SOLUTION BRIEF

Security
Algo-Shield* DDoS Access Control List (ACL)
Management Appliance

Stop DDoS Attacks before They Disrupt the Customer Experience

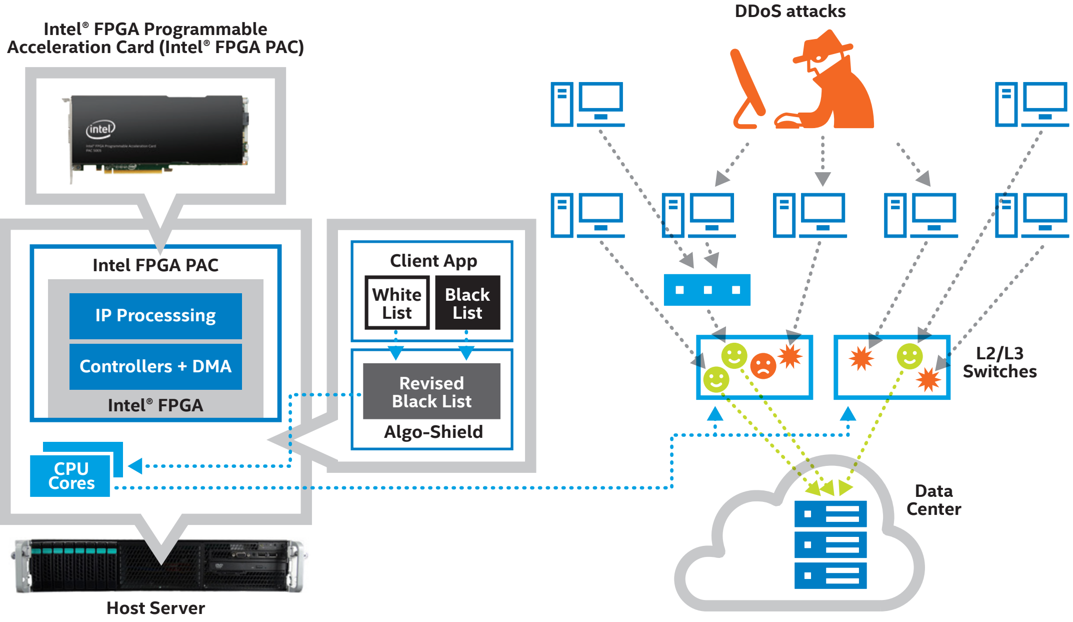
Algo-Logic's low-latency, easy-to-deploy solution featuring the Intel® FPGA Programmable Acceleration Card D5005 enables L3 switches to help protect the network at the edge

Executive summary

Large enterprises and government agencies are under constant threat of distributed denial of service (DDoS) attacks, which attempt to bottleneck or crash online services by overwhelming firewalls with malicious traffic from hundreds to millions of sources. Limiting customer access for hours or days can directly cost organizations millions of dollars and indirectly cause lasting damage to their reputation and consumer confidence.

To strengthen organizations' defenses against DDoS attacks, Algo-Logic has leveraged its expertise in developing ultralow-latency solutions for real-time applications to develop Algo-Shield*, a DDoS Access Control List (ACL) management appliance that can filter terabytes of data in seconds. Algo-Shield is accelerated on the Intel® FPGA Programmable Acceleration Card (Intel® FPGA PAC) D5005, which runs on Intel® Xeon® processor-based servers and is supported by the Intel® Acceleration Stack for Intel® Xeon® CPUs with FPGAs.

By reducing ACL management cycles from tens of minutes to seconds, Algo-Shield and Intel are helping organizations better protect their networks from DDoS-related slowdowns and crashes, and avoid costly disruptions to the customer experience.



Challenges: Rise in DDoS attacks

According to Gartner, "DDoS attacks continue to rise in complexity, volume, and frequency, threatening the network security of even the smallest enterprises."[1] Cybersecurity firm Kaspersky Lab found that the total number of DDoS attacks increased by 84 percent in the first quarter of 2019 compared to the previous quarter, and the number of attacks lasting more than an hour doubled, with more than 21 percent lasting over five hours.[2]

DDoS attacks take place daily against a wide array of primarily customer-focused organizations, including media, gaming, retail, finance, and professional services organizations. The length, size, and sophistication of attacks varies greatly, but even relatively small attacks can quickly overwhelm networks. The code-sharing site GitHub was hit with 1.35 terabits per second of malicious traffic in 2018, and other attacks have involved hundreds of millions of attack packets per second.

To defend against DDoS attacks, organizations need to quickly assess and filter web traffic by placing malicious traffic on a blacklist and subtracting a white list of verified and potential customers. Many organizations rely on ACL management software to continually update their blacklist and white list, but the update cycle can take 12 minutes or more. That delay leaves organizations vulnerable to DDoS attacks, with the first indication of an attack often coming only when network firewalls are already overwhelmed and customer-facing websites slow down or crash.

Solution: Faster filtering with Algo-Shield

Algo-Shield is a fast filtering system that helps reduce DDoS mitigation time by offloading time-consuming computations from software onto an Intel FPGA PAC D5005, supported by the Intel Acceleration Stack for Intel Xeon CPUs with FPGAs.

Algo-Shield receives a white list of valid customer addresses and a blacklist of up to tens of millions of addresses of known or suspected malicious sites. The blacklist is compiled from third parties, including network firewall vendors and network intelligence and security firms, and from historical data of previous attacks on the website.

Algo-Shield compares the white list and blacklist, rapidly filtering terabytes of data to create a revised blacklist. The revised blacklist stops DDoS attacks at the network perimeter (L2/L3 switches) while allowing network access by verified users and potential customers with previously unknown addresses.

With Algo-Shield running on an Intel FPGA PAC D5005, the entire ACL management cycle can be repeated in just seconds, instead of requiring tens of minutes during which organizations are left vulnerable to attack.

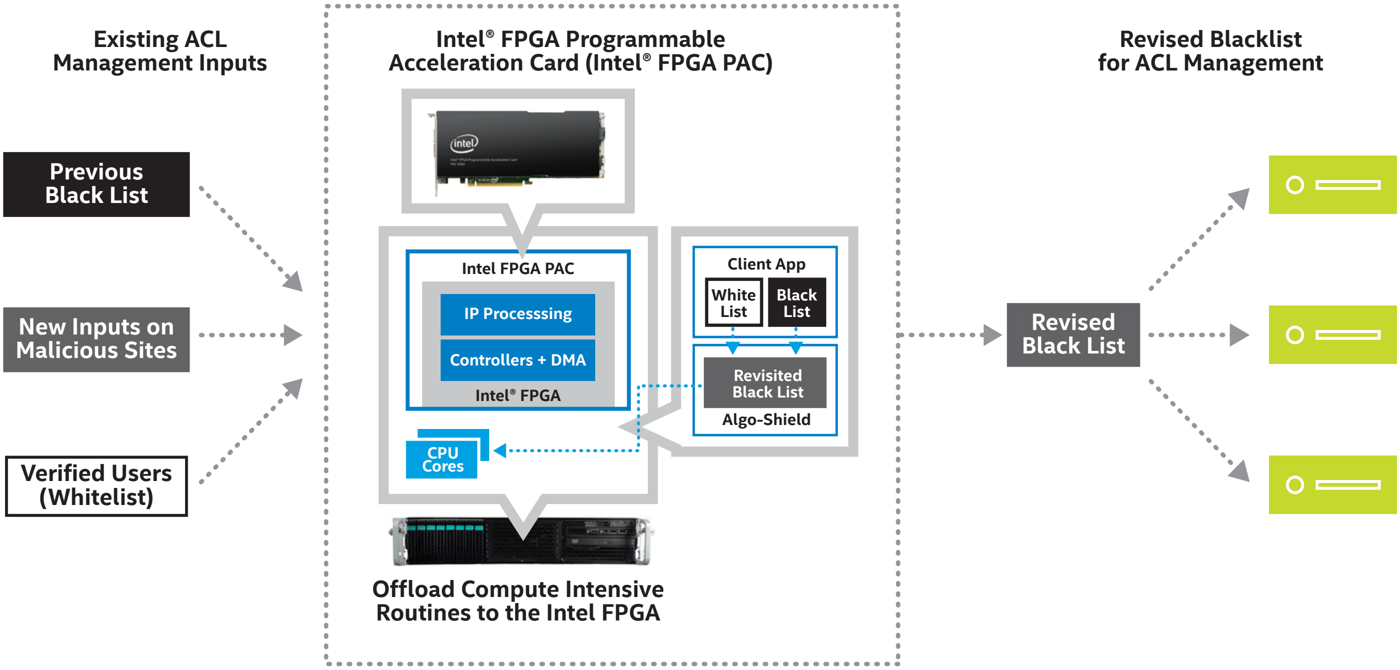

Existing ACL Management Inputs
Previous Black List
New Inputs on Malicious Sites
Verified Users (Whitelist)
Intel® FPGA Programmable Acceleration Card (Intel® FPGA PAC)
Intel FPGA PAC
IP Processsing
Controllers + DMA
Intel® FPGA
CPU Cores
Client App
White List
Black List
Revisited Black List
Algo-Shield
Offload Compute Intensive Routines to the Intel FPGA
Revised Blacklist for ACL Management
Revised Black List

Figure 1: Algo-Shield* accelerates ACL management cycles, creating revised blacklists in seconds instead of tens of minutes.

Solution components

- Algo-Shield*, an accelerated DDoS Access Control List management appliance
- Intel® FPGA PAC D5005, a high-performance PCI Express* (PCIe*)-based FPGA acceleration card for data centers
- Intel® Acceleration Stack for Intel® Xeon® CPUs with FPGAs, which provides a common interface, drivers, APIs, and an FPGA Interface Manager to save developers time
- High-volume, Intel® Xeon® processor-based servers

Use case: Multimedia company cuts latency by 50x[3]

One of the world's largest multimedia companies was battling near-constant DDoS attacks using a traditional software solution. Each ACL cycle took the company 12 minutes or more, leaving them exposed to network slowdowns and crashes—and, in fact, customer experience had been impacted more than once by DDoS attacks.

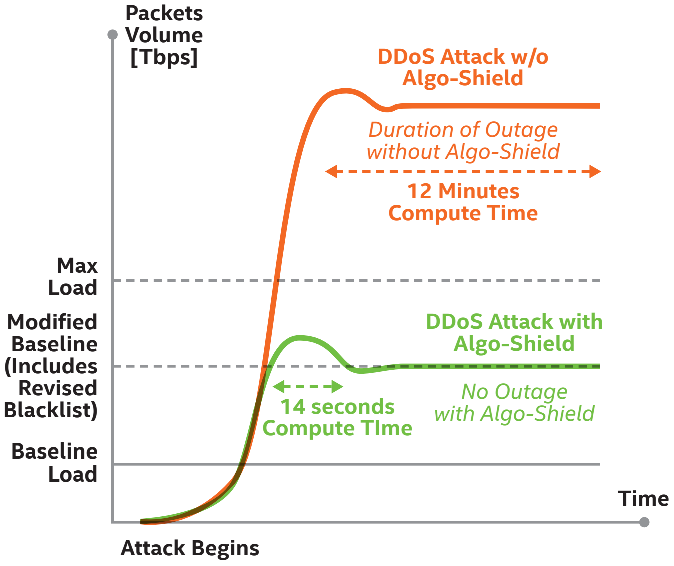
The company recognized that adding traditional DDoS appliances would require a tremendous investment in capital and an expensive and complicated mitigation plan that could still be overwhelmed by an extreme, highly determined attack. Instead, they chose to implement a hybrid DDoS defense strategy enabled by Algo-Shield.

With the hybrid approach, once the company had a revised blacklist, they could redirect and discard terabytes of traffic from malicious addresses using relatively inexpensive 10/25/40/100 GbE switches, allowing only a small subset of traffic to hit the company's firewalls. Algo-Shield enabled this approach by generating the revised blacklist quickly with the help of Intel FPGA PACs (at the time, Intel® Arria® 10 FPGA PACs), supported by the Intel® Acceleration Stack.

Algo-Logic's accelerated DDoS ACL management solution significantly reduced latency and increased throughput, shortening the time necessary to generate a revised blacklist from 12 minutes or more to just 14 seconds.[3] The updated solution, running on the latest Intel FPGA PAC D5005, is expected to accelerate generation of revised blacklists even more, and enable the company to continue managing blacklists of up to 40 million entries and white lists of up to one million entries.[3]

Benefits of Algo-Shield on Intel® FPGA PAC D5005

- **Performance:** Up to 50x reduction in latency[3]
- **Operational cost:** Save network operators time and money with an easy-to-manage solution
- **Capital expenditures:** Reduce need for purchasing hundreds or thousands of expensive firewall switches
- **Integration:** Integrate into existing cybersecurity solutions in hours, using a C++ API
- **Failover protection:** Failover software effectively provides two solutions in one system
- **Short ACL cycles:** Recombining fragmented subnets in the revised blacklist keeps ACL cycles as short as possible
- **User experience:** Ensure strong network performance, even under repeated DDoS attacks



In testing, Algo-Shield has been able to prevent network outages by reducing cycle times and reducing the amount of traffic reaching firewalls.

INCREASED ACCELERATION

With Intel® FPGA PAC D5005 running acceleration of revised blacklist calculation

50x[3]

REVISED BLACKLIST CALCULATION TIME

Algo-Shield* **14 sec.**[3]

Existing SW **12 min.**[3]

ACL SIZE:

100,000 white list

10,000,000 black list

Algo-Shield* helped a multimedia company reduce ACL cycle times.

Solution architecture

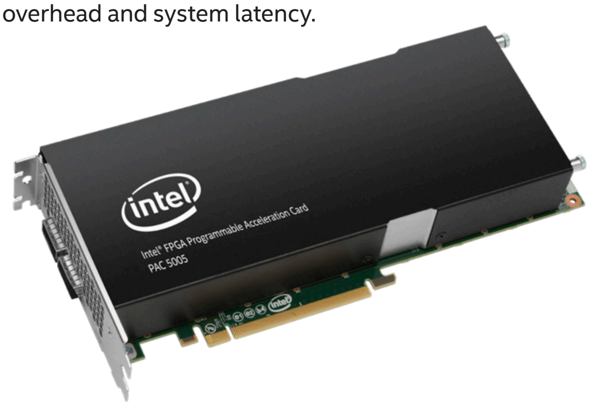
Algo-Shield is accelerated on the Intel FPGA PAC D5005, which is supported by the Intel Acceleration Stack for Intel Xeon CPUs with FPGAs.

To run Algo-Shield, organizations simply install the Intel FPGA PAC D5005 in an Intel Xeon processor-based server, then load drivers and Algo-Shield to begin accelerating their ACL management cycles. From the operating system's point of view, the FPGA hardware appears as a regular PCIe device, and the FPGA accelerator appears as a set of features accessible by software programs running on the host.

Algo-Shield runs as a C++ program in the host, with a software version acting as a fallback program. Multiple instances of Algo-Shield can be run with staggered starts every one to 30 seconds to ensure that the revised blacklist always contains the latest, previously unknown addresses with malicious content.

Benefits of Intel FPGAs

The key advantage of running Algo-Shield on Intel FPGAs is that they enable higher-speed data processing by providing customized high-bandwidth, low-latency connections to network and storage systems. By offloading high performance computing tasks to an Intel FPGA operating on a high-performance server, organizations can reduce their CPU overhead and system latency.



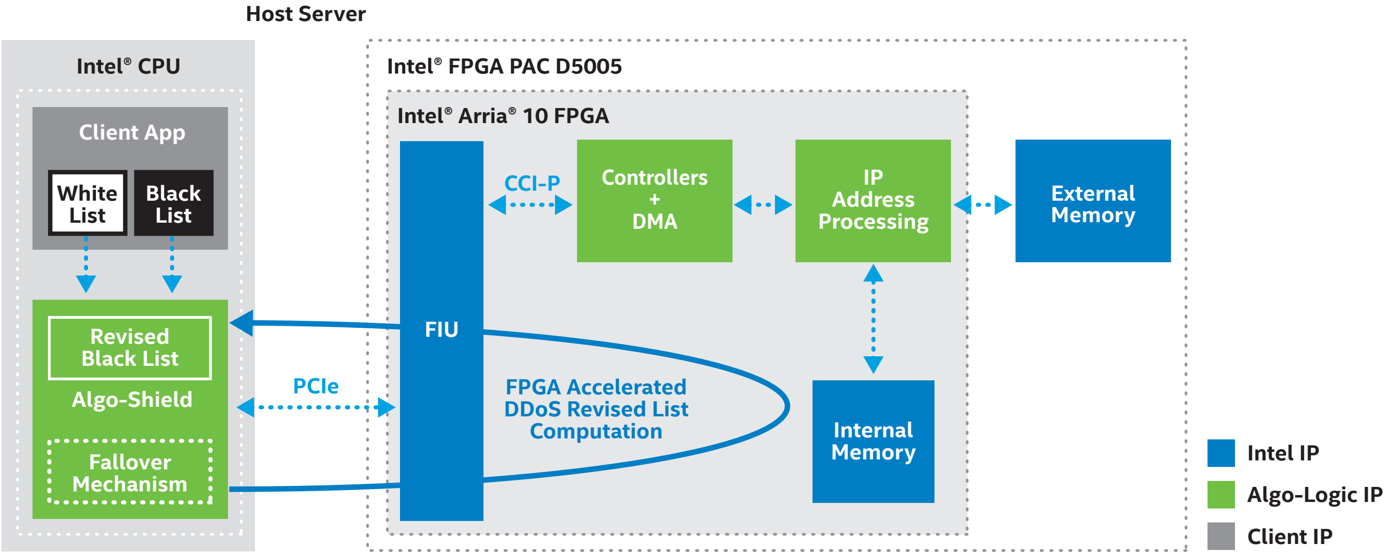


Figure 3: Algo-Shield* accelerates ACL management cycles, creating revised blacklists in seconds instead of tens of minutes.

The Intel FPGA PAC D5005 inherits many technological benefits of FPGA technology. With algorithms implemented in hardware circuitry, FPGAs respond deterministically, enabling real-time processing of the data. FPGAs also have a significant advantage over GPUs in workload latency performance because of their massively parallel, low-latency architecture.

FPGAs can be dynamically configured with a custom hardware logic block for a given workload, ensuring optimized performance for a task. This same configurability makes it easy to perform algorithm updates and upgrades. Additionally, the same server hardware can be used for many workloads, so as algorithms evolve in an application, businesses can use the same hardware and simply change the workload.

The Intel FPGA PAC D5005 is supported by the Intel Acceleration Stack for Intel Xeon CPUs with FPGAs, which provides a common developer interface and includes drivers, application programming interfaces, and an FPGA Interface Manager. The acceleration stack works with industry-leading operating systems and virtualization and orchestration software, providing a common interface for software developers to get fast time to revenue, simplified management, and access to a growing ecosystem of acceleration workloads.

Conclusion

Algo-Logic's fast-filtering DDoS solution, Algo-Shield, provides a powerful and cost-effective alternative for government agencies and consumer-focused enterprises, especially those that have experienced major DDoS attacks, have numerous distributed IP devices such as game consoles, or for any reason cannot tolerate downtime due to DDoS attacks. With Algo-Logic and Intel, organizations can benefit from Intel FPGA acceleration for lower latency, higher throughput, and a stronger network defense against costly DDoS attacks.

Learn More

Learn more about Algo-Shield DDoS ACL management at **algo-logic.com** or by email at **support@algo-logic.com**.

Learn more about **Intel® FPGA solutions** and about **Intel Programmable Acceleration Cards and the Acceleration Stack**.

About Algo-Logic Systems

Algo-Logic Systems Inc., is a recognized leader of Gateware Defined Networking* (GDN) products and solutions. Algo-Logic's FPGA-accelerated GDN solutions achieve high throughput with minimal power and submicrosecond latency on commercially available FPGA platforms.

algo-logic.com

1. Thomas Lintemuth, Patrick Hevesi. "DDoS: A Comparison of Defense Approaches," April 24, 2019. www.gartner.com/en/documents/3907156/ddos-a-comparison-of-defense-approaches
2. Kaspersky Lab, "DDoS Attacks in 2019," May 21, 2019. https://securelist.com/ddos-report-q1-2019/90792.
3. Test conducted by Algo-Logic using a blacklist of 10 million and white list of 100,000. Both Algo-Shield* and the client solution used the same data to create scripts for the benchmark. Test relied on Intel® PAC with Intel® Arria® 10 GX FPGA, Intel® Xeon® E5-1620 v4 at 3.5 GHz x86 with 64 GB memory. Operating system: CentOS* 7 1.2.5 V.

Intel® technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system or device can be absolutely secure. Check with your system manufacturer or retailer, or learn more at intel.com/iot.

0819/YLR/CMD/PDF