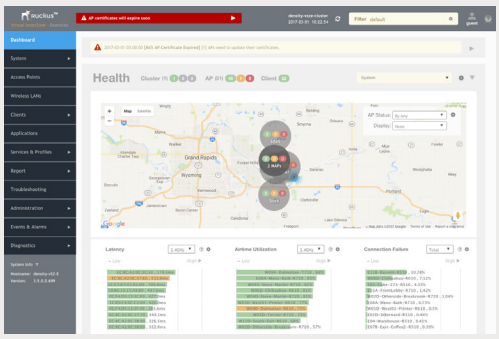
Virtual SmartZone - High Scale

Scalable Virtual Wireless LAN Controller

DATA SHEET



BENEFITS

MASS SCALE, VIRTUALLY

The vSZ-H makes possible an all-virtual data center deployment on commodity hardware at 30,000-AP scale, minimizing CAPEX and maximizing server reuse and flexibility.

ALL-IN-ONE SIMPLICITY

Virtual SmartZone (vSZ-H and vSZ-D) is a WLAN "network-in-a-box," enabling IT to easily and cost-effectively deploy and scale a high-performance WLAN, with no requirement for stand-alone elements.

MULTI-TIER MANAGED SERVICES

Multi-tenancy, domain segmentation and containerization enable secure delivery of managed WLAN services in complex, multi-tier business model and multi-geo contexts, including MVNO.

COMPREHENSIVE EXPERIENCE MANAGEMENT

Visual Connection Diagnostics speeds and simplifies troubleshooting and client problem resolution while unique "super-KPIs" enable IT to more quickly detect and react to potential user experience degradation.

MULTI-VARIATE, ROLE-BASED POLICIES

Optional Ruckus Cloudpath integration lets IT to create rich location-, device- and user-based policy rules, enabling network segmentation based on real security and policy needs rather than on a one-size-fits-all approach.

HIGH-FIDELITY STREAMING DATA

For organizations using their own network analytics tools, SmartZone supplies a near real-time feed of all KPIs, enabling IT to effectively respond in the event of rapidly deteriorating network conditions, without requiring firewall pinholes.

FULL AUTHENTICATION SUPPORT

Supports authentication via EAP-SIM, EAP-AKA, EAP-TLS (x.509), EAP-TTLS and WISPr.

ADDITIONAL ADVANCE FEATURES

Rogue AP detection, interference detection and mitigation, band steering, airtime fairness, hotspot, guest networking services and more.

The Virtual SmartZone™-High Scale (vSZ-H) represents a new class of scalable and versatile virtual WLAN controllers designed for data center deployment. Powered by the SmartZone OS, it addresses the large-scale distributed network challenges faced by service providers of all types, as well as those of large enterprises and institutions.

MULTI-SERVICE AND MOBILE NETWORK OPERATORS

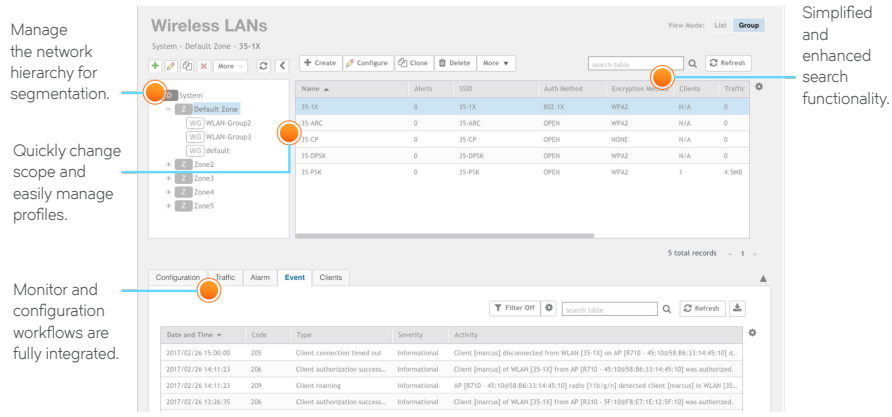
Operator deployment scenarios are among the most complex in the world, with some operators simultaneously delivering public access Wi-Fi, employee Wi-Fi and Wi-Fi as a managed service to their enterprise and small business customers. The vSZ-H allows operators to address these scenarios collectively or independently while working within the unique constraints of the operator's public and private networks.

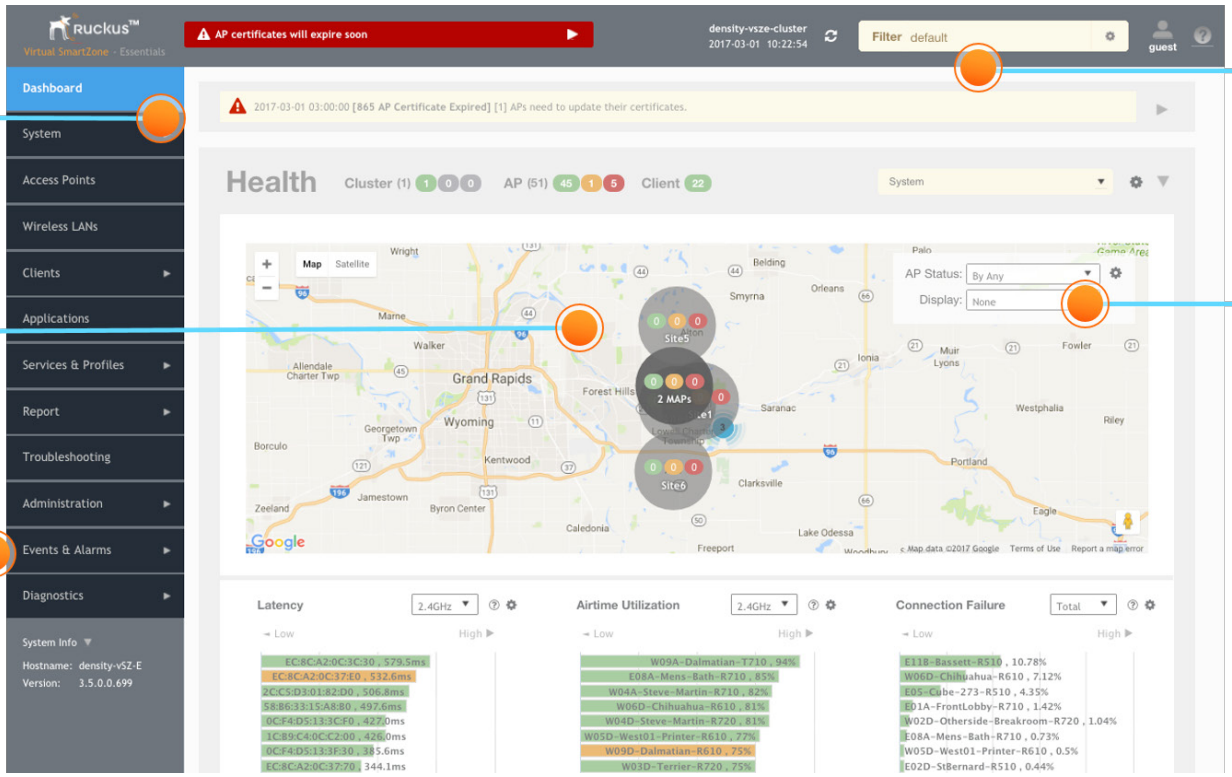
INTERNET SERVICE PROVIDERS

As Wi-Fi moves through the technology adoption lifecycle, internet service providers are changing how this infrastructure has traditionally been delivered to end-customers. By capitalizing on the Wi-Fi-as-a-Service trend, service providers are creating new revenue streams while simultaneously solving customer's problems with managing an increasingly complex network component. The multi-tenant-capable vSZ-H enables these service providers to implement sophisticated, multi-tier business and operational models, even across geographic and commercial boundaries.

LARGE CAMPUS ORGANIZATIONS

End-user quality-of-service expectations are on the rise. Capital equipment budgets are not. The vSZ-H provides IT departments with intuitive, visual tools to manage end-user experience, proactively and reactively. Its active/active redundancy architecture provides the budget flexibility that comes from having no idle capacity.





MANAGEMENT / OA&M

Multi-tier Administrative Hierarchy

A multi-tier administrative hierarchy provides more flexibility for service providers, allowing administrators to create and reuse configuration profiles within domains and zones. Role-based access control (RBAC) with pre-grouped administration permissions to makes common roles easier to setup. Define read-only or modify permissions that apply across zones, and easily add new administrator profiles and set permissions that apply across tenants.

Partner Domain Layer

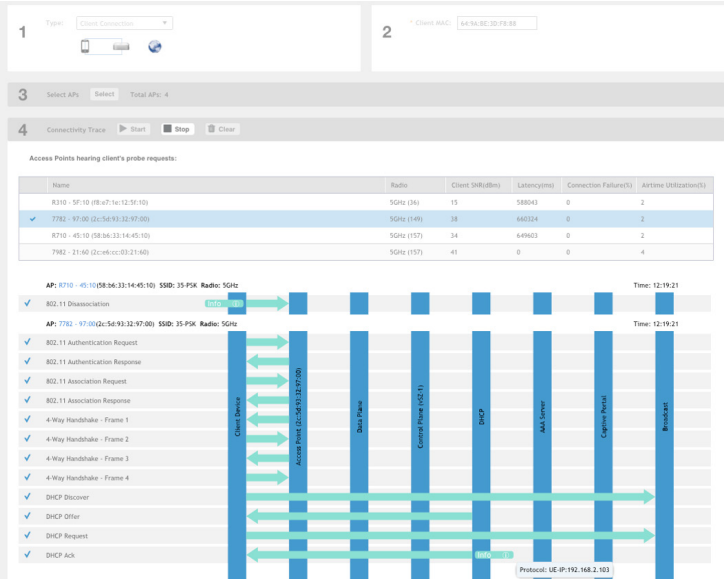
The Partner Domain Layer enables operators to separate tenants with their own unique set of configurations, profiles, and system objects that are not shared with other tenants. This creates a wall between tenants to ensure privacy and alleviate operational headaches associated with tenant management.

Administrative Dashboard

The Dashboard is a customizable and contextually rich interface that reduces the time required to support large-scale networks. Consistent menus and consolidated and streamlined navigation shortens time to perform routine tasks such as AP configuration or monitoring actions. Configurable visual filter settings for the Dashboard personalize visual network alerts and WLAN statistics; settings are preserved throughout sub-pages. View maps, health and traffic analysis, spectrum analysis, and more.

Visual Connection Diagnostics

Visual Connection Diagnostics speeds and simplifies troubleshooting and client problem resolution. This troubleshooting tool allows an administrator to focus on a specific client device and its connection status. An intuitive interface tracks the step-by-step progress of the client's connection through 802.11 stages, RADIUS, EAP authentication, captive portal redirects, encryption key setup, DHCP, and roaming. Administrators can identify information in each step, like EAP type or IP address assigned and then pinpoint where in the process a failure occurs. This enhanced visibility helps determine the likely cause of client problems and, based on the failure stage, gives useful guidance for remediation. Visual Connection Diagnostics supports open, PSK, 802.1X, and WISPr networks.



API Enhancements

A rich set of RESTful JSON APIs enables the use of 3rd party configuration, monitoring, reporting and analytics tools. Each SmartZone controller supports access to a complete set of Wi-Fi network machine-level metrics enabling it to plug directly into existing automated backend systems and to provide a 'headless' interface for the WLAN infrastructure.

Public API support includes zone and WLAN details, AP group override settings and AP override settings. API improvements are supported by near real-time monitoring with data granularity as fine as three minutes. The real-time push streaming data driven framework enable SmartZone to deliver better report and management support.

Multi-Zone Control

Multi-Zone is used to segment the WLAN into independent organizational units. IT can create policies that group AAA, DPSKs, Hotspot portals, Bonjour policies, and WebAuth portals and assign them to one or multiple zones. Different zones can operate using different firmware versions or different country codes. Administrators can also upgrade AP zones independently from the controller software and manage APs with firmware up to two releases old. IT can update firmware one zone at a time or within a dedicated test zone before upgrading the entire network.

Lawful Intercept

All SmartZone WLAN controllers support lawful intercept of encrypted traffic to maintain CALEA compliance on public or government-owned networks. Enable the mirroring of client traffic to a LIG (Lawful Intercept Gateway) over L2oGRE (Soft-GRE).

SECURITY AND POLICY

Automated Enhanced Client Security / DPSK

Ruckus patented Dynamic PSK™ (DPSK) enhances client security by automating randomized passphrase keys for use with each device. The vSZ-H supports 50,000 DPSKs, with up to 10,000 per zone. Group DPSK, user-specified passphrase and number-only DPSK further enhance client security in all settings.

Group DPSK allows IT to create a DPSK that can be shared by multiple different devices, with up to sixty-four Group DPSKs in a zone. Administrators can also specify a number-only DPSK, which makes guest or other "easy entry" scenarios more user-friendly.

WIDS / WIPS / Rogue AP Detection

The vSZ-H includes Wireless Intrusion Detection and Prevention System (WIDS/WIPS) functionality, enabling rogue AP detection. Rogue access points exhibiting malicious behavior such as spoofing the SSID or BSSID of a connected Ruckus AP are prevented from connecting clients to the network.

APs can be classified as "rogue" or "known" to minimize disruption towards unowned neighboring APs or lab equipment, preventing the network from acting against these discovered APs.

Role-Based Policy Management

Granular role-based policies enable the creation of policy groups segmented by user role, domain, location, OS type, certificate status, VLAN and many more factors. Roles are assigned during the authentication phase of new user onboarding, then VLAN, OS, and L3-7 policies are assigned as desired. Policy enforcement actions include allow, deny, and rate-limit based on VLAN or VLAN pool and L3/L4 Access Control Lists (ACLs).

Hotspot 2.0 / Passpoint

Hotspot 2.0 enables 802.1x/EAP mobile devices to automatically discover, select and authenticate to APs for which a roaming arrangement exists. Hotspot 2.0 is automatic and requires no user intervention after proper device provisioning. Self-service provisioning can be accomplished by the Ruckus Cloudpath security and policy management platform.

Isolation Whitelist

Administrators can manually configure a whitelist entry, either to add non-gateway devices such as printers or to allow additional gateway MAC addresses that may be required for load balancing or other functions. The isolation whitelist can be auto-only, manual-only, or auto and manual.

Bonjour Management

Bonjour Management enables the detection of Bonjour services (such as AirPlay, Apple TV and other Apple network services) and other mDNS-based services such as ChromeCast across VLANs and subnets for both wired and wireless networks. The vSZ-H is preconfigured with common Bonjour service types, making Bonjour service detection automatic.

Bonjour Fencing allows administrators to control the physical area in which a given Bonjour-based service is discoverable. This is accomplished by mapping to nearby APs devices that are advertising Bonjour services and allowing only that AP or its neighbors to advertise the Bonjour record. This prevents users/devices from discovering Bonjour services that are not nearby and thus not relevant to their search.

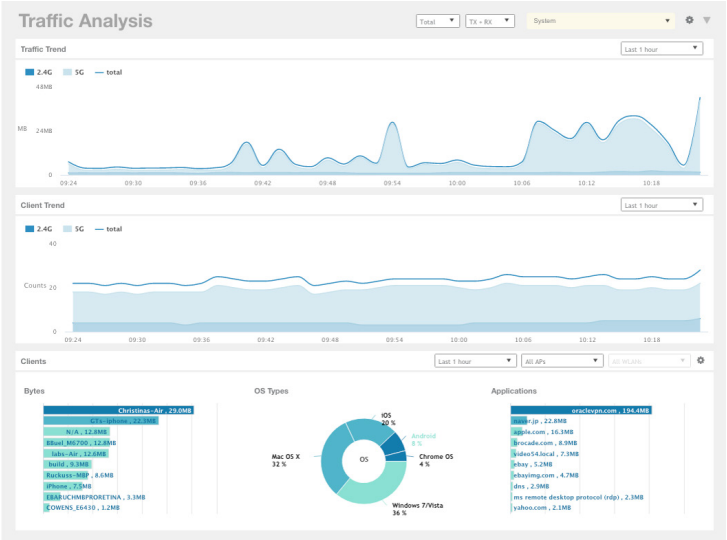
Additional Security and Policy Features

- **DoS Prevention –** Admins can monitor connected clients and easily block a specific device if suspicious behavior is detected or a device is stolen. Block a user device if it fails authentication too many times in a short period. Includes configurable settings for number of failures, span of time to measure failures, and duration of block. This prevents common authentication hacks or other DoS attacks that consume AP resources.
- **Manual-Block -** Admins can select one or more wireless clients and create a system/zone-wide block. This block prevents the device from connecting to any AP on the system. This can be useful in situations in which devices have been stolen or compromised, or in which a user has violated an acceptable use policy.
- **LDAP over SSL -** Allows the vSZ-H connection to use LDAPS, which initiates a TLS-encrypted session before LDAP messages are transferred, thus providing an additional layer of data privacy.

NETWORK INTELLIGENCE

Traffic Analysis

Traffic analysis displays domain, zone, AP group, WLAN, and AP traffic and client trends over time. Quickly find the most heavily loaded AP or top network users and devices. View client OS types and application consumption. Filter statistics by band (2.4 GHz, 5 GHz, or both) and traffic direction (uplink, downlink, or both), and monitor client load over time.



Indoor and Outdoor Maps

With Maps, centrally view all sites at the same time with Google Maps integration and display sites, floorplans and APs on the map. Simplify routine checkups of AP health on a site-by-site basis with one click. Inspect the status of APs across floorplans to find online, flagged, and offline APs. View health and traffic data for each AP to evaluate site performance. Administrators can choose an AP to view details like health status, IP address or other operational metrics. APs are color-coded by status, and administrators can overlay operational data—like operating channel, traffic, client count, airtime utilization—for each AP on the map.

Layer 7 Application Visibility and Control

Robust Layer 7 application recognition and control pinpoints top applications and top users, among other metrics. The vSZ-H allows rate limiting, blocking and QoS actions by application to support organizational network usage policies. The application signature database is updated independently of SmartZone firmware upgrades, ensuring that administrators can always manage and control the latest applications.

Super-KPIs

Unique “super-KPIs” enable IT to more quickly detect and react to potential user experience degradation. vSZ-H proactively monitors a core set of metrics that consistently correlate well with common problems, and presents a summary metric as a starting point for problem isolation. Using aggregate measurements that capture a broad range of problems associated to the Wi-Fi network simplifies troubleshooting by narrowing the scope and location of the problem. These holistic, proprietary, “super” metrics include Latency, Airtime Utilization, and Connection Failure.

AP Health

AP health is a key indicator of user experience quality and with vSZ-H this information is presented front-and-center. On the Dashboard, AP status is categorized based on health/performance thresholds defined by an administrator. On a map, APs are color-coded based on this status. vSZ-H automatically identifies APs that cross performance thresholds and visually ranks the worst-performing APs. With this data and historical trend analysis, admins can easily compare individual APs with groups of APs to look for isolated trouble spots or identify broader patterns.

Cluster Health

Monitor and flag cluster node status and keep critical cluster health alerts highlighted within the Dashboard through status symbols showing Green/Yellow/Red for each cluster node. Displays historical line charts and allows threshold settings for Cluster Health, spanning CPU, RAM and disk utilization, port/interface usage, and packet rates.

Client Health

Check on real-time client performance metrics, connectivity, and traffic. View client signal-to-noise ratio (SNR) and data rate, as well as historical traffic, to help troubleshoot connectivity problems.

Topology Health

The Topology view contained within the Dashboard uses a system hierarchy tree to enable easy identification of network problems inside domains, zones, and AP groups. Visually identify with Green/Yellow/Red status indicators nodes in the tree with offline APs or APs with poor performance that have crossed admin-defined performance thresholds.

Spectrum Analysis

On-demand real-time spectrum analysis make use of existing radios within the AP, removing the requirement to have dedicated APs for spectrum reporting. Visualize RF spectrum by real-time energy, real-time utilization, density, energy waterfall, and utilization waterfall. While an AP conducts a spectrum scan, clients are offloaded to nearby APs to minimize connection disruptions. In the case of APs with three radios, the 3rd radio can provide spectrum analysis of both 2.4 and 5 GHz bands without impacting client connectivity. Spectrum Analysis is supported on 802.11n, 802.11ac Wave 1 and Wave 2 APs.

Report Generation and Export

View rich statistics on subscribers (including client fingerprinting), APs, SSIDs, backhaul (mesh), and the vSZ-H cluster itself, with granularity as low as three minutes. Reports encompassing durations of hours to weeks can be generated for a variety of key performance indicators (KPIs) and exported in multiple formats. For operators seeking richer information, the Ruckus SmartCell Insight (SCI) network analytics tool provides for long-term data storage, data analytics and more complex reports.

CONNECTIVITY

Distributed Connectivity Optimization

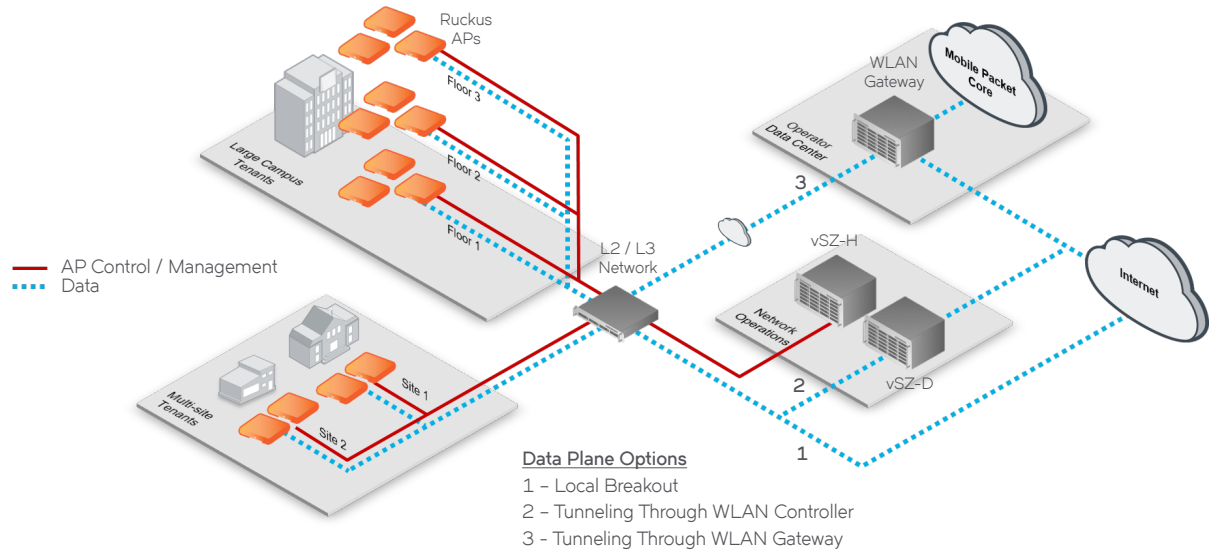
With an encrypted AP-to-AP communications protocol, managed APs discover neighboring APs over-the-air and build encrypted communication channels to share network load, operating channels, roaming and other relevant RF parameters. This enables smarter roaming and load balancing behavior and is supported on both IPv4 or IPv6 networks.

SmartMesh Wireless Backhaul

Ruckus SmartMesh supports wireless backhaul redundancy by creating self-forming, self-healing mesh networks automatically with a single checked box on the administrative interface. With Ruckus APs and BeamFlex+ technology, APs adapt to changing conditions to further ensure a solid mesh connection between APs, making use of the 5 GHz band to backhaul AP traffic to a point where wireline facilities are available. Mesh backhaul configurations dynamically reconfigured to reroute traffic over different paths as conditions change.

Radio and Wi-Fi Optimization

- **BeamFlex+ -** BeamFlex+ adaptive antenna technology increases every Ruckus AP's performance and range. Multiple antenna elements inside each AP manipulate RF patterns in real time to maximize, on a per packet basis, signal gain for each client, while accommodating changes in client device orientation. This technology mitigates radio interference, noise related performance issues, and improves application flows especially for mobile devices.
- **ChannelFly -** The ChannelFly dynamic channel management technology in all Ruckus APs improves wireless performance in highly congested environments by dynamically switching a client to a better channel when the one it's using starts to degrade. This capability allows APs to automatically select the optimum 2.4 and 5 GHz channels to maximize performance and minimize interference. ChannelFly also supports a channel-change cost metric that refines client channel migration using channel capacity prediction models and initial learning and settling time updates.
- **Capacity-Based Admission Control -** To help ensure existing clients' quality of service during periods of heavy load, Ruckus APs implement a capacity-based client access control algorithm that declines connection requests from new clients if already-connected clients are at risk of service quality degradation.



ARCHITECTURE

Separate Control and Data Plane

The SmartZone platform addresses deployment and latency constraints with traditional WLAN architectures by implementing a customized Local MAC architecture which places all essential WLAN services including authentication and association requests within the Ruckus AP. This enables all SmartZone controllers to separate control and management traffic from data traffic while optimizing for both using SSH-based and GRE-based protocols, thus improving deployment flexibility and network latency.

A single SmartZone controller placed within a centralized data center can manage multiple remote sites without forcing all authentication requests or client data to tunnel through the SmartZone controller.

User traffic is bridged through the local L2/L3 network which improves latency between clients and services.

Branch office deployments and direct integration between APs and local IT infrastructure Active Directory, LDAP, RADIUS, DHCP, DNS, and Firewalls are also enabled.

Data encryption of payloads being transmitted over a public network connection, such as the Internet, are encrypted with SmartZone.

Scalable Cluster Architecture

Active/active clustering delivers higher availability and resiliency than traditional N+1 standby. The architecture ensures redundancy and balances AP loading with cluster-wide management across data centers and zero idle controller capacity.

AP Survivability

The vSZ-H minimizes the impact of lost connectivity between the controller and the AP by placing essential WLAN services within the AP. WAN link outages or controller failures do not affect the normal operation of WLAN services.

Offload DHCP/NAT Services

DHCP/NAT services are provided by the AP or separately by the Ruckus Virtual SmartZone Data Plane while the vSZ-H centrally manages the AP and maintains through-NAT client visibility. This topology simplifies the replication of a WLAN configuration across multiple sites while minimizing capital expenditures associated with separate routers and DHCP servers.

SMARTZONE OS: COMMON FEATURES AND ATTRIBUTES			
Active Clustering Ensures redundancy and balanced AP loading with cluster-wide management across data centers and zero idle controller capacity.	**Separate Control and Data Planes** Segment user traffic from management/ control traffic for flexible deployment, higher security and lower-cost scaling and tunneling.	**Flexible Tunneling** Allows for distributed or centralized L2 tunneling on a per-WLAN or per-zone basis using Ruckus or 3rd-party data plane nodes.	**Survivable AP Architecture** In the event of backhaul outage, new APs and clients can be added and full WLAN functionality persists.
Visual User Interface Intuitive, graphics-intensive interface simplifies and speeds control and management tasks, while enhancing visibility.	**Rich Northbound APIs** RESTful JSON APIs enable the use of 3rd party configuration, monitoring, reporting and analytics tools.	**Flexible Licensing** Migratable, single-AP licenses ensure linear pricing, while intra-cluster sharing eliminates duplicate license costs.	**Integrated Reporting** Customizable reports with visual alerts and pivot-table functionality makes it easy to prioritize and respond to network conditions.

Virtual SmartZone - High Scale

Scalable Virtual Wireless LAN Controller

DATA SHEET

SUPPORTED CONFIGURATIONS	
Managed APs	• Up to 10,000 per one unit vSZ-H • Up to 30,000 per cluster of 4 units
Client Devices (UEs)	• Up to 100,000 concurrent session per vSZ-H • Up to 300,000 per cluster of 4 units
WLANs	• 6,144 per vSZ-H
Controller Expansion	• Up to 4 controllers in N+1 active-active mode, supporting non-disruptive capacity expansion.
Controller Redundancy	• Distributed data preserving with 3:1 redundancy

# OF APS	# OF CLIENTS	vCPU (Core)	RAM (GB)	DISK (GB)
100	2,000	2	8	100
500	10,000	4	9	100
1,000	20,000	4	11	100
2,500	50,000	6	15	300
10,000	100,000	16	48	600
30,000	300,000	24	48	600

MODEL	DESCRIPTION
L09-0001-SG00	AP management license for SZ-100/vSZ 3.X, 1 Ruckus AP
L09-VSCG-WW00	Virtual SmartZone 3.0 or newer software virtual appliance, 1 instance, includes 1 AP license
S01-0001-1LSG	Partner WatchDog support per SZ/vSZ AP, 1 YR
S01-0001-3LSG	Partner WatchDog support per SZ/vSZ AP, 3 YR
S01-0001-5LSG	Partner WatchDog support per SZ/vSZ AP, 5 YR
S01-VSCG-1L00	End user WatchDog support - vSZ-RTU, 1 YR
S01-VSCG-3L00	End user WatchDog support - vSZ-RTU, 3 YR

Ruckus™ Simply Better Wireless.

Ruckus Wireless, Inc. | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065
ruckuswireless.com