SOLUTION BRIEF

EFFICIENT GI-LAN IN CONSOLIDATING DPI AND CGNAT INTO GI-FW

CONSOLIDATING GI-LAN COMPONENTS HELPS IMPROVE NETWORK LATENCY AND TOTAL COST OWNERSHIP (TCO)

Mobile network operators have reached a new stage in building the new 5G network that will enable and support rapid proliferation of mobile and the Internet of Things (IoT) devices. Today's LTE and 4G network has been playing an important role in providing mobile broadband services (e.g., video calling, high-definition content streaming, etc.) across millions of mobile and connected devices. 5G is designed not only for adopting more mobile devices, but also for supporting billions of emerging IoT devices. This enables digitalization and evolution among various industries such as medical, entertainment and smart cities, including business-critical and life-critical services that necessitate the avoidance of interruptions at all cost.

Mobile operators need to consider a scalable and high-performance network infrastructure to support huge volumes of traffic and connected devices. Meanwhile, the operators also need to maintain a wide range of network service functions in the Gi-LAN segment such as firewall, carrier-grade NAT (CGNAT), traffic optimization, deep packet inspection (DPI) and more. The motivation for inclusion of such Gi-LAN services is to offer better security and value-added services. However, operators need to take account of introducing extra network latency by chaining these services that run on different appliances. Consolidating Gi-LAN service components helps minimize network latency, improves operational efficiency and lowers the total cost of ownership (TCO).

CHALLENGE

While 5G opens great opportunities to introduce innovations, mobile providers have various network functions in the Gi-LAN segment, including firewall, CGNAT and DPI, to differentiate and monetize services. Deploying these functions from different vendors makes the 5G network inflexible and affects performance.

SOLUTION

A10 Thunder CFW provides a consolidation of Gi-LAN service components at scale, leveraging Gi/SGi firewall, CGNAT, DDoS protection, load balancing and DPI including application visibility. Using Thunder CFW, A10's 5G Gi-LAN solution greatly helps reduce network components as well as latency.

BENEFITS

- Flexible Gi-LAN with multiple network function consolidation
- 5G network performance improvement with latency reduction by eliminating extra hops
- Operational efficiency by simplifying Gi-LAN network structure
- Lower TCO with less-managed appliances

THE CHALLENGE

The continuous evolution of 5G is aimed at enhancing mobile broadband services, next-generation networks and standards designed for the emerging Internet of Things (IoT). 5G opens great opportunities to introduce new types of applications and services in various industries. These include high-definition (4k/8k) content streaming, real-time interactive AR/VR and tactile internet for entertainment and mission-/life-critical services like remote surgery, self-driving cars, smart cities and many more. In order to fulfill requirements, three use cases are defined for 5G:

1. Enhanced Mobile Broadband (eMBB) for use cases requiring a higher data rate
2. Ultra-Reliable and Low Latency (URLLC) for mission-critical services that require reliable, lower-latency connectivity
3. Massive Machine Type Communication (mMTC) for higher density and capacity to support a massive number of connected devices

Carrier-grade networking solutions may be implemented to scale the network infrastructure for speed and capacity upgrade—maintaining uninterrupted connectivity and high network availability—to provide the best possible customer experience. Adding networking nodes to scale out its capacity is a relatively easy change, however, it in turn adds more complexity and challenges from an operational and management perspective.

It is also true and noteworthy in the Gi-LAN segment, where service providers offer essential IP-based services like Gi/SGi firewall and CGNAT, enhanced security services and value-added services such as parental control and contents caching. Deploying these service functions using dedicated appliances from various vendors makes the Gi-LAN network inflexible and complex to manage and operate. Furthermore, multiple service functions are usually chained so that each service function adds extra latency to the traffic. This may severely impact the quality of mission-critical services.

THE A10 NETWORKS 5G GI-LAN SOLUTION

A10 Thunder® CFW is a high-performance, converged security solution for service providers that consolidates Gi/SGi firewall, CGNAT, IPsec VPN, ADC, DPI for visibility and other capabilities, including subscriber-aware intelligent traffic steering, into a single solution. Thunder CFW, whether physical or virtual, delivers unmatched performance and comprehensive security services to support the 5G-ready mobile infrastructure. This solution is a cost-effective approach for strengthening security postures and protecting network perimeters without the need for disparate point products.

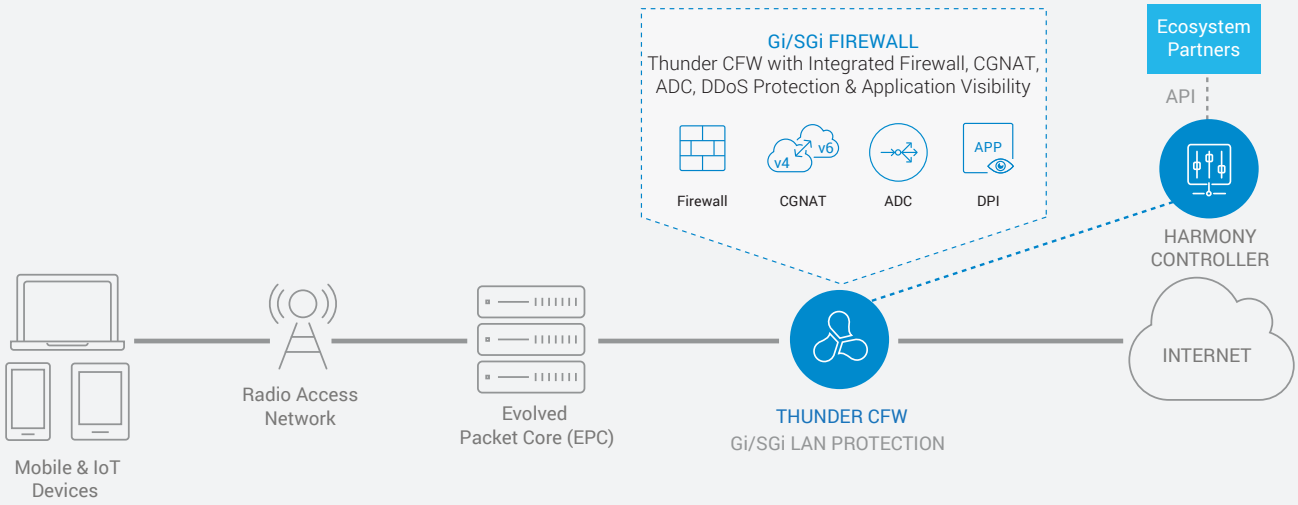

Figure1: Efficient Gi-LAN architecture using Thunder CFW, consolidating Gi-LAN services utilizing integrated firewall, CGNAT, load balancing, DDoS protection and deep packet inspection (DPI) capabilities into one. DPI provides subscriber awareness and application visibility for controlling and steering subscriber traffic to relevant service functions.

HIGHLY EFFICIENT GI-LAN SERVICE CONSOLIDATION

In the 5G network, most of the IP-based services, such as enhanced security services and value-added services to differentiate service experience and monetize new services, are deployed in the Gi-LAN segment. Due to the nature of the Internet, carrier-grade network address translation (CGNAT) continues to play a key role for service providers to preserve their current IPv4-based infrastructure investment, and to provide a smooth transition to IPv6 networking and seamless subscriber access to resources, regardless of the type of IP version used. Thunder CFW includes comprehensive CGNAT functionality for IPv4 preservation and IPv6 migration with industry-leading performance and capacity.

Thunder CFW also provides exceptionally high firewall connection rates, throughput and concurrent sessions for Gi/SGi LAN protection, which incorporates a stateful firewall with a rich feature set, performing granular traffic control over network resources and protecting subscribers' traffic as well as services from a wide array of threats. Deep packet inspection (DPI) is also one of the essential service functions in Gi-LAN that is available on Thunder CFW, which expands service offerings in many ways. Other capabilities such as ADC, traffic steering and integrated DDoS protection are inclusive and can be enabled concurrently.

A10's 5G Gi-LAN solution—consolidating the Gi/SGi firewall, CGNAT, DPI and other L4-7 functions like subscriber-aware intelligent traffic steering, etc.—helps improve end-to-end latency drastically as it removes extra hops for data packet to traverse and provides greater Gi-LAN efficiencies, simplifying operational tasks and maintaining low TCO objectives.

APPLICATION VISIBILITY USING DPI

Understanding network and application traffic trends enables effective network planning, deeper business intelligence, value-added services, tighter security controls, enhanced Law Enforcement Agency (LEA) compliance and service monetization.

Thunder CFW's DPI-based application visibility provides a detailed view of traffic trends in application types, categories, top sources for each application category and so on. Operators can gain full insight of network traffic, service and application-level visibility and subscriber awareness, including types and identities of subscribers, while applying Gi/SGi firewall and CGNAT functions onto the data traffic within the product.

Such detailed visibility into the applications, subscribers and content traversing the network empowers operators to control traffic granularly and flexibly using traffic steering, without adding extra latency. This enables new opportunities for differentiated value-added services and a better customer experience.

The application visibility feature can also be enabled in a passive or TAP mode deployment by having the TAP/SPAN device or port mirroring on routers forward the copy of the traffic to Thunder CFW. This enables operators to gain network and application visibility without interrupting service traffic.

HIGH-PERFORMANCE ARCHITECTURE WITH AGILITY

The A10 Networks Advanced Core Operating System (ACOS®) powers Thunder CFW, leveraging unique software and hardware design advantages to deliver exceptional performance and scalability. This enables Thunder CFW to deliver the performance that mobile operators require to scale and protect their networks, with the ability to provide up to 220 Gbps of throughput while supporting over 250 million concurrent sessions in small form factor (1 RU) hardware appliance. Thunder CFW is also available in software form factor, with an unmatched performance of a maximum of 100 Gbps, deployed as a virtual machine running on various kinds of hypervisors or bare metal (COTS). The solution is horizontally scalable, and up to eight nodes can be added as traffic grows.

ACOS also provides an open REST API that covers 100% of the configuration and operation, enabling easy integration with SDN controllers and NFV MANO—for example, OpenStack, Open Source MANO (OSM), Ericsson EO and NEC NetCracker to name a few. This provides flexibility and agility for network planning and operation to mobile operators.

INTUITIVE GI-FW AND APPLICATION VISIBILITY ANALYTICS

Thunder CFW provides detailed traffic data and statistics for each service such as CGNAT pools and Gi firewall rules, which helps mobile operators gain service-level visibility and insight into service traffic. This allows better prediction and effective network planning.

The A10 Harmony® Controller fully utilizes telemetry data and session logs from Thunder CFW and provides a comprehensive service traffic dashboard for operators as well as intuitive, per-service analytics for better operation. All of the telemetry data and session logs are accessible via A10's REST API or syslog, which offers easy integration with third-party NMS (Network Management System) and SIEM (Security Information and Event Management). Thunder CFW also offers a Splunk App for Gi-firewall and application visibility so that operators with existing deployments of Splunk can easily import application visibility data and analytics into their Splunk platforms.

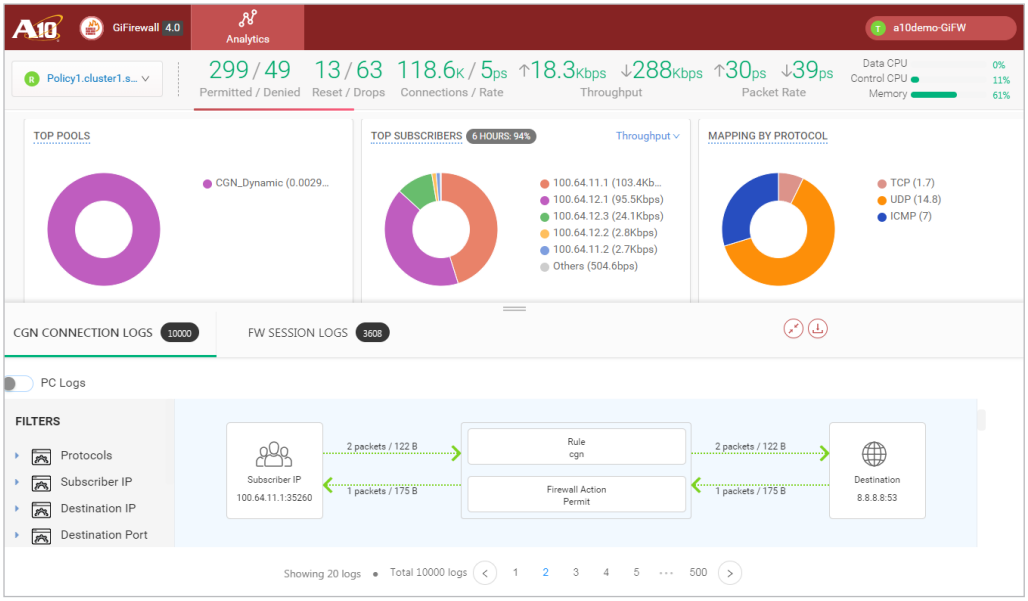

Figure 2: Harmony Controller analytics dashboard for GiFW, providing firewall counters, CGNAT pool status, top subscribers, application visibility, a detailed session log and much more.

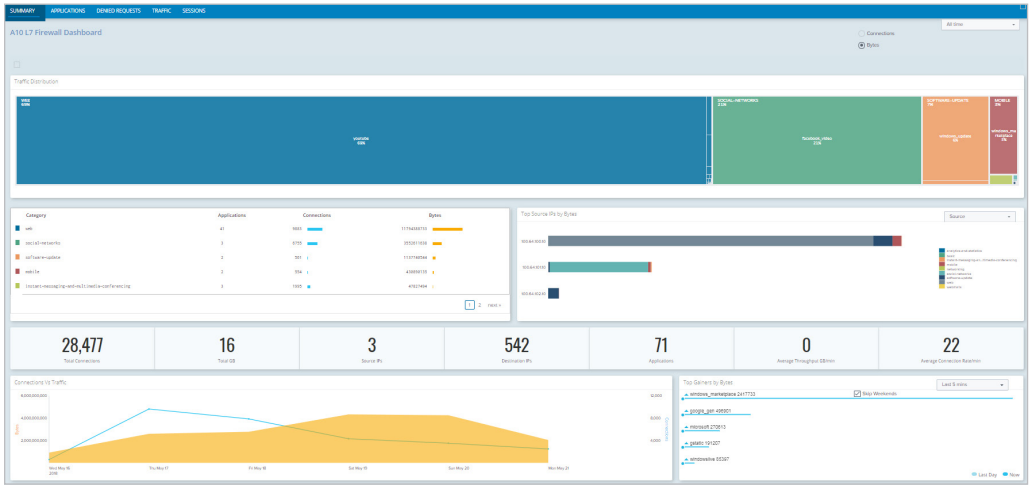

Figure 3: Splunk App for A10's Gi firewall and application visibility

SOLUTION COMPONENTS

- A10 Thunder Convergent Firewall (Thunder CFW)
- Gi/SGi Firewall
- Carrier-Grade NAT
- Deep Packet Inspection (DPI)
- Application Visibility and Control
- Traffic Steering
- Harmony Controller
- aXAPI® REST-based API

SUMMARY

A10's 5G-GiLAN solution enables Gi-LAN service consolidation and provides L4–L7 service functions, including Gi/SGi firewall, CGNAT, GTP firewall, DDoS protection, load balancing, traffic steering and DPI for application visibility and control concurrently on a single appliance, whether in a physical or virtual form factor. The consolidation architecture approach using Thunder CFW greatly helps simplify network components and reduce latency.

A10 Thunder CFW is a powerful and comprehensive security solution built on A10's Advanced Core Operating System (ACOS®) platform, delivering the ultra-high performance needed to meet current and future mobile and cloud network deployment needs. This comprehensive approach provides best-in-class performance and scale to protect the mobile infrastructure while reducing OPEX and CAPEX.

NEXT STEPS

For more information, please contact your A10 representative or visit a10networks.com/solutions/5g-mobile-network-security.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19196-EN-01 DEC 2018