

# Solution Brief

Fortinet FortiGate-VM Virtual Next Generation Firewall  
5th Gen Intel® Xeon® Scalable Processor  
Intel® Infrastructure Processing Unit (Intel® IPU)



## Reducing the Operational Cost of Fortinet FortiGate-VM on GCP

5th Gen Intel® Xeon® Scalable processors lower the total cost of ownership of Fortinet FortiGate-VM running on GCP by reducing the cost of high-bandwidth network throughput.



### Executive Summary

The GCP C4 machine series is a major step forward in terms of compute performance and networking capability featuring the 5th Gen Intel® Xeon® Scalable processor (code name Emerald Rapids) and a built-in, state-of-the-art Intel® IPU — a joint innovation from Intel and Google. These technologies present a cost advantageous environment for running network security workloads such as Fortinet FortiGate-VM, a Next Generation Firewall (NGFW) solution. This brief describes the potential cost savings of deploying FortiGate-VM on the GCP C4 machine series.

### Introduction

Improved performance at reduced operational costs in the public cloud requires advanced processor capability, smart infrastructure processing, and modern software component enablement. As such, in August 2024, the GCP C4 machine series reached general availability featuring the 5th Gen Intel Xeon Scalable processor alongside a custom Intel IPU. The C4 machine series is ideal for NetSec workloads including Fortinet FortiGate-VM virtual NGFW. The C4 machine series offers the cost-savings of a substantial network IO performance boost that provides FortiGate-VM with a high-performance operating environment at reduced costs.

The C4 machine series is powered by the 5th Gen Intel Xeon Scalable processor. The processor is equipped with several performance enhancing features including Intel® Advance Matrix Extension (Intel® AMX) for AI/ML workloads and Intel® Advanced Vector Extensions 512 (Intel® AVX-512) for workloads that benefit from fast vector instructions like the cryptographic operations of IPsec and TLS/SSL, or the regular expression pattern matching needed for packet inspection and rules matching.

FortiGate-VM is a next-generation firewall that delivers industry-leading threat detection and robust security functionality. It integrates advanced technologies such as AI-powered threat intelligence, intrusion prevention, and deep packet inspection to protect against sophisticated cyber threats. FortiGate-VM seamlessly extends security across data centers, branch locations, and cloud environments, ensuring consistent protection and policy enforcement.

For FortiGate-VM deployments running on the N1 or N2 machines series, migration to Google Compute Engine (GCE) instances with the latest Intel processors such as the C4 machine series is strongly recommended. This solution brief illustrates the performance boost and cost saving benefits of migrating to C4 from the N2 machine series on GCP.

## FortiGate-VM on GCP

Fortinet FortiGate-VM provides award-winning protection from a broad array of network threats. It delivers converged networking and security capabilities to protect deployments on Google Cloud against network threats and enables seamless connectivity across regions and hybrid cloud deployments. FortiGate-VM is essential for building your hybrid mesh firewall infrastructure, allowing you to protect applications no matter where they are deployed. It works as an additional security layer used to protect your environment from potential threats. FortiGate-VM can be used for different use cases, including Ingress and Egress threat protection, East/West traffic security with network segmentation, zero trust policy enforcement, and extending your secure SD-WAN to the Google Cloud.

Fortinet is a Google Cloud Partner and together, Fortinet and Google have integrated FortiGate-VM into the Google Cloud security ecosystem. With integrations into Google Cloud tools, including Network Connectivity Center (NCC), Network Security Integration (NSI), and others, Google Cloud customers can efficiently safeguard their workloads, optimize network performance, and simplify security management across hybrid and multi-cloud environments. FortiGate's security offerings are industry-leading solutions trusted by many.<sup>1</sup>

FortiGate VM is purpose built for use on public and private clouds. FortiGate's vSPU technology enhances performance by offloading part of packet processing to user space, while using a kernel bypass solution within the operating system. This support enables firewall performance to scale linearly by allocating additional virtual CPU cores. In addition, FortiGate's Google Cloud connector enables FortiGate firewalls to dynamically discover and synchronize Google Cloud Platform (GCP) resources, allowing the creation of dynamic firewall policies that automatically adapt to changes in cloud infrastructure. This integration streamlines security management, reduces manual updates, and ensures that security policies remain accurate and up-to-date as cloud workloads scale or shift.

## FortiGate-VM Network I/O Throughput

FortiGate-VM is a NGFW solution that is tuned to offer high-throughput I/O to meet the network performance service level agreements (SLAs) required by enterprises. To maintain optimized performance and costs, FortiGate-VM can take advantage of the modern cloud infrastructure and the latest VM instances powered by Intel processors on GCP. This section describes some of the hardware and software advances that provide high-throughput networking for FortiGate-VM use cases when running on the C4 machine series.

## Infrastructure Processing Offload and Intel® IPU

On the latest GCE VM machine series, including C4, Google's Andromeda network virtualization stack is offloaded to a custom Intel® IPU. That is, processor intensive tasks such as encryption, encapsulation, virtual switching, etc., that are performed by GCP infrastructure and might otherwise consume host resources are instead handled by the Intel IPU and other Titanium<sup>2</sup> offloads. The Intel IPU ensures reduced network latency and consistent throughput performance levels comparable to the underlying network interface hardware. As a result, tenant networking applications, such as FortiGate-VM, can expect improved network performance over prior generation VMs that do not utilize this hardware. FortiGate-VM deployments currently running on the N1 or N2 machine series can take advantage of the Intel IPU by upgrading to the C4 machine series.

## DPDK in GCP

DPDK is a set of drivers and APIs designed to speedup up network packet processing on general purpose CPUs such as Intel Xeon processors. While traditional Network Interface Card (NIC) drivers typically run in kernel space in an interrupt driven fashion, Poll Mode Drivers (PMDs) usually run in user space, logically closer to the client application, and use a busy poll mode method of detecting events from the network. In general, the userspace PMD dataplane architecture pioneered by DPDK can be significantly faster than kernel-based data plane processing. On GCP, PMD implementations exists for the C4 machine series and can be enabled by FortiGate-VM for improved network performance.<sup>3</sup>

**Table 1.** GCE Select General-Purpose Machine Types

Machine Type	Processor	Line Rate (Gbps)	Mem (GB)	On-Demand Price (\$/hr)
n2-standard-4	2nd / 3rd Gen Intel® Xeon® Scalable processor	Up to 10	16	\$0.194236
n2-standard-8	2nd / 3rd Gen Intel Xeon Scalable processor	Up to 16	32	\$0.388472
c4-standard-4	5th Gen Intel® Xeon® Scalable processor	Up to 23	15	\$0.19767
c4-standard-8	5th Gen Intel Xeon Scalable processor	Up to 23	30	\$0.39534

## Enabling DPDK on FortiGate-VM

DPDK enhances FortiGate-VM performance by offloading part of packet processing to user space while using a kernel bypass solution within the operating system. Enabling DPDK in FortiGate-VM can result in faster, more consistent network IO performance on GCP. DPDK can be enabled and configured for FortiGate-VM on GCP with FortiOS CLI commands—an example of which is shown in Figure 1.<sup>4</sup>

```
# Instructions To Enable DPDK for FortiGate-VM

config dpdk global
(global) # set status enable
(global) # get
status      : enable
interface   :
multiqueue  : disable
sleep-on-idle : disable
elasticbuffer : disable
per-session-accounting: traffic-log-only
ipsec-offload : disable
hugepage-percentage : 30
mbufpool-percentage : 25

(global) # set interface port1 port2 port3 port4
(global) # set multiqueue enable
(global) # set sleep-on-idle enable
(global) # set elasticbuffer enable
(global) # end
status, interface change will trigger system reboot and
will take effect after the reboot.
Enabling DPDK will adjust Tx/Rx ring size to max
allowable value by PMD for the best performance.
Do you want to continue? (y/n)y

config dpdk global
set status enable
set interface "port1" "port2" "port3" "port4"
set multiqueue enable
set sleep-on-idle enable
set elasticbuffer enable
set per-session-accounting traffic-log-only
set ipsec-offload disable
set hugepage-percentage 30
set mbufpool-percentage 25
end
```

Figure 1. Enabling DPDK on FortiGate-VM on GCP

## FortiGate-VM Firewall Throughput Performance with DPDK Enabled

To measure gen-to-gen network capability for FortiGate-VM on GCP, firewall throughput for different machine types and UDP frame sizes are compared. The benchmark data presented below consider the N2 machine series, a popular choice for NetSec applications, and the C4 machine series. DPDK is enabled for both the N2-Standard and C4-Standard configurations.

Figure 2 shows that the measured FortiGate-VM Firewall throughput of the C4 instances outperforms the prior generation for the selected instances sizes. FortiGate-VM with DPDK enabled running on 5th Gen Intel Xeon Scalable processor, coupled with the Intel IPU accelerated Andromeda network stack, offers consistently high packet throughput performance for FortiGate-VM.

## FortiGate-VM Firewall Operating Costs on GCP

Taking advantage of CSP innovations with Intel technologies is one of the most effective ways to lower operating expense (OpEx) in the public cloud. Upgrading workload VM images to take advantage of modern network interfaces, drivers, and VM generations can lead to significant cost savings. FortiGate-VM is a quintessential example of cost-savings using Intel architecture-based cloud modernization. For example, as illustrated in Figure 3, at the 64-byte packet size the cost characteristics of running FortiGate-VM are improved to 12.65 Gbps/\$ (C4-Standard-4) from 7.72 Gbps/\$ (for N2-Standard-4) at the hourly, on-demand pricing.

## Conclusion

The network protection provided by Fortinet FortiGate-VM is essential for enterprise cloud connectivity. Network security applications such as FortiGate-VM can achieve high throughput at reduced costs by utilizing the latest cloud innovations powered by Intel on GCP. This solution brief has shown that FortiGate-VM deployments running GCP C4 machine series using 5th Gen Intel Xeon and Intel IPU can significantly reduce operational costs versus prior generation GCP machine series.

## Terminology

Abbreviation	Description
DPDK	Data Plane Development Kit
PMD	Poll Mode Driver
Intel® IPU	Intel® Infrastructure Processing Unit
ASIC	Application Specific Integrated Circuit
GVE	Google Compute Engine Virtual Ethernet driver
VM	Virtual Machine
NGFW	Next Generation Firewall
OpEx	Operating Expense

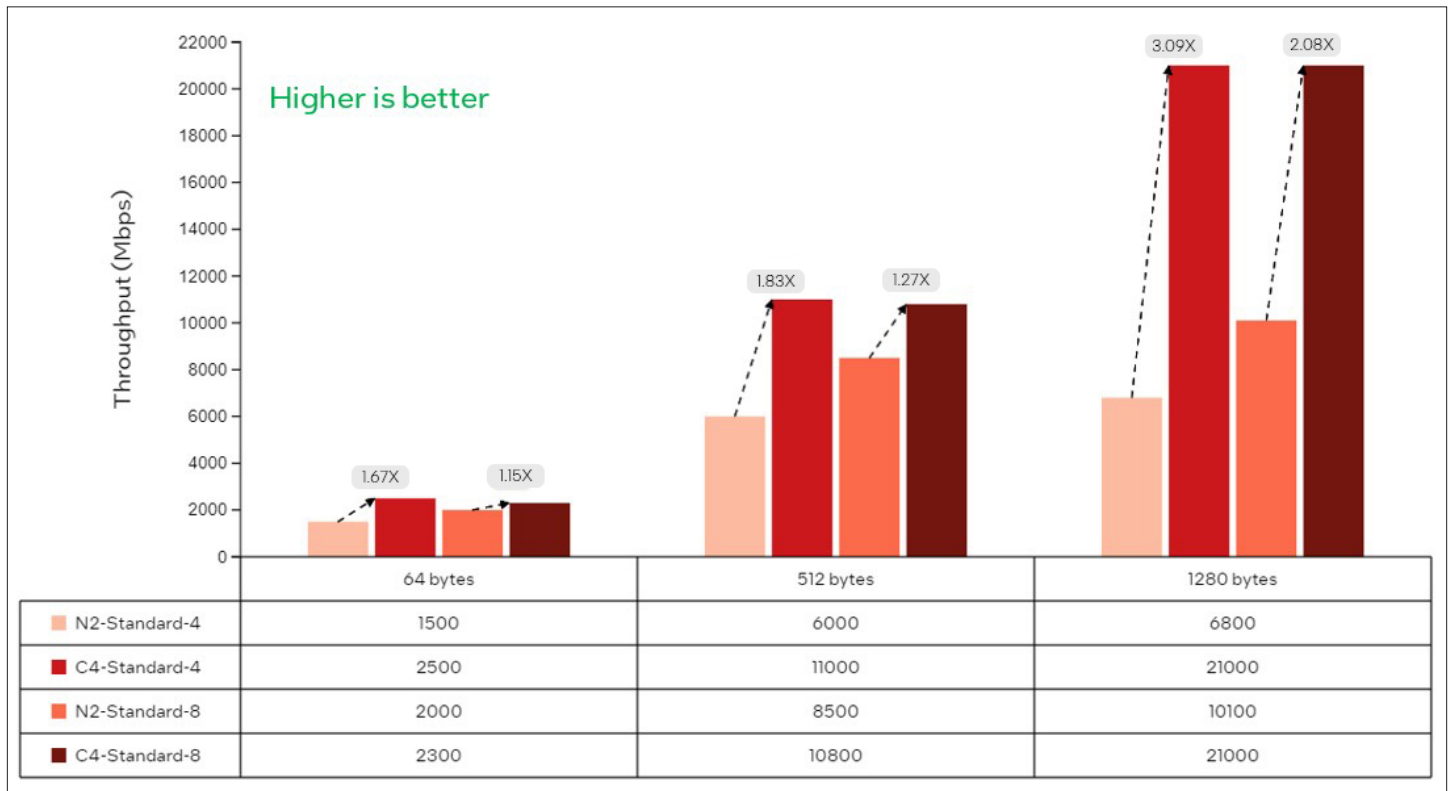


Figure 2. FortiGate-VM Firewall Throughput Performance UDP Frame Size Scaling (DPDK Enabled)

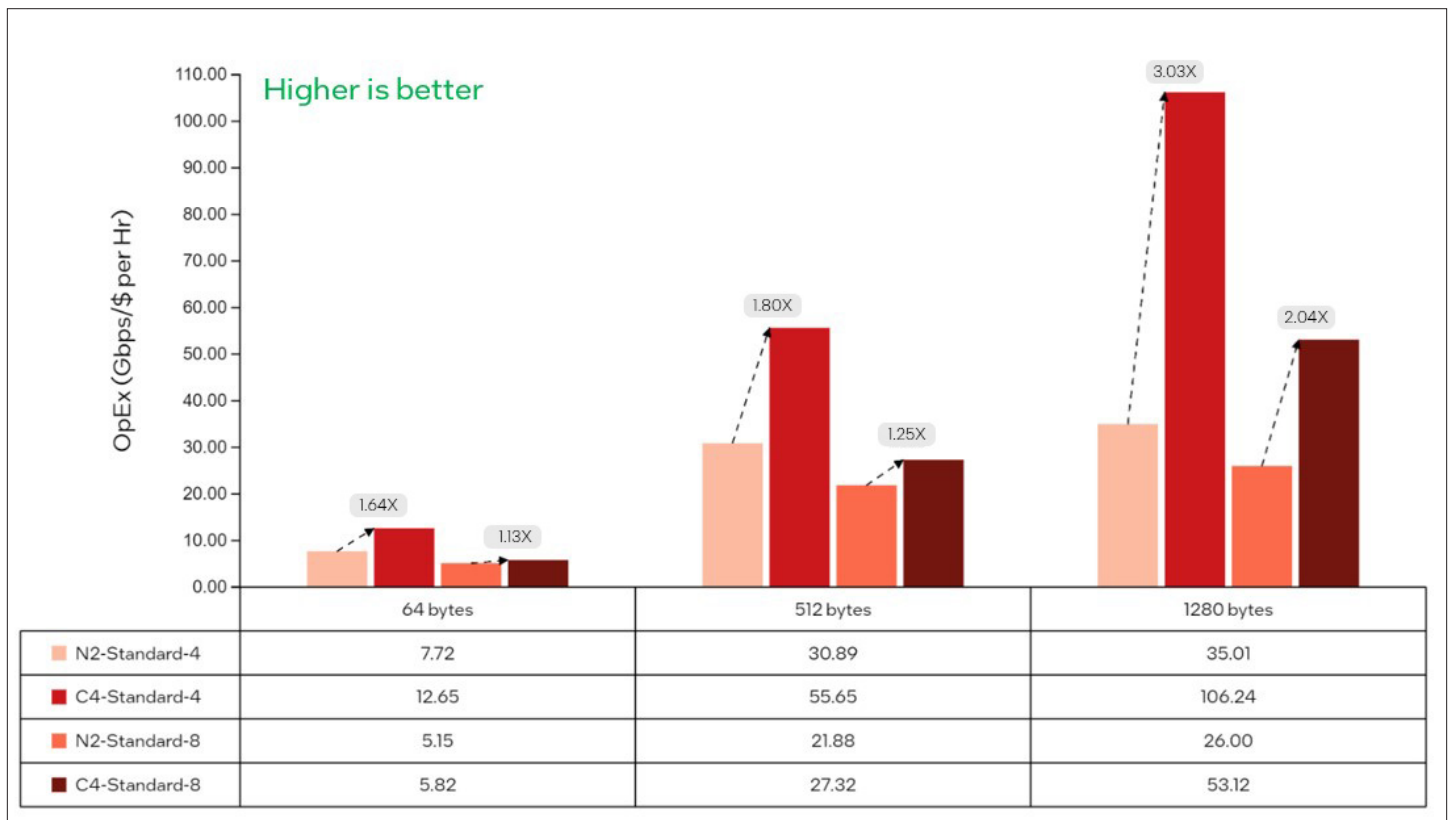


Figure 3. Generational Firewall Throughput Price-Performance Increase<sup>5,6</sup>

## Appendix A - System Configuration

Name	GCP: n2-std-4	GCP: n2-std-8	GCP: c4-std-4	GCP: c4-std-8
System	Google Compute Engine	Google Compute Engine	Google Compute Engine	Google Compute Engine
Base Board	Google Compute Engine	Google Compute Engine	Google Compute Engine	Google Compute Engine
Chassis	Google Other	Google Other	Google Other	Google Other
CPU Model	Intel® Xeon® Platinum 8373C @ 2.60GHz	Intel® Xeon® Platinum 8373C @ 2.60GHz	5th Gen Intel® Xeon® Processor	5th Gen Intel® Xeon® Processor
Microarchitecture	ICX	ICX	EMR	EMR
Sockets	1	1	1	1
CPUs	4	4	8	8
Intel Turbo Boost	Disabled	Disabled	Disabled	Disabled
Base Frequency	2.6 GHz	2.6 GHz		
Maximum Frequency	2600 MHz	2600 MHz	3100 MHz	3100 MHz
Numa Nodes	1	1	1	1
Accelerators	QAT:0, DSA:0, IAA:0, DLB:0	QAT:0, DSA:0, IAA:0, DLB:0	DLB:0, DSA:0, IAX:0, QAT (on CPU):0, QAT (on chipset):0	DLB:0, DSA:0, IAX:0, QAT (on CPU):0, QAT (on chipset):0
Installed Memory	16GB	32GB	15GB	30GB
Hugepagesize	2048 kB	2048 kB	2048 kB	2048 kB
Transparent Huge Pages	madvise	madvise	madvise	madvise
Automatic NUMA Balancing	Disabled	Disabled	Disabled	Disabled
NIC	1x Compute Engine Virtual Ethernet [gVNIC]	1x Compute Engine Virtual Ethernet [gVNIC]	1x Compute Engine Virtual Ethernet [gVNIC]	1x Compute Engine Virtual Ethernet [gVNIC]
Disk				
BIOS	Google	Google	Google	Google
Microcode	0x1	0x1	0xffffffff	0xffffffff
FortiOS Version	7.4.0	7.4.0	7.6.2	7.6.2
Max C-State	9	9	9	9

## References

Reference	Source
Data Plane Development Kit (DPDK)	Heqing Zhu, ed.; Data Plane Development Kit (DPDK), 2021
DPDK Online Documentation	<a href="https://doc.dpdk.org/guides/index.html">https://doc.dpdk.org/guides/index.html</a>
Using Google Virtual NIC	<a href="https://cloud.google.com/compute/docs/networking/using-gvnic">https://cloud.google.com/compute/docs/networking/using-gvnic</a>
Andromeda: Performance, Isolation, and Velocity at Scale in Cloud Network Virtualization	<a href="https://www.usenix.org/system/files/conference/nsdi18/nsdi18-dalton.pdf">https://www.usenix.org/system/files/conference/nsdi18/nsdi18-dalton.pdf</a>
C4 VMs now GA: Unmatched performance and control for your enterprise workloads	<a href="https://cloud.google.com/blog/products/compute/c4-machine-series-is-now-ga">https://cloud.google.com/blog/products/compute/c4-machine-series-is-now-ga</a>
FortiGate-VM on Google Cloud	<a href="https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_GCP.pdf">https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_GCP.pdf</a>
Enhancing FortiGate-VM performance	<a href="https://docs.fortinet.com/document/fortigate-public-cloud/7.6.0/gcp-administration-guide/843654/enhancing-fortigate-vm-performance">https://docs.fortinet.com/document/fortigate-public-cloud/7.6.0/gcp-administration-guide/843654/enhancing-fortigate-vm-performance</a>



### Notices & Disclaimers

<sup>1</sup> [cyberratings.org cloud network firewall](https://www.cyberratings.org/cloud-network-firewall)

<sup>2</sup> <https://cloud.google.com/titanium>

<sup>3</sup> [dpdk gve poll mode driver documentation](https://www.dpdk.org/guides/index.html)

<sup>4</sup> [enabling dpdk on a fortigate-vm deployed on google cloud](https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_GCP.pdf)

<sup>5</sup> All prices reflect hourly on demand rates in the GCP Iowa (us-central1) region. Prices are subject to change.

<sup>6</sup> Only VM demand pricing is considered. In practice, the determination of network IO costs may need to consider data transfer fees and other peripheral costs.

\* Other names and brands may be claimed as the property of others.

Performance varies by use, configuration and other factors.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See configuration disclosure for details. No product or component can be absolutely secure.

Intel optimizations, for Intel compilers or other products, may not optimize to the same degree for non-Intel products.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

See our complete legal [Notices and Disclaimers](#).

Intel is committed to respecting human rights and avoiding causing or contributing to adverse impacts on human rights. See Intel's [Global Human Rights Principles](#). Intel's products and software are intended only to be used in applications that do not cause or contribute to adverse impacts on human rights.

© Intel Corporation. Intel, the Intel logo, Xeon, the Xeon logo and other Intel marks are trademarks of Intel Corporation or its subsidiaries.

0625/MK/PDF

Please Recycle

365930-001US