DNA, la solution SDN SDA campus de Telecom-Paris

Masson Christophe
DSI
19 place Marguerite Perey
91120 Palaiseau

Résumé

Cet article décrit les différentes étapes qui nous a amené au choix d'un réseau DNA de chez Cisco et jusqu'à la mise en place de celui-ci.

Mots clé

DNA, SDA, SDN, 802.1x, niveau 3.

Contexte

Avec la multiplication des services offerts aux utilisateurs et une demande accrue de sécurité, les réseaux modernes sont devenus beaucoup plus complexes que par le passé. Ils demandent une grande sécurité et des moyens d'analyse de flux performants, et également une souplesse dans l'évolution et le déploiement.
Cette évolution a alourdi fortement la gestion des réseaux au quotidien. Nous avons vu la multiplication des access-list et la multiplication des Vlans. De plus, la plupart des attaques proviennent de l'intérieur. Par exemple, un réseau ouvert sur une « prise » expose celui-ci à des actes de malveillance. Les Vlans aussi posent problème. De nouveau virus performants utilisent la possibilité que les Machines puissent communiquer directement entre elles afin de se propager et d'infecter tout un parc de machines.

1 Introduction

Le déménagement de l'Institut Mines Telecom et de Telecom Paris sur le plateau de Saclay, nous a amené à réfléchir sur la direction à prendre pour notre nouveau réseau. Nos exigences étaient multiples, nous sommes partis à la recherche d'une solution permettant un réseau sécurisé résiliant, robuste et monitoré.
Également, nous voulions améliorer considérablement notre politique de sécurité. Cette politique de sécurité était essentiellement concentrée sur nos routeurs d'entrée internet et des cœurs de réseau par des access-list. Rapidement, nous sommes venus à la conclusion qu'il fallait un système de sécurité réparti sur tout le réseau et à chaque point d'entrée du réseau. Ces points d'accès sont aussi bien pour l'utilisateur que pour notre accès Internet. Pour une sécurité maximale, nous voulions un accès restreint des utilisateurs au réseau avec une authentification forte. Ces accès seraient couplés à une gestion des invités afin qu'ils puissent se connecter à notre réseau avec des droits restreints. Nous voulions aussi simplifier la gestion

du réseau en ayant une interface d'administration, et une gestion des règles de sécurité graphique et intuitive. Une exigence importante était que toutes les prises devaient être banalisées afin d'éliminer la gestion par prise. Un autre point concernait également l'auto configuration des équipements. Nous voulions, pour le déploiement et pour la gestion courante du réseau, que les équipements se provisionnent automatiquement. Concernant le réseau sans fil, celui-ci devra être intégré dans la solution SDN et devra avoir exactement les mêmes caractéristiques de gestion que le réseau filaire.

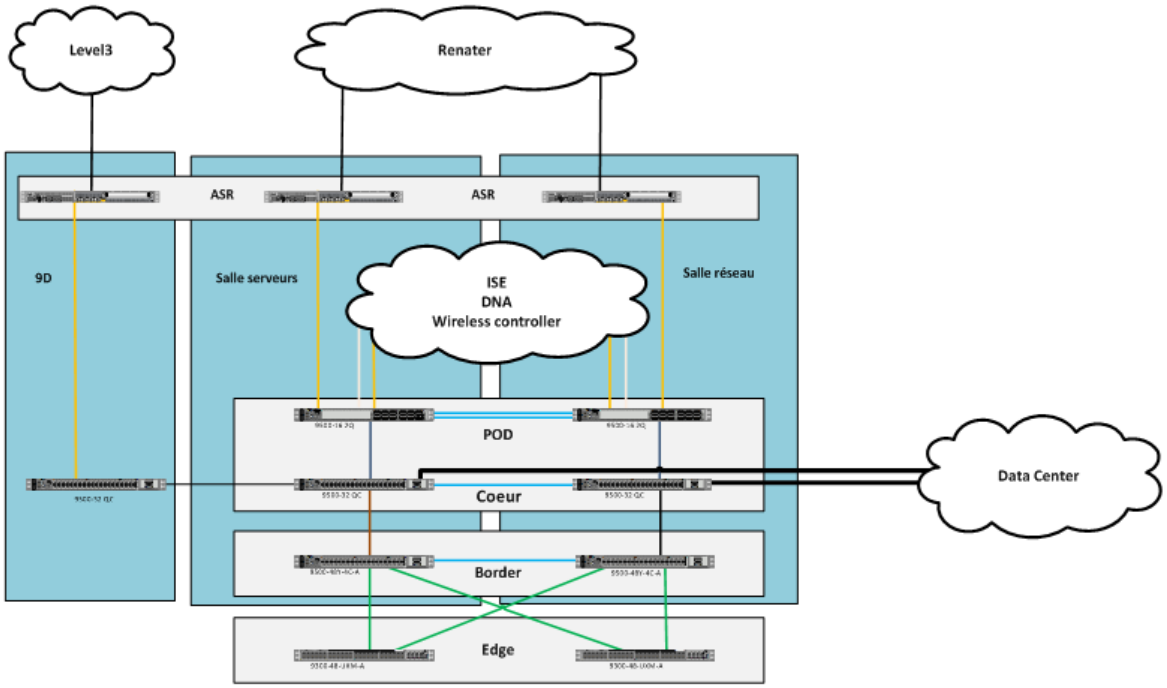
2 Choix de la solution Digital Network Architecture (DNA) de CISCO

Nous avons donc opté pour la solution DNA proposée par Cisco. Cette solution répond exactement à nos exigences. La robustesse a été apportée par le niveau 3. Grâce au routage, nous avons pu nous libérer du spanning-tree et également mettre fin aux boucles régulières provoquées par les utilisateurs. Le niveau 3 nous protège également des tempêtes de broadcast.
Cette solution, basée uniquement sur du niveau 3, permet une macro et une micro segmentation, offrant ainsi une grande robustesse et une sécurité accrue. Celle-ci est améliorée par un système de règles entre groupe d'utilisateurs (SGT). Ce niveau 3 est de type fabrique. Cette fabrique repose sur les protocoles Vxlan, LISP, BGP, ISIS. Elle possède deux couches l'underlay et l'overlay. Underlay utilise ISIS comme protocole de routage à l'intérieur de la fabrique et BGP pour s'interconnecter avec le cœur du réseau qui se trouve à l'extérieur de la fabrique. Pour constituer l'overlay de la fabrique, la solution utilise des VRF pour la macro segmentation et Vxlan pour la micro segmentation. Des acces-lists sont en complément de cette micro segmentation. Elles renforcent la granularité du filtrage et de la segmentation. Le 802.1x, supporté par la solution DNA, permet une souplesse dans la gestion des prises d'accès. Il banalise la configuration des ports d'accès. Le SDN de chez Cisco possède un système d'auto provisionnement permettant d'ajouter automatiquement un équipement dans la fabrique. Enfin, le DNA embarque beaucoup d'outils d'analyse permettant un diagnostic rapide et précis des anomalies. Les bornes wifi sont intégrées dans la fabrique et possède les mêmes caractéristiques que le réseau filaire.

3 L'infrastructure

Le système repose sur plusieurs briques Cisco. La première brique est le DNA. Le DNA a pour but principal la configuration des équipements réseau. C'est avec le DNA que nous allons renseigner le plan d'adressage, le type d'authentification, et la configuration WIFI. Une fois le DNA configuré et prêt à fonctionner, celui-ci est très peu utilisé par la suite. La brique DNA est constituée de trois serveurs afin d'obtenir un Corum.
La deuxième brique est le contrôleur WIFI, celui-ci est configuré automatiquement par le DNA. À noter par rapport à une utilisation classique d'un contrôleur où les flux transitent par le contrôleur, ici les flux ne transitent pas par le contrôleur mais cheminent à travers la fabrique.
La dernière brique est l'ISE. L'ISE n'est pas obligatoire mais fortement recommandé. Il a pour rôle premier d'être un serveur d'authentification. C'est également grâce à lui que l'on peut configurer les SG tag appliqués dans la fabrique. La prise en main de l'ISE est assez fastidieuse, dans le système DNA. Il représente la majorité du travail à fournir.

Notre architecture a tenu compte des recommandations Cisco afin de bénéficier du support Cisco.
Le bâtiment de Saclay est relié à un site distant se trouvant à 40 kilomètres, ce site est le nœud parisien permettant de desservir les autres sites de Paris. Nous possédons également 3 accès internet, un accès par Level3 et deux accès par Renater, ces 3 accès sont en full BGP et nos annonces sont effectuées afin d'influencer les routes retour pour que les flux arrivent au plus proche de la source. Les flux sortant sont routés sur les accès les plus proches.
Les serveurs constituant le contrôle du réseau DNA sont connectés sur le POD, le POD se trouve hors du réseau DNA et sa configuration est manuelle. Le cœur de réseaux à pour but de router les flux vers leurs destinations, tout comme le POD le cœur de réseau se trouve hors de la fabric et se configure manuellement.



4 Les fonctionnalités du DNA

Une des fonctionnalités intéressantes pour notre projet est le Lan automation. Cette fonctionnalité permet de configurer « from scratch » et automatiquement tous les équipements internes au réseau campus DNA. Notre réseau est constitué de 162 switch donc cette fonctionnalité nous apporte un gain de temps de configuration importante.

Une des grandes réflexions a été le plan de migration de notre ancien réseau se trouvant à Paris vers la nouvelle infrastructure DNA de Palaiseau. À Paris, nous avions une architecture classique, de niveau 2 avec un nombre important de Vlan. Dans notre classe B public, nous avons pu récupérer beaucoup de subnet libres afin de remplacer les réseaux existants. Certains utilisateurs ont déclaré leur adresse publique à un tiers afin de renseigner leur adresse IP dans des firewalls distants. Nous avons dû prendre en compte cette donnée. Cisco a élaboré une procédure permettant un plan de migration correspondant à notre cas, mais cette procédure est

fastidieuse et n'a jamais été testée. Nous avons donc pris une solution radicale qui a consisté à supprimer les réseaux le jour du déménagement et de les reconfigurer dans le nouveau réseau DNA le jour même.

Concernant le 802.1 X, nous avons 3 types de population :

- les utilisateurs ayant une machine dans notre contrôleur de domaine : Pour eux, la solution a été très simple, nous configurons le 802.1 X avec l'authentification « utilisateur » de Windows. Cette manipulation rend complètement transparent le 802.1 x à l'utilisateur.
- les utilisateurs ayant une machine personnelle : Pour eux, nous mettons à disposition l'utilitaire cat Eduroam permettant de configurer en quelques clics aussi bien le réseau filaire que le réseau wifi. En effet, cat Eduroam permet effectivement de configurer le réseau wifi et Eduroam mais aussi, en option, d'ajouter d'autres réseaux wifi et des réseaux filaire en 802.1x.
- les invités : nous fournissons des comptes invités permettant une authentification sur notre réseau et également la possibilité d'utiliser cat Eduroam pour une configuration simple.

L'architecture DNA apporte une sécurisation accrue avec les SGT (security tag). Les SGT permettent de créer des règles à l'intérieur du réseau campus et uniquement dans ce réseau. Chaque type de population est identifié et en fonction des besoins héritent de droit. Par exemple les élèves ne peuvent pas communiquer ensemble et également avec aucun autre type de population.

Ces règles sont très basiques, elles permettent que les utilisateurs ne puissent pas communiquer entre plusieurs groupes d'utilisateurs et également la possibilité que les utilisateurs ne communiquent pas entre eux à l'intérieur de leur propre groupe. Grâce à cela, nous avons accru la sécurité de notre réseau. Mais les SGT ne permettent pas une sécurisation optimale. C'est pour cela que nous avons ajouté des access-list dans notre cœur de réseau. Pour éviter l'accumulation avec le temps des access-list dédié à un utilisateur, nous avons créé un script et une interface permettant l'ajout d'access-list lié à un utilisateur. L'accès-list est stocké dans le compte LDAP de l'utilisateur et un script permet d'appliquer cette access-list dans le cœur de réseau. Lorsqu'un utilisateur quitte l'école l'access-list disparaît avec la destruction du compte de celui-ci.

5 Mise en œuvre de DNA

La mise en œuvre a été essentiellement effectuée par nos soins, soit deux personnes de la DSI pour le désigne et la configuration des équipements, et 3 semaines d'assistance de notre intégrateur. Et concernant le déploiement une personne de la DSI pour le suivi du chantier et une équipe de notre intégrateur pour la pose et le brassage de nous 162 switches.

À ce jour, nous venons d'emménager dans nos locaux. Nous avons donc peu de recul sur l'exploitation de ce système.
Le 802.1 X permet une gestion simple des réseaux physiques filaires sans devoir configurer chaque prise manuellement. Toute modification dans notre réseau se fait facilement grâce au DNA. Et la gestion des access-list est simplifiée grâce à notre script et notre interface de gestion des access-list.

Concernant la configuration et l'installation du matériel et compte-tenu de la jeunesse de cette technologie, nous avons été confrontés à de nombreux problèmes. Ces problèmes ont été résolus un à un avec l'aide du TAC de Cisco. La brique DNA a concentré une grande partie de ceux-ci. Par exemple la non compatibilité des versions d'équipements entre eux.

Les équipements réseau de la famille 9000 sont également très jeunes. Quelques dysfonctionnements et incompatibilités sont apparus pendant l'installation. Ces dysfonctionnements ont été rapidement corrigés avec l'arrivée de nouvelles versions. Pour l'ISE et le contrôleur WiFi, ces deux derniers ont fait leurs preuves chez Cisco et n'ont posé que peu de problèmes.

6 Conclusion

En Conclusion, concernant la configuration et l'installation du matériel et compte-tenu de la jeunesse de cette technologie, nous avons été confrontés à de nombreux problèmes. Ces problèmes ont été résolus un à un avec l'aide du TAC de Cisco. La brique DNA a concentré une grande partie de ceux-ci. Les équipements réseau de la famille 9000 sont également très jeunes. Quelques dysfonctionnements et incompatibilités sont apparus pendant l'installation. Ces dysfonctionnements ont été rapidement corrigés avec l'arrivée de nouvelles versions. Pour l'ISE et le contrôleur WiFi, ces deux derniers ont fait leurs preuves chez Cisco et n'ont posé que peu de problèmes. Cette solution apporte beaucoup d'avantages dans la gestion des réseaux et leur mise en place. Il nous faudra encore quelques temps pour tirer d'autres conclusions sur cette nouvelle technologie.
Le cout d'une installation DNA nécessite un surplus par rapport à une infrastructure classique. Ce cout supplémentaire et attribué aux licences DNA, aux serveurs DNA, à la formation, et à l'installation de l'infrastructure. On compte résorber le surcout du CAPEX par l'OPEX.