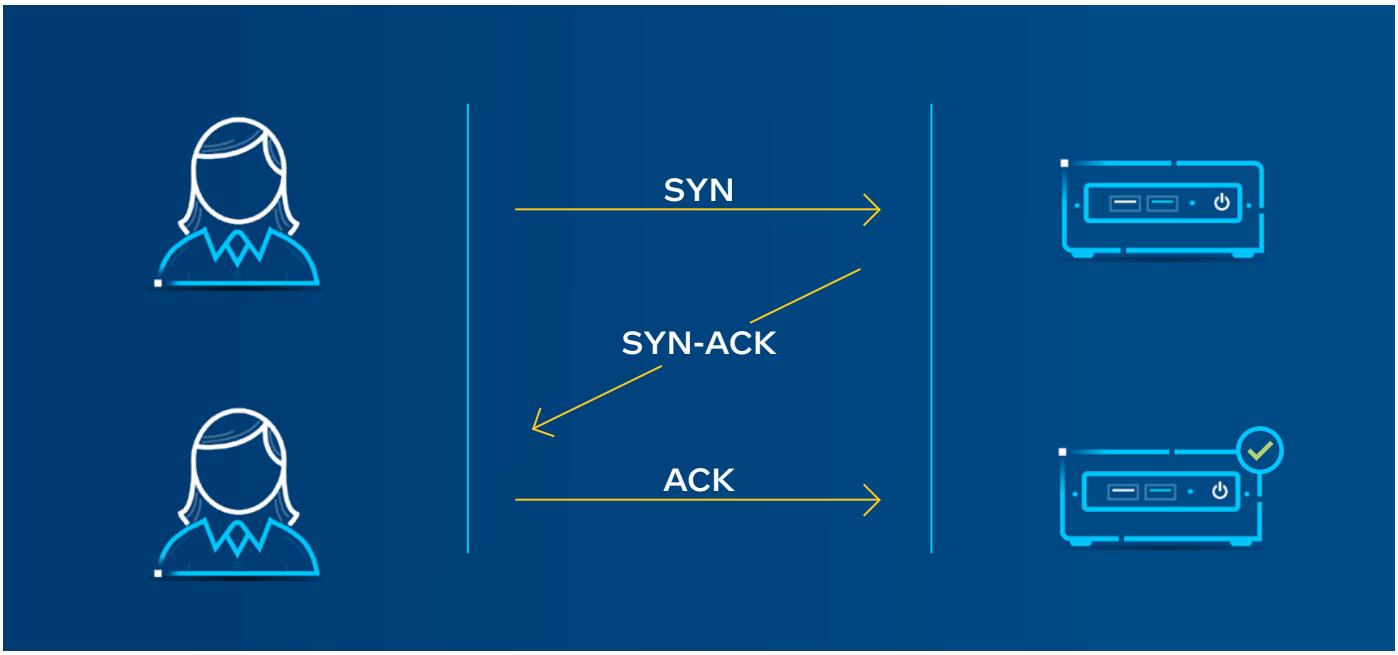

Figure 1: The normal process of connecting to a server using TCP's three-way handshake. A TCP SYN flood attack works by sending many SYN packets but not sending the ACK packets to establish the connections. This results in half-open connections that consume server resources.

Solution details

Gcore decided to build its own DDoS filtering solution, which could be hosted on the 1,000 nodes of its content delivery network (CDN). Instead of dedicating powerful servers to DDoS filtering, the idea was to use a small proportion of the resources on all its existing CDN servers. The CDN network can provide protection around the world.

An in-house solution can be scaled more effectively in the future, and without escalating license fees, as the intensity of attacks grows.

The project took at phased approach:

1. Replace the third-party DDoS software on the dedicated DDoS protection servers with Gcore's own software.
2. Move the software from dedicated servers to CDN nodes.

Gcore worked closely with Wargaming to build a UDP filtering solution. It used software hosted on both Wargaming's servers and Gcore's servers, so that it could differentiate between spoofed and legitimate gaming traffic. Gcore also developed its own software to mitigate against TCP SYN flood attacks.

Express Data Path (XDP) was used to enable fast packet filtering, because it could be integrated easily with the CDN nodes.

The change in DDoS software has given Gcore an opportunity to upgrade the processor it was using, from 2nd Generation Intel® Xeon® Scalable processors to 3rd Generation Intel® Xeon® Scalable processors. "We benefit a lot from having more cores on the processors than we had on the previous processors," said Koveshnikov.

The solution also uses 100GbE Intel® Ethernet 800 Series Network Adapters. These cards have capabilities to optimize high-performance server workloads and cater for bandwidth-intensive workloads.

To increase the filtering capacity per appliance further, Gcore is researching the potential to use the latest generation 200GbE network interface cards and Intel® Field Programmable Gate Arrays (FPGAs).

The company also plans to build a dynamic solution that analyzes the traffic to work out the best countermeasure to deploy.

Technical components of solution

- **3rd Generation Intel® Xeon® Scalable processors.** Intel® Xeon® Gold processors deliver improved four socket performance, built-in workload acceleration and advanced security technologies for cloud and network workloads.
- **100GbE Intel® Ethernet 800 Series Network Adapters.** These offer innovative and versatile capabilities that optimize high-performance server workloads with support for up to 100GbE for bandwidth-intensive workloads.
- **Intel® Hyperscan.** Hyperscan is a high-performance regex matching library that is available as open source with a C application programming interface (API). Hyperscan enables simultaneous matching of large numbers of regular expressions across streams of data.

Intel brings high-performance software expertise

Intel has collaborated closely with Gcore, sharing insights on its technology, XDP and performance optimization. "We have monthly calls with the Intel developers who are working on the hardware," said Koveshnikov. "The team has been supportive analyzing our sometimes-complicated situations. They've given us many ideas about how we can optimize our workflows."

He adds: "We told Intel about a problem that we discovered during testing. Intel replicated our tests, found the bug, and fixed it in the main software distribution."

"When you adopt a new technology, it's always a challenge," he said. "We're creating high-performance traffic filtering solutions, and a generic approach can't make a fast enough solution. It's hard to find people who have experience with this, but we found them at Intel. As a contributor to XDP, Intel was able to share their insights with us about upcoming features for the Linux kernel."

Gcore is using Intel® Hyperscan, a high-performance library for matching regular expressions (regex), which are search patterns. Hyperscan enables large numbers of regular expressions to be matched across streams of data. "We use Hyperscan to match packet data using regular expressions, and drop or pass traffic accordingly," said Slastenov. "Hyperscan is a powerful tool that is ideal for traffic filtering at the application layer. It delivers great performance and enables us to match a lot of data simultaneously."

Results

Gcore has conducted testing on its new software, running on dedicated DDoS protection servers. The company plans to integrate the software with the CDN over the coming months, in time for the peak season of DDoS attacks, which runs from September to February. Using the new software on the latest 3rd Generation Intel® Xeon® Scalable processors has increased the filtering capacity from 100 Gbps to up to 400 Gbps per alliance[1].

Gcore ran a series of TCP SYN flood tests on its minimum viable product (MVP) DDoS software. The tests used realistic traffic generated by Cisco TRex traffic generator. Although Gcore will be deploying on 3rd Generation Intel Xeon Gold processors, the tests were conducted using 2nd Generation Intel® Xeon® Scalable processors, which were in the existing DDoS servers.

The tests included the following test cases:

- **Traffic drop test.** In this test, a packet is examined, evaluated against coarse rules, and dropped before the server acknowledges the connection request.
- **SYN cookie challenge test.** To mitigate against TCP SYN flood attacks, the server can send a targeted cookie and demand a response to that cookie before it allocates server resources.

The tests measured the processing capacity in megapackets per second (Mpps) and in gigabits per second (Gbps). "Most of our customers suffer from the bandwidth of the attack (Gbps) not from the number of packets (Mpps)," said Koveshnikov. "However, when we filter the traffic, we only look at the headers, so it's the number of packets that matters most when it comes to the filtering capacity."

The in-house solution was as performant as the commercial solution, and in some respects achieved higher performance. As Table 1 shows, the traffic drop test had a maximum throughput of 108 Mpps and 51.9 Gbps[2]. The SYN cookie challenge test achieved 62 Mpps and 31.6 Gbps[2]. The tests also showed the CPU load of the solution was up to 56%, leaving enough capacity for the CDN application[2].

"Our tests showed that there are no hardware bottlenecks and the raw power of the Intel Xeon Gold processor can filter this traffic," said Slastenov.

Traffic drop test		SYN cookie challenge test	
Mpps @ Gbps	CPU load	Mpps @ Gbps	CPU load
108 @ 51.9	56%	62 @ 31.6	52%

Table 1: Maximum throughput achieved on Gcore's minimum viable product TCP SYN flood protection solution[2].

Gcore also worked with Wargaming to test the DDoS protection for UDP gaming traffic. The test worked by increasing the garbage traffic rate until it resulted in packet drops of legitimate traffic. Table 2 shows the test results, based on the packet size of the garbage traffic. The Filtered column shows how many packets can be filtered until there is an impact on legitimate traffic. The Line rate column shows how many packets the network can accommodate. The last column shows how many packets can be filtered as a percentage of the whole network channel.

The tests show that attacks with packet sizes of 256 bytes or larger can be filtered at close to line rate speed. "This is an impressive result," said Koveshnikov, "because now a single server can mitigate a 400 Gbps attack. Most attacks use a bigger packet size, where we can see the filtering solution works effectively with a low CPU usage."

Packet size	Filtered		CPU usage	Line rate		Band-width filtered
	Mpps	Gbps		Mpps	Gbps	
1500	31	383.0	12%	31.4	383.5	100%
1000	47.3	378.5	12%	47.7	379.0	100%
512	85.0	349.0	52%	85.4	349.5	100%
256	144.0	294.5	92%	162.0	340.0	89%
128	142.4	146.0	91%	384.0	340.0	37%
64	143.0	73.0	91%	432.0	236.0	33%

Table 2: Working with Wargaming, Gcore tested DDoS protection for UDP gaming traffic. The tests show that packet sizes of 256 bytes and larger can be filtered at close to line rate speed[3].

Spotlight on Gcore

Gcore is an international cloud and edge leader in content delivery and broadcasting, hosting, security solutions and public cloud services. The company is headquartered in Luxembourg.

Gcore provides a wide range of services for customers of all industries that develop their businesses online. The company's services include managed hosting, public cloud, content delivery network (CDN), an advanced media platform for professional broadcasts and streaming, protection against DDoS attacks and cloud content storage. Gcore has built its own global infrastructure on all continents (more than 140 points of presence in reliable Tier 4 and Tier 3 data centers).

www.Gcore.com

Spotlight on Wargaming

Wargaming is an award-winning online game developer and publisher. One of the leaders in the free-to-play massively multiplayer online (MMO) market, the company delivers authentic gaming experiences and services across PC, console and mobile platforms. The company has more than 15 released titles, with millions of fans worldwide. The games include the World of Tanks series, World of Warships and Master of Orion.

wargaming.net

Learn more

- Intel® Xeon® Gold processors
- 100GbE Intel® Ethernet Network Adapter E810
- Intel® Hyperscan

Find the solution that is right for your organization. Contact your Intel representative or visit **intel.com/cloud**.

[1] Configurations: Intel® Xeon® Gold 6348 processor, 32GB RDIMM memory, 960GB SSD SATA RI storage, Intel® Ethernet Network Adapter E810-2CQDA2, PowerEdge R750 Motherboard

[2] Configurations: **System under test:** 2x Intel® Xeon® Gold 6242R processors; 192GB RAM; 2x 100GbE Intel® Ethernet Network Adapter E810 (one per NUMA node, only one port per NIC is connected); Ubuntu 20.04 LTS with Linux 5.13. **Traffic generator:** 2x Intel® Xeon® Gold 6242R processors; 192GB RAM; 2x 100GbE Intel® Ethernet Network Adapter E810 (one per NUMA node, only one port per NIC is connected); Ubuntu 20.04 LTS with Linux 5.4; Cisco TRex v2.95

[3] Configuration: 2x Intel® Xeon® Gold 6348 processors @ 2.60GHz. 2x 100GbE Intel® Ethernet Network Adapter E810-2cqda2 (2 ports)