Chapitre 1

Analyse et spécification des besoins

Introduction

Ce chapitre se concentre sur l'analyse et la spécification des besoins, en distinguant entre les besoins fonctionnels et non fonctionnels. Nous procéderons ensuite à une étude comparative des solutions SD-WAN pour choisir la plus adaptée.

1.1 Les besoins fonctionnels et non fonctionnels

1.1.1 Les besoins fonctionnels

Routage intelligent

Le routage intelligent représente la capacité d'un système à diriger le trafic de manière dynamique et efficace en fonction des exigences de performance et des politiques définies. Dans le contexte des réseaux SD-WAN, plusieurs protocoles de routage sont utilisés. Parmi eux, le BGP (Border Gateway Protocol) est un protocole de routage largement utilisé pour échanger des informations de routage entre différents systèmes autonomes (AS) sur Internet. Dans un environnement SD-WAN, le BGP facilite l'échange de routes entre les sites distants et le centre de données centralisé, assurant ainsi une connectivité fiable et dynamique.

De plus, l'OSPF (Open Shortest Path First) est un protocole de routage intérieur beaucoup utilisé dans les réseaux d'entreprise pour calculer les chemins les plus courts entre les routeurs. Dans un déploiement SD-WAN, l'OSPF peut être utilisé pour optimiser la connectivité entre les différents sites distants et les nœuds du réseau SD-WAN.

Optimisation du trafic

Il y'avait de nombreuses solutions qui ont été proposées pour transporter plus de trafic et soutenir un partage équitable, l'idée la plus importante est de définir des priorités pour différents types de trafic. Dans SDWAN, le trafic est classé en trois catégories , on parle du trafic interactif, élastique et de fond, en fonction des caractéristiques des services qui les

génèrent. Prenons l'exemple des requêtes et des réponses dans les moteurs de recherche, ils sont considérées comme du trafic interactif puisque il sont très sensibles à la perte de paquets et aux retards, et elles devraient être planifiées avec la plus haute priorité .

SDWAN permet au trafic interactif de préempter la bande passante. Il est envoyé dès que possible, alors que, pour les autres types de trafic, tels que le trafic élastique et de fond, SDWAN calcule la quantité de trafic que chaque service peut envoyer et configure le plan de données du réseau pour transporter ce trafic tout en tenant compte de l'équité entre services similaires.

Par cet méthode , SDWAN peut optimiser la bande passante et prioriser les applications critiques pour garantir une expérience utilisateur optimale.

Gestion centralisée

La gestion centralisée dans un réseau SD-WAN offre aux administrateurs la possibilité de contrôler tous les aspects du réseau à partir d'une seule interface centralisée. Cela inclut la configuration des appareils, la définition des politiques de sécurité, la surveillance des performances du réseau, la gestion de la bande passante, et bien plus encore.

Grâce à cette approche centralisée, les administrateurs peuvent effectuer des tâches de gestion de manière efficace et cohérente sur l'ensemble du réseau, ce qui simplifie les opérations et garantit une visibilité globale sur l'état du réseau.

Sécurité avancée

La sécurité avancée dans SD-WAN implique l'intégration de plusieurs fonctionnalités de sécurité pour protéger le trafic réseau contre les menaces potentielles. Cela inclut le chiffrement des données qui est un élément essentiel pour garantir la confidentialité des informations transitant à travers le réseau SD-WAN. Les pare-feu intégrés filtrent et contrôlent le trafic en fonction de règles prédéfinies, bloquant les communications non autorisées et détectant les tentatives d'intrusion.

De plus, les IDS/IPS assurent la détection des menaces en utilisant des technologies

avancées telles que l'apprentissage automatique et l'analyse comportementale pour identifier les activités malveillantes ou suspectes sur le réseau, y compris la détection des logiciels malveillants et des attaques par déni de service distribué (DDoS).

Enfin, l'intégration d'un SIG, qui est une passerelle Internet sécurisée, permet de centraliser et de consolider les fonctions de sécurité au niveau de la connectivité Internet. Cela permet de filtrer le trafic Internet avant qu'il n'atteigne les sites distants, réduisant ainsi la surface d'attaque et améliorant la sécurité globale du réseau.

La segmentation

La segmentation réseau divise un réseau en plusieurs segments ou sous-réseaux,comme montre la figure . Elle permet d'améliorer la surveillance et le contrôle du réseau grâce à des politiques. Elle offre aussi la possibilité d'améliorer les aspects de sécurité , en empêchant l'accès simultané à l'ensemble des ressources. Par conséquent, en cas d'intrusion, seule la partie des ressources exposée à l'attaque sera compromise, alors que le reste des ressources restera sécurisé.

FIGURE 1.1 – La ségmentation dans SD-WAN

Haute disponibilité

Parmi les mécanismes de redondance et de basculement pour garantir la disponibilité continue des services, même en cas de panne de lien ou de périphérique dans le réseau, on trouve la redondance des liens, qui implique la mise en place de plusieurs connexions réseau pour un même point d'accès.

De plus, la redondance des périphériques consiste à disposer de plusieurs équipements réseau configurés pour prendre le relais en cas de défaillance d'un périphérique principal. Les protocoles de basculement automatique, tels que HSRP, VRRP ou FHRP, permettent une transition transparente vers les équipements de secours en cas de défaillance.

Le load balancing peut aussi être utilisé pour répartir le trafic entre plusieurs

équipements ou liens réseau redondants, améliorant ainsi les performances de l'application en optimisant l'agrégation, l'accélération et le déchargement.

Ainsi, en cas de défaillance d'un équipement ou d'un lien, le trafic peut être automatiquement redirigé vers d'autres ressources disponibles, assurant ainsi la continuité du service sans interruption pour les utilisateurs finaux.

Évolutivité

la gestion centralisée facilite l'extension du réseau SD-WAN en permettant l'ajout de nouveaux sites et appareils de manière transparente. Les administrateurs peuvent facilement provisionner de nouveaux équipements, mettre à jour des configurations et adapter le réseau aux besoins changeants de l'entreprise, le tout à partir d'une interface centralisée.

1.1.2 Les besoins non fonctionnels

Performance

SD-WAN est capable de fournir des performances optimales en termes de débit, Garantir des temps de réponse rapides et une faible latence pour les applications critiques afin de garantir une expérience utilisateur satisfaisante pour les applications et les services hébergés sur le réseau. Fiabilité : Assurer une disponibilité élevée du réseau et des applications, avec des mécanismes de redondance et de récupération en cas de défaillance.

Coût

Le SD-WAN offre une rentabilité accrue en minimisant les dépenses liées à l'exploitation et à la maintenance, tout en améliorant l'efficacité opérationnelle.

Contrairement aux technologies traditionnelles qui exigent souvent des déplacements sur site pour l'installation de nouvelles configurations et mises à jour, le SD-WAN permet

des déploiements à distance, réduisant ainsi les coûts associés à la main-d'œuvre et aux déplacements.

Interopérabilité

Le SD-WAN est compatible avec les infrastructures et les systèmes existants de l'entreprise .Cette compatibilité permet une intégration harmonieuse du SD-WAN avec les équipements réseau existants, tels que les routeurs, les commutateurs et les pare-feu, ainsi qu'avec les applications et les services cloud utilisés par l'entreprise et c'est grâce a cette interopérabilité, les entreprises peuvent bénéficier des avantages du SD-WAN tout en minimisant les perturbations et les coûts associés à la transition vers cette technologie.

1.2 Étude comparative et choix de la solution SD-WAN

1.2.1 Étude comparative

TABLE 1.1 – Tableau comparatif

	Cisco	Fortinet	Silver Peak	Versa
La plateforme prend en charge à la fois le routage classique et le SD-WAN.	-Services de routage classiques complets. - Migration fluide et intégration harmonieuse des fonctionnalités SD-WAN avec le routage classique sur une même plateforme.	-Le déploiement d'un SD-WAN n'implique ni l'ajout de composants supplémentaires ni la nécessité de modifier votre infrastructure existante.	-Migration sans protection des investissements. -fonctionnalités classiques de routage restreintes sur la même plateforme SD-WAN.	- L'utilisation d'un SD-WAN nécessite l'ajout de matériel.
Architecture SD-WAN personnalisée	- Les composants dédiés à l'évolutivité et aux performances, répartis entre les plans de contrôle, de données et de gestion, fournissent une architecture compatible avec SDN. -Flexibilité pour ajuster l'architecture à l'objectif de l'entreprise. - le déploiement dans le cloud est pris en charge et géré par l'équipe Cisco Cloud Ops.	- Ancienne infrastructure reposant sur un pare-feu.	- Ancienne infrastructure combinant les plans de contrôle et de données.	- Des composants spécialisés pour le contrôle, les données et la gestion.

Modèle de politique évolutif	-La sélection dynamique des chemins permet aux applications critiques d'éviter automatiquement les problèmes de réseau. - la microsegmentation et la gestion des politiques basée sur l'identité facilitent l'application cohérente de politiques multisites pour assurer une expérience utilisateur uniforme.	- La gestion séparée des politiques pour le SD-WAN et le pare-feu complique l'ingénierie du trafic et la transmission de politiques centralisées pour les plans de contrôle et de données.	-Bien que les politiques puissent être créées et réutilisées pour répondre aux besoins de l'entreprise, la microsegmentation et l'application de politiques multidomaines sont restreintes.	Bien qu'il soit possible d'effectuer l'ingénierie du trafic en fonction de politiques sensibles aux applications, l'application de politiques multidomaines est restreinte.
AAAAAAA	BBBBBBB			
5) Nez en l'air	6) Sur le dos			

1.2.2 Choix de la solution SD-WAN

Le choix de la solution dépend de quatre éléments essentiels ,l'infrastructure réseau, la sécurité réseau, l'intégration cloud et la périphérie du réseau.

L'infrastructure réseau

La plateforme Cisco offre une solution complète en prenant en charge à la fois le routage classique et le SD-WAN, offrant ainsi une flexibilité et une évolutivité optimales pour les entreprises. Elle propose des services de routage classiques complets, ce qui garantit une transition fluide et une intégration harmonieuse des fonctionnalités SD-WAN avec le routage traditionnel sur une même plateforme.

De plus, le déploiement d'un SD-WAN avec Cisco n'implique ni l'ajout de composants supplémentaires ni la nécessité de modifier l'infrastructure existante, ce qui réduit les coûts

et simplifie le processus. Par contre, d'autres solutions comme Fortinet, Silver Peak et Versa peuvent présenter des limitations telles que des fonctionnalités de routage restreintes sur la même plateforme SD-WAN ou la nécessité d'ajouter du matériel pour utiliser le SD-WAN, ce qui peut rendre la migration moins fluide et moins rentable. Ainsi, la simplicité et l'intégration transparente font de Cisco une option supérieure pour les entreprises cherchant à adopter le SD-WAN.

La force de Cisco réside dans sa capacité à offrir une architecture SD-WAN personnalisée. Avec des composants dédiés à l'évolutivité et aux performances répartis entre les plans de contrôle, de données et de gestion, Cisco assure une compatibilité avec les principes du SDN. Cette approche permet d'ajuster facilement l'architecture en fonction des objectifs de l'entreprise. De plus, Cisco propose une prise en charge complète du déploiement dans le cloud, avec une gestion assurée par l'équipe experte de Cisco Cloud Ops. Comparé avec d'autres solutions qui repose sur des infrastructures Anciennes reposant sur un pare-feu et combinant les plans de contrôle et de données..cette approche garantit une efficacité opérationnelle et une meilleure adaptabilité aux besoins changeants des entreprises.

En outre,cisco se distingue par son modèle de politique évolutif, qui offre une sélection dynamique des chemins pour permettre aux applications critiques d'éviter automatiquement les problèmes de réseau. De plus, sa microsegmentation et sa gestion des politiques basée sur l'identité facilitent une application cohérente des politiques multisites, garantissant ainsi une expérience utilisateur uniforme.Contrairement à certaines autres solutions, la gestion distincte des politiques pour le SD-WAN et le pare-feu ajoute une complexité à l'ingénierie du trafic et à la transmission des politiques centralisées pour les plans de contrôle et de données. De même pour d'autres solutions, bien que les politiques puissent être créées et réutilisées pour répondre aux besoins de l'entreprise, les capacités de microsegmentation et de gestion des politiques multidomaines sont limitées dans d'autres solutions.

En résumé, Cisco reste un choix supérieur en offrant une architecture SD-WAN

personnalisée et une solution complète prenant en charge à la fois le routage classique et le SD-WAN , garantissant ainsi une évolutivité et une flexibilité optimales pour répondre aux besoins variés des entreprises.

la sécurité réseau

Cisco intègre la technologie "Silicon root of trust" dans son matériel pour une sécurité renforcée au niveau du matériel, offrant ainsi une protection intégrée contre les attaques visant les bases du réseau et les accès non autorisés. En revanche, d'autres solutions telles que Fortinet, Silver Peak et Versa présentent des faiblesses en matière de sécurité. En effet, l'absence de détails concernant la protection intégrée offerte par leurs circuits intégrés personnalisés expose les entreprises à des risques de sécurité plus élevés. De plus, bien que ces solutions fournissent un matériel professionnel standard, elles ne disposent pas d'une solution de protection fiable connue, ce qui augmente le potentiel d'attaques ou d'accès non autorisés.

La segmentation réseau est une approche importante de l'architecture SD-WAN, et Cisco offre une segmentation MPLS/VRF complète et éprouvée. Cette solution prend en charge les topologies multisegments et la mutualisation, ce qui permet aux entreprises d'optimiser l'utilisation de leur infrastructure réseau tout en assurant la sécurité et la performance des données. En revanche, des solutions telles que Fortinet présentent des capacités de segmentation restreintes, avec des configurations VDOM complexes qui limitent la flexibilité pour créer des topologies multisegments dynamiques et adaptables aux besoins évolutifs des entreprises. De même, Silver Peak propose une segmentation basée sur VRF, mais elle est limitée en termes de routage avec le protocole OSPF et de priorisation des pairs.

En outre ,l'analyse du trafic chiffré est essentielle pour détecter les menaces potentielles et assurer la sécurité du réseau. Cisco a la capacité d'identifier les logiciels malveillants en comparant les modèles SHA chiffrés, sans avoir besoin de les déchiffrer, offrant ainsi une protection efficace contre les attaques. En revanche, des solutions

comme Fortinet présentent une faiblesse en termes de robustesse de leur solution d'analyse du trafic chiffré, qui peut ne pas être suffisamment efficace pour sécuriser les infrastructures ou les périphériques réseau. De même, Silver Peak ne permet pas la détection des malwares chiffrés, ce qui expose les entreprises à des risques de sécurité plus élevés.

En résumé, Cisco est le choix optimal pour la sécurité réseau, il propose la technologie "Silicon root of trust" offrant une sécurité intégrée au niveau matériel, une segmentation MPLS/VRF complète, et une capacité à détecter les logiciels malveillants sans déchiffrement. En comparaison avec des solutions comme Fortinet et Silver Peak, ils présentent des lacunes en matière de sécurité intégrée et de segmentation réseau, ce qui expose les entreprises à des risques de sécurité accrus.

L'intégration cloud

Pour la connectivité multicloud,Cisco est le meilleur choix grâce à son processus automatisé de déploiement sur diverses plateformes cloud telles qu'Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP). Avec des instructions détaillées guidant chaque étape du déploiement, Cisco offre une connectivité multicloud efficace et facile à mettre en œuvre.

En comparaison, des solutions telles que Fortinet présentent des workflows limités pour la connectivité multicloud, tandis que Silver Peak et Versa nécessitent une configuration manuelle pour le déploiement sur différents fournisseurs de cloud, ce qui compromet la rapidité et l'efficacité du déploiement.

la périphérie du réseau

Cisco est le choix optimal en termes de stockage en offrant une automatisation IoT/OT avec des fonctionnalités de stockage et de calcul intégrées pour les sites distants, le tout pris en charge par la gamme de commutateurs Cisco Catalyst 8200. En revanche, des solutions telles que Fortinet, Silver Peak et Versa présentent des lacunes en termes de

capacités d'hébergement de fonctions réseau virtuelles (VNF) en périphérie du réseau, avec une capacité limitée chez Versa, bien que ce dernier permet le déploiement de VNF sur les appliances Versa SD-WAN Edge. En outre , Cisco offre une intégration VoIP native grâce à ses plateformes Cisco Catalyst 8000 Edge, qui fournissent des services VoIP complets dans le cadre du SD-WAN et pour les piles de fonctions logicielles classiques IOS XE. De plus, Cisco est le seul fournisseur de SD-WAN à intégrer directement une adresse IP analogique/numérique dans un équipement terminal client unique, offrant ainsi une solution complète et native pour les besoins de voix sur IP. En comparaison, des solutions comme Fortinet souffrent d'une absence de fonctionnalité d'hébergement d'applications en périphérie du réseau, tandis que Silver Peak et Versa ne proposent aucune intégration native de la voix, ce qui peut limiter les fonctionnalités et l'efficacité des déploiements de communications unifiées.

Conclusion

Dans ce chapitre, nous avons examiné en détail les besoins de notre infrastructure réseau, en mettant en évidence les critères fonctionnels et non fonctionnels essentiels. Après avoir comparé les différentes solutions SD-WAN disponibles, nous avons choisi la solution optimale. Dans le chapitre suivant, nous allons analyser et concevoir la solution SD-WAN pour répondre à nos besoins spécifiques.