DATA SHEET

A10 Control

Unified Management, Control and Analytics Platform for Agile Operations and Automation

A centralized management and analytics platform providing full control of your A10 solutions, regardless of whether the solution is deployed on-premises, in the cloud, or in a hybrid environment.

Agile Management and Intelligent Analytics

The increasing complexity of modern network and security infrastructure, coupled with the rapid adoption of AI and cloud technologies, presents significant challenges for organizations to manage and support their mission-critical services and businesses.

It's a complex and a time-consuming task to understand network infrastructure resources and track service status when its deployment is spread across various geographical locations and multiple clouds. Precise capacity planning and prompt response to scaling demand are critical for AI-powered apps and application services infrastructure as they require higher traffic and transaction volume and are very sensitive to latency. Therefore, administrators should leverage agile management and intelligent analytics to establish efficient operation and management workflow.

A10 Control is the next generation of the management and analytics platform for A10 solutions, consolidating existing A10 Harmony Controller and aGalaxy capabilities. A10 Control provides centralized management for A10 security and infrastructure solutions including application delivery, DNS, CGNAT, SSL Insight, Gi-firewall and DDoS protection deployed in any network or cloud environment. A centralized platform helps collect, analyze and report on application and service traffic flowing through A10 appliances and visualize the service and security posture with intelligent analytics.

Platforms

Software/VM

Related Products & Services

ADC

A10 Defend DDoS Protection

CFW

CGN

SSLi

Learn More

A10Networks.com/a10-control

Benefits

Gain

Real-time Intelligent Analytics and Observability

Organizations must guarantee their services are up and running constantly. Thus, understanding the services' condition and gaining observability are critical tasks for their operation teams. A10 Control collects metrics data and transaction logs of the service traffic flowing through A10 devices running A10's Advanced Core Operating System (ACOS) and provides deep visibility into what's happing in the service and network infrastructure. Intelligent analytics and customizable alerts help identify potential issues before they impact end-users and enable proactive troubleshooting via access to contextualized traffic data and logs.

Simplify

Management for Services and Security

One management platform for any A10 solutions; One of A10's unique technical advantages is that all A10 solutions are running on a common OS (ACOS) regardless of platform or form factor. Now, A10 Control is the only management platform administrator needs as consolidating capabilities of A10 Harmony Controller and aGalaxy.

With A10 Control, streamline your IT operations and improve uptime of your services using rich intelligent analytics and embedded automation workflow tools.

Increase

Operational Efficiency

Organizations can improve their operation team's agility and efficiency by streamlining the workflow and automating processes. Device lifecycle management including backups, health checks, software upgrade, inventory and license management can be troublesome and time-consuming tasks. A10 Control's intelligent automation and tools enable efficient operation for managing a large number of appliances and services deployed over various underlying infrastructures — from data centers to any clouds.

Comprehensive APIs enable easy integration with popular DevOps, infrastructure-as-code and observability tool chains, and major public and private clouds infrastructure.

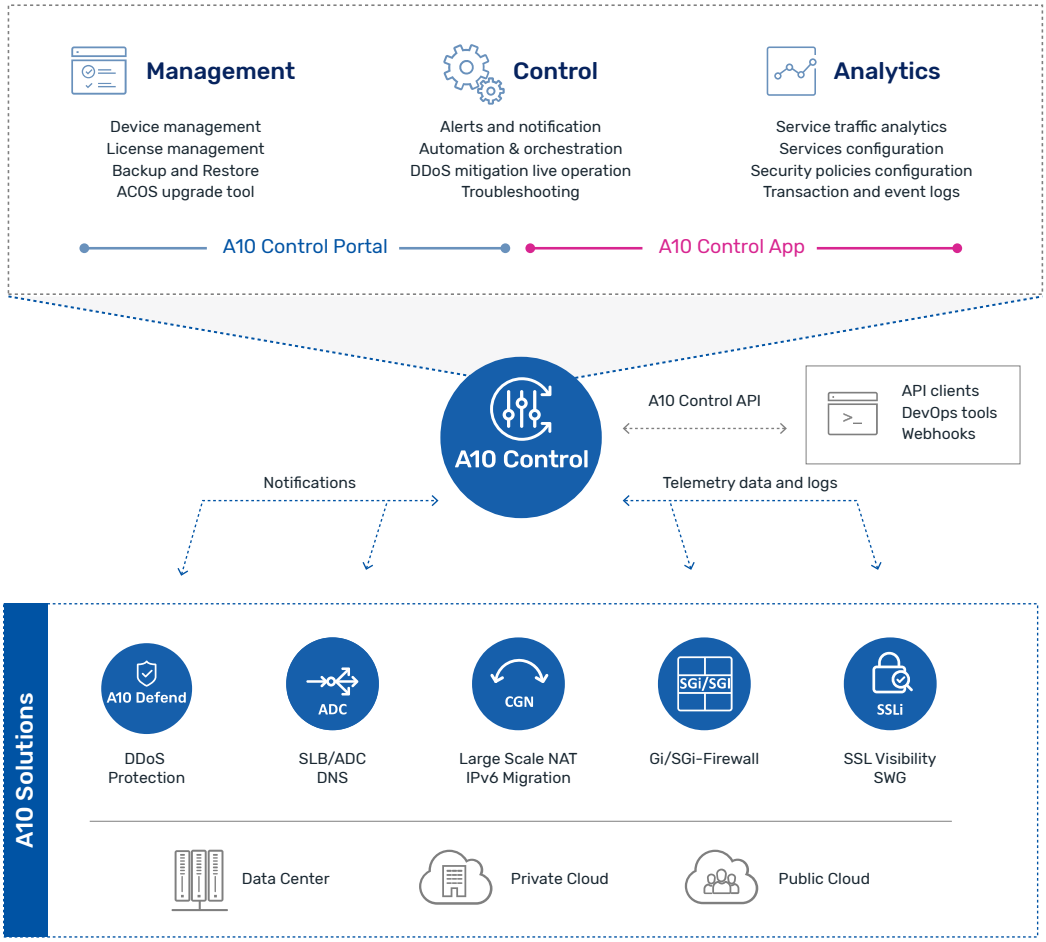

Figure 1. A10 Control is a centralized management and operations platform for A10 infrastructure services and security solutions.

Features

Centralized Management

Device Lifecyle Management

Centralized device lifecycle management for A10 hardware or virtual appliances including public, private cloud, and bare metal. Intuitive inventory and license management for multiple A10 Thunder and A10 Defend DDoS appliances. Automate routine tasks such as backup, inventory reports and schedule automated software upgrades.

Device Analytics

Detailed device-level analytics are available for A10 devices deployed across various network and cloud environments in different geographic locations. A device health monitor and dashboard provide system resource utilization, device location, traffic and connection metrics, transaction logs and event information.

Alert and Reporting

Metrics and logs collected from A10 devices are correlated and evaluated against user-defined rules for raising alerts against abnormal events. These alerts are delivered as email notifications and/or via webhook for automated action using collaboration tools such as Slack and Microsoft Teams.

Service Operations

Service and Policy Management

Make configuration changes and enforce security policy updates using shared resources such as class-list or IP list for A10 devices deployed across different geographical locations from a central console.

Multi-tenancy

With a flexible multi-tenancy architecture and role-based access control, each application team and service owner can have their own tenant workspace called organization-unit to manage their services and operations. Tenant allocation is as flexible as having multiple A10 device clusters in a tenant or as granular as assigning a tenant for each L3V/ADP partition of an A10 device.

API-driven Automation and Integration

Comprehensive A10 Control APIs allow easy integration using DevOps tool chains like Ansible, Chef, Jenkins to automate A10 device configuration management via A10 Control, and to streamline monitoring and operation workflow for the A10 solutions being managed.

Certificate Management and Auto-renewal

Certificate management utility allows administrators to effectively manage certificates, check their status (active, expiring, revoked), and even automate renewal process with certain certificate providers.

Architecture and System

Reliable Controller Platform

A10 Control is built upon a solid RHEL foundation with a microservices architecture using Kubernetes, which maximizes the availability of the controller and ensures full regulatory compliance, meeting the latest industry standard. The controller collects and processes various kinds of telemetry data from A10 devices in a secure manner, and never handles service traffic running through data plane of A10 devices. The architecture ensures that service traffic disruption never happens even if the connection between the controller and A10 devices is down.

Improved Security and Maintainability

A10 has years of expertise in using a microservices architecture in A10 product lines including Harmony Controller. A10 Control has been designed to use with the latest and greatest RHEL software and a next-generation architecture. This has enhanced security and maintainability of the system especially for security and CVE patches.

Re-architected for Stability and Performance

A10 Control has upgraded versions of all components, frameworks and technologies used in building of the product to boost stability and performance. A10 Control uses a different database system than Harmony Controller for simplified and low-latency data operations and a new and standards-based technology for user authentication management.

High Availability

The controller can be installed as a self-managed software solution in single node or multi-node high availability (HA) deployment within one of your sites. In HA, microservices as well as the data-store of the controller are distributed across nodes.

A10 Control also supports Disaster Recovery designed for a high availability architecture (active-passive) across geographically distributed sites, with ability to pre-provision a standby system and execute proactive health checks to ensure business continuity.

For details of system requirements and prerequisites for the A10 Control installation, refer to the latest product documentation or contact A10 sales representative.

Flexible Deployment Options

A10 Control offers flexible deployment choices to meet the needs of organizations of every size.

- **A10 Control Standard**: Designed for large-scale enterprises and service providers requiring high availability & scalability with support for up to 200 managed devices.
- **A10 Control Lite**: Ideal for small-scale deployments, offering essential management capabilities with reduced infrastructure and resource requirements.

A10 Control Apps

Solution-based comprehensive analytics, configuration and service operation tools are all built into A10 Control as an app.

Application Deliver Controller (ADC) App

Provides centralized configuration tool and visibility for single or multi-site ADC and DNS deployment. Rich analytics and contextualized logs help gain great insights into app and traffic, and simplify troubleshooting workflow when needed.

Carrier Grade NAT (CGN) App

Provides CGNAT technologies configuration tool, management and deep insight into subscribers traffic and NAT pool utilization. Rich service analytics including user session logs increase operational efficiency and help future planning.

Gi/SGi Firewall (Gi-FW) App

Provides detailed insights into user traffic going through the CFW-CGN device, including firewall rule-based analytics, CGNAT analytics and app category based classification.

A10 Defend Orchestrator (ADO) App

Previously known as aGalaxy is now available as the ADO app. Provides centralized protection configuration and real-time monitor for DDoS Detector and Mitigator. In case of DDoS incidents, orchestrates actions help streamline workflow with a live mitigation console.

SSL Insight (SSLi) App

Provides wizard-based configuration, guided troubleshooting tool and comprehensive observability into TLS/SSL encrypted traffic for SSL insight or secure web gateway deployment.

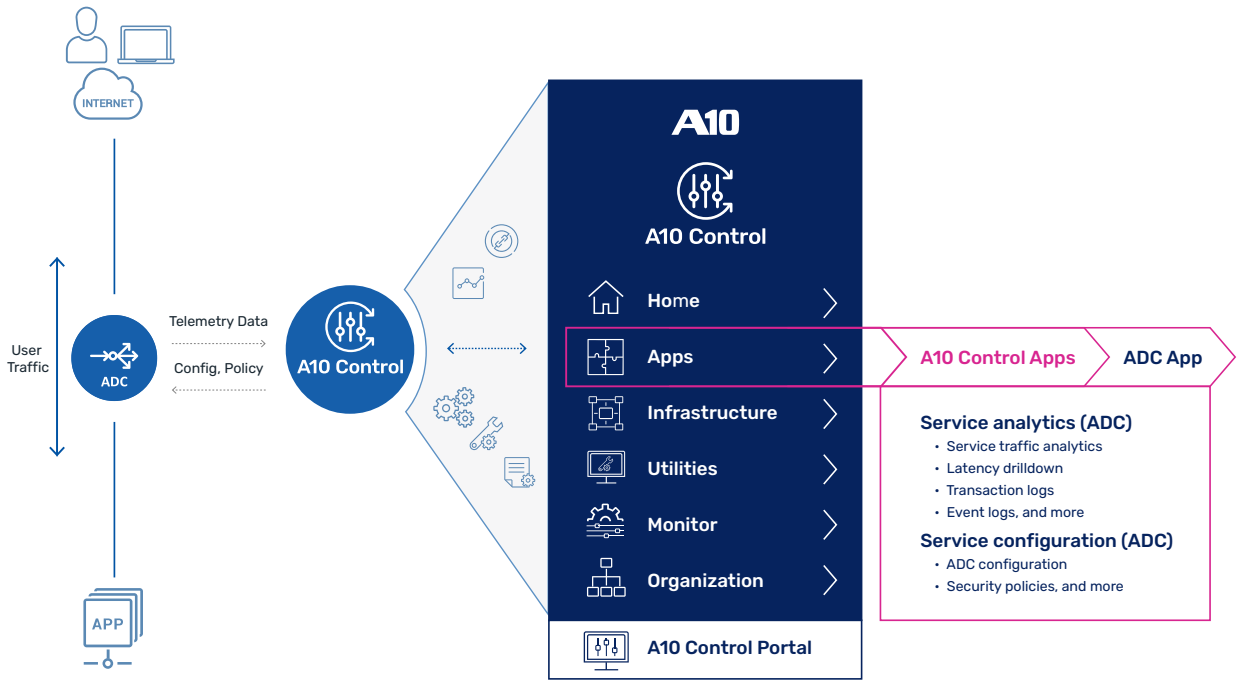

Figure 2. A10 Control collects telemetry from A10 device via control plane and provides analytics and control using a service specific A10 Control App.

Use Cases

Supported A10 Solutions

Application Delivery

High-performance advanced load balancing solution that enables applications to be highly available, accelerated and secure. Deploy with A10 Thunder ADCs or Thunder CFW-ADCs in any form factor including hardware, hypervisor-based software, bare metal, container or in hybrid and multi-cloud environments.

CGNAT and Gi/SGi-Firewall

Deply A10 Thunder CGNs for highly scalable and efficient NAT solution that allows service providers and enterprises to extend IPv4 connectivity while enabling smooth transition to IPv6 infrastructure. With A10 Thunder CFW-CGN, it enables consolidation of network function such as CGNAT, Gi/SGI firewall and app visibility, supporting efficient Gi-LAN and mobile core security.

DNS

Scalable and secure DNS load balancing and cache solution that makes DNS infrastructure more resilient and efficient. Deploy with A10 Thunder ADCs or Thunder CFW-ADCs in any form factor and environment.

DDoS Protection

Holistic DDoS defense solution that is scalable, economical, precise, and intelligent to help organizations ensure extended service uptime. Deploy with A10 Defend DDoS Detector and Mitigator.

SSL Insight

Comprehensive TLS/SSL decryption solution enabling security devices to analyze encrypted enterprise traffic, that can further augment security posture with integrated secure web gateway features. Deploy with A10 Thunder CFW-ADC in any form factor.

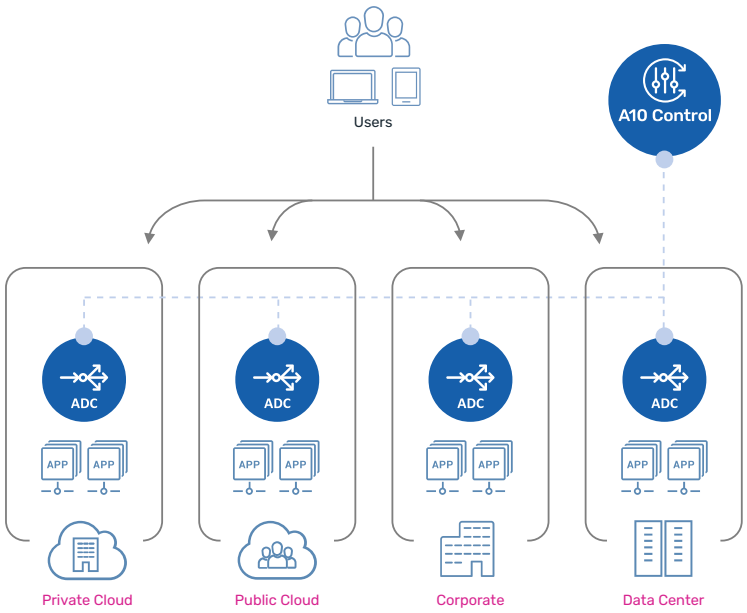

Figure 3: Multi-cloud ADC use case.

Multi-cloud application delivery deployment

A10 Control can centralize the management and control for application delivery services deployed in hybrid or multi-cloud environment, providing

- ADC analytics
- ADC and security policy enforcement
- ADC device & configuration management, and more.

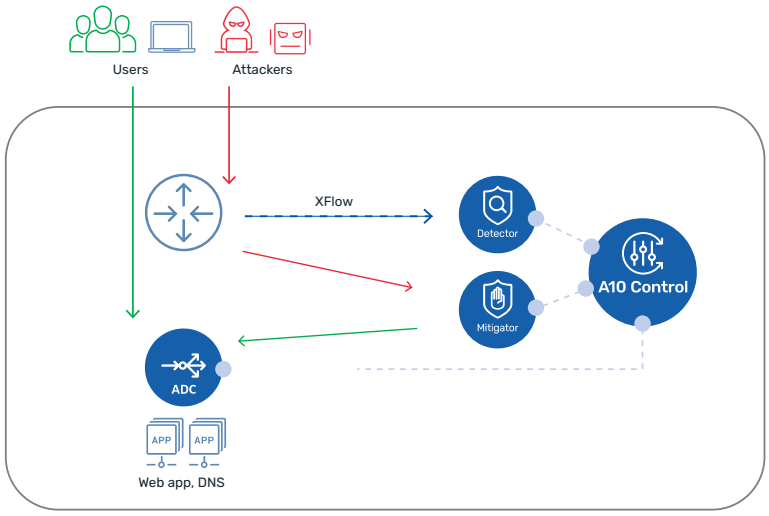

Figure 4: DDoS protection use case.

DDoS protection for web apps and DNS

A10 Defend DDoS Orchestrator (ADO) running on A10 Control, working together with Mitigator and Detector, enables intelligent automated protection against modern DDoS attack targeting application services and/or network infrastructure.

ADO app provides:

- DDoS defense orchestration and automation
- DDoS mitigation console
- DDoS defense policy configuration
- Incident reports, and more

If A10 ADC is used for application services, it can also be managed and control by the same A10 Control.

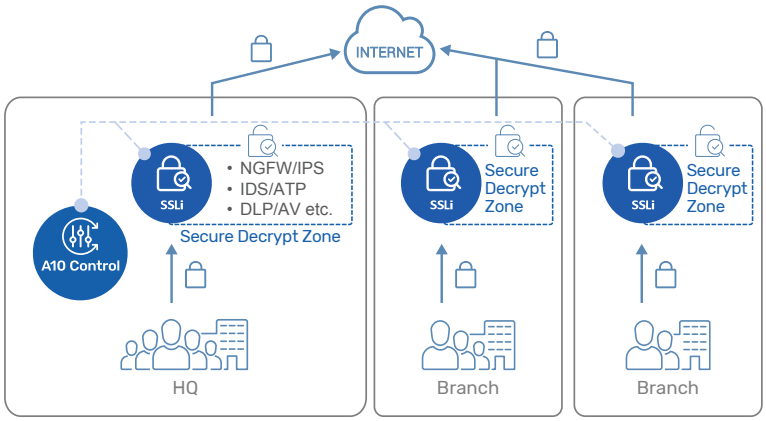

Figure 5: SSL Insight use case.

SSLi / Secure Web Gateway protects the enterprise perimeter

A10 Control centrally manages SSL Insight/ SWG deployments across different locations and branches for organization's perimeter protection.

SSLi app provides:

- SSLi analytics
- Centralized security and policy enforcement
- Troubleshooting tools
- Deployment wizard

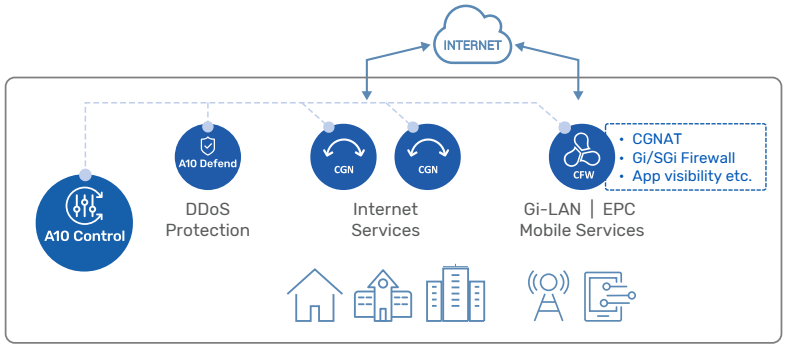

Figure 6: Mobile and service provider solution use case.

Network and security solutions for Mobile/SP network

CGNAT and GiFW services can be centrally managed by A10 Control, providing:

- Centralized CGNAT configuration and security policy enforcement
- Consolidated device management
- Detailed CGNAT and firewall analytics

In addition, DDoS protection solution can be managed with the same A10 Control.

Detailed Features List

A10 Control Portal

Device Management	
Device management dashboard	Complete device inventory provides general system and network information in individual device and cluster view (single node, VRRP-a pair etc.), and detailed analytics for system resource usage and traffic statistics.
Backup and restore	A10 device's configuration can be backed up periodically and stored in A10 Control. The backup can be used to restore the device as needed.
ACOS image upgrade	Image upgrade utility with pre- and post-upgrade checks, provides an intuitive and reliable ACOS image upgrade process for registered A10 devices with both manual and scheduled methods. All the upgrade operation logs and records are available in the history view.
Monitoring and Alerts	
Service-level health monitor and alerts	Service traffic and conditions can be monitored with custom trigger rules using a broad range of service-level metrics and thresholds. Alerts can be sent via email and webhook for easier integration with existing monitoring systems.
Device-level health monitor and alerts	Granular device-level trigger rules can be set based on infrastructure/device resource usage, device-level traffic-based thresholds, and system logs. Alerts can be sent via email and webhook for easier integration with existing monitoring systems.
Reporting	Comprehensive inventory and per-service operation reports can be generated on-demand or scheduled for automated delivery. Reports are available via PDF download or direct email distribution.
Event and audit logs	Event viewer provides consolidated system and service event logs from all registered A10 devices. Audit viewer provides access to audit logs from the A10 Controller, and all registered Thunder and license management activity logs. Granular log filters are available, and logs can be downloaded in CVS format.
Administration and Utilities	
Multi-tenancy management	Multi-tenancy is available with granular role-based access for application teams and service owners. Each tenant (organization-unit) can be mapped with A10 device's partition (ADP/L3V) level.
CLI command utilities	Single or a batch of CLI commands can be remotely executed on multiple device partitions simultaneously.
Shared configuration resource tool	Common configuration resources/templates such as class-list, black/white-list, SLB templates, security templates, TLS/SSL certificates can be created as a shared resource and used across any registered A10 devices regardless of service types.
Certificate management	TLS/SSL certificates and keys for ADC and SSLi services can be managed by A10 Control, allowing organization-admin to store, provision, renew and monitor status (active, expiring, revoked). Integration with certificate provider such as Venafi, enables full automation of the certificate lifecycle management including-auto renewal.
License management	A10 Control works as an enterprise license manager and can manage and control FlexPool capacity licenses for registered A10 devices.
User management	Flexible user management is available with role-based access control. For example, access areas can be set with organization, tenant, device or specific service/partition, and the permission level can be administrator, operator or custom rule with specific operations.
Authentication management	Besides local authentication, identity provider (IdP) such as Azure or Okta or LDAP can be selected for external authentication and single-sign-on (SSO).

A10 Control Apps

Application Delivery	
ADC App Home	• Consolidate view of virtual server (VIP) status and deployment map under the tenant (org-unit) • Top virtual servers • Events and alerts dashboard
Analytics	• ADC services analytics for each virtual service under the organization unit • Real-time ADC service-level KPIs including traffic info, error rate and latency • User traffic-based analytics, including user insights (location, browser), top-k, request insights, time-series latency and more. • ADC service analytics for common protocols (HTTP/S, SSL and HTTP2) • ADC cluster analytics for resource usage insight • Application service analytics for detailed app service conditions and trends • Application server analytics for server health and status • Latency drilldown and analytics for end-to-end latency and a full request-response cycle
Transaction Log Viewer	• Detailed session log (HTTP/TCP) with client, packet, protocol, request header, latency information and more • Events view from ADC system logs • Alerts viewer based on custom monitoring and alert rules
Configurations Tool	• Centralized ADC configuration for services objects (VIP, service group, servers) and shared objects including templates, aFleX and health monitors • Automatic config learning (brownfield deployment) and config sync

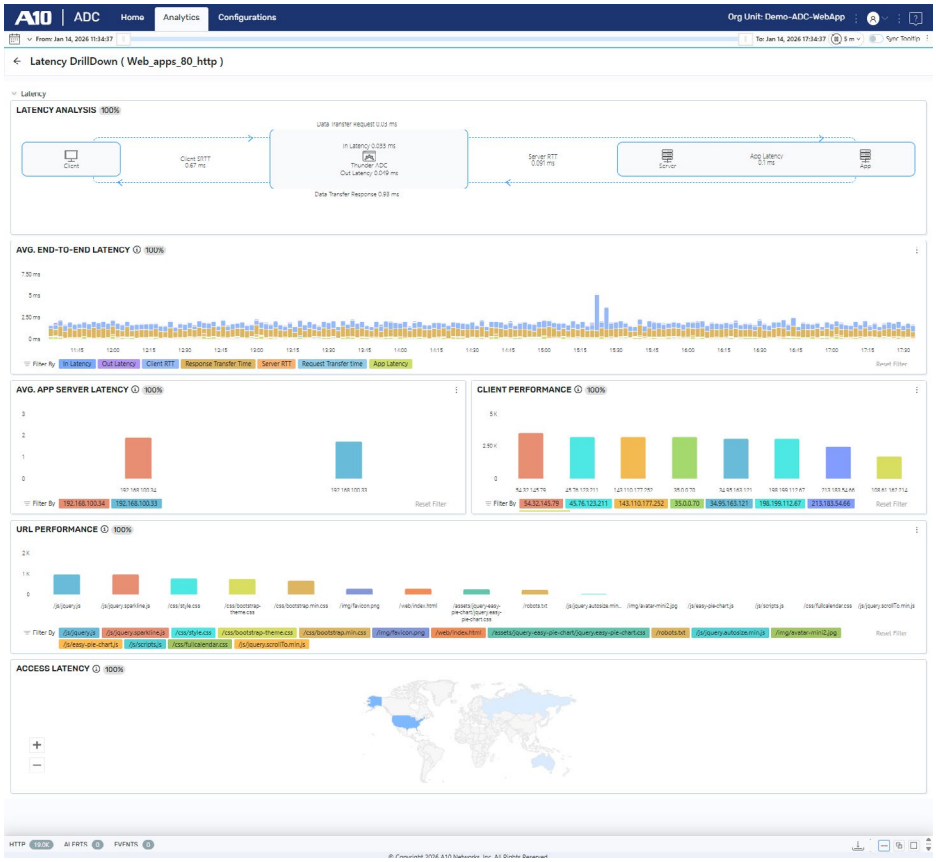

Figure 7. ADC analytics for latency drilldown.

Defend Orchestrator	
Protection Workflow Orchestration	• Enables seamless and automated DDoS protection from detection to mitigation and reporting • Automatic DDoS incident reporting after the attack is over
Orchestrator Dashboard	• DDoS incidents and activities overview • Overview of the DDoS protection status and activities • Dashboard for service protection health, aggregated traffic for mitigation • Attack trend insights (top-k) for attack types, sources, victims/destinations and more
DDoS Incidents Console	• Mitigation console for DDoS defense monitoring and live operation (drill-down to service port level) • Live traffic charts with packet rate, volume, traffic indicators, and packet drop chart based on countermeasures • Top-k (source and destination), incident and event logs, alerts viewer, and global and service port level mitigation statistics • Manual intervention for custom mitigation policy
Monitoring	• Real-time traffic charts and statistics under monitored zones/objects • Detailed IP visibility and insight for victim and source (top-k) • Remote triggered packet capture tool (on-demand or automated) • On-demand and scheduled reports for DDoS incidents, protected zones, device inventory, etc.
Configurations Tool	• Centralized DDoS protection profiles and operational policies configuration • Intuitive configuration with reusable predefined templates, protection profiles and operational policies • Support BGP based traffic redirection (in reactive deployment), RTBH, Flowspec • DDoS protection specific device management (Mitigator and Detector settings)

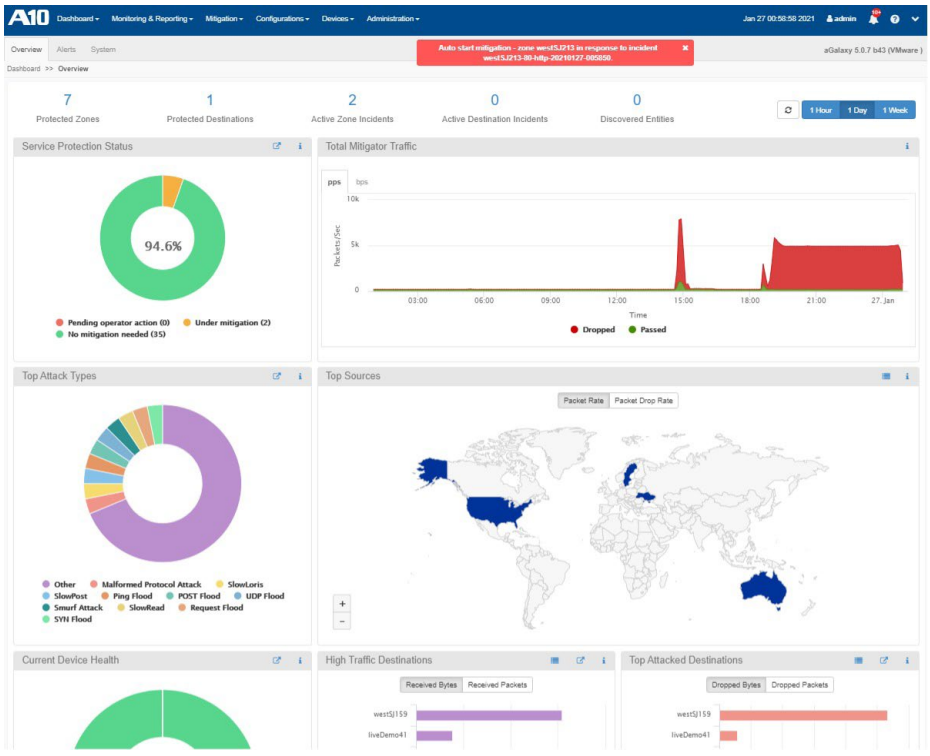

Figure 8. A10 Defend Orchestrator dashboard provides real-time attack statistics and summaries of DDoS incidents.

SSL Insight	
Deployment Wizard	• Intuitive configuration wizard with guided or unguided workflow options for SSLi and Secure Web Gateway • Support both greenfield and brownfield deployments for any deployment options (single or dual appliance, high availability, transparent/explicit proxy, service chaining, L2/L3/virtual wire, etc.) with recommended security policies • Quick access to global (site-group), site or device level configurations for new site deployment, policy or configuration change for specific sites or devices • Support config change review using config-diff, and rollback
Centralized Configuration Management	• Store and manage various SSLi configurations as shared objects, including ACLs, policy templates, SSL profiles, certificate management, URL filtering, ICAP, AAM, SAML, G-suites and Office 365 and so on • Tagging manager defines and manages physical and logical interfaces and connectivity attributes
SSLi Analytics	• Site group scoped SSL Insight analytics with real-time KPI including connection and rate, decryption rate, error and policy violation rate • TLS traffic observations and insights for decrypted traffic top-k (source/dest), TLS and cert specifics, cached certs, and else • Security related insights based on URL category, application category and threat intelligence, provide traffic trend and patterns in connection and volume perspective, visualize risky and suspicious access for each area • Watch list allows admins to create custom category lists of URL and application for real-time traffic monitoring and analysis
Troubleshooting Tools	• Guided step-by-step test for verifying system, resources, and end-to-end communication via SSL Insight • Metric correlation for comparing different KPIs of the same device and comparing the same KPI from different devices
Transaction Log Viewer	• Provide extended view and search functions of SSLi transaction, error and firewall event logs for troubleshooting and analysis • Detailed session drilldown with rich search filters (IP, TLS, URL/app categories, size, status, and many more) and embedded Threat Investigator lookup (powered by Webroot)

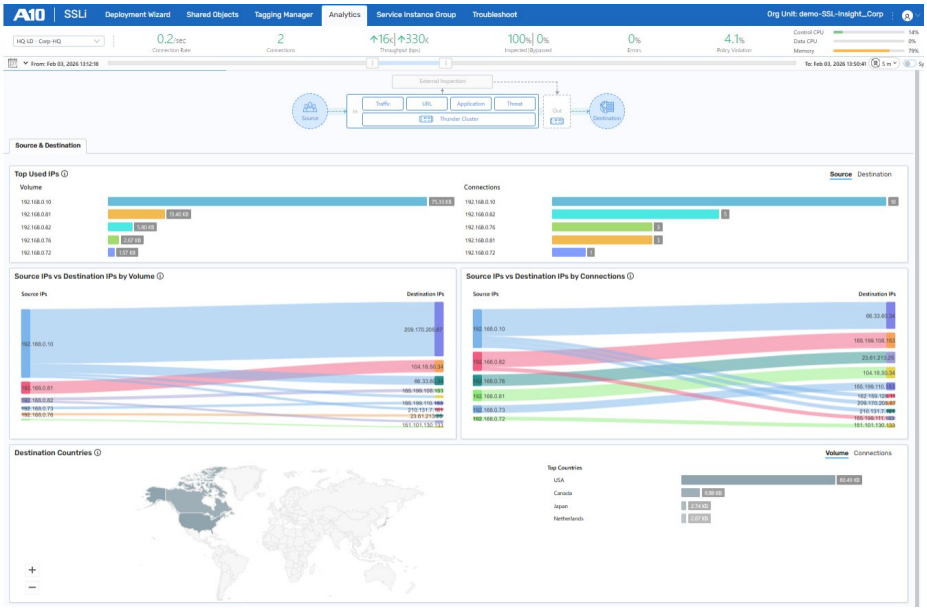

Figure 9. SSLi app for source and destination IP correlation analytics.

Carrier-grade NAT	
CGN App Home	• Consolidate view of CGNAT deployment information under the tenant (org-unit) • CGNAT services status breakdown for LSN/Fixed-NAT/1:1 NAT/DS-Lite/NAT64/NAT46-stateless technologies • Events and alerts dashboard
Analytics	• CGNAT services analytics for each CGN technology (LSN/Fixed-NAT/1:1 NAT/DS-Lite/NAT64/NAT46-stateless) under the organization unit • Real-time CGNAT service-level KPIs including traffic and session info, NAT pool usages etc. • CGNAT service insights for traffic, session, port mapping, dropped traffic & errors, link probe and CGN system • Detailed CGNAT technology-based analytics - traffic insights including session, top-k, user quota, CGN service insights including port mapping, pool usage and misbehaviors, and application category insights • Security analytics for integrated DDoS protection, black-listed IPs, and so on.
Transaction Log Viewer	• Provide extensive view of CGN sessions and transactions, including IP:port mapping, subscriber info (e.g., MSISDN, IMSI), session status, custom field and more • Detailed session drilldown with rich search filters and trace subscriber • Events viewer for from CGN error logs and system events and alerts
Configurations Tool	• Centralized CGNAT configuration (LSN/NAT64/DNS64) along with shared objects (NAT pool, class-list, EIM/EIF, ALG), integrated DDoS protection, and logging templates and more

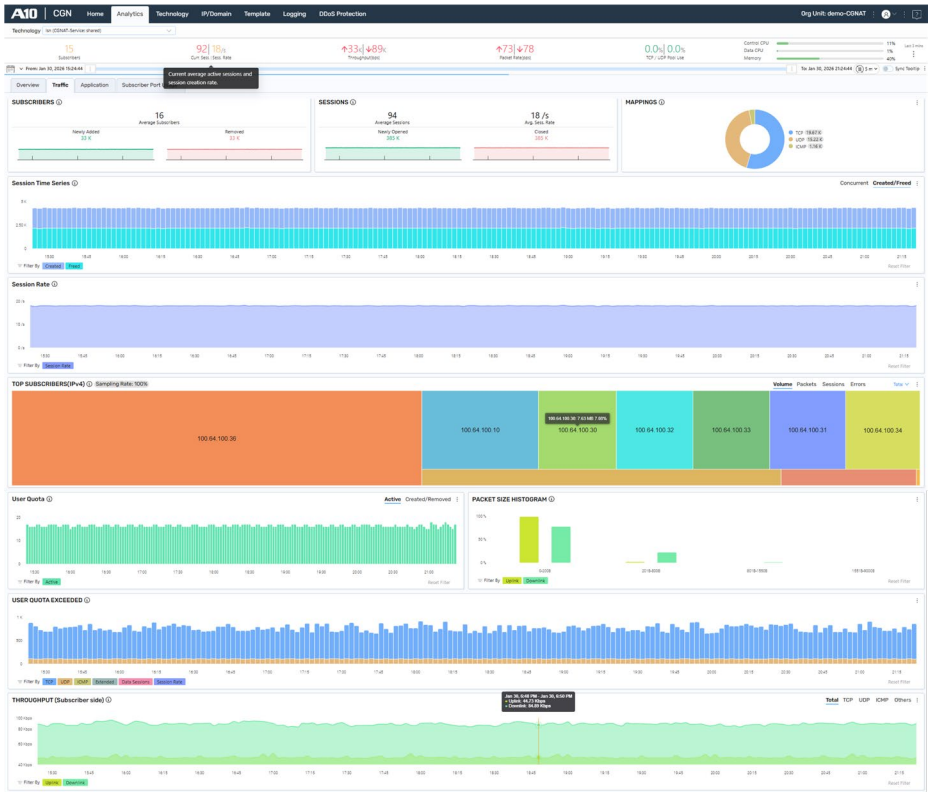

Figure 10. CGN app for LSN service traffic analytics.

Gi/SGi Firewall	
Gi Firewall App Home	• Consolidate view of Gi/SGi firewall deployment information under the tenant (org-unit) • Events and alerts dashboard
Analytics	• Gi Firewall services analytics for each firewall policy ruleset under the organization unit • Real-time GiFW service-level KPIs including traffic and session info, rule hit counters etc. • Detailed GiFW service analytics – firewall rule-based insights including rule performance, list of stale rules, top-k subscribers, and traffic insights including CGNAT mapping and utilization, application category and more
Transaction Log Viewer	• Provide extensive view of firewall sessions, including firewall zone and interfaces, associated rule and subscriber info and IP:port mapping and traced transaction for NAT'ed traffic, and more • Detailed session drilldown with rich search filters • Events viewer from GiFW/CFW system logs • Alerts viewer based on custom monitoring and alert rules

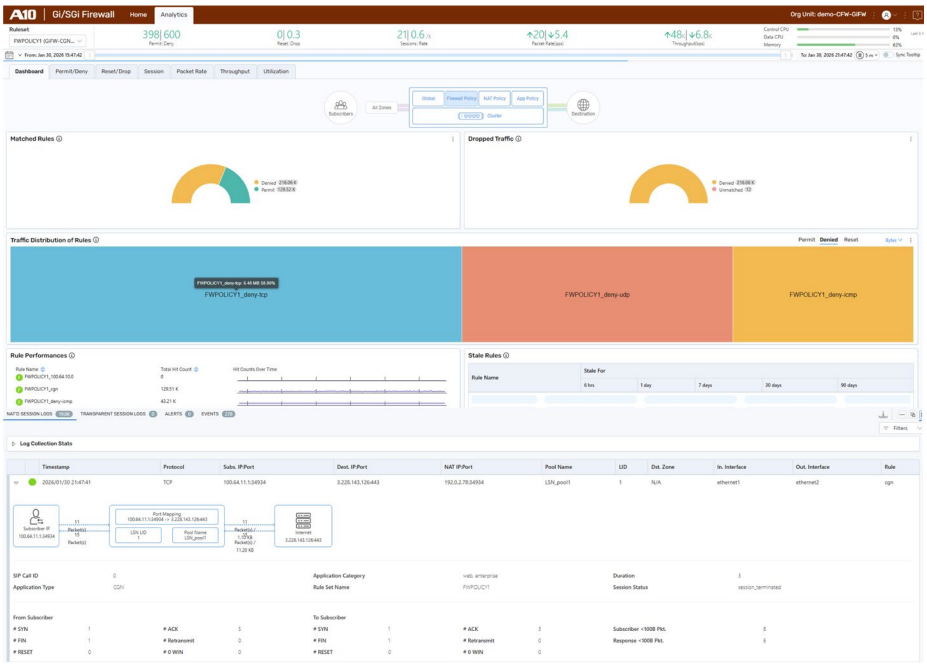

Figure 11. Gi/SGi firewall app for firewall policy analytics with detailed session viewer.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-DS-15139-EN-03 Feb 2026