A10

The Next Steps for Secure IPv6

The A10 security portfolio provides critical protection to vulnerable devices and subscribers as IPv6 adoption accelerates.

Exponential Growth Forecasted

Over the last ten years, there has been explosive growth of the Internet of Things (IoT) and other connected devices, with predictions of over

26 billion

by 2026 according to Ericsson.

The cyberthreat landscape has also rapidly expanded with increased levels of DDoS attacks, ransomware and other threats against connected devices, subscribers and networks. For cybercriminals, the unrelenting growth of often poorly protected connected devices is seen as a rich source of **potential weapons**.

Service providers have overcome the growth constraints of IPv4 exhaustion with a combination of carrier-grade NAT (CGNAT) and the near-unlimited quantities of IPv6. While many service providers are comfortable using (CGNAT) to expand IPv4 address pools, the security vulnerabilities of hybrid IPv4 and IPv6 networks are often not addressed, and service providers must protect both.

Global IPv6 Adoption Accelerates

Worldwide, the adoption of IPv6 to replace IPv4 continues to increase, albeit at a slower pace than many industry advocates had hoped.

Service providers recognise the benefits of IPv6 (including improved efficiency, heightened authentication and encryption security, more simplicity and better quality of service) and are committed to IPv6 adoption. Additionally, implementing IPv6 can lead to competitive advantage, service differentiation and increased market share, helping providers on their journey to further network and security benefits in the future.

However, the full switch to IPv6 usage requires the simultaneous conversion of endpoints, networks and internet hosts (web sites). This does not happen overnight. It seems clear that service providers - who must provide connectivity to all - will need to support both IPv4 and IPv6 in their networks for some time into the future.

In this document, we cover some of the growing cyber-risks of rising IPv6 adoption, and explore how the A10 security solutions portfolio, including A10 Defend and A10 Thunder Convergent Firewall (CFW), with carrier-grade NAT, can unlock additional value for service providers.

Implementing IPv6 can lead to **competitive advantage,** service differentiation and increased market share, helping providers on their journey to further network and security benefits in the future.

Larger Footprint Means Greater Exposure to Risk

A successful

Cyber attack

can lead to negative publicity, legal fines and a decline of subscriber trust

CGNAT is a standard for network address translation that helps providers bridge the transition to IPv6. CGNAT also provides additional security benefits as it acts as a barrier between the public-facing internet and internal devices. Without CGNAT, internal IPv4 devices are more exposed to threats from the public network.

With CGNAT, IPv4 addresses of individual devices are “hidden” in a pool of private IPv4 addresses behind one or more public IPv4 addresses. In contrast, devices using IPv6 are directly exposed to the internet, making them more easily accessible to cyber criminals.

As IPv6 is used for more and more of their subscribers’ devices, service provider networks and their customers are increasingly vulnerable to this growing digital threat landscape.

Service providers must protect both IPv4 and IPv6 environments.

A successful cyberattack can be devastating to a service provider, leading to negative publicity, legal proceedings and fines, and resulting in a decline in subscriber trust.

Demand for bandwidth is growing at an exponential rate, but the average revenue per unit is declining as service revenues grow at a much slower rate. When compounded by DDoS and other cyberattacks that exploit vulnerabilities and cause excessive network traffic, service providers may incur extra unexpected costs for additional bandwidth, traffic rerouting and network optimisation. Service providers therefore need to implement appropriate firewall, volumetric attack prevention and use threat intelligence to protect their own network and subscribers consuming revenue-generating services.

Delivering Robust Security

A10 Networks works with most of the leading alternative network and service providers, and we share their journey from conception and planning to network maturity, enabling diverse business and revenue streams. IPv6 adoption is needed, alongside other modernisation initiatives, to provide more scalable, secure, and efficient networking infrastructure. In fact, service providers should be positioning IPv6 as a service differentiation and using it as a springboard to attract new customers.

A10 Networks' security portfolio provides highly cost-efficient security solutions with the flexibility, scalability and protection service providers need as they evolve their networks.

Our portfolio provides a comprehensive security stack at service provider scale with other functions including a firewall, deep packet inspection (DPI), CGNAT and IPv6 migration, integrated DDoS threat protection, intelligent traffic steering and analytics.

The A10 Thunder Convergent Firewall® (CFW) solution provides robust security for both IPv4 and IPv6 traffic. As the industry transitions to IPv6, it is crucial to have a firewall ensuring that traffic is inspected and protected, minimising the risk of security breaches.

Our portfolio provides a comprehensive **security stack** at service provider scale

The A10 Thunder CFW also features CGNAT and contains several additional security capabilities that organisations need after they move to IPv6. In effect, it provides scalable high-performing GTP firewall, GiLAN firewall, IPsec VPN, secure web gateway, DNS over HTTPS (DoH), and CGNAT with integrated DDoS protection for the provider's network and customers. Furthermore, Thunder CFW provides exceptionally high firewall connection rates, low latency, throughput and concurrent sessions for the most demanding use cases in compact and flexible form factors.

Service providers can also use A10 Networks' advanced threat protection capabilities to block a wide range of malicious activities including DDoS attacks, malware, intrusion attempts, application layer attacks and more.

Moving from Cost Benefit to Security Benefit

A10 delivers protection at

high scale, high speed

and low latency

Given the high market price of scarce IPv4 addresses, organisations can also gain near-term cost benefits from moving to the nearly unlimited IPv6. However, as cyber threats grow and competition increases, cost alone is not a sufficient source of competitive advantage. Service providers must create a security benefit from their investment, with protection of both IPv4 and IPv6 environments a priority.

A10 Networks can deliver protection at high scale, high speed and low latency, enabling new services and better user experience via advanced features such as fair usage policies, ensuring subscriber retention remains high. Our portfolio of security solutions enables new business opportunities and revenue streams both today and in the future. We enable providers to tailor their services for business users with upsell opportunities to scale and grow at every stage of their journey.

Use case scenarios

Our security solutions help in the following scenarios:

IWF Filtering

The Internet Watch Foundation (IWF) focuses on making the internet a safer place by identifying and removing global online child sexual abuse imagery. As part of its mission, the IWF provides service providers with an accurate and current list of URLs to facilitate the blocking of inappropriate content. IWF Filtering allows providers to effectively block these URLs.

A10 Networks offers an engineered solution capable of receiving and accepting feeds of malicious networks, users and domains. The A10 Thunder CFW is designed to integrate with this intelligence, allowing for robust monitoring and action. Additionally, a Webroot subscription incorporates IWF information, enhancing our ability to provide comprehensive protection for users. Positioned strategically in the network, the A10 Thunder CFW effectively leverages this intelligence on behalf of service providers.

A10 Thunder CFW effectively leverages this **IWF intelligence** on behalf of service providers.

Fair Usage Policies

Service providers have experienced that events causing large downloads for high proportions of users on their network can cause other users to have a reduced experience, for example smart TV updates or game console updates. This leads to frustrations, complaints, and bad online reviews, which impact the provider's brand and reputation.

Fair usage policies are a way for providers to identify these events and limit the amount of bandwidth available when this happens, so they can provide the fastest average broadband speed to as many customers as possible. When enforced, such policies are barely noticeable to the person downloading the update and it allows providers to maintain the quality of service expected by people using their connection.

The A10 Thunder CFW supports service providers in offering fair usage policies and setting these policies based on the overall needs of their subscriber base.

A10 Thunder CFW supports service providers in offering fair usage policies

Rogue CPE Protection

The Telecom Security Code of Practice strongly recommends that all providers use a threat intelligence feed such as A10 Defend Threat Control to provide actionable insights into rogue customer premise equipment (CPE). For example, this could be a TV set top box that is compromised, allowing bad actors to take control and use the device as part of a large attack vector. In other words, a DDoS attack which enables all the compromised devices to send requests to a service at the same time to bring that service down.

Thunder CFW and A10 Defend Threat Control deliver a fully engineered and compliant solution. The A10 Defend portfolio provides a holistic DDoS protection solution that is scalable, economical, precise, and intelligent to help providers ensure optimal user and subscriber experiences.

The Telecommunications

Security Code of Practice

recommends that providers use a threat intelligence feed

A10 is committed to supporting service providers to deliver critical protection to vulnerable devices and subscribers as IPv6 adoption accelerates

Request a live demo and experience the

A10 Networks difference

Schedule a Demo

Find out more about:

Uber Solves IPv4 Exhaustion at Scale

Download Case Study

ABOUT A10 NETWORKS

A10 Networks provides security and infrastructure solutions for on-premises, hybrid cloud, and edge-cloud environments. Our 7000+ customers span global large enterprises and communications, cloud and web service providers who must ensure business-critical applications and networks are secure, available, and efficient.

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 is A10-BR-20117-EN-01 October 2024