



Présentation de la solution

Ruckus vSZ-D (Virtual SmartZone Data Plane)

VSZ-D - LES AVANTAGES

Introduction

Avec Virtual SmartZone Data Plane (vSZ-D), la plateforme Virtual SmartZone de Ruckus déploie des capacités de plan de données sophistiquées dans une conception virtualisée qui prend en charge les architectures WLAN tunnelisées. Il s'agit d'une offre véritablement unique en son genre dans le secteur. Elle propose une flexibilité d'architecture remarquable qui confère des avantages considérables sur plusieurs scénarios de déploiement.

Ruckus vSZ-D (Virtual SmartZone Data Plane)

vSZ-D - Les avantages

Présentation de la solution

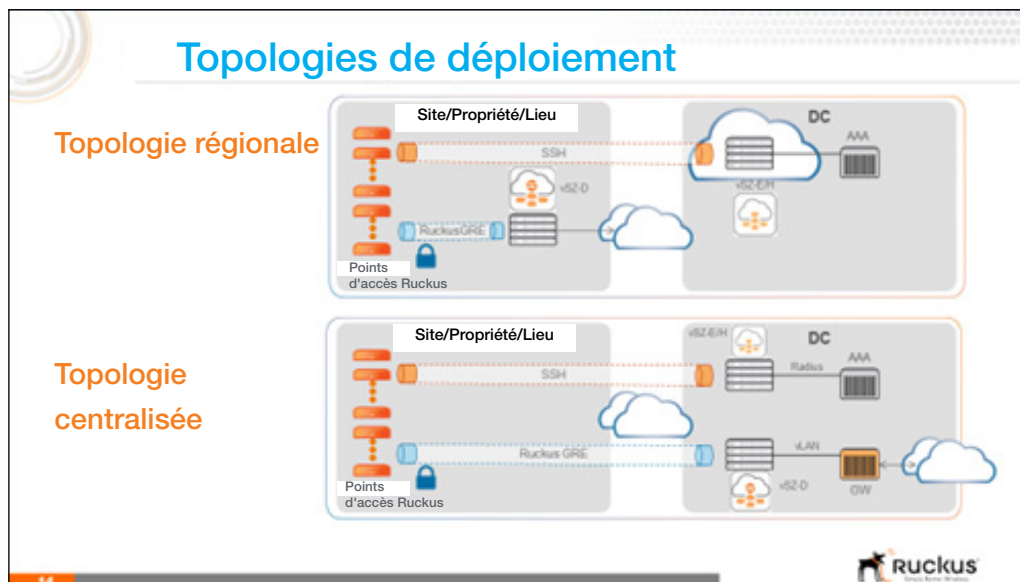


Figure 1 - Exemples de déploiements vSZ-D

vSZ-D est une solution de gestion de plan de données complémentaire pour les réseaux qui souhaitent tirer profit des avantages associés à la tunnelisation WLAN. La plateforme vSZ fournit configuration et surveillance pour les points d'accès Ruckus et le vSZ-D. Un cluster vSZ peut gérer plusieurs instances de vSZ-D qui partagent un site ou qui sont distribuées sur plusieurs sites. Le trafic de données client d'un réseau WLAN dont la tunnelisation est activée sera acheminé de manière sécurisée du point d'accès Ruckus au vSZ-D. Le contrôle des flux de données sécurisés en est ainsi simplifié et cela permet d'éviter la complexe gestion du réseau local. De par sa conception, le vSZ-D offre une flexibilité de déploiement qui n'existait pas auparavant.

La figure 1 montre un exemple d'options de déploiement régional et centralisé du vSZ-D. La topologie régionale met en évidence une architecture dans laquelle le vSZ est centralisé dans le centre de données, tandis que le vSZ-D est déployé à distance sur site de manière sélective, là où il est requis.

La topologie centralisée montre une architecture dans laquelle le vSZ et le vSZ-D partagent le même site dans un centre de données centralisé pour l'agrégation des données.

Fonctionnalités/avantages du vSZ-D

Le vSZ-D est un exemple de solution compatible NFV dont les fonctions de plan de données sont complètement découplées de la fonction de plan de contrôle. On obtient ainsi une flexibilité de déploiement étant donné que ces composants NFV ne sont plus dépendants de l'emplacement matériel ou géographique physique. Le tableau ci-dessous montre quelques fonctionnalités clés du vSZ-D

Produit	Avantage
Tunnelisation de plan de données sécurisée	Gère la création du trafic de données utilisateur via des tunnels sécurisés
Architecture de déploiement flexible et évolutive	Capacité à maintenir les configurations réseau distribuées et centralisées
Simplicité de déploiement et de fonctionnement	Intégration et gestion simples avec les installations de la plateforme vSZ
Qualité de service et contrôle de politique au niveau du site	Gestion de la politique de service et qualité de service des flux de données

¹ Sera pris en charge dans les versions qui suivent la version 1

Ruckus vSZ-D (Virtual SmartZone Data Plane)

vSZ-D - Les avantages

Cas d'utilisation

Le trafic WiFi n'a pas toujours besoin d'être tunnelisé au sein du réseau. Une grande partie des données est transmise sur le réseau local sans agrégation ou chiffrement et est acheminée directement vers Internet depuis ce site.

Dans certains cas, toutefois, la tunnelisation des données utilisateurs est indispensable.

Cas 1 : Service VoIP et vidéo sans fil

Le trafic VoIP d'un réseau est souvent redirigé vers un système PBX situé dans un sous-réseau différent au sein du réseau. Dans ce cas, le trafic vocal doit être géré via les capacités de tunnelisation et d'agrégation de données de vSZ-D. Il est ainsi acheminé à travers le réseau puis traverse les limites de sous-réseaux (couche 2) en conservant les priorités de qualité de service appropriées.

Cas 2 : Services sans fil invités dans l'hôtellerie et autres secteurs

Pour les entreprises qui fournissent un service WiFi/Internet, la tunnelisation des données utilisateur est logique du point de vue de la sécurité. Un produit tel que vSZ-D simplifie la gestion de ces données sur un réseau en les séparant logiquement du trafic de l'entreprise et en contrôlant toutes les ressources du réseau auxquelles cette classe d'utilisateurs a accès.

Cas 3 : Gestion du trafic IoT

De plus en plus de données réseau sont associées aux appareils IoT (Internet des objets). Il s'agit de nœuds de réseau généralement intelligents qui sont utilisés pour surveiller l'état de l'équipement (chauffage/air conditionné, portes/fenêtres pour l'accès au bâtiment, emplacement d'équipement onéreux ou flux de données vidéo/audio de l'équipement de sécurité). Ces informations sont généralement renvoyées à un centre de surveillance où elles sont analysées et archivées. Cette classe d'informations est souvent d'une importance critique et est soumise à des restrictions d'accès. Le WiFi est à présent utilisé comme relais pour ces appareils IoT et le vSZ-D simplifie le partitionnement et la hiérarchisation de ce trafic indépendamment de l'autre trafic de données Internet.

Cas 4 : Minimisation des coûts liés à l'évolutivité

Pour déployer et gérer un réseau distribué ou plusieurs réseaux du même type, il est souvent nécessaire de procéder à une répllication des ressources. Un matériel de contrôleur divers est généralement nécessaire à chaque site où la tunnelisation des données est requise. À mesure que la taille et les nombre de sites augmentent, cette opération peut rapidement s'avérer extrêmement onéreuse. Si une plateforme de contrôleur virtuel est installée à un emplacement central, des solutions vSZ-D peu coûteuses et fonctionnant sur un matériel COTS standard peuvent être déployées dans les sites gérés où la tunnelisation du trafic WiFi peut être nécessaire. Ruckus vSZ-D peut désormais simplifier ces types de déploiements à des coûts d'exploitation considérablement inférieurs.

Déploiement simple et flexible

Du point de vue du déploiement, le vSZ-D a été conçu sur les principes d'une configuration minimale.

La prise en charge de vSZ-D nécessite des plateformes de contrôleur Ruckus vSZ de la version 3.2. De là, le déploiement se fait en deux étapes manuelles simples :

1. L'installation du vSZ-D sur la machine virtuelle cible et sa configuration de sorte à pointer vers la plateforme vSZ qui l'héberge.
2. À l'invitation de l'interface utilisateur du vSZ, l'opérateur peut autoriser le vSZ-D à s'associer à ce réseau.

Le reste de la séquence d'installation est automatique. La gestion et la surveillance du vSZ-D sont effectuées à l'interface du vSZ.

Vu que le vSZ-D est virtualisé, l'évolutivité du réseau consiste tout simplement à effectuer le déploiement sur la bonne plateforme matérielle ou à ajouter une instance supplémentaire à un nouveau site ou au centre de données et à l'associer à la plateforme vSZ centrale.

SOMMAIRE

vSZ-D offre une flexibilité inédite qui consiste à construire un réseau flexible afin de tunneliser le trafic de données utilisateur de manière sécurisée, simplifier les dépenses du service informatique et réduire les coûts d'exploitation et le coût total de propriété. Ce produit est un autre outil Ruckus qui vous propose un « WiFi tout simplement meilleur ».

Vous souhaitez en savoir plus sur Ruckus vSZ-D ? Contactez votre revendeur local ou régional Ruckus autorisé pour plus d'informations.