The bridge to possible

Le Projet de déploiement SD-WAN en environnement Cisco 2.b

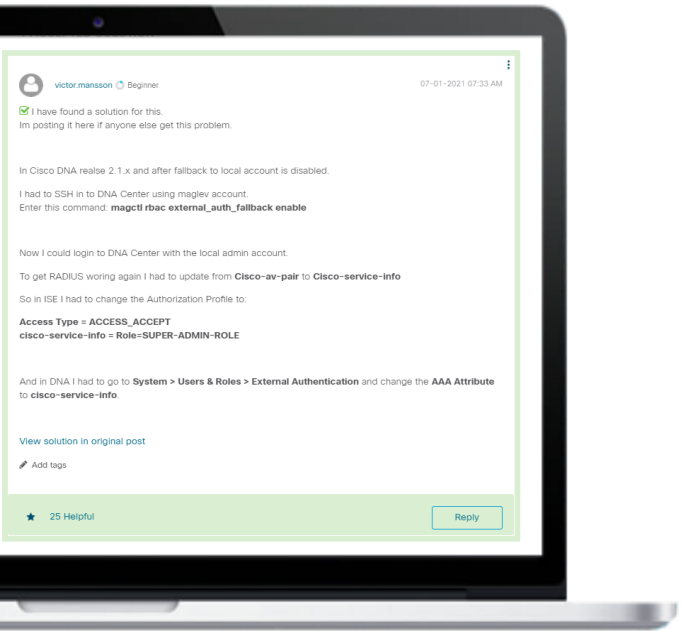
Appréhender les aspects techniques, humains et organisationnels.

Community Live – Routage et Commutation

Alain Faure – CCIE #8935 R&S

5 Mai 2022

Connect, Engage, Collaborate!



Lorsque vous recevez une réponse correcte, **acceptez-la comme solution !**

Cela aide les autres utilisateurs à trouver des réponses correctes

Accept as Solution

Mettez en évidence les autres membres

Les votes utiles motivent les membres enthousiastes en leur offrant **un signe de reconnaissance !**

★ 25 Helpful

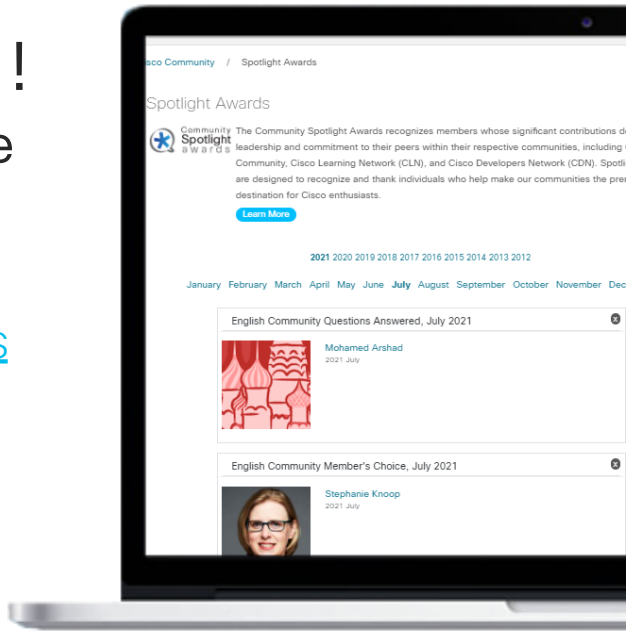
Spotlight Awards

De nouveaux lauréats tous les mois !

Gagnant du mois de Mars : **Redouane Meddane**

Démarquez-vous par vos efforts et votre engagement à améliorer la communauté et à aider les autres membres. Les Spotlight Awards sont distribués chaque mois pour mettre en valeur les membres les plus remarquables.

Maintenant vous pouvez aussi désigner un candidat ! Cliquez ici



Notre Expert

Alain Faure
Présentateur

Jimena Saez
Modérateur

[Téléchargez la présentation !]

Agenda

Partie Ia, 1b et 2a *(voir vidéo/pdf précédents)*

Partie 2b *(cette présentation)*

1. Licences
2. Focus Technique vEdge

La démarche

Les références de lectures que je vous donne sont indispensables, car il n'est pas possible de traiter un sujet aussi riche en 1h30.

La bonne façon d'aborder ce sujet est donc de relire ce document avec les références, pour ensuite élaborer son propre projet de déploiement SD-WAN.

Cela veut dire qu'outre les 1h30 vous devez passer quelques heures en plus pour faire une relecture de toute la documentation. Cisco reste le seul constructeur à proposer une documentation riche.

Aujourd'hui

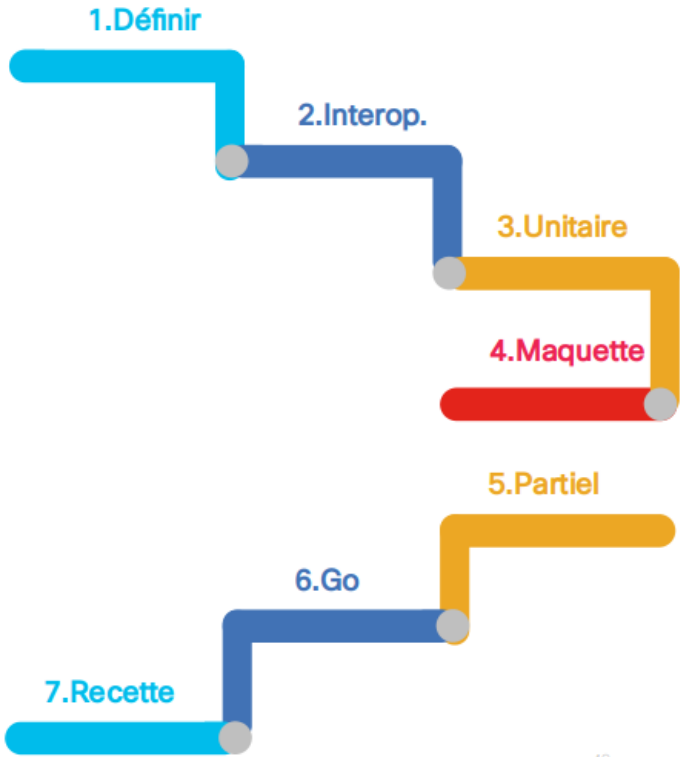
Vous devez vraiment avoir vu les présentations précédentes pour suivre celle de ce jour.

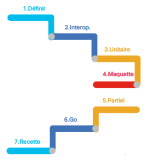
C'est aussi pourquoi je passerais sur les rappels. Et je ne reviens plus la méthode de travail que je pense acquise.

Nous allons voir aujourd'hui les détails d'implémentations du projet concernant le vEdge. Ce sera un espèce de « cookbook » des points à bien traiter dans le projet.

Ce sont des points qui ont un rôle « structurant » et/ou d'impact sur d'autres équipes et c'est pour cela qu'on en parle ici.

Rappel cycle du projet – Documentation





1. Licences

Les licences (1)

Outre l'aspect technique, le projet doit tenir compte des aspects comme les licences. Je vais essayer de vous donner ici quelques pistes de ce passage indispensable d'un projet SD-WAN Cisco.

Références : **Cisco SD-WAN Getting Started** Guide 2022-01-10, chapitre 10 **Licensing on Cisco SD-WAN**.

Les licences (2)

Pour le SD-WAN il existe 2 types de licences reliées à l'offre DNA:

- **Fonction du temps**
  - Essential (3 ans)
  - Advantage (3, 5 ou 7 ans)
  - Premier (5 ans)
- **Permanentes** (Network Essential, Network Advantage) qui sont attachées au matériel

Les licences (3)

Essential :

- Taille illimité pour le réseau overlay
- Support des protocoles de routage coté service
- Support du « dual stack »
- Hub-Spoke, Full mesh et topologies partielle de mesh
- ACL, Statefull firewall et IPS (Talos)

Les licences (4)

Advantage :

- Cisco AMP
- URL filtering
- Déploiement en Cloud Public (vEdge Cloud router, Cloud on Ramp dans AWS ou Azure)
- Support « avancé » de BGP support ou du multicast !
- Voix « avancées » (SRST !, voice ports FXS/FXO !, SIP trunk !)

Les licences (5)

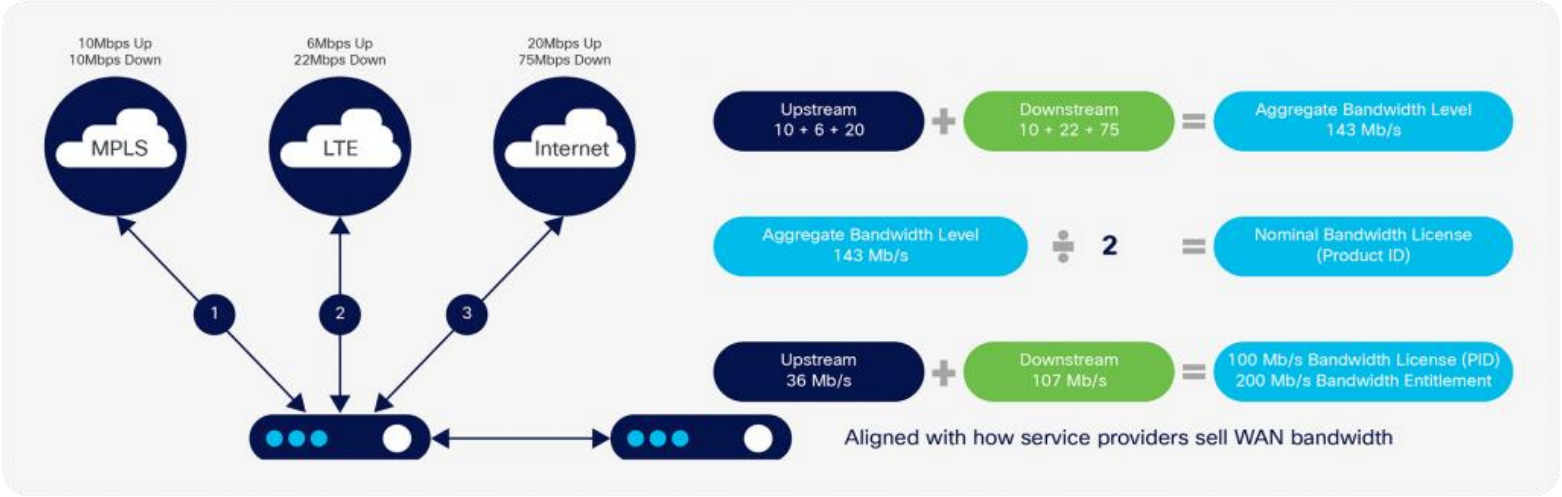
Premier :

- Cisco Umbrella SIG (Secure Internet Gateway)

Les licences (6)

La couche « trafic » :

Outre les fonctionnalités, il faut aussi tenir compte de la bande passante.



Les licences (7)

Comment sont désignées les licences ?

DNA – DNA licensing : DNA – X – Y – Z – N

X – C pour Cloud / P pour local au client « on Premise »

Y – Bande passante -Ex:100M-

Z – E : Essential / A : Advantage / P : Premier

N – durée de validité en années (3Y, 5Y, 7Y)

Les licences (8)

Les licences seront déterminées dans la document de « **spécifications détaillées** » puisque cela concerne chacun des équipements.

2. Focus Technique vEdge

Points d’intérêt

Le reste de cette présentation est dédié à différents points d’intérêts concernant le vEdge et le Data Plan.

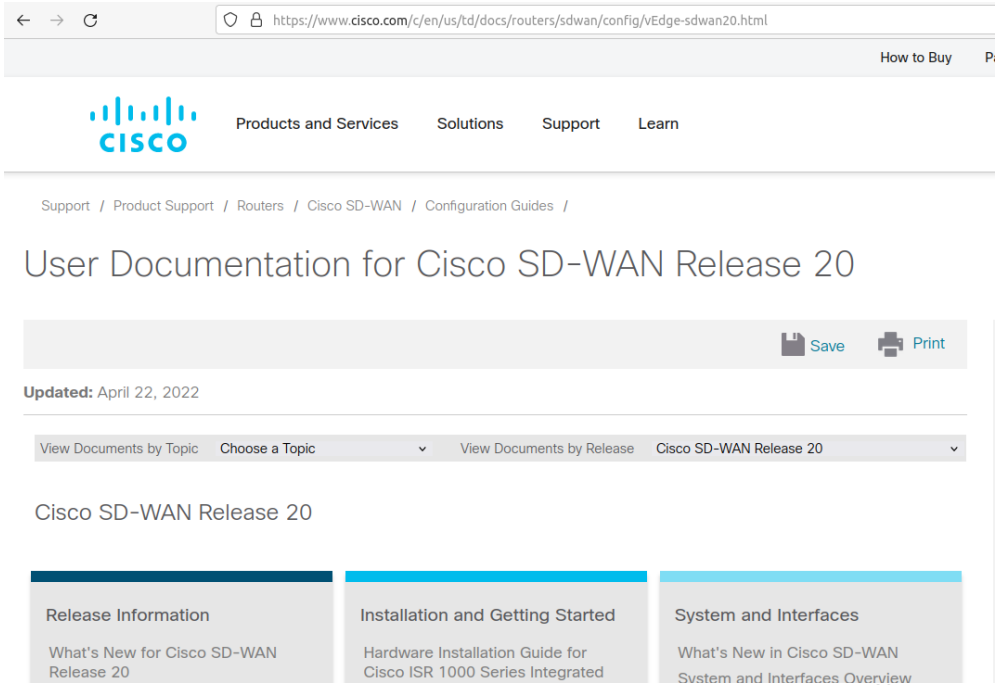
Ces points n’ont pas nécessairement de liens entre eux, mais sont indispensables à traiter lors d’un projet de déploiement SDWAN.

Où trouver la documentation vEdge ?

Référence :

Support/ Product Support / Routers / Cisco SD-WAN/ Configuration Guides

User Documentation for Cisco SD-WAN Release 20

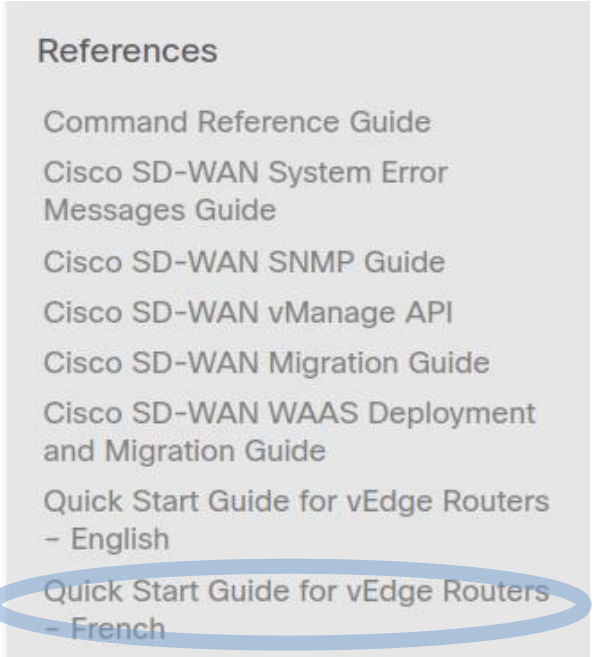


Organisez votre documentation vEdge

1) Récupérez les pdf de tous les documents et placez les dans un répertoire.

2) Les renommer, exemple:

SDWAN-CISCO-VEDGE-20-20220505-EN.pdf

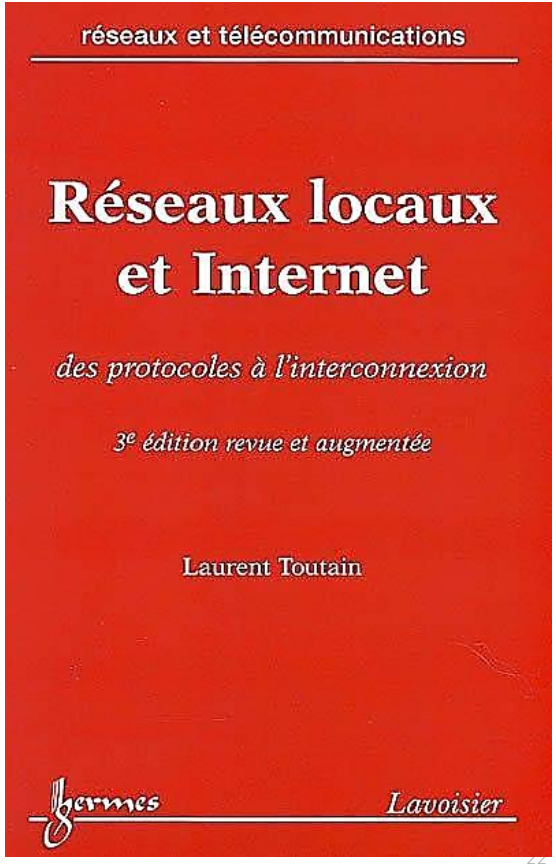


Optimisation TCP (1)

R.O.I.

Les vEdges sont en prise directe avec le trafic utilisateur. C'est pourquoi ils ont en charge l'optimisation du trafic.

En particulier, TCP a un comportement particulier qui peut être complexe et bien décrit dans le livre de Laurent Toutain que je vous recommande chaudement.



Optimisation TCP (2)

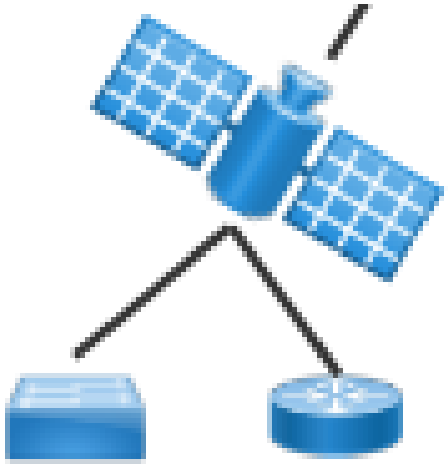
Cette fonctionnalité est décrite dans Cisco SD-WAN/ End-User Guides /

TCP Optimization Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20.x

Elle est très pratique dans le cas d'utilisation de réseaux physiques particuliers - Ex:satellites-.

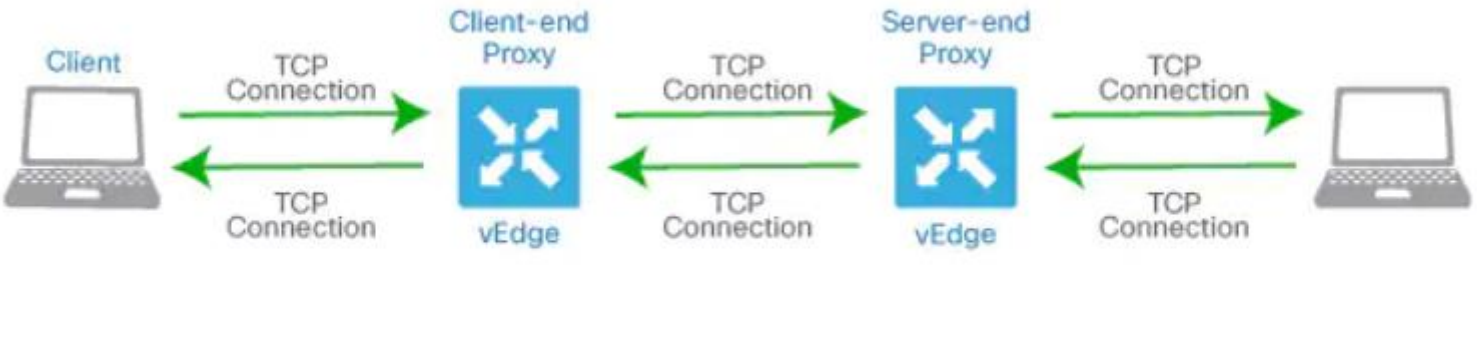
vEdge :1000, 2000

ISR1100 6G



Optimisation TCP (3)

Les vEdge agissent comme des « proxy TCP » ce qui va permettre de gérer les fenêtres, retransmissions etc. en les adaptant mieux aux types de liens physiques.



Optimisation TCP (4)

Détails d'application, vous utilisez un process de CPU pour mettre en place cette fonctionnalité, il faut en tenir compte dans le choix du matériel et la maquette.

C'est typiquement le type de chose à tester lors de la maquette.

Configuration très simple :

```
vSmart# show running-config policy data-policy tcp_optimization_data_policy
policy
 data-policy tcp_optimization_data_policy
  vpn-list vpn_2
   sequence 100
    match
     destination-port 22
    !
    action accept
     count                sample_count
     tcp-optimization
    !
   !
   default-action accept
```

Optimisation TCP (5)

Cette partie doit être traitée dans les « **spécifications détaillées** » puis vérifiée et validée sur la maquette.

C'est un détail d'implémentation qui concerne des types de liens ou d'architectures spécifiques. Créer une note d'implémentation en fonction des retour de la maquette. Cela devra être mis dans les **documents de déploiement**.

Discuter avec l'équipe sécurité (1)

Quels ports TCP/UDP sont nécessaires pour un vEdge ?

Vous devez rechercher dans la documentation la liste des ports pour pouvoir vous concerter avec l'équipe sécurité IT pour l'ouverture des ports en question.

Référence : Cisco SD-WAN / End-User Guides /

Security Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20.

N'oubliez pas de jeter un œil aux Release Note concernées.

Discuter avec l'équipe sécurité (2)

Voir : Solutions/Enterprise/Design Zone/Design Zone for WAN and Branch/Remote Sites/ Design Guides **Cisco SD-WAN Design Guide** « **Firewall Port Considerations** »

Table 2. DTLS, TLS, and IPsec ports for SD-WAN device connections

Source device	Source port	Destination device	Destination port
WAN Edge (DTLS)	UDP 12346+n, 12366+n, 12386+n, 12406+n, and 12426+n, where n=0-19 and represents the configured offset	vBond	UDP 12346

Discuter avec l'équipe sécurité (3)

« Discuter avec l'équipe de sécurité » demande généralement une demande officielle d'ouverture de ports avec un formulaire particulier.

Il est bon/nécessaire de leur expliquer les tenants et les aboutissants de l'architecture. Pour cela, il est souhaitable de créer un document spécifique sur les ports à ouvrir avec explications, détails d'implémentation et évolution future.

Cela devra être consigné dans un document spécifique compris dans les « **spécifications fonctionnelles** » : il s'agit de relations entre « modules »

Définir les ressources du SD-WAN / vEdge (1)

Voir référence :

Cisco SD-WAN End-to-End Deployment Guide

Voir les exemples de « branch ».

L'idée va être de définir des typologies d'objets en fonction des architectures cibles.

Définir les ressources du SD-WAN / vEdge (2)

Vous devez définir les ressources SD-WAN (TLOC etc.) qui vont être utilisés pour l'infrastructure SDWAN. C'est le coté « **Transport** ».

- TLOC (voir la présentation SDWAN)
- protocole -Ex:BGP-

Cela devra être défini dans un document de type « **spécifications détaillées** » phase 3 (on reste dans le data plan)

Définir les ressources du SD-WAN / vEdge (3)

Vous devez définir les ressources SD-WAN (TLOC etc.) disponibles localement pour réaliser des interconnexions. C'est l'aspect « **Services** »

Nous allons voir cela dans les slides suivants :

- Interfaçage local avec le routage

- Interfaçage local avec le niveau 2 -Ex:VLAN-

Cela devra être défini dans un document de type « **spécifications détaillées** » phase 3

Interfaçage avec protocoles de routage (1)

Décrit dans : Cisco SD-WAN/ End-User Guides

Routing Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20.x

```
omp
  no shutdown
  graceful-restart
  address-family ipv4 vrf 1
   advertise connected
   advertise static
   advertise network X.X.X.X/X
  !
```

Interfaçage avec protocoles de routage (2)

Créer une typologie pour le routage, c'est lister les types de réseaux IP différents et déterminer s'ils doivent être redistribués dans le cadre omp et avec quelle politique.

Par exemple, les vlans imprimantes, WiFi, VoIP etc.

Interfaçage avec protocoles de routage (3)

Chaque organisation a des protocoles de routage avec des domaines de routage particuliers.

Il faudra avoir fait l'audit des différents domaines de routage de toute l'infrastructure réseau, puis déterminer les points de redistribution et de diffusion des adresses réseaux.

La « typologie » sera décrite dans un document de « **spécifications unitaires** ». [justification : c'est local vis à vis du projet de SDWAN]

Interfaçage avec le niveau 2 (1)

Il vous faudra définir les interconnexions avec le niveau 2. C'est à dire ce que vous reliez sur les VLANs locaux.

- Trunk
- VLAN

Accessoirement, associés à quel infrastructure SD-WAN ?

- *TLOC*
- *VPN*

Interfaçage avec le niveau 2 (2)

Références :

Bridging Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20

Interfaçage avec le niveau 2 (3)

Documents « **spécifications détaillées** ».

Pour rappel aussi les « **tests unitaires** » !

Considérations d'opérateurs (1)

Références :

Systems and Interfaces Configuration Guide, Cisco SD-WAN Release 20.x / Cisco SD-WAN Multitenancy (Cisco SD-WAN Releases 20.4.x and 20.5.x)

Table 1. Feature History

Feature Name	Release Information	Feature Description
Cisco SD-WAN Multitenancy	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	With Cisco SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco vManage. In a multitenant Cisco SD-WAN deployment, tenants share Cisco vManage instances, Cisco vBond Orchestrators and Cisco vSmart Controllers. Tenant data is logically isolated on these shared resources.

Considérations d’opérateurs (2)

Et à propos du vEdge :

Hardware Supported and Specifications

The following platforms support multitenancy.

Table 2. Router Models

Platform	Router Models
Cisco vEdge device	• vEdge 100, vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud • ISR1100-6G/ISR1100-4G, ISR1100-4GLTENA, ISR1100-4GLTEGB

La QoS et les applicatifs (1)

Traduire la QoS dans les templates.

On ne parle pas de déterminer la valeur des paramètres, cela se fait lors de la mise en place de la maquette, mais plutôt les applications présentes sur quels sites et leurs caractéristiques/comportement.

Voir: « **Procedure 2: Define QoS classification access list** »

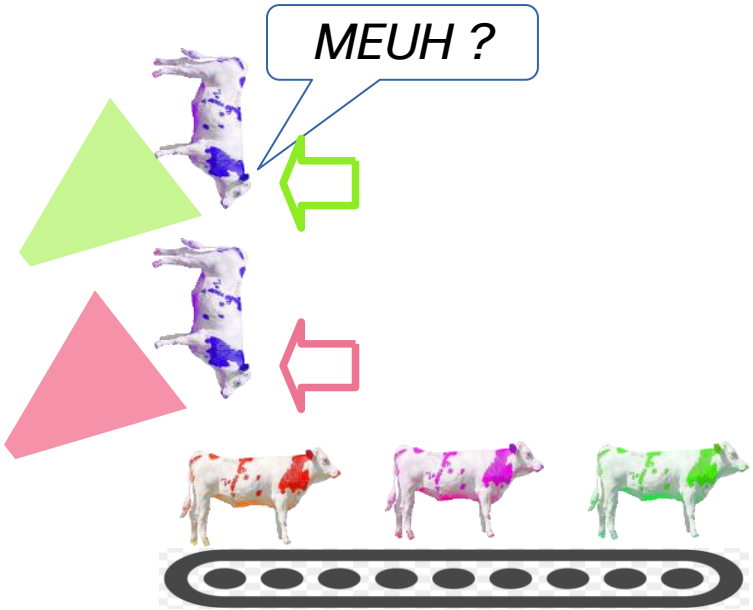
La QoS et les applicatifs (2)

Tableau avec par classes QoS:

- Les applications

- Leurs besoins -Ex :bande passante, RTT, gigue, possibilité d'élaguer, comportement à l'élagage-

Je vous propose de revoir la présentation que j'avais faite sur la QoS et sur SMB ou j'explique des bases de la QoS.



La QoS et les applicatifs (3)

Ces considérations sur la QoS doivent être tirées de l'audit préalable. (vous devez comprendre à quel point cet audit est important).

Voir aussi : **Forwarding and QoS Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20**

La QoS concerne le DATA plan en conséquence, la définition des typologies de QoS concerne les « **spécifications unitaires** ».

Tester le trafic à travers le vEdge (1)

Obtenez un pattern de trafic et rejouez le à travers les vEdge.

Il doit y avoir une phase de compréhension de ce qui passe à travers le WAN.

Faites des relevés de trafic **avant** - > AUDIT.

Et attention aux applications spécifiques -Ex :imprimantes splash-

Tester le trafic à travers le vEdge (2)

Utilisez des générateurs de trafic -Ex : NetScanTools Packet Generator, solar wind wan killer, PB Software.

Autres : IXIA, Spirent, IXIA/BreakingPoint, Avalanche, Chariot Seagull, Iperf

Open source : Packet Sender, Ostinato, TREX, Nping,NetScanTools Packet Generator

Utilisez les applications Netflow et les captures de packet.

Tester le trafic à travers le vEdge (3)

Ces tests ne servent pas à régler des valeurs de paramètre, mais à comprendre et **créer des typologies de trafic**.

Documentation, les typologies de trafic seront décrites dans les « **spécifications détaillées** » -propre au Data plan-

Bien entendu, cela sert aussi et c'est important à **qualifier** tel ou tel type d'équipement pour l'utilisation que l'on veut en faire.

Documentation, les documents de la maquette pour la partie qualification des équipements (et des firmwares !)

Sécurisation du vEdge (1)

C’est un aspect qui mérite plus de détail car il convient de décrire comment sont sécurisés les vEdge.

Rappelons qu’il faut absolument éviter qu’ils soient volés ! (et en ce moment, en Europe on s’en prend aux infra physiques).

Le vEdge est une partie du réseau et il faut éviter qu’un pirate puisse s’en emparer puis le connecter à un autre endroit (avec des complicités éventuelles, c’est triste mais oui).

Sécurisation du vEdge (2)

Il faut sécuriser l'équipement vEdge de manière spécifique :

- Physique : rack sécurisé, coffre, pièce forte. Au passage n'oubliez pas les contraintes électriques !

- Utilisation d'anti-vols et de localisation d'équipement volé.

- Mécanisme de connexions « géographiques »

Du matériel sérieux **(militaire ?)**.

Sécurisation du vEdge (3)

Voir le document de configuration vEdge sur le GPS

Configure the GPS Location

To configure a device location, select the **GPS** tab and configure the following parameters. This location is used to place the device on the Cisco vManage network map. Setting the location also allows Cisco vManage to send a notification if the device is moved to another location.

Table 4.

Parameter Field	Description
Latitude	Enter the latitude of the device, in the format *decimal-degrees*.
Longitude	Enter the longitude of the device, in the format *decimal-degrees*.

To save the feature template, click **Save**.

CLI equivalent:

```
system  gps-location  (latitude decimal-degrees | longitude decimal-degrees)
```

Sécurisation du vEdge (4)

Voir aussi l'article sur le blog de Cisco en Français par Jérôme DURAND. J'en ai parlé la dernière fois

La documentation de **déploiement partielle** et à plus forte raison **générale** doivent comporter des indications à ce sujet.

Le réseau de management (1)

Toujours dans le domaine de la sécurité. Je vous recommande chaudement (et donc à mettre en application) un réseau d'administration physique séparé. -et donc pas dans un VLAN-.

Cela veut dire de la fibre ou du cuivre allant sur tous les ports admin de tous les équipements.

La raison est que les équipements réseaux généraux peuvent être compromis ou hors service. Il faut un secours.

Il faut aussi prévoir un moyen de comm. De secours spécifique au réseau d'admin. (admin, exploit, supervision).

Le réseau de management (2)

Ce type de mise en place doit être défini dans la partie « **spécifications fonctionnelles** » car cela touche à différents niveau de l'architecture.

Note : le débat sur les documents qui doivent porter ces définitions est important pour une bonne compréhension de l'architecture.

L’alimentation électrique (1)

Les vEdge sont prévus pour (série 1000) avoir deux connections vers l’alimentation secteur.

Il est nécessaire de prévoir un raccordement vers deux sources électriques (généralement une « brute » et une secourue). La source secourue l’est sur un circuit protégé par batteries et générateurs autonomes.

Selon les circonstance je rajouterais un UPS en coupure sur l’alimentation brute.

Dans tous les cas prenez des mesures pour que la masse soit vérifiée et validée.

L’alimentation électrique (2)

La définition de l’alimentation électrique doit être portée dans un document de « **spécifications fonctionnelles** ». Puis dans les documents sur les déploiements.

Cet aspect doit se discuter avec les équipes de management des bâtiments physiques. C’est un très gros travail que de bien border l’aspect physique (*COMME LE CABLAGE !*) du déploiement.

Bien plus impactant en terme de coût que la haute technologie des équipements et configuration.

Le choix des composants internes (1)

Les tests de performance peuvent vous aider à déterminer si vous avez besoin de plus de mémoire par exemple.

Mais ce n'est peut être pas nécessaire pour tous les sites.

La encore on s'applique plus à déterminer des typologies et des abaques pour le volume de trafic.

Le choix des composants internes (2)

Mémoire sur un vEdge virtuel.

Recommended Core and RAM	• Cisco recommends a 1:1 ratio of Core to RAM • Cisco recommends a minimum two cores and 2 GB RAM Primary Combination: ◦ 2 Core / 2GB RAM ◦ 4 Core / 4GB RAM ◦ 8 Core / 8GB RAM Secondary Combination: ◦ 6 Core / 4 GB RAM ◦ 8 Core / 2 GB RAM ◦ 4 Core / 2 GB RAM ◦ 2 Core / 4 GB RAM

Le choix des composants internes (3)

Ces résultats doivent vous permettre de mettre à jour les « **spécifications détaillées** »

Le choix des options logicielles (1)

Nous avons vu lors de la présentation des licences, les options logicielles rendues disponibles par les licences.

Normalement le choix est fait quand on entame la maquette.

MAIS, Il faudra déterminer la « **bonne version** ». Prévoyez des tests exhaustifs sur les types de trafics attendus et les options nécessaires pour vérifier et valider le bon fonctionnement de telle ou telle version/sous version.

Ces tests feront partis de la procédure de test des mises à jour.

Le choix des options logicielles (2)

La documentation qui porte ces informations doit être les « **spécifications détaillées** »

Les types de site (1)

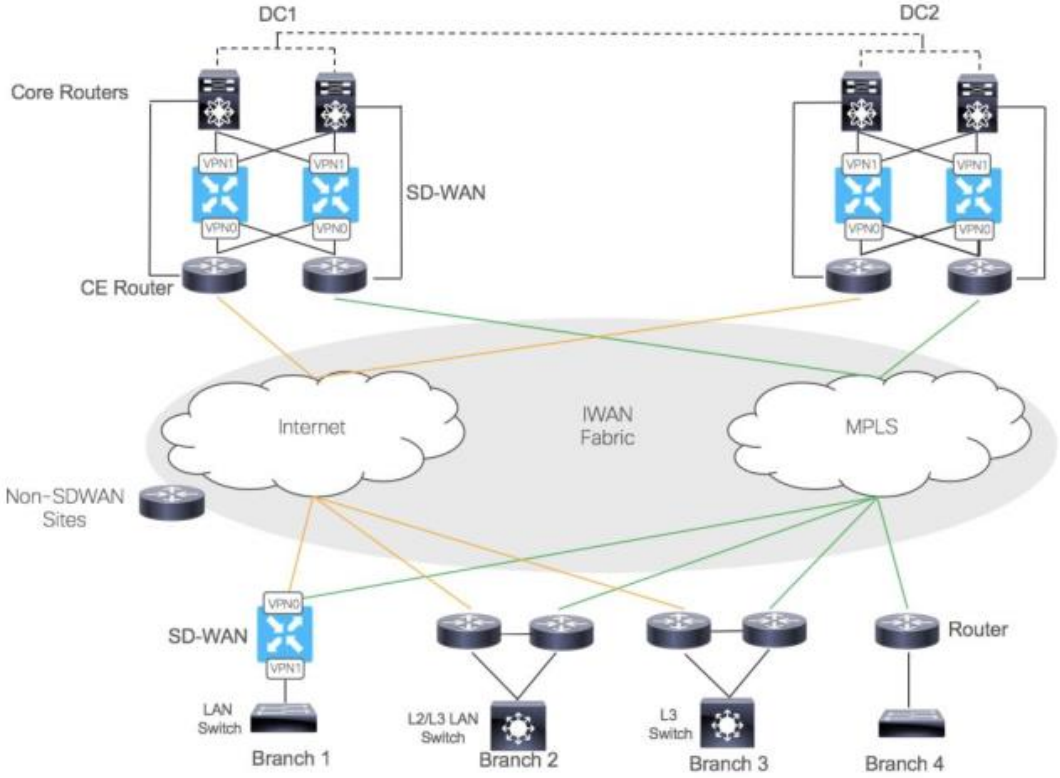
La typologie des sites est particulièrement importante, car elle va déterminer les types de déploiement et aussi les types de template etc.

La documentation -Ex: tableaux, protocoles de routages- est nécessairement dans les « **spécifications fonctionnelles** » car cela concerne nombre d'entités dans l'architecture SDWAN.

Les types de site (2)

Voir :

Cisco SD-WAN Migration Guide



Nommages, Adressages, Template

Par définition la politique de nommage, d'adressage et les templates sont issus du travail de « **spécifications détaillées** », ce doivent donc être décrits dans ces documents.

Sauvegardes et restaurations (1)

Discutions avec l'équipe en charge des sauvegardes est à prévoir dès le début du projet pour voir les solutions et protocoles disponibles. Il est bon que cet aspect ne soit pas géré par les mêmes personnes que ceux qui gèrent le SDWAN. Et que des tests soit réalisés régulièrement.

Nous aurons l'occasion de revoir ce sujet par la suite (vManage) pour les autres équipements qui sont plus concernés, mais les sauvegardes sont essentielles.

Veillez à ce que les vEdges soit bien sauvegardés, ainsi que les clés, certificats etc.

Sauvegardes et restaurations (2)

La documentation sur les sauvegardes, comme pour tout ce qui est PRA, PCA, est nécessairement dans les « **spécifications fonctionnelles** » car cela concerne nombre d'entités dans l'architecture SDWAN.

Avez-vous encore des questions ?
Utilisez le panneau « Q&R »

Forum Ask Me Anything

Retrouvez notre expert sur la page de Discussion

Toutes les nouvelles questions sur le sujet de ce webinaire seront répondues par la suite jusqu'à la semaine prochaine: 13 mai.

Postez une question ici
https://bit.ly/AMAd-may22

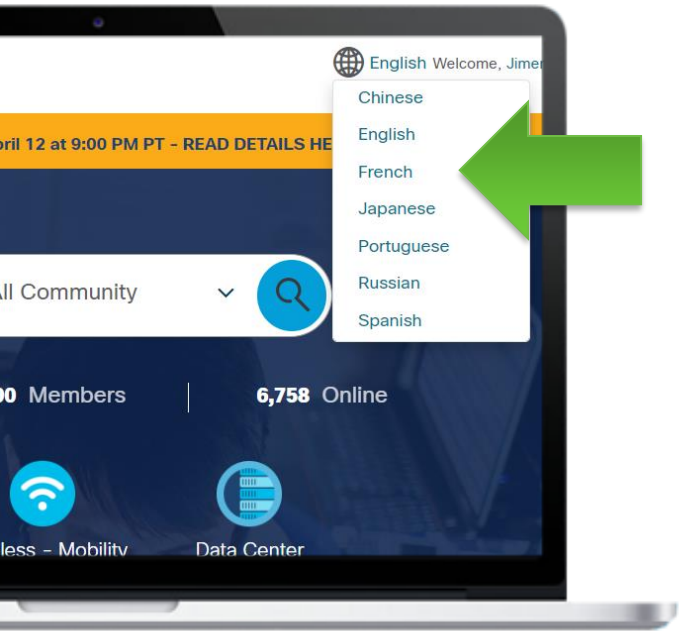
Prochains événements

24 MAI **Webinar sur Cisco Meraki**
Description en attente
Inscrivez-vous https://bit.ly/WEB2-FRmay22

Webinaires du mois de mai 2022

Calendrier : Inscrivez-vous ici !

Où que vous soyez restez connecté…



- Facebook CiscoSupportCommunity
- Twitter @cisco_support
- YouTube CiscoSupportChannel
- LinkedIn Cisco Community
- Instagram CiscoSupportCommunity


Avez-vous des commentaires ?
Répondez à notre enquête !

The bridge to possible