

SOLUTION BRIEF

Telecommunications
DDoS Protection



High Capacity DDoS Protection in Cloud Environments with F5 BIG-IP VE for SmartNICs and Intel FPGA PAC N3000

Automated 5G cyberthreat mitigation for service providers and enterprises

The transition to 5G infrastructure will likely increase the risk of a new series of DDoS attacks. These are expected to increase in size, severity, and complexity. Service providers building 5G infrastructure must implement a strategy to help mitigate the impact of attacks on bandwidth and subscribers.

Fortunately, the move to using more virtualized technology can enable service providers to reduce the force and effectiveness of DDoS attacks more quickly and at scale. For example, the F5 BIG-IP VE for SmartNICs solution—integrated with an Intel® FPGA Programmable Acceleration Card (PAC) N3000, an FPGA-based smartNIC—offers such an opportunity. By combining this solution with virtualized 5G infrastructure using commercial off-the-shelf (COTS) servers, service provider networks can automatically detect and better protect themselves faster than current methods against evolving, volumetric DDoS attacks that can negatively affect subscriber and user access to applications and other services.

In addition to service providers, enterprise organizations undergoing digital transformation will need to respond to these new types of DDoS attacks. The solution described here can offer them the same protection.

In production and available today, many tier 1 server OEMs are qualifying the card in their respective servers. [Click here](#) for a current list of qualified servers. The Intel FPGA PAC N3000 is dynamically configurable to accelerate multiple workloads such as 5G vRAN, Open vSwitch, Segment Routing v6, Tungsten Fabric, 5G User Plane Function (UPF), vBNG, and security solutions. This allows service providers to deploy a server plus the Intel FPGA PAC N3000 to support many cloud-native network functions or virtual appliances based on services demand at the edge.

Disruptive and sophisticated DDoS attacks are difficult to defend

While DDoS attacks range from targeted acts of retaliation, protest, theft, or extortion to pranksters, they all have one objective: disrupt service availability and reduce the ability of a business to function.

Depending on an attacker's skills, they may use readily available DDoS tools or launch customized, sophisticated strikes. In general, such attacks may come in a combination of four types:

- **Volumetric:** Flood-based attacks—often using botnets—at layer 3, 4, or 7
- **Asymmetric:** Invoking timeouts or session-state changes
- **Computational:** Consuming CPU and memory
- **Vulnerability-based:** Exploiting application software vulnerabilities

The most damaging DDoS assaults often blend volumetric attacks, in order to create a diversion, with application-specific attacks, making the actual target or targets difficult to assess. These types of complex attacks are difficult to defend against and can indicate more-advanced, persistent threats to come.

By rapidly discovering and stopping attacks, service providers can provide better service continuity and maintain subscriber satisfaction. With 'F5's BIG-IP VE for SmartNICs solution', service providers gain comprehensive and high-performance layer 3–7 DDoS software mitigation solution. This high-performance, stateful, full-proxy network security on-premise solution can also be combined with F5's Silverline cloud DDoS scrubbing service to help alleviate network, application, and volumetric attacks that can enter the network on the most widely deployed protocols.



ATTACK TESTING RESULTS

In testing performed by F5, the BIG-IP VE for SmartNICs solution integrated with an Intel® FPGA PAC N3000, withstood a 300X higher level DDoS attack (IP Short Fragment attack) than processing in software in a COTS server. The solution detected and blocked the “bad” attack traffic while letting in “good” traffic.¹

See footnote 1 for configuration details. For more complete information about performance and benchmark results, visit www.intel.com/benchmarks.

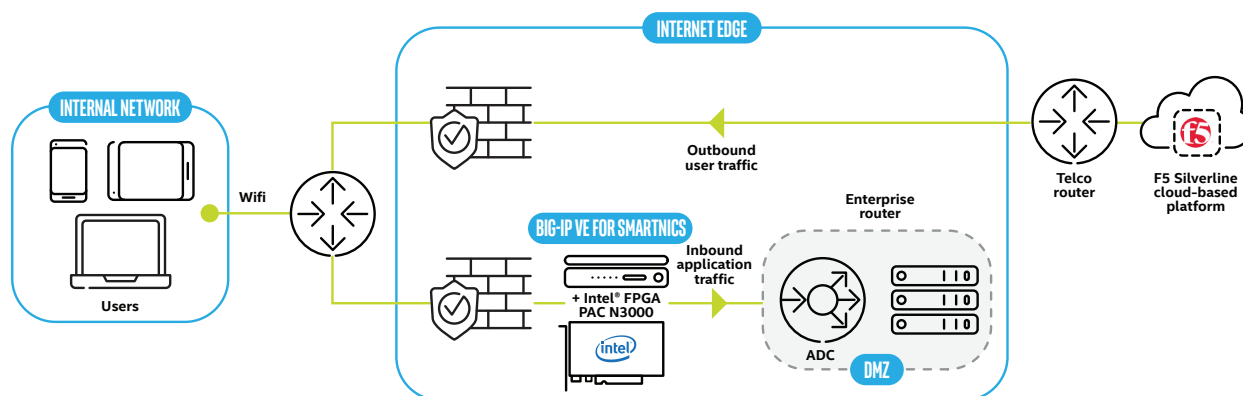


Figure 1. The F5 solution helps protect service providers from sophisticated DDoS attacks.

The on-premise platform can combine F5's purpose-built software and cloud scrubbing service—known as F5 Silverline DDoS Protection—which helps provide both reactive and proactive hybrid DDoS defenses. Together they can facilitate always-up services by rerouting attacks away from the data center for cloud-based mitigation.

Working with Intel, F5 integrated the Intel® FPGA PAC N3000 with BIG-IP VE for SmartNICs into a commercial off-the-shelf (COTS) server. By moving DDoS specific functions from the CPU on to the SmartNIC FPGAs, the CPU is freed up and allowed to perform as designed. FPGAs can be programmed to quickly execute different tasks. With future F5 software releases, additional offload functions can be accelerated within the FPGA, making the system flexible for a wide range of high-performance use cases.

The combination of purpose-built software, plus the Intel FPGA PAC N3000, is designed to allow the BIG-IP VE for SmartNICs solution to offer service providers and enterprises the ideal NFV firewall/DDoS protection for virtual or software-based architecture in their data centers. This combination provides equivalent capabilities to dedicated custom hardware helping protect their services and applications.

By applying network threat intelligence and machine learning, packet-based analysis, the solution can more efficiently block network attacks at scale while minimizing compute cycles, providing a CPU-efficient solution lowering TCO by approximately 47% over a 4 year period². The solution also supports updating black and white lists,

implemented in the SmartNIC, to keep current with evolving threat landscapes.

Service providers using the solution to deploy DDoS protection in new areas and closer to the edge can gain visibility into cyberthreats and attacks that are difficult to see with today's technology. This visibility, combined with automation, makes it easier to prevent attacks from damaging the network at a low total cost of ownership.

DDoS mitigation for the cloud and 5G

BIG-IP VE for SmartNICs provides unparalleled DDoS mitigation capabilities in cloud environments as service providers build out their 5G architectures, helping to:

- Increase service availability and reduce latency
- Facilitate a swifter transition from hardware to software without sacrificing performance
- Reduce operating costs through scalability and CPU efficiency while avoiding revenue losses associated with outages

Learn More

Learn more about the Intel FPGA PAC N3000 at intel.com/pacn3000.

Contact an F5 security expert >

ABOUT F5

F5 (NASDAQ: FFIV) powers applications from development through their entire lifecycle, across any multi-cloud environment, so our customers—enterprise businesses, service providers, governments, and consumer brands—can deliver differentiated, high-performing, and secure digital experiences. For more information, go to f5.com. You can also follow @f5networks on Twitter or visit us on LinkedIn and Facebook for more information about F5, its partners, and technologies.



F5 Networks, Inc.
801 5th Avenue
Seattle, WA 98014
888-882-4447
f5.com



1. Based on F5 internal testing using Ixia traffic generators to simulate both "good" traffic and "bad" and comparing the results with Intel® FPGA PAC N3000 DDoS protection enabled and running BIG-IP AFM VE firewall in SW only. Test configuration: Supermicro SYS-1019P-WTR; CPU: Intel(R) Xeon(R) Gold 6240 CPU @ 2.60GHz (18 core/36 threads); KVM version: 1.5.3; Base OS: CentOS Linux release 7.7.1908 (Core), 1 x Intel® FPGA PAC N3000 smartNIC; Firewall SW: BIG-IP Advanced Firewall Manager Virtual Edition (VE) v15.1.0.4. Traffic generation configuration: bad traffic: Ixia IxExplorer IxOS 8.5.1700.5 EA.Ink.; good traffic: Ixia XGS12.

2. This number is derived from comparing the cost of a High Performance (24vCPU) BIG-IP VE AFM license + annual support costs with the cost of the BIG-IP VE for SmartNICs solution (High Performance 8vCPU VE AFM + Intel FPGA PAC N3000 price + F5 SmartNIC add-on license + annual support costs) over a 4 year period.

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 product or component can be absolutely secure. For more complete information about performance and benchmark results, visit intel.com/benchmarks.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available security updates. See backup for configuration details. No product or component can be absolutely secure. Results have been estimated or simulated. Your costs and results may vary. Intel technologies may require enabled hardware, software or service activation.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands may be claimed as the property of others.