White Paper

Service Providers
Mobile/Wireless

A10 Thunder® CFW Virtual Appliance Delivers 100Gbps Throughput[1]

A10 Networks achieves 100Gbps throughput and 328,000 connections per second on tests of its A10 Thunder CFW virtual appliance using 3rd Gen Intel® Xeon® Scalable processor and Intel® Ethernet 800 Series Network Adapters

Communications service providers (CoSPs) face challenges in scaling networks to keep up with connectivity demands created by an explosion of internet-connected devices, and expanding coverage into remote, rural geographies. Threat actors are quickly scaling their attacks to keep up with the tremendous growth in connectivity, and CoSPs must protect their expanding customer bases and coverage areas.

The A10 Thunder Convergent Firewall (CFW) provides critical core networking functions that enable CoSPs to help secure and scale their networks. A10 Networks has worked with Intel to benchmark performance1 of its integrated Thunder CFW virtual appliance (vThunder CFW) on servers based on 3rd Gen Intel® Xeon® Scalable processors, showing performance of 100Gbps throughput and 328,000 connections per second (CPS). A10 expects that the product could have tested beyond 100Gbps with additional adapters and more powerful traffic generator.

Security, Capacity and Coverage Challenges Converge

CoSPs must build and manage high performance, resilient networks at a time of exploding internet traffic, continued network expansion, and increasing cyberthreats.

Almost half of the world population is still offline. In the US, an estimated 25 million homes[2] do not have adequate broadband connectivity, mostly located in remote, rural areas that are more costly to provide service. Extending coverage to unserved or underserved areas will require use of multiple access technologies – mobile / 5G, fiber to the home (FTTH), fixed wireless, satellite and others. As more subscribers are connected, more traffic must be carried, and so the core network capacity must be expanded as well.

For mobile networks, global mobile data traffic reached 84 exabytes (EB) per month by the end of 2021 and is projected to reach 868 EB by the end of 2027.[3] While video traffic is estimated to represent 69% of all mobile data traffic today, future growth is driven by the expanding adoption of high-bandwidth, next-generation apps such as augmented reality (AR) and virtual reality (VR). In addition, IDC forecasts the number of connected Internet of Things (IoT) devices will reach over 42 billion by 2025[4].

Multiple technologies are being used to bridge the digital divide. While 55% of the world's population is using the mobile internet, future growth of mobile internet adoption will occur in low- and middle-income countries[5]. Fixed wireless access is expected to have a 73% CAGR between 2021 and 2026[6] according to Mordor Intelligence. Wireline broadband access revenue from both CoSPs and cable operators will grow at 4.56% to total $102.6 billion by 2027 according to GlobalData[7].

IPv4 capacity continues to be a challenge as operators add subscribers to their networks. The number of available IPv4 addresses is dwindling and are expensive to acquire via third parties. Not many operators have made the costly transition to IPv6.

Table of Contents

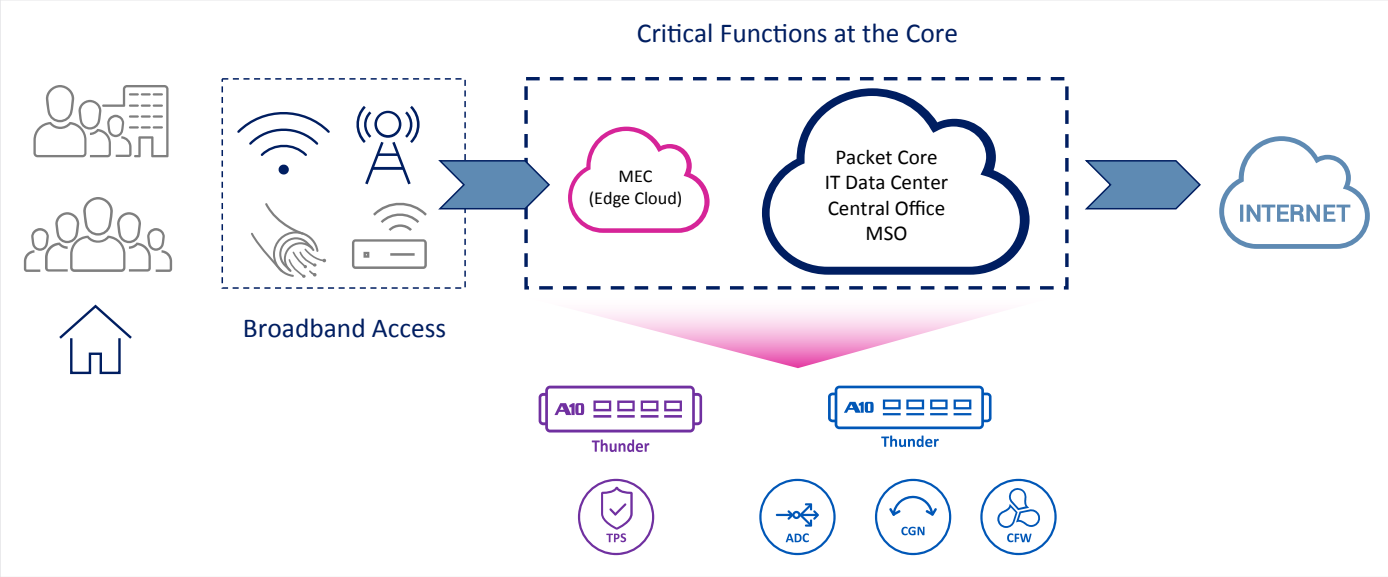

Figure 1. A10 vThunder CFW secures the heart of service provider networks

As the internet expands, so do the security threats. Today, threats to the most sensitive data have become increasingly advanced, creating tremendous risks for companies, governments, cloud providers, network operators, and more. Threats such as distributed denial of service (DDoS) attacks keep accelerating year after year. IDC estimates multiple record-breaking attacks resulted in more than 2.5Tbps of stolen data in 2020.[8]

Investment in security and risk avoidance solutions is critical for CoSPs to protect their customers and stay in compliance with privacy regulations. According to Gartner "by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations, up from 10% in 2020."[9]

A10 Thunder Convergent Firewall Virtual Appliance (vThunder CFW)

A10 vThunder CFW is a converged security solution for service providers, cloud providers and large enterprises that unites application delivery control (ADC), carrier grade networking (for IPv4 preservation and IPv6 transition), and security on a single platform to reduce hardware and operating costs. A10 vThunder CFW is a cost-effective approach for optimizing the delivery and security for potentially hundreds of applications in each data center, strengthening security postures, and enhancing the protection for network perimeters without the need for disparate point products.

A10 vThunder Convergent Firewall Features

Firewall

- Stateful layer 4 network firewall
- L7 application visibility
- L4-L7 services consolidation
- Gi/SGi firewall
- GTP firewall
- Application layer gateways

DDoS Protection

- Integrated DDoS protection for NAT IP pools
- IP anomaly detection
- DDoS protection for Gi/SGi firewall

IPv4 Preservation

- CGNAT (also known as large-scale NAT (LSN)), NAT444, NAT44

IPv6 Migration

- Dual-stack support, full-native IPv6 management and features
- SLB-PT (protocol translation), SLB-65 (IPv4ß àIPv6, IPv6 ß à IPv4)
- NAT 64/DNS64, NAT46, DS-Lite, 6rd, LW4o6, MAP-T, MAP-E

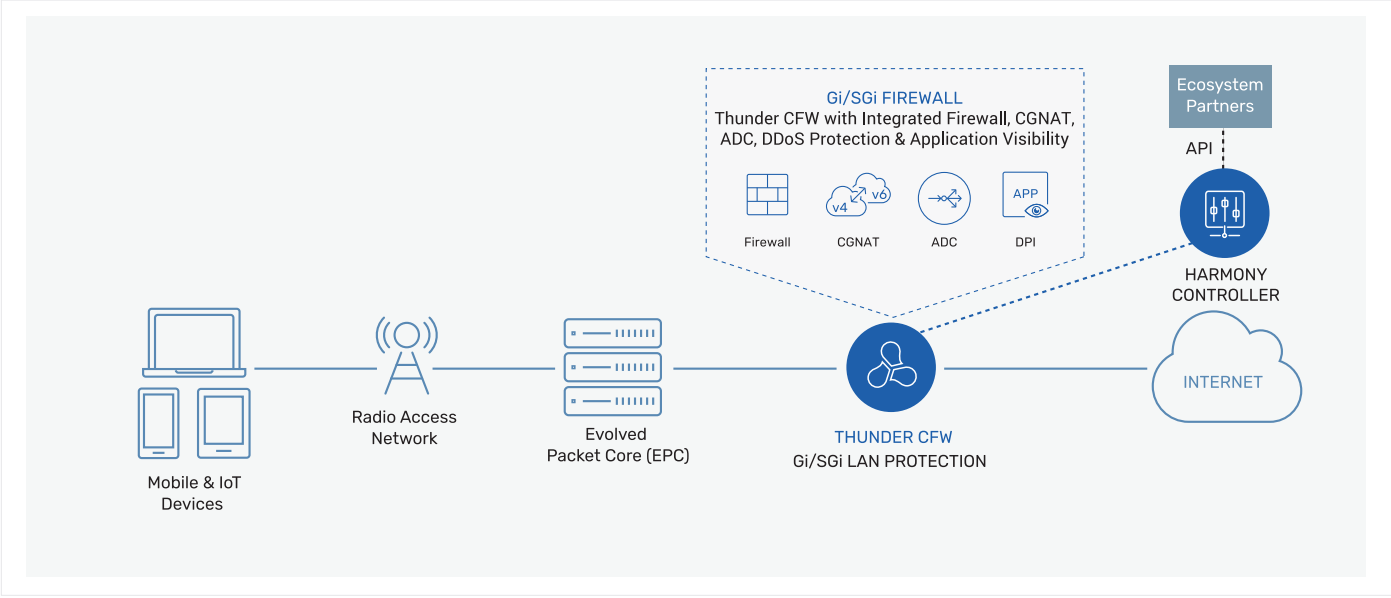

Figure 2. In this scenario, a mobile network operator deploys the vThunder CFW to secure communication between the evolved packet core (EPC) and the internet to protect the mobile core infrastructure. Integrated CGNAT enables carriers to manage communication with both IPv4 and IPv6 address protocols. Built-in DDoS protection safeguards the NAT IP pools to avoid service interruption.

Built on A10's market-proven Advanced Core Operating System (ACOS®), vThunder CFW helps to protect subscribers and shield core infrastructure from cyber-attacks and signaling storms to help minimize operations interruptions, including key mobile network locations like the Gi/SGi, GPRS tunneling protocol (GTP)/Roaming and radio area network (RAN). Deep packet inspection (DPI)-based application visibility with comprehensive subscriber awareness provides granular insights into network traffic. Thunder CFW combines the security of a Layer 4 carrier-grade firewall with integrated DDoS protection features to serve as a carrier-grade networking and server load-balancing solution to protect carrier network assets from the inside out.

Integrated CGN functionality includes carrier-grade network address translation (CGNAT) to both preserve investments in existing IPv4 address infrastructure and deliver comprehensive IPv6 migration capabilities to facilitate a smooth transition to IPv6. Integrated application layer gateways (ALGs) allow applications to remain addressable and to operate transparently through address translation.

A10 vThunder CFW enables carriers to achieve exceptionally high firewall connection rates, throughput, and higher CGNAT session capacity to meet service providers' current and future traffic requirements. The vThunder CFW simplifies operational tasks and reduces capital and operational expenditures through its integrated CGNAT, stateful firewall, and DDoS protection capabilities (Figure 2).

Security Acceleration with Intel

A10 Networks is an Intel® Network Builders ecosystem member and recommends the use of servers based on 3rd Gen Intel® Xeon® Scalable processors and Intel® Ethernet 800 Series Network Adapters for vThunder CFW deployments. 3rd Gen Intel Xeon Scalable processors are optimized for network security - from the network edge to the data center - with the ability to enhance protection for data and applications while in use. With a built-in set of security capabilities, these CPUs help address the current and future data privacy and cyber security concerns.

A10 also makes use of the Intel® QuickAssist Technology (Intel® QAT) cryptography acceleration technology for processing secure sockets layer (SSL) and IPsec traffic. Intel® QAT provides acceleration of data encryption and compression for applications from networking to enterprise, cloud to storage, and content delivery to database.

Select 3rd Gen Intel Xeon Gold Scalable processors support up to 32 cores per processor and up to 8 memory channels at up to 3200 MT/s, driving enhanced performance, throughput, and CPU frequencies compared to previous-gen processors.

The 100GbE Intel® Ethernet 800 Series Network Adapters offer exceptional compatibility, interoperability, and performance to meet the requirements of a demanding range of communications workloads. Features include dual port configuration and 100/50/25/10GbE per port data rates, packet-classification, and sorting optimizations, hardware-enhanced timing capabilities, and a fully programmable pipeline.

Test Network Set Up

The goal of this test is to show scalability and maximum throughput by testing the firewall's performance when the vThunder CFW is run at different CPU core counts.

The system under test (SUT) server was based on a 2.20GHz Intel® Xeon® Gold 6338N processor, which also utilized the Intel® Ethernet Network Adapter E810-CQDA1 E810CQDA1 operating at 100Gbps.

The test set up can be seen in Figure 3. Data flows are generated by the tRex1 and tRex2 servers and transported to the firewall via four 25GbE connections to a switch. The data is switched to the A10 vThunder CFW at 100 Gbps. The firewall creates sessions and processes incoming traffic according to preconfigured firewall rules. These include rules to permit traffic, deny traffic, and CGN rules for NAT translation. Throughput is measured both on the tRex1 and tRex2 servers as well as on A10 vThunder server. Test traffic generation used simple HTTP request/responses with an average packet size of 780 bytes.

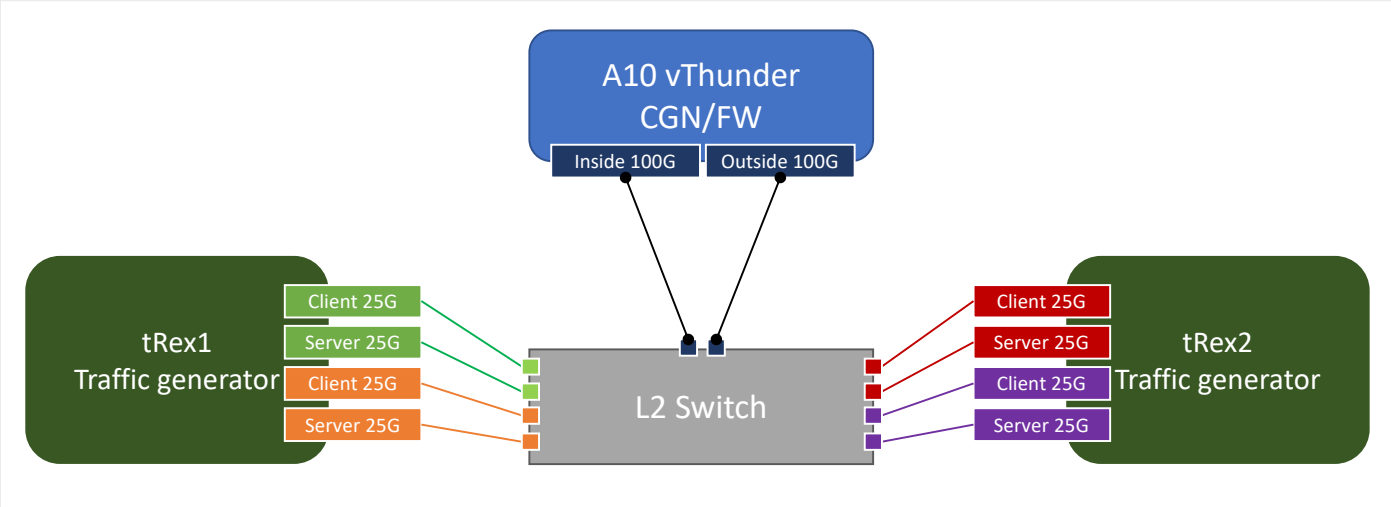

Figure 3. Test configuration for 3rd Gen DUT with traffic flowing from the tRex1 server through a switch to the firewall and then to the tRex2 server.

Software Configuration

The SUT utilized the A10 vThunder CFW software configurations including A10 ACOS operating system (OS) and the ACOS 5.2.1 kernel and workload.

Test Results

The testing results showed a nearly linear response in both data throughput and CPS. These performance metrics were measured at four levels: eight cores, 12 cores, 18 cores and 24 cores. Figure 4 shows the throughput test results with 30Gbps of throughput when using eight cores to 100Gbps at 24 cores. CPS also improved with additional cores – from 100,000 at eight cores to 328,000 at 24 cores.

These results demonstrate that the vThunder CFW can operate at a wide range of network egress / ingress points in a CoSPs network providing a cost-effective solution that can be used network wide for many CoSPs. Based on these tests, A10 believes the limited availability of high bandwidth network adapters kept the vThunder CFW from higher throughput levels and expect that the product could have tested beyond 100Gbps with additional adapters.

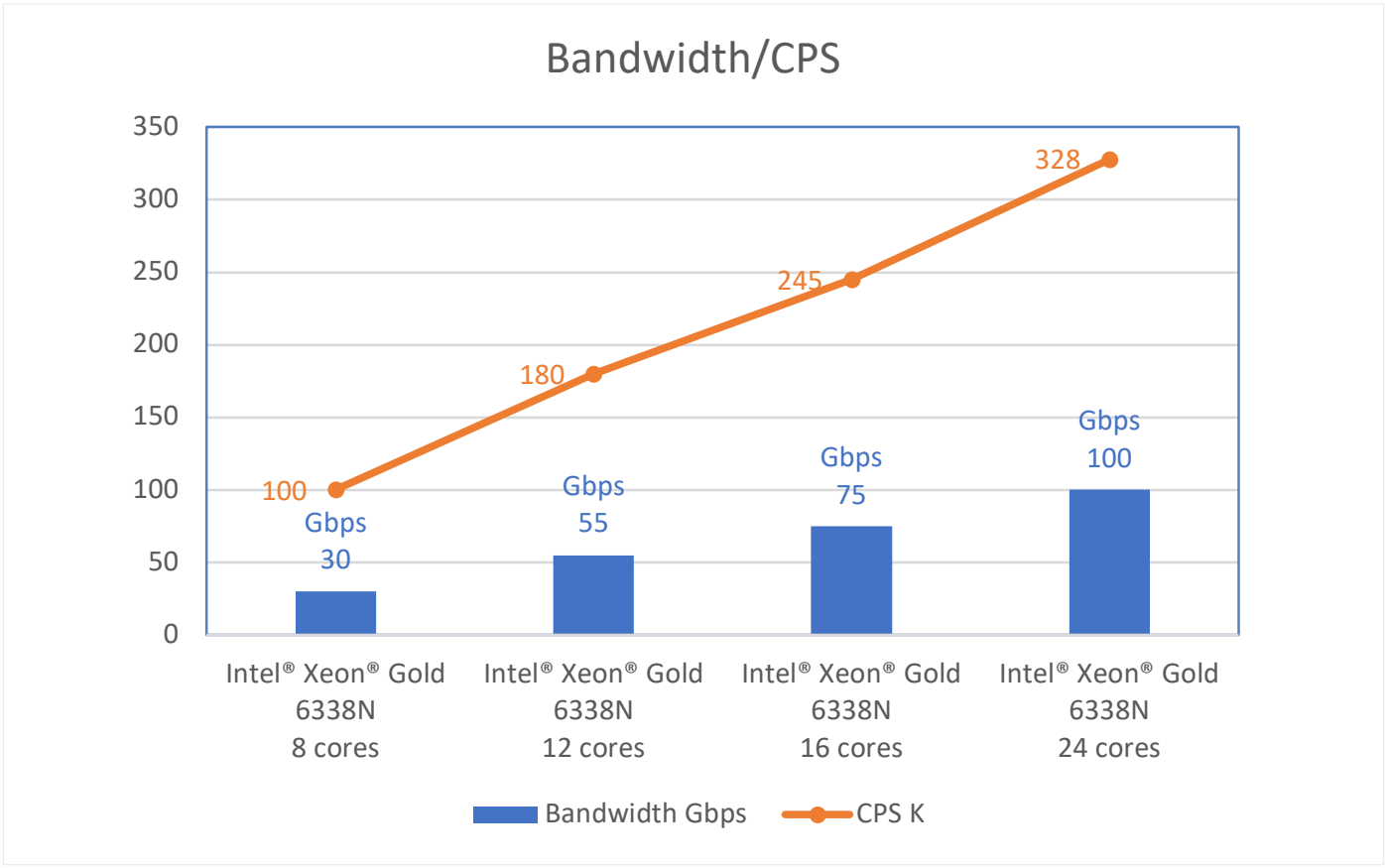

Figure 4. The 3rd Gen Intel ® Xeon® Gold 6338N achieves a 10-15% performance gain over earlier models (higher is better).

Conclusion

With both data traffic levels and cyber security events increasing, it's important to demonstrate state-of-the-art performance for firewalls. The A10 vThunder CFW provides a range of security and networking services and runs on servers powered by 3rd Gen Intel® Xeon® Scalable processors and Intel® Ethernet 800 Series Network Adapters. The vThunder CFE is able to scale with the number of dedicated cores to deliver 100Gbps throughput on real world traffic profiles using only 24 cores. This performance and the vThunder CFW feature can help CoSPs to offer improved security services throughout their network.

Learn More

A10 vThunder Convergent Firewall

A10 Network

Intel® Xeon® Gold Scalable processors

Intel® QAT

Intel® Network Builders

Notices & Disclaimers

[1] SUT: 2-nodes, 1x 2.20GHz Intel® Xeon® Gold 6338N with Intel® Ethernet Network Adapter E810-CQDA1 E810CQDA1, and 16 slots/32GB/2666 MT/s total DDR4 memory, microcode revision=0xd000363, HT Yes, Turbo No, A10 ACOS operating system (OS) and the ACOS 5.2.1 kernel and workload. Test conducted by A10 Networks on Aug. 10, 2022

[2] https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2020-broadband-deployment-report

[3] https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast

[4] https://www.a10networks.com/wp-content/uploads/IDC-DDoS-Defenses-Enter-the-AI-Era-Automation-Drives-Business-Resilience-and-Growth.pdf

[5] https://www.gsma.com/r/somic/

[6] https://www.mordorintelligence.com/industry-reports/fixed-wireless-access-market

[7] https://www.broadbandtechreport.com/docsis/article/14280145/report-hfc-will-remain-dominant-in-us-home-cable-broadband-market-share

[8] https://www.a10networks.com/wp-content/uploads/IDC-DDoS-Defenses-Enter-the-AI-Era-Automation-Drives-Business-Resilience-and-Growth.pdf

[9] https://www.gartner.com/en/newsroom/press-releases/2020-09-14-gartner-says-by-2023--65--of-the-world-s-population-w

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

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

Your costs and results may vary.

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

0123/LV/H09/PDF ♻Please Recycle 354191-001US