Ruckus
Simply Better Wireless.

Lösungsüberblick

Ruckus vSZ-D (Virtual SmartZone Data Plane)

VSZ-D – DIE VORZÜGE

Einführung

Mit der Virtual SmartZone Data Plane (vSZ-D) wird die Ruckus Virtual SmartZone-Plattform um ausgereifte Funktionen für die Datenebene erweitert, und zwar in einem virtualisierten Design, das getunnelte WLAN-Architekturen ermöglicht. Dieses branchenweit führende, wirklich differenzierte und herausragende Angebot überzeugt durch eine Architekturflexibilität, die sich in unternehmerischen Vorteilen in den unterschiedlichsten Anwendungsszenarien zeigt.

Ruckus vSZ-D (Virtual SmartZone Data Plane)

VSZ-D – die Vorzüge

Lösungsüberblick

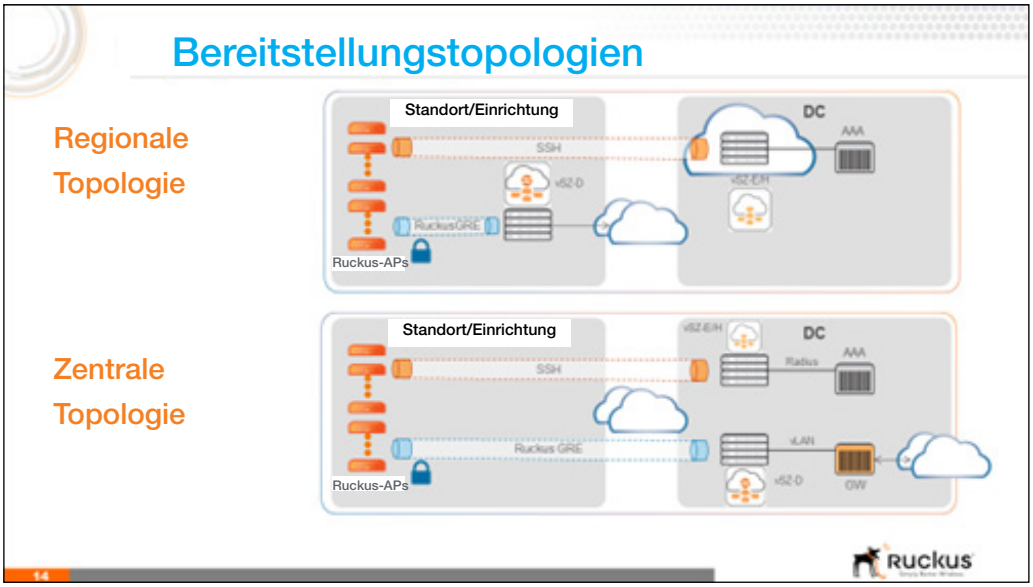

Abbildung 1: Beispiele der vSZ-D-Bereitstellung

vSZ-D wurde als ergänzende Lösung zur Verwaltung der Datenebene für Netzwerke konzipiert, die auf die Vorzüge des WLAN-Tunneling angewiesen sind. Die vSZ-Plattform sorgt für die Konfiguration und Überwachung der Ruckus-APs, und mit dem vSZ-D. A vSZ-Cluster lassen sich mehrere vSZ-D-Instanzen verwalten, die sich entweder am gleichen Standort befinden oder über mehrere Standorte verteilt sein können. Der Client-Datenverkehr von einem WLAN mit aktiviertem Tunneling wird sicher vom Ruckus-AP zur vSZ-D getunnelt, wodurch die Steuerung der gesicherten Datenströme vereinfacht und eine komplexe lokale Netzwerkverwaltung vermieden wird. Mit dem vSZ-D-Design gibt es jetzt eine Bereitstellungsflexibilität, die zuvor nicht möglich war.

Abbildung 1 zeigt ein Beispiel sowohl regionaler als auch zentraler vSZ-D-Bereitstellungsoptionen. Die regionale Topologie zeigt eine Architektur, bei der sich die vSZ an zentraler Stelle im Rechenzentrum befindet, während die vSZ-D dezentral an einem Ort je nach Bedarf bereitgestellt ist.

Dagegen zeigt die zentrale Topologie eine Architektur, bei der sich die vSZ und die vSZ-D am selben Standort in einem zentralen Rechenzentrum zur zentralen Datenaggregierung befinden (bzw. sind beide dort gehostet).

Features/Vorzüge von vSZ-D

vSZ-D ist ein Beispiel für eine NFV-konforme (Networks Functions Virtualization) Lösung, bei der die Funktionen der Datenebene vollständig von den Funktionen der Controllebene abgekoppelt sind. Dadurch entsteht eine hohe Bereitstellungsflexibilität, da diese NFV-Komponenten nicht mehr an physische Hardware oder denselben geografischen Standort gebunden sind. Die nachstehende Tabelle zeigt einige der Schlüsselfeatures der vSZ-D.

Feature	Vorzug
Sicheres Tunneling der Datenebene	Verwaltet die Schaffung von aggregiertem Benutzerdatenverkehr durch sichere Tunnel
Flexible und skalierbare Bereitstellungs-architekturen	Möglichkeit zur Verwaltung sowohl verteilter als auch zentraler Konfigurationen
Einfachheit bei Bereitstellung und Betrieb	Einfache Integration und Verwaltung mit vSZ-Plattforminstallationen
QoS- und Richtlinienkontrolle auf Standortebene	Verwaltung von Dienstrichtlinien und Datenstream-QoS

[1]Wird in einem Release nach Version 1 unterstützt

Ruckus vSZ-D (Virtual SmartZone Data Plane)

VSZ-D – die Vorzüge

Anwendungsfälle

Nicht der gesamte WiFi-Traffic muss innerhalb des Netzwerks getunnelt werden. Ein großer Teil der Daten wird ganz ohne Aggregierung oder Verschlüsselung im lokalen Netzwerk übertragen und von diesem Standort aus unmittelbar in das Internet geroutet.

Es gibt jedoch einige Fälle, in denen das Tunneln der Benutzerdaten unerlässlich sein kann.

Fall 1: Wireless VoIP und Videodienste

Der Netzwerk-VoIP-Traffic wird oftmals zu einem PBX-System zurückgelenkt, das sich in einem anderen Subnetz innerhalb des Netzwerks befindet. In einem derartigen Fall lässt sich der Sprachdatenverkehr besser über die vSZ-D-Funktionen zur Datentunnelung und -aggregierung verwalten, bei denen er sicher das Netzwerk durchlaufen und unter Wahrung entsprechender QoS-Prioritäten transparent die Layer-2-Subnetzgrenzen überwinden kann.

Fall 2: Wireless-Dienste für Gäste in Gastronomie/Gastgewerbe und anderen Unternehmen

Für Unternehmen, die ihren Gästen WiFi-/Internet-Dienste anbieten, ist die Tunnelung der Benutzerdaten aus Sicherheitsgründen sinnvoll. Mit einem Produkt wie vSZ-D lässt sich die Verwaltung dieser Daten in einem Netzwerk vereinfachen, indem sie logisch separiert und gegenüber dem Firmendatenverkehr abgesichert werden und ein Controlling sämtlicher Netzwerkressourcen möglich ist, auf die von dieser Benutzerklasse zugegriffen werden kann.

Fall 3: Verwaltung von IoT-Datenverkehr

Eine wachsende Klasse der Netzwerkdaten gehört zu den neuen IoT-Geräten (Internet of Things). Dabei handelt es sich üblicherweise um intelligente Netzwerkknoten, die zur Zustandsüberwachung von Ausrüstung (Heizung/Klimaanlage, Türen/Fenster als Gebäudezugang, Position wertvoller Ausrüstungsteile oder Video-/Datenstreams für Sicherheitssysteme) verwendet werden. Diese Daten werden typischerweise zu einem Überwachungszentrum zurückgeleitet, wo sie analysiert und archiviert werden. Diese Klasse von Informationen ist oftmals operationskritisch und unterliegt Zugriffsbeschränkungen. Mittlerweile wird WiFi als Backhaul für diese IoT-Geräte genutzt, und mit der Verfügbarkeit einer vSZ-D vereinfacht sich die Partitionierung und Priorisierung dieses Traffics unabhängig vom sonstigen Internet-Datenverkehr.

Fall 4: Minimieren der Skalierungskosten

Zur Bereitstellung und Verwaltung eines verteilten Netzwerks oder gar einer Vielzahl derartiger Netzwerke ist die Replikation von Ressourcen oftmals unerlässlich. An jedem verwalteten Standort, wo Daten getunnelt werden müssen, ist üblicherweise Controller-Hardware in mehrfacher Ausführung erforderlich. Mit zunehmender Größe und Anzahl der Standorte kann das schnell zu einer extrem teuren Angelegenheit werden. Wird dagegen eine virtuelle Controller-Plattform an zentraler Stelle installiert, können an den verwalteten Standorten, an denen eventuell eine Tunnelung des WiFi-Traffics erforderlich ist, preisgünstige vSZ-D-Lösungen bereitgestellt werden, die auf standardmäßiger COTS-Hardware ausgeführt werden. Mit vSZ-D von Ruckus lassen sich jetzt diese Bereitstellungstypen vereinfachen, und was noch wichtiger ist: mit deutlich geringeren CAPEX-Kosten.

Einfache und flexible Bereitstellung

Aus Sicht der Bereitstellung stand bei der Konzeption von vSZ-D das Prinzip eines minimalen Konfigurationsaufwands im Mittelpunkt.

Die Unterstützung von vSZ-D setzt Version 3.2 der vSZ-Controller-Plattformen voraus. Ab diesem Ausgangspunkt umfasst die Bereitstellung zwei unkomplizierte manuelle Schritte:

1. das Installieren von vSZ-D auf dem Ziel-VM-System und das Konfigurieren für das "Hosting" der vSZ-Plattform.
2. Bei entsprechender Aufforderung in der vSZ-Benutzeroberfläche kann der Betreiber die vSZ-D autorisieren, die Verknüpfung mit dem jeweiligen Netzwerk herzustellen.

Die gesamte sonstige Installationssequenz läuft automatisch ab. Die Verwaltung und Überwachung der vSZ-D erfolgen über die vSZ-Benutzeroberfläche.

Da vSZ-D virtualisiert ist, wird die Skalierung des Netzwerks zu einer einfachen Angelegenheit: Es muss lediglich die Bereitstellung auf der richtigen Hardware-Plattform erfolgen bzw. es muss eine zusätzliche Instanz an einem neuen Standort oder im Rechenzentrum hinzugefügt und diese mit der zentralen vSZ-Plattform verknüpft werden.

Zusammenfassung

vSZ-D bietet eine neue, bisher nicht gekannte Flexibilität, wenn es um die Schaffung eines flexiblen Netzwerks zur sicheren Tunnelung des Benutzerdatenverkehrs, die Vereinfachung des IT-Aufwands und die Senkung der TCO/CAPEX-Kosten geht. Dieses Produkt ergänzt die Palette der Tools von Ruckus, die WiFi einfach besser machen.

Sie möchten mehr über Ruckus vSZ-D erfahren? Fordern Sie bei Ihrem lokalen oder regionalen autorisierten Vertriebspartner für Ruckus-Produkte weitere Informationen an.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
+1 (650) 265-4200 Tel. \ +1 (408) 738-2065 Fax

Ruckus
Simply Better Wireless.
www.ruckuswireless.com