SOLUTION BRIEF

# Critical Core Network Technology for Rural Broadband Buildout

Carrier-grade Security and Availability for Regional ISPs

## Overview

Regional ISPs play a key role in closing the digital divide – covering unserved and underserved communities – and providing faster, more secure, and innovative services to all subscribers. It is a daunting task for the thousands of WISPs, FTTH providers, MNOs, electric utilities/co-ops, incumbent LECs, and other rural providers that are stepping up to close the gaps. They often do so with fewer resources, less funding and lower revenue per location than their tier 1 counterparts.

Regional ISPs must consider multiple critical core network functions, including IP connectivity, application delivery and DDoS protection, early in the planning process for a new build-out or network expansion. The price of scarce IPv4 addresses keeps rising and IPv4 must co-exist with IPv6 for years to come. In addition, threat actors are eyeing the broadband expansion with a different view—millions of new potential victims in remote, lightly secured areas.

Regional ISPs need trusted technology vendors that align with their business goals and can provide solutions with carrier-grade resilience and security. For over a decade, A10 Networks has focused on meeting regional and global service providers' unique requirements, and now counts hundreds of live deployments across the globe. Our mission is to help ensure the success of regional service providers as they strive to close the broadband gap.

### Challenge

To meet business growth and subscriber expectations, regional ISPs must look beyond last-mile access and modernize their core network for critical carrier-grade functions such as IP connectivity, application delivery and security within limited budget and resource constraints.

### Solution

The A10 Networks portfolio for regional ISPs provides advanced carrier-grade networking solutions at an affordable price and suitable form factor. The portfolio includes high-performance CGNAT with IPv4-IPv6 migration, application delivery control and DDoS threat detection and mitigation.

### Benefits

A10 Networks' industry expertise and portfolio enables worry-free deployment. The A10 solutions help minimize initial investment and reduce investment risk with flexible deployment and price options for rapidly expanding networks.

# The Challenges

## Broadband Investment Risk

Regional ISPs have aggressive plans to extend broadband to new or underserved communities and must build the core network so that it will continue to meet growing traffic and subscriber demands yet stay within limited budget and resource constraints. Despite recent government incentives, many investment risks remain in growth of the core network.

- How quickly will subscribers adopt services?
- How much will traffic distribution change and volume grow?
- What protection is needed against cyberthreats?

Build-out plans over the next 3-7 years may be doubling or tripling network coverage, but core network investment decisions must be made today to meet the capacity and functionality for long-term network size. Regional ISPs must make sound decisions despite demand uncertainty and still closely align investment dollars to revenue growth. These decisions determine whether higher subscriber expectations are met over the long term and impact the return on the broadband investment.

The A10 portfolio for regional ISPs helps reduce investment risk and minimize initial investment through carrier-grade technology designed so ISPs can pay as they grow. The portfolio includes Thunder® CGN, Thunder® TPS, Thunder® ADC, and Thunder® CFW with flexible deployment, form factor and price options for rapidly expanding broadband networks.

## IPv4 Demand is High, Supply Uncertain and Costs Rising

To grow the subscriber base, regional ISPs need an IP address assigned for every new subscriber. Many regional ISPs do not have sufficient IPv4 addresses to extend their networks and cannot easily integrate readily available IPv6 addresses into existing network architecture. New supply for IPv4 addresses through the regional internet registries (RIR) is limited with long wait times. Acquisition of IPv4 on the public market is costly—up to $60 per IPv4 address. Regional ISPs need both a cost-effective solution for the immediate IPv4 exhaustion and a seamless longer-term path to eventual IPv6 transition.

This urgent capacity shortage can be eliminated with A10 Thunder CGN, which includes carrier-grade network address translation (CGNAT), enabling one IPv4 address to be shared by as many as 64 subscribers. The same solution also provides IPv6 transition features, so ISPs can be assured that their investment will last for years into the future as the traffic becomes more IPv6 dominant. Market-proven in Tier 1 operator deployments across the globe, the Thunder CGN software and appliances provide the carrier-grade performance, features and scalability needed by regional ISPs, at a budget they can afford.

## DDoS Threatens Vulnerable Communities and Critical Infrastructure

Distributed denial of service (DDoS) attacks have surged in the last couple of years and now comprise over half of all security incidents. Every year, the size, duration, and frequency of DDoS attacks increases. Rural communities are especially vulnerable to DDoS attacks due to underinvestment in security infrastructure, lack of cybersecurity expertise and dependence on few sources of critical infrastructure such as healthcare that are favorite targets for attackers. Regional ISPs are being called into the front lines of today's cyber battle, serving the remote edges of the connected society, but without the resources, capital budget or expertise of their much larger Tier 1 counterparts.

A10 Thunder Threat Protection System (TPS) provides a highly scalable, highly configurable DDoS mitigation solution for regional service providers trying to maintain the integrity of network availability to their communities and provide advanced protection for critical business customers. Deployed by regional ISPs, Tier 1 operators, and top gaming companies, A10 has the market-proven expertise to meet the needs of a growing ISP.

## Growing Traffic Demand with Limited Staff and Budget

Regional service providers that are now upgrading their networks and extending broadband access face challenges that are radically different from those seen only a few years ago. Complex new virtualization architectures and cloud data centers are on the rise. Network traffic is expanding exponentially as are the number of connected devices per household and business. Now nearly all traffic is encrypted, placing additional processing burdens on legacy network elements not designed for decryption functions.

The limited IT resources of regional ISPs are being asked to do more with less—budget, workforce, and infrastructure. Yet expansion plans are aggressive and subscriber expectations keep rising for higher availability, speed and security and lower latency.

Thunder ADC can optimize network efficiency and services, keep pace with growing traffic loads and offload strained backend network elements. Functions include traffic steering and service chaining to multiple value-added services, load balancing, and reliable termination of encrypted traffic. Thunder ADC helps ensure your business applications are secure, consistent, and highly available in your on-premises data center or any multi-cloud environment. With our high-performance and efficient solution, you can build and operate critical business applications with lower TCO.

## A10 Networks Portfolio for Regional ISPS

The A10 Networks portfolio provides critical core networking functions that help regional ISPs scale and secure their network more efficiently. Tier 1-proven for over a decade, the same carrier-grade functionality and resilience is available for regional ISPs in capacity sizes, form factors and price points that meet their budget and technical requirements and provide worry-free deployment.

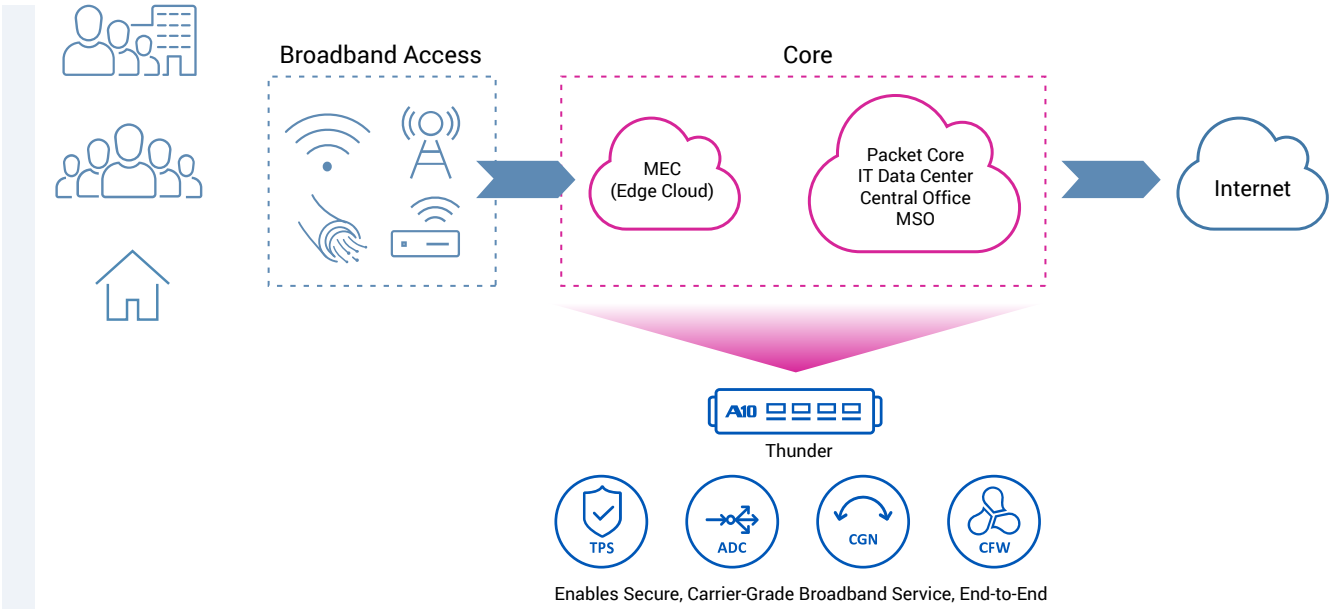


**Figure 1**: A10 secures the heart of service provider networks

# Features and Benefits

## High Performance and Scalability

All Thunder physical, virtual and container appliances are designed for the highest performance and scalability. ISPs can build capacity incrementally, starting at 5 Gbps up to 370 Gbps in a single 1.5 RU device, depending upon solution and form factor.

## Thunder Convergent Firewall (CFW)

Thunder CFW provides industry-leading high performance as a physical, virtual, or containerized solution. Thunder CFW is a high-performance, all-inclusive security product and includes all Thunder ADC and CGN features. Thunder CGN and Thunder ADC can also be licensed individually.

### Flexible Deployment and Pricing Options (Thunder CFW, ADC, CGN)

All Thunder CFW options run on A10's ACOS® software, providing feature parity, regardless of form factor, which helps simplify and consolidate operations in any deployment environment. Pricing and licensing options enable regional ISPs to "pay as they grow" to minimize initial investment.

- FlexPool® options allow ISPs to allocate and change licensed capacity across multiple locations or instances.
- Subscriber-based licensing (Thunder CGN only), enables ISPs to minimize initial capital outlay for CGNAT and IPv4 addresses and align IPv4 investment with revenue. This software-only option starts at 1,000 subscribers and can be licensed in increments of 1-5 years.
- Scale-out features ensure all devices operate as one and enable easy integration of new devices.

### Management and Analytics

- A10 Harmony® Controller provides management and analytics to gain subscriber and network services visibility, detect anomalous trends, centrally configure, and manage policies and simplify capacity planning, improve service reliability
- Thunder TPS supports an industry-standard CLI, on-box GUI, and the aGalaxy management system. The CLI allows sophisticated operators easy troubleshooting and debugging. The intuitive on-box GUI enables ease of use and basic graphical reporting. aGalaxy offers a comprehensive dashboard with advanced reporting mitigation console, and policy enforcement for multiple TPS devices.

## Thunder Carrier Grade Networking (CGN)

A10 Thunder® CGN provides high-performance CGNAT with protocol translation that allows service providers and enterprise to extend IPv4 investment while simultaneously transitioning to IPv6 standards.

- IPv4 preservation with CGNAT enables IPv4 addresses to be shared by multiple devices. Typically, broadband ISPs can support 16-64 locations (homes) with a single IPv4 address.
- IPv4-IPv6 transition enables a smooth transition to IPv6 by supporting translation and tunneling, including DS-Lite, 6rd, Lw4o6, NAT64/DNS64 and MAP-T/MAP-E.
- Advanced features for logging and sensitive applications ensure service continuity for all subscribers.
- Security capabilities protect IPv4 address pools from DDoS attacks

## Thunder Application Delivery Control (ADC)

A10 Thunder ADC ensures these applications are highly available, accelerated, and secure. It helps reduce downtime, ensure business continuity, and build highly available applications across data centers or clouds. Thunder ADC delivers L4-7 load balancing and multiple layers of security via web and DNS app firewalls, single sign-on (SSO) authentication and in-depth support for advanced encryption, including high-performance PFS/ECC.

- **Application Delivery Partitions**: Support multi-tenant environments with application delivery partitions (ADP). Configure more than 1,000 ADC tenant partitions on a single appliance that also enables Layer 3 virtualization.

- **Advanced Server Load Balancing**: Thunder ADC is a full-proxy, load-balancing and content switching solution. With aFleX® scripting, deep packet inspection, comprehensive load-balancing algorithms and persistence support, Thunder ADC enables application-layer visibility to optimally route inbound requests.
- **Recursive DNS**: Thunder ADC provides a powerful recursive DNS capability enabling a one-stop DNS solution that makes it a perfect solution for a regional ISP seeking to consolidate DNS services and drive higher customer satisfaction.

## Thunder Threat Protection System (TPS)

Downtime results in immediate productivity and revenue loss for any business. Thunder TPS ensures service availability by automatically spotting anomalies across the traffic spectrum and mitigating multi-vector DDoS attacks. Thunder TPS protects organizations from attacks of all sizes, from 1 to 380 Gbps (or 3 TBps in a list synchronization cluster). It is available in 1-3 RU appliances or virtual appliances.

- **Multi-vector Attack Prevention:** Detect and mitigate DDoS attacks of many types, including volumetric, protocol, application-level attacks and IoT-based attacks.
- **ZAP**: The Zero-day Automated Protection engine utilizes heuristic and machine learning to automatically discover mitigation filters without advanced configuration or manual intervention.
- **aGalaxy**: Is available with an optional integrated Thunder TPS detector that supports tightly integrated interworking of Thunder TPS DDoS mitigation, flow-based DDoS detection, system-wide management, and robust reporting.

## Summary

Regional internet service providers (R-ISPs), including wireless and wireline/FTTH operators, electric cooperatives and municipalities have long played a vital role in supplying critical power and connectivity to rural and remote communities. Now, these diverse regional ISPs are poised to play a crucial role in connecting the remaining unserved communities. Leveraging new government funding, ISPs have a unique opportunity to help their communities leap ahead in digital adoption, providing them new capabilities that are often absent in high-tech urban areas with older infrastructure.

But leaping ahead will require a focus on the network end-to-end—not just on the critical last-mile. The supporting core network technologies and systems must also be strengthened to provide overall digital resiliency and security of their network, while meeting rising subscriber expectations.

The A10 Networks portfolio for regional ISPs provides the most advanced carrier-grade networking solutions in a price point and form factor that meets the requirements of rapidly expanding regional ISPs. The portfolio includes high-performance CGNAT with IPv4-IPv6 migration, application delivery control, carrier class firewalls, and DDoS threat detection and mitigation.

The same functionality is provided regardless of device size or form factor. A10 solutions are deployed in over 270 service providers across the globe, including the largest telcos, mobile network operators, cloud providers and gaming companies. In the U.S., regional ISPs of all sizes use A10 technology to support subscriber growth for rural broadband build-out.

## Next Steps

For more information, go to the rural broadband solution page or contact A10 today to learn more.

## About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

## Learn More

About A10 Networks

Contact Us

A10networks.com/contact



Part Number: A10-SB-19210-EN-01 Jan 2023