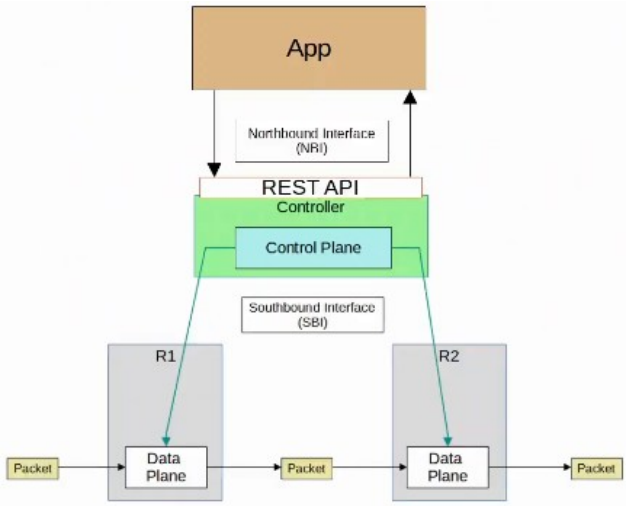
Cours 62 : Software-Defined Networking

Dans ce cours nous verrons Software-Define Networking (SDN). Nous verrons plus en détail les offre que Cisco propose comme SD-Access ou Software Defined Access.
Nous ferons en premier temps rappel du fonctionnement de SDN, puis verrons Cisco SD-Acces, le Cisco DNA Center, Une comparaison entre Gestion DNA Center Network et une gestion réseau traditionnel.

SDN est l'acronyme de Software-Define Networking il s'agit d'une approche du réseau pour centraliser le plan de contrôle dans une application appelé Contrôleur.
Les plans de contrôle traditionnel utilise une architecture distribué c'est à dire que chaque appareil a son propre plan de contrôle. Le plan de contrôle de chaque appareil du réseau utilise des protocoles comme OSPF pour communiquer entre eux partager des informations de routage. Chaque appareil a ses propres ACL et règles de sécurité, etc...
Un contrôleur SDN centralise les fonctions du plan de contrôle comme le calcul des routes.
Le contrôleur peut interagir de manière programmé avec les appareils du réseau en utilisant des APIs. Le SBI est utilisé pour communiquer entre le contrôleur et les appareils du réseau qu'il contrôle. Le NBI est ce qui permet d'intéragir avec le contrôleur avec un script et l'application.
Voici à quoi ressemble une architecture SDN :

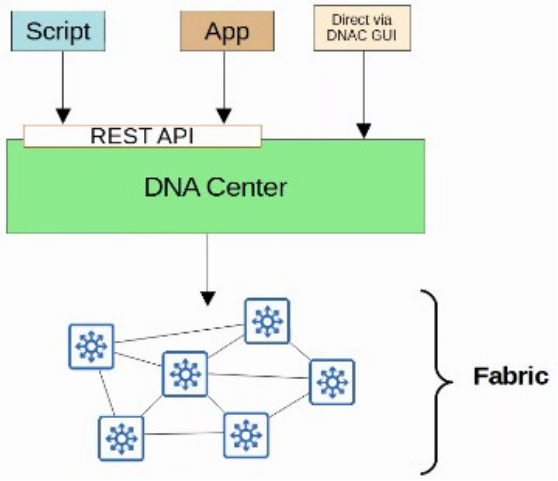


Ces 3 couches de l'architecture ont un nom, au dessus la couche application qui contient les scripts/applications qui disent au contrôleur SDN quelle comportement du réseau est désiré.
En deuxième niveau la couche de contrôle avec le REST API qui contient le contrôleur SDN qui reçoit et traite les instructions reçu par la couche application.
La dernière couche est la couche Infrastructure qui contient les appareils du réseau responsables de transmettre les messages sur le réseau Sur le schéma R1 et R2).

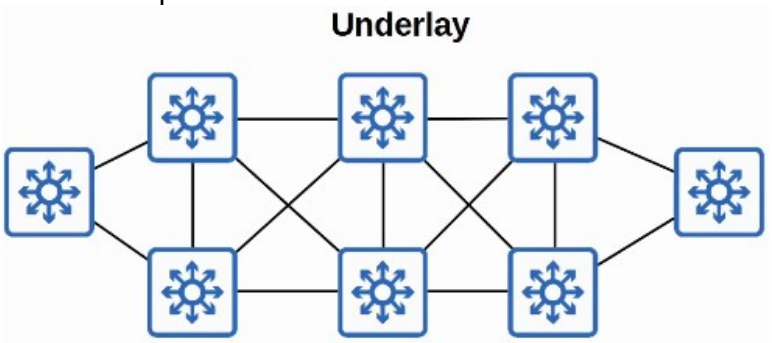
Cisco SD-Acces est une solution Cisco pour automatiser des LAN dans un campus.
ACI (Application Centric Infrastructure) est la solution SDN pour automatiser les centre de données d'un réseau. SD-WAN est la solution SDN pour automatiser des WAN.

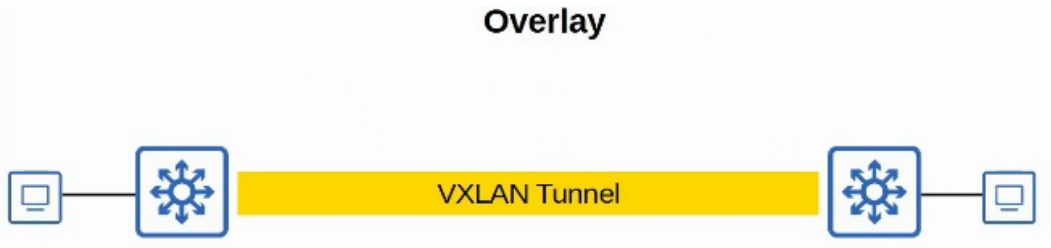
Cisco DNA (Digital Network Architecture) Center est le contrôleur au centre du SD-Access.

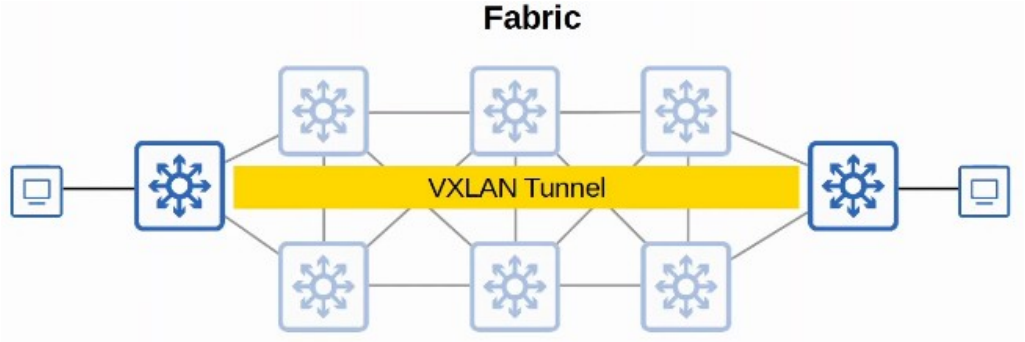
Voyons une architecture SD-Access basique :



Pour comprendre la « fabrique » ou appareil du réseau, il faut tout d'abord comprendre les dessous du réseau (underlay) physique des appareil et de leurs connexions (Incluant connexion câblé et sans fil) qui fournit une connectivité IP (par exemple en utilisant IS-IS).
Le Multilayer est constitué des Switchs et leurs connexions.
Le Overlay est le réseau virtuel construit au dessus du réseau physique underlay.
SD-Access utilise VXLAN (Virtual Extensible LAN) pour construire des tunnels.
La « fabrique » est la combinaison du overlay et du underlay, le réseau physique et virtuel tout entier.
Voici des exemples de ces concepts schématisé :



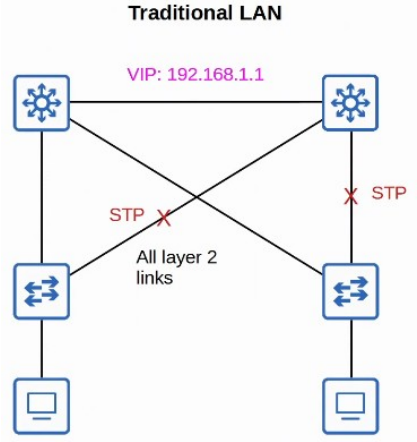




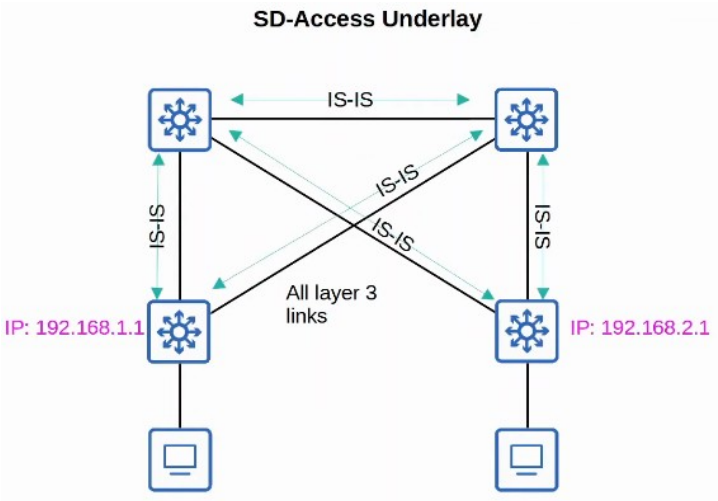
L’utilisation du underlay est conçu pour supporter les tunnels VXLAN du overlay.
Il y a trois différents rôles pour les Switchs dans le SD-Access :
- Edge nodes : connecte aux hôte finaux
- Border nodes : connecte aux appareils en dehors du domaine SD-Access par exemple le routeur WAN.
- Control nodes : utilise LISP (Locator ID Separation Protocol) pour faire fonctionner plusieurs fonctionnalités variés du plan de contrôle.

Il est possible d’ajouter SD-Access au dessus d’un réseau existant (brownfield deployment) si le matériel réseau et logiciel le supporte.
Dans ce cas DNA Center ne configure pas le underlay.
Un nouveau déploiement (greenfiel deployment) sera configuré par le DNA Center pour utiliser le SD-Access underlay :
- Tous les Switchs sont de couche 3 et utilise IS-IS pour protocole de routage.
- Tout est lié entre les Switchs et les ports de routage. Cela signifie que STP n’est pas nécessaire.
- Edge Nodes (Access Switch) fonctionnent comme passerelle par défaut de l’hôte final (couche de routage d’accès).

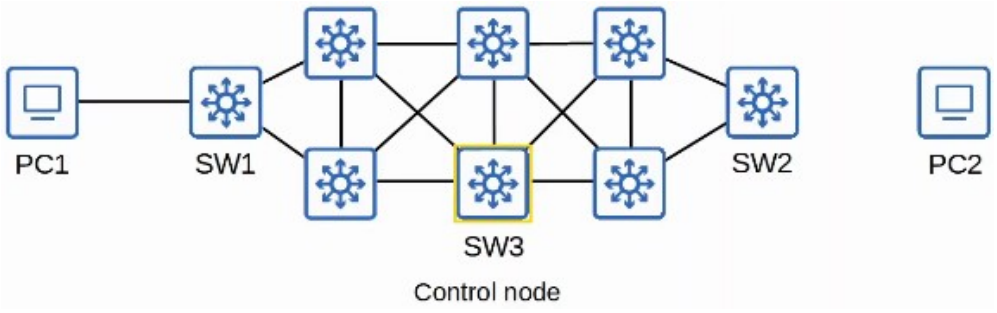
Un LAN Traditionnel se présente ainsi :
Pour envoyer des messages ils enverront vers le Virtual IP fournit par le FHRP (192.168.1.1) :



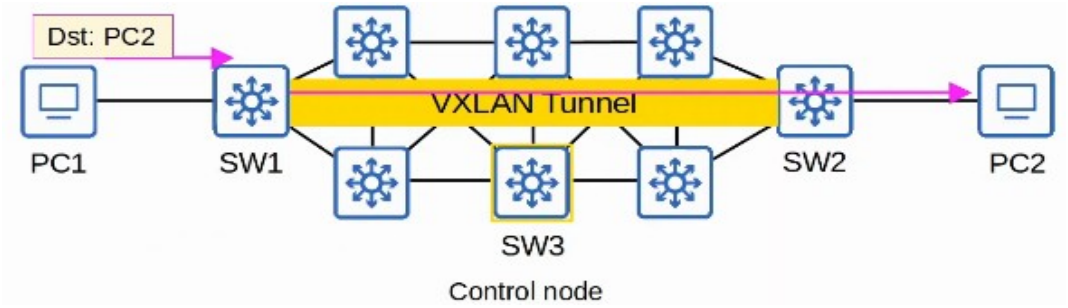
Dans un réseau SD-Access le fonctionnement est différent :
Les connexions entre Switch sont de couche 3 et IS-IS est utilisé pour échanger les informations.



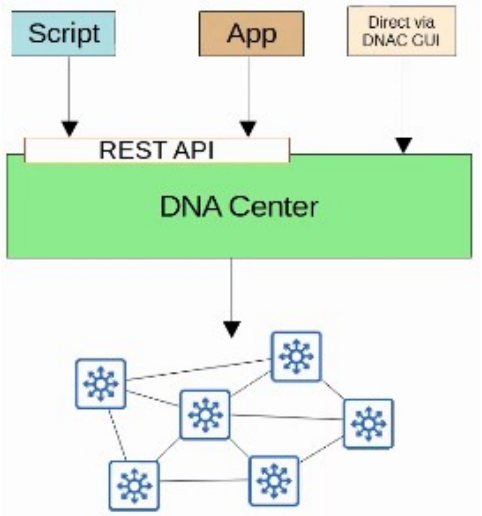
Le SD-Access Overlay est un autre concept différent.
LISP fournit le plan de contrôle au SD-Access, une liste de cartographie de EID (Endpoint Identifiers) vers le RLOC (localisation du routage) est conservé.
Les EID identifient les hôtes finaux connectés aux Switchs pont, et RLOC identifie le Switch pont qui sera utilisé pour joindre l'hôte final.
Il y a bien d'autres détails à propos de LISP, mais il possible de voir en quoi il diffère d'un plan de contrôle traditionnel.
Cisco TrustSec (CTS) fournit un contrôle des politiques (QoS, politique de sécurité, etc.)
VXLAN fournit le plan de données du SD-Access.
SW3 est le Control Node.



SW3 signal que PC2 est joignable par SW2.
PC1 souhaite joindre PC2, il envoie donc le message à sa passerelle par défaut (SW1), SW1 interroge SW3 de comment joindre PC2. Le SW3 lui répond que PC2 est joignable par SW2.
Le message de PC2 est donc transmis par un tunnel VXLAN entre SW1 et SW2.



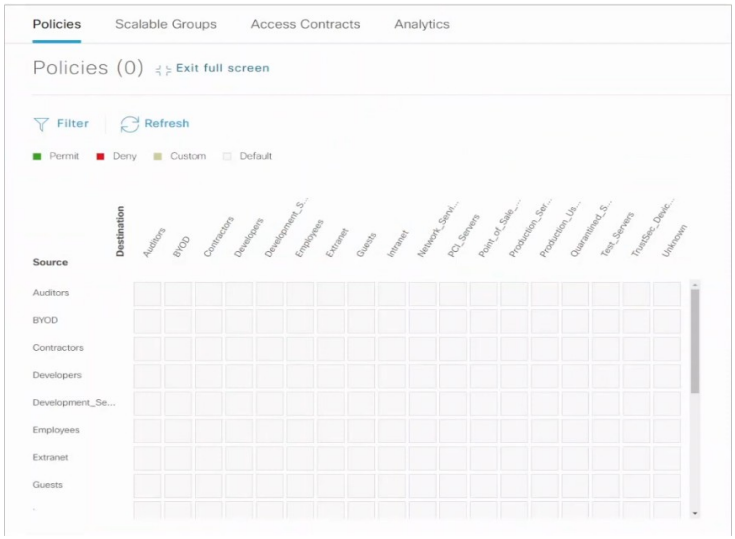
Le DNA Center a deux rôle principaux :
- C'est le SDN controller utilisé dans le SD-Access
- Un gestionnaire réseau dans un réseau traditionnel (Non SD-Access)



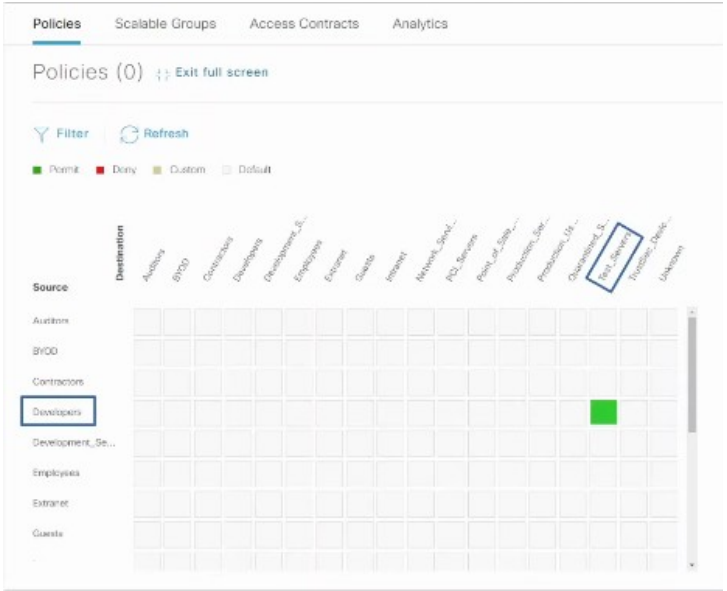
Un DNA Center est une application installé sur du matériel de serveur Cisco UCS
- DNA Center a un REST API qui peut être utilisé pour interagir avec le DNA Center
- Le SBI supporte des protocoles comme NETCONF et RESTCONF (Tout comme des protocoles traditionnels comme Telnet, SSH, SNMP)
- Un DNA Center active Intent-Based Networking (IBN)
Le but est de permettre à l'ingénieur de communiquer avec leur intention du comportement au DNA Center, le DNA Center fait attention aux détails de la configuration actuelle et des politiques des appareils.

Les politique de sécurité traditionnel utilisant ACL peuvent devenir très encombrantes.
Les ACL peuvent avoir des milliers d'entrées. L'objectif des entrées est oublié avec le temps et un ingénieur qui part d'une entreprise est remplacé par un autre ne connaissant par les ACL établit par l'ancien ingénieur.
Configurer et appliquer des ACL correctement à travers le réseau est encombrant et peut poser problème en cas d'erreur.

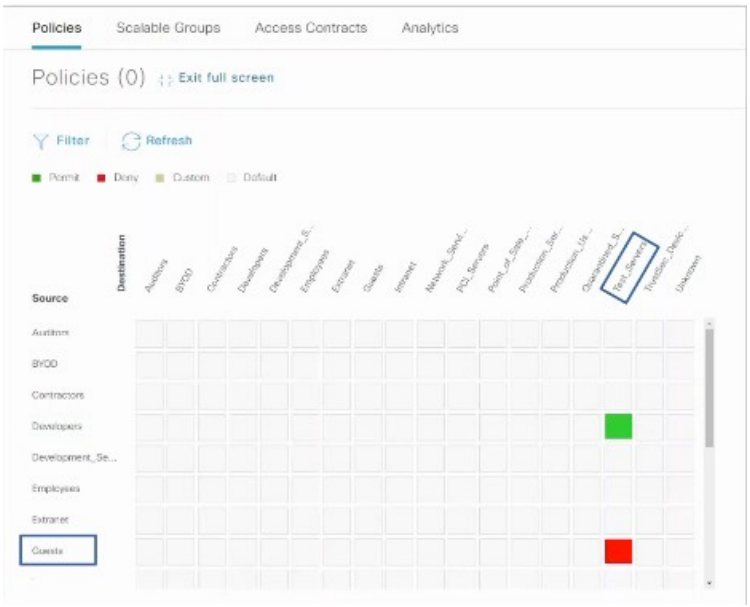
Le DNA Center permet à l'ingénieur de spécifier l'objectif de la politique (Ce groupe d'utilisateurs ne peuvent pas communiquer avec ce groupe, ce groupe peut accéder à ce serveur mais pas à tous les serveurs, etc.) Le DNA Center fera attention aux détails exact de l'implémentation de la politique.
Voici à quoi ressemble de configurer des politiques dans un serveur DNA :



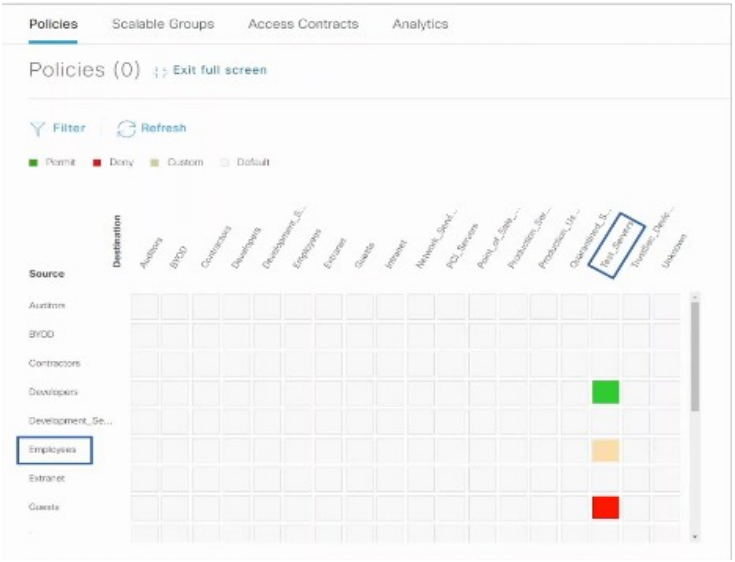
Si l'on veut configurer afin que les développeurs aient accès au Test_Servers on configure ainsi :



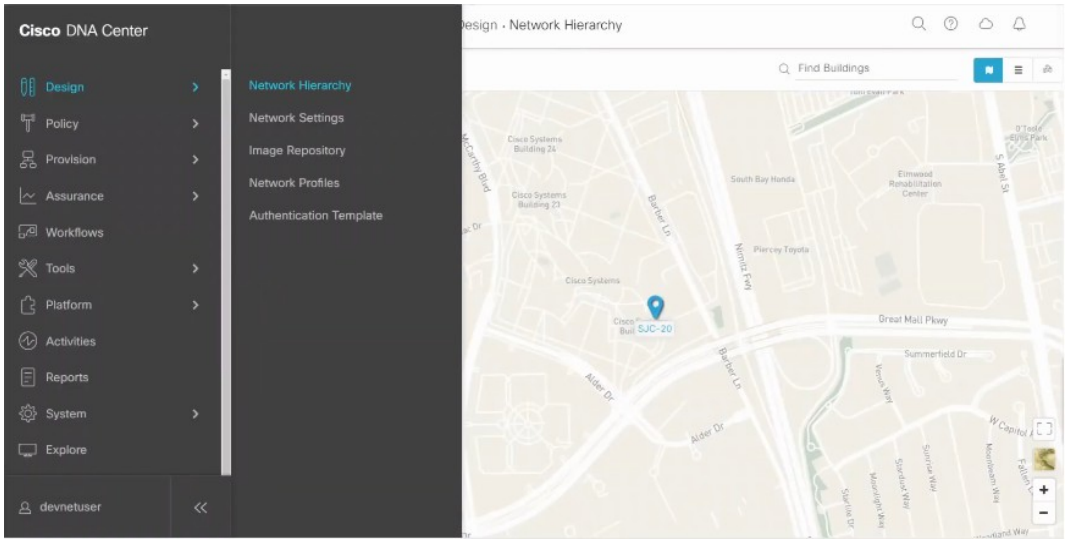
Si l’on veut bloquer le trafique des Guest pour Test_Servers on configure ainsi :



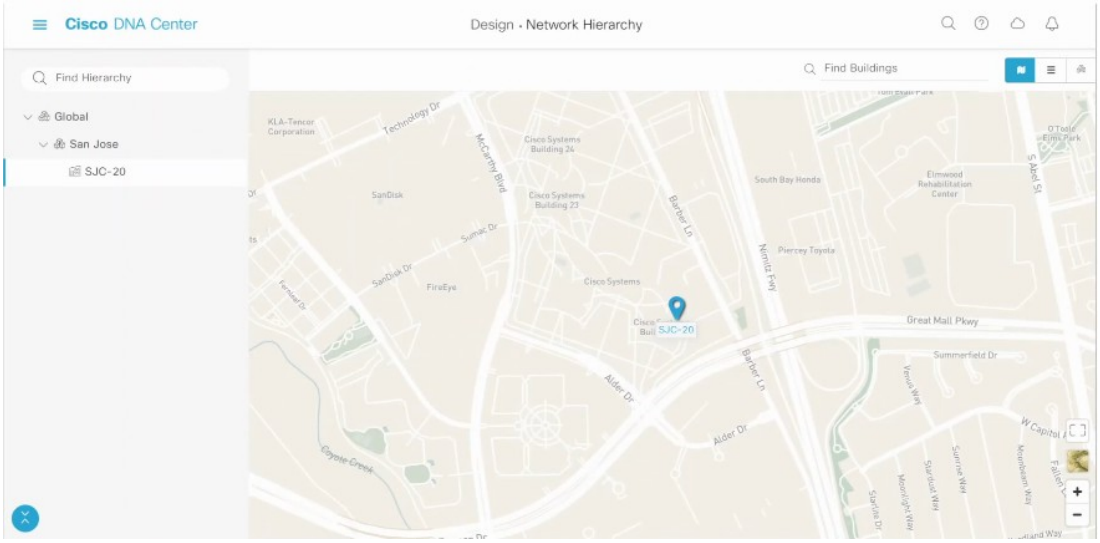
Pour personnaliser l’ACL employees et Test_Servers on configure ainsi :



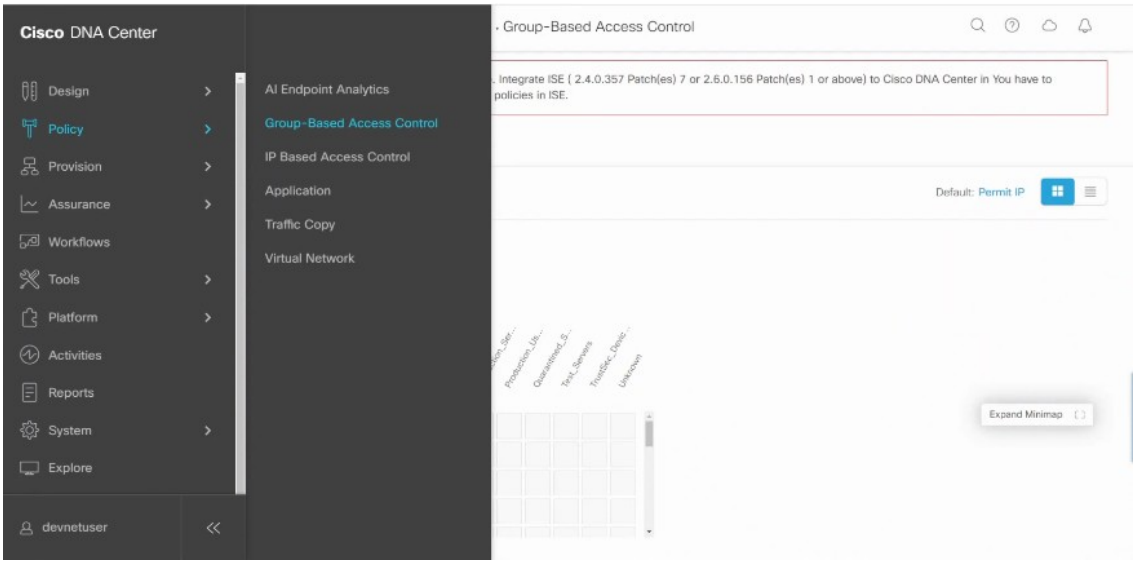
Voici à quoi ressemble le panel de connexion DNA Center :



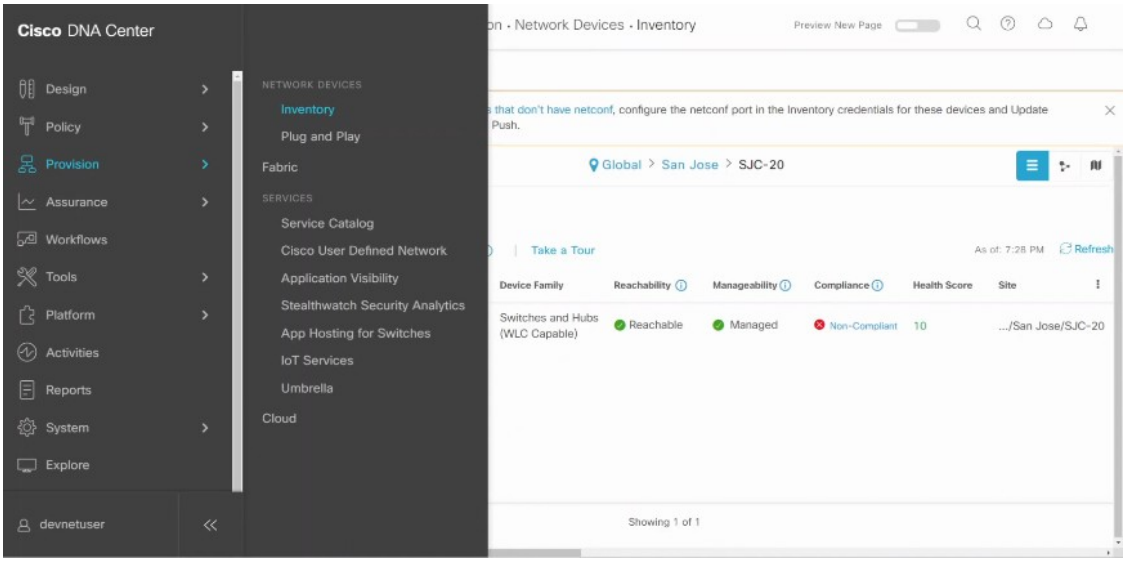
On peut cartographier le site de l’entreprise avec Cisco DNA Center :



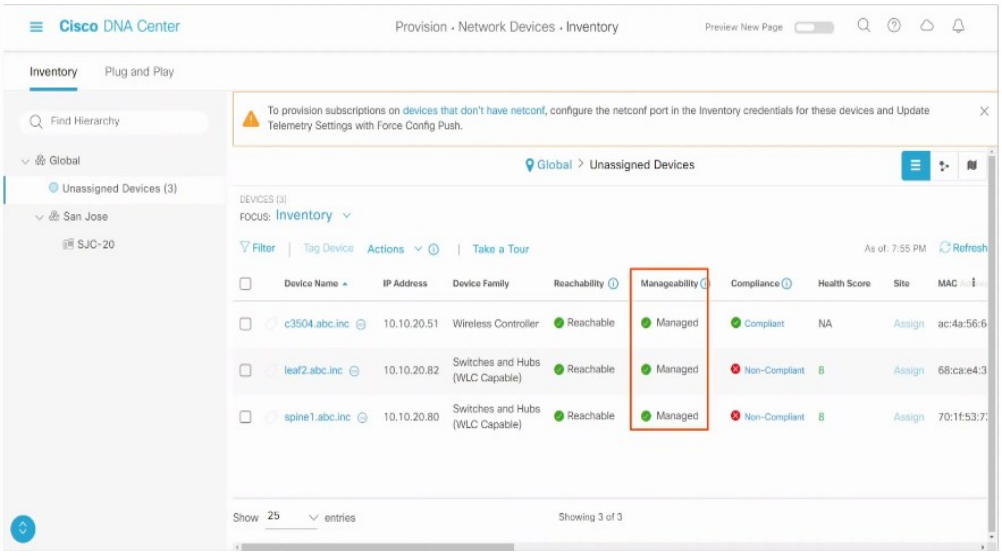
On configure la politique en accédant à Group-Based Access Control :



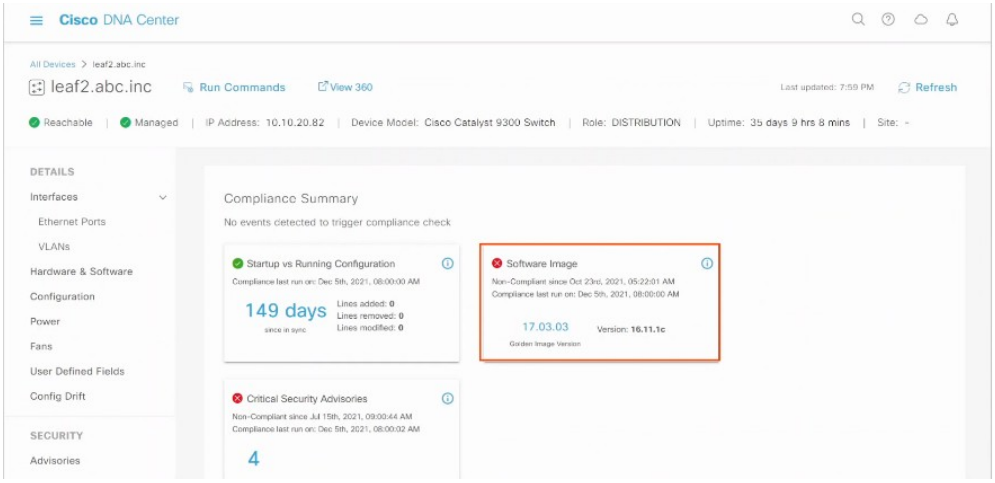
On peut accéder à l’inventaire des différents sites :



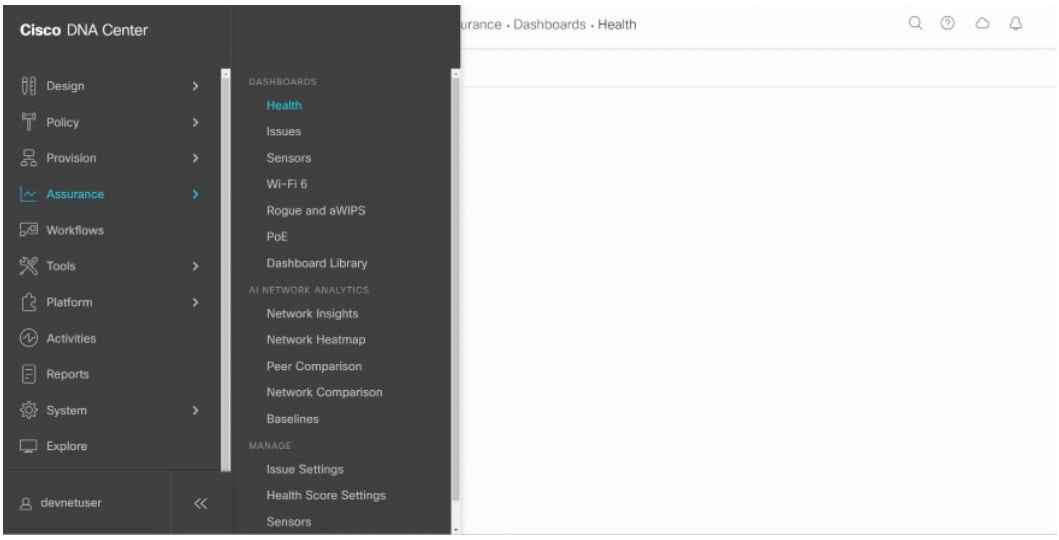
On peut par exemple voir les appareils qui ne sont pas assignés et adapter leur configuration pour qu'elle soit conforme :



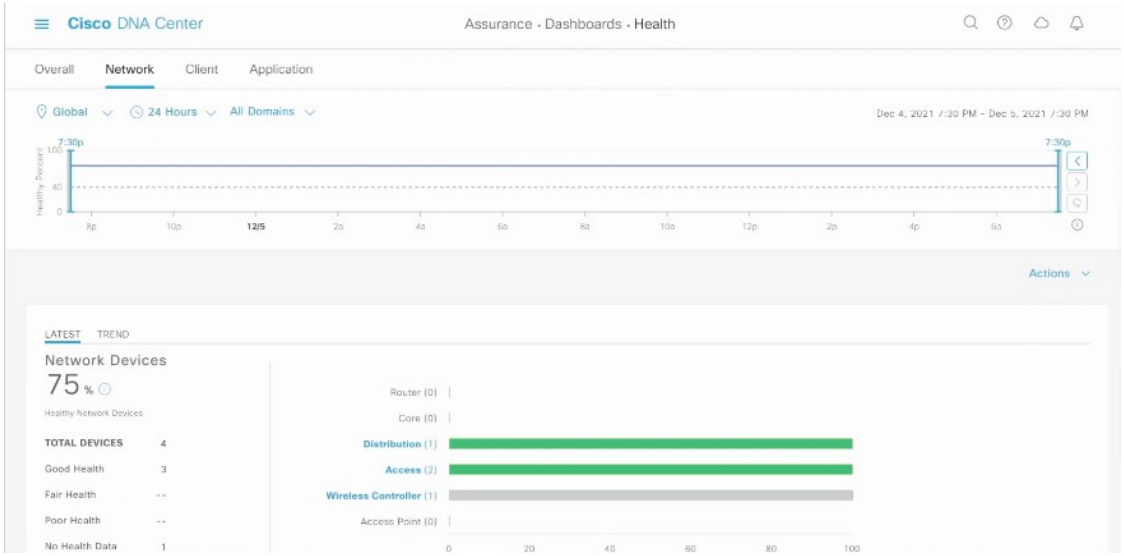
L'appareil par exemple n'a pas la dernière version de logiciel à jour :



Dans la section Health du menu on peut gérer le statut du réseau :



Voici un réseau considéré « en bonne santé » :



Faisons un comparatif entre un réseau réseau DNA Center et une gestion de réseau traditionnel :
- Dans la gestion d'un réseau traditionnel :
Les appareils sont configurés un à un par SSH ou une connexion console, Les appareils sont configurés par une connexion à la console avant d'être déployés.
La configuration et les politiques sont géré par appareil (distribué).
Le déploiement de nouveau réseau peut prendre un long moment à cause du laborieux manuel requis. Les erreurs et défaillances sont plus dû à l'effort manuel qui augmente.

- Dans la gestion d'un réseau DNA Center-Based :
Les appareils sont géré de manière centralisé et sont monitorés depuis un DNA Center GUI ou autres applications utilisant son REST API.
L'administrateur communique le comportement du réseau prévu au DNA Center, qui change leurs comportement avec les configurations et la gestion des appareils du réseau.
Les configurations et politiques sont géré de manière centralisé.
Les versions logiciel sont aussi géré de manière centralisés. Le DNA Center peut gérer le serveur Cloud pour de nouvelles versions et mettre à jour les appareils gérés.
Le déploiement de nouveau réseau est bien plus rapide, les nouveaux appareil peuvente automatiquement recevoir leurs configuration depuis le DNA Center sans que cela nécessite de configuration manuelle.