SOLUTION OVERVIEW

Augment Performance in Virtualized Environments With BIG-IP VE for SmartNICs

Offload compute-intensive VE functions and lower TCO

KEY BENEFITS

Assorted Use Cases
Augment various network functions including CGNAT, L4 traffic transmission, and DDoS protection.

Boost Performance
Offload to a high performance, FPGA-enabled SmartNIC to significantly improve performance.

Liberate Compute Cycles
Alleviate strain on BIG-IP VE's available compute by up to 95%.

Reduce TCO
Provision BIG-IP VE with up to 67% fewer vCPU cores without affecting performance.

Cut Power Usage
Achieve 25%+ power savings against comparable BIG-IP systems or VEs.

Save Space
Compact solution ideal for deployment within edge locations.

High Programmability
SmartNIC can be re-programmed to support evolving use cases.

Deployment Simplicity
Container-based orchestrator streamlines SmartNIC onboarding and configuration.

The Challenge: The Demand for Superior Performance and Lower TCO in Virtualized Environments

The pace of application migration and creation within cloud and virtualized environments continues to accelerate across every industry and region, as companies are lured in by the promise of enhanced agility, greater architectural flexibility, and lower costs. At the same time, many companies are undergoing dramatic digital transformations that place additional strain on workloads as usage surges. When this is coupled with the global transition to 5G and the unrelenting expectation of flawless, ultra-fast user experiences, it's clear that application scalability and performance will continue to be of utmost importance in years to come.

Ironically, transitioning to a software-first strategy typically has a performance cost, as organizations sacrifice the power of in-house, purpose-built appliances in favor of the common-off-the-shelf (COTS) servers needed to build out their private cloud environments. The performance offered by these COTS servers is targeted for general purpose workloads, meaning that any software or application that performs specialized networking and security functions may lack the computational power to effectively perform complex, resource-intensive tasks. For instance, the vast majority of BIG-IP Virtual Edition traffic management and security capacities can be efficiently performed when running on COTS servers. But certain demanding functions, such as DDoS mitigation, may exhaust all available compute resources and leave networks and applications vulnerable.

Additionally, as application services continue to move closer to end users in edge and far-edge locations, this issue will only be exacerbated. Space, power, and cost confinements will limit organizations to using only the smallest, most power-efficient servers, which will likely have further performance implications. Organizations clearly need a way to bolster system performance within these distributed, virtualized environments while lowering costs. SmartNICs are one innovative solution to this challenge.

The Solution: BIG-IP VE Augmentation via SmartNICs

SmartNICs are the latest addition to the Network Interface Card (NIC) family. Boasting onboard programmable components such as FPGAs, NPUs, or SoCs, SmartNICs can perform user-specified networking functions on behalf of the applications or servers they're connected to—alleviating strain on CPU resources and significantly improving performance. They also maintain all the usual NIC functions needed to connect devices to networks.

The BIG-IP VE for SmartNICs® solution is the product of an integration between F5® BIG-IP Virtual Edition® and Intel® FPGA N3000 SmartNIC®. Leveraging F5's more than 10 years of FPGA expertise, this SmartNIC can be programmed to assume responsibility for performing various VE functions, depending on an organization's use case. By offloading these tasks to the SmartNIC, not only can significant performance improvements be realized, but less compute power (virtual cores) may be required to operate the VE—lowering server and energy costs or freeing up CPUs for other purposes. As the FPGA within the SmartNIC can be reprogrammed at any time, its function can be changed to support evolving use cases as needed—delivering the architectural flexibility and agility that organizations deploying cloud-native network functions desire. The following section outlines the current BIG-IP VE functions that can be augmented by offloading to the SmartNIC.

BIG-IP VE for SmartNICs Use Cases

1: CARRIER GRADE NAT (CGNAT)

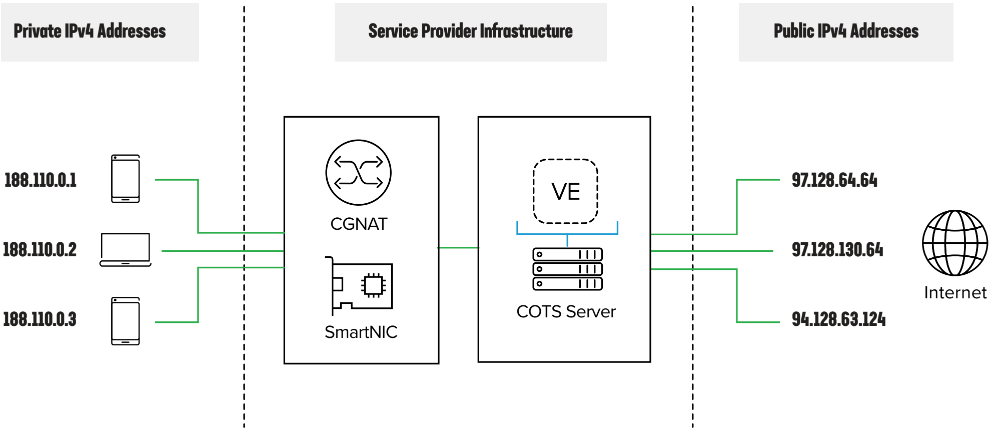

Figure 1: Showing NAT44 offload from BIG-IP VE to Intel FPGA PAC N3000 SmartNIC

IMPROVE CGNAT THROUGHPUT BY 30% WHILE LOWERING VE CPU USAGE BY 80%.

According to most research reports and analysts, there are now well over 20 billion interconnected, internet-enabled devices worldwide. With this figure expected to increase exponentially in years to come, the existing challenges that service providers face as a result of IPv4 address depletion will only be amplified. And while the introduction of IPv6 provides the long-term solution to this problem, in the short term it has only complicated matters, as IPv4 and IPv6 applications and devices must co-exist on shared networks. Carrier Grade Network Address Translation (CGNAT) is now a critical function within most service providers' networks, not only enabling these heterogeneous components to connect and communicate with one another, but also enabling address sharing through the mapping of readily available private IP addresses to increasingly sparse public IP addresses. Unsurprisingly, as internet traffic continues to surge, CGNAT infrastructure is one area of a service provider's network that can quickly become overwhelmed.

When performing CGNAT, there are two primary functions that require significant compute power: executing the actual translation from one IP address to another; and then logging that translation—as required by the U.S. Communications Assistance for Law Enforcement Act (CALEA). By offloading these functions from BIG-IP VE to an Intel FPGA PAC N3000 SmartNIC, the total system throughput can be improved by around 30%. More importantly, the BIG-IP VE's CPU utilization can also be reduced by approximately 80%—helping to prevent the VE from becoming overloaded. In the case of NAT44 offload, which is depicted above in figure 1, when operating in NAPT (Network Address & Port Translation) mode, the exact performance and CPU improvements can be seen in table 1.

CGNAT Performance Comparison

	L4 Throughput	VE CPU Utilization
BIG-IP VE	37 Gbps	87%
BIG-IP VE for SmartNICs	48 Gbps	4%

Table 1: Performance comparison for the BIG-IP VE for SmartNICs solution when operating NAT44 in NAPT mode

2: LAYER 4 TRAFFIC ACCELERATION

DELIVER 30% GREATER L4 PERFORMANCE WHILE REDUCING VE CPU USAGE BY 80%.

Application Delivery Controllers (ADC) typically manage and manipulate traffic based on either layer 4 or layer 7 packet information. For example, layer 4 load balancing acts upon data found in the network and transport layer protocols, such as TCP & UDP, while layer 7 load balancing distributes requests based upon data found in the application layer protocols, such as HTTP and HTTPS. As both the number of applications and the number of people using those applications continues to grow at an unprecedented pace, the ability of ADCs to scale to process requests becomes increasingly vital to ensuring application availability, security, and performance.

Operating in a similar fashion to the ePVA functionality (leveraging high performance FPGAs) that optimize layer 4 connections and flows in BIG-IP physical appliances, the BIG-IP VE for SmartNICs solution can be configured for layer 4 transmission acceleration, which increases layer 4 throughput and connections per second. Doing so allows BIG-IP VE to manage a greater number of application users while operating at around 75% lower CPU utilization—significantly lowering the risk of compute exhaustion and packet loss. When operating in this mode, the SmartNIC is also capable of improving the processing performance of layer 4 iRule commands, which could otherwise deplete CPU resources when enforcing complex rules in large volumes. Table 2 highlights the performance and CPU improvements observed when offloading L4 processing to the SmartNIC.

Layer 4 Performance Comparison

Table 2: Layer 4 throughput and VE CPU utilization improvements when employing SmartNIC offload.

	L4 Throughput	CPU Utilization
BIG-IP VE	36 Gbps	81%
BIG-IP VE for SmartNICs	48 Gbps	4%

3: DDOS PROTECTION

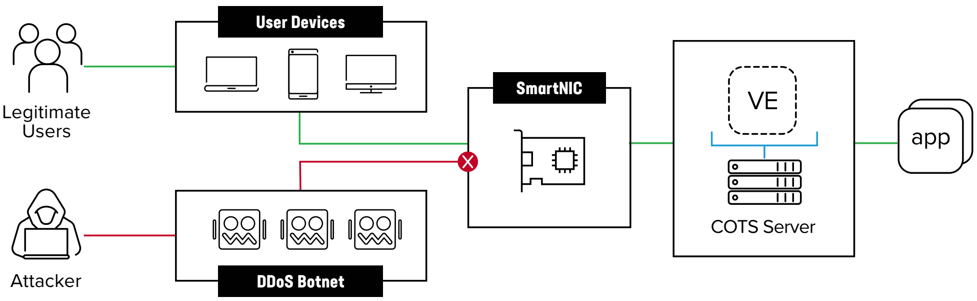

Figure 2: Offloading DDoS mitigation from BIG-IP VE to Intel's FPGA PAC N3000 SmartNIC

BLOCK ATTACKS UP TO 300 TIMES GREATER IN SIZE WHEN COMPARED TO SOFTWARE-ONLY SOLUTIONS.

As DDoS attacks continue to rise, in terms of both frequency and magnitude, protecting virtualized infrastructure against these malicious threats has become even more necessary. By offloading responsibility for detecting and mitigating DDoS attacks from the BIG-IP VE to the Intel SmartNIC (as seen in figure 2), organizations can block attacks up to 300 times greater in size when compared to software-only solutions, while consistently thwarting attacks over 35 Gbps in size.

The SmartNIC is not only programmed to detect and block over 100 different types of DDoS attacks, but it can do so on a global or per-app basis—allowing you to focus protection on individual workloads or your entire network, depending on your specific requirements. Critically, traffic inspection also occurs at line rate, meaning the SmartNIC can identify and drop malicious packets without legitimate requests incurring additional latency. On top of this, the SmartNIC also alleviates strain on the BIG-IP VE's allocated compute resources, with around 70% of available vCPUs being freed up and made available to perform other traffic management and security tasks. In essence, this means the BIG-IP VE can operate efficiently with fewer allocated vCPUs, lowering your total cost of ownership. Table 3 shows the maximum DDoS attack size that a standalone BIG-IP VE and the BIG-IP VE for SmartNICs solution can withstand.

DDoS Protection Comparison

Table 3: Performance data for the BIG-IP VE and BIG-IP VE for SmartNICs solution when mitigating a combined SYN-ACK flood, UDP flood, and ICMPv4 flood DDoS attack.

	Max. Withstandable Attack Size	VE CPU Utilization
BIG-IP VE	2.4 Gbps	100%
BIG-IP VE for SmartNICs	40 Gbps	29.8%

Simplified Deployment with F5's SmartNIC Orchestrator

While FPGA-based SmartNICs offer the greatest performance and programming flexibility, the onboarding process for most can be complex and somewhat arduous. That's why F5 has developed its own SmartNIC orchestrator tool to simplify the solutions deployment. Operating within a Docker container and accessible via API or a web-based user interface, the SmartNIC orchestrator performs all the necessary steps required to onboard the SmartNIC. From programming the embedded FPGA to support the desired use case, to connecting the SmartNIC with the BIG-IP Virtual Edition, the orchestrator tool simplifies and streamlines every step of the deployment process.

Conclusion

As organizations undergo digital transformation and shift application workloads to virtualized environments in the cloud and out at the edge, the desire to optimize costs while meeting the performance requirements of thriving applications increases. By augmenting F5's BIG-IP Virtual Edition and offloading complex, compute-intensive functions such as CGNAT and DDoS protection to a high-performance, FPGA-enabled Intel SmartNIC, companies can not only lower compute requirements, power usage, rack space, and total cost of ownership in general, but also bolster performance to support the growing demand for their application portfolio. Looking forward, F5 will continue to develop and deliver support for new use cases on the BIG-IP VE for SmartNICs solution beyond those covered in this overview, based on customer requests and market research.

To learn more, contact your F5 representative or contact F5 Sales.

More Information

For more information about how F5 BIG-IP VE for SmartNICs can help your business, please visit these resources:

BIG-IP VE for SmartNICs Demo—DDoS Protection

BIG-IP VE for SmartNICs Technical Whitepaper–DDoS Protection

BIG-IP VE for SmartNICs–Deployment Guide

F5 & Intel Technology Alliance

Intel FPGA PAC N3000 SmartNIC