DATA SHEET

A10 HARMONY CONTROLLER

AGILE MANAGEMENT, AUTOMATION, ANALYTICS FOR MULTI-CLOUD ENVIRONMENTS

A10 Harmony® Controller provides centralized agile management, automation and analytics for A10 secure application services deployed over various underlying infrastructure —from data centers to private, public and hybrid clouds.

PLATFORMS

aws

ORACLE Cloud

vmware

NUTANIX

openstack.

TALK WITH A10

WEB
a10networks.com/controller

CONTACT US
a10networks.com/contact

AGILE MANAGEMENT & ANALYTICS FOR ANY APPLICATION ENVIRONMENT

The A10 Harmony Controller provides centralized management and analytics for A10 secure application services including A10 Thunder® ADC, SSLi®, CFW, and CGN in multi-cloud environments for application configuration and policy enforcement.

The integrated application delivery and security solution collects, analyzes and reports on traffic flowing through A10 Thunder and A10 Lightning® ADC. The centralized analytics over A10 SSLi, CGNAT, and CFW visualize security posture with integrated dashboards for better operational efficiency.

With the Harmony Controller, organizations can efficiently automate deployment and operations of application services, increase operational efficiency and agility, enhance end-user experiences and reduce TCO, simplify the management of distributed application services to dramatically shorten troubleshooting times, receive alerts on performance or security anomalies, improve capacity planning and optimize IT infrastructure and cloud environments.

FEATURES AND BENEFITS

The Harmony Controller simplifies operations and increases the agility of the operations teams. Infrastructure and application operations teams can centrally manage infrastructure configuration and application policies for A10 Thunder and Lightning application services — such as load balancing, application delivery and web application firewall. Configuration and control can also be automated via APIs and integrated with orchestration systems used within organizations. In addition, the controller provides comprehensive infrastructure and per-application metrics and analytics for performance and security monitoring, anomaly detection and faster troubleshooting.

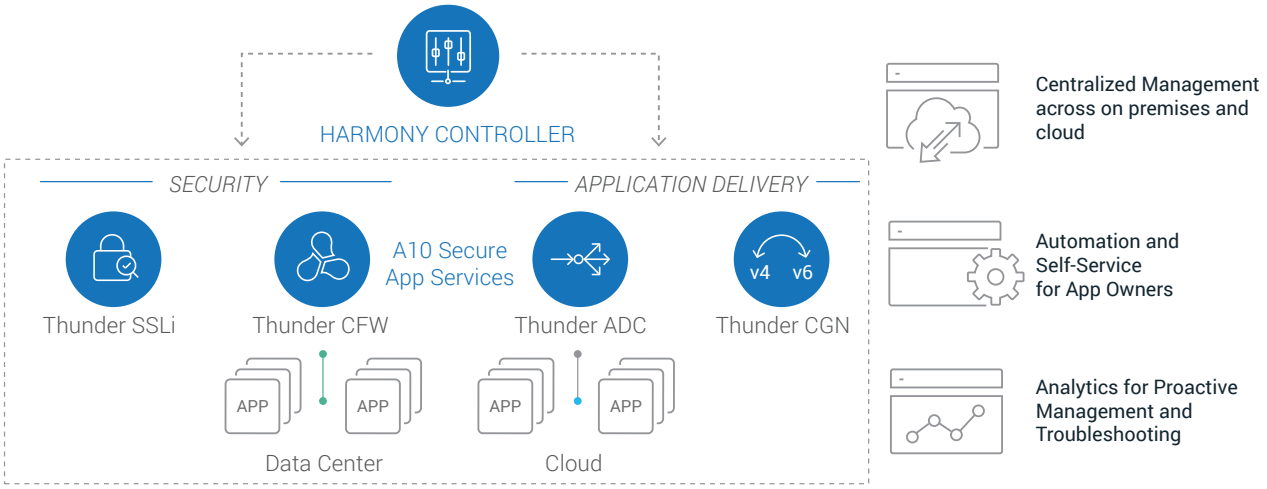


Figure 1. The Harmony Controller and Lighting ADCs can function in multiple clouds. Harmony Controller is centralized management with automation and visibility.

CENTRALIZED MANAGEMENT

Centralized management for A10's broad product portfolio of secure application services including ADC, SSLi, CFW and CGN. Easily configure and manage policies across applications deployed in data centers, private and public clouds.

TRAFFIC AND SECURITY ANALYTICS

Gain visibility and actionable insights into the application traffic. Simplify troubleshooting via access to contextualized data and logs. Analyze collected data to detect anomalous trends. Get alerts based on various metrics and customizable fields. Alerts delivered via email or web-hook URL for automated and rapid action.

MULTI-TENANCY AND SELF-SERVICE

Hierarchical tenancy model enhances agility without compromising governance across the infrastructure. Create application teams and service owners as tenants and allow them to manage their own infrastructure and application policies.

DEVICE LIFECYCLE MANAGEMENT

Centralized device lifecycle management for A10 hardware appliances or virtual instances. Easily manage large number of devices by grouping devices and applying common templates. Backup and restore configuration and perform scheduled software upgrades.

API DRIVEN AUTOMATION

Comprehensive APIs to integrate with DevOps tool chains like Ansible, Chef, Jenkins and orchestration systems like VMware VRO/VRA, Cisco Cloud Center, Microsoft Azure, Google Cloud Platform, Amazon Web Services and more. REST APIs are available for application configuration, device operations and accessing analytics data.

HIGHLY SCALABLE AND PLATFORM AGNOSTIC

The Harmony Controller's container-based, microservices architecture allows controller capacity to be scaled without interrupting operations. Deployments can be on bare-metal, virtualized servers and on public or private clouds.

INGRESS CONTROLLER FOR KUBERNETES

A cloud-native approach for traffic management and application networking services for enterprise-class load balancing, service discovery, security, and analytics for container-based applications running in any Kubernetes clusters.

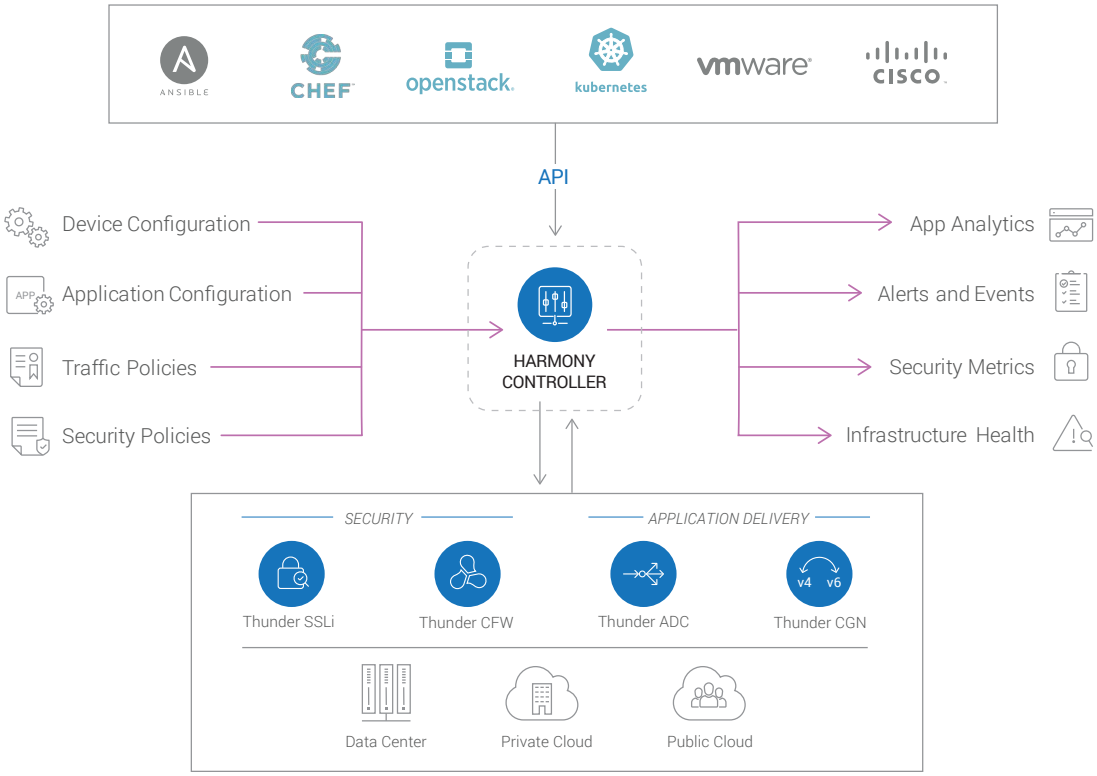


Figure 2. Harmony Controller provides analytics and security metrics and serves as a device manager for Thunder and Lightning ADCs, which can be deployed in a private, public or hybrid cloud. Harmony Controller supports self-service with full RESTful APIs.

HARMONY CONTROLLER INTERFACES

The Harmony Controller allows organizations to achieve centralized management and control over A10 application services, their various policies and obtain real-time visibility with analytics and alerts. Administrators utilize the Harmony Portal to interface with and configure the controller, which leverages Harmony APIs to manage the various application services.

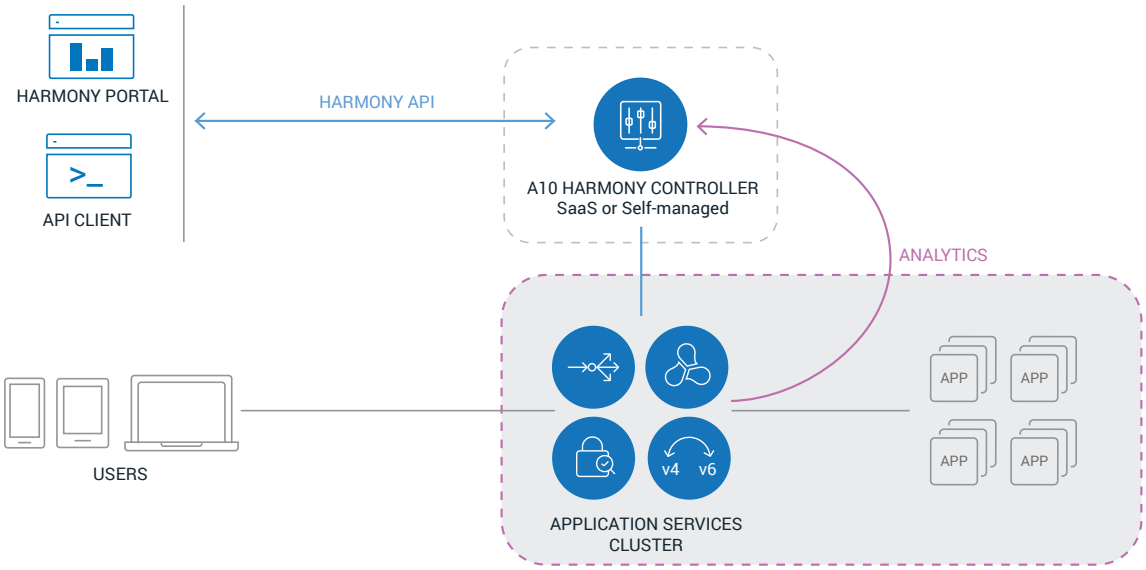


Figure 3. The A10 Harmony Controller manages various application services, client APIs and administrative capabilities. This deployment model helps organizations configure all policies in a central location, regardless of where application services are deployed.

HARMONY PORTAL

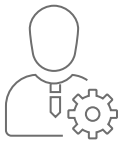
The portal is an intuitive graphical user interface for managing application delivery infrastructure and associated policies on a Per-App basis. The self-service capability eliminates the need for centralized IT admins to set up and configure the per-application infrastructure, maximizing agility and operational savings to support multiple application teams.

HARMONY APIs

These APIs enable orchestration and configuration. All application service capabilities are available via the RESTful interface. APIs may be used to integrate with deployment automation tools like Chef, Puppet and Ansible, as well as CI/CD tools like Jenkins. Analytics APIs also provide access to Per-App metrics and logs. They may be used to integrate with third-party tools or to help build custom dashboards.

DEPLOYMENT MODELS

The A10 Harmony Controller is available in two deployment models – A10 Managed SaaS or as a self-managed, on premise deployment. Consuming it as a SaaS makes it extremely simple and cost-effective to deploy and operate.



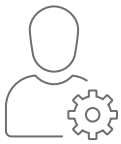
SAAS – MANAGED BY A10

Available as a service, the cloud-based Harmony Controller subsystem is fully managed and monitored by A10. Application teams can directly get a 'Tenant' account on SaaS Harmony Controller or the IT team of the organization can get a 'Provider' account and manage their own internal or external tenants.

Only control messages, metrics and telemetry data are sent between the controller and service instances, via a secure, SSL-encrypted channel. Application traffic does not flow through the controller. This ensures application data remains within the customer's network.

The controller is built on top of a hardened operating system, installed in a highly available configuration and hosted at a public cloud provider. The A10 Networks' team runs regular security scans and audits for security vulnerabilities. The controller offers multiple layers of security that are reviewed to ensure security and compliance.

The SaaS controller is in an isolated environment with network – layer ACLs and access is granted to authorized personnel. Data exchanges within the subsystems are encrypted using strong ciphers and sensitive data like passwords; SSL private keys are stored in the database with strong encryption. External access is always through industry-standard SSL communication. Harmony Controller is available in AWS Marketplace and AWS GovCloud regions as a SaaS offer with Lightning ADC.



ON PREMISES DATA CENTER

The controller may also be deployed as a customer-managed, scalable software solution or hardware appliance within a customer's environment in data centers or clouds, including bare metal server, VMware-powered clouds, Amazon Web Services, Google Cloud Platform and Microsoft Azure.

The self-managed controller can be installed on any physical or virtual machine instance running CentOS or RHEL 7.4 and up operating system. The internal microservices architecture of the controller maximizes the availability of the controller. Additionally, the architecture ensures that the traffic disruption never happens even if connection between the controller and application services is down.

SYSTEM REQUIREMENTS

Harmony Controller software can be installed on odd number of machines. For production deployments, three nodes in the cluster are appropriate. Actual resource requirement depends on the number of managed devices and analytics needed. Microservices of the controller are distributed over these three instances. Data storage is also distributed over these three instances.

NODE CONFIGURATION	DESCRIPTION
Single node deployment	16 CPU, 64 GB RAM, 1.2 TB persistent storage (SSD preferred)
Three node deployment	8 CPU, 32 GB RAM, 500 MB persistent storage (SSD preferred) for each

A10 HARDWARE APPLIANCE MODELS

The Harmony Controller is also available as A10 hardware appliance. These applications may be used for the self-managed controller. The following appliance models are available:

MODEL	HC8000	HC2000
Appliance Form Factor	2U rack mountable	1U rack mountable
CPU	Intel Xeon	Intel Communication Processor SoC
	20 Cores (40 HT)	16 Cores (16 HT)
Memory (RAM)	128 GB	64 GB
Storage: Removable Disk Drives	4 x 3.5"	1 x 3.5"
	4 x 6 TB HDD	6 TB HDD
	No Bay blank	No Bay blank
Power Supply	Dual 500W RPS	Dual 750W RPS; DC option available
	80 Plus Silver efficiency	80 Plus Platinum efficiency

PRICING

The controller software subscription is priced based on the bandwidth units consumed by managed devices. The bandwidth unit pool can be used flexibly to managed different devices with varied bandwidth units. The subscription packages are available for one or three year packages. Gold support is included with all software subscription packages. Device licenses are required to be purchased separately.

SUPPORTED APPLICATION SERVICES

The Harmony Controller currently supports a variety of A10 secure application services and third-party solutions.

A10 THUNDER ADC

(HARDWARE, VIRTUAL AND BARE METAL)

The traditional A10 ADCs are available as an appliance, virtual appliance or machine image for bare metal servers.

The A10 Networks team runs regular security scans and audits for security vulnerabilities. The controller offers multiple layers of security that are reviewed to ensure security and compliance.

A10 LIGHTNING ADC

The cloud-native ADC software is available for public clouds, private clouds and container environments.

A10 THUNDER SSLI

A10 Thunder SSLi product line's SSL Insight® feature eliminates the blind spot imposed by SSL encryption, offloading CPU-intensive SSL decryption functions that enable security devices to inspect encrypted traffic.

A10 THUNDER CFW

A10 Thunder Convergent Firewall features a data center firewall, site-to-site IPsec VPN, Gi/SGi firewall and secure web gateway for service providers and enterprises.

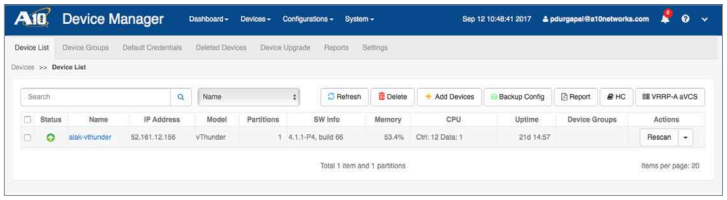
A10 THUNDER CGN

A10 Thunder® CGN provides high-performance, highly transparent network address and protocol translation that allows service providers and enterprises to extend IPv4 network connectivity while simultaneously transitioning to IPv6 standards.

DETAILED FEATURE LIST

CENTRAL DEVICE MANAGEMENT

Device Groups	Multiple Thunder ADCs can be grouped into logical groups so that same operation can be done on all of them in one shot.
Running Commands on Devices	Single or a batch of CLI commands can be pushed to individual device or to a group.
Device Upgrades	Upgrade of Thunder ADC can be done remotely using Harmony Portal.
Health Monitoring of Devices	Harmony Controller monitors both Lightning ADC as well as Thunder ADC and trigger appropriate action.
Device Config Backup and Restore	Thunder ADC is a state-full device. Its configuration can be backed up from Device Manager of Harmony Portal. Backups can be copied and stored outside Harmony Controller.
Automatics Orchestration and Auto-Scale of ADCs	In certain environments, Harmony Controller launches the Lightning ADCs as per configuration. It also scales up/down the Lightning ADC instances as required for traffic.
Manage ADCs in Multiple Clouds	Harmony Controller manages Thunder ADC, as well as Lightning ADC, deployed across various cloud environment in different geographies.
Automate Lightning ADC in Kubernetes Clusters	Integrated with Ingress resources for enterprise routing configuration and dynamically deploy Lightning ADC on demand.



OPERATIONS

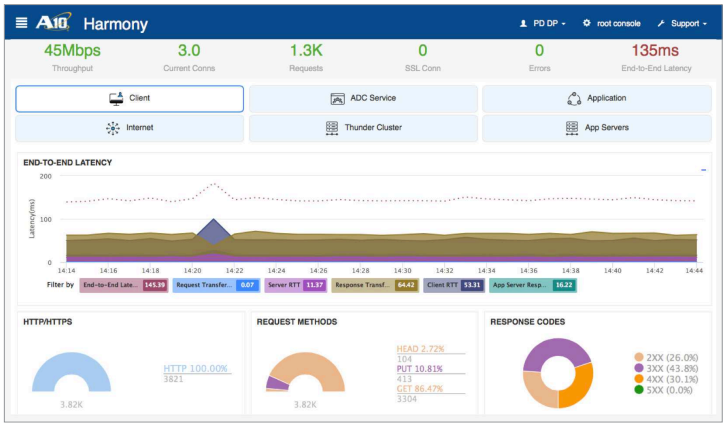
RESTful APIs	Every operation including device management, application configuration, reading analytics data etc., can be done using Harmony APIs. Any integration or automation can be achieved using these APIs.
Multi-tenancy via Provider-Tenant Model	Management functions are divided between Provider and Tenant. Harmony Controller can host multiple providers. Each provider can have multiple tenants and multiple users. There is no limit or license imposed on the number of management entities (Providers, Tenants or Users). 500+ management entities may be created as needed.
Role-based Access Control	Users with appropriate permissions at provider, tenant or device level can access only the areas they are authorized to. Multiple users can login simultaneously and administer their respective areas.
Alerts	Metrics collected from ADCs are correlated and evaluated against user-defined rules for raising alerts. These alerts are delivered via email for manual action and via webhook for automation.
Periodic Security Data Updates	A10 Networks subscribes to security updates released periodically by researchers. A10 security teams monitor and publish relevant updates regularly. The controller facilitates threat intelligence updates from the central repository to the Lightning ADCs.
External Authentication	A provider can select the authentication provider for its users. Other than local user authentication, Google OAuth or Any LDAP based server can be chosen.
Configuration Backup	Harmony Controller configuration can be backed up by copying and storing externally.

INSTALLATION AND MAINTENANCE

Platform Agnostic Installation	The Harmony Controller software can be installed in any environment on physical or virtual Linux machines.
Scalable and Self-healing Micro-services Based Architecture	The controller internally consists of multiple micro-services. The framework brings back the micro-service automatically if it dies. Capacity of controller can be increased at runtime without impacting the traffic.
Configuration via APIs	Configuration of controller itself can be monitored and changed via the APIs exposed by the controller.
Alerts	Metrics collected from ADCs are correlated and evaluated against user-defined rules for raising alerts. These alerts are delivered via email for manual action and via webhook for automation.

ANALYTICS

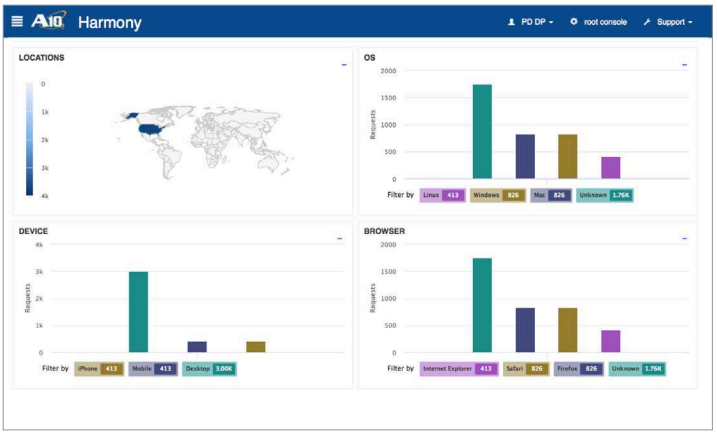
Response Time Monitoring and Details	End-to-end response time between client and server is reported with the ability to drill-down into any specific area.
Granular Traffic Insights and Analytics	Traffic information is aggregated at account level and can be drilled down to per-application and per-request level.
Security Insights and Analytics	Traffic passing through ADC is inspected for security threats and reported for better protection.
Server Health Monitoring	Server monitoring and traffic information coming from ADCs is correlated for predicting health of the server.
Per-Request Analysis and Application Access Logs	Analysis capabilities are provided on per-request application access logs for better troubleshooting.



CHARTS

CLIENT CHARTS

End-to-End Latency	Shows response time clients are experiencing for the app traffic and components of latency.
Requests Rate HTTP/HTTPS Request Methods	At what rate requests are being sent, how many of them are using SSL and what HTTP methods are being used.
Response Codes	Shows if clients are getting successful response or errors.
Locations	Geographical distribution of client requests, bandwidth, latency distribution on world maps.
OS Device Browser	Distribution of technical properties of the client in form of clients' Operating System, Device Type (phone, tablet or desktop) and web browser being used.
Top Clients	Displays IP addresses of the clients sending maximum requests.



ADC SERVICES

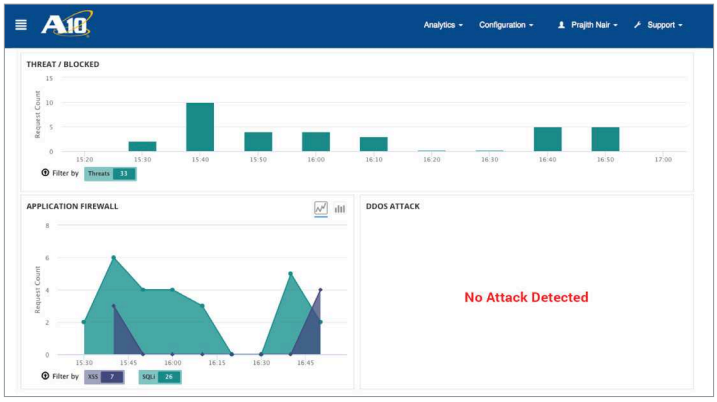
Cache Hits Cache Utilization Cached Entries	Number of requests and bandwidth served from the cache.
Throughput	Aggregate and time-series distribution of throughput.
Client SSL Connection	Aggregate and time-series distribution of SSL connections made by clients.
Load Distribution	Distribution of requests to different application servers.
CPU Utilization Memory Utilization Bandwidth	Health parameters of the ADC cluster.

APPLICATIONS

Response Time	Time series of response time from servers.
Top URL Top Domains Top Services Top Port	Each graph displays URLs, Domains, Services and Ports getting maximum traffic.
Servers Health	Server health index calculated from various health parameters.
Connections	Time series graph of number of connections to servers from ADC.

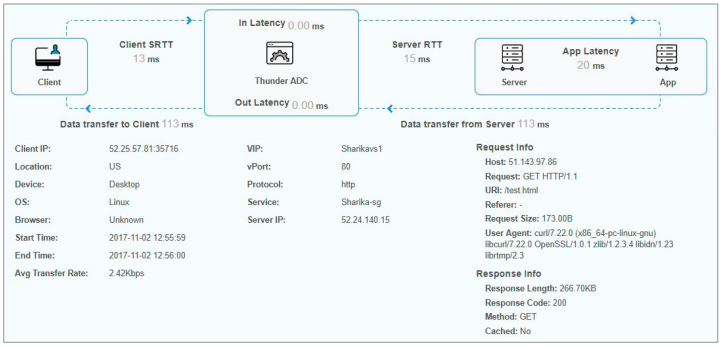
SECURITY (LIGHTNING ADC)

Threat Detected / Blocked	Summary of threats detected and blocked at various times.
Application Firewall	Time based distribution of attacks by their type.
Blacklisted / Bad Reputation	Information of requests blocked over time because of black-listing or bad reputation of clients.
DDoS Attack Mitigation	Requests/sessions blocked for mitigating volumetric application layer DDoS attack.



PER TRANSACTION LOGS

Response Time Distribution	Visual representation of time spent in various phases of request and response.
Client Info	IP address, device type, operating system and browser of the client.
Server Info	IP address, port and micro-service that served the request.
Request and Response Info	Method, protocol, URI of request and size of response data.
Security Info	Details of threat detected in request or response along with its OWASP classification.



SSLI ANALYTICS*

SSL Status & Reporting	• Inspection details • Bypassed categories • Key Exchange details • Access details
System Health Status & Reporting	• System status • Certificates in cache • CPS, sessions & traffic

*GI-FW ANALYTICS**

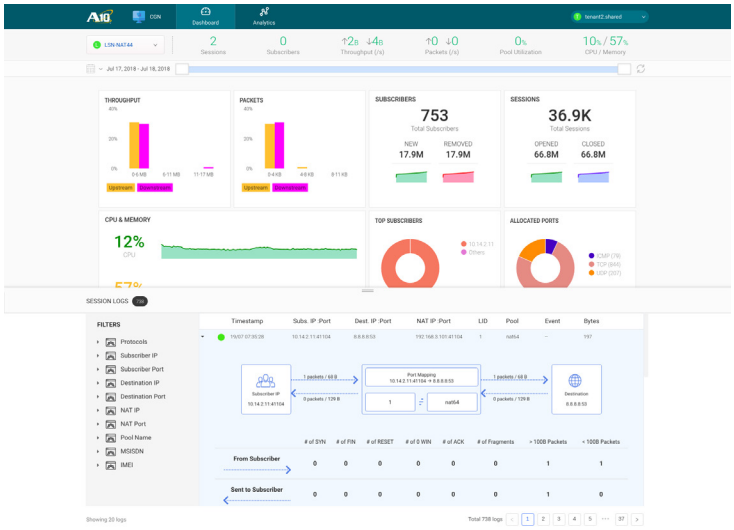
Subscriber Session Insights	• Session opening/closing rates – Behavioral indicators of potential DDoS attack • Top bandwidth/flow consuming subscribers - Indicators of potential network abuse • Top bandwidth/flow consuming subscribers
CGN Resource Tracking	• Mappings per protocol & technology - Behavioral indicators of potential botnet DDoS attack • NAT IP pool utilization - Indication of attacks on NAT IP pools
Traffic Distribution Alerts	• Subscriber user quota alerts
Firewall Analytics	• Firewall rule performance and rule distribution by protocol • Top firewall rules by state – allow, deny • Complete log with source/Destination IP, Port and firewall actions for better visibility and faster troubleshooting
Application Visibility	• Application distribution by category • Top destination IP by application distribution • Bytes consumed by application category and more...

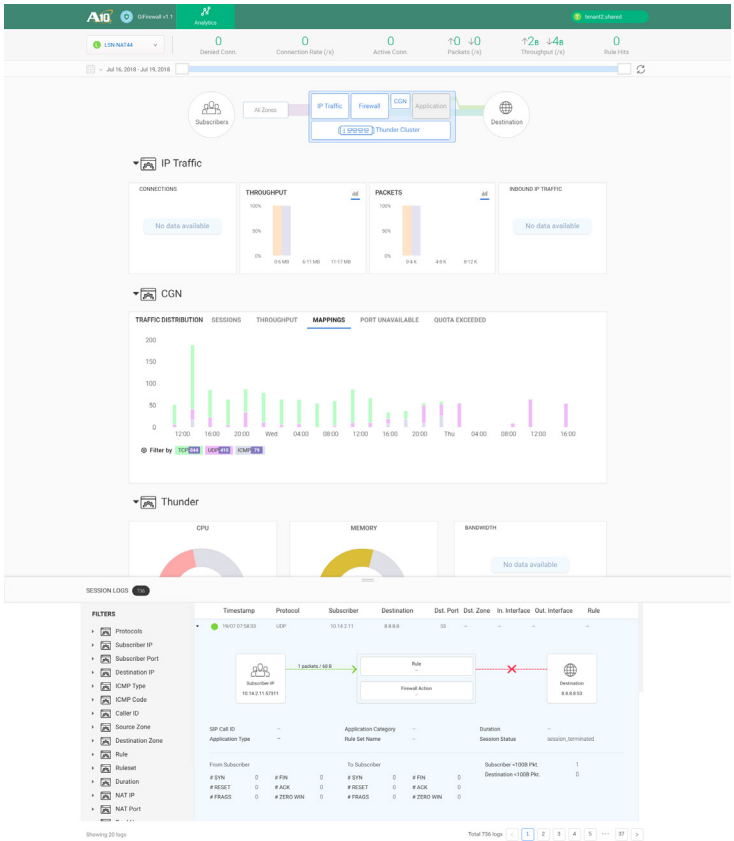
*CGN ANALYTICS**

Subscribers	• Total throughput consumed with user quota alerts • Opened/closed sessions per subscriber • Top subscribers by throughput consumed
CGN Services	• Port allocation by protocol. • Mapping errors • Top pool consumption stats • Full cone session distribution and more
Destination	• Overall packet rate • Analytics on fragmented/malformed traffic • Flow open attempts from Internet
Subscriber Session Insights	• Session opening/closing rates - Behavioral indicators of potential DDoS attack • Top bandwidth/flow consuming subscribers - Indicators of potential network abuse
CGN Resource Tracking	• Mappings per protocol & technology - Behavioral indicators of potential botnet DDoS attack • NAT IP pool utilization - Indication of attacks on NAT IP pools
Traffic Distribution Alerts	• Subscriber user quota alerts
Misbehaviors	• User Quota Alerts – Session exceeded, Connection rate exceeded, and more. • Session creation failure • Hair pinning, EIM/EIF failures
Consolidated Logs	• Granular log messages for faster troubleshooting • Subscriber info • Protocol • MSISDN • IMEI/IMSI • Radio Access Type and more...

*Available in Q3 2018

*CGN ANALYTICS**





*Available in Q3 2018

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-DS-15122-EN-10 APR 2019