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.

Agile Management & Analytics for Any Application Deployment

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 with Harmony Controller helps collect, analyze and report on application traffic flowing through A10 Thunder ADC. The centralized analytics over A10's SSL Insight, CGNAT, Gi/SGI firewall, and GTP firewall 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.

Platforms

aws

ORACLE Cloud

vmware

NUTANIX

openstack.

Talk With A10

Web

a10networks.com/harmony

Features and Benefits

The Harmony Controller simplifies application services operation and increases the agility of the operation teams. As a centralized management solution over A10's secure application services, the controller supports DevOps/ SecOps workflow by automating configuration and control using APIs. The controller can be single point of integration with orchestration systems used within organizations. It also provides comprehensive infrastructure & per-application insights, analytics for performance & security, anomaly detection and faster troubleshooting.

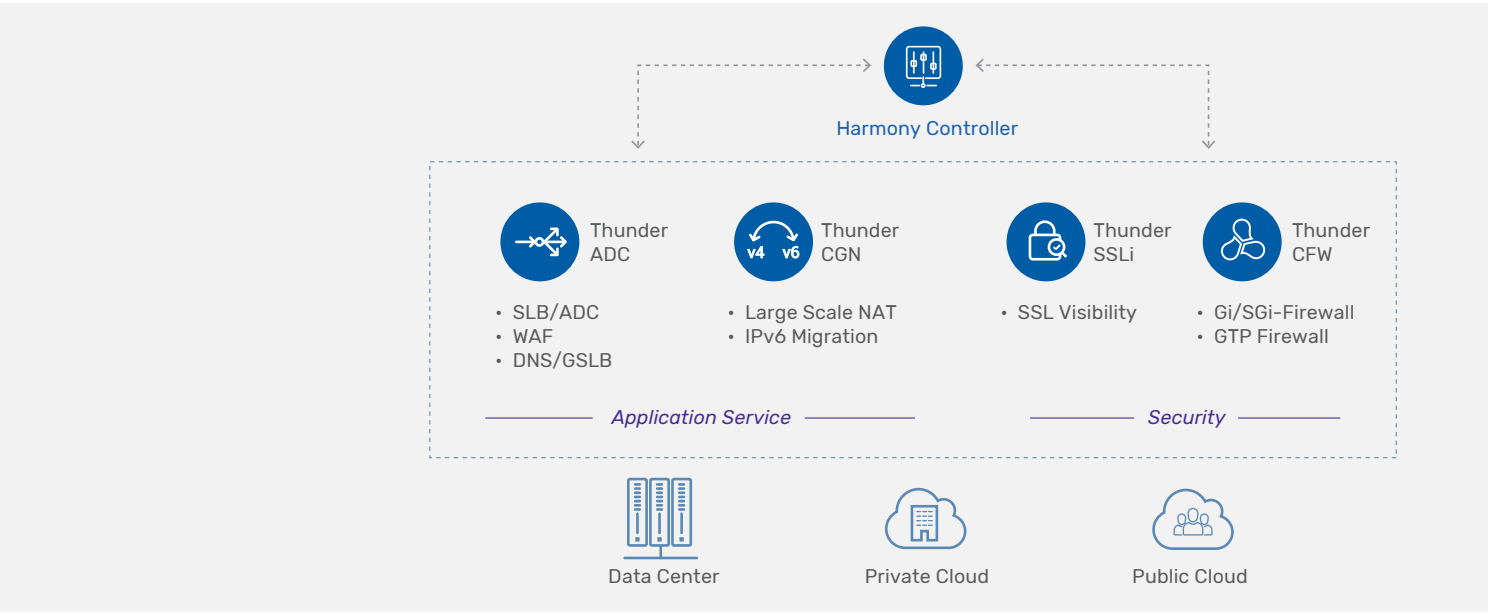

Figure 1. Harmony Controller is centralized management solution enabling application service analytics and automation across multiple data centers and cloud environments.

Centralized Management

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

Application Traffic and Security Analytics

Gain visibility and actionable insights into the application traffic. Harmony Apps help analyze collected data to detect anomalous trends, and simplify troubleshooting via access to contextualized data and logs. Operators can get alerts based on various metrics and customizable fields, 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 application policies.

Device Lifecycle Management

Centralized device lifecycle management for A10 hardware appliances or virtual instances. Easily manage large number of devices by 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.

Platform Agnostic Installation

The Harmony Controller's container-based, microservices architecture allows controller to be deployed in any environment in a Linux machine on bare-metal, virtualized servers and on public or private clouds.

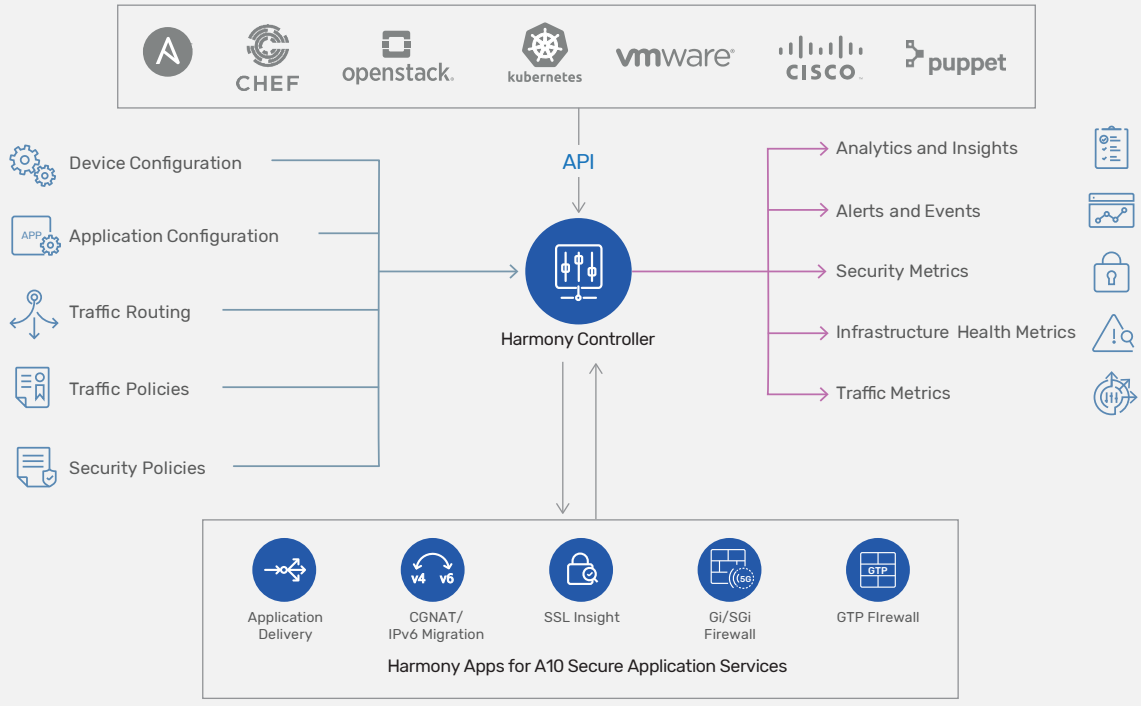

Figure 2. Harmony Controller simplifies and automates application management and operation in any and multi-cloud environment.

Harmony Controller Interfaces

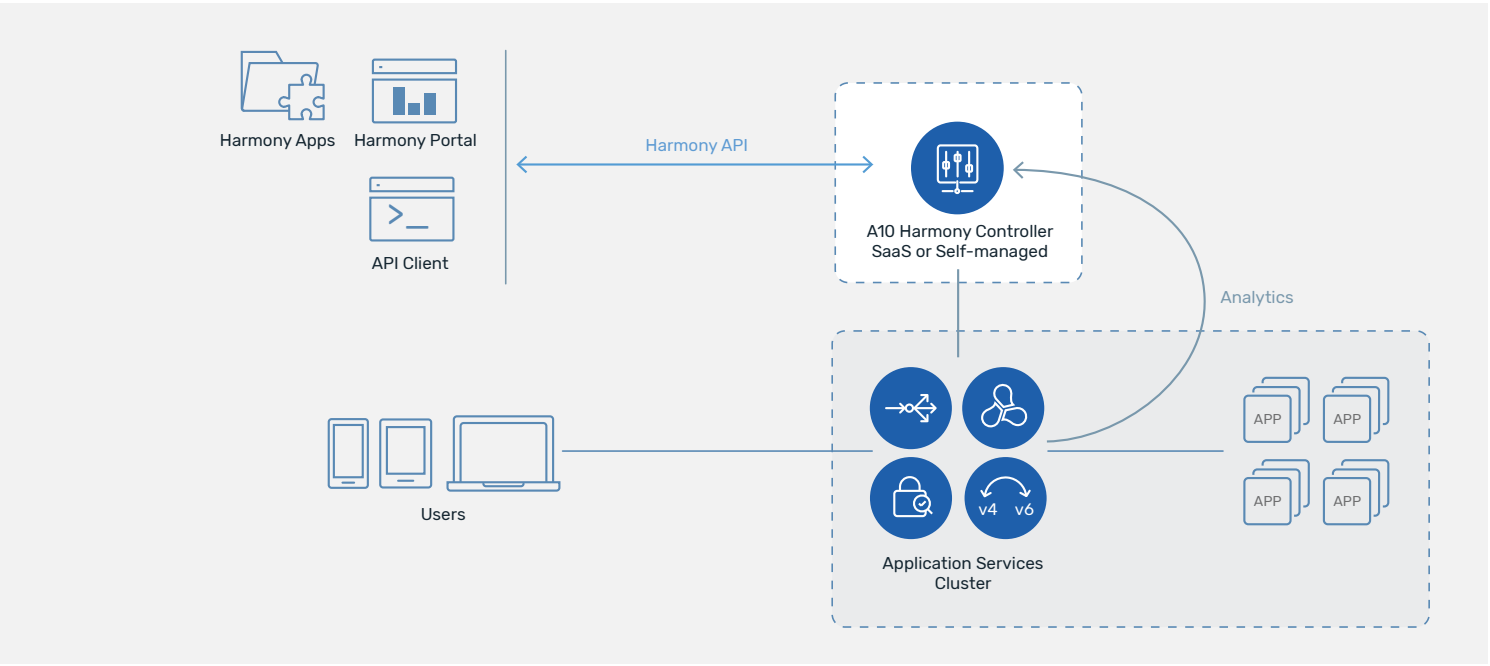

Figure 3. Harmony Controller manages various application services, client APIs and administrative capabilities. This deployment model helps organizations configure all policies in a central location, regardless of where application services are deployed.

Harmony Portal

The portal is an intuitive graphical user interface for managing secure application services infrastructure and associated policies on a per-app basis, with role-based access control (RBAC). Per-app based visibility and insights are available via Harmony Apps which operators can pick and enable on the Portal. 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

SaaS – Managed by A10

Available as a service, the cloud-based Harmony Controller 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 such as A10 Thunder devices via a secure, TLS-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 TLS communication.

Self-Managed – On-Premise and Cloud

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, hypervisor based VM, 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.

Harmony Controller Software System Requirements

Harmony Controller can be installed standalone or high-availability (HA) in Linux machines (CentOS or RHEL) on any bare metal, hypervisor or cloud instance. HA is supported with three nodes deployments (i.e. virtual machines or devices), providing resiliency in case of a node failure. Microservices as well as data-stores of the controller are distributed over these three nodes.

Actual resource requirement depends on the number of managed devices and analytics needed. For Harmony Controller installation, it's not required to prepare special or high-spec hardware, you can use any grade of server hardware. SSD (solid state drive) storage is preferred because of its high IOPS value. For more details of system requirements and pre-requisites for the controller installation, refer to the latest product documentation or contact A10 sales representative.

Licensing

The controller software subscription is priced based on the bandwidth units consumed by managed devices. These bandwidth units are called Managed Bandwidth Units or MBU. Each Thunder device has a fixed MBU value. 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. A10 Thunder device licenses are required to be purchased separately.

Supported Application Services

A10 Thunder ADC

A10 Thunder® ADCs are high-performance advanced load balancing solution that enables your applications to be highly available, accelerated, and secure.

A10 Thunder SSLi

SSL Insight® feature is the comprehensive SSL/TLS decryption solution that enables your security devices to efficiently analyze all enterprise traffic while ensuring compliance, privacy, and boosting ROI.

A10 Thunder CFW

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

A10 Thunder CGN

A10 Thunder® CGN provides high-performance, transparent network address, and protocol translation, enabling service providers and enterprises to extend IPv4 connectivity and transition to IPv6 standards.

Harmony Controller Features List

Harmony Portal

Device Inventory	Complete device inventory is available in multiple forms like individual device view, physical cluster view, logical cluster view etc.
CLI Command Utilities	Single or a batch of CLI commands can be pushed to multiple device partitions simultaneously.
Device Upgrade	Upgrade of Thunder devices can be done remotely using Harmony Portal.
Health Monitoring of Devices	Harmony Controller monitors health of connected devices and provides intuitive dashboard including the system utilization, device location, events and alerts information per tenant service.
Device Config Backup and Restore	Thunder is a state-full device. Its configuration can be backed up from Harmony Portal and restored back as needed.
Manage Devices in Multiple Clouds	Harmony Controller manages Thunder devices deployed across various cloud environment in different geographies.
Centralized Configuration Tool (Objects Explorer)	Object Explorer enables application service level configurations for ADC, GSLB, CGNAT, Gi/SGi FW, WAF, and other application and security features. It also allows to scan current configuration from the connected Thunder devices.
Auto Provisioning of Thunder in Cloud	Harmony Controller can interoperate with private/public cloud infrastructure environments to auto-launch and manage virtual Thunder devices. It includes AWS, Micrsoft Azure VMware ESXi, Kubernetes and more.

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 using with collaboration tools such as Slack and Microsoft Teams.
External Authentication	A provider can select the authentication provider for its users. Other than local user authentication, Any LDAP, Radius or TACACS based server can be used.
Configuration Backup	Harmony Controller configuration can be backed up by copying and storing externally.
Scheduled Reports	Various reports (in PDF format) can be scheduled for periodic consumption of management. In addition, any analytics page can also be printed to PDF.

Installation and Maintenance

Platform Agnostic Installation	The Harmony Controller software can be installed in any environment on physical or virtual Linux machines.
Self-healing Micro-services Based Architecture	The controller internally consists of multiple micro-services. The framework brings back the micro-service automatically if it stops working.
Configuration via APIs	Configuration of controller itself can be monitored and changed via the APIs exposed by the controller.
Disaster Recovery	Active and passive Controllers can be deployed in different geographies for quickly recovering in case primary location becomes unavailable because of any disaster.

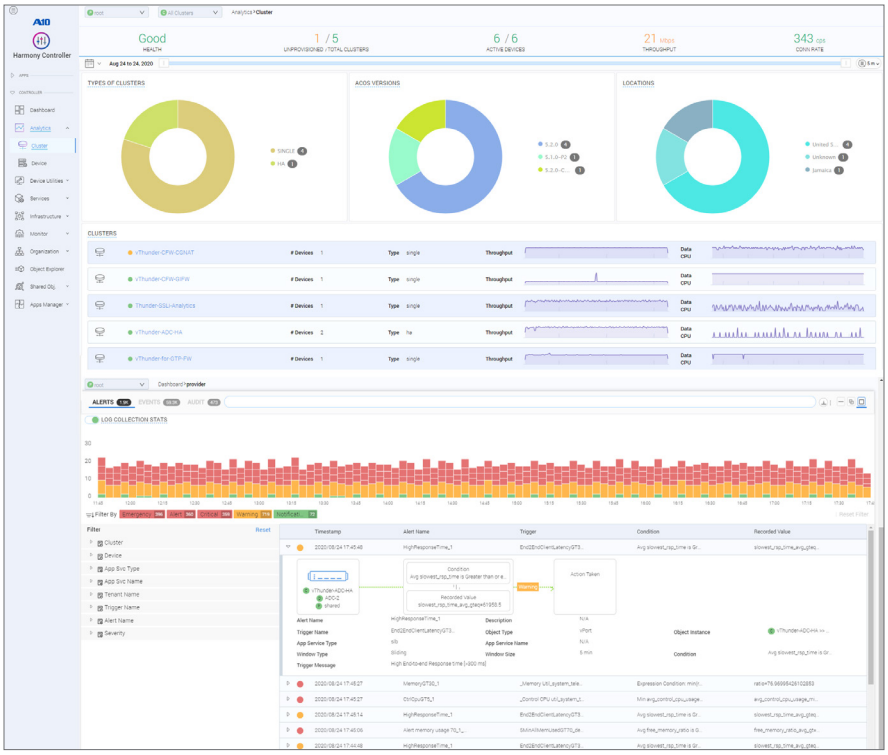

Figure 4. Harmony Portal provides comprehensive dashboard and analytics showing health and events for the secure application service infrastructure. The sample shows devices status and detailed alert insights

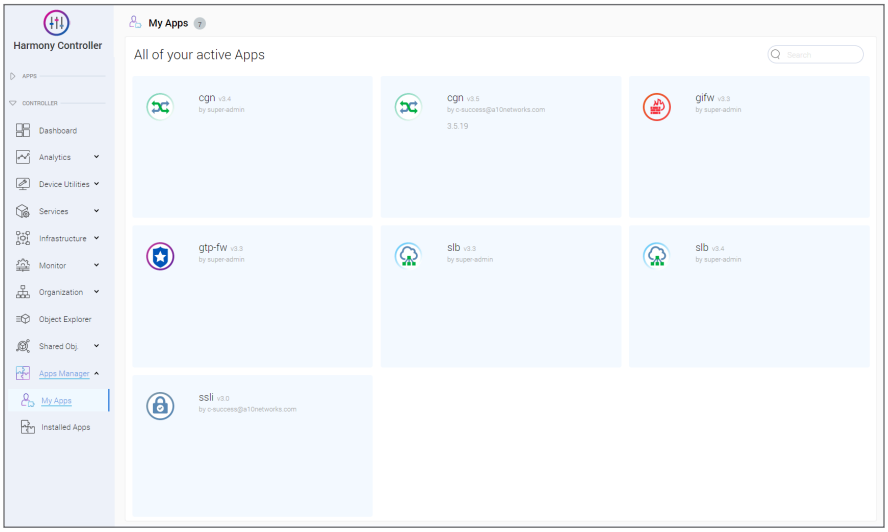

Figure 5. Harmony Apps collection. Harmony Apps provide full visibility and analytics on per-application basis, and are available for SLB/ADC, CGNAT, SSL Insight, Gi/SGi Firewall, GTP Firewall and else.

Harmony Apps Features List

ADC/SLB App

Analytics & Insights (Service Port Level)	Client	• User request insights – request methods, response code and time-series request statistics • Average end-to-end latency showing response time clients are experiencing for each segment (client – ADC – app server) • Clients insights - geographical distribution, client properties including operating system, device, browser type • Top clients by requests and throughput
	Internet	• Application traffic analytics by geographical locations for latency, number of requests (HTTP/HTTPS) and throughput
	WAF	• WAF policy violation insights including violation types distribution, HTTP threshold violations and protocol violations • Time-series WAF violation statistics by types • Time-series WAF request handling and events statistics • Cookie security insights • Top sources for received requests that triggered WAF policy violations
	ADC Service	• Time-series chart for distribution of connections and response counts across application servers • Time-series application traffic throughput (uplink/ downlink) • Time-series chart for average reverse and forward latency • Time-series chart for number of error traffic with response code 3xx, 4xx and 5xx • HTTP2 insights – time-series of HTTPs traffic including proxy connection stats, volume, streams closed, frame types sent to client and else • TLS/SSL insights – time-series of TLS connections for both client side and server side • HTTP acceleration insights for RAM caching utilization and compression usage
	Applications & App Servers	• Time-series applications performance including response time and end-to-end latency • Application service insights including top visited URLs/ Domains, slowest URLs, etc. • Time-series backend server insights including server health, response time, new connections and current connections
	ADC Cluster	• ADC devices/ cluster system utilization (CPU, Memory) and bandwidth (peak and average) • Deployment locations in world map • Time-series cluster traffic chart based on throughput and active sessions for both directions (ingress and egress) • Time-series service partition level latency insight (forward, reverse, time to first byte (TTFB), time to last byte (TTLB))
	Latency Drilldown	• Latency analysis overview • Time-series average end-to-end latency for a full request-response cycle
ADC Service Dashboard (Global)		• ADC service level KPI (key performance indicator) bar including global real-time ADC traffic statistics including throughput, current connections, connection rate and error traffic rate • Service inventory information including service ports statistics and status, global deployed locations, events logs and alerts • Global (tenant level) ADC traffic insight dashboard showing traffic patterns, characteristic, average end-to-end latency and top 10 application services
Centralized ADC Configuration Tool		• Shared Object enabling centralized policy and template management for ADC service templates, WAF rules, security policies, aFleX scripts, health monitor templates and else, which can be shared and used to multiple devices • Service Objects providing intuitive ADC virtual server (VIP) configuration tool by associating service templates, security policies and other objects created in shared objects • ADC configuration revision control with diff capability to compare with previous configuration versions
Session Log Drilldown		• Detailed ADC transaction logs providing client information (IP, location, device, etc.), ADC service information (e.g., VIP, service port, protocol) and transaction details including request and response details) • Response time distribution representing session latency (RTT) in various phases of request and response transaction • Detailed transaction logs for WAF event providing violation details (types, category, WAF policy and action) • Easy to use searching and filtering capability to support faster troubleshooting of ADC services • Pinpoint possible issues/ bottlenecks in both network and application layer

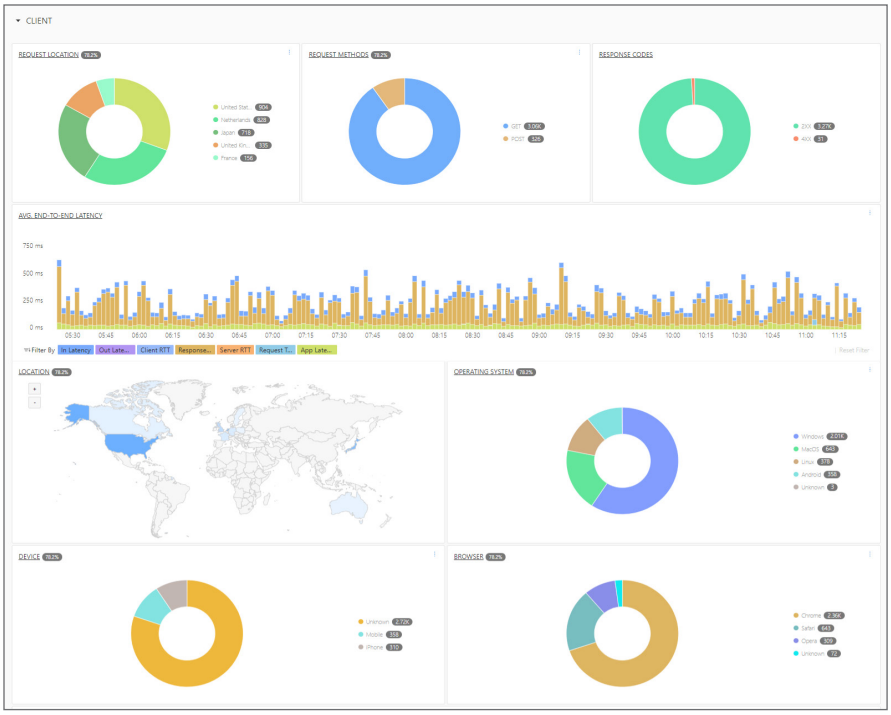

Figure 6. ADC Harmony App provides application analytics and insights from multiple aspects, including client (sample), Internet, ADC services, Applications, App servers and more.

Figure 7. Latency drilldown analytics provides time-series average end-to-end latency for a full request-response cycle. This greatly helps troubleshoot application performance issue related to delayed response time.

SSL Insight App

Analytics & Insights	Traffic Insight	• TLS inspection status for total counts and time-series chart by connections and volume • TLS cipher analytics for key exchange methods, TLS versions, based on client and server connections • Time-series traffic distribution by protocol and segment based on connections and volume • Time-series TLS connections per second and volume • Top source IPs for TLS deceryption by connections and volume
	Application Insight	• Top applications based on connections and volume • Top SaaS applications based on connections and volume • Top risky applications based on connections and volume • Application traffic distribution • Top gaining applications and categories • List of all the application protocols observed
	URL Insight	• Top URL categories based on connections and volume • URL category insight by Productivity, Sensitive, IT Resource, and Privacy groups • Suspicious URL categories by connection• Time-series connection chart for the suspicious category group • Time-series connection chart for top 5 URL categories
	Source & Destination Insight	• Source & destination IP analysis using Sankey diagram based on connections and volume • Pareto analysis for source and destination IP based on connections and volume • Top destination countries based on connections and volume
	Threat Investigator	• Threat intelligence research and investigation tool that allows to quickly look up and investigate a potential risk of the individual internet objects including IPs, URLs, files, and applications.
	Watch List	• Monitor TLS traffic based on URL and application categories • Create custom lists of applications to monitor user traffic in time-series chart • Create custom lists of URL categories to monitor user traffic in time-series chart
Device Management & Configuration Tools		• SSL Insight service level KPI (key performance indicator) bar including device group health, real time SSLi traffic statistics, service availability, error rate and else • Deployment Wizard provides intuitive guided configuration for various deployment options (single or dual appliance, with or without high-availability, L2 or L3) with recommended security policies • Site group and site topology supports many prevailing deployment topologies. Adding new devices/ sites in the same site group is as easy as cloning an existing site • Single device level configuration & management is supported for general system settings, interface and networking, add-on security licenses • Policy manager to enable centralized SSL insight service and policy configuration for all devices in a device group • Shared Object are an abstraction of the various SSLi configuration including ACLs, policy templates, SSL profiles, URL filtering, ICAP, AAM, G-suites and Office 365 and so on
Session Log Drilldown		• Log view provides expanded view and search functions of access log, SSLi connection log, error log, and system log for troubleshooting • Searching session logs with uncategorized URLs

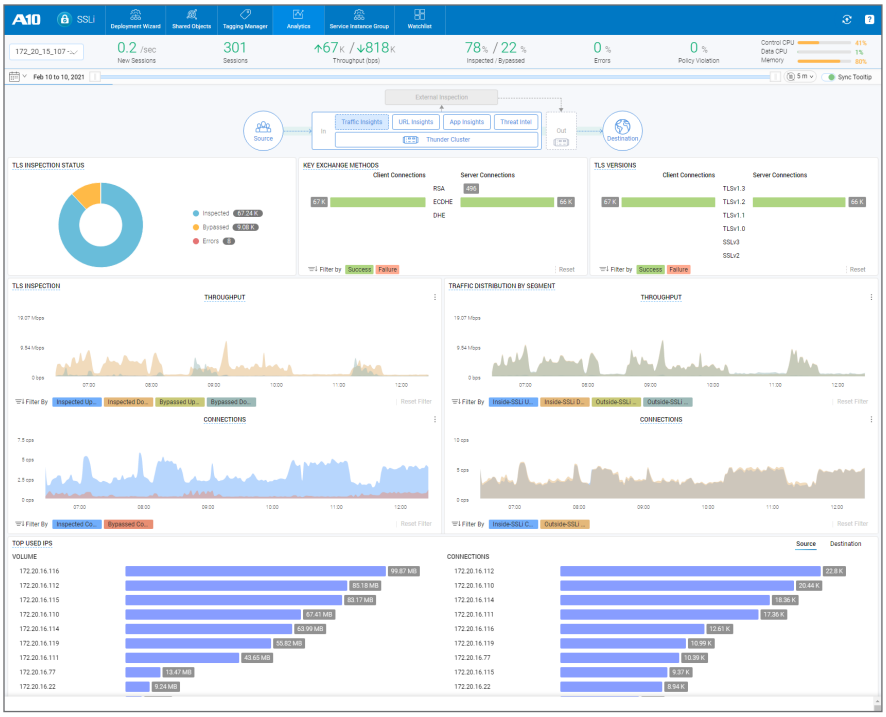

Figure 8. SSL Insight App provides comprehensive analytics for application traffic over TLS, centralized policy control and intuitive wizard-based configuration tools.

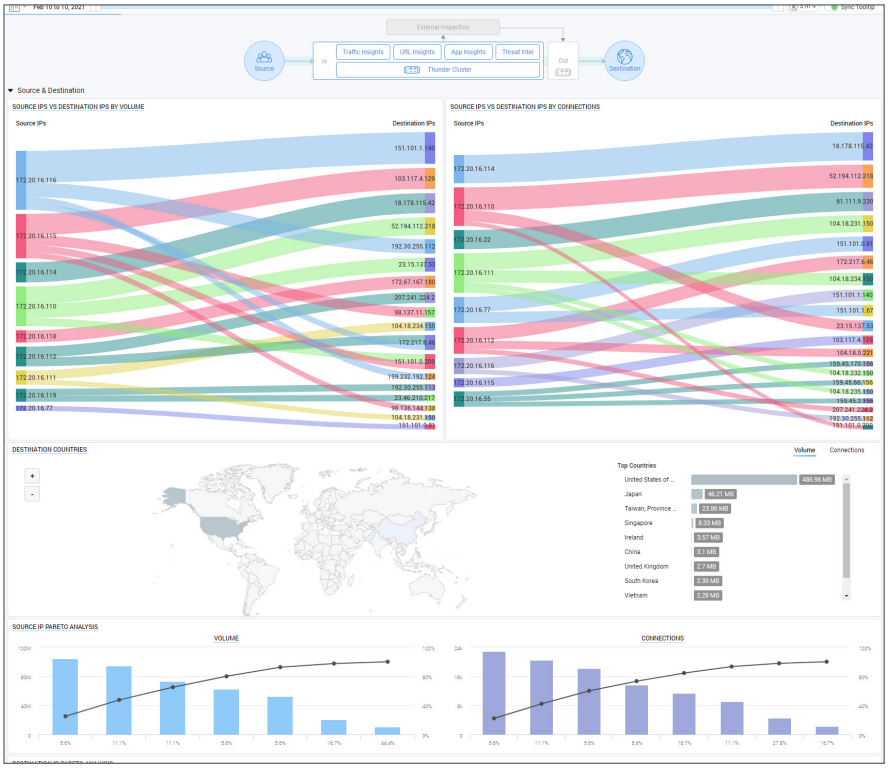

Figure 9. SSL Insight analytics visualizes the traffic insights from the aspect of IPs, TLS traffic pattern, URL, application categories, devices and more.

CGNAT App

Analytics & Insights	Traffic Analytics	• CGNAT service level KPI (key performance indicator) bar including real-time service traffic statistics and device health • Top subscribers (IPv4/IPv6) and time-series concurrent session counts and session rate • Subscriber side time-series total traffic (throughput and packet rate) measured on uplink and downlink • CGNAT service analytics for port mapping (protocol), time-series sessions stats (user quota, full-cone sessions, EIM/EIF, hairpinning), NAT pools, misbehaviors /error traffic statistics • CGN device/ cluster statistics, and internet (uplink) side of traffic statistics and insights
	Subscriber Port Usage (for Fixed-NAT)	• Subscribers port usage correlation (TCP/UDP) • Subscribers traffic pattern insights in port range • Active subscribers
	Application Visibility	• Top applications chart (per rule-set) • Application traffic distribution based on connections and volume • Applications insights by categories / watchlist
	IP Anomaly	• Normal packets vs. anomaly events insight with filter by • Filter by downlink, uplink, layer 3 and layer 4 • Distribution of anomaly types and layers
Dashboard		• Overall CGNAT service tenant view, including alerts and events, geographical deployment locations, CGNAT service KPI scorecards • CGN service type view provides a KPI snapshot bar and drilldown statistic for subscribers, current session counts and rate, throughput (bps), packet rate (pps), NAT pool use (TCP/ UDP), device status (usage of data and control CPU, memory) etc.
Troubleshooting		• Drop analysis helps to visualize where the packet drops happen in the processing chain so as to quickly identify issues and the root causes • Time series charts are overlaid by alerts and events in time axis so user can easily correlate the performance or errors and quickly identify issues • Anomaly Detection feature, once configured, can detect spikes of any time series data and generate alerts
Session Log Drilldown		• Detailed CGNAT transaction logs providing subscriber information (IP, MSISDN, IMEI, IMSI) , NAT session, port mapping, protocols, CGN policy and else • Detailed error transaction logs providing subscriber information, NAT pool, protocol and reason/ error type • Easy to use searching and filtering option for both session and error logs

Figure 10. CGNAT App provides comprehensive visibility and insights of the subscriber traffic on a per-CGNAT service basis.

GTP Firewall App

Analytics & Insights	Traffic Insight	• GTP FW service level KPI (key performance indicator) bar including real-time service traffic statistics and device health • Roaming geographical view based on GTP session counts for both roam-in and roam-out • Time-series GTP traffic insight for GTPv0-C, GTPv1-C, GTPv2-C and GTP-U (uplink/ downlink) • Time-series GTP traffic distribution and comparison chart at - Signaling Gateway (SGW) and Signaling Gateway Secure Network (SGSN) - Packet Data Network Gateway (PGW) and Gateway GPRS Support Node (GGSN) - Access Point Name (APN) • Time-series CFW cluster traffic statistics for GTP sessions
	Policy Violations	• Time-series of GTP firewall policy actions statistics and policy violation insight based on violation categories • Time-series GTP firewall policy violation analytics using violation type distribution and comparison at - Signaling Gateway (SGW) and Signaling Gateway Secure Network (SGSN) - Packet Data Network Gateway (PGW) and Gateway GPRS Support Node (GGSN) - Access Point Name (APN) • Firewall rule performance analysis and stale rules indicator
	Roam In	• GTP roam-in session stats by their origin countries in the world map view • List of roaming origin countries based on log counts, MMC and MNC
	Roam Out	• GTP roam-out session stats by their destination countries in the world map view • List of roaming destination countries based on log counts, MMC and MNC
Session Log Drilldown		• Detailed GTP firewall session logs providing source/origin, destination, message type, session details (protocol, user location info (LUI), QoS etc.), log reason and firewall rule /action information • Easy to use searching and filtering option using GTP protocol types, IP, TEID and else

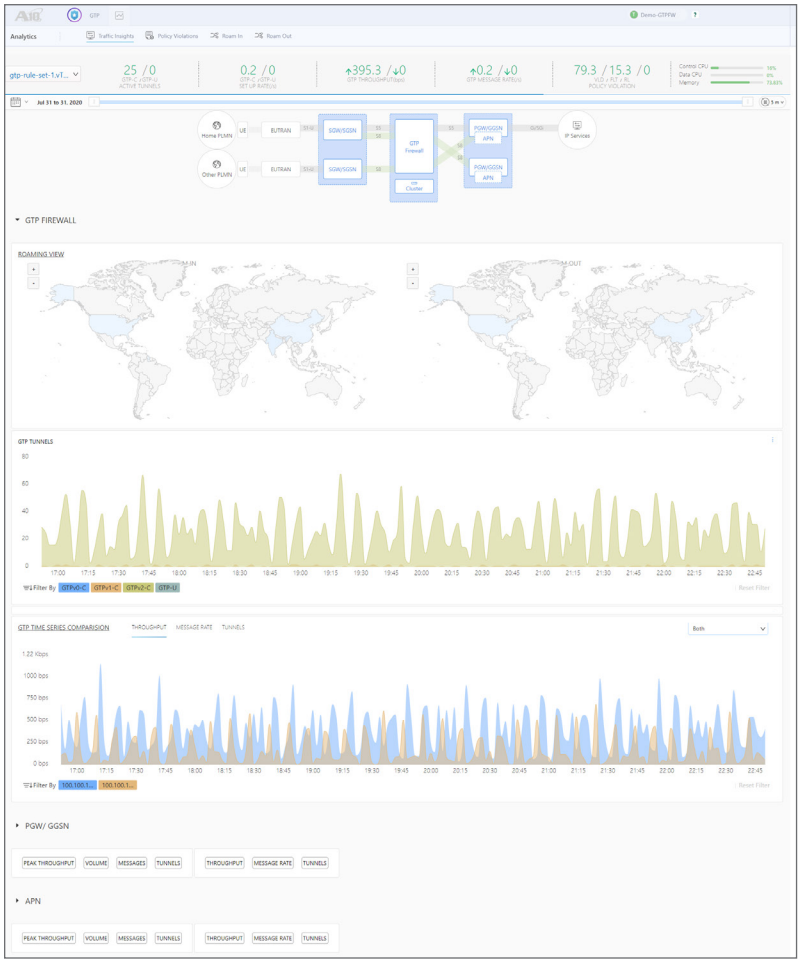

Figure 11. GTP Firewall App provides holistic view and analytics for roaming traffic using time-series GTP traffic insights, GTP FW service level KPI, roam (in/out) session statistics, detailed session log and more.

Gi/SGi Firewall App

Analytics & Insights	IP Traffic	• CGN and GiFW service level KPI (key performance indicator) bar including real-time traffic stats, firewall rule stats, and device health • Total session counts and rate • Total time-series traffic statistics (throughput and packet rate) • Traffic analytics with top-K IPs based on throughput, session, protocols for source and destination (IPv4/IPv6)
	Firewall	• Time-series traffic insight based on firewall rule action • Traffic pattern statistics based on rules matched and dropped traffic • Traffic distribution of firewall rules for each action • Firewall rule performance scorecard and stale rule indicator • Top subscribers based on volume, packets and sessions (IPv4/IPv6)
	CGN	• Protocol based port mapping insights • Time-series port mapping statistics • Time-series port error and quota exceeded statistics • Time-series NAT pool utilization (port-based, NAT IP-based, subscriber per NAT IP)
	Cluster	• CFW devices/cluster system utilization (CPU, Memory) and bandwidth • Deployment locations in world map • luster traffic insight based on throughput and active sessions
Session Log Drilldown	• Detailed CGNAT transaction logs providing subscriber information, NAT session, port mapping, CGN policy and else • Detailed firewall / transparent session logs providing subscriber information, firewall rule and action, zone, in/out interface and session status • Easy to use searching and filtering option for both NAT and firewall session logs	

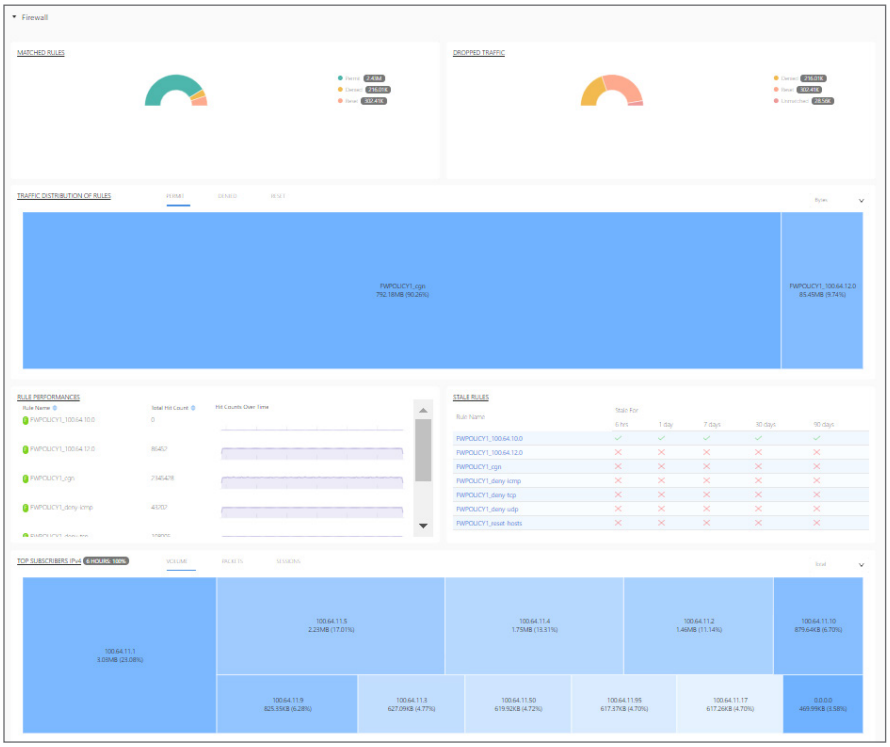

Figure 12. Gi/SGi Firewall App provides detailed analytics of the user traffic with time-series traffic insights, firewall rule permanence, CGN and GiFW service level KPI and many more.

Learn More

About A10 Networks

Contact Us

a10networks.com/contact

Part Number: A10-DS-15122-EN-12 FEB 2021