Institut Universitaire de Technologie,
Aix-Marseille Université

ANNEXES
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

Installation de salles IoT (Objets Connectés) en réseau pour le Master Réseaux & Télécommunications de Luminy

Adrien CAILLEAU-LEPETIT

UFR Sciences

Responsable entreprise : Didier TONNEAU

Responsable académique : Roland DEPEYRE

2021

Table des matières

Annexe n° 1

Documentation selon les recommandations de l'ANSSI

Auteurs :
- BOYER Alexis
- CAILLEAU-LEPETIT Adrien

Préface

Ce document a pour but de synthétiser les différentes normes de sécurité des réseaux, selon des critères fournis par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Son contenu concernera les principes de sécurité grâce aux firewalls, la sécurisation des réseau LAN (Local Area Network), ainsi que d'autres normes et protocoles pouvant être utiles. Cette documentation sera également accompagnée de différentes maquettes démontrant la mise en place des principes énoncés et leurs cas d'usage.
Tous les documents utilisés sont disponibles sur le site de l'ANSSI à cette adresse :
https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/reseaux/

Sommaire

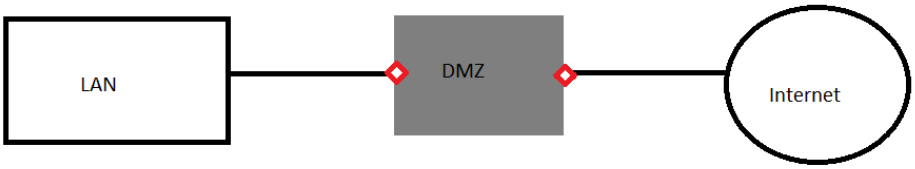
I – Pare-feu (firewall)

1 – Architecture

Dans le cadre d'une interconnexion à Internet que cela soit pour un particulier ou une entreprise, nous avons besoin d'un bouclier de protection, et ce bouclier est le firewall. Dans le cadre d'une entreprise un seul firewall n'est pas suffisant à la bonne protection des services informatiques, pour cela nous allons adapter cela selon une méthode recommandée par l'ANSSI, le concept d'une création d'une DMZ (DeMilitarized Zone).

1.1 – DMZ

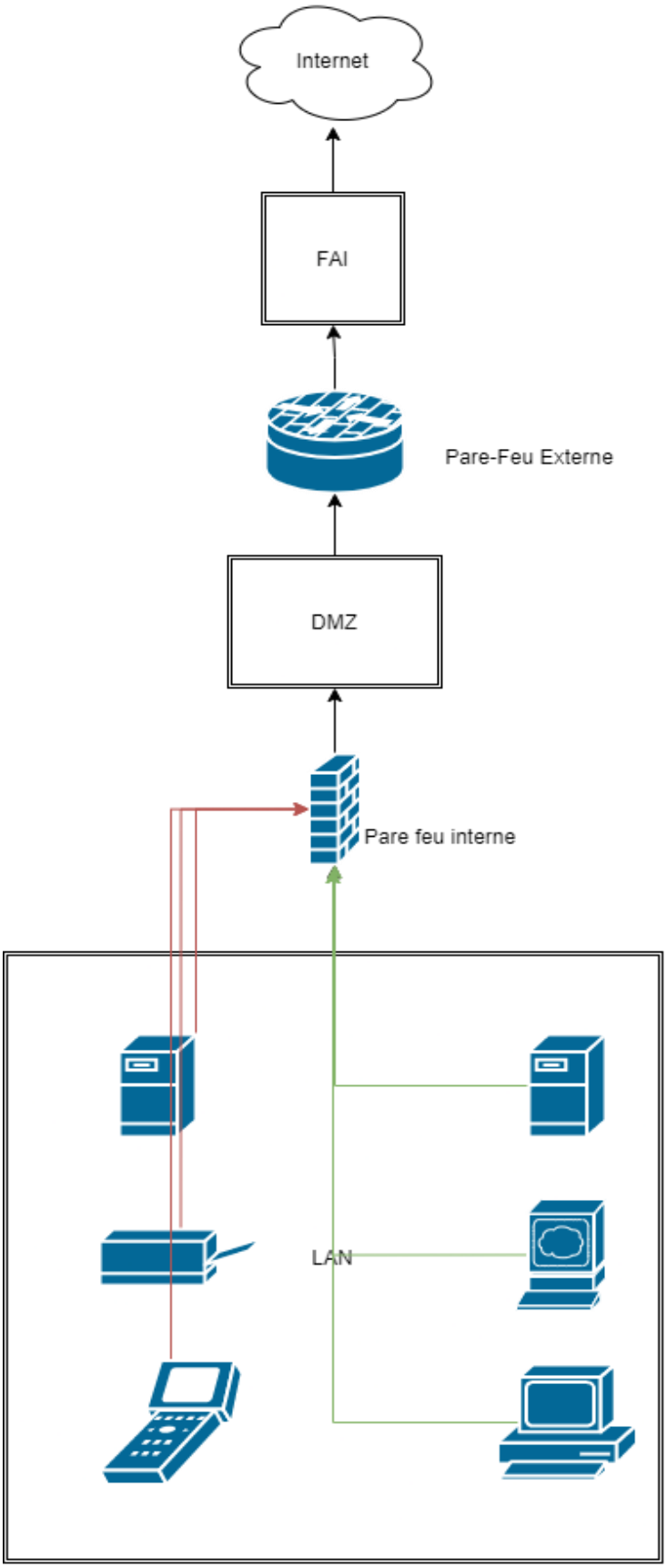
Quel est le principe d'une DMZ ? Son but est de créer une zone de protection entre l'accès internet et notre réseau LAN, comme le représente le schéma ci-dessous.



Pour donner suite à cet exemple, nous constatons que nous mettons 2 protections à notre lien avec internet, une à l'entrée de la DMZ et une autre à la sortie. Cette zone est la zone tampon des flux de notre réseau, tout transitera par cette zone. Mais nous savons que cette zone peut être compromise et remplaçable en cas de problème, contrairement à notre zone LAN.

1.2 – Filtrage et cloisonnement du réseau

L'accès à internet est fourni par un FAI (Fournisseur d'Accès Internet), il fournit également une mini-solution de firewall, cette solution est certes convenable pour un particulier, mais pour une entreprise il faut une entité de protection forte dès l'entrée de notre réseau. Il nous faut donc installer un firewall incontournable qui fait du filtrage IP.
Dans un second temps, en interne, il est important savoir quels serveurs et postes informatiques ont besoin de cet accès à internet afin de pouvoir filtrer et créer des sous réseaux internes, permettant de pouvoir savoir qui peut passer la passerelle interne. Cette zone est bien évidement obligatoire dans les flux du trafic. Le schéma ci-dessous montre un exemple de filtrage via notre DMZ.


Internet
FAI
Pare-Feu Externe
DMZ
Pare feu interne
LAN

Les pares-feux internes et externes doivent différer dans des cas de problèmes de sécurité lié à un pare-feu. Par exemple, on peut combiner des pares-feux matériels avec des pares-feux logiciels (ex : un pare-feu matériel Cisco avec un pare-feu logiciel pfsense). Il faut également se référer aux normes de sécurité relatives aux conseils de l'ANSSI sur le pare-feu.
Pour passer de la zone externe à la zone interne nous pouvons installer des serveurs relais qui communiquent avec ceux à l'intérieur, ce qui permet de limiter les risques de pertes de services des suites de tentatives d'attaques. Nous pouvons créer une zone sur différentes entités afin de pouvoir restreindre les accès, par exemple sur un serveur DNS, nous autorisons que le DNS à passer, pour un serveur de mail nous autorisons seulement ce qui est lié au mail. Cependant cela fait de nombreux firewall à gérer pour chaque solution. On peut en conclure qu'à minima, il faudrait au moins une DMZ pour une défense convenable de notre réseau d'entreprise, mais si l'on veut une défense maximale, il faudrait différents firewalls protégeant différentes instances ne filtrant que les zones applicatives dont nous avons besoin.

2 – Politique de filtrage des pares-feux

Précédemment, nous parlions de zones applicatives filtrées par des firewalls. Ici, nous allons expliquer plus précisément ces politiques appliquées à ces différentes zones.
L'ensemble de ces règles ont pour but de pouvoir filtrer au mieux le trafic et de pouvoir protéger le réseau interne. Il ne faut pas oublier de documenter et décrire toute politique de pare-feu pour aider à la maintenance système, à la restitution du pare-feu en cas de problème, et pour la transmission du flambeau dans la gestion des systèmes d'informations.

2.1 – Flux en destination du pare-feu

Ici, nous allons filtrer les services utiles à la gestion de notre pare-feu. Nous n'allons autoriser que les flux utiles à sa gestion, cela permet de réduire la surface d'attaque de notre pare-feu. Dans l'exemple, on suppose que nous avons accès à une interface CLI et une interface Web, donc nous allons autoriser le ssh et le https, mais si nous utilisons également de la supervision, nous allons autoriser les snmp-get afin de pouvoir avoir des informations sur notre réseau.

2.2 – Flux émis du pare-feu

Ici, nous allons voir ce que nous allons laisser passer par le pare-feu dans la gestion de notre réseau. Par exemple, dans le cadre de l'administration, nous allons laisser passer les syslog, les snmp-trap et le ssh. Ces services nous permettent d'avoir un retour de notre service d'administration si des problèmes sont présents sur notre réseau.

2.3 – Protection du pare-feu

Si nous n'avons pas besoin de certains services, la règle par défaut sera automatiquement **DROP**. Ce qui correspond à interdire le trafic, sans réponse de notre pare-feu.

2.4 – Autorisation des flux métiers

Ces règles ont pour but de restreindre les accès aux simples ressources que nous voulons demander et pouvons accéder, par exemple autoriser le trafic vers un simple serveur de fichier ou vers une page web interne.

2.5 – Règles antiparasites

Elles sont là pour filtrer les flux que nous ne voulons pas voir affichés dans la journalisation, par exemple les broadcasts qui peuvent polluer les logs. Cela permet un allègement des logs pour pouvoir les lire plus facilement en cas de problèmes.

3 – Règles de nettoyage des politiques de pare-feu

Dans le cadre de l'utilisation à long terme d'un même firewall, à de nombreuses reprises nous avons pu changer les politiques, tout aussi bien en ajouter ou en retirer. Nous allons voir comment nous

pouvons nettoyer nos politiques de pare-feu afin de pouvoir maintenir une méthode de gestion convenable.

3.1 – Nettoyage des objets

3.1.1 – Doublons

Dans l'utilisation de notre firewall, nous avons pu ajouter à de nombreuses reprises des politiques. Au fil du temps, nous pouvons avoir des politiques ayant des doublons, ce qui équivaut à retrouver une même adresse sur plusieurs règles. Nous pouvons donc compacter toutes ces règles en une seule ce qui facilite la gestion de cette règle en elle-même.

3.1.2 – Règles inutilisées

Nous pouvons également trouver des politiques inutilisées à la suite des potentielles modifications du réseau, nous pouvons avoir des anciennes politiques qui ne sont plus d'actualités. Il faut donc les enlever pour limiter la taille de la liste de filtrage et d'éviter les confusions.

3.1.3 – Règles redondantes

Une règle peut être redondante si une règle en amont autorise le même flux. Ces règles peuvent compromettre le réseau car elle ne colle plus à la rigueur mise plus en amont dans les règles de filtrage.

3.2 – Suppression des règles

La suppression des règles, qu'elles soient redondantes, désactivées ou inutilisées, devra être effectuée de façon méthodique. Nous ne devons pas affaiblir les performances ou la sécurité de notre réseau, ou bien désactiver la mauvaise règle.

3.2.1 – Suppression des règles inutilisées

Pour supprimer des règles inutilisées, nous devons premièrement marquer soigneusement toutes les règles avec la date de coupure, et définir un intervalle pour la suppression de ces règles afin de voir si le réseau reste autant performant qu'avant la désactivation/suppression de la règles. Mais il est tout aussi important de le faire morceau par morceau, afin d'identifier au mieux les problèmes potentiels en cas de suppression.

3.2.2 – Suppression des règles redondantes

Pour les règles redondantes, il est important d'étudier le cadre des règles. Si elles sont exactement similaires, une des deux règles peut être supprimée. Si la règle est assez proche mais reste redondante il faudra affiner pour pouvoir regrouper l'ensemble en une seule règle, et pouvoir supprimer les règles en trop par la suite.

II – Réseaux locaux

1 – Protection des commutateurs

Cette partie ne traite que des commutateurs (switchs) de desserte (couche d'accès). Il y a occasionnellement des références au RGS (Référentiel Général de Sécurité) de l'ANSSI disponible à l'adresse : https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_Corps_du_texte.pdf

1.1 – Administration et sécurité

1.1.1 – Réseau d'administration

Afin d'administrer des commutateurs, il faut donc privilégier l'utilisation d'un réseau d'administration, un flux de données distinct des autres avec un port physique dédié. Si cela n'est pas possible ou compliqué à mettre en place, l'utilisation d'un VLAN (Virtual Local Area Network) d'administration (différent du VLAN par défaut) peut très bien faire l'affaire, même si cette solution reste moins sécurisée que la première.

1.1.2 – Ports d'accès

Il existe plusieurs types d'interfaces d'accès aux commutateurs, mais nous ne nous concentrerons que sur les 3 suivantes :

- CTY (port console physique)
- VTY (port console virtuel)
- Interface web d'administration

Pour ces interfaces, les recommandations sont les suivantes :

- CTY : l'interface ne doit JAMAIS être désactivée, il s'agit du seul moyen de récupération ultime
- VTY : l'utilisation de telnet doit être proscrite, il est préférable d'utiliser SSHv2 avec une authentification par mot de passe ou par clé publique (voir annexe B du RGS)
- Interface web : proscrire son utilisation et supprimer les certificats créés par défaut pour son utilisation, elle augmente la surface d'attaque potentielle et ajoute des vulnérabilités au commutateur

Il est également conseillé de n'attribuer qu'UNE seule adresse IP (et un port) pour l'administration du commutateur et d'ajouter une règle de pare-feu (à défaut, une ACL (Access Control List)) afin de restreindre l'accès des ports d'administration seulement aux administrateurs. Afin d'éviter les attaques par bruteforce, il est recommandé d'utiliser une protection anti-bruteforce et d'activer la journalisation des authentifications et tentatives d'authentifications.

1.1.3 – Comptes d'administration

Pour des mesures de sécurité et de traçabilité, il est conseillé d'utiliser des comptes nominatifs (un compte pour une personne) pour les personnels ayant accès aux commutateurs. De même, il est recommandé de rester sur une logique de compte utilisateur et compte administrateur, l'attribution de droits spéciaux à des utilisateurs complique la gestion des comptes et peut mener à une faille. Par ailleurs, il est préconisé de supprimer ou désactiver les comptes présents par défaut, et de désactiver la fonction "enable" (qui permet aux utilisateurs d'accéder aux droits d'administration s'ils ont le mot de passe, et qui ne sert à rien aux comptes administrateurs).
Afin de gérer plus efficacement les comptes utilisés sur les commutateurs, la centralisation de ces comptes grâce à un annuaire est vivement conseillé. Cependant, la création d'un compte local de secours avec un mot de passe différent pour chaque équipement est une solution idéale en cas de dysfonctionnement de la connexion à l'annuaire ou de tout autre problème inopiné sur le commutateur.
Enfin, pour sécuriser les mots de passe des comptes, il est préconisé d'utiliser la méthode de chiffrement la plus robuste disponible sur les équipements (pour Cisco, chiffrement de type 5 MD5-salt) et de protéger les fichiers de configurations où les mots de passe chiffrés sont affichés (par exemple lors d'une capture d'écran ou d'un partage de configuration).

1.1.4 – Accès, mots de passe et bannière

Comme énoncé précédemment, il est préférable de centraliser les comptes sur un serveur distant. Il est important de configurer le contrôle d'accès distant sur toutes les lignes d'accès du commutateur (physiques et virtuelles), seul le compte d'administration de secours doit utiliser une authentification locale. Concernant le serveur de contrôle d'accès distant, il peut utiliser le protocole RADIUS ou TACACS+, le protocole TACACS+ étant le plus sécurisé.
Pour la création et la gestion des mots de passe, il faut regarder la section correspondante dans la PSSI (Politique de Sécurité du Système d'Information) en vigueur afin d'en connaitre les critères.
Il est également déconseillé d'utiliser une bannière de connexion (motd) sur les lignes d'accès du commutateur, celles-ci peuvent contenir des informations sensibles permettant à un acteur malveillant de cartographier le réseau et de cibler les équipements intéressants.

1.2 – Cloisonnement et VLANs

1.2.1 – Cloisonnement et configuration des VLANs

Par soucis de sécurité, l'idéal pour un cloisonnement des réseaux serait de le réaliser physiquement. Cependant, cela n'est pas toujours possible ou très compliqué à mettre en place. Pour pallier ce problème, on peut utiliser des VLANs, mais il faut faire attention à respecter une logique d'utilité et de simplicité pour segmenter son réseau, ainsi leur gestion n'en deviendra pas une tâche trop complexe.
Il est important de noter que l'utilisation des services de configuration automatique des VLANs envoient plein d'informations par rapport à votre réseau et des attaques peuvent cibler ce genre de services (services VTP, MVRP, GVCRP, DTP, ...). De même, il est crucial de forcer les modes de configuration (access et trunk) afin de ne pas laisser la possibilité aux commutateurs de choisir automatiquement, et éventuellement d'être victime d'une attaque.
Puisque l'on parle de cloisonnement, il faut faire en sorte de n'autoriser que le VLAN nécessaire sur un port donné lorsque celui-ci est en mode access, et s'il est en mode trunk, il est important de filtrer les VLANs devant passer par le trunk.

1.2.2 – VLANs spéciaux

1.2.2.a – VLAN de quarantaine

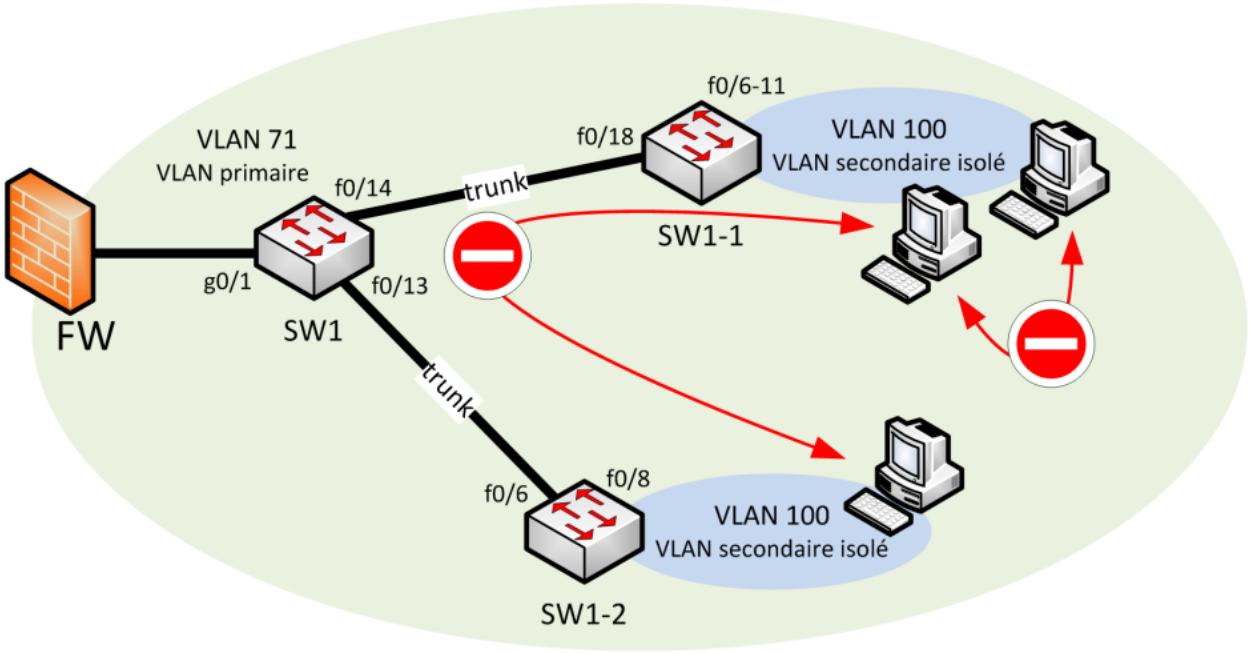
Pour améliorer le cloisonnement, il est fortement conseillé de créer un VLAN de quarantaine (différent du VLAN par défaut) et de l'attribuer aux ports inutilisés. Ce VLAN de quarantaine ne doit donner accès à strictement rien, pas même les autres équipements présents sur ce VLAN. Ensuite, il faut désactiver les ports inutilisés, ce VLAN de quarantaine et toutes les interfaces associées à celui-ci.

1.2.2.b – VLAN par défaut et VLAN natif

Le VLAN par défaut (généralement le VLAN 1) est celui attribué à tous les ports par défaut. Ce VLAN par défaut ne doit JAMAIS être attribué à un port et utilisé.
Le VLAN natif doit être obligatoirement différent du VLAN par défaut (puisqu'il ne faut pas l'utiliser), et ne JAMAIS être attribué à un port en mode access. Il est recommandé que le VLAN natif soit le même sur tous les commutateurs du domaine de diffusion (et du Système d'Information global de préférence) afin d'éviter les comportements inadéquats et pour garder une cohérence au sein du SI.

1.2.2.c – PVLAN (Private VLAN) et Protected Port

Le PVLAN permet d'ajouter un niveau de compartimentation au sein même des VLANs. Si cela est possible, il est conseillé d'utiliser des PVLAN en mode isolé pour restreindre les accès aux autres équipements partageant le même réseau si cela n'est pas nécessaire.



S'il n'est pas possible d'utiliser les PVLAN, il convient d'utiliser le Protected Port (ou Port Isolation) afin d'empêcher les machines sur un même commutateurs de communiquer entre elles.

1.3 – Routage

Les commutateurs de desserte sont censés seulement donner l'accès à un réseau, il faut donc désactiver tout mécanisme concernant le routage comme le routage interVLAN, les mandataires ARP et le source routing. Ces fonctionnalités seront gérées par des équipement de niveau 3 si besoin (sauf pour le source routing qu'il est conseillé de désactiver afin d'éviter les problèmes de sécurité).

1.4 – Sécurisation des ports

D'après les recommandations, il est important de désactiver les ports inutilisés et d'utiliser 802.1X (à défaut, utiliser port security).
Port security permet de mettre en place une limitation du nombre d'adresses MAC sur les ports physiques ainsi qu'un filtrage par adresse MAC pour n'autoriser que les appareils connus à se connecter au réseau.
802.1X permet une authentification du client connecté par un serveur RADIUS distant. Il est conseillé d'utiliser le le standard reposant sur EAP-TLS pour l'authentification des clients.

1.5 – Mécanismes liés à la disponibilité

1.5.1 – DHCP Snooping, IP Source Guard et Inspection ARP

Pour prévenir les attaques, il est crucial d'activer les fonctions de DHCP Snooping, d'IP Source Guard et d'Inspection ARP. En effet, ces contre-mesures sont efficaces pour éviter qu'un acteur malveillant réussisse à exploiter les faiblesses des protocoles DHCP et ARP.
Le DHCP Snooping sert à déclarer des ports de confiance de source DHCP, maintenir une table DHCP en temps réel et limiter le nombre de requêtes DHCP.
L'IP Source Guard quant à lui, vérifie la cohérence entre les adresses IP utilisées par les terminaux et la table DHCP en temps réel pour empêcher le "spoofing" d'adresses IP.
L'inspection ARP permet de contrôler l'homogénéité du contenu des trames ARP et de la table DHCP afin de prévenir les attaques de type ARP spoofing/poisoning.

1.5.2 – STP (Spanning Tree Protocol)

Concernant le protocole Spanning Tree, il est recommandé d'activer les protections BPDU Guard ainsi que le portfast (pour les commutateurs Cisco) sur les ports d'accès. Cependant, il faut faire très attention

à ne pas activer ces fonctionnalités sur des ports connectés à d'autres commutateurs, sous peine de voir un dysfonctionnement du réseau.

1.5.3 – Storm Control et protection contre les trames indésirables

Le Storm Control permet de limiter le traitement massif de trames broadcast, multicast et unicast, d'avertir et éventuellement couper temporairement l'accès à un port si une tempête (storm) de paquets est détectée. Il est intéressant à mettre en place pour améliorer la robustesse du réseau, il faut cependant faire attention à bien le configurer.
Cependant, le Storm Control ne prend en compte que les trames de 67 octets ou plus. Le small-frame arrival rate permet donc de limiter le nombre de trames de petite taille qu'une interface peut accepter par seconde.
Dans le même genre de mesures, il existe le PSP (Protocol Storm Protection) permettant de limiter le nombre de paquets par seconde pour les protocoles ARP, DHCP et IGMP.
Une autre mesure, nommé le port blocking, permet de bloquer les trames ne contenant pas de paquets IP (purement de niveau 2). Il peut s'avérer utile d'activer cette mesure pour limiter la pollution réseau de niveau 2 mais peut causer des dysfonctionnements au niveau du réseau dans certains contextes.

1.6 – Horodatage et journaux

1.6.1 – Synchronisation horaire et horodatage

Afin de garder une cohérence temporelle globale au sein du SI, il est conseillé d'utiliser un protocole de temps (ex : NTP) avec plusieurs sources dans le SI. Il est également recommandé de faire passer le flux de données pour le temps par un réseau différents de celui des métiers (par exemple le réseau d'administration ou un réseau autre réservé à ce cas).
Il est aussi très important d'activer l'horodatage des évènements sur tous les équipements du SI. Cela permet d'avoir les informations nécessaires pour maintenir une cohérence temporelle entre les évènements sans tenir compte de la localisation physique des équipements.

1.6.2 – Journalisation

Les journaux permettent de tenir compte des activités et des actions effectuées sur le commutateur, il est donc crucial de régler le niveau de journalisation en accord avec les besoins de journalisation du SI. Il peut être également utile d'activer l'envoi de ces journaux vers un serveur de collecte centralisé pour une meilleure gestion de ceux-ci. Cependant, les journaux peuvent contenir des informations sensibles, il est donc vital de faire passer ce flux par le réseau d'administration afin d'éviter la fuite de ces informations.
Il est possible que le commutateur perdre la connexion au réseau dans le cas d'un problème, il ne pourra donc pas envoyer ses journaux sur le serveur de collecte. Il est donc important d'activer le stockage local des évènements et adapter la taille maximale des journaux locaux en fonction du nombre d'évènements estimés nécessaires à enregistrer et à la taille du disque. De même, il est possible d'augmenter la taille du cache des journaux en cas de problèmes d'envoi, en faisant attention à ne pas trop impacter les performances du commutateur.
Les journaux peuvent aussi apparaitre sur la console, cependant il faut limiter le nombre d'évènements affichés pour éviter de perturber le fonctionnement du commutateur (plus d'évènements affichés entraine plus d'utilisation des ressources CPU).
Il est également vivement conseillé d'activer la journalisation des commandes entrées pour faciliter la découverte de la cause d'un problème qui surviendrait.

1.7 – Supervision SNMP

Dans le cas d'utilisation de SNMP en tant qu'outil de supervision réseau, il est préconisé d'utiliser SNMPv3 AuthPriv (à défaut, utiliser SNMPv2c) et de ne jamais utiliser snmp-set.
S'il existe, utiliser le service snmp-trap en mode inform, cela permet d'avoir confirmation de la réception de l'alerte. Il est également important de respecter les recommandations cryptographiques dans l'annexe B du RGS.

1.8 – Gestion du par cet MCO/MCS (Maintien en Condition Opérationnelle/de Sécurité)

Comme dans tout Système d'Information, il est vital de régulièrement mettre à jour ses équipements pour les protéger contre les vulnérabilités les plus récentes.
Il est également important d'homogénéiser les configurations (matérielles et logicielles) des commutateurs de son SI pour faciliter leur MCO/MCS, tout comme il est critique de vérifier la cohérence des configurations à chaque changement du SI afin d'éviter de mauvaises surprises. Il est aussi possible de mettre en place un système de vérification des configurations automatique.
Pour plus de praticité, il est également conseillé de centraliser l'administration des commutateurs et si possible d'utiliser des macros pour les opérations récurrentes afin d'éviter les erreurs de configuration.
Un autre aspect crucial à évoquer est la sauvegarde, elle est très importante dans un SI et permet de vite rebondir en cas de problème de configuration. Il est préconisé de mettre en place un système de sauvegarde des configurations distant et automatique sauvegardant régulièrement les configurations des équipements du SI. De plus, il est utile de tester régulièrement les procédures de restauration de ces configurations.

1.9 – Autres recommandations (agrégation de liens, fonctionnalités, disponibilité)

1.9.1 – Agrégation de liens (EtherChannel)

Il est recommandé d'utiliser l'agrégation de liens (EtherChannel ou Bridge Aggregation) pour augmenter la bande passante disponible ainsi qu'assurer une redondance des liens réseaux entre les commutateurs d'accès et de distribution.

1.9.2 – Protocoles à désactiver

Un commutateur est un équipement de couche 2 ne donnant que l'accès au réseau. Par conséquent, les fonctionnalités DNS, CDP et DHCP sont à proscrire pour ces appareils. Même si elles peuvent s'avérer utiles, elles sont soit superflues par rapport à la fonctionnalité principale du commutateur, ou transportent des informations sensibles sans chiffrement (notamment le protocole CDP).

1.9.3 – Disponibilité du système

Afin d'assurer une disponibilité maximale de ses équipements, il peut être utile de prendre des mesures préventives contre ces problèmes de disponibilité du commutateur en agissant au niveau des ressources mémoire et processeur.
Il est possible de mettre en place une supervision de l'utilisation des ressources du commutateur afin de détecter un possible dysfonctionnement, par exemple en envoyant un snmp-trap en cas de surutilisation des ressources.
Il peut également être intéressant de paramétrer un timeout pour l'établissement de connexions TCP afin d'éviter les attaques communes de déni de service (DoS, ici attaques de types SYN Flood).

2 – Sécurisation avec 802.1X (réseau à accès contrôlé)

2.1 – Composants d'un réseau local à accès contrôlé (802.1X)

2.1.1 – Composants

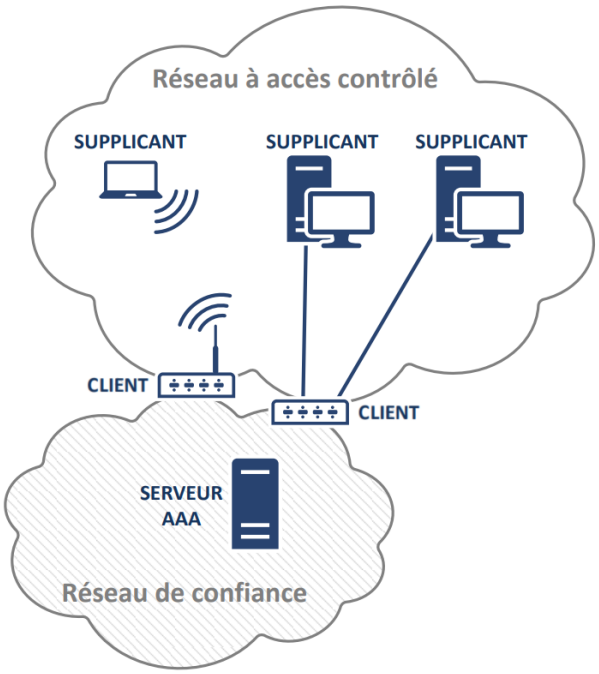
Pour l'installation d'un réseau local à accès contrôlé (802.1X), il faut mettre en place 2 réseaux :

- Un réseau à accès contrôlé où se connectent les appareils demandant l'accès au réseau
- Un réseau de confiance permettant l'échange des informations d'identification et d'autorisation d'accès

Selon cette même installation, on peut identifier 3 types d'équipements :

- **Serveur :** composant central d'un réseau 802.1X puisqu'il centralise les fonctions d'authentification et d'autorisation ainsi que la journalisation des évènements, il est connecté seulement au réseau de confiance

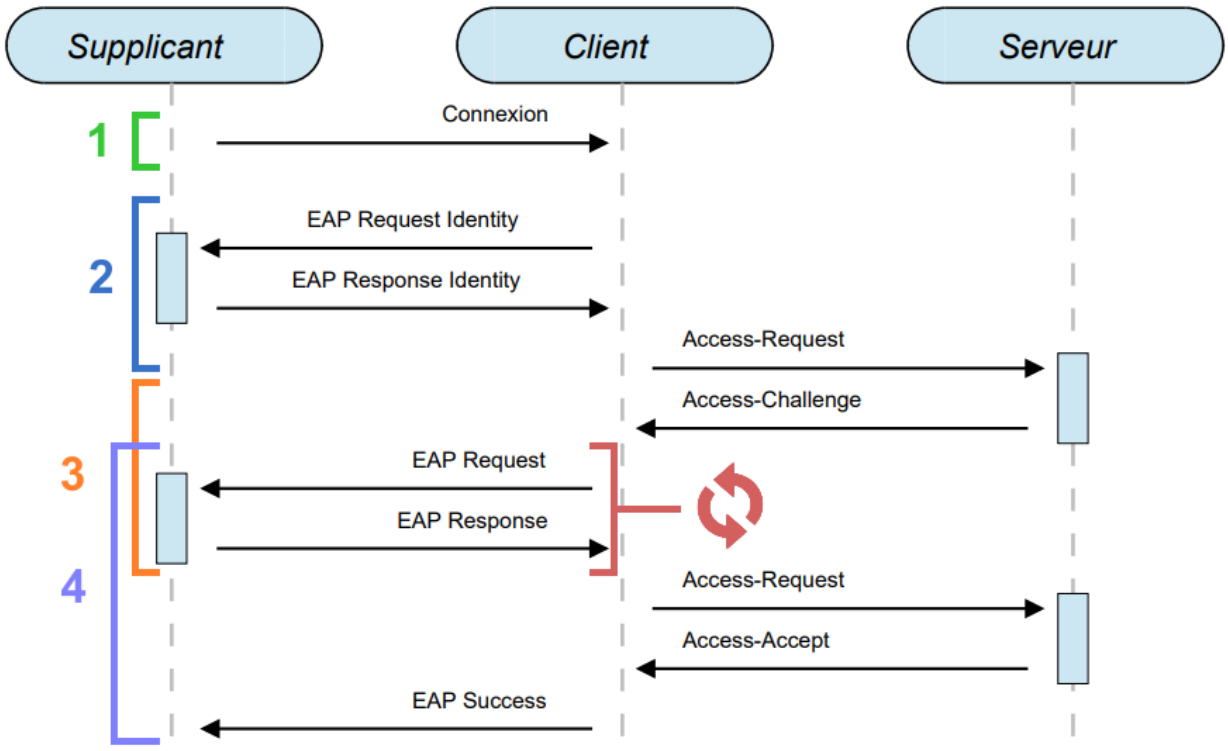
- **Clients :** commutateurs ou points d'accès wifi, ils sont à la fois connectés au réseau à accès contrôlé et au réseau de confiance et vont communiquer avec le serveur pour identifier le supplicant et autoriser l'accès au réseau contrôlé
- **Supplicants :** appareils demandant l'accès au réseau contrôlé, n'ayant aucun accès au réseau de confiance, ils s'identifient au serveur par l'intermédiaire d'un client



2.1.2 – Procédure de connexion à un réseau 802.1X

La connexion à un réseau 802.1X se fait en quatre grandes étapes :

- **Initialisation :** le client détecte le supplicant et passe le port en mode non autorisé
- **Identification :** le client demande au supplicant de s'identifier et le client passe l'identité du supplicant au serveur
- **Négociation EAP :** le serveur envoie un paquet avec la méthode d'authentification demandée au client à destination du supplicant, le client fait passer le paquet et le supplicant répond au client en lui disant s'il accepte, ou l'informe des méthodes qu'il supporte
- **Authentification :** le serveur et le supplicant échangent des paquets via le client en suivant la méthode d'authentification négociée auparavant, le serveur vérifie l'identité du supplicant et détermine s'il a le droit d'accéder au réseau. Si tel est le cas, le client bascule le port en mode autorisé, sinon il reste non autorisé



2.1.3 – Protocoles d'authentification

Dans une infrastructure 802.1X, l'authentification des supplicants repose sur le protocole EAP (Extensible Authentication Protocol). EAP définit plusieurs méthodes utilisables (et donc différents niveaux de sécurité).
Les méthodes EAP les plus courantes sont :

- **EAP-MD5 :** niveau de sécurité faible, ne permet pas d'authentifier le serveur et ne négocie pas de clés cryptographiques (impossible à utiliser pour les réseaux sans fil)
- **EAP-MSCHAPv2 :** niveau de sécurité faible, authentification mutuelle mais les défis cryptographiques sont faciles à craquer
- **EAP-TLS :** niveau de sécurité correct, authentification mutuelle par certificats (gestion de clés dans le SI)
- **EAP-PEAP :** niveau de sécurité correct, authentification mutuelle au travers d'un tunnel TLS grâce au certificat TLS du serveur, permet l'authentification du supplicant avec un couple identifiant/mot de passe ou par certificat
- **EAP-TTLSv0 :** niveau de sécurité correct, même principe que la méthode EAP-PEAP à la différence que les paquets échangés ne contiennent pas forcément une authentification EAP (par exemple : PAP, CHAP, MS-CHAP, ...)

2.2 – Déploiement avec 802.1X

2.2.1 – Authentification, autorisation et protocoles

Lors de la mise en place d'un réseau 802.1X, il est fortement recommandé d'authentifier les supplicants tentant de se connecter au réseau ainsi que d'avoir une liste exhaustive d'identité à autoriser côté server. De ce fait, cela limitera l'accès au réseau à des appareils inconnus. Il faut aussi faire attention à la cohérence de l'identité au cours des échanges entre les phases d'identification et d'authentification.
Les équipements contenant des éléments secrets, il est important de mettre en œuvre des mesures permettant d'assurer la confidentialité et l'intégrité de ceux-ci, que ce soit le serveur, les clients ou les supplicants. Il est également préconisé d'utiliser des protocoles d'authentification sécurisés. Afin de déterminer s'ils sont suffisamment sécurisés, il suffit qu'il respecte au moins les propriétés suivantes :

- Utilisation d'une couche cryptographique standard

- Authentification mutuelle entre le supplicant et le serveur
- Masquage de l'identité du supplicant durant la phase d'authentification (selon les besoins, critère optionnel)

D'après les conditions ci-dessus, il est grandement déconseillé d'utiliser des méthodes d'authentification non encapsulées. En effet, elles font transiter les données telles quelles qui peuvent ensuite être déchiffrées et lues par un acteur malveillant. Pour ne pas dégrader la sécurité du système mis en place, le serveur doit explicitement interdire les méthodes non encapsulées. Les méthodes en accord avec ces critères sont EAP-TLS, EAP-TTLS et EAP-PEAP. Les méthodes à proscrire sont donc EAP-MD5 et EAP-MSCHAPv2.
Concernant le protocole TLS, il est recommandé d'utiliser une version récente (supérieure ou égale à TLSv1.2) et une suite cryptographique robuste dont le protocole d'échange de clé assure une confidentialité persistante. Dès qu'un protocole d'authentification asymétrique (utilisation de clés privée/publique ou certificats), il est préférable d'utiliser un protocole générant les clés cryptographiques à partir d'éléments négociés pendant les deux authentifications, ainsi que d'utiliser une méthode interne qui génère des éléments partagés. Ci-dessous se trouve un tableau comparant les méthodes EAP communes les plus sécurisés.

		EAP-TLS	EAP-TTLS	PEAP	EAP-Double-TLS
Spécification		RFC 2716	Internet-Draft	Internet-Draft	Internet-Draft
Méthode d'authentification		Certificat X.509	Méthodes EAP, MS-CHAP, EAP-TLS		PSK, express, méthodes EAP
Structure basique		Etablissement d'une session TLS et validation de certificats des entités	Deux phases : - établissement d'une session TLS - échange de paires (attributs, valeurs) entre les entités	Deux parties : - établissement d'une session TLS - effectué une méthode EAP à l'intérieur du tunnel TLS	Deux phases : - établissement d'une session PSK - la 2ème phase est optionnellement établie afin de rafraîchir le triplet
Session résumée		Oui	Oui		Oui
Intégration du WEP		Oui	Oui		Oui
Certificat serveur		Requis	Requis		Optionnel
Certificat client		Requis	Optionnel		Optionnel
Vérification de la chaîne de certification		Oui	Oui		Optionnel
Conséquence de la compromission de la clé privée		Réémission de tous les certificats	Réémission le certificat du serveur et celle du client s'il est utilisé dans la 1ère phase		Réémission un simple nouveau triplet
Protection de l'identité du client		Non	Oui		Oui
Vulnérable à l'attaque *Man-In-The-Middle*		Non	Oui		Non
Nombre de Round Trip nécessaires		7.5	- 1ère phase : 7 (5 sans le certificat du client) - 2ème phase (ex. CHAP) : 2 - total : 9 (7 sans le certificat du client)	- 1ère phase : 7 (5 sans le certificat du client) - 2ème phase (ex. MD5) : 3 - total : 10 (8 sans le certificat du client)	1ère et 2ème phases : - 5.5 avec l'exécution du TLS sans certificats en 2ème phase - 3.5 avec CHAP - 4.5 avec MD5
Taille de données à échanger et à transférer		6.5 Ko	5.1 Ko + la taille des données de la méthode d'authentification utilisée à l'intérieur du tunnel		1.3 Ko
Opérations cryptographique asymétriques	client	1 signature, $(1 + x^a)$ vérifications et 1 chiffrement	$(1 + x^c)$ vérifications et 1 chiffrement		1 chiffrement
	serveur	1 déchiffrement et $(1 + y^b)$ vérification	1 déchiffrement		1 déchiffrement

a, b, c : les tailles des chaînes de certification

Tableau 5.2. Comparaison entre EAP-TLS, PEAP, EAP-TTLS et EAP-Double-TLS.

Source : Mohamad Badra, "Le transport et la sécurisation des échanges sur les réseaux sans fil", Page 88-89, Télécom ParisTech, 2004, https://pastel.archives-ouvertes.fr/pastel-00000952

Lorsqu'un réseau sans fil doit être mis en place, il est recommandé de déployer un réseau WPA2-Enterprise. Ce choix permet de contrôler l'authentification de chaque supplicant de façon indépendante et de bénéficier de protections cryptographiques robustes.

2.2.2 – Réseau de confiance

Le réseau de confiance transporte plusieurs types d'informations sensibles telles que :

- Les messages d'authentification et d'autorisation échangés entre les supplicants et le serveur
- La clé maitresse de protection utilisée entre le supplicant et une borne d'accès sans fil
- Les informations de journalisation échangées entre le client et le serveur

Afin de sécuriser au maximum ce réseau de confiance ainsi que ses équipements et les échanges, il faut agir à plusieurs niveaux.
Premièrement, il est important de renforcer la sécurité du serveur. Elément central du réseau 802.1X, il est critique de protéger ce service, notamment en durcissant la configuration du système sur lequel est installé le service RADIUS. Il est aussi recommandé d'implémenter le rôle de serveur sur une machine physique dédiée, ou un socle virtualisé hébergeant les services soumis à un niveau d'exposition, ainsi qu'à des besoins de sécurité identiques. De plus, il est fortement conseillé de disposer d'au minimum de deux serveurs afin de garantir la disponibilité du service.
Concernant le flux et les échanges, il est préconisé de cloisonner le réseau de confiance dans un réseau dédié, distinct des réseaux utilisateurs et d'administration et de protéger les équipements et câbles réseaux contre les intrusions. De plus, il est très fortement conseillé d'authentifier les clients auprès du serveur afin d'accéder au réseau de confiance, et d'utiliser un protocole de communication sécurisé afin d'assurer la confidentialité et l'intégrité des informations échangées sur le réseau de confiance. Afin d'assurer à minima l'intégrité des messages échangés entre le serveur et les clients, il est fortement recommandé :

- D'utiliser un secret partagé distinct par client
- De générer des secrets aléatoires d'au moins 22 caractères ASCII imprimables (majuscules, minuscules, chiffres)
- De superviser l'utilisation de ces secrets partagés, pour détecter toute utilisation anormale (authentification erronée d'un client, modification des fichiers de configuration, ...)
- De renouveler ces secrets sur une base régulière, afin de réduire la possibilité d'un attaquant à forger des trames intègres à destination du serveur en cas de découverte de l'un des secrets

Enfin, il est également préconisé de mettre en œuvre une fonction de journalisation des évènements générés par une infrastructure 802.1X, ainsi que de les superviser pour anticiper et répondre aux menaces.

2.2.3 – Affectation des VLANs

Pour plus de sécurité, il est important d'affecter statiquement les VLANs. Si cela n'est pas possible, il est possible de procéder à une affectation dynamique des VLANs (qui est plus sécurisé que l'absence de VLAN). En revanche, il faut faire bien attention à ce que les VLANs d'administration ne soient JAMAIS affectés dynamiquement.

2.2.4 – Limites du 802.1X

Comme pour toute technologie, 802.1X a ses limites concernant la sécurité. En effet, cette ne permet pas de protéger le SI contre toutes les menaces envisageables. Il y a cependant certaines contre-mesures permettant de limiter les potentiels dégâts.
Par exemple, il est recommandé de les configurer les équipements réseaux en autorisant les connexions en provenance et à destination d'une seule adresse MAC par port. Il est également conseillé de cloisonner et superviser les services offerts aux utilisateurs et d'authentifier leurs accès à ces services.
Concernant les appareils à connexion automatique au réseau 802.1X, il est recommandé de limiter au strict nécessaire les services offerts à ces appareils. De plus, il est indispensable de maîtriser la configuration des équipements se connectant légitimement à un réseau à accès contrôlé, afin d'assurer la sécurité du réseau et limiter les possibilités de connexion d'équipements non autorisés.

2.3 – Recommandations par cas d'usage

Pour rappel, voici les recommandations de l'ANSSI concernant 802.1X qui nous intéressent par rapport au schéma décisionnel :

R18 : Lutte contre les branchements de commutateurs

Il est recommandé de configurer les équipements réseaux pour qu'ils autorisent les connexions en provenance et à destination d'une seule adresse MAC par port.

R19 : Cloisonnement et supervision des réseaux utilisateurs

Il est conseillé de cloisonner et de superviser les services offerts aux utilisateurs et d'authentifier les accès à ces services.

R20 : Restreindre les services accessibles en authentification automatique

Il est recommandé de limiter au strict nécessaire les services offerts sur un réseau à accès contrôlé où les équipements se connectent de façon automatique.

R22 (renvoi R7) : Sécurisation d'un réseau local sans fil (Mise en place d'un réseau sans fil 802.1X)

Lorsqu'un réseau sans fil doit être mis en place, il est recommandé de déployer un réseau WPA2-Enterprise. Ce choix permet de contrôler l'authentification de chaque supplicant de façon indépendante et de bénéficier de protections cryptographiques robustes.

R23 : Déploiement dans des conditions maîtrisés

Lorsqu'aucun accès au réseau à protéger ne peut être atteint par un attaquant, l'application de la recommandation R18 sur la limitation du nombre d'adresses MAC autorisées est indispensable. Les accès brassés en avance et non utilisés doivent être traités avec précaution :

- Soit en désactivant l'apprentissage automatique de l'adresse MAC, ce qui nécessite une action d'administration avant le premier branchement
- Soit en déployant le protocole 802.1X

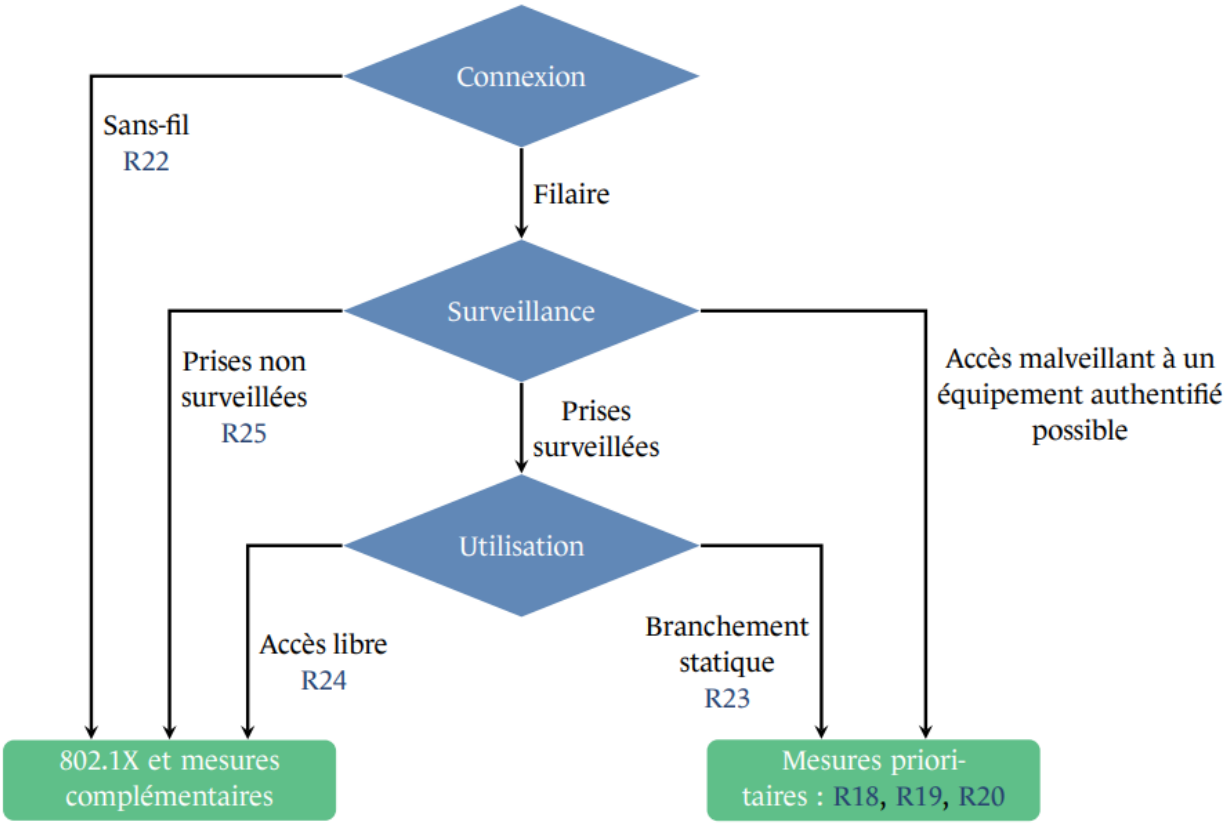
La décision de déploiement du protocole 802.1X est du ressort des équipes en charge de la sécurité du réseau à protéger, en fonction des contraintes métier et des services offerts.

R24 : Gestion des prises en accès libre

Il est recommandé de mettre en œuvre le protocole 802.1X sur les ports de connexion en accès libre aux collaborateurs. Dans ce cas, il est nécessaire d'appliquer la recommandation R17 portant sur l'affectation dynamique de VLAN et de se conformer aux recommandations du document "Recommandations pour la sécurisation d'un commutateur de desserte" (ou la grande partie précédente traitant de cette partie).

R25 : Connexion possible d'individus malveillants

Si la sécurité physique de certains accès au réseau à protéger ne peut pas être garantie, il est recommandé de déployer le protocole 802.1X pour restreindre son accès aux seuls équipements authentifiés.


Connexion
Sans-fil
R22
Filaire
Surveillance
Prises non surveillées
R25
Prises surveillées
Accès malveillant à un équipement authentifié possible
Utilisation
Accès libre
R24
Branchement statique
R23
802.1X et mesures complémentaires
Mesures priori-taires : R18, R19, R20

Annexe n° 2

Cahier des charges version 1

Introduction

Auteurs : Adrien Cailleau-Lepetit (ACL), Alexis Boyer (AB)
Nom du projet : Installation de salle réseau pour le Master Pro IoT
Description : Le projet a pour but de mettre en place des salles de TP pour le master pro IOT de Luminy. Nous devons mettre en réseau les salles pour fournir un accès internet au PC, mais également fournir un accès au serveur du datacenter de Luminy pour les données capteurs et les données caméra des TP.

Expression fonctionnelle du besoin

Informations globales

Il serait utile de prévoir un mécanisme de redondance physique ainsi que de configurer un réseau d'administration afin de faciliter l'accès aux équipements à distance.

Fonction 1 - Connexion des équipements

Description : Les équipements doivent être connectés au réseau selon différentes spécificités. Les ordinateurs sont fixes et ne seront pas déplacés une fois leur emplacement défini, cela signifie donc qu'ils auront chacun une prise réseau attribuée et qu'aucun autre équipement n'est censé pouvoir se connecter sur celles-ci. La même règle doit être appliqué sur le matériel utilisé pour les TP vidéo pour plus de sécurité. Concernant les capteurs ou tout autre objet connecté, des prises seront attribuées mais les appareils changeront assez régulièrement.
Critères :

- Connexion physique au réseau
- Connexion logique au réseau
- Sécurité

Fonction 2 – Accès vers l'extérieur

Description : Tous les appareils doivent pouvoir accéder à un serveur spécifique (à préciser) dans le datacenter de Luminy et seulement les PCs peuvent avoir un accès à Internet. Les objets connectés stockeront des données sur ce serveur et les PCs serviront à les récupérer. Les connexions seront sécurisées pour éviter l'interception des informations transmises.
Critères :

- Accès à Internet (pour les PCs uniquements)
- Accès au serveur dans le datacenter (pour tous les équipements)
- Sécurité des connexions

Fonction 3 – Sécurité du réseau

Description : Par mesure de sécurité, les flux de données doivent être différenciés les uns des autres et les appareils de type objets connectés ne doivent pas être en mesure de contacter un autre équipement à part le serveur du datacenter pour y stocker ses données. De plus, afin d'éviter les menaces, il serait idéal de filtrer les flux réseaux afin de déterminer lesquels sont légitimes et d'empêcher le trafic illégitime.
Critères :

- Protection contre les menaces internes et externes
- Protection des flux de données

Solutions techniques

Informations globales

Concernant la redondance physique, il est possible d'utiliser EtherChannel et d'utiliser deux prises physiques (TP4-10 & TP4-11) pour la connexion au réseau de la DOSI. Pour la partie administration, la configuration d'un VLAN dédié est à prévoir en cohérence avec les configurations de la DOSI.

Fonction 1 - Connexion des équipements

- Les connexions physiques des équipements seront établies via des prises Ethernet sur un commutateur (switch). Les prises avec un nombre pair seront les prises des PCs et les prises avec un nombre impair seront les prises pour les objets connectés (cependant, une exception sera faite pour le matériel vidéo afin de renforcer la protection de ces appareils).
- Concernant les connexions logiques au réseau, l'implémentation d'un service DHCP (ou l'utilisation d'un existant) est nécessaire. Le mieux serait un serveur DHCP de la DOSI afin d'attribuer des adresses en cohérence avec les autres réseaux si possible. De plus, il faudrait prévoir une solution de routage afin d'accéder au réseau interne de l'université.
- Afin d'éviter qu'un appareil illégitime se connecte au réseau, il est important de prévoir des protections comme un filtrage par adresse MAC ainsi qu'une identification et authentification (802.1X) pour les appareils destinés à rester fixes. Le flux des appareils seront séparés par des VLAN (Virtual LAN) qui seront attribués aux prises spécifiques. Nous prévoyons 3 VLANs : le VLAN X prévu pour les PC qui correspond au VLAN de l'université (géré par la DOSI), le VLAN Y prévu pour les capteurs et le VLAN Z pour les appareils des TP vidéo (sécurité renforcée).

Fonction 2 – Accès vers l'extérieur

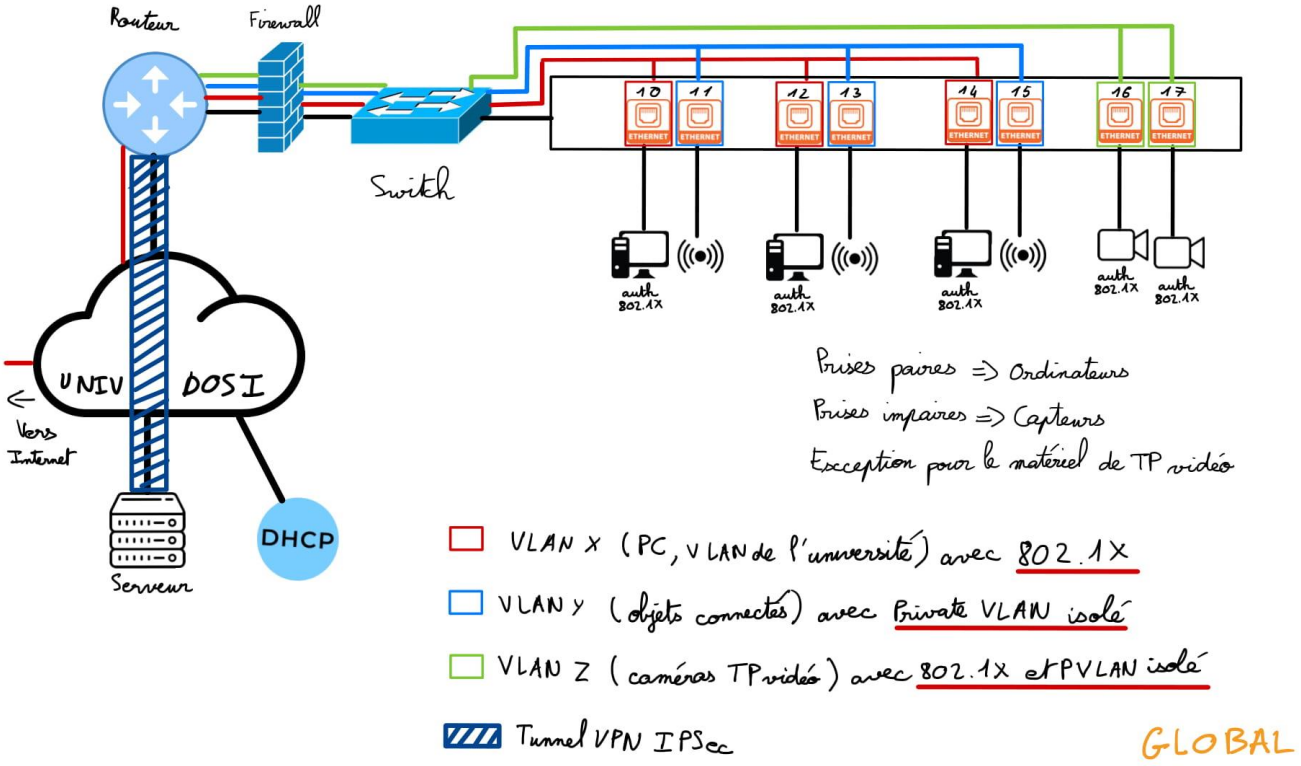
- Afin d'assurer la connexion à Internet des PCs, nous allons leur attribuer le VLAN de l'université fournissant cette connexion d'après la fonction précédente. De ce fait, seulement ces équipements auront un accès vers l'extérieur du réseau de l'université.
- L'accès au serveur dans le datacenter est un élément primordial, puisque les appareils devront souvent échanger des données avec celui-ci. Nous proposons donc d'utiliser un VPN IPSec pour fournir un accès direct sécurisé à ce dernier, cela permettra d'assurer la sécurité et l'intégrité des données qui transitent par ce tunnel.
- La sécurité des connexions sera assurée par le tunnel VPN pour l'accès au serveur, et par les protections de la DOSI pour l'accès externe au réseau de l'université.

Fonction 3 – Sécurité du réseau

- Afin de garantir la protection du réseau contre les menaces internes et externes, il est important de mettre en place un pare-feu (firewall). Nous prévoyons d'en mettre un juste avant le réseau interne afin de filtrer les flux internes au plus près et éviter la fuite d'informations et de contrôler les flux dans les deux sens.
- Les flux seront répartis dans différents VLAN selon les prises sur lesquelles les appareils sont branchés. Le VLAN ordinateur sera probablement géré par la DOSI afin de se soumettre aux normes de leur PSSI et leur permettre de maintenir ce réseau si besoin. Nous pensons qu'il est nécessaire d'appliquer une protection avec 802.1X (identification et authentification) afin de garantir la légitimité des appareils. Concernant les objets connectés, ils ne sont pas censés communiquer avec d'autres appareils sur le réseau, nous pensons que l'utilisation d'un PVLAN (Private VLAN) isolé peut être utile dans ce cas afin de renforcer la sécurité. Enfin, pour le matériel destiné au TP vidéo, nous préconisons l'installation d'un réseau 802.1X ainsi que l'utilisation d'un PVLAN isolé.

Annexe n° 3

Schéma de l'architecture version 1


Routeur
Firewall
Switch
10
11
12
13
14
15
16
17
ETHERNET
auth 802.1X
UNIV
DOSI
Vers Internet
DHCP
Serveur
Prises paires => Ordinateurs
Prises impaires => Capteurs
Exception pour le matériel de TP vidéo
VLAN X (PC, VLAN de l'université) avec 802.1X
VLAN Y (objets connectés) avec Private VLAN isolé
VLAN Z (caméras TP vidéo) avec 802.1X et PVLAN isolé
Tunnel VPN IPSec
GLOBAL

Annexe n° 4

Cahier des charges version 2

Introduction

Auteurs : Adrien Cailleau-Lepetit (ACL), Alexis Boyer (AB)
Nom du projet : Installation de salle réseau pour le Master Pro IoT
Description : Le projet a pour but de mettre en place des salles de TP pour le master pro IOT de Luminy. Nous devons mettre en réseau les salles pour fournir un accès internet au PC, mais également fournir un accès au serveur du datacenter de Luminy pour les données capteurs et les données caméra des TP.

Expression fonctionnelle du besoin

Informations globales

Il serait utile de prévoir un mécanisme de redondance physique ainsi que de configurer un réseau d'administration afin de faciliter l'accès aux équipements à distance.

Fonction 1 - Connexion des équipements

Description : Les équipements doivent être connectés au réseau selon différentes spécificités. Les ordinateurs sont fixes et ne seront pas déplacés une fois leur emplacement défini, cela signifie donc qu'ils auront chacun une prise réseau attribuée et qu'aucun autre équipement n'est censé pouvoir se connecter sur celles-ci. La même règle doit être appliqué sur le matériel utilisé pour les TP vidéo pour plus de sécurité. Concernant les capteurs ou tout autre objet connecté, des prises seront attribuées mais les appareils changeront assez régulièrement.
Critères :

- Connexion physique au réseau
- Connexion logique au réseau
- Sécurité

Fonction 2 – Accès vers l'extérieur

Description : Tous les appareils doivent pouvoir accéder à un serveur spécifique (à préciser) dans le datacenter de Luminy et seulement les PCs peuvent avoir un accès à Internet. Les objets connectés stockeront des données sur ce serveur et les PCs serviront à les récupérer. Les connexions seront sécurisées pour éviter l'interception des informations transmises.
Critères :

- Accès à Internet (pour les PCs uniquement)
- Accès au serveur dans le datacenter (pour tous les équipements)
- Sécurité des connexions

Fonction 3 – Sécurité du réseau

Description : Par mesure de sécurité, les flux de données doivent être différenciés les uns des autres et les appareils de type objets connectés ne doivent pas être en mesure de contacter un autre équipement à part le serveur du datacenter pour y stocker ses données. De plus, afin d'éviter les menaces, il serait idéal de filtrer les flux réseaux afin de déterminer lesquels sont légitimes et d'empêcher le trafic illégitime.
Critères :

- Protection contre les menaces internes et externes
- Protection des flux de données

Solutions techniques

Informations globales

Concernant la redondance physique, il est possible d'utiliser EtherChannel et d'utiliser deux prises physiques (TP4-10 & TP4-11) pour la connexion au réseau de la DOSI. Pour la partie administration, la configuration d'un VLAN dédié est à prévoir en cohérence avec les configurations de la DOSI.

Fonction 1 - Connexion des équipements

- Les connexions physiques des équipements seront établies via des prises Ethernet sur un commutateur (switch). Les prises avec un nombre pair seront les prises des PCs et les prises avec un nombre impair seront les prises pour les objets connectés (cependant, une exception sera faite pour le matériel vidéo afin de renforcer la protection de ces appareils). Concernant la connexion de la salle au commutateur de distribution, des tests de performance seront nécessaires afin d'évaluer le débit et d'éventuellement installer de nouveaux câbles (RJ45 CAT 6) pour atteindre une vitesse de transmission de données plus élevée. Afin d'assurer une grande performance ainsi qu'une redondance, il est intéressant de mettre en place une agrégation de lien (EtherChannel) via les ports 10 Gb entre les commutateurs des salles ainsi que le commutateur de distribution. De ce fait, cela créera une boucle de couche 2 assurant ainsi la connectivité des deux salles mêmes si certaines liaisons venaient à se rompre tout en assurant un débit correct.
- Concernant les connexions logiques au réseau, l'implémentation d'un service DHCP (ou l'utilisation d'un existant) est nécessaire. Ce service sera hébergé dans une machine virtuelle (VM) avec d'autres services réseau sur le serveur du master dans le datacenter de Luminy, mais temporairement disponible sur le commutateur. Ce service DHCP sera configuré d'après les spécifications (adressage) données par la DOSI.
- Afin d'éviter qu'un appareil illégitime se connecte au réseau, il est important de prévoir des protections comme un filtrage par adresse MAC ainsi qu'une identification et authentification (802.1X) pour les appareils destinés à rester fixes. Le flux des appareils seront séparés par des VLAN (Virtual LAN) qui seront attribués aux prises spécifiques. Nous prévoyons 3 VLANs : le VLAN X prévu pour les PC qui correspond au VLAN de l'université (géré par la DOSI), le VLAN Y prévu pour les capteurs et le VLAN Z pour les appareils des TP vidéo (sécurité renforcée). Pour mettre en place l'authentification 802.1X nous avons besoin d'utiliser un serveur Radius, qui sera hébergé dans la même machine virtuelle (VM) que le service DHCP. Afin d'héberger ces services à distance de manière sécurisée, il est possible d'utiliser une machine virtuelle standard ou des conteneurs type Docker afin de simplifier leur administration.

Fonction 2 – Accès vers l'extérieur

- Afin d'assurer la connexion à Internet des PCs, nous allons leur attribuer le VLAN de l'université fournissant cette connexion d'après la fonction précédente. De ce fait, seulement ces équipements auront un accès vers l'extérieur du réseau de l'université.
- L'accès au serveur dans le datacenter est un élément primordial, puisque les appareils devront souvent échanger des données avec celui-ci. Nous proposons donc d'utiliser un une double encapsulation (Q in Q) pour fournir un accès direct à ce dernier.

Fonction 3 – Sécurité du réseau

- Afin de garantir la protection du réseau contre les menaces internes et externes, il est important de mettre en place un pare-feu (firewall). Nous prévoyons d'en mettre un juste avant le réseau interne afin de filtrer les flux internes au plus près et éviter la fuite d'informations et de contrôler les flux dans les deux sens. Le firewall sera placé au niveau du switch de distribution et fera du routage afin de trier que nos propres flux réseau.
- Les flux seront répartis dans différents VLAN selon les prises sur lesquelles les appareils sont branchés. Le VLAN ordinateur sera probablement géré par la DOSI afin de se soumettre aux normes de leur PSSI et leur permettre de maintenir ce réseau si besoin. Nous pensons qu'il est nécessaire d'appliquer une protection avec 802.1X (identification et authentification) afin de garantir la légitimité des appareils. Concernant les objets connectés et matériel pour les TP vidéo, ils ne sont pas censés communiquer avec d'autres appareils sur le réseau, nous pensons que

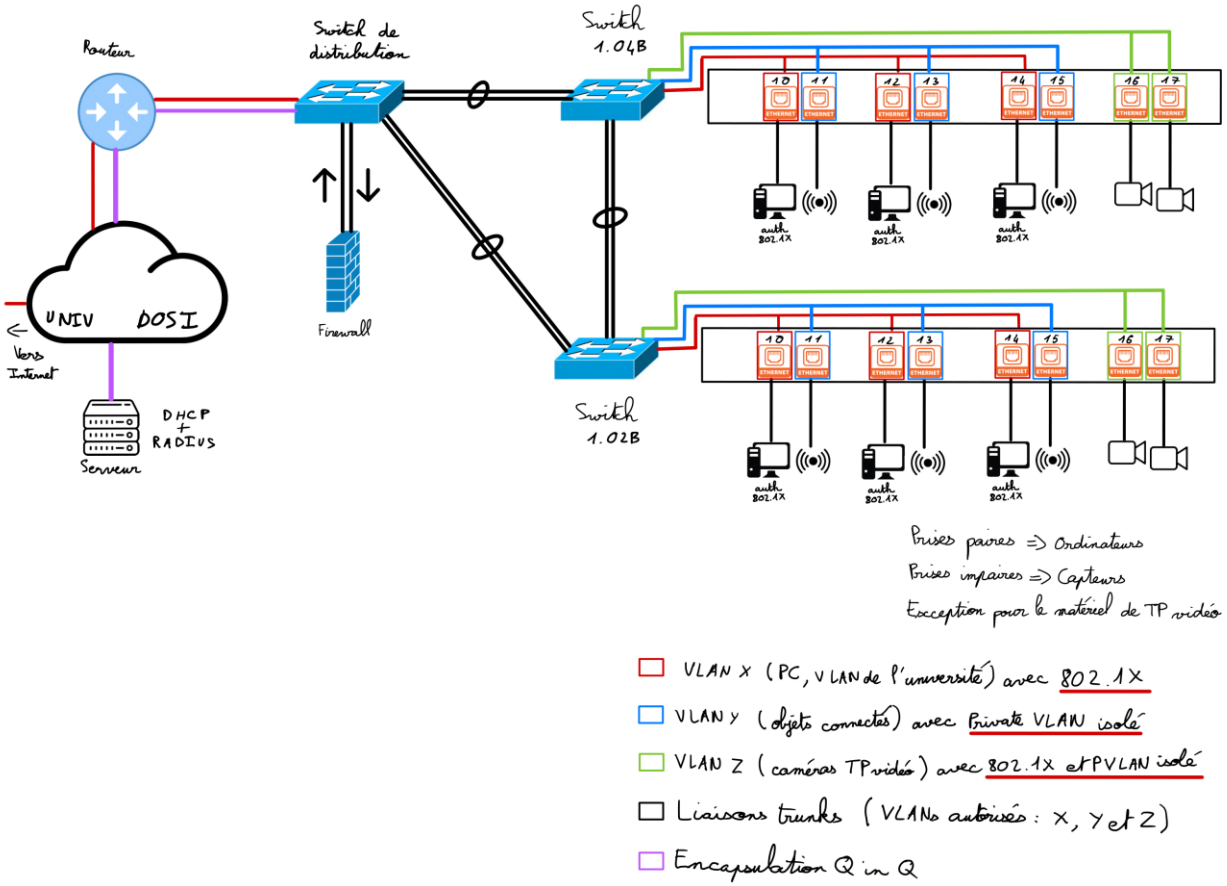
l'utilisation d'un PVLAN (Private VLAN) isolé peut être utile dans ce cas afin de renforcer la sécurité.

Switch proposé :

Cisco SG250X-48P : https://www.cisco.com/c/en/us/support/switches/sg250x-48p-48-port-gigabit-poe-4-port-10-gigabit-smart-switch/model.html

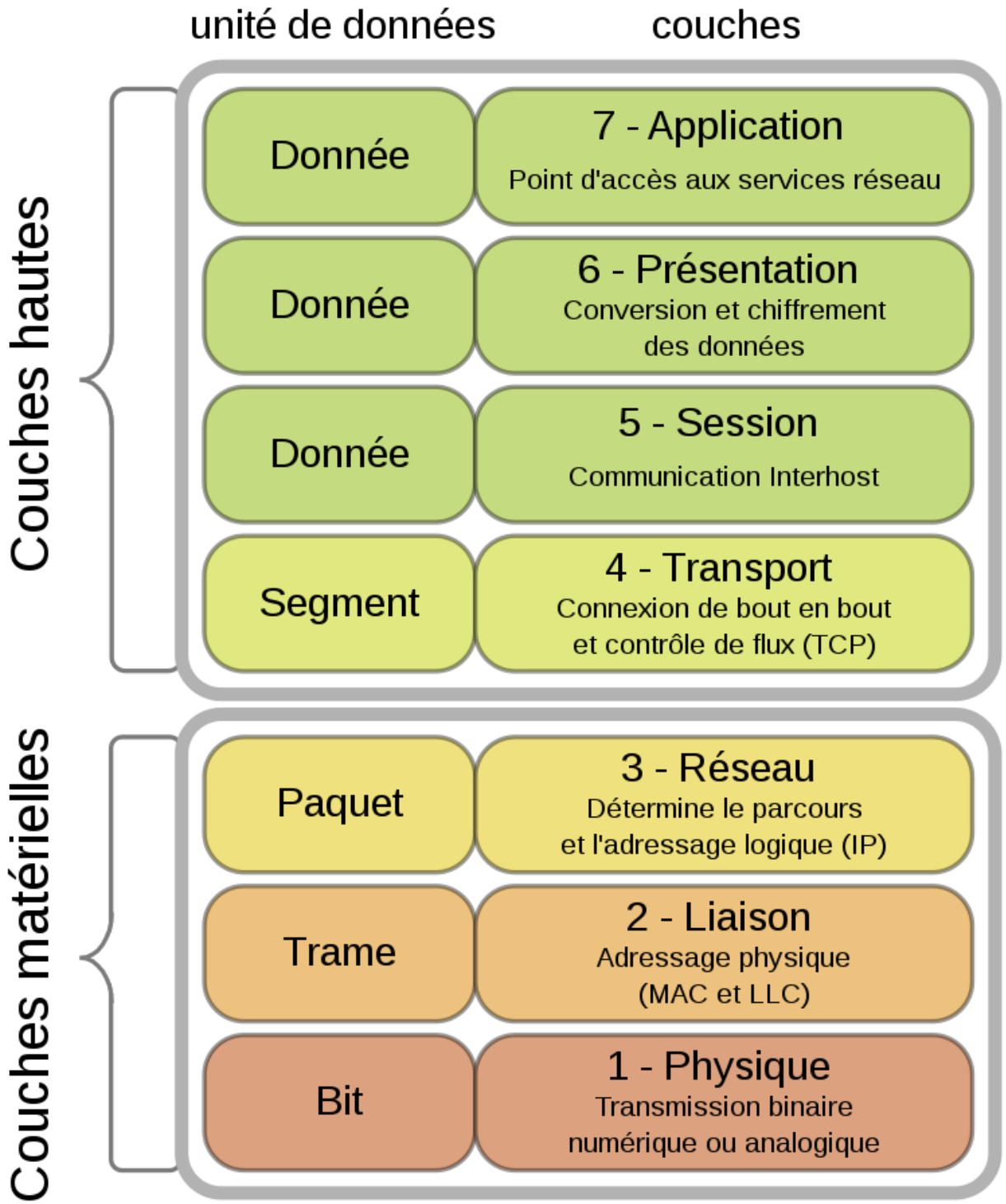
Annexe n° 5

Schéma de l'architecture version 2


Routeur
Switch de distribution
Switch 1.04B
Switch 1.02B
Firewall
UNIV DOSI
Vers Internet
DHCP + RADIUS
Serveur
auth 802.1X
Prises paires => Ordinateurs
Prises impaires => Capteurs
Exception pour le matériel de TP vidéo
VLAN X (PC, VLAN de l'université) avec 802.1X
VLAN Y (objets connectés) avec Private VLAN isolé
VLAN Z (caméras TP vidéo) avec 802.1X et PVLAN isolé
Liaisons trunks (VLANs autorisés : X, Y et Z)
Encapsulation Q in Q

Annexe n° 6

Modèle OSI


unité de données
couches
Couches hautes
Couches matérielles
Donnée
7 - Application
Point d'accès aux services réseau
Donnée
6 - Présentation
Conversion et chiffrement des données
Donnée
5 - Session
Communication Interhost
Segment
4 - Transport
Connexion de bout en bout et contrôle de flux (TCP)
Paquet
3 - Réseau
Détermine le parcours et l'adressage logique (IP)
Trame
2 - Liaison
Adressage physique (MAC et LLC)
Bit
1 - Physique
Transmission binaire numérique ou analogique