KARTA KATALOGOWA

RUCKUS® SmartZone

Ultraskalowalne i odporne na awarie kontrolery sieciowe dla dostawców sieci jako usługi i dużych przedsiębiorstw

COMMSCOPE® RUCKUS®

KORZYŚCI

Łatwe tworzenie konkurencyjnych ofert usług zarządzanych
Opcje wielopoziomowego klienta, hierarchicznego podziału klientów oraz wirtualne/fizyczne kontrolery umożliwiają tworzenie wyrafinowanych ofert typu „sieć jako usługa" o złożonych poziomach jakości.

Skalowanie sieci na żądanie
Klienci mogą wdrożyć wirtualnego SmartZone w chmurze prywatnej na platformach AWS Cloud, Azure Cloud i Google Cloud, aby zminimalizować początkowe koszty i zmaksymalizować elastyczność wdrożenia i skalowania.

Wzmocnienie odporności sieci
SmartZone chroni przed katastrofalnymi awariami, zapewniając przełączanie awaryjne w obrębie klastra i między klastrami za pomocą georedundancji i redundancji active/active klastrów, która przewyższa dostępnością architekturę hot standby.

Personalizacja pulpitów klientów
Rozbudowane interfejsy API ułatwiają dodawanie, konfigurowanie i monitorowanie punktów dostępowych i przełączników w aplikacjach innych firm. Pulpity dla administratorów klientów mogą być personalizowane i zaopatrzone w szatę graficzną zgodną z identyfikacją wizualną firmy.

Automatyczne wykrywanie i konfigurowanie
Automatyczne wykrywanie i konfigurowanie punktów dostępowych i przełączników zmniejsza konieczność kierowania się intuicją, obniża koszty administracji i przyspiesza wdrażanie przy użyciu domyślnych reguł.

Koszt współmierny do wzrostu
Każdy kontroler sieci SmartZone jest w stanie zarządzać 10 000 punktów dostępowych, 150 000 klientów i pasmem o szerokości do 20 Gb/s zależnie od modelu. Licencje bezterminowe, z możliwością migrowania oraz zależne od liczby punktów dostępowych lub przełączników pozwalają uzyskać wyższy zwrot z inwestycji.

Szybka diagnostyka
Funkcja Visual Connection Diagnostics przyspiesza i upraszcza rozwiązywanie problemów z klientami bezprzewodowymi. Dział IT może również szybciej wykrywać pogorszenie jakości sieci i reagować na nie, obserwując wskaźniki na pulpicie SmartZone.

Roaming Wi-Fi nowej generacji
Zarządzanie roamingiem opartym na hotspotach i Wi-Fi między własnymi i innymi sieciami dzięki obsłudze HotSpot 2.0 Release 3, zabezpieczeniu RadSec i Google Orion.

Dodatkowe funkcje zaawansowane
SmartZone obsługuje także m.in. konwergencję zarządzania siecią przewodową i bezprzewodową, filtrowanie treści, wykrywanie i zwalczanie nieautoryzowanych punktów dostępowych, równoważenie obciążenia, airtime fairness, onboarding gości i kontrolę dostępu zależna od pojemności.

Kontrolery sieciowe RUCKUS SmartZone redukują zawiłości skalowania przełączników przewodowych i bezprzewodowych punktów dostępowych oraz zarządzania nimi, stanowiąc wspólny interfejs do obsługi ofert sieci jako usługi (NaaS) w chmurze prywatnej, a także sieci korporacyjnych ogólnego użytku. Wszystkie fizyczne i wirtualne urządzenia SmartZone obsługują funkcje konfigurowania, monitorowania, dodawania, wykrywania, planowania, diagnostyki, sterowania wydajnością, zabezpieczania i raportowania sieci. Scentralizowany, łatwy w obsłudze interfejs przeglądarkowy SmartZone umożliwia wgląd w funkcjonowanie sieci od bezprzewodowej krawędzi do rdzenia i ułatwia administratorom IT wykonywanie rutynowych zadań zarządzania, rozwiązywanie problemów użytkowników z połączeniami oraz wyznaczanie i monitorowanie polityk na poziomie użytkowników i aplikacji, nie wymagając od nich zarazem posiadania wysokich kwalifikacji w dziedzinie sieci ani umiejętności obsługi CLI.

OPERATORZY SIECI WIELOUSŁUGOWYCH I MOBILNYCH

Wdrożenia u operatorów należą do najbardziej skomplikowanych na świecie, tym bardziej, że niektórzy operatorzy równocześnie dostarczają sieć Wi-Fi do publicznego dostępu i Wi-Fi jako usługę zarządzaną dla przedsiębiorstw i małych firm. Wersje SmartZone 300 (SZ300) i Virtual SmartZone – High Scale (vSZ-H) wychodzą naprzeciw takim potrzebom, umożliwiając elastyczne instalowanie przełączników i punktów dostępowych w sposób podporządkowany specyficznym ograniczeniom równoległego funkcjonowania sieci publicznych i prywatnych jednego operatora.

DOSTAWCY USŁUG

Dostawcy Internetu dostarczają Wi-Fi jako usługę (WaaS) i sieć jako usługę (Naas), aby zyskać nowe źródła przychodu, chcąc równocześnie upraszczać swoim klientom zarządzanie coraz bardziej złożonym środowiskiem sieciowym. Hierarchiczna obsługa wielu klientów w SZ300 i vSZ-H umożliwia dostawcom usług wdrożenie wielopoziomowych modeli biznesowych i operacyjnych dla różnych rejonów geograficznych i sektorów rynku.

PRZEDSIĘBIORSTWA

Potrzeba zapewnienia jak najlepiej działającego Internetu dla pracowników i klientów wzbudza zainteresowanie firm i instytucji z każdego sektora optymalizacją infrastruktury sieciowej. SmartZone 144 (SZ144) i Virtual SmartZone – Essentials (vSZ-E) umożliwiają wszystkim przedsiębiorstwom wdrożenie przystępnej i odpornej na awarie sieci przewodowej i bezprzewodowej, która będzie obsługiwała strategie korzystania z własnych urządzeń, aplikacje multimedialne i IoT. Ponadto SmartZone wyposaża działy informatyki (IT) i technologii przemysłowej (OT) w intuicyjne, wizualne narzędzia do centralnego zarządzania działaniem usług u użytkownika w rozproszonych i zdalnych biurach. Architektura redundancji active/active zapewnia elastyczność budżetową wynikającą z wyeliminowania niewykorzystanych mocy.

Odbiorcy	Sprzętowy	Wirtualny
Średnie i duże przedsiębiorstwa	SmartZone 144 (SZ144)	Virtual SmartZone -Essentials (vSZ-E)
Operatorzy i dostawcy usług	SmartZone 300 (SZ300)	Virtual SmartZone - High Scale (vSZ-H)

EKSPLOATACJA, ADMINISTRACJA I ZARZĄDZANIE

Wielopoziomowa obsługa klientów

Hierarchia administracyjna zapewnia dostawcom usług elastyczność wielopoziomowego zarządzania klientami, aby administratorzy mogli tworzyć profile konfiguracji w obrębie domen i stref oraz wielokrotnie z nich korzystać. Kontrola dostępu oparta na rolach z domyślnie pogrupowanymi uprawnieniami administracyjnymi ułatwiają konfigurowanie typowych ról. Definiowane lub modyfikowane uprawnienia, w tym także tylko do odczytu, mogą dotyczyć wielu stref, a dodawanie profili administratora i ustawianie uprawnień obejmujących wielu klientów nie sprawia żadnego problemu.

Tylko: SZ300, vSZ-H

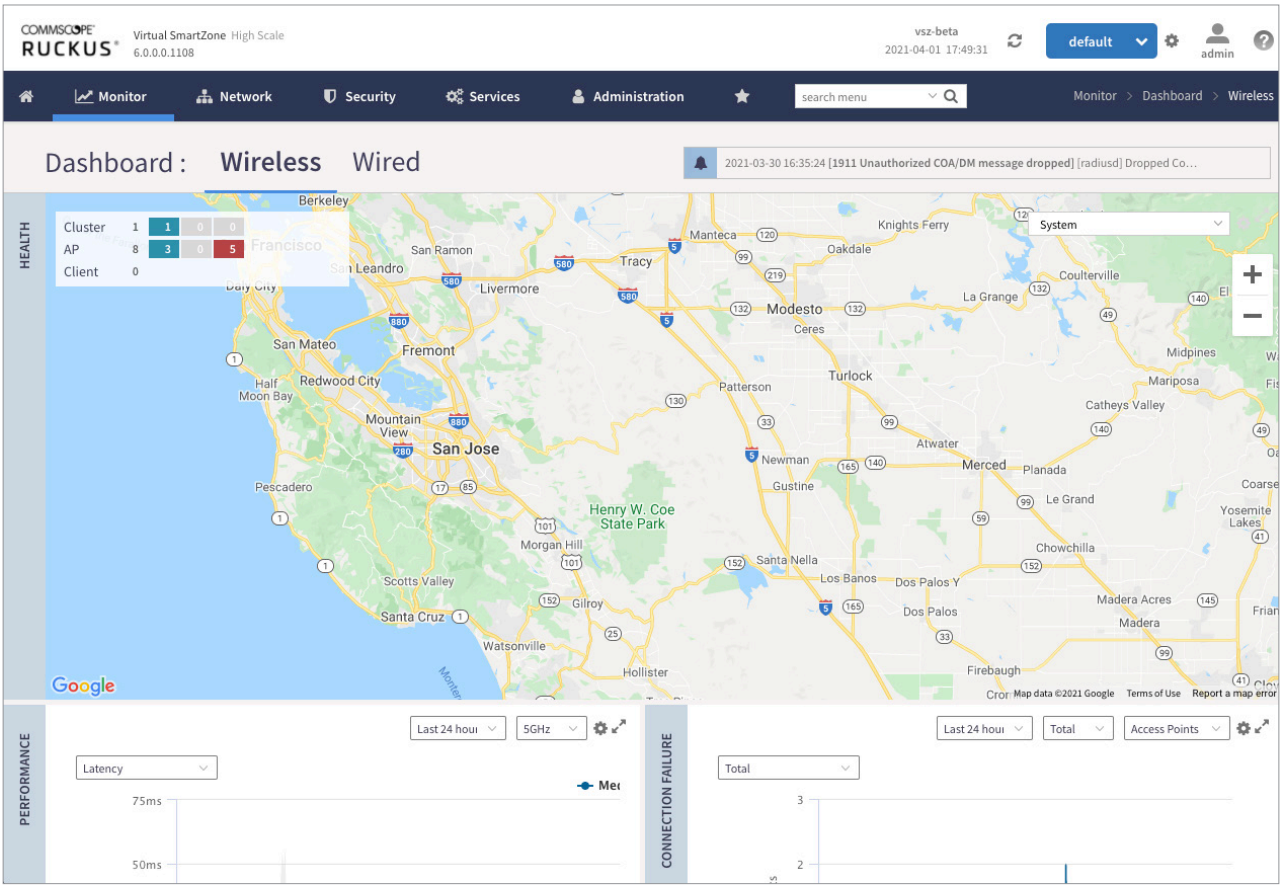
Domena partnera

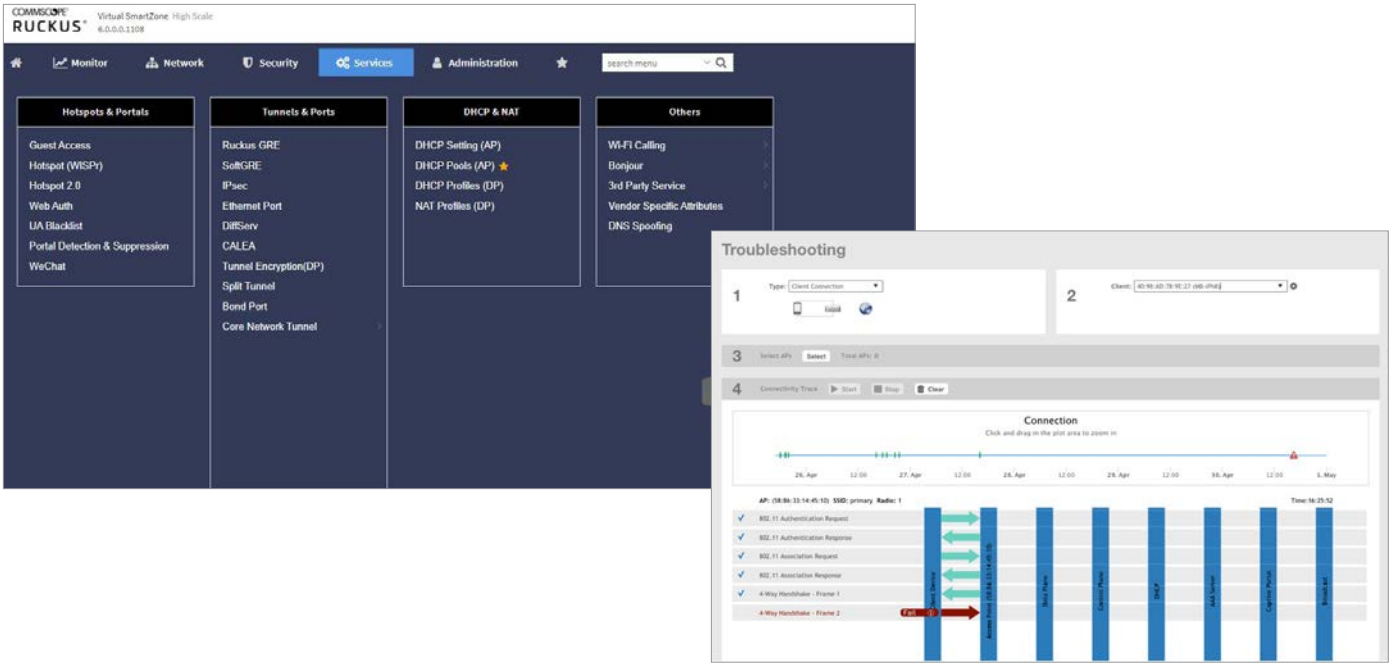
Domena partnera umożliwia operatorom odseparowanie klientów z ich własnym zestawem konfiguracji, profili i obiektów systemowych, które nie są współużytkowane z innymi klientami. Można to porównać do budowy ściany między klientami w celu zapewnienia poufności i złagodzenia trudności operacyjnych związanych z zarządzaniem klientami. Ponadto dostawcy usług mogą spersonalizować pulpit administracyjny dla swoich klientów, dodając ich logo oraz teksty.

Tylko: SZ300, vSZ-H

Pulpit administracyjny i menu

Pulpit jest personalizowanym i rozbudowanym kontekstowo interfejsem przystosowanym do potrzeb dużych sieci. Funkcja wyszukiwania umożliwia szybkie znalezienie określonego menu. Często używane menu można natomiast dodać do menu Ulubione, aby móc szybko wykonywać rutynowe zadania, jak konfigurowanie punktu dostępowego i przełącznika. Podmenu także są podzielone na grupy, jak systemy klienckie, diagnostyka, kontrola aplikacji, kontrola dostępu, sieci bezprzewodowe i sieci przewodowe. Wizualne ustawienia pulpitu personalizują alerty i statystyki sieciowe, które są wyświetlane niezależnie od strony podrzędnej. Topologię całej sieci można obejrzeć na różne sposoby w widokach topologii lub kuli. Wśród wykresów i widoków znajdują się także mapy oraz analizy kondycji, ruchu i widma. Wskaźnik Brak połączenia na pulpicie pozwala administratorom obserwować trendy zrywania połączeń w całym systemie oraz wykrywać nieprawidłowości połączeniowe wywołane problemami o charakterze systemowym.





Wizualna diagnostyka połączeń
Funkcja Visual Connection Diagnostics do bezprzewodowych systemów klienckich przyspiesza i upraszcza rozwiązywanie problemów klientów. Korzystając z tego narzędzia diagnostycznego, administrator może skupić się na konkretnym systemie klienckim i jego statusie połączenia. Sekwencja połączenia klienta wyświetlana jest w intuicyjnym interfejsie, etap po etapie, jak 802.11, RADIUS, uwierzytelnienie EAP, przekierowanie do strony startowej, konfiguracja klucza szyfrowania, DHCP i roaming. Administratorzy mogą przeglądać poszczególne kroki, jak przypisanie adresu IP, i precyzować, na którym etapie procesu występuje błąd. Ta rozbudowana strona wizualna ułatwia ustalenie prawdopodobnej przyczyny problemów i, zależnie od etapu, może od razu sugerować sposób postępowania. Visual Connection Diagnostics obsługuje sieci otwarte, PSK, 802.1X i WISPr.

Interfejsy API zarządzania siecią
Duża biblioteka dobrze udokumentowanych interfejsów API REST umożliwia wywoływanie w aplikacjach innej firmy praktycznie dowolnej zmiany konfiguracji wyświetlanej w graficznym interfejsie użytkownika (GUI) lub interfejsie wiersza polecenia (CLI) systemu operacyjnego SmartZone. Umożliwia to menedżerom IT korzystającym z aplikacji innej firmy dostęp do funkcji systemu operacyjnego SmartZone bez opuszczania ich systemu zarządzania i wydawanie bezpośrednich poleceń bez konieczności tworzenia podatnych na błędy własnych skryptów.

Komplet strumieni danych bufora protokołu/MQTT w czasie zbliżonym do rzeczywistego umożliwia przekazywanie do aplikacji innej firmy wszystkich danych sieciowych, statystyk i alarmów (z klienta, punktu dostępowego, przełącznika, WLAN, kontrolera, klastra) z niewielkim opóźnieniem, bez utraty wierności i bez potrzeby tworzenia luki w zaporze. Te strumienie danych umożliwiają odtworzenie elementów pulpitu SmartZone lub spersonalizowanych pulpitów do użytku wewnętrznego i zewnętrznego. Na tej zasadzie opiera się działanie oprogramowania do raportowania i analityki sieci RUCKUS.

Każdy kontroler SmartZone obsługuje dostęp do kompletu wskaźników na poziomie urządzenia, umożliwiając podłączenie bezpośrednio do istniejących zautomatyzowanych systemów zaplecza i stanowiąc interfejs „headless" do infrastruktury sieci.

Autonomia stref
Funkcja wielu stref służy do podziału sieci bezprzewodowych na niezależne jednostki organizacyjne. Może tworzyć zasady grupowania AAA, kluczy DPSK, portali Hotspot, zasad Bonjour i portali WebAuth oraz przypisywać te grupy do dowolnej liczby stref. W różnych strefach mogą być wykorzystywane różne wersje oprogramowania oraz różne kody kraju.

Administratorzy mogą także niezależnie aktualizować strefy punktu dostępowego lub przełącznika z poziomu oprogramowania kontrolera i zarządzać punktami dostępowymi z oprogramowaniem w dowolnej z trzech ostatnich wersji. Dział IT może aktualizować oprogramowanie strefa po strefie lub w wydzielonej strefie testowej, zanim zostanie zaktualizowana cała sieć. Administratorzy mogą także grupować przełączniki w grupy, aby zaktualizować oprogramowanie w całej grupie lub monitorować grupę jako całość i np. rozpoznawać porty top talker w grupie.

Konfiguracja CLI przełącznika
Polecenia CLI (interfejs wiersza polecenia) do przełączników mogą być wydawane w trakcie zdalnej sesji CLI z danym przełącznikiem lub za pośrednictwem szablonów CLI, które narzucają grupie przełączników konfigurację CLI zgodnie z określonymi zasadami.

Obsługa wielu języków
Portale dostępne dla użytkownika końcowego i administratora sieci mogą działać w 10 językach, aby ułatwić ich obsługę na całym świecie. Dostępne są następujące języki: hiszpański, brazylijski portugalski, francuski, niemiecki, włoski, rosyjski, chiński uproszczony, chiński tradycyjny, koreański i japoński.

Podsłuch
Wszystkie kontrolery WLAN SmartZone umożliwiają podsłuch szyfrowanego ruchu w sieciach publicznych lub rządowych zgodnie z wymaganiami CALEA. Istnieje też możliwość kopiowania ruchu klienta do bramki podsłuchowej LIG (Lawful Intercept Gateway) przez L2oGRE (Soft-GRE).

ZABEZPIECZENIA I ZASADY

Filtrowanie URL
Filtrowanie URL na klientach bezprzewodowych umożliwia firmom tworzenie i egzekwowanie polityk chroniących użytkowników przed niestosownymi i szkodliwymi stronami internetowymi, zapewniając im zarazem dostęp do dozwolonych adresów URL. Polityki są stosowane na poziomie bezprzewodowej sieci LAN lub grupy użytkowników z opcjami pierwszeństwa przed listami dozwolonych i zakazanych. Rozbudowane pulpity umożliwiają wyświetlanie milionów dozwolonych lub zakazanych adresów URL, podzielonych na ponad 83 kategorii. Ponadto filtrowanie URL obsługuje funkcje bezpiecznej wyszukiwarki Google, YouTube i Bing.

Automatyczne wzmocnione zabezpieczenia klienta / DPSK
Opatentowany dynamiczny klucz PSKTM (DPSK) RUCKUS wzmacnia zabezpieczenie systemów klienckich, automatyzując losowy wybór kluczy hasła dla poszczególnych urządzeń. SmartZone obsługuje 50 000 kluczy DPSK, w tym do 25 000 w jednej strefie. Grupowy DPSK, hasło podane przez użytkownika i numeryczny klucz DPSK dodatkowo wzmacniają zabezpieczenie systemów klienckich we wszystkich sytuacjach.

Grupowy DPSK umożliwia działowi IT utworzenie DPSK, który będzie współużytkowany przez różne urządzenia, przy czym w danej strefie może być maksymalnie 500 grupowych DPSK. Administratorzy mogą ponadto określić numeryczny DPSK, dzięki któremu proces uzyskiwania dostępu dla gości lub w innych scenariuszach „łatwego dostępu" będzie bardziej przyjazny dla użytkownika.

Typ DPSK	Maks. w systemie	Maks. w domenie	Maks. w strefie	Uwagi
Nieprzypisane	50 000	25 000	500	Tylko nieprzypisane klucze DPSK w systemie
Przypisane	50 000	25 000	25 000	Tylko przypisane klucze DPSK w systemie
Grupa	50 000	25 000	500	Tylko klucze DPSK grupy w systemie
Kombinacja	50 000	25 000	25 000	Z zachowaniem powyższych limitów

Wykrywanie nieautoryzowanych punktów dostępowych WIDS / WIPS
SmartZone zawiera funkcję Wireless Intrusion Detection and Prevention System (WIDS/WIPS) umożliwiającą wykrywanie nieautoryzowanych punktów dostępowych. Na nieautoryzowane punkty dostępowe wykazujące szkodliwe zachowania jak spoofing SSID lub BSSID podłączonego punktu dostępowego RUCKUS nakładany jest zakaz podłączania systemów klienckich do sieci.

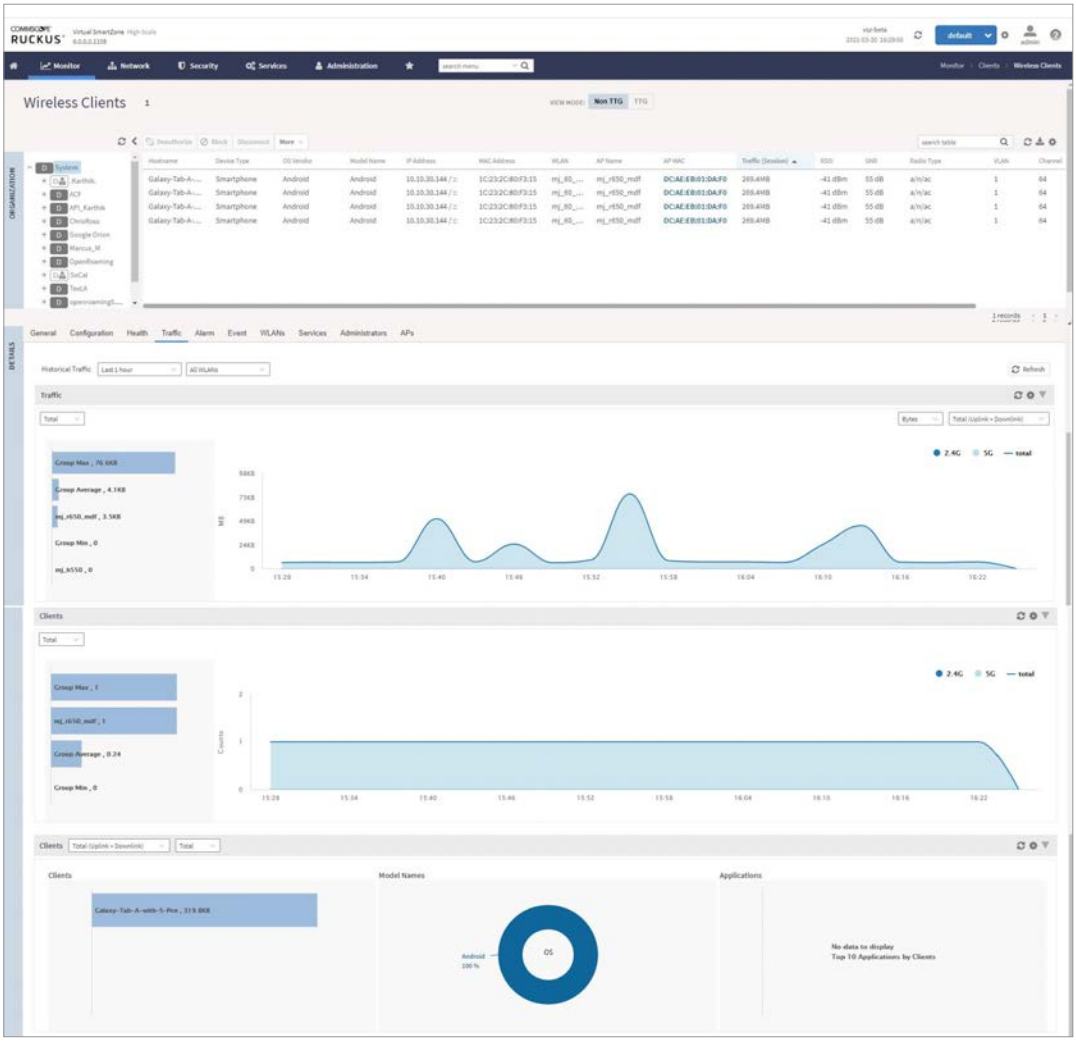
Punkty dostępowe mogą zostać sklasyfikowane jako Ignorowane, Znane, Nieautoryzowane lub Szkodliwe, aby zminimalizować zakłócenia w działaniu dozwolonych punktów dostępowych lub aparatury laboratoryjnej, a zatem nie wywoływać interwencji sieci wobec tych wykrytych punktów dostępowych. Reguły klasyfikacji umożliwiają wykrywanie nieautoryzowanych punktów dostępowych na podstawie porównania SSID, MAC OUI i progu RSSI.

Zarządzanie politykami oparte na rolach
Granularne polityki oparte na rolach dotyczące bezprzewodowych systemów klienckich umożliwiają tworzenie grup zasad w podziale na role użytkowników, domeny, lokalizacje, systemy operacyjne, statusy certyfikatu, VLAN i wiele innych czynników. Role są przypisywane w fazie uwierzytelniania onboardingu nowego użytkownika, a następnie do nich są przypisywane wymagane polityki OS i L3-7 oraz VLAN. Polityki mogą być egzekwowane za pomocą takich działań, jak zezwolenie, zakaz i limit prędkości na podstawie VLAN lub puli VLAN oraz list kontroli dostępu (ACL) L3/L4.

Hotspot 2.0 / Passpoint
SmartZone tworzy wydajną sieć zdolną do przyjmowania ruchu komórkowego użytkowników. Zarządzanie roamingiem opartym na hotspotach i Wi-Fi między własnymi i kompatybilnymi sieciami zewnętrznymi dzięki obsłudze HotSpot 2.0 Release 3 i zabezpieczeniu RadSec. Hotspot 2.0 działa automatycznie i nie wymaga interwencji użytkownika, o ile konfiguracja urządzenia została przeprowadzona poprawnie. Ponadto SmartZone spełnia wymagania inicjatywy Wi-Fi Google Orion. Samoobsługowa konfiguracja może być realizowana przez platformę zarządzania zabezpieczeniami i politykami RUCKUS Cloudpath®.

Lista zwolnionych z izolacji
Administratorzy mogą ręcznie dopisać do listy dozwolonych urządzenie bezprzewodowe, aby dodać urządzenia niepełniące funkcji bramy, jak drukarki, lub zezwolić na dodatkowe adresy MAC bramy, które mogą być wymagane do równoważenia obciążenia lub działania innych funkcji. Lista zwolnionych z izolacji może być tylko automatyczna, tylko ręczna lub ręczna i automatyczna.

Zarządzanie mDNS/Bonjour
Zjawisko burzy broadcastowej mDNS minimalizuje się przy użyciu zarządzania mDNS/Bonjour, które wykrywa usługi Bonjour (w tym AirPlay, Apple TV i inne usługi sieci Apple) i inne usługi oparte na mDNS, jak Chromecast, w sieciach VLAN i podsieciach, zarówno przewodowych, jak i bezprzewodowych. W SmartZone są domyślnie skonfigurowane typowe usługi Bonjour, dzięki czemu wykrywanie usług Bonjour odbywa się automatycznie.



Odgradzanie Bonjour umożliwia administratorom sterowanie fizycznym obszarem, w którym usługi oparte na Bonjour mogą być wykrywane. Jest to realizowane za pomocą mapowania na pobliskie punkty dostępowe, które ogłaszają usługi Bonjour, i zezwolenie tylko temu punktowi dostępowemu lub jego sąsiadom ogłaszanie rekordu Bonjour. Zapobiega to wykrywaniu przez użytkowników/urządzenia usług Bonjour, które nie znajdują się w pobliżu.

Uwierzytelnianie dwuskładnikowe

Zabezpieczenia SmartZone wzmacnia uwierzytelnianie dwuskładnikowe oznaczające, że administratorzy, wszyscy lub niektórzy, muszą podawać zarówno nazwę użytkownika i hasło, jak i kod wysłany w wiadomości SMS podczas logowania.

Obsługa Social Login

Administratorzy mogą podłączać urządzenia użytkowników w SmartZone, logując się za pomocą poświadczeń konta mediów społecznościowych. Obsługiwane są następujące popularne metody logowania do mediów społecznościowych: Facebook, Google, LinkedIn i Microsoft.

WYWIAD SIECIOWY

Analiza ruchu

Analiza ruchu pokazuje trendy ruchu i systemów klienckich w domenie, strefie, grupie punktów dostępowych i przełączników, WLAN i punkcie dostępowym w funkcji czasu. Pozwala to szybko znaleźć najbardziej obciążone punkty dostępowe, przełączniki lub porty oraz utworzyć ranking użytkowników sieci i urządzeń. W przypadku bezprzewodowych systemów klienckich wyświetlane jest zużycie zależnie od typu systemu operacyjnego i aplikacji. Statystyki mogą być filtrowane na podstawie pasma (2,4 GHz, 5 GHz lub oba) i kierunku ruchu (z sieci, do sieci lub oba). Ponadto monitorowana jest liczba systemów klienckich w funkcji czasu.

Mapy rozkładu pomieszczeń i terenu

Funkcja map pozwala na centralne wyświetlanie wszystkich lokalizacji równocześnie na Google Maps oraz wyświetlanie na mapie lokalizacji, rozkładów pomieszczeń i punktów dostępowych. Rutynowe badanie kondycji punktu dostępowego w poszczególnych lokalizacjach można wykonywać w prosty sposób za pomocą jednego kliknięcia. Na rozkładach pomieszczeń jest pokazane, które punkty dostępowe są online, oznakowane lub offline. Dane kondycji i ruchu poszczególnych punktów

dostępowych pozwalają oszacować wydajność lokalizacji. Administratorzy mogą poznać takie szczegóły, jak status kondycji, adres IP lub inne wskaźniki operacyjne, wskazując punkt dostępowy. Status punktu dostępowego jest sygnalizowany kolorystycznie, a administratorzy mogą nakładać na mapę dane operacyjne poszczególnych punktów dostępowych, jak używany kanał, ruch, liczba klientów oraz wykorzystanie łącza bezprzewodowego.

Kontrola i sterowanie aplikacjami w warstwie 7
Skuteczne rozpoznawanie aplikacji w warstwie 7 dla bezprzewodowych systemów klienckich pozwala sporządzić ranking aplikacji i użytkowników, który znajduje się wśród innych wskaźników. SmartZone umożliwia limitowanie prędkości, blokowanie i podejmowanie działań QoS zależnie od aplikacji, zgodnie z zasadami organizacji dotyczącymi korzystania z sieci. Baza danych sygnatur aplikacji jest aktualizowana niezależnie od aktualizacji oprogramowania SmartZone, aby administratorzy mogli zawsze kontrolować najnowsze aplikacje i zarządzać nimi.

Wskaźniki Super KPI
Korzystając ze wskaźników sieciowych („Super KPI"), dział IT może szybciej wykrywać potencjalne pogorszenie działania Wi-Fi u użytkownika oraz reagować na nie. SmartZone proaktywnie monitoruje podstawowy zestaw wskaźników, które są dobrze skorelowane z typowymi problemami, i wyświetla zbiorczy wskaźnik jako punkt wyjścia do rozwiązania problemu. Korzystanie ze zagregowanych miar, które są objawem szerokiego zakresu problemów związanych z siecią Wi-Fi, upraszcza diagnostykę dzięki zawężeniu zakresu i lokalizacji problemu. Do tych holistycznych, historycznych i inteligentnych wskaźników należą opóźnienie, wykorzystanie łącza bezprzewodowego i brak połączenia.

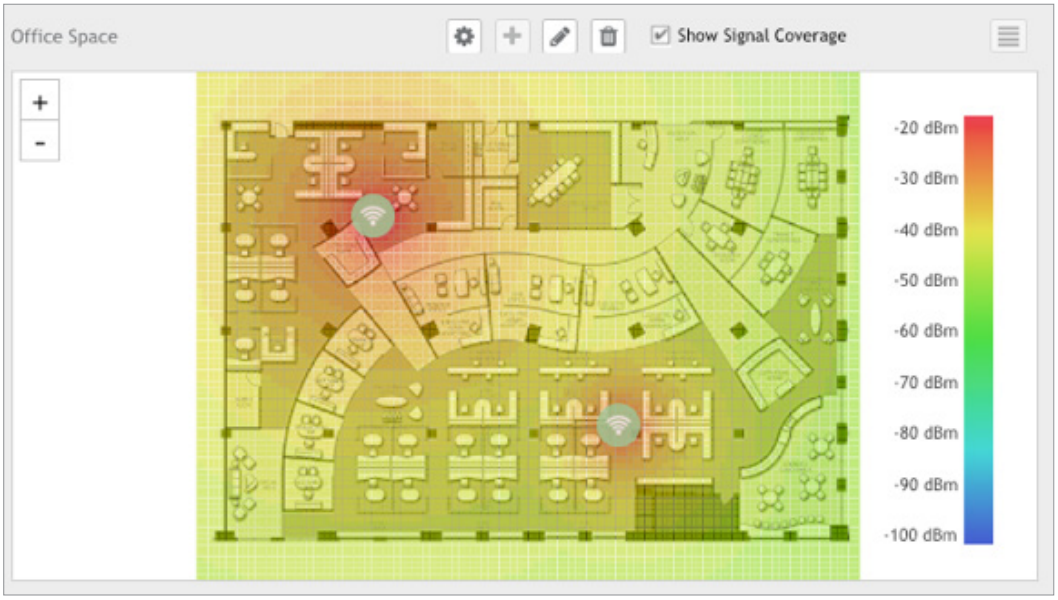
Mapa zasięgu sygnału radiowego
Na mapie zasięgu sygnału radiowego jest wizualnie pokazana przybliżona siła sygnału poszczególnych punktów dostępowych nałożona na zaimportowany rozkład pomieszczeń. Na tej podstawie dział IT może szybko dostrzec potencjalne przerwy w zasięgu punktów dostępowych w obsługiwanym obszarze.

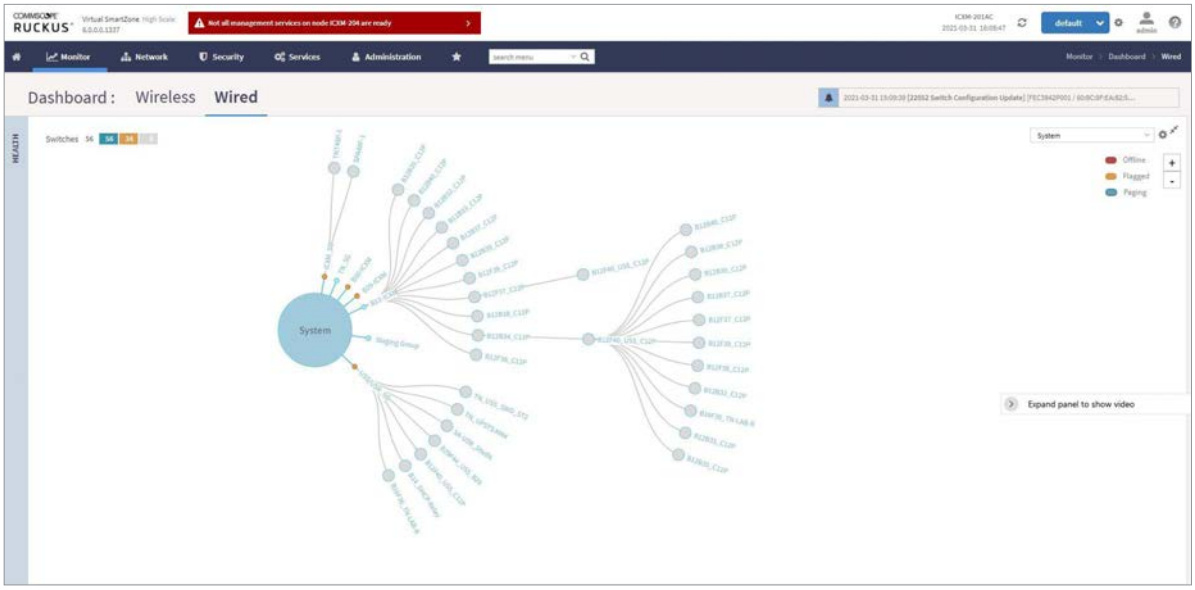
Kondycja punktu dostępowego i przełącznika
Kondycja punktu dostępowego to ważny wyznacznik jakości działania z punktu widzenia użytkownika. Dlatego w SmartZone ta informacja jest wyświetlana na pierwszym planie. Na pulpicie status punktu dostępowego jest klasyfikowany zależnie od progów kondycji/wydajności określonych przez administratora. Na mapie punkty dostępowe są wyświetlane w różnych kolorach zależnie od tego statusu. SmartZone automatycznie rozpoznaje punkty dostępowe wykraczające poza progi wydajności i sygnalizuje wizualnie najgorzej działające punkty dostępowe. Na podstawie tych danych i analizy historycznych trendów administratorzy mogą z łatwością porównać poszczególne punkty dostępowe z grupami punktów dostępowych, aby znajdować odseparowane miejsca problemów lub dostrzegać ogólniejsze wzorce.

Kondycja przełącznika polega na monitorowaniu trendów CPU i pamięci, statusu zasilacza i wentylatora oraz odczytów temperatury, a także ważnych zdarzeń i wywoływaniu alarmów zależnie od zaprogramowanych reguł.

Kondycja klastra
Poszczególne węzły klastra wyświetlane są na pulpicie w kolorze zielonym, żółtym lub czerwonym zależnie od statusu, co pozwala na monitorowanie i oznaczanie węzłów klastra i utrzymywanie na widoku ostrzeżeń o krytycznym stanie kondycji klastra. Ponadto wyświetlane są dane historyczne w formie wykresów liniowych i można określać progi kondycji klastra obejmujące wykorzystanie CPU, RAM i dysku oraz użycie portu/interfejsu i prędkości pakietów.

Kondycja systemu klienckiego
Wskaźniki wydajności systemów klienckich wraz ze stanem łączności i ruchem wyświetlane są w czasie rzeczywistym. Znajomość stosunku sygnału do szumu (SNR) oraz prędkości transmisji danych, a także historycznych danych ruchu, ułatwia diagnostykę problemów z połączeniem.

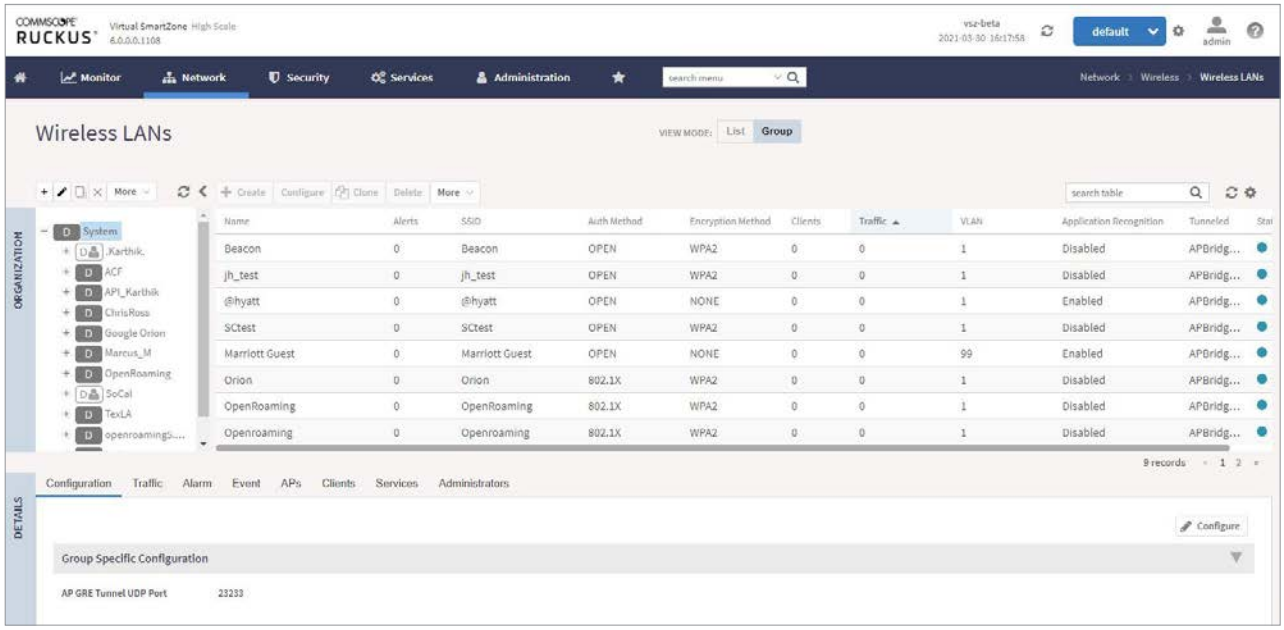




Kondycja topologii
Widok topologii i kuli na pulpicie jest oparty na hierarchii systemów, co ułatwia rozpoznawanie problemów z Wi-Fi w domenach, strefach i grupach punktów dostępowych. Sygnalizacja statusu kolorem zielonym, żółtym lub czerwonym umożliwia lokalizowanie punktów dostępu, które są offline lub gorzej działają.

Analiza widma
Analiza widma w czasie rzeczywistym na żądanie wykorzystuje urządzenia radiowe znajdujące się w punkcie dostępowym, dzięki czemu nie są potrzebne specjalne punkty dostępowe do raportowania widma. Widmo częstotliwości radiowych może być wizualizowane w formie energii w czasie rzeczywistym, wykorzystania w czasie rzeczywistym, gęstości, wykresu wodospadowego energii i wykresu wodospadowego wykorzystania. W czasie, gdy punkt dostępowy skanuje widmo, systemy klienckie są przełączane na pobliskie punkty dostępowe, aby zminimalizować zakłócenia połączeń. W przypadku punktu dostępowego z trzema modułami radiowymi 3. radio może przeprowadzać analizę widma w pasmach 2,4 i 5 GHz bez wpływu na połączenia systemu klienckiego. Analiza Widma jest obsługiwana w punktach dostępowych 802.11n, 802.11ac i Wi-Fi 6.

Generowanie i eksportowanie raportów
Dostępne są rozbudowane statystyki o abonentach (włącznie z odciskami palca systemu klienckiego), punktach dostępowych, SSID, przełącznikach, łączu dosyłowym (mesh) i samym klastrze SmartZone z dokładnością do trzech minut i okresu do 14 dni wstecz. Istnieje możliwość generowania raportów przedstawiających zmiany różnych wskaźniki KPI na przestrzeni pewnego okresu, od godzin do tygodni, i eksportowania ich w wielu formatach. Operatorom potrzebujących więcej informacji przyda się narzędzie analityczne RUCKUS SmartCell® Insight (SCI), które oferuje przechowywanie danych z dłuższego okresu, analizy danych i raporty o wyższym poziomie złożoności.



POŁĄCZENIA

Łącze dosyłowe sieci bezprzewodowej SmartMesh

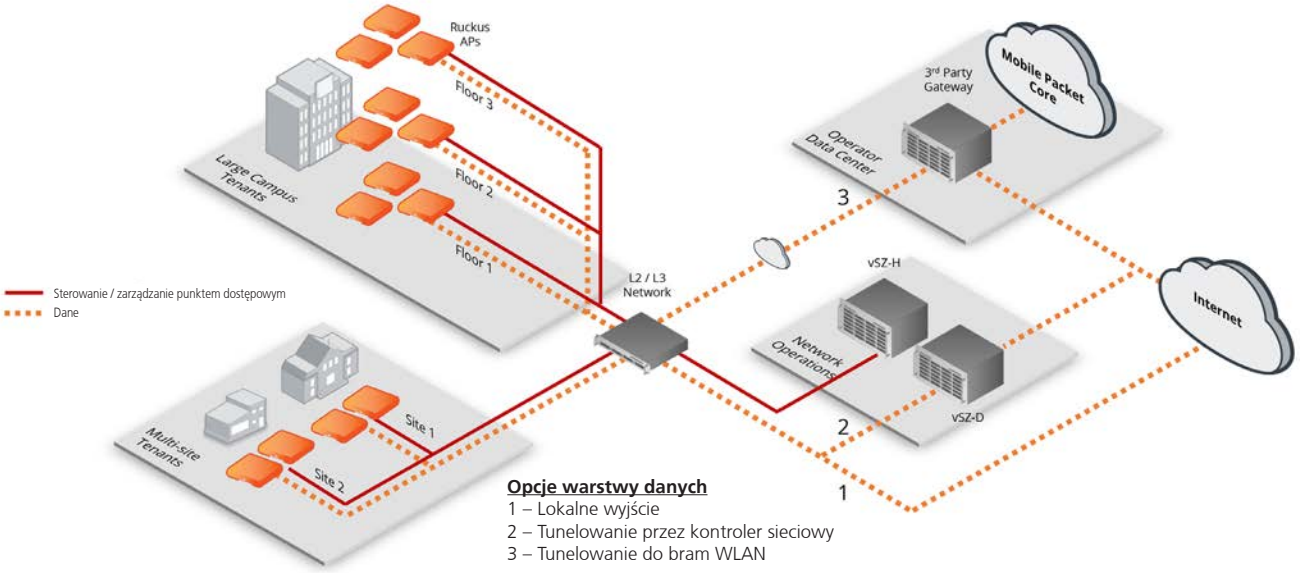
RUCKUS SmartMesh i bezdotykowa konfiguracja mesh upraszczają tworzenie nadmiarowego łącza dosyłowego sieci bezprzewodowej opartego na samoformujących i samoregenerujących się sieciach mesh, które można uaktywnić, zaznaczając pole wyboru w interfejsie administracyjnym, bez konieczności wstępnej konfiguracji punktu dostępowego. Korzystając z technologii BeamFlex®+, punkty dostępowe RUCKUS adaptują się do zmian warunków, aby jeszcze bardziej utrwalić połączenie mesh między punktami dostępowymi. Łącze dosyłowe ruchu punktu dostępowego zestawiane jest w paśmie 5 GHz do miejsca, w którym jest dostępna sieć przewodowa. Konfiguracja łącza dosyłowego mesh zmieniana jest dynamicznie, aby kierować ruch różnymi drogami zależnie od zmian warunków.

Optymalizacje połączeń

Punkty dostępowe pod kontrolą SmartZone wykrywają sąsiednie punkty dostępowe bezprzewodowo i tworzą zaszyfrowane kanały komunikacyjne do przekazywania informacji o obciążeniu sieci, kanałach roboczych i roamingu oraz innych ważnych parametrach komunikacji radiowej. Usprawnia to działanie routingu i równoważenia obciążenia w sieciach IPv4 i IPv6.

Optymalizacja komunikacji radiowej i Wi-Fi

- **BeamFlex+:** adaptacyjna antena BeamFlex+ zwiększa wydajność i zasięg każdego punktu dostępowego RUCKUS. W każdym punkcie dostępowym znajduje się wiele elementów anteny, które umożliwiają kształtowanie charakterystyki promieniowania w czasie rzeczywistym, aby zmaksymalizować, na poziomie każdego pakietu, wzmocnienie sygnału dochodzącego do poszczególnych systemów klienckich, dostosowując się jednocześnie do zmian ich ustawienia. Ta technologia łagodzi zakłócenia komunikacji radiowej, tłumi szumy negatywnie wpływające na wydajność i usprawnia działanie aplikacji, zwłaszcza na urządzeniach mobilnych.
- **ChannelFly®:** technologia dynamicznego zarządzania kanałami ChannelFly we wszystkich punktach dostępowych RUCKUS poprawia działanie komunikacji bezprzewodowej w bardzo zatłoczonych środowiskach, dynamicznie przełączając system kliencki na lepszy kanał, gdy działanie dotychczasowego zaczyna się pogarszać. Ta funkcja umożliwia wybór optymalnych kanałów 2,4 i 5 GHz punktów dostępowych, aby osiągnąć jak najlepszą wydajność i zminimalizować zakłócenia. ChannelFly obsługuje także wskaźnik kosztu zmiany kanału, który doskonali migrację kanału systemu klienckiego na podstawie modeli prognozowania pojemności kanału i aktualizacji początkowego czasu uczenia i ustalania.
- **Kontrola dostępu zależna od pojemności:** punkty dostępowe RUCKUS zawierają algorytm kontroli dostępu zależnej od pojemności, który ułatwia zapewnienie odpowiedniej jakości usług w okresach szczytowego obciążenia. Odrzuca on żądania połączenia od nowych systemów klienckich, jeśli groziłoby to pogorszeniem jakości usługi na już podłączonych systemach klienckich.
- **Adaptacyjne wymiarowanie komórki radiowej:** SmartZone poprawia wydajność w sieciach ze zbyt dużą lub zbyt małą liczbą zainstalowanych punktów dostępowych, dynamicznie powiększając lub pomniejszając komórki radiowe. Redukuje to zakłócenia kanałów wywoływane przez sąsiednie punkty dostępowe i zwiększa ogólną średnią przepustowość na system kliencki.
- **Adaptacyjne równoważenie obciążenia ruchu:** adaptacyjne równoważenie obciążenia pasm radiowych punktu dostępowego w czasie rzeczywistym jest sposobem na poprawę wydajności użytkownika i sieci w sytuacji, gdy czynniki otoczenia ulegają zmianie. Znające system kliencki uczenie maszynowe ponownie wykonuje kalibrację obciążenia na poziomie punktu dostępowego w paśmie 2,4 i 5 GHz.



ARCHITEKTURA

Oddzielne warstwy sterowania i danych

Na platformie SmartZone występujące w tradycyjnej architekturze WLAN problemy z wdrażaniem i opóźnieniem rozwiązano, stosując specjalną lokalną architekturę MAC, która umieszcza wszystkie istotne usługi WLAN, włącznie z żądaniami uwierzytelnienia i powiązania, w punkcie dostępowym RUCKUS. Dzięki temu wszystkie kontrolery SmartZone są w stanie odseparować ruch sterowania i zarządzania od ruchu danych, zarówno w przypadku użycia protokołów opartych na SSH, jak i na GRE, co przekłada się na poprawę elastyczności wdrażania i opóźnienia sieci.

Kontroler SmartZone umieszczony w scentralizowanym centrum danych może zarządzać wieloma zdalnymi lokalizacjami, nie wymuszając tunelowania wszystkich żądań uwierzytelnienia lub danych systemów klienckich przez kontroler SmartZone.

Ruch użytkowników przechodzi nad lokalną siecią L2/L3, co poprawia opóźnienie między systemami klienckimi a usługami. Umożliwia to także wdrożenia w oddziałach i bezpośrednią integrację między punktami dostępowymi a Active Directory, LDAP, RADIUS, DHCP, DNS i zaporami lokalnej infrastruktury IT.

Dane przesyłane w sieci publicznej, jak Internet, są szyfrowane w SmartZone.

Obsługa wielu warstw danych

Operatorzy mogą kierować ruch równocześnie do wielu dostawców usług zarządzanych i przedsiębiorstw niebędących hostem z jednego punktu dostępowego, aby zmaksymalizować wykorzystanie infrastruktury i zwrot z inwestycji.

W każdym punkcie dostępowym RUCKUS mogą być skonfigurowane równocześnie różne topologie routingu warstwy danych z możliwością użycia jednego tunelu RUCKUSGRE, maksymalnie trzech tuneli SoftGRE i lokalnego wyjścia danych w różnych kombinacjach.

Redundancja klastra active/active

Klastry kontrolery sieci active/active odznaczają się wyższą dostępnością i odpornością niż tradycyjna architektura rezerwy N+1 oraz zapewniają redundancję, równoważąc obciążenie punktów dostępowych i przełączników między kontrolerami tak, aby żaden kontroler nie pozostawał bezczynny.

Georedundancja klastra

Kontrolery SmartZone obsługują wiele warstw redundancji, aby zagwarantować przetrwanie WLAN nawet w przypadku katastrofalnych awarii sieci. Ponieważ klaster zawiera wiele węzłów kontrolera, w razie awarii kontrolera punkty dostępowe i przełączniki mogą zostać skojarzone z dowolnym kontrolerem, który zachowuje sprawność. Jeśli cały klaster znajdzie się off-line w centrum danych, możliwe jest przełączenie awaryjne punktów dostępowych i przełączników na inny klaster usytuowany w geograficznie odległym centrum danych, aby zapewnić przetrwanie sieci. Ponadto architektura klastra „wiele do jednego" sprzyja wysokiej dostępności, obniżając zarazem koszty redundantnego klastra, dzięki temu, że jeden klaster rezerwowy może służyć jako opcja przełączania awaryjnego dla wielu rozproszonych aktywnych klastrów.

Tylko: SZ300, vSZ-H

Zdolność przetrwania punktu dostępowego i przełącznika
SmartZone minimalizuje wpływ zerwania łączności między kontrolerem a punktem dostępowym lub przełącznikiem, umieszczając istotne usługi WLAN w samym punkcie dostępowym lub przełączniku. Przerwy w działaniu łącza WAN lub awarie kontrolera nie szkodzą normalnemu działaniu usług WLAN. Natywna obsługa WISPr na urządzeniach pod kontrolą SmartZone umożliwia dalsze uwierzytelnianie systemów klienckich w punktach dostępowych i przełącznikach nawet bez połączenia ze SmartZone.

Kopie zapasowe konfiguracji przełącznika
SmartZone na bieżąco tworzy kopię zapasową pliku konfiguracyjnego każdego przełącznika z zadaną częstotliwością i przechowuje siedem ostatnich wersji konfiguracji przełącznika. Administrator sieci ma dzięki temu pewność, że zawsze może przywrócić konfigurację o wypróbowanej poprawności, gdyby sieć nie zachowywała się zgodnie z oczekiwaniami po zmianie konfiguracji przełącznika.

Kontrola aktualizacji oprogramowania
Punkty dostępowe i przełączniki mogą być aktualizowane indywidualnie lub zbiorczo. Administratorzy mogą precyzyjnie kontrolować aktualizacje oprogramowania wbudowanego przełączników w całej zarządzanej sieci, zlecając ich natychmiastowe wykonanie lub odkładając je na później.

Wydzielenie usług DHCP/NAT
Usługi DHCP/NAT są realizowane przez punkt dostępowy lub, w dużych sieciach, przez oddzielny kontroler RUCKUS Virtual SmartZone Data Plane (vSZ-D). Rozdzielenie zarządzania punktami dostępowymi, które odbywa się w SmartZone, od routingu ruchu WLAN i zarządzania nim przez vSZ-D umożliwia operatorom szybkie replikowanie instalacji WLAN w wielu lokalizacjach bez ponoszenia wydatków związanych z zakupem nowych routerów i serwerów DHCP.

DHCP	Do 100 000 dzierżaw adresu IP na vSZ-D (w krokach co 1000 dzierżaw adresu IP)
NAT	Do 2 milionów przepływów sesji na vSZ-D (w krokach co 100 000 przepływów sesji)

Product information	
Products	• P01-S300-WW10: SmartZone 300 (SZ300)—redundant AC power, six (6) Fans, two (2) 10 Gbps data cards, and six (6) 1 GigE ports. No power cords included. • P01-S300-WW00: SmartZone 300 (SZ300)—redundant DC power, six (6) Fans, two (2) 10 Gbps data cards, and six (6) 1 GigE ports. Includes two DC power cables. • P01-S144-XX00: SmartZone 144 (SZ144)—four (4) 10 GigE and four (4) 1 GigE ports • L09-VSCG-WW00: Virtual SmartZone 3.0 or newer software virtual appliance, 1 instance, includes 1 AP license
Management Licenses	• L09-0001-SG00: Access Point management license for SZ144/vSZ 3.X, 1 RUCKUS AP access point • L09-0001-SGCX: Switch management license for SZ144/SZ300/vSZ 5.X, 1 RUCKUS ICX switch
Accessories and Spares	• 902-S310-AC00: KIT, SPARE, AC Power Supply, SZ300 (use with 902-1174-xx00 power cord) • 902-S301-DC00: KIT, SPARE, DC Power Supply, SZ300 • 902-S320-0000: KIT, SPARE, FAN ASSY, SZ300 (6 fans) • 902-S330-0000: KIT, SPARES, Slide Rail Rack Mount Kit, SmartZone 300 • 902-S340-0000: KIT, SPARE, Console Cable, (RJ45 to USB), SZ300 • 902-S350-0000: KIT, SPARE (FRU), Hard Disk Drive, SZ300 • 902-S351-0000: KIT, SPARE (FRU), Solid State Disk 64GB, SZ300 • L09-0001-RXGW: Soft GRE tunnel license from AP to 3rd party concentrator • L09-0001-SGHA: Per AP management license for High Availability. Supported products (Standby mode only): SZ-300, vSZ-H. For each AP on Standby Cluster only
URL Filtering	• S01-URL1-1LSZ: SmartZone URL Filtering 1 year subscription for 1 AP • S01-URL1-3LSZ: SmartZone URL Filtering 3 year subscription for 1 AP • S01-URL1-5LSZ: SmartZone URL Filtering 5 year subscription for 1 AP • S21-URL1-1LSZ: SmartZone URL Filtering 1 year subscription renewal for 1 AP • S21-URL1-3LSZ: SmartZone URL Filtering 3 year subscription renewal for 1 AP • S21-URL1-5LSZ: SmartZone URL Filtering 5 year subscription renewal for 1 AP

PLEASE NOTE: When ordering the AC power cord, you must specify the destination region by indicating -US, -EU, -CN, -IN, -JP, -KR, -SA, -UK or -UN instead of -XX.

Capacity	SZ300	VSZ-H	SZ144	VSZ-E
Managed APs	• Up to 10,000 per controller • Up to 30,000 per cluster	• Up to 10,000 per controller • Up to 30,000 per cluster	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 1,024 per controller • Up to 3,000 per cluster
Managed Switches*	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 2,000 per controller • Up to 6,000 per cluster	• Up to 400 per controller • Up to 1,200 per cluster	• Up to 200 per controller • Up to 600 per cluster
WLANs	• Up to 2,048 per zone • Up to 65,534 per cluster	• Up to 2,048 per zone • Up to 65,534 per cluster	• Up to 2,048 per cluster	• Up to 2,048 per cluster
VLANS	• Up to 4,094	• Up to 4,094	• Up to 4,094	• Up to 4,094
Concurrent Devices	• Up to 100,000 per vSZ-H • Up to 300,000 per vSZ-H cluster • Up to 150,000 per SZ300 • Up to 450,000 per SZ300 cluster	• Up to 100,000 per vSZ-H • Up to 300,000 per vSZ-H cluster • Up to 150,000 per SZ300 • Up to 450,000 per SZ300 cluster	• Up to 40,000 per controller • Up to 120,000 per cluster	• Up to 25,000 per controller • Up to 60,000 per cluster

* Each managed switch added to a cluster/controller reduces the capacity count for managed APs by 5.

Key functionality		
Device Management	• RUCKUS Wi-Fi APs supported: R850, R750, R730, R720, R710, R650, R610, R550, R510, R320, R310, M510, H510, H320, C110, E510, T811CM, T750, T710, T710S, T610, T610S, T504, T310, T301, FZM300, FZP300 • RUCKUS ICX 7000 series switches running FastIron 8.0.80 and above supported; FastIron 80.0.90a required for Zero-Touch Provisioning	
Device Type Support	• Wi-Fi APs, Switches	
Controller Expansion	• Up to 4 controllers in N+1 active-active mode, supporting non-disruptive capacity expansion	
Controller Redundancy	• 3+1 distributed data preserving with N+1 redundancy within a cluster	
Cluster Redundancy	• Geo-redundancy between clusters; many-to-one cluster support	
Data Offload	• Local offload of traffic directly to the Internet	
AP	• WPA, WPA2-AES, 802.11i, 802.1x/EAP, PSK, WISPr, WEP, WPA3, Enhanced Open, MAC Address* • Fast EAP-SIM re-authentication • EAP-SIM, EAP-AKA, EAP-AKA over WLAN for 802.1x • Wi-Fi Locations with the SZ AAA-Proxy functionality enabled	
User Database	• Internal database up to 25,000 users • External: RADIUS, LDAP, Active Directory	
Access Control	• L2 (MAC address-based)L3/4 (IP and Protocol based) • L2 client isolation • Management interface access control	• Time-based WLANs • Device type access policies • Two-factor authentication password, SMS
Wireless Intrusion Detection (WIDS/ WIPS)	• Rogue AP detection / prevention • Evil-twin/AP spoofing detection • Ad hoc detection	
AAA	• RADIUS (primary and backup)	
Hotspot	• WISPr, Wi-Fi CERTIFIED, Passpoint™, HotSpot 2.0*	
Guest Access	• Supported	
Captive Portal	• Supported	
Mesh	• Self-healing, Self-forming, Zero-touch provisioning	
DHCP Server	• Up to 100,000 IP address leases per vSZ-D (in increments of 1,000 IP address leases)	
NAT	• Up to 2 million sessions flows per vSZ-D (in increments of 100,000 session flows)	
Media	• 802.11e/WMM, U-APSD, Wi-Fi Calling Prioritization*	
mDNS Bonjour Fencing	• Supported	
WISPr	• WISPr authentication, SZ downlink AP Survivability*	
Software Queues	• Per traffic type (4), per client	
SmartCast Traffic Classification	• Automatic, heuristics and TOS based or VLAN-defined	
Rate Limiting	• Supported	
WLAN Prioritization	• Supported	
Client Load Balancing	• Automatic	
Band Load Balancing	• Supported	

* SmartZone controllers do not contain embedded radios or antennas

Key functionality *(continued)*		
AP Provisioning	• L3 or L2 auto-discovery • Auto-software upgrade • Automatic channel optimization	
Configuration Management	• Secure multi-operator login (RBAC) • Large scale (bulk) AP management tools • Switch software and firmware upgrades • Switch configuration management to be supported in an upcoming SmartZone release • Per zone firmware versioning control • Configuration audit trails	• Alarm and event notification (SNMP V1 / V2 / V3) • Event Logging (Syslog) • Integrated on-board remote accessible EMS functionality • RESTful APIs (JSON) • Web-UI • CLI

Physical characteristics		
Hypervisor Support for VSZ	• VMware 6.5, KVM CentOS 7.3 and above, Hyper-V Windows 2012 R2 and above, AWS, Azure, GCE	
Power	• Dual (redundant) AC or DC hot-swappable power supplies • DC power consumption: 1400W • Power Rating: -36 to -72VDC • AC power consumption: 1500W • Power Rating: 100-127VAC/200-240VAC, 47-63HZ • SZ144: AC power consumption: 250W	
Dimensions	• SZ300: 2RU rack mountable: 430 mm (W) x 518 mm (D) x 88.6 mm (H); 16.93 in (W) x 20.4 in (D) x 3.48 in (H) • SZ144: 1RU rack mountable: 438 mm (W) x 292.1 mm (D) x 44 mm (H); 17.25 in (W) x 11.5 in (D) x 1.73 in (H)	
Weight	• SZ300: 24.3 kg; 53.6 lbs • SZ144: 5 kg; 11.02 lbs	
Connections	SZ300 • Control, management, cluster ports • Six 10/100/1000 Mbps, RJ-45 ports • Data: Four 10Gbps data ports (SFP+) • Console ports: two RJ-45, one front, one rear • USB ports: two front, two rear • Serial port	SZ144 • 4 - 1GbE ports • 4 - 10GbE ports
SZ300 LED	• Front panel LEDs, one rear LED	
SZ300 Fans	• Six redundant, field-swappable fans in three sets	
Mean-Time-Between-Failure (MBTF)	SZ 300 at 25C: • AC version: 44126 hours • DC version: 39094 hours	SZ144 at 25C: • AC: 48649 hours • AC: w/ 10G 45818 hours
Environmental Conditions	SZ300 • Operating Temperature: 5°C (41°F) – 55°C (131°F)Operating Humidity: 5% to 85%, non-condensing • Humidity storage: 95%, non-condensing	SZ144 • Operating Temperature: 0°C (32°F) – 40°C (104°F) • Operating Humidity: 5% to 85%, non-condensing • Humidity storage: 95%, non-condensing

Regulatory/certifications		
EMC (for SZ144, SZ300)	• FCC/ICES-003-Emissions (USA/Canada) • CISPR 22-Emissions (International) • EN55022-Emissions (Europe) • EN55024-Immunity (Europe) • EN61000-3-2-Harmonics (Europe) • EN61000-3-3-Voltage flicker (Europe)	• CE-EMC Directive 89/336/EEC (Europe) • VCCI Emissions (Japan) • AS/NZS: CISPR 22 Emissions (Australia/New Zealand) • BSMI CNS13438 (Taiwan) • CCC Certification (China)
Safety (for SZ144, SZ300)	• UL60950-1/CSA 60950-1 (USA/Canada) • EN60950-1 (Europe) • IEC60950-1 (International), CB Certificate & Report including all international deviations • CE-Low Voltage Directive 73/23/EEE (Europe) • CCC Certification (China)	
Miscellaneous (for SZ144, SZ300)	• NEBS level 3 design	

CommScope przesuwa granice technologii komunikacyjnej przełomowymi pomysłami i odkryciami, które inspirują wspaniałe ludzkie osiągnięcia. Współpracujemy z klientami i partnerami w fazach projektowania, tworzenia i konstruowania najbardziej zaawansowanych sieci na świecie.
Z pasją i zaangażowaniem szukamy nowych możliwości kształtowania lepszego jutra.
Dowiedz się więcej na commscope.com

COMMSCOPE®

commscope.com

Więcej informacji można znaleźć na naszej stronie internetowej lub uzyskać od lokalnego przedstawiciela CommScope.

PA-114067.8-EN (07/21)